Peter Roquette *5. September 2020*

Transkription der Aufzeichnungen von Hasse über Klassenkörpertheorie

Die handschriftlichen Originale dieser Aufzeichnungen finden sich im Hasse-Nachlass in der Handschriftenabteilung der Universitätsbibliothek Göttingen. Leider habe ich dort keine Datums-Angaben gefunden. Es ist wahrscheinlich, dass es sich um die Ausarbeitung für die Vorlesung handelt, die Hasse im Sommersemester 1924 in Kiel gehalten hat. Er hatte dazu am 23.4.1923 an seinen akademischen Lehrer Kurt Hensel geschrieben:

„*. . . Außerdem habe ich gerade die Ausarbeitung eines Kollegs über die Klassenkörpertheorie von Takagi vor, die ich mit unseren Methoden sehr schön darstellen kann.*“

Mit „unseren Methoden“ meint Hasse die von Hensel geschaffenen p-adischen Methoden, deren Fortführung im Rahmen der algebraischen Zahlentheorie sich Hasse zum Ziel gesetzt hatte.

In jedem Falle sind diese Aufzeichnungen als Vorbereitung für den dreiteiligen „Klassenkörperbericht“ von Hasse anzusehen, der im Jahresbericht der DMV in den Jahren 1926, 1927 und 1930 erschienen ist. Daher dürften sie für die historische Forschung wohl von einigem Interesse sein.

Aufzeichnungen von Helmut Hasse zur Klassenkörpertheorie

---

^{tk} Klassenkörper
^{tk} L–Reihen mit Größencharakteren
^{tk} Reziprozitätsgesetz
^{tk} Existenzsatz/Strahlklassenkörper

t – fertig transkribiert, k – nach Tippfehlern durchgesehen

Version vom 24.10.2007
Letztmalig geändert am 24.10.2007

Quelltext: klk_071024.tex
übersetzt am 1. August 2009

Inhaltsverzeichnis

Übersicht

Vorbemerkung

Die Symbolfolge □□□ steht stellvertretend für Text, der von Hasse ausgestrichen wurde.[1]
Unleserlicher Text wurde durch `[...]` ersetzt.[2]
ſ steht für ein schwer lesbares Zeichen Hasses, das an zahlreichen Stellen, u. a. als unteres Argument im Normenrestsymbol, vorkommt.[3]
Hasses Fußnoten werden hier mit Symbolen ausgezeichnet, bei der Transkription hinzugefügte Fußnoten mit Ziffern.

[1] erreichbar mit `\boxes`
[2] erreichbar mit `\xxx`
[3] erreichbar mit `\y`

Teil I

Die Aufzeichnungen

Kapitel 1

Klassenkörper

Überblick

NB. Weiterarbeit hier *abgebrochen. Erst bei zweiter Bearbeitung in „L–Reihen mit Größencharakteren" §8 und „Existenzsatz/Strahlklassenkörper" abgeschlossen.*

1.1 Relativkörper und relativ–galoissche Körper

2 I

Es sei k ein algebraischer Zahlkörper vom Grade n und K ein algebraischer Körper über k. Der Grad von K in Bezug auf k sei r. Dann ist K ein algebraischer Körper vom Grade $M = nr$.

Der Grad r heißt der *Relativgrad* von K in Bezug auf k, die r in Bezug auf k konjugierten Körper $K, K^{(1)}, K^{(2)}, \ldots, K^{(r-1)}$ die *relativ konjugierten Körper* zu K. Die Normenbildung im Körper K an Idealen oder Zahlen werde mit N_K bezeichnet, im Gegensatz zu der Norm N in k. Bei N_K sind also alle $nr = M$ zu K konjugierten Körper in Betracht zu ziehen, deren r erste die relativ konjugierten sind. Die Ideale aus k mögen mit kleinen, die aus K mit großen deutschen Buchstaben bezeichnet werden. Die Ideale aus k liegen natürlich auch im Oberkörper K.

Ist A oder $\mathfrak{A}$ eine Zahl oder ein Ideal aus K, so heißen die entsprechenden, in den r relativ–konjugierten Körpern $K, K^{(1)}, K^{(2)}, \ldots, K^{(r-1)}$ liegenden Zahlen $\mathsf{A}, \mathsf{A}^{(1)}, \ldots, \mathsf{A}^{(r-1)}$ bezw. $\mathfrak{A}, \mathfrak{A}^{(1)}, \ldots, \mathfrak{A}^{(r-1)}$ die zu A bezw. $\mathfrak{A}$ *relativ–konjugierten*. Ihr Produkt heißt die *Relativnorm*, die mit $n(\mathsf{A})$, $n(\mathfrak{A})$ bezeichnet werde:

$$n(\mathsf{A}) = \mathsf{A}\mathsf{A}^{(1)} \ldots \mathsf{A}^{(r-1)}; \qquad n(\mathfrak{A}) = \mathfrak{A}.\mathfrak{A}^{(1)} \ldots \mathfrak{A}^{(r-1)}.$$

$n(\mathsf{A})$ und $n(\mathfrak{A})$ sind Zahlen bezw. Ideale aus k. Von $n(\mathsf{A})$ ist dies als symmetrische Funktion der Konjugierten klar. Wenn ferner F eine Form aus K mit dem Inhalt $\mathfrak{A}$ ist, ist $n(\mathfrak{A})$ der Inhalt von $F.F^{(1)} \ldots F^{(r-1)}$. Die Koeffizienten dieser letzten Form liegen aber als symmetrische

3 I

Funktionen relativ–konjugierter Zahlen in k.

Geht man von k zu einem konjugierten Körper k_i über, so geht die Gleichung in k für eine primitive Größe von K über in eine Gleichung in k_i. Das Produkt aller dieser n Gleichungen ist eine rationale Gleichung vom Grade $M = nr$, also *die* irreduzible Gleichung für alle nr konjugierten Größen unserer primitiven. Geht man also von k zu k_i über, so gehen die r konjugierten Körper $K, K^{(1)}, \ldots, K^{(r-1)}$ in die r anderen zu K konjugierten

$K_i, K_i^{(1)}, \ldots, K_i^{(r-1)}$ über und man erhält so jeden zu K konjugierten Körper. Daraus folgt leicht:

$$\mathsf{N}_K(\mathsf{A}) = \mathsf{N}\big(n(\mathsf{A})\big) \quad \text{und} \quad \mathsf{N}_K(\mathfrak{A}) = \mathsf{N}\big(n(\mathfrak{A})\big).$$

Ist $\mathfrak{P}$ ein Primideal in K und p die rationale Primzahl in der $\mathfrak{P}$ aufgeht, so muß p in einem und nur einem der verschiedenen Primidealfaktoren $\mathfrak{p}$ von p in k aufgehen. Man erhält also alle Primideale aus K, wenn man die aus k in K zerlegt.

Sei etwa $\mathfrak{p} = \mathfrak{P}\mathfrak{A}$; dann ist

$$n(\mathfrak{p}) = \mathfrak{p}^r = n(\mathfrak{P}) \cdot n(\mathfrak{A})$$

also $n(\mathfrak{P})$ eine gewisse Potenz $\mathfrak{p}^{\bar{\mathfrak{f}}}$. $\bar{\mathfrak{f}}$ heißt der Relativgrad von $\mathfrak{P}$ in Bezug auf k. Ist $\mathfrak{f}$ der Grad von $\mathfrak{p}$, so ist

$$\mathsf{N}_K(\mathfrak{P}) = \mathsf{N}\big(n(\mathfrak{P})\big) = \mathsf{N}(\mathfrak{p}^{\bar{\mathfrak{f}}}) = p^{\mathfrak{f}\bar{\mathfrak{f}}},$$

also $\mathfrak{f}\bar{\mathfrak{f}}$ der Grad von $\mathfrak{P}$ „*schlechthin*“. Ist ferner

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_\nu^{e_\nu},$$

und $\bar{\mathfrak{f}}_\mu$ der Grad von $\mathfrak{P}_\mu$, so folgt:

$$n(\mathfrak{p})\square\square\square = \mathfrak{p}^r = \mathfrak{p}^{\bar{\mathfrak{f}}_1 e_1 + \cdots + \bar{\mathfrak{f}}_\nu e_\nu}$$

also

$$r = \bar{\mathfrak{f}}_1 e_1 + \cdots + \bar{\mathfrak{f}}_\nu e_\nu \,.$$

Ist nun das Ideal $\mathfrak{a}$ aus k durch $\mathfrak{P}$ teilbar, so hat es mit $\mathfrak{p}$ einen Faktor in K, also auch in k gemein. Da aber $\mathfrak{p}$ Primideal, muß $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar sein. Es ist also $\mathfrak{p}$ selbst das kleinste Ideal aus k, das durch $\mathfrak{P}$ teilbar ist, somit der Durchschnitt von $\mathfrak{P}$ mit k.

Satz 1. Ist das in $\mathfrak{p}$ aufgehende Primideal $\mathfrak{P}$ gleichzeitig Teiler von $\mathfrak{a}$ aus k, so ist $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar. $\mathfrak{p}$ ist der Durchschnitt von $\mathfrak{P}$ mit k.

Es sei nun $\mathsf{N}(\mathfrak{p}) = q$ (eine Potenz von p) und der Relativgrad von $\mathfrak{P}$ (abweichend von der eben angew. Bezeichnung) $\mathfrak{f}$. Offenbar folgt aus der Kongruenz□□□

$$\square\square\square \qquad \alpha \equiv \beta \mod \mathfrak{p}$$

auch

$$\square\square\square \qquad \alpha \equiv \beta \mod \mathfrak{P}$$

aber nach Satz 1 auch umgekehrt (α, β Zahlen in k). Folglich können die Repräsentanten eines vollständigen Restsystems mod $\mathfrak{p}$ in k als Bestandteil eines vollständigen Restsystems mod $\mathfrak{P}$ in K genommen werden. Die Restklassen mod $\mathfrak{P}$ bilden dann ein Galoissches Feld der Ordnung $\mathsf{N}_K(\mathfrak{P}) = q^{\mathfrak{f}}$, welches das Galoissche Feld mod $\mathfrak{p}$ der Ordnung q in sich enthält. Jede Primitivzahl ϱ aus K mod $\mathfrak{P}$ genügt also mod $\mathfrak{P}$ einer in k irreduziblen (mod $\mathfrak{p}$) Kongruenz $\mathfrak{f}$–ten Grades, nämlich:

5 I

$$P(x) \equiv (x-\varrho)(x-\varrho^q)\cdots(x-\varrho^{q^{\mathfrak{f}-1}}) \equiv 0 \mod \mathfrak{P}.$$

Deren Koeffizienten in k liegen. $P(x)$ ist Primfunktion mod $\mathfrak{p}$.

Mit ihrer Hilfe kann jede ganze Körperzahl aus K nach dem Modul $\mathfrak{P}$ einer ganzen Funktion von ϱ kongruent gesetzt werden, mit ganzen Koeffizienten in k, höchstens vom Grade $\mathfrak{f}-1$.

Die Primitivzahl ϱ wählen wir geeignet so, daß $P(\varrho) \not\equiv 0 \mod \mathfrak{P}^2$ wird. Sollte dies für ϱ^* noch nicht zutreffen, so wähle man eine genau durch $\mathfrak{P}^1$ teilbare Zahl π. Dann ist $\varrho = \varrho^* + \pi$ wieder Primitivzahl mod $\mathfrak{P}$, doch ist

$$P(\varrho) \equiv P(\varrho^* + \pi) = P(\varrho^*) + \pi P'(\varrho^*) \not\equiv 0 \mod \mathfrak{P}^2$$

□□□

da $P(\varrho^*) \equiv 0 \mod \mathfrak{P}$, aber $P'(\varrho^*) \not\equiv 0 \mod \mathfrak{P}$ ist, weil ja $P(x)$ Primfunktion ist. Aus demselben Grunde ist auch das Absolutglied von $P(x)$ nicht durch $\mathfrak{p}$ teilbar, also prim zu $\mathfrak{p}$. Ist nun $\mathfrak{p} = \mathfrak{P}^e\mathfrak{A}$, wo $\mathfrak{A}$ zu $\mathfrak{P}$ prim ist, so bestimmen wir eine durch $\mathfrak{A}$ teilbare zu $\mathfrak{P}$ prime Zahl α. Dann ist

$$\alpha^{\Phi_K(\mathfrak{P}^2)} \equiv \alpha^{q^{\mathfrak{f}}(q^{\mathfrak{f}}-1)} \equiv 1 \mod \mathfrak{P}^2$$

Ersetzen wir also x durch $\varrho^* = \varrho\alpha^{\mathfrak{q}^{\mathfrak{f}}(\mathfrak{q}^{\mathfrak{f}}-1)}$, so ist in $P(\varrho^*)$, □□□ nach Potenzen von ϱ entwickelt, jeder Koeffizient durch $\mathfrak{A}$ teilbar, mit Ausnahme des letzten der zu $\mathfrak{p}$ also auch zu $\mathfrak{A}$ prim ist. Es ist daher $P(\varrho^*)$ prim zu $\mathfrak{A}$. Ferner ist

$$\varrho^* \equiv \varrho \mod \mathfrak{P}^2$$

also

$$P(\varrho^*) \equiv P(\varrho) \not\equiv 0 \mod \mathfrak{P}^2 \qquad \text{aber} \equiv 0 \mod \mathfrak{P}.$$

6 ı

Folglich ist der größte gemeinsame Teiler von $P(\varrho^*)$ und $\mathfrak{p}$ genau $\mathfrak{P}^1$. Ist also ϱ^* eine Primitivzahl, wie wir sie eben bestimmt haben und $P(x) \equiv (x-\varrho)\cdots(x-\varrho^{\mathfrak{q}^{\mathfrak{f}-1}})$ wo ϱ Primitivzahl nach $\mathfrak{P}$, sodaß $P(\varrho) \equiv 0 \mod \mathfrak{P}$ aber $\not\equiv 0 \mod \mathfrak{P}^2$, so gilt:

$$\mathfrak{P} = \big(\mathfrak{p}, P(\varrho^*)\big)$$

oder wenn π_0 eine durch $\mathfrak{p}$ teilbare Zahl aus k ist, sodaß $\frac{P(\varrho^*)}{\mathfrak{p}}$ prim zu π_0 ist,

$$\mathfrak{P} = \big(\pi_0, P(\varrho^*)\big).$$

Beim Beweise der Irreduzibilitätssätze für die Fundamentalgleichung etz. im gewöhnlichen algebraischen Körper über dem rationalen Körper wird lediglich von der Tatsache Gebrauch gemacht, daß die Restklassen nach p ein Galoissches Feld bilden. Diese Sätze gelten also unverändert in jedem Galoisschen Feld, speziell also für den hier vorliegenden Fall des Relativkörpers zu k, wo die Restklassen mod $\mathfrak{p}$ ein Galoissches Feld bilden.

Sei $\omega_1, \omega_2, \ldots, \omega_M$ eine Basis aus K und

$$\Xi = U_1\omega_1 + \cdots + U_M\omega_M$$

eine Fundamentalform von K. Die Gleichung

$$F_r(X, \Xi) = (X-\Xi)(X-\Xi^{(1)})\cdots(X-\Xi^{(r-1)})$$

liegt in k und heißt die *Fundamentalgleichung* von K in Bezug auf k.

Mit Hilfe unserer Primitivzahl ϱ (die wir kurz mit ϱ bezeichnen) können wir, da jede ganze Zahl aus K einer ganzen Funktion in k von ϱ mod $\mathfrak{P}$ kongruent ist, etwa schreiben:

7 ı

$$\Xi = L(\varrho; U_1, U_2, \ldots, U_M) = L(\varrho \mid U_i) \bmod \mathfrak{P}$$

(indem wir die ω_i durch ϱ ausdrücken).

Wir bilden dann den Ausdruck

$$\Pi(X; U_i) \equiv \big(X - L(\varrho \mid U_i)\big(X - L(\varrho^q \mid U_i) \cdots \big(X - L(\varrho^{q^{\mathfrak{f}-1}} \mid U_i)\big) \bmod \mathfrak{P}$$

Ist $\varrho = \mathsf{A}_1\omega_1 + \cdots + \mathsf{A}_M\omega_M$, so wird, wenn $U_i = \mathsf{A}_i$ gesetzt wird:

$$\Xi(\mathsf{A}_i) \equiv \varrho \mod \mathfrak{P}$$

Da nun ersichtlich

$$\Pi(\Xi \mid U_i) \equiv 0 \mod \mathfrak{P}$$

ist, muß

$$\Pi(\varrho \mid \mathsf{A}_i) \equiv 0 \mod \mathfrak{P}$$

sein. Nun hat $\Pi(x \mid \mathsf{A}_i)$ den gleichen Grad wie $P(x)$. Da $P(x)$ den niedrigsten Grad in k hat, (der für eine solche Beziehung vorkommen kann), muß

$$\Pi(x \mid \mathsf{A}_i) \equiv P(x) \mod \mathfrak{P}$$

sein. Daß die Koeffizienten von $\Pi(x \mid u_i)$ in k liegen, erkennt man daraus, daß die symmetrischen Funktionen von $\varrho, \varrho^q, \ldots, \varrho^{q^{\mathfrak{f}-1}}$ nach $\mathfrak{P}$ Zahlen in k kongruent sind.

Aus $\Pi(x \mid \mathsf{A}_i) \equiv P(x) \mod \mathfrak{P}$ folgt aber nach Satz 1.

$$\Pi(x \mid \mathsf{A}_i) \equiv P(x) \mod \mathfrak{p}$$

Also auch $\Pi(\varrho \mid \mathsf{A}_i) \equiv P(\varrho) \mod \mathfrak{p}$. Wären die Koeffizienten von $\Pi(X \mid U_i)$ durch ein von $\mathfrak{P}$

8 ı

durch ein von $\mathfrak{P}$ verschiedenes Primideal, das Teiler von $\mathfrak{p}$ ist, teilbar, so gälte dasselbe für $\Pi(\varrho \mid \mathsf{A}_i)$ also von $P(\varrho)$ entgegen der Voraussetzung über die Wahl von ϱ (S. 6▶). Ist ferner $\mathfrak{p}$ teilbar durch $\mathfrak{P}^2$, so ist aus dem gleichen Grunde $\Pi(x \mid U_i)$ nicht teilbar durch $\mathfrak{P}^2$. Sollte aber $\mathfrak{P}$ nur einmal in $\mathfrak{p}$ aufgehen, so bestimme man eine durch $\mathfrak{P}$ teilbare Zahl π so, daß π teilbar

durch jeden anderen Faktor von $\mathfrak{p}$, dagegen nicht durch $\mathfrak{P}^2$. Dann leistet, falls $\Pi(x \mid U_i)$ durch $\mathfrak{p}^2$ teilbar sein sollte, $\Pi(x \mid U_i) + \pi$ die gleichen Dienste und ist nicht durch $\mathfrak{p}^2$ teilbar. Bei diesen Teilbarkeitsbetrachtungen denken wir uns natürlich immer X durch Ξ ersetzt, da ja $\Pi(\Xi \mid U_i) \equiv 0 \mod \mathfrak{P}$ ist. Dagegen gilt die Kongruenz für kein anderes in $\mathfrak{p}$ aufgehendes Primideal und auch nicht für $\mathfrak{P}^2$.

Es sei nun $\Phi(X \mid U_i)$ eine Funktion in Ω, sodaß $\Phi(\Xi \mid U_i) \equiv 0 \mod \mathfrak{P}$ ist. Wäre Φ nicht teilbar durch Π, so wären sie prim, denn $\Pi(x \mid U_i)$ ist nach dem vorigen ersichtlich Primfunktion mod $\mathfrak{p}$. Also ließen sich in k die Funktionen Y, Z so wählen, daß

$$Y\Phi + Z\Pi \equiv U \mod \mathfrak{p}$$

ist, wo U eine Funktion in k, die nur von den U_i abhängt, und nicht identisch $\equiv 0 \bmod \mathfrak{p}$ ist. Für $X = \Xi$ erhielte man aber

$$U \equiv 0 \mod \mathfrak{P} \quad \text{also auch mod } \mathfrak{p},$$

was nicht der Fall sein soll; es ist also Φ teilbar durch Π nach dem Modul $\mathfrak{p}$.

9 I

Gilt sogar $\Phi(\Xi \mid U_i) \equiv 0 \mod \mathfrak{P}^{e_i}$, wo $\mathfrak{P}^{e_i}$ in $\mathfrak{p}$ noch aufgeht, so ist Φ sogar durch Π^{e_i} teilbar.

Beweis: Man setze $\Phi(X \mid U_i) \equiv \Pi^{e'} F \mod (\mathfrak{p})$ wo F nicht teilbar durch Π, sodaß $F(\Xi)$ nicht $\equiv 0 \mod \mathfrak{P}$ sein kann. Dann ist, da der Inhalt von $\Pi(\Xi)$ nur durch $\mathfrak{P}$ teilbar ist, der Inhalt der rechten Seite für $X = \Xi$ durch $\mathfrak{P}^{e'}$ genau teilbar. Da $\mathfrak{P}^{e_1}$ in $\mathfrak{p}$ aufgeht, muß er mindestens durch $\mathfrak{P}^{e_1}$ teilbar sein, was $e' \geqq e_1$ ergibt.

Nun sei $\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_\nu^{e_\nu}$ und die Relativgrade $\mathfrak{f}_1, \dots, \mathfrak{f}_\nu$. Wir bestimmen das zu $\mathfrak{P}$ gehörige $\Pi_i(X \mid U_i)$. Es ist vom $\mathfrak{f}_i$–ten Grade, mit Koeffizienten aus k und $e_1\mathfrak{f}_1 + \dots + e_\nu\mathfrak{f}_\nu = r$. Ferner ist Π_i von Π_k verschieden, da für $X = \Xi_i$ die Inhalte zu $\mathfrak{P}_k$ resp. $\mathfrak{P}_i$ prim sind. Nun ist

$$F_r(\Xi \mid U_i) \equiv 0 \mod \mathfrak{p}, \quad \text{also sicher mod } \mathfrak{P}_i^{e_i}$$

Somit ist $F_r(X \mid U_i)$ durch $\Pi_i(X \mid U_i)$ nach $\mathfrak{p}$ teilbar; da die Grade stimmen ist genau

$$F_r(X \mid U_i) \equiv \Pi_1^{e_1} \dots \Pi_\nu^{e_\nu} \mod \mathfrak{p}$$

Wir haben also den analogen Satz, wie für „absolute“ Körper.

Wir bilden wieder die in K liegende Form:

$$\frac{\partial}{\partial X}F_r(X \mid U_i)_{X=\Xi} \equiv F_r'(\Xi \mid U_i) \quad \text{wo:}$$
$$F_r'(\Xi \mid U_i) = (\Xi - \Xi^{(1)}) \dots (\Xi - \Xi^{(r-1)}).$$

Wie in der absoluten Theorie weist man leicht nach, daß ihr Inhalt, der in K liegt, von der Basis von K unabhängig ist.

10

Definition 1. Der Inhalt $\mathfrak{D}_k$ der von der Basis unabhängigen Form $(\Xi - \Xi^{(1)}) \dots (\Xi - \Xi^{(r-1)})$ heißt die *Relativdifferente* von K in Bezug auf k. Ihre Relativnorm (Ideal in k) heißt die *Relativdiskriminante*

$$D_k = n(\mathfrak{D}_k)$$

Es ist $F_r(X \mid U_i) = \Pi_1^{e_1} H + G$, wo H eine Funktion in k ist und die Zahlen von G durch $\mathfrak{p}$ teilbar sind. Man hat

$$F_r'(\Xi \mid U_i) = e_1 \Pi_1^{e_1 - 1} \Pi_1' H + \Pi_1^{e_1} H' + G'$$

wo rechts für X die Form Ξ zu setzen ist. Man erkennt also wieder

Satz 2. Die Relativdifferente $\mathfrak{D}_k$ ist mindestens durch $\mathfrak{P}_i^{e_i - 1}$ teilbar, wenn $\square\square\square$ e_i die „*Ordnung*“ von $\mathfrak{P}_i$. Ist e_i prim zu p, so ist $\mathfrak{D}_k$ genau durch $\mathfrak{P}_i^{e_i - 1}$ teilbar, sonst durch eine höhere Potenz.

Beweis: Wäre $\Pi_1'(\Xi \mid U_i)$ durch $\mathfrak{P}_1$ teilbar, so setze man $U_i = \mathsf{A}_i$, sodaß $\Pi_1'(X \mid \mathsf{A}_i) \equiv P_1'(x) \mod \mathfrak{p}$ wird. Es müßte dann $P_1'(\varrho) \equiv 0 \mod \mathfrak{P}_1$ sein, was nicht der Fall ist. Daraus ist der Satz leicht zu entnehmen.

Bildet man die Relativnorm, so folgt leicht:

Satz 3. Ist $\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_\nu^{e_\nu}$ und $\mathfrak{f}_i$ der Rel. Grad von $\mathfrak{P}_i$, so ist die Relativdiskriminante mindestens durch $\mathfrak{p}^{(e_1-1)\mathfrak{f}_1 + \dots + (e_i-1)\mathfrak{f}_i}$ teilbar. Sie ist genau durch diese Potenz teilbar, wenn alle e_i prim zu p, sonst durch eine höhere.

11

Ist also ein $e_i > 1$, so ist D_k sicher durch $\mathfrak{p}$ teilbar. Sind alle $e_i = 1$, also prim zu p, so ist D_k prim zu $\mathfrak{p}$. Also:

Satz 4. In der Relativdiskriminante D_k von K in Bezug auf k gehen alle und

nur die Primideale aus k auf, die in K durch das Quadrat eines Primideals teilbar sind (Verzweigungsteiler von K).

Damit sind für die Relativdiskriminanten und Differenten genau die entsprechenden Sätze hergeleitet, wie für diese Begriffe im „absoluten“ Körper.

Die zu k konjugierten Körper bezeichnen wir mit $k, k_1, \ldots, k_{n-1}$ und ordnen die zu K konjugierten Körper in n Serien $K_i^{(\nu)}$; $(i = 0, 1, \ldots, n-1;\ \nu = 0, 1, \ldots, r-1)$

□□□ Analog sollen die konjugierten Formen bezeichnet werden:

Die Form

$$\Phi_i(X, U_i) = (X - \Xi_i)(X - \Xi_i^{(1)}) \cdots (X - \Xi_i^{(r-1)})$$

ist eine Form aus k_i und es ist:

$$\Phi_i(\Xi_i^{(\nu)}, U_i) = 0.$$

Wenn irgendeine Form des Körpers k_i: $\Psi(X)$ für $X = \Xi_i^{(\nu)}$ verschwindet, ist $\Psi(X)$ teilbar durch $\Phi_i(X, U_i)$. In der Tat, wenn etwa $\Psi(\Xi_i) = 0$ ist, und wir gehen zu einem relativ–konjugierten Körper über, so ändern sich die Koeffizienten von $\Psi(X)$ nicht, und es wird

$$\Psi(\Xi_i^{(\nu)}) = 0.$$

Nun ist $\Psi(X) = \Psi(X) - \Psi(\Xi_i) = (X - \Xi_i)\Psi_1(X)$

12 ı

Da $\Psi(X)$ für $X = \Xi_i^{(1)}$ verschwindet $\Psi_1(X)$ für $X = \Xi_i^{(1)}$ verschwinden, also $\Psi_1(X) = \Psi_1(X) - \Psi_1(\Xi_i^{(1)}) = (X - \Xi_i^{(1)})\Psi_2(X)$[1] u.s.w. Damit ist der Beweis erbracht.

Es sei nun ξ die Fundamentalform für k in den Variablen u_i. Aus der „absoluten“ Theorie folgt, daß sich jede Zahl aus K rational mit ganzen rationalen Koeffizienten durch eine Funktion von Ξ darstellen läßt, wenn man sie mit einer Einheitsform mit ganzen rationalen Koeffizienten multipliziert. Die Form ξ läßt sich also darstellen in der Form:

$$U\xi = \Theta(\Xi, U_i, u_k) = \Theta(\Xi)$$

[1] undeutlich

mit ganzen rationalen Koeffizienten. Geht man zum konjugierten Körper K_h über, so geht unsere Gleichung, da die Koeffizienten von U und Θ ganz rational sind, über in

$$U\xi_h = \Theta(\Xi_h)$$

Die Funktion $\Theta(X) - U\xi_h$ hat Koeffizienten in k_h und verschwindet für $X = \Xi_h$. Sie hat also die Form:[2]

$$\Theta(X) - U\xi_h = (X - \Xi_h)(X - \Xi_h^{(1)}) \cdots (X - \Xi_h^{(r-1)})\mathfrak{D}(x)$$

Setzt man $X = \Xi$ so erhält man:

$$U(\xi - \xi_h) = \Phi_h(\Xi, U_i)\mathfrak{D}(x)$$

Da der Inhalt von U gleich 1 ist, ist also der Inhalt von $\xi - \xi_h$ teilbar durch den von $\Phi_h(\Xi \mid U_i)$

Die Funktion $\Phi_h(X, U_i)$ hat Koeffizienten in k_h. Sie läßt sich also, wenn man sie mit einer rationalen

13 I

Einheitsform u der u_i multipliziert, rational ganzzahlig durch ξ_h ausdrücken. Sei

$$\begin{aligned} u\Phi_h(X, U_i) &= \Lambda(X, \xi_h, U_i, u_i) \\ &= \Lambda(X, \xi_h), \end{aligned}$$

wo $\Lambda(x, y)$ eine Funktion mit ganzen rationalen Koeffizienten ist. Geht man mit dieser Gleichung zu einem konjugierten Körper über, so ändern sich rechts die Koeffizienten nicht, also:

$$\begin{aligned} u\Phi_i(X, U_j) &= \Lambda(X, \xi_i) \qquad \text{insbesondere also:} \\ u\Phi(X, U_j) &= \Lambda(X, \xi) \end{aligned}$$

□□□
Da nun $\Phi(\Xi, U_j) = 0$ ist, ist also $\Lambda(\Xi, \xi) = 0$ und somit

$$\Lambda(\Xi, \xi_h) = \Lambda(\Xi, \xi_h) - \Lambda(\Xi, \xi).$$

[2] undeutlich

Sammelt man die Potenzen von ξ_h und ξ, so stehen rechts Ausdrücke von der Form $(\xi_h^\mu - \xi_h^\mu)\rho$ die durch $\xi - \xi_h$ teilbar sind. Also ist:

$$\Lambda(\Xi, \xi_h) = (\xi - \xi_h)G(\Xi, \xi, \xi_h) \qquad \text{oder}$$
$$u\Phi_h(\Xi, U_i) = (\xi - \xi_h)G(\Xi, \xi, \xi_h)$$

Da nun u eine Einheitsform ist, ist also der Inhalt von $\Phi_h(\Xi, U_i)$ durch den Inhalt von $(\xi - \xi_h)$ teilbar. *Es sind also die Inhalte von* $(\xi - \xi_h)$ *und* $\Phi(\Xi, U_i)$ *identisch.*

Die Relativdifferente $\mathfrak{D}_k$ von K war nun der Inhalt der Form $(\Xi - \Xi^{(1)}) \cdots (\Xi - \Xi^{(r-1)})$. Die Differente $\mathfrak{D}$ von K ist aber der Inhalt der Form

$$(\Xi - \Xi^{(1)}) \ldots (\Xi - \Xi^{(r-1)})(\Xi - \Xi_1) \ldots (\Xi - \Xi_1^{(r-1)})$$
$$\cdot(\Xi - \Xi_{n-1}) \ldots (\Xi - \Xi_{n-1}^{(r-1)})$$
$$= (\Xi - \Xi^{(1)}) \ldots (\Xi - \Xi^{(r-1)}).\Phi_1(\Xi, U_i) \ldots \Phi_{n-1}(\Xi, U_i)$$

Nach dem Bewiesenen ist also, da der Inhalt von

$$(\xi - \xi_1) \ldots (\xi - \xi_{n-1})$$

die Differente $\mathfrak{d}$ von k ist:[3]

$$\mathfrak{D} = \mathfrak{d}\mathfrak{D}_k$$

Satz 5. Die Differente $\mathfrak{D}$ des Körpers K ist das Produkt aus der Differente $\mathfrak{d}$ von k mit der Relativdifferente $\mathfrak{D}_k$ von K in Bezug auf k.

Geht man zur Relativnorm über, so folgt:

Satz 6. Die Diskriminante D von K ist bis aufs Vorzeichen:

$$D = \pm d^r \mathsf{N}(D_k)$$

wo d die Diskriminante von k und D_k die Relativdiskriminante von K in Bezug auf k bezeichnet.

Satz 5 läßt sich unmittelbar verallgemeinern: Es seien $K_1, K_2, \ldots, K_\nu$ eine

[3] $\mathfrak{d}$ und $\mathfrak{D}$ sind optisch kaum zu unterscheiden.

Reihe von übereinandergeschachtelten Körpern, $\mathfrak{D}_i$ sei die Differente von K_i, $\mathfrak{D}_{i,k}$ die Relativdifferente von K_i in Bezug auf K_k $(i > k)$. Nach Satz 5 ist

$$\mathfrak{D}_\nu = \mathfrak{D}_{\nu,\nu-1}\mathfrak{D}_{\nu-1} = \mathfrak{D}_{\nu,\nu-1}\mathfrak{D}_{\nu-1,\nu-2}\mathfrak{D}_{\nu-2} = \cdots = \mathfrak{D}_{\nu,\nu-1}\cdots\mathfrak{D}_{21}\cdot\mathfrak{D}_1$$

15 ı

Andererseits ist wieder nach Satz 5:

$$\mathfrak{D}_\nu = \mathfrak{D}_{\nu,1}\mathfrak{D}_1$$

also $\mathfrak{D}_{\nu,1} = \mathfrak{D}_{2,1}.\mathfrak{D}_{3,2}\ldots\mathfrak{D}_{\nu,\nu-1}$ und somit:

Satz 7. Sind $K_1, K_2, \ldots, K_\nu$ ineinandergeschachtelte Körper (K_i Unterkörper aller folgenden), und bezeichnet für $i > k$ $\mathfrak{D}_{i,k}$ die Relativdifferente von K_i in Bezug auf K_k, dann gilt:

$$\mathfrak{D}_{\nu,1} = \mathfrak{D}_{2,1}.\mathfrak{D}_{3,2}\ldots\mathfrak{D}_{\nu,\nu-1}$$

Nehmen wir nur 3 Körper K_1, K_2, K_3, so gilt:

$$\mathfrak{D}_{3,1} = \mathfrak{D}_{2,1}.\mathfrak{D}_{3,2}$$

Bezeichnen wir die Relativdiskriminanten analog und ebenfalls die Relativnormen, ist ferner r der Relativgrad von K_3 zu K_2, so ist:

$$n_{3,1}(\mathfrak{D}_{3,1}) = D_{3,1} = n_{2,1}\big(n_{3,2}(\mathfrak{D}_{2,1}\cdot\mathfrak{D}_{3,2})\big) = D_{2,1}^r\cdot n_{2,1}(D_{3,2})$$

Satz 8. Sind K_1, K_2, K_3 ineinandergeschachtelte Körper, so ist die Relativdiskriminante von K_3 zu K_1 durch die r–te Potenz der Relativdiskriminante von K_2 zu K_1 teilbar, wenn r der Relativgrad (K_3, K_2) ist.

(Wir beweisen nun einen einfachen Diskriminantensatz, der aber erst später Verwendung finden soll (2.) S.76▸ f.)

16 ı

Es sei $(a_{ik})_m$ eine Matrix von m^2, $(b_{rs})_n$ eine von n^2 Elementen. $a_{ik}(b_{rs})$, wo a_{ik} fest ist, bedeute die Matrix, wo jedes b_{rs} mit demselben a_{ik} multipliziert ist. Für die in Bezug auf i, k gebildete Determinante $|a_{ik}(b_{rs})|$ gilt nun:

Satz 9. Es ist[4] $|a_{ik}(b_{rs})| = |b_{rs}(a_{ik})| = |a_{ik}|^n|b_{rs}|^m$.

[4] Indizes undeutlich

Beweis. 1.) Für $m = 1$ wird einfach $|a_{11}(b_{rs})| = a_{11}^n |b_{rs}| = |a_{11}|^n |b_{rs}|^1$, wie es sein soll.

2.) Sei $m > 1$ und der Satz richtig bis $m-1$. Wir multiplizieren die ersten n Zeilen mit $\frac{a_{i1}}{a_{11}}$ und ziehen sie vom i–ten Komplex von von je n Zeilen ab. Dann geht unsere Determinante über in:

$$\begin{vmatrix} a_{11}(b_{rs}) & a_{12}(b_{rs}) & \cdots\cdots & a_{1m}(b_{rs}) \\ 0 & \left(a_{22} - \frac{a_{12}a_{21}}{a_{11}}\right)(b_{rs}) & \cdots\cdots & \left(a_{2m} - \frac{a_{1m}a_{21}}{a_{11}}\right)(b_{rs}) \\ \vdots & \vdots & & \vdots \\ 0 & \left(a_{m2} - \frac{a_{12}a_{m1}}{a_{11}}\right)(b_{rs}) & \cdots\cdots & \left(a_{mm} - \frac{a_{1m}a_{m1}}{a_{11}}\right)(b_{rs}) \end{vmatrix}$$

$= |a_{11}(b_{rs})| \left|\left(a_{ik} - \frac{a_{1k}a_{i1}}{a_{11}}\right)(b_{rs})\right|$, wo die 2te Determinante in Bezug auf $i, k = 2, \ldots, m$ zu bilden ist. Da für $m-1$ der Satz als richtig angenommen wird, ist dieses[5]

$$= |a_{11}(b_{rs})| \left|a_{ik} - \frac{a_{1k}a_{i1}}{a_{11}}\right|^n \cdot |b_{rs}|^{m-1} = \left(a_{11}\left|a_{ik} - \frac{a_{1k}a_{i1}}{a_{11}}\right|\right)^n |b_{rs}|^m$$

Wenn wir nun in der m–reihigen Determinante $|a_{ik}|$ von der i–ten Zeile die mit $\frac{a_{i1}}{a_{11}}$ multiplizierte erste abziehen, verschwindet die erste Kolonne bis auf das erste Glied und es wird

$$|a_{ik}| = a_{11}\left|a_{ik} - \frac{a_{i1}a_{1k}}{a_{11}}\right| \qquad (i, k = 2, \ldots, m)$$

Daraus folgt die Behauptung.)

Nun seien K_1, K_2 zwei Körper über k von den Relativgraden r_1, r_2. ξ sei eine Basisform in K_1, η in K_2. x und y seien Variable. Wir betrachten die Form:

$$F = x\xi + y\eta$$

und setzen $F_{\mu,\nu} = x\xi_\mu + y\eta_\nu$, wo ξ_μ, η_ν die relativ konjugierten Formen bezeichnet. Dann ist

$$\Phi(X) = \prod_{\mu=0}^{r_1-1} \prod_{\nu=0}^{r_2-1} (X - F_{\mu,\nu})$$

[5]Formel teilweise undeutlich

symmetrisch in den ξ_μ und η_ν, hat also Koeffizienten in k. Ferner hat $\Phi(X)$ keine Doppelwurzel, da die ξ_μ und η_ν untereinander, also auch die $F_{\mu,\nu}$ verschieden sind.

Sei $\Psi(\xi,\eta)$ irgend eine Funktion von ξ,η und Unbestimmten mit Koeffizienten in k. Dann ist:

$$\Phi(X)\left(\frac{\Psi(\xi,\eta)}{X-F_{0,0}}+\cdots+\frac{\Psi(\xi_\mu,\eta_\nu)}{X-F_{\mu,\nu}}+\cdots\right)=H(X)$$

eine Funktion in k. Setzt man $X=F_{0,0}=F$, so wird

18 ı

$$\Psi(\xi,\eta)=\frac{H(F)}{\Phi'(F)}$$

wo der Nenner nicht verschwindet.

Es sei nun K_3 der aus K_1 und K_2 komponierte Körper. Die Zahlen aus K_1 lassen sich rational durch ξ die aus K_2 durch η, die aus K_3 also, wie eben gezeigt, rational durch die Form F darstellen. Also läßt sich auch jede Form in K_3 rational durch F darstellen. Ist r der Relativgrad von K_3 zu k, so seien $F,F_1,\ldots,F_{r-1}$ die relativ konjugierten zu F, die einen Teil der $F_{\mu,\nu}$ ausmachen, sodaß $\Phi'(F_\nu)\neq 0$ ist. Erweitern wir also mit $\Phi'(F_1)\ldots\Phi'(F_{r-1})$, so wird der Nenner rational in k. Mithilfe der Gleichung in k:

$$(X-F)\cdots(X-F_{r-1})=0$$

kann der Darstellungsgrad in F auf den $(r-1)$ten erniedrigt werden. Jede Form in K_3, also auch die Potenzen der Basisform Ξ lassen sich darstellen in der Form:

$$\Xi^\nu=\sum_{i=0}^{r-1}\Lambda_{\nu i}F^i$$

wo die $\Lambda_{\nu i}$ rationale Funktionen von Unbestimmten mit Koeffizienten in k seien[6]. Gehen wir zu den relativ konjugierten über und bilden für $\nu=0,1,\ldots,r-1$ die Vandermondesche Determinante der Ξ, so ist:

$$|\Xi^\nu_{(\mu)}|^2_{(r-1)}=|\Lambda_{ik}|^2\cdot|F^k_{(i)}|^2$$

[6] vielleicht auch ‘sind’

19 ı

Rechts steht die Relativdiskriminante von Ξ, die nicht verschwindet, also ist auch

$$|F^k_{(i)}| \neq 0.$$

Nun ist $|F^k_{(i)}|$ ein Produkt der Größen

$$(F_k - F_{k'}) = (x\xi_\alpha + y\eta_\beta) - (x\xi_\varrho + y\eta_\sigma),$$

die nicht verschwinden. Sie haben die Form:

$$x(\xi_\alpha - \xi_\varrho) + y(\eta_\beta - \eta_\sigma)$$

Als Inhalt kommen nur Primideale in Frage, die sowohl im Inhalt von $(\xi_\alpha - \xi_\varrho)$ als von $(\eta_\beta - \eta_\sigma)$ aufgehen. Da ev. eines von ihnen verschwindet, gehen also im Inhalt von $|F^{(k)}_i|$ nur Primideale von $\prod(\xi_\alpha - \xi_\varrho)$ oder $\prod(\eta_\beta - \eta_\sigma)$ auf. Die Inhalte der Quadrate sind aber gerade die Relativdiskriminanten D_1 und D_2 von K_1 und K_2.

Nun läßt sich jede Zahl aus K_3 rational ganzzahlig mit Koeffizienten in k durch Ξ vom $(r-1)$–ten Grade darstellen, wenn man sie mit einer Einheitsform, die für alle Zahlen dieselbe ist (in k liegend), multipliziert. Also läßt sich auch F^i darstellen in der Form:

$$UF^i = \sum_{\nu=0}^{r-1} H_{i\nu}\Xi^\nu$$

wo $H_{i\nu}$ in k. Geht man zu den relativ–konjugierten über und bildet die Vandermonde'sche Determinante, so folgt

$$U^{2r}|F^i_{(k)}|^2 = |H_{i\nu}|^2|\Xi^i_{(k)}|^2$$

20 ı

Da U eine Einheitsform und $H_{i\nu}$ diesmal ganzzahlig ist, geht der Inhalt von $|\Xi^i_{(k)}|$, d.h. die Relativdiskriminante D_3 von K_3, im Inhalt von $|F^i_{(k)}|^2$ auf. In D_3 können also nur solche Primideale aufgehen, die entweder in D_1 oder in D_2 oder auch in beiden enthalten sind. Satz 8 lehrt, da K_1 und K_2 Unterkörper von K_3 sind, daß D_3 sowohl durch D_1 wie D_2 teilbar ist. Daraus folgt unmittelbar:

Satz 10. In der Relativdiskriminante D_3 des aus K_1 und K_2 komponierten Körpers K_3, alle auf einen gemeinsamen Grundkörper k genommen, gehen alle und nur die Primideale von k auf, die wenigstens in einer der Relativdiskriminanten D_1 und D_2 von K_1 und K_2 zu k aufgehen. D_3 ist ferner sicher teilbar durch D_1 und D_2, sodaß von jedem Primideal mindestens die höchste Potenz in D_3 aufgeht, die in D_1 oder D_2 vorkommt.

Besonders einfache und wichtige Zerlegungsgesetze treten auf, wenn es sich um einen *Galoisschen Körper* handelt.

Es sei also k ein algebraischer Grundbereich, dessen Ideale mit kleinen, K ein Galoisscher Körper in Bezug auf k, dessen Ideale mit großen Buchstaben bezeichnet werden.

$n(A)$ bezeichne die Relativnorm, $\mathfrak{G}$ sei die Substitutionsgruppe von K. Der Relativgrad sei n, die Substitutionen von $\mathfrak{G}$ seien $\sigma_0 = 1, \sigma_1, \ldots, \sigma_{n-1}$. [...] und $\sigma_h\mathfrak{A}$ bezeichnen die durch die Substitution σ_h aus A und $\mathfrak{A}$ hervorgehenden Größen. Da alle Gleichungen zwischen Idealen auf solche zwischen Zahlen hinauslaufen und auf diese die Substitutionen von $\mathfrak{G}$ angewandt werden dürfen, bleibt jede Gleichung zwischen Idealen richtig, wenn man die Substitutionen aus $\mathfrak{G}$ auf sie anwendet. Zahlen und Ideale aus k werden durch $\mathfrak{G}$ nicht geändert. Unsere Betrachtungen gelten natürlich auch für den Spezialfall, daß k der rationale Körper ist.

Sei $\mathfrak{P}$ ein Primideal aus K. Dann sind auch $\sigma_1\mathfrak{P}, \ldots, \sigma_{n-1}\mathfrak{P}$ Primideale, die ebenfalls in K liegen, da K Galois'sch ist. Statt $\sigma_\nu\mathfrak{P}$ schreiben wir auch $\mathfrak{P}^{(\nu)}$. Ist $\mathfrak{f}$ der Relativgrad von $\mathfrak{P}$, so ist

$$\mathfrak{P} \cdot \sigma_1\mathfrak{P} \cdots \sigma_{n-1}\mathfrak{P} = \mathfrak{P} \cdot \mathfrak{P}^{(1)} \cdots \mathfrak{P}^{(n-1)} = \mathfrak{p}^{\mathfrak{f}},$$

wo $\mathfrak{p}$ das zu $\mathfrak{P}$ gehörige Primideal aus k ist. Also ist auch der Relativgrad eines jeden der konjugierten Primideale $\mathfrak{P}^{(\nu)}$ gleich $\mathfrak{f}$. Ist

$$\mathfrak{p} = \mathfrak{P}^e \cdot \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_\nu^{e_\nu} \cdots \mathfrak{P}_{r-1}^{e_r-1}$$

die Zerlegung von $\mathfrak{p}$ in K, so muß

$$\mathfrak{P}^{e\mathfrak{f}} \ldots \mathfrak{P}^{(r-1)^{e_{r-1}\mathfrak{f}}} = \mathfrak{P}\mathfrak{P}^{(1)} \ldots \mathfrak{P}^{n-1}$$

sein.

22 ı

Also muß etwa

$$\mathfrak{P} = \mathfrak{P}^{(1)} = \cdots = \mathfrak{P}^{(e\mathfrak{f}-1)}$$

sein dagegen $\mathfrak{P}$ von jedem anderen konjugierten verschieden. Wenden wir auf diese Gleichung alle Substitutionen an, so erkennen wir, daß die $\mathfrak{P}^{(\nu)}$ in Gruppen von je $e\mathfrak{f}$ gleichen zerfallen. Es muß also

$$e = e_1 = \cdots = e_{r-1}$$

sein, sodaß

$$\mathfrak{p} = (\mathfrak{P}\mathfrak{P}_1 \ldots \mathfrak{P}_{r-1})^e$$

die Zerlegung von $\mathfrak{p}$ ist. Da ferner

$$e\mathfrak{f} + e_1\mathfrak{f}_1 + \cdots + e_{r-1}\mathfrak{f}_{r-1} = n$$

sein muß und die e_ν und $\mathfrak{f}_\nu$ alle gleich sind, muß

$$re\mathfrak{f} = n$$

sein.

Satz 11. In dem Galoisschen Körper K über k zerfällt jedes Primideal $\mathfrak{p}$ aus k in r Primideale gleichen Grades $\mathfrak{f}$, gleicher Ordnung e, und es ist

$$e\mathfrak{f}r = n$$

wo n der Relativgrad von k.

Jedes Primideal $\mathfrak{P}$ in K gibt nun Anlaß zu gewissen *Untergruppen von* $\mathfrak{G}$. Die Gesamtheit der Substitutionen, welche $\mathfrak{P}$ ungeändert lassen, bilden ersichtlich eine Untergruppe $\mathfrak{G}_Z(\mathfrak{P})$. Ihr Grad ist nach dem vorigen offenbar $e\mathfrak{f}$, also ihr Index r.

23 ı

Ist $\mathfrak{P}_1$ ein anderer Teiler von $\mathfrak{p}$, so wird er, falls

$$\sigma_1\mathfrak{P} = \mathfrak{P}_1\,,$$

durch die Untergruppe

$$\mathfrak{G}_Z(\mathfrak{P}_1) = \sigma_1^{-1}\mathfrak{G}_Z(\mathfrak{P})\sigma_1^{+1}$$

ungeändert gelassen. Ist umgekehrt

$$\sigma\mathfrak{P}_1 = \mathfrak{P}_1\,,$$

so ist $\sigma_1^{+1}\sigma\sigma_1^{-1}$ eine Substitution, die $\mathfrak{P}$ ungeändert läßt, also zu $\mathfrak{G}_Z(\mathfrak{P})$ gehört, sodaß σ zu $\sigma_1^{-1}\mathfrak{G}_Z(\mathfrak{P})\sigma_1^{+1}$ gehört.

Definition 2. Ist $\mathfrak{p} = (\mathfrak{P}\mathfrak{P}_1 \dots \mathfrak{P}_{r-1})^e$ die Zerlegung von $\mathfrak{p}$ in K, wo $\mathfrak{P}$ den Relativgrad $\mathfrak{f}$ hat, so bilden die Substitutionen von $\mathfrak{G}$, welche $\mathfrak{P}$ ungeändert lassen, eine Untergruppe $\mathfrak{G}_Z(\mathfrak{P})$ von $\mathfrak{G}$ vom Index r und Grad $e\mathfrak{f}$, die *Zerlegungsgruppe* des Primideals $\mathfrak{P}$. Die Zerlegungsgruppen der übrigen Primideale $\mathfrak{P}_\nu$ sind die konjugierten Gruppen zu $\mathfrak{G}_Z(\mathfrak{P})$.

Eine weitere Untergruppe $\mathfrak{G}_T(\mathfrak{P})$ erhält man offenbar durch alle Substitutionen $\tau, \tau_1, \dots$ für die für jede ganze Körperzahl □□□ ω gilt:

$$\tau\omega \equiv \omega \mod \mathfrak{P}$$

Es gibt also eine durch $\mathfrak{P}$ teilbare Zahl π, sodaß:

$$\tau\omega = \omega + \pi$$

ist. Ist speziell ω selbst durch $\mathfrak{P}$ teilbar, so ist $\tau\omega$ auch durch $\mathfrak{P}$ teilbar, □□□ also ω durch $\tau^{-1}\mathfrak{P}$. Jede durch $\mathfrak{P}$ teilbare Körperzahl ist also auch durch $\tau^{-1}\mathfrak{P}$ teilbar, und da

24 I

beides Primideale sind

$$\tau^{-1}\mathfrak{P} = \mathfrak{P}.$$

Da τ^{-1} jede Substitution von $\mathfrak{G}_T(\mathfrak{P})$ bedeuten kann, läßt also $\mathfrak{G}_T(\mathfrak{P})$ das Primideal $\mathfrak{P}$ invariant, d.h. $\mathfrak{G}_T(\mathfrak{P})$ ist Untergruppe von $\mathfrak{G}_Z(\mathfrak{P})$.

Da sich aus den Basiszahlen von K jede Zahl aus K zusammensetzen läßt, genügt es, die Forderung $\tau\omega \equiv \omega \mod \mathfrak{P}$ für eine Basis zu stellen. Dies ist offenbar, wenn ξ eine Fundamentalform von K bedeutet, mit der Forderung

$$\tau\xi \equiv \xi \mod \mathfrak{P}$$

gleichbedeutend. Nun genügt, wenn $\xi^{(1)}, \dots, \xi^{(n-1)}$ die relativ–konjugierten zu ξ sind, ξ der Gleichung in k:

$$F(x) = (x - \xi) \dots (x - \xi^{(n-1)}) = 0$$

Es sei ferner

$$\mathsf{N}(\mathfrak{p}) = p^\nu = q$$

Dann gilt für jede Zahl α aus k:

$$\alpha^q \equiv \alpha \mod \mathfrak{p}, \quad \text{also erst recht mod } \mathfrak{P}.$$

Erhebt man nun $F(x)$ in die p–te Potenz, so bedeutet dies mod $\mathfrak{p}$ nach bekannten Sätzen nichts anderes, als daß jedes Glied des entwickelten $F(x)$ mit p potenziert wird. Gehen wir also bis zur $p^\nu = q$–ten Potenz und beachten $\alpha^q \equiv \alpha \bmod \mathfrak{P}$, so bedeutet mod $\mathfrak{P}$ das Erheben in die q–te Potenz nichts anderes, als das Ersetzen der Variablen durch ihre q–te Potenz:

$$[F(x)]^q \equiv (x^q - \overline{\xi}) \dots (x^q - \overline{\xi}^{(n-1)}) \mod \mathfrak{P},$$

wo $\overline{\xi}$ aus ξ hervorgeht, indem jedes u_i durch u_i^q ersetzt wird ($\xi = \sum u_i \omega_i$).

25 I

Setzen wir hierin $x = \xi$, so verschwindet die linke Seite; also muß einer der Faktoren rechts durch $\mathfrak{P}$ teilbar sein, etwa

$$\xi^q \equiv \overline{\xi}^{(k-1)} \mod \mathfrak{P}$$

Legen wir den Unbestimmten u_i in ξ irgendwelche ganzen Zahlwerte bei, so geht ξ in jede Körperzahl ω über. $\overline{\xi}$ aber ist $\equiv \omega$ mod $\mathfrak{P}$, da für ganzzahliges u_i:

$$u_i^q \equiv u_i \mod p \quad \text{also mod} \mathfrak{P}.$$

Also folgt für diese ganzen rat. u_i

$$\xi = \omega \equiv \overline{\xi} \mod \mathfrak{P}$$

$$\left.\begin{array}{ll} \text{und somit} & \overline{\xi}^q \equiv \overline{\xi}^{(k-1)} \\ \text{also} & \omega^q \equiv \omega^{(k-1)} \end{array}\right\} \mod \mathfrak{P}$$

(Da offenbar aus $\omega \equiv \overline{\xi}$ auch $\omega^{(k-1)} \equiv \overline{\xi}^{(k-1)}$ mod $\mathfrak{P}$ folgt).

Demnach ist für jedes ganze ω aus K:

$$\omega^q \equiv \omega^{(k-1)} \mod \mathfrak{P},$$

wo k eine feste Zahl ist, *die von ω nicht abhängt*, (da die Kongruenz auf dieser Seite oben schon vor der Spezialisierung auf ein bestimmtes ω gewonnen war).

Setzen wir $\omega^{(k-1)} = \sigma\omega$, so sehen wir, daß es in $\mathfrak{G}$ eine ganz bestimmte Substitution σ geben muß, sodaß für jedes ganze ω aus K gilt:

$$\omega^q \equiv \sigma\omega \mod \mathfrak{P}.$$

Sei nun ϱ eine Primitivzahl nach $\mathfrak{P}$, dann zeigten wir früher, daß es eine in k ganzzahlige, ganze mod $\mathfrak{P}$ irreduzible Funktion □□□

$$\Phi(x) \equiv (x-\varrho)(x-\varrho^q)\cdots(x-\varrho^{q^{\mathfrak{f}-1}}) \mod \mathfrak{P}$$

26 I

gibt, sodaß

$$\Phi(\varrho) \equiv 0 \mod \mathfrak{P}$$

Sei nun κ irgendeine Substitution der Zerlegungsgruppe $\mathfrak{G}_Z$. Da dann $\mathfrak{P}$ und die (in k liegenden) Koeffiz. von $\Phi(x)$ ungeändert bleiben, wird:

$$\Phi[\kappa\cdot\varrho] \equiv 0 \mod \mathfrak{P},$$

sodaß gelten muß

$$\kappa\varrho \equiv \varrho^{q^\nu} \mod \mathfrak{P}$$

Nun gilt für jede Zahl ω aus K, die zu $\mathfrak{P}$ prim ist:

$$\omega \equiv \varrho^\lambda \mod \mathfrak{P}$$

für einen gewissen Exponenten λ. Also folgt:

$$\kappa\omega \equiv (\kappa\varrho)^\lambda \equiv (\varrho^{q^\nu})^\lambda \equiv (\varrho^\lambda)^{q^\nu} \equiv \omega^{q^\nu} \mod \mathfrak{P}.$$

Zu jedem κ aus $\mathfrak{G}_Z$ gibt es also ein ν zwischen 0 und $\mathfrak{f}-1$, sodaß für jede ganze Körperzahl (auch für die durch $\mathfrak{P}$ teilbaren, was ohne weiteres klar),

$$\kappa\omega \equiv \omega^{q^\nu} \mod \mathfrak{P}$$

ist. Wenden wir die Kongruenz, die eben gefunden war:

$$\sigma\omega \equiv \omega^q \mod \mathfrak{P}$$

die ebenfalls für jedes ganze ω aus K gilt, ν mal an, so wird:

$$\sigma^\nu\omega \equiv \omega^{q^\nu} \mod \mathfrak{P}$$

also

$$\kappa\omega \equiv \sigma^\nu\omega \mod \mathfrak{P}$$

Hierauf wenden wir einerseits κ^{-1} an, was wegen $\kappa \mid \mathfrak{G}_Z$ also $\kappa\mathfrak{P} = \mathfrak{P}$ geht, so wird:

$$\omega \equiv \sigma^\nu\kappa^{-1}\omega \mod \mathfrak{P}$$

Andererseits ersetzen wir ω durch $\kappa^{-1}\omega$, das ja mit ω alle Körperzahlen durchläuft, dann wird offenbar $\sigma^\nu\omega$ durch $\kappa^{-1}\sigma^\nu\omega$ zu ersetzen sein (nämlich das, was auf $\kappa^{-1}\omega$ durch σ^ν entsteht — zweckmäßiger wären die Substitutionen *hinten* anzuhängen).

27 I

also

$$\omega \equiv \kappa^{-1}\sigma^\nu\omega \mod \mathfrak{P}.$$

Aus den beiden letzten Kongruenzen folgt, daß sowohl $\sigma^\nu\kappa^{-1}$ als auch $\kappa^{-1}\sigma^\nu$ zu $\mathfrak{G}_T$ gehören.

Jede Substitution κ von $\mathfrak{G}_Z$ gehört also zu einer bestimmten der Nebengruppen:

$$\mathfrak{G}_T; \sigma\mathfrak{G}_T; \ldots; \sigma^{\mathfrak{f}-1}\mathfrak{G}_T$$

Nun war σ definiert durch

$$\sigma\omega \equiv \omega^q \mod \mathfrak{P}$$

Ist also ω durch $\mathfrak{P}$ teilbar, so ist auch $\sigma\omega$ durch $\mathfrak{P}$ teilbar, also, wie oben (S.23▸ u.) $\sigma\mathfrak{P} = \mathfrak{P}$, d.h. $\sigma \mid \mathfrak{G}_Z$. Daraus folgt, daß jede Nebengruppe $\sigma^\nu\mathfrak{G}_T$ zu $\mathfrak{G}_Z$ gehört.

□□□

Daraus folgt also weiter, daß

$$\mathfrak{G}_Z = \mathfrak{G}_T + \sigma\mathfrak{G}_T + \sigma^2\mathfrak{G}_T + \cdots$$

die Zerlegung von $\mathfrak{G}_Z$ nach $\mathfrak{G}_T$ ist, wobei nur noch die Anzahl der Nebengruppen zu bestimmen ist. Wegen der (S.27▸ oben) bewiesenen Tatsache folgt, daß wenn die Substitution κ aus $\mathfrak{G}_Z$ gerade zu der ν–ten Nebengruppe $\sigma^\nu\mathfrak{G}_T$

gehört, dann auch κ zur ebenderselben ν–ten Nebengruppe $\mathfrak{G}_T\sigma^\nu$ gehört und umgekehrt, daß

$$\sigma^\nu \mathfrak{G}_T = \mathfrak{G}_T \sigma^\nu$$

ist. Daraus folgt, daß $\mathfrak{G}_T$ invariante Untergruppe von $\mathfrak{G}_Z$ ist. Um Grad und Index zu bestimmen, nehmen wir an es sei μ der niedrigste Exponent, für den σ^μ in $\mathfrak{G}_T$ liegt ($\sigma^{e\mathfrak{f}}$ liegt sicher in $\mathfrak{G}_T$, da es 1 ist)

Dann ist für beliebiges ω:

$$\sigma^\mu \omega \equiv \omega \mod \mathfrak{P}$$

andererseits nach Konstruktion von σ:

$$\sigma^\mu \omega \equiv \omega^{q^\mu} \mod \mathfrak{P}$$

also

$$\omega \equiv \omega^{q^\mu} \mod \mathfrak{P}$$

für beliebiges ω. Ist dies umgekehrt für μ erfüllt, so folgt aus $\sigma^\mu\omega \equiv \omega^{q^\mu} \equiv \omega \mod \mathfrak{P}$, daß σ^μ zu $\mathfrak{G}_T$ gehört.

Nehmen wir nun einerseits $\omega = \varrho$, so muß μ mindestens gleich $\mathfrak{f}$ sein, da erst $\varrho^{q^\mathfrak{f}} \equiv \varrho \mod \mathfrak{P}$, andererseits ist für $\mu = \mathfrak{f}$ die Relation

$$\omega \equiv \omega^{q^\mathfrak{f}} \mod \mathfrak{P}$$

nach dem Fermat'schen Satz sicher erfüllt, also ist $\sigma^\mathfrak{f}$ die gesuchte niedrigste Potenz von σ, die in $\mathfrak{G}_T$ vorkommt, und somit

$$\mathfrak{G}_Z = \mathfrak{G}_T + \sigma\mathfrak{G}_T + \cdots + \sigma^{\mathfrak{f}-1}\mathfrak{G}_T.$$

Definition 3. Alle Substitutionen τ, für die für jedes ω aus K gilt:

$$\tau\omega \equiv \omega \mod \mathfrak{P}$$

bilden eine Gruppe $\mathfrak{G}_T(\mathfrak{P})$, die *Trägheitsgruppe* des Primideals $\mathfrak{P}$. Diese ist invariante Untergruppe der Zerlegungsgruppe $\mathfrak{G}_Z(\mathfrak{P})$ und hat in Bezug auf diese den Index $\mathfrak{f}$ also den Grad e. Die Faktorgruppe $\frac{\mathfrak{G}_Z}{\mathfrak{G}_T}$ ist ersichtlich zyklisch vom Grade $\mathfrak{f}$.

Daß $\mathfrak{G}_T$ *invariante* Untergruppe von $\mathfrak{G}_Z$ ist, kann man auch leicht so einsehen:

Sei τ eine Substitution aus $\mathfrak{G}_T$, σ irgendeine

29 ı

aus $\mathfrak{G}$ und etwa $\sigma\mathfrak{P} = \mathfrak{P}_i$

Wir setzen $\sigma^{-1}\omega = \omega_1$. Es ist $\tau\omega_1 = \omega_1 + \pi$, wo π durch $\mathfrak{P}$ teilbar. Wegen $\sigma\mathfrak{P} = \mathfrak{P}_i$ ist $\sigma\pi = \pi_i \equiv 0 \bmod \mathfrak{P}_i$, also

$$\sigma^{-1}\tau\sigma \cdot \omega = \tau\sigma\omega_1 = \sigma(\omega_1 + \pi) = \omega + \pi_i \quad \text{oder}$$
$$\sigma^{-1}\tau\sigma \cdot \omega \equiv \omega \bmod \mathfrak{P}_i$$

für jedes ω. Es ist also $\sigma^{-1}\tau\sigma$ eine Substitution aus $\mathfrak{G}_T(\mathfrak{P}_i)$

also:

$$\mathfrak{G}_T(\mathfrak{P}_i) = \sigma^{-1}\mathfrak{G}_T(\mathfrak{P})\sigma.$$

Gehört σ speziell zu $\mathfrak{G}_Z$, also $\sigma\mathfrak{P} = \mathfrak{P}$, so folgt offenbar, daß $\mathfrak{G}_T$ invariante Untergruppe von $\mathfrak{G}_Z$ ist. Wir entnehmen dem:

Satz 12. Die Trägheitsgruppe eines anderen in $\mathfrak{p}$ aufgehenden Primideals $\mathfrak{P}_i$ ist die in Bezug auf $\mathfrak{G}$ konjugierte Gruppe, die mit einer $\mathfrak{P}$ in $\mathfrak{P}_i$ überführenden Substitution transformiert ist.

Wir betrachten nun die über k liegenden Unterkörper $\overline{K}$ von K. Ein solcher ist nach der Galoisschen Theorie vollständig charakterisiert durch die zugehörige Untergruppe $\overline{\mathfrak{G}}$ von $\mathfrak{G}$, in dem Sinne, daß $\overline{K}$ aus allen und nur den Elementen von K besteht, die bei $\overline{\mathfrak{G}}$ ungeändert bleiben.

Sei $\overline{K}$ der zur Gruppe $\overline{\mathfrak{G}}$ gehörige Unterkörper von K. Der Grad von $\overline{\mathfrak{G}}$ sei $\overline{n}$, der Index $\overline{m}$, sodaß $n = \overline{n}\,\overline{m}$.

$\mathfrak{p}$ sei ein Primideal aus k, das wir in $\overline{K}$ zerlegen wollen. In K sei

30 ı

$$\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_r)^e$$

und $n = e\mathfrak{f}r$, also $\mathfrak{f}$ der Relativgrad von $\mathfrak{P}_i$ in Bezug auf k.

In Bezug auf $\overline{K}$ ist K ein Galoisscher Körper vom Grade $\overline{n}$ und der Gruppe $\overline{\mathfrak{G}}$. Wird auf ein Primideal aus K die Gruppe $\overline{\mathfrak{G}}$ angewandt, so geht es in alle jene über, die in □□□ ein– u. demselben Primideal in $\overline{K}$ aufgehen (S. 21▸). Wenden wir also $\overline{\mathfrak{G}}$ auf $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_r$ an, so zerfallen diese Primideale in

gewisse Verbände, die durch $\overline{\mathfrak{G}}$ nicht ineinander übergehen. Nur die Ideale jedes Verbandes gehen durch $\overline{\mathfrak{G}}$ (da Gruppe) alle in einander über. Es mögen λ Verbände resultieren:

$$\begin{array}{cccc} \mathfrak{P}_{11}, & \mathfrak{P}_{12}, & \dots & \mathfrak{P}_{1r_1} \\ \dots & \dots & \dots & \dots \\ \mathfrak{P}_{\lambda 1}, & \mathfrak{P}_{\lambda 2}, & \dots & \mathfrak{P}_{\lambda r_\lambda}\,. \end{array}$$

Zu jedem dieser Verbände gehört ein Primideal $\mathfrak{q}_\nu$ aus $\overline{k}$, und nach Satz 11 ist:

$$\mathfrak{q}_\nu = (\mathfrak{P}_{\nu 1} \dots \mathfrak{P}_{\nu r_\nu})^{e_\nu} \qquad (\mathfrak{P}_{\nu\mu} \text{ vom Rel. Grad } \mathfrak{f}_\nu \text{ in Bezug auf } \overline{K}).$$

Dabei ist $r_\nu e_\nu \mathfrak{f}_\nu = \overline{n}$. Der Grad der Zerlegungsgruppe $\overline{\mathfrak{G}}_{(\nu\mu)Z}$ von $\mathfrak{P}_{\nu\mu}$ in Bezug auf $\overline{K}$ ist dann $e_\nu \mathfrak{f}_\nu$, der Index in Bezug auf $\overline{\mathfrak{G}}$ gleich r_ν.

$\overline{\mathfrak{G}}_{(\nu\mu)Z}$ enthält alle und nur die Substitutionen aus $\overline{\mathfrak{G}}$, die $\mathfrak{P}_{\nu\mu}$ ungeändert lassen. Offenbar ist also

31 I

$\overline{\mathfrak{G}}_{(\nu\mu)Z}$ der Durchschnitt der Zerlegungsgruppe $\mathfrak{G}_{(\nu\mu)Z}$ mit $\overline{\mathfrak{G}}$ □□□

Offenbar sind die □□□ Zerlegungsgruppen

$$\overline{\mathfrak{G}}_{(\nu 1)Z}, \overline{\mathfrak{G}}_{(\nu 2),Z}, \dots, \overline{\mathfrak{G}}_{(\nu r_\nu),Z}$$

der Primideale $\mathfrak{P}_{\nu 1}, \mathfrak{P}_{\nu 2}, \dots, \mathfrak{P}_{\nu r_\nu}$ die in $\mathfrak{q}_\nu$ aufgehen als konjugierte Gruppen (in Bezug auf $\overline{\mathfrak{G}}$, Definition 2, S. 23▶) zu einander isomorph, sodaß das Studium einer von ihnen genügt.

Die Trägheitsgruppe $\overline{\mathfrak{G}}_{(\nu\mu)T}$ von $\mathfrak{P}_{\mu\nu}$ in Bezug auf $\overline{K}$ ist ersichtlich wieder der Durchschnitt der Trägheitsgruppe $\mathfrak{G}_{(\nu\mu)T}$ von $\mathfrak{P}_{\nu\mu}$ in Bezug auf k mit $\overline{\mathfrak{G}}$. Ihr Index in Bezug auf $\overline{\mathfrak{G}}_{(\nu\mu)Z}$ ist $\mathfrak{f}_\nu$. Die Zahlen $r_\nu, \mathfrak{f}_\nu$ und somit e_ν sind also gruppentheoretisch bestimmt.

Die so festgelegten Primideale $\mathfrak{q}_\nu$ aus $\overline{K}$ sind alle verschieden, da die $\mathfrak{P}_{\nu\mu}$ verschieden sind, und folglich relativ prim. Es sind alle Teiler von $\mathfrak{p}$ in $\overline{K}$. Sei nun

$$\mathfrak{p} = \mathfrak{q}_1^{a_1} \dots \mathfrak{q}_\lambda^{a_\lambda}.$$

Setzen wir für $\mathfrak{q}_\nu$ die Zerlegungen ein, so tritt $\mathfrak{P}_{\nu\mu}$ mit dem Exponenten $a_\nu e_\nu$ auf. Es ist also

$$a_\nu e_\nu = e$$

und damit auch die a_ν bestimmt. Die Zahlen r_ν müssen natürlich noch der Relation

$$r_1 + r_2 + \cdots + r_\lambda = r$$

genügen, damit die Anzahl der $\mathfrak{P}_{\nu\mu}$ stimmt.

Um schließlich noch den Grad $\mathfrak{f}'_\nu$ von $\mathfrak{q}_\nu$ in Bezug auf k zu bestimmen, bilden wir die Relativnorm

32 ı

von

$$\mathfrak{q}_\nu = (\mathfrak{P}_{\nu 1}\mathfrak{P}_{\nu 2}\ldots\mathfrak{P}_{\nu r_\nu})^{e_\nu}$$

erst in K in Bezug auf $\overline{K}$ □□□ , dies ergibt:

$$\mathfrak{q}_\nu^{\overline{n}} = n_{(K,\overline{K})}\left[(\mathfrak{P}_{\nu 1}\ldots\mathfrak{P}_{\nu r_\nu})^{e_\nu}\right]$$

dann die Relativnorm in $\overline{K}$ in Bezug auf k, dies ergibt:

$$\begin{aligned}\mathfrak{p}^{\overline{n}\mathfrak{f}'_\nu} &= n_{(K,k)}\left[(\mathfrak{P}_{\nu 1}\ldots\mathfrak{P}_{\nu r_\nu})\right]^{e_\nu}\\ &= \mathfrak{p}^{\mathfrak{f}r_\nu e_\nu}\end{aligned}$$

Es ist also

$$\overline{n}\mathfrak{f}'_\nu = \mathfrak{f}r_\nu e_\nu$$

Da ferner $\overline{n} = e_\nu\mathfrak{f}_\nu r_\nu$ ist, folgt:

$$\mathfrak{f}_\nu\mathfrak{f}'_\nu = \mathfrak{f}$$

Wir haben jetzt insgesamt folgende Vorschrift zur Bestimmung der Zerlegung von $\mathfrak{p}$ in $\overline{K}$, wenn die in K bekannt ist:

Satz 13. Ist die Zerlegung von $\mathfrak{p}$ in K gegeben:

$$\mathfrak{p} = (\mathfrak{P}_1\ldots\mathfrak{P}_r)^e, \quad (\mathfrak{P}_\nu \text{ vom Grad } \mathfrak{f})$$

so findet man die Zerlegung von $\mathfrak{p}$ in einem Unterkörper $\overline{K}$ von K, der zur Untergruppe $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ gehört folgendermaßen:

Man wende auf die $\mathfrak{P}_\nu$ die Substitutionen von $\overline{\mathfrak{G}}$ an, wodurch sie in λ Verbände von je r_ν Primidealen $\mathfrak{P}_{\nu 1},\ldots,\mathfrak{P}_{\nu r_\nu}$; $(\nu = 1,2,\ldots,\lambda)$ zerfallen, derart daß durch $\overline{\mathfrak{G}}$ nur die Ideale der einzelnen Verbände zusammenhängen.

33

Dabei ist also $r_1 + r_2 + \cdots + r_\nu = r$. Nun bilde man die Zerlegungsgruppe von $\mathfrak{P}_{\nu\mu}$ in Bezug auf k, die $\mathfrak{G}_{(\nu\mu)Z}$ sein möge, und ihren Durchschnitt $\overline{\mathfrak{G}}_{(\nu\mu)Z}$ mit $\overline{\mathfrak{G}}$. Dann ist $\overline{\mathfrak{G}}_{(\nu\mu)Z}$ die Zerlegungsgruppe von $\mathfrak{P}_{\nu\mu}$ in Bezug auf $\overline{K}$ und ihr Index in Bezug auf $\overline{\mathfrak{G}}$ liefert die Anzahl der mit $\mathfrak{P}_{\nu\mu}$ in einem Verbande vorkommenden Primideale, r_ν.

Ferner bilde man die Trägheitsgruppe $\mathfrak{G}_{(\nu\mu)T}$ von $\mathfrak{P}_{\nu\mu}$ in Bezug auf k und ihren Durchschnitt $\overline{\mathfrak{G}}_{(\nu\mu)T}$ mit $\overline{\mathfrak{G}}$. Er ist die Trägheitsgruppe von $\mathfrak{P}_{\nu\mu}$ in Bezug auf $\overline{K}$.

Der Grad von $\overline{\mathfrak{G}}_{(\nu\mu)T}$ sei e_ν, der Index in Bezug auf $\overline{\mathfrak{G}}_{(\nu\mu)Z}$ sei $\mathfrak{f}_\nu$. Dann ist $e_\nu \mathfrak{f}_\nu r_\nu = \overline{n}$, wo $\overline{n}$ der Grad von $\overline{\mathfrak{G}}$ ist.

Setzt man weiter $a_\nu e_\nu = e$ und $\mathfrak{f}_\nu \mathfrak{f}'_\nu = \mathfrak{f}$ so gilt:

$$\mathfrak{q}_\nu = (\mathfrak{P}_{\nu 1} \ldots \mathfrak{P}_{\nu r_\nu})^{e_\nu}$$

ist ein Primideal von $\overline{K}$. Die Relativgrade der $\mathfrak{P}_{\nu\mu}$ in Bezug auf $\overline{K}$ sind $\mathfrak{f}_\nu$. $\mathfrak{q}_\nu$ selbst hat den Relativgrad $\mathfrak{f}'_\nu$ in Bezug auf k.

Ferner ist:

$$\mathfrak{p} = \mathfrak{q}_1^{a_1} \ldots \mathfrak{q}_\lambda^{a_\lambda}$$

die Zerlegung von $\mathfrak{p}$ in Primideale in $\overline{K}$. Ist also $\overline{m}$ der Index von $\overline{\mathfrak{G}}$ in Bezug auf $\mathfrak{G}$, also der Grad von $\overline{K}$ in Bezug auf k, so muß die Relation:

$$a_1 \mathfrak{f}'_1 + \cdots + a_\lambda \mathfrak{f}'_\lambda = \overline{m}$$

bestehen.

34

Diese Vorschrift haben wir nun anzuwenden auf die durch das Primideal $\mathfrak{P}$ erzeugten Unterkörper von K:

Definition 4. Der zur Zerlegungsgruppe $\mathfrak{G}_Z$ von $\mathfrak{P}$ in Bezug auf k gehörige Unterkörper K_Z von K vom Relativgrad r in Bezug auf k heißt der *Zerlegungskörper* des Primideals $\mathfrak{P}$.

Wenden wir nach Vorschrift von Satz 13 die Substitutionen von $\mathfrak{G}_Z$ auf $\mathfrak{P}$ an, so geht durch sie nach Definition $\mathfrak{P}$ in sich über. $\mathfrak{P}$ bildet also einen Verband für sich, sodaß $r_1 = 1$ ist.

Da die Trägheitsgruppe $\mathfrak{G}_T$ von $\mathfrak{P}$ Untergruppe von $\mathfrak{G}_Z$ ist, ist ihr jetzt zu bildender Durchschnitt mit $\mathfrak{G}_Z$ wieder $\mathfrak{G}_T$. Es sind also $\mathfrak{G}_Z$ und $\mathfrak{G}_T$ auch die Zerlegungs– u. Trägheitsgruppen in Bezug auf K_Z. Also ist $\mathfrak{f}_1 = \mathfrak{f}$; $e_1 = e$; $a_1 = 1$; $\mathfrak{f}'_1 = 1$. Somit ist

$$\mathfrak{P}^e = \mathfrak{q}$$

ein Primideal ersten □□□ Relativgrades in K_Z und geht genau einmal in $\mathfrak{p}$ auf. Der Grad $\mathfrak{f}_1$ von $\mathfrak{P}$ in Bezug auf K_Z ist derselbe wie in Bezug auf k[7], nämlich $\mathfrak{f}$.

Satz 14. Ist $\mathfrak{P}^e$ die höchste Potenz von $\mathfrak{P}$, durch die $\mathfrak{p}$ teilbar ist, und $\mathfrak{f}$ der Relativgrad von $\mathfrak{P}$ in Bezug auf k, so ist $\mathfrak{q} = \mathfrak{P}^e$ ein Primideal ersten Grades in Bezug auf k im Zerlegungskörper K_Z.

35 ı

Definition 5. Der zur Trägheitsgruppe von $\mathfrak{P}$ in Bezug auf k gehörige Unterkörper K_T von K, gleichzeitig Oberkörper von K_Z, heißt der *Trägheitskörper* des Primideals $\mathfrak{P}$. K_T hat den Grad $r\mathfrak{f}$ in Bezug auf k, $\mathfrak{f}$ in Bezug auf K_Z, und K den Grad e in Bezug auf K_T. Da die Faktorgruppe $\frac{\mathfrak{G}_Z}{\mathfrak{G}_T}$ zyklisch ist, ist K_T relativ zyklisch vom Grade $\mathfrak{f}$ in Bezug auf K_Z.

Um nun □□□ die weitere Zerlegung von $\mathfrak{p}$ bei Übergang von K_Z zu K_T zu verfolgen, wenden wir gemäß Satz 13 $\mathfrak{G}_T$ auf $\mathfrak{P}$ an. Da $\mathfrak{G}_T$ Untergruppe von $\mathfrak{G}_Z$ bleibt $\mathfrak{P}$ ungeändert, bildet also einen Verband für sich: $r_1 = 1$. Der Durchschnitt der Zerlegungsgruppe $\mathfrak{G}_Z$ von $\mathfrak{P}$ in Bezug auf k mit $\mathfrak{G}_T$, also $\mathfrak{G}_T$ selbst, ist die Zerlegungsgruppe von $\mathfrak{P}$ in Bezug auf K_T. Ebenso ist der Durchschnitt der Trägheitsgruppe $\mathfrak{G}_T$ von $\mathfrak{P}$ in Bezug auf k mit $\mathfrak{G}_T$ die Trägheitsgruppe von $\mathfrak{P}$ in Bezug auf K_T. $\mathfrak{G}_T$ ist also sowohl Trägheits–, wie Zerlegungsgruppe von $\mathfrak{P}$ in Bezug auf K_T. Es ist also:

$$r_1 = 1; \quad e_1 = e; \quad \mathfrak{f}_1 = 1; \quad a_1 = 1; \quad \mathfrak{f}'_1 = \mathfrak{f}$$

Somit ist wieder

$$\mathfrak{q} = \mathfrak{P}^e$$

ein Primideal in K_T. Sein Relativgrad $\mathfrak{f}'_1$ in Bezug auf k ist $\mathfrak{f}$ (in K_Z war er noch 1), während $\mathfrak{P}$ in Bezug auf K_T den Relativgrad $\mathfrak{f}_1 = 1$ hat (in Bezug auf K_Z noch $\mathfrak{f}$).

[7] undeutlich; vielleicht auch 'K'

□□□

$\mathfrak{q}$ ist also:

$$\left.\begin{array}{llllllllllll} 1.) & \text{als} & \text{Primideal} & \text{in} & K_Z & : & \text{vom} & \text{Rel.} & \text{Gr.} & 1 & \text{zu} & k \\ 2.) & \shortparallel & \shortparallel & \shortparallel & K_T & : & \shortparallel & \shortparallel & \shortparallel & \mathfrak{f} & \shortparallel & k \\ 3.) & \shortparallel & \shortparallel & \shortparallel & \shortparallel & : & \shortparallel & \shortparallel & \shortparallel & \mathfrak{f} & \shortparallel & K_Z \end{array}\right\}$$

$$\text{stets } \mathfrak{q} = \begin{cases} = \mathfrak{P}^e \\ = \mathfrak{P}^e \\ = \mathfrak{P}^e \end{cases}$$

Satz 15. Das Primideal $\mathfrak{q} = \mathfrak{P}^e$ wird im Trägheitskörper nicht weiter zerlegt, sondern bleibt Primideal. Sowohl in Bezug auf k als K_Z hat jedoch $\mathfrak{q}$ jetzt den Relativgrad $\mathfrak{f}$. In Bezug auf K_T ist $\mathfrak{P}$ nunmehr Primideal ersten Grades.

Der Vorgang ist also der:

1.) Durch Adjunktion von K_Z zu k wird aus $\mathfrak{p}$ ein Primideal $\mathfrak{q}$ vom ersten Grade abgespalten. Dieses zerfällt, wenn K jetzt als Oberkörper von K_Z betrachtet wird, in K in die e–te Potenz eines Primideals $\mathfrak{P}$ vom Relativgrade $\mathfrak{f}$ zu K_Z (und k).

2.) Durch Adjunktion von K_T zu k □□□ wird aus $\mathfrak{p}$ ein Primideal $\mathfrak{f}$–ten Grades $\mathfrak{q}$ abgespalten. Dieses zerfällt in K in die e–te Potenz eines Primideals $\mathfrak{P}$ vom Relativgrade 1 zu K_T.

3.) Beim Übergang von K_Z zu K_T erhöht sich also lediglich der Grad von $\mathfrak{q}$ von 1 auf $\mathfrak{f}$.

Nun sei wieder q die Norm von $\mathfrak{p}$ in Bezug auf den rationalen Körper: $\mathsf{N}(\mathfrak{p}) = p^\nu = q$. Da q in K_T den Relativgrad $\mathfrak{f}$ hat, ist

$$\mathsf{N}_{K_T}(\mathfrak{q}) = n_{K_T}\mathsf{N}(\mathfrak{q}) = \mathsf{N}(\mathfrak{p}^\mathfrak{f}) = q^\mathfrak{f}$$

In K_T zerfallen also die Zahlen mod $\mathfrak{q}$ in $q^{\mathfrak{f}}$ Restklassen. Sind nun zwei Zahlen aus K_T mod $\mathfrak{q}$ inkongruent, so hat ihre Differenz mit q keinen Teiler gemein, □□□ da $\mathfrak{q}$ in K_T Primideal, also auch nicht mit $\mathfrak{P}$. Da nun $\mathfrak{P}$ in Bezug auf k ebenfalls den Relativgrad $\mathfrak{f}$ hat, die Anzahl der Restklassen mod $\mathfrak{P}$ in K also ebenfalls $q^{\mathfrak{f}}$ ist, und wie eben gezeigt, zwei mod $\mathfrak{q}$ inkongruente Zahlen von K_T ebenfalls mod $\mathfrak{P}$ inkongruent sind, folgt:

Satz 16. Die Restklassen von K_T mod $\mathfrak{q}$ bilden ein vollständiges System von Restklassen auch in K mod $\mathfrak{P}$.

Wir bestimmen jetzt die Gruppe $\mathfrak{G}_v(\mathfrak{P})$ aller Substitutionen von $\mathfrak{G}$, für die für jede Körperzahl ω: □□□

$$\omega/v \equiv \omega \mod \mathfrak{P}^2$$

gilt. Ihre Substitutionen seien $v, v_1, \ldots$. Ersichtlich ist $\mathfrak{G}_0$ Untergruppe von $\mathfrak{G}_T$. Ist ferner σ_1 eine Substitution von $\mathfrak{G}$, die $\mathfrak{P}$ in $\mathfrak{P}_1$ überführt:

$$\mathfrak{P}/\sigma_1 = \mathfrak{P}_1$$

und setzen wir: $\omega/\sigma_1^{-1} = \omega_1$

so ist: $\omega/v = \omega_1 + \pi; \quad (\pi \equiv 0 \bmod \mathfrak{P}^2).$

Da ferner $\pi/\sigma_1 = \pi_1 \equiv 0 \bmod \mathfrak{P}_1^2$

ist, folgt:

$$\omega/\sigma_1^{-1}v\sigma_1 = \omega_1/v\sigma_1 = (\omega_1 + \pi)/\sigma_1 = \omega + \pi_1 \equiv \omega \bmod \mathfrak{P}_1^2$$

Es ist also

$$\sigma_1^{-1}\mathfrak{G}_v(\mathfrak{P})\sigma_1 = \mathfrak{G}_v(\mathfrak{P}_1)$$

Ist σ_1 eine Substitution aus $\mathfrak{G}_Z$ oder $\mathfrak{G}_T$, so ist $\mathfrak{P}/\sigma_1 = \mathfrak{P}_1 = \mathfrak{P}$ also $\sigma_1^{-1}\mathfrak{G}_v(\mathfrak{P})\sigma_1 = \mathfrak{G}_v(\mathfrak{P})$ und somit $\mathfrak{G}_v$ *invariante* Untergruppe von $\mathfrak{G}_Z$ und $\mathfrak{G}_T$.

Es sei nun □□□

$$\pi \equiv 0 \bmod \mathfrak{P} \quad \text{aber nicht mod } \mathfrak{P}^2\big\} \quad \text{in } K$$

(Von π dürfen wir ferner voraussetzen, daß es K erzeugt (prim. Element von K ist), denn wäre dies nicht der Fall und erzeugt β den Körper K, so hat $\pi + \beta p^2$ die gleichen Kongruenzeigenschaften wie π, erzeugt aber K).

Durchläuft nun ξ ein volles Restsystem mod $\mathfrak{P}$, so durchläuft $\pi\xi$ alle durch $\mathfrak{P}$ teilbaren Restklassen mod $\mathfrak{P}^2$. Ist also $\alpha \equiv 0 \bmod \mathfrak{P}$, so ist die Kongruenz

$$\pi\xi \equiv \alpha \mod \mathfrak{P}^2$$

stets lösbar.

Sei nun v eine Substitution aus $\mathfrak{G}_T$ für die

$$\pi/v \equiv \pi \mod \mathfrak{P}^2$$

ist. Ist ω irgendeine Zahl aus K, so gibt es ein ω_0 aus K_T (Satz 16), so daß

$$\omega \equiv \omega_0 \mod \mathfrak{P}$$

ist. Wir bestimmen dann, wie eben gezeigt, ξ aus der Kongruenz

$$\pi\xi \equiv \omega - \omega_0$$

da v zu $\mathfrak{G}_T$ gehört und ω_0 zu K_T ist:

$$\omega_0/v = \omega_0$$

und

$$\xi/v \equiv \xi \mod \mathfrak{P}$$

also

$$(\pi\xi)/v \equiv \pi\xi \mod \mathfrak{P}^2$$

39 I

Also ist: □□□

$$(\omega - \omega_0)/v \equiv \omega - \omega_0 \mod \mathfrak{P}^2$$

und also

$$w/v \equiv \omega \mod \mathfrak{P}^2$$

v gehört also zu $\mathfrak{G}_v$. Ist umgekehrt v eine Substitution aus $\mathfrak{G}_v$, so ist sicher

$$\pi/v \equiv \pi \mod \mathfrak{P}^2$$

und erst v zu $\mathfrak{G}_T$ gehörig.

Demnach läßt sich $\mathfrak{G}_0$ auch erklären als die Gesamtheit derjenigen Substitutionen von $\mathfrak{G}_T$, die nur die Bedingung

$$\pi/v \equiv \pi \mod \mathfrak{P}^2$$

erfüllen, wo π eine bestimmte „Primzahl“ zu $\mathfrak{P}$ ist.

Sei nun τ irgendeine Substitution von $\mathfrak{G}_\tau$[8]. Dann ist wenigstens

$$\pi/\tau \equiv \pi \mod \mathfrak{P}$$

also auch π/τ durch $\mathfrak{P}$ teilbar. π/τ ist aber auch „Primzahl“ für $\mathfrak{P}$. Denn sonst wäre

$$\pi/\tau\tau^{-1} = \pi \quad \text{durch } \tau^{-1}\mathfrak{P}^2 = \mathfrak{P}^2 \text{ teilbar.}$$

Da $\pi/\tau \equiv 0 \bmod \mathfrak{P}$, ist die Kongruenz

$$\pi\xi \equiv \pi/\tau \mod \mathfrak{P}^2$$

sicher lösbar. Daher ist $\xi \not\equiv 0 \bmod \mathfrak{P}$, da sonst $\pi/\tau \equiv 0(\mathfrak{P}^2)$ wäre.

Ist nun ϱ eine primitive Wurzel mod $\mathfrak{P}$ und wie früher $\mathsf{N}(\mathfrak{P}) = q^{\mathfrak{f}}$, so stellen die Zahlen

$$1, \varrho, \varrho^2, \ldots, \varrho^{q^{\mathfrak{f}}-2}$$

alle $q^{\mathfrak{f}} - 1$ zu $\mathfrak{P}$ teilerfremden Restklassen dar. Wir können also eindeutig setzen:

$$\xi \equiv \varrho^\lambda \mod \mathfrak{P}$$

Zu jedem τ aus $\mathfrak{G}_\tau$ gibt es also eindeutig ein λ, sodaß

$$\pi/\tau \equiv \pi \cdot \varrho^\lambda \bmod \mathfrak{P}^2; \quad (\lambda = 0, 1, \ldots q^{\mathfrak{f}} - 2).$$

[8] uneindeutiges Schriftbild (auch an späteren Stellen): τ oder T ?

wird. Für $\lambda = 0$ gehört τ zu $\mathfrak{G}_v$.

Unter allen vorkommenden Werten von λ sei a der kleinste positive, der etwa zu τ_0 gehört:

$$\pi/\tau_0 \equiv \pi\varrho^a \mod \mathfrak{P}^2$$

□□□

und demnach

$$\pi/\tau_0^2 \equiv \pi/\tau_0\Big/\tau_0 \equiv \pi\cdot\varrho^a/\tau_0 \equiv \pi\varrho^{2a} \mod \mathfrak{P}^2$$

. . . . . .

(da $\varrho^2/\tau_0 \equiv \varrho^2 \mod \mathfrak{P}$, weil τ_0 zu $\mathfrak{G}_T$)

allgemein

$$\pi/\tau_0^\nu \equiv \pi\varrho^{a\nu} \mod \mathfrak{P}^2.$$

Ist andererseits λ ein vorkommender Exponent, so setzen wir:

$$\lambda \equiv \nu a + a'; \quad (0 \leqq a' < a)$$

λ komme bei τ vor. Dann setzen wir:

$$\tau' \equiv \tau_0^{-\nu}\tau$$

sodaß

$$\pi/\tau' = \pi/\tau_0^{-\nu}\tau \equiv \pi\varrho^{-a\nu}/\tau \equiv \pi\varrho^{\lambda-a\nu} \equiv \pi\varrho^{a'} \mod \mathfrak{P}^2$$

Es muß also nach Bestimmung von a der Exponent $a' = 0$ sein, d.h. jedes vorkommende λ ist durch a teilbar. Es können also gerade die Exponenten $0, a, 2a, \ldots$ vorkommen. a muß Teiler von $q^\mathfrak{f} - 1$ sein; denn setzen wir

$$q^\mathfrak{f} - 1 = \nu a + a'; \quad (0 \leqq a' < a)$$

so ist

$$\pi/\tau_0^{-\nu} \equiv \pi\varrho^{-\nu a} \equiv \pi\varrho^{q^\mathfrak{f}-1-\nu a} \equiv \pi\varrho^{a'} \mod \mathfrak{P}^2$$

sodaß $a' = 0$ sein muß. Setzen wir also:

$$ah = q^\mathfrak{f} - 1$$

so kommen höchstens die h Exponenten

$$0, a, 2a, \ldots, (h-1)a$$

vorkommen, diese aber auch sicher bei $1, \tau_0, \tau_0^2, \ldots, \tau_0^{h-1}$

Nun folgt aus

$$\pi/\tau_1 \equiv \pi/\tau_0^\nu \mod \mathfrak{P}^2$$

auch:

$$\pi/\tau_0^\nu \tau_1^{-1} \equiv \pi \mod \mathfrak{P}^2$$

$\tau_0^\nu \tau_1^{-1}$ ist als Substitution aus $\mathfrak{G}_0$ d.h. τ_1 gehört zur Nebengruppe $\mathfrak{G}_0\tau_0^\nu$ [9]. Ist umgekehrt τ_1 ein Element aus □□□ der Nebengruppe $\mathfrak{G}_\nu\tau_0^\nu$:

$$\tau_1 = v\tau_0^\nu$$

so ist

$$\pi/\tau_1 \equiv \pi/v\tau_0^\nu \equiv \pi/\tau_0^\nu \mod \mathfrak{P}^2$$

Da nun für jedes τ_1 aus $\mathfrak{G}_T$ sicher eine Kongruenz

$$\pi/\tau_1 \equiv \pi\varrho^{\nu a} \equiv \pi/\tau_0^\nu \quad (0 \leqq \nu \leqq h-1)$$

besteht, folgt somit, daß die Nebengruppen durch $\mathfrak{G}_v\tau_0^\nu$ gerade erschöpft werden:

$$\mathfrak{G}_\tau = \mathfrak{G}_v + \mathfrak{G}_v\tau_0 + \cdots + \mathfrak{G}_v\tau_0^{h-1}.$$

Da $\mathfrak{G}_v$ invariante Untergruppe von $\mathfrak{G}_\tau$ ist, geht aus der Zerlegung noch hervor, daß der Index h von $\mathfrak{G}_v$ nach $\mathfrak{G}_\tau$ ein Teiler von $q^\mathfrak{f} - 1$ ist. Die Faktorgruppe $\frac{\mathfrak{G}_\tau}{\mathfrak{G}_v}$ ferner ist zyklisch vom Grade h.

42 I

Es ist schließlich noch der Grad g von $\mathfrak{G}_v$ zu bestimmen, der offenbar der Bedingung $gh = e$ genügt (e ist Grad von $\mathfrak{G}_T$).

Sei v eine Substitution von $\mathfrak{G}_v$. Dann ist

$$\pi/v \equiv \pi \mod \mathfrak{P}^2$$

Also ist nach entsprechenden Schlüssen, wie S. 38▶, die Kongruenz

$$\pi^2\xi \equiv \pi/v - \pi \mod \mathfrak{P}^3$$

sicher lösbar. Wir können also setzen:

$$\pi/v \equiv \pi + \pi^2\xi \mod \mathfrak{P}^3.$$

[9] undeutlich

Da $\xi/v \equiv \xi \bmod \mathfrak{P}$, also $(\pi^2\xi)/v \equiv \pi^2\xi \bmod \mathfrak{P}^3$, wird

$$\left.\begin{array}{rcl} \pi/v^2 & \equiv & \pi + 2\pi^2\xi \\ \pi/v^3 & \equiv & \pi + 3\pi^2\xi \\ \cdots\cdots\cdots\cdots & & \\ \pi/v^p & \equiv & \pi + p\pi^2\xi \\ & \equiv & \pi \end{array}\right\} \bmod \mathfrak{P}^3$$

□□□

Sei schon gezeigt, daß

$$\pi/v^{p^\nu} \equiv \pi \mod \mathfrak{P}^{\nu+2},$$

so bestimmen wir ξ so, daß

$$\pi/v^{p^\nu} \equiv \pi + \pi^{\nu+2}\xi \mod \mathfrak{P}^{\nu+3}$$

Wiederholte Anwendung von v^{p^ν} zeigt, daß

$$\left.\begin{array}{rcl} \pi/v^{2p^\nu} & \equiv & \pi + 2\pi^{\nu+2}\xi \\ \cdots\cdots\cdots\cdots & & \\ \pi/v^{p^{\nu+1}} & \equiv & \pi + p\pi^{\nu+2}\xi \equiv \pi \end{array}\right\} \bmod \mathfrak{P}^{\nu+3}$$

Die Formel:

$$\pi/v^{p^\nu} \equiv \pi \mod \mathfrak{P}^{\nu+2}$$

ist also allgemein richtig. Da nun, wie wir früher zeigten,

die „Primzahl“ π als *primitives* Element aus K gewählt werden darf, können die verschiedenen Werte

$$\pi/\sigma - \pi,$$

wo σ zu $\mathfrak{G}$ gehört, nicht durch beliebig hohe Potenzen von $\mathfrak{P}$ teilbar sein, wenn $\sigma \neq 1$ ist. Es muß also schließlich einmal $v^{p^\nu} = 1$ sein. Der Exponent von v ist demnach eine gewisse Potenz von p, und da dieses für jedes Element aus $\mathfrak{G}_v$ gilt, muß der Grad g von $\mathfrak{G}_v$ □□□ ebenfalls Potenz von p sein. Da der Index h zu $\mathfrak{G}_\tau$ Teiler von $q^{\mathfrak{f}} - 1$, also zu p prim ist, folgt aus

$$e = gh$$

daß g die höchste in e enthaltene Potenz von p ist: $g = p^\kappa$

Definition 6a. Die Substitutionen v aus $\mathfrak{G}$, für die bei jeder Körperzahl ω:

$$\omega/v \equiv \omega \mod \mathfrak{P}^2$$

ist, bilden eine Gruppe $\mathfrak{G}_v$, die *Verzweigungsgruppe* von $\mathfrak{P}$. $\mathfrak{G}_v$ ist invariante Untergruppe von $\mathfrak{G}_\tau$ und $\mathfrak{G}_Z$ und die Verzweigungsgruppen der übrigen in $\mathfrak{p}$ aufgehenden Primideale die in Bezug auf $\mathfrak{G}$ konjugierten Gruppen von $\mathfrak{G}_v$. $\mathfrak{G}_v$ hat den Grad p^κ, wo p^κ die höchste in der Relativordnung von $\mathfrak{P}$ zu k enthaltene Potenz von p ist, ferner in Bezug auf $\mathfrak{G}_T$ den index h, wenn

$$e = p^\kappa h$$

gesetzt wird. h ist notwendig Teiler von $q^\mathfrak{f} - 1 = \mathsf{N}_K(\mathfrak{P}) - 1$. Die Gruppe $\frac{\mathfrak{G}_T}{\mathfrak{G}_v}$ ist zyklisch vom Grade h.

44 ı

Definition 6b. Der zur Gruppe $\mathfrak{G}_v$ gehörige Unterkörper K_v von K heißt der Verzweigungskörper von $\mathfrak{P}$. Er ist relativ–zyklisch vom Grade h in Bezug auf K_T, vom Grade $\mathfrak{f}h$ in Bezug auf K_Z, vom Grade $r\mathfrak{f}h$ in Bezug auf k.

Um die Vorschrift von Satz 13 anzuwenden auf das Primideal $\mathfrak{q} = \mathfrak{P}^e$ in K_T und K_Z, haben wir den Durchschnitt von $\mathfrak{G}_v$ mit $\mathfrak{G}_Z$ und $\mathfrak{G}_T$ zu bilden, der beidesmal $\mathfrak{G}_v$ ist. $\mathfrak{G}_v$ ist also für $\mathfrak{P}$ in Bezug auf K_v Trägheits– und Zerlegungsgruppe. Also ist in der dortigen Bezeichnung

$$\begin{array}{l} r_1 = 1; \\ e_1 = p^\kappa; \\ a_1 = h \end{array} \quad \left\{ \begin{array}{llll} \mathfrak{f}_1 = 1; & \mathfrak{f}_1' = \mathfrak{f} & \text{für} & K \text{ oder } K_Z \text{ als Grundbereich} \\ \mathfrak{f}_1 = 1; & \mathfrak{f}_1' = 1 & \text{"} & K_T \text{ als Grundbereich.} \end{array} \right.$$

Also:

Satz 17. Das Primideal $\mathfrak{q} = \mathfrak{P}^e$ des Zerlegungs– und Trägheitskörpers wird in K_v die h–te Potenz eines Primideals $\mathfrak{q}_1 = \mathfrak{P}^{p^\kappa}$:

$$\mathfrak{q} = \mathfrak{q}_1^h$$

In Bezug auf K_v hat $\mathfrak{P}$ den ersten Grad; □□□ das Primideal $\mathfrak{q}_1$ in K_v hat die Relativgrade:

$$\begin{array}{ccccc} 1 & \text{in} & \text{Bezug} & \text{auf} & K_T \\ \mathfrak{f} & \text{"} & \text{"} & \text{"} & K_Z \\ \mathfrak{f} & \text{"} & \text{"} & \text{"} & k \end{array}$$

Beim Übergang von K_T zu K_v wird also $\mathfrak{q}$ in die h–te Potenz eines Primideals $\mathfrak{q}_1$ in K_v zerlegt.

45 ı

So fortfahrend bilden wir die „*höheren Verzweigungsgruppen*“ $\square\square\square\ \mathfrak{V}_i$. In $\mathfrak{V}_i$ sollen alle die Substitutionen v_i enthalten sein, für die

$$\omega/v_i \equiv \omega \mod \mathfrak{P}^{i+1}$$

für jedes ganze ω aus K gilt. Wie früher läßt sich zeigen, daß $\mathfrak{V}_i$ invariante Untergruppe aller vorhergehend gebildeten Gruppen $\mathfrak{G}_Z, \mathfrak{G}_T, \mathfrak{G}_v, \mathfrak{V}_2, \mathfrak{V}_3, \ldots,$ $\mathfrak{V}_{i-1}$ ist und daß die Gruppe $\mathfrak{V}_i$ eines anderen in $\mathfrak{p}$ aufgehenden Primideals aus $\mathfrak{V}_i$ durch Transformation (in Bezug auf $\mathfrak{G}$) hervorgeht. Als Untergruppe von $\mathfrak{G}_v$ ist der Grad von $\mathfrak{V}_i$ eine Potenz von p, er sei p^{κ_i}. Da die definierende Kongruenz für genügend hohes i nur für die identische Substitution stets erfüllt sein kann, wird schließlich $\mathfrak{V}_i = 1$; $\kappa_i = 0$. Ferner können mehrere aufeinanderfolgende $\mathfrak{V}_i$ miteinander übereinstimmen.

Sei wieder π eine durch $\mathfrak{P}$ aber nicht durch $\mathfrak{P}^2$ teilbare Zahl. Ist v_i eine Substitution aus $\mathfrak{V}_i$, so bilden wir die Größe ξ aus der wegen

$$\omega/v_i \equiv \omega \mod \mathfrak{P}^{i+1}$$

stets lösbaren Kongruenz

$$\omega/v_i \equiv \omega + \xi\pi^{i+1} \mod \mathfrak{P}^{i+2}$$

Dabei ist wegen $\xi/v_i' \equiv \xi \bmod \mathfrak{P}^{i+1}$ sicher

$$\xi\pi^{i+1}/v_i' \equiv \xi\pi^{i+1} \mod \mathfrak{P}^{i+2}$$

für jedes v_i' aus $\mathfrak{V}_i$.

46 ı

Gilt also für v_i':

$$\omega/v_i' \equiv \omega + \eta\pi^{i+1} \mod \mathfrak{P}^{i+2}$$

so ist:

$$\begin{aligned} \omega/v_i'v_i &\equiv \omega + (\xi+\eta)\pi^{i+1} \bmod \mathfrak{P}^{i+2} \\ &\equiv \omega/v_iv_i' \bmod \mathfrak{P}^{i+2} \end{aligned}$$

oder, wenn man $v_i^{-1}v_i'^{-1}$ auf die Gleichung

$$\omega/v_iv_i' = \omega/v_i'v_i + \pi_{i+2}\,,$$

wo π_{i+2} durch $\mathfrak{P}^{i+2}$ teilbar, so folgt:

$$\omega/v_iv_i'v_i^{-1}v_i'^{-1} \equiv \omega \mod \mathfrak{P}^{i+2}$$

Es ist also $v_iv_i'v_i^{-1}v_i'^{-1}$ eine Substitution aus $\mathfrak{V}_{i+1}$. Sind also $v_i\mathfrak{V}_{i+1}$ und $v_i'\mathfrak{V}_{i+1}$ zwei Nebengruppen folgt wegen $v_iv_i' = v_i'v_iv_{i+1}$ für sie

$$v_i\mathfrak{V}_{i+1}\cdot v_i'\mathfrak{V}_{i+1} = v_iv_i'\mathfrak{V}_{i+1} = v_i'v_iv_{i+1}\mathfrak{V}_{i+1} \\ = v_i'v_i\mathfrak{V}_{i+1} = v_i'\mathfrak{V}_{i+1}\cdot v_i\mathfrak{V}_{i+1}\,.$$

Es ist also $\frac{\mathfrak{V}_i}{\mathfrak{V}_{i+1}}$ kommutativ.
Endlich folgt aus

$$\begin{array}{rcll} \omega/v_i & \equiv & \omega + \pi^{i+1}\xi & \mod \mathfrak{P}^{i+2} \\ \omega/v_i^2 & \equiv & \omega + 2\pi^{i+1}\xi & \mod \mathfrak{P}^{i+2} \\ \cdots & \cdots & \cdots & \cdots \\ \omega/v_i^p & \equiv & \omega & \mod \mathfrak{P}^{i+2} \end{array}$$

sodaß v_i^p stets eine Substitution aus $\mathfrak{V}_{i+1}$ ist.

Definition 7. Die Gruppe der Substitutionen v_i, für die bei jeder ganzen Körperzahl $\omega/v_i \equiv \omega \mod \mathfrak{P}^{i+1}$ gilt, heißt die i–te Verzweigungsgruppe $\mathfrak{V}_i$ von $\mathfrak{P}$. Sie ist invariante Untergruppe aller niedrigeren Verzweigungsgruppen und von $\mathfrak{G}_Z$ und $\mathfrak{G}_T$

Ihr Grad ist eine Potenz p^{κ_i} von p. Für genügend hohe i wird $\mathfrak{V}_i = 1$. Die Gruppe $\frac{\mathfrak{V}_i}{\mathfrak{V}_{i+1}}$ ist kommutativ und für jedes v_i aus $\mathfrak{V}_i$ gilt, daß v_i^p in $\mathfrak{V}_{i+1}$ enthalten ist. Endlich erhält man das zu einem anderen in $\mathfrak{p}$ aufgehenden Primideal gehörige $\mathfrak{V}_i$ durch Transformation. Der zu $\mathfrak{V}_i$ gehörige Körper heißt *Verzweigungskörper i–ter Ordnung* und werde mit $K_{\mathfrak{V}_i}$ bezeichnet.

Aus Satz 13 folgt unmittelbar, daß

$$\mathfrak{q}_{i+1} = \mathfrak{P}^{p^{\kappa_i}}$$

ein Primideal in $K_{\mathfrak{V}_i}$ ist. Das Primideal

$$\mathfrak{q}_i = \mathfrak{P}^{p^{\kappa_i - 1}}$$

aus $K_{\mathfrak{B}_{i-1}}$ wird die $p^{\kappa_{i-1}-\kappa_i}$te[10] Potenz von $\mathfrak{q}_{i+1}$ in $K_{\mathfrak{B}_i}$. In Bezug auf K_2 und k hat $\mathfrak{q}_{i+1}$ den Grad $\mathfrak{f}$, in Bezug auf $K_T, K_{\mathfrak{B}_1} = K_v, K_{\mathfrak{B}_1} \ldots K_{\mathfrak{B}_{i-1}}$ den Grad 1.

Da das Primideal $\mathfrak{p}$ im Trägheitskörper K_T die Zerlegung $\mathfrak{p} = \mathfrak{q} \cdot \mathfrak{a}$ hat, wo $\mathfrak{q} = \mathfrak{P}^e$ und $\mathfrak{a}$ zu $\mathfrak{P}$ also zu $\mathfrak{q}$ prim ist, enthält also $\mathfrak{p}$ das Primideal $\mathfrak{q}$ des Trägheitskörpers nur in der ersten Potenz. Daher geht $\mathfrak{q}$ also auch $\mathfrak{P}$ in der Relativdifferente des Trägheitskörpers nicht auf. Dieser läßt sich übrigens dadurch definieren. Es sei nämlich K_1 ein zur Gruppe $\mathfrak{G}_1$ gehöriger Unterkörper von K und seine Relativdifferente in Bezug auf k zu $\mathfrak{P}$ prim. Ist nach Satz 13 $\mathfrak{q}_1$ das $\mathfrak{P}$ enthaltende Primideal in K_1, so muß, damit die Differente zu $\mathfrak{P}$ also zu $\mathfrak{q}_1$ prim ist, notwendig $a_1 = 1$, also $e_1 = e$ sein. e_1 ist aber der Grad der Trägheitsgruppe von K in Bezug auf K_1, die sich als Durchschnitt von $\mathfrak{G}_T$ mit $\mathfrak{G}_1$ darstellt. Da $\mathfrak{G}_T$ selbst

den Grad e hat, muß also $\mathfrak{G}_T$ in $\mathfrak{G}_1$ enthalten, d.h. K_1 ein Unterkörper von K_T sein. Also:

Satz 18. Der Trägheitskörper $K_T(\mathfrak{P})$ ist der „größte“ Unterkörper von K, dessen Relativdifferente zu $\mathfrak{P}$ prim ist. Er umfaßt alle Körper dieser Art.

Da h prim zu p ist, ist nach Satz 2 u. 17 die Relativdifferente von K_v in Bezug auf K_T genau durch $\mathfrak{q}_1^{h-1} = \mathfrak{P}^{p^\kappa(h-1)} = p^{e-p^\kappa}$ teilbar. Um gleich die Relativdifferente von K zu k zu ermitteln, sei ξ eine Fundamentalform von K. Die Konjugierten sind ξ/σ_1, ξ/σ_2, …, ξ/σ_{n-1}, wo σ_i die Substitutionen aus $\mathfrak{G}$ sind. Dann haben wir den Inhalt der Form:

$$(\xi - \xi/\sigma_1)(\xi - \xi/\sigma_2)(\xi - \xi/\sigma_3)\ldots(\xi - \xi/\sigma_{n-1})$$

zu untersuchen.

$\xi \equiv \xi/\sigma_i \bmod \mathfrak{P}$ gilt dann und nur dann, wenn σ_i zur Trägheitsgruppe gehört. Da $\sigma_0 = 1$ nicht vorkommt, geschieht dies genau für $(e-1)$ Faktoren

$\xi \equiv \xi/\sigma_i \bmod \mathfrak{P}^2$ gilt nur für σ_i der Verzweigungsgruppe. Dies liefert neu: $(p^\kappa - 1)$mal den Faktor $\mathfrak{P}$. Endlich liefert ihn $\mathfrak{V}_i$ noch $(p^{k_i} - 1)$ mal. Im Ganzen also:

$$\mathfrak{P}^{(e-1)+(p^\kappa-1)+(p^{\kappa_2}-1)+\cdots+(p^{\kappa_i}-1)+\cdots}$$

[10] undeutlich

Satz 19. Die Relativdifferente $\mathfrak{D}_k$ von K ist genau durch

$$\mathfrak{P}^{(e-1)+(p^\kappa-1)+(p^{\kappa_2}-1)+\cdots+(p^{\kappa_i}-1)+\cdots}$$

teilbar. Der Exponent bricht ab, da schließlich einmal $\kappa_i = 0$ ist.

Für die anderen in $\mathfrak{p}$ aufgehenden Primideale gilt genau dasselbe, da ja ihre „Gruppenreihe“ isomorph zu der für $\mathfrak{P}$ ist (konjugierte Untergruppen).

Daher ist $\mathfrak{D}_k$ genau durch

$$(\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{(e-1)+(p^\kappa-1)+\cdots}$$

teilbar. Daraus folgt daß die Relativdiskriminante $D_k = n(\mathfrak{D}_k)$ genau durch

$$\mathfrak{p}^{r\mathfrak{f}[(e-1)+(p^\kappa-1)+(p^{\kappa_2}-1)+\cdots+(p^{\kappa_i}-1)+\cdots]}$$

teilbar ist.

Einen besonders einfachen Ausdruck nehmen die entwickelten Sätze an, wenn es sich um *relativ–Abelsche Körper* handelt. Da jede Untergruppe einer Abelschen Gruppe kommutativ und invariante Untergruppe ist, sind die Gruppen $\mathfrak{G}_Z, \mathfrak{G}_T, \ldots$ für alle in $\mathfrak{p}$ aufgehenden Primideale die gleichen. Wir erhalten also:

Satz 20. Ist K relativ Abelsch zu k und $\mathfrak{p} = (\mathfrak{P}_1 \ldots \mathfrak{P}_r)^e$ die Zerlegung von $\mathfrak{p}$, so sind im Zerlegungskörper die $\mathfrak{P}_i^e$ Primideale ersten, im Trägheitskörper $\mathfrak{f}$–ten $\left(\mathfrak{f} = \frac{n}{er}\right)$ Grades. Setzt man $\mathfrak{q}_i = \mathfrak{P}_i^e$, so ist in K_Z und K_T:

$$\mathfrak{p} = \mathfrak{q}_1 \ldots \mathfrak{q}_r$$

In K_v ist $\mathfrak{q}_i' = \mathfrak{P}^{p^\kappa}$ Primideal, wo p^κ die höchste in e aufgehende Potenz von p ist. Setzt man $e = hp^\kappa$, so ist in K_v:

$$\mathfrak{p} = (\mathfrak{q}_1' \ldots \mathfrak{q}_r')^h.$$

In $K_{\mathfrak{B}_i}$ ist $\mathfrak{P}_j^{p^{\kappa_i}} = \mathfrak{q}_j^{(i)}$ Primideal und es ist:

$$\mathfrak{p} = (\mathfrak{q}_1^{(i)} \ldots \mathfrak{q}_r^{(i)})^h p^{\kappa-\kappa_i}$$

50 ı

Im relativ–Abelschen Körper ist[11] ferner Satz 13 einfacher zu formulieren. Da es nämlich nur eine Gruppe $\mathfrak{G}_Z$ und $\mathfrak{G}_T$ gibt, werden alle $r_\nu, e_\nu, \mathfrak{f}_\nu, \mathfrak{f}'_\nu, a_\nu$ einander gleich und wir haben:

Satz 21. Ist K relativ Abelsch zu k und $\overline{K}$ der zur Gruppe $\overline{\mathfrak{G}}$ gehörige (Abelsche) Unterkörper, und ist die Zerlegung eines Primideals $\mathfrak{p}$ aus k in K:

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e; \quad (\mathfrak{P}_i \text{ vom Grad } \mathfrak{f})$$

bekannt, so findet man die Zerlegung von $\mathfrak{p}$ in $\overline{K}$ so:

Zerlegungs– und Trägheitsgruppe von K und $\overline{K}$ ist der Durchschnitt von $\overline{\mathfrak{G}}$ mit $\mathfrak{G}_Z$ und $\mathfrak{G}_T$. Sie sind also leicht angebbar und seien $\overline{\mathfrak{G}}_Z$ und $\overline{\mathfrak{G}}_T$. Es sei ferner:

$$\begin{array}{lcll} \overline{\mathfrak{G}}_Z & \text{vom} & \text{Index} & \overline{r} \text{ nach } \overline{\mathfrak{G}} \\ \overline{\mathfrak{G}}_T & = & = & \overline{\mathfrak{f}} \text{ nach } \overline{\mathfrak{G}}_Z \text{ und Grad } \overline{e} \end{array}$$

ferner:

$$r = s\overline{r}, \quad e = a\overline{e}, \quad \mathfrak{f} = \mathfrak{f}'\overline{\mathfrak{f}}$$

Wendet man auf die $\mathfrak{P}_i$ die Substitutionen von $\overline{\mathfrak{G}}$ an, so zerfallen sie in genau s Verbände von je $\overline{r}$ Primidealen: $\mathfrak{P}_{\nu 1}, \dots, \mathfrak{P}_{\nu\overline{r}}$ (S. 30▸). Dann ist

$$\mathfrak{q}_\nu = (\mathfrak{P}_{\nu 1} \dots \mathfrak{P}_{\nu\overline{r}})^{\overline{e}}$$

ein Primideal in $\overline{K}$ vom Grade $\mathfrak{f}'$ nach k. Der Grad von $\mathfrak{P}_{\nu\mu}$ nach $\overline{K}$ ist $\overline{\mathfrak{f}}$. Für $\mathfrak{p}$ gilt dann die Zerlegung in $\overline{K}$:

$$\mathfrak{p} = (\mathfrak{q}_1 \dots \mathfrak{q}_s)^a; \quad (\mathfrak{q}_j \text{ vom Grade } \mathfrak{f}')$$

51 ı

Satz 18 spricht sich hier so aus:

Satz 22. Im relativ–Abelschen Körper K (nach k) ist der Trägheitskörper der in $\mathfrak{p}$ (aus k) aufgehenden Primideale der größte Unterkörper, dessen Relativ*diskriminante* in Bezug auf k prim zu $\mathfrak{p}$ ist. Jeder Körper dieser Eigenschaft

[11] undeutlich

ist Unterkörper des Trägheitskörpers.

(Für bel. Galoissche Körper läßt sich Satz 18 deshalb nicht auf die Relativ*diskriminante* formulieren, weil die Trägheitskörper verschiedener in $\mathfrak{p}$ aufgehender Primideale verschieden sind).

Auch der *Zerlegungskörper* läßt sich hier einfach charakterisieren, er ist nämlich der größte Körper in dem $\mathfrak{p}$ in lauter verschiedene Primideale ersten Grades zerfällt.

Ist nämlich $\overline{K}$ ein solcher Körper, so muß nach Satz 21 $\mathfrak{f}' = 1$, also $\mathfrak{f} = \bar{\mathfrak{f}}$ sein. Die Grade der Zerlegungsgruppen von K in Bezug auf k und $\overline{K}$ sind also gleich, denn es muß außerdem auch $a = 1$ sein, und also:

$$\begin{array}{ccc} \text{Grad} & \text{von} & \mathfrak{G}_Z = e\mathfrak{f} \\ \| & \| & \overline{\mathfrak{G}}_Z = \bar{e}\,\bar{\mathfrak{f}} = \dfrac{e}{a} \cdot \dfrac{\mathfrak{f}}{\mathfrak{f}'} = e\mathfrak{f}. \end{array}$$

Da $\overline{\mathfrak{G}}_Z = (\overline{\mathfrak{G}}, \mathfrak{G}_Z)$ ist, muß also $\mathfrak{G}_Z = \overline{\mathfrak{G}}_Z$, da $\mathfrak{G}_Z$ Teiler von $\overline{\mathfrak{G}}$ sein, also $\overline{K}$ Unterkörper von K_Z. Also:

Satz 23. Für einen relativ–Abelschen Körper K nach k ist der Zerlegungskörper K_Z der größte Unterkörper von K, in dem $\mathfrak{p}$ in lauter verschiedene Primideale ersten Grades zerfällt. Jeder Körper, in dem dies der Fall ist, ist Unterkörper von K_Z.

Ist umgekehrt $\overline{K}$ Unterkörper von K_Z, also $\mathfrak{G}_Z$ Untergruppe von $\overline{\mathfrak{G}}$, so ist $\overline{\mathfrak{G}}_Z = (\overline{\mathfrak{G}}, \mathfrak{G}_Z) = \mathfrak{G}_Z$, ferner $\overline{\mathfrak{G}}_T = (\overline{\mathfrak{G}}, \mathfrak{G}_T) = \mathfrak{G}_T$, also die Grade von $\overline{\mathfrak{G}}_T$ und $\mathfrak{G}_T$ gleich: $\bar{e} = e,\ a = 1$, da weiter

52 ı

die Grade von $\mathfrak{G}_Z$ und $\overline{\mathfrak{G}}_Z$ gleich sind:

$$\bar{e}\,\bar{\mathfrak{f}} = ef$$

folgt

$$\bar{\mathfrak{f}} = \mathfrak{f}, \quad \mathfrak{f}' = 1$$

Es zerfällt also dann in $\overline{K}$ $\mathfrak{p}$ sicher in lauter verschiedene Primideale ersten Grades.

Da für *relativ–Abelsche Körper* die Untergruppen $\mathfrak{G}_Z, \ldots$ für alle Teiler $\mathfrak{P}_\nu$ von $\mathfrak{p}$ dieselben sind, wollen wir in diesem Falle von Zerlegungsgruppen, $\ldots$ für $\mathfrak{p}$ *selbst* sprechen.

1.2 Minkowskische Sätze über Gitter und Körperdiskriminante.

53 ı

Es seien $\xi_1, \xi_2, \ldots, \xi_n$ n unabhängige reelle Variable, die als „kartesische Koordinaten“ eines Punktes (ξ) eines R_n interpretiert werden mögen.

Die ξ seien ferner verknüpft mit n weiteren Variablen $x_1, \ldots, x_n$ durch n reelle, lineare, homogene Relationen mit nicht verschwindender Determinante:

$$\xi_i = \sum_{\nu=1}^{n} a_{i\nu} x_\nu; \quad i = 1, 2, \ldots, n; \qquad \Delta = \big|\,|a_{ik}|\,\big| > 0$$

wo also Δ der absolute Betrag der Determinante ist.

Wegen $\Delta > 0$ sind die ξ und die x ein–eindeutig auf einander bezogen, sodaß auch die x als Koordinaten in einem „schiefwinkligen“ Koordinatensystem aufgefaßt werden können. Die x_i heißen die „*Gitterkoordinaten*“ des Punktes (ξ). Wir bezeichnen sie symbolisch mit $[x]$, schreiben also $(\xi) = [x]$.

Zwei Punkte $[x]$ und $[x']$ heißen *kongruent*,

$$[x] \equiv [x'],$$

wenn die Differenzen ihrer Gitterkoordinaten ganze Zahlen sind. Punkte mit ganzzahligen Gitterkoordinaten heißen „*Gitterpunkte*“. Diese sind also alle untereinander und mit dem Ursprung kongruent. Ohne weiteres erkennt man ferner:

$$\text{Aus } [x] \equiv [x'] \text{ folgt } [x'] \equiv [x]$$
$$\text{Aus } [x] \equiv [x'] \text{ und } [x'] \equiv [x''] \text{ folgt } [x] \equiv [x''].$$

54 ı

Die Menge der Punkte $[x]$, für welche

$$k_i \leqq x_i < k_i + 1$$

mit ganzzahligem festem k_i heißen eine „*Gittermasche*“ des Raumes. Insbesondere heißt die Menge der Punkte

$$0 \leqq x_i < 1$$

die „*Grundmasche*“.

Unmittelbar erkennt man:

Jeder Punkt gehört genau einer Gittermasche an. Zu jedem Punkt gibt es genau einen kongruenten Punkt der Grundmasche.

Unter einem „*Körper K*“ des Raumes verstehen wir eine Punktmenge K, für die

$$\int_K \cdots \int d\xi_1 d\xi_2 \ldots d\xi_n$$

einen Sinn hat und endlich ist. Das Integral

$$V_K = \int_K \cdots \int d\xi_1 \ldots d\xi_n$$

heißt das „*Volumen*“ des Körpers. (Dieses wird also „kartesisch“ gemessen, nicht „schiefwinklig“).

Wenn wir die Gitterkoordinaten $[x]$ eines Körpers sämtlich um feste ganze Zahlen k_i vermindern, erhalten wir wieder einen Körper K' mit den Gitterkoordinaten $[x-k]$. Wir wollen ihn einen „*zu K kongruenten Körper*“ nennen.

Kongruente Körper haben offenbar gleiche Volumina. Haben zwei Körper K und K' keinen Punkt gemein, so bildet die Vereinigungsmenge $K + K'$ wieder einen Körper und es ist:

$$V_{K+K'} = V_K + V_{K'}$$

55 ı

Jede Gittermasche ist ein Körper und alle Gittermaschen sind kongruente Körper. Ihr Volumen ist gleich dem Volumen der Grundmasche. Es berechnet sich zu:

$$\int_{0 \leqq x_i < 1} \cdots \int d\xi_1 \ldots d\xi_n = \int_0^1 \ldots \int_0^1 \left| \left| \frac{\partial \xi_i}{\partial x_k} \right| \right| dx_1 \ldots dx_n = \Delta$$

Ein Körper heißt beschränkt, wenn es eine Zahl g gibt, sodaß für alle seine Punkte: $|x_i| < g$ ist. Die Beschränktheit mag mit in die Definition aufgenommen werden. Dann folgt:

Die Punkte eines Körpers verteilen sich nur auf endlich viele Gittermaschen.

Es sei $\mathfrak{G}_\nu$ eine in Betracht kommende Gittermasche. Der Durchschnitt von $\mathfrak{G}_\nu$ und K werden K_ν genannt. Als Durchschnitt quadrierbarer Mengen ist K_ν wieder quadrierbar, also ist K_ν ein Körper.

Da verschiedene Gittermaschen keine Punkte gemein haben, haben verschiedene K_ν auch keine Punkte gemein. Da ferner nur endlich viele $\mathfrak{G}_\nu$ in Frage kommen, haben wir eine Zerlegung von K:

$$K = K_1 + K_2 + \cdots + K_r$$

von K, so daß in einem K_ν immer nur Punkte derselben Masche liegen und in verschiedenen K_ν verschiedene Punkte. Es gilt:

$$V_K = V_{K_1} + V_{K_2} + \cdots + V_{K_r}.$$

Wir nennen diesen Prozeß die *Zerlegung von K nach dem Gitter.*

Wenn alle Punkte eines Körpers ein– u. derselben Masche, etwa $\mathfrak{G}_\nu$, angehören, so sagen wir K liege in $\mathfrak{G}_\nu$.

Wenn K in $\mathfrak{G}_\nu$ liegt, ist $V_K \leqq \Delta$. Beweis klar.

Wenn K in $\mathfrak{G}_\nu$ liegt, so gibt es genau einen kongruenten Körper K^0, der in $\mathfrak{G}_0$ liegt. Beweis klar.

Es seien K_1 und K_2 zwei Körper, die in den Maschen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ liegen. Wir bilden die kongruenten Körper K_1^0 und K_2^0 in $\mathfrak{G}_0$. Dann gilt:

In K_1 und K_2 liegen dann und nur dann kongruente Punkte, wenn K_1^0 und K_2^0 mindestens einen Punkt (ξ^0) gemein haben.

Beweis. Ist (ξ^0) gemeinsamer Punkt von $K_1^{(0)}$ und $K_2^{(0)}$ und ist $(\xi^0) \equiv (\xi^{01})$ aus K_1 und $(\xi^0) \equiv (\xi^{02})$ aus K_2, so ist $(\xi^{01}) \equiv (\xi^{02})$.

Ist umgekehrt $(\xi^{01}) \equiv (\xi^{02})$ und $(\xi^{01}) \equiv (\xi^0)$ aus $\mathfrak{G}_0$, so ist $(\xi^{02}) \equiv (\xi^0)$. Der Punkt (ξ^0) gehört also sowohl zu K_1^0 als auch zu K_2^0.

Satz 1. Gilt für das Volumen V_K eines Körpers

$$V_K > \Delta$$

so enthält K zwei einander kongruente, aber verschiedene Punkte.

Beweis. Wir zerlegen K nach dem Gitter:

$$K = K_1 + \cdots + K_r.$$

und bilden die □□□ in der Grundmasche

57 ı

gelegenen Körper K_ν^0. Dann ist:

$$V_K = V_{K_1^0} + \cdots + V_{K_\nu^0} > \Delta$$

Also ist zunächst sicher $r \geqq 2$. Denn für $r = 1$ wäre, da K_1^0 in der Grundmasche liegt, $V_{K_1^0} \leqq \Delta$, also $V_K \leqq \Delta$.

Nun haben mindestens zwei der Körper K_ν^0 einen Punkt gemein; denn andernfalls könnte der ganz in der Grundmasche gelegene Körper

$$\overline{K}^0 = K_1^0 + \cdots + K_r^0$$

gebildet werden, für den also einerseits $V_{\overline{K}^0} \leqq \Delta$ andererseits $V_{\overline{K}^0} = V_{K_1^0} + \cdots + V_{K_\nu^0} = V_K > \Delta$ wäre. Das ist aber unmöglich.

Also haben wenigstens zwei der Körper K_ν^0, etwa K_1^0 und K_2^0 einen Punkt gemein; die Körper K_1 und K_2 haben also zwei kongruente Punkte. Da K_1 und K_2 keinen Punkt gemein haben, sind diese kongruenten Punkte verschieden, w.z.b.w.

Es seien (ξ) und (ξ') zwei Punkte. Dann heißt die Menge der Punkte $(t\xi + t'\xi')$, wo die Parameter t und t' die Bedingungen $0 \leqq t, t' \leqq 1$ und $t + t' = 1$ befriedigen, die „*Verbindungsstrecke*“ von (ξ) und (ξ').

Da kartesische und Gitterkoordinaten linear, homogen zusammenhängen, ist

$$(t\xi + t'\xi') = [tx + t'x']$$

wenn $(\xi) = [x]$ und $(\xi') = [x']$.

58 ı

Definition 1. Ein Körper K heißt *konvex mit Mittelpunkt im Ursprung*,

wenn mit zweien seiner Punkte (ξ) und (ξ') auch alle Punkte der Verbindungsstrecke zu K gehören, und mit (ξ) auch der „*Spiegelpunkt*“ $(-\xi)$ zu K gehört.

Satz 2. Ist K konvex mit Mittelpunkt im Ursprung, so gehört mit $[x]$ und $[x']$ auch $\left[\frac{x-x'}{2}\right]$ zu K.

Beweis. $\left[\frac{x-x'}{2}\right] = \left[\frac{1}{2}\cdot x + \frac{1}{2}(-x')\right]$ ist ein Punkt der nach Definition zu K gehörenden Verbindungsstrecke der beiden zu K gehörigen Punkte $[x]$ und $[-x']$.

Satz 3. Ist $a > 0$ eine feste positive Zahl und durchläuft $[x]$ die Punkte eines konvexen Körpers K mit Mittelpunkt im Ursprung, so durchläuft $[ax]$ einen ebenfalls konvexen Körper mit Mittelpunkt im Ursprung, der aK genannt werden soll. Es ist $V_{aK} = aV_K$.

Beweis. $[x]$ und $[-x]$ sind gleichzeitig Punkte aus K, also: $[ax]$ und $[-ax]$ stets gleichzeitig Punkte aus aK. Ebenso ist:

$$[atx + at'x'] = [a(tx + t'x')] \quad \text{Punkt aus } aK,$$

also mit $[ax]$ und $[ax']$ auch die ganze Strecke. Schließlich ist

$$V_{aK} = \int\limits_{aK} \cdots \int d\xi_1 \ldots d\xi_n = \int\limits_{K} \cdots \int d(a\xi_1) \ldots d(a\xi_n) = a^n V_K\,.$$

Ein Körper K heißt „*abgeschlossen*“, wenn alle seine „*Grenzpunkte*“ zu ihm gehören. Ist K abgeschlossen konvex mit Mittelpunkt und liegt $[x]$ außerhalb K, so gibt es offenbar ein $\varepsilon > 0$, sodaß $[x]$ auch außerhalb $(1+\varepsilon)K$ liegt.

Hauptsatz. Es sei K ein (abgeschlossener) konvexer Körper mit Mittelpunkt im Ursprung, für den

$$V_K \geqq 2^n \Delta.$$

Dann enthält K außer dem Ursprung mindestens einen, also sicher zwei weitere Gitterpunkte.

Beweis. Wir bilden $\frac{1}{2}K$, dessen Volumen

$$V_{\frac{1}{2}K} = \left(\frac{1}{2}\right)^n V_K \geqq \Delta$$

ist. Nach Satz 1 enthält also $\frac{1}{2}K$, falls $V_{\frac{1}{2}K} > \Delta$, mindestens zwei verschiedene kongruente Punkte. Entspricht ihnen in K: $[x]$ und $[x']$, so sind also die Differenzen $\frac{1}{2}x_i - \frac{1}{2}x'_i$ ganze nicht sämtlich verschwindende Zahlen. $\left[\frac{x-x'}{2}\right]$ ist also ein vom Ursprung verschiedener Gitterpunkt. Nach Satz 2 gehört dieser zu K und ebenso sein Mittelpunkt, womit der Beweis erbracht ist.

Dieser Beweis ist aber nur bindend, falls $V_K > 2^n\Delta$ (Satz 1). Ist $V_K = 2^n\Delta$, so ist $V_{(1+\varepsilon)K} = (1+\varepsilon)^n V_K > 2^n\Delta$ □□□. Für jedes noch so kleine $\varepsilon > 0$ enthält also $V_{(1+\varepsilon)K}$ mindestens einen Gitterpunkt. Läge nun in K außer $[0]$ kein Gitterpunkt, so müßte sich wegen der Abgeschlossenheit ein ε bestimmen lassen, sodaß auch in □□□ $(1+\varepsilon)K$ kein weiterer Gitterpunkt läge, dem Bewiesenen zuwider. *Die Voraussetzung „abgeschlossen“ ist also nur notwendig, falls $V_K = 2^n\Delta$ vorgegeben.*

Von den Anwendungen greifen wir zwei für uns wichtige heraus.

60 I

Es seien n beliebige reelle oder komplexe, lineare Formen y_i der Variablen x_i vorgelegt, doch solcher Art, daß zu jeder komplexen Form auch die mit den konjugiert komplexen Werten der Koeffizienten vorkommt und daß ihre Determinante $\neq 0$ ist. Wir denken uns diese Formen so geordnet, daß:

$$\left.\begin{array}{c} y_1, \ldots, y_{r_1} \text{ die reellen Formen sind } (r_1 \geqq 0), \\ y_{r_1+1}, \ldots, y_{r_1+r_2} \\ y_{r_1+r_2+1}, \ldots, y_{r_1+2r_2} \end{array}\right\} \text{ die komplexen Formen } (r_2 \geqq 0),$$

wobei immer: $y_{r_1+r_2+i}$ zu y_{r_1+i} konjugiert komplex ist. Es ist also $n = r_1 + 2r_2$. Die Formen seien:

$$y_i = \sum_{\nu=1}^{n} \alpha_{i\nu} x_\nu \quad \text{und} \quad \Delta = \left|\left|\alpha_{i\nu}\right|\right| > 0.$$

Als Gitterkoordinaten wählen wir die x_i als kartesische die ξ_i, die mit den x_i durch die Formen:

$$\begin{array}{rcl} \xi_i = y_i\,; & & 1 \leqq i \leqq r_1 \\ \left.\begin{array}{rcl} \xi_{r_1+i} & = & \frac{1}{\sqrt{2}}(y_{r_1+i} + y_{r_1+r_2+i}) \\ \xi_{r_1+r_2+i} & = & \frac{1}{i\sqrt{2}}(y_{r_1+i} - y_{r_1+r_2+i}) \end{array}\right\}; & & 1 \leqq i \leqq r_2 \end{array}$$

verbunden sind. Die Formen ξ_i sind jetzt auch reell. Wir bestimmen zunächst das Volumen der Grundmasche, d.h. den Betrag ihrer Determinante. Dieser ist gerade Δ. Denn die reellen Zeilen der Determinante der ξ_i stimmen mit denen der Determinante $|\alpha_{i\nu}|$ der y_i überein. Sind ferner U und V zwei konjugiert komplexe Zeilen der Determinante der y_i

dann darf man sie sukzessive ersetzen durch

$$\begin{array}{ll} U+V; & V \\ U+V; & V-\frac{U+V}{2} \\ U+V; & -\frac{U-V}{2} \\ \frac{U+V}{\sqrt{2}}; & \frac{1}{i}\,\frac{U-V}{i\sqrt{2}} \end{array}$$

Da es nur auf den absoluten Betrag ankommt also durch

$$\frac{U+V}{\sqrt{2}}; \quad \frac{U-V}{i\sqrt{2}}$$

Jetzt stimmen alle Zeilen mit denen der Determinante der ξ_i überein, das Volumen der Grundmasche ist also Δ und nach Voraussetzung > 0.

Als konvexen Körper wählen wir nun die Menge der Punkte, für die:

$$|y_1| + |y_2| + \cdots + |y_n| \leqq h,$$

wo h eine feste, positive Zahl. Der Körper hat einen Mittelpunkt, und zwar im Ursprung, denn falls $[x]$ zu ihm gehört, ist dies auch für $[-x]$ der Fall, da dann die zugehörigen y_i in $-y_i$ übergehen, der Betrag also derselbe bleibt.

Er ist ferner konvex. Denn entsprechen zweien seiner Punkte □□□ $[x]$ und $[x']$ die Formen y_i und y_i', so entsprechen dem Punkt $[tx + t'x']$ mit $0 \leqq t, t' \leqq 1$ und $t + t' = 1$ die Formen $ty_i + t'y_i'$, und es ist

$$|ty_i + t'y_i'| \leqq t|y_i| + t'|y_i'|,$$

also

$$\sum_{i=1}^{n} |ty_i + t'y_i'| \leqq t\sum_{i=1}^{n} |y_i| + t'\sum_{i=1}^{n} |y_i'| \leqq (t+t')h = h.$$

In den ξ_i schreibt sich die Bedingung, die unseren Körper definiert, so:

$$|\xi_1| + \cdots + |\xi_{r_1}| + |\sqrt{2(\xi^2_{r_1+1} + \xi^2_{r_1+r_2+1})}| + \cdots + |\sqrt{2(\xi^2_{r_1+r_2} + \xi^2_{r_1+2r_2})}| \leqq h$$

(denn es ist offenbar

$$\begin{aligned} y_{r_1+\nu} &= \frac{1}{\sqrt{2}}(\xi_{r_1+\nu} + i\xi_{r_1+r_2+\nu}) \\ y_{r_1+r_2+\nu} &= \frac{1}{\sqrt{2}}(\xi_{r_1+\nu} - i\xi_{r_1+r_2+\nu}) \end{aligned}$$

also

$$|y_{r_1+\nu}| + |y_{r_1+r_2+\nu}| = \frac{2}{\sqrt{2}}|\sqrt{\xi^2_{r_1+\nu} + \xi^2_{r_1+r_2+\nu}}| \ ).$$

Für das Volumen ergibt sich also:

$$\begin{aligned} V_{r_1,r_2}(h) &= \int\cdots\int_{|\xi_1|+\cdots+|\sqrt{2(\ )}|+\cdots\leqq h} d\xi_1 \ldots d\xi_n = h^n \int\cdots\int_{|\xi_1|+\cdots\leqq 1} d\xi_1 \ldots d\xi_n \\ &= h^n V_{r_1,r_2}(1) = h^n C_{r_1,r_2}\,, \quad \text{wo} \\ C_{r_1,r_2} &= \int\cdots\int_{|\xi_1|+\cdots\leqq 1} d\xi_1 \ldots d\xi_n \int_{-1}^{+1} d\xi_1 \int\cdots\int_{|\xi_2|+\cdots\leqq 1-|\xi_1|} d\xi_2 \ldots d\xi_n \\ &= \int_{-1}^{+1} V_{r_1-1,r_2}(1-|\xi_1|)d\xi_1 \end{aligned}$$

Da nun allgemein $V(h) = h^n V(1)$ oben gezeigt, wenn V ein n faches Integral ist, folgt hier:

$$\begin{aligned} C_{r_1,r_2} &= C_{r_1-1,r_2}\int_{-1}^{+1}(1-|\xi_1|)^{n-1}d\xi_1 = 2C_{r_1-1,r_2}\int_0^1(1-\xi_1)^{n-1}d\xi_1 \\ &= \frac{2}{n}C_{r_1-1,r_2} = \cdots = \frac{2^{r_1}}{n(n-1)\cdots(n-r_1+1)}C_{0,r_2} \\ &= \frac{2^{r_1}}{n(n-1)\cdots(2r_2+1)}C_{0,r_2}\,, \end{aligned}$$

wo also bei passender Bezeichnung ist:

63 I

$$C_{0,r_2} = \int\cdots\int_{|\sqrt{2(\xi_1^2+\cdots\xi_{1+r_2}^2)}|+\cdots+|\sqrt{2(\xi_{r_2}^2+\cdots\xi_{2r_2}^2)}|\leqq 1} d\xi_1\ldots d\xi_{2r_2}$$

Setzen wir

$$\left.\begin{array}{rcl}\xi_i & = & \frac{1}{\sqrt{2}}R_i\cos\varphi_i \\ \xi_{r_2+i} & = & \frac{1}{\sqrt{2}}R_i\sin\varphi_i\end{array}\right\};R_i\geqq 0$$

so ist diese Bedingung bei der Integration einfach:

$$R_1+R_2+\cdots+R_{r_2}\leqq 1.$$

Da ferner die ξ_i,ξ_{i+r_2} jeden Wert zwischen $-\frac{1}{\sqrt{2}}$ und $+\frac{1}{\sqrt{2}}$ annehmen können, in beliebiger Kombination, hat man φ_i von 0 bis 2π laufen zu lassen (mit anderen Worten: Die Integrationsbedingung ist unabhängig von den φ_i, und da das angegebene Intervall für φ_i gerade alle verschiedenen Wertepaare ξ_i,ξ_{r_2+i} erschöpft, ist dies die richtige Begrenzung für φ_i).

□□□

Die Funktionaldeterminante der ξ_i und ξ_{i+r_2} nach den R_i und φ_i wird, da jedes bestimmte Paar ξ_i und ξ_{i+r_2} nur von R_i und φ_i abhängt, das Produkt der r_2 Determinanten:

$$\begin{vmatrix}\frac{\partial\xi_i}{\partial R_i} & \frac{\partial\xi_i}{\partial\varphi_i}\\ \frac{\partial\xi_{i+r_2}}{\partial R_i} & \frac{\partial\xi_{i+r_2}}{\partial\varphi_i}\end{vmatrix} = \begin{vmatrix}\frac{1}{2}\sqrt{2}\cos\varphi_i & -\frac{R_i}{\sqrt{2}}\sin\varphi_i\\ \frac{1}{2}\sqrt{2}\sin\varphi_i & -\frac{R_i}{\sqrt{2}}\cos\varphi_i\end{vmatrix} = \frac{R_i}{2}\,,\quad (i=1,\ldots,r_2)$$

Die Funktionaldeterminante wird also: $\frac{1}{2^{r_2}}R_1\ldots R_{r_2}$ Unsere Konstante C_{0,r_2} wird damit:

$$C_{0,r_2} = 2^{-r_2}\int\cdots\int_{\substack{R_1+\cdots R_{r_2}\leqq 1\\ R_i\geqq 0}} R_1\ldots R_{r_2}dR_1\ldots dR_{r_2}\int_0^{2\pi}\cdots\int_0^{2\pi} d\varphi_1\ldots d\varphi_{r_2}$$

$$\begin{aligned} C_{0,r_2} &= \pi^{r_2} \int\limits_{\substack{R_1+\cdots+R_{r_2}\leqq 1 \\ R_i \geqq 0}} \cdots \int R_1 \ldots R_{r_2} dR_1 \ldots dR_{r_2} \\ &= \pi \int\limits_0^1 R_1 dR_1 \int\limits_{\substack{R_2+\cdots+R_{r_2}\leqq 1-R_1 \\ R_i \geqq 0}} \cdots \int R_2 \ldots R_{r_2} dR_2 \ldots dR_{r_2} \pi^{r_2-1} \end{aligned}$$

Setzt man im inneren Integral $R_i = (1-R_1)R_i'$ für $i \geqq 2$, so wird

$$\begin{aligned} C_{0,r_2} &= \pi \int\limits_0^1 R_1(1-R_1)^{2r_2-2}\pi^{r_2-1} dR_1 \int\limits_{\substack{R_2'+\cdots+R_{r_2}'\leqq 1 \\ R_i' \geqq 0}} \cdots \int R_2' \ldots R_{r_2}' dR_2' \ldots dR_{r_2}' \\ &= \pi \int\limits_0^1 R_1(1-R_1)^{2r_2-2} dR_1 C_{0,r_2-1} \\ &= C_{0,r_2-1} \cdot \pi \int\limits_0^1 k(1-k)^{2r_2-2} dk \end{aligned}$$

Da nun

$$\begin{aligned} \int\limits_0^1 (1-k)^{2r_2-2} k dk &= -\frac{(1-k)^{2r_2-1}}{2r_2-1} k \Big|_0^1 + \int\limits_0^1 \frac{(1-k)^{2r_2-1}}{2r_2-1} dk \\ &= 0 + \left[-\frac{(1-k)^{2r_2}}{2r_2(2r_2-1)} \right]_0^1 = \frac{1}{2r_2(2r_2-1)} \end{aligned}$$

ist, folgt:

$$C_{0,r_2} = \frac{\pi}{2r_2(2r_2-1)} C_{0,r_2-1} = \cdots = \frac{\pi^{r_2-1}}{2r_2(2r_2-1)\cdots 4 \cdot 3} \cdot C_{0,1}\,.$$

Da schließlich

$$C_{0,1} = \pi \int\limits_0^1 R_{r_2} dR_{r_2} = \frac{\pi}{2}$$

ist, folgt:

$$C_{0,r_2} = \frac{\pi^{r_2}}{(2r_2)!} \quad \text{und} \quad C_{r_1,r_2} = \frac{2^{r_1}\pi^{r_2}}{n!}\,.$$

Also

$$\boldsymbol{V_{r_1,r_2}(h) = \frac{2^{r_1}\pi^{r_2}}{n!}h^n}$$

65 I

Wenn nun das hiermit berechnete Volumen unseres Körpers:

$$V_{r_1,r_2}(h) = 2^n\Delta$$

ist, liegt nach unserem Hauptsatz im Inneren außer dem Ursprung noch mindestens ein Gitterpunkt (der Körper ist sicher abgeschlossen, da die Bedingung für ihn lautet:

$$|y_1| + \cdots + |y_n| \leqq h$$

mit *Einschluß* der Gleichheit. Daher ist der Hauptsatz *mit Gleichheitszeichen* anwendbar).

Es gibt daher mindestens ein ganzzahliges Wertsystem x_i das nicht identisch verschwindet, sodaß

$$|y_1| + \cdots + |y_n| \leqq h$$

ist. Die Bedingung hierfür:

$$V_{r_1,r_2}(h) = 2^n\Delta$$

ist nun dann und nur dann erfüllt, wenn

$$\frac{2^{r_1}\pi^{r_2}}{n!}h^n = 2^n\Delta$$

d.h.

$$h^n = \frac{2^{n-r_1}}{\pi^{r_2}}n!\Delta = \left(\frac{4}{\pi}\right)^{r_2} n!\Delta$$

ist. Es gibt also ganze nicht sämtlich verschwindende x_i, für die:

$$|y_1| + \cdots + |y_n| \leqq \sqrt[n]{\left(\frac{4}{\pi}\right)^{r_2} n!\Delta}$$

ist.

Man kann nun nachweisen:

Sind $a_1, \ldots, a_n$ reelle positive Zahlen, so ist:

$$a_1 + \cdots + a_n \geqq n \sqrt[n]{a_1 \ldots a_n}$$

66 I

Für $n = 1$ ist dies trivial, für $n = 2$ richtig, da stets

$$a_1 + a_2 - 2\sqrt{a_1 a_2} = (\sqrt{a_1} - \sqrt{a_2})^2 \geqq 0 \quad \text{ist.}$$

Es sei bis $n-1$ bewiesen. Von den n Größen ist eine die größte, etwa a_n (oder eine der größten). Also

$$\begin{aligned} a_n &\geqq a_i \\ a_n^{n-1} &\geqq a_1 \ldots a_{n-1} \\ a_n &\geqq \sqrt[n-1]{a_1 \ldots a_{n-1}} \end{aligned}$$

Nach Annahme ist nun, wenn $\sqrt[n-1]{a_1 \ldots a_{n-1}} = b$ gesetzt wird, sodaß $a_n - b \geqq 0$ ist,

$$\begin{aligned} & a_1 + \cdots + a_{n-1} \geqq (n-1)b \\ \text{also} \quad & a_1 + \cdots + a_{n-1} \geqq a_n + (n-1)b \\ & \frac{a_1 + \cdots + a_n}{n} \geqq b + \frac{a_n - b}{n} \\ & \left(\frac{a_1 + \cdots + a_n}{n}\right)^n \geqq b^n + b^{n-1}(a_n - b) = b^{n-1} a_n \\ & \qquad\qquad = a_1 \ldots a_n \end{aligned}$$

Somit $a_1 + \cdots + a_n \geqq n \sqrt[n]{a_1 \ldots a_n}$ w.z.b.w.

Setzt man $a_i = |y_i|$, so wird also:

$$n \sqrt[n]{|y_1 \ldots y_n|} \leqq |y_1| + \cdots + |y_n|$$

Erst recht gilt demnach für die y_i

$$|y_1 \ldots y_n| \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \Delta.$$

D.h. man kann stets ein nicht identisch verschwindendes Wertsystem von ganzen Zahlen x_i finden, sodaß diese Ungleichung besteht. Dabei ist n die Anzahl der Formen, r_2 die der komplexen Paare, Δ die Determinante der Formen y_i.

67 I

Für die zweite Anwendung wählen wir bei gleicher Bedeutung der x_i, y_i und ξ_i den folgenden konvexen Körper:

Für $i = 1, 2, \ldots, r_1$ seien $k_i > 0$ beliebig gegeben
für $i = r_1 + 1, \ldots, r_1 + r_2$ desgl.,
für $i = r_1 + r_2 + 1, \ldots, r_1 + 2r_2 = n$ sei stets $k_{r_1+r_2+\nu} = k_{r_1+\nu}$,

d.h. es ist zu konjugiert komplexen Formen y_i stets dasselbe k_i zu nehmen.

Der Körper sei durch

$$|\xi_i| \leqq k_i$$

definiert. Für die $|y_i|$ ergibt sich daraus

$$|y_i| = |\xi_i| \leqq k_i; \quad (i = 1, 2, \ldots, r_1)$$

$$\left.\begin{array}{rcl} |y_{r_1+\nu}| &=& |\frac{1}{\sqrt{2}}(\xi_{r_1+\nu} + i\xi_{r_1+r_2+\nu})| \\ |y_{r_1+r_2+\nu}| &=& |\frac{1}{\sqrt{2}}(\xi_{r_1+\nu} - i\xi_{r_1+r_2+\nu})| \end{array}\right\} = \frac{1}{\sqrt{2}}\sqrt{\xi_{r_1+\nu}^2 + \xi_{r_1+r_2+\nu}^2}$$

also:

$$|y_{r_1+\nu}| = |y_{r_1+r_2+\nu}| \leqq \sqrt{\frac{k_{r_1+\nu}^2 + k_{r_1+r_2+\nu}^2}{2}} = k_{r_1+\nu} = k_{r_1+r_2+\nu}$$

$(\nu = 1, 2, \ldots, r_2)$

Es gilt also für unseren Körper sicher:

$$|y_i| \leqq k_i\,; \quad (i = 1, 2, \ldots, n)$$

Der so definierte Körper ist konvex mit Mittelpunkt im Ursprung. Denn ist $|\xi_i| \leqq k_i$; $|\xi_i'| \leqq k_i$, so ist

$$|t\xi_i + t'\xi_i'| \leqq t|\xi_i| + t'|\xi_i'| \leqq k_i(t + t') = k_i$$

für $0 \leqq t, t' \leqq 1$, $t + t' = 1$. Ferner ist auch $| \sim \xi_i| \leqq k_i$. Schließlich ist er wegen des in die Definition eingegangenen Gleichheitszeichens abgeschlossen. Sein Volumen ist:

$$V = \int\limits_{|\xi_i| \leqq k_i} \cdots \int d\xi_1 \dots d\xi_n = \int\limits_{-k_1}^{k_1} d\xi_1 \int\limits_{-k_2}^{k_2} d\xi_2 \cdots \int\limits_{-k_n}^{k_n} d\xi_n = 2^n k_1 \dots k_n$$

Wenn $V = 2^n\Delta$, d.h. $k_1 \cdots k_n = \Delta$ ist, gibt es in ihm sicher einen Gitterpunkt. Die x_i lassen sich also ganzzahlig, nicht sämtlich verschwindend, so wählen, daß

$$|y_i| \leqq k_i$$

wird.

Satz 4. Sind $y_1, y_2, \dots, y_n$ irgendwelche n linearen homogenen Formen der Variablen $x_1, \dots, x_n$, von denen r_1 reell und r_2 Paare konjugiert komplex sind $(r_1 + 2r_2 = n)$, deren Determinante den Betrag $\Delta > 0$ hat, so gilt:

a.) Es lassen sich die x_i ganzzahlig und nicht sämtlich verschwindend so wählen, daß

$$|y_1 \dots y_n| \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\Delta \quad \text{ist.}$$

b.) Sind $k_i > 0$ reelle, den y_i zugeordnete Zahlen, so daß konjugiert komplexe y_i dasselbe k_i erhalten und außerdem $k_1 \dots k_n = \Delta$ ist, so lassen sich wieder die x_i ganzzahlig und nicht sämtlich verschwindend so wählen, daß

$$|y_1| \leqq k_1; \ \dots \ ; \ |y_n| \leqq k_n \quad \text{ist.}$$

(Darüber hinaus gilt sogar

c.) Sind alle Formen y_i reell, die k_i also bis auf die Forderung $k_1 \dots k_n = \Delta$ beliebig, so gibt es sogar ein nicht identisch verschwindendes ganzzahliges Wertsystem x_i, sodaß:

$$|y_1| \leqq k_1; \ |y_2| < k_2 \, ; \ \dots \ |y_n| < k_n \quad \text{ist.}$$

69 ı

Um c.) zu beweisen, gehen wir so vor: Es sei $\varepsilon > 0$ beliebig klein vorgegeben. Wir wählen

$$k_1' = k_1(1+\varepsilon)^{n-1};\ k_2' = \frac{k_2}{1+\varepsilon};\ \ldots\ k_n' = \frac{k_n}{1+\varepsilon}.$$

Dann ist $k_1' \ldots k_n' = k_1 \ldots k_n = \Delta$. Es lassen sich also die x_i so bestimmen, daß

$$|y_1| \leqq k_1(1+\varepsilon)^{n-1};\ |y_2| \leqq \frac{k_2}{1+\varepsilon};\ \ldots;\ |y_n| \leqq \frac{k_n}{1+\varepsilon}$$

erst recht also:

$$|y_1| \leqq k_1(1+\varepsilon)^{n-1};\ |y_2| < k_2;\ \ldots;\ |y_n| < k_n$$

wird. Nun sind alle in Betracht kommenden Wertsysteme Gitterpunkte im Inneren oder mit der Begrenzung des durch unsere früheren Ungleichungen bestimmten Körpers. Da er beschränkt ist, liegen nur endlich viele Gitterpunkte in seinem Inneren. Es sei unter diesen endlich vielen Wertsystemen x_i das System $\overline{x}_i$ dasjenige, welches □□□ der Form y_1 den kleinsten Absolutbetrag erteilt. Dieser sei $|\overline{y}_1|$. Ist $|\overline{y}_1| > k_1$, so wähle man ε so, daß

$$|\overline{y}_1| > k_1(1+\varepsilon)^{n-1} > k_1$$

Auch für dieses ε haben unsere neuen Ungleichungen Lösungen $\overline{\overline{x}}_i$, lieferten also ein $|\overline{\overline{y}}_1| \leqq k_1(1+\varepsilon)^{n-1} < |\overline{y}_1|$[1] entgegen der Annahme, daß $|\overline{y}_1|$ schon der kleinste vorkommende Absolutbetrag sei. Es ist also $|\overline{y}_1| \leqq k$, w.z.b.w.

(*Offenbar ist nur notwendig, daß die Form y_1 reell ist*).

Bevor wir zu den Anwendungen auf die Theorie der algebraischen Zahlen übergehen, beweisen wir einen einfachen Hilfssatz.

70 ı

Hilfssatz. Wenn der Grad n und eine positive Zahl a gegeben ist, gibt es nur eine endliche Anzahl ganzer algebraischer Zahlen n–ten Grades (deren Körper hier ohne Bedeutung ist), die mit aller ihren konjugierten □□□ absolut genommen kleiner als a sind.)

[1] undeutlich

(**Beweis.** Die ganzzahligen Koeffizienten einer solchen Gleichung n–ten Grades müßten dem Betrage nach als symmetrische Funktionen der konjugierten absolut unterhalb einer leicht angebbaren, nur von a und n abhängigen Zahl liegen. Hierfür gibt es nur endlich viele Möglichkeiten.)

Nun sei k ein Zahlkörper n–ten Grades mit der Diskriminante d. $k_1, \ldots, k_n$ seien die konjugierten Körper in irgendeiner Reihenfolge und $k_1 = k$. Wir betrachten die Basisformen

$$y_i = \omega_1^{(i)} x_1 + \cdots + \omega_n^{(i)} x_n\,; \quad (i = 1, 2, \ldots, n)$$

Sie genügen den in Satz 4 gestellten Anforderungen. Nach Satz 4, a.) lassen sich also die x_i ganzzahlig und nicht alle verschwindend so wählen, daß

$$|y_1 y_2 \ldots y_n| \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \Delta,$$

wo r_2 die Anzahl der Paare konjugiert komplexer Körper bedeutet und Δ die Diskriminante der y_i ist. Bekanntlich ist $\Delta^2 = |d|$. Da ferner die x_i nicht

alle verschwinden und wir eine Basis vor uns haben, gehen die y_i in lauter nicht verschwindende konjugierte ganze Zahlen über, ihr Produkt also in die Norm einer nicht verschw. ganzen Körperzahl. Da diese Norm rational ganz, also mindestens 1 ist, muß also:

$$1 \leqq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\sqrt{d}|$$

und somit

$$|d| \geqq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}$$

sein.

(Ferner ersetzen wir die Formen y_i durch andere: Ist y_i reell, so bleibt es. Ist es komplex und y_κ das konjugiert komplexe, so ersetzen wir etwa

$$\begin{array}{ccc} y_i & \text{durch} & \frac{y_i - y_\kappa}{i\sqrt{2}} \\ y_\kappa & \text{"} & \frac{y_i + y_\kappa}{\sqrt{2}} \end{array}$$

Das ist übrigens nichts anderes als die früheren ξ_i. Die neuen y_i werden dann alle reell und ihr Δ ist wieder $|\sqrt{d}|$, da es ja erhalten bleibt. Nun wählen wir gemäß Satz 4, c.) die κ_i so:

$$\kappa_1 = |\sqrt{d}|;\ \kappa_2 = \kappa_3 = \cdots = \kappa_n = 1.$$

Dann gibt es ein System der x_i, sodaß

$$|y_1| \leqq |\sqrt{d}|;\ |y_2| < 1;\ \ldots\ |y_n| < 1.$$

Diesem x_i–System entspricht eine ganze Zahl α aus $k = k_1$. Ist k reell, so ist $y_1 = \alpha$, ist k komplex und k' der konjugiert komplexe Körper, so ist $y_1 = \frac{\alpha - \alpha'}{i\sqrt{2}}$

Um die Norm von α zu bilden, haben wir die den reellen Körpern entsprechenden y_i zu multiplizieren. Ist aber α_i und α_κ konjugiert komplex, so ist

$$y_i = \frac{\alpha_i - \alpha_\kappa}{i\sqrt{2}}, \quad y_\kappa = \frac{\alpha_i + \alpha_\kappa}{\sqrt{2}} \quad \text{also}$$
$$\alpha_i = \frac{iy_i + y_\kappa}{\sqrt{2}}, \quad \alpha_\kappa = -\frac{iy_i + y_\kappa}{\sqrt{2}}$$

somit $\alpha_i \alpha_\kappa = \frac{y_i^2 + y_\kappa^2}{2}$

Demnach ist

$$|\mathsf{N}(\alpha)| = \prod |y_r| . \prod \frac{y_i^2 + y_\kappa^2}{2} \quad \text{(in leicht verständl. Beziehung)}$$

Wäre nun $|y_1| \leqq 1$, so wäre, da die übrigen $|y_i| < 1$ sind und $n \geqq 2$ ist,

$$|\mathsf{N}(\alpha)| < 1, \quad \text{was wegen } \alpha \neq 0 \text{ ausgeschlossen.}$$

Also ist $|y_1| > 1$ und somit

$$|\sqrt{d}| > 1; \quad |d| > 1.$$

Aus $|y_1| > 1;\ \ |y_2| < 1;\ \ldots\ |y_n| < 1$ ist zu schließen, daß α von seinen konjugierten verschieden ist, also den Körper k erzeugt. Denn ist k reell ist

$y_1 = \alpha$ und alles ist klar, da die reellen konjugierten < 1 sind, unter den imaginären aber keines mit α übereinstimmen kann, da sonst das konjugiert imaginäre auch übereinstimmte, also $|y_\kappa| = \left|\frac{\alpha+\alpha}{\sqrt{2}}\right| = |\alpha|\sqrt{2} > 1$ wäre. Ist aber k komplex,

73 I

so ist α komplex, da dann

$$\left|\frac{\alpha - \alpha'}{i\sqrt{2}}\right| = |y_1| > 1 \neq 0$$

ist. Mit den reellen konjugierten stimmt es also sicher nicht überein. Mit den übrigen imaginären aber auch nicht, da sonst $\frac{\alpha-\alpha'}{i\sqrt{2}}$ ein zweites Mal vorkäme, also noch ein $|y_i| > 1$ wäre.

Wenn also der Körper n–ten Grades die Diskriminante d hat, gibt es eine ihn erzeugende Zahl α, für die

$$|y_1| \leqq |\sqrt{d}|\,;\ |y_2| < 1;\ \ldots\ ;\ |y_n| < 1,$$

also sicher jedes $y_i \leqq |\sqrt{d}|$ ist.

Für ein reelles α_i bedeutet dies, daß $|\alpha_i| \leqq |\sqrt{d}|$, während für ein imaginäres: $\left|\frac{\alpha_i+\alpha_\kappa}{\sqrt{2}}\right| \leqq |\sqrt{d}|$ und $\left|\frac{\alpha_i-\alpha_\kappa}{i\sqrt{2}}\right| \leqq |\sqrt{d}|$ also:

$$\begin{aligned} |\alpha_i| = \left|\frac{\alpha_i + \alpha_\kappa}{2} + \frac{\alpha_i - \alpha_\kappa}{2}\right| &\leqq \left|\frac{\alpha_i + \alpha_\kappa}{2}\right| + \left|\frac{\alpha_i - \alpha_\kappa}{2}\right| \\ &\leqq \frac{\sqrt{d}}{\sqrt{2}} + \frac{\sqrt{d}}{\sqrt{2}} = |\sqrt{2d}| \end{aligned}$$

und ebenso

$$|\alpha_\kappa| = \left|\frac{\alpha_i + \alpha_\kappa}{2} - \frac{\alpha_i - \alpha_\kappa}{2}\right| \leqq |\sqrt{2d}|$$

ist.

Auf jeden Fall ist also jedes $|\alpha_i| \leqq |\sqrt{2d}|$

Nach Hilfssatz 1 gibt es aber bei gegebenem n nur endlich viele solcher Zahlen. Es gibt also nur endlich viele solche Körper, die durch solche Zahlen erzeugt werden, d.h. nur endlich viele Körper gegebenen Grades und gegebener Diskriminante.

74 I

Gäbe es nämlich unendlich viele, so gäbe es unendlich viele verschiedene, diese Körper erzeugende Zahlen, die mit allen ihren konjugierten absolut $\leqq 2|\sqrt{d}|$ wären, was nach Hilfssatz 1 bei gegebenem n unmöglich.)

Kehren wir zu $|d| \geqq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}$ zurück.

Da $\frac{\pi}{4} < 1$ und $2r_2 \leqq n$ ist, gilt also sicher

$$|d| \geqq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}.$$

Nun ist $n! < \sqrt{2\pi n} n^n e^{-n+\frac{1}{12n}}$. Also:

$$|d| \geqq \left(\frac{\pi}{4}\right)^n \frac{1}{2\pi n} e^{2n-\frac{1}{6n}} = \frac{1}{2\pi n}\left(\frac{\pi e^2}{4}\right)^n e^{-\frac{1}{6n}}.$$

Da $\frac{\pi e}{4} > 1$ ist, wächst die rechte Seite mit n über alle Grenzen. Vereinigen wir die erhaltenen Resultate, so haben wir die Sätze:

Satz 5. Außer dem Körper der rationalen Zahlen gibt es keinen algebraischen Körper mit der Diskriminante ± 1. In der Diskriminante eines algebraischen Körpers geht also mindestens eine Primzahl auf.

(**Satz 6.** Bei gegebenem Grade gibt es nur endlich viele Körper gegebener Diskriminante.)

(**Satz 7.** Es gibt überhaupt nur endlich viele Körper beliebigen Grades mit gegebener Diskriminante. Ist n der Grad, r_2 die Zahl der konjugiert komplexen Körperpaare, so gilt

$$|d| \geqq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}\ .\ )$$

75 I

Beweis. Gäbe es unendlich viele Körper mit der Diskriminante d, so kann ihr Grad nicht beliebig hoch sein, da

$$\frac{1}{2\pi n}\left(\frac{\pi e}{4}\right)^{2n} e^{-\frac{1}{6n}} \leqq d$$

sein muß. Es kommen also nur endlich viele Grade in Frage, woraus nach Satz 6 die Behauptung folgt.

Für Relativkörper gilt Satz 5 nicht mehr. Wegen 1.) Satz 6 (S. 14▸) folgt aber aus unserm Satz 6 unmittelbar das Analogon:

Satz 8. Zu gegebenem Grundkörper und Relativgrad r gibt es nur endlich viele Relativkörper gleicher Relativdiskriminante.

Besonders Satz 5 gestattet mannigfache Anwendungen, von denen wir auf eine eingehen wollen.

Satz 9. Seien k_1 und k_2 zwei algebr. Körper der Grade n_1 und n_2 und der Diskriminanten d_1 und d_2. Ihre Basen seien $\omega_1, \ldots, \omega_{n_1}$ und $\overline{\omega}_1, \ldots, \overline{\omega}_{n_2}$. Ferner seien die Diskriminanten d_1, d_2 relativ prim. Dann hat der aus ihnen komponierte Körper $k_3 = (k_1, k_2)$ den Grad $n_1 n_2$, die Diskriminante $d = d_1^{n_2} d_2^{n_1}$ und die Basis:

$$(\omega_i \overline{\omega}_k)\,; \quad \left\{\begin{matrix} i = 1, 2, \ldots, n_1 \\ k = 1, 2, \ldots, n_2 \end{matrix}\right\}.$$

76 ı

Beweis. k_3 hat den Relativgrad n_2 in Bezug auf k_1, d.h. die Gleichung für eine positive Zahl aus k_2 ist in k_1 irreduzibel. Denn in k_1 wird, wie aus der Galoisschen Theorie bekannt ist, die gleiche Zerfällung hervorgerufen, wie im Durchschnitt von k_1 und k_2.

(Satz über Adjunktion akzessorischer Irrationalitäten, die `[...]` mehr erreicht, als Adjunktion natürlicher Irrationalitäten).

Dieser Durchschnitt von k_1 und k_2 ist Unterkörper von k_1 und k_2, seine Diskriminante ist also nach 1.) Satz 6 (S. 14▸), ein Teiler von d_1 und d_2, also n. V. ± 1. Nach Satz 5 ist also dieser Durchschnitt der rationale Körper, in dem die Gleichung für eine primitive Zahl aus k_2 irreduzibel ist. Also ist sie auch in k_1 irreduzibel, d.h. k_2 vom Grade n_2 zu k_1, also auch k_3 vom Relativgrad n_2 zu k_1, d.h. k_3 vom absoluten Grade $n_1 \cdot n_2$.

Die Relativdiskriminanten von k_3 zu k_1 und k_2 seien D_1 und D_2. Dann ist nach 1.) Satz 6 (S. 14▸):

$$d = \pm d_1^{n_2} n(D_1) = \pm d_2^{n_1} n(D_2)$$

Da $(d_1, d_2) = 1$ ist also d mindestens durch $d_1^{n_2} d_2^{n_1}$ teilbar, also

$$|d| \geqq |d_1^{n_2} d_2^{n_1}|$$

Nun nehmen wir das System von $n_1 n_2$ ganzen Zahlen unseres Satzes: $\omega_i \overline{\omega}_\kappa$. Die konjugierten erhalten wir, wenn wir unabhängig ω_i und $\overline{\omega}_\kappa$ alle konjugierten durchlaufen lassen: $\omega_i^{(\mu)} \overline{\omega}_\kappa^{(\nu)}$. Das Diskriminantenquadrat dieses Systems ist eine Determinante der Form des Satzes 9 aus 1.) (S. 16▶). Sie hat also den Wert:

$$|\omega_i^{(\mu)} \cdot \overline{\omega}_k^{(\nu)}|^2 = (|\omega_i^{(\mu)}|^{n_2} |\overline{\omega}_k^{(\nu)}|^{n_1})^2 = d_1^{n_2} d_2^{n_1} \neq 0$$

Nun ist nach der elementaren Theorie der algebr. Zahlen das Diskriminantenquadrat eines Systems von $n_1 n_2$ linear unabhängigen Zahlen, wie sie hier vorliegen, eines Körpers vom Grade $n_1 n_2$ durch die Körperdiskriminante teilbar und der Quotient eine ganze rationale Quadratzahl. Es ist also hier sicher zunächst

$$|d| \leqq |d_1^{n_1} d_2^{n_2}|$$

also

$$d = \pm d_1^{n_1} d_2^{n_2}$$

und weiter das Vorzeichen positiv, da -1 Nichtquadrat, also, wie behauptet:

$$d = d_1^{n_1} d_2^{n_2}$$

und gleichzeitig unser System $\omega_i \overline{\omega}_k$ eine Körperbasis, da sein Diskriminantenquadrat die Körperdiskriminante ist. Damit ist Satz 9 bewiesen.

Durch vollständige Induktion läßt sich Satz 9 unmittelbar verallgemeinern:

Satz 10. Sind $k_1, \ldots, k_i$ algebraische Körper der Grade $n_1, \ldots, n_i$ und den Diskriminanten $d_1, \ldots, d_i$, die zu je zweien relativ prim sind. Dann hat der aus den k_ν komponierte Körper $k = (k_1, \ldots, k_i)$ den Grad $n = (n_1 \ldots n_i)$, die Diskriminante

$$d = d_1^{\frac{n}{n_1}} d_2^{\frac{n}{n_2}} \ldots d_i^{\frac{n}{n_i}}$$

Eine Basis von k erhält man indem man die Basiszahlen der k_ν untereinander auf alle möglichen Weisen multipliziert, so daß aus jedem Körper genau eine Basiszahl in jedem solchen Produkte auftritt.

1.3 Die Einheiten, der Strahl und der allgemeine Klassenbegriff

78 I

Es sei k ein algebraischer Körper,

dessen Zahlen mit $, \alpha, \alpha_1, \ldots, \beta, \ldots$ bezeichnet werden mögen. Seine konjugierten Körper, unter denen k selbst vorkommt, seien mit:

$$k_1, \ldots, k_{r_1};\ k_{r_1+1}, \ldots, k_{r_1+r_2};\ k_{r_1+r_2+1}, \ldots, k_{r_1+2r_2}$$

bezeichnet, wo $r_1 + 2r_2 = n$ ist, und die r_1 ersten Körper reell, die r_2 weiteren Paare $k_{r_1+\nu}$ und $k_{r_1+r_2+\nu}$ konjugiert komplex sind. ($r_1 \geqq 0$; $r_2 \geqq 0$).

Wir setzen: $r = r_1 + r_2 - 1$.

Der Fall $r = 0$ erfordert entweder:

$$r_1 = 1; \quad r_2 = 0 \quad \text{also} \quad n = 1 \quad \text{(rat. Körper)}$$

oder:

$$r_1 = 0; \quad r_2 = 1 \quad \text{also} \quad n = 2 \quad \text{(imag. quadr. Körper)}$$

Die zu α konjugierten Zahlen seien $\alpha^{(1)}, \ldots, \alpha^{(n)}$. Wir setzen ferner $d_\kappa = 1$ oder 2, je nachdem k_κ reell oder imaginär ist. Dann ist gerade:

$$\sum_{\kappa=1}^{r+1} d_\kappa = \sum_{\kappa=1}^{r_1} 1 + \sum_{\kappa=r_1+1}^{r_1+r_2} 2 = r_1 + 2r_2 = n.$$

Jeder Zahl α aus k ordnen wir nun $r+1$ Zahlen zu, die wir „*das System konjugierter Logarithmen*“ nennen, nämlich:

$$\ell_\kappa(\alpha) = d_\kappa \log |\alpha^{(\kappa)}|$$

Wir haben dann:

79 I

$$\sum_{\kappa=1}^{r+1} \ell_\kappa(\alpha) = \log |\mathsf{N}(\alpha)|$$

unter log immer den (reellen) Hauptwert des Logarithmus verstanden. Denn für $\kappa \leqq r_1$ ist:

$$\ell_\kappa(\alpha) = \log|\alpha^{(\kappa)}|$$

für $r_1 < \kappa \leqq r_2$ aber

$$\ell_\kappa(\alpha) = 2\log|\alpha^{(\kappa)}| = \log|\alpha^{(\kappa)}| + \log|\alpha^{(\kappa+r_2)}|.$$

Eine ganze Zahl ε ist dann u. nur dann eine Einheit, wenn $\mathsf{N}(\varepsilon) = \pm 1$ ist. Also haben wir:

Satz 1. Eine Zahl ε ist dann und nur dann eine Einheit, wenn

$$\sum_{\kappa=1}^{r+1} \ell_\kappa(\varepsilon) = 0$$

ist.

Satz 2. Es sei $r > 0$. Ferner $\gamma_1, \gamma_2, \ldots, \gamma_r$ irgendwelche reelle nicht sämtlich verschwindende Zahlen. Dann gibt es in k eine Einheit ε, für die

$$\sum_{\nu=1}^{r} \gamma_\nu \ell_\nu(\varepsilon) \neq 0$$

ist.

Beweis. Man bestimme r feste reelle Zahlen $\lambda_1, \lambda_2, \ldots, \lambda_r$ irgendwie so, daß

$$\sum_{\nu=1}^{r} d_\nu \gamma_\nu \lambda_\nu = 1$$

ist. (Da nicht alle γ_ν verschwinden, und $r > 0$, ist dies stets möglich). t sei ein noch näher zu bestimmender Parameter.

80 I

Wir setzen:

$$v_i = e^{\lambda_i t} \qquad (i = 1, 2, \ldots, r)$$

Auf diese Art sind $v_1, v_2, \ldots, v_{r_1+r_2-1}$ bestimmt. Ein eventuelles $v_{r_1+r_2+i}$ mit $i > 0$ werde durch

$$v_{r+r_2+i} = v_{r_1+i}$$

erklärt. Die restlichen Glieder □□□

$$v_{r+1} = v_{r_1+r_2} \quad \text{und} \quad v_{r_1+2r_2} = v_n$$

werden einander gleich gesetzt und so gewählt, daß

$$v_1 \dots v_n = |\sqrt{d}|$$

ist, wo d die Körperdiskriminante bedeutet. Nun wollen wir 2.) Satz 4 (S. 68▸) anwenden, und zwar auf die Formen

$$y_i = \omega_1^{(i)} x_1 + \dots + \omega_n^{(i)} x_n$$

indem wir ihnen die bestimmten v_i zuordnen. Diese Formen, deren Determinante den Absolutbetrag $|\sqrt{d}|$ hat und unsere Zahlen genügen den Bedingungen des Satzes 4 (S. 68▸). Es gibt also ein ganzzahliges, nicht identisch verschwindendes Wertsystem (x_i), d.h. eine von Null verschiedene ganze Zahl α in k, sodaß

$$|\alpha^{(\kappa)}| \leqq v_\kappa$$

wird. Durch Multiplikation folgt:

$$|\mathsf{N}(\alpha)| \leqq |\sqrt{d}|$$

Nun ist

$$|\alpha^{(\kappa)}| = \frac{|\mathsf{N}(\alpha)|}{|\alpha^{(1)}| \cdots |\alpha^{(\kappa-1)}||\alpha^{(\kappa+1)}| \cdots |\alpha^{(n)}|},$$

also wegen $|\mathsf{N}(\alpha)| \geqq 1$:

81 ı

$$|\alpha^{(\kappa)}| \geqq \frac{1}{|\alpha^{(1)}| \cdots (\text{ohne } |\alpha^{(\kappa)}|) \cdots |\alpha^{(n)}|} \geqq \frac{1}{v_1 \dots v_{\kappa-1} v_{\kappa+1} \dots v_n} = \frac{v_\kappa}{|\sqrt{d}|}$$

Im Ganzen ist also:

$$\frac{v_\kappa}{|\sqrt{d}|} \leqq |\alpha^{(\kappa)}| \leqq v_\kappa$$

also:

$$\log v_\kappa - \log |\sqrt{d}| \leqq \log |\alpha^{(\kappa)}| \leqq \log v_\kappa$$

Für $\kappa = 1, 2, \ldots, r$ also nach Multiplikation mit d_κ, wenn noch $\beta = \log|\sqrt{d}|$ gesetzt wird

$$d_\kappa\lambda_\kappa t - d_\kappa\beta \leqq \ell_\kappa(\alpha) \leqq d_\kappa\lambda_\kappa t$$

Jedenfalls ist also

$$|\ell_\kappa(\alpha) - d_\kappa\lambda_\kappa t| \leqq d_\kappa\beta \leqq 2\beta$$

Setzen wir also:

$$\mathsf{L}(\alpha) = \sum_{\nu=1}^{r} \gamma_\nu \ell_\nu(\alpha)$$

so ist wegen $\sum_{\nu=1}^{r} d_\nu\gamma_\nu\lambda_\nu = 1$

$$\begin{aligned} \mathsf{L}(\alpha) - t &= \sum_{\nu=1}^{r} \gamma_\nu(\ell_\nu(\alpha) - d_\nu\lambda_\nu t), \quad \text{sodaß} \\ |\mathsf{L}(\alpha) - t| &\leqq \sum_{\nu=1}^{r} |\gamma_\nu||\ell_\nu(\alpha) - d_\nu\lambda_\nu t| \leqq 2\beta \sum_{\nu=1}^{r} |\gamma_\nu| = B \end{aligned}$$

wo B eine feste von t nicht abhängige Zahl ist.

Wir haben dann:

$$t - B \leqq \mathsf{L}(\alpha) \leqq t + B$$

Die so bestimmte Zahl κ ist natürlich von t abhängig. Nun bestimmen wir sie für die Parameterwerte $t = B, 3B, 5B, \ldots$ und nennen die entstehenden

Zahlen $\alpha_1, \alpha_2, \ldots$. Für diese gilt

$$\begin{array}{rcl} 0 & \leqq & \mathsf{L}(\alpha_1) \leqq 2B \\ 2B & \leqq & \mathsf{L}(\alpha_2) \leqq 4B \\ 4B & \leqq & \mathsf{L}(\alpha_2) \leqq 6B \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots \end{array}$$

Also sind die Zahlen α_i wirklich lauter verschiedene Zahlen und es ist für $i \neq \kappa$ sicher $\mathsf{L}(\alpha_i) \neq \mathsf{L}(\alpha_\kappa)$.

Andererseits gilt für jedes α_i

$$|\mathsf{N}(\alpha_i)| \leqq |\sqrt{d}|$$

Nun gibt es aber nur endlich viele Ideale, erst recht also Hauptideale, deren Norm unterhalb einer festen Schranke liegt. Unter unseren unendlich vielen α_i gibt es also sicher zwei verschiedene α_i, α_κ, welche das gleiche Hauptideal erzeugen. Ihr Quotient $\frac{\alpha_i}{\alpha_\kappa}$ ist also eine Einheit ε und es ist

$$\mathsf{L}(\varepsilon) = \mathsf{L}\left(\frac{\alpha_i}{\alpha_\kappa}\right) = \mathsf{L}(\alpha_i) - \mathsf{L}(\alpha_\kappa) \neq 0, \quad \text{da} \quad \mathsf{L}(\alpha_i) \neq \mathsf{L}(\alpha_\kappa)$$

Unser Beweis ist damit erbracht. Unmittelbar folgt:

Satz 3. Ist $r > 0$, so enthält der Körper unendlich viele von Einheitswurzeln verschiedene Einheiten.

Beweis. Sei ε eine Einheit, für die $\mathsf{L}(\varepsilon) \neq 0$ ist. Wegen $\mathsf{L}(\varepsilon^a) = a\mathsf{L}(\varepsilon)$ ist auch $\mathsf{L}(\varepsilon^a) \neq 0$. Für $a \neq b$ ist ferner $\mathsf{L}(\varepsilon^a) - \mathsf{L}(\varepsilon^b) = (a-b)\mathsf{L}(\varepsilon) \neq 0$, sodaß ε^a und ε^b verschieden sind. In $\varepsilon, \varepsilon^2, \ldots$ haben wir also unendlich viele verschiedene Einheiten, was nicht möglich wäre, wenn eine von ihnen Einheitswurzel

Satz 4. Damit eine Einheit ε eine Einheitswurzel ist, ist notwendig und hinreichend, daß $|\varepsilon^{(\kappa)}| = 1$ für alle konjugierten.

Beweis. Der erste Teil ist selbstverständlich. Ist andrerseits $|\varepsilon^{(\kappa)}| = 1$, so ist auch $|\varepsilon^{(\kappa)^a}| = 1$ für jedes a. Nach dem Hilfssatz 1 (S. 70▶) müssen also zwei der Potenzen identisch sein, etwa ε^a und $\varepsilon^{a+\kappa}$. Daraus folgt aber $\varepsilon^\kappa = 1$.

Satz 4 lehrt in Verbindung mit dem eben benutzten Hilfssatz 1:

Satz 5. In jedem algebraischen Körper gibt es nur endlich viele Einheitswurzeln, deren Anzahl mit w bezeichnet werde.

Wir betrachten nun zunächst den einfachen Fall:

1.) $r = 0$.

Nach S. 78▶ ist dann k entweder der rationale Körper mit den einzigen Einheiten ± 1, also $w = 2$, oder *ein imaginär quadratischer Körper*. Für letzteren gilt:

Satz 6. Im imaginär quadratischen Köper gibt es nur die Einheiten ± 1, sodaß $w = 2$ ist, mit Ausnahme von

a.) $k(\sqrt{-1})$ mit den Einheiten $\pm 1, \pm i$, also $w = 4$

b.) $k(\sqrt{-3})$ 〃 〃 〃 $\pm 1, \pm\frac{1}{2}, \pm\frac{i}{2}\sqrt{3}$, also $w = 6$

Ein imaginär quadratischer Körper hat also lediglich Einheitswurzeln zu Einheiten.

84 ı

Beweis. Jede Einheit ε muß einer quadratischen Gleichung:

$$x^2 - (\varepsilon + \varepsilon')x + \varepsilon\varepsilon' = 0$$

genügen. Da ε und ε' konjugiert komplex sind, ist

$$|\varepsilon| = |\varepsilon'|,$$

ferner

$$\mathsf{N}(\varepsilon) = \varepsilon\varepsilon' = \pm 1,$$

also

$$|\varepsilon\varepsilon'| = |\varepsilon^2| = 1$$

d.h. $|\varepsilon| = |\varepsilon'| = 1$
Daher ist nach Satz 4 ε Einheitswurzel. Ferner ist

$$|\varepsilon + \varepsilon'| \leqq |\varepsilon| + |\varepsilon'| = 2$$

Es kommen also nur die Gleichungen in Frage:

$$x^2 \pm 1 = 0; \quad x^2 \pm x \pm 1 = 0; \quad x^2 \pm 2x \pm 1 = 0.$$

Die Gleichungen $x^2 \pm 2x - 1 = 0$ fallen weg, da ihre Wurzeln □□□ $1 \pm \sqrt{2}$ und $-1 \pm \sqrt{2}$ sind, also nicht in einem imag. quadr. Körper enthalten. $x^2 \pm 2x + 1 = 0$ liefert die trivialen Einheiten ± 1. $x^2 \pm 1 = 0$ liefert ± 1 und $\pm i$.
$x^2 \pm x + 1 = 0$ liefert $\pm\left(-\frac{1}{2} \pm \frac{i}{2}\sqrt{3}\right)$; $x^2 \pm x - 1 = 0$ liefert wieder die nicht in Frage kommenden Werte $\pm\left(-\frac{1}{2} \pm \frac{i}{2}\sqrt{5}\right)$. Damit ist alles bewiesen.

Wir betrachten nun den allgemeinen Fall

2.) $r > 0$.

Satz 7. Im Falle $r > 0$ gibt es ein System von r Einheiten, *die Grundeinheiten des Körpers*, sodaß der Ausdruck

$$\varrho\varepsilon_1^{a_1}\varepsilon_2^{a_2}\ldots\varepsilon_r^{a_r}$$

alle Einheiten des Körpers und jede nur einmal darstellt, wenn ϱ alle w Einheitswurzeln des Körpers und die a_i alle ganzen pos. u. neg. Zahlen durchlaufen.

85 ı

Beweis. In Satz 2 wählen wir:

1.) $\gamma_1 = 1$, $\gamma_2 = \gamma_3 = \cdots = \gamma_r = 0$

Dann resultiert nach Satz 2 eine Einheit η_1 für die $\ell_1(\eta_1) \neq 0$.

2.) $\gamma_1 = -\ell_2(\eta_1)$; $\gamma_2 = \ell_1(\eta_1)$; $\gamma_3 = \cdots = \gamma_r = 0$.

Dann ist wegen 1.) $\gamma_2 \neq 0$ und es resultiert eine Einheit η_2, für die

$$-\ell_2(\eta_1)\ell_1(\eta_2) + \ell_1(\eta_1)\ell_2(\eta_2) \neq 0, \qquad \text{d.h.}$$
$$\begin{vmatrix} \ell_1(\eta_1) & \ell_2(\eta_1) \\ \ell_1(\eta_2) & \ell_2(\eta_2) \end{vmatrix} \neq 0.$$

3.) Es sei allgemein für $\nu < r$: $\eta_1, \eta_2, \ldots, \eta_\nu$ so bestimmt, daß

$$\begin{vmatrix} \ell_1(\eta_1) & \cdots & \ell_\nu(\eta_1) \\ \ell_1(\eta_\nu) & \cdots & \ell_\nu(\eta_\nu) \end{vmatrix} \neq 0.$$

Durch passende Wahl von $\gamma_1, \gamma_2, \ldots, \gamma_{\nu+1}$ als Unterdeterminanten der Matrix

$$\begin{pmatrix} \ell_1(\eta_1) & \cdots & \ell_\nu(\eta_1) & \ell_{\nu+1}(\eta_1) \\ & & & \\ \ell_1(\eta_\nu) & \cdots & \ell_\nu(\eta_\nu) & \ell_{\nu+1}(\eta_\nu) \end{pmatrix}$$

und $\gamma_{\nu+2} = \cdots = \gamma_r = 0$ erhält man nach Satz 2 eine Einheit $\eta_{\nu+1}$, sodaß

$$|\ell_\kappa(\eta_i)| \neq 0; \quad (i, \kappa = 1, 2, \ldots, \nu + 1),$$

also schließlich ein System von r Einheiten $\eta_1, \ldots, \eta_r$,

86 ı

sodaß

$$|\ell_\kappa(\eta_i)| \neq 0; \quad (i, \kappa = 1, 2, \ldots, r)$$

Dann läßt sich, wenn H irgendeine Einheit aus k ist, das System der r Gleichungen mit den r Unbekannten ξ_γ

$$\ell_\kappa(\mathsf{H}) = \sum_{\nu=1}^{r} \xi_\nu \ell_\kappa(\eta_\nu)$$

eindeutig lösen. Wir setzen

$$\xi_\nu = \mathfrak{m}_\nu + \tau_\nu$$

wo $\mathfrak{m}_\nu$ die größte ganze Zahl $\leqq \xi_\nu$ ist, ferner

$$\zeta_\kappa = \sum_{\nu=1}^{r} \tau_\nu \ell_\kappa(\eta_\nu).$$

Dann ist

$$|\zeta_\kappa| \leqq \sum_{\nu=1}^{r} |\tau_\nu| \cdot |\ell_\kappa(\eta_\nu)| < \sum_{\nu=1}^{r} |\ell_\kappa(\eta_\nu)| = \mathsf{S}_\kappa\,,$$

also unterhalb einer von H unabhängigen Schranke S_κ, also *alle* ζ_κ unterhalb einer von H und κ unabhängigen, nur von den festen η_i abhängigen Schranke S.

Ferner ist dann:

$$\ell_\kappa(\mathsf{H}) = \sum_{\nu=1}^{r} \mathfrak{m}_\nu \ell_\kappa(\eta_\nu) + \zeta_\kappa$$

Nun ist

$$\mathsf{E} = \frac{\mathsf{H}}{\eta_1^{\mathfrak{m}_1} \eta_r^{\mathfrak{m}_r}}$$

ebenfalls eine Einheit. Für diese ist gerade

$$\ell_\kappa(\mathsf{E}) = \zeta_\kappa$$

also: $\quad |\ell_\kappa(\mathsf{E})| < \mathsf{S} \quad$ für $\kappa = 1, 2, \ldots, r$.
Da E eine Einheit ist, ist

$$\sum_{\nu=1}^{n} \log |\mathsf{E}^{(\nu)}| = \ell_1(\mathsf{E}) + \cdots + \ell_{r+1}(\mathsf{E}) = 0$$

Daraus ergibt sich für $\ell_{r+1}(\mathsf{E})$ die Abschätzung:

$$|\ell_{r+1}(\mathsf{E})| \leqq \sum_{\nu=1}^{r} |\ell_\nu(\mathsf{E})| < r\mathsf{S}.$$

Es gilt daher für alle $\kappa \leqq r+1$:

$$|\ell_\kappa(\mathsf{E})| < r\mathsf{S}.$$

Da nun

$$|\ell_\kappa(\mathsf{E})| = \left|d_\kappa \log|\mathsf{E}^{(\kappa)}|\right| \geqq \left|\log|\mathsf{E}^{(\kappa)}|\right| \quad \text{und}$$

die konjugiert komplexen $\mathsf{E}^{(\kappa)}$ gleiche absolute Beträge haben, gilt für alle $\kappa \leqq n$

$$\left|\log|\mathsf{E}^{(\kappa)}|\right| < r\mathsf{S}$$

oder $\quad |\mathsf{E}^{(\kappa)}| < e^{r\mathsf{S}}$

Nach dem Hilfssatz 1.) (S. 70▶) stammt also E aus einem endlichen Wertevorrat. Es gibt also endlich viele Einheiten $\mathsf{E}_1, \ldots, \mathsf{E}_N$, sodaß jede beliebige Einheit H mit ganzzahligen $\mathfrak{m}_\nu$ in der Form

$$\mathsf{H} = \mathsf{E}_i \eta_1^{\mathfrak{m}_1} \ldots \eta_r^{\mathfrak{m}_r}$$

darstellbar ist.

Sei E_K eine der N Einheiten $\mathsf{E}_1, \ldots, \mathsf{E}_N$. Die Potenzen $1, \mathsf{E}_K, \mathsf{E}_K^2, \ldots$ sind wieder Einheiten. Denken wir uns diese in der eben angegebenen Form dargestellt, so muß sicher bei der Darstellung zweier verschiedener dieser Potenzen das gleiche E_i auftreten. Ihr Quotient ist dann eine von der nullten Potenz verschiedene Potenz mit der Darstellung:

$$\mathsf{E}_K^{j_K} = \eta_1^{q_1} \ldots \eta_r^{q_r}$$

Ist j das kleinste gemeinsame Vielfache von $j_1, j_2, \ldots, j_N$, so ist offenbar jede beliebige Einheit H in der Form darstellbar

$$\mathsf{H}^j = \eta_1^{b_1} \ldots \eta_r^{b_r}$$

mit ganzz. b_i. Demnach ist

$$\ell_\kappa(\mathsf{H}) = \frac{1}{j} \sum_{\nu=1}^{r} b_\nu \ell_\kappa(\eta_\nu)$$

Insbesondere gibt es zu jedem ν Einheiten, deren konj. Logarithmen von der Form sind:

$$\ell_\kappa(\varepsilon_\nu) = \frac{1}{j} \sum_{\mu=1}^{\nu} b_\mu \ell_\kappa(\eta_\mu), \quad \text{da ja z.B. } \eta_\mu \text{ selbst eine solche Einheit ist.}$$

Es sei nun ε_ν eine jener Einheiten, für die in dieser Darstellung:

$$\ell_\kappa(\varepsilon_\nu) = \frac{1}{j}\sum_{\mu=1}^{\nu} b_{\nu\mu}\ell_\kappa(\eta_\mu)$$

der Koeffizient $b_{\nu\nu}$ den kleinsten positiven Wert hat. Ist dann H_ν irgendeine Einheit dieser Form:

$$\ell_\kappa(\mathsf{H}_\nu) = \frac{1}{j}\sum_{\mu=1}^{\nu} a_\mu\ell_\kappa(\eta_\mu)$$

so muß a_ν durch $b_{\nu\nu}$ teilbar sein. Denn setzen wir $a_\nu = qb_{\nu\nu}+r_\nu$[1] wo $r_\nu < b_{\nu\nu}$, so ist $\overline{\mathsf{H}}_\nu = \frac{\mathsf{H}_\nu}{\varepsilon_\nu^q}$ eine Einheit mit der Darstellung

$$\ell_\kappa(\overline{\mathsf{H}}_\nu) = \frac{1}{j}\left[c_1\ell_\kappa(\eta_1) + \cdots + c_{\nu-1}\ell_\kappa(\eta_{\nu-1}) + r_\nu\ell_\kappa(\eta_\nu)\right]$$

entgegen der Auswahl von ε_ν, wenn nicht $r_\nu = 0$ ist.

Nun sei H eine beliebige Einheit, und

$$\ell_\kappa(\mathsf{H}) = \frac{1}{j}\sum_{\mu=1}^{r} a_\mu\ell_\kappa(\eta_\mu)$$

Dann ist a_r durch b_{rr} teilbar: $a_r = b_{rr}\cdot q_r$ und

$$\mathsf{H}_1 = \frac{\mathsf{H}}{\varepsilon_r^{q_r}}$$

ist eine Einheit mit der Darstellung

$$\ell_\kappa(\mathsf{H}_1) = \frac{1}{j}\sum_{\mu=1}^{r-1} \overline{a}_\mu\ell_\kappa(\eta_\mu)$$

Dann ist $\overline{a}_{r-1}$ durch $b_{r-1,r-1}$ teilbar: $a_{r-1} = b_{r-1,r-1}\cdot q_{r-1}$ und $\mathsf{H}_2 = \frac{\mathsf{H}}{\varepsilon_r^{q_r}\varepsilon_{r-1}^{q_{r-1}}}$ eine Einheit, deren Darstellung nur bis $\ell_\kappa(\eta_{r-2})$ reicht u.s.f. So gelangen wir schließlich zu einer Einheit

$$\mathsf{H}_r = \frac{\mathsf{H}}{\varepsilon_r^{q_r}\ldots\varepsilon_1^{q_1}}, \quad \text{sodaß}$$

[1] undeutlich

$$\ell_\kappa(\mathsf{H}_r) = 0$$

ist. Wegen $\ell_{r+1}(\mathsf{H}_r) = -\ell_1(\mathsf{H}_r) - \cdots - \ell_r(\mathsf{H}_r)$ ist dann auch $\ell_{r+1}(\mathsf{H}_r) = 0$ und also

$$\log |\mathsf{H}_r^{(\kappa)}| = 0, \quad \text{für } \kappa = 1, 2, \ldots, n.$$

Daher ist $|\mathsf{H}_r^{(\kappa)}| = 1$ und nach Satz 4 ist H_r eine Einheitswurzel ϱ aus k. H gestattet also die Darstellung:

$$\mathsf{H} = \varrho \varepsilon_1^{q_1} \ldots \varepsilon_r^{q_r}.$$

Da ϱ und die ε_i Einheiten aus k sind, ist auch umgekehrt jeder solche Ausdruck eine Körpereinheit. Wir zeigen schließlich die Eindeutigkeit. Gäbe es zwei verschiedene Darstellungen für H, so gäbe es durch Division eine nicht identische Darstellung der 1:

$$1 = \varrho \varepsilon_1^{\nu_1} \ldots \varepsilon_r^{\nu_r}$$

wo nicht gleichzeitig alle $\nu_1, \ldots, \nu_r = 0$ und also $\varrho = 1$ ist. Durch Logarithmierung würden folgen:

$$0 = \sum_{i=1}^{r} \nu_i \ell_\kappa(\varepsilon_i)$$

Hieraus folgt aber sofort, daß alle $\nu_i = 0$, und daher $\varrho = 1$ sein müssen, wenn noch gezeigt wird, daß die Determinante

$$|\ell_\kappa(\varepsilon_i)|\,; \quad (i, \kappa = 1, 2, \ldots, r)$$

nicht verschwindet.

Nun lassen sich die früheren η_s sicher in der Form darstellen:

$$\eta_s = \varrho_s \varepsilon_1^{a_{s1}} \ldots \varepsilon_r^{a_{sr}}$$

also

$$\ell_\kappa(\eta_s) = \sum_{\mu=1}^{r} a_{s\mu} \ell_\kappa(\varepsilon_\mu)$$

Daraus folgt für die Determinanten

$$|\ell_\kappa(\eta_s)| = |a_{s\mu}| \cdot |\ell_\kappa(\varepsilon_\mu)|$$

und daraus folgt wegen $|\ell_\kappa(\eta_s)| \neq 0$ auch $\ell_\kappa(\varepsilon_\mu)| \neq 0$, w.z.b.w.

90 I

Satz 8. Die von Null verschiedene r gliedrige Determinante

$$|\ell_\kappa(\varepsilon_i)|$$

ist bis aufs Vorzeichen unabhängig von der Wahl der Grundeinheiten ε_i und der Reihenfolge der konjugierten Körper, soweit sie noch wahlfrei ist.

Beweis. Ist $\overline{\varepsilon}_i$ ein anderes System von Grundeinheiten (charakterisiert durch die Darstellungseigenschaft von Satz 7), so müssen sich sowohl die $\overline{\varepsilon}_i$ durch die ε_i, als auch die ε_i durch die $\overline{\varepsilon}_i$ in der Form von Satz 7 darstellen lassen. Wie vorhin erhalten wir daraus:

$$\begin{aligned} |\ell_\kappa(\overline{\varepsilon}_i)| &= |a_{i\kappa}| \cdot |\ell_\kappa(\varepsilon_i)| \\ |\ell_\kappa(\varepsilon_i)| &= |b_{i\kappa}| \cdot |\ell_\kappa(\overline{\varepsilon}_i)| \end{aligned}$$

wo $(a_{i\kappa})$ und $(b_{i\kappa})$ ganzzahlige r–reihige Matrizen sind. Also ist wegen $|\ell_\kappa(\varepsilon_i)| \neq 0$ auch $|\ell_\kappa(\overline{\varepsilon}_i)| \neq 0$ und also

$$|a_{i\kappa}| \cdot |b_{i\kappa}| = 1$$

also:

$$|a_{i\kappa}| = \pm 1$$

also

$$\big||\ell_\kappa(\overline{\varepsilon}_i)|\big| = \big||\ell_\kappa(\varepsilon_i)|\big| \qquad \text{(Betrag!)}.$$

Werden ferner die ersten r Körper permutiert oder durch ihre konjugiert komplexen ersetzt, so ändert sich die Determinante nur im Vorzeichen, da höchstens ihre Kolonnen vertauscht werden und die $\ell_\kappa(\varepsilon_i)$ nur von den Beträgen der ε_i abhängen. Wird ferner der Körper k_r durch k_{r+1} ersetzt, so entsteht ebenfalls derselbe absolute Betrag der Determinante. Denn es gilt

$$-\ell_{r+1} = +(\ell_1 + \cdots + \ell_r)$$

sodaß also diese Ersetzung bis aufs Vorzeichen durch Addition der Kolonnen $\ell_1, \ell_2, \ldots, \ell_{r-1}$ zu ℓ_r erreicht wird. Damit ist alles bewiesen.

91 ı

Definition 1. Der absolute Betrag der reellen Determinante $|\ell_\kappa(\varepsilon_i)|$ [2] eines Systems von Grundeinheiten des Körpers, der nach dem vorigen nur vom Körper abhängt, heißt der Regulator R des Körpers.

Dieser Regulator R ist ein Maß für die „*Dichtigkeit*“ der Einheiten: Je größer R, umso weniger unter allen Körperzahlen sind Einheiten, sodaß $\frac{1}{R}$ = *Dichtigkeit der Einheiten im Körper* gedeutet werden kann. Man erkennt dies zunächst deutlich am Beispiel des reellen quadratischen Körpers ($r = 1$; $w = 2$), wo jede Einheit H sich darstellen läßt:

$$\mathsf{H} = \pm\varepsilon^a.$$

Der Regulator ist: $R = \big|\log|\varepsilon|\big|$

Je größer R umso größer ist (falls $|\varepsilon| > 1$ genommen wird, was zulässig, da auch $\frac{1}{\varepsilon}$ Grundeinheit) $|\varepsilon|$, umso weniger dicht liegen also die Potenzen von ε in der reellen Achse verteilt.

□□□

Im allgemeinen Falle deuten wir die $\ell_\kappa(\varepsilon)$ als Koordinaten im r dimensionalen Raum. Dann bestimmen die r Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ vermöge dieser r Systeme von je r Koordinaten ein Gitter im Raum, dessen Gitterpunkte die Einheiten repräsentieren. Jedem Gitterpunkte entsprechen dann genau

92 ı

w Körpereinheiten. Der Inhalt der Grundgittermasche wird offenbar gerade R. Es ist also $\frac{1}{R}$, genauer $\frac{w}{R}$ ein Maß für die Dichtigkeit der Gitterpunkte und als solches als Maß für die Dichtigkeit den Einheiten im Körper anzusprechen. Die Größe $\frac{w}{R}$ wird uns später noch öfter begegnen.

Bei passender Integration bleiben unsere Ergebnisse auch für $r = 0$ richtig. Hier ist $R = 1$ zu setzen, die Grundeinheiten sind als sämtlich zu 1 geworden vorzustellen.

[2] undeutlich

Wir haben jetzt die Rechenregeln für *Kongruenzen* auf *gebrochene Zahlen* auszudehnen.

Definition 2. Sei $\mathfrak{m}$ ein beliebiges Ideal (ganz). Zwei ganze oder gebrochene Zahlen des Körpers heißen kongruent mod $\mathfrak{m}$:

$$\alpha \equiv \beta \mod \mathfrak{m},$$

wenn $\alpha - \beta$, als reduzierter Bruch $\frac{\mathfrak{c}}{\mathfrak{d}}$ geschrieben, $\mathfrak{m}$ im Zähler enthält.

Es wird sich dann sicher eine ganze zu $\mathfrak{m}$ prime Zahl ν bestimmen lassen, sodaß $(\alpha - \beta)\nu$ eine *ganze*, durch $\mathfrak{m}$ teilbare Zahl ist; denn man kann $\mathfrak{d}_1$ so wählen, daß $\mathfrak{d}\mathfrak{d}_1 = (\nu)$ Hauptideal und $\mathfrak{d}_1$ zu $\mathfrak{m}$ prim ist. Dann ist auch ν zu $\mathfrak{m}$ prim und

$$\big(\nu(\alpha - \beta)\big) = \mathfrak{c}\mathfrak{d}_1$$

ganz und durch $\mathfrak{m}$ teilbar. Ist dies umgekehrt für ein

ν erfüllt, also $\nu(\alpha - \beta)$ ganz und durch $\mathfrak{m}$ teilbar, so setze man

$$\big(\nu(\alpha - \beta)\big) = \mathfrak{d}_2 \qquad (\mathfrak{d}_2 \text{ durch } \mathfrak{m} \text{ teilbar})$$
$$(\alpha - \beta) = \frac{\mathfrak{d}_2}{(\nu)}$$

und da sich der Faktor $\mathfrak{m}$ im Zähler nach Annahme nicht gegen (ν) wegheben kann, ist

$$\alpha - \beta = \frac{\mathfrak{c}}{\mathfrak{d}}; \quad (\text{reduziert, } \mathfrak{c} \text{ durch } \mathfrak{m} \text{ teilbar}).$$

Offenbar gilt:

Satz 9. Zwei ganze Zahlen des Körpers sind dann und nur dann in diesem erweiterten Sinne kongruent mod $\mathfrak{m}$, wenn sie es im alten Sinne sind. Die neue Kongruenz ist transitiv. Aus $\alpha \equiv \beta \mod \mathfrak{m}$; $\gamma \equiv \delta \mod \mathfrak{m}$ folgt

$$\alpha \pm \beta \equiv \gamma \pm \delta \mod \mathfrak{m}.$$

Beweis.

a.) Sind α, β ganz und $(\alpha - \beta) = \frac{\mathfrak{c}}{\mathfrak{d}}$ ($\mathfrak{c}$ durch $\mathfrak{m}$ teilbar), so muß, wenn der Bruch reduziert ist, $\mathfrak{d} = 1$ sein, sodaß $(\alpha - \beta) = (\gamma)$ wo γ durch $\mathfrak{m}$ teilbar.

b.) Sind α, β ganz und $\alpha - \beta = \gamma$ wo γ durch $\mathfrak{m}$ teilbar, so ist $(\alpha - \beta) = \frac{\mathfrak{c}}{\mathfrak{i}}$ wo $\mathfrak{c}$ durch $\mathfrak{m}$ teilbar.

c.) Ist $\alpha - \beta = \frac{\mathfrak{c}_1}{\mathfrak{d}_1}$; $\beta - \gamma = \frac{\mathfrak{c}_2}{\mathfrak{d}_2}$, so $\mathfrak{c}_1, \mathfrak{c}_2$ durch $\mathfrak{m}$ teilbar □□□ und ν_1, ν_2 durch $\mathfrak{d}_1, \mathfrak{d}_2$ teilbare, zu $\mathfrak{m}$ prime Hauptideale

$$(\nu_1) = \mathfrak{d}_1 \mathfrak{d}_1' ; \quad (\nu_2) = \mathfrak{d}_2 \mathfrak{d}_2'$$

so ist

$$\nu_1(\alpha - \beta) = \mathfrak{c}_1 \mathfrak{d}_1' = \delta_1 ; \quad \nu_2(\beta - \gamma) = \mathfrak{c}_2 \mathfrak{d}_2' = \delta_2$$

also

$$\nu_1 \nu_2 (\mathfrak{a} - \gamma) = \nu_2 \delta_1 - \nu_1 \delta_2$$

$$\mathfrak{a} - \gamma = \frac{\nu_2 \delta_1 - \nu_1 \delta_2}{\nu_1 \nu_2}, \quad \text{wo der Zähler durch } \mathfrak{m} \text{ teilbar, der Nenner nicht.}$$

94 ı

d.) Ist $\left.\begin{array}{l} \nu_1(\alpha - \beta) = \varrho_1 \\ \nu_2(\gamma - \delta) = \varrho_2 \end{array}\right\} \varrho_1, \varrho_2$ durch $\mathfrak{m}$ teilbar, so ist

$$\nu_1 \nu_2 [(\alpha \pm \gamma) - (\beta \pm \delta)] = \nu_1 \nu_2 [(\alpha - \beta) \pm (\gamma - \delta)] = \nu_2 \varrho_1 \pm \nu_1 \varrho_2$$

woraus wie unter c.) die Behauptung folgt.

Satz 9 zeigt, daß der Begriff der Restklasse vollständig erhalten bleibt und die Restklassen der ganzen Zahlen beibehalten werden. Wir zeigen jetzt, daß zu diesen Restklassen der ganzen Zahlen auch bei der Zulassung gebrochener Zahlen jedenfalls keine zu $\mathfrak{m}$ primen neuen hinzukommen, und daß die Gruppe der zu $\mathfrak{m}$ primen Restklassen genau die gleiche bleibt:

Definition 3. Eine Zahl des Körpers heißt prim zu $\mathfrak{m}$, wenn in ihrer Darstellung als reduzierter Idealbruch, $\mathfrak{m}$ weder im Zähler noch im Nenner vorkommt. Ebendasselbe soll für zu $\mathfrak{m}$ prime Ideale gelten.

Wieder erkennt man:

Satz 10. Für ganze Zahlen und Ideale stimmt der neue Begriff mit dem alten überein. Produkt und Quotient von zu $\mathfrak{m}$ primen Idealen und Zahlen ist

wieder prim zu $\mathfrak{m}$.

Satz 11. Ist α prim zu $\mathfrak{m}$, so gibt es ein ganzes zu $\mathfrak{m}$ primes ν, sodaß $\nu\alpha$ ganz, prim zu $\mathfrak{m}$ und

$$\nu\alpha \equiv \alpha \mod \mathfrak{m}$$

ist.

Beweis. Sei $\alpha = \frac{\mathfrak{a}}{\mathfrak{b}}$, wo $\mathfrak{a}$ und $\mathfrak{b}$ zu $\mathfrak{m}$ prim sind.

Ist $(\mathfrak{bc}) \leqq (\beta)$ Hauptideal ($\mathfrak{c}$ prim zu $\mathfrak{m}$), so bestimme man ν aus den Kongruenzen:

$$\begin{aligned} \nu &\equiv 0 \mod \beta \\ \nu &\equiv 1 \mod \mathfrak{m} \end{aligned}$$

was wegen $(\beta, \mathfrak{m}) = 1$ stets möglich. Dann ist

$$\nu = \beta\beta'$$

und prim zu $\mathfrak{m}$; wir haben dann

$$\alpha = \frac{\mathfrak{ac}}{\beta} = \frac{\mathfrak{ac}\beta'}{\nu}; \quad \mathfrak{ac}\beta' = \nu\alpha$$

also $\mathfrak{ac}\beta'$ ein zu $\mathfrak{m}$ primes Hauptideal γ. So wird:

$$\nu\alpha = \gamma$$

eine ganze zu $\mathfrak{m}$ prime Zahl. Wegen $\nu \equiv 1 \mod \mathfrak{m}$ ist

$$\begin{aligned} \alpha &\equiv \gamma \mod \mathfrak{m} \\ \text{also} \quad \alpha &\equiv \nu\alpha \mod \mathfrak{m} \end{aligned}$$

Satz 12 Ist α prim zu $\mathfrak{m}$ und $\alpha \equiv \beta \mod \mathfrak{m}$, so ist auch β prim zu $\mathfrak{m}$.

Beweis. Sind ν_1, ν Zahlen, sodaß $\nu(\alpha - \beta)$ eine ganze durch $\mathfrak{m}$ teilbare Zahl, $\nu_1\alpha \equiv \alpha \mod \mathfrak{m}$ im Sinne von Satz 11 ist. Dann ist auch $\nu_1\nu(\alpha - \beta)$ eine ganze, durch $\mathfrak{m}$ teilbare Zahl, und da $\nu_1\nu\alpha$ ganz ist, auch $\nu_1\nu\beta$. Ferner ist

$$\nu_1\nu\alpha \equiv \nu_1\nu\beta \mod \mathfrak{m}$$

Da die Behauptung für ganze Zahlen richtig ist, ist auch $\nu_1\nu\beta$ prim zu $\mathfrak{m}$, also auch β.

Damit ist gezeigt, daß der Begriff der primen Restklasse erhalten bleibt. Da ferner nach Satz 11 jede zu $\mathfrak{m}$ prime Zahl einer ganzen Zahl kongruent ist,

96 ı

die ebenfalls zu $\mathfrak{m}$ prim ist, bleibt nach Satz 9 und 10 auch die Anzahl der zu $\mathfrak{m}$ primen Restklassen die gleiche: $\phi(\mathfrak{m})$, und ebenso die Einteilung der ganzen, zu $\mathfrak{m}$ primen Zahlen die gleiche.

Satz 13. Sind $\alpha, \beta, \gamma, \delta$ zu $\mathfrak{m}$ prim. Dann folgt aus

$$\begin{gathered}\alpha \equiv \beta \bmod \mathfrak{m} \\ \gamma \equiv \delta \bmod \mathfrak{m} \\ \hline\end{gathered}$$

$$\alpha\gamma \equiv \beta\delta \bmod \mathfrak{m}; \quad \frac{\alpha}{\gamma} \equiv \frac{\beta}{\delta} \bmod \mathfrak{m}.$$

Es bleibt also die ganze Gruppe der zu $\mathfrak{m}$ primen Restklassen dieselbe. Ihr Grad ist $\phi(m)$, ihr Einheitselement die Klasse 1 mod $\mathfrak{m}$. Es gilt der Fermatsche Satz

$$\alpha^{\phi(\mathfrak{m})} \equiv 1 \mod \mathfrak{m}.$$

Beweis. Seien $\nu_1(\alpha - \beta) = \varrho_1$ und $\nu_2(\gamma - \delta) = \varrho_2$ durch $\mathfrak{m}$ teilbare ganze Zahlen (ν_1, ν_2 prim zu $\mathfrak{m}$). ν_3 und ν_4 seien zu $\mathfrak{m}$ prim und $\nu_3\alpha, \nu_4\delta$ ganz. Dann ist

$$\begin{aligned}\nu_1\nu_2\nu_3\nu_4(\alpha\gamma - \beta\delta) &= \nu_1\nu_2\nu_3\nu_4[\alpha(\gamma - \delta) + \delta(\alpha - \beta)] \\ &= \nu_1\nu_3\nu_4\alpha\varrho_2 + \nu_2\nu_3\nu_4\delta\varrho_1\end{aligned}$$

Dies ist eine ganze durch $\mathfrak{m}$ teilbare Zahl, also

$$\alpha\gamma \equiv \beta\delta \mod \mathfrak{m}.$$

Sei dann ν prim zu $\mathfrak{m}$ und

$$\nu(\alpha\gamma - \beta\delta) = \varrho$$

ganz durch $\mathfrak{m}$ teilbar, ν' prim zu $\mathfrak{m}$, sodaß $\frac{\nu'}{\gamma\delta}$ ganz ist. Dann folgt

$$\nu\nu'\left(\frac{\alpha}{\gamma} - \frac{\beta}{\delta}\right) = \frac{\nu'}{\gamma\delta} \cdot \nu(\alpha\delta - \beta\gamma) = \frac{\nu'}{\gamma\delta}\varrho$$

ganz und durch $\mathfrak{m}$ teilbar, also

$\frac{\alpha}{\gamma} \equiv \frac{\beta}{\delta} \bmod \mathfrak{m}$, w.z.b.w.

97 I

Definition 4. Eine Menge von Körperzahlen heißt ein *Strahl*, wenn in ihr uneingeschränkt und eindeutig Multiplikation und Division ausführbar ist.

Als Beispiel führen wir etwa die Einheiten an.

Nun sei $\mathfrak{g}$ eine Untergruppe der Gruppe der primen Restklassen mod $\mathfrak{m}$. Die Zahlen aus $\mathfrak{g}$ bilden dann offenbar einen Strahl. Ist $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ ein Repräsentantensystem der Restklassen von $\mathfrak{g}$, so gilt für jede Zahl des Strahls eine Kongruenz $\alpha \equiv \alpha_i \bmod \mathfrak{m}$. Als Gruppe enthält $\mathfrak{g}$ sicher die Klasse 1 mod $\mathfrak{m}$, der Strahl also alle Zahlen $\equiv 1 \bmod \mathfrak{m}$. Ist $\mathfrak{g}$ die Gruppe der zu $\mathfrak{m}$ primen Restklassen selbst, so umfaßt der Strahl alle zu $\mathfrak{m}$ primen Körperzahlen.

Mit solchen aus Untergruppen der Gruppe der zu $\mathfrak{m}$ primen Restklassen entspringenden Strahlen sind noch nicht alle für uns in Betracht kommenden Strahlen erschöpft. Wir haben noch die „*Signaturgruppen*“ hinzuzuziehen. Unter „*Signatur*“ einer Zahl α aus k versteht man das System von r_1 Vorzeichen, das die zu α konjugierten in den r_1 reellen Körpern aufweisen. Die 2^{r_1} möglichen Signaturen des Körpers bilden eine Abelsche Gruppe vom Grade 2^{r_1} vom Typus $(2, 2, \ldots, 2)$; (r_1 mal).

(Daß alle 2^{r_1} Signaturen im Körper durch wirkliche Zahlen vertreten sind, erkennt man so: Seien die r_1 reellen Basisformen

$$\begin{aligned} y_1 &= \omega_1^{(1)} x_1 + \cdots + \omega_n^{(1)} x_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_{r_1} &= \omega_1^{(r_1)} x_1 + \cdots + \omega_n^{(r_1)} x_n \end{aligned}$$

98 I

Da ihre Matrix den Rang r_1 hat, kann man $n - r_1$ Unbestimmte x_i beliebig rational und die übrigen r_1 zunächst reell so wählen, daß ein bestimmtes der y_i, etwa y_1 negativ, alle anderen positiv werden. Durch genügend kleine Variation der x_i in rationale Zahlwerte, bleiben die Vorzeichen der y_i erhalten. Damit ist die Existenz jeder Signatur, die nur ein -1 an bestimmter Stelle hat gezeigt, und damit durch Komposition die Existenz jeder).

Wenn wir nun eine Untergruppe Σ der Signaturgruppe nehmen, und aus dem vorhin genannten, durch die Untergruppe $\mathfrak{g}$ bestimmten Strahl nur die

Zahlen herausgreifen, deren Signatur zu Σ gehört, so erhalten wir einen neuen Strahl, dessen Zahlen außer den vorhin genannten Kongruenzbedingungen noch gewissen Vorzeichenbedingungen für die reellen konjugierten genügen.

Wir zeigen zunächst, daß jede mögliche Signatur in den durch $\mathfrak{g}$ definierten Strahl tatsächlich vorkommt. Sei α irgendeine Körperzahl mit der vorgeschriebenen Signatur, ferner m eine ganze positive Zahl so, daß $m\alpha$ ganz ist. Dann hat $m\alpha$ dieselbe Signatur wie α. Ist ferner ϱ eine durch $\mathfrak{m}$ teilbare Zahl, so ist ϱ^2 ebenfalls durch $\mathfrak{m}$ teilbar und total positiv. $m\alpha\varrho^2$ ist also eine ganze, durch $\mathfrak{m}$ teilbare Zahl mit der vorgeschriebenen Signatur. Durch Multiplikation mit einer geeigneten ganzen, positiven rationalen Zahl N kann man noch erreichen, daß $\mathsf{N}m\alpha\varrho^2$ beliebig hohe Beträge mit sämtlichen konjugierten annimmt.

99 I

Ist nun ξ eine Zahl aus $\mathfrak{g}$, so ist auch $\xi + \mathsf{N}m\alpha\varrho^2 \equiv \xi \bmod \mathfrak{m}$ eine Zahl aus $\mathfrak{g}$. Durch genügend große Wahl von $\mathsf{N} > 0$ erreicht man es, daß $\xi + \mathsf{N}m\alpha\varrho^2$ die vorgeschriebene Signatur erhält.

Definition 5. Die Menge aller Zahlen des Körpers, die einer bestimmten Untergruppe der Gruppe der zu dem Ideal $\mathfrak{m}$ primen Restklassen mod $\mathfrak{m}$ angehören, und deren Signaturen zu einer bestimmten Untergruppe der Signaturgruppe gehören, bilden einen Strahl, genauer einen „*Kongruenzstrahl mod* $\mathfrak{m}$“.

Da im Folgenden nur von Kongruenzstrahlen die Rede sein wird, bezeichnen wir diese auch kurz als „*Strahlen*“ mod $\mathfrak{m}$.

Definition 6. Eine Einheit die in einem bestimmten Strahl vorkommt, heißt kurz eine *Strahleinheit*.

Satz 14. Ist ε eine Körpereinheit, S ein Strahl mod $\mathfrak{m}$, dann ist sicher $\varepsilon^{2\phi(\mathfrak{m})}$ Strahleinheit.

Beweis. Jede Signaturgruppe enthält die Einheitssignaturgruppe, nämlich die Gruppe aller total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$. Also enthält jeder Strahl sicher die Menge der total positiven Zahlen, die $\equiv 1 \bmod \mathfrak{m}$ sind. Als Einheit ist ε sicher prim zu $\mathfrak{m}$, also $\varepsilon^{\phi(\mathfrak{m})} \equiv 1 \bmod \mathfrak{m}$, $\varepsilon^{2\phi(\mathfrak{m})} \equiv 1 \bmod \mathfrak{m}$ und total positiv, außerdem Einheit, also Strahleinheit.

100 I

Ist $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ ein System von Grundeinheiten für R, so gibt es in S sicher Strahleinheiten der Form:

$$\eta_i = \varrho \varepsilon_1^{e_1} \ldots \varepsilon_i^{e_i}; \qquad (i = 1, 2, \ldots, r)$$

Denn $\varepsilon_i^{2\phi(\mathfrak{m})}$ ist eine solche. Sei nun η_i diejenige unter den Strahleinheiten dieser Form, deren $e_i > 0$ möglichst klein ist. Ist dann in S:

$$\mathsf{H} = \varrho' \varepsilon_1^{h_1} \ldots \varepsilon_i^{h_i}$$

eine Strahleinheit, so muß offenbar h_i durch e_i teilbar sein, da man sonst eine Strahleinheit mit kleinerem Exponenten von ε_i als e_i finden könnte. Daraus ergibt sich in bekannter Weise:

Satz 15. Es gibt in S ein System von r Einheiten $\eta_1, \eta_2, \ldots, \eta_r$, sodaß jede Strahleinheit H sich eindeutig in der Form

$$\mathsf{H} = \varrho \eta_1^{a_1} \ldots \eta_r^{a_r}; \qquad (a_i \text{ ganzz.})$$

darstellen läßt, wo ϱ eine Einheitswurzel des Strahles ist. Die Einheiten $\eta_1, \ldots, \eta_r$ heißen die *Grundeinheiten des Strahls.*

Ebenso zeigt man wie früher, daß der absolute Wert der reellen Determinante $|\ell_\kappa(\eta_i)|$ eine von Null verschiedene, nur vom Strahl S abhängige Zahl R_S ist, die der Regulator des Strahls genannt wird. Da sich die η_i durch die ε_i mit ganzzahligen Exponenten ausdrücken lassen ist der Quotient $\frac{R_S}{R}$ eine positive, ganze Zahl.

Die w Einheitswurzeln des Körpers bilden eine Gruppe, ebenso die w_S Einheitswurzeln des Strahls; letztere ist also Untergruppe der ersteren, als $\frac{w}{w_S}$ ganz.

Wie alles dies im Falle $r = 0$ zu verstehen ist, ist klar.

Wir haben nun noch einen wichtigen Begriff einzuführen, den des *Einheitenverbandes.*

Definition 7. Sei ℓ eine beliebige, fest gewählte Primzahl, E eine Strahleinheit. Dann heißt die Gesamtheit aller Einheiten $\mathsf{E}\mathsf{H}^\ell$, wo H alle Strahleinheiten durchläuft, ein Einheitenverband nach ℓ des Strahls.

Satz 16. Zwei Einheitenverbände $\mathsf{E}_1\mathsf{H}^\ell$ und $\mathsf{E}_2\mathsf{H}^\ell$ sind entweder ganz verschieden oder identisch, letzteres dann und nur dann, wenn $\frac{\mathsf{E}_1}{\mathsf{E}_2}$ die ℓ–te Potenz

einer Strahleinheit ist.

Beweis. Sei $(\mathsf{E}_1\mathsf{H}^\ell) = (\mathsf{E}_2\mathsf{H}^\ell)$; dann ist speziell:

$$\mathsf{E}_1\mathsf{H}_1^\ell = \mathsf{E}_2\mathsf{H}_2^\ell$$

also $\quad \frac{\mathsf{E}_1}{\mathsf{E}_2} = \left(\frac{\mathsf{H}_2}{\mathsf{H}_1}\right)^\ell$

Ist dies umgekehrt erfüllt, so folgt:

$$(\mathsf{E}_1\mathsf{H}^\ell) = \mathsf{E}_2\left(\frac{\mathsf{H}_2}{\mathsf{H}_1}\mathsf{H}\right)^\ell$$

also die Identität. Ist ferner auch nur ein Element gemeinsam:

$$\mathsf{E}_1\mathsf{H}_1^\ell = \mathsf{E}_2\mathsf{H}_2^\ell$$

so folgt wie oben die Identität, w.z.b.w.

Damit also E_1 und E_2 dieselben Einheitenverbände definieren, ist notwendig und hinreichend, daß, wenn

$$\mathsf{E}_1 = \varrho_1\eta_1^{a_1}\dots\eta_r^{a_r} \qquad\qquad \mathsf{E}_2 = \varrho_2\eta_1^{b_1}\dots\eta_r^{b_r}$$

ist, dann $a_i \equiv b_i \bmod \ell$ und $\frac{\varrho_1}{\varrho_2}$ die ℓ–te Potenz einer

Einheitswurzel des Strahls ist. Typisch für *alle* Einheitenverbände sind also die Einheiten

$$\mathsf{E} = \varrho\eta_1^{a_1}\dots\eta_r^{a_r}$$

wo die a_i je ein reelles Restsystem mod ℓ (etwa $0, 1, \dots, \ell-1$) durchlaufen und ϱ alle jene Einheitswurzeln des Strahls, deren Quotient nicht die ℓ–te Potenz einer Einheitswurzel des Strahls ist.

Sind nun ϱ_1 und ϱ_2 zwei verschiedene solche Einheitswurzeln und enthielte S keine primitive ℓ–te Einheitswurzel, sodaß also die Grade $\mathfrak{m}_1$ und $\mathfrak{m}_2$ von ϱ_1 und ϱ_2 prim zu ℓ sind; dann kann

□□□

$$\left.\begin{aligned} x_1\mathfrak{m}_1 + y_1\ell &= 1 \\ x_2\mathfrak{m}_2 + y_2\ell &= 1 \end{aligned}\right\} \text{gesetzt werden,}$$

und

$$\begin{array}{rcccl} \varrho_1 & = & \varrho_1^{1-x_1\mathfrak{m}_1} & = & \varrho_1^{y_1\ell} \\ \varrho_2 & = & \varrho_2^{1-x_2\mathfrak{m}_2} & = & \varrho_2^{y_2\ell} \end{array}$$

also

$$\frac{\varrho_1}{\varrho_2} = \left(\frac{\varrho_1^{y_1}}{\varrho_2^{y_2}}\right)^{\ell}$$

entgegen der Voraussetzung. Wenn also S keine primitive ℓ–te Einheitswurzel enthält, ist nur $\varrho = 1$ typisch für die Verbände und somit die Zahl der Verbände ℓ^r. (Denn wäre auch nur eine von 1 verschiedene E.W. ϱ typisch, so bildete diese mit 1 zusammen ein solches System ϱ_1, ϱ_2 dessen Unmöglichkeit wir nachwiesen. 1 ist stets typisch, da alle $\eta_1, \ldots, \eta_r$ Strahleinheiten sind.)

Wenn aber S eine primitive ℓ–te E.W. enthält und ϱ eine primitive ℓ^k–te E.W. von möglichst hohem Exponenten ist, so läßt sich jede E.W. ϱ aus S in der Form

103 I

darstellen:

$$\varrho = \zeta^i \varrho_1$$

wo ϱ_1 vom Grad $\mathfrak{m}_1$ ist, und $(\mathfrak{m}_1, \ell) = 1$ ist. Da dann wie vorhin ϱ_1 die ℓ–te Potenz einer E.W. aus S ist, brauchen für ϱ nur die Potenzen ζ^i in Betracht gezogen zu werden. ϱ^i ist dann und nur dann ℓ–te Potenz einer Strahleinheit, wenn i durch ℓ teilbar ist, ein Quotient $\frac{\varrho^i}{\varrho^k}$ also dann und nur dann, wenn $i \equiv k \bmod \ell$ ist. Wir haben also nur die Typen:

$$1, \zeta, \zeta^2, \ldots, \zeta^{\ell-1}.$$

Satz 17. Die Anzahl der Einheitenverbände nach ℓ im Strahl S ist ℓ^r oder ℓ^{r+1}, je nachdem S keine primitive ℓ–te Einheitswurzel enthält, oder eine enthält.

Multipliziert man alle Einheiten des Verbandes $V = (\mathsf{E}\mathsf{H}^\ell)$ mit allen aus $V_1 = (\mathsf{E}_1\mathsf{H}^\ell)$, so erhält man den Verband $(\mathsf{E}\mathsf{E}_1\mathsf{H}^\ell)$, den wir das Produkt der Verbände V und V_1 nennen; analog der Quotient:

$$VV_1 = (\mathsf{E}\mathsf{E}_1\mathsf{H}^\ell)$$
$$\frac{V}{V_1} = \left(\frac{\mathsf{E}}{\mathsf{E}_1}\mathsf{H}^\ell\right)$$

Daraus ergibt sich:

Satz 18. Die Verbände der Einheiten in S bilden eine Abelsche Gruppe vom Grade ℓ^r oder ℓ^{r+1}. Das Einheitselement bildet der Verband (H^ℓ) bestehend aus allen ℓ–ten Potenzen von Strahleinheiten. Ersichtlich ist der Gruppenexponent

104 I

eines jeden Elementes gleich ℓ. Die Basisdarstellung der Gruppe hat also die Form:

$$\begin{aligned} V &= V_1^{a_1} \dots V_r^{a_r} \\ \text{resp. } V &= V_0^{a_0} V_1^{a_1} \dots V_r^{a_r} \end{aligned}$$

wo die a_i von 0 bis $\ell - 1$ laufen, und die Basiselemente etwa als:

$$V_0 = (\varrho \mathsf{H}^\ell); \quad V_i = (\eta_i \mathsf{H}^\ell); \quad (i = 1, 2, \dots, r)$$

gewählt werden können.

Um nun die Struktur aller Strahlen nach einem festen Modul $\mathfrak{m}$ zu untersuchen, sei S ein solcher Strahl. Wir betrachten dann die Gesamtheit aller zu $\mathfrak{m}$ primen Zahlen und teilen sie in Komplexe ein, indem wir in ein– und denselben Komplex alle und nur die Zahlen nehmen, deren Quotient zu S gehört. Daß dies geht, sieht man so:

Ist $\frac{\alpha}{\beta}$ und $\frac{\beta}{\gamma}$ Zahl aus S, so ist auch $\frac{\alpha}{\gamma}$ Zahl aus S. Gehört demnach β zum Komplex von α und γ zum Komplex von β, so gehört auch γ zum Komplex von α. Es kann daher keine Zweideutigkeit in der Zuordnung entstehen.

Diese Einteilung möge zuerst für den Strahl S_0 aller total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$ geschehen. In einem Komplex kommen dann immer alle Zahlen einer bestimmten Restklasse gleicher Signatur. Nach dem Schluß auf S.98▸/99▸ gibt es in jeder Restklasse mod $\mathfrak{m}$ Zahlen aller möglichen Signaturen. Es zerfällt daher jede Restklasse

105 I

in genau 2^{r_1} Komplexe. Die Gesamtanzahl aller Komplexe ist somit $\mathsf{N} = 2^{r_1}\phi(\mathfrak{m})$. Seien $S_0, S_1, \dots, S_{\mathsf{N}-1}$ diese Komplexe. Ist nun S irgendein Strahl, so enthält er, wie gezeigt wurde, sicher S_0. Wenn also S eine Zahl α_i aus S_i enthält, so enthält S gleichzeitig den ganzen Komplex S_i, denn es ist ja $S_i = \alpha_i S_0$, und da α_i und S_0 zu S gehören, gehört auch $S_i = \alpha_i S_0$ zu S. Nun bilden unsere N Komplexe sicher eine Abelsche Gruppe, wenn die Multiplikation so definiert ist:

$$S_i = \alpha_i S_0; \quad S_k = \alpha_k S_0$$
$$S_i S_k = \alpha_i \alpha_k S_0 \,.$$

Es seien nun $S_0, S_1, \ldots, S_{K-1}$ die in S liegenden Komplexe. Da S ein Strahl ist, liegt auch $S_i S_k$ in S, wenn S_i und S_k in S liegen. Die Komplexe von S bilden also eine Untergruppe der Gruppe aller N Komplexe.

Umgekehrt, fassen wir irgendeine Untergruppe der Gruppe aller N Komplexe zu einem System S zusammen, so ist S der Gruppeneigenschaft wegen ein Strahl, und da die einzelnen Komplexe nur durch Kongruenz– und Vorzeichenbedingungen entstehen, ein Kongruenzstrahl.

Wir erfahren also alle Strahlen nach $\mathfrak{m}$, wenn wir alle Untergruppen unserer Gruppe von N Komplexen aufsuchen. □□□

Diese Gruppe nennen wir die Komplexgruppe nach S_0

Die auf S. 104 definierte Zerlegung in Komplexe nach S ist dann nichts anderes als die Zerlegung der Komplexgruppe S_0 □□□ in Nebengruppen nach S. Ist also K die Anzahl der Komplexe nach S_0 aus denen S besteht, so ist die Anzahl der Komplexe nach S gleich dem Index von S in Bezug auf die Komplexgruppe nach S_0, also gleich $\frac{2^{r_1}\phi(\mathfrak{m})}{K}$, also endlich. Jeder Komplex nach S besteht dann aus gleich vielen Komplexen nach S_0. K ist Teiler von $2^{r_1}\phi(\mathfrak{m})$.

Alles dies gilt noch allgemeiner:

Seien $S, S^{(1)}, \ldots, S^{(n_1-1)}$ die Komplexe nach S. Sie bilden eine Abelsche Gruppe. Jede ihrer Untergruppen bildet wieder einen Kongruenzstrahl, und ihre Nebengruppen sind die zugehörigen Komplexe. Ist andererseits s ein Strahl der ganz in S liegt, so besteht S aus einer gewissen Anzahl n_2 von Komplexen nach s:

$$S = s + s_1 + \cdots + s_{n_2-1}$$

Jeder Komplex $S^{(i)}$ zerfällt dann in ebenfalls n_2 Komplexe nach s. Die Zahl der Komplexe nach s ist dann $n_1 n_2$.

Mit Hilfe des Strahlbegriffs geben wir nun eine sehr weitgehende Verallgemeinerung des Klassenbegriffs.

Zu diesem Zweck betrachten wir die Gesamtheit aller zu $\mathfrak{m}$ primen Ideale.

Definition 8. Ist S ein Strahl nach dem Modul $\mathfrak{m}$, so heißen zwei zu $\mathfrak{m}$ prime (ganze oder gebrochene) Ideale $\mathfrak{a}$ und $\mathfrak{b}$ äquivalent, wenn ihr Quotient

$\frac{\mathfrak{a}}{\mathfrak{b}}$ gleich einem Hauptideal (α) gesetzt werden kann wo α Strahlzahl aus S ist.

Auf Grund der Eigenschaften des Strahles S erkennt man unmittelbar, daß die so definierte Äquivalenz transitiv ist, und daß ferner

$$\begin{array}{lrcl} \text{aus} & \mathfrak{a}_1 & \sim & \mathfrak{b}_1 \\ & \mathfrak{a}_2 & \sim & \mathfrak{b}_2 \\ \hline \text{folgt} & \mathfrak{a}_1\mathfrak{a}_2 & \sim & \mathfrak{b}_1\mathfrak{b}_2 \\ & \frac{\mathfrak{a}_1}{\mathfrak{a}_2} & \sim & \frac{\mathfrak{b}_1}{\mathfrak{b}_2} \end{array}$$

Wir können also alle zu $\mathfrak{m}$ primen Ideale in Klassen untereinander äquivalenter teilen und mit diesen Klassen eindeutig und unbeschränkt multiplizieren und dividieren. Diese Klassen bilden eine Abelsche Gruppe, deren Endlichkeit sich gleich zeigen wird. Wir nennen dies: *Idealklassen nach S*. Das Einheitselement dieser Klassengruppe ist offenbar die Klasse aller Hauptideale, die sich durch Zahlen aus S darstellen lassen, und soll „*Hauptklasse*“ heißen.

Unsere Definition umfaßt offenbar □□□ die beiden in der elementaren algebr. Zahlentheorie benutzten „*Idealklassen im weiteren und engeren Sinne*“.

Die erste entsteht aus $\mathfrak{m} = (1)$ und dem Strahl aller von Null verschiedenen Körperzahlen,

die zweite aus $\mathfrak{m} = (1)$ und dem Strahl aller total positiven Körperzahlen.

Nun sei $\mathfrak{m}$ beliebig. Als Strahl S_1 wählen wir den Strahl *aller zu $\mathfrak{m}$ primer Zahlen*, d.h. den umfassendsten

108 I

Strahl nach dem Modul $\mathfrak{m}$ (alle primen Restklassen). Es sei $\mathfrak{K}$ eine Idealklasse im alten, gewöhnlichen Sinn, $\mathfrak{b}$ ein Ideal aus $\mathfrak{K}^{-1}$. Wir wählen ein zu $\mathfrak{m}$ primes Ideal $\mathfrak{a}$ so, daß $\mathfrak{ab}$ Hauptideal ist, dann gehört $\mathfrak{a}$ zu $\mathfrak{K}$. Dies ist offenbar stets möglich, denn ist $\mathfrak{b}$ genau durch $\mathfrak{m}^\nu$ teilbar, so gibt es stets Körperzahlen γ die genau durch $\mathfrak{m}^\nu$ teilbar sind. Dann ist $\mathfrak{a} = \frac{\gamma}{\mathfrak{b}}$ ein solches Ideal, wie wir es verlangen. Damit ist gezeigt, daß jede Idealklasse im alten Sinn zu $\mathfrak{m}$ prime Ideale enthält.

Seien $\mathfrak{a}_1, \mathfrak{a}_2$ zwei zu $\mathfrak{m}$ prime Ideale aus $\mathfrak{K}$. Dann ist ihr Quotient $\frac{\mathfrak{a}_1}{\mathfrak{a}_2}$ auch prim zu $\mathfrak{m}$. Sie sind also nach S_1 äquivalent. Daß umgekehrt zwei nach S_1 äquivalente Ideale auch im „*absoluten*“ Sinne äquivalent sind, ist klar. Die zu $\mathfrak{m}$ primen Ideale einer absoluten Idealklasse $\mathfrak{K}$ bilden also gerade eine

Idealklasse nach S_1. Ist h die absolute Klassenzahl, so gibt es mithin ebenfalls h Klassen nach S_1 und die beiden Klassengruppen (nach S_1 und die absolute) sind identisch. (Nur sind bei den Klassen nach S_1 die durch $\mathfrak{m}$ teilbaren Ideale nicht mit zu den einzelnen Klassen zu rechnen, was jedoch für das Rechnen mit Idealklassen ohne Bedeutung ist).

Sei jetzt S ein beliebiger Strahl nach dem Modul $\mathfrak{m}$. $S, S_1, \ldots, S_{K-1}$ seien die Komplexe der zu $\mathfrak{m}$ primen Zahlen nach S (die Nebengruppen der Zahlengruppe S in Bezug auf die Gruppe aller zu $\mathfrak{m}$ primen Zahlen). Die Zahlen aus diesen Komplexen erzeugen Hauptideale.

109 I

Von diesen werden zunächst alle Hauptideale eines Komplexes S_i äquivalent, da sie sich nur um Faktoren aus S unterscheiden. Darüber hinaus werden aber auch Hauptideale verschiedener Komplexe äquivalent sein können. □□□

Dazu genügt es zu untersuchen, welche Komplexe solche Hauptideale enthalten, die zu den „*Hauptidealen nach S*“ äquivalent sind, d.h. selbst Hauptideale nach S sind.

Wir beweisen:

1.) Enthält ein Komplex S_i ein Hauptideal nach S, so liefert der ganze Komplex nur Hauptideale nach S

2.) Dies tritt dann und nur dann ein, wenn S_i eine Einheit enthält.

3.) Die Komplexe $S, S_1, \ldots, S_{q-1}$, die aus Hauptidealen nach S bestehen bilden eine Abelsche Gruppe, Untergruppe der Komplexgruppe nach S

4.) Alle und nur die Nebengruppen zu dieser durch 3.) definierten Untergruppe im Bezug auf die ganze Komplexgruppe nach S liefern untereinander äquivalente (nach S) Ideale (absolute Hauptideale).

Beweis. 1.) 2.) Sei (α_i) ein Hauptideal (absolut) aus S_i, das auch als Hauptideal nach S geschrieben werden kann:

$$(\alpha_i) = (\alpha); \quad (\alpha \text{ aus } S)$$

Dann ist $\varepsilon_i = \frac{\alpha_i}{\alpha}$ Zahl aus S_i und Einheit. Der ganze Komplex S_i läßt sich dann darstellen

$$S_i = \varepsilon_i \alpha,$$

wo α alle Zahlen aus S durchläuft, alle Hauptideale (absolut) aus S_i sind also Hauptideale nach S. Damit ist 1.) u. 2.) gezeigt.

3.) Enthält S_i die Einheit ε_i und S_k die Einheit ε_k, so enthalten:

$$\begin{array}{ccccc} S_iS_k & \text{die} & \text{Einheit} & \varepsilon_i\varepsilon_k \\ \dfrac{S_i}{S_k} & \| & \| & \dfrac{\varepsilon_i}{\varepsilon_k} \end{array}$$

Daraus folgt die Gruppeneigenschaft der Komplexe S_i mit Einheiten. Ihre Anzahl q ist ein Teiler von K.

4.) Ist $(\overline{S})$ das System der q Komplexe mit Einheiten und $q = \frac{K}{K_1}$, so gibt es K_1 Komplexe $\square\square\square$ $S^{(0)} = S;\ S^{(1)};\ \ldots;\ S^{(K_1)}$, sodaß das System (S) aller K Komplexe sich darstellen läßt:

$$(S) = S^{(0)}(\overline{S}) + S^{(1)}(\overline{S}) + \cdots + S^{(K_1)}(\overline{S}).$$

(Zerlegung nach Nebengruppen). Alle Komplexe einer dieser Nebengruppen unterscheiden sich nur um Hauptideale nach S, da das System $(\overline{S})$ nur solche liefert, und umgekehrt, wenn $\square\square\square$ zwei Komplexe sich nur um Hauptideale nach S unterscheiden, sind sie in derselben Nebengruppe (charakteristische Eigenschaft der Nebengruppen).

Damit ist 3.) u. 4.) ebenfalls bewiesen. Es ergibt sich daraus unmittelbar:

Die zu $\mathfrak{m}$ primen absoluten Hauptideale zerfallen nach S in $K_1 = \frac{K}{q}$ Klassen:

$$\mathfrak{K}_0 = \overline{\mathfrak{K}}_0 + \overline{\mathfrak{K}}_1 + \cdots + \overline{\mathfrak{K}}_{K_1}$$

die eben genau den Nebengruppen in 4.) entsprechen.

Ist nun $\mathfrak{K}$ eine absolute Idealklasse, so enthält sie sicher eine Klasse $\overline{\mathfrak{K}}$ nach S. Sie enthält dann gleichzeitig auch jedes $\overline{\mathfrak{K}}\,\overline{\mathfrak{K}}_i\,;\ (i = 0, 1, \ldots, K_1 - 1)$ und besteht nur aus diesen K_1 Klassen nach S, da ja jedes als Idealquotient bei der Äquivalenz auftretende absolute Hauptideal in eine und nur eine dieser K_1 Klassen fällt. Also zerfällt jede absolute Klasse in K_1 nach S:

$$\mathfrak{K} = \overline{\mathfrak{K}}\,\overline{\mathfrak{K}}_0 + \overline{\mathfrak{K}}\,\overline{\mathfrak{K}}_1 + \cdots + \overline{\mathfrak{K}}\,\overline{\mathfrak{K}}_{K_1-1}$$

Die Klassenzahl h_S nach S ist also: $h_S = K_1 h$ und

111

somit endlich.

Diese Sätze gelten wieder allgemeiner. Seien S und s zwei Strahlen und s in S enthalten. Es gelte die Zerlegung in Komplexe:

$$S = s + s_1 + \cdots + s_{\kappa-1}$$

In $s, s_1, \ldots, s_{\mu-1}$ mögen Einheiten vorkommen. Dann ist der Gruppeneigenschaft wegen μ ein Teiler von κ, $\kappa = \mu\kappa_1$ und je μ unserer Komplexe erzeugen immer untereinander äquivalente Ideale (Hauptideale) nach s.

Die Hauptklasse $\overline{\mathfrak{K}}_0$ nach S zerfällt also in genau κ_1 Klassen nach s:

$$\overline{\mathfrak{K}}_0 = \mathfrak{k}_0 + \mathfrak{k}_1 + \cdots + \mathfrak{k}_{\kappa_1-1}\,.$$

Ebenso zerfällt jede andere Klasse

$$\overline{\mathfrak{K}}_1 = \mathfrak{k}\mathfrak{k}_0 + \mathfrak{k}\mathfrak{k}_1 + \cdots + \mathfrak{k}\mathfrak{k}_{\kappa_1-1}\,,$$

sodaß für die Klassenzahlen folgt:

$$h_s = h_S\kappa_1\,.$$

Die Faktoren $K_1 = \frac{K}{q}$ bezw. $\kappa_1 = \frac{\kappa}{\mu}$ haben eine einfache Bedeutung. Es ist ja jeder Strahl eine unendliche Abelsche Gruppe, deren Elemente die Zahlen des Strahles sind. Ein in ihm enthaltener Strahl ist eine Untergruppe und die Zerlegung in Komplexe die Zerlegung in Nebengruppen. Es ist also

$$K = (S_1 : S)$$

wo S_1 den Strahl aller zu $\mathfrak{m}$ primen Zahlen und das Symbol den Gruppenindex bedeutet, ebenso

$$\kappa = (S : s)$$

112

Sei ferner E die Gruppe aller Einheiten in k, E_S die Gruppe aller Einheiten in S. Die in den Komplexen $S, S_1, \ldots, S_{q-1}$ enthaltenen Einheiten sind nichts anderes als die Nebengruppen von E nach E_S, ebenso die in $s, s_1, \ldots, s_{\mu-1}$ vorkommenden Einheiten die Nebengruppen von E_S nach E_s,

wie man sich leicht nach Definition der Nebengruppen klar macht.

Satz 19. Jede absolute Idealklasse zerfällt, (von den durch $\mathfrak{m}$ teilbaren Idealen abgesehen), in gleich viel Idealklassen nach S, nämlich in $\frac{(S_1:S)}{(E_{S_1}:E_S)}$ Idealklassen nach S, wo S_1 die Gruppe aller zu $\mathfrak{m}$ primen Zahlen, E_{S_1} und E_S die Gruppen der Einheiten in k (d.h. in S_1) und in S bezeichnen und das Symbol $(P : Q)$ den Untergruppen–Index bedeutet. Daraus ergibt sich als Klassenzahl nach S:

$$h_S = \frac{(S_1 : S)}{(E_{S_1} : E_S)} \cdot h_{S_1}$$

wo $h_{S_1} = h$ die absolute Klassenzahl ist.

Ebenso gilt für die Klasenzahlen nach einem Strahl S und einem ganz in ihm enthaltenen Strahl s, daß jede Klasse nach S in genau $\frac{(S:s)}{(E_S:E_s)}$ Klassen nach s zerfällt, und also

$$h_s = \frac{(S : s)}{(E_S : E_s)} \cdot h_S$$

ist.

Nun geben wir noch eine weitere kleine Verallgemeinerung des Idealklassenbegriffs.

113 I

Definition 9. Jede Untergruppe H der Gruppe G_S aller Idealklassen nach S heißt eine Klassengruppe. Ist

$$G_S = \mathsf{H} + \mathsf{H}_1 + \cdots + H_j$$

die Zerlegung von G_S nach H, so fassen wir alle Klassen einer Nebengruppe H_i in eine Klasse in weitestem Sinne zusammen. Die Gruppe H spielt dann die Rolle der Hauptklasse.

Ist $\mathfrak{K}$ irgendeine Klasse nach S, so wird also der ganze Komplex $\mathfrak{K}\mathsf{H}$ als Klasse in weitestem Sinne betrachtet. Die Klassenzahl ist gleich dem Index j_{H} von H nach der Gruppe aller Idealklassen nach S. Ist also g der Grad von H, so ist die Klassenzahl:

$$j_{\mathsf{H}} = \frac{h_S}{g}$$

Gehen wir von S zu einem in S enthaltenen Strahl s über, so zerfällt jede Klasse nach S in gleich viel, etwa d Klassen nach s. Der Grad g von H erhöht sich also auf das d–fache:

$$\overline{g} = gd,$$

ebenso auch die Klassenzahl h_S: (Satz 19):

$$h_s = h_S \cdot d$$

Die Klassenzahl j_{H} in weitestem Sinne bleibt also dieselbe. Ebenso bleibt auch die Klasseneinteilung selbst erhalten. In der Tat ist ja

$$\mathfrak{K} = \mathfrak{k}\mathfrak{k}_0 + \mathfrak{k}\mathfrak{k}_1 + \cdots + \mathfrak{k}\mathfrak{k}_{d-1}\,,$$

wenn

$$\mathfrak{K}_0 = \mathfrak{k}_0 + \mathfrak{k}_1 + \cdots + \mathfrak{k}_{d-1}$$

Die Zerfällung der Hauptklasse nach S beim Übergang zu s ist.

114

Da nun H ursprünglich aus den $\mathfrak{K}$ definiert war, ist

$$\mathfrak{k}_i\mathsf{H} = \mathsf{H} \qquad \text{(da } \mathfrak{k}_i \text{ zur Hauptklasse } \mathfrak{K}_0 \text{ gehört)}$$

also $\qquad \mathfrak{K}\mathsf{H} = \mathfrak{k}\mathsf{H} = \mathfrak{k}\mathfrak{k}_i\mathsf{H}$

sodaß also die Nebengruppen von H, die mittels der $\mathfrak{K}$ gebildet werden, immer mit je d Nebengruppen, die aus den k gebildet sind, identisch sind. ($\longrightarrow$ Dieses System von einer bezw. d Nebengruppen bildet dann unsere allgemeinste Klasse.)

Dieser weiteste Klassenbegriff ist also unabhängig davon, ob wir vom Strahle S zu einem in S enthaltenen Strahl s übergehen.

(Die vorher ausführlich behandelte Klasseneinteilung erhält man aus dieser allgemeinsten, wenn man für die Untergruppe H die Hauptklasse $\mathfrak{K}_0$ allein nimmt).

Wegen der eben gezeigten Unabhängigkeit vom Strahl *erhält man auf jeden Fall alle möglichen Klasseneinteilungen, wenn man als Strahl S_0 den Strahl aller total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$ nimmt, der in allen Strahlen enthalten ist, und alle Untergruppen der Klassengruppe nach S_0 bestimmt.*

Andererseits braucht man nicht bei jeder Klasseneinteilung bis zu diesem Strahl hinabzusteigen. Dies gilt insbesondere für die Klasseneinteilungen ungerader Klassenzahl. In der Tat, seien die Idealklassen nach S_0 bestimmt, H eine Klassengruppe von ungeradem Index, $\mathfrak{K}_0$ die Hauptklasse der Klasseneinteilung nach dem Strahl $\overline{S}_0$ der Zahlen $\equiv 1 \bmod \mathfrak{m}$,

$$\mathfrak{K}_0 = \mathfrak{k}_0 + \mathfrak{k}_1 + \cdots + \mathfrak{k}_{\nu-1}$$

die Zerlegung von $\mathfrak{K}_0$ nach S_0. Dann ist $\mathfrak{k}_i^2 = \mathfrak{k}_0$, da

115 ı

alle Klassen aus $\mathfrak{K}_0$ nur absolute Hauptideale $\equiv 1 \bmod \mathfrak{m}$ enthalten, deren Quadrate total positiv $\equiv 1 \bmod \mathfrak{m}$ sind. Wäre nun $\mathfrak{k}_i$ nicht in H enthalten, so wäre $\mathfrak{k}_i\mathsf{H} = \mathsf{H}_i$ eine von H verschiedene Klasse nach S_0 und $\mathsf{H}_i^2 = \mathsf{H}$. Der Grad der Gruppe der Nebengruppen H_i, d.h. der Index von H, □□□ wäre also entgegen der Voraussetzung gerade. Also muß H alle in $\mathfrak{K}_0$ vorkommenden Klassen $\mathfrak{k}_i$ enthalten. $\mathfrak{K}_0$ ist also Untergruppe von H. Zerlegen wir nun H in Nebengruppen nach der Untergruppe $\mathfrak{K}_0$, so sehen wir, daß H als Klassengruppe nach $\overline{S}_0$ erklärt werden kann, □□□ (da eben H dann ein Aggregat von lauter Idealklassen nach $\overline{S}_0$ wird).

Man erhält also alle Klasseneinteilungen mit ungerader Klassenzahl, wenn man die sämtlichen Klassengruppen nach dem Strahl $\overline{S}_0$ aller Zahlen $\equiv 1 \bmod \mathfrak{m}$ bildet.

Sei nun $\mathfrak{a}$ ein zu $\mathfrak{m}$ primes Ideal. Dann gibt es in einem beliebigen Strahl S nach $\mathfrak{m}$ eine durch r teilbare ganze Zahl α, sodaß $\frac{\alpha}{\mathfrak{a}}$ prim zu einem beliebig gegebenen Ideal $\mathfrak{b}$ ausfällt. Es seien nämlich $\mathfrak{q}_1, \mathfrak{q}_2, \ldots$ die verschiedenen Primideale von $\mathfrak{b}$, welche nicht in $\mathfrak{m}$ aufgehen; dann gibt es eine durch $\mathfrak{a}$ teilbare Zahl α_0, sodaß $\frac{\alpha_0}{\mathfrak{a}}$ durch kein $\mathfrak{q}_i$ teilbar ist. Nun bestimme man α aus den Kongruenzen

$$\alpha \equiv \alpha_0 \bmod [\ldots]\mathfrak{q}_1\mathfrak{q}_2\ldots; \quad \alpha \equiv 1 \bmod \mathfrak{m}$$

und wähle noch α total positiv (S. 98▶/99▶). Dann ist α sicher Strahlzahl und $\frac{\alpha}{\mathfrak{a}}$ prim zu $\mathfrak{m}$ und $\mathfrak{q}_1\mathfrak{q}_2\ldots$ also prim zu $\mathfrak{b}$.

116 ı

Nun sei α eine durch $\mathfrak{a}$ teilbare Strahlzahl und β eine durch $\mathfrak{a}$ teilbare Strahlzahl, sodaß $\frac{\beta}{\mathfrak{a}}$ prim zu $\frac{\alpha}{\mathfrak{a}}$ ist. Dann ist $\mathfrak{a} = (\alpha, \beta)$, also:

Satz 20. Jedes zu $\mathfrak{m}$ prime Ideal kann als größter gemeinsamer Teiler zweier Zahlen eines beliebigen Strahls mod $\mathfrak{m}$ dargestellt werden.

Ist $\mathfrak{a}$ irgend ein Ideal der Klasse $\mathfrak{K}^{-1}$ nach S, $\mathfrak{b}$ ein vorgegebenes Ideal. In S gibt es dann eine durch $\mathfrak{a}$ teilbare Zahl α, sodaß $\frac{\alpha}{\mathfrak{a}} = \mathfrak{c}$ prim zu $\mathfrak{b}$ wird. $\mathfrak{c}$ ist demnach Ideal aus $\mathfrak{K}$, prim zu $\mathfrak{b}$. Also:

Satz 21. In jeder Idealklasse nach S gibt es Ideale, welche prim zu einem beliebig gegebenen Ideal $\mathfrak{b}$ sind.

Wenn wir daher in den Idealklassen nach S nur die zu $\mathfrak{b}$ primen Ideale beibehalten, ändert sich die Klassenzahl und Struktur der Klassengruppe nicht. Daher werden wir zwei Idealklassen als nicht wesentlich verschieden ansehen, wenn die eine aus der anderen dadurch entsteht, daß man die zu einem gegebenen Ideal $\mathfrak{b}$ primen Ideale allein betrachtet. Das Gleiche soll für die Klassengruppen gelten. Allgemein setzen wir fest:

Definition 10. H_1 und H_2 seien zwei Klassengruppen nach den Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$. H_1 und H_2 werden als nicht wesentlich verschieden betrachtet, wenn H_1 alle zu $\mathfrak{m}_1$ primen Ideale aus H_2 und H_2 alle zu $\mathfrak{m}_2$ primen Ideale aus H_1 enthält.

117 ı

Zur Rechtfertigung dieser Definition müssen wir nachweisen:

1.) Sind H_1 und H_2, sowie H_2 und H_3 gleichbedeutend, so sind es auch H_1 und H_3

2.) Struktur und Grad der Idealklassengruppe nach H_1 und H_2 ist dieselbe.

Beweis. (Es bezeichnet allgemein $S_0^{(i)}$ den Strahl mod $\mathfrak{m}_i$ aller tot. pos. Zahlen $\equiv 1 \bmod \mathfrak{m}_i$)

1.) H_2 enthält alle zu $\mathfrak{m}_2$ primen Ideale aus H_3 und H_1 alle zu $\mathfrak{m}_1$ primen Ideale aus H_2. Also enthält H_1 alle zu $\mathfrak{m}_1\mathfrak{m}_2$ primen Ideale aus H_3. In jeder Idealklasse □□□ nach dem Strahl $S_0^{([\ldots])}$ von H_3 liegen nun zu $\mathfrak{m}_1\mathfrak{m}_2$ prime Ideale, ebenso in H_1 (Satz 21). Ist nun $\mathfrak{a}$ ein nur zu $\mathfrak{m}_1$ primes Ideal aus H_3 und ist es etwa teilbar durch den zu $\mathfrak{m}_1$ und $\mathfrak{m}_3$ primen Teiler $\mathfrak{c}$ von $\mathfrak{m}_2$, so sei $\mathfrak{K}$ die Klasse nach dem Strahl $S_0^{(1,3)}$ mod $\mathfrak{m}_1\mathfrak{m}_3$, der $\mathfrak{c}$ angehört, und in ihr $\mathfrak{d}$ ein zu $\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3$ primes Ideal. Dann ist $\frac{\mathfrak{d}}{\mathfrak{c}}$ ein Ideal der Hauptklasse nach $S_0^{([\ldots])}$, also ein Ideal aus H_3, sodaß $\mathfrak{a} \cdot \frac{\mathfrak{d}}{\mathfrak{c}}$ auch zu H_3 gehört, aber zu $\mathfrak{m}_1\mathfrak{m}_2$ prim ist, also in H_1 liegt. $\frac{\mathfrak{d}}{\mathfrak{c}}$ ist ferner Ideal der Hauptklasse nach $S_0^{(1)}$, liegt also auch in H_1.
□□□

Also liegt auch $\mathfrak{a}$ in H_1. Umgekehrt zeigt man, daß jedes zu $\mathfrak{m}_{[\ldots]}$ prime Ideal aus H_1 in H_3 liegt.

2.) Sei $\mathsf{H}_1^{(i)}$ irgend eine Klasse nach H_1. In ihr gibt es sicher ein zu $\mathfrak{m}_1\mathfrak{m}_2$ primes Ideal $\mathfrak{a}_i$. Dann ist $\mathsf{H}_1^{(i)} = \mathfrak{a}_i\mathsf{H}_1$. Der Klasse $\mathsf{H}_1^{(i)}$ ordnen wir nun die Klasse $\mathsf{H}_2^{(i)} = \mathfrak{a}_i\mathsf{H}_2$ nach H_2

118 ı

zu. Dies ist möglich, da $\mathfrak{a}_2$ prim zu $\mathfrak{m}_2$ ist. Aus $\mathfrak{a}_i\mathsf{H}_2 = \mathfrak{a}_j\mathsf{H}_2$ würde folgen, daß $\frac{\mathfrak{a}_i}{\mathfrak{a}_j}$ in H_2, also da es prim zu $\mathfrak{m}_1$ ist, auch in H_1 liegt. Es wären also auch $\mathsf{H}_1^{(i)} = \mathsf{H}_1^{(j)}$. Da nun umgekehrt auch von H_2 ausgegangen werden kann und vollständige Symmetrie besteht, sind also die Klassenzahlen in beiden Fällen dieselben und jeder Klasse $\mathsf{H}_1^{(i)}$ ist eine Klasse $\mathsf{H}_2^{(i)}$ zugeordnet. Aus

$$\begin{array}{rclcrcl} \mathsf{H}_1^{(i)} & = & \mathfrak{a}_i\mathsf{H}_1 & ; & \mathsf{H}_2^{(i)} & = & \mathfrak{a}_i\mathsf{H}_2 \\ \mathsf{H}_1^{(j)} & = & \mathfrak{a}_j\mathsf{H}_1 & ; & \mathsf{H}_2^{(j)} & = & \mathfrak{a}_j\mathsf{H}_2 \end{array}$$

folgt: $$\mathsf{H}_1^{(i)}\mathsf{H}_1^{(j)} = \mathfrak{a}_i\mathfrak{a}_j\mathsf{H}_1 = \mathfrak{a}_i\mathfrak{a}_j\mathsf{H}_2 = \mathsf{H}_2^{(i)}\mathsf{H}_2^{(j)}$$

Daraus folgt leicht die Isomorphie beider Klasseneinteilungen.
Die aufgestellte Zuordnung $\mathsf{H}_1^{(i)} \longleftrightarrow \mathsf{H}_2^{(i)}$ ist noch derart, daß dabei $\mathsf{H}_1^{(i)}$ alle zu $\mathfrak{m}_1$ primen Ideale aus $\mathsf{H}_2^{(i)}$ und $\mathsf{H}_2^{(i)}$ alle zu $\mathfrak{m}_2$ primen Ideale aus $\mathsf{H}_1^{(i)}$ enthält.

Es sei nun H eine Klassengruppe, die im Sinne der Definition 10 sowohl nach $\mathfrak{m}_1$ als auch nach $\mathfrak{m}_2$ erklärt ist. Der größte gemeinsame Teiler von $\mathfrak{m}_1$ und $\mathfrak{m}_2$ sei $\mathfrak{m}$. S_0 sei der Strahl aller total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$, $\overline{S}_0$ der Strahl bestehend aus den zu $\mathfrak{m}_1\mathfrak{m}_2$ primen Zahlen von S_0. Es sei α_0 irgendeine Zahl aus $\overline{S}_0$, also $\equiv 1 \bmod \mathfrak{m}$, total positiv, prim zu $\mathfrak{m}_1\mathfrak{m}_2$. Wir bestimmen nun α aus den Kongruenzen

$$\begin{aligned} \alpha &\equiv \alpha_0 \bmod \mathfrak{m}_1 \\ \alpha &\equiv 1 \bmod \mathfrak{m}_2\,, \end{aligned}$$

die wegen $\alpha_0 \equiv 1 \bmod (\mathfrak{m}_1, \mathfrak{m}_2)$ zu keinem Widerspruch führen, und dürfen α total positiv annehmen (S. 98▶/99▶). α ist dann sicher prim zu $\mathfrak{m}_1, \mathfrak{m}_2$. Wegen $\alpha \equiv 1 \bmod \mathfrak{m}_2$ und total positiv, ist α sicher Zahl aus H. Da nun H auch nach $\mathfrak{m}_1$ erklärbar ist und also mit einer Zahl sicher

119 ı

jede mod $\mathfrak{m}_1$ kongruente gleicher Signatur in H liegt, (da der Quotient dann total positiv $\equiv 1 \bmod \mathfrak{m}_1$ ist), □□□ liegt α_0 in H, also da α_0 eine beliebige Zahl aus $\overline{S}_0$ war, der ganze Strahl $\overline{S}_0$.

Werden nun von den Idealklassen nach S_0 nur jene beibehalten, welche Ideale aus H enthalten, so bilden diese eine Klassengruppe H_1 nach S_0 mod $\mathfrak{m}$. Sei $\mathfrak{a}$ ein zu $\mathfrak{m}_1$ primes Ideal aus H_1 und $\mathfrak{b}$ ein nach Definition von H_1 in

derselben Klasse nach S_0 vorkommendes Ideal aus H. Dann ist $\frac{\mathfrak{a}}{\mathfrak{b}}$ Ideal der Hauptklasse nach S_0, also Ideal aus S_0.

Außerdem ist $\frac{\mathfrak{a}}{\mathfrak{b}}$ prim zu $\mathfrak{m}_1$. Sollte es mit $\mathfrak{m}_2$ den zu $\mathfrak{m}_1$ (und $\mathfrak{m}$) primen Faktor $\mathfrak{c}$ enthalten, so sei $\mathfrak{d}$ ein zu $\mathfrak{m}_1\mathfrak{m}_2$ primes Ideal derselben Klasse. Dann ist $\frac{\mathfrak{a}}{\mathfrak{b}} \cdot \frac{\mathfrak{d}}{\mathfrak{c}}$ sicher Zahl aus $\overline{S}_0$, also Ideal aus H. $\frac{\mathfrak{c}}{\mathfrak{d}}$ ist prim zu $\mathfrak{m}_1$ und Zahl aus S_0. Da man sich diese Operation im engeren Klassenbereich nach $\mathfrak{m}_1$ ausgeführt denken kann, darf $\mathfrak{d}$ noch so gewählt werden, daß $\frac{\mathfrak{c}}{\mathfrak{d}}$ der Hauptklasse in H nach $\mathfrak{m}_1$ angehört. Also ist $\frac{\mathfrak{a}}{\mathfrak{b}}$ und somit auch $\mathfrak{a}$ (da ja $\mathfrak{b}$ zu H gehört) in H enthalten. Andererseits ist nach Definition von H_1 jedes Ideal aus H in H_1 enthalten. Es ist also im Sinne unserer Definition 10 H_1 nicht wesentlich von H verschieden.

Also:

Satz 22. Wenn die Klassengruppe H erklärbar ist nach den Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$, so ist sie auch erklärbar als Klassengruppe nach dem Modul $\mathfrak{m} = (\mathfrak{m}_1, \mathfrak{m}_2)$.

Ferner folgt hieraus unmittelbar:

Satz 23. Zu jeder Klassengruppe H gibt es unter allen Moduln, nach denen sie erklärbar ist, einen kleinsten, den wir den „*Führer*“ der Klassengruppe nennen. Jeder Modul nach dem H erklärbar ist, muß durch den Führer von H teilbar sein.

Beweis. *F*

Der in Definition 9 aufgestellte allgemeinste Klassenbegriff umfaßt alle früheren speziellen. Wie schon hervorgehoben, erhält man die Idealklassen nach S, wenn man als Klassengruppe die Hauptklasse nach S nimmt. Die weitaus wichtigste Klasseneinteilung ist die nach einem beliebigen Strahle S (Definition 8), darunter wieder besonders die nach dem Strahl aller Zahlen $\equiv 1 \bmod \mathfrak{m}$ mit oder ohne Vorzeichenbedingung.

Beweis. □□□

Sei $\mathfrak{m}$ der größte gemeinsame Teiler aller Moduln, nach denen H erklärbar ist. Dann ist jeder solche Modul Multiplum von $\mathfrak{m}$. (Der Modul $\mathfrak{m}$ kann auch 1 sein).

1.4 Transzendente Bestimmung der Klassenzahl. Begriff des Klassenkörpers.

121 I

Es sei im n–dimensionalen Raum ein stückweise analytisch begrenztes, beschränktes Gebiet G mit dem Volumen V gegeben. Ferner sei im Raum ein Gitter, (nicht notwendig im Ursprung beginnend) mit Würfeln der Seitenlänge δ gegeben. Mit T bezeichnen wir die Anzahl der Gitterpunkte im Inneren von G, mit T_0 die Anzahl derer, deren Würfel ganz in G liegen, mit O die Anzahl derer, deren Würfel Punkte mit der Begrenzung gemein haben.

Dann ist

$$T_0 \leqq T \leqq T_0 + O$$

Ferner gilt für das Volumen:

$$T_0\delta^n \leqq V \leqq T_0\delta^n + O\delta^n.$$

(Man hat sich jedem Gitterpunkt nach einer bestimmten Vorschrift genau einen der an ihn grenzenden Würfel zugeordnet zu denken).

Wenn nun die Begrenzung stückweise analytisch ist, kann das Volumen $O\delta^n$ abgeschätzt werden. Wir legen um jeden Begrenzungspunkt eine Kugel vom Radius der Würfeldiagonale □□□ $\delta\sqrt{n}$. Dann ist $O\delta^n$ kleiner als das Volumen des entstehenden Gebiets, und dieses kleiner als $ko\delta$, wo k eine von δ unabhängige Schranke, o die Oberfläche des Gebietes ist. Es ist also:

$$O \leqq \frac{ko}{\delta^{n-1}}$$

Wir haben also:

$$T_0\delta^n \leqq T\delta^n \leqq T_0\delta^n + O\delta^n \leqq T_0\delta^n + ko\delta$$
$$T_0\delta^n \leqq V \leqq T_0\delta^n + O\delta^n \leqq T_0\delta^n + ko\delta$$

122 I

also

$$|T\delta^n - V| \leqq ko\delta,$$

oder unter μ eine von δ abhängige Zahl verstanden,

$$\tfrac{1}{\delta} = t^{\frac{1}{n}} \qquad \boldsymbol{T = \frac{V}{\delta^n} + \frac{\mu_\delta}{\delta^{n-1}}\,;\quad (|\mu| \leqq ko)} \quad \Big| \quad T = Vt + o(\dots)$$

ko hängt dabei nur vom Körper ab. Diesen Satz haben wir jetzt bald anzuwenden. Wir stellen uns nämlich die Aufgabe, die Anzahl $T(t)$ aller ganzen durch ein Ideal $\mathfrak{a}$ teilbaren Hauptideale eines Strahles zu berechnen, deren Norm $\leqq t$ ist.

Es sei S_0 der Strahl der total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$, S_1 der Strahl aller Zahlen $\equiv 1 \bmod \mathfrak{m}$, $\mathfrak{a}$ ein zu $\mathfrak{m}$ primes ganzes Ideal[1], α eine zu $\mathfrak{m}$ prime durch $\mathfrak{a}$ teilbare ganze Zahl. Dann ist $\alpha_0 = \alpha^{2\phi(\mathfrak{m})}$ sicher eine durch $\mathfrak{a}$ teilbare, sowohl zu S_1 als auch zu S_0 gehörige Zahl. Es gibt also stets ganze Strahlzahlen (für S_0 oder S_1) α_0, die durch ein beliebiges zu $\mathfrak{m}$ primes Ideal $\mathfrak{a}$ teilbar sind. Aus einer solchen α_0 erhält man für S_1 alle, indem man irgendein ganzes Multiplum von $\mathfrak{am}$ zu α_0 addiert. In der Tat, sind α_0 und α_1 durch $\mathfrak{a}$ teilbar, ganz und in S_1 gelegen, so ist

$$1 \equiv \alpha_1 \equiv \alpha_0 \bmod \mathfrak{m}$$

also $\alpha_1 - \alpha_0 \equiv 0 \bmod \mathfrak{m}$ und $\equiv 0 \bmod \mathfrak{a}$, also $\equiv 0 \bmod \mathfrak{am}$ und ganz. Ist andererseits γ ein ganzes Multiplum von $\mathfrak{am}$ und setzt man $\alpha_1 = \alpha_0 + \gamma$ so ist α_1 ganz durch $\mathfrak{a}$ teilbar und $\equiv \alpha_0 \equiv 1 \bmod \mathfrak{m}$.

(Für S_0 erhält man aus einem durch $\mathfrak{a}$ teilbaren α_0 alle derartigen, indem man wieder irgendein Multiplum von $\mathfrak{am}$ zu α_0 addiert und nur die total positiven auswählt).

Sei nun $\varrho_1, \varrho_2, \dots, \varrho_n$ eine Basis für das Ideal $\mathfrak{am}$, und setzt man

$$y = \alpha_0 + \varrho_1 x_1 + \dots + \varrho_n x_n\,,$$

wo die x_ν alle ganzen rationalen Zahlen durchlaufen,

so durchläuft y alle ganzen Zahlen aus S_1 die durch $\mathfrak{a}$ teilbar sind. Will man nur die Zahlen aus S_0 erhalten, so muß man noch die total positiven auswählen, ($y_i > 0$ für $i = 1, 2, \dots, n_1$).

[1] In diesem Abschnitt ist $\mathfrak{m}$ optisch schwer von m zu unterscheiden, sofern nicht dasselbe gemeint ist.

Es seien jetzt die x_ν Variable, t ein positiver Parameter. Die n Körper seien in der üblichen Reihenfolge: $r_1, 2r_2$ geordnet. Wir setzen:

$$y_i = \alpha_0^{(i)} t^{-\frac{1}{n}} + \varrho_1^{(i)} x_1 + \cdots + \varrho_n^{(i)} x_n\,; \quad (i = 1, 2, \ldots, n)$$

ferner unter d_i die früher bei den Einheiten eingeführten Größen verstanden:

$$z_i = d_i \log |y_i|,$$

und wenn $\eta_1, \ldots, \eta_r$ ein System von Grundeinheiten für den Strahl S_0 oder S_1 sind,

$$\sum_{\nu=1}^{r} \xi_\nu \ell_i(\eta_\nu) + d_i \xi_{r+1} = z_i\,; \quad (i = 1, 2, \ldots, r+1).$$

Der Betrag der Determinante dieses Systems von $r+1$ linearen Gleichungen für die ξ_ν berechnet sich leicht, wenn man alle Zeilen zur letzten addiert und beachtet, daß die Summe der $(r+1)$ konjugierten Logarithmen einer Einheit verschwindet und daß $\sum_{i=1}^{r+1} d_i = n$ ist, zu

$$nR_S \neq 0,$$

wo R_S der Regulator von S_0 bezw. S_1 bezeichnet. Ferner findet man durch Addition aller Gleichungen:

$$\xi_{r+1} = \frac{1}{n} \log |y_1^{d_1} \ldots y_{r+1}^{d_{r+1}}| = \frac{1}{n} \log |y_1 \ldots y_n|.$$

Nun wollen wir für die x_ν alle Werte der Form $\dfrac{\mathfrak{m}_\nu}{\sqrt[n]{t}}$ einsetzen, wo $\mathfrak{m}_\nu$ ganz rational ist. Dann durchläuft

y_i alle Zahlen der Form $\frac{\alpha^{(i)}}{\sqrt[n]{t}}$, wo α die durch $\mathfrak{a}$ teilbaren ganzen Zahlen aus S_1 durchläuft, und wenn die Bedingung $y_i > 0$ für $i = 1, 2, \ldots, r_1$ hinzugefügt wird, nur alle durch $\mathfrak{a}$ teilbaren ganzen Zahlen aus S_0.

Für assoziierte Zahlen dieser Form ist $\frac{\alpha_1}{\alpha_2}$ eine Strahleinheit, also $z_i^{(1)} - z_i^{(2)} = d_i \log \left|\frac{\alpha_1^{(i)}}{\alpha_2^{(i)}}\right|$ von der Form $\sum_{\nu=1}^{r} \kappa_\nu \ell_i(\eta_\nu)$, (da es der konjugierte Logarithmus ℓ_i dieser Einheit ist), wo die κ_ν ganz rational sind. Die zugehörigen ξ_ν unterscheiden sich also nur um die ganzen Zahlen κ_ν (für $\nu = 1, 2, \ldots, r$), da die ξ_ν eindeutig bestimmt sind, während ξ_{r+1} ungeändert bleibt. Umgekehrt kann man jedes vorkommende α immer mit einer solchen Strahleinheit

ε multiplizieren, daß sich die zugehörigen ξ_ν $(\nu = 1, 2, \ldots, r)$ um beliebig vorgegebene ganze Zahlen κ_ν ändern, indem man $\varepsilon = \eta_1^{\kappa_1} \ldots \eta_r^{\kappa_r}$ wählt, also $\ell_i(\varepsilon) = d_i \log |\varepsilon^{(i)}| = \sum_{\nu=1}^{r} \kappa_\nu \ell_i(\eta_\nu)$. Dann wird für das neue $\overline{\alpha} = \varepsilon\alpha$:

$$\begin{aligned} \overline{z}_i - z_i = d_i \log \left| \frac{\overline{\alpha}^{(i)}}{\alpha^{(i)}} \right| &= d_i \big(\log |\varepsilon^{(i)}| \big) \\ &= \ell_i(\varepsilon) = \sum_{\nu=1}^{r} \kappa_\nu \ell_i(\eta_\nu) \end{aligned}$$

also $\quad \overline{\xi}_\nu = \xi_\nu + \kappa_\nu \,;\ (\nu = 1, 2, \ldots, r).$

Für ξ_{r+1} findet man dabei stets den invarianten Wert:

$$\xi_{r+1} = \frac{1}{n} \log \frac{|\mathsf{N}(\alpha)|}{t} \,.$$

Beschränkt man also die ξ_ν auf das Gebiet $0 \leqq \xi_\nu < 1$; $\xi_{r+1} \leqq 0$, so □□□ wird unter allen assoziierten zu α bis auf alle Strahleinheitswurzeln als Faktoren eine einzige ausgewählt, und außerdem $|\mathsf{N}(\alpha)| \leqq t$ festgesetzt. Falls man mit dem Strahl S_0 operiert, kommen noch die Bedingungen $y_i > 0$; $(i = 1, \ldots, r_1)$ hinzu.

125 ı

Läßt man also die x_ν das System aller Zahlen $\frac{\mathfrak{m}_\nu}{\sqrt[n]{t}}$ mit ganzzahligem $\mathfrak{m}_\nu$ durchlaufen und beschränkt sie dabei durch die Bedingungen

$$\begin{aligned} 0 \leqq & \xi_\nu < 1 \,;\ (\nu = 1, 2, \ldots, r); \\ & \xi_{r+1} \leqq 0 \,; \\ \text{eventuell} \qquad & y_i > 0 \,;\ (i = 1, 2, \ldots, r_1), \end{aligned}$$

so durchlaufen also die x_ν die Gitterpunkte eines bestimmten Gebietes G_t im n dimensionalen Raum mit der Gittermaschenlänge $\delta = \frac{1}{\sqrt[n]{t}}$. Jedem solchen Gitterpunkt entspricht eine durch $\mathfrak{a}$ teilbare ganze Zahl α aus S_1 bezw. S_0 mit $|\mathsf{N}(\alpha)| \leqq t$. Unter diesen durch die Gitterpunkte unseres Gebietes G_t gelieferten α kommen keine solchen vor, die sich um andere Einheitsfaktoren als um Einheitswurzeln aus S_1 bezw. S_0 unterscheiden. Ist umgekehrt $\overline{\alpha}$ eine durch $\mathfrak{a}$ teilbare ganze Zahl aus S_1 bezw. S_0 mit $|\mathsf{N}(\overline{\alpha})| \leqq t$, so entspricht ihr

zunächst eine „normierte“ α mit ebenfalls $|\mathsf{N}(\alpha)| \leqq t$, für die die aus □□□

$$y_i = \frac{\alpha^{(i)}}{\sqrt[n]{t}} \quad \square\square\square \quad ; \quad z_i = d_i \log |y_i| \qquad \text{etz. –}$$

berechneten ξ_ν unsere Bedingungen erfüllen, gleichzeitig damit alle durch Multiplikation mit jeder Einheitswurzel des Strahles hervorgehenden, für die ebenfalls die ξ_ν die Bedingungen erfüllen, aber keine durch Multiplikation mit einer anderen Einheit aus α entstehende, für die, wie aus unserer Herleitung folgt, die ξ_ν die Bedingungen nicht mehr erfüllen. Jeder solchen ganzen, durch $\mathfrak{a}$ teilbaren Zahl $\overline{\alpha}$ des Strahles mit $|\mathsf{N}(\overline{\alpha})| \leqq t$ und ihren sämtlichen assoziierten, □□□ d.h. jedem ganzen durch $\mathfrak{a}$ teilbaren Hauptideal $(\overline{\alpha})$ des Strahles, mit $\mathsf{N}[(\overline{\alpha})] \leqq t$ entsprechen also genau w_S verschiedene Gitterpunkte unseres

126 I

Gebietes G_t und umgekehrt. Daher ist die Anzahl $T(t)$ aller ganzen, durch $\mathfrak{a}$ teilbaren Hauptideale des Strahles, deren Norm $\leqq t$ ist, gleich $\frac{1}{w_S}$ mal der Anzahl der Gitterpunkte unseres Gebietes G_t mit der Gittermaschenlänge $\delta = \frac{1}{\sqrt[n]{t}}$. Es ergibt sich also aus unserer Formel S. 122▸, wenn V das Volumen des Gebietes bezeichnet, das sich von t unabhängig ergeben wird:

$$w_S T(t) = \frac{V}{\left(\frac{1}{\sqrt[n]{t}}\right)^n} + \frac{\mu_t}{\left(\frac{1}{\sqrt[n]{t}}\right)^{n-1}} = Vt + \mu_t t^{1-\frac{1}{n}}, \qquad \text{wo } |\mu_t| \leqq K_t$$

und K_t eine von der Oberfläche des Gebietes abhängige Schranke ist, die wir hier, da das Gebiet selbst von t abhängt, ebenfalls von t abhängig ansetzen müssen. Wir können aber K_t durch eine nur vom Ideal $\mathfrak{a}$ und Strahl S_1 bezw. S_0 abhängige Schranke K ersetzen, wenn wir nachweisen, daß das Gebiet G_t für $t \to \infty$ gegen ein festes Grenzgebiet G konvergiert, und zwar gleichmäßig. Dies ist nun in der Tat der Fall.

Wegen $\xi_{r+1} \leqq 0, \quad 0 \leqq \xi_\nu < 1$ sind nämlich zunächst alle z_i nach oben beschränkt, etwa $z_i < M_i$. Daraus folgt:

$$|y_i| < e^{\frac{M_i}{d_i}} \leqq e^{M_i}$$

und wenn $M = \max M_i$, gleichmäßig:

$$|y_i| < e^M.$$

Die x_ν ergeben sich durch Auflösung der n Gleichungen

$$\sum_{\nu=1}^{n} \varrho_\nu^{(i)} x_\nu = y_i - \frac{\alpha_0^{(i)}}{\sqrt[n]{t}}\,; \quad (i = 1, 2, \ldots, n)$$

als lineare Verbindungen der y_i und $\frac{\alpha_0^{(i)}}{\sqrt[n]{t}}$ mit Koeffizienten, die von der Basis des Ideals $\mathfrak{am}$ abhängen. Da die $\frac{\alpha_0^{(i)}}{\sqrt[n]{t}}$ für $t \to \infty$ gleichmäßig gegen Null gehen, sind also die $|x_\nu|$ ebenfalls unterhalb einer nur von

127 I

den Idealen $\mathfrak{a}$ und $\mathfrak{m}$ abhängigen Schranke gelegen (e^M hängt ja ebenfalls nur von den Grund Einheiten des Strahles, also von $\mathfrak{m}$ ab). Die x_ν sind also für $t \to \infty$ gleichmäßig beschränkt, so daß G_t ganz im Endlichen bleibt. G_t konvergiert □□□ ferner gleichmäßig gegen ein festes, endliches Gebiet G, das entsteht, wenn man in unseren Formeln $t = \infty$ setzt, das also durch die Gleichungen:

$$y_i = \sum_{\nu=1}^{n} \varrho_\nu^{(i)} x_\nu\,; \quad z_i = d_i \log |y_i|\,;$$

$$\sum_{\nu=1}^{r} \xi_\nu \ell_i(\eta_\nu) + d_i \xi_{r+1} = z_i$$

mit den Bedingungen:

$$\begin{aligned} 0 \leqq \xi_\nu &< 1\,; \quad (\nu = 1, 2, \ldots, r) \\ \xi_{r+1} &\leqq 0\,; \\ \text{ev.} \quad y_i &> 0 \quad (i = 1, 2, \ldots, r_1). \end{aligned}$$

bestimmt ist. Denkt man sich nämlich hier die x_ν durch die y_i ausgedrückt, so unterscheiden sich diese Werte der x_ν nur um Größen der Ordnung $\frac{1}{\sqrt[n]{t}}$ von den x_ν–Werten, die aus den Bedingungen für endliches t in gleicher Weise entstehen. Das gilt insbesondere für die Grenzen des Gebietes G und G_t, sodaß G_t also gleichmäßig gegen G konvergiert inkl. Begrenzung.

Daher dürfen wir in unserer Formel S. 126 oben die Schranke K_t durch eine von t nicht mehr abhängige, nur vom Ideal $\mathfrak{a}$ und Strahl abhängige Schranke K ersetzen:

$$w_S T(t) = Vt + \mu_t t^{1-\frac{1}{n}}; \qquad |\mu_t| \leqq K.$$

Es bleibt also zur Bestimmung von $T(t)$ nur noch die Bestimmung des Volumens V von G_t oder G, (was sich als dasselbe herausstellen wird), übrig.

128 I

Es ist:

$$V = \int_{G_t} \cdots \int dx_1 \dots dx_n \; \square\square\square$$

Wir setzen:

$$\begin{aligned} y_i &= u_i\,; \quad (i = 1, 2, \dots, r_1), \\ \left.\begin{aligned} y_{r_1+\kappa} &= u_{r_1+\kappa} e^{i\varphi_\kappa} \\ y_{r_1+r_2+\kappa} &= u_{r_1+\kappa} e^{-i\varphi_\kappa} \end{aligned}\right\}\,; &\quad (\kappa = 1, 2, \dots, r_2), \end{aligned}$$

mit den Nebenbedingungen:

$$\begin{aligned} u_{r_1+\kappa} &\geqq 0, \\ 0 \leqq \varphi_\kappa &< 2\pi. \end{aligned}$$

Dann entsprechen sich die y_i und die u_i, φ_i gegenseitig eindeutig, $\square\square\square$ also auch die x_i und u_i, φ_i. Für den *Betrag* der Funktionaldeterminante finden wir:

$$\begin{aligned} &\left|\frac{d(x_1, \dots, x_n)}{d(u_1, \dots, u_{r_1+r_2}; \varphi_1, \dots, \varphi_{r_2})}\right| \\ &= \left|\frac{d(x_1, \dots, x_n)}{d(y_1, \dots, y_n)}\right| \left|\frac{d(y_1, \dots, y_n)}{d(u, \varphi)}\right| \\ &= \left|\frac{1}{|\varrho_\nu^{(i)}|}\right| \cdot \left|\frac{d(y_1, \dots, y_n)}{d(u, \varphi)}\right| \\ &= \frac{1}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} \cdot \left|\frac{d(y_{r_1+1}, y_{r_1+r_2+1})}{d(u_{r_1+1}, \varphi_1)}\right| \cdots \left|\frac{d(y_{r_1+r_2}, y_{r_1+2r_2})}{d(u_{r_1+r_2}, \varphi_{r_2})}\right| \\ &= \frac{1}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} \cdot \left|\prod_{\nu=1}^{r_2} \begin{vmatrix} e^{i\varphi_\nu} & e^{-i\varphi_\nu} \\ iu_{r_1+\nu} e^{i\varphi_\nu} & -iu_{r_1+\nu} e^{-i\varphi_\nu} \end{vmatrix}\right| \\ &= \frac{1}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} \prod_{\nu=1}^{r_2} 2u_{r_1+\nu} = \frac{2^{r_2}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} u_{r_1+1} \dots u_{r_1+r_2} \end{aligned}$$

$\square\square\square$

(Für die Volumenbestimmung kommt es nur auf den absoluten Betrag der

Funktionaldeterminante an).

129 I

In die Grenzbedingungen gehen von den Größen $y_{r_1+1}, \ldots, y_n$ nur die absoluten Beträge ein, die φ_ν also nicht, sodaß jedes φ_ν von 0 bis 2π läuft. Wir finden demnach:

$$V = \frac{2^{r_2}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} \int_0^{2\pi} d\varphi_1 \ldots \int_0^{2\pi} d\varphi_{r_2} \int_{G_t} \cdots \int u_{r_1+1} \ldots u_{r_1+r_2} du_1 \ldots du_{r_1+r_2}$$

Schon hier sieht man, daß V unabhängig von t wird, da sich das in den Substitutionsgleichungen vorkommende t bei Bildung der Funktionaldeterminante herausgehoben hat. Es wird weiter:

$$V = \frac{2^{r_2}(2\pi)^{r_2}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} \int_{G_t} \cdots \int u_{r_1+1} \ldots u_{r_1+r_2} du_1 \ldots du_{r_1+r_2} .$$

Handelt es sich um den Strahl S_0 so ist $u_1, \ldots, u_{r_1}$ nur positiv zu nehmen, andernfalls ist zu jedem positiven Wert dieser Größen auch der entgegengesetzt gleiche möglich, da in die Grenzbedingungen nur die Beträge der $y_i = u_i$ eingehen. Spalten wir in letzterem Falle das Integral, so tritt der Faktor 2^{r_2} hinzu. Wir haben also:

$$\left.\begin{array}{rcl} \text{Für} \quad S_0 & : & V = \frac{2^{2r_2}\pi^{r_2}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} I \\ \text{Für} \quad S_1 & : & V = \frac{2^{r_1+2r_2}\pi^{r_2}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|} I \end{array}\right\}$$

, wo $I = \int_{G(u)} \cdots \int u_{r_1+1} \ldots u_{r_1+r_2} du_1 \ldots du_{r_1+r_2}$ und $G(u)$ das durch

$$\begin{gathered} u_i > 0; \quad (i = 1, 2, \ldots, r_1 + r_2) \\ 0 \leqq \xi_\nu < 1; \quad (\nu = 1, 2, \ldots, r) \\ \xi_{r+1} \leqq 0 \end{gathered}$$

bestimmte Gebiet ist (Zwischen $u_i > 0$ und $u_i \geqq 0$ ist für die Integration kein Unterschied).

Setzen wir also: $z_i = d_i \log u_i$ oder $u_i = e^{\frac{z_i}{d_i}}$ also $du_i = \frac{1}{d_i} e^{\frac{z_i}{d_i}} dz_i$, so wird:

$$du_1 \dots du_{r_1+r_2} = \frac{1}{2^{r_2}} e^{\sum_{i=1}^{r_1+r_2} dz_1 \dots dz_{r_1+r_2}}$$
$$u_{r_1+1} \dots u_{r_1+r_2} du_1 \dots du_{r_1+r_2} = 2^{-r_2} e^{z_1+\dots+z_{r+1}} dz_1 \dots dz_{r_1+r_2}$$
$$= 2^{-r_2} e^{n\xi_{r+1}} dz_1 \dots dz_{r_1+r_2}$$

da $z_1 + \dots + z_{r+1} = n\xi_{r+1}$ ist.

Die Bedingung $u_i > 0$ ist wegen $u_i = e^{\frac{z_i}{d_i}}$ und da z_i reell, von selbst erfüllt. □□□ Um schließlich auf die [...] zu kommen bilden wir

□□□ $$\left|\frac{d(z_1, \dots, z_{r+1})}{d(\xi_1, \dots, \xi_{r+1})}\right| = \left| \begin{vmatrix} \ell_i(\eta_\nu) & d_i \\ \ell_{r+1}(\eta_\nu) & d_{r+1} \end{vmatrix} \right| = nR_S$$

Also wird:

$$I = \int_{G(u)} \cdots \int 2^{-r_2} e^{n\xi_{r+1}} nR_S d\xi_1 \dots d\xi_{r+1}$$
$$= \int_0^1 d\xi_1 \dots \int_0^1 d\xi_r \int_{-\infty}^0 ne^{n\xi_{r+1}} d\xi_{r+1} \cdot 2^{-r_2} R_s$$
$$= 2^{-r_2} R_S$$

und somit das Volumen:

$$\text{Für} \quad S_0 \quad : \quad V = \frac{(2\pi)^{r_2} R_{S_0}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|},$$
$$\text{Für} \quad S_1 \quad : \quad V = \frac{2^{r_1+r_2}\pi^{r_2}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|}.$$

Daraus ergibt sich für die Anzahl $T(t)$:

$$\left.\begin{array}{lll} \text{Für} \quad S_0 & : & T(t) = \frac{(2\pi)^{r_2} R_{S_0}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|w_{S_0}} t + \mu_t t^{1-\frac{1}{n}} \\ \text{Für} \quad S_1 & : & T(t) = \frac{2^{r_1+r_2}\pi^{r_2} R_{S_1}}{\mathsf{N}(\mathfrak{am})|\sqrt{d}|w_{S_1}} t + \mu_t t^{1-\frac{1}{n}} \end{array}\right\} \; |\mu_t| \leqq K$$

Nun seien die Idealklassen nach einem dieser Strahlen definiert, $\mathfrak{K}$ eine dieser Klassen. Unter $T(t, \mathfrak{K})$ wollen wir die Anzahl der ganzen Ideale aus $\mathfrak{K}$ verstehen, deren Norm $\leqq t$ ist. Es sei $\mathfrak{a}$ ein festes, ganzes Ideal aus $\mathfrak{K}^{-1}$. Ist α eine ganze Zahl des Strahls, die durch $\mathfrak{a}$ teilbar ist, so ist $(\alpha) = \mathfrak{ab}$, wo $\mathfrak{b}$ zu $\mathfrak{K}$ gehört und umgekehrt, wenn $\mathfrak{b}$ ein ganzes Ideal aus $\mathfrak{K}$ ist, ist $\mathfrak{ab}$ eine durch $\mathfrak{a}$ teilbare ganze Strahlzahl α. Diese Beziehung ist gegenseitig eindeutig, wenn man nur die *Hauptideale* (α) des Strahles betrachtet. Wenn nun, wie verlangt, $\mathsf{N}(\mathfrak{b}) \leqq t$ ist, ist $\mathsf{N}[(\alpha)] \leqq \mathsf{N}(\mathfrak{a}) \cdot t$ und umgekehrt. Es ist also:

$$T(t, \mathfrak{K}) = T\big(t \cdot \mathsf{N}(\mathfrak{a})\big).$$

Da nun aus jeder Klasse $\mathfrak{K}^{-1}$ nur ein Ideal $\mathfrak{a}$ benutzt wird, liegen alle $\mathsf{N}(\mathfrak{a})$ unter einer festen Schranke. Also ist:

$$\text{Für} \quad S_0 \quad : \quad T(t, \mathfrak{K}) = \frac{(2\pi)^{r_2} R_{S_0}}{\mathsf{N}(\mathfrak{m})|\sqrt{d}|w_{S_0}} t + \mu(t, \mathfrak{K}) t^{1-\frac{1}{n}},$$

$$\text{Für} \quad S_1 \quad : \quad T(t, \mathfrak{K}) = \frac{2^{r_1+r_2}\pi^{r_2} R_{S_1}}{\mathsf{N}(\mathfrak{m})|\sqrt{d}|w_{S_1}} t + \mu(t, \mathfrak{K}) t^{1-\frac{1}{n}},$$

wo $\mu(t, \mathfrak{K})$ unter einer nur vom Strahl abhängigen festen Schranke liegt.

Nun führen wir die „ζ–*Funktion der Klasse* $\mathfrak{K}$“ ein:

$$\zeta(s, \mathfrak{K}) = \sum_{\mathfrak{a}|\mathfrak{K}} \frac{1}{\mathsf{N}(\mathfrak{a})^s} \qquad \text{über alle ganzen } \mathfrak{a} \text{ aus } \mathfrak{K}.$$

Wir ordnen nach der Größe der Idealnormen. Es gibt in $\mathfrak{K}$ genau $T(\nu, \mathfrak{K}) - T(\nu - 1, \mathfrak{K})$ Ideale der Norm ν, wo ν eine ganze, positive Zahl bedeutet.

132 I

Also wird:

$$\zeta(s, \mathfrak{K}) = \sum_{\nu=1}^{\infty} \frac{T(\nu, \mathfrak{K}) - T(\nu - 1, \mathfrak{K})}{\nu^s}.$$

Wir setzen zur Abkürzung

$$T(\nu, \mathfrak{K}) = g \cdot \nu + \mu(\nu) \nu^{1-\frac{1}{n}}$$

wo g die Bedeutung:

$$\text{Für} \quad S_0 \quad : \quad g_{S_0} = \frac{(2\pi)^{r_2} R_{S_0}}{\mathsf{N}(\mathfrak{m})|\sqrt{d}|w_{S_0}}$$

$$\text{Für} \quad S_1 \quad : \quad g_{S_1} = \frac{2^{r_1+r_2}\pi^{r_2} R_{S_1}}{\mathsf{N}(\mathfrak{m})|\sqrt{d}|w_{S_1}}$$

hat, und $|\mu(\nu)| \leqq \mathsf{A}$, wo A nur vom Strahl abhängt, ist.

Bedeutet $\zeta(s)$ die Riemannsche ζ–Funktion:

$$\zeta(s) = \sum_{\nu=1}^{\infty} \frac{1}{\nu^s} \quad \text{abs. konv. für } \sigma > 1;\ (s = \sigma + it),$$

so ist bekanntlich

$$\zeta(1) = \frac{1}{s-1} + f(s),$$

wo $f(s)$ eine ganze Funktion ist. Setzen wir also:

$$\phi(s) = \zeta(s, \mathfrak{K}) - g\zeta(s)$$

so ist

$$\phi(s) = \sum_{\nu=1}^{\infty} \frac{\mu(\nu)\nu^{1-\frac{1}{n}} - \mu(\nu-1)\cdot(\nu-1)^{1-\frac{1}{n}}}{\nu^s}\,.$$

Die Summe der ersten m Koeffizienten der Dirichletschen Reihe rechts ist absolut kleiner als $\mathsf{B}m^{1-\frac{1}{n}}$, die Reihe also für $\sigma > 1 - \frac{1}{n}$ konvergent. $\phi(s)$ stellt also rechts von $\sigma = 1 - \frac{1}{n}$ eine reguläre Funktion dar. Da $\zeta(s)$ für $\sigma > 1$ konvergiert, konvergiert dort auch $\zeta(s, \mathfrak{K})$ und da jedes Glied für reelle s positiv ist, absolut. Ferner gilt nach unseren Resultaten:

$$\zeta(s, \mathfrak{K}) = \frac{g}{s-1} + \varphi(s, \mathfrak{K})$$

wo $\varphi(s, \mathfrak{K})$ für $\sigma > 1 - \frac{1}{n}$ regulär ist. $\zeta(s, \mathfrak{K})$ hat also in $s = 1$ einen Pol erster Ordnung mit dem Residuum g.

Zunächst wenden wir dieses Ergebnis zur Bestimmung der absoluten Klassenzahl h an. Wir wählen also $m = 1$ und den Strahl S_1, d.h. den Strahl aller von Null verschiedenen Körperzahlen. Für ihn ist

$$g = \frac{2^{r+1}\pi^{r_2}R}{|\sqrt{d}|w}\,,$$

wo R den Regulator und w die Anzahl der Einheitswurzeln des Körpers bezeichnet. Ferner führen wir die *Dedekindsche ζ–Funktion*:

$$\zeta(s) = \sum_{\mathfrak{a}} \frac{1}{\mathsf{N}(\mathfrak{a})^s} \qquad \text{über alle ganzen } \mathfrak{a} \text{ aus } k$$

ein. (Eine Verwechslung mit der gleichbezeichneten Riemannschen ζ–Funktion wird, wenn nötig durch die Bezeichnung $\zeta_k(s)$ für die Dedekindsche verhütet).

Es gilt:

$$\zeta(s) = \sum_{\mathfrak{K}} \zeta(s, \mathfrak{K})$$

erstreckt über alle Idealklassen $\mathfrak{K}$, sodaß $\zeta(s)$ ebenfalls für $\sigma > 1$ □□□ absolut konvergiert. Ferner ergibt sich:

$$\zeta(s) = \frac{gh}{s-1} + \varphi(s),$$

wo $\varphi(s)$ für $\sigma > 1 - \frac{1}{n}$ regulär ist. In $s = 1$ hat also $\zeta(s)$ einen Pol erster Ordnung mit dem Residuum gh. Für die Klassenzahl finden wir also:

$$\boldsymbol{h = \frac{w}{R} \frac{|\sqrt{d}|}{2^{r+1}\pi^{r_2}} \lim_{s=1}(s-1)\zeta(s).}$$

Nun kehren wir wieder zum Allgemeinen zurück. Die Bedeutung von $\zeta(s, \mathfrak{K})$ liegt darin, daß

$$\zeta(s, \mathfrak{K}) = \frac{g}{s-1} + \varphi(s, \mathfrak{K})$$

ist, wo g nicht von $\mathfrak{K}$ abhängt. Dies läßt sich nun unmittelbar auf den allgemeinsten Klassenbegriff verallgemeinern.

Es seien die Idealklassen nach irgendeiner Klassengruppe H mod $\mathfrak{m}$ erklärt. Wir nennen diese Klassen $\mathfrak{K}$. Da man alle Klassengruppen sicher durch den Strahl S_0 erhält, definieren wir außerdem die Idealklassen nach S_0 und nennen sie $\mathfrak{k}$. Jede □□□ Klasse $\mathfrak{K}$ zerfällt dann in die gleiche Anzahl d von Klassen $\mathfrak{k}$:

$$\mathfrak{K} = \mathfrak{k}_{\mathfrak{K}} + \mathfrak{k}'_{\mathfrak{K}} + \cdots + \mathfrak{k}^{(d-1)}_{\mathfrak{K}} .$$

Führen wir also die ζ–Funktion der Klasse $\mathfrak{K}$ ein:

$$\zeta(s, \mathfrak{K}) = \sum_{\mathfrak{a}|\mathfrak{K}} \frac{1}{\mathsf{N}(\mathfrak{a})^s} ,$$

so ist

$$\zeta(s,\mathfrak{K}) = \zeta(s,\mathfrak{k}_{\mathfrak{K}}) + \cdots + \zeta(s,\mathfrak{k}_{\mathfrak{K}}^{(d-1)}).$$

Da nun $\zeta(s,\mathfrak{k}) = \frac{g_0}{s-1} + \varphi(s,\mathfrak{k})$ ist, wo g_0 von $\mathfrak{k}$ nicht abhängt, und $\varphi(s,\mathfrak{k})$ für $\sigma > 1 - \frac{1}{n}$ regulär ist, haben wir, wenn $g = dg_0$ gesetzt wird:

Satz 1. Ist H eine Klassengruppe und $\mathfrak{K}$ eine Idealklasse nach H mod $\mathfrak{m}$, so gilt:

$$\zeta(s,\mathfrak{k}) = \frac{g}{s-1} + \varphi(s,\mathfrak{K}),$$

wo g von der Klasse $\mathfrak{K}$ nicht abhängt, und $\varphi(s,\mathfrak{K})$ für $\sigma > 1 - \frac{1}{n}$ regulär ist.

Die Klassen nach H bilden eine Abelsche Gruppe. h sei ihr Grad, dann besitzt diese Gruppe genau h Charaktere: $\chi_i(\mathfrak{K})$; $(i = 1, 2, \ldots, h)$, die entstehen, wenn man an Stelle der Basiselemente der Abelschen Gruppe irgendwelche Einheitswurzeln der gleichen Grade setzt, und die Exponenten der Darstellung von $\mathfrak{K}$ anbringt. Wir ordnen nun jedem Ideal aus $\mathfrak{K}$ den Charakter seiner Klasse zu: $\chi_i(\mathfrak{a}) = \chi_i(\mathfrak{K})$. Dann ist jedem Ideal (wir beschränken uns auf die ganzen) der gleichen Klasse auch für jedes i der gleiche Charakterenwert χ_i zugeordnet. Ist $\mathfrak{a}_1$ aus $\mathfrak{K}_1$, $\mathfrak{a}_2$ aus $\mathfrak{K}_2$, so ist $\mathfrak{a}_1\mathfrak{a}_2$ aus $\mathfrak{K}_1\mathfrak{K}_2$. Also gilt wegen der Eigenschaft der Charaktere:

$$\chi_i(\mathfrak{a}_1\mathfrak{a}_2) = \chi_i(\mathfrak{a}_1)\chi_i(\mathfrak{a}_2)$$

Da wir die Idealklassen nach $\mathfrak{m}$ definieren, ist natürlich so nur den zu $\mathfrak{m}$ primen Idealen ein Charakter zugeordnet. Wir nennen diese Charaktere „*Klassencharaktere nach* H“.

Definition 1. Ist χ_i ein Klassencharakter nach H mod $\mathfrak{m}$, so verstehen wir unter der ihm *zugeordneten L–Reihe* die Reihe:

$$L(s,\chi_i) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\chi_i(\mathfrak{a})}{\mathsf{N}(\mathfrak{a})^s} = \sum_{\mathfrak{K}} \chi_i(\mathfrak{K})\zeta(s,\mathfrak{K})$$

wo die erste Summe über alle zu $\mathfrak{m}$ primen Ideale, die zweite über alle Klassen nach H mod $\mathfrak{m}$ zu erstrecken ist.

Die Richtigkeit der hingeschriebenen Formel ist ohne weiteres klar. Aus ihr folgt unmittelbar, daß $L(s,\chi_i)$ für $\sigma > 1$

136 ı

absolut konvergent ist. Für die Charaktere $\chi_i(\mathfrak{K})$ gilt bekanntlich:

$$\sum_{\mathfrak{K}} \chi_i(\mathfrak{K}) = \begin{cases} h & \text{für den Hauptcharakter } \chi_1, \\ 0 & \text{für alle anderen } \chi_i. \end{cases}$$

Daraus folgt nach Satz 1:

Satz 2. Für den Hauptcharakter $\chi_1 = +1$ gilt:

$$L(s, \chi_1) = \frac{gh}{s-1} + \varphi(s)\,; \quad \varphi(s) \text{ regulär für } \sigma > 1 - \frac{1}{n}$$

für jeden anderen Charakter ist $L(s, \chi_i)$ selbst regulär für $\sigma > 1 - \frac{1}{n}$. Insbesondere hat also $L(1, \chi_i)$ einen endlichen Wert (der möglicherweise Null sein könnte).

Da sich jedes Ideal eindeutig in Primideale zerlegen läßt, beweist man leicht, wie bei der Riemannschen ζ–Funktion:

Satz 3. Für $\sigma > 1$ gilt für jeden Charakter

$$L(s, \chi_i) = \prod_{(\mathfrak{p},\mathfrak{m})=1} \frac{1}{1 - \frac{\chi_i(\mathfrak{p})}{\mathsf{N}(\mathfrak{p})^s}}$$

ebenso für die Dedekind'sche Zetafunktion:

$$\zeta(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathsf{N}(\mathfrak{p})^s}}$$

Die Produkte konvergieren absolut für $\sigma > 1$. Daher haben $\zeta(s)$ und $L(s, \chi_i)$ in der Halbebene $\sigma > 1$ keine Nullstelle.

□□□

137 ı

□□□

Aus der letzten Bemerkung folgern wir sofort, daß wir für $\sigma > 1$ die Funktionen $\log L(s, \chi)$ und $\log \zeta(s)$ eindeutig dadurch erklären können, daß sie in einem bestimmten Punkte dieses Gebietes einen ganz bestimmten Zweig des Logarithmus bedeuten. Dadurch ist dann wegen des Nichtverschwindens für $\sigma > 1$ eine eindeutige Erklärung auch für jeden Punkt der rechten Halbebene

gegeben. Wir wählen den Punkt $s = +\infty$ der reellen Achse und setzen fest, daß dort $\log L(s,\chi)$ und $\log \zeta(s)$ die Hauptwerte des log haben sollen. Dann gilt:

$$\log L(s,\chi) = \sum_{(\mathfrak{p},\mathfrak{m})=1} -\log\left(1 - \frac{\chi_i(\mathfrak{p})}{\mathsf{N}(\mathfrak{p})^s}\right)$$
$$\log \zeta(s) = \sum_{\mathfrak{p}} -\log\left(1 - \frac{1}{\mathsf{N}(\mathfrak{p})^s}\right)$$

unter log rechts den Wert verstanden der in $s = +\infty$ Hauptwert ist. Denn für $s = +\infty$ sind die Hauptwerte rechts alle Null, also hat auch die linke Seite den Hauptwert. Aus

$$-\log\left(1 - \frac{\chi_i(\mathfrak{p})}{\mathsf{N}(\mathfrak{p})^s}\right) = \sum_{m=1}^{\infty} \frac{\chi_i(\mathfrak{p}^m)}{m\mathsf{N}(\mathfrak{p}^m)^s}$$

und nach dem Weyerstrassschen Doppelreihensatz folgt dann:

Definition 2. Durch die Reihen:

$$\log L(s,\chi_i) = \sum_{\mathfrak{p},m} \frac{\chi_i(\mathfrak{p}^m)}{m\mathsf{N}(\mathfrak{p})^{ms}}\,; \quad (\mathfrak{p},m) = 1$$

ist eindeutig ein bestimmter Wert von $\operatorname{Log} L(s,\chi_i)$ für $\sigma > 1$ definiert. Die Reihen konvergieren dort absolut. Ebenso ist durch:

$$\log \zeta(s) = \sum_{\mathfrak{p},m} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}}$$

ein eindeutig bestimmter Wert von $\operatorname{Log} \zeta(s)$ für $\sigma > 1$ erklärt und die Reihe dort absolut konverg.

Wir bilden jetzt das Produkt aller L–Reihen $L(s,\chi_i)$ für $i = 1, 2, \ldots, h$. Für den Logarithmus ergibt sich:

□□□ $$\sum_{i=1}^{h} \log L(s,\chi_i) = 2\mathfrak{k}_1\pi i + \log \prod_{i=1}^{h} L(s,\chi_i)$$

da ein Vielfaches von $2\pi i$ unbestimmt bleibt. Demnach ist

$$\log\prod_{i=1}^{h} L(s,\chi_i) + 2\mathfrak{k}_1\pi i = \sum_{i=1}^{h}\sum_{\mathfrak{p},\mathfrak{m}} \frac{\chi_i(\mathfrak{p}^m)}{m\mathsf{N}(\mathfrak{p})^{ms}}$$

$$= \sum_{m=1}^{\infty} \sum_{\substack{(\mathfrak{p},\mathfrak{m})=1 \\ \mathfrak{p}^m \text{ zur Hauptklasse } \mathsf{H}}} \frac{h}{m\mathsf{N}(\mathfrak{p}^m)^s} = h \sum_{\mathfrak{p}^m \text{ aus } \mathsf{H}} \frac{1}{m\mathsf{N}(\mathfrak{p}^m)^s}$$

da $\sum_{i=1}^{h} \chi_i(\mathfrak{a}) = \begin{cases} h & \text{wenn } \mathfrak{a} \text{ in der Hauptklasse } \mathsf{H} \\ 0 & \text{wenn } \mathfrak{a} \text{ nicht in } \mathsf{H}. \end{cases}$

Der rechts stehende Wert ist für reelle s positiv reell, das Produkt links ebenfalls, da mit jedem komplexen χ_i das konjugiert komplexe $\overline{\chi}_i = \chi_i$ auftritt und die reellen $L(s,\chi)$ positiv sind für $s \to \infty$ also überhaupt. Also ist $\mathfrak{k}_1 = 0$ zu setzen,

139 I

wenn links der für reelles positives Argument reelle Wert des log verstanden wird:

$$\log\prod_{i=1}^{h} L(s,\chi_i) = h \sum_{\mathfrak{p}^m \text{ aus } \mathsf{H}} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}}$$

Nun sind $(s-1)L(s,\chi_1)$ und $L(s,\chi_i)\,;\ (i=2,\ldots,h)$ für $\sigma > 1 - \frac{1}{n}$ regulär. Wir schreiben dementsprechend

$$\log\left[(s-1)L(s,\chi_1)\cdot L(s,\chi_2)\cdots L(s,\chi_h)\right] = \log(s-1) + h \sum_{\mathfrak{p}^m \text{ aus } \mathsf{H}} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}}$$

Für reelle $s > 1$ ist das Produkt links positiv, und für $\sigma > 1 - \frac{1}{n}$ regulär. Ist es für $s = 1$ von Null verschieden, so bleibt die linke Seite endlich, wenn $s \to 1$, ist es aber für $s = 1$ Null, so strebt die linke Seite bei Annäherung von s an 1 von rechts her zu $-\infty$. Demnach gilt jedenfalls

$$\sum_{\mathfrak{p}^m \text{ aus } \mathsf{H}} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}} = \frac{1}{h}\log\frac{1}{s-1} + \psi(s)$$

wo $\psi(s)$ entweder für $s \to 1$ einen endlichen limes hat, oder unter einer festen positiven Schranke bleibt.

Nun ist

$$\sum_{\mathfrak{p}^m \text{ aus } \mathsf{H}} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p} \text{ aus } \mathsf{H}} \frac{1}{\mathsf{N}(\mathfrak{p})^{s}} + \sum_{\substack{\mathfrak{p}^m \text{ aus } \mathsf{H} \\ m \geqq 2}} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}}$$

Für reelles s ist:

$$\sum_{\substack{m \geqq 2 \\ \mathfrak{p}^m \text{ aus } \mathsf{H}}} \frac{1}{m\mathsf{N}(\mathfrak{p})^{ms}} < \sum_{\mathfrak{a}} \frac{1}{\mathsf{N}(\mathfrak{a})^{2s}}$$

und da diese Reihe für $\sigma > \frac{1}{2}$ konvergiert, ist sie bei $s = 1$ regulär. Also ergibt sich:

140 I

Satz 4. Sei H eine Klassengruppe, h die Klassenzahl nach H. $\mathfrak{p}$ bedeute jedes Primideal aus H. Dann gilt für $\sigma > 1$

$$\sum_{\mathfrak{p}|\mathsf{H}} \frac{1}{\mathsf{N}(\mathfrak{p})^{s}} = \frac{1}{h} \log \frac{1}{s-1} + \varphi(s)$$

wo $\varphi(s)$ für reelles $s \to 1$ unterhalb einer endlichen positiven Schranke bleibt, möglicherweise nach $-\infty$ strebt.

Greifen wir in dieser Summe die Primideale von höherem als 1. Grad heraus, deren Norm also mindestens p^2 ist, und beachten wir, daß zu jeder Primzahl p höchstens n Primideale gehören, so hat die zugehörige Summe die Majorante

$$n \sum_{p} \frac{1}{p^{2s}}$$

die für $s > \frac{1}{2}$ konvergent ist, in $s = 1$ also endlich bleibt.
Wir schließen also

Satz 5. Die Aussage in Satz 4 bleibt bestehen, wenn man unter $\sum_{\mathfrak{p}}$ nur die Primideale ersten Grades aus der Klassengruppe H versteht.

Den Sätzen 4 und 5 haben wir Sätze über relativ Galoissche Körper, analoger Art an die Seite zu stellen.

Es sei K ein relativ–Galois'scher Körper über k. $\mathfrak{P}$ die Primideale in K, $\mathfrak{p}$ die in k. Für jedes $\mathfrak{p}$ gilt eine Zerlegung:

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_e)^g; \quad \mathfrak{P}_i \text{ vom Grad } f; \quad efg = n$$

wenn n der Relativgrad von K. □□□

141 ı

□□□

Es ist dann $\mathsf{N}_K(\mathfrak{P}_i) = \mathsf{N}(\mathfrak{p})^f$ wenn N_K die Norm in K bezeichnet. Ist also $\zeta(s)$ die ζ–Funktion in K, so ist

$$\log \zeta(s) = \sum_{\mathfrak{P},m} \frac{1}{m\mathsf{N}_K(\mathfrak{P})^{ms}} = \sum_{\mathfrak{p},m} \frac{e}{m\mathsf{N}(\mathfrak{p})^{mfs}}$$

Solange nun $f \geqq 2$ ist, läßt sich wie vorhin eine Majorante angeben, die für $s \geqq \frac{1}{2}$ konvergent ist. Wenn aber $f = 1$ ist, und wir von den endlich vielen in der Relativdiskriminante aufgehenden Primidealen absehen, ist $e = n$. Ebenso kann man für unsere Summe bei $m \geqq 2$ eine Majorante angeben. Andererseits ist $(s-1)\zeta(s)$ regulär in $s = 1$. Es ist also:

$$\log \zeta(s) = \log \frac{1}{s-1} + \psi(s)$$

wo $\psi(s)$ für $s = 1$ endlich bleibt. Daraus folgt insgesamt:

Satz 6. Wenn K ein relativ–Galoisscher Körper über k vom Relativgrad n ist und $\mathfrak{p}$ alle Primideale aus k durchläuft, die in K in lauter lauter verschiedene Primideale ersten Relativgrades zerfallen, so gilt für $s > 1$:

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{n} \log \frac{1}{s-1} + \psi(s)$$

wo $\psi(s)$ für $s = 1$ endlich ist. Aus demselben Grunde bleibt der Satz richtig, wenn $\mathfrak{p}$ nur alle Primideale *ersten Grades aus* k mit der genannten Eigenschaft durchläuft.

142 ı

Nun haben wir einige weitere Begriffe einzuführen. Es sei K wieder relativ–Galoisscher Körper vom Relativgrad n. Die Idealklassen in k seien nach dem Modul m und dem Strahl S_0 der total positiven Zahlen $\equiv 1 \bmod m$ erklärt. Die Gesamtheit der Idealklassen in k welche Relativnormen der Ideale des Oberkörpers K enthalten, bilden offenbar eine Klassengruppe H. Denn enthält $\mathfrak{k}_1$ die Relativnorm $n(\mathfrak{A}_1)$, $\mathfrak{k}_2$ die Relativnorm $n(\mathfrak{A}_2)$ so enthält $\mathfrak{k}_1\mathfrak{k}_2$ die Relativnorm $n(\mathfrak{A}_1\mathfrak{A}_2)$.

Definition 3. Die Klassengruppe H welche alle und nur die Klassen aus k enthält, in denen Relativnormen von Idealen aus K liegen, und der Galoissche Relativkörper K heißen einander zugeordnet.

Satz 7. Der Relativgrad n des relativ Galoisschen Körpers K ist nie kleiner als die Anzahl h der Idealklassen nach der zugeordneten Klassengruppe H (Index der Klassengruppe).

Beweis. Nach Satz 4 gilt, wenn $\mathfrak{p}$ die Primideale aus H durchläuft:

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + \varphi(s); \quad \big(\varphi(s) \leqq M\big) \text{ (für } s \to 1)$$

(Der Index h ist, wie auf S. 113 gezeigt, allein durch H bestimmt, von der Strahlklassenzahl unabhängig). Nach Satz 6 ist, wenn $\mathfrak{p}_1$ die Primideale aus k durchläuft, die in K in lauter Primideale ersten Grades zerfallen

$$\sum_{\mathfrak{p}_1} \frac{1}{\mathsf{N}(\mathfrak{p}_1)^s} = \frac{1}{n} \log \frac{1}{s-1} + \psi(s)\,; \quad (\psi(s) \text{ endlich für } s \to 1)$$

Wenn nun $\mathfrak{p}_1$ in Primideale ersten Grades zerfällt,

ist $\mathfrak{p}_1$ Relativnorm eines Primideals aus K, also in H enthalten. Es ist also

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} - \sum_{\mathfrak{p}_1} \frac{1}{\mathsf{N}(\mathfrak{p}_1)^s} \geqq 0$$

oder

$$\left(\frac{1}{h} - \frac{1}{n}\right) \log \frac{1}{s-1} + \big[\varphi(s) - \psi(s)\big] \geqq 0$$

Dabei bleibt auch $\varphi(s) - \psi(s)$ unter einer endlichen, positiven Schranke. Da $\log \frac{1}{s-1}$ positiv unendlich wird, wenn $s \to$ von rechts, folgt, daß $\frac{1}{h} - \frac{1}{n}$ nicht negativ sein kann. Daher ist $n \geqq h$ w.z.b.w.

Für spätere Zwecke benötigen wir noch den

Satz 8. Es sei H irgendeine Klassengruppe, K irgendein relativ Galoisscher Körper über k. Der Index h von H sei > 2. Dann gibt es unendlich viele Primideale ersten Grades in k, die weder zu H gehören, noch in K in lauter Primideale ersten Grades zerfallen.

Beweis. Liegt $\mathfrak{p}$ in H, so ist

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + \varphi(s); \quad (\varphi(s) \leqq M \text{ für } s \to 1)$$

Andererseits folgt aus Definition 2 leicht, daß

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \log \frac{1}{s-1} + \mathfrak{f}(s); \qquad (\mathfrak{f}(s) \text{ endlich für } s \to 1)$$

wenn $\mathfrak{p}$ alle Primideale ersten Grades durchläuft. Durch Subtraktion findet man,

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{h-1}{h} \log \frac{1}{s-1} + \phi(s)$$

wenn $\mathfrak{p}$ jetzt alle Primideale ersten Grades bedeutet, die nicht in H liegen, und $\phi(s)$ für $s \to 1$ endlich bleibt oder gegen $+\infty$ strebt.

Andererseits ist, wenn $\mathfrak{p}_1$ alle Primideale ersten Grades in k, die in K in lauter Primideale ersten Relativgrades zerfallen, bedeutet, nach Satz 6:

$$\sum_{\mathfrak{p}_1} \frac{1}{\mathsf{N}(\mathfrak{p}_1)^s} = \frac{1}{n} \log \frac{1}{s-1} + \psi(s); \quad (\psi(s) \text{ endlich für } s \to 1)$$

Für $h > 2$ ist nun $\frac{h-1}{h} > \frac{1}{n}$. Es muß also unendlich viele Primideale $\mathfrak{p}$ geben, die nicht $\mathfrak{p}_1$ sind, w.z.b.w.

Definition 4. Ist der Relativgrad n eines relativ–Galoisschen Körpers K *gleich* dem Index h der zugeordneten Klassengruppe, so heißt K ein *Klassenkörper* von k für die Klassengruppe H.

Satz 9. Seien H und H' Klassengruppen in k, K und K' Klassenkörper für H und H' von den Relativgraden h und h'. Ist H' Untergruppe von H so ist K' Oberkörper von K.

Beweis. Sei $K^\star$ der aus K und K' komponierte Körper vom Grade $n^\star$. Dann ist auch $K^\star$ relativ Galoissch. Ein Primideal $\mathfrak{p}$ das in K und K' in lauter Primideale ersten Grades zerfällt, zerfällt auch in $K^\star$ in Primideale ersten Grades. Denn ist $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in $K^\star$, $\mathfrak{G}_Z$ seine Zerlegungsgruppe,

so ist nach Satz 13 (S. 37) angewendet auf K, da $\mathfrak{p}$ in K in Primideale ersten Grades zerfällt, $f'_\nu = 1$, also $f = f_\nu$. Da $e = e_\nu = 1$ ist (die Relativdiskriminante von $K^\star$ enthält nur die in der Relativdiskriminante von K und K' aufgehenden Primideale, die nicht in lauter verschiedene Primideale 1. Grades zerfallen), ist f der Grad der Zerlegungsgruppe von $K^\star$ in Bezug auf K und k. Die Gruppe zu der K gehört, hat also $\mathfrak{G}_Z$ als Untergruppe, der Zerlegungskörper enthält also K, ebenso K'. Er enthält also auch $K^\star$ und

145 I

Seite nicht vorhanden

146 I

ist somit mit $K^\star$ identisch. Da aber im Zerlegungskörper das zugehörige Primideal vom 1. Relativgrad in Bezug auf k ist, ist $f = 1$. Zerfällt umgekehrt $\mathfrak{p}$ in $K^\star$ in Primideale ersten Grades, dann auch in K und K' (Satz 13, S. 32).

Bilden wir also die Summen $\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = S_\nu$ und zwar bei S_1 über die Primideale, die sowohl in K als K' in Primideale ersten Grades zerfallen, bei S_2 die zwar in K nicht in K' und bei S_3 umgekehrt, so sind die in Satz 6 auftretenden Summen für die Körper $K^\star, K, K'$ gerade

$$S_1;\ S_1 + S_2;\ S_1 + S_3$$

Satz 6 ergibt also, wenn die Funktionen $F_i(s)$ für $s = 1$ endlich bleiben:

$$\begin{aligned} S_1 &= \frac{1}{n^\star} \log \frac{1}{s-1} + F_1(s) \\ S_1 + S_2 &= \frac{1}{h} \log \frac{1}{s-1} + F_2(s) \\ S_1 + S_3 &= \frac{1}{h'} \log \frac{1}{s-1} + F_3(s) \end{aligned}$$

also:

$$S_1 + S_2 + S_3 = \left(\frac{1}{h} + \frac{1}{h'} - \frac{1}{n^\star} \right) \log \frac{1}{s-1} + F_4(s).$$

H enthält alle Primideale, die in K in Primideale ersten Grades zerfallen, da sie dann als Relativnormen auftreten. Da H' Untergruppe von H ist, enthält H auch die in K' zerfallenden Primideale, also alle 3 Kategorien. Satz 4 liefert

$$\sum \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + \varphi(s); \quad (\varphi(s) \leqq M \text{ für } s \to 1),$$

wenn $\mathfrak{p}$ die Primideale aus H durchläuft. Nach dem Gesagten ist also

$$\sum_{\mathfrak{p} \text{ in } \mathsf{H}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} \geqq S_1 + S_2 + S_3$$

also

$$\left(\frac{1}{n^\star} - \frac{1}{h'}\right) \log \frac{1}{s-1} + \varphi(s) - F_4(s) \geqq 0$$

Dies geht nur, wenn $\frac{1}{n^\star} - \frac{1}{h'} \geqq 0$ ist, also $h' \geqq n^\star$. Als Oberkörper von K' ist aber der Grad $n^\star$ von $K^\star$ sicher $\geqq h'$, also $h' = n^\star$, $K^\star = K'$, d.h. K ist Unterkörper von K' w.z.b.w.

Daraus folgt unmittelbar:

Satz 10. Zu einer Klassengruppe H kann es höchstens einen Klassenkörper geben.

□□□

Denn gehört K zu H und K' zu H als Klassenkörper, so muß K' Unterkörper von K und umgekehrt sein, also $K' = K$.

Wir bemerken noch, daß die Schlüsse des letzten Beweises richtig bleiben, wenn man voraussetzt, daß die in K bezw. K' in zerfallenden Primideale ersten Grades zerfallenden Primideale aus k bis auf endlich viele Ausnahmen in H und H' enthalten sind. Dies zeigt uns sofort, daß der Klassenkörper auch unabhängig davon ist, nach welchem Modul im Sinne von Definition 10 (S. 116▸) die Klassengruppe definiert ist.

Satz 11. Zu einer Klassengruppe H gibt es (wenn überhaupt) nur einen Klassenkörper, nach welchem Modul $\mathfrak{m}$ auch H definiert ist.

1.5 Die Geschlechter im relativ zyklischen Körper von Primzahlgrad ℓ.

148 I

a) Allgemeine Sätze

Satz 1. Ist K relativ zyklisch von Primzahl*potenz*grad ℓ^ν zu k und geht ein zu ℓ primes Primideal $\mathfrak{p}$ des Grundkörpers k in der Relativdiskriminante des in K enthaltenen relativ zyklischen Körpers vom Grade ℓ in Bezug auf k auf, so ist die Relativdiskriminante von K nach k genau durch die $(\ell^\nu - 1)$–te Potenz von $\mathfrak{p}$ teilbar. Ferner gilt:

$$\mathsf{N}(\mathfrak{p}) \equiv 1 \bmod \ell^\nu,$$

und die Zerlegung $\mathfrak{p} = \mathfrak{P}^{\ell^\nu}$

Beweis. 1.) Jeder Unterkörper von K, Oberkörper von k ist eindeutig durch seine Relativgruppe bestimmt. Die zyklische Gruppe vom Grad ℓ^ν hat nun nur eine Untergruppe vom Grade ℓ, nämlich die zyklische. Daher kann es auch nur einen solchen „Zwischenkörper“ K_ℓ vom Grade ℓ zwischen K und k geben.

2.) □□□ Geht $\mathfrak{p}$ in der Relativdiskriminante von K_ℓ auf, so zerfällt es in K_ℓ in der allgemeinen Form:

$$\mathfrak{p} = (\overline{\mathfrak{P}}_1 \dots \overline{\mathfrak{P}}_g)^e; \quad \mathfrak{P}_i \text{ vom Rel. Gr. } f$$
$$efg = \ell$$

und es ist $e \geqq 2$ (Satz 3, S. 10▸). Daher muß $e = \ell$, $f = g = 1$ also

$$\mathfrak{p} = \overline{\mathfrak{P}}^\ell; \qquad \overline{\mathfrak{P}} \text{ vom 1. Rel. Gr.}$$

sein. Der Zerlegungskörper eines Primfaktors $\mathfrak{P}$ von $\mathfrak{p}$ in K ist also sicher Unterkörper von K_ℓ; denn in K_ℓ und jedem

149 I

weiteren Unterkörper von K (es gibt nur noch solche vom Grade $\ell^2, \ell^3, \dots,$ $\ell^{\nu-1}$) zerfällt $\mathfrak{p}$ schon nicht mehr in verschiedene Primideale ersten Grades.

Der Zerlegungskörper ist also k selbst, die Zerlegungsgruppe die ganze zyklische Gruppe vom Grad ℓ^ν. Der Primteiler $\mathfrak{P}$ gestattet also alle ℓ^ν Substitutionen, sodaß $\mathfrak{p} = \mathfrak{P}^{\ell^\nu}$ ist. Da $\mathfrak{P}$ den ersten Relativgrad hat, hat nach Definition 5 (S. 35▸) der Trägheitskörper von $\mathfrak{P}$ den Grad 1, ist also ebenfalls k, der Verzweigungskörper von $\mathfrak{P}$ den Grad $h = \ell^\nu$ (da ℓ prim zu p; Definition 6a, S. 43▸), ist also K. Nach der zitierten Stelle ist ℓ^ν Teiler von $\mathsf{N}_K(\mathfrak{P}) - 1 = \mathsf{N}(\mathfrak{p}) - 1$. Die Verzweigungsgruppe hat den Grad 1, also auch alle höheren Verzweigungsgruppen und es ist somit nach Satz 19, S. 48▸ die Relativdiskriminante von K genau durch $\mathfrak{p}^{\ell^\nu - 1}$ teilbar, w.z.b.w.

Satz 2. Es sei K relativzyklisch vom Primzahlgrad ℓ in Bezug auf k. Ferner sei $\mathfrak{l}$ ein in ℓ aufgehendes Primideal von k. Wenn dann die Relativdiskriminante durch $\mathfrak{l}$ teilbar ist, ist sie genau durch die $(v+1)(\ell-1)$ te Potenz von $\mathfrak{l}$ teilbar, wo die Zahl $v \geqq 1$ dadurch charakterisiert ist, daß `[...]` für jede ganze Zahl A aus K die Kongruenz besteht

$$\sigma\mathsf{A} \equiv \mathsf{A} \mod L^{v+1},$$

wenn σ die erzeugende Substitution der Gruppe von K und $\mathfrak{l} = L^\ell$ in K gilt (nur diese Zerlegung ist überhaupt möglich).

Ist ferner Λ ein „Primzahl“ zu L, so ist $\sigma\Lambda - \Lambda$ genau durch die $(v+1)$ te Potenz von L teilbar. Für v besteht die Ungleichung

$$\frac{s\ell}{\ell - 1} \geqq v \geqq 1,$$

wenn s der Exponent der höchsten in ℓ aufgehenden Potenz von $\mathfrak{l}$ (die „Ordnung“ von $\mathfrak{l}$) ist. Ferner ist v dann und nur dann durch ℓ teilbar, wenn

$$v = \frac{s\ell}{\ell - 1}$$

also speziell auch s durch $\ell - 1$ teilbar ist.

Beweis. 1.) Da v die höchste Potenz ist für die $\sigma\mathsf{A} \equiv \mathsf{A} \bmod L^{v+1}$ noch allgemein gilt, und die Gruppe von K nur die Einheitsgruppe und sich selbst zu Untergruppen hat, gibt es insgesamt gerade v Verzweigungsgruppen, die den Grad ℓ haben. Nach Satz 19, S. 48▸ ist also die Relativdiskriminante von

K genau durch

$$\mathfrak{l} \overset{(e-1)}{\downarrow} \overset{(\ell-1)+}{} \overset{1.\,\text{V.Gr.}}{\downarrow} \overset{(\ell-1)+}{} \cdots + \overset{v.\,\text{V.Gr.}}{\downarrow} \overset{(\ell-1)}{} = \mathfrak{l}^{(v+1)(\ell-1)}$$

teilbar. v muß mindestens 1 sein, da der Grad d. ersten Verzw. Gruppe nach Def. 6a, S. 43▸ sicher ℓ ist.

2.) Es sei Λ Primzahl für L und $\sigma\Lambda - \Lambda$ durch L^{v+2} teilbar. Da L den Rel.Gr. 1 hat, ist jede Zahl aus K einer Zahl aus k mod L kongruent. Sei A irgend eine Zahl aus K, so können

□□□

wir A nach Potenzen von Λ mit Koeffizienten aus k entwickeln:

$$\mathsf{A} \equiv \alpha_0 + \alpha_1\Lambda + \cdots + \alpha_{v+1}\Lambda^{v+1} \bmod L^{v+2}$$

Dann ist

$$\sigma\mathsf{A} - \mathsf{A} \equiv \alpha_1(\sigma\Lambda - \Lambda) + \cdots + \alpha_{v+1}\big((\sigma\mathsf{A})^{v+1} - \Lambda^{v+1}\big) \bmod L^{v+2},$$

da $\sigma L = L$. Da $(\sigma\mathsf{A})^k - \mathsf{A}^k$ teilbar durch $\sigma\Lambda - \Lambda$ ist, ist $\sigma\mathsf{A} - \mathsf{A} \equiv 0 \bmod L^{v+2}$ für jedes A aus K entgegen der Voraussetzung. Da andererseits $\sigma\Lambda - \Lambda$ mindestens durch L^{v+1} teilbar sein muß, ist es genau durch diese Potenz teilbar.

3.) Sei A genau durch L^e teilbar ($e \geqq 1$). Dann bestimme man B aus der Kongruenz:

$$\mathsf{A} \equiv \mathsf{B}\lambda^e \bmod L^{\overline{u}}$$

für einen hinreichend großen Exponenten $\overline{u}$.

151 I

Nun ist ($e \geqq 2$)[1]

$$(x^e - y^e) = [(x-y)+y]^e - y^e = (x-y)^e + \binom{e}{1}(x-y)^{e-1}y + \cdots$$
$$\cdots + \binom{e}{e-1}(x-y)y^{e-1}$$

[1] Formelende undeutlich

Hierin setze man $x = \sigma\Lambda$; $y = \Lambda$. Ist nun $e \not\equiv 0 \bmod \ell$, so ist das Glied

$$\binom{e}{\nu}(\sigma\Lambda - \Lambda)^{e-\nu}\Lambda^{\nu}$$

mindestens durch $L^{(v+1)(e-\nu)+\nu}$, also wenn $\nu \leqq e-2$, mindestens durch L^{2v+e} teilbar, das letzte Glied aber genau durch L^{v+e} teilbar. Ist aber $e \equiv 0 \bmod \ell$, so gilt für die Anfangsglieder dasselbe, während das letzte Glied sicher durch eine höhere Potenz als L^{v+e} teilbar. Für $e \not\equiv 0 \bmod \ell$ ist also, da $\sigma L = L$ und

$$\sigma\mathsf{A} - \mathsf{A} \equiv \mathsf{B}\,[(\sigma\Lambda)^e - \Lambda^e] + (\sigma\mathsf{B} - \mathsf{B})(\sigma\Lambda)^e \bmod L^{\overline{u}}$$

ist, das erste Glied rechts genau durch L^{v+e} teilbar (B ist prim zu L); das zweite Glied rechts ist sicher durch eine höhere Potenz von L teilbar, da

$$\sigma\mathsf{B} - \mathsf{B} \equiv 0 \bmod L^{v+1}$$
$$(\sigma\Lambda)^e \equiv 0 \bmod L^e$$

Da u beliebig groß sein kann, ist also dann $\sigma\mathsf{A} - \mathsf{A}$ genau durch L^{v+e} teilbar. Dies gilt für $e \geqq 2$. Für $e = 1$ ist $\sigma\mathsf{A} - \mathsf{A}$ ebenfalls genau durch L^{v+1} teilbar nach 2.).□□□

Wenn aber $e \equiv 0 \bmod \ell$ ist, und etwa $e = \mu\ell$, und λ aus k genau durch $\mathfrak{l}^{\mu}$ also L^e teilbar ist, so bestimmen wir B aus

$$\mathsf{A} \equiv \mathsf{B}\lambda \bmod L^{\overline{u}},$$

was stets mit zu L primem B möglich; dann ist

$$\sigma\mathsf{A} - \mathsf{A} \equiv \lambda(\sigma\mathsf{B} - \mathsf{B}) \bmod L^{\overline{u}}$$

also $\sigma\mathsf{A} - \mathsf{A}$ mindestens durch L^{v+1+e} teilbar.

Ist also A genau durch L^e teilbar ($e \geqq 1$), so ist im Falle $e \not\equiv 0 \bmod \ell$ $\mathsf{A}_1 = \sigma\mathsf{A} - \mathsf{A}$ genau durch L^{v+e} teilbar, im Falle $e \equiv 0 \bmod \ell$ sicher durch eine höhere Potenz von L. □□□

Nun setzen wir:

$$\mathsf{A}_1 = \sigma\mathsf{A} - \mathsf{A}; \quad \mathsf{A}_2 = \sigma\mathsf{A}_1 - \mathsf{A}_1; \quad \ldots\ldots \quad \mathsf{A}_{\ell-1} = \sigma\mathsf{A}_{\ell-2} - \mathsf{A}_{\ell-2}$$

und führen folgende symbolische Bezeichnung ein:

Ist $F(\sigma) = \alpha_0 + \alpha_1\sigma + \cdots + \alpha_\nu\sigma^\nu$; ($\alpha_i$ aus k) so soll

$$F(\sigma)\mathsf{A} = \alpha_0\mathsf{A} + \alpha_1(\sigma\mathsf{A}) + \cdots + \alpha_\nu(\sigma^\nu\mathsf{A})$$

sein. Es gilt dann offenbar:

$$\begin{aligned}[F(\sigma)+\phi(\sigma)]\mathsf{A} &= F(\sigma)\mathsf{A} + \phi(\sigma)\mathsf{A},\\ F(\sigma)\cdot[\phi(\sigma)\mathsf{A}] &= [F(\sigma)\phi(\sigma)]\mathsf{A},\\ F(\sigma)[\phi(\sigma)+\psi(\sigma)]\mathsf{A} &= [F(\sigma)\phi(\sigma) + F(\sigma)\psi(\sigma)]\mathsf{A},\end{aligned}$$

also die formalen Gesetze der Addition und Multiplikation. Dann kann man also schreiben:

$$\mathsf{A}_1 = (\sigma-1)\mathsf{A}; \quad \mathsf{A}_2 = (\sigma-1)\mathsf{A}_1 = (\sigma-1)^2\mathsf{A}; \quad \ldots \quad \mathsf{A}_{\ell-1} = (\sigma-1)^{\ell-1}\mathsf{A}.$$

Da nun gilt:

$$x^\ell - 1 = [(x-1)+1]^\ell - 1 = \ell(x-1) + \binom{\ell}{2}(x-1)^2 + \cdots + \ell(x-1)^{\ell-1} + (x-1)^\ell$$

also:

$$1 + x + \cdots + x^{\ell-1} = \ell + \binom{\ell}{2}(x-1) + \cdots + \ell(x-1)^{\ell-2} + (x-1)^{\ell-1},$$

so folgt, wenn

$$S(\mathsf{A}) = \mathsf{A} + \sigma\mathsf{A} + \cdots + \sigma^{\ell-1}\mathsf{A} = (1 + \sigma + \cdots + \sigma^{\ell-1})\mathsf{A}$$

die Spur von A bezeichnet:

$$\begin{aligned}S(\mathsf{A}) = [\ell + \binom{\ell}{2}(\sigma-1) + \cdots + (\sigma-1)^{\ell-1}]\mathsf{A} =&\\ = \ell\mathsf{A} + \binom{\ell}{2}\mathsf{A}_1 + \binom{\ell}{3}\mathsf{A}_2 + \cdots + \ell\mathsf{A}_{\ell-2} + \mathsf{A}_{\ell-1}\,.&\end{aligned}$$

Nach der vorigen Untersuchung ist nun A_i genau durch L^{e+iv} teilbar, wenn keine der Zahlen $e, e+v, \ldots, e+(i-1)v$ durch ℓ teilbar ist, andernfalls gewiß durch eine höhere Potenz.

Setzen wir nun $\mathsf{A} = \Lambda$, so ist $e = 1$ und das erste Glied rechts genau durch die $(s\ell+1)$–te Potenz von L teilbar wenn s die im Satz angegebene

Bedeutung hat, also $\ell \sim \mathfrak{l}^s$ □□□ $\sim L^{\ell s}$ ist.

153

Das letzte Glied sei genau durch L^a teilbar. Da nun eine der Zahlen $1, 1+v, 1+2v, \ldots, 1+(\ell-2)v$ sicher durch ℓ teilbar ist, wenn nicht $v \equiv 0$ oder $1 \bmod \ell$ ist, so ist abgesehen von diesen Fällen sicher $a > 1+(\ell-1)v$. Da nun die Spur von Λ in k liegt, also durch $\mathfrak{l}$ teilbar ist, wenn sie durch L teilbar ist, die höchste in $S(\Lambda)$ aufgehende Potenz von L also einen durch ℓ teilbaren Exponenten haben muß, kann nicht der Exponent des ersten Gliedes, nämlich $s\ell+1$, der niedrigste vorkommende sein. □□□ Da nun die Exponenten der Glieder bis $\ell \mathsf{A}_{\ell-2}$ alle $> s\ell+1$ sind, muß notwendig $a \leqq s\ell+1$ sein. Daraus folgt aber mit der vorhin gefundenen Ungleichung zusammen:

$$1+(\ell-1)v < s\ell+1$$
$$v < \frac{s\ell}{\ell-1}$$

Für $v \equiv 1 \bmod \ell$ ist ferner $a = 1+v(\ell-1)$, also a durch ℓ teilbar. Wie vorhin muß $a \leqq s\ell+1$ sein, diesmal aber sogar $a < s\ell+1$, da $a = s\ell+1$ wegen $a \equiv 0 \bmod \ell$ unmöglich. Also gilt auch hier $1+v(\ell-1) < s\ell+1$, d.h. $v < \frac{s\ell}{\ell-1}$.

Für $v \equiv 0 \bmod \ell$ schließlich ist wieder $a = 1+v(\ell-1)$ und $a \equiv 1 \bmod \ell$, also nicht durch ℓ teilbar. □□□ Wie vorhin ist sicher $a \leqq s\ell+1$ sein, aber sogar $a = s\ell+1$, da sonst die höchste in $S(\Lambda)$ aufgehende Potenz L^a, also ihr Exponent nicht durch ℓ teilbar wäre. Also ist hier

$$v = \frac{s\ell}{\ell-1}$$

Damit ist Satz 2 vollständig bewiesen.

Nun sei K_2 relativ zyklisch vom Grade ℓ^2 in Bezug auf k und K_1 der zyklische Unterkörper vom Relativgrad ℓ. Das in ℓ aufgehende Primideal $\mathfrak{l}$ zerfällt in K_1, also

154

$$\mathfrak{l} = L_1^{\ell}$$

Der Zerlegungskörper von $\mathfrak{l}$ in K_2 ist dann wie S. 149 oben k selbst, also wie vorhin:

$$\mathfrak{l} = L_2^{\ell^2} \quad \text{in} \quad K_2; \quad L_1 = L_2^{\ell}.$$

Es sei nun v die im vorigen Satz definierte Zahl für K_1 nach k, v_1 die für K_2 nach K_1. Sind $\mathfrak{D}_{20}, \mathfrak{D}_{10}, \mathfrak{D}_{21}$ bez. die Relativdiskriminanten von (K_2, k); (K_1, k); (K_2, K_1), so ist:

$$\mathfrak{D}_{21} \sim L_1^{(v_1+1)(\ell-1)}$$

die Relativnorm nach k also:

$$n_{10}(\mathfrak{D}_{21}) \sim \mathfrak{l}^{(v_1+1)(\ell-1)}$$

ferner

$$\mathfrak{D}_{10} \sim \mathfrak{l}^{(v+1)(\ell-1)}$$

nach Satz 8, S. 15▸ also

$$\mathfrak{D}_{20} = \mathfrak{D}_{10}^{\ell} n_{10}(\mathfrak{D}_{21}) \sim \mathfrak{l}^{(v+1)\ell(\ell-1)+(v_1+1)(\ell-1)}$$

v_1 ist die Anzahl der von 1 verschiedenen Verzweigungsgruppen von K_2 nach K_1. Diese sind die Durchschnitte der Gruppe, zu der K_1 als Unterkörper von K_2 gehört, mit den Verzweigungsgruppen von K_2 nach k. Da die erstere Gruppe die zyklische vom Grade ℓ ist, folgt daß v_1 auch die Anzahl der von 1 verschiedenen Verzweigungsgruppen von K_2 nach k ist. Unter ihnen seien μ vom Grade ℓ^2, sodaß $(v_1 - \mu)$ [2] vom Grade ℓ sind. Nach Satz 19, S. 49▸ ist also $\mathfrak{D}_{20}$ genau teilbar durch:

$$\mathfrak{D}_{20} \sim \mathfrak{l}^{(\ell^2-1)+\mu(\ell^2-1)+(v_1-\mu)(\ell-1)}.$$

Es ist also:

$$(\mu+1)(\ell^2-1) + (v_1-\mu)(\ell-1) = (v+1)\ell(\ell-1) + (v_1+1)(\ell-1)$$

oder

$$\begin{aligned}(\mu+1)(\ell+1) + (v_1-\mu) &= (v+1)\ell + (v_1+1)\\ (\mu+1)\ell &= (v+1)\ell\\ \mu &= v.\end{aligned}$$

[2] undeutlich

Es gibt also genau v Verzweigungsgruppen von K_2 nach k vom Grade ℓ^2 und $v_1 - v$ vom Grade ℓ, d.h. wenn σ die erzeugende Substitution von K_2 nach k ist, ist $v+1$ die höchste Potenz, sodaß für jedes A aus K_2 gilt

$$\sigma\mathsf{A} \equiv \mathsf{A} \mod L_2^{v+1}$$

(da für höhere Potenzen die Verzweigungsgruppen nicht mehr alle Substitutionen $1, \sigma, \sigma^2, \ldots, \sigma^{\ell^2-1}$ umfassen). σ^ℓ ist die erzeugende Substitution von K_2 nach K_1. Es ist also v_1+1 die höchste Potenz, für die:

$$\sigma^\ell\mathsf{A} \equiv \mathsf{A} \mod L_2^{v_1+1}$$

für jedes A aus K_2 gilt.[3]

Nun ist, wenn Λ_ℓ genau durch L_2^ℓ, Λ genau durch L_2 teilbar ist, für beliebig großes $\overline{u}$ die Kongruenz

$$\Lambda_e \equiv \Lambda^e\xi \mod L_2^{\overline{u}}$$

durch ein zu L_2 primes ξ aus K_2 lösbar.

Wir haben ferner:

$$(\sigma\Lambda)^e - \Lambda^e = (\sigma\Lambda - \Lambda)^e + \binom{e}{1}(\sigma\Lambda-\Lambda)^{e-1}\Lambda + \cdots + \binom{e}{e-1}(\sigma\Lambda-\Lambda)\Lambda^{e-1}$$

Nun ist $\sigma\Lambda - \Lambda$ mindestens durch L_2^{v+1} teilbar, also $(\sigma\Lambda)^\ell - \Lambda^\ell$ mindestens durch L_2^{v+e}. Wegen

$$\sigma\Lambda_\ell - \Lambda_\ell \equiv \xi[(\sigma\Lambda)^\ell - \Lambda^\ell] + [\sigma\xi - \xi](\sigma\Lambda)^\ell \bmod L_2^{\overline{u}}$$

ist also auch $\sigma\Lambda_e - \Lambda_e$ mindestens durch L_2^{v+e} teilbar. Daher ist

$$\left\{\begin{array}{lcl} (\sigma-1)\mathsf{A} & \text{durch} & L_2^{v+1} \\ (\sigma-1)^2\mathsf{A} & \shortparallel & L_2^{2v+1} \\ \cdots\cdots\cdots\cdots & & \\ (\sigma-1)^\nu\mathsf{A} & \shortparallel & L_2^{\nu v+1} \end{array}\right\} \text{ mindestens teilbar}$$

Wegen $\sigma^\ell - 1 = (\sigma-1)^\ell + \binom{\ell}{1}(\sigma-1)^{\ell-1} + \cdots + \binom{\ell}{\ell-1}(\sigma-1)$ ist also $(\sigma^\ell-1)\mathsf{A}$ mindestens so oft durch L_2 teilbar, wie $\binom{\ell}{\ell-1}(\sigma-1)\mathsf{A}$,

[3] ℓ und e sind im Folgenden optisch schwer zu unterscheiden, vor allem als Sub– und Superskripte.

also sicher durch eine höhere Potenz als L_2^{v+1}. Da dies für jedes A gilt, ist sicher $v_1 > v$.

Das läßt sich nun □□□ bedeutend verallgemeinern. Es gilt nämlich:

Satz 3. Sei K_ν ein relativ zyklischer Körper vom Grade ℓ^ν, K_μ (für $\mu = 1, 2, \ldots, \nu-1$) der Unterkörper vom Grade ℓ^μ über k. Der Primteiler $\mathfrak{l}$ von ℓ in k gehe in der Relativdiskriminante von K_1 auf, sodaß wie früher

$$\mathfrak{l} = L_1^\ell \quad \text{in} \quad K_1$$

und k der Zerlegungskörper für alle K_μ ist. Daraus folgt:

$$\mathfrak{l} = L_\mu^{\ell^\mu} \quad \text{in} \quad K_\mu.$$

Ist wieder v_μ die Anzahl der von 1 verschiedenen Verzweigungsgruppen von $K_{\mu+1}$ nach K_μ, □□□ so gilt:

$$1 \leqq v < v_1 < \cdots < v_{\nu-1} \leqq \frac{s\ell^\nu}{\ell - 1}$$

und □□□ $\mathfrak{l}$ geht in der Relativdiskriminante von K_ν genau in der Potenz von $\mathfrak{l}$ mit dem Exponenten:

$$\begin{aligned}\ell^{\nu-1}(v+1)(\ell-1) + \ell^{\nu-2}(v_1+1)(\ell-1) + \cdots + (v_{\nu-1}+1)(\ell-1) \\ = (\ell^\nu - 1) + (\ell-1)[v\ell^{\nu-1} + v_1\ell^{\nu-2} + \cdots + v_{\nu-1}]\end{aligned}$$

auf.

Beweis. $1 \leqq v < v_1 < v_2 < \cdots < v_{\nu-1}$ ist nach dem vorigen klar, da die Bedeutung □□□ z.B. von v_2 in Bezug auf K_1 als Grundkörper dieselbe ist, wie die von v_1 in Bezug auf k etz. Es ist ferner nach Satz 2 $v_{\nu-1} \leqq \frac{\bar{s}\ell}{\ell-1}$ wo $\bar{s}$ der Exponent der höchsten Potenz von $L_{\nu-1}$ ist, die in ℓ aufgeht. Nun ist $\mathfrak{l} = L_1^\ell = L_2^{\ell^2} = \cdots = L_{\nu-1}^{\ell^{\nu-1}}$ und $\ell \sim \mathfrak{l}^s$ also $\bar{s} = s\ell^{\nu-1}$, woraus $v_{\nu-1} \leqq \frac{s\ell^\nu}{\ell-1}$ folgt.

Für die in der Relativdiskriminante von K_ν aufgehende Potenz von $\mathfrak{l}$ ergibt sich nach Satz 8, S. 15▸: □□□

$$\mathfrak{D}_{\nu,0} = \mathfrak{D}_{\nu-1,0} n_{\nu-1,0}(\mathfrak{D}_{\nu,\nu-1})$$

Nun ist unsere Formel nach S. 154 Mitte richtig für $\nu = 2$. Sei sie richtig bis $\nu - 1$, so ist:

$$\mathfrak{D}^{\ell}_{\nu-1,0} \sim \mathfrak{l}^{[\ell^{\nu-2}(v+1)(\ell-1)+\ell^{\nu-3}(v_1+1)(\ell-1)+\cdots+(v_{\nu-2}+1)(\ell-1)]\ell}$$

Ferner ist: □□□

$$\mathfrak{D}_{\nu,\nu-1} \sim L_{\nu-1}^{(v_{\nu-1}+1)(\ell-1)} \quad \text{(nach Satz 2)},$$

also

$$n_{\nu-1,0}(\mathfrak{D}_{\nu,\nu-1}) \sim \mathfrak{l}^{(v_{\nu-1}+1)(\ell-1)}$$

Daraus folgt:

$$\mathfrak{D}_{\nu,0} \sim \mathfrak{l}^{\ell^{\nu-1}(v+1)(\ell-1)+\cdots+(v_{\nu-1}+1)(\ell-1)}$$

und somit die Allgemeingültigkeit unserer Behauptung.

Auf Grund von Satz 1 und 2 können wir speziell sagen:

Satz 4. Die Relativdiskriminante eines relativzyklischen Körpers K von Primzahlgrad ℓ über k hat die Form:

$$\mathfrak{D} = f^{\ell-1},$$

wo

$$f = \prod \mathfrak{p} \cdot \prod \mathfrak{l}^{v+1}$$

ist und $\mathfrak{p}$ die zu ℓ primen, $\mathfrak{l}$ die in ℓ aufgehenden Primideale von $\mathfrak{D}$ durchläuft.

b) Normenreste

b.) Normenreste im relativ zyklischen Körper von Primzahlgrad.

Definition 1. Sei k ein algebr. Körper, ℓ eine Primzahl, $\mathfrak{m}$ ein Ideal aus k. Dann heißt die zu $\mathfrak{m}$ prime Zahl α ℓ–ter Potenzrest nach $\mathfrak{m}$, wenn die Kongruenz:

$$x^{\ell} \equiv \alpha \mod \mathfrak{m}$$

in k lösbar ist. (Dabei sollen hier wie im Folgenden alle Zahlen und Ideale ganz sein).

Satz 5. Sei $\mathfrak{m} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_i^{\nu_i}$ und alle $\mathfrak{p}_i$ prim zu ℓ [4]. Damit α ein ℓ–ter Potenzrest nach $\mathfrak{m}$ ist, ist notwendig und hinreichend, daß α nach jedem Primteiler $\mathfrak{p}_{[\dots]}$ von $\mathfrak{m}$ ℓ–ter Potenzrest ist.

Beweis.

1.) Aus $\lambda^\ell \equiv \alpha \bmod \mathfrak{m}$ folgt erst recht $\lambda^\ell \equiv \alpha \bmod \mathfrak{p}_s$.

2.) Sei $\lambda^\ell \equiv \alpha \bmod \mathfrak{p}^\kappa$. Wir setzen $\lambda^\ell \equiv \alpha + \pi\xi \bmod \mathfrak{p}^{\kappa+1}$ wo π genau durch $\mathfrak{p}^\kappa$ teilbar ist. Dann ist auch

$$(\lambda + \eta\pi)^\ell \equiv \ \square\square\square\ \alpha \mod \mathfrak{p}^\kappa$$

und

$$(\lambda + \eta\pi)^\ell \equiv \lambda^\ell + \ell\eta\pi \bmod \mathfrak{p}^{\kappa+1}$$

Wählt man also η so, daß $\ell\eta \equiv -\xi \bmod \mathfrak{p}$ ist, was wegen $(\ell, \eta) = 1$ möglich, so folgt:

$$(\lambda + \eta\pi)^\ell \equiv \lambda^\ell + \ell\eta\pi \equiv \alpha \bmod \mathfrak{p}^{\kappa+1}$$

Ist also α ℓ–ter Potenzrest nach $\mathfrak{p}$, so ist es auch ℓ–ter Potenzrest nach jeder Potenz $\mathfrak{p}^\nu$.

3.) Sei $\lambda_s^\ell \equiv \alpha \bmod \mathfrak{p}_s^{\nu_s}$. Dann wählen wir λ so, daß

$$\lambda \equiv \lambda_s \mod \mathfrak{p}_s^{\nu_s}$$

wird. Dann gilt $\lambda^\ell \equiv \alpha \bmod \mathfrak{m}$, w.z.b.w.

Speziell ergab sich bei 2.)

159 I

Satz 6. Ist α ℓ–ter Potenzrest nach dem zu ℓ primen $\mathfrak{p}$, so ist es auch ℓ–ter Potenzrest nach jeder Potenz $\mathfrak{p}^\nu$.

Satz 7. Das Primideal $\mathfrak{l}$ gehe in ℓ auf. Dann ist jede zu ℓ prime Zahl ℓ–ter Potenzrest nach $\mathfrak{l}$.

Beweis. Es ist

$$\alpha^\ell - \beta^\ell = (\alpha - \beta)^\ell + \binom{\ell}{1}(\alpha - \beta)^{\ell-1}\beta + \dots + \binom{\ell}{\ell-1}(\alpha - \beta)\beta^{\ell-1}.$$

[4] undeutlich

Aus $\alpha^\ell \equiv \beta^\ell \bmod \mathfrak{l}$ folgt also, da rechts alle späteren Glieder $\equiv 0 \bmod \mathfrak{l}$ sind

$$(\alpha - \beta)^\ell \equiv 0 \mod \mathfrak{l}$$

Da $\mathfrak{l}$ Primideal ist, muß dann

$$\alpha - \beta \equiv 0 \bmod \mathfrak{l}$$
$$\alpha \equiv \beta \bmod \mathfrak{l}$$

sein. Die ℓ–ten Potenzen der Körperzahlen erzeugen also ebensoviel Restklassen, wie die Zahlen selbst. Jede Zahl ist daher einer ℓ–ten Potenz nach $\mathfrak{l}$ kongruent.

Nun sei K ein relativzyklischer Körper vom Primzahlgrad ℓ in Bezug auf k.

Definition 2. Eine Zahl α aus k heißt Normenrest von K nach dem Modul $\mathfrak{m}$, wenn es eine Zahl A in K gibt, für die

$$n(\mathsf{A}) \equiv \alpha \mod \mathfrak{m}$$

ist.

Satz 8.

1.) Geht $\mathfrak{p}$ nicht in der Relativdiskriminante von K auf, dann ist jedes zu $\mathfrak{p}$ prime α Normenrest von K nach jeder Potenz $\mathfrak{p}^e$ (e beliebig)

2.) Geht $\mathfrak{p}$ in der Relativdiskriminante auf, und ist prim zu ℓ, dann ist von allen Zahlen des verkürzten Restsystems mod $\mathfrak{p}^e$ genau der ℓ–te Teil Normenrest nach $\mathfrak{p}^e$ (e beliebig).

3.) Das gleiche gilt auch für jedes $\mathfrak{l}^e$, wo $\mathfrak{l}$ in ℓ und der Relativdiskriminante aufgeht, falls $e > v$ ist. Für $e \leqq v$ ist jedoch wieder jede zu $\mathfrak{l}$ prime Zahl Normenrest nach $\mathfrak{l}^e$. Dabei hat v die Bedeutung wie in Satz 2.

Beweis.

Beweis für 1.)

Wir unterscheiden 4 Fälle:

$$\begin{array}{llllll} \text{a.)} & \mathfrak{p} & = & \mathfrak{P}_1 \dots \mathfrak{P}_\ell & , \quad \text{prim} \quad \text{zu} & \ell \\ \text{b.)} & \mathfrak{p} & = & \mathfrak{P} & , \quad \shortparallel \quad \shortparallel & \ell \\ \text{c.)} & \mathfrak{l} & = & L_1 \dots L_\ell & , \quad \text{Teiler} \quad \text{von} & \ell \\ \text{d.)} & \mathfrak{l} & = & L & , \quad \shortparallel \quad \shortparallel & \ell \end{array}$$

andere Zerlegungen können, da ℓ Primzahl, nicht eintreten.

a.) Die $\mathfrak{P}_i$ haben den Relativgrad 1. Es sei f der Grad von $\mathfrak{p}$ also auch der von $\mathfrak{P}_i$ und ϱ eine Primitivzahl nach $\mathfrak{p}$. Jedes zu $\mathfrak{p}$ prime α aus k genügt einer Kongruenz:

$$\alpha \equiv \varrho^\nu \bmod \mathfrak{p}$$

Setzen wir also, $\alpha \equiv \alpha_0 \varrho^\nu \bmod \mathfrak{p}^e$

so ist: $\alpha_0 \equiv 1 \bmod \mathfrak{p}$

also α_0 ℓ–ter Potenzrest nach $\mathfrak{p}$ und somit nach $\mathfrak{p}^e$. Es sei

$$\alpha_0 \equiv \gamma^\ell \mod \mathfrak{p}^e$$

Nun bestimmen wir in K die Zahl A aus den Kongruenzen:

$$\begin{aligned} \mathsf{A} &\equiv \varrho \bmod \mathfrak{P}_1^e \\ \mathsf{A} &\equiv 1 \bmod \mathfrak{P}_2^e \dots \mathfrak{P}_\ell^e \end{aligned}$$

Gehen wir zu den relativ konjugierten über, so geht jedes $\mathfrak{P}$ in alle anderen über. Jedenfalls gilt dann:

$$\mathsf{A}' \equiv 1 \bmod \mathfrak{P}_1^e, \quad \mathsf{A}'' \equiv 1 \bmod \mathfrak{P}_1^e, \quad \dots, \quad \mathsf{A}^{(\ell-1)} \equiv 1 \bmod \mathfrak{P}_1^e$$

Also gilt

$$n(\mathsf{A}) \equiv \varrho \mod \mathfrak{P}_1^e.$$

Da aber $n(\mathsf{A}) - \varrho$ in k liegt und die $\mathfrak{P}_i$ alle verschieden sind, folgt

$$n(\mathsf{A}) \equiv \varrho \mod \mathfrak{p}^e$$

Also ist

$$\alpha \equiv n(\gamma \mathsf{A}^{\nu}) \mod \mathfrak{p}^{e} \qquad \text{w.z.b.w.}$$

b.) Sei P eine Primitivzahl nach dem Primideal $\mathfrak{p}$ in K. Ist wieder f der Grad von $\mathfrak{p}$ in k, so ist wegen $n(\mathfrak{p}) = \mathfrak{p}^{\ell}$ der Grad von $\mathfrak{p}$ in K gleich $f\ell$. Es sind also die Potenzen:

$$1, \mathsf{P}, \mathsf{P}^2, \ldots, \mathsf{P}^{p^{f\ell}-2}$$

inkongruent mod $\mathfrak{p}$. Von der Zahl

$$\mathsf{P}^{1+p^f+p^{2f}+\cdots+p^{(\ell-1)f}}$$

ist also erst die (p^f-1)–te Potenz $\equiv 1 \bmod \mathfrak{p}$. Diese Zahl ist aber nach den Ergebnissen von S. 4▶/5▶ $\equiv n(\mathsf{P}) \bmod \mathfrak{p}$. Von der Zahl $\varrho = n(\mathsf{P})$ ist also erst die (p^f-1)–te Potenz $\equiv 1\,(\mathfrak{p})$, ϱ also, da es in k liegt, Primitivzahl nach $\mathfrak{p}$. Setzen wir wieder wie vorhin

$$\alpha \equiv \alpha_0 \varrho^{\nu} \mod \mathfrak{p}^{e}; \quad \alpha_0 \equiv \gamma^{\ell} \mod \mathfrak{p}^{e}$$

so ist also:

$$\alpha \equiv n(\gamma \mathsf{P}^{\nu}) \qquad \text{w.z.b.w.}$$

c.) Nach Satz 7 ist auf jeden Fall (auch für d.)) $\alpha \equiv \gamma^{\ell} = n(\gamma) \bmod \mathfrak{l}$, für die erste Potenz von $\mathfrak{l}$ die Behauptung 1.) also richtig. Wir wählen die Zahl Θ aus K so, daß

$$\Theta \equiv 1 \bmod L_1; \quad \Theta \equiv 0 \bmod L_2 \ldots L_{\ell}, \quad \text{also}$$

für die Relativspur:

$$S(\Theta) \equiv 1 \bmod L_1,$$

da $S(\Theta)$ in k liegt also

$$S(\Theta) \equiv 1 \bmod \mathfrak{l}.$$

Ehe wir den Beweis zu Ende führen, zeigen wir, daß es auch im Falle d.) stets ein Θ gibt, sodaß $S(\Theta) \equiv 1 \bmod \mathfrak{l}$ ist.

162 ı

d.) Sei P Primitivzahl nach $\mathfrak{l}$ in K. $\mathfrak{l}$ hat den Relativgrad ℓ in Bezug auf k; also genügt P einer Kongruenz:

$$\mathsf{P}^{\ell} + \alpha_1 \mathsf{P}^{\ell-1} + \cdots + \alpha_{\ell} \equiv 0 \mod \mathfrak{l}$$

die irreduzibel ist. Da der Relativgrad von K ebenfalls ℓ ist, genügt also P einer *irreduziblen* Gleichung ℓ–ten Grades:

$$\mathsf{P}^\ell + \beta_1 \mathsf{P}^{\ell-1} + \cdots + \beta_\ell = 0 \qquad \text{in} \quad k.$$

Wäre nun für jedes ν: $S(\mathsf{P}^\nu) \equiv 0 \mod \mathfrak{l}$, so lehrten die Newtonschen Potenzformeln, daß $\beta_1, \ldots, \beta_{\ell-1}$ durch $\mathfrak{l}$ teilbar wäre, und somit

$$\mathsf{P}^\ell \equiv -\beta_\ell \mod \mathfrak{l}$$

Ist ℓ gerade, so ist $\beta_\ell \equiv -\beta_\ell \bmod \mathfrak{l}$, also $\beta_\ell \equiv -n(\mathsf{P})\,(\mathfrak{l})$ sonst ohne weiteres $\beta_\ell \equiv -n(\mathsf{P}) \mod \mathfrak{l}$. Es wäre also stets

$$\mathsf{P}^\ell \equiv n(\mathsf{P}) \mod \mathfrak{l}$$

Nun ist wie vorhin

$$\left.\begin{array}{rrcll} & n(\mathsf{P}) & \equiv & \mathsf{P}^{1+\ell^f+\ell^{2f}+\cdots+\ell^{(\ell-1)f}} & \mod \mathfrak{l} \\ \text{also} & \mathsf{P}^\ell & \equiv & \mathsf{P}^{1+\ell^f+\cdots+\ell^{(\ell-1)f}} & \mod \mathfrak{l} \end{array}\right\} \text{ in } K$$

Da beide Potenzen kleiner als $\mathsf{P}^{\ell^\ell f-1}$ sind, folgte

$$\ell = 1 + \ell^f + \cdots + \ell^{(\ell-1)f}$$

was unmöglich ist. Es gibt also ein ν, sodaß

$$S(\mathsf{P}^\nu) \not\equiv 0 \mod \mathfrak{l}$$

wird.

$$\left.\begin{array}{rrcll} \text{Sei} & S(\mathsf{P}^\nu) & \equiv & \xi & \mod \mathfrak{l} \\ \text{und} & \xi\xi' & \equiv & 1 & \mod \mathfrak{l} \end{array}\right\} \text{ in } K,$$

so setzen wir $\Theta = \xi' \mathsf{P}^\nu$. Dann ist da ξ und ξ' in k liegen

$$S(\theta) \equiv \xi\xi' \equiv 1 \mod \mathfrak{l}, \quad \text{wie behauptet.}$$

In beiden Fällen c.) und d.) gibt es also in K ein Θ, sodaß

$$S(\Theta) \equiv 1 \mod \mathfrak{l}$$

Unser Satz sei nun richtig für $\mathfrak{l}^e$, also

$$\alpha \equiv n(\mathsf{A}) \mod \mathfrak{l}^e$$

Wir setzen dann

$$\alpha \equiv n(\mathsf{A}) - \beta\lambda^e \mod y^{e+1}$$

wo λ Primzahl für $\mathfrak{l}$ in k. Es ist

$$\begin{aligned} n(1+\xi\Theta\lambda^e) &\equiv 1+\xi S(\Theta)\lambda^e \mod \mathfrak{l}^{e+1} \\ &\equiv 1+\xi\lambda^e \mod \mathfrak{l}^{e+1} \end{aligned}$$

Also:[5]

$$n\big(\mathsf{A}(1+\xi\Theta\lambda^e)\big) = n(\mathsf{A})n(1+\xi\Theta\lambda^e) \equiv \alpha + (\beta+\xi\alpha)\lambda^e \,(\mathfrak{l}^{e+1})$$

Wählen wir also ξ so, daß $\alpha\xi+\beta \equiv 0 \mod \mathfrak{l}$ wird, was für zu $\mathfrak{l}$ primes α möglich, so wird $\alpha \equiv n(\mathsf{B}) \mod \mathfrak{l}^{e+1}$. Da für $e=1$ der Satz stimmt, ist damit 1.) für jeden der Fälle a.) b.) c.) d.) bewiesen.

Beweis für 2.)[6]

Ist $\mathfrak{p}$ ein zu ℓ primer Faktor der Relativdiskriminante, sodaß in K: $\mathfrak{p} = \mathfrak{P}^\ell$ ist, wo $\mathfrak{P}$ vom Relativgrad 1, so ist

$$\mathsf{N}_K(\mathfrak{P}) = \mathsf{N}(\mathfrak{p}), \quad \text{also} \quad \mathsf{N}_K(\mathfrak{P}^e) = \mathsf{N}(\mathfrak{p}^e),$$

also die Anzahl der Restklassen in K nach $\mathfrak{P}^e$ und in k nach $\mathfrak{p}^e$ dieselbe, insbesondere auch die der zu $\mathfrak{p}$ primen Restklassen $\square\square\square$ mod $\mathfrak{P}^e$ und $\mathfrak{p}^e$. Denn es ist dann

$$\begin{aligned} \phi(\mathfrak{p}^e) = \phi_K(\mathfrak{P}^e) &= \mathsf{N}_K(\mathfrak{P}^e)\left(1-\frac{1}{\mathsf{N}_K(\mathfrak{P})}\right) = \mathsf{N}(\mathfrak{p}^e)\left(1-\frac{1}{\mathsf{N}(\mathfrak{p})}\right) \\ &= p^{ef}\left(1-\frac{1}{p^f}\right) = p^{(e-1)f}(p^f-1) \end{aligned}$$

Daher ist jede zu $\mathfrak{p}$ prime Zahl A aus K nach jeder Potenz $\mathfrak{P}^e$ einer Zahl α aus k kongruent, also auch

$$\mathsf{A} \equiv \alpha \mod \mathfrak{P}^{e\ell}$$

[5] Modulus undeutlich

[6] spätestens ab hier werden e und ℓ optisch kaum noch unterscheidbar, insbesondere im Exponenten.

Daraus folgt $\mathsf{N}(\mathsf{A}) \equiv \alpha^\ell \bmod \mathfrak{p}^e$.

164 I

Jeder Normenrest ist also ℓ–ter Potenzrest. Das umgekehrte ist trivial.

Es sei nun ϱ Primitivzahl nach $\mathfrak{p}$, sodaß wieder für jedes α eine Darstellung:

$$\alpha \equiv \alpha_0 \varrho^\nu \mod \mathfrak{p}^e; \quad \alpha_0 \equiv 1 \mod \mathfrak{p};$$

$(\nu = 0, 1, \ldots, p^f - 2)$ gilt, wo ν durch α festgelegt ist. Es ist $\alpha_0 \equiv \gamma^\ell \bmod \mathfrak{p}^e$, sodaß es sich nun darum handelt, wann ϱ^ν Potenzrest ist, wann also $\varrho^\nu \equiv \lambda^\ell \bmod \mathfrak{p}$ ist. Sei $\lambda \equiv \varrho^\mu \bmod \mathfrak{p}$. Dann muß $\mu\ell \equiv \nu \bmod (p^f - 1)$ sein. Nach Satz 1 ist $p^f - 1$ teilbar durch ℓ, also muß auch ν durch ℓ teilbar sein, und umgekehrt, wenn ν durch ℓ teilbar ist ϱ^ν ℓ–ter Potenzrest. Normenreste sind also genau die Zahlen, für die $\nu = 0, \ell, 2\ell, \ldots, \left(\frac{p^f-1}{\ell} - 1\right)\ell$ ist. Dies ist genau der ℓ–te Teil aller primen Restklassen nach $\mathfrak{p}$, also auch nach $\mathfrak{p}^e$.

Beweis für 3.)

Ist $\mathfrak{l}$ ein Primfaktor von ℓ der in der Relativdiskriminante aufgeht, also nach Satz 2 genau in der $(v+1)(\ell-1)$–ten Potenz. Dann ist in K: $\mathfrak{l} = L^\ell$. Wir bezeichnen im Folgenden mit λ_e bezw. Λ_e Zahlen, die genau durch $\mathfrak{l}^e$ bezw. L^e teilbar sind. ℓ sei genau durch $\mathfrak{l}^s$ teilbar.

Für die Relativspur erhalten wir wie im Beweise von Satz 2:

$$S(\Lambda_e) = \ell\Lambda_e + \binom{\ell}{2}(\sigma - 1)\Lambda_e + \cdots + (\sigma - 1)^{\ell-1}\Lambda_e$$

Das erste Glied rechts ist genau durch die Potenz $s\ell + e$ von L, jedes folgende aber, wie im Satz 2, durch eine höhere Potenz, ausgenommen das letzte, das wenigstens durch die $e + v(\ell - 1)$ te Potenz teilbar ist. Da die in $S(\Lambda e)$ aufgehende Potenz von L durch ℓ teilbar sein muß (Zahl aus k), ist wegen der Relation

$$s\ell \geqq v(\ell - 1)$$

d.h.

$$s\ell + e \geqq v(\ell - 1) + e$$

165 I

auf folgendes zu schließen:

$$\text{Für} \quad e < v \quad \text{ist} \quad s\ell + e \geqq e + v(\ell - 1) > e + e(\ell - 1) = e\ell$$

also $S(\Lambda_e)$ mindestens durch $L^{e\ell+1}$, d.h. mindestens durch $L^{(e+1)\ell}$ teilbar. Somit

$$S(\Lambda_e) \equiv 0 \mod \mathfrak{l}^{e+1}$$

Für $e = v$ ist $e + v(\ell - 1) = v\ell$, also $S(\Lambda_e)$ mindestens durch $L^{v\ell}$ teilbar:

$$S(\Lambda_e) \equiv 0 \mod \mathfrak{l}^{v}$$

Für $e > v$ ist $e + v(\ell - 1) > v + v(\ell - 1) = v\ell$, also $S(\Lambda_e)$ mindestens durch $L^{v\ell+1}$, d.h. durch $L^{(v+1)\ell} = \mathfrak{l}^{v+1}$ teilbar:

$$S(\Lambda_e) \equiv 0 \mod \mathfrak{l}^{v+1}$$

Wir haben also:

Ist Λ_e eine genau durch L^e teilbare Zahl aus K, so ist sicher

$$\text{(I)} \qquad S(\Lambda_e) \equiv 0 \begin{cases} \mod \mathfrak{l}^{e+1} & \text{für} \quad e < v \\ \mod \mathfrak{l}^{v} & \text{"} \quad e = v \\ \mod \mathfrak{l}^{v+1} & \text{"} \quad e > v \end{cases}$$

Mit $s_1, s_2, \ldots$ bezeichnen wir nun die Potenzsummen von Λ_e und den konjugierten, mit $a_1, a_2, \ldots$ die symmetrischen Grundfunktionen. Dann ist

$$\begin{aligned} &s_1 + a_1 = 0 \\ &s_2 + a_1 s_1 + 2a_2 = 0 \\ &\ldots\ldots\ldots\ldots\ldots \\ &s_{\ell-1} + a_1 s_{\ell-2} + \cdots + a_{\ell-2} s_1 + (\ell - 1)a_{\ell-1} = 0 \end{aligned}$$

1.) $\boldsymbol{e < v}$. Setzen wir $i = \left[\frac{v}{e}\right]$, so ist sicher $s_1, s_2, \ldots, s_{i-1}$ durch $\mathfrak{l}^{e+1}, \mathfrak{l}^{2e+1}, \ldots, \mathfrak{l}^{(i-1)e+1}$ teilbar □□□, da $(i-1)e$ sicher noch $< v$ ist. □□□

s_i ist sicher durch $\mathfrak{l}^{ei}$ und $s_{i+1}, \ldots, s_{\ell-1}$ sicher durch $\mathfrak{l}^{v+1}$ teilbar. s_i ist sogar durch y^{ei+1} teilbar, wenn nicht $\frac{v}{e} = i$ (ganzzahlig). Da aber letzteres wegen $v > e$ nur mit $i \geqq 2$ möglich, ist dann $ei \geqq e + 1$; ebenso ist $v + 1 > e + 1$, also für alle s_κ:

s_κ mindestens durch $\mathfrak{l}^{e+1}$ teilbar.

Daraus folgt, daß $a_1, a_2, \ldots, a_{\ell-1}$ mindestens durch $\mathfrak{l}^{e+1}$ teilbar sind. a_ℓ ist als □□□ $\pm n(\Lambda_e)$ genau durch $L^{e\ell} = \mathfrak{l}^e$ teilbar. Es ist also

$$n(1+\Lambda_e) = 1 + \lambda_e$$

2.) $e = v$. Dann ist s_1 durch $\mathfrak{l}^v$ teilbar, $s_2, \ldots, s_{\ell-1}$ durch $\mathfrak{l}^{v+1}$. Also ist a_1 durch $\mathfrak{l}^v$ teilbar, $a_2, \ldots, a_{\ell-1}$ sicher durch $\mathfrak{l}^{v+1}$ a_ℓ genau durch $L^{v\ell} = \mathfrak{l}^v$. □□□ Wegen $a_\ell = \pm n(\Lambda_e)$; $a_1 = -S(\Lambda_e)$ ergibt sich also:

$$n(1+\Lambda_e) \equiv 1 + S(\Lambda_e) + n(\Lambda_e) \bmod \mathfrak{l}^{v+1}$$

3.) $e > v$. Hier sind alle s_ν also auch alle a_ν einschl. a_ℓ durch $\mathfrak{l}^{v+1}$ teilbar, also

$$n(1+\Lambda_e) \equiv 1 \mod \mathfrak{l}^{v+1}.$$

Im ganzen also wird

(1) $n(1+\Lambda_e) = 1 + \lambda_e$ für $e < v$

(2) $n(1+\Lambda_v) \equiv 1 + S(\Lambda_v) + n(\Lambda_v) \mod \mathfrak{l}^{v+1}$

(3) $n(1+\Lambda_e) \equiv 1 \mod \mathfrak{l}^{v+1}$ für $e > 0$

Daraus folgt also, daß dann und nur dann

$$n(1+\Lambda_e) \equiv 1 \mod \mathfrak{l}^v$$

gilt, wenn $e \geqq v$ ist, und daraus weiter:

Wenn A, B prim zu L sind und

$$n(\mathsf{A}) \equiv n(\mathsf{B}) \mod \mathfrak{l}^v,$$

so bestimme man Γ so, daß $\mathsf{B}\Gamma \equiv 1 \bmod \mathfrak{l}^v$, also

$$n(\mathsf{A}\Gamma) \equiv 1 \mod \mathfrak{l}^v.$$

Daraus folgt dann nach dem vorigen, daß

$$\mathsf{A}\Gamma \equiv 1 \mod L^v$$

also

$$\mathsf{A} \equiv \mathsf{B} \mod L^v$$

ist. Das Umgekehrte folgt ebenso: Wenn $\mathsf{A} \equiv \mathsf{B} \bmod L^v$ ist $n(\mathsf{A}) \equiv n(\mathsf{B}) \bmod \mathfrak{l}^v$.

Aus (3) folgt, daß aus der Kongruenz:

$$\mathsf{A} \equiv \mathsf{B} \mod L^{v+1}$$

geschlossen werden kann:

$$n(\mathsf{A}) \equiv n(\mathsf{B}) \mod \mathfrak{l}^{v+1},$$

indem man wie oben schließt.

Es soll nun bewiesen werden, daß für $\mathfrak{l}^{v+1}$ genau der ℓ–te Teil aller primen Restklassen Normenreste sind.

Wenn nun gezeigt werden kann, daß $n(\mathsf{A}) \equiv 1 \mod y^{v+1}$ durch genau ℓ zueinander inkongruente Zahlen mod L^{v+1} befriedigt wird, so liefern immer ℓ prime Restklassen nach L^{v+1} denselben Normenrest (zu $\mathfrak{l}$ prim). Denn sind $1 = \mathsf{A}_1, \ldots, \mathsf{A}_\ell$ diese ℓ mod L^{v+1} inkongruenten (zu L prime) Lösungen, so folgt aus:

$$n(\mathsf{B}) \equiv \beta \mod \mathfrak{l}^{v+1}$$

gleichzeitig

$$n(\mathsf{A}_i\mathsf{B}) \equiv \beta \mod \mathfrak{l}^{v+1}.$$

Umgekehrt folgt aber auch aus

$$\beta \equiv n(\mathsf{B}) \equiv n(\Gamma) \mod \mathfrak{l}^{v+1}$$

daß sich B und Γ nur um ein A_i unterscheiden. Alle $\phi_K(L^{v+1})$ zu L primen Restklassen nach L^{v+1} zerfallen dann also in genau ℓ Komplexe (Nebengruppen zu den A_i), sodaß jeder Komplex einen einzigen Normenrest β mod $\mathfrak{l}^{v+1}$ liefert, und die verschiedenen Komplexe nach $\mathfrak{l}^{v+1}$ inkongruente Normenreste β.

168 ı

Da nun $\Phi_K(L^{v+1}) = \phi_k(\mathfrak{l}^{v+1})$ ist, folgt, daß nur der ℓ–te Teil aller primen Restklassen mod $\mathfrak{l}^{v+1}$ Normenrest ist.

(Daß immer eine ganze *Restklasse* nach L^{v+1} denselben Normenrest liefert, folgt aus S. 167 Mitte).

Zum Beweise unseres Satzes 3.) für $\mathfrak{l}^{v+1}$ genügt es demnach zu zeigen, daß die Kongruenz $n(\mathsf{A}) \equiv 1 \mod \mathfrak{l}^{v+1}$ genau ℓ mal L^{v+1} inkongruente Lösungen A hat.

Wir erledigen ihn zunächst kurz für alle niedrigeren Potenzen von $\mathfrak{l}$.

$$\begin{array}{ll} \text{Aus} & n(\mathsf{A}) \equiv n(\mathsf{B}) \mod \mathfrak{l}^v \\ \text{folgt:} & \mathsf{A} \equiv \mathsf{B} \mod L^v \end{array}$$

und umgekehrt. Da $\phi_K(L^v) = \phi_k(\mathfrak{l}^v)$ [7] ist, gibt es also ebensoviel prime Restklassen nach $\mathfrak{l}^v$ mit Normenresten, als es überhaupt Restklassen mod $\mathfrak{l}^v$ gibt, d.h. jede zu $\mathfrak{l}$ prime Zahl ist Normenrest nach $\mathfrak{l}^v$ also auch nach jeder niedrigeren Potenz, w.z.b.w.

Um den Satz 3.) nun schließlich noch für y^{v+1} und höhere Potenzen zu beweisen, haben wir die Kongruenz

$$n(\mathsf{A}) \equiv 1 \mod \mathfrak{l}^{v+1}$$

zu betrachten. Ist A nicht gerade $\equiv 1 \bmod L^{v+1}$, so kann A nach (1) nur die Gestalt haben:

$$\mathsf{A} = 1 + \Lambda_v \,.$$

Eine solche Lösung gibt es aber auch, denn $\sigma\Lambda_1 - \Lambda_1$ ist nach Satz 2 genau durch L^{v+1} teilbar. Bringen wir nun den Bruch $\frac{\sigma\Lambda_1}{\Lambda_1}$ in die Gestalt $\frac{\mathsf{A}_0}{\alpha}$, wo Zähler und Nenner zu L prim sind, und α in k liegt, (dies ist stets möglich), und bestimmen ξ aus

$$\alpha\xi \equiv 1 \mod \mathfrak{l}^{\overline{u}}; \quad (\overline{u} \text{ beliebig groß})$$

so dürfen wir nach Multiplikation von Zähler und Nenner mit ξ offenbar $\alpha \equiv 1 \mod \mathfrak{l}^{\overline{u}}$ annehmen. Dann ist

$$\mathsf{A}_0 = \alpha\frac{\sigma\Lambda_1}{\Lambda_1} \quad \text{also} \quad \sigma^i\mathsf{A}_0 = \alpha\frac{\sigma^{i+1}\Lambda_1}{\sigma^i\Lambda_1}$$

169 I

und demnach:

$$(4) \qquad n(\mathsf{A}_0) = \alpha^\ell \equiv 1 \mod \mathfrak{l}^{v+1}$$

[7] undeutlich

Andererseits folgt aus:

$$\alpha\sigma\Lambda_1 = \mathsf{A}_0\Lambda_1$$

oder

$$\Lambda_1(\mathsf{A}_0 - \alpha) = \alpha(\sigma\Lambda_1 - \Lambda_1)$$

daß $\mathsf{A}_0 - \alpha$ genau durch L^v teilbar und somit nach Annahme über α:

$$\mathsf{A}_0 = 1 + \Lambda_v^{(0)}\,.$$

Nach (2) gilt nun:

$$n(\mathsf{A}_0) = n(1 + \Lambda_v^{(0)}) \equiv 1 + S(\Lambda_v^{(0)}) + n(\Lambda_v^{(0)}) \mod \mathfrak{l}^{v+1}$$

also nach (4):

$$S(\Lambda_v^{(0)}) + n(\Lambda_v^{(0)}) \equiv 0 \mod \mathfrak{l}^{v+1} \tag{5}$$

Jede Zahl A kann nun in die Form

$$\mathsf{A} \equiv 1 + \varrho\Lambda_v^{(0)} \mod L^{v+1}$$

gesetzt werden, wo ϱ prim zu L und außerdem, da die Zahl der Restklassen nach L und $\mathfrak{l}$ gleich ist, in k liegend angenommen werden kann. Nach (3) und (2) gilt nun, wenn wir den Fall $\varrho \equiv 0\,(L)$ auch zulassen:

$$n(\mathsf{A}) \equiv 1 + \varrho S(\Lambda_v^{(0)}) + \varrho^{\ell} n(\Lambda_v^{(0)}) \mod \mathfrak{l}^{v+1}$$

Es ist also dann und nur dann

$$n(\mathsf{A}) \equiv 1 \mod \mathfrak{l}^{v+1}$$

wenn

$$\varrho S(\Lambda_v^{(0)}) + \varrho^{\ell} n(\Lambda_v^{(0)}) \equiv 0 \mod \mathfrak{l}^{v+1}$$

ist, oder nach (3):

$$\varrho(\varrho^{\ell-1} - 1) n(\Lambda_v^{(0)}) \equiv 0 \mod \mathfrak{l}^{v+1}$$

Da $n(\Lambda_v^{(0)})$ genau durch $\mathfrak{l}^v$ teilbar ist, muß also

$$\varrho(\varrho^{\ell-1} - 1) \equiv 0 \mod \mathfrak{l}$$

sein, was nach dem Fermat'schen Satze nur zutrifft, wenn

170 I

ϱ einer ganzen rationalen Zahl nach $\mathfrak{l}$ kongruent ist. Dies gilt für ϱ genau ℓ nach $\mathfrak{l}$ und somit nach L inkongruente Möglichkeiten, für A also auch ℓ nach $L^{\nu+1}$ inkongruente Möglichkeiten. Damit ist nach dem Gesagten der Fall 3.) für den Modul $\mathfrak{l}^{\nu+1}$ bewiesen.

Bezeichnen wir nun, unter ϱ eine zu $\mathfrak{l}$ prime Zahl aus k verstehend, für positives t mit s_ν [8] die Summen der ν–ten Potenzen von $\varrho\lambda_t\Lambda_v^{(0)}$, so ist s_1 durch $\mathfrak{l}^{v+t}$, $s_2, \ldots$ durch höhere Potenzen, nämlich s_ν mindestens durch $\mathfrak{l}^{\nu t+v+1}$ teilbar ((I), S. 165). Also ist $a_2, a_3, \ldots$ mindestens durch $\mathfrak{l}^{v+t+1}$ teilbar und auch $a_\ell = \pm n(\varrho\lambda_t\Lambda_v^{(0)})$ mindestens durch $\mathfrak{l}^{\ell t+v}$, also $\mathfrak{l}^{v+t+1}$. Es gilt also:

$$n(1+\varrho\lambda_t\Lambda_v^{(0)}) \equiv 1+\varrho\lambda_t S(\Lambda_v^{(0)}) \mod \mathfrak{l}^{v+t+1} \tag{II}$$

Nach (5) ist nun $S(\Lambda_v^{(0)})$ genau durch $\mathfrak{l}^v$ teilbar, sodaß

$$n(1+\varrho\lambda_t\Lambda_v^{(0)}) \equiv 1+\varrho\lambda_{t+v} \mod \mathfrak{l}^{v+t+1} \tag{6}$$

ist. Es sei nun α Normenrest nach $\mathfrak{l}^{v+1}$ und zwar sei

$$n(\mathsf{A}) \equiv \alpha+\beta\lambda'_{t+v} \mod \mathfrak{l}^{t+v+1}$$

d.h. α auch Normenrest nach $\mathfrak{l}^{t+v}$. Dann ist

$$n[\mathsf{A}(1+\varrho\lambda_t\Lambda_v^{(0)})] \equiv \alpha+\left(\alpha\varrho+\beta\frac{\lambda'_{t+v}}{\lambda_{t+v}}\right)\lambda_{t+v} \mod \mathfrak{l}^{t+v+1}$$

Ist nun β durch $\mathfrak{l}$ teilbar, so ist α auch Normenrest nach $\mathfrak{l}^{v+t+1}$, sonst wähle man ϱ so, daß

$$\alpha\varrho+\beta\frac{\lambda'_{t+v}}{\lambda_{t+v}} \equiv 0 \mod \mathfrak{l}$$

was wegen $(\alpha, \mathfrak{l}) = 1$ stets möglich. Dann ist α auch Normenrest nach $\mathfrak{l}^{v+t+1}$, also nach jeder noch so hohen Potenz von $\mathfrak{l}$.

171 I

Da jeder Normennichtrest nach $\mathfrak{l}^{v+1}$ erst recht für höhere Potenzen Normennichtrest ist, und sich jede Restklasse (prim zu $\mathfrak{l}$) nach $\mathfrak{l}^{v+1}$ in gleich viele nach jeder höheren Potenz zerlegt, ist somit 3.) vollständig bewiesen und

[8] ν und v stellenweise optisch schwer unterscheidbar

damit Satz 8.

Satz 9. Ist $\mathfrak{m} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_t^{\nu_t}$ ein Ideal aus k, so ist □□□ irgendein α dann und nur dann Normenrest nach $\mathfrak{m}$, wenn es nach der Potenz $\mathfrak{p}_i^{\nu_i}$ Normenrest ist.

Beweis: 1.) Sei $n(\mathsf{A}) \equiv \alpha \bmod \mathfrak{m}$, so gilt dies erst recht mod $\mathfrak{p}_i^{\nu_i}$.

2.) Sei $n(\mathsf{A}_i) \equiv \alpha \bmod \mathfrak{p}_i^{\nu_i}$ und setzen wir

$$\mathsf{A} \equiv \mathsf{A}_i \mod \mathfrak{p}_i^{\nu_i} \quad \text{für alle } i$$

Da $\mathfrak{p}_i$ in k liegt, ist dann auch

$$\begin{array}{lrcl} & \sigma^\mu \mathsf{A} & \equiv & \sigma^\mu \mathsf{A}_i \mod \mathfrak{p}_i^{\nu_i} \\ \text{also} & n(\mathsf{A}) & \equiv & n(\mathsf{A}_i) \mod \mathfrak{p}_i^{\nu_i} \\ \text{und daher} & n(\mathsf{A}) & \equiv & \alpha \mod \mathfrak{m}, \qquad \text{w.z.b.w.} \end{array}$$

Hieraus und aus Satz 8 folgt unmittelbar:

Satz 10. ist K relativ zyklisch zu k vom Primzahlgrad ℓ und $\mathfrak{D} = \mathfrak{f}^{\ell-1}$, wo $\mathfrak{f} = \prod \mathfrak{p} \prod \mathfrak{l}^{v+1}$ im Sinne von Satz 6 die Relativdiskriminante; gehen ferner in $\mathfrak{D}$ genau d voneinander verschiedene Primideale auf. Ist dann $\mathfrak{m}$ ein beliebiges, durch $\mathfrak{f}$ teilbares Ideal aus k, dann ist von allen zu $\mathfrak{m}$ primen und nach $\mathfrak{m}$ inkongruenten Zahlen von k genau der ℓ^d–te Teil Normenrest von K nach $\mathfrak{m}$.

Beweis. Nach Satz 8 kommen nur die in $\mathfrak{D}$ aufgehenden Primideale in Frage. Diese sind aber, da $\mathfrak{m}$ durch $\mathfrak{f}$ teilbar in $\mathfrak{m}$ immer in einer solchen Potenz enthalten, daß genau

der ℓ–te Teil aller Restklassen nach dieser Potenz Normenreste sind. Da d solche Potenzen in $\mathfrak{m}$ aufgehen, folgt der Satz.

c) Einheiten

c.) Einheiten im relativ–zyklischen Körper von Primzahlgrad.

Es sei in K ein Strahl O gegeben von der speziellen Eigenschaft, daß er gegenüber den Substitutionen von K invariant ist, d.h. mit A auch $\sigma\mathsf{A}$ Strahlzahl ist. Die Gesamtheit der in k enthaltenen Zahlen von O, d.h. der Durchschnitt von O mit k bildet dann auch einen Strahl o. Dann ist α_0 Zahl aus o und $\alpha_0 \equiv \mathsf{A}_0 \bmod \mathfrak{M}$ die Kongruenzbedingung, aus deren Bestehen die Zugehörigkeit von α_0 zu dem Strahl O mod $\mathfrak{M}$ erschlossen wird, so können wir in jeder solchen Bedingung A_0 durch α_0 ersetzen. Dies denken wir uns für

alle in Betracht kommenden Restklassen getan. Ist dann α irgend eine andere Zahl aus o und $\alpha \equiv \alpha_0 \bmod \mathfrak{M}$, ferner $\mathfrak{m}$ das kleinste Ideal aus k, welches durch $\mathfrak{M}$ teilbar ist, so ist auch $\alpha \equiv \alpha_0 \bmod m$. Ist andererseits $\alpha \equiv \alpha_0 \bmod \mathfrak{m}$, dann erst recht mod $\mathfrak{M}$, sodaß nur noch die Vorzeichenbedingungen zu prüfen sind. Nun sind aber die konjugierten zu α in k und K die Gleichen, die Vorzeichenbedingungen übertragen sich also ohne weiteres.

Auf diese Strahlen O und o sollen sich die folgenden Sätze beziehen.

Es seien R und r die Anzahl der Grundeinheiten in K und k, also auch in O und o.

Ist ℓ ungerade, so gilt folgendes: Ist k_i ein reeller zu k konjugierter Körper, so ist auch K_i reell. Denn eine Gleichung ungeraden Grades mit reellen Koeffizienten, hat mindestens eine reelle Wurzel, und da K_i Galoissch zu k ist, sind alle Wurzeln reell, also auch K_i

Ist aber k_i komplex, so ist natürlich auch K_i komplex. Jedem reellen k_i sind also ℓ reelle konjugierte (zusammenfallende) Körper K_i zugeordnet, ebenso jedem komplexen k_i ℓ komplexe K_i. Es ist also

$$R_1 = \ell r_1 \qquad R_2 = \ell r_2$$
$$R = R_1 + R_2 - 1 = \ell(r_1 + r_2 - 1) + \ell - 1 = \ell r + \ell - 1$$

Somit:

$$\textbf{(1)} \qquad \boldsymbol{R - r = (\ell - 1)(r + 1).}$$

Ist aber $\ell = 2$, also $K = k(\sqrt{\mu})$, wo μ ein Nichtquadrat aus k ist, so sei ν die Anzahl derjenigen reellen, zu k konjugierten Körper, in denen μ negativ ausfällt. Dann ist:

$$R_2 = 2r_2 + \nu \qquad R_1 = 2(r_1 - \nu)$$

also:

$$R = R_1 + R_2 - 1 = 2(r_1 + r_2 - 1) + 1 - \nu = 2r + 1 - \nu$$

also:

$$\textbf{(2)} \qquad \boldsymbol{R - r = r + 1 - \nu.}$$

Wir führen jetzt folgende symbolische Schreibweise ein:

$$\mathsf{A}^{a_0}(\sigma\mathsf{A})^{a_1}\ldots(\sigma^\kappa\mathsf{A})^{a_\kappa}=\mathsf{A}^{a_0+\sigma a_1+\cdots+\sigma^\kappa a_\kappa}=\mathsf{A}^{F(\sigma)}$$

wo die a_i ganze rationale (pos. od. neg.) Zahlen sind. Ersichtlich gilt:

$$\begin{array}{rcll}
\mathsf{A}^{F(\sigma)}\cdot\mathsf{A}^{\phi(\sigma)} & = & \mathsf{A}^{F(\sigma)+\phi(\sigma)} & ;\ \big(\text{da}\quad (\sigma^\kappa\mathsf{A})^{a_\kappa}\cdot(\sigma^\kappa\mathsf{A})^{b_\kappa}=(\sigma^\kappa\mathsf{A})^{a_\kappa+b_\kappa}\big)\\
\mathsf{A}^{F(\sigma)}\cdot\mathsf{B}^{F(\sigma)} & = & (\mathsf{AB})^{F(\sigma)} & ;\ \big(\text{da}\quad (\sigma^\kappa\mathsf{A})^{a_\kappa}\cdot(\sigma^\kappa\mathsf{B})^{a_\kappa}=(\sigma^\kappa\mathsf{AB})^{a_\kappa}\big)\\
\dfrac{1}{\mathsf{A}^{F(\sigma)}} & = & \mathsf{A}^{-F(\sigma)} & ;\\
\big(\sigma^i(\mathsf{A}^{F(\sigma)})\big)^\kappa & = & \big(\mathsf{A}^{\sigma^i F(\sigma)}\big)^\kappa & \\
 & = & \mathsf{A}^{\kappa\sigma^i F(\sigma)} & \\
 & = & \big(\mathsf{A}^{F(\sigma)}\big)^{\kappa\sigma^i} & ;
\end{array}$$

also allgemein: $\big(\mathsf{A}^{F(\sigma)}\big)^{\phi(\sigma)}=\mathsf{A}^{F(\sigma)\cdot\phi(\sigma)}$

sodaß mit den symbolischen Potenzen wie mit gewöhnlichen gerechnet werden kann.

174 I

Speziell ist:

$$n(\mathsf{A})=\mathsf{A}^{1+\sigma+\cdots+\sigma^{\ell-1}}.$$

Satz 11. Im Strahl O gibt es ein System von n Einheiten $\mathsf{H}_1,\mathsf{H}_2,\ldots,\mathsf{H}_n$, sodaß jede Einheit E aus O in der Form

$$\mathsf{E}=\mathsf{H}_1^{u_1}\ldots\mathsf{H}_n^{u_n}\mathsf{H}^{1-\sigma}\ [\xi] \tag{3}$$

darstellbar ist, wo die u_i Zahlen der Reihe $0,1,\ldots,\ell-1$ sind, die durch E eindeutig festgelegt sind, H eine Einheit aus O und $[\xi]$ eine Einheit aus o ist, oder aber eine solche Einheit aus O, deren ℓ–te Potenz in o liegt. Die Einheiten $\mathsf{H}_1,\ldots,\mathsf{H}_n$ sind in dem Sinne voneinander unabhängig, daß $\mathsf{E}=1$ notwendig $u_1=\cdots=u_n=0$ nach sich zieht. Die Zahl n ist:

$$\begin{array}{rcll}
n & = & r+1 & \text{wenn}\quad \ell \text{ ungerade}\\
n & = & r+1-\nu & \text{ll}\quad \ell=2.
\end{array}$$

Beweis. Wie früher ist $1+\sigma+\cdots+\sigma^{\ell-1}=\ell+(\sigma-1)Q(\sigma)$ (S. 152▸, Mitte). Setzt man, wenn E irgendeine Einheit in O ist, $\mathsf{E}^{+Q(\sigma)}=\mathsf{E}_1$, so ist $n(\mathsf{E})=\mathsf{E}^\ell\mathsf{E}_1^{-(1-\sigma)}$, also, da $n(\mathsf{E})$ eine Einheit aus k und somit als Produkt der konjugierten aus o ist,

$$\mathsf{E}^\ell=\mathsf{E}_1^{1-\sigma}\ [\xi]$$

die $\boldsymbol{\ell}$–te Potenz einer jeden Einheit ist also in der Form $\mathsf{H}^{\mathbf{1-\sigma}}\,[\boldsymbol{\xi}]$ enthalten. Ferner ist

$$\mathsf{H}_1^{1-\sigma}\,[\xi]\cdot\mathsf{H}_2^{1-\sigma}\,[\xi']=(\mathsf{H}_1\mathsf{H}_2)^{1-\sigma}\,[\xi\xi']$$

Die Form $\mathsf{H}^{1-\sigma}[\xi]$ bildet also eine Untergruppe der Einheiten in O, die den Einheitenverband E^ℓ (Hauptverband) enthält, und somit, da es nur endlich viele Einheitenverbände gibt, ebenfalls sicher einen endlichen Index haben muß.

175 I

Die Nebengruppen zu der Untergruppe $\mathsf{H}^{(1-\sigma)}[\xi]$ bilden eine Abelsche Gruppe von endlichem Grad. Da jede solche Nebengruppe zum Exponenten ℓ gehört, wie wir eben zeigten, ist der Grad der Faktorgruppe, also der Index von $\mathsf{H}^{(1-\sigma)}[\xi]$ zu O gleich einer Potenz ℓ^n, □□□ und der Typus $(\ell,\ell,\ldots,\ell)$; (n mal). Jede Nebengruppe ist

$$\mathsf{N}_i=\mathsf{H}_i(\mathsf{H}^{1-\sigma}[\xi])$$

Bilden $\mathsf{N}_1,\ldots,\mathsf{N}_n$ eine Basis der Faktorgruppe und sind $\mathsf{H}_1,\ldots,\mathsf{H}_n$ erzeugende Elemente von $\mathsf{N}_1,\ldots,\mathsf{N}_n$ so folgt leicht für jedes H unsere behauptete Darstellung (3). Aus der Eindeutigkeit der Basisdarstellung folgt die Unabhängigkeit der H_i. Es ist also nur noch die Zahl n zu ermitteln.

Sei also E in der Form (3) dargestellt. Da sich die Einheit H wieder in der Form

$$\mathsf{H}=\mathsf{H}_1^{u_1'}\ldots\mathsf{H}_n^{u_n'}\mathsf{H}'^{(1-\sigma)}\,[\xi']$$

darstellen lassen muß, und $[\xi']^{1-\sigma}$ nach Definition von $[\xi]$ entweder 1 oder eine primitive ℓ–te Einheitswurzel ζ sein kann,

$$(\text{aus } [\xi']^\ell=\varepsilon;\quad [\sigma\xi']^\ell=\sigma\varepsilon=\varepsilon\qquad\text{folgt ja}\qquad ([\xi']^{1-\sigma})^\ell=1)$$

und ferner sicher nur dann ein ζ ist, wenn $[\xi']\neq\sigma[\xi']$, also $[\xi']$ den Körper K erzeugt, so daß, da ζ einer Gleichung $(\ell-1)$ ten Grades genügt, dann ζ in k also als Quotient der konjugierten $[\xi']$ und $\sigma[\xi']$ aus O in o enthalten sein muß, so kann man setzen:

$$\mathsf{E}=\mathsf{H}_1^{u_1+u_1'(1-\sigma)}\ldots\mathsf{H}_n^{u_n+u_n'(1-\sigma)}\mathsf{H}^{(1-\sigma)^2}\,[\xi]$$

So fortfahrend kommen wir zu

$$\mathsf{E}=\mathsf{H}_1^{F_1(\sigma)}\ldots\mathsf{H}_n^{F_n(\sigma)}\mathsf{H}^{(1-\sigma)^{\ell-1}}\,[\xi]$$

wo $F_i(\sigma) = u_i + u_i'(1-\sigma) + \cdots + u_i^{(\ell-2)}(1-\sigma)^{\ell-2}$ ist,

und die $u_i^{(\kappa)}$ Zahlen der Reihe $0, 1, \ldots, \ell-1$ sind.

Wir untersuchen nun die Annahme, es sei

$$1 = \mathsf{H}_1^{F_1(\sigma)} \ldots \mathsf{H}_n^{F_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-1}} [\xi].$$

Indem wir von $F_i(\sigma)$ den durch $(1-\sigma)$ teilbaren Term zu $\mathsf{H}^{(1-\sigma)^{\ell-1}}$ ziehen, folgt nach dem schon bewiesenen

$$u_i = 0; \quad (i = 1, 2, \ldots, n).$$

Also kann man für $\ell = 2$ schon schließen: $F_i(\sigma) = 0$. Für ungerades ℓ aber folgt weiter:

$$1 = \left(\mathsf{H}_1^{G_1(\sigma)} \ldots \mathsf{H}_n^{G_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-2}} \right)^{1-\sigma} [\xi]$$

wo $G_i(\sigma) = u_i' + u_i''(1-\sigma) + \cdots + u_i^{(\ell-2)}(1-\sigma)^{\ell-3}$ ist. Diese Relation von der Gestalt $\mathsf{H}^{1-\sigma} = [\xi]$ zieht aber nach sich:

$$n(\mathsf{H}^{1-\sigma}) = 1 - n([\xi])$$

Ist $[\xi]$ aus o, so ist also $[\xi]^\ell = 1$. Ist aber erst $[\xi]^\ell$ in o enthalten, dann sind die konjugierten zu $[\xi]$: $[\xi], \zeta[\xi], \zeta^2[\xi], \ldots$ Also $n[\xi] = [\xi]^\ell$ und ebenfalls $[\xi]^\ell = 1$. Daraus folgt aber $[\xi] = 1$ oder ζ, also entweder $\mathsf{H}^{1-\sigma} = 1$, also $\mathsf{H} = \sigma\mathsf{H}$ in o enthalten, oder $\mathsf{H}^{1-\sigma} = \zeta$, sodaß $\mathsf{H}^\ell = \sigma\mathsf{H}^\ell$ in o enthalten ist. Jedenfalls ist dann H ein $[\xi]$. Daraus folgt, daß

$$1 = \mathsf{H}_1^{G_1(\sigma)} \ldots \mathsf{H}_n^{G_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-2}} [\xi']$$

Drückt man H durch (3) aus, so erhält man eine Darstellung der Form:

$$1 = \mathsf{H}_1^{F_1'(\sigma)+\cdots+F_n'(\sigma)} \mathsf{H}'^{(1-\sigma)^{\ell-1}} [\xi]$$

wo $F_i'(\sigma) = u_i' + u_i''(1-\sigma) + \cdots + u_i^{(\ell-2)}(1-\sigma)^{\ell-3} + v_i(1-\sigma)^{\ell-2}$
Nun folgt wieder, wie oben

$$u_i' = 0; \quad (i = 1, 2, \ldots, n)$$

177 ı

So fortfahrend erhält man also:

Aus $1 = \mathsf{H}_1^{F_1(\sigma)} \dots \mathsf{H}_n^{F_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ folgt $F_i(\sigma) = 0$; $(i = 1, 2, \dots, n)$.

Das bedeutet, daß die $n(\ell-1)$ Einheiten

$$\begin{array}{c} \mathsf{H}_1, \mathsf{H}_1^{(1-\sigma)}, \dots, \mathsf{H}_1^{(1-\sigma)^{\ell-2}} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \mathsf{H}_n, \mathsf{H}_n^{(1-\sigma)}, \dots, \mathsf{H}_n^{(1-\sigma)^{\ell-2}} \end{array}$$

in Bezug auf die Gruppe aller Einheiten $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ unabhängig sind, andererseits aber jede Einheit darstellen (S. 175▸, unten).

□□□

178 ı

Es ist also dieses System von $n(\ell-1)$ Einheiten eine Basis für die Faktorgruppe der Untergruppe $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ in Bezug auf O.

Nun ist, wie sich jetzt zeigen wird, diese Untergruppe identisch mit der Untergruppe $\mathsf{H}^{\ell}[\xi]$ von O, sodaß also die Bestimmung von n zurückgeführt wird auf die Bestimmung der Anzahl der unabhängigen Basiselemente der Faktorgruppe zu der Untergruppe $\mathsf{H}^{\ell}[\xi]$ von O.

Die Identität der Untergruppen $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ und $\mathsf{H}^{\ell}[\xi]$ erkennt man leicht so:

Einerseits ist nach S. 152▸ Mitte identisch in x

$$(1-x)^{\ell-1} = \pm(1 + x + \dots + x^{\ell-1}) + \ell\varphi(x)$$

wo $\varphi(x)$ eine ganze rationale Funktion von x ist, also

$$\begin{aligned} (1-\sigma)^{\ell-1} &= \pm(1 + \sigma + \dots + \sigma^{\ell-1}) + \ell\varphi(\sigma) \\ \mathsf{H}^{(1-\sigma)^{\ell-1}} &= \mathsf{H}^{\pm(1+\sigma+\dots+\sigma^{\ell-1})} \left(\mathsf{H}^{\varphi(\sigma)}\right)^{\ell} \\ &= \mathsf{H}_1^{\ell}[\xi']; \quad ([\xi'] \text{ aus } o) \end{aligned}$$

d.h. $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi] = \mathsf{H}_1^{\ell}[\xi\xi']$.

Andrerseits ist bekanntlich (Kreisteilungstheorie!)

$$\ell = (1-\zeta)^{\ell-1} \cdot \varphi(\zeta)$$

(da ℓ durch $(1-\zeta)^{\ell-1}$ teilbar), wo $\varphi(\zeta)$ eine ganze ganzz. Funktion von ζ. Da nun der Körper $k(\zeta)$ mit dem Kongruenzkörper

$[\ldots]$ $(x, \bmod 1 + x + \cdots + x^{\ell-1})$ isomorph ist, gilt

also identisch in x, (was man auch leicht direkt nachweist):

$$\ell = (1-x)^{\ell-1}\varphi(x) + (1 + x + \cdots + x^{\ell-1})\psi(x)$$

mit ganzem ganzz. $\psi(x)$. Daher

$$\ell = (1-\sigma)^{\ell-1}\varphi(\sigma) + (1 + \sigma + \cdots + \sigma^{\ell-1})\psi(\sigma)$$

$$\mathsf{H}^{\ell} = (\mathsf{H}^{\varphi(\sigma)})^{(1-\sigma)^{\ell-1}} . (\mathsf{H}^{\psi(\sigma)})^{1+\sigma+\cdots+\sigma^{\ell-1}} = \mathsf{H}_1^{(1-\sigma)^{\ell-1}}[\xi'], \quad \text{wo } [\xi'] \text{ aus } o,$$

Damit ist die Identität der beiden Untergruppen gezeigt.

Wir zeigen jetzt weiter, daß die Untergruppe $\mathsf{H}^{\ell}[\xi]$ von O, die offenbar mit einer Einheit H_1 aus O gleichzeitig den ganzen Verband $\mathsf{H}_1\mathsf{H}_0^{\ell}$ aus O enthält, genau ebensoviel Einheitenverbände enthält, wie überhaupt solche in o existieren.

Ist dies gezeigt, dann folgt unsere Behauptung leicht so: Die Zahl der Einheitenverbände in O und o ist ℓ^{R+1} und ℓ^{r+1} bezw. ℓ^{R} und ℓ^{r}, je nachdem O und somit auch o die Einheitswurzel ζ enthält, (ζ genügt einer Gleichung $\boldsymbol{(\ell-1)}$ten Grades) oder nicht. Die Zahl der Nebengruppen von $\mathsf{H}^{\ell}[\xi]$ ist also dann ℓ^{R-r}, und da jede Nebengruppe zum Exponenten ℓ gehört, (da die ℓ–te Potenz jeder Einheit sicher in $\mathsf{H}^{\ell}[\xi]$ enthalten ist), hat die Faktorgruppe dann genau $R-r$ Basiselemente. Es ist also dann

$$n(\ell-1) = R - r = \begin{cases} (\ell-1)(r+1) & ; \quad (\ell \text{ ungerade}) \\ (\ell-1)(r+1-\nu) & ; \quad (\ell = 2) \end{cases}$$

also

$$n = \begin{cases} r+1 & ; \quad (\text{für } \ell \text{ ungerade}) \\ r+1-\nu & ; \quad (\text{für } \ell = 2), \end{cases} \qquad \text{w.z.b.w}$$

Es bleibt also nur noch zu zeigen, daß die Zahl der Einheitenverbände der Form $[\xi]\mathsf{H}^{\ell}$ genau so groß ist, wie die Zahl der Verbände in o. Dazu ordnen wir jedem Verband $[\xi]\mathsf{H}^{\ell}$ in O gegenseitig eindeutig einen Verband in o zu.

Ist zunächst in O keine Einheit vorhanden, deren ℓ–te Potenz in o liegt, so sind alle $[\xi]$ Einheiten ξ aus o. Dann ordnen wir dem Verband $\xi\mathsf{H}^{\ell}$ in O den Verband $\xi\eta^{\ell}$ in o zu und umgekehrt. Es bleibt zu zeigen, daß diese

Zuordnung gegenseitig eindeutig ist. Sind ξ_1 und ξ_2 zwei Einheiten aus o, die in O verschiedene Verbände liefern, so liefern sie natürlich auch in o verschiedene Verbände. Liefern umgekehrt ξ_1 und ξ_2

180 I

□□□

in o verschiedene Verbände, ist also $\frac{\xi_1}{\xi_2}$ nicht ℓ–te Potenz einer Einheit in o, so könnte es a priori doch ℓ–te Potenz einer Einheit in O sein, sodaß ξ_1 und ξ_2 in O denselben Verband ergäben. Dann existierte jedoch in O ein H, sodaß H^ℓ eine Einheit $\frac{\xi_1}{\xi_2}$ aus o ergäbe, entgegen der Voraussetzung.

Da ξ jede beliebige Einheit aus o bedeuten kann, hat also O ebensoviel Verbände $\xi\mathsf{H}^\ell$ wie o überhaupt.

Etwas komplizierter wird die entsprechende Betrachtung für den allgemeinen Fall, daß in O Einheiten $[\xi]$ existieren, deren ℓ–te Potenz in o liegt.

□□□

181 I

□□□

In diesem Falle ist der Körper K offenbar gleich $(k, \sqrt[\ell]{\xi_0})$, wo ξ_0 eine Einheit in o ist, und $[\xi_0] = \sqrt[\ell]{\xi_0}$ ist eine solche Einheit in O. Dann muß ferner jede Einheit $[\xi]$ in O, deren ℓ–te Potenz in o liegt, sich schreiben lassen: °

$$[\xi] = [\xi_0]^{u_0}\xi'; \qquad (\xi' \text{ aus } o)$$

Sei nun $\xi_0, \xi_1, \ldots, \xi_\kappa$ eine Basis für die Gruppe der Einheitenverbände in o, in die offenbar ξ_0 aufgenommen werden darf, so bilden demnach die Einheiten $[\xi_0], \xi_0, \xi_1, \ldots, \xi_\kappa$ eine Basis für die □□□ Einheitenverbände $[\xi]\mathsf{H}^\ell$ in O. In dieser Basis darf noch das Element ξ_0 als ℓ–te Potenz in O weggelassen werden. Es ist dann noch nachzuweisen, daß die $\ell^{\kappa+1}$ Verbände in O:

$$[\xi_0]^{u_0}\xi_1^{u_1}\ldots\xi_\kappa^{u_\kappa}\mathsf{H}^\ell; \quad (u_i = 0, 1, 2, \ldots, \ell-1)$$

sämtlich verschieden sind. Wäre dies nun nicht der Fall, so bestünde eine Relation:

$$[\xi_0]^{v_0}\xi_1^{v_1}\ldots\xi_\kappa^{v_\kappa} = [\xi_0]^{v_0}\xi = \mathsf{H}^\ell$$

□□□

Da $n[\xi_0] = n(\sqrt[\ell]{\xi_0}) = (-1)^{\ell-1}\xi_0$ ist, folgte *für ungerades* ℓ:

$$\xi_0^{v_0}\xi^\ell = \big(n(\mathsf{H})\big)^\ell = \eta^\ell; \quad \xi_0^{v_0} = \eta'^\ell$$

was nur für $v_0 = 0$ möglich. Dann wäre also:

$$\xi = \xi_1^{v_1} \dots \xi_\kappa^{v_\kappa} = \mathsf{H}^\ell$$

was nur mit $v_1 = v_2 = \cdots = v_\kappa = 0$ möglich, da sonst H nicht in o liegen kann, und die K definierende Gleichung $x^\ell = \xi_0^{u_0}\xi^\ell$ sein muß.

Für gerades $\ell = 2$ versagt wegen $n[\xi_0] = -\xi_0$ diese Schlußweise. Auch hier folgt aber aus

$$[\xi_0]^{v_0}\xi = (\sqrt{\xi_0})^{v_0}\xi = \mathsf{H}^2$$

□□□

daß $v_0 = 0$ sein muß. Denn für $v_0 = 1$

kann zunächst H nicht in k liegen. Es wäre also die Zahl

$$\mathsf{H} = \pm\sqrt{\pm\sqrt{\varepsilon_0}\cdot\xi}\,,$$

□□□ aus K eine Zahl mit 4 offenbar von einander verschiedenen relativ konjugierten, was unmöglich. Es ist also $v_0 = 0$ und dann folgt alles wir vorher.

Damit ist gezeigt, daß die Anzahl aller Verbände $[\xi]\mathsf{H}^\ell$ in O genau mit der Anzahl der Einheitenverbände in o übereinstimmt, □□□ und damit nach dem schon Gezeigten der Beweis für Satz 11 vollständig erbracht.

Weiter gilt:

Satz 12. Machen die Relativnormen sämtlicher Einheiten in O ℓ^{v_0} Einheitenverbände in o aus, dann gibt es in O

$$\varrho = \begin{cases} r + 1 + \delta - v_0 & ; \quad (\ell \text{ ungerade}) \\ r + 1 + \delta - \nu - v_0 & ; \quad (\ell = 2) \end{cases}$$

Einheiten $\mathsf{E}_1, \dots, \mathsf{E}_\varrho$ mit der Relativnorm 1, sodaß jede Einheit E in O mit der Relativnorm 1 in der Form:

$$\mathsf{E} = \mathsf{E}_1^{u_1} \dots \mathsf{E}_\varrho^{u_\varrho}\mathsf{H}^{1-\sigma}; \quad (u_i = 0, 1, \dots, \ell - 1)$$

darstellbar ist, wo H eine Einheit in O ist. Aus $\mathsf{E} = 1$ folgt notwendig $u_i = 0$. Die Zahl δ ist $= 1$ oder 0 zu setzen, je nachdem o die prim. ℓ–te Einheitswurzel

ϱ enthält oder nicht.

Beweis. 1.) Ist $\eta_0 = n(\mathsf{H})$ so ist $\eta_0\eta^\ell = n(\mathsf{H}\eta)$. Die Relativnormen von Einheiten in O machen also immer ganze Einheitenverbände aus. Die *Gruppe* in o der Relativnormverbände von Einheiten in O ist also Untergruppe der Gruppe aller Einheitenverbände in o und als solche von einem Grade ℓ^{v_0}.

2.) Die *Gruppe* aller Einheiten der Form $\mathsf{H}^{1-\sigma}$ in O hat die Eigenschaft, daß ihre Relativnormen sämtlich 1 sind. Wir betrachten diese Gruppe $\mathsf{H}^{1-\sigma}$ in O als Untergruppe der *Gruppe* aller Einheiten in O, deren Relativnorm 1 ist. Da jede Einheit E in O nach Satz 11

183 I

in der Form darstellbar ist:

$$\mathsf{E} = \mathsf{H}_1^{u_1} \dots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma}[\xi]\,; \qquad (u_i = 0, 1, \dots, \ell - 1)$$

so gilt dies insbesondere auch für die eben genannte Gruppe, deren Rel. Normen 1 sind. Soll $n(\mathsf{E}) = 1$ sein, so ist wegen $n(\mathsf{H}^{1-\sigma}) = 1$ offenbar $n[\xi]$ auf das System der ℓ^n Größen $n(\mathsf{H}_1)^{u_1} \dots n(\mathsf{H}_n)^{u_n})$ beschränkt; die in der Darstellung unserer Gruppe vorkommenden $[\xi]$ haben also die Eigenschaft, daß $n[\xi]$ nur endlich viele Möglichkeiten hat. Daraus folgt aber daß auch $[\xi]$ selbst nur endliche viele Möglichkeiten hat. Denn es ist

$$\begin{array}{cccccccc} \text{für} & \text{ungerades} & \ell & \text{stets} & : & n[\xi] & = & [\xi]^\ell \\ \shortparallel & \text{gerades} & \ell = 2 & \text{und } \xi \text{ in } o & : & n[\xi] & = & [\xi]^2 \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & \text{erst } [\xi]^2 \text{ in } o: & n[\xi] & = & -[\xi]^2\,, \end{array}$$

sodaß auch für $[\xi]$ selbst (ganz roh!) nur endlich viele Möglichkeiten bestehen.

Die Untergruppe $\mathsf{H}^{1-\sigma}$ der Gruppe mit $n(\mathsf{E}) = 1$ hat also einen endlichen Index. Ferner gehört jede Nebengruppe $\mathsf{E} = \mathsf{H}_1^{u_1} \dots \mathsf{H}_n^{u_n}[\xi]\mathsf{H}^{1-\sigma}$ zum Exponenten ℓ. Dann, wie wir S. 174 sahen, ist E^ℓ stets von der Form:

$$\mathsf{E}^\ell = \mathsf{H}_0^{1-\sigma}[\xi_0]$$

□□□

wo $[\xi_0] = n(\mathsf{E})$, also in o liegt. Daher folgt aus $n(\mathsf{E}) = 1$ jetzt: $[\xi_0] = 1$, also $\mathsf{E}^\ell = \mathsf{H}_0^{1-\sigma}$, sodaß E zum Exponenten ℓ in Bezug auf $\mathsf{H}^{1-\sigma}$ gehört.

Aus dem Bewiesenen folgt, daß die Gruppe der Nebengruppen von einem endlichen Grade sein muß, der eine Potenz ℓ^ϱ von ℓ ist, □□□ und daß ihr

Typus $(\ell, \ell, \ldots, \ell)$; ($\varrho$ mal) ist. Also existiert für jede Einheit E mit $n(\mathsf{E}) = 1$ eine Darstellung, wie die behauptete, und diese ist eindeutig in dem Sinne des Satzes, da es die Basisdarstellung der Gruppe unserer Nebengruppen ist. Es bleibt also nur noch der Satz über die Größe von ϱ zu beweisen.

3.) ζ komme in o und also auch in O nicht vor. Dann kann keine Einheit $[\xi]$ existieren, die nicht in o liegt, da sonst K durch eine ℓ'te Wurzel in O erzeugt würde, deren $(\sigma - 1)$ te Potenz ζ wäre. Sei nun nach Satz 11:

$$\mathsf{E}_1 = \mathsf{H}_1^{u_1} \ldots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma}\, \xi$$

□□□

Wären alle $u_i = 0$, so folgte $n(\xi) = \pm\xi^\ell = 1$, also da o keine ℓ–te E.W. (umsomehr für $\ell = 2$ keine $2\ell = 4$ te E.W.) enthält, $\xi = 1$; $\mathsf{E}_1 = \mathsf{H}^{1-\sigma}$ entgegen der Voraussetzung, daß E_1 Basiselement für die Gruppe der Nebengruppen zu $\mathsf{H}^{1-\sigma}$. Sei also etwa $u_1 \neq 0$. Dann kann in der Basis $\mathsf{H}_1, \ldots, \mathsf{H}_n$ offenbar H_1 durch E_1 ersetzt werden. Nun sei weiter

$$\mathsf{E}_2 = \mathsf{E}_1^{a_1} \mathsf{H}_2^{u_2} \ldots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma} \xi$$

Wären alle $u_i = 0$, so wäre, wie vorhin $\xi = 1$, also $\mathsf{E}_2 = \mathsf{E}_1^{a_1} \mathsf{H}^{1-\sigma}$, was wegen der Unabh. von E_1 u. E_2 in Bezug auf $\mathsf{H}^{1-\sigma}$ nicht geht. Sei also etwa $\overline{u}_2 \neq 0$, dann kann H_2 durch E_2 ersetzt werden. So kann man fortfahren, solange noch E_i da sind. Wären mehr als n E_i vorhanden, so bestünde zwischen ihnen eine Relation, was unmöglich, also $\varrho \leqq n$ und $\mathsf{H}_1 \ldots \mathsf{H}_\varrho$ können durch $\mathsf{E}_1, \ldots \mathsf{E}_\varrho$ ersetzt werden.

In

$$\mathsf{E} = \mathsf{E}_1^{u_1} \ldots \mathsf{E}_\varrho^{u_\varrho} \mathsf{H}_{\varrho+1}^{u_{\varrho+1}} \ldots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma}\, \xi$$

(welche Darstellung für jedes E aus O *eindeutig* möglich ist, Satz 11) kann dabei E nur dann die Relativnorm 1 haben, wenn $u_{\varrho+1}, \ldots, u_n = 0$ sind, da ja ein solches E nach 2.) schon durch die Basis $\mathsf{E}_1, \ldots, \mathsf{E}_\varrho$ darstellbar ist. Setzen wir also:

$$\eta_1 = n(\mathsf{H}_{\varrho+1}); \quad \ldots ; \quad \eta_{n-\varrho} = n(\mathsf{H}_n)$$

so gilt für *jede* Einheit E aus O:

$$n(\mathsf{E}) = \eta_1^{u_{\varrho+1}} \dots \eta_n^{u_n} \xi^\ell; \qquad (0 \leqq u_i < \ell)$$

und zwar eindeutig; denn wäre dies noch auf eine zweite Weise möglich, so existierte eine Darstellung

$$1 = \eta_1^{v_{\varrho+1}} \dots \eta_n^{v_n} \xi'^\ell$$

Die Einheit $\mathsf{E}' = \mathsf{H}_1^{v_{\varrho+1}} \dots \mathsf{H}_n^{v_n} \xi'$ hätte also die Norm 1, und dann muß, wie eben gezeigt $v_{\varrho+1}, \dots, v_n = 0$ sein.

Umgekehrt ist jede in der obenstehenden Form dargestellte Einheit aus o Relativnorm einer sofort angebbaren Einheit aus O. Die Relativnormen machen also $n - \varrho$ unabhängige Einheitenverbände in o aus, sodaß $v_0 = n - \varrho, \varrho = n - v_0 = \begin{cases} r + 1 - v_0 \\ r + 1 - \nu - v_0 \end{cases}$ was wegen $\delta = 0$ die Behauptung ist.

4.) ζ komme in o vor, jedoch in O sei □□□ *nicht* die ℓ–te Wurzel einer Einheit in o enthalten. Dann ist in Satz 11 $[\xi]$ wieder nur eine Einheit ξ aus o, es gibt keine Einheiten $[\xi]$ deren ℓ–te Potenz erst in o liegt. Dann kann auch nicht $\zeta = \mathsf{H}^{1-\sigma}$ sein, □□□ da sonst einerseits H aus O aber nicht aus o wäre, andererseits $\mathsf{H}^\ell = \sigma(\mathsf{H})^\ell$ [9] seinen konjugierten gleich, also H ein $[\xi]$ wäre. Daher kann in 2.) das nicht in $\mathsf{H}^{1-\sigma}$ enthaltene ζ als ein Basiselement E_ϱ genommen werden denn $n(\zeta) = \zeta^\ell = 1$[10]. Seien $\mathsf{E}_1, \dots, \mathsf{E}_{\varrho-1}$ die anderen. Ist dann nach Satz 11:

$$\mathsf{E}_1 = \mathsf{H}_1^{u_1} \dots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma} \xi$$

und wären alle $u_i = 0$, so wäre $n(\mathsf{E}_1) = \xi^\ell = 1$ also $\xi = 1$ oder ζ^i, $\mathsf{E}_1 = \mathsf{H}^{1-\sigma} \zeta^i$ was wegen der Unabhängigkeit der Basiselemente nicht möglich. Wir können also, wie vorhin $\mathsf{H}_1, \dots, \mathsf{H}_{\varrho-1}$ durch $\mathsf{E}_1, \dots, \mathsf{E}_{\varrho-1}$ ersetzen, und haben dann, □□□ nach Satz 11 für jedes E aus O:

$$\mathsf{E} = \mathsf{E}_1^{u_1} \dots \mathsf{E}_{\varrho-1}^{u_{\varrho-1}} \mathsf{H}_\varrho^{u_\varrho} \dots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma} \xi$$

Hat dann E die Rel. Norm 1, so ist es schon durch die Basis $\mathsf{E}_1, \dots, \mathsf{E}_{\varrho-1}, \mathsf{E}_\varrho = \zeta$ darstellbar

$$\mathsf{E} = \mathsf{E}_1^{u'_1} \dots \mathsf{E}_{\varrho-1}^{u'_{\varrho-1}} \zeta^i \mathsf{H}'^{1-\sigma}$$

[9] undeutlich
[10] undeutlich

186 ı

und durch Division:

$$1 = \mathsf{E}_1^{u_1-u_1'} \dots \mathsf{E}_{\varrho-1}^{u_{\varrho-1}-u_{\varrho-1}'} \mathsf{H}_\varrho^{u_\varrho} \dots \mathsf{H}_n^{u_n} \left(\frac{\mathsf{H}}{\mathsf{H}'}\right)^{1-\sigma} \frac{\xi}{\zeta^i}$$

also wegen der Eindeutigkeit nach Satz 11:

$$u_1 - u_1' = 0; \ \dots \ ; \ u_{\varrho-1} - u_{\varrho-1}' = 0$$
$$u_\varrho = \dots = u_n = 0$$

Für alle Relativnormen folgt dann

$$n(\mathsf{E}) = \eta_\varrho^{u_\varrho} \dots \eta_n^{u_n} \xi^\ell ; \quad (u_i = 0, 1, \dots, \ell - 1)$$

und zwar eindeutig, da sonst eine Einheit mit Rel. 1 und $u_\varrho, \dots, u_\kappa \neq 0$ folgte, was eben als unmöglich erkannt. Umgekehrt ist jede solche Einheit aus o Relativnorm. Also $v_0 = n - \varrho + 1$, was wegen $\delta = 1$ unsere Behauptung ergibt.

5.) ζ komme in o vor und in O existiere die ℓ–te Wurzel einer Einheit η_0 aus o. Dann ist

$$K = (k, \sqrt[\ell]{\eta_0})$$

Es sei

$$\mathsf{H}_0 = \sqrt[\ell]{\eta_0}$$

Dann kann man in Satz 11 die Einheiten $[\xi]$ durch $\mathsf{H}_0^u \xi$ (ξ in o, $u = 0, 1, \dots, \ell - 1$) ersetzen. Ferner ist $\zeta = \mathsf{H}_0^{\sigma-1} = \left(\frac{1}{\mathsf{H}_0}\right)^{1-\sigma}$, also ζ in der Gruppe $\mathsf{H}^{1-\sigma}$ enthalten.

□□□

187 ı

Jede Einheit E aus O hat dann eine Darstellung:

$$\mathsf{E} = \mathsf{H}_0^{u_0} \mathsf{H}_1^{u_1} \dots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma} \xi; \quad (u_i = 0, 1, \dots, \ell - 1)$$

Diese Darstellung ist im allgemeinen ebenfalls noch eindeutig, sodaß aus $\mathsf{E} = 1$ folgt $u_0 = u_1 = \dots = u_n = 0$. Denn zunächst folgt nach Satz 11 aus $\mathsf{E} = 1$ daß $u_1 = \dots = u_n = 0$ ist, also:

$$1 = \mathsf{H}_0^{u_0} \mathsf{H}^{1-\sigma} \xi$$

Für *ungerades* ℓ folgt weiter durch Normbildung:

$$1 = \eta_0^{u_0} \xi^\ell$$

also, da η_0 als erzeugendes Element von K nicht ℓ–te Potenz in o sein kann, $u_0 = 0$.

Für $\ell = 2$ ist $n(\mathsf{H}_0) = -\eta_0$. Also folgte, wenn $u_0 = 1$ wäre,

$$1 = -\eta_0 \xi^2$$

□□□

d.h. wenn K nicht durch $\sqrt{-1}$ erzeugt wird, ebenfalls ein Widerspruch. Nur falls K durch $\sqrt{-1}$ erzeugt wird, also $\eta_0 = -\xi_0^2$ in o ist, darf nicht so geschlossen werden. In diesem Falle brauchen wir gleich, daß dann $\mathsf{H}_0 = \sqrt{-\xi_0^2}$ nicht in der Form $\mathsf{H}^{1-\sigma}$ enthalten ist. Denn wäre

$$\sqrt{-\xi_0^2} = \frac{\alpha + \beta\sqrt{-\xi_0^2}}{\alpha - \beta\sqrt{-\xi_0^2}}$$

so folgte $(\alpha - \beta)\sqrt{-\xi_0}^{\,2} = \alpha - \beta\xi_0^2$, also $\alpha = \beta$

$$\sqrt{-\xi_0^2} = \frac{1 + i\xi_0}{1 - i\xi_0} = (1 + i\xi_0)^{1-\sigma}$$

□□□ also wäre $\mathsf{H} = 1 + i\xi_0$. Dies ist aber keine Einheit. Denn $n(\mathsf{H}) = 1 + \xi_0^2$ ist eine Zahl in o die mit ihren sämtlichen konjugierten > 1 also deren Norm in k nicht ± 1 sein kann. Es ist also tatsächlich $\mathsf{H}_0 = \mathsf{H}^{1-\sigma}$ unmöglich.

Sei nun die Darstellung unseres Basiselementes E_1

$$\mathsf{E}_1 = \mathsf{H}_0^{u_0} \dots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma} \xi.$$

Dann können nicht alle $u_0, u_1, \dots, u_n = 0$ sein. Denn sonst wäre $n(\mathsf{E}_1) = 1 = \xi^\ell$ und also $\xi = \zeta$. Da dann $\xi = \zeta$ in $\mathsf{H}^{1-\sigma}$ hineingezogen werden kann, wäre $\mathsf{E}_1 = \mathsf{H}'^{1-\sigma}$ was unmöglich. kann also eins der H_i durch E_1 ersetzt werden.
□□□

So fortfahrend gelangen wir zu einer Darstellung für jedes E aus O:

$$\mathsf{E} = \mathsf{E}_1^{u_1} \dots \mathsf{E}_\varrho^{u_\varrho} \mathsf{H}_\varrho^{u_\varrho} \mathsf{H}_{\varrho+1}^{u_{\varrho+1}} \dots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma} \xi$$

In dem Spezialfalle $\ell = 2$; $\eta_0 = -\xi_0^2$ können wir es dabei sicher so einrichten, daß H_0 nicht mehr unter den $\mathsf{H}_\varrho \square\square\square \ldots \mathsf{H}_n$ vorkommt. Denn dann darf das Element $\mathsf{H}_0 = \sqrt{-\xi_0^2}$ als Basiselement E_1 gewählt werden?, da H_0 nicht $\mathsf{H}^{1-\sigma}$ ist, wie gezeigt.

Ist nun $n(\mathsf{E}) = 1$, so folgt, daß

$$\mathsf{E} = \mathsf{E}_1^{u_1'} \ldots \mathsf{E}_\varrho^{u_\varrho'} \mathsf{H}'^{1-\sigma}$$

also:

$$1 = \mathsf{E}_1^{u_1 - u_1'} \ldots \mathsf{E}_\varrho^{u_\varrho - u_\varrho'} \mathsf{H}_\varrho^{u_\varrho} \mathsf{H}_{\varrho+1}^{u_{\varrho+1}} \ldots \mathsf{H}_n^{u_n} \mathsf{H}^{1-\sigma}\, \xi$$

also jedenfalls $u_\varrho, \ldots, u_n = 0$ *ist*, $\square\square\square$ da diese Darstellung im allgemeinen nach Satz 11 eindeutig und in dem einzigen kritischen Falle $\eta_0 = -\xi_0^2$; $\ell = 2$ die kritische Einheit H_0 nicht unter den $\mathsf{H}_\varrho, \ldots, \mathsf{H}_n$ vorkommt.

Nun ist jedes:

$$n(\mathsf{E}) = \eta_\varrho^{u_\varrho} \ldots \eta_n^{u_n} \xi^\ell$$

und zwar eindeutig, da sonst wie unter 3.) eine Einheit in O mit der Norm 1 existiert, für die die Exponenten von $\mathsf{H}_\varrho, \ldots, \mathsf{H}_n$ nicht alle Null wären. Da andererseits jeder solche Ausdruck eine Relativnorm liefert, ist wieder $v_0 = n - \varrho + 1$, was wegen $\delta = 1$ die Behauptung liefert.

---

d) Anzahl der ambigen Klassen

d.) Die Anzahl der ambigen Klassen im rel.–zykl. Körper von Primzahlgrad.

Zunächst sei bemerkt, daß wir das Rechnen mit symbolischen Potenzen ohne weiteres auf Ideale übertragen können, ebenso auf Idealklassen.

Definition 3. Ein Ideal $\mathfrak{A}$ aus K heißt *ambig*, wenn es nicht in k liegt, und $\mathfrak{A}^{1-\sigma} = 1$, also $\mathfrak{A} = \sigma\mathfrak{A}$ ist. Eine absolute Idealklasse $\mathfrak{K}$ aus K heißt ambig, wenn $\mathfrak{K}^{1-\sigma} = 1$ d.h. $\mathfrak{K} = \sigma\mathfrak{K}$ ist.

$\mathfrak{K}$ ist sicher ambig, wenn es ein ambiges Ideal aus K oder ein Ideal aus k oder das Produkt eines ambigen Ideals mit einem Ideal aus k enthält.

189 ı

Denn ist $\mathfrak{Aj}$ ein solches Produkt, so entsteht die Klasse $\mathfrak{K}$ von $\mathfrak{Aj}$ durch

Multiplikation von $\mathfrak{A}\mathsf{j}$ mit *allen absoluten* Hauptidealen: $\mathfrak{K} = \mathfrak{A}\mathsf{j}(\mathsf{A})$. Also $\sigma\mathfrak{K} = \sigma\mathfrak{A}\ \sigma\mathsf{j}\ (\sigma\mathsf{A}) = \mathfrak{A}\mathsf{j}(\sigma\mathsf{A})$ und (A) durchläuft mit $(\sigma\mathsf{A})$ die sämtlichen absoluten Hauptideale. Dasselbe gilt offenbar auch noch, wenn die Idealklassen nach einem solchen speziellen Strahl O definiert werden, der mit seinen konjugierten gleich ist.

Das Umgekehrte braucht nicht immer der Fall zu sein. Es kann sehr wohl ambige Klassen ohne ambige Ideale geben.

Satz 13. Ein Primideal aus K ist dann und nur dann ambig, wenn es in der Relativdiskriminante von K aufgeht, seine ℓ–te Potenz also Primideal in k ist.

Beweis. Sei $\mathfrak{P}^{1-\sigma} = 1$ und $\mathfrak{p}$ das zugehörige Primideal von k. Dann ist nicht $\mathfrak{p} = \mathfrak{P}$, da sonst $\mathfrak{P}$ ein Ideal in k wäre (Def. 3), auch nicht $\mathfrak{p} = \mathfrak{P}\mathfrak{P}_1 \dots \mathfrak{P}_{\ell-1}$, da sonst $\sigma\mathfrak{P} = \mathfrak{P}_1 = \mathfrak{P}$ wäre. Also $\mathfrak{p} = \mathfrak{P}^\ell$. Umgekehrt ist dann auch $\mathfrak{P} = \sigma\mathfrak{P}$.

Satz 14. Es seien $\mathfrak{P}_1, \dots, \mathfrak{P}_d$ die d verschiedenen in der Relativdiskriminante von K aufgehenden Primideale, die also alle ambig sind. Dann läßt sich jedes Ideal $\mathfrak{A}$, für das $\mathfrak{A}^{1-\sigma} = 1$ ist, eindeutig darstellen:

$$\mathfrak{A} = \mathfrak{P}_1^{u_1} \dots \mathfrak{P}_d^{u_d}\mathfrak{a}$$

wo $\mathfrak{a}$ ein Ideal aus k ist und $u_i = 0, 1, \dots, \ell - 1$. Es ist weiter $\mathfrak{A}$ dann und nur dann in k enthalten, wenn $u_1 = \dots = u_d = 0$ ist. Soll zudem $\mathfrak{A}$ Hauptideal in k sein, so muß $\mathfrak{a}$ Hauptideal sein.

Beweis. Aus $\mathfrak{A} = \sigma\mathfrak{A} = \sigma^2\mathfrak{A} = \dots = \sigma^{\ell-1}\mathfrak{A}$ folgt:

$$n(\mathfrak{A}) = \mathfrak{A}^\ell$$

Es ist also $\mathfrak{A}^\ell$ ein Ideal aus k. Ginge nun in $\mathfrak{A}$ ein $\mathfrak{P}^\lambda$ auf, wo $\mathfrak{P}$ ein nicht ambiges Primideal aus K und auch nicht Ideal aus k ist, sodaß $\mathfrak{p} = \mathfrak{P}\mathfrak{P}_1^{(0)} \dots \mathfrak{P}_{\ell-1}^{(0)}$ wäre, so ist $\mathfrak{A}^\ell$ durch $\mathfrak{P}^{\lambda\ell}$ teilbar und Ideal aus k, also durch $\mathfrak{p}^{\lambda\ell}$ teilbar. Somit ist

$\mathfrak{A}$ selbst durch $\mathfrak{p}^\lambda$ teilbar. □□□ Jedem einzelnen Faktor $\mathfrak{P}^\lambda$ entspricht also gleich der ganze Faktor $\mathfrak{p}^\lambda$ aus k. $\mathfrak{A}$ hat also die angegebene Form, in der die u_i in der angegebenen Weise reduziert werden dürfen, da $\mathfrak{P}_i^\ell$ in k liegt. Diese Darstellung ist eindeutig, da die Zerlegung in Primideale in K eindeutig ist. Liegt $\mathfrak{A}$ in k, so muß $\mathfrak{P}_1^{u_1} \dots \mathfrak{P}_d^{u_d}$ in k liegen, also durch $\mathfrak{p}_i = \mathfrak{P}_i^\ell$ teilbar sein,

falls $\mathfrak{P}_i$ vorkommt. Das geht nur für $u_i = 0$. Alles weitere folgt daraus. Die Darstellung gilt offenbar auch für gebrochene $\mathfrak{A}$, dann ist auch $\mathfrak{a}$ gebrochen.

Satz 15. Die Gruppe der Ideale $\mathfrak{A}$ aus K, für die $\mathfrak{A}^{1-\sigma} = 1$ ist, hat in Bezug auf die Untergruppe der Hauptideale (in absolutem Sinne) aus k den Index $\ell^d h$, wo h die absolute Klassenzahl und d die Anzahl der Diskriminantenteiler ist. In Bezug auf die Untergruppe der absoluten Hauptideale (A) aus K, für die $(\mathsf{A})^{1-\sigma} = 1$ ist, hat sie den Index $h\ell^{d-\varrho}$, wo ϱ die Bedeutung von Satz 12 hat, d.h. von der Gruppe $\mathfrak{A}^{1-\sigma} = 1$ werden genau $h \cdot \ell^{d-\varrho}$ Idealklassen in K im absoluten Sinne erzeugt.

Beweis. 1.) Der erste Teil folgt sofort aus Satz 14.

2.) Sei D die Untergruppe der Hauptideale aus K, die in unserer Gruppe $\mathfrak{A}^{1-\sigma} = 1$ vorkommen, D_0 die der Hauptideale aus k, die sicher alle in unserer Gruppe vorkommen. Ist dann $(\mathsf{D} : \mathsf{D}_0)$ der Gruppenindex, so gilt wegen der multiplikativen Eigenschaft des Gruppenindex, da $\mathfrak{A}^{1-\sigma} = 1$, D, D_0 ineinander geschachtelte Untergruppen sind

$$h\ell^d = j \cdot (\mathsf{D}, \mathsf{D}_0)$$

wenn j der gesuchte Index unserer Gruppe $\mathfrak{A}^{1-\sigma} = 1$ zu D ist. Es ist also $j = \frac{h\ell^d}{(\mathsf{D}:\mathsf{D}_0)}$ und somit $(\mathsf{D} : \mathsf{D}_0) = \ell^{\varrho}$ nachzuweisen.

Wir beweisen zunächst:

Hilfssatz. Ist A eine ganze oder gebrochene Zahl aus K mit $n(\mathsf{A}) = 1$, so gibt es eine ganze Zahl B aus K, sodaß $\mathsf{A} = \mathsf{B}^{1-\sigma}$ ist.

Beweis. Wir wählen m ganz rational so, daß

$$\mathsf{B} = m(1 + \mathsf{A}^1 + \mathsf{A}^{1+\sigma} + \cdots + \mathsf{A}^{1+\sigma+\cdots+\sigma^{\ell-2}})$$

eine ganze Körperzahl aus K wird. Dann ist

$$\begin{aligned}\mathsf{B}^{1-\sigma} &= \frac{1 + \mathsf{A}^1 + \mathsf{A}^{1+\sigma} + \cdots + \mathsf{A}^{1+\sigma+\cdots+\sigma^{\ell-2}}}{1 + \mathsf{A}^{\sigma} + \mathsf{A}^{\sigma+\sigma^2} + \cdots + \mathsf{A}^{\sigma+\sigma^2+\cdots+\sigma^{\ell-1}}} \\ &= \frac{1 + \mathsf{A}^1 + \mathsf{A}^{1+\sigma} + \cdots + \mathsf{A}^{1+\sigma+\cdots+\sigma^{\ell-2}}}{\mathsf{A}^{-1}\left(\mathsf{A} + \mathsf{A}^{1+\sigma} + \mathsf{A}^{1+\sigma+\sigma^2} + \cdots + \mathsf{A}^{1+\sigma+\sigma^2+\cdots+\sigma^{\ell-1}}\right)} = \mathsf{A}\end{aligned}$$

(Es könnte $\mathsf{B} = 0$ sein, siehe Zahlbericht!).

Da nun die Einheiten $\mathsf{E}_1, \ldots, \mathsf{E}_\varrho$ von Satz 12 für $O = K$, $o = k$ sämtlich die Norm 1 haben, gibt es ganze Zahlen $\mathsf{A}_1, \ldots, \mathsf{A}_\varrho$ in K, sodaß

$$\mathsf{E}_i = \mathsf{A}_i^{1-\sigma}$$

ist. A_i ist sicher keine Einheit, da □□□ nach Satz 12 E_i von der Gruppe $\mathsf{H}^{1-\sigma}$ unabhängig ist. Also ist, wenn $\mathfrak{A}_i = (\mathsf{A}_i)$ gesetzt wird:

$$\mathfrak{A}_i^{1-\sigma} = 1; \qquad \mathfrak{A}_i \neq 1.$$

Wäre nun

$$\mathfrak{A}_1^{u_1} \ldots \mathfrak{A}_\varrho^{u_\varrho} = (\alpha); \quad (\alpha) \text{ in } k$$

so würde folgen

$$\mathsf{A}_1^{u_1} \ldots \mathsf{A}_\varrho^{u_\varrho} = \alpha\mathsf{H}; \qquad \mathsf{H} \text{ Einheit in } K$$

Also $\quad \mathsf{E}_1^{u_1} \ldots \mathsf{E}_\varrho^{u_\varrho} = \mathsf{H}^{1-\sigma}$

woraus, wie eben, $u_1 = u_2 = \cdots = u_\varrho = 0$ folgt.

Ist andererseits $\mathfrak{A} = (\mathsf{A})$ ein Hauptideal aus K und $\mathfrak{A}^{1-\sigma} = 1$, so ist also $\mathsf{A}^{1-\sigma} = \mathsf{E}$, wo E Einheit in K ist, für die

$$n(\mathsf{E}) = \mathsf{A}^{(1-\sigma)(1+\sigma+\cdots+\sigma^{\ell-1})} = \mathsf{A}^{1-\sigma^\ell} = 1$$

ist. Demnach gilt:

$$\mathsf{E} = \mathsf{E}_1^{u_1} \ldots \mathsf{E}_\varrho^{u_\varrho} \mathsf{H}^{1-\sigma}$$

oder $\qquad \mathsf{A}^{1-\sigma} = \left(\mathsf{A}_1^{u_1} \ldots \mathsf{A}_\varrho^{u_\varrho} \mathsf{H}\right)^{1-\sigma}.$

192 I

Nun zieht aber $\mathsf{A}^{1-\sigma} = \mathsf{B}^{1-\sigma}$ nach sich:

$$\left(\frac{\mathsf{A}}{\mathsf{B}}\right)^{1-\sigma} = 1$$

$$\frac{\mathsf{A}}{\mathsf{B}} = \sigma\left(\frac{\mathsf{A}}{\mathsf{B}}\right) = \cdots = \text{Zahl } \alpha \text{ aus } k.$$

Es ist also $\quad \mathsf{A} = \mathsf{A}_1^{u_1} \ldots \mathsf{A}_\varrho^{u_\varrho} \mathsf{H}\alpha$

oder für die Hauptideale

□□□

$$\mathfrak{A} = \mathfrak{A}_1^{u_1} \ldots \mathfrak{A}_\varrho^{u_\varrho} \ (\alpha)$$

wo (α) Hauptideal aus k und $u_i = 0, 1, \ldots, \ell - 1$. Die Ideale $\mathfrak{A}_1, \ldots, \mathfrak{A}_\varrho$ haben also die Eigenschaft, daß sie □□□ eine Basis für die Gruppe D aller Hauptideale $\mathfrak{A} = (\mathsf{A})$ mit $\mathfrak{A}^{1-\sigma} = 1$ aus K in Bezug auf die Gruppe D_0 aller Hauptideale in k bilden. Jedes Element der Basis gehört nach Satz 14 genau zum Exponenten ℓ, es ist also der Index $(\mathsf{D} : \mathsf{D}_0) = \ell^\varrho$, w.z.b.w.

Satz 16. Die Idealklassen von K und k seien wieder im absoluten Sinne definiert. ℓ^v bedeute die Anzahl der Einheitenverbände in k, die durch Relativnormen von Einheiten und gebrochenen Zahlen von K gebildet sind. Die übrigen Größen seien wie bisher definiert, insbesondere für $\ell = 2$ die Zahl ν wie früher. Ist a die Anzahl der ambigen Klassen in K, so gilt:

$$a = h \cdot \ell^{d+v-(r+1+\delta)} \qquad \text{für ungerades } \ell$$
$$a = h \cdot 2^{d+v+\nu-(r+2)} \qquad \text{für } \ell = 2 \text{ (also } \delta = 1)$$

Beweis. 1.) Ist $n(\theta) = \varepsilon$, wo ε Einheit in k, so ist für jede Einheit □□□ η: $\varepsilon\eta^\ell = n(\theta\eta)$. Unsere Normen machen also wirklich ganze Verbände aus.

193 I

2.) Die ℓ^ν [11] Relativnormverbände in k bilden eine Abelsche Gruppe, in der jedes Element den Exponenten ℓ hat. Außer den v_0[12] nach Satz 12 in k vorhandenen Basiselementen gibt es also noch $\nu - v_0$ davon unabhängige Einheiten in k, die als Normen gebrochener Zahlen geliefert werden. Es seien dies:

$$\varepsilon_1 = n(\Theta_1);\ \ldots;\ \varepsilon_{\nu-v_0} = n(\Theta_{\nu-v_0})$$

Dann hat also, wenn wir die Normen von Einheiten zusammenziehen, ebenso die ℓ–ten Potenzen von Einheiten in k als Normen schreiben, jede Relativnormeinheit aus k die Gestalt:

$$\varepsilon = \varepsilon_1^{u_1} \ldots \varepsilon_{\nu-v_0}^{u_{\nu-v_0}} n(\mathsf{H})\ ;\ \left(\begin{array}{l} u_i = 0, 1, \ldots, \ell - 1 \\ \mathsf{H} \text{ Einheit aus } K \end{array} \right)$$

in der die u_i eindeutig festgelegt sind (Basis einer Abelschen Gruppe). Da insbesondere $1 = n(1)$ ist, kann

$$1 = \varepsilon_1^{v_1} \ldots \varepsilon_{\nu-v_0}^{v_{\nu-v_0}} n(\mathsf{H}')$$

[11] undeutlich
[12] ν und v optisch tw. nicht unterscheidbar

nur für $v_1 = \cdots = v_{\nu-v_0} = 0$ bestehen.

Es sei nun symbolisch:

$$(\Theta_i) = \prod \mathfrak{P}^{F_i(\sigma)}$$

erstreckt über die verschiedenen nicht zu einander konjugierten Primideale von Θ_i in K. Wegen $n(\Theta_i) = \varepsilon_i$ ist also:

$$n[(\Theta_i)] = \prod \mathfrak{P}^{(1+\sigma+\cdots+\sigma^{\ell-1})F_i(\sigma)} = 1.$$

□□□

Nun ist: □□□

$$F_i(\sigma) = \phi_i(\sigma-1)\cdot(\sigma-1) + a_i$$

ist, wenn nach Potenzen von $(\sigma-1)$ entwickelt wird, also

$$(1+\sigma+\cdots+\sigma^{\ell-1})F_i(\sigma) = (\sigma^\ell - 1)\phi_i(\sigma-1) + a_i(1+\sigma+\cdots+\sigma^{\ell-1})$$

und daher

$$1 = \prod \mathfrak{P}^{(\sigma^\ell-1)\phi_i(\sigma-1)}\mathfrak{P}^{a_i(1+\sigma+\cdots+\sigma^{\ell-1})} = \prod n(\mathfrak{P})^{a_i}$$

also $a_i = 0$ und $F_i(\sigma)$ durch $1-\sigma$ teilbar. Es kann also gesetzt werden

$$(\Theta_i) = \mathfrak{A}_i^{1-\sigma}$$

wo $\mathfrak{A}_i$ ein ganzes oder gebrochenes Ideal aus K ist. Setzen wir wieder

$$\ell = (1+\sigma+\cdots+\sigma^{\ell-1})\varphi(\sigma) + (1-\sigma)\psi(\sigma) \qquad \text{(S. 178▸)}.$$

so wird

$$\mathfrak{A}_i^\ell = n(\mathfrak{A}_i)^{\varphi(\sigma)}\cdot(\mathfrak{A}_i^{1-\sigma})^{\psi(\sigma)} = \mathfrak{a}_i(\theta_i)^{\psi(\sigma)}$$

Wäre

$$\mathfrak{A}_1^{u_1}\ldots\mathfrak{A}_{\nu-v_0}^{u_{\nu-v_0}} = \overline{\mathfrak{A}}\,(\mathsf{A}), \quad \text{wo} \quad \overline{\mathfrak{A}}^{1-\sigma} = 1$$

und (A) Ideal aus K, so können nach dem eben gezeigten alle Exponenten $u_i = 0, 1, \ldots, \ell-1$ angenommen werden, da der Faktor $\mathfrak{a}_i$ unbeschadet $\overline{\mathfrak{A}}^{1-\sigma} =$

1 zu $\overline{\mathfrak{A}}$ und der Faktor $(\Theta_i)^{\psi(\sigma)}$ zu (A) genommen werden kann. Dann folgte durch Erheben in die $(1-\sigma)$ te Potenz:

$$\Theta_1^{u_1} \dots \Theta_{\nu-v_0}^{u_{\nu-v_0}} = \mathsf{H}\mathsf{A}^{1-\sigma}; \quad (\mathsf{H} \text{ Einheit aus } K)$$

also durch Normbildung

$$\varepsilon_1^{u_1} \dots \varepsilon_{\nu-v_0}^{u_{\nu-v_0}} = n(\mathsf{H})$$

Dann muß aber nach dem vorhin gezeigten

$$u_1 = \dots = u_{\nu-v_0} = 0$$

sein. Das bedeutet aber, daß die durch die $\mathfrak{A}_i$ definierten wegen $\mathfrak{A}_i^{1-\sigma} = (\Theta_i)$ offenbar ambigen Klassen □□□ in Bezug auf die ambigen Klassen mit ambigen Idealen und untereinander unabhängig sind.

Ist andererseits $\mathfrak{A}$ ein Ideal aus einer ambigen Klasse, dann muß $\mathfrak{A}^{1-\sigma} = \Theta$ in K sein, also

$$n\big((\theta)\big) = (1)$$
$$n(\theta) = \varepsilon \quad \text{in} \quad k$$

Somit

$$\varepsilon = \varepsilon_1^{u_1} \dots \varepsilon_{\nu-v_0}^{u_{\nu-v_0}} n(\mathsf{H}); \quad \mathsf{H} \quad \text{in} \quad K$$
$$n(\theta) = n(\Theta_1^{u_1} \dots \Theta_{\nu-v_0}^{u_{\nu-v_0}} \mathsf{H})$$

Da aus $n(\mathsf{B}) = 1$ nach unserem Hilfssatz $\mathsf{B} = \mathsf{A}^{1-\sigma}$ folgt, muß

$$\Theta = \Theta_1^{u_1} \dots \Theta_{\nu-v_0}^{u_{\nu-v_0}} \mathsf{H}\mathsf{A}^{1-\sigma}$$

d.h.

$$\mathfrak{A}^{1-\sigma} = (\mathfrak{A}_1^{u_1} \dots \mathfrak{A}_{\nu-v_0}^{u_{\nu-v_0}} \mathsf{A})^{1-\sigma}$$

sein. Somit ist

$$\mathfrak{A} = (\mathfrak{A}_1^{u_1} \dots \mathfrak{A}_{\nu-v_0}^{u_{\nu-v_0}} (\mathsf{A})\overline{\mathfrak{A}}, \quad \text{wo } \overline{\mathfrak{A}}^{1-\sigma} = 1 \text{ ist.}$$

Jedes Ideal einer ambigen Klasse läßt sich also durch die Basis $\mathfrak{A}_1, \dots,$ $\mathfrak{A}_{\nu-v_0}$ und Ideale $\overline{\mathfrak{A}}$ mit $\overline{\mathfrak{A}}^{1-\sigma} = 1$ darstellen.

Zusammengenommen haben wir also:

Die Gruppe G aller ambigen Klassen ist in Bezug auf die Untergruppe der Klassen, die aus ambigen Idealen entspringen von endlichem Index. Die Nebengruppen bilden eine Gruppe vom Typus $(\ell, \ell, \ldots, \ell)$; ($\nu - v_0$ mal) sodaß der Index $\ell^{\nu - v_0}$ ist.

Nach Satz 15 erzeugen die ambigen Ideale in K genau $h\ell^{d-\varrho}$ Klassen, sodaß die Anzahl aller ambigen Klassen

$$a = h\ell^{d-\varrho+v-v_0} = h\ell^{v+d-(\varrho+v_0)}$$

ist. Nach Satz 12 ist

$$\begin{aligned} \varrho &= r + 1 + \delta - v_0 && \text{für ungerades } \ell \\ \varrho &= r + 1 + \delta - \nu - v_0 && \text{für } \ell = 2. \end{aligned}$$

Für $\ell = 2$ enthält k sicher die prim. 2. E. W. -1, also $\delta = 1$. Somit wird

$$\begin{aligned} a &= h\ell^{d+v-(r+1+\delta)} && \text{für ungerades } \ell \\ a &= h \cdot \ell^{d+v-(r+2-\nu)} && \text{für } \ell = 2 \end{aligned}$$

Unser Satz ist damit bewiesen.

e) Die Geschlechter für $\ell \neq 2$

e.) Die Geschlechter für ungerades ℓ.

Definition 4. Es sei K relativ zyklisch vom Primzahlgrad ℓ (gerade oder ungerade) zu k. Dann heißt eine ganze oder gebrochene Zahl α aus k Normenrest des Körpers K nach dem Modul m, wenn es in K eine ganze oder gebrochene Zahl A gibt, sodaß im Sinne von Definition 2 (S. 93▸) $\alpha \equiv n(\mathsf{A}) \bmod m$ ist, und α, A zu m prim sind.

Diese Definition wird gerechtfertigt durch den

Satz 17. Eine ganze Zahl α ist dann und nur dann Normenrest im Sinne der vorigen Definition, wenn sie es im Sinne der Definition 2 (S. 159▸) ist. Da die Anzahl der zu m primen Restklassen für ganze oder gebrochene Zahlen übereinstimmt, gilt auch im Sinne unserer neuen Definition der Satz 8 und

10 (S. 159▸ und 171▸).

Beweis. Sei α ganz und Normenrest im neuen Sinne, also $\alpha \equiv n(\mathsf{A}) \bmod m$, wo A aber gebrochen ist und prim zu m: $\mathsf{A} = \frac{\mathsf{B}}{\nu}$, wo ν ganz rational, prim zu m ist. Dann ist $\nu^\ell \alpha = n(\nu\mathsf{A}) \equiv n(\mathsf{B}) \bmod m$. Wählen wir ν_1 aus k so, daß $\nu\nu_1 \equiv 1 \bmod m$ ist, so ist $\alpha \equiv \nu_1^\ell n(\mathsf{B}) \equiv n(\nu_1\mathsf{B}) \bmod m$, also α auch Normenrest im früheren Sinne, w.z.b.w.

Nun sei ℓ ungerade und $f^{\ell-1}$ Relativdiskriminante von K. Da immer eine ganze Restklasse Normenrest oder Nichtrest ist, bildet die Gesamtheit der Normenreste von

197 ı

K nach dem Modul f einen Strahl o in k. Nach diesem Strahl o seien die Idealklassen in k definiert und ihre Klassenzahl sei h' (Vergl. hierzu Satz 10, S. 171▸)

Ist h die absolute Klassenzahl, also auch nach dem Strahl o_1 *aller* zu f primen Zahlen, so ist nach Satz 19 (S. 112▸):

$$h' = \frac{(o_1 : o)}{(E_1 : E)} h$$

wenn E_1 und E die Gruppen der Einheiten in o_1 (in k) und in o bedeuten.

Nach Satz 10 (S. 171▸) ist, wenn d verschiedene Primideale in f aufgehen (d Diskriminantenteiler existieren), genau der ℓ^d–te Teil aller zu f primen Restklassen Normenrest nach f, also in o, sodaß $(o_1 : o) = \ell^d$ wird.

Hat δ die bisher benutzte Bedeutung (Satz 12, S. 182▸), so liegen in o_1 nach Satz 17 (S. 103▸) genau $\ell^{r+\delta}$ Einheitenverbände. Ist nun ε in o, und η irgendeine Einheit aus o_1, so ist auch $\varepsilon\eta^\ell$ in o, das dieses mit ε Normenrest nach f ist. In E liegen also immer ganze Einheitenverbände von E_1; diese haben (als Untergruppe aller Einheitenverbände) eine □□□ Anzahl ℓ^n. (Nach Satz 17, S. 103▸ ist zwar die Anzahl der Verbände in `[...]` ebenfalls $\ell^{r+\delta}$, das ist aber kein Widerspruch gegen die hiesige Anzahl ℓ^n. Letztere bedeutet die Anzahl der Verbände *in* o_1, die in o liegen. Diese Verbände spalten sich jedoch *in* o_1 im allgemeinen in mehrere, da $\varepsilon\eta^\ell$, wo η in o_1 liegt und alle Einheiten aus o_1 durchläuft mehrere Verbände in o darstellt, wenn nicht alle η auch in o liegen, also o mit o_1 identisch ist). Der Index $(E_1 : E)$ ist nun leicht zu bestimmen. Er ist gleich dem Index der Gruppe *aller* Einheitenverbände in o_1 zu der Untergruppe aller Einheitenverbände in o_1, die in o liegen, also gleich

198 ı

$\ell^{r+\delta-n}$. Damit wird:

$$h' = h \cdot \ell^{d+n-(r+\delta)} \tag{1}$$

Die Idealklassen in K seien im absoluten Sinne definiert, aber nur die zu f primen Ideale in Betracht gezogen (Def. 10, S. 116▸)

Sind nun $\mathfrak{A}$ und $\mathfrak{B}$ zwei Ideale aus K und

$$\mathfrak{A} \sim \mathfrak{B}, \quad \text{also} \quad \mathfrak{A} = (\mathsf{A})\mathfrak{B}$$

wo A Zahl aus K, dann ist

$$n(\mathfrak{A}) = n[(\mathsf{A})]n(\mathfrak{B}) = \big(n(\mathsf{A})\big) \cdot n(\mathfrak{B})$$

Die Ideale $n(\mathfrak{A})$ und $n(\mathfrak{B})$ liegen also in der gleichen nach o definierten Klasse von k, da ihr Quotient gleich dem Hauptideal $(\alpha) = \big(n(\mathsf{A})\big)$ ist, und α als Zahlnorm erst recht Normenrest nach f ist. (α ist prim zu f, da $\mathfrak{A}$ und $\mathfrak{B}$ so vorausgesetzt werden).

Infolgedessen ist jeder Klasse $\mathfrak{K}$ von K eine Idealklasse $\mathfrak{k}$ von k nach o zugeordnet, die wir die Relativnorm von $\mathfrak{K}$ nennen:

$$\mathfrak{k} = n(\mathfrak{K}). \tag{2}$$

Wie leicht ersichtlich, ist $n(\mathfrak{K}\mathfrak{K}_1) = n(\mathfrak{K}) \cdot n(\mathfrak{K}_1)$, sodaß die Relativnormen der Klassen $\mathfrak{K}$ eine Klassengruppe H in k bilden, deren Index wir i nennen (in Bezug auf die Gruppe aller h' Klassen nach o in k). Im Sinne von Definition 3, (S. 142▸) ist die Klassengruppe H dem Körper K zugeordnet. Nach Satz 7 (S. 142▸) ist also der Grad ℓ von K sicher $\geqq i$. In H kommt sicher die Hauptklasse $\mathfrak{k}_0$ vor, und es seien $\mathfrak{K}_0, \mathfrak{K}_1, \ldots, \mathfrak{K}_{t-1}$ alle Klassen aus K, deren Relativnormen $\mathfrak{k}_0$ sind. Auch sie bilden eine Gruppe H_0. Jede Nebengruppe zu H_0 enthält immer gerade alle und nur die Klassen,

199 ı

deren Relativnormen sich nur um $\mathfrak{k}_0$ unterscheiden, also identisch sind. Ist also G_0 die Gruppe aller Idealklassen aus K, so ist der Index $(G_0 : \mathsf{H}_0)$ gleich dem Grad der Gruppe H, da es eben soviel verschiedene Nebengruppen zu H_0 geben muß, als es Klassen $\mathfrak{K}$ mit verschiedener Relativnorm gibt, und das ist gerade der Grad von H. Der Grad von H ist nun $\frac{h'}{i}$, da h' Klassen nach o

existieren und der Index von H gleich i gesetzt wurde. Nach dem obigen ist also

$$(3) \qquad (G_0 : \mathsf{H}_0) = \frac{h'}{i} \geqq \frac{h'}{\ell}\,.$$

Man bezeichne nun mit H° die Gruppe aller Klassen von K, die symbolische $(1-\sigma)$ te Potenzen von Klassen in K sind. Da $\sigma\mathfrak{K}$ die gleiche Norm wie $\mathfrak{K}$ hat, ist die Norm einer Klasse H° die Hauptklasse, H° also Untergruppe von H_0, also

$$(G_0 : \mathsf{H}^\circ) \geqq (G_0 : \mathsf{H}_0).$$

Ist andererseits $\mathfrak{K}^\circ$ eine Klasse aus H° und wird $\mathfrak{K}^\circ$ von $\mathfrak{K}$ erzeugt: $\mathfrak{K}^\circ = \mathfrak{K}^{1-\sigma}$, so wird $\mathfrak{K}^\circ$ auch von $\mathfrak{K}\mathfrak{K}_i$ erzeugt, wo $\mathfrak{K}_i$ eine ambige Klasse von K ist. Ist umgekehrt $\mathfrak{K}^{1-\sigma} = \mathfrak{K}'^{1-\sigma}$, so ist $\left(\frac{\mathfrak{K}}{\mathfrak{K}'}\right)^{1-\sigma} = 1$, also $\mathfrak{K}\mathfrak{K}'^{-1}$ eine ambige Klasse. Ist also a die Anzahl der ambigen Klassen, so erzeugen immer genau a Klassen aus K die gleiche Klasse von H°. Es ist also $(G_0 : \mathsf{H}^\circ) = a = h\ell^{d+v-(r+1+\delta)}$ nach Satz 16 (S. 192▸); denn alle g_0 Klassen von G_0 zerfallen in $\frac{g_0}{a}$ Systeme von je a Klassen, deren $(1-\sigma)$–te Potenz je ein und dieselbe Klasse von H° bilden. Der Grad von H° ist also $\frac{g_0}{a}$, also der Index zu G_0 ist $\dfrac{g_0}{\frac{g_0}{a}} = a$.

Somit folgt aus (3) und (1):

$$(4) \qquad h \cdot \ell^{d+v-(r+1+\delta)} = (G_0 : \mathsf{H}^\circ) \geqq (G : \mathsf{H}_0) \geqq \frac{h'}{\ell} = h\ell^{d+n-(r+\delta+1)},$$

Es ist somit:

$$\boldsymbol{v \geqq n.}$$

Nun ist v die Anzahl der unabh. Einheitenverbände aus k, welche durch Relativnormen von Zahlen aus K geliefert werden, n die Anzahl der unabh. Einheitenverbände, welche Normenreste nach f sind (also nur $\equiv$ der Norm einer Zahl aus K nach f) Daher ist:

$$n \geqq v$$

woraus:

$$(5) \qquad \boldsymbol{n = v}$$

zu schließen ist.

Es muß daher in (4) überall das Gleichheitszeichen gelten, also auch in (3) und somit ist $i = \ell$. Wir haben also:

$$a = \frac{h'}{\ell}\,, \tag{6}$$

$$\mathsf{H}^\circ = \mathsf{H}_0\,, \tag{7}$$

$$i = \ell. \tag{8}$$

Definition 5. Alle Klassen in K, deren Relativnorm ein und dieselbe Klasse in k nach o bildet, fassen wir in ein Geschlecht zusammen. Insbesondere definieren wir das Hauptgeschlecht durch alle jene Klassen, deren Relativnorm die Hauptklasse in k ist. Das Hauptgeschlecht ist also die Klassengruppe H_0, sodaß jedes Geschlecht eine Nebengruppe von H_0 ist.

Dann gilt nach dem vorigen:

Satz 18. Die Anzahl der Geschlechter von K ist gleich dem ℓ–ten Teil $\frac{h'}{\ell}$ der Klassenzahl h' des Körpers k nach o und gleich der Anzahl der ambigen Klassen des Körpers K. Die Klassenzahl des Körpers K ist teilbar durch die Anzahl der Geschlechter (Index der Klassengruppe H_0), also teilbar durch $\frac{h'}{\ell} = a$.

Wegen (7) folgt noch:

Satz 19. Jede Klasse des Hauptgeschlechts ist die symbolische $(1 - \sigma)$ te Potenz einer Klasse von $\mathfrak{K}$.

Aus (5) folgt nach der Bedeutung von n und v:

Satz 20. Wenn eine Einheit in k Normenrest von K nach dem Modul f ist, dann ist sie wirklich Relativnorm einer ganzen oder gebrochenen Zahl von K.

Satz 21. Wenn eine ganze oder gebr. Zahl α die ℓ–te Potenz eines Ideals $\mathfrak{a}$ aus k ist, und außerdem Normenrest nach f, dann ist die Relativnorm einer ganzen oder gebrochenen Zahl aus K.

Beweis. Sei $(\alpha) = \mathfrak{a}^\ell$ und α Normenrest nach f. Dann gehört α zu o (α ist nach Def. des Normenrestes, S. 196, zu f prim). Da ferner

$$n(\mathfrak{a}) = \mathfrak{a}^\ell = (\alpha)$$

ist, ist $\mathfrak{a}$ zu einer Klasse des Hauptgeschlechts in K gehörig, also $\mathfrak{a} = \mathfrak{A}^{1-\sigma}(\Theta)$, wo $\mathfrak{A}$ und Θ Ideal und Zahl aus K sind. Durch Normbildung folgt:

$$\alpha = \varepsilon n(\Theta)$$

202 I

wo ε Einheit in k ist. Da α Normenrest nach f ist, ist es auch ε, folglich nach Satz 20: $\varepsilon = n(\mathsf{A})$, also $\alpha = n(\mathsf{A}\Theta)$.

Aus (8) folgt noch nach Definition 4 (S. 144), daß K ein *Klassenkörper* nach der Klassengruppe H ist. Der Modul war bei uns bisher f selbst. Nehmen wir statt dessen irgendeinen durch f teilbaren Modul m, so ändert sich, wie früher gezeigt an H nichts wesentliches. Ebenso, wenn man, statt vom Strahl o, vom engeren Strahl aller Zahlen $\equiv 1 \bmod m$ ausgeht, der ja nach S. 114 alle in Betracht kommenden Klassengruppen erzeugt (für ungerades ℓ spielen die Signaturen keine Rolle).

Satz 22. Sei $f^{\ell-1}$ die Relativdiskriminante von K nach k und ℓ ungerade, ferner m ein durch f teilbares Ideal aus k und o der Strahl aller Zahlen $\equiv 1 \bmod m$ aus K. Dann ist K Klassenkörper für eine Klassengruppe H vom Index ℓ nach dem Modul m und dem Strahl o.

203 I

f) Die Geschlechter für $\ell = 2$

f.) Die Geschlechter im relativquadratischen Zahlkörper.

Es sei $K = k(\sqrt{\mu})$ relativ–quadratisch in Bezug auf k. ν sei, wie früher die Anzahl der reellen, mit k konjugierten Körper, in denen die zu μ konjugierten negativ sind.

Als Strahl o legen wir *die* Normenreste nach der Relativdiskriminante $\mathfrak{D} = f^{\ell-1} = [\ldots]$ zugrunde, welche in den fraglichen ν Körpern positiv sind. o enthält also alle zu f primen Zahlen α, für die

1.) $\alpha \equiv n(\mathsf{A}) \mod f$

2.) α positiv in den ν Körpern, für die μ negativ.

Daß o ein Strahl mod f ist, ist unmittelbar klar. h' sei die Anzahl der Idealklassen von k (nach o definiert). Es ist

$$h' = \frac{(o_1 : o)}{(E_1 : E)} h$$

wo h die absolute Klassenzahl, o_1 der Strahl *aller* zu f primen Zahlen, und E_1 und E die Gruppen der Einheiten in o_1 (d.h. k) und o sind.

Nach Satz 10 (S. 171) ist genau der 2^d–te Teil aller zu f primen □□□ Restklassen nach f Normenreste (d = Anzahl der Diskriminantenteiler, Teiler von $\mathfrak{D} = f$). Jede solche Restklasse hat Zahlen aller Signaturen, also für die ν „kritischen“ konjugierten 2^ν Möglichkeiten. Zerlegen wir also die Normenreste nach o nach der Untergruppe mit nur positiven Normenresten in den ν kritischen Körpern, so erhalten wir 2^ν Nebengruppen. Es ist also $(o_1 : o) = 2^{d+\nu}$.

Zur Bestimmung von $(E_1 : E)$ bemerken wir zunächst, daß k stets die prim. 2–te E.W. -1 enthält, sodaß es in o_1 genau 2^{r+1} Einheitenverbände gibt. Ist ε eine Einheit in o, also

Normenrest mit Vorzeichenbedingung, dann gehört auch jedes $\varepsilon\eta^2$ mit beliebigem η aus o_1 wieder in o, da $\eta^2 = n(\eta)$ und total positiv ist. Wieder machen also die □□□ Einheiten von o ganze Einheitenverbände *in* o_1 aus. Sei 2^n die Anzahl der Einheitenverbände (*in* o_1), die E zusammensetzen, so ist

$$(E_1 : E) = 2^{r+1-n}$$

also:

$$h' = h 2^{d+\nu+n-(r+1)} \tag{1}$$

In K seien die Idealklassen im absoluten Sinne (unter Beschränkung auf die zu f primen Ideale) erklärt. Sind $\mathfrak{A}, \mathfrak{B}$ zwei Ideale gleicher Klasse aus K, also $\mathfrak{A} = \mathfrak{B}(\mathsf{A})$, so ist:

$$n(\mathfrak{A}) = n(\mathfrak{B}) \cdot \big(n(\mathsf{A})\big)$$

Ist nun μ_i negativ, der Körper $K_i = k_i(\sqrt{\mu_i})$ also imaginär, so ist $n(\mathsf{A}) = \mathsf{A}\mathsf{A}'$ sicher positiv □□□ in k_i, also $n(\mathsf{A})$ sicher Zahl aus o. Wieder haben also

Ideale einer Klasse in K äquivalente Relativnormen (nach o) in k. Ist $\mathfrak{A}$ ein Ideal aus $\mathfrak{K}$ und $\mathfrak{k}$ die Klasse nach o in k, der $n(\mathfrak{A})$ angehört, so setzen wir wieder $\mathfrak{k} = n(\mathfrak{K})$.

Die Klassengruppe H der Relativnormen von Klassen aus K ist dann dem Körper K zugeordnet. Ist i ihr Index so gilt, wie oben:

$$i \leqq 2 \tag{2}$$

Verstehen wir unter H_0 und H°, G_0 dieselben Klassengruppen von K, wie im vorigen Abschnitt:

$\mathsf{H}_0 =$ Gruppe aller Klassen $\mathfrak{K}$, für die $n(\mathfrak{K}) = \mathfrak{k}_0$ die Hauptklasse nach o in k.
$\mathsf{H}^\circ =$ Gruppe aller $(1-\sigma)$ ten Klassenpotenzen in K,
$G_0 =$ Gruppe aller Klassen in K,
□□□

so gilt wieder:

$$(G_0 : \mathsf{H}_0) = \frac{h'}{i} \geqq \frac{h'}{2}\,, \qquad \text{(Beweis wie oben)}, \tag{3}$$

und H° ist Untergruppe von H_0. Wieder ist $(G_0 : \mathsf{H}^\circ) = a$ die Anzahl der ambigen Klassen in K, also:

$$(G_0 : \mathsf{H}^\circ) = a = h \cdot 2^{d+v+\nu-(r+2)}$$

$$h \cdot 2^{d+v+\nu-(r+2)} = (G_0 : \mathsf{H}^\circ) \geqq (G_0 : \mathsf{H}_0) = \frac{h'}{i} \geqq \frac{h'}{2} = 2^{d+\nu+n-(r+2)} \tag{4}$$

Also:

$$v \geqq n.$$

Nun ist wieder v die Anzahl der unabh. Einheitenverbände aus k, welche Relativnormen von Zahlen aus K sind, n die Anzahl der unabh. Einheitenverbände aus o_1 (d.h. k) welche Normenreste nach f und der Vorzeichenbedingung genügen. Da jeder der v Verbände

1.) Normenrestverband nach f,

2.) In den fraglichen Körpern positiv (vorige Seite!) ist, muß auch: $v \leqq n$ □□□ sein, also

$$v = n \tag{5}$$

$$a = \frac{h'}{2} \tag{6}$$

$$\mathsf{H}^\circ = \mathsf{H}_0 \tag{7}$$

$$i = 2 \tag{8}$$

Definieren wir also die Geschlechter wie in Definition 5, so folgt:

Satz 23. Die Anzahl der Geschlechter ist gleich der halben Klassenzahl h' des Körpers k nach o und gleich der Anzahl der ambigen Idealklassen in K, nämlich gleich:

$$a = \frac{h'}{2}$$

Satz 24. Jede Klasse des Hauptgeschlechtes ist die $(1-\sigma)$–te symbolische Potenz einer Klasse aus K.

Aus (5) folgt:

206 I

Satz 25. Wenn eine Einheit von k Normenrest nach f und in den ν kritischen Körpern positiv ist, so ist sie wirklich Relativnorm einer Zahl A aus K.

Satz 26. Wenn eine Zahl α aus k Quadrat eines Ideals $\mathfrak{a}$ aus k ist, ferner in den ν kritischen Körpern positiv und Normenrest nach f, so ist sie die Norm einer Zahl A aus K.

Beweis. Sei $(\alpha) = \mathfrak{a}^2$. Wegen $n(\mathfrak{a}) = \mathfrak{a}^2 = (\alpha)$ ist

$\sim\sim\sim\sim\sim$ $\mathfrak{a}$ Ideal des Hauptgeschlechtes, nach den Vorauss.

$\sim\sim\sim\sim\sim$ über α. Daher nach Satz 24

$$\mathfrak{a} = \mathfrak{A}^{1-\sigma}(\Theta)$$

$$(\alpha) = n(\mathfrak{a}) = \big(n(\Theta)\big)$$

$$\alpha = \varepsilon n(\Theta); \qquad (\varepsilon \text{ Einheit in } k)$$

Da α, so ist auch ε Normenrest, □□□ ferner in den ν kritischen Körpern positiv, da dies von α und $n(\Theta)$ gilt. Also ist nach Satz 25: $e = n(\mathsf{A})$; $\alpha = n(\mathsf{A}\Theta)$.

Aus (8) folgt, daß K Klassenkörper nach k ist für die Klassengruppe H. Der Strahl aller Zahlen $\equiv 1 \bmod f$, welche in den ν kritischen Körpern positiv ausfallen, oder auch überhaupt total positiv sind, liegt ganz in o, kann also zur Charakterisierung von H ebenfalls benutzt werden, ebenso jeder durch f teilbare Modul m.

Satz 27. f sei die Relativdiskriminante des relativquadratischen Zahlkörpers $K = k(\sqrt{\mu})$. m sei ein durch f teilbares Ideal aus k und o der Strahl aller Zahlen $\equiv 1 \bmod m$, die in jenen reellen konjugierten Körpern, in denen μ negativ ist, positiv sind (oder auch der Strahl aller total

207 ı

positiven Zahlen $\equiv 1 \bmod m$). Dann ist K Klassenkörper zu k[13] für eine Klassengruppe H vom Index 2 nach dem Modul m und Strahl o.

Daraus folgt □□□ in Verbindung mit Satz 22:

Satz 28. Jeder relativ–zyklische Körper K von Primzahlgrad ℓ und der Relativdiskriminante $f^{\ell-1}$ in Bezug auf k ist ein Klassenkörper für eine Klassengruppe nach dem Modul f.

Der eben bewiesene Satz, der uns noch gute Dienste leisten wird, ist ein spezieller □□□ Fall eines allgemeinen Satzes, den wir erst später herleiten können, nach dem überhaupt *jeder relativ Abelsche Körper Klassenkörper* für einen gewissen Modul m ist.

208 ı

g) Verallgemeinerung des Geschlechtsbegriffs

Hilfssatz 1. Sei $\mathfrak{q}$ ein Primideal in k, welches prim ist zur Relativdiskriminante $f^{\ell-1}$ des Körpers K (ℓ gerade oder ungerade). Θ sei eine Zahl aus K, für die

$$n(\Theta) \equiv 1 \bmod \mathfrak{q}^e \tag{1}$$

ist, wo e beliebig $\geqq 1$. Dann gibt es in K eine zu $\mathfrak{q}$ prime Zahl A, sodaß

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{q}^e \tag{2}$$

[13] undeutlich

ist.

Beweis. Sei G die Gruppe der primen Restklassen mod $\mathfrak{q}^e$ in K, H die Untergruppe derselben, die (1) genügen, H_0 diejenige, deren Zahlen (2) erfüllen. (2) wird ersichtlich immer durch *ganze* Restklassen mod $\mathfrak{q}^e$ erfüllt, für (1) folgt dies so: Ist $\Theta \equiv \Theta_1 \bmod \mathfrak{q}^e$, so ist, da $\mathfrak{q}^e$ in k liegt: $\sigma^\nu\Theta \equiv \sigma^\nu\Theta_1 \bmod \mathfrak{q}^e$, also $n(\Theta) \equiv n(\Theta_1) \bmod \mathfrak{q}^e$.

Es sei umgekehrt $n(\Theta) \equiv n(\Theta_1) \bmod \mathfrak{q}^e$. Dann ist $n\left(\frac{\Theta}{\Theta_1}\right) \equiv 1 \bmod \mathfrak{q}^e$. Die Normen der Zahlen einer Nebengruppe von H nach G sind also einander kongruent und nur diese. Es gibt also genau soviel Nebengruppen, als es Normenrestklassen □□□ in k gibt. Der Index $(G : \mathsf{H})$ ist also gleich der Anzahl der Normenrestklassen nach $\mathfrak{q}^e$ in k. Auf Grund von Satz 8 (S. 159▸) ist also

$$(G : \mathsf{H}) = \Phi_k(\mathfrak{q}^e)$$

wo Φ_k die Eulersche Funktion in k ist.

Aus $\Theta \equiv \mathsf{A}^{1-\sigma} \bmod \mathfrak{q}^e$ folgt andererseits, daß

$n(\Theta) \equiv 1 \bmod \mathfrak{q}^e$, sodaß H_0 Untergruppe von H ist; daher

$$(G : \mathsf{H}_0) \geqq (G : \mathsf{H})$$

Wir haben also nur zu zeigen, daß hier das Gleichheitszeichen stehen muß.

Wenn nun für Θ aus H_0 und die inkongruenten[14] Zahlen $\mathsf{A}_1, \ldots, \mathsf{A}_t$ gilt:

$$\Theta \equiv \mathsf{A}_1^{1-\sigma} \equiv \mathsf{A}_2^{1-\sigma} \equiv \cdots \equiv \mathsf{A}_t^{1-\sigma} \mod \mathfrak{q}^e,$$

so ist

$$\left(\frac{\mathsf{A}_i}{\mathsf{A}_1}\right)^{1-\sigma} \equiv 1 \mod \mathfrak{q}^e$$

also

$$\frac{\mathsf{A}_i}{\mathsf{A}_1} = \mathsf{A} \qquad \text{eine Zahl für die } \mathsf{A}^{1-\sigma} \equiv 1 \bmod \mathfrak{q}^e$$

ist. Die gleiche Restklasse Θ wird also von genau ebensovielen primen Restklassen $\mathsf{A}_1, \ldots, \mathsf{A}_t$ erzeugt, als es prime Restklassen A gibt, für die $\mathsf{A}^{1-\sigma} \equiv 1$ ist. (Zahlen A einer Restklasse liefern kongruente $\mathsf{A}^{1-\sigma}$, da der Modul in k liegt). Daher ist der Index $(G : \mathsf{H}_0)$ gleich der Anzahl dieser Restklassen A.

[14] undeutlich

Es bleibt zu zeigen, daß diese Anzahl gleich $\Phi_k(\mathfrak{q}^e)$ *ist, d.h. daß jedes prime* A, *für das* $\mathsf{A}^{1-\sigma} \equiv 1 \bmod \mathfrak{q}^e$ *einer primen Zahl aus* k *nach* $\mathfrak{q}^e$ *kongruent ist* Da nämlich umgekehrt für jede prime Zahl α aus k: $\alpha^{1-\sigma} = 1 \equiv 1 \bmod \mathfrak{q}^e$ ist, folgt dieses dann ohne weiteres.

1) $\mathfrak{q}$ zerfalle in K: $\mathfrak{q} = \mathfrak{Q}_1 \dots \mathfrak{Q}_\ell$ in ℓ verschiedene Primideale ersten Relativgrades, sodaß $\mathsf{N}_K(\mathfrak{Q}_i) = \mathsf{N}_k\big(n(\mathfrak{Q}_i)\big) = \mathsf{N}[\dots](\mathfrak{q}_i)$, also

$$\Phi_K(\mathfrak{Q}_i^e) = \Phi_k(\mathfrak{q}_i^e)$$

ist. Daher gibt es Zahlen $\alpha, \alpha', \dots,$ sodaß

$$\mathsf{A} \equiv \alpha \mod \mathfrak{Q}_1^e; \quad \mathsf{A} \equiv \alpha' \mod \mathfrak{Q}_2^e \quad \dots$$

ist. Dann ist, wenn man σ auf die erste Gleichung anwendet und $\mathsf{A}^{1-\sigma} \equiv 1$ berücksichtigt[15]

$$\sigma\mathsf{A} \equiv \mathsf{A} \equiv \alpha \mod \mathfrak{Q}_2^e$$

210 I

ebenso $\mathsf{A} \equiv \alpha \bmod \mathfrak{Q}_3^e, \dots$ also für jedes i

$$\begin{aligned} \mathsf{A} - \alpha &\equiv 0 \mod \mathfrak{Q}_i^e \\ \text{also} \qquad \mathsf{A} &\equiv \alpha \mod \mathfrak{q}^e \end{aligned}$$

2) $\mathfrak{q}$ bleibe Primideal in K. A genügt einer Relativgleichung

$$f(x) = (x - \mathsf{A})(x - \sigma\mathsf{A}) \cdots (x - \sigma^{\ell-1}\mathsf{A}) = 0$$

und, wenn f der Grad von $\mathfrak{q}$ in k ist, also ef der Grad von $\mathfrak{Q}$ in K, und $\mathfrak{q}$ in der Primzahl q [16] aufgeht, einer Kongruenz:

$$\overline{f}(x) \equiv (x - \mathsf{A})(x - \mathsf{A}^{q^f}) \cdots (x - \mathsf{A}^{q^{ef}}) \equiv 0 \mod \mathfrak{q} \quad \text{in} \quad k.$$

Bei passender Wahl von σ ist also

$$\sigma\mathsf{A} \equiv \mathsf{A}^{q^f} \mod \mathfrak{q},$$

also nach Voraussetzung

$$\mathsf{A} \equiv \mathsf{A}^{q^f} \mod \mathfrak{q}.$$

[15] undeutlich

[16] Bei $\mathfrak{q}$ kommen zahlreiche Kombinationen von Größe und Unterstrich zur Darstellung.

Da A prim zu $\mathfrak{q}$ ist, folgt

$$\mathsf{A}^{q^f-1} \equiv 1 \mod \mathfrak{q}$$

Nun hat die Kongruenz $x^{q^f-1} \equiv 1 \bmod \mathfrak{q}$ die q^f-1 inkongruenten Restklassen von k nach $\mathfrak{q}$ zu Lösungen und keine weiteren. Da $\mathfrak{q}$ auch in K Primideal ist, kann sie auch dort keine weiteren haben. Also ist A einer Zahl in k mod q kongruent. Daraus folgt das weitere durch vollständige Induktion.

Unser Satz sei für $\mathfrak{q}^e$ bewiesen. Es sei $\mathsf{A}^{1-\sigma} \equiv 1 \bmod \mathfrak{q}^{e+1}$, also auch mod $\mathfrak{q}^e$, sodaß $\mathsf{A} \equiv \alpha \bmod \mathfrak{q}^e$ gilt, wo α in k liegt. Gilt dann $\mathsf{A} \equiv \alpha \bmod \mathfrak{q}^{e+1}$ so ist alles bewiesen. Andernfalls sei π eine genau durch $\mathfrak{q}^e$ teilbare Zahl aus k und $\mathsf{A} \equiv \alpha + \pi\mathsf{B} \bmod \mathfrak{q}^{e+1}$, wo B prim zu $\mathfrak{q}$. Wegen $\sigma\mathsf{A} \equiv \mathsf{A} \bmod \mathfrak{q}^{e+1}$, muß $\sigma\mathsf{B} \equiv \mathsf{B} \bmod \mathfrak{q}$, also nach dem Bewiesenen $\mathsf{B} \equiv \beta \bmod \mathfrak{q}$ (aus k) sein. Also $\mathsf{A} \equiv \alpha + \pi\beta \bmod \mathfrak{q}^{e+1}$, w.z.b.w.

Hilfssatz 2. Für die in der Relativdiskriminante von K aufgehenden Primideale gilt:

1.) Sei $\mathfrak{p}$ prim zu ℓ und $\mathfrak{p} = \mathfrak{P}^\ell$ in K; Θ sei eine Zahl aus K, für die gilt:

$$n(\Theta) \equiv 1 \mod \mathfrak{p}^e; \quad (e \geqq 1) \tag{3}$$

Dann gibt es in K eine (möglicherweise durch $\mathfrak{P}$ teilbare) Zahl A, sodaß

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{P}^{(e-1)\ell+1} \tag{4}$$

ist.

2.) $\mathfrak{l}$ gehe in ℓ auf und es sei $\mathfrak{l} = L^\ell$. Ferner sei im Sinne von Satz 2 (S. 149) $\mathfrak{l}^{(v+1)(\ell-1)}$ die genaue Potenz von $\mathfrak{l}$, die in der Relativdiskriminante aufgeht, und n eine positive ganze Zahl. Ist dann Θ eine Zahl aus K, für die gilt:

$$n(\Theta) \equiv 1 \mod \mathfrak{l}^{v+n}, \tag{5}$$

so gibt es in K eine (möglicherweise durch L teilbare) Zahl A, sodaß

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod L^{v+n\ell} \tag{6}$$

ist.

Beweis. Sei G die Gruppe aller primen Restklassen mod $\mathfrak{P}^{(e-1)\ell+1}$ bezw. $L^{v+n\ell}$.

Ist nun $\Theta \equiv 1 \mod \mathfrak{P}^{(e-1)\ell+1}$, d.h. $\Theta = 1 + \Pi_0$ wo Π_0 durch $\mathfrak{P}^{(e-1)\ell+1}$ teilbar, so ist $n(\Theta) = n(1 + \Pi_0)$, also $n(\Theta) \equiv 1 + S(\Pi_0) \mod \mathfrak{p}^e$, falls $e > 1$ ist (wie man leicht bestätigt). Es ist $S(\Pi_0)$ durch $\mathfrak{P}^{(e-1)\ell+1}$ teilbar. Da $S(\Pi_0)$ in k liegt, muß es durch $\mathfrak{p}^e$ teilbar sein, also

$$n(\Theta) \equiv 1 \mod \mathfrak{p}^e$$

Für $e = 1$ ist aber, wenn $\Theta \equiv 1 \bmod \mathfrak{P}$, sicher $n(\Theta) \equiv 1 \bmod \mathfrak{P}$,

212 I

also auch $\equiv 1 \bmod \mathfrak{p}$. Ist also $\Theta \equiv \theta_1 \bmod \mathfrak{P}^{(e-1)\ell+1}$, so ist $n(\Theta) \equiv n(\theta_1) \bmod \mathfrak{p}^e$. Die Bedingung (3) wird also immer durch ganze Restklassen mod $\mathfrak{P}^{(e-1)\ell+1}$ aus K erfüllt. Nennen wir nun H die Gruppe aller Restklassen (primen), für die (3) gilt. Dann ist H Untergruppe von G. Ferner liefern uns wie oben gerade die Zahlen einer Nebengruppe zu H noch $[\ldots]$ kongruente Normen und umgekehrt. Der Index $(G : \mathsf{H})$ ist also gleich der Anzahl der Normenrestklassen mod $\mathfrak{p}^e$, nach Satz 8 (S. 159▸) also: $(G : \mathsf{H}) = \frac{1}{\ell}\phi_k(\mathfrak{p}^e)$.

Ist ferner $\Theta \equiv 1 \bmod L^{v+n\ell}$, also wenn λ eine genau durch $\mathfrak{l}$, Λ_0 eine mindestens durch L^v teilbare Zahl bedeutet,

$$\Theta = 1 + \lambda^n \Lambda_v$$

(λ sei in k ein– für allemal gegeben, Λ_v dadurch bestimmt). Dann lehrt die im Beweis zu Satz 8 mit (II) bezeichnete Gleichung S. 170▸

$$n(\Theta) \equiv 1 + \lambda^n S(\Lambda_v) \mod \mathfrak{l}^{v+n+1}$$

da ja bei ihrer Herleitung die spezielle Eigenschaft des dortigen $\Lambda_v^{(0)}$ noch nicht benutzt war.

Also gilt:

$$n(\Theta) \equiv 1 \mod \mathfrak{l}^{v+n}$$

Da nach (I) S. 165▸ $S(\Lambda_v) \equiv 0 \bmod \mathfrak{l}^v$ gilt.

Auch die Bedingung (5) wird also von ganzen Restklassen mod $L^{v+n\ell}$ erfüllt, da ja wie oben

$$\begin{array}{lll} \text{aus} & \Theta & \equiv \Theta_1 \mod L^{v+n\ell} \\ \text{folgt} & n(\Theta) & \equiv n(\Theta_1) \mod \mathfrak{l}^{v+n} \end{array}$$

Bezeichnen wir wieder mit H die durch (5) gekennzeichnete Untergruppe, so folgt wie oben, daß $(G : \mathsf{H})$ gleich der Anzahl der Normenrestklassen mod

$\mathfrak{l}^{v+n}$ ist, nach Satz 8 also:

213 ı

$$(G : \mathsf{H}) = \frac{1}{\ell}\phi_k(\mathfrak{l}^{v+n}).$$

Nun bezeichnen wir wieder mit H_0 die Gruppe, für die (4) bezw. (6) erfüllt ist, wo aber A eine zu $\mathfrak{P}$ bezw. L prime Zahl bedeutet. Diese ist nach dem Vorhergehenden wegen $n(\mathsf{A}^{1-\sigma}) = 1$ Untergruppe von H. Es sei Λ genau durch $\mathfrak{P}$ bezw. L teilbar. Dann ist $\Lambda^{1-\sigma}$ prim zu $\mathfrak{P}$ bezw. L und $n(\Lambda^{1-\sigma}) = 1$ Also ist $\Lambda^{1-\sigma}$ Element von H. Dagegen ist $(\Lambda^{1-\sigma})^\nu$ erst für $\nu \geqq \ell$ Zahl aus H_0. Denn aus

$$(\Lambda^{1-\sigma})^\nu = (\Lambda^\nu)^{1-\sigma} \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{P} \quad \text{bezw.} \quad L^{v+1}$$

folgt, wenn A zu $\mathfrak{P}$ bezw. L prim ist:

$$\left(\frac{\Lambda^\nu}{\mathsf{A}}\right)^{1-\sigma} \equiv 1 \mod \mathfrak{P} \quad \text{bezw.} \quad L^{v+1}$$

Da man $\frac{\Lambda^\nu}{\mathsf{A}}$ in die Form $\frac{\Lambda_\nu}{m}$ mit ganzem rat. m setzen kann, müßte es eine ganze genau durch $\mathfrak{P}^\nu$ bezw. L^ν teilbare Zahl Λ_ν geben, für die $\Lambda_\nu^{1-\sigma} \equiv 1 \bmod \mathfrak{P}$ bezw. L^{v+1}, also $\Lambda_\nu \equiv \sigma\Lambda_\nu \bmod \mathfrak{P}^{v+1}$ bezw. $L^{v+\nu+1}$. Für den Fall L wurde nun auf S. 151▸ unten gezeigt, daß $\Lambda_\nu - \sigma\Lambda_\nu$ für zu ℓ primes ν *genau* durch $L^{v+\nu}$ teilbar ist, was hier einen Widerspruch mit $\nu < \ell$ ergäbe. Also ist tatsächlich $\nu \geqq \ell$. Für den Fall $\mathfrak{P}$ ist die Unmöglichkeit von $\Lambda_\nu - \sigma\Lambda_\nu \equiv 0 \mod \mathfrak{P}^{v+1}$ darzutun. Es ist $\Lambda_\nu = \mathsf{B}\Lambda^\nu$, wo B prim zu $\mathfrak{P}$. □□□ Da in diesem Falle die Trägheitsgruppe den Grad ℓ hat (S. 28▸), also die Gruppe $1, \sigma, \ldots, \sigma^{\ell-1}$ selbst ist, folgt $\mathsf{B} \equiv \sigma\mathsf{B} \bmod \mathfrak{P}$. Nun ist $\mathsf{B}(\Lambda^\nu - \sigma\Lambda^\nu) = \big(\mathsf{B}\Lambda^\nu - \sigma(\mathsf{B}\Lambda^\nu)\big) - \sigma\Lambda^\nu(\mathsf{B} - \sigma\mathsf{B})$. Also wäre $\mathsf{B}(\Lambda^\nu - \sigma\Lambda^\nu) \equiv 0 \bmod \mathfrak{P}^{\nu+1}$, also

214 ı

$$\Lambda^\nu \equiv \sigma\Lambda^\nu \mod \mathfrak{P}^{\nu+1}$$

oder

$$\Lambda^\nu = \sigma\Lambda^\nu + \Pi_{\nu+1}$$

wo $\Pi_{\nu+1}$ durch $\mathfrak{P}^{\nu+1}$ teilbar ist. Also:

$$\Lambda^{\mu\nu} = (\sigma\Lambda^\nu + \Pi_{\nu+1})^\mu$$

□□□

Da $\sigma\Lambda^\nu$ durch $\mathfrak{P}^\nu$ teilbar ist, ist $\binom{\mu}{r}(\sigma\Lambda^\nu)^{\mu-r}\Pi^r_{\nu+1}$ durch $\mathfrak{P}^{\nu(\mu-r)+(\nu+1)r} = \mathfrak{P}^{\mu\nu+r}$, für $r \geqq 1$ also durch $\mathfrak{P}^{\mu\nu+1}$ teilbar, sodaß $\Lambda^{\mu\nu} \equiv \sigma\Lambda^{\mu\nu} \bmod \mathfrak{P}^{\mu\nu+1}$ gilt. Sei nun π genau durch $\mathfrak{p} = \mathfrak{P}^\ell$ teilbar (in k) und μ so gewählt, daß $\mu\nu \equiv 1 \bmod \ell$ (was für $\nu < \ell$ möglich), also $\mu\nu = 1 + m\ell$. Dann kann für beliebig große n die Kongruenz $\Lambda^{\mu\nu} \equiv \pi^m\Lambda_0 \bmod \mathfrak{P}^n$ gelöst werden, wo dann Λ_0 genau durch $\mathfrak{P}$ teilbar ist. Also □□□ wenn n groß genug gewählt war:

$$\Lambda^{\mu\nu} - \sigma\Lambda^{\mu\nu} \equiv \Pi^m(\Lambda_0 - \sigma\Lambda_0) \equiv 0 \mod \mathfrak{P}^{\mu\nu+1} = \mathfrak{P}^{m\ell+2}$$

d.h.

$$\Lambda_0 - \sigma\Lambda_0 \equiv 0 \mod \mathfrak{P}^2$$

Λ_0 gehört nicht zu k, da es sonst durch $\mathfrak{p}$ teilbar wäre. Nach unseren Ausführungen nach Satz 16 (S. 38▸ Mitte) gehört σ und damit die ganze Gruppe $1, \sigma, \ldots, \sigma^{\ell-1}$ zur Verzweigungsgruppe. Denn dort war gezeigt, daß eine Substitution v der Trägheitsgruppe, die eine den Körper erzeugende Primzahl $\pi \bmod \mathfrak{P}^2$ invariant läßt, zur Verzweigungsgruppe gehört. Damit ist gesagt, daß $\nu < \ell$ zu einem Widerspruch führt. Denn die Verzweigungsgruppe hat hier den Grad 1 (höchste in der Relat. Ordnung ℓ von $\mathfrak{P}$ enthaltenen Potenz von p), kann also nicht σ enthalten. Es ist also auch hier, und somit stets $\boldsymbol{\nu \geqq \ell}$.

Der Gruppen Index $(\mathsf{H} : \mathsf{H}_0)$ hat demnach mindestens den Wert ℓ, da es ein in H enthaltenes Element $\Lambda^{1-\sigma}$ gibt, dessen Potenzen $(\Lambda^{1-\sigma})^1$, $(\Lambda^{1-\sigma})^2$, …, $(\Lambda^{1-\sigma})^{\ell-1}$ sicher nicht in H_0 liegen und in Bezug auf H_0 unabhängig sind.

215 ı

$$(\mathsf{H} : \mathsf{H}_0) \geqq \ell$$

Wenn noch gezeigt werden kann, daß $(G : \mathsf{H}_0) = \phi_k(\mathfrak{p}^\ell)$ bezw. $\phi_k(\mathfrak{l}^{v+n})$ ist, so wäre nach dem Obigen (S. 212▸/13▸)

$$(\mathsf{H} : \mathsf{H}_0) = \ell$$

nachgewiesen und sogar noch mehr, daß nämlich die folgende Zerlegung in Nebengruppen bestände:

$$\mathsf{H} = \mathsf{H}_0 + \Lambda^{1-\sigma}\mathsf{H}_0 + (\Lambda^{1-\sigma})^2\mathsf{H}_0 + \cdots + (\Lambda^{1-\sigma})^{\ell-1}\mathsf{H}_0$$

Für jedes Θ aus H würde also gelten:

$$\Theta = (\Lambda^i \mathsf{A})^{1-\sigma}; \quad (0 \leqq i < \ell)$$

wo A prim zu $\mathfrak{P}$ bezw. L und unser Satz wäre bewiesen.

Es kommt also auf den Nachweis:

$$(G : \mathsf{H}_0) = \phi_k(\mathfrak{p}^c) \quad \text{bezw.} \quad \phi_k(\mathfrak{l}^{v+n})$$

an. □□□

(siehe S. 218 oben.)

1.) Sei $\mathfrak{P}$ prim zu ℓ. Da $\mathfrak{P}$ ambig ist, gilt für unser A:

$$\left.\begin{array}{c} \mathsf{A} \equiv \sigma\mathsf{A} \equiv \cdots \equiv \sigma^{\ell-1}\mathsf{A} \\ \text{also} \qquad \ell\mathsf{A} \equiv S(\mathsf{A}) \end{array}\right\} \mod \mathfrak{P}^{(e-1)\ell+1}$$

Da ℓ prim zu $\mathfrak{P}$ ist, ist $\ell\alpha \equiv 1 \bmod \mathfrak{p}^n$ für beliebig hohes n durch ein α aus k lösbar. Dann folgt

$$\mathsf{A} \equiv \alpha S(\mathsf{A}) \mod \mathfrak{P}^{(e-1)\ell+1}$$

Da $S(\mathsf{A})$ aus k, ist alles bewiesen.

2.) Für L schlagen wir einen anderen Weg ein indem wir $(G : \mathsf{H}_0) = \phi_k(\mathfrak{l}^{v+n})$ direkt beweisen. Wegen $\Phi_K(L) = \Phi_k(\mathfrak{l})$ (da der Relativgrad von L gleich 1) ist A einer Zahl α aus k mod L kongruent. Entweder ist nun

$$\mathsf{A} \equiv \alpha \mod L^{v+n\ell}$$

oder aber es ist $t < v + n\ell$ der höchste Exponent, für den $\mathsf{A} \equiv \alpha \bmod L^t$ also:

$$\mathsf{A} \equiv \alpha + \Lambda_t \mod L^{v+n\ell}$$

gilt, wo Λ_t genau durch L^t teilbar und α *irgendeine* Zahl aus k ist. Dann kann t nicht durch ℓ teilbar sein. Denn wäre $t = \mu\ell$ und $\lambda\mu$ eine genau durch $\mathfrak{l}^\mu = L^t$ teilbare Zahl, so wäre $\Lambda_t \equiv \mathsf{B}\lambda\mu \bmod L^{v+n\ell}$, wo B prim zu L. Setzen wir dann $\mathsf{B} \equiv \alpha_1 + \Lambda_x \bmod L^{v+n\ell}$ mit $x \geqq 1$, so ist

$$\mathsf{A} \equiv \alpha + \alpha_1\lambda\mu + \lambda\mu\Lambda_x \equiv \alpha_2 + \Lambda_{t+x} \bmod L^{v+n\ell}$$

entgegen der Bestimmung von t.

Aus $\sigma\mathsf{A} \equiv \mathsf{A} \bmod L^{v+n\ell}$ folgt dann $\sigma\Lambda_t \equiv \Lambda_t \bmod L^{v+n\ell}$

Nach S. 151 unten ist nun aber wegen $t \not\equiv 0 \bmod \ell$ $\sigma\Lambda_t - \Lambda_t$ genau durch L^{v+t} teilbar, sodaß folgt:

$$n\ell < t.$$

Auf jeden Fall ist also, wenn Λ fest und genau durch L teilbar, für jedes A, das unserer Bedingung genügt:

$$\mathsf{A} \equiv \alpha_0 + \mathsf{B}\Lambda^{n\ell+1} \bmod L^{v+n\ell}$$

□□□

Entwickelt man B nach Potenzen von Λ:

$$\mathsf{B} = \beta_0 + \beta_1\Lambda + \cdots$$

so wird:

$$\mathsf{A} \equiv \alpha_0 + \beta_1\Lambda^{n\ell+1} + \beta_2\Lambda^{n\ell+2} + \ldots + \beta_{v-1}\Lambda^{n\ell+v-1} \mod L^{n\ell+[\ldots]}$$

wo α_0 prim zu $\mathfrak{l}$ ist und wie die β_i zu k gehört.

Umgekehrt ist jeder solche Ausdruck eines unserer zu untersuchenden A. Denn $\sigma\Lambda^{n\ell+\mu} - \Lambda^{n\ell+\mu}$ ist nach S. 151 unten mindestens durch $L^{n\ell+\mu+v}$ teilbar, also sicher $\mathsf{A} \equiv \sigma\mathsf{A} \bmod L^{n\ell+[\ldots]}$.

Ist

$$\mathsf{A}' \equiv \alpha'_0 + \beta'_1\Lambda^{n\ell+1} + \cdots + \beta'_{v-1}\Lambda^{n\ell+v-1} \bmod L^{\ell+v}$$

und $\mathsf{A} \equiv \mathsf{A}' \bmod L^{n\ell+v}$, so folgt in leichter Weise

$$\alpha_0 \equiv \alpha'_0 \bmod L^{n\ell+1}, \quad \text{also} \quad \bmod \mathfrak{l}^{n+1}$$

Wird andererseits in A für α_0 ein mod $\mathfrak{l}^{n+1} = L^{n\ell+\ell}$ kongruentes α'_0 gesetzt, so kann man ersichtlich durch passende Wahl der β_i ein zu A mod $L^{n\ell+v}$ kongruentes A' dieser Form herstellen, das mit α'_0 beginnt. Wir können also alle unsere A so transformiert denken, daß ihr Anfangsglied α_0 einem festen primen Restsystem mod $\mathfrak{l}^{n+1}$ angehört, dann folgt also aus $\mathsf{A} \equiv \mathsf{A}' \bmod L^{n\ell+v}$, daß $\alpha_0 = \alpha'_0$, also $\beta_1 \equiv \beta'_1 \bmod L$ also mod $\mathfrak{l}$ ist. Wieder kann β auf ein festes Restsystem eingeschränkt werden etz. . . . , sodaß also schließlich jedes A mod

$L^{n\ell+v}$ in obiger Form darstellbar ist, sodaß $\alpha_0, \beta_1, \ldots, \beta_{v-1}$ sämtlich feste Restsysteme mod $\mathfrak{l}$ durchlaufen, (dabei α_0 prim zu ℓ), und daß zwei mod $L^{n\ell+v}$ kongruente so dargestellte A identisch sind. Die Anzahl der mod $L^{n\ell+v}$ inkongruenten A ist also: $\phi_k(\mathfrak{l}^{n+1})(\ell^f)^{v-1}$, wenn f der Grad von $\mathfrak{l}$ ist. Also:

$$(\ell^{f(n+1)} - \ell^{fn})\ell^{f(v-1)} = \ell^{f(n+v)}\left(1 - \frac{1}{\ell^f}\right) = \Phi_k(\mathfrak{l}^{n+v}),$$

da die Anzahl der für unsere A möglichen Restklassen mod $L^{n\ell+v}$ nach S. 218▸ gleich $(G_0 : \mathsf{H}_0)$ ist, ist somit $(G : \mathsf{H}_0) = \Phi_k(\mathfrak{l}^{v+n})$ auch im letzten Falle gezeigt.

F Bemerkung zu S. 215▸.

Genau wie beim Beweis zu Hilfssatz 1 sieht man nun ein, daß $(G : \mathsf{H}_0)$ gleich der Anzahl derjenigen primen Restklassen mod $\mathfrak{P}^{(e-1)\ell+1}$ bezw. $L^{v+n\ell}$ ist, für deren Zahlen A die Bedingung besteht:

$$\mathsf{A} \equiv \sigma\mathsf{A} \mod \mathfrak{P}^{(e-1)\ell+1} \quad \text{bezw.} \quad L^{v+n\ell}.$$

□□□

Für den Fall L werden wir in 2.) S. 216▸ direkt nachweisen, daß diese Restklassenzahl für die A gleich $\phi_k(\mathfrak{l}^{v+n})$ ist. Für $\mathfrak{P}$ prim zu ℓ dagegen zeigen wir, daß jedes dieser Bedingung genügende (prime) A einer Zahl α aus k nach dem mod $\mathfrak{P}^{(e-1)\ell+1}$ kongruent ist (1.) S. 215▸). Die Anzahl unserer A–Restklassen ist also □□□ höchstens so groß, wie die der primen Restklassen in k nach $\mathfrak{p}^{e-1+\frac{1}{\ell}}$, d.h. $\mathfrak{p}^{\ell}$, also $(G : \mathsf{H}_0) \leqq \phi_k(\mathfrak{p}^e)$. □□□ Da andererseits die $\phi_k(\mathfrak{p}^e)$ Restklassen mod $\mathfrak{p}^e$ in k auch nach dem Modul $\mathfrak{P}^{(e-1)\ell+1}$ verschieden sind (π–adische Entwicklung), so liefert jede prime Restklasse mod $\mathfrak{p}^e$ in k eine Restklasse mod $\mathfrak{P}^{(e-1)\ell+1}$ in K, die offensichtlich der Bedingung auch dieser Seite oben genügt, womit nach dem schon Gesagten dann alles gezeigt ist.

Die beiden bewiesenen Hilfssätze benutzen wir jetzt zur Aufstellung des folgenden allgemeinsten Hilfssatzes in derselben Richtung:

Hilfssatz 3. Es sei $f^{\ell-1}$ die Relativdiskriminante von K,

$$f = \Pi\mathfrak{p}\Pi\mathfrak{l}^{v+1}; \quad \mathfrak{p} = \mathfrak{P}^{\ell}; \quad \mathfrak{l} = L^{\ell} \quad \text{und}$$

$\mathfrak{m} = f\mathfrak{a}$ ein beliebiges, durch f teilbares Ideal in k. Wir setzen

$$\mathfrak{F} = \Pi\mathfrak{P}\Pi L^{v+\ell}$$

(jedes $\mathfrak{P}$ und L einmal genommen) und

$$\mathfrak{M} = \mathfrak{F} \cdot \mathfrak{a}$$

sodaß also $\mathfrak{M}$ in K liegt.

Ist Θ eine zu $\mathfrak{M}$ prime Zahl in K, welche der Bedingung

$$n(\Theta) \equiv 1 \mod \mathfrak{m}$$

genügt, dann gibt es in K eine Zahl A derart, daß

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{M}$$

wird.

Dieses A ist unter Umständen nicht prim zu $\mathfrak{M}$, aber von der Art, daß

$$(\mathsf{A})^{1-\sigma} = \mathfrak{A}^{1-\sigma}$$

ist, wo $\mathfrak{A}$ ein zu $\mathfrak{M}$ primes Ideal in K ist.

Für $\ell = 2$ kann A auch noch eine beliebig vorgeschriebene Signatur haben.

Beweis. Setzt man, unter $\mathfrak{q}$ zu f prime Primideale verstehend,

$$\mathfrak{m} = \Pi\mathfrak{p}^{e}\Pi\mathfrak{l}^{v+n}\Pi\mathfrak{q}^{e'},$$

so ist nach Voraussetzung

$$e \geqq 1; \quad n \geqq 1; \quad e' \geqq 0.$$

und

$$\mathfrak{M} = \Pi\mathfrak{P}^{(e-1)\ell+1}\Pi L^{v+n\ell}\Pi\mathfrak{q}^{e'}.$$

Erstreckt man $\Pi\mathfrak{q}^{e'}$ nur auf die in $\mathfrak{m}$ wirklich vorkommenden Primideale, so kann auch $e' \geqq 1$ angenommen werden.

Nach unseren Hilfssätzen 1 und 2 ergeben sich, wenn man noch die auf S. 215 angegebene Zerlegung von H in Nebengruppen nach H_0 beachtet, für Θ die Kongruenzen:

$$\begin{array}{lcll} \Theta & \equiv & (\Pi^{\alpha}\mathsf{A}_1)^{1-\sigma} & \mod \mathfrak{P}^{(e-1)\ell+1} \quad \text{für alle } \mathfrak{P} \\ \Theta & \equiv & (\Lambda^{\beta}\mathsf{A}_2)^{1-\sigma} & \mod L^{v+n\ell} \quad \text{" " } L \\ \Theta & \equiv & \mathsf{A}_3^{1-\sigma} & \mod \mathfrak{q}^{e'} \quad \text{" " } \mathfrak{q}, \end{array}$$

wo Π, Λ genau durch $\mathfrak{P}, L$ teilbare Zahlen aus K und α, β Zahlen $0, 1, \ldots, \ell-1$ sind. Da Π, Λ sonst beliebig sind, können sie nach den Forderungen:

$$\Pi \equiv 1 \bmod \frac{\mathfrak{M}}{\mathfrak{P}^{(e-1)\ell+1}}; \quad \Lambda \equiv 1 \bmod \frac{\mathfrak{M}}{L^{v+n\ell}}$$

unterworfen werden. $\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$ sind zu den betr. Moduln prime Zahlen, die nach genügenden hohen Potenzen von $\mathfrak{P}, L, \mathfrak{q}$ als Moduln durch beliebige kongruente ersetzt werden dürfen, also noch den Forderungen:

$$\mathsf{A}_1 \equiv 1 \bmod \frac{\mathfrak{M}}{\mathfrak{P}^{(e-1)\ell+1}}; \quad \mathsf{A}_2 \equiv 1 \bmod \frac{\mathfrak{M}}{L^{v+n\ell}}; \quad \mathsf{A}_3 \equiv 1 \bmod \frac{\mathfrak{M}}{\mathfrak{q}^{e'}}$$

unterworfen werden dürfen.

Setzt man dann:

$$\mathsf{A} = (\Pi^{\alpha}\mathsf{A}_1)\ldots \quad (\Lambda^{\beta}\mathsf{A}_2)\ldots \quad \mathsf{A}_3 \ldots$$

so wird:

$$\mathsf{A}^{1-\sigma} \equiv \Theta$$

nach jedem der Primidealpotenzmoduln, also mod $\mathfrak{M}$. Dabei ist A nach einem genügend hohen Modul $\mathfrak{M}^t$ beliebig teilbar, kann also jede Signatur erhalten.

Endlich sei

$$(\Pi) = \mathfrak{P}\mathfrak{A}_1 \ldots; \quad (\Lambda) = L\mathfrak{A}_2 \ldots$$

Dann ist, da nach unseren Forderungen Π, Λ prim zu allen übrigen Faktoren von $\mathfrak{M}$ sind, $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ prim zu $\mathfrak{M}_1$ und daher, wie leicht ersichtlich

$$(\mathsf{A})^{1-\sigma} = \mathfrak{A}^{1-\sigma}$$

wo $\mathfrak{A}$ prim zu $\mathfrak{M}$ ist. (Dann $\mathfrak{P}^{1-\sigma} = 1$; $L^{1-\sigma} = 1$)

221 I

Nun können wir die angekündigte Erweiterung des Geschlechtsbegriffs geben:

Es mögen $\mathfrak{m}$ und $\mathfrak{M}$ die in Hilfssatz 3 erklärte Bedeutung haben; dann wählen wir in k und K die Strahlen der Zahlen

$$\begin{array}{rcl} \alpha & \equiv & 1 \bmod \mathfrak{m} \quad \text{und für } \ell = 2 \text{ total positiv} : \text{Strahl } o \\ \mathsf{A} & \equiv & 1 \bmod \mathfrak{M} \quad \text{" " " " " " } : \text{Strahl } O. \end{array}$$

Wir definieren die Idealklassen in k und K nach diesen Strahlen.

Es seien nun die Ideale $\mathfrak{A}, \mathfrak{B}$ aus K prim zu $\mathfrak{M}$ und äquivalent. Dann ist $\frac{\mathfrak{A}}{\mathfrak{B}} = (\Theta)$, wo $\Theta \equiv 1 \bmod \mathfrak{M}$ ist, also auch nach jeder in $\mathfrak{M}$ aufgehenden Primidealpotenz. Wie im Beweise von Hilfssatz 1 und 2 gezeigt, ist dann $n(\Theta) \equiv 1$ nach jeder zugehörigen Primidealpotenz von $\mathfrak{m}$, also $n(\Theta) \equiv 1 \bmod \mathfrak{m}$. Im Falle $\ell = 2$ ist Θ auch noch total positiv. Dann ist auch $n(\Theta)$ in k total positiv, denn eine in reellen Körpern liegende konjugierte zu $n(\Theta)$ ist entweder das Produkt zweier konjugiert komplexer Größen, also > 0 oder das Produkt zweier reellen, *positiven* da Θ total positiv, also auch dann > 0. Es ist also $n(\Theta)$ in o enthalten.

Ist also $\frac{\mathfrak{A}}{\mathfrak{B}} = (\Theta)$ und Θ in O enthalten, so ist $\frac{n(\mathfrak{A})}{n(\mathfrak{B})} = \big(n(\Theta)\big)$ und $n(\Theta)$ in o enthalten, d.h. $n(\mathfrak{A})$ und $n(\mathfrak{B})$ sind äquivalent. Die Relativnormen aller Ideale einer Klasse $\mathfrak{K}$ von K liegen also in *einer* Klasse $\mathfrak{k}$ von k, sodaß wieder

$$k = n(\mathfrak{K})$$

gesetzt werden kann.

Ohne weiteres sieht man wieder, daß $n(\mathfrak{K}_1\mathfrak{K}_2) = n(\mathfrak{K}_1)n(\mathfrak{K}_2)$ ist. Die Relativnormen der Klassen in K bilden also eine

222 I

Klassengruppe H in k. Diese Klassengruppe besteht einfach aus allen Klassen, die Relativnormen der zu $\mathfrak{m}$ primen Ideale aus K enthalten und ist somit von der früher in e.) f.) eingeführten Klassengruppe H (S. 198▶, 204▶) nicht verschieden. Denn die eben ausgesprochene Definition lehrt ja, daß H gar nicht von der Einteilung in Idealklassen in k und K abhängt. Ihr Index (dieser war stets invariant), ist also derselbe, d.h. gleich ℓ. Unsere neue Definition dieser Klassengruppe hat gegenüber der früheren in e.) und f.) den Vorzug,

daß sie nicht mehr die Normenreste verwendet. Unsere Wahl des Strahles o gewährleistet, daß *jede* Klassengruppe vom Index ℓ wirklich erscheint als Gruppe von *Idealklassen nach o*. (Weil eben o der engste Strahl $[\ldots]\ \mathfrak{m}$ ist und somit alle Klassengruppen nach diesem Strahl definierbar sind).

Wir haben nun wie früher die Idealklassen von K in Geschlechter, indem in das gleiche Geschlecht alle Klassen $\mathfrak{K}$ gleicher Relativnorm zusammengefaßt werden. Insbesondere ist das Hauptgeschlecht der Inbegriff aller Klassen aus K, deren Relativnorm die Hauptklasse von k nach o, d.h. o selbst, ist.

Haben zwei Klassen $\mathfrak{K}_1$ und $\mathfrak{K}_2$ gleiche Relativnorm, so hat ihr Quotient als Relativnorm o, liegt also im Hauptgeschlecht, und umgekehrt. Das Hauptgeschlecht ist Untergruppe zur Gruppe aller Geschlechter, die als Nebengruppen auftreten, also alle gleich viel Klassen enthalten. Jeder Klasse von H entspricht ein Geschlecht und umgekehrt, sodaß die Anzahl der Geschlechter gleich der Anzahl der Klassen nach o in H ist. Ist h die Klassenzahl nach o, so hat H, da es den Index ℓ hat, $\frac{h}{\ell}$ Klassen, sodaß die Anzahl der Geschlechter $\frac{h}{\ell}$ ist.

223 I

Da mit Θ auch $\sigma\Theta$ zu O gehört ($\mathfrak{M}^{1-\sigma} = 1$), liegen, wenn $\mathfrak{A}$ alle Ideale der Klassen $\mathfrak{K}$ durchläuft, auch die $\sigma\mathfrak{A}$ sämtlich in *einer* Klasse $\sigma\mathfrak{K}$, wodurch das Symbol $\mathfrak{K}^{1-\sigma} = \frac{\mathfrak{K}}{\sigma\mathfrak{K}}$ erklärt ist. Z.B. liegt $\mathfrak{A}^{1-\sigma}$ in $\mathfrak{K}^{1-\sigma}$. Da $n(\mathfrak{A}^{1-\sigma}) = 1$, gehört $\mathfrak{K}^{1-\sigma}$ zum Hauptgeschlecht.

Es gilt aber auch die Umkehrung: *Jede Klasse* $\mathfrak{K}_1$ *des Hauptgeschlechts ist* $\mathfrak{K}_1 = \mathfrak{K}^{1-\sigma}$.

Beweis. Für Ideale ausgesprochen bedeutet dies: Jedes zu $\mathfrak{M}$ prime Ideal $\mathfrak{A}$ aus K, dessen Relativnorm in o liegt, läßt sich in der Form $\mathfrak{A} = \mathfrak{B}^{1-\sigma}\Theta$ darstellen, wo $\mathfrak{B}$ prim zu $\mathfrak{M}$ und Θ Zahl in O ist.

Die Sätze 19 und 24, in dieser Form ausgesprochen, lehren uns nun schon, daß für ein $\mathfrak{A}$, dessen Relativnorm in o, also sicher in dem dort zugrundegelegten Strahl, liegt, eine Darstellung

$$\mathfrak{A} = \mathfrak{C}^{1-\sigma}(\mathsf{A})$$

gilt, wo $\mathfrak{C}$ prim zu f ist, und A prim zu f,

□□□

$\mathfrak{C}$ darf dann ohne weiteres auch prim zu $\mathfrak{M}$ angenommen werden, da in der Klasse von $\mathfrak{C}$ (im Sinne von e.), f.)) sicher zu $\mathfrak{M}$ prime Ideale enthalten sind. Dann ist auch A prim zu $\mathfrak{M}$.

Dagegen wissen wir vorläufig noch nicht, ob wir A so wählen dürfen, daß es in O liegt, womit unser Satz bewiesen wäre.

Das zeigen wir so:

224 I

Es ist $n(\mathfrak{A}) = (\alpha)$, wo α in o liegt, also

$$n(\mathsf{A}) = \varepsilon\alpha; \quad \varepsilon \text{ Einheit aus } k.$$

Da nun $\alpha \equiv 1 \bmod \mathfrak{m}$, also erst recht mod f, ist ε Normenrest nach f. Ferner ist für $\ell = 2$ α total positiv und $n(\mathsf{A})$ wenigstens in jenen reellen konjugierten zu k positiv, in denen die den Körper $K = k(\sqrt{\mu})$ bestimmende Zahl μ negativ ist. ε ist dann also in jenen reellen Körpern positiv. Nach Satz 20 bezw. 25 ist also

$$\varepsilon = n(\mathsf{B}); \quad \mathsf{B} \text{ aus } K.$$

Wie auf S. 193 gezeigt, folgt daraus

$$(\mathsf{B}) = \mathfrak{B}^{1-\sigma}; \quad \mathfrak{B} \text{ Ideal in } K.$$

Die Zahl B ist nur bis auf einen Faktor $\mathsf{A}_1^{1-\sigma}$ bestimmt, da ja $n(\mathsf{B}\mathsf{A}_1^{1-\sigma}) = n(\mathsf{B}) = \varepsilon$ ist. Infolgedessen darf $\mathfrak{B}$ noch mit einer beliebigen Zahl A_1 aus K multipliziert werden. Sei $\mathfrak{B}_1$ der Faktor von $\mathfrak{B}$, der □□□ mit $\mathfrak{M}$ Teiler gemein hat, dann wählen wir $\mathfrak{B}_2$ prim zu $\mathfrak{M}$ so, daß $\mathfrak{B}_1\mathfrak{B}_2$ ein Ideal (A_1) aus O wird und ersetzen $\mathfrak{B}$ durch $\frac{\mathfrak{B}}{(\mathsf{A}_1)}$. So erkennt man, daß $\mathfrak{B}$ von vorneherein prim zu $\mathfrak{M}$ angenommen werden darf.

Es ist dann auch B prim zu $\mathfrak{M}$ und:

$$n\left(\frac{\mathsf{A}}{\mathsf{B}}\right) = \alpha; \quad \alpha \text{ in } o.$$

Nach Hilfssatz 3 ist also:

$$\frac{\mathsf{A}}{\mathsf{B}} \equiv \mathsf{A}_1^{1-\sigma} \mod \mathfrak{M}.$$

Da A und B prim zu $\mathfrak{M}$, ist $\mathsf{A}_1^{1-\sigma}$ sicher prim zu $\mathfrak{M}$, (nicht aber immer A_1 selbst). Also ist

$$\frac{\mathsf{A}}{\mathsf{B}} = \mathsf{A}_1^{1-\sigma}\Omega; \quad \Omega \text{ aus } O$$

Da A_1 beliebige Signatur haben kann, darf im Falle $\ell = 2$ A_1 so gewählt werden, daß $\mathsf{A}_1^{1-\sigma}$ die gleiche Signatur wie $\frac{\mathsf{A}}{\mathsf{B}}$ hat, also Ω total positiv wird. Um dies genau zu begründen machen wir folgende Überlegung. Die Signatur von $\mathsf{A}_1^{1-\sigma}$ ist so beschaffen, daß in zwei

reellen relativ konjugierten Körpern K sicher $\mathsf{A}_1^{1-\sigma}$ gleiche Signatur hat, denn die konjugierten sind $\frac{\mathsf{A}_1}{\sigma\mathsf{A}_1}$ und $\frac{\sigma\mathsf{A}_1}{\mathsf{A}_1}$, von gleicher Signatur. □□□ In einem bestimmten Paar reeller, relativ konjugierter Körper K sei nun $\operatorname{sgn}(\mathsf{A}\sigma\mathsf{A}) = (-1)^c$. Da α total positiv ist, ist in dem entsprechenden Körper k $\operatorname{sgn}\varepsilon = (-1)^c$, also $\operatorname{sgn}(\mathsf{B}\sigma\mathsf{B}) = (-1)^c$, d.h. $\operatorname{sgn}(\mathsf{A}\cdot\sigma\mathsf{A}) = \operatorname{sgn}(\mathsf{B}\cdot\sigma\mathsf{B})$

$$\operatorname{sgn}\left(\frac{\mathsf{A}}{\mathsf{B}}\right) = \operatorname{sgn}\left(\frac{\sigma\mathsf{A}}{\sigma\mathsf{B}}\right) = \operatorname{sgn}\sigma\left(\frac{\mathsf{A}}{\mathsf{B}}\right)$$

Es erfüllt also $\left(\frac{\mathsf{A}}{\mathsf{B}}\right)$ die notwendige Bedingung zur Vorzeichenbestimmung von A_1.

Es liegt also dann in

$$\frac{\mathsf{A}}{\mathsf{B}} = \mathsf{A}_1^{1-\sigma}\Omega$$

die Zahl Ω auch im Falle $\ell = 2$ in O.

Nach Hilfssatz 3 kann ferner

$$(\mathsf{A}_1)^{1-\sigma} = \mathfrak{A}_1^{1-\sigma}$$

mit zu $\mathfrak{M}$ primem $\mathfrak{A}_1$ gesetzt werden, somit

$$\mathsf{A} = \mathsf{B}\mathsf{A}_1^{1-\sigma}\Omega$$
$$(\mathsf{A}) = (\mathfrak{B}\mathfrak{A}_1)^{1-\sigma}(\Omega)$$

wo $\mathfrak{B}\mathfrak{A}_1$ prim zu $\mathfrak{M}$ und Ω in O. Schließlich

$$\mathfrak{A} = \mathfrak{B}^{1-\sigma}(\mathsf{A}) = (\mathfrak{C}\mathfrak{B}\mathfrak{A}_1)^{1-\sigma}(\Omega)$$

wo $\mathfrak{C}\mathfrak{B}\mathfrak{A}_1$ prim zu $\mathfrak{M}$ und Ω in O, w.z.b.w.

Satz 29. Werden die Idealklassen in k und K nach den Moduln $\mathfrak{m}$ und $\mathfrak{M}$ in der angegebenen Weise definiert, und der Begriff des Geschlechtes, wie eben, erklärt, so gilt:

a.) Die Anzahl der Geschlechter ist gleich dem ℓ–ten Teil der Klassenanzahl h von k nach o.

b.) Jedes Geschlecht in K enthält gleich viele Klassen in K mit gleicher Relativnorm.

c.) Das Hauptgeschlecht ist der Inbegriff aller Klassen der Form $\mathfrak{K}^{1-\sigma}$ und ist eine Klassengruppe in K.

1.6 Der Rang Abelscher Gruppen.

226 I

a) Die Zerlegungsgesetze im ℓ–ten Kreiskörper

a) Die Zerlegungsgesetze im Kreiskörper der ℓ–ten Einheitswurzeln

Im weiteren Verlaufe brauchen wir einige wenige Tatsachen aus der Theorie des Körpers $R(\zeta)$, wo $\zeta = e^{\frac{2\pi i}{\ell}}$ eine ℓ–te Einheitswurzel und ℓ eine ungerade Primzahl ist.

ζ genügt der Gleichung $(\ell-1)$–ten Grades

$$F(x) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1 = (x-\zeta)\ldots(x-\zeta^{\ell-1}) = 0$$

Der Körper $R(\zeta)$ ist also Galoissch und höchstens vom Grade $\ell - 1$. Wir beweisen zunächst, daß sein Grad genau $\ell - 1$ ist, d.h. daß $F(x)$ irreduzibel ist.

In der Tat, setzen wir in obiger Identität $x = 1$, so wird

$$\ell = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{\ell-1})$$

Wir betrachten nun das Hauptideal $(1-\zeta^a)$, wo a prim zu ℓ ist, und zeigen, daß es mit $(1-\zeta)$ übereinstimmt. In der Tat ist ja $\frac{1-\zeta^a}{1-\zeta} = 1+\zeta+\zeta^2+\cdots+\zeta^{a-1}$ ganz, da ζ ganz, ferner aber auch, wenn $aa' \equiv 1 \bmod \ell$, also $\zeta = \zeta^{aa'}$:

$$\frac{1-\zeta}{1-\zeta^a} = \frac{1-\zeta^{aa'}}{1-\zeta^a} = 1 + \zeta^a + \zeta^{2a} + \cdots + \zeta^{(a'-1)a} \quad \text{ganz, was}$$

gezeigt werden sollte. Nebenbei ist $\frac{1-\zeta^a}{1-\zeta}$ als Einheit erkannt.

Es ist also, wenn $(1-\zeta) = \mathfrak{l}$ gesetzt wird

$$\ell = \left((1-\zeta)^{\ell-1}\right) = \mathfrak{l}^{\ell-1}$$

Da nun eine Primzahl in einem Körper n–ten Grades in höchstens n Primfaktoren zerlegbar ist, und wenn dies der Fall ist, diese wirklich alle Primfaktoren

sind, ist der Grad von $R(\zeta)$ mindestens $\ell - 1$, also genau $\ell - 1$, also $F(x)$ irreduzibel.

Gleichzeitig ist

$$\ell = \mathfrak{l}^{\ell-1}$$

die $(\ell - 1)$ te Potenz eines Primideals $\mathfrak{l}$ in $R(\zeta)$.

227 I

Daher muß noch ℓ in der Diskriminante aufgehen.

Die Substitutionsgruppe von $R(\zeta)$ besteht aus den Substitutionen (ζ/ζ^a); $(a = 1, 2, \ldots, \ell - 1)$. Zwei von ihnen setzen sich so zusammen:

$$(\zeta/\zeta^a)(\zeta/\zeta^b) = (\zeta/\zeta^{ab}) = (\zeta/\zeta^c) \quad \text{wenn} \quad ab \equiv c \bmod \ell$$

Sie sind ersichtlich kommutativ, $R(\zeta)$ also Abel'scher Körper. Sei g primitive Wurzel mod ℓ. Dann lassen sich die Substitutionen so ordnen.

$$\sigma_0 = (\zeta/\zeta); \quad \sigma_1 = (\zeta/\zeta^g); \quad \sigma_2 = (\zeta/\zeta^{g^2}); \quad \ldots; \quad \sigma_{\ell-2} = (\zeta/\zeta^{g^{\ell-2}})$$

Dann ist

$$\sigma_i \sigma_k = (\zeta/\zeta^{g^i})(\zeta/\zeta^{g^k}) = (\zeta/\zeta^{g^{i+k}}) = \sigma_{i+k}$$

also $\sigma_\nu = \sigma_1^\nu$. Setzt man somit $\sigma = \sigma_1 = (\zeta/\zeta^g)$, so sind die Substitutionen:

$$\sigma^0, \sigma^1, \sigma^2, \ldots, \sigma^{\ell-2}$$

Die Gruppe ist also zyklisch vom Grade $\ell - 1$, unser Körper also auch.

Da $\ell = \mathfrak{l}^{\ell-1}$ ist, ist $\mathfrak{l}$ vom Grad 1. Eine Verzweigungsgruppe ist, da $\ell - 1$ prim zu ℓ, nicht vorhanden. Nach Satz 19 (S. 48) geht also in der Körperdiskriminante genau die Potenz $\ell^{\ell-2}$ von ℓ auf.

Nun betrachten wir das System der Zahlen:

$$\omega_1 = \zeta; \quad \omega_2 = \zeta^2; \quad \ldots \quad ; \quad \omega_{\ell-1} = \zeta^{\ell-1},$$

von denen wir nachweisen wollen, daß sie eine Basis des Körpers bilden. In der Tat ist die Diskriminante dieses Systems gleich der Diskriminante der Gleichung $F(x) = 0$, d.h. gleich

$$(\zeta - \zeta^2)^2(\zeta - \zeta^3)^2 \ldots (\zeta - \zeta^{\ell-1})^2 \cdot (\zeta^2 - \zeta^3)^2 \ldots (\zeta^2 - \zeta^{\ell-1})^2 \ldots\ldots (\zeta^{\ell-2} - \zeta^{\ell-1})^2$$

$$= [(\zeta - \zeta^2)(\zeta - \zeta^3)\dots(\zeta - \zeta^{\ell-1})][-(\zeta^2 - \zeta)(\zeta^2 - \zeta^3)\dots(\zeta^2 - \zeta^{\ell-1})]\dots$$
$$\cdot [(-1)^{\nu-1}(\zeta^\nu - \zeta)(\zeta^\nu - \zeta^2)\dots(\zeta^\nu - \zeta^{\ell-1})]\cdots$$

$$= (-1)^{1+2+\cdots+\ell-2}, \quad F'(\zeta)\cdot F'(\zeta^2)\dots F'(\zeta^{\ell-1})$$
$$= (-1)^{\frac{\ell-1}{2}} F'(\zeta)\dots F'(\zeta^{\ell-1}).$$

Nun ist $(x-1)F(x) = x^\ell - 1$, also $F(x) + (x-1)F'(x) = \ell x^{\ell-1}$ sodaß $F'(\zeta^{[\dots]}) = \frac{\ell\zeta^{\nu(\ell-1)}}{\zeta^\nu - 1} = -\ell\frac{\zeta^{-\nu}}{1-\zeta^\nu}$
Wir finden somit

$$F'(\zeta)\dots F'(\zeta^{\ell-1}) = \ell^{\ell-1}\frac{\zeta^{-1-2\cdots-(\ell-1)}}{(1-\zeta)\cdots(1-\zeta^{\ell-1})} = \ell^{\ell-1}\cdot\frac{1}{\ell} = \ell^{\ell-2}.$$

Die Diskriminante des Systems wird also $(-1)^{\frac{\ell-1}{2}}\ell^{\ell-2}$. Es ist also $\ell^{\ell-2}$ die einzige in der Körperdiskriminante aufgehende Primzahlpotenz. Da ferner der Quotient jeder Gleichungsdiskriminante durch die Körperdiskriminante ein Quadrat sein muß, ist letztere genau $(-1)^{\frac{\ell-1}{2}}\ell^{\ell-2}$. Ferner ist das System $\zeta, \zeta^2, \dots, \zeta^{\ell-1}$ eine Basis.

Nun sei p eine von ℓ verschiedene Primzahl. Sei f der kleinste Exponent, für den $p^f \equiv 1 \bmod \ell$, sodaß nach dem Fermatschen Satz $\ell - 1 = ef$ gesetzt werden kann.

Jede ganze Körperzahl ist mit ganzen a_i in der Form darstellbar:

$$\alpha = a_1\zeta + \cdots + a_{\ell-1}\zeta^{\ell-1}$$

Da $\zeta^{\ell-1} = -1 - \zeta\cdots - \zeta^{\ell-2}$ ist, kann α auch dargestellt werden:

$$\alpha = b_0 + b_1\zeta + \cdots + b_{\ell-2}\zeta^{\ell-2}; \quad (b_i \text{ ganz})$$

d.h. auch $1, \zeta, \dots, \zeta^{\ell-2}$ bilden eine Basis. Erhebt man in die p–te Potenz, so wird nach dem Fermatschen Satz:

$$\begin{aligned}
\alpha^p &\equiv b_0 + b_1\zeta^p + \cdots + b_{\ell-2}\zeta^{(\ell-2)p} \mod p \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
\alpha^{p^f} &\equiv b_0 + b_1\zeta^{p^f} + \cdots + b_{\ell-2}\zeta^{(\ell-2)p^f} \mod p \\
&\equiv \alpha \mod p, \quad \text{da} \quad p^f \equiv 1 \bmod \ell \ [1]
\end{aligned}$$

229 I

Es gilt also für jedes ganze α:

$$\alpha^{p^f} \equiv \alpha \mod p$$

also erst recht: $\alpha^{p^f} \equiv \alpha \bmod \mathfrak{p}$, wenn $\mathfrak{p}$ ein Primteiler von p. Ist nun f' der Grad von $\mathfrak{p}$, so gilt für jede Körperzahl nach dem Fermat'schen Satz:

$$\alpha^{p^{f'}} \equiv \alpha \mod \mathfrak{p}$$

Wäre $f' > f$, so hätte die Kongruenz $x^{p^f} \equiv x \bmod \mathfrak{p}$ vom Grade $p^f \bmod \mathfrak{p}$ mehr als p^f Wurzeln, was unmöglich. Es ist also $f' \leqq f$. Andererseits gilt nach dem Fermatschen Satz, da ζ Einheit, also zu $\mathfrak{p}$ prim ist,

$$\zeta^{p^{f'}-1} \equiv 1 \mod \mathfrak{p}$$

Wäre nun $p^{f'} - 1$ prim zu ℓ, so wäre $(\zeta^{p^{f'}-1} - 1) = \mathfrak{l}$, also nicht durch $\mathfrak{p}$ teilbar. Also ist $p^{f'} - 1 \equiv 0 \bmod \ell$, d.h. nach Definition von f: $f' \geqq f$. Es ist also $f' = f$. Jedes in p aufgehende Primideal $\mathfrak{p}$ hat den Grad f, und da p kein Teiler der Körperdiskriminante, ist:

$$p = \mathfrak{p}_1 \dots \mathfrak{p}_\ell\,; \quad (\mathfrak{p}_i \text{ vom Grad } f,\ ef = \ell - 1)$$

und $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ verschieden.

Um diese Primideale $\mathfrak{p}_i$ wirklich darzustellen, beachten wir, daß $F(x)$ die Körperdiskriminante zur Diskriminante hat. Es muß daher folgende Zerlegung in Primfunktionen mod p gelten:

$$F(x) \equiv P_1(x) \dots P_e(x) \bmod p$$

Dann ist einfach:

$$\mathfrak{p}_1 = \big(p, P_1(\zeta)\big); \quad \dots; \quad \mathfrak{p}_e = \big(p, P_e(\zeta)\big).$$

Zusammenfassend haben wir folgenden Satz:

230 I

Satz 1. Der Kreiskörper $R(\zeta)$ der primitiven ℓ–ten Einheitswurzel $\zeta = e^{\frac{2\pi i}{\ell}}$,

wo ℓ eine ungerade Primzahl ist, ist ein zyklischer Körper $(\ell-1)$ ten Grades. Seine Diskriminante ist $(-1)^{\frac{\ell-1}{2}}\ell^{\ell-2}$. Die Zahlen $1, \zeta, \ldots, \zeta^{\ell-1}$ bilden eine Basis. Die Zahlen

$$\frac{1-\zeta^a}{1-\zeta^b}; \quad (a, b \text{ prim zu } \ell)$$

sind Einheiten.

Die Primzahl ℓ wird die $(\ell-1)$ te Potenz des Primideals $\mathfrak{l} = (1-\zeta) : \ell = \mathfrak{l}^{\ell-1}$.

Jede von ℓ verschiedene Primzahl p zerfällt so:
Ist f der kleinste positive Exponent, für den $p^f \equiv 1 \bmod \ell$ wird, und $\ell - 1 = ef$, so zerfällt p in das Produkt von e verschiedenen Primidealen f–ten Grades:

$$p = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_e.$$

Da $n(\mathfrak{p}_i) = p^f$, gilt für jedes von $\mathfrak{l}$ verschiedene Primideal $\mathfrak{p}$:

$$n(\mathfrak{p}) \equiv 1 \mod \ell$$

Es zerfällt $F(x) = 1 + x + \cdots + x^{\ell-1} \bmod p$ in e Primfunktionen f–ten Grades (verschiedene):

$$F(x) \equiv P_1(x) \ldots P_e(x) \mod p$$

Dann ist der Primteiler $\mathfrak{p}_i$ von p dargestellt durch:

$$\mathfrak{p}_i = \big(p, P_i(\zeta)\big).$$

Damit sind alle für uns in Frage kommenden Eigenschaften des Kreiskörpers $R(\zeta)$ hergeleitet.

231 I

b) Abelsche Gruppen

Sei zunächst $\mathfrak{G}$ eine endliche Abelsche Gruppe vom Grade N, $\mathsf{A}_1, \ldots, \mathsf{A}_m$ eine Basis, deren Elemente bekanntlich so gewählt werden dürfen, daß sie zu Primzahlpotenzexponenten gehören. Sei also $p_\nu^{r_\nu}$ der „*Grad*“ von A_ν, ferner ζ_ν eine Einheitswurzel des Grades $p_\nu^{r_\nu}$. Ist dann

$$\mathsf{B} = \mathsf{A}_1^{x_1} \ldots \mathsf{A}_m^{x_m}$$

ein Element von $\mathfrak{G}$, so ordnen wir B einen „*Charakter*“ χ_{B} so zu:

Für jedes Element $\mathsf{A} = \mathsf{A}_1^{y_1} \dots \mathsf{A}_m^{y_m}$ sei

$$\chi_{\mathsf{B}}(\mathsf{A}) = \zeta_1^{x_1 y_1} \dots \zeta_m^{x_m y_m}$$

Auf diese Weise erhält man N Charaktere $\chi_{\mathsf{B}_1}, \dots, \chi_{\mathsf{B}_n}$, deren jeder für jedes Element A gebildet werden, also N Werte annehmen kann. Es ist übrigens

$$N = p_1^{r_1} \dots p_m^{r_m}$$

wobei aber die p_ν nicht notwendig verschieden sind. Es gilt offenbar:

$$\chi_{\mathsf{B}}(\mathsf{A}) = \chi_{\mathsf{A}}(\mathsf{B}) \quad \text{und} \quad \begin{cases} \chi_{\mathsf{B}}\chi_{\mathsf{B}'} = \chi_{\mathsf{B}\mathsf{B}'} \\ \chi(\mathsf{A})\chi(\mathsf{A}') = \chi(\mathsf{A}\mathsf{A}') \end{cases}$$

Es sei nun g eine Untergruppe vom Grade n und Index $j = \frac{N}{n}$. Wir betrachten die Faktorgruppe:

$$g, a_1 g, \dots, a_{j-1} g$$

Sie besitzt j Charaktere. Ordnet man jedem dieser Charaktere einen Charakter von $\mathfrak{G}$ zu, derart, daß sein Wert für ein Element A gleich dem Wert des Charakters von $\frac{\mathfrak{G}}{g}$[2] für die Nebengruppe $\mathsf{A}g$ ist, so erhält man genau j Charaktere, die für die Elemente von g den Wert 1 haben. □□□

232 I

(daß diese Zuordnung möglich erkennt man so: □□□
Definieren wir eine Funktion $\chi(\mathsf{A})$ durch die gegebene Erklärung, so gilt

a.) $\chi(1) = 1$

b.) $\chi(\mathsf{A})\chi(\mathsf{B}) = \chi(\mathsf{A}\mathsf{B})$

Da beides wegen der „Charaktereigenschaft“ von χ für $\frac{\mathfrak{G}}{g}$ gilt. Ferner

c.) $\sum_{\mathsf{A}|g} \chi(\mathsf{A}) = \begin{cases} 0 & \text{wenn} \quad \chi \text{ nicht identisch 1} \\ N & \text{wenn} \quad \chi \text{ identisch 1} \end{cases}$

[2] $\mathfrak{G}$, $\mathfrak{g}$ und g sind stellenweise optisch schwach differenziert.

Denn

$$\begin{aligned}\sum_{\mathsf{A}|g}\chi(\mathsf{A}) &= \sum_{\mathsf{A}|g}\chi(\mathsf{A}) + \sum_{\mathsf{A}|ga_1}\chi(\mathsf{A}) + \cdots + \sum_{\mathsf{A}|ga_{j-1}}\chi(\mathsf{A}) \\ &= \frac{N}{j}\{\chi(g) + \chi(a_1 g) + \cdots + \chi(a_{j-1}g)\} \\ &= \frac{N}{j}\sum_{a_i g}\chi(a_i g)\end{aligned}$$

und die letztere Summe ist $\frac{N}{j}\cdot 0$ oder $\frac{N}{j}j = N$, je nachdem χ nicht identisch 1 oder identisch 1 ist.

Da aber jede a.) b.) c.) genügende, für alle A aus g erklärte Funktion $\chi(\mathsf{A})$ nach dem bekannten Fundamentalsatz über Gruppencharaktere ein Charakter für g ist, folgt die Möglichkeit der getroffenen Zuordnung.)

Ist umgekehrt χ ein Charakter von $\mathfrak{G}$, der für jedes Element aus g den Wert 1 hat, so hat er für je eine ganze Nebengruppe denselben Wert, sodaß ihm ein Charakter von $\frac{\mathfrak{G}}{g}$ entspricht. (Begründung analog der obigen).

Es gibt also genau j Charaktere, sodaß $\chi(g) = 1$. Diese bilden eine mit der Faktorgruppe $\frac{\mathfrak{G}}{g}$ isomorphe Gruppe.

233 I

Es seien dies etwa:

$$\chi_1, \chi_{\mathsf{B}_1}, \ldots, \chi_{\mathsf{B}_{j-1}}.$$

Da $\chi_{\mathsf{B}_i}\chi_{\mathsf{B}_k} = \chi_{\mathsf{B}_i\mathsf{B}_k}$ ist, bilden die Elemente $1, \mathsf{B}_1, \ldots, \mathsf{B}_{j-1}$ ebenfalls eine mit $\frac{\mathfrak{G}}{g}$ isomorphe Gruppe, die die *zu g reziproke Gruppe* $\overline{g}$ genannt wird.

Es ist

$$\begin{array}{lrcl} \text{Es ist} & \chi_{\mathsf{B}_i}(C_k) & = & 1, \quad \text{wenn} \quad C_k \quad \text{in} \quad g, \quad \mathsf{B}_i \quad \text{in} \quad \overline{g} \\ \text{also auch} & \chi_{C_k}(\mathsf{B}_i) & = & 1, \quad \text{"} \quad \text{"} \quad \text{"} \quad \text{"}, \quad \text{"} \quad \text{"} \quad \text{"} \end{array}$$

Die Charaktere $\chi_1, \chi_{C_1}, \ldots, \chi_{C_{n-1}}$ spielen also für die Untergruppe $\overline{g}$ dieselbe Rolle, wie $\chi_1, \ldots, \chi_{\mathsf{B}_{j-1}}$ für g, d.h. es ist die zu $\overline{g}$ reziproke Gruppe wieder g. Die *Reziprozität der Gruppen* ist also gegenseitig und somit eineindeutig.

Jeder Untergruppe vom Grade n ist also genau eine Untergruppe vom Grade j reziprok und umgekehrt. Also gilt:

Satz 2. Ist $\mathfrak{G}$ eine Abelsche Gruppe vom Grade N, und $n = \frac{N}{j}$ ein Teiler von N, so ist die Anzahl der Untergruppen vom Grade n gleich der Anzahl

der Untergruppen vom Grade j.

Unsern weiteren Überlegungen sei nun zunächst eine beliebige Abelsche Gruppe $\mathfrak{G}$ (endlich oder unendlich) zugrundegelegt.

Es sei ℓ eine Primzahl. Wieder fassen wir, wie bei den Einheitenverbänden, die Elemente ax^ℓ in einen *Verband* zusammen, wo a ein festes Element aus $\mathfrak{G}$, x aber alle durchläuft. Zwei Verbände sind dann entweder identisch, oder enthalten kein gemeinsames Element.

Die Verbände bilden wieder eine Abelsche Gruppe, in der jedes Element den Exponenten ℓ hat. Uns interessiert nur der Fall, daß die Anzahl der verschiedenen Verbände endlich ist. Wie leicht zu sehen, tritt dieser Fall sicher dann ein, wenn unsere Gruppe $\mathfrak{G}$ eine endliche Basis $\mathsf{A}_1, \ldots, \mathsf{A}_m$ besitzt, sodaß jedes Element in der Form $\mathsf{A}_1^{x_1} \ldots \mathsf{A}_m^{x_m}$ darstellbar ist, wo die x ganze rationale Zahlen durchlaufen. Dann ist der Grad der Gruppe der Verbände eine Potenz ℓ^t von ℓ, und sie hat genau t Basiselemente, sodaß jeder Verband V sich so darstellen läßt:

$$V = V_1^{a_1} \ldots V_t^{a_t}; \quad (a_i = 0, 1, \ldots, \ell - 1),$$

und zwar eindeutig. Für die Elemente von $\mathfrak{G}$ bedeutet dies, daß es t Elemente $v_1, \ldots, v_t$ in $\mathfrak{G}$ gibt, sodaß jedes A aus $\mathfrak{G}$ sich eindeutig in der Form darstellen läßt:

$$\mathsf{A} = v_1^{x_1} \ldots v_t^{x_t} \xi^\ell; \quad (x_i = 0, 1, \ldots, \ell - 1; \quad \xi \text{ in } \mathfrak{G})$$

Die Zahl t heiße der *Rang unserer Gruppe* $\mathfrak{G}$.

Mithilfe des Ranges kann die Anzahl der Untergruppen vom □□□ Index ℓ ermittelt werden.

In einer solchen Untergruppe g ist nämlich die ℓ–te Potenz eines jeden Elementes aus $\mathfrak{G}$ enthalten, da die Faktorgruppe die zyklische Gruppe vom Grade ℓ ist. Daher ist der ganze „*Hauptverband*“ x^ℓ in g enthalten, ein anderer Verband also entweder ganz oder gar nicht (d.h. keines seiner Elemente). g kann also auch als Untergruppe der Verbände–Gruppe vom selben Index ℓ aufgefaßt werden. □□□ die Anzahl solcher Untergruppen vom Index ℓ ist nach Satz 2 gleich der Anzahl der Untergruppen vom Grad ℓ. Diese Anzahl läßt sich aber für die Verbändegruppe leicht angeben, da ihr Typus $(\ell, \ell, \ldots, \ell)$ (t mal) ist.

235 I

Jedes von 1 verschiedene Element (Verband) gibt nämlich zu einer zyklischen Untergruppe vom Grade ℓ Anlaß, und gerade die $\ell - 1$ Potenzen eines Elementes und keine anderen Elemente erzeugen den gleichen Cyklus. Wir haben also $\frac{\ell^t-1}{\ell-1}$ solcher Gruppen.

Satz 3. Hat die Abel'sche Gruppe $\mathfrak{G}$ den endlichen Rang t nach der Primzahl ℓ, so gibt es genau $\frac{\ell^t-1}{\ell-1}$ Untergruppen von $\mathfrak{G}$ vom Index ℓ.

Nunmehr kehren wir zu dem Ausdruck

$$\mathsf{A} = v_1^{x_1} \dots v_t^{x_t} \xi^\ell$$

für die Elemente von $\mathfrak{G}$ zurück. Es seien die Elemente A durch irgendeine Bedingung eingeschränkt, welche bei Multiplikation erhalten bleibt und der alle ℓ–ten Potenzen von Elementen genügen. Dadurch ist eine Untergruppe g definiert, die wieder den Hauptverband enthält, und jeden anderen Verband somit ganz oder gar nicht, sodaß g als Untergruppe der Verbändegruppe betrachtet werden kann, und als solche eine Potenz ℓ^n zum Grad und eine Basisdarstellung: $\overline{V}_1^{x_1} \dots \overline{V}_n^{x_n}$; $(x_i = 0, 1, \dots, \ell - 1)$ hat. Ist V ein nicht in g enthaltener Verband, so ist erst V^ℓ in g enthalten, dann aber $V^\ell = 1$. (Denn wäre V^i für $1 < i < \ell$ in g enthalten, und $ik \equiv 1 \bmod \ell$, so ist auch $V^{ix} = V$ in g enthalten). Demnach ist $\overline{V}_1^{x_1} \dots V_n^{\overline{x}_n} V^x$ eine Untergruppe vom Grade ℓ^{n+1} in ihrer Basisdarstellung. So weiterschließend erhält man, wenn man diese Überlegungen für die Elemente von $\mathfrak{G}$ selbst ausspricht:

236 I

Satz 4. Die Abelsche Gruppe $\mathfrak{G}$ habe den Rang t nach der Primzahl ℓ. Durch irgendeine Bedingung, der alle ℓ–ten Potenzen genügen, sei eine Untergruppe g von $\mathfrak{G}$ definiert, die dann einen endlichen Rang $n \leqq t$ besitzt. Die Elemente von g gestatten dann die eindeutige Darstellung:

$$a = \overline{v}_1^{\overline{x}_1} \dots v_n^{\overline{x}_n} \xi^\ell; \qquad 0 \leqq \overline{x}_i \leqq \ell - 1$$

Dann lassen sich in $\mathfrak{G}$ noch weitere $t - n$ Elemente $v_1, \dots, v_{t-n}$ finden, sodaß jedes Element von $\mathfrak{G}$ darstellbar ist in der Form:

$$\mathsf{A} = v_1^{x_1} \dots v_{t-n}^{x_{t-n}} \overline{v}_1^{\overline{x}_1} \dots \overline{v}_n^{\overline{x}_n} \xi^\ell; \qquad 0 \leqq x_i, \overline{x}_i \leqq \ell - 1$$

A gehört dann und nur dann zu g, wenn $x_1, x_2, \dots, x_{t-n} = 0$ ist.

c) Die prime Restklassengruppe

c.) Die Gruppe der primen Restklassen.

Es sei $\mathfrak{m}$ ein Ideal aus k. Wir wollen dann den Rang $R(\mathfrak{m})$ der Gruppe der zu $\mathfrak{m}$ primen Restklassen bestimmen. Da die Gruppe endlich ist, ist ihr Rang endlich. Es sei $\mu = R(\mathfrak{m})$. Dann muß es also μ zu $\mathfrak{m}$ prime Zahlen $\gamma_1, \ldots, \gamma_\mu$ geben, sodaß jede zu $\mathfrak{m}$ prime Zahl α einer eindeutig bestimmten Kongruenz

$$\alpha \equiv \gamma_1^{x_1} \ldots \gamma_\mu^{x_\mu} \xi^\ell \mod \mathfrak{m}; \qquad 0 \leqq x_i \leqq \ell - 1.$$

genügt. α ist dann und nur dann ℓ–ter Potenzrest nach $\mathfrak{m}$, wenn $x_1, \ldots, x_\mu = 0$ ist. Insbesondere sind also $\gamma_1, \ldots, \gamma_\mu$ selbst Nichtreste nach $\mathfrak{m}$. Wir nennen sie ein *System unabhängiger Nichtreste.*

237 I

Bei festgewählten x_i erhält man alle dazu gehörigen, inkongruenten α, wenn man alle primen inkongruenten Werte ξ^ℓ einsetzt. Nennt man deren Anzahl ν, und ist $\phi(\mathfrak{m})$ die Euler'sche Funktion in k, so ist also

$$\ell^\mu = \frac{\phi(\mathfrak{m})}{\nu}.$$

Läßt man nun in ξ^ℓ die Zahl ξ ein primes Restsystem mod $\mathfrak{m}$ durchlaufen, so erscheint eine feste Restklasse genau so oft, als es inkongruente Lösungen von $\xi^\ell \equiv 1 \mod \mathfrak{m}$ gibt (notwendig prim!). Ist deren Anzahl ν_1, so ist also $\nu = \frac{\phi(\mathfrak{m})}{\nu_1}$, also $\nu_1 = \ell^\mu$. Für den gesuchten Rang $\mu = R(\mathfrak{m})$ finden wir also, daß ℓ^μ die Anzahl der inkongruenten Lösungen von $\xi^\ell \equiv 1 \mod \mathfrak{m}$ ist; diese Anzahl soll jetzt ermittelt werden.

Ist $\mathfrak{m} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_v^{\nu_v}$, so gehört zu jeder Lösung mod $\mathfrak{m}$ genau eine Lösung nach jeder Primidealpotenz $\mathfrak{p}_i^{\nu_i}$ und umgekehrt. Die Lösungszahl nach $\mathfrak{m}$ ergibt sich also als Produkt der Lösungszahlen den den $\mathfrak{p}_i^{\nu_i}$. Für den Exponenten von ℓ geht dies in die Summe über. Also:

Satz 5. Ist $\mathfrak{m} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_v^{\nu_v}$, so ist

$$R(\mathfrak{m}) = R(\mathfrak{p}_1^{\nu_1}) + \cdots + R(\mathfrak{p}_v^{\nu_v}).$$

Es ist also nur noch $R(\mathfrak{p}^\nu)$ für ein Primideal $\mathfrak{p}$ zu ermitteln. Zunächst sei $\mathfrak{p}$ prim zu ℓ. Ist α eine zu $\mathfrak{p}$ prime Zahl und ϱ eine primitive Wurzel mod $\mathfrak{p}$, so setzen wir:

$$\alpha \equiv \alpha_0 \varrho^x \mod \mathfrak{p}^\nu, \quad \text{sodaß } \alpha_0 \equiv 1 \mod \mathfrak{p}.$$

Nach Satz 5, S. 158 ist also α_0 ℓ–ter Potenzrest nach $\mathfrak{p}^\nu$.

238 I

$$\alpha_0 \equiv \lambda^\ell \bmod \mathfrak{p}^\nu$$

α ist also ℓ–ter Potenzrest oder nicht, je nachdem ϱ^x ℓ–ter Potenzrest nach $\mathfrak{p}^\nu$, d.h. nach $\mathfrak{p}$ ist oder nicht.

1.) $n(\mathfrak{p})-1 = \phi(\mathfrak{p})$ ist prim zu ℓ. Dann ist die Kongruenz $\ell y \equiv x \bmod \phi(\mathfrak{p})$ lösbar, d.h. ϱ^x stets ℓ–ter Potenzrest nach $\mathfrak{p}$ und $\mathfrak{p}^\nu$. ξ^ℓ durchläuft also *alle* Restklassen, somit jede nur einmal. Die fragliche Lösungszahl ist also 1, d.h. $R(\mathfrak{p}^\nu) = 0$.

2.) $n(\mathfrak{p})-1 = \phi(\mathfrak{p})$ ist teilbar durch ℓ: $\phi(\mathfrak{p}) = i\ell$. Wenn $\varrho^x \equiv \varrho^{y\ell} \bmod \mathfrak{p}$ sein soll, muß $y\ell \equiv x \bmod i\ell$ d.h. x durch ℓ teilbar sein, was umgekehrt hinreicht. Für x kommen also nur[3] die i Werte $0, \ell, 2\ell, \ldots, (i-1)\ell$ in Frage, wenn ϱ^x ℓ–ter Potenzrest sein soll. Es ist also genau der ℓ–te Teil aller Restklassen ℓ–ter Potenzrest nach $\mathfrak{p}^\nu$. ξ^ℓ stellt also jede Restklasse genau ℓ–mal dar, die gesuchte Lösungszahl ist ℓ, d.h. $R(\mathfrak{p}^\nu) = 1$.

Satz 6. Ist $\mathfrak{p}$ prim zu ℓ, so gilt

$$\begin{array}{rcccl} R(\mathfrak{p}^\nu) & = & 1 & \text{wenn} & \phi(\mathfrak{p}) \equiv 0 \mod \ell \\ R(\mathfrak{p}^\nu) & = & 0 & \text{"} & \phi(\mathfrak{p}) \not\equiv 0 \mod \ell \end{array}$$

Es bleiben noch die in ℓ aufgehenden Primideale zu untersuchen. Über sie gilt, wenn $[x]$ = größte ganze Zahl $\leqq x$,

Satz 7. Geht $\mathfrak{l}$ in ℓ genau zur s–ten Potenz auf und hat den Grad f, so ist:

$$R(\mathfrak{l}^g) = \left[g - \frac{g}{\ell}\right] f, \quad \text{wenn} \quad \frac{s\ell}{\ell - 1} \geqq g > 0$$

Wenn aber $g > \frac{s\ell}{\ell-1}$ ist, gilt folgendes:

239 I

[3] undeutlich

1.) $R(\mathfrak{l}^g) = sf$,
wenn $s \not\equiv 0 \bmod \ell - 1$
oder $s \equiv 0 \bmod \ell - 1$, jedoch $\xi^{\ell-1} \equiv -\ell \bmod \mathfrak{l}^{s+1}$ unlösbar.

2.) $R(\mathfrak{l}^g) = sf + 1$,
wenn $s \equiv 0 \bmod \ell - 1$
und $\xi^{\ell-1} \equiv -\ell \bmod \mathfrak{l}^{s+1}$ lösbar.

Enthält k die ℓ–te Einheitswurzel ζ, so tritt der
Fall 2.) immer ein, es ist also dann stets

$$R(\mathfrak{l}^g) = sf + 1.$$

Beweis. Es bedeute λ_n eine genau durch $\mathfrak{l}^n$ teilbare Zahl ($n \geqq 0$). In der Entwicklung von $(1+\lambda_n)^\ell$ nach dem binomischen Satz sind die Glieder $\binom{\ell}{\nu}\lambda_n^\nu$ für $\nu \geqq 2$, $\nu \leqq \ell - 1$ sicher □□□ durch eine höhere Potenz wie $\binom{\ell}{1}\lambda_n$ oder für $n = 0$, wie λ_n^ℓ teilbar. Bis auf Glieder, die durch höhere Potenzen von $\mathfrak{l}$ teilbar sind ist also $(1 + \lambda_n)^\ell$ gleich $1 + \ell\lambda_n + \lambda_n^\ell$. Das erste Glied ist durch $\mathfrak{l}^{s+n}$, das zweite durch $\mathfrak{l}^{n\ell}$ teilbar. Es ist $s + n < n\ell$ für $n > \frac{s}{\ell-1}$, $s + n > n\ell$ für $n < \frac{s}{\ell-1}$. Demnach finden wir

(1) für $n < \frac{s}{\ell-1}$: $(1 + \lambda_n)^\ell = 1 + \lambda_{n\ell}$

(2) ‖ $n > \frac{s}{\ell-1}$: $(1 + \lambda_n)^\ell = 1 + \lambda_{s+n}$

Ist endlich $s \equiv 0 \bmod (\ell - 1)$: $s = (\ell - 1)s_0$, so wird:

(3) für $n = \frac{s}{\ell-1} = s_0$: $(1 + \lambda_{s_0})^\ell \equiv 1 + \ell\lambda_{s_0} + \lambda_{s_0}^\ell \bmod \mathfrak{l}^{s_0\ell+1}$

1.) Ist also $\frac{s\ell}{\ell-1} \geqq g > 0$, so ist für $n > \frac{s}{\ell-1}$ sicher $n\ell > g$ und $s + n > \frac{s\ell}{\ell-1} \geqq g$, also $(1 + \lambda_n)^\ell \equiv 1 \bmod \mathfrak{l}^g$, für $n = \frac{s}{\ell-1} = s_0$, sicher $n\ell \geqq g$ und $n + s \geqq g$ also $(1 + \lambda_{s_0})^\ell \equiv 1 \bmod \mathfrak{l}^g$, für $n < \frac{s}{\ell-1}$ aber $(1 + \lambda_n)^\ell$ dann und nur dann $\equiv 1 \bmod \mathfrak{l}^g$, wenn $n\ell \geqq g$. Es ist also allgemein:

$$(1 + \lambda_n)^\ell \equiv 1 \mod \mathfrak{l}^g$$

dann und nur dann, wenn $n\ell \geqq g$ ist, d.h. $n \geqq \frac{g}{\ell}$ oder $n \geqq g_0$, wo g_0 die kleinste $\frac{g}{\ell}$ übertreffende Zahl ist. Die Lösungen der Kongruenz □□□ $\xi^\ell \equiv 1$

mod $\mathfrak{l}^g$ sind also durch die Zahlen $\xi \equiv 1 \mod \mathfrak{l}^{g_0}$ gegeben. Jede Restklasse nach $\mathfrak{l}^{g_0}$ zerfällt aber in $\frac{n(\mathfrak{l}^g)}{n(\mathfrak{l}^{g_0})} = \ell^{(g-g_0)f}$ Restklassen nach $\mathfrak{l}^g$, so daß diese Zahl unsere Lösungszahl ist, somit $R(\mathfrak{l}^g) = (g-g_0)f = \left[g - \frac{g}{\ell}\right] f$, w.z.b.w.

2.) a.) Nun sei $g > \frac{s\ell}{\ell-1}$, aber $s \not\equiv 0 \mod (\ell-1)$. Für $n < \frac{s}{\ell-1}$ ist dann $n\ell < g$, $1+\lambda_n$ also keine Lösung von $\xi^\ell \equiv 1 \mod \mathfrak{l}^g$. Für $n > \frac{s}{\ell-1}$ ist aber $1+\lambda_n$ wegen (2) dann und nur dann Lösung, wenn $n+s \geqq g$ oder $n \geqq g-s$ ist. Unsere Kongruenz wird also durch alle u. nur [...] die Zahlen $\xi \equiv 1 \mod \mathfrak{l}^{g-s}$ welche offenbar ℓ^{sf} Restklassen mod $\mathfrak{l}^g$ darstellen. Also ist $R(\mathfrak{l}^g) = sf$.

b.) Ist aber s teilbar durch $\ell-1$ so kommt noch (3) in Frage. Ist nun die Kongruenz $\xi^{\ell-1} \equiv -\ell \mod \mathfrak{l}^{s+1}$ unlösbar, so kann nicht $\lambda_{s_0}^\ell + \ell\lambda_{s_0} \equiv 0 \mod \mathfrak{l}^{s_0\ell+1}$ statthaben, da dies

$\lambda_{s_0}^{\ell-1} + \ell \equiv 0 \mod \mathfrak{l}^{s+1}$ zur Folge hätte (□□□).

Also ist in diesem Falle $(1+\lambda_{s_0})^\ell = 1+\lambda_{s+s_0}$. Wegen $s+s_0 = \frac{s\ell}{[\ldots]-1} < g$ kann also $1+\lambda_{s_0}$ nicht Lösung sein, sodaß wie vorher $R(\mathfrak{l}^g) = sf$ ist.

c.) Endlich werde noch die Lösbarkeit von

$$\xi^{\ell-1} \equiv -\ell \mod \mathfrak{l}^{s+1}$$

angenommen. Da ℓ genau durch $\mathfrak{l}^s$ teilbar, muß auch $\xi^{\ell-1}$ genau durch $\mathfrak{l}^s$ teilbar sein, also s durch $\ell-1$: $s = (\ell-1)s_0$. ξ muß dann ein λ_{s_0} sein. Sei $\lambda_{s_0}^{(1)}$ eine Lösung dieser Kongruenz. Dann ist

$$\lambda_{s_0}^{(1)^\ell} + \ell\lambda_{s_0}^{(1)} \equiv 0 \mod \mathfrak{l}^{s_0\ell+1},$$

und demnach $(1+\lambda_{s_0}^{(1)})^\ell \equiv 1 \mod \mathfrak{l}^{s_0\ell+1}$.

Angenommen es sei:

$$(1+\lambda_{s_0}^{(i)})^\ell \equiv 1 \mod \mathfrak{l}^{s_0\ell+i}$$

Dann setzen wir: $(1+\lambda_{s_0}^{(i)})^\ell \equiv 1 + \eta_0\lambda_{s_0\ell+i} \mod \mathfrak{l}^{s_0\ell+i+1}$
Ferner ist: $(1+\eta\lambda_{s_0+i})^\ell \equiv 1 + \eta\ell\lambda_{s_0+i} \mod \mathfrak{l}^{s_0\ell+i+1}$,
also, wenn $(1+\lambda_{s_0}^{(i)})(1+\eta\lambda_{s_0+i}) = 1+\lambda_{s_0}^{(i+1)}$ gesetzt wird,

$$(1+\lambda_{s_0}^{(i+1)})^\ell \equiv 1 + (\eta_0\lambda_{s_0\ell+i} + \eta\ell\lambda_{s_0+i}) \mod \mathfrak{l}^{s_0\ell+i+1},$$

Wählt man η so, daß

$$\eta\ell\lambda_{s_0+i} + \eta_0\lambda_{s_0\ell+i} \equiv 0 \mod \mathfrak{l}^{s_0\ell+i+1},$$

was stets möglich, so ist:

$$(1+\lambda_{s_0}^{(i+1)})^\ell \equiv 1 \bmod \mathfrak{l}^{s_0\ell+i+1}$$

Durch Induktion finden wir also stets (für $g > \frac{s\ell}{\ell-1} = sgl$ [4]) ein λ_{s_0}, etwa $\lambda_{s_0}^{(0)}$, sodaß:

$$(1+\lambda_{s_0}^{(0)})^\ell \equiv 1 \bmod \mathfrak{l}^g.$$

Jedenfalls ist dann $\ell\lambda_{s_0}^{(0)} + {\lambda_{s_0}^{(0)}}^\ell \equiv 0 \bmod \mathfrak{l}^g$, also mal $\mathfrak{l}^{s_0\ell+1}$ und demnach

$$\ell + {\lambda_{s_0}^{(0)}}^{\ell-1} \equiv 0 \bmod \mathfrak{l}^{s+1},$$

also $\lambda_{s_0}^{(0)}$ [5] Lösung unser Hilfskongruenz.

242 ı

Wir setzen $\beta_0 = 1+\lambda_{s_0}^{(0)}$. Jede Zahl $\beta = 1+\lambda_{s_0}$ kann nun in die Form

$$\beta \equiv 1 + \gamma\lambda_{s_0}^{(0)} \mod \mathfrak{l}^g$$

gesetzt werden. Soll $\beta^\ell \equiv 1 \bmod \mathfrak{l}^g$ sein, so muß, wie wir eben sahen, $\gamma\lambda_{s_0}^{(0)}$ Lösung von $\xi^{\ell-1} + \ell \equiv 0 \bmod \mathfrak{l}^{s+1}$ sein. Da $\lambda_{s_0}^{(0)}$ Lösung ist, folgt

$${\lambda_{s_0}^{(0)}}^{\ell-1}(\gamma^{\ell-1}-1) \equiv 0 \bmod \mathfrak{l}^{s+1}$$

oder

$$\gamma^{\ell-1} \equiv 1 \mod \mathfrak{l}$$

was nach dem Fermatschen Satz nur für $\gamma \equiv c \bmod \mathfrak{l}$ stimmt, wo c rational, zu ℓ prim. Wegen $g > \frac{s\ell}{\ell-1} = s_0\ell \geqq s_0+1$ ist jedenfalls

$$\beta \equiv 1+\gamma\lambda_{s_0}^{(0)} \equiv 1 + c\lambda_{s_0}^{(0)} \mod \mathfrak{l}^{s_0+1}$$

Da nun $\beta_0^c \equiv 1 + c\lambda_{s_0} \bmod \mathfrak{l}^{s_0+1}$ ist, muß

$$\beta \equiv \beta_0^c \bmod \mathfrak{l}^{s_0+1}$$

[4] undeutlich
[5] undeutlich

sein. Setzen wir also:

$$\beta \equiv \beta_0^c(1+\lambda_n) \bmod \mathfrak{l}^g,$$

so muß λ_n □□□ durch die gleiche Potenz wie $\beta - \beta_0^c$ □□□ oder durch $\mathfrak{l}^g$ teilbar sein, also auf jeden Fall $n \geqq s_0 + 1$. Soll nun überdies $\beta^\ell \equiv 1 \bmod \mathfrak{l}^s$ sein, so muß wegen $\beta_0^\ell \equiv 1 \bmod \mathfrak{l}^g$ auch $(1+\lambda_n)^\ell \equiv 1 \bmod \mathfrak{l}^g$ sein, und dies ist auch hinreichend (Nach (2) u. 2.a.) ist die Lösungszahl ℓ^{sf})

Sollen ferner zwei solche β kongruent mod $\mathfrak{l}^g$ sein, so müssen sie nach $\mathfrak{l}^{s_0+1}$ kongruent sein, also die Potenzen $\beta_0^{c_1} \equiv \beta_0^{c_2} \bmod \mathfrak{l}^{s_0+1}$ oder $c_1 \equiv c_2 \bmod \ell$. Da $c < \ell$ vorausgesetzt werden kann, folgt $c_1 = c_2$. Also müssen die zweiten Faktoren mod $\mathfrak{l}^g$ kongruent sein. Diese zweiten Faktoren haben aber nach den vorigen Ausführungen genau ℓ^{sf} mod $\mathfrak{l}^g$ inkongruente Möglichkeiten. Mit $1, \beta_0, \beta_0^2, \ldots, \beta_0^{\ell-1}$ kombiniert ergeben sie also ℓ^{sf+1} inkongruente Lösungen. (Die 1 entspricht dabei gerade den Fällen in 2. a.) b.).) Also $R(\mathfrak{l}^g) = \ell^{sf+1}$.

Ist schließlich ζ in k enthalten, so ist $\ell = \big((1-\zeta)^{\ell-1}\big)$. Jedes in ℓ aufgehende Primideal geht also in $(1-\zeta)$, etwa zur Potenz s_0 auf, in ℓ also zur Potenz $s_0(\ell-1)$. Nun ist

$$\frac{\ell}{(1-\zeta)^{\ell-1}} = \frac{(1-\zeta)\cdots(1-\zeta^{\ell-1})}{(1-\zeta)^{\ell-1}} = (1+\zeta)(1+\zeta+\zeta^2)\cdots(1+\zeta+\cdots+\zeta^{\ell-2}).$$

Da nun $1+\zeta+\cdots+\zeta^{i-1} \equiv i \bmod (1-\zeta)$ ist, wird

$$\frac{\ell}{(1-\zeta)^{\ell-1}} \equiv (\ell-1)! \bmod (1-\zeta)$$

Nach dem Wilsonschen Satz also: $\frac{\ell}{(1-\zeta)^{\ell-1}} \equiv -1 \bmod (1-\zeta)$, also:

$$\ell + (1-\zeta)^{\ell-1} \equiv 0 \mod (1-\zeta)^\ell$$

also: $\ell + (1-\zeta)^{\ell-1} \equiv 0 \bmod \mathfrak{l}^{s_0\ell}$ umsomehr noch mod $\mathfrak{l}^{s+1}$.

Unsere fragliche Kongruenz ist also hier stets lösbar, wenn ℓ ungerade. Für $\ell = 2$ folgt sofort $2 + 2^{2-1} \equiv 0 \bmod 2^2$ als Lösung.

Damit ist unser Satz in allen Teilen bewiesen.

Anm. Die Betrachtungen dieses Abschnittes lassen sich mit [...]ls multiplikativer Normalform erheblich vereinfachen.

d) Die Idealklassengruppe

d.) Die Gruppe der Idealklassen.

Es sei $\mathfrak{m}$ ein Ideal aus k. Die Idealklassen seien nach dem Strahl der Zahlen $\equiv 1 \bmod \mathfrak{m}$ definiert. G sei die Gruppe der Idealklassen, h ihre Anzahl. h sei genau durch ℓ^ν teilbar. Dann hat G eine Untergruppe G_0 vom Grade ℓ^ν, deren Elemente als Exponenten Potenzen von ℓ haben. (Diese Untergruppe ist durch den Inbegriff aller Elemente von G definiert, die zu Potenzen von ℓ als Exponenten gehören, wie aus der Basisdarstellung von G leicht folgt).

Bezeichnen wir mit D die Gruppe der Klassen, deren Exponent zu ℓ prim ist, so ist G das *direkte Produkt* $G = G_0 \cdot D$.

Nun betrachten wir die Gesamtheit der Idealklassen *im absoluten Sinn*, welche mit G_0 Ideale gemein haben. Sie bilden ersichtlich eine Gruppe $\mathfrak{G}$. Wir stellen $\mathfrak{G}$ durch eine Basis von Idealklassen *im absoluten Sinn* dar. □□□ $\mathfrak{r}_1, \ldots, \mathfrak{r}_t$ sei ein System von Idealen aus diesen t Basisklassen von $\mathfrak{G}$, so gewählt, daß die $\mathfrak{r}_i$ in $\mathfrak{G}_0$ liegen, ferner untereinander und zu ℓ und $\mathfrak{m}$ prim sind. Dann ist jedes Ideal aus $\mathfrak{G}$, erst recht also jedes Ideal aus $\mathfrak{G}_0$ in der Form

$$(-\beta)\mathfrak{r}_1^{a_1} \ldots \mathfrak{r}_t^{a_t}$$

eindeutig darstellbar. (Ist $\mathfrak{K}$ die absolute Klasse von $\mathfrak{r}$, also $\mathfrak{K} = \mathfrak{r}(\beta)$, wo β alle Körperzahlen durchläuft, so ist in $\mathfrak{K}$ sicher jedes Ideal $\mathfrak{r}(\gamma)$ aus der Klasse $\mathfrak{k}$ nach $\mathfrak{m}$ enthalten ($\gamma \equiv 1 \bmod \mathfrak{m}$), es enthält also $\mathfrak{G}$ *alle* Ideale aus G_0).

Wegen $G = G_0 \cdot D$ ist nun jedes Ideal aus G, d.h. jedes zu $\mathfrak{m}$ prime Ideal $\mathfrak{r}$ als Produkt eines Ideals aus G_0 mit einem Ideal aus D darstellbar und diese Darstellung *in den Klassen* eindeutig. Da die Exponenten der Klassen von D prim zu ℓ sind, ist jede Klasse von D als ℓ–te Potenz einer Klasse darstellbar. Jedes Ideal aus D ist also mit der ℓ–ten Potenz eines Ideals äquivalent.

Jedes Ideal $\mathfrak{r}$, das zu $\mathfrak{m}$ prim ist, gestattet also eine eindeutige Darstellung (eindeutig in den a_i):

$$\mathfrak{r} = \mathfrak{r}_1^{a_1} \ldots \mathfrak{r}_t^{a_1}(\beta)j^\ell \tag{1}$$

wo $a_i = 0, 1, \ldots, \ell - 1$ und j zu $\mathfrak{m}$ prim also auch β zu $\mathfrak{m}$ prim angenommen werden darf. Die $\mathfrak{r}_i$ wollen wir als ganz voraussetzen.

Da $\mathfrak{r}_i$ zu G_0 gehört, ist eine gewisse Potenz $\mathfrak{r}_i^{\ell^{\kappa_i}}$ eine Strahlzahl. □□□ Daher ist auch der Exponent, zu dem $\mathfrak{r}_i$ im absoluten Sinne gehört eine Potenz von ℓ; denn □□□ dieser □□□

245 I

ist nach gruppentheoretischen Sätzen ein Teiler von ℓ^{κ_i}
□□□

Es mögen nun $(\varrho_1), \ldots, (\varrho_t)$ die niedrigsten Potenzen von $\mathfrak{r}_1, \ldots, \mathfrak{r}_t$ sein, die absolute Hauptideale sind, also Potenzen von $\mathfrak{r}_i$ mit Exponenten ℓ^{ν_i}:

$$\mathfrak{r}_i^{\ell^{\nu_i}} = (\varrho_i); \quad (\nu_i \geqq 1, \text{ da } \mathfrak{r}_i \text{ kein absolutes Hauptideal.})$$

Zu den Grundeinheiten von k möge, falls sie vorkommt, die höchste Einheitswurzel des Grades ℓ^{ν}, (d.h. ν möglichst groß), hinzugenommen werden, welche in k enthalten ist. Dann seien also $\varepsilon_1, \ldots, \varepsilon_{r+\delta}$ diese Einheiten und eben $\delta = 1$ oder 0, je nachdem die prim. ℓ–ten Einheitswurzeln in k vorkommen oder nicht.

Nun betrachten wir alle Zahlen der Form:

$$\alpha = \varepsilon_1^{u_1} \ldots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \ldots \varrho_t^{v_t}; \quad 0 \leqq u_i, v_i \leqq \ell - 1. \tag{2}$$

Soll eine Zahl α dieser Form ℓ–te Potenz einer Zahl sein, so muß also zunächst $\prod_i \mathfrak{r}_i^{\ell^{\nu_i} v_i}$ die ℓ–te Potenz eines Hauptideals sein, also $\prod_i \mathfrak{r}_i^{\ell^{\nu_i - 1} v_i}$ Hauptideal. Da die $\mathfrak{r}_i$ als Elemente aus absoluten Basisklassen unabhängig sind und die Exponenten ℓ^{ν_i} haben, muß v_i durch ℓ teilbar sein, d.h. $v_i = 0$. Es bleibt dann zu untersuchen, wann $\varepsilon_1^{u_1} \ldots \varepsilon_{r+\delta}^{u_{r+\delta}}$ die ℓ–te Potenz einer Einheit ist. Für die gewöhnlichen Grundeinheiten muß $u_i = 0$ sein, für die ℓ^{ν}–te Einheitswurzel auch, da keine höhere in k liegt. (2) stellt also nur für $u_i = v_i = 0$ die ℓ–te Potenz einer Zahl dar.

Die Zahlen der Form:

246 I

Die Zahlen der Form:

$$\alpha = \varepsilon_1^{u_1} \ldots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \ldots \varrho_t^{v_t} \xi^{\ell}; \quad 0 \leqq u_i, v_i \leqq \ell - 1, \tag{3}$$

wo ξ alle Zahlen aus k, die prim zu $\mathfrak{m}$ sind, durchläuft, bilden also eine Abelsche Gruppe vom Range $r + \delta + t$ in Bezug auf ℓ.

Wir betrachten nun die Untergruppe aller jener Zahlen (3), welche ℓ–te Potenzreste nach $\mathfrak{m}$ sind. Dieser Bedingung genügen alle Zahlen ξ^ℓ, sodaß Satz 4 anwendbar ist. Ihr Rang sei n, sodaß $n \leqq r + \delta + t$, □□□ dann ist offenbar ℓ^n die Anzahl der im System (2) enthaltenen ℓ–ten Potenzreste nach $\mathfrak{m}$. Die Basis dieser Untergruppe im Sinne von Satz 4 sei $\alpha_1, \ldots, \alpha_n$, die ℓ–ten Potenzreste von (3) also die Zahlen:

$$(4^\circ) \qquad \varrho = \alpha_1^{x_1}\alpha_2^{x_2}\ldots\alpha_n^{x_n}\xi^\ell; \quad 0 \leqq x_i \leqq \ell - 1$$

Nach Satz 4 kann man dann noch $r + \delta + t - n = N'$ Zahlen $\gamma_1, \ldots, \gamma_{N'}$ finden, sodaß sich alle Zahlen (3) auch in der Form

$$(4) \qquad \alpha = \gamma_1^{y_1}\ldots\gamma_{N'}^{y_{N'}}\alpha_1^{x_1}\ldots\alpha_n^{x_n}\xi^\ell; \quad 0 \leqq x_i, y_i \leqq \ell - 1$$

darstellen lassen. Ein solches α ist dann und nur dann ℓ–ter Potenzrest, wenn alle y_i Null sind. □□□

Die $\gamma_1, \ldots, \gamma_{N'}$, die ja Nichtreste sind, sind „unabhängige Nichtreste“ □□□ [...] daß kein Produkt aus ihnen ℓ–ter Potenzrest ist. In der Tat folgt aus

$$\gamma_1^{y_1}\ldots\gamma_{N'}^{y_{N'}} \equiv \xi^\ell \bmod \mathfrak{m}; \quad (y_i = 0, \ldots, \ell - 1)$$

nach (4), daß alle Exponenten $y_i = 0$ sein müssen

Die Zahlen

$$\gamma \equiv \gamma_1^{y_1}\ldots\gamma_{N'}^{y_{N'}}\xi^\ell \bmod \mathfrak{m}; \quad y_i = 0, 1, \ldots, \ell - 1$$

bilden eine Untergruppe der Gruppe aller zu $\mathfrak{m}$ primen Zahlen vom Range N', in der alle Zahlen ξ^ℓ vorkommen.

Es lassen sich also, wieder nach Satz 4, wenn wie im vorigen Abschnitt $R(\mathfrak{m})$ den Rang der Gruppe der primen Restklassen nach $\mathfrak{m}$ bedeutet, $N = R(\mathfrak{m}) - N'$ Zahlen $\eta_1, \ldots, \eta_N$ finden, sodaß jede zu $\mathfrak{m}$ prime Zahl β in der Form:

$$\beta \equiv \eta_1^{z_1}\ldots\eta_N^{z_N}\gamma_1^{y_1}\ldots\gamma_{N'}^{y_{N'}}\xi^\ell \bmod \mathfrak{m}$$

mit $0 \leqq z_i, y_i \leqq \ell - 1$ eindeutig darstellbar ist. Die η_i sind dann ebenfalls unter sich und von den γ_i unabhängige Nichtreste. Es ist, wenn man:

$$\beta = \eta_1^{z_1}\ldots\eta_N^{z_N}\gamma_1^{y_1}\ldots\gamma_{N'}^{y_{N'}}\alpha\xi^\ell \quad \text{setzt,}$$
$$\alpha \equiv 1 \mod \mathfrak{m}, \quad (\text{da die } \eta_i, \gamma_i, \xi \text{ prim zu } \mathfrak{m}),$$

also Strahlzahl.

Wendet man dies auf (1) an, so sieht man, daß jedes zu $\mathfrak{m}$ prime Ideal $\mathfrak{w}$ in der Form:

$$\mathfrak{r} = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} (\eta_1^{z_1} \dots \eta_N^{z_N} \alpha) j^\ell; \quad 0 \leqq a_i, z_i \leqq \ell - 1 \tag{5}$$

darstellbar ist. Denn die $\gamma_1^{y_1}, \dots, \gamma_{N'}^{y_{N'}}$ können wir, da sie dem System (3) angehören, □□□ und somit mindestens ℓ^1–te Potenzen der Ideale $\mathfrak{r}_1, \dots, \mathfrak{r}_t$ sind, (s. S. 245▶ oben) in j^ℓ hineinziehen, ebenso ξ^ℓ. Dabei bleibt j zu $\mathfrak{m}$ prim.

248 I

Ein Ideal (5) kann zunächst nur dann absolutes Hauptideal sein, wenn $a_1, \dots, a_t = 0$ ist, da (1) eindeutig in den a_i ist. Soll umsomehr $\mathfrak{r}$ ein Strahlhauptideal sein, so muß $a_1, \dots, a_t = 0$, also $(\eta_1^{z_1} \dots \eta_N^{z_N} \alpha) j^\ell$ Strahlzahl sein. Zunächst muß also j^ℓ Hauptideal sein. Setzt man der Zerlegung $G = G_0 D$ entsprechend:

$$j = \mathfrak{a} \cdot \mathfrak{b}; \quad (\mathfrak{a} \text{ aus } G_0;\ \mathfrak{b} \text{ aus } D),$$

so muß also der Unabhängigkeit von $\mathfrak{a}$ und $\mathfrak{b}$ wegen $\mathfrak{b}^\ell$ Hauptideal sein. Da aber $\mathfrak{b}$ zu D gehört, muß $\mathfrak{b}$ selbst Hauptideal (α_1) sein:

$$j = \mathfrak{a}(\alpha_1).$$

Das Ideal $\mathfrak{a}$ hat die Form: $\mathfrak{a} = (\alpha_1)\mathfrak{r}_1^{c_1} \dots \mathfrak{r}_t^{c_t}$, wo jetzt natürlich die c_i unbeschränkt sind. Da $\mathfrak{a}^\ell$ Hauptideal sein soll, und die $\mathfrak{r}_i$ als Basiselemente „absolut“ unabhängig sind, muß $\mathfrak{r}_i^{c_i \ell}$ Hauptideal, also eine Potenz von $(\varrho_i) = \mathfrak{r}_i^{\ell^{\nu_i}}$ sein. Somit ist: $j^\ell = (\varrho_1^{b_1} \dots \varrho_t^{b_t} \xi^\ell)$. Hier kann $0 \leqq b_i < \ell$ angenommen werden.

Soll nun $\mathfrak{r}$ Strahlhauptideal sein, also $(\eta_1^{z_1} \dots \eta_N^{z_N} \alpha) j^\ell$ Strahlhauptideal, so muß nach dem eben Bemerkten

$$\eta_1^{z_1} \dots \eta_N^{z_N} \alpha \varrho_1^{b_1} \dots \varrho_t^{b_t} \xi^\ell \cdot \varepsilon$$

Strahlzahl sein, wo ε eine geeignete Einheit in k ist. Die Einheit ε werde durch die $r + \delta$ Grundeinheiten dargestellt und alle ℓ–ten Potenzen aus ihr, speziell also die [...] Einheitswurzel von zu ℓ primem Grade, in ξ^ℓ hereingezogen. Dann muß also, da α Strahlzahl ist, der Ausdruck

$$\eta_1^{z_1} \dots \eta_N^{z_N} \varrho_1^{b_1} \dots \varrho_t^{b_t} \varepsilon_1^{d_1} \dots \varepsilon_{r+\delta}^{d_{r+\delta}} \xi^\ell \equiv 1 \mod \mathfrak{m}$$

sein, wo alle Exponenten zwischen 0 und $\ell - 1$ liegen.

249 I

□□□

Der Ausdruck

$$\varrho_1^{b_1} \dots \varrho_t^{b_t} \varepsilon_1^{d_1} \dots \varepsilon_{r+\delta}^{d_{r+\delta}} \xi^{\ell}$$

ist aber von der Form (3) und läßt sich mithin in der Form (4) darstellen, sodaß

$$\eta_1^{z_1} \dots \eta_N^{z_N} \gamma_1^{y_1} \dots \gamma_{N'}^{y_{N'}} \alpha_1^{x_1} \dots \alpha_n^{x_n} \xi^{\ell} \equiv 1 \mod \mathfrak{m}$$

sein muß, wo wieder $0 \leqq y_i, x_i \leqq \ell - 1$ gesetzt werden kann.

Die α_i können noch in ξ^{ℓ} hereingezogen werden, da sie Reste sind. Da die Nichtreste η_i unter sich und von den γ_i unabhängig sind, muß also insbesondere $z_i = 0$ sein. Damit ist gezeigt, daß ein Ideal (5) nur dann der Hauptklasse nach unserm Strahl o angehören kann, wenn alle Exponenten $a_1, \dots, a_t; z_1, \dots, z_N = 0$ sind.

Daraus folgt, daß zwei in der Form (5) dargestellte Ideale nur dann nach o äquivalent sein können, wenn ihre Exponentenreihen übereinstimmen, sodaß jeder Klasse nach o eindeutig eine Exponentenreihe entspricht.

Umgekehrt liefert jede Exponentenreihe, wenn j ein beliebiges, zu $\mathfrak{m}$ primes Ideal bedeutet eine bestimmte Klasse nach o vermöge (5). Der Rang der Gruppe G aller Klassen nach o ist also hiermit zu $N + t = t + R(\mathfrak{m}) - N'$ bestimmt. Setzt man für N' seinen Wert $r + \delta + t - n$ ein, so findet man also als Rang von G die Zahl: $R(\mathfrak{m}) + n - (r + \delta)$.

Satz 8. Es seien die Idealklassen nach dem Strahl o der Zahlen $\equiv 1 \mod \mathfrak{m}$ definiert. Dann hat die Gruppe der Idealklassen nach der Primzahl ℓ den Rang:

$$\bar{t} = R(\mathfrak{m}) + n - (r + \delta).$$

250 I

Darin bedeutet ℓ^n die Anzahl der ℓ–ten Potenzreste im System der Zahlen

$$\varepsilon_1^{x_1} \dots \varepsilon_{r+\delta}^{x_{r+\delta}} \varrho_1^{y_1} \dots \varrho_t^{y_t}; \qquad (0 \leqq x_i, y_i \leqq \ell - 1),$$

wo die ε_i und ϱ_i die erklärte Bedeutung haben; $R(\mathfrak{m})$ ist der Rang der Gruppe der primen Restklassen nach $\mathfrak{m}$.

Für ungerades ℓ genügt die in diesem Satz zugrundegelegte Idealklassendefinition. Für $\ell = 2$ kommen wir mit ihr nicht aus, sondern brauchen noch Vorzeichenfestsetzungen.

Es mögen, für $\ell = 2$, r_1 reelle Körper vorkommen, sodaß 2^{r_1} Signaturen denkbar sind. o sei, wie bisher, der Strahl der Zahlen $\equiv 1 \bmod \mathfrak{m}$, und $\mathfrak{r}_i$, ϱ_i mögen die gleiche Bedeutung haben, wie bisher.

V sei irgend eine Signaturgruppe vom Grade 2^{r_0} und o^+ der Strahl der Zahlen aus o mit Signatur aus V. Wegen $\ell = 2$ ist sicher $\delta = 1$.

Wir betrachten wieder die Gruppe der Zahlen (4°)

$$\alpha_1^{x_1} \dots \alpha_n^{x_n} \xi^2 ; \qquad x_i = 0 \text{ oder } 1. \tag{6}$$

Sie sind quadratische Reste, und mögen nun durch die Vorzeichenbeschränkung V eingeschränkt werden. Da ξ^2 total positiv ist, liegt ξ^2 in der entstehenden Untergruppe, sodaß Satz 4 anwendbar ist. Es sei n_0 der Rang dieser Untergruppe, 2^{n_0} also die Anzahl der quadratischen Reste mit Bedingung V im System der Zahlen (2)[6]. Die Untergruppe selbst sei $\beta_1^{x_1} \dots \beta_{n_0}^{x_{n_0}} \xi^2$. Nach Satz 4 gibt es in (6) genau $n - n_0$ Zahlen $\alpha'_1, \dots, \alpha'_{n-n_0}$, sodaß:

$$\alpha_1'^{\,y_1} \dots \alpha_{n-n_0}'^{\,y_{n-n_0}} \beta_1^{x_1} \dots \beta_{n_0}^{n_0} \xi^2 ; \qquad 0 \leqq x_i, y_i \leqq 1 \tag{7}$$

wieder das System (6) darstellt. Eine Zahl in (7) hat eine Signatur aus V dann und nur dann, wenn alle $y_i = 0$ sind. Die Signaturen der α'_i sind also untereinander und in Bezug auf die Signaturen V unabhängig.

Da in der Restklasse $\alpha \equiv 1 \bmod \mathfrak{m}$, die sicher quadratischer Rest ist, alle 2^{r_1} Signaturen vorkommen, kann man weitere Zahlen $\beta'_1, \dots, \beta'_p$, die quadratische Reste sind, so finden $\big(p = (r_1 - r_0) - (n - n_0)\big)$, daß durch

$$\beta_1'^{\,z_1} \dots \beta_p'^{\,z_p} \alpha_1'^{\,y_1} \dots \alpha_{n-n_0}'^{\,y_p} \xi^2 ; \qquad (z_i, y_i = 0, 1)$$

alle von V unabhängigen $2^{r_1 - r_0}$ Signaturen dargestellt werden, jede nur einmal. Nimmt man also noch $\beta_1, \dots, \beta_{n_0}$ hinzu, so wird jede Signatur dargestellt.

[6] undeutlich

In (5) ist $\alpha \equiv 1 \bmod \mathfrak{m}$. Bestimmt man die $x_i, y_i, z_i = 0, 1$ so, daß $\beta_1^{x_1} \ldots \beta_{n_0}^{x_{n_0}} {\alpha'_1}^{y_1} \ldots {\alpha'_{n-n_0}}^{y_{n-n_0}} {\beta'_1}^{z_1} \ldots {\beta'_p}^{z_p}$ die Signatur von α hat, so ist

$$\alpha_0 = \alpha \beta_1^{-x_1} \ldots {\alpha'_1}^{-y_1} \ldots {\beta'_1}^{-z_1} \ldots$$

total positiver quadratischer Rest,

$$\overline{\alpha}_0 = \alpha {\alpha'_1}^{-y_1} \ldots {\alpha'_{n-n_0}}^{-y_{n-n_0}} {\beta'_1}^{-z_1} \ldots {\beta'_p}^{-z_p}$$

quadratischer Rest mit Signatur aus V. Ist etwa $\overline{\alpha}_0 \equiv \xi^2 \bmod \mathfrak{m}$, und setzt man $\overline{\alpha}_0 = \alpha' \xi^2$, so ist $\alpha' \equiv 1 \bmod \mathfrak{m}$ und hat eine Signatur aus V, ist also Zahl aus o^+. Demnach kann man setzen:

$$\alpha = {\alpha'_1}^{y_1} \ldots {\alpha'_{n-n_0}}^{y_{n-n_0}} {\beta'_1}^{z_1} \ldots {\beta'_p}^{z_p} \alpha' \xi^2$$

wo α' in o^+ liegt. Setzt man dies in (5) ein, und beachtet, daß die α'_i Zahlen des Systems (3) sind, so folgt wie oben, daß

jedes Ideal $\mathfrak{r}$ (zu $\mathfrak{m}$ prim) in die Form:

$$\mathfrak{r} = \mathfrak{r}_1^{a_1} \ldots \mathfrak{r}_t^{a_t} \left(\eta_1^{c_1} \ldots \eta_N^{c_N} {\beta'_1}^{z_1} \ldots {\beta'_p}^{z_p} \alpha' \right) j^2 \tag{8}$$

mit $0 \leqq a_i, c_i, z_i \leqq 1$ und α' aus o^+, j prim zu $\mathfrak{m}$, gebracht werden kann.

Das Ideal (8) gehört nur dann zu o^+, wenn $a_i = 0$ und $c_i = 0$, was wie oben folgt, □□□ da die β'_i quadratische Reste sind, und anderes in unserem obigen Schluß für α nicht angewandt wurde.

Also muß $({\beta'_1}^{z_1} \ldots {\beta'_p}^{z_p} \alpha') j^2$ Strahlzahl aus o^+ sein, und da wieder, wie oben, j^2 die Form $(\varrho_1^{b_1} \ldots \varrho_t^{b_t} \xi^2)$ haben muß, eine Gleichung:

$${\beta'_1}^{z_1} \ldots {\beta'_p}^{z_p} \varepsilon_1^{d_1} \ldots \varepsilon_{r+\delta}^{d_{r+\delta}} \varrho_1^{b_1} \ldots \varrho_t^{b_t} \xi^2 \equiv 1 \mod \mathfrak{m}$$

und Signatur aus V bestehen. Da nun aber nach Konstruktion die Signaturen der β'_i untereinander und von denen der α'_1, β_i, □□□ unabhängig sind, und weil, da alle β'_i Reste sind, auch das Aggregat der ε_i, ϱ_i in unserer Kongruenz Rest sein muß, also als Rest des Systems (3) sich in der Form (6), d.h. (7) darstellen lassen muß, müssen die $z_i = 0$ sein. Denn es muß eine Gleichung bestehen:

$${\beta'_1}^{z_1} \ldots {\alpha'_1}^{y_1} \ldots \beta_1^{x_1} \ldots \xi^2 = \text{Zahl mit Signatur } V$$

Die Zahlen a_i, c_i, z_i in (8) sind also wieder durch die Klasse von $\mathfrak{r}$ nach o^+ eindeutig bestimmt, sodaß wie oben als Rang unser Idealklassengruppe nach o^+ der Wert herauskommt: $t+N+p$, der nun $p=(r_1-r_0)-(n-n_0)$ größer ist, und sich auch darstellt als $R(\mathfrak{m})+n_0+r_1-(r+r_0+1)$.

253 ı

Satz 9. Es seien die Idealklassen nach dem Strahl o^+ der Zahlen $\equiv 1 \bmod \mathfrak{m}$ mit der Vorzeichenbedingung V (Gruppe von 2^{r_0} Signaturen) definiert. Das System (2) dagegen sei auf Grund des vorigen Klassenbegriffes (nach o und absolut) erklärt. Der Rang der Gruppe der Idealklassen nach o^+ bestimmt sich dann für $\ell=2$ zu:

$$\bar{t}=R(\mathfrak{m})+n_0+r_1-(r+r_0+1).$$

Darin ist 2^{n_0} die Anzahl der den Vorzeichenbedingungen V genügenden quadratischen Reste des Systems (2), r_1 die Anzahl der reellen Körper, 2^{r_0} der Grad von V.

Auf Grund von Satz 3 bestimmt sich jetzt leicht in allen diesen Fällen die Anzahl der Klassengruppen vom Index ℓ. Man findet nach diesem Satze genau $\frac{\ell^{\bar{t}}-1}{\ell-1}$ Untergruppen der □□□ Gruppe aller Klassen vom Index ℓ, wo $\bar{t}$ die Zahl aus Satz 8 oder 9 bedeutet.

Es mag noch hervorgehoben werden, daß nach den Strahlen o und o^+ *alle* Klassengruppen mod $\mathfrak{m}$ *überhaupt* erhalten werden, wenn man alle Untergruppen der Gruppe der Klassen nach o und o^+ bildet (o^+ für total positive Zahlen gebildet), ferner daß die Forderung, daß der Index ℓ sein soll eine von der Definition der Klassengruppe unabhängige ist.

1.7 Kummersche Körper.

254 I

a) Das Potenzrestsymbol

In diesem Abschnitt wird durchweg vorausgesetzt, daß k die primitive ℓ–te Einheitswurzel ζ enthält. Für $\ell = 2$ ist dies selbstverständlich.

α sei prim zum Primideal $\mathfrak{p}$ und dieses prim zu ℓ. Dann gilt

$$\alpha^{\mathsf{N}(\mathfrak{p})-1} \equiv 1 \mod \mathfrak{p}.$$

In k ist nun $R(\zeta)$ als Unterkörper enthalten. $\mathfrak{p}$ gehe im Primideal $\overline{\mathfrak{p}}$ von $R(\zeta)$ auf. Bedeutet n und n_r die Norm in $R(\zeta)$ und die Relativnorm $\big(k, R(\zeta)\big)$, so ist:

$$n(\overline{\mathfrak{p}}) \equiv 1 \bmod \ell$$
$$\mathsf{N}(\mathfrak{p}) = n n_r(\mathfrak{p}) = n(\overline{\mathfrak{p}}^{f_r}) = \big(n(\overline{\mathfrak{p}})\big)^{f_r}$$

wo f_r der Relativgrad von $\mathfrak{p}$ zu $R(\zeta)$ ist. Also ist

$$\mathsf{N}(\mathfrak{p}) \equiv 1 \mod \ell$$

und für jedes zu ℓ prime Primideal in k:

$$\phi(\mathfrak{p}) = \mathsf{N}(\mathfrak{p}) - 1 \equiv 0 \mod \ell.$$

Setzen wir also vorübergehend $\mathsf{N}(\mathfrak{p}) - 1 = \ell\nu$, so ist:

$$\alpha^{\ell\nu} \equiv 1 \bmod \mathfrak{p} \qquad \text{oder:}$$
$$(\alpha^\nu - 1)(\alpha^\nu - \zeta) \cdots (\alpha^\nu - \zeta^{\ell-1}) \equiv 0 \bmod \mathfrak{p}.$$

Es muß also mindestens einer der Faktoren links[1] durch $\mathfrak{p}$ teilbar sein. Da die Differenz zweier der Faktoren:

$$\zeta^r - \zeta^{r+s} = \zeta^r(1 - \zeta^s)$$

[1] undeutlich

255 I

stets nur durch den Faktor $(1-\zeta)$ von ℓ teilbar, also zu $\mathfrak{p}$ prim ist, kann auch *nur ein* Faktor durch $\mathfrak{p}$ teilbar sein. Es gibt also genau eine ℓ–te Einheitswurzel ζ^c, sodaß:

$$\alpha^{\frac{\mathsf{N}(\mathfrak{p})-1}{\ell}} \equiv \zeta^c \mod \mathfrak{p} \quad \text{ist.} \tag{1}$$

Definition 1. Die durch die Kongruenz (1) definierte ℓ–te Einheitswurzel ζ^c heißt der ℓ–te Potenzcharakter von α nach $\mathfrak{p}$: □□□

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \zeta^c.$$

Unmittelbar klar ist:

Satz 1. Es ist $\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\beta}{\mathfrak{p}}\right)$

Satz 2. Es ist $\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$ dann und nur dann, wenn α ℓ–ter Potenzrest nach $\mathfrak{p}$ ist.

Beweis. a.) Sei $\alpha \equiv \alpha_0^\ell \mod \mathfrak{p}$. Dann ist

$$\alpha^{\frac{\mathsf{N}(\mathfrak{p})-1}{\ell}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha_0^{\mathsf{N}(\mathfrak{p})-1} \equiv 1 \mod \mathfrak{p};$$

Da die Potenzen $1, \zeta, \ldots, \zeta^{\ell-1} \mod \mathfrak{p}$ inkongruent sind (S. 254▶) folgt $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$.

b.) Sei $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$ und ϱ primitive Wurzel mod $\mathfrak{p}$. Dann ist sicher $\left(\frac{\varrho}{\mathfrak{p}}\right) \neq 1$, da $\varrho^{\frac{\mathsf{N}(\varrho)-1}{\ell}} \not\equiv 1 \mod \mathfrak{p}$. Sei $\left(\frac{\varrho}{\mathfrak{p}}\right) = \zeta^g$; $(g \not\equiv 0 \mod \ell)$ und $g^\star$ eine solche zu $\mathsf{N}(\mathfrak{p})-1$ prime Zahl, daß $gg^\star \equiv 1 \mod \ell$. Das ist stets möglich;□□□

256 I

(Denn ist $\mathsf{N}(\mathfrak{p}) - 1 = \nu\ell = \nu_0\ell^k$; $(\nu_0, \ell) = 1$ so bestimme man $g^\star$ [2] aus:

$$g^\star \equiv \frac{1}{g} \mod \ell^k$$
$$g^\star \equiv 1 \mod \nu_0.$$

[2] g ist hier und an einigen weiteren Stellen mit einem Superskript versehen, wohl ein $\star$.

Dann wird offenbar $gg^\star \equiv 1 \bmod \ell$ und $g^\star$ zu ℓ und ν_0, also zu $\mathsf{N}(\mathfrak{p})-1$ prim).

Dann ist $\varrho^{g^\star}$ ebenfalls primitive Wurzel mod $\mathfrak{p}$ und nach Satz 1:

$$\left(\frac{\varrho^{g^\star}}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\mathfrak{p}}\right)^{g^\star} = \zeta^{gg^\star} = \zeta$$

Wir können also von ϱ von vorneherein annehmen, daß $\left(\frac{\varrho}{\mathfrak{p}}\right) = \zeta$ ist.

Wenn nun $\alpha \equiv \varrho^c \bmod \mathfrak{p}$ ist, ist $\left(\frac{\alpha}{\mathfrak{p}}\right) = \left(\frac{\varrho^c}{\mathfrak{p}}\right) = \zeta^c$. □□□ Also ist nach Voraussetzung $\zeta^c = 1$, $c \equiv 0 \bmod \ell$, $\alpha \equiv (\varrho^{c'})^\ell$ ℓ–ter Potenzrest.

Ferner folgt aus der letzten Diskussion gleich folgendes:

Den Potenzcharakter ζ^c haben genau die Restklassen:

$$\alpha \equiv \varrho^c, \varrho^{c+\ell}, \varrho^{c+2\ell}, \ldots, \varrho^{c+\left(\frac{\mathsf{N}(\mathfrak{p})-1}{\ell}-1\right)\ell} \bmod \mathfrak{p},$$

also genau der ℓ–te Teil aller primen Restklassen.

Satz 3. Die primen Restklassen nach dem Primideal $\mathfrak{p}$ (prim zu ℓ) zerfallen in ℓ Teilsysteme von je $\frac{\mathsf{N}(\mathfrak{p})-1}{\ell}$ Restklassen gleichen Potenzcharakters. Jeder vorgeschriebene Potenzcharakter gehört zu einem jener Systeme, insbesondere der Potenzcharakter 1 zu dem System von $\frac{\mathsf{N}(\mathfrak{p})-1}{\ell}$ Restklassen von ℓ–ten Potenzresten nach $\mathfrak{p}$.

b) Die Primideale

b.) Die Primideale des Kummerschen Körpers.

Definition 2. Es sei μ eine Zahl aus k, welche nicht die ℓ–te Potenz einer Zahl aus k ist. Dann ist die Gleichung

$$x^\ell - \mu = 0$$

irreduzibel in k. Da die ℓ–te Einheitswurzel ζ in k enthalten ist, ist durch $k(\sqrt[\ell]{\mu})$ ein relativ zyklischer Körper vom Primzahlgrad ℓ gegeben. Die zu $\sqrt[\ell]{\mu}$ relativ konjugierten sind $\zeta^i\sqrt[\ell]{\mu}$.

Den Körper nennen wir einen *Kummerschen Körper.*

Wir unterteilen nun die Zerlegung der Primideale von k in $k(\sqrt[\ell]{\mu}) = K$.

Geht das Primideal $\mathfrak{p}$ in μ auf, so können wir vereinfachende Annahmen machen.

1.) Es gehe in μ mit einem durch ℓ teilbaren Exponenten $\ell\nu$ auf. Ist π Primzahl für $\mathfrak{p}$, □□□ dann ist $\mu^\times = \frac{\mu}{\pi^{\ell\nu}}$ nicht durch $\mathfrak{p}$ teilbar und $\sqrt[\ell]{\mu^\times} = \frac{\sqrt[\ell]{\mu}}{\pi^\nu}$ definiert K ebenfalls. Es kann also μ prim zu $\mathfrak{p}$ angenommen werden.

2.) $\mathfrak{p}$ gehe genau zur Potenz $\mathfrak{p}^\nu$ in μ auf, und ν sei prim zu ℓ. Dann lassen sich a und b so bestimmen, daß $a\nu + b\ell = 1$, also $\mu^\times = \square\square\square\mu^a\pi^{b\ell}$ genau durch $\mathfrak{p}$ teilbar wird, und $\sqrt[\ell]{\mu^\times} = \pi^b(\sqrt[\ell]{\mu})^a$, wie man leicht sieht,

denselben Körper wie $\sqrt[\ell]{\mu}$ definiert. Denn ist $aa' = 1 + e\ell$, so wird:

$$(\sqrt[\ell]{\mu^\times})^{a'} = \pi^{a'b}\sqrt[\ell]{\mu}\cdot\mu^e, \quad \text{d.h.} \quad \sqrt[\ell]{\mu} = \pi^{-a'b}\mu^{-e}\sqrt[\ell]{\mu^\times}^{a'}.$$

Es darf also angenommen werden, daß μ entweder gar nicht, oder genau durch $\mathfrak{p}^1$ teilbar ist.

1.) $\mathfrak{p}$ *geht genau zur ersten Potenz in* μ *auf.*

Wir setzen $\mathfrak{P} = (\mathfrak{p}, \sqrt[\ell]{\mu})$. Dann ist:

$$\mathfrak{P}^\ell = (\mathfrak{p}^\ell, \mu) = \mathfrak{p}$$

Also ist $\mathfrak{p}$ die ℓ–te Potenz des Ideals $\mathfrak{P}$ in K, das dann notwendig Primideal sein muß (allgemeiner Satz über Galoissche Körper). □□□ $\mathfrak{p}$ geht in der Relativdiskriminante auf.

a.) $\mathfrak{p}$ *ist prim zu* ℓ. Nach Satz 1 (S. 148▸) ist die Relativdiskriminante genau durch $\mathfrak{p}^{\ell-1}$ teilbar.

b.) $\mathfrak{l}$ gehe in ℓ genau zur s–ten Potenz auf und in μ zur ersten. Da in $R(\zeta)$: $\ell = (1-\zeta)^{\ell-1}$ ist, muß s durch $\ell - 1$ teilbar sein: $s = s_0(\ell-1)$. In K ist $\mathfrak{l} = L^\ell$, und $\sqrt[\ell]{\mu}$ genau durch L teilbar. Nun ist $\sigma\sqrt[\ell]{\mu} - \sqrt[\ell]{\mu} = (\zeta-1)\sqrt[\ell]{\mu}$. $(1-\zeta)$ ist genau durch $\mathfrak{l}^{s_0} = L^{\ell s_0}$ teilbar, $\sigma\sqrt[\ell]{\mu} - \sqrt[\ell]{\mu}$ also genau durch $L^{s_0\ell+1}$. Nach Satz 2 (S. 149▸) ist also das dortige $v+1$ gerade $s_0\ell+1$, also $v = s_0\ell$. Die Relativdiskriminante ist also genau durch die Potenz $\mathfrak{l}^{(s_0\ell+1)(\ell-1)}$ teilbar.

2.) $\mathfrak{p}$ *sei prim zu* μ *und prim zu* ℓ.

a.) $\frac{\mu}{\mathfrak{p}} = 1$. Dann gibt es ein λ, sodaß

$$\mu \equiv \lambda^\ell \bmod \mathfrak{p}$$

259 I

Dabei können wir annehmen, es sei $\lambda^\ell \not\equiv \mu \bmod \mathfrak{p}^2$; denn ist $\lambda^\ell \equiv \mu \bmod \mathfrak{p}^2$ und π Primzahl, so ist

$$(\lambda + \pi)^\ell \equiv \mu \mod \mathfrak{p}$$

dagegen $(\lambda + \pi)^\ell \equiv \mu + \ell\lambda^{\ell-1}\pi \not\equiv \mu \bmod \mathfrak{p}^2$, da λ u. ℓ prim zu $\mathfrak{p}$ sind.

Nun setzen wir

$$\mathfrak{P} = (\mathfrak{p}, \sqrt[\ell]{\mu} - \lambda); \quad \mathfrak{P}_1 = \sigma\mathfrak{P} = (\mathfrak{p}, \zeta\sqrt[\ell]{\mu} - \lambda); \quad \dots$$
$$\mathfrak{P}_{\ell-1} = \sigma^{\ell-1}\mathfrak{P} = (\mathfrak{p}, \zeta^{\ell-1}\sqrt[\ell]{\mu} - \lambda).$$

Nun ist $(\mathfrak{p}, \mathfrak{a}_1\mathfrak{a}_2) = (\mathfrak{p}, \mathfrak{a}_1)\cdot(\mathfrak{p}, \mathfrak{a}_2)$ falls $(\mathfrak{a}_1, \mathfrak{a}_2)$ prim zu $\mathfrak{p}$, und entsprechend für mehr Faktoren.

Da hier:

$$(\zeta^i\sqrt[\ell]{\mu} - \lambda, \zeta^k\sqrt[\ell]{\mu} - \lambda) = (\sqrt[\ell]{\mu}(\zeta^i - \zeta^k), \zeta^k\sqrt[\ell]{\mu} - \lambda)$$

ist, und $\sqrt[\ell]{\mu}$ und $\zeta^i - \zeta^k \sim (1 - \zeta)$ prim zu $\mathfrak{p}$ sind, folgt

$$\mathfrak{P}\mathfrak{P}_1 \dots \mathfrak{P}_{\ell-1} = (\mathfrak{p}, \mu - \lambda^\ell) = \mathfrak{p}.$$

Also sind die $\mathfrak{P}_i$ Primideale in K, die alle voneinander verschieden sind, weil aus

$$(\mathfrak{p}, \sqrt[\ell]{\mu} - \lambda) = (\mathfrak{p}, \zeta\sqrt[\ell]{\mu} - \lambda)$$

folgen würde, daß $\sqrt[\ell]{\mu} - \lambda$ und $\zeta\sqrt[\ell]{\mu} - \lambda$ einen gemeinsamen Teiler hätten, der in $\mathfrak{p}$ aufginge, was soeben als unmöglich erkannt.

$\mathfrak{p}$ zerfällt also in ℓ verschiedene Primideale ersten Grades. Wenn umgekehrt $\mathfrak{p} = \mathfrak{P}\mathfrak{P}_1 \dots \mathfrak{P}_{\ell-1}$ in ℓ gleiche oder verschiedene Primideale ersten Grades zerfällt, so ist die Anzahl der Restklassen nach $\mathfrak{P}$ gleich der nach $\mathfrak{p}$. Jede Zahl aus K

260 I

also einer Zahl aus k kongruent nach $\mathfrak{P}$, insbesondere:

$$\sqrt[\ell]{\mu} \equiv \alpha \mod \mathfrak{P},$$

also $\mu \equiv \alpha^\ell \bmod \mathfrak{P}$, also auch mod $\mathfrak{p}$

μ ist also ℓ–ter Potenzrest nach $\mathfrak{p}$, $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$, und somit nach der Betrachtung vorher alle Primfaktoren $\mathfrak{P}_i$ verschieden, $\mathfrak{p}$ also kein Relativdiskriminantenteiler.

b.) $\left(\frac{\mu}{\mathfrak{p}}\right) \neq 1$. Dann muß notwendig $\mathfrak{p}$ in K Primideal bleiben. Denn nach der Diskussion in a.) ist $\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_\ell$ und $\mathfrak{P} = \mathfrak{P}^\ell$ ausgeschlossen, da jedesmal (immer unter der Voraussetzung 2.) μ prim zu $\mathfrak{p}$) $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$ folgen würde, entgegen der Annahme b.).

$\mathfrak{p}$ geht also nicht in der Relativdiskriminante auf und wird in K ein Primideal ℓ–ten Relativgrades.

3.) $\mathfrak{l}$ *sei prim zu* μ *und* $\ell \sim \mathfrak{l}^s = \mathfrak{l}^{s_0(\ell-1)}$.

Hier ist für die Zerfällung von $\mathfrak{l}$ maßgebend, welches der höchste Exponent m ist, für den die Kongruenz:

$$x^\ell \equiv \mu \mod \mathfrak{l}^m \tag{1}$$

lösbar ist (m kann auch ∞ sein).

Zunächst gilt folgendes:

Wenn die Kongruenz

$$x^\ell \equiv \mu \bmod \mathfrak{l}^{\nu\ell}; \qquad (\nu < s_0)$$

lösbar ist, so ist sie sicher auch mod $\mathfrak{l}^{\nu\ell+1}$ lösbar.

In der Tat, sei $\alpha^\ell \equiv \mu \bmod \mathfrak{l}^{\nu\ell}$ und λ_ν genau durch $\mathfrak{l}^\nu$ teilbar. Wir setzen: $\alpha^\ell \equiv \mu + \lambda_\nu^\ell \xi \bmod \mathfrak{l}^{\nu\ell+1}$.

261 ı

Dann ist □□□

$$(\alpha + \lambda_\nu \eta)^\ell = \alpha^\ell + \binom{\ell}{1}\alpha^{\ell-1}\lambda\eta + \binom{\ell}{2}\alpha^{\ell-2}\lambda_\nu^2\eta^2 + \dots + \lambda_\nu^\ell \eta^\ell$$

Das Glied $\binom{\ell}{\kappa}\lambda_\nu^\kappa$ ist durch $\mathfrak{l}^{s_0(\ell-1)+\nu\kappa}$, also wegen

$$\nu < s_0; \quad (s_0 - \nu)(\ell - 1) > 0; \quad s_0\ell - \nu\ell - s_0 + \nu > 0; \quad s_0(\ell-1) + \nu > \nu\ell$$

sicher durch $\mathfrak{l}^{\nu\ell+1}$ teilbar, sodaß

$$(\alpha+\lambda_\nu\eta)^\ell \equiv \alpha^\ell + \lambda_\nu^\ell\eta^\ell \mod \mathfrak{l}^{\nu\ell+1}.$$

Auf Grund von Satz 7 (S. 159▸) werde η so bestimmt, daß (falls überhaupt ξ Einheit):

$$\eta^\ell \equiv -\xi \mod \mathfrak{l}$$

ist. Dann ist $(\alpha+\lambda_\nu\eta)^\ell \equiv \alpha^\ell - \lambda_\nu^\ell\xi \equiv \mu \bmod \mathfrak{l}^{\nu\ell+1}$, w.z.b.w.

Nun sei $\boldsymbol{m \leqq \ell s_0}$ die höchste Potenz von ℓ, bei der die Kongruenz (1) noch lösbar ist. α sei eine Lösung. Wir setzen $m = \ell\nu+\kappa$; $0 \leqq \kappa \leqq \ell-1$; also $\nu \leqq s_0$. Im Falle $\nu < s_0$ ist nach dem Gezeigten sicher $\kappa > 0$, im Falle $\nu = s_0$; $m = \ell s_0$ also $\kappa = 0$.

Die Zahl $x = (\sqrt[\ell]{\mu} - \alpha)\lambda^{-\nu}$, wo λ Primzahl, genügt der Gleichung:

$$(\lambda^\nu x + \alpha)^\ell - \mu = 0$$

d.h.

$$\left(x + \frac{\alpha}{\lambda^\nu}\right)^\ell - \frac{\mu}{\lambda^{\nu\ell}} = 0$$

$$x^\ell + \binom{\ell}{1}\frac{\alpha}{\lambda^\nu}x^{\ell-1} + \binom{\ell}{2}\frac{\alpha^2}{\lambda^{2\nu}}x^{\ell-2} + \cdots + \binom{\ell}{\ell-1}\frac{\alpha^{\ell-1}}{\lambda^{\nu(\ell-1)}} + \frac{1}{\lambda^{\nu\ell}}\binom{\ell}{\alpha-\mu} = 0$$

Das Glied $\binom{\ell}{i}$ ist für $1 \leqq i \leqq \ell-1$ durch $\mathfrak{l}^{s_0(\ell-1)}$ also jedes mittlere Glied durch $\mathfrak{l}^{(s_0-\nu)(\ell-1)}$ teilbar, □□□

262 I

also wegen $s_0 \geqq \nu$ sicher für den Bereich von $\mathfrak{l}$ ganz. Das letzte Glied ist wegen $\alpha^\ell \equiv \mu \bmod \mathfrak{l}^m = \mathfrak{l}^{\nu\ell+\kappa}$ sicher ganz für den Bereich von $\mathfrak{l}$. Die Zahl □□□ $A = (\sqrt[\ell]{\mu} - \alpha)\lambda^{-\nu}$ ist also ganz für den Bereich von $\mathfrak{l}$. Die Relativnorm von A ist:

$$n(A) = \pm\frac{\alpha^\ell - \mu}{\lambda^{\nu\ell}} \sim \mathfrak{l}^{\nu\ell+\kappa-\nu\ell} = \mathfrak{l}^\kappa$$

A kann nicht mehr durch $\mathfrak{l}$ teilbar sein, da sonst $n(A)$ durch $\mathfrak{l}^\ell$ teilbar, während doch $\kappa < \ell$ ist.

Ist nun $m < \ell s_0$, so ist $\kappa > 0$, $n(A)$ also durch $\mathfrak{l}$ teilbar, ohne daß A durch $\mathfrak{l}$ teilbar ist, A also nicht prim zu $\mathfrak{l}$, da es sonst jede konjugierte, also $n(A)$ wäre; es haben also A und $\mathfrak{l}$ einen von 1 verschiedenen Primteiler L gemeinsam. $\mathfrak{l}$ zerfällt also.

Wäre nun $\mathfrak{l} = L_1 \dots L_\ell$, wo alle L_i verschieden, so müßte, da $n(A)$ durch $\mathfrak{l}$ teilbar ist, □□□ muß jedes L_i in einem bestimmten $A^{(i)}$ aufgehen. □□□ (das so bezeichnet werden darf). Der größte gemeinsame Teiler von A und $A^{(i)}$ ist nun

$$(A, A^{(i)}) = \left((\sqrt[\ell]{\mu} - \alpha)\lambda^{-\nu}, (\zeta^i \sqrt[\ell]{\mu} - \alpha)\lambda^{-\nu}\right) = \left((1-\zeta^i)\sqrt[\ell]{\mu}\lambda^{-\nu}, A^{(i)}\right)$$

Da $(1-\zeta^i)$ durch $\mathfrak{l}$, also durch L_i und $A^{(i)}$ ebenfalls durch L_i teilbar ist, wäre A durch L_i teilbar.
□□□

263 I

A wäre also durch jedes L_i, also durch $\mathfrak{l}$ teilbar, was nicht der Fall. Daher ist sicher $\mathfrak{l} = L^\ell$. $\mathfrak{l}$ geht also in der Relativdiskriminante auf. $\alpha^\ell - \mu$ ist genau durch $\mathfrak{l}^m = L^{\ell m}$ teilbar, die Zahl $B = \alpha - \sqrt[\ell]{\mu}$ also genau durch L^m, da sonst

$$\begin{array}{rrcll} \text{aus} & \alpha - \sqrt[\ell]{\mu} & \equiv & 0 & \bmod L^{m+1} \\ \text{folgte} & \alpha - \zeta\sqrt[\ell]{\mu} & \equiv & 0 & \bmod L^{m+1} \\ \hline & \alpha^\ell - \mu & \equiv & 0 & \bmod L^{(m+1)\ell} = \mathfrak{l}^{m+1} \end{array}$$

was nach Definition von m nicht der Fall. $\sigma B - B = \sqrt[\ell]{\mu}(1-\zeta)$ ist aber genau durch $\mathfrak{l}^{s_0} = L^{\ell s_0}$ teilbar, da $\sqrt[\ell]{\mu}$ prim zu L. Wie auf S. 151 unten gezeigt wurde, ist andererseits, da m prim zu ℓ (S. 261 Mitte) $\sigma B - B$ genau durch L^{v+m} teilbar, also $s_0\ell = v + m$; $v = s_0\ell - m$. In der Relativdiskriminante geht also genau die Potenz $\mathfrak{l}^{(s_0\ell - m + 1)(\ell-1)}$ auf.

Im Falle $m \geqq s_0\ell$ ist wenigstens $\alpha^\ell \equiv \mu \bmod \mathfrak{l}^{s_0\ell}$ lösbar. Die Zahl α sei im Falle $m > s_0\ell$ als Lösung der Kongruenz mod $\mathfrak{l}^{s_0\ell+1}$ gewählt.

Wieder bilden wir $A = (\sqrt[\ell]{\mu} - \alpha)\lambda^{-s_0}$. Dies A genügt der Gleichung

$$F(x) = \left(x + \frac{\alpha}{\lambda^{s_0}}\right)^\ell - \frac{\mu}{\lambda^{s_0\ell}} = 0 \quad \text{oder}$$
$$x^\ell + \dots + \binom{\ell}{i} x^{\ell-i}\frac{\alpha^i}{\lambda^{is_0}} + \dots + \frac{1}{\lambda^{s_0\ell}}(\alpha^\ell - \mu) = 0.$$

Die mittleren Glieder haben wie vorhin nicht negative Ordnungszahl. $\alpha^\ell - \mu$ ist durch $\mathfrak{l}^{s_0\ell}$ teilbar, also alle Koeffizienten

264 I

ganz für $\mathfrak{l}$, A ganz für $\mathfrak{l}$. Die Relativdiskriminante von A ist durch die Relativdiskriminante für K teilbar, da letztere der Inhalt der ℓ–gliedrigen Determinante $|\Xi_i^{(k)}|^2$ ist, aus der die Relativdiskriminante für A hervorgeht, wenn für die Unbestimmten diejenigen Werte gesetzt werden, die A erzeugen, die also keine Potenzen von $\mathfrak{l}$ im Nenner haben können. Nun ist:

$$F'(A^{(i)}) = \ell\left(x + \frac{\alpha}{\lambda^{s_0}}\right)^{\ell-1} \quad \text{für} \quad x = A^{(i)} = (\zeta^i \sqrt[\ell]{\mu} - \alpha)\lambda^{-s_0}$$
$$= \ell\lambda^{-s_0(\ell-1)}\zeta^{i(\ell-1)}\sqrt[\ell]{\mu}^{\ell-1}$$

Da $\ell \sim \mathfrak{l}^{s_0(\ell-1)}$, ζ Einheit und μ prim zu $\mathfrak{l}$ ist, ist $F'(A^{(i)})$ prim zu $\mathfrak{l}$, also auch die Relativdiskriminante von A, die ja bis aufs Vorzeichen das Produkt aller $F'(A^{(i)})$ ist.

$\mathfrak{l}$ geht also auch in der Relativdiskriminante von K nicht auf.

Ferner kann A nicht durch $\mathfrak{l}$ teilbar sein, da sonst auch $A^{(i)}$ es wäre, und somit die Relativdiskriminante von A.

Für $m > s_0\ell$ ist andererseits A *nicht* prim zu $\mathfrak{l}$, denn sonst wäre es auch $A^{(i)}$, also auch die Relativnorm $n(A) = \pm\frac{\alpha^\ell - \mu}{\lambda^{s_0\ell}}$, die nach Voraussetzung mindestens durch $\mathfrak{l}$ teilbar ist. Also müssen $\mathfrak{l}$ und A einen von 1 verschiedenen Faktor gemein haben, d.h. $\mathfrak{l}$ muß zerfallen. Es bleibt daher für $\mathfrak{l}$ nur die Möglichkeit, daß es in ℓ *verschiedene* Primideale

zerfällt:

$$\mathfrak{l} = L_1 \ldots L_\ell\,.$$

Wenn andererseits eine solche Zerfällung stattfindet, geht $\mathfrak{l}$ nicht in der Relativdiskriminante auf. Es gibt also ein α, sodaß:

$$\alpha^\ell \equiv \mu \mod \mathfrak{l}^{s_0\ell},$$

da sonst $m < s_0\ell$ und, wie gezeigt $\mathfrak{l} = L^\ell$, also $\mathfrak{l}$ Teiler der Relativdiskriminante ist. Wir zeigen, daß dann sicher $m > s_0\ell$, d.h. unsere Kongruenz auch mod $\mathfrak{l}^{s_0\ell+1}$ lösbar ist.

Es ist nämlich dann, wie immer, jede Zahl aus K einer Zahl aus k mod L_1 kongruent. Sei

$$A = (\alpha - \sqrt[\ell]{\mu})\lambda^{-s_0} \equiv \xi \mod L_1; \quad (\xi \text{ in } k).$$

Da $(A-\xi)$ durch L_1 teilbar ist, ist $(A^{(i)}-\xi)$ durch L_i teilbar, also:

$$n(A-\xi)=\lambda^{-s_0\ell}(\alpha^\ell-\mu)\equiv 0 \mod \mathfrak{l}$$
$$\alpha^\ell-\mu\equiv 0 \mod \mathfrak{l}^{s_0\ell+1}, \quad \text{w.z.b.w.}$$

Wenn also schließlich $\boldsymbol{m=s_0\ell}$ ist, muß $\mathfrak{l}$ in K selbst Primideal bleiben. Denn sonst wäre entweder die Relativdiskriminante durch $\mathfrak{l}$ teilbar, was auf S. 264 Mitte für $m\geqq s_0\ell$ als unmöglich erkannt, oder $\mathfrak{l}=L_1\dots L_\ell$, was zu $m>s_0\ell$ führen würde.

Wir fassen alle Resultate in folgende Sätze zusammen.

Satz 4. Ist μ prim zu $\mathfrak{p}$ oder durch eine Potenz von $\mathfrak{p}$ teilbar, deren Exponent ein Vielfaches von ℓ ist, so geht $\mathfrak{p}$ nicht in der Relativdiskriminante von $K=k(\sqrt[\ell]{\mu})$ auf, wenn $\mathfrak{p}$ prim zu ℓ ist. Es kann dann stets μ prim zu $\mathfrak{p}$ angenommen werden.

Ist dann

1.) $\left(\frac{\mu}{\mathfrak{p}}\right)=+1$, so zerfällt $\mathfrak{p}$ in ℓ verschiedene Primideale in K.

2.) $\left(\frac{\mu}{\mathfrak{p}}\right)\neq 1$, so bleibt $\mathfrak{p}$ Primideal in K.

Satz 5. Ist $\mathfrak{p}$ prim zu ℓ und geht in μ in einer Potenz auf, deren Exponent prim zu ℓ ist, so wird $\mathfrak{p}$ in K die ℓ–te Potenz eines Primideals. Dasselbe gilt, wenn $\mathfrak{p}$ nicht prim zu ℓ ist. Über die Relativdiskriminante gilt:

1.) Ist $\mathfrak{p}$ prim zu ℓ, so ist sie genau durch $\mathfrak{p}^{\ell-1}$ teilbar.

2.) Ist $\mathfrak{p}=\mathfrak{l}$ ein Primfaktor von ℓ, der in ℓ in der $s=s_0(\ell-1)$ ten Potenz aufgeht, so ist die Relativdiskriminante von K genau durch $\mathfrak{l}^{(s_0\ell+1)(\ell-1)}$ teilbar.

Satz 6. Geht $\mathfrak{l}$ in ℓ zur $s_0(\ell-1)$ ten und in μ zu einer Potenz auf, deren Exponent ein Vielfaches von ℓ ist, so kann μ prim zu $\mathfrak{l}$ angenommen werden.

Es sei m die größte ganze Zahl (ev. ∞), für die die Kogruenz $x^\ell\equiv\mu \mod \mathfrak{l}^m$ lösbar ist.

1.) Für $m<s_0\ell$ ist m prim zu ℓ, $\mathfrak{l}$ die ℓ–te Potenz eines Primideals in K und die Relativdiskriminante genau durch $\mathfrak{l}^{(s_0\ell-m+1)(\ell-1)}$ teilbar.

2.) Für $m = s_0\ell$ bleibt $\mathfrak{l}$ Primideal in K.

3.) Für $m > s_0\ell$ wird $\mathfrak{l}$ in K das Produkt von ℓ verschiedenen Primidealen in K.

In den beiden Fällen 2.) 3.) geht also $\mathfrak{l}$ nicht in der Relativdiskriminante auf.

c) Unabhängigkeit Kummerscher Körper

c) Unabhängigkeit mehrerer Kummerscher Körper.

Es sei $k(\sqrt[\ell]{\mu_1})$ ein Kummerscher Körper. Ein anderer $k(\sqrt[\ell]{\mu})$ ist, da er Primzahlrelativgrad ℓ hat, entweder mit $k(\sqrt[\ell]{\mu_1})$ identisch, oder der Durchschnitt beider Körper ist k.

Es sei $k(\sqrt[\ell]{\mu}) = k(\sqrt[\ell]{\mu_1})$. Dann läßt sich $\sqrt[\ell]{\mu}$ rational durch $\sqrt[\ell]{\mu_1}$ darstellen in der Form:

$$\sqrt[\ell]{\mu} = \varphi(\sqrt[\ell]{\mu_1}) = \gamma_0 + \gamma_1\sqrt[\ell]{\mu_1} + \gamma_2\sqrt[\ell]{\mu_1}^2 + \cdots + \gamma_{\ell-1}\sqrt[\ell]{\mu_1}^{\ell-1}\,.$$

Ersetzt man $\sqrt[\ell]{\mu_1}$ durch die konjugierte $\zeta\sqrt[\ell]{\mu_1}$, so geht auch $\sqrt[\ell]{\mu}$ in eine konjugierte, etwa $\zeta^k\sqrt[\ell]{\mu}$ über. Also ist

$$\begin{gathered}\zeta^k\sqrt[\ell]{\mu} = \varphi(\zeta\sqrt[\ell]{\mu_1}) \quad \text{oder}\\ \zeta^k\varphi(\sqrt[\ell]{\mu_1}) = \varphi(\zeta\sqrt[\ell]{\mu_1}).\\ \sum_{i=0}^{\ell-1}\zeta^k\gamma_i\sqrt[\ell]{\mu_1}^i = \sum_{i=0}^{\ell-1}\zeta^i\gamma_i\sqrt[\ell]{\mu_1}^i\end{gathered}$$

Der Eindeutigkeit wegen, und da ζ in k liegt, folgt also

$$\zeta^k\gamma_i = \zeta^i\gamma_i; \quad i = 0, 1, \ldots, \ell-1$$

d.h.
$$\gamma_i = 0 \text{ für } i \neq k$$

Es ist also $\sqrt[\ell]{\mu} = \varphi(\sqrt[\ell]{\mu_1}) = \gamma_k\sqrt[\ell]{\mu_1}^k$, d.h. $\sqrt[\ell]{\mu}$ im wesentlichen eine Potenz von $\sqrt[\ell]{\mu}$ mit zu ℓ primem Exponenten.

Dies läßt sich sofort verallgemeinern:

Es sei der Körper $k(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_\nu})$ vorgelegt. $k(\sqrt[\ell]{\mu})$ ist entweder ganz in ihm enthalten, oder hat mit ihm den Durchschnitt k. Im ersten Falle weisen

wir nach, daß dann

268 I

$$\sqrt[\ell]{\mu} = \alpha(\sqrt[\ell]{\mu_1})^{x_1} \cdots (\sqrt[\ell]{\mu_\nu})^{x_\nu}$$

ist, wo α in k liegt.

Für $\nu = 1$ ist dies in der Tat richtig. Unser Satz sei bis $\nu - 1$ bewiesen; □□□ ist $\sqrt[\ell]{\mu}$ schon in $k_1 = k(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_{\nu-1}})$ enthalten, so ist nach dieser Annahme unser Satz richtig. Sei also $\sqrt[\ell]{\mu}$ nicht in k_1 enthalten. Dann ist auch $\sqrt[\ell]{\mu_\nu}$ nicht in k_1 enthalten, da ja $\sqrt[\ell]{\mu}$ in $k_1(\sqrt[\ell]{\mu_\nu})$ vorkommen soll, der dann $= k_1$ wäre, sodaß $\sqrt[\ell]{\mu}$ doch in k_1 enthalten wäre. Nach Voraussetzung sind also $k_1(\sqrt[\ell]{\mu}) = k_1(\sqrt[\ell]{\mu_\nu})$ identische Kummersche Körper, da ja $\sqrt[\ell]{\mu}$ in $k_1(\sqrt[\ell]{\mu_\nu})$ enthalten, also der Durchschnitt von $k_1(\sqrt[\ell]{\mu})$ und $k_1(\sqrt[\ell]{\mu_1})$ jedenfalls nicht k_1 ist. Daher ist, weil unser Satz für $\nu = 1$ stimmt:

$$\sqrt[\ell]{\mu} = \alpha_1(\sqrt[\ell]{\mu_\nu})^{x_\nu},$$

wo α_1 Zahl aus k_1 ist. Es ist $\alpha_1 = \sqrt[\ell]{\frac{\mu}{\mu_\nu^{x_\nu}}}$. Daher muß nach Annahme

$$\alpha_1 = \sqrt[\ell]{\frac{\mu}{\mu^{x_\nu}}} = \alpha(\sqrt[\ell]{\mu_1})^{x_1} \ldots (\sqrt[\ell]{\mu_{\nu-1}})^{x_{\nu-1}}; \quad (\alpha \text{ in } k)$$

$$\sqrt[\ell]{\mu} = \alpha\sqrt[\ell]{\mu_1}^{x_1} \cdots \sqrt[\ell]{\mu_\nu}^{x_\nu} \qquad \text{w.z.b.w.}$$

Satz 7. Ist der Kummersche Körper $k(\sqrt[\ell]{\mu})$ enthalten im Körper $k(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_\nu})$, so ist

$$\sqrt[\ell]{\mu} = \alpha\sqrt[\ell]{\mu_1}^{x_1} \cdots \sqrt[\ell]{\mu_\nu}^{x_\nu}; \qquad (\alpha \text{ in } k)$$

und umgekehrt. Die x_i dürfen offenbar als Zahlen $0, \ldots, \ell - 1$ vorausgesetzt werden.

Definition 3. ν Kummersche Körper $k(\sqrt[\ell]{\mu_1}), \ldots, k(\sqrt[\ell]{\mu_1})$ heißen von einander unabhängig, wenn für jedes i der Körper $k(\sqrt[\ell]{\mu_i})$ teilerfremd ist zu dem aus den übrigen komponierten Körper $k(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_{i-1}}, \sqrt[\ell]{\mu_{i+1}}, \ldots, \sqrt[\ell]{\mu_\nu})$. Natürlich genügt die

269 I

Forderung, daß er nicht in ihm enthalten ist.

Satz 8. Für die Unabhängigkeit der ν Kummerschen Körper aus Definition 3 ist notwendig und hinreichend, daß im System der ℓ^ν Zahlen:

$$\mu_1^{x_1} \dots \mu_\nu^{x_\nu}; \qquad (0 \leqq x_i \leqq \ell - 1)$$

des Körpers k außer für $x_1, \dots, x_\nu = 0$ keine ℓ–te Potenz vorkommt.

Beweis. a.) Die Bedingung ist notwendig. Denn ist

$$\mu_1^{a_1} \dots \mu_\nu^{a_\nu} = \xi^\ell$$

und etwa $a_1 \neq 0$, ferner $a_1 a_1' \equiv 1 \bmod \ell$; dann ist

$$\mu_1 = \mu_2^{-a_2 a_1'} \dots \mu_\nu^{-a_\nu a_1'} \xi'^\ell$$
$$\sqrt[\ell]{\mu_1} = \xi' (\sqrt[\ell]{\mu_2})^{-a_2 a_1'} \dots (\sqrt[\ell]{\mu_\nu})^{-a_\nu a_1'}$$

also $k(\sqrt[\ell]{\mu_1})$ in $k(\sqrt[\ell]{\mu_2}, \dots, \sqrt[\ell]{\mu_\nu})$ enthalten.

b.) Die Bedingung ist hinreichend; denn ist etwa $k(\sqrt[\ell]{\mu_1})$ in $k(\sqrt[\ell]{\mu_2}, \dots, \sqrt[\ell]{\mu_\nu})$ enthalten, so folgt aus Satz 7:

$$\sqrt[\ell]{\mu_1} = \xi (\sqrt[\ell]{\mu_2})^{x_2} \cdots (\sqrt[\ell]{\mu_\nu})^{x_\nu}; \qquad (\xi \text{ in } k)$$

und daraus leicht eine Relation von der Form im Satze, bei der der Exponent von μ_1 nicht Null ist, w.z.b.w.

Sind die Körper unabhängig, so ist offenbar die Galoissche Gruppe von $k(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_\nu})$ folgende Abelsche Gruppe:

$$\sigma_1^{x_1} \dots \sigma_\nu^{x_\nu}; \qquad 0 \leqq x_i \leqq \ell - 1$$

vom Grade ℓ^ν, wo σ_i die Substitution $(\sqrt[\ell]{\mu_i} : \zeta \sqrt[\ell]{\mu_i})$ ist. Zunächst *sind* dies alles Substitutionen unseres Normalkörpers (das ist er ja, da ζ in k enthalten). Ferner sind sie kommutativ, da im allgemeinen Glied einer Zahl des Körpers:

$$A = \sum_{s, c_i} \alpha_s (\sqrt[\ell]{\mu_1})^{c_1} \dots (\sqrt[\ell]{\mu_\nu})^{c_\nu}; \qquad 0 \leqq c_i \leqq \ell - 1; \quad \alpha_s \text{ in } k$$

die aufeinanderfolgende Ausübung von $\sigma_1^{x_1} \dots \sigma_\nu^{x_\nu}$ und $\sigma_1^{y_1} \dots \sigma_\nu^{y_\nu}$ den Faktor:

$$\zeta^{c_1(x_1+y_1)+c_2(x_2+y_2)+\cdots+c_\nu(x_\nu+y_\nu)}$$

unabhängig von der Reihenfolge der beiden Substitutionen erzeugt. Es ist also nur nachzuweisen, daß alle diese ℓ^ν Substitutionen verschieden sind. Dies folgt aber einfach daraus, daß unser Körper ein Normalkörper ℓ^ν–ten Grades über k ist, da ja allgemein $k(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_{i+1}})$ vom ℓ–ten Relativgrade zu $k(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_i})$ ist, und der Gesamtrelativgrad ineinandergeschachtelter Körper das Produkt der Einzelrelativgrade ist. Daher hat auch die Galoissche Gruppe unseres Körpers den Grad ℓ^ν, und da keine anderen als die angegebenen ℓ^ν Substitutionen existieren, bilden diese die Galoissche Gruppe und sind alle verschieden.

Jedes Element der Gruppe gehört zum Exponenten ℓ. Jeder Unterkörper vom Grade ℓ von $K = k(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_\nu})$ gehört zu einer Untergruppe vom Index ℓ, die seine Galoissche Gruppe ist. Diese ist notwendig zyklisch, und da k die ℓ–te Einheitswurzel enthält, ist der Unterkörper ein Kummerscher Körper $k(\sqrt[\ell]{\mu})$ über k. Denn in bekannter Weise ist, wenn A eine prim[...] Zahl des fraglichen Unterkörpers ist, $\sigma A, \sigma^2 A, \dots, \sigma^{\ell-1} A$ ihre konjugierten, der Ausdruck (Lagrangesche Resolvente):

$$(\zeta, A) = A + \zeta\sigma A + \cdots + \zeta^{\ell-1}\sigma^{\ell-1} A,$$

dessen konjugierte sind:

$$(\zeta, \sigma A) = \sigma A + \zeta\sigma^2 A + \cdots + \zeta^{\ell-1} A = \zeta^{-1}(\zeta, A)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

so beschaffen, daß seine ℓ–te Potenz $(\zeta, A)^\ell = \mu$ in k ist. Es ist also $k(A) = k\big((\zeta, A)\big) = k(\sqrt[\ell]{\mu})$.

Die Anzahl der Unterkörper vom Grade ℓ ist demnach gleich der Anzahl der Untergruppen unserer Gruppe vom Grade ℓ^ν, die den Index ℓ haben, und diese ist nach Satz 3, S. 235 gleich $\frac{\ell^\nu - 1}{\ell - 1}$, da der

Rang unserer Gruppe offenbar ν ist. Also:

Satz 9. Sind die Kummerschen Körper $k(\sqrt[\ell]{\mu_1}), \dots, k(\sqrt[\ell]{\mu_\nu})$ unabhängig, so enthält der Körper $K = k(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_\nu})$ genau $\frac{\ell^\nu - 1}{\ell - 1}$ Kummersche Körper $k(\sqrt[\ell]{\mu})$, wo man offenbar $\mu = \mu_1^{x_1} \dots \mu_\nu^{x_\nu}$ setzen kann.

(Eine leichte Abzählung lehrt dann auch direkt, daß genau so viel verschiedene Körper $k(\sqrt[\ell]{\mu})$ herauskommen, was in Verbindung mit den ersten Sätzen dieses Abschnitts direkt zu Satz 9 führt).

Satz 10. Damit das zu $\mu_1, \mu_2, \ldots, \mu_\nu$ und ℓ prime Primideal $\mathfrak{p}$ aus k in K in lauter verschiedene Primideale ersten Relativgrades zerfällt, ist notwendig und hinreichend, daß $\left(\frac{\mu_1}{\mathfrak{p}}\right) = \cdots = \left(\frac{\mu_\nu}{\mathfrak{p}}\right) = 1$ ist.

Beweis. a.) Zerfällt $\mathfrak{p}$ in K in lauter verschiedene Primideale ersten Relativgrades, so gilt dasselbe für $k\sqrt[\ell]{\mu_i}$, da der Relativgrad für diesen Körper Teiler desjenigen für K sein muß, (Satz 13, S. 32▸), □□□ und $\mathfrak{p}$ in $k(\sqrt[\ell]{\mu_i})$ nicht in gleiche Primideale ersten Grades zerfallen kann, da $\mathfrak{p}$ prim zu μ_i und ℓ. Es ist also nach Satz 4 des vorigen Abschnittes $\left(\frac{\mu_i}{\mathfrak{p}}\right) = 1$ für alle i.

b.) Ist andererseits $\left(\frac{\mu_i}{\mathfrak{p}}\right) = +1$ für alle i, so zerfällt $\mathfrak{p}$ in allen $k(\sqrt[\ell]{\mu_i})$ nach Satz 4 in lauter verschiedene Primideale ersten Relativgrades. $\mathfrak{P}$ sei ein Primteiler von $\mathfrak{p}$ in K vom Relativgrade f, $\mathfrak{G}_Z$ seine Zerlegungsgruppe; □□□ zunächst kann $\mathfrak{P}$ höchstens zur 1. ten Potenz in $\mathfrak{p}$ aufgehen, da sonst die Relativdiskriminante von K durch $\mathfrak{p}$ teilbar wäre, während doch die Rel. Diskr. aller $k(\sqrt[\ell]{\mu_i})$ prim zu $\mathfrak{p}$ sind, was nach Satz 10, S. 20▸ unmöglich. Nach Definition 2, S. 23▸ hat also, wegen $e = 1$, die Gruppe $\mathfrak{G}_Z$

272 ı

den Grad f. Nach Satz 21, S. 50▸, angewendet auf $k(\sqrt[\ell]{\mu_i})$ ist, wegen $f' = 1$, □□□ $f = \overline{f}$ (Relativgrad von $\mathfrak{P}$ zu $k(\sqrt[\ell]{\mu_i})$), also die Gruppe $\overline{\mathfrak{G}}_Z$ (Zerlegungsgruppe von $\mathfrak{P}$ zu $k(\sqrt[\ell]{\mu_i})$) vom Grade $\overline{f} = f$; als Untergruppe zu $\mathfrak{G}_Z$ vom Grad $f = \overline{f}$ muß daher $\mathfrak{G}_Z = \overline{\mathfrak{G}}_Z$ sein. Weil es $\overline{\mathfrak{G}}_Z$ ist, ist somit auch $\mathfrak{G}_Z$ Untergruppe zur Gruppe $\overline{\mathfrak{G}}$, zu der $k(\sqrt[\ell]{\mu_i})$ als Unterkörper von K gehört, daher der Zerlegungskörper K_Z von [...] Oberkörper zu $k(\sqrt[\ell]{\mu_i})$. Da dies für alle i gilt, ist der Zerlegungskörper K_Z Oberkörper zu K selbst, also $K_Z = K$, d.h. $\mathfrak{G}_Z = 1$, somit $f = 1$, d.h. $\mathfrak{p}$ zerfällt in K in ℓ^ν Primideale (verschiedene) ersten Relativgrades, w.z.b.w.

Wir verwenden Satz 10 zum Beweis des Satzes:

Satz 11. Sind $\mu_1, \ldots, \mu_\nu$ Zahlen aus k, sodaß keine der Zahlen $\mu_1^{x_1} \ldots \mu_\nu^{x_\nu}$; $0 \leqq x_i \leqq \ell - 1$ eine ℓ–te Potenz in k ist, wenn nicht alle $x_i = 0$ sind, so gibt es unendlich viele Primideale ersten Grades in k, für die:

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) \neq 1; \quad \left(\frac{\mu_2}{\mathfrak{p}}\right) = \left(\frac{\mu_3}{\mathfrak{p}}\right) = \cdots = \left(\frac{\mu_\nu}{\mathfrak{p}}\right) = 1$$

ist.

Beweis. Wir betrachten den Körper $k_1 = k(\sqrt[\ell]{\mu_2}, \ldots, \sqrt[\ell]{\mu_\nu})$ und $k_2 = k_1(\sqrt[\ell]{\mu_1}) = k(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_\nu})$. Die Primideale ersten Grades in k, welche in k_1 in lauter verschiedene Primideale ersten Relativgrades zerfallen, bestehen aus 2 Arten:

1.) solche $\mathfrak{p}_1$, die in k_2 *nicht* in verschiedene
2.) " $\mathfrak{p}_2$, " " " doch " "

Primideale ersten Rel.Gr. zerfallen
" " " "

Von den endlich vielen Primidealen, die in k_1 in verschiedene Primideale ersten Rel.Gr. zerfallen, in k_2 jedoch gleiche Faktoren bekommen, dürfen wir absehen, ebenso von den endlich vielen zu ℓ nicht primen Primidealen.

273 I

Nach Satz 6, S. 141▸ angewendet auf k_1 und k_2 ist nun

$$\left.\begin{array}{rrcll} \displaystyle\sum_{\mathfrak{p}_1} \frac{1}{\mathsf{N}(\mathfrak{p}_1)^s} + \sum_{\mathfrak{p}_2} \frac{1}{\mathsf{N}(\mathfrak{p}_2)^s} & = & \frac{1}{\ell^{\nu-1}} \log \frac{1}{s-1} & +\psi_1(s) & \\ \displaystyle\sum_{\mathfrak{p}_2} \frac{1}{\mathsf{N}(\mathfrak{p}_2)^s} & = & \frac{1}{\ell^{\nu}} \log \frac{1}{s-1} & +\psi_2(s) & \\ \text{Also:} \quad \displaystyle\sum_{\mathfrak{p}_1} \frac{1}{\mathsf{N}(\mathfrak{p}_1)^s} & = & \frac{\ell-1}{\ell^{\nu}} \log \frac{1}{s-1} & +\psi_3(s) & \end{array}\right\} \quad \begin{array}{l} \psi_1, \psi_2, \psi_3 \\ \text{für } s \to 1 \\ \text{endlich.} \end{array}$$

Für $s \to 1$ erkennt man, daß die Primideale $\mathfrak{p}_1$ in unendlicher Anzahl vorhanden sind. Auf Grund von Satz 10 angewendet auf k_2 und k_1 haben aber diese Primideale gerade die verlangte Eigenschaft.

1.8 Existenz des Klassenkörpers.

274 ı

a) Existenz bei Primzahlgrad ℓ mit ℓ–ter E.W.

a.) Existenz des Klassenkörpers vom Primzahlrelativgrad ℓ, wenn der Grundkörper k eine ℓ–te Einheitswurzel enthält.

Es enthalte k die ℓ–te Einheitswurzel ζ, was für $\ell = 2$ stets der Fall. Wie schon S. 254 gezeigt wurde, ist dann für jedes zu ℓ prime $\mathfrak{p}$:

$$\Phi(\mathfrak{p}) = \mathsf{N}(\mathfrak{p}) - 1 \equiv 0 \mod \ell$$

Es sei ein Ideal $\mathfrak{m}$ als Modul vorgelegt. In $\mathfrak{m}$ mögen aufgehen:

1.) d verschiedene zu ℓ prime Primideale $\mathfrak{p}$ in irgendeiner Potenz [...],

2.) d' verschiedene Teiler $\mathfrak{l}$ von ℓ, wo $\ell \sim \mathfrak{l}^{\tau(\ell-1)}$, in [...] Potenz $g \geqq \tau\ell+1$. $[s = \tau(\ell-1)]$

3.) Eventuell eine Anzahl (auf die es nicht ankommt) von Teilern $\mathfrak{l}_1$ von $\ell \sim \mathfrak{l}_1^{\tau_1(\ell-1)}$ in einer niedrigeren als der $(\tau_1\ell+1)$ ten Potenz $\mathfrak{l}^{g_1}$; $(g_1 \leqq \tau_1\ell)$ $[s_1 = \tau_1(\ell-1)]$

Die eventuell noch übrigen, nicht in $\mathfrak{m}$ aufgehenden Teiler seien $\mathfrak{l}'$ von $\ell \sim \mathfrak{l}'^{\tau'(\ell-1)}$; $\big(s' = \tau'(\ell-1)\big)$.*)

Nach Satz 5, S. 237 ist dann:

$$R(\mathfrak{m}) = \sum_{\mathfrak{p}} R(\mathfrak{p}^{\nu}) + \sum_{\mathfrak{l}} R(\mathfrak{l}^{g}) + \sum_{\mathfrak{l}_1} R(\mathfrak{l}_1^{g_1})$$

Nach Satz 6, 7, S. 238 also:

$$R(\mathfrak{m}) = d + d' + \sum sf + \sum \left[g_1 - \frac{g_1}{\ell}\right] f_1$$

wenn f, f_1 die Grade der Primideale $\mathfrak{l}, \mathfrak{l}_1$ sind.

*) τ, τ_1, τ' entsprechen dem früheren s_0.

Im Falle $\ell = 2$ möge unter den r_1 reellen konjugierten Körpern eine beliebige Anzahl, etwa $k_1, \ldots, k_\nu$ ausgewählt sein,

275 I

wo auch $\nu = 0$ zugelassen ist.

Im Falle $\ell > 2$ sei nun o der Strahl der Zahlen $\equiv 1 \bmod \mathfrak{m}$, im Falle $\ell = 2$ seien die Zahlen des Strahles o außerdem noch der Vorzeichenbedingung unterworfen, daß sie in $k_1, \ldots, k_\nu$ positiv sind. Dies bedeutet eine Vorzeichengruppe V vom Grade $2^{r_1-\nu}$ (da die Vorzeichen in $r_1 - \nu$ Körpern willkürlich sind), der die Vorzeichenkombinationen von den Zahlen aus o angehören sollen.

Die Idealklassen von k seien nun nach o definiert. Der Rang $\bar{t}$ der Gruppe der Idealklassen ist dann nach Satz 8, 9, S. 249▸/253▸ wegen $\delta = 1$; $r_0 = r_1 - \nu$:

$$\begin{aligned} \bar{t} &= R(\mathfrak{m}) + n - (r+1) \quad ; \text{ für } \ell > 2, \\ \bar{t} &= R(\mathfrak{m}) + n_0 + \nu - (r+1) \quad ; \text{ ‖ } \ell = 2. \end{aligned}$$

Dabei ist ℓ^n bezw. 2^{n_0} die Anzahl der ℓ–ten Potenzreste, ev. mit der Vorzeichenbedingung V für $k_1, \ldots, k_\nu$, die in dem System

$$(1) \qquad \varepsilon_1^{x_1} \ldots \varepsilon_{r+1}^{x_{r+1}} \varrho_1^{y_1} \ldots \varrho_t^{y_t}; \qquad (0 \leqq x_i, y_i \leqq \ell - 1)$$

enthalten sind. Dabei haben die ε_i und ϱ_i die frühere Bedeutung (S. 245▸). Die Ideale $\mathfrak{r}_i$, aus den die $(\varrho_i) = \mathfrak{r}_i^{\ell^{\nu_i}}$ entstehen seien untereinander, und □□□ zu ℓ und den $\mathfrak{p}$, somit auch zu $\mathfrak{m}$ prim, was offenbar angenommen werden darf, (da in jeder Idealklasse zu einem beliebigen Ideal prime Ideale vorkommen).

Im Falle $\ell = 2$ wollen wir von jetzt ab n statt n_0 schreiben.

Setzt man für $R(\mathfrak{m})$ den oben angegebenen Wert ein, so wird dann:

276 I

$$(2) \qquad \bar{t} = d + d' + \sum sf + \sum \left[g_1 - \frac{g_1}{\ell} \right] f_1 + n - (r+1) \quad \text{für} \quad \ell > 2$$

$$(3) \qquad \bar{t} = d + d' + \sum sf + \sum \left[g_1 - \frac{g_1}{\ell} \right] f_1 + n + \nu - (r+1) \quad \text{‖} \quad \ell > 2$$

Die Anzahl der Klassengruppen vom Index ℓ berechnet sich dann nach Satz 3, S. 235▸ zu $\frac{\ell^{\bar{t}}-1}{\ell-1}$.

Die Rangbasis der Untergruppe vom Rang ℓ^n der Gruppe

$$\varepsilon_1^{x_1} \dots \varepsilon_{r+1}^{x_{r+1}} \varrho_1^{y_1} \dots \varrho_t^{y_t} \xi^\ell; \qquad 0 \leqq x_i, y_i \leqq \ell - 1, \tag{4}$$

bestehend aus den ℓ–ten Potenzresten mod $\mathfrak{m}$ von (4), ev. mit Vorzeichenbedingung V, sei $\alpha_1, \dots, \alpha_n$, sodaß diese Untergruppe wird:

$$\alpha_1^{x_1} \dots \alpha_n^{x_n} \xi^\ell; \qquad (0 \leqq x_i \leqq \ell - 1),$$

und keine Zahl dieser Art ℓ–te Potenz in k ist, wenn nicht alle $x_i = 0$ sind.

Daher gibt es nach Satz 11, S. 272 sicher unendlich viele Systeme von je n Primidealen $\mathfrak{q}_i$ aus k, sodaß

$$\left(\frac{\alpha_1}{\mathfrak{q}_i}\right) = 1, \dots, \left(\frac{\alpha_{i-1}}{\mathfrak{q}_i}\right) = 1, \left(\frac{\alpha_{i+1}}{\mathfrak{q}_i}\right) = 1, \dots, \left(\frac{\alpha_n}{\mathfrak{q}_i}\right) = 1$$

aber

$$\left(\frac{\alpha_i}{\mathfrak{q}_i}\right) \neq 1$$

wird, für $i = 1, 2, \dots, n$.

Wir können also diese $\mathfrak{q}_i$ auch so bestimmen, daß sie sämtlich prim zu ℓ, $\mathfrak{m}$, und den $\mathfrak{r}_i$ sind.

Nach dem Modul $\overline{\mathfrak{m}} = \mathfrak{m}\mathfrak{q}_1 \dots \mathfrak{q}_n$ ist dann im System (1) nur der eine einzige ℓ–te Potenzrest 1 enthalten, wenn für $\ell = 2$ noch die Vorzeichenbedingung

277 [1]

V gefordert wird. In der Tat müßte ein solcher zunächst ℓ–ter Potenzrest mit Signatur aus V nach dem Modul $\mathfrak{m}$ sein, also von der Form $\alpha_1^{x_1} \dots \alpha_n^{x_n} \xi^\ell$, wo ξ zu den $\mathfrak{q}_i$ prim, weil es die ϱ_i und α_i sind. Ist etwa $x_1 \neq 0$, so ist dies aber kein ℓ–ter Potenzrest nach $\mathfrak{q}_1$, da es $\alpha_2, \dots, \alpha_n$ sind, nicht aber α_1. Also müssen alle $x_i = 0$ sein, und daher in (1) $x_i, y_i = 0$, der vorgelegte Rest also als Zahl aus dem System (1) gleich 1.

Werden nun die Idealklassen in der gleichen Weise nach dem Modul $\overline{\mathfrak{m}}$ definiert, also nach dem Strahl

$$\begin{aligned} &\equiv 1 \bmod \overline{\mathfrak{m}}, \quad \text{für} \quad \ell > 2 \\ &\equiv 1 \bmod \overline{\mathfrak{m}}, \quad \text{Signatur aus } V, \text{ für} \quad \ell = 2 \end{aligned}$$

so ist zunächst zu beachten, daß die zugehörigen Ideale $\bar{\mathfrak{r}}_i$ sicher aus unserem ursprünglichen System $\mathfrak{r}_i$ genommen werden dürfen. Denn die $\mathfrak{r}_i$ waren

(S. 244) so gewählt, daß sie Elemente aus den Basisklassen derjenigen absoluten Klassengruppe $\mathfrak{G}$ waren, in deren Klassen Ideale vorkommen, die in Bezug auf den Strahl $\equiv 1 \bmod \mathfrak{m}$ zu einem Exponenten ℓ^κ gehören. Die entsprechende Klassengruppe $\overline{\mathfrak{G}}$ für den Modul $\overline{\mathfrak{m}}$ ist nun ersichtlich Untergruppe zu $\mathfrak{G}$. Denn ist $\mathfrak{a}^{\ell^{\overline{\kappa}}} = (\alpha)$, wo $\alpha \equiv 1 \bmod \overline{\mathfrak{m}}$, □□□ so ist auch $\alpha \equiv 1 \bmod \mathfrak{m}$ und folglich der Exponent, zu dem $\mathfrak{a}$ in Bezug auf den Strahl $\equiv 1 \bmod \mathfrak{m}$ gehört, ein Teiler von $\ell^{\overline{\kappa}}$, also auch eine Potenz von ℓ, d.h. $\mathfrak{a}$ gehört auch zu $\mathfrak{G}$. Also können die neuen $\overline{\mathfrak{r}}_i$ als Produkte der alten $\mathfrak{r}_i$ gewählt

278 I

werden, □□□ die Exponenten, zu denen sie absolut gehören sind wieder Potenzen von ℓ und die neuen $\overline{\varrho}_i$ werden die entsprechenden Produkte der ϱ_i. Daraus ergibt sich, daß auch für das aus ihnen gebildete System (1) keine Zahl außer 1 ℓ–ter Potenzrest nach $\overline{\mathfrak{m}}$ ist, (für $\ell = 2$ mit Vorzeichenbedingung V).

Wird also $\overline{\mathfrak{m}}$ als neuer Modul eingeführt, so ist in (2) und (3) für n der Wert 0 zu setzen, dafür aber d zu ersetzen durch $d + n$, da gerade n neue Primideale $\mathfrak{q}_i$ der Sorte 1.) S. 274 hinzugekommen sind. Alles andere in (2) und (3) bleibt. Der Rang der Gruppe der Idealklassen nach dem Modul $\overline{\mathfrak{m}}$ und entspr. Strahl o und somit die Anzahl der Klassengruppen vom Index ℓ ist die gleiche, wie vorher.

Da nun sicher jede Klassengruppe nach $\mathfrak{m}$ auch Klassengruppe nach $\overline{\mathfrak{m}}$ vom selben Index ist, sind die Klassengruppen vom Index ℓ für $\mathfrak{m}$ und $\overline{\mathfrak{m}}$ identisch.

Bezeichnen wir vorübergehend mit $\overline{\mathfrak{p}}$ eines der Primideale $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ und seine absolute Klasse mit $\mathfrak{K}$. Der Zerlegung $G = G_0 D$ (S. 244) entsprechend setzen wir

$$\mathfrak{K}^{-1} = \mathfrak{K}_0 \mathfrak{K}_D = \mathfrak{K}_0 \mathfrak{K}_1^\ell$$

da der Exponent von $\mathfrak{K}_D$ zu ℓ prim ist. Bis auf ein absolutes Hauptideal als Faktor lassen sich die Ideale aus $\mathfrak{K}_0$ in die Form bringen $\mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t}$. In $\mathfrak{K}_1$ liege das zu $\mathfrak{m}, \mathfrak{q}_i, \ell$ und $\mathfrak{r}_i$ prime Ideal $\mathfrak{j}$. Dann ist also

$$\overline{\mathfrak{p}} \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} \mathfrak{j}^\ell$$

ein absolutes Hauptideal, welches prim ist, zu jedem der übrigen Ideale $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ und auch zu den $\mathfrak{l}_1$ und [...].

279 I

Auf diese Art erhalten wir:

$$(\omega) = \mathfrak{p}\mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t}\mathfrak{j}^{\ell} \quad : \quad d \text{ Zahlen } \omega \tag{5}$$

$$(\lambda) = \mathfrak{l}\mathfrak{r}_1^{b_1} \dots \mathfrak{r}_t^{b_t}\mathfrak{j}'^{\ell} \quad : \quad d' \text{ Zahlen } \lambda \tag{6}$$

$$(\kappa) = \mathfrak{q}\mathfrak{r}_1^{c_1} \dots \mathfrak{r}_t^{c_t}\mathfrak{j}''^{\ell} \quad : \quad n \text{ Zahlen } \kappa. \tag{7}$$

Nunmehr betrachten wir die $\ell^{r+1+t+d+d'+n}$ Zahlen:

$$\varepsilon_1^{x_1} \dots \varepsilon_{r+1}^{x_{r+1}} \varrho_1^{y_1} \dots \varrho_t^{y_t} \omega_1^{u_1} \dots \omega_d^{u_d} \lambda_1^{v_1} \dots \lambda_{d'}^{v_{d'}} \kappa_1^{w_1} \dots \kappa_n^{w_n} \tag{8}$$

wo $0 \leqq x_i, y_i, u_i, v_i, w_i \leqq \ell - 1$.

Soll eine Zahl (8) ℓ–te Potenz einer Zahl aus k sein, so müssen die Primideale $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ in ℓ–ten Potenzen in ihr enthalten sein; da diese in (5),(6),(7) je einmal vorkommen, müssen alle $u_i, v_i, w_i = 0$ sein. Es bleibt also eine Zahl des Systems (1) übrig, die aber wie von früher bekannt (S. 245▸), nur ℓ–te Potenz sein kann, wenn $x_i, y_i = 0$ sind.

Die Gruppe aller Zahlen (8) mit unbeschränkten Exponenten hat also den Rang

$$r + 1 + t + d + d' + n \tag{9}$$

und jede ihrer Zahlen ist eindeutig darstellbar in der Form:

$$\varepsilon_1^{x_1} \dots \varepsilon_{r+1}^{x_{r+1}} \varrho_1^{y_1} \dots \varrho_t^{y_t} \omega_1^{\overline{u}_1} \dots \omega_d^{\overline{u}_d} \lambda_1^{v_1} \dots \lambda_{d'}^{v_{d'}} \kappa_1^{w_1} \dots \kappa_n^{w_n} \xi^{\ell} \tag{10}$$

wo ξ wieder eine Zahl unserer[1] Gruppe ist und alle Exponenten zwischen 0 u. $\ell - 1$ liegen.

Aus dieser Gruppe werde jetzt eine Untergruppe ausgewählt durch folgende Bedingungen:

[1] undeutlich

1.) *Jedes Ideal $\mathfrak{r}_i$ soll mit einem durch ℓ teilbaren Exponenten in (10) aufgehen.* Da die Ideale $\mathfrak{r}_i$ prim zu allen anderen vorkommenden sind, besagt diese Forderung nach (5),(6),(7) und da sie in den ϱ_i ja sowieso mit durch ℓ teilbarem Exponenten aufgehen, daß die x_i, y_i, u_i, v_i, w_i folgenden Kongruenzen genügen sollen:

$$\sum_{i=1}^{d} a_k u_i + \sum_{i=1}^{d'} b_k v_i + \sum_{i=1}^{n} c_k w_i \equiv 0 \mod \ell.$$

für $k = 1, 2, \ldots, t.$

Es sind dies t Bedingungskongruenzen mod ℓ.

2.) *Die Zahlen der Untergruppe von (10) sollen ℓ–te Potenzreste nach der $\tau'\ell$–ten Potenz von $\mathfrak{l}'$ für jedes $\mathfrak{l}'$ sein.*

Der Rang $R(\mathfrak{l}'^{\tau'\ell})$ ist nach Satz 7, S. 238 gleich $\left[\tau'\ell - \frac{\tau'\ell}{\ell}\right] f' = s'f'$. Es gibt also $s'f'$ unabhängige Nichtreste nach $\mathfrak{l}'^{\tau'\ell}$, etwa $\gamma_1, \ldots, \gamma_{s'f'}$. Ist nun

$$\left.\begin{array}{rcll}
\varepsilon_1 & \equiv & \gamma_1^{e_1} \cdots \gamma_{s'f'}^{e_{s'f'}} & \alpha^\ell \\
\cdots\cdots & & \cdots\cdots & \cdots\cdots \\
\varrho_1 & \equiv & \gamma_1^{r_1} \cdots \gamma_{s'f'}^{r_{s'f'}} & \beta^\ell \\
\cdots\cdots & & \cdots\cdots & \cdots\cdots \\
\omega_1 & \equiv & \gamma_1^{p_1} \cdots \gamma_{s'f'}^{p_{s'f'}} & \gamma^\ell \\
\cdots\cdots & & \cdots\cdots & \cdots\cdots \\
\lambda_1 & \equiv & \gamma_1^{\ell_1} \cdots \gamma_{s'f'}^{\ell_{s'f'}} & \delta^\ell \\
\cdots\cdots & & \cdots\cdots & \cdots\cdots \\
\kappa_1 & \equiv & \gamma_1^{k_1} \cdots \gamma_{s'f'}^{k_{s'f'}} & \varepsilon^\ell
\end{array}\right\} \mod \mathfrak{l}'^{\tau'\ell}$$

so ist nach der Bedeutung der unabhängigen Nichtreste unsere Einschränkung 2.) gleichwertig mit den Kongruenzen:

$$\sum_{i=1}^{r+1} e_k^{(i)} x_i + \sum_{i=1}^{t} r_k^{(i)} y_i + \sum_{i=1}^{d} p_k^{(i)} u_i + \sum_{i=1}^{d'} \ell_k^{(i)} v_i + \sum_{i=1}^{n} \mathfrak{k}_k^{(i)} w_i \equiv 0 \mod \ell$$

$$k = 1, 2, \ldots, s'f',$$

also mit $s'f'$ Bedingungskongruenzen. Im Ganzen also behalten wir $\sum s'f'$ Bedingungskongruenzen.

3.) *Für jedes* $\mathfrak{l}_1$ *sollen die Zahlen unserer Untergruppe* ℓ*–te Potenzreste nach* $\mathfrak{l}_1^{\tau_1\ell+1-g_1}$ *sein.*

Wie eben ergibt sich hier, da der Rang $R(\mathfrak{l}_1^{\tau_1\ell+1-g_1})$ gleich

$$\left[\tau_1\ell + 1 - g_1 - \frac{\tau_1\ell + 1 - g_1}{\ell}\right] f_1$$

ist, daß hierzu

$$\sum R\left(\mathfrak{l}_1^{\tau_1\ell+1-g_1}\right) = \sum\left[\tau_1\ell + 1 - g_1 - \tau_1 + \frac{g_1 - 1}{\ell}\right] f_1$$

Bedingungskongruenzen bestehen müssen.

4.) *Für die von* $\mathfrak{k}_1, \ldots, \mathfrak{k}_\nu$ *verschiedenen, reellen konjugierten Körper sollen im Falle* $\ell = 2$ *die betreffenden konjugierten unserer Untergruppe positiv sein.*

Da in diesen Körpern alle Zahlen reell sind, bedeutet dies, daß für jeden der Körper gewisse Kongruenzen mod 2 bestehen müssen, in denen jene der Exponenten x_i, y_i, u_i, v_i, w_i auftreten, für die das zugehörige $\varepsilon_i, \varrho_i, \omega_i, \lambda_i, \kappa_i$ negativ in dem betr. Körper ist. (Da für diese Körper die höchste 2^ν–te Einheitswurzel ε_{r+1} sicher $= -1$ also total negativ ist, ist keine dieser Kongruenzen identisch erfüllt. Es sind im ganzen $r_1 - \nu$ Bedingungskongruenzen).

Diese 4 Bedingungskongruenzen definieren ersichtlich eine Untergruppe der Zahlen (10), in der jede ℓ–te Potenz ξ^ℓ jedes in Frage kommenden ξ enthalten ist. Im Ganzen sind zur Definition dieser Untergruppe

282 ı

benutzt:

$$\begin{array}{lll} t_0 = t + \sum s'f' + \sum \left[\tau_1\ell + 1 - g_1 - \tau_1 + \frac{g_1-1}{\ell}\right] f_1 & \text{für} & \ell > 2 \\ t_0 = t + \sum s'f' + \sum \left[\tau_1\ell + 1 - g_i - \tau_1 + \frac{g_1-1}{\ell}\right] f_1 + (r_1 - \nu) & \text{für} & \ell = 2 \end{array}$$

Bedingungskongruenzen. Dann bleiben, da der Rang unserer Gruppe (10) $r + 1 + d + d' + n + t$ ist, noch mindestens $r + 1 + d + d' + n + t - t_0$

unserer Exponenten in der Darstellung (10) frei, wenn man, was auf Grund der Bedingungskongruenzen das höchstmögliche ist, t_0 Exponenten durch die übrigen ausdrückt.

Wenn also t' der Rang der soeben definierten Untergruppe ist, und ihre Darstellung etwa:

$$(11) \qquad \mu_1^{x_1} \dots \mu_{t'}^{x_{t'}} \xi^{\ell}; \qquad 0 \leqq x_i \leqq \ell - 1; \qquad \xi \text{ Zahl aus (10)}$$

sodaß (11) nur dann eine ℓ–te Potenz ist*), wenn alle $x_i = 0$ sind, so ist:

$$t' \geqq r + 1 + d + d' + n + t - t_0$$

Für $\ell > 2$ ist also nach (2):

$$t' - \bar{t} \geqq 2(r+1) - \Big\{ \sum sf + \sum s'f' + \sum \Big([\tau_1 \ell + 1 - g_1 + \\ + \frac{g_1 - 1}{\ell}] + [g_1 - \frac{g_1}{\ell}] \Big) f_1 \Big\}$$

während für $\ell = 2$ nach (3) rechts noch $-r_1$ hinzukommt.

Nun ist:

$$\Big[\tau_1 \ell + 1 - g_1 - \tau_1 + \frac{g_1 - 1}{\ell}\Big] = \tau_1 \ell + 1 - g_1 - \tau_1 + i + \\ + \begin{cases} 0 & \text{wenn} \quad g_1 = i\ell + \varrho; \quad \varrho > 0 \\ -1 & \text{"} \quad\ \ g_1 = i\ell \end{cases}$$

$$\Big[g_1 - \frac{g_1}{\ell}\Big] = g_1 - i + \begin{cases} -1 & \text{wenn} \quad g_1 = i\ell + \varrho; \quad \varrho > 0 \\ 0 & \text{"} \quad\ \ g_1 = i\ell \end{cases}$$

Also die Summe beider Ausdrücke: $\tau_1 \ell - \tau_1 = \tau_1(\ell - 1) = s_1$

Damit wird

$$t' - \bar{t} \geqq 2(r+1) - \{ \sum sf + \sum s'f' + \sum s_1 f_1 \}.$$

*) ℓ–te Potenz *in k*.

Die geschweifte Klammer ist nun $\sum sf$ über *alle* Teiler von ℓ, was bekanntlich den Körpergrad m gibt. Da ζ in k enthalten, ist für $\ell > 2$ k total imaginär, also $r = r_2 - 1$, $m = 2r_2 = 2(r+1)$. Daraus folgt:

$$t' \geqq \bar{t}$$

Für $\ell = 2$ folgt:

$$t' - \bar{t} \geqq 2(r+1) - r_1 - m$$

Nun ist $m = r_1 + 2r_2 = 2r_1 + 2r_2 - r_1 = 2(r+1) - r_1$, sodaß auch hier folgt: $t' \geqq \bar{t}$. Es gilt also stets:

$$t' \geqq \bar{t} \qquad \text{(also insbesondere } \geqq 0) \tag{12}$$

Nach dem über das System (11) Gesagten sind die t' Kummerschen Körper $k(\sqrt[\ell]{\mu_1}), \ldots, k(\sqrt[\ell]{\mu_{t'}})$ von einander unabhängig. In $K = k(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_{t'}})$ sind also $\frac{\ell^{t'}-1}{\ell-1}$ Kummersche Körper $k(\sqrt[\ell]{\mu})$ enthalten, wo μ sich in die Form

$$\mu = \mu_1^{x_1} \ldots \mu_{t'}^{x_{t'}}; \qquad 0 \leqq x_i \leqq \ell - 1 \tag{13}$$

setzen läßt. Wegen (12) erhält man also mindestens $\frac{\ell^{\bar{t}}-1}{\ell-1}$ verschiedene Körper dieser Art.

Wir haben zunächst die Relativdiskriminante von $k(\sqrt[\ell]{\mu})$ zu untersuchen. μ genügt unseren 3 bezw. 4 Bedingungen S. 280▸/281▸.

Wegen der ersten geht jedes Ideal $\mathfrak{r}_i$ in μ mit durch ℓ teilbarem Exponenten auf, also nicht in der Relativdiskriminante.

Nach Konstruktion (Zahl aus (10)) ist μ (bis auf ℓ–te Potenzen, die nichts ausmachen) durch kein von den $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{l}$ verschiedenes Primideal teilbar. Von den in ℓ nicht aufgehenden Primidealen von k können also nur die $\mathfrak{p}$ und $\mathfrak{q}$ in der Relativdiskriminante aufgehen, und dann nach Satz 5, S. 266▸ genau in der $(\ell-1)$ten Potenz.

Da μ ℓ–ter Potenzrest nach $\mathfrak{l}'^{\tau'\ell}$ ist (Bedingung 2.)) geht das Primideal $\mathfrak{l}'$ nicht in der Relativdiskriminante auf (Satz 6, S. 266▸).

Ist also die Relativdiskriminante $f^{\ell-1}$, so gehen in f höchstens die Primideale auf, die in $\overline{\mathfrak{m}}$ aufgehen, und zwar hat f die Form:

$$f = \prod{}' \mathfrak{p} \prod{}' \mathfrak{q} \prod{}' \mathfrak{l}^{\nu+1} \prod{}' \mathfrak{l}_1^{\nu_1+1}$$

wo die Akzente andeuten, daß man nicht über alle Primideale der betreffenden Art das Produkt notwendig zu erstrecken hat.

Nun ist $v \leqq \frac{s\ell}{\ell-1} = \tau\ell$ (Satz 2, S. 149▸). Nach Voraussetzung geht $\mathfrak{l}$ in $\mathfrak{m}$ mindestens zur $(\tau\ell+1)$–ten Potenz auf. Ferner ist μ ℓ–ter Potenzrest nach $\mathfrak{l}_1^{\tau_1\ell+1-g_1}$. Nach Satz 6 (S. 266▸) ist also $v_1 \leqq \tau_1\ell - (\tau_1\ell + 1 - g_1) = g_1 - 1$, $\mathfrak{l}_1$ geht also in f höchstens zur □□□ Potenz g_1 auf, in $\mathfrak{m}$ jedoch genau zu dieser.

Sicher ist also $\overline{\mathfrak{m}}$ teilbar durch f. Nach Satz 22, S. 202▸ und Satz 27, S. 206▸ (μ kann nach Bedingung 4.) nur in $k_1, \ldots, k_\nu$ negativ werden; für $\ell = 2$) ist also $k(\sqrt[\ell]{\mu})$

285 I

ein Klassenkörper für eine Klassengruppe H vom Index ℓ nach dem Modul $\overline{\mathfrak{m}}$ und unserem erklärten Strahl. Da es nun mindestens $\frac{\ell^{\bar{t}}-1}{\ell-1}$ verschiedene solche Körper gibt, andererseits genau soviel, nämlich $\frac{\ell^{\bar{t}}-1}{\ell-1}$ Klassengruppen vom Index ℓ vorhanden sind, da ferner nach Satz 10, S. 147 zu jeder Klassengruppe höchstens ein Klassenkörper gehört, ist jeder der $\frac{\ell^{\bar{t}}-1}{\ell-1}$ Klassengruppen vom Index ℓ auf diese Art genau ein Klassenkörper zugeordnet. Es folgt daher beiläufig noch $t' = \bar{t}$.

Damit ist auch jeder Klassengruppe vom Index ℓ nach $\mathfrak{m}$ eindeutig ein Klassenkörper zugeordnet, da ja nach S. 278 die Klassengruppen vom Index ℓ nach $\mathfrak{m}$ und $\overline{\mathfrak{m}}$ identisch sind.

Wir weisen noch nach, daß die $\mathfrak{q}_i$ in der Relativdiskriminante nicht aufgehen.

In der Tat, gingen sie in einer der möglichen Relativdiskriminanten auf, so könnten wir, da uns unendlich viele solche Primideale zur Verfügung stehen, ein vollständig anderes System von $\mathfrak{q}_i$ wählen. In den damit konstruierten Klassenkörpern nach $\mathfrak{m}$ gehen nun die alten $\mathfrak{q}_i$ sicher nicht in den Relativdiskriminanten auf. Da es aber nur einen Klassenkörper zu jeder Klassengruppe gibt, müssen die neugewonnenen Klassenkörper mit den alten identisch sein, d.h. die $\mathfrak{q}_i$ können nicht in den Relativdiskriminanten aufgehen. Es ist also schon $\mathfrak{m}$ teilbar durch f.

286 I

Die Einteilung der Hilfsprimideale $\mathfrak{q}_i$ hatte den Zweck, die notwendige Anzahl von Körpern zu erreichen. Wie man sich leicht überzeugt, wäre dies mit einfacheren Mitteln auf unserem Wege nicht zu erreichen gewesen.

Da für $\ell = 2$ μ in den von $k_1, \ldots, k_\nu$ verschiedenen Körpern positiv ist, sind den zu $k(\sqrt{\mu})$ konjugierten Körper $k_{\nu+1}(\sqrt{\mu}), \ldots, k_{r_1}(\sqrt{\mu})$ sicher reell. Da jedem dieser Körper 2 konjugierte darstellt, gibt es also wenigstens $2(r_1 - \nu)$ reelle konjugierte Körper.

Satz 1. Für jede Klassengruppe vom Primzahlindex ℓ nach dem Modul $\mathfrak{m}$ existiert, wenn k die ℓ–te Einheitswurzel ζ enthält, ein Klassenkörper und zwar ein Kummerscher Körper $k(\sqrt[\ell]{\mu})$. Ist $f^{\ell-1}$ die Relativdiskriminante desselben, so ist überdies $\mathfrak{m}$ teilbar durch f.

Für $\ell = 2$ gilt genauer:

Satz 2. Wenn von den r_1 reellen konjugierten zu k irgend ν Körper ausgewählt werden und der Strahl o aus den in jenen ν Körpern positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$ besteht, so sind von den zu $k(\sqrt{\mu})$ konjugierten Körpern mindestens $2(r_1 - \nu)$ reell, wenn $k(\sqrt{\mu})$ Klassenkörper einer Klassengruppe vom Index 2 nach dem Strahl o ist. Ist also $\nu = 0$, d.h. o der reelle Strahl $\equiv 1 \bmod \mathfrak{m}$, so sind für jeden Klassenkörper einer Klassengruppe vom Index 2 nach o mindestens $2r_1$, also genau $2r_1$ konjugierte reell.

Da man für $\nu = r_1$ [...] Strahl o aller total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$ erhält, ist der Existenznachweis des Klassenkörpers auch für jede mögliche Klassengruppe vom Index 2 mod $\mathfrak{m}$ erbracht.

b) Existenz bei Primzahlgrad ℓ ohne ℓ–te E.W.

b.) Klassenkörper vom Primzahlgrad ℓ, wenn der Grundkörper die ℓ–te Einheitswurzel nicht enthält.

Im Falle eines ungeraden ℓ müssen wir uns noch von der Voraussetzung befreien, daß der Körper k die ℓ–te Einheitswurzel enthält. Das Ziel dieses Abschnittes ist der Nachweis des Satzes:

Satz 3. Ist k irgend ein Grundkörper, H eine Klassengruppe vom Primzahlindex ℓ nach irgendeinem Modul $\mathfrak{m}$, so existiert ein Klassenkörper für H, der relativ–zyklisch vom Grade ℓ ist. Ist $f^{\ell-1}$ seine Relativdiskriminante, so ist $\mathfrak{m}$ teilbar durch f.

Zunächst zeigen wir:

Hilfssatz. Ist K relativ Galoissch aber nicht relativ zyklisch in Bezug auf k, so gibt es in k kein Primideal, das in K unzerlegt bleibt.

Beweis. Bliebe $\mathfrak{p}$ unzerlegt in K, so geht es zunächst nicht in der Relativdiskriminante auf. Seine Trägheitsgruppe ist also die identische; die Zerlegungsgruppe ist ferner die ganze Gruppe, da jedes $\sigma\mathfrak{P} = \mathfrak{P} = \mathfrak{p}$ ist. Da allgemein $\frac{\mathfrak{G}_Z}{\mathfrak{G}_T}$ zyklisch vom Grade f ist, ist demnach hier $\mathfrak{G}_Z$ zyklisch vom Grade f, was mit $\mathfrak{G}_Z = \mathfrak{G}$ und $\mathfrak{G}$ nicht zyklisch in Widerspruch steht.

Satz 3 wird bewiesen sein, wenn folgendes gezeigt ist:

288 I

Satz 4. Ist k' ein Oberkörper zu k, der relativ zyklisch vom Primzahlgrad $f \neq \ell$ in Bezug auf k ist und in dessen Relativdiskriminante nur die Primteiler $\mathfrak{l}$ von ℓ aufgehen können. Gilt dann Satz 3 für den Körper k' so gilt er auch für k.

In der Tat, sei ζ die ℓ–te Einheitswurzel. Dann ist der Körper $k(\zeta)$ zyklisch vom Grade n, wo n ein Teiler von $\ell - 1$ ist. In der Relativdiskriminante der Zahl $1 - \zeta$ gehen nur Primteiler von ℓ auf. Da diese durch die Relativdiskriminante von $k(\zeta)$ teilbar ist, gilt dasselbe für letztere.

Nun bilde man die ineinandergeschachtelten Körper:

$$k = k_0 \Big\{ k_1 \big\{ k_2 \ \cdots \{ k_\nu = k(\zeta)$$

derart, daß k_i relativ zyklisch von Primzahlgrad in Bezug auf k_{i-1} ist. Die Relativgrade von k_i zu k_{i-1} sind sämtlich Teiler von $\ell - 1$, also prim zu ℓ. In der Relativdiskriminante von k_i zu k_{i-1} gehen ebenfalls nur Primteiler von ℓ auf, da die Relativdiskriminante $D_{\nu,i-1}$ durch $D_{\nu-1,i-1}$ teilbar ist etz... also durch $D_{i,i-1}$ (S. 15▶, Satz 8). Die Richtigkeit von Satz 4 vorausgesetzt, folgt dann aus Satz 1, daß Satz 3 sukzessive richtig ist für $k_\nu, k_{\nu-1}, \ldots, k_1, k_0 = k$. Wir haben also nur noch Satz 4 zu beweisen.

Es sei $f_1^{[\ldots]}$ die Relativdiskriminante von k', die nur Primfaktoren von ℓ enthält. Da $\ell \neq p$ ist, der Relativgrad aber p, ist jeder dieser Primfaktoren nur in der ersten Potenz in f_1 enthalten: $f_1 = \prod \mathfrak{l}$ erstreckt über gewisse Primteiler von ℓ.

289 I

H sei eine vorgelegte Klassengruppe vom Index ℓ nach dem Modul $\mathfrak{m}$ in k. Sollten nicht alle in f_1 aufgehenden Primideale in $\mathfrak{m}$ vorkommen, so fügen

wir die fehlenden genau in der ersten Potenz hinzu. Der entstehende Modul heiße $\overline{\mathfrak{m}}$ und ist jetzt durch f_1 und natürlich $\mathfrak{m}$ teilbar. H ist auch nach dem Modul $\overline{\mathfrak{m}}$ Klassengruppe vom Index ℓ.

Nun erklären wir die Idealklassen in k nach dem Strahl der Zahlen $\equiv 1 \bmod \overline{\mathfrak{m}}$, in k' ebenfalls nach dem Strahl der Zahlen $\equiv 1 \bmod \overline{\mathfrak{m}}$. □□□

Im Falle $p = 2$ seien beide Strahlen total positiv. Dann folgt, wenn n die Relativnorm von k' nach k ist,

aus $$\mathsf{A} \equiv 1 \bmod \overline{\mathfrak{m}} \text{ in } k'$$

$$n(\mathsf{A}) \equiv 1 \bmod \overline{\mathfrak{m}} \text{ in } k$$

Denn aus dem ersten folgt: $\sigma\mathsf{A} \equiv 1 \bmod \overline{\mathfrak{m}}$, ...

Für $p = 2$ ist ferner, wenn k reell, k' reell und A total positiv in k' ist, auch $n(\mathsf{A}) = \mathsf{A}\sigma\mathsf{A}$ total positiv in k, und wenn k reell, k' imaginär ist, $n(\mathsf{A}) = \mathsf{A}\sigma\mathsf{A}$ sicher total positiv in k.

Daher ist die Relativnorm einer Strahlzahl aus k' sicher Strahlzahl in k, sodaß die Relativnormen aller Ideale aus k', die dort in einer Klasse liegen, in k ebenfalls in einer Klasse liegen. Wir können daher wieder von Relativnormen der Klassen von k' sprechen.

Seien G und G' die Gruppen der Idealklassen in k und k', D die Gruppe der Klassen aus k mit zu ℓ primem Exponenten und

$$G = G_0 \cdot D$$

die Zerlegung in ein direktes Produkt. Die Klassengruppe H aus k vom Index ℓ muß dann offenbar die ganze Gruppe D enthalten. □□□ Denn die Faktorgruppe zu H in Bezug auf G ist zyklisch vom Grad ℓ, jedes in H nicht enthaltene Element muß also zur ℓ–ten Potenz erhoben in H vorkommen.

Ist nun a ein zum Exponenten $\overline{u}$ gehöriges Element und $(\overline{u}, \ell) = 1$, und wäre a nicht in H enthalten, so müßte a^ℓ enthalten sein, also, wegen $a^{\overline{u}} = 1$, doch a selbst. Dementsprechend kann

$$\mathsf{H} = \mathsf{H}_0 \cdot \mathsf{D}$$

gesetzt werden. Sei $C_1', \ldots, C_n'$ ein System von Basisklassen für H_0 und C_0 nicht in H_0 enthalten, aber in G_0. Dann ist, wie wir eben sahen, doch C_0^ℓ in

H enthalten, und da C_0^ℓ als Element von G_0 zu einem Exponenten ℓ^k gehört, auch in H_0. Also:

$$C_0^\ell = C_1'^{a_1} \cdots C_n'^{a_n}$$

Ersetzt man C_0 durch ein passend gewähltes, gleichwertiges $C_0 C_1'^{b_1} \cdots C_n'^{b_n}$, das dann ebenfalls nicht in H_0, wohl aber in G_0 vorkommt, so kann man es erreichen, daß alle Exponenten a_i zwischen 0 und $\ell - 1$ liegen.

1.) Alle $a_i = 0$: $C_0^\ell = 1$. Dann ist

$$C_0 C_1' \ldots C_n'$$

eine Basis für G_0 (H_0 hat in Bezug auf G_0 den Index ℓ) und man kann die Basis für H_0 in der Form

$$C_0^\ell, C_1', \ldots, C_n'$$

schreiben (da eben $C_0^\ell = 1$).

2.) Nicht alle $a_i = 0$. Es sei etwa C_1' das Basiselement mit höchstem Exponenten ℓ^ν unter allen mit nicht verschwindenden a_i und $a_1 a_2 \ldots a_r \neq 0$, $a_{r+1} = \cdots = a_n = 0$.

□□□

Sei $a_1 a_1' \equiv 1 \bmod \ell^\nu$. Da $a_1' \not\equiv 0 \bmod \ell$, kann $C_0^{a_1'}$ an die Stelle von C_0 treten. Nennt man dies wieder C_0, so ist unsere Relation:

$$C_0^\ell = C_1' C_2'^{a_2'} \ldots C_r'^{a_r'} = C$$

C hat den Exponenten ℓ^ν, da dies der höchste der vorkommenden C_i' war. Daher kann C an die Stelle von C_1' als Basiselement treten. Dann ist offenbar

$$C_0, C_2', \ldots, C_n'$$

eine Basis für G_0 und

$$C_0^\ell, C_2', \ldots, C_n'$$

eine Basis für H_0.

(Die Fälle 1.) und 2.) sind grob gesprochen so unterschieden, daß in 1.) H_0 eine solche Untergruppe von $\mathfrak{G}_0$ ist, daß ein zum Exponenten ℓ gehöriges

Basiselement weggelassen ist, während in 2.) ein zum Exponenten $\ell^{\nu+1}$ gehöriges Basiselement von G_0 auf seine $a_0\ell$–ten Potenzen beschränkt, also in ein zu ℓ^ν gehöriges verwandelt wird. 1.) läßt sich sofort unter 2.) subsumieren).

Wir erkennen somit daß in leicht verständlicher Schreibweise eine Basis $C_1, C_2, \ldots, C_n$ (n in abgeänderter Bedeutung) für G_0 gewählt werden kann, sodaß

$$G = [C_1, C_2, \ldots, C_n; \mathsf{D}]$$
$$\mathsf{H} = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}]$$

ist.

Nun bedeute D_0 die Untergruppe von D, welche alle und nur die Relativnormen von Klassen aus k' enthält, ferner D' die Gruppe in k', deren Relativnormen D_0 bilden.

Nun beachten wir, daß zwei Ideale, die in k in einer Klasse liegen, es auch in k' tun. Die Ideale von C_i liegen also in k' in einer Klasse, die wir auch dort C_i nennen, obwohl hier mehrere dieser Klassen übereinstimmen können.

Nun sei C' eine Klasse von k'. Wir setzen:

$$n(C') = C_1^{e_1} \ldots C_n^{e_n}[\mathsf{D}]$$

wo $[\mathsf{D}]$ eine Klasse aus D bedeutet. Dann muß zunächst $[\mathsf{D}]$ sogar in D_0 liegen. Denn da p prim zu ℓ ist, können $x_1, \ldots, x_n$ so bestimmt werden, daß

$$C_i^{px_i} = C_i^{e_i}$$

ist. Nun ist $U = C'C_1^{-x_1} \cdots C_n^{-x_n}$ ebenfalls eine Klasse in k'. In C_i liegen die Ideale aus C_i von k. C_i ist also invariant gegenüber den Substitutionen von k'. Die Norm der Ideale von k ist einfach ihre p–te Potenz, also nach S. 289 unten:

$$n(C_i) = C_i^p \quad \text{in } k,$$

sodaß $n(U) = n(C')C_1^{-x_1 p} \ldots C_n^{-x_n p} = [\mathsf{D}]$ ist, also $[\mathsf{D}]$ zu D_0 gehört. Da weiter $n(U)$ in D_0 liegt, gehört U zu D'. Wir erkennen also zugleich, daß

für jede Klasse C' von k' sich $x_1, \ldots, x_n$ so bestimmen lassen, daß

$$C' = C_1^{x_1} \ldots C_n^{x_n} [\mathsf{D}']$$

ist, wo $[\mathsf{D}']$ eine Klasse aus D' bedeutet. Die Gleichung:

$$1 = C_1^{x_1} \ldots C_n^{x_n} [\mathsf{D}']$$

zieht nach sich, wenn man zur Relativnorm übergeht:

$$1 = C_1^{x_1 p} \ldots C_n^{x_n p} [\mathsf{D}_0] \quad \text{in } k$$

Da aber p prim zu ℓ, folgt wegen der Basiseigenschaft von $C_1, \ldots, C_n$, daß $C_1^{x_1} = \cdots = C_n^{x_n} = 1$, also auch $[\mathsf{D}_0] = 1$ ist. Die Klassen C_i haben also in k' genau die gleiche Ordnung und Unabhängigkeit wie in k. Sie sind wie gezeigt, auch von $[\mathsf{D}']$ unabhängig. Wir können also schreiben:

$$G' = [C_1, C_2, \ldots, C_n; \mathsf{D}']$$

Durch die Festsetzung:

$$\mathsf{H}' = [C_1^{\ell}, C_2, \ldots, C_n; \mathsf{D}']$$

ist uns also in k' eine Klassengruppe vom Index ℓ definiert.

Da nach Voraussetzung der Satz 3 richtig ist für k', gibt es zu H' über k' einen Klassenkörper K, der relativ zyklisch vom Primzahlgrad ℓ ist. Ist $\mathfrak{F}^{\ell-1}$ seine Relativdiskriminante, so ist $\overline{\mathfrak{m}}$ durch $\mathfrak{F}$ teilbar.

Durch die Substitutionen von k' geht, wie aus der Definition von D' ersichtlich, jede Klasse von D' in eine Klasse von D' über. Denn die Relativnormen der Klassen aus D' gestatten die Substitutionen. Da die C_i invariant gegenüber diesen Substitutionen sind, ist H' invariant gegenüber den Substitutionen von k' nach k. Geht man nun

294 I

von K zu einem nach k relativ–konjugierten Körper über, so entspricht dem in k' eine gewisse Substitution. Da H' invariant, bleibt auch der konjugierte Körper von K Klassenkörper für H', also da es nur einen Klassenkörper geben kann, ist er mit K identisch. K ist also relativ Galoissch in Bezug auf k.

Die Relativnormen der Ideale von K nach k' fallen nach Definition des Klassenkörpers sämtlich in H'. Die Relativnormen der Ideale von H' fallen ihrerseits, da p prim zu ℓ und $n(C_i) = C_i^p$ in k in die Gruppe

$$\mathsf{H}_0 = [C_1^{\ell}, C_2, \ldots, C_n; \mathsf{D}_0] \quad \text{von } k$$

□□□

Dieses gilt somit für die Relativnormen der Ideale von K nach k.

Nun ist $\overline{\mathfrak{m}}$ durch f_1 teilbar und k' vom Primzahlgrad p und zyklisch nach k. Auf Grund von Satz 22, 27, S. 202, 206 ist also k' ein Klassenkörper über k für eine Klassengruppe vom Index p nach $\overline{\mathfrak{m}}$.

Da k' der Gruppe $G_0 = [C_1, C_2, \ldots, C_n; \mathsf{D}_0]$ zugeordnet ist, in die die Relativnormen von k' nach k nach S. 292 fallen, hat also diese den Index p in Bezug auf G, d.h. D_0 den Index p in Bezug auf D. (Wegen $p \neq \ell$ machen die genannten Relativnormen offensichtlich diese *ganze* Gruppe aus).

Die Gruppe $[C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0] = \mathsf{H}_0$ hat also den Index $p\ell$ in Bezug auf G. Die Relativnormen von K nach k fallen alle in diese Gruppe. K ist also in Bezug auf k einer Untergruppe dieser Gruppe H_0 zugeordnet, und relativ Galoissch. Nach Satz 7, S. 142 muß also

295 I

□□□

der Index dieser Untergruppe in Bezug auf $G \leqq p\ell$ als Relativgrad (K, k) sein, und also die zugeordnete Untergruppe die Gruppe $\mathsf{H}_0 = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0]$ vom Index $p\ell$ selbst. Nach Definition 4, S. 144 ist also K Klassenkörper für k zu dieser Klassengruppe H_0.

Auf Grund von Satz 8, S. 143 gibt es nun in k sicher unendlich viele Primideale $\mathfrak{p}$ (ersten Grades), welche in k' nicht in lauter Primideale ersten Grades zerfallen (also unzerlegt bleiben, da der Relativgrad p Primzahl ist), und auch nicht in der Klassengruppe H vom Index $\ell > 2$ enthalten sind.

Würde nun ein solches in k' unzerlegtes Primideal $\mathfrak{p}$ in K zerfallen, also in ℓ Primideale ersten Relativgrades nach k', so wäre $\mathfrak{p}$ die Relativnorm eines jeden dieser Primideale von K nach k', also in der Klassengruppe H', deren Klassenkörper ja K zu k' ist, enthalten. $n(\mathfrak{p}) = \mathfrak{p}^p$ wäre also in H_0 enthalten. Da p prim zu ℓ ist, wäre dann $\mathfrak{p}$ selbst in $\mathsf{H} = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}]$ enthalten; denn sei A die Klasse von $\mathfrak{p}$, so wäre

$$\mathsf{A}^p = C_1^{\ell x_1} C_2^{x_2} \ldots C_n^{x_n} [\mathsf{D}_0]$$

und wenn $pp' = 1 + i\ell$

$$\mathsf{A}\mathsf{A}^{i\ell} = C_1^{\ell p' x_1} C_2^{p' x_2} \ldots C_n^{p' x_n} [\mathsf{D}_0]^{p'}$$

Sei $\mathsf{A} = C_1^{y_1} \ldots C_n^{y_n} [\mathsf{D}]$. Dann wird $\mathsf{A}^{i\ell} = C_1^{i\ell y_1} \ldots$

$$\mathsf{A} = C_1^{\ell(p' x_1 + i y_1)} \ldots [\mathsf{D}] \quad \text{also in } \mathsf{H} \text{ enthalten.}$$

296 I

Wir hatten aber gerade $\mathfrak{p}$ *nicht* in H annehmen dürfen. Also bleibt unser $\mathfrak{p}$ in K unzerlegt, und somit ist nach unserm Hilfssatz K relativ zyklisch zu k, vom Relativgrade $p\ell$.

In K ist also ein Unterkörper K_0 enthalten, der relativ zyklisch vom Grade ℓ in Bezug auf k ist. Wir zeigen jetzt, daß dieser Körper K_0 gerade unser gesuchter Klassenkörper für H ist.

Dies wird bewiesen sein, wenn wir die Teilbarkeit von $\overline{\mathfrak{m}}$ durch f gezeigt haben, wo $f^{\ell-1}$ die Relativdiskriminante von K_0 nach k ist. Denn dann ist nach Satz 22 (S. 202▸) K_0 Klassenkörper für eine Klassengruppe vom Index ℓ nach $\overline{\mathfrak{m}}$. □□□

Die Relativnormen von K nach k liegen, da K Klassenkörper für die Klassengruppe H_0 ist in $\mathsf{H}_0 = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0]$ und erfüllen diese Gruppe *ganz*. Ist $\mathfrak{A}$ ein Ideal aus K, so ist

$$\mathfrak{a} = n_K(\mathfrak{A}) = n_{K_0}[n_{K,K_0}(\mathfrak{A})] = n_{K_0}(\mathfrak{A}_{K_0}); \quad \mathfrak{A}_{K_0} \text{ aus } K_0$$

□□□

Jedes Ideal $\mathfrak{a}$ aus k, das Norm eines Ideals aus K ist, ist also auch Norm eines Ideals aus K_0 und folglich

297 I

jedes Ideal $\mathfrak{a}$ aus H_0 auch Norm aus K_0, sodaß H_0 eine Untergruppe der fraglichen Gruppe vom Index ℓ ist, für die K_0 Klassenkörper ist.

Nun kann über $\mathsf{H}_0 = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0]$ vom Index $p\ell$ und unter $G = [C_1, C_2, \ldots, C_n; \mathsf{D}]$ nur die Untergruppe $\mathsf{H} = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}]$ vom Index ℓ liegen. Denn nimmt man zu H_0 etwa C_1 hinzu, so entsteht G_0 vom Index p.

Also ist dann K_0 Klassenkörper zu H.

Wir zeigen jetzt also noch die Teilbarkeit von $\overline{\mathfrak{m}}$ durch f. Die Relativdiskriminante von K nach k hat nach Satz 8, S. 15▸ den Wert

$$(f_1^{p-1})^\ell n_{k',k}(\mathfrak{F}^{\ell-1}).$$

$\overline{\mathfrak{m}}$ ist durch f_1 teilbar, nach Konstruktion, ferner durch $\mathfrak{F}$ und auch durch dessen konjugierte in k', da $\overline{\mathfrak{m}}$ Ideal aus k ist. Also kommen in dieser Relativdiskriminante nur Primfaktoren von $\overline{\mathfrak{m}}$ vor, demnach auf in f keine anderen,

da f Teiler der eben aufgestellten Relativdiskriminante. Da K_0 den Relativgrad ℓ hat, geht jedes von den $\mathfrak{l}$ verschiedene Primideal nur in der ersten Potenz in f auf. Für alle solche Primideale ist also die Teilbarkeit von $\overline{\mathfrak{m}}$ durch f gesichert. Es handelt sich nur noch um die Primideale $\mathfrak{l}$.

$\mathfrak{m}$ möge genau durch $\mathfrak{l}^g$ teilbar sein. Geht $\mathfrak{l}$ nicht in der Relativdiskriminante von K nach k auf, so kann es auch nicht in f aufgehen. Im übrigen haben wir folgende Möglichkeiten von Zerlegungen in K

298 I

1.) $\mathfrak{l} = (\boldsymbol{L_1 \dots L_\ell})^{\boldsymbol{p}}$; (die L_i verschieden).

(Dann gilt in k': $\mathfrak{l} = \mathfrak{l}'^p$, da k' vom Grade p und infolgedessen einerseits die ℓ Primfaktoren in k' unmöglich sind, andererseits nicht $\mathfrak{l} = \mathfrak{l}'$ in k' sein kann). In K_0 vom Grade ℓ aber muß gelten: $\mathfrak{l} = \mathfrak{l}_1 \dots \mathfrak{l}_\ell$ aus ähnlichen Gründen. f ist also nicht durch $\mathfrak{l}$ teilbar.

2.) $\mathfrak{l} = \boldsymbol{L^p}$

Dann kann in K_0 vom Grade ℓ nur $\mathfrak{l} = L_0$ Primideal sein, $\mathfrak{l}$ geht also ebenfalls nicht in f auf.

3.) $\mathfrak{l} = (\boldsymbol{L_1 \dots L_p})^{\boldsymbol{\ell}}$. ($L_1, \dots, L_p$ verschieden).

Dann muß in k' gelten $\mathfrak{l} = \mathfrak{l}_1 \dots \mathfrak{l}_p$, wo $\mathfrak{l}_i = L_i^\ell$ ist. In K_0 muß $\mathfrak{l} = L^\ell$ sein, wo $L = L_1 \dots L_p$ ist. $\overline{\mathfrak{m}}$ ist durch $\mathfrak{l}^g$ also durch $\mathfrak{l}_i^g$ teilbar (genau), $\mathfrak{F}$ durch $\mathfrak{l}_i^{v'+1}$, wo v' die übliche Bedeutung für den relativzyklischen Körper □□□ K über k' vom Grade ℓ hat. Da $\overline{\mathfrak{m}}$ durch $\mathfrak{F}$ teilbar ist, ist $v' < g$. Die Relativdifferente von K nach k, als Produkt der Relativdifferenten von K nach k' und k' nach k (diese ist prim zu $\mathfrak{l}$) dargestellt, hat den Faktor $L_i^{(v'+1)(\ell-1)}$

K nach K_0 hat den Grad p, in der Relativdiskriminante geht L nicht auf. Unsere Gesamt–Relativdifferente, als Produkt der Rel. Diff. von K nach K_0 und K_0 nach k dargestellt, hat den Faktor $L^{(v+1)(\ell-1)}$, wenn $\mathfrak{l}^{v+1}$ der Faktor von f ist, also den Faktor $L_i^{(v+1)(\ell-1)}$. Es ist also $v' = v$ und folglich $v < g$, also $\overline{\mathfrak{m}}$ auch durch $\mathfrak{l}^{v+1}$ teilbar. Im Falle $g = 1$ übrigens folgt noch, daß $\mathfrak{l}$ nicht in f aufgeht, da $v < 1$ unmöglich (Satz 2, S. 149▶).

299 I

4.) $\mathfrak{l} = \boldsymbol{L^\ell}$

Dann ist:

$$\begin{aligned} &\text{in } k' && \mathfrak{l} = \mathfrak{l}' \\ &\text{in } K_0 && \mathfrak{l} = L^{\ell} \end{aligned}$$

In k' bleibt also $\mathfrak{l}$ Primideal; $\overline{\mathfrak{m}}$ ist in k' durch $\mathfrak{l}'^{g}$ teilbar, also wenn $\mathfrak{F}$ durch $\mathfrak{l}'^{(v'+1)}$ teilbar ist, $v' < g$. Das Primideal L aus K_0 bleibt es in K. Wie vorhin findet man, wenn $\mathfrak{l}^{v+1}$ in f aufgeht, für den Faktor der Gesamt–Relativdifferente

$$L^{(v'+1)(\ell-1)} = L^{(v+1)(\ell-1)}, \quad \text{also} \quad v = v'$$

oder $v < g$ und alles wie vorhin.

5.) $\mathfrak{l} = L^{p\ell}$

Also:

$$\begin{array}{lcllcll} \mathfrak{l} & = & \mathfrak{l}'^{p} & \text{in} & k' & \text{wo} & \mathfrak{l}' = L^{\ell} \quad \text{ist,} \\ \mathfrak{l} & = & L'^{\ell} & \text{in} & K_0 & = & L' = L^{p} \quad \text{ist.} \end{array}$$

$\overline{\mathfrak{m}}$ ist durch y'^{pg} teilbar. Ist also $\mathfrak{F}$ durch $\mathfrak{l}'^{(v'+1)}$ teilbar, so ist $v' < pg$. f_1 ist durch $\mathfrak{l}$ teilbar, die Relativdiskriminante von K nach K_0, da der Grad p prim zu ℓ ist, durch L'^{p-1}. Wie vorhin ist der Faktor der Gesamt–Relativdifferente:

$$L^{\ell(p-1)} L^{(v'+1)(\ell-1)} = L^{p(v+1)(\ell-1)} L^{p-1}$$

oder

$$\underline{\ell p} - \underline{\ell} + v'\ell + \underline{\ell} - v'\underline{-1} = pv\ell + \underline{p}\ell - pv - \underline{p} + \underline{p} - \underline{1}$$

$$v'(\ell - 1) = pv(\ell - 1)$$

$$v' = pv$$

also

$$pv < pg$$

$$v < g,$$

und somit wieder $\overline{\mathfrak{m}}$ durch den Faktor von f teilbar.

300 ı

Auf jeden Fall ist also $\overline{\mathfrak{m}}$ durch f teilbar, ja es ist sogar $\mathfrak{m}$ selbst durch f teilbar. Denn $\overline{\mathfrak{m}}$ entstand aus $\mathfrak{m}$ durch Hinzufügen einfacher Faktoren $\mathfrak{l}$, und zwar solcher, die in $\mathfrak{m}$ fehlen. Wie wir aber unter 3.) zeigten, und wie bei 4.) 5.) ebenso folgt, kann f durch einfache Faktoren von $\overline{\mathfrak{m}}$ nicht teilbar sein. Satz 4 ist damit vollständig bewiesen, somit gilt Satz 3 für jeden Körper k.

Weiter folgt:

Satz 5. Ist $\mathfrak{H}$ eine Klassengruppe vom Index ℓ in k und $f^{\ell-1}$ die Relativdiskriminante des Klassenkörpers zu H (der ja nach dem eben Gezeigten relativ zyklisch vom Grade ℓ ist), so ist f der *Führer* der Klassengruppe H.

Beweis. Satz 22, 27 (S. 202, 206) ist in der Tat der gegebene Klassenkörper K als solcher nach einer Klassengruppe H' mit dem Modul f erklärbar. Diese Klassengruppe H' ist aber als Gruppe der Relativnormen der Ideale aus K eindeutig bestimmt, und somit gleich H, d.h. H ist auch nach dem Modul f erklärbar.

Nach dem allgemeinen Existenzsatz 3 aber ist f ein Teiler jedes Moduls, nach dem H erklärbar ist.

Nach Definition dieses Begriffs ist also f Führer der Klassengruppe H.

c) Existenz bei Primzahlpotenzgrad

c.) Relativ–zyklische Klassenkörper von Primzahlpotenzgrad.

Wir werden in diesem Abschnitt folgenden Satz beweisen:

Satz 6. In einem beliebigen Körper k sei eine Klassengruppe H nach dem Modul $\mathfrak{m}$ vorgelegt, derart daß die Gruppe $\frac{G}{\mathsf{H}}$ zyklisch vom Primzahlpotenzgrad ℓ^ν ist, wo G die Gruppe aller Klassen nach dem mod $\mathfrak{m}$ bedeutet (für $\ell = 2$ mit genügend scharfer Vorzeichenbedingung). Dann existiert ein Klassenkörper K für die Gruppe H, welcher überdies die folgenden Eigenschaften besitzt:

1.) Er ist relativ–zyklisch vom Primzahlpotenzgrad ℓ^ν in Bezug auf k.

2.) Die Relativdiskriminante von K nach k enthält kein Primideal als Faktor, das nicht in $\mathfrak{m}$ aufgeht.

Der Satz ist für $\nu = 1$, wo es sich um Gruppen von Primzahlindex handelt, vollständig durch Satz 3 bewiesen. Wir können also vollständige Induktion anwenden, also annehmen Satz 6 sei richtig für alle Körper und Klassengruppen vom Index $\ell^{\nu-1}$.

Wir definieren die Klassen von k nach dem Strahl o der Zahlen $\equiv 1 \bmod \mathfrak{m}$ (im Falle $\ell = 2$ total positiv). G sei die Gruppe der Idealklassen, H die vorgelegte Klassengruppe.

Da $\frac{G}{\mathsf{H}}$ relativ zyklisch vom Grade ℓ^ν sein soll, gibt es eine Klasse C, sodaß

$$G = \mathsf{H} + C\mathsf{H} + C^2\mathsf{H} + \cdots + C^{\ell^\nu - 1}\mathsf{H} \quad \text{kurz} \quad = (C; \mathsf{H})$$

ist, sodaß also erst die ℓ^ν–te Potenz von C in H liegt.

302 I

Unter G_0 verstehen wir die Gruppe

$$G_0 = \mathsf{H} + C^\ell\mathsf{H} + C^{2\ell}\mathsf{H} + \cdots + C^{(\ell^{\nu-1}-1)\ell}\mathsf{H}$$

oder kurz $G_0 = (C^\ell; \mathsf{H})$

Dann ist

$$G = G_0 + CG_0 + \cdots + C^{\ell-1}G_0 = (C; G_0)$$

d.h. $\frac{G}{G_0}$ zyklisch vom Grade ℓ.

Nach Satz 3 existiert also ein Klassenkörper k' von k für die Gruppe G_0, der relativ zyklisch vom Grade ℓ ist. □□□ Nach den Ausführungen auf S. 219▸ ff. gibt es in k' ein in $\mathfrak{m}$ aufgehendes, *invariantes* Ideal $\mathfrak{M}$ derart, daß, wenn in k' die Idealklassen nach dem Strahl $O \equiv 1 \bmod \mathfrak{M}$ erklärt werden, die Relativnormen einer Klasse von k' in eine Klasse von k fallen, sodaß wieder von Relativnormen der Klassen in k' gesprochen werden kann.

Es sei nun H' die Gruppe derjenigen Klassen von k', deren Relativnormen in die Gruppe H fallen. Wie im vorigen Abschnitt soll ferner unter C auch gleichzeitig die Klasse von k' verstanden werden, welche die Ideale von C aus k enthält. Dann ist $n(C) = C^\ell$

k' ist Klassenkörper für G_0. Die Relativnorm einer Klasse C' von k' fällt also in die Gruppe G_0, hat also die Form

$$n(C') = C^{a\ell}[\mathsf{H}]$$

wo $[\mathsf{H}]$ eine Klasse aus H bedeutet. Setzen wir also

$$C' = C^a U'$$

so ist $n(U') = [\mathsf{H}]$, U' also Klasse aus H'. Wir können also jede Klasse von k' in der Form schreiben:

303 ı

$$C' = C^a[H']$$

Um die Ordnung von C in k' nach $[\mathsf{H}']$ festzustellen, sei

$$C^a = [\mathsf{H}'] \quad \text{in} \quad k'$$

also $$C^{\ell a} = [\mathsf{H}] \text{ in } k$$

Es muß also ℓa durch ℓ^ν, d.h. a durch $\ell^{\nu-1}$ teilbar sein. Umgekehrt ist

$$C^{\ell^{\nu-1}} = [\mathsf{H}']$$

da die Norm in H fällt und H' so definiert war.

Es gehört also C in k' in Bezug auf H' zum Exponenten $\ell^{\nu-1}$. Die Gruppe G' aller Klassen von k' gestattet also die Darstellung:

$$G' = (C; \mathsf{H}') = \mathsf{H}' + C\mathsf{H}' + \cdots + C^{\ell^{\nu-1}-1}\mathsf{H}'$$

und $C^{\ell^{\nu-1}}$ liegt in H'. Die Gruppe $\frac{G'}{\mathsf{H}'}$ ist also relativ–zyklisch vom Grade $\ell^{\nu-1}$.

Nach Annahme existiert also ein relativ–zyklischer Klassenkörper K über k' für die Gruppe H' vom Grade $\ell^{\nu-1}$ und den in Satz 6 genannten Eigenschaften. Dabei sind die Klassen in k', also auch H' nach dem Modul $\mathfrak{M}$ erklärt.

$\mathfrak{M}$ ist nun ein invariantes Ideal von k', die Gruppe H' also laut ihrer Definition invariant gegenüber den Substitutionen von k' nach k. Jeder in Bezug auf k konjugierte Körper von K ist also auch Klassenkörper für H', fällt also der Eindeutigkeit wegen mit K zusammen. Es ist also K relativ–Galoissch zu k.

Da K Klassenkörper zu k' für H' ist, fallen die Relativnormen der Ideale von K nach k' in die Gruppe H'. Die

304 ı

Relativnormen der Ideale aus H' nach k sind aber nach Definition von H' in H enthalten. Also fallen die Relativnormen von K nach k sämtlich in H, K ist somit einer Untergruppe von H zugeordnet. Nun hat aber K den Grad ℓ^ν in Bezug auf k. Da dieser Grad den Index der zugeordneten Klassengruppe nicht unterschreiten darf, ist also der letztere $\leqq \ell^\nu$, also $= \ell^\nu$ und K der Gruppe H selbst zugeordnet und Klassenkörper zu ihr.

Es sei nun $\mathfrak{G}$ die Gruppe von K nach k. $\mathfrak{G}$ hat den Grad ℓ^ν. Wir stützen uns nun auf folgenden Satz der Gruppentheorie (Weber, II, S. 140, Satz VI):

Hilfssatz: Ist $\mathfrak{G}$ eine Gruppe vom Grade ℓ^ν, $\mathfrak{g}$ eine Untergruppe von Grade ℓ^μ $(\mu < \nu)$, so gibt es stets eine Untergruppe $\mathfrak{g}_1$ vom Grade $\ell^{\mu+1}$, von der $\mathfrak{g}$ invariante Untergruppe ist.

Für $\mu = \nu - 1$ ergibt sich also, daß jede Untergruppe $\mathfrak{G}_0$ vom Grade $\ell^{\nu-1}$ invariante Untergruppe zu $\mathfrak{G}$ ist, ferner daß $\mathfrak{G}_0$ noch so gewählt werden kann, daß es die vorgegebene Untergruppe $\mathfrak{g}$ vom Grade ℓ^μ $(\mu < \nu)$ [...]. (nicht notwendig als invariante).

Sei nun $\mathfrak{G}_0$ eine Untergruppe vom Grade $\ell^{\nu-1}$ unserer Gruppe $\mathfrak{G}$. Zu $\mathfrak{G}_0$ gehört, da sie invariant ist, ein relativ zyklischer Körper vom Primzahlgrad ℓ über k. Die $\ell^{\nu-1}$–ten Potenzen der Relativnormen seiner Ideale sind nun die Relativnormen dieser Ideale in K, liegen also in H. Die Relativnormen selbst liegen also □□□ in Klassen, deren $\ell^{\nu-1}$–te Potenzen in H liegen, also die Form $C^{\ell a}[\mathsf{H}]$ haben, d.h. in $\mathfrak{G}_0$ liegen. Unser Körper ist also einer Klassengruppe

zugeordnet, die Untergruppe von $\mathfrak{G}_0$ ist; da ihr Index in Bezug auf G den Relativgrad ℓ nicht überschreiten darf, ist es die Gruppe G_0 vom Index ℓ selbst. Der Körper ist also Klassenkörper für G_0, d.h., da auch k' Klassenkörper zu G_0 ist, mit k' identisch. Es gibt also nur einen relativ–zyklischen Körper vom Grade ℓ in K, d.h. nur eine einzige Untergruppe $\mathfrak{G}_0$ von $\mathfrak{G}$ vom Index ℓ.

Sei nun

$$\mathfrak{G} = \mathfrak{G}_0 + \sigma\mathfrak{G}_0 + \sigma^2\mathfrak{G}_0 + \cdots + \sigma^{\ell-1}\mathfrak{G}_0$$

Wäre der Exponent von σ kleiner als ℓ^ν, so würde durch σ eine Untergruppe $\mathfrak{g}$ vom Grade ℓ^μ $(\mu < \nu)$ erzeugt, und es gäbe nach unserm Hilfssatz eine Untergruppe $\overline{\mathfrak{G}}_0$ vom Index ℓ, die $\mathfrak{g}$ enthält.

Diese Untergruppe $\overline{\mathfrak{G}}_0$ enthält σ, ist also nach unserer Zerlegung von $\mathfrak{G}_0$ sicher verschieden, was soeben als unmöglich erkannt. Also gehört σ zum Exponenten ℓ^ν, seine Potenzen erschöpfen die ganze Gruppe, die somit zyklisch vom Grade ℓ^ν ist, also auch K.

Die Relativdiskriminante von k' nach k enthält nach Satz 3 keine anderen Primideale, als die in $\mathfrak{m}$ aufgehenden. Wir nennen sie $\mathfrak{d}_1$. Die Relativdiskriminante von K nach k' enthält nach Annahme keine anderen Primideale, als in $\mathfrak{M}$ aufgehen. Wir nennen sie $\mathfrak{d}_2$. Ihre Relativnorm enthält also da $\mathfrak{M}$ nur invariante Primfaktoren in k' enthält und $\mathfrak{M}$ in $\mathfrak{m}$ aufgeht, nur Teiler von $\mathfrak{m}$. Die Gesamtrelativdiskriminante ist $\mathfrak{d}_1^{\ell^{\nu-1}} n_{k'}(\mathfrak{d}_2)$, enthält also ebenfalls nur Teiler von $\mathfrak{m}$.

306 I

Damit ist der Beweis von Satz 6 in allen Teilen erbracht.

Der Existenzbeweis für den Klassenkörper einer beliebigen Gruppe H und seine ersten grundlegenden Eigenschaften werden sich nun leicht herleiten lassen.

d) Existenz im allgemeinen Fall

d.) Klassenkörper für beliebige Klassengruppen.

Hauptsatz I. In einem algebraischen Körper k sei irgendeine Klassengruppe H nach dem Modul $\mathfrak{m}$ gegeben (mit oder ohne Vorzeichenbedingung). Dann existiert stets ein Klassenkörper K über k für diese Klassengruppe mit folgenden Eigenschaften:

1.) K ist relativ–Abelsch zu k, und der Relativgrad ist gleich dem Index der Gruppe H nach der Gruppe G aller Idealklassen in k nach $\mathfrak{m}$.

2.) Die Relativgruppe von K ist einstufig isomorph mit der Faktorgruppe $\frac{G}{\mathsf{H}}$.

3.) Die Relativdiskriminante von K enthält kein Primideal als Faktor, das nicht in $\mathfrak{m}$ aufgeht.

Dem Beweise schicken wir folgenden Satz voraus:

Satz 7. Die Relativnormen der Ideale der Körper über k: $K_1, K_2, \ldots, K_s$ mögen bezw. in die Gruppen $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_s$ von k nach ein- und demselben Modul $\mathfrak{m}$ fallen. Dann fallen die Relativnormen der Ideale des komponierten Körpers $K = K_1 K_2 \ldots K_s$ in den Durchschnitt der Gruppen $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_s$.

307 I

Beweis. Bilden wir die Relativnorm eines Ideals von K nach k, indem wir zuerst die Relativnorm nach K_i, dann von K_i nach k bilden, so sehen wir,

daß die Relativnormen von K nach k in die Gruppe H_i fallen, also in den Durchschnitt aller H_i, w.z.b.w.

Nun bilden wir die Faktorgruppe $\frac{G}{\mathsf{H}}$, die ja eine Abelsche Gruppe ist, und stellen sie durch eine Basis dar. Dieser Basisdarstellung entsprechend gibt es Klassen $C_1, \ldots, C_s$ sodaß die $\ell_i^{\nu_i}$–te Potenz von C_i nicht in H liegt, und jede Nebengruppe von H eindeutig in der Form:

$$C_1^{a_1} \ldots C_s^{a_s} \mathsf{H}\,; \qquad 0 \leqq a_i \leqq \ell_i^{\nu_i} - 1$$

darstellbar ist, wo die ℓ_i Primzahlen sind, und $\ell_1^{\nu_1} \ldots \ell_s^{\nu_s}$ der Index von H ist.

Unter H_i verstehen wir nun die Gruppe, die aus allen Nebengruppen folgender Form besteht:

$$\mathsf{H}_i = C_1^{a_1} \ldots C_{i-1}^{a_{i-1}} C_{i+1}^{a_{i+1}} \ldots C_s^{a_s} \mathsf{H}\,; \qquad 0 \leqq a_k \leqq \ell_k^{\nu_k} - 1$$

wo also die Klasse C_i fehlt.

Dann ist offenbar

$$G = \mathsf{H}_i + C_i \mathsf{H}_i + C_i^2 \mathsf{H}_i + \cdots + C_i^{\ell_i^{\nu_i} - 1} \mathsf{H}_i,$$

sodaß $\frac{G}{\mathsf{H}_i}$ zyklisch vom Grade $\ell_i^{\nu_i}$ ist.

Nach Satz 6 existiert über k ein relativ–zyklischer Körper K_i vom Grade $\ell_i^{\nu_i}$, $\square\square\square$ der Klassenkörper zu H_i ist.

Der komponierte Körper $K = K_1 \ldots K_s$ hat folgende Eigenschaften:

1.) Sein Grad in Bezug auf k hat *höchstens* den Wert $\ell_1^{\nu_1} \ldots \ell_s^{\nu_s}$, da $\ell_i^{\nu_i}$ der Grad von K_i ist.

2.) Er ist relativ Abel'sch, da es alle K_i sind.

3.) Nach Satz 7 liegen die Relativnormen nach k seiner Ideale im Durchschnitt von $\mathsf{H}_1, \ldots, \mathsf{H}_s$, also in H.

(Zu 2.) Sind K_1, K_2 zwei rel. Abel'sche Körper zu k, $\square\square\square$ so läßt sich jede Zahl γ aus dem komponierten Körper in der Form darstellen

$$\gamma = \varphi(\alpha, \beta) = \sum c_{ik} \alpha_i \beta_k; \quad (c_{ik} \text{ in } k;\ \alpha_i \text{ in } k_1;\ \beta_k \text{ in } k_2)$$

wo die α_i und β_k je ein System linear in Bezug auf k unabhängiger Zahlen durchlaufen. Durch nacheinander folgende Anwendung zweier Substitutionen σ und τ für k_1 und k_2 entsteht *unabhängig von der Reihenfolge*:

$$\gamma|\sigma\tau = \sum c_{ik}\alpha_i|\sigma \cdot \beta_k|\tau.$$

sodaß die Substitutionen von k_1 und k_2 vertauschbar sind. Diese erzeugen sicher alle konjugierten, und ein Teil von ihnen bildet daher die Galoissche Gruppe des *Normalkörpers* K_1K_2. Da die σ und τ unter sich je vertauschbar sind, ist also K_1K_2 Abelsch zu k; das gleiche gilt mithin für beliebig viele komponierte Körper).

Nach 3.) ist K einer Untergruppe von H zugeordnet. Der Index von H ist $\ell_1^{\nu_1} \dots \ell_s^{\nu_s}$. Da der Index der zugeordneten Klassengruppe den Grad des Körpers nicht übersteigen kann, also $\leqq \ell_1^{\nu_1} \dots \ell_s^{\nu_s}$ sein muß, andererseits als Index einer Untergruppe von H sicher $\geqq \ell_1^{\nu_1} \dots \ell_s^{\nu_s}$ sein muß, folgt:

1.) Der Grad von K ist $\ell_1^{\nu_1} \dots \ell_s^{\nu_s}$

2.) K ist der Gruppe H zugeordnet.

K ist also der Klassenkörper zu H. Die komponierten Körper K_i haben keinen Durchschnitt gemein. Daher

309 ı

ist die Substitutionsgruppe von K isomorph mit dem direkten Produkt der Gruppen von K_i. Da diese letzteren zyklisch von den Graden $\ell_i^{\nu_i}$ sind, hat also die Gruppe von K die Darstellung:

$$\sigma_1^{a_1} \dots \sigma_s^{a_s}; \qquad 0 \leqq a_i < \ell_i^{\nu_i}$$

Sie ist also isomorph mit $\frac{G}{\mathsf{H}}$.

Auf Grund von Satz 6 enthält endlich die Relativdiskriminante von K_i nach k keine anderen Primfaktoren, als die von $\mathfrak{m}$. Nach Satz 10, S. 20 gilt also dasselbe von der Relativdiskriminante von K nach k.

Unser Satz ist somit vollständig bewiesen. Die in ihm enthaltenen Eigenschaften 1.) 2.) des Klassenkörpers kann man auch so aussprechen:

Satz 8. Ist K der Klassenkörper für die Klassengruppe H und definiert man die Idealklassen des Körpers k nach der Gruppe H, (indem man immer eine ganze Nebengruppe in eine Klasse zusammennimmt), so gilt:

1.) Der Grad von K nach k ist gleich der so herauskommenden Klassenzahl von k.

2.) Die Gruppe von K nach k ist isomorph mit der so herauskommenden Klassengruppe von k.

1.9 Relativabelsche Körper als Klassenkörper.

310 ı

Beim Beweis unseres Existenzsatzes hat sich herausgestellt, daß jeder Klassenkörper relativ–Abelsch ist. Wir beweisen in diesem Abschnitt die Umkehrung, nämlich:

Hauptsatz II. Jeder relativ–Abelsche Körper K in Bezug auf k ist Klassenkörper für eine gewisse Klassengruppe nach einem bestimmten Modul $\mathfrak{m}$. Dies $\mathfrak{m}$ kann außerdem so gewählt werden, daß in $\mathfrak{m}$ nur die Teiler der Relativdiskriminante von K nach k aufgehen.

Vergleicht man die letzte Aussage dieses Satzes mit dem Hauptsatz des vorigen Abschnittes, so kann unmittelbar gefolgert werden:

Satz 1. In der Relativdiskriminante des Klassenkörpers einer Klassengruppe H gehen die und nur die Primideale auf, welche im Führer der Klassengruppe aufgehen.

(Vergl. die ganz analoge Überlegung S. 300▸).

Es sei also K relativ–Abelsch in Bezug auf k. Unser Hauptsatz wird bewiesen sein, wenn er für alle relativzyklischen Körper von Primzahlpotenzgrad als richtig erkannt ist. Dann, wie in der Galoisschen Theorie gezeigt wird, läßt sich K aus solchen Körpern komponieren. Nun gilt aber folgendes: Es seien K_1 und K_2 zwei Klassenkörper von k, die den Durchschnitt k haben.

311 ı

Sie mögen zu den Gruppen H_1 und H_2 vom Index n_1 und n_2 gehören, die resp. nach $\mathfrak{m}_1$ und $\mathfrak{m}_2$ erklärt seien. Dann sind sie beide auch Klassenkörper nach dem Modul $\mathfrak{m}$, wo $\mathfrak{m}$ das kleinste gemeinsame Vielfache von $\mathfrak{m}_1$ und $\mathfrak{m}_2$ ist.

Aus H_1 und H_2 bilden wir die durch sie erzeugte Untergruppe der Gruppe G aller Idealklassen nach $\mathfrak{m}$:

$$\overline{\mathfrak{H}} = \mathsf{H}_1 \cdot \mathsf{H}_2$$

Sowohl H_1 als H_2 sind Untergruppen von $\overline{G}$. Nach Satz 9, S. 144 ist also der Klassenkörper von $\overline{\mathfrak{G}}$ ein Unterkörper von K_1 und K_2, also k. Demnach

muß $\overline{\mathfrak{G}}$ die Gruppe aller Idealklassen sein (Eigenschaft 1.) von Hauptsatz I):

$$G = \mathsf{H}_1 \cdot \mathsf{H}_2$$

Es sei nun H_0 der Durchschnitt von H_1 und H_2 und:

$$\begin{aligned} \mathsf{H}_1 &= \mathsf{H}_0 + a_1\mathsf{H}_0 + \cdots + a_\nu\mathsf{H}_0 \\ \mathsf{H}_2 &= \mathsf{H}_0 + b_1\mathsf{H}_0 + \cdots\cdots\cdots + b_\mu\mathsf{H}_0 \end{aligned}$$

$\mathsf{H}_1\mathsf{H}_2$ besteht aus den Komplexen $a_ib_k\mathsf{H}_0$. Diese sind alle voneinander verschieden, da aus

$$a_ib_k\mathsf{H}_0 = a_i'b_k'\mathsf{H}_0$$

folgt:

$$a_ia_i'^{-1}\mathsf{H}_0 = b_kb_k'^{-1}\mathsf{H}_0$$

was nach Definition von H_0 nur geht, wenn beide Komplexe mit H_0 übereinstimmen, d.h. $a_i\mathsf{H}_0 = a_i'\mathsf{H}_0$; $b_k\mathsf{H}_0 = b_k'\mathsf{H}_0$ ist. Es ist also der Index von H_0 nach G gleich $\mu\nu$. Ferner ist

$$\begin{array}{rcl} G & = & \mathsf{H}_1 + b_1\mathsf{H}_1 + \cdots + b_\mu\mathsf{H}_1 \quad \text{also} \quad \mu = n_1 \\ & = & \mathsf{H}_2 + a_1\mathsf{H}_2 + \cdots + a_\nu\mathsf{H}_2 \quad \text{||} \quad \nu = n_2 \end{array}$$

da $b_1\mathsf{H}_1 = b_1\mathsf{H}_0 + b_1a_1\mathsf{H}_0 + \cdots + b_1a_\nu\mathsf{H}_0$ von $b_2\mathsf{H}_1 = b_2\mathsf{H}_0 + b_2a_1\mathsf{H}_0 + \cdots + b_2a_\nu\mathsf{H}_0$ verschieden wie oben

312 I

H_0 hat also den Index n_1n_2. Der aus K_1 und K_2 komponierte Körper hat den Grad n_1n_2. Auf Grund des im vorigen Abschnitt bewiesenen Hilfssatzes fallen die Relativnormen der Ideale aus $K_1K_2 = K$ in H_0, K ist einer Untergruppe von H_0 zugeordnet, und da □□□ deren Index $\leqq n_1n_2$ sein muß, ist sie H_0 selbst. K ist also Klassenkörper für H_0.

Bei der Komposition eines Abelschen Körpers K aus Körpern vom Primzahlpotenzgrad $K_1, \ldots, K_s$ können diese nun teilerfremd genommen werden. Ist unser Hauptsatz also für diese Körper bewiesen und sind $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ die Moduln, so folgt durch sukzessive Anwendung der eben ausgeführten Schlußweise, daß K Klassenkörper für den Modul $\mathfrak{m}$, nämlich das kleinste gemeinsame Vielfache der $\mathfrak{m}_i$ ist. □□□ In $\mathfrak{m}$ gehen also nur Teiler der $\mathfrak{m}_i$ auf und in $\mathfrak{m}_i$ nach unserem Hauptsatz nur Teiler der Relativdiskriminante von K_i. In der Relativdiskriminante von K gehen aber nach Satz 10, S. 20▸ *alle* Teiler der $\mathfrak{m}_i$ auf, also in $\mathfrak{m}$ jedenfalls *nur* Teiler der Relativdiskriminante von K.

Wir haben somit unseren Hauptsatz II nur noch für relativ zyklische Körper von Primzahlpotenzgrad zu beweisen. Im Interesse der anzuwendenden vollständigen Induktion beweisen wir gleich den schärferen Satz:

Satz 2. Es sei K relativ zyklisch von Primzahlpotenzgrad ℓ^ν zu k. Dann gibt es stets ein Ideal $\mathfrak{m}$ in k, welches nur die Primideale der Relativdiskriminante von K enthält, und zwar

313 ı

die zu ℓ primen in der ersten Potenz, die Teiler von `[...]` in einer genügend hohen, sodaß K Klassenkörper für eine Klassengruppe vom Index ℓ^ν nach $\mathfrak{m}$ ist.

Ferner gibt es in K ein in $\mathfrak{m}$ aufgehendes Ideal $\mathfrak{M}$ derart, daß wenn die Klassen in K und k nach $\mathfrak{M}$ und $\mathfrak{m}$ (d.h. den Strahlen $\equiv 1 \bmod \mathfrak{M}$ und $\mathfrak{m}$ ev. mit total positiven Zahlen für $\ell = 2$) definiert werden, und σ eine erzeugende Substitution von K ist, jede Klasse von K deren Relativnorm, (die also auch existiert), die Hauptklasse von k ist, die $(1-\sigma)$ te Potenz einer Klasse von K ist. Zu $\mathfrak{m}$ und $\mathfrak{M}$ kann noch ein beliebiger Faktor aus k hinzugezogen werden.

Beweis. Satz 29, S. 225▸ lehrt, daß unser Satz für $\nu = 1$ richtig ist. Wir können also vollständige Induktion anwenden und annehmen, er sei bis $\ell^{\nu-1}$ bewiesen.

K sei nunmehr ein vorgelegter, relativ–zyklischer Körper vom Grade ℓ^ν, σ seine erzeugende Substitution. In K ist ein relativ zyklischer Unterkörper K' vom Grade $\ell^{\nu-1}$ enthalten, der zur Gruppe $\mathfrak{g}$: $(1, \sigma^{\ell^{\nu-1}}, \ldots, \sigma^{(\ell-1)\ell^{\nu-1}})$ vom Index $\ell^{\nu-1}$ gehört. Die Zahlen und Ideale aus K' erleiden, wenn man sie in K [1] betrachtet, durch σ gerade die Substitution, welche die Gruppe von K' erzeugt. Wir können also ruhig σ auch als die erzeugende Substitution in K' betrachten, nur daß bereits $\sigma^{\ell^{\nu-1}}$ den Körper K' nicht ändert. In Bezug auf K' ist K relativ zyklisch vom Primzahlgrad ℓ und der Gruppe $\mathfrak{g}$. Hier ist also $\sigma^{\ell^{\nu-1}}$ die erzeugende Substitution.

314 ı

Die in der Relativdiskriminante von K aufgehenden Primideale mögen mit $\mathfrak{p}$ bezw. $\mathfrak{l}$ bezeichnet werden. Ihre Idealfaktoren in K' und K, deren es auch mehrere geben kann, und die dann *alle* in den Produkten auftreten

[1] undeutlich

sollen, seien mit $\mathfrak{P}', \mathfrak{L}'$ bezw. $\mathfrak{P}, \mathfrak{L}$ bezeichnet. (Dabei braucht aber $\mathfrak{p}, \mathfrak{l}$ in der Relativdiskriminante von K' noch nicht aufzugehen).

Nun ist Satz 2 richtig für K'. Setzen wir also:

$$\mathfrak{m} = \prod \mathfrak{p} \prod \mathfrak{l}^u \cdot \mathfrak{a}; \quad \mathfrak{M}' = \prod \mathfrak{P}' \prod \mathfrak{L}'^{U'} \mathfrak{a},$$

wo $\mathfrak{a}$ ein beliebiges Ideal aus k ist, das für unsere Hauptanwendung gleich 1 zu setzen ist, so ist für genügend großes u und U' folgendes richtig:

Werden in k und K' die Idealklassen nach den Strahlen $\equiv 1 \bmod \mathfrak{m}$ und $\mathfrak{M}'$ (für $\ell = 2$ total positiv) erklärt, so ist K' der Klassenkörper für eine Klassengruppe H' vom Index $\ell^{\nu-1}$ in k nach $\mathfrak{m}$. Die Klassen von K' deren Relativnormen die Hauptklasse nach $\mathfrak{m}$ in k sind, werden durch die symbolischen $(1-\sigma)$ ten Potenzen der Klassen von K' erschöpft.

Die Relativdiskriminante von K nach K' sei nun genau durch $\mathfrak{L}'^{(v+1)(\ell-1)}$ teilbar. Wir denken uns u und U' eventuell noch so vergrößert, daß

$$U' > v; \quad U' = v + n$$

und setzen $$U = (U' - v)\ell + v = v + n\ell$$

Nun bilden wir

$$\mathfrak{M} = \prod \mathfrak{P} \prod \mathfrak{L}^U \mathfrak{a}$$

Dann steht $\mathfrak{M}'$ zu $\mathfrak{M}$ in Bezug auf die beiden Körper

315 I

K' und K in derselben Beziehung, wie in Hilfssatz 3, S. 219 $\mathfrak{m}$ zu $\mathfrak{M}$ für k und K. (aller Überschuß über das dortige kann ja in das dortige $\mathfrak{a}$ gezogen werden).

Erklären wir also in K die Idealklassen nach $\mathfrak{M}$, (für $\ell = 2$ total positiv), so ist K nach Satz 29, S. 225 Klassenkörper zu K' für eine Klassengruppe $\mathfrak{H}'_0$ nach $\mathfrak{M}'$, ferner sind alle Klassen von K, deren Relativnorm nach K' die Hauptklasse von K' ist, symbolische $(1-\sigma^{\ell^{\nu-1}})$ te Potenzen von Klassen in K.

Als Klassengruppe der Relativnormen ist H'_0 offenbar invariant gegenüber der Substitution σ (da auch der Modul nach Konstruktion es ist). Es sei nun C' eine nicht in H'_0 enthaltene Klasse von K'. Da H'_0 den Index ℓ hat und invariant gegen σ ist, ist also auch C'^{σ} nicht in H'_0, also in einer Nebengruppe $C'^{a}\mathsf{H}'_0$ enthalten $(a = 1 \ldots \ell - 1)$. Also ist C'^{σ^2} in $(C'^{\sigma})^a \mathsf{H}'_0 = C'^{a^2}\mathsf{H}'_0, \ldots$ also

$C'^{\sigma^{\ell^{\nu-1}}}$ in der Nebengruppe $C'^{a^{\ell^{\nu-1}}}\mathsf{H}'_0$ enthalten. Da aber K' die Substitution $\sigma^{\ell^{\nu-1}}$ gestattet, ist $C'^{\sigma^{\ell^{\nu-1}}} = C'$, C' also in $C'^{a^{\ell^{\nu-1}}}\mathsf{H}'_0$ enthalten. $C'^{a^{\ell^{\nu-1}}-1}$ ist also in H'_0 enthalten, sodaß $a^{\ell^{\nu-1}} \equiv 1 \bmod \ell$, und demnach wegen $a^{\ell-1} \equiv 1 \bmod \ell$ auch $a \equiv 1 \bmod \ell$, also $a = 1$. Die Klasse C'^{σ} ist also in $C'\mathsf{H}'_0$ enthalten, es liegt somit $C'^{1-\sigma}$ in H'_0.

Nach Voraussetzung über K' liegen somit in H'_0 alle Klassen, deren Relativnormen nach k die Hauptklasse in k sind, d.h. wenn wir es so nennen wollen, das Hauptgeschlecht von K'. In einer Nebengruppe zu H'_0 liegen also immer

316 ı

gleich alle Klassen, welche dieselbe Relativnorm nach k haben. Nun ist aber H'_0 der ℓ–te Teil aller Klassen aus K'. Seien diese

$$\mathsf{H}'_0 + C\mathsf{H}'_0 + \cdots + C^{\ell-1}\mathsf{H}'_0$$

ferner H die Klassengruppe in k, die aus den Relativnormen der Klassen von H'_0 besteht. Sie ist Untergruppe der Gruppe H' aller Relativnormen von K' (als Klassenkörper zu H'). Da C nicht in H'_0 enthalten ist, ist $n(C)$ nicht in H enthalten. Aus $\big(n(C)\big)^a\mathsf{H} = \mathsf{H}$ folgt, daß $\big(n(C)\big)^a$ in H, d.h. $n(C^a)$ in H, d.h. C^a in H'_0 enthalten ist. Es hat demnach H ebenfalls den Index ℓ in Bezug auf H', also den Index ℓ^ν in Bezug auf die Gruppe aller Idealklassen aus k. Die Relativnormen von K nach k, liegen auf dem Umweg über K', d.h. H'_0 in H, da der Index der zugeordneten Klassengruppe den Grad von K nicht übersteigen kann, ist somit diese Klassengruppe H selbst, also K Klassenkörper zu H. Ist G die Gruppe der Idealklassen von k, so ist also nach dem Hauptsatz I die Faktorgruppe $\frac{G}{\mathsf{H}}$ zyklisch vom Grad ℓ^ν.

Um den zweiten Teil des Satzes vollständig zu beweisen, denken wir uns G durch eine Basis dargestellt. Dann kann nicht jede Basisklasse in H enthalten sein. Ist C in H nicht enthalten, so ist erst C^{ℓ^ν} in H enthalten, □□□. Da es sonst noch eine andere nicht in H enthaltene Basisklasse gäbe, und somit $\frac{G}{\mathsf{H}}$ nicht zyklisch wäre. Wie man leicht einsieht, muß die Ordnung von C eine Potenz von ℓ sein, da die Basis aus Element mit Primzahlpotenzordnung gewählt werden darf, und aus

317 ı

$C^{p^k} = 1$; $C^{\ell^\nu} = [\mathsf{H}]$ für $p \neq \ell$ folgen würde $C = [\mathsf{H}]$

Wir stellen G als direktes Produkt der zyklischen Gruppe von C mit einer

Gruppe D dar. Dann ist in leicht verständlicher Abkürzung:

$$G = (C; \mathsf{D}); \quad \mathsf{H} = (C^{\ell^\nu}; \mathsf{D}) \quad \mathsf{H}' = (C^{\ell^{\nu-1}}; \mathsf{D})$$

da H' [2] Untergruppe von $\mathfrak{G}'$ [3] vom Index $\ell^{\nu-1}$, also die gleiche Betrachtung für H' durchgeführt werden kann, und offenbar nicht auf eine neue Basisklasse C führen kann, da H in H' enthalten ist.

Unter D' wollen wir die Gruppe der Klassen von K' verstehen, deren Relativnormen in D fallen.

Wie immer, wollen wir C auch in K' betrachten. n sei die Relativnorm von K' nach k. Es sei C' eine Klasse von K'. Da $n(C')$ in H' liegen muß, sei

$$n(C') = C^{a\ell^{\nu-1}}[\mathsf{D}]$$

und

$$C' = C^a\, U$$

Da $n(C) = C^{\ell^{\nu-1}}$ ist, muß $n(U) = [\mathsf{D}]$ sein, U also in D' liegen. Aus

$$C^a[\mathsf{D}'] = 1$$

folgt

$$C^{a\ell^{\nu-1}}[\mathsf{D}] = 1 \quad \text{also} \quad C^{a\ell^{\nu-1}} = 1$$

Die Ordnung von C in Bezug auf D' in K' ist also der $\ell^{\nu-1}$ te Teil der Ordnung von C in k. Jedenfalls aber ist

$$G' = (C; \mathsf{D}')$$

wo G' die Gruppe aller Idealklassen von K bedeutet.

Nun sei C_0 eine Klasse von K, deren Relativnorm nach k die Hauptklasse in k ist. Unter N sei die Relativnorm von K nach K' verstanden. Nach Annahme über C_0 und K' ist dann:

318 I

$$\mathsf{N}(C_0) = C'^{1-\sigma}$$

wo C' Klasse aus K' ist. Sei nun $C' = C^a[\mathsf{D}']$.

Die Relativnorm von $[\mathsf{D}']$ nach k ist eine Klasse von D, liegt also in H. H ist aber die Gruppe der Relativnormen von H'_0. □□□ Also ist $[\mathsf{D}']$ eine

[2] undeutlich
[3] undeutlich

Klasse aus H_0'. H_0' ist aber die Klassengruppe der Relativnormen von K nach K', also ist $[\mathsf{D}']$ Relativnorm aus K:

$$[\mathsf{D}'] = \mathsf{N}(\mathsf{D}_0); \qquad \mathsf{D}_0 \text{ in } K$$

Wir haben also, da ja C als Klasse von K invariant gegen σ ist

$$C'^{1-\sigma} = \mathsf{N}(\mathsf{D}_0^{1-\sigma}) \quad \text{oder} \quad \mathsf{N}(C_0) = \mathsf{N}(\mathsf{D}_0^{1-\sigma})$$

Nun setzen wir in K

$$C_0 = \mathsf{A}\mathsf{D}_0^{1-\sigma}$$

Dann ist $\mathsf{N}(\mathsf{A}) = 1$, also nach dem früher gesagten

$$\mathsf{A} = \mathsf{B}^{1-\sigma^{\ell^{\nu-1}}}$$

Nun setzen wir:

$$\mathsf{B}^{1+\sigma+\cdots+\sigma^{\ell^{\nu-1}-1}}\mathsf{D}_0 = \mathfrak{K}$$

Dann ist:

$$C_0 = \mathfrak{K}^{1-\sigma} \quad \text{in} \quad K$$

womit der letzte Teil von Satz 2 und somit unser Hauptsatz bewiesen ist.

Den Wert der Exponenten u, mit denen man sicher auskommt, kann man sukzessive leicht bestimmen, da er für $\nu = 1$ genau bekannt ist, nämlich $v+1$.

1.10 Die Primideale in relativ–abelschen Körpern.

319 I

a) Die Primideale der Klassen des Grundkörpers

a.) Die Primideale der Klassen von k.

Hilfssatz. Es sei k irgend ein algebraischer Körper, in dem die Idealklassen nach dem Strahl der total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$ definiert sind. $\mathfrak{p}$ sei ein zu $\mathfrak{m}$ primes Primideal aus der Klasse $\mathfrak{K}$. Ist nun für irgend eine Primzahl ℓ die Klasse $\mathfrak{K}$ die ℓ–te Potenz einer Klasse ist, so gibt es ein Primideal $\mathfrak{q} \neq \mathfrak{p}$, sodaß, wenn man die Idealklassen nach dem Modul $\overline{\mathfrak{m}} = \mathfrak{m}\mathfrak{q}$ statt nach $\mathfrak{m}$ definiert, $\mathfrak{p}$ in einer Klasse liegt, die nicht ℓ–te Potenz einer (neuartigen) Klasse ist.

Beweis. Nach Annahme gibt es ein zu $\mathfrak{m}$ primes ganzes $\mathfrak{j}$, sodaß

$$\mathfrak{p}\mathfrak{j}^{\ell} = (\alpha); \qquad \alpha \text{ tot. pos.} \equiv 1 \bmod \mathfrak{m}.$$

Unter $\mathfrak{r}_i, \varepsilon_i, \varrho_i$ mögen die Ideale und Zahlen verstanden werden, die wir S. 245▸ einführten, die $\mathfrak{r}_i$ mögen zudem prim zu $\mathfrak{p}$ gewählt sein.

Nun betrachten wir die Zahlen:

$$\beta = \alpha^a \varepsilon_1^{x_1} \dots \varrho_{r+\delta}^{x_{r+\delta}} \varrho_1^{y_1} \dots \varrho_t^{y_t}; \qquad 0 \leqq a, x_i, y_i \leqq \ell - 1.$$

Ferner adjungieren wir dem Körper k die ℓ–te Einheitswurzel ζ. Wir fragen, wann eine Zahl β die ℓ–te Potenz einer Zahl A aus $k(\zeta)$ wird. $k(\zeta)$ hat den Relativgrad n zu k, wo n Teiler von $\ell - 1$, also prim zu ℓ ist. Aus $\mathsf{A}^{\ell} = \beta$ folgt durch Normenbildung,

320 I

da β in k liegt, wenn noch $\gamma = n(\mathsf{A})$ gesetzt wird: $\beta^n = \gamma^{\ell}$. Es muß also β^n die ℓ–te Potenz einer Zahl aus k sein. Zunächst muß also in β^n das Primideal $\mathfrak{p}$ in ℓ–ter Potenz aufgehen, also na durch ℓ teilbar, d.h. $a = 0$ sein.

Aus der auf S. 245▸ durchgeführten Diskussion geht nun hervor, daß auch $x_i = y_i = 0$ sein müssen.

Auf Grund von Satz 11, S. 272 gibt es also in $k(\zeta)$ ein zu $\mathfrak{m}, \mathfrak{p}, \mathfrak{r}_i$ primes Ideal $\mathfrak{Q}$ derart, daß in $k(\zeta)$:

$$\left(\frac{\alpha}{\mathfrak{Q}}\right) \neq 1; \quad \left(\frac{\varepsilon_1}{\mathfrak{Q}}\right) = 1; \quad \ldots \quad \left(\frac{\varepsilon_{r+\delta}}{\mathfrak{Q}}\right) = 1; \quad \left(\frac{\varrho_1}{\mathfrak{Q}}\right) = 1; \quad \ldots \quad \left(\frac{\varrho_t}{\mathfrak{Q}}\right) = 1$$

ist; $\mathfrak{q}$ sei das durch $\mathfrak{Q}$ teilbare Primideal aus k, das wir zu $\mathfrak{m}, \mathfrak{p}, \mathfrak{r}_i$ prim annehmen können. Wäre in k

$$x^\ell \equiv \alpha \mod \mathfrak{q}$$

lösbar, dann erst recht in $k(\zeta)$. Also ist α Nichtrest mod $\mathfrak{q}$. Das Primideal $\mathfrak{Q}$ kann auch noch vom ersten Grade genommen werden. Dann ist jede Zahl von $k(\zeta)$ einer Zahl von k kongruent mod $\mathfrak{Q}$ (da auch der Relativgrad 1 ist). Wenn also $\mathsf{A}^\ell \equiv (\varepsilon, \varrho) \bmod \mathfrak{Q}$ ist, wo (ε, ϱ) ein Ausdruck unseres Systems S. 319 ist, eine Kongruenz die nach Bestimmung von $\mathfrak{Q}$ lösbar ist, so sei $\mathsf{A} \equiv \xi \bmod \mathfrak{Q}$. Dann ist $\xi^\ell \equiv (\varepsilon, \varrho) \bmod \mathfrak{Q}$ also mod $\mathfrak{q}$.

Also ist α Nichtrest nach $\mathfrak{q}$, jedes (ε, ϱ) aber Rest. Wir setzen nun $\overline{\mathfrak{m}} = \mathfrak{m}\mathfrak{q}$ und definieren die Idealklassen in k nach $\overline{\mathfrak{m}}$. $\mathfrak{p}$ liege in $\overline{\mathfrak{K}}$. Wäre $\overline{\mathfrak{K}}$ die ℓ–te Potenz einer Klasse nach $\overline{\mathfrak{m}}$, so gäbe es

321 I

ein zu $\overline{\mathfrak{m}}$ primes, ganzes $\mathfrak{a}$, sodaß

$$\mathfrak{p}\mathfrak{a}^\ell = (\overline{\alpha}); \qquad \overline{\alpha} \text{ tot.pos.} \equiv 1 \bmod \overline{\mathfrak{m}}$$

wäre. Also

$$(\alpha) = \mathfrak{p}\mathfrak{j}^\ell = (\overline{\alpha})\left(\frac{\mathfrak{j}}{\mathfrak{a}}\right)^\ell$$

Dann ist also $\left(\frac{\mathfrak{j}}{\mathfrak{a}}\right)^\ell$ ein Hauptideal (β), welches die ℓ–te Potenz des Ideals $\mathfrak{b} = \frac{\mathfrak{j}}{\mathfrak{a}}$ ist. Stellt man $\mathfrak{b}$ in der Form (1) von S. 244 dar, so sieht man, wie beim Beweise an jener Stelle (etwas später S. 248), daß $(\beta) = \mathfrak{b}^\ell$ eine Zahl der Form $(\varepsilon, \varrho)\xi^\ell$ ist. Es hat also auch α diese Form:

$$\alpha = \overline{\alpha}(\varepsilon, \varrho)\xi^\ell$$

da alle Einheiten in (ε, ϱ) hineingezogen werden können.

Nun ist $\overline{\alpha} \equiv 1 \bmod \mathfrak{q}$, also $\overline{\alpha}$ und auch $(\varepsilon, \varrho)\xi^\ell$ ℓ–te Potenzreste mod $\mathfrak{q}$, es wäre also auch α ein solcher, was falsch ist. $\overline{\mathfrak{K}}$ ist also nicht ℓ–te Potenz einer

Klasse nach $\overline{\mathfrak{m}}$.

Satz 1. Ist K relativ zyklisch vom Primzahlgrad ℓ^ν und Klassenkörper für die Gruppe H, so zerfallen von den zur Relativdiskriminante primen Primidealen in k alle und nur die in H enthaltenen in K in ℓ^ν verschiedene Primideale ersten Relativgrades.

Beweis. 1.) Zerfällt $\mathfrak{p}$ in ℓ^ν verschiedene Primideale ersten Relativgrades (ist also prim zur Relativdiskriminante), so ist es Relativnorm eines Primideals in K, also, wenn H nach einem Modul $\mathfrak{m}$ erklärt wird, der nur Teiler der Rel. Diskr. enthält, in H enthalten, nach Definition des Klassenkörpers.

2.) Sei $\mathfrak{p}$ ein zur Relativdiskriminante primes Primideal aus H und H nach einem zu $\mathfrak{p}$ primen Modul $\mathfrak{m}$ erklärt, (was nach Hauptsatz II möglich), der außerdem nach unserm Hilfssatz so gewählt werden darf, daß die Klasse C von $\mathfrak{p}$ nach dem Strahl $\equiv 1 \bmod \mathfrak{m}$ (total positiv) nicht die ℓ–te Potenz einer Klasse ist.

Dann hat die Klassengruppe $C^i\mathfrak{K}^\ell$, wo $\mathfrak{K}$ alle Klassen durchläuft und $i = 0, 1, \ldots, \ell - 1$ ist, sicher den Rang 1. Für die Klassengruppe G aller Idealklassen gibt es also sicher eine Rangbasis, die C als Basiselement enthält. Läßt man C aus, so erhält man eine Klassengruppe H' vom Index ℓ, welche C nicht enthält. Erst C^ℓ ist wieder in H' enthalten. Also:

$$G = \mathsf{H}' + C\mathsf{H}' + \cdots + C^{\ell-1}\mathsf{H}'$$

Da C in H liegt, ist also „Vereinigungsgruppe“ $(\mathsf{H}, \mathsf{H}') = G$. $\frac{G}{\mathsf{H}}$ ist zyklisch vom Grad ℓ^ν. Sei etwa:

$$G = \mathsf{H} + \mathsf{A}\mathsf{H} + \cdots + \mathsf{A}^{\ell^{[\ldots]}-1}\mathsf{H}$$

Unter H_0 werde der Durchschnitt von H und H' verstanden. □□□ H ist dadurch charakterisiert, daß es alle Elemente aus G, außer dem Zyklus (A) (und den daraus sich ergebenden Elementen) enthält; ebenso H' den Zyklus (C). Ferner ist H nicht Untergruppe zu H', da H' das in H enthaltene C nicht enthält. Also ist H_0 dadurch charakterisiert, daß es alle Elemente von G bis auf die Zyklen (A) und (C) enthält, d.h.

$$\mathsf{H} = \sum_{i=0}^{\ell-1} \mathsf{H}_0 C^i; \quad \mathsf{H}' = \sum_{i=0}^{\ell^\nu-1} \mathsf{H}_0 \mathsf{A}^i; \quad G = \sum_{i=0}^{\ell-1} \sum_{k=0}^{\ell^\nu-1} \mathsf{H}_0 C^i \mathsf{A}^k$$

(C kann im Durchschnitt H, H' nicht enthalten sein, jedes andere Element von H, das nicht C^i enthält aber sicher nach Definition von H', also gilt die erste Zerlegung; durch Einsetzen in $G = \mathsf{H} + \mathsf{A}\mathsf{H} + \cdots$ folgt die dritte, daraus durch Vergleich mit $G = \mathsf{H}' + C\mathsf{H}' + \cdots$ die zweite).

323 ı

H_0 hat also den Index $\ell^{\nu+1}$.

Sei nun K' der Klassenkörper für H'. Wäre K' Unterkörper von K, so müßte H Untergruppe von H' sein, was eben als unmöglich erkannt. Da weiter K' den Primzahlgrad ℓ hat, sind K' und K teilerfremd, der komponierte Körper KK' also vom Grad $\ell^{\nu+1}$. Die Relativnormen seiner Ideale fallen nach Satz 7, S. 306▸ in H_0. Da H_0 den Index $\ell^{\nu+1}$ hat, also KK' nicht einer Untergruppe von H_0 zugeordnet sein kann, ist KK' Klassenkörper zu H_0.

Nach Hauptsatz II ist es möglich den Modul $\mathfrak{m}$ durch Hinzunahme von Teilern der Relativdiskriminante von KK' □□□ so zu erweitern, daß auch jeder Unterkörper von KK' Klassenkörper nach $\mathfrak{m}$ ist (die Relativdiskriminante von KK' ist ja teilbar durch die sämtlichen Unterkörper). Die Relativdiskriminante von KK' ist ferner prim zu $\mathfrak{p}$, da sie mit dem Führer der Klassengruppe H_0 in Bezug auf ihre Teiler übereinstimmt (Satz 1, S. 310▸), und dieser Führer von H_0 sicher teilbar ist durch den Modul $\mathfrak{m}$, nach dem die Obergruppe H erklärt war, und der prim zu $\mathfrak{p}$ war.

Wir denken uns also $\mathfrak{m}$, prim zu $\mathfrak{p}$ in der angegebenen Weise erweitert.

Die Gruppe von KK' ist, da beide teilerfremd, gleich dem direkten Produkt der Gruppen von K und K'. Man kann sie also darstellen:

$$\sigma_1^a \sigma_2^b; \quad 0 \leqq a \leqq \ell^\nu - 1; \quad 0 \leqq b \leqq \ell - 1.$$

Dann gehört K zur Gruppe σ_2^b, K' zur Gruppe σ_1^a. Da $\mathfrak{p}$ nicht in der Relativdiskriminante von KK' aufgeht, ist die Trägheitsgruppe die identische, die Zerlegungsgruppe $\mathfrak{G}_Z$[1] also

324 ı

zyklisch. K_Z sei der Zerlegungskörper für $\mathfrak{p}$ in KK'. In K_Z zerfällt $\mathfrak{p}$ in verschiedene Primideale ersten Relativgrades. Ist K_Z Klassenkörper für die Gruppe H_1, so ist also die Klasse C in H_1 enthalten, nach dem unter 1.) gezeigten. Da ferner K_Z Unterkörper von KK' ist, ist die Gruppe H_0 in H_1 enthalten, (als Gruppe der Relativnormen über K_Z von KK'). Daher ist auch

[1] Subskripte '2' und 'Z' schwer unterscheidbar

$\mathsf{H} = \sum \mathsf{H}_0 C^i$ in H_1 enthalten, sodaß nach Satz 9, S. 144 K_Z Unterkörper von K ist. Ist ℓ^μ der Relativgrad von K nach K_Z, so gehört also, da nach dem Gesagten σ_2^b Untergruppe der Gruppe $\mathfrak{G}_Z$ sein muß, zu der K_Z gehört, K_Z zu einer Gruppe $\mathfrak{G}_Z = \sigma_1^{a\ell^{\nu-\mu}}\sigma_2^b$; $0 \leqq a \leqq \ell^\mu - 1$; $0 \leqq b \leqq \ell - 1$.

Da aber $\mathfrak{G}_Z$, wie gezeigt, zyklisch sein muß, folgt, daß $\mu = 0$; $\mathfrak{G}_Z = \sigma_2^b$; $K_Z = K$ ist. Da $\mathfrak{p}$ in K_Z zerfällt, gilt dies auch für K, und zwar des Grades wegen in ℓ^ν Primideale ersten Grades.

Satz 2. Sei K ein beliebiger relativ Abelscher Körper über k, der Klassenkörper für die Gruppe H mit dem Führer $\mathfrak{m}$ ist. Dann zerfallen in K alle und nur die in H enthaltenen Primideale von K in lauter verschiedene Primideale ersten Relativgrades.

Beweis. 1.) Zerfällt $\mathfrak{p}$ in dieser Weise, so ist es prim zur Relativdiskriminante, also zu $\mathfrak{m}$; ferner ist $\mathfrak{p} = n(\mathfrak{P})$ also nach Definition des Klassenkörpers in H enthalten.

2.) Wir stellen $\frac{G}{\mathsf{H}}$, wo G die Gruppe aller Klassen nach $\mathfrak{m}$ ist, durch eine Basis dar, und setzen K, wie beim Beweis des Hauptsatzes I aus den relativ zyklischen Körpern $K_1, \ldots, K_s$ von Primzahlpotenzgrad zusammen (S. 307 f). Diese seien Klassenkörper für $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_s$. Dann ist, wie dort, H der Durchschnitt von $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_s$. Ein in H enthaltenes, zu $\mathfrak{m}$

primes Primideal $\mathfrak{p}$, liegt also in allen H_i und ist zu den Einzelrelativdiskriminanten prim, da diese nur Teiler von $\mathfrak{m}$ enthalten können. Daher zerfällt $\mathfrak{p}$ nach dem vorigen Satz in allen K_i in lauter verschiedene Primideale ersten Relativgrades. $\mathfrak{G}_Z$ sei die Zerlegungsgruppe von $\mathfrak{p}$ in K. Wir wenden Satz 21, S. 50 an: In den dortigen Bezeichnungen ist hier, wenn K als Oberkörper, K_i als Unterkörper genommen wird, $f' = 1$; $e = \overline{e} = a = 1$; $f = \overline{f}$. Da $\mathfrak{G}_Z$ vom Grade $ef = f$, $\overline{\mathfrak{G}}_Z$ vom Grade $\overline{e}\,\overline{f} = \overline{f} = f$ und $\overline{\mathfrak{G}}_Z/\mathfrak{G}_Z$ ist, folgt $\mathfrak{G}_Z = \overline{\mathfrak{G}}_Z$. $\mathfrak{G}_Z$ ist also Untergruppe zu der Gruppe $\overline{\mathfrak{G}}$, zu der K_i gehört, der Zerlegungskörper K_Z somit Oberkörper aller K_i, und somit K selbst: $K_Z = K$, sodaß $\mathfrak{p}$ in K in lauter Primideale ersten Relativgrades zerfällt, w.z.b.w.

Hauptsatz III. K sei relativ Abelsch zu k und Klassenkörper für die Klassengruppe H mit dem Führer $\mathfrak{m}$. Die Idealklassen in k seien nach H definiert (Klasse=Nebengruppe zu H). h sei die entsprechende Klassenzahl (Index von H), also auch der Grad von K. $\mathfrak{K}$ sei eine Idealklasse in diesem Sinne, sodaß erst $\mathfrak{K}^f = \mathsf{H}$ ist, und $h = ef$. Dann zerfällt jedes (zu $\mathfrak{m}$ prime) in $\mathfrak{K}$ enthaltene

Primideal von k in K in e verschiedene Primideale f–ten Rel. Grades.

Beweis. Für $\mathfrak{K} = \mathsf{H}$ ist der Satz identisch mit Satz 2. Sei $\mathfrak{p}$ in der Klasse $\mathfrak{K}$ enthalten, K_Z der Zerlegungskörper von $\mathfrak{p}$ in K. K_Z sei Klassenkörper für die Gruppe H_1. Dann ist die Gruppe H (als Relativnormgruppe von K) in H_1 enthalten (der Modul läßt sich wieder entsprechend wählen, wie S. 323▸). Da $\mathfrak{p}$ in K_Z in verschiedene Primideale ersten Relativgrades zerfällt, ist auch

326 ı

$\mathfrak{p}$ und somit □□□ $\mathfrak{p} \cdot \mathsf{H} = \mathfrak{K}$ in H_1 enthalten.

H_1 enthält also sicher die Gruppe:

$$\mathsf{H}_2 = \mathsf{H} + \mathfrak{K}\mathsf{H} + \cdots + \mathfrak{K}^{f-1}\mathsf{H}$$

K_Z ist also Unterkörper des zu H_2 gehörigen Klassenkörpers. Da in diesem, weil $\mathfrak{p}$ in H_2 enthalten ist, $\mathfrak{p}$ in verschiedene Primideale ersten Relativgrades zerfällt (Satz 2), muß nach Satz 23, S. 51▸ dieser Körper Unterkörper zu K_Z, also nach dem eben gezeigten $= K_Z$ sein. Es ist also $\mathsf{H}_1 = \mathsf{H}_2$. H hat den Index h die Gruppe H_1 also den Index $\frac{h}{f} = e$. Der Grad von K_Z ist also e; der Grad der Zerlegungsgruppe muß so beschaffen sein, daß ihr Index in Bezug auf die ganze Galoissche Gruppe von K vom Grade h gleich dem Grade des Körpers ist, der zu ihr gehört, also gleich dem Grade e von K_Z. Somit ist f der Grad der Zerlegungsgruppe. Die Trägheitsgruppe ist 1, da $\mathfrak{p}$ kein Teiler der Relativdiskriminante. Folglich ist der Index der Trägheitsgruppe zur Zerlegungsgruppe, der den Grad der Primideale von $\mathfrak{p}$ angibt, gleich f und $\mathfrak{p}$ zerfällt somit in e verschiedene Primideale f–ten Grades.

An dieser Stelle können wir gleich die wichtige Frage behandeln, ob es in jeder Idealklasse eines Körpers k unendlich viele Primideale gibt.

Zu diesem Zweck kehren wir zu Satz 6, S. 141▸ zurück. Es sei K der Klassenkörper für die Gruppe H und h die Anzahl der Idealklassen nach H. Dann ist h auch der Grad von K. Wenn $\mathfrak{p}$ die Primideale ersten Grades durchläuft, welche in K in Primideale ersten Relativgrades zerfallen, was gleichbedeutend damit ist, daß $\mathfrak{p}$ die Primideale von H durchläuft, so ist nach dem genannten Satz:

327 ı

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{h} \log \frac{1}{s-1} + \psi(s); \qquad \psi(s) \text{ endlich für } s \to 1$$

Demnach ist jetzt die Aussage von Satz 4, S. 140 präziser so auszusprechen, daß die dort $\varphi(s)$ genannte Funktion tatsächlich für $s = 1$ endlich bleibt.

Nach dem Beweise S. 139 ist nunmehr zu schließen, daß die Funktion $(s-1)L(s,\chi_1)\cdots L(s,\chi_k)$ für $s \to 1$ einem endlichen, *von Null verschiedenen* Wert zustrebt. Nach Satz 2 S. 136, sind also die □□□ Werte $L(1,\chi_i)$ für die Nichthauptcharaktere $\neq 0$. Damit haben wir:

Satz 3. Ist χ ein vom Hauptcharakter verschiedener Klassencharakter, so strebt die L–Reihe $L(s,\chi)$ für $s = 1$ einem endlichen, von Null verschiedenen Wert zu, es ist also $L(1,\chi) \neq 0$.

Nun haben wir $L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathsf{N}(\mathfrak{a})^s}$ und

$$\log L(s,\chi) = +\sum_{\mathfrak{p},m} \frac{\chi(\mathfrak{p}^m)}{m\mathsf{N}(\mathfrak{p})^{sm}}$$

wo über alle zum Modul $\mathfrak{m}$ primen Ideale bezw. Primideale zu summieren ist.

Ist nun $\mathfrak{K}$ eine vorgegebene Idealklasse nach H und durchläuft χ alle Charaktere von $\frac{G}{\mathsf{H}}$, so ist:

$$F_{\mathfrak{K}}(s) = \sum_{\chi} \chi(\mathfrak{K}^{-1}) \log L(s,\chi) = \sum_{\mathfrak{p},m} \frac{\sum_{\chi} \chi(\mathfrak{K}^{-1})\chi(\mathfrak{p}^m)}{m\mathsf{N}(\mathfrak{p})^{sm}}$$

Da nun $\sum_{\chi} \chi(\mathfrak{K}^{-1}\mathfrak{p}^m) = \left\{ \begin{array}{ccc} 0 & \text{für} & \mathfrak{p}^m \text{ in } \mathfrak{K} \\ h & \text{=} & \mathfrak{p}^m \text{ nicht in } \mathfrak{K} \end{array} \right\}$ ist folgt

$$F_{\mathfrak{K}}(s) = \sum_{\mathfrak{p}^m \text{ aus } \mathfrak{K}} \frac{h}{m\mathsf{N}(\mathfrak{p})^{sm}}$$

In $F_{\mathfrak{K}}(s)$ wird nach Satz 3 nur das Glied mit dem Hauptcharakter für $s \to 1$ singulär. Da ferner nach Satz 2, S. 136

$$\lim_{s=1}(s-1)L(s,\chi_1) = gh \neq 0$$

ist, folgt, daß

$$\square\square\square \qquad F_{\mathfrak{K}}(s) = \log\frac{1}{s-1} + \varphi(s); \qquad \varphi(s) \text{ endlich für } s \to 1$$

ist. Von der Reihe rechts bleibt, wie S. 138 ff mehrfach ausgeführt

$$\sum_{\substack{\mathfrak{p}^m \text{ aus } \mathfrak{K} \\ m \geqq 2}} \frac{h}{m\mathsf{N}(\mathfrak{p})^{ms}} \qquad \text{für } s \to 1 \qquad \text{endlich.}$$

Also wird:

$$\sum_{\mathfrak{p}|\mathfrak{K}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{h}\log\frac{1}{s-1} + \psi(s); \qquad \psi(s) \text{ endlich für } s \to 1,$$

und daraus folgt, daß unendlich viele $\mathfrak{p}$ in $\mathfrak{K}$ liegen müssen.

Satz 4. Die Idealklasse $\mathfrak{K}$ sei auf irgendeine der möglichen Weisen erklärt. Dann liegen in $\mathfrak{K}$ unendlich viele Primideale, sogar ersten Grades.

Als wichtigsten Fall, der alle anderen einschließt haben wir, daß in jeder Idealklasse nach dem Strahl der total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$ für irgend ein $\mathfrak{m}$ (auch $\mathfrak{m} = 1$) unendlich viele Primideale ersten Grades liegen.

Es sei, um einen speziellen Fall zu besprechen, β eine zu $\mathfrak{m}$ prime Zahl. Dann bildet die Gesamtheit aller Zahlen $\beta' \equiv \beta \bmod \mathfrak{m}$ und von gleicher Signatur, wenn man sie als Hauptideale betrachtet, eine Klasse nach dem Strahl der total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$. Unter den Hauptidealen (β') müssen also unendlich viele Primideale vorhanden sein, die dann gleichzeitig Primzahlen sind. Wir haben also

329 I

Satz 5. Ist $\mathfrak{m}$ ein gegebener Modul, β eine zu $\mathfrak{m}$ prime Zahl, so liegen in der Restklasse $\beta' \equiv \beta \bmod \mathfrak{m}$ unendlich viele Primzahlen π des Körpers, welche gleiche Signatur wie β haben. Da innerhalb einer Restklasse jede Signatur vorkommt, gibt es also in jeder primen Restklasse nach $\mathfrak{m}$ unendlich viele Primzahlen jeder Signatur. Ihr Grad kann sogar noch gleich 1 angenommen werden, sodaß $\mathsf{N}(\pi) = \pm p$ eine natürliche Primzahl ist. Wählt man die Signatur total positiv, so ist $\mathsf{N}(\pi) = +p$. Ist k der rationale Körper, so ist dies der Satz von der arithmetischen Progression.

330 I

b) Die Zetafunktion des Klassenkörpers

Unter $\mathfrak{k}$ verstehen wir im Folgenden Idealklassen definiert nach dem Strahl der total positiven Zahlen $\equiv 1 \bmod \mathfrak{m}$, unter $\mathfrak{K}$ die Klassen nach einer Klassengruppe H.□□□

Sei K relativ Abelsch zu k und Klassenkörper für die Gruppe H nach dem Führer $\mathfrak{m}$.

$$\zeta_K = \prod \frac{1}{1 - \mathsf{N}(\mathfrak{P})^{-s}}\,; \quad (\mathsf{N} \text{ die Norm im absoluten Sinne})$$

sei die ζ–Funktion von K. (n sei die Norm in k im absoluten Sinne). $\mathfrak{p}$ sei ein zu $\mathfrak{m}$ primes Primideal von k der Klasse $\mathfrak{K}$, f der Exponent von $\mathfrak{K}$. Dann ist in K:

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_e; \quad ef = h; \quad (h = \text{Index von } \mathsf{H})$$

sodaß zu unserem Produkte von $\mathfrak{p}$ der Beitrag

$$\prod_{i=1}^{e} \frac{1}{1 - \mathsf{N}(\mathfrak{P}_i)^{-s}} = \prod_{i=1}^{e} \frac{1}{1 - n(\mathfrak{p})^{-fs}} = \prod_{\nu=0}^{f-1} \left(\frac{1}{1 - \varepsilon^\nu n(\mathfrak{p})^{-s}} \right)^e$$

geliefert wird, wo ε eine primitive f–te Einheitswurzel ist. χ durchlaufe die Charaktere der Gruppe aller Klassen $\mathfrak{K}$ nach H. Diejenigen, für die $\chi(\mathfrak{K}) = 1$, also $\chi = 1$ für die Gruppe $1, \mathfrak{K}, \dots, \mathfrak{K}^{f-1}$ ist, sind die zu dieser Gruppe *gehörigen* Charaktere in der Anzahl $\frac{h}{f} = e$.
□□□

Demnach haben immer genau e Charaktere für $\mathfrak{K}$ denselben Wert, sodaß es genau f verschiedene Werte $\chi(\mathfrak{K})$ gibt. Andererseits ist $\big(\chi(\mathfrak{K})\big)^f = 1$. $\chi(\mathfrak{K})$ nimmt also jede f–te Einheitswurzel ε^ν genau e–mal an.

(Genauer Begründung: Die Forderung $\chi(\mathfrak{K}) = 1$, also auch $\chi(\mathfrak{K}^i) = 1$, definiert eine Untergruppe der Charakterengruppe, die so beschaffen ist, daß sie für die ganze Untergruppe $1, \mathfrak{K}, \dots, \mathfrak{K}^{f-1}$ den Wert 1 liefert; also für jede Nebengruppe den gleichen Wert. □□□ An Hand der charakteristischen Eigenschaften der Charaktere ergibt sich dann, ähnlich wir S. 231▸, daß diese Charakterenuntergruppe mit der Faktorgruppe zu $1, \mathfrak{K}, \dots, \mathfrak{K}^{f-1}$ isomorph ist, also den Grad e hat.)

Damit können wir also den Beitrag des Primideals $\mathfrak{p}$ zu unserem Produkt so schreiben:

$$\prod_{\chi} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathsf{N}(\mathfrak{p})^s}}$$

wo χ alle Charaktere der Gruppe der Klassen nach H durchläuft.

Um nun auch die Beiträge der in $\mathfrak{m}$ aufgehenden Primideale zu bestimmen, haben wir den Begriff des eigentlichen Charakters einzuführen.

Es sei χ ein Charakter der Klassen $\mathfrak{k}$ nach $\mathfrak{m}$, H_1 die Klassengruppe zu der χ gehört, d.h. die Menge der Klassen, für die $\chi(\mathfrak{k}) = 1$ ist.

H_1 sei Klassengruppe für den Führer $\mathfrak{m}_1$, wo $\mathfrak{m}_1$ ein Teiler von $\mathfrak{m}$ ist. Da die Konstitution der Klassen nach H_1 und $\mathfrak{m}_1$ dieselbe ist, wie nach H_1 und $\mathfrak{m}$, gibt es einen Charakter $\overline{\chi}$ nach H_1 und $\mathfrak{m}_1$, der für die

zu $\mathfrak{m}$ primen Ideale mit χ übereinstimmt, und zwar nur einen, da es in jeder Klasse nach H_1 und $\mathfrak{m}_1$ zu $\mathfrak{m}$ prime Ideale gibt, oder besser, da in jeder Klasse nach H_1 und $\mathfrak{m}_1$ genau eine Klasse nach H_1 und $\mathfrak{m}$ enthalten ist. Dieser Charakter $\overline{\chi}$ heißt der dem Charakter χ zugeordnete eigentliche Charakter. Sollte nun $\mathfrak{p}$ in $\mathfrak{m}$, aber nicht in $\mathfrak{m}_1$ aufgehen, so ist also $\overline{\chi}(\mathfrak{p})$ eindeutig bestimmt.

Der Bequemlichkeit halber wollen wir also festsetzen:

Definition 1. Sei χ ein Charakter nach $\mathfrak{m}$, $\overline{\chi}$ der zu χ gehörige eigentliche Charakter mit dem Führer $\mathfrak{m}_1$. Für jedes Ideal $\mathfrak{a}$, für das nach unseren bisherigen Festsetzungen $\overline{\chi}(\mathfrak{a})$ definiert ist, soll $\chi(\mathfrak{a}) = \overline{\chi}(\mathfrak{a})$ gesetzt werden. Für jedes Ideal aber, für das $\overline{\chi}$ nicht definiert ist, (das also nicht prim zu $\mathfrak{m}_1$ ist), soll $\chi(\mathfrak{a}) = 0$ gesetzt werden. $\mathfrak{m}_1$ heißt der Führer des Charakters χ. Er ist Teiler von $\mathfrak{m}$. χ ist so für jedes zum Führer $\mathfrak{m}_1$ prime Ideal $\mathfrak{a}$ erklärt. Für die zu $\mathfrak{m}$ primen Ideale fällt unsere Definition mit der bisher benutzten zusammen.

Nun kehren wir zum Körper K zurück. $\mathfrak{p}$ sei ein in $\mathfrak{m}$ aufgehendes Primideal, also da $\mathfrak{m}$ der Führer von H ist, Teiler der Relativdiskriminante von K.

K_T sei der Trägheitskörper von $\mathfrak{p}$. Er sei Klassenkörper für die Gruppe H_T, die H enthält. Da $\mathfrak{p}$ nicht in der Relativdiskriminante von K_T aufgeht, ist der Führer $\mathfrak{m}_1$ von H_T prim zu $\mathfrak{p}$ und Teiler von $\mathfrak{m}$, da H_T auch Gruppe nach $\mathfrak{m}$ ist.

Sei nun χ ein Charakter nach H und $\chi(\mathfrak{p}) \neq 0$. χ gehört zu einer Gruppe $\overline{\mathsf{H}}$, die H zur Untergruppe hat. Da $\chi(\mathfrak{p}) \neq 0$, ist der Führer $\overline{\mathfrak{m}}$ von $\overline{\mathsf{H}}$ prim zu $\mathfrak{p}$. Der zu $\overline{\mathsf{H}}$ gehörige Klassenkörper $\overline{K}$ ist einerseits, da H Untergruppe zu $\overline{\mathsf{H}}$ Unterkörper von K. In der Relativdiskriminante von $\overline{K}$ geht $\mathfrak{p}$ nicht auf, da es prim zu $\overline{\mathfrak{m}}$ ist. Nun ist aber nach Satz 22, S. 51 K_T der größte Unterkörper, in dem noch $\mathfrak{p}$ in lauter verschiedene Primideale zerfällt. Also muß $\overline{K}$ Unterkörper von K_T, also H_T Untergruppe zu $\overline{\mathsf{H}}$ sein. χ ist also ein Charakter nach H_T. Daß umgekehrt für jeden Charakter nach H_T, der, da H Untergruppe von H_T ist, auch Charakter nach H ist, $\chi(\mathfrak{p}) \neq 0$ ist, folgt daraus, daß $\mathfrak{m}_1$ prim zu $\mathfrak{p}$ ist.

In K_T lautet also der Beitrag zur Zetafunktion von K_T:

$$\prod_{\chi \text{ nach } \mathsf{H}_T} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{n(\mathfrak{p})^s}}$$

Da aber nach dem gezeigten für jeden nicht zu H_T gehörigen Charakter $\chi(\mathfrak{p}) = 0$ ist, kann man dies auch so schreiben:

$$\prod_{\chi} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{n(\mathfrak{p})^s}}$$

wo χ alle Charaktere nach H durchläuft. Ein Primideal von K hat aber den ersten Relativgrad nach K_T und die Primideale von K_T sind Potenzen der Primideale von K. Es ist also der Beitrag aus K:

$$\prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathsf{N}(\mathfrak{P})^s}} = \prod_{\mathfrak{P}_T|\mathfrak{p}} \frac{1}{1 - \frac{1}{n_T(\mathfrak{P}_T)^s}}$$

wo $\mathfrak{P}$ alle Primteiler von $\mathfrak{p}$ in K, $\mathfrak{P}_T$ alle Primteiler von $\mathfrak{p}$ in

K_T und n_T die Norm in K_T bezeichnet, und letzteres ist gerade der Beitrag zur ζ–Funktion in K_T. Es ist also demnach unser Ausdruck $\prod_{\chi} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{n(\mathfrak{p})^s}}$ in allen Fällen der gewünschte Beitrag und somit

$$\zeta_K(s) = \prod_{\chi} \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{n(\mathfrak{p})^s}}$$

wo χ über alle Charaktere nach H, $\mathfrak{p}$ über alle Primideale von k zu erstrecken ist. Oder:

$$\zeta_K(s) = \prod_{\chi} \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{n(\mathfrak{a})^s} = \prod_{\chi} L(s, \chi)$$

wo $L(s, \chi)$ die zum Charakter χ gehörige L–Reihe ist (allerdings nicht mehr im früheren Sinne). Im früheren Sinne ist es eine L–Reihe für den zugeordneten eigentlichen Charakter $\overline{\chi}$ nach dem Führer $\mathfrak{m}_1$.

Satz 6. Es sei der □□□ relativ Abelsche Körper K Klassenkörper für die Gruppe H mit dem Führer $\mathfrak{m}$. χ durchlaufe alle Charaktere nach der Gruppe H im Sinne der Definition 1 (eigentlich also immer die zugehörigen eigentlichen Charaktere). $L(s, \chi)$ sei die damit gebildete L–Reihe. Dann gilt für die Dedekind'sche ζ–Funktion von K:

$$\zeta_K(s) = \prod_{\chi} L(s, \chi).$$

c) Kennzeichnung d. Klassenkörpers durch Primzerlegung

c.) Umkehrung von Satz 2.

Satz 7. Es sei K ein Relativkörper vom Grade n über k. $\mathfrak{p}_0$ durchlaufe die Primideale ersten Grades von k, welche in K als Faktor wenigstens ein Primideal ersten Grades $\mathfrak{P}$ aufweisen. Wenn dann, von einer endlichen Anzahl von Ausnahmen abgesehen, die $\mathfrak{p}_0$ in lauter Primideale ersten Grades in K zerfallen, ist K relativ–Galoissch zu k.

Beweis. Es ist, wie mehrfach ausgeführt,

$$\zeta_K(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \mathsf{N}(\mathfrak{P})^{-s}} \cdot \psi(s),$$

wo $\mathfrak{P}$ alle Primideale ersten Grades von K mit endlich vielen Ausnahmen durchläuft und $\psi(s)$ endlich bleibt für $s = 1$ und $\neq 0$ ist.

Nach Annahme also:

$$\zeta_K(s) = \prod_{\mathfrak{p}_0} \left(\frac{1}{1 - n(\mathfrak{p}_0)^{-s}} \right)^n \varphi(s)$$

Da $\lim\limits_{s=1}(s-1)\zeta_K(s)$ endlich und $\neq 0$ ist, ist:

$$\lim_{s=1}(s-1)^{\frac{1}{n}} \prod_{\mathfrak{p}_0} \left(\frac{1}{1 - n(\mathfrak{p}_0)^{-s}} \right)$$

endlich und $\neq 0$.

Für den relativ konjugierten Körper K' erfüllen die Primideale $\mathfrak{p}_0$ die gleiche Voraussetzung, somit auch für den aus allen konjugierten zusammengesetzten relativ–Galoisschen Körper $\overline{K}$, denn wenn $\mathfrak{p}_0$ in $\overline{K}$ in lauter Primideale ersten Grades zerfällt, dann auch in K. Zerfällt es aber in K, dann auch in jedem $K^{(i)}$. Alle $K^{(i)}$ sind also Unterkörper des Zerlegungskörpers für jeden Faktor in $\overline{K}$. $\overline{K}$ selbst ist also der Zerlegungskörper, woraus alles folgt. Ist also $\overline{n}$ der Relativgrad von $\overline{K}$, so ist auch

$$\lim_{s=1}(s-1)^{\frac{1}{n}} \prod_{\mathfrak{p}_0} \frac{1}{1 - n(\mathfrak{p}_0)^{-s}} \qquad \text{endlich} \neq 0.$$

Das geht nur für $n = \overline{n}$, $K = \overline{K}$. K ist also relativ–Galoissch.

Es sei nun H eine Klassengruppe vom Index h für k.

Ferner sei K ein Relativkörper mit folgenden Eigenschaften:

1.) die Primideale ersten Grades $\mathfrak{p}_0$ von H sollen in K in lauter Primideale ersten Grades zerfallen, bis auf endlich viele Ausnahmen.

2.) Jedes Primideal von k, das in K einen Faktor ersten Relativgrades aufweist, und vom ersten Grade ist, soll bis auf endlich viele Ausnahmen in H enthalten sein.

Der Klassenkörper für H ist z.B. ein solcher Körper. Wir wollen zeigen, daß er der einzige ist.

Aus 1.) 2.) folgt zunächst nach Satz 7, daß K relativ–Galoissch ist. Ist n der Relativgrad von K und durchläuft $\mathfrak{p}$ die Primideale ersten Grades von H

(endlich viele Ausnahmen sind belanglos), so ist nach Satz 6, S. 141, Satz 5, S. 140 und dem Beweise von Satz 3, S. 327 oben

$$\sum_{\mathfrak{p}} \frac{1}{\mathsf{N}(\mathfrak{p})^s} = \frac{1}{n} \log \frac{1}{s-1} + \psi(s) = \frac{1}{h} \log \frac{1}{s-1} + \varphi(s)$$

wo $\psi(s)$ und $\varphi(s)$ endlich bleiben für $s \to 1$. Also ist $n = h$. Der Relativgrad von K also h.

Ist ferner K_1 der Klassenkörper zu H, der die gleiche Eigenschaft hat, die wir von K voraussetzen, so hat KK_1, wie schon oft gezeigt, dieselbe Eigenschaft, daß nämlich alle Primideale 1. Grades von H in lauter verschiedene Primideale 1. Grades zerfallen, bis auf evtl. endlich viele Ausnahmen. Daher hat auch KK_1 den Grad h, was nur für $K = K_1$ möglich.

Satz 8. Der Klassenkörper K für die Gruppe H von k ist auch eindeutig festgelegt durch die folgenden Eigenschaften:

1.) Die Primideale ersten Grades von k, welche in H liegen, zerfallen in K in lauter Primideale ersten Grades

2.) Jedes Primideal ersten Grades von k, welches in K einen Primfaktor 1. Grades aufweist liegt in H.

Endlich viele Ausnahmen von 1.) u. 2.) sind zulässig.

Aus Satz 8 folgt weiter:

Satz 9. Wenn K *relativ Galoissch* zu k ist und alle in einer Klassengruppe H von k enthaltenen Primideale ersten Grades und nur diese in K wieder in Primideale ersten Grades zerfallen, dann ist K *relativ–Abelsch* zu k und der Relativgrad ist gleich dem Index von H. K ist nämlich Klassenkörper zur Gruppe H.

Denn wenn K relativ Galoissch, folgt daraus, daß $\mathfrak{p}$ in K *einen* Faktor ersten Grades hat, daß es *nur* solche hat.

An Stelle von Satz 8 können wir ein weiteres Kriterium für den Klassenkörper aufstellen:

Satz 10. Der Relativkörper K ist Klassenkörper für die Gruppe H vom Index h in k, wenn (bis auf endlich viele Ausnahmen bei 3.))

1.) K relativ Galoissch nach k ist,

2.) Der Relativgrad $n \leqq h$ ist,

3.) Jedes in Primideale 1. Grades zerfallende Primideal 1. Grades aus k in H enthalten ist.

(Es fehlt also hier die Voraussetzung 1.) von Satz 8 und ist durch zwei andere ersetzt. Insbesondere folgert man dann nachträglich, daß $n = h$ sein muß).

Beweis. In K seien die Idealklassen nach dem Führer $\mathfrak{m}$ der Klassengruppe H von k erklärt (tot. positiv $\equiv 1 \bmod \mathfrak{m}$). Dann liegen die Relativnormen von den Idealen einer Klasse von K in einer Klasse von k. $\mathfrak{A}$ sei ein Ideal von $\mathfrak{K}$. Nach Satz 4 gibt es ein äquivalentes Primideal ersten Grades $\mathfrak{P}$. Die Relativnorm $n(\mathfrak{P}) = \mathfrak{p}$ ist somit auch Primideal 1. Grades, das in K in lauter Primideale 1. Grades zerfällt. Nach 3.) kann also $\mathfrak{P}$ so gewählt werden (Ausnahmen!), daß $n(\mathfrak{P}) = \mathfrak{p}$ in H liegt. $n(\mathfrak{A})$ ist mit $\mathfrak{p}$ äquivalent, also in H enthalten. Der Körper K ist also einer Untergruppe von H zugeordnet, also $n \geqq h$. Aus 2.) folgt $n = h$, also unsere Behauptung. 1.) ist übrigens auch benutzt, da sonst nicht aus $n(\mathfrak{P}) = \mathfrak{p}$ auf $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_n$ geschlossen werden kann.

1.11 Absolut–abelsche Körper.

338 I

a) Einheitswurzelkörper

a.) Der durch Einheitswurzeln bestimmte Kreiskörper.

Als Beispiel zur bisher entwickelten Theorie betrachten wir die in Bezug auf den Körper R der rationalen Zahlen Abelschen Körper und beginnen mit dem Studium der durch Einheitswurzeln erzeugten Körper.

Da die Adjunktion mehrerer Einheitswurzeln auf die eines einzigen genügend hohen Grades zurückgeführt werden kann, können wir uns gleich auf diesen Fall beschränken.

Sei $m = p_1^{a_1} \dots p_r^{a_r}$ eine vorgegebene positive Zahl in ihre Primfaktoren zerlegt und $\varepsilon = e^{\frac{2\pi i}{m}}$.

Die sämtlichen Wurzeln von $x^m = 1$ fallen mit den sämtlichen Potenzen von ε zusammen. □□□ In Ω liegen auch alle $p_i^{a_i}$–ten Einheitswurzeln, speziell $\varepsilon_i = e^{\frac{2\pi i}{p_i^{a_i}}} = \varepsilon^{\frac{m}{p_i^{a_i}}}$. Andererseits sind die r Zahlen $\frac{m}{p_i^{a_i}}$ teilerfremd, sodaß wenn die x_i eine Lösung der (sicher lösbaren) Dioph. Gleichung

$$\sum_{i=1}^{n} x_i \frac{m}{p_i^{a_i}} = 1$$

sind,

$$\varepsilon = \varepsilon_1^{x_1} \dots \varepsilon_r^{x_r}$$

ist. Es ist also $\Omega = R(\varepsilon_1, \dots, \varepsilon_r)$, entsteht also durch Komposition der Körper $\Omega_i = R(\varepsilon_i)$.

Wir erledigen zunächst den Fall, daß $m = p^a$ eine Primzahlpotenz ist. Es genügt zunächst die Anzahl einer oberen Grenze für den Grad von Ω. Da nun ε der Gleichung

$$\frac{x^{p^a} - 1}{x^{p^{a-1}} - 1} = x^{p^{a-1}(p-1)} + x^{p^{a-1}(p-2)} + \dots + x^{p^{a-1}} + 1 = 0$$

genügt, weil ja $\varepsilon^{p^{a-1}} \neq 1$ ist, ist der Grad von Ω sicher $\leqq \varphi(p^a) = p^{a-1}(p-1)$

Im allgemeinen Fall eines beliebigen m ist somit der Grad von Ω höchstens $\varphi(p_1^{a_1}) \cdots \varphi(p_r^{a_r}) = \varphi(m)$.

339 I

Sei nun $\mathfrak{q}$ ein Primideal ersten Grades von Ω, welches prim ist zu den Zahlen $1 - \varepsilon^a$. Nach dem Fermatschen Satz muß dann

$$\varepsilon^q \equiv \varepsilon \mod \mathfrak{q}$$

sein, wenn $\mathfrak{q}$ zur Primzahl q gehört, also $n(\mathfrak{q}) = q$ ist, also

$$\varepsilon(\varepsilon^{q-1} - 1) \equiv 0 \mod \mathfrak{q}.$$

Da $\mathfrak{q}$ zu allen $\varepsilon^a - 1$ prim vorausgesetzt, muß $\varepsilon^{q-1} - 1 = 0$ also

$$q \equiv 1 \mod m$$

sein. □□□

Die Bedingung 3.) von Satz 10, S. 337▸ ist also für alle in Primideale ersten Grades zerfallenden q dann erfüllt (mit den endlich vielen Ausnahmen der zu $1 - \varepsilon^a$ nicht primen q), wenn wir als Klassengruppe H die positiven Zahlen $\equiv 1 \bmod m$ nehmen. Ihr Index ist offenbar $\varphi(m)$ und der Grad $\leqq \varphi(m)$, also auch die Bedingung 2.) erfüllt, 1.) natürlich.

Also ist Ω Klassenkörper für den Strahl der positiven Zahlen $\equiv 1 \bmod m$.

Der Grad von Ω ist somit genau $\varphi(m)$. Bezeichnen wir also mit $F_m(x)$ die irreduzible Gleichung vom Grade $\varphi(m)$, der ε genügt, und beachten, daß unter den m–ten Einheitswurzeln auch die d–ten sämtlich vorkommen, wenn $d|m$, daß ferner $x^m - 1 = 0$ nur einfache Wurzeln hat, so folgt:

$$x^m - 1 = \prod_{d|m} F_d(x)$$

Bedeutet $\mu(d)$ die Möbiussche Funktion, so erhält man damit durch Umkehrung:

$$F_m(x) = \prod_{d|m} (x^d - 1)^{\mu\left(\frac{m}{d}\right)}$$

Dies ist die irreduzible Gleichung für ε.

Wir gehen nun an die Bestimmung der Basis und Diskriminante von Ω, und setzen wieder zunächst voraus, es sei $m = \ell^n$ die Potenz einer Primzahl.

340 I

Dann ist

$$\begin{aligned} F_m(x) &= \frac{x^{\ell^n} - 1}{x^{\ell^{n-1}} - 1} + x^{\ell^{n-1}(\ell-2)} + \cdots + x^{\ell^{n-1}} + 1 \\ &= \prod_{\substack{(g,\ell)=1 \\ 0<g<\ell^n}} (x - \varepsilon^g) \end{aligned}$$

Setzen wir $x = 1$ und beachten, daß die Zahlen $\lambda = 1-\varepsilon$ und $1-\varepsilon^g$ assoziiert sind (da $gg' \equiv 1 \bmod \ell^n$ lösbar), so folgt die Idealgleichung:

$$(\ell) = (\lambda)^{\ell^{n-1}(\ell-1)} = (\lambda)^{\varphi(\ell^n)}$$

Da aber $\varphi(\ell^n)$ der Grad von Ω ist, ist (λ) ein Primideal ersten Grades in Ω.

Wir beweisen jetzt, $\mu = \ell^{n-1}(\ell-1) = \varphi(\ell^n)$ gesetzt:
Ist eine ganze Körperzahl der Form:

$$\alpha = x_0 + x_1\lambda + \cdots + x_{\mu-1}\lambda^{\mu-1}$$

mit ganzen rationalen x_i teilbar durch ℓ, so sind alle x_i teilbar durch ℓ.

Nach dem gezeigten ist nämlich zunächst x_0 durch λ, also durch ℓ teilbar. Sei x_i die erste nicht durch ℓ teilbare Zahl, dann ist $x_i\lambda^i$, wie man leicht sieht, durch λ^{i+1}, also x_i durch λ und somit doch durch ℓ teilbar.

Sei $\lambda_i = 1-\varepsilon^i$; $(i,\ell) = 1$; eine der konjugierten zu λ. Dann ist $\lambda - \lambda_i = \varepsilon^i - \varepsilon$. Bis aufs Vorzeichen ist also die Differente der Zahl λ gleich der Differente der Zahl ε. Diese hat aber den Wert

$$\delta = \frac{dF_m(x)}{dx}\Big|_{x=\varepsilon} \quad \square\square\square \quad \text{Wegen } (x^{\ell^{n-1}} - 1)F_m(x) = x^{\ell^n} - 1$$

ist also:

$$\begin{aligned} (\varepsilon^{\ell^{n-1}} - 1)\delta &= \square\square\square \quad \ell^n\varepsilon^{\ell^n - 1} \\ \delta &= -\frac{\ell^n\varepsilon^{\ell^n-1}}{1-\varepsilon^{\ell^{n-1}}} \qquad (\varepsilon^{\ell^{n-1}} = \ell\text{–te Einheitswurzel}) \end{aligned}$$

Bis aufs Vorzeichen ist also ersichtlich die Diskriminante der Zahl λ eine Potenz ℓ^ν von ℓ.

341 I

Demnach läßt sich also nach elementaren Sätzen jede ganze Körperzahl in die Form

$$\alpha = \frac{x_0 + x_1\lambda + \cdots + x_{\mu-1}\lambda^{\mu-1}}{\ell^\nu}$$

bringen. Nach dem vorhin gezeigten müssen alle x_i teilbar durch ℓ^ν sein. *Somit bilden die Zahlen* $1, \lambda, \ldots, \lambda^{\mu-1}$ *eine Basis.*

Nehmen wir nach dem binomischen Satz die Potenzen λ^i aus und reduzieren mithilfe von $F_m(x) = 0$, so erkennen wir, daß auch die Zahlen $1, \varepsilon, \ldots, \varepsilon^{\mu-1}$ eine Basis für Ω bilden. (Folgt auch schon daraus, daß $d(\lambda) = d(\varepsilon)$ ist).

Sind also $\varepsilon, \varepsilon^{i_1}, \varepsilon^{i_2}, \ldots, \varepsilon^{i_{\mu-1}}$ alle Wurzeln von $F_m(x)$, so ist die Diskriminante von Ω gleich:

$$d = \begin{vmatrix} 1 & \varepsilon & \varepsilon^2 & \ldots & \ldots & \varepsilon^{\mu-1} \\ 1 & \varepsilon^{i_1} & \varepsilon^{2i_1} & \ldots & \ldots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \varepsilon^{i_{\mu-1}} & \ldots & \ldots & \ldots & \ldots \end{vmatrix}^2 = (-1)^{\frac{\mu(\mu-1)}{2}} n(\delta) \quad \text{(Zahlbericht §3)}$$

$$= (-1)^{\frac{\mu(\mu-1)}{2}} + \mu\ell^n \varepsilon^{(\ell^n-1)(1+i_1+\cdots+i_{\mu-1})} \cdot \frac{1}{\ell^{\ell^{n-1}}}$$

Da wir für $\ell = 2$ stets $n \geqq 2$ voraussetzen können, ist $\mu = \varphi(\ell^n)$ immer gerade. Ferner ist

$$1 + i_1 + \cdots + i_{\mu-1} = \quad \square\square\square \quad = \frac{\ell^n(\ell^n - 1)}{2} - \ell^n \frac{(\ell^{n-1} - 1)}{2} = \ell^n \frac{\mu}{2}$$

wo der zweite Faktor ganz ist und also $\varepsilon^{(\ell^n-1)(1+i_1+\cdots)} = 1$.

Somit

$$d = (-1)^{\frac{\mu}{2}} \ell^{\ell^{n-1}(n\ell-n-1)} = (-1)^{\frac{1}{2}\varphi(\ell)} \ell^{\varphi(\ell^n)n-\ell^{n-1}}.$$

Ist nun $m = \ell_1^{n_1} \ldots \ell_r^{n_r}$ beliebig, wobei für den Fall $\ell_1 = 2$: $n_1 \geqq 2$ vorausgesetzt wird, (sonst führt der Faktor $\ell_1^{n_1}$ zu keiner algebr. Erweiterung), so folgt aus Satz 10, S. 77▸

342 I

nach leichten Reduktionen:

Satz 1. Die Zahlen $1, \varepsilon, \ldots, \varepsilon^{\varphi(m)-1}$ bilden eine Basis für Ω. Die Diskriminante von Ω hat den Wert

$$d = (-1)^{\frac{1}{2}\varphi(m)} m^{\varphi(m)} \prod_{i=1}^{r} \ell_i^{-\frac{\varphi(m)}{\ell_i - 1}}$$

(Das Vorzeichen ergibt sich zunächst zu $(-1)^{\frac{1}{2}\varphi(m)r}$. Für $r = 1$ ist das in Übereinstimmung, für $r > 1$ aber ist $\frac{1}{2}\varphi(m)$ stets gerade, es stimmt also auch.

Da Ω Klassenkörper für die Gruppe der total positiven Zahlen $\equiv 1 \bmod m$ ist, folgt folgendes Zerlegungsgesetz für die zu m primen Primzahlen p:

Satz 2. Es sei f der kleinste positive Exponent, sodaß $p^f \equiv 1\,(m)$ ist, und $\varphi(m) = ef$. Dann zerfällt p in e Primideale f–ten Grades.

Es ist noch die Zerlegung einer in m aufgehenden Primzahl ℓ zu untersuchen. Wir setzen $m = \ell^n m_0$; $(m_0, \ell) = 1$. Ω_0 sei der Körper der m_0–ten Einheitswurzeln, Ω_{ℓ^n} der der ℓ^n–ten E.W. Beide sind teilerfremd und geben komponiert den Körper Ω.

Nach Satz 22, S. 51 ist der Trägheitskörper von ℓ der größte Körper, in dem ℓ in lauter *verschiedene* Primideale zerfällt. Ω_0 ist also Unterkörper von Ω_T. Es entstehe Ω_T durch Komposition von Ω_0 mit einem Unterkörper Ω_1 von Ω_{ℓ^n}. Da in der Diskriminante von Ω_{ℓ^n} nur die Primzahl ℓ aufgeht, gilt gleiches für Ω_1 da aber ℓ nicht in der Diskr. von Ω_T aufgeht, muß die von Ω_1 gleich 1 sein, d.h. nach Satz 5, S. 74: $\Omega_T = R$.

Ω_0 ist also der Trägheitskörper von ℓ. Sei f die kleinste positive Zahl, für die

$$\ell^f \equiv 1 \mod m_0$$

und

$$\varphi(m_0) = ef.$$

In Ω_0 ist dann $\ell = \mathfrak{q}_1 \ldots \mathfrak{q}_e$, wo die $\mathfrak{q}_i$ den Relativgrad f haben. Nach Satz 15, S. 36 wird $\mathfrak{q}_i$ in Ω die Potenz eines Primideals f–ten Grades. In Ω gilt also:

$$\ell = (L_1 \ldots L_e)^a; \qquad L_i \text{ vom Grad } f.$$

□□□

Es muß $aef = \varphi(m)$ sein, also $a = \frac{\varphi(m)}{\varphi(m_0)} = \varphi(\ell^n)$. Damit haben wir:

Satz 3. Ist ℓ^n ein Teiler von m, so zerfällt ℓ in Ω in folgender Weise:

$$\ell = (L_1 \dots L_e)^{\ell^{n-1}(\ell-1)},$$

wenn $m = m_0\ell^n$ ist, und ℓ mod m zum Exponenten f gehört $\big(\varphi(m_0) = ef\big)$.

Da die Diskriminante der Kreisteilungsgleichung mit der Körperdiskriminante übereinstimmt, erhält man wirkliche Darstellungen der Primideale einer beliebigen Primzahl p, wenn man $F_m(x)$ mod p in Primfunktionen zerlegt. Ist $P(x)$ eine solche, so ist $\mathfrak{p} = (p, P(\varepsilon)$ ein Primteiler von p in Ω, und es ist:

$$p = \prod_{P|F_m(x)} \big(p, P(\varepsilon)\big)^{\nu}$$

wo ν der Grad der Vielfachheit von $P(x)$ in $F_m(x)$ ist. Diese Zerlegung muß mit den von uns auf anderem Wege gefundenen übereinstimmen.

Kapitel 2

L–Reihen mit Größencharakteren

Überblick

2.1 §1 Größencharaktere einer Zahl mod. f.

1 II

Sei k ein beliebiger algebraischer Körper vom Grade n, mit r_1 reellen konjugierten

$$k^{(1)}, \ldots, k^{(r_1)}$$

und r_2 Paaren konjugiert–komplexer konjugierter:

$$\left(k^{(r_1+1)}, k^{(r_1+r_2+1)}\right); \ \ldots \ ; \left(k^{(r_1+r_2)}, k^{(r_1+2r_2)}\right).$$

Wir legen den folgenden Betrachtungen den

Strahl $o : \alpha \equiv 1 \mod f$, total positiv

zugrunde, wo f ein beliebiger ganzer Idealmodul in k ist. Es seien $\eta_1, \ldots, \eta_r$ ein System von

$$r = r_1 + r_2 - 1$$

Grundeinheiten für o und ξ die höchste in o vorkommende Einheitswurzel vom Grade g, sodaß für jede Einheit η aus o eine eindeutige Darstellung besteht:

$$\eta = \xi^a \eta_1^{n_1} \ldots \eta_r^{n_r},$$

mit ganzen rationalen $a, n_1, \ldots, n_r$ und $0 \leqq a < g$.

Die Fälle $f = 1$, d. h. o der Strahl aller total positiven Körperzahlen, ferner $r = 0$, d. h. Grundkörper k rational oder imaginär–quadratisch, und auch $g = 1$ sind im folgenden sämtlich einbegriffen. (Der Fall $g \neq 1$ kann nur in total imaginären Körpern ($r_1 = 0$) eintreten. Denn die

2 II

einzige nicht total imaginäre, von 1 verschiedene Einheitswurzel -1 ist total negativ, gehört also für $r_1 > 0$ sicher nicht zu 0).

Wir stellen uns nun die Aufgabe, den Zahlen α von k Funktionen $\lambda(\alpha)$ zuzuordnen, die erstens die Produkteigenschaft haben:

$$\lambda(\alpha)\lambda(\beta) = \lambda(\alpha\beta),$$

zweitens invariant bleiben, wenn α mit beliebigen Strahleinheiten η multipliziert wird:

$$\lambda(\eta\alpha) = \lambda(\alpha).$$

Diese Funktionen $\lambda(\alpha)$ sollen nicht nur α allein, sondern alle zu α konjugierten im Argument enthalten können. Ferner sollen sie später auch für ideale, also nicht dem Körper k angehörige Zahlen definiert werden. Daher formulieren wir unsere Aufgabe so:

Es werde dem Körper k ein n–dimensionaler Vektor x zugeordnet, sodaß jedem der n konjugierten $k^{(p)}$ eine Komponente x_p entspricht. Die Komponenten x_p sollen denselben Bedingungen unterworfen werden, wie eine total positive Körperzahl:

$$x_p \text{ positiv reell für } p = 1, 2, \ldots, r_1\,,$$
$$x_{p+r_2} \text{ konjugiert–komplex zu } x_p \text{ und } \neq 0 \text{ für } p = r_1 + 1, \ldots, r_1 + r_2\,.$$

Jeden solchen Vektor x nennen wir einen *dem Körper k zugeordneten Vektor*, kurz *Körpervektor*. Speziell stellt also jede total positive Zahl aus k einen solchen Körpervektor dar, und aus jeder beliebigen Zahl $\alpha \neq 0$ von k

kann ein solcher hergeleitet werden, indem von den reellen konjugierten die absoluten Beträge genommen werden. Dieser soll der *der Zahl α zugeordnete Vektor* heißen, und als Argument von Funktionen ebenfalls durch α bezeichnet werden.

Wir fragen dann nach der allgemeinsten, stetigen Funktion $F(x) = F(x_1, \ldots, x_n)$ mit folgenden beiden Eigenschaften:

$$F(x)F(y) = F(xy) \tag{1}$$
$$F(\eta x) = F(x) \tag{2}$$

für jedes Paar x, y von Körpervektoren, bezw für jeden Strahleinheit–Vektor η. Dabei bezeichnet xy das innere Produkt der Vektoren x, y mit den Komponenten $x_p y_p$.

Wir suchen zunächst die allgemeinste stetige Lösung von (1) allein. Aus der zu erfüllenden Relation

$$F(x_1, \ldots, x_n)F(y_1, \ldots, y_n) = F(x_1y_1, \ldots, x_ny_n)$$

folgt sofort durch geeignete Spezialisierung der Komponenten x_p, y_p, (so daß alle bis auf eine bestimmte p–te* gleich 1 sind), daß

$$F(x_1, \ldots, x_n) = f_1(x_1) \ldots f_{r_1}(x_{r_1}) f_{r_1+1}(x_{r_1+1}, x_{r_1+r_2+1}) \ldots$$
$$\ldots f_{r_1+r_2}(x_{r_1+r_2}, x_{r_1+2r_2})$$

*bezw. ein bestimmtes Paar konjugiert komplexer x_p, x_{p+r_2}

gesetzt werden kann, wo die Faktoren rechts nur von

4 II

einer (reellen–positiven) bezw. einem Paar konjugiert komplexer Variablen abhängen, und unter der selbstverständlichen Voraussetzung, daß F nicht identisch verschwindet, für sich den Bedingungen

$$f_\nu(x_\nu)f_\nu(y_\nu) = f_\nu(x_\nu y_\nu); \quad (\nu = 1, 2, \dots r_1)$$

bezw.

$$f_\nu(x_\nu, x_{\nu+r_2})f_\nu(y_\nu, y_{\nu+r_2}) = f_\nu(x_\nu y_\nu, x_{\nu+r_2}y_{\nu+r_2}); \quad (\nu = r_1+1, \dots r_1+r_2)$$

genügen müssen.

Soll nun erstens für eine reelle positive Variable x eine Funktion $f(x)$ der Bedingung

$$f(x) = f(y) = f(xy)$$

genügen, so folgt für einen beliebigen positiven ganzzahligen Exponenten a:

$$f(x^a) = \big(f(x)\big)^a$$

und daraus sofort durch geeignete Transformation von x das Bestehen dieser Gleichung für jedes rationale a, also wenn noch die Stetigkeit von $f(x)$ gefordert wird für jedes reelle a. Setzt man dann speziell

$$f(e) = e^s,$$

wo s irgendeine komplexe Zahl, also $f(e)$ irgendein komplexer Zahlenwert ist, so folgt

$$f(x) = f\left(e^{\log x}\right) = \big(f(e)\big)^{\log x} = e^{s\log x} = x^s$$

wo $\log x$ den reellen Wert bezeichnet und x^s etwa durch $e^{s\log x}$ definiert ist. Die Funktionen $f_1(x_1), \dots f_{r_1}(x_{r_1})$ müssen also notwendig von der Gestalt

$$x_1^{s_1}, \dots, x_{r_1}^{s_{r_1}}$$

mit irgendwelchen komplexen Parametern s_p sein.

5 II

Soll zweitens für ein Paar konjugiert komplexer Variablen

$$\begin{aligned} x &= re^{i\varphi} \\ \overline{x} &= re^{-i\varphi} \end{aligned}$$

eine solche Funktion $f(x, \overline{x})$ der Bedingung

$$f(x, \overline{x}) f(y, \overline{y}) = f(xy, \overline{x}\,\overline{y})$$

genügen, und schreiben wir f als Funktion von r und φ in der Form

$$g(x, \overline{x}) = g(r, \varphi),$$

so muß $g(r, \varphi)$ stetig in r und φ und periodisch mit der Periode 2π in φ sein und der Bedingung

$$g(r_1, \varphi_1) g(r_2, \varphi_2) = g(r_1 r_2, \varphi_1 + \varphi_2)$$

genügen, vermöge der sich ähnlich wie oben g auflösen lassen muß in ein Produkt

$$g(r, \varphi) = g_1(r) g_2(\varphi)$$

zweier stetiger Funktionen $g_1(r), g_2(\varphi)$ deren zweite periodisch in φ mit der Periode 2π ist und die einzeln den Bedingungen

$$\begin{aligned} g_1(r_1) g_1(r_2) &= g_1(r_1 r_2), \\ g_2(\varphi_1) g_2(\varphi_2) &= g_2(\varphi_1 + \varphi_2) \end{aligned}$$

genügen müssen.

Es muß also wie vorhin

$$g_1(r) = r^s$$

mit einem komplexen Parameter s sein, ferner g_2 für positives ganzzahliges und daher wie oben beliebiges reelles b der Bedingung genügen:

$$\big(g_2(\varphi)\big)^b = g_2(b\varphi).$$

Setzt man daher

$$g_2(1) = e^s,$$

wo s irgendeine komplexe Zahl, also e^s irgendein komplexer Zahlenwert ist, so folgt

$$g_2(\varphi) = e^{s\varphi}.$$

Damit endlich $e^{s\varphi}$ die Periode 2π in φ hat, muß

$$e^{2\pi ks} = 1$$

für jedes ganze k sein, was nur für $s = ai$ mit ganzzahligem a zutrifft. Daher folgt für $g(r, \varphi)$ die allgemeinste Lösung

$$g(r, \varphi) = r^s e^{ai\varphi} = f(x, \overline{x})$$

mit beliebigem komplexen s und beliebigem ganzzahligen a.

Wir bezeichnen fortan die Amplituden der komplexen x_p mit φ_p, sodaß

$$\varphi_p = -\varphi_{p+r_2}\,; \quad (p = r_1 + 1, \ldots\, r_1 + r_2)$$

ist. Dann haben wir:

Satz 1. Die allgemeinste stetige Lösung der Funktionalgleichung (1) für den Körpervektor x hat die Form

$$F(x) = \prod_{p=1}^{r_1} x_p^{s_p} \cdot \prod_{p=r_1+1}^{r_1+r_2} |x_p|^{s_p} e^{ia_p\varphi_p}, \tag{3}$$

wo die s_p beliebige komplexe und die a_p beliebige ganze Zahlen sind.

Offenbar sind die Exponenten s_p, a_p durch $F(x)$ eindeutig bestimmt, d. h. zwei solche $F(x)$ dann und nur dann

identisch, wenn alle s_p, a_p übereinstimmen. Dazu genügt es ersichtlich zu zeigen, daß $F(x)$ nur so identisch 1 sein kann, daß alle $s_p, a_p = 0$ sind. Da nun die

$$x_1, \ldots, x_{r_1};\ |x_{r_1+1}|, \ldots\, |x_{r_1+r_2}|;\ \varphi_{r_1+1}, \ldots, \varphi_{r_1+r_2}$$

unabhängige Variable sind, folgte aus $F(x) \equiv 1$, daß

$$\begin{aligned} x_p^{s_p} &\equiv 1 \quad ; \quad (p = 1, \ldots, r_1), \\ |x_p|^{s_p} &\equiv 1 \quad ; \quad (p = r_1 + 1, \ldots, r_1 + r_2), \\ e^{ia_p\varphi_p} &\equiv 1 \quad ; \quad (p = r_1 + 1, \ldots, r_1 + r_2) \end{aligned}$$

wäre, was natürlich nur für $s_p, a_p \equiv 0$ möglich ist.

Satz 2. Die Exponenten s_p, a_p der allgemeinen Lösung (3) von (1) sind durch $F(x)$ eindeutig bestimmt, d. h. zwei solche Lösungen dann und nur dann identisch, wenn alle s_p, a_p übereinstimmen.

Wir haben nunmehr diejenigen Einschränkungen zu suchen, die den s_p, a_p aufzuerlegen sind, damit $F(x)$ in (3) auch noch der obigen Forderung (2) genügt. Diese Forderung (2) ist ersichtlich vermöge (1) gleichbedeutend mit

$$F(\eta) = 1 \tag{4}$$

für jeden Strahleinheit–Vektor η, und (4) wieder äquivalent mit der Bedingungsserie:

$$\begin{cases} F(\eta_k) = 1\,; & (k = 1, 2, \dots r) \\ F(\xi) = 1 \end{cases} \tag{4a}$$

für die Grundeinheiten und ξ.

8 II

Um nun trotzdem übersehen zu können, welche Bedingungen den s_p, a_p aufzuerlegen sind, damit (4a) erfüllt ist, ist es zweckmäßig die Exponenten s_p und damit $F(x)$ zunächst in eine solche Gestalt zu transformieren, daß $F(\eta_k)$ unmittelbar gebildet werden kann.

Dazu gehen wir aus von der Matrix

$$\begin{pmatrix} \frac{1}{n} & \log|\eta_1^{(1)}| & \cdots\cdots & \log|\eta_r^{(1)}| \\ \frac{1}{n} & \log|\eta_1^{(2)}| & \cdots\cdots & \log|\eta_r^{(2)}| \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \frac{1}{n} & \log|\eta_1^{(r+1)}| & \cdots\cdots & \log|\eta_r^{(r+1)}| \end{pmatrix}. \tag{5}$$

□□□

Multipliziert man die den r_2 komplexen konjugierten entsprechenden Zeilen mit 2, so folgt nach Definition des Regulators R des Strahles o sofort, daß die Unterdeterminanten der ersten Spalte dann sämtlich R mit alternierenden Vorzeichen sind, sodaß sich der absolute Wert der Determinante obiger Matrix zu

$$|\Delta| = \frac{R}{2^{r_2}}\left(\frac{1}{n} + \cdots + \frac{1}{n} + \frac{2}{n} + \cdots + \frac{2}{n}\right) = \frac{R}{2^{r_2}} \neq 0$$

ergibt. Daher existiert die reziproke Matrix, die wir im folgenden mit

9 II

(6)
$$\begin{pmatrix} e_1 & e_2 & \cdots\cdots & e_{r+1} \\ e_1^{(1)} & e_2^{(1)} & \cdots\cdots & e_{r+1}^{(1)} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ e_1^{(r)} & e_2^{(r)} & \cdots\cdots & e_{r+1}^{(r)} \end{pmatrix}$$

bezeichnen. Speziell ergibt sich nach dem eben Gesagten für die erste Zeile

(6a) $$e_1 = 1, \ldots, e_{r_1} = 1; \quad e_{r_1+1} = 2, \ldots e_{r_1+r_2} = 2,$$

also gerade die (sonst mit d_k bezeichnete) Multiplikatoren für die „konjugierten Logarithmen“ (s. Landau). Denn die Unterdeterminanten zu den $\frac{1}{n}$ sind $\pm\frac{R}{2^{r_2}}$ bezw. $\pm\frac{R}{2^{r_2-1}}$, je nachdem ob das $\frac{1}{n}$ aus einer „reellen“ oder „komplexen“ Zeile stammt. Die Vorzeichen beginnen mit $+$, wenn die Reihenfolge der Zeilen so ist, daß $\Delta = +\frac{R}{2^{r_2}}$, sonst mit $-$, und alternieren, sodaß auf alle Fälle die e_q, als mit alternierenden Vorzeichen zu nehmende Quotienten obiger Unterdeterminanten durch Δ positiv sind, und die angegebenen Werte haben.

Wir schreiben nun die Funktion $F(x)$ aus Satz 1 in der Form

$$F(x) = \prod_{p=1}^{r+1} |x_p|^{s_p} \cdot \prod_{p=r_1+1}^{r_1+r_2} e^{ia_p\varphi_p}$$

und betrachten allein den ersten Faktor:

$$\prod_{p=1}^{r+1} |x_p|^{s_p} = \prod_{p=1}^{r+1} e^{s_p \log|x_p|} = e^{\sum_{p=1}^{r+1} s_p \log|x_p|}.$$

10 II

Die im Exponenten stehende lineare Form der $\log|x_p|$ transformieren wir in eine lineare Form neuer, äquivalenter Variablen, nämlich

$$c(x) = \sum_{p=1}^{r+1} e_p \log|x_p|,$$

(7)
$$c_q(x) = \sum_{p=1}^{r+1} e_p^{(q)} \log|x_p|; \qquad (q = 1, \ldots, r).$$

Wegen des Nichtverschwindens der Determinante unserer obigen reziproken Matrix (6) ist so jedem System $|x_p|$ eindeutig ein reelles System $c(x), c_q(x)$ zugeordnet und umgekehrt jedem System $c(x), c_q(x)$ (reell) ein System reeller $\log|x_p|$, also auch eindeutig ein System positiver $|x_p| = e^{\log|x_p|}$. Diese neuen Variablen $c(x), c_q(x)$ können daher an Stelle von $x_1, \dots x_{r_1}$, $|x_{r_1+1}|, \dots, |x_{r_1+r_2}|$ zur Charakterisierung des Vektors x benutzt werden, sodaß der Vektor auch eindeutig durch

$$c(x), c_1(x), \dots, c_r(x),\ \varphi_{r_1+1}, \dots, \varphi_{r_1+r_2}$$

bestimmt ist und umgekehrt.

Transformiert man dann die s_p kogredient, also auch gegenseitig eindeutig, in die s'_p so wird der obige erste Faktor von $F(x)$:

$$e^{\sum_{p=1}^{r+1} s_p \log|x_p|} = e^{s'c(x)+\sum_{q=1}^{r} s'_q c_q(x)}$$

$F(x)$ selbst bekommt in den neuen Variablen die Gestalt

$$F(x) = e^{s'c(x)+\sum_{q=1}^{r} s'_q c_q(x)+i\sum_{p=r_1+1}^{r_1+r_2} a_p\varphi_p}$$

und nach Satz 2 sind auch in dieser Gestalt die Exponenten s'_p, a_p eindeutig durch $F(x)$ bestimmt.

Vermöge der speziellen Wahl der transformierenden Matrix (6) haben die neuen Variablen $c(x), c_q(x)$ folgende Bedeutung:

1.) Nach (6a) ist

$$\begin{aligned} e^{c(x)} &= x_1 \dots x_{r_1}|x_{r_1+1}|^2 \dots |x_{r_1+r_2}|^2 \\ &= x_1 \dots x_n = N(x), \end{aligned}$$

wie wir aus Analogie zur gewöhnlichen Norm schreiben wollen, sodaß für einen total positiven Zahlvektor α diese Norm mit der gewöhnlichen übereinstimmt, für einen beliebigen Zahlvektor nur im Betrage.

2.) Vermöge der Reziprozität der Matrizen (5) und (6) drücken sich die $\log|x_p|$ durch die $c(x), c_q(x)$ so aus

$$\log|x_p| = \frac{c(x)}{n} + \sum_{q=1}^{r} c_q(x)\log|\eta_q^{(p)}|; \qquad (p = 1, 2, \dots\ r+1)$$

also

$$\log|x_p| = \big(N(x)\big)^{\frac{1}{n}} \prod_{q=1}^{r} |\eta_q^{(p)}|^{c_q(x)}. \tag{8}$$

Die $c_q(x)$ sind also anzusehen als die Exponenten, die die Beträge der Komponenten eines beliebigen Körpervektors bei der Darstellung durch die Basiselemente $|\eta_1|, \ldots, |\eta_r|$ erfordern. Der Term $\big(N(x)\big)^{\frac{1}{n}}$ ist dabei darauf zurückzuführen, daß die $\eta_1, \ldots, \eta_r$ alle die Norm 1 haben. Bezeichnet man noch die Amplituden der $\eta_q^{(p)}$ mit $\vartheta_q^{(p)}$ und setzt fest, daß die Amplituden der x_p und $\eta_q^{(p)}$ in den reellen konjugierten Null sein sollen,

(die $\eta_q^{(p)}$ sind als Strahleinheiten in den reellen konjugierten positiv), so folgt aus (8):

Satz 3. Ist $x = (x_1, \ldots, x_{r_1}, |x_{r_1+1}|, \ldots |x_{r_1+r_2}|, \varphi_{r_1+1}, \ldots \varphi_{r_1+r_2})$ ein beliebiger Körpervektor, so besteht eine eindeutige Darstellung[†]

$$x = \big(N(x)\big)^{\frac{1}{n}} \eta_1^{c_1(x)} \ldots \eta_r^{c_r(x)} e^{i\{\varphi - \sum_{q=1}^{r} \vartheta_q c_q(x)\}} \tag{9}$$

die vektoriell aufzufassen ist, d. h. die n Gleichungen

$$x_p = \big(N(x)\big)^{\frac{1}{n}} \eta_1^{(p)c_1(x)} \ldots \eta_r^{(p)c_r(x)} e^{i\{\varphi_p - \sum_{q=1}^{r} \vartheta_q^{(p)} c_q(x)\}} \tag{10}$$

für $p = 1, 2, \ldots n$ verteilt. Dabei bestimmen sich die $c_q(x)$ aus (7)[1]

Beweis: 1.) Beständen zwei solche Darstellungen für x, so folgte durch Übergang zu den Beträgen und logarithmieren ein Gleichungssystem der Form

$$\sum_{q=1}^{r} (c_q - c'_q) \log|\eta_q^{(p)}| = 0; \qquad (p = 1, 2, \ldots r+1),$$

was wegen der linearen Unabhängigkeit der letzten r Spalten von (5) nur mit $c_q = c'_q$ bestehen kann. Da außer den $c_q(x)$ in (9)[2] alles andere bestimmt ist, ist die Darstellung (9) eindeutig.

[†]die Amplituden $\vartheta_q^{(p)}$ der komplexen η_q sollen *feste* Zahlen sein (ein- für allemal fest gewählte Multipla von 2π [...]!)

[1]Die Zahl in (..) ist nicht eindeutig zu entziffern.

[2]Verweis ist nicht eindeutig.

2.) Daß sie überhaupt möglich ist und die $c_q(x)$ die in (7) bestimmten Werte haben müssen, folgt unmittelbar aus (8).

Da speziell jede Strahleinheit

$$\eta = \eta_1^{n_1} \cdots \eta_r^{n_r} \xi^a$$

die vektorielle Darstellung liefert:

$$\eta^{(p)} = \eta_1^{(p)n_1} \ldots \eta_r^{(p)n_r} e^{\frac{2\pi i A_p}{g} a},$$

wobei die n_q ganze Zahlen, ebenso a, und die A_p ganze, zu g prime Zahlen sind, nämlich die Exponenten der konjugierten von $\xi = e^{\frac{2\pi i}{g}}$

$$\xi^{A_{r_1+1}}, \ldots \xi^{A_{r_1+r_2}}; \xi^{-A_{r_1+1}}, \ldots \xi^{-A_{r_1+r_2}},$$

folgt, daß x dann und nur dann eine Strahleinheit darstellt, wenn die $c_q(x)$ ganze Zahlen n_q sind, ferner $N(x) = 1$ ist und außerdem noch für $p = r_1 + 1, \ldots r_1 + r_2$:

$$\varphi_p \equiv \sum_{q=1}^{r} n_q \vartheta_q^{(p)} + \frac{2\pi A_p}{g} a \bmod 2\pi$$

mit ganzzahligem a ist.

Es ist demnach x dann und nur dann Strahleinheit, wenn die Bedingungen bestehen:

(11) $\qquad N(x) = 1;$

(12) $\qquad c_q(x) = n_q; \qquad (q = 1, 2, \ldots r),$

(13) $q_p \equiv \sum_{q=1}^{r} n_q \vartheta_q^{(p)} + a \frac{2\pi A_p}{g} \mod 2\pi; \qquad (p = r_1 + 1, \ldots r_1 + r_2).$

□□□

Satz 4. Ein in der Form (9), d. h. (10) dargestellter Körpervektor ist dann und nur dann Strahleinheit, wenn die Bedingungen (11), (12), (13) bestehen.

14 II

Die unseren eigentlichen Betrachtungen eingefügten Überlegungen von S. 11▸—13▸ sollten dazu dienen, die Bedeutung der $c_q(x)$ etwas klar zu machen. Wir brauchen Satz 3 und 4 nicht unmittelbar, entnehmen jedoch aus ihnen folgende Auffassung:

Alle Körpervektoren $x = (x_1, \ldots, x_n)$

$$= (x_1, \ldots, x_{r_1};\ |x_{r_1+1}|, \ldots, |x_{r_1+r_2}|;\ \varphi_{r_1+1}, \ldots, \varphi_{r_1+r_2})$$

bestimmen einen n–dimensionalen Raum, genauer ein Gebiet im n–dimensionalen Raum, charakterisiert durch die Koordinaten:

$$\begin{aligned} N(x) > 0 \quad &; \\ -\infty \leqq c_q(x) \leqq +\infty \quad &; \quad (q = 1, \ldots, r); \\ 0 \leqq \varphi_p < 2\pi \quad &; \quad (p = r_1 + 1, \ldots, r_1 + r_2). \end{aligned}$$

Dieses Gebiet entspricht der in Henselschem Sinne transzendent erweiterten Gesamtheit aller total positiven Körperzahlen. Durch $N(x) = 1$ wird ein $n-1$ dimensionales Gebiet herausgeschnitten. Die Strahleinheiten werden dann durch diejenigen Punkte dieses $(n-1)$–dimensionalen Gebietes repräsentiert, die ganzzahlige Koordinaten $c_q(x)$ haben, und deren φ_p auch noch gewissen Bedingungen (13) genügen, die □□□ ebenfalls von „Ganzzahligkeitstypus“ sind. Die Strahleinheiten bestimmen also in jenem $(n-1)$ dimensionalen Raum ein gewisses Punktgitter. Für einen beliebigen Körpervektor wird dann durch die Abstände seiner Koordinaten

15 II

$c_q(x)$ von den nächsten ganzen Zahlen n_q sowie durch die Abstände der Ausdrücke

$$\varphi_p - \sum_{q=1}^{r} \vartheta_q^{(p)} n_q$$

von den nächsten festen Punkten $\frac{2\pi}{g} A_p a$ (a konstant für alle p) mod 2π ein Maß gegeben, wie weit x von einer Strahleinheit absteht.

Nach dieser Zwischenschaltung kehren wir zu unserer Aufgabe zurück, die bisher erhaltene allgemeinste, stetige Lösung von (1), die wir nunmehr unter Ersetzung von s'_p durch s_p in der Form

$$F(x) = \big(N(x)\big)^s e^{\sum\limits_{q=1}^{r} s_q c_q(x) + i \sum\limits_{p=r_1+1}^{r_1+r_2} a_p \varphi_p}$$

schreiben, so einzuschränken, daß (2), also (4a) erfüllt ist.

Nun wird wegen $N(\eta_k) = 1$, $c_q(\eta_k) = \delta_{qk}$:

$$F(\eta_k) = e^{s_k + i \sum\limits_{p=r_1+1}^{r_1+r_2} a_p \vartheta_k^{(p)}},$$

sodaß wir fordern müssen:

$$s_k + i \sum_{p=r_1+1}^{r_1+r_2} a_p \vartheta_k^{(p)} = 2\pi i m_k$$

mit ganzzahligen m_k; werden diese m_k für die s_k in $F(x)$ eingeführt, so wird:

$$F(x) = \big(N(x)\big)^s e^{2\pi i \sum\limits_{q=1}^{r} m_q c_q(x) + i \sum\limits_{p=r_1+1}^{r_1+r_2} a_p \{\varphi_p - \sum\limits_{q=1}^{r} \vartheta_q^{(p)} c_q(x)\}}.$$

Da die m_k durch die a_p und s_k eindeutig bestimmt sind, sind nach der Bemerkung a. S. 11 ▸ oben und Satz 2 auch die m_k durch $F(x)$ eindeutig bestimmt.

16 II

Im Falle $g > 1$ muß F außerdem noch die zweite Bedingung (4a) befriedigen. Sind wie vorher

$$\xi^{A_{r_1+1}}, \ldots, \xi^{A_{r_1+r_2}}$$

(übrigens ist nach S. 1/2 ▸ hier $r_1 = 0$) die konjugierten zu $\xi = e^{\frac{2\pi i}{g}}$ in den $k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}$, wobei die A_p gewisse ganze, zu g prime, nur vom Körper abhängige Zahlen sind, so wird wegen $N(\xi) = 1$, $c_q(\xi) = 0$:

$$F(\xi) = e^{i \sum\limits_{p=r_1+1}^{r_1+r_2} \frac{2\pi A_p}{g} a_p}$$

Es muß also die Kongruenz

$$g(a_p) = \sum_{p=r_1+1}^{r_1+r_2} A_p a_p \equiv 0 \mod g \tag{14}$$

für die a_p bestehen. Damit haben wir jetzt folgendes Resultat:

Satz 5. Die allgemeinste, stetige Lösung der Funktionalgleichungen (1), (2) für eine Funktion $F(x)$ des Körpervektors x ist gegeben durch

$$F(x) = \big(N(x)\big)^s \prod_{q=1}^{r} e^{2\pi i m_q c_q(x)} \prod_{p=r_1+1}^{r_1+r_2} e^{i a_p \{\varphi_p - \sum\limits_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\}}. \tag{15}$$

Darin bedeuten $N(x)$ die Norm von x, $c_q(x)$ die Ausdrücke (7), φ_p die Amplituden der komplexen x_p, $\vartheta_k^{(p)}$ die Amplituden der komplexen $\eta_k^{(p)}$. Ferner sind die m_q beliebige ganze Zahlen, s eine komplexe Zahl und die a_p ganze Zahlen, die im Falle $g = 1$ beliebig sind, im Falle $g > 1$ der Kongruenz (14) gemäß bestimmt werden müssen. Die s, a_p, m_q sind durch $F(x)$ eindeutig bestimmt, d. h. zwei $F(x)$ der Form (15) sind dann und nur dann identisch, wenn alle s, a_p, m_q übereinstimmen.

17 II

Der Faktor $\big(N(x)\big)^s$ in $F(x)$ interessiert uns in der Folge nicht. Wir können uns von ihm befreien, wenn wir fordern, daß $F(x)$ außer (1) und (2) noch der weiteren Bedingung

$$F(cx) = F(x)$$

für eine beliebige Konstante (Skalar) $c > 0$ genügen soll, oder auch, was gleichbedeutend ist, daß

$$F(c) = 1$$

sein soll.

Da nämlich ersichtlich für einen positiven Skalar c:

$$\begin{aligned} c_q(c) &= 0 \quad ; \quad (q = 1, 2, \dots r) \\ \varphi_p &= 0 \quad ; \quad (p = r_1 + 1, \dots r_1 + r_2) \end{aligned}$$

ist, ersteres entweder nach Satz (9) oder weil nach (7), (6), (5):

$$c_q(c) = \log c \sum_{p=1}^{r+1} e_p^{(q)} = 0$$

ist, wird

$$F(c) = \big(N(c)\big)^s = c^{ns} = e^{ns \log c}$$

und dies wird dann und nur dann für jedes $c > 0$ gleich 1, wenn $s = 0$ ist.

Jedes solche $F(x)$ soll ein *Größencharakter* mod. f *des Körpervektors* x heißen und mit $\lambda(x)$ bezeichnet werden. Wir haben dann:

Satz 6. Der allgemeinste Größencharakter mod f des Körpervektors x, d. h. die allgemeinste, stetige Lösung der drei Funktionalgleichungen:

18 II

$$(16)\qquad \begin{cases} \lambda(x)\lambda(y) &= \lambda(xy), \\ \lambda(\eta x) &= \lambda(x), \\ \lambda(cx) &= \lambda(x), \end{cases}$$

wo x, y variable Körpervektoren, η jeden Strahleinheit–Vektor und c jeden positiven Skalar bezeichnet, wird gegeben durch

$$(17)\qquad \lambda(x) = \prod_{q=1}^{r} e^{2\pi i m_q c_q(x)} \prod_{p=r_1+1}^{r_1+r_2} e^{ia_p\{\varphi_p - \sum_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\}},$$

wo die Bezeichnungen dieselben wie in Satz 5 sind, insbesondere auch $\lambda(x)$ die Exponenten m_q, a_p eindeutig bestimmt. Jeder Größencharakter hat außer (16) noch die Eigenschaft

$$(18)\qquad |\lambda(x)| = 1.$$

Wir beweisen weiter den folgenden fundamentalen Satz über Größencharaktere:

Satz 7. Die Größencharaktere mod. f bilden bei Komposition durch Multiplikation eine unendliche Abelsche Gruppe mit $n-1$ Basiselementen

$$\lambda_1(x), \ldots, \lambda_{n-1}(x),$$

welche die *Grundcharaktere* mod. f heißen. Durch die Werte dieser $n-1$ Funktionen und die Angabe von $N(x)$ wird der Körpervektor x bis auf einen Strahleinheit–Vektor als Faktor eindeutig festgelegt.

Beweis: 1.) Natürlich ist Produkt und Quotient zweier Größencharaktere (17) wiederum ein solcher, da sich die Exponenten m_p, a_p dabei einfach addieren, bezw. subtrahieren und folglich ihre charakteristischen Eigenschaften von Satz 5 behalten. Also bilden die $\lambda(x)$ eine Abelsche Gruppe.

2.) Um eine Basis für diese Gruppe zu erhalten, nehmen wir erstens die r Basiselemente

$$(19)\qquad \begin{cases} \lambda_1(x) &= e^{2\pi i c_1(x)} \\ \cdots\cdots\cdots\cdots\cdots \\ \lambda_r(x) &= e^{2\pi i c_r(x)} \end{cases}$$

Ferner betrachten wir die Kongruenz (14):

$$g(a_p) = A_{r_1+1}a_{r_1+1} + \cdots + A_{r_1+r_2}a_{r_1+r_2} \equiv 0 \mod g \tag{14}$$

im r_2 dimensionalen Raum der a_p. Die Lösungen dieser Kongruenz, die die zulässigen Exponenten a_p ergeben, bilden bekanntlich ein Parallel–Punktgitter in diesem Raum, dessen Grundmasche den Inhalt g hat (für $g = 1$ das gewöhnliche kartesische Gitter). Legen wir die Grundmasche mit einer Ecke in den Nullpunkt, so ergeben die r_2 benachbarten Ecken:

$$\left(a_p^{(1)}\right), \left(a_p^{(2)}\right), \ldots, \left(a_p^{(r_2)}\right)$$

r_2 unabhängige Fundamentallösungen unserer Kongruenz (14) aus denen sich jede weitere Lösung linear ganzzahlig kombinieren läßt. Dann bilden wir die weiteren Größencharaktere:

$$\left\{\begin{array}{rcl} \lambda_{r+1}(x) & = & \prod\limits_{p=r_1+1}^{r_1+r_2} e^{ia_p^{(1)}\{\varphi_p - \sum\limits_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\}} \\ \cdots\cdots & & \cdots\cdots \\ \lambda_{r+r_2}(x) & = & \prod\limits_{p=r_1+1}^{r_1+r_2} e^{ia_p^{(r_2)}\{\varphi_p - \sum\limits_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\}} \end{array}\right. \tag{20}$$

Die $n - 1 = r + r_2$ Charaktere (19) bis (20) bilden dann eine Basis unserer Größencharakteren–Gruppe. Denn einerseits läßt sich der allgemeine Größencharakter (17) aus ihnen als

$$\lambda(x) = \lambda_1^{m_1}(x)\lambda_2^{m_2}(x)\ldots\lambda_r^{m_r}(x)\lambda_{r+1}^{n_1}(x)\ldots\lambda_{r+r_2}^{n_{r_2}}(x) \tag{21}$$

zusammensetzen, weil die allgemeine Lösung von (14) sich in der Form

$$a_p = n_1 a_p^{(1)} + \cdots + n^{(r_2)} a_p^{(r_2)}; \qquad (p = r_1 + 1, \ldots, r_1 + r_2)$$

darstellen läßt, (wobei die m_q, n_q ganzzahlige Exponenten bedeuten, wie es bei der Basisdarstellung einer Abelschen Gruppe sein muß. Andererseits ist diese Basisdarstellung eine wichtige *Basis*darstellung, d. h. eindeutig. Hierzu genügt es zu zeigen, daß in (21) $\lambda(x)$ dann und nur dann identisch 1 ist, wenn alle $m_q, n_q = 0$ sind.

Nun folgt aus $\lambda(x) \equiv 1$ zunächst nach der bewiesenen eindeutigen Bestimmtheit der m_q durch $\lambda(x)$, daß alle $m_q = 0$ sind, ferner aus der eindeutigen Bestimmtheit der a_p daß die linearen Formen

$$a_p = n_1 a_p^{(1)} + \cdots + n^{(r_2)} a_p^{(r_2)}; \qquad (p = r_1 + 1, \ldots, r_1 + r_2)$$

sämtlich Null sind. Da aber die Determinante $\left|a_p^{(q)}\right|$ als Inhalt der oben genannten Grundmasche den Wert $g \neq 0$

hat, müssen auch alle $n_q = 0$ sein, w. z. b. w.

3.) Ich beweise schließlich die letzte Behauptung von Satz 7, die wegen der Produkteigenschaft von $N(x)$ und den $\lambda_\nu(x)$ offenbar mit folgender Behauptung identisch ist:

Sind für einen Körpervektor x alle Größen

$$N(x), \lambda_1(x), \ldots \lambda_{n-1}(x) = 1,$$

so ist x ein Strahleinheitsvektor.

Nun folgt aus $N(x) = 1$ und $\lambda_1(x), \ldots, \lambda_r(x) = 1$ nach (19) das Gleichungssystem

$$\begin{cases} N(x) = 1, \\ c_q(x) = n_q; \qquad (q = 1, 2, \ldots, r), \end{cases} \tag{22}$$

wo die n_q ganze Zahlen sind. Ferner folgt aus $\lambda_{r+1}(x), \ldots, \lambda_{r+r_2}(x) = 1$ nach (20) und dem eben erhaltenen (22)

$$\sum_{p=r_1+1}^{r_1+r_2} a_p^{(q)} \left\{ \varphi_p - \sum_{k=1}^{r} \vartheta_k^{(p)} n_k \right\} \equiv 0 \mod 2\pi; \qquad (q = 1, 2, \ldots r_2),$$

oder anders geschrieben

$$\sum_{p=r_1+1}^{r_1+r_2} a_p^{(q)} \frac{\varphi - \sum_{k=1}^{r} \vartheta_k^{(p)} n_k}{\frac{2\pi}{g}} \equiv 0 \mod g; \qquad (q = 1, 2, \ldots r_2).$$

Hieraus folgt, da rechts ganze Multipla von g stehen und die Determinante $\left|a_p^{(q)}\right| = g$ ist, durch Auflösung nach den $\frac{\varphi_p - \sum_{k=1}^{r} \vartheta_k^{(p)} n_k}{\frac{2\pi}{g}}$, daß diese ganze Zahlen B_p sein müssen. Es wären also unsere Fundamentallösungen

$a_p^{(q)}$ auch Lösungen der ganzzahligen Kongruenz

$$\overline{g}(a_p) = \sum_{p=r_1+1}^{r_1+r_2} B_p a_p^{(q)} \equiv 0 \mod g.$$

Da aber durch die Fundamentallösungen (d. h. durch das zugehörige Punktgitter) die erzeugende Kongruenz bis auf einen ganzen Zahlfaktor eindeutig bestimmt ist, muß

$$\overline{g}(a_p) \equiv a g(a_p) \mod g$$

mit ganzzahligem a sein.[‡] Es folgt also:

$$\frac{\varphi_p - \sum_{k=1}^{r} \vartheta_k^{(p)} n_k}{\frac{2\pi}{g}} \equiv a A_p \mod g$$

oder

$$\varphi_p = \sum_{k=1}^{r} \vartheta_k^{(p)} n_k + a \frac{2\pi A_p}{g} \mod 2\pi. \tag{23}$$

Aus (22), (23) folgt dann nach Satz 4, daß x eine Strahleinheit $\eta = \eta_1^{n_1} \dots \eta_r^{n_r} \xi^a$ ist, w. z. b. w.

Es ist für das folgende zweckmäßig die Größencharaktere $\lambda(x)$ etwas anders als bisher zu schreiben. Der zweite Faktor

$$\prod_{p=r_1+1}^{r_1+r_2} e^{i a_p \{\varphi_p - \sum_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\}}$$

des allgemeinen Größencharakters (17) kann nämlich positive und negative a_p enthalten. Es ist jedoch später notwendig, daß diese a_p alle positiv sind.

[‡] $\overline{g}(a_p) \equiv 0$ braucht nicht notwendig „gittererzeugend“ zu sein, sondern nur eine Folge von $g(a_p) \equiv 0$; d. h. a kann auch einen Teiler mit g gemeinsam haben, speziell $\equiv 0 \mod g$ sein.

Dies läßt sich leicht lediglich durch Veränderung der Schreibweise, ohne Einschränkung der Allgemeinheit in eindeutiger Weise erreichen.

23 II

Bedenkt man nämlich die Beziehungen

$$\left.\begin{aligned} \varphi_{p+r_2} &= -\varphi_p\,; \\ \vartheta_k^{(p+r_2)} &= -\vartheta_k^{(p)}\,; \end{aligned}\right\} \qquad (p = r_1+1, \dots\, r_1+r_2),$$

denen gemäß wir sowohl die festen $\vartheta_k^{(p)}$ als auch die variablen φ_p wählen können und wollen, so erkennt man, daß man ein etwaiges negatives a_p stets so formal in ein positives verwandeln kann, daß man an Stelle der auf $k^{(p)}$ bezüglichen Größen die auf $k^{(p+r_2)}$ bezüglichen einführt. Man erhält dann für den obigen zweiten Faktor von $\lambda(x)$ die offenbar ebenfalls eindeutige Form:

$$\prod_{p=r_1+1}^{n} e^{ia_p\left\{\varphi_p - \sum\limits_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\right\}},$$

wobei die a_p den Bedingungen genügen:

$$\begin{cases} a_p \geqq 0; & (p = r_1+1, \dots\, n), \\ a_p a_{p+r_2} = 0; & (p = r_1+1, \dots\, r_1+r_2), \end{cases} \tag{24}$$

die eben besagen, daß alle a_p nicht negativ sind, und daß von zwei konjugiert–komplexen Körpern entsprechenden a_p stets nur eins auftritt.

Satz 8. Der allgemeine Größencharakter mod. f läßt sich auch in der Form

$$\lambda(x) = \prod_{q=1}^{r} e^{2\pi i m_q c_q(x)} \prod_{p=r_1+1}^{n} e^{ia_p\left\{\varphi_p - \sum\limits_{k=1}^{r} \vartheta_k^{(p)} c_k(x)\right\}}$$

schreiben, wobei die a_p außer einer zu (14) analogen Kongruenzbedingung mod g noch den Bedingungen (24) genügen. Auch in dieser Form sind die Exponenten a_p durch $\lambda(x)$ eindeutig bestimmt.

24 II

Anmerkung: Natürlich transformiert sich hierbei die Bedingungskongruenz (14) in die allgemeinere:

$$A_{r_1+1}a_{r_1+1} + \dots + A_{r_1+r_2}a_{r_1+r_2} - A_{r_1+1}a_{r_1+r_2+1} - \dots - A_{r_1+r_2}a_{r_1+2r_2} \equiv \\ \equiv 0 \bmod g,$$

in der die Exponenten $-A_{r_1+1}, \ldots - A_{r_1+r_2}$ der übrigen zu ξ konjugierten ebenfalls mitberücksichtigt sind, und in der in Wahrheit immer nur r_2 Glieder wirklich auftreten, die irgendwelchen r_2 nicht untereinander konjugiert komplexen Körpern entsprechen. — Die eindeutige Bestimmtheit auch der neuen a_p durch $\lambda(x)$ ergibt sich einfach daraus, daß nicht nur der Übergang von den früheren zu den neuen a_p eindeutig ist, sondern offenbar auch umgekehrt der Übergang von den neuen a_p zu den früheren.

Die Größencharaktere $\lambda(x)$ sind bisher nur für Körpervektoren x, speziell also nur für total positive Körperzahlen definiert, da ja in die Definition des Körpervektors die Forderung „total positiv“ mit einbegriffen war. Wir erweitern nun die Definition der $\lambda(x)$ noch auf allgemeinere Vektoren, derart, daß speziell *alle* Körperzahlen und sogar noch mehr einbegriffen sind, indem wir für einen beliebigen Vektor

$$x = (x_1, \ldots, x_n)$$

dessen Komponenten x_p von Null verschiedene komplexe Zahlen sind, von denen nur immer je zwei konjugiert–komplexen Körpern entsprechende selbst konjugiert–komplex sind, festsetzen:

$$\lambda(x) = \lambda(x_1, \ldots, x_n) = \lambda\big(|x_1|, \ldots |x_{r_1}|, x_{r_1+1}, \ldots, x_n\big),$$

also festsetzen, daß von den den r_1 reellen konjugierten entsprechenden Komponenten x_p nur die Beträge $|x_p|$ berücksichtigt werden sollen. Hierdurch ist die Definition von $\lambda(x)$ für solche beliebige Vektoren auf die für Körpervektoren zurückgeführt, da $\big(|x_1|, \ldots |x_{r_1}|, x_{r_1+1}, \ldots, x_n\big)$ ersichtlich ein Körpervektor ist. Natürlich gelten auch für diese erweiterte Bedeutung von $\lambda(x)$ die Fundamentalgesetze:

$$\text{(25)} \qquad \begin{cases} \lambda(x)\lambda(y) &= \lambda(xy)\,, \\ \lambda(\eta x) &= \lambda(x)\,, \\ \lambda(cx) &= \lambda(x)\,, \\ \big|\lambda(x)\big| &= 1\,. \end{cases}$$

Satz 9. Definiert man für Vektoren $x = (x_1, \ldots, x_n)$ mit beliebigen komplexen Komponenten $x_p \neq 0$, von denen nur die $2r_2$ letzten immer paarweise konjugiert–komplex sind:

$$\lambda(x) = \lambda\big(|x_1|, \ldots |x_{r_1}|, x_{r_1+1}, \ldots, x_n\big),$$

so genügt $\lambda(x)$ den Bedingungen (25). Speziell kann so jeder beliebigen von Null verschiedenen Körperzahl α der *Größencharakter* mod. f $\lambda(\alpha)$ mit den Eigenschaften (25) zugeordnet werden, indem λ im Sinne von Satz 6 für den α zugeordneten Zahlvektor (S. 2▶/3▶) gebildet wird.

26 II

Schlußbemerkung: Der Bau des allgemeinen Größencharakters $\lambda(x)$ in (17) oder besser noch der ihm äquivalenten Grundcharaktere (19), (23)[3] läßt unmittelbar den engen Zusammenhang dieser Größencharaktere mit der Basisdarstellung (9), (10) und den daran geknüpften Überlegungen erkennen. Die Grundcharaktere messen gerade in dem a. S. 14▶/15▶ erläuterten Sinne den Abstand von x_0 im zugeordneten $(n-1)$ dimensionalen Raum $\big(N(x) = 1\big)$ der $c_q(x)$ und φ_p von der nächsten Strahleinheit, geben also ein Maß für die Lage des in Bezug auf die Grundmasche des Strahleinheitsgitters in jenem Raum reduzierten Endpunktes des Vektors x. Speziell für Strahleinheiten und nur für solche, sind alle Grundcharaktere 1 (Satz 7). Da dieses Maß sich auf die wirkliche „Größe“ der Vektorkomponenten, speziell also der konjugierten zu einer Körperzahl (allerdings reduziert nach den Strahleinheiten, bezieht, ist der Name „Größencharakter“ gewählt.

[3] Verweis nicht eindeutig lesbar

2.2 §2 Die idealen Zahlen.

27 II

Das Rechnen mit den Idealklassen im allgemeinsten Sinne (nach einem Kongruenzstrahl mit Vorzeichenbedingung) legt es nahe an Stelle der Ideale wirkliche Zahlrepräsentanten, die *idealen Zahlen*, einzuführen, die selbst Kongruenz– und Vorzeichenbedingungen unterworfen werden können. Wesentlich ist auch, daß so den Idealen neben der Teilbarkeitseigenschaft auch eine Größeneigenschaft zugeordnet wird. Die Möglichkeit der Einführung solcher Zahlrepräsentanten für die Ideale beruht auf der Endlichkeit der Klassenzahl h des Körpers k.

Es seien $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_e$ ein Repräsentantensystem für die e Basisklassen der Idealklassengruppe in gewöhnlichem (weitesten) Sinn, sodaß für jedes Ideal $\mathfrak{a}$ aus k eine Darstellung besteht

$$\mathfrak{a} = (\varrho)\mathfrak{b}_1^{a_1} \ldots \mathfrak{b}_e^{a_e}, \tag{1}$$

wo ϱ eine Zahl aus k ist und die ganzzahligen Exponenten $a_i \mod h_i$ eindeutig bestimmt sind, wenn h_i die kleinste positive Zahl ist für die

$$\mathfrak{b}_i^{h_i} = (\beta_i)$$

ein Hauptideal aus k wird. Es ist dann

$$h = h_1 h_2 \ldots h_e$$

die absolute Klassenzahl von k.

28 II

Wir konstruieren dann über dem Körper k einen *Bereich* $\mathfrak{Z}$ *von idealen Zahlen*, indem wir zu k noch die h Größen

$$\widehat{\beta}_i = \sqrt[h_i]{\beta_i}$$

mit irgendwie, aber fest bestimmter Wurzel hinzufügen, und außerdem alle Produkte und Quotienten aus diesen Größen und Körperzahlen. Jede Zahl

des Bereiches $\mathfrak{Z}$, die wir fortan als ideale Zahlen bezeichnen und durch das Zeichen $\wedge$ andeuten, hat also die Form

$$\widehat{\alpha} = \varrho \widehat{\beta}_1^{a_1} \dots \widehat{\beta}_e^{a_e} \tag{2}$$

mit ganzzahligen a_i.

Die $\widehat{\alpha}$ sind als Ideale betrachtet zunächst Ideale eines gewissen algebraischen Körpers über k, aber solche, die schon in k liegen. Denn für Ideale folgt aus

$$\mathfrak{b}_i^{h_i} = (\widehat{\beta}_i)^{h_i}$$

wegen der Eindeutigkeit der h_i–ten Wurzel bei Idealgleichheiten:

$$\mathfrak{b}_i = (\widehat{\beta}_i).$$

Somit ist die allgemeine ideale Zahl $\widehat{\alpha}$ in (2) als Ideal $(\widehat{\alpha})$ betrachtet gleich dem in entsprechender Form dargestellten Ideal $\mathfrak{a}$ in (1).

Die idealen Zahlen bilden offenbar eine den Körper k enthaltende Abelsche Gruppe, die zur Gruppe der Ideale in k isomorph ist und in (2) in eindeutiger Basisdarstellung vorliegt. Denn es entspricht eben jedem Ideal $\mathfrak{a}$

auf Grund von (1) und (2) eindeutig eine ideale Zahl $\widehat{\alpha}$ und umgekehrt, sodaß $\mathfrak{a} = (\widehat{\alpha})$ ist.

Sind ferner zwei ideale Zahlen $\widehat{\alpha}$ und $\widehat{\beta}$ als Ideale betrachtet einander gleich, also die zugeordneten Körperideale gleich, so folgt sofort, daß ihre Exponenten a_i in der Darstellung (2) und auch die Zahlfaktoren ϱ als Hauptideale genommen übereinstimmen müssen, sodaß also $\widehat{\alpha} = \varepsilon\widehat{\beta}$ ist, wo ε eine Körpereinheit bezeichnet. Wir haben also:

Satz 10: Der Bereich $\mathfrak{Z}$ von idealen Zahlen (2) bildet eine mit der Gruppe der Ideale von k isomorphe, unendliche Abelsche Gruppe, die in (2) mit $\mod h_i$ reduzierten Exponenten a_i in eindeutiger Basisdarstellung vorliegt. Der Isomorphismus wird dargestellt durch die korrespondierende Basisdarstellung (1) der Idealgruppe von k und zwischen zwei zugeordneten Elementen von (1) und (2) besteht die Idealgleichheit

$$\mathfrak{a} = (\widehat{\alpha}).$$

Zwei ideale Zahlen $\widehat{\alpha}, \widehat{\beta}$ sind als Ideale betrachtet dann und nur dann gleich, wenn

$$\frac{\widehat{\alpha}}{\widehat{\beta}} = \varepsilon$$

eine Einheit aus k ist.

30 II

(Anstelle der β_i hätte oben auch jedes $\varepsilon\beta_i$ genommen werden können. Da aber nur endlich viele Einheitenverbände nach dem Exponenten h_i in k existieren, und auch die h_i–te Wurzel nur endlich vieldeutig ist, ist die Auswahl unter den das Ideal $\mathfrak{b}_i$ repräsentierenden Systemen $\varepsilon\widehat{\beta}_i$, wo ε alle Körpereinheiten durchläuft, nur auf eine endliche Anzahl beschränkt und damit überhaupt die Auswahl eines Bereiches $\mathfrak{Z}$ idealer Zahlen mit den Eigenschaften von Satz 10 nur in endlich vielen Weisen möglich).

Wir definieren nun weiter was unter den n konjugierten idealen Zahlen $\widehat{\alpha}^{(1)}, \ldots, \widehat{\alpha}^{(n)}$ zu verstehen ist, wo n den Grad von k bezeichnet. Dazu setzen wir fest, daß für die Basiselemente $\widehat{\beta}_i$ von $\mathfrak{Z}$ gelten soll:

$$\widehat{\beta}_i^{(p)} = \sqrt[h_i]{\beta_i^{(p)}}\,; \qquad (p = 1, 2, \ldots\ n)$$

wo die h_i–ten Wurzeln stets irgendwie, aber fest gewählt sind, nur mit der einen Einschränkung, daß für konjugiert–komplexe konjugierte $k^{(p)}$ und $k^{(p+r_2)}$ (in der Bezeichnung wie in §1) auch $\widehat{\beta}_i^{(p)}$ und $\widehat{\beta}_i^{(p+r_2)}$ konjugiert–komplex sein sollen, was offenbar stets zu erreichen ist. Ferner verstehen wir dann unter den $\widehat{\alpha}^{(p)}$ das auf Grund von (2) aus den $\widehat{\beta}_i^{(p)}$ und $\varrho^{(p)}$ gebildete Kompositum

$$\widehat{\alpha}^{(p)} = \varrho^{(p)} \widehat{\beta}_1^{(p)\,a_1} \ldots \widehat{\beta}_e^{(p)\,a_e}$$

31 II

Nach dieser Definition ist ersichtlich dem System der konjugierten $\widehat{\alpha}^{(p)}$ das System der konjugierten Ideale $\mathfrak{a}^{(p)}$ zugeordnet im Sinne von Satz 10. Denn wegen der Isomorphie der n konjugierten Körper $k^{(p)}$ haben ja die Ideale $\mathfrak{a}^{(p)}$ die eindeutigen Darstellungen

$$\mathfrak{a}^{(p)} = \varrho^{(p)} \mathfrak{b}_1^{(p)\,a_1} \ldots \mathfrak{b}_e^{(p)\,a_e}, \qquad (p = 1, \ldots, n)$$

woraus die Behauptung unmittelbar folgt.

Ferner gilt offenbar, daß die konjugierten zu $\widehat{\alpha}\widehat{\beta}$ durch $\widehat{\alpha}^{(p)}\widehat{\beta}^{(p)}$ gegeben werden. Definiert man daher die Norm in $\mathfrak{Z}$ durch

$$N(\widehat{\alpha}) = \widehat{\alpha}^{(1)} \ldots \widehat{\alpha}^{(n)}$$

so gilt

$$N(\widehat{\alpha})N(\widehat{\beta}) = N(\widehat{\alpha}\widehat{\beta}).$$

Diese Norm ist weiter eine rationale Zahl, wenn nur ihr Betrag betrachtet wird, und sogar eine ganze Zahl, wenn $(\widehat{\alpha}) = \mathfrak{a}$ ein ganzes Ideal ist. Denn zunächst ist

$$\begin{aligned} N(\widehat{\beta}_i) &= \widehat{\beta}_i^{(1)} \dots \widehat{\beta}_i^{(n)} = \sqrt[h_i]{\beta_i^{(1)} \cdots \beta_i^{(n)}} \\ &= \sqrt[h_i]{N(\beta_i)} \end{aligned}$$

Nun ist $\pm N(\beta_i) = N(\mathfrak{b}_i^{h_i}) = b_i^{h_i}$ eine h_i–te Potenz einer rationalen Zahl, nämlich der $N(\mathfrak{b}_i)$, also $N(\widehat{\beta}_i)$ bis auf $2h_i$–te Einheitswurzeln $= b_i = N(\mathfrak{b}_i)$ und somit wegen der Produkteigenschaft der Norm:

$$|N(\widehat{\alpha})| = N(\mathfrak{a})$$

wenn $\widehat{\alpha}$ und $\mathfrak{a}$ auf Grund von (1) und (2) einander entsprechen.

32 II

Satz 11. Wird allgemein die Norm einer idealen Zahl $\widehat{\alpha}$ durch

$$N(\widehat{\alpha}) = \widehat{\alpha}^{(1)} \dots \widehat{\alpha}^{(n)}$$

definiert, so gilt

$$N(\widehat{\alpha})N(\widehat{\beta}) = N(\widehat{\alpha}\widehat{\beta}),$$

ferner

$$\left|N(\widehat{\alpha})\right| = N(\mathfrak{a}),$$

(also eine rationale und für ganzes $\mathfrak{a} = (\widehat{\alpha})$ ganze rationale Zahl), wenn $\mathfrak{a} = (\widehat{\alpha})$ das $\widehat{\alpha}$ zugeordnete Ideal von k ist.

Entsprechend den h Idealklassen von k zerfällt auch der Bereich $\mathfrak{Z}$ in h Klassen, die Nebengruppen zur Untergruppe aller Körperzahlen, sodaß alle und nur die idealen Zahlen einer Klasse multiplikativ nur um Körperzahlen unterschieden sind. Es gilt nun der wichtige Satz:

Satz 12: Für die idealen Zahlen einer Klasse C läßt sich Addition und Subtraktion so definieren, daß sie in C unbeschränkt und eindeutig ausführbar sind.

Beweis: Sei $\widehat{\alpha}$ eine ideale Zahl aus C, so ist C die Gesamtheit aller Zahlen $\widehat{\alpha}\varrho$, wo ϱ alle Körperzahlen durchläuft. Wir definieren dann:

$$\widehat{\alpha}\varrho_1 \pm \widehat{\alpha}\varrho_2 = \widehat{\alpha}(\varrho_1 \pm \varrho_2).$$

Es entsteht also eine wieder zu C gehörige ideale Zahl. Diese ist unabhängig von dem gerade gewählten Repräsentanten $\widehat{\alpha}$ von C. Denn ist $\widehat{\beta} = \gamma\widehat{\alpha}$ ein anderer, so wird

$$\widehat{\alpha}\varrho_1 = \widehat{\beta}\frac{\varrho_1}{\gamma}\,; \quad \widehat{\alpha}\varrho_2 = \widehat{\beta}\frac{\varrho_2}{\gamma}$$

also

$$\widehat{\alpha}\varrho_1 \pm \widehat{\alpha}\varrho_2 = \widehat{\beta}\left(\frac{\varrho_1}{\gamma} \pm \frac{\varrho_2}{\gamma}\right) = \widehat{\beta}\frac{\varrho_1 \pm \varrho_2}{\gamma} = \widehat{\alpha}(\varrho_1 \pm \varrho_2).$$

Wir nennen eine ideale Zahl $\widehat{\alpha}$ ganz, wenn das Ideal $(\widehat{\alpha}) = \mathfrak{a}$ ganz ist. Dann gilt:

Satz 13: Summe und Differenz zweier ganzen idealen Zahlen einer Klasse C sind wieder ganz.

Beweis: Sind $\widehat{\alpha}$ und $\widehat{\alpha}\varrho$ zwei den ganzen Idealen $\mathfrak{a}$ und $\mathfrak{b} = \mathfrak{a}(\varrho)$ entsprechende ideale Zahlen aus C, so ist

$$\widehat{\alpha} \pm \widehat{\alpha}\varrho = \widehat{\alpha}(1 \pm \varrho)$$

Sei nun $\varrho = \frac{\gamma}{\delta}$ als Quotient zweier ganzer Zahlen dargestellt, so ist einerseits

$$1 \pm \varrho = \frac{\delta \pm \gamma}{\delta}\,,$$

andererseits

$$\mathfrak{b}(\delta) = \mathfrak{a}(\gamma).$$

$$\begin{array}{lrcll} \text{Nun ist} & \gamma & \equiv & 0 \mod \frac{\delta}{\mathfrak{a}}, & \text{weil } \frac{\mathfrak{a}(\gamma)}{(\delta)} = \mathfrak{b} \text{ ganz,} \\ & \delta & \equiv & 0 \mod \frac{\delta}{\mathfrak{a}}, & \text{“ } \mathfrak{a} \text{ ganz,} \\ \hline \text{also} & \delta \pm \gamma & \equiv & 0 \mod \frac{\delta}{\mathfrak{a}} & \end{array}$$

und somit $\mathfrak{a}\frac{(\delta\pm\gamma)}{(\delta)} = \mathfrak{a}(1 \pm \varrho)$ ganz, also auch $\widehat{\alpha}(1 \pm \varrho)$, w. z. b. w.

Wir beweisen weiter:

Satz 14. Für jede Klasse C gibt es eine Basis $\widehat{\omega}_1, \ldots, \widehat{\omega_n}$ von n ganzen idealen Zahlen aus C, sodaß jede ganze Zahl $\widehat{\alpha}$ aus C eindeutig in der Form:

$$\widehat{\alpha} = c_1\widehat{\omega}_1 + \cdots + c_n\widehat{\omega}_n$$

mit ganzen rationalen Koeffizienten c_i darstellbar ist. Der Betrag der Determinante

$$\Delta = \left|\widehat{\omega}_i^{(k)}\right|$$

ist $|\Delta| = |\sqrt{d}|$, wo d die Körperdiskriminante ist.

Beweis: Sei $\widehat{\gamma}$ ein Repräsentant von C und $(\widehat{\gamma}) = c$, ferner $\gamma_1, \ldots, \gamma_n$ eine Basis für das Ideal $\frac{1}{c}$. Dann erfüllen die n idealen Zahlen

$$\widehat{\omega}_i = \widehat{\gamma}\gamma_i\,; \qquad (i = 1, \ldots, n)$$

die im Satz genannten Behauptungen.

1.) Es sind tatsächlich ganze ideale Zahlen, weil die γ_i ganze Multipla von $\frac{1}{c}$, also die $\widehat{\gamma}\gamma_i$ ganze Multipla von (1) sind.

2.) Ist $\widehat{\alpha}$ eine ganze Zahl aus C und $\widehat{\alpha} = \widehat{\gamma}\varrho$, so ist sicher ϱ teilbar durch $\frac{1}{c}$, also mit ganzen rationalen c_i

$$\varrho = c_1\gamma_1 + \cdots + c_n\gamma_n\,,$$

da ja die γ_i eine Basis für $\frac{1}{c}$ bilden. Daraus folgt aber

$$\widehat{\alpha} = c_1\widehat{\omega}_1 + \cdots + c_n\widehat{\omega}_n\,.$$

3.) Diese Darstellung ist eindeutig, denn aus $\widehat{\alpha} = 0$ folgte $\frac{\widehat{\alpha}}{\widehat{\gamma}} = 0$, also $\varrho = 0$ und somit wegen der Eindeutigkeit der Basisdarstellung für Ideale: alle $c_i = 0$.

4.) Bekanntlich ist dem Betrage nach

$$\left|\gamma_i^{(k)}\right| = N\left(\frac{1}{c}\right) + |\sqrt{d}|,$$

also

$$\begin{aligned} |\Delta| = |\widehat{\omega}_i^{(k)}| &= |\widehat{\gamma}^{(k)}\gamma_i^{(k)}| = |N(\widehat{\gamma})||\gamma_i^{(k)}| \\ &= |N(\widehat{\gamma})|N\left(\frac{1}{c}\right)|\sqrt{d}| \end{aligned}$$

und nach Satz 11: $|\Delta| = |\sqrt{d}|$, w. z. b. w.

Die *Teilbarkeit für ideale Zahlen* ist auf Grund der Teilbarkeit der entsprechenden Ideale ohne weiteres definiert, ebenso der Begriff „*relativ prim*“. Daher können wir nunmehr den Begriff der Kongruenz auf ideale Zahlen übertragen; da es sich hierbei auch um Addition/Subtraktion handelt, müssen die zu betrachtenden idealen Zahlen einer Klasse angehören. Dies nehmen wir in die Definition der Kongruenz mit auf, indem wir festsetzen:

$$\widehat{\alpha} \equiv \widehat{\beta} \mod \widehat{\varphi}$$

bedeutet:

$\widehat{\alpha}$ und $\widehat{\beta}$ gehören einer Klasse an und
$\widehat{\alpha} - \widehat{\beta}$ ist durch $\widehat{\varphi}$ teilbar. *

Satz 15. Es gelten die elementaren Regeln für das Rechnen mit Kongruenzen zwischen idealen Zahlen.

Beweis.

1.) *Transitivität*:

$$\text{aus} \quad \widehat{\alpha} \equiv \widehat{\beta};\ \widehat{\beta} \equiv \widehat{\gamma} \mod \widehat{\varphi}$$
$$\text{folgt} \quad \widehat{\alpha} \equiv \widehat{\gamma} \mod \widehat{\varphi}.$$

* $\widehat{\varphi}$ braucht natürlich nicht zur Klasse von $\widehat{\alpha}$ und $\widehat{\beta}$ zu gehören. — Der Modul $\widehat{\varphi}$ soll stets *ganz* sein.

36 II

Denn dann sind

$$\frac{\widehat{\alpha}-\widehat{\beta}}{\widehat{\varphi}};\ \frac{\widehat{\beta}-\widehat{\gamma}}{\widehat{\varphi}}$$

ganze ideale Zahlen einer Klasse, also auch ihre Summe

$$\frac{\widehat{\alpha}-\widehat{\gamma}}{\widehat{\varphi}}$$

(distributives Gesetz für Addition/Subtraktion, Multiplikation/Division! Dies ist natürlich nach Definition der Addition richtig, wie man sofort nachweist).

2.) *Addition von Kongruenzen.*

Zwei Kongruenzen in ein– und derselben Klasse dürfen addiert und subtrahiert werden. Es genügt zu zeigen:

$$\text{aus}\quad \widehat{\alpha}\equiv 0;\ \widehat{\beta}\equiv 0 \mod \widehat{\varphi}\ ^{\dagger}\quad\text{und}\quad \widehat{\alpha}=\widehat{\beta}\varrho$$
$$\text{folgt}\quad \widehat{\alpha}\pm\widehat{\beta}\equiv 0 \mod \widehat{\varphi}.$$

Das ist richtig. Denn n. V. sind $\frac{\widehat{\alpha}}{\widehat{\varphi}}$, $\frac{\widehat{\beta}}{\widehat{\varphi}}$ zwei ganze ideale Zahlen einer Klasse, also auch

$$\frac{\widehat{\alpha}}{\widehat{\varphi}}\pm\frac{\widehat{\beta}}{\widehat{\varphi}}=\frac{\widehat{\alpha}\pm\widehat{\beta}}{\widehat{\varphi}}$$

ganz.

3.) *Multiplikation von Kongruenzen.*

Es ist zu zeigen:

a.) Aus $\widehat{\alpha}\equiv 0 \mod \widehat{\varphi}$ folgt $\widehat{\beta}\widehat{\alpha}\equiv 0 \mod \widehat{\varphi}$, wenn $\widehat{\beta}$ prim zu $\widehat{\varphi}$.

Das ist idealtheoretisch klar. Hiernach ist jede lineare Kongruenz

$$\widehat{\beta}\widehat{x}\equiv\widehat{\alpha}\mod\widehat{\varphi},\qquad(\widehat{\beta}\ \text{ prim zu }\ \widehat{\varphi})$$

37 II

[†]Die Kongruenz $\widehat{\alpha}\equiv 0 \mod \widehat{\varphi}$ stellt natürlich an die Klasse von $\widehat{\alpha}$ keine Anforderung, da nach Satz 12 die Null jeder Klasse angehört.

auflösbar durch $\widehat{x} \equiv \frac{\widehat{\alpha}}{\widehat{\beta}} \mod \widehat{\varphi}$ und auch eindeutig.

b.) Ersichtlich folgt aus $\widehat{\alpha} \equiv 1 \mod \widehat{\varphi}$, daß $\widehat{\alpha} = \alpha$ eine Körperzahl und $\alpha \equiv 1 \mod \widehat{\varphi}$, also prim zu $\widehat{\varphi}$ ist. Natürlich folgt dann aus

$$\widehat{\alpha} \equiv 1 \mod \widehat{\varphi};\ \widehat{\beta} \equiv 1 \mod \widehat{\varphi},$$

daß

$$\widehat{\alpha}\widehat{\beta} \equiv 1 \mod \widehat{\varphi} \quad \text{ist.}$$

Übrigens folgt aus $\widehat{\alpha} \equiv \widehat{\beta} \mod \widehat{\varphi}$, daß $\widehat{\alpha}$ und $\widehat{\beta}$ stets gleichzeitig prim oder nicht prim zu $\widehat{\varphi}$ sind. Denn ist $\widehat{\alpha}$ prim zu $\widehat{\varphi}$, so ist nach a.)

$$\frac{\widehat{\beta}}{\widehat{\alpha}} \equiv 1 \mod \widehat{\varphi},$$

also $\frac{\widehat{\beta}}{\widehat{\alpha}}$ prim zu $\widehat{\varphi}$, und somit auch $\widehat{\beta}$.

Nach a.) und b.) gilt für zu $\widehat{\varphi}$ prime Zahlen:

$$\text{Aus} \quad \widehat{\alpha} \equiv \widehat{\beta};\ \widehat{\gamma} \equiv \widehat{\delta} \mod \widehat{\varphi}$$

folgt:

$$\widehat{\alpha}\widehat{\gamma} \equiv \widehat{\beta}\widehat{\delta} \mod \widehat{\varphi}.$$

Damit sind die elementaren Rechenregeln für Kongruenzen hergeleitet. Wir beweisen auf Grund derselben:

Satz 16. Die für den Bereich von $\widehat{\varphi}$ ganzen Zahlen jeder Klasse C von $\mathfrak{Z}$ zerfallen nach jedem Modul $\widehat{\varphi}$ in *Restklassen*, sodaß alle und nur die Zahlen einer Restklasse mod $\widehat{\varphi}$ kongruent sind. Die Anzahl der Restklassen mod $\widehat{\varphi}$ innerhalb jeder Klasse C ist $|N(\widehat{\varphi})|$. Sie bilden nach der Addition eine Abelsche Gruppe vom Grade $|N(\widehat{\varphi})|$. Die zu $\widehat{\varphi}$ primen Restklassen innerhalb aller h Klassen bilden eine Abelsche Gruppe bezüglich der Multiplikation vom Grade $h\Phi(\widehat{\varphi})$, wo Φ die Eulersche Funktion ist.

Beweis: 1.) Die Möglichkeit der Einteilung in Restklassen ist selbstverständlich nach 1.) S. 35▸.

2.) Nach 2.) S. 36▸ bilden die idealen Zahlen der Eigenschaft $\widehat{\alpha} \equiv 0 \mod \widehat{\varphi}$ innerhalb jeder Klasse eine Gruppe bezüglich Addition. Deren Nebengruppen‡ sind gerade die Restklassen innerhalb der zugrundegelegten Klasse. Es ist nur zu zeigen, daß die Anzahl $|N(\widehat{\varphi})|$ ist. Für die Hauptklasse ist dies klar. Sei $\gamma_1, \ldots, \gamma_N$ ein Repräsentantensystem von $|N(\widehat{\varphi})|$ Restklassen mod $\widehat{\varphi}$ in der Hauptklasse und $\widehat{\gamma}$ eine zu $\widehat{\varphi}$ prime Zahl innerhalb einer beliebigen Klasse C. Dann ist

$$\widehat{\gamma}\gamma_1, \ldots \widehat{\gamma}\gamma_N$$

ein vollständiges Repräsentantensystem für die Restklassen in C. Denn ist einerseits $\widehat{\alpha} = \widehat{\gamma}\varrho$ eine beliebige Zahl aus C und $\varrho \equiv \gamma_i \mod \widehat{\varphi}$, so folgt nach 3.) a.) S. 36▸:

$$\widehat{\alpha} = \widehat{\gamma}\varrho \equiv \widehat{\gamma}\gamma_i \mod \widehat{\varphi}.$$

Ist andererseits

$$\widehat{\gamma}\gamma_i \equiv \widehat{\gamma}\gamma_k \mod \widehat{\varphi},$$

so folgt

$$\gamma_i \equiv \gamma_k \mod \widehat{\varphi}, \quad \text{also} \quad i = k.$$

3.) Natürlich bilden die primen Restklassen mod $\widehat{\varphi}$ innerhalb der Hauptklasse eine Gruppe bezüglich der Multiplikation. Diese hat bekanntlich den Grad $\Phi(\widehat{\varphi})$. Ferner bilden *alle* primen Restklassen mod. $\widehat{\varphi}$ (innerhalb aller Klassen) eine Gruppe bezüglich der Multiplikation, wie leicht aus 3.) S. 36/37▸

39 II

folgt, nämlich einfach die Gruppe der Nebengruppen zur Gruppe $\widehat{\alpha} \equiv 1 \mod \widehat{\varphi}$ innerhalb der Gruppe aller zu $\widehat{\varphi}$ primen idealen Zahlen. Daraus folgt sofort, daß diese Gruppe den Grad $h\Phi(\widehat{\varphi})$ hat, weil die primen Restklassen innerhalb der übrigen Klassen die Nebengruppen zur Untergruppe der primen Restklassen in der Hauptklasse sind, und somit in jeder Klasse genau $\phi(\widehat{\varphi})$ prime Restklassen enthalten sind.

(Unter $\Phi(\widehat{\varphi})$ ist natürlich $\phi(f)$ zu verstehen, wenn $(\widehat{\varphi}) = f$ ist. Für die Kongruenzmoduln $\widehat{\varphi}$ ist offenbar die Schreibweise als ideale Zahlen nur formal, so daß wir hier auch einfach Ideale f schreiben können, während für

‡innerhalb der Gruppe aller für $\widehat{\varphi}$ ganzen Zahlen der betr. Klasse.

die den Kongruenzen zu unterwerfenden idealen Zahlen die Schreibweise als ideale Zahlen den Hauptgrund für die Einführung derselben liefert und mehr als eine formale Abänderung der Schreibweise als Ideal bedeutet).

Für uns wichtiger ist die zweite Gruppe von Satz 16, die Gruppe der sämtlichen primen Restklassen mod f innerhalb des Systems aller Klassen von $\mathfrak{Z}$. Wie bezeichnen fortan diese Restklassen mod f kurz als „*Klassen in weiterem Sinne*“ mod f und ihre Abelsche Gruppe, die den Bereich aller zu f primen Zahlen von $\mathfrak{Z}$ umfaßt, vom Grade $h\phi(f)$ mit $\mathfrak{Z}(f)$. Die Hauptklasse mod f in diesem weiteren Sinne besteht also aus allen $\widehat{\alpha} \equiv 1 \mod f$, d. h. aus allen Körperzahlen $\equiv 1 \mod f$.

Neben dieser Klasseneinteilung mod f der zu f primen Zahlen von $\mathfrak{Z}$ *in weiterem Sinne* führen wir noch eine solche *in engerem Sinne*, d. h. mit Vorzeichenbedingung ein, indem wir als Hauptklasse die Zahlen

$$\widehat{\alpha} \equiv 1 \mod f, \quad \text{total positiv},$$

d. h. die total positiven Körperzahlen $\equiv 1 \mod f$ wählen. Bekanntlich zerfällt dann die Hauptklasse mod f in weiterem Sinne in 2^{r_1} Klassen mod f im engeren Sinne, und somit nach gruppentheoretischen Prinzipien jede Klasse in weiterem Sinne in 2^{r_1} Klassen in engerem Sinne. Die Klassen in engerem Sinne bilden also eine Abelsche Gruppe $\mathfrak{Z}_0(f)$ vom Grad $2^{r_1} h\Phi(f)$.

Satz 17. Teilt man alle zu dem ganzen Modul f primen Zahlen von $\mathfrak{Z}$ in Klassen mod f ein, und zwar

a.) *im weiteren Sinne*:

$\widehat{\alpha}$ und $\widehat{\beta}$ kommen in dieselbe Klasse mod f, wenn

$$\widehat{\alpha} \equiv \widehat{\beta} \mod f,$$

also Hauptklasse

$$\widehat{\alpha} \equiv 1 \mod f,$$

b.) *im engeren Sinne*:

$\widehat{\alpha}$ und $\widehat{\beta}$ kommen in dieselbe Klasse mod f, wenn

$$\widehat{\alpha} \equiv \widehat{\beta} \mod f, \quad \frac{\widehat{\alpha}}{\widehat{\beta}} \text{ total positiv},$$

also Hauptklasse

$$\widehat{\alpha} \equiv 1 \mod f, \quad \text{total positiv},$$

41 II

so bilden diese Klassen mod f eine Abelsche Gruppe $\mathfrak{Z}(f)$ bezw. $\mathfrak{Z}_0(f)$ vom Grade $h\Phi(f)$ bezw. $2^{r_1}h\phi(f)$ und jede Klasse von $\mathfrak{Z}(f)$ zerfällt in 2^{r_1} Klassen von $\mathfrak{Z}_0(f)$.

Jeder Klasse mod f im Sinne a.) oder b.) kommen innerhalb ihrer Gruppe ein System von Gruppencharakteren zu. Ist $\widehat{\alpha}$ eine zu f prime Zahl, so seien die Gruppencharaktere der Klasse von $\widehat{\alpha}$

$$\begin{aligned} &\text{im Falle a.) mit } \chi(\widehat{\alpha}) \\ &\text{im Falle b.) mit } \chi_0(\widehat{\alpha}) \end{aligned}$$

bezeichnet. Es gilt also für zu f prime $\widehat{\alpha}, \widehat{\beta}$:

$$\begin{cases} \chi(\widehat{\alpha}) = \chi(\widehat{\beta}), & \text{wenn} \quad \widehat{\alpha} \equiv \widehat{\beta} \mod f \\ \chi(\widehat{\alpha})\chi(\widehat{\beta}) = \chi(\widehat{\alpha}\widehat{\beta}) \end{cases} \tag{3}$$

$$\begin{cases} \chi_0(\widehat{\alpha}) = \chi_0(\widehat{\beta}), & \text{wenn} \quad \widehat{\alpha} \equiv \widehat{\beta} \mod f, \quad \frac{\widehat{\alpha}}{\widehat{\beta}} \quad \text{total positiv} \\ \chi_0(\widehat{\alpha})\chi_0(\widehat{\beta}) = \chi_0(\widehat{\alpha}\widehat{\beta}) \end{cases} \tag{4}$$

Durch (3) und (4) werden bekanntlich die Charaktere χ, χ_0 vollständig charakterisiert, d. h. eine Funktion χ, χ_0 mit den Eigenschaften (3) bezw. (4) ist sicher ein Gruppencharakter für $\mathfrak{Z}(f)$ bezw. $\mathfrak{Z}_0(f)$. Es gibt genau $h\phi(f)$ bezw. $2^{r_1}h\phi(f)$ Charaktere χ bezw. χ_0. Natürlich kann in (3), (4) an Stelle der ersten Bedingung vermöge der zweiten die äquivalente

$$\begin{aligned} \chi(\widehat{\alpha}) = 1, \quad &\text{wenn} \quad \widehat{\alpha} \equiv 1 \mod f \\ \chi_0(\widehat{\alpha}) = 1, \quad &\text{wenn} \quad \widehat{\alpha} \equiv 1 \mod f, \quad \text{total positiv} \end{aligned}$$

42 II

treten, was für die Anwendung brauchbarer ist.

Wir haben noch den Zusammenhang der χ und χ_0 näher zu untersuchen. Sei χ_0 ein Charakter von $\mathfrak{Z}_0(f)$. Für die Hauptklasse mod f in weiterem Sinne

$$\widehat{\alpha} = \alpha \equiv 1 \mod f$$

ist $\big(\chi_0(\alpha)\big)^2 = \chi_0(\alpha^2) = 1$, weil α^2 total positiv, $\equiv 1 \mod f$ ist, also $\chi_0(\alpha) = \pm 1$. Wir können aber die Form von $\chi_0(\alpha)$ für $\alpha \equiv 1 \mod f$ noch genauer angeben, wenn wir $\chi_0(\alpha)$ für diese α als Charaktere derjenigen Abelschen Gruppe auffassen, in die die weitere Hauptklasse durch die engeren Klassen zerfällt. Dies ist gruppentheoretisch natürlich ohne weiteres begründet, da χ_0 die Produktbedingung erfüllt und für das Einheitselement, d. h. $\alpha \equiv 1 \mod f$, total positiv, den Wert 1 hat. Nun ist die Basisdarstellung der genannten Gruppe, d. h. der Gruppe der engeren Klassen mit der Bedingung $\alpha \equiv 1 \mod f$ von der Form

$$\mathfrak{k} = \mathfrak{k}_1^{b_1} \dots \mathfrak{k}_{r_1}^{b_{r_1}}; \qquad (b_i = 0, 1),$$

wo die r_1 Basiselemente $\mathfrak{k}_1, \dots, \mathfrak{k}_{r_1}$ den r_1 Signaturen

$$(-1, +1, \dots, +1)$$
$$(+1, -1, \dots, +1)$$
$$(+1, +1, \dots, -1)$$

entsprechend gewählt werden können. Ist dann α ein Repräsentant aus $\mathfrak{k}$, also von der Signatur

$$(-1)^{b_1}, (-1)^{b_2}, \dots, (-1)^{b_{r_1}}$$

so werden bekanntlich die 2^{r_1} der genannten Gruppe entsprechenden

Charaktere durch

$$\chi_0(\alpha) = (-1)^{a_1 b_1} \cdots (-1)^{a_{r_1} b_{r_1}}; \qquad (a_i = 0, 1)$$

mit irgendwelchen[§] Exponenten a_i gegeben, haben also die Form

$$\chi_0(\alpha) = (\operatorname{sgn} \alpha^{(1)})^{a_1} \dots (\operatorname{sgn} \alpha^{(r_1)})^{a_{r_1}}$$

für jedes $\alpha \equiv 1 \mod f$.

[§] eindeutig durch $\chi_0(\alpha)$ bestimmten

Nun ist $\operatorname{sgn}\alpha$ eine nur für reelles α definierte Funktion von α; die Verallgemeinerung für beliebige α[1] wird durch die Funktion $\frac{\alpha}{|\alpha|}$ gegeben, die für reelles α gleich $\operatorname{sgn}\alpha$ ist. Dementsprechend bilden wir jetzt aus unserem gegebenen $\chi_0(\widehat{\alpha})$ die Funktion

$$g(\widehat{\alpha}) = \chi_0(\widehat{\alpha}) \left(\frac{\widehat{\alpha}^{(1)}}{|\widehat{\alpha}^{(1)}|}\right)^{-a_1} \cdots \left(\frac{\widehat{\alpha}^{(r_1)}}{|\widehat{\alpha}^{(r_1)}|}\right)^{-a_{r_1}},$$

indem wir den a_i die eben bestimmten Werte 0 oder 1 beilegen, die χ_0 nach der durchgeführten Betrachtung zugeordnet sind.

Dieses $g(\widehat{\alpha})$ erfüllt erstens die Produktbedingung, da es die $\left(\frac{\widehat{\alpha}^{(i)}}{|\widehat{\alpha}^{(i)}|}\right)$ und $\chi_0(\widehat{\alpha})$ tun, zweitens ist für $\widehat{\alpha} \equiv 1 \mod f$ nach Wahl der a_i:

$$g(\widehat{\alpha}) = 1$$

Nach (3) ist daher $g(\widehat{\alpha})$ ein Charakter von $\mathfrak{Z}(f)$, also ein bestimmtes $\chi(\widehat{\alpha})$. Es gibt somit zu jedem $\chi_0(\widehat{\alpha})$ ein $\chi(\widehat{\alpha})$, sodaß

$$\chi_0(\widehat{\alpha}) = v(\widehat{\alpha})\chi(\widehat{\alpha}) \tag{5}$$

ist, wobei

$$v(\widehat{\alpha}) = \left(\frac{\widehat{\alpha}^{(1)}}{|\widehat{\alpha}^{(1)}|}\right)^{a_1} \cdots \left(\frac{\widehat{\alpha}^{(r_1)}}{|\widehat{\alpha}^{(r_1)}|}\right)^{a_{r_1}}; \qquad (a_i = 0, 1) \tag{6}$$

eine Funktion von $\widehat{\alpha}$ ist, die wir *Vorzeichencharakter* von $\widehat{\alpha}$ nennen, weil sie für Körperzahlen α ein solcher ist.

Die Zerlegung (5) von $\chi_0(\widehat{\alpha})$ ist ferner eine eindeutige; denn beständen zwei Zerlegungen dieser Art für ein $\chi_0(\widehat{\alpha})$, so folgte eine Gleichung

$$1 = v(\widehat{\alpha})\chi(\widehat{\alpha})$$

für alle $\widehat{\alpha}$, wo die Exponenten von $v(\widehat{\alpha})$ die Werte $0, \pm 1$ haben können, und $\chi(\widehat{\alpha})$ ein Charakter von $\mathfrak{Z}(f)$ ist. Bezeichnet wie üblich $\overline{\chi}(\widehat{\alpha}) = \frac{1}{\chi(\widehat{\alpha})}$ den konjugiert komplexen Charakter, so folgte

$$\overline{\chi}(\widehat{\alpha}) = v(\widehat{\alpha})$$

[1] Variablenname ist nicht eindeutig lesbar; vielleicht auch d.

also speziell für $\widehat{\alpha} = \alpha \equiv 1 \mod f$:

$$v(\alpha) = 1.$$

Dann müssen aber die Exponenten in $v(\alpha)$ alle Null sein, da sonst ein $\alpha \equiv 1 \mod f$ angebbar wäre, für das $v(\alpha) \neq 1$ wäre. Es ist also identisch $v(\widehat{\alpha}) = 1$ und somit auch identisch $\chi(\widehat{\alpha}) = 1$, woraus die Eindeutigkeit von (5) ohne weiteres folgt.

Für den konjugiert komplexen Charakter $\overline{\chi}_0(\widehat{\alpha}) = \frac{1}{\chi_0(\widehat{\alpha})}$ folgt aus (5):

$$\overline{\chi}_0(\widehat{\alpha}) = \frac{1}{v(\widehat{\alpha})} \cdot \overline{\chi}(\widehat{\alpha}) = v(\widehat{\alpha}) \cdot \frac{\overline{\chi}(\widehat{\alpha})}{v^2(\widehat{\alpha})}\,.$$

Da $v^2(\widehat{\alpha}) = 1$ ist für alle Körperzahlen (Zahlen der Hauptklasse mod 1) ist $v^2(\widehat{\alpha})$ schon Charakter für die absolute Klassengruppe $\mathfrak{Z}(1)$, umsomehr für $\mathfrak{Z}(f)$, also sicher ein $\chi(\widehat{\alpha})$. Daher ist

$$\overline{\chi}_0(\widehat{\alpha}) = v(\widehat{\alpha})\,\frac{\overline{\chi}(\widehat{\alpha})}{v^2(\widehat{\alpha})} \tag{5a}$$

die eindeutige Zerlegung (5) für den konjugiert komplexen Charakter.

Da natürlich umgekehrt jedes $\chi(\widehat{\alpha})$ ein $\chi_0(\widehat{\alpha})$ ist, haben wir folgendes Resultat:

Satz 18. Zwischen den Gruppencharakteren $\chi(\widehat{\alpha})$ von $\mathfrak{Z}(f)$ und $\chi_0(\widehat{\alpha})$ von $\mathfrak{Z}_0(f)$ besteht folgender Zusammenhang:

1.) Jedes $\chi(\widehat{\alpha})$ ist ein $\chi_0(\widehat{\alpha})$.

2.) Zu jedem $\chi_0(\widehat{\alpha})$ gibt es einen eindeutig bestimmten Vorzeichencharakter $v(\widehat{\alpha})$ der Form (6), sodaß die Zerlegung (5) besteht. Der konjugiert komplexe Charakter $\overline{\chi}_0(\alpha)$ zerlegt sich dann nach (5a).

2.3 §3 Gruppen– und Größencharaktere für Ideale.

46 II

Analog wie die Einteilung der zu f primen *Zahlen* $\widehat{\alpha}$ von $\mathfrak{Z}$ in Klassen mod f läßt sich auch eine Einteilung der zu f primen Ideale $(\widehat{\alpha})$ von $\mathfrak{Z}$ in Klassen mod f definieren:

a.) *Weiterer Klassenbegriff* mod f.

Zwei zu f prime Ideale $(\widehat{\alpha})$ und $(\widehat{\beta})$ heißen äquivalent mod f, wenn es eine Körpereinheit ε gibt, sodaß

$$\widehat{\alpha} \equiv \varepsilon\widehat{\beta} \mod f$$

ist. Die Hauptklasse ist also

$$\widehat{\alpha} = \alpha \equiv \varepsilon \mod f,$$

die übrigen Klassen die Nebengruppen hierzu und ihre Gruppe $\mathfrak{J}(f)$ Abelsch von einem Grade $h(f)$.

b.) *Engerer Klassenbegriff* mod f.

Zwei zu f prime Ideale $(\widehat{\alpha})$ und $(\widehat{\beta})$ heißen äquivalent mod f, wenn es eine Körpereinheit ε gibt, sodaß

$$\widehat{\alpha} \equiv \varepsilon\widehat{\beta} \mod f, \quad \frac{\widehat{\alpha}}{\varepsilon\widehat{\beta}} \text{ total positiv}$$

ist. Die Hauptklasse ist also

$$\widehat{\alpha} = \alpha \equiv \varepsilon \mod f, \quad \frac{\alpha}{\varepsilon} \text{ total positiv}$$

und die übrigen Klassen die Nebengruppen hierzu, ihre Gruppe $\mathfrak{J}_0(f)$ Abelsch von einem Grade $h_0(f)$.

47 II

Es gilt für diese Klasseneinteilung:

Satz 19. Die soeben definierten Idealklassen in weiterem und engerem Sinne mod f sind mit den Strahlklassen mod f nach dem Strahl der (total positiven) Zahlen $\equiv 1 \mod f$ identisch.

Beweis: 1.) Sind $(\widehat{\alpha}) = \mathfrak{a}$, $(\widehat{\beta}) = \mathfrak{b}$ zwei in dem eben definierten Sinne a.) bezw. b.) äquivalente (zu f prime) Ideale, also

$$\frac{\widehat{\alpha}}{\widehat{\beta}} \equiv \varepsilon \mod f; \quad \left(\text{ev.} \quad \frac{\widehat{\alpha}}{\varepsilon\widehat{\beta}} \quad \text{total positiv}\right)$$

so ist zunächst nach Definition der Kongruenz für ideale Zahlen $\frac{\widehat{\alpha}}{\widehat{\beta}} = \gamma$ eine zu f prime Körperzahl und

$$\gamma \equiv \varepsilon \mod f; \quad \left(\text{ev.} \quad \frac{\gamma}{\varepsilon} \quad \text{total positiv}\right).$$

Ferner ist $\frac{\mathfrak{a}}{\mathfrak{b}} = \left(\frac{\widehat{\alpha}}{\widehat{\beta}}\right) = (\gamma) = \left(\frac{\gamma}{\varepsilon}\right)$, woraus die Äquivalenz im Sinne der Strahlklassen mod f (im engeren oder weiteren Sinne) sofort folgt.

2.) Ist $\frac{\mathfrak{a}}{\mathfrak{b}} = (\gamma)$ und $\gamma \equiv 1 \mod f$ (ev. tot. pos.), so ist nach Satz 10 wegen der Gleichheit der Ideale

$$(\gamma) = \frac{\mathfrak{a}}{\mathfrak{b}} \quad \text{und} \quad \left(\frac{\widehat{\alpha}}{\widehat{\beta}}\right):$$

$$\frac{\widehat{\alpha}}{\widehat{\beta}} = \gamma\varepsilon,$$

wo ε eine Körpereinheit ist, also

$$\frac{\widehat{\alpha}}{\widehat{\beta}} \equiv \varepsilon \mod f \qquad \left(\text{ev.} \quad \frac{\widehat{\alpha}}{\varepsilon\widehat{\beta}} \quad \text{total positiv}\right)$$

w. z. b. w.

Den Gruppen $\mathfrak{J}(f), \mathfrak{J}_0(f)$ entsprechen Systeme von $h(f)$ bzw. $h_0(f)$ Gruppencharakteren, die mit

$$\chi\big((\widehat{\alpha})\big) \quad \text{bezw.} \quad \chi_0\big((\widehat{\alpha})\big)$$

bezeichnet werden sollen und *Klassen– oder Gruppencharaktere des Ideals* $(\widehat{\alpha})$ heißen sollen.

Da offenbar die Klassen für Ideale $(\widehat{\alpha})$ dieses §▸ jede in gleich viel Zahlklassen mod f im Sinne des vorigen §▸ zerfallen — die Hauptklasse $\alpha \equiv 1 \mod f$ von §2▸ ist Untergruppe der Hauptklasse $\alpha \equiv \varepsilon \mod f$ dieses §3▸ — ist jeder Charakter $\chi\big((\widehat{\alpha})\big)$ bezw. $\chi_0\big((\widehat{\alpha})\big)$ a fortiori ein Charakter $\chi(\widehat{\alpha})$ bezw. $\chi_0(\widehat{\alpha})$ im Sinne von §2.

Zu diesen auch auf Grund der Strahlklasseneinteilung in früherem Sinne resultierenden Klassencharakteren $\chi\big((\widehat{\alpha})\big), \chi_0\big((\widehat{\alpha})\big)$ von Idealen treten nun weiter als neuartige Elemente die *Größencharaktere von Idealen*, die aus den Größencharakteren $\lambda(\widehat{\alpha})$ im Sinne von §1▸, speziell Satz 9 entspringen.

In der Tat stellt jede ideale Zahl $\widehat{\alpha}$ im Sinne von Satz 9 einen Vektor dar, der nach Definition der konjugierten $\widehat{\alpha}^{(p)}$ a. S. 30▸ der einzigen im Satz 9 gestellten Forderung bezüglich der konjugiert–komplexen Körper genügt, sodaß die Funktionen $\lambda(\widehat{\alpha})$ im Sinne von §1▸ gebildet werden können.

Aus jedem solchen Größencharakter mod f *der Zahl* $\widehat{\alpha}$, $\lambda(\widehat{\alpha})$, soll nun ein Größencharakter $\lambda\big((\widehat{\alpha})\big)$ *des Ideals* $(\widehat{\alpha})$ hergeleitet werden durch folgende Forderungen:

1. $\lambda\big((\widehat{\alpha})\big)\lambda\big((\widehat{\beta})\big) = \lambda\big((\widehat{\alpha}\widehat{\beta})\big)$,
2. $\lambda\big((\alpha)\big) = \lambda(\alpha)$, wenn $\alpha \equiv 1 \mod f$, total positiv,
3. $\lambda\big((\varepsilon\widehat{\alpha})\big) = \lambda\big((\widehat{\alpha})\big)$, oder (was wegen 1.) gleichbedeutend)
   $\lambda\big((\varepsilon)\big) = 1$, wenn ε Körpereinheit,

für irgendwelche zu f prime $\widehat{\alpha}, \widehat{\beta}$ aus $\mathfrak{Z}$.

Ich beweise zuerst:

Satz 20. Zu jedem $\lambda(\widehat{\alpha})$ im Sinne von §1 gibt es tatsächlich ein $\lambda\big((\widehat{\alpha})\big)$ mit den Eigenschaften 1.), 2.), 3.).

Beweis: Wir setzen $\lambda\big((\widehat{\alpha})\big)$ in der Form

$$\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi_0(\widehat{\alpha})$$

mit einem vorläufig unbestimmten Charakter $\chi_0(\widehat{\alpha})$ im Sinne von §2 an. Jedes so gebildete $\lambda\big((\widehat{\alpha})\big)$ hat ersichtlich die Eigenschaften 1.) und 2.). Es ist nur

zu zeigen, daß man $\chi_0(\widehat{\alpha})$ speziell so wählen kann, daß auch 3.) erfüllt ist. Nun hat die Funktion $\lambda(\varepsilon)$ für beliebige Körpereinheiten ε die Eigenschaften (s. Satz 9):

$$\lambda(\varepsilon_1)\lambda(\varepsilon_2) = \lambda(\varepsilon_1\varepsilon_2)$$

und

$$\lambda(\varepsilon) = 1, \qquad \text{wenn} \quad \varepsilon \equiv 1 \mod f, \quad \text{total positiv},$$

d. h.

$$\lambda(\varepsilon_1) = \lambda(\varepsilon_2), \qquad \text{wenn} \quad \varepsilon_1 \equiv \varepsilon_2 \mod f, \qquad \frac{\varepsilon_1}{\varepsilon_2} \quad \text{total positiv.}$$

Definiert man daher eine Funktion $\varphi(\alpha)$ für alle zu

f primen α, die einer Kongruenz

$$\alpha \equiv \varepsilon \mod f; \qquad \frac{\alpha}{\varepsilon} \quad \text{total positiv}$$

genügen*, durch

$$\varphi(\alpha) = \lambda(\varepsilon),$$

wo ε eine zu α kongruente Einheit gleicher Signatur ist, so gilt ersichtlich

$$\begin{aligned} \varphi(\alpha)\varphi(\beta) &= \varphi(\alpha\beta), \\ \varphi(\alpha) &= \varphi(\beta), \qquad \text{wenn } \alpha \equiv \beta \mod f \text{ und } \tfrac{\alpha}{\beta} \text{ total positiv,} \end{aligned}$$

für alle genannten Argumente α, β. $\varphi(\alpha)$ ist also ein Charakter der Gruppe derjenigen Zahlklassen (§2) im engeren Sinne mod f, die durch Einheiten ε geliefert werden, und da diese Gruppe Untergruppe von $\mathfrak{Z}_0(f)$ ist, gibt es bekanntlich einen Charakter $\overline{\chi}_0(\widehat{\alpha})$ von $\mathfrak{Z}_0(f)$, der für jene Untergruppe mit $\varphi(\alpha)$ identisch ist. Es ist dann $\overline{\chi}_0(\widehat{\alpha})$ speziell für Einheiten ε selbst mit $\lambda(\varepsilon)$ identisch, also für den konjugiert–komplexen Charakter $\chi_0(\widehat{\alpha})$:

$$\lambda(\varepsilon)\chi_0(\varepsilon) = 1 \qquad \text{für jede Körpereinheit } \varepsilon.$$

*also für die Hauptklasse von $\mathfrak{J}_0(f)$

Wählt man in der vorangestellten Betrachtung für $\chi_0(\widehat{\alpha})$ speziell den eben gefundenen Charakter, so ist auch 3.) erfüllt, denn für jede Körpereinheit ε folgt:

$$\lambda\big((\varepsilon)\big) = \lambda(\varepsilon)\chi_0(\varepsilon) = 1, \qquad \text{wie es sein soll.}$$

Damit ist Satz 20 bewiesen.

51 II

Ich beweise weiter:

Satz 21. Jeder Größencharakter $\lambda\big((\widehat{\alpha})\big)$ läßt sich eindeutig zerlegen in ein Produkt

$$\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi_0(\widehat{\alpha}) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha}) \cdot v(\widehat{\alpha}). \tag{1}$$

Beweis: Sei $\lambda\big((\widehat{\alpha})\big)$ eine nach Satz 20 sicher existierende Funktion mit den Eigenschaften 1.), 2.), 3.) und $\lambda(\widehat{\alpha})$ die in der Definitionsgleichung 2.) benutzte Funktion; dann ist $g(\widehat{\alpha}) = \frac{\lambda\big((\widehat{\alpha})\big)}{\lambda(\widehat{\alpha})}$ eine Funktion von $\widehat{\alpha}$ mit den Eigenschaften

$$\begin{aligned} g(\widehat{\alpha})g(\widehat{\beta}) &= g(\widehat{\alpha}\widehat{\beta}), \\ g(\alpha) &= 1, \qquad \text{wenn} \quad \alpha \equiv 1 \mod f, \quad \text{total pos.}, \end{aligned}$$

also nach (4) S. 41 ein Charakter $\chi_0(\widehat{\alpha})$. Es ist somit

$$\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi_0(\widehat{\alpha}).$$

Bestände noch eine zweite Zerlegung dieser Art, so folgte eine Relation der Form

$$\frac{\lambda'}{\lambda}(\widehat{\alpha})\,\frac{\chi_0'}{\chi_0}(\widehat{\alpha}) = 1$$

für alle $\widehat{\alpha}$, da ja die λ und die χ Gruppen bezüglich Multiplikation bilden. Dann folgte aber:

$$\frac{\lambda'}{\lambda}(\alpha) = 1 \quad \text{für} \quad \alpha \equiv 1 \mod f, \quad \text{total positiv.}$$

Nun gibt es sicher zu f prime Körperzahlen, deren konjugierte in beliebiger Nähe eines vorgegebenen Körpervektors liegen, weil bekanntlich die Körperzahlen im n–dimensionalen Körpervektoren–Raum (Koordinaten $|x_1|, \ldots, |x_{r_1}|, |x_{r_1+1}|, \ldots, |x_{r_1+r_2}|$,

52 II

$\varphi_{r_1+1}, \dots \varphi_{r_1+r_2}$) überall dicht liegen und ersichtlich (Addition einer sehr kleinen rationalen Zahl) in jeder beliebigen Nähe einer zu f nicht primen Körperzahl auch eine zu f prime liegt. Durch passende Wahl des vorzugebenden Körpervektors folgt so, daß auch ein beliebiger Körpervektor beliebig nahe durch eine total positive Zahl $\alpha \equiv 1 \mod f$ approximiert werden kann. Denn ist γ prim zu f so ist $\gamma^{2\phi(f)} \equiv 1 \mod f$ und total positiv.

Wäre also $\frac{\lambda'}{\lambda}(\widehat{\alpha})$ nicht identisch 1, so gäbe es einen Körpervektor x, für den $\frac{\lambda'}{\lambda}(x) \neq 1$ wäre. Approximiert man dann x beliebig nahe durch eine Zahl $\alpha \equiv 1 \mod f$, total positiv, so folgte wegen der Stetigkeit von $\frac{\lambda'}{\lambda}(x)$, daß auch $\frac{\lambda'}{\lambda}(\alpha) \neq 1$ wäre, worin ein Widerspruch liegt. Daher ist $\frac{\lambda'}{\lambda}(\widehat{\alpha})$ identisch 1, also auch $\frac{\chi_0'}{\chi}(\widehat{\alpha})$, und somit folgt die Identität beider Darstellungen von $\lambda\big((\widehat{\alpha})\big)$.

Nach Satz 18 bestimmt dann $\chi_0(\widehat{\alpha})$ weiter eindeutig ein $v(\widehat{\alpha})$, sodaß $\chi_0(\widehat{\alpha}) = v(\widehat{\alpha})\chi(\widehat{\alpha})$ ist. Damit ist Satz 21 bewiesen.

Wir nennen $\lambda\big((\widehat{\alpha})\big)$ einen *echten Größencharakter*, wenn in der Zerlegung (1) $\lambda(\widehat{\alpha})$ nicht identisch 1 ist. Wegen $|\lambda(\widehat{\alpha})| = 1$, (Satz 9) ist $\overline{\lambda}(\widehat{\alpha}) = \frac{1}{\lambda(\widehat{\alpha})}$. Wegen der Gruppeneigenschaft der λ ist dies wieder ein Größencharakter, somit auch

$$\overline{\lambda}\big((\widehat{\alpha})\big) = \frac{1}{\lambda\big((\widehat{\alpha})\big)} = \overline{\lambda}(\widehat{\alpha})\,\frac{\overline{\chi}(\widehat{\alpha})}{v^2(\widehat{\alpha})}\,v(\widehat{\alpha})$$

53 II

Größencharakter für Ideale $(\widehat{\alpha})$ im Sinne unserer Definition (das ist klar, weil die Definitionsgleichungen erfüllt sind), in seiner Darstellung (1) nach Satz 21.

Es gilt also:

Satz 22. Ist $\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha})v(\widehat{\alpha})$ ein Größencharakter für Ideale in seiner eindeutigen Zerlegung nach Satz 21, so ist

$$\overline{\lambda}\big((\widehat{\alpha})\big) = \overline{\lambda}(\widehat{\alpha})\frac{\overline{\chi}(\widehat{\alpha})}{v^2(\widehat{\alpha})}v(\widehat{\alpha}) \tag{2}$$

die eindeutige Zerlegung des konjugiert–komplexen (reziproken) Größencharakters.

Jedem Größencharakter $\lambda\big((\widehat{\alpha})\big)$ können wir nach Satz 21 ein eindeutig bestimmtes Exponentensystem

$$a_1, \ldots, a_n$$

von n ganzen, nicht negativen Zahlen zuordnen, die *das Exponentensystem von* $\lambda\big((\widehat{\alpha})\big)$ heißen sollen.

Dies System soll bestehen:

1. aus den r_1 Exponenten $a_1, \ldots, a_{r_1}$ $(= 0$ oder $1)$ von $v(\widehat{\alpha})$
2. aus den $2r_2$ Exponenten $a_{r_1+1}, \ldots, a_n$ von $\lambda(\widehat{\alpha})$ aus Satz 8, von denen stets die eine Hälfte Null ist, die andere nicht negativ.

Da $v(\widehat{\alpha})$ für sich durch $\lambda\big((\widehat{\alpha})\big)$ eindeutig bestimmt sind, ferner die $a_1, \ldots, a_{r_1}$ nach S. 43 ▸ durch $v(\widehat{\alpha})$ und die $a_{r_1+1}, \ldots, a_n$ nach Satz 8 eindeutig durch $\lambda(\widehat{\alpha})$ bestimmt sind, ist das

54 II

Exponentensystem (a_i) ersichtlich eindeutig durch $\lambda\big((\widehat{\alpha})\big)$ bestimmt.

Ich beweise noch:

Satz 23. Das zum reziproken Charakter $\overline{\lambda}\big((\widehat{\alpha})\big)$ gehörige Exponentensystem (a_i') wird gegeben durch:

$$(3) \qquad \begin{cases} a_p' = a_p & ; \quad (p = 1, \ldots, r_1) \\ a_{p+r_2}' = a_p\,, \ a_p' = a_{p+r_2} & ; \quad (p = r_1+1, \ldots, r_1+r_2), \end{cases}$$

d. h. bei den von $\lambda(\widehat{\alpha})$ herrührenden Exponenten treten die a_p jetzt gerade an die „konjugiert–komplexe Stelle“.

Beweis: $a_p' = a_p$ für die ersten r_1 Exponenten ist klar nach Satz 22, da zu $\overline{\lambda}\big((\widehat{\alpha})\big)$ dasselbe $v(\widehat{\alpha})$ gehört. Die weitere Behauptung folgt unmittelbar aus Satz 22 und Satz 8, da für das konjugiert–komplexe $\overline{\lambda}(\widehat{\alpha})$ sich die a_p zunächst in $-a_p$ verwandeln und dann nach der dortigen Normierung gerade durch Auswechslung mit den „konjugiert–komplexen Stellen“ wieder in $+a_p$ transformiert werden.

Anmerkung: Die Größencharaktere $\lambda\big((\widehat{\alpha})\big)$ für Ideale sind die allgemeinsten für uns in Frage kommenden Charaktere. Sie umfassen als Spezialfälle $\big(\lambda(\widehat{\alpha}) \equiv 1\big)$ die Klassencharaktere $\chi\big((\widehat{\alpha})\big), \chi_0\big((\widehat{\alpha})\big)$ im engeren und weiteren Sinne, da für $\lambda(\widehat{\alpha}) \equiv 1$ die Definitionsgleichungen in die für $\chi_0\big((\widehat{\alpha})\big)$ übergehen.

2.4 §4 Eigentliche und uneigentliche Charaktere. Verallgemeinerte Gausssche Summen.

55 II

Wir betrachten zunächst die Charaktere $\chi(\widehat{\alpha})$ der Gruppe $\mathfrak{Z}(f)$, (§2), deren charakteristische Definitionsgleichungen (3), S. 41 sind. Es kann sein, daß es einen echten Teiler f_1 des Moduls f gibt, sodaß für einen solchen Charakter $\chi(\widehat{\alpha})$ für alle zu f primen $\widehat{\alpha}, \widehat{\beta}$ gilt:

$$\chi(\widehat{\alpha}) = \chi(\widehat{\beta}), \quad \text{wenn} \quad \widehat{\alpha} \equiv \widehat{\beta} \mod f_1. \tag{1}$$

Dann heißt $\chi(\widehat{\alpha})$ ein *uneigentlicher Charakter* $\mod f$, andernfalls, wenn also kein solcher echter Teiler f_1 existiert, *ein eigentlicher Charakter* $\mod f$.

Satz 24. Jeder uneigentliche Charakter $\chi(\widehat{\alpha}) \mod f$ bestimmt eindeutig einen Charakter $\chi'(\widehat{\alpha})$ nach einem echten Teiler f_1 von f, sodaß für zu f prime $\widehat{\alpha}$ gilt:

$$\chi(\widehat{\alpha}) = \chi'(\widehat{\alpha}).$$

Beweis: Setzen wir, falls (1) für $\chi(\widehat{\alpha})$ besteht,

$$\chi'(\widehat{\alpha}) = \chi(\widehat{\alpha}), \quad \text{wenn } \widehat{\alpha} \text{ prim zu } f,$$

dagegen

$$\chi'(\widehat{\alpha}) = \chi(\widehat{\beta}),$$

wenn $\widehat{\alpha}$ nur prim zu f_1 und $\widehat{\beta} \equiv \widehat{\alpha} \mod f_1$ so gewählt ist, daß $\widehat{\beta}$ prim zu f (was offenbar stets möglich),

56 II

so ist $\chi'(\widehat{\alpha})$ ein Charakter $mod f_1$. Denn erstens ist nach (1) diese Definition eindeutig, zweitens besteht die Produktbedingung

$$\chi'(\widehat{\alpha})\chi'(\widehat{\gamma}) = \chi'(\widehat{\alpha}\widehat{\gamma}),$$

drittens ist $\chi'(\widehat{\alpha})$ für alle zu f_1 primen $\widehat{\alpha}$ definiert und genügt der Bedingung

$$\chi'(\widehat{\alpha}) = \chi'(\widehat{\gamma}), \quad \text{wenn} \quad \widehat{\alpha} \equiv \widehat{\gamma} \mod f_1.$$

Dieser Charakter $\chi'(\widehat{\alpha})$ mod f_1 ist schließlich eindeutig durch $\chi(\widehat{\alpha})$ bestimmt. Denn wäre $\chi''(\widehat{\alpha})$ ein zweiter solcher, Satz 24 genügender, so folgte für alle zu f primen $\widehat{\alpha}$

$$\frac{\chi'}{\chi''}(\widehat{\alpha}) = 1,$$

also da in jeder primen Restklasse mod f_1 zu f prime $\widehat{\alpha}$ existieren

$$\frac{\chi'}{\chi''}(\widehat{\alpha}) = 1, \quad \text{für } \widehat{\alpha} \text{ prim zu } f_1$$

d. h. $\frac{\chi'}{\chi''}(\widehat{\alpha})$ ist der Hauptcharakter von $\mathfrak{Z}(f_1)$, woraus die Eindeutigkeit sofort folgt.

Satz 25. Ist $\chi(\widehat{\alpha})$ ein uneigentlicher Charakter mod f, so existiert ein eindeutig bestimmter Teiler f_0 von f, sodaß $\chi(\widehat{\alpha})$ einen eigentlichen Charakter mod f_0 erzeugt. f_0 ist der größte gemeinsame Teiler aller f_i, nach denen $\chi(\widehat{\alpha})$ überhaupt Charaktere erzeugt, also auch erklärbar als der niedrigste Modul, nach dem überhaupt $\chi(\widehat{\alpha})$ einen Charakter erzeugt.

Beweis: 1.) Erzeugt χ einen Charakter nach f_1 und f_2, so erzeugt er auch einen nach $f_3 = (f_1, f_2)$.

Sind nämlich $\widehat{\alpha}, \widehat{\beta}$ prim zu f und

$$\widehat{\alpha} \equiv \widehat{\beta} \mod f_3,$$

so gibt es eine zu f prime Zahl $\widehat{\mu}$, sodaß

$$\begin{aligned} \widehat{\mu} &\equiv \widehat{\alpha} \mod f_1, \\ \widehat{\mu} &\equiv \widehat{\beta} \mod f_2 \end{aligned}$$

ist (dieser Satz ist für wirkliche Zahlen bekanntlich richtig, für ideale Zahlen folgt er daraus leicht durch „Hin– und Rücktransformation“ auf die Klasse der Körperzahlen mittels eines zu f primen Multiplikators $\widehat{\gamma}$ der inversen Klasse zu $\widehat{\alpha}, \widehat{\beta}$). Dann folgt nach Voraussetzung über χ:

$$\chi(\widehat{\alpha}) = \chi(\widehat{\mu}) = \chi(\widehat{\beta}), \qquad \text{w. z. b. w.}$$

2.) Somit erzeugt γ wirklich einen Charakter nach dem größten gemeinsamen Teiler f_0 aller f_i dieser muß aber eigentlich sein. Denn sonst würde er

einen Charakter nach einem echten Teiler f_0' von f_0 erzeugen, der ersichtlich auch schon von χ selbst erzeugt würde, was mit der Eigenschaft von f_0 als Teiler aller f_i unvereinbar

3.) Natürlich sind die durch χ erzeugten Charaktere nach den echten Multipla von f_0 uneigentlich, da sie einen Charakter nach dem echten Teiler f_0 erzeugen. Es gibt also auch *nur* einen zugeordneten eigentlichen Charakter, eben nach dem Modul f_0.

Die Unterscheidung zwischen eigentlichen und uneigentlichen Charakteren χ übertragen wir auch auf die Größencharaktere $\lambda\big((\widehat{\alpha})\big)$ für Ideale. Sei

$$\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha})v(\widehat{\alpha})$$

ein Größencharakter mod f. Der durch $\lambda\big((\widehat{\alpha})\big)$ eindeutig bestimmte $\chi(\widehat{\alpha})$ ist ein Charakter mod f. Je nachdem χ eigentlich oder uneigentlich, heißt auch $\lambda\big((\widehat{\alpha})\big)$ eigentlich oder uneigentlich.

Satz 26. Zu jedem Größencharakter $\lambda\big((\widehat{\alpha})\big) \mod f$ gibt es einen eindeutig bestimmten Modul f_1, sodaß $\lambda\big((\widehat{\alpha})\big)$ einen eindeutig bestimmten eigentlichen Größencharakter $\lambda_1\big((\widehat{\alpha})\big)$ nach f_1 erzeugt derart, daß

$$\lambda_1\big((\widehat{\alpha})\big) = \lambda\big((\widehat{\alpha})\big), \quad \text{wenn } \widehat{\alpha} \text{ prim zu } f.$$

f_1 ist ein Teiler von f.

Beweis: 1.) Sei $\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha})v(\widehat{\alpha})$, so gibt es einen eindeutig bestimmten Modul $f_1|f$, nach dem $\chi(\widehat{\alpha})$ einen eigentlichen Charakter $\chi_1(\widehat{\alpha})$ erzeugt. Ist dann η irgendeine total positive Einheit $\equiv 1 \mod f_1$, so ist

$$\begin{aligned} v(\eta) &= 1 \quad , \quad \text{da } \eta \text{ total positiv,} \\ \chi(\eta) &= 1 \quad , \quad \text{da } \eta \equiv 1 \mod f_1 \text{ und } \chi \text{ nach } f_1 \text{ einen} \\ &\qquad\qquad \text{eigentlichen Charakter erzeugt,} \end{aligned}$$

also

$$\lambda\big((\eta)\big) = 1 = \lambda(\eta).$$

$\lambda(x)$ hat also die Eigenschaft $\lambda(\eta) = 1$ für jedes solche η,

ist also nach Satz 6 schon ein Größencharakter mod f_1 im Sinne von §1. Bilden wir daher

$$\lambda_1\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi_1(\widehat{\alpha})v(\widehat{\alpha}),$$

so ist

$$\lambda_1\big((\varepsilon)\big) = \lambda(\varepsilon)\chi_1(\varepsilon)v(\varepsilon) = \lambda(\varepsilon)\chi(\varepsilon)v(\varepsilon) = \lambda\big((\varepsilon)\big)$$
(weil ε prim zu f)

für jede Körpereinheit ε und für $\alpha \equiv 1 \mod f_1$, total positiv:

$$\lambda_1\big((\alpha)\big) = \lambda(\alpha)\chi_1(\alpha)v(\alpha) = \lambda(\alpha).$$

$\lambda_1\big((\alpha)\big)$ erfüllt also die Definitionsgleichungen 1.), 2.), 3.) S. 49 für den $\lambda(\widehat{\alpha})$ zugeordneten Größencharakter mod f_1 für Ideale, und für zu f prime $\widehat{\alpha}$ ist ersichtlich

$$\lambda_1\big((\widehat{\alpha})\big) = \lambda\big((\widehat{\alpha})\big),$$

weil für diese $\widehat{\alpha}$:

$$\chi_1(\widehat{\alpha}) = \chi(\widehat{\alpha}).$$

2.) Sei umgekehrt $\lambda_1\big((\widehat{\alpha})\big)$ ein Größencharakter mit den Eigenschaften von Satz 26 und

$$\lambda_1\big((\widehat{\alpha})\big) = \lambda_1(\widehat{\alpha})\chi_1(\widehat{\alpha})v_1(\widehat{\alpha}).$$

Dann folgt zunächst für jedes $\alpha \equiv 1 \mod ff_1$, total positiv, da für diese χ, χ_1, v, v_1 gleich 1 sind,

$$\lambda_1(\alpha) = \lambda(\alpha),$$

und hieraus, wie a. S. 51/52 die Identität von λ_1 und λ. Ferner ist für jede Einheit ε

$$1 = \lambda_1\big((\varepsilon)\big) = \lambda(\varepsilon)\chi_1(\varepsilon)v_1(\varepsilon) = \lambda(\varepsilon)\chi(\varepsilon)v(\varepsilon) = \lambda\big((\varepsilon)\big),$$

also

$$\chi_1(\varepsilon)v_1(\varepsilon) = \chi(\varepsilon)v(\varepsilon),$$

und da man $\varepsilon \equiv 1 \mod ff_1$ mit beliebiger Signatur wählen kann,

die Identität von v_1 mit v. Es folgt somit

$$\chi_1(\widehat{\alpha}) = \chi(\widehat{\alpha}), \quad \text{wenn } \widehat{\alpha} \text{ prim zu } f,$$

und da nach Voraussetzung $\lambda_1\big((\widehat{\alpha})\big)$ eigentlich nach f_1 sein sollte, daß $\chi_1(\widehat{\alpha})$ der durch $\chi(\widehat{\alpha})$ erzeugte eigentliche Charakter mod f_1 sein muß. (f_1 muß also Teiler von f sein).

f_1 und der zugeordnete eigentliche Charakter $\lambda_1\big((\widehat{\alpha})\big)$ sind also eindeutig durch $\lambda\big((\widehat{\alpha})\big)$ bestimmt, w. z. b. w.

Mit den eigentlichen Charakteren $\chi(\widehat{\alpha})$ bilden wir jetzt gewisse Summen über vollständige Restsystemene einer Klasse idealer Zahlen, die eine Verallgemeinerung der bekannten Gaussschen Summen (Lagrangeschen Wurzelzahlen) darstellen.

Sei

$$f = (\widehat{\varphi})$$

ein beliebiger ganzer Idealmodul und

$$\mathfrak{d} = (\widehat{\delta})$$

die Körperdifferente von k. $\widehat{\varphi}$ und $\widehat{\delta}$ sind bis auf Einheiten aus k bestimmt und sollen fest gewählt werden. Wir beweisen zunächst den für das folgende sehr wichtigen Satz:

Satz 27. Ist α eine solche Körperzahl, daß $\alpha\widehat{\delta}$ ganz ist, so ist die Spur

$$S(\alpha) = \sum_{p=1}^{n} \alpha^{(p)}$$

eine ganze rationale Zahl.

Beweis: Es ist zu zeigen, daß alle durch das Ideal $\frac{1}{\mathfrak{d}}$ teilbaren Körperzahlen ganze Spuren haben. Ist nun

$$(\omega_q) = (\omega_1, \ldots, \omega_n)$$

eine Körperbasis, so entspringt bekanntlich (Satz von Hensel–Landsberg–Dedekind) aus der zu

$$(\omega_q^{(p)}); \quad (p, q = 1, \ldots n) \quad \left\{ \begin{array}{ll} p & \text{Zeilen} \\ q & \text{Spalten} \end{array} \right\}$$

reziproken Matrix

$$(\Omega_q^{(p)})\,; \quad (p,q=1,\dots n) \quad \left\{ \begin{array}{ll} q & \text{Zeilen} \\ p & \text{Spalten} \end{array} \right\}$$

die Basis

$$\Omega_q = (\Omega_1, \dots \Omega_n)$$

für das Ideal $\frac{1}{\mathfrak{d}}$. Demnach ist, wenn

$$\gamma = \sum_{q=1}^{n} c_q \omega_q$$

eine beliebige ganze Körperzahl bedeutet, (also die c_q ganze rationale Zahlen sind),

$$S(\gamma\Omega_r) = \sum_{p=1}^{n} \gamma^{(p)}\Omega_r^{(p)} = \sum_{q=1}^{n} c_q \sum_{p=1}^{n} \omega_q^{(p)}\Omega_r^{(p)} = \sum_{q=1}^{n} c_q \delta_{qr} = c_r$$

eine ganze rationale Zahl, und somit auch die Spur jeder durch $\frac{1}{\mathfrak{d}}$ teilbaren Zahl, die ja in der Form

$$\alpha = \sum_{q=1}^{n} a_q \Omega_q$$

mit ganzen a_q geschrieben werden kann ganz, weil

$$S(\alpha) = \sum_{q=1}^{n} S(a_q\Omega_q)$$

ist, und die einzelnen Summanden soeben als ganz erkannt wurden.

62 II

Wir betrachten nun den Ausdruck

$$e^{2\pi i S\left(\frac{\hat{\varrho}}{\hat{\varphi}\delta}\right)},$$

wo $\widehat{\varrho}$ eine ganze ideale Zahl aus derselben Klasse, wie $\widehat{\varphi}\widehat{\delta}$ ist, sodaß also $\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}$ eine Körperzahl ist, deren Spur gebildet werden kann. ist $\widehat{\varrho}_1 \equiv \widehat{\varrho} \mod f$, so $\frac{\widehat{\varrho}_1 - \widehat{\varrho}}{\widehat{\varphi}}$ ganz, also $\frac{\widehat{\varrho}_1 - \widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}$ eine Körperzahl wie α in Satz 27. Daher wird

$$e^{2\pi i S\left(\frac{\widehat{\varrho}_1}{\widehat{\varphi}\widehat{\delta}}\right)} = e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)},$$

unser Ausdruck also nur von der Restklasse abhängig, der $\widehat{\varrho}$ mod f angehört.

Sei nun $\widehat{\nu}$ eine beliebige ganze* ideale Zahl, $\widehat{\varrho}$ durchlaufe ein vollständiges System von $N(f) \mod f$ inkongruenten, ganzen idealen Zahlen aus einer solchen Klasse $\mathfrak{K}$, daß

$$\frac{\widehat{\nu}\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}} = \text{Körperzahl},$$

sodaß $\mathfrak{K}$ eindeutig durch $\widehat{\nu}$ bestimmt ist, wenn $\widehat{\varphi}$ und $\widehat{\delta}$ als fest gelten. Ferner sei $\chi(\widehat{\alpha})$ ein beliebiger Charakter mod f (§2)▸, dessen Definition wir hier zweckmäßig noch dadurch ergänzen, daß wir

$$\chi(\widehat{\alpha}) = 0, \quad \text{wenn } \widehat{\alpha} \text{ nicht prim zu } f \tag{2}$$

setzen. Dann bilden wir die Summe

$$G(\widehat{\nu}, \chi) = \sum_{\widehat{\varrho}} \chi(\widehat{\varrho}) e^{2\pi i S\left(\frac{\widehat{\nu}\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)}. \tag{3}$$

Wir beweisen:

Satz 28. $G(\widehat{\nu}, \chi)$ hängt bei festen $\widehat{\varphi}$, $\widehat{\delta}$ nur von $\widehat{\nu}$ und χ ab. Es ist

$$G(\widehat{\nu}_1, \chi) = G(\widehat{\nu}_2, \chi), \quad \text{wenn} \quad \widehat{\nu}_1 \equiv \widehat{\nu}_2 \mod f \tag{4}$$

und

$$G(\widehat{\alpha}\widehat{\nu}, \chi) = \overline{\chi}(\widehat{\alpha}) G(\widehat{\nu}, \chi), \quad \text{wenn } \widehat{\alpha} \text{ prim zu } f. \tag{5}$$

Beweis: $G(\widehat{\nu}, \chi)$ ist von den Repräsentanten $\widehat{\varrho}$ der Restklassen innerhalb der Klasse $\mathfrak{K}$ unabhängig. Denn für

$$\widehat{\varrho}_1 \equiv \widehat{\varrho} \mod f$$

ist auch

$$\widehat{\nu}\widehat{\varrho}_1 \equiv \widehat{\nu}\widehat{\varrho} \mod f,$$

*s. Anm. a. folgender Seite 64▸.

da $\widehat{\nu}$ ganz, also jedes Glied nur von der Restklasse von $\widehat{\varrho} \mod f$ abhängig, daher die ganze Summe nur von $\widehat{\nu}$ und χ. Ist ferner

$$\begin{aligned} \widehat{\nu}_1 &\equiv \widehat{\nu}_2 \mod f \quad \text{so ist auch} \\ \widehat{\nu}_1\widehat{\varrho} &\equiv \widehat{\nu}_2\widehat{\varrho} \mod f, \end{aligned}$$

da die $\widehat{\varrho}$ ganz, also jedes Glied der Summe auch nur von der Restklasse von $\widehat{\nu}$ mod f abhängig, womit (4) bewiesen ist. Ist schließlich $\widehat{\alpha}$ prim zu f so wird

$$\chi(\widehat{\alpha})G(\widehat{\alpha}\widehat{\nu},\chi) = \sum_{\widehat{\varrho}} \chi(\widehat{\alpha}\widehat{\varrho}) e^{2\pi i S\left(\frac{\widehat{\nu}\widehat{\alpha}\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)},$$

da natürlich auch für die durch (2) erweiterte Definition von χ gilt:

$$\chi(\widehat{\alpha})\chi(\widehat{\beta}) = \chi(\widehat{\alpha}\widehat{\beta}), \quad \text{wenn } \widehat{\alpha} \text{ prim zu } f$$

(und auch

$$\chi(\widehat{\alpha}) = \chi(\widehat{\beta}), \quad \text{wenn } \widehat{\alpha} \equiv \widehat{\beta} \mod f).$$

64 II

Nun durchläuft hier $\widehat{\varrho}$ ein vollständiges System von mod f inkongruenten ganzen Zahlen, sodaß

$$\frac{\widehat{\nu}\widehat{\alpha}\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}} = \text{Körperzahl}$$

Also durchläuft $\widehat{\sigma} = \widehat{\alpha}\widehat{\varrho}$ ein vollständiges System von mod f inkongruenten Zahlen, sodaß

$$\frac{\widehat{\nu}\widehat{\sigma}}{\widehat{\varphi}\widehat{\delta}} = \text{Körperzahl},$$

(und da es nur auf die Restklasse von $\widehat{\alpha} \mod f$ ankommt, dürfen die $\widehat{\sigma}$ auch als ganz angenommen werden †).
Daher wird

$$\chi(\widehat{\alpha})G(\widehat{\nu}\widehat{\alpha},\chi) = G(\widehat{\nu},\chi),$$

†die gemachte Voraussetzung, daß die $\widehat{\varrho}$ ganz sind, ist unwesentlich, sie müssen nur ein Repräsentantensystem für die Restklassen mod f, also für den Bereich von f ganz sein. Ebenso darf überall im Vorhergehenden „*ganz*“ durch „*ganz für den Bereich von f*“ ersetzt werden, die Exponenten von e unter dem Spurzeichen sind dann natürlich wegen des anzuwendenden Hensel–Landsbergschen Satzes immer ganze Repräsentanten der betr. Restklassen zu denken.

was wegen $\widehat{\alpha}$ prim zu f mit (5) identisch, w. z. b. w.

Weiter gilt:

Satz 29. Ist $\widehat{\nu}$ prim zu f, so ist

$$G(\widehat{\nu},\chi)=\overline{\chi}(\widehat{\nu})C(\chi,\widehat{\varphi}\widehat{\delta}),$$

wobei

$$C(\chi,\widehat{\varphi}\widehat{\delta})=\sum_{\widehat{\varrho}}\chi(\widehat{\varrho})e^{2\pi iS\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)},$$

summiert über ein Restsystem $\widehat{\varrho}$ sodaß $\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}=$ Körperzahl, nur von χ und $\widehat{\varphi}\widehat{\delta}$, nicht von $\widehat{\nu}$ abhängt.

Beweis: Nach Voraussetzung gibt es ein $\widehat{\alpha}$, sodaß

$$\widehat{\alpha}\widehat{\nu}\equiv 1 \mod f,$$

also

$$\chi(\widehat{\alpha})\chi(\widehat{\nu})=1$$

ist. Damit folgt aus (5)

$$\overline{\chi}(\widehat{\alpha})G(\widehat{\nu},\chi)=\chi(\widehat{\nu})G(\widehat{\nu},\chi)=G(1,\chi)$$

also

$$G(\widehat{\nu},\chi)=\overline{\chi}(\widehat{\nu})G(1,\chi)=\overline{\chi}(\widehat{\nu})\sum_{\widehat{\varrho}}\chi(\widehat{\varrho})e^{2\pi iS\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)}$$

und $G(1,\chi)=C(\chi,\widehat{\varphi}\widehat{\delta})$ hängt natürlich nur noch von χ und $\widehat{\varphi}\widehat{\delta}$ ab.

Schließlich gilt:

Satz 30. Ist $\widehat{\nu}$ nicht prim zu f und χ eigentlicher Charakter mod f, so ist

$$G(\widehat{\nu},\chi)=0.$$

Es gilt somit allgemein für eigentliches $\chi \mod f$ und ganzes $\widehat{\nu}$:

(6) $$G(\widehat{\nu},\chi)=\overline{\chi}(\widehat{\nu})C(\chi,\widehat{\varphi}\widehat{\delta}),$$

wo $C(\chi, \widehat{\varphi}\widehat{\delta})$ die Bedeutung von Satz 29 hat.

Beweis: Ist nämlich $(\widehat{\nu}, f) = f_1 \neq 1$ und α eine zu f prime Zahl, sodaß

$$\alpha \equiv 1 \mod \frac{f}{f_1},$$

so ist

$$\alpha\widehat{\nu} \equiv \widehat{\nu} \mod f$$

66 II

und nach (4)

$$G(\alpha\widehat{\nu}, \chi) = G(\widehat{\nu}, \chi),$$

nach (5)

$$G(\alpha\widehat{\nu}, \chi) = \overline{\chi}(\alpha) G(\widehat{\nu}, \chi),$$

folglich

$$G(\widehat{\nu}, \chi)\big(\overline{\chi}(\alpha) - 1\big) = 0.$$

Wäre nun für alle solche α: $\overline{\chi}(\alpha) = 1$, so wäre für alle $\widehat{\alpha}, \widehat{\beta}$ die zu f prim sind:

$$\overline{\chi}(\widehat{\alpha}) = \overline{\chi}(\widehat{\beta}), \quad \text{wenn} \quad \widehat{\alpha} \equiv \widehat{\beta} \mod \frac{f}{f_1},$$

also $\overline{\chi}$ kein eigentlicher Charakter[‡] mod f. Es gibt somit ein α der obigen Eigenschaften, sodaß $\overline{\chi}(\alpha) \neq 1$, und daher folgt $G(\widehat{\nu}, \chi) = 0$, w. z. b. w.

Aus dem Bewiesenen folgt noch:

Satz 31. Ist $\lambda\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha})v(\widehat{\alpha})$ ein Größencharakter für Ideale, so ist

$$\lambda(\widehat{\varphi}\widehat{\delta})v(\widehat{\varphi}\widehat{\delta})C(\chi, \widehat{\varphi}\widehat{\delta})$$

nur von $\lambda\big((\widehat{\alpha})\big)$ und dem Ideal $f = (\widehat{\varphi})$, dagegen nicht von der speziellen Wahl von $\widehat{\varphi}$ und $\widehat{\delta}$ abhängig.

[‡] $\overline{\chi}$ und χ sind natürlich stets gleichzeitig eigentlich oder uneigentlich.

Beweis: Statt $\widehat{\varphi\delta}$ tritt im allgemeinsten Falle $\varepsilon\widehat{\varphi\delta}$ mit einer beliebigen Körpereinheit ε. Da $\frac{\widehat{\varrho}}{\varepsilon}$ mit $\widehat{\varrho}$ ein entsprechendes Restsystem durchläuft wird (s. Satz 29)

$$C(\chi, \varepsilon\widehat{\varphi\delta}) = \chi(\varepsilon)C(\chi, \widehat{\varphi\delta})$$

(folgt natürlich auch aus (5) in Satz 28). Daher bekommt bei

67 II

Einführung von $\varepsilon\widehat{\varphi\delta}$ an Stelle von $\widehat{\varphi\delta}$ der Ausdruck von Satz 31 den Faktor

$$\lambda(\varepsilon)v(\varepsilon)\chi(\varepsilon) = \lambda\big((\varepsilon)\big),$$

der nach Definition von $\lambda\big((\widehat{\alpha})\big)$ sicher 1 ist.

Da $\lambda\big((\widehat{\alpha})\big)$ die Charaktere $\lambda(\widehat{\alpha}), v(\widehat{\alpha}), \chi(\widehat{\alpha})$ nach Satz 21 eindeutig bestimmt, hängt der Ausdruck des Satzes in der Tat nur von $\lambda\big((\widehat{\alpha})\big)$ und dem *Ideal* f ab, w. z. b. w.

68 II

2.5 §5 Eine Thetatransformationsformel.

69 II

Wir beweisen zuerst folgenden grundlegenden Satz, der die Quelle für eine der Funktionalgleichung der allgemeinsten L–Reihen im wesentlichen äquivalente Thetatransformationsformel ist.

Satz 32. Sei $B = (b_{ik})$ eine solche reelle symmetrische Matrix nicht verschwindenden Determinantenbetrages $|B|$, daß für reelle $(x) = (x_1, \ldots, x_n)$

$$B(x) = \sum_{i,k} b_{ik} x_i x_k$$

eine positiv definite quadratische Form ist. Dann gilt für alle reellen (x) die beliebig oft gliedweise nach allen x_i differenzierbare Relation

$$f(x) = \sum_{(m)} e^{-\pi B(x+m)} = \frac{1}{\sqrt{|B|}} \sum_{(m)} e^{-\pi B^{-1}(m) + 2\pi i (mx)},$$

wo beiderseits über alle ganzzahligen Systeme (Gitterpunkte des n–dimensionalen Raumes) $(m) = (m_1, \ldots, m_n)$ zu summieren ist, die Quadratwurzel positiv zu verstehen ist* und (mx) das innere Produkt $\sum_{i=1}^{n} m_i x_i$ bedeutet.

70 II

Beweis: Ich zeige zunächst, daß die Summe

$$f(x) = \sum_{(m)} e^{-\pi B(x+m)}$$

für alle reellen x konvergiert und beliebig oft gliedweise differenzierbar ist. Daraus folgt dann durch Fourier–Entwicklung von $f(x)$ die zu beweisende Relation und ihre beliebig häufige Differenzierbarkeit.

Um die einzelnen Glieder unserer Reihe abschätzen zu können, brauchen wir eine Abschätzung von $B(x)$ nach unten. Nun ist, da $B(x)$ positiv definit ist,

$$B(y) > 0$$

*Alle in diesem Abschnitt auftretenden Quadratwurzeln sind positiv zu verstehen.

für die Punkte der n–dimensionalen Einheitskugel

$$\sum_{i=1}^{n} y_i^2 = |y|^2 = (yy) = 1.$$

Da $B(y)$ stetig, hat also $B(y)$ auf dieser Kugel ein positives Minimum c. Ist dann $(x) = \frac{(x)}{|x|} \cdot |x|$ ein beliebiges Wertsystem, so zerlegt, daß der erste Faktor $\frac{(x)}{|x|}$ den Betrag 1 hat, so wird

$$B(x) = |x|^2 B\left(\frac{(x)}{|x|}\right) \geqq c|x|^2.$$

Wendet man dies auf $f(x)$ an, so wird

$$e^{-\pi B(x+m)} \leqq e^{-\pi c|x+m|^2}$$

Wegen der Periodizität von $f(x)$ in den x_i mit den Perioden 1 genügt es ersichtlich, die Behauptung für $0 \leqq x_i \leqq 1$ zu beweisen, d. h. für $|x| \leqq C$. Dann ist aber

$$\begin{aligned} |x+m|^2 &\geqq |m-1|^2 = \sum_{i=1}^{n}(m_i - C)^2 = \sum_{i=1}^{n} m_i^2 - 2C\sum_{i=1}^{n} m_i + nC^2 \\ &= |m|^2 - 2C(m \cdot 1) + nC^2 \end{aligned}$$

also

$$e^{-\pi B(x+m)} \leqq e^{-\pi c|m|^2 + 2\pi cC(m\cdot 1) - \pi cnC^2}$$

Nun ist bekanntlich für reelle $(u) = (u_1, \ldots, u_n)$; $(v) = (v_1, \ldots, v_n)$:

$$(uv)^2 \leqq |u|^2 \cdot |v|^2\,; \quad \text{(Schwarzsche Ungleichung)},$$

also speziell

$$\begin{aligned} (m \cdot 1)^2 &\leqq |m|^2 \cdot n \\ (m \cdot 1) &\leqq \sqrt{n}|m|. \end{aligned}$$

Beschränken wir uns (unter Auslassung von endlich vielen Anfangsgliedern) auf die Glieder mit

$$|m| > \frac{1}{\varepsilon}; \qquad (\varepsilon > 0),$$

so wird

$$|m| = \frac{|m|^2}{|m|} < \varepsilon |m|^2,$$

also (es ist $c > 0$, $C > 0$):

$$\begin{aligned} e^{-\pi B(x+m)} &< e^{-\pi c|m|^2 + 2\pi cC\sqrt{n}\varepsilon|m|^2 - \pi cnC^2} \\ &= e^{-\pi c|m|^2(1-2\varepsilon C\sqrt{n}) - \pi cnC^2}. \end{aligned}$$

Wird daher $\varepsilon < \frac{1}{2C\sqrt{n}}$ angenommen, und

$$a = 1 - 2\varepsilon C\sqrt{n} > 0$$

gesetzt, so sind „fast alle“ Glieder unserer Reihe $f(x)$ kleiner als die Glieder der Reihe

$$e^{-\pi cnC^2} \sum_{(m)} e^{-\pi ac|m|^2} = e^{-\pi cnC^2} \left(\sum_{k=-\infty}^{+\infty} e^{-\pi ack^2} \right)^n,$$

die wegen $\pi ac > 0$ und elementaren Regeln konvergiert. Da beide Reihen positive Glieder haben, ist also die Reihe $f(x)$ gleichmäßig konvergent für $|x| \leqq C$, und somit wegen der Periodizität von $f(x)$ für alle reellen (x).

Um die gleichmäßige Konvergenz der aus $f(x)$ durch gliedweise Differentiation nach den x_i entstehenden Reihen nachzuweisen, bemerken wir, daß diese erstens sämtlich von dem Typus sind

$$\sum_{(m)} F(x,m) e^{-\pi B(x+m)},$$

wo $F(x,m)$ ein Polynom in den x_i und m_i ist, zweitens sämtlich periodisch in den x_i mit den Perioden 1. Es genügt daher wieder die gleichmäßige Konvergenz für $|x| \leqq C$ zu beweisen, und dabei darf man sich auf die einzelnen

Bestandteile der Form

$$\sum_{(m)} h(x) m_1^{c_1} \cdots m_n^{c_n} e^{-\pi B(x+m)}$$

beschränken; wegen der erlaubten Annahme $|x| \leqq C$ genügt es also die gleichmäßige Konvergenz von

$$\sum_{(m)} m_1^{c_1} \cdots m_n^{c_n} e^{-\pi B(x+m)}$$

zu beweisen, wo $c_1, \ldots, c_n$ irgendein nicht negatives Exponentensystem ist. Wegen $|u| < e^{|u|}$ ist nun

$$|m_1^{c_1} \cdots m_n^{c_n}| < e^{c_1|m_1|+\cdots+c_n|m_n|} \leqq e^{C_1 \sum_{i=1}^{n} |m_i|}$$

und weiter

$$\sum_{i=1}^{n} |m_i| \leqq \sqrt{n}|m|$$

nach der Schwarzschen Ungleichung, also wie oben

$$|m_1^{c_1} \cdots m_n^{c_n}| < e^{\varepsilon C_1 \sqrt{n}|m|^2},$$

wo $C_1 = \operatorname{Max} c_i$ eine positive Konstante ist, daher

$$\left|m_1^{c_1} \cdots m_n^{c_n} e^{-\pi B(x+m)}\right| < e^{-\pi c|m|^2 + 2\pi\varepsilon c C\sqrt{n}|m|^2 + \varepsilon C_1\sqrt{n}|m|^2 - \pi C n^2}$$

woraus für hinreichend kleine ε ähnlich wie oben folgt, daß die Beträge unserer Reihenglieder (von endlich vielen abgesehen) kleiner sind als die Glieder einer konvergenten Reihe mit positiven Gliedern. Daher sind alle durch Differentiation aus $f(x)$ entstehenden Reihen für alle reellen (x) gleichmäßig konvergent und stellen mithin die entsprechenden Ableitungen der Funktion $f(x)$ dar, die demnach beliebig oft stetig differenzierbar ist.

2.) Wir wenden folgenden Satz über Fourier–Entwicklung an, der für $n = 1$ in den Elementen der Analysis bewiesen wird, für $n > 1$ daraus leicht durch Induktion folgt:

Ist $f(x)$ eine stetige, beliebig oft differenzierbare Funktion der reellen Variablen $(x) = (x_1, \ldots, x_n)$, die periodisch in den x_i mit der Periode 1 ist, so hat $f(x)$ eine gleichmäßig konvergente Fourier–Entwicklung

74 II

$$f(x) = \sum_{(m)} g(m) e^{2\pi i (mx)},$$

wo die Fourier–Entwicklungskoeffizienten $g(m)$ durch

$$g(m) = \int_0^1 \cdots \int f(x) e^{-2\pi i (mx)} dx$$

gegeben werden (dx steht zur Abkürzung für $dx_1 \ldots dx_n$. Die Fourier–Entwicklungen der Ableitungen von $f(x)$ sind ebenfalls gleichmäßig konvergent und entstehen aus der von $f(x)$ durch entsprechende gliedweise Differentiation.

In unserem Falle haben wir also nur noch nachzuweisen, daß die Fourier–Koeffizienten der nach 1.) für alle reellen (x) stetigen, beliebig oft differenzierbaren Funktion[1]

$$f(x) = \sum_{(m)} e^{-\pi B(x+m)}$$

die Werte

$$g(m) = \frac{1}{\sqrt{|B|}} e^{-\pi B^{-1}(m)}$$

haben. Dann folgen alle übrigen Behauptungen des Satzes aus den bei 1.) bewiesenen und dem eben genannten Theorem über Fourier–Entwicklungen.

Nun ist nach dem obigen hier

$$g(m) = \int_0^1 \cdots \int f(x) e^{-2\pi i (mx)} dx = \int_0^1 \cdots \int \sum_{(r)} e^{-\pi B(x+r) - 2\pi i (mx)} dx.$$

75 II

[1] unklar, ob $f(x)$ oder $\dot{f}(x)$

Wegen der gleichmäßigen Konvergenz der $\sum_{(r)}$ darf Summation und Integration vertauscht werden:

$$g(m) = \sum_{(r)} \int_0^1 \cdots \int e^{-\pi B(x+r)-2\pi i(mx)} dx,$$

und dies ist wegen der Periodizität von $e^{-2\pi i(mx)}$

$$\begin{aligned} g(m) &= \sum_{(r)} \int_{(r)}^{(r+1)} \cdots \int e^{-\pi B(x)-2\pi i(mx)} dx \\ &= \int_{-\infty}^{+\infty} \cdots \int e^{-\pi B(x)-2\pi i(mx)} dx. \end{aligned}$$

Ist nun $L = (\ell_{ik})$ eine wegen $|B| \neq 0$ sicher existierende Matrix nicht verschwindenden Determinantenbetrages $|L|$, sodaß

$$L'BL = E$$

die Einheitsmatrix ist, also

$$|L|^2|B| = 1\,; \qquad |L| = \frac{1}{\sqrt{|B|}}\,,$$

so transformieren wir (x) linear durch L:

$$(x) = L(y),$$

also

$$dx = |L|\,dy = \frac{1}{\sqrt{|B|}}\,dy,$$

weil der Betrag der Funktionaldeterminante gleich $|L|$ ist, und es wird so:

$$\begin{gathered} B(x) = E(y) = (y)^2, \\ (mx) = \big(m \cdot L(y)\big) = \big(y \cdot L'(m)\big), \end{gathered}$$

also

$$g(m) = \frac{1}{\sqrt{|B|}} \int_{-\infty}^{+\infty} \cdots \int e^{-\pi\{(y)^2 + 2i(y \cdot L'(m))\}} dy,$$

weil (y) wegen $|L| \neq 0$ mit (x) umkehrbar eindeutig den ganzen Raum durchläuft. Im Exponenten machen wir die quadratische Ergänzung:

$$(y)^2 + 2i\big(y \cdot L'(m)\big) = \big(y + iL'(m)\big)^2 + \big(L'(m) \cdot L'(m)\big).$$

Nun ist

$$\big(L'(m) \cdot L'(m)\big) = \left(\sum_{k=1}^{n} \ell_{ki} m_k \cdot \sum_{k=1}^{n} \ell_{ki} m_k\right)$$
$$= \sum_{i=1}^{n} \sum_{k=1}^{n} \ell_{ki} m_k \cdot \sum_{k'=1}^{n} \ell_{k'i} m_{k'} = \sum_{k,k'=1}^{n} m_k m_{k'} \sum_{i=1}^{n} \ell_{ki} \ell_{k'i}$$
$$= LL'(m) = B^{-1}(m),$$

weil wegen $L'BL = E$ die quadratische Form LL' mit der quadratischen Form B^{-1} identisch ist. Somit wird

$$g(m) = \frac{1}{\sqrt{|B|}} e^{-\pi B^{-1}(m)} \int_{-\infty}^{+\infty} \cdots \int e^{-\pi(y + iL'(m))^2} dy.$$

Das letztere Integral ist aber gleich 1. Denn es zerfällt in das Produkt von n einfachen Integralen der Form

$$\int_{-\infty}^{+\infty} e^{-\pi\left(y_k + iL'_k(m)\right)^2} dy_k.$$

In diesen darf der Integrationsweg nach dem Cauchyschen Satz in „$iL'_k(m) - \infty$ bis $iL'_k(m) + \infty$ (geradlinig)“ verändert werden, oder also

$$\int_{-\infty}^{+\infty} e^{-\pi y_k^2} dy_k$$

geschrieben werden. Letzteres Integral ist aber bekanntlich 1. Damit ist Satz 32 bewiesen.

77 II

Wir spezialisieren nun die Matrix B in der Formel von Satz 32 auf eine gewisse, nur durch den Körper k und ein Ideal $\mathfrak{a}$ in k bestimmte Form, die außerdem noch von n positiven Parametern $(t) = (t_1, \ldots, t_n)$ abhängt. Diese Parameter sollen der Bedingung

$$t_p = t_{p+r_2}\,; \qquad (p = r_1 + 1, \ldots, r_1 + r_2)$$

genügen. Außerdem verabreden wir zur Vereinfachung folgende Bezeichnungsweise:

$$N(t) = t_1 \ldots t_n,$$
$$S(\alpha t) = \sum_{p=1}^{n} \alpha^{(p)} t_p.$$

Das Ideal $\mathfrak{a}$ habe die Basis (α_q); $(q = 1, \ldots, n)$ Diese Basis bestimmt die Matrix:

$$A = \left(\alpha_q^{(p)}\right)\,; \qquad \begin{matrix}(p, q = 1, 2, \ldots, n).\\ (p \text{ Zeilen–}, q \text{ Spalten–Index})\end{matrix}$$

Wir setzen dann, wenn t die Diagonalmatrix der t_p bezeichnet, und $\overline{A}$ die zu A konjugiert komplexe Matrix ist:

$$B = A' t \overline{A}.$$

Diese Matrix B ist erstens *reell*. Denn ihr allgemeines Glied lautet:

$$b_{rq} = \sum_{p=1}^{n} \alpha_q^{(p)} t_p \overline{\alpha}_r^{(p)} = \sum_{p=1}^{r_1} \alpha_q^{(p)} t_p \alpha_r^{(p)} + \sum_{p=r_1+1}^{r_1+r_2} t_p \left(\alpha_q^{(p)} \alpha_r^{(p+r_2)} + \alpha_q^{(p+r_2)} \alpha_r^{(p)}\right)$$

78 II

und die ersten r_1 Glieder sind a fortiori reell, die r_2 folgenden ebenfalls, da $\alpha_q^{(p)} \alpha_r^{(p+r_2)}$ konjugiert–komplex zu $\alpha_q^{(p+r_2)} \alpha_r^{(p)}$ ist. Gleichzeitig folgt aus der eben angegebenen Darstellung von b_{qr}, daß

$$b_{qr} = b_{rq},$$

also B *symmetrisch* ist.

Wegen dieser beiden Eigenschaften ist noch

$$B' = \overline{B} = B = \overline{A'}tA,$$

was wir später verwenden werden.

Schließlich erzeugt B eine *positiv–definite* quadratische Form. Denn setzen wir

$$u^{(p)} = \sum_{q=1}^{n} \alpha_q^{(p)} x_q; \quad \text{allgemein} \quad q = \sum_{p=1}^{n} \alpha_q x_q,$$

so wird

$$B(x) = \sum_{r,q=1}^{n} b_{qr} x_q x_r = \sum_{p=1}^{n} t_p u^{(p)} \overline{u}^{(p)} = \sum_{p=1}^{n} t_p \left|u^{(p)}\right|^2 > 0$$

für alle (x).

Wir wollen jetzt die Formel von Satz 32 für diese Matrix B, die ja alle Voraussetzungen von Satz 32 erfüllt[†], spezialisieren.

Es wird zunächst die links auftretende quadratische Form $B(x+m)$ hier:

$$B(x+m) = \sum_{p=1}^{n} t_p \left|\mu^{(p)} + u^{(p)}\right|^2 = S\left\{t|\mu+u|^2\right\},$$

wenn entsprechend zu den schon eingeführten $u^{(p)}$ noch

79 II

$$\mu^{(p)} = \sum_{q=1}^{n} \alpha_q^{(p)} m_q; \quad \text{allgemein} \quad \mu = \sum_{q=1}^{n} \alpha_q m_q$$

gesetzt wird. Durchläuft hier (m) den ganzen Raum, so durchläuft wegen der Bedeutung der α_q offenbar μ alle durch das Ideal $\mathfrak{a}$ teilbaren Zahlen, jede einmal. Es wird also die linke Seite unserer Transformationsgleichung von Satz 32:

$$f(x) = \sum_{\mu \equiv 0 \ (\mathfrak{a})} e^{-\pi S\left\{t|\mu+u|^2\right\}}$$

[†]auch $|B| \neq 0$, s. S. 79▶.

Auf der rechten Seite wird weiter:

$$|B| = |\overline{A}||A|N(t),$$

wenn die Determinanten stets als Beträge gemeint sind. Nun ist

$$|\overline{A}||A| = |A|^2 = N(\mathfrak{a}^2)d = N(\mathfrak{a}^2\mathfrak{d})$$

wenn $\mathfrak{d}$ die Körperdifferente, also $d = N(\mathfrak{d})$ den Betrag der Körperdiskriminante bezeichnet, somit

$$|B| = N(\mathfrak{a}^2\mathfrak{d}t) \qquad (\neq 0 \text{ wie es erforderlich})$$

Ferner wird nach der zweiten Darstellung von B a. S. 78▶:

$$B^{-1} = A^{-1}t^{-1}\overline{A}'^{-1} = \left(A'^{-1}\right)' t^{-1} \left(\overline{A'^{-1}}\right).$$

B^{-1} entsteht also aus A'^{-1} ebenso wie B aus A. Nun hat bekanntlich (Hensel–Landsbergscher Satz) A'^{-1} in Bezug auf das Ideal $\frac{1}{\mathfrak{a}\mathfrak{d}}$ die gleiche Bedeutung wie A in Bezug auf $\mathfrak{a}$, d. h. die Zeilen von A'^{-1}

80 II

bilden Basen für die konjugierten Ideale zu $\frac{1}{\mathfrak{a}\mathfrak{d}}$. Daher wird

$$B^{-1}(m) = S\left\{\frac{1}{t}\cdot|\nu|^2\right\},$$

wo $\nu = A'^{-1}(m)$ alle durch $\frac{1}{\mathfrak{a}\mathfrak{d}}$ teilbaren Zahlen, jede einmal durchläuft, wenn (m) den ganzen Raum durchläuft. Schließlich ist noch (mx) zu bilden. Auch hier führen wir (u) statt (x) ein, vermöge der obigen Transformationsgleichungen, die kurz als

$$(u) = A(x)$$

geschrieben werden können, sodaß umgekehrt

$$(x) = A^{-1}(u)$$

wird. Daher wird

$$(mx) = \left(m\cdot A^{-1}(u)\right) = \left(A'^{-1}(m)\cdot u\right),$$

also wegen der Bedeutung von A'^{-1} als Basismatrix für $\frac{1}{\mathfrak{a}\mathfrak{d}}$ und nach Definition des inneren Produktes:

$$(mx) = S(\nu u),$$

wo ν dieselbe Bedeutung, wie oben hat. Damit wird nunmehr unsere Transformationsformel:

$$f(x) = \sum_{\mu \equiv 0\ (\mathfrak{a})} e^{-\pi S\{t|\mu+u|^2\}} = \frac{1}{\sqrt{N(\mathfrak{a}^2\mathfrak{d}t)}} \sum_{\nu \equiv 0\left(\frac{1}{\mathfrak{a}\mathfrak{d}}\right)} e^{-\pi S\left\{\frac{|\nu|^2}{t}\right\}+2\pi i S(\nu u)}$$

wobei $(u) = A(x)$ gesetzt ist.

81 II

Wir haben schon beim Aufbau der Formel durchweg die (x) durch (u) ersetzt, wie es der späteren Anwendung entspricht. Die Transformation

$$(u) = A(x)$$

ist wegen $|A| \neq 0$ umkehrbar eindeutig und bildet, wie man sofort bestätigt, den Raum aller reellen (x) eineindeutig auf den Raum aller Vektoren (u) mit r_1 reellen und r_2 Paaren konjugiert komplexer Komponenten, (entsprechend den konjugierten Körpern), ab. Daher bleiben alle Aussagen von Satz 32, insbesondere die über die beliebig häufige Differenzierbarkeit, richtig, wenn man an Stelle der (x) die in dem genannt Raum variablen (u) als *unabhängige* Variable einführt. Wir erhalten somit folgendes Resultat, bei dessen Aussprache wir, ähnlich (jedoch *ohne* die Forderung der „Total–Positivität“) wie in §1 ▸ (u) einen k zugeordneten *variablen Körpervektor*, und dementsprechend (t) einen *total–reellen* positiven Körpervektor nennen:

82 II

Satz 33. Ist $\mathfrak{a}$ ein beliebiges Ideal aus k, (u) ein variabler und (t) ein total reeller positiver Körpervektor, und $\mathfrak{d}$ die Differente von k, so gilt die beliebig oft nach den Komponenten von (u) differenzierbare Transformationsformel:

$$\Theta\big((u),(t),\mathfrak{a}\big) = \sum_{\mu \equiv 0\ (\mathfrak{a})} e^{-\pi S\left[t|\mu+u|^2\right]}$$

$$= \frac{1}{\sqrt{N(\mathfrak{a}^2\mathfrak{d}t)}} \sum_{\nu \equiv 0\left(\frac{1}{\mathfrak{a}\mathfrak{d}}\right)} e^{-\pi S\left(\frac{|\nu|^2}{t}\right)+2\pi i S(\nu u)}.$$

Wir machen nunmehr Anwendung von der Differenzierbarkeit dieser Formel. Dazu müssen natürlich die in den Exponenten zur Abkürzung geschriebenen Spur– und Betragzeichen durch ihre wahre Bedeutung ersetzt werden, die Spur also durch $\sum_{p=1}^{n}$ über alle konjugierten und die Betragzeichen, entsprechend ihrer Entstehung, durch das Produkt der konjugiert komplexen. In dieser Schreibweise wird:

$$S\left[t|\mu+u|^2\right] = \sum_{p=1}^{r_1} t_p \left(\mu^{(p)}+u^{(p)}\right)^2 +$$

$$+2\sum_{p=r_1+1}^{r_1+r_2} t_p \left(\mu^{(p)}+u^{(p)}\right)\left(\mu^{(p+r_1)}+u^{(p+r_1)}\right),$$

$$S(\nu u) = \sum_{p=1}^{n} \nu^{(p)} u^{(p)}.$$

Wir führen ferner durch eine „Parallelverschiebung“ statt (u) den neuen variablen Körpervektor

$$(v) = (u - \varrho)$$

ein, wo ϱ eine beliebige, später zu fixierende Körperzahl bedeutet. (v) durchläuft mit (u) denselben Bereich aller Körpervektoren in obigem Sinne, sodaß natürlich auch nach den neuen Variablen $v^{(p)}$ beliebig oft differenziert werden darf.

Den zu bildenden Differentialquotienten bestimmen wir unter Zugrundelegung eines beliebigen Größencharakters $\lambda\big((\widehat{\alpha})\big)$ nach dem Modul f so:

$\lambda\big((\widehat{\alpha})\big)$ bestimmt eindeutig (S. 53▸) ein System von n positiven oder verschwindenden Exponenten:

$$a_1, a_2, \ldots, a_n,$$

und ebenso der reziproke (konjugiert–komplexe) Charakter $\overline{\lambda}\big((\widehat{\alpha})\big)$ das System

$$a'_1, a'_2, \ldots, a'_n,$$

das mit dem von $\lambda\big((\widehat{\alpha})\big)$ auf Grund von Satz 23 zusammenhängt.

Wir setzen dann:

1.) $v^{(p)} = 0$, für $a'_p = 0$,

2.) differenzieren die so entstehende Formel a'_p mal nach $v^{(p)}$, für $a'_p > 0$ und setzen dann $v^{(p)} = 0$

(Natürlich lassen sich die Operationen 1.) unter 2.) subsummieren, sind jedoch getrennt aufgeführt, weil die angegebene Reihenfolge wesentlich ist).

84 II

Der Exponent links schreibt sich in den $v^{(p)}$ so:

$$S\big[t|\mu+\varrho+v|^2\big] = \sum_{p=1}^{r_1} t_p \left(\mu^{(p)} + \varrho^{(p)} + v^{(p)}\right)^2 + 2\sum_{p=r_1+1}^{r_1+r_2} t_p \left(\mu^{(p)} + \varrho^{(p)} + v^{(p)}\right)\left(\mu^{(p+r_2)} + \varrho^{(p+r_2)} + v^{(p+r_2)}\right)$$

oder nach leichter Umformung, sodaß die $v^{(p)}$ heraustreten:

$$= \sum_{p=1}^{n} t_p \left|\mu^{(p)} + \varrho^{(p)}\right|^2 + 2\sum_{p=1}^{n} t_p v^{(p)} \left(\overline{\mu}^{(p)} + \overline{\varrho}^{(p)}\right) + \sum_{p=1}^{r_1} t_p {v^{(p)}}^2 + 2\sum_{p=r_1+1}^{r_1+r_2} t_p v^{(p)} v^{(p+r_2)}$$

Wegen 1.), und weil nach (2) S. 53 stets $a'_p a'_{p+r_2} = 0$ ist ($p = r_1{+}1, \dots r_1{+}r_2$) fällt hier der letzte Term weg. Bei den Differentiationen 2.) ist zu berücksichtigen, daß nach (1) S. 53 die $a'_p = 0$ oder 1 sind für $p = 1, 2, \dots r_1$. Daher bekommt das allgemeine Glied der Summe auf der linken Seite unserer Transformationsgleichung bei a'_p–maliger Differentiation nach einem der ersten r_1 $v^{(p)}$ den Faktor $\left(-2\pi t_p(\overline{\mu}^{(p)} + \overline{\varrho}^{(p)}) - 2\pi t_p v^{(p)}\right)^{a'_p}$, während bei a'_p–maliger Differentiation nach den noch nicht gleich Null gesetzen[2], übrigen r_2 Größen $v^{(p)}$ der Faktor $\left(-2\pi t_p(\overline{\mu}^{(p)} + \overline{\varrho}^{(p)})\right)^{a'_p}$ vortritt. Insgesamt geht also auf diese Weise die linke Seite über in

$$\sum_{\mu\equiv 0\,(\mathfrak{a})} \prod_{p=1}^{n} \left[-2\pi t_p(\overline{\mu}^{(p)} + \overline{\varrho}^{(p)})\right]^{a'_p} e^{-\pi S\{t|\mu+\varrho|^2\}} = \prod_{p=1}^{n}(-2\pi t_p)^{a'_p} \sum_{\mu\equiv 0\,(\mathfrak{a})} \prod_{p=1}^{n} \left(\overline{\mu}^{(p)} + \overline{\varrho}^{(p)}\right)^{a'_p} e^{-\pi S\{t|\mu+\varrho|^2\}},$$

[2] nicht eindeutig zu entziffern

85 II

da ja nachher alle $v^{(p)} = 0$ zu setzen sind und die *formal* hinzugesetzten r_2 vortretenden Faktoren, die den $a'_p = 0$ entsprechen in *Wirklichkeit* 1 *sind*. Nach Satz 23 kann dies auch so geschrieben werden:

$$\prod_{p=1}^{n}(-2\pi t_p)^{a_p} \sum_{\mu\equiv 0\ (\mathfrak{a})} \prod_{p=1}^{n} \left(\mu^{(p)} + \varrho^{(p)}\right)^{a_p} e^{-\pi S\left\{t|\mu+\varrho|^2\right\}}.$$

Auf der rechten Seite unserer Transformationsgleichung tritt vor das allgemeine Glied der Summe der Faktor:

$$\prod_{p=1}^{n} \left(2\pi i \nu^{(p)}\right)^{a'_p}.$$

Somit geht unsere Transformationsformel über in:

$$\prod_{p=1}^{n}(-2\pi t_p)^{a_p} \sum_{\mu\equiv 0\ (\mathfrak{a})} \prod_{p=1}^{n} \left(\mu^{(p)} + \varrho^{(p)}\right)^{a_p} e^{-\pi S\left\{t|\mu+\varrho|^2\right\}}$$

$$= \frac{\prod_{p=1}^{n}(2\pi i)^{a'_p}}{\sqrt{N(\mathfrak{a}^2\mathfrak{d}t)}} \sum_{\nu\equiv 0\ \left(\frac{1}{\mathfrak{a}\mathfrak{d}}\right)} \prod_{p=1}^{n} \left(\nu^{(p)}\right)^{a'_p} e^{-\pi S\left(\frac{|\nu|^2}{t}\right)+2\pi i S(\nu\varrho)}$$

Die Summationsbedingung $\mu \equiv 0\ (\mathfrak{a})$ links transformieren wir jetzt durch geeignete Wahl von ϱ in eine neue derart, daß über alle ganzen idealen Zahlen einer bestimmten Restklasse nach dem ganzen Modul $f = (\widehat{\varphi})$ summiert wird. Die absolute Klasse $\mathfrak{K}$ $\left(\text{von } \mathfrak{Z}(1)\right)$, innerhalb deren diese Restklasse liegen soll, soll die Klasse von $\frac{\widehat{\varphi}}{\widehat{\alpha}}$ sein, wenn

86 II

$\mathfrak{a} = (\widehat{\alpha})$ gesetzt ist. Durch geeignete Wahl von $\mathfrak{a}$ kann man so jede Klasse $\mathfrak{K}$ von $\mathfrak{Z}(1)$ erhalten. Innerhalb dieser sei eine Restklasse $\widehat{\varrho} \bmod f$ durch einen ganzen Repräsentanten $\widehat{\varrho}$ ausgewählt.

Setzen wir dann

$$\widehat{\mu} = \widehat{\gamma}\widehat{\varphi} + \widehat{\varrho},$$

und lassen $\widehat{\gamma}$ alle ganzen Zahlen aus der Klasse von $\frac{\widehat{\varrho}}{\widehat{\varphi}}$, d. h. von $\frac{1}{\widehat{\alpha}}$ durchlaufen, so durchläuft $\widehat{\mu}$ alle ganzen Zahlen $\equiv \widehat{\varrho} \mod f$, jede einmal. Setzen wir also

weiter

$$\widehat{\gamma} = \frac{\mu}{\widehat{\alpha}},$$

und lassen μ alle durch $\mathfrak{a}$ teilbaren Körperzahlen durchlaufen — (gerade damit diese μ wirklich der Hauptklasse von $\mathfrak{Z}(1)$ angehören müssen, mußte oben die Klasse $\mathfrak{K}$ in der Form $\frac{\widehat{\varphi}}{\widehat{\alpha}}$ angenommen werden) — so durchläuft $\widehat{\gamma}$ gerade alle ganzen Zahlen aus der Klasse $\frac{1}{\widehat{\alpha}}$, also

$$\widehat{\mu} = \frac{\widehat{\varphi}\mu}{\widehat{\alpha}} + \widehat{\varrho}$$

alle ganzen Zahlen $\equiv \widehat{\varrho} \mod f$.

Dementsprechend haben wir in unserer Formel zu setzen

$$\mu = \frac{\widehat{\alpha}(\widehat{\mu} - \widehat{\varrho})}{\widehat{\varphi}},$$

und um keine Differenz im Exponenten zu haben,

$$\varrho = \frac{\widehat{\alpha}\widehat{\varrho}}{\widehat{\varphi}},$$

also

$$\mu + \varrho = \frac{\widehat{\alpha}\widehat{\mu}}{\widehat{\varphi}}.$$

Rechts führen wir an Stelle von $\nu \equiv 0 \left(\frac{1}{\mathfrak{a}\mathfrak{d}}\right)$ den neuen Summationsbuchstaben $\widehat{\nu}$ durch

$$\nu = \frac{\widehat{\nu}}{\widehat{\alpha}\widehat{\delta}}$$

ein, wo $(\widehat{\delta}) = \mathfrak{d}$ gesetzt ist, sodaß $\widehat{\nu}$ alle ganzen Zahlen der Klasse $\widehat{\alpha}\widehat{\delta}$ durchlaufen muß.

Damit geht unsere Transformationsformel über in

$$\prod_{p=1}^{n}(-2\pi t_p)^{a_p} \sum_{\widehat{\mu} \equiv \widehat{\varrho}\ (f)} \prod_{p=1}^{n} \left(\frac{\widehat{\alpha}^{(p)}\widehat{\mu}^{(p)}}{\widehat{\varphi}^{(p)}} \right)^{a_p} e^{-\pi S\left\{t \left| \frac{\widehat{\alpha}\widehat{\mu}}{\widehat{\varphi}} \right|^2\right\}}$$

$$= \frac{\prod_{p=1}^{n}(2\pi i)^{a'_p}}{\sqrt{N(\mathfrak{a}^2\mathfrak{d}t)}} \sum_{\widehat{\nu} \text{ aus } \widehat{\alpha}\widehat{\delta}} \prod_{p=1}^{n} \left(\frac{\widehat{\nu}^{(p)}}{\widehat{\alpha}^{(p)}\widehat{\delta}^{(p)}} \right)^{a'_p} e^{-\pi S\left\{\frac{1}{t} \left| \frac{\widehat{\nu}}{\widehat{\alpha}\widehat{\delta}} \right|^2\right\} + 2\pi i S\left(\frac{\widehat{\nu}\widehat{\varrho}}{\widehat{\delta}\widehat{\varphi}}\right)}$$

Um diese Formel noch zu vereinfachen, bemerken wir erstens, daß sicher wegen $\sum_{p=1}^{n} a_p = \sum_{p=1}^{n} a'_p$ der Faktor 2π beiderseits hebt. Ferner führen wir für (t) den ebenfalls total reellen positiven Vektor (t') durch

$$(t) = \left(\frac{t'}{|\widehat{\alpha}|^2} \left| \frac{\widehat{\varphi}}{\widehat{\delta}} \right| \right)$$

ein, der nach Bestimmung der konjugiert komplexen konjugierten der idealen Zahlen dieselbe Struktur hat, wie sie (t) notwendig haben muß.

Wegen

$$N(t) = N(t') \frac{N(f)}{N(\mathfrak{a}^2 \mathfrak{d})}$$

geht hierdurch die [...] [...][3] rechts in $\sqrt{N(f)}\sqrt{N(t')}$ [...][4] Vereinigen wir die t'_p alle auf der rechten [...][5], so tritt also dort das Produkt

$$\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}$$

auf. Nunmehr richten wir unser Augenmerk auf die Exponenten von e. Links wird:

$$S\left\{ t \left| \frac{\widehat{\alpha}\widehat{\mu}}{\widehat{\varphi}} \right|^2 \right\} = S\left\{ t' \frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|} \right\},$$

rechts

$$S\left\{ \frac{1}{t} \left| \frac{\widehat{\nu}}{\widehat{\alpha}\widehat{\delta}} \right|^2 \right\} = S\left\{ \frac{1}{t'} \frac{|\widehat{\nu}|^2}{|\widehat{\varphi}\widehat{\delta}|} \right\}.$$

Den Faktor $(-1)^{\sum_{p=1}^{n} a_p}$ links können wir wegen $\sum_{p=1}^{n} a_p = \sum_{p=1}^{n} a'_p$ rechts mit dem noch übrigen $i^{\sum_{p=1}^{n} a'_p}$ zu

$$(-i)^{\sum_{p=1}^{n} a_p}$$

[3] „Quadratwurzel“ ?
[4] „über“ ?
[5] „Seite“ ?

vereinigen.

Alles noch übrige, was von der Summation unabhängig ist, bringen wir nach links vor das Summenzeichen, sodaß dort folgender Ausdruck entsteht:

$$\prod_{p=1}^{n}\left(\frac{|\widehat{\varphi}^{(p)}|}{|\widehat{\alpha}^{(p)}|^2|\widehat{\delta}^{(p)}|}\right)^{a_p}\cdot\prod_{p=1}^{n}\left(\frac{\widehat{\alpha}^{(p)}}{\widehat{\varphi}^{(p)}}\right)^{a_p}\cdot\prod_{p=1}^{n}\left(\widehat{\alpha}^{(p)}\widehat{\delta}^{(p)}\right)^{a'_p}.$$

Ist nun

$$\lambda\big((\widehat{\alpha})\big)=\lambda(\widehat{\alpha})v(\widehat{\alpha})\chi(\widehat{\alpha})$$

die Zerlegung des zugrundegelegten Größencharakters, dem die a_p entnommen waren nach Satz 21 und entsprechend (6) S. 44:

$$v(\widehat{\alpha})=\prod_{p=1}^{r_1}\left(\frac{\widehat{\alpha}^{(p)}}{|\widehat{\alpha}^{(p)}|}\right)^{a_p}$$

die Darstellung von $v(\widehat{\alpha})$, so läßt sich aus diesem Ausdruck der Faktor $v^2(\widehat{\alpha}\widehat{\delta})$ abspalten. Der übrig bleibende Rest berechnet sich dann auf Grund der Beziehung:

$$\prod_{p=r_1+1}^{n}\frac{(\widehat{\alpha}^{(p)})^{a_p+a'_p}}{|\widehat{\alpha}^{(p)}|^{2a_p}}=\prod_{p=r_1+1}^{n}\frac{(\widehat{\alpha}^{(p)})^{a_p+a'_p}}{(\widehat{\alpha}^{(p)}\widehat{\overline{\alpha}}^{(p)})^{a_p}}$$

$$=\prod_{p=r_1+1}^{n}\frac{(\widehat{\alpha}^{(p)})^{a'_p}}{(\widehat{\overline{\alpha}}^{(p)})^{a_p}}=1,\quad\text{(weil die Exponenten } a_p, a'_p$$

nur in der Reihenfolge verschieden, und wegen der zwischen ihnen bestehenden Relation Glieder mit demselben Exponenten auch dieselbe Basis haben), die für $\widehat{\alpha}$ und $\widehat{\delta}$ anzuwenden ist, nach elementaren Methoden zu

$$\prod_{p=1}^{n}\left(\frac{\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}\right)^{-a_p}$$

Durch alle genannten Umrechnungen wird also unsere Transformationsformel von S. 87▸ Mitte endlich, wenn wieder t statt t' geschrieben wird

$$v^2(\widehat{\alpha}\widehat{\delta})\prod_{p=1}^{n}\left(\frac{\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}\right)^{-a_p}\sum_{\widehat{\mu}\equiv\widehat{\varrho}\ (f)}\prod_{p=1}^{n}(\widehat{\mu}^{(p)})^{a_p}\cdot e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}}$$

$$=\frac{(-i)^{\sum_{p=1}^{n}a_p}}{\sqrt{N(f)}}\prod_{p=1}^{n}t_p^{-\frac{1}{2}-a_p}\sum_{\widehat{\nu}\text{ aus }\widehat{\alpha}\widehat{\delta}}\prod_{p=1}^{n}(\widehat{\nu}^{(p)})^{a'_p}\cdot e^{-\pi S\left\{\frac{1}{t}\frac{|\widehat{\nu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}+2\pi i S\left\{\frac{\widehat{\nu}\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right\}}.$$

Diese Relation liefert nunmehr die genannte Thetaformel. Wir definieren nämlich zu der Klasse $\mathfrak{K}$, dem *eigentlichen* Größencharakter $\lambda\big((\widehat{\mu})\big)$, und den (ebenfalls in gewissem Sinne variablen) $\widehat{\varphi},\widehat{\delta}$ eine *Thetafunktion* durch

$$\vartheta(t;\mathfrak{K},\lambda,\widehat{\varphi}\widehat{\delta}\,)=\sum_{\widehat{\mu}|\mathfrak{K}}\chi(\widehat{\mu})\prod_{p=1}^{n}\left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p}\cdot e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}},$$

($\widehat{\mu}$ durchläuft alle *ganzen* Zahlen aus $\mathfrak{K}$),

wo $\lambda\big((\widehat{\mu})\big)$ die Zerlegung:

$$\lambda\big((\widehat{\mu})\big)=\lambda(\widehat{\mu})v(\widehat{\mu})\chi(\widehat{\mu})$$

und das Exponentensystem $a_1,\ldots,a_n$ hat.

Ersichtlich hängt diese Funktion nur von den angegebenen Exponenten ab. Sie läßt sich aus der linken Seite obiger Transformationsgleichung bilden, indem diese mit $\chi(\widehat{\varrho})$ multipliziert und über ein volles Restsystem $\widehat{\varrho}$ mod f in $\mathfrak{K}$ summiert wird. Dabei ist also oben $\mathfrak{a}=(\widehat{\alpha})$ so zu wählen, daß $\frac{\widehat{\varrho}}{\widehat{\alpha}}$ gerade der

gewünschten Klasse angehört, was stets möglich. Durch diesen Prozeß geht dann die *linke Seite* über in:

$$v^2(\widehat{\alpha}\widehat{\delta})\prod_{p=1}^{n}\left(\frac{\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}\right)^{-a_p}\prod_{p=1}^{n}|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|^{\frac{a_p}{2}}\vartheta(t;\mathfrak{K},\lambda,\widehat{\varphi}\widehat{\delta}),$$

da ja $\chi(\widehat{\mu}) = \chi(\widehat{\varrho})$ ist für $\widehat{\mu} \equiv \widehat{\varrho} \mod f$. Auf der rechten Seite entsteht

$$\frac{(-i)^{\sum_{p=1}^{n} a_p}}{\sqrt{N(f)}} \prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p} \sum_{\widehat{\nu}|\mathfrak{K}'} \prod_{p=1}^{n} (\widehat{\nu}^{(p)})^{a'_p} e^{-\pi S\left(\frac{1}{t}\left|\frac{|\widehat{\nu}|^2}{\widehat{\varphi}\widehat{\delta}}\right|\right)} G(\widehat{\nu}, \chi),$$

wo $\mathfrak{K}'$ die Klasse von $\widehat{\alpha}\widehat{\delta}$, also

$$\mathfrak{K}\mathfrak{K}' \quad \text{die Klasse von} \quad \widehat{\varphi}\widehat{\delta}$$

bezeichnet, und $G(\widehat{\nu}, \chi)$ die Bedeutung von (3) S. 63 hat. Da nach Voraussetzung $\lambda\big((\widehat{\mu})\big)$ eigentlich, also auch $\chi(\widehat{\mu})$ eigentlich ist, folgt nach Satz 30 für die *rechte Seite*

$$\frac{(-i)^{\sum_{p=1}^{n} a_p}}{\sqrt{N(f)}} C(\chi, \widehat{\varphi}\widehat{\delta}) \prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p} \prod_{p=1}^{n} |\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|^{\frac{a'_p}{2}} \cdot \sum_{\widehat{\nu}|\mathfrak{K}'} \overline{\chi}(\widehat{\nu}) \prod_{p=1}^{n} \left(\frac{\widehat{\nu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}} \right)^{a'_p} e^{-\pi S\left(\frac{1}{t}\frac{|\widehat{\nu}|^2}{\widehat{\varphi}\widehat{\delta}}\right)}.$$

Bedenken wir nun, daß für jede Körperzahl $v^2(\nu) = 1$, also für alle $\widehat{\nu}$ aus $\mathfrak{K}'$

$$v^2(\widehat{\nu}) = v^2(\widehat{\alpha}\widehat{\delta})$$

ist, so können wir den Faktor $v^2(\widehat{\alpha}\widehat{\delta})$ von links in den Nenner unter $\overline{\chi}(\widehat{\nu})$ rechts als $v^2(\widehat{\nu})$ schreiben, und

nach Satz 23 steht dann rechts

$$\frac{(-i)^{\sum_{p=1}^{n} a_p}}{\sqrt{N(f)}} C(\chi, \widehat{\varphi}\widehat{\delta}) \prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p} \prod_{p=1}^{n} |\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|^{\frac{a'_p}{2}} \vartheta\left(\frac{1}{t}; \mathfrak{K}', \overline{\lambda}, \widehat{\varphi}\widehat{\delta}\right).$$

Damit haben wir die Relation:

$$\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}) = \mathsf{H}(\lambda, \widehat{\varphi}\widehat{\delta}) \vartheta\left(\frac{1}{t}; \mathfrak{K}', \overline{\lambda}, \widehat{\varphi}\widehat{\delta}\right) \prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}$$

also eine Transformationsformel, bei der das eigentliche Argument t ins reziproke $\frac{1}{t}$ übergeht, die Klassen in der Beziehung

$$\mathfrak{K}\mathfrak{K}' = \text{Klasse von } \widehat{\varphi}\widehat{\delta}$$

stehen und die Charaktere konjugiert komplex (reziprok) sind.

Der Faktor $\mathsf{H}(\lambda, \widehat{\varphi}\widehat{\delta})$ hat nach dem obigen die Gestalt:

$$\frac{(-i)^{\sum_{p=1}^{n} a_p}}{\sqrt{N(f)}} C(\chi, \widehat{\varphi}\widehat{\delta}) \prod_{p=1}^{n} \left(\frac{\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|} \right)^{a_p} \frac{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|^{\frac{a'_p}{2}}}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|^{\frac{a_p}{2}}}.$$

Der letzte Faktor im Produkt kann ersichtlich weggelassen werden, da für „reelle“ p: $a'_p = a_p$ ist, für je zwei „konjugiert komplexe“ p_1, p_2: $a'_{p_1} = a_{p_2}$ und hier die Beträge in Zähler und Nenner übereinstimmen. Der erste Faktor

$$\prod_{p=1}^{n} \left(\frac{\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|} \right)^{a_p}$$

läßt sich noch durch die Elemente von $\lambda\big((\widehat{\varphi}\widehat{\delta})\big)$ ausdrücken;

denn nach Satz 8 (S. 23) und (6) (S. 44) wird allgemein

$$\frac{\lambda(\widehat{\mu})}{\lambda(|\widehat{\mu}|)} v(\widehat{\mu}) = \prod_{p=1}^{n} \left(\frac{\widehat{\mu}^{(p)}}{|\widehat{\mu}^{(p)}|} \right)^{a_p},$$

somit

$$\mathsf{H}(\lambda, \widehat{\varphi}\widehat{\delta}) = (-i)^{\sum_{p=1}^{n} a_p} \frac{C(\chi, \widehat{\varphi}\widehat{\delta}) \lambda(\widehat{\varphi}\widehat{\delta}) v(\widehat{\varphi}\widehat{\delta})}{\lambda(|\widehat{\varphi}\widehat{\delta}|)\sqrt{N(f)}}.$$

Dieser Ausdruck zerlegt sich noch in

$$\mathsf{H}(\lambda, \widehat{\varphi}\widehat{\delta}) = \frac{\mathsf{W}(\lambda)}{\lambda(|\widehat{\varphi}\widehat{\delta}|)},$$

wobei[6]

$$\mathsf{W}(\lambda) = (-i)^{\sum_{p=1}^{n} a_p} \frac{\lambda(\widehat{\varphi}\widehat{\delta}) v(\widehat{\varphi}\widehat{\delta}) C(\chi, \widehat{\varphi}\widehat{\delta})}{\sqrt{N(f)}}$$

[6] Hasse schreibt „$\cdots v(\widehat{\varphi}\delta) \cdots$“

nach Satz 31 nur von $\lambda\big((\widehat{\mu})\big)$ und dem Ideal f, aber nicht von der speziellen Wahl von $\widehat{\varphi}\widehat{\delta}$ abhängt.

Zusammenfassend haben wir:

Satz 34. Sei $f = (\widehat{\varphi})$ ein ganzer Idealmodul, $\mathfrak{d} = (\widehat{\delta})$ die Körperdifferente, ferner

$$\lambda\big((\widehat{\mu})\big) = \lambda(\widehat{\mu})v(\widehat{\mu})\chi(\widehat{\mu})$$

ein eigentlicher Größencharakter mod f und $a_1, \ldots, a_n$ sein Exponentensystem, (t) ein totalreeller, positiver Körpervektor[‡] (variabel), $\mathfrak{K}$ eine beliebige Klasse von $\mathfrak{Z}(1)$ (absolute Idealklasse). Es werde die zu $\mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}$ gehörige Thetafunktion

94 II

durch

$$\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}) = \sum_{\widehat{\mu}|\mathfrak{K}} \chi(\widehat{\mu}) \prod_{p=1}^{n} \left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}} \right)^{a_p} \cdot e^{-\pi S\left\{ t \frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|} \right\}}$$

definiert. Dann konvergiert diese Reihe für alle genannten (t) und genügt der Funktionalgleichung:

$$\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}) = \frac{\mathsf{W}(\lambda)}{\lambda(|\widehat{\varphi}\widehat{\delta}|)} \cdot \prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p} \cdot \vartheta\left(\frac{1}{t}; \mathfrak{K}', \overline{\lambda}, \widehat{\varphi}\widehat{\delta} \right).$$

Hierbei ist $\mathfrak{K}'$ diejenige eindeutig bestimmte Klasse von $\mathfrak{Z}(1)$, für die $\mathfrak{K}\mathfrak{K}'$ die Klasse von $f\mathfrak{d}$ ist, $\overline{\lambda}$ der konjugiert komplexe Charakter zu λ, und $\mathsf{W}(\lambda)$ die nur von $\lambda\big((\widehat{\mu})\big)$ (und f) abhängige Größe

$$\mathsf{W}(\lambda) = (-i)^{\sum_{p=1}^{n} a_p} \frac{\lambda(\widehat{\varphi}\widehat{\delta})v(\widehat{\varphi}\widehat{\delta})C(\chi, \widehat{\varphi}\widehat{\delta})}{\sqrt{N(f)}},$$

wobei $C(\chi, \widehat{\varphi}\widehat{\delta})$ die Bedeutung von Satz 29 hat.

Wir wissen vorläufig nicht, ob die betrachteten Thetafunktionen nicht identisch verschwinden. Dies wird sich im nächsten §▸ aus dem Nichtverschwinden der allgemeinsten L–Reihen ergeben. Nehmen wir daher vorläufig schon an, daß keine der $\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta})$ identisch verschwindet, so folgt durch zweimalige

[‡] s. S. 81▸

Anwendung unserer Funktionalgleichung, und Wegdivision der Thetafunktion:

95 II

$$\frac{\mathsf{W}(\lambda)}{\lambda(|\widehat{\varphi\delta}|)}\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}\cdot\frac{\mathsf{W}(\overline{\lambda})}{\overline{\lambda}(|\widehat{\varphi\delta}|)}\prod_{p=1}^{n} t_p^{\frac{1}{2}+a'_p}=1$$

für alle (t). Die (t) heben sich natürlich heraus, denn es ist nach Wahl der t_p und wegen der Eigenschaften der a_p:

$$\prod_{p=1}^{n} t_p^{a'_p}=\prod_{p=1}^{n} t_p^{a_p}.$$

Wegen $\lambda(|\widehat{\varphi\delta}|)\overline{\lambda}(|\widehat{\varphi\delta}|)=1$ (als Produkt konjugiert–komplexer Größen vom Betrage 1) folgt also

$$\mathsf{W}(\lambda)\mathsf{W}(\overline{\lambda})=1.$$

Andererseits ist die konjugiert komplexe Größe:

$$\overline{\mathsf{W}(\lambda)}=(-i)^{-\sum_{p=1}^{n} a_p}\frac{\overline{\lambda}(\widehat{\varphi\delta})\overline{v}(\widehat{\varphi\delta})\overline{C(\chi,\widehat{\varphi\delta})}}{\sqrt{N(f)}}.$$

Nun war

$$C(\chi,\widehat{\varphi\delta})=\sum_{\widehat{\varrho}}\chi(\widehat{\varrho})e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi\delta}}\right)},$$

summiert über ein volles Restsystem $\widehat{\varrho}$ mod f aus der Klasse von $\widehat{\varphi\delta}$. Also wird

$$\begin{aligned}\overline{C(\chi,\widehat{\varphi\delta})} &= \sum_{\widehat{\varrho}}\overline{\chi}(\widehat{\varrho})e^{-2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi\delta}}\right)}\\ &= \chi(-1)C(\overline{\chi},\widehat{\varphi\delta})\end{aligned}$$

Also wird:

$$\overline{\mathsf{W}(\lambda)}=(-1)^{\sum_{p=1}^{n} a_p}\chi(-1)\mathsf{W}(\overline{\lambda}),$$

96 II

weil ja

$$\begin{aligned}\mathsf{W}(\overline{\lambda}) &= (-i)^{\sum_{p=1}^{n} a'_p} \frac{\overline{\lambda}(\widehat{\varphi}\widehat{\delta})v(\widehat{\varphi}\widehat{\delta})C\left(\frac{\overline{\chi}}{v^2}, \widehat{\varphi}\widehat{\delta}\right)}{\sqrt{N(f)}} \\ &= (-i)^{\sum_{p=1}^{n} a_p} \frac{\overline{\lambda}(\widehat{\varphi}\widehat{\delta})\overline{v}(\widehat{\varphi}\widehat{\delta})C\left(\overline{\chi}, \widehat{\varphi}\widehat{\delta}\right)}{\sqrt{N(f)}}\end{aligned}$$

ist, da v^2 Charakter von $\mathfrak{Z}(1)$, also $v^2(\widehat{\varrho}) = v^2(\widehat{\varphi}\widehat{\delta})$ und

$$C\left(\frac{\overline{\chi}}{v^2}, \widehat{\varphi}\widehat{\delta}\right) = \frac{1}{v^2(\widehat{\varphi}\widehat{\delta})} C(\overline{\chi}, \widehat{\varphi}\widehat{\delta}) \quad \text{ist.}$$

Nun ist offenbar

$$(-1)^{\sum_{p=1}^{n} a_p} = \lambda(-1)v(-1),$$

also

$$\overline{\mathsf{W}(\lambda)} = \lambda\big((-1)\big)\mathsf{W}(\overline{\lambda}) = \mathsf{W}(\overline{\lambda}).$$

Nach dem vorhin Gezeigten ist also

$$\big|\mathsf{W}(\lambda)\big| = 1$$

Satz 35. Der Faktor

$$\mathsf{W}(\overline{\lambda}) = (-i)^{\sum_{p=1}^{n} a_p} \frac{\lambda(\widehat{\varphi}\widehat{\delta})v(\widehat{\varphi}\widehat{\delta})C\left(\chi, \widehat{\varphi}\widehat{\delta}\right)}{\sqrt{N(f)}}$$

in der Funktionalgleichung für $\vartheta(t, \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta})$ hat den absoluten Betrag 1.

Wir beweisen ferner noch einen Satz über die Konvergenz der Reihe für $\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta})$.

Satz 36. Die Reihe

$$\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}) = \sum_{\widehat{\mu}|\mathfrak{K}} \chi(\widehat{\mu}) \prod_{p=1}^{n} \left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p} \cdot e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}}$$

konvergiert gleichmäßig für alle $t_p > \varepsilon_p > 0$[§]. Für $t_p \to 0$ ist:

$$\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}) = O\left(\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}\right)$$

und für $t_p \to \infty$:

$$\vartheta_0(t; \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}) = o\left(\prod_{p=1}^{n} t_p^{-c_p}\right); \quad (c_p > 0 \text{ beliebig}),$$

wo ϑ_0 die Thetareihe ohne das ev. Glied mit $\widehat{\mu} = 0$ bezeichnet.

Beweis: 1.) Zunächst ist die Konvergenz der Reihe *überhaupt* für alle $t_p > 0$ klar aus ihrer Entstehungsweise und nach Satz 32. Wir beweisen ferner ihre *absolute* Konvergenz für alle $t_p > 0$. Dazu genügt es □□□, die Konvergenz von

$$\sum_{\widehat{\mu}|\mathfrak{K}} \prod_{p=1}^{n} \left|\widehat{\mu}^{(p)}\right|^{a_p} e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}}$$

zu beweisen. Ist $\widehat{\alpha}$ ein Repräsentant aus $\mathfrak{K}^{-1}$, so durchläuft $\widehat{\mu}$ alle ganzen Zahlen aus $\mathfrak{K}$, wenn in $\widehat{\mu} = \frac{\mu}{\widehat{\alpha}}\,\mu$ alle durch $(\widehat{\alpha})$ teilbaren Körperzahlen durchläuft. Daher kommt es nur darauf an, die Konvergenz von

$$\sum_{\mu \equiv 0\ (\mathfrak{a})} \prod_{p=1}^{n} \left|\mu^{(p)}\right|^{a_p} e^{-\pi \sum\limits_{p=1}^{n} t_p \kappa_p |\mu^{(p)}|^2}$$

zu zeigen, wo die κ_p irgendwelche reellen Zahlen > 0 sind.

98 II

Denkt man sich die μ durch ein Basis (α_q) von $\mathfrak{a}$ in der Form

$$\mu = \sum_{q=1}^{n} m_q \alpha_q$$

dargestellt, wo jetzt $(m) = (m_1, \ldots, m_n)$ den ganzen „ganzzahligen“ Raum zu durchlaufen hat, so steht im Exponenten ein Ausdruck $-\pi B(m)$ wo B eine positiv–definite quadratische Form ist und als Koeffizienten der Exponentialgrößen treten Polynome in den m_q auf. Nach dem Beweis a. S. 70▶–73▶

[§] und ist daher stetig für alle $t_p > 0$.

folgt daher die absolute Konvergenz, also auch die absolute Konvergenz der Thetareihe für alle $t_p > 0$.

2.) Die gleichmäßige Konvergenz für $t_p > \varepsilon_p > 0$ folgt nun leicht. Ersichtlich verkleinert man nämlich jedes einzelne Glied der Thetareihe absolut, wenn man irgendein t_p vergrößert. Die nach 1.) absolut konvergente Reihe $\vartheta(\varepsilon_p; \mathfrak{K}, \lambda, \widehat{\varphi\delta})$ liefert also für alle $t_p > \varepsilon_p$ eine gliedweise Majorante, woraus die Behauptung folgt.

3.) □□□ Das Verhalten bei $t_p \to 0$ lesen wir aus der Funktionalgleichung ab. Da nämlich für $t_p \to 0$ (d. h. *irgendwelche* der $t_p \to 0$) rechts alles bis auf $\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}$ endlichen Grenzwerten zustrebt, folgt die Behauptung des Satzes unmittelbar.

99 II

4.) Das Verhalten bei $t_p \to \infty$ beweisen wir so: Es genügt zu zeigen, daß die aus $\vartheta_0(t, \mathfrak{K}, \lambda, \widehat{\varphi\delta})$ durch (gliedweise) Multiplikation mit dem Faktor $\prod_{p=1}^{n} t_p^{c_p}$ ($c_p > 0$ beliebig) entstehende Reihe für alle $t_p > G$[7] gleichmäßig konvergiert. Denn dann hat die Funktion $\prod_{p=1}^{n} t_p^{c_p} \vartheta_0(t, \mathfrak{K}, \lambda, \widehat{\varphi\delta})$ im Punkte $t_p = \infty$ (d. h. irgendwelche $t_p = \infty$) den Wert 0, weil jedes Glied der (ausmultiplizierten) Reihe dort den Wert Null hat, (e^{-t} wird stärker Null als jede Potenz t^c von t unendlich wird), und ist wegen der gleichmäßigen Konvergenz stetig, sodaß

$$\lim_{t\to\infty} \prod_{p=1}^{n} t_p^{c_p} \vartheta_0(t, \mathfrak{K}, \lambda, \widehat{\varphi\delta}) = 0$$

folgt, was die Behauptung ist.

Zum Beweise der gleichmäßigen Konvergenz obiger Reihe genügt es ähnlich wie oben, eine von t unabhängige, absolut konvergente gliedweise Majorante für

$$\sum_{\mu \equiv 0 \ (\mathfrak{a})} \prod_{p=1}^{n} \left|\mu^{(p)}\right|^{a_p} \prod_{p=1}^{n} t_p^{c_p} e^{-\pi \sum_{p=1}^{n} t_p \kappa_p |\mu^{(p)}|^2}$$

□□□

100 II

[7] Das vorangehende Zeichen ist schwer lesbar.

□□□

anzugeben. Nun gibt es zu jedem $\varepsilon > 0$ ein G, sodaß für alle $t_p > G(\varepsilon)$

$$\sum_{p=1}^{n} c_p \log t_p < \varepsilon \sum_{p=1}^{n} t_p$$

wird. Demnach wird für alle $t_p > G$ obige Reihe die gliedweise Majorante haben:

$$\sum_{\mu \equiv 0 \ (\mathfrak{a})} \prod_{p=1}^{n} |\mu^{(p)}|^{a_p} e^{-\pi \sum_{p=1}^{n} t_p \kappa_p |\mu^{(p)}|^2 + \varepsilon \sum_{p=1}^{n} t_p}$$

$$= \sum_{\mu \equiv 0 \ (\mathfrak{a})} \prod_{p=1}^{n} |\mu^{(p)}|^{a_p} e^{-\pi \sum_{p=1}^{n} t_p \kappa_p \left(|\mu^{(p)}|^2 - \varepsilon'\right)}$$

wo ε' mit ε leicht angebbar zusammenhängt (von t unabhängig). Denkt man sich hier wieder die μ in der Form

$$\mu = \sum_{i=1}^{n} m_i \alpha_i$$

dargestellt, sodaß (m) das ganzzahlige Gitter durchläuft, so zerlegt sich diese Summe in Teile

$$\sum_{(m)} \left| \prod_{i=1}^{n} m_i^{d_i} \right| e^{-\pi \sum_{p=1}^{n} t_p \kappa_p (A_p(m) - \varepsilon')}$$

wo $A_p(m)$ eine positive definite quadratische Form der m_i ist. Wegen

$$\varepsilon' \leqq \varepsilon' \sum_{i=1}^{n} m_i^2 \quad \square\square\square$$

hat diese Summe zur gliedweisen Majorante:

$$\sum_{(m)} \left| \prod_{i=1}^{n} m_i^{d_i} \right| e^{-\pi \sum_{p=1}^{n} t_p \kappa_p (A_p - \varepsilon' E)(m)}$$

Für hinreichend kleine ε' ist aber $\left(A_p - \varepsilon' E\right)(m)$ bekanntlich immer noch positiv definit, also auch die gesamte Quadratische Form im Exponenten,

sodaß diese Reihe absolut konvergiert und ersichtlich für alle $t_p > G$ die mit $t_p = G$ gebildete Reihe zur gliedweisen absolut konvergenten Majorante hat. Daraus folgt dann sofort eine ebensolche Majorante für unsere zugrundegelegte Thetareihe, gültig für alle $t_p > G$, woraus die Behauptung, wie schon gesagt, folgt.

2.6 §6 Die Funktionalgleichung der allgemeinsten L–Reihen.

102 II

Satz 37. Ist $\lambda\big((\widehat{\mu})\big)$ irgendein Größencharakter für Ideale, so konvergiert die unendliche Reihe

$$L(s,\lambda) = \sum_{(\widehat{\mu})}{}' \frac{\lambda\big((\widehat{\mu})\big)}{|N(\widehat{\mu})|^s},$$

erstreckt über alle ganzen (nicht assoziierten) Ideale $(\widehat{\mu}) \neq 0$, absolut und gleichmäßig für $\Re(s) > 1$, stellt also dort eine reguläre analytische Funktion der komplexen Variablen s dar. Es gilt ferner für $\Re(s) > 1$ die absolut konvergente Produktdarstellung

$$L(s,\lambda) = \prod_{(\widehat{\pi})} \frac{1}{1 - \frac{\lambda((\widehat{\pi}))}{|N(\widehat{\pi})|^s}},$$

erstreckt über alle (nicht assoziierten) Primideale $(\widehat{\pi})$ des Körpers, sodaß demnach

$$L(s,\lambda) \neq 0 \quad \text{für} \quad \Re(s) > 1$$

ist.

Beweis: Die erste Behauptung ist klar, da wegen $|\lambda\big((\widehat{\mu})\big)| = 1$ die Dedekindsche ζ–Funktion von k:

$$\zeta_k(s) = \sum_{(\widehat{\mu})}{}' \frac{1}{|N(\widehat{\mu})|^s},$$

gebildet für $s = 1 + \varepsilon$ eine für alle $\Re(s) > 1 + \varepsilon$ gültige, absolut konvergente, gliedweise Majorante liefert. Wegen der Produkteigenschaft $\lambda\big((\widehat{\mu})\big)\lambda\big((\widehat{\nu})\big) = \lambda\big((\widehat{\mu})(\widehat{\nu})\big)$

103 II

folgt aus der absoluten Konvergenz in bekannter Weise die zweite Behauptung.

Die in Satz 37 eingeführten *allgemeinsten L–Reihen mit Größencharakteren*, die als spezielle Fälle die L–Reihen mit Klassencharakteren (absolut

und mod f), speziell also auch $\zeta_k(s)$ und für den rationalen Grundkörper $\zeta(s)$ und die Dirichletschen L–Reihen enthalten, genügen sämtlich Funktionalgleichungen vom Typus der Riemannschen Funktionalgleichung für $\zeta(s)$. Der Weg zur Herleitung dieser Funktionalgleichungen ergibt sich durch eine entsprechende Verallgemeinerung der von Riemann bei $\zeta(s)$ eingeschlagenen Methode der Zurückführung auf die Funktionalgleichung (Transformationsformel) einer ϑ–Funktion. Der andere von Riemann bei $\zeta(s)$ eingeschlagene Weg, der an Stelle der ϑ–Reihe die bequemere geometrische Reihe $\sum_{n=0}^{\infty} e^{-nt}$ verwendet, führt in unserem allgemeinen Falle nicht zum Ziele (nur für total reelle Grundkörper). Die sämtlichen genannten Spezialfälle werden durch die folgenden allgemeinst–möglichen Betrachtungen mit umfaßt, sodaß aus der Theorie der ζ_k–Funktion nichts weiter vorausgesetzt wird, als die elementar zu beweisende, eben benutzte Konvergenz. Es werden vielmehr auch die

Sätze über das Verhalten von $\zeta_k(s)$ bei $s = 1$ zwanglos aus den folgenden Betrachtungen herausspringen.

Die fundamentale Thetatransformationsformel von Satz 34, die mit der abzuleitenden Funktionalgleichung der $L(s, \lambda)$ im wesentlichen äquivalent ist, gilt nur für *eigentliche* Charaktere $\lambda\big((\widehat{\mu})\big)$. Es wird also auch die resultierende Funktionalgleichung sich nur auf L–Reihen mit eigentlichen Charakteren beziehen. Hierdurch beherrscht man aber auch *sämtliche* L–Reihen.

Ist nämlich $\lambda\big((\widehat{\mu})\big)$ irgendein Größencharakter mod f, so erzeugt dieser nach Satz 26, S. 58 stets einen eindeutig bestimmten eigentlichen Größencharakter $\lambda_1\big((\widehat{\mu})\big)$ nach einem eindeutig bestimmten Teiler f_1 von f, derart daß beide Charaktere für alle zu f primen $(\widehat{\mu})$ übereinstimmen. Offenbar ist dann

$$L(s, \lambda) = L(s, \lambda_1) \prod_{(\widehat{\pi})|f} \left(1 - \frac{\lambda_1\big((\widehat{\pi})\big)}{|N\big(\widehat{\pi}\big)|^s}\right),$$

denn auf diese Weise werden wegen

$$\lambda_1\big((\widehat{\mu})\big) = \lambda_1(\widehat{\mu}) v_1(\widehat{\mu}) \chi_1(\widehat{\mu})$$

und

$$\chi_1(\widehat{\mu}) = 0, \quad \text{wenn} \quad (\widehat{\mu}, f_1) \neq 1$$

aus dem Produkt $L(s, \lambda_1)$ gerade alle die Faktoren herausgehoben, die den zu f_1 aber nicht zu f primen $(\widehat{\pi})$

105 II

entsprechen, und in denen allein $L(s,\lambda)$ und $L(s,\lambda_1)$ differieren.

Die so den $L(s,\lambda)$ eindeutig zugeordneten $L(s,\lambda_1)$ sollen *eigentliche L–Reihen mod* f_1 heißen. Jede L–Reihe unterscheidet sich also von der zugehörigen eigentlichen nur um eine elementare Funktion von s. Die im folgenden abzuleitenden Funktionalgleichungen beziehen sich dann stets auf eigentliche L–Reihen. Natürlich genügen auch die nicht–eigentlichen L–Reihen Funktionalgleichungen, in denen jedoch jene elementaren Funktionen auftreten, und die in Wahrheit mit den Funktionalgleichungen der zugehörigen eigentlichen L–Reihen identisch sind. Gerade diese Tatsache führt zu einer der Hauptanwendungen der Funktionalgleichung der L–Reihen auf die Arithmetik der Zahlkörper.

Es sei also jetzt

$$\lambda\big((\widehat{\mu})\big) = \lambda(\widehat{\mu})v(\widehat{\mu})\chi(\widehat{\mu})$$

ein *eigentlicher* Charakter mod f in seiner eindeutigen Zerlegung nach §3▸. Entsprechend dem Riemannschen Wege haben wir zunächst das allgemeine Glied

$$\frac{\lambda\big((\widehat{\mu})\big)}{|N(\widehat{\mu})|^s} = \frac{\lambda(\widehat{\mu})\chi(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}$$

der unendlichen Summe für $L(s,\lambda)$ durch ein Γ–Integral

106 II

auszudrücken. Wir führen dies zuerst für

$$\frac{\lambda(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}$$

aus. Dazu müssen wir auf die Ausdrücke für $\lambda(\widehat{\mu})$ und $v(\widehat{\mu})$ zurückgehen. Um nachher auf die Thetareihe von §5▸ zu kommen, bilden wir diese zunächst für einen beliebigen Vektor $y = (y_1, \ldots, y_n)$, dessen Komponenten komplex, die $2r_2$ letzten in bekannter Weise konjugiert–komplex sind. Nachher werden wir dann y so spezialisieren, daß einerseits ein das zu bildende allgemeine Glied der L–Reihe enthaltender Ausdruck entsteht, andererseits gerade die Thetareihe herauskommt.

Es sei entsprechend Satz 8 (S. 23▸) und Satz 18 (S. 45▸):

$$(1)\qquad \begin{cases} \lambda(y) = \prod\limits_{q=1}^{r} e^{2\pi i m_q c_q(y)} \prod\limits_{p=r_1+1}^{n} e^{ia_p\left\{\varphi_p - \sum\limits_{k=1}^{r} \vartheta_k^{(p)} c_k(y)\right\}}, \\ v(y) = \prod\limits_{p=1}^{r_1} \left(\frac{y^{(p)}}{|y^{(p)}|}\right)^{a_p}, \end{cases}$$

wo die φ_p die Amplituden der y_p, also

$$e^{i\varphi_p} = \frac{y_p}{|y_p|}; \qquad (p = r_1 + 1, \dots n)$$

und die $c_q(y)$ die früheren Ausdrücke((7), S. 10)

$$c_q(y) = \sum_{p=1}^{r+1} e_p^{(q)} \log |y_p|; \qquad (q = 1, \dots, r)$$

sind. Wir schreiben jetzt $\lambda(y)$ in anderer Form, sodaß die φ_p und $c_q(y)$ durch die y_p und $|y_p|$ ersetzt werden:

$$\begin{aligned}
\lambda(y) &= \prod_{q=1}^{r} e^{2\pi i m_q \sum_{p=1}^{r+1} e_p^{(q)} \log |y_p|} \prod_{p=r_1+1}^{n} \left[\left(\frac{y_p}{|y_p|} \right)^{a_p} e^{-i a_p \sum_{k=1}^{r} \vartheta_k^{(p)} \sum_{j=1}^{r+1} e_j^{(k)} \log |y_j|} \right] \\
&= \prod_{p=1}^{r+1} |y_p|^{\sum_{q=1}^{r} 2\pi i m_q e_p^{(q)}} \cdot \prod_{p=r_1+1}^{n} \left(\frac{y_p}{|y_p|} \right)^{a_p} \cdot e^{-i \sum_{p=r_1+1}^{n} a_p \sum_{k=1}^{r} \vartheta_k^{(p)} \sum_{j=1}^{r+1} e_j^{(k)} \log |y_j|} \\
&= \prod_{p=1}^{r+1} |y_p|^{\sum_{q=1}^{r} 2\pi i m_q e_p^{(q)}} \cdot \prod_{p=r_1+1}^{n} \left(\frac{y_p}{|y_p|} \right)^{a_p} \cdot \prod_{p=1}^{r+1} |y_p|^{-i \sum_{q=1}^{r} e_p^{(q)} \sum_{k=r_1+1}^{n} a_k \vartheta_q^{(k)}} \\
&= \prod_{p=1}^{r+1} |y_p|^{\sum_{q=1}^{r} e_p^{(q)} \left\{ 2\pi i m_q - i \sum_{k=1}^{n} a_k \vartheta_q^{(k)} \right\}} \cdot \prod_{p=r_1+1}^{n} \left(\frac{y_p}{|y_p|} \right)^{a_p},
\end{aligned}$$

wo die $\sum_{k=r_1+1}^{n}$ wegen des Verschwindens der r_1 ersten $\vartheta_q^{(k)}$ durch $\sum_{1}^{n}$ ersetzt werden dürfte. Es ist demnach $\lambda(y)$ wieder in eine zu (3) in Satz 1, S. 6 analoge Form transformiert und so die dort noch nicht weiter beschränkten Exponenten s_p in eine den dortigen späteren Entwicklungen entsprechende *beschränkte* Form gesetzt, eben so, daß $\lambda(y)$ Größencharakter ist.

Damit wird jetzt:

$$\frac{\lambda(y) v(y)}{|N(y)|^s} = |N(y)|^{-s} \prod_{p=1}^{r+1} |y_p|^{\sum_{q=1}^{r} e_p^{(q)} \psi_q(\lambda)} \prod_{p=1}^{n} \left(\frac{y_p}{|y_p|} \right)^{a_p},$$

wo zur Abkürzung gesetzt ist:

$$\psi_q(\lambda) = 2\pi i m_q - i\sum_{k=1}^{n} a_k \vartheta_q^{(k)}. \tag{2}$$

$\psi_q(\lambda)$ ist eine durch die Exponenten m_q, a_p von $\lambda(y)$ allein bestimmte Größe.

Wir schreiben weiter

$$|N(y)| = \prod_{p=1}^{r+1} |y_p|^{e_p},$$

wo die e_p die Bedeutung von §1 ((6) und (6a), S. 9) haben. Sind a'_p die Exponenten von $\overline{\lambda}$, so können wir, wie leicht aus Satz 23 (S. 54) folgt formal anders schreiben:

$$\prod_{p=1}^{n} |y_p|^{a_p} = \prod_{p=1}^{r+1} |y_p|^{e_p \frac{a_p + a'_p}{2}},$$

weil $e_p \frac{a_p + a'_p}{2}$ die Gesamtheit der a_p darstellt, und „konjugiert–komplexe“ $|y_p|$ gleich sind.

Somit wird

$$\frac{\lambda(y) v(y)}{|N(y)|^s} = \prod_{p=1}^{r+1} |y_p|^{-z_p} \prod_{p=1}^{n} y_p^{e_p}, \tag{3}$$

wo gesetzt ist:

$$z_p = z_p(s,\lambda) = e_p\left(s + \frac{a_p + a'_p}{2}\right) - \sum_{q=1}^{r} e_p^{(q)} \psi_q(\lambda); \qquad (p = 1, \dots r+1). \tag{4}$$

Wir haben nunmehr für (3) ein Γ–Integral einzuführen. Dazu stellen wir zunächst jeden Faktor $|y_p|^{-z_p}$ durch ein solches dar:

$$\Gamma\left(\frac{z_p}{2}\right) |y_p|^{-z_p} = \int_0^\infty e^{-t_p |y_p|^2} t_p^{\frac{z_p}{2} - 1} dt_p,$$

wie man leicht aus

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt; \qquad \big(\Re(z) > 0\big)$$

berechnet. Unser Γ–Integral konvergiert also für alle

$\Re(z_p) > 0$, also wegen (s. (2) u. (4))

$$\Re(z_p) = e_p \left(\Re(s) + \frac{a_p + a_p'}{2} \right) \geqq \Re(s)$$

sicher für $\Re(s) > 0$, was für uns ausreicht. Durch Produktbildung folgt dann:

$$(5) \qquad \prod_{p=1}^{r+1} \Gamma\left(\frac{z_p}{2}\right) |y_p|^{-z_p} = \int_0^\infty \cdots \int e^{-\sum_{p=1}^{r+1} t_p |y_p|^2} \prod_{p=1}^{r+1} t_p^{\frac{z_p}{2}} \frac{dt_1 \ldots dt_{r+1}}{t_1 \ldots t_{r+1}}.$$

Führen wir also die Abkürzung

$$(6) \qquad \Gamma(s, \lambda) = \prod_{p=1}^{r+1} \Gamma\left(\frac{z_p}{2}\right) = \prod_{p=1}^{r+1} \Gamma\left\{ \frac{e_p}{2} \left(s + \frac{a_p + a_p'}{2} \right) - \frac{1}{2} \sum_{q=1}^{r} e_p^{(q)} \psi_p(\lambda) \right\}$$

ein, so wird nach (3):

$$(7) \qquad \Gamma(s, \lambda) \frac{\lambda(y) v(y)}{|N(y)|^s} = \int_0^\infty \cdots \int \prod_{p=1}^{n} y_p^{a_p} e^{-\sum_{p=1}^{r+1} t_p |y_p|^2} \prod_{p=1}^{r+1} t_p^{\frac{z_p}{2}} \frac{dt_1 \ldots dt_{r+1}}{t_1 \ldots t_{r+1}}.$$

Wir wollen nun unter dem Integral das allgemeine Glied der Thetareihe von §5▸ herstellen, dessen Exponentialgröße lautet:

$$e^{-\pi \sum_{p=1}^{n} t_p \frac{|\widehat{\mu}^{(p)}|^2}{|\widehat{\varphi}^{(p)} \widehat{\delta}^{(p)}|}}.$$

Dazu haben wir zu setzen:

$$(8) \qquad y_p = \frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)} \widehat{\delta}^{(p)}|}} \sqrt{e_p \pi}.$$

Diese y_p bilden nach Definition der konjugierten zu idealen Zahlen, und wegen der Werte der e_p tatsächlich einen solchen Vektor, wie wir ihn oben für y zugrundegelegt hatten, und es wird nach Bedeutung der e_p:

$$\sum_{p=1}^{r+1} t_p |y_p|^2 = \pi \sum_{p=1}^{n} t_p \frac{|\widehat{\mu}^{(p)}|^2}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|},$$

wenn wir entsprechend den früheren Formeln

$$(t_{r_1+r_2+1}, \ldots, t_n) = (t_{r_1+1}, \ldots, t_{r_1+r_2})$$

festsetzen. Für das y aus (8) wird:

$$\begin{aligned} \lambda(y) &= \lambda(\widehat{\mu})\overline{\lambda}(\sqrt{|\widehat{\varphi}\widehat{\delta}|})\lambda(\sqrt{e_p\pi}), \\ v(y) &= v(\widehat{\mu})\overline{v}(\sqrt{|\widehat{\varphi}\widehat{\delta}|})v(\sqrt{e_p\pi}). \end{aligned}$$

Nun ist nach Satz 9, S. 25▶:

$$\lambda(\sqrt{e_p\pi}) = \lambda(\sqrt{e_p}) = \sqrt{2}^{\sum_{p=r_1+1}^{r_1+r_2} \sum_{q=1}^{r} e_p^{(q)}\psi_q(\lambda)} = 2^{\frac{1}{2}\sum_{q=1}^{r}\psi_q(\lambda)\sum_{p=r_1+1}^{r_1+r_2} e_p^{(q)}} \tag{9}$$

nach S. 107▶ oben und (2). Ferner

$$v(\sqrt{e_p\pi}) = \overline{v}(\sqrt{|\widehat{\varphi}\widehat{\delta}|}) = 1,$$

da die Wurzeln hier, wie im folgenden stets positiv zu verstehen sind. Schließlich wird:

$$|N(y)| = |N(\widehat{\mu})| 2^{r_2}\pi^{\frac{\pi}{2}} \cdot \frac{1}{\sqrt{N(f\vartheta)}},$$

somit

$$\frac{\lambda(y)v(y)}{|N(y)|^s} = \frac{\lambda(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}\overline{\lambda}(\sqrt{|\widehat{\varphi}\widehat{\delta}|})\lambda(\sqrt{e_q})\left(\frac{\sqrt{N(f\vartheta)}}{2^{r_2}\pi^{\frac{n}{2}}}\right)^s.$$

Wird also noch zur Abkürzung:

$$\mathsf{A} = \frac{\sqrt{N(f\vartheta)}}{2^{r_2}\pi^{\frac{n}{2}}} = \sqrt{\frac{d\,N(f)}{2^{2r_2}\pi^n}} \tag{10}$$

gesetzt, so geht (7) durch die Substitution (8) über in:

$$\lambda(\sqrt{e_p})\overline{\lambda}(\sqrt{|\widehat{\varphi}\widehat{\delta}|})\mathsf{A}^s\Gamma(s,\lambda)\frac{\lambda(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}$$

$$= \prod_{p=1}^{n}(\sqrt{e_p\pi})^{a_p}\int_0^\infty\cdots\int\prod_{p=1}^{n}\left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p} e^{-\pi\sum\limits_{p=1}^{n}t_p\frac{|\widehat{\mu}^{(p)}|^2}{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\cdot$$
$$\cdot\prod_{p=1}^{r+1}t_p^{\frac{z_p}{2}}\frac{dt_1\ldots dt_{r+1}}{t_1\ldots t_{r+1}}.$$

Setzen wir schließlich zur Abkürzung (siehe (9))*:

$$\gamma(\lambda)=\frac{\lambda(\sqrt{e_p})}{\prod\limits_{p=1}^{n}(\sqrt{e_p\pi})^{a_p}}=2^{\frac{1}{2}\sum\limits_{q=1}^{r}\psi_q(\lambda)\sum\limits_{p=r_1+1}^{r_1+r_2}e_p^{(q)}-\frac{1}{2}\sum\limits_{p=r_1+1}^{n}a_p}\cdot\pi^{-\frac{1}{2}\sum\limits_{p=1}^{n}a_p}, \tag{11}$$

so erhalten wir folgende Formel:

$$\gamma(\lambda)\Gamma(s,\lambda)\mathsf{A}^s\frac{\lambda(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}\overline{\lambda}(\sqrt{|\widehat{\varphi}\widehat{\delta}|})$$
$$= \int_0^\infty\cdots\int\prod_{p=1}^{n}\left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p}\cdot e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}}\cdot\prod_{p=1}^{r+1}t_p^{\frac{z_p}{2}}\cdot\frac{dt_1\ldots dt_{r+1}}{t_1\ldots t_{r+1}}. \tag{12}$$

Unter dem Integral steht jetzt gerade das allgemeine Glied unserer ϑ–Reihe von §5▶ (bis auf den auch links noch nicht angebrachten Faktor $\chi(\widehat{\mu})$), und nunmehr wird ersichtlich, weshalb wir damals die ursprüngliche Relation in der beschriebenen Weise differenzieren mußten, aber weil in (3) außer dem

*bei Hecke ist der Faktor $\prod\limits_{p=1}^{n}(\sqrt{e_p\pi})^{-a_p}$ wohl versehentlich übersehen; s. aber Anm. 1 a. S. 145, wonach das Resultat hierdurch nicht beeinflußt wird.

von s abhängigen, in ein Γ–Integral umgewandelten Faktor $\prod_{p=1}^{r+1} |y_p|^{-z_p}$ noch der Faktor $\prod_{p=1}^{n} y_p^{a_p}$ auftritt.

Um jetzt unsere L–Reihe zu bilden, hätten wir in (12) links mit $\chi(\widehat{\mu})$ zu multiplizieren und über alle ganzen *Ideale* $(\widehat{\mu}) \neq 0$ zu summieren. Diese Summation wäre

112 II

erstens zweckmäßig gesondert für die einzelnen Idealklassen $\mathfrak{K}$ auszuführen, um rechts unter dem Integral auf die einzelnen $\vartheta(t, \mathfrak{K})$ zu kommen. Das würde aber *zweitens* rechts noch nicht auf die $\vartheta(t, \mathfrak{K})$ führen, da diese ja Summen über alle ganzen *Zahlen* $\widehat{\mu}$ aus $\mathfrak{K}$ sind. Um diesem Umstand gerecht zu werden, liegt es nahe, vor Ausführung der Summation über die verschiedenen *Ideale* $(\widehat{\mu})$ die rechte Seite so umzuformen, daß sie schon eine Summe über alle zu der idealen Zahl $\widehat{\mu}$ assoziierten Zahlen $\varepsilon\widehat{\mu}$ wird. Diese würde dann mit der nachher auszuführenden Summation über die verschiedenen *Ideale* $(\widehat{\mu})$ rechts gerade auf die Summe über alle ganzen *Zahlen* $\widehat{\mu} \neq 0$ aus $\mathfrak{K}$, also im wesentlichen auf unsere ϑ–Reihe führen.

In der Tat läßt sich nun die rechte Seite von (12) in die angegebene Gestalt setzen, indem man die zu erzeugende Summe über alle $\varepsilon\widehat{\mu}$ durch Zerlegung des Integrals $\int_0^\infty \cdots \int$ in Integrale über endliche Intervalle zusammensetzt. Hierzu sind jedoch an Stelle der Variablen t_p neue Variable u, x_q einzuführen, die mit den Einheiten, über die ja summiert werden soll, in Zusammenhang stehen. Wir setzen, indem wir vorläufig nur die Strahleinheiten $\equiv 1 \mod f$, total positiv berücksichtigen:

113 II

$$t_p = u e^{2\sum_{q=1}^{r} x_q \log|\eta_q^{(p)}|} = u \prod_{q=1}^{r} |\eta_q^{(p)}|^{2x_q}; \qquad (p = 1, 2, \ldots, r+1) \tag{13}$$

sodaß nach (7), (8) S. 10/11 umgekehrt wird:

$$\begin{cases} u = \sqrt[n]{N(t)} = \sqrt[n]{t_1 \ldots t_n} \\ x_q = \frac{1}{2} c_q(t) = \frac{1}{2} \sum_{p=1}^{r+1} e_p^{(q)} \log t_p\,; \qquad (q = 1, 2, \ldots r) \end{cases} \tag{13a}$$

Der Sinn ist der, daß wir den Vektor t erstens durch Wegdivision von $\sqrt[n]{N(t)}$ in einen „Einheitsvektor“ verwandeln und diesen dann durch die Beträge der Grundeinheiten unseres Strahles 0: „$\equiv 1 \mod f$, total positiv“ darstellen. Durchläuft dabei t den Raum aller total–reell–positiven Körpervektoren, wie es ja in dem Integral rechts in (12) der Fall ist, so durchlaufen auch (13), (13a) die u, x_q in umkehrbar eindeutiger Zuordnung das Gebiet:

$$\left\{ \begin{array}{c} u \geqq 0 \\ -\infty \leqq x_q \leqq +\infty \end{array} \right. ; \qquad (q = 1, 2, \dots r). \tag{14}$$

Nunmehr wird, grob gesagt, das Integral über die t so zerlegt, daß nur über alle „nicht assoziierten“ t, d. h. nicht um Potenzprodukte aus den Beträgen der Strahlgrundeinheiten $|\eta_q|$ unterschiedene t integriert wird. Die so entstehende Summe über Einzelintegrale transformiert sich dann leicht in ein Integral über eine Summe nach assoziierten $\widehat{\mu}$.

114 II

Wir haben also jetzt das Integral rechts in (12) auf die neuen Variablen u, x_q zu transformieren. Das t in der Spur im Exponenten von e lassen wir stehen, da es auf seine Transformation nicht ankommt, fassen es aber nach (13) als Funktion der u, x_q auf. Es bleiben somit zu transformieren:

1.) die Integrationsgrenzen,

2.) der Faktor $\frac{dt_1 \dots dt_{r+1}}{t_1 \dots t_{r+1}}$,

3.) der Faktor $\prod_{p=1}^{r+1} t_p^{\frac{z_p}{2}}$.

1.) ist durch (14) erledigt. Wird zur Abkürzung

$$dX = dx_1 \dots dx_r$$

und X für jedes x_q eingeführt, so wird

$$\int_0^\infty \cdots \int dt_1 \dots dt_{r+1} = \int_{u=0}^{\infty} \int_{X=-\infty}^{+\infty} \Delta \, du \, dX,$$

wo Δ die Funktionaldeterminante $\left|\frac{\partial(t_1,\dots t_{r+1})}{\partial(u,X)}\right|$ bezeichnet.
2.) führt auf die Berechnung von Δ. Man erhält aus (13)

$$\Delta = \begin{vmatrix} \frac{t_1}{u} & 2t_1 \log|\eta_1^{(1)}| & \cdots\cdots & 2t_1 \log|\eta_r^{(1)}| \\ \frac{t_2}{u} & 2t_2 \log|\eta_1^{(2)}| & \cdots\cdots & 2t_2 \log|\eta_r^{(2)}| \\ \vdots & \vdots & & \\ \vdots & \vdots & & \\ \frac{t_{r+1}}{u} & 2t_{r+1} \log|\eta_1^{(r+1)}| & \cdots\cdots & 2t_{r+1} \log|\eta_r^{(r+1)}| \end{vmatrix}$$

(wobei natürlich, wie es der Integraltransformation entspricht, die absoluten Beträge gemeint sind).

115 II

Nach S. 8▶ wird demnach

$$\Delta = \frac{n}{u} t_1 \dots t_{r+1} 2^r \frac{R(f)}{2^{r_2}} = \frac{t_1 \dots t_{r+1}}{u} \cdot 2^{r_1 - 1} n R(f),$$

wenn $R(f)$ den Regulator von o bezeichnet, und somit

$$\int_0^\infty \cdots \int \frac{dt_1 \dots dt_{r+1}}{t_1 \dots t_{r+1}} = \int_{u=0}^{\infty} \int_{X=-\infty}^{+\infty} 2^{r_1-1} n R(f) \frac{du}{u} dX. \tag{15}$$

3.) Der Faktor $\prod_{p=1}^{r+1} t_p^{\frac{z_p}{2}}$ berechnet sich nach (13) so:

$$\prod_{p=1}^{r+1} t_p^{\frac{z_p}{2}} = u^{\frac{1}{2}\sum_{p=1}^{r+1} z_p} e^{\sum_{q=1}^{r} x_q \sum_{p=1}^{r+1} z_p \log|\eta_q^{(p)}|}.$$

Nach (4) wird wegen $\sum_{p=1}^{r+1} e_p = n$; $\sum_{p=1}^{r+1} e_p^{(q)} = 0$ (s. S. 8▶/9▶):

$$\frac{1}{2}\sum_{p=1}^{r+1} z_p = \frac{ns}{2} + \frac{1}{2}\sum_{p=1}^{r+1} e_p \frac{a_p + a'_p}{2} = \frac{ns}{2} + \frac{1}{2}\sum_{p=1}^{n} a_p.$$

Ferner wird nach (4), (2) wegen der Reziprozität der Matrizen (5), (6) in §1, S. 8/9.:

$$\begin{aligned}
&\sum_{p=1}^{r+1} z_p \log|\eta_q^{(p)}| \\
= &\sum_{p=1}^{r+1} \log|\eta_q^{(p)}| \left\{ e_p\Big(s+\frac{a_p+a_p'}{2}\Big) - \sum_{j=1}^{r} e_p^{(j)} \left(2\pi i m_j - i\sum_{k=1}^{n} a_k \vartheta_j^{(k)} \right) \right\} \\
= &\sum_{p=1}^{n} a_p \log|\eta_q^{(p)}| - \sum_{j=1}^{r} \left\{ \left(2\pi i m_j - i\sum_{k=1}^{n} a_k \vartheta_j^{(k)} \right) \sum_{p=1}^{r+1} e_p^{(j)} \log|\eta_q^{(p)}| \right\} \\
= &\sum_{p=1}^{n} a_p \log|\eta_q^{(p)}| - 2\pi i m_q + i\sum_{k=1}^{n} a_k \vartheta_q^{(k)} \\
= &-2\pi i m_q + \sum_{p=1}^{n} a_p \left(\log|\eta_q^{(p)}| + i\vartheta_q^{(p)} \right).
\end{aligned}$$

Es hat sich also s vollständig herausgehoben und ist ein nur von den Exponenten m_q, a_p von $\lambda\big((\widehat{\mu})\big)$ abhängender Ausdruck übrig geblieben, den wir zur Abkürzung mit

$$b_q(\lambda) = -2\pi i m_q + \sum_{p=1}^{n} a_p \left(\log|\eta_q^{(p)}| + i\vartheta_q^{(p)} \right); \qquad (q = 1, \ldots, r) \tag{16}$$

bezeichnen. Offenbar gehören zu dem reziproken Charakter $\overline{\lambda}\big((\widehat{\mu})\big)$ die Ausdrücke

$$b_q(\overline{\lambda}) = -2\pi i(-m_q) + \sum_{p=1}^{n} a_p' \left(\log|\eta_q^{(p)}| + i\vartheta_q^{(p)} \right), \tag{17}$$

was wir nachher verwenden werden. Für den zu transformierenden Faktor 3.) erhalten wir so:

$$\prod_{p=1}^{r+1} t_p^{\frac{z_p}{2}} = u^{\frac{ns}{2} + \frac{1}{2}\sum_1^n a_p} e^{\sum_{q=1}^{r} x_q b_q(\lambda)}. \tag{18}$$

Wir haben nunmehr (12) transformiert in folgende Formel, die sich aus (15), (18) sofort ergibt:

$$(19)\quad \left\{\begin{array}{c} \gamma(\lambda)\Gamma(s,\lambda)\mathsf{A}^s \frac{\lambda(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}\overline{\lambda}\left(\sqrt{|\widehat{\varphi}\widehat{\delta}|}\right) \\ = 2^{r_1-1}nR(f)\int\limits_{u=0}^{\infty}\int\limits_{X=-\infty}^{+\infty}\prod\limits_{p=1}^{n}\left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p} \cdot e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}+\sum\limits_{q=1}^{r}x_q b_q(\lambda)} \\ \cdot u^{\frac{ns}{2}+\frac{1}{2}\sum\limits_{1}^{n}a_p}\frac{du}{u}dX. \end{array}\right.$$

Wir setzen zur Abkürzung:

$$(20)\qquad F(u,\widehat{\mu},x_q)=\prod_{p=1}^{n}\left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p} e^{-\pi S\left\{t\frac{|\widehat{\mu}|^2}{|\widehat{\varphi}\widehat{\delta}|}\right\}+\sum\limits_{q=1}^{r}x_q b_q(\lambda)}$$

wodurch (19) übergeht in

$$(21)\quad \left\{\begin{array}{c} \gamma(\lambda)\Gamma(s,\lambda)\mathsf{A}^s \frac{\lambda(\widehat{\mu})v(\widehat{\mu})}{|N(\widehat{\mu})|^s}\overline{\lambda}\left(\sqrt{|\widehat{\varphi}\widehat{\delta}|}\right) \\ = 2^{r_1-1}nR(f)\int\limits_{u=0}^{\infty}\int\limits_{X=-\infty}^{+\infty}F(u,\widehat{\mu},x_q)u^{\frac{ns}{2}+\frac{1}{2}\sum\limits_{1}^{n}a_p}\frac{du}{u}dX. \end{array}\right.$$

Die Funktion $F(u,\widehat{\mu},x_q)$ hat nun folgende beiden Eigenschaften

$$(22)\qquad F(u,\widehat{\mu},x_1,\ldots,x_\ell+1,\ldots,x_r)=F(u,\eta_\ell\widehat{\mu},x_1,\ldots,x_r);\quad (\ell=1,2,\ldots,r)$$

$$(23)\qquad F(u,\widehat{\mu},x_1,\ldots,x_r)=F(u,\xi\widehat{\mu},x_1,\ldots,x_r)\quad \text{für jede Strahleinheitswurzel } \xi,$$

d. h. die Ersetzung von $\widehat{\mu}$ durch $\eta_\ell\widehat{\mu}$ hat denselben Erfolg, wie die Vermehrung von x_ℓ um 1 und die Ersetzung von $\widehat{\mu}$ durch $\xi\widehat{\mu}$ ändert gar nichts.

Dann wird $\widehat{\mu}$ durch $\eta_\ell\widehat{\mu}$ ersetzt, so bekommt nach (20) F den Zusatzfaktor

$$\prod_{p=1}^{n}\left(\eta_\ell^{(p)}\right)^{a_p}=e^{\sum\limits_{p=1}^{n}a_p\left(\log|\eta_\ell^{(p)}|+i\vartheta_\ell^{(p)}\right)}$$

und im Spurglied ist t durch $t|\eta_\ell|^2$ zu ersetzen, was wegen $N|\eta_\ell|^2 = 1$ die Variable u, die wir als Argument von F anzusehen haben, nicht ändert nach (13a), und die Variablen x_q, die in t ebenfalls stecken, nach (13a) so ändert, daß jetzt

$$x'_q = x_q + \sum_{p=1}^{r+1} e_p^{(q)} \log |\eta_\ell^{(p)}| = x_q + \delta_{q\ell}$$

an die Stelle von x_q zu treten hat, d. h. alle x_q außer x_ℓ invariant bleiben, dagegen x_ℓ durch $x_\ell + 1$ zu ersetzen ist. Der erstgenannte Zusatzfaktor ist schließlich mit genau derselben Änderung der noch explizit rechts in (20) vorkommenden x_q äquivalent, da er sich in der Form

$$e^{b_\ell(\lambda)}$$

darstellt, wie aus (16) sofort folgt. Damit ist (22) bewiesen.

118 II

Wird ferner $\widehat{\mu}$ durch $\xi\widehat{\mu}$ ersetzt, wo ξ eine der $w(f)$ in o vorkommenden Einheitswurzeln ist, so bekommt F zunächst den Zusatzfaktor

$$\prod_{p=1}^{n} (\xi^{(p)})^{a_p} = \xi^{\sum_{p=1}^{n} A_p a_p},$$

der nach (14), S. 16, bezw. der dazu analogen, der nunmehrigen Normierung der a_p entsprechenden, in Satz 8, S. 23▸ genannten Kongruenzbedingung den Wert 1 hat. (Nach S. 1▸ ist ja für $g \neq 1$, also $\xi \neq 1 : r_1 = 0$). Ferner ist t durch $t|\xi|^2 = t$ zu ersetzen, sodaß u, x_q ungeändert bleiben, womit (23) bewiesen ist.

Nach (22), (23) hat die Substitution:

$$\widehat{\mu} \to \widehat{\mu}\eta = \widehat{\mu}\eta_1^{n_1} \cdots \eta_r^{n_r} \xi^n$$

für eine beliebige Strahleinheit η denselben Erfolg, wie die Ersetzung von $x_1, \ldots, x_r$ durch

$$\begin{aligned} x'_1 &= x_1 + n_1 \\ x'_2 &= x_2 + n_2 \\ &\cdots\cdots\cdots\cdots \\ x'_r &= x_r + n_r, \end{aligned}$$

und umgekehrt ist die letztere Substitution gleichbedeutend mit der Substitution

$$\widehat{\mu} \to \widehat{\mu}\eta_1^{n_1} \dots \eta_r^{n_r}\xi^n$$

wo n beliebig ist. Da durch diese Substitution der $x_q\ dX$ ungeändert bleibt, folgt also, daß das Integral

$$\int_{X=-\infty}^{+\infty} F(u, \widehat{\mu}, x_q)dX$$

aus (21) in der Form:

$$\sum_{(n)} \int_{-\frac{1}{2}+n_1}^{+\frac{1}{2}+n_1} \cdots \int_{-\frac{1}{2}+n_r}^{+\frac{1}{2}+n_r} F(u, \widehat{\mu}, x_q)dx_1 \dots dx_r$$

geschrieben, wo (n) alle Systeme ganzer Zahlen $(n_1, \dots, n_r)$ durchläuft, gleich ist der Summe

$$\sum_{\eta'} \int_{-\frac{1}{2}}^{+\frac{1}{2}} \cdots \int F(u, \widehat{\mu}\eta', x_q)dx_1 \dots dx_r,$$

wo

$$\eta' = \eta_1^{n_1} \dots \eta_r^{n_r}$$

alle in dieser Form darstellbaren Strahleinheiten durchläuft, oder wegen der Invarianz von F gemäß (23) gleich

$$\frac{1}{w(f)} \sum_{\eta} \int_{-\frac{1}{2}}^{+\frac{1}{2}} \cdots \int F(u, \widehat{\mu}\eta, x_q)dx_1 \dots dx_r, \tag{24}$$

wo jetzt η *alle* (auch die nur um Strahleinheitswurzeln unterschiedenen) Strahleinheiten

$$\eta = \eta_1^{n_1} \dots \eta_r^{n_r}\xi^n$$

durchläuft. In (24) darf nun Summation und Integration vertauscht werden. Denn die Summe

$$\chi(\widehat{\mu}) \sum_{\eta} F(u, \widehat{\mu}\eta, x_q) \tag{25}$$

ist ein Bestandteil der reellen Summe

$$\sum_{\widehat{\mu}|\mathfrak{K}} F(u,\widehat{\mu},x_q)\chi(\widehat{\mu}) = e^{\sum_{q=1}^{r} x_q b_q(\lambda)}\vartheta(t,\mathfrak{K},\lambda,\widehat{\varphi}\widehat{\delta})$$

wo $\widehat{\mu}$ alle idealen Zahlen einer Klasse $\mathfrak{K}$ durchläuft, (nämlich der Klasse des gerade vorliegenden $\widehat{\mu}$). Der Faktor $e^{\sum_{1}^{r} x_q b_q(\lambda)}$ hat nach (16) dem Betrage nach eine von den x_q unabhängige obere Schranke, wenn $|x_q| \leqq \frac{1}{2}$, wie es unserer Integration entspricht, und die Thetareihe

ist nach Satz 36 für alle $t > \varepsilon > 0$ gleichmäßig konvergent, also bei festem $u > 0$ auch für alle $|x_q| \leqq \frac{1}{2}$ gleichmäßig konvergent, also auch unsere Summe (25), womit die Vertauschung von Summation und Integration in (24) für jedes $u > 0$ als zulässig erkannt ist. (Der Punkt $u = 0$ ist nur für die spätere Integration $\int_{u=0}^{\infty}$ kritisch und wird dann zu untersuchen sein). Wir erhalten somit aus (24) in der schon früher angewandten Bezeichnung:

$$\int_{X=-\infty}^{+\infty} F(u,\widehat{\mu},x_q)dX = \frac{1}{w(f)}\int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \sum_{\eta} F(u,\eta\widehat{\mu},x_q)dX \tag{26}$$

Wir haben nunmehr auch noch die übrigen Einheiten des Körpers heranzuziehen. Während wir bisher den Bestandteil $\chi(\widehat{\mu})$ von $\lambda\big((\widehat{\mu})\big)$ noch nicht mit in die Betrachtung hineinzogen, muß dies nunmehr geschehen, da zwar

$$\chi(\eta\widehat{\mu}) = \chi(\widehat{\mu}) \tag{27}$$

für Strahleinheiten η ist, aber nicht mehr für beliebige Körpereinheiten. Wir schreiben daher unter Benutzung von (27) das bisher erhaltene Resultat (21), (26) in der Form:

$$\left\{\begin{array}{c} \gamma(\lambda)\Gamma(s,\lambda)\mathsf{A}^s \frac{\lambda\left((\widehat{\mu})\right)}{|N(\widehat{\mu})|^s}\overline{\lambda}\left(\sqrt{|\widehat{\varphi}\widehat{\delta}|}\right) \\ = 2^{r_1-1}n\frac{R(f)}{w(f)}\int_{u=0}^{\infty}\int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \sum_{\eta} F(u,\eta\widehat{\mu},x_q)\chi(\eta\widehat{\mu})u^{\frac{ns}{2}+\frac{1}{2}\sum_{1}^{n}a_p}\frac{du}{u}dX, \end{array}\right. \tag{28}$$

121 II

und suche, um auf die Thetareihe zu kommen, unter dem Integral eine $\sum_{\varepsilon}$ über *alle* Körpereinheiten, also über *alle* assoziierten zu $\widehat{\mu}$ zu bekommen.

Nun haben die Strahleinheiten η in Bezug auf die Körpereinheiten ε einen endlichen Index $e(f)$, da ja die Gruppe der Körpereinheiten eine endliche Basis hat. Sei $\varepsilon_1, \ldots, \varepsilon_f$ ein Repräsentantensystem für die Faktorgruppe der Strahleinheiten in Bezug auf die Körpereinheiten, sodaß sich jede Körpereinheit ε eindeutig darstellen läßt in der Form:

$$\varepsilon = \varepsilon_i \eta\,; \qquad \big(\eta \text{ Strahleinheit, } i = 1, 2, \ldots\, e(f)\big).$$

Wegen $\lambda\big((\varepsilon_i)\big) = 1$, $|N(\varepsilon_i)| = 1$ ist dann

$$\frac{\lambda\big((\widehat{\mu})\big)}{|N(\widehat{\mu})|^s} = \frac{1}{e(f)} \sum_{i=1}^{e(f)} \frac{\lambda\big((\varepsilon_i \widehat{\mu})\big)}{|N(\varepsilon_i \widehat{\mu})|^s}.$$

Somit folgt aus (28):

$$(29) \qquad \left\{ \begin{array}{c} \gamma(\lambda)\Gamma(s,\lambda)\mathsf{A}^s \frac{\lambda\big((\widehat{\mu})\big)}{|N(\widehat{\mu})|^s} \overline{\lambda}\big(\sqrt{|\widehat{\varphi}\widehat{\delta}|}\big) \\ = M(f) \int\limits_{u=0}^{\infty} \int\limits_{X=-\frac{1}{2}}^{+\frac{1}{2}} \sum_{\varepsilon} F(u, \varepsilon\widehat{\mu}, x_q) \chi(\varepsilon\widehat{\mu}) u^{\frac{ns}{2} + \frac{1}{2}\sum_1^n a_p} \frac{du}{u} dX, \end{array} \right.$$

wo ε alle Körpereinheiten durchläuft und

$$(30) \qquad M(f) = \frac{2^{r_1 - 1} n R(f)}{e(f) w(f)}$$

gesetzt ist. Denn die unter dem Integral entstehende Summe

$$\sum_{i=1}^{e(f)} \sum_{\eta} F(u, \eta\varepsilon_i\widehat{\mu}, x_q) \chi(\eta\varepsilon_i\widehat{\mu})$$

122 II

ist ja nach Bestimmung der ε_i gerade gleich

$$\sum_{\varepsilon} F(u, \varepsilon\widehat{\mu}, x_q) \chi(\varepsilon\widehat{\mu})$$

erstreckt über alle Körpereinheiten.

In (29) haben wir nunmehr den Baustein für den Aufbau von $L(s,\lambda)$ so transformiert, daß bei Ausführung der Summation über alle ganzen Ideale $(\widehat{\mu}) \neq 0$ einer Klasse $\mathfrak{K}$ rechts gerade eine Summe über alle ganzen Zahlen $\widehat{\mu} \neq 0$ der Klasse $\mathfrak{K}$, und somit im wesentlichen die Thetareihe entsteht. Denn nach dam Schluß von Satz 10, S. 29▸ durchläuft der Ausdruck $\varepsilon\widehat{\mu}$ gerade alle ganzen Zahlen $\neq 0$ aus $\mathfrak{K}$, jede einmal, wenn $(\widehat{\mu})$ alle nicht assoziierten idealen Zahlen aus $\mathfrak{K}$ durchläuft und ε alle Körpereinheiten. Wir erhalten somit aus (29), wenn der Akzent am Summenzeichen stets den Ausschluß von $\widehat{\mu} = 0$ bedeutet:

$$(31)\qquad \left\{\begin{array}{c} \gamma(\lambda)\cdot\Gamma(s,\lambda)\cdot \mathsf{A}^s \cdot L(s,\lambda,\mathfrak{K})\cdot\overline{\lambda}\big(\sqrt{|\widehat{\varphi}\widehat{\delta}|}\big) \\ = M(f)\int\limits_{u=0}^{\infty}\int\limits_{X=-\frac{1}{2}}^{+\frac{1}{2}}\sum_{\widehat{\mu}|\mathfrak{K}}{}' F(u,\widehat{\mu},x_q)\chi(\widehat{\mu})u^{\frac{ns}{2}+\frac{1}{2}\sum\limits_1^n a_p}\frac{du}{u}dX, \end{array}\right.$$

wobei gesetzt ist:

$$(32)\qquad L(s,\lambda,\mathfrak{K}) = \sum_{(\widehat{\mu})|\mathfrak{K}}{}' \frac{\lambda\big((\widehat{\mu})\big)}{|N(\widehat{\mu})|^s},$$

sodaß ist:

$$(33)\qquad L(s,\lambda) = \sum_{\mathfrak{K}} L(s,\lambda,\mathfrak{K}).$$

Um die Richtigkeit von (31) einzusehen, muß aber noch die Berechtigung der ausgeführten Vertauschung von $\sum\limits_{(\widehat{\mu})}{}'$ mit den Integrationen nachgewiesen werden, also gezeigt werden, daß die $\sum\limits_{\widehat{\mu}|\mathfrak{K}}{}'$ unter dem Integral in (31) im Integrationsbereich gleichmäßig konvergiert. Die gleichmäßige Konvergenz dieser Summe für alle $u > \varepsilon$, $|x_q| \leqq \frac{1}{2}$ wurde schon oben S. 119▸/120▸ gezeigt. Für die Berechtigung der Summations– und Integrationsvertauschung bleibt also noch nachzuweisen, daß in $u = 0$, und wegen des Faktors $u^{\frac{ns}{2}+\frac{1}{2}\sum\limits_1^n a_p}$ auch, daß in $u = \infty$ hereinintegriert werden darf.

Nun ist nach Satz 36 für irgendwelche $t_p \to 0$ was wegen $|x_q| \leqq \frac{1}{2}$ nach (13) mit $u \to 0$ gleichbedeutend ist:

$$\vartheta(t, \mathfrak{K}, \lambda, \widehat{\varphi\delta}) = O\left(\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}\right).$$

Da nach (20) der Integrand in (31) gleich

$$\vartheta_0(t, \mathfrak{K}, \lambda, \widehat{\varphi\delta}) e^{\sum_{q=1}^{r} x_q b_q(\lambda)} u^{\frac{ns}{2}+\frac{1}{2}\sum_1^n a_p} \cdot \frac{1}{u}$$

ist, wo ϑ_0 von jetzt an die Thetareihe aus §5 ohne das ev. Glied mit $\widehat{\mu} = 0$ bedeutet, folgt also für unseren Integranden die Abschätzung (das Glied mit $\widehat{\mu} = 0$ stört nicht):

$$O\left(\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}\right) \cdot O\left(u^{\frac{ns}{2}+\frac{1}{2}\sum_1^n a_p - 1}\right),$$

was nach (13) wegen $|x_q| \leqq \frac{1}{2}$ gleich

$$O\left(u^{-\frac{n}{2}-\sum_1^n a_p+\frac{ns}{2}+\frac{1}{2}\sum_1^n a_p - 1}\right) = O\left(u^{\frac{n}{2}(s-1)-\frac{1}{2}\sum_1^n a_p - 1}\right)$$

ist. Für hinreichend großes $\Re(s)$ strebt also der Integrand für $u \to 0$ sogar zu Null, sodaß für solche s in Null herein integriert werden darf, was für uns genügt.

Für $u \to \infty$ ist nach Satz 36 unser Integrand von kleinerer Ordnung als jedes Potenzprodukt der t_p, also sicher $o\left(\frac{1}{u}\right)$, weil $u^{\frac{ns}{2}+\frac{1}{2}\sum_1^n a_p}$ einem solchen Potenzprodukt der t_p wegen $|x_q| \leqq \frac{1}{2}$ äquivalent ist. Daher darf auch in $u = \infty$ hineinintegriert werden.

Damit ist die Richtigkeit von (31) bewiesen, was wir jetzt unter Einführung der ϑ–Reihe so schreiben:

$$(34) \quad \begin{cases} \overline{\lambda}(\sqrt{|\widehat{\varphi\delta}|})\xi(s, \lambda, \mathfrak{K}) \\ = M(f) \int_{u=0}^{\infty} \int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta_0(t; \mathfrak{K}, \lambda, \widehat{\varphi\delta}) \cdot e^{\sum_{q=1}^{r} x_q b_q(\lambda)} \cdot u^{\frac{ns}{2}+\frac{1}{2}\sum_1^n a_p} \frac{du}{u} dX, \end{cases}$$

wobei gesetzt ist:

$$\xi(s,\lambda,\mathfrak{K}) = \gamma(\lambda)\cdot\Gamma(s,\lambda)\cdot \mathsf{A}^s\cdot L(s,\lambda,\mathfrak{K}), \tag{35}$$

sodaß wegen (33)

$$\xi(s,\lambda) = \sum_{\mathfrak{K}} \xi(s,\lambda,\mathfrak{K}) = \gamma(\lambda)\cdot\Gamma(s,\lambda)\cdot \mathsf{A}^s\cdot L(s,\lambda) \tag{36}$$

ist.

(34) führt nun in Analogie zu dem Riemannschen Beweise bei $\zeta(s)$ zur Funktionalgleichung der $\xi(s,\lambda,\mathfrak{K})$ und damit nach (36) auch der $\xi(s,\lambda)$ und $L(s,\lambda)$.

125 II

Es sind dabei 2 Fälle zu unterscheiden, je nachdem in der Thetareihe das $\widehat{\mu} = 0$ entsprechende Glied herausfällt, oder nicht. Aus dem Anblick der Thetareihe in Satz 34 folgt unmittelbar, das für $f \neq 1$ wegen $\chi(0) = 0$ jenes Glied herausfällt; für $f = 1$ darf nicht so geschlossen werden, weil hier auf Grund der Festsetzung von S. 62▸ keine zu 1 nicht primen Zahlen, also auch keine $\widehat{\mu}$ mit $\chi(\widehat{\mu}) = 0$ existieren. χ ist dann vielmehr ein nur von der absoluten Klasse von $\widehat{\mu}$ abhängiger Klassencharakter $\big($von $\mathfrak{Z}(1)\big)$, der für alle Glieder der Thetareihe denselben Wert $\chi(\mathfrak{K})$ hat, und als gemeinsamer Faktor vorwegtritt. In diesem Falle $f = 1$ fällt jedoch das Glied mit $\widehat{\mu} = 0$ sicher dann heraus, wenn nicht alle $a_p = 0$ sind, weil ja dann der Faktor $\prod_{p=1}^{n}\left(\frac{\widehat{\mu}^{(p)}}{\sqrt{|\widehat{\varphi}^{(p)}\widehat{\delta}^{(p)}|}}\right)^{a_p}$ für $\widehat{\mu} = 0$ den Wert 0 hat.

Es kann somit jenes Glied überhaupt nur auftreten, wenn $f = 1$ und alle $a_p = 0$ sind, und hat dann den Wert $\chi(\mathfrak{K})$, wobei χ der in $\lambda\big((\widehat{\mu})\big)$ steckende, in diesem Falle einen Charakter von $\mathfrak{Z}(1)$ darstellende, Charakter der Klasse $\mathfrak{K}$ ist. Ich zeige nun weiter, daß dieses Glied $\chi(\mathfrak{K})$ der Thetareihe in unserem Integral (34) unbeschadet der Richtigkeit von (34) mit aufgenommen werden darf, wenn nicht auch noch alle m_q aus $\lambda\big((\widehat{\mu})\big)$ verschwinden. Für den vorliegenden

126 II

Fall $f = 1$ und alle $a_p = 0$ wird nämlich nach (16):

$$b_q(\lambda) = -2\pi i m_q$$

also

$$\int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \chi(\mathfrak{K}) e^{\sum_{q=1}^{r} x_q b_q(\lambda)} dX$$
$$= \chi(\mathfrak{K}) \int_{-\frac{1}{2}}^{+\frac{1}{2}} \cdots \int e^{-2\pi i \sum x_q m_q} dx_1 \ldots dx_r$$

Nun ist

$$\int_{-\frac{1}{2}}^{+\frac{1}{2}} e^{-2\pi i m x} dx = \begin{cases} 1 & \text{für} \quad m = 0 \\ 0 & \text{"} \quad m \neq 0, \end{cases}$$

sodaß obiges Integral nur dann nicht verschwindet und den Wert $\chi(\mathfrak{K})$ hat, wenn alle $m_q = 0$ sind.

Wir haben also folgendes:

Wenn nicht gleichzeitig $f = 1$ und alle $a_p, m_q = 0$, darf in (34) unbeschadet der Richtigkeit dieser Gleichung ϑ statt ϑ_0 geschrieben werden, da entweder ϑ mit ϑ_0 identisch, oder doch das überflüssige Glied von ϑ durch die Integration von selbst herausfällt.

Nur wenn $f = 1$ und alle $a_p, m_q = 0$ sind, darf nicht so verfahren werden. Dann ist vielmehr bei Einführung von ϑ statt ϑ_0 dafür rechts in (34) $\vartheta - \chi(\mathfrak{K})$ zu schreiben. Der Charakter $\lambda\big((\widehat{\mu})\big)$ reduziert sich in diesem Falle, wegen $\lambda(\widehat{\mu}) \equiv 1$, $v(\widehat{\mu}) \equiv 1$ auf

$$\lambda\big((\widehat{\mu})\big) = \chi(\widehat{\mu}),$$

wo χ ein Klassencharakter von $\mathfrak{Z}(1)$ ist. Der Hauptcharakter,

dem die Dedekindsche ζ_k–Funktion entspricht, fällt ersichtlich auch mit unter diesen Fall.

Wir wenden uns nunmehr zu dem ersten Fall, daß also $\lambda\big((\widehat{\mu})\big)$ kein Klassencharakter von $\mathfrak{Z}(1)$ ist. Dann darf also für (34) auch geschrieben werden: (37)

$$\overline{\lambda}(\sqrt{|\widehat{\varphi}\widehat{\delta}|})\xi(s,\lambda,\mathfrak{K}) = M(f)\int_{u=0}^{\infty}\int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta(t,\mathfrak{K},\lambda,\widehat{\varphi}\widehat{\delta})\, u^{\sum_1^r x_q b_q(\lambda)}\, u^{\frac{ns}{2}+\frac{1}{2}\sum_1^n a_p}\frac{du}{u}dX.$$

Wir zerlegen nun das Integral $\int_{u=0}^{\infty}$ in $\int_{u=0}^{1}$ und $\int_{u=1}^{\infty}$. Das letztere Integral lassen wir stehen, das erstere formen wir mittels unserer Thetatransformationsformel um:

$$\vartheta(t,\mathfrak{K},\lambda,\widehat{\varphi}\widehat{\delta}) = \frac{\mathsf{W}(\lambda)}{\lambda\big(|\widehat{\varphi}\widehat{\delta}|\big)}\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}\vartheta\left(\frac{1}{t},\mathfrak{K}',\overline{\lambda},\widehat{\varphi}\widehat{\delta}\right),$$

wo $\mathfrak{K}\mathfrak{K}'$ die Klasse von $\widehat{\varphi}\widehat{\delta}$, $\overline{\lambda}$ der reziproke Charakter und $\mathsf{W}(\lambda)$ der Ausdruck von Satz 34 ist. Wir haben dann den im wesentlichen auftretenden Zusatzfaktor $\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p}$ zu berechnen, d. h. in den Variablen u, x_q auszudrücken. Nach (13) ist

$$\begin{aligned}\prod_{p=1}^{n} t_p^{-\frac{1}{2}-a_p} &= u^{-\frac{n}{2}-\sum_1^n a_p}\, e^{-2\sum_{p=1}^{n}\left(\frac{1}{2}+a_p\right)\sum_{q=1}^{r} x_q \log|\eta_q^{(p)}|}\\ &= u^{-\frac{n}{2}-\sum_1^n a_p}\, e^{-2\sum_{q=1}^{r} x_q\sum_{p=1}^{n}\left(\frac{1}{2}+a_p\right)\log|\eta_q^{(p)}|},\end{aligned}$$

was wegen $\sum_{p=1}^{n}\log|\eta_q^{(p)}| = 0$ übergeht in

$$u^{-\frac{n}{2}-\sum a_p}\, e^{-2\sum_{q=1}^{r} x_q\sum_{p=1}^{n} a_p\log|\eta_q^{(p)}|}$$

Diesen Zusatzfaktor vereinigen wir mit den gleichartigen Faktoren unter dem Integral (37) und erhalten so einerseits den Faktor

$$u^{\frac{n}{2}(s-1)-\frac{1}{2}\sum_1^n a_p}$$

andererseits den Faktor (s. (16)):

$$\begin{aligned} & e^{\sum\limits_{q=1}^{r} x_q \left\{ -2\pi i m_q - \sum\limits_{p=1}^{n} a_p \left(\log|\eta_q^{(p)}| - i\vartheta_q^{(p)} \right) \right\}} \\ = \quad & e^{-\sum\limits_{q=1}^{r} x_q \left\{ -2\pi i(-m_q) + \sum\limits_{p=1}^{n} a'_p \left(\log|\eta_q^{(p)}| + i\vartheta_q^{(p)} \right) \right\}} \end{aligned}$$

weil die Gesamtheit der $a_p \left(\log|\eta_q^{(p)}| - i\vartheta_q^{(p)} \right)$ für $p = 1, \ldots, n$ nach Satz 23, S. 54 mit der Gesamtheit der $a'_p \left(\log|\eta_q^{(p)}| + i\vartheta_q^{(p)} \right)$ identisch ist. Letzterer Faktor ist aber nach (16) und (17)

$$= e^{-\sum\limits_{q=1}^{r} x_q b_q(\overline{\lambda})}.$$

Wir erhalten somit für unser erstes Integral $\int\limits_{u=0}^{1}$ aus (37) den Wert:

$$(38) \quad \mathsf{W}(\lambda)\overline{\lambda}(|\widehat{\varphi}\widehat{\delta}|) \int\limits_{u=0}^{1} \int\limits_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta\left(\frac{1}{t}, \mathfrak{K}, \overline{\lambda}, \widehat{\varphi}\widehat{\delta}\right) e^{-\sum\limits_{q=1}^{r} x_q b_q(\overline{\lambda})} u^{\frac{n}{2}(s-1) - \frac{1}{2}\sum\limits_{1}^{n} a_p} \frac{du}{u} dX$$

während das zweite mit

$$(39) \qquad g(s, \lambda, \mathfrak{K}) = \int\limits_{u=1}^{\infty} \int\limits_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta\left(t, \mathfrak{K}, \lambda, \widehat{\varphi}\widehat{\delta}\right) e^{\sum\limits_{q=1}^{r} x_q b_q(\lambda)} u^{\frac{ns}{2} + \frac{1}{2}\sum\limits_{1}^{n} a_p} \frac{du}{u} dX$$

bezeichnet werden soll. Nunmehr führen wir in (38) die Substitution $t \to \frac{1}{t}$ aus, die nach (13a) zur Folge hat:

$$u \to \frac{1}{u}; \qquad x_q \to -x_q.$$

Dadurch geht der Integrand in (38) über in

$$\vartheta(t, \mathfrak{K}', \overline{\lambda}, \widehat{\varphi}\widehat{\delta}) e^{\sum\limits_{q=1}^{r} x_q b_q(\overline{\lambda})} u^{\frac{n(1-s)}{2} + \frac{1}{2}\sum\limits_{1}^{n} a'_p}$$

weil ja statt $\sum_1^n a_p$ auch $\sum_1^n a'_p$ geschrieben werden darf. $\int_0^1 \frac{du}{u}$ geht in $-\int_\infty^1 \frac{du}{u} = \int_1^\infty \frac{du}{u}$ über und ähnlich jedes Integral $\int_{-\frac12}^{+\frac12} dx_q$ in $-\int_{+\frac12}^{-\frac12} dx_q = \int_{-\frac12}^{+\frac12} dx_q$, somit (38) in

$$(40)\quad \left\{ \mathsf{W}(\lambda)\overline{\lambda}(|\widehat{\varphi\delta}|) \int_{u=1}^{\infty} \int_{X=-\frac12}^{+\frac12} \vartheta\left(t, \mathfrak{K}', \overline{\lambda}, \widehat{\varphi\delta}\right) e^{\sum_{q=1}^{r} x_q b_q(\overline{\lambda})} u^{\frac{n(1-s)}{2} + \frac12 \sum_1^n a'_p} \frac{du}{u} dX \right.$$
$$\left. = \mathsf{W}(\lambda)\overline{\lambda}(|\widehat{\varphi\delta}|) g(1-s, \overline{\lambda}, \mathfrak{K}'). \right.$$

Nach (37), (39), (40) wird also:

$$(41)\quad \xi(s, \lambda, \mathfrak{K}) = M(f)\left[\lambda(\sqrt{|\widehat{\varphi\delta}|}) g(s, \lambda, \mathfrak{K}) + \mathsf{W}(\lambda)\overline{\lambda}(\sqrt{|\widehat{\varphi\delta}|}) g(1-s, \overline{\lambda}, \mathfrak{K}')\right].$$

Diese Gleichung (41) ist (s. S. 124 oben) unter der Voraussetzung eines hinreichend großen $\Re(s)$ hergeleitet. Nun folgt aber aus (39), daß $g(s, \lambda, \mathfrak{K})$ eine *ganze Funktion* von s ist. Denn das Integral in (34) konvergiert, da nunmehr der kritische Punkt $u = 0$ wegfällt, nach einer analogen Bemerkung, wie S. 124 oben für jedes endliche komplexe s. Es ist folglich auch $g(s, \overline{\lambda}, \mathfrak{K}')$ ganz und somit $\xi(s, \lambda, \mathfrak{K})$ eine ganze Funktion von s, daher auch nach (35), (36) $\xi(s, \lambda)$, $L(s, \lambda, \mathfrak{K})$, $L(s, \lambda)$, weil ja die reziproke Γ–Funktion bekanntlich ganz ist. (41) *gilt somit für alle* s.

Aus (41) ergibt sich ferner

$$(42)\quad \xi(1-s, \overline{\lambda}, \mathfrak{K}') = M(f)\left[\overline{\lambda}(\sqrt{|\widehat{\varphi\delta}|}) g(1-s, \overline{\lambda}, \mathfrak{K}') + \mathsf{W}(\overline{\lambda})\lambda(\sqrt{|\widehat{\varphi\delta}|}) g(s, \lambda, \mathfrak{K})\right]$$

Ist nun $\vartheta(t; \mathfrak{K}, \lambda, \widehat{\varphi\delta})$ nicht identisch Null, so ist nach S. 95

$$\mathsf{W}(\lambda)\mathsf{W}(\overline{\lambda}) = 1,$$

also nach (41), (42):

$$(43)\qquad \xi(1-s, \overline{\lambda}, \mathfrak{K}') = \mathsf{W}(\overline{\lambda})\xi(s, \lambda, \mathfrak{K}).$$

Sollte jedoch die Thetafunktion $\vartheta(t, \mathfrak{K}, \lambda, \widehat{\varphi\delta})$ identisch verschwinden, so folgt aus der Transformationsformel:

$$\vartheta(t, \mathfrak{K}', \overline{\lambda}, \widehat{\varphi\delta}) = \frac{\mathsf{W}(\overline{\lambda})}{\overline{\lambda}(|\widehat{\varphi\delta}|)} \prod_{p=1}^{n} t_p^{-\frac{1}{2}-a'_p} \vartheta\left(\frac{1}{t}, \mathfrak{K}, \lambda, \widehat{\varphi\delta}\right)$$

daß auch $\vartheta(t, \mathfrak{K}', \overline{\lambda}, \widehat{\varphi\delta})$ identisch verschwindet, somit auch $g(s, \lambda, \mathfrak{K})$ und $g(1-s, \overline{\lambda}, \mathfrak{K}')$ nach (39) und (40), also auch $\xi(s, \lambda, \mathfrak{K})$ und $\xi(1-s, \overline{\lambda}, \mathfrak{K}')$ nach (41), (42) und dann ist (43) identisch erfüllt.

Summieren wir (43) über alle $\mathfrak{K}$, so durchläuft auch $\mathfrak{K}'$ alle Klassen und es folgt nach (36):

$$\xi(1-s, \overline{\lambda}) = \mathsf{W}(\overline{\lambda})\xi(s, \lambda), \tag{44}$$

was mit (36) zusammen die gesuchte Funktionalgleichung von $L(s, \lambda)$ liefert. Aus (44) folgt noch, weil $L(s, \lambda)$ wegen der Produktdarstellung nicht identisch verschwindet, also auch $\xi(s, \lambda)$ nicht, durch zweimalige Anwendung $\mathsf{W}(\lambda)\mathsf{W}(\overline{\lambda}) = 1$, d. h. wie S. 95▶ ff.

$$|\mathsf{W}(\lambda)| = 1\,; \qquad \mathsf{W}(\overline{\lambda}) = \overline{\mathsf{W}(\lambda)} \neq 0$$

unabhängig von dem beim Beweis von Satz 35 benutzten Nichtverschwinden der ϑ–Reihen.

131 II

Zusammenfassend haben wir:

Satz 38 Ist $\lambda\big((\widehat{\mu})\big)$ ein solcher eigentlicher Größencharakter mod f, der nicht schon ein Klassencharakter von $\mathfrak{Z}(1)$ (der absoluten Klassengruppe) ist, so definiert die für $\Re(s) > 1$ absolut konvergente Reihe

$$L(s, \lambda) = \sum_{(\widehat{\mu})}{}' \frac{\lambda\big((\widehat{\mu})\big)}{|N(\widehat{\mu})|^s} = \prod_{(\widehat{\pi})} \frac{1}{1 - \frac{\lambda\left((\widehat{\pi})\right)}{|N(\widehat{\pi})|^s}}$$

eine ganze transzendente Funktion von s. Wird

$$\xi(s, \lambda) = \gamma(\lambda)\Gamma(s, \lambda)\mathsf{A}^s L(s, \lambda)$$

gesetzt, so ist auch $\xi(s, \lambda)$ eine ganze transzendente Funktion von s und genügt der Funktionalgleichung:

$$\xi(s, \lambda) = \mathsf{W}(\lambda)\xi(1-s, \overline{\lambda}).$$

Dabei ist:

$$\begin{aligned}
\lambda\big((\widehat{\mu})\big) &= \lambda(\widehat{\mu})v(\widehat{\mu})\chi(\widehat{\mu}),\\
\gamma(\lambda) &= \lambda(\sqrt{e_p})\prod_{p=1}^{n}(\sqrt{e_p\pi})^{-a_p}, \quad \text{s. Anm. 1 a. S. 145}\\
\Gamma(s,\lambda) &= \prod_{p=1}^{r+1}\Gamma\Big\{\frac{e_p}{2}\left(s+\frac{a_p+a'_p}{2}\right)-\frac{1}{2}\sum_{q=1}^{r}e_p^{(q)}\cdot\\
&\quad\cdot\left(2\pi i m_q - i\sum_{k=1}^{n}a_k\vartheta_q^{(k)}\right)\Big\},\\
\mathsf{A} &= \sqrt{\frac{d\,N(f)}{2^{2r_2}\pi^n}},\\
\mathsf{W}(\lambda) &= \frac{(-i)^{\sum_1^n a_p}}{\sqrt{N(f)}}\lambda(\widehat{\varphi}\widehat{\delta})v(\widehat{\varphi}\widehat{\delta})\sum_{\widehat{\varrho}}\chi(\widehat{\varrho})e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)}.
\end{aligned}$$

$\mathsf{W}(\lambda)$ ist von der speziellen Wahl von $\widehat{\varphi}\widehat{\delta}$ unabhängig (Satz 31), genügt den Bedingungen:

$$\mathsf{W}(\lambda)\mathsf{W}(\overline{\lambda})=1\,,\qquad \mathsf{W}(\overline{\lambda})=\overline{\mathsf{W}(\lambda)}$$
$$\text{und}\qquad |\mathsf{W}(\lambda)|=1.$$

Wir haben nunmehr noch den zweiten Fall von S. 126 zu erledigen, wo $\lambda\big((\widehat{\mu})\big)=\chi(\widehat{\mu})$ ein Klassencharakter von $\mathfrak{Z}(1)$ ist, also $f=1$ und alle $m_q, a_p = 0$ sind. Dann werden die $b_q(\lambda)$ aus (16) sämtlich 0, $\widehat{\varphi}$ kann gleich 1 genommen werden und $\lambda(\widehat{\mu}), \overline{\lambda}(\widehat{\mu})$ sind identisch 1, ferner nach (30)

$$M(1)=\frac{2^{r_1-1}nR(1)}{e(1)w(1)}, \tag{45}$$

wo sich die Größen $R(1), e(1), w(1)$ nunmehr auf den Strahl aller total positiven Körperzahlen, also auf die Gruppe aller total positiven Körpereinheiten

beziehen, und nach (10), (11), (7):

$$(46)\qquad \begin{cases} \mathsf{A} = \sqrt{\frac{d}{2^{2r_2}\pi^n}}, \\ \gamma(\lambda) = 1, \\ \Gamma(s,\lambda) = \left(\Gamma(\frac{s}{2})\right)^{r_1} \left(\Gamma(s)\right)^{r_2}. \end{cases}$$

Die Formel (34), auf die sich das weitere aufzubauen hat, wird, wenn noch die Ausführungen von S. 125▸ berücksichtigt werden:

$$(47)\qquad \xi(s,\chi,\mathfrak{K}) = M(1) \int_{u=0}^{\infty} \int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \left(\vartheta(t;\mathfrak{K},\chi,\widehat{\delta}) - \chi(\mathfrak{K})\right) u^{\frac{ns}{2}} \frac{du}{u} dX,$$

wobei gesetzt ist:

$$(48)\qquad \xi(s,\chi,\mathfrak{K}) = \left(\Gamma\left(\frac{s}{2}\right)\right)^{r_1} \left(\Gamma(s)\right)^{r_2} \mathsf{A}^s L(x,\chi,\mathfrak{K}).$$

Wir zerlegen wieder in (47) das $\int_{u=0}^{\infty}$ in $\int_{u=0}^{1} + \int_{u=1}^{\infty}$. Das erstere Integral wird:

$$-\chi(\mathfrak{K}) \int_{u=0}^{1} u^{\frac{ns}{2}-1} du + \int_{u=0}^{1} \int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta(t;\mathfrak{K},\chi,\widehat{\delta}) u^{\frac{ns}{2}} \frac{du}{u} dX.$$

Diese Aufspaltung ist für das volle Integral $\int_{u=0}^{\infty}$ nicht möglich, weil $\int_{0}^{\infty} u^{\frac{ns}{2}-1} du$ für die auf $\Re(s) > 1$ (s. S. 123▸ unten) zu beschränkenden s im allgemeinen nicht konvergiert. Durch Auswertung des vorangetretenen Integrals[†] und Anwendung der Thetatransformationsformel geht dann unser obiger Ausdruck über in:

$$-\frac{\chi(\mathfrak{K})}{\frac{ns}{2}} + \mathsf{W}(\chi) \int_{u=0}^{1} \int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta\left(\frac{1}{t};\mathfrak{K}',\overline{\chi},\widehat{\delta}\right) \prod_{p=1}^{n} t_p^{-\frac{1}{2}} \cdot u^{\frac{ns}{2}} \frac{du}{u} dX.$$

[†]das sicher für $\Re(s) > 1$ konvergiert,

Das $\mathsf{W}(\chi)$ aus der Thetatransformationsformel berechnet sich hier nach Satz 34 zu:

$$\mathsf{W}(\chi) = C(\chi, \widehat{\delta}) = \sum_{\widehat{\varrho}} \chi(\widehat{\varrho}) e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\delta}}\right)},$$

wo $\widehat{\varrho}$ ein volles Restsystem der Klasse von $\widehat{\delta}$ mod 1 zu durchlaufen hat, das also aus einem beliebigen, ganzen Repräsentanten dieser Klasse besteht. Da dann $S\left(\frac{\widehat{\varrho}}{\widehat{\delta}}\right)$ eine ganze Zahl ist und χ absoluter Klassencharakter, wird

$$\mathsf{W}(\chi) = \chi(\mathfrak{d}).$$

$\mathfrak{K}$ und $\mathfrak{K}'$ hängen zusammen durch

$$\mathfrak{K}\mathfrak{K}' = \text{Klasse von } \mathfrak{d}. \tag{49}$$

Ferner wird

$$\prod_{p=1}^{n} t_p^{-\frac{1}{2}} = \big(N(t)\big)^{-\frac{1}{2}} = u^{-\frac{u}{2}}$$

nach (13a). Durch die Substitution $t \to \frac{1}{t}$, d. h. $u \to \frac{1}{u}$, $x_q \to -x_q$ geht dann genau wie oben S. 129 unser Integral über in

$$-\chi(\mathfrak{K}) \cdot \frac{1}{\frac{ns}{2}} + \chi(\mathfrak{d}) \int_{u=1}^{\infty} \int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \vartheta(t; \mathfrak{K}', \overline{\chi}, \widehat{\delta}) u^{\frac{n}{2}(1-s)} \frac{du}{u} dX.$$

Um dieses auf die gleiche Form, wie das verbleibende Integral $\int_{u=1}^{\infty}$ in (47):

$$g(s, \chi, \mathfrak{K}) = \int_{u=1}^{\infty} \int_{X=-\frac{1}{2}}^{+\frac{1}{2}} \big(\vartheta(t; \mathfrak{K}, \chi, \widehat{\delta}) - \chi(\mathfrak{K})\big) u^{\frac{ns}{2}} \frac{du}{u} dX \tag{50}$$

zu bringen, ist noch

$$\chi(\mathfrak{d}) \int_{u=1}^{\infty} \overline{\chi}(\mathfrak{K}') u^{\frac{n}{2}(1-s)-1} du$$

$$= -\chi(\mathfrak{d})\overline{\chi}(\mathfrak{K}') \frac{1}{\frac{n}{2}(1-s)} = -\chi(\mathfrak{K}) \frac{1}{\frac{n}{2}(1-s)}$$

(unter Verwendung von (49)) hinzuzufügen[‡] und dafür unter dem Integral $\overline{\chi}(\mathfrak{K}')$ von $\vartheta(t;\mathfrak{K}',\overline{\chi},\widehat{\delta})$ abzuziehen. Dann wird (47) zu:

$$\xi(s,\chi,\mathfrak{K}) = \chi(\mathfrak{K})\cdot\frac{2}{n}\cdot M(1)\frac{1}{s(s-1)} + M(1)\big[g(s,\chi,\mathfrak{K}) + \chi(\mathfrak{d})g(1-s,\overline{\chi},\mathfrak{K}')\big] \tag{51}$$

gültig für $\Re(s)>1$. Da aber nach (50) $g(s,\chi,\mathfrak{K})$ eine

ganze Funktion von s ist, weil ihre Integraldarstellung wegen des Fortfalls des kritischen Punktes 0 wie oben für alle komplexen s konvergiert, ist auch

$$\xi(s,\chi,\mathfrak{K}) - \chi(\mathfrak{K})\frac{2}{n}M(1)\frac{1}{s(s-1)}$$

ganz und (51) richtig für alle s. Der Faktor $\frac{2}{n}M(1)$ wird noch nach (45) zu:

$$M = \frac{2^{r_1}R(1)}{e(1)w(1)} \tag{52}$$

Aus (51) folgt

$$\xi(1-s,\overline{\chi},\mathfrak{K}') = \overline{\chi}(\mathfrak{K}')\frac{M}{s(s-1)} + M(1)\big[g(1-s,\overline{\chi},\mathfrak{K}') + \overline{\chi}(\mathfrak{d})g(s,\chi,\mathfrak{K})\big].$$

Multipliziert man dies mit $\chi(\mathfrak{d})$, so entsteht wegen

$$\chi(\mathfrak{d})\overline{\chi}(\mathfrak{K}') = \chi\left(\frac{\mathfrak{d}}{\mathfrak{K}'}\right) = \chi(\mathfrak{K})$$

rechts gerade $\xi(s,\chi,\mathfrak{K})$ nach (51). Es gilt also die Funktionalgleichung:

$$\xi(s,\chi,\mathfrak{K}) = \chi(\mathfrak{d})\xi(1-s,\overline{\chi},\mathfrak{K}'). \tag{53}$$

Für $\xi(s,\chi) = \sum_{\mathfrak{K}}\xi(s,\chi,\mathfrak{K})$ folgt hieraus ebenfalls

$$\xi(s,\chi) = \chi(\mathfrak{d})\xi(1-s,\mathfrak{K}') \tag{54}$$

[‡]das Integral konvergiert unter unserer Voraussetzung $\Re(s)>1$.

und daraus vermöge (36) die Funktionalgleichung für $L(s,\chi)$.

$\xi(s,\chi,\mathfrak{K})$ ist nach (51) meromorph mit den beiden Polen $s=0, s=1$. Daher haben auch $\xi(s,\chi), L(s,\chi)$

136 II

höchstens diese Pole, und zwar von der ersten Ordnung. Wir berechnen noch die Residuen. Zunächst ist jedes $L(s,\chi)$ regulär in $s=0$. Denn aus (36), was hier

$$L(s,\chi)=\mathsf{A}^{-s}\frac{1}{\left(\Gamma\left(\frac{s}{2}\right)\right)^{r_1}}\cdot\frac{1}{\left(\Gamma\left(s\right)\right)^{r_2}}\xi(s,\chi)$$

lautet folgt, weil $\Gamma(s)$ in $s=0$ von der ersten Ordnung unendlich wird, daß der Faktor vor $\xi(s,\chi)$ in $s=0$ von der r_1+r_2–ten, also mindestens von der 1. Ordnung Null wird, sodaß der Pol von $\xi(s,\chi)$ sich auf alle Fälle (falls überhaupt noch vorhanden, was nach dem sofort zu zeigenden nur für den Hauptcharakter eintritt) kompensiert.

Für $s=1$ hat $\xi(s,\chi,\mathfrak{K})$ das Residuum

$$\chi(\mathfrak{K})M,$$

also nach (48) $L(s,\chi,\mathfrak{K})$ das Residuum

$$\chi(\mathfrak{K})\frac{M}{\mathsf{A}}\frac{1}{\left(\Gamma\left(\frac{1}{2}\right)\right)^{r_1}}=\chi(\mathfrak{K})\frac{M}{\mathsf{A}}\frac{1}{\sqrt{\pi}^{\,r_1}},$$

also nach (46), (52)

$$=\chi(\mathfrak{K})\frac{2^{r_1+r_2}\pi^{r_2}R(1)}{\sqrt{d}w(1)e(1)}=\chi(\mathfrak{K})\cdot\kappa$$

Wegen $\sum\limits_{\mathfrak{K}}\chi(\mathfrak{K})=0$ oder h, je nachdem χ nicht der Hauptcharakter oder doch, ist also $L(s,\chi)$ $\big($und auch $\xi(s,\chi)\big)$ regulär bei $s=1$, wenn χ nicht der Hauptcharakter, sonst hat dort $L(s,\chi_0)=\zeta_k(s)$ einen Pol 1. Ordnung mit dem Residuum

137 II

$$h\kappa=h\frac{2^{r_1+r_2}\pi^{r_2}R(1)}{\sqrt{d}w(1)e(1)}.$$

der bekannte Ausdruck für $h\kappa$ lautet

$$h\kappa = h\frac{2^{r_1+r_2}\pi^{r_2}R}{\sqrt{d}w}$$

wo R und w sich auf den Strahl *aller* Körperzahlen (ohne Vorzeichenbedingung) bezieht. Man überlegt sich auch leicht gruppentheoretisch, daß der Index

$$e(1) = \frac{R(1)}{R} \qquad \text{oder} \qquad 2\frac{R(1)}{R}$$

ist, je nachdem k total imaginär oder nicht, was mit

$$w(1) = w \qquad \text{oder} \qquad \frac{1}{2}w$$

in denselben beiden Fällen auf den bekannten Ausdruck führt.

In Ergänzung zu Satz 38 haben wir nunmehr folgendes Resultat:

Satz 39. Ist $\chi(\widehat{\mu})$ ein Klassencharakter der absoluten Klassengruppe (Grad h), der nicht der Hauptcharakter ist, so definiert die für $\Re(s) > 1$ absolut konvergente Reihe

$$L(s,\chi) = \sum_{(\widehat{\mu})}{}' \frac{\chi(\widehat{\mu})}{|N(\widehat{\mu})|^s} = \prod_{(\widehat{\pi})} \frac{1}{1-\frac{\chi(\widehat{\pi})}{|N(\widehat{\pi})|^s}}$$

eine ganze transzendente Funktion von s.

138 II

Wird

$$\xi(s,\chi) = \left(\Gamma\left(\frac{s}{2}\right)\right)^{r_1}\left(\Gamma(s)\right)^{r_2}\mathsf{A}^s L(s,\chi)$$

gesetzt, so ist auch $\xi(s,\chi)$ eine ganze transzendente Funktion von s und genügt der Funktionalgleichung

$$\xi(s,\chi) = \chi(\mathfrak{d})\xi(1-s,\overline{\chi}).$$

Dabei ist $\mathfrak{d}$ die Differente des Körpers und

$$\mathsf{A} = \sqrt{d}\,2^{-r_2}\pi^{-\frac{n}{2}}.$$

Satz 40. Für den Hauptcharakter ist $L(s,\chi) = \zeta_k(s)$ die Dedekindsche ζ–Funktion:

$$\zeta_k(s) = \sum_{(\widehat{\mu})}{}' \frac{1}{|N(\widehat{\mu})|^s} = \prod_{(\widehat{\pi})} \frac{1}{1-\frac{1}{|N(\widehat{\pi})|^s}}.$$

$\zeta_k(s)$ ist für alle $s \neq 1$ regulär und hat bei $s = 1$ einen Pol 1. Ordnung mit dem Residuum

$$h\kappa = h\frac{2^{r_1+r_2}\pi^{r_2}R}{\sqrt{d}w}.$$

Wird

$$\xi(s) = \left(\Gamma\left(\frac{s}{2}\right)\right)^{r_1}\left(\Gamma(s)\right)^{r_2}\mathsf{A}^s\zeta_k(s)$$

gesetzt, so ist auch $\xi(s)$ bis auf einen Pol 1. Ordnung in $s = 1$ regulär und genügt der Funktionalgleichung

$$\xi(s) = \xi(1-s).$$

Zusatz. Ersichtlich sind die Funktionalgleichungen von Satz 39, 40 als Spezialfälle in der allgemeinen Funktionalgleichung von Satz 38 enthalten.

2.7 §7 Anwendung auf die Theorie relativ–abelscher Körper.

139 II

§7. Anwendung der Funktionalgleichung der L–Reihen mit Klassencharakteren auf die Theorie des relativ Abelschen Körpers.

A. Die Relativdiskriminante und die Zerlegung ihrer Primteiler.

Sei wie bisher k ein beliebiger algebraischer Körper vom Grade $n = r_1 + 2r_2$ mit r_1 reellen und r_2 Paaren komplexer konjugierter, ferner K ein relativ–Abelscher Körper vom Grade h über k, der Klassenkörper nach der Klassengruppe H in k vom Index h und Führer $\mathfrak{F}$ ist. χ bedeute die sämtlichen Charaktere nach H, d. h. der Gruppe der Nebengruppen zu H. Im Sinne von §3 sind diese Charaktere χ eine gewissse Untergruppe X der dort mit $\chi_0\big((\widehat{\alpha})\big)$ bezeichneten Charaktere der Gruppe $\mathfrak{I}_0(\mathfrak{F})$, da H eine Untergruppe von $\mathfrak{I}_0(\mathfrak{F})$ ist; die Charakterengruppe X der χ besteht offenbar aus der Gesamtheit der $\chi_0\big((\widehat{\alpha})\big)$, die für die Ideale aus H den Wert 1 haben. Denn erstens muß jeder Charakter χ nach H für die Ideale aus H den Wert 1 haben, zweitens hat jeder Charakter $\chi_0\big((\widehat{\alpha})\big)$, der für H den Wert 1 hat, für alle Ideale einer Nebengruppe zu H den gleichen Wert, ist also

140 II

Charakter nach H. Wir verstehen im folgenden unter den Charakteren χ stets die zugeordneten *eigentlichen* Charaktere. $f(\chi)$ seien die Führer der χ, sodaß jedes $f(\chi)$ ein Teiler von $\mathfrak{F}$ ist (Satz 26). Es gilt aber genauer:

Satz 41. Der Führer $\mathfrak{F}$ von H ist das kleinste gemeinsame Vielfache der Führer $f(\chi)$ aller Charaktere χ nach H.

Beweis: Daß $\mathfrak{F}$ ein gemeinsames Vielfaches aller $f(\chi)$ ist, wurde soeben gezeigt. Umgekehrt ist aber die Klassengruppe H nach dem kleinsten gemeinsamen Vielfachen $\mathfrak{F}_0$ aller $f(\chi)$ erklärbar, nämlich:

H = Gesamtheit der Strahlklassen $\mathfrak{k}$ nach dem Strahl „$\equiv 1 \bmod \mathfrak{F}_0$, total positiv“, für die

$$\chi(\mathfrak{k}) = 1$$

für alle χ gilt.

Ist nämlich $\mathfrak{a}$ ein zu H gehöriges, also zu $\mathfrak{F}$ und somit auch zu dem Teiler $\mathfrak{F}_0$ von $\mathfrak{F}$ primes Ideal, so ist nach Definition der χ für alle χ: $\chi(\mathfrak{a}) = 1$, und gehört ein zu $\mathfrak{F}$ primes Ideal $\mathfrak{a}$ nicht zu H, so muß mindestens einer der Charaktere χ von X von 1 verschieden sein, weil eben X die Charakterengruppe nach H ist. H besteht also aus der Gesamtheit der zu $\mathfrak{F}$ primen Ideale, für die $\chi(\mathfrak{a}) = 1$ für alle χ aus X ist. Jede einzelne Forderung $\chi(\mathfrak{a}) = 1$ ist mit gewissen Kongruenzforderungen* mod $f(\chi)$ identisch, also die

141 II

Gesamtheit der Forderungen $\chi(\mathfrak{a}) = 1$ mit gewissen Kongruenzbedingungen mod $\mathfrak{F}_0$, d. h. H läßt sich tatsächlich in der oben angegebenen Weise nach dem Modul $\mathfrak{F}_0$ erklären. Daher kann $\mathfrak{F}$ kein echtes Multiplum des ebenfalls möglichen Moduls $\mathfrak{F}_0$ für H sein und es folgt:

$$\mathfrak{F}_0 = \mathfrak{F}, \qquad \text{w. z. b. w.}$$

Die Quelle für die zu entwickelnden Anwendungen der Funktionalgleichung bildet die Aufspaltung der Dedekindschen ζ–Funktion von K:

$$\zeta_K(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \mathsf{N}\mathfrak{P}^{-s}},$$

wo $\mathfrak{P}$ alle Primideale von K durchläuft und N die Norm in K zum Unterschied von der Norm N in k bezeichnet.

Für die zu $\mathfrak{F}$ primen $\mathfrak{p}$ aus k und die ihnen entsprechenden Primteiler $\mathfrak{P}$ aus K ergibt sich die Möglichkeit einer solchen Aufspaltung leicht aus dem Zerlegungssatz für den Klassenkörper.

Sei $\mathfrak{p}$ prim zu $\mathfrak{F}$ und zerfalle in K so:

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_g\,; \qquad (\text{Grad } f;\ gf = h),$$

*und Signaturforderungen, die aber an keinen Modul gebunden sind.

also

$$\mathsf{N}\mathfrak{P}_i = N\mathfrak{p}^f.$$

Dann wird der Beitrag von $\mathfrak{p}$ zu $\zeta_K(s)$:

$$\left(\frac{1}{1-N\mathfrak{p}^{-fs}}\right)^g = \left(\frac{1}{\prod\limits_{\nu=0}^{f-1}(1-\varepsilon^\nu N\mathfrak{p}^{-s})}\right)^g = \prod_{\nu=0}^{f-1}\left(\frac{1}{1-\varepsilon^\nu N\mathfrak{p}^{-s}}\right)^g,$$

wo ε eine primitive f–te Einheitswurzel ist.

142 II

Nach dem Zerlegungssatz ist ferner f der kleinste Exponent, sodaß $\mathfrak{p}^f$ zu H gehört. Ist $\mathfrak{K}$ die Klasse nach H von $\mathfrak{p}$, so definiert also $\mathfrak{K}$ eine zyklische Untergruppe vom Grade f: $1, \mathfrak{K}, \ldots, \mathfrak{K}^{f-1}$, also Index $\frac{h}{f} = g$. Es gibt also genau g Charaktere χ (die Charaktere der zugehörigen Faktorgruppe), sodaß diese g Charaktere für $1, \mathfrak{K}, \ldots\ \mathfrak{K}^{f-1}$ den Wert 1 haben. Alle h Charaktere zerfallen also in f Nebengruppen, derart, daß immer für eine ganze Nebengruppe alle $\chi(\mathfrak{K}^\nu)$ bei festem ν gleich sind. Wäre ferner für zwei Charaktere χ_1, χ_2 aus zwei solchen Nebengruppen $\chi_1(\mathfrak{K}) = \chi_2(\mathfrak{K})$ so folgte $\frac{\chi_1}{\chi_2}(\mathfrak{K}) = 1$ also $\frac{\chi_1}{\chi_2}(\mathfrak{K}^\nu) = 1$, also $\frac{\chi_1}{\chi_2}$ zu der oben genannten Untergruppe gehörig, und somit χ_1, χ_2 zur gleichen Nebengruppe. $\chi(\mathfrak{K})$ nimmt also, wenn χ alle Charaktere durchläuft jeden seiner f Werte genau g mal an und diese f Werte sind sämtlich verschieden, also wegen $\chi(\mathfrak{K}^f) = \big(\chi(\mathfrak{K})\big)^f = 1$ die f Potenzen $1, \varepsilon, \ldots\ \varepsilon^{f-1}$. Es kann daher der obige Beitrag von $\mathfrak{p}$ zu $\zeta_K(s)$ in der Form

$$\prod_\chi \frac{1}{1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}}$$

geschrieben werden. Er ist also gleich dem Produkt der Beiträge von $\mathfrak{p}$ zu den h L–Reihen $L(s,\chi)$, die mit den h Charakteren χ nach H gebildet sind.

Dies gilt für alle zu $\mathfrak{F}$ primen $\mathfrak{p}$. Bezeichnet also $L(s,\chi)$ die *eigentlichen* L–Reihen, so gilt:

143 II

$$(1) \qquad \zeta_K(s) = \prod_{\mathfrak{P}|\mathfrak{F}} \left(1 - \mathsf{N}\mathfrak{P}^{-s}\right) = \prod_{\chi} L(s,\chi) \cdot \prod_{\chi} \prod_{\mathfrak{p}|\mathfrak{F}} \left(1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}\right).$$

Es ist das Ziel der folgenden Betrachtungen, nachzuweisen, daß sogar genau

$$(2) \qquad \zeta_K(s) = \prod_{\chi} L(s,\chi)$$

ist, daß also auch die Beiträge der Teiler $\mathfrak{p}$ von $\mathfrak{F}$ sich kompensieren, und sogar, wie wir überdies beweisen werden *für jedes* $\mathfrak{p}$ *gesondert* sich aufheben, genau wie es bei den zu $\mathfrak{F}$ primen $\mathfrak{p}$ der Fall ist. Ersteres wird sich analytisch aus der Funktionalgleichung von $\zeta_K(s)$ und der $L(s,\chi)$ ergeben, während das letztere genauere Resultat im allgemeinen Falle durch unsere analytischen Methoden nicht herauskommt, vielmehr arithmetisch bewiesen werden muß.

Für die Anwendung unseres analytischen Schlusses schreiben wir (1) in der Form

$$(3) \qquad \frac{\prod_{\chi} L(s,\chi)}{\zeta_K(s)} = G(s),$$

wo also

$$G(s) = \frac{\prod_{\mathfrak{P}|\mathfrak{F}} (1 - \mathsf{N}\mathfrak{P}^{-s})}{\prod_{\chi} \prod_{\mathfrak{p}|\mathfrak{F}} (1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s})}$$

gesetzt ist. Wir können $G(s)$ noch etwas anders schreiben. Sei nämlich:

144 II

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e; \qquad (\text{Grad } f; \quad efg = h)$$

die Zerlegung eines der Teiler $\mathfrak{p}$ von $\mathfrak{F}$ in K. Dann wird der Zähler ersichtlich:

$$\prod_{\mathfrak{p}|\mathfrak{F}} \left(1 - N\mathfrak{p}^{-fs}\right)^g.$$

Den Nenner können wir durch eine entsprechende Überlegung, wie oben umformen. Für ein bestimmtes $\mathfrak{p}$ treten nämlich nur solche $\chi(\mathfrak{p}) \neq 0$ im Produkt

auf, deren Führer $f(\chi)$ prim zu $\mathfrak{p}$ sind. Die Gesamtheit dieser χ_0 bildet eine Gruppe $X_\mathfrak{p}$[†] und die Gesamtheit der Ideale, für die $X_\mathfrak{p}$ die Werte 1 liefert, eine Klassengruppe $\mathsf{H}_\mathfrak{p}$, die H enthält, und deren Führer $\mathfrak{F}_\mathfrak{p}$ prim zu $\mathfrak{p}$ ist, (Satz 41). Ist dann f' der kleinste Exponent, sodaß $\mathfrak{p}^{f'}$ zu $\mathsf{H}_\mathfrak{p}$ gehört, und j der Index von $\mathsf{H}_\mathfrak{p}$ (d. h. der Grad von $X_\mathfrak{p}$), sodaß $f' \mid j$ und

$$f'g' = j$$

ist, so stellen wie oben die $\chi_0(\mathfrak{p})$ in ihrer Gesamtheit die g' mal genommene Reihe $1, \varepsilon, \dots \varepsilon^{f'-1}$ dar, wenn ε eine primitive f'–te Einheitswurzel ist. Also ist

$$\prod_\chi \prod_{\mathfrak{p}|\mathfrak{F}} \left(1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}\right) = \prod_{\mathfrak{p}|\mathfrak{F}} \left(1 - N\mathfrak{p}^{-f's}\right)^{g'} \qquad \text{und:}$$

$$G(s) = \prod_{\mathfrak{p}|\mathfrak{F}} \frac{\left(1 - N\mathfrak{p}^{-fs}\right)^g}{\left(1 - N\mathfrak{p}^{-f's}\right)^{g'}}. \tag{4}$$

Wir bilden uns nunmehr aus den Funktionalgleichungen für $\zeta_K(s)$ und die $L(s,\chi)$ die Funktionalgleichung für

$$\frac{\prod_\chi L(s,\chi)}{\zeta_K(s)} = G(s).$$

Sei $a_1, \dots, a_{r_1}$ das Exponentensystem eines eigentlichen Charakters χ nach H, wobei natürlich die früher mit $a_{r_1+1}, \dots a_n$, $m_1, \dots, m_r$ bezeichneten Exponenten hier gleich Null zu setzen sind, da wir ja keine Größencharaktere betrachten. (Die Exponenten $a_1, \dots, a_{r_1}$ entsprechen dem in χ nach Satz 18 steckenden Vorzeichencharakter). Dann lauten die Elemente für die Funktionalgleichung von $L(s,\chi)$ so:

$$\gamma(\chi) = \prod_{p=1}^{r_1} \sqrt{\pi}^{-a_p} = \pi^{-\frac{1}{2}\sum_1^{r_1} a_p}$$

[†]Das Produkt zweier Charaktere hat offenbar das kleinste gemeinsame Multiplum der Führer der Faktoren zum Führer.

Wegen $\gamma(\chi) = \gamma(\overline{\chi})$ kann also dieser Faktor aus der Funktionalgleichung ganz weggelassen werden.[‡]

$$\Gamma(s,\chi) = \prod_{p=1}^{r+1} \Gamma\left(\frac{e_p}{2}(s+a_p)\right) = \prod_{p=1}^{r_1} \Gamma\left(\frac{s+a_p}{2}\right) \cdot \big(\Gamma(s)\big)^{r_2} \tag{5}$$

(Ersichtlich ist $\Gamma(s,\overline{\chi}) = \Gamma(s,\chi)$, weil die a_p für χ und $\overline{\chi}$ übereinstimmen).

$$\mathsf{A} = \mathsf{A}(\chi) = 2^{-r_2}\pi^{-\frac{n}{2}}\sqrt{d}\sqrt{Nf(x)} \tag{6}$$

$$\mathsf{W}(\chi) = \frac{(-i)^{\sum_1^{r_1} a_p}}{\sqrt{Nf(\chi)}} v(\widehat{\varphi}\widehat{\delta}) \sum_{\widehat{\varrho}} \chi(\widehat{\varrho}) e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)}, \tag{7}$$

Wird $\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}$ auch noch tot. pos. vorausgesetzt, so ist $v(\widehat{\varphi}\widehat{\delta}) = v(\widehat{\varrho})$ und somit die Gausssche Summe einfach

$$\sum_{\widehat{\varrho}} \chi\big((\widehat{\varrho})\big) e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\widehat{\delta}}\right)}$$

mit dem *Ideal*charakter $\chi\big((\widehat{\varrho})\big)$

wenn $v(\widehat{\mu})\chi(\widehat{\mu})$ die Zerlegung des *Ideal*charakters $\chi\big((\widehat{\alpha})\big)$ nach Satz 21, S. 51 ist.

Die Funktionalgleichung für $\prod_{\chi} L(s,\chi)$ lautet dann nach Satz 38 so:

Die Funktion

$$\varphi(s) = \prod_{p=1}^{r_1} \prod_{\chi} \Gamma\left(\frac{s+a_p}{2}\right) \big(\Gamma(s)\big)^{hr_2} \left(\prod_{\chi} \mathsf{A}(\chi)\right)^{s} \prod_{\chi} L(s,\chi)$$

genügt der Funktionalgleichung:

$$\varphi(s) = \prod_{\chi} \mathsf{W}(\chi) \cdot \varphi(1-s).$$

[‡] Überhaupt kann in Satz 38 der Faktor $\prod_{p=1}^{n} \sqrt{e_p\pi}^{-a_p}$ aus der allgemeinen Funktionalgleichung aus demselben Grunde weggelassen werden.

(Denn $\overline{\chi}$ durchläuft mit χ alle Charaktere). Für das Produkt $\prod_{p=1}^{r_1}\prod_{\chi}\Gamma\left(\frac{s+a_p}{2}\right)$ schreiben wir noch einen etwas anderen Ausdruck. Sei nämlich

$$\left.\begin{array}{ccccccc} \nu_p^{(1)} & \text{die} & \text{Anzahl} & \text{der} & \chi & \text{mit} & a_0 = 0 \\ \nu_p^{(2)} & \shortparallel & \shortparallel & \shortparallel & \chi & \shortparallel & a_p = 1 \end{array}\right\}; \quad \nu_p^{(1)} + \nu_p^{(2)} = h$$

so ist

$$\prod_{\chi}\Gamma\left(\frac{s+a_p}{2}\right) = \left(\Gamma\left(\frac{s}{2}\right)\right)^{\nu_p^{(1)}}\left(\Gamma\left(\frac{s+1}{2}\right)\right)^{\nu_p^{(2)}}$$

und wenn

$$\left.\begin{array}{rcl} \sum\limits_{p=1}^{r_1}\nu_p^{(1)} & = & n_1 \\ \sum\limits_{p=1}^{r_1}\nu_p^{(2)} & = & n_2 \end{array}\right\}; \quad \text{also} \quad n_1 + n_2 = r_1 h$$

gesetzt wird, unser Faktor:

$$\left(\Gamma\left(\frac{s}{2}\right)\right)^{n_1}\left(\Gamma\left(\frac{s+1}{2}\right)\right)^{n_2},$$

sodaß $\varphi(s)$ übergeht in

$$\varphi(s) = \left(\Gamma\left(\frac{s}{2}\right)\right)^{n_1}\left(\Gamma\left(\frac{s+1}{2}\right)\right)^{n_2}\left(\Gamma(s)\right)^{hr_2}\left(\prod_{\chi}\mathsf{A}(\chi)\right)^{s}\prod_{\chi}L(s,\chi).$$

Die Funktionalgleichung für $\zeta_K(s)$ lautet für

$$\xi(s) = \left(\Gamma\left(\frac{s}{2}\right)\right)^{R_1}\left(\Gamma(s)\right)^{R_2}\mathsf{A}_K^s\zeta_K(s): \\ \xi(s) = \xi(1-s).$$

Dabei sind R_1, R_2 die r_1, r_2 entspr. Zahlen für K und

$$\mathsf{A}_K = 2^{-R_2}\pi^{-\frac{nh}{2}}\sqrt{D}, \tag{8}$$

wo

$$D = d^h N(\mathfrak{D}) \tag{9}$$

den Betrag der Diskriminante von K, also $\mathfrak{D}$ die Relativdiskriminante bezeichnet.

Daher folgt als Funktionalgleichung für $G(s)$ nach (3), wenn

$$\psi(s) = \frac{\varphi(s)}{\xi(s)} = \frac{\left(\Gamma\left(\frac{s}{2}\right)\right)^{n_1}\left(\Gamma\left(\frac{s+1}{2}\right)\right)^{n_2}(\Gamma(s))^{hr_2}\left(\prod_{\chi}\mathsf{A}(\chi)\right)^{s}}{\left(\Gamma\left(\frac{s}{2}\right)\right)^{R_1}(\Gamma(s))^{R_2}\,\mathsf{A}_K^{s}}G(s)$$

gesetzt wird:

$$\psi(s) = \prod_{\chi}\mathsf{W}(\chi)\cdot\psi(1-s).$$

Durch Betrachtung der Nullstellen und Pole von $\psi(s)$ folgt nun leicht, daß diese Funktionalgleichung nur so bestehen kann, daß $\psi(s) \equiv 1$ und die einzelnen Faktoren von $\psi(s)$ sich gegenseitig kompensieren. Um dies einzusehen, transformieren wir zunächst die Γ–Funktionen so, daß ihre Pole sich nicht überdecken. Dazu ist die Formel

$$\Gamma(2s) = \frac{2^{2s}}{2\sqrt{\pi}}\Gamma(s)\Gamma\left(s+\frac{1}{2}\right),$$

d. h.

$$\Gamma(s) = \frac{2^{s}}{2\sqrt{\pi}}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)$$

148 II

zu verwenden. Durch sie wird

$$\psi(s) = \frac{\left(\Gamma\left(\frac{s}{2}\right)\right)^{n_1+hr_2}\left(\Gamma\left(\frac{s+1}{2}\right)\right)^{n_2+hr_2}2^{-hr_2}\sqrt{\pi}^{-hr_2}\left(\prod_{\chi}2^{r_2}\mathsf{A}(\chi)\right)^{s}}{\left(\Gamma\left(\frac{s}{2}\right)\right)^{R_1+R_2}\left(\Gamma\left(\frac{s+1}{2}\right)\right)^{R_2}2^{-R_2}\sqrt{\pi}^{-R_2}\left(2^{r_2}\mathsf{A}_K\right)^{s}}G(s)$$

Nun hat $G(s)$ nach (4) Nullstellen und Pole höchstens auf der Geraden $\sigma = 0$, die Γ–Faktoren erzeugen Nullstellen und Pole nur auf der negativ–reellen Achse, sonst sind keine Nullstellen und Pole von $\psi(s)$ vorhanden. Wegen $\psi(s) = \prod_{\chi}\mathsf{W}(\chi)\cdot\psi(1-s)$ müssen also die Nullstellen und Pole der Γ–Faktoren einerseits sich aufheben, und die von $G(s)$ andererseits.

Da $\Gamma(s)$ Pole in $0, -1, -2, \ldots$ von 1. Ordnung und sonst keine Nullstellen und Pole hat, folgt für die funktionentheoretische Ordnungszahl von $\psi(s)$:

$$\begin{array}{lll} \text{in} & 0, -2, -4, \ldots & : \quad n_1 + hr_2 - (R_1 + R_2) \\ \text{in} & -1, -3, -5, \ldots & : \quad n_2 + hr_2 - R_2 \end{array}$$

Diese Ordnungszahlen müssen Null sein, also

$$\begin{aligned} n_1 + hr_2 &= R_1 + R_2, \\ n_2 + hr_2 &= R_2 \end{aligned}$$

und somit die Γ–Faktoren ganz aus $\psi(s)$ herausfallen. Es muß also die Funktion

$$\Psi(s) = \left(\frac{\prod\limits_{\chi} 2^{r_2} \mathsf{A}(\chi)}{2^{R_2} \mathsf{A}_K} \right)^s G(s)$$

der Funktionalgleichung

$$\Psi(s) = \prod_{\chi} \mathsf{W}(\chi) \cdot \Psi(1 - s)$$

149 II

genügen. Hieraus folgt durch Betrachtungen der Nullstellen und Pole von $G(s)$ in (4) zwar funktionentheoretisch leicht $G(s) \equiv 1$, aber nicht das gliedweise Herausfallen der Beiträge der einzelnen $\mathfrak{p}$, da ja ev. mehrere $\mathfrak{p}$ mit gleicher $N\mathfrak{p}$ existieren können, die sich dann etwa zyklisch vertauscht in Zähler und Nenner kompensieren könnten. Wir beweisen nachher arithmetisch das gliedweise Wegheben der Faktoren von $G(s)$, stellen hier nur fest, daß die Funktionentheorie jedenfalls $G(s) \equiv 1$, also die gesuchte Relation (2) (und damit auch alles notwendige für den im nächsten Abschnitt zu erbringenden Beweis von der arithmetischen Progression) liefert.

Aus $G(s) \equiv 1$ folgt dann schließlich, daß

$$\left(\frac{\prod\limits_{\chi} 2^{r_2} \mathsf{A}(\chi)}{2^{R_2} \mathsf{A}_K} \right)^{2s-1} \equiv \prod_{\chi} \mathsf{W}(\chi)$$

für alle s sein muß, was nur für

$$\prod_{\chi} 2^{r_2} \mathsf{A}(\chi) = 2^{R_2} \mathsf{A}_K \tag{10}$$

und

$$\prod_{\chi} \mathsf{W}(\chi) = 1 \tag{11}$$

geht.

(10) liefert nach (6), (8), (9)

$$d^h N\left(\prod_{\chi} f(\chi)\right) = D = d^h N(\mathfrak{D})$$

also

$$\mathfrak{D} = \prod_{\chi} f(\chi). \tag{12}$$

Dieser Schluß ist unkorrekt, da aus $N(\mathfrak{a}) = N(\mathfrak{b})$ nicht notwendig $\mathfrak{a} = \mathfrak{b}$ folgt. Siehe S. 324 f.

150 II

Durch (12) ist die Relativdiskriminante von K genau bestimmt, gleichzeitig erkannt, daß $\mathfrak{D}$ im allgemeinen ein echtes Multiplum von $\mathfrak{F}$ ist, nur im Falle, daß alle $f(\chi)$ relativ prim sind, $\mathfrak{D} = \mathfrak{F}$ (Satz 41).

(11) liefert eine Relation zwischen den $\mathsf{W}(\chi)$, also nach (7) den Gaussschen Summen. Im Falle $h = 2$, wo außer dem Hauptcharakter nur ein einziger Charakter χ existiert, liefert also dann (11) den genauen Wert der Gaussschen Summe. Wir geben diesen für den wichtigsten Fall, daß χ keinen Vorzeichencharakter enthält (also schon Charakter für $\mathfrak{I}(f)$ im Sinne von §3 ist) an:

$$\sum_{\widehat{\varrho}} \chi(\widehat{\varrho}) e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi}\delta}\right)} = \sqrt{N(f)}$$

wenn χ ein solcher Charakter von $\mathfrak{I}(f)$ ist, daß χ^2 der Hauptcharakter, und f sein Führer. (Offenbar gilt dies für jeden Charakter der angegebenen Art, indem man in obigen Betrachtungen dann den Körper K als den Klassenkörper zu der durch $\chi(\mathfrak{a}) = 1$ definierten Klassengruppe H vom Führer f wählt).

Wir haben somit durch unsere analytischen Betrachtungen folgendes Resultat:

151 II

Satz 42. Ist K relativ–Abelsch zu k und Klassenkörper für die Klassengruppe H vom Index h und Führer $\mathfrak{F}$, durchläuft ferner χ alle eigentlichen Charaktere nach H, deren Führer $f(\chi)$ seien, so gilt die Relation:

$$\zeta_K(s) = \prod_{\chi} L(s, \chi).$$

Ferner ist die Relativdiskriminante $\mathfrak{D}$ von K nach k durch

$$\mathfrak{D} = \prod_{\chi} f(\chi)$$

gegeben, also nach Satz 41 ein Multiplum von

$$\mathfrak{F} = [f(x)].$$

Satz 43. Ist speziell χ ein solcher eigentlicher Charakter[§] mod f, ohne Vorzeichenbedingungen, daß χ^2 der Hauptcharakter, so gilt für die Gausssche Summe

$$C(\chi, \widehat{\varphi\delta}) = \sum_{\widehat{\varrho}} \chi(\widehat{\varrho}) e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi\delta}}\right)}$$

im Sinne von Satz 29/30 die Formel:

$$C(\chi, \widehat{\varphi\delta}) = \sqrt{N(f)}$$

mit positiver Quadratwurzel (s. a. Satz 43a, S. 154▸)

Wir bringen schließlich den noch aufgeschobenen Nachweis, daß $G(s)$ in (4) gliedweise (für jedes $\mathfrak{p}$) gleich 1 ist. Dazu weisen wir nach, daß die oben mit

$\mathsf{H}_\mathfrak{p}$ bezeichnete, zu einem Teiler $\mathfrak{p}$ von $\mathfrak{F}$ konstruierte Klassengruppe diejenige Klassengruppe H_T ist, der der Trägheitskörper K_T von $\mathfrak{p}$ als Klassenkörper zugeordnet ist. Denn der Führer $\mathfrak{F}_T$ von H_T muß prim zu $\mathfrak{p}$ sein, da $\mathfrak{p}$ nicht in der Relativdiskriminante von K_T aufgeht. Also haben alle Charaktere nach H_T zu $\mathfrak{p}$ prime Führer, sodaß ihre Gruppe X_T Untergruppe von $X_\mathfrak{p}$ ist. Da $\mathsf{H}_T, \mathsf{H}_\mathfrak{p}$ bezw. die Gesamtheit der Ideale sind, für die $X_T, X_\mathfrak{p}$ den Wert 1 liefert, muß also $\mathsf{H}_\mathfrak{p} \mid \mathsf{H}_T$ sein.

[§] Charakter $\chi\big((\widehat{\alpha})\big)$ für *Ideale* im Sinne von §3.

Andererseits ist K_T der größte Unterkörper von K, dessen Relativdiskriminante prim zu $\mathfrak{p}$ ist. Daher aber der $\mathsf{H}_\mathfrak{p}$ zugeordnete Klassenkörper $K_\mathfrak{p}$ eine zu $\mathfrak{p}$ prime Relativdiskriminante hat, weil die Führer aller Charaktere nach $\mathsf{H}_\mathfrak{p}$ prim zu $\mathfrak{p}$ sind (Satz 42), muß $K_\mathfrak{p} \mid K_T$, also $\mathsf{H}_T \mid \mathsf{H}_\mathfrak{p}$ folglich

$$\mathsf{H}_\mathfrak{p} = \mathsf{H}_T$$

sein. Nun zerfällt im Trägheitskörper K_T bekanntlich $\mathfrak{p}$ so:

$$\mathfrak{p} = \overline{\mathfrak{P}}_1 \dots \overline{\mathfrak{P}}_g\,; \qquad \text{Grad } f,$$

wo f, g die auch für die Zerlegung in K so bezeichneten Größen sind. In Verbindung mit dem obigen folgt also aus $\mathsf{H}_T = \mathsf{H}_\mathfrak{p}$ und nach dem Zerlegungssatz angewendet auf K_T, daß f der kleinste Exponent für den $\mathfrak{p}^f$ in $\mathsf{H}_T = \mathsf{H}_\mathfrak{p}$, also

153 II

$f = f'$ ist. Weiter muß dann wegen

$$fg = f'g' = \text{Index von} \quad \mathsf{H}_T = \mathsf{H}_\mathfrak{p} = j$$

sein, also $g' = g$, womit das gliedweise Herausfallen der Faktoren von $G(s)$ in (4), wie behauptet, bewiesen ist. Da ferner H Untergruppe von $\mathsf{H}_\mathfrak{p} = \mathsf{H}_T$ ist, ist

$$h = j(\mathsf{H}_\mathfrak{p} : \mathsf{H}) = j \cdot e = fge$$

also die Ordnung e der Primteiler von $\mathfrak{p}$ zu

$$e = (\mathsf{H}_\mathfrak{p} : \mathsf{H})$$

bestimmt, oder was nach dem obigen dasselbe:

$$e = (X : X_\mathfrak{p}).$$

Es gilt somit:

Satz 44. Ist K relativ–Abelsch zu k und Klassenkörper für die Klassengruppe H vom Index h und Führer $\mathfrak{F}$. Ist dann $\mathfrak{p}$ ein Teiler von $\mathfrak{F}$, oder was dasselbe ist ein Teiler der Relativdiskriminante $\mathfrak{D}$ von K nach k, so bestimmen sich die charakteristischen Zahlen e, f, g der Zerlegung:

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e; \quad \text{Grad } f; \quad efg = h$$

von $\mathfrak{p}$ in K folgendermaßen: Sei $X_\mathfrak{p}$ diejenige Untergruppe der Gruppe X aller Charaktere nach H, deren Führer prim zu $\mathfrak{p}$ sind, und $\mathsf{H}_\mathfrak{p}$ die $X_\mathfrak{p}$ zugeordnete Klassengruppe (Gesamtheit der Klassen nach H, für die $X_\mathfrak{p}$ den Wert 1 liefert), deren Führer dann prim zu $\mathfrak{p}$ ist, so ist:

$$\begin{aligned} f &\quad \text{der kleinste Exponent für den } \mathfrak{p}^f \text{ zu } \mathsf{H}_\mathfrak{p} \text{ gehört.} \\ e &= (\mathsf{H}_\mathfrak{p} : \mathsf{H}) = (X : X_\mathfrak{p}) \\ g &= \frac{h}{ef} = \frac{j}{f}, \quad \text{wenn } j \text{ der Index von } \mathsf{H}_\mathfrak{p} \\ &\quad \text{und Grad von } X_\mathfrak{p} \text{ ist.} \end{aligned}$$

Überdies ist $\mathsf{H}_\mathfrak{p} = \mathsf{H}_T$ die dem Trägheitskörper K_T von $\mathfrak{p}$ zugeordnete Klassengruppe. Ersichtlich umfaßt dies Zerlegungsgesetz auch die zu $\mathfrak{D}$ primen $\mathfrak{p}$.

Anmerkung zu Satz 43. Dieser Satz läßt sich für beliebige „*quadratische*“ Charaktere, d. h. solche deren Quadrat der Hauptcharakter ist, so aussprechen:

Satz 43a. Ist χ irgendein quadratischer Idealcharakter mod f vom Führer f, so hat die mit ihm gebildete Gausssche Summe

$$G(\chi) = \sum_{\widehat{\varrho}} \chi\big((\widehat{\varrho})\big) e^{2\pi i S\left(\frac{\widehat{\varrho}}{\widehat{\varphi\delta}}\right)}$$

unabhängig von der speziellen Wahl von $\widehat{\varphi\delta}$ den Wert

$$G(\chi) = i^\nu \sqrt{N(f)},$$

wenn ν die Anzahl der von χ betroffenen reellen konjugierten ist (also $\nu = \sum_1^{r_1} a_p$, wo die a_p die Exponenten des in χ steckenden Vorzeichencharakters v sind). Dabei hat $\widehat{\varrho}$ in $G(\chi)$ ein vollständiges Restsystem mod f der Klasse von $\widehat{\varphi\delta}$ zu durchlaufen, dessen Repräsentanten zudem die gleiche Signatur wie $\widehat{\varphi\delta}$ haben, also ein vollst. Restsystem der Klasse von $\widehat{\varphi\delta}$ die Zugrundelegung der Klasseneinteilung $\mathfrak{Z}_0(1)$ (nicht nur $\mathfrak{Z}(1)$, wie bisher).

Beweis: Für dieses Restsystem spaltet sich $\chi\big((\widehat{\varrho})\big)$ in das frühere $\chi(\widehat{\varrho})$ und $v(\widehat{\varrho})$. $v(\widehat{\varrho})$ ist aber gleich $v(\widehat{\varphi\delta})$, weil $\frac{\widehat{\varrho}}{\widehat{\varphi\delta}}$ total positive Körperzahl. Daher geht

$G(\chi)$ in $v(\widehat{\varphi\delta})C(\chi, \widehat{\varphi\delta})$ über. Dies ist von $\widehat{\varphi\delta}$ unabh. nach Satz 31. Da ferner $\mathsf{W}(\chi) = 1$ ist, weil für den Hauptcharakter $\mathsf{W} = 1$ ist, folgt die Behauptung aus (7) und (11).

155 II

B. Der Satz von der arithmetischen Progression in k.

Aus der fundamentalen Zerfällungsgleichung

$$\zeta_K(s) = \prod_{\chi} L(s, \chi) \tag{1}$$

ergibt sich der einfachste und naturgemäßeste Beweis des allgemeinsten Satzes von der arithmetischen Progression in einem beliebigen algebraischen Körper k.

Sei H eine beliebige Kongruenzklassengruppe vom Führer $\mathfrak{F}$ mit oder ohne Vorzeichenbedingungen in k. h sei ihr Index und K der zugehörige relativ–Abelsche Klassenkörper vom Relativgrade h. Durchläuft dann χ alle Charaktere nach H, so besteht die Relation (1) zwischen der Dedekindschen ζ–Funktion von K und den h eigentlichen L–Reihen nach H. Aus dieser Relation folgt der wichtige

Satz 45. Es ist $L(1, \chi)$ endlich und von Null verschieden, wenn χ nicht der Hauptcharakter ist.

Beweis: 1.) Daß $L(1, \chi)$ endlich ist, wenn χ nicht der Hauptcharakter, folgt schon aus Satz 38/39, da die hiesigen χ Spezialfälle der dortigen λ sind.

2.) Die linke Seite von (1) hat nach Satz 40 einen Pol 1. Ordnung in $s = 1$. Auf der rechten Seite erzeugt der dem Hauptcharakter entsprechende Faktor $\zeta_k(s)$ ebenfalls nach Satz 40 einen Pol 1. Ordnung. Die anderen Faktoren können also keine Nullstellen haben, da sonst links kein Pol herauskommen könnte, w. z. b. w.

156 II

Dieser Beweis des Nichtverschwindens der L–Reihen bis $s = 1$ läßt den wesentlichen Kern des Dirichletschen Beweises für die quadratischen Charakteren[1] zugeordneten L–Reihen [...] rationalen Grundkörper deutlich erkennen. Der Schluß beruht eben darauf, daß die ζ–Funktion des Klassenkörpers

[1] nicht vollständig lesbar

bei $s = 1$ einen Pol 1. Ordnung, d. h. ein nicht verschwindendes Residuum hat, und da dieses Residuum im wesentlichen die Klassenzahl von K ist, eben auf dem Nichtverschwinden der Klassenzahl. Genauer ist für den Dirichletschen Fall die Relation (1):

$$\zeta_K(s) = \zeta(s)L(1,\chi)$$

weil dort nur ein „Nichthauptcharakter“ existiert (das Nichtverschwinden der L–Reihen mit komplexen Charakteren wird ja dort einfach funktionentheoretisch gezeigt). Diese Relation geht für $s \to 1$ durch Multiplikation mit $s-1$ über in[¶]

$$H\mathsf{K} = h\mathsf{k}L(1,\chi)$$

und $h\mathsf{k} = 1$, weil k der rationale Grundkörper, also

$$L(1,\chi) = H\mathsf{K}$$

wo H die Klassenzahl von K und K eine von Null verschiedene Konstante ist. Daher ist $L(1,\chi) \neq 0$. Man sieht, daß man im Dirichletschen Falle auch das Nichtverschwinden der komplexen Charakteren entsprechenden L–Reihen gleichzeitig erhält, wenn man anstelle des einem reellen χ entsprechenden *quadratischen* Klassenkörpers K denjenigen Klassenkörper K betrachtet, der der engsten Klasseneinteilung, also nach dem Strahl $\equiv 1 \mod m$, total positiv nimmt, der dann der Kreiskörper der m–ten Einheitswurzeln ist [‖]. Das

157 II

Produkt aller $L(1,\chi)$ stellt sich dann im wesentlichen als die Klassenzahl dieses Kreiskörpers dar.

Aus (1) folgt übrigens in Fortführung dieser Gedankengänge ein unendlicher Ausdruck für die Klassenzahl Abelscher Körper, oder genauer für die *Relativklassenzahl*. Multipliziert man nämlich beiderseits mit $s-1$ und geht zu $s = 1$ über, so folgt

$$\frac{H\mathsf{K}}{h\mathsf{k}} = \prod{}' L(1,\chi),$$

[¶] dies h hat eine andere Bedeutung als das obige

[‖] s. unten

d. h. wenn die Werte

$$\mathsf{K} = \frac{2^{R_1+R_2}\pi^{R_2}R_K}{\sqrt{D}w_K}$$
$$\mathsf{k} = \frac{2^{r_1+r_2}\pi^{r_2}R_k}{\sqrt{d}w_k}$$

eingesetzt werden, folgender Ausdruck für den Quotienten der Klassenzahlen H und h von K und k:

$$\frac{H}{h} = \frac{2^{r_1+r_2}\pi^{r_2}R_k}{2^{R_1+R_2}\pi^{R_2}R_K} \cdot \frac{\sqrt{D}w_K}{\sqrt{d}w_k} \cdot \prod{}' L(1,\chi), \tag{2}$$

wo das Produkt über alle Nichthauptcharaktere nach H zu erstrecken ist. Für $L(1,\chi)$ kann man dabei die unendlichen Summen

$$L(1,\chi) = \sum_{\mathfrak{a}}{}' \frac{\chi(\mathfrak{a})}{N\mathfrak{a}} \tag{3}$$

konvergent nach dem Abelschen Stetigkeitssatz

erstreckt über alle ganzen Ideale $\mathfrak{a} \neq 0$ aus k einsetzen.

Satz 46. Die Relativklassenzahl jedes relativ Abelschen Körpers läßt sich in der Form (2), (3) als ein Produkt unendlicher Reihen darstellen.

158 II

Für den Fall des rationalen Grundkörpers läßt sich das Produkt rechts noch in endlicher Form darstellen, und somit ein expliziter Ausdruck für die Klassenzahl H absolut Abelscher Körper angeben, das allerdings die Kenntnis des Regulators R_K erfordert. (siehe mein Tagebuch I, S. 44 ff). Im Falle eines imaginär quadratischen Grundkörpers führt (2) auf die sogenannte Kroneckersche Grenzformel und steht mit der Theorie der komplexen Multiplikation und der elliptischen Modulfunktion $\eta(\omega)$ in engem Zusammenhang. Für andere spezielle Grundkörper haben Hecke und seine Schüler auf Grund der Formel (2) durch Auswertung der Reihen (3) Analoga zu dieser Kroneckerschen Grenzformel entwickelt und Hecke eine darauf bezügliche Vermutung ausgesprochen**. Abschließende Resultate liegen hingegen noch nicht vor.

**s. Hecke, Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern, Gött. Nachr. 1921, S. 1.

Wir folgern nunmehr aus Satz 45 leicht den Satz von der arithmetischen Progression. Es seien mit $\varphi_1(s), \varphi_2(s), \ldots$ durchweg Funktionen bezeichnet, die bei $s = 1$ endlich sind.

Aus Satz 40 folgt durch Logarithmierung von

$$(s-1)\zeta_k(s) = \text{ganze Funktion} \neq 0 \text{ für } s = 1:$$

$$\log \zeta_k(s) = \log \frac{1}{s-1} + \varphi_1(s). \tag{4}$$

Nach Satz 45 ist ferner

$$\log L(s, \chi) = \varphi_2(s, \chi), \tag{5}$$

wenn χ nicht der Hauptcharakter. Aus (4) und (5) folgt, wenn mit dem reziproken Charakter $\overline{\chi}(\mathfrak{K})$ für eine beliebige Klasse $\mathfrak{K}$ nach H multipliziert und über alle χ summiert wird:

$$\sum_{\chi} \overline{\chi}(\mathfrak{K}) \log L(s, \chi) = \varphi_3(s) + \log \frac{1}{s-1}. \tag{6}$$

Andererseits ist wegen der absoluten Konvergenz für $\Re(s) > 1$

$$\log L(s, \chi) = -\sum_{\mathfrak{p}} \log \left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s}\right) = \sum_{m=1}^{\infty} \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p}^m)}{mN\mathfrak{p}^{ms}}.$$

Die rechts stehende Summe zerfällt in bekannter Weise in

$$\sum_{\mathfrak{p}_1} \frac{\chi(\mathfrak{p}_1)}{N\mathfrak{p}_1^s} + \varphi_4(s)$$

wo $\mathfrak{p}_1$ alle Primideale 1. Grades aus k durchläuft, da alle anderen Glieder unterhalb einer leicht angebbaren für $\Re(s) > \frac{1}{2}$ absolut konvergenten Majorante liegen. Also ist

$$\log L(s, \chi) = \sum_{\mathfrak{p}_1} \frac{\chi(\mathfrak{p}_1)}{N\mathfrak{p}_1^s} + \varphi_4(s). \tag{7}$$

Durch Multiplikation mit $\overline{\chi}(\mathfrak{K})$ und Summation über alle χ folgt hieraus:

$$(8) \qquad \sum_{\chi} \overline{\chi}(\mathfrak{K}) \log L(s,\chi) = \sum_{\mathfrak{p}_1} \frac{\sum_{\chi} \chi\left(\frac{\mathfrak{p}_1}{\mathfrak{K}}\right)}{N\mathfrak{p}_1^s} + \varphi_5(s),$$

wobei $\chi\left(\frac{\mathfrak{p}_1}{\mathfrak{K}}\right)$ den Charakter für die Klasse $\frac{\mathfrak{K}_{\mathfrak{p}_1}}{\mathfrak{K}}$ bedeutet, wenn $\mathfrak{p}_1$ zu $\mathfrak{K}_{\mathfrak{p}_1}$ gehört.

160 II

Nun ist

$$\sum_{\chi} \chi\left(\frac{\mathfrak{p}_1}{\mathfrak{K}}\right) = \begin{cases} h, & \text{wenn } \mathfrak{p}_1 \text{ zu } \mathfrak{K} \text{ gehört,} \\ 0, & \text{andernfalls.} \end{cases}$$

Also wird nach (6), (8):

$$\sum_{\mathfrak{p}_1 \text{ in } \mathfrak{K}} \frac{1}{N\mathfrak{p}_1^s} = \frac{1}{h} \log \frac{1}{s-1} + \varphi_6(s),$$

und somit für $s \to 1$, daß in $\mathfrak{K}$ unendlich viele $\mathfrak{p}_1$ vorkommen.

Satz 47. Ist H eine beliebige Kongruenzklassengruppe in k, so kommen in jeder Klasse nach H unendlich viele Primideale 1. Grades vor.

Dies ist der Satz von der arithmetischen Progression in seiner allgemeinst–möglichen Form. Wir spezialisieren ihn noch für den Fall der engsten Klasseneinteilung. Die Klassengruppe H sei der Strahl der total positiven Zahlen $\equiv 1 \mod f$, wo f irgendein ganzer Idealmodul ist. Die Klassengruppe nach H ist dann die Gruppe $\mathfrak{J}_0(f)$ von §3▸. Es gibt somit in jeder Klasse von $\mathfrak{J}_0(f)$ unendlich viele Primideale $(\widehat{\pi})$ vom ersten Grade, also bei gegebenem $\widehat{\varrho}$ unendlich viele Primideale $(\widehat{\pi})$, sodaß

$$\widehat{\pi} \equiv \varepsilon\widehat{\varrho} \mod f, \qquad \frac{\widehat{\pi}}{\varepsilon\widehat{\varrho}} \text{ total positiv.}$$

Nimmt man $\widehat{\pi}\varepsilon$ als Repräsentant, so folgt also:

Satz 48. In jeder Restklasse mod f gibt es unendlich viele ideale Zahlen $\widehat{\pi}$ vorgeschriebener Signatur[††], sodaß $(\widehat{\pi})$ Primideal 1. Grades ist. Speziell gibt es also unendlich viele Prim–Hauptideale 1. Grades vorgeschriebener Signatur.

NB. Fortsetzung in „Reziprozitätsgesetz“ §10▸, 305▸–325▸

[††] also in jeder Klasse von $\mathfrak{Z}_0(f)$ im Sinne von §2▸.

2.8 §8 Die absolut Abelschen Körper.

161 II

A. Der Kreiskörper der m–ten Einheitswurzeln.

Als Grundkörper legen wir in diesem § den Körper R der rationalen Zahlen zugrunde. Wir gehen zunächst kurz auf die in R möglichen Klasseneinteilungen ein. Im absoluten Sinne gibt es in R nur eine Idealklasse, die Hauptklasse, der alle rationalen Zahlen angehören. Auch im sogenannten engeren Sinne, d. h. mit der Forderung „total positiv“ gibt es nur eine Idealklasse, denn die Ideale $(+a)$ und $(-a)$ sind eben als *Ideale* gleich. Es bestehen also die Gruppen $\mathfrak{J}(1)$ und $\mathfrak{J}_0(1)$ je nur aus einer einzigen Klasse, der Gruppe aller rationalen Zahlen. $\big($$\mathfrak{Z}(1)$ und $\mathfrak{Z}_0(1)$ sind dagegen verschieden, nämlich $\mathfrak{Z}(1)$ die Gruppe *aller* positiven *und* negativen, dagegen $\mathfrak{Z}_0(1)$ die aus 2 Klassen, den positiven und den negativen Zahlen *einzeln* bestehenden Gruppen$\big)$.

Die allgemeinste Klasseneinteilung von R erhält man, wenn man irgendeinen ganzen Modul m zugrundelegt. Dann resultieren für die zu m primen *Zahlen* folgende Klasseneinteilungen:

1.) $\mathfrak{Z}(m)$: Gruppe aller primen Restklassen mod m, Grad $\varphi(m)$
2.) $\mathfrak{Z}_0(m)$: Gruppe aller primen Restklassen gleichen Vorzeichens mod m, Grad $2\varphi(m)$.

162 II

Diese liefern folgende *Ideal*klasseneinteilungen:

1.) *Die Gruppe* $\mathfrak{J}(m)$. Zwei Ideale (a) und (b) gehören zur selben Klasse von $\mathfrak{J}(m)$, wenn

$$a \equiv \pm b \mod m$$

(± 1 sind ja die einzigen Einheiten in R; siehe zu all' diesen Entwicklungen §2▸/§3▸). Die Hauptklasse, d. h. die Klasse von (1) ist:

$$a \equiv \pm 1 \mod m.$$

Die Klassen werden also gebildet, durch je ein Paar entgegengesetzt gleicher Restklassen mod m. Für $m \neq 2$ ist die Klassenzahl von $\mathfrak{J}(m)$

also $\frac{1}{2}\varphi(m)$ $\big(\varphi(m)$ ist dann auch stets gerade$\big)$, für $m = 2$ gleich $\varphi(2) = 1$, ebenso für $m = 1$.

2.) *Die Gruppe* $\mathfrak{I}_0(m)$. Zwei Ideale (a) und (b) gehören zur selben Klasse von $\mathfrak{I}_0(m)$, wenn

$$a \equiv \pm b \mod m, \qquad \frac{a}{\pm b} \quad \text{positiv.}$$

Die Hauptklasse von $\mathfrak{I}_0(m)$ besteht also aus allen

$$\begin{aligned} a &\equiv 1 \mod m \quad , \quad \text{positiv,} \\ a &\equiv -1 \mod m \quad , \quad \text{negativ,} \end{aligned}$$

d. h. jede Klasse immer aus allen positiven Zahlen einer und allen negativen der entgegengesetzten Restklasse. Die Anzahl der Klassen von $\mathfrak{I}_0(m)$ ist somit stets $\varphi(m)$.

Satz 49. Die Gruppen $\mathfrak{Z}(m), \mathfrak{Z}_0(m), \mathfrak{I}(m), \mathfrak{I}_0(m)$ von §2▸/§3▸ haben für den rationalen Körper und einen ganzen Modul m in ihm folgende Bedeutung:

1. $\mathfrak{Z}(m)$: Gruppe aller primen Restklassen mod m, Grad $\varphi(m)$
2. $\mathfrak{Z}_0(m)$: Gruppe aller primen „Halbrestklassen“ mod m, d. h. Restklassen mit Vorzeichenbedingung, Grad $2\varphi(m)$.
3. $\mathfrak{I}(m)$: Gruppe aller primen, entgegengesetzt gleichen Restklassenpaare mod m, Grad $\frac{1}{2}\varphi(m)$, jedoch für $m = 1$ und 2 Grad $\varphi(m) = 1$.

4.) $\mathfrak{I}_0(m)$: Gruppe aller primen Halbrestklassenpaare, sodaß die beiden Halbrestklassen eines Paares entgegengesetzte Vorzeichen, aber absolut gleiche Elemente haben (entgegengesetzten Restklassen angehören), Grad in allen Fällen $\varphi(m)$.

Wir haben nunmehr die Charaktere nach diesen Gruppen zu untersuchen. Als grundlegende Elemente betrachten wir die Charaktere $\chi(a)$ von $\mathfrak{Z}(m)$. Eine Funktion χ „multiplikative[...] Eigenschaft“ ist Charakter von $\mathfrak{Z}(m)$, wenn für zu m prime a, b

$$\chi(a) = \chi(b)\,, \quad \text{wenn} \quad a \equiv b \mod m,$$

oder was gleichbedeutend, wenn

$$\chi(a) = 1\,, \quad \text{wenn} \quad a \equiv 1 \mod m. \tag{1}$$

164 II

Einen solchen Charakter nennen wir einen *Restklassencharakter mod* m, speziell einen *eigentlichen*, wenn (1) für keinen kleineren Modul gilt. Dann gilt, wie im allgemeinen Falle:

Es gibt einen eindeutig bestimmten Teiler f *von* m*, sodaß* χ *eigentlicher Restklassencharakter mod* f*. Für alle zu* f *nicht primen Restklassen mod* f *setzen wir* $\chi = 0$. Das so erweiterte χ genügt ebenfalls seinen beiden Definitionsgleichungen

$$\begin{cases} \chi(ab) = \chi(a)\chi(b) \\ \chi(a) = \chi(b)\,, \quad \text{wenn} \quad a \equiv b \mod f \end{cases} \tag{2}$$

für beliebige rationale (*für* f *ganze*) *Zahlen* a, b.

Aus diesen Restklassencharakteren mod m bauen sich die Charaktere nach den übrigen Gruppen $\mathfrak{Z}_0(m)$, $\mathfrak{I}(m)$, $\mathfrak{I}_0(m)$ leicht auf.

Die Charaktere $\chi_0(a)$ nach $\mathfrak{Z}_0(m)$ haben nach Satz 18 die eindeutige Zerlegung:

$$\chi_0(a) = v(a)\chi(a) = (\operatorname{sgn} a)^\alpha \chi(a)\,; \qquad (\alpha = 0, 1)$$

und umgekehrt ist jeder Charakter $(\operatorname{sgn} a)^\alpha \chi(a)$ ein $\chi_0(a)$, sodaß auch die richtige Anzahl $2\varphi(m)$ herauskommt, weil eben jedem der $\varphi(m)$ Charaktere $\chi(a)$ zwei Charaktere $\chi_0(a)$:

$$\begin{aligned} \chi_0(a) &= \chi(a) \\ \chi_0(a) &= \operatorname{sgn} a.\chi(a) \end{aligned}$$

zugeordnet sind.

165 II

Die Charaktere $\chi\big((a)\big)$ von $\mathfrak{I}(m)$ sind natürlich spezielle $\chi(a)$; damit ein $\chi(a)$ *Ideal*charakter von $\mathfrak{I}(m)$ ist, muß

$$\chi(a) = \chi(-a)$$

also

$$\chi(-1) = +1 \tag{3}$$

sein. Umgekehrt ist ein solches $\chi(a)$ sicher ein $\chi\big((a)\big)$, denn es hat denselben Wert für je zwei entgegengesetzt gleiche Restklassen. Die Charaktere $\chi(a)$ der Eigenschaft (3) bilden im allgemeinen eine Untergruppe vom Index 2 aller $\chi(a)$, da jedes Quadrat χ^2 (3) erfüllt und wenn $\chi_1(-1) = -1$ ist entweder χ oder $\chi\chi_1$ (3) erfüllt. Existiert ein χ_1 mit $\chi_1(-1) = -1$, so ist der Index tatsächlich 2, sonst 1. Letzteres kann dann und nur dann eintreten, wenn -1 zur Hauptklasse von $\mathfrak{Z}(m)$ gehört, also

$$-1 \equiv 1 \mod m$$

d. h. $m = 1$ oder 2 ist. Daher kommt die richtige Anzahl von $\chi\big((a)\big)$ heraus, nämlich $\frac{1}{2}\varphi(m)$ im allgemeinen, $\varphi(m) = 1$ für $m = 1, 2$.

Schließlich haben die Charaktere $\chi_0\big((a)\big)$ von $\mathfrak{I}_0(m)$ die eindeutige Zerlegung nach Satz 18:

$$\chi_0\big((a)\big) = v(a)\chi(a) = (\operatorname{sgn} a)^\alpha \chi(a).$$

Wir dürfen uns dabei der Einfachheit halber, und auch naturgemäß auf *positive* a beschränken, da es sich ja nur um *Ideale* handelt. Alsdann ist

$$\chi_0\big((a)\big) = \chi(a)\,; \qquad (a > 0)$$

also jeder Charakter von $\mathfrak{I}_0(m)$ ein Charakter von $\mathfrak{Z}(m)$,

166 II

wenn man nur positive Argumente ins Auge faßt. Umgekehrt ist aber auch jedes $\chi(a)$ für positive Argumente ein $\chi_0\big((a)\big)$. Denn für $a > 0$ ist ja die Klasseneinteilung $\mathfrak{Z}(m)$ identisch mit $\mathfrak{I}_0(m)$. (Für negative Argumente sind natürlich die $\chi_0\big((a)\big)$ nicht mehr demselben $\chi(a)$ zugeordnet).

Für die uns in der Hauptsache interessierden Idealcharaktere haben wir also:

Satz 50. Die $\varphi(m)$ Charaktere der engsten Klasseneinteilung $\mathfrak{I}_0(m)$ mod m werden für positive Argumente a durch die $\varphi(m)$ Charaktere $\chi(a)$ der Gruppe $\mathfrak{Z}(m)$ der primen Restklassen mod m geliefert. Ein solcher Charakter $\chi(a)$ ist dann und nur dann schon Charakter für $\mathfrak{I}(m)$, wenn $\chi(-1) = +1$ ist. Für $m \neq 1, 2$ erfüllen diese Bedingung genau die Hälfte aller Charaktere $\chi(a)$; für

$m = 1, 2$ existiert sowohl in $\mathfrak{I}(m)$, wie in $\mathfrak{I}_0(m)$ nur die Hauptklasse, also der Hauptcharakter.

Ehe wir zum allgemeinen Kreiskörper der m–ten Einheitswurzeln übergehen, machen wir noch folgende Bemerkung:

Satz 51. Die Klasseneinteilungen $\mathfrak{I}(2m)$, $\mathfrak{I}_0(2m)$ für ungerades m sind mit $\mathfrak{I}(m)$, $\mathfrak{I}_0(m)$ wesentlich (d. h. für zu 2 prime Zahlen) identisch.

167 II

Beweis: Für ungerade a, b, m folgt aus

$$a \equiv b \mod m,$$

daß auch

$$a \equiv b \mod 2m$$

ist. Daher sind in diesem Falle für zu 2 prime Zahlen die Restklassen mod m und mod $2m$ identisch, also auch die auf ihnen aufgebauten Klasseneinteilungen mod m und $2m$. Da es im Sinne der „wesentlichen Identität“ zweier Klassengruppen auf die zu endlich vielen Idealen nicht primen Ideale nicht ankommt, ist der Beweis erbracht. Der Satz lehrt, etwas anders ausgedrückt:

Satz 52. Der Führer m jeder Klassengruppe in R ist entweder ungerade oder durch 4 teilbar.

Denn das Doppelte einer ungeraden Zahl kann er nicht sein, weil schon die engste Klasseneinteilung $\mathfrak{I}_0(2m)$ für ungerades m auch mod m als $\mathfrak{I}_0(m)$ definiert werden kann.

Ebenso wie für die Klasseneinteilungen in R kommen auch für die Kreiskörper der m–ten Einheitswurzeln nur ungerade m oder durch 4 teilbare in Frage. Denn für ungerades m ist ersichtlich der Körper der $2m$–ten Einheitswurzeln $\pm 1, \pm\varepsilon, \ldots, \pm\varepsilon^{m-1}$ identisch mit dem der m–ten $1, \varepsilon, \ldots, \varepsilon^{m-1}$. Beide Tatsachen, diese und die von Satz 51/52 stehen auf Grund der folgenden Entwicklungen in unmittelbarem Zusammenhang. Wir beweisen nämlich:

168 II

Satz 53. Der Körper K_m der m–ten Einheitswurzeln ist Klassenkörper für die Klasseneinteilung $\mathfrak{I}_0(m)$ in R.

Beweis: 1.) Auf Grund der eben gemachten Bemerkung genügt es, m ungerade oder durch 4 teilbar vorauszusetzen. Denn ist $m \equiv 2m_0$; (m_0 ungerade), so ist einerseits $K_m = K_{m_0}$, andererseits $\mathfrak{I}_0(m)$ wesentlich identisch mit $\mathfrak{I}_0(m_0)$.

2.) K_m ist Galoissch, da alle Wurzeln von $x^m - 1 = 0$ Potenzen einer primitiven ε.

3.) K_m ist der komponierte Körper:

$$K_m = \left(K_{\ell_1^{\nu_1}}, \ldots, K_{\ell_t^{\nu_t}}\right)$$

wenn $m = \ell_1^{\nu_1} \ldots \ell_t^{\nu_t}$ die Zerlegung von m in Primzahlpotenzen ist. Denn bekanntlich läßt sich die primitive m–te Einheitswurzel ε in der Form darstellen:

$$\varepsilon = \varepsilon_1^{c_1} \ldots \varepsilon_t^{c_t},$$

wo ε_k eine primitive $\ell_k^{\nu_k}$–te Einheitswurzel ist, weil dieser Ausdruck alle m–ten Einheitswurzeln darstellt, wenn die c_k volle Restsysteme mod $\ell_k^{\nu_k}$ durchlaufen.

4.) Der Grad von K_{ℓ^ν} ist höchstens $\varphi(\ell^\nu) = \ell^{\nu-1}(\ell - 1)$. Denn es ist

$$x^{\ell^\nu} - 1 = \left(x^{\ell^{\nu-1}} - 1\right)\left(x^{\ell^{\nu-1}(\ell-1)} + x^{\ell^{\nu-1}(\ell-2)} + \cdots + 1\right)$$

und eine *primitive* ℓ^ν–te Einheitswurzel muß dem *zweiten* Faktor vom Grade $\varphi(\ell^\nu)$ genügen.

169 II

5.) Aus 3.) 4.) folgt, daß der Grad von K_m höchstens $\varphi(m) = \varphi(\ell_1^{\nu_1}) \ldots \varphi(\ell_k^{\nu_k})$ ist.

6.) Sei $\mathfrak{p}$ ein Primideal 1. Grades von K_m, das prim ist zu den Zahlen $1 - \varepsilon^c$. (Ein solches $\mathfrak{p}$ muß natürlich stets in K_m existieren, da es ja in jedem Körper unendlich viele Primideale 1. Grades gibt). Dann ist $N\mathfrak{p} = p$ eine rationale Primzahl. Nach dem Fermatschen Satz ist ferner

$$\varepsilon^{N\mathfrak{p}-1} \equiv 1 \mod \mathfrak{p}$$

d. h. $\varepsilon^{p-1} - 1$ durch $\mathfrak{p}$ teilbar, was nach Voraussetzung über $\mathfrak{p}$ nur für $\varepsilon^{p-1} - 1 = 0$, d. h.

$$p \equiv 1 \mod m$$

geht. Abgesehen von endlich vielen Ausnahmen liegen also alle in Primideale 1. Grades zerfallenden p (s. 2.)) in der Klassengruppe $\equiv 1 \mod m$, positiv, d. h. in der Hauptklasse von $\mathfrak{J}_0(m)$, deren Index nach obigem $\varphi(m)$ ist.

Wenden wir also K. K. **III**, Satz 56, S. 210* an, so sind alle dortigen Voraussetzungen für den Körper K_m und die Klassengruppe: Hauptklasse von

*Mit K. K. zitiere ich meine Neubearbeitung des Takagischen Existenzbeweises für den allgemeinen Strahlklassenkörper.

$\mathfrak{J}_0(m)$ erfüllt. K_m ist also der Klassenkörper für diese Klassengruppe, d. h. für die Klasseneinteilung $\mathfrak{J}_0(m)$, w. z. b. w.

Überdies folgt dann:

170 II

Satz 54. K_m hat genau den Grad $\varphi(m)$, d. h. nach 3.), 4.) a. S. 168 die einzelnen Körper K_{ℓ^ν} sind zu je zweien relativ prim und jeder K_{ℓ^ν} ist prim zu einem Kompositum aus irgendwelchen anderen (mit *anderen* ℓ), ferner K_m ist Abelsch.

Anmerkung: Zum Beweis von Satz 53/54 wurde Satz 56 von K. K., also nach dem dortigen Beweis der Satz von der arithmetischen Progression (Satz 47) benutzt.

Vermöge Satz 53 beherrschen wir nunmehr den Körper K_m genau. Für die Zerlegung der Primzahlen p in K_m folgt aus dem allgemeinen Zerlegungsgesetz für den Klassenkörper:

Satz 55. Ist p eine zum Führer von $\mathfrak{J}_0(m)$, d. h. nach Voraussetzung über m, zu m prime Primzahl, und f der kleinste Exponent, sodaß p^f zur Hauptklasse von $\mathfrak{J}_0(m)$ gehört, d. h. daß

$$p^f \equiv 1 \mod m$$

ist, so zerfällt p in K_m in $\frac{\varphi(m)}{f} = g$ Primideale f–ten Grades.

Anmerkung: Der Führer von $\mathfrak{J}_0(m)$, genauer der Führer der Hauptklasse von $\mathfrak{J}_0(m)$ die für positive a durch

$$a \equiv 1 \mod m$$

definiert ist, ist ersichtlich m. Denn ist $m = km_0$ und nicht m_0 ungerade, $k = 2$, so gibt es stets unendlich viele zu m prime Zahlen, sodaß

171 II

$$\begin{aligned} & a \equiv 1 \mod m_0, \\ & a \not\equiv 1 \mod k \\ \text{also auch} \quad & a \not\equiv 1 \mod m \end{aligned}$$

ist. Es kann daher die Gruppe $a \equiv 1 \mod m$, positiv nicht schon nach einem niedrigeren Modul m_0 definiert werden, abgesehen von dem genannten Spezialfall, den wir stets ausschließen können und wollen.

Wir können ferner auf Grund von §7▶, A. die Diskriminante von K_m bestimmen. Wir brauchen diese Bestimmung nur für den Fall K_{ℓ^ν} durchzuführen, da sich dann die Diskriminante von K_m auf Grund von Satz 54 nach einem allgemeinen Diskriminantensatze ergibt.

Wir haben demgemäß auf Grund von Satz 42 die Führer der Charaktere von $\mathfrak{J}_0(\ell^\nu)$ zu bestimmen.

a.) ℓ ungerade.

Jede prime Restklasse mod ℓ^ν läßt sich eindeutig in der Form

$$a \equiv w^b(1+\ell)^c \mod \ell^\nu$$

darstellen, wo w eine primitive $(\ell-1)$–te Einheitswurzel im Körper $R(\ell)$ der ℓ–adischen Zahlen ist und

$$\begin{aligned} b &\mod \ell-1, \\ c &\mod \ell^{\nu-1} \end{aligned}$$

eindeutig bestimmte ganze Zahlen sind. Dementsprechend ist (immer unter Beschränkung auf positive Zahlen — Satz 50) jede Funktion

$$\chi(a) = w^{bb'}\omega^{cc'}, \tag{4}$$

wo ω eine primitive $\ell^{\nu-1}$–te Einheitswurzel bedeutet, ein

172 II

Charakter von $\mathfrak{J}_0(\ell^\nu)$, denn er hat die multiplikative Eigenschaft und die Eigenschaft (1). Wegen der Unabhängigkeit von w und ω als Einheitswurzeln von zueinander primen Graden, sind zwei solche Funktionen nur dann identisch, wenn ihre Exponenten $b' \mod \ell-1$ und $c' \mod \ell^{\nu-1}$ übereinstimmen. Daher liefert (4) genau $(\ell-1)\ell^{\nu-1} = \varphi(\ell^\nu)$ verschiedene Charaktere von $\mathfrak{J}_0(\ell^\nu)$ und somit alle, wenn b', c' volle Restsysteme mod $\ell-1$, und mod $\ell^{\nu-1}$ durchlaufen. Die Führer dieser Charaktere sind natürlich sämtlich Potenzen von ℓ, da sie Restklassencharaktere mod ℓ^ν sind. Den Führer 1 kann ersichtlich nur der Hauptcharakter haben. Denn soll $\chi(a) = 1$ für *alle* primen a sein, so muß in (4) $b' \equiv 0 \mod \ell-1$, $c' \equiv 0 \mod \ell^{\nu-1}$ sein.

Aus

$$a \equiv 1 \mod \ell^{\mu}; \qquad (1 \leqq \mu \leqq \nu)$$

folgt offenbar zunächst mod ℓ:

$$b \equiv 0 \mod \ell - 1,$$

dann mod ℓ^{μ}:

$$c \equiv 0 \mod \ell^{\mu-1}.$$

Umgekehrt ist für solche b, c:

$$a \equiv 1 \mod \ell^{\mu}.$$

Soll nun $\chi(a)$ den Führer ℓ^{μ} haben, so muß zunächst für alle $a \equiv 1 \mod \ell^{\mu}$: $\chi(a) = 1$ sein; also für alle

$$\left\{ \begin{array}{ll} b \equiv 0 & \mod \ell - 1 \\ c \equiv 0 & \mod \ell^{\mu-1} \end{array} \right\} : \left\{ \begin{array}{ll} bb' \equiv 0 & \mod \ell - 1 \\ cc' \equiv 0 & \mod \ell^{\nu-1} \end{array} \right\}$$

sein, was

$$c' \equiv 0 \mod \ell^{\nu-\mu} \tag{5}$$

zur Folge hat.

Ist dies umgekehrt erfüllt, so folgt rückwärts unmittelbar, daß $\chi(a) = 1$ für $a \equiv 1 \mod \ell^{\mu}$ ist. Damit also weiter μ der niedrigste Exponent dieser Eigenschaft ist, muß für $\mu > 1$:

$$c' \not\equiv 0 \mod \ell^{\nu-(\mu-1)} \tag{6}$$

sein, und im Falle $\mu = 1$, wo sich nach (5) χ auf

$$\chi(a) = w^{bb'}$$

reduziert

$$b' \not\equiv 0 \mod \ell - 1. \tag{7}$$

Es ist also nach (5) – (7) zunächst:

$$\begin{array}{cccccccccc} \text{Anzahl} & \text{der} & \chi & \text{vom} & \text{Führer} & 1 & \text{gleich} & 1 \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \ell & \shortparallel & \ell - 2 \end{array}$$

Für die höheren Führer hat b' alle $\ell - 1$ Möglichkeiten, c' kann alle Multipla von $\ell^{\nu-\mu}$, die nicht Multipla von $\ell^{\nu-\mu+1}$ sind annehmen. Denkt man sich also c' in der Form

$$c' = c_0 + c_1\ell + \cdots + c_{\nu-2}\ell^{\nu-2}\,; \qquad (c_k = 0, 1, \ldots, \ell - 1)$$

dargestellt, in der alle in Frage kommenden c', jedes einmal enthalten sind, so muß für den Führer ℓ^μ:

$$\begin{gathered} c_0, c_1, \ldots, c_{\nu-\mu-1} = 0, \\ c_{\nu-\mu} \neq 0, \\ c_{\nu-\mu+1}, \ldots, c_{\nu-2} \quad \text{beliebig} \end{gathered}$$

sein. Das sind genau $(\ell - 1)\ell^{\mu-2}$ Möglichkeiten. Somit folgt:

$$\begin{array}{cccccccccc} \text{Anzahl} & \text{der} & \chi & \text{vom} & \text{Führer} & \ell^2 & \text{gleich} & (\ell-1)(\ell-1) \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \ell^3 & \shortparallel & (\ell-1)(\ell-1)\ell \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \ell^\nu & \shortparallel & (\ell-1)(\ell-1)\ell^{\nu-2} \end{array}$$

174 II

Ersichtlich wird so die Anzahl aller χ

$$\begin{aligned} &1 + (\ell - 2) + (\ell - 1)\left\{\ell - 1 + \ell^2 - \ell + \cdots + \ell^{\nu-1} - \ell^{\nu-2}\right\} \\ &= (\ell - 1) + (\ell - 1)\left\{\ell^{\nu-1} - 1\right\} = (\ell - 1)\ell^{\nu-1} = \varphi(\ell^\nu), \end{aligned}$$

wie es sein soll.

Für das Produkt aller Führer und somit die Diskriminante (ihren Betrag) $|d|$ ergibt sich so:

$$\begin{aligned} |d| &= \ell^{(\ell-2)+(\ell-1)\left\{2(\ell-1)+3(\ell^2-\ell)+\cdots+\nu(\ell^{\nu-1}-\ell^{\nu-2})\right\}} \\ &= \ell^{\ell-2+(\ell-1)\left\{-2-\ell-\ell^2-\cdots-\ell^{\nu-2}+\nu\ell^{\nu-1}\right\}} \\ &= \ell^{\ell-2+(\ell-1)\left\{\nu\ell^{\nu-1}-1-\frac{\ell^{\nu-1}-1}{\ell-1}\right\}} \\ &= \ell^{\ell-2+(\ell-1)\nu\ell^{\nu-1}-(\ell-1)-\ell^{\nu-1}+1} \\ &= \ell^{\ell^{\nu-1}(\nu\ell-\nu-1)}. \end{aligned}$$

b.) $\ell = 2$.

Dann setzen wir also $\nu \geqq 2$ voraus und haben die Führer der Charaktere von $\mathfrak{I}_0(2^\nu)$ zu untersuchen. Für den Fall $\nu = 2$ hat $\mathfrak{I}_0(4)$ nur $\varphi(4) = 2$ Klassen, die für positive a durch

$$a \equiv 1, 3 \mod 4$$

repräsentiert werden. Außer dem Hauptcharakter existiert nur noch der Charakter

$$\chi(a) = (-1)^b$$

wenn $a \equiv (-1)^b \mod 4$,

der ersichtlich den Führer 4 hat. Also ist hier

$$d = 4,$$

entsprechend der bekannten Tatsache das der Körper $R(\sqrt{-1})$ der 4ten Einheitswurzeln die Diskriminante -4 hat.

Sei also $\nu \geqq 3$. Dann lassen sich die primen Restklassen mod 2^ν eindeutig in der Form darstellen

$$a \equiv (-1)^b 5^c \mod 2^\nu$$

wo $b \mod 2$ und $c \mod 2^{\nu-2}$ eindeutig bestimmt sind. Dem entsprechen die Charaktere

$$\chi(a) = (-1)^{bb'}\omega^{cc'} \tag{8}$$

wo ω eine primitive $2^{\nu-2}$–te Einheitswurzel ist. Soll ein solches $\chi(a)$ für alle Restklassen $a \mod 2^{\nu-1}$ gleich 1 sein, so folgt sofort, daß $b', c' \mod 2$ und

mod $2^{\nu-2}$ Null sein müssen. Daher liefert (8) genau $2 \cdot 2^{\nu-2} = \varphi(2^\nu)$ verschiedene Charaktere, und somit alle Charaktere von $\mathfrak{J}_0(2^\nu)$, wenn b', c' volle Restsysteme mod 2, mod $2^{\nu-2}$ durchlaufen.

Vom Führer 1 existiert wie oben wieder nur 1 Charakter, der Hauptcharakter, vom Führer 2 gar keiner, da dieser Charakter von $\mathfrak{J}_0(2)$ also $\mathfrak{J}_0(1)$ sein müßte, also der Hauptcharakter vom Führer 1. Vom Führer 4 existiert genau ein Charakter, da dieser Charakter von $\mathfrak{J}_0(4)$ sein muß, also nach obigem der Charakter $(-1)^b$ ist. Sei nun $\mu \geqq 3$ und suchen wir die Charaktere vom Führer 2^μ.

Aus $a \equiv 1 \mod 2^\mu$ folgt $\left\{ \begin{array}{l} b \equiv 0 \mod 2 \\ c \equiv 0 \mod 2^{\mu-2} \end{array} \right\}$ und umgekehrt. Soll daher $\chi(a) = 1$ für $a \equiv 1 \mod 2^\mu$ sein, so muß für alle $\left\{ \begin{array}{l} b \equiv 0 \mod 2 \\ c \equiv 0 \mod 2^{\mu-2} \end{array} \right\}$:

$cc' \equiv 0 \mod 2^{\nu-2}$,

176 II

also

$$c' \equiv 0 \mod 2^{\nu-\mu} \tag{9}$$

sein. Da umgekehrt hieraus $\chi(a) = 1$ für $a \equiv 1 \mod 2^\mu$ folgt, hat für $\mu \geqq 3$ $\chi(a)$ dann und nur dann den Führer 2^μ, wenn außer (9) noch

$$c' \not\equiv 0 \mod 2^{\nu-(\mu-1)} \tag{10}$$

ist. Das gibt für c' genau $2^{\mu-3}$ Möglichkeiten, wie genau wie oben erkannt wird, also weil b' jedesmal 2 Möglichkeiten hat, genau $2^{\mu-2}$ Möglichkeiten. Wir haben demnach insgesamt:

1	Charakter	vom	Führer	1
0	Charaktere	II	II	2
1	II	II	II	$4 = 2^2$
2	II	II	II	$8 = 2^3$
.....				
$2^{\nu-2}$	II	II	II	2^ν,

sodaß also Gesamtsumme richtig $1+2^{\nu-1}-1=2^{\nu-1}=\varphi(2^\nu)$ herauskommt. Das Produkt aller Führer ist dann:

$$\begin{aligned}|d| &= 2^{2+3\cdot 2+4\cdot 2^2+\cdots+\nu\cdot 2^{\nu-2}} = 2^{2+3(2^2-2)+4(2^3-2^2)+\cdots+\nu(2^{\nu-1}-2^{\nu-2})}\\ &= 2^{2-3\cdot 2-2^2-3^3-\cdots-2^{\nu-2}+\nu 2^{\nu-1}}\\ &= 2^{-1-1-2-\cdots-2^{\nu-2}+\nu 2^{\nu-1}} = 2^{\nu 2^{\nu-1}-1-2^{\nu-1}+1}\\ &= 2^{2^{\nu-1}(\nu-1)} = 2^{2^{\nu-1}(2\nu-\nu-1)}.\end{aligned}$$

Es resultiert somit dieselbe Formel, wie für ungerades ℓ.

Da schließlich der Körper der m–ten Einheitswurzeln stets total imaginär, d. h. $r_2=\frac{1}{2}\varphi(m)$ ist, ist das Vorzeichen $(-1)^{r_2}$ von d gleich $(-1)^{\frac{1}{2}\varphi(m)}$.

177 II

Satz 56. Die Diskriminante d von K_{2^ν}, wobei $\nu\geqq 1$, für $\ell=2$ jedoch $\nu\geqq 2$ ist, hat den Wert

$$d=(-1)^{\frac{1}{2}\varphi(\ell^\nu)}\ell^{\nu\varphi(\ell^\nu)-\frac{\varphi(\ell^\nu)}{\ell-1}}$$

Allgemein ist für $m=\prod_k \ell_k^{\nu_k}$, wenn nur der Exponent von 2 mindestens 2 ist, wenn 2 unter den ℓ_k vorkommt:

$$d=(-1)^{\frac{1}{2}\varphi(m)}m^{\varphi(m)}\prod_k \ell_k^{-\frac{\varphi(m)}{\ell_k-1}}$$

Beweis: 1.) Für $m=\ell^\nu$ folgt die obige Darstellung unmittelbar aus unseren Resultaten von a.) und b.), weil für jedes ℓ

$$\ell^{\nu-1}(\nu\ell-\nu-1)=\nu\ell^{\nu-1}(\ell-1)-\ell^{\nu-1}=\nu\varphi(\ell^\nu)-\frac{\varphi(\ell^\nu)}{\ell-1}$$

ist.

2.) Ist $m=\prod_k \ell_k^{\nu_k}$, wobei für ungerades ℓ_k: $\nu_k\geqq 1$, für $\ell_k=2$: $\nu_k\geqq 2$ sein soll, so ist nach Satz 54 und 3.) S. 168 der Körper K_m komponiert aus den Körpern $K_{\ell_k^{\nu_k}}$ mit den in Satz 54 genannten Eigenschaften. Nun gilt (A. Z. I) für die Diskriminante eines aus solchen Körpern komponierten Körpers:

$$|d|=|d_1|^{\frac{n}{n_1}}|d_2|^{\frac{n}{n_2}}\cdots|d_t|^{\frac{n}{n_t}}$$

wenn $n=n_1\cdots n_t$ das Produkt der Grade der $K_{\ell_k^{\nu_k}}$ ist. Hier ist

$$n_k=\varphi(\ell_k^{\nu_k}),$$

$$n=\varphi(m)\,;\qquad \frac{n}{n_k}=\varphi\left(\frac{m}{\ell_k^{\nu_k}}\right)$$

178 II

also

$$\begin{aligned} |d_k|^{\frac{n}{n_k}} &= (\ell_k^{\nu_k})^{\varphi(\ell_k^{\nu_k})\varphi\left(\frac{m}{\ell_k^{\nu_k}}\right)} \cdot \ell_k^{-\frac{\varphi(\ell_k^{\nu_k})}{\ell_k-1}\cdot\varphi\left(\frac{m}{\ell_k^{\nu_k}}\right)} \\ &= (\ell_k^{\nu_k})^{\varphi(m)} \cdot \ell_k^{-\frac{\varphi(m)}{\ell_k-1}}, \end{aligned}$$

somit

$$|d| = m^{\varphi(m)} \prod_k \ell_k^{-\frac{\varphi(m)}{\ell_k-1}}$$

und das Vorzeichen nach obigem $\frac{1}{2}\varphi(m)$, w. z. b. w.

Bekanntlich sind die Gruppen $\mathfrak{J}_0(\ell^\nu)$ für ungerades ℓ zyklisch, weil die Restklassengruppe mod ℓ^ν, mit der $\mathfrak{J}_0(\ell^\nu)$ isomorph ist, zyklisch ist. Für ungerades ℓ ist also K_{ℓ^ν} zyklisch. Für $\ell = 2$ ist die Restklassengruppe mod 2^ν ($\nu \geqq 3$) dagegen die Diedergruppe für ein reguläres $2^{\nu-2}$–Eck, d. h. K_{2^ν} nicht zyklisch, aber zusammengesetzt aus einem zyklischen Körper $2^{\nu-2}$–ten Grades und einem zyklischen Körper 2–ten Grades. Dem letzteren muß offenbar der zyklische Bestandteil der Restklassengruppe, d. h. die ihn erzeugende Klassengruppe

$$a \equiv 1 \mod 4$$

zugeordnet sein, die mit dem anderen□□□ Bestandteil

$$a \equiv \pm 1 \mod 2^\nu \qquad \text{mit zyklischer Faktorgruppe}$$

zusammen als Durchschnitt die Hauptklasse von $\mathfrak{J}_0(2^\nu)$ ergibt. Es ist mithin der zyklische Körper 2–ten Grades der nach Satz 53 der Klassengruppe $a \equiv 1 \mod 4$, also der Klasseneinteilung $\mathfrak{J}_0(4)$ zugeordnete Körper $R(i)$ der 4–ten Einheitswurzeln.

179 II

Satz 57. Der Körper K_{ℓ^ν} der ℓ^ν–ten Einheitswurzeln ist für ungerade Primzahlen ℓ zyklisch vom Grade $\varphi(\ell^\nu)$, für $\ell = 2$ ($\nu \geqq 3$) dagegen komponiert aus einem zyklischen Körper $2^{\nu-2}$–ten Grades und dem quadratischen Körper $R(\sqrt{-1})$.

Wir haben nun noch die Zerlegung der Diskriminantenteiler von K_m, d. h. der Teiler von m zu untersuchen. Hierzu wenden wir Satz 44 an. Die Gruppe

aller Charaktere χ von $\mathfrak{J}_0(m)$, deren Führer prim zu einem Teiler ℓ von m sind, ist offenbar die Gruppe X_ℓ der Charaktere von $\mathfrak{J}_0\left(\frac{m}{\ell^\nu}\right)$, wenn ℓ^ν genau in m aufgeht. Denn erstens sind alle Charaktere von $\mathfrak{J}_0\left(\frac{m}{\ell^\nu}\right)$ auch Charaktere von $\mathfrak{J}_0(m)$, und zwar solche, deren Führer prim zu ℓ sind, weil es $\frac{m}{\ell^\nu}$ ist. Ist zweitens χ ein Charakter, dessen Führer prim zu ℓ ist, so muß dieser Führer sogar Teiler von $\frac{m}{\ell^\nu}$ sein. χ ist also Restklassencharakter mod $\frac{m}{\ell^\nu}$, also (für pos. Argumente) Charakter von $\mathfrak{J}_0\left(\frac{m}{\ell^\nu}\right)$. Die charakteristischen Zahlen e, f, g der Zerlegung:

$$\ell = (L_1 \ldots L_g)^e; \quad \text{Grad}\, f\,; \quad efg = \varphi(m)$$

bestimmen sich also so:

$$f \quad \text{ist der kleinste Exponent, sodaß} \quad \ell^f \equiv 1 \mod \frac{m}{\ell^\nu}$$

$$e = (X : X_\ell) = \frac{\varphi(m)}{\varphi\left(\frac{m}{\ell^\nu}\right)} = \varphi(\ell^\nu) = \ell^{\nu-1}(\ell - 1)$$

180 II

$$g = \frac{\varphi(m)}{ef} = \frac{\varphi\left(\frac{m}{\ell^\nu}\right)}{f}\,.$$

Überdies ist die Klasseneinteilung $\mathfrak{J}_0\left(\frac{m}{\ell^\nu}\right)$ die dem Trägheitskörper von ℓ zugeordnete, also $K_{\frac{m}{\ell^\nu}}$ der Trägheitskörper für ℓ.

Satz 58. Geht ℓ in m genau zur ν–ten Potenz auf, und wird $m = \ell^\nu m_0$ gesetzt, ist ferner f der kleinste Exponent, für den

$$\ell^f \equiv 1 \mod m_0$$

ist, und

$$g = \frac{\varphi(m_0)}{f}\,,$$

so zerfällt ℓ in K_m in g Primteiler f–ten Grades von der Ordnung $e = \varphi(\ell^\nu)$. K_{m_0} ist der Trägheitskörper für ℓ.

181 II

B. Der Fundamentalsatz für absolut–Abelsche Körper

Sei K ein absolut–Abelscher Körper mit der Diskriminante d. Dann ist K nach dem Takagischen Hauptsatz Klassenkörper für eine Kongruenzklassengruppe $\mathsf{H}(m)$ in R, deren Führer m alle und nur die Primteiler von d enthält. In dieser Klassengruppe $\mathsf{H}(m)$ ist sicher die engste Klassengruppe mod m, nämlich die Hauptklasse von $\mathfrak{J}_0(m)$ als Untergruppe enthalten. Also ist K sicher Unterkörper des zugehörigen Klassenkörpers K_m der m–ten Einheitswurzeln.

Satz 59. Jeder absolut–Abelsche Körper ist Unterkörper eines Kreiskörpers, alle absolut–Abelschen Zahlen also rationale Funktionen einer genügend hohen m–ten Einheitswurzel; m kann zudem so gewählt werden, daß es nur die Primteiler der Diskriminante d von K enthält. Die Zerlegung der rationalen Primzahlen p in K hängt nur von Restklasse ab, der $p \mod m$ angehört, oder falls p ein Teiler von m, der p nach einem durch Wegdivision von p aus m entstehenden Modul m_0 angehört.

Letzteres folgt unmittelbar aus dem allgemeinen Zerlegungssatz für den Klassenkörper. Die Nebengruppen zu H sind eben gewisse Restklassenkomplexe mod m

182 II

und für den Fall, daß $p|m$ sind die Gruppen H_p Klassengruppen nach einem gewissen zu p primen Teiler m_0 von m.

Die *Diskriminante* jedes absolut Abelschen Körpers läßt sich, wenn man die zugehörige Klassengruppe H kennt, unmittelbar nach Satz 42 berechnen.

Über die *Klassenzahl* absolut–Abelscher Körper, speziell auch der eigentlichen Kreiskörper siehe mein Tagebuch **I**, S. 44 ff.

183 II

C. Quadratische Körper.

Sei χ ein quadratischer Restklassencharakter vom Führer f, d. h. ein solcher, dessen Quadrat der Hauptcharakter ist. Durch $\chi(a) = 1$ wird dann eine Untergruppe von $\mathfrak{Z}(f)$ vom Index 2 definiert, da nur die beiden Nebengruppen $\chi(a) = +1$ und $\chi(a) = -1$ existieren können. Denn χ^2 ist 1 also $\chi = \pm 1$, und es gibt sicher a mit $\chi(a) = -1$, wenn χ nicht der Hauptcharakter, was wir ausschließen wollen.

Je nachdem $\chi(-1) = +1$ ist oder nicht, ist χ ein Charakter von $\mathfrak{I}(f)$ oder nicht. Im letzteren Falle ist dann

$$(-1)^b\chi(a) \qquad \text{für} \quad a = (-1)^b|a|$$

ein Charakter von $\mathfrak{I}_0(f)$, da er für alle mod f kongruenten Zahlen gleichen Vorzeichens denselben Wert hat, und für $\pm a$ übereinstimmt.

Auf alle Fälle wird also

$$\chi_0\big((a)\big) = \big(\chi(-1)\big)^b\chi(a)$$

ein Idealcharakter von $\mathfrak{I}_0(f)$, der quadratisch ist, somit eine Idealgruppe vom Index 2 in R definiert. Zu ihr gehört ein quadratischer Klassenkörper $R(\sqrt{d})$. (Umgekehrt erhält man nach dem Fundamentalsatz über Abelsche Körper so auch jeden quadratischen Körper). Die Diskriminante von $R(\sqrt{d})$, wird dem Betrage

184 II

nach durch

$$|d| = \prod_{\chi_0} f(\chi_0) = f$$

gegeben, weil eben nur der eine Charakter χ_0 vom Führer f für unsere Klasseneinteilung existiert.

Ferner folgt nach den Überlegungen von S. 146▶/48▶, weil hier $r_1 = 1$, also $n_1 = \nu^{(1)}$; $n_2 = \nu^{(2)}$ ist,

$$\begin{aligned} \nu^{(1)} = R_1 + R_2 &= \begin{cases} 2, & \text{wenn} \quad d > 0 \\ 1, & \text{"} \quad\ d < 0 \end{cases} \\ \nu^{(2)} = R_2 &= \begin{cases} 0, & \text{wenn} \quad d > 0 \\ 1, & \text{"} \quad\ d < 0\,. \end{cases} \end{aligned}$$

Nun ist offenbar nach Definition der $\nu^{(1)}, \nu^{(2)}$

$\left.\begin{matrix}\nu^{(1)} = 2 \\ \nu^{(2)} = 0\end{matrix}\right\}$, wenn χ_0 reiner Restklassencharakter, also für $\chi(-1) = +1$

$\left.\begin{matrix}\nu^{(1)} = 1 \\ \nu^{(2)} = 1\end{matrix}\right\}$, wenn χ_0 einen echten Vorzeichencharakter enthält, also für $\chi(-1) = -1$.

Daher folgt:

Satz 60. Die Diskriminante des durch den quadratischen Restklassencharakter χ vom Führer f erzeugten quadratischen Körpers $R(\sqrt{d})$ hat den Wert

$$d = \chi(-1)f.$$

Der Satz 43a über Gausssche Summen ergibt hier, daß die Summe

185 II

$$G(\chi) = \sum_r \chi_0\big((r)\big)e^{2\pi i\frac{r}{f}},$$

wo r ein volles Restsystem positiver Zahlen mod f durchläuft, den Wert

$$G(\chi) = i^\nu\sqrt{f}$$

hat, wo $\nu = 0$ oder 1 je nachdem $\chi(-1) = +1$ oder -1, sodaß man auch

$$G(\chi) = \sqrt{\chi(-1)f}$$

schreiben kann, wo die Quadratwurzel positiv oder positiv imaginär zu nehmen ist. In $G(\chi)$ darf ferner $\chi_0\big((r)\big)$ durch $\chi(r)$ ersetzt werden, weil $r > 0$ angenommen wird. Nach Satz 30 folgt somit wegen $\overline{\chi} = \chi$:

$$G(n,\chi) = \chi(n)\sqrt{\chi(-1)f},$$

wo

$$G(n,\chi) = \sum_r \chi(r)e^{2\pi i\frac{nr}{f}}$$

gesetzt ist.

Satz 61. Die mit einem quadratischen Restcharakter χ vom Führer f gebildete Summe

$$G(n,\chi) = \sum_r \chi(r)e^{2\pi i\frac{nr}{f}},$$

wo r ein volles, positives Restsystem mod f durchläuft und n eine beliebige ganze Zahl ist, hat den Wert

$$G(n,\chi) = \chi(n)\sqrt{\chi(-1)f},$$

wo die Quadratwurzel positiv oder positiv imaginär ist.

186 II

Damit ist die wichtige Vorzeichenbestimmung der Gaussschen Summen in R (in üblichem Sinne) geleistet.

Wenn wir die anderweitig bekannte Tatsache brauchen, daß die Diskriminante d eines quadratischen Körpers durch ungerade Primzahlen p höchstens zur ersten und durch 2 höchstens zur dritten Potenz aufgeht, folgt dasselbe für den Führer f jedes quadratischen Restklassencharakters aus Satz 60. Dies läßt sich aber auch direkt einsehen. Ist nämlich

$$a \equiv 1 \mod 2^3 p_1 \dots p_t \tag{1}$$

so ist bekanntlich a Quadratzahl im Bereich von $2^3 p_1 \dots p_t$, also

$$a \equiv a_0^2 \mod 2^\nu p_1^\nu \dots p_t^{\nu_t} \tag{2}$$

für irgendwelche $\nu \geqq 3, \nu_1, \dots, \nu_t \geqq 1$. Hätte also χ den Führer $2^\nu p_1^{\nu_1} \dots p_t^{\nu_t}$, d. h. folgte aus (2)

$$\chi(a) = \chi(a_0^2) = \chi(a_0)^2 = 1 \tag{3}$$

so folgte (3) auch schon aus (1), d. h. der Führer wäre doch höchstens $2^3 p_1 \dots p_t$. Damit ist auf anderem Wege bewiesen:

Satz 62. Die Diskriminante eines quadratischen Körpers ist durch kein Quadrat außer 2, und durch 2 höchstens zur zweiten oder dritten Potenz teilbar (Satz 52).

187 II

Für den Beweis des quadratischen Reziprozitätsgesetzes benutzen wir folgende Richtlinien:

Nach dem Zerlegungssatz für den Klassenkörper ist die Zerfällung der rationalen, zu d primen Primzahlen p allein von der Klasse abhängig, der sie bei unserer durch χ erzeugten Klasseneinteilung angehören, d. h. da wir uns auf positive p beschränken können, von dem Werte $\chi(p)$. Andererseits ist nach dem Zerlegungsgesetz für Kummersche Körper das Symbol $\left(\frac{d}{p}\right)$ maßgebend. Da beide Symbole nur ± 1 sein können, folgt:

Satz 63. Für positive, zu d prime Primzahlen p ist

$$\chi(p) = \left(\frac{d}{p}\right),$$

d. h. das Symbol $\left(\frac{d}{p}\right)$ nur von der Restklasse abhängig, der $p \mod d$ angehört. Dieser Satz ist als der Hauptinhalt des quadratischen Reziprozitätsgesetzes anzusehen. Die bekannte Formulierung erhalten wir dann durch anderweitige Aufstellung von χ vermöge seiner Eigenschaft als quadratischer Restklassencharakter. Wir beweisen zuerst den ersten Ergänzungssatz. Dazu wählen wir $f = 4$. Dann existiert nur ein quadratischer Restklassencharakter χ, nämlich

$$\chi(a) = (-1)^b, \quad \text{wenn} \quad a \equiv (-1)^b \mod 4,$$

(s. S. 174), oder auch

$$\chi(a) = (-1)^{\frac{a-1}{2}}, \quad \text{für} \quad (a, 2) = 1.$$

188 II

So folgt also aus Satz 60:

$$(-1)^{\frac{p-1}{2}} = \left(\frac{4\chi(-1)}{p}\right) = \left(\frac{-1}{p}\right)$$

d. h. der erste Ergänzungssatz.

Für den zweiten Ergänzungssatz wählen wir $f = 8$. Für den Führer 8 existieren nach S. 176 nur zwei Restklassencharaktere überhaupt. Diese sind nach den dortigen Entwicklungen

$$\left.\begin{array}{l}\chi_1(a) = (-1)^c \\ \chi_2(a) = (-1)^{b+c}\end{array}\right\} \text{wenn} \quad a \equiv (-1)^b 5^c \mod 8$$

Der erstere ist offenbar

$$\chi_1(a) = (-1)^{\frac{a^2-1}{8}} \quad \text{für} \quad (a, 2) = 1,$$

der zweite entsteht hieraus durch Multiplikation mit dem vorhin betrachteten Charakter $(-1)^{\frac{a-1}{2}} \mod 4$, und ist

$$\chi_2(a) = (-1)^{\frac{a-1}{2}+\frac{a^2-1}{8}} \quad \text{für} \quad (a, 2) = 1.$$

Beide Charaktere sind ersichtlich quadratisch. Es ist ferner

$$\begin{array}{lllll}\chi_1(-1) = & 1, & \text{also} & d = & 8 \\ \chi_2(-1) = & -1, & \text{II} & d = & -8\end{array}$$

Aus Satz 60 folgt also:

$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)$$
$$(-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}} = \left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right),$$

d. h. der zweite Ergänzungssatz.

Für das allgemeine Reziprozitätsgesetz wählen wir $f = q$, wo q eine ungerade Primzahl ist. Der Charakter

$$\chi(a) = \left(\frac{a}{q}\right); \qquad (q, a) = 1$$

ist ersichtlich ein Restklassencharakter mod q, da er nur von der Restklasse $a \mod q$ abhängt, ferner quadratisch. Nun hat die Gruppe der primen Restklassen mod q nach der Primzahl 2 den Rang 1 (K. K., Satz 27, S. 94), also nur eine Untergruppe vom Index 2; es muß daher $\chi(a) = \left(\frac{a}{q}\right)$ Charakter für diese Untergruppe sein und ist der einzige quadratische Restklassencharakter vom Führer q.

Wegen

$$\chi(-1) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$$

ist

$$d = (-1)^{\frac{q-1}{2}} q,$$

entsprechend der bekannten Tatsache, daß ein ungerades $d \equiv 1 \mod 4$ sein muß. Aus Satz 60 folgt dann

$$\chi(p) = \left(\frac{p}{q}\right) = \left(\frac{d}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

d. h. das quadratische Reziprozitätsgesetz.

Satz 61. Das quadratische Reziprozitätsgesetz und seine beiden Ergänzungssätze in R, die ihren Hauptinhalt in Satz 60 haben, folgen in einfachster Weise durch Aufstellung der quadratischen Restklassencharaktere von den Führern

$4, 8, q$.

190 II

Es interessiert noch der allgemeinste Ausdruck für einen quadratischen Restklassencharakter vom Führer f. Sei entsprechend Satz 62

$$f = 2^\nu p_1 \dots p_t\,; \qquad (\nu = 0, 2 \text{ oder } 3).$$

Dann setzen wir mit Exponenten $c_k = 0, 1$:

$$\chi(a) = (-1)^{c\frac{a-1}{2}} (-1)^{c'\frac{a^2-1}{8}} \left(\frac{a}{p_1}\right)^{c_1} \cdots \left(\frac{a}{p_t}\right)^{c_t}$$

für $(a, f) = 1$. Dabei sollen sinngemäß c und c' je nach dem Wert von ν Null sein:

$$\begin{array}{rrrl} \text{für} & \nu = 0 & : & c = c' = 0 \\ \text{II} & \nu = 2 & : & c' = 0 \\ \text{II} & \nu = 3 & : & c, c' \quad \text{beliebig.} \end{array}$$

Diese 2^t, 2^{t+1}, 2^{t+2} Charaktere $\chi(a)$ sind sämtlich Restklassencharaktere mod f und quadratisch. Soll ein $\chi(a)$ für alle primen Restklassen mod f gleich 1 sein, so müssen alle Exponenten c_k verschwinden, da man sonst stets leicht ein a finden kann, für das $\chi(a) \neq 1$. Daher sind die $2^t, 2^{t+1}, 2^{t+2}$ Charaktere $\chi(a)$ alle verschieden, und außer dem Hauptcharakter in der Anzahl

$$2^t - 1 \quad \text{etz.}$$

vorhanden. Andererseits ist nach K. K. Satz 27/28, S. 94/96 der Rang der Gruppe der primen Restklassen mod f:

$$t,\ t+1,\ t+2$$

also die Anzahl der Untergruppen vom Index 2:

$$2^t - 1 \quad \text{etz.}$$

191 II

Daher existieren auch nicht mehr quadratische Restklassencharaktere mod f

Ist nun einer der Exponenten $c_k = 0$, so ist der Führer von $\chi(a)$ ersichtlich kleiner als f, (sinngemäß auch für c, c': hier muß für f genau durch 4 teilbar $c \neq 0$, für f genau durch 8 teilbar c beliebig, $c' \neq 0$ sein).

Somit folgt:

Satz 62. Ist $f = 2^\nu p_1 \dots p_t$; ($\nu = 0, 2$ oder 3) ein beliebiger Körper, so gibt es im Falle $\nu = 0$ zu ihm nur den einen quadratischen Restklassencharakter:

$$\chi(a) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_t}\right) = \left(\frac{a}{f}\right)$$

Für $\nu = 2$ und $f = 4f_0$ gibt es ebenfalls nur den einen quadratischen Restklassencharakter:

$$\chi(a) = \left(\frac{a}{f_0}\right) \cdot (-1)^{\frac{a-1}{2}} = \left(\frac{a}{f_0}\right)\left(\frac{-1}{a}\right)$$

dagegen für $\nu = 3$ und $f = 8f_0$ die beiden:

$$\begin{aligned} \chi_1(a) &= \left(\frac{a}{f_0}\right)(-1)^{\frac{a^2-1}{8}} = \left(\frac{a}{f_0}\right)\left(\frac{2}{a}\right) \\ \chi_2(a) &= \left(\frac{a}{f_0}\right)(-1)^{\frac{a-1}{2}+\frac{a^2-1}{8}} = \left(\frac{a}{f_0}\right)\left(\frac{-2}{a}\right), \end{aligned}$$

wo die Symbole *Jacobische Symbole* sind.

Für die Diskriminanten der entsprechenden quadratischen Körper folgt:

a.) f *ungerade.*

$$\chi(-1) = \left(\frac{-1}{f}\right); \qquad d = \left(\frac{-1}{f}\right) f$$

also wie bekannt: $d \equiv 1 \mod 4$

b.) f *genau durch* 4 *teilbar* $= 4f_0$

$$\chi(-1) = \left(\frac{-1}{f_0}\right)(-1)^{\frac{-1-1}{2}} = -\left(\frac{-1}{f_0}\right) = -\left(\frac{-1}{f}\right)$$

$$d = -\left(\frac{-1}{f}\right) f$$

d. h. d ist stets das 4 fache einer Zahl $\equiv 3 \mod 4$.

c.) f *genau durch* 8 *teilbar* $= 8f_0$

Hier sind $\chi_1(-1)$ und $\chi_2(-1)$ von verschiedenem Zeichen, also existieren 2 quadratischen Körper mit den Diskriminanten $d = \pm f$.

Satz 63. Auch die bekannten Tatsachen über die Diskriminanten quadratischer Körper ergeben sich unmittelbar aus der Betrachtung der Führer quadratischer Restklassencharaktere.

Über die Klassenzahl quadratischer Körper siehe mein Tagebuch **I**, S. 44 ff.

Kapitel 3

Reziprozitätsgesetz

Das allgemeine Reziprozitätsgesetz für ℓ–te Potenzreste in einem beliebigen algebraischen Körper. (Nach T. Takagi).

Überblick

3.1 §1 Die Charaktere nach einer Klassengruppe vom Index ℓ

193 III

Sei k ein beliebiger algebraischer Körper, der die ℓ–te Einheitswurzel ζ enthält, μ eine Zahl aus k die nicht ℓ–te Potenz einer Zahl aus k ist. Dann definiert $\sqrt[\ell]{\mu}$ einen relativ–zyklischen Körper ℓ–ten Grades über k, der Klassenkörper für eine Klassengruppe H vom Index ℓ in k ist. Die Zerlegung eines zur Relativdiskriminante von $k(\sqrt[\ell]{\mu})$, sicher also jedes zu μ und ℓ primen Primideals $\mathfrak{p}$ aus k wird dann durch das Legendresche Symbol $\left(\frac{\mu}{\mathfrak{p}}\right)$ bestimmt. Andererseits gilt das Zerlegungsgesetz für den Klassenkörper, wonach die Zerlegung von $\mathfrak{p}$ nur von der Klasse nach H abhängt, der $\mathfrak{p}$ angehört. Die Klassengruppe H kann nun eindeutig durch einen Klassencharakter $\chi(\mathfrak{a})$ charakterisiert werden, sodaß ein zur Relativdiskriminante primes $\mathfrak{a}$ dann und nur dann zu H gehört, wenn

$$\chi(\mathfrak{a}) = 1$$

ist. χ ist Charakter der Faktorgruppe nach H und

194 III

als solcher nur der Werte ζ^c fähig. Ferner ist jeder der $\ell - 1$ Nichthauptcharaktere $\chi, \chi^2, \ldots, \chi^{\ell-1}$ nach H mit χ gleichberechtigt.

Durch Vergleich der beiden Zerlegungsgesetze folgt für die genannten $\mathfrak{p}$:

$$\left(\frac{\mu}{\mathfrak{p}}\right) = 1 \quad \text{dann und nur dann, wenn} \quad \chi(\mathfrak{p}) = 1.$$

Satz 1. Ist μ eine Zahl aus k, die nicht ℓ–te Potenz einer Zahl aus k ist, χ ein vom Hauptcharakter verschiedener Charakter nach derjenigen Klassengruppe in k, für die $k(\sqrt[\ell]{\mu})$ Klassenkörper ist, so ist für ein zu μ und ℓ primes Primideal $\mathfrak{p}$ dann und nur dann

$$\left(\frac{\mu}{\mathfrak{p}}\right) = 1,$$

wenn $\chi(\mathfrak{p}) = 1$ ist.

Dieser Satz bildet die Grundlage für das allgemeine Reziprozitätsgesetz in k. Da $\left(\frac{\mu}{\mathfrak{p}}\right)$ und $\chi(\mathfrak{p})$ beide nur der Werte ζ^c fähig sind, liegt die Vermutung

nahe, daß man den Charakter $\chi(\mathfrak{p})$, der nach obigem noch mit einem beliebigen, zu ℓ primen Exponenten versehen werden darf, so normieren kann, daß sogar

$$\left(\frac{\mu}{\mathfrak{p}}\right) = \chi(\mathfrak{p})$$

wird, d. h. das Symbol $\left(\frac{\mu}{\mathfrak{p}}\right)$ nur von der Klasse nach H abhängt, der $\mathfrak{p}$ angehört. Diese Tatsache, die

195 III

als Hauptinhalt des Reziprozitätsgesetzes anzusehen ist, (für $\ell = 2$ ist sie übrigens schon in Satz 1 enthalten), sowie den weitergehenden folgenden Satz 2 werden wir zu beweisen haben:

Satz 2. Der Charakter χ von Satz 1 läßt sich so normieren, daß für alle zu μ und ℓ primen Ideale $\mathfrak{a}$:

$$\left(\frac{\mu}{\mathfrak{a}}\right) = \chi(\mathfrak{a})$$

gilt.

Um diesen Satz zu beweisen, haben wir vor allem die Gruppencharaktere χ nach einer Klassengruppe vom Index ℓ einer genaueren Untersuchung zu unterziehen, was zunächst geschehen soll.

Wir fragen also nach dem allgemeinen Ausdruck für die Charaktere χ nach Klassengruppen vom Index ℓ. Seien die Idealklassen in k zunächst nach dem Strahl o

$$\alpha \equiv 1 \mod m \qquad (\text{für } \ell = 2 \text{ total positiv})$$

definiert. Jede Untergruppe der so entstehenden Klassengruppe mod m vom Index ℓ enthält die sämtlichen ℓ–ten Potenzen von Klassen, sodaß wir jede solche Untergruppe auch schon erhalten, wenn wir die Idealklassen nach der Gruppe der ℓ–ten Potenzen der Klassen mod m definieren. Die Hauptklasse

196 III

besteht dann aus allen einer ℓ–ten Potenz nach o äquivalenten Idealen, d. h. allen Idealen:

$$(\alpha)j^{\ell}, \quad \text{wo} \quad \alpha \equiv 1 \mod m \quad (\text{f. } \ell = 2 \text{ tot. positiv})$$

An dieser Bedeutung von α soll in diesem § festgehalten werden. (Natürlich ist stets alles prim zu m anzunehmen).

□□□

Bezeichnet G die Gruppe der so definierten Idealklassen, so ist offenbar jeder Charakter χ von G Charakter nach einer Klassengruppe vom Index $\ell \mod m$ und umgekehrt.□□□
Denn ist χ ein Charakter von G, so ist

$$\chi(\mathfrak{a}^\ell) = \big(\chi(\mathfrak{a})\big)^\ell = 1$$

weil $\mathfrak{a}^\ell$ zur Hauptklasse von G gehört. χ hat also nur die ℓ Werte ζ^c, die Forderung $\chi(\mathfrak{a}) = 1$ definiert also, wenn χ nicht der Hauptcharakter, eine Klassengruppe vom Index $\ell \mod m$ nach der χ Charakter ist, wenn χ der Hauptcharakter ist er natürlich Charakter nach jeder Klassengruppe vom Index $\ell \mod m$. Ist umgekehrt χ Charakter nach einer Klassengruppe vom Index $\ell \mod m$, so ist $\chi\big((\alpha)j^\ell\big) = 1$, weil ja die Klasse von $(\alpha)j^\ell$ ℓ–te Potenz ist, also zur Klassengruppe

197 III

vom Index ℓ gehören muß. χ ist also für die Hauptklasse von G gleich 1, d. h. Charakter von G.

Satz 3. Ist G die Klassengruppe nach der Hauptklasse: „ℓ–te Potenzen von Klassen mod m (nach o)“, so ist jeder Charakter von G Charakter nach einer Klassengruppe vom Index $\ell \mod m$ (nach o) und umgekehrt.

Wir haben daher nur alle Charaktere von G aufzustellen. Der Grad von G ist offenbar $\ell^{\bar{t}}$, wenn $\bar{t}$ den in K. K. §2 definierten und näher bestimmten Rang der Klassengruppe nach o, oder was dasselbe ist, den Rang von G bezeichnet. Der Basisdarstellung von G (Rangbasisdarstellung der Gruppe der Klassen nach o) entsprechend läßt sich nun jedes zu m prime Ideal $\mathfrak{a}$ eindeutig in der Form darstellen:

$$\mathfrak{a} = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} (\eta_1^{z_1} \dots \eta_N^{z_N} \alpha) j^\ell; \qquad (\ell \text{ ungerade}) \tag{1}$$

$$\mathfrak{a} = {\mathfrak{r}_1}^{a_1} \dots \mathfrak{r}_t^{a_t} (\eta_1^{z_1} \dots \eta_N^{z_N} {\beta'_1}^{e_1} \dots {\beta'_p}^{e_p} \alpha) j^2; \qquad (\ell = 2). \tag{1a}$$

Siehe hierzu K. K. S. 101, (12.) u. S. 109, (12a.). Die Bezeichnungen seien dieselben wie da, jedoch hier die für $\ell = 2$ gewählte Vorzeichengruppe $\mathsf{V} = 1$, (o der Strahl der total–positiven Zahlen $\equiv 1 \mod m$), also $r_0 = 0$. Die Exponenten in dieser Darstellung sind eindeutig durch $\mathfrak{a}$ und natürlich

198 III

sogar schon durch die Klasse, der $\mathfrak{a}$ bei der Klasseneinteilung G angehört, eindeutig bestimmt, als Zahlen der Reihe $0, 1, \dots \ell - 1$.

Dieser Basisdarstellung (1) bezw. (1a) entnehmen wir zunächst folgende speziellen Charaktere von G:

$$\chi_i(\mathfrak{a}) = \zeta^{a_i}; \qquad (i = 1, 2, \dots, t) \tag{2}$$

Diese hängen nur von der absoluten Klasse von $\mathfrak{a}$ ab, und sollen daher *absolute Klassencharaktere* heißen.

Sodann haben wir weiter folgende speziellen Charaktere von G:

$$\psi_i(\mathfrak{a}) = \zeta^{z_i}; \qquad (i = 1, 2, \dots N)$$

und für $\ell = 2$ noch:

$$\varphi_i(\mathfrak{a}) = (-1)^{e_i}; \qquad (i = 1, 2, \dots, p).$$

Die so definierten $t + N$ bezw. $t + N + p$ speziellen Charaktere sind von einander unabhängig und ergeben nach allgemeinen Sätzen über Gruppencharaktere die sämtlichen $\ell^{\bar{t}} = \ell^{t+N}$ bezw. ℓ^{t+N+p} Gruppencharaktere für G durch Komposition. Sie bilden eine Basis der Gruppe aller $\ell^{\bar{t}}$ Charaktere von G. Für unsere Zwecke ist es vorteilhaft die Charaktere ψ und φ noch durch andere transformierte zu ersetzen, die mit dem *Legendreschen Symbol* und der *Signatur* in unmittelbarem

Zusammenhang stehen. Zu diesem Zweck ist auf die Bedeutung der η_i und β_i' aus K. K. einzugehen. Nach (10.), (11.) S. 101 in K. K. läßt sich jedes zu m prime β eindeutig in der Form:

$$\beta = \eta_1^{z_1} \dots \eta_N^{z_N} \gamma_1^{y_1} \dots \gamma_{N'}^{y_{N'}} \alpha \xi^{\ell} \qquad (z_i, y_i = 0, \dots \ell - 1) \tag{3}$$

darstellen, wo die $N + N' = R(m)$ Basiselemente η_i, γ_i ein vollständiges System unabhängiger Nichtreste mod m sind, und zwar ein solches, dessen Elemente $\gamma_1, \dots, \gamma_{N'}$ die sämtlichen aus dem dortigen System (6.) der Einheiten und ℓ–ten Idealpotenzen gewinnbaren unabhängigen Nichtreste sind.

Für $\ell = 2$ tritt an die Stelle von (3):

$$\beta = \eta_1^{z_1} \dots \eta_N^{z_N} \gamma_1^{y_1} \dots \gamma_{N'}^{y_{N'}} \beta_1'^{e_1} \dots \beta_p'^{e_p} \alpha_1'^{c_1} \dots \alpha'_{n-n_0}{}^{c_{n-n_0}} \alpha \xi^2 \tag{3a}$$

(K. K. S. 109), wo die η_i, γ_i dieselbe Bedeutung haben und die β_i', α_i' zusammen ein System quadratischer Reste mod m mit unabhängigen Signaturen

sind, also in der Anzahl r_1, dessen $n - n_0$ Elemente α'_i durch die unter den n unabhängigen quadratischen Resten des Systems (6.) von K. K. enthaltenen unabhängigen Signaturen geliefert werden.

Die Darstellungen (3), (3a) können durch andere äquivalente ersetzt werden:

$$\beta = \omega_1^{a_1} \dots \omega_d^{a_d} \prod_{\mathfrak{l}} \gamma_1'^{b_1} \dots \gamma_R'^{b_R} \alpha \xi^{\ell} \tag{4}$$

200 III

$$\beta = \omega_1^{a_1} \dots \omega_d^{a_d} \cdot \prod_{\mathfrak{l}} \gamma_1'^{b_1} \dots \gamma_R'^{b_R} \cdot \delta_1^{d_1} \dots \delta_{r_1}^{d_{r_1}} \alpha \xi^2 \tag{4a}$$

Dabei bedeuten die ω_i je einen Nichtrest für die d zu $\mathfrak{l}$ primen Primteiler $\mathfrak{p}_i$ von m, die γ'_i für jeden Teiler $\mathfrak{l}^g$ von ℓ und m ein System von $R(\mathfrak{l}^g)$ unabhängigen Nichtresten, und für $\ell = 2$ die δ_i ein System von Resten mod m, die für $k^{(i)}$ negativ, sonst positiv sind, und die einzelnen Systeme sollen so gewählt angenommen werden, daß sie für die Bereiche der übrigen Primstellen nach genügend hohen Potenzen 1, (bezw. positiv) sind, sodaß (4), (4a) als die aus den Basisdarstellungen für die einzelnen Primstellen komponierte Basisdarstellung der Restgruppe mod m (mit Vorzeichenbedingung) anzusehen ist.

Denkt man sich dann die zu m primen Ideale in der eindeutigen Form:

$$\mathfrak{a} = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} (\beta) j^{\ell} \tag{5}$$

dargestellt, und β in der Form (4), (4a), so resultieren folgende Charaktere für $\mathfrak{a}$, außer den schon genannten absoluten Klassencharakteren (1):*

$$\chi'_i(\mathfrak{a}) = \left(\frac{\beta}{\mathfrak{p}_i}\right) = \zeta^{a_i}; \qquad (i = 1, 2, \dots d), \tag{6}$$

$$\chi''_{\mathfrak{l},i}(\mathfrak{a}) = \zeta^{b_i}; \qquad (i = 1, 2, \dots R(\mathfrak{p}^g)); \tag{7}$$

$$\chi'''_i(\mathfrak{a}) = (-1)^{d_i} = \operatorname{sgn} \beta^{(i)}; \qquad (i = 1, 2, \dots r_1). \quad \text{für} \quad \ell = 2. \tag{8}$$

201 III

*wenn die ω_i geeignet normiert gewählt werden, was möglich

Da (3), (3a) sowohl wie (4), (4a) eindeutige Basisdarstellungen der Restgruppe mod m (für $\ell = 2$ mit Vorzeichenbedingung) bezüglich der Untergruppe der ℓ–ten Potenzreste sind, stehen die Exponenten von (3), (3a) mit denen von (4), (4a) in umkehrbar eindeutigem Zusammenhang.

Daher läßt sich einerseits jeder aus obigen Charakteren $\psi_i(\mathfrak{a})$ und $\varphi_i(\mathfrak{a})$ zusammengesetzte Charakter auch aus den Charakteren (6), (7) ev. (8) zusammensetzen. Umgekehrt läßt sich jedoch ein aus (6) – (8) zusammengesetzter Charakter dann und nur dann schon aus den unabhängigen Charakteren $\psi_i(\mathfrak{a})$ (ev. $\varphi_i(\mathfrak{a})$) zusammensetzen, wenn diejenigen Relationen erfüllt sind, die sich aus dem Nichtauftreten der den ℓ–ten Idealpotenzen γ_i und d_i' in (3), (3a) in dem allgemeinen Charakter von G ergeben, d. h. wenn das Kompositum χ aus (6) – (8) die Bedingungen erfüllt:

$$\chi(\gamma_i) = 1\,; \qquad (i = 1, 2, \dots N') \tag{9}$$

$$\chi(\alpha_i') = 1\,; \qquad (i = 1, 2, \dots n - n_0). \tag{9a}$$

Denn eine lineare Funktion der $a_i, b_i, (d_i)$ ist dann und nur dann schon linear durch die $z_i, (e_i)$ allein darstellbar, wenn sie verschwindet, wenn in die $a_i, b_i, (d_i)$, als lineare Funktionen der $z_i, y_i, (e_i, c_i)$ aufgefaßt, $z_i, (e_i) = 0$ und ein $y_i, (c_i) \neq 0$ eingesetzt wird.

Die Bedingungen (9), (9a) sondern aus den $\ell^{R(m)}$ bezw.

$2^{R(m)+r_1}$ Charakteren (6) – (8) und ihren komponierten genau $\ell^{N'}$ bezw. $2^{N'+(n-n_0)}$ aus, sodaß mit (1)

$$\ell^{t+R(m)-N'} = \ell^{t+N} = \ell^{\bar{t}}$$

bezw.
$$2^{t+R(m)+r_1-N'-(n-n_0)} = 2^{t+N+p} = 2^{\bar{t}}$$

Charaktere übrig bleiben, wie es sein muß, weil $\ell^{\bar{t}}$ der Rang von G, und auch der Grad von G ist. Daß diese genau Anzahl wirklich übrig bleibt, folgt entweder aus der Unabhängigkeit der Bedingungen (9), (9a) oder aber einfacher aus der ja bewiesenen Tatsache, daß jedes den Bedingungen (9), (9a) unterworfene Kompositum aus (6) – (8) ein Kompositum der $\psi_i(\mathfrak{a}), \varphi_i(\mathfrak{a})$ ist und umgekehrt, letztere aber nach Konstruktion genau in der Anzahl $\ell^{\bar{t}}$ vorhanden sind. Zusammenfassend haben wir also:

Satz 4. Man erhält die sämtlichen $\ell^{\bar{t}}$ Charaktere von G in der Form:

$$\chi(\mathfrak{a}) = \prod_{i=1}^{t} \zeta^{a_i u_i} \cdot \prod_{i=1}^{d} \left(\frac{\beta}{\mathfrak{p}_i}\right)^{v_i} \cdot \prod_{\mathfrak{l} \mid m} \prod_{i=1}^{R} \zeta^{b_i w_i} \cdot \left(\prod_{i=1}^{r_1} (\operatorname{sgn} \beta^{(i)})^{z_i} \right)$$

(für $\ell \neq 2$ fällt der letzte Faktor weg), wenn die Exponenten u, v, w, z den Bedingungen

$$\chi(\gamma_i) = 1\,; \qquad (i = 1, 2, \ldots, N')$$

und für $\ell = 2$ noch

$$\chi(\alpha_i') = 1\,; \qquad (i = 1, 2, \ldots, n - n_0)$$

unterworfen werden und außerdem natürlich Zahlen der Reihe $0, 1, \ldots \ell - 1$ sein sollen. Dabei ist für $\mathfrak{a}$ die

eindeutige Darstellung

$$\mathfrak{a} = \mathfrak{r}_1^{a_1} \ldots \mathfrak{r}_t^{a_t} (\beta) j^{\ell}$$

durch die Repräsentanten $\mathfrak{r}_i$ der absoluten, zu Exponenten ℓ^{ν} gehörigen Basisklassen zugrundegelegt. $\mathfrak{p}_i$ bedeutet die d zu ℓ primen Teiler von m, $\mathfrak{l}$ die in ℓ aufgehenden Teiler von m, $R = R(\mathfrak{l}^g)$ den Rang der Restklassengruppe mod $\mathfrak{l}^g$ und b_i die Exponenten bei der Darstellung von β durch ein System von R unabhängigen Nichtresten mod $\mathfrak{l}^g$. Schließlich sind die γ_i ein System unabhängiger Nichtreste aus dem System der Einheiten und ℓ–ten Idealpotenzen

$$\varepsilon_1^{x_1} \ldots \varepsilon_{r+1}^{x_{r+1}} \rho_1^{y_1} \ldots \rho_t^{y_t} \xi^{\ell}$$

und die α_i' ein System von quadratischen Resten aus diesem System mit unabhängigen Signaturen.

Durch diesen Satz ist nach dem schon gesagten unsere Aufgabe gelöst, einen allgemeinen Ausdruck für die Charaktere der Klassengruppen mod m vom Index ℓ zu finden. Die Charaktere (6), (7) sollen *Potenzcharaktere mod* $\mathfrak{p}_i$ *bezw. mod* $\mathfrak{l}^g$ heißen, die Charaktere (8) *Vorzeichencharaktere*. Natürlich sind die Charaktere (6) – (8) für sich nicht schon Charaktere von G, sondern nur solche Komposita von ihnen, die den Bedingungen von Satz 4 genügen.

3.2 §2 Der absolute Klassenkörper und die singulären Primärzahlen.

204 III

Der Rang der absoluten Klassengruppe, d. h. der Gruppe der Idealklassen in gewöhnlichem Sinne ist die im vorigen § angegebene Zahl t (siehe „Rangbasisdarstellung“ (5)). Nach den Resultaten von K. K., §4, A. existieren also genau t unabhängige Zahlen $\omega_1, \ldots, \omega_t$ derart, daß die Körper $k(\sqrt[\ell]{\omega_i})$ *absolute Klassenkörper* zu k sind, und daß jeder Klassenkörper zu einer absoluten Klassengruppe vom Index ℓ durch die ℓ–te Wurzel einer Zahl der Form

$$\omega = \omega_1^{u_1} \ldots \omega_t^{u_t} \xi^{\ell}\,; \qquad (u_i = 0, 1, \ldots \ell - 1) \tag{1}$$

definiert werden kann.

Da die Relativdiskriminante eines solchen absoluten Klassenkörpers gleich 1 sein muß ($m = 1$), können die ω_i durch kein Primideal zu nicht durch ℓ teilbarem Exponenten aufgehen, d. h. sind Einheiten oder ℓ–te Idealpotenzen. Sie müssen ferner nach den Primteilern von

$$\ell = \mathfrak{l}_1^{e_1} \ldots \mathfrak{l}_z^{e_z}$$

Kongruenzbedingungen genügen, die wir in die Bezeichnung *primär* zusammenfassen. Dabei verstehen wir unter einer primären Zahl ω eine solche, die *für alle Primteiler* $\mathfrak{l}_i$ *von* ℓ der Bedingung

205 III

$$\omega \equiv \xi^{\ell} \mod \mathfrak{l}_i^{\frac{e_i \ell}{\ell - 1} + a_i} \tag{2}$$

genügt, wenn ω genau durch $\mathfrak{l}_i^{a_i}$ teilbar ist. Es muß also nach Wegdivision der Primzahlpotenz $\lambda_i^{a_i}$, deren Exponent a_i notwendig durch ℓ teilbar sein muß, $\frac{\omega}{\lambda_i^{a_i}}$ ein ℓ–ter Potenzrest mod $\mathfrak{l}_i^{\frac{e_i \ell}{\ell - 1}}$ sein. Diese Bedingung ist bekanntlich notwendig und hinreichend dafür, daß die Relativdiskriminante von $k(\sqrt[\ell]{\omega})$ prim zu $\mathfrak{l}_i$ ist.

Wir nennen fortan eine ℓ–te Idealpotenz, die außerdem primär ist, eine *singuläre Primärzahl*. Dann definiert also jede singuläre Primärzahl ω einen

relativ–zyklischen Körper ℓ–ten Grades $k(\sqrt[\ell]{\omega})$, dessen Relativdiskriminante 1 ist. Für ungerades ℓ muß dieser also Klassenkörper zu einer Klassengruppe mod 1 ohne Vorzeichenbedingungen, d. h. zu einer absoluten Klassengruppe vom Index ℓ sein, d. h. nach dem Gesagten ω eine Zahl der Form (1).

Satz 5. Ist ℓ ungerade und t der Rang der absoluten Klassengruppe von k nach ℓ, so existieren t unabhängige singuläre Primärzahlen $\omega_1, \ldots, \omega_t$, sodaß sich jede singuläre Primärzahl ω eindeutig in der Form (1) darstellen läßt.

Für $\ell = 2$ ist noch auf die Signaturen der ω zu achten. Bei Zugrundelegung der absoluten Klasseneinteilung (ohne

206 III

Vorzeichenbedingungen) sind nach K. K., Satz 42a die t singulären Primärzahlen $\omega_1, \ldots, \omega_t$ total positiv. Ist umgekehrt ω eine total positive singuläre Primärzahl, so ist $k(\sqrt{\omega})$ nach den Ausführungen von K. K. S. 59 ff sicher ebenfalls Klassenkörper für eine absolute Klassengruppe *ohne* Vorzeichenbedingungen, also ω eine Zahl der Form (1).

Definieren wir nun die Idealklassen in k in absolutem, aber engeren Sinne, d. h. mit Vorzeichenbedingung „total positiv“, so wird der Rang der Idealklassengruppe nach 2 eine Vermehrung um eine gewisse Zahl t' erfahren (die Anzahl der Untergruppen vom Index 2 vermehrt sich ja). Zu dieser Klasseneinteilung existieren dann nach K. K. §4.A. genau $t + t'$ unabhängige singuläre Primärzahlen. Da die vorher gefundenen t eine Untergruppe von ihnen bilden, lassen sich nach dem Prinzip von K. K., Satz 25 also zu den schon genannten t singulären, total positiven Primärzahlen $\omega_1, \ldots, \omega_t$ noch t' weitere $\omega'_1, \ldots, \omega'_{t'}$ bestimmen, sodaß jede beliebige singuläre Primärzahl, da sie ja einen Klassenkörper zu einer absoluten Klassengruppe mit Vorzeichenbedingung definiert, sich eindeutig in der Form

$$\omega = \omega_1^{u_1} \ldots \omega_t^{u_t} {\omega'_1}^{u'_1} \ldots {\omega'_{t'}}^{u'_{t'}} \xi^2 ; \qquad (u_i, u'_i = 0, 1) \tag{3}$$

darstellen läßt. Die hinzutretenden singulären Primärzahlen $\omega'_1, \ldots, \omega'_{t'}$ müssen dann unabhängige Signaturen

207 III

haben. Denn wäre ein Produkt aus ihnen total positiv, so wäre es nach obigem schon in der Form (1) darstellbar entgegen der Eindeutigkeit von (3).

Satz 6. Für $\ell = 2$ möge die absolute Klassengruppe bei Einführung der Vorzeichenbedingung „total positiv“ einen Rangzuwachs um t' erfahren. Dann

existieren $t + t'$ unabhängige singuläre Primärzahlen $\omega_1, \ldots, \omega_t; \omega'_1, \ldots, \omega'_{t'}$, von denen die t ersten total positiv sind, die t' letzten unabhängige Signaturen haben, sodaß jede singuläre Primärzahl ω eindeutig in der Form (3) darstellbar ist.

Die singulären Primärzahlen sind als ℓ–te Idealpotenzen sicher Zahlen des Systems:

$$\varepsilon_1^{x_1} \ldots \varepsilon_{r+1}^{x_{r+1}} \rho_1^{y_1} \ldots \rho_t^{y_t} \xi^\ell, \tag{4}$$

wo die ε, ρ die bekannte Bedeutung haben (K. K., S. 99). Es gilt nämlich:

Satz 7. Jede Zahl $\gamma = \mathfrak{a}^\ell$ aus k ist im System (4) enthalten.

Beweis: Siehe den für das dortige j^ℓ in K. K. S. 102/103 geführten Beweis.

Für ungerades ℓ lassen sich daher nach dem Prinzip von Satz 25 in K. K. noch $r+1$ ℓ–te Idealpotenzen $\eta_1, \ldots, \eta_{r+1}$ finden, sodaß die Gruppe (4) aller ℓ–ten Idealpotenzen die eindeutige Basisdarstellung:

$$\eta_1^{v_1} \ldots \eta_{r+1}^{v_{r+1}} \omega_1^{u_1} \ldots \omega_t^{u_t} \xi^\ell; \qquad (u_i, v_i = 0, 1, \ldots \ell - 1) \tag{5}$$

hat. Da es auf Faktoren ξ^ℓ nicht ankommt, dürfen übrigens die η, ω sämtlich prim zu ℓ angenommen werden. Da die ω eindeutig als Basis der Gruppe der primären ℓ–ten Idealpotenzen, d. h. der Gruppe der ℓ–ten Idealpotenzen, die ℓ–te Potenzreste nach dem Modul $\prod_i \mathfrak{l}_i^{\frac{e_i \ell}{\ell-1}} = \ell^{\frac{\ell}{\ell-1}}$ sind (sie sollen ja prim zu ℓ sein), bestimmt sind, sind dann also die $\eta_1, \ldots, \eta_{r+1}$ die in der Gruppe (4) enthaltenen unabhängigen Nichtreste nach diesem Modul, genauer *ein* vollständiges System solcher.

Satz 8. Für ungerades ℓ läßt sich die Gruppe (4) der sämtlichen ℓ–ten Idealpotenzen auch durch die t (prim zu ℓ gewählten) singulären Primärzahlen ω_i und ein vollständiges System in (4) enthaltener unabhängiger Nichtreste $\eta_i \mod \mathfrak{l}_0^{\ell *}$ der Anzahl $r+1$ eindeutig darstellen in der Form (5).

Für $\ell = 2$ betrachten wir zunächst nur die total positiven ℓ–ten Idealpotenzen, die sich nach demselben Prinzip in der Form

$$\eta_1^{v_1} \ldots \eta_{n_0}^{v_{n_0}} \omega_1^{u_1} \ldots \omega_t^{u_t} \xi^2; \qquad (u_i, v_i = 0, 1) \tag{6}$$

*$\mathfrak{l}_0$ soll stets den Primteiler des Kreiskörpers k_ζ, also $\mathfrak{l}_0 \sim \ell^{\frac{1}{\ell-1}}$ bez[...]

eindeutig darstellen lassen, wo $\eta_1, \ldots, \eta_{n_0}$ ein vollständiges System total positiver unabhängiger Nichtreste mod 2^2 aus der Gruppe (4) ist. Die weiteren t' singulären Primärzahlen $\omega'_1, \ldots \omega'_t$ sind von der Gruppe (6) unabhängig, da kein Produkt aus ihnen total positiv ist. Es

209 III

existieren dann also noch $n-n_0 = (r+1+t)-t-t'-n_0$ (also ist $n = r+1-t'$)† weitere ℓ–te Idealpotenzen (Idealquadrate!) $\eta_{n_0+1}, \ldots \eta_n$, sodaß

$$\eta_1^{v_1} \ldots \eta_n^{v_n} \omega_1^{u_1} \ldots \omega_t^{u_t} {\omega'_1}^{u'_1} \ldots {\omega'_{t'}}^{u'_{t'}} \xi^2 \tag{7}$$
$$(v_i, u_i, u'_i = 0, 1)$$

wieder die Gruppe (4) aller Idealquadrate in eindeutiger Basisdarstellung ist. Die hinzutretenden Zahlen $\eta_{n_0+1}, \ldots \eta_n$ sind dann erstens mit $\eta_1, \ldots, \eta_{n_0}$ zusammen ein System unabhängiger Nichtreste mod 2^2 aus (4), da die $\omega_1, \ldots, \omega_t, \omega'_1, \ldots, \omega'_{t'}$ das vollständiges System der Reste mod 2^2 aus (4) sind, zweitens haben die $\eta_{[\ldots]}, \ldots, \eta_n$ mit $\omega'_1, \ldots, \omega'_{t'}$ zusammen unabhängige Signaturen, da die $\eta_1, \ldots, \eta_{n_0}, \omega_1, \ldots, \omega_t$ das vollständige System der total positiven Zahlen aus (4) sind, und beidesmal aus der Eindeutigkeit von (7) ein Widerspruch folgen würde.

Satz 9 Für $\ell = 2$ läßt sich die Gruppe (4) der sämtlichen Idealquadrate auch durch die $t + t'$ singulären Primärzahlen ω_i, ω'_i (zu 2 prim gewählt) und ein vollständiges System in (4) enthaltener unabhängiger Nichtreste $\eta_i \mod 2^2$ der Anzahl n darstellen in der eindeutigen Form (7). Dabei ist $n = r + 1 - t'$. Die η_i können ferner so gewählt werden, daß die n_0 ersten unter ihnen total positiv sind, die $n - n_0$ letzten mit den ω'_i zusammen unabhängige Signaturen haben.

210 III

Zwischen den Zahlen t', n, n_0 besteht außer der schon genannten Gleichung

$$t' = r + 1 - n \tag{8}$$

noch eine weitere. Nach K. K. Satz 31 ist nämlich

$$t + t' = \overline{n}_0 + r_1 - (r + 1)$$

†Da $t + t'$ der Rang der abs. Kl. Gr. mit Vorz. Bed. tot. pos. ist, ist nach K. K. Satz 31: $t + t' \leqq (r + 1 + t) + r_1 - (r + 1) = t + r_1$, d. h. $t' \leqq r_1$, also $r + 1 - t' \geqq 0$, somit unser hier eingeführtes $n \geqq 0$, was auch aus seiner Definition folgt.

wo $\overline{n}_0$ die Anzahl der total positiven Zahlen in (4)[1] ist. Diese ist aber auf Grund von Satz 9 gerade $n_0 + t$, sodaß

$$t' = n_0 + r_1 - r + 1 = n_0 - r_2 \tag{9}$$

folgt. Aus (8) und (9) folgt durch Addition:

$$2t' = r_1 - (n - n_0). \tag{10}$$

Satz 10. Ist t' der Rangzuwachs, den die absolute Klassengruppe bei Zugrundelegung des engeren Äquivalenzbegriffes (total positiv) nach der Primzahl `[...]` erfährt, n die Anzahl der unabhängigen quadratischen Nichtreste mod 2^2 im System (4) und n_0 die Anzahl der unabhängigen total positiven unter ihnen, so gelten die Relationen (8), (9), (10)

Die in diesem § bewiesenen Sätze über die singulären Primärzahlen bilden die Grundlage für unseren Beweis des Reziprozitätsgesetzes.

[1] Ziffer schwer lesbar

3.3 §3 Beziehungen zwischen Potenzrestsymbolen oben u. unten

§3 Beziehungen zwischen den Potenzrestsymbolen in Oberkörper und Unterkörper.

Für den Beweis des allgemeinen Reziprozitätsgesetzes ist aus dem als bekannt anzusehenden Eisensteinschen Reziprozitätsgesetz im Kreiskörper auf eine Beziehung zwischen Legendre–Symbolen in einem beliebigen Oberkörper zu schließen. Wir beweisen daher in diesem § zwei Sätze allgemeiner Natur, die uns als notwendiges Handwerkszeug für einen derartigen Schluß dienen werden.

Satz 11. k enthalte die ℓ–te Einheitswurzel ζ und K sei ein beliebiger Oberkörper von k. Ist dann α irgendeine Zahl aus k, $\mathfrak{A}$ ein zu α und ℓ primes Ideal aus K mit der Relativnorm $n(\mathfrak{A}) = \mathfrak{a}$ in bezug auf k, so gilt für die ℓ–ten Potenzrestsymbole $\{\ \}$ in K und $(\ )$ in k:

$$\left\{\frac{\alpha}{\mathfrak{A}}\right\} = \left(\frac{\alpha}{\mathfrak{a}}\right).$$

Beweis: Es genügt den Satz für ein Primideal $\mathfrak{P}$ und seine Relativnorm $n(\mathfrak{P}) = \mathfrak{p}^f$ zu beweisen, da er dann nach Definition der Potenzrestsymbole allgemein gilt. Sei die absolute Norm $N(\mathfrak{p}) = p^{f_1}$. Dann ist nach Definition des Legendreschen Symbols

$$\left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{\frac{p^{f_1}-1}{\ell}} \mod \mathfrak{p},$$

also

$$\left(\frac{\alpha}{\mathfrak{p}^f}\right) \equiv \alpha^{f\frac{p^{f_1}-1}{\ell}} \mod \mathfrak{p}.$$

212 III

Andererseits ist

$$\left\{\frac{\alpha}{\mathfrak{P}}\right\} \equiv \alpha^{\frac{p^{ff_1}-1}{\ell}} \mod \mathfrak{P}, \quad \text{also} \quad \mod \mathfrak{p}.$$

Nun ist

$$\frac{p^{ff_1}-1}{\ell} = \frac{p^{ff_1}-1}{p^{f_1}-1} \cdot \frac{p^{f_1}-1}{\ell},$$

und wegen

$$\frac{p^{ff_1}-1}{p^{f_1}-1} = p^{(f-1)f_1} + p^{(f-2)f_1} + \cdots + p^{f_1} + 1 \equiv f \mod \ell,$$

weil

$$p^{f_1} \equiv 1 \mod \ell \qquad (\zeta \text{ kommt in } k \text{ vor!})$$

folgt also:

$$\frac{p^{ff_1-1}}{\ell} \equiv f\frac{p^{f_1}-1}{\ell} \mod (p^{f_1}-1),$$

d. h. wegen $\alpha^{p^{f_1}-1} \equiv 1 \mod \mathfrak{p}$:

$$\left\{\frac{\alpha}{\mathfrak{P}}\right\} \equiv \alpha^{\frac{p^{ff_1}-1}{\ell}} \equiv \alpha^{f\frac{p^{f_1}-1}{\ell}} \equiv \left(\frac{\alpha}{\mathfrak{p}^f}\right) = \left(\frac{\alpha}{n(\mathfrak{P})}\right) \mod \mathfrak{p}$$

sodaß, weil beide Symbole Potenzen von ζ sind,

$$\left\{\frac{\alpha}{\mathfrak{P}}\right\} = \left(\frac{\alpha}{n(\mathfrak{P})}\right)$$

folgt, w. z. b. w.

Satz 12. k enthalte die ℓ–te Einheitswurzel ζ und K sei ein beliebiger Oberkörper von k. Ist dann A irgendeine Zahl aus k, $n(\mathsf{A}) = \alpha$ ihre Relativnorm

nach k und $\mathfrak{a}$ ein zu ℓ und A primes Ideal aus k, so gilt mit den Bezeichnungen von Satz 11:

$$\left\{\frac{\mathsf{A}}{\mathfrak{a}}\right\} = \left(\frac{\alpha}{\mathfrak{a}}\right).$$

Beweis: Es genügt wieder, den Satz für ein zu ℓ und A primes Primideal $\mathfrak{p}$ aus k zu beweisen. $\mathfrak{p}$ habe den Grad f und seine Zerlegung in K sei:

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_z^{e_z}\,; \qquad (\text{Grade} \quad f_i)$$

Sei Ω_i je eine primitive $(p^{ff_i}-1)$–te Einheitswurzel aus den Henselschen Erweiterungskörpern $K(\mathfrak{P}_i)$. Die Relativnorm von Ω_i nach $k(\mathfrak{p})$ ist dann bekanntlich die e_i–te Potenz von

$$\Omega_i^{1+p^f+p^{2f}+\dots+p^{(f_i-1)f}} = \Omega_i^{\frac{p^{ff_i}-1}{p^f-1}}$$

und diese Zahl ist eine primitive (p^f-1)–te Einheitswurzel ω_i aus $k(\mathfrak{p})$. Durch Potenzierung mit einem bestimmten, zu p^f-1, also sicher auch zu dem Teiler ℓ von p^f-1 primen Exponenten c_i läßt sich ω_i in eine derjenigen, □□□ primitiven (p^f-1) ten Einheitswurzeln $\omega = \omega_i^{c_i}$ überführen, deren $\frac{p^f-1}{\ell}$–te Potenz

$$\omega^{\frac{p^f-1}{\ell}} = \zeta$$

die primitive ℓ–te Einheitswurzel ζ ist, auf Grund deren die Potenzrestsymbole definiert werden. Es ist also dann

$$n_i(\Omega_i^{c_i}) = \omega^{e_i}$$

und

$$\Omega_i^{c_i\frac{p^{ff_i}-1}{\ell}} = \Omega_i^{c_i\frac{p^{ff_i}-1}{p^f-1}\cdot\frac{p^f-1}{\ell}} = \omega^{\frac{p^f-1}{\ell}} = \zeta,$$

wenn n_i die Relativnorm von $K(\mathfrak{P}_i)$ nach $k(\mathfrak{p})$ bezeichnet.

Sei nun

$$\mathsf{A} = \Omega_i^{b_i}\mathsf{H}_i(\mathfrak{P}_i)$$

die Entwicklung von A in $K(\mathfrak{P}_i)$, wobei H_i eine Einseinheiten in $K(\mathfrak{P}_i)$ bezeichnet. Dann ist

$$\left\{\frac{\mathsf{A}}{\mathfrak{P}_i}\right\} \equiv \mathsf{A}^{\frac{p^{ff_i}-1}{\ell}} \equiv \Omega_i^{b_i\frac{p^{ff_i}-1}{\ell}},$$

also

$$\left\{\frac{\mathsf{A}}{\mathfrak{P}_i}\right\}^{c_i} = \Omega_i^{b_i c_i \frac{p^{f f_i}-1}{\ell}} = \zeta^{b_i},$$

und weil c_i prim zu ℓ ist:

$$\left\{\frac{\mathsf{A}}{\mathfrak{P}_i}\right\} = \zeta^{\frac{b_i}{c_i}}.$$

Daraus folgt:

$$\left\{\frac{\mathsf{A}}{\mathfrak{p}}\right\} = \prod_i \left\{\frac{\mathsf{A}}{\mathfrak{P}_i}\right\}^{e_i} = \zeta^{\sum_i \frac{b_i}{c_i} e_i}$$

Andererseits ist:

$$\begin{aligned} n_i(\mathsf{A}^{c_i}) = \big(n_i(\mathsf{A})\big)^{c_i} &= n_i\big(\Omega_i^{c_i b_i}\big) n_i\left(\mathsf{H}_i^{c_i}\right) \ (\mathfrak{p}), \\ &= \omega^{e_i b_i} \eta_i^{c_i} \ (\mathfrak{p}), \\ \text{also} \qquad n_i(\mathsf{A}) &= \omega^{e_i \frac{b_i}{c_i}} \eta_i \ (\mathfrak{p}), \end{aligned}$$

wo η_i eine Einseinheit aus $k(\mathfrak{p})$ ist. Dabei darf im Exponenten von ω durch c_i dividiert werden, weil c_i prim zu $p^f - 1$ ist. Für die Gesamtnorm $n(\mathsf{A})$ (für alle $\mathfrak{P}_i$, d. h. für den Bereich von $\mathfrak{p}$) folgt also:

$$\alpha = n(\mathsf{A}) = \prod_i n_i(\mathsf{A}) = \omega^{\sum_i \frac{b_i}{c_i} e_i} \eta \ (\mathfrak{p}),$$

wo η wieder eine Einseinheit aus $k(\mathfrak{p})$ ist. Daher ist vermöge der Bestimmung von ω:

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \zeta^{\sum_i \frac{b_i}{c_i} e_i} = \left\{\frac{\mathsf{A}}{\mathfrak{p}}\right\}, \qquad \text{w. z. b. w.}$$

Bemerkung: Dieser § überträgt sich wörtlich auf den Fall der ℓ^n–ten Potenzreste, wenn

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{\frac{N(\mathfrak{p})-1}{\ell^n}} \mod \mathfrak{p}$$

als Symbol eingeführt wird.

3.4 §4 Primäre und hyperprimäre Primideale.

215 III

Wir definieren zunächst noch einmal im Zusammenhang den Begriff der *primären*, und dazu auch den der *hyperprimären Zahlen*, wobei wir uns auf zu ℓ prime Zahlen beschränken dürfen. Es seien im folgenden folgende Bezeichnungen festgehalten:

$$\ell \mathfrak{l}_0 = \mathfrak{l}_0^\ell = (\lambda_0^\ell) = (1-\zeta)^\ell \sim \ell^{\frac{\ell}{\ell-1}} \sim \prod_i \mathfrak{l}_i^{\frac{e_i \ell}{\ell-1}}$$

($\mathfrak{l}_0$ Primteiler von ℓ im Kreiskörper k_ζ),

$$\mathfrak{L}_0 = \mathfrak{l}_0^\ell \mathfrak{l}_1 \dots \mathfrak{l}_z = \ell \mathfrak{l}_0 \mathfrak{l}_1 \dots \mathfrak{l}_z$$

wobei, wie schon oben die Zerlegung von ℓ in k in der Form:

$$\ell = \mathfrak{l}_1^{e_1} \dots \mathfrak{l}_z^{e_z}$$

angesetzt wird. (Für $\ell = 2$ alles sinnentsprechend!)
Dann definieren wir:

Definition 1: Eine zu ℓ prime *Zahl* heißt *primär*, bezw. *hyperprimär*, wenn sie ℓ–ter Potenzrest mod $\mathfrak{l}_0^\ell$ bezw. mod $\mathfrak{L}_0$ ist.

Ist α primär, so ist die Relativdiskriminante von $k(\sqrt[\ell]{\alpha})$ prim zu ℓ und umgekehrt, erzeugt α einen derartigen Körper, so darf es zunächst prim zu ℓ angenommen werden und muß dann primär sein (K. K., Satz 34). Ist ferner α hyperprimär, so ist überdies $k(\sqrt[\ell]{\alpha})$ so beschaffen, daß in ihm alle $\mathfrak{l}_i$ in Primideale 1. Rel. Grades zerfallen, und umgekehrt, erzeugt α einen derartigen Körper, so darf es zunächst prim zu ℓ angenommen werden, und muß dann

216 III

hyperprimär sein (K. K., Satz 34). Es gilt also:

Satz 13: Damit die Relativdiskriminante von $k(\sqrt[\ell]{\alpha})$, wo α prim zu ℓ gewählt werden darf, prim zu ℓ ist, ist notwendig und hinreichend, daß α primär ist. Damit überdies in $k(\sqrt[\ell]{\alpha})$ jeder Primteiler $\mathfrak{l}_i$ von ℓ in Primteiler 1. Rel. Grades zerfällt, ist notwendig und hinreichend, daß α hyperprimär ist.

Wir definieren nun weiter, auf einer ganz verschiedenartigen Grundlage den Begriff zunächst des *primären Ideals*. Wir legen die folgende Definition zu Grunde:

Definition 2. Ein Ideal (zu ℓ prim!) $\mathfrak{a}$, nach dem alle Legendreschen Symbole $\left(\frac{\alpha}{\mathfrak{a}}\right) = 1$ sind, wenn α eine beliebige ℓ–te Idealpotenz in k ist, heißt primär.

Anmerkung: Es braucht über α nicht vorausgesetzt zu werden, daß es zu $\mathfrak{a}$ prim ist, da man jede ℓ–te Idealpotenz α durch Multiplikation mit geeigneten ℓ–ten Zahlpotenzen stets prim zu beliebig vorgegebenen Idealen machen kann.

Wir beweisen nun, zunächst für ungerades ℓ, den folgenden Satz, der die für Ideale und Zahlen auf verschiedenen Grundlagen getroffene Definition 1 und 2 verbin[...][1].

217 III

Satz 14. Ist $\mathfrak{p}$ ein primäres Primideal, so gibt es eine primäre Zahl ω in k, sodaß

$$(\omega) = \mathfrak{p} j^{\ell}$$

ist, wo j ein Ideal in k bedeutet (ℓ ungerade!)

Beweis: Wir können diesen Satz auf zwei sehr einfache Arten beweisen:

1.) Nach K. K. Satz 30 ist der Rang der Klassengruppe nach dem Strahl $\equiv 1 \mod \mathfrak{p}$

$$\bar{t} = R(\mathfrak{p}) + \overline{n} - (r+1) = 1 + \overline{n} - (r+1),$$

wo $\overline{n}$ die Anzahl der ℓ–ten Potenzreste mod $\mathfrak{p}$ im System der ℓ–ten Idealpotenzen (4) (S. 207▸) ist. Da $\mathfrak{p}$ nach Voraussetzung primär ist, sind alle ℓ–ten Idealpotenzen ℓ–te Potenzreste mod $\mathfrak{p}$, also

$$\overline{n} = t + (r+1)$$

mithin

$$\bar{t} = t + 1.$$

Es muß also außer den t singulären Primärzahlen ω_i noch eine davon unabhängige Zahl ω existieren, sodaß $k(\sqrt[\ell]{\omega})$ Klassenkörper für eine Klassengruppe vom Index ℓ ist, die nicht schon auf Grund der absoluten Klasseneinteilung definierbar, deren Führer also $\mathfrak{p}$ ist. Die Relativdiskriminante von

[1] „verbindet“ ?

$k(\sqrt[\ell]{\omega})$ muß also durch $\mathfrak{p}$ teilbar sein; dann darf ω genau durch $\mathfrak{p}^1$ teilbar angenommen werden. Da keine anderen Teiler in der Relativdiskriminante aufgehen können, weil $\mathfrak{p}$ der Führer ist, muß ω die Form

$$(\omega) = \mathfrak{p} j^{\ell}$$

haben, und primär sein, weil die Relativdiskr. prim zu ℓ ist.

218 III

2.) Nach dem Modul $\mathfrak{l}_0^{\ell}$ ist der Rang der Klassengruppe

$$\bar{t} = R(\mathfrak{l}_0^{\ell}) + n - (r+1).$$

Die Anzahl n der ℓ–ten Potenzreste (4) im System der ℓ–ten Idealpotenzen ist gleich t, weil diese mit den singulären Primärzahlen übereinstimmen. Ferner ist

$$R(\mathfrak{l}_0^{\ell}) = \sum_i R\left(\mathfrak{l}_i^{\frac{e_i \ell}{\ell-1}}\right) = \sum e_i f_i = m$$

wo m den Grad von k bedeutet, und da ℓ ungerade, [...] k als Oberkörper von k_ζ total imaginär: $m = 2r_2 = 2(r+1)$ und

$$\bar{t} = t + r + 1.$$

Werden die Idealklassen also nach dem Strahl $\equiv 1 \mod \mathfrak{l}_0$ definiert und die ℓ–ten Potenzen in die Hauptklasse zusammengefaßt, so hat die so entstehende Klassengruppe den Grad $\ell^{\bar{t}} = \ell^{t+r+1}$ und $t+r+1$ unabhängige Basiselemente. Nach K. K. §4 D. erhält man dann den zugehörigen Klassenkörper vom Grade $\ell^{\bar{t}} = \ell^{t+r+1}$ durch Komposition der $t+r+1$ unabhängigen Kummerschen Klassenkörper für die $t+r+1$ „unabhängigen“ Untergruppen der Klassengruppe vom Index ℓ. Diese $t+r+1$ Kummerschen Körper müssen durch $t+r+1$ unabhängige Zahlen definiert werden, die außer durch ℓ–te Idealpotenzen höchstens durch Primteiler von $\mathfrak{l}$ teilbar sind. Nun liefert aber das System (4) der ℓ–ten Idealpotenzen für sich schon $t+r+1$ unabhängige Zahlen, die nach dem Existenzbeweis K. K. §4, A. schon zur Konstruktion unserer $t+r+1$ unabhängigen Kummerschen Körper ausreichen. Denn in den dortigen Entwicklungen treten ja für unseren speziellen

219 III

Modul $\mathfrak{l}_0^{\ell}$ weder die π_i noch die λ_i auf. Daher kann nach K. K. §4 D. der

Klassenkörper vom Grade $\ell^{\bar{t}}$ zunächst aus $t+r+1$ geeignet gewählten, also natürlich auch aus irgendwelchen $t+r+1$ unabhängigen Zahlen aus (4) konstruiert werden, (da ja so stets derselbe Körper herauskommt) und ist mithin:

$$K = k\left(\sqrt[\ell]{\varepsilon_1}, \ldots, \sqrt[\ell]{\varepsilon_{r+1}}, \sqrt[\ell]{\rho_1}, \ldots, \sqrt[\ell]{\rho_t}\right).$$

Nach K. K. Satz 39 (S. 125) zerfällt also unser n. V. primäres Primideal $\mathfrak{p}$ in K in ℓ^{t+r+1} verschiedene Primteiler 1. Rel. Grades, gehört somit nach dem Zerlegungssatz zur Hauptklasse der K entsprechenden Klasseneinteilung, d. h. ist einer ℓ–ten Idealpotenz $\overline{j}^{\ell}$ nach dem Strahl $\equiv 1 \mod \mathfrak{l}_0^{\ell}$ äquivalent:

$$\mathfrak{p} = \overline{j}^{\ell}(\omega); \qquad \omega \equiv 1 \mod \mathfrak{l}_0^{\ell},$$

was mit $j^{-1} = \overline{j}$ die Behauptung ergibt.

Offenbar ist ω nur bis auf Faktoren ξ^{ℓ}, was selbstverständlich, und singuläre Primärzahlen bestimmt. Denn erstens leistet mit ω auch jedes $\omega\omega_i$, wo ω_i singuläre Primärzahl ist, die gleichen Dienste, andrerseits folgt aus:

$$(\omega) = \mathfrak{p}\mathfrak{j}^{\ell},$$
$$(\omega') = \mathfrak{p}\mathfrak{j}'^{\ell},$$

daß $\frac{\omega}{\omega'}$ primär und ℓ–te Idealpotenz $\left(\frac{\mathfrak{j}}{\mathfrak{j}'}\right)^{\ell}$ ist.

Daher gilt:

Satz 15. Ist $\mathfrak{p}$ ein primäres Primideal und gemäß Satz 14

$$(\omega) = \mathfrak{p}\mathfrak{j}^{\ell},$$

so heißt ω eine zu $\mathfrak{p}$ gehörige Primärzahl. Alle zu $\mathfrak{p}$ gehörigen Primärzahlen entstehen aus einer in der Form:

$$\omega\omega_1^{u_1} \ldots \omega_t^{u_t}\xi^{\ell},$$

wo die ω_i die t singulären Primärzahlen von k sind (ℓ ungerade!).

Für $\ell = 2$ sind wieder die Signaturen zu berücksichtigen. Wir beweisen:

Satz 16. Ist $\mathfrak{p}$ ein primäres Primideal ($\ell = 2$), so gibt es in k eine total positive, primäre Zahl ω, sodaß

$$(\omega) = \mathfrak{p}\mathfrak{j}^2$$

ist, wo j ein Ideal aus k ist.

Beweis:
□□□
1.) Der erste der obigen Beweise von Satz 14 überträgt sich ohne weiteres. Das resultierende ω muß nach K. K. Satz 42a. total positiv sein, weil der Körper $k(\sqrt[\ell]{\omega})$ Klassenkörper nach einer Klassengruppe vom Führer $\mathfrak{p}$ ohne Vorzeichenbedingung[2] ist.

221 III

2.) Auch der zweite jener Beweise überträgt sich leicht. Wir definieren die Idealklassen zunächst nach dem Strahl $\equiv 1 \mod \mathfrak{l}_0^{\ell *}$, total positiv und fassen die Quadrate in die Hauptklasse zusammen. Für den Rang der Klassengruppe mod $\mathfrak{l}_0^{\ell}$ mit Vorzeichenbedingung folgt nach K. K. Satz 31:

$$\bar{t} = m + \overline{n}_0 + r_1 - (r+1),$$

wo $\overline{n}_0$ die Anzahl der total positiven quadratischen Reste im System (4) der Idealquadrate ist. In den Bezeichnungen von §2 ist $\overline{n}_0 = t$, weil letztere mit den t total positiven singulären Primärzahlen zusammenfallen, und

$$m + r_1 - (r+1) = m - r_2 = r + 1$$

also wieder $\bar{t} = t + r + 1$.

Alle Schlüsse von S. 218▸/219▸ übertragen sich dann wörtlich.
Es muß also wieder $\mathfrak{p}$ zur Hauptklasse obiger Klasseneinteilung gehören, d. h.

$$\mathfrak{p} = \bar{j}^2(\omega)\,; \qquad \omega \equiv 1 \mod \mathfrak{l}_0^2, \quad \text{tot. positiv}$$

sein, w. z. b. w.

Satz 15 wird dann:

Satz 17: Ist $\mathfrak{p}$ ein primäres Primideal ($\ell = 2$) und gemäß Satz 16

$$(\omega) = \mathfrak{p} j^2,$$

so heißt ω eine zu $\mathfrak{p}$ gehörige total positive Primärzahl. Alle zu $\mathfrak{p}$ gehörigen total positiven Primärzahlen entstehen aus einer in der Form

$$\omega \omega_1^{u_1} \dots \omega_t^{u_t} \xi^2,$$

[2] undeutlich
[*] $\mathfrak{l}_0^{\ell} = 2^2$.

wo ω_i die t total positiven singulären Primärzahlen von k sind.

222 III

Über die Sätze 16, 17 hinaus beweisen wir noch die Existenz weiterer Primärzahlen zu $\mathfrak{p}$, die aber nicht mehr total positiv sind.
Wir legen dazu die Gruppe (4) der Idealquadrate zugrunde, fordern aber von $\mathfrak{p}$ jetzt nur, daß alle total positiven Zahlen aus (4) (es genügt also die Zahlen $\omega_1, \dots \omega_t, \eta_1, \dots \eta_{n_0}$ von Satz 9 in Betracht zu ziehen) quadratische Reste nach $\mathfrak{p}$ sein sollen.

Satz 18. Ist für ein zu 2 primes Primideal $\mathfrak{p}$:

$$\left(\frac{\omega_i}{\mathfrak{p}}\right) = 1; \qquad (i = 1, \dots, t),$$
$$\left(\frac{\eta_i}{\mathfrak{p}}\right) = 1; \qquad (i = 1, \dots, n_0),$$

wo die ω_i die t unabhängigen total positiven Primärzahlen und die η_i die n_0 unabhängigen quadratischen Nichtreste, die total positiv sind, aus (4) bedeuten, so existiert in k eine *zu* $\mathfrak{p}$ *gehörige Primärzahl* ω, sodaß

$$(\omega) = \mathfrak{p}j^2$$

ist.

Beweis: Wieder lasssen sich beide Beweisverfahren vom Vorhergehenden anwenden:

1.) Der Rang der Klassengruppe nach dem Strahl $\equiv 1 \mod \mathfrak{p}$, total positiv ist nach K. K. Satz 31:

$$\bar{t} = 1 + \overline{n}_0 + r_1 - (r + 1),$$

wo $\overline{n}_0$ die Anzahl der total positiven quadratischen Reste mod $\mathfrak{p}$ im System (4) ist. Da nach Voraussetzung über $\mathfrak{p}$

223 III

alle total positiven Zahlen aus (4) quadratische Reste nach $\mathfrak{p}$ sind, ist

$$\overline{n}_0 = t + n_0$$

und somit nach Satz 10:

$$\bar{t} = t + t' + 1.$$

Daraus folgt, wie a. S. 217 die Existenz eines ω, der einen Klassenkörper für eine Klassengruppe vom Führer $\mathfrak{p}$ mit Vorzeichenbedingung erzeugt, also die Form

$$(\omega) = \mathfrak{p} j^2$$

haben muß und primär ist, während sich über die Signatur von ω jetzt nichts aussagen läßt.

2.) Der Rang der Klassengruppe nach dem Strahl $\equiv 1 \mod \mathfrak{l}_0^2$ *ohne* Vorzeichenbedingung ist nach K. K. Satz 30

$$\bar{t} = m + \overline{n} - (r+1),$$

wo $\overline{n}$ die Anzahl der quadratischen Reste mod $\mathfrak{l}_0^2$ im System (4), also $\overline{n} = t + t'$ ist. Daher ist nach Satz 10, Gl. (9):

$$\bar{t} = t + n_0,$$

wo n_0 die Anzahl der unabhängigen, total positiven quadratischen Nichtreste mod $\mathfrak{l}_0^2$ in (4) ist. Der Klassenkörper für die Klassengruppe: „Quadrate von Klassen mod $\mathfrak{l}_0^2$“ muß daher ein aus $t + n_0$ unabhängigen Kummerschen Körpern komponierbar sein. Nach dem Existenzbeweis von K K, §4 A werden wieder diese $t + n_0$ Körper schon geliefert durch gewisse der Zahlen (4), und zwar, da wir keine Vorzeichenbedingung haben, durch die total positiven unter ihnen. Da letztere aber aus $t + n_0$ unabhängigen zusammengesetzt sind, folgt, daß der gesuchte

224 III

Klassenkörper

$$K = k\left(\sqrt[2]{\eta_1}, \dots \sqrt[2]{\eta_{n_0}}, \sqrt[2]{\omega_1}, \dots \sqrt[2]{\omega_t}\right)$$

ist, also n. V. über $\mathfrak{p}$ und dem Zerlegungssatz für den Klassenkörper $\mathfrak{p}$ zur Hauptklasse unserer Klasseneinteilung gehört, woraus wieder die Behauptung folgt.

Die im Sinne von Satz 18 zu $\mathfrak{p}$ gehörigen Primärzahlen sind ersichtlich nur bis auf Zahlquadrate und singuläre Primärzahlen bestimmt und jede so aus einer ω gebildete Zahl leistet die gleichen Dienste.
Daher gilt, analog zu Satz 17:

Satz 19. Erfüllt $\mathfrak{p}$ die Voraussetzungen von Satz 18 ($\ell = 2$), so sind alle zu $\mathfrak{p}$ gehörigen Primärzahlen in der Form

$$\omega \omega_1^{u_1} \dots \omega_t^{u_t} \omega'^{u'_1}_1 \dots \omega'^{u'_{t'}}_{t'} \xi^2$$

enthalten, wo die ω_i, ω_i' die sämtlichen singulären Primärzahlen von k sind.

Wir gehen nun zu den entsprechenden Sätzen über hyperprimäre Zahlen und Primideale über. Ehe wir das hyperprimäre Ideal definieren, haben wir folgende Betrachtung anzustellen:

Sei zunächst ℓ ungerade. Ferner seien, wie schon früher, die singulären Primärzahlen stets prim zu ℓ gewählt, und die Gruppe

$$\omega_1^{u_1} \dots \omega_t^{u_t} \xi^{\ell}; \qquad (u_i = 0, \dots \ell - 1)$$

enthalte ν unabhängige hyperprimäre Zahlen, sodaß also ν die Anzahl der unabhängigen ℓ–ten Potenzreste mod $\mathfrak{L}_0$ im System (4) der ℓ–ten Idealpotenzen ist. Daher ist nach K. K.

225 III

Satz 30 der Rang der Klassengruppe mod $\mathfrak{L}_0$ gleich

$$\bar{t} = R(\mathfrak{L}_0) + \nu - (r+1).$$

Es ist nach K. K. Satz 28

$$R(\mathfrak{L}_0) = \sum_{i=1}^{z} R\left(\mathfrak{l}_i^{\frac{e_i \ell}{\ell-1}+1}\right) = m + z,$$

also wegen $m - (r+1) = r + 1$; (k tot. imaginär):

$$\begin{aligned} \bar{t} = r + 1 + \nu + z &= t + r + 1 + [z - (t - \nu)] \\ &= t + r + 1 + z_0, \end{aligned}$$

wenn

$$z_0 = z - (t - \nu)$$

gesetzt wird. Es gibt somit genau $t + r + 1 + z_0$ unabhängige Kummersche Körper, die Klassenkörper für Klassengruppen mod $\mathfrak{L}_0$ vom Index ℓ sind, also außer den $t + r + 1$ Zahlen $\eta_1, \dots, \eta_{r+1}, \omega_1, \dots, \omega_t$ die nach S. 219 als Repräsentanten für die Klassenkörper mod $\mathfrak{l}_0^{\ell}$ genommen werden können, noch z_0 weitere Zahlen:

$$\lambda_1, \dots, \lambda_{z_0},$$

die außer durch ℓ–te Idealpotenzen nur durch Primteiler von ℓ' teilbar sind (und auch wirklich *keine* ℓ–ten Idealpotenzen sind), derart, daß die $t + r + 1 + z_0$ Zahlen $\eta_i, \omega_i, \lambda_i$ unabhängig sind. Umgekehrt muß sich aber jede Zahl dieser Beschaffenheit in der Form

$$\eta_1^{v_1} \dots \eta_{r+1}^{v_{r+1}} \omega_1^{u_1} \dots \omega_t^{u_t} \lambda_1^{w_1} \dots \lambda_{z_0}^{w_{z_0}} \xi^{\ell} \tag{1}$$

vorfinden, also dies die eindeutige Basisdarstellung für die Gruppe aller derartigen Zahlen sein. Denn ist α eine solche Zahl, so ist $k(\sqrt[\ell]{\alpha})$ Klassenkörper für eine Klassengruppe, deren Führer ein Potenzprodukt der $\mathfrak{l}_i$ ist. Da aber durch Erhöhung des Moduls $\mathfrak{L}_0$ nach K. K. Satz 28

der Rang der Klassengruppe nicht mehr erhöht wird, muß $k(\sqrt[\ell]{\alpha})$ schon als Klassenkörper mod $\mathfrak{L}_0$ resultieren, also α in obiger Form (1) darstellbar sein.

Wir definieren jetzt:

Definition 3. Für ungerades ℓ heißt ein zu ℓ primes Ideal $\mathfrak{a}$ hyperprimär, wenn jedes Legendre Symbol

$$\left(\frac{\alpha}{\mathfrak{a}}\right) = 1$$

ist, wo α irgendeine Zahl aus (1) bedeutet.

Dann beweisen wir den folgenden Satz, der die Beziehung zu den hyperprimären Zahlen liefert:

Satz 20. Ist $\mathfrak{p}$ ein hyperprimäres Primideal, dann gibt es eine $\mathfrak{p}$ *zugeordnete Hyperprimärzahl* ω, sodaß

$$(\omega) = \mathfrak{p} j^{\ell}$$

ist (ℓ ungerade).

Beweis: Nach dem Vorhergehenden entsteht der Klassenkörper K für die Klassengruppe: „ℓ–te Potenzen der Klassen mod $\mathfrak{L}_0$“ als Kompositum

$$K = k\left(\sqrt[\ell]{\eta_1}, \dots, \sqrt[\ell]{\omega_1}, \dots, \sqrt[\ell]{\lambda_1}, \dots\right)$$

Nach Voraussetzung zerfällt $\mathfrak{p}$ in K in versch. Primteiler 1. Rel. Grades, gehört also zur Hauptklasse, d. h.

$$j \equiv \overline{j}^{\ell}(\omega)\,; \qquad \omega \equiv 1 \mod \mathfrak{L}_0$$

was die Behauptung ergibt.

Entsprechend dem früheren gilt hier:

Satz 21. Alle zu $\mathfrak{p}$ gehörigen Hyperprimärzahlen ω entstehen aus einer durch Multiplikation mit den hyperprimären unter den singulären Primärzahlen. (ℓ ungerade)

227 III

Für $\ell = 2$ sei wieder ν die Anzahl der total positiven hyperprimären unabhängigen der Gruppe

$$\omega_1^{u_1} \dots \omega_t^{u_t} \xi^2$$

der total positiven singulären Primärzahlen, also ν auch die Anzahl der total positiven quadratischen Reste mod $\mathfrak{L}_0$ unter den Idealquadraten. Dann ist der Rang der Klassengruppe $\equiv 1 \mod \mathfrak{L}_0$, total positiv gleich

$$\bar{t} = m + z + \nu + r_1 - (r+1),$$

also wegen $m + r_1 - (r+1) = r + 1$:

$$\bar{t} = t + r + 1 + z_0,$$

wobei $z_0 = z - (t - \nu)$

gesetzt ist. Außer den nach obigem (S. 221) als Repräsentanten für die unabhängigen Klassenkörper nach $\mathfrak{l}_0^\ell$ geeigneten $\eta_1, \dots \eta_n, \omega_1, \dots \omega_t, \omega'_1, \dots \omega'_{t'}$, die ja an Stelle der $t + r + 1$ Elemente $\varepsilon_1, \dots, \varepsilon_{r+1}, \rho_1, \dots, \rho_t$ genommen werden dürfen, müssen also noch weitere z_0 Zahlen $\lambda_1, \dots, \lambda_{z_0}$ existieren, die von den vorher genannten und unter sich unabhängig sind, sodaß wie oben alle Zahlen, die außer durch Idealquadrate nur durch Primteiler $\mathfrak{l}_i$ von ℓ teilbar sind in eindeutiger Basisdarstellung durch

$$\eta_1^{v_1} \dots \eta_n^{v_n} \omega_1^{u_1} \dots \omega_t^{u_t} \omega'^{u'_1}_1 \dots \omega'^{u'_{t'}}_{t'} \lambda_1^{w_1} \dots \lambda_{z_0}^{w_{z_0}} \xi^2 \tag{2}$$

gegeben werden.

Wir definieren dann

Definition 4. Für $\ell = 2$ heißt ein zu 2 primes Ideal $\mathfrak{a}$ hyperprimär, wenn für alle Zahlen α aus (2)

$$\left(\frac{\alpha}{\mathfrak{a}}\right) = 1$$

ist.

228 III

Ersichtlich ist diese Definition mit Definition 3 für ungerades ℓ identisch. Genau ebenso, unter Berücksichtigung der Tatsache, daß die jetzige Klasseneinteilung die Vorzeichenbedingung total positiv hat, folgen dann die beiden Sätze:

Satz 22. Ist für $\ell = 2$ $\mathfrak{p}$ ein hyperprimäres Primideal, so gibt es eine $\mathfrak{p}$ *zugeordnete*, total positive *Hyperprimärzahl* ω, sodaß

$$(\omega) = \mathfrak{p} j^2$$

ist.

Satz 23. Alle zu $\mathfrak{p}$ zugeordneten[3] Hyperprimärzahlen entstehen aus einer durch Multiplikation mit den hyperprimären unter den total positiven singulären Primärzahlen.

Schließlich beweisen wir noch die entsprechenden Sätze, wenn der Begriff des hyperprimären Primideals weiter gefaßt wird.

Es möge außer den ν unabhängigen hyperprimären Zahlen unter den t total positiven singulären Primärzahlen noch ν' weitere von jenen unabhängige hyperprimäre Zahlen unter den t' übrigen singulären Primärzahlen geben. Dementsprechend betrachten wir dann die Klassengruppe mod $\mathfrak{L}_0$ ohne Vorzeichenbedingung, deren Rang dann

$$\begin{aligned} \bar{t} &= m + z + \nu + \nu' - (r+1) \\ &= t + n_0 + z_0', \quad \text{(s. S. 223)} \quad \text{ist,} \end{aligned}$$

wo

$$z_0' = z - (t - \nu) - (t' - \nu') \qquad \text{(s. S. 210)}$$

gesetzt ist.

229 III

Nach S. 223/224 bilden die Zahlen $\eta_1, \ldots, \eta_{n_0}, \omega_1, \ldots, \omega_t$ ein System von solchen unabhängigen Zahlen, die die sämtlichen Klassenkörper vom Grade

[3] undeutlich

2 nach dem Strahl $\equiv 1 \mod \mathfrak{l}_0^2$ ohne Vorzeichenbedingung erzeugen. Es existieren daher noch weitere z_0' Zahlen $\lambda_1, \ldots, \lambda_{z_0'}$, die von jenen unabhängig sind (und nach K. K. Satz 42a total positiv), sodaß durch

$$\eta_1, \ldots, \eta_{n_0}, \omega_1, \ldots, \omega_t, \lambda_1, \ldots, \lambda_{z_0'}$$

alle relativquadratischen Klassenkörper mod $\mathfrak{L}_0$ erzeugt werden, und die $\lambda_1, \ldots, \lambda_{z_0'}$ sind durch keine anderen, als Primteiler von ℓ mit zu ℓ primen Exponenten teilbar. Umgekehrt muß dann auch jede total positive Zahl dieser Eigenschaft in der Form

$$\eta_1^{v_1} \ldots \eta_{n_0}^{v_{n_0}} \omega_1^{u_1} \ldots \omega_t^{u_t} \lambda_1^{w_1} \ldots \lambda_{z_0'}^{w_{z_0'}} \xi^2$$

in eindeutiger Basisdarstellung enthalten sein. Denn ihr Körper ist Klassenkörper, wie oben sicher für den Strahl mod $\mathfrak{L}_0$, und nach K. K. Satz 21a, (S. 60[4] oben), sicher ohne Vorzeichenbedingung.

Übrigens können natürlich die obigen Zahlen $\lambda_1, \ldots, \lambda_{z_0}$ so gewählt werden, daß ihre $z_0' = z_0 - (t' - \nu')$ ersten die jetzigen $\lambda_1, \ldots, \lambda_{z_0'}$, also total positiv sind, da ja die obigen Klassenkörper mod $\mathfrak{L}_0$ *mit* Vorzeichenbedingung enthalten sein müssen.

Genau, wie schon mehrfach geschlossen, folgen hieraus die folgenden beiden Sätze:

230 III

Satz 24. Ist für $\ell = 2$ $\mathfrak{p}$ ein solches zu 2 primes Primideal, daß

$$\left(\frac{\eta_i}{\mathfrak{p}}\right) = 1; \qquad (i = 1, \ldots n_0)$$
$$\left(\frac{\omega_i}{\mathfrak{p}}\right) = 1; \qquad (i = 1, \ldots t)$$
$$\left(\frac{\lambda_i}{\mathfrak{p}}\right) = 1; \qquad (i = 1, \ldots z_0'),$$

also daß alle total positiven Zahlen der Gruppe (2) quadratische Reste nach $\mathfrak{p}$ sind, so gibt es eine $\mathfrak{p}$ *zugeordnete Hyperprimärzahl* ω (über deren Signatur nichts ausgesagt werden kann), sodaß

$$(\omega) = \mathfrak{p} j^2$$

[4] zweite Ziffer undeutlich

ist.

Satz 25. Alle im Sinne von Satz 24 $\mathfrak{p}$ zugeordneten Hyperprimärzahlen entstehen aus einer durch Multiplikation mit irgendwelchen der hyperprimären unter den *sämtlichen* singulären Primärzahlen.

Wir stellen noch die erhaltenen Resultate über die Klassenkörper nach den Moduln $1, \mathfrak{l}_0^\ell, \mathfrak{L}_0$ mit und ohne Vorzeichenbedingung zusammen. Jedesmal entsteht der Klassenkörper für die Klassengruppe: „Hauptklasse = Gruppe der ℓ–ten Klassenpotenzen der betr. Art“ durch Zusammenfassung von ebensoviel unabhängigen Kummerschen Körpern, als der Rang $\bar{t}$ der Klassengruppe nach dem betr. Modul angibt. Es gilt:

Satz 26. Die $\bar{t}$ unabhängigen Kummerschen Klassenkörper für die sämtlichen Klassengruppen vom Index ℓ werden durch folgende $\bar{t}$ unabhängigen Zahlen gegeben:

a.) ℓ *ungerade.*

1.) Modul 1, $\bar{t} = t$,

Zahlen: $\omega_1, \ldots, \omega_t$.

2.) Modul $\mathfrak{l}_0^\ell$, $\bar{t} = t + r + 1$,

Zahlen: $\omega_1, \ldots, \omega_t; \eta_1, \ldots, \eta_{r+1}$.

3.) Modul $\mathfrak{L}_0$, $\bar{t} = t + r + 1 + z_0$,

Zahlen: $\omega_1, \ldots, \omega_t; \eta_1, \ldots, \eta_{r+1}; \lambda_1, \ldots, \lambda_{z_0}$.

b.) $\ell = 2$, *Vorzeichenbedingung total positiv.*

1.) Modul 1, $\bar{t} = t + t'$,

Zahlen: $\omega_1, \ldots, \omega_t; \omega'_1, \ldots, \omega'_{t'}$.

2.) Modul $\mathfrak{l}_0^2 = 4$, $\bar{t} = t + t' + n = t + r + 1$,

Zahlen: $\omega_1, \ldots, \omega_t; \omega'_1, \ldots, \omega'_{t'}; \eta_1, \ldots, \eta_n$.

3.) Modul $\mathfrak{L}_0$, $\bar{t} = t + t' + n + z_0 = t + r + 1 + z_0$,

Zahlen: $\omega_1, \ldots, \omega_t; \omega'_1, \ldots, \omega'_{t'}; \eta_1, \ldots, \eta_n; \lambda_1, \ldots, \lambda_{z_0}$.

c.) $\ell = 2$, *keine Vorzeichenbedingung.*

1.) Modul 1, $\bar{t} = t$,

Zahlen: $\omega_1, \ldots, \omega_t$.

2.) Modul $\mathfrak{l}_0^2 = 4$, $\bar{t} = t + n_0$,

Zahlen: $\omega_1, \ldots, \omega_t; \eta_1, \ldots, \eta_{n_0}$.

3.) Modul $\mathfrak{L}_0$, $\bar{t} = t + n_0 + z_0'$,

Zahlen: $\omega_1, \ldots, \omega_t; \eta_1, \ldots, \eta_{n_0}; \lambda_1, \ldots, \lambda_{z_0'}$.

3.5 §5 Das Reziprozitätsgesetz zwischen primärer und primer Zahl ($\ell \neq 2$)

§5 Das Reziprozitätsgesetz zwischen einer primären und einer beliebigen, zu ℓ primen Zahl für ungerades ℓ.

Wir beweisen zunächst folgenden Satz (in diesem § stets ℓ ungerade).

Satz 27. Sind $\omega_1, \ldots, \omega_t$ die t singulären Primärzahlen und $i_1, \ldots, i_t$ ein solches System von t zu ℓ primen Primidealen, daß

$$\left(\frac{\omega_a}{i_a}\right) \neq 1\,; \qquad \left(\frac{\omega_a}{i_b}\right) = 1\,; \qquad (a \neq b),$$

so repräsentieren die i_a die t unabhängigen Basisklassen von k in absolutem Sinne, d. h. es gilt für jedes Ideal $\mathfrak{a}$ eine eindeutige Darstellung:

$$\mathfrak{a} = i_1^{c_1} \ldots i_t^{c_t}(\alpha) j^\ell\,; \qquad (c_i = 0, 1, \ldots\ \ell - 1).$$

Beweis: Nach K. K. Satz 40 (S. 126) können wegen der Unabhängigkeit der ω_i stets solche Primideale i_a gefunden werden. Es ist nur zu zeigen, daß solche t Primideale i_a in Bezug auf die Gruppe der ℓ–ten Idealpotenzen unabhängig sind, d. h. keine Relation

$$(\alpha) = i_1^{c_1} \ldots i_t^{c_t} j^\ell\,; \qquad (c_i = 0, 1, \ldots, \ell - 1) \tag{1}$$

besteht, wenn nicht alle $c_i = 0$ sind. Denn dann sind die i_a als „Rangbasis“ für die absolute Klassengruppe vom Range t geeignet.

Dazu bemerken wir, daß genau wie beim Existenzbeweis in K. K. §4 A. für die q_i, hier für die i_a gilt, daß der Rang der Klassengruppe mod $\mathfrak{l}_0^\ell$ gleich dem Rang der Klassengruppe mod $\mathfrak{l}_0^\ell i_1 \ldots i_t$ ist. Der erstere ist nämlich

nach dem obigen (s. S. 231) gleich $t + r + 1$, beim letzteren vermehrt sich $R(\mathfrak{l}_0^\ell)$ um t, da t zu ℓ prime Primideale hinzutreten. Dafür vermindert sich

die Anzahl der ℓ–ten Potenzreste im System der ℓ–ten Idealpotenzen um t, da die einzigen mod $\mathfrak{l}_0^\ell$ noch vorhandenen t unabhängigen ℓ–ten Potenzreste $\omega_1, \ldots, \omega_t$ nach $\mathfrak{l}_0^\ell i_1 \ldots i_t$ wegen der $[\ldots]$stimmung der i_a Nichtreste sind.

Es ist somit jede Klassengruppe vom Index ℓ nach dem Modul $\mathfrak{l}_0^\ell i_1 \ldots i_t$ schon Klassengruppe vom Index ℓ nach $[\ldots]^\ell$. Nun definiert ein ev. in der Form (1) darstellbares α einen Kummerschen Körper $k(\sqrt[\ell]{\alpha})$, der Klassenkörper für eine Klassengruppe H vom Index ℓ ist. Ist $f^{\ell-1}$ seine Relativdiskriminante, so kann H nach f definiert werden. f ist zunächst durch die zu ℓ primen i_a höchstens in der ersten Potenz teilbar, (wenn $c_{[\ldots]} \neq 0$), außerdem noch durch Potenzen $\mathfrak{l}_i^{v_i+1}$ der Teiler von ℓ. Da α nicht durch die $\mathfrak{l}_i$ teilbar ist (bis auf ev. ℓ–te Potenzfaktoren), kann hier die Größe v_i den Höchstwert $\frac{e_i \ell}{\ell-1}$ nicht annehmen (vergl. K. K. §3 A.). Es ist also f ein Teiler von $\prod_i \mathfrak{l}_i^{\frac{e_i\ell}{\ell-1}} i_1 \ldots i_t = \mathfrak{l}_0^\ell i_1 \ldots i_t$. Dann muß aber nach obigem H schon mod $\mathfrak{l}_0^\ell$ erklärbar sein, also die Relativdiskriminante von $k(\sqrt[\ell]{\alpha})$ prim zu den i_a, d. h. alle $c_a = 0$, w. z. b. w.

Natürlich dürfen die i_a von Satz 27 ihrer Entstehung nach prim zu beliebig gegebenen Zahlen und Idealen vorausgesetzt werden.

234 III

Wir nennen ferner ein System $i_1, \ldots, i_t$, kurz $[i]$ dieser Art *gegen eine Zahl* μ *normiert*, wenn μ ℓ–ter Potenzrest nach allen i_a ist, kurz:

$$\left(\frac{\mu}{[i]}\right) = 1. \tag{2}$$

Ist dann μ eine von der Gruppe

$$\omega_1^{u_1} \ldots \omega_t^{u_t} \xi^\ell$$

unabhängige Zahl, also keine singuläre Primärzahl (ℓ–te Potenzen dürfen für μ a fortiori zugelassen werden), so können die i_a nach K. K. Satz 40 noch den weiteren Bedingungen

$$\left(\frac{\mu}{i_1}\right) = \cdots = \left(\frac{\mu}{i_t}\right) = 1$$

unterworfen werden, d. h. (2) entsprechend gewählt werden, also:

Satz 28. Ist μ keine singuläre Primärzahl, so darf das Repräsentantensystem $[i]$ von Satz 27 gegen μ normiert angenommen werden, d. h. außer den Bedingungen von Satz 27 noch den Bedingungen (2) entsprechend gewählt werden.

Umgekehrt kann offenbar auch eine beliebige Zahl μ durch Multiplikation mit einem geeigneten Potenzprodukt

$$\omega_1^{u_1} \dots \omega_t^{u_t}$$

singulärer Primärzahlen gegen ein gegebenes Repräsentanten–System $[i]$ normiert werden.

Um nicht dauernd unnötige und unwesentliche Annahmen über Teilerfremdheit machen zu müssen, setzen

wir für das folgende fest, daß die Bedeutung des Legendre Symbols $\left(\frac{\mu}{\mathfrak{a}}\right)$ wie folgt erweitert werden soll:

1.) ist $\mathfrak{a}$ prim zu μ, so ist $\left(\frac{\mu}{\mathfrak{a}}\right)$ eindeutig definiert.

2.) Ist $\mathfrak{a}$ nicht prim zu μ, wohl aber der *Kern* von $\mathfrak{a}$ prim zum *Kern* von μ, d. h. $\mathfrak{a}$ und μ bis auf ℓ–te Idealpotenzen prim zu einander, so soll zunächst durch

$$\left(\frac{\mu}{\mathfrak{a}}\right) = \left(\frac{\mu}{\mathfrak{a}_0 j^\ell}\right) = \left(\frac{\mu}{\mathfrak{a}_0}\right)$$

das Symbol auf den Kern $\mathfrak{a}_0$ von $\mathfrak{a}$ zurückgeführt werden. Ist ferner

$$(\mu) = m j^\ell,$$

so läßt sich unter der Voraussetzung $(m, \mathfrak{a}_0) = 1$ μ stets durch Multiplikation mit einer ℓ–ten Zahlpotenz ξ^ℓ so transformieren, daß

$$(\mu_0) = (\mu \xi^\ell) = m(j\xi)^\ell$$

prim zu $\mathfrak{a}_0$ ist. Dann sei

$$\left(\frac{\mu}{\mathfrak{a}_0}\right) = \left(\frac{\mu\xi^\ell}{\mathfrak{a}_0}\right) = \left(\frac{\mu_0}{\mathfrak{a}_0}\right),$$

was nach 1.) definiert ist.

Wie man leicht übersieht, ist diese erweiterte Definition eindeutig, ferner genügt das Symbol auch so noch einerseits der Multiplikationsregel für „Zähler“ und „Nenner“ und auch falls der Nenner ein Primideal $\mathfrak{p}$ zum Kern hat, seiner Beziehung zur Zerlegung von $\mathfrak{p}$ in $k(\sqrt[\ell]{\mu})$.

236 III

Ist nun μ eine solche Zahl, deren Kern zu $[i]$ prim ist, und

$$\left(\frac{\mu}{i_a}\right) = \zeta_a^{c_a}, \quad \text{wo } \zeta_a \text{ aus } \left(\frac{\omega_a}{i_a}\right) = \zeta_a \neq 1 \text{ [...]}$$

so hat nach Satz 27: $\overline{\mu} = \mu\omega_1^{-c_1} \dots \omega_t^{-c_t}$ die Eigenschaften

$$\left(\frac{\overline{\mu}}{i_a}\right) = \left(\frac{\mu}{i_a}\right)\left(\frac{\omega_a}{i_a}\right)^{-c_a} = \zeta_a^{c_a} \cdot \zeta_a^{-c_a} = 1,$$

d. h. $\overline{\mu}$ ist gegen $[i]$ normiert.

Da insbesondere nach Satz 15 die Primärzahl π eines primären Primideals $\mathfrak{p}$ nur bis auf ein Potenzprodukt singulärer Primärzahlen bestimmt ist, folgt, daß für ein zu $i_1, \dots, i_t$ primes $\mathfrak{p}$ die Primärzahl π, und zwar eindeutig bis auf ℓ–te Zahlpotenzen, so normiert werden darf, daß π gegen $[i]$ normiert ist.

Satz 29. Ist $[i]$ ein vorgegebenes Repräsentantensystem im Sinne von Satz 27 und μ eine Zahl, deren Kern zu $[i]$ prim ist, so kann μ bis auf ℓ–te Zahlpotenzen durch Multiplikation mit singulären Primärzahlen eindeutig gegen $[i]$ normiert werden. Insbesondere existiert zu jedem, von den i_a verschiedenen, primären Primideal $\mathfrak{p}$ stets eine bis auf ℓ–te Zahlpotenzen eindeutig bestimmte, gegen $[i]$ normierte Primärzahl π:

$$(\pi) = \mathfrak{p}j^{\ell}.$$

237 III

Beim Beweis des Reziprozitätsgesetzes haben wir zwei Teile zu unterscheiden:

1.) Den Beweis des Reziprozitätsgesetzes für die *Reste*,

2.) den Beweis des Reziprozitätsgesetzes für die *Nichtreste*.

Unter 1.) verstehen wir dabei die Behauptung:

$$\left(\frac{\mu}{\nu}\right) = 1 \quad \text{dann und nur dann, wenn} \quad \left(\frac{\nu}{\mu}\right) = 1,$$

unter 2.) die weitergehende

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right),$$

die beide in diesem § für beliebige zueinander und zu ℓ prime μ, ν, von denen eine, etwa μ primär ist, bewiesen werden sollen.
□□□

Für den Beweis erweist es sich als zweckmäßig, beide Teile nicht zu trennen, da bei dem Beweis 1.) für zusammengesetzte μ schon ein Teil von 2.), nämlich für Primärzahlen primärer Primideale, zweckmäßig angewendet wird. Wir beginnen mit dem Beweis 1.), falls μ Primärzahl eines primären Primideals $\mathfrak{p}$. Da wir dann ν später in gewisser Weise in einfachste Bestandteile, entsprechend seiner Primidealzerlegung, zerlegen

werden, genügt es, folgenden Satz zu beweisen:

Satz 30. Sei π Primärzahl des primären Primideals $\mathfrak{p}$ und $[i]$ ein gegen π normiertes Repräsentantensystem im Sinne von Satz 27/28*. Ist dann $\mathfrak{r}$ ein beliebiges zu ℓ und $\mathfrak{p}$ primes Primideal und

$$\mathfrak{r} = (\varrho) i_1^{c_1} \dots i_t^{c_t} j^{\ell},$$

kurz

$$\mathfrak{r} = (\varrho)[i]$$

seine Darstellung durch $[i]$, so ist

$$\left(\frac{\pi}{\mathfrak{r}}\right) = \left(\frac{\pi}{\varrho}\right) = 1$$

*π ist genau durch $\mathfrak{p}^1$ teilbar, also nicht singulär primär.

dann und nur dann, wenn

$$\left(\frac{\varrho}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\pi}\right) = 1$$

ist.

Beweis: Da $\mathfrak{r}$ und $[i]$ prim zu ℓ, ist der Kern von ϱ prim zu ℓ, sodaß $\left(\frac{\pi}{\varrho}\right)$ einen Sinn hat. Wegen der Normiertheit von π gegen $[i]$ ist ersichtlich $\left(\frac{\pi}{\varrho}\right) = \left(\frac{\pi}{\mathfrak{r}}\right)$. Andererseits ist natürlich $\left(\frac{\varrho}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\pi}\right)$, weil ja $(\pi) = \mathfrak{p}j^{\ell}$.

Wir betrachten den Körper $k(\sqrt[\ell]{\pi})$, dessen Relativdiskriminante $\mathfrak{p}^{\ell-1}$ ist, weil π primär ist. Unser Satz folgt dann durch Vergleich des „Kummerschen“ mit dem „Klassenkörper“: Zerlegungsgesetz für $\mathfrak{r}$.

Nach dem *Kummerschen Zerlegungsgesetz* zerfällt $\mathfrak{r}$ in $k(\sqrt[\ell]{\pi})$ dann und nur dann, wenn

$$\left(\frac{\pi}{\mathfrak{r}}\right) = 1$$

ist.

Andererseits ist $k(\sqrt[\ell]{\pi})$ Klassenkörper für eine Klassengruppe H vom Index ℓ und Führer $\mathfrak{p}$ (K. K. Satz 45). Diese Klassengruppe muß nach den Überlegungen von §1 bei Satz 3 durch eine Forderung

$$\chi(\mathfrak{a}) = 1$$

charakterisiert werden können, wo χ ein Charakter der Gruppe G mod $\mathfrak{p}$ von §1 ist. Nach Satz 4 hat χ die Form:

$$\chi(\mathfrak{a}) = \zeta^{\sum_{i=1}^{t} a_i u_i} \left(\frac{\alpha}{\mathfrak{p}}\right)^{v},$$

wenn $\mathfrak{a} = (\alpha)[i]$[†] ist, da ja in den Überlegungen von §1 natürlich statt der $\mathfrak{r}_a$ auch die äquivalenten i_a genommen werden dürfen. □□□ Es muß $\chi(i_a) = 1$ sein, da die i_a wegen der Normiertheit gegen π in $k(\sqrt[\ell]{\pi})$ zerfallen. Daraus folgt $u_a \equiv 0 \mod \ell$, also

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{p}}\right)^{v}$$

[†]mit den Exponenten a_i: $\mathfrak{a} = (\alpha) i_1^{a_1} \dots i_t^{a_t} j^{\ell}$

und $v \not\equiv 0 \mod \ell$, weil χ nicht der Hauptcharakter sein kann. Also zerfällt nach dem *Klassenkörper–Zerlegungssatz*

$$\mathfrak{r} = (\varrho)[i]$$

dann und nur dann, wenn

$$\chi(\mathfrak{r}) = \left(\frac{\varrho}{\mathfrak{p}}\right)^v = 1$$

d. h. $\left(\frac{\varrho}{\mathfrak{p}}\right) = 1$ ist, w. z. b. w.

240 III

Um die Unterscheidung der Nichtreste hereinzubekommen, ist das Eisensteinsche Reziprozitätsgesetz zugrundezulegen, das dieselbe im Kreiskörper k_ζ leistet (s. m. Tagebuch **I**, S. 77. ff). Durch die Sätze von §3 folgt daraus für den beliebigen Oberkörper k von k_ζ folgender Satz:

Satz 31. Ist π Primärzahl eines primären Primideals $\mathfrak{p}$ und q eine zu $\mathfrak{p}$ prime rationale Primzahl $\neq \ell$, so ist

$$\left(\frac{\pi}{q}\right) = \left(\frac{q}{\pi}\right).$$

Beweis: Sei $\pi_0 = n(\pi)$ die Relativnorm nach k_ζ. Aus

$$\pi \equiv \xi^\ell \mod \mathfrak{l}_0^\ell$$

(wobei ja π prim zu ℓ angenommen werden darf), folgt

$$\pi_0 = n(\pi) \equiv n(\xi^\ell) \equiv \xi_0^\ell \mod \mathfrak{l}_0^\ell.$$

Also ist π_0 primäre, d. h. sicher semiprimäre Zahl von k_ζ, und folglich nach dem Eisensteinschen Reziprozitätsgesetz:

$$\left[\frac{\pi_0}{q}\right] = \left[\frac{q}{\pi_0}\right],$$

wo die Symbole [ ] sich auf k_ζ beziehen (der Kern von π_0 ist natürlich prim zu q, da der Kern $\mathfrak{p}$ von π es ist). Nach Satz 11 und 12 folgt dann ohne weiteres die Behauptung.

Um nun den Satz 30 und auch diesen Satz für ein beliebiges ν für das dortige ϱ auch für die Nichtreste zu beweisen, haben wir von der Existenz von

241 III

Hilfsprimidealen Gebrauch zu machen, für die das Reziprozitätsgesetz von Satz 30 auch *mit* Unterscheidung der Nichtreste gilt. Diese wird durch folgenden Satz gegeben:

Satz 32. Seien $\mathfrak{q}, \mathfrak{r}$ zwei solche zu ℓ prime Primideale, daß

1.) ihre Ordnungen u, v prim zu ℓ,

2.) die zugeordneten rationalen Primzahlen q, r verschieden

sind, $[i]$ ein zu $\mathfrak{q}, \mathfrak{r}$ primes Repräsentantensystem im Sinne von Satz 27 und

$$\mathfrak{q} = (\kappa)[i]\,; \qquad \mathfrak{r} = (\varrho)[i]$$

die Darstellungen von $\mathfrak{q}$ und $\mathfrak{r}$ durch $[i]$. Sind dann ζ_1, ζ_2 irgendzwei ℓ–te Einheitswurzeln, so gibt es unendlich viele primäre Primideale $\mathfrak{p}_0$, sodaß für die zugehörigen, gegen $[i]$ normierten Primärzahlen π_0 mit einem jeweils durch $\mathfrak{p}_0$ bestimmten, zu ℓ primen Exponenten n gilt:

$$\left(\frac{\kappa}{\pi_0}\right) = \left(\frac{\pi_0}{\kappa}\right) = \zeta_1^n,$$
$$\left(\frac{\varrho}{\pi_0}\right) = \left(\frac{\pi_0}{\varrho}\right) = \zeta_2^n.$$

Beweis: Der Sinn dieses Satzes ist also der, daß unendliche viele $\mathfrak{p}_0$ mit den zugehörigen, gegen $[i]$ normierten π_0 existieren, für die das Reziprozitätsgesetz von Satz 30 *mit* Nichtrestunterscheidung für $\mathfrak{q}$ und $\mathfrak{r}$ *gleichzeitig* gilt.

242 III

Sei

$$q = \mathfrak{q}^u \mathfrak{q}'^{u'} \cdots\,;\ (u \not\equiv 0 \mod \ell)$$
$$r = \mathfrak{r}^v \mathfrak{r}'^{v'} \cdots\,;\ (v \not\equiv 0 \mod \ell)$$

und

$$\mathfrak{q} = (\kappa)[i]\,; \quad \mathfrak{q}' = (\kappa')[i]\,; \ \ldots$$
$$\mathfrak{r} = (\varrho)[i]\,; \quad \mathfrak{r}' = (\varrho')[i]\,; \ \ldots$$

Dann ist also

$$(\kappa^u \kappa'^{u'} \ldots) = (q)[i]\,,$$

also $[i]$ Hauptideal, somit wegen der Unabhängigkeit der i_a

$$[i] = j^\ell = \text{Hauptideal} = [\eta, \omega]\,,$$

wenn $[\eta, \omega]$ einen Ausdruck der Form

$$\eta_1^{x_1} \ldots \eta_{r+1}^{x_{r+1}} \omega_1^{y_1} \ldots \omega_t^{y_t} \xi^\ell$$

bedeutet, in der nach Satz 8 alle ℓ–ten Idealpotenzen der absoluten Hauptklasse enthalten sind. Da Einheiten zu $[\eta, \omega]$ gezogen werden können, ist also:

$$\kappa^u \kappa'^{u'} \cdots = q[\eta, \omega]\,,$$
$$\varrho^v \varrho'^{v'} \cdots = r[\eta, \omega]\,.$$

Nun sind sicher die $\kappa, \kappa', \ldots, \varrho, \varrho', \ldots$ untereinander und von den $[\eta, \omega]$ unabhängig. Denn aus einer Relation

$$\kappa^c \kappa'^{c'} \cdots \varrho^d \varrho'^{d'} \cdots = [\eta, \omega]$$

würde folgen:

$$\mathfrak{q}^c \mathfrak{q}'^{c_1} \cdots \mathfrak{r}^d \mathfrak{r}'^{d'} \cdots = [i]\,.$$

Da aber nach Voraussetzung 2.) die $\mathfrak{q}, \mathfrak{q}', \ldots\ \mathfrak{r}, \mathfrak{r}', \ldots$ sämtlich verschieden, und auch von den i_a verschieden sind, müssen alle Exponenten durch ℓ teilbar, (und rechts $[i] = j^\ell$) sein.

Auf Grund von K. K. Satz 41 folgt daraus die Existenz von unendlich vielen Primidealen $\mathfrak{p}_0$, die den Bedingungen:

$$\left(\frac{\kappa}{\mathfrak{p}_0}\right) = \zeta_1^n, \quad \left(\frac{\kappa'}{\mathfrak{p}_0}\right) = \cdots = 1, \quad \left(\frac{\varrho}{\mathfrak{p}_0}\right) = \zeta_2^n, \quad \left(\frac{\varrho'}{\mathfrak{p}_0}\right) = \cdots = 1$$
$$\left(\frac{[\eta, \omega]}{\mathfrak{p}_0}\right) = 1\,, \quad \text{d. h. } \mathfrak{p}_0 \text{ primär}$$

mit einem jeweils durch $\mathfrak{p}_0$ bestimmten $n \not\equiv 0 \mod \ell$ genügen. Sei dann π_0 die gegen $[i]$ normierte Primärzahl von $\mathfrak{p}_0$, so ist einerseits

$$\left(\frac{\kappa}{\pi_0}\right) = \left(\frac{\kappa}{\mathfrak{p}_0}\right) = \zeta_1^n\,; \quad \left(\frac{\varrho}{\pi_0}\right) = \left(\frac{\varrho}{\mathfrak{p}_0}\right) = \zeta_2^n.$$

Andererseits ist

$$\left(\frac{\kappa^u \kappa'^{u'} \cdots}{\mathfrak{p}_0}\right) = \left(\frac{q}{\mathfrak{p}_0}\right) = \zeta_1^{nu},$$
$$\left(\frac{\varrho^v \varrho'^{v'} \cdots}{\mathfrak{p}_0}\right) = \left(\frac{r}{\mathfrak{p}_0}\right) = \zeta_2^{nv}.$$

Nach Satz 31 ist somit, weil $\mathfrak{p}_0$ prim zu $q, r \neq \ell$:

$$\left(\frac{\pi_0}{q}\right) = \zeta_1^{nu}; \quad \left(\frac{\pi_0}{r}\right) = \zeta_2^{nv}.$$

Ferner ist nach Satz 30, weil π_0 gegen $[i]$ normiert ist

$$\left(\frac{\pi_0}{\mathfrak{q}'}\right) = \cdots = 1; \quad \left(\frac{\pi_0}{\mathfrak{r}'}\right) = \cdots = 1,$$

also

$$\left(\frac{\pi_0}{\kappa}\right) = \left(\frac{\pi_0}{\mathfrak{q}}\right) = \zeta_1^{n}; \quad \left(\frac{\pi_0}{\varrho}\right) = \left(\frac{\pi_0}{\mathfrak{r}}\right) = \zeta_2^{n},$$

weil ja $u, v \not\equiv 0 \mod \ell$. Damit ist die Behauptung bewiesen.

244 III

Anmerkung 1: Natürlich gilt Satz 32 a fortiori auch für nur ein einziges Primideal $\mathfrak{q} = (\kappa)[i]$, wobei natürlich die dann gegenstandslose Voraussetzung 2.) wegfällt.

Anmerkung 2: Wir bezeichnen alle Primideale $\mathfrak{q}$, für die Satz 32[‡] richtig ist, als *regulär*. Ein zu ℓ primes Primideal $\mathfrak{q}$ ist also sicher dann regulär, wenn die Voraussetzung 1.) von Satz 32 für $\mathfrak{q}$ richtig ist, also die Ordnung u von $\mathfrak{q}$ prim zu ℓ ist. Es existieren also höchstens *endlich viele* nicht reguläre $\mathfrak{q}$. Im nächsten §▶ wird jedoch gezeigt werden, *daß jedes zu ℓ prime $\mathfrak{q}$ regulär ist.* Ebenso soll eine Zahl μ regulär heißen, wenn ihr Kern nur reguläre Primideale enthält.

Satz 32 ist für *zwei* reguläre Primideale $\mathfrak{q}, \mathfrak{r}$ sicher richtig, wenn zudem die Voraussetzung 2.) erfüllt ist, d. h. $\mathfrak{q}, \mathfrak{r}$ zu verschiedenen rationalen Primzahlen q, r gehören.

Die Verwendung der Hilfsprimideale $\mathfrak{p}_0$ von Satz 32 geschieht mittels des folgenden Satzes, der zugleich eine Verallgemeinerung von Satz 30 auf ein

[‡] im Sinne von Anmerkung 1, also für $\mathfrak{q}$ allein

Produkt primärer Primideale ist.

245 III

Satz 33. Sind $\mathfrak{p}, \mathfrak{p}_0$ zwei reguläre, primäre zu verschiedenen rationalen Primzahlen gehörige (nicht konjugierte) Primideale mit den gegen ein zu $\mathfrak{p}, \mathfrak{p}_0$ primes Repräsentantensystem $[i]$ normierten Primärzahlen π, π_0, ferner $\mathfrak{r}$ ein zu $\mathfrak{p}, \mathfrak{p}_0, \ell$ primes Primideal mit der Darstellung

$$\mathfrak{r} = (\varrho)[i]$$

durch $[i]$, und e irgend ein ganzzahliger Exponent. Dann ist

$$\left(\frac{\pi\pi_0^e}{\mathfrak{r}}\right) = \left(\frac{\pi\pi_0^e}{\varrho}\right) = 1$$

dann und nur dann, wenn

$$\left(\frac{\varrho}{\pi\pi_0^e}\right) = \left(\frac{\varrho}{\pi\pi_0^e}\right) = 1$$

ist.

Beweis: Der Beweis verläuft ganz analog zum Beweis von Satz 30. Hier ist $k(\sqrt[\ell]{\pi\pi_0^e})$ zu betrachten, dessen Relativdiskriminante, weil $\pi\pi_0^e$ primär ist, $\mathfrak{p}^{\ell-1}$ oder $(\mathfrak{p}\mathfrak{p}_0)^{\ell-1}$ ist. Für die Zerlegung von $\mathfrak{r}$ ist einerseits nach dem Kummerschen Zerlegungsgesetz das Symbol

$$\left(\frac{\pi\pi_0^e}{\mathfrak{r}}\right) = \left(\frac{\pi\pi_0^e}{\varrho}\right); \qquad (\pi, \pi_0 \text{ gegen } [i] \text{ normiert})$$

maßgebend.

Andererseits ist $k(\sqrt[\ell]{\pi\pi_0^e})$ Klassenkörper für eine Klassengruppe H vom Index ℓ, die jedenfalls mod $\mathfrak{p}\mathfrak{p}_0$ erklärbar

246 III

ist und die nach §1▸ durch eine Charaktergleichung:

$$\chi(\mathfrak{a}) = \zeta^{\sum_{i=1}^{t} a_i u_i} \left(\frac{\alpha}{\mathfrak{p}}\right)^v \left(\frac{\alpha}{\mathfrak{p}_0}\right)^{v_0} \quad \text{für} \quad \mathfrak{a} = (\alpha)[i]$$

definiert sein muß. Wegen der Normiertheit von π, π_0 zerfallen die i_a in $k(\sqrt[\ell]{\pi\pi_0^e})$, gehören also zu H, sodaß aus $\chi(i_a) = 1$ folgt: $u_a \equiv 0 \mod \ell$, d. h.

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{p}}\right)^v \left(\frac{\alpha}{\mathfrak{p}_0}\right)^{v_0}.$$

Speziell ist also unser über die Zerlegung von $\mathfrak{r}$ entscheidender Charakter:

$$\chi(\mathfrak{r}) = \left(\frac{\varrho}{\mathfrak{p}}\right)^{v} \left(\frac{\varrho}{\mathfrak{p}_0}\right)^{v_0},$$

sodaß nur

$$\begin{cases} v_0 \equiv ve \mod \ell \\ v \not\equiv 0 \mod \ell \end{cases}$$

nachzuweisen ist.

Dieser letztere Nachweis geschieht nun durch Benutzung eines Hilfsprimideals $\mathfrak{p}_1$, das für $\mathfrak{p}, \mathfrak{p}_0$ die Eigenschaften von Satz 32 hat. Nach Voraussetzung über $\mathfrak{p}, \mathfrak{p}_0$ existiert stets ein solches $\mathfrak{p}_1$ mit der gegen $[i]$ normierten Primärzahl π_1, sodaß

$$\left\{ \begin{array}{l} \left(\frac{\pi}{\pi_1}\right) = \left(\frac{\pi_1}{\pi}\right) = \zeta_1^n \\ \left(\frac{\pi_0}{\pi_1}\right) = \left(\frac{\pi_1}{\pi_0}\right) = \zeta_2^n \end{array} \right\} ; \quad n \not\equiv 0 \mod \ell$$

ist, wenn ζ_1, ζ_2 zwei beliebige ℓ–te Einheitswurzeln

247 III

sind, die wir hier als

$$\zeta_1 = \zeta^{-e}, \qquad \zeta_2 = \zeta$$

wählen. Auf Grund dieser Wahl ist dann

$$\left(\frac{\pi\pi_0^e}{\pi_1}\right) = \left(\frac{\pi\pi_0^e}{\mathfrak{p}_1}\right) = 1,$$

d. h. $\mathfrak{p}_1$ zu H gehörig und daher

$$\chi(\mathfrak{p}_1) = \left(\frac{\pi_1}{\mathfrak{p}}\right)^{v} \left(\frac{\pi_1}{\mathfrak{p}_0}\right)^{v_0} = 1.$$

Andererseits ist nach obigem

$$\begin{aligned} \left(\frac{\pi_1}{\mathfrak{p}}\right) &= \zeta_1^n = \zeta^{-en} \\ \left(\frac{\pi_1}{\mathfrak{p}_0}\right) &= \zeta_2^n = \zeta^n, \end{aligned}$$

also

$$\zeta^{-env+nv_0} = 1,$$

d. h. wegen $n \not\equiv 0 \mod \ell$:

$$v_0 \equiv ev \mod \ell.$$

$v \not\equiv 0 \mod \ell$ ist klar, da sonst χ der Hauptcharakter wäre. Damit ist Satz 33 bewiesen.

Nunmehr können wir das Reziprozitätsgesetz *mit* Nichtrestunterscheidung für eine beliebige Zahl ν und eine Primärzahl π eines primären Primideals $\mathfrak{p}$ beweisen:

Satz 34. Sei π Primärzahl eines regulären, primären Primideals $\mathfrak{p}$ und ν eine beliebige reguläre Zahl, deren Kern zu ℓ und $\mathfrak{p}$ prim ist. Dann gilt das Reziprozitätsgesetz:

$$\left(\frac{\pi}{\nu}\right) = \left(\frac{\nu}{\pi}\right).$$

248 III

Beweis: Da π nicht singulär–primär, weil genau durch $\mathfrak{p}_1$ teilbar, kann ein gegen π normiertes zu ℓ und ν primes Repräsentantensystem $[i]$ im Sinne von Satz 27 gewählt werden.

1.) Sei dann zunächst $\mathfrak{r}$ ein im Kern von ν aufgehendes, also reguläres Primideal und

$$\mathfrak{r} = (\varrho)[i],$$

so beweisen wir den Satz zunächst für ϱ, d. h.

$$\left(\frac{\pi}{\varrho}\right) = \left(\frac{\varrho}{\pi}\right).$$

Für $\left(\frac{\pi}{\varrho}\right) = \left(\frac{\pi}{\mathfrak{r}}\right) = 1$ ist dies nach Satz 30 richtig. Sei also

$$\left(\frac{\pi}{\varrho}\right) = \zeta_1 \neq 1.$$

Nach Satz 32 (Anm. 1) gibt es dann ein primäres Hilfsprimideal $\mathfrak{p}_0$ mit der gegen $[i]$ normierten Primärzahl π_0, sodaß

$$\left(\frac{\pi_0}{\varrho}\right) = \left(\frac{\varrho}{\pi_0}\right) = \zeta_2 \neq 1$$

ist. e sei so gewählt, daß

$$\zeta_1 \zeta_2^e = 1$$

ist; dann ist also

$$\left(\frac{\pi \pi_0^e}{\varrho}\right) = \zeta_1 \zeta_2^e = 1.$$

Da für $\mathfrak{p}_0$ unendlich viele Primideale zur Verfügung stehen, darf $\mathfrak{p}_0$ auch noch regulär und nicht konjugiert zu $\mathfrak{p}$ angenommen werden. Dann folgt nach Satz 33:

249 III

$$\left(\frac{\varrho}{\pi \pi_0^e}\right) = 1,$$

also wegen $\left(\frac{\varrho}{\pi_0^e}\right) = \zeta_2^e$:

$$\left(\frac{\varrho}{\pi}\right) = \zeta_1 = \left(\frac{\pi}{\varrho}\right).$$

2.) Sei nunmehr

$$(\nu) = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_s^{a_s} \mathfrak{j}^{\ell}$$

die „Kerndarstellung“ von (ν), also $a_1, \dots, a_s \not\equiv 0 \mod \ell$ und $\mathfrak{r}_1, \dots, \mathfrak{r}_s$ verschiedene Primideale, die nach Voraussetzung alle regulär sind. Wir setzen

$$\mathfrak{r}_k = (\varrho_k)[i],$$

sodaß ähnlich wie a. S. 242

$$\nu = \varrho_1^{a_1} \dots \varrho_s^{a_s} [\eta, \omega]$$

wird. Dann ist nach 1.)

$$\begin{aligned} \left(\frac{\pi}{\nu}\right) &= \left(\frac{\pi}{\varrho_1}\right)^{a_1} \cdots \left(\frac{\pi}{\varrho_s}\right)^{a_s} = \left(\frac{\varrho_1}{\pi}\right)^{a_1} \cdots \left(\frac{\varrho_s}{\pi}\right)^{a_s} \\ &= \left(\frac{\varrho_1^{a_1} \cdots \varrho_s^{a_s}}{\pi}\right) = \left(\frac{\nu}{\pi}\right), \end{aligned}$$

letzteres, weil $\mathfrak{p}$ primär, also $\left(\frac{[\eta,\omega]}{\mathfrak{p}}\right) = 1$ ist.

Damit ist Satz 34 bewiesen. Wir beweisen nunmehr den Hauptsatz dieses §, nämlich das Reziprozitätsgesetz zwischen einer beliebigen und einer primären Zahl, vorläufig wieder unter der Voraussetzung, daß beide regulär sind.

Satz 35. Sind ν und μ zwei reguläre Zahlen, deren Kerne zu ℓ und zueinander prim sind und μ primär, so besteht das Reziprozitätsgesetz:

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right).$$

Beweis: Ebenso wie wir im vorigen Beweis ν in gewisser Weise entsprechend seiner Kerndarstellung in Zahlfaktoren zerlegten, deren Kern *ein* Primideal war, zerlegen wir jetzt auch μ:

$$(\mu) = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r} j^{\ell}\,; \qquad \mathfrak{p}_k = (\pi_k)[i]$$

also

$$\mu = \pi_1^{a_1} \dots \pi_r^{a_r}[\eta,\omega]\,; \qquad (a_k \not\equiv 0 \mod \ell),$$

wobei $[i]$ ein zum Kern von ν und μ primes Repräsentantensystem im Sinne von Satz 27 ist.

Die Fälle $r = 0, 1$, in denen μ singulär primär bezw., wie sich herausstellen wird, Primärzahl eines primären Primideals $\mathfrak{p}_1$ ist, werden wir nachher leicht gesondert erledigen. Sei also

$$\textbf{a.)} \quad \boldsymbol{r \geqq 2}.$$

Wir beweisen den Satz wie bei Satz 34 zuerst für einen „*Kernprimfaktor*“

$$\mathfrak{r} = (\varrho)[i]$$

von ν, und zwar zuerst das Gesetz für die *Reste*:

$$(3) \qquad \left(\frac{\mu}{\mathfrak{r}}\right) = \left(\frac{\mu}{\varrho}\right) = 1 \quad \text{dann und nur dann, wenn} \quad \left(\frac{\varrho}{\mu}\right) = 1,$$

darauf das vollständige Gesetz für die *Nichtreste*:

(4) $$\left(\frac{\mu}{\varrho}\right) = \left(\frac{\varrho}{\mu}\right)$$

und schließlich leicht durch Zerlegung von ν in Kernprimfaktoren die allgemeine Formel

(5) $$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right)$$

des Satzes. Es ist wesentlich, daß zum Nachweis von (3) nicht vorausgesetzt zu werden braucht, daß $\mathfrak{r}$ regulär ist, während dies für (4) und (5) bezüglich $\mathfrak{r}$, ϱ und ν vorauszusetzen ist.

1.) *Beweis von* (3)

Da für $r \geqq 2$ μ nicht singulär primär ist, *darf* $[i]$ *gegen* μ *normiert angenommen werden*, was in (3) bei $\left(\frac{\mu}{\mathfrak{r}}\right) = \left(\frac{\mu}{\varrho}\right)$ schon vorausgesetzt war.

Dann ist, wie schon mehrfach gezeigt, wegen der Normiertheit von μ gegen $[i]$ die $k(\sqrt[\ell]{\mu})$ zugeordnete Klassengruppe H vom Index ℓ durch eine Charaktergleichung

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{p}_1}\right)^{v_1} \cdots \left(\frac{\alpha}{\mathfrak{p}_r}\right)^{v_r} = 1, \quad \text{wenn} \quad \mathfrak{a} = (\alpha)[i]$$

definiert. (§1▶, μ ist primär!). Es ist also dann und nur dann

(6) $$\left(\frac{\mu}{\mathfrak{r}}\right) = \left(\frac{\mu}{\varrho}\right) = 1,$$

wenn

(7) $$\chi(\mathfrak{r}) = \left(\frac{\varrho}{\mathfrak{p}_1}\right)^{v_1} \cdots \left(\frac{\varrho}{\mathfrak{p}_r}\right)^{v_r} = 1$$

ist. Aus (6), (7) folgt (3), wenn

(8) $$\begin{cases} v_i \equiv a_i w & \mod \ell \\ w \not\equiv 0 & \mod \ell \end{cases}$$

gezeigt werden kann, da dann

$$\chi(\mathfrak{r}) = \left(\frac{\varrho}{\mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}}\right)^w = \left(\frac{\varrho}{\mu}\right)^w$$

folgt.

Um (8) zu beweisen, verfahren wir unter Anwendung derselben Schlußweise, wie a. S. 246▸, so:

Wir bestimmen ein Primideal $\mathfrak{p}_0$ aus:

$$\left(\frac{\pi_1}{\mathfrak{p}_0}\right) = \zeta^{na_2}\,; \quad \left(\frac{\pi_2}{\mathfrak{p}_0}\right) = \zeta^{-na_1}\,; \quad \left(\frac{\pi_3}{\mathfrak{p}_0}\right) = \dots = \left(\frac{\pi_r}{\mathfrak{p}_0}\right) = 1,$$
$$\left(\frac{[\eta,\omega]}{\mathfrak{p}_0}\right) = 1\,, \quad \text{d. h. } \mathfrak{p}_0 \text{ primär},$$

$\mathfrak{p}_0$ hat zu ℓ prime Ordnung und ist prim zu ℓ, ist also regulär.

Dies ist mit einem gewissen Exponenten $n \not\equiv 0 \mod \ell$ sicher möglich, da die π_k von den $[\eta,\omega]$ und untereinander unabhängig sind, weil sie ja durch die erste Potenz der verschiedenen Primideale $\mathfrak{p}_k$ und sonst nur durch die von den $\mathfrak{p}_k$ verschiedenen i_k und ℓ–te [...]potenzen teilbar sind. Da unendlich viele $\mathfrak{p}_0$ zur Verfügung stehen, darf auch $\mathfrak{p}_0$ von zu ℓ primer Ordnung angenommen werden.

Sei π_0 die gegen $[i]$ normierte Primärzahl von $\mathfrak{p}_0$. Da nach Voraussetzung μ, also die $\mathfrak{p}_k$ regulär sind, ist nach 1.) im Beweise von Satz 34:

$$\left(\frac{\pi_k}{\mathfrak{p}_0}\right) = \left(\frac{\pi_k}{\pi_0}\right) = \left(\frac{\pi_0}{\pi_k}\right) = \left(\frac{\pi_0}{\mathfrak{p}_k}\right).$$

(π_0 ist das dortige π, $\mathfrak{p}_k$ entspricht $\mathfrak{r}$, π_k entspricht ϱ)

253 III

Aus den Konstruktionsgleichungen für $\mathfrak{p}_0$ folgt also:

$$\left(\frac{\pi_0}{\mathfrak{p}_1}\right) = \zeta^{na_2}\,; \quad \left(\frac{\pi_0}{\mathfrak{p}_2}\right) = \zeta^{-na_1}\,; \quad \left(\frac{\pi_0}{\mathfrak{p}_3}\right) = \dots = \left(\frac{\pi_0}{\mathfrak{p}_r}\right) = 1$$

d. h.

$$\left(\frac{\pi_0}{\mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r}}\right) = \left(\frac{\pi_0}{\mu}\right) = 1.$$

Da π_0 und μ nach Voraussetzung regulär und ihre Kerne prim zu einander und auch zu ℓ sind, folgt also nach Satz 34:

$$\left(\frac{\mu}{\mathfrak{p}_0}\right) = \left(\frac{\mu}{\pi_0}\right) = 1.$$

$\mathfrak{p}_0$ gehört also zu H und daher ist

$$\chi(\mathfrak{p}_0) = \left(\frac{\pi_0}{\mathfrak{p}_1}\right)^{v_1} \cdots \left(\frac{\pi_0}{\mathfrak{p}_r}\right)^{v_r} = 1.$$

Das ergibt nach obigem:

$$\zeta^{na_2v_1 - na_1v_2} = 1,$$
$$a_2v_1 - a_1v_2 \equiv 0 \mod \ell$$

Da dies für alle Paare von Indizes i, k statt $1, 2$ gilt, folgt

$$v_1 : v_2 : \cdots : v_r \equiv a_1 : a_2 : \cdots : a_r \mod \ell$$

d. h.

$$v_i \equiv a_i w \mod \ell,$$

wobei sicher $w \not\equiv 0 \mod \ell$, da χ nicht der Hauptcharakter sein kann. Damit ist (8) und somit (3) bewiesen.

2.) *Beweis von* (4).

Für $\left(\frac{\mu}{\varrho}\right) = 1$ ist (4) eben bewiesen. Sei jetzt

$$\left(\frac{\mu}{\varrho}\right) = \left(\frac{\mu}{\mathfrak{r}}\right) = \zeta_1 \neq 1.$$

Nach Satz 32 (Anm. 1) existiert, da $\mathfrak{r}$ als Kernteiler

von ν nach Voraussetzung regulär ist, ein primäres Hilfsprimideal $\mathfrak{p}_0$ mit der gegen $[i]$ normierten Primärzahl $\mathfrak{p}_0$ mit der gegen $[i]$ normierten Primärzahl π_0, sodaß

$$\left(\frac{\pi_0}{\varrho}\right) = \left(\frac{\varrho}{\pi_0}\right) = \zeta_2 \neq 1$$

ist. Ist dann

$$\zeta_1 \zeta_2^e = 1,$$

so folgt:

$$\left(\frac{\mu\pi_0^e}{\varrho}\right) = 1.$$

$\mu\pi_0^e$ ist primär und darf regulär vorausgesetzt werden, da für $\mathfrak{p}_0$ unendlich viele Primideale zur Verfügung stehen. Dann ist nach (3) angewendet auf $\mu\pi_0^e$:

$$\left(\frac{\varrho}{\mu\pi_0^e}\right) = 1,$$

also

$$\left(\frac{\varrho}{\mu}\right) \cdot \zeta_2^e = 1$$

d. h.

$$\left(\frac{\varrho}{\mu}\right) = \zeta_1 = \left(\frac{\mu}{\varrho}\right)$$

womit (4) bewiesen ist.

3.) *Beweis von* (5)

Sei jetzt

$$(\nu) = \mathfrak{r}_1^{b_1} \cdots \mathfrak{r}_s^{b_s} j^{\ell}\,; \qquad \mathfrak{r}_i = (\varrho_i)[i]$$

also wie früher

$$\nu = \varrho_1^{b_1} \ldots \varrho_s^{b_s}[\eta, \omega].$$

Dann wird nach dem eben bewiesenen:

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\mu}{\varrho_1}\right)^{b_1} \cdots \left(\frac{\mu}{\varrho_s}\right)^{b_s} = \left(\frac{\varrho_1}{\mu}\right)^{b_1} \cdots \left(\frac{\varrho_s}{\mu}\right)^{b_s} = \left(\frac{\varrho_1^{b_1} \cdots \varrho_s^{b_s}}{\mu}\right) = \left(\frac{\nu}{\mu}\right).$$

Das letztere folgt aus $\left(\frac{[\eta,\omega]}{\mu}\right) = 1$, was wie folgt zu begründen ist:

$[\eta, \omega]$ ist als ℓ–te Idealpotenz in obiger Klassengruppe H

enthalten, also

$$\chi([\eta,\omega]) = 1.$$

Dieser Charakter wird aber, da $[\eta,\omega]$ Hauptideal nach §1 durch den obigen Ausdruck:

$$\chi([\eta,\omega]) = \left(\frac{[\eta,\omega]}{\mathfrak{p}_1}\right)^{a_1 w} \cdots \left(\frac{[\eta,\omega]}{\mathfrak{p}_r}\right)^{a_r w} = \left(\frac{[\eta,\omega]}{\mu}\right)^{w}$$

gegeben, woraus wegen $w \not\equiv 0 \mod \ell$ die Behauptung folgt.

(Sachlich kommt dieser Schluß auf die Anwendung des Bestehens der Bedingungen (9) v. S. 201 für χ heraus).

Damit ist Satz 35 im Falle $r \geqq 2$ bewiesen.

b.) $r = 1$.

Dann ist also

$$(\mu) = \mathfrak{p}^a j^\ell\,; \qquad a \not\equiv 0 \mod \ell.$$

Es sei $aa' \equiv 1 \mod \ell$. Dann kann man auch schreiben:

$$(\mu') = (\mu^{a'}) = \mathfrak{p} j_1^\ell.$$

Wir zeigen, daß dann μ' Primärzahl des notwendig primären (regulären) Primideals $\mathfrak{p}$ ist, sodaß nach Satz 34 für reguläres, zu μ' d. h. auch μ „kernprimes“ ν folgt:

$$\left(\frac{\mu'}{\nu}\right) = \left(\frac{\nu}{\mu'}\right).$$

Wegen $a' \not\equiv 0 \mod \ell$ ist dann auch

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right).$$

Die zu beweisende Behauptung, daß $\mathfrak{p}$ primär und folglich das primäre μ' zugeordnete Primärzahl ist, ist als Umkehrung von Satz 14 anzusehen. Wir formulieren sie so:

Satz 36. Ist $(\mu) = \mathfrak{p}^a j^\ell\,; \quad (a \not\equiv 0 \mod \ell)$ eine primäre Zahl, so ist $\mathfrak{p}$ ein primäres Primideal.

Beweis: Die Relativdiskriminante von $k(\sqrt[\ell]{\mu})$ ist $\mathfrak{p}^{\ell-1}$, $k(\sqrt[\ell]{\mu})$ also Klassenkörper für eine Klassengruppe H vom Faktor $\mathfrak{p}$ und Index ℓ, die durch eine Charaktergleichung

$$\chi(\mathfrak{a}) = 1$$

definiert sein muß. Da μ nicht singulär primär ist, darf ein gegen μ normiertes Repräsentantensystem $[i]$ gewählt werden. Bezogen auf dieses muß für

$$\mathfrak{a} = (\alpha)[i]$$

χ die Form haben:

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{p}}\right)^{v}; \qquad v \not\equiv 0 \mod \ell.$$

Da speziell alle ℓ–ten Idealpotenzen $[\eta, \omega]$ zu H gehören, muß also

$$\left(\frac{[\eta, \omega]}{\mathfrak{p}}\right) = 1$$

sein, d. h. $\mathfrak{p}$ primär, wie behauptet.

c.) $r = 0$

Dann ist also $(\mu) = j^{\ell}$, d. h. μ eine singuläre Primärzahl. Es sei μ_0 eine beliebige primäre, reguläre, aber nicht singulär primäre Zahl. Eine solche kann natürlich stets angegeben werden, etwa als Primzahl für ein reguläres Primideal in der Restklasse $\equiv 1 \mod \mathfrak{l}_0^{\ell}$. Dann ist $\mu\mu_0$ ebenfalls regulär, primär, aber nicht singulär primär, also, (wenn μ_0 auch noch kernprim zu ν gedacht wird),

$$\left(\frac{\mu\mu_0}{\nu}\right) = \left(\frac{\nu}{\mu\mu_0}\right)$$

und

$$\left(\frac{\mu_0}{\nu}\right) = \left(\frac{\nu}{\mu_0}\right),$$

also auch

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right), \qquad \text{w. z. b. w.}$$

Damit ist Satz 53 auch in diesem letzten Fall bewiesen. Natürlich haben hier beide Symbole den Wert 1, da μ eine ℓ–te Idealpotenz. Es gilt also:

Satz 37. Ist ω singuläre Primärzahl und ν eine zu ℓ prime, reguläre Zahl, so ist

$$\left(\frac{\omega}{\nu}\right) = 1.$$

Der letzte Satz ist als Spezialfall des vorangestellten Hauptsatzes 2 anzusehen. Denn $k(\sqrt[\ell]{\omega})$ ist Klassenkörper für die Klassengruppe: „H = Körperzahlen“ und $\left(\frac{\omega}{\nu}\right)$ ist dann eben für die ganze Hauptklasse H gleich 1.

3.6 §6 Beseitigung der Beschränkungen.

258 III

Wir [...][1] in diesem § den Satz:

Satz 38. Jedes zu ℓ prime Primideal, also jede zu ℓ kernprime Zahl aus k ist regulär. Es gelten mithin die Sätze 32–37 von §5 allgemein ohne Beschränkung auf reguläre Zahlen.

Zum Beweise leiten wir eine Reihe Hilfssätze her. Der Hauptschluß liegt in folgendem Hilfssatz.

Hilfssatz 1. Ist μ regulär, primär*, ν eine zu μ u. ℓ kernprime Zahl, deren Kern außer durch reguläre nur durch ein ev. nicht reguläres Primideal $\mathfrak{q}$ in einer zu ℓ primen Potenz $\mathfrak{q}^a$ genau teilbar ist, und ist gleichzeitig

$$\left(\frac{\mu}{\mathfrak{q}}\right) \neq 1\,; \qquad \left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right),$$

so ist $\mathfrak{q}$ regulär.

Beweis: Sei $[i]$ ein gegen μ normiertes zu $\mathfrak{q}$ primes Repräsentantensystem im Sinne von Satz 27, wie es stets existiert, weil μ nicht singulär primär sein soll. Es sei

$$\mathfrak{q} = (\kappa)[i].$$

Nach der Bemerkung von S. 251 oben gilt dann (ersichtlich auch für $r = 1$) die dortige Gleichung (3):

259 III

$$\left(\frac{\mu}{\mathfrak{q}}\right) = 1 \quad \text{dann und nur dann, wenn} \quad \left(\frac{\kappa}{\mu}\right) = 1.$$

Ist aber $\left(\frac{\mu}{\mathfrak{q}}\right) \neq 1$, so kann jetzt nicht, entsprechend dem dortigen (4) auf

$$\left(\frac{\mu}{\mathfrak{q}}\right) = \left(\frac{\mu}{\kappa}\right) = \left(\frac{\kappa}{\mu}\right)$$

[1] „beweisen“ ?

*aber nicht singulär primär

geschlossen werden, sondern nur auf

$$\left(\frac{\kappa}{\mu}\right) = \left(\frac{\mu}{\mathfrak{q}}\right)^e; \qquad (e \not\equiv 0 \mod \ell.)$$

Wir zeigen, daß der hier auftretende Exponent e von μ unabhängig, *sondern nur* $\mathfrak{q}$ *eigentümlich ist.*

Sei nämlich $\mathfrak{p}$ ein reguläres, primäres Primideal, sodaß

$$\left(\frac{\kappa}{\mathfrak{p}}\right) \neq 1,$$

was wegen der Unabhängigkeit von κ von den ℓ–ten Idealpotenzen $[\eta, \omega]$ stets gefunden werden kann, und π die gegen $[i]$ normierte Primärzahl zu $\mathfrak{p}$, das auch prim zu $[i]$ angenommen werden kann.

Nach Satz 30 ist dann

$$\left(\frac{\pi}{\mathfrak{q}}\right) \neq 1.$$

Wir setzen:

$$\left(\frac{\kappa}{\mathfrak{p}}\right) = \left(\frac{\kappa}{\pi}\right) = \left(\frac{\pi}{\mathfrak{q}}\right)^e; \qquad (e \not\equiv 0 \mod \ell).$$

Ferner sei (mit $n \not\equiv 0 \mod \ell$):

$$\left(\frac{\mu\pi^n}{\mathfrak{q}}\right) = 1.$$

Da $\mu\pi^n$ regulär primär ist, folgt nach derselben Schlußweise, wie oben für μ, daß

$$\left(\frac{\kappa}{\mu\pi^n}\right) = 1$$

260 III

ist. Es ist also

$$\left(\frac{\mu}{\mathfrak{q}}\right)\left(\frac{\pi}{\mathfrak{q}}\right)^n = \left(\frac{\kappa}{\mu}\right)\left(\frac{\kappa}{\pi}\right)^n = 1$$

und

$$\left(\frac{\pi}{\mathfrak{q}}\right)^e = \left(\frac{\kappa}{\pi}\right)$$

also:

$$\left(\frac{\mu}{\mathfrak{q}}\right)\left(\frac{\pi}{\mathfrak{q}}\right)^n = \left(\frac{\kappa}{\mu}\right)\left(\frac{\pi}{\mathfrak{q}}\right)^{ne} = 1$$

d. h.

$$\left(\frac{\mu}{\mathfrak{q}}\right) = \left(\frac{\pi}{\mathfrak{q}}\right)^{-n}$$
$$\left(\frac{\kappa}{\mu}\right) = \left(\frac{\pi}{\mathfrak{q}}\right)^{-ne} = \left(\frac{\mu}{\mathfrak{q}}\right)^e$$

Der Exponent e ist also seiner Entstehung nach von μ unabhängig, vielmehr $\mathfrak{q}$ eigentümlich.

Ist $e = 1$, so ist also für alle regulären primären μ:

$$\left(\frac{\kappa}{\mu}\right) = \left(\frac{\mu}{\mathfrak{q}}\right).$$

Dann gibt es also sicher unendlich viele $\mathfrak{p}_0$, wie in Satz 32 gefordert, für $\mathfrak{q}$, also ist $\mathfrak{q}$ regulär.

Sei nun ν eine Zahl, wie im Hilfssatz 1 angegeben:

$$(\nu) = \mathfrak{q}^a \mathfrak{q}'^{a'} \ldots j^\ell$$

wo $\mathfrak{q}', \ldots$ regulär, und die entsprechende *Zahl*zerlegung

$$\nu = \kappa^a \kappa'^{a'} \ldots [\eta, \omega].$$

Dann ist, wie beim Beweise von Satz 35:

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\mu}{\kappa}\right)^a \left(\frac{\mu}{\kappa'}\right)^{a'} \ldots = \left(\frac{\mu}{\mathfrak{q}}\right)^a \left(\frac{\kappa'^{a'} \ldots [\eta, \omega]}{\mu}\right) = \left(\frac{\mu}{\mathfrak{q}}\right)^a \left(\frac{\kappa}{\mu}\right)^{-a} \left(\frac{\nu}{\mu}\right)$$

261 III

also

$$\left(\frac{\mu}{\nu}\right)\left(\frac{\mu}{\mathfrak{q}}\right)^{a(e-1)} = \left(\frac{\nu}{\mu}\right),$$

weil ja wegen der Regularität der $\mathfrak{q}', \ldots$

$$\left(\frac{\kappa'}{\mu}\right) = \left(\frac{\mu}{\kappa'}\right), \ldots$$

ist.

Ist also bekannt, daß $\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right)$ ist, und $a \not\equiv 0 \mod \ell$, so folgt $e \equiv 1 \mod \ell$, also ist nach dem eben bewiesenen $\mathfrak{q}$ regulär, w. z. b. w.

Hilfssatz 2. Es sei K ein Oberkörper von k, ζ in k enthalten und $\mathfrak{Q}$ ein Primteiler f–ten Relativgrades des zu ℓ primen Primteilers $\mathfrak{q}$ in k, sodaß

$$n(\mathfrak{Q}) = \mathfrak{q}^f\,; \qquad \boldsymbol{f \not\equiv 0 \mod \ell}$$

ist. Ist dann $\mathfrak{q}$ regulär in k, so ist $\mathfrak{Q}$ regulär in K und umgekehrt.

Beweis: 1.) Sei

$$(\mathsf{A}) = \mathfrak{Q}\mathfrak{A},$$

also

$$(\alpha) = \big(n(\mathsf{A})\big) = \mathfrak{q}^f\mathfrak{a},$$

wobei $\mathfrak{A}$ prim zu $\mathfrak{Q}$ und seinen konjugierten, also $\mathfrak{a} = n(\mathfrak{A})$ prim zu $\mathfrak{q}$ ist. $\mathfrak{A}$ und $\mathfrak{a}$ dürfen ferner prim zu ℓ und auch regulär in K bezw. k angenommen werden, da sie ja aus Primteilern von zu ℓ primer Ordnung zusammengesetzt werden können. Es sei ferner μ eine reguläre, primäre Zahl aus k, die auch in K regulär und primär ist, und für die

262 III

(1)
$$\left(\frac{\mu}{\mathfrak{q}}\right) \neq 1$$

ist, und wie sie etwa als Primzahl eines regulären Primideals in der Restklasse $\equiv 1 \mod \mathfrak{l}_0^\ell$, $\equiv$ Nichtrest mod $\mathfrak{q}$ gefunden werden kann, so daß μ außerdem auch noch kernprim zu A, α ist.

Nach §3, Satz 11, 12 ist dann

$$\left\{\frac{\mu}{\mathsf{A}}\right\} = \left(\frac{\mu}{\alpha}\right), \qquad \left\{\frac{\mathsf{A}}{\mu}\right\} = \left(\frac{\alpha}{\mu}\right)$$

wenn $\{\ \}$ das Legendre Symbol in K bezeichnet. Ist daher $\mathfrak{q}$ regulär in k, also da $\mathfrak{a}$ regulär in k,□□□ auch α, so ist

$$\left(\frac{\mu}{\alpha}\right) = \left(\frac{\alpha}{\mu}\right) \tag{2}$$

also

$$\left\{\frac{\mu}{\mathsf{A}}\right\} = \left\{\frac{\mathsf{A}}{\mu}\right\}. \tag{3}$$

A ist nach Konstruktion nur durch die erste Potenz der möglicherweise nicht regulären $\mathfrak{Q}$ teilbar, ferner nach (1)

$$\left\{\frac{\mu}{\mathfrak{Q}}\right\} = \left(\frac{\mu}{n(\mathfrak{Q})}\right) = \left(\frac{\mu}{\mathfrak{q}}\right)^f \neq 1.$$

Daher ist nach Hilfssatz 1 $\mathfrak{Q}$ regulär in K.

2.) Ist umgekehrt $\mathfrak{Q}$ regulär in K, also auch A, so gilt (3), also (2). α ist nach Konstruktion nur durch die zu ℓ prime f–te Potenz des ev. nicht regulären $\mathfrak{q}$ teilbar. Also lehrt (2) und (1) nach Hilfssatz (1.), daß $\mathfrak{q}$ regulär in k.

263 III

Hilfssatz 3. Ist K ein Oberkörper von k, ζ in k enthalten, und zerfalle das zu ℓ prime Primideal $\mathfrak{q}$ von k in K so:

$$\mathfrak{q} = \mathfrak{Q}$$

oder $$\mathfrak{q} = \mathfrak{Q}^g; \qquad (g \not\equiv 0 \mod \ell),$$

so ist $\mathfrak{q}$ mit $\mathfrak{Q}$ gleichzeitig regulär oder nicht regulär im betr. Körper.

Beweis: 1.) Es sei wieder

$$(\alpha) = \mathfrak{q}\mathfrak{a}$$

und α prim zu $\mathfrak{q}, \ell$; $\mathfrak{a}$ sei regulär in k und K, was alles stets erreicht werden kann.

Ferner sei M eine zu α prime, primäre Zahl aus K, sodaß auch

$$\mu = n(\mathsf{M})$$

primär in k ist. Wir dürfen μ und M so annehmen, daß sie regulär in k und K sind, etwa M als Primzahl eines Primideals zu ℓ primer Ordnung in der Restklasse $\equiv 1 \mod \mathfrak{l}_0^{\ell}$, und außerdem auch noch so, daß

$$\left\{\frac{\mathsf{M}}{\mathfrak{q}}\right\} = \left(\frac{\mu}{\mathfrak{q}}\right) \neq 1 \tag{4}$$

ist, indem wir noch eine geeignete Restklasse mod $\mathfrak{Q}$ vorschreiben.

Ist dann $\mathfrak{q}$, also α regulär in k, so ist wieder

$$\left(\frac{\mu}{\alpha}\right) = \left(\frac{\alpha}{\mu}\right), \tag{5}$$

also

$$\left\{\frac{\mathsf{M}}{\alpha}\right\} = \left\{\frac{\alpha}{\mathsf{M}}\right\}. \tag{6}$$

264 III

Da

$$\left\{\frac{\mathsf{M}}{\mathfrak{q}}\right\} = \left\{\frac{\mathsf{M}}{\mathfrak{Q}}\right\}^g \neq 1, \quad \text{also} \quad \left\{\frac{\mathsf{M}}{\mathfrak{Q}}\right\} \neq 1$$

ist, folgt nach Hilfssatz 1, daß $\mathfrak{Q}$ regulär in K.

2.) Ist umgekehrt $\mathfrak{Q}$ regulär in K, so gilt, da dann auch α regulär in K ist, die Gleichung (6), also (5), die mit (4) nach Hilfssatz 1 lehrt, daß $\mathfrak{q}$ regulär in k.

Hilfssatz 2, 3 genügen nunmehr zu dem sehr einfachen Beweis von Satz 38.

Beweis von Satz 38: Sei $\mathfrak{q}$ ein zu ℓ primes Primideal in k, q die zugehörige rationale Primzahl, $\mathfrak{q}_0$ der $\mathfrak{q}$ entsprechende Primteiler von q im Kreiskörper k_ζ. Dann ist $\mathfrak{q}_0$ sicher regulär in k_ζ, da seine Ordnung 1 ist.

Es sei nun K der zu k gehörige Normalkörper über k_ζ, und K_T der Trägheitskörper eines in $\mathfrak{q}_0$ aufgehenden Primideals $\mathfrak{Q}$ aus K. Das $\mathfrak{Q}$ entsprechende Primideal $\mathfrak{Q}_T$ von K_T ist dann□□□ regulär in K_T, weil es in bezug auf $\mathfrak{q}_0$ die Relativordnung 1, also insgesamt die Ordnung 1 hat.

Da aber $\mathfrak{Q}$ in bezug auf $\mathfrak{Q}_T$ den Relativgrad $f = 1$ hat, ist nach Hilfssatz 2 $\mathfrak{Q}$ regulär in K. Das gilt für jeden Teiler $\mathfrak{Q}$ von $\mathfrak{q}_0$ in K.

Sei jetzt $\mathfrak{Q}$ ein in $\mathfrak{q}$ aufgehender Primteiler von K, k_z und k_t Zerlegungs und Trägheitskörper von $\mathfrak{Q}$ in Bezug auf k, und $\mathfrak{q}_z, \mathfrak{q}_t$ die entsprechenden Primteiler. Da $\mathfrak{Q}$ nach $\mathfrak{q}_t$ den Relativgrad 1 hat, ist nach H. S. 2 $\mathfrak{q}$ regulär in k_t, da $\mathfrak{q}_t = \mathfrak{q}_z$ nach Hilfssatz 2 $\mathfrak{q}_z$ regulär in k_z, da $\mathfrak{q}_z$ nach $\mathfrak{q}$ den Rel. Gr. 1 hat, $\mathfrak{q}$ regulär in k, w. z. b. w.

§7 Erster und zweiter Ergänzungssatz (ℓ ungerade).[2]

Aus Satz 35 und 38 folgt jetzt unmittelbar, wenn $\nu = \varepsilon = \mathfrak{a}^\ell$ eine ℓ–te Idealpotenz ist:

Satz 39. (Erster Ergänzungssatz).
Ist α primär und ε eine ℓ–te Idealpotenz so gilt

$$\left(\frac{\varepsilon}{\alpha}\right) = 1.$$

Ferner gilt:

Satz 40. (Zweiter Ergänzungssatz).
Ist α hyperprimär und λ außer durch Primteiler $\mathfrak{l}_i$ von ℓ nur durch ℓ–te Idealpotenzen teilbar, d. h. der Kern von λ ein Potenzprodukt der $\mathfrak{l}_i$, so gilt:

$$\left(\frac{\lambda}{\alpha}\right) = 1.$$

Satz 40 ist ersichtlich in folgendem allgemeineren Satz enthalten, den wir zwecks späterer Anwendung beweisen:

Satz 41. Ist

$$\beta = \prod_{i=1}^{z} \mathfrak{l}_i^{a_i} \mathfrak{b} j^\ell; \qquad (0 \leqq a_i \leqq \ell - 1),$$

wo der Kern $\mathfrak{b}$ prim zu ℓ, und α eine zu β kernprime primäre Zahl, welche überdies für die $\mathfrak{l}_i$ mit $a_i \neq 0$ hyperprimär ist*, so gilt:

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right)$$

[2]Hasse listet diesen Paragraphen nicht im Inhaltsverzeichnis auf. Dort steht „§7 Das Hilbertsche Reziprozitätsgesetz ($\ell \neq 2$).“

*d. h. der betr. Kongr. für jedes solche $\mathfrak{l}_i$ einzeln genügt.

Beweis: Sei $[i]$ ein gegen α normiertes Repräsentantensystem im Sinne von Satz 27/28. Das kann stets gefunden werden, wenn nicht gerade α singulär primär ist, was wir vorläufig ausschließen.

Wegen der Normiertheit ist dann die $k(\sqrt[\ell]{\alpha})$ zugeordnete Klassengruppe durch

$$\chi(\mathfrak{c}) = \left(\frac{\gamma}{\alpha}\right)^w = 1\,; \qquad w \not\equiv 0 \mod \ell, \quad \text{für} \quad \mathfrak{c} = (\mu)[i]$$

charakterisiert, wie unmittelbar aus dem Beweis von Satz 35 zu entnehmen. Nach Voraussetzung über α zerfallen die $\mathfrak{l}_i$ mit $a_i \neq 0$ in $k(\sqrt[\ell]{\alpha})$, sodaß für sie und:

$$\mathfrak{l}_i = (\lambda_i)[i]$$

folgt:

$$1 = \chi(\mathfrak{l}_i) = \left(\frac{\lambda_i}{\alpha}\right)^w, \quad \text{d. h.} \quad \left(\frac{\lambda_i}{\alpha}\right) = 1, \quad \text{wenn} \quad a_i \neq 0.$$

Wird ferner

$$\mathfrak{b} = (\beta_0)[i]$$

gesetzt, so folgt, wie schon häufig:

$$\beta = \beta_0 \prod_{i=1}^{z} \lambda_i^{a_i}[\eta, \omega].$$

Also ist:

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\beta_0}{\alpha}\right) \prod_{i=1}^{z} \left(\frac{\lambda_i}{\alpha}\right)^{a_i} \qquad \text{(s. S. 255}^{\blacktriangleright}\text{)},$$

und weil β_0 zu ℓ kernprim, nach Satz 35:

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\alpha}{\beta_0}\right) \prod_{i=1}^{z} \left(\frac{\lambda_i}{\alpha}\right)^{a_i} = \left(\frac{\alpha}{\beta_0}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right),$$

weil die $\left(\frac{\lambda_i}{\alpha}\right)$ mit $a_i = 0$ von selbst herausfallen.

Für $\mathfrak{b} = j^\ell$ folgt daraus speziell Satz 40.

Ist α singulär primär, so kann es durch Multiplikation mit einer geeigneten Hyperprimärzahl, wie bei Satz 37, S. 257$^{\blacktriangleright}$, so transformiert werden, daß es nicht mehr singulär ist, und der Satz gilt.

3.7 §7 Das Hilbertsche Reziprozitätsgesetz ($\ell \neq 2$).

§7 Das Hilbertsche Reziprozitätsgesetz (ℓ ungerade).

Wir führen zunächst für die zu ℓ primen $\mathfrak{p}$ das Hilbertsche Normenrestsymbol ein:

Sind α, β zwei Zahlen aus $k(\zeta)$ mit den Darstellungen

$$\left.\begin{array}{rcl} \alpha & = & \pi^a \omega^b \xi^\ell \\ \beta & = & \pi^c \omega^d \eta^\ell \end{array}\right\} (\mathfrak{p}),$$

wo π Primzahl für $\mathfrak{p}$ und ω eine solche $(p^f - 1)$ te Einheitswurzel (f Grad von $\mathfrak{p}$), daß

$$\omega^{\frac{p^f-1}{\ell}} = \zeta$$

ist, so sei

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \zeta^{bc-ad}.$$

Nach den Ergebnissen von einer Henselschen Arbeit (Ann. **85**) folgt:

Satz 42. Es ist dann und nur dann $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = 1$, wenn α Normzahl von $k(\sqrt[\ell]{\beta})$ für den Bereich von $\mathfrak{p}$ ist. Das Symbol genügt den Gleichungen

$$\left.\begin{array}{rcl} \left(\frac{\alpha_1,\beta}{\mathfrak{p}}\right)\left(\frac{\alpha_2,\beta}{\mathfrak{p}}\right) & = & \left(\frac{\alpha_1\alpha_2,\beta}{\mathfrak{p}}\right) \\ \left(\frac{\alpha,\beta_1}{\mathfrak{p}}\right)\left(\frac{\alpha,\beta_2}{\mathfrak{p}}\right) & = & \left(\frac{\alpha,\beta_1\beta_2}{\mathfrak{p}}\right) \end{array}\right\}; \quad \text{(Zerlegungssatz)},$$

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)\left(\frac{\beta, \alpha}{\mathfrak{p}}\right) = 1; \qquad \text{(Vertauschungssatz)}.$$

Ferner gilt der folgende Satz, der die Bedeutung des Symbols für das Reziprozitätsgesetz darlegt:

Satz 43. Sind α, β zwei* kernprime Zahlen aus k mit den Idealzerlegungen

$$(\alpha) = \mathfrak{a} \cdot j_1^{\ell} \prod_i \mathfrak{l}_i^{a_i}\,; \qquad (\beta) = \mathfrak{b} \cdot j_2^{\ell} \prod_i \mathfrak{l}_i^{b_i},$$

wo $\mathfrak{a}, \mathfrak{b}$ die zu ℓ primen Bestandteile der Kerne und $\mathfrak{l}_i$ Primteiler von ℓ sind, so ist

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right) \cdot \left(\frac{\beta}{\mathfrak{a}}\right)^{-1}$$

wo $\mathfrak{p}$ alle zu ℓ primen Primteiler durchläuft.

Beweis: Sei

$$\mathfrak{a} = \prod_{\mathfrak{q}} \mathfrak{q}^a\,; \qquad \mathfrak{b} = \prod_{\mathfrak{r}} \mathfrak{r}^c$$

die Primidealzerlegung von $\mathfrak{a}$ und $\mathfrak{b}$. Für ein von den $\mathfrak{q}, \mathfrak{r}$ verschiedenes, zu ℓ primes $\mathfrak{p}$ ist nach Definition $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = 1$. Ferner ist

$$\prod_{\mathfrak{r}} \left(\frac{\alpha, \beta}{\mathfrak{r}}\right) = \prod_{\mathfrak{r}} \zeta^{bc},$$

da die $\mathfrak{r}$ von den $\mathfrak{q}$ verschieden, also die betr. Ordnungszahlen der Zahl α gleich Null sind. b bedeutet die Indizes von α für die $\mathfrak{r}$, und somit ist nach Definition des Legendresymbols

$$\zeta^b = \left(\frac{\alpha}{\mathfrak{r}}\right),$$

also

$$\prod_{\mathfrak{r}} \zeta^{bc} = \prod_{\mathfrak{r}} \left(\frac{\alpha}{\mathfrak{r}^c}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right).$$

Ebenso folgt

$$\prod_{\mathfrak{q}} \left(\frac{\alpha, \beta}{\mathfrak{q}}\right) = \prod_{\mathfrak{q}} \zeta^{-ad} = \left(\frac{\beta}{\mathfrak{a}}\right)^{-1},$$

also die Behauptung.

Für die $\mathfrak{l}_i$ können wir vorerst die Normenrestsymbole $\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right)$ nur *vorläufig* definieren, nämlich

*für die zu ℓ primen Primteiler $\mathfrak{p}$

269 III

$$\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right) = 1 \quad \text{oder} \quad \zeta^r \qquad (r \not\equiv 0 \mod \ell)$$

je nachdem α Normzahl von $k(\sqrt[\ell]{\beta})$ für den Bereich von $\mathfrak{l}_i$ oder nicht. Wie ich in Ann..... gezeigt habe, läßt sich ohne das Reziprozitätsgesetz beweisen, daß man diese vorläufige Definition so ergänzen kann, daß diese Symbole ebenfalls Vertauschungs– u. Zerlegungssatz genügen, und daß hierdurch der Wert *aller* Symbole $\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right)$ für festes $\mathfrak{l}_i$ bis auf einen konstanten Faktor $c_i \not\equiv 0 \mod \ell$ im Exponenten von ζ eindeutig festgelegt ist. Die Festlegung dieser z Faktoren c_i für $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ muß notwendig auf Grund des allgemeinen Reziprozitätsgesetzes geschehen. Da die hierzu erforderlichen Betrachtungen den Vertauschungs– und Zerlegungssatz für $\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right)$ indirekt aus Satz 42 her liefern werden, und damit auch die Eindeutigkeit der Definition der $\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right)$ als Normenrestsymbole mit der Eigenschaft, dem Zerlegungs– und Vertauschungssatz zu genügen, nachträglich erschlossen werden kann, soll hier von den Entwicklungen meiner genannten Arbeit in Ann. .... nichts vorausgesetzt werden.

Wir führen jetzt die Symbole $\left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right)$ indirekt ein, indem wir zunächst gewisse Symbole $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right]$ einführen, von denen wir nachweisen, daß sie erstens Normenrestsymbole "für die $\mathfrak{l}_i$ im Sinne obiger vorläufigen Definition sind, zweitens Zerlegungs– und Vertauschungssatz genügen.

270 III

Diese Symbole $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right]$ können dann also $= \left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right)$ gesetzt werden, und liefern so die oben bei dem skizzierten Wege nicht zu erhaltende Normierung der $\left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right)$.

Seien im folgenden zwei ganz beliebige α und β aus k gegeben. Wir bestimmen dann ein System von z zu β kernprimen[†] Zahlen α_i aus k, die den einzelnen $\mathfrak{l}_i$ zugeordnet sind, sodaß

$$\alpha_i = \alpha\xi_{ii}^{\ell}(\mathfrak{l}_i); \qquad \alpha_i = \xi_{i\kappa}^{\ell}(\mathfrak{l}_\kappa); \qquad (i \neq \kappa) \qquad (i,\kappa = 1,\ldots,z)$$

wird. Dies ist durch Auflösung eines Systems von Kongruenzen nach hinreichend hohen Potenzen der verschiedenen Primteiler $\mathfrak{l}_i$ stets möglich, weil ja jede Einseinheit hinreichend hohen $\left(\left(\frac{e_i\ell}{\ell-1}+1\right)\text{–ten}\right)$ Grades ℓ–te Potenz in $k(\mathfrak{l}_i)$ ist. Es sind dabei also die $\xi_{i\kappa}$ solche Zahlen aus $k(\mathfrak{l}_\kappa)$, deren ℓ–te Potenzen Zahlen aus k sind. Da es für die α_i nur auf gewisse Restklassen ankommt,

[†] für die zu ℓ primen $\mathfrak{p}$

dürfen sie auch, wie verlangt, kernprim zu β angenommen werden. Es wird dann noch:

$$\alpha_1 \dots \alpha_z = \alpha \prod_i \xi_{i\kappa}^{\ell}(\mathfrak{l}_\kappa); \qquad (\text{für} \quad \kappa = 1, \dots, z)$$

d. h. $$\frac{\alpha_1 \dots \alpha_z}{\alpha} = \gamma$$

eine hyperprimäre Zahl aus k, (hyperprimär = ℓ–te Potenz in allen $k(\mathfrak{l}_\kappa)$. □□□

271 III

Satz 44. Es werde mit den eben erklärten Bezeichnungen

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right] = \prod_{\mathfrak{p}} \left(\frac{\alpha_i, \beta}{\mathfrak{p}}\right); \qquad (\text{für} \quad i = 1, 2, \dots, z)$$

gesetzt, wo $\mathfrak{p}$ alle zu ℓ primen Primteiler von k durchläuft. Dann ist das so definierte Symbol $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right]$ unabhängig von der speziellen Auswahl der α_i.
Ferner gilt:

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right] = 1 \quad \text{für alle } i, \text{ wenn } \beta \text{ hyperprimär},$$

$$\left.\begin{aligned} \left[\tfrac{\beta_1,\alpha}{\mathfrak{l}_i}\right]\left[\tfrac{\beta_2,\alpha}{\mathfrak{l}_i}\right] &= \left[\tfrac{\beta_1\beta_2,\alpha}{\mathfrak{l}_i}\right] \\ \left[\tfrac{\beta,\alpha^{(1)}}{\mathfrak{l}_i}\right]\left[\tfrac{\beta,\alpha^{(2)}}{\mathfrak{l}_i}\right] &= \left[\tfrac{\beta,\alpha^{(1)}\alpha^{(2)}}{\mathfrak{l}_i}\right] \end{aligned}\right\}; \quad (\text{Zerlegungssatz}),$$

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right]\left[\frac{\alpha, \beta}{\mathfrak{l}_i}\right] = 1; \qquad (\text{Vertauschungssatz})$$

Beweis: 1.) Ist β hyperprimär und $\mathfrak{a}_i$ der zu ℓ prime Kernbestandteil von α_i, also prim zum Kern von β, so folgt nach Satz 43:

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right] = \left(\frac{\alpha_i}{\beta}\right)\left(\frac{\beta}{\mathfrak{a}_i}\right)^{-1}.$$

Nach Satz 41 ist also $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = 1$.

2.) Daraus folgt leicht die Eindeutigkeit der Definition. Zunächst ist nämlich der Zerlegungssatz für β unmittelbar klar nach Satz 42 und für α ebenfalls, da zu $\alpha^{(1)}\alpha^{(2)}$ offenbar $\alpha_i^{(1)}\alpha_i^{(2)}$ ein geeignetes System ist, wenn $\alpha_i^{(1)}$ zu

$\alpha^{(1)}$ und $\alpha_i^{(2)}$ zu $\alpha^{(2)}$ gehört. Ist nun α_i' ein anderes System obiger Eigenschaften zu α, so ist $\gamma_i = \frac{\alpha_i'}{\alpha_i}$ hyperprimär, also nach

Satz 42:

$$\prod_{\mathfrak{p}} \left(\frac{\alpha_i', \beta}{\mathfrak{p}}\right) : \prod_{\mathfrak{p}} \left(\frac{\alpha_i, \beta}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}} \left(\frac{\gamma_i, \beta}{\mathfrak{p}}\right) = \left(\frac{\gamma_i}{\mathfrak{b}}\right)\left(\frac{\beta}{\gamma_i}\right)^{-1},$$

wenn $\mathfrak{b}$ der zu ℓ prime Kernbestandteil von β ist. Nach Satz 41 ist dies dann $= 1$, woraus die Eindeutigkeit folgt.

3.) Für den Beweis des Vertauschungssatzes benötigen wir die aus dem nächsten Satz sich ergebende Beziehung

$$\left[\frac{\alpha, \alpha}{\mathfrak{l}_i}\right] = 1.$$

Aus dieser und Zerlegungssatz folgt der Vertauschungssatz einfach so:

$$[\beta, \alpha] = [\beta\alpha^{\ell-1}, \alpha] = [\beta\alpha^{\ell-1}, \beta\alpha^{\ell}] = [\beta, \beta][\alpha^{\ell-1}, \beta] = [\alpha, \beta]^{-1},$$

wenn nacheinander mit $[\alpha^{\ell-1}, \alpha] = [\alpha, \alpha]^{\ell-1} = 1$ und $[\beta\alpha^{\ell-1}, \beta\alpha^{\ell-1}] = 1$ multipliziert, ferner $[\beta\alpha^{\ell-1}, \alpha^{\ell}] = 1$ und $[\alpha^{\ell-1}, \beta] = [\alpha, \beta]^{\ell-1} = [\alpha, \beta]^{-1}$ berücksichtigt wird. (Die $\mathfrak{l}_i$ unter den Symbolen sind der Kürze halber fortgelassen).

Wir zeigen jetzt, daß das eingeführte Symbol $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right]$ das Normenrestsymbol für $\mathfrak{l}_i$ ist. Dies geschieht durch folgenden Satz:

Satz 45. Es ist dann und nur dann

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right] = 1,$$

wenn

$$\left(\frac{\beta, \alpha}{\mathfrak{l}_i}\right) = 1$$

ist.

Beweis: 1.) Es sei $\left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right) = 1$, also β Normzahl von $k(\sqrt[\ell]{\alpha})$ für $\mathfrak{l}_i$, also da $k(\sqrt[\ell]{\alpha}) = k(\sqrt[\ell]{\alpha_i})$ für den Bereich

von $\mathfrak{l}_i$ ist, auch β Normzahl von $k(\sqrt[\ell]{\alpha_i})$ nach $\mathfrak{l}_i$. Es sei

$$(\alpha_i) = \mathfrak{l}_i^{a_i}\mathfrak{a}_i j^{\ell}$$

wo nach Bestimmung von α_i $\mathfrak{a}_i$ zu ℓ prim angenommen werden kann. $\mathfrak{a}_i$ ist dann der zu ℓ prime Kernbestandteil von α_i. Die Relativdiskriminante $\mathfrak{D} = f^{\ell-1}$ von $k(\sqrt[\ell]{\alpha_i})$ ist dann so beschaffen, daß f ein Teiler von

$$\mathfrak{l}_i^{\frac{e_i\ell}{\ell-1}+1}\mathfrak{a}_i$$

ist, denn da α_i für die übrigen $\mathfrak{l}_k$ hyperprimär, gehen diese in f nicht auf, und $\mathfrak{l}_i$ höchstens zum angegebenen Exponenten, die Teiler von $\mathfrak{a}_i$ genau zur ersten Potenz. Wir bestimmen nun auf Grund des Satzes von der arithmetischen Progression (S. 160▸) eine Zahl ϱ, sodaß

$$\varrho = \beta i_\kappa^{\ell}(\mathfrak{l}_\kappa); \qquad (\kappa = 1, 2, \ldots, z)$$
$$\varrho \equiv 1 \mod \mathfrak{a}_i; \qquad (\varrho) = \mathfrak{r}\prod_\kappa \mathfrak{l}_\kappa^{b_\kappa}; \qquad (\mathfrak{r} \text{ Primideal})$$

wird, was stets möglich, da auch die Bedingungen für die $\mathfrak{l}_\kappa$ als Kongruenzbedingungen nach genügend hohen Moduln auffaßbar sind, und da durch die angegebenen Kongruenzbedingungen und Wegdivision der gemeinsamen Teiler $\mathfrak{l}_\kappa^{b_\kappa}$ in den für die $\mathfrak{l}_\kappa$ eine eindeutig bestimmte Strahlklasse mod $\ell^N\mathfrak{a}_i$ für hinreichend großes N fixieren. (Genauere Ausführung siehe in meiner Arbeit über quadr. Formen in algebr. Körpern, Cr. **153**, I/II).

Wenn wir nun nachweisen, daß das Primideal $\mathfrak{r}$ zur Hauptklasse der $k(\sqrt[\ell]{\alpha_i})$ zugeordneten Klasseneinteilung gehört, so folgt

$$\left(\frac{\alpha_i}{\mathfrak{r}}\right) = 1$$

Andererseits ist nach Wahl von ϱ:

$$\left(\frac{\varrho}{\mathfrak{a}_i}\right) = 1,$$

also [...]:

$$\left[\frac{[\ldots]}{\mathfrak{l}_i}\right] = \prod_{\mathfrak{p}}\left(\frac{\alpha_i, \varrho}{\mathfrak{p}}\right) = \left(\frac{\alpha_i}{\mathfrak{r}}\right)\left(\frac{\varrho}{\mathfrak{a}_i}\right)^{-1} = 1$$

und weiter, da nach Wahl von ϱ: $\frac{\varrho}{\beta}$ hyperprimär ist, auf Grund von Satz 44 auch $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = 1$.

Wir haben also nur zu zeigen, daß $\mathfrak{r}$ zur genannten Klassengruppe H gehört, die erzeugt wird durch die Relativnormen der zu f primen Ideale aus $k(\sqrt[\ell]{\alpha_i})$ und nach dem Strahl der Normenreste mod f erklärbar ist.

a.) α *hyperprimär für* $\mathfrak{l}_i$.

Dann zerfallen *alle* $\mathfrak{l}_\kappa$ in $k(\sqrt[\ell]{\alpha_i})$, da α_i für sie hyperprimär, gehören also zu H. β ist kernprim zu α_i (nach Wahl von α_i) für die zu ℓ primen $\mathfrak{p}$, also prim zu f, da f prim zu ℓ; also ist ϱ nach Konstruktion ein zu f primer Normenrest mod f, gehört also zu H, und somit auch $\mathfrak{r} = \frac{(\varrho)}{\prod\limits_\kappa \mathfrak{l}_\kappa^{b_\kappa}}$.

b.) α *primär, aber nicht hyperprimär für* $\mathfrak{l}_i$.

Dann zerfallen die $\mathfrak{l}_\kappa$ $(\kappa \neq i)$ wie vorher, gehören also zu H. $\mathfrak{l}_i, \mathfrak{l}_\kappa$ geht nicht in f auf, also ist β wieder kernprim zu f, ϱ nach Konstruktion ein zu f primer Normenrest mod f. β muß aber auch kernprim zu $\mathfrak{l}_i$ sein,

da es sonst nicht Normzahl für $\mathfrak{l}_i$ sein kann. Also ist die obige Größe $\mathfrak{l}_i^{b_i} = \mathfrak{l}_i^{\ell c_i} = n(\mathfrak{l}_i^{c_i})$. Daher gehört

$$\frac{(\varrho)}{\mathfrak{l}_i^{b_i}} = \frac{(\varrho)}{n(\mathfrak{l}_i^{c_i})}$$

zu H, da ϱ und jede Relativnorm eines zu f primen Ideals zu H gehört, und somit auch $\mathfrak{r}$.

c.) α *nicht primär für* $\mathfrak{l}_i$.

Es kommt wieder nur darauf an, zu zeigen, daß $\frac{(\varrho)}{\mathfrak{l}_i^{b_i}}$ zu H gehört. Hier ist $\mathfrak{l}_i$ ein Teiler von f und daher $\mathfrak{l}_i = n(\mathfrak{L}_i)$, wo $\mathfrak{L}_i$ den Teiler von $\mathfrak{l}_i$ in $k(\sqrt[\ell]{\alpha})$ bezeichnet. Sei nun $\mathfrak{L}_i^{b_i}\mathfrak{A} = (\mathsf{A})$ Hauptideal, wobei $\mathfrak{A}$ prim zu f angenommen werden darf, so ist

$$\frac{(\varrho)}{\mathfrak{l}_i^{b_i}} = \frac{(\varrho)n(\mathfrak{A})}{n(\mathsf{A})}.$$

ϱ ist nach Konstruktion Normenrest mod $\mathfrak{a}_i$ und nach einer genügend hohen Potenz von $\mathfrak{l}_i$ (weil es β ist), also $\frac{\varrho}{n(\mathsf{A})}$ sicher Normenrest mod f, womit wieder alles bewiesen ist.

2.) Wir haben nun umgekehrt nachzuweisen, daß für $\left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right) \neq 1$ auch $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] \neq 1$ ist. Dazu genügt eine gruppentheoretische Überlegung. Die Normzahlen β von $k(\sqrt[\ell]{\alpha})$ nach $\mathfrak{l}_i$[1] bilden eine Untergruppe von $k(\mathfrak{l}_i)$ vom Index 1 oder ℓ, je nachdem α hyperprimär für $\mathfrak{l}_i$ oder nicht.

276 III

a.) α *hyperprimär für* $\mathfrak{l}_i$.

Dann ist jedes β Normzahl, also nach 1.) auch stets $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = 1$. Unsere Behauptung ist in diesem Falle gar nicht mehr zu beweisen, da sie inhaltslos.

b.) α *primär, aber nicht hyperprimär für* $\mathfrak{l}_i$.

Dann bilden die Normzahlen β eine Untergruppe vom Index ℓ von $k(\mathfrak{l}_i)$. Die β mit $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = 1$ bilden ebenfalls eine Gruppe, die als Untergruppe von $k(\mathfrak{l}_i)$ aufgefaßt werden kann, weil ja für hinreichend „nahe an 1 gelegenes β für den Bereich von $\mathfrak{l}_i$“ sicher $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = 1$ ist (Satz 44). Nach 1.) gehören die Normzahlen zu letzterer Untergruppe, sodaß demnach entweder diese mit $k(\mathfrak{l}_i)$ oder mit der Normzahluntergruppe identisch ist. Wir haben also nur die erstere Möglichkeit auszuschließen, also die Existenz *eines* β mit $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] \neq 1$ nachzuweisen, und zwar sowohl in diesem Falle b.) als auch im letzten Falle c.) (wie oben).

In unserem Falle b.) bestimmen wir dazu ϱ gemäß

$$\begin{aligned} \varrho &= \lambda_i \xi_i^{\ell}(\mathfrak{l}_i) \\ \varrho &= \xi_\kappa^{\ell}(\mathfrak{l}_\kappa); \qquad (\kappa \neq i) \\ \varrho &\equiv 1 \mod \mathfrak{a}_i \\ (\varrho) &= \mathfrak{r}\mathfrak{l}_i; \qquad (\mathfrak{r} \text{ Primideal}), \end{aligned}$$

wobei λ_i genau durch $\mathfrak{l}_i$ teilbar ist. Diese Bestimmung

277 III

ist ähnlich wie oben nach dem Satz von der arithmetischen Progression stets möglich. Es ist dann ϱ eine Zahl der obigen Klassengruppe H für $k(\sqrt[\ell]{\alpha_i})$, weil die Relativdiskriminante $f^{\ell-1}$ zu ℓ prim und also f Teiler von $\mathfrak{a}_i$ ist. $\mathfrak{l}_i$

[1] undeutlich

dagegen gehört sicher nicht zu H, da es ein nicht zerfallendes Primideal ist, also auch $\mathfrak{r}$ nicht, sodaß

$$\left(\frac{\alpha_i}{\mathfrak{r}}\right) \neq 1$$

ist. Andererseits ist $\left(\frac{\varrho}{\alpha_i}\right) = \left(\frac{\varrho}{\mathfrak{a}_i}\right) = 1$, also

$$\left[\frac{\varrho, \alpha}{\mathfrak{l}_i}\right] = \prod_{\mathfrak{p}} \left(\frac{\alpha_i, \varrho}{\mathfrak{p}}\right) = \left(\frac{\alpha_i}{\mathfrak{r}}\right)\left(\frac{\varrho}{\alpha_i}\right)^{-1} \neq 1\,, \qquad \text{w. z. b. w.}$$

c.) α *nicht primär für* $\mathfrak{l}_i$.

Wäre dann für alle β:

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right] = \prod_{\mathfrak{p}} \left(\frac{\alpha_i, \beta}{\mathfrak{p}}\right) = 1,$$

so wäre für alle zu ℓ primen β (prim zu α_i zu wählen!):

$$\left(\frac{\alpha_i}{\beta}\right)\left(\frac{\beta}{\mathfrak{a}_i}\right)^{-1} = 1, \quad \text{d. h.} \quad \left(\frac{\alpha_i}{\beta}\right) = \left(\frac{\beta}{\mathfrak{a}_i}\right),$$

speziell also für alle zu $\mathfrak{a}_i$ primen Primhauptideale $\beta = \pi$ Das ergibt aber einen Widerspruch, da man sicher ein solches Primhauptideal π finden kann, sodaß

$$\begin{aligned} &\pi \equiv 1 \mod \mathfrak{a}_i \\ &\pi = \text{Nichtnormzahl für } \mathfrak{l}_i \end{aligned}$$

ist, das also nicht zerfällt, und somit $\left(\frac{\alpha_i}{\pi}\right) \neq 1$, $\left(\frac{\pi}{\mathfrak{a}_i}\right) = 1$ macht[2]. Denn würden alle solchen π zerfallen, so würden alle Nichtnormzahlen für $\mathfrak{l}_i$ zu H gehören, H also einen zu $\mathfrak{l}_i$ primen Führer haben, während doch $\mathfrak{l}_i$ in f aufgeht.

278 III

Damit ist Satz 45 vollständig bewiesen. Wir können danach

$$\left[\frac{\beta, \alpha}{\mathfrak{l}_i}\right] = \left(\frac{\beta, \alpha}{\mathfrak{l}_i}\right)$$

[2]Wort nicht eindeutig lesbar

setzen und erhalten dadurch die schon oben erwähnte Normierung der Normenrestsymbole. Gleichzeitig folgt

$$\left[\frac{\alpha,\alpha}{\mathfrak{l}_i}\right] = \left(\frac{\alpha,\alpha}{\mathfrak{l}_i}\right) = 1, \quad \text{weil} \quad \alpha = n(\sqrt[\ell]{[\ldots]}$$

also die obige Bemerkung zum Beweis des Vertauschungssatzes. Natürlich gelten dann also Zerlegungs– und Vertauschungssatz für das Symbol $\left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right)$.

Wir können nunmehr leicht das Hilbertsche Reziprozitätsgesetz beweisen, als dessen Hauptinhalt eben die schon erhaltenen Resultate, insbesondere Satz 41, 45 anzusehen sind.

Satz 46 (Hilbertsches Reziprozitätsgesetz.)
Für beliebige α, β aus k ist

$$\prod_{\mathfrak{w}} \left(\frac{\alpha,\beta}{\mathfrak{w}}\right) = 1,$$

wo $\mathfrak{w}$ alle Primteiler von k durchläuft.

Beweis: Es ist

$$\prod_{\mathfrak{w}} \left(\frac{\alpha,\beta}{\mathfrak{w}}\right) = \prod_{\mathfrak{p}} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right) \cdot \prod_{i} \left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right).$$

Andererseits ist

$$\prod_{i} \left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right) = \prod_{i} \left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = \prod_{\mathfrak{p}} \prod_{i} \left(\frac{\alpha_i,\beta}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}} \left(\frac{\alpha_1 \ldots \alpha_z,\beta}{\mathfrak{p}}\right)$$
$$= \prod_{\mathfrak{p}} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right) \cdot \prod_{\mathfrak{p}} \left(\frac{\gamma,\beta}{\mathfrak{p}}\right),$$

wenn $\alpha_1 \ldots \alpha_z = \gamma\alpha$, (also γ hyperprimär) gesetzt wird. Also wird

$$\prod_{\mathfrak{w}} \left(\frac{\alpha,\beta}{\mathfrak{w}}\right) = \prod_{\mathfrak{p}} \left(\frac{\gamma,\beta}{\mathfrak{p}}\right)^{-1} \prod_{i} \left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right) \prod_{i} \left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right) = \prod_{\mathfrak{p}} \left(\frac{\beta,\gamma}{\mathfrak{p}}\right)$$

nach dem Vertauschungssatz. Es kommt also auf den Nachweis von

$$\prod_{\mathfrak{p}} \left(\frac{\beta,\gamma}{\mathfrak{p}}\right) = 1, \quad \text{für } \gamma \text{ hyperprimär, } \beta \text{ beliebig}$$

an. Sind β und γ für die zu ℓ primen $\mathfrak{p}$ kernprim, so ist dies nach Satz 41, 43 erfüllt. Es sei jetzt $\mathfrak{a}$ der größte gemeinsame Kernteiler von β, γ (also prim zu ℓ, da γ hyperprimär) und also

$$(\beta) = \mathfrak{a} \cdot \mathfrak{b} \cdot \prod \mathfrak{l}_i^{b_i} \cdot j_1^{\ell},$$
$$(\gamma) = \mathfrak{a} \cdot \mathfrak{c} \cdot \qquad j_2^{\ell}.$$

Wir betrachten dann $k(\sqrt[\ell]{\gamma})$, dessen Relativdiskriminante alle Primteiler von $\mathfrak{a}$ enthält, sodaß $\mathfrak{a} = n(\mathfrak{A})$ Relativnorm eines Ideals aus $k(\sqrt[\ell]{\gamma})$ ist. Ist dann $\mathfrak{B}$ ein solches zu γ primes Ideal aus $k(\sqrt[\ell]{\gamma})$, daß

$$\mathfrak{A}\mathfrak{B} = (\mathsf{A})$$

Hauptideal, so ist

$$\nu = n(\mathsf{A}) = \mathfrak{a} n(\mathfrak{B}) = \mathfrak{a}\mathfrak{b}_1$$

eine Normzahl von $k(\sqrt[\ell]{\gamma})$ und

$$\frac{\beta}{\nu} = \frac{\mathfrak{b}}{\mathfrak{b}_1} \prod \mathfrak{l}_i^{b_i} j_1^{\ell}$$

zu γ kernprim, also $\prod_{\mathfrak{p}} \left(\frac{\frac{\beta}{\nu}, \gamma}{\mathfrak{p}}\right) = 1$, ferner da ν Norm, $\left(\frac{\nu, \gamma}{\mathfrak{p}}\right) = 1$, also auch $\prod_{\mathfrak{p}} \left(\frac{\beta, \gamma}{\mathfrak{p}}\right) = 1$, w. z. b. w.

Satz 46 enthält alle Reziprozitätsbeziehungen in k für ℓ–te Potenzreste, die man bei geeigneten Spezialisierungen daraus ablesen kann. Es ergeben sich in der üblichen Trennung folgende Formeln:

Satz 47. Es gelten die Formeln:

Allgem. Rez. Ges.:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_i \left(\frac{\beta, \alpha}{\mathfrak{l}_i}\right), \quad \left\{ \begin{array}{c} \text{wenn } \alpha, \beta \text{ zueinander} \\ \text{und zu } \ell \text{ kernprim.} \end{array} \right.$$

Erster Erg. Satz:

$$\left(\frac{\varepsilon}{\alpha}\right) = \prod_i \left(\frac{\alpha, \varepsilon}{\mathfrak{l}_i}\right), \quad \left\{ \begin{array}{c} \text{wenn } \varepsilon = \mathfrak{a}^{\ell}, \\ \alpha \text{ kernprim zu } \ell. \end{array} \right.$$

Zweiter Erg. Satz:

$$\left(\frac{\lambda}{\alpha}\right) = \prod_i \left(\frac{\alpha, \lambda}{\mathfrak{l}_i}\right), \quad \left\{ \begin{array}{c} \text{wenn } \lambda = \prod \mathfrak{l}_i^{a_i} \mathfrak{a}^{\ell}, \\ \alpha \text{ kernprim zu } \ell. \end{array} \right.$$

Wir haben nunmehr auch den Beweis zu der mehr *inhaltlichen* Formulierung des Reziprozitätsgesetzes, wie sie in Satz 2 formuliert wurde in der Hand, die gegenüber der bisherigen *formalen* Formulierung von Satz 46/47 für die Anwendungen vorzuziehen ist.

Es sei μ eine beliebige Zahl aus k, die nicht ℓ–te Potenz einer Zahl aus k ist mit der Kernzerlegung

$$(\mu) = \mathfrak{m} \prod \mathfrak{l}_i^{m_i} j^{\ell}; \qquad (\mathfrak{m} \text{ prim zu } \ell)$$

und $k(\sqrt[\ell]{\mu})$ Klassenkörper für die Klassengruppe H vom Index ℓ in k, deren Führer f ein Teiler von $\mathfrak{m}\ell\mathfrak{l}_0\mathfrak{l}_1 \dots \mathfrak{l}_z$ ist. Ferner sei $\mathfrak{a}$ ein beliebiges zu f und ℓ primes Ideal aus k, dessen Darstellung durch ein festes Repräsentantensystem $[i]$ der t absoluten Basisklassen

$$\mathfrak{a} = (\alpha) i_1^{a_1} \dots i_t^{a_t} j^{\ell}$$

sei.

281 III

Die i_k seien prim zu ℓ und f, sodaß auch der Kern von α es ist. Dann betrachten wir das Symbol $\left(\frac{\mu}{\mathfrak{a}}\right)$ in seiner Abhängigkeit von $\mathfrak{a}$. Es ist:

$$\left(\frac{\mu}{\mathfrak{a}}\right) = \left(\frac{\mu}{i_1}\right)^{a_1} \cdots \left(\frac{\mu}{i_t}\right)^{a_t} \left(\frac{\mu}{\alpha}\right) = \left(\frac{\mu}{i_1}\right)^{a_1} \cdots \left(\frac{\mu}{i_t}\right)^{a_t} \left(\frac{\alpha}{\mathfrak{m}}\right) \left(\frac{\mu, \alpha}{\mathfrak{l}_1}\right) \cdots \left(\frac{\mu, \alpha}{\mathfrak{l}_z}\right).$$

Daraus folgt speziell für ein zur Hauptklasse nach dem Strahl $\equiv 1 \mod f$ gehöriges $\mathfrak{a} = (\alpha)$; $(\alpha \equiv 1 \mod f)$

$$\left(\frac{\mu}{\mathfrak{a}}\right) = \left(\frac{\mu}{\alpha}\right) = \left(\frac{\alpha}{\mathfrak{m}}\right) \left(\frac{\mu, \alpha}{\mathfrak{l}_1}\right) \cdots \left(\frac{\mu, \alpha}{\mathfrak{l}_z}\right).$$

Da aber in $\mathfrak{m}$ nur Primteiler von f aufgehen, ist $\left(\frac{\alpha}{\mathfrak{m}}\right) = 1$, und da weiter speziell $\alpha \equiv 1 \mod \mathfrak{l}_i^{v_i+1}$ für $i = 1, \dots, z$ ist, ist α Normzahl für jedes $\mathfrak{l}_i$, also $\left(\frac{\mu, \alpha}{\mathfrak{l}_i}\right) = 1$. Daher folgt:

$$\left(\frac{\mu}{\mathfrak{a}}\right) = 1\,, \quad \text{wenn} \quad \mathfrak{a} \sim 1 \mod f.$$

$\left(\frac{\mu}{\mathfrak{a}}\right)$ hat demnach je für eine ganze Klasse $\mathfrak{a} \mod f$ den gleichen Wert, und hängt somit nur von der Strahlklasse $\mathfrak{a} \mod f$ ab. Die Gesamtheit der

Strahlklassen mod f mit $\left(\frac{\mu}{\mathfrak{a}}\right) = 1$ bildet dann eine Klassengruppe H'; H' muß H enthalten, da für $\mathfrak{p}|\mathsf{H}$ sicher $\left(\frac{\mu}{\mathfrak{p}}\right) = 1$, und alle Klassen durch Primideale $\mathfrak{p}$ charakterisiert werden können. Da es zu H' genau ℓ Nebengruppen gibt, den ℓ Symbolwerten $1, \zeta, \zeta^2, \dots \zeta^{\ell-1}$ entsprechend, (die alle auftreten müssen, weil $\mathfrak{p}$ mit $\left(\frac{\mu}{\mathfrak{p}}\right) \neq 1$ existieren, und dann $\mathfrak{p}, \mathfrak{p}^2, \dots \mathfrak{p}^\ell$ alle ζ–Potenzen ergeben), hat H' denselben Index ℓ wie H, ist also mit H identisch.

282 III

Daher hängt $\left(\frac{\mu}{\mathfrak{a}}\right)$ in Wahrheit nur von der Klasse nach H ab, der $\mathfrak{a}$ angehört, und hat nun auch für verschiedene solche Klassen verschiedene Werte. $\left(\frac{\mu}{\mathfrak{a}}\right)$ ist daher einer der $\ell - 1$ Nichthauptcharaktere $\chi(\mathfrak{a})$ nach H, und H kann durch $\chi(\mathfrak{a}) = \left(\frac{\mu}{\mathfrak{a}}\right) = 1$ charakterisiert werden. Somit ist in der a. S. 281 ▸ oben angegebenen Form auch der Charakter $\chi(\mathfrak{a})$ bestimmt, durch den H definiert werden kann, was in Satz 4 (S. 202 ▸) nur der allgemeinen Form nach, mit Einschränkung durch gewisse Bedingungskongruenzen für die unbestimmten Exponenten geschehen konnte.

Satz 48. Ist μ eine beliebige Zahl $\neq \xi^\ell$ aus k, und $k(\sqrt[\ell]{\mu})$ Klassenkörper für die Klassengruppe H vom Führer f, so ist das Symbol $\left(\frac{\mu}{\mathfrak{a}}\right)$, für zu f und ℓ kernprimes $\mathfrak{a}$ nur von der Strahlklasse nach H abhängig, der $\mathfrak{a}$ angehört, d. h. Gruppencharakter $\chi(\mathfrak{a})$ nach H.

In diesem Zusammenhang, der den Ausgangspunkt (Satz 1, 2[3]) unserer Betrachtungen nunmehr zum Abschluß gebracht hat, soll auch die *Artin*sche Formulierung des Reziprozitätsgesetzes besprochen werden, da diese im Gegensatz zu den bisherigen Formulierungen einer Verallgemeinerung auf *beliebige* Abelsche Körper an Stelle von $k(\sqrt[\ell]{\mu})$ fähig ist.

Artin geht aus von einem beliebigen, relativ–Abelschen Körper K über k, wobei nicht notwendig die ℓ–te Einheitswurzel ζ in k vorzukommen braucht. Sei $\mathfrak{p}$ ein

283 III

zur Relativdiskriminante von K primes Primideal aus k und σ eine Substitution der Zerlegungsgruppe $\mathfrak{G}_z$ von $\mathfrak{p}$ von K nach k. Es sei f_0 der Grad von $\mathfrak{p}$ und f der Grad der Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in K nach k. Die primen Restklassen mod $\mathfrak{P}$ werden durch die Potenzen einer primitiven $(p^{ff_0} - 1)$–ten Einheitswurzel Ω erzeugt, deren relativ–konjugierte sind:

$$\Omega, \Omega^{p^{f_0}}, \Omega^{p^{2f_0}}, \dots, \Omega^{p^{(f-1)f_0}}.$$

[3] Ziffer nicht vollständig lesbar

Jedem σ entspricht also eine bestimmte Zahl $\nu(\sigma)$, sodaß

$$\sigma\Omega = \Omega^{p^{\nu f_0}}(\mathfrak{P}),$$

also für jedes zu $\mathfrak{P}$ prime A aus K:

$$\sigma\mathsf{A} \equiv \mathsf{A}^{p^{\nu f_0}} \mod \mathfrak{P}$$

gilt. Denn ist

$$\mathsf{A} \equiv \Omega^b \mod \mathfrak{P},$$

so ist

$$\sigma\mathsf{A} \equiv \sigma\Omega^b \equiv \Omega^{p^{\nu f_0} \cdot b} \equiv \mathsf{A}^{p^{\nu f_0}} \mod \mathfrak{P}.$$

Speziell gibt es eine Substitution σ, sodaß $\nu(\sigma) = 1$, also

$$\sigma\Omega = \Omega^{p^{f_0}}(\mathfrak{P})$$

und somit

$$\sigma\mathsf{A} \equiv \mathsf{A}^{p^{f_0}} \equiv \mathsf{A}^{N\mathfrak{p}} \mod \mathfrak{P}$$

für jedes zu $\mathfrak{P}$ prime A aus K gilt, und σ ist bis auf eine Substitution der Trägheitsgruppe $\mathfrak{G}_T$ bestimmt. Da aber $\mathfrak{G}_T = 1$ ist, weil $\mathfrak{p}$ nicht in der Relativdiskriminante aufgeht, ist σ *eindeutig* durch $\mathfrak{p}$ bestimmt, und (eine in gewisser Weise normierte erzeugende Substitution

der zyklischen Zerlegungsgruppe $\mathfrak{G}_Z$[4] vom Grade f.

Die Artinsche Formulierung des Reziprozitätsgesetzes lautet dann:

Satz 49. Ist K relativ Abelsch zu k, $\mathfrak{p}$ ein zur Relativdiskriminante von K primes Primideal aus k und σ diejenige, eindeutig bestimmte, erzeugende Substitution der Zerlegungsgruppe für $\mathfrak{p}$ in K, für die

$$\sigma\mathsf{A} \equiv \mathsf{A}^{N\mathfrak{p}} \mod \mathfrak{P}$$

[4]Subskript nicht eindeutig lesbar

für alle primen Restklassen A nach jedem Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in K ist, ist ferner K Klassenkörper für die Klassengruppe H in k, so hängt σ nur von[5] der Klasse nach H ab, der $\mathfrak{p}$ angehört. Ist G die Gruppe der Klassen nach H, so entspricht also jeder Klasse von G eindeutig ein σ. Umgekehrt entspricht aber auch jedem σ eindeutig eine Klasse von G. Diese Zuordnung ist *isomorph*. Es wird also durch diese Formulierung des Reziprozitätsgesetzes der *Isomorphismus* zwischen G und der Galoisschen Gruppe $\mathfrak{G}$ von K nach k *dargestellt*.

Daß σ nur von $\mathfrak{p}$, nicht von den $\mathfrak{P}$ abhängt, ist leicht zu sehen. Denn ist

$$\sigma\mathsf{A} \equiv \mathsf{A}^{N\mathfrak{p}} \mod \mathfrak{P}$$

so folgt

$$\tau(\sigma\mathsf{A}) \equiv (\tau\mathsf{A})^{N\mathfrak{p}} \mod \tau\mathfrak{P}.$$

Da aber K, also $\mathfrak{G}$ Abelsch, ist $\tau\sigma = \sigma\tau$, und somit

$$\tau(\sigma\mathsf{A}) = \sigma(\tau\mathsf{A}) \equiv (\tau\mathsf{A})^{N\mathfrak{p}} \mod \tau\mathfrak{P},$$

285 III

und $\tau\mathsf{A}$ durchläuft mit A alle zu $\mathfrak{P}$ bezw. $\tau\mathfrak{P}$ primen Restklassen.

Für den Fall, daß $K = k(\sqrt[\ell]{\mu})$ ist, werden wir sogleich die Identität von Satz 49 mit Satz 48 nachweisen. Für den Fall, daß K relativ–zyklisch vom Primzahlgrad ℓ ist, ohne daß ζ in k vorkommt, sowie für alle aus solchen Körpern komponierten Körper hat Artin den Satz 49 ebenfalls bewiesen, indem er ähnlich verfährt, wie beim Existenzbeweis des Klassenkörpers. Der Beweis für relativ–zyklische Körper von Primzahlpotenzgrad, und somit für beliebige relativ–Abelsche Körper steht jedoch noch aus.

Beweis von Satz 49 für $K = k(\sqrt[\ell]{\mu})$.

Wir setzen $\mathsf{A} = \sqrt[\ell]{\mu}$. Dann wird

$$\sigma\mathsf{A} = \zeta^c \sqrt[\ell]{\mu}\,; \qquad (c \not\equiv 0 \mod \ell).$$

[5] undeutlich

Der Exponent c bestimmt sich aus der Forderung

$$\sigma \mathsf{A} \equiv \mathsf{A}^{N\mathfrak{p}} \mod \mathfrak{P}.$$

Nun ist hier

$$\mathsf{A}^{N\mathfrak{p}} = \sqrt[\ell]{\mu}^{N\mathfrak{p}-1} \sqrt[\ell]{\mu} = \mu^{\frac{N\mathfrak{p}-1}{\ell}} \sqrt[\ell]{\mu},$$

also wenn μ prim zu $\mathfrak{p}$ angenommen wird, was zulässig,

$$\mathsf{A}^{N\mathfrak{p}} \equiv \left(\frac{\mu}{\mathfrak{p}}\right) \sqrt[\ell]{\mu} \mod \mathfrak{p}$$

Es ist also hier

$$\sigma = \left(\sqrt[\ell]{\mu} : \left(\frac{\mu}{\mathfrak{p}}\right) \sqrt[\ell]{\mu}\right)$$

und dies $\sigma = \sigma(\mathfrak{p})$ hängt nach Satz 48 tatsächlich nur von der Klasse nach H ab, der $\mathfrak{p}$ angehört.

Ferner wird durch diese Zuordnung der Substitutionen σ der zyklischen Galoisschen Gruppe vom Grade ℓ zu den Klassen nach H wirklich der Isomorphismus vermittelt.

Ist nämlich $\mathfrak{p}$ irgendein nicht zu H gehöriges Primideal, dann ist $\sigma(\mathfrak{p}) \neq 1$, da $\left(\frac{\mu}{\mathfrak{p}}\right) \neq 1$. Wir können dann die Klassen nach H durch $\mathfrak{p}, \mathfrak{p}^2, \ldots \mathfrak{p}^\ell$ erzeugen. Sei $\mathfrak{q} \sim \mathfrak{p}^c$
Dann ist

$$\begin{aligned}\sigma(\mathfrak{q}) &= \left(\sqrt[\ell]{\mu} : \left(\frac{\mu}{\mathfrak{q}}\right) \sqrt[\ell]{\mu}\right) = \left(\sqrt[\ell]{\mu} : \left(\frac{\mu}{\mathfrak{p}^c}\right) \sqrt[\ell]{\mu}\right) = \left(\sqrt[\ell]{\mu} : \left(\frac{\mu}{\mathfrak{p}}\right)^c \sqrt[\ell]{\mu}\right) \\ &= \big(\sigma(\mathfrak{p})\big)^c,\end{aligned}$$

woraus der Isomorphismus folgt.

3.8 §8 Das quadratische Reziprozitätsgesetz.

287 III

Wir haben jetzt noch den seit §5 (S. 232) ausgeschlossenen Fall $\ell = 2$ zu erledigen.

Wir beweisen zuerst in Analogie zu Satz 27:

Satz 50. Sind $\omega_1, \ldots, \omega_t$ die t total positiven singulären Primärzahlen und $[i] = (i_1, i_2, \ldots, i_t)$ ein solches System von t zu 2 primen Primidealen, daß

$$\left(\frac{\omega_\kappa}{i_\kappa}\right) \neq 1; \qquad \left(\frac{\omega_\kappa}{i_r}\right) = 1; \qquad (r \neq \kappa)$$

ist, so repräsentieren die i_κ die t unabhängigen Basisklassen von k in absolutem Sinne, d. h. es gilt für jedes Ideal $\mathfrak{a}$ aus k eine eindeutige Darstellung

$$\mathfrak{a} = i_1^{c_1} \ldots i_t^{c_t}(\alpha)j^2; \qquad (c_\kappa = 0, 1)$$

kurz

$$\mathfrak{a} = (\alpha)[i].$$

Wenn außerdem noch weitere t' zu 2 prime Primideale i'_κ gewählt werden, sodaß für die t' nicht total positiven singulären Primärzahlen $\omega'_1, \ldots \omega'_{t'}$ gilt:

$$\left(\frac{\omega'_\kappa}{i'_\kappa}\right) \neq 1; \qquad \left(\frac{\omega'_\kappa}{i'_r}\right) = 1; \qquad \left(\frac{\omega^{[\ldots]}}{i'_r}\right) = 1; \qquad (r \neq \kappa)$$

so repräsentieren die i_κ, i'_κ die $t + t'$ unabhängigen Basisklassen in engerem Sinne, d. h. es gilt für jedes Ideal $\mathfrak{a}$ aus k eine eindeutige Darstellung:

$$\mathfrak{a} = i_1^{c_1} \ldots i_t^{c_t} i'^{c'_1}_1 \cdots i'^{c'_{t'}}_{t'}(\alpha)j^2 = (\alpha)[i, i'],$$
$$\text{wo} \quad c_\kappa, c'_\kappa = 0, 1 \quad \text{und} \quad \alpha \quad \text{total positiv.}$$

288 III

Beweis: Natürlich können wegen der Unabhängigkeit der ω, ω' stets unendlich viele Systeme von solchen Primidealen i_κ, i'_κ gefunden werden. Es ist wieder nur zu zeigen, daß die i_κ in Bezug auf die Gruppe $(\alpha)j^2$, die i_κ, i'_κ in Bezug auf die Gruppe $(\alpha)j^2$ mit total positivem α unabhängig sind.

1.) Der Rang der Klassengruppe mod $\mathfrak{l}_0^2$ mit Vorzeichenbedingung ist $t + r + 1$, der Rang der Klassengruppe mit Vorzeichenbedingung mod $\mathfrak{l}_0^2 i_1 \dots i_t$ ebensogroß, weil zwar die Anzahl der zu 2 primen Teiler des Moduls um t erhöht, dafür aber die Anzahl der unabhängigen total positiven quadratischen Reste unter den Idealquadraten von t auf 0 erniedrigt ist, nach Wahl der i_κ.

Wäre nun

$$(\alpha) = i_1^{c_1} \dots i_t^{c_t} j^2 ; \qquad (c_\kappa = 0, 1),$$

so ist $k(\sqrt[\ell]{\alpha})$ Klassenkörper für eine Klassengruppe H vom Führer f mit Vorzeichenbedingung. Da α nicht durch die $\mathfrak{l}_i$ teilbar ist, müßte f Teiler von $\mathfrak{l}_0^2 i_1 \dots i_t$, also H schon Klassengruppe mit Vorzeichenbedingung mod $\mathfrak{l}_0^2$ sein. Das erfordert aber, daß alle $c_\kappa = 0$ sind.

2.) Der Rang der Klassengruppe mod $\mathfrak{l}_0^2$ ohne Vorzeichenbedingung ist $t+n_0$ (S. 231▸), der Rang mod $\mathfrak{l}_0^2 i_1 \dots i_t\, i'_1 \dots i'_{t'}$ ebensogroß, da zwar $t+t'$ neue Primteiler zum Modul hinzukommen, dafür aber die Anzahl der unabhängigen quadratischen Reste unter den Idealquadraten von $t + t'$ auf 0 erniedrigt wird. Soll nämlich ein Idealquadrat quadratischer Rest mod $\mathfrak{l}_0^2 i_1 \dots i_t\, i'_1 \dots i'_{t'}$ sein, so zunächst mod $\mathfrak{l}_0^2$, also von der

Form $\omega_1^{a_1} \dots \omega_t^{a_t}\, \omega'^{a'_1}_1 \dots \omega'^{a'_{t'}}_{t'} \xi^2$. Soll dies ferner quadratischer Rest nach den i'_κ sein, so müssen alle Exponenten a'_κ Null sein, und soll dann $\omega_1^{a_1} \dots \omega_t^{a_t} \xi^2$ Rest nach den i_κ sein, so auch alle a_κ, beidesmal nach Wahl der i_κ, i'_κ.

Wäre nun

$$(\alpha) = i_1^{c_1} \dots i_t^{c_t}\, i'^{c'_1}_1 \dots i'^{c'_t}_t j^2 ; \qquad (\alpha \text{ total positiv}) \qquad (c_\kappa, c'_\kappa = 0, 1),$$

so ist $k(\sqrt[\ell]{\alpha})$ Klassenkörper für eine Klassengruppe H vom Führer f ohne Vorzeichenbedingung; da α nicht durch die $\mathfrak{l}_i$ teilbar, muß f ein Teiler von $\mathfrak{l}_0^2 i_1 \dots i_t\, i'_1 \dots i'_{t'}$ sein, also H schon mod $\mathfrak{l}_0^2$ erklärbar, und das erfordert, daß alle $c_\kappa, c'_\kappa = 0$ sind.

Wir beweisen ferner analog zu Satz 28:

Satz 51. Ist μ keine total positive singuläre Primärzahl, so darf $[i]$ gegen μ normiert angenommen werden, ist μ überhaupt keine singuläre Primärzahl, so darf $[i, i']$ gegen μ normiert angenommen werden.

Beweis: μ ist im ersten Falle von den $[\omega]$ im zweiten von den $[\omega, \omega']$ unabhängig, sodaß den Forderungen für $[i]$ bezw. $[i, i']$ noch die Forderungen

$$\left(\frac{\mu}{i_\kappa}\right) = 1 \quad \text{bezw.} \quad \left(\frac{\mu}{i_\kappa}\right) = 1, \ \left(\frac{\mu}{i'_\kappa}\right) = 1$$

an die Seite gestellt und erfüllt werden können.

Schließlich haben wir noch analog zu Satz 29:

Satz 52. Ist $[i]$ ein vorgegebenes Repräsentantensystem wie in Satz 50, μ kernprim zu $[i]$, so kann μ durch Multiplikation mit total positiven singulären Primärzahlen gegen $[i]$ normiert werden. Ist μ überdies kernprim zu $[i']$, so darf μ durch Multiplikation mit irgendwelchen singulären Primärzahlen gegen $[i, i']$ normiert werden.

Insbesondere darf also die Primärzahl eines primären Primideals $\mathfrak{p}$ gegen $[i]$ bezw. $[i, i']$ normiert werden, wenn $\mathfrak{p}$ von den $[i]$ bezw. $[i, i']$ verschieden ist. (Siehe Satz 16–19, S. 220 ff.).

Beweis: 1.) Sei $\left(\frac{\mu}{i_\kappa}\right) = (-1)^{c_\kappa}$; $(c_\kappa = 0, 1)$.
Dann ist

$$\left(\frac{\mu\omega_1^{c_1} \dots \omega_t^{c_t}}{i_\kappa}\right) = \left(\frac{\mu}{i_\kappa}\right)\left(\frac{\omega_\kappa}{i_\kappa}\right)^{c_\kappa} = (-1)^{c_\kappa}(-1)^{c_\kappa} = 1$$

2.) Sei $\left(\frac{\mu}{i_\kappa}\right) = (-1)^{c_\kappa}$; $\left(\frac{\mu}{i'_\kappa}\right) = (-1)^{c'_\kappa}$; $(c_\kappa, c'_\kappa = 0, 1)$.
Dann ist zunächst

$$\left(\frac{\overline{\mu}}{i'_\kappa}\right) = \left(\frac{\mu\omega'^{c'_1}_1 \dots \omega'^{c'_{t'}}_{t'}}{i'_\kappa}\right) = \left(\frac{\mu}{i'_\kappa}\right)\left(\frac{\omega'_\kappa}{i'_\kappa}\right)^{c_\kappa} = 1.$$

Sei dann ferner

$$\left(\frac{\overline{\mu}}{i_\kappa}\right) = (-1)^{\bar{c}_\kappa},$$

so wird

$$\left(\frac{\overline{\mu}\omega_1^{\bar{c}_1} \dots \omega_t^{\bar{c}_t}}{i_\kappa}\right) = 1, \quad \text{wie oben,}$$

aber auch

$$\left(\frac{\overline{\mu}\omega_1^{\bar{c}_1} \dots \omega_t^{\bar{c}_t}}{i'_\kappa}\right) = 1,$$

weil

$$\left(\frac{\omega_r}{i'_\kappa}\right) = 1$$

ist.

291 III

Wir gehen nach diesen vorbereitenden Sätzen, von denen wir übrigens die auf $[i']$ bezüglichen Teile nicht brauchen* und nur der Vollständigkeit halber mitgeführt haben, an den Beweis des allgemeinen quadratischen Reziprozitätsgesetzes. Dieser gestaltet sich viel einfacher, als für ungerades ℓ, da hier die Schwierigkeit der Unterscheidung der Nichtreste ganz fortfällt.

Wir können von vorneherein auf den zu Satz 35 analogen Satz, also das Reziprozitätsgesetz zwischen einer primären und einer beliebigen zu λ primen Zahl lossteuern. Die Formulierung erfordert jedoch Vorzeichenbedingungen, die wir zweckmäßig sofort durch Einführung des Normenrestsymbols für die $\mathfrak{p}_\infty^{(i)}$ darstellen. Wir setzen

$$\left(\frac{\mu, \nu}{\mathfrak{p}_\infty^{(i)}}\right) = \operatorname{sgn}\mu^{(i)} \operatorname{sgn}\nu^{(i)},$$

wenn $\mathfrak{p}_\infty^{(i)}$ die den reellen konjugierten $k^{(i)}$ entsprechenden Primstellen und $\mu^{(i)}, \nu^{(i)}$ die Werte in $k^{(i)}$ (die reellen konjugierten) bezeichnen. Es ist offenbar dann und nur dann $\left(\frac{\mu,\nu}{\mathfrak{p}_\infty^{(i)}}\right) = 1$, wenn ν Normzahl von $k(\sqrt{\mu})$ für $\mathfrak{p}_\infty^{(i)}$ ist. Denn ist $\mu^{(i)}$ positiv, so ist jedes Element ν von k Normzahl für $k^{(i)}$, weil

$$\nu = (-1)^b \xi^2 \,(\mathfrak{p}_\infty^{(i)})$$

und

$$-1 = n\left(\frac{\sqrt{\mu}}{|\sqrt{\mu}|}\right) \mathfrak{p}_\infty^{(i)} \qquad \text{ist.}$$

Ist aber $\mu^{(i)}$ negativ, so sind nur die in $k^{(i)}$ positiven ν Normzahlen, diese aber als Quadrate in $k^{(i)}(\mathfrak{p}_\infty^{(i)})$ sämtlich.

292 III

Mit diesem Normenrestsymbol lautet nun unser zu beweisendes Reziprozitätsgesetz:

*siehe jedoch Beweis zu Satz 54! Hier wird $[i']$ doch gebraucht.

Satz 53. Sind ν, μ kernprim zu 2 und zueinander und μ primär, so ist

$$\left(\frac{\mu}{\nu}\right)\left(\frac{\nu}{\mu}\right) = \prod_i \left(\frac{\mu, \nu}{\mathfrak{p}_\infty^{(i)}}\right).$$

Beweis: Sei $(\mu) = \mathfrak{p}_1 \dots \mathfrak{p}_r j^2$ die Kernzerlegung von μ, ferner μ vorläufig nicht total positive singuläre Primärzahl und $[i]$ ein Repräsentantensystem im Sinne von Satz 50, das dann nach Satz 51 gegen μ normiert angenommen werden darf. Ferner sei $\mathfrak{r}$ ein Kernprimteiler von ν, also prim zu 2 und den $\mathfrak{p}_i$, und

$$\mathfrak{r} = (\varrho)[i].$$

Wir betrachten $k(\sqrt{\mu})$. Da μ primär ist die Relativdiskriminante

$$f = \mathfrak{p}_1 \dots \mathfrak{p}_r.$$

1.) *μ total positiv.*

Dann ist die $k(\sqrt{\mu})$ zugeordnete Klassengruppe H mod f ohne Vorzeichenbedingungen erklärbar. Wegen der Normiertheit von μ gegen $[i]$ ist H durch eine Charaktergleichung

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{p}_1}\right)^{v_1} \cdots \left(\frac{\alpha}{\mathfrak{p}_r}\right)^{v_r} = 1 \quad \text{für} \quad \mathfrak{a} = (\alpha)[i]$$

definiert. Hierin kann kein v_i verschwinden, da sonst $\mathfrak{p}_i$ nicht im Führer f aufginge. Es ist also

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{p}_1}\right) \cdots \left(\frac{\alpha}{\mathfrak{p}_r}\right) = \left(\frac{\alpha}{\mu}\right)$$

und folglich

$$\chi(\mathfrak{r}) = \left(\frac{\varrho}{\mu}\right).$$

Dann und nur dann, wenn

$$\left(\frac{\mu}{\mathfrak{r}}\right) = \left(\frac{\mu}{\varrho}\right) = 1,$$

ist $\mathfrak{r}$ in H, also

$$\chi(\mathfrak{r}) = \left(\frac{\varrho}{\mu}\right) = 1.$$

Da $\left(\frac{\mu}{\mathfrak{r}}\right)$ nur ± 1 sein kann, folgt also

$$\left(\frac{\mu}{\varrho}\right) = \left(\frac{\varrho}{\mu}\right).$$

Ist dann

$$(\nu) = \mathfrak{r}_1 \dots \mathfrak{r}_s j^2\,; \qquad \mathfrak{r}_i = (\varrho_i)[i];$$

so ist

$$\nu = \varrho_1 \dots \varrho_s[\eta, \omega, \omega'] \qquad \text{(s. S. 209}\blacktriangleright\text{)},$$

weil der entstehende Ausdruck $[i]$ Hauptideal, also Idealquadrat, also in der Form $[\eta, \omega, \omega']$ enthalten sein muß. (s. a. S. 242$\blacktriangleright$). Daher folgt:

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\mu}{\varrho_1}\right) \cdots \left(\frac{\mu}{\varrho_s}\right) = \left(\frac{\varrho_1}{\mu}\right) \cdots \left(\frac{\varrho_s}{\mu}\right) = \left(\frac{\nu}{\mu}\right),$$

weil ja $\left(\frac{[\eta,\omega,\omega']}{\mu}\right) = 1$ ist, da $\chi([\eta, \omega, \omega']) = 1$.

Damit ist der Satz für total positives, nicht singulär primäres μ bewiesen. Ist μ total positiv und singulär primär, so sei μ_0 eine total positive, nicht singuläre, primäre Zahl. Dann gilt der Satz für μ_0[1], $\mu\mu_0$ also auch für μ.

2.) *μ primär aber nur in $k^{(1)}$ negativ.*

$k(\sqrt{\mu})$ ist dann Klassenkörper für eine Klassengruppe H, deren Führer $f = \mathfrak{p}_1 \dots \mathfrak{p}_r$ ist, und zu deren Definition außerdem noch eine Vorzeichenbedingung, nämlich die Forderung „positiv in $k^{(1)}$“ notwendig ist. Ohne Vorzeichenbedingung ist H nicht erklärbar, denn sonst würde

[1] Subskript nicht eindeutig lesbar

nach früheren Sätzen der H zugeordnete Klassenkörper $k(\sqrt{\mu})$ durch ein total positives μ erzeugt. Der H definierende Charakter muß dann (s. Satz 4) entsprechend dem vorhin Bewiesenen

$$\chi(\mathfrak{a}) = \left(\frac{\alpha}{\mu}\right)\operatorname{sgn}\alpha^{(1)} \quad \text{für} \quad \mathfrak{a} = (\alpha)[i]$$

sein, also folgt wie vorhin:

$$\left(\frac{\mu}{\varrho}\right) = \left(\frac{\varrho}{\mu}\right)\left(\frac{\mu,\varrho}{\mathfrak{p}_\infty^{(1)}}\right) = \left(\frac{\varrho}{\mu}\right)\prod_i\left(\frac{\mu,\varrho}{\mathfrak{p}_\infty^{(i)}}\right),$$

denn es ist ja

$$\left(\frac{\mu,\varrho}{\mathfrak{p}_\infty^{(1)}}\right) = \operatorname{sgn}\varrho^{(1)}, \quad \left(\frac{\mu,\varrho}{\mathfrak{p}_\infty^{(2)}}\right) = \cdots = 1.$$

Diese Formel umfaßt natürlich den vorigen Fall.

Ist ferner, wie oben

$$\nu = \varrho_1 \ldots \varrho_s[\eta,\omega,\omega'].$$

Dann folgt:

$$\begin{aligned}\left(\frac{\mu}{\nu}\right) = \left(\frac{\mu}{\varrho_1}\right)\cdots\left(\frac{\mu}{\varrho_s}\right) &= \left(\frac{\varrho_1\ldots\varrho_s}{\mu}\right)\operatorname{sgn.}(\varrho_1^{(1)}\ldots\varrho_s^{(1)}) \\ &= \left(\frac{\nu}{\mu}\right)\operatorname{sg}\nu^{(1)} = \left(\frac{\nu}{\mu}\right)\prod_i\left(\frac{\mu,\nu}{\mathfrak{p}_\infty^{(i)}}\right),\end{aligned}$$

weil

$$\left(\frac{[\eta,\omega,\omega']}{\mu}\right)\operatorname{sgn.}[\eta,\omega,\omega'] = \chi([\eta,\omega,\omega']) = 1 \quad \text{sein muß.}$$

3.) *μ beliebige primäre Zahl.*

Sei μ in r_0 Körpern $k^{(i)}$ negativ. Dann seien $\mu_1,\ldots,\mu_{r_0}$ zu ν kernprime, primäre Zahlen, die ja nur in einem jener r_0 Körper negativ sind, sodaß $\mu\mu_1\ldots\mu_{r_0}$ eine total positive, primäre, zu ν kernprime Zahl ist, für die also

$$\left(\frac{\mu\mu_1\ldots\mu_{r_0}}{\nu}\right) = \left(\frac{\nu}{\mu\mu_1\ldots\mu_{r_0}}\right)$$

nach 1.) ist. Ferner ist

295 III

$$\left(\frac{\mu_i}{\nu}\right) = \left(\frac{\nu}{\mu_i}\right)\operatorname{sgn}.\,\nu^{(i)} = \left(\frac{\nu}{\mu_i}\right)\left(\frac{\mu,\nu}{\mathfrak{p}_\infty^{(i)}}\right),$$

weil $\mu^{(i)}$ negativ. Also folgt

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right)\prod_i \left(\frac{\mu,\nu}{\mathfrak{p}_\infty^{(i)}}\right),$$

wo das Produkt natürlich über alle $k^{(i)}$ erstreckt werden darf, da ja μ in den restlichen $r_1 - r_0$ Körpern positiv ist.

Damit ist Satz 53 bewiesen. In Analogie zu Satz 41 beweisen wir nunmehr:

Satz 54. Ist $\beta = \prod_{i=1}^{z} \mathfrak{l}_i^{a_i} \cdot \mathfrak{b} \cdot j^2$; $(a_i = 0, 1)$, wo der Kern $\mathfrak{b}$ prim zu 2 ist, und α eine total–positive, zu β kernprime, primäre Zahl, die überdies für die $\mathfrak{l}_i$ mit $a_i \neq 0$ hyperprimär ist, so gilt:

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right).$$

Dasselbe gilt auch, wenn α beliebige Signatur hat, dafür aber β total positiv ist†

Beweis: 1.) Ist α total positiv, so ist die $k(\sqrt{\alpha})$ zugeordnete Klassengruppe ohne Vorzeichenbedingungen erklärbar, und der Beweis verläuft ganz analog wie der von Satz 41.

2.) Ist β total positiv, so ist eine kleine Modifikation dieses Beweises nötig. Wir verwenden hier am zweckmäßigsten ein gegen α normiertes Repräsentantensystem $[i, i']$ im Sinne von Satz 50, 51, setzen also vorläufig voraus, daß α nicht singulär primär ist. Wegen der Normiertheit von α ist dann die $k(\sqrt{\alpha})$ zugeordnete Klassengruppe durch

296 III

$$\chi(\mathfrak{c}) = \left(\frac{\gamma}{\alpha}\right)(\operatorname{sgn}\gamma^{(1)})^{b_1} \cdots (\operatorname{sgn}\gamma^{(r_1)})^{b_{r_1}} \quad \text{für} \quad \mathfrak{c} = (\gamma)[i]$$

†siehe auch den ebenfalls hierher gehörigen Satz 57, S. 299▶.

definiert. Nach Voraussetzung über die $\mathfrak{l}_i$ mit $a_i \neq 0$ zerfallen diese in $k(\sqrt{\alpha})$, sodaß für sie bei der Zerlegung:

$$\mathfrak{l}_i = (\lambda_i)[i, i'] = (\lambda_i)[i'][i]\,; \quad (\lambda_i \text{ tot. pos.})$$

gilt:

$$1 = \chi(\mathfrak{l}_i) \begin{matrix}\square\square\square \\ \square\square\square\end{matrix} = \chi(\lambda_i)\chi[i', i]$$

Wegen der Normiertheit gegen $[i', i]$ ist weiter $\chi[i', i] = 1$, also auch

$$\chi(\lambda_i) = \left(\frac{\lambda_i}{\alpha}\right) \prod_{\kappa} (\text{sgn. } \lambda_i^{[\ldots]})^{b_\kappa} = \left(\frac{\lambda_i}{\alpha}\right) = 1 \quad (\text{für } a_i = 1)$$

folgt. Wird ferner

$$\mathfrak{b} = (\beta_0)[i, i']\,; \qquad (\beta_0 \text{ total positiv})$$

gesetzt, so folgt

$$\beta = \beta_0 \prod_{i=1}^{z} \lambda_i^{a_i} [\eta, \omega]$$

wo $[\eta, \omega]$ ein total positives Idealquadrat ist, für das also

$$1 = \chi([\eta, \omega]) = \left(\frac{[\eta, \omega]}{\alpha}\right)$$

ist. Daher wird nach Satz 53:

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\beta_0}{\alpha}\right) \prod_{i=1}^{z} \left(\frac{\lambda_i}{\alpha}\right)^{a_i} = \left(\frac{\alpha}{\beta_0}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right),$$

weil die $\left(\frac{\lambda_i}{\alpha}\right)$ mit $a_i = 1$ gleich 1 sind, die mit $a_i = 0$ herausfallen.

und β_0 total positiv ist.

Ist α singulär primär, so führt man, wie schon mehrfach eine nicht singuläre primäre Hilfszahl α_0 mit denselben Bedingungen wie für α ein, sodaß der Satz für α_0, $\alpha\alpha_0$ also auch für α gilt.

Wir führen sodann entsprechend §8 die Normenrestsymbole für die zu 2 primen $\mathfrak{p}$ ein, für die Satz 42, 43 unverändert gelten. Die Normenrestsymbole $\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right)$ für die Teiler $\mathfrak{l}_i$ von 2 können wir hier ebenfalls von vornherein „endgültig“ definieren, [...] es nur eine Sorte von Normennichtresten (Normnichtzahlen) entsprechend dem Symbolwert -1 gibt. Die Gültigkeit von Zerlegungs– und Vertauschungssatz ist in diesem Falle unmittelbar einzusehen, denn der Zerlegungssatz für die erste Komponente folgt unmittelbar aus der Gruppeneigenschaft der Normzahlen, der Vertauschungssatz aus der Symmetrie der zu erfüllenden Gleichung

$$\alpha x^2 + \beta y^2 = z^2 \,(\mathfrak{l}_i),$$

und aus beiden der Zerlegungssatz für die zweite Komponente.

Bei der nunmehrigen Einführung der Symbole $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right]$ unterwerfen wir die Hilfsgrößen α_i außer den früheren Forderungen noch der Forderung „total positiv“. □□□

Dann überträgt sich Satz 44 wörtlich. Der Beweis wird z. T. etwas anderes. (s. S. 271▸)

ad 1.) Der Hauptschluß $\left(\frac{\alpha_i}{\beta}\right)\left(\frac{\beta}{\mathfrak{a}_i}\right)^{-1} = 1$ ist nach dem eben bewiesenen 2. Teil von Satz 54 richtig, weil α_i n. V. total positiv.

ad 3.) Zerlegungs– und Vertauschungssatz gelten für $\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right]$, ersterer auf Grund von Satz 42 und der Definition des Symbols, letzterer wegen der später zu beweisenden Gleichheit mit $\left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right)$.

ad 2.) Die Definition ist eindeutig, da der dortige Hauptschluß

$$\left(\frac{\gamma_i}{\mathfrak{b}}\right)\left(\frac{\beta}{\gamma_i}\right)^{-1} = 1$$

für $\gamma_i = \left(\frac{\alpha_i'}{\alpha_i}\right)$ richtig ist, weil γ_i hyperprimär und total positiv ist, und daher der 1. Teil von Satz 54 anwendbar ist.

Nunmehr ist der Hauptsatz 45 zu übertragen, den wir hier nur für total positives x zu beweisen brauchen:

Satz 55. Es ist für beliebige α, β:

$$\left[\frac{\beta,\alpha}{\mathfrak{l}_i}\right] = \left(\frac{\beta,\alpha}{\mathfrak{l}_i}\right).$$

Beweis: 1.) Der erste Teil des Beweises von Satz 45 überträgt sich wörtlich, da α_i total positiv vorausgesetzt, also $k(\sqrt{\alpha_i})$ eine Klassengruppe ohne Vorzeichenbedingungen zugeordnet ist.

2.) Genau eben daher überträgt sich auch der zweite Teil des Beweises.

Wir beweisen nunmehr in Analogie zu Satz 46 das Hilbertsche Reziprozitätsgesetz zunächst unter der Voraussetzung, daß α total positiv ist.

Satz 56. Für total positives α und beliebiges β ist

$$\prod_{\mathfrak{w}} \left(\frac{\alpha,\beta}{\mathfrak{w}}\right) = 1,$$

wenn $\mathfrak{w}$ alle Primteiler von k durchläuft.

Beweis: Da α total positiv, die α_i auch, ist auch

$$\gamma = \frac{\alpha_1 \dots \alpha_z}{\alpha}$$

total positiv und wie früher hyperprimär. Der Hauptschluß, nämlich

$$\prod_{\mathfrak{p}} \left(\frac{\beta,\gamma}{\mathfrak{p}}\right) = 1,$$

ist auch hier richtig, da für kernprime β, γ [...] die zu 2 primen $\mathfrak{p}$ folgt:

$$\prod_{\mathfrak{p}} \left(\frac{\beta,\gamma}{\mathfrak{p}}\right) = \left(\frac{\beta}{\gamma}\right)\left(\frac{\gamma}{\mathfrak{b}}\right)^{-1} = 1$$

nach Satz 54, 1. Teil. Für nicht kernprime β, γ kann genau so, wie a. S. 279 geschlossen werden.

Um nun das vollständige Hilbertsche Reziprozitätsgesetz für beliebige α und β zu erhalten, brauchen wir noch eine Verallgemeinerung von Satz 54.

Satz 57. Ist β beliebig, α_i für die zu 2 primen Primteiler kernprim zu β und hyperprimär und außerdem nur in $k^{(i)}$ negativ. Dann ist

$$\left(\frac{\alpha_i}{\mathfrak{b}}\right)\left(\frac{\beta}{\alpha_i}\right) = \operatorname{sgn}.\,\beta^{(i)},$$

wenn $\mathfrak{b}$ den zu 2 primen Kernbestandteil von β bezeichnet.

Beweis: (Ganz analog zum Beweis von Satz 41). Hier ist die $k(\sqrt{\alpha_i})$ zugeordnete Klassengruppe notwendig mit einer Vorzeichenbedingung, und zwar für $k^{(i)}$ allein behaftet.

Ist daher $[i]$ ein gegen α_i normiertes Repräsentantensystem im Sinne von Satz 50/51, □□□ welches nach Satz 51 wegen $\operatorname{sgn}\alpha_i^{(i)} = -1$ stets existiert und

$$\mathfrak{c} = (\gamma)[i],$$

so ist die $k(\sqrt{\alpha_i})$ zugeordnete Klassengruppe durch

$$1 = \chi(\mathfrak{c}) = \left(\frac{\gamma}{\alpha_i}\right)\operatorname{sgn}\gamma^{(i)}$$

definiert. die $\mathfrak{l}_i$ zerfallen in $k(\sqrt{\alpha_i})$, da α_i hyperprimär, sodaß für

$$\mathfrak{l}_\kappa = (\lambda_\kappa)[i]$$

gilt:

$$1 = \chi(\mathfrak{l}_\kappa) = \chi(\lambda_\kappa)\chi[i] = \chi(\lambda_\kappa) = \left(\frac{\lambda_\kappa}{\alpha_i}\right)\operatorname{sgn}.\,\lambda_\kappa^{(i)}.$$

300 III

Wird dann noch

$$\beta = \mathfrak{b}\prod_\kappa \mathfrak{l}_\kappa^{a_\kappa} j^2$$

und

$$\mathfrak{b} = (\beta_0)[i]$$

gesetzt, so folgt, wie schon öfter:

$$\beta = \beta_0 \prod_\kappa \mathfrak{b}^{a_\kappa}[\eta, \omega, \omega'],$$

wo $[\eta, \omega, \omega']$ ein Idealquadrat ist, sodaß

$$1 = \chi([\eta, \omega, \omega']) = \left(\frac{[\eta, \omega, \omega']}{\alpha_i}\right) \operatorname{sgn}([\eta, \omega, \omega'])^{(i)}$$

ist. Es wird dann:

$$\begin{aligned}
\left(\frac{\beta}{\alpha_i}\right) &= \left(\frac{\beta_0}{\alpha_i}\right) \prod_{\kappa} \left(\frac{\lambda_\kappa}{\alpha_i}\right)^{a_\kappa} \left(\frac{[\eta, \omega, \omega']}{\alpha_i}\right) \quad \text{und nach Satz 53:} \\
&= \left(\frac{\alpha_i}{\beta_0}\right) \operatorname{sgn} \beta_0^{(i)} \prod_{\kappa} (\operatorname{sgn}. \lambda_\kappa^{(i)})^{a_\kappa} \operatorname{sgn}.([\eta, \omega, \omega'])^{(i)} \\
&= \left(\frac{\alpha_i}{\mathfrak{b}}\right) \operatorname{sgn}.\beta^{(i)}, \qquad \text{w. z. b. w.}
\end{aligned}$$

Nunmehr können wir das Hilbertsche Reziprozitätsgesetz vollständig beweisen:

Satz 58. Für beliebige α, β aus k ist

$$\prod_{\mathfrak{w}} \left(\frac{\alpha, \beta}{\mathfrak{w}}\right) = 1,$$

wenn $\mathfrak{w}$ alle Primteiler von k einschließlich der r_1 Stellen $\mathfrak{p}_\infty^{(i)}$[2] durchläuft.

Beweis: Seien $k^{(1)}, k^{(2)}, \ldots, k^{(r_0)}$ die r_0 Körper in denen α negativ. Dann bestimmen wir r_0 hyperprimäre, zu β kernprime Hilfsgrößen $\alpha_1, \alpha_2, \ldots, \alpha_{r_0}$ die je nur in dem ersten[3] dieser Körper negativ sind. Es ist dann:

$$\prod_{\mathfrak{w}} \left(\frac{\alpha_i, \beta}{\mathfrak{w}}\right) = \prod_{\mathfrak{p}} \left(\frac{\alpha_i, \beta}{\mathfrak{p}}\right) \cdot \prod_{\mathfrak{l}} \left(\frac{\alpha_i, \beta}{\mathfrak{l}}\right) \cdot \prod_{\mathfrak{p}_\infty} \left(\frac{\alpha_i, \beta}{\mathfrak{p}_\infty}\right)$$

Da α_i hyperprimär sind die $\left(\frac{\alpha_i, \beta}{\mathfrak{l}}\right) = 1$. Ferner reduziert sich

das Produkt über die $\mathfrak{p}_\infty$ auf

$$\left(\frac{\alpha_i, \beta}{\mathfrak{p}_\infty^{(i)}}\right) = \operatorname{sgn} \beta^{(i)},$$

[2] Superskript von $\mathfrak{p}$ nicht eindeutig zu entziffern
[3] Wort ist schwer zu entziffern

schließlich ist, wenn $\mathfrak{b}$ der zu 2 prime Kernbestandteil von β ist:

$$\prod_{\mathfrak{p}} \left(\frac{\alpha_i, \beta}{\mathfrak{p}}\right) = \left(\frac{\alpha_i}{\mathfrak{b}}\right)\left(\frac{\beta}{\alpha_i}\right)$$

Nach Satz 57 folgt also

$$\prod_{\mathfrak{w}} \left(\frac{\alpha_i, \beta}{\mathfrak{w}}\right) = \left(\frac{\alpha_i}{\mathfrak{b}}\right)\left(\frac{\beta}{\alpha_i}\right)\operatorname{sgn}\beta^{(i)} = 1.$$

Weiter folgt dann also nach dem Zerlegungssatz:

$$\prod_{\mathfrak{w}} \left(\frac{\alpha_1 \dots \alpha_{r_0}, \beta}{\mathfrak{w}}\right) = 1.$$

Nach Satz 56 ist

$$\prod_{\mathfrak{w}} \left(\frac{\alpha\alpha_1\alpha_2 \dots \alpha_{r_0}, \beta}{\mathfrak{w}}\right) = 1,$$

weil $\alpha\alpha_1 \dots \alpha_{r_0}$ total positiv, und daher die in der Formel von Satz 56 noch nicht mit auftretenden $\mathfrak{p}_\infty$ keinen Beitrag -1 liefern.

Nach nochmaliger Anwendung des Zerlegungssatzes folgt endlich

$$\prod \left(\frac{\alpha, \beta}{\mathfrak{w}}\right) = 1$$

w. z. b. w.

3.9 §9 Eine charakteristische Eigenschaft des Normsymbols.

§9 Eine charakteristische Eigenschaft des Normenrestsymbols.

In K. K. §1, E und F wurden die beiden Sätze 19, 19a, 20, 20a über die Normenreste eines relativ zyklischen Körpers von Primzahlgrad bewiesen. Für den Fall, daß k die ℓ–te Einheitswurzel ζ enthält, lassen sich diese Sätze unter Anwendung des Hilbertschen Normenrestsymbols erheblich verallgemeinern. Es gilt folgender weitgehendste Satz dieser Richtung:

Satz 59. Dann und nur dann, wenn ein Element β von k für alle Primstellen (einschl. der $\mathfrak{p}_\infty$) Normzahl von $k(\sqrt[\ell]{\alpha})$ ist, ist es Relativnorm $\beta = n(\mathsf{A})$ einer Zahl A von $k(\sqrt[\ell]{\alpha})$, d. h. dann und nur dann wenn

$$\left(\frac{\beta, \alpha}{\mathfrak{w}}\right) \equiv 1$$

ist, ist

$$\beta = n(\mathsf{A}).$$

Beweis: 1.) Ist $\beta = n(\mathsf{A})$, so ist natürlich β Normzahl für alle $\mathfrak{w}$, also $\left(\frac{\beta,\alpha}{\mathfrak{w}}\right) \equiv 1$ (identisch 1 bedeutet: $= 1$ für alle $\mathfrak{w}$).

2.) Sei $\left(\frac{\beta,\alpha}{\mathfrak{w}}\right) \equiv 1$. Dann ist β sicher Relativnorm eines Ideals aus $k(\sqrt[\ell]{\alpha}$. Denn enthielte β einen Primteiler $\mathfrak{q}$, der nicht zerfällt, mit zu ℓ primem Exponenten c, so wäre

$$\left(\frac{\beta, \alpha}{\mathfrak{q}}\right) = \left(\frac{\alpha}{\mathfrak{q}}\right)^{-c} \neq 1,$$

falls $\mathfrak{q}$ prim zu ℓ, und nach dem Auswertungsgesetz[1] für die Teiler von ℓ auch

$$\left(\frac{\beta, \alpha}{\mathfrak{q}}\right) = 1,$$

[1] undeutlich

falls $\mathfrak{q}$ ein Teiler von ℓ ist. β enthält also kein solches $\mathfrak{q}$. Da alle übrigen Primteiler Relativnormen ihrer Primteiler in $k(\sqrt[\ell]{\alpha})$

sind, und ℓ–te Idealpotenzen a fortiori Relativnormen von Idealen sind, kann also

$$\beta = n(\mathfrak{A})$$

gesetzt werden.

$k(\sqrt[\ell]{\alpha})$ sei Klassenkörper für die Klassengruppe H vom Führer f. Wenn $\mathfrak{A}$ nicht prim zu f ist, so sei □□□ $\mathfrak{B}$ aus

$$\mathfrak{A}\mathfrak{B} = (\mathsf{B})$$

prim zu f bestimmt. Dann ist

$$\big(n(\mathsf{B})\big) = (\beta)n(\mathfrak{B}),$$

also $n(\mathfrak{B})$ Hauptideal, dessen Zahlrepräsentant β_0 so bestimmt sei, daß

$$n(\mathsf{B}) = \beta\beta_0$$

ist. Es ist dann auch

$$\left(\frac{\beta_0, \alpha}{\mathfrak{w}}\right) \equiv 1,$$

weil nach 1.) $\left(\frac{n(\mathsf{B}),\alpha}{\mathfrak{w}}\right) \equiv 1$ ist. Es genügt dann, den Satz für β_0 zu beweisen, da aus

$$\beta_0 = n(\mathsf{A}_0)$$

folgt

$$\beta = n\left(\frac{\mathsf{B}}{\mathsf{A}_0}\right) = n(\mathsf{A}).$$

Da $\beta_0 = n(\mathfrak{B})$ mit zu f primem $\mathfrak{B}$ ist, darf also das obige $\mathfrak{A}$ von vornherein prim zu f angenommen werden, sodaß auch β prim zu f ist.

Dann ist aber β nach Voraussetzung speziell Normenrest mod f und für $\ell = 2$ außerdem positiv in den $k^{(i)}$, für die α negativ ist. Daher gehört

β zur Strahlhauptklasse mod f der in K. K. §1 E u. F zugrundegelegten Strahlklasseneinteilung[2] nach den Normenresten mod f.

304 III

Das Ideal $\mathfrak{A}$ hat eine in der Hauptklasse mod f liegende Relativnorm $\beta = n(\mathfrak{A})$, gehört also nach der früheren Definition zum Hauptgeschlecht von $k(\sqrt[\ell]{\alpha})$ und ist daher nach K. K. Satz 18 von der Form:

$$\mathfrak{A} = \mathfrak{B}^{1-\sigma}(\mathsf{B})$$

sodaß für $\beta = n(\mathfrak{A})$ folgt

$$(\beta) = n(\mathfrak{B}^{1-\sigma}\mathsf{B}) = n(\mathsf{B})$$

d. h.

$$\beta = \varepsilon n(\mathsf{B})$$

wo ε eine Einheit in k ist. B darf prim zu f genommen werden (indem man vorerst $\mathfrak{B}$ in seiner Klasse prim zu f wählt, sodaß $n(\mathsf{B})$ und somit ε Normenrest mod f ist. Nach K. K. Satz 19, 19a ist dann, (weil ε für $\ell = 2$ auch offenbar in den „kritischen Körpern positiv ist, weil es $n(\mathsf{B})$ ist),

$$\varepsilon = n(\mathsf{B}_0)$$

Daraus folgt

$$\beta = n(\mathsf{B}\mathsf{B}_0) = n(\mathsf{A}), \qquad \text{w. z. b. w.}$$

Für $\ell = 2$ bildet der bewiesene Satz die Grundlage für die Theorie der ternären und höheren quadratischen Formen in k. Offensichtlich läßt er sich nämlich auch so aussprechen:

Satz 60. Die Gleichung

$$\alpha x^2 + \beta y^2 = z^2$$

ist für beliebige α, β in k dann und nur dann durch 3 Zahlen x, y, z aus k nicht identisch lösbar, wenn

$$\left(\frac{\alpha, \beta}{\mathfrak{w}}\right) \equiv 1,$$

wenn sie also für alle Primstellen in k einzeln lösbar ist.

Näheres siehe in meiner Arbeit in Crelle **153** über die quadratischen Formen in k.

[2] undeutlich

3.10 §10 Die Produktformel für die L–Reihen und Größencharakteren des Klassenkörpers.

§10 Produktformel für die $L_K(s, \Lambda)$ des Klassenkörpers.

(Ergänzung zu §7 von „Funktionalgleichung der allgemeinsten L–Reihen mit Größencharakteren“, siehe Seite 139, ff.).

Die a. a. O. für den Klassenkörper K entwickelte Formel

$$\zeta_K(s) = \prod_{\chi} L(s, \chi)$$

ist einer weitgehenden Verallgemeinerung fähig, wenn man die L–Reihen mit Größencharakteren ähnlichen Betrachtungen unterwirft.

Sei K Klassenkörper für k nach der Klassengruppe H vom Index h, χ bedeute die Charaktere nach H, deren Führer $f(x)$ Teiler des Führers $\mathfrak{F}$ von H sind.

Es sei λ ein Größencharakter für den Strahl in k *aller* Körperzahlen (ohne Vorzeichenbedingung), der also entsprechend der früheren Vorschrift mithilfe eines Systems absoluter Grundeinheiten definiert wird, vermöge der charakteristischen Eigenschaften:

$$\begin{aligned} \lambda(\widehat{\alpha})\lambda(\widehat{\beta}) &= \lambda(\widehat{\alpha}\widehat{\beta}), \\ \lambda(\varepsilon) &= 1 \quad \text{für Körpereinheiten}, \\ |\lambda(\widehat{\alpha})| &= 1. \end{aligned}$$

$\lambda(\widehat{\alpha})$ ist also gleichzeitig ein „*Größencharakter für Ideale*“, der in früherem Sinne auch als zum Strahl aller total positiven Körperzahlen gehörig aufgefaßt werden kann.

Wir bilden nun die h Charaktere

$$\lambda_\chi\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha}).$$

Diese sind ebenfalls Größencharaktere für Ideale, da sie die Definitionsgleichungen solcher erfüllen:

$$\begin{aligned} \lambda_\chi\big((\widehat{\alpha})\big)\lambda_\chi\big((\widehat{\beta})\big) &= \lambda_\chi\big((\widehat{\alpha})(\widehat{\beta})\big), \\ \lambda_\chi\big((\alpha)\big) &= \lambda(\alpha), \quad \text{wenn} \quad \alpha \equiv 1 \mod f, \text{ total positiv}, \\ \lambda_\chi\big((\varepsilon)\big) &= 1, \end{aligned}$$

und zwar gehört $\lambda_\chi\big((\widehat{\alpha})\big)$ in früherem Sinne zu dem als Größencharakter für den Strahl aller total positiven Körperzahlen gehörig aufzufassenden $\lambda(\widehat{\alpha})$. Die frühere eindeutige Zerlegung wird

$$\lambda_\chi\big((\widehat{\alpha})\big) = \lambda(\widehat{\alpha})\chi(\widehat{\alpha}) = \lambda(\widehat{\alpha})v(\widehat{\alpha})\chi_0(\widehat{\alpha}),$$

wenn (mit gegen früher abgeänderter Bezeichnung)

$$\chi(\widehat{\alpha}) = v(\widehat{\alpha})\chi_0(\widehat{\alpha})$$

die eindeutige Zerlegung von $\chi(\widehat{\alpha})$ in einen Vorzeichencharakter und einen „Zahlcharakter mod f“ ist.

□□□ $\lambda(\widehat{\alpha})$ hat verschiedene Darstellungen (Exponentensysteme m_q, a_p), je nachdem welchen Strahl man seiner Definition zugrundegelegt denkt. Prinzipiell ist dies für jeden Strahl möglich, da jede solche im umfassendsten Strahl aller Körperzahlen, zu dem $\lambda(\widehat{\alpha})$ ebenfalls Größencharakter ist, enthalten ist, also die Definitionsgleichungen für jeden Strahl befriedigt. Jedenfalls ist aber $\lambda(\widehat{\alpha})$ eine der in Satz 1, S. 6 bestimmten Funktionen $F(\widehat{\alpha})$ und hat daher eine Darstellung:

$$\lambda(\widehat{\alpha}) = \prod_{p=1}^{r_1+r_2} |\widehat{\alpha}^{(p)}|^{is_p} \cdot \prod_{p=r_1+1}^{n} \left(\frac{\widehat{\alpha}^{(p)}}{|\widehat{\alpha}^{(p)}|}\right)^{a_p},$$

wobei die s_p, a_p (letztere positiv in der bekannten Weise) durch $\lambda(\widehat{\alpha})$ *eindeutig* bestimmt sind, und gewissen Beschränkungen durch die Forderung

$$\lambda(\varepsilon) = 1 \quad \text{für Körpereinheiten } \varepsilon$$

unterworfen sind. Die a_p sind also gegenüber der Darstellung von $\lambda(\widehat{\alpha})$ (Wahl des zugrundegelegten Strahls) invariant, während die m_q vom zugrundegelegten Strahl abhängen, (sie erfordern die Logarithmen der betr. Strahlgrundeinheiten, d. h. die Größen $e_q^{(p)}$, zu ihrer Darstellung). Im übrigen kommt es uns auf die m_q nicht an, wir kommen mit den s_p vollständig aus.

Die Funktion $\lambda(\widehat{\alpha}) = \lambda(\mathfrak{a})$ gibt Anlaß zu einem bestimmten Größencharakter $\Lambda(\mathfrak{A})$ in K:

$$\Lambda(\mathfrak{A}) = \lambda\big(n(\mathfrak{A})\big).$$

$\Lambda(\mathfrak{A})$ hängt nach dieser Definition nur vom *Ideal* $\mathfrak{A}$ ab, da dasselbe für $\lambda(\mathfrak{a})$ gilt, ferner ist

$$\Lambda(\mathfrak{A})\Lambda(\mathfrak{B}) = \Lambda(\mathfrak{A}\mathfrak{B})$$

wegen der entsprechenden Eigenschaft von $n(\mathfrak{A})$, schließlich ist für Körperzahlen A aus K:

$$\Lambda(\mathsf{A}) \quad \text{Zahlgrößencharakter in } K \mod 1,$$

denn es erfüllt die Definitionsgleichungen eines solchen, sogar für den Strahl aller Körperzahlen in K.

308 III

Daher ist tatsächlich $\Lambda(\mathfrak{A})$ Größencharakter für Ideale in K, und entspricht in früherem Sinne aus dem Zahlgrößencharakter $\Lambda(\mathsf{A})$ (ohne Vorzeichencharakter und Klassencharakter `[...]` seiner Zerlegung).

Wir berechnen noch das entsprechende Exponentensystem S_p, A_p von $\Lambda(\mathfrak{A})$. Sei X ein Körpervektor von K mit den Komponenten $X_p^{(\kappa)}$, wobei der Index κ die relativ–konjugierten zu K in Bezug auf k anzeigt. Dann ist

$$\begin{aligned}\Lambda(X) &= \lambda\big(n(X)\big) = \lambda(X^{(1)} \cdots X^{(h)}) \\ &= \prod_{p=1}^{r_1+r_2} |X_p^{(1)} \dots X_p^{(h)}|^{is_p} \cdot \prod_{p=r_1+1}^{n} \left(\frac{X_p^{(1)} \dots X_p^{(h)}}{|X_p^{(1)} \dots X_p^{(h)}|}\right)^{a_p}.\end{aligned}$$

Es seien nun von den hr_1 konjugierten Körpern, die den r_1 reellen konjugierten zu k entsprechen hr_0 reell, die übrigen $h(r_1 - r_0)$ komplex, also

$$R_1 = hr_0; \quad R_2 = \frac{h(r_1 - r_0)}{2} + hr_2,$$

so wird

$$\begin{aligned}\Lambda(X) &= \prod_{p=1}^{r_1+r_2}\prod_{\kappa=1}^{h}|X_p^{(\kappa)}|^{is_p}\prod_{p=r_1+1}^{n}\prod_{\kappa=1}^{h}\left(\frac{X_p^{(\kappa)}}{|X_p^{(\kappa)}|}\right)^{a_p}\\ &= \prod_{p=1}^{r_0}\prod_{\kappa=1}^{h}|X_p^{(\kappa)}|^{iS_p^{(\kappa)}}\prod_{p=r_0+1}^{r_1}\prod_{\kappa=1}^{\frac{h}{2}}|X_p^{(\kappa)}|^{iS_p^{(\kappa)}}\cdot\prod_{p=r_1+1}^{r_2}\prod_{\kappa=1}^{h}|X_p^{(\kappa)}|^{iS_p^{(\kappa)}}\\ &\quad\cdot\prod_{p=r_0+1}^{r_1}\prod_{\kappa=1}^{h}\left(\frac{X_p^{(\kappa)}}{|X_p^{(\kappa)}|}\right)^{A_p^{(\kappa)}}\prod_{p=r_1+1}^{n}\prod_{\kappa=1}^{h}\left(\frac{X_p^{(\kappa)}}{|X_p^{(\kappa)}|}\right)^{A_p^{(\kappa)}}.\end{aligned}$$

Durch Exponentenvergleich folgt also wegen der eindeutigen Bestimmtheit der $A_p^{(\kappa)}, S_p^{(\kappa)}$ durch $\Lambda(\mathfrak{A})$:

$$\begin{aligned}
S_p^{(\kappa)} &= s_p \quad \text{für} \quad p=1,\dots,r_0 \quad \text{und} \quad r_1+1,\dots,r_2\,; \\
&\qquad (\kappa=1,\dots,h)\\
S_p^{(\kappa)} &= 2s_p \quad \text{für} \quad p=r_0+1,\dots,r_1\,; \quad (\kappa=1,\dots,\tfrac{h}{2})\\
&\qquad (\text{die } h \text{ konjugierten geeignet geordnet!})\\
A_p^{(\kappa)} &= 0 \quad \text{für} \quad p=r_0+1,\dots,r_1\,; \quad (\kappa=1,\dots,h)\\
A_p^{(\kappa)} &= a_p \quad \text{für} \quad p=r_1+1,\dots,n\,; \quad (\kappa=1,\dots,h).
\end{aligned}$$

Wir stellen ferner noch die zu verwendenden Größen $\mathsf{E}_p^{(\kappa)}$ her, die den e_p in k entsprechen:

$$\begin{aligned}
\mathsf{E}_p^{(\kappa)} &= 1 \quad \text{für} \quad p=1,\dots,r_0; \quad (\kappa=1,\dots,h)\\
\mathsf{E}_p^{(\kappa)} &= 2 \quad \text{für} \quad p=r_0+1,\dots,n; \quad (\kappa=1,\dots,h)
\end{aligned}$$

und somit

$$n(\mathsf{E}_p^{(\kappa)}) = \left(\prod_{\kappa=1}^{h}\mathsf{E}_p^{(\kappa)}\right) = (\underbrace{1,\dots,1}_{1,\dots,r_0};\ \underbrace{2^h,\dots,2^h}_{r_0+1,\dots,n})$$

Nach diesen Vorbereitungen bilden wir

$$L_K(s,\Lambda) = \prod_{\mathfrak{P}}\frac{1}{1-\frac{\Lambda(\mathfrak{P})}{\mathsf{N}\mathfrak{P}^s}} = \sum_{\mathfrak{A}}\frac{\Lambda(\mathfrak{A})}{\mathsf{N}\mathfrak{A}^s}\,.$$

Wir suchen diese L–Reihe mit dem Größencharakter Λ aus K in ein Produkt von $L(s,\lambda)$ aus k zu zerspalten. Dazu bestimmen wir zunächst den Beitrag eines zu $\mathfrak{F}$ primen $\mathfrak{p}$ aus k zu $L_K(s,\Lambda)$. Es gilt:[1]

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_g\,; \qquad n(\mathfrak{P}_i) = \mathfrak{p}^{\mathfrak{f}}$$

wenn $\mathfrak{f}$ der kleinste Exponent, sodaß $\mathfrak{p}^f$ in H ist.

310 III

Es wird also

$$\Lambda(\mathfrak{P}_i) = \big(\lambda(\mathfrak{p})\big)^f\,; \qquad \mathsf{N}(\mathfrak{P}_i) = N\mathfrak{p}^f\,;$$

$$\prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1-\frac{\Lambda(\mathfrak{P})}{\mathsf{N}\mathfrak{P}^s}} = \frac{1}{\left(1-\left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^f\right)^g} = \prod_{\chi} \frac{1}{1-\frac{\chi(\mathfrak{p})\lambda(\mathfrak{p})}{N\mathfrak{p}^s}}\,,$$

weil, wie früher gezeigt, $\chi(\mathfrak{p})$ jede $\mathfrak{f}$–te Einheitswurzel genau $\mathfrak{p}$ mal annimmt.

Wir betrachten demnach

$$G(s,\lambda) = \frac{\prod\limits_{\chi} L(s,\lambda_\chi)}{L_K(s,\Lambda)} = \frac{\prod\limits_{\mathfrak{p}|\mathfrak{F}}\prod\limits_{\chi}\left(1-\frac{\lambda(\mathfrak{p})\chi(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{-1}}{\prod\limits_{\mathfrak{p}|\mathfrak{F}}\left(1-\left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^f\right)^{-g}}\,,$$

wenn die vorläufig als unbekannt betrachtete Zerlegung dieser $\mathfrak{p}$ in der Form

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e\,; \quad n(\mathfrak{P}_i) = \mathfrak{p}^{\mathfrak{f}}\,; \quad efg = h$$

angesetzt wird.

Bezeichnet ferner $\mathsf{H}_\mathfrak{p}$ diejenige Klassengruppe, die durch die Forderungen

$$\chi(\mathfrak{a}) = 1, \quad \text{wenn } f(\chi) \text{ prim zu } \mathfrak{p}$$

definiert ist, so nimmt $\chi(\mathfrak{p})$ außer den keinen Beitrag zum Produkt liefernden Werten 0 (falls $f(\chi)$ nicht prim zu $\mathfrak{p}$) genau jede $\mathfrak{f}'$–te Einheitswurzel g' mal an, wenn $\mathfrak{f}'$ der kleinste Exponent ist, sodaß $\mathfrak{p}^{\mathfrak{f}'}$ in $\mathsf{H}_\mathfrak{p}$ und g' der komplementäre Teiler bezüglich des Index $h_\mathfrak{p}$ von $\mathsf{H}_\mathfrak{p}$, also $g' = \frac{h_\mathfrak{p}}{\mathfrak{f}'}$. $h_\mathfrak{p}$ ist ferner Teiler

[1] Hasse verwendet auf dieser und den folgenden Seiten den Buchstaben f in zwei verschiedenen Schreibweisen. Das f mit zwei Schlaufen (je eine oben und unten) wird hier als $\mathfrak{f}$ wiedergegeben, für das f mit nur einer Schlaufe (oben) wird hier f geschrieben.

von h, sodaß $h = h_{\mathfrak{p}} e' = e' f' g'$ wird, und unser früheres Zerlegungsgesetz für die Teiler von $\mathfrak{F}$ lautete

$c = c',\ f = f',\ g = g'$. Dies werden wir jetzt mithilfe der $L(s, \lambda_\chi)$, $L_K(s, \Lambda)$ und ihren Funktionalgleichungen beweisen können, was oben in §7 mit $\zeta_K(s)$ und den $L(s, \chi)$ allein nicht möglich war. Wir haben nämlich nur zu zeigen, daß in dem Quotienten

$$G(s,\lambda) = \frac{\prod\limits_{\chi} L(s,\lambda_\chi)}{L_K(s,\Lambda)} = \frac{\prod\limits_{\mathfrak{p}|\mathfrak{F}} \left(1 - \left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{f'}\right)^{-g'}}{\prod\limits_{\mathfrak{p}|\mathfrak{F}} \left(1 - \left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{f}\right)^{-g}}$$

sich die Faktoren rechts gliedweise herausheben müssen, wobei dann gleichzeitig

$$G(s,\lambda) \equiv 1,$$

also die Produktrelation

$$\prod_{\chi} L(s,\lambda_\chi) = L_K(s,\Lambda)$$

herauskommen wird.

1.) *Funktionalgleichung für* $L_K(s,\Lambda)$.

Die Funktionalgleichung für $L_K(s,\Lambda)$ erfordert nach Satz 38, S. 131 die Aufstellung folgender Ausdrücke:

$$\gamma(\Lambda) = \Lambda(\sqrt{\mathsf{E}_p^{(\kappa)}}) = (\sqrt{2})^{i\frac{h}{2}\sum\limits_{p=r_0+1}^{r_1} 2s_p + ih\sum\limits_{p=r_1+1}^{r_2} s_p},$$

$$= (\sqrt{2})^{ih\sum\limits_{p=r_0+1}^{r_2} s_p},$$

$$\Gamma(s,\Lambda) = \prod_{p=1}^{r_0} \Gamma^h\left(\frac{s}{2} - \frac{is_p}{2}\right) \cdot \prod_{p=r_0+1}^{r_1} \Gamma^{\frac{h}{2}}(s - is_p) \cdot$$

$$\cdot \prod_{p=r_1+1}^{r_1+r_2} \Gamma^h\left(s + \frac{a_p + a'_p}{2} - \frac{is_p}{2}\right),$$

wie leicht aus den Werten von $A_p^{(\kappa)}$, $S_p^{(\kappa)}$, $\mathsf{E}_p^{(\kappa)}$ sowie der allgemeinen Formel von Satz 38 in der Form

$$\Gamma(s,\lambda)=\prod_{p=1}^{r+1}\Gamma\left(\frac{e_p}{2}\left(s+\frac{a_p+a_p'}{2}\right)-\frac{is_p}{2}\right)$$

(ausgedrückt durch die Invarianten s_p von Satz 1 zu $\lambda(x)$) hervorgeht.

Ferner ist

$$\mathsf{A}_K=\sqrt{\frac{\mathsf{D}}{2^{2hr_2+hr}[\ldots]hr_0\,.\,\pi^{nh}}}=\sqrt{\frac{\mathsf{D}}{2^{nh-r_0h}\pi^{nh}}}\,,$$

weil Λ den Führer 1 hat.

Die Funktionalgleichung für $L_K(s,\Lambda)$ besagt dann:

$$\boldsymbol{\gamma(\Lambda)\Gamma(s,\Lambda)\mathsf{A}_K^s L_K(s,\Lambda)=\Xi(s,\Lambda)}\quad \textit{genügt der Relation}$$
$$\boldsymbol{\Xi(s,\Lambda)=\Xi(1-s,\overline{\Lambda})W(\Lambda)}$$
$$\textit{wo}\quad \boldsymbol{|W(\Lambda)|=1}.$$

2.) *Funktionalgleichung für die $L(s,\lambda_\chi)$.*

Hier ist:

$$\gamma(\lambda_\chi)=\lambda(\sqrt{e_p})=(\sqrt{2})^{i\sum\limits_{r_1+1}^{r_1+r_2}s_p}$$
$$\Gamma(s,\lambda_\chi)=\prod_{p=1}^{r+1}\Gamma\left(\frac{e_p}{2}\left(s+\frac{a_p+a_p'}{2}\right)-\frac{is_p}{2}\right)$$
$$=\prod_{p=1}^{r_1}\Gamma\left(\frac{s+a_p}{2}-\frac{is_p}{2}\right)\cdot\prod_{p=r_1+1}^{r_1+r_2}\Gamma\left(s+\frac{a_p+a_p'}{2}-\frac{is_p}{2}\right)$$
$$\mathsf{A}_{\lambda_\chi}=\sqrt{\frac{dN\big(f(\chi)\big)}{2^{2r_2}\pi^n}}$$

Für die Funktionalgleichung von $\prod_\chi L(s,\lambda_\chi)$ brauchen wir:

$$\prod_\chi \gamma(\lambda_\chi) = (\sqrt{2})^{ih\sum_{r_1+1}^{r_1+r_2} s_p}$$

$$\prod_\chi \Gamma(s,\lambda_\chi) = \prod_{p=1}^{r_1} \Gamma\left(\frac{s}{2} - \frac{is_p}{2}\right)^{\nu_p^{(1)}} \cdot \prod_{p=1}^{r_1} \Gamma\left(\frac{s+1}{2} - \frac{is_p}{2}\right)^{\nu_p^{(2)}} \cdot \cdot \prod_{p=r_1+1}^{r_1+r_2} \Gamma^h\left(s + \frac{a_p + a_p'}{2} - \frac{is_p}{2}\right)$$

$$\prod_\chi \mathsf{A}_{\lambda_\chi} = \sqrt{\frac{d^h N \prod f(\chi)}{2^{2r_2 h}\pi^{nh}}},$$

wo $\nu_p^{(1)}, \nu_p^{(2)}$ die Anzahlen der χ mit $a_p = 0$, $a_p = 1$ bezeichnen. (Die a_p für $p = 1, 2, \ldots r_1$ hängen nur von χ, die a_p für $r_1+1, \ldots r_1+r_2$ dagegen von λ ab, letztere ebenso wie die s_p[2] sind also für alle λ_χ dieselben).

Die Funktionalgleichung für ein $L(s,\lambda_\chi)$ besagt dann:

$$\boldsymbol{\xi(s,\lambda_\chi)\gamma(\lambda_\chi)\Gamma(s,\lambda_\chi)\mathsf{A}_{\lambda_\chi}^s L(s,\lambda_\chi)} \quad \textit{genügt der Relation}$$

$$\boldsymbol{\xi(s,\lambda_\chi) = \mathsf{W}(\lambda_\chi)\xi(1-s,\overline{\lambda}_{\overline{\chi}})}$$

$$\textit{wo} \quad \boldsymbol{|\mathsf{W}(\lambda_\chi)| = 1}.$$

Denn $\overline{\lambda}_\chi = \overline{\lambda}_{\overline{\chi}}$. Nun durchläuft $\overline{\chi}$ mit χ dieselben Charaktere, also

$$\prod_\chi \xi(1-s,\overline{\lambda}_{\overline{\chi}}) = \prod_\chi \xi(1-s,\overline{\lambda}_\chi).$$

Wird also

$$\prod_\chi \xi(s,\lambda_\chi) = \prod_\chi \gamma(\lambda_\chi) \cdot \prod_\chi \Gamma(s,\lambda_\chi) \cdot \prod_\chi \mathsf{A}_{\lambda_\chi} \cdot \prod_\chi L(s,\lambda_\chi) = \eta(s,\lambda)$$

gesetzt, so gilt

[2] undeutlich

$$\eta(s,\lambda) = \prod_{\chi} \mathsf{W}(\lambda_\chi) \cdot \eta(1-s,\overline{\lambda})$$

wo $|\prod_{\chi} \mathsf{W}(\lambda_\chi)| = 1$ ist.

Die aufzustellende Funktionalgleichung für $\frac{\prod_\chi L(s,\lambda_\chi)}{L_K(s,\Lambda)}$ folgt nun durch Division beider Funktionalgleichungen:

$$\mathsf{H}(s,\lambda) = \frac{\eta(s,\lambda)}{\Xi(s,\lambda)} = \frac{\prod_\chi \gamma(\lambda_\chi)\cdot\prod_\chi \Gamma(s,\lambda_\chi)\cdot\prod_\chi \mathsf{A}_{\lambda_\chi}^s \cdot \prod_\chi L(s,\lambda_\chi)}{\gamma(\Lambda)\cdot\Gamma(s,\Lambda)\cdot\mathsf{A}_K^s L_K(s,\Lambda)}$$
$$= \frac{\eta(1-s,\overline{\lambda})}{\Xi(1-s,\overline{\Lambda})} \cdot \frac{\prod_\chi \mathsf{W}(\lambda_\chi)}{\mathsf{W}(\Lambda)} = \frac{\prod_\chi \mathsf{W}(\lambda_\chi)}{\mathsf{W}(\Lambda)} \cdot \mathsf{H}(1-s,\overline{\lambda}),$$

denn $\overline{\Lambda}$ ist $\overline{\lambda}$ ebenso zugeordnet, wie Λ zu λ.

314 III

Durch Einsetzen der aufgestellten Ausdrücke folgt also:[3]

$$\mathsf{H}(s,\lambda) = G(s,\lambda)\frac{(\sqrt{2})^{ih\sum_{r_1+1}^{r_2} s_p} \cdot \prod_{p=1}^{r_1} \Gamma\left(\frac{s}{2} - \frac{is_p}{2}\right)^{\nu_p^{(1)}} \cdot \prod_{p=1}^{r_1} \Gamma\left(\frac{s+1}{2} - \frac{is_p}{2}\right)^{\nu_p^{(2)}} \cdot}{(\sqrt{2})^{ih\sum_{r_0+1}^{r_1} s_p} \cdot \prod_{p=1}^{r_0} \Gamma^h\left(\frac{s}{2} - \frac{is_p}{2}\right) \cdot \prod_{p=r_0+1}^{r_1} \Gamma^{\frac{h}{2}}(s - is_p) \cdot}$$
$$\frac{\cdot \prod_{p=r_1+1}^{r_1+r_2} \Gamma^h\left(s + \frac{a_p+a_p'}{2} - \frac{is_p}{2}\right) \sqrt{\frac{d^h N \prod f(\chi)}{2^{2r_2 h}\pi^{nh}}}^s}{\cdot \prod_{p=r_1+1}^{r_1+r_2} \Gamma^h\left(s + \frac{a_p+a_p'}{2} - \frac{is_p}{2}\right) \sqrt{\frac{g}{2^{nh-r_0 h}\pi^{nh}}}^s}$$
$$= G(s,\lambda)\frac{\prod_{p=1}^{r_1} \Gamma^{\nu_p^{(1)}}\left(\frac{s-is_p}{2}\right) \cdot \prod_{p=1}^{r_1} \Gamma^{\nu_p^{(2)}}\left(\frac{s+1-is_p}{2}\right)}{(\sqrt{2})^{ih\sum_{r_0+1}^{r_1} s_p} \cdot \prod_{p=1}^{r_0} \Gamma^h\left(\frac{s-is_p}{2}\right) \cdot \prod_{p=r_0+1}^{r_1} \Gamma^{\frac{h}{2}}(s - is_p)} \cdot$$
$$\cdot \sqrt{N\frac{\prod f(\chi)}{\mathfrak{D}}}^s \cdot \sqrt{2}^{(r_1-r_0)hs}$$

Ferner ist nach der dritten Funktionalgleichung der Γ–Funktion:

$$\Gamma(s-is_p) = \frac{2^{s-is_p}}{2\sqrt{\pi}}\Gamma\left(\frac{s-is_p}{2}\right) \cdot \Gamma\left(\frac{s+1-is_p}{2}\right),$$

[3] Die Summationsgrenzen sind in einigen Fällen schwer lesbar.

daß

$$\Gamma^{\frac{h}{2}}(s-is_p) = \frac{(\sqrt{2})^{h(s-is_p)}}{2^{\frac{h}{2}}(\sqrt{\pi})^{\frac{h}{2}}}\Gamma^{\frac{h}{2}}\left(\frac{s-is_p}{2}\right)\cdot\Gamma^{\frac{h}{2}}\left(\frac{s+1-is_p}{2}\right),$$

$$\prod_{p=r_0+1}^{r_1}\Gamma^{\frac{h}{2}}(s-is_p) = \frac{(\sqrt{2})^{h(r_1-r_0)s}\cdot\prod_{p=r_0+1}^{r_1}\Gamma^{\frac{h}{2}}\left(\frac{s-is_p}{2}\right)\cdot\prod_{p=r_0+1}^{r_1}\Gamma^{\frac{h}{2}}\left(\frac{s+1-is_p}{2}\right)}{(\sqrt{2})^{ih\sum_{p=r_0+1}^{r_1}s_p}2^{\frac{h}{2}(r_1-r_0)}(\sqrt{\pi})^{\frac{h}{2}(r_1-r_0)}}$$

Damit wird:

$$\mathsf{H}(s,\lambda) = C\cdot G(s,\lambda)\cdot\frac{\prod_{p=1}^{r_1}\Gamma^{\nu_p^{(1)}}\left(\frac{s-is_p}{2}\right)\cdot\prod_{p=1}^{r_1}\Gamma^{\nu_p^{(2)}}\left(\frac{s+1-is_p}{2}\right)}{\prod_{p=1}^{r_0}\Gamma^{h}\left(\frac{s-is_p}{2}\right)\cdot\prod_{p=r_0+1}^{r_1}\Gamma^{\frac{h}{2}}\left(\frac{s-is_p}{2}\right)\cdot\prod_{r_0+1}^{r_1}\Gamma^{\frac{h}{2}}\left(\frac{s+1-is_p}{2}\right)}\cdot$$
$$\cdot\sqrt{N\frac{\prod f(\chi)}{\mathfrak{D}}}^{s},$$

wenn $C = (2\sqrt{\pi})^{\frac{h}{2}(r_1-r_0)}$ gesetzt ist.

Aus der Funktionalgleichung

$$\mathsf{H}(s,\lambda) = \frac{\prod_\chi \mathsf{W}(\lambda_\chi)}{\mathsf{W}(\lambda)}\cdot\mathsf{H}(1-s,\overline{\lambda}) = \mathsf{V}(\lambda)\cdot\mathsf{H}(1-s,\overline{\lambda})$$

folgt nun, daß die Nullstellen und Pole von $\mathsf{H}(s,\lambda)$ symmetrisch zu $\sigma = \frac{1}{2}$ liegen müssen.

315 III

Nun liegen die Nullstellen und Pole, die der Faktor $G(s,\lambda)$ erzeugt, wegen der Darstellung auf S. 311 ▸ oben und $|\lambda(\mathfrak{p})| = 1$ alle auf der vertikalen Geraden $\sigma = 0$, die Nullstellen und Pole, die durch die Γ–Faktoren hereinkommen auf gewissen (durch die s_p bestimmten) horizontalen Geraden, und zwar auf diesen, weil s_p reell, entweder bei den Abszissen

$$\sigma = 0,-2,-4,\ldots \qquad (\text{Faktoren}\quad \Gamma\left(\tfrac{s-is_p}{2}\right)),$$

oder

$$\sigma = -1,-3,-5,\ldots \qquad (\text{Faktoren}\quad \Gamma\left(\tfrac{s+1-is_p}{2}\right)).$$

Damit sind alle Nullstellen und Pole erschöpft. Damit die Funktionalgleichung für $\mathsf{H}(s,\lambda)$ also überhaupt bestehen kann, müssen sämtliche dieser Nullstellen und Pole herausfallen.

Wir verfolgen dieses zuerst für die Γ–Faktoren. Es sei für den Augenblick $\lambda(x)$ ein spezieller Größencharakter, für den Strahl aller total positiven Körperzahlen betrachtet, derart, daß die zugehörigen s_p, die sich nach dem in Satz 38 (S. 131) gegebenen Ausdruck als

$$s_p = \sum_{q=1}^{r} e_p^{(q)} \left(2\pi m_q - \sum_{\kappa=1}^{n} a_\kappa \vartheta_q^{(\kappa)} \right); \qquad (p = 1, 2, \dots r+1)$$

darstellen, alle verschieden sind. Wegen der Willkürlichkeit der ganzen Zahlen m_q und des Nichtverschwindens der aus den $e_p^{(q)}$ und e_p des Strahls aller tot. pos. Zahlen gebildeten

316 III

Determinante, sind die $r+1$ Linearformen

$$\sum_{q=1}^{r} e_p^{(q)} m_q$$

der m_q linear unabhängig und können mithin die m_q als *reelle* Zahlen so bestimmt werden, daß beliebig vorgegebene reelle Werte resultieren, also bei gegebenen a_p auch die s_p beliebig vorgegebene Werte annehmen. Nimmt man diese genügend weit auseinander, so entstehen offenbar auch verschiedene s_p, wenn man die m_q durch die nächsten ganzen Zahlen ersetzt, da ja die entspr. Änderung der s_p eine von den $e_p^{(q)}$ abhängige feste Schranke nicht übersteigt.

Für ein solches λ sind dann also die „Nullstellengeraden“ $t = s_p$ alle verschieden, also müssen sich die Nullstellen *auf jeder solchen Geraden* mit den Polen auf ihr *für sich* kompensieren.

$$1.)\ p = 1, \dots, r_0$$

Dann liegen auf der Geraden $t = s_p$

a.) Pole $\nu_p^{(1)}$–ter Ordnung in $\sigma = 0, -2, -4, \dots$

b.) Pole $\nu_p^{(2)}$–ter Ordnung in $\sigma = -1, -3, -5, \dots$

c.) Nullstellen h–ter Ordnung in $\sigma = 0, -2, -4, \ldots$

Es folgt also:

$$\nu_p^{(1)} = h\,; \qquad \nu_p^{(2)} = 0.$$

2.) $p = r_0 + 1, \ldots, r_1$

Dann liegen auf der Geraden $t = s_p$

a.) Pole $\nu_p^{(1)}$–ter Ordnung in $\sigma = 0, -2, -4, \ldots$

b.) Pole $\nu_p^{(2)}$–ter Ordnung in $\sigma = -1, -3, -5, \ldots$

c.) Nullstellen $\frac{h}{2}$–ter Ordnung in $\sigma = 0, -2, -4, \ldots$

d.) Nullstellen $\frac{h}{2}$–ter Ordnung in $\sigma = -1, -3, -5, \ldots$

Es folgt also:

$$\nu_p^{(1)} = \frac{h}{2}\,; \qquad \nu_p^{(2)} = \frac{h}{2}\,.$$

Da die Zahlen $\nu_p^{(1)}, \nu_p^{(2)}$ nicht von λ, sondern nur von χ abhängen, ist somit allgemein bewiesen, daß für jedes λ in $\mathsf{H}(s, \lambda)$ die Γ–Faktoren sich vollständig herausheben:

$$\boldsymbol{\mathsf{H}(s, \lambda) = C \cdot G(s, \lambda) \sqrt{N \frac{\prod f(\chi)}{\mathfrak{D}}}^{\,s}}$$

Es müssen nun ferner aus dem gleichen Grunde wie vorher alle Nullstellen und Pole von $G(s, \lambda)$ sich kompensieren. Es war

$$G(s, \lambda) = \frac{\prod_{\mathfrak{p}|\mathfrak{F}} \left(1 - \left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^f\right)^g}{\prod_{\mathfrak{p}|\mathfrak{F}} \left(1 - \left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{f'}\right)^{g'}}\,.$$

Wir teilen die Faktoren in Zähler und Nenner zunächst nach den rationalen Primzahlen p ein, in denen die $\mathfrak{p}$ aufgehen.

Jeder Faktor des Zählers $\left(1-\left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^f\right)^g$ erzeugt eine Serie von g–fachen Nullstellen:

$$s = i\left\{\frac{\mu(\mathfrak{p})}{\log N\mathfrak{p}} + \frac{2k\pi}{\mathfrak{f}\log N\mathfrak{p}}\right\}; \qquad (k = 0, \pm 1, \pm 2, \dots)$$

wenn

$$\lambda(\mathfrak{p}) = e^{i\mu(\mathfrak{p})}$$

gesetzt wird ($|\lambda(\mathfrak{p})| = 1$, also $\mu(\mathfrak{p})$ reell). Ebenso erzeugt jeder Faktor der Nenner $\left(1-\left(\frac{\lambda(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{f'}\right)^{g'}$ eine g'fache Serie von Polen

$$s = i\left\{\frac{\mu(\mathfrak{p})}{\log N\mathfrak{p}} + \frac{2k\pi}{\mathfrak{f}'\lg N\mathfrak{p}}\right\}; \qquad (k = 0, \pm 1, \pm 2, \dots).$$

Ich zeige zunächst, daß eine von der rationalen Primzahl p herrührende solche Serie des Zählers höchstens einen Punkt mit einer von $p' \neq p$ herrührenden Serie des Nenners gemein haben kann.

Hat nämlich eine Serie, die von p' herrührt, und durch den Teiler $\mathfrak{p}'$ von p' erzeugt wird, einen Punkt mit einer von p herrührenden, durch $\mathfrak{p}$ erzeugten Serie gemein, so besteht eine Gleichung

$$\frac{\mu(\mathfrak{p})}{\log N\mathfrak{p}} + \frac{2k\pi}{\mathfrak{f}\log N\mathfrak{p}} = \frac{\mu(\mathfrak{p}')}{\log N\mathfrak{p}'} + \frac{2k'\pi}{\mathfrak{f}\log N\mathfrak{p}'};$$

Bestände nun noch eine weitere solche Gleichung mit einem von k, k' verschiedenen Paar ℓ, ℓ' ganzer Zahlen, so folgte durch Subtraktion eine Gleichung der Form

$$\frac{\log N\mathfrak{p}}{\log N\mathfrak{p}'} = q, \quad \text{d. h.} \quad \log\left(\frac{N\mathfrak{p}}{N\mathfrak{p}'^q}\right) = 0$$

wo q rational ist. Da aber $N\mathfrak{p}$ und $N\mathfrak{p}'$ verschiedene Primzahlpotenzen sind, ist dies nach dem Fundamentalsatz der Zahlentheorie unmöglich.

Die von p herrührenden Nullstellen des Zählers müssen sich also bis auf endlich viele gegen die von demselben p herrührenden Nullstellen des Nenners kompensieren.

Nunmehr betrachten wir ein p allein, und setzen

$$p = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_\nu^{a_\nu},$$

wobei wir mit $\mathfrak{f}_i, \mathfrak{f}_i', g_i, g_i'$ die $\mathfrak{p}_i$ zugeordneten Zahlen $\mathfrak{f}, \mathfrak{f}', g, g'$ bezeichnen.

Dann lösen sich die Nullstellen zu p von Zähler und Nenner je in ν Serien mit den „*Distanzen*“

$$\frac{2\pi}{\mathfrak{f}_i \log N\mathfrak{p}_i}; \qquad \frac{2\pi}{\mathfrak{f}_i' \log N\mathfrak{p}_i}; \qquad (i = 1, \dots, \nu)$$

auf. Diese Distanzen sind sämtlich untereinander kommensurabel (in rationalem Verhältnis), weil die $\log N\mathfrak{p}_i$ es untereinander sind. Durch Hinzunahme neuer Punkte können also sowohl die dem Zähler, wie die dem Nenner entsprechenden Punktserien je in eine

320 III

Serie äquidistanter Punkte mit der gemeinsamen Distanz $\frac{2\pi}{\mathsf{N} \log p}$ verwandelt werden, wo N ganz rational ist. Denn $\log p$ ist ja die einzige in allen Distanz–Nennern steckende Irrationalität.

Die so entstehenden 2ν Serien sind durch ihre 2ν Anfangsglieder

$$\frac{\mu(\mathfrak{p}_i)}{\log N\mathfrak{p}_i} \quad \text{und} \quad \frac{\mu(\mathfrak{p}_i)}{\log N\mathfrak{p}_i}; \qquad (i = 1, 2, \dots \nu)$$

bestimmt und wir wissen, daß sich unendlich viele Punkte jeder Zähler–Serie gegen Punkte des Nenners wegheben müssen.

Wenn es uns gelingt, ein spezielles λ so anzugeben, daß etwa das ihm entsprechende Anfangsglied $\frac{\mu(\mathfrak{p}_1)}{\log N\mathfrak{p}_1} \mod \frac{2\pi}{\mathsf{N} \log p}$ von allen übrigen Anfangsgliedern $\frac{\mu(\mathfrak{p}_i)}{\log N\mathfrak{p}_i}$ verschieden ist, so haben für dieses λ die $i = 2, \dots \nu$ entsprechenden (erweiterten) Serien des Nenners keinen Punkt mit der $i = 1$ entsprechenden (erweiterten) Serie des Zählers gemeinsam*, umso mehr also nicht die ursprünglichen Serien. Das Herausheben muß dann also so erfolgen, daß die $\mathfrak{p}_1$–Serie des Zählers und dieselbe $\mathfrak{p}_1$–Serie des Nenners sich (bis auf endlich viele Punkte) kompensieren.

321 III

*u. a. umgekehrt unter Vert. von Zähler u. Nenner

Das kann nur so sein, daß beide Serien total identisch sind (als *volle* äquidistante Punktserien). Es müssen daher sowohl die Distanzen gleich sein, also $\mathfrak{f}_1 = \mathfrak{f}_1'$ als auch die Ordnungen $g_1 = g_1'$.

Analog schließt man natürlich für $i = 2, \ldots, \nu$.

□□□

Es bleibt also zu zeigen, daß der Größencharakter λ so gewählt werden darf, daß

$$\frac{\mu(\mathfrak{p}_1)}{\log N\mathfrak{p}_1} \not\equiv \frac{\mu(\mathfrak{p}_i)}{\log N\mathfrak{p}_i} \mod \frac{2\pi}{\mathsf{N}\log p} \qquad (\text{für} \quad i = 2, \ldots, \nu)$$

ist, wenn $\lambda(x) = e^{i\mu(x)}$ gesetzt ist. λ ist dabei nach S. 305 als Größencharakter für den Strahl *aller* Körperzahlen zu wählen. Es genügt aber, nur einen Größencharakter λ für den Strahl der *total positiven* Körperzahlen mit diesen Eigenschaften anzugeben; denn hat man einen

322 III

solchen, so definieren die Werte ± 1, die er für die Körpereinheiten annimmt, einen gewissen Vorzeichencharakter für diejenige Untergruppe der Signaturen, die durch Einheiten repräsentiert werden. Dieser läßt sich dann (im allgemeinen noch in mehrfacher Art) zu einem Vorzeichencharakter für alle Signaturen erweitern, der $v(x)$ heißen möge. Dann erfüllt $\lambda(x)v(x)$ die Definitionsgleichungen eines Größencharakters für den Strahl *aller* Körperzahlen (Größencharakter für Ideale schlechthin). □□□

Die $\lambda(\mathfrak{p}_i)$ ändern sich dabei nur um Einheitswurzeln, die $\mu(\mathfrak{p}_i)$ also um rationale Vielfache von 2π. Wir werden aber beweisen, daß die obigen Inkongruenzen für die $\mu(\mathfrak{p}_i)$ sich sogar im Sinne der *Irrationalität* der entsprechenden Differenzen mod 2π befriedigen lassen, sodaß die Anfügung von $v(x)$ an ihrem Bestehen nichts ändert.

Wir haben zur Konstruktion von $\lambda(x)$ zu berücksichtigen, daß die obige ganze Zahl N ein gemeinsames Multiplum aller $f_i F_i$, $f_i' F_i$ ist, wenn F_i den absoluten Grad von $\mathfrak{p}_i$ bezeichnet (und als kleinstes gemeinsames Vielfache gewählt werden darf, was aber nicht wesentlich!). Daher sind die Quotienten $\frac{\mathsf{N}\log p}{\log N\mathfrak{p}_i} = \frac{\mathsf{N}\log p}{F_i \log p} = \frac{\mathsf{N}}{F_i} = n_i$ ganze Zahlen und es ist wegen $n_i F_i = \mathsf{N}$ für $i = 1, 2, \ldots, \nu$

$$N\mathfrak{p}_1^{n_1} = N\mathfrak{p}_2^{n_2} = \cdots = N\mathfrak{p}_\nu^{n_\nu}.$$

Die obigen Inkongruenzen gehen über in die gleichwertigen

$$n_1\mu(\mathfrak{p}_1) \not\equiv n_i\mu(\mathfrak{p}_i) \mod 2\pi\,; \qquad (i = 2, \ldots \nu)$$

wo n_i die eben definierten ganzen Zahlen bedeutet. Wir werden zeigen, daß ein solches $\lambda(x) = e^{i\mu(x)}$ existiert, daß diese sämtlichen Inkongruenzen *im Sinne der Irrationalität* mod 2π bestehen.

Dazu bezeichnen wir mit $\mu_1, \ldots, \mu_{n-1}$ in irgendeiner Reihenfolge die Exponenten der $n-1$ Grundcharaktere $\lambda_1, \ldots, \lambda_{n-1}$ für den Strahl aller total positiven Körperzahlen. Es gibt zunächst sicher ein μ_1, sodaß

$$n_1\mu_1(\mathfrak{p}_1) \not\equiv n_2\mu_1(\mathfrak{p}_2) \mod 2\pi,$$

wo $\not\equiv$ das Zeichen für die Irrationalität der Differenz beider Seiten mod 2π ist. Wäre nämlich für alle μ_i

$$n_1\mu_i(\mathfrak{p}_1) \equiv n_2\mu_i(\mathfrak{p}_2) \mod \frac{2\pi}{K},$$

wo K hinreichend groß ist, so folgte $Kn_1\mu_i(\mathfrak{p}_1) \equiv Kn_2\mu_i(\mathfrak{p}_2) \mod 2\pi$, also $\lambda_i(\mathfrak{p}_1^{n_1})^K = \lambda_i(\mathfrak{p}_2^{n_2})^K$. Wegen $N(\mathfrak{p}_1^{n_1}) = N(\mathfrak{p}_2^{n_2})$ wären also die Bedingungen

für das Übereinstimmen der Argumente von λ sämtlich erfüllt, und es folgte zunächst für die zugeordneten idealen Zahlen:

$$\widehat{\pi}_1^{n_1K} = \widehat{\pi}_2^{n_2K} \cdot \eta \qquad (\eta \quad \text{Strahleinheit})$$

also

$$\mathfrak{p}_1^{n_1K} = \mathfrak{p}_2^{n_2K}; \qquad \mathfrak{p}_1 = \mathfrak{p}_2$$

während doch $\mathfrak{p}_1, \mathfrak{p}_2$ verschieden sein sollten.

Es kann nun sein, daß auch schon die weitere Forderung

$$n_1\mu_1(\mathfrak{p}_1) \not\equiv n_3\mu_1(\mathfrak{p}_3) \mod 2\pi$$

für μ_1 erfüllt ist. Dann behalten wir μ_1 bei. Ist aber

$$n_1\mu_1(\mathfrak{p}_1) \equiv n_3\mu_1(\mathfrak{p}_3) \mod \frac{2\pi}{K},$$

so bilden wir durch lineare Kombination ein neues μ_1'. Es gibt nämlich sicher ein μ_2, sodaß

$$n_1\mu_2(\mathfrak{p}_1) \not\equiv n_3\mu_2(\mathfrak{p}_3) \mod 2\pi$$

ist. Wir bilden dann mit ganzem m_2

$$\mu_1'(x) = \mu_1(x) + m_2\mu_2(x).$$

Hierbei wählen wir m_2 ganzzahlig so, daß gleichzeitig

$$n_1[\mu_1(\mathfrak{p}_1) + m_2\mu_2(\mathfrak{p}_1)] \not\equiv \left\{ \begin{array}{c} n_2[\mu_1(\mathfrak{p}_2) + m_2\mu_2(\mathfrak{p}_2)] \\ n_3[\mu_1(\mathfrak{p}_3) + m_2\mu_2(\mathfrak{p}_3)] \end{array} \right\} \mod 2\pi$$

wird. Das letztere ist sicher richtig, wenn nur $m_2 \neq 0$ genommen wird, weil nach Annahme $n_1\mu_1(\mathfrak{p}_1) - n_3\mu_1(\mathfrak{p}_3)$ rational mod 2π, dagegen $n_1\mu_2(\mathfrak{p}_1) - n_3\mu_2(\mathfrak{p}_3)$ irrational. Das erstere läßt sich ebenfalls durch $m_2 \neq 0$ gleichzeitig erfüllen, denn schreibt man es in der Form

$$m_2[n_1\mu_2(\mathfrak{p}_1) - n_2\mu_2(\mathfrak{p}_2)] \not\equiv n_2\mu_1(\mathfrak{p}_2) - n_1\mu_1(\mathfrak{p}_1) \mod 2\pi,$$

□□□

so ist für rationale [ ] m_2 ganz beliebig, da die rechte Seite irrational ist, für irrationale [ ] muß aber ebenfalls für alle m_2 bis auf höchstens eins die Bedingung erfüllt sein, da aus zwei verschiedenen m_2 die Rationalität beider Irrationalitäten[4] folgen würde.

Nunmehr haben wir in $\mu_1'(x)$ schon die Bedingungen für $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ füllt und prüfen jetzt weiter, ob auch diejenige für $\mathfrak{p}_4$:

$$n_1\mu_1'(\mathfrak{p}_1) \not\equiv n_4\mu_1'(\mathfrak{p}_4) \mod 2\pi$$

besteht. Ist dies der Fall, so setzen wir $\mu_1' = \mu_1''$. Sonst wählen wir wieder ein μ_3, das die Bedingung bezüglich $\mathfrak{p}_1$ allein erfüllt und setzen

$$\mu_1'' = \mu_1' + m_3\mu_3$$

m_3 ist so zu bestimmen, daß einmal die Bedingung für $\mathfrak{p}_4$ erhalten bleibt, wozu wieder $m_3 \neq 0$ genügt. Zweitens aber die für $\mathfrak{p}_2, \mathfrak{p}_3$ bestehen, also

$$n_1[\mu_1'(\mathfrak{p}_1) + m_3\mu_3(\mathfrak{p}_1)] \not\equiv \left\{ \begin{array}{c} n_2[\mu_1'(\mathfrak{p}_2) + m_3\mu_3(\mathfrak{p}_2)] \\ n_3[\mu_1'(\mathfrak{p}_3) + m_3\mu_3(\mathfrak{p}_3)] \end{array} \right\} \mod 2\pi$$

Ist dabei $n_1\mu_3(\mathfrak{p}_1) - n_i\mu_3(\mathfrak{p}_i)$ rational, so genügt jedes m_3; für irrationale Werte eines dieser beiden Ausdrücke ist jedesmal höchstens ein m_3 auszuschließen. Daher existiert ein m_3, wie wir es suchen.

[4] undeutlich

So fahren wir fort. Wenn wir bis zu

$$\mu_1^{(n-2)}(x) = \mu_1(x) + m_2\mu_2(x) + \cdots + m_{n-1}\mu_{n-1}(x)$$

gelangt sind, sind die Bedingungen gerade bis $\mathfrak{p}_n$ erfüllt, und da n das größtmögliche ν ist, ist das Verfahren stets ausführbar. Der resultierende Charakter

$$\lambda^{n-2}(x) = \lambda_1\lambda_2^{m_2} \dots \lambda_{n-1}^{m_{n-1}}$$

erfüllt dann die gestellten Bedingungen. Die $\lambda_1, \dots, \lambda_{n-1}$ sind dabei nicht notwendig verschieden. Schlimmstenfalls braucht man sie aber tatsächlich alle und auch die Tatsache, daß $n-1$ Grundcharaktere vorhanden sind.

Bemerkung zu S. 149 unten.

Um aus $N(\prod_\chi f_\chi) = N(\vartheta)$ auf $\prod_\chi f_\chi = \vartheta$ schließen zu können, brauchen wir noch die Relation

$$\prod_\chi L(s, \lambda_\chi) = L_K(s, \Lambda)$$

von S. 311. Aus d. a. S. 313 aufgestellten Funktionalgleichung

$$\mathsf{H}(s, \lambda) = \frac{\prod_\chi W(\lambda_\chi)}{W(\Lambda)} \mathsf{H}(1-s, \overline{\lambda})$$

und der a. S. 317 festgestellten Relation

$$\mathsf{H}(s, \lambda) = C = (2\sqrt{\pi})^{\frac{h}{2}\cdot(r_1-r_0)} \qquad (C, \text{ S. } 319 \text{ u.}),$$

bei der wir schon $G(s, \lambda) = 1$ und $N(\prod f_\chi) = N(\vartheta)$ berücksichtigt haben, folgt, weil C reell ist, daß

$$\prod_\chi W(\lambda_\chi) = W(\Lambda)$$

(denn $\mathsf{H}(s, \overline{\lambda}) = \mathsf{H}(s, \lambda)$)

(weil C von λ unabhängig)

Wenn man nun $\prod_{\chi} W(\lambda_\chi)$ und $W(\Lambda)$ ausrechnet, so findet man, weil

$$\prod_{\chi} W(\chi) = 1$$

schon früher festgestellt war, leicht, daß

$$\lambda(\vartheta) = \lambda(\prod_{\chi} f_\chi)$$

für alle in Frage kommenden λ gilt. Nach Satz 7 (S. 18) ergibt sich daraus

$$\vartheta = \prod_{\chi} f_\chi \,.$$

Kapitel 4

Existenzsatz/Strahlklassenkörper

Überblick

4.1 §1 Die Geschlechter im relativ–zyklischen Körper von Primzahlgrad ℓ

1 IV

A. Allgemeine Sätze

Satz 1. Ist K relativ–zyklisch vom Primzahlpotenzgrad ℓ^ν zu k und geht ein zu ℓ primes Primideal $\mathfrak{p}$ von k in der Relativdiskriminante des in K enthaltenen zyklischen Körpers vom Grade ℓ in Bezug auf k auf, so ist die Relativdiskriminante von K nach k genau durch

$$\mathfrak{D}_\mathfrak{p} = \mathfrak{p}^{\ell^\nu - 1}$$

teilbar. Ferner gilt

$$\mathfrak{p} = \mathfrak{P}^{\ell^\nu}; \qquad \text{(Grad 1)}$$

und $N\mathfrak{p} \equiv 1 \bmod \ell^\nu$.

Beweis. 1.) Da die zyklische Gruppe vom Grade ℓ^ν nur eine Untergruppe vom Grade ℓ, nämlich die zyklische, hat, gibt es einen eindeutig bestimmten Zwischenkörper K_ℓ vom Relativgrad ℓ über k. Geht $\mathfrak{p}$ in der Relativdiskriminante von K_ℓ auf, so gilt in K_ℓ:

$$\mathfrak{p} = \mathfrak{P}_\ell^\ell; \qquad \text{(Grad 1).}$$

2.) Für den Zerlegungskörper eines Primfaktors $\mathfrak{P}$ von $\mathfrak{p}$

2 IV

in K kommen nur die ineinandergeschachtelten (relativ–zyklischen) Körper $k, K_\ell, K_{\ell^2}, \ldots, K_{\ell^\nu} = K$ in Frage. Da aber $\mathfrak{p}$ schon in K_ℓ nicht mehr in verschiedene Primideale ersten Grades zerfällt, ist nach A.Z. I, S. 51, Satz 23 der Zerlegungskörper k selbst, die Zerlegungsgruppe also die volle zyklische Gruppe vom Grade ℓ^ν, und somit

$$\mathfrak{p} = \mathfrak{P}^{\ell^\nu}; \qquad \text{(Grad 1)} \quad \square\square\square$$

3.) Da der Relativgrad von $\mathfrak{P}$ gleich 1 ist, ist der Trägheitskörper mit dem Zerlegungskörper identisch, also ebenfalls k, der erste Verzweigungskörper

ist vom Grade ℓ^ν über dem Trägheitskörper, also über k, weil ℓ^ν die größte in der Ordnung ℓ^ν von $\mathfrak{P}$ enthaltene, zu p prime Zahl ist; also ist der erste Verzweigungskörper K, also da keine höheren Verzweigungskörper existieren,

$$\mathfrak{D}_\mathfrak{p} = \mathfrak{p}^{\ell^\nu - 1}.$$

Ferner ist nach A.Z. I, S. 43, Def. $6 \overset{a}{=} \ell^\nu$ ein Teiler von $N\mathfrak{p} - 1$. Damit ist Satz 1 bewiesen.

Satz 2. Es sei K relativ–zyklisch vom Primzahlgrad ℓ über k und $\mathfrak{l}$ ein in der Relativdiskriminante von K aufgehendes Primideal von ℓ in k, also

$$\mathfrak{l} = \mathfrak{L}^\ell; \qquad \text{(Grad 1)}$$

in K. $\mathfrak{l}$ habe die Ordnung e und v sei die größte ganze Zahl, sodaß für jedes für $\mathfrak{L}$ ganze A aus K gilt

$$\sigma\mathsf{A} \equiv \mathsf{A} \mod \mathfrak{L}^{v+1}.$$

(σ erzeugende Substitution von K).

3 IV

Dann gilt für die Relativdiskriminante

$$\mathfrak{D}_\mathfrak{l} = \mathfrak{l}^{(v+1)(\ell-1)}.$$

Ist ferner Λ Primzahl zu $\mathfrak{L}$ aus K, so ist $\sigma\Lambda - \Lambda$ genau durch $\mathfrak{L}^{v+1}$ teilbar. Die Zahl v genügt der Ungleichung

$$1 \leqq v \leqq \frac{e\ell}{\ell - 1}$$

und ist dann und nur dann durch ℓ teilbar, wenn

$$v = \frac{e\ell}{\ell - 1}$$

also speziell auch e durch $\ell - 1$ teilbar ist.

Beweis. 1.) Wenn für ein w die Kongruenz

$$\sigma\mathsf{A} \equiv \mathsf{A} \mod \mathfrak{L}^{w+1}$$

für jedes für $\mathfrak{L}$ ganze A aus K gilt, gehört σ und folglich die ganze zyklische Gruppe $1, \sigma, \ldots, \sigma^{\ell-1}$ zur w–ten Verzweigungsgruppe, und umgekehrt. Es gibt demnach genau v Verzweigungsgruppen, die gleich der ganzen zyklischen Gruppe sind, während alle weiteren notwendig 1 werden. Nach A.Z. I, S. 49 ist also die Relativdiskriminante

$$\mathfrak{D}_{\mathfrak{l}} = \mathfrak{l}^{(v+1)(\ell-1)}$$

Da die Ordnung von $\mathfrak{L}$ durch ℓ teilbar ist, ist der Grad der ersten Verzweigungsgruppe ℓ, daher

$$v \geqq 1.$$

2.) Sei Λ Primzahl für $\mathfrak{L}$ und $\sigma\Lambda - \Lambda \equiv 0 \bmod \mathfrak{L}^{v+2}$. Da $\mathfrak{L}$ den Relativgrad 1 hat, läßt sich jedes für $\mathfrak{L}$ ganze A aus K nach Potenzen von Λ mit Koeffizienten aus

k in der Form

$$\mathsf{A} \equiv \alpha_0 + \alpha_1\Lambda + \alpha_2\Lambda^2 + \cdots + \alpha_{v+1}\Lambda^{v+1} \mod \mathfrak{L}^{v+2}$$

entwickeln. Dann ist

$$\sigma\mathsf{A} \equiv \alpha_0 + \alpha_1\sigma\Lambda + \alpha_2\sigma\Lambda^2 + \cdots + \alpha_{v+1}\sigma\Lambda^{v+1} \mod \mathfrak{L}^{v+2},$$

weil $\sigma\mathfrak{L} = \mathfrak{L}$. Da $\sigma\Lambda^i - \Lambda^i$ teilbar durch $\sigma\Lambda - \Lambda$ ist, ist also

$$\begin{aligned}\sigma\mathsf{A} - \mathsf{A} &\equiv X + \alpha_1(\sigma\Lambda - \Lambda) + \cdots + \alpha_{v+1}(\sigma\Lambda^{v+1} - \Lambda^{v+1}) \mod \mathfrak{L}^{v+2} \\ &\equiv 0 \mod \mathfrak{L}^{v+2},\end{aligned}$$

entgegen der Bestimmung von v. Andererseits muß sicher $\sigma\Lambda - \Lambda$ durch $\mathfrak{L}^{v+1}$ teilbar sein. Also ist es *genau* durch diese Potenz teilbar.

3.) Sei Λ_a genau durch $\mathfrak{L}^a$ teilbar ($a \geqq 1$) und

$$\Lambda_a = \Lambda^a\mathsf{E} \ (\mathfrak{L})$$

wo E Einheit aus $K(\mathfrak{L})$ ist. (Dann ist

$$\sigma\Lambda_a - \Lambda_a = \mathsf{E}(\sigma\Lambda^a - \Lambda^a) + (\sigma\mathsf{E} - \mathsf{E})\sigma\Lambda^a \ (\mathfrak{L}). \tag{1}$$

Nun ist für $a \geqq 2$

$$\begin{aligned}(\sigma\Lambda^a - \Lambda^a) &= [(\sigma\Lambda - \Lambda) + \Lambda]^a - \Lambda^a \\ &= \sum_{\nu=0}^{a-1} \binom{a}{\nu} (\sigma\Lambda - \Lambda)^{a-\nu}\Lambda^\nu\end{aligned}$$

Hier ist das allgemeine Glied mindestens durch $\mathfrak{L}^{(v+1)(a-\nu)+\nu}$, also wenn $0 \leqq \nu \leqq a-2$ mindestens durch $\mathfrak{L}^{2v+a}$ teilbar, während das letzte Glied ($\nu = a-1$)

a.) für $a \not\equiv 0 \bmod \ell$ genau durch $\mathfrak{L}^{v+a}$
b.) || $a \equiv 0 \bmod \ell$ durch mehr als $\mathfrak{L}^{v+a}$

teilbar ist. Also gilt:

5 IV

a.) für $a \not\equiv 0 \bmod \ell$: $\sigma\Lambda^a - \Lambda^a$ genau durch $\mathfrak{L}^{v+a}$ teilbar,
b.) || $a \equiv 0 \bmod \ell$: $\sigma\Lambda^a - \Lambda^a$ durch mehr als $\mathfrak{L}^{v+a}$ || .

Das zweite Glied rechts in (1) ist mindestens durch $\mathfrak{L}^{v+1+a}$ teilbar und daher

a.) für $a \not\equiv 0 \bmod \ell$: $\sigma\Lambda_a - \Lambda_a$ genau durch $\mathfrak{L}^{v+a}$ teilbar,
b.) || $a \equiv 0 \bmod \ell$: $\sigma\Lambda_a - \Lambda_a$ durch mehr als $\mathfrak{L}^{v+a}$ || .

und dies gilt ersichtlich auch für $a = 1$.)

Einfacher sieht man dies *nach Hensel* so ein:

Es ist

$$\frac{\sigma\Lambda_a}{\Lambda_a} = \left(\frac{\sigma\Lambda}{\Lambda}\right)^a \frac{\sigma\mathsf{E}}{\mathsf{E}} \ (\mathfrak{L})$$

also da nach dem vorhergehenden

$$\begin{aligned}\tfrac{\sigma\Lambda}{\Lambda} &= 1 + \gamma\Lambda^v + \cdots \quad (\mathfrak{L}) \ ; \quad \left(\begin{smallmatrix}\gamma \text{ aus } k \\ \gamma \text{ prim zu } \mathfrak{l}\end{smallmatrix}\right) \\ \tfrac{\sigma\mathsf{E}}{\mathsf{E}} &= 1 + \delta\Lambda^{v+1} + \cdots \quad (\mathfrak{L}) \ ; \quad (\delta \text{ aus } k)\end{aligned}$$

ist,

a.) für $a \not\equiv 0 \bmod \ell$ $\frac{\sigma\Lambda_a}{\Lambda_a}$ Einseinheit genau vom Grad v,
b.) für $a \equiv 0 \bmod \ell$ $\frac{\sigma\Lambda_a}{\Lambda_a}$ Einseinheit von höherem Grad als v,

was mit obigem identisch.

Ich benutze nun die symbolische Identität:

$$s(\Lambda) = (1 + \sigma + \cdots + \sigma^{\ell-1})\Lambda = (\ell + \binom{\ell}{2}(\sigma - 1) + \cdots + (\sigma - 1)^{\ell-1})\Lambda$$

wo s die Relativspur und σ die erzeugende Substitution von K nach k bezeichnet. Nach dem obigen, angewendet sukzessive für $\Lambda_a = \Lambda$, $(\sigma - 1)\Lambda$, $(\sigma - 1)^2\Lambda$, ...

6 IV

ist nun $(\sigma - 1)^i\Lambda$ genau durch $\square\square\square$ $\mathfrak{L}^{1+iv}$ teilbar, wenn keine der Zahlen $1, 1 + v, 1 + 2v, \ldots, 1 + (i - 1)v$ durch ℓ teilbar ist, sonst durch eine höhere Potenz, speziell also $(\sigma - 1)^{\ell-1}\Lambda$ genau durch $\mathfrak{L}^{1+(\ell-1)v}$ teilbar, wenn keine der Zahlen $1, 1+v, \ldots, 1+(\ell-2)v$ durch ℓ teilbar ist, sonst durch eine höhere Potenz. Nun sieht man sofort, daß für

$$v \equiv 0, 1 \mod \ell$$

keine der genannten Zahlen durch ℓ teilbar ist, sonst sicher eine und nur eine.

a.) $v \not\equiv 0, 1 \bmod \ell$.

Dann ist also $(\sigma - 1)^{\ell-1}\Lambda \equiv 0 \bmod \mathfrak{L}^{1+(\ell-1)v+1}$. Das erste Glied in der Darstellung von $s(\Lambda)$ ist genau durch $\mathfrak{L}^{e\ell+1}$ teilbar, kann also, da $s(\Lambda)$ in k liegt nicht das niedrigste Glied sein. Alle mittleren Glieder sind von höherer Ordnung, also folgt

$$e\ell + 1 \geqq 1 + (\ell - 1)v + 1 > (\ell - 1)v + 1$$

d.h.

$$v < \frac{e\ell}{\ell - 1}\,.$$

b.) $v \equiv 1 \bmod \ell$.

Dann hat das letzte Glied in $s(\Lambda)$ genau die Ordnungszahl $1 + (\ell - 1)v$ und wie unter a.) muß

$$e\ell + 1 \geqq 1 + (\ell - 1)v$$

sein. Das Gleichheitszeichen kann jedoch nicht gelten, da hier

$$1 + (\ell - 1)v \equiv 0 \mod \ell$$

ist. Demnach gilt auch hier

$$v < \frac{e\ell}{\ell - 1}\,.$$

7 IV

c.) $v \equiv 0 \bmod \ell$.

Dann hat wieder das letzte Glied genau die Ordnungszahl $1 + (\ell - 1)v \equiv 1 \bmod \ell$, und wie unter a.) muß

$$e\ell + 1 \geqq 1 + (\ell - 1)v$$

sein. Hier *muß* aber das Gleichheitszeichen gelten, da sonst die Ordnungszahl von $s(\Lambda)$ genau $1 + (\ell - 1)v \equiv 1 \bmod \ell$ wäre. Also ist hier

$$v = \frac{e\ell}{\ell - 1}$$

und somit auch sicher $e \equiv 0 \bmod \ell - 1$.

Damit ist Satz 2 vollständig bewiesen.

Ich verallgemeinere jetzt die Resultate von Satz 2 auf beliebige relativ–zyklische Oberkörper von Primzahlpotenzgrad.

Sei zunächst K_2 relativ–zyklisch zu k vom Grade ℓ^2 und K_1 der zyklische Unterkörper vom Grade ℓ. $\mathfrak{l}$ sei ein Teiler von ℓ der in der Relativdiskriminante von K_1 auf, also

$$\mathfrak{l} = \mathfrak{L}_1^{\ell}; \qquad \text{(Grad 1)}$$

in K_1. Der Zerlegungskörper von $\mathfrak{l}$ in K_2 ist dann, wie S. 2 oben k selbst, also

$$\mathfrak{l} = \mathfrak{L}_2^{\ell^2}; \qquad \text{(Grad 1)}$$

in K_2 und

$$\mathfrak{L}_1 = \mathfrak{L}_2^{\ell}; \qquad \text{(Grad 1)}$$

von K_1 zu K_2.

Es sei nun v die in Satz 2 definierte Zahl von K_1 nach k, v_1 die von K_2 nach K_1. Sind dann $\mathfrak{D}_{20}, \mathfrak{D}_{10}, \mathfrak{D}_{21}$ die auf $\mathfrak{l}$ bezüglichen Teile der Relativdiskriminanten,

8 IV

so ist:

$$\mathfrak{D}_{21} = \mathfrak{L}_1^{(v_1+1)(\ell-1)}$$

also die Relativnorm nach k:

$$n_{10}(\mathfrak{D}_{21}) = \mathfrak{l}^{(v_1+1)(\ell-1)},$$

ferner

$$\mathfrak{D}_{10} = \mathfrak{l}^{(v+1)(\ell-1)},$$

also nach dem bekannten Diskriminantensatz:

$$\mathfrak{D}_{20} = \mathfrak{D}_{10}^{\ell} n_{10}(\mathfrak{D}_{21}) = \mathfrak{l}^{(v+1)\ell(\ell-1)+(v_1+1)(\ell-1)}.$$

v_1 ist die Anzahl der von 1 verschiedenen Verzweigungsgruppen von K_2 nach K_1. Diese sind bekanntlich die Durchschnitte der zu K_1 gehörigen Untergruppe mit den Verzweigungsgruppen von K_2 nach k. Da K_1 zur zyklischen Gruppe vom Grade ℓ gehört, und als Verzweigungsgruppen von K_2 nach k nur die zyklischen Gruppen vom Grade ℓ^2, ℓ, 1 in Frage kommen, wird ein solcher Durchschnitt dann und nur dann von 1 verschieden sein, wenn die entsprechende Verzweigungsgruppe von K_2 nach k es ist. Also ist v_1 auch die Anzahl der von 1 verschiedenen Verzweigungsgruppen von K_2 nach k. Unter diesen seien w vom Grade ℓ^2, also $v_1 - w$ vom Grade ℓ. Dann ist nach dem allgemeinen Satz

$$\mathfrak{D}_{20} = \mathfrak{l}^{\ell^2-1+w(\ell^2-1)+(v_1-w)(\ell-1)}$$

Es ist also

$$(v+1)\ell(\ell-1) + (v_1+1)(\ell-1) = (w+1)(\ell^2-1) + (v_1-w)(\ell-1)$$

oder

$$(v+1)\ell + (v_1+1) = (w+1)(\ell+1) + (v_1-w)$$

d.h.

$$v = w$$

9 IV

Es gibt also genau v Verzweigungsgruppen von K_2 nach k vom Grade ℓ^2 und $v_1 - v$ vom Grade ℓ, d.h. wenn σ die erzeugende Substitution von K_2 nach k ist, ist $v+1$ die größte Zahl, sodaß für jedes für $\mathfrak{L}_2$ ganze A aus K_2 gilt:

$$\sigma\mathsf{A} \equiv \mathsf{A} \mod \mathfrak{L}_2^{v+1},$$

und weil σ^ℓ die erzeugende Substitution von K_2 nach K_1 ist, v_1+1 die größte Zahl, sodaß für jedes solche A aus K_2 gilt:

$$\sigma^\ell\mathsf{A} \equiv \mathsf{A} \mod \mathfrak{L}_2^{v_1+1}.$$

Nun folgt, ähnlich wie oben, wenn Λ_a genau durch $\mathfrak{L}_2^a$ teilbar ist, Λ genau durch $\mathfrak{L}_2$, und

$$\Lambda_a = \Lambda^a\mathsf{E}\ (\mathfrak{L}_2); \qquad (\mathsf{E} \text{ Einheit aus } K_2)$$

gesetzt wird:

$$\frac{\sigma\Lambda_a}{\Lambda_a} = \left(\frac{\sigma\Lambda}{\Lambda}\right)^a \frac{\sigma\mathsf{E}}{\mathsf{E}}\ (\mathfrak{L}_2)$$

und da $\frac{\sigma\Lambda}{\Lambda}$ Einseinheit mindestens vom Grade v, $\frac{\sigma\mathsf{E}}{\mathsf{E}}$ vom Grade $v+1$ ist, daß $\frac{\sigma\Lambda_a}{\Lambda_a}$ Einseinheit mindestens vom Grade v, also

$$\sigma\Lambda_a - \Lambda_a \equiv 0 \bmod \mathfrak{L}_2^{v+a}$$

ist. Daher ist für jedes für $\mathfrak{L}_2$ ganze A aus K_2:

$$\begin{aligned}
(\sigma-1)\mathsf{A} &\equiv 0 \bmod \mathfrak{L}_2^{v+1}\\
(\sigma-1)^2\mathsf{A} &\equiv 0 \bmod \mathfrak{L}_2^{2v+1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
(\sigma-1)^\ell\mathsf{A} &\equiv 0 \bmod \mathfrak{L}_2^{\ell v+1}
\end{aligned}$$

Wegen $\sigma^\ell - 1 = \big((\sigma-1)+1\big)^\ell = (\sigma-1)^\ell + \binom{\ell}{1}(\sigma-1)^{\ell-1} + \cdots + \binom{\ell}{\ell-1}(\sigma-1)$ ist also:

$$\sigma^\ell\mathsf{A} - \mathsf{A} = (\sigma-1)^\ell\mathsf{A} + \binom{\ell}{1}(\sigma-1)^{\ell-1}\mathsf{A} + \cdots + \binom{\ell}{\ell-1}(\sigma-1)\mathsf{A}$$

Hier hat jedes Glied in $\mathfrak{L}_2$ eine höhere Ordnungszahl als $v+1$, sodaß für jedes für L_2 ganze A aus K_2 gilt

$$\sigma^\ell \mathsf{A} - \mathsf{A} \equiv 0 \mod \mathfrak{L}_2^{v+1+1},$$

es ist also sicher

$$v_1 > v,$$

sodaß tatsächlich Verzweigungsgruppen vom Grade ℓ existieren.

Nunmehr läßt sich leicht durch Induktion folgender Satz herleiten:

Satz 3. Sei K_ν ein relativ zyklischer Körper vom Primzahlpotenzgrad ℓ^ν über k und K_μ für $\mu = 1, 2, \ldots, \nu-1$ der Unterkörper vom Grade ℓ^μ. Der Primteiler $\mathfrak{l}$ von ℓ in k gehe in der Relativdiskriminante von K_1 auf. Dann gilt:

$$\mathfrak{l} = \mathfrak{L}_\mu^{\ell^\mu}; \qquad \text{(Grad 1)}$$

in K_μ. Bezeichnet v_μ die Anzahl der von 1 verschiedenen Verzweigungsgruppen von $K_{\mu+1}$ nach K_μ, so gilt:

$$1 \leqq v < v_1 < v_2 < \cdots < v_{\nu-1} \leqq \frac{e\ell^\nu}{\ell - 1}$$

wo e die Ordnung von $\mathfrak{l}$, und die Relativdiskriminante von K_ν nach k ist

$$\begin{aligned}\mathfrak{D}_\mathfrak{l} &= \mathfrak{l}^{\ell^{\nu-1}(v+1)(\ell-1)+\ell^{\nu-2}(v_1+1)(\ell-1)+\cdots+(v_{\nu-1}+1)(\ell-1)} \\ &= \mathfrak{l}^{(\ell^\nu-1)+(\ell-1)[v\ell^{\nu-1}+v_1\ell^{\nu-2}+\cdots+v_{\nu-1}]}\end{aligned}$$

Beweis. 1.) Die angegebenen Zerlegungen von $\mathfrak{l}$ in den K_μ folgen wie oben einfach daraus, daß k selbst Zerlegungskörper für alle K_μ ist.

2.) Die Ungleichung $1 \leqq v < v_1 < v_2 < \cdots < v_{\nu-1}$ ist nach

dem ausgeführten klar. Denn v_2 hat in Bezug auf K_1 als Grundkörper dieselbe Bedeutung, wie v_1 in Bezug auf k, etz... Es ist ferner, wenn $K_{\nu-1}$ als Grundkörper gedacht wird,

$$v_{\nu-1} \leqq \frac{e\ell^{\nu-1} \cdot \ell}{\ell - 1} = \frac{e\ell^\nu}{\ell - 1}$$

3.) Für die auf $\mathfrak{l}$ bezügliche Relativdiskriminante ergibt sich

$$\mathfrak{D}_\mathfrak{l} = \mathfrak{D}_{\nu 0} = \mathfrak{D}_{\nu-1,0}^\ell n_{\nu-1,0}(\mathfrak{D}_{\nu,\nu-1}).$$

Nun ist die angegebene Formel nach S. 8 richtig für $\nu = 1, 2$. Sei sie richtig bis $\nu - 1$ ($\nu \geqq 2$), dann ist

$$\mathfrak{D}^{\ell}_{\nu-1,0} = \mathfrak{l}^{\ell^{\nu-1}(v+1)(\ell-1)+\ell^{\nu-2}(v_1+1)(\ell-1)+\cdots+\ell(v_{\nu-2}+1)(\ell-1)}$$

ferner $$\mathfrak{D}_{\nu,\nu-1} = \mathfrak{L}_{\nu-1}^{(v_{\nu-1}+1)(\ell-1)}$$ also

$$n_{\nu-1,0}(\mathfrak{D}_{\nu,\nu-1}) = \mathfrak{l}^{(v_{\nu-1}+1)(\ell-1)}$$

woraus die Richtigkeit für ν unmittelbar folgt.

Damit ist Satz 3 bewiesen.

Auf Grund von Satz 1, 2 gilt speziell:

Satz 4. Die Relativdiskriminante eines relativ–zyklischen Körpers vom Primzahlgrad ℓ hat die Form:

$$\mathfrak{D} = \mathfrak{f}^{\ell-1},$$

wo $$\mathfrak{f} = \prod \mathfrak{p} \cdot \prod \mathfrak{l}^{v+1}$$

ist und $\mathfrak{p}$ die zu ℓ primen, $\mathfrak{l}$ die in ℓ aufgehenden Teiler von $\mathfrak{D}$ durchläuft und v zu jedem $\mathfrak{l}$ die erläuterte Bedeutung hat.

B. Normenreste

B. Normenreste im relativ–zyklischen Körper von Primzahlgrad.

Von jetzt an sei K ein relativ–zyklischer Körper vom Primzahlgrad ℓ über k, σ die erzeugende Substitution $\mathfrak{D} = \mathfrak{f}^{\ell-1} = \prod \mathfrak{p} \cdot \prod \mathfrak{l}^{v+1}$ seine Relativdiskriminante.

Definition 1. Ist $\mathfrak{m}$ ein beliebiger (ganzer) Idealmodul aus k, so heißt eine für $\mathfrak{m}$ ganze Zahl α aus k *Normenrest* von K mod. $\mathfrak{m}$, wenn es in K ein A gibt, sodaß

$$n(\mathsf{A}) \equiv \alpha \mod \mathfrak{m}$$

ist.

Satz 5. Geht $\mathfrak{p}$ nicht in der Relativdiskriminante von K auf, so ist jedes zu $\mathfrak{p}$ prime α Normenrest von K nach jeder Potenz $\mathfrak{p}^a$.

Beweis. Es sind folgende 4 Fälle zu unterscheiden:

1.) $\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_\ell$ prim zu ℓ,

2.) $\mathfrak{p} = \mathfrak{P}$ prim zu ℓ,

3.) $\mathfrak{l} = \mathfrak{L}_1 \dots \mathfrak{L}_\ell$ Teiler von ℓ,

4.) $\mathfrak{l} = \mathfrak{L}$ Teiler von ℓ.

1.) 3.) In diesen Fällen ist K für den Bereich von $\mathfrak{p}$ (bezw. $\mathfrak{l}$, ich lasse diesen Zusatz hier weg) ein aus ℓ Körpern $k(\mathfrak{p})$ zusammengesetzter Ring. Ist α eine beliebige Zahl aus $k(\mathfrak{[\dots]})$, so gibt es in diesem Ringe stets ein Element A, das für alle Stellen $\mathfrak{P}_i$ den Wert 1, außer etwa für $\mathfrak{P}_1$ den Wert α hat. Dann ist

$$n(\mathsf{A}) = \alpha \cdot 1 \cdot 1 \cdot \dots \cdot 1 = \alpha \ (\mathfrak{p}),$$

also natürlich auch

$$n(\mathsf{A}) \equiv \alpha \mod \mathfrak{p}^a$$

13 IV

durch ein A aus K selbst lösbar.

2.) Dann ist $K(\mathfrak{P})$ Körper vom Grade ℓ über $k(\mathfrak{p})$. Jedes zu $\mathfrak{p}$ prime α aus $k(\mathfrak{p})$ läßt sich eindeutig in der Form darstellen:

$$\alpha = \omega^b \xi^\ell \ (\mathfrak{p}); \qquad (0 \leqq b < \ell - 1)$$

wo ω eine $(N\mathfrak{p} - 1)$ te, d.h. $(p^f - 1)$–te[1] primitive Einheitswurzel aus $k(\mathfrak{p})$ ist. In $K(\mathfrak{P})$ kommt eine primitive $(p^{\ell f} - 1)$–te Einheitswurzel Ω vor, deren relativkonjugierte zu $k(\mathfrak{p})$ die ℓ Größen

$$\Omega, \Omega^{p^f}, \Omega^{p^{2f}}, \dots, \Omega^{p^{(\ell-1)f}}$$

sind. Es ist also

$$n(\Omega) = \Omega^{1+p^f+p^{2f}+\dots+p^{(\ell-1)f}} = \Omega^{\frac{p^{\ell f}-1}{p^f-1}} \ (\mathfrak{P})$$

eine primitive $(p^f - 1)$–te Einheitswurzel, die in obiger Darstellung als ω genommen werden darf. Dann ist

$$\alpha = n(\Omega^b \xi) \ (\mathfrak{p})$$

[1] optisch unklar, ob f identisch mit $\mathfrak{f}$

also sicher Normenrest für jede Potenz $\mathfrak{p}^a$.

4.) Siehe Abschnitt a.) meiner gemeinsam mit *Hensel* bearbeiteten Abhandlung in den Math. Ann. oder auch Hensel, Ein neues Normenrestsymbol und seine Anwendung…, Crelle 152, Bd. III/IV.

Bemerkung. Ist ein α aus k nach jeder noch so hohen Potenz von $\mathfrak{p}$ Normenrest, oder was auf dasselbe hinauskommt, Relativnorm eines Elementes der zugehörigen Henselschen Erweiterung, so soll α zum Unterschied *Normzahl* nach $\mathfrak{p}$ genannt werden. Die Identität beider genannten Wendungen folgt exakt vermöge der beiden Tatsachen:

a.) Ist $\mathsf{A} \equiv 1 \mod \mathfrak{p}^a$;

so ist $n(\mathsf{A}) \equiv 1 \mod \mathfrak{p}^a$.

b.) Ist $\alpha \equiv 1 \mod \mathfrak{p}^a$; ($a$ hinreichend groß),

so ist $\alpha \equiv \xi^\ell \ (\mathfrak{p})$.

Wir haben somit sogar bewiesen:

Satz 5a. Geht $\mathfrak{p}$ nicht in der Relativdiskriminante von K auf, so ist jedes zu $\mathfrak{p}$ prime α aus k *Normzahl* nach $\mathfrak{p}$.

Weiter erkennen wir allgemein, daß es zu jedem $\mathfrak{p}$ einen bestimmten Exponenten u geben muß, sodaß jeder zu $\mathfrak{p}$ prime Normenrest mod $\mathfrak{p}^u$ Normzahl nach $\mathfrak{p}$ ist und u der kleinstmögliche Exponent dieser Art ist. Für ein zu ℓ primes $\mathfrak{p}$ ist ersichtlich $u = 1$, denn ist

$$\alpha \equiv n(\mathsf{A}) \mod \mathfrak{p}$$

und α prim zu $\mathfrak{p}$, so folgt

$$\frac{\alpha}{n(\mathsf{A})} \equiv 1 \mod \mathfrak{p},$$

also

$$\frac{\alpha}{n(\mathsf{A})} = \xi^\ell \ (\mathfrak{p}),$$

$$\alpha = n(\mathsf{A}\xi) \ (\mathfrak{p})$$

Für Teiler $\mathfrak{l}$ von ℓ ist sicher $u \leqq \frac{e\ell}{\ell-1} + 1$, wenn $\mathfrak{l}$ die Ordnung e hat, da in $k(\mathfrak{l})$ jede Einseinheit vom Grade $\geqq \frac{e\ell}{\ell-1} + 1$ eine ℓ–te Potenz ist.

In dieser Hinsicht haben wir bewiesen:

Satz 5b. Geht $\mathfrak{p}$ nicht in der Relativdiskriminante von K auf, so ist das zugehörige $u = 1$.

Wir beweisen nun weiter:

Satz 6. Geht $\mathfrak{p}$ in der Relativdiskriminante von K auf und ist prim zu ℓ, so ist von allen zu $\mathfrak{p}$ primen, mod $\mathfrak{p}^a$ inkongruenten Zahlen genau der ℓ–te Teil Normenrest mod $\mathfrak{p}^a$ ($a \geqq 1$), nämlich die ℓ–ten Potenzreste mod $\mathfrak{p}^a$ Von allen Einheiten aus $k(\mathfrak{p})$ ist genau

15 IV

der ℓ–te Teil (eine Untergruppe vom Index ℓ) Normzahl, nämlich die ℓ–ten Potenzen aus $k(\mathfrak{p})$.

Beweis. Es braucht nur der zweite Teil bewiesen zu werden, aus dem nach dem Gesagten der erste unmittelbar folgt.

Nun ist $\mathfrak{p} = \mathfrak{P}^\ell$; (Grad 1), also jedes zu $\mathfrak{P}$ prime Element aus $K(\mathfrak{P})$ in der Form darstellbar

$$\mathsf{A} = \omega^b \Xi^\ell \ (\mathfrak{P})$$

wo ω eine schon in $k(\mathfrak{p})$ enthaltene, primitive $(p^f - 1)$ te Einheitswurzel ist. Daher

$$n(\mathsf{A}) = \omega^{b\ell} n(\Xi)^\ell = (\omega^b \xi)^\ell \ (\mathfrak{p})$$

durch Relativnormbildung von zu $\mathfrak{p}$ primen Zahlen, kann man also nur ℓ–te Potenzen aus $k(\mathfrak{p})$ erreichen, jede solche aber natürlich stets.

Satz 7. Geht der Teiler $\mathfrak{l}$ von ℓ in der Relativdiskriminante von K auf und zwar zur Potenz $\mathfrak{l}^{(v+1)(\ell-1)}$, so ist der oben definierte Exponent $u = v + 1$. Von allen □□□ zu $\mathfrak{l}$ primen, nach $\mathfrak{l}^a$ inkongruenten Zahlen ist für $a \geqq v + 1$ genau der ℓ–te Teil Normenrest mod $\mathfrak{l}^a$, von allen Einheiten aus $k(\mathfrak{l})$ genau der ℓ–te Teil Normzahl nach $\mathfrak{l}$. Nach einem Modul $\mathfrak{l}^a$ mit $a \leqq v$ ist jede zu $\mathfrak{l}$ prime Zahl Normenrest.

Beweis. Ich zeige zunächst den auf $k(\mathfrak{l})$ und „Normzahlen“ bezüglichen Teil des Satzes. Daraus wird sich der auf Normenreste mod $\mathfrak{l}^a$ bezügliche Teil ohne weiteres ergeben, die Tatsache $u = v + 1$ ebenfalls (folgt leicht aus dem letzten Teil des Satzes).

16 IV

Ich konstruiere mir zu diesem Zweck zuerst ein Fundamentalsystem für die multiplikative Darstellung in $K(\mathfrak{L})$, wenn $\mathfrak{l} = \mathfrak{L}^\ell$ gesetzt wird, und zwar, da es nur auf Einheiten ankommt, ein solches für die Einheiten allein. Dieses besteht:

1.) Aus $\ell e.f$ Einseinheiten der Form

$$\mathsf{H}_{i,\varrho} = 1 + w_i \Lambda_\varrho \,,$$

wo f der Grad von $\mathfrak{l}$ und $\mathfrak{L}$, $w_1, \ldots, w_f$ ein in $k(\mathfrak{l})$ enthaltenes System von f mod $\mathfrak{l}$ linear unabhängigen Einheiten ist, und Λ_ϱ für $\varrho = 1, 2, \ldots, \frac{e\ell^2}{\ell-1}$ und prim zu ℓ je eine genau durch $\mathfrak{L}^\varrho$ teilbare Zahl aus $K(\mathfrak{L})$ bedeutet.

(2.) Falls $K(\mathfrak{L})$ die ℓ–te Einheitswurzel ζ enthält, noch eine ausgezeichnete Einseinheit H_a. Ich sehe jedoch hier von diesem, in meiner mit *Hensel* gemeinsamen Arbeit behandelten Falle ab, da H_a und das entsprechende η_a in $k(\mathfrak{l})$ keinerlei besondere Bedeutung haben, falls $v < \frac{e\ell}{\ell-1}$, andererseits $v = \frac{e\ell}{\ell-1}$, also „η_a kritisches Element“ nur eintreten kann, wenn ζ enthalten ist, da sonst η_a ℓ–te Potenz) (s. unten S 22[2]

Jede Einheit aus $K(\mathfrak{L})$ ist also eindeutig darstellbar in der Form:

$$\mathsf{H} = \prod_{i,\varrho} \mathsf{H}_{i,\varrho}^{c_{i\varrho}} \Xi^\ell \ (\mathfrak{L}); \qquad (c_{i\varrho} = 0, 1, \ldots, \ell - 1).$$

Ich untersuche nun die Relativnormen $n(\mathsf{H}_{i\varrho})$ und suche aus ihnen ein Fundamentalsystem für $k(\mathfrak{l})$ zusammenzustellen. Es wird

17 IV

$$n(\mathsf{H}_{i\varrho}) = 1 + w_i S_1(\Lambda_\varrho) + w_i^2 S_2(\Lambda_\varrho) + \cdots + w_i^\ell S_\ell(\Lambda_\varrho) \ (\mathfrak{l}),$$

wo $S_1, S_2, \ldots, S_\ell$ die symmetrischen Grundfunktionen von Λ_ϱ und seinen relativkonjugierten bezeichnet. Diese führe ich auf die Potenzsummen zurück, die zunächst zu berechnen sind. Bezeichnet man letztere mit $P_1, P_2, \ldots$, so ist

$$P_\nu(\Lambda_\varrho) = P_1(\Lambda_\varrho^\nu) = P_1(\overline{\Lambda}_{\nu\varrho}).$$

[2] undeutlich

Es ist also nur $P_1(\Lambda_a)$ für beliebiges a zu berechnen. $P_1(\Lambda_a)$ ist aber die Relativspur

$$s(\Lambda_a) = \ell\Lambda_a + \binom{\ell}{2}(\sigma-1)\Lambda_a + \cdots + \binom{\ell}{\ell-1}(\sigma-1)^{\ell-2}\Lambda_a + (\sigma-1)^{\ell-1}\Lambda_a$$

(s. S. 5 unten). Wie aus den dortigen Ausführungen hervorgeht, ist hier jedes mittlere Glied von höherer Ordnung als das erste, das letzte mindestens von der Ordnung

$$a + (\ell-1)v,$$

während das erste Glied die Ordnung (genau)

$$e\ell + a$$

hat. Wegen $e\ell \geqq (\ell-1)v$

d.h. $e\ell + a \geqq a + (\ell-1)v$

ist auf folgendes zu schließen:

1.) $a < v$.

Dann ist $e\ell + a \geqq a + (\ell-1)v > a\ell$

also $s(\Lambda_a)$ mindestens durch $\mathfrak{L}^{a\ell+1}$, d.h. als Zahl aus $k(\mathfrak{l})$ durch $\mathfrak{L}^{(a+1)\ell} = \mathfrak{l}^{a+1}$ teilbar

2.) $a = v$.

Dann ist $e\ell + a \geqq a + (\ell-1)v = v\ell$, also $s(\Lambda_a)$ mindestens durch $\mathfrak{l}^v$ teilbar.

3.) $a > v$.

Dann ist $e\ell + a \geqq a + (\ell-1)v > v\ell$, also $s(\Lambda_a)$ mindestens durch $\mathfrak{L}^{v\ell+1}$, d.h. durch $\mathfrak{l}^{v+1}$ teilbar.

Damit ist für die Potenzsummen $P_\nu(\Lambda_\varrho)$ folgendes Resultat gewonnen:

$$P_\nu(\Lambda_\varrho) \equiv 0 \begin{cases} \bmod \mathfrak{l}^{\nu\varrho+1} & \text{für} \quad \nu\varrho < v \\ \bmod \mathfrak{l}^{v} & = \quad \nu\varrho = v \\ \bmod \mathfrak{l}^{v+1} & = \quad \nu\varrho > v \end{cases}$$

Die P_ν hängen mit den benötigten S_ν durch die Newtonschen Formeln zusammen:

$$\begin{aligned}
&P_1 - S_1 = 0\\
&P_2 - P_1S_1 + 2S_2 = 0\\
&P_3 - P_2S_1 + P_1S_2 - 3S_3 = 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&P_i - P_{i-1}S_1 + \cdots \mp P_1S_{i-1} \pm iS_i = 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&P_{\ell-1} - P_{\ell-2}S_1 + \cdots - P_1S_{\ell-2} + (\ell-1)S_{\ell-1} = 0.
\end{aligned}$$

Also ergibt sich:

1.) $\varrho < v$.

Sei $i\varrho \leqq v < (i+1)\varrho$, d.h. $i = \left[\frac{v}{\varrho}\right]$.

Dann ist $P_1, P_2, \ldots, P_{i-1} \equiv 0 \mod \mathfrak{l}^{\varrho+1}$,

also $S_1, S_2, \ldots, S_{i-1} \equiv 0 \mod \mathfrak{l}^{\varrho+1}$.

19 IV

Ist $i\varrho < v$, dann auch noch

$$\begin{aligned}
P_i &\equiv 0 \mod \mathfrak{l}^{\varrho+1},\\
S_i &\equiv 0 \mod \mathfrak{l}^{\varrho+1}.
\end{aligned}$$

Ist aber $i\varrho = v$, also $i \geqq 2$, so ist

$$P_i \equiv 0 \mod \mathfrak{l}^v = \mathfrak{l}^{i\varrho}, \quad \text{also} \quad \mod \mathfrak{l}^{\varrho+1}$$

und auch $S_i \equiv 0 \mod \mathfrak{l}^{\varrho+1}$

Da schließlich $P_{i+1}, \ldots, P_{\ell-1} \equiv 0 \bmod \mathfrak{l}^{v+1}$, d.h. $\bmod \mathfrak{l}^{\varrho+1}$, ist auch

$$S_{i+1}, \ldots, S_{\ell-1} \equiv 0 \mod y^{\varrho+1}.$$

Da $S_\ell(\Lambda_\varrho) = n(\Lambda_\varrho) = \lambda_\varrho$ eine genau durch $\mathfrak{l}^\varrho$ teilbare Zahl aus $k(\mathfrak{l})$ ist, folgt:

(1) $$\boldsymbol{n(\mathsf{H}_{i\varrho}) = 1 + w_i^\ell \lambda_\varrho + \cdots \ (\mathfrak{l}), \quad \text{für} \quad \varrho < v.}$$

2.) $\varrho = v$.

Dann ist

$$P_1 \equiv 0 \mod \mathfrak{l}^v,$$
$$P_2, \ldots, P_{\ell-1} \equiv 0 \mod \mathfrak{l}^{v+1},$$

also $$S_1 \equiv 0 \mod \mathfrak{l}^v,$$

und da jedes Glied $P_1 S_i \equiv 0 \bmod \mathfrak{l}^{v+1}$, auch

$$S_2, \ldots, S_{\ell-1} \equiv 0 \mod \mathfrak{l}^{v+1}$$

Schließlich $S_\ell(\Lambda_v) = n(\Lambda_v) = \lambda_v$ genau durch $\mathfrak{l}^v$ teilbar. Daher wird

$$n(\mathsf{H}_{iv}) = 1 + w_i s(\Lambda_v) + w_i^\ell n(\Lambda_v) + \cdots \ (\mathfrak{l}).$$

Man kann hier sicher Λ_v so wählen, daß auch $s(\Lambda_v)$ genau die Ordnung v hat. Nach Satz 2, S. 2 ist nämlich für irgendeine Primzahl Λ von $K(\mathfrak{L})$:

$$\frac{\sigma\Lambda}{\Lambda} = 1 + \Lambda_v$$

20 IV

mit genau durch $\mathfrak{L}^v$ teilbarem Λ_v. Daraus folgt durch Normbildung

$$1 = n(1 + \Lambda_v) = 1 + s(\Lambda_v) + n(\Lambda_v) + \cdots \ (\mathfrak{l})$$

also $$-s(\Lambda_v) \equiv n(\Lambda_v) \equiv \lambda_v \mod \mathfrak{l}^{v+1},$$

sodaß dies Λ_v die gewünschte Eigenschaft hat. Es werde daher für H_{iv} dies Λ_v gewählt, dann wird

(2) $$\boldsymbol{n(\mathsf{H}_{iv}) = 1 + (w_i^\ell - w_i)\lambda_v + \cdots}$$

3.) $\varrho > v$.

Dann sind alle P_ν, also auch alle $S_\nu \equiv 0 \mod \mathfrak{l}^{v+1}$, ebenso $S_\ell = n(\Lambda_\varrho)$, sodaß gilt:

(3) $$\boldsymbol{n(\mathsf{H}_{i\varrho}) \equiv 1 \mod \mathfrak{l}^{v+1}}, \text{ für } \boldsymbol{\varrho > v}$$

Die Gleichung (1) lehrt, daß zur Konstruktion des Fundamentalsystems für $k(\mathfrak{l})$ die Normen der $\mathsf{H}_{i\varrho}$ mit $\varrho < v$ sämtlich Verwendung finden können und

gerade alle Basissysteme $\eta_{i\varrho}$ der Grade $\varrho < v$ liefern. Denn die w_i^ℓ sind mit den w_i gleichzeitig ein System mod $\mathfrak{l}$ linear unabhängiger Einheiten.

Auf Grund von (2) erhält man ferner in bekannter Weise nur $f-1$ der Basiseinheiten η_{iv} vom Grade v, wenn man $w_f = 1$ wählt, da dann $w_1^\ell - w_1, \ldots, w_{f-1}^\ell - w_{f-1}$ sicher mod ℓ linear unabhängig sind. Die f–te Basiseinheit kann nicht als Norm erzeugt werden, und muß passend dazugewählt werden. Sie möge das „*kritische Element*“ heißen.

Um schließlich Basissysteme $\eta_{i\varrho}$ für die Grade $\varrho > v$ zu erhalten, setzen wir

$$\mathsf{H}_{i,v+\ell a} = 1 + w_i \lambda_a \Lambda_v,$$

wo $\lambda_a \sim \mathfrak{l}^a$ und Λ_v die oben bestimmte Zahl ist. Dann wird

$$n(\mathsf{H}_{i,v+\ell a}) = 1 + w_i \lambda_a s(\Lambda_v) + w_i^2 \lambda_a^2 S_2(\Lambda_v) + \cdots + w_i^\ell \lambda_a^\ell S_\ell(\Lambda_v)$$

Hier ist das 1. Glied $\sim \mathfrak{l}^{v+a}$, die folgenden nach dem obigen (Fall 2.) $\varrho = v$) $\equiv 0 \bmod \mathfrak{l}^{\nu a+v+1}$, d.h. $\equiv 0 \bmod \mathfrak{l}^{v+a+1}$, ebenso das letzte Glied $\sim \mathfrak{l}^{\ell a+v}$, d.h. $\equiv 0 \bmod \mathfrak{l}^{v+a+1}$. Daher wird in obiger Bezeichnung

$$n(\mathsf{H}_{i,v+\ell a}) = 1 - w_i \lambda_a \lambda_v + \cdots = 1 + w_i \lambda_{a+v} + \cdots \quad (\mathfrak{l})$$

liefert also ein Basissystem für den Grad $a+v$ in $k(\mathfrak{l})$. So kann man alle noch fehlenden Basissysteme $\eta_{i\varrho}$ für $\varrho > v$ erzeugen (ev. auch die ausgez. Einseinheit η_a).

Auf Grund der entwickelten beiden Fundamentalsysteme und ihrer Eigenschaften folgt nun dies:

1.) Jede Norm einer Einheit aus $K(\mathfrak{L})$ enthält bei der Darstellung durch das konstruierte Fundamentalsystem für $k(\mathfrak{l})$ dessen kritisches Element nicht.

Denn die Normen der $\mathsf{H}_{i\varrho}$ mit $\varrho < v$ sind andere Basiselemente, ebenso die Normen der $(f-1)\,\mathsf{H}_{iv}$ mit $i \neq 1$. Die $n(\mathsf{H}_{1v})$ ist nach (2) von höherem Grade als der Grad v des kritischen Elements, ebenso die $n(\mathsf{H}_{i\varrho})$ mit $\varrho > v$ nach (3) Schließlich ist die $n(\Xi^\ell) = \xi^\ell$ ℓte Potenz in $k(\mathfrak{l})$

2.) Jede Einheit aus $k(\mathfrak{l})$, die bei der Darstellung durch das konstruierte Fundamentalsystem dessen kritisches Element nicht enthält, ist Normzahl von $K(\mathfrak{L})$

Denn alle Basiselemente außer dem kritischen sind Normzahlen, ebenso jede ℓ–te Potenz ξ^ℓ.

Damit ist der auf $k(\mathfrak{l})$ und „Normzahlen“ bezügliche Teil von Satz 7 bewiesen, denn die Normzahlen bilden ersichtlich eine Untergruppe von $k(\mathfrak{l})$ vom Index ℓ, deren Faktorgruppe durch die Potenzen $\eta, \eta^2, \ldots, \eta^{\ell-1}$ des kritischen Elementes gebildet wird. Da dieses Element den Grad v hat, fällt es in der Basisdarstellung mod $\mathfrak{l}^a$ heraus, wenn $a \leqq v$, sodaß hier jede prime Restklasse Normenrest ist, während es mod $\mathfrak{l}^a$ für $a > v$ auftritt, sodaß hier wieder nur der ℓ–te Teil aller primen Restklassen Normenrest ist. Daß endlich $u = v+1$, ist auch klar, denn $u \leqq v$ kommt nach dem eben Gesagten nicht in Frage. Ist aber α Normenrest mod $\mathfrak{l}^{v+1}$, so enthält α in der Basisdarstellung mod $\mathfrak{l}^{v+1}$ das kritische Element nicht, also auch in der Basisdarstellung in $k(\mathfrak{l})$ höchstens in ℓ–ter Potenz.

Damit ist Satz 7 bewiesen.

Anmerkung. Der Fall, wo ζ enthalten ist, ist auch in diesem Beweise enthalten. Für $1 \leqq v < \frac{e\ell}{\ell-1}$ ändert sich fast gar nichts, für $v = \frac{e\ell}{\ell-1}$ wird eben das kritische Element η_a. Wie schon S. 16 angedeutet, kann $v = \frac{e\ell}{\ell-1}$ nur für diesen Fall, daß ζ enthalten ist, eintreten. Denn sonst würde sich ergeben, daß eine

Einseinheit vom Grade $\frac{e\ell}{\ell-1}$ Normennichtrest wäre, während sie doch in diesem Falle sicher ℓ–te Potenz in $k(\mathfrak{l})$ ist. Man kann dies auch direkt einsehen. Wäre nämlich, wenn ζ nicht enthalten ist

$$\frac{\sigma\Lambda}{\Lambda} = \mathsf{H} = 1 + \Lambda_{\frac{e\ell}{\ell-1}}$$

vom Grade $\frac{e\ell}{\ell-1}$, so wäre durch Normbildung nach S. 20 oben:

$$1 = n\left(\frac{\sigma\Lambda}{\Lambda}\right) = n(\mathsf{H}) = \eta = 1 + s\left(\Lambda_{\frac{e\ell}{\ell-1}}\right) + n\left(\Lambda_{\frac{e\ell}{\ell-1}}\right) + \cdots$$

mindestens vom Grade $\frac{e\ell}{\ell-1}$, also ℓ–te Potenz in $k(\mathfrak{l})$. Es wäre also in $k(\mathfrak{l})$

$$1 = \eta_0^\ell \ (\mathfrak{l})$$

d.h. ζ enthalten.

Ich benutze die Sätze 5, 6, 7 um über die Normenreste nach einem beliebigen zusammengesetzten Idealmodul $\mathfrak{m}$ aus k eine Aussage zu machen. Es gilt zunächst:

Satz 8. Ist $\mathfrak{m} = \prod_i \mathfrak{p}_i^{\nu_i}$, so ist irgendein für $\mathfrak{m}$ ganzes α aus k dann und nur dann Normenrest mod $\mathfrak{m}$, wenn es nach jeder in $\mathfrak{m}$ enthaltenen Primteilerpotenz $\mathfrak{p}_i^{\nu_i}$ Normenrest ist.

Beweis. 1.) Ist $\alpha \equiv n(\mathsf{A}) \mod \mathfrak{m}$, so gilt erst recht:

$$\alpha \equiv n(\mathsf{A}) \mod \mathfrak{p}_i^{\nu_i}$$

2.) Ist $\alpha \equiv n(\mathsf{A}_i) \mod \mathfrak{p}_i^{\nu_i}$ und bestimmen wir ein A aus K so, daß

$$\mathsf{A} \equiv \mathsf{A}_i \mod \mathfrak{p}_i^{\nu_i}; \qquad \text{(für jedes } i\text{)}$$

gilt, so gilt, da $\mathfrak{p}_i$ in k liegt, auch

$$n(\mathsf{A}) \equiv n(\mathsf{A}_i) \mod \mathfrak{p}_i^{\nu_i}$$

also $\quad n(\mathsf{A}) \equiv \alpha \bmod \mathfrak{p}_i^{\nu_i}$ für jedes i, d.h. mod $\mathfrak{m}$.

Daraus folgt nun leicht folgender Hauptsatz:

Satz 9. Ist K relativ–zyklisch vom Primzahlgrad ℓ und

$$\mathfrak{D} = \mathfrak{f}^{\ell-1}, \quad \text{wo} \quad \mathfrak{f} = \prod \mathfrak{p} \cdot \prod \mathfrak{l}^{v+1}$$

seine Relativdiskriminante in Bezug auf k, gehen ferner in $\mathfrak{D}$ genau d von einander verschiedene Primteiler auf und ist $\mathfrak{m}$ ein beliebiges, durch $\mathfrak{f}$ teilbares, ganzes Ideal aus k, dann ist von allen zu $\mathfrak{m}$ primen Restklassen in k genau der ℓ^d–te Teil Normenrest von K mod $\mathfrak{m}$.

Beweis. Nach Satz 5 ist für die nicht in $\mathfrak{D}$ aufgehenden Primteilerpotenzen von $\mathfrak{m}$ jede prime Restklasse Normenrest. Die in $\mathfrak{D}$ aufgehenden Primteilerpotenzen sind nach Wahl von $\mathfrak{m} \equiv 0 \bmod \mathfrak{f}$ mindestens so hoch, daß für sie

genau der ℓ–te Teil aller primen Restklassen Normenrest ist. Da die Reste nach den einzelnen Primteilerpotenzen von einander unabhängig sind und genau d Primteiler der zweiten Art vorhanden sein sollen, folgt aus Satz 8 unsere Behauptung.

25 IV

C. Einheiten

C. Einheiten im relativ–zyklischen Körper von Primzahlgrad.

Es sei K relativ–zyklisch vom Primzahlgrad ℓ zu k und σ die erzeugende Substitution. In K sei ein Kongruenzstrahl O mod $\mathfrak{M}$ gegeben von der speziellen Eigenschaft, daß er gegenüber den Substitutionen von K invariant ist:

$$\sigma O = O,$$

d.h. mit A ist auch $\sigma\mathsf{A}$ Strahlzahl.

Der Durchschnitt von O mit k bildet dann einen Kongruenzstrahl o in k. Denn ist α_0 Zahl aus o und

$$\alpha_0 \equiv \mathsf{A}_0 \mod \mathfrak{M}$$

die Kongruenzbedingung, aus deren Bestehen die Zugehörigkeit von α_0 zu O erschlossen wird, so darf in jeder entsprechenden Bedingung A_0 durch α_0 ersetzt werden. Denken wir uns dies für alle in Betracht kommenden Restklassen, also alle Restklassen mod $\mathfrak{M}$, die Zahlen aus k enthalten und zu O gehören, getan, ferner mit $\mathfrak{m}$ das kleinste Ideal aus k bezeichnet, das durch $\mathfrak{M}$ teilbar ist; ist dann α irgendeine Zahl aus O und k, also aus o und

$$\alpha \equiv \alpha_0 \mod \mathfrak{M}$$

so ist auch

$$\alpha \equiv \alpha_0 \mod \mathfrak{m}$$

und umgekehrt a fortiori. Der *Strahl* o (natürlich!) ist also *Kongruenzstrahl* mod $\mathfrak{m}$ in k, da die Zugehörigkeit

26 IV

zu o aus Kongruenzbedingungen mod $\mathfrak{m}$ erschlossen werden kann (die α_0 bilden *natürlich* eine Gruppe mod $\mathfrak{m}$). Sind noch Vorzeichenbedingungen in der Definition von O enthalten, so gilt das vorige unverändert, weil die

Signatur von α aus k invariant ist, $\square\square\square$ (die konjugierten zu α in K sind dieselben in entsprechender Vielfachheit).

Auf diese Strahlen O und o sollen sich die folgenden Sätze beziehen.

Es seien R und r die Anzahl der Grundeinheiten in K und k, also auch in O und o.

Satz 10. Es ist

$$\begin{aligned} R - r &= (\ell - 1)(r + 1) \quad \text{für} \quad \ell \neq 2, \\ R - r &= r + 1 - \nu \qquad \text{für} \quad \ell = 2, \end{aligned}$$

wenn ν die Anzahl der negativen, reellen konjugierten zur Grundzahl μ von $K = k(\sqrt{\mu})$.

Beweis. 1.) $\ell \neq 2$. Dann ist für einen reellen konjugierten Körper k_i auch die zugehörige Serie von ℓ konjugierten K_{ij} reell, denn eine Gleichung ungeraden Grades mit reellen Koeffizienten hat eine, also als zyklische Gleichung lauter reelle Wurzeln. Für einen komplexen k_i ist natürlich auch K_{ij} komplex. Die charakteristischen Zahlen R_1, R_2 für K sind also

$$R_1 = \ell r_1; \qquad R_2 = \ell r_2$$

also

$$R = R_1 + R_2 - 1 = \ell(r_1 + r_2) - 1 = \ell r + \ell - 1$$

$$R - r = (\ell - 1)(r + 1).$$

2.) $\ell = 2$. Sei $K = k(\sqrt{\mu})$ und ν die Anzahl der reellen, negativen, zu μ konjugierten. Dann entspricht jedem komplexen k_i ein Paar komplexer K_{ij}, jedem der genannten ν reellen k_i ebenfalls, den übrigen reellen k_i ein Paar reeller K_{ij}. Also ist

$$\begin{gathered} R_1 = 2(r_1 - \nu); \qquad R_2 = 2r_2 + \nu, \\ R = R_1 + R_2 - 1 = 2(r_1 + r_2) - \nu = 2r + 1 - \nu, \\ R - r = r + 1 - \nu. \end{gathered}$$

Satz 11. Im Strahl O gibt es ein System von n Einheiten $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_n$, sodaß jede Einheit E aus O, in der Form

$$\mathsf{E} = \mathsf{H}_1^{c_1} \ldots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma}\ [\xi]; \qquad (c_i = 0, 1, \ldots, \ell - 1)$$

eindeutig in den c_i darstellbar ist, wobei H eine Einheit aus O und $[\xi]$ eine Einheit aus o oder aber eine solche Einheit aus O ist, deren ℓ–te Potenz in o liegt. Die Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_n$ sind also in dem Sinne voneinander unabhängig, daß $\mathsf{E} = 1$ notwendig $c_i = 0$ nach sich zieht. Die Zahl n ist

$$\begin{array}{lll} n = r + 1, & \text{wenn} & \ell \neq 2, \\ n = r + 1 - \nu, & \text{"} & \ell = 2. \end{array}$$

(Siehe jedoch Zusatz a. S. 36▸)

Beweis. Es ist $1 + \sigma + \cdots + \sigma^{\ell-1} = \ell + \binom{\ell}{2}(\sigma - 1) + \cdots + (\sigma - 1)^{\ell-1} = \ell + (\sigma - 1)Q(\sigma)$ [3], also für jede Einheit E aus O:

$$n(\mathsf{E}) = \mathsf{E}^{\ell}\mathsf{E}^{(\sigma-1)Q(\sigma)} = \mathsf{E}^{\ell}\mathsf{H}^{\sigma-1}$$

d.h. $\mathsf{E}^{\ell} = \mathsf{H}^{1-\sigma} \cdot \varepsilon$,

wo $\varepsilon = n(\mathsf{E})$ erstens Einheit aus k und zweitens als Produkt der sämtlich in O vorkommenden konjugierten $\sigma^i\mathsf{E}$ Einheit aus O ist, also insgesamt Einheit aus o ist. Die ℓ–te Potenz jeder Einheit aus O ist also in der Form $\mathsf{H}^{1-\sigma}[\xi]$ enthalten. Die Einheiten dieser Form bilden ferner eine Gruppe, denn

$$\mathsf{H}_1^{1-\sigma}[\xi_1] \cdot \mathsf{H}_2^{1-\sigma}[\xi_2] = (\mathsf{H}_1\mathsf{H}_2)^{1-\sigma}[\xi_1\xi_2]$$

und $[\xi_1][\xi_2] = [\xi_1\xi_2]$ ist wieder von der genannten Beschaffenheit.

Die Einheiten der Form $\mathsf{H}^{1-\sigma}[\xi]$ aus O bilden also eine Untergruppe der Einheiten in O, die den Haupteinheitenverband E^{ℓ} enthält, und folglich, wenn überhaupt eine Einheit, dann auch ihren ganzen Verband in O enthält. Da es nur endlich viele Einheitenverbände gibt, hat also die Gruppe $\mathsf{H}^{1-\sigma}[\xi]$ einen endlichen Index, der ein Teiler ℓ^n des Index von E^{ℓ}, d.h. der Anzahl $\ell^{R+\delta}$ aller Einheitenverbände in O sein muß. (Es bilden eine Anzahl von Verbänden die Gruppe $\mathsf{H}^{1-\sigma}[\xi]$, eine ebenso große Anzahl von Verbänden entfällt auf jede Nebengruppe). Jede Nebengruppe zu $\mathsf{H}^{1-\sigma}[\xi]$ gehört zum Exponenten ℓ, folglich existiert sicher eine eindeutige Darstellung, wie im Satz behauptet mit gewissen n Basiselementen $\mathsf{H}_1, \ldots, \mathsf{H}_n$ (aus den n Nebengruppen, die eine Basis für die Faktorgruppe bilden). Es ist somit nur noch die Anzahl n zu bestimmen.

Sei demgemäß

$$\mathsf{E} = \mathsf{H}_1^{c_1} \ldots \mathsf{H}_n^{c_n}\mathsf{H}^{1-\sigma}[\xi]$$

[3] undeutlich

die Darstellung eines beliebigen E aus O in der genannten Form. Dann läßt sich die Einheit H in derselben Form darstellen:

$$\mathsf{H} = \mathsf{H}_1^{c_1'} \dots \mathsf{H}_n^{c_n'} \mathsf{H}'^{1-\sigma} [\xi'].$$

Die Einheit $[\xi']^{1-\sigma}$ ist nach Definition von $[\xi']$ entweder 1, wenn $[\xi']$ in o oder eine primitive ℓ–te Einheitswurzel ζ, wenn erst $[\xi']^\ell$ in o liegt. Denn im letzteren Falle wird K durch $[\xi']$ erzeugt, also ist $\sigma[\xi'] = \zeta[\xi']$. (Es kommt dann natürlich ζ in k vor und muß überdies auch in o vorkommen, da es gleich $[\xi']^{1-\sigma}$, also Zahl aus O ist). $[\xi']^{1-\sigma}$ ist also auf alle Fälle Einheit aus o, also in der Form $[\xi]$ enthalten. Daher folgt durch Einsetzen:

$$\mathsf{E} = \mathsf{H}_1^{c_1 + c_1'(1-\sigma)} \dots \mathsf{H}_n^{c_n + c_n'(1-\sigma)} \mathsf{H}'^{(1-\sigma)^2} [\xi'']$$

und so fortfahrend eine Gleichung der Form

$$\mathsf{E} = \mathsf{H}_1^{F_1(\sigma)} \dots \mathsf{H}_n^{F_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-1}} [\xi] \tag{1}$$

wo $F_i(\sigma) = c_i + c_i'(1-\sigma) + \dots + c_i^{(\ell-2)}(1-\sigma)^{\ell-2}$ ist, (mit Koeffizienten der Reihe $0, 1, \dots, \ell - 1$). Wir untersuchen nun die Annahme, daß ein solcher Ausdruck gleich 1 sei. Zieht man den durch $1-\sigma$ teilbaren Teil der $F_i(\sigma)$ zu $\mathsf{H}^{(1-\sigma)^{\ell-1}}$, so folgt nach obigem:

$$c_i = 0; \qquad (i = 1, 2, \dots, n).$$

Für $\ell = 2$ kann man also schon auf $F_i(\sigma) = 0$ schließen. Für $\ell > 2$ folgt weiter:

$$1 = \left(\mathsf{H}_1^{G_1(\sigma)} \mathsf{H}_2^{G_2(\sigma)} \dots \mathsf{H}_n^{G_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-2}} \right)^{1-\sigma} [\xi],$$

wo

$$G_i(\sigma) = c_i' + c_i''(1-\sigma) + \dots + c_i^{(\ell-2)}(1-\sigma)^{\ell-3}$$

ist. Aus dieser Relation der Gestalt

$$\mathsf{H}^{1-\sigma} = [\xi]$$

folgt aber

$$1 = n(\mathsf{H}^{1-\sigma}) = n[\xi]$$

Liegt $[\xi]$ in o, so folgt also $[\xi]^\ell = 1$. Liegt aber erst $[\xi]^\ell$ in o, so ist

$$n[\xi] = [\xi] \cdot \zeta[\xi] \cdot \cdots \cdot \zeta^{\ell-1}[\xi] = [\xi]^\ell$$

also ebenfalls $[\xi]^\ell = 1$. Es muß somit sein

entweder: $[\xi] = 1$ also $\mathsf{H}^{1-\sigma} = 1$, d.h. $\mathsf{H} = \sigma\mathsf{H}$ in o enthalten

oder: $[\xi] = \zeta$, also $\mathsf{H}^{1-\sigma} = \zeta$, d.h. $\mathsf{H}^\ell = \sigma\mathsf{H}^\ell$ in o enthalten.

Auf jeden Fall also H von der Form $[\xi]$. (Bei diesem Schluß kommt die Notwendigkeit für die Einführung von $[\xi]$ herein. Aus $\mathsf{H}^{1-\sigma} = \xi$ aus o folgt eben *nicht* stets **H in o**, sondern ev. nur **H^ℓ in o**).

Auf unseren obigen Ausdruck angewendet, folgt also

$$\mathsf{H}_1^{G_1(\sigma)} \ldots \mathsf{H}_n^{G_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-2}}[\xi] = 1,$$

d.h. wenn man wieder die $(1-\sigma)$–ten Potenzen in $\mathsf{H}^{(1-\sigma)^{\ell-2}}$ vereinigt, daß auch

$$c_i' = 0; \qquad (i = 1, 2, \ldots, n).$$

So fortfahrend folgt sukzessive das Verschwinden aller Koeffizienten, also

$$F_i(\sigma) = 0; \qquad (i = 1, 2, \ldots, n).$$

31 IV

Es gilt also:

$$\text{Aus} \qquad 1 = \mathsf{H}_1^{F_1(\sigma)} \ldots \mathsf{H}_n^{F_n(\sigma)} \mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$$

wo die $F_i(\sigma)$ (nach $1-\sigma$ entwickelt gedachte) ganzzahlige Polynome vom Grade $\ell - 2$ und Koeffizienten $0, 1, \ldots, \ell - 1$ sind, folgt $F_i(\sigma) = 0$; $(i = 1, 2, \ldots, n)$.

Daraus folgt, daß die $n(\ell - 1)$ Einheiten

$$\begin{array}{llll} \mathsf{H}_1, & \mathsf{H}_1^{1-\sigma}, & \mathsf{H}_1^{(1-\sigma)^2}, & \ldots \quad \mathsf{H}_1^{(1-\sigma)^{\ell-2}} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \mathsf{H}_n, & \mathsf{H}_n^{1-\sigma}, & \mathsf{H}_n^{(1-\sigma)^2}, & \ldots \quad \mathsf{H}_n^{(1-\sigma)^{\ell-2}} \end{array}$$

in Bezug auf die Gruppe aller Einheiten $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ unabhängig sind. Dies gilt vorläufig nur insoweit, als nur Exponenten $0, 1, \ldots, \ell-1$ zugelassen werden. Wir werden aber sofort beweisen, daß die Gruppe aller Einheiten $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ mit der Gruppe $\mathsf{H}^{\ell}[\xi]$ identisch ist, sodaß die Unabhängigkeit der genannten Einheiten auch für beliebige Exponenten (Koeffizienten der $F_i(\sigma)$) folgt. Da nach dem Bewiesenen andererseits jede Einheit aus O in der Form (1) darstellbar ist, folgt dann, daß unsere $n(\ell-1)$ Einheiten eine Basis für die Faktorgruppe zu $\mathsf{H}^{\ell}[\xi]$ als Untergruppe der Gruppe aller Einheiten in O bilden. Ich weise zunächst die Identität der Gruppen $\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi]$ und $\mathsf{H}^{\ell}[\xi]$ nach. Einerseits ist (S. 5 unten)

$$(1-\sigma)^{\ell-1} = 1 + \sigma + \cdots + \sigma^{\ell-1} + \ell\varphi(\sigma)$$

also

$$\mathsf{H}^{(1-\sigma)^{\ell-1}} = (\mathsf{H}^{\varphi(\sigma)})^{\ell} n(\mathsf{H}) = (\mathsf{H}^{\varphi(\sigma)})^{\ell}\eta$$
$$\mathsf{H}^{(1-\sigma)^{\ell-1}}[\xi] = \mathsf{H}'^{\ell}[\xi'].$$

32 IV

Andrerseits ist

$$\ell = (1-\zeta)^{\ell-1}\varphi(\zeta)$$

also $$\ell = (1-x)^{\ell-1}\varphi(x) + (1 + x + \cdots + x^{\ell-1})\psi(x)$$

d.h. $$\ell = (1-\sigma)^{\ell-1}\varphi(\sigma) + (1 + \sigma + \cdots + \sigma^{\ell-1})\psi(\sigma)$$

mit ganzzahligem φ und ψ. Daher:

$$\mathsf{H}^{\ell} = \left(\mathsf{H}^{\varphi(\sigma)}\right)^{(1-\sigma)^{\ell-1}} n(\mathsf{H})^{\psi(\sigma)} = \mathsf{H}'^{(1-\sigma)^{\ell-1}}\eta$$

also $$\mathsf{H}^{\ell}[\xi] = \mathsf{H}'^{(1-\sigma)^{\ell-1}}[\xi'].$$

Es bleibt somit noch die Anzahl der Nebengruppen zu $\mathsf{H}^{\ell}[\xi]$ als Untergruppe der Gruppe aller Einheiten von O zu ermitteln, deren Anzahl mit $\ell^{(\ell-1)n}$ identifiziert, den gesuchten Wert von n liefern muß.

Dazu zeigen wir, daß die Untergruppe $\mathsf{H}^{\ell}[\xi]$, die offenbar stets ganze Verbände aus O enthält, genau ebensoviele Einheitenverbände in O enthält, als Einheitenverbände in o existieren. Ist dies gezeigt, dann folgt unsere Behauptung für n leicht so:

Die Zahl der Einheitenverbände in O und o ist $\ell^{R+\delta}$ und $\ell^{r+\delta}$; ($\delta = 1$ oder 0 je nachdem ζ in O, somit auch in o vorkommt oder nicht in O, somit auch nicht in o vorkommt: $o =$ Durchschnitt von O, k.)
Enthält also $\mathsf{H}^\ell[\xi]$ genau $\ell^{r+\delta}$ Einheitenverbände aus O, so ist sein Index zur Gruppe aller Einheiten in O gleich dem Quotienten $\ell^{R+\delta}$: $\ell^{r+\delta} = \ell^{R-r} = \ell^{(\ell-1)(r+1)}$ für $\ell \neq 2$ und $= \ell^{r+1-\nu}$ für $\ell = 2$, woraus die Behauptung für n sofort folgt.

33 IV

Es bleibt also noch die Behauptung von S. 32▸ Mitte zu beweisen. Dazu ordnen wir jedem Verband $[\xi]\mathsf{H}^\ell$ in O eindeutig einen bestimmten Verband in o zu und umgekehrt.

Ist zunächst in O keine Einheit vorhanden, deren ℓ–te Potenz in o liegt, also jedes $[\xi]$ Einheit ξ aus o, dann werde dem Verband $\xi\mathsf{H}^\ell$ in O der Verband $\xi\eta^\ell$ in o zugeordnet. Sind dann ξ_1, ξ_2 zwei Einheiten aus o die in O verschiedenen Verbänden angehören, so liefern sie natürlich auch in o verschiedene Verbände. Liefern umgekehrt ξ_1 und ξ_2 in o verschiedene Verbände, so kann nicht $\frac{\xi_1}{\xi_2} = \mathsf{H}^\ell$ in O sein, weil sonst $\sqrt[\ell]{\frac{\xi_1}{\xi_2}} = \mathsf{H}$ ein $[\xi]$ wäre. Somit ist die getroffene Zuordnung gegenseitig eindeutig und alles bewiesen.

Etwas komplizierter wird die entsprechende Betrachtung, wenn Einheiten $[\xi]$ aus O aber nicht o vorhanden sind. In diesem Fall ist offenbar $K = k(\sqrt[\ell]{\xi_0})$ und ξ_0 eine Einheit aus o, $\sqrt[\ell]{\xi_0}$ eine Einheit vom Typus $[\xi]$ aus O, ferner*) jede Einheit dieses Typus von der Form $\sqrt[\ell]{\xi_0}^c\xi$ mit beliebigem Exponenten c und beliebiger Einheit ξ aus o.

Sei nun $\xi_0, \xi_1, \ldots, \xi_\kappa$ eine Basis für die Gruppe der Einheitenverbände in o, in die offenbar ξ_0 mit aufgenommen werden darf, da es keine ℓ–te Potenz ist,

34 IV

dann läßt sich jeder Einheitenverband $[\xi]\mathsf{H}^\ell$ in O in der Form schreiben:

$$[\xi]\mathsf{H}^\ell = \sqrt[\ell]{\xi_0}^c\xi_0^{c_0}\xi_1^{c_1}\ldots\xi_\kappa^{c_\kappa}\mathsf{H}^\ell; \qquad (c, c_i = 0, 1, \ldots, \ell-1)$$

Da aber ξ_0 in O ℓ–te Potenz von $\sqrt[\ell]{\xi_0}$ ist, darf es in H^ℓ hereingezogen gedacht werden, also:

$$[\xi]\mathsf{H}^\ell = \sqrt[\ell]{\xi_0}^c\xi_1^{c_1}\ldots\xi_\kappa^{c_\kappa}\mathsf{H}'^\ell$$

*) Theorie des Kummerschen Körpers, A.Z. III, S. 267▸.

Es ist dann nur zu zeigen, daß diese $\ell^{\kappa+1}$ Verbände in O sämtlich verschieden sind. Wäre dies nicht der Fall, so bestände eine Relation:

$$\sqrt[\ell]{\xi_0}^{a}\xi_1^{a_1}\dots\xi_\kappa^{a_\kappa} = \sqrt[\ell]{\xi_0}^{a}\xi = \mathsf{H}^\ell; \qquad (a, a_0 = 0, 1, \dots, \ell-1)$$

Wegen $n\sqrt[\ell]{\xi_0} = (-1)^{\ell-1}\xi_0$ folgte für ungerades ℓ:

$$\xi_0^a\xi^\ell = n(\mathsf{H})^\ell = \eta^\ell$$

also $$\xi_0^a = \eta'^\ell, \text{ d.h. } a = 0$$

und $$\xi = \xi_1^{a_1}\dots\xi_\kappa^{a_\kappa} = \mathsf{H}^\ell.$$

Diese Gleichung ist aber nur für $a_1 = \dots = a_\kappa = 0$ möglich, da sonst $\xi = \xi_0^c\xi'^\ell$ sein müßte[†)] mit $c \not\equiv 0 \bmod \ell$, was wegen der Unabhängigkeit der Basiselemente $\xi_0, \xi_1, \dots, \xi_\kappa$ unmöglich.

Für $\ell = 2$ versagt wegen $n(\sqrt{\xi_0}) = -\xi_0$ diese Schlußweise. Auch hier folgt aber im allgemeinen aus:

$$\sqrt{\xi_0}^{a}\xi = \mathsf{H}^2$$

daß $a = 0$ sein muß. □□□

35 IV

Durch Normbildung folgt nämlich jetzt, falls $a = 1$ sein sollte:

$$-\xi_0\xi^2 = \eta^2, \qquad \text{d.h.} \qquad -\xi_0 = \eta'^2$$

also ein Widerspruch, falls nicht speziell $-\xi_0$ Quadrat einer Einheit aus o ist, und dann alles übrige wie vorher.

Ist aber $-\xi_0 = \eta_0^2$ Quadrat in o, so wird K durch $\sqrt{-1}$ erzeugt. $\pm\sqrt{-1}$ muß dann auch in O liegen, denn η_0 und $\pm\sqrt{\xi_0} = \pm\sqrt{-1}\eta_0$ liegen dann in O (-1 selbstverständlich als $\sqrt{-\xi_0}^{1-\sigma}$). In diesem Falle kann □□□ dann $\sqrt{-1}$ als erzeugendes Element von O genommen werden, sodaß direkt $\xi_0 = -1$ und $[\xi_0] = \sqrt{-1}$ gesetzt werden kann.

Hier ist aber eine Relation[‡)]

$$\sqrt{-1}\xi = \mathsf{H}^2$$

[†)] Siehe Anm. a. voriger Seite.

[‡)] Nach S. 27 unten ist eine Relation $\sqrt{-1}\xi = \mathsf{H}^2$ und $\sqrt{-1}\xi' = \mathsf{H}'^{1-\sigma}$ gleichbedeutend.

unter Umständen möglich, z.B. wenn $k = R(\sqrt{-2})$ [4] und $K = k(\sqrt{-1})$ betrachtet wird, wo

$$\sqrt{-1} = \left(\frac{1-\sqrt{-1}}{\sqrt{-2}}\right)^2$$

ist (O, o Strahlen aller Körperzahlen!). Ist nun zunächst keine solche Relation möglich, so folgt alles wie vorher. Ist aber eine solche Relation vorhanden, so läßt sich jeder Verband $[\xi]\mathsf{H}^2$ in der Form

$$[\xi]\mathsf{H}^2 = \sqrt{-1}^c \xi_1^{c_1} \dots \xi_\kappa^{c_\kappa} \mathsf{H}'^2 = \xi_1^{\overline{c_1}} \dots \xi_\kappa^{\overline{c_\kappa}} \overline{\mathsf{H}}^2$$

schreiben und diese 2^κ Verbände sind wie vorher verschieden. Dann sind also nur die Hälfte Verbände $[\xi]\mathsf{H}^2$, wie vorher, vorhanden, sodaß sich unser n um eins vermehren muß. Es gilt also:

36 IV

Zusatz zu Satz 11: Ist $\ell = 2$, $K = k(\sqrt{-1})$ und besteht eine Relation

$$\sqrt{-1} = \xi\mathsf{H}^2$$

wo ξ Einheit aus o, H Einheit aus O ist, so ist das n von Satz 11 vielmehr

$$n = r + 2 - \nu.$$

Ich beweise nunmehr weiter:

Satz 12. Machen die Relativnormen sämtlicher Einheiten aus O insgesamt ℓ^{v_0} Einheitenverbände in o aus, dann gibt es in O

$$\varrho = \begin{cases} r + 1 + \delta - v_0 & \text{für } \ell \neq 2 \\ r + 1 + \delta - \nu - v_0 & \text{für } \ell = 2 \end{cases}$$

Einheiten $\mathsf{E}_1, \mathsf{E}_2, \dots, \mathsf{E}_\varrho$ mit der Relativnorm 1, sodaß jede Einheit E aus O mit der Relativnorm 1 mit eindeutig bestimmten Exponenten $c_i = 0, 1, \dots, \ell - 1$ in der Form

$$\mathsf{E} = \mathsf{E}_1^{c_1} \dots \mathsf{E}_\varrho^{c_\varrho} \mathsf{H}^{1-\sigma}$$

darstellbar ist, wo H eine Einheit aus O ist. Aus $\mathsf{E} = 1$ folgt also notwendig $c_i = 0$. Die Zahl δ ist, wie früher, 1 oder 0, je nachdem o und O die primitive

[4] undeutlich

ℓ–te Einheitswurzel ζ enthalten oder nicht.

Beweis. 1.) Ist $\eta_0 = n(\mathsf{H})$, so ist $\eta_0\eta^\ell = n(\mathsf{H}\eta)$. Die Relativnormen von Einheiten aus O machen also immer ganze Einheitenverbände in o aus. Die Gruppe der Relativnorm–Einheitenverbände in o aus O ist also Untergruppe der Gruppe aller Einheitenverbände in o und als solche von einem Grade ℓ^{v_0}, wo $v_0 \leqq r + \delta$.

37 IV

2.) Die Gruppe aller Einheiten der Form $\mathsf{H}^{1-\sigma}$ aus O hat die Eigenschaft, daß ihre Relativnormen sämtlich 1 sind. Wir betrachten die Gruppe $\mathsf{H}^{1-\sigma}$ als Untergruppe aller Einheiten aus O, deren Relativnorm 1 ist. Da nach Satz 11 jede Einheit E aus O in der Form

$$\mathsf{E} = \mathsf{H}_1^{c_1} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma}[\xi]; \qquad (c_i = 0, 1 \dots, \ell - 1)$$

darstellbar ist, so gilt dies auch für die letztgenannte Gruppe. Soll nun $n(\mathsf{E}) = 1$ sein, so ist wegen $n(\mathsf{H}^{1-\sigma}) = 1$ offenbar $n[\xi]$ auf das System der ℓ^n Größen $n(\mathsf{H}_1)^{c_1}, \dots, n(\mathsf{H}_n)^{c_n}$ beschränkt. Die in der Darstellung unserer Gruppe vorkommenden $[\xi]$ sind also von der Art, daß $n([\xi])$ nur endlich viele Möglichkeiten hat; daraus folgt aber, daß auch $[\xi]$ selbst nur endlich viele Möglichkeiten hat. Denn es ist:

$$\begin{array}{ccccc} \text{für} & \ell \neq 2 & \text{stets} & n([\xi]) = [\xi]^\ell \\ \shortparallel & \ell = 2 & \shortparallel & n([\xi]) = \pm[\xi]^2. \end{array}$$

Also hat die Gruppe $\mathsf{H}^{1-\sigma}$ als Untergruppe von „$n(\mathsf{E}) = 1$“ einen endlichen Index.

Ferner gehört jede Nebengruppe $\mathsf{E} = \mathsf{H}_1^{c_1} \dots \mathsf{H}_n^{c_n}[\xi]\mathsf{H}^{1-\sigma}$ mit bestimmten $c_1, \dots, c_n, [\xi]$ zum Exponenten ℓ. Denn wie wir oben (S. 27▸) sahen, ist E^ℓ stets von der Form:

$$\mathsf{E}^\ell = \mathsf{H}^{1-\sigma} n(\mathsf{E})$$

Ist also überdies $n(\mathsf{E}) = 1$, so folgt $\mathsf{E} = \mathsf{H}^{1-\sigma}$.

Daher muß die Faktorgruppe von $\mathsf{H}^{1-\sigma}$ in Bezug auf $n(\mathsf{E}) = 1$ von einem Grade ℓ^ϱ und Typus $(\ell, \ell, \dots, \ell)$ sein.

38 IV

Also existiert für jede Einheit E mit $n(\mathsf{E}) = 1$ eine Darstellung, wie die behauptete, und diese ist eindeutig im Sinne des Satzes, weil das die Basisdarstellung der Faktorgruppe ist. Es bleibt demnach nur noch die Behauptung über den Wert von ϱ nachzuweisen.

3.) ζ komme in o und O nicht vor. Dann kann keine Einheit $[\xi]$ existieren, die nicht schon in o liegt, da sonst $[\xi]^{\sigma-1} = \zeta$ in O und o vorkäme. Sie nun nach Satz 11:

$$\mathsf{E}_1 = \mathsf{H}_1^{c_1} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi$$

die Darstellung des ersten Basiselementes E_1, (dessen Existenz soeben bewiesen wurde): Wären hier alle $c_i = 0$, so folgte $n(\xi) = \xi^\ell = 1$, also $\xi = 1$, weil ζ nicht in o. Es wäre also $\mathsf{E}_1 = \mathsf{H}^{1-\sigma}$ ein Widerspruch zu seiner Eigenschaft als Basiselement für die Gruppe der Nebengruppen zu $\mathsf{H}^{1-\sigma'}$. Es ist also etwa $c_1 \neq 0$, und dann darf in dem System $\mathsf{H}_1, \dots, \mathsf{H}_n$ offenbar H_1 durch E_1 ersetzt werden, ohne seine Eigenschaft von Satz 11 zu beeinträchtigen. Sei dann weiter

$$\mathsf{E}_2 = \mathsf{E}_1^{a_1} \mathsf{H}_2^{c_2} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi.$$

Wären dann alle $c_i = 0$, so wäre wie vorhin $\xi = 1$, also $\mathsf{E}_2 = \mathsf{E}_1^{a_1} \mathsf{H}^{1-\sigma}$ was mit der Eigenschaft der E_i unverträglich. Also ist etwa $c_2 \neq 0$ und H_2 darf durch E_2 ersetzt werden. So kann man fortfahren, solange noch E_i vorhanden sind. Wären mehr E_i als H_i, also mehr als n E_i vorhanden, so folgte aus der dann nach Satz 11 bestehenden Darstellung (alle $\mathsf{H}_1, \dots, \mathsf{H}_n$ sind durch $\mathsf{E}_1, \dots, \mathsf{E}_n$ schon ersetzt):

$$\mathsf{E}_{n+1} = \mathsf{E}_1^{c_1} \dots \mathsf{E}_n^{c_n} \mathsf{H}^{1-\sigma} \xi,$$

daß $\xi = 1$, wie oben, also eine Relation zwischen den E_i bestände, was unmöglich. Es ist also $\varrho \leqq n$ und $\mathsf{H}_1, \dots, \mathsf{H}_\varrho$ können durch $\mathsf{E}_1, \dots, \mathsf{E}_\varrho$ ersetzt werden.

Jedes E aus O läßt sich dann eindeutig in der Form

$$\mathsf{E} = \mathsf{E}_1^{c_1} \dots \mathsf{E}_\varrho^{c_\varrho} \mathsf{H}_{\varrho+1}^{c_{\varrho+1}} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi; \qquad (c_i = 0, 1, \dots, \ell - 1)$$

darstellen. Ein so dargestelltes E kann dabei nur dann die Relativnorm 1 haben, wenn $c_{\varrho+1}, \dots, c_n = 0$ sind, da ja ein solches E schon in der Form

$$\mathsf{E} = \mathsf{E}_1^{c_1} \dots \mathsf{E}_\varrho^{c_\varrho} \mathsf{H}^{1-\sigma}$$

darstellbar ist. Setzen wir also

$$\eta_{\varrho+1} = n(\mathsf{H}_{\varrho+1}); \ \dots \ ; \ \eta_n = n(\mathsf{H}_n),$$

so gilt für jede Einheit E aus O:

$$\varepsilon = n(\mathsf{E}) = \eta_{\varrho+1}^{c_{\varrho+1}} \dots \eta_n^{c_n} \xi^{\ell}; \qquad (c_i = 0, 1, \dots, \ell - 1).$$

Diese Darstellung ist auch eindeutig. Denn existierte eine Darstellung

$$1 = \eta_{\varrho+1}^{b_{\varrho+1}} \dots \eta_n^{b_n} \xi_0^{\ell},$$

so hätte die Einheit

$$\mathsf{E}_0 = \mathsf{H}_{\varrho+1}^{b_{\varrho+1}} \dots \mathsf{H}_n^{b_n} \xi_0$$

die Relativnorm 1, und dann muß, wie soeben gezeigt, $b_{\varrho+1}, \dots, b_n = 0$ sein.

Umgekehrt ist jede in der angegebenen Form dargestellte Einheit ε aus o Relativnorm einer sofort angebbaren Einheit E aus O. Die Relativnormen der Einheiten aus O machen also $n - \varrho$ unabhängige Einheitenverbände in o aus, sodaß $v_0 = n - \varrho$, $\varrho = n - v_0 = \left\{ \begin{array}{l} r + 1 - v_0 \\ r + 1 - \nu - v_0 \end{array} \right\}$ ist, was wegen $\delta = 0$ unsere Behauptung ist.

4.) ζ komme in o und O vor, jedoch sei in O nicht die ℓ–te Wurzel einer Einheit aus o enthalten. Dann ist in der Darstellung von Satz 11 wieder $[\xi] = \xi$ Einheit aus o. Es kann dann auch nicht $\zeta = \mathsf{H}^{1-\sigma}$ sein; □□□ denn dann wäre $\mathsf{H} \neq \sigma\mathsf{H}$, also H nicht in o enthalten, andererseits $\mathsf{H}^{\ell} = \sigma\mathsf{H}^{\ell}$, also H^{ℓ} in o enthalten, also ein „echtes“ $[\xi]$. Daher kann in 2.) das nicht in der Form $\mathsf{H}^{1-\sigma}$ enthaltene ζ als ein Basiselement E_{ϱ} genommen werden, weil ja $n(\zeta) = \zeta^{\ell} = 1$ ist. Seien $\mathsf{E}_1, \dots, \mathsf{E}_{\varrho-1}$ die übrigen Basiselemente. Ist dann

$$\mathsf{E}_1 = \mathsf{H}_1^{c_1} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi$$

und wären alle $c_i = 0$, so wäre $n(\mathsf{E}_1) = \xi^{\ell} = 1$, also $\xi = 1$ oder $\xi = \zeta^c$ und $\mathsf{E}_1 = \mathsf{H}^{1-\sigma}\zeta^c$, was wegen der Unabhängigkeit der Basiselemente nicht möglich. Wir können also, wie vorhin, $\mathsf{E}_1, \dots, \mathsf{E}_{\varrho-1}$ an Stelle von $\mathsf{H}_1, \dots, \mathsf{H}_{\varrho-1}$ einführen[§)] und haben dann für jedes E aus O eine eindeutige Darstellung:

$$\mathsf{E} = \mathsf{E}_1^{c_1} \dots \mathsf{E}_{\varrho-1}^{c_{\varrho-1}} \mathsf{H}_{\varrho}^{c_{\varrho}} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi; \qquad (c_i = 0, \dots, \ell - 1)$$

Hat dann E die Relativnorm 1, so ist es schon in der Form

$$\mathsf{E} = \mathsf{E}_1^{c'_1} \dots \mathsf{E}_{\varrho-1}^{c'_{\varrho-1}} \zeta^c \mathsf{H}'^{1-\sigma}$$

[§)] Hier folgt, ähnlich wie oben, leicht $n + 1 \geqq \varrho$.

darstellbar, und es folgt:

$$1 = \mathsf{E}_1^{c_1 - c_1'} \dots \mathsf{E}_{\varrho-1}^{c_{\varrho-1} - c_{\varrho-1}'} \mathsf{H}_\varrho^{c_\varrho} \dots \mathsf{H}_n^{c_n} \mathsf{H}''^{1-\sigma} \frac{\xi}{\zeta^c}$$

also, da $\frac{\xi}{\zeta^c} = \xi'$ Einheit aus o wegen der Eindeutigkeit nach Satz 11:

$$c_1 - c_1' = \dots = c_{\varrho-1} - c_{\varrho-1}' = 0,$$

hauptsächlich aber:

$$c_\varrho = \dots = c_n = 0.$$

41 IV

Für alle Relativnormen folgt dann

$$\varepsilon = n(\mathsf{E}) = \eta_\varrho^{c_\varrho} \dots \eta_n^{c_n} \xi^\ell; \qquad (c_\varrho, \dots, c_n = 0, 1, \dots, \ell - 1)$$

und zwar eindeutig, da sonst eine Einheit

$$\mathsf{E}_0 = \mathsf{H}_\varrho^{b_\varrho} \dots \mathsf{H}_n^{b_n} \xi_0$$

mit $n(\mathsf{E}_0) = 1$ und nicht allen $b_i = 0$ folgte, was soeben als unmöglich erkannt wurde. Umgekehrt ist jede solche Einheit ε Relativnorm einer sofort angebbaren Einheit E aus O. Also ist $v_0 = n - \varrho + 1$, $\varrho = n + 1 - v_0 = \left\{ \begin{array}{l} r + 2 - v_0 \\ r + 2 - \nu - v_0 \end{array} \right\}$, was wegen $\delta = 1$ unsere Behauptung ist.

5.) ζ komme in o und O vor und in O existiere die ℓ–te Wurzel einer Einheit ξ_0 aus o. Dann ist $K = k(\sqrt[\ell]{\xi_0})$ und jedes $[\xi] = \sqrt[\ell]{\xi_0}^{c_0} \cdot \xi$, wo ξ eine Einheit aus o ist. Es sei $\mathsf{H}_0 = \sqrt[\ell]{\xi_0}$. Dann kann man in Satz 11 die Einheiten $[\xi]$ durch $\mathsf{H}_0^{c_0} \xi$ ersetzen und hat für jede Einheit E aus O folgende Darstellung:

$$\mathsf{E} = \mathsf{H}_0^{c_0} \mathsf{H}_1^{c_1} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi; \qquad (c_i = 0, \dots, \ell - 1).$$

Diese Darstellung ist im allgemeinen ebenfalls noch eindeutig in den Exponenten $c_0, \dots, c_n$, sodaß aus $\mathsf{E} = 1$ folgt: $c_0 = \dots = c_n = 0$. Denn zunächst folgt nach Satz 11 aus $\mathsf{E} = 1$: $c_1 = \dots = c_n = 0$, also:

$$1 = \mathsf{H}_0^{c_0} \mathsf{H}^{1-\sigma} \xi$$

Für ungerades ℓ folgt daraus durch Normbildung:

$$1 = \xi_0^{c_0} \xi^{\ell},$$

also da ξ_0 als erzeugendes Element von K nicht ℓ–te Potenz in k sein kann, $c_0 = 0$.

42 IV

Für $\ell = 2$ folgt, falls $c_0 = 1$: $1 = -\xi_0 \xi^2$, also ξ_0 im wesentlichen $= -1$. Da dann die Relation $1 = \sqrt{-1}\mathsf{H}^{1-\sigma}\xi$ mit $\sqrt{-1} = \mathsf{H}'^2\xi'$ gleichbedeutend ist, folgt also, falls nicht der Spezialfall von *Zusatz S. 36* vorliegt, ebenfalls $c_0 = 0$. Sehen wir also von diesem Spezialfall vorläufig ab, so ist die obige Darstellung eindeutig in den $c_0, \ldots, c_n$.

Sei dann

$$\mathsf{E}_1 = \mathsf{H}_0^{c_0} \ldots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi$$

die Darstellung des ersten Basiselementes E_1 und wären alle $c_i = 0$, so folgte aus $n(\mathsf{E}_1) = 1$:

$$\xi^{\ell} = 1,$$

entweder also $\xi = 1$, oder $\xi = \zeta^c = (\mathsf{H}_0^c)^{\sigma-1}$, auf jeden Fall also

$$\mathsf{E}_1 = \mathsf{H}'^{1-\sigma}$$

was unmöglich. Es kann also wieder eins der H_i durch E_1 ersetzt werden. So fortfahrend gelangen wir zu einer eindeutigen Darstellung jeder Einheit E aus O in der Form:

$$\mathsf{E} = \mathsf{E}_1^{c_1} \ldots \mathsf{E}_{\varrho}^{c_{\varrho}} \mathsf{H}_{\varrho}^{c_{\varrho}} \ldots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi$$

(Dabei folgt dann wieder, wie oben, $\varrho \leqq n+1$). Dabei kann H_0 unter den stehen gebliebenen $\mathsf{H}_{\varrho}, \ldots, \mathsf{H}_n$ vorkommen oder auch ersetzt worden sein.

Ist nun $n(\mathsf{E}) = 1$, so folgt

$$\mathsf{E} = \mathsf{E}_1^{c'_1} \ldots \mathsf{E}_{\varrho}^{c'_{\varrho}} \mathsf{H}'^{1-\sigma}$$

also

$$1 = \mathsf{E}_1^{c_1 - c'_1} \ldots \mathsf{E}_{\varrho}^{c_{\varrho} - c'_{\varrho}} \mathsf{H}_{\varrho}^{c_{\varrho}} \ldots \mathsf{H}_n^{c_n} \mathsf{H}''^{1-\sigma} \xi$$

d.h.

$$c_1 - c'_1 = \cdots = c_{\varrho} - c'_{\varrho} = 0$$

Hauptsächlich aber:

$$c_{\varrho} = \cdots = c_n = 0.$$

Nun folgt wie oben für jede Relativnorm:

43 IV

$$\varepsilon = n(\mathsf{E}) = \eta_\varrho^{c_\varrho} \dots \eta_n^{c_n} \xi^\ell$$

und zwar eindeutig, da sonst eine Einheit

$$\mathsf{E}_0 = \mathsf{H}_\varrho^{b_\varrho} \dots \mathsf{H}_n^{b_n} \xi_0$$

mit $n(\mathsf{E}_0) = 1$ und nicht allen $b_i = 0$ folgte, was soeben als unmöglich erkannt wurde. Umgekehrt ist jede solche Einheit ε Relativnorm einer sofort angebbaren Einheit E aus O. Daher folgt wieder $v_0 = n+1-\varrho$, was wie oben wegen $\delta = 1$ die Behauptung liefert.

6.) Es möge schließlich der Spezialfall von *Zusatz S. 36*▸ vorliegen, also $K = k(\sqrt{-1})$ und $\sqrt{-1} = \xi' \mathsf{H}'^2 = \xi \mathsf{H}^{1-\sigma}$ sein. Dann ist die Darstellung für E a. S. 41▸ Mitte nicht eindeutig, vielmehr kann $\mathsf{H}_0^{c_0} = \sqrt{-1}^{c_0} = \xi^{c_0} (\mathsf{H}^{c_0})^{1-\sigma}$ in den Schluß hineingezogen werden, und es resultiert die nunmehr eindeutige Darstellung:

$$\mathsf{E} = \mathsf{H}_1^{c_1} \dots \mathsf{H}_n^{c_n} \mathsf{H}^{1-\sigma} \xi.$$

und alle Betrachtungen von 5.) übertragen sich wörtlich, nur daß das Basiselement H_0 □□□ fortfällt. Man kommt also zu $v_0 = n - \varrho$. Nun ist aber nach dem Zusatz S. 36▸ hier n um 1 größer als im vorigen Fall 5.), nämlich $r + 2 - \nu$, also $\varrho = r + 2 - \nu - v_0$, was wegen $\delta = 1$ die Behauptung liefert.

Damit ist Satz 12 vollständig bewiesen.

44 IV

D. Anzahl der ambigen Klassen

D. Die Anzahl der ambigen Klassen im relativ–zyklischen Körper K vom Primzahlgrad ℓ.

Definition 2. Ein Ideal $\mathfrak{A}$ aus K heißt ambig, wenn es nicht schon in k liegt und $\mathfrak{A} = \sigma\mathfrak{A}$, d.h. $\mathfrak{A}^{1-\sigma} = 1$ ist. Eine Idealklasse $\mathfrak{K}$ aus K heißt ambig, wenn $\mathfrak{K} = \sigma\mathfrak{K}$, d.h. $\mathfrak{K}^{1-\sigma} = 1$ ist.

Eine Klasse $\mathfrak{K}$ ist sicher ambig, wenn sie ein ambiges Ideal oder ein Ideal aus k oder das Produkt eines ambigen Ideals mit einem Ideal aus k enthält. Denn

ist $\mathfrak{A}\mathsf{j}$ ein solches Produkt, so entsteht die in absolutem Sinne verstandene Klasse $\mathfrak{K}$ von $\mathfrak{A}\mathsf{j}$ als

$$\mathfrak{K} = \mathfrak{A}\mathsf{j}(\mathsf{A}),$$

wo A alle Zahlen aus K durchläuft. Also wird

$$\sigma\mathfrak{K} = \sigma\mathfrak{A} \cdot \sigma\mathsf{j} \cdot (\sigma\mathsf{A}) = \mathfrak{A}\mathsf{j}(\sigma\mathsf{A})$$

und $\sigma\mathsf{A}$ durchläuft mit A alle Körperzahlen. Dasselbe gilt offenbar auch noch, wenn die Idealklassen in K nach einem solchen Strahl O definiert werden, wie er im vorigen Abschnitt zugrundelag, wenn also $\sigma O = O$ ist. Denn dann durchläuft $\sigma\mathsf{A}$ alle Zahlen von $\sigma O = O$, wenn A alle Zahlen von O durchläuft.

Umgekehrt kann es sehr wohl ambige Klassen geben, die keine ambigen Ideale enthalten.

Satz 13. Ein Primideal $\mathfrak{P}$ aus K ist dann und nur dann ambig, wenn es in der Relativdiskriminante von K aufgeht, also $\mathfrak{P}^\ell = \mathfrak{p}$ Primideal in k ist.

Beweis. Ist $\mathfrak{p} = \mathfrak{P}^\ell$ so ist natürlich $\sigma\mathfrak{P} = \mathfrak{P}$. Ist umgekehrt $\sigma\mathfrak{P} = \mathfrak{P}$ ein ambiges Primideal, und $\mathfrak{p}$ das zugehörige Primideal in k, so ist dessen Zerlegung nicht $\mathfrak{p} = \mathfrak{P}$, weil $\mathfrak{P}$ sonst Ideal aus k wäre (entgegen der Definition von ambig), auch nicht $\mathfrak{p} = \mathfrak{P}\mathfrak{P}_1 \dots \mathfrak{P}_{\ell-1}$ mit lauter verschiedenen Faktoren, da ja $\mathfrak{P}_1 = \sigma\mathfrak{P} = \mathfrak{P}$ folgte, also $\mathfrak{p} = \mathfrak{P}^\ell$.

Satz 14. Sind $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_d$ die d verschiedenen in der Relativdiskriminante von K aufgehenden, ambigen Primideale, so läßt sich jedes Ideal $\mathfrak{A}$ aus k, für das $\mathfrak{A}^{1-\sigma} = 1$ ist eindeutig in der Form darstellen:

$$\mathfrak{A} = \mathfrak{P}_1^{c_1}\mathfrak{P}_2^{c_2} \dots \mathfrak{P}_d^{c_d}\mathfrak{a}; \qquad (c_i = 0, 1, \dots, \ell - 1)$$

wo $\mathfrak{a}$ ein Ideal aus k ist. $\mathfrak{A}$ ist ferner dann und nur dann in k enthalten, wenn alle $u_i = 0$ sind. Soll $\mathfrak{A}$ Hauptideal in k sein, so muß $\mathfrak{a}$ Hauptideal sein.

Beweis. Aus $\mathfrak{A} = \sigma\mathfrak{A}$ folgt $n(\mathfrak{A}) = \mathfrak{A}^\ell$. Es ist also $\mathfrak{A}^\ell$ Ideal aus k. Ginge nun in $\mathfrak{A}$ ein $\mathfrak{P}^\lambda$ auf, wo $\mathfrak{P}$ ein nicht ambiges Primideal aus K, und auch nicht Ideal aus k ist, also $\mathfrak{p} = \mathfrak{P} \cdot \sigma\mathfrak{P} \dots \sigma^{(\ell-1)}\mathfrak{P}$ die Zerlegung des zugehörigen Primideals aus k ist, so wäre $\mathfrak{A}^\ell$ durch $\mathfrak{P}^{\lambda\ell}$, also als Ideal aus k durch $\mathfrak{p}^{\lambda\ell}$ teilbar, also $\mathfrak{A}$ selbst durch $\mathfrak{p}^\lambda$. Jedem solchen Faktor $\mathfrak{P}^\lambda$ entspricht also gleich der ganze Faktor $\mathfrak{p}^\lambda$ aus k. $\mathfrak{A}$ hat also die angegebene Form, wo die c_i wegen $\mathfrak{P}_i^\ell = \mathfrak{p}_i$ nach ℓ reduziert werden dürfen. Die Eindeutigkeit folgt aus der Eindeutigkeit der Primidealzerlegung. Liegt $\mathfrak{A}$ in k,

46 IV

so muß $\mathfrak{P}_1^{c_1} \dots \mathfrak{P}_d^{c_d}$ in k liegen, also durch $\mathfrak{p}_i = \mathfrak{P}_i^{\ell}$ teilbar sein, falls $c_i \neq 0$. Das ist wegen $c_i < \ell$ unmöglich, also $c_i = 0$. Ist zudem $\mathfrak{A}$ Hauptideal in k, so folgt aus $\mathfrak{A} = \mathfrak{a}$, daß auch $\mathfrak{a}$ es ist.

Satz 15. Die Gruppe der Ideale $\mathfrak{A}$ aus K, für die $\mathfrak{A}^{1-\sigma} = 1$ ist, hat in Bezug auf die Untergruppe der Hauptideale aus k den Index $\ell^d h$, wo h die absolute Klassenzahl von k und d die Anzahl der Diskriminantenteiler ist. In Bezug auf die Untergruppe der Hauptideale (A) aus K, für die $(\mathsf{A})^{1-\sigma} = 1$ ist, hat sie den Index $h\ell^{d-\varrho}$, wo ϱ die Bedeutung von Satz 12 hat, d.h. von der Gruppe $\mathfrak{A}^{1-\sigma} = 1$ werden genau $h\ell^{d-\varrho}$ (ambige) Idealklassen aus K in absolutem Sinne erzeugt.

Beweis. 1.) Der erste Teil folgt unmittelbar aus Satz 14.

2.) Sei D die Untergruppe der Hauptideale aus K, für die $(\mathsf{A})^{1-\sigma} = 1$ ist, D_0 die der Hauptideale aus k. Dann sind D und D_0 Untergruppen der zu untersuchenden Gruppe $\mathfrak{A}^{1-\sigma} = 1$ (bestehend aus allen ambigen Idealen aus K und den Idealen aus k), ferner ist D_0 Untergruppe von D. Wegen der multiplikativen Eigenschaft des Gruppenindex gilt dann für die drei ineinandergeschachtelten Gruppen: $\mathfrak{A}^{1-\sigma} = 1$, D, D_0:

$$h\ell^d = \mathfrak{j} \cdot (D : D_0),$$

wenn $\mathfrak{j}$ der gesuchte Index ist. Es ist also:

$$\mathfrak{j} = \frac{h\ell^d}{(D : D_0)},$$

47 IV

und somit nur noch $(D : D_0) = \ell^{\varrho}$ zu beweisen.

Seien dazu $\mathsf{E}_1, \dots, \mathsf{E}_{\varrho}$ die Einheiten von Satz 12[¶]. Nach Zahlbericht, Satz 90 (S. 272) gibt es dann ϱ Zahlen $\mathsf{A}_1, \dots, \mathsf{A}_{\varrho}$ aus K, sodaß

$$\mathsf{E}_i = \mathsf{A}_i^{1-\sigma}; \qquad (i = 1, 2, \dots, \varrho)$$

ist. A_i ist sicher keine Einheit, da nach Satz 12 die E_i von der Gruppe $\mathsf{H}^{1-\sigma}$ unabhängig sind. Also ist, wenn $\mathfrak{A}_i = (\mathsf{A}_i)$ gesetzt wird:

$$\mathfrak{A}_i^{1-\sigma} = 1; \qquad \mathfrak{A}_i \neq 1; \qquad (i = 1, 2, \dots, \varrho).$$

[¶] Als Strahlen O und o sind hier alle Körperzahlen zu nehmen.

Wäre nun

$$\mathfrak{A}_1^{c_1} \dots \mathfrak{A}_\varrho^{c_\varrho} = (\alpha) \quad \text{mit} \quad c_i = 0, 1, \dots, \ell - 1$$

ein Hauptideal aus k, so folgte

$$\mathsf{A}_1^{c_1} \dots \mathsf{A}_\varrho^{c_\varrho} = \alpha \mathsf{H}; \qquad (\mathsf{H} \text{ Einheit aus } K),$$

also

$$\mathsf{E}_1^{c_1} \dots \mathsf{E}_\varrho^{c_\varrho} = \mathsf{H}^{1-\sigma}$$

und somit nach Satz 12: $c_1, \dots, c_\varrho = 0.$

Andererseits sei $\mathfrak{A} = (\mathsf{A})$ ein beliebiges Hauptideal aus K mit $\mathfrak{A}^{1-\sigma} = 1$, also $\mathsf{A}^{1-\sigma} = \mathsf{E}$ und E Einheit in K mit $n(\mathsf{E}) = 1$. Dann ist nach Satz 12:

$$\mathsf{E} = \mathsf{E}_1^{c_1} \dots \mathsf{E}_\varrho^{c_\varrho} \mathsf{H}^{1-\sigma}; \qquad (c_i = 0, 1, \dots, \ell - 1)$$

also $$\mathsf{A}^{1-\sigma} = (\mathsf{A}_1^{c_1} \dots \mathsf{A}_\varrho^{c_\varrho} \mathsf{H})^{1-\sigma}.$$

Nun folgt aus $\mathsf{A}^{1-\sigma} = \mathsf{B}^{1-\sigma}$ daß $\left(\frac{\mathsf{A}}{\mathsf{B}}\right)^{1-\sigma} = 1$, also $\frac{\mathsf{A}}{\mathsf{B}} = \sigma\left(\frac{\mathsf{A}}{\mathsf{B}}\right)$ Zahl α aus k ist. Es gilt also

$$\mathsf{A} = \mathsf{A}_1^{c_1} \dots \mathsf{A}_\varrho^{c_\varrho} \mathsf{H} \alpha$$

oder $$\mathfrak{A} = \mathfrak{A}_1^{c_1} \dots \mathfrak{A}_\varrho^{c_\varrho} (\alpha); \qquad (c_i = 0, 1, \dots, \ell - 1)$$

Die Ideale $\mathfrak{A}_1, \dots, \mathfrak{A}_\varrho$ bilden also eine Basis für die

48 IV

Gruppe D aller Hauptideale $\mathfrak{A} = (\mathsf{A})$ mit $\mathfrak{A}^{1-\sigma} = 1$ aus K in Bezug auf die Untergruppe D_0 aller Hauptideale (α) aus k. (Daß die Nebengruppen alle zum Exponenten ℓ gehören, wie es bei einer derartigen Basisdarstellung notwendig sein muß, folgt leicht so: Wegen

$$1 + \sigma + \dots + \sigma^{\ell-1} = \ell + (\sigma - 1)Q(\sigma)$$

ist $$n(\mathfrak{A}) = \mathfrak{A}^\ell (\mathfrak{A}^{\sigma-1})^{Q(\sigma)} = \mathfrak{A}^\ell$$

d.h. $$\mathfrak{A}^\ell = n(\mathfrak{A}) = \big(n(\mathsf{A})\big) = (\alpha) \text{ Hauptideal in } k\ \Big).$$

Aus dem Bewiesenen folgt sofort $(D : D_0) = \ell^\varrho$, w.z.b.w.

Satz 16. Die Idealklassen in K und k seien in absolutem Sinne definiert. ℓ^v sei die Anzahl der Einheitenverbände in k, die durch Relativnormen von

Einheiten und gebrochenen Zahlen von K gebildet werden. Die übrigen Bezeichnungen seien die früheren. Dann ist die Anzahl a der ambigen Klassen in K:

$$\begin{array}{rcll} a & = & h\ell^{d+v-(r+\delta+1)} & \text{für} \quad \ell \neq 2, \\ a & = & h\ell^{d+v+\nu-(r+2)} & \text{für} \quad \ell = 2. \end{array}$$

Beweis. 1.) Ist $n(\Theta) = \varepsilon$ eine Einheit in k, so ist für jede Einheit η aus k: $\varepsilon\eta^{\ell} = n(\Theta\eta)$. Die Relativnormen machen also wirklich immer ganze Einheitenverbände aus.

2.) Die ℓ^v Relativnormverbände in k bilden eine Abelsche Gruppe, in der jedes Element den Exponenten ℓ hat. Es gibt also im ganzen v Basiselemente, die durch je eine Einheit als charakteristisch für den zugehörigen Verband charakterisiert werden können. v_0 von diesen

Einheiten werden nach der Terminologie von Satz 12 durch Relativnormen von Einheiten aus K erzeugt. Es gibt also noch $v - v_0$ von diesen in Bezug auf den Hauptverband η^{ℓ} unabhängige Einheiten, die als Relativnormen gebrochener Zahlen aus K geliefert werden. Es seien dies:

$$\varepsilon_1 = n(\Theta_1);\ \ldots\ ;\ \varepsilon_{v-v_0} = n(\Theta_{v-v_0}).$$

Dann hat also, wenn wir die Relativnormen von Einheiten zusammenziehen, ebenso die ℓ–ten Potenzen von Einheiten in k als Relativnormen schreiben, jede Relativnormeinheit aus k die Gestalt:

$$\varepsilon = \varepsilon_1^{c_1} \ldots \varepsilon_{v-v_0}^{c_{v-v_0}} n(\mathsf{H}); \qquad (c_i = 0, 1, \ldots, \ell - 1),$$

wo H eine Einheit aus K ist. Aus der Eindeutigkeit dieser Darstellung (als Basisdarstellung der Abelschen Gruppe) ergibt sich, daß aus $\varepsilon = 1$ notwendig $c_i = 0$ folgt.

Es sei nun

$$(\Theta_i) = \prod \mathfrak{P}^{F_i(\sigma)}$$

erstreckt über die verschiedenen, zueinander nicht konjugierten Primteiler von Θ_i in K. Wegen $n(\Theta_i) = \varepsilon_i$ ist also

$$\prod \mathfrak{P}^{(1+\sigma+\cdots+\sigma^{\ell-1})F_i(\sigma)} = 1$$

Wird nun $F_i(\sigma)$ nach Potenzen von $\sigma - 1$ entwickelt:

$$F_i(\sigma) = a_i + (\sigma - 1)\Phi_i(\sigma),$$

so ist

$$(1+\sigma+\cdots+\sigma^{\ell-1})F_i(\sigma) = (1+\sigma+\cdots+\sigma^{\ell-1})a_i$$

weil

$$(1+\sigma+\cdots+\sigma^{\ell-1})(\sigma-1) = \sigma^\ell - 1 = 0$$

ist.

50 IV

Es wird also

$$\prod \mathfrak{P}^{a_i(1+\sigma+\cdots+\sigma^{\ell-1})} = \prod n(\mathfrak{P})^{a_i} = 1$$

also, da die $n(\mathfrak{P})$ alle verschiedene Primidealpotenzen in k sind, $a_i = 0$, d.h.

$$F_i(\sigma) = (\sigma-1)\phi_i(\sigma).$$

Es kann also

$$(\Theta_i) = \mathfrak{A}_i^{1-\sigma}$$

gesetzt werden. Setzen wir wieder

$$\ell = (1+\sigma+\cdots+\sigma^{\ell-1})\varphi(\sigma) + (1-\sigma)\psi(\sigma),$$

so wird

$$\mathfrak{A}_i^\ell = n(\mathfrak{A}_i)^{\varphi(\sigma)}(\mathfrak{A}_i^{1-\sigma})^{\psi(\sigma)} = \mathfrak{a}_i(\Theta_i)^{\psi(\sigma)}.$$

Wäre nun

$$\mathfrak{A}_1^{c_1}\ldots\mathfrak{A}_{v-v_0}^{c_{v-v_0}} = \overline{\mathfrak{A}}(\mathsf{A})$$

wo $\overline{\mathfrak{A}}^{1-\sigma} = 1$ und (A) Hauptideal aus K ist, so dürften zunächst nach dem eben gezeigten alle Exponenten c_i mod ℓ reduziert angenommen werden, da der Faktor $\mathfrak{a}_i$ unbeschadet $\overline{\mathfrak{A}}^{1-\sigma} = 1$ in $\overline{\mathfrak{A}}$, der Faktor $(\Theta_i)^{\psi(\sigma)}$ in (A) gezogen werden kann. Dann folgte durch Erheben in die $(1-\sigma)$–te Potenz

$$\Theta_1^{c_1}\ldots\Theta_{v-v_0}^{c_{v-v_0}} = \mathsf{H}\mathsf{A}^{1-\sigma}; \qquad (\mathsf{H} \text{ Einheit aus } K)$$

also durch Normbildung:

$$\varepsilon_1^{c_1}\ldots\varepsilon_{v-v_0}^{c_{v-v_0}} = n(\mathsf{H}),$$

sodaß nach dem vorigen $c_1,\ldots,c_{v-v_0} = 0$ sein muß. Das bedeutet aber, daß die durch $\mathfrak{A}_i$ definierten, wegen $\mathfrak{A}_i^{1-\sigma}(\Theta_i)$ offenbar ambigen Klassen in Bezug auf

51 IV

die ambigen Klassen mit ambigen Idealen $\big($d.h. genauer die Klassen der Form $\overline{\mathfrak{A}}^{1-\sigma}(\mathsf{A})\big)$ unabhängig sind.

(Die durch die $\mathfrak{A}_i$ gelieferten ambigen Klassen enthalten also weder ambige Ideale, noch überhaupt Ideale, für die $\overline{\mathfrak{A}}^{1-\sigma} = 1$ ist).

Ist andererseits $\mathfrak{A}$ ein Ideal aus irgendeiner ambigen Klasse, also $\mathfrak{A}^{1-\sigma} = (\Theta)$ ein Hauptideal in K, so ist

$$n\big((\Theta)\big) = 1$$

also $$n(\Theta) = \varepsilon$$

eine Einheit in k, somit

$$\varepsilon = \varepsilon_1^{c_1} \dots \varepsilon_{v-v_0}^{c_{v-v_0}} n(\mathsf{H}); \qquad (\mathsf{H} \text{ Einheit aus } K) \quad (c_i = 0, 1, \dots, \ell - 1)$$

und $n(\Theta) = n\left(\Theta_1^{c_1} \dots \Theta_{v-v_0}^{c_{v-v_0}} \mathsf{H}\right)$. Nach dem Satz aus dem Zahlbericht (S. 272) ist also

$$\Theta = \Theta_1^{c_1} \dots \Theta_{v-v_0}^{c_{v-v_0}} \mathsf{H}\mathsf{A}^{1-\sigma}$$

d.h.

$$\mathfrak{A}^{1-\sigma} = \left(\mathfrak{A}_1^{c_1} \dots \mathfrak{A}_{v-v_0}^{c_{v-v_0}}(\mathsf{A})\right)^{1-\sigma}$$

Somit ist

$$\mathfrak{A} = \mathfrak{A}_1^{c_1} \dots \mathfrak{A}_{v-v_0}^{c_{v-v_0}}(\mathsf{A})\overline{\mathfrak{A}}, \quad \text{wo} \quad \overline{\mathfrak{A}}^{1-\sigma} = 1.$$

Jedes Ideal einer ambigen Klasse läßt sich also in Bezug auf die Untergruppe $\overline{\mathfrak{A}}(\mathsf{A})$ mit $\overline{\mathfrak{A}}^{1-\sigma} = 1$ eindeutig durch die Basis $\mathfrak{A}_1, \dots, \mathfrak{A}_{v-v_0}$ mit Exponenten $c_i = 0, 1, \dots, \ell - 1$ darstellen.

Zusammenfassend haben wir also:

Die Gruppe G aller ambigen Klassen ist in Bezug auf die Untergruppe der Klassen $\overline{\mathfrak{A}}(\mathsf{A})$ mit $\overline{\mathfrak{A}}^{1-\sigma} = 1$, d.h. der Klassen die aus ambigen Idealen und Idealen aus k entspringen von endlichem Index. Die Faktorgruppe ist vom

52 IV

Grade ℓ^{v-v_0} und Typus $(\ell, \ell, \dots, \ell)$. Der Gruppenindex ist ℓ^{v-v_0}.

Nach Satz 15 erzeugen die ambigen Ideale und Ideale aus k genau $h\ell^{d-\varrho}$ Klassen, sodaß die Anzahl aller ambigen Klassen

$$a = h\ell^{d-\varrho+v-v_0} = h\ell^{v+d-(\varrho+v_0)}$$

ist. Nach Satz 12 ist

$$\varrho = \begin{cases} r+\delta+1-v_0 & \text{für} \quad \ell \neq 2, \\ r+\delta+1-v-v_0 & \text{für} \quad \ell = 2. \end{cases}$$

Für $\ell = 2$ ist sicher $\delta = 1$, da k die 2–te Einheitswurzel -1 enthält. Somit wird

$$a = \begin{cases} h\ell^{d+v-(r+\delta+1)} & \text{für} \quad \ell \neq 2, \\ h\ell^{d+v+\nu-(r+2)} & \text{für} \quad \ell = 2. \end{cases}$$

Damit ist Satz 16 bewiesen.

E. Die Geschlechter für $\ell \neq 2$

E. Die Geschlechter für ungerades ℓ.

Sei ℓ ungerade und $f^{\ell-1}$ die Relativdiskriminante von K. Da immer eine ganze Restklasse gleichzeitig Normenrest oder Nichtrest ist, bildet die Gesamtheit der Normenreste mod $\mathfrak{f}$ von K einen Strahl o nach dem Modul $\mathfrak{f}$ in k. Nach diesem Strahl o seien die Idealklassen in k definiert und h_1 die zugehörige Klassenzahl. Diese ist nach A.Z. I, S.112:

$$h_1 = \frac{(o_1 : o)}{(E_1 : E)} h$$

wenn o_1 den Strahl aller zu $\mathfrak{f}$ primen Körperzahlen und E_1 und E die Gruppen der Einheiten in o_1 (in k) und o bedeuten.

Der Gruppenindex $(o_1 : o)$ kann aus den entsprechenden Anzahlen von Restklassen mod $\mathfrak{f}$ bestimmt werden, die o_1 und o zusammensetzen. Nach Satz 9, S. 24 ist genau der ℓ^d–te Teil der $\Phi(\mathfrak{f})$ Restklassen von o_1 in o enthalten, wenn d verschiedene Primteiler in $\mathfrak{f}$ aufgehen. Daher ist $(o_1 : o) = \ell^d$.

$(E_1 : E)$ bestimmt sich aus den entsprechenden Anzahlen von Einheitenverbänden von o_1, die E_1 und E zusammensetzen. E_1 besteht aus $\ell^{r+\delta}$ Einheitenverbänden o_1; in E gehen wirklich auch immer ganze Verbände von o_1 ein, da mit ε natürlich auch jedes $\varepsilon\eta^\ell$ Normenrest mod $\mathfrak{f}$ ist. Es mögen ℓ^n Einheitenverbände von o_1 in E liegen. Dann ist $(E_1 : E) = \ell^{r+\delta-n}$.

Damit wird

$$h_1 = h\ell^{d+n-(r+\delta)}. \tag{1}$$

54 IV

Die Idealklassen in K seien in absolutem Sinne definiert, aber nur die zu $\mathfrak{f}$ primen Ideale in Betracht gezogen. Sind dann $\mathfrak{A}$, $\mathfrak{B}$ zwei äquivalente Ideale aus K, also

$$\mathfrak{A} = (\mathsf{A})\mathfrak{B},$$

so folgt

$$n(\mathfrak{A}) = \big(n(\mathsf{A})\big) \cdot n(\mathfrak{B}).$$

Das Hauptideal $\big(n(\mathsf{A})\big)$ aus k gehört dann zur Hauptklasse unserer Klasseneinteilung in k, da $n(\mathsf{A})$ sicher Normenrest ist. Die Ideale $n(\mathfrak{A})$ und $n(\mathfrak{B})$ gehören also derselben Klasse in k an. Es ist somit jeder Klasse $\mathfrak{K}$ von K eine bestimmte Klasse $\mathfrak{k}$ von k nach o zugeordnet, die wir mit

$$\mathfrak{k} = n(\mathfrak{K})$$

bezeichnen.

Offenbar ist $n(\mathfrak{K}_1\mathfrak{K}_2) = n(\mathfrak{K}_1)\cdot n(\mathfrak{K}_2)$, sodaß die Relativnormen der Klassen $\mathfrak{K}$ eine Klassengruppe H in k bilden, die nach dem Modul $\mathfrak{f}$ definierbar ist. Wir nennen deren Index in Bezug auf die Gruppe G aller h_1 Klassen nach o:

$$(G : \mathsf{H}) = i.$$

Dann ist die Klassengruppe H dem Körper K in dem Sinne zugeordnet, daß sie aus allen Klassen nach o besteht, die Relativnormen von Idealen aus K enthalten. Daher ist nach A.Z. II, S. 142, Satz 7:

$$i \leqq \ell. \tag{2}$$

55 IV

In H kommt sicher die Hauptklasse $\mathfrak{k}_0$ nach o vor, und es seien $\mathfrak{K}_0, \mathfrak{K}_1, \ldots,$ $\mathfrak{K}_{t-1}$ alle Klassen aus K, deren Relativnormen $\mathfrak{k}_0$ sind. Auch sie bilden eine

Gruppe H_0. Jede Nebengruppe zu H_0 enthält immer gerade alle und nur die Klassen, deren Relativnormen sich nur um $\mathfrak{k}_0$ unterscheiden, also identisch sind.

Definition 3. Alle Klassen aus K, deren Relativnorm ein und dieselbe Klasse aus k nach o ist, bilden ein *Geschlecht*. Insbesondere ist das *Hauptgeschlecht* diejenige Klassengruppe H_0 in K, deren Relativnorm die Hauptklasse nach o in k ist. Die übrigen Geschlechter (Nebengeschlechter) werden durch die Nebengruppen zu H_0 gebildet.

Es gibt also ebensoviel Nebengruppen zu H_0, d.h. Geschlechter, als es Klassen nach o in k gibt, die Relativnormen von Klassen aus K sind, d.h. als der Grad der Klassengruppe H beträgt. Bezeichnet demnach G_0 die Gruppe aller Klassen aus K, so ist die Anzahl der Geschlechter:

$$(G_0 : \mathsf{H}_0) = \frac{h_1}{i} \geqq \frac{h_1}{\ell} \tag{3}$$

Wir bezeichnen nun mit H^0 die Gruppe aller Klassen aus K, die symbolische $(1-\sigma)$–te Potenzen von Klassen aus K sind. Da $\sigma\mathfrak{K}$ die gleiche Norm wie $\mathfrak{K}$ hat,

ist $n(\mathfrak{K}^{1-\sigma}) = \mathfrak{k}_0$ die Hauptklasse, also H^0 Untergruppe von H_0 und

$$(G_0 : \mathsf{H}^0) \geqq (G_0 : \mathsf{H}_0). \tag{4}$$

Der Gruppenindex $(G_0 : \mathsf{H}^0)$ läßt sich aber mittels der Anzahl der ambigen Klassen in K bestimmen. Ist nämlich $\mathfrak{K}^0 = \mathfrak{K}^{1-\sigma}$ eine Klasse aus H^0, so wird dasselbe $\mathfrak{K}^0$ auch von $\mathfrak{K}\mathfrak{K}_i$ erzeugt, wo $\mathfrak{K}_i$ eine ambige Klasse ist. Ist umgekehrt $\mathfrak{K}_1^{1-\sigma} = \mathfrak{K}_2^{1-\sigma}$, so ist $\left(\frac{\mathfrak{K}_1}{\mathfrak{K}_2}\right)^{1-\sigma} = 1$, also $\frac{\mathfrak{K}_1}{\mathfrak{K}_2}$ eine ambige Klasse. Ist also a die Anzahl der ambigen Klassen, so erzeugen immer genau a Klassen und nicht mehr die gleiche Klasse $\mathfrak{K}^\bullet$ aus H^0. Ist also H die (absolute) Klassenzahl von K, d.h. der Grad von G_0, g der (nicht weiter interessierende) Grad von H^0, so ist

$$g = \frac{H}{a}$$

also der gesuchte Index von H^0:

$$(G_0 : \mathsf{H}_0) = \frac{H}{g} = a = h\ell^{d+v-(r+\delta+1)}. \tag{5}$$

Aus den Relationen (1) – (5) folgt nun folgende fundamentale Ungleichungsfolge:

$$(6)\quad a = h\ell^{d+v-(r+\delta+1)} = (G_0 : \mathsf{H}^0) \geqq (G_0 : \mathsf{H}_0) = \frac{h_1}{i} \geqq \frac{h_1}{\ell} = h\ell^{d+n-(r+\delta+1)}.$$

57 IV

Es ist somit $v \geqq n$. Nun ist aber v die Anzahl der unabhängigen Einheitenverbände aus k, die durch Relativnormen von Zahlen aus K geliefert werden, n die Anzahl der unabhängigen Einheitenverbände aus o_1, d.h. aus k, die in E, d.h. in o liegen, also die Normenreste mod $\mathfrak{f}$ sind. Erstere sind somit unter letzteren enthalten d.h. $v \leqq n$. Daraus folgt:

$$(7)\qquad n = v.$$

Es muß daher in (6), also auch (2), (3), (4) überall das Gleichheitszeichen gelten. Wir haben demnach:

$$(2a.)\qquad i = \ell,$$

$$(4a.)\qquad \mathsf{H}_0 = \mathsf{H}^0,$$

$$(6a.)\qquad a = \frac{h_1}{\ell} = (G_0 : \mathsf{H}_0).$$

Aus (6a.) folgt:

Satz 17. Die Anzahl der Geschlechter von K ist gleich dem ℓ–ten Teil der Klassenzahl h_1 des Körpers k nach o und gleich der Anzahl der ambigen Klassen des Körpers K. Die Klassenzahl H des Körpers K ist teilbar durch $\frac{h_1}{\ell}$, speziell also, wenn die absolute Klassenzahl h von k prim zu ℓ ist oder wenn $h_1 > h$ ist, teilbar durch h.

Aus (4a.) folgt:

Satz 18. Jede Klasse des Hauptgeschlechts ist die symbolische $(1-\sigma)$–te Potenz $\mathfrak{K}^{1-\sigma}$ einer Klasse $\mathfrak{K}$ von K, das Hauptgeschlecht also der Inbegriff aller Klassen $\mathfrak{K}^{1-\sigma}$ von K.

58 IV

Aus (7) folgt:

Satz 19. Wenn eine Einheit aus k Normenrest von K nach dem Modul $\mathfrak{f}$ ist, so ist sie Relativnorm einer Einheit oder gebrochenen Zahl aus K.

Daraus ergibt sich noch folgender Satz:

Satz 20. Wenn eine zu $\mathfrak{f}$ prime Zahl α aus k die ℓ–te Potenz eines Ideals $\mathfrak{a}$ aus k und überdies Normenrest mod $\mathfrak{f}$ ist, so ist sie Relativnorm einer Zahl aus K.

Beweis. Sei $(\alpha) = \mathfrak{a}^i$ und α Normenrest von K mod $\mathfrak{f}$. Dann ist

$$n(\mathfrak{a}) = \mathfrak{a}^\ell = (\alpha).$$

$\mathfrak{a}$ gehört also als Ideal aus K betrachtet zum Hauptgeschlecht, da seine Relativnorm in der Hauptklasse von k nach o liegt. Also ist nach Satz 18:

$$\mathfrak{a} = \mathfrak{A}^{1-\sigma}(\mathsf{A}),$$

wo $\mathfrak{A}$ ein Ideal und A eine Zahl aus K bedeutet. Durch Normbildung folgt

$$\alpha = \varepsilon n(\mathsf{A}),$$

wo ε Einheit aus k ist. Es ist somit ε Normenrest mod $\mathfrak{f}$, also nach Satz 19:

$$\varepsilon = n(\mathsf{B}),$$

also $$\alpha = n(\mathsf{AB}), \qquad \text{w.z.b.w.}$$

Aus (2a.) folgt endlich nach Definition des Klassenkörpers:

59 IV

Satz 21. Sei K ein relativ–zyklischer Körper vom ungeraden Primzahlgrad ℓ über k, ferner $\mathfrak{f}^{\ell-1}$ seine Relativdiskriminante. Dann ist K Klassenkörper zu k für eine nach dem Modul $\mathfrak{f}$ erklärbare Klassengruppe H aus k vom Index ℓ (ohne Vorzeichenbedingungen). H ist also jedenfalls nach dem Strahl „$\equiv 1 \bmod \mathfrak{f}$“ ohne Vorzeichenbedingung erklärbar.

F. Die Geschlechter für $\ell = 2$

F. Die Geschlechter im relativ–quadratischen Körper.

Für $\ell = 2$ lassen sich die vorstehenden Betrachtungen deshalb nicht unverändert durchführen, weil hier in der fundamentalen Ungleichungsfolge (6)

für das linksstehende a der Wert $h\ell^{d+v+\nu-(r+2)}$ gesetzt werden muß, der mit dem rechtsstehenden $h\ell^{d+n-(r+2)}$ — (es ist $\delta = 1$) — verglichen für $\nu > 0$ nicht $v \geqq n$ zu schließen erlaubt. Man muß hier also auch in den rechtsstehenden, als $\frac{h_1}{\ell}$ hereinkommenden Ausdruck das ν hereinbringen, also die Klassenzahl h_1 entsprechend vergrößern, und dies kann durch Zugrundelegung eines engeren Klassenbegriffs im Körper k bewirkt werden.

Dementsprechend wählen wir den Strahl o hier so:

60 IV

α gehört zu o, wenn

1.) α Normenrest mod $\mathfrak{f}$,

2.) α positiv in den ν reellen zu k konjugierten Körpern, in denen μ negativ ist.

Dabei ist wie früher $K = k(\sqrt{\mu})$ gesetzt. Daß o ein Kongruenzstrahl mod $\mathfrak{f}$ ist, ist unmittelbar klar. Es mögen die Klassen in k nach dem Strahl o definiert werden. Für die Klassenzahl h_1 nach o gilt dann wie oben:

$$h_1 = \frac{(o_1 : o)}{(E_1 : E)} h,$$

wo h die absolute Klassenzahl von k, o_1 die Gruppe aller zu $\mathfrak{f}$ primen Körperzahlen und E_1 und E die o_1 und o entsprechenden Einheitengruppen sind.

Der Gruppenindex $(o_1 : o)$ bestimmt sich hier so: Zunächst ist wieder der 2^d–te Teil aller primen Restklassen mod $\mathfrak{f}$ Normenrest, wenn d verschiedene Primteiler in $\mathfrak{f}$ aufgehen. Jede solche Restklasse hat Zahlen aller Signaturen. Schränkt man diese Signaturen noch durch die obigen ν Forderungen ein, so wird von jeder Restklasse nur der 2^ν–te Teil beibehalten. Es ist also $(o_1 : o) = 2^{d+\nu}$.

Zur Bestimmung von $(E_1 : E)$ gehen wir wieder auf die Einheitenverbände zurück. Wegen $\delta = 1$ enthält o_1 genau 2^{r+1} Einheitenverbände. Ist ferner ε Einheit aus o, als Normenrest mod $\mathfrak{f}$ mit Vorzeichenbedingung, so ist der ganze Verband $\varepsilon\eta^2$, den ε in o_1 bestimmt,

61 IV

zu o gehörig, da η^2 einerseits $n(\eta)$, andererseits total positiv ist. Wieder machen also die Einheiten von o ganze Verbände von o_1 aus. Sei 2^n die Anzahl der Einheitenverbände von o_1, aus denen E besteht, dann ist

$$(E_1 : E) = 2^{r+1-n}$$

Damit wird:

$$h_1 = h2^{d+n+\nu-(r+1)}.$$

Die Idealklassen in K seien wieder in absolutem Sinne erklärt, unter Beschränkung auf die zu $\mathfrak{f}$ primen Ideale. Sind $\mathfrak{A}$, $\mathfrak{B}$ zwei äquivalente Ideale aus K, also

$$\mathfrak{A} = (\mathsf{A})\mathfrak{B},$$

so ist

$$n(\mathfrak{a}) = \big(n(\mathsf{A})\big)n(\mathfrak{B}).$$

Ist nun μ_i negativ, der Körper $K_i = k_i(\sqrt{\mu_i})$ also imaginär, so ist $n(\mathsf{A}_i) = \mathsf{A}_i\mathsf{A}_i'$ als Produkt zweier konjugiert–komplexen Zahlen positiv in k_i, also $n(\mathsf{A})$ sicher Zahl aus o. Wieder haben also die Ideale einer Klasse von K nach o äquivalente Relativnormen in k, sodaß jeder Klasse $\mathfrak{K}$ von K eine bestimmte Klasse

$$\mathfrak{k} = n(\mathfrak{K})$$

nach o von k zugeordnet ist.

Die weiteren Betrachtungen des vorigen Abschnitts übertragen sich dann wörtlich und führen zu der Ungleichungsfolge

$$a = h\ell^{d+v+\nu-(r+2)} = (G_0 : \mathsf{H}^0) \geqq (G_0 : \mathsf{H}_0) = \frac{h_1}{i} \geqq \frac{h_1}{\ell} = h\ell^{d+n+\nu-(r+2)},$$

62 IV

die wie oben auf $v \geqq n$ und somit $v = n$ zu schließen erlaubt, weil v die Anzahl der unabhängigen Einheitenverbände in k ist, die aus Relativnormen von K entspringen, während n die Anzahl der unabhängigen Einheitenverbände in o_1, d.h. k, ist, die in E, d.h. in o liegen, also Normenreste mod $\mathfrak{f}$ mit Vorzeichenbedingung sind, und jede Einheit $\varepsilon = n(\mathsf{A})$ aus jenen v Verbänden

1.) Normenrest mod $\mathfrak{f}$ ist,

2.) die Vorzeichenbedingung erfüllt (s. S. 61▶ Mitte), also zu den n Verbänden gehört.

Satz 17, 18 übertragen sich wörtlich, Satz 19 lautet hier so:

Satz 19a. Wenn eine Einheit aus k Normenrest von K nach dem Modul $\mathfrak{f}$ und in den ν „kritischen“ Körpern positiv ist, so ist sie Relativnorm einer Einheit oder gebrochenen Zahl aus K[5].

[5] undeutlich

Satz 20 geht über in:

Satz 20a. Wenn eine zu $\mathfrak{f}$ prime Zahl α aus k Quadrat eines Ideals $\mathfrak{a}$ aus k, überdies Normenrest von K mod $\mathfrak{f}$ und in den ν kritischen Körpern positiv ist, so ist sie Relativnorm einer Zahl aus k.

Beweis. Der Beweis zu Satz 20 überträgt sich wörtlich, wenn man bemerkt, daß das dortige $n(\mathsf{A})$ in den ν kritischen Körpern positiv ist.

Endlich wird Satz 21 zu:

Satz 21a. Sei $K = k(\sqrt{\mu})$ relativ–quadratisch zu k und $\mathfrak{f}$ seine Relativdiskriminante. Dann ist K Klassenkörper zu k für eine Klassengruppe H vom Index 2, die nach dem Modul $\mathfrak{f}$ mit Vorzeichenbedingungen erklärbar ist. H ist also jedenfalls nach dem Strahl „$\equiv 1 \bmod \mathfrak{f}$, total positiv“ erklärbar.

63 IV

G. Verallgemeinerung des Geschlechtsbegriffes

□□□

64 IV

Ich beweise zunächst drei anzuwendende Hilfssätze:

Hilfssatz 1. Ist $\mathfrak{p}$ ein beliebiges Primideal aus k und Θ eine zu $\mathfrak{p}$ prime Zahl aus der zu $\mathfrak{p}$ gehörigen Henselschen Erweiterung $K_\mathfrak{p}$ von K, für die

$$n(\Theta) = 1 \ (\mathfrak{p})$$

ist, so gibt es in $K_\mathfrak{p}$ eine Zahl A, sodaß

$$\Theta = \mathsf{A}^{1-\sigma} \ (\mathfrak{p})$$

ist. Falls $\mathfrak{p}$ nicht in der Relativdiskriminante von K aufgeht, darf A prim zu $\mathfrak{p}$ angenommen werden.

Beweis. Es sind die beiden Fälle zu unterscheiden:

1.) $\mathfrak{p} = \mathfrak{P}_1.\mathfrak{P}_2 \dots \mathfrak{P}_\ell$,

2.) $\mathfrak{p} = \mathfrak{P}$ oder $\mathfrak{P}^\ell$.

1.) $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_\ell = \mathfrak{P} \cdot \sigma\mathfrak{P} \dots \sigma^{\ell-1}\mathfrak{P}.$

Dann ist $K_\mathfrak{p}$ ein aus ℓ Kongruenzkörpern $k(\mathfrak{p})$ zusammengesetzter Kongruenzring und durch die Substitutionen σ^c vertauschen sich diese ℓ Kongruenzkörper. Ihre Reihenfolge darf so angenommen werden, daß sie bei σ zyklisch um eins vorrücken. Jedes Element A aus $K_\mathfrak{p}$ hat dann

eine eindeutige Komponentendarstellung

$$\mathsf{A} = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)\ (\mathfrak{p})$$

durch ℓ Elemente aus $k(\mathfrak{p})$ und es wird

$$\sigma\mathsf{A} = (\alpha_\ell, \alpha_1, \ldots, \alpha_{\ell-2}, \alpha_{\ell-1}),$$

weil aus $\mathsf{A} = \alpha_i(\sigma^{i-1}\mathfrak{P})$ folgt $\sigma\mathsf{A} = \alpha_i(\sigma^i\mathfrak{P})$.

Ist nun

$$\Theta = (\vartheta_1, \vartheta_2, \ldots, \vartheta_\ell)\ (\mathfrak{p}),$$

so sind alle Komponenten ϑ_i prim zu $\mathfrak{p}$, weil es n. V. Θ ist, und ferner besteht die Relation

$$n(\Theta) = \vartheta_1\vartheta_2 \ldots \vartheta_\ell = 1\ (\mathfrak{p}).$$

Aus diesem Grunde läßt sich ersichtlich das Gleichungssystem

$$\vartheta_1 = \frac{\alpha_1}{\alpha_\ell}; \quad \vartheta_2 = \frac{\alpha_2}{\alpha_1}; \quad \ldots; \quad \vartheta_\ell = \frac{\alpha_\ell}{\alpha_{\ell-1}}$$

durch ℓ zu $\mathfrak{p}$ prime Zahlen $\alpha_1, \ldots, \alpha_\ell$ aus $k(\mathfrak{p})$ lösen. Setzt man dann

$$\mathsf{A} = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$$

so wird

$$\mathsf{A}^{1-\sigma} = \frac{\mathsf{A}}{\sigma\mathsf{A}} = \left(\frac{\alpha_1}{\alpha_\ell}, \frac{\alpha_2}{\alpha_1}, \ldots, \frac{\alpha_\ell}{\alpha_{\ell-1}}\right) = \Theta\ (\mathfrak{p}).$$

A ist also eine zu $\mathfrak{p}$ prime Zahl der verlangten Eigenschaft.

2.) $\mathfrak{p} = \mathfrak{P}$ oder $\mathfrak{P}^\ell$.

Dann ist $K_\mathfrak{p} = K(\mathfrak{P})$ ein Körper ℓ–ten Grades über $k(\mathfrak{p})$, und es folgt die Existenz eines A, für das $\Theta = \mathsf{A}^{1-\sigma}\ (\mathfrak{p})$ wörtlich ebenso, wie im Zahlbericht, S. 272, Satz 90. Ist $\mathfrak{p} = \mathfrak{P}$, und sollte A durch $\mathfrak{P}$ teilbar sein, so kann es mittels einer schon in $k(\mathfrak{p})$ gelegenen Primzahl π für $\mathfrak{P} = \mathfrak{p}$ in der Form

$\mathsf{A} = \pi^{\alpha}\mathsf{H}\,(\mathfrak{p})$ geschrieben werden, wo H eine Einheit aus $K(\mathfrak{P})$ ist. Es wird dann

$$\mathsf{A}^{1-\sigma} = \mathsf{H}^{1-\sigma}\ (\mathfrak{p}), \qquad \text{w.z.b.w.}$$

66 IV

Hilfssatz 2. 1.) Ist $\mathfrak{q}$ ein Primideal aus k, das nicht in der Relativdiskriminante von K aufgeht, und Θ eine zu $\mathfrak{q}$ prime Zahl aus K, für die

$$n(\Theta) \equiv 1 \mod \mathfrak{q}^a; \qquad (a \geqq 1)$$

ist, so gibt es in K eine zu $\mathfrak{q}$ prime Zahl A, sodaß

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{q}^a$$

ist.

2.) Ist ferner $\mathfrak{p} = \mathfrak{P}^{\ell}$ ein zu ℓ primer Teiler der Relativdiskriminante und Θ eine zu $\mathfrak{p}$ prime Zahl aus K, für die gilt:

$$n(\Theta) \equiv 1 \mod \mathfrak{p}^a; \qquad (a \geqq 1),$$

so gibt es in K eine Zahl A, sodaß gilt:

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{P}^{a\ell}.$$

3.) Ist schließlich $\mathfrak{l} = \mathfrak{L}^{\ell}$ ein in ℓ aufgehender Teiler der Relativdiskriminante und $\mathfrak{D}_{\mathfrak{l}} = \mathfrak{l}^{(v+1)(\ell-1)}$, ferner Θ eine zu $\mathfrak{l}$ prime Zahl aus K für gilt:

$$n(\Theta) \equiv 1 \mod \mathfrak{l}^{v+a}; \qquad (a \geqq 1),$$

so gibt es in K eine Zahl A, sodaß gilt:

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{L}^{v+a\ell}.$$

Beweis. 1.) Nach Voraussetzung ist

$$n(\Theta) = \eta\ (\mathfrak{q}),$$

wo η eine Einseinheit mindestens a–ten Grades aus $k(\mathfrak{q})$ ist. Nach den Normzahlsätzen (Satz 5a, S. 14▶) ist dann

$$\eta = n(\Theta_0)\ (\mathfrak{q})$$

und wie aus deren Beweisen hervorgeht, darf

$$\Theta_0 \equiv 1 \mod \mathfrak{q}^a$$

angenommen werden. Ist nämlich erstens $\mathfrak{q}$ prim zu ℓ und zerfällt in K, so darf

$$\Theta_0 = (\eta, 1, \ldots, 1)$$

im Sinne von S. 65 gesetzt werden, woraus alles folgt, und dasselbe gilt wenn $\mathfrak{q}$ ein zerfallender Teiler von ℓ ist. Ist zweitens $\mathfrak{q}$ ein nicht zerfallender, zu ℓ primer Primteiler, so ist η als Einseinheit a–ten Grades sicher ℓ–te Potenz einer Einseinheit a–ten Grades aus $k(\mathfrak{q})$ (multipl. Normalf.), die als Θ_0 genommen werden darf. Ist schließlich $\mathfrak{q}$ ein nicht zerfallender Teiler von ℓ, so folgt aus dem entsprechenden Normzahlbeweise (Hensel–Hasse, Math. Ann.; Hensel, Crelle 152), daß η Norm einer Einseinheit a–ten Grades aus $K(\mathfrak{q})$ ist.

Es ist dann $\frac{\Theta}{\Theta_0}$ prim zu $\mathfrak{q}$ und

$$n\left(\frac{\Theta}{\Theta_0}\right) = 1 \ (\mathfrak{q}),$$

also existiert nach Hilfssatz 1 ein zu $\mathfrak{q}$ primes A_0 in $K_\mathfrak{q}$, sodaß

$$\frac{\Theta}{\Theta_0} = \mathsf{A}_0^{1-\sigma} \ (\mathfrak{q})$$

ist. Betrachtet man diese Gleichung mod $\mathfrak{q}^a$, so fällt Θ_0 heraus und es resultiert, wenn A einen genügend hohen Näherungswert von A_0 aus K bezeichnet,

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{q}^a, \qquad \text{w.z.b.w.}$$

2.) Nach Voraussetzung ist

$$n(\Theta) = \eta \ (\mathfrak{p}),$$

wo η eine Einseinheit mindestens a–ten Grades aus $k(\mathfrak{p})$ ist. Diese ist wegen $\mathfrak{p}$ prim zu ℓ sicher ℓ–te Potenz einer ebensolchen Einseinheit η_0 vom a–ten Grade aus $k(\mathfrak{p})$, also

$$\eta = n(\eta_0) \ (\mathfrak{p}),$$
$$n\left(\frac{\Theta}{\eta_0}\right) = 1 \ (\mathfrak{p}).$$

68 IV

Also existiert nach Hilfssatz 1 ein (möglicherweise durch $\mathfrak{P}$ teilbares) A_0 aus $K(\mathfrak{P})$, sodaß

$$\frac{\Theta}{\eta_0} = \mathsf{A}_0^{1-\sigma} \ (\mathfrak{p})$$

ist. Betrachtet man dies nur mod $\mathfrak{p}^a$, so fällt η_0 heraus und es wird, wenn A einen genügend hohen Näherungswert von A_0 aus K bezeichnet

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{p}^a, \quad \text{d.h. mod } \mathfrak{P}^{a\ell}.$$

3.) Nach Voraussetzung ist

$$n(\Theta) = \eta \ (\mathfrak{l}),$$

wo η eine Einseinheit mindestens $(v+a)$–ten Grades aus $k(\mathfrak{l})$ ist. Da diese das „kritische Element“ v–ten Grades des „Normzahlbasissystems“ nicht enthalten kann, ist sie Norm einer Einseinheit Θ_0 aus $K(\mathfrak{L})$, und zwar wie die Betrachtung a. S. 21 lehrt, einer solchen mindestens vom Grade $v + a\ell$ in $\mathfrak{L}$. Es ist dann wieder

$$n\left(\frac{\Theta}{\Theta_0}\right) = 1 \ (\mathfrak{l}),$$

also existiert nach Hilfssatz 1 ein (möglicherweise durch $\mathfrak{L}$ teilbares) A_0 aus $K(\mathfrak{L})$, sodaß

$$\frac{\Theta}{\Theta_0} = \mathsf{A}_0^{1-\sigma} \ (\mathfrak{l})$$

ist. Betrachtet man dies nur mod $\mathfrak{L}^{v+a\ell}$, und versteht unter A einen genügend hohen Näherungswert von A_0 aus K, so folgt

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{L}^{v+a\ell}, \qquad \text{w.z.b.w.}$$

Aus Hilfssatz 2 erhalten wir nun leicht durch Zusammenfassung:

69 IV

Hilfssatz 3. Es sei $\mathfrak{f}^{\ell-1}$ die Relativdiskriminante von K,

$$\mathfrak{f} = \prod \mathfrak{p} \cdot \prod \mathfrak{l}^{v+1}; \qquad \mathfrak{p} = \mathfrak{P}^{\ell}; \qquad \mathfrak{l} = \mathfrak{L}^{\ell}$$

und $\mathfrak{m} = \mathfrak{f}\mathfrak{a}$ ein beliebiges durch $\mathfrak{f}$ teilbares Ideal (ganz) in k. Wir setzen

$$\mathfrak{F} = \prod \mathfrak{P} \cdot \prod \mathfrak{L}^{v+\ell}$$

und

$$\mathfrak{M} = \mathfrak{F} \cdot \mathfrak{a}.$$

Ist dann Θ eine zu $\mathfrak{M}$ prime Zahl aus K, für die gilt:

$$n(\Theta) \equiv 1 \mod \mathfrak{m},$$

so gibt es in K eine Zahl A derart, daß

$$\Theta \equiv \mathsf{A}^{1-\sigma} \mod \mathfrak{M}$$

ist. A ist möglicherweise nicht prim zu M, aber jedenfalls

$$(\mathsf{A})^{1-\sigma} = \mathfrak{A}^{1-\sigma},$$

wo $\mathfrak{A}$ ein zu $\mathfrak{M}$ primes Ideal ist.[‖)]

Beweis. Setzt man, unter $\mathfrak{q}$ zu $\mathfrak{f}$ prime Primideale verstehend,

$$\mathfrak{m} = \prod \mathfrak{p}^a \cdot \prod \mathfrak{l}^{v+b} \cdot \prod \mathfrak{q}^c,$$

so ist nach Wahl von $\mathfrak{m}$:

$$a \geqq 1; \qquad b \geqq 1; \qquad c \geqq 0$$

und

$$\mathfrak{M} = \prod \mathfrak{P}^{(a-1)\ell+1} \cdot \prod \mathfrak{L}^{v+b\ell} \cdot \prod \mathfrak{q}^c.$$

Natürlich darf $c \geqq 1$ angenommen werden. Nach Hilfssatz 2 ergeben sich dann für jeden einzelnen Primteiler $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ von $\mathfrak{m}$ Zahlen A der dort genannten Beschaffenheit, sodaß sich ein System von Kongruenzen folgender Art ergibt:

$$\Theta \equiv (\Pi^{\varrho}\mathsf{A}_1)^{1-\sigma} \mod \mathfrak{P}^{a\ell} \quad \text{also sicher mod } \mathfrak{P}^{(a-1)\ell+1},$$
$$\Theta \equiv (\Lambda^{\tau}\mathsf{A}_2)^{1-\sigma} \mod \mathfrak{L}^{v+b\ell},$$
$$\Theta \equiv \mathsf{A}_3^{1-\sigma} \mod \mathfrak{q}^c,$$

[‖)] Außerdem kann man A mit vorgeschriebener Signatur wählen.

wobei die Π, Λ Primzahlen aus K für die $\mathfrak{P}, \mathfrak{L}$ und die $\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$ zu den betr. Moduln prime Zahlen sind. Die $\Pi, \Lambda, \mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$ können ferner nach genügend hohen Potenzen der entsprechenden Moduln durch kongruente ersetzt werden, also so gewählt werden, daß sie für alle nicht zu ihnen gehörigen Primteilerpotenzen von $\mathfrak{M}$ kongruent 1 werden. Setzt man dann

$$\mathsf{A} = (\Pi^{\varrho}\mathsf{A}_1)\ldots(\Lambda^{\tau}\mathsf{A}_2)\ldots\mathsf{A}_3\ldots$$

so wird

$$\mathsf{A}^{1-\sigma} \equiv \Theta$$

nach jeder der Primteilerpotenzen aus $\mathfrak{M}$, also mod $\mathfrak{M}$. Da A nach einer genügend hohen Potenz von $\mathfrak{M}$ als Modul durch eine kongruente Zahl ersetzt werden darf, ohne die Restklasse von $\frac{\mathsf{A}}{\sigma\mathsf{A}}$ mod $\mathfrak{M}$ zu verändern (die ℓ^{κ}–ten Potenzen von $\mathfrak{M}$ liegen in k, sodaß aus $\mathsf{A} \equiv \mathsf{A}'$ mod $\mathfrak{M}^{\ell^{\kappa}}$ [6] folgt $\sigma\mathsf{A} \equiv \sigma\mathsf{A}'$ mod $\mathfrak{M}^{\ell^{\kappa}}$), kann man ein A der verlangten Beschaffenheit mit vorgeschriebener Signatur finden.

Endlich sei

$$(\Pi) = \mathfrak{P}\mathfrak{A}_1, \ldots \;;\; (\Lambda) = \mathfrak{L}\mathfrak{A}_2, \ldots$$

Dann ist, da nach unseren Forderungen Π, Λ prim zu allen übrigen Faktoren von $\mathfrak{M}$ sind, $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ prim zu $\mathfrak{M}$ und daher, weil sich alle Faktoren $\mathfrak{P}, \mathfrak{L}$ herausheben

$$(\mathsf{A})^{1-\sigma} = \mathfrak{A}^{1-\sigma},$$

wo $\mathfrak{A}$ prim zu $\mathfrak{M}$ ist. Damit ist Hilfssatz 3 bewiesen.

71 IV

Mittels der bewiesenen Hilfssätze soll nun eine Verallgemeinerung des Geschlechtsbegriffes in folgender Richtung dargelegt werden:

In E.▶, F.▶ wurde bewiesen, daß jeder relativ–zyklische Körper K Klassenkörper für eine bestimmte Klassengruppe H des Grundkörpers k ist, die nach dem dortigen Strahl o aller Normenreste mod $\mathfrak{f}$. (für $\ell = 2$ mit einer gewissen Vorzeichenbedingung) erklärbar ist. □□□ Wenn sich auch später herausstellen wird, daß der Modul $\mathfrak{f}$ für diese Klassengruppe eine ausgezeichnete Bedeutung hat, nämlich ihr *Führer* ist, so ist es doch für den Beweis des Hauptsatzes über relativ Abelsche Körper□□□ notwendig, davon Gebrauch zu machen, daß H auch nach jedem beliebigen ganzen Vielfachen $\mathfrak{m} = \mathfrak{a}\mathfrak{f}$ von

[6] undeutlich

$\mathfrak{f}$ erklärbar ist. Die allgemeinste Klasseneinteilung nach einem solchen Modul $\mathfrak{m}$ erhält man, wenn man den *Strahl* o, definiert durch:

$$\boldsymbol{\alpha \equiv 1 \bmod \mathfrak{m}\ \text{(und für } \ell = 2 \text{ total positiv)},}^{\|)}$$

zugrundeliegt, und die Klassen nach o definiert. H läßt sich dann auch auffassen als Klassengruppe vom Index ℓ, die aus diesen allgemeinsten Klassen zusammengesetzt ist.

Es entsteht dann die wichtige Frage, ob auch für diese Klasseneinteilung in k die Klassen von K in *Geschlechter* eingeteilt werden können, sodaß die beiden Fundamentalsätze über die Geschlechter, Satz 17 und 18 ihre Gültigkeit haben, also

1.) Die Anzahl der Geschlechter in K, d.h. Index der Klassengruppe: „Hauptgeschlecht“ aus K gleich dem ℓ–ten Teil der Klassenzahl h_1 nach o in k ist,

2.) Das Hauptgeschlecht der Inbegriff aller symbolischen $(1-\sigma)$ ten Potenzen von Klassen aus K ist.

Soll dies der Fall sein, so muß jedenfalls im Oberkörper ebenfalls ein engerer Klassenbegriff, als der oben benutzte absolute, angewendet werden. Denn die Möglichkeit der Geschlechtereinteilung beruhte auf der eindeutigen Definierbarkeit der Relativnormen von Klassen aus K, diese wieder darauf, daß die Normen aus der Hauptklasse von K in die Hauptklasse von k fielen. Das ist aber bei absoluter Klasseneinteilung in K nicht allgemein der Fall, da eine Zahlnorm $n(\mathsf{A})$ zwar Normenrest mod $\mathfrak{m}$, nicht aber notwendig $\equiv 1$ mod $\mathfrak{a}\mathfrak{f}$ zu sein braucht. Es muß also ein geeigneter Idealmodul $\mathfrak{M}$ in K angegeben werden, sodaß für die Klasseneinteilung nach dem *Strahl* O, definiert durch

$$\mathsf{A} \equiv 1 \bmod \mathfrak{M}\ \text{(und für } \ell = 2 \text{ total positiv)},$$

die Normen aus der Hauptklasse von K in die Hauptklasse von k fallen. Es soll also aus

$$\begin{aligned} & \mathsf{A} \equiv 1 \mod \mathfrak{M} \\ \text{folgen} \qquad & n(\mathsf{A}) \equiv 1 \bmod \mathfrak{m}, \end{aligned}$$

$^{\|)}$Die Vorzeichenbedingung ist nur für $\ell = 2$ wesentlich; für ungerades ℓ würde man sie unnötig mitführen.

(und für $\ell = 2$ noch die Vorzeichenbedingung „total positiv“, wenn für A auch für $n(\mathsf{A})$ erfüllt sein; letzteres ist aber stets

der Fall, denn eine in einem reellen Körper liegende konjugierte zu $n(\mathsf{A})$ ist entweder als Produkt zweier konjugiert komplexer Zahlen positiv, oder das Produkt zweier reellen positiven Größen, da A total positiv sein soll).

Um die gestellte Forderung zu befriedigen, muß zunächst offenbar in $\mathfrak{M}$ jeder Primteiler aus K aufgenommen werden, der einem in $\mathfrak{m}$ vorkommenden Primteiler aus k entspricht, damit überhaupt auf eine Kongruenzeigenschaft mod $\mathfrak{m}$ von $n(\mathsf{A})$ geschlossen werden kann. Es müssen also zunächst alle nicht zerfallenden und nicht in der Relativdiskriminante aufgehenden $\mathfrak{q} = \mathfrak{Q}$ von $\mathfrak{m}$ in $\mathfrak{M}$ aufgenommen werden. Geht ein solches $\mathfrak{q}$ in $\mathfrak{m}$ zur Potenz $\mathfrak{q}^c$ auf, so folgt aus

$$\mathsf{A} \equiv 1 \bmod \mathfrak{q}^c$$

Hensel'sch sofort

$$n(\mathsf{A}) \equiv 1 \bmod \mathfrak{q}^c,$$

wie man sich leicht überzeugt, aber für keine niedrigere Potenz in der ersten Kongruenz. Ist ferner $\mathfrak{q} = \mathfrak{Q}_1 \dots \mathfrak{Q}_\ell$ ein zerfallender Primteiler von $\mathfrak{m}$, so würde aus

$$\mathsf{A} \equiv 1 \bmod \mathfrak{Q}_1^c$$

noch nicht auf

$$n(\mathsf{A}) \equiv 1 \bmod \mathfrak{q}^c$$

geschlossen werden können, wohl aber aus

$$\mathsf{A} \equiv 1 \bmod \mathfrak{q}^c,$$

und wie man sich sofort Hensel'sch überzeugt, auch aus keinem niedrigeren Potenzprodukt in der ersten Kongruenz.

Die nicht in der Relativdiskriminante aufgehenden (zu $\mathfrak{f}$ primen) Teiler von $\mathfrak{m}$ müssen also *vollständig* in denselben Potenzen in $\mathfrak{M}$ aufgenommen werden, wie sie in $\mathfrak{m}$ aufgehen.

Geht ein Teiler $\mathfrak{p}$ von $\mathfrak{f}$, der prim zu ℓ ist, in $\mathfrak{m}$ zur Potenz $\mathfrak{p}^a$[**)] auf, so überzeugt man sich leicht, daß aus

$$\mathsf{A} \equiv 1 \mod \mathfrak{P}^{(a-1)\ell+1}; \qquad (\mathfrak{p} = \mathfrak{P}^\ell)$$

folgt

$$\alpha \equiv 1 \mod \mathfrak{p}^a.$$

Denn A hat eine Entwicklung:

$$\mathsf{A} = 1 + \pi^{a-1}\Pi\alpha_1 + \cdots \ (\mathfrak{P}),$$

also $n(\mathsf{A}) = 1 + \pi^{a-1}s(\Pi)\alpha_1 + \cdots + \pi^{\ell(a-1)}n(\Pi)\alpha_1^\ell + \cdots \ (\mathfrak{p}) \equiv 1 \bmod \mathfrak{p}^a$,

was für $a > 1$, sowohl wie $a = 1$ unter Berücksichtigung von

$$s(\Pi) \equiv 0 \mod \mathfrak{p}$$

folgt. Offensichtlich darf der Modul $\mathfrak{P}^{(a-1)\ell+1}$ der Voraussetzung auch nicht niedriger gewählt werden, um auf $\mathfrak{p}^a$ schließen zu können, da schon für $\mathfrak{P}^{(a-1)\ell} = \mathfrak{p}^{a-1}$ die Zahl $\mathsf{A} = 1 + \pi^{a-1}$ zu einem Widerspruch führen würde.

Ist endlich $\mathfrak{l}$ ein Teiler von $\mathfrak{f}$ und ℓ, der in $\mathfrak{m}$ als Vielfachem von $\mathfrak{f}$ zu einer Potenz $\mathfrak{l}^{v+b}$ aufgehen muß ($b \geqq 1$), so folgt aus den Betrachtungen von S. 21▸, daß aus

$$\mathsf{A} \equiv 1 \mod \mathfrak{L}^{v+b\ell}; \qquad (\mathfrak{l} = \mathfrak{L}^\ell)$$

auf

$$n(\mathsf{A}) \equiv 1 \mod \mathfrak{l}^{\mathfrak{v}+\mathfrak{b}}$$

geschlossen werden kann, denn A läßt sich mittels der dort bestimmten Zahl Λ_v und einer Primzahl λ für $\mathfrak{l}$ in der Form

$$\mathsf{A} = 1 + w\lambda^b\Lambda_v + \cdots \ (\mathfrak{L})$$

schreiben, wo w ganzes Element aus $k(\mathfrak{l})$ ist, und dann wird

$$\begin{aligned} n(\mathsf{A}) &= 1 + \overline{w}\lambda^{b+v} + \cdots \ (\mathfrak{l}) \\ &\equiv 1 \bmod \mathfrak{l}^{v+b} \end{aligned}$$

[**)] Für alle solchen $\mathfrak{p}$ muß $a \geqq 1$ sein, da $\mathfrak{m}$ durch $\mathfrak{f}$ teilbar ist.

75 IV

Für einen niedrigeren Modul als $\mathfrak{L}^{v+b\ell}$ in der Ausgangskongruenz jedoch kann man, wie die Betrachtungen a. S. 21 lehren, nicht allgemein auf $\mathfrak{l}^{v+b}$ schließen. (?)

Damit haben wir gezeigt, daß gerade der Modul $\mathfrak{M}$ von Hilfssatz 3 der kleinste Modul ist, für den bei unserem zugrundegelegten Modul $\mathfrak{m}$ in k allgemein aus

$$\mathsf{A} \equiv 1 \mod \mathfrak{M}$$

auf

$$n(\mathsf{A}) \equiv 1 \mod \mathfrak{m}$$

geschlossen werden kann.

Demgemäß definieren wir jetzt die Idealklassen in K nach dem oben genannten Strahl O für diesen Modul $\mathfrak{M}$. Wie bewiesen, liegen dann die Normen der Ideale der Hauptklasse in K in der Hauptklasse (nach o) in k und somit die Idealnormen irgendeiner Klasse von K in ein und derselben Klasse von k, sodaß die Relativnormen der Klassen nach O von K eindeutig bestimmte Klassen nach o von k sind.

Die Gesamtheit dieser Relativnormklassen in k bilden dann wieder eine Klassengruppe H in k. Diese Klassengruppe besteht aus allen Klassen, die Relativnormen zu $\mathfrak{m}$ primer Ideale aus K enthalten. Ich weise nun nach, daß diese Klassengruppe H von der früher für den speziellen Strahl mod $\mathfrak{f}$ so bezeichneten Klassengruppe nicht wesentlich verschieden ist, dh. abgesehen von den zu $\mathfrak{f}$ aber nicht zu $\mathfrak{m}$ primen Idealen übereinstimmt.

Dazu bemerke ich, daß sich jede der früheren Klassen nach $\mathfrak{f}$ bei unser jetzigen, engeren Klasseneinteilung nach $\mathfrak{m}$ in ein– u. derselben Anzahl von engeren Klassen auflöst.

76 IV

Sei

$$\mathfrak{k} = \mathsf{K}_1 + \mathsf{K}_2 + \cdots + \mathsf{K}_t$$

eine solche Zerlegung, wobei natürlich in $\mathfrak{k}$ nur die sogar zu $\mathfrak{m}$ primen Ideale in Betracht zu ziehen sind, so ist einfach zu zeigen, daß wenn $\mathfrak{k}$ in früherem Sinne zu dem dortigen H gehört, d.h. Relativnormen von Idealen aus K enthält[††], dann gleichzeitig *alle* engeren Klassen $\mathsf{K}_1, \ldots, \mathsf{K}_t$ im neuen Sinne

[††] Die dann natürlich auch prim zu $\mathfrak{m}$ angenommen werden dürfen, weil in jeder Klasse von K zu $\mathfrak{m}$ prime Ideale vorkommen.

zu H gehören, also Relativnormen zu $\mathfrak{m}$ primer Ideale enthalten. Sei nun

$$\mathfrak{a} = n(\mathfrak{A})$$

die Relativnorm eines zu $\mathfrak{m}$ primen Ideals $\mathfrak{A}$ aus K, die in $\mathfrak{k}$ vorkommt. Die Klassen $\mathsf{K}_1, \ldots, \mathsf{K}_t$ können dann durch ein volles Repräsentantensystem ihnen angehöriger Ideale charakterisiert werden, das den Typus:

$$\mathfrak{a}(\alpha_1), \ldots, \mathfrak{a}(\alpha_t)$$

haben muß, wo $\alpha_1, \ldots, \alpha_t$ gewisse t zu $\mathfrak{m}$ prime Zahlen mit den Eigenschaften

$$\alpha_i \equiv n(\mathsf{A}_i) \mod \mathfrak{f}; \qquad (i = 1, 2, \ldots, t)$$

sind, und für $\ell = 2$ nach der Vorzeichenbedingung von Abschnitt F.▸ genügen. Da in jeder Restklasse mod $\mathfrak{f}$ Zahlen jeder Signatur liegen, darf überdies vorausgesetzt werden, daß die α_i dieselbe Signatur wie $n(\mathsf{A}_i)$ haben, denn dies ist ersichtlich mit der Vorzeichenbedingung von Abschn. F.▸ in Einklang. Ferner darf sogar

$$\alpha_i \equiv n(\mathsf{A}_i) \mod \mathfrak{m}; \qquad (i = 1, 2, \ldots, t)$$

77 IV

angenommen werden, weil ja die in $\mathfrak{f}$ aufgehenden Primteilerpotenzen so hoch sind, daß aus „Normenrest für sie als Modul“ auf „Normzahl für ihren Bereich“ geschlossen werden kann und die zu $\mathfrak{f}$ primen in $\mathfrak{m}$ aufgehenden Primteilerpotenzen die Eigenschaft haben, daß jede prime Restklasse nach ihnen Normenrest ist. Sind die α_i nun allen diesen Bedingungen entsprechend gewählt, so ist

$$\frac{\alpha_i}{n(\mathsf{A}_i)} \equiv 1 \mod \mathfrak{m}; \qquad (\text{und für } \ell = 2 \text{ total positiv}).$$

Also gehören die Ideale

$$\mathfrak{a}\big(n(\mathsf{A}_1)\big); \quad \mathfrak{a}\big(n(\mathsf{A}_2)\big); \quad \ldots; \quad \mathfrak{a}\big(n(\mathsf{A}_t)\big)$$

ebenfalls zu den Klassen $\mathsf{K}_1, \ldots, \mathsf{K}_t$ und sind Relativnormen der zu $\mathfrak{m}$ primen Ideale[‡‡)]

$$\mathfrak{A}_(\mathsf{A}_1); \quad \mathfrak{A}(\mathsf{A}_2); \quad \ldots; \quad \mathfrak{A}(\mathsf{A}_t).$$

[‡‡)] Die A_i dürfen tatsächlich prim zu $\mathfrak{m}$ angenommen werden. Für die nicht zerfallenden Teiler von $\mathfrak{m}$ folgt dies aus $\alpha_i \equiv n(\mathsf{A}_i) \mod \mathfrak{m}$, für die zerfallenden aus der Konstruktion der zu α_i gehörigen A_i nach dem Henselschen „Ringverfahren”.

Damit ist also gezeigt, daß *alle* Klassen $\mathsf{K}_1, \ldots, \mathsf{K}_t$ Relativnormen zu $\mathfrak{m}$ primer Ideale enthalten, wenn dies für die ihnen zugeordnete Klasse $\mathfrak{k}$ der Fall ist, also die Identität des früheren mit dem jetzt auf allgemeinere Weise herauskommenden H. Die jetzige Definition von H auf Grund der allgemeineren Strahlen $o \bmod \mathfrak{m}$ und $O \bmod \mathfrak{M}$ hat vor der früheren speziellen Definition den Vorzug, daß sie nicht mehr den Begriff der Normenreste verwendet.

Die Klassengruppe H hat auch als Gruppe der neuen engeren Klassen als Elemente den Index ℓ, da allgemein der Index einer Klassengruppe von der Wahl der Klasseneinteilung

78 IV

unabhängig ist.

Wir teilen nun, wie früher die Idealklassen in K in *Geschlechter* ein, indem wir alle und nur die Klassen gleicher Relativnorm in ein Geschlecht zusammenfassen. Insbesondere ist also das *Hauptgeschlecht* der Inbegriff aller Klassen aus K, deren Relativnorm die Hauptklasse von k nach o, d.h. die Hauptideale des Strahles o sind. Dann ist das Hauptgeschlecht eine Klassengruppe H_0 in K, deren Nebengruppen die übrigen Geschlechter sind. Jeder Klasse von H entspricht ein Geschlecht und umgekehrt, sodaß die Anzahl der Geschlechter gleich der Anzahl der Klassen nach o von H ist. Ist h_1 die Klassenzahl nach o, so enthält H, weil sein Index ℓ ist, $\frac{h_1}{\ell}$ Klassen, und so groß ist also die Anzahl der Geschlechter. Damit ist der erste der beiden Punkte a. S. 72 oben bewiesen.

Ich zeige letztens noch, daß für unsere verallgemeinerte Geschlechtereinteilung auch der dortige Punkt 2.) richtig ist, also das Hauptgeschlecht der Inbegriff aller symbolischen $(1-\sigma)$ ten Klassenpotenzen nach O von K ist.

Daß jede Potenz $\mathfrak{K}^{1-\sigma}$ zum Hauptgeschlecht gehört, ist wie früher, leicht zu zeigen. Es hat zunächst $\mathfrak{K}^{1-\sigma} = \frac{\mathfrak{K}}{\sigma\mathfrak{K}}$ auch für unsere allgemeineren Klassen nach O einen Sinn. Denn wenn $\mathfrak{A}$ alle Ideale einer Klasse $\mathfrak{K}$ nach O durchläuft,

79 IV

also alle Ideale der Form $\mathfrak{A} = \mathfrak{A}_0(\mathsf{A})$, wo A in O liegt, so durchläuft $\sigma\mathfrak{A}$ alle Ideale der Form

$$\sigma\mathfrak{A} = \sigma\mathfrak{A}_0\ (\sigma\mathsf{A}),$$

und aus $\mathfrak{M} = \sigma\mathfrak{M}$ nach Konstruktion folgt:

$$\sigma\mathsf{A} \equiv 1 \mod \mathfrak{M}; \qquad \text{(total positiv für } \ell = 2).$$

Daher durchläuft $\sigma\mathsf{A}$, wie leicht zu sehen mit A den ganzen Strahl O, also $\sigma\mathfrak{A}$ eine ganz bestimmte Klasse $\sigma\mathfrak{K}$[7] nach O, wodurch $\mathfrak{K}^{1-\sigma} = \frac{\mathfrak{K}}{\sigma\mathfrak{K}}$ erklärt ist. Liegt $\mathfrak{A}$ in $\mathfrak{K}$, so liegt ersichtlich $\mathfrak{A}^{1-\sigma}$ in $\mathfrak{K}^{1-\sigma}$, und da $n(\mathfrak{A}^{1-\sigma}) = 1$ ist, gehört $\mathfrak{K}^{1-\sigma}$ zum Hauptgeschlecht.

Ich zeige, daß auch umgekehrt jede Klasse des Hauptgeschlechts von der Form $\mathfrak{K}^{1-\sigma}$ ist. Dazu brauche ich die drei vorangeschickten Hilfssätze. Die Behauptung lautet, für Ideale ausgesprochen, so:

Jedes zu $\mathfrak{M}$ prime Ideal $\mathfrak{A}$ aus K, dessen Relativnorm in o liegt, läßt sich in der Form

$$\mathfrak{A} = \mathfrak{B}^{1-\sigma}(\Theta)$$

darstellen, wo $\mathfrak{B}$ prim zu $\mathfrak{M}$ und Θ Zahl aus O ist.

Beweis. Der Satz 18 lehrt, daß für ein solches Ideal $\mathfrak{A}$ aus K, dessen Relativnorm ja sicher in dem dortigen weiteren[8] Strahl o liegt, eine Darstellung gilt:

$$\mathfrak{A} = \mathfrak{C}^{1-\sigma}(\mathsf{A}),$$

wo $\mathfrak{C}$ prim zu $\mathfrak{f}$ und A ebenfalls prim zu $\mathfrak{f}$ ist. $\mathfrak{C}$ darf dann ohne weiteres auch prim zu $\mathfrak{M}$ angenommen werden, da in der absoluten Klasse von $\mathfrak{C}$ sicher zu $\mathfrak{M}$ prime Ideale vorkommen, und dann ist auch A prim zu $\mathfrak{M}$.

Es ist nun zu zeigen, daß A als Zahl aus O gewählt werden darf.

Wenn

$$n(\mathfrak{A}) = (\alpha)$$

gesetzt wird, wobei nach Voraussetzung α als Zahl aus o angenommen werden darf, so folgt für A:

$$n(\mathsf{A}) = \varepsilon\alpha,$$

wo ε eine Einheit aus k ist. Nun ist

$$\alpha \equiv 1 \mod \mathfrak{m}, \quad \text{also mod } \mathfrak{f},$$

[7] undeutlich
[8] undeutlich

also ε Normenrest mod $\mathfrak{f}$. Für $\ell = 2$ ist ferner α total positiv und $n(\mathsf{A})$ wenigstens in den ν kritischen reellen konjugierten*) positiv, also auch ε in diesen konjugierten positiv. Somit ist nach Satz 19, 19a:

$$\varepsilon = n(\mathsf{B})$$

Relativnorm einer Zahl B aus K. Wie a. S. 49/50 gezeigt folgt daraus, daß

$$(\mathsf{B}) = \mathfrak{B}^{1-\sigma}$$

gesetzt werden kann, wo $\mathfrak{B}$ ein Ideal aus K ist. Die Zahl B ist nur bis auf einen Faktor $\Gamma^{1-\sigma}$ bestimmt, da ja $n(\mathsf{B}\Gamma^{1-\sigma}) = n(\mathsf{B}) = \varepsilon$ ist; infolgedessen darf das Ideal $\mathfrak{B}$ noch mit einer beliebigen Zahl Γ aus K multipliziert werden, darf mithin von vorneherein prim zu $\mathfrak{M}$ angenommen werden. Es ist dann auch B prim zu $\mathfrak{M}$, weil wegen $\mathfrak{M} = \sigma\mathfrak{M}$ auch $\sigma\mathfrak{B}$ es ist.

81 IV

Aus der nunmehr erhaltenen Gleichung

$$n(\mathsf{A}) = n(\mathsf{B})\alpha,$$

d.h.
$$n\left(\frac{\mathsf{A}}{\mathsf{B}}\right) \equiv 1 \bmod \mathfrak{m}$$

folgt nun nach Hilfssatz 3 die Existenz einer Zahl A_1 in K, sodaß

$$\frac{\mathsf{A}}{\mathsf{B}} \equiv \mathsf{A}_1^{1-\sigma} \mod \mathfrak{M}$$

ist. $\mathsf{A}_1^{1-\sigma}$ ist sicher prim zu $\mathfrak{M}$, da A und B es sind. Also ist

$$\frac{\mathsf{A}}{\mathsf{B}} = \mathsf{A}_1^{1-\sigma}\Omega$$

wo Ω Zahl aus O ist. Für $\ell = 2$ ist dazu zu zeigen, daß man A_1 so wählen kann, daß Ω total positiv wird. Nach Hilfssatz 3, Anm. 1 darf zunächst die Signatur von A_1 beliebig gewählt werden. Die Signatur von $\mathsf{A}_1^{1-\sigma}$ ist nun so beschaffen, daß in zwei reellen relativ–konjugierten von K in Bezug auf k sicher $\mathsf{A}_1^{1-\sigma}$ dasselbe Vorzeichen hat. Denn die relativ konjugierten sind für

*) Siehe S. 61.

ein solches Paar $\frac{\mathsf{A}_1^{(i)}}{\sigma\mathsf{A}_1^{(i)}}$ und $\frac{\sigma\mathsf{A}_1^{(i)}}{\mathsf{A}_1^{(i)}}$, von gleichem Vorzeichen. Sei nun für den reellen konjugierten Körper $k^{(i)}$ und das zugeordnete (identische) Paar $K^{(i)}$

$$\operatorname{sgn} n(\mathsf{A}^{(i)}) = (-1)^{c_i}.$$

Da α total positiv ist, folgt aus $n(\mathsf{A}^{(i)}) = \varepsilon^{(i)}\alpha^{(i)} = n(\mathsf{B}^{(i)})\alpha^{(i)}$, daß

$$\operatorname{sgn} n(\mathsf{B}^{(i)}) = (-1)^{c_i}$$

also

$$\operatorname{sgn} n(\mathsf{A}^{(i)}) = \operatorname{sgn}\left(\mathsf{A}^{(i)} \cdot \sigma\mathsf{A}^{(i)}\right) = \operatorname{sgn}\left(\mathsf{B}^{(i)} \cdot \sigma\mathsf{B}^{(i)}\right) = \operatorname{sgn} n(\mathsf{B}^{(i)})$$

ist, und somit

$$\operatorname{sgn}\left(\frac{\mathsf{A}^{(i)}}{\mathsf{B}^{(i)}}\right) = \operatorname{sgn}\left(\sigma\frac{\mathsf{A}^{(i)}}{\mathsf{B}^{(i)}}\right)$$

die Signatur von $\frac{\mathsf{A}}{\mathsf{B}}$ genügt also denselben Relationen, wie die von $\mathsf{A}_1^{1-\sigma}$. Da letztere wegen der freien Verfügbarkeit über

82 IV

die Signatur von A_1 bis auf die genannten Relationen willkürlich bleibt, kann also A_1 so gewählt werden, daß $\mathsf{A}_1^{1-\sigma}$ die gleiche Signatur wie $\frac{\mathsf{A}}{\mathsf{B}}$ bekommt und somit Ω total positiv wird.

Nach Hilfssatz 3 kann ferner

$$\mathsf{A}_1^{1-\sigma} = \mathfrak{A}_1^{1-\sigma}$$

mit zu $\mathfrak{M}$ primem $\mathfrak{A}_1$ gesetzt werden, sodaß

$$(\mathsf{A}) = (\mathsf{B})\mathfrak{A}_1^{1-\sigma}(\Omega) = (\mathfrak{B}\mathfrak{A}_1)^{1-\sigma}(\Omega)$$

wird. Dann wird endlich

$$\mathfrak{A} = \mathfrak{C}^{1-\sigma}(\mathsf{A}) = (\mathfrak{C}\mathfrak{B}\mathfrak{A}_1)^{1-\sigma}(\Omega),$$

wo $\mathfrak{C}\mathfrak{B}\mathfrak{A}_1$ prim zu $\mathfrak{M}$ und Ω Zahl aus O ist, w.z.b.w.

Zusammenfassend haben wir also:

Satz 22. Sei K relativ zyklisch vom Primzahlgrad ℓ über k, σ die erzeugende Substitution und

$$\mathfrak{D} = \mathfrak{f}^{\ell-1} = \left(\prod \mathfrak{p} \cdot \prod \mathfrak{l}^{\nu+1}\right)^{\ell-1}$$

die Relativdiskriminante von K. Sei ferner

$$\mathfrak{m} = \mathfrak{a}\mathfrak{f} = \prod \mathfrak{p}^a \prod \mathfrak{l}^{v+b} \prod \mathfrak{q}^c; \qquad (a, b, c \geqq 1)$$

ein beliebiger, durch $\mathfrak{f}$ teilbarer, ganzer Idealmodul aus k und die Idealklassen in k nach dem Strahl o, definiert durch

$$\alpha \equiv 1 \mod \mathfrak{m} \qquad \text{(und für } \ell = 2 \text{ total positiv)},$$

erklärt. In K sei, wenn $\mathfrak{P}, \mathfrak{L}$, die den $\mathfrak{p}, \mathfrak{l}$ zugeordneten ambigen Primideale von K bezeichnen und

$$\mathfrak{F} = \prod \mathfrak{P} \prod \mathfrak{L}^{v+\ell}$$

gesetzt wird, der Modul

$$\mathfrak{M} = \mathfrak{a}^{\mathfrak{F}} = \prod \mathfrak{P}^{(a-1)\ell+1} \prod \mathfrak{L}^{v+b\ell} \prod \mathfrak{q}^c$$

für die Klasseneinteilung zugrundegelegt, d.h. die Idealklassen nach dem Strahl O, definiert durch

$$\mathsf{A} \equiv 1 \mod \mathfrak{M} \qquad \text{(und für } \ell = 2 \text{ total positiv)},$$

definiert.

Werden dann alle Klassen von K, deren Relativnorm ein und dieselbe Klasse von k ist, in ein Geschlecht zusammengefaßt, insbesondere also diejenige Klassengruppe in K, deren Relativnorm die Hauptklasse in k ist, das Hauptgeschlecht genannt, so gelten folgende Tatsachen:

1.) Jedes Geschlecht besteht aus einer u. derselben Anzahl von Klassen von K.

2.) Die Anzahl der Geschlechter, d.h. der Index der Klassengruppe: Hauptgeschlecht, deren Nebengruppen die übrigen Geschlechter sind, ist gleich dem ℓ–ten Teil der Anzahl h_1 der Klassen nach o in k.

3.) Das Hauptgeschlecht ist der Inbegriff aller symbolischen $(1 - \sigma)$ten Klassenpotenzen aus K.

4.2 §2 Rang von Restklassen– u. Strahlklassengruppen

§2. Der Rang Abelscher Gruppen, insbesondere der Zahlengruppe der primen Restklassen mod $\mathfrak{m}$ sowie der Klassengruppe nach dem Strahl „$= 1 \bmod \mathfrak{m}$, (für $\ell = 2$ total positiv").

A. Allgemeines

A. Allgemeines über den Rang Abelscher Gruppen.

Sei $\mathfrak{G}$ eine endliche Abelsche Gruppe vom Grade N. Dann lehrt die Theorie der Gruppencharaktere, daß ein System von N Charakteren χ_{B} existiert, die den Gruppenelementen B eindeutig zugeordnet sind, sodaß für irgendzwei Gruppenelemente $\mathsf{A}_1, \mathsf{A}_2$ gilt:

$$\chi_{\mathsf{B}}(\mathsf{A}_1\mathsf{A}_2) = \chi_{\mathsf{B}}(\mathsf{A}_1) \cdot \chi_{\mathsf{B}}(\mathsf{A}_2).$$

Die Charaktere χ_{B} bilden vermöge der Eigenschaft

$$\chi_{\mathsf{B}_1}\chi_{\mathsf{B}_2} = \chi_{\mathsf{B}_1\mathsf{B}_2}$$

selbst eine Gruppe, die zu $\mathfrak{G}$ isomorph ist, und es gilt die Relation

$$\chi_{\mathsf{B}}(\mathsf{A}) = \chi_{\mathsf{A}}(\mathsf{B}).$$

(Siehe zu diesen elementaren Sätzen Weber, Algebra II, §.11.)

Es sei nun $\mathfrak{g}$ eine Untergruppe vom Grade n und Index $j = \frac{\mathsf{N}}{n}$ von $\mathfrak{G}$, und

$$\mathfrak{g}, \mathsf{A}_1\mathfrak{g}, \ldots, \mathsf{A}_{j-1}\mathfrak{g}$$

ihre Faktorgruppe $\frac{\mathfrak{G}}{\mathfrak{g}}$ vom Grade j. Dann besitzt diese Faktorgruppe j Charaktere X. Ordnet man dann jedem dieser j Charaktere X eine Funktion χ

der Elemente von $\mathfrak{G}$ so zu, daß ihr Wert für ein Element A von $\mathfrak{G}$ gleich dem

85 IV

Werte jenes Charakters X für die durch A erzeugte Nebengruppe $\mathsf{A}\mathfrak{g}$ ist, so ist diese Funktion χ ein *Charakter von* $\mathfrak{G}$. Denn aus der Eigenschaft

$$X(\mathsf{A}_1\mathfrak{g}) \cdot X(\mathsf{A}_2\mathfrak{g}) = X(\mathsf{A}_1\mathsf{A}_2\mathfrak{g})$$

der Charaktere X der Faktorgruppe folgt für die zugeordnete Funktion χ:

$$\chi(\mathsf{A}_1)\chi(\mathsf{A}_2) = \chi(\mathsf{A}_1\mathsf{A}_2)$$

für irgendzwei Elemente $\mathsf{A}_1, \mathsf{A}_2$ von $\mathfrak{G}$, was bekanntlich für einen Charakter hinreichend ist.

Man erhält also so j Charaktere χ von $\mathfrak{G}$, die die besondere Eigenschaft haben, daß ihr Wert für alle Elemente von $\mathfrak{g}$ gleich 1 ist, weil ja die Charaktere X für $\mathfrak{g}$ als Einheitselement der Faktorgruppe den Wert 1 haben.

Ist umgekehrt χ ein Charakter von $\mathfrak{G}$, der für jedes Element aus $\mathfrak{g}$ den Wert 1 hat, so hat er für je eine ganze Nebengruppe $\mathsf{A}\mathfrak{g}$ ein– und denselben Wert $\chi(\mathsf{A})$ und für das Kompositum $\mathsf{A}_1\mathsf{A}_2\mathfrak{g}$ zweier Nebengruppen $\mathsf{A}_1\mathfrak{g}$ und $\mathsf{A}_2\mathfrak{g}$ den Wert

$$\chi(\mathsf{A}_1\mathsf{A}_2) = \chi(\mathsf{A}_1)\chi(\mathsf{A}_2).$$

Es ist also χ ein Charakter der Faktorgruppe $\frac{\mathfrak{G}}{\mathfrak{g}}$, wenn $\chi(\mathsf{A}\mathfrak{g})$ als $\chi(\mathsf{A})$ definiert wird.

Es kann daher auch nicht mehr als j Charaktere χ der Art geben, daß χ für alle Elemente von $\mathfrak{g}$ den Wert 1 hat. Die Gesamtheit der Charaktere von $\mathfrak{G}$, die für die Elemente von $\mathfrak{g}$ den Wert 1 haben, bildet also eine mit der Charakterengruppe von $\frac{\mathfrak{G}}{\mathfrak{g}}$, d.h. mit $\frac{\mathfrak{G}}{\mathfrak{g}}$ selbst

86 IV

isomorphe Gruppe vom Grade j. Es seien dies die Charaktere

$$\chi_1, \chi_{\mathsf{B}_1}, \ldots, \chi_{\mathsf{B}_{j-1}},$$

unter denen natürlich der dem Einheitselement zugeordnete Hauptcharakter χ_1 vorkommt. Wegen der Gruppeneigenschaft dieser Charakterengruppe muß dann das Kompositum

$$\chi_{\mathsf{B}_i}\chi_{\mathsf{B}_k} = \chi_{\mathsf{B}_i\mathsf{B}_k}$$

zweier solcher Charaktere wieder ein solcher Charakter χ_{B_ℓ} sein, sodaß die Elemente

$$1, \mathsf{B}_1, \ldots, \mathsf{B}_{j-1}$$

eine ebenfalls mit $\frac{\mathfrak{G}}{\mathfrak{g}}$ isomorphe Gruppe $\overline{\mathfrak{g}}$ bilden, die die *reziproke Gruppe zu* $\mathfrak{g}$ heißt.*)

Es ist $\chi_{\mathsf{B}_i}(C_k) = 1$, wenn C_k in $\mathfrak{g}$, B_i in $\overline{g}$,

also auch $\chi_{C_k}(\mathsf{B_i}) = 1$, " " " " " " .

Die Charaktere $\chi_1, \chi_{C_1}, \ldots, \chi_{C_{n-1}}$ spielen also für die Untergruppe $\overline{\mathfrak{g}}$ dieselbe Rolle, wie $\chi_1, \chi_{\mathsf{B}_1}, \ldots, \chi_{\mathsf{B}_{j-1}}$ für $\mathfrak{g}$, d.h. es ist die zu $\overline{\mathfrak{g}}$ reziproke Gruppe wieder $\mathfrak{g}$. Die Reziprozität der Gruppen ist also gegenseitig eindeutig.

(wenn ein– für allemal eine feste Zuordnung der Gruppenelemente von $\mathfrak{G}$ zu den Gruppencharakteren von $\mathfrak{G}$ zugrundegelegt wird).

Jeder Untergruppe vom Grade n ist also genau eine Untergruppe vom Grade j als reziproke zugeordnet und umgekehrt. Also gilt:

Satz 23. Ist $\mathfrak{G}$ eine Abelsche Gruppe vom Grade N und $n = \frac{\mathsf{N}}{j}$ ein Teiler von N, so ist die Anzahl der Untergruppen vom Grade n von $\mathfrak{G}$ gleich der Anzahl der Untergruppen vom Grade j.

Unseren weiteren Überlegungen sei nun zunächst eine beliebige Abelsche Gruppe $\mathfrak{G}$ von endlich oder unendlich vielen Elementen zugrundegelegt.

Es sei ℓ eine Primzahl. Wir fassen alle Elemente der Form $a = a_0 x^\ell$, wo a_0 ein festes Element von $\mathfrak{A}$ ist und x die ganze Gruppe durchläuft, in einen *Verband* zusammen. Zwei Verbände sind dann entweder identisch, oder enthalten kein gemeinsames Element.

Die Verbände bilden wieder eine Abelsche Gruppe, wenn die Kompositionsregel $(a_0 x^\ell) \cdot (b_0 y^\ell) = (a_0 b_0 z^\ell)$ festgesetzt wird, die so beschaffen ist, daß der Produktverband alle und nur die Produkte aus Elementen der beiden Faktoren enthält. Jedes Element der Verbändegruppe gehört zum Exponenten ℓ, da seine ℓ–te Potenz sicher der Hauptverband x^ℓ ist, der die Rolle des Einheitselementes übernimmt.

*) Da die Zuordnung der Gruppenelemente zu den Gruppencharakteren keine absolute ist, sondern in mannigfacher Art auf Grund verschiedener Basisdarstellungen der Gruppe geschehen kann, ist auch die reziproke Gruppe *nur im Sinne der Isomorphie* eindeutig definiert.

Uns interessiert hier nur der Fall, daß *die Anzahl der Verbände endlich ist*, daß also die Untergruppe x^ℓ von $\mathfrak{G}$ von endlichem Index ist, (denn die Verbände sind ja ersichtlich nichts anderes, als Nebengruppen zu dieser Untergruppe x^ℓ aller ℓ–ten Potenzen von $\mathfrak{G}$).

88 IV

(Wie leicht zu sehen, tritt dieser Fall sicher dann ein, wenn unsere Gruppe $\mathfrak{G}$ eine endliche Basis $a_1, \ldots, a_m$ besitzt, sodaß jedes Element in der Form

$$a = a_1^{x_1} \ldots a_m^{x_m}$$

darstellbar ist, wo die Exponenten x_i ganze rationale Zahlen durchlaufen). Unter obiger Voraussetzung ist der Grad der Verbändegruppe, weil jedes Element derselben zum Exponenten ℓ gehört, eine Potenz ℓ^t von ℓ, und sie hat genau t Basiselemente, sodaß jeder Verband sich in der Form darstellen läßt:

$$\mathsf{V} = \mathsf{V}_1^{c_1} \ldots \mathsf{V}_t^{c_t}; \qquad (c_i = 0, 1, \ldots, \ell - 1),$$

und zwar eindeutig. Für die Elemente von $\mathfrak{G}$ bedeutet dies, daß es t Elemente $v_1, v_2, \ldots, v_t$ in $\mathfrak{G}$ gibt, sodaß jedes Element a aus $\mathfrak{G}$ sich eindeutig in der Form darstellen läßt:

$$a = v_1^{c_1} \ldots v_t^{c_t} x^\ell; \qquad (c_i = 0, 1, \ldots, \ell - 1).$$

Die Zahl t heiße der *Rang der Gruppe* $\mathfrak{G}$ *nach* ℓ, oder wo kein Mißverständnis zu befürchten auch kurz der Rang [...].

Mittels des Ranges t von $\mathfrak{G}$ nach ℓ kann die Anzahl der Untergruppen von $\mathfrak{G}$ vom Index ℓ ausgedrückt werden. In einer solchen Untergruppe $\mathfrak{g}$ sind nämlich alle ℓ–ten Potenzen von Elementen aus $\mathfrak{G}$ enthalten, [...] die Faktorgruppe zyklisch vom Grade ℓ ist. Daher ist der ganze Hauptverband x^ℓ in $\mathfrak{g}$ enthalten, ein anderer Verband also entweder ganz oder keins seiner Elemente. $\mathfrak{g}$ kann also auch als Untergruppe der Gruppe aller

89 IV

Verbände aufgefaßt werden, und hat als solche ebenfalls den Index ℓ (letzteres unmittelbar klar!). Die Anzahl aller Untergruppen vom Index ℓ der Verbändegruppe ist aber nach Satz 23 gleich der Anzahl der Untergruppen vom Grad ℓ. Letztere Anzahl läßt sich für die Verbändegruppe wegen ihrer einfachen Struktur leicht angeben. Jeder vom Hauptverband verschiedene Verband gibt nämlich Anlaß zu einer zyklischen Untergruppe vom Grade ℓ,

und andere Untergruppen vom Grade ℓ sind nicht denkbar. Jede solche zyklische Untergruppe ℓ–ten Grades wird aber genau $(\ell-1)$ mal erzeugt, nämlich von den $\ell-1$ vom Hauptverband verschiedenen Potenzen eines Verbandes. Da es ℓ^t-1 Nichthauptverbände gibt, resultieren also $\frac{\ell^t-1}{\ell-1}$ verschiedene Untergruppen vom Grade ℓ, also:

Satz 24. Hat die Abelsche Gruppe $\mathfrak{G}$ den endlichen Rang t nach der Primzahl ℓ, so hat sie genau $\frac{\ell^t-1}{\ell-1}$ Untergruppen vom Index ℓ.

Wir beweisen noch einen wichtigen Satz über Abelsche Gruppen von endlichem Rang t nach ℓ. Es seien die Elemente

$$a = v_1^{c_1} \dots v_t^{c_t} x^{\ell}; \qquad (c_i = 0, 1, \dots, \ell-1)$$

von $\mathfrak{G}$ durch irgendeine Bedingung eingeschränkt, welche bei Multiplikation erhalten bleibt, und der alle ℓ–ten Potenzen von Elementen genügen. Dadurch ist eine Untergruppe $\mathfrak{g}$ von $\mathfrak{G}$ definiert, die wieder den Hauptverband enthält und jeden anderen Verband entweder ganz oder keins seiner Elemente. $\mathfrak{g}$ kann also als Untergruppe

der Verbändegruppe betrachtet werden und hat als solche (in den Verbänden als Elementen) einen Grad ℓ^n und eine Basisdarstellung $\overline{\mathsf{V}}_1^{\bar{c}_1} \dots \overline{\mathsf{V}}_n^{\bar{c}_n}$; $(\bar{c}_i = 0, 1, \dots, \ell-1)$. $\Big($Ist V ein nicht in $\mathfrak{g}$ enthaltener Verband, so ist erst V^{ℓ} in $\mathfrak{g}$ enthalten, weil aus

$$\mathsf{V}^{a} \quad \text{zu} \quad \mathfrak{g}; \qquad (a, \ell) = 1$$

folgte

$$\mathsf{V}^{aa_1 - \ell\ell_1} = \mathsf{V} \quad \text{zu} \quad \mathfrak{g},$$

wenn $aa_1 - \ell\ell_1 = 1\Big)$. Demnach hat die Faktorgruppe zu $\mathfrak{g}$ in Bezug auf die Verbändegruppe eine Basisdarstellung der Form

$$\mathsf{V}\mathfrak{g} = \mathsf{V}_1^{c_1} \dots \mathsf{V}_{t-n}^{c_{t-n}} \mathfrak{g}; \qquad (c_i = 0, 1, \dots, \ell-1),$$

weil jedes ihrer Elemente zum Exponenten ℓ gehört und der Grad ℓ^{t-n} sein muß. Es läßt sich also jeder Verband eindeutig in der Form darstellen:

$$\mathsf{V} = \mathsf{V}_1^{c_1} \dots \mathsf{V}_{t-n}^{c_{t-n}} \overline{\mathsf{V}}_1^{\bar{c}_1} \dots \overline{\mathsf{V}}_n^{\bar{c}_n}; \qquad (c_i, \bar{c}_i = 0, 1, \dots, \ell-1)$$

Spricht man dieses Resultat für die Elemente von $\mathfrak{G}$ selbst aus so erhält man:

Satz 25. Die Abelsche Gruppe $\mathfrak{G}$ habe den endlichen Rang t nach der Primzahl ℓ. Durch irgendeine Bedingung, der alle ℓ–ten Potenzen[1] aus $\mathfrak{G}$ genügen, sei eine Untergruppe $\mathfrak{g}$ von $\mathfrak{G}$ definiert, die dann einen endlichen Rang $n \leqq t$ hat, sodaß die Elemente von $\mathfrak{g}$ die eindeutige Darstellung gestatten:

$$\overline{a} = \overline{v}_1^{\overline{c}_1} \dots \overline{v}_n^{\overline{c}_n} x^\ell; \qquad (\overline{c}_i = 0, 1, \dots, \ell - 1).$$

Dann lassen sich in $\mathfrak{G}$ noch weitere $t - n$ Elemente v_i finden, sodaß jedes Element von $\mathfrak{G}$ eindeutig in der Form darstellbar ist:

$$a = v_1^{c_1} \dots v_{t-n}^{c_{t-n}} \overline{v}_1^{\overline{c}_1} \dots \overline{v}_n^{\overline{c}_n} x^\ell; \qquad (\overline{c}_i, c_i = 0, 1, \dots, \ell - 1).$$

a gehört dann und nur dann zu $\mathfrak{g}$, wenn alle $c_i = 0$ sind.

B. Die prime Restklassengruppe mod $\mathfrak{m}$

B. Der Rang der Gruppe der primen Restklassen mod $\mathfrak{m}$.

Es sei $\mathfrak{m}$ ein ganzes Ideal aus k und ℓ eine beliebige Primzahl. Dann hat die Gruppe der primen Restklassen mod $\mathfrak{m}$ als endliche Abelsche Gruppe einen endlichen Rang $\mu = R(\mathfrak{m})$ nach ℓ. Es gibt also μ zu $\mathfrak{m}$ prime Zahlen $\gamma_1, \dots, \gamma_\mu$, sodaß jede zu $\mathfrak{m}$ prime Zahl α mod $\mathfrak{m}$ eindeutig in der Form darstellbar ist:

$$\alpha \equiv \gamma_1^{c_1} \dots \gamma_\mu^{c_\mu} \xi^\ell \bmod \mathfrak{m}; (c_i = 0, 1, \dots, \ell - 1) \tag{1}$$

α ist also dann und nur dann ℓ–ter Potenzrest mod $\mathfrak{m}$, wenn alle $c_i = 0$ sind. Insbesondere sind $\gamma_1, \dots, \gamma_\mu$ selbst ℓ–te Potenz–Nichtreste mod $\mathfrak{m}$ und von der Art, daß kein Potenzprodukt aus ihnen ℓ–ter Potenzrest mod $\mathfrak{m}$ ist, wenn nicht alle Exponenten durch ℓ teilbar sind. Aus diesem Grunde soll ein solches System $\gamma_1, \dots, \gamma_\mu$ ein

System unabhängiger Nichtreste mod $\mathfrak{m}$ heißen.

Die Bestimmung von $\mu = R(\mathfrak{m})$ läßt sich sofort zurückführen auf die Bestimmung der entsprechenden Anzahlen für die verschiedenen in $\mathfrak{m}$ aufgehenden Primteilerpotenzen.

[1] undeutlich

*) Das in Klammern eingeschlossene ist überflüssig, es genügt: „Jedes V^ℓ zu $\mathfrak{g}$".

Satz 26. Ist $\mathfrak{m} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_Z^{\nu_Z}$, so ist (für beliebiges ℓ):

$$R(\mathfrak{m}) = R(\mathfrak{p}_1^{\nu_1}) + \dots + R(\mathfrak{p}_Z^{\nu_Z})$$

Beweis. Läßt man in (1) die Exponenten c_i alle unabhängig von einander die Werte $0, 1, \dots, \ell - 1$ durchlaufen, so erhält man ℓ^μ inkongruente α. Man erhält dann *alle* primen Restklassen mod $\mathfrak{m}$, jede nur einmal, wenn ξ noch alle*) Werte durchlaufen läßt, für die die zugehörigen ξ^ℓ mod $\mathfrak{m}$ inkongruent sind. Nennt man deren Anzahl ν, so ist

demnach

$$\nu \cdot \ell^\mu = \Phi(\mathfrak{m}),$$

wo $\Phi(\mathfrak{m})$ die Eulersche Funktion ist.

Läßt man nun in ξ^ℓ die Zahl ξ ein primes Restsystem mod $\mathfrak{m}$ durchlaufen, so erscheint eine feste Restklasse genau so oft, als es inkongruente Lösungen von $\xi^\ell \equiv 1 \bmod \mathfrak{m}$ gibt. Ist deren Anzahl ν_1, so ist also

$$\nu\nu_1 = \Phi(\mathfrak{m})$$

und folglich

$$\ell^\mu = \nu_1. \tag{2}$$

Die Lösungszahl ν_1 von $\xi^\ell \equiv 1 \bmod \mathfrak{m}$ ist nun ersichtlich das Produkt der Lösungszahlen für die einzelnen Primteilerpotenzmoduln, die in $\mathfrak{m}$ aufgehen, da jeder Lösung mod $\mathfrak{m}$ [2] eine solche für jedes $\mathfrak{p}_i^{\nu_i}$ und inkongruenten Lösungen mod [...] auch nach mindestens einem $\mathfrak{p}_i^{\nu_i}$ inkongruente Lösungssysteme nach den $\mathfrak{p}_i^{\nu_i}$ entsprechen, umgekehrt aber jedem Lösungssystem nach den $\mathfrak{p}_i^{\nu_i}$ eine Lösung mod $\mathfrak{m}$. Wendet man dann (2) auf die Lösungszahlen nach den $\mathfrak{p}_i^{\nu_i}$ an, so folgt

$$\ell^{R(\mathfrak{m})} = \ell^\mu = \nu_1 = \ell^{R(\mathfrak{p}_1^{\nu_1})} \cdot \ell^{R(\mathfrak{p}_2^{\nu_2})} \dots \ell^{R(\mathfrak{p}_Z^{\nu_Z})}$$

also die Behauptung.†)

Die nunmehr noch zu leistende Bestimmung der $R(\mathfrak{p}_i^{\nu_i})$ läßt sich auf Grund der Henselschen multiplikativen Normalform unmittelbar durchführen. Es sind die beiden Fälle $\mathfrak{p}$ prim zu ℓ und $\mathfrak{p}$ Teiler $\mathfrak{l}$ von ℓ zu unterscheiden.

*) zu $\mathfrak{m}$ primen Werte

[2] undeutlich

†) Der Satz läßt sich einfacher durch Komponentenzerlegung des Körpers der Restklassen mod $\mathfrak{m}$ beweisen.

1.) $\mathfrak{p}$ prim zu ℓ.

Dann besteht für jedes*) Element α aus $k(\mathfrak{p})$ die Basisdarstellung:

$$\alpha = \omega^c \eta \ (\mathfrak{p}); \qquad (c = 0, 1, \ldots, p^{\mathfrak{f}} - 2), \tag{3}$$

wo ω eine primitive $(p^{\mathfrak{f}} - 1)$ te, d.h. $\Phi(\mathfrak{p})$–te Einheitswurzel ist, und η eine Einseinheit aus $k(\mathfrak{p})$ bezeichnet. Ist nun erstens $p^{\mathfrak{f}} - 1 = \Phi(\mathfrak{p}) \not\equiv 0 \bmod \ell$, so ist ω eine ℓ–te Potenz, ebenso jedes η, weil $\mathfrak{p}$ prim zu ℓ, und daher jedes zu $\mathfrak{p}$ prime α ℓ–te Potenz in $k(\mathfrak{p})$, umsomehr ℓ–ter Potenzrest nach jedem Modul $\mathfrak{p}^a$ $(a \geqq 1)$:

$$\alpha \equiv \xi^\ell \mod \mathfrak{p}^a.$$

Dann ist also $R(\mathfrak{p}^a) = 0$.

Ist aber zweitens $p^{\mathfrak{f}} - 1 = \Phi(\mathfrak{p}) \equiv 0 \bmod \ell$, was z.B. für jedes zu ℓ prime $\mathfrak{p}$ im Kreiskörper der ℓ–ten Einheitswurzel ζ, und also in jedem Körper der ζ enthält, eintritt, so ist ω sicher ℓ–ter Potenznichtrest schon mod $\mathfrak{p}$; da aus

$$\omega \equiv \xi^\ell \mod \mathfrak{p}$$

folgte

$$\frac{\omega}{\xi^\ell} \equiv 1 \mod \mathfrak{p},$$

also $\frac{\omega}{\xi^\ell}$ Einseinheit und ℓ–te Potenz in $k(\mathfrak{p})$, also

$$\omega = \omega_0^\ell(\mathfrak{p});$$

□□□ dann wäre aber ω_0 primitive $\ell(p^{\mathfrak{f}} - 1)$ te Einheitswurzel, weil aus

$$\omega_0^b = 1$$

folgte $\omega_0^{\ell b} = \omega^b = 1$, also

$$b \equiv 0 \mod p^{\mathfrak{f}} - 1$$

und $\omega_0^{c(p^{\mathfrak{f}}-1)} = \omega^{c\frac{p^{\mathfrak{f}}-1}{\ell}} = 1,$

*) zu $\mathfrak{p}$ prime Element.

d.h. $$c \equiv 0 \mod \ell$$

also $$b \equiv 0 \mod \ell(p^{\mathfrak{f}} - 1);$$

andererseits aber können in $k(\mathfrak{p})$ höchstens die $(p^{\mathfrak{f}} - 1)$ ten Einheitswurzeln, außer ev. p^{ν}–ten vorkommen.

94 IV

Es ist also ω ℓ–ter Nichtrest mod $\mathfrak{p}$, umsomehr mod $\mathfrak{p}^a$, und somit folgt aus (3) unter Berücksichtigung von $\eta = \xi^{\ell}(\mathfrak{p})$ für jeden Modul $\mathfrak{p}^a$ die eindeutige Darstellung

$$\alpha \equiv \omega^c \xi^{\ell} \bmod \mathfrak{p}^a; \qquad (c = 0, 1, \ldots, \ell - 1)$$

Daraus folgt:

$$R(\mathfrak{p}^a) = 1.$$

Satz 27. Ist $\mathfrak{p}$ prim zu ℓ so gilt für jedes $a \geqq 1$:

$$\begin{array}{lll} R(\mathfrak{p}^a) = 1, & \text{wenn} & \Phi(\mathfrak{p}) \equiv 0 \mod \ell, \\ R(\mathfrak{p}^a) = 0, & \text{"} & \Phi(\mathfrak{p}) \equiv 0 \mod \ell. \end{array}$$

2.) Teiler $\mathfrak{l}$ von ℓ.

a.) $k(\mathfrak{l})$ enthält die ℓ–te Einheitswurzel ζ.

Hier läßt sich jedes zu $\mathfrak{l}$ prime α aus $k(\mathfrak{l})$ eindeutig in der Form darstellen:

$$\alpha = \eta_1^{c_1} \ldots \eta_m^{c_m} \eta_a^{c_a} \xi^{\ell} \ (\mathfrak{l}); \qquad (c_i = 0, 1, \ldots, \ell - 1), \tag{4}$$

wobei $m = ef$ und e und f Ordnung und Grad von $\mathfrak{l}$ bedeuten: Die $\eta_1, \ldots, \eta_m$ zerfallen in e Basissysteme von je f Basiseinheiten für die Einseinheiten der e zu ℓ primen Grade der Reihe $1, 2, \ldots, \left[\frac{e\ell}{\ell-1}\right] = \frac{e\ell}{\ell-1}$ *). Ein solches Basissystem für einen bestimmten Grad g ist in dem Sinne unabhängig, daß kein Potenzprodukt aus seinen Einseinheiten ℓ–ter Potenzrest mod $\mathfrak{l}^{g+1}$ ist, wenn nicht alle Exponenten durch ℓ teilbar sind†). Daraus folgt leicht, daß die sämtlichen Basissysteme bis zu einem bestimmten Grad $g < \frac{e\ell}{\ell-1}$ ein System *unabhängiger Nichtreste mod* $\mathfrak{l}^{g+1}$ bilden, da man

95 IV

aus einer etwa doch bestehenden Relation sukzessive auf das Verschwinden

*) Falls ζ in $k(\mathfrak{l})$ enthalten ist, ist $e \equiv 0 \bmod \ell - 1$.

†) Folgt leicht aus den Henselschen Entwicklungen, Cr. 146.

mod ℓ der Exponenten des ersten, zweiten, ... Basissystems schließen kann. Dieses System ist aber auch ein *vollständiges* System unabhängiger Nichtreste mod $\mathfrak{l}^{g+1}$, weil jedes zu $\mathfrak{l}$ prime α auf Grund von (4) auch mod $\mathfrak{l}^{g+1}$ durch dasselbe darstellbar ist. Für $0 \leqq g < \frac{e\ell}{\ell-1}$ ist also $R(\mathfrak{l}^{g+1})$ [3] gleich der Anzahl der Basissysteme bis zum Grade g einschließlich mal f. Da den Multipla von ℓ bis g [4] keine Basissysteme entsprechen, wird die Anzahl jener Basissysteme $g - \left[\frac{g}{\ell}\right]$ also:

$$R(\mathfrak{l}^{g+1}) = gf - \left[\frac{g}{\ell}\right] f \quad \text{für} \quad 0 \leqq g < \frac{e\ell}{\ell - 1}$$

Für den Modul $\mathfrak{l}^{\frac{e\ell}{\ell-1}+1}$ und alle höheren tritt zu den a fortiori unabhängig bleibenden Nichtresten $\eta_1, \ldots, \eta_m$ noch der Nichtrest η_a hinzu, der von ihnen nach den genannten Moduln unabhängig ist, weil aus einer Relation

$$\eta_a \equiv \eta_1^{c_1} \ldots \eta_m^{c_m} \xi^\ell \bmod \mathfrak{l}^{\frac{e\ell}{\ell-1}+1}$$

zunächst mod $\mathfrak{l}^{\frac{e\ell}{\ell-1}}$ folgen würde (es ist $\eta_a \equiv 1 \bmod \mathfrak{l}^{\frac{e\ell}{\ell-1}}$): $c_1, \ldots, c_m = 0$ also

$$\eta_a \equiv \xi^\ell \mod \mathfrak{l}^{\frac{e\ell}{\ell-1}+1}$$

und somit $$\eta_a = \eta^\ell \ (\mathfrak{l}),$$

weil jede Einseinheit $\left(\frac{e\ell}{\ell-1} + 1\right)$ ten Grades nach (4) ℓ–te Potenz in $k(\mathfrak{l})$ ist. Dies ist aber wegen der Eindeutigkeit von (4) nicht möglich.

Es ist also:

$$R(\mathfrak{l}^{g+1}) = ef + 1 \quad \text{für} \quad g \geqq \frac{e\ell}{\ell - 1}.$$

b.) $k(\mathfrak{l})$ enthält keine ℓ–te Einheitswurzel.

Dann tritt an Stelle von (4) eine eindeutige Darstellung:

(4a.) $$\alpha = \eta_1^{c_1} \ldots \eta_m^{c_m} \xi^\ell \ (\mathfrak{l}); \qquad (c_i = 0, 1, \ldots, \ell - 1)$$

in der die ausgezeichnete Einseinheit η_a fehlt. Die $\eta_1, \ldots, \eta_m$ sind wie oben e

[3] undeutlich
[4] undeutlich

Basissysteme von je f Basiseinheiten für die Einseinheiten der e zu ℓ primen Grade der Reihe $1, 2, \ldots, \left[\frac{e\ell}{\ell-1}\right]$, und es folgt genau wie eben, unter Berücksichtigung des Fortfallens von η_a:

$$\begin{aligned} R(\mathfrak{l}^{g+1}) &= gf - \left[\tfrac{g}{\ell}\right] f \quad \text{für} \quad 0 \leqq g < \left[\tfrac{e\ell}{\ell-1}\right], \\ R(\mathfrak{l}^{g+1}) &= ef \qquad\qquad\quad \text{für} \quad g \geqq \left[\tfrac{e\ell}{\ell-1}\right]. \end{aligned}$$

Satz 28. Ist $\mathfrak{l}$ ein Teiler von ℓ der Ordnung e vom Grade f, so gilt für den Rang der Gruppe der primen Restklassen mod $\mathfrak{l}^{g+1}$ nach der Primzahl ℓ:

$$\begin{aligned} R(\mathfrak{l}^{g+1}) &= \left(g - \left[\tfrac{g}{\ell}\right]\right) f, \quad \text{wenn} \quad 0 \leqq g < \left[\tfrac{e\ell}{\ell-1}\right], \\ R(\mathfrak{l}^{g+1}) &= ef + \delta, \qquad\quad \text{wenn} \quad g \geqq \left[\tfrac{e\ell}{\ell-1}\right]. \end{aligned}$$

Dabei ist $\delta = 1$ oder 0, je nachdem $k(\mathfrak{l})$ die primitive ℓ–te Einheitswurzel ζ enthält oder nicht.

Nach Satz 26–28 ist der Rang der Gruppe der primen Restklassen eines beliebigen, ganzen Idealmoduls $\mathfrak{m}$ nach der Primzahl ℓ ohne weiteres angebbar.

C. Die Strahlklassengruppe mod $\mathfrak{m}$

C. Der Rang der Klassengruppe nach dem Strahl $\equiv 1 \bmod \mathfrak{m}$ (für $\ell = 2$ total positiv).

Wir betrachten zunächst die absolute Klassengruppe G vom Grade h. Sei ℓ^ν die genaue Potenz der Primzahl ℓ die in h aufgeht, dann bildet bekanntlich die Gesamtheit aller absoluten Klassen, die zu Potenzen von ℓ als Exponenten gehören, eine Gruppe G_0 vom Grad ℓ^ν und G ist das direkte Produkt

$$G = G_0 \times \mathsf{D} \tag{1}$$

von G_0 mit der Gruppe D aller absoluten Klassen, deren Exponent zu ℓ prim ist.

Es sei dann $\mathfrak{r}_1, \ldots, \mathfrak{r}_t$ ein System der Repräsentanten der Basisklassen von G_0. Diese dürfen prim zu einander, □□□ und überhaupt zu beliebigen (endlich vielen) Idealen angenommen werden, was wir später mehrfach verwenden werden, und sollen überdies als ganz vorausgesetzt werden.

Auf Grund von (1) läßt sich dann jedes Ideal $\mathfrak{a}$ aus k in der Form darstellen:

$$\mathfrak{a} = \mathfrak{r}_1^{\overline{a}_1} \dots \mathfrak{r}_t^{\overline{a}_t} \cdot \mathfrak{d}, \tag{2}$$

wo $\mathfrak{d}$ ein Ideal aus D ist, und die Exponenten $\overline{a}_i$ sind nach den Exponenten ℓ^{ν_i} der $\mathfrak{r}_i$ als Moduln durch die absolute Klasse von $\mathfrak{a}$ eindeutig bestimmt. Da die Exponenten der Ideale $\mathfrak{d}$ von D sämtlich prim zu ℓ sind, können diese in die Form

$$\mathfrak{d} = \mathfrak{j}_0^{\ell}(\beta_0) \tag{3}$$

gebracht werden, wo $\mathfrak{j}_0$ ein Ideal aus D und β_0 eine Zahl aus k ist. Auch $\mathfrak{j}_0$ darf ersichtlich zu beliebigen, endlich vielen Idealen prim angenommen werden. Auf die Tatsache, daß $\mathfrak{j}_0$ zu D gehörig angenommen werden kann, kommt es im folgenden nicht an, nur darauf, daß $\mathfrak{d}$ der ℓ–ten Potenz eines Ideales äquivalent ist. Daher sollen die ℓ–ten Potenzen aus den Faktoren $\mathfrak{r}_i^{\overline{a}_i}$ noch in $\mathfrak{j}_0^{\ell}$ hineingezogen werden, was stets in eindeutiger Weise durch Reduktion der $\overline{a}_i$ auf ihren kleinsten positiven Rest a_i mod ℓ geschehen kann. Da wir uns für das Studium der Klassengruppe nach dem Idealmodul $\mathfrak{m}$ nur mit zu $\mathfrak{m}$ primen Idealen zu beschäftigen haben, sollen die $\mathfrak{r}_i$ prim zu $\mathfrak{m}$ angenommen werden. Dann folgt aus (2), (3)

Satz 29. Sind $\mathfrak{r}_1, \mathfrak{r}_2, \dots, \mathfrak{r}_t$ die zu $\mathfrak{m}$ primen Repräsentanten aus den Basisklassen von G_0, so läßt sich jedes zu $\mathfrak{m}$ prime Ideal $\mathfrak{a}$ aus k mit eindeutig bestimmten Exponenten in der Form:

$$\mathfrak{a} = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} \mathfrak{j}^{\ell}(\beta); \qquad (a_i = 0, 1, \dots, \ell - 1) \tag{4}$$

darstellen, wo $\mathfrak{j}$ ein zu $\mathfrak{m}$ primes Ideal und β eine zu $\mathfrak{m}$ prime Zahl aus k bedeutet.

Es seien weiter $\varrho_1, \dots, \varrho_t$ die kleinsten Potenzen der $\mathfrak{r}_1, \dots, \mathfrak{r}_t$ die Hauptideale sind, also

$$(\varrho_i) = \mathfrak{r}_i^{\ell^{\nu_i}}; \qquad (\nu_i \geqq 1); \qquad (i = 1, 2, \dots, t),$$

weil die $\mathfrak{r}_i$ als Elemente aus G_0 zu Potenzen von ℓ

99 IV

als Exponenten gehören und natürlich selbst nicht Hauptideale sind.

Ferner seien $\varepsilon_1, \ldots, \varepsilon_r$ die r Grundeinheiten von k und ε_{r+1}, falls k die ℓ–te Einheitswurzel ζ enthält, eine primitive ℓ^μ–te Einheitswurzel aus k von möglichst großem μ ($\geqq 1$), also $\varepsilon_1, \ldots, \varepsilon_{r+\delta}$ bei der von früher her geläufigen Bedeutung von δ ein vollständiges Repräsentantensystem für die $r+\delta$ unabhängigen Einheitenverbände in k.

Wir betrachten dann alle Zahlen der Form

$$\alpha = \varepsilon_1^{u_1} \ldots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \ldots \varrho_t^{v_t}; \qquad (u_i, v_i = 0, 1, \ldots, \ell - 1). \tag{5}$$

Soll eine solche Zahl ℓ–te Potenz in k sein, so muß zunächst $\prod_i \mathfrak{r}_i^{\ell^{\nu_i} v_i}$ die ℓ–te Potenz eines Hauptideals sein, also $\prod_i \mathfrak{r}_i^{\ell^{\nu_i - 1} v_i}$ Hauptideal. Da aber die $\mathfrak{r}_i$ als Repräsentanten absoluter Basisklassen in Bezug auf die Gruppe der Hauptideale in dem Sinne unabhängig sind, daß kein Potenzprodukt aus ihnen Hauptideal ist, wenn nicht jeder Exponent durch das zugehörige ℓ^{ν_i} teilbar ist, müssen alle v_i durch ℓ teilbar, also Null sein. Dann müssen aber auch die $u_i = 0$ sein, weil die ε_i Repräsentanten der unabhängigen Einheitenverbände sind.

Die Zahlen (5) sind also in Bezug auf die Gruppe der ℓ–ten Potenzen von Zahlen aus k unabhängig, d.h. die Zahlen der Form:

100 IV

$$\alpha = \varepsilon_1^{u_1} \ldots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \ldots \varrho_t^{v_t} \xi^\ell; \qquad (u_i, v_i = 0, 1, \ldots, \ell - 1), \tag{6}$$

wo ξ alle zu $\mathfrak{m}$ primen Körperzahlen durchläuft, bilden eine Abelsche Gruppe vom Rang $r + \delta + t$ nach ℓ.*)

Wir betrachten nun weiter die Untergruppe aller derjenigen Zahlen (6), die ℓ–te Potenzreste mod $\mathfrak{m}$ sind. Da in ihr alle ℓ–ten Potenzen von Elementen der Gruppe (6) enthalten sind, folgt nach Satz 25, S. 90▶, wenn $n \leqq r + \delta + t$ ihren Rang bezeichnet und

$$\overline{\alpha} = \alpha_1^{x_1} \ldots \alpha_n^{x_n} \xi^\ell; \qquad (x_i = 0, 1, \ldots, \ell - 1) \tag{7}$$

*) Da die $\mathfrak{r}_i$, also die ϱ_i prim zu $\mathfrak{m}$ sind, enthält die Gruppe (6) nur zu $\mathfrak{m}$ prime Zahlen, sodaß es einen Sinn hat, wenn gleich von ℓ–ten Potenzresten mod $\mathfrak{m}$ in dieser Gruppe geredet wird.

ihre eindeutige Basisdarstellung ist, daß $r + \delta + t - n = \mathsf{N}'$ weitere, zu $\mathfrak{m}$ prime Zahlen $\gamma_1, \ldots, \gamma_{\mathsf{N}'}$ in (6) gefunden werden können, sodaß alle Zahlen der Gruppe (6) sich auch eindeutig in der Form darstellen lassen:

$$\alpha = \gamma_1^{y_1} \ldots \gamma_{\mathsf{N}'}^{y_{\mathsf{N}'}} \alpha_1^{x_1} \ldots \alpha_n^{x_n} \xi^{\ell}; \qquad (x_i, y_i = 0, 1, \ldots, \ell - 1). \tag{8}$$

Die Basisdarstellung (7) der genannten Untergruppe lehrt, daß es abgesehen von ℓ–ten Potenzfaktoren in der Gruppe (6) genau ℓ^n verschiedene ℓ–te Potenzreste gibt. Die Zahl n läßt sich also dadurch charakterisieren, daß ℓ^n die Anzahl der verschiedenen ℓ–ten Potenzreste mod $\mathfrak{m}$ unter den $\ell^{r+\delta+t} = \ell^{n+\mathsf{N}'}$ Zahlen (5) ist.

Ein in der Form (8) dargestelltes α aus der Gruppe (6) ist dann und nur dann ℓ–ter Potenzrest mod $\mathfrak{m}$, wenn alle Exponenten $y_i = 0$ sind (Satz 25). Daher sind die

Zahlen $\gamma_1, \ldots, \gamma_{\mathsf{N}'}$ unabhängige Nichtreste mod $\mathfrak{m}$; es hat somit die Gruppe aller Restklassen mod $\mathfrak{m}$ der Form:

$$\gamma \equiv \gamma_1^{y_1} \ldots \gamma_{\mathsf{N}'}^{y_{\mathsf{N}'}} \xi^{\ell} \mod \mathfrak{m}, \tag{9}$$

wo ξ alle zu $\mathfrak{m}$ primen Restklassen durchläuft, den Rang N' nach ℓ. Diese Gruppe (9) ist Untergruppe der Gruppe aller primen Restklassen mod $\mathfrak{m}$ vom Range $R(\mathfrak{m})$. Es lassen sich somit, wieder nach Satz 25, weitere $\mathsf{N} = R(\mathfrak{m}) - \mathsf{N}'$ Restklassen mit den Repräsentanten $\eta_1, \ldots, \eta_{\mathsf{N}}$ finden, sodaß jede zu $\mathfrak{m}$ prime Zahl β in der Form

$$\beta \equiv \eta_1^{z_1} \ldots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \gamma_1^{y_1} \ldots \gamma_{\mathsf{N}'}^{y_{\mathsf{N}'}} \xi^{\ell} \mod \mathfrak{m} \qquad (z_i, y_i = 0, 1, \ldots, \ell - 1) \tag{10}$$

eindeutig darstellbar ist.

Die η_i sind dann ebenfalls unter sich und von den γ_i unabhängige Nichtreste, die mit den γ_i zusammen ein volles System solcher bilden.

Setzt man für jedes in der Form (10) dargestellte β:

$$\beta = \eta_1^{z_1} \ldots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \gamma_1^{y_1} \ldots \gamma_{\mathsf{N}'}^{y_{\mathsf{N}'}} \alpha \xi^{\ell}, \tag{11}$$

so ist

$$\alpha \equiv 1 \mod \mathfrak{m},$$

gehört also zu dem für die zu untersuchende Klasseneinteilung zugrundezulegenden Strahl o, definiert durch

$$\alpha \equiv 1 \mod \mathfrak{m}.$$

Die Darstellung (11) aller zu $\mathfrak{m}$ primen β führen wir nun in die Darstellung (4) aller zu $\mathfrak{m}$ primen Ideale $\mathfrak{a}$ ein und erhalten, daß jedes zu $\mathfrak{m}$ prime Ideal $\mathfrak{a}$ in der Form darstellbar ist:

$$(12) \qquad \mathfrak{a} = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} (\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \alpha)\, \mathfrak{j}^{\ell}; \qquad (a_i, z_i = 0, 1, \dots, \ell - 1),$$

102 IV

wo α Zahl aus o und $\mathfrak{j}$ ein zu $\mathfrak{m}$ primes Ideal ist, weil ja die γ_i als Zahlen der Gruppe (6) sicher ℓ–te Idealpotenzen sind und daher in $\mathfrak{j}^{\ell}$ hineingezogen werden dürfen, ebenso auch ξ^{ℓ}. (Dabei bleibt $\mathfrak{j}$ zu $\mathfrak{m}$ prim).

Ich behaupte nun, daß zwei in der Form (12) dargestellte, zu $\mathfrak{m}$ prime Ideale □□□ nur dann nach dem Strahl o äquivalent sein können, wenn ihre Exponentenreihen a_i, z_i übereinstimmen. Dazu ist nur zu zeigen, daß ein in dieser Form (12) dargestelltes Ideal $\mathfrak{a}$ nur dann Strahlhauptideal nach dem Strahl o sein kann, wenn alle $a_i, z_i = 0$ sind.

Damit $\mathfrak{a}$ in (12) Strahlhauptideal ist, muß es zunächst absolutes Hauptideal sein, und dann müssen nach Satz 29, (4) alle Exponenten $a_i = 0$ sein. Es muß dann ferner

$$\mathfrak{r} = (\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \alpha)\mathfrak{j}^{\ell}$$

Strahlhauptideal sein, also jedenfalls $\mathfrak{j}^{\ell}$ absolutes Hauptideal. Setzt man nun der Zerlegung (1) entsprechend*):

$$\mathfrak{j} = \mathfrak{b} \cdot \mathfrak{c}, \quad \text{also} \quad \mathfrak{j}^{\ell} = \mathfrak{b}^{\ell} \cdot \mathfrak{c}^{\ell}; \qquad (\mathfrak{b} \text{ aus } G_0;\ \mathfrak{c} \text{ aus } \mathsf{D}),$$

so muß der Unabhängigkeit von G_0 und D wegen jeder Faktor für sich Hauptideal sein. Daraus folgt, daß der zu D gehörige Faktor $\mathfrak{c}$ selbst Hauptideal sein muß, also

$$\mathfrak{j} = \mathfrak{b} \cdot (\gamma).$$

Das Ideal $\mathfrak{b}$ aus G_0 läßt sich durch die Repräsentanten

103 IV

der (absoluten) Basisklassen von G_0 in der Form:

$$\mathfrak{b} = \mathfrak{r}_1^{c_1} \dots \mathfrak{r}_t^{c_t} (\beta)$$

*) Natürlich dürfen die Faktoren $\mathfrak{b}, \mathfrak{c}$ von $\mathfrak{j}$ zu $\mathfrak{m}$ prim angenommen werden, weil es $\mathfrak{j}$ ist, und es nur auf deren (absolute) Klasse ankommt.

schreiben. Da $\mathfrak{b}^\ell$ Hauptideal sein muß, folgt

$$c_i\ell \equiv 0 \mod \ell^{\nu_i}; \qquad \text{(S. 98 unten)}$$

also

$$\mathfrak{b}^\ell = \mathfrak{r}_1^{c_1\ell} \dots \mathfrak{r}_t^{c_t\ell}(\beta^\ell) = \left(\varrho_1^{b_1} \cdots \varrho_t^{b_t}\beta^\ell\right),$$

wo die b_i aus $c_i\ell = b_i\ell^{\nu_i}$ bestimmt sind. Reduziert man die b_i noch auf ihre kleinsten positiven Reste v_i mod ℓ, so folgt somit für $\mathfrak{j}^\ell$ eine Darstellung:

$$\mathfrak{j}^\ell = \left(\varrho_1^{v_1} \dots \varrho_t^{v_t}\xi^\ell\right); \qquad (v_i = 0, 1, \dots, \ell-1),$$

wo ξ zu $\mathfrak{m}$ prim ist.

Es muß dann also

$$\mathfrak{a} = \left(\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \varrho_1^{v_1} \dots \varrho_t^{v_t}\alpha\xi^\ell\right)$$

Strahlhauptideal, also mit einer passenden Einheit ε

$$\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \varrho_1^{v_1} \dots \varrho_t^{v_t}\varepsilon\alpha\xi^\ell \equiv 1 \mod \mathfrak{m}$$

sein. Stellt man ε durch die $r+\delta$ unabhängigen Verbände–Repräsentanten $\varepsilon_1, \dots, \varepsilon_{r+\delta}$ in der Form

$$\varepsilon = \varepsilon_1^{u_1} \dots \varepsilon_{r+\delta}^{u_{r+\delta}}\eta^\ell; \qquad (u_i = 0, 1, \dots, \ell-1)$$

dar, und läßt α, das sicher zu o gehört, fort, so muß also

$$\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \varrho_1^{v_1} \dots \varrho_t^{v_t} \varepsilon_1^{u_1} \dots \varepsilon_{r+\delta}^{u_{r+\delta}} \overline{\xi}^\ell \equiv 1 \mod \mathfrak{m}$$

sein, wo alle Exponenten zwischen 0 und $\ell-1$ liegen. Der Ausdruck $\varrho_1^{v_1} \dots \varrho_t^{v_t} \varepsilon_1^{u_1} \dots \varepsilon_{r+\delta}^{u_{r+\delta}} \overline{\xi}^\ell$ ist aber von der Form (6) und läßt sich mithin auch in der Form (8) darstellen, sodaß

$$\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \gamma_1^{y_1} \dots \gamma_{\mathsf{N}'}^{y_{\mathsf{N}'}} \alpha_1^{x_1} \dots \alpha_n^{x_n} \overline{\overline{\xi}}^\ell \equiv 1 \mod \mathfrak{m}$$

sein muß, wo wieder alle Exponenten zwischen 0 und $\ell-1$ angenommen werden dürfen. Die α_i können dann als ℓ–te Potenzreste mod $\mathfrak{m}$ in $\overline{\overline{\xi}}^\ell$ hineingezogen werden, da sie η_i und γ_i, wie oben gezeigt, untereinander unabhängige

Nichtreste sind, müssen also alle $y_i = 0$ und insbesondere alle $z_i = 0$ sein, w.z.b.w.

Damit ist jetzt gezeigt, daß die Ideale (12), wenn die a_i, z_i unabhängig von 0 bis $\ell - 1$ laufen, sämtlich verschiedenen Klassen nach dem Strahl o angehören. Umgekehrt aber läßt sich jedes zu $\mathfrak{m}$ prime Ideal auf die Form (12) bringen. Geht man zu den Idealklassen nach o über und bezeichnet die Klassen nach o von:

$$\mathfrak{r}_1, \ldots, \mathfrak{r}_t; \;\; \eta_1, \ldots, \eta_{\mathsf{N}}$$

bezw. mit

$$\mathfrak{k}_1, \ldots, \mathfrak{k}_t; \;\; \mathfrak{k}_{t+1}, \ldots, \mathfrak{k}_{t+\mathsf{N}},$$

so läßt sich jede Klasse $\mathfrak{k}$ nach o in der Form

$$\mathfrak{k} = \mathfrak{k}_1^{a_1} \ldots \mathfrak{k}_t^{a_t} \mathfrak{k}_{t+1}^{z_1} \ldots \mathfrak{k}_{t+\mathsf{N}}^{z_{\mathsf{N}}} \mathfrak{k}_0^{\ell}; \qquad (a_i, z_i = 0, 1, \ldots, \ell - 1)$$

schreiben, und andererseits folgt aus dem Bewiesenen, daß $\mathfrak{k}$ dann und nur dann die Hauptklasse nach o, oder noch allgemeiner ℓ–te Potenz einer Klasse nach o ist, wenn alle Exponenten $a_i, z_i = 0$ sind. Es ist somit $\mathfrak{k}_1, \ldots, \mathfrak{k}_t, \mathfrak{k}_{t+1}, \ldots, \mathfrak{k}_{[\ldots]}$ ein System in Bezug auf die Gruppe k_0^{ℓ} unabhängiger Klassen, und zwar das vollständige System solcher Klassen, und die Zahl $t + \mathsf{N}$ der Rang der Klassengruppe nach o für die Primzahl ℓ. Führt man für N seinen Wert

$$\mathsf{N} = R(\mathfrak{m}) - \mathsf{N}' = R(\mathfrak{m}) + n - (r + \delta) - t$$

ein, so folgt also:

105 IV

Satz 30. Es seien die Idealklassen in k nach dem Strahl o der Zahlen $\equiv 1 \bmod \mathfrak{m}$ definiert. Dann hat die Gruppe der Idealklassen nach der Primzahl ℓ den Rang

$$\bar{t} = R(\mathfrak{m}) + n - (r + \delta).$$

Dabei bedeutet $R(\mathfrak{m})$ den Rang der Gruppe der primen Restklassen mod $\mathfrak{m}$ nach ℓ, $r + \delta$ die Anzahl der unabhängigen Einheitenverbände in k und ℓ^n die Anzahl der ℓ–ten Potenzreste mod $\mathfrak{m}$ in dem System der Zahlen

$$\varepsilon_1^{u_1} \ldots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \ldots \varrho_t^{v_t}; \qquad (u_i, v_i = 0, 1, \ldots, \ell - 1),$$

wobei die ε_i, ϱ_i die oben erklärte Bedeutung haben.

Für $\ell \neq 2$ genügt die in diesem Satz zugrundegelegte Idealklassendefinition. Für $\ell = 2$ kommen wir jedoch mit ihr nicht aus, sondern brauchen noch Vorzeichenfestsetzungen.

Es mögen für $\ell = 2$ r_1 reelle konjugierte zu k vorkommen, sodaß 2^{r_1} Signaturen vorhanden sind. o sei wie bisher der Strahl der Zahlen $\equiv 1 \bmod \mathfrak{m}$, die $\mathfrak{r}_i, \varrho_i, \varepsilon_i$ haben die bisherige Bedeutung ($\delta = 1$). Ferner Sei V eine Signaturgruppe vom Grade 2^{r_0} und o^+ [5] der Strahl der Zahlen aus o mit Signatur aus V.

Wir führen dann die obigen Betrachtungen bis zur Aufstellung der Gruppe (6) und ihrer Untergruppe (7) unverändert durch. Nunmehr betrachten wir die Untergruppe

106 IV

derjenigen Zahlen von (7), die eine Signatur aus V haben. Da jedes Quadrat eines Elementes von (7) total positiv ist, also sicher eine Signatur aus V hat, ist wieder Satz 25, S. 90 anwendbar:

Sei n_0 ($\leqq n$) der Rang der eben definierten Untergruppe und

$$\overline{\beta} = \beta_1^{b_1} \dots \beta_{n_0}^{b_{n_0}} \xi^2; \qquad (b_i = 0, 1) \tag{7a.}$$

ihre eindeutige Basisdarstellung, so müssen noch $n - n_0$ weitere Zahlen $a\alpha'_1, \dots, \alpha'_{n-n_0}$ in (7) existieren, sodaß

$$\overline{\alpha} = \alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} \beta_1^{b_1} \dots \beta_{n_0}^{b_{n_0}} \xi^2; \qquad (b_i, c_i = 0, 1) \tag{7b.}$$

wieder die Gruppe (7) in eindeutiger Basisdarstellung ist. Eine Zahl aus (7b.) hat also dann und nur dann eine Signatur aus V, wenn alle $c_i = 0$ sind.

□□□

107 IV

Die Zahl n_0 ist dann dadurch charakterisiert, daß 2^{n_0} die Anzahl der quadratischen Reste mit Signatur aus V in der Gruppe (6) ist, wenn man von den Faktoren ξ^2, die stets quadratische Reste mit Signatur aus V sind, absieht; 2^{n_0} ist also entsprechend dem früheren die Anzahl der quadratischen Reste mod $\mathfrak{m}$ mit Signatur aus V in dem System (5).

Die α'_i bestimmen eine Signaturgruppe V' von 2^{n-n_0} Signaturen, d.h. vom Range $n - n_0$; (da eine Signatur dann und nur dann Quadrat einer Signatur ist, wenn sie die total positive, also das Einheitselement aller Signaturgruppen, ist, fallen für die Signaturgruppen die Begriffe „Rang nach der Primzahl

[5] undeutlich

2“ und „Anzahl der unabhängigen Basiselemente“ zusammen). Denn wie bei (7b.) festgestellt, kann speziell kein Potenzprodukt aus den α'_i total positiv sein, wenn nicht alle Exponenten durch 2 teilbar sind. Es kann aber überdies sogar keine Relation

$$\alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} = \text{Zahl mit Sign. aus } V; \qquad (c_i = 0, 1)$$

bestehen, wenn nicht alle c_i Null sind, wie sich ebenfalls aus (7b.) ergab.

Betrachten wir also die volle Signaturgruppe Σ und zerlegen sie in das direkte Produkt

$$\Sigma = V \times W, \tag{13}$$

so ist V' Untergruppe von W. Denn W ist infolge dieser Zerlegung als die Gesamtheit aller derjenigen Signaturen

charakterisiert, von denen außer dem Einheitselement (total positive Signatur) kein Produkt zu V gehört. W hat den Rang $r - r_0$. Setzt man also

$$W = V' \times W',$$

so hat W' den Rang $p = (r_1 - r_0) - (n - n_0)$. Eine Basis von W' liefert also weitere p Signaturen, die durch die Elemente $\beta'_1, \dots, \beta'_p$ charakterisiert sein mögen, sodaß in der Form

$$\alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} \beta'^{e_1}_1 \dots \beta'^{e_p}_p; \qquad (c_i, e_i = 0, 1) \tag{14}$$

alle Signaturen aus W eindeutig darstellbar sind. Da in jeder Restklasse mod $\mathfrak{m}$ Zahlen jeder Signatur vorhanden sind, dürfen wir die Vertreter β'_i unserer p Signaturen $\equiv 1 \bmod \mathfrak{m}$ annehmen.

Wir verwenden diese Überlegungen, um die Zahl $\alpha \equiv 1 \bmod \mathfrak{m}$ (aus o), die in unserer obigen Darstellung (12) jedes zu $\mathfrak{m}$ primen Ideals $\mathfrak{a}$ auftritt noch weiter zu zerspalten, nämlich in einen Faktor α^{+}[6] aus o^+ und ein Potenzprodukt aus unseren neu erhaltenen Elementen β'_i.

Habe α die Signatur σ und sei

$$\sigma = \sigma_V \cdot \sigma_W$$

[6] undeutlich

die Zerlegung von σ nach V und W auf Grund von (13). Dann bestimmen wir zunächst eine Zahl $\overline{\alpha}^+ \equiv 1 \bmod \mathfrak{m}$ mit der Signatur σ_V, die also zu o^+ gehört. Der Quotient $\frac{\alpha}{\overline{\alpha}^+}$ hat dann die Signatur σ_W, stellt sich also bis auf

109 IV

einen total positiven Faktor η eindeutig durch ein bestimmtes Potenzprodukt (14) in der Form dar:

$$\frac{\alpha}{\overline{\alpha}^+} = \alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} \beta'^{e_1}_1 \dots \beta'^{e_p}_p \eta.$$

Da die α'_i quadratische Reste und $\frac{\alpha}{\alpha^+}$ sowie die $\beta'_i \equiv 1 \bmod \mathfrak{m}$ sind, ist auch η quadratischer Rest mod $\mathfrak{m}$:

$$\eta \equiv \xi^2 \bmod \mathfrak{m},$$

sodaß

$$\eta = \overline{\overline{\alpha}}^+ \xi^2$$

gesetzt werden kann, wo auch $\overline{\overline{\alpha}}^+$ als total positive Zahl jedenfalls zu o^+ gehört. Somit wird

$$\alpha = \alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} \beta'^{e_1}_1 \dots \beta'^{e_p}_p \alpha^+ \xi^2; \qquad (c_i, e_i = 0, 1)$$

wo α^+ Zahl aus o^+, und wenn man diesen Ausdruck für α in (12) einführt, jedes zu $\mathfrak{m}$ prime Ideal $\mathfrak{a}$ in der Form darstellbar:

(12a.)
$$\mathfrak{a} = \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} \left(\eta_1^{z_1} \dots \eta_{\mathsf{N}}^{z_{\mathsf{N}}} \beta'^{e_1}_1 \dots \beta'^{e_p}_p \alpha^+\right) \mathfrak{j}^2; \qquad (a_i, z_i, e_i = 0, 1),$$

weil ja die α'_i als Zahlen der Gruppe (7), also (6) Idealquadrate sind und ebenso wie ξ^2 in $\mathfrak{j}^2$ hereingezogen werden dürfen.

Ein Ideal $\mathfrak{a}$ der Form (12a.) kann nun nur dann Strahlhauptideal nach dem Strahl o^+ sein, wenn alle Exponenten $a_1, \dots, a_t, z_1, \dots, z_{\mathsf{N}}, e_1, \dots, e_p$ Null sind. Zunächst müssen nämlich alle a_i, z_i verschwinden, weil ja $\mathfrak{a}$ a fortiori Strahlhauptideal nach o sein muß, und also wegen $\beta'^{e_1}_1 \dots \beta'^{e_p}_p \alpha^+ \equiv 1 \bmod \mathfrak{m}$ die Betrachtungen von vorhin über den Ausdruck (12) anwendbar sind.

110 IV

Es muß also nunmehr

$$(\beta'^{e_1}_1 \dots \beta'^{e_p}_p \alpha^+)\mathfrak{j}^2$$

Strahlhauptideal nach o^+ sein. $\mathfrak{j}^2$ muß wie oben wieder die Form haben:

$$\mathfrak{j}^2 = (\varrho_1^{v_1} \dots \varrho_t^{v_t} \xi^2),$$

wenn es überhaupt (absolutes) Hauptideal sein soll. Daher folgt wie oben, daß eine Kongruenz

$$\beta'^{e_1}_1 \dots \beta'^{e_p}_p \varepsilon_1^{u_1} \dots \varepsilon_{r+1}^{u_{r+1}} \varrho_1^{v_1} \dots \varrho_t^{v_t} \xi^2 \equiv 1 \bmod \mathfrak{m}$$

mit der Vorzeichenbedingung: „Signatur aus V“ bestehen muß. Da die $\beta'_i \equiv 1 \bmod \mathfrak{m}$ sind, muß dann das Aggregat der ε_i, ϱ_i quadratischer Rest mod $\mathfrak{m}$, also als Element der Gruppe (7) in der Form in der Form (7b.) darstellbar sein, sodaß eine Kongruenz resultiert:

$$\beta'^{e_1}_1 \dots \beta'^{e_p}_p \alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} \beta_1^{b_1} \dots \beta_{n_0}^{b_{n_0}} \xi^2 \equiv 1 \bmod \mathfrak{m} \quad \text{und Signatur aus } V,$$

d.h.

$$\beta'^{e_1}_1 \dots \beta'^{e_p}_p \alpha'^{c_1}_1 \dots \alpha'^{c_{n-n_0}}_{n-n_0} \longrightarrow \text{Signatur aus } V.$$

Da dies nach der eindeutigen Darstellung (14) der Gruppe W infolge der Bedeutung von W nur so möglich ist, daß alle Exponenten Null sind, folgt also speziell: $e_i = 0$, w.z.b.w.

Da umgekehrt durch jeden Ausdruck (12a.) bis auf das Quadrat einer Klasse nach o^+ eine bestimmte Klasse nach o^+ dargestellt wird, folgt wie oben für den Rang der Klassengruppe nach o^+ der Wert:

$$\begin{aligned} t + \mathsf{N} + p &= R(\mathfrak{m}) + n - (r+1) + (r_1 - r_0) - (n - n_0) \\ &= R(\mathfrak{m}) + n_0 + r_1 - (r + r_0 + 1). \end{aligned}$$

Satz 31. Es seien die Idealklassen in k nach dem Strahl o^+ der Zahlen $\equiv 1 \bmod \mathfrak{m}$ mit der Vorzeichenbedingung V definiert, wo V eine Gruppe von 2^{r_0} Signaturen ist. Dann hat die Gruppe der Idealklassen nach der Primzahl 2 den Rang

$$\bar{t} = R(\mathfrak{m}) + n_0 + r_1 - (r + r_0 + 1).$$

Dabei bedeutet $R(\mathfrak{m})$ den Rang der Gruppe der primen Restklassen mod $\mathfrak{m}$ nach 2, r_1 die Anzahl der reellen konjugierten zu k, $r+1$ die Anzahl der unabhängigen Einheitenverbände (nach 2) in k und 2^{n_0} die Anzahl der quadratischen Reste mit Signatur aus V in dem System der Zahlen:

$$\varepsilon_1^{u_1} \dots \varepsilon_{r+1}^{u_{r+1}} \varrho_1^{v_1} \dots \varrho_t^{v_t},$$

wo die ε_i, ϱ_i die oben erklärte Bedeutung haben.

4.3 §3 Die Kummerschen Körper

112 IV

A. Primideale und Relativdiskriminante

In diesem § werde durchweg vorausgesetzt, daß der Grundkörper k die primitive ℓ–te Einheitswurzel ζ enthält, was im Spezialfalle $\ell = 2$ a fortiori erfüllt ist. Unter dieser Voraussetzung läßt sich jeder relativ–zyklische Körper K vom Primzahlgrad ℓ über k durch eine reine Gleichung

$$x^\ell - \mu = 0$$

aus k erzeugen, wo μ eine Zahl aus k ist, die in k keine ℓ–te Potenz ist.

Ist nämlich A irgendein erzeugendes Element von K, σ die erzeugende Substitution der zyklischen Gruppe von K nach k, also $\sigma^\ell = 1$, so betrachten wir die Lagrangesche Resolvente:

$$\mathsf{A} = \mathsf{A} + \zeta\sigma\mathsf{A} + \zeta^2\sigma^2\mathsf{A} + \cdots + \zeta^{\ell-1}\sigma^{\ell-1}\mathsf{A}$$

Diese ist sicher $\neq 0$, weil A keiner Gleichung $(\ell-1)$–ten Grades in k genügen kann. Ferner ist

$$\sigma\Lambda = \zeta^{-1}\Lambda,$$

also Λ^ℓ invariant gegen σ, d.h. ein Element μ aus k, und wie man leicht zeigt, natürlich keine ℓ–te Potenz in k. Daher kann $\Lambda = \sqrt[\ell]{\mu}$ als erzeugendes Element von K genommen werden.

Man nennt jeden solchen Körper $k(\sqrt[\ell]{\mu})$ einen *Kummerschen Körper* über k; es ist also unter unserer Voraussetzung über k jeder relativ–zyklische Körper vom Primzahlgrad ℓ über k ein Kummerscher Körper.

113 IV

Die Substitutionsgruppe eines Kummerschen Körpers $K = k(\sqrt[\ell]{\mu})$ kann durch die Substitution

$$\sigma = (\sqrt[\ell]{\mu} : \zeta\sqrt[\ell]{\mu})$$

erzeugt werden.

Infolge unserer Voraussetzung, daß die ℓ–te Einheitswurzeln ζ in k enthalten sein soll, gilt für jedes zu ℓ prime Primideal $\mathfrak{p}$ aus k die Kongruenz

$$N\mathfrak{p} \equiv 1 \bmod \ell.$$

Es müssen nämlich die ℓ–ten Einheitswurzeln auch in jedem $k(\mathfrak{p})$ vorkommen, also wenn $N\mathfrak{p} = p^f$ ist, ℓ ein Teiler von $p^f - 1$ sein, da $k(\mathfrak{p})$ außer ev. p^ν–ten Einheitswurzeln nur die $(p^f - 1)$ ten enthält.

Jede Zahl μ aus $k(\mathfrak{p})$ gestattet dann eine Darstellung:

$$\mu = \pi^a \omega^b \xi^\ell \ (\mathfrak{p}); \qquad (a, b = 0, 1, \dots \ell - 1)$$

wo π Primzahl für $\mathfrak{p}$ und ω eine primitive $(p^f - 1)$ te Einheitswurzel aus $k(\mathfrak{p})$ ist. Nach S. 93 ist wegen $\Phi(\mathfrak{p}) = N\mathfrak{p} - 1$ hier stets ω keine ℓ–te Potenz in $k(\mathfrak{p})$ und auch kein ℓ–ter Potenzrest mod $\mathfrak{p}$ (was übrigens gleichwertig, da jede Einseinheit aus $k(\mathfrak{p})$ ℓ–te Potenz in $k(\mathfrak{p})$ ist). Daher ist die obige Darstellung *eindeutig*.

Die Einheitswurzel ω darf so gewählt werden, daß

$$\omega^{\frac{p^f-1}{\ell}} = \zeta$$

die ein– für allemal fest gewählte, primitive ℓ–te Einheitswurzel ζ ist. Ist dann für ein zu $\mathfrak{p}$ primes μ:

$$\mu = \omega^b \xi^\ell \ (\mathfrak{p})$$

so heißt

$$\left(\frac{\mu}{\mathfrak{p}}\right) = \zeta^b \equiv \mu^{\frac{p^f-1}{\ell}} \bmod \mathfrak{p}$$

der *ℓ–te Potenzrestcharakter* von μ nach $\mathfrak{p}$, und es gilt:

Satz 32. Ein zu $\mathfrak{p}$ primes μ ist dann und nur dann ℓ–ter Potenzrest nach $\mathfrak{p}$, wenn $\left(\frac{\mu}{\mathfrak{p}}\right) = 1$ ist. Die sämtlichen primen Restklassen mod $\mathfrak{p}$ zerfallen in ℓ gleich starke Teilsysteme mit den Potenzrestcharakteren $1, \zeta, \dots, \zeta^{\ell-1}$.

Beweis. Ist $\mu \equiv \xi_0^\ell \bmod \mathfrak{p}$, so ist $\mu = \xi^\ell \, (\mathfrak{p})$, also in obiger Darstellung $b = 0$ und umgekehrt. Daraus folgt der erste Teil. Der zweite Teil einfach daraus,

daß die ℓ–ten Potenzreste mod $\mathfrak{p}$ eine Untergruppe der primen Restklassen mod $\mathfrak{p}$ bilden. Deren Nebengruppen sind dann jedesmal alle Restklassen gleichen Potenzrestcharakters. Daß jedem Potenzrestcharakter eine Nebengruppe entspricht ist klar, weil $\left(\frac{\omega^b}{\mathfrak{p}}\right) = \zeta^b$ ist.

Wie aus den Henselschen Arbeiten (Cr. 151) folgt, gilt folgendes Zerlegungsgesetz für die zu ℓ primen $\mathfrak{p}$ in $K = k\left(\sqrt[\ell]{\mu}\right)$.

Satz 33. Ist $\mathfrak{p}$ ein zu ℓ primes Primideal aus k und geht $\mathfrak{p}$ in μ zu einer Potenz auf, deren Exponent prim zu ℓ ist, so wird in $K = k\left(\sqrt[\ell]{\mu}\right)$:

$$\mathfrak{p} = \mathfrak{P}^\ell; \qquad \text{(Grad 1)}.$$

Ist aber μ durch eine Potenz von $\mathfrak{p}$ genau teilbar, deren Exponent ein Vielfaches von ℓ ist, so darf ohne Beschränkung μ prim zu $\mathfrak{p}$ angenommen werden und es ist in $K = \left(\sqrt[\ell]{\mu}\right)$:

115 IV

$$\mathfrak{p} = \mathfrak{P} \cdot \sigma\mathfrak{P} \dots \sigma^{\ell-1}\mathfrak{P}; \quad \text{(Grad 1), wenn } \left(\frac{\mu}{\mathfrak{p}}\right) = 1,$$

$$\mathfrak{p} = \mathfrak{P}; \quad \text{(Grad } \ell\text{), wenn } \left(\frac{\mu}{\mathfrak{p}}\right) \neq 1.$$

Für die Zerlegung der Primteiler $\mathfrak{l}$ von ℓ ist die multiplikative Normalform in $k(\mathfrak{l})$ heranzuziehen. Sind e, f Ordnung und Grad von $\mathfrak{l}$, $ef = m$, so läßt sich jedes Element aus $k(\mathfrak{l})$ eindeutig in der Form darstellen:*):

$$\mu = \lambda^a \eta_1^{c_1} \dots \eta_m^{c_m} \eta_a^{c_a} \xi^\ell \ (\mathfrak{l}); \qquad (a, c_i = 0, 1, \dots, \ell - 1).$$

Dabei ist λ Primzahl für $\mathfrak{l}$, $\eta_1, \dots, \eta_m$ ein System von e Basissystemen von je f Einseinheiten für die e zu ℓ primen Grade der Reihe $1, 2, \dots, \frac{e\ell}{\ell-1}$ und $\eta_a = 1 + w\lambda_0^\ell$; $(\lambda_0 = 1 - \zeta)$ eine „ausgezeichnete Einseinheit“ $\left(s_\mathfrak{l}(w) = w + w^\ell + \dots + w^{\ell^{f-1}} \neq 0 \bmod \ell\right)$ des Grades $\frac{ef}{\ell-1}$.

Hat ein zu $\mathfrak{l}$ primes μ die Darstellung

$$\mu = \eta_r^{c_r} \dots \eta_m^{c_m} \eta^{c\left[\begin{smallmatrix}\cdot\cdot\cdot\\ \cdot\cdot\cdot\end{smallmatrix}\right]} \xi^\ell \ (\mathfrak{l}); \qquad (c_i = 0, 1, \dots, \ell - 1),$$

*) Hensel–Hasse, Math. Ann.

wo der erste nicht verschwindende Exponent c_r (bei nach steigenden Graden geordnetem Fundamentalsystem) zu einem η_r vom Grade g gehört, so ist für $1 \leqq g \leqq \frac{e\ell}{\ell-1}$:

$$\mu \equiv \xi^{\ell} \mod \mathfrak{l}^{g}$$

aber nicht $\mu \equiv \xi^{\ell} \mod \mathfrak{l}^{g+1}$; (s. S. 94▶).

Mit dieser Bemerkung läßt sich das Henselsche Resultat über die Zerlegung von $\mathfrak{l}$ in $k\left(\sqrt[\ell]{\mu}\right)$ so aussprechen:

116 IV

Satz 34. Ist $\mathfrak{l}$ ein Primteiler von ℓ aus k der Ordnung e vom Grade f und geht $\mathfrak{l}$ in μ zu einer Potenz auf, deren Exponent prim zu ℓ ist, so wird in $K = k\left(\sqrt[\ell]{\mu}\right)$:

$$\mathfrak{l} = \mathfrak{L}^{\ell}; \qquad \text{(Grad 1)}.$$

Ist aber μ durch eine Potenz von $\mathfrak{l}$ genau teilbar, deren Exponent ein Vielfaches von ℓ ist, so darf ohne Beschränkung μ prim zu $\mathfrak{l}$ angenommen werden. Ist dann $\mathfrak{l}^{g}$ der höchste Modul für den noch

$$\mu \equiv \xi^{\ell} \mod \mathfrak{l}^{g}$$

ist, so ist in $K = k\left(\sqrt[\ell]{\mu}\right)$:

$$\begin{array}{lcll} \mathfrak{l} & = & \mathfrak{L}^{\ell}; & \text{(Grad 1)}, \quad \text{wenn } 1 \leqq g < \frac{e\ell}{\ell-1}, \\ \mathfrak{l} & = & \mathfrak{L}; & \text{(Grad } \ell\text{)}, \quad \text{wenn } g = \frac{e\ell}{\ell-1}, \\ \mathfrak{l} & = & \mathfrak{L} \cdot \sigma\mathfrak{L} \cdots \sigma^{\ell-1}\mathfrak{L}; & \text{(Grad 1)}, \quad \text{wenn } g = \infty.^{\dagger)} \end{array}$$

Nach den allgemeinen Sätzen von §1, A. (S. 1▶–11▶), läßt sich ferner die Relativdiskriminante von K hier vollständig bestimmen. Geht ein zu ℓ primes Primideal $\mathfrak{p}$ in ihr auf (also $\mathfrak{p} = \mathfrak{P}^{\ell}$), so ist natürlich schon nach Satz 1, S. 1

$$\mathfrak{D}_{\mathfrak{p}} = \mathfrak{p}^{\ell-1}.$$

Für die Diskriminantenteiler unter den $\mathfrak{l}$ muß aber der Exponent v von

$$\mathfrak{D}_{\mathfrak{p}} = \mathfrak{l}^{(v+1)(\ell-1)}; \qquad \text{(Satz 2, S. 2▶/3▶)}$$

noch bestimmt werden.

$^{\dagger)}$Im Falle $g > \frac{e\ell}{\ell-1}$ ist nämlich $\mu = \xi^{\ell}$ ($\mathfrak{l}$), also nach jeder noch so hohen Potenz von $\mathfrak{l}$ ℓ–ter Potenzrest.

117 IV

Liegt nun erstens der erste Fall von Satz 34 vor, so darf durch geeignete Transformation der Grundgleichung und Einführung einer geeigneten Primzahl λ:

$$\mu = \lambda \ (\mathfrak{l})$$

angenommen werden. Dann wird $\Lambda = \sqrt[\ell]{\lambda}$ Primzahl von $K(\mathfrak{L})$ und

$$\frac{\sigma\Lambda}{\Lambda} = \zeta = 1 - \lambda_0,$$

wo λ_0 die Primzahl $1-\zeta$ des Kreiskörpers k_ζ ist. Wegen

$$\lambda_0 \sim \ell^{\frac{1}{\ell-1}} \sim \mathfrak{l}^{\frac{e}{\ell-1}} \sim \mathfrak{L}^{\frac{e\ell}{\ell-1}}$$

ist $\frac{\sigma\Lambda}{\Lambda}$ Einseinheit genau vom Grade $\frac{e\ell}{\ell-1}$, also das v von Satz 2:*)

$$v = \frac{e\ell}{\ell-1},$$

somit

$$\mathfrak{D}_\mathfrak{l} = \mathfrak{l}^{\left(\frac{e\ell}{\ell-1}+1\right)(\ell-1)} = \mathfrak{l}^{e\ell+\ell-1}.$$

Liegt zweitens der andere Fall von Satz 34 vor, wo $\mathfrak{l} = \mathfrak{L}^\ell$, also die Relativdiskriminante $\mathfrak{D}_\mathfrak{l}$ durch $\mathfrak{l}$ teilbar ist, so darf (Hensel, Cr. 151) μ in der Form

$$\mu = 1 - w\lambda^g \ (\mathfrak{l})$$

angenommen werden, wo g als einer der Grade des Fundamentalsystems $\eta_1, \ldots, \eta_m$ prim zu ℓ ist, und w eine Einheit aus $k(\mathfrak{l})$ ist. Dann ist

$$\Lambda = \frac{(1-\sqrt[\ell]{\mu})^{g_1}}{\lambda^{\ell_1}}; \qquad (gg_1 - \ell\ell_1 = 1)$$

eine Primzahl für $K(\mathfrak{L})$ und

118 IV

$$\frac{\sigma\Lambda}{\Lambda} = \left(\frac{1-\zeta\sqrt[\ell]{\mu}}{1-\sqrt[\ell]{\mu}}\right)^{g_1} = \left(\frac{1-\sqrt[\ell]{\mu}+(1-\zeta)\sqrt[\ell]{\mu}}{1-\sqrt[\ell]{\mu}}\right)^{g_1}$$
$$= \left(1+\sqrt[\ell]{\mu}\frac{\lambda_0}{\Lambda_g}\right)^{g_1}$$

*) s.a. S. 22, Anmerkung.

wo $\Lambda_g = 1 - \sqrt[\ell]{\mu}$ genau durch $\mathfrak{L}^g$ teilbar ist. In der Klammer steht also eine Einseinheit genau vom Grade $\frac{e\ell}{\ell-1} - g$ in $\mathfrak{L}$, der g_1–te Potenz genau von demselben Grade ist, weil g_1 prim zu ℓ ist. Nach Satz 2 ist somit

$$v = \frac{e\ell}{\ell - 1} - g,$$

in Übereinstimmung mit der letzten Behauptung von Satz 2, weil $1 \leqq g < \frac{e\ell}{\ell-1}$, also auch $1 \leqq v < \frac{e\ell}{\ell-1}$ wird, und mit g auch v prim zu ℓ ist, weil $\frac{e\ell}{\ell-1} \equiv 0 \bmod \ell$ ist. Wir haben dann

$$\mathfrak{D}_\mathfrak{l} = \mathfrak{l}^{\left(\frac{e\ell}{\ell-1}-g+1\right)(\ell-1)} = \mathfrak{l}^{e\ell-(g-1)(\ell-1)}.$$

Um beide Fälle in eins zusammenfassen zu können, setzen wir im ersten Falle $g = 0$. Das stimmt mit der Definition von g überein, □□□ wenn wir diese etwas allgemeiner so fassen:

„Sei μ genau durch $\mathfrak{l}^a$ teilbar[†)] und g die größte □□□ Zahl, für die noch die Kongruenz

$$\mu \equiv \xi^\ell \mod \mathfrak{l}^{a+g}$$

lösbar ist."

Denn wenn a prim zu ℓ ist, ist diese Kongruenz mod $\mathfrak{l}^a$ noch durch $\xi = 0$ lösbar, mod $\mathfrak{l}^{a+1}$ aber nicht mehr, da dann μ mod $\mathfrak{l}^{a+1}$ nicht mehr verschwindet, andererseits ξ^ℓ stets eine durch ℓ teilbare Ordnung [...] hat.

Mit dieser Verallgemeinerung kann übrigens auch die in Satz 34 der Einfachheit halber gemachte Annahme: „μ prim zu $\mathfrak{l}$, wenn genau durch $\mathfrak{l}^{a\ell}$ teilbar" entbehrt werden:

Für die Relativdiskriminante erhalten wir:

Satz 35. Geht ein zu ℓ primes Primideal $\mathfrak{p}$ in der Relativdiskriminante $\mathfrak{D}$ des Kummerschen Körpers $k\left(\sqrt[\ell]{\mu}\right)$ auf, so ist

$$\mathfrak{D}_\mathfrak{p} = \mathfrak{p}^{\ell-1}.$$

Geht ein Teiler $\mathfrak{l}$ von ℓ der Ordnung e in der Relativdiskriminante von $k\left(\sqrt[\ell]{\mu}\right)$ auf und ist $\mathfrak{p}$ die größte ganze Zahl, für die noch die Kongruenz

$$\mu \equiv \xi^\ell \bmod \mathfrak{l}^{a+g}$$

[†)] a kann dabei positiv, Null oder negativ sein!

lösbar ist, wo μ genau durch $\mathfrak{l}^a$ teilbar ist, also nach Satz 34:

$$0 \leqq g < \frac{e\ell}{\ell - 1},$$

so ist:

$$\mathfrak{D}_\mathfrak{l} = \mathfrak{l}^{\left(\frac{e\ell}{\ell-1} - g + 1\right)(\ell-1)} = \mathfrak{l}^{e\ell - (g-1)(\ell-1)}$$

B. Unabhängigkeit Kummerscher Körper

Satz 36. Ist der Kummersche Körper $k\left(\sqrt[\ell]{\mu}\right)$ enthalten im Kompositum $k\left(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2}, \ldots, \sqrt[\ell]{\mu_\nu}\right)$ der ν Kummerschen Körper $k\left(\sqrt[\ell]{\mu_i}\right)$, so besteht eine Relation

$$\mu = \mu_1^{c_1} \ldots \mu_\nu^{c_\nu} \alpha^\ell; \qquad (c_i = 0, 1, \ldots, \ell - 1)$$

wo α eine Zahl aus k ist.

Beweis. Wir beweisen den Satz zuerst für $\nu = 1$. Es sei also $k\left(\sqrt[\ell]{\mu_1}\right)$ ein Kummerscher Körper über k. Ist dann $k\left(\sqrt[\ell]{\mu}\right)$ irgendein anderer Kummerscher Körper, so ist entweder $k\left(\sqrt[\ell]{\mu}\right)$ mit $k\left(\sqrt[\ell]{\mu_1}\right)$ identisch, oder der Durchschnitt beider Körper gleich k, da ja, weil der Relativgrad ℓ eine Primzahl ist, keine echten Teilkörper der zyklischen Körper $k\left(\sqrt[\ell]{\mu_1}\right)$, $k\left(\sqrt[\ell]{\mu}\right)$ existieren.

Aus unserer Voraussetzung folgt also für $\nu = 1$ zunächst:

$$k\left(\sqrt[\ell]{\mu}\right) = k\left(\sqrt[\ell]{\mu_1}\right).$$

Dann läßt sich $\sqrt[\ell]{\mu}$ rational durch $\sqrt[\ell]{\mu_1}$ in der Form darstellen:

$$\sqrt[\ell]{\mu} = \varphi\left(\sqrt[\ell]{\mu_1}\right) = \gamma_0 + \gamma_1 \sqrt[\ell]{\mu_1} + \cdots + \gamma_{\ell-1} \sqrt[\ell]{\mu_1}^{\ell-1},$$

wo die γ_i in k liegen. Ersetzt man $\sqrt[\ell]{\mu_1}$ durch die konjugierte $\zeta\sqrt[\ell]{\mu_1}$, so muß auch $\sqrt[\ell]{\mu}$ in eine konjugierte $\zeta^\kappa \sqrt[\ell]{\mu}$ übergehen. Also ist

$$\zeta^\kappa \left(\sqrt[\ell]{\mu}\right) = \varphi\left(\zeta\sqrt[\ell]{\mu_1}\right)$$

oder

$$\zeta^\kappa \varphi\left(\sqrt[\ell]{\mu}\right) = \varphi\left(\zeta\sqrt[\ell]{\mu_1}\right),$$

d.h.

$$\sum_{i=0}^{\ell-1} \zeta^{\kappa}\gamma_i \sqrt[\ell]{\mu_1}^{i} = \sum_{i=0}^{\ell-1} \gamma_i \zeta^{i} \sqrt[\ell]{\mu_1}^{i}.$$

Der Eindeutigkeit wegen (ζ liegt in k) muß also sein:

$$\zeta^{\kappa}\gamma_i = \zeta^{i}\gamma_i; \qquad (i = 0, 1, \ldots, \ell - 1)$$

d.h. $$\gamma_i = 0 \qquad \text{für } \kappa \neq i$$

Es ist also

$$\sqrt[\ell]{\mu} = \gamma_{\kappa} \sqrt[\ell]{\mu_1}^{\kappa},$$

(und da $\sqrt[\ell]{\mu}$ nicht in k liegt, $\kappa \neq 0$) d.h.

$$\mu = \mu_1^{\kappa}\gamma_{\kappa}^{\ell}$$

womit der Satz für $\nu = 1$ bewiesen ist.

Sei nun der Satz schon bis $\nu - 1$ bewiesen. Ist $\sqrt[\ell]{\mu}$ schon in $k_1 = k\left(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_{\nu-1}}\right)$ enthalten, so ist nach dieser Annahme der Satz richtig. Sei also $\sqrt[\ell]{\mu}$ noch nicht in k_1 enthalten, wohl aber in $k_1\left(\sqrt[\ell]{\mu_\nu}\right)$. Dann ist auch $\sqrt[\ell]{\mu_\nu}$ nicht in k_1 enthalten, da sonst $\sqrt[\ell]{\mu}$ doch in $k_1 = k_1\left(\sqrt[\ell]{\mu_\nu}\right)$ enthalten wäre. $\sqrt[\ell]{\mu_\nu}$ definiert also einen Kummerschen Körper über k_1, der den Kummerschen Körper $k_1\left(\sqrt[\ell]{\mu_\nu}\right)$ enthält, und daher mit ihm identisch ist:

$$k_1\left(\sqrt[\ell]{\mu}\right) = k_1\left(\sqrt[\ell]{\mu_\nu}\right).$$

Nach dem Bewiesenen ist daher

$$\mu = \mu_\nu^{c_\nu}\alpha_1^{\ell},$$

wo α_1 Zahl aus k_1 ist. Diese Zahl stellt sich in der Form

$$\alpha_1 = \sqrt[\ell]{\frac{\mu}{\mu_\nu^{c_\nu}}}$$

dar. k_1 muß also den Kummerschen Körper $k(\alpha_1) = k\left(\sqrt[\ell]{\frac{\mu}{\mu_\nu^{c_\nu}}}\right)$ enthalten, und also nach Annahme (für $\nu - 1$):

$$\alpha_1^{\ell} = \frac{\mu}{\mu_\nu^{c_\nu}} = \mu_1^{c_1} \ldots \mu_{\nu-1}^{c_{\nu-1}}\alpha^{\ell}; \qquad (\alpha \text{ in } k)$$

also $$\mu = \mu_1^{c_1} \dots \mu_\nu^{c_\nu} \alpha^\ell, \qquad \text{w.z.b.w.}$$

(Natürlich darf dann $0 \leqq c_i \leqq \ell - 1$ angenommen werden.

122 IV

Wir nennen nun ν Kummersche Körper $k\left(\sqrt[\ell]{\mu_1}\right), \dots, k\left(\sqrt[\ell]{\mu_\nu}\right)$ *voneinander unabhängig*, wenn für jedes i der Körper $k_i = k\left(\sqrt[\ell]{\mu_i}\right)$ teilerfremd ist zu dem Kompositum der übrigen $K_i = k\left(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_{i-1}}, \sqrt[\ell]{\mu_{i+1}}, \dots, \sqrt[\ell]{\mu_\nu}\right)$. Natürlich genügt die Forderung, daß er nicht in diesem Kompositum enthalten sein soll.

Satz 37. Für die Unabhängigkeit der ν durch $\mu_1, \dots, \mu_\nu$ definierten Kummerschen Körper $k_i = k\left(\sqrt[\ell]{\mu_i}\right)$ ist notwendig und hinreichend, daß die ν Zahlen μ_i in Bezug auf die Gruppe der ℓ–ten Potenzen in k unabhängig sind, d.h. daß keine Zahl

$$\mu_1^{c_1} \dots \mu_\nu^{c_\nu}; \qquad (c_i = 0, 1, \dots, \ell - 1)$$

außer wenn alle $c_i = 0$ sind, ℓ–te Potenz in k ist.

Beweis. 1.) Die Bedingung ist notwendig. Denn ist

$$\mu_1^{c_1} \dots \mu_\nu^{c_\nu} = \xi^\ell$$

und etwa $c_1 \not\equiv 0 \bmod \ell$, ferner $c_1 c_1' \equiv 1 \bmod \ell$, dann ist

$$\mu_1 = \mu_2^{-c_2 c_1'} \mu_3^{-c_3 c_1'} \dots \mu_\nu^{-c_\nu c_1'} \xi'^\ell,$$

also $k_1 = k\left(\sqrt[\ell]{\mu_1}\right)$ in $K_1 = k\left(\sqrt[\ell]{\mu_2}, \dots, \sqrt[\ell]{\mu_\nu}\right)$ enthalten.

2.) Die Bedingung ist auch hinreichend. Denn ist etwa k_1 in K_1 enthalten, so folgt aus Satz 36:

$$\mu_1 = \mu_2^{c_2} \dots \mu_\nu^{c_\nu} \xi^\ell,$$

also eine Relation von der im Satze ausgeschlossenen Form, da der Exponent von μ_1 nicht $\equiv 0 \bmod \ell$ ist.

123 IV

Sind ν Kummersche Körper $k_i = k\left(\sqrt[\ell]{\mu_i}\right)$ unabhängig, so ist offenbar die Galoissche Gruppe des komponierten Körpers

$$K = k\left(\sqrt[\ell]{\mu_1}, \dots, \sqrt[\ell]{\mu_\nu}\right)$$

die Abelsche Gruppe

$$\sigma_1^{c_1} \dots \sigma_\nu^{c_\nu}; \qquad (0 \leqq c_i \leqq \ell - 1) \tag{1}$$

vom Grade ℓ^ν, wo $\sigma_i = \left(\sqrt[\ell]{\mu_i} : \zeta\sqrt[\ell]{\mu_i}\right)$ die erzeugende Substitution der Gruppe von k_i ist.

Zunächst ist nämlich K Normalkörper über k und die Substitutionen (1) sämtlich Substitutionen von K. Ferner sind die Substitutionen (1) kommutativ, also (1) eine Abelsche Gruppe. Denn führt man in jedem Summanden der Darstellung

$$\mathsf{A} = \sum_j \alpha_j \sqrt[\ell]{\mu_1}^{c_{j1}} \dots \sqrt[\ell]{\mu_\nu}^{c_{j\nu}}; \qquad (c_{ji} = 0, 1, \dots, \ell - 1) \qquad (\alpha_j \text{ aus } k)$$

einer beliebigen Zahl von K nacheinander die Substitutionen $\tau_1 = \sigma_1^{a_1} \dots \sigma_\nu^{a_\nu}$ und $\tau_2 = \sigma_1^{b_1} \dots \sigma_\nu^{b_\nu}$ aus, so wird

$$\tau_1\tau_2\mathsf{A} = \tau_2\tau_1\mathsf{A} = \sum_j \alpha_j \zeta^{c_{j1}(a_1+b_1)+\dots+c_{j\nu}(a_\nu+b_\nu)} \sqrt[\ell]{\mu_1}^{c_{j1}} \dots \sqrt[\ell]{\mu_\nu}^{c_{j\nu}},$$

unabhängig von der Reihenfolge. Schließlich sind die ℓ^ν Substitutionen (1) sämtlich verschwinden. Dies folgt indirekt daraus, daß K vom Grade ℓ^ν über k ist. Es ist nämlich wegen der Unabhängigkeit speziell $\sqrt[\ell]{\mu_i}$ nicht in $k\left(\sqrt[\ell]{\mu_1} \dots \sqrt[\ell]{\mu_{i-1}}\right)$ enthalten, also $k\left(\sqrt[\ell]{\mu_1} \dots \sqrt[\ell]{\mu_i}\right)$ vom ℓ–ten Relativgrade über $k\left(\sqrt[\ell]{\mu_1} \dots \sqrt[\ell]{\mu_{i-1}}\right)$ für $i = 1, \dots, \nu$, und der Gesamtrelativgrad ineinandergeschachtelter Körper allgemein stets das Produkt der sukzessiven Relativgrade. Daher muß die Galoissche Gruppe von K den Grad ℓ^ν haben, und da keine anderen, als die Substitutionen (1), die alle denkbaren „Konjugierten–Bildungen“ erschöpfen, existieren, müssen sie alle verschieden sein und die Galoissche Gruppe von K bilden.

Jedes Element der Gruppe (1) gehört zum Exponenten ℓ, bestimmt also eine zyklische Untergruppe ℓ–ten Grades. Andrerseits gehört jeder Unterkörper von K vom Grade ℓ zu einer Untergruppe von (1) vom Index ℓ, deren Faktorgruppe zyklisch vom Grade ℓ ist und seine Galoissche Gruppe in Bezug auf k darstellt. Als zyklischer Körper ℓ–ten Grades ist jeder solche Unterkörper ein Kummerscher Körper $k\left(\sqrt[\ell]{\mu}\right)$ über k, also nach Satz 36:

$$\mu = \mu_1^{c_1} \dots \mu_\nu^{c_\nu} \alpha^\ell; \qquad (c_i = 0, 1, \dots \ell - 1). \tag{2}$$

Die Anzahl der Unterkörper ℓ–ten Grades von K läßt sich demnach leicht angeben. Entweder zählt man die Anzahl der in der Form (2) enthaltenen, nicht durch Relationen

$$\mu' = \mu^c \alpha^\ell; \qquad (c_i = 0, 1, \ldots, \ell - 1)$$

zusammenhängenden μ ab und findet leicht $\frac{\ell^\nu - 1}{\ell - 1}$ auf Grund der Unabhängigkeit der μ_i. Oder man benutzt die eindeutige Zuordnung der Unterkörper ℓ–ten Grades zu den Untergruppen vom Index ℓ. Aus der gegenseitigen Eindeutigkeit folgt, daß die gesuchte Körperanzahl gleich der Anzahl der Untergruppen von (1) vom Index ℓ, und somit nach Satz 24 gleich $\frac{\ell^\nu - 1}{\ell - 1}$ ist, weil (1) ersichtlich den Rang ν hat. Es gilt also:

Satz 38. Sind die ν Kummerschen Körper $k\left(\sqrt[\ell]{\mu_i}\right)$ unabhängig, so enthält der Abelsche Körper ℓ^ν–ten Grades

$$K = k\left(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_\nu}\right)$$

genau $\frac{\ell^\nu - 1}{\ell - 1}$ verschiedene Kummersche Körper $k\left(\sqrt[\ell]{\mu}\right)$, wo dann jedesmal

$$\mu = \mu_1^{c_1} \ldots \mu_\nu^{c_\nu}; \qquad (c_i = 0, 1, \ldots, \ell - 1)$$

gesetzt werden kann.

125 IV

Ich beweise ferner noch einen wichtigen Satz über das Legendresche Symbol. Dazu ist zunächst folgender Satz zu beweisen:

Satz 39. Damit das zu $\mu_1, \ldots, \mu_\nu$ und ℓ prime Primideal $\mathfrak{p}$ aus k in K in lauter verschiedene Primideale ersten Relativgrades zerfällt, ist notwendig und hinreichend, daß

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) = \left(\frac{\mu_2}{\mathfrak{p}}\right) = \cdots = \left(\frac{\mu_\nu}{\mathfrak{p}}\right) = 1$$

ist. (Voraussetzung und Bezeichnungen wie in Satz 38).

Beweis. 1.) Zerfällt $\mathfrak{p}$ in K in lauter verschiedene Primideale ersten Relativgrades, so gilt dasselbe für $k_i = k\left(\sqrt[\ell]{\mu_i}\right)$, da der Relativgrad für k_i ein Teiler desjenigen für K sein muß, und die Zerlegung $\mathfrak{p} = \mathfrak{P}^\ell$ in k_i nach den Voraussetzungen über $\mathfrak{p}$ ausgeschlossen ist. Nach Satz 33 ist also $\left(\frac{\mu_i}{\mathfrak{p}}\right) = 1$ für jedes i.

2.) Ist umgekehrt $\left(\frac{\mu_i}{\mathfrak{p}}\right) = 1$ für jedes i, so zerfällt $\mathfrak{p}$ nach Satz 33 in allen k_i in ℓ verschiedene Primideale ersten Relativgrades. Sei dann $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in K, f sein Relativgrad und $\mathfrak{G}_Z$ seine Zerlegungsgruppe. Zunächst kann $\mathfrak{P}$ höchstens zur ersten Potenz in $\mathfrak{p}$ aufgehen, da sonst die Relativdiskriminante von K durch $\mathfrak{p}$ teilbar wäre, während nach den Voraussetzungen über $\mathfrak{p}$ die Relativdiskriminanten aller k_i, also auch die von K prim zu $\mathfrak{p}$ sind (A.Z. I, S. 20, Satz 10). Die Zerlegungsgruppe $\mathfrak{G}_Z$ hat also den Grad f. Da ferner f auch der Relativgrad von $\mathfrak{P}$ nach k_i ist – (Relativgrade der Teiler von $\mathfrak{p}$ in k_i nach k sind 1) – hat auch die Zerlegungsgruppe $\overline{\mathfrak{G}}_Z$ von $\mathfrak{P}$ in Bezug auf k_i den Grad f. Nun gilt

$$\overline{\mathfrak{G}}_Z = (\mathfrak{G}_Z, \mathfrak{H}),$$

wenn k_i zur Gruppe $\mathfrak{H}$ gehört. Also ist $\overline{\mathfrak{G}}_Z = \mathfrak{G}_Z$ und $\mathfrak{G}_Z/\mathfrak{H}$, d.h. der Zerlegungskörper K_Z Oberkörper von k_i[1]. Da dies für jedes i gilt, ist K_Z Oberkörper von

$$(k_1, \ldots, k_\nu) = K$$

also $$K_Z = K,$$

d.h. $$\mathfrak{G}_Z = 1,\ f = 1, \qquad \text{w.z.b.w.}$$

Wir verwenden nun Satz 39 zum Beweis des folgenden Satzes:

Satz 40. Sind $\mu_1, \ldots, \mu_\nu$ in Bezug auf die Gruppe der ℓ–ten Potenzen unabhängige Zahlen aus k, so gibt es unendlich viele Primideale ersten Grades in k, für die gilt:

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) \neq 1; \quad \left(\frac{\mu_2}{\mathfrak{p}}\right) = \cdots = \left(\frac{\mu_\nu}{\mathfrak{p}}\right) = 1.$$

Beweis. Wir betrachten die Körper $k_1 = k\left(\sqrt[\ell]{\mu_2}, \ldots, \sqrt[\ell]{\mu_\nu}\right)$ und $K = k_1\left(\sqrt[\ell]{\mu_1}\right) = k\left(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_\nu}\right)$. Die Primideale ersten Grades aus k, welche in k_1 in lauter verschiedene Primideale ersten Relativgrades zerfallen, bestehen aus 2 Arten:

1.) solche $\mathfrak{p}_1$, die in K nicht in versch. Primideale 1. R.Gr. zerfallen
2.) " $\mathfrak{p}_2$, " " " doch " " " " " "

Dabei dürfen wir von den endlich vielen Primidealen der betrachteten Art absehen, die in K gleiche Faktoren bekommen, ebenso von den endlich vielen

[1] undeutlich

zu ℓ nicht primen Primidealen.

127 IV

Nach A.Z. II, S. 141 angewendet auf k_1 und K ist nun

$$\left.\begin{array}{rrcll} \sum_{\mathfrak{p}_1} \frac{1}{N\mathfrak{p}_1^s} + \sum_{\mathfrak{p}_2} \frac{1}{N\mathfrak{p}_2^s} & = & \frac{1}{\ell^{\nu-1}} \log \frac{1}{s-1} & +\psi_1(s), & \\ \sum_{\mathfrak{p}_2} \frac{1}{N\mathfrak{p}_2^s} & = & \frac{1}{\ell^{\nu}} \log \frac{1}{s-1} & +\psi_2(s), & \\ \text{also:} \quad \sum_{\mathfrak{p}_1} \frac{1}{N\mathfrak{p}_1^s} & = & \frac{\ell-1}{\ell^{\nu}} \log \frac{1}{s-1} & +\psi_3(s). & \end{array}\right\} \quad \begin{array}{l} \psi_1, \psi_2, \psi_3 \text{ endlich} \\ \text{für } s \to 1. \end{array}$$

Für $s \to 1$ folgt, daß die $\mathfrak{p}_1$ in unendlicher Anzahl vorhanden sind. Nach Satz 39 angewendet auf k_1 und K haben aber die $\mathfrak{p}_1$ gerade die verlangte Eigenschaft.

Durch passende Kombination der μ_i (Matrizenreduktion) erhält man aus Satz 40 noch leicht folgenden allgemeineren Satz:

Satz 41. Sind $\mu_1, \ldots, \mu_\nu$ Zahlen aus k wie in Satz 40, ferner $a_1, \ldots, a_\nu$ beliebige ganze Zahlen, so gibt es in k unendlich viele Primideale 1. Grades, für die gilt:

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) = \zeta^{ca_1}; \ \ldots \ ; \ \left(\frac{\mu_\nu}{\mathfrak{p}}\right) = \zeta^{ca_\nu}.$$

Dabei ist c eine mit dem jeweiligen $\mathfrak{p}$ veränderliche, zu ℓ prime ganze Zahl.

Beweis. Ist $a_1 \equiv \cdots \equiv a_\nu \equiv 0 \bmod \ell$, so ist der Satz klar, (sogar unabhängig von der Voraussetzung unabhängiger μ_i), da es ja in K unendlich viele Primideale absolut 1. Grades gibt. Ist aber etwa $a_1 \not\equiv 0 \bmod \ell$, so kann man $\nu - 1$ ganze Zahlen $b_2, \ldots, b_\nu$ bestimmen, sodaß $\zeta^{a_1 b_2 + a_2}, \ldots, \zeta^{a_1 b_\nu + a_\nu} = 1$ wird. Setzt man dementsprechend $\mu_1^{b_2}\mu_2 = \alpha_2, \ldots, \mu_1^{b_\nu}\mu_\nu = \alpha_\nu$, so wird die gestellte Forderung gleichwertig mit:

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) = \zeta^{ca_1} \neq 1; \quad \left(\frac{\alpha_2}{\mathfrak{p}}\right) = \cdots = \left(\frac{\alpha_\nu}{\mathfrak{p}}\right) = 1$$

also, da auch die $\mu_1, \alpha_2, \ldots, \alpha_\nu$ unabhängig, mit einem gewissen $c \not\equiv 0$ ([...] erfüllbar nach Satz 40.

4.4 §4 Existenz des Klassenkörpers

§4. Existenzbeweis des Klassenkörpers.

A. Existenz bei Primzahlgrad ℓ mit ℓ–ter E.W.

A. Existenz des Klassenkörpers vom Primzahlrelativgrad ℓ, wenn der Grundkörper k die ℓ–te Einheitswurzel ζ enthält.

Es enthalte k die ℓ–te Einheitswurzel ζ, was für $\ell = 2$ stets zutrifft. In k sei ein beliebiger ganzer Idealmodul $\mathfrak{m}$ gegeben. In $\mathfrak{m}$ mögen aufgehen:

1.) d verschiedene zu ℓ prime Primideale $\mathfrak{p}$ in irgendeiner Potenz $\mathfrak{p}^a$; $(a \geqq 1)$.

2.) d' verschiedene Teiler $\mathfrak{l}$ von ℓ in einer Potenz $\mathfrak{l}^{g+1}$ [1], wo $g \geqq \frac{e\ell}{\ell-1}$; ($e$ Ordnung von $\mathfrak{l}$).

3.) Eventuell eine Anzahl, (auf die es nicht ankommt), von Teilern $\mathfrak{l}_1$ von ℓ in einer Potenz $\mathfrak{l}_1^{g_1+1}$, wo $0 \leqq g_1 < \frac{e_1\ell}{\ell-1}$; ($e_1$ Ordnung von $\mathfrak{l}_1$).

Die eventuell noch übrigen, nicht in $\mathfrak{m}$ aufgehenden Teiler von ℓ seien mit $\mathfrak{l}'$, ihre Ordnung und Grad mit e', f' bezeichnet.

Nach Satz 25, S. 91 ist dann

$$R(\mathfrak{m}) = \sum_{\mathfrak{p}} R(\mathfrak{p}^a) + \sum_{\mathfrak{l}} R(\mathfrak{l}^g) + \sum_{\mathfrak{l}_1} R(\mathfrak{l}_1^{g_1}),$$

also nach Satz 27, 28, S. 94, 96, weil nach Annahme über k stets $\Phi(\mathfrak{p}) = N\mathfrak{p} - 1$ durch ℓ teilbar ist:

$$R(\mathfrak{m}) = d + d' + \sum_{\mathfrak{l}} ef + \sum_{\mathfrak{l}_1} \left(g_1 - \left[\frac{g_1}{\ell} \right] \right) f_1,$$

[1] undeutlich

wenn f, f_1 die Grade von $\mathfrak{l}, \mathfrak{l}_1$ sind.

Im Falle $\ell = 2$ mögen unter den r_1 reellen konjugierten Körpern eine beliebige Anzahl $k_1, \ldots, k_\nu$ ausgewählt sein.

129 IV

Für alle bisher definierten Anzahlen d, d', Anzahl der $\mathfrak{l}_1, \mathfrak{l}'$ und ν sei auch der Wert 0 zugelassen, sodaß z.B. speziell auch $\mathfrak{m} = 1$ mit umfaßt wird. Alle Entwicklungen werden auch für diesen Spezialfall gelten.

Im Falle $\ell \neq 2$ sei nun o der Strahl der Zahlen $\equiv 1 \bmod \mathfrak{m}$, im Falle $\ell = 2$ seien die Zahlen des Strahles o außerdem noch der Vorzeichenbedingung V unterworfen, daß sie in $k_1, \ldots, k_\nu$ positiv sind. Dies bedeutet eine Signaturgruppe V vom Grade $2^{r_1-\nu}$, (da die Vorzeichen in $r_1 - \nu$ Körpern willkürlich sind), der die Signaturen der Zahlen aus o angehören sollen.

Die Idealklassen in k seien dann nach dem Strahl o definiert. Der Rang $\bar{t}$ ihrer Gruppe ist dann nach Satz 30, 31, S. 105, 111 wegen $\delta = 1$, $r_0 = r_1 - \nu$:

$$\begin{aligned} \bar{t} &= R(\mathfrak{m}) + n - (r+1), && \text{wenn} \quad \ell \neq 2, \\ \bar{t} &= R(\mathfrak{m}) + n_0 + \nu - (r+1), && \text{wenn} \quad \ell = 2. \end{aligned}$$

Dabei ist ℓ^n bezw. 2^{n_0} die Anzahl der ℓ–ten Potenzreste, ev. mit Vorzeichenbedingung V, die in dem System

$$(1) \qquad \varepsilon_1^{u_1} \ldots \varepsilon_{r+1}^{u_{r+1}} \varrho_1^{v_1} \ldots \varrho_t^{v_t}; \qquad (u_i, v_i = 0, 1, \ldots, \ell - 1)$$

enthalten sind. Die ε_i, ϱ_i haben die frühere Bedeutung. Die Ideale $\mathfrak{r}_i$, aus denen die $(\varrho_i) = \mathfrak{r}_i^{\ell^{\nu_i}}$ entstehen, seien jetzt untereinander, zu ℓ und den $\mathfrak{p}$, somit auch zu $\mathfrak{m}$ prim, was anzunehmen nach dem a. S. 97 gesagten gestattet ist.

Im Falle $\ell = 2$ soll von jetzt an n statt n_0 geschrieben werden.

130 IV

Setzt man für $R(\mathfrak{m})$ den oben angegebenen Wert ein, so wird dann:

$$(2.) \quad \bar{t} = d + d' + \sum_{\mathfrak{l}} ef + \sum_{\mathfrak{l}_1} \left(g_1 - \left[\tfrac{g_1}{\ell}\right]\right) f_1 + n - (r+1) \qquad \text{für } \ell \neq 2,$$

$$(2a.) \quad \bar{t} = d + d' + \sum_{\mathfrak{l}} ef + \sum_{\mathfrak{l}_1} \left(g_1 - \left[\tfrac{g_1}{\ell}\right]\right) f_1 + n + \nu - (r+1) \qquad \text{für } \ell = 2.$$

Die Anzahl der Klassengruppen vom Index ℓ berechnet sich dann auf Grund von Satz 24, S. 89 zu $\frac{\ell^{\bar{t}}-1}{\ell-1}$.

Wir führen nun den Existenzbeweis des Klassenkörpers für jede Klassengruppe mod $\mathfrak{m}$ vom Index ℓ nicht einzeln sondern gleich für alle diese $\frac{\ell^{\bar{t}}-1}{\ell-1}$ Klassengruppen gemeinsam, indem wir die Existenz von mindestens ebensoviel relativ–zyklischen Körpern vom Primzahlgrad ℓ über k (also Kummerschen Körpern) nachweisen, deren Klassenkörper–Eigenschaft für eine Klassengruppe mod $\mathfrak{m}$ wir auf Grund der Sätze 21, 21a, S. 59, 62 erschließen. Aus der Eindeutigkeit des Klassenkörpers ergibt sich dann die Existenz für jede einzelne Klassengruppe.

Zu unserm Beweis ist es erforderlich, in den Modul $\mathfrak{m}$ noch eine Anzahl Hilfsprimideale mitaufzunehmen, ohne die es nicht möglich ist, die Existenz der mindest–notwendigen Anzahl von $\frac{\ell^{\bar{t}}-1}{\ell-1}$ verschiedenen Kummerschen Körpern mit den erforderlichen Eigenschaften zu beweisen. Diese Hilfsprimideale entstammen aus folgenden Betrachtungen:

Wir verwendeten früher (S. 100, (7)) die Untergruppe:

131 IV

$$\overline{\alpha} = \alpha_1^{x_1} \dots \alpha_n^{x_n} \xi^{\ell}; \qquad (x_i = 0, 1, \dots, \ell - 1) \tag{3}$$

der Gruppe

$$\alpha = \varepsilon_1^{u_1} \dots \varepsilon_{r+1}^{u_{r+1}} \varrho_1^{v_1} \dots \varrho_t^{v_t} \xi^{\ell}; \qquad (u_i, v_i = 0, 1, \dots, \ell - 1), \tag{4}$$

bestehend aus den ℓ–ten Potenzresten mod $\mathfrak{m}$, ev. mit Vorzeichenbedingung V. (Bei der festgesetzten Bedeutung von n ist diese Untergruppe im Falle $\ell = 2$ zu identifizieren mit der Untergruppe (7a.), S. 106). Da die α_i nach ihrer Bedeutung als „Rangbasis“ in Bezug auf die ℓ–ten Potenzen in k unabhängig sind, gibt es nach Satz 40, S. 126 unendliche viele Systeme von je n Primidealen $\mathfrak{q}_i$ aus k, für die gilt:

$$\left(\frac{\alpha_i}{\mathfrak{q}_i}\right) \neq 1; \quad \left(\frac{\alpha_i}{\mathfrak{q}_j}\right) = 1; \quad (i \neq j)\ ; \quad (i = 1, 2, \dots, n) \tag{5}$$

Wir bestimmen ein solches System $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ so, daß die $\mathfrak{q}_i$ sämtlich prim sind zu ℓ, $\mathfrak{m}$, und den $\mathfrak{r}_i$ sind, und bilden den Modul

$$\overline{\mathfrak{m}} = \mathfrak{m}\mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_n.$$

Nach diesem Modul $\overline{\mathfrak{m}}$ ist dann im System (1) nur der eine einzige ℓ–te Potenzrest 1 enthalten, wenn für $\ell = 2$ noch die Vorzeichenbedingung V

gefordert wird. In der Tat müßte ein solcher zunächst ℓ–ter Potenzrest (ev. mit Vorzeichenbedingung) mod $\mathfrak{m}$ sein, also von der Form

$$\overline{\alpha} = \alpha_1^{x_1} \dots \alpha_n^{x_n} \xi^{\ell}; \qquad (x_i = 0, 1, \dots, \ell - 1),$$

wo ξ prim zu den $\mathfrak{q}_i$ ist, wenn wir uns jetzt in (3) und (4) durchweg auf zu $\mathfrak{m}$ und den $\mathfrak{q}_i$, also zu $\overline{\mathfrak{m}}$ prime Zahlen beschränken. (Die ϱ_i sind nach Wahl der $\mathfrak{q}_i$ sicher prim zu den $\mathfrak{q}_i$). Ist nun etwa $x_1 \neq 0$, so ist $\overline{\alpha}$ kein ℓ–ter Potenzrest nach $\mathfrak{q}_1$, nach (5). Also müssen alle $x_i = 0$ sein, $\overline{\alpha}$ also als Zahl aus dem System (1) gleich 1.

132 IV

Wird also $\overline{\mathfrak{m}}$ als neuer Modul eingeführt — dabei dürfen die $\mathfrak{r}_i$, da prim zu den $\mathfrak{q}_i$, beibehalten werden — so ist in (2.) und (2a.) für n der Wert 0 zu setzen, dafür aber d durch $d + n$ zu ersetzen, da gerade n neue Primideale hinzugekommen sind. Alles andere in (2.) und (2a.) bleibt, sodaß der Rang der Gruppe der Idealklassen mod $\overline{\mathfrak{m}}$ nach dem entsprechenden Strahl o und somit die Anzahl ihrer Untergruppen vom Index ℓ unverändert durch (2.) und (2a.) gegeben wird. Da nun sicher jede Klassengruppe nach $\mathfrak{m}$ auch Klassengruppe nach $\overline{\mathfrak{m}}$ vom selben Index ist, sind die Klassengruppen vom Index ℓ für $\mathfrak{m}$ und $\overline{\mathfrak{m}}$ identisch.

Bezeichnen wir nun vorübergehend mit $\overline{\mathfrak{p}}$ eines der Primideale $\mathfrak{p}$, $\mathfrak{l}$, $\mathfrak{q}$ und seine absolute Klasse mit $\mathfrak{K}$. Der Zerlegung $G = G_0 \times \mathsf{D}$ (S. 97, (1)) entsprechend setzen wir

$$\mathfrak{K}^{-1} = \mathfrak{K}_0 \mathfrak{K}_{\mathsf{D}} = \mathfrak{K}_0 \mathfrak{K}_1^2,$$

da der Exponent von $\mathfrak{K}_{\mathsf{D}}$ prim zu ℓ ist. Bis auf absolute Hauptidealfaktoren lassen sich die Ideale aus $\mathfrak{K}_0$ auf die Form $\mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t}$ bringen. In $\mathfrak{K}_1$ liege das zu $\overline{\mathfrak{m}}$, ℓ und den $\mathfrak{r}_i$ prime Ideal $\mathfrak{j}$. Dann ist

$$\overline{\mathfrak{p}} \mathfrak{r}_1^{a_1} \dots \mathfrak{r}_t^{a_t} \mathfrak{j}^{\ell}$$

ein absolutes Hauptideal, welches nach Konstruktion prim ist zu jedem der übrigen Ideale $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ und auch zu den $\mathfrak{l}_1, \mathfrak{l}'$. Auf diese Art erhalten wir in der Form:

133 IV

(6) $$\pi_i = \mathfrak{p}_i \mathfrak{r}_1^{a_{i1}} \dots \mathfrak{r}_t^{a_{it}} \mathfrak{j}_i^{\ell} \qquad : \qquad d \text{ Zahlen } \pi_i,$$

$$\lambda_i = \mathfrak{l}_i \mathfrak{r}_1^{b_{i1}} \dots \mathfrak{r}_t^{b_{it}} \mathfrak{j}'^{\ell}_i \qquad : \qquad d' \text{ Zahlen } \lambda_i, \tag{7}$$

$$\kappa_i = \mathfrak{q}_i \mathfrak{r}_1^{c_{i1}} \dots \mathfrak{r}_t^{c_{it}} \mathfrak{j}''^{\ell}_i \qquad : \qquad n \text{ Zahlen } \kappa_i. \tag{8}$$

Nunmehr betrachten wir die $\ell^{r+1+t+d+d'+n}$ Zahlen

$$\varepsilon_1^{u_1} \dots \varepsilon_{r+1}^{u_{r+1}} \varrho_1^{v_1} \dots \varrho_t^{v_t} \pi_1^{x_1} \dots \pi_d^{x_d} \lambda_1^{y_1} \dots \lambda_{d'}^{y_{d'}} \kappa_1^{z_1} \dots \kappa_n^{z_n}, \tag{9}$$

wo alle Exponenten dem Intervall $0, 1, \dots, \ell - 1$ angehören.

Soll eine Zahl dieser Form (9) ℓ–te Potenz einer Zahl aus k sein, so müssen die Primideale $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ in ℓ–ten Potenzen in ihr enthalten sein. Da diese in (6), (7), (8) je einmal vorkommen, müssen alle $x_i, y_i, z_i = 0$ sein. Es bleibt also eine Zahl des Systems (1) übrig, die wie a. S. 99▸ gezeigt nur so ℓ–te Potenz einer Zahl sein kann, daß alle $u_i, v_i = 0$ sind.

Die Gruppe $\mathfrak{G}$ der Zahlen (9) mit unbeschränkten Exponenten hat also die eindeutige „Rangbasisdarstellung“:

$$\varepsilon_1^{u_1} \dots \varepsilon_{r+1}^{u_{r+1}} \varrho_1^{v_1} \dots \varrho_t^{v_t} \pi_1^{x_1} \dots \pi_d^{x_d} \lambda_1^{y_1} \dots \lambda_{d'}^{y_{d'}} \kappa_1^{z_1} \dots \kappa_n^{z_n} \xi^{\ell}, \tag{10}$$

wo ξ wieder eine Zahl dieser Gruppe $\mathfrak{G}$ ist, und alle Exponenten zwischen 0 und $\ell - 1$ liegen, d.h. ihr Rang ist

$$r + 1 + t + d + d' + n.$$

Aus dieser Gruppe $\mathfrak{G}$ werde jetzt eine Untergruppe $\mathfrak{H}$ ausgewählt durch folgende Bedingungen:

1.) *Jedes Ideal $\mathfrak{r}_i$ soll in den Zahlen aus $\mathfrak{H}$ genau zu einem durch ℓ teilbaren Exponenten aufgehen*:

Da die Ideale $\mathfrak{r}_i$ prim zu allen anderen vorkommenden sind, besagt diese Forderung nach (6)–(8), und da die $\mathfrak{r}_i$ in den ϱ_i schon nach Konstruktion zu einem durch ℓ teilbaren Exponenten aufgehen,

daß die Exponenten in (10) folgenden Kongruenzen genügen sollen

$$\sum_{i=1}^{d} a_{ij} x_i + \sum_{i=1}^{d'} b_{ij} y_i + \sum_{i=1}^{n} c_{ij} z_i \equiv 0 \mod \ell \quad \text{für} \quad j = 1, 2, \dots, t.$$

Das sind t *Bedingungskongruenzen.*

2.) *Die Zahlen der Untergruppe $\mathfrak{H}$ sollen ℓ–te Potenzreste nach der $\frac{e'\ell}{\ell-1}$–ten Potenz jedes $\mathfrak{l}'$ sein.*

Ist $m' = e'f'$ und $\eta_1, \ldots, \eta_{m'}$ ein Fundamentalsystem (ohne η_a) für $k(\mathfrak{l}')$, d.h. ein System unabhängiger Nichtreste nach dem Modul $\mathfrak{l}'^{\frac{e'\ell}{\ell-1}}$ und

$$\left.\begin{array}{rcccll} \varepsilon_i & \equiv & \eta_1^{e_{i1}} & \cdots & \eta_{m'}^{e_{im'}}\xi_{1i}^{\ell} & ; \quad (i = 1, \ldots, r+1) \\ \varrho_i & \equiv & \eta_1^{r_{i1}} & \cdots & \eta_{m'}^{r_{im'}}\xi_{2i}^{\ell} & ; \quad (i = 1, \ldots, t) \\ \pi_1 & \equiv & \eta_1^{p_{i1}} & \cdots & \eta_{m'}^{p_{im'}}\xi_{3i}^{\ell} & ; \quad (i = 1, \ldots, d) \\ \lambda_1 & \equiv & \eta_1^{\ell_{i1}} & \cdots & \eta_{m'}^{\ell_{im'}}\xi_{4i}^{\ell} & ; \quad (i = 1, \ldots, d') \\ \kappa_1 & \equiv & \eta_1^{q_{i1}} & \cdots & \eta_{m'}^{q_{im'}}\xi_{5i}^{\ell} & ; \quad (i = 1, \ldots, n) \end{array}\right\} \mod \mathfrak{l}'^{\frac{e'\ell}{\ell-1}},$$

so ist nach Bedeutung der unabhängigen Nichtreste unsere Forderung 2.) gleichwertig mit den Kongruenzen:

$$\sum_{i=1}^{r+1} e_{ij}u_i + \sum_{i=1}^{t} r_{ij}v_i + \sum_{i=1}^{d} p_{ij}x_i + \sum_{i=1}^{d'} \ell_{ij}y_i + \sum_{i=1}^{n} q_{ij}z_i \equiv 0 \mod \ell$$

$$\text{für} \quad j = 1, 2, \ldots, m'.$$

Das sind $m' = e'f'$ Bedingungskongruenzen. Im ganzen bedeutet also 2.)

$$\sum_{\mathfrak{l}'} \boldsymbol{e'f'} \textbf{ Bedingungskongruenzen.}$$

3.) *Die Zahlen der Untergruppe $\mathfrak{H}$ sollen ℓ–te Potenzreste nach der $\left(\frac{e_1\ell}{\ell-1} - g_1\right)$–ten Potenz jedes $\mathfrak{l}_1$ sein.*

Für die Potenz $\mathfrak{l}_1^{\frac{e_1\ell}{\ell-1}-g_1}$ ist nach Satz 28, S. 96 der Rang:*)

$$\begin{aligned} R\left(\mathfrak{l}_1^{\frac{e_1\ell}{\ell-1}-g_1}\right) &= \left(\frac{e_1\ell}{\ell-1} - g_1 - 1 - \left[\frac{e_1}{\ell-1} - \frac{g_1+1}{\ell}\right]\right) f_1 \\ &= \left(e_1 - (g_1+1) + \left\{\frac{g_1+1}{\ell}\right\}\right) f_1 \end{aligned}$$

*) $\{a\}$ bedeutet: kleinstes Ganze über a.

Soviel unabhängige Nichtreste existieren mod $\mathfrak{l}_1^{\frac{e_1\ell}{\ell-1}-g_1}$, sodaß wie unter 2.) hier resultieren:

$$\sum_{\mathfrak{l}_1}\left(e_1-(g_1+1)+\left\{\frac{g_1+1}{\ell}\right\}\right)f_1 \quad \text{Bedingungskongruenzen.}$$

4.) *Im Falle $\ell=2$ sollen die Zahlen der Untergruppe $\mathfrak{H}$ in den von der Vorzeichengruppe V nicht betroffenen reellen konjugierten zu k positiv sein.*

Da nach Annahme $r_1-\nu$ solche Körper vorhanden sind, bedeutet dies für die Exponenten u_i, v_i, x_i, y_i, z_i in (10) noch weitere $\boldsymbol{r_1-\nu}$ **Bedingungskongruenzen.**

Die Bedingungen 1.) – 4.) definieren ersichtlich eine Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$, und zwar eine solche, in der jede ℓ–te Potenz ξ^ℓ eines ξ aus $\mathfrak{G}$ vorkommt. Im ganzen sind zur Definition von $\mathfrak{H}$ benutzt:

$$t_0 = t+\sum_{\mathfrak{l}'}e'f'+\sum_{\mathfrak{l}_1}\left(e_1-(g_1+1)+\left\{\tfrac{g_1+1}{\ell}\right\}\right)f_1 \qquad \text{für } \ell\neq 2,$$

$$t_0 = t+\sum_{\mathfrak{l}'}e'f'+\sum_{\mathfrak{l}_1}\left(e_1-(g_1+1)+\left\{\tfrac{g_1+1}{\ell}\right\}\right)f_1+(r_1-\nu) \quad \text{für } \ell=2$$

Bedingungskongruenzen mod ℓ. Von den $r+1+t+d+d'+n$

Exponenten u_i, v_i, x_i, y_i, z_i in (10) bleiben also noch mindestens $r+1+d+d'+n+t-t_0$ frei, weil das System der Bedingungskongruenzen 1.) – 4.) eben höchstens den Rang t_0 hat.

Sei nun t' der Rang von $\mathfrak{H}$ und ihre Darstellung:

$$\mu=\mu_1^{w_1}\dots\mu_{t'}^{w_{t'}}\xi^\ell; \qquad (w_i=0,1,\dots,\ell-1,\ \xi \quad \text{aus} \quad \mathfrak{G}), \tag{11}$$

sodaß μ dann und nur dann ℓ–te Potenz einer Zahl aus $\mathfrak{G}$ (oder, was gleichbedeutend, aus k[*)]) ist, wenn alle $w_i=0$ sind, so ist

$$t'\geqq r+1+d+d'+n+t-t_0,$$

weil man auf Grund der t_0 Bedingungskongruenzen auch höchstens t_0 von den $r+1+d+d'+n+t$ Basiselementen von $\mathfrak{G}$ in (10) wegtransformieren

[*)] Ist ein μ aus $\mathfrak{G}$ ℓ–te Potenz einer Zahl aus $\mathfrak{G}$, so natürlich auch aus k. Ist aber μ aus $\mathfrak{G}$ ℓ–te Potenz einer Zahl aus k, so wurde gezeigt, daß in (10) alle Exponenten Null sein müssen, sodaß $\mu=\xi^\ell$ mit ξ aus $\mathfrak{G}$ stehen bleibt.

kann. Für $\ell \neq 2$ ist also nach (2.):

$$t' - \bar{t} \geqq 2(r+1) - \sum_{\mathfrak{l}} ef - \sum_{\mathfrak{l}'} e'f' - \\ - \sum_{\mathfrak{l}_1} \left(g_1 - \left[\frac{g_1}{\ell}\right] + e_1 - (g_1+1) + \left\{\frac{g_1+1}{\ell}\right\} \right) f_1,$$

während für $\ell = 2$ rechts noch $-r_1$ hinzukommt. Nun ist

$$\left\{\frac{g_1+1}{\ell}\right\} - \left[\frac{g_1}{\ell}\right] = \left\{\frac{g_1+1}{\ell}\right\} + \left\{-\frac{g_1}{\ell}\right\} = \left\{\frac{1}{\ell}\right\} = 1,$$

also die $\sum_{\mathfrak{l}_1}$ gleich $\sum_{\mathfrak{l}_1} e_1 f_1$ und bekanntlich

$$\sum_{\mathfrak{l}} ef + \sum_{\mathfrak{l}'} e'f' + \sum_{\mathfrak{l}_1} e_1 f_1 = m$$

wo m der Körpergrad von k ist, also für $\ell \neq 2$:

$$t' - \bar{t} \geqq 2(r+1) - m = 2(r_1 + r_2) - 2r_2 - r_1 = 0$$

da wegen ζ in k hier $r_1 = 0$ ist, während für $\ell = 2$ wird:

137 IV

$$t' - \bar{t} \geqq 2(r+1) - m - r_1 = 2(r_1 + r_2) - 2r_2 - r_1 - r_1 = 0.$$

Es gilt also stets

$$t' \geqq \bar{t}, \qquad \text{(also insbesondere } \geqq 0\text{)}. \tag{12}$$

Nach dem über die Gruppe $\mathfrak{H}$ in (11) gesagten sind die aus ihr entspringenden t' Kummerschen Körper

$$k\left(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_{t'}}\right)$$

von einander unabhängig. Nach Satz 38, S. 124 folgt also die Existenz von $\frac{\ell^{t'}-1}{\ell-1}$ Kummerschen Körpern $k\left(\sqrt[\ell]{\mu}\right)$, die sämtlich von einander verschieden sind, und deren sie definierende Elemente μ aus k in die Form

$$\mu = \mu_1^{w_1} \ldots \mu_{t'}^{w_{t'}}; \qquad (w_i = 0, 1, \ldots, \ell - 1)$$

gesetzt werden können. Wegen (12) erhält man also jedenfalls $\frac{\ell^{\bar{t}}-1}{\ell-1}$ verschiedene Körper dieser Art.

Wir untersuchen zunächst die Relativdiskriminante dieser Körper und haben dazu von der Zugehörigkeit jedes unserer μ zur Untergruppe $\mathfrak{H}$ Gebrauch zu machen, d.h. von den Tatsachen, die sich für μ aus den Bedingungen 1.) — 4.) für $\mathfrak{H}$ ergeben.

Wegen 1.) geht jeder Primfaktor der $\mathfrak{r}_i$ in μ genau zu einem durch ℓ teilbaren Exponenten auf, also weil die $\mathfrak{r}_i$ prim zu ℓ sind, nicht in der Relativdiskriminante.

Nach Konstruktion ist μ als Zahl aus $\mathfrak{G}$ (siehe (10)) durch kein von den $\mathfrak{p}, \mathfrak{l}, \mathfrak{q}$ verschiedenes Primideal teilbar, bis auf ev. ℓ–te Potenzfaktoren, die durch die $\mathfrak{j}_i^\ell, \mathfrak{j}'^\ell_i, \mathfrak{j}''^\ell_i$ in (6)–(8) hereinkommen. Da letztere prim zu ℓ angenommen

werden konnten (S. 132 unten), machen sie für die Relativdiskriminante nichts aus. Es kommen also an Faktoren der Relativdiskriminante nur noch die $\mathfrak{p}, \mathfrak{q}, \mathfrak{l}$ sowie die $\mathfrak{l}_1, \mathfrak{l}'$ in Frage.

Nach 2.) in μ ℓ–ter Potenzrest mod $\mathfrak{l}'^{\frac{e'\ell}{\ell-1}}$, also nach Satz 34, S. 116 die Relativdiskriminante prim zu den $\mathfrak{l}'$.[2]

Ist also $\mathfrak{f}^{\ell-1}$ die Relativdiskriminante, so gehen in $\mathfrak{f}$ höchstens die Primteiler $\mathfrak{p}, \mathfrak{q}, \mathfrak{l}, \mathfrak{l}_1$ auf, die sämtlich auch in $\overline{\mathfrak{m}}$ aufgehen, und $\mathfrak{f}$ hat dann die Form:

$$\mathfrak{f} = \prod{}' \mathfrak{p} \cdot \prod{}' \mathfrak{q} \cdot \prod{}' \mathfrak{l}^{v+1} \cdot \prod{}' \mathfrak{l}_1^{v_1+1},$$

wo die Akzente andeuten, daß die Produkte nicht notwendig über alle Primteiler der betr. Art zu erstrecken sind.

Ich zeige nun noch, daß $\overline{\mathfrak{m}}$ durch $\mathfrak{f}$ teilbar ist, daß also die ev. in $\mathfrak{f}$ vorkommenden Potenzen der $\mathfrak{j}, \mathfrak{q}, \mathfrak{l}, \mathfrak{l}_1$ die in $\overline{\mathfrak{m}}$ vorkommenden nicht übersteigen. Für die $\mathfrak{p}, \mathfrak{q}$ ist dies klar, da sie je nur einmal vorkommen. Für die $\mathfrak{l}$ ist nach §1, h.

$$v \leqq \frac{e\ell}{\ell-1},$$

während nach Voraussetzung mindestens $\mathfrak{l}^{\frac{e\ell}{\ell-1}+1}$ in $\mathfrak{m}$, also $\overline{\mathfrak{m}}$ aufgeht, also jedenfalls keine kleinere Potenz als ev. in $\mathfrak{f}$. Für die $\mathfrak{l}_1$ ist μ ℓ–ter Potenzrest

[2] undeutlich

mod $\mathfrak{l}_1^{\frac{e_1\ell}{\ell-1}-g_1}$, also ($\mu$ ist prim zu den $\mathfrak{l}_1$) das g von Satz 35, S. 119 sicher $\geqq \frac{e_1\ell}{\ell-1} - g_1$, d.h. die in der Relativdiskriminante aufgehende Potenz von $\mathfrak{l}_1$ sicher niedriger oder gleich

$$\mathfrak{l}_1^{(g_1+1)(\ell-1)}, \qquad \text{d.h. in } \mathfrak{f} \text{ geht höchstens } \mathfrak{l}_1^{g_1+1} \text{ auf,}$$

139 IV

und in $\overline{\mathfrak{m}}$ nach Voraussetzung genau $\mathfrak{l}_1^{g_1+1}$. Es ist somit $\overline{\mathfrak{m}}$ durch $\mathfrak{f}$ teilbar.

Für $\ell \neq 2$ folgt nun aus Satz 21, S. 59, daß alle unsere Körper $k\left(\sqrt[\ell]{\mu}\right)$ Klassenkörper sind für gewisse Klassengruppen H in k vom Index ℓ, die jedenfalls nach dem Modul $\mathfrak{f}$, der zu dem betreffenden μ gehört, ohne Vorzeichenbedingungen erklärbar sind. Da aber, wie eben gezeigt, alle diese $\mathfrak{f}$ Teiler von $\overline{\mathfrak{m}}$ sind, können jene Klassengruppen auch nach dem Modul $\overline{\mathfrak{m}}$ erklärt werden.

Für $\ell = 2$ folgt aus Satz 21a, S. 62, daß alle unsere Körper $k\left(\sqrt[\ell]{\mu}\right)$ Klassenkörper sind für gewisse Klassengruppen H in k vom Index 2, die jedenfalls nach dem Modul $\mathfrak{f}$, der zu dem betr. μ gehört, erklärbar sind und die außerdem zu ihrer Definition noch eine Vorzeichenbedingung V' der Form:

„Strahlzahl (Hauptklasse) positiv in denjenigen reellen konjugierten, in denen μ negativ ist,“

erfordern. Nach 4.) ist aber für $\ell = 2$ jedes unserer μ in den □□□ von der Vorzeichengruppe V, die zur Definition unseres Strahles o benutzt wurde, nicht betroffenen Körpern positiv, sodaß die zur Definition der H erforderlichen Vorzeichenbedingungen V' sich höchstens auf gewisse der zu Beginn ausgewählten ν reellen Körper $k_1, \ldots, k_\nu$ beziehen können. V ist also Untergruppe der V', sodaß eine Klasseneinteilung, die V' für die Hauptklasse fordert, sicher durch eine geeignete Gruppenbildung (Faktorgruppe V'/V) aus den auf Grund der weitergehenden Forderung V definierten Klassen gewonnen werden kann. Da auch hier zur Definition sämtlicher Klassengruppen H das Vielfache $\overline{\mathfrak{m}}$ von allen $\mathfrak{f}$ zugrundegelegt

140 IV

werden darf, ergibt sich:

Die $\frac{\ell^{t'}-1}{\ell-1}$ Klassengruppen H, nach denen unsere konstruierten $\frac{\ell^{t'}-1}{\ell-1}$ Kummerschen Körper Klassenkörper sind, können sämtlich nach dem Strahl:

$$\begin{aligned} &\equiv 1 \bmod \overline{\mathfrak{m}}, && \text{für} \quad \ell \neq 2, \\ \equiv 1 \bmod \overline{\mathfrak{m}} \quad &\text{mit } V, && \text{für} \quad \ell = 2 \end{aligned}$$

erklärt werden, und sind nach Definition der zugeordneten Klassengruppe alle verschieden.[3]

Die Anzahl der Klassengruppen $\mathfrak{H}$ vom Index ℓ nach dem Modul $\overline{\mathfrak{m}}$*) war oben (S. 130▸ u. 132▸) zu $\frac{\ell^{\bar{t}}-1}{\ell-1}$ erkannt. Wegen (12) muß also auf jede solche Klassengruppe H sicher ein Klassenkörper $k\left(\sqrt[\ell]{\mu}\right)$ entfallen. □□□ Da aber umgekehrt zu einer Klassengruppe auch nur ein Klassenkörper gehört, müssen die $\frac{\ell^{t'}-1}{\ell-1}$ Kummerschen Körper sich den $\frac{\ell^{\bar{t}}-1}{\ell-1}$ Klassengruppen H vom Index ℓ nach $\overline{\mathfrak{m}}$ eineindeutig zuordnen lassen, sodaß beiläufig noch

$$t' = \bar{t}$$

folgt.

Da, wie oben gezeigt, die Klassengruppen vom Index [...] nach $\mathfrak{m}$ und $\overline{\mathfrak{m}}$ identisch sind, ist so auch jeder Klassengruppe vom Index ℓ nach $\mathfrak{m}$*) eindeutig ein Klassenkörper zugeordnet.

(Daß man tatsächlich *jede* Klassengruppe vom Index ℓ nach $\mathfrak{m}$ in der angegebenen Weise erhält, sieht man

141 IV

sofort. Für $\ell \neq 2$ wurde der Strahl $\equiv 1 \bmod \mathfrak{m}$ ohne Vorzeichenbedingung zugrundegelegt. Aus den nach ihm definierten Klassen erhält man a fortiori zwar noch nicht *alle* Klassengruppen vom Index ℓ, da eventuell noch solche auf Grund einer engeren Klasseneinteilung mod $\mathfrak{m}$ *mit Vorzeichenbedingungen* entstehen könnten. Sei nun H eine solche Klassengruppe vom Index ℓ, deren Elemente Klassen *mit* Vorzeichenbedingungen sind, und α eine beliebige Zahl $\equiv 1 \bmod \mathfrak{m}$, so gehört einerseits α^ℓ zu H, da der Index ℓ ist, andererseits α^2 zu H, da es total positiv und $\equiv 1 \bmod \mathfrak{m}$ ist, also zur engsten Hauptklasse gehört, also auch α selbst als $\alpha^\ell : (\alpha^2)^{\frac{\ell-1}{2}}$. Es gehört also der ganze Strahl $\equiv 1 \bmod \mathfrak{m}$ *ohne Vorzeichenbedingungen* zu H, d.h. es gehören immer schon ganze Klassen nach diesem weiteren Strahl zu H. Man erhält

[3] undeutlich

*) Für $\ell \neq 2$ ohne, für $\ell = 2$ mit Vorzeichenbedingung V.

also für $\ell \neq 2$ tatsächlich schon alle Klassengruppen vom Index ℓ aus den Klassen nach dem obigen Strahl o.

Für $\ell = 2$ wurde in die Definition von o oben noch die Vorzeichenbedingung V aufgenommen. Selbstverständlich erhält man so *jede* Klassengruppe mod $\mathfrak{m}$ vom Index 2^c, da man ja speziell bis zur engstmöglichen Klasseneinteilung $V = 1$ aufsteigen kann).

Wir weisen letztens noch nach, daß die Hilfsprimideale $\mathfrak{q}_i$ nicht in den Relativdiskriminanten der $k\left(\sqrt[\ell]{\mu}\right)$ aufgehen. In der Tat, gingen sie z.T. in irgendeiner dieser Relativdiskriminanten auf, so könnten wir, da uns bei (5) unendlich viele Primidealsysteme $\mathfrak{q}_i$ zur Verfügung stehen, ein vollständig neues System von $\mathfrak{q}_i'$ wählen. In den damit konstruierten Klassenkörpern gehen aber die alten $\mathfrak{q}_i$, da sie von den $\mathfrak{p}, \mathfrak{l}, \mathfrak{l}_1$ und $\mathfrak{q}_i'$ verschieden sind, nach

142 IV

unserem obigen Beweis sicher nicht in den Relativdiskriminanten auf. Der Eindeutigkeit halber sind aber die neuen Klassenkörper in ihrer Gesamtheit mit den früheren identisch. Also können die $\mathfrak{q}_i$ nicht in den Relativdiskriminanten der $k\left(\sqrt[\ell]{\mu}\right)$ aufgehen. Es ist mithin schon $\mathfrak{m}$ teilbar durch jedes $\mathfrak{f}$.

Damit ist bewiesen:

Satz 42. Enthält k die ℓ–te Einheitswurzel ζ und ist H eine beliebige nach dem Modul $\mathfrak{m}$ erklärbare Klassengruppe in k vom Index ℓ, so existiert ein Kummerscher Körper $K = k\left(\sqrt[\ell]{\mu}\right)$, der Klassenkörper zu H ist. Ist $\mathfrak{f}^{\ell-1}$ seine Relativdiskriminante, so ist überdies $\mathfrak{f}$ ein Teiler von $\mathfrak{m}$. (Ist also speziell $\mathfrak{m} = 1$, so ist die Relativdiskriminante von K gleich 1, d.h. K *unverzweigt*).

Für $\ell = 2$ folgt noch etwas genauer, da hier nach 4.) μ in den $r_1 - \nu$ von V nicht betroffenen reellen konjugierten positiv ist, also die entsprechenden Paare relativ–konjugierter $k\left(\sqrt[\ell]{\mu}\right)$ reell sind:

Satz 42a. Wenn von den r_1 reellen konjugierten zu k irgendwelche ν ausgewählt werden, und der Strahl o aus den in jenen ν Körpern positiven $\equiv 1 \bmod \mathfrak{m}$ besteht, so sind von den zu $k\left(\sqrt[\ell]{\mu}\right)$ konjugierten Körpern mindestens $2(r_1 - \nu)$ reell, wenn $k\left(\sqrt[\ell]{\mu}\right)$ Klassenkörper für eine Klassengruppe vom Index 2 nach o ist. Ist also speziell $\nu = 0$, d.h. o der volle Strahl $\equiv 1 \bmod \mathfrak{m}$, so sind für jeden Klassenkörper zu einer Klassengruppe vom Index 2 nach o mindestens $2r_1$, also genau $2r_1$ konjugierte reell.

143 IV

B. Existenz bei Primzahlgrad ℓ ohne ℓ–te E.W.

B. Existenz des Klassenkörpers vom Primzahlrelativgrad ℓ, wenn der Grundkörper k die ℓ–te Einheitswurzel ζ nicht enthält.

Im Falle eines $\ell \neq 2$ müssen wir uns noch von der Voraussetzung befreien, daß der Körper k die ℓ–te Einheitswurzel ζ enthält. Das Ziel dieses Abschnittes ist der Nachweis des Satzes:

Satz 43. Ist k ein beliebiger Körper, H eine Klassengruppe in k vom Primzahlindex ℓ nach irgendeinem Modul $\mathfrak{m}$, so existiert ein Klassenkörper zu H, der relativ–zyklisch vom Grade ℓ in Bezug auf k ist. Ist $\mathfrak{f}^{\ell-1}$ seine Relativdiskriminante, so ist $\mathfrak{f}$ ein Teiler von $\mathfrak{m}$.

Wir beweisen zunächst einen Hilfssatz:

Hilfssatz. Ist K relativ–Galoissch aber nicht relativ zyklisch zu k, so gibt es in k kein Primideal, das in K unzerlegt bleibt.

Beweis. Bliebe $\mathfrak{p}$ unzerlegt in K, so ginge es zunächst nicht in der Relativdiskriminante von K auf. Seine Trägheitsgruppe wäre also die identische. Seine Zerlegungsgruppe wäre ferner die ganze Gruppe, da $\mathfrak{p} = \mathfrak{P}$ gegenüber allen Substitutionen invariant wäre. Da allgemein $\frac{\mathfrak{G}_Z}{\mathfrak{G}_T}$ zyklisch vom Grade $\mathfrak{f}$ ist ($\mathfrak{f}$ Relativgrad von $\mathfrak{P}$), wäre demnach hier $\mathfrak{G}_Z$ selbst zyklisch vom Grade $\mathfrak{f}$, also die ganze Gruppe zyklisch, entgegen der Voraussetzung.

Satz 43 wird bewiesen sein, wenn folgendes gezeigt ist:

144 IV

Satz 44. Ist k_1 ein Oberkörper zu k, der relativ–zyklisch vom Primzahlgrad $p \neq \ell$ in Bezug auf k ist und in dessen Relativdiskriminante nur Primteiler $\mathfrak{l}$ von ℓ aus k aufgehen können, und gilt Satz 43 für k_1, so gilt er auch für k.

In der Tat, sei $k(\zeta)$ der durch Adjunktion von ζ zu k entstehende Körper, der also zyklisch zu k von einem Grade n ist, wo n ein Teiler von $\ell - 1$ ist. In der Relativdiskriminante der Zahl $1 - \zeta$ gehen dann nur Primteiler $\mathfrak{l}$ aus k von ℓ auf, umso mehr in der Relativdiskriminante von $k(\zeta)$. Nun läßt sich $k(\zeta)$ von k aus durch ineinandergeschachtelte zyklische Körper erreichen:

$$k = k_0\{k_1\{k_2 \cdots \{k_{\nu-1}\{k_\nu = k(\zeta),$$

deren sukzessive Relativgrade die in n aufgehenden Primzahlen p, also sämtlich Teiler von $\ell - 1$, d.h. $\neq \ell$ sind. In den sukzessiven Relativdiskriminanten

gehen ebenfalls nur Primteiler von ℓ aus den k_i auf, da die Gesamtrelativdifferente das Produkt der sukzessiven Relativdifferenten ist. Die Richtigkeit von Satz 44 vorausgesetzt, folgt also die Richtigkeit von Satz 43 sukzessive für $k_{\nu-1}, k_{\nu-2}, \ldots, k_1, k_0 = k$. Wir beweisen also jetzt den Satz 44.

Es sei $\mathfrak{f}_1^{p-1}$ die Relativdiskriminante von k_1, die also nur Primteiler von ℓ aus k enthält. Da $\ell \neq p$ ist, der Relativgrad aber p, geht jeder dieser Primfaktoren nur zur ersten Potenz in $\mathfrak{f}_1$ auf, sodaß

$$\mathfrak{f}_1 = \prod \mathfrak{l}$$

erstreckt über gewisse Primteiler $\mathfrak{l}$ von ℓ aus k ist.

145 IV

H sei eine vorgelegte Klassengruppe vom Index ℓ nach dem Modul $\mathfrak{m}$ in k. Sollten nicht alle Primteiler von $\mathfrak{f}_1$ in $\mathfrak{m}$ vorkommen, so fügen wir die fehlenden genau in der ersten Potenz hinzu. Der entstehende Modul heiße $\overline{\mathfrak{m}}$ und ist jetzt durch $\mathfrak{f}_1$ und natürlich durch $\mathfrak{m}$ teilbar. $\mathfrak{H}$ ist auch nach dem Modul $\overline{\mathfrak{m}}$ erklärbar, also auch Klassengruppe vom Index ℓ mod $\overline{\mathfrak{m}}$.

Wir definieren jetzt die Idealklassen in k und k_1 beidesmal nach dem Strahl $\equiv 1 \bmod \overline{\mathfrak{m}}$ (für $p = 2$ total positiv). Dann folgt, wenn n die Relativnorm von k_1 nach k bezeichnet, aus

$$\begin{aligned} \mathsf{A} &\equiv 1 \bmod \overline{\mathfrak{m}} \quad \text{in} \quad k_1 \\ n(\mathsf{A}) &\equiv 1 \bmod \overline{\mathfrak{m}} \quad \text{in} \quad k. \end{aligned}$$

Denn wegen $\sigma\overline{\mathfrak{m}} = \overline{\mathfrak{m}}$, wo σ die erzeugende Substitution von k_1 und k ist ($\sigma^p = 1$), folgt aus $\mathsf{A} \equiv 1 \bmod \overline{\mathfrak{m}}$ auch $\sigma\mathsf{A} \equiv 1 \bmod \overline{\mathfrak{m}}, \ldots$. Für $p = 2$ ist ferner, wenn für einen reellen konjugierten $k^{(i)}$ auch die zugehörige Serie der $2 \quad k_1^{(i)}$ reell ist, und A positiv in beiden $k_1^{(i)}$ auch $n(\mathsf{A}) = \mathsf{A}\sigma\mathsf{A}$ positiv in $k^{(i)}$, und wenn für reelles $k^{(i)}$ die beiden $k_1^{(i)}$ imaginär sind, natürlich $n(\mathsf{A}) = \mathsf{A}\sigma\mathsf{A}$ positiv in $k^{(i)}$. Also für $p = 2$:

Aus	A	total	positiv	in	k_1
folgt	$n(\mathsf{A})$	$\shortparallel$	$\shortparallel$	$\shortparallel$	k.

Es ist somit für die beiden definierten Strahlen die Relativnorm einer Strahlzahl aus k_1 Strahlzahl aus k und daher bei der definierten Klasseneinteilung in k_1 und k die Relativnormen einer ganzen Klasse von k_1 in einer

bestimmten Klasse von k enthalten, sodaß wieder

146 IV

wie in §1, S. 54 von Relativnormen der Klassen aus k_1 geredet werden kann.

Seien G und G_1 die Gruppen der Idealklassen in k und k_1, D die Gruppe der Klassen aus k mit zu ℓ primem Exponenten, G_0 die Gruppe der Klassen, deren Exponenten Potenzen von ℓ sind, also

$$G = G_0 \times \mathsf{D}$$

die Zerlegung unserer Gesamtklassengruppe von k in ein direktes Produkt. Die Klassengruppe H aus k vom Index ℓ muß dann offenbar die ganze Gruppe D enthalten. Denn ist C irgendeine Klasse aus D also $C^{\overline{u}}$ für zu ℓ primes $\overline{u}$ die Hauptklasse (stets nach unserm definierten Strahl), so ist natürlich C^u in H enthalten, andererseits aber auch C^ℓ, da H den Index ℓ hat, und somit auch durch geeignete Kombination $C = (C^u)^{u_1} \cdot (C^\ell)^{\ell_1}$ ein Element von H. Dementsprechend kann

$$\mathsf{H} = \mathsf{H}_0 \times \mathsf{D}$$

gesetzt werden, wo H_0 für H die entsprechende Bedeutung hat, wie G_0 für G.[4]

□□□

147 IV

Aus dieser Zerlegung folgt, daß die Gruppe H_0 Untergruppe von G_0 ist, nämlich genau der Gruppendurchschnitt

$$\mathsf{H}_0 = (\mathsf{H}, G_0).$$

Der Index $(G_0 : \mathsf{H}_0)$ ist gleich ℓ. Denn ist C ein Element aus G_0, aber nicht aus H_0, was sicher existiert, da sonst $\mathsf{H} = G$ folgte, so gehört C^ℓ einerseits zu H, andererseits zu G_0, also auch zum Durchschnitt H_0.

Ich zeige nun gruppentheoretisch, daß man eine Basis $C_1, C_2, \ldots, C_n$ für G_0 so wählen kann, daß $C_1^\ell, C_2, \ldots, C_n$ eine Basis für H_0 ist, wobei diese letztere Basis entweder nur $n-1$ Elemente enthält, wenn $C_1^\ell = 1$ ist, oder wieder n Elemente, wenn $C_1^\ell \neq 1$ ist.

[4] Nebensatz undeutlich

Dazu gehe ich aus von einer Basis $C'_1, \ldots, C'_{n'}$ für H_0. Dann kann man zunächst ein nicht zu H_0 gehöriges Element C_1 aus G_0 bestimmen, für das in der sicher bestehenden Darstellung

$$C_1^{\ell} = C_1'^{a_1} \ldots C_{n'}'^{a_{n'}}$$

des zu H_0 gehörigen C_1^{ℓ} durch die Basis von H_0 alle Exponenten a_i der Reihe $0, 1, \ldots, \ell - 1$ angehören. Denn ist $a_i = \overline{a}_i + \ell b_i$ so hat $C_1 C'^{-b_1}_1 \ldots C'^{-b_{n'}}_{n'}$ die verlangte Eigenschaft und gehört zu G_0, da C_1 und die C'_i es tun, aber nicht zu H_0, da die C'_i zu H_0 gehören, nicht aber C_1. Es sei also C_1 ein solches Element.

148 IV

Sind dann erstens alle $a_i = 0$, also $C_1^{\ell} = 1$, so ist jedes Element C aus G_0 eindeutig in der Form darstellbar

$$C = C_1^{\overline{c}_1} C'^{c_1}_1 \ldots C'^{c_{n'}}_{n'},$$

wo $0 \leqq \overline{c}_1 \leqq \ell - 1$ und die Exponenten c_i den durch C'_i bestimmten Intervallen angehören. Da C_1 zum Exponenten `[...]` gehört, ist dies eine Basisdarstellung der Gruppe G_0; dann ist in diesem Falle die Behauptung bewiesen $(n' = n - 1)$.

Sind zweitens nicht alle $a_i = 0$, so sei C'_1 das Basiselement mit höchstem Exponenten ℓ^{ν} unter allen C'_i mit nicht verschwindendem a_i und $a_1, a_2, \ldots, a_r \neq 0$, $a_{r+1}, a_{r+2}, \ldots, a_{n'} = 0$. Sei $a_1 a'_1 \equiv 1 \bmod \ell$, dann darf $C_1^{a'_1}$ an Stelle von C_1 genommen, also von vorneherein $a_1 = 1$ vorausgesetzt werden, d.h.

$$C_1^{\ell} = C'_1 C'^{a_2}_2 \ldots C'^{a_r}_r = C.$$

C hat den Exponenten ℓ^{ν}, da dies der höchste Exponent unter denen der vorkommenden C'_i ist. Daher kann C an Stelle von C'_1 als Basiselement treten. Dann ist offenbar

$$C_1, C'_2, \ldots, C'_n$$

eine Basis für G_0, während die Basis für H_0 nunmehr in

$$C_1^{\ell}, C'_2, \ldots, C'_n$$

transformiert ist. Denn es läßt sich zunächst jedes Element aus G_0 eindeutig in der Form schreiben:

$$C = C_1^{\overline{c}_1} \cdot C_{\mathsf{H}_0} = C_1^{\overline{c}_1} C_1^{c_1 \ell} C'^{c_2}_2 \ldots C'^{c_{n'}}_{n'}$$

wo $0 \leqq \bar{c}_1 \leqq \ell - 1$ und die Exponenten $c_1, \ldots, c_{n'}$ den durch

149 IV

$C_1^\ell, C_2', \ldots, C_{n'}'$ bestimmten Intervallen angehören, also auch eindeutig in der Form

$$C = C_1^{\bar{\bar{c}}_1} C_2'^{c_2} \ldots C_{n'}^{c_{n'}},$$

wo jetzt $\bar{\bar{c}}_1$ dem zu C_1 gehörigen Intervall $(0, 1, \ldots, \ell^{\nu+1} - 1$ in obiger Bezeichnung) angehört. Damit ist unsere Behauptung auch in diesem zweiten Falle bewiesen ($n' = n$).

Sei also jetzt

$$G_0 = [C_1, C_2, \ldots, C_n],$$
$$\mathsf{H}_0 = [C_1^\ell, C_2, \ldots, C_n],$$

wo die [ ] nach dem Gesagten keiner Erläuterung mehr bedürfen, so kann in derselben Symbolik

$$G = [C_1, C_2, \ldots, C_n; \mathsf{D}]$$
$$\mathsf{H} = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}]$$

geschrieben werden.

Es sei nun D_0 diejenige Untergruppe von D, welche durch die Relativnormen der Klassen von k_1 aus D herausgeschnitten wird, ferner D_1 die Gruppe in k_1, deren Relativnormen D_0 erzeugen, und $C^{(1)}$ eine Klasse aus k_1. Dann besteht eine Darstellung

$$n(C^{(1)}) = C_1^{a_1} \ldots C_n^{a_n} \ [\mathsf{D}]$$

wo $[\mathsf{D}]$ eine Klasse aus D bedeutet. Ich zeige, daß $[\mathsf{D}]$ sogar in D_0 liegen muß, d.h. Relativnorm einer Klasse von k_1 ist.

Da nämlich $p \neq \ell$ ist, können $b_1, \ldots, b_n$ so bestimmt

150 IV

werden, daß

$$C_i^{pb_i} = C_i^{a_i}$$

ist. Faßt man dann die Klassen C_i, deren Elemente sicher in k_1 ebenfalls äquivalent sind, als Klassen in `[...]` auf, wobei natürlich ev. mehrere C_i die

gleiche Klasse in k_1 liefern*), so ist

$$U = C^{(1)} C_1^{-b_1} \dots C_n^{-b_n}$$

ebenfalls eine bestimmte Klasse in k_1. Da in C_i, als Klasse von k, gedacht, die Ideale von C_i aus k liegen, ist $n(C_i)$ die Klasse C_i^p aus k, also

$$n(U) = n(C^{(1)}) C_1^{-b_1 p} \dots C_n^{-b_n p} = [\mathsf{D}],$$

sodaß tatsächlich $[\mathsf{D}]$ zu D_0 gehört.

Zugleich erkennen wir, da $n(U)$ zu D_0 gehört, also U zu D_1, daß sich für jede Klasse $C^{(1)}$ von k_1 Exponenten $b_1, \dots, b_n$ so bestimmen lassen, daß

$$C^{(1)} = C_1^{b_1} \dots C_n^{b_n} [\mathsf{D}_1]$$

ist, wo $[\mathsf{D}_1]$ eine Klasse aus D_1 bedeutet.

Diese Darstellung ist überdies eindeutig (speziell also die durch die C_i in k_1 gelieferten Klassen, die ebenso bezeichnet wurden, in k_1 verschieden), wenn die Exponenten b_i der C_i ebenso beschränkt werden, wie es der Basisdarstellung durch die C_i in k entspricht. Bestände nämlich eine Relation

$$1 = C_1^{b_1} \dots C_n^{b_n} [\mathsf{D}_1]$$

in k_1, so folgte durch Übergang zur Relativnorm in k:

$$1 = C_1^{b_1 p} \dots C_n^{b_n p} [\mathsf{D}_0],$$

also wegen $p \neq \ell$, und da die C_i zu Exponenten ℓ^{ν_i} gehören, wegen der Unabhängigkeit der Basisklassen C_i in k unter sich und von D:

$$b_i \equiv 0 \mod \ell^{\nu_i}, \quad \text{d.h.} \quad C_i^{b_i} = 1,$$

also auch $[\mathsf{D}_0] = 1$, $[\mathsf{D}_1] = 1$.

Die Klassen C_i in k_1 haben also genau dieselben Exponenten, wie in k, und sind auch in k_1 unter sich und von D_1 unabhängig. Da sie umgekehrt

*) Man versteht also unter den Klassen C_i in k_1 einfach die durch die C_i aus [...] erzeugten Klassen in k_1. Besser wäre es, eine neue Bezeichnung zu nehmen

mit D_1 jede Klasse $C^{(1)}$ aus k_1 darstellen, folgt also in obiger Symbolik für die Klassengruppe G_1 von k_1 folgende eindeutige Basisdarstellung:

$$G_1 = [C_1, \ldots, C_n; \mathsf{D}_1].$$

Wir definieren dann durch die Festsetzung

$$\mathsf{H}_1 = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_1]$$

eine Klassengruppe H_1 in k_1 vom Index ℓ.

Da nach Voraussetzung der Satz 43 richtig ist für k_1, gibt es zu H_1 über k_1 einen Klassenkörper K_1, der relativ zyklisch vom Primzahlgrad ℓ ist. Ist $\mathfrak{F}_1^{\ell-1}$ seine Relativdiskriminante, so ist $\mathfrak{F}_1$ ein Teiler von $\overline{\mathfrak{m}}$, denn H_1 ist ja auf Grund der Klasseneinteilung mod $\overline{\mathfrak{m}}$ in k_1 erklärt.

Druch die Substitution σ von k_1 geht, wie aus der Definition von D_1 ersichtlich, jede Klasse von D_1 in eine solche von D_1 über. (Überhaupt geht natürlich jede Klasse durch σ in eine bestimmte Klasse über, weil wegen $\sigma\overline{\mathfrak{m}} = \overline{\mathfrak{m}}\,\sigma\mathsf{A}$ mit A den ganzen Strahl $\equiv 1 \bmod \overline{\mathfrak{m}}$ (tot. pos. f. $p = 2$) durchläuft).

152 IV

Da die C_i als Klassen in k_1 gedacht invariant gegen σ sind, ist auch die Klassengruppe H_1 invariant gegen σ. Geht man nun von K_1 zu einem in Bezug auf k relativ konjugierten Körper über, so entspricht dem eine bestimmte Substitution σ^c von k_1. Da H_1 dagegen invariant bleibt, bleibt auch der konjugierte Körper von[5] Klassenkörper für H_1, ist also der Eindeutigkeit wegen mit K_1 identisch, d.h. K_1 *ist Galoissch in Bezug auf* k.

Die Relativnormen der Ideale von K_1 nach k_1 fallen nach Definition des Klassenkörpers sämtlich in H_1. Die Relativnormen der Ideale von H_1 in Bezug auf `[...]` fallen ihrerseits in die Gruppe

$$\overline{\mathsf{H}}_0 = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0]$$

von k, da ja $n(C_i) = C_i^p$; $n[\mathsf{D}_1] = [\mathsf{D}_0]$ ist. Dieses[6] gilt somit auch von den Relativnormen von K_1 nach k.

Nun ist $\overline{\mathfrak{m}}$ durch $\mathfrak{f}_1$ teilbar und k_1 zyklisch vom Primzahlgrad p in Bezug auf k. Nach Satz 21, 21a, S. 59▸, 62▸ ist also k_1 Klassenkörper über k für

[5] undeutlich
[6] undeutlich

eine Gruppe $\overline{\mathbf{G}}_0$ vom Index p in k, die sicherlich nach unserem zugrundegelegten Strahl mod $\overline{\mathfrak{m}}$ erklärt werden kann. Nach S. 149 unten sind nun die Relativnormen von k_1 nach k in der Klassengruppe

$$[C_1, \ldots, C_n; \mathsf{D}_0]$$

enthalten. Umgekehrt ist auch jede Klasse dieser Gruppe

153 IV

Relativnorm einer Klasse aus k_1, da ja wegen $p \neq \ell$ Zahlen a_i so bestimmt werden können, daß

$$n(C_i^{a_i}) = C_i^{pa_i} = C_i$$

wird, und jede Klasse von D_0 nach Definition von D_0 Relativnorm ist. Die genannte Gruppe besteht also aus der Gesamtheit Klassen von k, die Relativnormen von Klassen aus k_1 sind, d.h. aus der Gesamtheit aller Klassen von k, die Relativnormen von Idealen aus k_1 enthalten, und ist somit die k_1 zugeordnete Klassengruppe, also mit obigem $\overline{G}_0$ identisch:

$$\overline{G}_0 = [C_1, C_2, \ldots, C_n; \mathsf{D}_0].$$

Also hat $\overline{G}_0$ den Index p in Bezug auf G, (d.h. D_0 den Index p in Bezug auf D).

Die Gruppe

$$\overline{\mathsf{H}}_0 = [C_1^{\ell}, C_2, \ldots, C_n; \mathsf{D}_0]$$

hat also den Index $p\ell$ in Bezug auf G. Da $\overline{\mathsf{H}}_0$ die Relativnormen von K_1 nach k enthält, muß die dem Galoisschen Körper K_1 über k zugeordnete Klassengruppe ein Teiler von $\overline{\mathsf{H}}_0$ sein, also einen Index $\geqq p\ell$ haben. Andererseits muß aber der Index der K_1 zugeordneten Klassengruppe $\leqq p\ell$ sein, weil $p\ell$ der Relativgrad von K_1 nach k ist. Es ist also $\overline{\mathsf{H}}_0$ selbst diese Klassengruppe und K_1 Klassenkörper über k für $\overline{\mathsf{H}}_0$.

154 IV

Nach A.Z. II, Satz 8, S. 143 gibt es nun in k unendlich viele Primideale $\mathfrak{p}$ (vom ersten Grade), welche in k_1 nicht in lauter verschiedene Primideale ersten Grades zerfallen (also unzerlegt bleiben!), und auch nicht in der Klassengruppe H vom Index $\ell > 2$ enthalten sind. Würde nun ein solches, in k_1 unzerlegtes Primideal $\mathfrak{p}$ in K_1 zerfallen, so wäre $\mathfrak{p}$ Relativnorm eines jeden dieser Primteiler ersten Grades aus K_1, genommen von K_1 nach k_1. Dann

läge also □□□ $n(\mathfrak{p}) = \mathfrak{p}^p$ in $\overline{\mathsf{H}}_0$ als Relativnorm von K_1 nach k. Ist dann C die Klasse von $\mathfrak{p}$, so wäre

$$C^p = C_1^{\ell a_1} C_2^{a_2} \dots C_n^{a_n} [\mathsf{D}_0],$$

und wenn $pp_1 = 1 + \ell\ell_1$:

$$CC^{\ell\ell_1} = C_1^{\ell p_1 a_1} C_2^{p_1 a_2} \dots C_n^{p_1 a_n} [\mathsf{D}_0]^{p_1}.$$

Ist also C selbst dargestellt durch:

$$C = C_1^{b_1} \dots C_n^{b_n} [\mathsf{D}],$$

so wäre

$$C = C_1^{\ell(p_1 a_1 - \ell_1 b_1)} C_2^{p_1 a_2 - \ell\ell_1 b_2} \dots C_n^{p_1 a_n - \ell\ell_1 b_n} [\mathsf{D}\,[\dots]]$$

also C und somit $\mathfrak{p}$ in H enthalten, entgegen der erlaubten Annahme, daß $\mathfrak{p}$ nicht in H enthalten sei.

Es bleibt somit $\mathfrak{p}$ in K_1 unzerlegt, sodaß nach dem vorangestellten Hilfssatz (S. 143▸) K_1 *relativ–zyklisch in Bezug auf* k ist, (vom Relativgrade $p\ell$).

155 IV

In K_1 ist somit ein relativ–zyklischer Unterkörper K vom Grade ℓ in Bezug auf k enthalten, und wir zeigen jetzt, daß dieser Körper K der gesuchte Klassenkörper für H ist.

Dies wird bewiesen sein, wenn wir die Teilbarkeit von $\overline{\mathfrak{m}}$ durch $\mathfrak{f}$ gezeigt haben, wo $\mathfrak{f}^{\ell-1}$ die Relativdiskriminante von K nach k ist. Denn dann ist nach Satz 21, 21a, S. 59▸, 62▸ K Klassenkörper für eine Klassengruppe H' vom Index ℓ in k, die jedenfalls nach unserem zugrundegelegten Strahl mod $\overline{\mathfrak{m}}$ erklärt werden kann. Diese Klassengruppe H' muß aber mit H identisch sein, wie folgende Betrachtung lehrt:*)

[Die Relativnormen von K_1 nach k liegen nach dem obigen in der Klassengruppe $\overline{\mathsf{H}}_0$ und umgekehrt enthält auch jede Klasse von $\overline{\mathsf{H}}_0$ Relativnormen aus K_1, weil K_1 Klassenkörper für $\overline{\mathsf{H}}_0$, also $\overline{\mathsf{H}}_0$ die K_1 zugeordnete Klassengruppe in k ist. Ist nun $\mathfrak{A}_1$ ein Ideal aus K_1, so ist

$$\mathfrak{a} = n_{K_1}(\mathfrak{A}_1) = n_K\big[n_{K_1 K}(\mathfrak{A}_1)\big] = n_K(\mathfrak{A})$$

*) Einfacher: Da K_1 Klassenkörper zu $\overline{\mathsf{H}}_0$ und K Klassenkörper zu H' und ferner K_1 Oberkörper von K, muß $\overline{\mathsf{H}}_0$ Untergruppe von H' sein, weil zudem $\overline{\mathsf{H}}_0$ und H' beide nach demselben Modul $\overline{\mathfrak{m}}$ erklärbar sind.

wo $\mathfrak{A}$ ein Ideal aus K ist. Jede Relativnorm $\mathfrak{a}$ aus K_1 ist also auch Relativnorm aus K und folglich jede Klasse die Relativnormen aus K_1 enthält (d.h. jede Klasse aus $\overline{\mathsf{H}}_0$) auch eine solche die Relativnormen aus K enthält (d.h. zu H' gehört).]

156 IV

Es ist also $\overline{\mathsf{H}}_0 < \mathsf{H}' < G$. Nun kann über

$$\overline{\mathsf{H}}_0 = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0]; \qquad (\text{Index } p\ell)$$

und unter

$$G = [C_1, C_2, \ldots, C_n; \mathsf{D}]$$

nur die Untergruppe von G:

$$\mathsf{H} = [C_1^\ell, C_2, \ldots, C_n; \mathsf{D}_0]; \qquad (\text{Index } \ell)$$

liegen, wenn der Index ℓ sein soll. Denn nimmt man zu $\overline{\mathsf{H}}_0$ das Element C_1 (oder, was gleichbedeutend, eine Potenz C_1^a mit zu ℓ primem a) hinzu, so enthält [...] $\overline{G}_0$ vom Index p und darüber kann, da p Primzahl, keine Untergruppe vom Index ℓ mehr liegen. Es kann also H' nur so aus $\overline{\mathsf{H}}_0$ entstehen, daß über D_0 eine solche Zwischengruppe $\mathsf{D}_0 < \mathsf{D}' < \mathsf{D}$ gelegt wird, daß der Index zu G gleich ℓ wird. Dazu muß aber $(\mathsf{D} : \mathsf{D}') = 1$ sein, da sich dieser Index wegen des Fehlens von C_1 zu $\ell \cdot (\mathsf{D} : \mathsf{D}')$ ergibt. Somit kommt für H' tatsächlich nur H in Frage, und K ist dann Klassenkörper zu H.

Es nun nur noch nachzuweisen, daß H' tatsächlich nach dem Modul $\overline{\mathfrak{m}}$ erklärt angenommen werden darf, also, wie soeben gesagt, die Teilbarkeit von $\overline{\mathfrak{m}}$ durch $\mathfrak{f}$ (d.h. daß H' keine engere Klasseneinteilung erfordert, als die von vorneherein zugrundegelegte).

157 IV

Die Relativdiskriminante von K_1 nach k hat nach den schon festgesetzten Bezeichnungen den Wert

$$(\mathfrak{f}_1^{p-1})^\ell n_{k_1 k}(\mathfrak{F}_1^{\ell-1}).$$

$\overline{\mathfrak{m}}$ ist nach Konstruktion durch $\mathfrak{f}_1$ teilbar, ferner nach S. 151 durch $\mathfrak{F}_1$ und als Ideal aus k auch durch die konjugierten zu $\mathfrak{F}_1$. Also kommen in dieser Relativdiskriminante nur Primfaktoren von $\overline{\mathfrak{m}}$ vor, demnach auch in $\mathfrak{f}$ keine anderen, da $\mathfrak{f}$ nach einer entsprechenden Formel Teiler der eben aufgestellten

Relativdiskriminante ist. Da ferner K den Relativgrad ℓ hat, geht jedes von den $\mathfrak{l}$ verschiedene Primideal $\mathfrak{p}$ von k höchstens zur ersten Potenz in $\mathfrak{f}$ auf. Für alle von den $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{p}$ ist also die Teilbarkeit von $\overline{\mathfrak{m}}$ durch $\mathfrak{f}$ gesichert. Es handelt sich nur noch um die Teiler $\mathfrak{l}$ von ℓ.

$\overline{\mathfrak{m}}$ möge genau durch $\mathfrak{l}^g$ teilbar sein. Geht $\mathfrak{l}$ nicht in der Relativdiskriminante von K_1 nach k auf, so geht es auch nicht in $\mathfrak{f}$ auf. Im übrigen haben wir folgende Zerlegungsmöglichkeiten für $\mathfrak{l}$ in K_1:

$$\textbf{1.)}\ \mathfrak{l} = (\mathfrak{L}_1 \dots \mathfrak{L}_\ell)^p.$$

Dann gilt in k_1: $\mathfrak{l} = \mathfrak{l}_1^p$, da k_1 vom Grade p, also einerseits die ℓ verschiedenen Primfaktoren in k_1 unmöglich, andererseits aus $\mathfrak{l} = \mathfrak{l}_1$ eine „Doppelzerlegung“ für (K_1, k_1) folgen würde. In K gilt: $\mathfrak{l} = \overline{\mathfrak{L}}_1 \dots \overline{\mathfrak{L}}_\ell$ aus ähnlichen Gründen, und es ist somit $\mathfrak{f}$ nicht durch $\mathfrak{l}$ teilbar.

158 IV

$$\textbf{2.)}\ \mathfrak{l} = \mathfrak{L}^p.$$

Dann kann in K nur $\mathfrak{l}$ unzerlegt bleiben, $\mathfrak{l}$ geht also ebenfalls in $\mathfrak{f}$ nicht auf.

$$\textbf{3.)}\ \mathfrak{l} = (\mathfrak{L}_1 \dots \mathfrak{L}_p)^\ell.$$

Dann muß in k_1 gelten: $\mathfrak{l} = \mathfrak{l}_1 \dots \mathfrak{l}_p$; $\mathfrak{l}_i = \mathfrak{L}_i^\ell$

und in K: $\mathfrak{l} = \mathfrak{L}^\ell$; $\mathfrak{L} = \mathfrak{L}_1 \dots \mathfrak{L}_p$.

$\overline{\mathfrak{m}}$ ist dann durch $\mathfrak{l}^g$, also durch jedes $\mathfrak{l}_i^g$ genau teilbar, $\mathfrak{F}_1$ durch $\mathfrak{l}_i^{v_1+1}$, wo v_1 die übliche Bedeutung für den relativ–zyklischen Körper K_1 über k_1 hat. Da $\overline{\mathfrak{m}}$ durch $\mathfrak{F}_1$[7] teilbar ist, ist $v_1 < g$. Die Relativdifferente von K_1 nach k hat als Produkt der beiden Relativdifferenten von K_1 nach k_1 und k_1 nach k (letztere ist prim zu ℓ), den Faktor $\mathfrak{L}_i^{(v_1+1)(\ell-1)}$.

Dieselbe Relativdifferente, als Produkt der beiden Relativdifferenten von K_1 nach K und K nach k (erstere prim zu ℓ), hat den Faktor $\mathfrak{L}^{(v+1)(\ell-1)}$, wenn $\mathfrak{l}^{v+1}$ der Faktor von $\mathfrak{f}$ ist, also jeden Faktor $\mathfrak{L}_i^{(v+1)(\ell-1)}$. Es ist somit $v = v_1$, folglich $v < g$, also $\overline{\mathfrak{m}}$ durch $\mathfrak{l}^{v+1}$ teilbar. Im Falle $g = 1$ übrigens folgt noch, daß $\mathfrak{l}$ in $\mathfrak{f}$ nicht aufgeht*), da $v < 1$ unmöglich.

[7] undeutlich

*) Präzis folgt, daß die angegebene Zerlegung unmöglich ist, ebenso unter 4.), [...] und somit keine Möglichkeit bleibt, wie $\mathfrak{l}$ in $\mathfrak{f}$ aufgehen kann.

4.) $\mathfrak{l} = \mathfrak{L}^{\ell}$.

Dann ist in k_1: $\mathfrak{l} = \mathfrak{l}_1$; $\mathfrak{l}_1 = \mathfrak{L}^{\ell}$

und in K: $\mathfrak{l} = \overline{\mathfrak{L}}^{\ell}$; $\overline{\mathfrak{L}} = \mathfrak{L}$.

$\overline{\mathfrak{m}}$ ist durch $\mathfrak{l}^g = \mathfrak{l}_1^g$ genau teilbar, also wenn $\mathfrak{F}_1$ durch $\mathfrak{l}_1^{(v_1+1)}$ teilbar ist, $v_1 < g$. Wie vorhin findet man ferner

159 IV

für den Faktor der Gesamtrelativdifferente auf den beiden möglichen Wegen

$$\mathfrak{L}^{(v_1+1)(\ell-1)} = \mathfrak{L}^{(v+1)(\ell-1)}, \quad \text{also} \quad v_1 = v,$$

und alles wie unter 3).

5.) $\mathfrak{l} = \mathfrak{L}^{p^{\ell}}$.

Dann ist in k_1: $\mathfrak{l} = \mathfrak{l}_1^p$; $\mathfrak{l}_1 = \mathfrak{L}^{\ell}$

und in K: $\mathfrak{l} = \overline{\mathfrak{L}}^{\ell}$; $\overline{\mathfrak{L}} = \mathfrak{L}^p$.

$\overline{\mathfrak{m}}$ ist durch $\mathfrak{l}_1^{pg}$ teilbar. Ist also $\mathfrak{F}_1$ durch $\mathfrak{l}_1^{v_1+1}$ teilbar, so ist $v_1 < pg$. $\mathfrak{f}_1$ ist durch y^1 teilbar, da $p \neq \ell$, ebenso die Relativdiskriminante von K_1 nach K durch $\overline{\mathfrak{L}}^{p-1}$. Es ergibt sich somit für die Gesamtrelativdifferente auf den beiden möglichen Wegen

$$\mathfrak{L}^{(v_1+1)(\ell-1)}\mathfrak{L}^{\ell(p-1)} = \mathfrak{L}^{p-1}\mathfrak{L}^{p(v+1)(\ell-1)}$$

wenn $\mathfrak{f}$ durch $\mathfrak{l}^{v+1}$ teilbar ist, also nach leichter Rechnung:

$$v_1 = pv,$$

also

$$pv < pg,$$

$$v < g,$$

und somit wieder $\overline{\mathfrak{m}}$ durch den Faktor $\mathfrak{l}^{v+1}$ von $\mathfrak{f}$ teilbar, und für $g = 1$ speziell $\mathfrak{f}$ prim zu $\mathfrak{l}$.

□□□

160 IV

Damit ist die Teilbarkeit von $\overline{\mathfrak{m}}$ durch $\mathfrak{f}$ gezeigt, und somit bewiesen, daß der Körper K Klassenkörper für die vorgelegte Klassengruppe H ist. Zum vollständigen Beweis unseres Satzes 44 und damit 43 ist letzens nur noch zu zeigen, daß auch die Schlußbehauptung von Satz 43 für den Körper K richtig ist, d.h. $\mathfrak{f}$ sogar Teiler des ursprünglichen Moduls $\mathfrak{m}$ ist. Nun entstand $\overline{\mathfrak{m}}$ aus $\mathfrak{m}$ durch Hinzufügung gewisser in $\mathfrak{m}$ nicht vorkommender Primteiler $\mathfrak{l}$ in der ersten Potenz. Nach der Schlußbemerkung unter 3.), 4.), 5.) ist aber $\mathfrak{f}$ durch diese Faktoren nicht teilbar. Also ist tatsächlich $\mathfrak{f}$ Teiler von $\mathfrak{m}$ und damit Satz 44 und also Satz 43 vollständig bewiesen.

Weiter folgt:

Satz 45. Ist H eine Klassengruppe vom Index ℓ in k und $\mathfrak{f}^{\ell-1}$ die Relativdiskriminante des Klassenkörpers zu H, so ist $\mathfrak{f}$ der *Führer* der Klassengruppe H.

Beweis. Nach Satz 21, 21a, S. 59▸, 62▸ ist in der Tat der Klassenkörper K zu H nach einer Klassengruppe H' mit dem Modul $\mathfrak{f}$ erklärbar. Diese Klassengruppe H' ist aber als K zugeordnete Klassengruppe eindeutig bestimmt, und somit $\mathsf{H}' = \mathsf{H}$, d.h. H ist auch dem Modul $\mathfrak{f}$ erklärbar.

Nach dem allgemeinen Existenzsatz 43 aber ist $\mathfrak{f}$ Teiler eines jeden Moduls $\mathfrak{m}$, nach dem H erklärbar ist.

Nach Definition dieses Begriffs ist also $\mathfrak{f}$ Führer der Klassengruppe H.

C. Existenz bei Primzahlpotenzgrad

C. Existenz des relativ–zyklischen Klassenkörpers von Primzahlpotenzgrad ℓ^ν.

Wir beweisen in diesem Abschnitt den folgenden Satz:

Satz 46. In einem beliebigen Körper k sei eine Klassengruppe H nach dem Modul $\mathfrak{m}$ vorgelegt, derart daß die Gruppe $\frac{G}{\mathsf{H}}$ zyklisch vom Primzahlpotenzgrad ℓ^ν ist, wo G die Gruppe aller Klassen nach dem Modul $\mathfrak{m}$ bedeutet (für $\ell = 2$ mit irgendeiner Vorzeichenbedingung definiert). Dann existiert ein Klassenkörper K für die Gruppe H, welcher überdies folgende Eigenschaften besitzt:

1.) K ist relativ–zyklisch vom Primzahlpotenzgrad ℓ^ν in Bezug auf k

2.) Die Relativdiskriminante von K nach k enthält kein Primideal als Faktor, das nicht in $\mathfrak{m}$ aufgeht.

Beweis. Für $\nu = 1$ ist der Satz vollständig durch Satz 43 bewiesen. Wir nehmen an Satz 46 sei richtig für Klassengruppen bis zum Index $\ell^{\nu-1}$ (bei *jedem* Körper k) und weisen daraus seine Richtigkeit für Klassengruppen vom Index ℓ^ν nach. Dann folgt seine Allgemeingültigkeit durch vollständige Induktion.

Wir definieren die Idealklassen in k nach dem Strahl o der Zahlen $\equiv 1 \bmod \mathfrak{m}$ (für $\ell = 2$ total positiv), womit wir, wie S. 141▸ gezeigt, *alle* Klassengruppen H

nach dem Modul $\mathfrak{m}$ erreichen können. G sei die Gruppe aller Klassen, H die vorgelegte Klassengruppe vom Index ℓ[...]. Da $\frac{G}{\mathsf{H}}$ zyklisch vom Grade ℓ^ν sein soll, gibt es eine Klasse C, sodaß

$$G = \mathsf{H} + C\mathsf{H} + C^2\mathsf{H} + \cdots + C^{\ell^\nu - 1}\mathsf{H},$$

kurz
$$G = (C; \mathsf{H})$$

ist, sodaß erst C^{ℓ^ν} in H liegt. Unter G_0 verstehen wir die Gruppe

$$G_0 = \mathsf{H} + C^\ell\mathsf{H} + C^{2\ell}\mathsf{H} + \cdots + C^{(\ell^{\nu-1}-1)\ell}\mathsf{H},$$

kurz
$$G_0 = (C^\ell; \mathsf{H}).$$

Dann ist
$$G = G_0 + CG_0 + \cdots + C^{\ell-1}G_0 = (C; G_0),$$

d.h. $\dfrac{G}{G_0}$ zyklisch vom Grade ℓ.

Nach Satz 43 existiert also ein Klassenkörper k_1 zu k für die Gruppe G_0, der relativ–zyklisch vom Grade ℓ ist.

Nach den Ausführungen von S. 72▸ ff gibt es in k_1 ein in $\mathfrak{m}$ aufgehendes, invariantes Ideal $\mathfrak{m}_1$ (das dortige $\mathfrak{M}$), sodaß, wenn in k_1 die Idealklassen nach dem Strahl o_1 der Zahlen $\equiv 1 \bmod \mathfrak{m}_1$ (für $\ell = 2$ total positiv) erklärt werden, die Relativnormen von o_1 in o fallen, sodaß die Relativnormen einer Klasse nach o_1 in k_1 in eine bestimmte Klasse nach o in k fallen und somit von Relativnormen der Klassen aus k_1 nach k gesprochen werden kann.

Es sei nun H_1 die Gruppe derjenigen Klassen von k_1, deren Relativnormen in die Gruppe H fallen. Wie im vorigen Abschnitt soll ferner unter C auch gleichzeitig diejenige Klasse in k_1 verstanden werden, die die Ideale

von C in k enthält, also die durch C in k_1 induzierte Klasse. Dann ist $n(C) = C^{\ell}$.

Da k_1 Klassenkörper für G_0 ist, fällt die Relativnorm irgendeiner Klasse C_1 von k_1 in die Gruppe G_0, hat also die Form

$$n(C_1) = C^{a\ell}[\mathsf{H}],$$

wo $[\mathsf{H}]$ eine Klasse aus H bedeutet. Setzen wir also

$$C_1 = C^a U_1,$$

so ist $$n(C_1) = C^{a\ell} n(U_1),$$

also $$n(U_1) = [\mathsf{H}].$$

U_1 ist also eine Klasse aus H_1, sodaß wir jede Klasse C_1 von k_1 in der Form schreiben können:

$$C_1 = C^a[\mathsf{H}_1].$$

Um den Exponenten von C in k_1 in Bezug auf H_1 festzustellen, sei

$$C^a = [\mathsf{H}_1]$$

in k_1, also

$$C^{a\ell} = [\mathsf{H}]$$

in k. Daraus folgt: $$a\ell \equiv 0 \bmod \ell^{\nu},$$

also: $$a \equiv 0 \bmod \ell^{\nu-1}.$$

Umgekehrt ist sicher:

$$C^{\ell^{\nu-1}} = [\mathsf{H}_1],$$

weil die Norm $C^{\ell^{\nu}}$ in H fällt. Es gehört also C in k_1 in Bezug auf H_1 zum Exponenten $\ell^{\nu-1}$, d.h. die Gruppe G_1 aller Klassen von k_1 gestattet die Darstellung:

$$G_1 = (C; \mathsf{H}_1) = \mathsf{H}_1 + C\mathsf{H}_1 + \cdots + C^{\ell^{\nu-1}-1}\mathsf{H}_1.$$

Die Gruppe $\frac{G_1}{\mathsf{H}_1}$ ist also zyklisch vom Grade $\ell^{\nu-1}$.

164 IV

Nach Annahme existiert also ein relativ–zyklischer Klassenkörper K über k_1 für die Gruppe H_1 vom Relativgrade $\ell^{\nu-1}$ und der in Satz 46 genannten Eigenschaft 2.), d.h. die Relativdiskriminante von K nach k_1 enthält nur Primfaktoren, die in $\mathfrak{m}_1$ vorkommen.

Nun ist $\mathfrak{m}_1$ ein invariantes Ideal von k_1, also (s. S. 151▸ unten) führen die Substitutionen von k_1 jede Klasse von k_1 nach o_1 in eine bestimmte andere Klasse nach o_1 über. Da die Gruppe H_1 laut ihrer Definition demnach invariant gegenüber den Substitutionen von k_1 ist, folgt wie S. 152▸, daß K *relativ–Galoissch zu* k ist.

Die Relativnormen der Ideale von K fallen in k_1 in die Gruppe H_1, für die K Klassenkörper ist; die Relativnormen von H_1 nach k fallen nach Definition von H_1 in H; also fallen die Relativnormen von K nach k in die Gruppe H. Dem Galoisschen Körper K über k ist somit eine Untergruppe von H zugeordnet. Nun hat aber K den Grad ℓ^ν über k. Die zugeordnete Klassengruppe in k muß also einen Index $\leqq \ell^\nu$ haben, also als Untergruppe der Gruppe H vom Index ℓ^ν mit H identisch sein. K ist also der Gruppe H selbst zugeordnet und folglich Klassenkörper für H.

Es bleiben nunmehr noch die Eigenschaften 1.) und 2.) von Satz 46 nachzuweisen. Für den Nachweis von 1.) stützen wir uns auf folgenden Hilfssatz (Weber, Alg. II, S. 128, Satz II; 2. Aufl. S. 140, Satz VI). (Speiser, Satz 56)

165 IV

Hilfssatz. Ist $\mathfrak{G}$ eine Gruppe vom Grade ℓ^ν, $\mathfrak{g}$ eine Untergruppe vom Grade ℓ^ν $(\mu < \nu)$, so gibt es stets eine Untergruppe $\mathfrak{g}_1$ vom Grade $\ell^{\mu+1}$ von der $\mathfrak{g}$ invariante Untergruppe ist.

Für $\mu = \nu - 1$ ergibt sich also, daß jede Untergruppe $\mathfrak{G}_0$ vom Grade $\ell^{\nu-1}$ invariante Untergruppe zu $\mathfrak{G}$ ist, ferner, daß $\mathfrak{G}_0$ so gewählt werden darf, daß es eine vorgelegte Untergruppe $\mathfrak{g}$ vom Grade ℓ^μ $(\mu < \nu)$ enthält (nicht notwendig als invariante Untergruppe).

Sei nun $\mathfrak{G}$ die Galoissche Gruppe von K vom Grade ℓ^ν in Bezug auf k, $\mathfrak{G}_0$ irgendeine Untergruppe vom Grade $\ell^{\nu-1}$. Ein solches $\mathfrak{G}_0$ existiert sicher, da K den Unterkörper k_1 vom Grade ℓ enthält, der zu einer Untergruppe vom Grade $\ell^{\nu-1}$ gehören muß. Ich zeige aber, daß auch nur diese Untergruppe vom Grade $\ell^{\nu-1}$ in $\mathfrak{G}$ enthalten ist, also jedes $\mathfrak{G}_0$ vom Grade $\ell^{\nu-1}$ den Körper k_1 als zugeordneten Körper hat. Da nämlich $\mathfrak{G}_0$ nach dem Hilfssatz invariante Untergruppe ist, gehört zu ihr ein relativ–zyklischer Körper k_0 vom Primzahl-

grad ℓ über k. Die $\ell^{\nu-1}$–ten Potenzen der Relativnormen seiner Ideale sind dann Relativnormen aus K, liegen also in H. Diese Relativnormen selbst liegen also in Klassen, deren $\ell^{\nu-1}$–te Potenzen in H liegen, also die Form $C^{a\ell}[\mathsf{H}]$ haben, d.h. in G_0 liegen. k_0 ist also einer Klassengruppe zugeordnet, die Untergruppe von G_0

166 IV

ist, also da deren Index in Bezug auf G den Relativgrad ℓ von k_0 nicht überschreiten darf, und G_0 den Index ℓ hat, mit G_0 identisch ist. k_0 ist also Klassenkörper zu G_0, d.h. $k_0 = k_1$, also $\mathfrak{G}_0$ die eine einzige Gruppe, zu der k_1 gehört.□□□ Es gibt also nur eine einzige Untergruppe $\mathfrak{G}_0$ von $\mathfrak{G}$ vom Grade $\ell^{\nu-1}$.

Sei nun

$$\mathfrak{G} = \mathfrak{G}_0 + \sigma\mathfrak{G}_0 + \cdots + \sigma^{\ell-1}\mathfrak{G}_0.$$

Wäre der Exponent, zu dem σ als Element von $\mathfrak{G}$ gehört, kleiner als ℓ^ν, so würde durch σ eine Untergruppe $\mathfrak{g}$ vom Grade $\ell^\mu < \ell^\nu$ erzeugt, und es gäbe nach unserem Hilfssatz eine Untergruppe $\overline{\mathfrak{G}}_0$ vom Grade $\ell^{\nu-1}$, die $\mathfrak{g}$ enthält. Nach dem Gezeigten wäre $\overline{\mathfrak{G}}_0 = \mathfrak{G}_0$, also σ in $\mathfrak{G}_0$ enthalten, während es doch als von $\mathfrak{G}_0$ verschieden ausgewählt war. Also gehört σ zum Exponenten ℓ^ν, seine Potenzen erschöpfen die Gruppe $\mathfrak{G}$ vom Grade ℓ^ν vollständig, d.h. $\mathfrak{G}$ ist zyklisch vom Grade ℓ^ν, also auch K *zyklisch vom Grade* ℓ^ν.

Der Nachweis der Eigenschaft 2.) von Satz 46 gestaltet sich so: Die Relativdiskriminante $\mathfrak{D}_1$ von k_1 nach k enthält nach Satz 43 nur Primteiler von $\mathfrak{m}$, die Relativdiskriminante $\mathfrak{D}_2$ von K nach k_1 nach Annahme nur solche von $\mathfrak{m}_1$. Die Gesamtrelativdiskriminante ist:

$$\mathfrak{D} = \mathfrak{D}_1^{\ell^{\nu-1}} n_{k_1}(\mathfrak{D}_2).$$

Da $\mathfrak{m}_1$ in $\mathfrak{m}$ aufgeht, kommt die Relativnorm n_{k_1} eines jeden Primteilers von $\mathfrak{m}_1$ in $\mathfrak{m}$ vor, also auch sicher jeder Primteiler von $n_{k_1}(\mathfrak{D}_2)$. Also enthält auch $\mathfrak{D}$ nur Primfaktoren von $\mathfrak{m}$.

Damit ist Satz 46 vollständig bewiesen.

167 IV

D. Existenz im allgemeinen Fall

D. Existenz des Klassenkörpers für beliebige Klassengruppen.

Hauptsatz I. In einem algebraischen Körper k sei irgendeine Klassengruppe H nach dem Modul $\mathfrak{m}$ (mit oder ohne Vorzeichenbedingungen) gegeben. Dann existiert stets ein Klassenkörper K über k für H mit folgenden Eigenschaften:

1.) K ist relativ–Abelsch zu k und der Relativgrad ist gleich dem Index der Gruppe H.

2.) Ist G die Gruppe aller Idealklassen mod $\mathfrak{m}$ in k, so ist die Relativgruppe von K einstufig isomorph mit der Faktorgruppe $\frac{G}{\mathsf{H}}$.

3.) Die Relativdiskriminante von K enthält kein Primideal als Faktor, das nicht in $\mathfrak{m}$ aufgeht.

Dem Beweise schicken wir folgenden Satz voraus:

Satz 47. Die Relativnormen aus den Körpern $K_1, \ldots, K_s$ über k mögen bezw. in die Klassengruppen $\mathsf{H}_1, \ldots, \mathsf{H}_s$ von k nach einem– und demselben Modul $\mathfrak{m}$ fallen. Dann fallen die Relativnormen aus dem komponierten Körper

$$K = (K_1, K_2, \ldots, K_s)$$

in den Gruppendurchschnitt

$$\mathsf{H} = (\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_s).$$

Beweis. Bilden wir die Relativnorm eines Ideals aus K nach k über K_i, so sehen wir, daß sie in die Gruppe H_i fällt. Da dies für jedes i gilt, fällt sie in den, wegen des übereinstimmenden Moduls $\mathfrak{m}$*) sicher zu bildenden, Durchschnitt der H_i, w.z.b.w.

(Natürlich kann man die Voraussetzung betr. $\mathfrak{m}$ stets durch Einführung eines genügend hohen Moduls erreichen).

Wir beweisen nun unseren Hauptsatz I. Dazu bilden wir die Faktorgruppe $\frac{G}{\mathsf{H}}$ und stellen sie durch eine Basis dar. Dieser Basisdarstellung entsprechend

*) Natürlich müssen, falls die H_i Vorzeichenbedingungen erfordern, für alle H_i gleichzeitig hinreichende Vorzeichenbedingungen der Klasseneinteilung zugrundegelegt werden. Wesentlich ist nur, daß die H_i sämtlich als Gruppen von *derselben* Sorte von Elementen (Klassen) erklärt sind.

gibt es Klassen $C_1, \ldots, C_s$, sodaß erst die $\ell_i^{\nu_i}$–te Potenz von C_i in H liegt und jede Nebengruppe von H eindeutig in der Form darstellbar ist:

$$C_1^{a_1} \ldots C_s^{a_s} \mathsf{H}; \qquad (0 \leqq a_k \leqq \ell^{\nu_k} - 1),$$

wobei die ℓ_i Primzahlen und die ℓ^{ν_i} die Invarianten der Abelschen Gruppe $\dfrac{G}{\mathsf{H}}$ sind.

Wir verstehen dann unter H_i die Gruppe aller Nebengruppen, in denen das Basiselement C_i fehlt:

$$\mathsf{H}_i = C_1^{a_1} \ldots C_{i-1}^{a_{i-1}} C_{i+1}^{a_{i+1}} \ldots C_s^{a_s} \mathsf{H}; \qquad (0 \leqq a_k \leqq \ell^k - 1),$$

sodaß offenbar

$$G = \mathsf{H}_i + C_i \mathsf{H}_i + \cdots + C_i^{\ell_i^{\nu_i} - 1} \mathsf{H}_i$$

ist, also $\dfrac{G}{\mathsf{H}_i}$ zyklisch vom Grade $\ell_i^{\nu_i}$ ist.

Nach Satz 46 existiert für jedes solche H_i ein relativ–zyklischer Klassenkörper K_i vom Grade $\ell_i^{\nu_i}$ über k mit der

167b IV

Eigenschaft 2.) von Satz 46. Der komponierte Körper

$$K = (K_1, \ldots, K_s)$$

hat dann folgende Eigenschaften:

1.) Sein Grad nach k hat höchstens den Wert $\ell_1^{\nu_1} \ldots \ell_s^{\nu_s}$.

2.) Er ist relativ–Abelsch über k.

3.) Die Relativnormen nach k seiner Ideale liegen sämtlich im Durchschnitt von $\mathsf{H}_1, \ldots, \mathsf{H}_s$, der offensichtlich gleich H ist.

1.) ist klar, da der komponierte Körper höchstens das Produkt der Grade der Komponenten zum Grade haben kann.

3.) folgt unmittelbar aus Satz 47.

2.) ist ein Satz der Galoisschen Theorie, den man wie folgt einsieht: Sind K_1, K_2 Abelsch über k und α, β erzeugende Elemente aus K_1, K_2, die c_{ik}

Elemente aus k, so läßt sich jede Zahl A des komponierten Körpers (K_1, K_2) in der Form schreiben

$$\mathsf{A} = \varphi(\alpha, \beta) = \sum_{i,\kappa} c_{i\kappa}\alpha_i\beta_\kappa$$

wo die α_i, β_κ je ein System in Bezug auf k linear unabhängiger Elemente aus K_1, K_2 durchlaufen. Sind nun σ, τ je eine Substitution von K_1, K_2, so wird

$$\sigma\tau\mathsf{A} = \sum_{i,\kappa} c_{i\kappa} \cdot \sigma\alpha_i \cdot \tau\beta_\kappa = \tau\sigma\mathsf{A},$$

da ja die α_i von τ, die β_κ von σ unberührt bleiben. Die Substitutionen σ unter sich und τ unter sich sind sicher vertauschbar, also auch alle Substitutionen die aus den σ und τ zusammengesetzt sind. Da durch diese Substitutionen sicher

168b IV

alle überhaupt denkbaren „Konjugierten–Bildungen“ in (K_1, K_2) erschöpft werden, muß die Galoissche Gruppe des Normalkörpers (K_1, K_2) durch einen Teil der σ, τ und ihrer Produkte dargestellt werden können, ist somit Abelsch. Das gleiche gilt natürlich für beliebig viele komponierte Körper.

Nach 3.) ist K eine Untergruppe von H zugeordnet. Diese muß aber mit H identisch sein. Denn der Grad g von K ist nach 1.) $g \leqq \ell_1^{\nu_1} \dots \ell_s^{\nu_s}$, also der Index jener zugeordneten Klassengruppe $j \leqq g \leqq \ell_1^{\nu_1} \dots \ell_s^{\nu_s}$, andererseits der Index von H genau $\ell_1^{\nu_1} \dots \ell_s^{\nu_s}$, also der jener Untergruppe $j \geqq \ell_1^{\nu_1} \dots \ell_s^{\nu_s}$. Also ist

$$j = g = \ell_1^{\nu_1} \dots \ell_s^{\nu_s}.$$

K ist also vom Grade $\ell_1^{\nu_1} \dots \ell_s^{\nu_s}$ und Klassenkörper zu H.
□□□

169 IV

Die Galoissche Gruppe $\mathfrak{G}$ von K muß nach den oben ausgeführten Überlegungen durch einen Teil der Substitutionen

$$\sigma_1^{a_1} \dots \sigma_s^{a_s}; \qquad (0 \leqq a_i \leqq \ell^{\nu_i} - 1)$$

dargestellt werden, wo die σ_i die erzeugenden Substitutionen der zyklischen Gruppen $\mathfrak{G}_i$ der K_i sind. Da dies höchstens $\ell_1^{\nu_1} \dots \ell_s^{\nu_s}$ verschiedene Substitu-

tionen sind, K aber genau den Grad $g = \ell_1^{\nu_1} \dots \ell_s^{\nu_s}$ hat, müssen diese Substitutionen alle verschieden sein, und in ihrer Gesamtheit die Gruppe $\mathfrak{G}$ bilden. $\mathfrak{G}$ ist also isomorph zu der eben betrachteten Faktorgruppe $\frac{G}{\mathsf{H}}$.

Nach Satz 46 enthält schließlich jeder Körper K_i in seiner Relativdiskriminante keine anderen Primteiler, als in $\mathfrak{m}$ aufgehen. Nach A.Z. I, Satz 19, S. 20 gilt also dasselbe für die Relativdiskriminante von K.

Damit ist Hauptsatz I vollständig bewiesen. Die in ihm ausgesagten Eigenschaften 1.) – 2.) des Klassenkörpers kann man auch so aussprechen:

Satz 48. Ist K der Klassenkörper für die Klassengruppe H in k und definiert man die Idealklassen in k nach der Gruppe H als Hauptklasse, so gilt:

1.) Der Grad von K nach k ist gleich der Klassenzahl in k

2.) Die Gruppe von K ist isomorph mit der Gruppe der Idealklassen in k.

4.5 §5 Relativ–abelsche Körper als Klassenkörper

170 IV

§5. Relativ–Abelsche Körper als Klassenkörper.

Beim Beweise des Existenzsatzes hat sich herausgestellt, daß jeder Klassenkörper relativ–Abelsch ist. Wir beweisen in diesem Abschnitt die Umkehrung, nämlich:

Hauptsatz II. Jeder relativ–Abelsche Körper K über k ist Klassenkörper für eine gewisse Klassengruppe H in k nach einem gewissen Modul $\mathfrak{m}$. Dieser Modul $\mathfrak{m}$ kann überdies so gewählt werden, daß in $\mathfrak{m}$ nur die Teiler der Relativdiskriminante von K nach k aufgehen*).

Vergleicht man die letzte Aussage dieses Satzes mit der Eigenschaft 3.) aus Hauptsatz 1, so kann unmittelbar gefolgert werden, (vergl. die analoge Überlegung S. 160▶):

Satz 49. In der Relativdiskriminante des Klassenkörpers zu einer Klassengruppe H gehen alle und nur die Primideale auf, die im Führer der Klassengruppe H aufgehen.

Wir führen den Beweis von Hauptsatz II zunächst auf den Fall zurück, daß K relativ–zyklisch von Primzahlpotenzgrad zu k ist.

Sei also K relativ–Abelsch zu k und zusammengesetzt aus den Körpern $K_1, K_2, \ldots, K_s$, die relativ–zyklisch von Primzahlpotenzgraden angenommen werden dürfen und überdies so, daß jedes K_i zum Kompositum der übrigen in Bezug auf k teilerfremd ist (den Durchschnitt k liefert),

171 IV

wie sich unmittelbar aus der Galoisschen Theorie ergibt†)

*) und diese alle nach Hauptsatz I, 3.).

†) Sei $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_s$ die entsprechend der Basisdarstellung in ein direktes Produkt zerlegte Gruppe von K, (also die $\mathfrak{G}_i$ zyklisch von Primzahlpotenzgrad $\ell_i^{\nu_i}$). Dann gehören zu den i Gruppen $\mathfrak{g}_i = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_{i-1} \times \mathfrak{G}_{i+1} \cdots \times \mathfrak{G}_s$ i Körper K_i, die zyklisch von den

Wir betrachten zunächst die ersten beiden Körper K_1, K_2, deren Durchschnitt nach dem Gesagten k ist. Sie mögen Klassenkörper für die Klassengruppen $\mathsf{H}_1, \mathsf{H}_2$ von den Indizes n_1, n_2 resp. nach den Moduln $\mathfrak{m}_1, \mathfrak{m}_2$ sein. H_1 und H_2 können nach dem kleinsten gemeinsamen Multiplum $\mathfrak{m}_{12}$ von $\mathfrak{m}_1, \mathfrak{m}_2$ gleichzeitig erklärt werden. Aus H_1 und H_2 bilden wir die durch sie erzeugte Untergruppe

$$\overline{G} = \mathsf{H}_1 \cdot \mathsf{H}_2$$

der Gruppe G aller Idealklassen nach $\mathfrak{m}$ (mit hinreichend scharfer Vorzeichenbedingung). H_1 und H_2 sind Untergruppen von $\overline{G}$, also der Klassenkörper für $\overline{G}$ ein Unterkörper von K_1 und K_2, also k, demnach $\overline{G} = G$ und

$$G = \mathsf{H}_1 \cdot \mathsf{H}_2.$$

Es sei nun $\mathsf{H}_0 = (\mathsf{H}_1, \mathsf{H}_2)$ der Durchschnitt und

$$\begin{aligned} \mathsf{H}_1 &= \mathsf{H}_0 + a_1\mathsf{H}_0 + \cdots a_{\mu-1}\mathsf{H}_0, \\ \mathsf{H}_2 &= \mathsf{H}_0 + b_1\mathsf{H}_0 + \cdots b_{\nu-1}\mathsf{H}_0. \end{aligned}$$

$\mathsf{H}_1\mathsf{H}_2$ besteht dann aus allen Komplexen $a_i b_\kappa \mathsf{H}_0$. Diese sind alle verschieden, da aus

$$a_i b_\kappa \mathsf{H}_0 = a_p b_q \mathsf{H}_0$$

folgt:

$$a_i a_p^{-1} \mathsf{H}_0 = b_q b_\kappa^{-1} \mathsf{H}_0,$$

was nach Definition von H_0 nur möglich ist, wenn beide Komplexe mit H_0 übereinstimmen. Es ist also der Index von H_0 nach $\mathsf{H}_1\mathsf{H}_2 = G$ gleich $\mu \cdot \nu$. Ferner ist

$$\begin{aligned} G &= \mathsf{H}_1 + b_1\mathsf{H}_1 + \cdots + b_{\nu-1}\mathsf{H}_1 \\ &= \mathsf{H}_2 + a_1\mathsf{H}_2 + \cdots + a_{\mu-1}\mathsf{H}_2 \end{aligned}$$

entsprechenden Primzahlpotenzgraden $\ell_i^{\nu_i}$ sind. Ihr Kompositum gehört zum Durchschnitt aller $\mathfrak{g}_i$, also zur identischen Gruppe, ist mithin K. K_i ist ferner teilerfremd zu $k_i = (K_1, \ldots, K_{i-1}, K_{i+1}, \ldots, K_s)$, da k_i höchstens den Grad $\ell_1^{\nu_1} \ldots \ell_{i-1}^{\nu_{i-1}} \ell_{i+1}^{\nu_{i+1}} \ldots \ell_s^{\nu_s}$ und K_i den Grad $\ell_i^{\nu_i}$ hat, $(k_i, K_i) = K$ aber den Grad $\ell_1^{\nu_1} \ldots \ell_s^{\nu_s}$, sodaß nach Weber, Kl. Alg., S. 267, 7.) k_i und K_i teilerfremd sein müssen (und überdies der Grad von k_i den angegebenen Höchstwert erreicht).

und die Komplexe $b_i\mathsf{H}_1$ sowie $a_i\mathsf{H}_2$ verschieden untereinander, da z.B.

$$b_1\mathsf{H}_1 = b_1\mathsf{H}_0 + b_1a_1\mathsf{H}_0 + \cdots + b_1a_{\mu-1}\mathsf{H}_0,$$
$$b_2\mathsf{H}_1 = b_2\mathsf{H}_0 + b_2a_1\mathsf{H}_0 + \cdots + b_2a_{\mu-1}\mathsf{H}_0$$

ist und die $a_ib_\kappa\mathsf{H}_0$ sämtlich verschieden sind. Daher ist der eben so bezeichnete Index n_1 von H_1 gleich ν und $n_2 = \mu$.

Es hat somit H_0 *den Index* n_1n_2. Der aus K_1 und K_2 komponierte Körper K_{12} hat den Grad n_1n_2 *).

Nach Satz 47 (S. 167▸) fallen die Relativnormen der Ideale aus K_{12} in H_0, sodaß K_{12} eine Untergruppe von H_0 zugeordnet ist, und da deren Index $\leqq n_1n_2$ sein muß, die Gruppe H_0 selbst. K_{12} ist also Klassenkörper für H_0.

Da K_3 teilerfremd zu K_{12} ist, kann man so fortfahren und erhält schließlich, daß $K = (K_1, \ldots, K_s)$ Klassenkörper

173 IV

nach der Klassengruppe $\mathsf{H} = (\mathsf{H}_1, \ldots, \mathsf{H}_s)$ ist, wobei der Modul sich auf das kleinste gemeinsame Vielfache $\mathfrak{m}$ aller $\mathfrak{m}_i$ erhöht, nachdem die H_i definiert sind. In $\mathfrak{m}$ gehen also nur die Primteiler auf, die auch in den $\mathfrak{m}_i$ vorkommen, und in den $\mathfrak{m}_i$, wenn der Hauptsatz II für Primzahlpotenzgrad als richtig angenommen wird, nur die Teiler der Relativdiskriminanten $\mathfrak{D}_i$ der K_i. Nach A.Z. I, Satz 10, S. 20▸†) gehen aber in den $\mathfrak{D}_i$ keine anderen Primteiler auf als in in der Relativdiskriminante $\mathfrak{D}$ von K. Also enthält $\mathfrak{m}$ keine anderen Primfaktoren, als in $\mathfrak{D}$ vorkommen.

Wir haben somit den Hauptsatz II nur noch für zyklische Körper K vom Primzahlpotenzgrad ℓ^ν über k zu beweisen und zeigen dazu im Interesse der anzuwendenden vollständigen Induktion gleich den folgenden schärferen Satz:

Satz 50. Es sei K relativ–zyklisch vom Primzahlpotenzgrad ℓ^ν über k. Dann gibt es stets ein Ideal $\mathfrak{m}$ in k, welches nur die Primteiler der Relativdiskriminante von K enthält, und zwar die zu ℓ primen in der ersten Potenz, die Teiler von ℓ in einer genügend hohen, sodaß K Klassenkörper für eine Klassengruppe H vom Index ℓ^ν mod $\mathfrak{m}$ ist.

Ferner gibt es in K ein in $\mathfrak{m}$ aufgehendes, invariantes

174 IV

*)Weber, kl. Alg., S. 267, 7.)

†)oder einfach, weil $\mathfrak{D}$ durch alle $\mathfrak{D}_i$ teilbar ist.

Ideal $\mathfrak{M}$ derart, daß, wenn die Idealklassen nach den Strahlen

$$\begin{array}{lcll} o & : & \alpha \equiv 1 \bmod \mathfrak{m} & (\text{f. } \ell = 2 \text{ tot.pos.}) \quad \text{in } k, \\ O & : & \mathsf{A} \equiv 1 \bmod \mathfrak{M} & (\text{f. } \ell = 2 \text{ tot.pos.}) \quad \text{in } K \end{array}$$

definiert werden und σ eine erzeugende Substitution von K ist, sich die Relativnormen der Klassen aus K als bestimmte Klassen aus k erklären lassen, ebenso die konjugierten zu einer Klasse in K als bestimmte Klassen in K.

Werden dann alle Klassen von K deren Relativnorm ein– und dieselbe Klasse von k ist, in ein *Geschlecht* zusammengefaßt, insbesondere also diejenige Klassengruppe in K, deren Relativnorm die Hauptklasse in k ist, das *Hauptgeschlecht* genannt, so gelten die folgenden Tatsachen*):

1.) Jedes Geschlecht besteht aus ein– u. derselben Anzahl von Klassen von K.

2.) Die Anzahl der Geschlechter, d.h. der Index der Klassengruppe: Hauptgeschlecht, deren Nebengruppen die übrigen Geschlechter sind, ist gleich dem ℓ^{ν}–ten Teil der Anzahl h_1 der Klassen nach o in k.

3.) Das Hauptgeschlecht ist der Inbegriff aller symbolischen $(1 - \sigma)$–ten Klassenpotenzen aus K.

Zu $\mathfrak{m}$ und $\mathfrak{M}$ kann noch unbeschadet der Richtigkeit aller Behauptungen ein beliebiger Faktor $\mathfrak{a}$ aus k genommen werden.

175 IV

Beweis. In Satz 22, S. 82▸/83▸ wurde die Existenz zweier Moduln $\mathfrak{m}$ und $\mathfrak{M}$ mit den genannten Eigenschaften vollständig bewiesen für den Fall des relativ–zyklischen Körpers vom Primzahlgrade ℓ; $(\nu = 1)$. Wir können also vollständige Induktion anwenden und annehmen, der Satz 50 sei bis $\ell^{\nu-1}$ richtig.

Was dabei die Tatsachen 1.) und 2.) anbelangt, so folgt ihre Richtigkeit aus den vorher aufgestellten Behauptungen ohne weiteres, wie im Beweis zu Satz 22 (s. S. 78▸).

1.) folgt einfach daraus, daß das Hauptgeschlecht eine Klassengruppe in K ist, deren Nebengruppen die übrigen Geschlechter sind.

*) Das soll besagen: $\mathfrak{m}$ und $\mathfrak{M}$ lassen sich so wählen, daß diese Tatsachen gelten.

2.) ergibt sich daraus, daß die Anzahl der Geschlechter nach Definition derselben mit der Anzahl der Relativnormklassen in k ist. Letztere machen aber gerade die Klassengruppe H in k aus, nach der K Klassenkörper ist. Ihre Anzahl ist somit gleich $\frac{h_1}{\ell^\nu}$, wenn h_1 die Anzahl aller Klassen nach o in k bezeichnet, weil ℓ^ν der Index von H ist.

Es sind also bei der vollständigen Induktion nur die zu Beginn ausgesprochenen Behauptungen über die Moduln $\mathfrak{m}$ und $\mathfrak{M}$, sowie die Tatsache 3.) zu berücksichtigen.

Sei nunmehr K ein vorgelegter, relativ–zyklischer Körper ℓ^ν–ten Grades über k, σ seine erzeugende Substitution und K' der in K enthaltene relativ–zyklische Unterkörper vom Grade $\ell^{\nu-1}$ der zur Gruppe

$$\mathfrak{g} = (1, \sigma^{\ell^{\nu-1}}, \ldots, \sigma^{(\ell-1)\ell^{\nu-1}})$$

gehört. Die Zahlen und Ideale aus K' erleiden, wenn man sie in K betrachtet, durch σ gerade die Substitution, welche die Gruppe von K' in Bezug auf k erzeugt, sodaß wir σ als erzeugende Substitution von K' betrachten können, mit der Bemerkung, daß bereits $\sigma^{\ell^{\nu-1}}$ in Bezug auf K' die Einheitssubstitution ist. K ist in Bezug auf K' relativ–zyklisch vom Primzahlgrad ℓ mit der Gruppe $\mathfrak{g}$, deren erzeugende Substitution $\sigma^{\ell^{\nu-1}}$ ist.

Die in der Relativdiskriminante von K aufgehenden Primideale mögen mit $\mathfrak{p}$ (prim zu ℓ) und $\mathfrak{l}$ (Teiler von ℓ) bezeichnet werden. Ihre Idealfaktoren in K' und K, deren es auch mehrere geben kann, die dann *alle* in den Produkten auftreten sollen, seien mit $\mathfrak{P}', \mathfrak{L}'$ und $\mathfrak{P}, \mathfrak{L}$ bezeichnet. (Dabei braucht aber $\mathfrak{p}, \mathfrak{l}$ in der Relativdiskriminante von K' nicht aufzugehen).

Nun ist Satz 50 richtig für K'. Setzen wir also:

$$\mathfrak{m} = \prod \mathfrak{p} \cdot \prod \mathfrak{l}^u \cdot \mathfrak{a}; \qquad \mathfrak{M}' = \prod \mathfrak{P}' \cdot \prod \mathfrak{L}'^{U'} \cdot \mathfrak{a},$$

wo $\mathfrak{a}$ ein beliebiges Ideal aus k ist, (das für unsere Hauptanwendung*) gleich 1 zu setzen ist), so ist für genügend große u und U' folgendes richtig:

Werden in k und K' die Idealklassen nach den Strahlen:

$$\begin{aligned} o \quad &: \quad \alpha \equiv 1 \bmod \mathfrak{m}; \quad (\text{für } \ell = 2 \text{ total positiv}), \\ O' \quad &: \quad \mathsf{A}' \equiv 1 \bmod \mathfrak{M}'; \quad (\text{für } \ell = 2 \text{ total positiv}) \end{aligned}$$

*) d.h. nachher für den Körper K. Für die Induktion brauchen wir aber $\mathfrak{a}$ zur Berücksichtigung

erklärt, so ist K' Klassenkörper für eine Klassengruppe H' vom Index $\ell^{\nu-1}$ in k mod $\mathfrak{m}$. Ferner ist nach Annahme

177 IV

$\mathfrak{M}'$ als invariantes Ideal aus K' wählbar, also die konjugierten zu einer Klasse C' von K' eindeutig bestimmte Klassen in K' (die Strahlzahlen von O' gehen durch die Substitutionen von K' wieder in die Strahlzahlen von O' über). Weiter liegen nach Annahme der Richtigkeit des Satzes 50 für K' die Relativnormen aus O' in o, womit die Möglichkeit der Definition der Relativnormen der Klassen aus K' gesichert ist. Schließlich ist jede Klasse in K', deren Relativnorm die Hauptklasse in k ist, $(1-\sigma)$ te Potenz einer Klasse von K' und umgekehrt. (Letzteres ist klar, und braucht auch bei der Induktion nicht mitbewiesen zu werden, da sicher $n(C') = n(\sigma C'\texttt{[...]})$, also $n(C'^{1-\sigma}) = 1$ ist). Endlich kann $\mathfrak{m}$ durch $\mathfrak{M}'$ teilbar angenommen werden, und gelten alle genannten Tatsachen unverändert, wie auch $\mathfrak{a}$ gewählt sein mag. (Die eigentlichen, zu Beginn des Satzes 50 genannten Moduln $\mathfrak{m}$ und $\mathfrak{M}'$ für den Körper K' sollen ja nur die Primfaktoren der Relativdiskriminante *von* K' enthalten. In unserm eben gemachten Ansatz sind in $\mathfrak{m}$ und $\mathfrak{M}'$ alle Primfaktoren der Relativdiskriminante *von* K (also mehr) aufgenommen. Die überschüssigen sind nach Konstruktion von $\mathfrak{M}'$ Ideale aus k und fallen im Sinne des Satzes 50 für den Körper K' in den willkürlichen, im letzten Satz von Satz 50 genannten Faktor aus k. Das hier gewählte, noch hinzutretende $\mathfrak{a}$ ist in Hinsicht auf die Allgemeingültigkeit dieses letzten Satzes auch für den Körper K, und somit Fortsetzbarkeit der induktiven

178 IV

Schlußweise auf K übergeordnete Körper aufgenommen und notwendig).

Wir geben nun einen entsprechenden Modul $\mathfrak{M}$ für den Körper K an, der alle gestellten Anforderungen befriedigt, und zwar in der Form:

$$\mathfrak{M} = \prod \mathfrak{P} \cdot \prod \mathfrak{L}^U \cdot \mathfrak{a}.$$

Dabei bestimmen wir die Exponenten U so:

1.) Geht $\mathfrak{L}'$ nicht in der Relativdiskriminante von K nach K' auf, so sei für alle Teiler $\mathfrak{L}$ von $\mathfrak{L}'$ in K:

$$U = U'.$$

2.) Geht $\mathfrak{L}'$ in der Relativdiskriminante von K nach K' auf, also zu einer Potenz $L'^{(v+1)(\ell-1)}$, so dürfen wir infolge der Willkürlichkeit eines Zusatzfaktors aus k zu den Moduln $\mathfrak{m}, \mathfrak{M}'$ unbeschadet aller genannten

Behauptungen über diese (a. S. 176▸,177▸) die Exponenten u, U' von vorneherein so hoch gewählt annehmen, daß für alle solche $\mathfrak{L}'$ gilt:

$$U' > v.$$

Wir setzen dann

$$U' = v + b; \qquad (b \geqq 1)$$

und nehmen*)

$$U = v + b\ell.$$

Bezeichnen wir dann mit Π_1, Π_2 die Produkte über alle Primteiler der betr. Art die in der Relativdiskriminante von K nach K' aufgehen, bezw. nicht aufgehen, so wird der auf Grund von Satz 22

179 IV

für K' als Grundkörper, K als Oberkörper dem Modul

$$\mathfrak{M}' = \Pi_1\mathfrak{P}' \cdot \Pi_1\mathfrak{L}'^{v+b} \cdot \Pi_2\mathfrak{P}' \cdot \Pi_2\mathfrak{L}'^{U'} \cdot \mathfrak{a}$$

zugeordnete Modul in K:

$$\Pi_1\mathfrak{P} \cdot \Pi_1\mathfrak{L}^{v+b\ell} \cdot \Pi_2\mathfrak{P}' \cdot \Pi_2\mathfrak{L}'^{U'} \cdot \mathfrak{a},$$

also da $\Pi_2\mathfrak{P}' = \Pi_2\mathfrak{P}$, $\Pi_2\mathfrak{L}'^{U'} = \Pi_2\mathfrak{L}^{U'}$ ist, weil diese $\mathfrak{P}', \mathfrak{L}'$ nur erste Potenzen von $\mathfrak{P}, \mathfrak{L}$ enthalten, gleich

$$\prod \mathfrak{P} \cdot \prod\nolimits_1 \mathfrak{L}^U \cdot \prod\nolimits_2 \mathfrak{L}^U\mathfrak{a} = \prod \mathfrak{P} \cdot \prod \mathfrak{L}^U \cdot \mathfrak{a} = \mathfrak{M}.$$

Der angegebene Modul $\mathfrak{M}$ steht also zu $\mathfrak{M}'$ genau in der Beziehung, die die Anwendung des Satzes 22 auf K' und K erlaubt.

Erklären wir also die Idealklassen in K nach dem Strahl:

$$O \ : \ \mathsf{A} \equiv 1 \bmod \mathfrak{M}; \qquad (\text{für } \ell = 2 \text{ total positiv}),$$

so gilt folgendes (s.a. Satz 21, 21a, S. 59▸, 62▸):

1.) K ist Klassenkörper zu K' für eine Klassengruppe H'_0, die nach dem Strahl O' erklärbar ist.

*)Den kleinsten Wert der Exponenten $U, \overline{u}$ kann man sukzessive leicht berechnen, weil für $\nu = 1$ nach Satz 22 die Minimalwerte bekannt sind.

2.) $\mathfrak{M}$ ist Teiler von $\mathfrak{M}'$ (klar nach Konstruktion von $\mathfrak{M}$), konjugierte und Relativnormen von Klassen in K nach K' sind eindeutig erklärbar.

3.) Jede Klasse von K, deren Relativnorm die Hauptklasse von K' ist, ist symbolische $(1-\sigma^{\ell^{\nu-1}})$ te Potenz einer Klasse von K. (s. S. 176 oben).

Durch Kombination dieser Tatsachen „für K nach K'“ mit den obigen, nach Annahme richtigen „für K' nach k“

180 IV

ergeben sich nun leicht die behaupteten Tatsachen „für K nach k“:*)

1.) *K ist Klassenkörper zu k für eine Klassengruppe* H *nach o vom Index* ℓ^ν.

Die Klassengruppe H'_0 der Relativnormklassen von K nach K' ist invariant gegenüber der Substitution σ, denn einerseits sind die Moduln $\mathfrak{M}$ und $\mathfrak{M}'$ nach Konstruktion invariant gegen σ ($\mathfrak{M}'$ ist invariant gegen die erzeugende Substitution σ von K' nach Annahme, $\mathfrak{M}$ nach Konstruktion aus $\mathfrak{M}'$ gegen die erzeugende Substitution $\sigma^{\ell^{\nu-1}}$ von K nach K', also wegen der Invarianz von $\mathfrak{M}'$ gegen σ ebenfalls invariant gegen alle Substitutionen). Daher geht jede Klasse nach O oder O' durch σ in eine bestimmte andere Klasse nach O oder O' über. Andererseits folgt aus:

$$C' = n(C) = C^{1+\sigma^{\ell^{\nu-1}}+\cdots+\sigma^{(\ell-1)\ell^{\nu-1}}}$$

daß
$$\sigma C' = n(\sigma C) = C^{\sigma+\sigma\cdot\sigma^{\ell^{\nu-1}}+\cdots+\sigma\cdot\sigma^{(\ell-1)\ell^{\nu-1}}}$$

ist, also wenn C', dann auch $\sigma C'$ zu H'_0 gehört.

Es sei nun C' eine nicht in H'_0 enthaltene Klasse von K', dann ist auch $\sigma C'$ nicht in H'_0 $(=\sigma\mathsf{H}'_0)$ enthalten, also jedenfalls in einer Nebengruppe:

$$C'^a\mathsf{H}'_0,$$

wobei $a = 1, 2, \ldots, \ell-1$ genommen werden darf, da H'_0 als K zugeordnete Klassengruppe in K' nach 1.) S. 179 den Index ℓ hat. Daraus folgt weiter:

181 IV

$$\begin{array}{ccc} \sigma^2 C' & \text{zu} & (\sigma C')^a\mathsf{H}'_0 = C'^{a^2}\mathsf{H}'_0 \\ \cdots\cdots & \cdots & \cdots\cdots \\ \sigma^{\ell^{\nu-1}}C' & \text{zu} & \sigma C'^{a^{\ell^{\nu-1}}}\mathsf{H}'_0. \end{array}$$

*) Es ist besser erst den Punkt 2.) S. 183 zu erledigen, da er für 1.) gebraucht wird.

Da aber C' in K' liegt, ist $\sigma^{\ell^{\nu-1}} C' = C'$, also

$$C'^{a^{\ell^{\nu-1}}} \mathsf{H}'_0 = C' \mathsf{H}'_0,$$

d.h.

$$C'^{a^{\ell^{\nu-1}}-1} \quad \text{zu} \quad \mathsf{H}'_0,$$

also

$$a^{\ell^{\nu-1}} \equiv 1 \mod \ell.$$

Da aber a prim zu ℓ und mithin $a^{\ell-1} \equiv 1 \bmod \ell$ ist, folgt $a \equiv 1 \bmod \ell$, also $a = 1$, d.h.

$$\sigma C' \quad \text{zu} \quad C' \mathsf{H}'_0$$

oder

$$C'^{1-\sigma} \quad \text{zu} \quad \mathsf{H}'_0.$$

Da nach Annahme über „K' nach k“ die Klassen $C'^{1-\sigma}$ von K' mit den Klassen des Hauptgeschlechtes in K' identisch sind, gehört mithin jede Klasse des Hauptgeschlechtes in K' zu H'_0.

Sei nun H diejenige Klassengruppe in k, die aus den Relativnormen der Klassen von H'_0 besteht, so ist H Untergruppe der Klassengruppe H' vom Index $\ell^{\nu-1}$ in k, für die K' Klassenkörper ist, da letztere *alle* Relativnormklassen aus K' enthält. Ich zeige dann, daß H in Bezug auf H' denselben Index ℓ hat, wie H'_0 in Bezug auf die Gruppe aller Klassen von K' (anschaulich also, daß durch die Relativnormbildung aus K' nach k der Index ℓ erhalten bleibt) (Geometrische Verdeutlichung!!).

182 IV

Ist nämlich

$$\mathsf{H}'_0 + C' \mathsf{H}'_0 + \cdots + C'^{\ell-1} \mathsf{H}'_0$$

die volle Klassengruppe von K', so ist zunächst

$$C = n(C'); \qquad (\text{Norm von } K' \text{ nach } k)$$

nicht in H enthalten; denn sonst folgte

$$C = n(C') = n(C'_0), \quad \text{wo} \quad C'_0 \quad \text{zu} \quad \mathsf{H}'_0$$

also

$$n(C' C_0'^{-1}) = 1, \text{ (Hauptklasse)}.$$

Es gehörte also $C' C_0'^{-1}$ zum Hauptgeschlecht in K', d.h. nach dem Bewiesenen zu H'_0, also auch C' entgegen der Annahme von C'.

Ferner ist aber C^ℓ sicher in H enthalten, wenn C eine beliebige Klasse aus H' ist. Denn dann ist

$$C = n(\overline{C}'); \qquad \text{(weil } C \text{ zu } \mathsf{H}')$$

also

$$C^\ell = n(\overline{C}'^\ell)$$

und $\overline{C}'^\ell$ gehört sicher zu H'_0.

Somit ist tatsächlich

$$\begin{aligned}\mathsf{H}' &= n(\mathsf{H}'_0 + C'\mathsf{H}'_0 + \cdots + C'^{\ell-1}\mathsf{H}'_0)\\ &= \mathsf{H} + C\mathsf{H} + \cdots + C^{\ell-1}\mathsf{H}\end{aligned}$$

vom Index ℓ zu H. Also hat H in Bezug auf die Gruppe aller Klassen von k den Index ℓ^ν.

H enthält auf dem Umweg über H'_0 alle Relativnormklassen von K nach k. Da diese eine Klassengruppe vom Index $\leqq \ell^\nu$ bilden müssen, weil ℓ^ν der Grad von K ist, ist H selbst die K zugeordnete Klassengruppe, und K Klassenkörper für H.

183 IV

2.) der Nachweis der weiteren Behauptungen des Satzes „für K nach k“, daß $\mathfrak{M}$ Teiler von $\mathfrak{m}$, daß konjugierte und Relativnormen von Klassen eindeutig erklärbar, ist im vorhergehenden teilweise schon erbracht oder vorausgesetzt.

Natürlich ist $\mathfrak{M}$ Teiler von $\mathfrak{m}$, da nach 2.) S. 179 Teiler von $\mathfrak{M}$ und $\mathfrak{M}'$ nach S. 177 als Teiler von $\mathfrak{m}$ gewählt angenommen werden dürfte.

Daß die konjugierten zu Klassen nach O eindeutig erklärbar sind, wurde a. S. 180 gezeigt.

Dorthin gehörte eigentlich auch der durch folgende einfache Bemerkung zu erbringende Nachweis, daß die Relativnormen der Klassen nach O eindeutig erklärbar sind. Es ist nämlich nach Satz 22 die Relativnorm nach K' einer Zahl aus O Zahl aus O', ferner nach Annahme $\mathfrak{m}$ und $\mathfrak{M}'$ so gewählt, daß die Relativnormen von K' nach k der Zahlen aus O' Zahlen aus o sind. Somit sind auch die Relativnormen der Zahlen aus O von K nach k Zahlen aus o.

3.) Es fehlt also nur noch der für die Fortsetzung des Induktionsverfahrens notwendige Nachweis, daß *jede Klasse des Hauptgeschlechts in K die $(1-\sigma)$ te Potenz einer Klasse in K* ist.

Dazu denken wir uns die Gruppe G aller Idealklassen nach o durch eine Basis dargestellt. Da K Klassenkörper zur Untergruppe H von G ist, ist die Faktorgruppe $\frac{G}{\mathsf{H}}$ nach Hauptsatz I zyklisch vom Grade

184 IV

ℓ^ν. Ist also C eine nicht in H enthaltene Basisklasse für G, so gehört erst C^{ℓ^ν} zu H, da sonst noch eine andere, nicht zu H gehörige Basisklasse existieren müßte, und dann $\frac{G}{\mathsf{H}}$ nicht zyklisch wäre.

Denkt man sich die Basis aus Elementen mit Primzahlpotenzordnung bestehend gewählt, so muß C zu einem Exponenten ℓ^μ gehören, da sonst schon C zu H gehörig sein müßte. Stellt man also G als direktes Produkt des ℓ^μ gliedrigen Zyklus von C mit der Gruppe D der übrigen Basiselemente in der Form dar:

$$G = (C; \mathsf{D}),$$

so ist

$$\mathsf{H} = (C^{\ell^\nu}; \mathsf{D})$$

und die obige Gruppe H' offenbar

$$\mathsf{H}' = (C^{\ell^{\nu-1}}; \mathsf{D}),$$

da H' Untergruppe von G vom Index $\ell^{\nu-1}$ und zyklischer Faktorgruppe ist, also die gleiche Betrachtung auch für H' durchgeführt werden kann. Da H Untergruppe von H' ist, muß tatsächlich eine nicht in H' enthaltene Basisklasse C auch nicht zu H gehören, sodaß C für beide Gruppen dasselbe sein muß.

Sei nun D' die Gruppe der Klassen von K', deren Relativnormen in D fallen. Wie schon früher, sei unter C *in* K' die durch C in K' erzeugte Klasse verstanden. Ist dann C' irgendeine Klasse von K',

185 IV

so liegt $n(C')$ in H', also kann

$$n(C') = C^{a\ell^{\nu-1}}[\mathsf{D}]$$

und

$$C' = C^a U'$$

gesetzt werden, sodaß wegen $n(C) = C^{\ell^{\nu-1}}$ folgt:

$$n(U') = [\mathsf{D}],$$

also $$U' = [\mathsf{D}'].$$

Es kann somit stets

$$C' = C^a[\mathsf{D}']$$

gesetzt werden.

Aus $$C^a[\mathsf{D}'] = 1$$

folgt $$C^{a\ell^{\nu-1}}[\mathsf{D}] = 1,$$

also $$C^{a\ell^{\nu-1}} = 1$$

wegen der Unabhängigkeit von C von der Gruppe D. Die Ordnung von C in Bezug auf D' in K' ist also der $\ell^{\nu-1}$–te Teil der Ordnung ℓ^μ von C in k, und mit dieser Ordnung in der Basisdarstellung ist

$$G' = (C; \mathsf{D}')$$

die Gruppe aller Klassen aus K'.

Nun sei C_0 eine Klasse aus K, deren Relativnorm nach k die Hauptklasse ist (Klasse des Hauptgeschlechts in K). Bezeichnet N die Relativnorm von K nach K', so ist dann:

$$\mathsf{N}(C_0) = C'^{1-\sigma},$$

weil $\mathsf{N}(C_0)$ in K' zum Hauptgeschlecht gehört.

186 IV

C' sei im obigen Sinne als

$$C' = C^a[\mathsf{D}']$$

dargestellt. Die Relativnorm von $[\mathsf{D}']$ nach k ist ein $[\mathsf{D}]$, also Klasse aus H, folglich nach Definition von H eine Relativnorm aus H'_0. Folglich unterscheidet sich $[\mathsf{D}']$ von einer Klasse aus H'_0 nur um eine Klasse des Hauptgeschlechtes in K', die nach S. 181 sicher zu H'_0 gehört. Es ist somit $[\mathsf{D}']$ selbst Klasse □□□ aus H'_0 und somit Relativnorm einer Klasse D_0 aus K:

$$[\mathsf{D}'] = \mathsf{N}(\mathsf{D}_0).$$

Daraus folgt:

$$C'^{1-\sigma} = \mathsf{N}(\mathsf{D}_0^{1-\sigma}),$$

weil $\sigma C = C$; also weiter:

$$\mathsf{N}(C_0) = \mathsf{N}(\mathsf{D}_0^{1-\sigma}),$$

also

$$\mathsf{N}\left(\frac{C_0}{\mathsf{D}_0^{1-\sigma}}\right) = 1,$$

und somit $\dfrac{C_0}{\mathsf{D}_0^{1-\sigma}}$ Klasse des Hauptgeschlechtes von K in Bezug auf K', also nach S. 179, 3.):

$$\frac{C_0}{\mathsf{D}_0^{1-\sigma}} = \mathsf{B}_0^{1-\sigma^{\ell^{\nu-1}}},$$

wo B_0 eine Klasse aus K ist, und weiter

$$C_0 = (\mathsf{D}_0\mathsf{B}_0^{1+\sigma+\cdots+\sigma^{\ell^{\nu-1}-1}})^{1-\sigma}, \qquad \text{w.z.b.w.}$$

Damit ist Satz 50 vollständig bewiesen. Für $\mathfrak{a} = 1$ folgt die Richtigkeit von Hauptsatz II für relativ–zyklische Körper von Primzahlpotenzgrad und damit seine Allgemeingültigkeit.

187 IV

Auf Grund der vorstehenden Entwicklungen beweise ich noch folgenden Satz:

Satz 51. Ist K relativ–Abelsch über k und Klassenkörper für die Klassengruppe H in k, so ist der Führer f von H ein Teiler der Relativdiskriminante $\mathfrak{D}$ von K nach k.

Beweis. Denkt man sich K wieder, wie beim Beginn des Beweises von Hauptsatz II S. 170 ff aus den s^2 zyklischen Körpern K_i vom Primzahlpotenzgrad $\ell_i^{\nu_i}$ komponiert, deren Relativdiskriminanten $\mathfrak{D}_i$ seien, sind ferner die K_i Klassenkörper für die Klassengruppen H_i mit den Führern f_i in k, und ist der Satz für relativ–zyklische Körper von Primzahlpotenzgrad schon bewiesen, also jedes f_i ein Teiler des zugehörigen $\mathfrak{D}_i$, so ist nach S. 173 K Klassenkörper für den Durchschnitt

$$\mathsf{H} = (\mathsf{H}_1, \ldots, \mathsf{H}_s).$$

Der Führer f von H ist sicher Teiler des kleinsten gemeinsamen Vielfachen

$$\overline{f} = [f_1, \ldots, f_s],$$

da alle H_i, also H sicher nach $\overline{f}$ erklärbar sind.

Andererseits ist die Relativdiskriminante $\mathfrak{D}$ sicher ein Multiplum des kleinsten gemeinsamen Vielfachen

$$\overline{\mathfrak{D}} = [\mathfrak{D}_1, \ldots, \mathfrak{D}_s],$$

da $\mathfrak{D}$ sicher durch jedes $\mathfrak{D}_i$ teilbar ist. Nun ist wegen $f_i|\mathfrak{D}_i$ sicher $\overline{f}|\overline{\mathfrak{D}}$ (elementar!), also auch $f|\mathfrak{D}$, w.z.b.w.

188 IV

Es bleibt also der Satz nur noch für einen relativ–zyklischen Körper K vom Primzahlpotenzgrad ℓ^ν zu beweisen. Hierzu ist es erforderlich, einen hinreichend niedrigen Modul $\mathfrak{m}$ anzugeben, nach dem die K zugeordnete Klassengruppe H in k erklärbar ist, für den also Satz 50 richtig ist. Dazu sind zunächst die Zerlegungsvorgänge in den in K steckenden, relativ–zyklischen Unterkörpern zu betrachten. Sei

$$k = K_0\{K_1\{K_2 \ \ldots \ \{K_\nu = K$$

die ineinandergeschachtelten Körperreihe, also K_i relativ–zyklisch vom Grade ℓ^i über k, ℓ über K_{i-1} und K relativ–zyklisch vom Grade $\ell^{\nu-i}$ über K_i. Sei ferner K_τ der Trägheitskörper für einen in der Relativdiskriminante von K nach k aufgehenden Primteiler $\mathfrak{l}$ von $\mathfrak{L}$, also $0 \leqq \tau < \nu$. Dann gilt in K_τ:

$$\mathfrak{l} = \mathfrak{L}_{\tau 1} \ldots \mathfrak{L}_{\tau \ell^z}; \qquad (\text{Grad } \ell^{\tau - z})$$

wenn K_z $(0 \leqq z \leqq \tau)$ der Zerlegungskörper für $\mathfrak{l}$ ist. Von K_τ ab tritt in jedem folgenden Körper eine ℓ–fache Verzweigung der $\mathfrak{L}_{\tau j}$ ein, bis schließlich in $K_\nu = K$ wird:

$$\mathfrak{L}_{\tau j} = \mathfrak{L}_j^{\ell^{\nu-\tau}}.$$

Ich bezeichne nun mit $\mathfrak{m}_i, \mathfrak{M}_i$ ein auf den Körper K_i bezügliches Modulpaar im Sinne von Satz 50, und zwar nur die auf den Primteiler $\mathfrak{l}$ bezüglichen Teile dieser Moduln.

189 IV

Da $\mathfrak{l}$ in der Relativdiskriminante von K_τ noch nicht aufgeht, genügt es für K_τ zu wählen:

$$\mathfrak{m}_\tau = 1; \qquad \mathfrak{M}_\tau = 1.$$

Für die weiteren Körper seien $v_{\tau+1}, \dots, v_\nu$ die charakteristischen Zahlen im Sinne von Satz 3 (S. 10▸), es gehen also die $\mathfrak{L}_{\tau+i-1,j}$ aus $K_{\tau+i-1}$ in der Relativdiskriminante von $K_{\tau+i}$ zur Potenz $\mathfrak{L}_{\tau+i-1,j}^{(v_{\tau+i}+1)(\ell-1)}$ auf. Für K_τ als Grundkörper gilt dann nach Satz 3:

$$1 \leqq v_{\tau+1} < v_{\tau+2} < \cdots < v_\nu \leqq \frac{e\ell^{\nu-\tau}}{\ell-1},$$

wenn e die Ordnung der $\mathfrak{L}_{\tau,j}$, d.h. die Ordnung von $\mathfrak{l}$ bezeichnet, und es ist die Relativdiskriminante von K nach K_τ:

$$\prod_j \mathfrak{D}_{\mathfrak{L}_{\tau,j}} = \prod_j \mathfrak{L}_{\tau,j}^{(\ell^{\nu-\tau}-1)+(\ell-1)\left[v_{\tau+1}\ell^{\nu-\tau-1}+v_{\tau+2}\ell^{\nu-\tau-2}+\cdots+v_\nu\right]}$$

also die Relativdiskriminante von K nach k (d.h. stets der auf $\mathfrak{l}$ bezügliche Teil):

$$\begin{aligned}\mathfrak{D}_{\mathfrak{l}} = n_{K_\tau k}(\mathfrak{D}_{\mathfrak{L}_{\tau,j}}) &= \prod_{j=1}^{\ell^z} \mathfrak{l}^{\ell^{\tau-z}\left\{(\ell^{\nu-\tau}-1)+(\ell-1)\left[v_{\tau+1}\ell^{\nu-\tau-1}+\cdots+v_\nu\right]\right\}} \\ &= \mathfrak{l}^{\ell^\tau\left\{(\ell^{\nu-\tau}-1)+(\ell-1)\left[v_{\tau+1}\ell^{\nu-\tau-1}+\cdots+v_\nu\right]\right\}}.\end{aligned}$$

Ein passendes Modulpaar $\mathfrak{m}_{\tau+1}, \mathfrak{M}_{\tau+1}$ ergibt sich nach S. 178▸ so: Die $\mathfrak{L}_{\tau j}$ gehen in der Relativdiskriminante von $K_{\tau+1}$ nach K_τ[1] zur Potenz $\mathfrak{L}_{\tau j}^{(v_{\tau+1}+1)(\ell-1)}$ auf. Es müssen also $\mathfrak{m}_\tau$ und $\mathfrak{M}_\tau$ zunächst durch Faktoren aus k so erweitert

190 IV

werden, daß die Potenz von $\mathfrak{L}_{\tau j}$ in $\mathfrak{M}_\tau$ mindestens $\mathfrak{L}_{\tau j}^{v_{\tau+1}+1}$ wird, was durch:

$$\mathfrak{m}'_\tau = \mathfrak{l}^{v_{\tau+1}+1}; \qquad \mathfrak{M}'_\tau = \prod_j \mathfrak{L}_{\tau j}^{v_{\tau+1}+1}$$

erreicht wird. Daraus ergibt sich nach S. 178▸:

$$\mathfrak{m}_{\tau+1} = \mathfrak{l}^{v_{\tau+1}+1}; \qquad \mathfrak{M}_{\tau+1} = \prod_j \mathfrak{L}_{\tau+1,j}^{v_{\tau+1}+\ell}$$

als geeignetes Modulpaar für $K_{\tau+1}$.

[1] undeutlich

Weiter ist jetzt die Relativdiskriminante von $K_{\tau+2}$ nach $K_{\tau+1}$, durch $\mathfrak{L}_{\tau+1,j}^{(v_{\tau+2}+1)(\ell-1)}$ teilbar, und es müssen $\mathfrak{m}_{\tau+1}$ und $\mathfrak{M}_{\tau+1}$ durch Faktoren aus k so erweitert werden, daß die Potenz von $\mathfrak{L}_{\tau+1,j}$ in $\mathfrak{M}_{\tau+1}$ mindestens $\mathfrak{L}_{\tau+1,j}^{v_{\tau+2}+1}$ wird. Wegen $v_{\tau+2} > v_{\tau+1}$ wird dies sicher durch

$$\mathfrak{m}'_{\tau+1} = \mathfrak{l}^{v_{\tau+2}+1}; \qquad \mathfrak{M}'_{\tau+1} = \prod_j \mathfrak{L}_{\tau+1,j}^{(v_{\tau+1}+\ell)+\ell(v_{\tau+2}-v_{\tau+1})}$$

erreicht, indem in beiden der Faktor aus k:

$$\mathfrak{l}^{v_{\tau+2}-v_{\tau+1}} = \prod_j \mathfrak{L}_{\tau+1,j}^{\ell(v_{\tau+2}-v_{\tau+1})}$$

hinzugefügt wird. Damit wird nach S. 178▸:

$$\mathfrak{m}_{\tau+2} = \mathfrak{l}^{v_{\tau+2}+1}; \qquad \mathfrak{M}_{\tau+2} = \prod_j \mathfrak{L}_{\tau+2,j}^{v_{\tau+2}+\ell(\ell-1)(v_{\tau+2}-v_{\tau+1})+\ell^2}.$$

So fortfahrend erhält man durch weitere Hinzufügung der Faktoren aus k:

$$\mathfrak{l}^{v_{\tau+3}-v_{\tau+2}} = \prod_j \mathfrak{L}_{\tau+2,j}^{\ell^2(v_{\tau+3}-v_{\tau+2})},$$

191 IV

$$\begin{aligned} \mathfrak{l}^{v_{\tau+4}-v_{\tau+3}} &= \textstyle\prod_j \mathfrak{L}_{\tau+3,j}^{\ell^3(v_{\tau+4}-v_{\tau+3})}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{l}^{v_\nu-v_{\nu-1}} &= \textstyle\prod_j \mathfrak{L}_{\nu-1,j}^{\ell^{\nu-1}(v_\nu-v_{\nu-1})} \end{aligned}$$

nach leichter Rechnung das Modulpaar:

$$\mathfrak{m}_\nu = \mathfrak{l}^{v_\nu+1}$$

$$\mathfrak{M}_\nu = \prod_j \mathfrak{L}_{\nu j}^{v_\nu+\ell(\ell^{\nu-\tau-1}-1)(v_\nu-v_{\nu-1})+\ell^2(\ell^{\nu-\tau-2}-1)(v_{\nu-1}-v_{\nu-2})+\cdots}$$

$$\cdots+\ell^{\nu-\tau-1}(\ell-1)(v_{\tau+2}-v_{\tau+1})+\ell^{\nu-\tau}$$

Der Wert $\mathfrak{M}_\nu$ interessiert uns nicht weiter. Der Wert für $\mathfrak{m}_\nu$, mit dem man auskommt, läßt auf Grund der Formel für $\mathfrak{D}_\mathfrak{l}$ auf S. 189▸ ohne weiteres

erkennen, daß $\mathfrak{m}_\nu = \mathfrak{l}^{v_\nu+1}$ in $\mathfrak{D}_\mathfrak{l}$ aufgeht, denn $\mathfrak{D}_\mathfrak{l}$ enthält ja, weil alles übrige im Exponenten positiv ist, sicher die Potenz $\mathfrak{l}^{\ell^\tau(\ell-1)v_\nu}$, und es ist offenbar

$$\ell^\tau(\ell-1)v_\nu \geqq (\ell-1)v_\nu \geqq v_\nu.$$

Da aber der vernachlässigte Term $\ell^{\nu-\tau}-1$ im Exponenten von $\mathfrak{D}_\mathfrak{l}$ wegen $\tau < \nu$ mindestens 1 ist, ist der Exponent von $\mathfrak{D}_\mathfrak{l}$ mindestens $v_\nu + 1$, was ausreicht.

Da diese Betrachtung für alle in ℓ aufgehenden Teiler $\mathfrak{l}$ der Relativdiskriminante $\mathfrak{D}$ von K nach k gilt, ferner die zu ℓ primen Teiler von $\mathfrak{D}$ nach Satz 50 nur zur ersten Potenz in $\mathfrak{m}$ aufgenommen zu werden brauchen, kann der vollständige Modul $\mathfrak{m}$ so gewählt werden, daß er in $\mathfrak{D}$ aufgeht, sodaß also der Führer f von H als Teiler von $\mathfrak{m}$ sicher ebenfalls ein Teiler von $\mathfrak{D}$ ist, w.z.b.w.

4.6 §6 Zerlegung der Primideale in relativ–abelschen Körpern

192 IV

§6. Die Zerlegung der Primideale in relativ Abelschen Körpern.

Der Hauptsatz II ermöglicht es, die Zerlegungsgesetze für die Primideale eines beliebigen Grundkörpers k in einem relativ–Abelschen Oberkörper K vollständig aufzustellen. Ich beweise zunächst einen Hilfssatz:

Hilfssatz. Seien die Idealklassen in k nach dem Strahl

$$\alpha \equiv 1 \bmod \mathfrak{m} \qquad \text{(total positiv)}$$

erklärt, und $\mathfrak{p}$ ein zu $\mathfrak{m}$ primes Primideal aus der Klasse C. Ist dann für irgendeine Primzahl ℓ die Klasse C die ℓ–te Potenz einer Klasse, so gibt es ein Primideal $\mathfrak{q} \neq \mathfrak{p}$, sodaß für die entsprechende Klassendefinition mod $\mathfrak{m}\mathfrak{q}$ $\mathfrak{p}$ in einer Klasse liegt, die nicht ℓ–te Potenz einer Klasse ist.

Beweis. Nach Annahme gibt es ein zu $\mathfrak{m}$ primes $\mathfrak{j}$, sodaß

$$\mathfrak{p}\mathfrak{j}^{\ell} = (\alpha); \qquad \alpha \equiv 1 \bmod \mathfrak{m}, \quad \text{tot. pos.}$$

ist. Es mögen nun unter $\mathfrak{r}_i, \varrho_i, \varepsilon_i$ wieder die zum Existenzbeweis des Klassenkörpers (S. 97 ff.) eingeführten Größen sein, wobei die $\mathfrak{r}_i$ prim zu $\mathfrak{p}$ gewählt seien. Wir betrachten dann die Zahlen

$$\beta = \alpha^{a}\varepsilon_1^{u_1} \dots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \dots \varrho_t^{v_t}; \qquad (a, u_i, v_i = 0, 1, \dots, \ell - 1) \tag{1}$$

Ferner adjungieren wir dem Körper k die ℓ–te Einheitswurzel

193 IV

ζ, und untersuchen, wann eine Zahl β der Form (1) ℓ–te Potenz einer Zahl A aus $k(\zeta)$ wird. $k(\zeta)$ habe den Grad n über k, wo also $n \mid \ell - 1$ prim zu ℓ ist. Aus

$$\mathsf{A}^{\ell} = \beta$$

folgt durch Übergang zur Relativnorm nach k:

$$\gamma^\ell = n(\mathsf{A})^\ell = \beta^n,$$

wo γ eine Zahl aus k ist. Daraus folgt zunächst, weil der Exponent von $\mathfrak{p}$ in β^n durch ℓ teilbar sein muß, daß $an \equiv 0 \bmod \ell$, also $a = 0$ ist, und dann weiter nach S. 99▸, daß alle u_i und v_i Null sind.

Auf Grund von Satz 40, S. 126▸ gibt es also in $k(\zeta)$ ein zu $\mathfrak{m}, \mathfrak{j}, \mathfrak{p}, \ell$ und den $\mathfrak{r}_i$ primes Ideal $\mathfrak{Q}$, sodaß in $k(\zeta)$ gilt:

$$\left(\frac{\alpha}{\mathfrak{Q}}\right) \neq 1; \qquad \left(\frac{\varepsilon_i}{\mathfrak{Q}}\right) = 1; \qquad \left(\frac{\varrho_i}{\mathfrak{Q}}\right) = 1. \tag{2}$$

$\mathfrak{q}$ sei das durch $\mathfrak{Q}$ teilbare Primideal von k, das wir dann ebenfalls noch zu $\mathfrak{m}, \mathfrak{j}, \mathfrak{p}, \ell$ und den $\mathfrak{r}_i$ prim annehmen dürfen, da nur endlich viele $\mathfrak{Q}$ nicht zu einem solchen $\mathfrak{q}$ führen.

Wäre nun in k

$$x^\ell \equiv \alpha \mod \mathfrak{q}$$

lösbar, dann erst recht in $k(\zeta)$. Also ist α Nichtrest mod $\mathfrak{q}$. Da nach Satz 40 $\mathfrak{Q}$ auch noch vom ersten Grade angenommen werden darf, ist jede Zahl aus $k(\zeta)$ mod $\mathfrak{Q}$

einer Zahl aus k kongruent. Wenn also

$$(\varepsilon, \varrho) \equiv \mathsf{A}^\ell \mod \mathfrak{Q}$$

ist, wo (ε, ϱ) eine Zahl der Form $\varepsilon_1^{u_1} \dots \varepsilon_{r+\delta}^{u_{r+\delta}} \varrho_1^{v_1} \dots \varrho_t^{v_t}$ ist und A Zahl aus $k(\zeta)$, was nach Bestimmung von $\mathfrak{Q}$ in (2) stets lösbar ist, so folgt aus

$$(\varepsilon, \varrho) \equiv \xi^\ell \bmod \mathfrak{Q}, \quad \text{also mod } \mathfrak{q},$$

wenn $\mathsf{A} \equiv \xi \bmod \mathfrak{Q}$, wo ξ aus k.

Es ist also α Nichtrest, jeder Ausdruck (ε, ϱ) dagegen Rest mod $\mathfrak{q}$.

Wir setzen nun $\overline{\mathfrak{m}} = \mathfrak{m}\mathfrak{q}$ und definieren die Idealklassen in k nach dem Strahl $\equiv 1 \bmod \overline{\mathfrak{m}}$ (tot. positiv). $\mathfrak{p}$ liege in $\overline{C}$. Wäre $\overline{C}$ ℓ–te Potenz einer Klasse nach $\overline{\mathfrak{m}}$, so gäbe es ein zu $\overline{\mathfrak{m}}$ primes $\mathfrak{a}$, sodaß

$$\mathfrak{p}\mathfrak{a}^\ell = (\overline{\alpha}); \qquad \overline{\alpha} \equiv 1 \bmod \overline{\mathfrak{m}} \quad \text{(total positiv)}$$

wäre. Dann folgte

$$(\alpha) = \mathfrak{p}\mathfrak{j}^\ell = (\overline{\alpha})\left(\frac{\mathfrak{j}}{\mathfrak{a}}\right)^\ell,$$

es wäre also $\left(\frac{\mathfrak{j}}{\mathfrak{a}}\right)^\ell$ ein (absolutes) Hauptideal (β), welches ℓ–te Idealpotenz ist. Wie a. S. 102▶/103▶ folgt daraus

$$(\beta) = \left(\frac{\mathfrak{j}}{\mathfrak{a}}\right)^\ell = (\varrho_1^{v_1} \dots \varrho_t^{v_t} \xi^\ell); \qquad (v_i = 0, 1, \dots, \ell - 1)$$

d.h.
$$\frac{\alpha}{\overline{\alpha}} = \beta = (\varepsilon, \varrho)\xi^\ell$$

also
$$\alpha = \overline{\alpha}(\varepsilon, \varrho)\xi^\ell,$$

wo ξ prim zu $\mathfrak{q}$ ist, weil es α und $\overline{\alpha}$, sowie die $\mathfrak{r}_i$ sind. Wegen $\overline{\alpha} \equiv 1 \bmod \mathfrak{q}$ wäre also α ein

195 IV

ℓ–ter Potenzrest mod $\mathfrak{q}$ entgegen dem Gezeigten. Daher kann nicht $\overline{C}$ ℓ–te Potenz einer Klasse nach $\overline{\mathfrak{m}}$ sein, w.z.b.w.

Wir beweisen nun zunächst den wichtigsten Teil des Zerlegungsgesetzes für relativ–zyklische Körper von Primzahlpotenzgrad, aus dem dann alles weitere leicht folgt.

Satz 52. Ist K relativ–zyklisch vom Primzahlpotenzgrad ℓ^ν über k und Klassenkörper für die Klassengruppe H in k, so zerfällt ein nicht in der Relativdiskriminante von K aufgehendes Primideal $\mathfrak{p}$ von k dann und nur dann in K in ℓ^ν verschiedene Primideale ersten Relativgrades, wenn $\mathfrak{p}$ in H enthalten ist.

Beweis. 1.) Sei $\mathfrak{p}$ ein in ℓ^ν verschiedene Primteiler ersten Relativgrades zerfallendes Primideal aus k, so ist es Relativnorm jedes seiner Primteiler in K. Da $\mathfrak{p}$ nach Satz 49 prim zum Führer von H ist, kommt es also in der Klassengruppe H vor, welche ja Relativnormen aus K enthält.

2.) Sei $\mathfrak{p}$ ein zur Relativdiskriminante primes Primideal aus H (und H natürlich nach einem zu $\mathfrak{p}$ primen Modul erklärt, was nach Satz 49 möglich). Wir dürfen nach dem eben bewiesenen Hilfssatz ferner den Modul $\mathfrak{m}$, nach dem wir die Idealklassen und die

196 IV

Klassengruppe H erklären, so annehmen, daß die Klasse C von $\mathfrak{p}$ nicht ℓ–te Potenz einer Klasse ist.

Dann hat die Klassengruppe

$$C^i\mathfrak{K}^\ell; \qquad (i = 0, 1, \ldots \ell - 1),$$

wo $\mathfrak{K}$ alle Klassen durchläuft, den Rang 1. Nach Satz 25, S. 90 gibt es also eine „Rangbasis“ für die Gruppe G aller Idealklassen, die C als Basiselement enthält. Läßt man in dieser Basisdarstellung von G das Element C aus, so erhält man eine Klassengruppe H' vom Index ℓ, welche C nicht enthält, sondern erst C^ℓ, also:

$$G = \mathsf{H}' + C\mathsf{H}' + \cdots + C^{\ell-1}\mathsf{H}'.$$

Andererseits ist $\frac{G}{\mathsf{H}}$ zyklisch vom Grade ℓ^ν, also

$$G = \mathsf{H} + \mathsf{A}\mathsf{H} + \cdots + \mathsf{A}^{\ell^\nu - 1}\mathsf{H}.$$

Sei dann $\mathsf{H}_0 = (\mathsf{H}, \mathsf{H}')$ der Durchschnitt von H und H'. Weil $\mathsf{H} \cdot \mathsf{H}' = G$, da C in H enthalten, folgt durch genau dieselbe, rein gruppentheoretische Überlegung, wie a. S. 171/172, daß H_0 in Bezug auf G den Index $\ell^{\nu+1}$ hat und $\mathsf{H} = \sum_{i=0}^{\ell-1} C^i\mathsf{H}_0$ ist, weil C in H aber nicht H_0 vorkommt.

□□□

□□□

Sei dann K' der Klassenkörper für H', also relativ–zyklisch vom Grade ℓ über k. K' kann nicht Unterkörper von K sein, weil sonst H Untergruppe von H' wäre, und dann $\mathsf{H}_0 = \mathsf{H}$ vom Index ℓ^ν zu G wäre. Also muß K' teilerfremd zu K (relativ zu k) sein, weil ja K' Primzahlgrad hat. Somit hat der komponierte Körper KK' den Relativgrad $\ell^{\nu+1}$ über k; die Relativnormen seiner Ideale fallen nach Satz 47, S. 167 in H_0, also ist nach der schon oft benutzten Schlußweise KK' der Klassenkörper zu H_0.

Nach Hauptsatz II ist es möglich, den Modul $\mathfrak{m}$ durch Hinzunahme von Teilern der Relativdiskriminante von KK' so zu erweitern, daß auch jeder Unterkörper von KK' über k Klassenkörper für eine Klassengruppe mod $\mathfrak{m}$ ist, denn die etwa in Frage kommenden Teiler der Relativdiskriminanten

jener Unterkörper gehen ja sämtlich in der Relativdiskriminante von KK' auf. Hierbei darf der entstehende Modul $\mathfrak{m}$ ebenfalls noch prim zu $\mathfrak{p}$ angenommen werden, weil $\mathfrak{p}$ ja in dem bisherigen Modul $\mathfrak{m}$, nachdem H_0 erklärt war, also im Führer von H_0 nicht aufgeht, und somit nach Satz 49 auch nicht in der Relativdiskriminante von KK'.

198 IV

Da K und K' teilerfremd sind, ist die Galoissche Gruppe $\mathfrak{G}$ von KK' das direkte Produkt der Gruppen

$$\begin{aligned} \mathfrak{g} &= \sigma^a\,; \quad (a = 0, 1, \ldots, \ell^\nu - 1) \\ \mathfrak{g}' &= \sigma'^b\,; \quad (b = 0, 1, \ldots, \ell - 1) \end{aligned}$$

von K und K', also in der Form darstellbar

$$\mathfrak{G} = \sigma^a \sigma'^b; \quad \left\{ \begin{array}{l} a = 0, 1, \ldots, \ell^\nu - 1 \\ b = 0, 1, \ldots, \ell - 1 \end{array} \right\}.$$

(s. S. 169▶). Dann gehört K als Unterkörper von KK' zur Untergruppe $\mathfrak{g}'$.

Da $\mathfrak{p}$ nicht in der Relativdiskriminante von KK' aufgeht, ist die Trägheitsgruppe für $\mathfrak{p}$ die Einheitsgruppe, die Zerlegungsgruppe $\mathfrak{G}_Z$ also zyklisch. Sei K_Z der Zerlegungskörper für $\mathfrak{p}$ in KK' und Klassenkörper für die Klassengruppe H_Z, die also nach Wahl von $\mathfrak{m}$ auch mod $\mathfrak{m}$ erklärbar ist und die Gruppe H_0 enthalten muß. Dann muß H_Z die Klasse C enthalten, weil $\mathfrak{p}$ in K_Z in verschiedene Primideale 1. Grades zerfällt, also Relativnorm aus K_Z ist. Daher ist die ganze Gruppe $\mathsf{H} = \sum_{i=0}^{\ell-1} C^i \mathsf{H}_0$ in $\mathsf{H_Z}$ enthalten, also K_Z Unterkörper von K.

K_Z gehört also zu einer Gruppe $\mathfrak{G}_Z$, die $\mathfrak{g}'$ enthält, also, wenn ℓ^μ der Relativgrad von K_Z nach K, d.h. der Index von $\mathfrak{G}_Z$ nach $\mathfrak{g}'$ ist,

$$\mathfrak{G}_Z = \left(\sigma^{\ell^{\nu-\mu}}\right)^a \mathfrak{g}'; \qquad (a = 0, 1, \ldots, \ell^\mu - 1)$$

sein muß. Da aber $\mathfrak{G}_Z$ zyklisch ist, muß $\mu = 0$, d.h.

199 IV

$K_Z = K$ sein. $\mathfrak{p}$ zerfällt also in K in verschiedene Primideale ersten Relativgrades, und zwar natürlich in ℓ^ν.

Aus dem damit bewiesenen Satz 52 folgt sofort der entsprechende Satz für beliebige relativ–Abelsche Körper:

Satz 53. Sei K ein beliebiger relativ–Abelscher Körper über k und Klassenkörper für die Klassengruppe H in k. Dann zerfällt ein nicht in der Relativdiskriminante von K aufgehendes Primideal $\mathfrak{p}$ von k dann und nur dann in K in lauter verschiedene Primideale ersten Relativgrades, wenn $\mathfrak{p}$ in H enthalten ist.

Beweis. 1.) Zerfällt $\mathfrak{p}$ in dieser Weise, so ist es Relativnorm seiner Primteiler in K, also in H enthalten, da der Führer f von H prim zu $\mathfrak{p}$ ist.

2.) Sei $\mathfrak{p}$ in H enthalten, G die Gruppe aller Klassen von k (nach dem Führer f von H definiert) und $\mathsf{H}_1, \ldots, \mathsf{H}_s$ die aus der Basisdarstellung von $\frac{G}{\mathsf{H}}$ wie beim Beweis des Hauptsatzes I, S. 168 gewonnenen Klassengruppen, $K_1, \ldots, K_s$ die ihnen zugeordneten Klassenkörper, also

$$K = (K_1, \ldots, K_s)$$

der komponierte Körper und

$$\mathsf{H} = (\mathsf{H}_1, \ldots, \mathsf{H}_s)$$

der Gruppendurchschnitt. Nach Annahme ist $\mathfrak{p}$ in allen H_i

200 IV

enthalten, (und natürlich prim zu den Relativdiskriminanten der K_i, da es sogar zu der von K prim sein soll). Daher zerfällt nach Satz 52 $\mathfrak{p}$ in jedem K_i in verschiedene Primideale ersten Relativgrades.

□□□

Nach A.Z. I, Satz 23, S. 51 ist also der Zerlegungskörper K_Z für $\mathfrak{p}$ Oberkörper aller K_i, somit $K_Z = K$ und alles bewiesen.

Nunmehr können wir sehr leicht das allgemeine Zerlegungsgesetz für die zur Relativdiskriminante primen Primideale in einem relativ–Abelschen Oberkörper angeben:

Hauptsatz III. Sei K relativ Abelsch zu k, und Klassenkörper für die Klassengruppe H in k vom Führer f. Die Idealklassen in k seien nach H definiert und h ihre Anzahl, also auch der Grad von K. Ist dann C eine zum Exponenten $\mathfrak{f}$ gehörige Klasse und $h = e\mathfrak{f}$, so zerfällt jedes

201 IV

in C enthaltene Primideal von k in K in e verschiedene Primteiler vom Relativgrade $\mathfrak{f}$.

Beweis. Für $C = \mathsf{H}$, also die Hauptklasse ist der Satz identisch mit Satz 53. Es werden ferner infolge der Definition der Klassen nach *dem Führer f von* H tatsächlich alle und nur die zur Relativdiskriminante primen Primideale von dem angegebenen Zerlegungsgesetz betroffen (Satz 49).

Sei nun $\mathfrak{p}$ in irgendeiner Klasse C enthalten, K_Z der Zerlegungskörper für $\mathfrak{p}$ in K und K_Z Klassenkörper für die Klassengruppe H_Z. Die Moduln, nach denen H und H_Z definiert sind, können wie a. S. 197▸ identisch und zu $\mathfrak{p}$ prim angenommen werden. Da $\mathfrak{p}$ in K_Z in verschiedene Primideale ersten Relativgrades zerfällt, ist $\mathfrak{p}$ in H_Z enthalten, und da andererseits K_Z Unterkörper von K ist, muß H_Z die Gruppe H enthalten; es ist somit die ganze Klasse nach H von $\mathfrak{p}$, nämlich $[\ldots] = \mathfrak{p}\mathsf{H}$ in H_Z enthalten, und daher auch die Gruppe:

$$\mathsf{H}' = \mathsf{H} + C\mathsf{H} + \cdots + C^{\mathfrak{f}-1}\mathsf{H}.$$

K_Z ist also Unterkörper des zu H' gehörigen Klassenkörpers K'. Da $\mathfrak{p}$ in H' enthalten, zerfällt $\mathfrak{p}$ in K' in verschiedene Primideale ersten Relativgrades (Satz 53), sodaß nach Satz 23, S. 51▸ von A.Z. I der Körper K' Unterkörper von K_Z, also $K' = K_Z$, somit $\mathsf{H}' = \mathsf{H}_Z$ sein muß. Daher hat H_Z den Index e, also K_Z den Grad e.

Nun bestimmen sich □□□ Grad und Index der Zerlegungsgruppe als Relativgrad K nach K_Z und Relativgrad K_Z nach k. Letzterer ist e, also ersterer $\frac{h}{e} = \mathfrak{f}$. Die Zerlegungsgruppe hat also den Grad $\mathfrak{f}$. Da $\mathfrak{p}$ kein Teiler der Relativdiskriminante, ist die Trägheitsgruppe die identische, folglich ist ihr Index zur Zerlegungsgruppe, der den Grad der Primteiler von $\mathfrak{p}$ in K angibt, gleich dem Grade $\mathfrak{f}$ der Zerlegungsgruppe. $\mathfrak{p}$ zerfällt somit in e Primteiler $\mathfrak{f}$–ten Grades, w.z.b.w.

4.7 §7 Weitere Sätze über Klassenkörper

203 IV

§7. Weitere Sätze über den Klassenkörper.

Man kann, wie *Weber* es getan hat, den Klassenkörper auch auf eine etwas verschiedene Art von der unsrigen (*Takagi*schen) charakterisieren, indem man von dem in Satz 53 erhaltenen Zerlegungsgesetz ausgeht*), und daraus die von Takagi zur Definition benutzte Übereinstimmung des Relativgrades mit dem Index der zugeordneten Klassengruppe folgert. Für den Existenzbeweis, der Weber auf seine Art nicht gelang, ist der Takagische Ausgangspunkt besser, jedoch ist die Webersche Auffassung zweckmäßig für die Anwendung in der komplexen Multiplikation. Es soll daher jetzt nachträglich ein Satz aufgestellt werden, der mittels der Takagischen Ergebnisse das Webersche Resultat abrundet.

Wir beweisen zunächst einen Hilfssatz, der zeigt, daß in den Weberschen Forderungen für den Klassenkörper die Forderung „relativ–Galoissch“ enthalten ist:

Hilfssatz. Sei K ein Körper über k und $\mathfrak{p}_1$ jedes Primideal ersten Grades von k, das in K mindestens einen Primfaktor ersten Grades hat. Wenn dann „fast alle“ $\mathfrak{p}_1$ in K in *lauter* Primideale ersten Grades zerfallen, ist K relativ–Galoissch zu k.

204 IV

Beweis. Es ist

$$\zeta_K(s) = \prod_{\mathfrak{P}_1} \frac{1}{1 - N_K \mathfrak{P}_1^{-s}} \cdot \prod_{\mathfrak{P}}{}' \frac{1}{1 - N_K \mathfrak{P}^{-s}},$$

wo $\mathfrak{P}_1$ alle Primideale ersten Grades von K, $\mathfrak{P}$ in $\prod'$ alle übrigen Primideale von K durchläuft, und N_K die Norm in K ist. Das Produkt $\prod'$ läßt sich

*) das mit dem vollständigen Zerlegungsgesetz von Hauptsatz III im Wesentlichen identisch ist, da letzteres leicht aus dem ersteren folgt, wenn man die Klassenkörpersätze hat.

durch Entwicklung seiner Faktoren in geometrische Reihen leicht unter eine absolute Majorante bringen, die für $s = 1$ regulär ist, d.h. bleibt endlich für $s \to 1$ und ist dort von 0 verschieden; also ist

$$\zeta_K(s) = \prod_{\mathfrak{P}_1} \frac{1}{1 - N_K \mathfrak{P}_1^{-s}} \cdot \varphi(s)$$

und nach Annahme:

$$\zeta_K(s) = \prod_{\mathfrak{P}_1} \frac{1}{(1 - N\mathfrak{p}_1^{-s})^n} \cdot \psi(s),$$

wo $\psi(s)$ endlich und $\neq 0$ für $s \to 1$ und n den Relativgrad von K bezeichnet. Also ist

$$\lim(s-1)^{\frac{1}{n}} \prod_{\mathfrak{p}_1} \frac{1}{1 - N\mathfrak{p}_1^{-s}}$$

endlich und $\neq 0$ für $s \to 1$.

Die Primideale $\mathfrak{p}_1$ erfüllen dieselbe Voraussetzung für jeden zu K relativ–konjugierten Körper, somit auch für den aus allen konjugierten K zusammengesetzten Galoisschen Körper $\overline{K}$. Denn zerfällt $\mathfrak{p}_1$ in K, also allen konjugierten in lauter verschiedene Primideale ersten Grades, so ist der Grad der Zerlegungsgruppe $\mathfrak{G}_Z$ eines

205 IV

Primteilers $\overline{\mathfrak{P}}$ von $\mathfrak{p}_1$ in $\overline{K}$ gleich dem Grade $\mathfrak{f}$ von $\overline{\mathfrak{P}}$ (da $\overline{\mathfrak{P}}$ kein Teiler der Relativdiskriminante), der Grad der Zerlegungsgruppe $\mathfrak{H}_Z$ von $\overline{\mathfrak{P}}$ in Bezug auf K gleich dem Relativgrade von $\overline{\mathfrak{P}}$ in Bezug auf K; letzterer ist aber sicher ebenfalls $\mathfrak{f}$, da alle Primteiler von $\mathfrak{p}_1$ in K vom ersten Grade sind. Aus

$$\mathfrak{H}_Z = (\mathfrak{H}, \mathfrak{G}_Z),$$

wo $\mathfrak{H}$ zu K gehört, folgt also wie üblich

$$\mathfrak{G}_Z/\mathfrak{H},$$

d.h. K_Z ist Oberkörper von K und ebenso von allen konjugierten, also $K_Z = \overline{K}$, sodaß $\mathfrak{p}_1$ in $\overline{K}$ in lauter verschiedene Primideale 1. Grades zerfällt.

Da umgekehrt jedes in $\overline{K}$ „vollständig“ zerfallende $\mathfrak{p}_1$ auch in allen konjugierten K vollständig zerfällt, sind bis auf endliche viele Ausnahmen die

$\mathfrak{p}_1$ die Gesamtheit derjenigen Primteiler, die in $\overline{K}$ einen und somit lauter Primfaktoren 1. Grades haben, sodaß wie oben

$$\lim(s-1)^{\frac{1}{\overline{n}}} \prod_{\mathfrak{p}_1} \frac{1}{1 - N\mathfrak{p}_1^{-s}}$$

für $s \to 1$ endlich, $\neq 0$ ist, wo $\overline{n}$ der Relativgrad von $\overline{K}$ nach k ist. Es muß also $\overline{n} = n$ und daher $\overline{K} = K$ sein, sodaß K selbst relativ–Galoissch ist, w.z.b.w.

Wir betrachten nun mit Weber einen Relativkörper K über k mit folgenden Eigenschaften:

206 IV

Es sei H eine Klassengruppe vom Führer f in k. Dann soll:

1.) Jedes zu f prime Primideal ersten Grades $\mathfrak{p}_1$ aus H in K in lauter Primideale ersten Grades zerfallen,

2.) Jedes zu f prime Primideal ersten Grades aus k, das in K einen Primteiler ersten Grades hat, in H enthalten sein.

Von 1.), 2.) dürfen endlich viele Ausnahmen zugelassen sein.

Einen Körper K dieser Eigenschaften nennt Weber (Alg. III, S. 607) Klassenkörper zu H und beweist:

a.) Der Relativgrad n von K ist nie kleiner als der Index h von H:

$$n \geqq h.$$

b.) Es kann nur einen solchen Körper K geben.

c.) K ist relativ–Galoissch zu k.

d.) $n = h$.

Die Behauptung c.) folgt unmittelbar aus 1.), 2.) vermöge des Hilfssatzes, ist also implicite, unabhängig von der Klasseneinteilung mod f in den Forderungen 1.), 2.) enthalten.

Ferner ergibt sich leicht, daß

I.) K Klassenkörper zu H in Takagischem Sinne ist.

II.) der Takagische Klassenkörper zu H die Eigenschaften 1.), 2.) hat.

207 IV

II.) ist selbstverständlich auf Grund von Satz 53 vermöge der Voraussetzungen 1.) und 2.). Damit ist also die von Weber offengelassene Existenzfrage auf Grund des Takagischen Existenzbeweises gelöst, und zwar schon nach dem Weberschen Resultat b.) in eindeutigem Sinne, gleichzeitig c.) zu „relativ Abelsch“ präzisiert, und d.) bewiesen.

Um uns aber unabhängig von dem Weberschen Nachweis b.) zu machen, beweisen wir die Eindeutigkeit dadurch, daß wir I.) beweisen und uns auf unseren Eindeutigkeitssatz stützen.

Sei also K' der Takagische Klassenkörper zu H vom Relativgrade h. $\mathfrak{p}_1$ durchlaufe alle Primideale ersten Grades aus H. Dann ist (A.Z. II, S. 140▸, Satz 4/5)

$$\sum_{\mathfrak{p}_1} \frac{1}{N\mathfrak{p}_1^s} = \frac{1}{h} \log \frac{1}{s-1} + \varphi(s)$$

wo $\varphi(s)$ unterhalb einer endlichen Schranke bleibt für $s \to 1$. Da aber andererseits die $\mathfrak{p}_1$ die Gesamtheit der in K' in Primideale 1. Grades zerfallenden Primideale 1. Grades von k ausmachen (Satz 53) folgt nach A.Z. II, S. 141▸, Satz 6:

$$\sum_{\mathfrak{p}_1} \frac{1}{N\mathfrak{p}_1^s} = \frac{1}{h} \log \frac{1}{s-1} + \psi(s),$$

wo $\psi(s)$ endlich für $s \to 1$. Es gilt somit in dem zitierten Satz 4, 5 von A.Z. II für jede Klassengruppe H in k, daß die dort mit $\varphi(s)$ bezeichnete Funktion *sogar endlich bleibt, wenn* $s \to 1$.*)

208 IV

Da nun nach 1.) und 2.) die $\mathfrak{p}_1$ bis auf endlich viele Ausnahmen auch die im Körper K in Primideale 1. Grades zerfallenden Primideale 1. Grades von

*) Hieraus ist sofort auf das Nichtverschwinden der L–Reihen nach H in k und somit auf den Satz von der arithmetischen Progression in k zu schließen. Wir werden es jedoch später etwas anders erschließen.

k ausmachen, muß nach A.Z. II, Satz 6, S. 141 auch

$$\sum_{\mathfrak{p}_1} \frac{1}{N\mathfrak{p}_1^s} = \frac{1}{n} \log \frac{1}{s-1} + \psi(s)$$

sein, wo n der Grad von K ist und $\psi(s)$ endlich für $s \to 1$. Mit dem vorigen zusammen folgt also:

$$n = h,$$

d.h. die Webersche Vermutung d.).

Betrachten wir dann den komponierten Körper KK', so muß nach demselben Schluß, wie S. 204/205 bis auf endlich viele Ausnahmen jedes $\mathfrak{p}_1$ auch in KK' in verschiedene Primideale 1. Grades zerfallen und umgekehrt jedes $\mathfrak{p}_1$ dieser Eigenschaft es auch in K tun, also zu H gehören, sodaß auch

$$\sum_{\mathfrak{p}_1} \frac{1}{N\mathfrak{p}_1^s} = \frac{1}{m} \log \frac{1}{s-1} + \psi(s)$$

ist, wo $\psi(s)$ endlich für $s \to 1$ und m der Grad von KK'. Es ist also $m = h$, was nur für $K = K'$ möglich. Damit ist I.) bewiesen.

Wir haben also folgenden Satz:

Satz 54. Der Klassenkörper K für die Klassengruppe H in k ist auch durch folgende beiden Forderungen eindeutig bestimmt:

1.) Die Primideale ersten Grades von k aus H zerfallen in K in lauter Primideale ersten Grades.

2.) Jedes Primideal ersten Grades aus k, welches in K einen Primfaktor ersten Grades enthält, (und somit nach d. Hilfssatz lauter solche), liegt in H.

Von 1.) und 2.) sind endlich viele Ausnahmen zugelassen und natürlich nur die zum Führer f von H primen Primideale in Betracht zu ziehen.

Aus Satz 54 folgt weiter der folgende Satz, der anzeigt, daß für einen relativ–Galoisschen aber nicht relativ–Abelschen Körper K sich die Primideale ersten

Grades aus k, die in K in verschiedene Primideale ersten Grades zerfallen, sich nicht in eine Kongruenzklassengruppe H so einschließen lassen, daß von endlich vielen Ausnahmen abgesehen, alle Primideale 1. Grades aus H in K angegebener Weise zerfallen, daß also m.a.W. sich jene Primideale nicht durch ihre Zugehörigkeit zu einer Kongruenzklassengruppe (speziell etwa für den rationalen Körper durch irgendwelche Kongruenzbedingungen) *charakterisieren* lassen. Es gilt nämlich:

Satz 55. Ist K relativ Galoissch zu k und zerfallen alle und nur die in einer Kongruenzklassengruppe H enthaltenen Primideale (mit endlich vielen Ausnahmen) ersten Grades in K wieder in Primideale ersten Grades, so ist K relativ Abelsch zu k (nämlich Klassenkörper zu H).

Der Beweis folgt unmittelbar aus Satz 54. —

Die Zerlegungsgesetze für nicht–Abelsche Relativkörper sind also notwendig von einem komplizierteren Bau, als die durch einfache Kongruenzbedingungen bestimmte für Abelsche.

Zum Schluß sei noch die folgende Möglichkeit hervorgehoben, den Klassenkörper zu charakterisieren.

Satz 56. Der Relativkörper K ist Klassenkörper für die Klassengruppe H vom Index h in k, wenn (bis auf endliche viele Ausnahmen bei 3.)

1.) K relativ Galoissch,

2.) der Relativgrad $n \leqq h$,

3.) jedes in Primideale 1. Grades zerfallende Primideal 1. Grades aus k in H enthalten ist.

Es fehlt also die Voraussetzung 1.) von Satz 54 und ist durch 1.) 2.) ersetzt. — Nachträglich folgt dann natürlich $n = h$.

Beweis. In K seien die Idealklassen nach dem Führer f von H erklärt ($\equiv 1 \bmod f$, total positiv). Dann liegen die Relativnormen der Ideale einer Klasse von K offenbar in einer Klasse nach f von k, da aus

$$\mathsf{A} \equiv 1 \mod f \qquad \text{(total positiv)}.$$

folgt

$$n(\mathsf{A}) \equiv 1 \bmod f \qquad \text{(total positiv)}.$$

Ist $\mathfrak{A}$ ein Ideal aus K, so gibt es nach dem später zu beweisenden Satz von der arithmetischen Progression in der Klasse von $\mathfrak{A}$ ein Primideal $\mathfrak{P}$ vom ersten Grade, sodaß $n(\mathfrak{P}) = \mathfrak{p}$ Primideal ersten Grades in k ist, das in K nach 1.) in lauter Primideale ersten Grades zerfällt. Nach 3.) kann (unbeschadet der endlich vielen Ausnahmen) $\mathfrak{P}$ auch so gewählt werden, daß $n(\mathfrak{P}) = \mathfrak{p}$ in H liegt. Also liegt auch das äquivalente $n(\mathfrak{A})$ in H, sodaß alle Relativnormen von Idealen (zu f primen) aus K in H liegen. K ist also einer Untergruppe von H zugeordnet, also $n \geqq h$. Aus 2.) folgt also $n = h$, also unsere Behauptung.

Teil II

Anhang

Kapitel 5

Verzeichnisse

5.1 Namenverzeichnis

5.2 Stichwortverzeichnis