Vortragsmanuskripte
von Helmut Hasse

$^{t\,k}$ Vorträge von **1923 – 26 – 28 – 29 – 30 – 31 – 32 – 33 – 38 – 53 – 55 – 63**

t – fertig transkribiert, k – nach Tippfehlern durchgesehen

Version vom 25.09.11
Letztmalig geändert am 27.09.11

Quelltext: hasvtr_111110.tex
übersetzt am 14. März 2015

Inhaltsverzeichnis

2 Register **313**

Vorbemerkung

`[...]` steht als Platzhalter für Text, der nicht oder nicht eindeutig zu entziffern war. [1]
□□□ steht für durchgestrichene, aber lesbare Passagen. [2]
ſ steht für ein spezielles Zeichen, das von Hasse an mehreren Stellen verwendet wird; es handelt sich um den kleinen Buchstaben ℓ in deutscher Schrift und bezeichnet in der Regel ein verzweigtes Primideal. [3]

1. erreichbar mit `\xxx`
2. erreichbar mit `\boxes`
3. erreichbar mit `\y`

Kapitel 1

Die Vorträge von Hasse

1.1 Marburg 1923

Vortrag, Marburg, September 1923.

k beliebiger algebraischer Körper, der ℓ-te E.W. ζ enthält (für $\ell = 2$ ganz beliebig). Ferner sei in k:

$$\ell = \mathfrak{l}_1^{e_1} \dots \mathfrak{l}_z^{e_z}.$$

Alle Reziprozitätsbeziehungen für die ℓ-ten Potenzreste in k lassen sich nach Hilbert in die eine Formel

$$\prod_{\mathfrak{w}} \left(\frac{\alpha, \beta}{\mathfrak{w}}\right) = 1; \qquad (\alpha, \beta \text{ beliebige Zahlen aus } k)$$

zusammenfassen. Darin bedeutet $\mathfrak{w}$ alle Primteiler des Körpers k, für $\ell = 2$ einschl. der Primstellen $\mathfrak{p}_\infty$ für die reellen zu k konjugierten, $\left(\frac{\alpha,\beta}{\mathfrak{w}}\right)$ *Normenrestsymbol.*

Aus dieser Formel entstehen *allgemeines Reziprozitätsgesetz, erster u. zweiter Ergänzungssatz*, wenn für α, β spezielle Werte eingesetzt werden. Die zu ℓ primen $\mathfrak{p}$ liefern die *Legendre-Jacobischen Symbole*, die übrigen $\mathfrak{l}$ und $\mathfrak{p}_\infty$ schafft man dann durch *Vertauschungssatz* nach rechts.

Allgem. Rez.gesetz

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{l}} \left(\frac{\beta, \alpha}{\mathfrak{l}}\right) \cdot \prod_{\mathfrak{p}_\infty} \left(\frac{\beta, \alpha}{\mathfrak{p}_\infty}\right);$$

α, β prim zu einander und zu ℓ

erster Ergänzungssatz

$$\left(\frac{\varepsilon}{\alpha}\right) = \prod_{\mathfrak{l}} \left(\frac{\alpha, \varepsilon}{\mathfrak{l}}\right) \cdot \prod_{\mathfrak{p}_\infty} \left(\frac{\alpha, \varepsilon}{\mathfrak{p}_\infty}\right);$$

α prim zu ℓ, $\varepsilon = \mathfrak{a}^\ell$ prim zu α (speziell Einheit)

zweiter Ergänzungssatz

$$\left(\frac{\lambda}{\alpha}\right) = \prod_{\mathfrak{l}} \left(\frac{\alpha, \lambda}{\mathfrak{l}}\right) \cdot \prod_{\mathfrak{p}_\infty} \left(\frac{\alpha, \lambda}{\mathfrak{p}_\infty}\right);$$

α prim zu ℓ, $\lambda = \prod \mathfrak{l}_i^{a_i} \mathfrak{a}^\ell$ prim zu α (also eine durch Primteiler von ℓ teilbare Zahl).

Man beherrscht diese 3 Gesetze erst dann, wenn man die rechten Seiten *explizit* kennt. Für [1] die $\mathfrak{p}_\infty$-Symbole ist das nicht schwer. Sie sind nach ihrer Definition falls $\ell = 2$:

$$\prod_{\mathfrak{p}_\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}_\infty}\right) = (-1)^{\sum_i \frac{\operatorname{sgn}\alpha^{(i)}-1}{2}\cdot\frac{\operatorname{sgn}\beta^{(i)}-1}{2}}; \qquad \textit{Vorzeichencharaktere}$$

Ohne Beschränkung sei einfachheitshalber: *Für* $\ell = 2$: α *total positiv*, sodaß die $\mathfrak{p}_\infty$-Symbole identisch 1 sind.

Dann kommt es also nur auf die *Normenrestsymbole nach den* $\mathfrak{l}_i$ an.

Abgesehen von Spezialfällen (rat. Grdk., Kreiskörper, *Eisenstein*) beherrschte man diese Symbole bisher nur insofern, als man *Bedingungen für* α angeben kann, unter denen sie identisch 1 sind. Hierzu *Begriffe primär, hyperprimär.*

Sei $\mathfrak{l}_0$ Primteiler $(1-\zeta) = (\lambda_0)$ des Kreiskörpers k_ζ (für $\ell = 2$: $\mathfrak{l}_0 = 2$).

$$\left.\begin{array}{rll} \alpha \textit{ primär}, & \text{wenn} & \alpha \equiv \xi^\ell \bmod \ell\mathfrak{l}_0 \\ \alpha \textit{ hyperprimär}, & \text{wenn} & \alpha \equiv \xi^\ell \bmod \ell\mathfrak{l}_0\mathfrak{l}_1 \dots \mathfrak{l}_z \end{array}\right\} \begin{array}{l}\text{prim zu } \ell \\ \text{(u. für } \ell = 2 \text{ tot. positiv).}\end{array}$$

Dann gilt:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = 1, \quad \text{wenn } \alpha, \beta \text{ prim zu } \ell, \text{ zueinander und } \alpha \textit{ primär.}$$

$$\left(\frac{\varepsilon}{\alpha}\right) = 1, \quad \text{wenn } \alpha \textit{ primär}, \varepsilon = \mathfrak{a}^\ell \text{ prim zu } \alpha$$

$$\left(\frac{\lambda}{\alpha}\right) = 1, \quad \text{wenn } \alpha \textit{ hyperprimär}, \lambda = \prod_i \mathfrak{l}_i^{\alpha_i} \cdot \mathfrak{a}^\ell \text{ prim zu } \alpha$$

Es ist mir nun auf Grund der Henselschen Methoden gelungen, die Normenrestsymbole für die $[\ldots]$ in weiteren Fällen, wo sie nicht identisch 1 sind, in einfache Form zu setzen und folgende Gesetze zu beweisen, in denen α nicht mehr primär zu sein braucht:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\mathsf{S}\left(\frac{\alpha-1}{\ell}\cdot\frac{\beta-1}{\lambda_0}\right)}, \quad \text{wenn} \quad \left\{\begin{array}{l}\alpha \equiv 1 \bmod \ell \\ \beta \equiv 1 \bmod \lambda_0\end{array}\right\} \quad \text{und } (\alpha, \beta) = 1$$

$$\left(\frac{\zeta}{\alpha}\right) = \zeta^{\mathsf{S}\left(\frac{\alpha-1}{\ell}\right)}, \quad \text{wenn } \alpha \equiv 1 \bmod \ell$$

$$\left(\frac{\ell}{\alpha}\right) = \zeta^{\mathsf{S}\left(\frac{\alpha-1}{\ell\lambda_0}\right)}, \quad \text{wenn } \alpha \equiv 1 \bmod \ell\lambda_0$$

1. undeutlich

S = Spur in k. Die Ergänzungssätze sind nicht die allgemeinsten. Diese haben sehr verwickelten Typus. Der erste für beliebiges ε ist als im allgemeinen Gesetz enthalten anzusehen, der zweite läßt sich ähnlich auch noch für λ_0 statt ℓ aussprechen, jedoch für beliebige *unsymmetrische* Verbindungen der $\mathfrak{l}_i$ habe ich ihn noch nicht.

Ergänzungssätze in dieser Form geschrieben, wegen Analogie zum bekannten quadr. Rez. Ges. im rat. Körper:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}, \quad \text{wenn} \quad \left\{\begin{array}{l} a \equiv 1 \bmod 2 \\ b \equiv 1 \bmod 2 \end{array}\right\} \quad (a,b)=1,\ a \text{ pos.}$$

$$\left(\frac{-1}{a}\right) = (-1)^{\left(\frac{a-1}{2}\right)}, \quad \text{wenn } a \equiv 1 \bmod 2,\ a \text{ pos.}$$

$$\left(\frac{2}{a}\right) = (-1)^{\left(\frac{a-1}{4}\right)}, \quad \text{wenn } a \equiv 1 \bmod 4$$

(hier kann a pos. entbehrt werden, da 2 positiv ist).

Das allgemeine Gesetz ist auch als Verallgem. d. Eisensteinschen Rez. Ges. anzusehen.

1.) Die Bedingung $\equiv 1$ ist unwesentl. ebenso gut:

$$\equiv \textit{rat.} \text{ (zu } \ell \text{ primer Zahl).}$$

Dann muß das Gesetz geschrieben werden

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\mathsf{S}\left(\frac{\alpha^{\ell-1}-1}{\ell}\cdot\frac{\beta^{\ell-1}-1}{\lambda_0}\right)}$$

2.) Ist nun k der Kreiskörper und

$$\begin{aligned} \alpha &\equiv a \bmod \ell \\ \beta &\equiv b \bmod \lambda_0^2 \quad \text{(semiprimär)} \end{aligned}$$

so wird $\beta^{\ell-1} \equiv b^{\ell-1} \equiv 1 \bmod \lambda_0^2$, also $\frac{\beta^{\ell-1}-1}{\lambda_0}$ durch λ_0 teilbar, also Spur $\equiv 0\ (\ell)$, d.h.

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = 1 \qquad \text{wenn im Kreiskörper} \left\{\begin{array}{l} \alpha \equiv \text{rat. Zahl mod } \ell \\ \beta \equiv \text{rat. Zahl mod } \lambda_0^2 \end{array}\right\}$$

Das ist das bekannte *Eisensteinsche Reziprozitätsgesetz.*

Es entsteht natürlich die Frage, ob sich die *notwendigen Voraussetzungen* nicht noch weiter herabdrücken lassen, also die Moduln noch weiter verkleinern.

In dieser Richtung habe ich noch kein abschließendes Resultat. Den Ausgangspunkt für die Aufstellung einer ganz allgemeinen Formel findet man am zweckmäßigsten in der *Kummer*schen Formel *für den Kreiskörper* k_ζ.

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\sum_{k=1}^{\ell-1}(-1)^k \ell_k(\alpha)\ell_{(\ell-k)}(\beta)}$$

(α, β prim zu ℓ und zueinander und $\equiv 1 \bmod \lambda_0$). wo die $\ell_k(\alpha)$ die Kummerschen *logarithmischen Diff.Quot.* sind. Dies entsteht aus

$$\alpha = \alpha(\zeta)$$

als

$$\ell_k(\alpha) \equiv \frac{d^k \log \alpha(e^v)}{dv^k}\Big|_{k=0} \bmod \ell.$$

Ich habe zeigen können, daß man diese unerfreulichen Ausdrücke durch einfachere ersetzen kann, die zu ihrer Bildung nicht erst den formalen Differentiationsprozeß erfordern, sondern direkt angebbare *Spuren* von *Polynomen in* α sind.

Sei $\log \alpha = (\alpha-1) - \frac{(\alpha-1)^2}{2} + \frac{(\alpha-1)^3}{3} - \cdots$ für $\alpha \equiv 1 \bmod \lambda_0$ hinreichend weit fortgesetzt. Die Glieder werden schließlich durch jede noch so hohe Potenz von λ_0 teilbar, also hat

$$\mathsf{S}\log\alpha \quad \begin{cases} 1.) \text{ teilbar durch } \ell \\ 2.) \text{ ganz bestimmten Kongruenzwert mod } \ell. \end{cases}$$

Damit ist

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\sum_{\kappa=1}^{\ell-1} \kappa \cdot \frac{\mathsf{S}(\zeta^{-\kappa}\log\alpha)}{\ell} \cdot \frac{\mathsf{S}(\zeta^{\kappa}\log\beta)}{\ell} + \mathsf{S}\left(\frac{\alpha-1}{\lambda_0}\right)\frac{\mathsf{S}\log\beta}{\ell} - \mathsf{S}\left(\frac{\beta-1}{\lambda_0}\right)\mathsf{S}\left(\frac{\log\alpha}{\ell}\right)}$$

für $\alpha, \beta \equiv 1 \bmod \lambda_0$, prim zu ℓ und zueinander *im Kreiskörper*. Das ist *soweit heruntergedrückt, als möglich*. Höchstens noch $\alpha \equiv$ rat. Zahl mod λ_0, das aber leicht durch $\alpha^{\ell-1}$ zu erreichen. Letzten beiden Glieder treten nur für

$$\alpha, \beta \not\equiv \bmod \lambda_0^2$$

auf. Für *semiprimäre* α, β nur das erste Glied.

Nach einem allgemeinen Satz über Legendre Symbole im Ober- und Unterkörper folgt hieraus:

$$\left(\frac{\mathsf{A}}{\beta}\right)\left(\frac{\beta}{\mathsf{A}}\right)^{-1} = \zeta^{\sum_{\kappa=1}^{\ell-1}\kappa\cdot\frac{\mathsf{S}_k(\zeta^{-\kappa}\log \mathsf{A})}{\ell}\cdot\frac{\mathsf{S}_\zeta(\zeta^{\kappa}\log \beta)}{\ell}+\mathsf{S}_k\left(\frac{\mathsf{A}-1}{\lambda_0}\right)\frac{\mathsf{S}_\zeta \log\beta}{\ell}-\mathsf{S}\left(\frac{\beta-1}{\lambda_0}\right)\left(\frac{\mathsf{S}_k \log \mathsf{A}}{\ell}\right)}$$

für $\mathsf{A}, \beta \equiv 1 \bmod \lambda_0$ prim zu einander, β im Kreiskörper k_ζ.

Es fehlt also noch die entspr. Formel, wenn A, B *beide* im Oberkörper liegen, und auch nur nach niedrigeren Potenzen, als λ_0, $\equiv 1$ sind.

Den *ersten Ergänzungssatz* besonders zu führen, ist nicht notwendig, da er für $\beta = \ell$-te Idealpotenz im allgem. Gesetz unmittelbar enthalten ist.

Der *zweite Ergänzungssatz* läßt eine entsprechende Darstellung zu. *Mitteilungen von Artin*. Wieder erhält man zunächst den allgemeinsten zweiten Ergänzungssatz in k_ζ, der dort offenbar nur die beiden Symbole

$$\left(\frac{\ell}{\alpha}\right) \quad \text{und} \quad \left(\frac{\lambda_0}{\alpha}\right)$$

zu behandeln braucht:

$$\left(\frac{\ell}{\alpha}\right) = \zeta^{-\mathsf{S}\left(\frac{\log \alpha}{\lambda_0^\ell}\right)}; \quad \left(\frac{\lambda_0}{\alpha}\right) = \zeta^{-\mathsf{S}\left(\frac{\zeta \log \alpha}{\ell\lambda_0}\right)}$$

für $\alpha \equiv 1 \bmod \lambda_0$ im Kreiskörper.

Für beliebigen Grundkörper k wird dann, wenn ebenfalls λ auf die beiden Werte $\lambda = \lambda_0$, ℓ, *die schon im Kreiskörper liegen*, beschränkt wird

$$\left(\frac{\ell}{\mathsf{A}}\right) = \zeta^{-\mathsf{S}\left(\frac{\log \mathsf{A}}{\lambda_0^\ell}\right)}; \quad \left(\frac{\lambda_0}{\mathsf{A}}\right) = \zeta^{-\mathsf{S}\left(\frac{\zeta \log \mathsf{A}}{\ell\lambda_0}\right)}$$

für $\mathsf{A} \equiv 1 \bmod \lambda_\nu$.

Es fehlt also wieder eine entspr. Formel für

1.) beliebiges λ

2.) niedrigere Kongruenzbedingung für A.

1.2 Marburg 1926

Vortrag Marburg 26.XI.26.

Die Klassenkörper der komplexen Multiplikation.

I. Es sei k ein (endlicher) algebraischer Zahlkörper. Zweck der Klassenkörpertheorie ist, die *relativ-Abelschen* Zahlkörper K über k zu beherrschen. Das geschieht durch eineindeutige Zuordnung mit bestimmten Eigenschaften zu den *Idealgruppen H mod m in k.*

Idealgruppen H mod m in k.

k besitzt eine Anzahl *Primstellen*:

1.) die *endlichen Primstellen* $\mathfrak{p}$ *(Primideale).* Für diese ist im Bereich der $\alpha \neq 0$ aus k eine *genaue Teilbarkeit durch* $\mathfrak{p}^a$ erklärt. Ist $a = 0$, so heißt α *prim zu* $\mathfrak{p}$. Im Bereich der zu $\mathfrak{p}$ primen α, β ist ferner eine *Relation* $\alpha \equiv \beta \bmod \mathfrak{p}^a$ erklärt, (in der bekannten Weise: $\alpha - \beta$ hat positive Ordnungszahl für $\mathfrak{p}$). Das führt zu einer *primen Restklassengruppe mod* $\mathfrak{p}^a$ (Ordnung $N(\mathfrak{p})\big(N(\mathfrak{p}) - 1\big)$).

2.) die *unendlichen Primstellen* $\mathfrak{p}_\infty$, die den reellen konjugierten und den Paaren konjugiert-komplexer konjugierter zu k entsprechen. Für diese ist keine Teilbarkeit erklärt, wir rechnen jedes $\alpha \neq 0$ prim zu $\mathfrak{p}_\infty$, und es ist dann im Bereich der zu $\mathfrak{p}_\infty$ primen α, β eine *Relation* $\alpha \equiv \beta \bmod \mathfrak{p}_\infty$ erklärt, (durch die Festsetzung: $\operatorname{sgn}\alpha \equiv \operatorname{sgn}\beta$ für den $\mathfrak{p}_\infty$ entsprechenden Körper, wenn dieser reell; stets, wenn dieser komplex). Das führt zu einer *primen Restklassengruppe mod* $\mathfrak{p}_\infty$ (Ordnung 2 oder 1).

Es sei jetzt

$$\mathfrak{m} = \prod{}' \mathfrak{p}^a \prod{}' \mathfrak{p}_\infty \qquad (a > 0)$$

ein „endliches“ Produkt von Primstellenpotenzen (bei den $\mathfrak{p}_\infty$ stets 1. Potenz); dann reden wir von einem *Modul* $\mathfrak{m}$.

Es ist dann durch Zusammensetzung erklärt:

1.) α *prim zu* $\mathfrak{m}$ (α prim zu den $\mathfrak{p}^a$ und $\mathfrak{p}_\infty$)

2.) Im Bereich der zu $\mathfrak{m}$ primen α, β die *Relation* $\alpha \equiv \beta \bmod \mathfrak{m}$ ($\alpha \equiv \beta \bmod \mathfrak{p}^a$ und mod $\mathfrak{p}_\infty$)

3.) Die *prime Restklassengruppe mod* $\mathfrak{m}$ (Ordnung endlich) (direktes Produkt der gr. Restkl. Gr. mod $\mathfrak{p}^a$, mod $\mathfrak{p}_\infty$).

Wir betrachten nun den Bereich aller zu $\mathfrak{m}$ primen (endlichen) *Ideale* $\mathfrak{a}, \mathfrak{b}$ von k und erklären die Relation

$$\mathfrak{a} \sim \mathfrak{b} \bmod \mathfrak{m}$$

durch die Existenz einer Zahl α, sodaß

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \alpha \equiv 1 \bmod \mathfrak{m}$$

fortan also Gleichheit der *absoluten Idealklasse* von $\mathfrak{a}, \mathfrak{b}$ und überdies (falls $\mathfrak{m} \neq 1$) eine *Restklassenbedingung mod* $\mathfrak{m}$. Diese Relation führt zu einer Einteilung der zu $\mathfrak{m}$ primen Ideale in die *Strahlklassen mod* $\mathfrak{m}$ und zu der *Strahlklassengruppe* mod $\mathfrak{m}$, deren Ordnung endlich ist, weil die absolute Idealklassengruppe und die prime Restklassengruppe endliche Ordnung haben. (Nicht etwa das Produkt, weil hier „Ideale“, dort sogar „Zahlen“) [1].

Idealgruppe H mod $\mathfrak{m}$ heißt dann jede Gruppe von zu $\mathfrak{m}$ primen Idealen, die sich aus ganzen Strahlklassen mod $\mathfrak{m}$ zusammensetzt, oder was dasselbe, die die Idealgruppe $\mathfrak{a} \sim 1 \bmod \mathfrak{m}$, den sog. *Strahl mod* $\mathfrak{m}$ enthält.

Idealklassengruppe nach H heißt die Gruppe der Nebengruppen zu H in der Gruppe A aller zu $\mathfrak{m}$ primen Ideale (Faktorgruppe A/H). Wir schreiben dann auch

$$\mathfrak{a} \sim \mathfrak{b} \bmod H \quad \text{für } \frac{\mathfrak{a}}{\mathfrak{b}} \text{ in } H$$

also

$$\mathfrak{a} \sim 1 \bmod H \quad \text{für } a \text{ in } H$$

(Für den Strahl mod $\mathfrak{m}$ ist das mit $\mathfrak{a} \sim \mathfrak{b} \bmod \mathfrak{m}$, $\mathfrak{a} \sim 1 \bmod \mathfrak{m}$ identisch). Die Ordnung h der Idealklassengruppe nach H (Index von H, *Klassenzahl nach* H) ist natürlich endlich.

$\boldsymbol{(H \bmod \mathfrak{m}) = (H' \bmod \mathfrak{m}')}$, wenn ein Ideal $\mathfrak{m}_0$ existiert, sodaß die zu $\mathfrak{m}_0$ primen Ideale von H und H' übereinstimmen.

> *Beispiel*: k der rationale Körper, $m = 3p_\infty$. Dann ist der Strahl mod $3p_\infty$ die Gesamtheit der zu 3 primen Zahlen a mit
>
> $$a \equiv 1 \bmod 3p_\infty \qquad (\text{d.h. } \equiv 1 \bmod 3, > 0)$$
>
> und ihrer entgegengesetzten $-a$ (letzteres, weil nur Hauptideale genommen werden). Dieser ist gleich mit dem Strahl mod $2 \cdot 3 \cdot p_\infty$, weil $m_0 = 2$ gewählt werden kann.

Unter allen zu H mod $\mathfrak{m}$ gleichen

$$H \bmod \mathfrak{m},\ H' \bmod \mathfrak{m}',\ \ldots$$

1. Randvermerk

existiert ein ausgezeichnetes

$$H_0 \bmod f$$

derart, daß f der größte gemeinsame Teiler aller $\mathfrak{m}, \mathfrak{m}', \ldots$ ist und wenn $\mathfrak{m} = f\mathfrak{m}_0$ ist, so entsteht H aus H_0 einfach durch Weglassen der zu $\mathfrak{m}_0$ nicht primen Ideale aus H. Es gibt umgekehrt für jedes $\mathfrak{m}_0'$ ein $(H' \bmod \mathfrak{m}_0' f) = (H \bmod \mathfrak{m})$

f heißt der *Führer von* H.

Die Relation $(H_1 \bmod \mathfrak{m}_1) \leqq (H_2 \bmod \mathfrak{m}_2)$ wird durch Bestehen im gewöhnlichen Sinne für geeignete gleiche $H_1' \bmod \mathfrak{m}$, $H_2' \bmod \mathfrak{m}$ mit gleichem $\mathfrak{m}$ erklärt.

Das ist unabhängig von $\mathfrak{m}$ und es gilt auch im gewöhnlichen Sinne

$$(H_{10} \bmod f_1) \leqq (H_{20} \bmod f_2) \qquad f_1 \text{ Multiplum von } f_2$$

Hiernach ist auch erklärt:

$$\begin{array}{ll} [H_1 \bmod \mathfrak{m}_1, \ldots, H_r \bmod \mathfrak{m}_r] & \text{Durchschnitt} \\ (H_1 \bmod \mathfrak{m}_1, \ldots, H_r \bmod \mathfrak{m}_r) & \text{Vereinigungsgruppe.} \end{array}$$

Der Fundamentalsatz.

Wir erörtern nun die beiden Zuordnungsprinzipien:

$$K \longrightarrow H \bmod \mathfrak{m} \qquad K \longleftarrow H \bmod \mathfrak{m},$$

die sich zu der eineindeutigen Zuordnung zusammenfügen.

I.) *Ist K ein Relativkörper über k, so ist K eine bestimmte Idealgruppe $H \bmod \mathfrak{m}$ (für jedes $\mathfrak{m}$ eine) zugeordnet, nämlich die Gesamtheit der Strahlklassen mod $\mathfrak{m}$, die Relativnormen von Idealen aus K enthalten. $H \bmod \mathfrak{m}$ heißt die Relativnormgruppe mod $\mathfrak{m}$ von K.*

(Hier weiß man also a priori zwar die Existenz aber nicht die Eindeutigkeit der Zuordnung)

II.) *Ist $H \bmod \mathfrak{m}$ eine Idealgruppe in k, so kann ihr ein Relativkörper K über k so zugeordnet sein, daß gilt*:

a.) *alle zu $\mathfrak{m}$ primen Primideale 1. Grades aus H zerfallen in K in verschiedene Primideale 1. Relativgrades (und 1. Grades)*

b.) *alle nicht zu H gehörigen zu $\mathfrak{m}$ primen Primideale 1. Grades aus k haben in K mindestens einen Primfaktor höheren als 1. Relativgrades.*

(Hier weiß man a priori weder die Existenz noch die Eindeutigkeit der Zuordnung)
Es heißt dann K Klassenkörper zu H mod $\mathfrak{m}$

Hauptsatz. Zwischen den sämtlichen relativ-Abelschen Zahlkörpern K über k (Relativgrad n, Relativdiskriminante $\mathfrak{d}$, Galoissche Relativgruppe $\mathfrak{G}$) und den sämtlichen Idealgruppen H mod $\mathfrak{m}$ aus k (Klassenzahl h, Führer f, Klassengruppe A/H) läßt sich eine eineindeutige (bzgl. der H mod $\mathfrak{m}$ im erklärten Sinne) Zuordnung festlegen derart, daß folgende Bedingungen bestehen, wenn K und H mod $\mathfrak{m}$ zueinander zugeordnet sind:

I.) H mod $\mathfrak{m}$ (diese also eindeutig, soweit $\mathfrak{d} \mid \mathfrak{m}$) ist die Relativnormgruppe mod $\mathfrak{m}$ von K und gleich der Relativnormgruppe mod $\mathfrak{d}$ von K.

II.) K (dieser also stets vorhanden [2] und eindeutig, sowie rel. Abelsch.) ist Klassenkörper zu H mod $\mathfrak{m}$ (und jedem gleichen, insbesondere H_0 mod f)

III.) $\mathfrak{G} \cong A/H$, $h = n$. (Man kann nach Artin noch genauer angeben, wie! Rez.Ges.)

IV.) $\mathfrak{d}$ und f bestehen aus denselben Primidealen *) (Man kann das genau angeben)

V.) Die Primideale $\mathfrak{p}$ aus k zerfallen in K nach dem Gesetz:

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e, \qquad n(\mathfrak{P}_i) = \mathfrak{p}^f,$$

wenn $H_\mathfrak{p}$ die engste H enthaltende Idealgruppe von zu $\mathfrak{p}$ primem Führer (für $\mathfrak{p}$ prim zu $\mathfrak{m}$ also $H_\mathfrak{p} = H$) ist und

$$\begin{aligned} &a = (H_\mathfrak{p} : H) \\ &f \text{ der kleinste Exponent, sodaß } \mathfrak{p}^f \text{ in } H_\mathfrak{p} \ (\mathfrak{p}^f \sim 1 \bmod H_\mathfrak{p}) \\ &g = \frac{h}{ef} = \frac{n}{ef}. \end{aligned}$$

(Das ist Ausdruck der Definition des Klassenkörpers. Für die $\mathfrak{p}_\infty$ gilt ein entsprechendes Gesetz, wenn man an Stelle von $\mathfrak{p}$ in $H_\mathfrak{p}$ setzt $\mathfrak{p}_\infty \nmid f$.)

VI.) Die Relationen

$$K_1 \leqq K_2, \qquad H_1 \bmod \mathfrak{m}_1 \geqq H_2 \bmod \mathfrak{m}_2$$

sind gleichbedeutend. Demnach sind auch zugeordnet

$$\begin{aligned} (K_1, \dots, K_r) \quad &\text{und} \quad [H_1 \bmod \mathfrak{m}_1, \dots, H_r \bmod \mathfrak{m}_r] \\ [K_1, \dots, K_r] \quad &\text{und} \quad (H_1 \bmod \mathfrak{m}_1, \dots, H_r \bmod \mathfrak{m}_r) \end{aligned}$$

2. undeutlich

*). Die $\mathfrak{p}_\infty$ kommen dabei nicht in Betracht, weil sie in $\mathfrak{d}$ nicht eingehen.

Beispiel.

k rational, H der Strahl mod mp_∞, K der Körper der m-ten E.W. (d.h. $K = k\left(e^{\frac{2\pi i}{m}}\right)$) Denn in K gilt tatsächlich das Zerlegungsgesetz V.) also gilt insbesondere das Gesetz II.), was wegen der Eineindeutigkeit festzustellen hinreicht.

Allgemein genügt zur Feststellung, daß H mod m und K sich im Sinne des Satzes entsprechen:

entw. a.) daß K Klassenkörper zu H mod $\mathfrak{m}$ ist

oder b.) daß die Idealgruppe (H' mod $\mathfrak{d}$) = (H mod $\mathfrak{m}$) die Relativnormgruppe mod $\mathfrak{d}$ von K ist.

Im gegebenen Beispiel folgt daraus weiter, weil der Strahl mod mp_∞ in jeder Idealgruppe mod $\mathfrak{m}$ enthalten ist, daß die Körper der m-ten E.W. alle Abelschen Zahlkörper über k enthalten (*absolut Abelsche Körper – Kroneckersche Vermutung*) und man beherrscht die letzteren völlig in den Hinsichten

Gegenseitiges Enthalten, Rel. diskr., Zerlegungsgesetze, Galoissche Gruppe

Dadurch, daß man die Strahlklassengruppen in k genau beherrscht.

II.) Das Ziel der *komplexen Multiplikation* ist, eine ebensolche Beherrschung für einen imaginär-quadratischen Grundkörper k, Diskriminante d, zu erzielen. Während für den *rationalen* Körper das durch die Werte der Funktion

$$e^{2\pi i u}$$

für *rationale Werte* u geschieht, indem so *alle* absolut-Abelschen Körper geliefert werden, hat man für ein solches k die beiden Funktionen

$$j(\mathfrak{w}), \qquad \tau(u, \mathfrak{w})$$

zu nehmen, und darin $\mathfrak{w}$ *alle Ideale aus* k und u *alle Zahlen aus* k durchlaufen zu lassen. Jedes solche Paar definiert darin einen rel. Abelschen Körper

$$K = k\big(j(\mathfrak{w}), \tau(u, \mathfrak{w})\big)$$

über k und man erhält so alle zu k Abelschen Körper. (*Verbesserter Kroneckerscher Jugendtraum!*)

Erklärung der Funktionen $j(\mathfrak{w}), \tau(u, \mathfrak{w})$.

a.) w_1, w_2 komplexe Variable im *Bereich: linear unabhängig in Bezug auf reelle Zahlen*

$\omega = \frac{w_1}{w_2}$ also komplexe Variable im *Bereich* $\Im(\omega) \neq 0$

$w = n_1 w_1 + n_2 w_2$ durchläuft den aus w_1, w_2 erzeugten *Modul* $\mathfrak{w}$ mit ganzzahligen Koeffizienten.

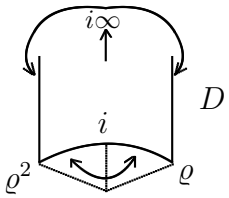
$$\begin{aligned} g_2(\mathfrak{w}) &= 60 \sum_{\substack{w \text{ in } \mathfrak{w} \\ w \neq 0}} \frac{1}{w^4} \\ g_3(\mathfrak{w}) &= 140 \sum_{\substack{w \text{ in } \mathfrak{w} \\ w \neq 0}} \frac{1}{w^6} \\ \Delta(\mathfrak{w}) &= g_2^3(\mathfrak{w}) - 27 g_3^2(\mathfrak{w}) \\ j(\mathfrak{w}) &= 2^6 3^3 \frac{g_2^3(\mathfrak{w})}{\Delta(\mathfrak{w})}. \end{aligned}$$

Eigenschaften von $j(\mathfrak{w})$:

1.) *Homogen von der Dimension 0*, d.h. nur von ω abhängig,

2.) Nur von $\mathfrak{w}$, nicht von w_1, w_2 abhängig, d.h. invariant bei der *weiteren homogenen Modulgruppe.*

Die *inhomogene weitere Modulgruppe* besitzt im Bereich $\Im(\omega) \neq 0$ einen *Diskontinuitätsbereich* D. Einfachster Repräsentant: Figur!



Uniformisierende Variable:

$\omega - \omega_0$	für ω_0 im Inneren von D und auf dem Rande außer Eckpunkten
$(\omega - \omega_0)^2$	für $\omega_0 = i$
$(\omega - \omega_0)^3$	für $\omega_0 = \varrho_1 \varrho^2$
$q = e^{2\pi i \omega}$	für $\omega_0 = i\infty$

3.) $j(\mathfrak{w})$ ist *analytische Funktion zu* D, d.h. von rationalem Charakter in den zu D gehörigen uniformisierenden Variablen. Sie ist Funktion *1. Ordnung zu* D, d.h. D gleichzeitig *Fundamentalbereich* für ihre Werte (gemessen [3] in D-Uniformisierenden). Speziell einziger *Pol 1. Ordnung* in $i\infty$.

Aus 3.) folgt nach funktionenth. Sätzen

3'.) Jede von der Dimension 0 homogene, bei weiterer Modulgruppe invariante Funktion, zu D analytische Funktion $f(\mathfrak{w})$ (sog. *Modulfunktion*) ist rationale Funktion von $j(\mathfrak{w})$, speziell jede Modulfunktion $g(\mathfrak{w})$ mit einzigem Pol n-ter Ordnung in $i\infty$ (*ganze Modulfunktion*) ganze rationale Funktion n-ten Grades von $j(\mathfrak{w})$; und umgekehrt.

4.) $j(\mathfrak{w})$ besitzt eine für $|q| < 1$ konvergente *q-Entwicklung*

$$j(\mathfrak{w}) = q^{-1}(1 + a_1 q + a_2 q^2 + \cdots)$$

mit *ganzzahligen Koeffizienten* $a_1, a_2, \ldots$.

Aus 4.) und 3.) folgt

4'.) *q-Entwicklungsprinzip.* Gehören die Koeffizienten einer ganzen Modulfunktion einem Zahlring an, so gehören auch die Koeffizienten ihrer ganz-rationalen Darstellung durch $j(\mathfrak{w})$ diesem Zahlring an.

b.) Außer den bisherigen Bezeichnungen:
u unbeschränkte komplexe Variable

$$\wp(u, \mathfrak{w}) = \frac{1}{u^2} + \sum_{\substack{w \text{ in } \mathfrak{w} \\ w \neq 0}} \left(\frac{1}{(u-w)^2} - \frac{1}{w^2} \right)$$

Ω imaginär-quadratischer Körper
d Diskriminante, e Anzahl der Einheiten (E.W.)
also

$$\begin{aligned} e &= 2 \quad \text{für} \quad d \neq -3, -4 \\ e &= 4 \quad \text{für} \quad d = -4 \\ e &= 6 \quad \text{für} \quad d = -6. \end{aligned}$$

3. undeutlich

$$\tau_\Omega(u,\mathfrak{w}) = g^{(e)}(\mathfrak{w})(-1)^{\frac{e}{2}}\wp^{\frac{e}{2}}(u,\mathfrak{w})$$

wobei

$$\begin{aligned} g^{(2)}(\mathfrak{w}) &= 2^7 3^5 \frac{g_2(\mathfrak{w})g_3(\mathfrak{w})}{\Delta(\mathfrak{w})} \\ g^{(4)}(\mathfrak{w}) &= 2^8 3^4 \frac{g_2^2(\mathfrak{w})}{\Delta(\mathfrak{w})} \\ g^{(6)}(\mathfrak{w}) &= 2^9 3^6 \frac{g_3(\mathfrak{w})}{\Delta(\mathfrak{w})} \end{aligned}$$

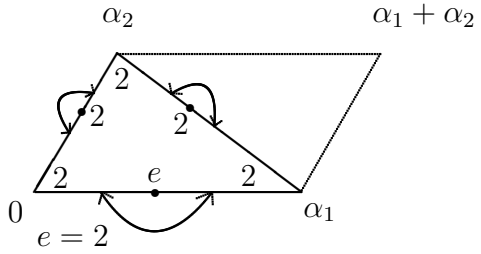
Eigenschaften von $\tau_\Omega(u,\mathfrak{w})$:

1.) Homogen von der Dimension 0 in $u, \mathfrak{w}$, (d.h. nur von $\frac{u}{w_2}, \frac{w_1}{w_2}$ abhängig)

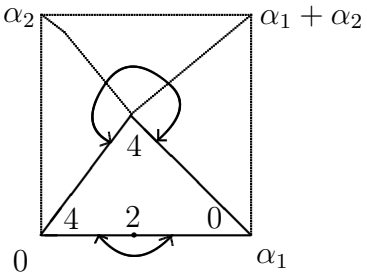
2.) Nur von $\mathfrak{w}$, nicht von w_1, w_2 abhängig, also invariant bei weiterer homogener Modulgruppe. Invariant bei der folgenden Gruppe in u, wenn speziell $\mathfrak{w} = \mathfrak{a}$ *ein Ideal aus* Ω *(singulärer Periodenmodul)*:

$$u' = \varepsilon u + \alpha \qquad (\varepsilon \text{ Einheit aus } \Omega,\ \alpha \text{ Zahl aus } \mathfrak{a})$$

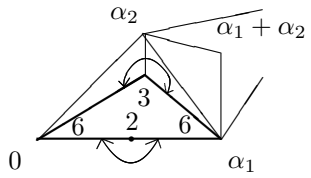
Diese Gruppe besitzt in der u-Ebene Diskontinuitätsbereich $D_\mathfrak{a}$. Einfachster Repräsentant:



$\boxed{e = 2}$



$\boxed{n = 4}$



Uniformisierende: $(u-u_0)^n$, mod $n=1$ i.a., sonst angegeben.

3.) $\tau_\Omega(u,\mathfrak{a})$ *analytische Funktion zu* $D_\mathfrak{a}$, *Funktion 1. Ordnung* zu $D_\mathfrak{a}$, *Pol 1. Ordnung* in $u=0$.

3'.) Jede bei der genannten Gruppe invariante, zu $D_\mathfrak{a}$ analytische Funktion ist rationale Funktion von $\tau_\Omega(u,\mathfrak{a})$ und umgekehrt.

(es genügt: *im Endlichen analytisch*, daraus folgt: zu $D_\mathfrak{a}$ analytisch, wegen Invarianz)

4.) $\tau_\Omega(u,\mathfrak{w})$ besitzt eine Entwicklung nach

$$\begin{aligned} q &= e^{2\pi i\omega}=e^{2\pi i\frac{w_1}{w_2}} \\ z &= e^{2\pi i\frac{u}{w_2}} \\ \tau_\Omega(u,\mathfrak{w}) &= q^{-1}(1+[q])\Bigg[1+\frac{12}{(z^{\frac12}-z^{-\frac12})^2}-24\sum_{n,n'=1}^{\infty}nq^{nn'}+ \\ &\qquad +12\sum_{n,n'=1}^{\infty}nq^{nn'}(z^n+z^{-n})\Bigg]^{\frac{e}{2}} \end{aligned}$$

wobei $[q]$ ganzzahlige bei $q=0$ verschwindende Potenzreihe in q. □□□

Behauptungen.

1.) Ist $\mathfrak{a}$ irgendein Ideal aus Ω, so erzeugt $j(\mathfrak{a})$ den *absoluten Klassenkörper* K (Strahl mod. 1) zu Ω.

2.) Ist $\mathfrak{m}\neq 1$ ein endlicher „Modul“ (Beschränkung auf endliche $\mathfrak{m}$ erlaubt, da mod $\mathfrak{p}_\infty$ nur eine Restklasse, also $\mathfrak{p}_\infty$ nie im Führer), $\mathfrak{a}$ irgendein Ideal aus Ω, $\mathfrak{r}$ ein zu $\mathfrak{m}$ primes Ideal, sodaß $\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}=\varrho$ Hauptideal, so erzeugten

$$j(\mathfrak{a}),\quad \tau_\Omega(\varrho,\mathfrak{a})=\tau_\Omega\left(\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a},\mathfrak{a}\right)$$

den Strahlklassenkörper $\mathsf{K}_\mathfrak{m}$ (Strahl mod $\mathfrak{m}$) zu Ω.

Bemerkungen.

1.) $j(\mathfrak{a})$ hängt nur von der absoluten Idealklasse k von $\mathfrak{a}$ ab und heißt daher *absolute Klasseninvariante*. Die h_1 abs. Klasseninvarianten sind *verschieden*.

2.) $\tau_\Omega\left(\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}, \mathfrak{a}\right)$ hängt nur von der Strahlklasse mod $\mathfrak{m}$ von $\mathfrak{r}$ ab, soweit diese in der festen, zu $\frac{\mathfrak{a}}{\mathfrak{m}}$ reziproken abs. Idealklasse bleibt, heißt daher *Strahlklasseninvariante mod* $\mathfrak{m}$.

Die h_m Systeme $j(\mathfrak{a})$, $\tau_\Omega\left(\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}, \mathfrak{a}\right)$, wo $\mathfrak{a}$ alle abs. Idealkl., $\mathfrak{r}$ alle Strahlkl. mod $\mathfrak{m}$ in den rez. abs. Id. Kl. zu $\frac{\mathfrak{a}}{\mathfrak{m}}$ durchläuft, sind *verschieden*.

Beweis.

Es genügt zu zeigen,

a.) $j(\mathfrak{a})$ und $\tau_\Omega\left(\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}, \mathfrak{a}\right)$ sind algebraische Zahlen

b.) in $\Omega\big(j(\mathfrak{a})\big)$ bezw. $\Omega\big(j(\mathfrak{a}), \tau_\Omega\left(\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}, \mathfrak{a}\right)\big)$ gilt das Klassenkörperzerlegungsgesetz:

Ist $\mathfrak{p}$ ein (zu geeign. $\mathfrak{m}_0$ primes – also endl. viele Ausnahmen gestattet) Primideal 1. Grades aus Ω, so zerfällt $\mathfrak{p}$ in versch. Primideale f. Grades, wenn zuerst

$$\mathfrak{p}^f \sim \mathrm{mod}\, 1 \qquad \text{bzw.} \qquad \mathfrak{p}^f \sim 1 \bmod \mathfrak{m}$$

Beweis a.)

Transformationstheorie für $j(\mathfrak{w})$

Transformation $\mathfrak{m}$. Grades: [4]

$$M = \begin{pmatrix} \mathfrak{m}_{11} & \mathfrak{m}_{12} \\ \mathfrak{m}_{21} & \mathfrak{m}_{22} \end{pmatrix}, \qquad \mathfrak{m}_{ij} \text{ ganz, teilerfremd}$$

$$|M| = m$$

$$M_1 \sim M_2, \quad \text{wenn } M_1 = SM_2 \ (S \text{ aus der weiteren Modulgruppe})$$

Dazu ist Klassenzahl *endlich*. Repräsentanten seien

$$M_1, \ldots, M_{\psi(m)}$$

ferner transformierte Funktionen

$$j\big(M_\nu(w_1, w_2)\big) \qquad \text{unabh. von Repräsentanten.}$$

4. unklar, ob m und $\mathfrak{m}$ hier und im Rest dieses Manuskripts verschiedene Zeichen sein sollen oder nicht.

Nach den Eigenschaften von $j(\mathfrak{w})$ ist

$$I_m\big(t, j(\mathfrak{w})\big) = \prod_{\nu=1}^{\psi(m)} \big\{t - j\big(M_\nu(w_1, w_2)\big)\big\}$$

Polynom in t, $j(\mathfrak{w})$ mit ganzen rat. Koeffizienten.

Insbesondere

$$I_m(t,t) \qquad \text{höchster Koeffiz } \pm 1, \text{ wenn } m \text{ kein Quadrat.}$$

Ist nun

$$\mathfrak{a} = (\alpha_1, \alpha_2)$$

und μ ganz in Ω, dann

$$\mu\mathfrak{a} = \mu(\alpha_1, \alpha_2) = M(\alpha_1, \alpha_2)$$

mit $|M| = m = N(\mu)$ in derselben Klasse.
Also

$$j(\mathfrak{a}) = j(\alpha_1, \alpha_2) = j\big(\mu(\alpha_1, \alpha_2)\big) = j\big(M(\alpha_1, \alpha_2)\big)$$

Wurzel von $I_m(t,t)$, wenn $m = N(\mu)$ als nicht-quadratische Norm eines ganzen μ aus Ω gewählt wird. Also sind die abs. Klasseninv. $j(\mathfrak{a})$ sogar ganze algebr. Zahlen.

Teilungstheorie von $\tau_\Omega(u, \mathfrak{w})$.

Wir bilden die Teilwerte m-ten Grades

$$\tau_\Omega\left(\frac{m_1 w_1 + m_2 w_2}{m}, \mathfrak{w}\right), \qquad m_1, m_2 \text{ ganz}, \qquad (m_1, m_2, m) = 1$$

Dann ist

$$T_m\big(t, j(\mathfrak{w})\big) = \prod_{\substack{m_1, m_2 \bmod m \\ (m_1, m_2, m)=1}} \left\{t - \tau_\Omega\left(\frac{m_1 w_1 + m_2 w_2}{m}, \mathfrak{w}\right)\right\}$$

ein Polynom in t, $j(\mathfrak{w})$ mit rationalen Koeffizienten, die höchstens Primteiler von m im Nenner haben.

Wird $\mathfrak{w} = \mathfrak{a}$ und m als kl. g.v. Multipl. von m gewählt, so ist

$$\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a} = \frac{m_1 w_1 + m_2 w_2}{m} \quad \text{mit } m_1, m_2 \text{ ganz}, (m_1, m_2, m) = 1.$$

Somit sind die $\tau_\Omega\left(\frac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}, \mathfrak{a}\right)$ algebraisch mit höchstens Primteilern von m im Nenner.

Zerlegungsgesetz.

Es genügt zu zeigen:

$$\left.\begin{aligned} j\left(\frac{\mathfrak{a}}{\mathfrak{p}}\right) &\equiv j(\mathfrak{a})^p \bmod \mathfrak{p} \\ \tau\left(\mathfrak{p}\frac{\mathfrak{r}}{\mathfrak{m}}\,\frac{\mathfrak{a}}{\mathfrak{p}}, \frac{\mathfrak{a}}{\mathfrak{p}}\right) &\equiv \tau\left(\tfrac{\mathfrak{r}}{\mathfrak{m}}\mathfrak{a}, \mathfrak{a}\right)^p \bmod \mathfrak{p} \end{aligned}\right\} \text{ für } \mathfrak{p} \text{ vom 1. Grade, prim zu geeign. } \mathfrak{m}_0$$

Denn daraus folgt wegen der Verschiedenheit der abs. Kl. Inv. und Strahlkl. Inv., daß man erst nach f-maliger Potenzierung mit p zum selben Kongruenzwert mod $\mathfrak{p}$ zurückkehrt, wenn f die Ordnung von $\mathfrak{p}$ mod 1 bezw. mod $\mathfrak{m}$ ist. Dabei ist nur $\mathfrak{p}$ prim zu den Differenzen der Invarianten zu nehmen.

Nach algebr. Zahlentheorie genügt das dann, wenn $\mathfrak{p}$ noch zur Diskr. der Invarianten prim, um auf das behauptete Zerlegungsgesetz zu schließen.

Der Beweis für jene Kongruenzen verläuft nun so:

Man konstruiert sich zunächst entsprechende Differenzen in Variablen:

$$\delta_{P_\nu}(w_1, w_2) = j^p(w_1, w_2) - j\big(P_\nu(w_1, w_2)\big)$$

$$\delta_{P_\nu}(m_1, m_2; w_1, w_2) = \tau_\Omega^p\left(\frac{m_1 w_1 + m_2 w_2}{m}; w_1, w_2\right) -$$

$$-\tau\left(\frac{m_1 w_1 + m_2 w_2}{m}, \frac{P_\nu(w_1, w_2)}{p}\right)$$

die für den singulären Fall

$$\mathfrak{w} = \mathfrak{a}, \qquad \frac{m_1 w_1 + m_2 w_2}{m} = \frac{\mathfrak{r}\mathfrak{a}}{\mathfrak{m}}, \qquad \frac{P_\nu(w_1, w_2)}{p} = \frac{\mathfrak{a}}{\mathfrak{p}}$$

in die gesuchten Differenzen übergehen, und zeigt daß die q-Entwicklungen durch p teilbare Koeffizienten haben. So einfach geht das nicht, weil $p = \mathfrak{p}\mathfrak{p}'$ und *diese* Tatsache gar nicht wahr ist. Man muß sich also geeignete Methodik entwickeln, die der Aufspaltung $p = \mathfrak{p}\mathfrak{p}'$ gerecht wird. Dazu bildet man die Multiplikatorgleichung für

$$\varphi_{P_\nu}(w_1, w_2) = p^{12}\frac{\Delta\big(P_\nu(w_1, w_2)\big)}{\Delta(w_1, w_2)}$$

$$\Phi_p\big(t, j(\mathfrak{w})\big) = \prod_{\nu=1}^{\psi(p)}\Big(t - \varphi\big(P_\nu(w_1, w_2)\big)\Big) \equiv t^{p+1} + \gamma t \bmod p$$

(durch q-Entwicklung dabei γ prim zu p)

Dann stellt man die $\delta_{P_\nu}(w_1, w_2)$ bezw. die elementarsymm. Fkt. $\delta^{(\mu)}_{P_\nu}(w_1, w_2)$ der $\delta_{P_\nu}(m_1, m_2; w_1, w_2)$ bzgl. der m_1, m_2 in der Form dar:

$$\delta^{(\mu)}_{P_\nu}(w_1, w_2) = \frac{G^{(\mu)}_p\left(\varphi_{P_\nu}(w_1, w_2), j(w_1, w_2)\right)}{\Phi'_p\big(t, j(w_1, w_2)\big)}$$

wo

$$G^{(\mu)}_p\big(t, j(w_1, w_2)\big) = \sum_{\nu=1}^{\psi(p)} \frac{\Phi_p\big(t, j(w_1, w_2)\big)}{t - \varphi_{P_\nu}(w_1, w_2)} \delta^{(\mu)}_{P_\nu}(w_1, w_2)$$

(Tschirnhausen Transformation).

Über die φ_{P_ν} muß man nun nach obigen

$$\varphi_P \sim \overline{\mathfrak{p}}^{12}, \qquad \varphi_{\overline{P}} \sim \mathfrak{p}^{12}, \qquad \varphi_{P_\nu} \sim 1 \quad \text{sonst } (\textit{sing. Fall})$$

und die Kongruenz von Zähler und Nenner in der Darstellung der $\delta^{(\mu)}_{P_\nu}$ beherrscht man so durch Zuhilfenahme der q-Entwicklungen. Man zeigt:
allgem. Zähler $\equiv 0 \bmod p$ (wegen q-Entwicklung)
singulär Nenner $\not\equiv 0 \bmod p$ (mit $\equiv \varphi_P + \gamma \sim \overline{\mathfrak{p}}^{12} + \mathfrak{p}$)
So kommt für den sing. Fall

$$\delta^{(\mu)}_{P_\nu} \equiv 0 \bmod \mathfrak{p}$$

und daraus auch

$$\delta_{P_\nu} \equiv 0 \bmod \mathfrak{p},$$

wenn $\mathfrak{p}$ nicht in Rel. Diskr. d. Körpers der δ_{P_ν} aufgeht.

Wenn man die Klassenkörpertheorie voraussetzt, ist damit die kompl. Multiplikation eingeordnet. Insbesondere ist der *Kroneckersche Jugendtraum* bewiesen.

Man kann aber nun weitergehend auch direkt die Klassenkörpertheorie für $k = \Omega$ herleiten. Nämlich so:

1.)
$$\begin{cases} H(t) &=& \prod_{\mathfrak{k}} \big(t - j(\mathfrak{k})\big) & \text{ist Polynom in } \Omega \\ S_{m,\mathfrak{k}}(t) &=& \prod_{\mathfrak{k}^* \text{ zu } \mathfrak{k}} \big(t - \tau(\mathfrak{k}^*)\big) & \text{ist Polynom in } \mathsf{K} \\ S_m(t) &=& \prod_{\mathfrak{k}} S_{m,\mathfrak{k}}(t) = \prod_{\mathfrak{k}^*} \big(t - \tau(\mathfrak{k}^*)\big) & \text{ist Polynom in } \Omega \end{cases}$$

Prinzip der größten gem. Teilerbildung mit geeigneten Transformations bezw. Teilungsgleichungen. Ähnlich kommt man ja beim Kreiskörper von $x^m - 1$ zur irreduziblen Gleichung.

2.)
$$\begin{cases} H(t) & \text{ist} & \text{irreduzibel} & \text{in} & \Omega \\ S_{m,\mathfrak{k}}(t) & = & = & = & \mathsf{K} \end{cases}$$

Leider gelingt nicht: $S_m(t)$ ist irreduzibel in Ω. (Das ginge, wenn man weiß, daß *alle* Strahlkl. Inv. verschieden.)

3.) $\left\{\begin{array}{lccccccc} H(t) & \text{hat} & \text{Abelsche} & \text{Gruppe} & \text{isomorph} & \text{zu} & \text{abs.} \\ & & & & & & \text{Klassengr.} \\ S_{m,\mathfrak{k}}(t) & = & = & = & = & = & \text{Gruppe der} \\ & & & & & & \text{Strahlkl.} \\ & & & & & & \text{mod } \mathfrak{m} \text{ zu } \mathfrak{k}. \end{array}\right.$

(Hierzu: Prinzip der *kompl. Multiplikation* besser allgem. [...] *Transforma* [...] $\tau(u, [\ldots]) \to \tau\left(u, \frac{\mathfrak{a}}{\mathfrak{m}}\right)$ für Hauptideale $m = \mu$ also in $\tau(\mu u, \mathfrak{a})$).

4.) $\left\{\begin{array}{l} \text{Es gilt das richtige Zerl. Ges. für die Prim. 2. Grades } p \text{ von } \Omega \\ \text{im Körper } \mathsf{K} \text{ bis auf endl. viele Ausnahmen} \end{array}\right.$

Leider gelingt nicht: Entspr. für K_m

5.) $\left\{\begin{array}{l} \text{Neuestens nach Fueter: Die Rel. Diskr. von } \mathsf{K} \text{ ist 1,} \\ \text{von } \mathsf{K}_m \text{ enth. sie nur Primteiler von } m. \end{array}\right.$

Man kriegt also *fast* alle Sätze der Klassenkörpertheorie analytisch heraus.

1.3 Leipzig 1928

Zur Theorie der Ringklassenkörper der komplexen Multiplikation.

Vortrag i. math. Koll. Leipzig, 2. Juli 1928.

Gegeben sei ein imaginär-quadratischer Grundkörper Ω, mit der Diskriminante d, also der Basis

$$(1, \omega) = \left(1, \frac{d + \sqrt{d}}{2}\right).$$

Der Einfachheit halber seien $d = -4, -3$ ausgeschlossen, wo zu den Einheiten ± 1 noch die Einheitswurzeln i, i^{-1} bezw. ϱ, ϱ^{-1} als Einheiten hinzukommen.

In Ω betrachten wir die *Zahlringe* R_m, d.h. die Gesamtheit aller ganzen α aus Ω mit

$$\alpha \equiv \text{g. rat. Zahl mod } m, \text{ alias } \alpha = x + y \cdot m\omega, \text{ wo } x, y \text{ ganz.}$$

m natürliche Zahl.

Jeder solche Ring R_m bestimmt eine multiplikative *Zahlgruppe* Z_m im Bereich der sämtlichen zu m primen Zahlen aus Ω, nämlich die Gesamtheit aller zu m primen α aus Ω mit

$$\alpha \equiv \text{zu } m \text{ primer rat. Zahl mod } m, \text{ alias } \alpha = \frac{x + ym\omega}{z},$$
$$\text{wo } x, y, z \text{ ganz, } x, \texttt{[...]} \text{ prim zu } m.$$

Die Zahlgruppe Z_m enthält mit α immer auch $-\alpha$. Werden diese nicht unterschieden, also nur die Hauptideale (α) betrachtet, so liefert die Zahlgruppe Z_m eine *Hauptidealgruppe* H_m.

Wird H_m als Hauptklasse und seine Nebengruppen in der Gruppe aller zu m primen Ideale von Ω als Nebenklassen betrachtet, so entsteht die Einteilung der zu m primen Ideale von Ω in die *Ringklassen* mod m. Für $m = 1$ sind das die gewöhnlichen, „abelschen“ Idealklassen. Für $m > 1$ entstehen sie aus diesen durch Aufspaltung (Einengung des Äquivalenzbegriffs). Die *Anzahl* h_m der Ringklassen mod m ergibt sich leicht als

$$h_m = \frac{\Phi(m)}{\varphi(m)} \cdot h = h_m^{(0)} \cdot h,$$

wo $h = h_1$ die „absolute“ Klassenzahl ist, und $\Phi(m), \varphi(m)$ die Eulerschen Funktionen in Ω und im rat. Zahlkörper P sind. Jede abs. Idealklasse zerfällt also in $\frac{\Phi(m)}{\varphi(m)}$ Ringklassen mod m.□□□

Die Ringklassen mod m bilden eine Abelsche Gruppe der Ordnung h_m, die *Ringklassengruppe mod m*.

Wir skizzieren nun zuerst die Verhältnisse, wie sie in der Tat nach der allgemeinen Klassenkörpertheorie liegen, um dann nachher möglichst viel mit den Methoden der komplexen Multiplikation zu beweisen.

(1.) *Zu jeder Gruppe H_m gibt es einen Klassenkörper K_m über Ω, den sog. Ringklassenkörper mod m. Dieser ist eindeutig bestimmt durch die Definitionseigenschaften*:

a.) *Die zu m primen Primideale 1. Grades $\mathfrak{p}$ aus Ω, welche in H_m liegen, zerfallen in K_m in verschiedene Primideale 1. Grades.*

b.) *Die zu m primen Primideale 1. Grades $\mathfrak{p}$ aus Ω, welche in K_m mindestens einen Primidealfaktor 1. Grades bekommen, liegen in H_m.*

In a.) und b.) sind endlich viele Ausnahmeprimideale $\mathfrak{p}$ zugelassen.

(2.) *Wenn $H_m \prec H_{m'}$, so $K_m \succ K_{m'}$ und umgekehrt.*

(3.) *K_m/Ω ist Abelsch, vom Relativgrad h_m, und die Galoissche Relativgruppe ist einstufig isomorph zur Ringklassengruppe mod m in Ω.*

(4.) *Ist $\mathfrak{p}$ ein nicht in m aufgehendes Primideal aus Ω, für das $\mathfrak{p}^{f_m}$ als früheste Potenz in H_m liegt, so zerfällt $\mathfrak{p}$ in K_m in $\frac{h_m}{f_m}$ verschiedene Primideale vom Relativgrade f_m.*

e	f	g
1	f_m	$h_m : f$
$h^{(0)}_{p^n}$	f_{m_0}	$h_{m_0} : f$

(5.) *Ist* $\mathfrak{p}$ *ein in* $m = p^n \cdot m_0$ *aufgehendes Primideal aus* Ω, *für das* $\mathfrak{p}^{f_{m_0}}$ *als früheste Potenz in* H_{m_0} *liegt, so zerfällt* $\mathfrak{p}$ *in* K_m *in* $h_{p^n}^{(0)}$*-te Potenzen von* $\dfrac{h_{m_0}}{f_{m_0}}$ *verschiedene Primideale vom Relativgrade* f_{m_0}.

([...] Relativdiskriminante von K/Ω gehen also höchstens Primteiler $\mathfrak{p}$ von m auf)

Nach (2.) ist der *absolute Klassenkörper* $K_1 = K$ zur *absoluten Hauptklasse* H in allen Ringklassenkörpern K_m enthalten. K selbst hat die Eigenschaften:

(3^1.) K/Ω *ist Abelsch, vom Relativgrad* h, *und die Galoissche Relativgruppe ist einstufig isomorph zur absoluten Idealklassengruppe in* Ω.

(4^1.) *Ist* $\mathfrak{p}$ *ein Primideal aus* Ω, *für das* $\mathfrak{p}^f$ *als früheste Potenz in* H *liegt, so zerfällt* $\mathfrak{p}$ *in* K *in* $\frac{h}{f}$ *verschiedene Primideale vom Relativgrade* f.

e	f	g
1	f	$h : f$

Die Relativdiskriminante von K/Ω ist also 1.

Und K_m/K hat die Eigenschaften:

(3'.) K_m/K *ist Abelsch, vom Relativgrade* $h_m^{(0)}$, *und die Galoissche Relativgruppe ist einstufig isomorph zur Gruppe der Ringklassen, die die absolute Hauptklasse zusammensetzen.*

(4'.) *Die nicht in* m *aufgehenden Primideale von* K *zerfallen in* K_m *in verschiedene Primideale vom Relativgrade* $\frac{f_m}{f}$.

(5'.) *Die in* $m = p^n \cdot m_0$ *aufgehenden Primideale von* K *zerfallen in* K_m *in* $h_{p^n}^{(0)}$*-te Potenzen verschiedener Primideale vom Relativgrade* $\frac{f_{m_0}}{f}$.

In der Relativdiskriminante von K_m/K gehen also höchstens Primteiler von m auf.

Diese Sätze folgen sämtlich aus der allgemeinen Klassenkörpertheorie. Und zwar ist das schwierigste für den Beweis die *Existenz* der K_m. Ihre *Eindeutigkeit* und die weiteren Sätze über *Grad*, *Gruppe*, *Zerlegung* ergeben sich dann erheblich leichter.

Die Hauptaufgabe, die durch die komplexe Multiplikation geleistet wird, ist der *Existenznachweis der* K_m mit Methoden der automorphen Funktionentheorie. Wenn man dann zwar auch alle die weiteren Sätze über *Eindeutigkeit*, *Grad*, *Gruppe*, *Zerlegung* verhältnismäßig leicht nach den Methoden

der allgemeinen Klassenkörpertheorie (unter anderm auch mittels „$s \to 1$“) gewinnen kann, so ist es doch ein berechtigter Versuch, nun auch jene weiteren Sätze mit denselben Mitteln, der automorphen Funktionentheorie zu beweisen.

Ich skizziere zunächst, was man in dieser Hinsicht bereits durch die *klassische komplexe Multiplikation* (bis Weber inkl.) hat.

ad (1.), Existenz. Die Grundtatsache der komplexen Multiplikation ist, daß Körper K_m, im Sinne der obigen Definition (1.), durch gewisse „singuläre“ Werte der Modulfunktion $j(\omega_1, \omega_2) = 2^6 \cdot 3^3 \cdot \dfrac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)}$ geliefert werden, indem man sie zu Ω adjungiert. Genauer so:

Ist α_1, α_2 ein linear-unabhängiges Zahlenpaar aus Ω, so bestimmt es eindeutig einen *Idealteiler* $\mathfrak{a}$ und einen *Führer* m, letzteren vermöge

$$\begin{vmatrix} \alpha_1 & \alpha_2 \\ \overline{\alpha}_1 & \overline{\alpha}_2 \end{vmatrix} = mN(\mathfrak{a})\sqrt{d}.$$

Es stellt sich dann heraus, daß

$$\Omega\big(j(\alpha_1, \alpha_2)\big)$$

ein Körper K_m in obigem Sinne (1.) ist.

ad (1.), Eindeutigkeit. ([...] der allgemeinen Klassenkörpertheorie leicht [...] mittels „$s \to 1$“ zu beweisen. Diese Tatsache fällt aber ihrer Natur nach nicht in den Kompetenzbereich der komplexen Multiplikation, weil zur [...] *beliebige* algebraische Körper über Ω zugelassen sind. [...])

ad (3.), Grad und Gruppe. $j(\alpha_1, \alpha_2)$ bleibt ungeändert, wenn (α_1, α_2) durch irgendein $\lambda\mathsf{S}(\alpha_1, \alpha_2)$ ersetzt wird, wo S eine Modulsubstitution und $\lambda \neq 0$ ein komplexer Parameter ist. Beschränkt man λ auf Ω, so transformiert sich dabei der Idealteiler $\mathfrak{a}$ in $\lambda\mathfrak{a}$, und der Führer m bleibt invariant. Man kann nun stets λ so wählen, daß $\lambda(\alpha_1, \alpha_2)$ (und somit alle $\lambda\mathsf{S}(\alpha_1, \alpha_2)$) Basis eines zu m primen Ideals $\lambda\mathfrak{a}$ im Ring R_m wird. Sei schon α_1, α_2 so beschaffen, also Basis in R_m eines zu m primen Ideals $\mathfrak{a}$. Dann zeigt sich, daß $\lambda\mathsf{S}(\alpha_1, \alpha_2)$ D.u.n.D. die gleiche Eigenschaft hat, wenn λ eine zu m prime Zahl aus dem Quotientenring zu R_m, also eine Zahl der Zahlgruppe Z_m ist.

Somit ist die Gesamtheit $\lambda\mathsf{S}(\alpha_1, \alpha_2)$ mit dieser Einschränkung zugeordnet der Ringklasse $\lambda\mathfrak{a} \bmod m$. Diese Zuordnung ist umkehrbar eindeutig. Man kann daher $j(\alpha_1, \alpha_2)$ als *Invariante der Ringklasse* $\mathfrak{k}^{(m)}$ *von* $\mathfrak{a} \bmod m$ bezeichnen:

$$j(\alpha_1, \alpha_2) = j(\mathfrak{k}^{(m)})$$

Es zeigt sich, daß auf Grund *dieser* Zuordnung der Ringklassen mod m zu den singulären Werten $j(\mathfrak{k}^{(m)})$ die Tatsache (3.) gilt; daß also

$$H_m(t) = \prod_{\mathfrak{k}^{(m)}} \left(t - j(\mathfrak{k}^{(m)})\right) \qquad \begin{cases} \text{Polynom in } \Omega \\ \text{irreduzibel} \\ \text{Abelsch} \\ \text{Gruppe isomorph zur Ringklassengruppe} \end{cases}$$

ist, letzteres so, daß jede Substitution der Galoisschen Gruppe durch Multiplikation aller [1] Argumente $\mathfrak{k}^{(m)}$ mit einer u. derselben Klasse entsteht.

ad (4.), Zerlegung der $\mathfrak{p} \nmid \boldsymbol{m}$. Das obige Gesetz ergibt sich bei dem Existenzbeweis, der ja einen Spezialfall dieses Gesetzes zu bestätigen hat, gleich vollständig mit, allerdings mit einer endlichen Anzahl von Ausnahmeprimidealen (Teilern gewisser Gleichungsdiskriminanten), insbesondere also noch nicht die Tatsache über die Relativdiskriminante von K_m/Ω.

ad (3^1.), (4^1.), absoluter Klassenkörper $\boldsymbol{K}$. Diese Tatsachen sind damit auch festgestellt, wieder allerdings mit endlich vielen Ausnahmeprimidealen in (4^1.). Insbesondere also noch nicht die Tatsache über die Relativdiskr. in K/Ω.

ad (2.), Unterkörper-Untergruppe. Hier hat Weber die eine Seite:

$$\textit{Wenn } H_m \prec H_{m'}, \textit{ so } K_m \succ K_{m'}.$$

Wie es mit der Umkehrung steht, erläutere ich nachher.

Damit ist insbesondere $K \prec K_m$ festgestellt.

ad (3'.), (4'.), Beziehung von $\boldsymbol{K_m/K}$.

Diese Tatsachen ergeben sich leicht aus der genaueren Formulierung der Weberschen Tatsache:

$$j\left(\mathfrak{k}^{(m')}\right) = \mathsf{R}\left(j(\mathfrak{k}^{(m)})\right), \quad \text{wenn} \quad \mathfrak{k}^{(m)} \prec \mathfrak{k}^{(m')},$$

wo R eine rationalzahlige rationale Funktion ist. Wieder sind in (4'.) endlich viele Ausnahmeprimideale möglich, sodaß insbesondere die Tatsache über die Relativdiskriminante von K_m/K noch nicht feststeht.

Soweit die klassische Theorie. Der Überblick zeigt folgende noch auszufüllende Lücken:

1. undeutlich

(a.) Beseitigung der Ausnahmen im Zerlegungsgesetz (4.), (4^1.), (4'.) für die $\mathfrak{p} \nmid m$, insbesondere also Nachweis der Tatsachen über die Relativdiskriminante

(b.) Herleitung des Zerlegungsgesetzes (5.), (5'.) für die $\mathfrak{p}/m$

(c.) Nachweis der Umkehrung zu (2.): Wenn $K_m \succ K_{m'}$, so $H_m \prec H_{m'}$.

(c.) folgt leicht aus (b.), da man aus dem Verzweigungsverhalten der $\mathfrak{p} \mid m$ Aussagen von der Form gewinnen kann: Wenn $m' \nmid m$, so $K_m \not\succ K_{m'}$. Und $H_m \prec H_{m'}$ kommt ja auf $m'|m$ (oder wegen einer Ausnahme für die 2 [2] jedenfalls $m' \mid 2m$) hinaus.

Nun hat Hecke (a.) und (b.) gleichzeitig vollständig mittels seiner Funktionalgleichung der ζ-Funktionen mit Größencharakteren erledigt. Aber das ist eine Methode, die eben Hilfsmittel aus der allgemeinen Klassenkörpertheorie (die Variable s in Dirichletschen Reihen) heranzieht.

Fueter kann mit analogen, weniger tiefen Hilfsmitteln (Existenz unendlich vieler Primideale in Ω mit vorgeschr. Potenzrestcharakteren) wenigstens (a.) erledigen.

Es scheint aber wenig Aussicht zu bestehen (a.) mit alleiniger Benutzung der Hilfsmittel der komplexen Multiplikation zu erledigen.

Ganz anders dagegen (b.) und damit dann auch (c.). Da ist es mir gelungen, in einer gewissen Klasse von Fällen heranzukommen. Es genügt ersichtlich, den Tatbestand (5'.) für K_m/K zu beweisen. Denn damit ist (5.) auch bewiesen, mit der naturgemäßen Einschränkung, daß die Ausnahmeprimideale in (4^1.) von K/Ω auszunehmen sind, und die in (4.) für K_{m_0}/K.

Ich studiere also die Zerlegung in K_m/K für die $\mathfrak{p} \mid m$, welche in K/Ω dem Gesetz (4^1.) folgen. Und zwar gelingt es mir durchzukommen, mit weiteren endlich vielen Ausnahmen, für diejenigen $\mathfrak{p} \mid m$, welche *den beiden letzten* der Zerlegungstypen

$$p = \mathfrak{p}\bar{\mathfrak{p}}, \qquad p = \mathfrak{p}, \qquad p = \mathfrak{p}^2$$

in Ω angehören. Wegen der Ausnahmen, und vor allem wegen des Versagens meiner Methode für den ersten Zerlegungstypus, reicht das allerdings dann noch nicht hin, um die Umkehrung (c.) allgemein zu beweisen. Doch liegt ja an dieser Umkehrung (c.) an sich weniger. Soweit ich sie als Hilfsmittel bei meinem Beweise gebrauche, kommt sie eben durch den Beweis mit heraus.

2. undeutlich

Ich möchte meine Methode an dem einfachsten Falle erläutern:

$$\begin{aligned} p &= \mathfrak{p} \quad \text{in} \quad \Omega \qquad \text{(Primideal 2. Grades)}, \\ m &= p, \\ \text{zu studieren} &\qquad \text{also} \quad K_p/K. \end{aligned}$$

In K/Ω ist

$$\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_h, \qquad \text{(Rel. Gr. 1)}$$

weil schon $\mathfrak{p}^1 = p$ in H liegt; von den endlich vielen Ausnahmen für p wird abgesehen.

Behauptung: In K_p/K ist jedes

$$\mathfrak{p}_i = \mathfrak{P}_i^{p+1}, \qquad \text{(Rel. Gr. 1)}.$$

Es ist nämlich

$$h_p = \frac{\Phi(p)}{\varphi(p)} h = \frac{p^2-1}{p-1} h = (p+1) \cdot h$$

also

$$h_p^{(0)} = p + 1,$$

ferner

$$m_0 = 1, \quad H_{m_0} = H, \quad h_{m_0} = h, \quad f_{m_0} = f = 1.$$

Es wird also „reelle Verzweigung“ der $\mathfrak{p}_i$ in K_p/K behauptet.

Denn es ist ja

$$K_p/K \quad \text{zyklisch vom Rel. Grade } h_p^{(0)} = p + 1,$$

zyklisch, weil die Restklassen mod $\mathfrak{p}$ in Ω zyklisch sind, also auch jede Restklassengruppe zyklische Faktorgruppe hat. Die Aufgabe ist ganz analog zu der entsprechenden für den Kreiskörper:

> ζ primitive p-te Einheitswurzel, $K_p = \mathsf{P}(\zeta)$, zykl. vom Grade $p-1$, (Klassenkörper zur Gruppe $a \equiv 1 \bmod p$). Behauptung $p = \mathfrak{P}^{p-1}$ in K_p ist „vollverzweigt“.

Nachweis dort aus den Kenntnissen:

a.) $1-\zeta$, $1-\zeta^2$, …, $1-\zeta^{p-1}$ sind assoziiert

b.) $(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1}) = p$.

Wir haben zunächst analog zu den ξ^ν die konjugierten Wurzeln einer erzeugenden Gleichung für K_p/K zu bestimmen. Das tun hier die Wurzeln der Invariantengleichung

$$I_p(t) = \big(t - j(\mathsf{P}_1)\big) \cdots \big(t - j(\mathsf{P}_{p+1})\big)$$

wo als Argument eine Idealbasis α_1, α_2 im Ring R *aller* ganzen Zahlen zu setzen ist. Die $\mathsf{P}_1, \ldots, \mathsf{P}_{p+1}$ durchlaufen die $\psi(p) = p + 1$ Klassen von ganzzahligen Matrizen (Transformationen) p-ten Grades:

$$\mathsf{P} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{mit} \quad |\mathsf{P}| = ad - bc = p.$$

Zwei solche $\mathsf{P}', \mathsf{P}''$ heißen äquivalent, wenn

$$\mathsf{P}'' = \mathsf{S}\mathsf{P}' \qquad \text{mit Modulsubst. } \mathsf{S},$$

was ja zum selben j-Wert führt.

Es zeigt sich, daß dazu $j(\mathsf{P}_\nu)$ als Ringklasseninvarianten mod p den die Klasse von $(\alpha_1, \alpha_2) = \mathfrak{a}$ zusammensetzenden Ringklassen mod p entsprechen. In der Tat ist der Führer von $\mathsf{P}_\nu(\alpha_1, \alpha_2)$ sofort als p zu bestimmen. $I_p(t)$ hat ganz-rationale Zahlkoeffizienten, sodaß eine erzeugende Gleichung für K_p/K (Grad ist ja $p + 1$) vorliegt, und die $j(\mathsf{P}_\nu)$ rel.konjugiert sind.

Jetzt haben wir das Analogon zu den $1 - \zeta^\nu$ zu suchen. Das leisten hier die „Multiplikatoren“

$$\varphi_\nu = p^{12} \frac{\Delta(\mathsf{P}_\nu)}{\Delta}.$$

Man zeigt, daß φ_ν rational durch j und $j(\mathsf{P}_\nu)$ darstellbar ist, daß also im singulären Falle α_1, α_2

$$\varphi_\nu \quad \text{in} \quad K_p = \mathsf{K}\big(j(\mathsf{P}_\nu)\big) = \Omega\big(j, j(\mathsf{P}_\nu)\big)$$

enthalten ist, und die φ_ν sind hiernach wieder relativ-konjugiert. Die *direkte* Bildung der „Multiplikatorgleichung“

$$M_p(t) = (t - \varphi_1) \cdots (t - \varphi_{p+1})$$

zeigt ferner, daß die φ_ν ganze algebraische Zahlen sind. $M_p(t)$ hat nämlich ganz-rationale Zahlkoeffizienten.

Insbesondere ergibt sich für das absolute Glied

$$\varphi_1 \cdots \varphi_{p+1} = p^{12},$$

als nirgends unendliche Modulfunktion.

Dagegen gelingt es hier nicht ohne weiteres zu zeigen, daß die φ_ν assoziiert sind. Im Kreiskörper kann man nun auch so schließen:

$$(1-\zeta)\cdots(1-\zeta^{p-1}) = p$$

$1-\zeta$ Wurzel von $t^{p-1} - \binom{p}{1}t^{p-2} + \cdots \pm p = 0$ also

$$1-\zeta \equiv 0 \mod \mathfrak{P} \qquad \text{für } \textit{jedes } \mathfrak{P}|p \text{ in } K_p.$$

Ist also

$$p = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g)^e \qquad (\text{Grad } f) \text{ in } \mathsf{K},\ efg = p-1$$
$$1-\zeta = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_g^{a_g}, \text{ so alle } a_\kappa \geqq 1.$$
$$N(1-\zeta) = p^{a_1 f_1 + \cdots + a_g f_g} = p^1, \text{ also } g=1,\ f=1,\ a=1 \text{ somit } e = p-1.$$
$$1-\zeta = \mathfrak{P} \qquad \text{und} \qquad p = \mathfrak{P}^{p-1}.$$

Das läßt sich nachmachen. Man weiß nämlich, daß

$$I_p(t) \equiv (t^p - j)(t - j^p) \bmod p$$
$$j \equiv j^{N(\mathfrak{p})} = j^{p^2} \bmod p \quad \text{weil } \mathfrak{p} \text{ in Pr.Id. 1. Rel.Gr. zerfällt.}$$

also

$$t^p - j \equiv t^p - j^{p^2} \equiv (t - j^p)^p \bmod p$$
$$I_p(t) \equiv \left(t - j^p\right)^{p+1} \bmod p$$
$$J(\mathsf{P}_\nu) - j^p \equiv 0 \bmod \mathfrak{P}_\kappa \quad \text{für jedes } \mathfrak{P}_\kappa|p \text{ in } K_p.$$

Und wenn man jetzt die Differenzen

$$\varphi_\nu - \left(j(\mathsf{P}_\nu) - j(p)\right)$$

betrachtet und ihre Relativgleichung bildet, so stellt aus den q-Entwicklungen heraus, daß deren Koeffizienten alle $\equiv 0 \bmod p$ sind, also

$$\varphi_\nu - \left(j(\mathsf{P}_\nu) - j^p\right) \equiv 0 \bmod \mathfrak{P}_\kappa$$
$$\varphi_\nu \equiv 0 \bmod \mathfrak{P}_\kappa \quad \text{für jedes } \mathfrak{P}_\kappa|p \text{ in } K_p.$$
$$\text{also insbesondere für jedes } \mathfrak{P}_{i\kappa}|\mathfrak{p}_i \text{ in } K_p.$$

Jetzt könnte genau so geschlossen werden, wie beim Kreiskörper, wenn nicht

$$\varphi_1 \cdots \varphi_{p+1} = p^{12}$$

eine 12-te Potenz wäre.

Daher ist zu den Funktionen

$$\psi_\nu = \sqrt[12]{\varphi_\nu}$$

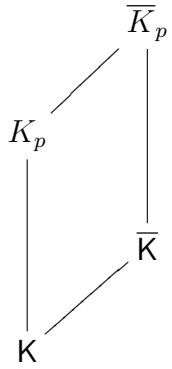
überzugehen, für die man wieder beweist:

$$\psi_1 \cdots \psi_{p+1} = p$$
$$\psi_\nu \equiv 0 \bmod \overline{\mathfrak{P}}_{ik} \quad \text{für jedes } \overline{\mathfrak{P}}_{ik} | \mathfrak{p}_i \text{ in } \overline{K}_p,$$

wo $\overline{K}_p$ der Körper ist, den die ψ_ν über K_p erzeugen.

Es stellt sich nun heraus, daß $\overline{K}_p$ aus K_p durch Adjunktion der 12-ten oder niedrigerer Einheitswurzeln und der Ringklasseninvarianten mod 12 oder nach einem Teiler von 12 entsteht.

Die obige Schlußweise klappt nun trotzdem noch, wenn man nur weiß, daß in $\overline{\mathsf{K}}/\mathsf{K}$ die Primteiler von p unverzweigt sind:



Dabei entsteht $\overline{\mathsf{K}}$ aus K in gleicher Weise, wie $\overline{K}_p$ aus K_p. Bis auf endlich viele Ausnahmen ist das nun der Fall nach (4'.). Insbesondere ist $p \neq 2, 3$ zu nehmen.

Man bekommt dann die Verzweigung der $\mathfrak{p}_i$ in K_p/K genau als die Verzweigung der $\overline{\mathfrak{p}}_i$ in $\overline{K}_p/\overline{\mathsf{K}}$, und die letzere eben nach der zitierten Kreiskörper-Schlußweise.

Meine Methode klappt ähnlich für $p = \mathfrak{p}^2$ in Ω, doch versagt sie für $p = \mathfrak{p}\overline{\mathfrak{p}}$ in Ω. In diesem Falle wird in

$$\begin{aligned} \varphi_1 \cdots \varphi_{p+1} &= p^{12} \\ \psi_1 \cdots \psi_{p+1} &= p \end{aligned}$$

schon das Produkt von zwei Faktoren, die zum *absoluten Klassenkörper* K, bzw. zu $\overline{\mathsf{K}}$ gehören, gleich der rechten Seite. Die übrigen, die hier die $p-1$ konjugierten zu K_p bezw. $\overline{K}_p$ gehörender [3] Größen sind, sind *Einheiten*. Über K_p lehrt dann die Methode nichts. Wohl aber über K etwas ganz anderes.

Denn die beiden zu K gehörigen Faktoren

$$\varphi = \psi^{12}, \overline{\varphi} = \overline{\psi}^{12}$$

erweisen sich als Darstellungen der Ideale

$$\mathfrak{p}^{12}, \qquad \overline{\mathfrak{p}}^{12}$$

als Hauptideale in K.

Es ist meinem Schüler W. Schäfer gelungen, zu zeigen, daß für Fall

$$d \text{ prim zu } 2 \text{ und } 3$$

die Hauptidealdarstellungen

$$\psi \text{ und } \overline{\psi} \text{ von } \mathfrak{p} \text{ und } \overline{\mathfrak{p}} \textit{ selbst}$$

bei geeigneter Normierung der $\sqrt[12]{\ }$ nicht nur zu $\overline{\mathsf{K}}$ sondern sogar zu K gehören. Bis auf *endlich* viele Ausnahmen werden also in diesen Fällen alle Primideale 1. Grades von Ω zu Hauptidealen in K, und somit ausnahmslos *alle* Ideale zu Hauptidealen in K.

Das ist der *Hilbertsche Hauptidealsatz*, der allgemein noch unbewiesen ist.

Für d nicht prim zu 6 ist er im Falle der komplexen Multiplikation auch richtig, wie ich allerdings bisher nur mittels transzendenter Schlüsse („$s \to 1$“) zeigen kann.

Einem rein-arithmetisch „automorphen“ Beweis bin ich aber schon auf der Spur.

---

3. undeutlich

1.4 Jena 1928

Das Reziprozitätsgesetz.

Vortrag i.d. Math. Gesellschaft Jena, 22.XI.1928.

Seit *Hilbert's* grundlegenden Arbeiten (1897/98) über das quadratische Reziprozitätsgesetz in beliebigen algebraischen Zahlkörpern ist durch die anschließenden Arbeiten von *Furtwängler* und *Takagi* immer deutlicher hervorgetreten, daß das allgemeine Reziprozitätsgesetz der m-ten Potenzreste in der sog. *Klassenkörpertheorie* wurzelt. Neuestens hat *Artin* eine ganz allgemeine Formulierung des Gesetzes gegeben, die diese Verankerung in besonders durchsichtiger Form hervortreten läßt, und die zudem zu einem ganz einfachen Beweis des Gesetzes auf Grund der Klassenkörpertheorie führt. Über diese Formulierung Artin's, sowie über die anschließend gemachten Untersuchungen von *Artin*, *Furtwängler* und *mir* will ich nachstehend berichten.

Zunächst sei der Begriff *Klassenkörper* kurz erläutert. Als Beispiel wähle ich den Körper K_m der m-ten Einheitswurzeln: $K_m = k_0(\zeta_m)$ über dem rationalen Körper k_0. Für diesen gilt bekanntlich das Zerlegungsgesetz:

Eine zu m prime Primzahl p zerfällt in K_m in verschiedene Primideale f-ten Grades:

$$p = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \qquad N(\mathfrak{P}_i) = p^f, \qquad fg = \varphi(m),$$

wenn f der kleinste positive Exponent mit

$$p^f \equiv 1 \bmod m$$

ist.

Die Zerlegungsform der Primzahlen p hängt also nur von der *Klasse* ab, der p bei der Einteilung in die primen Restklassen mod m angehört. Man nennt daher K_m Klassenkörper für die Klasseneinteilung in die primen Restklassen mod m im rationalen Körper k_0.

Man betrachtet ferner folgende Gesetzmäßigkeiten:

Die Galoissche Gruppe $\mathfrak{G}$ von K_m ist einstufig-isomorph zur Gruppe der „Klassen" in k_0. (Insbesondere der Grad von K_m gleich der Anzahl der „Klassen").

In der Tat werden die Substitutionen von $\mathfrak{G}$ durch $\zeta_m \to \zeta_m^r$ gegeben, und setzen sich so zusammen:

$$(\zeta_m \to \zeta_m^r)(\zeta_m \to \zeta_m^s) = (\zeta_m \to \zeta_m^{rs}).$$

Die Diskriminante $\mathfrak{d}$ *von* K_m *enthält nur Primteiler des Moduls* m *der Klassenteilung.*

Es ist nämlich $\mathfrak{d}$ Teiler der Diskriminante m^m von $x^m - 1$.

Man kann nun in k_0 auch andere, allgemeinere Klassenteilungen zugrundelegen, nämlich solche, die durch *Vergröberung* der Teilung in die primen Restklassen mod m entstehen. Das geschieht so, daß man anstelle der Gruppe H_0 $\{\equiv 1 \bmod m\}$ eine beliebige (umfassendere) Gruppe H von Restklassen mod m als Hauptklasse nimmt, und deren Nebengruppen (in der Gruppe aller zu m primen Zahlen) als Klassen. Beispiel: Die quadratischen Reste mod m, die k-ten Potenzreste mod m. Die neuen Klassen setzen sich dann aus einer bestimmten (festen) Anzahl der Restklassen mod m zusammen.

Zu jeder solchen gröberen Klasseneinteilung mod m erhält man nun, erzeugt durch die zugehörigen Gaussschen Kreisteilungsperioden $\sum_{\substack{a \text{ in } H \\ a \bmod m}} \zeta_m^a$, einen zugehörigen Klassenkörper K. Darunter ist ein Körper zu verstehen, in dem das zu obigem analoge *Zerlegungsgesetz* gilt: $\cdots$ □□□

Es gilt also der *Existenzsatz*:

Zu jeder Klassenteilung nach einer Kongruenzgruppe H mod m *existiert ein Klassenkörper* K.

Ferner zeigt sich, daß dabei analoge Gesetze zu den obigen *Gesetzen über Galoissche Gruppe und Diskriminante* gelten: $\cdots$

Schließlich stellt sich heraus, daß die Zuordnung „$H \to K$ als Klassenkörper“ eine eindeutige, umkehrbar eindeutige, anordnungsreziproke ist. Es gilt nämlich der *Anordnungssatz*, speziell *Eindeutigkeitssatz*:

Ist $H \to K$ *und* $H' \to K'$ *als Klassenkörper, so folgt aus* $H \leqq H'$, *daß* $K \geqq K'$ *ist, und umgekehrt.*

Der Vergröberung der Einteilung entspricht also eine Verkleinerung des Körpers.

Abgerundet wird diese ganze Satzgruppe durch den fundamentalen Satz von *Kronecker*. Alle Klassengruppen sind ja Abelsch, also alle Körper, die wir betrachteten, Abelsche Körper, was ja auch schon durch ihre Einbettung in die Kreiskörper klar ist. Es gilt nun der *Umkehrsatz*:

Jeder Abelsche Körper K *ist Klassenkörper zu der Klassenteilung nach einer geeigneten Kongruenzgruppe* H *nach geeignetem mod* m.

Damit wird die Theorie der *Klassenkörper* über dem rationalen Körper k_0 zu einer Theorie der *Abelschen Körper* über k_0. Man beherrscht diese vollständig von k_0 aus, indem man jede Aussage über sie als eine Aussage

über die zugehörige Klassenteilung aussprechen kann. Das ist der tiefere Sinn der Klassenkörpertheorie.

Diese ganze Theorie über k_0 gilt nun, wie *Furtwängler* und *Takagi* zeigten, mutatis mutandis auch über einen *beliebigen algebraischen Zahlkörper k als Grundkörper*. Definition und Sätze lauten dann eben so: $\cdots$

Unter „Kongruenzgruppe H mod m ist jetzt Folgendes zu verstehen: Man überlagert die Einteilung in die gewöhnlichen Idealklassen (Gruppe der Hauptideale) mit einer Restklassenteilung mod m (Gruppe der Hauptideale $\equiv 1 \bmod m$) und bildet dann irgendwelche Vergröberungen.

Nun zum *Artin*'schen Gesetz. Die Klassenkörpertheorie behauptet die abstrakte Isomorphie zwischen der Galoisschen Gruppe $\mathfrak{G}$ von K/k und der Klassengruppe nach H in k. Artin gibt nun eine konkrete Darstellung dieses Isomorphismus. Er gibt also eine Regel an, wie man einer Klasse $\mathfrak{C}$ nach H in k eine Substitution σ aus $\mathfrak{G}$ so zuordnen kann, daß der fragliche Isomorphismus herauskommt.

Die Artinsche Regel knüpft an Frobenius an. Es wird zunächst ein Primideal $\mathfrak{p}$ aus $\mathfrak{C}$ betrachtet. Ihm läßt sich eine Substitution σ aus $\mathfrak{G}$ eindeutig so zuordnen:

(F) $\qquad \mathsf{A}^{N(\mathfrak{p})} = \sigma\mathsf{A} \bmod \mathfrak{p} \qquad$ für jedes zu $\mathfrak{p}$ prime A aus K.

(σ ist eine bestimmte Erzeugende der sog. Zerlegungsgruppe für $\mathfrak{p}$ in K/k).

Das *Artinsche Gesetz* lautet nun:

Die gemäß der Frobeniusschen Regel (F) einem Primideal $\mathfrak{p}$ aus k zugeordnete Substitution σ aus $\mathfrak{G}$ hängt nur von der Klasse $\mathfrak{C}$ nach H ab, der $\mathfrak{p}$ angehört. Und die Frobeniussche Zuordnung ist überdies isomorph, d.h. ist

$$\begin{array}{ccccc} \sigma & \textit{den} & \textit{Primidealen} & \textit{aus} & \mathfrak{C}, \\ \sigma' & \| & \| & \| & \mathfrak{C}' \end{array}$$

zugeordnet, so ist

$$\sigma\sigma' \quad \| \quad \| \quad \| \quad \mathfrak{C}\mathfrak{C}'$$

zugeordnet.

Für den Kreiskörper ist das auf der Hand liegend. Denn (F) auf $\mathsf{A} = \zeta_m$ angewandt gibt:

$$\zeta_m^p \equiv \sigma\zeta_m \bmod p, \qquad \text{d.h.} \quad \zeta_m^p = \sigma\zeta_m.$$

$\sigma\zeta_m$ hängt hiernach in der Tat nur von $p \bmod m$ ab, und zwar isomorph.

Was hat das nun mit dem *Reziprozitätsgesetz* zu tun?

Das erkennt man sofort, wenn man es anwendet auf folgenden Fall:

$$k \text{ enthält die } m\text{-ten Einheitswurzeln } \zeta_m$$
$$K = k\,(\sqrt[m]{\alpha}), \text{ wo } \alpha \text{ in } k.$$

Es ist dann K/k Abelsch, also Klassenkörper zu einer ganz bestimmten Teilung in k. Die Zuordnung (F) auf $\mathsf{A} = \sqrt[m]{\alpha}$ angewandt gibt:

$$\sqrt[m]{\alpha}^{N(\mathfrak{p})} \equiv \sigma\sqrt[m]{\alpha} = \zeta_m \sqrt[m]{\alpha} \bmod \mathfrak{p}$$
$$\zeta_m \equiv \sqrt[m]{\alpha}^{N(\mathfrak{p})-1} = \alpha^{\frac{N(\mathfrak{p})-1}{m}} \bmod \mathfrak{p}$$
$$\zeta_m = \left(\frac{\alpha}{\mathfrak{p}}\right)_m = \text{Legendresches Symbol der } m\text{-ten } \texttt{[...]}$$

Also die $\mathfrak{p}$ zugeordnete Substitution ist:

$$\sigma = \left(\sqrt[m]{\alpha} \to \left(\frac{\alpha}{\mathfrak{p}}\right)_m \sqrt[m]{\alpha}\right)$$

Das Artinsche Gesetz liefert also:

$\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ *hängt nur von der Klasse ab, der* $\mathfrak{p}$ *bei der zu* $k(\sqrt[m]{\alpha})$ *gehörigen Klassenteilung in* k *angehört, und multipliziert sich isomorph, also auch* $\left(\frac{\alpha}{\mathfrak{b}}\right)_m$ *hängt nur von der Klasse ab, der das beliebige Ideal*[1] $\mathfrak{b}$ *angehört.*

$\left(\frac{\alpha}{\mathfrak{b}}\right)_m = \chi_m(\mathfrak{b}) =$ erz. Char. d. Klassengr. H

$\left(\frac{\alpha}{\mathfrak{b}}\right)_m = 1$ bedeutet $\mathfrak{b}$ in H.

Das ist die wesentliche Aussage des Reziprozitätsgesetzes. Nehmen wir etwa $m = 2$ und $\alpha = q =$ Primzahl $\equiv 1 \bmod 4$, so findet man: $\left(\frac{q}{p}\right)$ hängt nur von der Klasse ab, der p für die zu $k_0\left(\sqrt{q}\right)$ gehörige Teilung angehört. Das ist aber eine Teilung mod q, nämlich, wie man durch Einbettung in den Kreiskörper K_q findet, die nach den quadratischen Resten mod q. Also

$$\left(\frac{q}{p}\right) = +1 \quad \text{oder} \quad -1, \text{ je nachdem } \left(\frac{p}{q}\right) = +1 \text{ oder } -1.$$

1. undeutlich

Ähnlich allgemein.

Man kann zeigen, daß aus dem Artinschen Gesetz folgende elegante Formulierung des Reziprozitätsgesetzes der m-ten Potenzreste folgt:

$$\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\beta}{\alpha}\right)_m,$$

wenn $k\,(\sqrt[m]{\alpha})$ und $k\left(\sqrt[m]{\beta}\right)$ zueinander prime Rel. Diskr. haben.

Das habe ich in einer an Artin anschließenden Arbeit gezeigt. Ferner habe ich gezeigt, daß auch für beliebiges m die (durch Hilbert, Furtwängler, Takagi nur für $m =$ Primzahl ℓ bewiesene) *Produktformulierung* des Reziprozitätsgesetzes gilt:

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_m = 1.$$

Dabei ist $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m$ das m-te Normenrestsymbol, d.h. roh definiert:

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_m = 1 \quad \begin{array}{l} \text{dann u. nur dann, wenn } \beta \equiv N(\mathsf{A}_n) \bmod \mathfrak{p}^n \\ \mathsf{A}_n \text{ aus } k\,(\sqrt[m]{\alpha}) \text{ für belibig hohe } n. \end{array}$$

Diese Formel dient als Grundlage für die Aufstellung der sog. *expliziten* Reziprozitätsformeln, d.h. den allgem. Analoga zu:

$$\left(\frac{a}{b}\right) : \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\,\frac{b-1}{2}} \qquad \text{wenn} \qquad \left\{ \begin{array}{c} a, b \text{ prim zu } 2 \\ a > 0 \end{array} \right\}.$$

In dieser Hinsicht habe ich in einer Reihe von Arbeiten zahlreiche Spezialresultate gefunden, zum Teil auch schon für zusammengesetzte Exponenten m. Doch sind die letzteren Untersuchungen noch nicht abgeschlossen. Ich teile daher nur die beiden eleganten Formeln für primzahliges $m = \ell$ mit:

1.)

$$\left(\frac{\alpha}{\beta}\right)_\ell : \left(\frac{\beta}{\alpha}\right)_\ell = \zeta^{S\left(\frac{\alpha-1}{\ell}\,\frac{\beta-1}{\lambda}\right)}, \qquad \text{wenn} \qquad \left\{ \begin{array}{l} \alpha \equiv 1 \bmod \ell \\ \beta \equiv 1 \bmod \lambda, \quad \lambda = 1 - \zeta \end{array} \right\}$$

in beliebigen Oberkörpern der ℓ-ten Einheitswurzeln ζ.

2.)

$$\left(\frac{\alpha}{\beta}\right) : \left(\frac{\beta}{\alpha}\right) = \zeta^{\sum_{\kappa=1}^{\ell-1} \kappa \cdot \frac{N(\alpha^{\zeta^\kappa})-1}{\ell} \cdot \frac{N(\beta^{\zeta^\kappa})-1}{\ell}}, \qquad \text{wenn} \qquad \left\{ \begin{array}{l} \alpha \equiv 1 \bmod \lambda^2 \\ \beta \equiv 1 \bmod \lambda^2, \\ \text{für } \ell = 2 \\ \text{noch } \alpha \gg 0. \end{array} \right\}$$

im Körper der ℓ-ten Einheitswurzeln ζ.

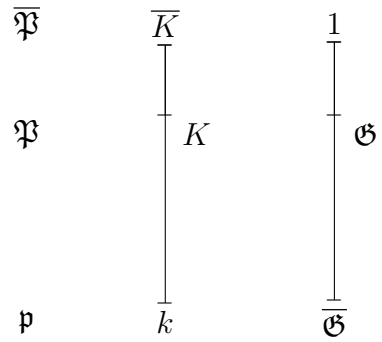
Seine schönste Anwendung fand das Artinsche Reziprozitätsgesetz auf den *Hauptidealsatz* der allgem. Klassenkörpertheorie. *Hilbert* hatte 1898 Folgendes, unter den vielen anderen längst bewiesenen Eigenschaften des Klassenkörpers, vermutet:

Im absoluten Klassenkörper K zu k werden alle Ideale des Grundkörpers k zu Hauptidealen.

Absoluter Klassenkörper heißt dabei: Klassenkörper für die Einteilung in die gewöhnlichen („absoluten“) Idealklassen (mod 1). Dies war die „populärste“ Eigenschaft des Klassenkörpers. Bewiesen war sie aber bisher nur für den Fall, daß K zyklisch über k ist.

Das Artinsche Gesetz erlaubt es doch nun, jede Aussage über die Klassen einer Klassenteilung zu übersetzen in eine Aussage über die Substitutionen der Galoisschen Gruppe des zugehörigen Klassenkörpers. Hier soll eine Aussage über die Klassen im Klassenkörper K zu k gemacht werden, nämlich über die, die durch Ideale aus k repräsentiert werden. Dazu wird man also über K noch einmal den absoluten Klassenkörper $\overline{K}$ zu bilden haben.

Es entsteht dann nach der Galoisschen Theorie folgendes Bild:



Da K nach der Theorie der *maximale* Abelsche Körper zwischen k und $\overline{K}$ ist, so ist die zu K gehörige Gruppe $\mathfrak{G}$ die *minimale* Untergruppe von $\overline{\mathfrak{G}}$ mit Abelscher Faktorgruppe, also die *Kommutatorgruppe*. Und $\overline{\mathfrak{G}}$ ist eine Gruppe mit *Abelscher Kommutatorgruppe*.

Es sei nun:

$$\mathfrak{C} = \mathfrak{C}_1^{x_1} \cdots \mathfrak{C}_r^{x_r} = \text{Basisdarst. der Klassengr. in } k$$
$$x_i \bmod f_i$$

Nach Artin sei isomorph zugeordnet:

$$\sigma\mathfrak{G} = \sigma_1^{x_1} \cdots \sigma_r^{x_r}\mathfrak{G} = \text{Basisdarst. der Gal.Gr. } \overline{\mathfrak{G}}/\mathfrak{G} \text{ von } K/k$$

Es genügt zu zeigen, daß die Basisklassen $\mathfrak{C}_i$ in K zur Hauptklasse werden.

Sei also $\mathfrak{p}_1$ ein Primideal aus $\mathfrak{C}_1$. Da $\mathfrak{p}_1^{f_1}$ als früheste Potenz in der Hauptklasse liegt, zerfällt

$$\mathfrak{p}_1 = \mathfrak{P}_{11} \cdots \mathfrak{P}_{1g} \quad \text{mit} \quad N(\mathfrak{P}_{1\nu}) = \mathfrak{p}_1^{f_1}$$

Man stellt leicht fest, daß die $\mathfrak{P}_{1\nu}$ zu einem $\mathfrak{P}_i$ aus ihnen konjugiert sind, und in folgender Weise entstehen

$$\mathfrak{p}_1 = \mathfrak{P}_1^{(1+\sigma_2+\cdots+\sigma_2^{f_2-1})\cdots(1+\sigma_r+\cdots+\sigma_r^{f_r-1})}$$

wobei $\mathfrak{P}_1^{\sigma} = \sigma\mathfrak{P}_1$ ist.

Um nun die Klasse von $\mathfrak{p}_1$ in K zu bilden, multipliziere man einfach die Klassen der richtigen $\sigma\mathfrak{P}_1$ in K. Wir müssen also diese Klassen durch Substitutionen aus $\mathfrak{G}$ ausdrücken. Nun kann die Frobeniussche Zuordnung auch für $\overline{K}/k$ gemacht werden, in folgender Weise

$$\overline{\mathsf{A}}^{N(\mathfrak{p})} \equiv \sigma\overline{\mathsf{A}} \bmod \overline{\mathfrak{P}} \text{ nicht mehr notw. mod } \mathfrak{p};$$

dann $\overline{\mathfrak{P}} \to \sigma$ für $\overline{K}/k$.

Auf die A aus K angewandt:

$$\mathsf{A}^{N(\mathfrak{p})} \equiv \sigma\mathsf{A} \bmod \overline{\mathfrak{P}} \text{ also mod } \mathfrak{p};$$

dann $\mathfrak{p} \to \sigma\mathfrak{G}$ für K/k.

Also haben obige σ_i folgende Bedeutung:

$$\overline{\mathsf{A}}^{N(\mathfrak{p}_i)} \equiv \sigma_i\overline{\mathsf{A}} \bmod \overline{\mathfrak{P}}_i \quad \text{d.h.} \quad \overline{\mathfrak{P}}_i \to \sigma_i \quad \text{für} \quad \overline{K}/K,$$

wo $\overline{\mathfrak{P}}_i$ ein Primt. von $\mathfrak{p}_i$ in $\overline{K}$.

Ist nun $\mathfrak{P}_i$ der $\overline{\mathfrak{P}}_i$ entsprechende Primteiler in K, so folgt:

$$N(\mathfrak{P}_i) = N(\mathfrak{p}_i)^{f_i}, \qquad \text{also}$$
$$\mathsf{A}^{N(\mathfrak{P}_i)} \equiv \sigma_i^{f_i}\overline{\mathsf{A}} \bmod \overline{\mathfrak{P}}_i \quad (\text{also mod } \mathfrak{P}_i);$$
$$\text{d.h.} \qquad \mathfrak{P}_i \to \sigma_i^{f_i} \quad \text{für } \overline{K}/K.$$

Ist ferner σ irgendeine Substitution, so folgt

$$\sigma\overline{\mathsf{A}}^{N(\sigma\mathfrak{P}_i)} \equiv \sigma\sigma_i^{f_i}\sigma^{-1}\sigma\overline{\mathsf{A}} \bmod \sigma\overline{\mathfrak{P}}_i;$$

$$\text{d.h.} \quad \sigma\overline{\mathfrak{P}}_i = \overline{\mathfrak{P}}_i^{\sigma} \to \sigma\sigma_i^{f_i}\sigma^{-1} = \sigma_i^{f_i\sigma} \quad \text{für} \quad \overline{K}/K.$$

Daher:

$$\mathfrak{p}_1 = \mathfrak{P}_1^{(1+\sigma_2+\cdots\sigma_2^{f_2-1})(1+\cdots)\cdots(1+\cdots)} \to \sigma_1^{f_1(1+\sigma_2+\cdots)\cdots(1+\sigma_r+\cdots)}$$

wegen der durch Artin bewiesenen *Isomorphie* der Zuordnung für $\overline{K}/K$.

$\sigma_1^{f_1}$ ist eine Substitution aus der Kommutatorgruppe $\mathfrak{G}$.

Dann und nur dann, wenn die symb. Potenz $\sigma_1^{f_1(1+\sigma_2+\cdots)\cdots(1+\sigma_r+\cdots)}$ davon, d.h. also ein Produkt aus transformierten, gleich 1 ist, ist $\mathfrak{p}_2$ in K in der Hauptklasse.

Der Hauptidealsatz wird also bewiesen sein, wenn die Relation

$$\sigma_1^{f_1(1+\sigma_2+\cdots+\sigma_2^{f_2-1})\cdots(1+\sigma_r+\cdots+\sigma_r^{f_r-1})} = 1$$

und die entsprechenden anderen für Gruppen mit Abelscher Komm. Gruppe bewiesen ist.

Auf Grund dieser *Artin*schen Reduktion des Problems auf ein rein-gruppentheoretisches Problem ist es *Furtwängler* eben gelungen, den Nachweis tatsächlich zu erbringen.

Die *Artin*sche Methode ist weitertragend. Sie ermöglicht die Behandlung ganz allgemeiner entsprechender Probleme.

Man kann mit ihr alle Fragen behandeln, die von folgendem Typus sind:

Gegeben eine Klassenteilung nach H in k. Dazu gibt es einen Klassenkörper K. Gegeben eine Klassenteilung nach G in K. In welche Klasse nach G fällt eine Klasse nach H?

Insbesondere ermöglicht die Artinsche Methode zu untersuchen, wie sich der Prozeß der Hauptidealisierung in den Unterkörpern des abs. [2] Klassenkörpers vollzieht [3]. Die Gesetze dafür gehören zu den reizvollsten Problemen der Gegenwart.

---

2. undeutlich
3. undeutlich

1.5 Erlangen 1929

Kummer's ideale Zahlen.

(Vortrag Erlangen, 15. Juni 1929)

Ich will nachstehend über diejenige geniale Idee Kummer's erzählen, die den Ausgangspunkt für die großartige moderne Entwicklung der Zahlentheorie gebildet hat.

E. Kummer lebte von 1810-1893, zuerst in Breslau, später in Berlin. Die hier zu besprechende Entdeckung fällt in das Jahr 1846 (wo er also 36 Jahre alt war) und steht in Crelle's Journal, Bd. 135. Zur ungefähren Orientierung über den Zeitpunkt mag noch gesagt werden: *Gauss* stand damals im 70. Lebensjahr und starb 1855, *Dirichlet* hatte seine berühmten Arbeiten über die Klassenzahl quadratischer Formen bereits geschrieben und war 41 Jahre alt, Kummer's Haupt- und Lieblingsschüler *Kronecker* war 23 Jahre alt und hatte gerade ein Jahr vorher mit einer Arbeit über einen eng verwandten Gegenstand: De unitatibus complexis promoviert.

Kummer kam als junger Mann mit einer Arbeit zu Dirichlet, die den großen Fermatschen Satz mittels der Zahlentheorie der aus Einheitswurzeln gebildeten ganzen Zahlen, sog. *Kreisteilungszahlen*, behandelte. In seinem jugendlichen Forscherdrang hatte aber Kummer einen Umstand ganz übersehen, der Dirichlet und wohl auch schon Gauss gut bekannt war, daß nämlich für diese Kreisteilungszahlen die Eindeutigkeit der Primzahlzerlegung verloren geht. Damit fiel Kummer's Beweis für die Unmöglichkeit der Fermatschen Gleichung unter den Tisch. Aber Kummer ließ sich dadurch nicht entmutigen. Er trat in ganz eingehende Untersuchungen der Zahlentheorie dieser Kreisteilungszahlen ein und fand in genialer Weise den richtigen Ausweg aus der Schwierigkeit des Versagens der eindeutigen Primzahlzerlegung, eben durch Einführung seiner *idealen Primfaktoren*. Er vergleicht diese Einführung mit der Einführung der imaginären Zahlen zur vollständigen Linearfaktorzerlegung ganzer rationaler Funktionen, sowie auch idealer Elemente in der Geometrie. Wenn es ihm auch nicht gelang, so zu einer völligen Erledigung des Fermat-Problems zu kommen – er fand nur, allerdings sehr bemerkenswerte, Teilresultate dazu –, so hat er damit doch den Grundstein zu der modernen Entwicklung der *algebraischen Zahlentheorie* gelegt. Seine Idee, die Einführung der idealen Zahlen, ist es, die im Prinzip allen späteren Verallgemeinerungen dieser Idee von *Kronecker*, *Dedekind*, *Hensel* zugrundeliegt, mag sie

sich dort auch in noch so abweichender äußerer Form darbieten. So hat das an sich ganz uninteressante Fermat-Problem den Anstoß zu einer großartigen Theorie gegeben, an deren Ausbau, sowohl was die Grundlagen als auch was die letzten Verästelungen anbetrifft, auch die heutige Generation noch zu tun hat.

Ich will im folgenden Kummer's Entdeckung nicht, wie Kummer selbst, an den Kreisteilungszahlen, sondern vielmehr an den einfachsten algebraischen Irrationalzahlen, den *quadratischen Irrationalzahlen* auseinandersetzen. Es soll und kann mir hier auch nicht darauf ankommen, Kummer's Entwicklungen in aller Vollständigkeit wiederzugeben. Vielmehr will ich nur versuchen, die Kummersche *Definition der idealen Zahlen* möglichst klar, verständlich und naturgemäß herauszuarbeiten.

Wir betrachten als Verallgemeinerung der gewöhnlichen ganzen Zahlen hier die ganzen quadratischen Irrationalzahlen

$$\alpha = a + b\sqrt{D}$$

die aus einer *festen* irrationalen Quadratwurzel aus einer ganzen *Zahl D* entspringen, wenn a, b beliebige ganze rationale Zahlen sind.

Im folgenden nenne ich[1] diese kurz quadratische Irrationalzahlen und bezeichne sie mit griechischen Buchstaben.

Das Ziel der Betrachtung ist, im Bereiche dieser Zahlen eine Zahlentheorie zu entwickeln, die zu der Zahlentheorie der ganzen rationalen Zahlen weitgehendst analog ist. Insbesondere soll es darauf ankommen, eine Zerlegungstheorie dieser Zahlen in Primfaktoren zu entwickeln. Dazu mögen zunächst vorangestellt werden einige

Vorbemerkungen über die Primzahlzerlegung der ganzen rationalen Zahlen.

Hier gilt ja bekanntlich das Gesetz von der eindeutigen Zerlegbarkeit in Primzahlen. Diese einfachsten Bausteine, die Primzahlen p, haben zwei grundlegende Eigenschaften:

(1.) (Definition) *p ist nicht echt zerlegbar* (d.h. nicht *in* zwei Faktoren aufspaltbar)

(2.) (Folge aus dem Eukl. Algorithmus) *Aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$* (d.h. p ist nicht *auf* zwei Faktoren aufspaltbar)

1. undeutlich

Die Eigenschaft (2.) ist deshalb fundamental, weil aus ihr sofort die Eindeutigkeit der Primzahlzerlegung folgt. Sind nämlich [2] $g = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ zwei Zerlegungen, so folgt aus $p_1 \mid g$, daß $p_1 \mid q_1$ oder ... oder $p_1 \mid q_s$, also, daß p_1 einem q_i gleich ...

Übrigens ist (1.) eine unmittelbare Folge aus (2.). Denn aus $p = ab$ folgt nach (2.) $p \mid a$ *) [3] oder $p \mid b$, also $\pm a = p$ oder $\pm b = p$. Umgekehrt folgt aber (2.) aus (1.) erst durch den komplizierten Mechanismus des Eukl. Algorithmus oder eine verwandte Schlußweise.

Bei den Zahlen $\alpha = a + b\sqrt{D}$ kann man nun auch Primzahlen π definieren durch die Eigenschaft (1.):

(1.) *π ist nicht echt zerlegbar.*

Das „echt“ muß dabei näher präzisiert werden. Bei den gewöhnlichen ganzen Zahlen sind unechte Zerlegungen diese:

$$p = \pm p \cdot \pm 1 = \pm 1 \cdot \pm p,$$

wo also ein Faktor ± 1 eine *Einheit* ist. Hier muß man allgemein als *Einheiten* ε alle *Teiler der* 1 rechnen, also alle solchen quadr. Irr. ε, für die eine ebensolche η mit $\varepsilon\eta = 1$ existiert. Z.B. sind ± 1 Einheiten, für $D = 2$ aber z.B. auch $1 - \sqrt{2}$, $3 - \sqrt{2}$. $\pi = \alpha\beta$ heißt dann eine echte Zerlegung, wenn weder α noch β eine Einheit ist. Zahlen die sich nur um Einheiten unterscheiden, sehen wir bei unserer Zerlegungstheorie als nicht wesentlich verschieden an.

Man kann jetzt jede quadr. Irr. α in Primfaktoren zerlegen, indem man (irgendwie) soweit als möglich aufspaltet:

$$\alpha = \pi_1 \pi_2 \cdots \pi_r.$$

Daß dabei nur endlich viele Faktoren auftreten können folgt auf eine Art und Weise, die im folgenden häufig anzuwenden ist. Man ersetze überall $\sqrt{D}$ durch $-\sqrt{D}$:

$$\alpha' = \pi_1' \pi_2' \cdots \pi_r'$$

also

$$\alpha\alpha' = \pi_1\pi_1' \; \pi_2\pi_2' \cdots \pi_r\pi_r'$$

2. Wort in anderer Handschrift

$*$). d.h. $a = \lambda p$, und λ ganz, also $p = \lambda p b$, d.h. $\lambda b = 1$, also λ Einheit, d.h. a und b gleich bis auf einen Einheitsfaktor.

3. Fußnote in anderer Handschrift

Nun ist

$$\alpha\alpha' = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D$$

ganz rational. Ebenso sind $\pi_1\pi_1', \ldots \pi_r\pi_r'$ ganz rational und keine Einheiten, da sonst $\pi_1, \ldots, \pi_r$ solche wären. Also ist die Anzahl r beschränkt.

Für diese Primfaktoren geht nun aber die Eigenschaft (2.) und damit die Eindeutigkeit der Zerlegung unter Umständen verloren. Wenn dennoch (2.) gilt:

(2.) *Aus* $\pi \mid \alpha\beta$ *folgt* $\pi \mid \alpha$ *oder* $\pi \mid \beta$,

so nennen wir π für den Augenblick *echte* Primzahl des Bereichs unserer quadr. Irr.

Wir wollen nun diese Frage genauer prüfen, insbesondere auch die Existenz unechter Primzahlen einsehen. Es ist gut, bei diesen Untersuchungen von vorneherein Kummer's Idee als leitenden Gesichtspunkt an die Spitze zu stellen. Diese Idee ist: Die unechten Primzahlen sind in Wahrheit zusammengesetzt aus gewissen idealen Primfaktoren, (um deren klare Herausschälung es sich handelt). Und wenn $\pi \mid \alpha\beta$ aber nicht $\pi \mid \alpha$ und nicht $\pi \mid \beta$, so ist das ebenso, als wenn die zusammengesetzte Zahl $6 = 2 \cdot 3$ die Eigenschaft hat:

$$6 \mid 10 \cdot 21 \quad \text{aber nicht } 6 \mid 10 \text{ und nicht } 6 \mid 21$$

Um nun alle idealen Primfaktoren zu erfassen, die als Faktoren irgendwelcher quadr. Irr. unseres Bereichs in Frage kommen, genügt es, die *gewöhnlichen ganzen Zahlen* in *ideale* Faktoren zu zerlegen, denn $\alpha = a + b\sqrt{D}$ kommt ja als Faktor in der Norm $N(\alpha) = \alpha\alpha' = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D$ vor. Und die Eindeutigkeit (der Zerlegung in ideale Primfaktoren) [4] im Sinne (2.) vorausgesetzt, genügt es dann weiter, die *gewöhnlichen Primzahlen* p in *ideale* Faktoren zu zerlegen.

Wir beschäftigen uns daher zuvor mit der Frage der Zerlegung der gewöhnlichen Primzahlen p in *reale* (ganze) [5] Faktoren (unseres Bereichs) [6], bestimmen also die (echten oder unechten) Primzahlen unseres Bereichs, die bei der Zerlegung der gewöhnlichen Primzahlen auftreten□□□ (aber keineswegs alle Primz. unseres Bereichs erschöpfen, z.B. ist für zusammengesetztes D die Zahl $\sqrt{D}$ Primzahl, aber nicht Teiler einer gewöhnlichen Primzahl, sondern nur Teiler von D). [7]

4. in anderer Handschrift
5. dito
6. dito
7. Klammerinhalt stellenweise in anderer Handschrift umformuliert

Zerlegung von p in reale (echte oder unechte) Primzahlen. [8]

Sei $\pi = x + y\sqrt{D}$ ein echter Teiler von p und keine Einheit, sodaß also

$$p = \pi\gamma$$

eine echte Zerlegung ist. [9] Dann ist

$$\begin{aligned} \pi\gamma &= p \\ \pi\pi' &= g \quad \text{eine ganz rationale Zahl.} \end{aligned}$$

Wenn dies g nicht durch p teilbar wäre, folgte $kp + \ell g = 1$, also

$$\pi(k\gamma + \ell\pi') = 1,$$

während doch π keine Einheit sein sollte. Also ist

$$g = \pi\pi' = x^2 - y^2 D \equiv 0 \ (p)$$

Hierbei ist nun

$$y \not\equiv 0 \ (p).$$

Denn sonst wäre auch $x \equiv 0 \ (p)$, also $\pi \equiv 0 \ (p)$, und somit π kein *echter* Teiler von p (sondern von p höchstens um eine Einheit unterschieden).

Folglich folgt in bekannter Weise:

$$u^2 - D \equiv 0 \ (p), \quad \text{d.h.} \left(\frac{D}{p}\right) = +1 \quad D \textit{ quadr. Rest nach } p$$

als *notwendige Bedingung der Zerfällbarkeit von p.*

Ferner ist dann auch $\pi' \mid p$, also $\pi\pi' \mid p^2$, und somit $\pi\pi'$ als ganze rationale Zahl:

$$\pi\pi' = \pm p \quad \text{oder} \quad \pm p^2,$$

denn ± 1 kommt nicht in Frage, weil π keine Einheit. Auch $\pm p^2$ kann nun nicht sein. Denn sonst folgte aus $\pi\gamma = p$, $\pi\pi'\gamma\gamma' = p^2$, daß $\gamma\gamma' \pm 1$ wäre, was wieder gegen die Annahme. Somit gilt

$$\pm p = \pi\pi',$$

8. dito
9. dito

d.h. $\gamma = \pm\pi'$. Hierbei sind schließlich π *und* π' *Primzahlen.* Denn aus $\pi = \alpha\beta$ folgte $\pm p = \alpha\alpha'\beta\beta'$.

Damit ist gezeigt, *daß eine Primzahl p nur dann echt zerlegbar sein kann, wenn D quadr. Rest nach p ist, und daß dann die Zerfällung, wenn vorhanden von der Form* $\pm p = \pi\pi'$ *ist, wo* π *und* π' *Primzahlen sind.*

Bei der Zerlegung aller gewöhnlichen Primzahlen p in reale Primfaktoren unseres Bereichs treten also folgende drei Fälle auf: □□□

a.) D quadr. Nichtrest nach p, dann p selbst Primzahl auch [10] im Bereich der qu. Irr.

b.) D quadr. Rest nach p und $\pm p = \pi\pi'$, wo π, π' Primzahlen im Bereich der qu. Irr.

c.) D quadr. Rest nach p und $\pm p \neq \pi\pi'$, also p selbst Primzahl im Bereich der qu. Irr.

Wir fragen nun weiter welchen von diesen, auf Grund der Eigenschaft (1.) als Primzahlen zu bezeichnenden Zahlen auch die Eigenschaft (2.) zukommt, d.h. *welche dieser Primzahlen echt sind.*

a.) *Diese Primzahlen p sind echt.* Sei nämlich $p \mid \alpha\beta$, dann $p \mid \alpha\alpha'\beta\beta'$, also etwa $p \mid \alpha\alpha'$. Ist $\alpha = a + b\sqrt{D}$, also $\alpha\alpha' = a^2 - b^2 D$, so folgt also $a^2 - b^2 D \equiv 0\ (p)$. Wäre darin $b \not\equiv 0(p)$, so wäre nach obigem D quadr. Rest nach p. Also ist $b \equiv 0$, $a \equiv 0(p)$, d.h. $\alpha \equiv 0(p)$, $p \mid \alpha$.

b.) *Auch diese Primzahlen* π, π' *sind echt.* Um das einzusehen, brauchen wir einen Hilfssatz, der für die Kummersche Idee entscheidend ist:

Es seien $\pm u$ die beiden Wurzeln von $u^2 \equiv D\ (p)$, (die auch zusammenfallen können, wenn nämlich $D \equiv 0\ (p)$).

Aus

$$\pm p = x^2 - y^2 D \equiv 0\ (p)$$

folgt dann

$$x^2 - y^2 u^2 = (x + yu)(x - yu) \equiv 0(p)$$

also

$$x + yu \equiv 0\ (p) \qquad \text{oder} \qquad x - yu \equiv 0\ (p).$$

Ohne Einschränkung sei

$$x + yu \equiv 0\ (p).$$

10. dito

Dann gilt:

Hilfssatz. *Dann und nur dann ist*

$$\alpha = \alpha(\sqrt{D}) = a + b\sqrt{D} \quad \textit{teilbar durch} \quad \pi = x + y\sqrt{D}$$

wenn

$$\alpha(u) = a + bu \quad \textit{teilbar durch} \quad p$$

ist. – Entsprechend für π' *und* $-u$.

Beweis: 1.) Ist $\alpha \equiv 0\ (\pi)$, also $\alpha = \pi\gamma$, ausführlich

$$a + b\sqrt{D} = (x + y\sqrt{D})(g + h\sqrt{D})$$

so bedeutet das

$$\begin{array}{rcl} a & = & xg + yhD \equiv xg + yhu^2\ (p) \\ b & = & xh + yg \\ \hline a + bu & \equiv & xg + yhu^2 + xhu + ygu\ (p) \\ & \equiv & (x + yu)(g + hu)\ (p) \\ & \equiv & 0\ (p). \end{array}$$

2.) Ist $a + bu \equiv 0\ (p)$, so zeige ich $\alpha\pi' \equiv 0\ (p)$, was ja $\alpha \equiv 0\ (\pi)$ ergibt. Das folgt so:

$$\alpha\pi' = (a + b\sqrt{D})(x - y\sqrt{D}) = (ax - byD) + (bx - ay)\sqrt{D}$$

Nun ist aber

$$\begin{array}{rcl} ax - byD & \equiv & ax - byu^2 \equiv ax + ayu \equiv a(x + yu) \equiv 0\ (p) \\ bx - ay & \equiv & bx + byu \equiv b(x + yu) \equiv 0\ (p). \end{array}$$

Damit ist der Hilfssatz bewiesen. Entsprechend kann man auch die Teilbarkeit durch höhere Potenzen π^n auf die Kongruenzen $a + bu \equiv 0\ (p^n)$ zurückführen, wenn man unter u nur gleich eine Wurzel von $u^2 \equiv D\ (p^n)$ versteht. Das erfordert allerdings unter Umständen die Einschränkung $p \neq 2$. Ich gehe hier nicht näher darauf ein.

Die π, π' in b.) sind jetzt sofort als *echt* erkannt. Denn aus $\pi \mid \alpha\beta$ folgt $p \mid \alpha(u)\beta(u)$, also etwa $p \mid \alpha(u)$ und somit $\pi \mid \alpha$.

Insbesondere folgt daraus die *Eindeutigkeit* der Zerlegung $\pm p = \pi\pi'$ bis auf Einheitsfaktoren.

c.) *Diese Primzahlen p sind unecht.* Denn hier ist zwar

$$p \mid u^2 - D, \quad \text{d.h.} \quad p \mid (u + \sqrt{D})(u - \sqrt{D})$$

aber

$$p \nmid u + \sqrt{D} \quad \text{und} \quad p \nmid u - \sqrt{D}.$$

Solche p gibt es tatsächlich für manche D, z.B. für $D = 6$:

$$p = 2, 3 \qquad \left\{ \begin{array}{l} D \equiv 0^2 \ (2) \\ D \equiv 0^2 \ (3) \end{array} \right.$$

$$\left. \begin{array}{l} \pm 2 \neq \pi\pi' = x^2 - 6y^2 \\ \pm 3 \neq \pi\pi' = x^2 - 6y^2 \end{array} \right\}, \text{ wie leicht zu sehen}$$

Mehrdeutigkeit:

$$6 = 2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}.$$

Oder für $D = -5$:

$$p = 3, 7 \qquad \begin{array}{l} D \equiv 1^2 \ (3) \\ D \equiv 3^2 \ (7) \end{array}$$

$$\left. \begin{array}{l} \pm 3 \neq \pi\pi' = x^2 + 5y^2 \\ \pm 7 \neq \pi\pi' = x^2 + 5y^2 \end{array} \right\}, \text{ wie leicht zu sehen.}$$

$$\text{Mehrdeutigkeiten: } 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

Vom Kummerschen Standpunkt handelt es sich nun darum, diese letzteren unechten Primzahlen p in ideale Faktoren aufzuspalten.

Kummer sagt so: In der Chemie kann es vorkommen, daß man einen zusammengesetzten Stoff tatsächlich in seine Elemente zerlegen kann. Es kann aber auch sein, daß eine isolierte Darstellung der Elemente (damals z.B. des Fluors) auf keine Weise gelingt. Dann ist man zur Erkenntnis, ob und zu welchem Index das betr. Element in einem gegebenen Stoff enthalten ist, auf indirekte Verfahren der chemischen Analyse angewiesen, etwa das Zusetzen von Reagentien, die dann das Vorhandensein des betr. Elementes durch Niederschlag anzeigen. Und die betr. Elemente sind letzten Endes nur auf diese indirekte Weise definiert, nicht durch konkretes Aufweisen des von [11] allen anderen getrennten Elements. Dieses indirekte Verfahren kann selbstverständlich auch oft mit Vorteil dort angewandt werden, wo an sich das direkte der Aufspaltung noch funktioniert.

11. undeutlich

In unserem Falle sind nun die gesuchten, idealen Primfaktoren der realen Primzahlen p (mit D quadr. Rest nach p) die Elemente. Im Falle b.) können wir sie separiert darstellen, in der Form $\pi = x+y\sqrt{D}$, $\pi' = x-y\sqrt{D}$, können uns dagegen auch von ihrem Vorhandensein in irgendeinem zusammengesetzten Element $\alpha = \alpha(\sqrt{D})$ durch die folgende *Reagenz* überzeugen:

Man bilde $\alpha(\pm u)$ und prüfe, ob das durch p teilbar ist und zu welchem Exponenten p darin aufgeht, wobei $\pm u$ die beiden Lösungen von $u^2 \equiv D(p^N)$ für hinreichend großes N sind.

Diese *Reagenz* bleibt aber ohne weiteres anwendbar, wenn auch die reale Zerlegung (von p) [12] fortfällt. Und sie definiert dann für jedes solche p zwei zugehörige ideale Primfaktoren $\mathfrak{p}$ und $\mathfrak{p}'$. Also explizit:

$$\begin{aligned} \alpha(\sqrt{D}) &\equiv 0 \ (\mathfrak{p}^n) \quad , \quad \text{wenn} \quad \alpha(u) \equiv 0 \ (p^n) \\ \alpha(\sqrt{D}) &\equiv 0 \ (\mathfrak{p}'^n) \quad , \quad \text{wenn} \quad \alpha(-u) \equiv 0 \ (p^n). \end{aligned}$$

Dabei u Wurzel von

$$u^2 \equiv D(p^N)$$

für $N \geqq n$.

Diese Primfaktoren $\mathfrak{p}, \mathfrak{p}'$ sind zwar unter Umständen nicht durch eine reale Zerlegung faßbar, aber es steht doch von ihnen genau fest, ob und zu welchen Potenzen sie in jeder realen Zahl α aufgehen. Insbesondere gehen sie in p selbst genau zur 1. Potenz auf. Da p keine weiteren idealen Primfaktoren hat, schreibt man daher auch

$$p = \mathfrak{p}\mathfrak{p}'.$$

Entsprechend setzt man

$$\alpha = \mathfrak{p}^m \mathfrak{q}^n \cdots ,$$

wenn $\mathfrak{p}, \mathfrak{q}, \ldots$ die Gesamtheit aller in α aufgehenden realen und idealen Primfaktoren bezeichnet, jeweils zum richtigen Exponenten. Diese Gleichung ist natürlich so zu verstehen, daß links eine beliebige Einheit als Faktor angebracht werden darf. Sonst aber nichts, denn einer der nun anschließend bewiesenen Kummerschen Hauptsätze ist, daß α bis auf eine Einheit durch das Aggregat seiner Primfaktoren bestimmt ist. Umgekehrt ist diese Zerlegung eindeutig. Denn die Regel, nach der sie definiert ist, ist eindeutig. Ferner ist sie endlich.

12. dito

Man kann mit ihr rechnen, wie mit der Primfaktorzerlegung der gewöhnlichen ganzen Zahlen, d.h. indem man die Exponenten beim Multiplizieren addiert. Insbesondere gilt:

$$\text{aus} \quad \mathfrak{p} \mid \alpha\beta \quad \text{folgt} \quad \mathfrak{p} \mid \alpha \quad \text{oder} \quad \mathfrak{p} \mid \beta,$$

ganz genau nach dem Schema, wie oben für die π. Die idealen Primfaktoren haben also in der Tat die grundlegende Eigenschaft (2.) der gewöhnlichen Primzahlen.

1.6 Marburg 1930

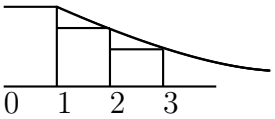
Einiges über die Riemannsche ζ-Funktion.

Koll. Vortr. Marburg 27.6.30, 4.7.30

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Absolute Konvergenz:

$$\begin{aligned}
\left|\frac{1}{n^s}\right| &= \frac{1}{n^\sigma} \qquad (s = \sigma + it) \\
\sum_{n=1}^{\infty} \frac{1}{n^\sigma} &\leqq 1 + \int_1^{\infty} \frac{1}{u^\sigma} du \\
&= 1 + \frac{1}{\sigma - 1} u^{1-\sigma} \Big|_{\infty}^{1} \\
&= 1 + \frac{1}{\sigma - 1} \qquad \text{für} \quad \sigma > 1 \\
&\quad \text{(gleichmäßig für } \sigma \geqq 1 + \delta,\ \delta > 0).
\end{aligned}$$



Für $\sigma \leqq 1$ nicht absolut konvergent, sogar divergent (klar für reelles s).

Verschiedene Methoden der analytischen Fortsetzung:

1.) Elementare Methode:

$$\begin{aligned}
\int_1^{\infty} \frac{1}{u^s} &= \tfrac{1}{s-1} \qquad \text{für} \quad \sigma > 1 \\
\sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{u^s} &= \tfrac{1}{s-1} \\
\sum_{n=1}^{\infty} \frac{1}{(n+1)^s} &= \zeta(s) - 1 \\
\hline
\sum_{n=1}^{\infty} \left\{ \frac{1}{(n+1)^s} - \int_n^{n+1} \frac{1}{u^s} \right\} &= \zeta(s) - \tfrac{1}{s-1} - 1
\end{aligned}$$

Oder auch:

$$\zeta(s) = 1 + \frac{1}{s-1} + \sum_{n=1}^{\infty} \left\{ \frac{1}{(n+1)^s} - \frac{1}{s-1} \left(\frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}} \right) \right\}$$

Oder auch durch partielle Integration:

$$\zeta(s) = 1 + \frac{1}{s-1} - s \sum_{n=1}^{\infty} \int_n^{n+1} \frac{(u-n)du}{u^{s+1}}$$

Zunächst für $\sigma > 1$. Konvergiert aber für $\sigma > 0$ (gleichmäßig für $\sigma \geqq \delta > 0$):

$$\left| \int_n^{n+1} \frac{(u-n)du}{u^{s+1}} \right| \leqq \int_n^{n+1} \frac{(u-n)du}{u^{\sigma+1}} \leqq \int_n^{n+1} \frac{du}{n^{\sigma+1}} = \frac{1}{n^{\sigma+1}}$$

Also $\zeta(s)$ mit Pol 1. Ordn. Res. 1 bei $s = 1$ behaftet, im übrigen regulär für $\sigma > 0$.

Verfahren fortsetzbar. Man integriere

$$\int_n^{n+1} \frac{(u-n)du}{u^{s+1}} = \int_0^1 \frac{udu}{(n+u)^{s+1}}$$

erneut partiell nach u. So schrittweise Fortsetzung in die ganze negative Halbebene, Schritte der Breite 1.

2.) Andere elementare Methode.

$$\begin{aligned} \zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ \varphi(s) &= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} \\ \varphi(s) &= \left(1 - \frac{2}{2^s}\right) \zeta(s) \end{aligned}$$

$\varphi(s)$ konvergiert für $\sigma > 0$ (klar für reelles s), und gleichmäßig für $\sigma \geqq \delta > 0$.

Auf $\varphi(s)$ kann man jetzt Summierungsverfahren der arithmetischen Mittel wiederholt anwenden und gelangt wieder in Schritten der Breite 1 zur Fortsetzung in die ganze negative Halbebene.

3.) Erste Riemannsche Methode.

$$\begin{aligned}\Gamma(s) &= \int_0^\infty e^{-t}t^{s-1}dt \qquad (\sigma > 0)\\ \Gamma(s) &= n^s\int_0^\infty e^{-nt}t^{s-1}dt\\ \frac{1}{n^s} &= \frac{1}{\Gamma(s)}\int_0^\infty e^{-nt}t^{s-1}dt\end{aligned}$$

Modifikation:

$$\frac{1}{n^s} = \frac{1}{(n^2)^{\frac{s}{2}}} = \frac{1}{\Gamma\left(\frac{s}{2}\right)}\int_0^\infty e^{-n^2t}t^{\frac{s}{2}-1}dt = \frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\int_0^\infty e^{-n^2\pi t}t^{\frac{s}{2}-1}dt$$

$$\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} = \frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\int_0^\infty \sum_{n=1}^\infty e^{-n^2\pi t}t^{\frac{s}{2}-1}dt \qquad (\sigma > 0)$$

(Reihe konvergiert gleichmäßig für $0 \leqq t \leqq \infty$)

$$\sum_{n=-\infty}^{\infty} e^{-n^2\pi t} = \vartheta_{00}(0, it)$$

$$= \vartheta_{00}\left(0, -\frac{1}{it}\right) = \frac{1}{\sqrt{t}}\sum_{n=-\infty}^{+\infty} e^{-\frac{n^2\pi}{t}}$$

□□□ $$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty \frac{\vartheta_{00}(it)-1}{2}\cdot t^{\frac{s}{2}-1}dt$$

$$= \int_0^1 + \int_1^\infty$$

Im $\int_0^1$ Ausführung der Theta-Transformation und $t \to \frac{1}{t}$. Dadurch Überführung in $\int_1^\infty$. So erkennt man Fortsetzbarkeit in die ganze Ebene und Funktionalgleichung:

$$F(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) \qquad \text{inv. bei} \quad s \to 1-s.$$

4.) Zweite Riemannsche Methode

$$\begin{aligned}\frac{1}{n^s} &= \frac{1}{\Gamma(s)}\int_0^\infty e^{-nt}t^{s-1}dt\\ \zeta(s) &= \frac{1}{\Gamma(s)}\int_0^\infty \frac{e^{-t}}{1-e^{-t}}t^{s-1}dt = \frac{1}{\Gamma(s)}\int_0^\infty \frac{t^{s-1}}{e^t-1}dt \quad (\sigma>1)\end{aligned}$$

Man betrachte

$$F(s) = \frac{1}{2\pi i}\int_{\rightrightarrows} \frac{t^{+(s-1)}}{1-e^{-t}}dt \qquad t^{s-1} = e^{(s-1)\log t}$$

Einerseits

$$\begin{aligned}F(s) &= \frac{1}{2\pi i}\int_{-\infty}^0 \frac{e^{+(s-1)[\log(-t)-\pi i]}}{1-e^{-t}}dt + \frac{1}{2\pi i}\int_0^{-\infty}\frac{e^{+(s-1)[\log(-t)+\pi i]}}{1-e^{-t}}dt\\ &= \frac{+(e^{(s-1)\pi i}-e^{-(s-1)\pi i})}{2\pi i}\int_0^\infty \frac{t^{s-1}}{e^{+t}-1}dt\\ &= \frac{\sin(s-1)\pi}{\pi}\Gamma(s)\zeta(s) \qquad (\sigma>1)\end{aligned}$$

Andererseits

$$F(s) = -\text{Residuensumme für die } t = 2n\pi i \qquad \sigma<0$$

□□□

$$\begin{aligned}F(s) &= -\sum_{n=1}^\infty (2n\pi i)^{s-1} - \sum_{n=1}^\infty (-2n\pi i)^{s-1}\\ &= -(2\pi)^{s-1}\zeta(1-s)\left(e^{\frac{s-1}{2}\pi i}+e^{-\frac{s-1}{2}\pi i}\right)\\ &= -(2\pi)^{s-1}\zeta(1-s)2\cos\frac{s-1}{2}\pi\end{aligned}$$

Also

$$\begin{aligned}\frac{1}{\pi}\sin\frac{s-1}{2}\pi\Gamma(s)\zeta(s) &= -(2\pi)^{s-1}\zeta(1-s)\\ \frac{2\cos\frac{s\pi}{2}\Gamma(s)\zeta(s)}{(2\pi)^s} &= \zeta(1-s)\end{aligned}$$

(andere Form der Funktionalgleichung, hängt mit der ursprünglichen durch elementare Transformation zusammen)

5.) Meine Methode.

Elementar, aber kräftiger als bisherige elementare Methoden. Liefert Fortsetzung gleich mit einem Schritt, wie Riemannsche Methoden, leider aber nicht die Funktionalgleichung. Gibt aber der Funktionalgleichung eine rein reelle Bedeutung, und zwar in einer einzigen Formel, gültig für $\sigma > 1$, während die obigen elementaren Methoden das nur mit mehreren Formeln, für jeden Streifen der Breite 1 eine neue, tun.□□□

1.7 Göttingen 1931

Über Schiefkörper.

13.1.1931 Vortrag in der Mathematischen Gesellschaft Göttingen

Nachdem die kommutative *algebraische Zahlentheorie* heute zu einem gewissen *Abschluß* gelangt ist, was die Theorie der *Abelschen* Zahlkörper betrifft, und zu einem gewissen *Stillstand*, was die Theorie der *Galoisschen* Zahlkörper betrifft, hat sich das Interesse der Verallgemeinerung ins nichtkommutative Gebiet zugewandt, nämlich der Algebra und Arithmetik der *hyperkomplexen Zahlsysteme*. Neben dem großen Interesse, das diese neue Theorie durch die Schönheit und Einfachheit ihrer Hauptresultate und die Beziehungsreichheit zu anderen Gebieten und Fragestellungen beansprucht, erhofft man von ihr insbesondere auch eine Förderung großer noch offener Fragen im kommutativen Spezialfall, der algebraischen Zahlentheorie.

Den ersten entscheidenden Vorstoß in die Theorie der hyperkomplexen Zahlsysteme hat *Wedderburn* gemacht, indem er die *algebraische Struktur* dieser Systeme weitgehend enthüllte. Unter Beschränkung auf die *halbeinfachen* hyperkomplexen Systeme, d.h. solche deren Diskriminante nicht verschwindet, lauten die Wedderburnschen Hauptsätze:

I. *Jedes halbeinfache hyperkomplexe System läßt sich (eindeutig bis auf die Reihenfolge) als direkte Summe einfacher Systeme darstellen (und umgekehrt).*

Hierdurch wird die Strukturfrage in jeder nur wünschenswerten Durchsichtigkeit auf den Fall der *einfachen* Systeme zurückgeführt, d.h. solcher, die keine echten invarianten Teilsysteme besitzen.

II. *Jedes einfache hyperkomplexe System läßt sich (bis auf Transformation eindeutig) als volles Matrizensystem aus einem Schiefkörper darstellen (und umgekehrt).*

Hierdurch wird die Strukturfrage weiter in völliger Durchsichtigkeit auf den Fall der *Schiefkörper* zurückgeführt, d.h. der nullteilerfreien Systeme. Solche Schiefkörper sind Systeme, die bis auf das kommutative Gesetz der Multiplikation allen formalen Gesetzen algebraischer Erweiterungskörper endlichen Grades des Koeffizientenkörpers genügen.

Über die algebraische Struktur der Schiefkörper hat man nun heute zwar eine Reihe von wichtigen Einsichten, aber doch noch kein abschließendes Resultat. Ich will darüber hier einiges erzählen.

Zunächst hat man als dritten Hauptsatz von Wedderburn:

III. *Jeder endliche Schiefkörper ist kommutativ.*

Dieses Resultat ist von entscheidender Bedeutung für die *arithmetische Theorie*, die sich im Anschluß an die Wedderburnsche Strukturtheorie in neuester Zeit entwickelt hat. Einerseits haben *Artin* und *Brandt* die Arithmetik der halbeinfachen hyperkomplexen Zahlsysteme mit rationalem Koeffizientenkörper in weitgehender Analogie zur kommutativen algebraischen Zahlentheorie aufgebaut. Sie gehen dabei nach dem Muster der Dedekindschen Idealtheorie vor. Ich selbst habe einen Aufbau der Artin-Brandtschen Theorie (mit leichter Verallgemeinerung auf einen algebraischen Zahlkörper endlichen Grades als Koeffizientenkörper) gegeben, der in Fortführung der ursprünglichen *Speiser*schen Ansätze nach dem Muster der *Hensel*schen p-adischen Grundlegung der algebraischen Zahlentheorie vorgeht.

Diese arithmetische Theorie ist nicht nur eine Krönung des algebraischen Unterbaus, sondern strahlt auch ihre Auswirkungen auf die Struktur dieses Unterbaus zurück.

Zur Durchführung meines Aufbaus mußte ich nämlich das Strukturproblem für Schiefkörper über *p-adischem Koeffizientenkörper* lösen. Aus dieser Lösung haben sich mir jetzt wichtige Einsichten in das Strukturproblem für Schiefkörper mit *algebraischem Zahlkörper endlichen Grades als Koeffizientenkörper* ergeben, über die ich nachstehend berichten will.

Zunächst will ich jedoch vorausschicken, was man allgemein über die Struktur der Schiefkörper weiß. Ich setze dabei gleich voraus, daß der Koeffizientenkörper ein algebraischer Zahlkörper K von endlichem Grade ist. Ist S ein Schiefkörper über K, so ist das Zentrum Z von S, d.h. die Gesamtheit der mit allen Elementen von S vertauschbaren Elemente von S, eine endliche algebraische Erweiterung von K und S kann als Schiefkörper mit dem Koeffizientenkörper Z angesehen werden. Die Struktur von Z über S ist aus der kommutativen Algebra hinlänglich bekannt. Das typisch nicht-Kommutative findet sich in der Struktur von S über Z. Ohne Einschränkung kann daher vorausgesetzt werden, daß *S Schiefkörper über dem algebraischen Zahlkörper endlichen Grades K als Zentrum* ist.

Aus der Wedderburnschen Theorie ergibt sich dann leicht:

IV. *Der Rang von S über K ist eine Quadratzahl n^2, und n ist der Grad von S über K.*

Ferner haben *E. Noether* und *R. Brauer* bewiesen:

V. *S besitzt eine (und nur eine) irreduzible Matrizendarstellung vom Grade n, diese ist in Zahlkörpern L n-ten Grades über K rational wählbar. Die Gesamtheit dieser Körper L ist identisch mit der Gesamtheit der kommutativen Teilkörper n-ten Grades von S. D.h. mit der Gesamtheit derjenigen Körper n-ten Grades L, für die SL über KL in ein volles Matrizensystem zerfällt (Zerfällungskörper).*

Aus dieser Beziehung zur Theorie der irreduziblen Matrizendarstellungen hat R. Brauer eine Übersicht über alle Schiefkörper entwickelt. Er charakterisiert die Schiefkörper eineindeutig durch Klassen assoziierter *Faktorensysteme* und gibt auch formelmäßig an, wie man vom Schiefkörper zum Faktorensystem kommt und umgekehrt. Jedoch ist diese Theorie nicht eine Lösung des Strukturproblems im tiefsten Sinne, weil sie die algebraische Struktur, d.h. das Multiplikationsschema, der Schiefkörper nicht mit derselben Einfachheit und Durchsichtigkeit in Evidenz setzt, wie das die beiden ersten Wedderburnschen Struktursätze für die Struktur der halbeinfachen und einfachen Systeme relativ zur Schiefkörperstruktur tun.

Ich schildere jetzt zunächst meine Lösung des Strukturproblems im p-adischen Falle.

Sei also K_p ein p-adischer Zahlkörper, d.h. die Henselsche Erweiterung eines gewöhnlichen algebraischen Zahlkörpers K nach einem Primideal p von K. Ferner sei S_p ein Schiefkörper mit K_p als Zentrum vom Grade n (Rang n^2). Dann ist S_p über K_p von folgender Struktur:

$$S_p = K_p(\omega, \pi) = L_p(\pi)$$

wobei:

$L_p = K_p(\omega)$ ein zyklischer Körper n-ten Grades über K_p in dessen Diskriminante p nicht aufgeht, und der somit durch eine primitive $(q^n - 1)$-te Einheitswurzel ω erzeugbar ist, wo $q = N(p)$, deren Konjugierte dann $\omega, \omega^q, \omega^{q^2}, \ldots, \omega^{q^{n-1}}$ lauten.

$\pi\omega\pi^{-1} = \omega^{q^{r_p}}$ mit $(r_p, n) = 1$

$\pi^n = p$ ein Primelement zu p aus K_p.

Durch diese Relationen ist die Multiplikation in S_p völlig übersehbar: S_p entsteht aus dem zyklischen Teilkörper $L_p = K_p(\omega)$ durch Hinzunahme eines Elements π, das durch Transformation die Automorphismen der Galoisschen

Gruppe von L_p erzeugt. *E. Noether* nennt daher S_p ein *verschränktes Produkt* von L_p mit seiner Galoisschen Gruppe.

Die Größe p ist keineswegs ein invariantes Bestimmungsstück von S_p, kann vielmehr durch jedes andere Primelement zu p aus K_p ersetzt werden. Dagegen ist der Exponent r_p eine charakteristische Invariante von S_p. Neben dem Grade n gibt es also nur diese eine charakteristische Invariante r_p, d.h. es gibt genau $\varphi(n)$ Typen p-adischer Schiefkörper S_p vom Grade n über K_p als Zentrum.

Auch die nach dem E. Noether–R. Brauerschen Satze in L_p vorhandene Matrizendarstellung n-ten Grades läßt sich unmittelbar hinschreiben:

Dem Element $\alpha = \alpha_0 + \alpha_1\pi + \cdots + \alpha_{n-1}\pi^{n-1}$, wo die α_i zu L_p gehören, ist die Matrix

$$\left\| \begin{matrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \\ p\alpha_{n-1}{}' & \alpha_0{}' & \dots & \alpha_{n-2}{}' \\ \dots & \dots & \dots & \dots \\ p\alpha_1{}^{(n-1)} & p\alpha_2{}^{(n-1)} & \dots & \alpha_0{}^{(n-1)} \end{matrix} \right\|$$

zugeordnet, wo der Strahl den Automorphismus $\omega \to \omega^{q^{r_p}}$ bezeichnet.

Das Resultat ist ganz analog zu der bekannten Tatsache, daß es über dem reellen Zahlkörper K_∞, der ja ein gewisses Analogon der p-adischen Zahlkörper ist, als Zentrum nur den einzigen Schiefkörper, die Quaternionen gibt:

$$\begin{aligned} S_\infty &= K_\infty(i,j) = L_\infty(j) \\ L_\infty &= K_\infty(i) \quad \text{der Körper aller komplexen Zahlen, die einzige algebraische Erweiterung von } K_\infty, \text{ zyklisch vom Grade 2} \\ jij^{-1} &= -i \\ j^2 &= -1, \\ \text{wo} \quad \alpha &= \alpha_0 + \alpha_1 j, \qquad \alpha_0, \alpha_1 \text{ aus } L_\infty \end{aligned}$$

die Matrix

$$\left\| \begin{matrix} \alpha_0 & \alpha_1 \\ -\alpha_1{}' & \alpha_0{}' \end{matrix} \right\|$$

zugeordnet ist.□□□

Die p-adischen Schiefkörper sind hiernach durchweg als verschränkte Produkte aus zyklischen Körpern darstellbar, und sogar aus besonders einfachen zyklischen Körpern. Ich will allgemein einen Schiefkörper *S zyklisch erzeugbar* nennen, wenn er als verschränktes Produkt aus einem über dem Zentrum

K zyklischen Teilkörper L und dessen Gruppe, also in der Form darstellbar ist:

$$\begin{aligned} S &= K(\alpha,\sigma) = L(\sigma) \\ L &= K(\alpha) \quad \text{zyklisch vom Grade } n \text{ über } K \\ &\quad \alpha, \alpha', \ldots, \alpha^{(n-1)} \quad \text{Zyklus der konjugierten} \\ \sigma\alpha\sigma^{-1} &= \alpha' \\ \sigma^n &= s \quad \text{aus} \quad K, \end{aligned}$$

wo dann zu

$$\alpha = \alpha_0 + \alpha_1\sigma + \cdots + \alpha_{n-1}\sigma^{n-1}$$

die Matrix

$$\left\| \begin{matrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ s\alpha_{n-1}{}' & \alpha_0{}' & \ldots & \alpha_{n-2}{}' \\ \ldots & \ldots & \ldots & \ldots \\ s\alpha_1{}^{(n-1)} & s\alpha_2{}^{(n-1)} & \ldots & \alpha_0{}^{(n-1)} \end{matrix} \right\|$$

zugeordnet ist.

Dieser Typus ist zuerst von *Dickson* aufgestellt und untersucht. Dickson beweist:

VI. *S ist sicher dann wirklich Schiefkörper, wenn erst die n-te Potenz von s Norm einer Zahl aus $L = K(\alpha)$ ist.*

Umgekehrt leicht zu sehen:

VII. *ist S Schiefkörper, so jedenfalls s selbst nicht Norm einer Zahl aus $L = K(\alpha)$.*

Bezeichnet allgemeiner ℓ den frühesten Exponenten, sodaß s^ℓ Norm aus L wird, so ist $\ell \mid n$ und besteht aus denselben Primfaktoren wie n.

Schließlich folgt aus einem Satze von Wedderburn-Artin:

VIII. *Damit S zyklisch erzeugbar ist, ist (notwendig und) hinreichend, daß S einen maximalen Teilkörper L enthält, der zyklisch ist.*

Man kann natürlich entsprechend auch die allgemeineren Begriffe bilden: Abelsch erzeugbar, Galoissch erzeugbar, durch Körper der Gruppe $\mathfrak{G}$ erzeugbar. Das tut *Dickson* auch und stellt Untersuchungen dieser Typen an. Im p-adischen Falle lassen sich alle diese allgemeineren Typen, die sehr wohl existieren, durchweg auch zyklisch erzeugen. Das legt die Vermutung nahe:

Jeder Schiefkörper S über einem algebraischen Zahlkörper endlichen Grades K als Zentrum ist zyklisch erzeugbar.

In dieser Hinsicht weiß man bisher trivialerweise, daß das für $n = 2$ gilt, ferner durch *Wedderburn*, daß es für $n = 3$ gilt. Für $n = 4$ ist eine gewisse Normierung in den neuen darauf bezüglichen Resultaten von *Albert*. Dieser weist jedenfalls nach, daß S für $n = 4$ stets Abelsch erzeugbar ist. Sein Beweis dagegen, daß man sogar stets mit $\mathfrak{G}$ vom Typus $(2, 2)$ auskommt, muß falsch sein, denn es gibt, wie leicht zu sehen, solche zyklisch erzeugbare S mit $n = 4$, □□□ die bestimmt nicht auch durch Körper der Gruppe $\mathfrak{G}$ vom Typus $(2, 2)$ erzeugbar sind. □□□

Für den p-adischen Fall ist ferner durchweg $\ell = n$. Das legt die Vermutung nahe:

Für jeden zyklisch erzeugbaren Schiefkörper S über einem algebraischen Zahlkörper endlichen Grades K als Zentrum ist $\ell = n$.

Alle Versuche, ein Gegenbeispiel zu finden, scheiterten bisher. Für Körper *mit Unbestimmten* hat aber R. Brauer ein solches.

Die vorstehenden Ausführungen sollten vor allem dazu dienen, die Bedeutung der zyklisch-erzeugbaren Schiefkörper für die Strukturtheorie der Schiefkörper ins rechte Licht zu setzen. Das Strukturproblem wäre in denkbar einfachster Weise gelöst, wenn es gelänge, die beiden ausgesprochenen Vermutungen zu beweisen. Um ev. zu solchen Beweisen zu gelangen, wird man gut tun, die zyklisch erzeugbaren Schiefkörper genau zu untersuchen. Hier erhebt sich vor allem die Frage nach der *Kennzeichnung durch Invarianten.*

Die Darstellung als verschränktes Produkt eines zyklischen Körpers mit seiner Galoisschen Gruppe setzt nämlich zwar die Struktur in helles Licht, aber weder der zyklische Körper L noch die Zahl s sind invariante Bestimmungsstücke. Es erhebt sich also die Frage nach invarianten Bestimmungsstücken für S. Damit wird dann zugleich das *Identitätsproblem* gelöst sein:

Wann sind $S = L(\sigma)$ und $S' = L'(\sigma')$ mit $\sigma^n = s$, $\sigma'^n = s'$ identisch?

Die Lösung dieses Problems sehe ich in folgender Richtung: Für die Frage ob S wirklich Schiefkörper ist, ist das Normenverhalten von s in bezug auf den Körper L bestimmend. Das legt es nahe, die Normenrestsymbole

$$\left(\frac{s, L}{p}\right)$$

für alle Primstellen p von K ins Auge zu fassen. Diese Normenrestsymbole sind im Sinne meiner allgemeinen Normenresttheorie Abelscher Körper zu verstehen, also bestimmte Elemente der Galoisschen Gruppe von L. Wie aber soll man diese Symbole für verschiedene Körper L, L', also verschiedene, nur

abstrakt-isomorph zyklische Gruppen in Beziehung setzen? Das geht nun höchst einfach in folgender Weise:

Ist $L = K(\alpha)$ und $\sigma\alpha\sigma^{-1} = \mathfrak{s}\alpha$, also dem σ die Substitution $\mathfrak{s}$ der zyklischen Gruppe von L durch die Transformationsgleichung zugeordnet, so setze man an:

$$\left(\frac{s, L}{p}\right) = \mathfrak{s}^{e_p}.$$

Die so definierten Exponenten e_p hängen nicht davon ab, welches Element als erzeugendes der Gruppen gewählt wird. Geht man von $\mathfrak{s}$ zu $\mathfrak{s}^a$, also von σ zu σ^a über, so ist auch s durch s^a zu ersetzen, und das Normenrestsymbol durch seine a-te Potenz, e_p bleibt also invariant.

Sei ebenso

$$\left(\frac{s', L'}{p}\right) = \mathfrak{s}'^{e'_p},$$

so nenne ich

$$\left(\frac{s, L}{p}\right) = \left(\frac{s', L'}{p}\right),$$

wenn $e_p \equiv e'_p \bmod n$. Es ist zu vermuten, daß die so definierten $\left(\frac{s,L}{p}\right)$ das vollständige Invariantensystem von S bilden:

Dann und nur dann ist $S = S'$, wenn für alle Primstellen p von K

$$\left(\frac{s, L}{p}\right) = \left(\frac{s', L'}{p}\right), \text{ d.h. } \quad e_p \equiv e'_p \bmod n$$

gilt.

Vom Beweis dieser Vermutung bin ich nicht mehr ganz so weit entfernt, wie vom Beweis der beiden anderen ausgesprochenen Vermutungen; ich kann sie im Spezialfall, daß der Grad n eine *Primzahl* ist, „fast“ beweisen. Speziell für $n = 2$ ist sie schon in den Resultaten meiner Dissertation und Habilitationsschrift enthalten.

Im Primzahlfalle fällt zunächst die Schwierigkeit der zweiten Vermutung fort, es ist $\ell = n$, und also S *dann und nur dann* wirklich Schiefkörper, wenn erst s^n Norm aus L ist.

Der schwierigste Punkt beim Beweis ist die Tatsache, *daß* $\left(\frac{s,L}{p}\right)$ eine Invariante ist. In dieser Hinsicht □□□ folgt aus dem Dicksonschen Satz, angewandt im p-adischen Körper K_p und dem p-adischen System S_p ohne weiteres, daß jedenfalls die Alternative $\left(\frac{s,L}{p}\right) = 1$ oder $\neq 1$ invariant ist; denn sie entscheidet ja darüber, ob S_p kein Schiefkörper ist oder doch.

Diese Invarianztatsache ist übrigens der *Deuring*sche Beweis des rohen Vertauschungssatzes für das Hilbertsche Normenrestsymbol. Denn wenn K die n-ten Einheitswurzeln enthält, sodaß $L = K(\sqrt[n]{a})$ gesetzt werden kann, so liefert die Anwendung von $\left(\frac{s,L}{p}\right)$ auf $\alpha = \sqrt[n]{a}$ die Multiplikation mit $\left(\frac{s,a}{p}\right)$, sodaß also dies letztere Symbol als Invariante dienen kann. Dann ist aber

$$S = K(\alpha, \sigma) \quad \text{mit} \quad \left\{ \begin{array}{rcl} \alpha^n & = & n \\ \sigma\alpha\sigma^{-1} & = & \zeta\alpha, \text{ also } \alpha\sigma\alpha^{-1} = \zeta^{-1}\sigma \\ \sigma^n & = & s \end{array} \right.$$

antisymmetrisch in a und s, sodaß für die Erzeugung aus $L' = K(\sigma)$ die Invariante $\left(\frac{a,s}{p}\right)^{-1}$ wird. Es folgt also, daß beide Symbole $\left(\frac{s,a}{p}\right)$ und $\left(\frac{a,s}{p}\right)$ gleichzeitig 1 oder $\neq 1$ sind. Aus meinem schärferen Invarianzbeweis, folgt natürlich der scharfe Vertauschungssatz

$$\left(\frac{s,a}{p}\right) = \left(\frac{a,s}{p}\right)^{-1}.$$

Ich beweise nun die genaue Invarianz so, daß ich als Bindeglied zwischen $S = L(\sigma)$ und $S = L'(\sigma')$ die p-adische Erzeugung $S_p = L_p(\pi)$ einschiebe, und also nur

$$\left(\frac{s,L}{p}\right) = \left(\frac{p,L_p}{p}\right)$$

beweise. In der Tat ist, sofern wirklich $\left(\frac{s,L}{p}\right) \neq 1$ ist, S_p Schiefkörper und von der zuvor angeführten Struktur:

$$\begin{array}{cc} S_p = L_p(\pi), & L_p = K_p(\omega) \\ \pi\omega\pi^{-1} = \omega^{q^{r_p}}, & (r_p, n) = 1 \\ \multicolumn{2}{c}{\pi^n = p} \end{array}$$

Man berechnet leicht:

$$\left(\frac{p,L_p}{p}\right) = \mathfrak{p}^{-r_p^{-1}}, \qquad \text{wenn } \pi\omega\pi^{-1} = \mathfrak{p}\omega \text{ gesetzt ist,}$$

sodaß also die Behauptung

$$e_p \equiv -r_p^{-1} \bmod n$$

lautet. Hierdurch ist zugleich auch die oben herausgehobene einzige Invariante r_p der p-adischen Schiefkörper als Normenrestsymbolexponent gedeutet.

Der Nachweis von $e_p \equiv -r_p^{-1} \bmod n$ ist mir nun zunächst für alle $p \nmid n$ gelungen, ferner auch für $p \mid n$ wenn für die Verzweigungsart von p in L ein besonders einfacher Typ vorausgesetzt wird. Die Erledigung für $p \mid n$ allgemein ist nur noch eine technische Frage. □□□

Der umgekehrte Beweis ist viel einfacher. Seien zwei zyklisch erzeugte Schiefkörper n-ten Grades:

$$S = L(\sigma) \quad \text{mit} \quad \sigma^n = s, \qquad S' = L'(\sigma') \quad \text{mit} \quad \sigma'^n = s'$$

gegeben mit

$$\left(\frac{s, L}{p}\right) = \left(\frac{s', L'}{p}\right) \qquad \text{für alle } p.$$

Dann ist nach dem vorigen Beweis jedenfalls $S_p = S'_p$ für alle p. Daher ist L_p für jedes p Zerfällungskörper für S'_p [1], d.h. das direkte Produkt $S'L$ hat über KL die Eigenschaft, daß die $\overline{p}$-adische Erweiterung $(S'L)_{\overline{p}}$ für jedes $\overline{p}$ aus KL zerfällt über $(KL)_{\overline{p}}$. Nach einem Satz von Hilbert-Furtwängler zerfällt aber ein zyklisch-erzeugter Schiefkörper n-ten Grades, der für jedes $\overline{p}$ zerfällt, auch im gewöhnlichen Sinne. Das bedeutet hier, daß $S'L$ über KL zerfällt, daß also L Zerfällungskörper für S' ist. Stellt man demgemäß dar:

$$S' = L(\tau), \qquad \tau^n = t,$$

so wird nach der Voraussetzung:

$$\left(\frac{t, L}{p}\right) = \left(\frac{s, L}{p}\right),$$

also ist t von s nur um eine Norm aus L unterschieden, und das bedeutet $S' = S$.

1. undeutlich

1.8 Marburg 1931

I. Zyklische Algebren von Primzahlgrad ℓ über $\mathfrak{R}$.

Vortrag auf dem „Schiefkörper-Kongreß“, Marburg 26.2.31

$\mathfrak{A} = \mathfrak{R}(\alpha, \beta)$ α Wurzel zykl. Polyn.

$$f(x) = (x-\alpha)(x-\alpha^{\mathsf{S}})\cdots(x-\alpha^{\mathsf{S}^{\ell-1}}) \text{in } \mathfrak{K}$$

$$\beta\alpha\beta^{-1} = \alpha^{\mathsf{S}}$$

$$\beta^{\ell} = b \neq 0 \quad \text{in } \mathfrak{R}$$

$\mathfrak{A}$ einfach, Zentrum $\mathfrak{R}$, Grad ℓ, Rang ℓ^2, max. Teilkörper $L = \mathfrak{K}(\alpha)$

Kurz $\mathfrak{A} = (L, \mathsf{S}, b)$, *zyklische Erzeugung.*

Abs. irred. Darstellung $\mathfrak{D}$ in L: $\mathsf{A} = \xi_0 + \xi_1\beta + \cdots + \xi_{\ell-1}\beta^{\ell-1}$, ξ_i aus L

$$M_{\mathsf{A}} = \begin{pmatrix} \xi_0 & \xi_1 & & & \xi_{n-1} \\ b\xi_{n-1}^{\mathsf{S}} & \xi_0^{\mathsf{S}} & \xi_1^{\mathsf{S}} & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & \xi_1^{\mathsf{S}^{n-2}} \\ b\xi_1^{\mathsf{S}^{n-1}} & & & b\xi_{n-1}^{\mathsf{S}^{n-1}} & \xi_0^{\mathsf{S}^{n-1}} \end{pmatrix}$$

$\mathfrak{A}$ dann und nur dann volles Matrizensystem, wenn b Norm `[...]` L; *zerfällt*

$\mathfrak{A}$ dann und nur dann Schiefkörper, wenn erst b^{ℓ} Norm aus L; *unzerlegt*

Zerfällungskörper für $\mathfrak{A}$ vom Grade ℓ = Teilkörper von `[...]` vom Grade ℓ = Darstellungskörper für $\mathfrak{D}$ vom Grade ℓ.

Problem: Kennzeichnung durch invariante Bestimmungsstücke,
speziell *Identitätsproblem:* Wann ist $(L, \mathsf{S}, b) = (L', \mathsf{S}', b')$?
Bei *festem* L leicht lösbar:

$$\begin{aligned} \beta' &= \xi\beta^k, \qquad \xi \neq 0 \quad \text{aus} \quad L, \quad (k, \ell) = 1 \\ b' &= N(\xi)b^k \end{aligned}$$

Relative Invariante: Normklasse

II. Übergang zu $\mathfrak{R}_p$.

p Primzahl, $\mathfrak{R}_p$ p-adischer Zahlkörper
$\mathfrak{A}_p$ Erweiterung auf $\mathfrak{R}_p$, bleibt einfach mit $\mathfrak{R}_p$ als Zentrum

Entw a.) $\mathfrak{A}_p$ zerfällt (in volles Matrizensystem)

oder b.) $\mathfrak{A}_p$ bleibt unzerlegt (Schiefkörper))

a.) dann und nur dann, wenn b Norm aus L_p, insbes. wenn L_p d.h. p in L zerfällt

b.) dann und nur dann, wenn erst b^ℓ Norm aus L_p.

Im Falle b.) ist eine weitere, ausgezeichnete zyklische Erzeugung da:

$$\mathfrak{A}_p = \mathfrak{R}_p(\omega, \pi) \qquad \begin{array}{ll} \omega^{p^\ell} = \omega & \text{(primitiv)} \\ \pi\omega\pi^{-1} = \omega^{p^{r_p}}, & (r_p, \ell) = 1 \\ \pi^\ell = p & \end{array}$$

Arithmetik in $\mathfrak{A}_p$: *Alle* ganzen Elemente bilden Integritätsbereich mit nur einem Primideal $\wp = (\pi)$, $\wp^n = p$; Restklassenkörper durch ω erzeugt, endlich vom Grade ℓ.

Einzige absolute Invariante: $r_p \bmod \ell$; bei Transformation mit beliebigem Primelement π zu $\wp$ erfährt der Restklassenkörper mod $\wp$ den Automorphismus $\gamma \to \gamma^{p^{r_p}}$.

Im Falle a.) sei $r_p \equiv 0 \bmod \ell$ gesetzt.

Dann bilden die r_p absolutes Invariantensystem.

III. Deutung der Invarianten durch Normenrestsymbole.

Die Unterscheidung a.), b.) kann durch das Symbol beschrieben werden:

$$\text{a.)} \quad \left(\frac{b, L}{p}\right) = 1, \qquad \text{b.)} \quad \left(\frac{b, L}{p}\right) \neq 1 \qquad \text{(Normenrestsymbol)}$$

Nun gibt es exakte Definition dieses Symbols als Element der Galoisschen Gruppe von L, also als Potenz von S:

$$\left(\frac{b, L}{p}\right) = \mathsf{S}^{e_p}.$$

Bildungsvorschrift:

$$b_0 \equiv b \bmod f_p, \quad b_0 \equiv 1 \bmod \frac{f}{f_p} \qquad f \text{ Führer von } L$$

$$b_0 = p^k q, \qquad (q,p) = 1$$

$$\left(\frac{b,L}{p}\right) = \frac{L}{q} = \left(\frac{L}{q_1}\right)\cdots\left(\frac{L}{q_n}\right) \qquad q = q_1 \ldots q_n$$

$\left(\frac{L}{q_i}\right)$ = Erz. d. Zerl. Gr. zu q_i, und zwar diejenige, die im Restklassenkörper mod $\mathfrak{q}_i$ den Automorphismus $\gamma \to \gamma^p$ erzeugt.

Haupteigenschaft dieses Symbols ist eben die obige Alternative a.), b.)

Es liegt nahe, Beziehung zwischen den r_p und e_p zu vermuten.

Diese besteht:

$$\begin{array}{rcl} e_p \equiv 0 & \text{für} & r_p \equiv 0 \bmod \ell \\ e_p \equiv r_p^{-1} & \shortparallel & r_p \not\equiv 0 \bmod \ell \end{array}$$

Folglich bilden auch die e_p, und somit die $\left(\frac{b,L}{p}\right)$ ein absolutes Invariantensystem. – Abhängigkeit:

$$\sum_p e_p \equiv 0 \bmod \ell, \qquad \prod_p \left(\frac{b,L}{p}\right) = 1.$$

Deurings Beweis, speziell $e_p \equiv 0 \bmod \ell \leftrightarrow \mathfrak{A}$ zerfällt (*Hilbert-Furtw.*) Beweis bisher leider nicht einfach. Für relative Invarianz leicht zu sehen.

NB. Deutung auch der r_p durch Normenrestsymbole möglich:

$$\mathfrak{W}_p = \mathfrak{R}_p(\omega) \qquad \mathsf{S}_p = (\omega \to \omega^{p^{r_p}})$$

$$\left(\frac{p,\mathfrak{W}_p}{p}\right) = \mathsf{S}^{-r_p^{-1}}$$

IV. Vollständigkeit der Invarianten.

Sei

$$\left(\frac{b,L}{p}\right) \equiv \left(\frac{b',L'}{p}\right), \qquad \text{d.h.} \quad e_p \equiv e'_p \bmod \ell$$

Dann auch

$$r_p \equiv r'_p \bmod \ell.$$

Wegen der Einzigkeit der r_p-Invarianten also:

$$\mathfrak{A}_p \equiv \mathfrak{A}'_p.$$

p der Sorte a.) und Sorte b.) sind insbesondere für $\mathfrak{A}$ und $\mathfrak{A}'$ dieselben.

p Sorte b.) Dann L_p Zerfällungskörper für $\mathfrak{A}'_p$, also $\mathfrak{A}'_p \times L_p = (\mathfrak{A}' \times L)_p$ zerfällt über L_p

p Sorte a.) Dann ev. p in L zerlegt in mehrere $\mathfrak{p}$. Jedenfalls gilt dann stets

$$(\mathfrak{A}' \times L)_\mathfrak{p} \qquad \text{zerfällt über } L_\mathfrak{p},$$

denn schon

$$\mathfrak{A}'_p \qquad \text{zerfällt über } \mathfrak{R}_p$$

Also

$$(\mathfrak{A}' \times L)_\mathfrak{p} \qquad \text{zerfällt für alle } \mathfrak{p} \text{ aus } L.$$

Wenn nun $L' \neq L$, ist $\mathfrak{A}' \times L$ ebenfalls zyklisch über L, erzeugt als $(L'L, \mathsf{S}', b')$ [1].

Aus dem vollständigen Zerfallen folgt:

$$\left(\frac{b', L'L}{\mathfrak{p}}\right) \equiv 1.$$

Daraus aber nach dem Hilbert-Furtwänglerschen Satz:

$$b' \text{ Norm aus } L'L \text{ in } L,$$

d.h.

$$\mathfrak{A}' \times L \quad \text{zerfällt über} \quad L.$$

Also ist L Zerfällungskörper vom Grade ℓ für $\mathfrak{A}'$. Daher auch Teilkörper von $\mathfrak{A}'$. Für $L' = L$ ist das von vornherein klar.

Sei demgemäß $\mathfrak{A}' = (L, \mathsf{S}, c)$ zyklisch aus L erzeugt. Dann nach Voraussetzung

$$\mathsf{S}^{e'_p} \equiv \left(\frac{c, L}{p}\right) \equiv \left(\frac{b, L}{p}\right) \equiv \mathsf{S}^{e_p},$$

1. undeutlich

also

$$\begin{aligned}\left(\frac{bc^{-1},L}{p}\right) &\equiv 1\\ bc^{-1} &\equiv \text{Norm aus } L\\ \mathfrak{A}' &\equiv \mathfrak{A}\end{aligned}$$

Damit also $\mathfrak{A}' = \mathfrak{A}$ ist, ist notwendig und hinreichend, daß die Invariantengleichheit $\left(\frac{b',L'}{p}\right) \equiv \left(\frac{b,L}{p}\right)$ gilt.

V. Verallgemeinerung auf zusammengesetzten Grad n und beliebigen algebraischen Grundkörper $\mathfrak{K}$ endlichen Grades.

Index m =Grad d. Div. Alg. $\mathfrak{B}$ i.d. Wedderburnschen Zerfällung $\mathfrak{A} = \mathfrak{B} \times \mathfrak{M}$

Exponent m_0 =frühester Exponent, für den b^{m_0} Norm aus L [2]

Satz. *$m_0 \mid m$ und enthält jeden Primteiler von m.*

Beweis. Zurückführung auf Index u. Exponent eines Faktorensyst. Nämlich für $\mathfrak{D}$ bzgl. L ist

$$c_{1,\mathsf{S}^\mu,\mathsf{S}^{\mu+\nu}} = \left\{ \begin{array}{ccc} 1 & \text{für} & 0 \leqq \mu+\nu < n \\ b & = & \mu+\nu > n \end{array} \right\} \quad 0 \leqq \mu < n,\ 0 \leqq \nu < n$$

Allgemein ist solches Faktorensystem dann und nur dann ~ 1, wenn b Norm aus L. Denn

a.) ist $c \sim 1$, so

$$c_{1,\mathsf{S}^\mu,\mathsf{S}^{\mu+\nu}} = \frac{\xi_{1,\mathsf{S}^\mu}\xi_{\mathsf{S}^\mu,\mathsf{S}^{\mu+\nu}}}{\xi_{1,\mathsf{S}^{\mu+\nu}}} = \frac{\xi_{1,\mathsf{S}^\mu}\xi_{1,\mathsf{S}^\nu}^{\mathsf{S}^\mu}}{\xi_{1,\mathsf{S}^{\mu+\nu}}}.$$

$$b = \prod_{\mu=0}^{n-1} c_{1,\mathsf{S}^\mu,\mathsf{S}^{\mu+1}} = N(\xi_{1,\mathsf{S}})$$

b.) ist $b = N(\xi) = \xi^{1+\mathsf{S}+\cdots+\mathsf{S}^{n-1}}$, so setze man

$$\xi_{1,\mathsf{S}^\nu} = \xi^{1+\mathsf{S}+\cdots+\mathsf{S}^{\nu-1}}, \quad \xi_{\mathsf{S}^\mu,\mathsf{S}^{\mu+\nu}} = \xi_{1,\mathsf{S}^\nu}^{\mathsf{S}^\mu}$$

2. undeutlich

und hat dann

$$c_{1,\mathsf{S}^\mu,\mathsf{S}^{\mu+\nu}} = \frac{\xi_{1,\mathsf{S}^\mu}\xi_{\mathsf{S}^\mu,\mathsf{S}^{\mu+\nu}}}{\xi_{1,\mathsf{S}^{\mu+\nu}}} \sim 1$$

Nun entspricht dem Faktorensystem c^k die Zahl b^k. Das beweist alles.

Anstelle der Unterscheidung a.) b.) tritt jetzt für jedes einzelne $\mathfrak{p}$ eine Unterscheidung in unsere Typen:

$$\mathfrak{A}_\mathfrak{p} \text{ einfach über } \mathfrak{K}_\mathfrak{p} \text{ als Zentrum}$$
$$\mathfrak{A}_\mathfrak{p} = \mathfrak{B}_\mathfrak{p} \times \mathfrak{M}_\mathfrak{p}$$

Index $m_\mathfrak{p}$ unterscheidet die Typen

Satz. *Exponent* $m_{0\mathfrak{p}} = m_\mathfrak{p}$.

Typen also auch durch die Ordnung $m_{0\mathfrak{p}}$ von $\left(\frac{b,L}{\mathfrak{p}}\right)$ unterschieden.

Diese daher absolut invariant.

Vermutung. Überdies

$$\left(\frac{b,L}{\mathfrak{p}}\right) = \mathsf{S}^{e_\mathfrak{p}}$$

selbst invariant, und wieder

$$e_\mathfrak{p} \equiv r_\mathfrak{p}^{-1} \bmod m_\mathfrak{p}$$

Beweis deshalb vorläufig nicht gelungen, weil Theorie der expliziten Formeln für die Normenrestsymbole nicht genügend bekannt. Auch macht die Adjunktion der $m_\mathfrak{p}$-ten Einheitswurzeln hier Schwierigkeiten, da der Grad ihres Körpers nicht notwendig prim zu $m_\mathfrak{p}$, wie für Primzahlgrad

Vollständigkeit läßt sich ebenso folgern, allerdings unter Benutzung des Analogons Hilbert-Furtwänglerschen Satzes, das bisher für zusammengesetzten Grad nicht bewiesen.

Insbesondere würde sich mit diesem Satze auch ergeben:

$$\textit{Index } m = \textit{Exponent } m_0.$$

1.9 Halle 1931

Der Wittsche Beweis des Wedderburnschen Satzes über endliche Schiefkörper.

Vortrag Halle, 1. Juli 1931.

S Schiefkörper, d.h. Körper abgesehen ev. vom komm. Ges. d. Mult.

Wedderburnscher Satz. *Ist* $\mathfrak{S}$ *endlich, so ist* $\mathfrak{S}$ *kommutativ, d.h. Körper.*

Beweise von Wedderburn, Artin, R. Brauer, E. Noether; kompliziert oder kunstvoll. Neuer, ganz elementarer Beweis von *Witt* (Herglotz-Schüler, Göttingen); benutzt allgemein die Idee, mit der Wedderburn gewisse Ausnahmefälle erledigt.

1.) Der Beweis beruht auf der Betrachtung gewisser Teilschiefkörper von $\mathfrak{S}$:

$a \neq 0$ aus $\mathfrak{S}$:

$$\begin{aligned}
\mathfrak{N}_a &= \text{Gesamtheit der mit } a \text{ vertauschbaren Elemente aus } \mathsf{S} \\
&= \textit{Normalisator} \text{ von } a \text{ in } \mathfrak{S}, \\
\mathfrak{Z} &= \text{Gesamtheit der mit allen } a \neq 0 \text{ (und natürlich auch mit 0) vertauschbaren Elemente aus } \mathfrak{S} \\
&= \text{Durchschnitt aller } \mathfrak{N}_a \\
&= \textit{Zentrum} \text{ von } \mathfrak{S}.
\end{aligned}$$

Hilfssatz 1. *Ist* $\mathfrak{T}$ *Teilschiefkörper von* $\mathfrak{S}$*, so ist die Elementzahl von* $\mathfrak{S}$ *eine Potenz der Elementzahl von* $\mathfrak{T}$.

Beweis. $\mathfrak{S}$ besitzt eine Basisdarstellung

$$a = a_1 X_1 + \cdots + a_r X_r,$$

wo $a_1, \ldots, a_r$ ein festes Maximalsystem in bezug auf $\mathfrak{T}$ rechtsseitig lin. unabh. Elemente aus $\mathfrak{S}$ ist, während $X_1, \ldots, X_r$ unabhängig von einander alle Elemente aus $\mathfrak{T}$ durchlaufen. Für die Elementzahlen folgt daraus:

$$s = t^r.$$

Anwendungen (Lateinische Buchstaben bezeichnen stets die zu den deutschen gehörigen El. Zahlen):

$$\begin{aligned} x &= z^r \\ n_a &= z^{r_a} \qquad s = (z^{r_a})^{q_a}, \quad \text{also} \quad r_a \mid r. \end{aligned}$$

2.) $\mathfrak{S}^*$, $\mathfrak{N}_a^*$, $\mathfrak{Z}^*$ seien die Gruppen, die durch Auslassung der 0 entstehen. Elementzahlen

$$s_1, \quad n_a - 1, \quad z - 1.$$

also

$$z^r - 1, \quad z^{r_a} - 1, \quad z - 1.$$

$$\begin{aligned} \mathfrak{N}_a^* &= \text{Normalisator von } a \text{ in } \mathfrak{S}^* \\ \mathfrak{Z}^* &= \text{Zentrum von } \mathfrak{S}^* \end{aligned}$$

Der Beweis beruht nun auf der Zerlegung von $\mathfrak{S}^*$ in Klassen konjugierter Elemente:

$$\mathfrak{S}^* = \sum_a \mathfrak{C}^a$$

wo a im folgenden ein festes Repräsentantensystem dieser Klassen durchläuft.

Hilfssatz 2. *Die Elementzahl c_a von $\mathfrak{C}_a$ ist gleich dem Index des Normalisators $\mathfrak{N}_a^*$ in $\mathfrak{S}^*$.*

$$\begin{aligned} \mathfrak{C}_a &= \{x^{-1}ax\} \qquad x \text{ läuft durch } \mathfrak{S}^* \\ c_a &= \text{Anz. der versch. unter den } x^{-1}ax \end{aligned}$$

Nun

$$\begin{aligned} y^{-1}ay = x^{-1}ax \quad &\leftrightarrow \quad (yx^{-1})^{-1}ayx^{-1} = a \\ &\leftrightarrow \quad yx^{-1} \text{ in } \mathfrak{N}_a^* \leftrightarrow y \text{ in } \mathfrak{N}_a^* X \end{aligned}$$

Ist also

$$\mathfrak{S}^* = \sum_i \mathfrak{N}_a^* x_i$$

die Zerlegung in Restklassen von $\mathfrak{S}^*$ nach $\mathfrak{N}_a^*$, so ist c_a die Anzahl dieser Restklassen:

$$c_a = \operatorname{Ind} \mathfrak{N}_a^* \quad \text{in } \mathfrak{S}^* = \frac{\operatorname{Ord} \mathfrak{S}^*}{\operatorname{Ord} \mathfrak{N}_a^*} = \frac{s-1}{n_a - 1} = \frac{z^r - 1}{z^{r_a} - 1}.$$

3.) Die Elementebilanz von $\mathfrak{S}^*$ liefert nun:

$$s - 1 = \sum_a c_a$$

d.h.

$$z^r - 1 = \sum_a \frac{z^r - 1}{z^{r_a} - 1}.$$

Hier trennen wir diejenigen Summanden ab, für die $r_a = r$ ist:

$$r_a = r \leftrightarrow \mathfrak{N}_a^* = \mathfrak{S}^* \leftrightarrow \mathfrak{N}_a = \mathfrak{S} \leftrightarrow a \text{ in } \mathfrak{Z}^*.$$

Also

$$z^r - 1 = z - 1 + \sum_a{}' \frac{z^r - 1}{z^{r_a} - 1},$$

wo in $\sum'$ alle r_a Teiler von r sind, die *kleiner* als r sind.

4.) Situation ganz analog zu Existenzbeweis des Zentrums $> E$ einer p-Gruppe $\mathfrak{G}$. Dort liefert Klassenaufzählung:

$$g = z + \sum_a{}' c_a,$$

und es resultierte aus $z = 1$ durch Betrachtung mod p ein Widerspruch.

Es handelt sich jetzt darum, einen geeigneten Teiler zu finden, der für $r > 1$ zum Widerspruch führt, also etwa der dann in $z^r - 1$ und den $\dfrac{z^r - 1}{z^{r_a} - 1}$ aufgeht, aber nicht in $z - 1$.

Ein solcher Teiler ist nun das r-te irreduzible Kreisteilungspolynom:

$$f_r(z) = \prod_{(k,r)=1} \left(z - e^{\frac{2\pi i k}{r}} \right)$$

Bekanntlich ist es ein ganz-rationalzahliges Polynom.

Ferner ist

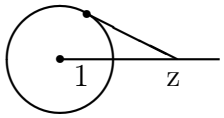
$\frac{z^r-1}{f_r(z)}$ ganzzahliges Polynom für max z, also ganze Zahl für unser z
$\frac{z^r-1}{(z^{r_a}-1)f_r(z)}$ = = = = = = = =

letzteres weil $r_a \mid r$ und $r_a < r$.

Daher folgt

$$f_r(z) \mid z-1.$$

Es ist aber jeder Faktor $\left|z - e^{\frac{2\pi ik}{r}}\right| \geqq z-1$:



also $|f_r(z)| \geqq z-1$, und $= z-1$ nur für $r=1$.

1.10 Zürich 1932

Vortrag Zürich September 1932 (Kiel, November 1932)

Grundbegriffe:

halbeinfache Algebra A	=	Algebra ohne nilpotente Ideale außer 0 (von Null versch. Basisdet.)
einfache Algebra A	=	Algebra ohne Ideale außer $0, A$
Divisionsalgebra A	=	Algebra ohne Nullteiler außer 0 (Schiefkörper endl. Ranges)

*Wedderburn*sche Struktursätze:

I. Jede halbeinfache Algebra ist (eindeutig bis auf die Reihenfolge) als direkte Summe einfacher Algebren darstellbar (und umgekehrt).

II. Jede einfache Algebra ist (eindeutig bis auf innere Automorphismen) als volles Matrizensystem über einer Divisionsalgebra darstellbar (und umgekehrt).

Hierdurch Strukturprobleme auf Untersuchung der Divisionsalgebren zurückgeführt.

Lösung für den Fall eines algebraischen Grundkörpers Ω im letzten Jahr gelungen; ergibt sich durch Kombination von

a.) algebraischer Theorie von *R. Brauer* und *E. Noether* (fußend auf *Dickson*, *Speiser*, *Schur*),

b.) arithmetischer Theorie von *Hasse* (fußend auf *Hensel*, *Speiser*).

a.) *Einiges aus der algebraischen Theorie.*

Da Zentrum algebraisch von endl. Grad über Grundkörper Ω, ohne Einschränkung Ω selbst Zentrum; *normale* Algebra über Ω.

Nach zweitem Struktursatz gehören Divisionsalgebren D und Matrixalgebren $A = D_r$ darüber eng zusammen; *Klasse* $\mathfrak{A}$, charakterisiert durch D. Grad m von D heißt *Index* von $\mathfrak{A}$; Grad von A ist dann $n = mr$. Klassen $\mathfrak{A}$ bilden bei direkter Multiplikation Gruppe $\mathfrak{G}$ (*R. Brauer*)

Algebraischer Hauptsatz (R. Brauer, E. Noether):

Zerfällungskörper K von $\mathfrak{A}$ vom Grad n (Erweiterung $\mathfrak{A}_K$ = Hauptklasse K)	=	Teilkörper max. Grades n von $A = D_r$ $(n = rm)$ (Darstellung als verschr. Prod. zu K, insbes. im galoisschen Fall)

Speziell, wenn K zyklischer Körper Z, ist A als *zyklische* Algebra darstellbar:

$$\left\{ \begin{array}{l} A = Z + uZ + \cdots + u^{n-1}Z \\ zu = uz^{\mathsf{S}} \quad (z \text{ bel. in } Z,\ \mathsf{S} \text{ erz. Aut. von } Z) \\ u^n = \alpha \quad \text{in} \quad \Omega. \end{array} \right\}, \quad \text{kurz} \quad A = (\alpha, Z, \mathsf{S}).$$

Diesen Typus zuerst von *Dickson* eingeführt und in seiner Bedeutung für Strukturproblem erkannt.

b.) *Einiges aus der arithmetischen Theorie.*

Durch Studium von D an den einzelnen Primstellen $\mathfrak{p}$ von Ω ist jeder Klasse $\mathfrak{A}$ in eindeutiger invariant definierter Weise ein System von Restklassen

$$\left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv \varrho_{\mathfrak{p}} \equiv \frac{\mu_{\mathfrak{p}}}{m_{\mathfrak{p}}} \bmod 1$$

zugeordnet. Dabei

$$\mathfrak{A}_1 = \mathfrak{A}_2 \leftrightarrow \left(\frac{\mathfrak{A}_1}{\mathfrak{p}}\right) \equiv \left(\frac{\mathfrak{A}_2}{\mathfrak{p}}\right) \bmod 1 \quad \text{für alle } \mathfrak{p}$$

(Hasse-Brauer-Noether || Albert)
(invariante Charakterisierung der Klasse $\mathfrak{A}$)

$$\left(\frac{\mathfrak{A}_1\mathfrak{A}_2}{\mathfrak{p}}\right) \equiv \left(\frac{\mathfrak{A}_1}{\mathfrak{p}}\right) + \left(\frac{\mathfrak{A}_2}{\mathfrak{p}}\right) \bmod 1 \quad (\text{Gruppe } \mathfrak{G})$$

$$\text{Summenrelation} \qquad \sum_{\mathfrak{p}} \left(\frac{\mathfrak{A}}{\mathfrak{p}}\right) \equiv 0 \bmod 1$$

Umgekehrt: *Jedes* Zahlsystem $\varrho_{\mathfrak{p}}$ mod 1 (mit naturgem. Einschr. bei den unendlichen $\mathfrak{p}$) mit $\sum_{\mathfrak{p}} \varrho_{\mathfrak{p}} \equiv 0 \bmod 1$ tritt als Invariantensystem einer Klasse $\mathfrak{A}$ auf; damit Struktur der abelschen Gruppe $\mathfrak{G}$ vollständig erkannt (Untergruppe eines direkten Produkts).

Arithmetischer Hauptsatz (Hasse)

Kriterium für Zerfällungskörper: K alg. Körper vom Grad n, Zerlegung nach $\mathfrak{p}$:

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad N(\mathfrak{P}_i) = \mathfrak{p}^{f_i}, \quad e_i f_i = n_{\mathfrak{P}_i},$$
$$(\mathfrak{P}_i \text{ Grad von } K = \text{Grad von } K_{\mathfrak{P}_i})$$
$$\sum_{i=1}^{r} n_{\mathfrak{P}_i} = n.$$
$$K \text{ Zerfällungskörper von } \mathfrak{A} \leftrightarrow m_{\mathfrak{p}} \mid n_{\mathfrak{P}_i} \quad \text{für alle } \mathfrak{p}, i.$$

D.h. die notwendigen Teilbarkeitsbedingungen an den sämtlichen Primstellen $\mathfrak{p}$ sind zusammengefaßt auch hinreichend; Zerfällungskörper im Großen dann und nur dann, wenn Zerfällungskörper überall im Kleinen.

c.) *Anwendungen.*

1.) Lösung des Strukturproblems der Divisionsalgebren.

Es existieren zyklische Zerfällungskörper Z für jeden möglichen Grad $n = mr$ (*Hasse*, *Grunwald*), insbesondere für m selbst als Grad. Demgemäß tritt den beiden Wedderburnschen Strukturätzen zur Seite:

III. Jede Divisionsalgebra über einem algebraischen Zahlkörper ist als zyklische Algebra (über ihrem Zentrum) darstellbar. – (Zyklisch im Großen, weil zyklisch überall im Kleinen)

Für die Fälle $n = 2, 3, 4$ wurde das bereits von *Dickson*, *Wedderburn*, *Albert* bewiesen.

Die Darstellung ist nicht eindeutig, und es gilt auch nicht die Umkehrung. Aber in beiden Richtungen gibt obige Invariantentheorie erschöpfende Auskunft.

IIIa. Jede zyklische Algebra $A = (\alpha, Z, \mathsf{S})$ ist einfach und normal über Ω. Ihren Index m gibt die früheste Potenz von α, die Norm aus Z ist. Insbesondere ist also A Divisionsalgebra dann und nur dann, wenn zuerst α^n Norm aus Z ist.

IIIb. Zwei zyklische Algebren $A = (\alpha, Z, \mathsf{S})$ und $A' = (\alpha', Z', \mathsf{S}')$ sind dann und nur dann identisch, wenn ihre Invarianten

$$\left(\frac{A}{\mathfrak{p}}\right) \equiv \left(\frac{A'}{\mathfrak{p}}\right) \bmod 1$$

für alle $\mathfrak{p}$ sind.

Dabei berechnen sich die Invarianten $\left(\frac{A}{\mathfrak{p}}\right)$ aus dem Normenrestsymbol $\left(\frac{\alpha,Z}{\mathfrak{p}}\right)$ nach der Regel:

$$\left(\frac{A}{\mathfrak{p}}\right) \equiv \left(\frac{\nu_{\mathfrak{p}}}{n}\right) \bmod 1, \qquad \text{wenn} \qquad \left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \mathsf{S}^{\nu_{\mathfrak{p}}}$$

Diese Regel kann umgekehrt als Definition des Normenrestsymbols auf lokale Art benutzt werden (*E. Noether*, *Chevalley*, *Hasse*). Sie läßt den [...] Satz der Klassenkp. i. Kl. unmittelbar erkennen.

2.) Aus der obigen Summenrelation ergibt sich bei Anwendung auf zyklische Algebren die Produktrelation für das Normenrestsymbol

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1,$$

d.h. das *Hilbert*sche Reziprozitätsgesetz für zyklische Körper Z. Daraus erschließt man dann leicht auch das *Artin*sche Reziprozitätsgesetz für Z (insbes. d. [...] Satz der Klassenkp Th. i. Gr.)

Voraussetzung aus der Klassenkörpertheorie dabei der Umkehrsatz im zykl. Fall, d.h.

a.) die analytische Theorie, $h \leqq n$;

b.) die arithmetische Theorie, $h \geqq n$, und zwar bestehend aus

α.) Dem Nachweis der entsprechenden Tatsache im Kleinen (für die einzelnen Primstellen $\mathfrak{p}$). – Das geht bereits sehr einfach hyperkomplex (*Chevalley*, *Hasse*); siehe oben.

β.) Dem Nachweis einer analogen Tatsache für das Komplement von endl. vielen Primstellen [...] [...] [...] – das muß noch hyperkomplex durchdacht [1] werden.

3.) Aus dem Kriterium für Zerfällungskörper folgt leicht die Antwort auf eine berühmte *I. Schur*sche Frage: Die absolut-irreduziblen Darstellungen einer endlichen Gruppe der Ordnung n sind stets im Körper der n^h-ten Einheitswurzeln für hinreichend hohes h möglich. (*Hasse*)

Ob man schon mit den n-ten Einheitswurzeln auskommt, ist noch unbekannt. Man muß dazu die Diskriminanten der einfachen Bestandteile des Gruppenrings genauer untersuchen.

1. undeutlich

4.) Das Kriterium für Zerfällungskörper zeigt einen einfachen Zusammenhang der Theorie der Algebren mit dem Zerlegungsgesetz der allgemeinen Zahlkörper. Schon heute steht fest, daß man hier an der Quelle der lange erstrebten Klassenkörpertheorie der allgem. galoisschen Zahlkörper ist. So konnte ich gestützt auf das Kriterium bereits den *Eindeutigkeitssatz* dieser Klassenkörpertheorie beweisen:

Ein galoisscher Körper K ist durch die von ihm zerfällte Untergruppe $\mathfrak{G}_K$ der vollen Algebrenklassengruppe eindeutig bestimmt.

Allgemeiner gilt der *Anordnungssatz*:

$$K \leqq K' \leftrightarrow \mathfrak{G}_K \leqq \mathfrak{G}_{K'}.$$

Allerdings geht aus den Untersuchungen von *Artin*, *E. Noether* und mir hervor, daß zum vollen Aufbau dieser Klassenkörpertheorie, insbesondere zum Aussprechen des Existenzsatzes, Isomorphiesatzes und Zerlegungsgesetzes, noch ein wesentlicher Gedanke fehlt.

1.11 Kiel, Hamburg 1932

Über das asymptotische Verhalten von Kongruenzlösungsanzahlen mod p.

Vortrag $\left\{ \begin{array}{c} \text{Kiel,} \\ \text{Hamburg} \end{array} \right\}$ November 1932.

0.) Zur Einübung der Fragestellungen und Begriffe beginne ich mit einem ganz einfachen Beispiel, nämlich der Fermatschen Kongruenz

$$x^\ell + y^\ell + z^\ell \equiv 0.$$

Im folgenden sind alle Kongruenzen stillschweigend nach einem Primzahlmodul p verstanden, der als Grundvariable zu betrachten ist. Es kommt auf $p \to \infty$ an; daher dürfen vorkommende Konstanten o. B. d. A. $\not\equiv 0$ angenommen werden. In unserem Falle ist es ferner keine Einschränkung, wenn man $\ell \mid p-1$ annimmt; denn allgemein ist die Lösungsanzahl obiger Kongruenz dieselbe wie für

$$x_0^{\ell_0} + y_0^{\ell_0} + z_0^{\ell_0} \equiv 0 \quad \text{mit} \quad \ell_0 = (\ell, p-1),$$

weil dann $x_0^{\ell_0} \equiv x^\ell$ eindeutig nach x auflösbar ist.

Schur hat gezeigt, daß jene Kongruenz für hinreichend hohes p stets (mit $xyz \not\equiv 0$) lösbar ist und auch eine untere Grenze für p angegeben, nämlich

$$p > e \cdot \ell! + 1.$$

Aber sowohl der Schursche Beweis (kombinatorisch) als auch seine Grenze für p sind lange nicht so gut, wie der folgende sehr einfache und verallgemeinerungsfähige Beweis von Mordell und Davenport (2 Varianten derselben Methode):

Natürlich interessiert man sich nur für nicht–identische Lösungen, kann also sogleich die inhomogene Kongruenz

$$x^\ell + y^\ell + 1 \equiv 0$$

zugrundelegen. Die fragliche Methode ist aber ebenso anwendbar auf den etwas allgemeineren Fall

$$ax^m + by^n + c \equiv 0, \quad \text{wo o. B. d. A.} \quad m, n \mid p-1 \quad \text{und} \quad a, b, c \not\equiv 0.$$

Sei N die Lösungszahl dieser Kongruenz. Dann hat man:

$$N = \frac{1}{p} \sum_{x,y,t} e\big[t(ax^m + by^n + c)\big].$$

Dabei soll, wie stets im folgenden, die Summation immer über ein volles Restsystem mod p erstreckt werden, und es bedeutet allgemein $e(u) = e^{\frac{2\pi i}{p} u}$.

Man findet heraus:

$$N = \frac{1}{p} \sum_{t} \sum_{x} e(tax^m) \cdot \sum_{y} e(tby^n) \cdot e(tc) = p + \frac{1}{p} \sum_{t}{}' \cdot \cdots\cdots$$

Nun ist

$$\sum_{x} e(tax^m) = \sum_{\xi} \sum_{\chi_m} \chi_m(\xi) e(ta\xi)$$

wo χ_m die m Charaktere nach der Gruppe der m–ten Potenzreste mod p durchläuft; denn dann ist $\sum\limits_{\chi_m} \chi_m(\xi)$ die Anzahl der Lösungen von $\xi \equiv x^m$.

Also weiter

$$\sum_{x} e(tax^m) = \sum_{\chi_m} \overline{\chi}_m(ta) \sum_{\xi} \chi_m(\xi) e(\xi) = \sum_{\chi_m} \overline{\chi}_m(ta) G(\chi_m),$$

wo $G(\chi_m) = \sum\limits_{\xi} \chi_m(\xi) e(\xi)$ die zu χ_m gehörige Gausssche Summe ist, Betrag $\sqrt{p}$. Daher

$$\begin{aligned} N &= p + \frac{1}{p} \sum_{t}{}' \sum_{\chi_m, \chi_n} \overline{\chi}_m(a) \overline{\chi}_n(b) G(\chi_m) G(\chi_n) \overline{\chi}_m \overline{\chi}_n(t) e(tc) \\ &= p + \frac{1}{p} \sum_{\chi_m, \chi_n} \overline{\chi}_m(a) \overline{\chi}_n(b) \chi_m \chi_n(c) G(\chi_m) G(\chi_n) G(\overline{\chi}_m \overline{\chi}_n) \end{aligned}$$

und somit

$$|N - p| < \sqrt{p} \cdot mn, \quad \text{oder} \quad N = p + \mathcal{O}(\sqrt{p}),$$

und also

$$N > 0, \quad \text{wenn} \quad p > m^2 n^2.$$

Im Falle der Fermatschen Kongruenz interessiert man sich für Lösungen mit $xy \not\equiv 0$. Solche mit $xy \equiv 0$ gibt es höchstens 2ℓ. Um dann $N > 2\ell$ zu erreichen, genügt es $p > (\ell^2+1)^2$ zu nehmen. Das ist viel besser, als die Schursche Schranke $e \cdot \ell! + 1$.

Mit analogen, komplizierteren Methoden haben Dickson und Hurwitz eine noch etwas bessere Schranke gefunden; jedoch ist die Verbesserung nicht wesentlich, das Hauptglied ist nach wie vor ℓ^4, und uns interessiert das hier nicht weiter. Wir vermerken nur noch folgendes:

Reduziert man die Restabschätzung auf ihren Mittelwert, so schreibt sich das allgemeine Resultat so:

$$\frac{N-p}{p} = \mathfrak{O}(p^{-\frac{1}{2}}) \quad \text{oder} \quad \frac{1}{p}N = 1 + \mathfrak{O}(p^{-\frac{1}{2}}).$$

Wir werden sehen, daß dies eine *bestmögliche* Restabschätzung im Sinne der späteren Überlegungen ist.

1.) Wir beginnen jetzt systematisch mit der Untersuchung von Kongruenzlösungsanzahlen mod p, indem wir zunächst die allgemeine Kongruenz in *einer* Variablen x behandeln. Es handelt sich also um die Lösungsanzahl N_a von

$$f_m(x) \equiv a,$$

wo mit $f_m(x)$ irgendein Polynom höchstens m–ten Grades bezeichnet sei. Natürlich ist N_a durch den Grad m beschränkt (außer für $m = 0$). Wenn man will kann man $f(x)$ ohne absolutes Glied annehmen, was ja durch Wahl von a kompensiert werden kann. Man weiß auch noch trivialerweise

$$\sum_a N_a = p.$$

Wir führen die *Verteilungsfunktion*

$$S(f_m) = \frac{1}{p}\sum_x e\big(f_m(x)\big) = \frac{1}{p}\sum_a N_a e(a)$$

($p \to \infty$, Konstanten prim zu p)

$\left(\begin{array}{c}\text{Bedeutung von } e(u)\\ \text{Summation}\end{array}\right)$

ein. Sie zeigt durch ihr Kleinwerden eine gleichmäßige Verteilung der Funktion N_a auf das Restsystem a an:

Völlig gleichverteilter Fall: $S(f_1) = 0$, alle $N_a = 1$, ($f_1(x) = a_0 + a_1 x$ mit $a_1 \not\equiv 0$).
Einer ungleichmäßigen Verteilung entspricht ein großer Wert der Verteilungsfunktion:

Extremer Fall: $|S(f_0)| = 1$, alle $N_a = 0$ bis auf $N(a_0) = p$.
Allgemein ist jedenfalls

$$|S(f_m)| \leqq 1.$$

Die Funktion $S(f_m)$ ist als Mittel aus allen p–ten Einheitswurzeln $e(a)$ mit den Gewichten N_a anzusehen.

Nächsthöherer Fall:

$$S(f_2) = \frac{1}{p} \sum_x e(a_0 + a_1 x + a_2 x^2), \qquad (a_2 \not\equiv 0)$$

Dies reduziert sich sofort auf die Gausssche Summe $\frac{1}{p} \sum\limits_y e(a_2 y^2)$, und man weiß also:

$$|S(f_2)| = p^{-\frac{1}{2}}.$$

Auch in gewissen höheren Fällen läßt sich $S(f_m)$ noch auf Gausssche Summen zurückführen, nämlich z. B. für $f_m(x) = a_0 + a_m x^m$, und man findet dann jedenfalls

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2}}), \qquad \text{(Bedeutung von } \mathfrak{O})$$

wenn auch kaum exakte Formel mehr für den Betrag.

Hiernach liegt es nahe zu vermuten, daß allgemein (von dem extremen Fall $m = 0$ fortan abgesehen) gilt:

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2}}).$$

Diese Vermutung ist bis heute noch nicht bestätigt.

Man kann jedoch über die Trivialität $|S(f_m)| \leqq 1$ hinausgehende Aussagen gewinnen. Der erste, der das allgemein anfaßte, war H. Weyl mit seiner schönen Gleichverteilungsmethode, die in iterierter Potenzierung des absoluten Betrages und Anwendung der Schwarzschen Ungleichung besteht. Weyls Methode liefert:

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2^{m-1}}+\varepsilon})$$

(Es sei allgemein bemerkt: Alle unsere Fehlerglieder sind absolut, d. h. auf den mittleren Wert 1 der zu untersuchenden Anzahlfunktion — hier N_a —

normiert; sie sind stets von der Form $\mathfrak{O}(p^{-r})$ mit positivem r — $r = 0$ wäre trivial — und je größer r ist, umso besser die Abschätzung; in nicht–linearen — völlig gleichverteilten — Fällen kommt man nie $\frac{1}{2}$ hinaus, während man $\frac{1}{2}$ nur selten erreicht; es ist leicht zu zeigen, daß $\frac{1}{2}$ oder $\frac{1}{2} + \varepsilon$ der *bestmögliche* Fehlerexponent in allen unseren Fällen ist.)

Weyls Methode ist aber für unsere Zwecke viel zu grob. Sie berücksichtigt gar nicht die arithmetische Eigenart unseres Problems, da sie auf beliebige reellzahlige Polynome $f_m(x)$ anwendbar ist.

Mordell hat nun eine auf ähnlichen Gedanken aufgebaute Methode entwickelt, die für dieses und höhere Probleme viel bessere Resultate gibt, als die Weylsche Methode. Sie liefert hier:

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{m}}).$$

Ich will die Methode an dem vorliegenden Problem genau auseinandersetzen, da sie mir von allgemeiner Bedeutung zu sein scheint. Sie beginnt wie die Weylsche Methode:

$$|S(f_m)|^2 = \frac{1}{p^2} \sum_{x,y} e\big(f_m(x) - f_m(y)\big)$$

Während aber Weyl jetzt $x - y = h$ als neue Summationsvariable einführt und die Schwarzsche Ungleichung anwendet, geht Mordell *direkt* zu höheren Potenzen des Betrages über:

$$|S(f_m)|^{2k} = \frac{1}{p^{2k}} \sum_{x_k, y_k} e\big[\big(f_m(x_1) - f_m(y_1)\big) + \cdots + \big(f_m(x_k) - f_m(y_k)\big)\big],$$

und summiert nunmehr über alle betrachteten Polynome f_m. Er setzt dabei die f_m bereits von ihren absoluten Gliedern befreit voraus, was auf den Betrag von $S(f_m)$ nichts ausmacht. Dann gibt es p^m verschiedene Polynome f_m (mod p gerechnet). Man erhält so

$$\sum_{f_m} |S(f_m)|^{2k} = \frac{1}{p^{2k}} \sum_{X_k, Y_k} \sum_{a_1, \ldots, a_m} e\big[a_1(X_k - Y_k) + \cdots + a_m(X_k^m - Y_k^m)\big].$$

Dabei ist zur Abkürzung gesetzt: $X_k^\mu = x_1^\mu + \cdots + x_k^\mu$. Die $\sum_{a_1, \ldots, a_m}$ zerspaltet sich in ein Produkt von Summen des Typus $\sum_{a_\mu} e\big(a_\mu(X_k^\mu - Y_k^\mu)\big)$, und diese

sind p oder 0, je nachdem $X_k^\mu \equiv Y_k^\mu$ oder nicht.
Also:

$$\sum_{f_m} |S(f_m)|^{2k} = \frac{1}{p^{2k-m}} N \left(\begin{array}{l} X_k \equiv Y_k \\ \cdots\cdots\cdots \\ X_k^m \equiv Y_k^m \end{array} \right).$$

Für $k = 1$ folgt $N = p$, also $\sum\limits_{f_m} |S|^2 = p^{m-1}$. Von den $p^m - 1$ Summanden für $f_m \neq 0$ muß also mindestens einer $\geqq \frac{p^{m-1}}{p^m-1} = \mathfrak{O}(p^{-1})$ sein, d. h. mindestens ein $|S| = \mathfrak{O}(p^{-\frac{1}{2}})$

Als bestgeeigneter Wert für k erweist sich hier $k = m$. Dann kann man nämlich die Lösungsanzahl unseres Kongruenzensystems sehr genau abschätzen. Das System fordert ja dann das Übereinstimmen der ersten m Potenzsummen der x_k und y_k, also nach den Newtonschen Formeln ($p > m$) auch ihrer elementarsymmetrischen Funktionen. Bei beliebig gegebenen y_k sind also die x_k dann bis auf die Reihenfolge eindeutig bestimmt. Man erhält somit höchstens $m!p^m$ Lösungen. Somit gilt:

$$(1 \leqq) \sum_{f_m} |S(f_m)|^{2m} \leqq m! = \mathfrak{O}(1).$$

Nun kommt der Hauptgedanke. Die Gesamtheit der Polynome f_m besitzt Substitutionen in sich, erzeugt durch ganze lineare Substitutionen der Variablen x (immer unter Auslassung des absoluten Gliedes), und zwar mod p gerechnet $p(p-1)$ solche. Dabei ändert sich jeweils der Betrag von $S(f_m)$ nicht. Daß eine solche Substitution ein Polynom f_m in sich überführt, kann vorkommen; ist aber $x' = \alpha x + \beta$ eine solche Substitution, so legt der höchste Koeffizient $\alpha^m \equiv 1$, also α höchstens m–deutig fest und der zweite dann β eindeutig, sodaß höchstens m solche Substitutionen für jedes f_m existieren, jedenfalls für die nichtlinearen f_m. Die linearen lassen p Substitutionen zu, das Nullpolynom alle $p(p-1)$. Läßt man die letzteren aus der Summe fort und summiert im übrigen nur über nicht–äquivalente f_m — Bezeichnung $\sum^*$ —, so erhält man eine Abschätzung

$$\frac{p(p-1)}{m} \sum_{f_m}^* |S(f_m)|^{2m} = \mathfrak{O}(1)$$

also sicherlich für nicht–lineare f_m

$$|S(f_m)|^{2m} = \mathfrak{O}(p^{-2}).$$

Daraus folgt

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{m}}), \qquad \text{w. z. b. w.}$$

Die Mordellsche Methode gibt in ihrer ersten Hälfte eine genaue Formel für den Mittelwert:

$$\frac{1}{p^m} \sum_{f_m} |S(f_m)|^{2k} = \frac{1}{p^{2k}} N \begin{pmatrix} X_k \equiv Y_k \\ \cdots\cdots\cdots \\ X_k^m \equiv Y_k^m \end{pmatrix}$$

bei beliebigem k. Nimmt man an, daß *alle* $S(f_m)$ von derselben *genauen* Größenordnung sind, so muß dieses die des Mittelwerts sein, d. h. $(k = m)$:

$$|S(f_m)|^{2m} = \frac{1}{p^{[\ldots]}} \mathfrak{O}(p^m) = \mathfrak{O}(p^m)$$

woraus

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2}})$$

folgen würde. Die Schwierigkeit des Problems liegt aber gerade darin, daß man nicht genug Automorphismen zur Verfügung hat. In f_m stecken p^m Parameter, aber nur $\mathfrak{O}(p^2)$ können durch Automorphismen eliminiert werden, es bleiben also $\mathfrak{O}(p^{m-2})$ unabhängige Parameter. In allen ähnlichen Problemen erhält man die bestmögliche Abschätzung $\mathfrak{O}(p^{-\frac{1}{2}})$ nur dann, wenn man *alle* Parameter durch Automorphismen entfernen kann.

Man könnte im Anschluß an die Mordellsche Methode darauf kommen, anstelle der Elimination der Parameter bei festem, möglichst günstig gewähltem k vielmehr durch $k \to \infty$ das größte Glied in der Summe links herauszuholen und abzuschätzen (Bernoullische Näherungsmethode!). Dazu müßte man die Lösungsanzahl des Kongruenzensystems

$$\begin{gathered} X_k \equiv Y_k \\ \cdots\cdots\cdots \\ X_k^m \equiv Y_k^m \end{gathered}$$

in $2k$ Variablen x_k, y_k sehr genau abschätzen. Der Hauptgrund, weswegen der ganze Gedanke auf Schwierigkeiten stößt, liegt zunächst darin, daß in der Summe links das Nullpolynom mit vorkommt und sicherlich das größte Glied liefert: $S(0) = 1$. Ihm entspricht rechts das Hauptglied der Lösungsanzahl, nämlich p^{2k-m} entsprechend der Anzahl $2k$ der Unbekannten und m

der Kongruenzen. Man hat also unter Auslassung dieser Glieder:

$$\sum_{f_m}{}' |S(f_m)|^{2k} = \frac{1}{p^{2k}} \left(N - p^{2k-m}\right),$$

und es kommt daher auf die Restabschätzung unserer Kongruenzlösungszahl an. Die Theorie der Kongruenz $f_m(x) \equiv a$ mit nur einer Unbekannten x aber Parametern wird durch die Mordellsche Methode zurückgeführt auf die Theorie des Kongruenzensystems $X_k \equiv Y_k, \ldots, X_k^m \equiv Y_k^m$ mit $2k$ Unbekannten x_k, y_k aber ohne Parameter, (und umgekehrt!).

Wüßte man für dessen Lösungsanzahl eine Abschätzung:

$$\frac{1}{p^{2k-m}} \left(N - p^{2k-m}\right) = \mathfrak{O}(p^{-k+r(m)}),$$

wo $r(m)$ nicht von k abhängt, so folgte auch:

$$|S(f_m)|^{2k} = \mathfrak{O}(p^{-k+r(m)})$$

und somit

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2}+\frac{r(m)}{2k}})$$

für jedes k, d. h.

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2}+\varepsilon}).$$

Aber die Behandlung des Kongruenzensystems ist sehr schwierig, und bis jetzt kommt man so nicht weiter.

Es gibt einige Fälle [von den parameterlosen Fällen (Gausssche Summen) abgesehen], wo man über die Mordellsche Abschätzung hinauskommt, nämlich zunächst den Fall $m = 3$. In diesem hat Davenport allgemein gezeigt, daß gilt:

$$S(f_3) = \mathfrak{O}(p^{-\frac{3}{8}}),$$

also besser als Mordells $\mathfrak{O}(p^{-\frac{1}{3}})$, aber noch nicht $\mathfrak{O}(p^{-\frac{1}{2}})$. Davenports Methode ist sehr speziell, aber sie läßt sich unserem Grundgedanken mit den Automorphismen unterordnen; er macht von der speziellen Tatsache Gebrauch,

daß sich die kubische Gleichung durch Wurzelzeichen auflösen läßt, und benutzt insbesondere gewisse quadratische Automorphismen zur Zurückführung auf Gausssche Summen, entsprechend der bei der Auflösung auftretenden Quadratwurzel. —

Ferner noch Davenport allgemein: $S(f_m) = \mathfrak{O}(p^{-\frac{1}{m_0}})$, wo m_0 Zahl einer der Formen $2^\nu, 3\cdot 2^\nu$ unter m inkl. m [1]

Ferner hat Mordell noch die bessere Abschätzung

$$S(f_m) = \mathfrak{O}(p^{-\frac{1}{2r}})$$

bewiesen für spezielle Polynome f_m, nämlich solche, die genau r nichtkonstante Glieder enthalten. Auch dies ist manchmal besser als $\mathfrak{O}(p^{-\frac{1}{m}})$, nämlich wenn wirklich Glieder fehlen. Die Methode ist dieselbe, nur daß man hier nur die $p-1$ Automorphismen $x' \equiv \alpha x$ zur Verfügung hat, die die vorausgesetzte Struktur von f_m invariant lassen. Daher nur $\frac{1}{2r}$ statt des früheren $\frac{1}{m}$.

Dies Mordellsche Resultat gilt auch wenn die Glieder *negative* Exponenten haben. Überhaupt ist ja unsere Fragestellung naturgemäß auch auf beliebige rationale Funktion $R(x)$ statt der Polynome $f_m(x)$ anwendbar:

$$S(R) = \frac{1}{p}\sum_x{}' e\big(R(x)\big),$$

wo jetzt nur die Nullstellen des reduzierten Nenners von $f(x)$ von der Summation auszuschließen sind und die Division natürlich mod p zu verstehen ist. Hier hat man jetzt zwar $\mathfrak{O}(p^3)$ Automorphismen $x' \equiv \frac{\alpha x+\beta}{\gamma x+\delta}$, aber die Mordellsche Methode überträgt sich nicht so ohne weiteres. Eventuell kommt man durch Partialbruchzerlegung von $R(x)$ zum Ziel.

Ein Spezialfall interessiert hier besonders, nämlich die sog. *Kloostermanschen Summen*:

$$S(ax+bx^{-1}) = \frac{1}{p}\sum_x{}' e(ax+bx^{-1}), \qquad (a,b \not\equiv 0).$$

Sie messen sozusagen die Gleichmäßigkeit der Verteilung der Reziproken mod p. Am einfachsten sieht man das, wenn man den einen Parameter a durch den Automorphismus $ax \equiv x'$ entfernt und dann schreibt:

$$S(x-\alpha x^{-1}) = \frac{1}{p}\sum_x{}' e(x-\frac{\alpha}{2}x^{-1}) = \frac{1}{p}\sum_{uv\equiv\alpha} e\left(\frac{u+v}{2}\right) = \frac{1}{p}\sum_a N_a e(a),$$

1. Ende des Satzes undeutlich

wo jetzt N_a angibt, wie oft von zwei zu a symmetrisch gelegenen Resten u, v das Produkt $uv \equiv \alpha$ wird.

Für diese Summen gibt das Mordellsche oben genannte Resultat ($r = 2$):

$$S(ax + bx^{-1}) = \mathfrak{O}(p^{-\frac{1}{4}}).$$

Das hatte schon Kloosterman bewiesen, der bei verfeinerten Untersuchungen der singulären Reihen aus der Hardy–Littlewoodschen Theorie auf diese Summen gekommen war.

Neuerdings haben jedoch Salié und Davenport unabhängig voneinander

$$S(ax + bx^{-1}) = \mathfrak{O}(p^{-\frac{1}{3}})$$

bewiesen. Natürlich vermutet man auch hier $\mathfrak{O}(p^{-\frac{1}{2}})$.

Schließlich sei noch gesagt, daß sich auch das allgemeine quadratische $R_2(x)$ auf eine Kloostermansche Summe reduzieren läßt. Eine Beziehung der Kloostermanschen Summen zu quadratischen Gleichungen erkennt man ja bereits an unserer homogenen Schreibweise: $\left\{ \begin{array}{c} u + v = 2a \\ uv = \alpha \end{array} \right\}$.

Ferner hat Davenport noch bewiesen:

$$\left.\begin{array}{rcl} S(ax^n + bx^{2n}) & = & \mathfrak{O}(p^{-\frac{3}{8}}) \\ S(ax^n + bx^{-n}) & = & \mathfrak{O}(p^{-\frac{1}{3}}) \end{array}\right\} n \neq 0 \quad \text{(pos. oder neg.)}$$

2.) Der nächsthöhere Fall sind die Kongruenzen mit *zwei* Variablen x, y, also ganz allgemein $f(x, y) \equiv 0$ mit Polynomen $f(x, y)$. Hier ist vor allem der Spezialfall $f(x, y) = f_m(x) - y^n$ untersucht, wo ohne Beschränkung $n \mid p - 1$ angenommen werden kann. Ich bezeichne ihre Lösungszahl mit

$$N\big(f_m(x) \equiv y^n\big) = N(f_m, n).$$

Ihr ungefährer Wert ist p, weil zwischen den p^2 Wertsystemen x, y eine Bedingung festgelegt ist. Wir werden also studieren den Mittelwert. Trivial ist die Abschätzung $N\big(f_m(x) \equiv y^n\big) \leqq np$, weil zu jedem x höchstens n Werte y gehören.

$$\frac{N(f_m, n)}{p} = \frac{1}{p} N(f_m, n).$$

Darstellung durch Exponentialsummen:

$$\begin{aligned}
\frac{1}{p}N(f_m,n) &= \frac{1}{p}\sum_x\sum_{\chi_n}\chi_n\big(f_m(x)\big)\\
&\quad\Big[=\frac{1}{p^2}\sum_{t,x,y}e\big[t\big(f_m(x)-y^n\big)\big]\quad\Big]\\
&= 1+\frac{1}{p}\sum_x{\sum_{\chi_n}}'\chi_n\big(f_m(x)\big)\\
&\quad\Big[=\frac{1}{p^2}\sum_t\sum_y e(-ty^n)\sum_x e\big(tf_m(x)\big)\quad\Big]\\
&= 1+\frac{1}{p}\sum_x{\sum_{\chi_n}}'\frac{G\big(f_m(x),\chi_n\big)}{G(\chi_n)}\\
&\quad\Big[=1+\frac{1}{p^2}{\sum_{\chi_n}}'G(\overline{\chi}_n)\chi_n(-1)\sum_{t,x}\chi_n(t)e\big(tf_m(x)\big)\quad\Big]\\
&= 1+\frac{1}{p}{\sum_{\chi_n}}'\frac{1}{G(\chi_n)}\sum_{t,x}\chi_n(t)e\big(tf_m(x)\big)\\
&\quad\Big[=1+{\sum_{\chi_n}}'\frac{\chi_n(-1)G(\overline{\chi}_n)}{\sqrt{p}}S(f_m,\chi_n)\quad\Big]\\
&= 1+{\sum_{\chi_n}}'\frac{\sqrt{p}}{G(\chi_n)}\cdot\frac{1}{p\sqrt{p}}\sum_{t,x}\chi_n(t)e\big(tf_m(x)\big)\\
&= 1+{\sum_{\chi_n}}'\varepsilon(\chi_n)\cdot S(f_m,\chi_n),\quad\text{wo}\quad|\varepsilon(\chi_n)|=1
\end{aligned}$$

und

$$S(f_m,\chi_n)=\frac{1}{p\sqrt{p}}\sum_{t,x}\chi_n(t)e\big(tf_m(x)\big);$$

NB. Es kommt nur $n>1$ und $\chi_n\neq\chi_1$ in Frage! Für $n=1$ wissen wir ja auch schon $N\big(f_m(x)\equiv y\big)=\sum\limits_a N_a=p$. Und allgemein ist für χ_1: $\sum\limits_{t,x}\chi_1(t)e\big(tf_m(x)\big)=N_0$

Hiernach gilt:

$$\frac{1}{p}N(f_m,\chi_n)=1+\mathfrak{O}\big(S(f_m,\chi_n)\big).$$

Einfachster Fall, $m = 1$:

$$S\big(f_1, \chi_n\big) = 0; \quad \text{denn}$$

$$\begin{aligned}\sum_{t,x} \chi_n(t)\varepsilon\big(t(a_0 + a_1 x)\big) &= \sum_{t,y} \chi_n(t) e(ty), \qquad (a_1 \not\equiv 0) \\ &= \sum_{y} \overline{\chi}_n(y) \cdot G(\chi_n) = 0, \quad \text{weil} \quad \chi_n \neq \chi_1\end{aligned}$$

Wieder vermutet man allgemein:

$$S(f_m, \chi_n) = \mathcal{O}(p^{-\frac{1}{2}}),$$

also dann

$$\frac{1}{p} N(f_m, n) = 1 + \mathcal{O}(p^{-\frac{1}{2}}),$$

und man vermutet auch dasselbe für $\frac{1}{p} N\big(f(x,y) \equiv 0\big)$ bei beliebigem absolut–irreduziblem $f(x,y)$.

Hier ist die Anwendung der Mordellschen Methode komplizierter. Fangen wir nämlich an:

$$|S(f_m, \chi_n)|^2 = \frac{1}{p^3} \sum_{\substack{t,x \\ u,y}} \chi_n(t)\overline{\chi}_n(u) e\big(t f_m(x) - u f_m(y)\big),$$

so würden beim sofortigen Weiterpotenzieren in die Charaktere Produkte $t_1 \dots t_k$, $u_1 \dots u_k$ eingehen, und eine Summe über die Lösungen gewisser Kongruenzen mit jeweils diesen Charakterwerten als Summanden entstehen. Das ist nicht brauchbar. Jedenfalls kann man aber folgendes tun:

$$\frac{1}{p} \sum_{a_0} |S(f_m, \chi_n)|^2 = \frac{1}{p^3} \sum_{t,x,y} e\big[t\big(f_m(x) - f_m(y)\big)\big],$$

(NB. Dies Mittel hat die Ordnung $\mathcal{O}(p^{-1})$, wenn wirklich $S(f_m, \chi_n) = \mathcal{O}(p^{-\frac{1}{2}})$ gilt.)

und jetzt durch Potenzierung:

$$\left(\frac{1}{p}\sum_{a_0}|S(f_m,\chi_n)|^2\right)^k = \frac{1}{p^{3k}}\sum_{t_\kappa,x_\kappa,y_\kappa} e\Big[t_1\big(f_m(x_1)-f_m(y_1)\big)+\cdots$$
$$\cdots+t_k\big(f_m(x_k)-f_m(y_k)\big)\Big]$$

$$\sum_{a_1,\ldots,a_m}\left(\frac{1}{p}\sum_{a_0}|S(f_m,\chi_n)|^2\right)^k = \frac{1}{p^{3k-m}}N\begin{pmatrix}(TX)_k & \equiv & (TY)_k\\ \cdots\cdots\cdots\cdots & & \\ (TX^m)_k & \equiv & (TY^m)_k\end{pmatrix},$$
$$\text{wo}\quad (TX^\mu)_k = t_1x_1^\mu+\cdots+t_kx_k^\mu.$$

Man erhält ein Kongruenzensystem von m Kongruenzen mit $3k$ Unbekannten ohne Parameter. Durch geeignete Wahl von k wird man so Abschätzungen jedenfalls für den Mittelwert $\frac{1}{p}\sum_{a_0}|S(f_m,\chi_n)|^2$ herleiten können, und damit dann auch Abschätzungen für $S(f_m,\chi_n)$ selbst. Bezüglich den Automorphismen muß man aber jetzt sich auf die $p-1$ Automorphismen $x'=\alpha x$ beschränken, weil nur bei ihnen die Summationseinteilung invariant ist. Auch kann man hier nicht ein $k>1$ finden, für das man dem Kongruenzensystem die Lösungszahl leicht ansieht; man ist auf die Behandlung spezieller Fälle (kleiner m) angewiesen. Man könnte allerdings vermuten, daß für $k=m$ bei willkürlich gegebenen t_κ wieder zu jedem System y_κ $\mathfrak{O}(1)$ Systeme x_κ existieren, sodaß man dann $\mathfrak{O}(p^{2m})$ Lösungen hätte. Das gäbe:

$$\sum_{a_1,\ldots,a_m}\left(\frac{1}{p}\sum_{a_0}|S(f_m,\chi_n)|^2\right)^m = \mathfrak{O}(1),$$

also unter Berücksichtigung der $\mathfrak{O}(p)$ Automorphismen

$$\frac{1}{p}\sum_{a_0}|S(f_m,\chi_n)|^2 = \mathfrak{O}(p^{-\frac{1}{m}})$$
$$S(f_m,\chi_n) = \mathfrak{O}(p^{\frac{1}{2}-\frac{1}{2m}}),$$

was etwas unter der trivialen Abschätzung $\mathfrak{O}(p^{\frac{1}{2}})$ liegt. Aber von $N(f(x)\equiv y^n)$ her ist sogar $\mathfrak{O}(1)$ trivial! Doch ist hier der Schluß mit den symmetrischen Funktionen nicht mehr angängig, und die Schlußweise bedarf noch der Klärung.

Um mit $k \to \infty$ das bestmögliche Resultat zu erhalten, müßte man für unser Kongruenzensystem eine Abschätzung

$$\frac{1}{p^{3k-m}} N \begin{pmatrix} (TX)_k \equiv (TY)_k \\ \cdots\cdots\cdots\cdots\cdots \\ (TX^m)_k \equiv (TY^m)_k \end{pmatrix} = \mathfrak{O}(p^{-k+r(m)})$$

kennen. Denn dann folgt:

$$\frac{1}{p} \sum_{a_0} |S(f_m, \chi_n)|^2 = \mathfrak{O}(p^{-1+\frac{r(m)}{k}}), \quad \text{also} \quad = \mathfrak{O}(p^{-1+\varepsilon}),$$

wie es dem bestmöglichen $S(f_m, \chi_n) = \mathfrak{O}(p^{-\frac{1}{2}+\varepsilon})$ entspricht. Doch ist jetzt kein Rückschluß auf $S(f_m, \chi_n)$ selbst möglich.

Wir wollen noch auf die von Mordell und Davenport behandelten Spezialfälle eingehen.

Zunächst der erste, nichttriviale Fall, $m = 2$:

Hier kann man auf Grund lin. Transf. $x' = x + \beta$, $t' = \gamma t$ zunächst die spezielle Gestalt

$$f_2(x) = x^2 - d$$

zugrundelegen, also

$$S(f_2, \chi_n) = \frac{1}{p\sqrt{p}} \sum_{x,\,t} \chi_n(t) e\big(t(x^2 - d)\big).$$

Aber auch der Parameter d kann noch durch lin. Transf. $x' = \alpha x$, $t' = \gamma t$ auf die drei Einzelfälle $\chi_2(d) = +1, -1, 0$ reduziert werden.

Der Fall $\chi_2(d) = 0$ steht für sich. Hier ist

$$\begin{aligned} S(x^2, \chi_n) &= \frac{1}{p\sqrt{p}} \sum_{t,x} \chi_n(t) e(tx^2) \\ &= \frac{1}{p\sqrt{p}} \sum_{t,y} \chi_n(t)\big(1 + \chi_2(y)\big) e(ty) \\ &= \frac{1}{p\sqrt{p}} \sum_{t,y} \chi_n(t)\chi_2(y) e(ty) \\ &= \frac{1}{p\sqrt{p}} \sum_{t} \chi_n(t)\chi_2(t) \cdot G(\chi_2) \\ &= \begin{cases} 0 & \text{für} \quad \chi_n \neq \chi_2, \quad \text{d. h. für} \quad n > 2 \\ \mathcal{O}(1) & \text{für} \quad \chi_n = \chi_2, \quad \text{d. h. für} \quad n = 2 \end{cases} \end{aligned}$$

$S(x^2, \chi_2)$ fällt also aus unserer Vermutung heraus, allgem. $S(f_2, \chi_2)$ mit $d = 0$.

Jedenfalls kann jetzt aus einer bestm. Absch. d. Mittels:

$$\frac{1}{p} \sum_{d} |S(f_2, \chi_n)|^2 = \mathcal{O}(p^{-1})$$

sofort auf

$$S(f_2, \chi_n) = \mathcal{O}(p^{-\frac{1}{2}}) \quad \text{(wenn nicht } n = 2 \text{ und } d = 0 \text{ ist)}$$

geschlossen werden.

Nach der Mordellschen Methode ist nun

$$\begin{aligned} \frac{1}{p} \sum_{d} |S(f_2, \chi_n)|^2 &= \frac{1}{p^3} \sum_{t,x,y} e\big(t(x^2 - y^2)\big) \\ &= \frac{1}{p^3} \cdot pN(x^2 \equiv y^2) \\ &= \frac{1}{p^2}\big(1 + 2(p-1)\big) = \mathcal{O}(p^{-1}). \end{aligned}$$

Daher folgt wirklich

$$S(f_2, \chi_n) = \mathcal{O}(p^{-\frac{1}{2}}),$$

bestmöglich, ausgenommen den Fall $n = 2$, $d = 0$.

Mit ähnlichen speziellen Methoden haben Mordell und Davenport folgende Resultate erhalten: Allgemeines $m \left\{ \begin{array}{c} = \\ = \end{array} \begin{array}{c} 2k-1 \\ 2k \end{array} \right\}$:

$$S(f_m, \chi_2) = \mathfrak{O}\left(p^{-\frac{1}{(k+1)2^{k-2}}}\right) \quad \text{(für } f_m \text{ mit rat. Wurzeln)}$$

(bis $k = 4$ sicher; sonst Kongruenzunabhängigkeit noch nicht voll bewiesen)

$m = 3$	$S(f_3, \chi_2)$	$=$	$\mathfrak{O}(p^{-\frac{1}{3}})$	(Mordell)
	$S(f_3, \chi_3)$	$=$	$\mathfrak{O}(p^{-\frac{1}{2}})$	(Mordell), bestmöglich!
	$S(f_3, \chi_n)$	$=$	$\mathfrak{O}(p^{-\frac{1}{4}})$	(Mordell)
$m = 4$	$S(f_4, \chi_2)$	$=$	$\mathfrak{O}(p^{-\frac{1}{3}})$	(Mordell)
	$S(f_4, \chi_4)$	$=$	$\mathfrak{O}(p^{-\frac{1}{3}})$	(Davenport)
	$S(f_4, \chi_n)$	$=$	$\mathfrak{O}(p^{-\frac{1}{6}})$	(Davenport)
$m = 5$	$S(f_5, \chi_2)$	$=$	$\mathfrak{O}(p^{-\frac{1}{8}})$	(Mordell)
	$S(f_5, \chi_5)$	$=$	$\mathfrak{O}(p^{-\frac{1}{6}})$	(Davenport)
$m = 6$	$S(f_6, \chi_2)$	$=$	$\mathfrak{O}(p^{-\frac{1}{8}})$	(Mordell)
	$S(f_6, \chi_3)$	$=$	$\mathfrak{O}(p^{-\frac{1}{8}})$	(Davenport)
	$S(f_6, \chi_6)$	$=$	$\mathfrak{O}(p^{-\frac{1}{8}})$	(Davenport)
$m = 7$	$S(f_7, \chi_2)$	$=$	$\mathfrak{O}(p^{-\frac{1}{20}})$	(Davenport)

NB. Natürlich sind wieder Fälle der Art $n = 2$, $d = 0$ auszunehmen, z. B. die $f_n(x) \equiv y^n$ entsprechenden Fälle!

Anwendungen auf Verteilungsfragen in der Theorie der n–ten Potenzreste

Wieder $n \mid p - 1$. Vorgegeben inkongruente $a_1, \ldots, a_r$ und zugeordnet n–te Einheitswurzeln $\varepsilon_1, \ldots, \varepsilon_r$.

$$\text{Anzahlfunktion:} \qquad N\begin{pmatrix} a_1, \ldots, a_r \\ \varepsilon_1, \ldots, \varepsilon_r \end{pmatrix} = N\begin{pmatrix} \chi_n(x + a_1) = \varepsilon_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \chi_n(x + a_r) = \varepsilon_r \end{pmatrix},$$

wo χ_n erzeugender n–ter Potenzrestcharakter.

Speziell Sequenzen: $(a_1,\dots,a_r)\equiv(0,1,\dots,r-1)$. — Mittelwert $\frac{p}{n^r}$

Ausdruck durch Charaktersumme:

$$\begin{aligned}\frac{N\begin{pmatrix}a_1,\dots,a_r\\ \varepsilon_1,\dots,\varepsilon_r\end{pmatrix}+\frac{1}{n}N_0\begin{pmatrix}a_1,\dots,a_r\\ \varepsilon_1,\dots,\varepsilon_r\end{pmatrix}}{\frac{p}{n^r}} &= \tfrac{1}{p}\sum_x\prod_{\rho=1}^{r}\sum_{\nu=0}^{n-1}\varepsilon_\rho^{-\nu}\chi_n^\nu(x+a_\rho)\\ &= \tfrac{1}{p}\sum_x\prod_{\rho=1}^{r}\sum_{\nu=0}^{n-1}\chi_n^\nu\big(\tfrac{x+a_\rho}{e_\rho}\big),\\ &\quad \text{wo}\quad \chi_n(e_\rho)=\varepsilon_\rho\,;\end{aligned}$$

Dabei $N_0\begin{pmatrix}a_1,\dots,a_r\\ \varepsilon_1,\dots,\varepsilon_r\end{pmatrix}$ = Anzahl der x, wo alle r Forderungen bis auf eine, und statt dieser $\chi(x+a_\rho)=0$, d. h. $x+a_\rho\equiv 0$, erfüllt sind; $N_0\leqq r$, also der Zusatzsummand links ist $\mathfrak{O}(p^{-1})$.

$$\begin{aligned}\frac{N\begin{pmatrix}a_1,\dots,a_r\\ \varepsilon_1,\dots,\varepsilon_r\end{pmatrix}}{\frac{p}{n^r}} &= 1+\frac{1}{p}\sum_x\sum_{\nu_\rho=0}^{n-1}{}'\,\chi_n^{\nu_1}\left(\frac{x+a_1}{e_1}\right)\cdots\chi_n^{\nu_r}\left(\frac{x+a_r}{e_r}\right)+\mathfrak{O}(p^{-1})\\ &= 1+\frac{1}{p}\sum_x\sum_{\substack{\nu_\rho=0\\ (\text{nicht }[\dots])}}^{n-1}{}''\ \sum_{\nu=0}^{n-1}{}'\,\chi_n^\nu\Big(\left(\frac{x+a_1}{e_1}\right)^{\nu_1}\cdots\\ &\qquad\qquad\cdots\left(\frac{x+a_r}{e_r}\right)^{\nu_r}\Big)+\mathfrak{O}(p^{-1})\\ &= 1+\frac{1}{p}\sum_x\sum_{\nu_\rho=0}^{n-1}{}''\ \sum_{\chi_n}{}'\,\chi_n\big(f_{\nu_\rho}(x)\big)+\mathfrak{O}(p^{-1})\\ &= 1+\mathfrak{O}\left(\frac{1}{p}\sum_x\sum_{\chi_n}{}'\,\chi_n\big(f_{\nu_\rho}(x)\big)\right)+\mathfrak{O}(p^{-1})\\ &= 1+\mathfrak{O}\Big(S\big(f_{\nu_\rho}(x),\chi_n\big)\Big)+\mathfrak{O}(p^{-1}).\end{aligned}$$

Ist also die obige Vermutung für die $S\big(f_{\nu_\rho}(x), \chi_n\big)$ richtig, so folgt

$$\frac{N\begin{pmatrix} a_1, \ldots, a_r \\ \varepsilon_1, \ldots, \varepsilon_r \end{pmatrix}}{\frac{p}{n^r}} = 1 + \mathfrak{O}(p^{-\frac{1}{2}}).$$

Im **Falle $n = 2$** ist der Höchstgrad m der auftretenden Polynome $f_{\nu_\rho}(x)$ gleich r selbst, allgemein $m = (n-1)r$. Man kann im Falle $n = 2$ die Mordellsche Methode etwas modifiziert für allgemeinen Grad m durchführen und erhält folgende Fehlerglieder:

$$n = 2, \qquad r = \begin{Bmatrix} 2k-1 \\ 2k \end{Bmatrix} \qquad \mathfrak{O}\left(p^{-\frac{1}{(k+1)2^{k-2}}}\right)$$

allerdings nur bis $k = 5$ sicher, sonst noch mit der Davenportschen Vermutung der Kongruenzunabhängigkeit belastet.

Im Falle der Sequenzen läßt sich für ungerades $r = 2k+1$ das Höchstglied besonders behandeln und auf den Grad $2k$ zurückführen, außer für $r = 5$, wo man so nur auf $\mathfrak{O}(p^{-\frac{1}{4}})$ statt $\mathfrak{O}(p^{-\frac{1}{3}})$ kommt. Das erniedrigt noch einige Resultate. Für $r = 2, 3$ hatte im Falle der Sequenzen schon Jacobsthal die besseren (bestmöglichen) Resultate:

$$\begin{aligned} &n = 2, \quad r = 2 \quad \mathfrak{O}(p^{-1}) \\ &n = 2, \quad r = 3 \quad \mathfrak{O}(p^{-\frac{1}{2}}). \end{aligned}$$

Für höhere n liefert die Mordellsche Methode, soweit sie oben auseinandergesetzt wurde, noch den Fall:

$$n = 3, \quad r = 2 \quad \mathfrak{O}(p^{-\frac{1}{6}})$$

Aber Davenport hat durch andere Methoden viel mehr bewiesen:

$$\begin{aligned} &n \text{ bel.} \quad r = 2 \quad \mathfrak{O}(p^{-\frac{1}{2}}) \qquad \text{(bestmöglich)} \\ &n \text{ bel.} \quad r = 3 \quad \mathfrak{O}(p^{-\frac{1}{4}}) \\ &n \text{ bel.} \quad r = 4 \quad \mathfrak{O}(p^{-\frac{1}{16}}), \qquad \text{für } n = 3 \text{ sogar} \quad \mathfrak{O}(p^{-\frac{1}{6}}) \end{aligned}$$

1.12 Göttingen 1933 I

Über die Nullstellen der Artinschen Kongruenzzetafunktionen.

Vortrag in der Math. Ges. Göttingen, 10. 1. 1933.

1.) In seiner Dissertation hat Artin gezeigt, daß der Körper $\mathsf{P}_p(t) = \mathsf{P}$ der rationalen Funktionen einer Unbestimmten t über dem endlichen Körper P_p von p Elementen weitgehend analoge zahlentheoretische Gesetzmäßigkeiten zum Körper der rationalen Zahlen besitzt. Den ganzen Zahlen entsprechen dabei die Polynome in t, d. h. der Ring $\mathsf{P}_p[t]$, den Primzahlen die Primpolynome (d. h. die irreduziblen ganzzahligen Polynome mod p), dem absoluten Betrag der Grad, oder richtiger p^{Grad}.

Artin entwickelt in voller Analogie zur Theorie der gewöhnlichen quadratischen Zahlkörper die Theorie der quadratischen Zahlkörper $\mathsf{K} = \mathsf{P}(\sqrt{D})$ über P, wo $D = D(t)$ ohne Einschränkung ein Polynom über P_p ohne quadratische Teiler ist. Er beweist mit ihrer Hilfe ein vollständiges Analogon zum quadratischen Reziprozitätsgesetz. Ferner entwickelt er auch in voller Analogie die analytische Theorie der quadratischen Zahlkörper K, indem er ihre Zetafunktionen definiert und für sie das Residuum bei $s = 1$, den Zusammenhang mit der Klassenzahl, eine Funktionalgleichung, und das Analogon der Riemannschen Vermutung studiert, sowie Anwendungen dieser Theorie auf asymptotische Verteilungsfragen der Primpolynome gibt (Analogon des Primzahlsatzes, sowie des Satzes über die Primzahlen in arithmetischen Progressionen).

Die Artinsche Theorie ist ohne weiteres verallgemeinerbar auf den Fall, wo statt P_p ein beliebiger endlicher Körper P_q von $q = p^r$ Elementen zugrundeliegt; doch hat es wenig Interesse gleich diesen allgemeineren Fall zu behandeln, weil gar keine neuen Gedanken hinzukommen.

Ferner hat F. K. Schmidt die Artinsche Theorie, oder jedenfalls die theoretischen Hauptpunkte dieser Theorie, auf die allgemeinsten Erweiterungen endlichen Grades K von P ausgedehnt, wobei neben der Analogie zu den gewöhnlichen algebraischen Zahlkörpern auch die Analogie zu den Körpern algebraischer Funktionen einer Variablen eine entscheidende Rolle spielt. Bei der letzteren Analogie hat man P_p selbst $\big($nicht erst $\mathsf{P}_p(t)\big)$ mit dem Körper der rationalen (oder der komplexen) Zahlen in Analogie zu setzen und $\mathsf{K} = \mathsf{P}_p(t, x)$, definiert durch eine irreduzible Gleichung $F(t, x) = 0$, als algebraischen Funktionenkörper über P_p aufzufassen. Bei dieser zweiten Analogie

erweist sich die Funktionalgleichung der Zetafunktion von K als formal identisch mit dem Analogon des Riemann–Rochschen Satzes der algebraischen Funktionentheorie.

Ich will mich hier im wesentlichen auf den ursprünglichen Artinschen Fall $\mathsf{K} = \mathsf{P}(\sqrt{D})$ beschränken, der vom Standpunkte der algebraischen Funktionentheorie als der **hyperelliptische Fall** zu bezeichnen ist.

Die gewöhnliche Zetafunktion (von P selbst) ist in der Artinschen Theorie ganz trivial. Sie ist die Summe bzw. das Produkt

$$\zeta(s) = \sum_A \frac{1}{|A|^s} = \prod_P \frac{1}{1 - \frac{1}{|P|^s}}$$

wo $\left\{ \begin{array}{ll} A & \text{alle Polynome} \\ P & \text{alle Primpolynome} \end{array} \right\}$ über P_p mit höchstem Koeffizienten 1 durchläuft und $|A| = p^{\text{Grad von } A}$ bedeutet. Da es von jedem Grad n genau p^n Polynome A gibt, ist

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{p^n}{p^{ns}} = \sum_{n=0}^{\infty} \frac{1}{p^{n(s-1)}} = \frac{1}{1 - \frac{1}{p^{s-1}}}\,.$$

Wesentlich interessanter ist die Zetafunktion des quadratischen Körpers $\mathsf{K} = \mathsf{P}(\sqrt{D})$. Sie ist

$$\zeta_D(s) = \sum_{\mathfrak{A}} \frac{1}{N(\mathfrak{A})^s} = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{N(\mathfrak{P})^s}}\,,$$

wo $\left\{ \begin{array}{ll} \mathfrak{A} & \text{alle ganzen Ideale} \\ \mathfrak{P} & \text{alle Primideale} \end{array} \right\}$ von K durchläuft, und N die Absolutnorm (Betrag der Norm = Anzahl der Restklassen) bedeutet. Analog zum Fall der gewöhnlichen quadratischen Körper zerspaltet sich diese Zetafunktion so:

$$\zeta_D(s) = \zeta(s) L_D(s),$$

wo

$$L_D(s) = \sum_A \left[\frac{D}{A}\right] \frac{1}{|A|^s} = \prod_P \frac{1}{1 - \left[\frac{D}{P}\right] \frac{1}{|P|^s}}\,,$$

wobei $\left[\frac{D}{P}\right] = +1, -1, 0$, je nachdem D quadr. Rest, quadr. Nichtrest, $\equiv 0$ mod P ist, und $\left[\frac{D}{A}\right]$ durch Zusammensetzung von A aus Primpolynomen

erklärt ist. Hier haben wir das Analogon zu den gewöhnlichen L–Funktionen mit quadr. Charakteren vor uns.

Diese L–Funktionen sind in Wahrheit Polynome in $\frac{1}{p^s}$, nämlich

$$L_D(s) = \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}},$$

wo n der Grad von D ist und

$$\sigma_\nu = \sum_{|A|=p^\nu} \left[\frac{D}{A}\right] \qquad (A \text{ höchsten Koeffizienten } 1).$$

Hierbei ist allerdings noch der triviale Fall auszuschließen, wo $n = 0$, also K schon über P_p algebraisch ist; dann ist $L_D(s) = \frac{1}{1+\frac{1}{p^{s-1}}}$. Wir lassen diesen Fall im folgenden beiseite.

$L_D(s)$ und $\zeta_D(s)$ sind periodisch mit der Periode $\frac{2\pi i}{\log p}$, und sind daher unendlich viel einfacher als die gewöhnlichen L–Funktionen und ζ–Funktionen, bei denen nur Fastperiodizität auf senkrechten Geraden gilt.

Es soll hier nicht meine Aufgabe sein, über Residuum bei $s = 1$, Funktionalgleichung, Klassenzahlformeln und asymptotische Verteilungsfragen zu berichten. Ich will nur auf das Nullstellenproblem eingehen.

Hier weiß man (vermöge Produktdarstellung und Funktionalgleichung), daß alle Nullstellen von $\zeta_D(s)$ und $L_D(s)$ im Streifen $0 \leqq \Re(s) \leqq 1$ liegen. Ist der Grad n von D gerade, so liegt je eine Nullstelle des Periodenstreifens $0 \cdots\cdots \frac{2\pi i}{\log p}$ auf $\Re(s) = 0$, nämlich entweder 0 oder $\frac{\pi i}{\log p}$. Für ungerades n ist das nicht der Fall. Im übrigen liegen alle Nullstellen wirklich im Inneren des kritischen Streifens. Durch linear gebrochene Transformation in t kann man stets auf D von ungeradem Grade n kommen. Dann liegen also im Inneren des kritischen Streifens im Periodenabschnitt genau $n-1$ Nullstellen $\rho_1, \ldots, \rho_{n-1}$. Diese sind gegeben durch die $n-1$ Nullstellen $\beta_1, \ldots, \beta_{n-1}$ des Polynoms

$$F(z) = \sigma_0 z^{n-1} + \sigma_1 z^{n-2} + \cdots + \sigma_{n-1},$$

vermöge der Substitution

$$z = p^s, \qquad \beta_i = p^{\rho_i}.$$

Das Analogon der Riemannschen Vermutung besagt, daß alle diese Nullstellen ρ_i auf der Geraden $\Re(s) = \frac{1}{2}$ liegen, d. h. daß alle β_i auf dem Kreise $|z| = p^{\frac{1}{2}}$ liegen (bekannt ist, daß die β_i in $1 < |z| < p$ liegen).

Die Bestimmung der β_i hängt von den Summen

$$\sigma_\nu = \sum_{|A|=p^\nu} \left[\frac{D}{A}\right]$$

ab. Von diesen ist

$$\sigma_0 = 1\,, \qquad \text{d. h. } F(2) \text{ hat höchsten Koeffiz. 1.}$$

Ferner ist

$$\sigma_1 = \sum_{a \mod p} \left[\frac{D(t)}{t-a}\right] = \sum_{a \mod p} \left[\frac{D(a)}{t-a}\right] = \sum_{a \mod p} \left(\frac{D(a)}{p}\right).$$

Das ist eine Summe über gewöhnliche Legendre–Symbole. Die höheren σ_ν lassen sich nicht so einfach durch gewöhnliche Legendre–Symbole ausdrücken. Man kann aber auf andere Art an sie herankommen. Es ist

$$-\sigma_1 = \beta_1 + \cdots + \beta_{n-1}.$$

Geht man nun von P_p zum endlichen Körper $\mathsf{P}_q = \mathsf{P}_{p^r}$ über, so ist einfach überall p durch p^r zu ersetzen, d. h. auch z durch z^r, β_i durch β_i^r, sodaß also

$$-\sigma_1^{(r)} = \beta_1^r + \cdots + \beta_{n-1}^r$$

(NB. Zur genaueren Ausführung hat man die Zerspaltung $\zeta_D(s) = \prod_\chi L_D(s,\chi)$ zu benutzen, wo $\chi(\mathfrak{A}) = \varepsilon^\nu$ wenn $|N(\mathfrak{A})| = p^\nu$, und ε alle r–ten Einheitswurzeln durchläuft.

wird. Kennt man also die Summen $\sigma_1^{(r)}$ für alle r, so beherrscht man alle Potenzsummen der Nullstellen β_i, und damit diese selbst. Genauer:

Weiß man, daß mit wachsendem r (bei festem p)

$$\sigma_1^{(r)} = \mathfrak{O}\left(q^{\frac{1}{2}+\varepsilon}\right) = \mathfrak{O}\left(p^{r(\frac{1}{2}+\varepsilon)}\right)$$

mit einem $\varepsilon > 0$ ist, das nicht von r (und p) abhängt, und wo auch $\mathfrak{O}$ gleichmäßig in r gemeint ist, so folgt nach dem vom Graeffeschen Näherungsverfahren her bekannten Schluß für die Nullstellen

$$|\beta_i| \leqq p^{\frac{1}{2}+\varepsilon},$$

sodaß also die ρ_i im Streifen $\frac{1}{2} - \varepsilon \leqq \Re(s) \leqq \frac{1}{2} + \varepsilon$ liegen.

Weiß man sogar, daß die genannte Abschätzung für beliebig kleine $\varepsilon > 0$ gilt, so folgt also

$$|\beta_i| = p^{\frac{1}{2}}, \qquad \Re(\varrho_i) = \frac{1}{2}$$

und überdies verschärft sich die Abschätzung von σ_1 zu

$$|\sigma_1| \leqq (n-1)p^{\frac{1}{2}}.$$

Entsprechende Tatsachen gelten auch für den allgemeinen von F. K. Schmidt behandelten Fall. Hier tritt an die Stelle von

$$\sigma_1 = \sum_{a \mod p} \left(\frac{D(a)}{p}\right) = \sum_{a \mod p} \left(1 + \left(\frac{D(a)}{p}\right)\right) - p$$
$$= N\left(D(t) \equiv x^2\right) - p$$

das entsprechend gebaute Fehlerglied

$$\sigma_1 = N\big(F(t,x) \equiv 0\big) - p.$$

Hierdurch ist also das Nullstellenproblem der Artinschen und F. K. Schmidtschen Zetafunktionen zurückgeführt auf die Restabschätzung der Lösungsanzahlen von Kongruenzen mod p. Man muß dabei diese Restabschätzung allerdings nicht nur in P_p, sondern in jedem $\mathsf{P}_q = \mathsf{P}_{p^r}$ durchführen, d. h. also bei gegebenem Polynom $D(t)$ bzw. $F(t,x)$ über P_p die Variablen t, x nicht nur in P_p sondern der Reihe nach in jedem P_q laufen lassen.

2.) Die Restabschätzung von Kongruenzlösungsanzahlen ist in letzter Zeit systematisch von den englischen Mathematikern Davenport und Mordell in Angriff genommen worden. Sie haben eine Fülle von Einzelresultaten gefunden, die sich auf spezielle solche Kongruenzen, vor allem solche mit niedrigen Gradzahlen beziehen. Diese Resultate ergeben sich durch mehr oder weniger spezielle, dem betr. Problem angepaßte Abschätzungsmethoden. Den meisten dieser Methoden gemeinsam ist eine sehr schöne Idee von Mordell, die ich hier auseinandersetzen will. Ich wähle dazu den allereinfachsten Fall der Kongruenzen mit nur *einer* Unbekannten:

$$N_a = N\big(F(t) \equiv a\big),$$

wo $F(t)$ ein Polynom über P_p ist. (Den allgemeineren Fall des beliebigen endlichen Körpers P_q, den Mordell nicht behandelt hat, lasse ich zunächst beiseite.) Zusammenhang mit ζ–Funktionen bisher unbekannt.

Über die Lösungsanzahlen N_a weiß man trivialerweise:

$$0 \leqq N_a \leqq n \quad \big(\text{Grad von } F(x)\big)$$
$$\sum_a N_a = p.$$

Ohne Einschränkung darf man $F(t) \equiv a_n t^n + \cdots + a_1 t$ ohne absolutes Glied annehmen: Die Verteilungsfunktion

$$S(F) = \sum_t e\big(F(t)\big), \quad \text{wo} \quad e(u) = e^{\frac{2\pi i u}{p}},$$
$$= \sum_a N_a e(a)$$

mißt die Abweichung der Anzahlfunktion N_a von der Gleichverteilung (Linearer Fall, $n = 1$, $F(t) \equiv a_1 t$, alle $N_a = 1$, $S(F) = 0$; extremer Fall $n = 0$, $F(t) \equiv 0$, $N_0 = p$, alle anderen $N_a = 0$, $S(F) = p$; allgemein $|S(F)| \leqq p$.) Der erste nichttriviale Fall ist $n = 2$, $F(t) \equiv a_2 t^2 + a_1 t$. Hier liegt eine Gaußsche Summe vor:

$$|S(F)| = p^{\frac{1}{2}}.$$

Auch gewisse höhere Fälle führen noch auf höhere Gaußsche Summen, nämlich $F(t) \equiv a_n t^n$, wo dann wieder jedenfalls

$$S(F) = \mathfrak{O}(p^{\frac{1}{2}})$$

gilt. Hierbei ist $\mathfrak{O}$ hier und im folgenden stets sogar gleichmäßig in den Konstanten von F zu verstehen, abhängig lediglich vom Grad n.

Man vermutet nun allgemein in diesem Sinne:

$$S(F) = \mathfrak{O}\left(p^{\frac{1}{2}}\right).$$

Bewiesen ist dies allerdings bisher in keinem über die Gaußschen Summen hinausgehenden Falle. Doch hat man weniger scharfe allgemein–gültige Aussagen, wo $\frac{1}{2}$ durch einen größeren Exponenten α (< 1) ersetzt ist.

Eine erste nichttriviale Aussage ergibt sich nach Weyl's schöner Gleichverteilungsmethode (iterierte Potenzierung des absoluten Betrags von $S(F)$ mit 2 und Anwendung der Schwarzschen Ungleichung). Man erhält damit

$$S(F) = \mathfrak{O}\left(p^{1-\frac{1}{2^{n-1}}+\varepsilon}\right) \quad \text{für jedes} \quad \varepsilon > 0.$$

Weyl's Methode ist aber für unser Problem inadäquat (zu grob), da sie auf beliebige reellzahlige Polynome anwendbar ist.

Mordell's Methode baut in ihrem ersten Schritt auf einem ganz ähnlichen Gedanken auf, nämlich Berechnung des absoluten Betrags wie bei Weyl:

$$|S(F)|^2 = \sum_{t,u} e\big(F(t) - F(u)\big).$$

Während aber Weyl jetzt $t - u = h$ als neue Summationsvariable einführt und die Schwarzsche Ungleichung anwendet, geht Mordell *direkt* zu höheren Potenzen des Betrags über:

$$|S(F)|^{2k} = \sum_{t_\kappa, u_\kappa} e[F(t_1) - F(u_1) + \cdots + F(t_k) - F(u_k)],$$

und summiert nunmehr über alle betrachteten Polynome F (vom Grade $\leqq n$, ohne abs. Glied), d. h. über p^n Polynome F, repräsentiert durch die p^n Wertsysteme $a_1, \ldots, a_n$. Er erhält so:

$$\sum_F |S(F)|^{2k} = \sum_{t_\kappa, u_\kappa} \sum_{a_1,\ldots,a_n} e[a_1(T_k - U_k) + \cdots + a_n(T_k^{(n)} - U_k^{(n)})],$$

$$\text{wo zur Abkürzung} \quad T_k^{(\nu)} = t_1^\nu + \cdots + t_k^{(\nu)}.$$

Die Summe $\sum_{a_1,\ldots,a_n}$ zerspaltet sich in ein Produkt von Summen

$$\sum_{a_\nu} e[a_\nu(T_k^{(\nu)} - U_k^{(\nu)})] = \left\{ \begin{array}{ll} p & \text{wenn} \quad T_k^{(\nu)} \equiv U_k^{(\nu)} \\ 0 & \text{sonst} \end{array} \right\}.$$

Somit wird

$$\sum_F |S(F)|^{2k} = p^n N\Big(T_k^{(\nu)} \equiv U_k^{(\nu)}\Big)_{(\nu=1,\ldots,n)}.$$

Bemerkung. Für $k = 1$ folgt $N = p$, also $\sum_F |S(F)|^2 = p^{n+1}$. Von den $p^n - 1$ Summanden mit $F \neq 0$ muß also mindestens einer $\geqq \frac{p^{n-1}}{p^n - 1} = \Omega(p)$ sein, d. h. mindestens ein $S(F) = \Omega(p^{\frac{1}{2}})$. Mehr als $\mathfrak{O}(p^{\frac{1}{2}})$ ist also allgemein nicht richtig.

Zur bestmöglichen Abschätzung der Lösungsanzahl des Kongruenzensystems $T_k^{(\nu)} \equiv U_k^{(\nu)}$ führt der Wert $k = n$. Dann fordert das System ja das

Übereinstimmen der ersten n Potenzsummen der t_κ und u_κ, also nach den Newtonschen Formeln ($p > n$) auch ihrer symmetrischen Grundfunktionen. Bei beliebig gegebenen u_κ sind also dann die t_κ bis auf die Reihenfolge eindeutig bestimmt. Man erhält somit höchstens $n!p^n$ Lösungen. Somit gilt:

$$\sum_F |S(F)|^{2n} \leqq n!p^{2n} = \mathfrak{O}(p^{2n}).$$

Nun kommt der Hauptgedanke. Die Gesamtheit der betrachteten Polynome $F(t)$ besitzt Automorphismen in sich, erzeugt durch lineare ganze Substitutionen der Variablen t (immer unter Auslassung des absoluten Gliedes), und zwar gibt es $p(p-1) = \mathfrak{O}(p^2)$ solche Substitutionen $t' \equiv \alpha t + \beta$. Dabei ändert sich jeweils der Betrag von $S(F)$ nicht. Zwar kann es vorkommen, daß ein F bei einer solchen Substitution in sich übergeht. Ist dabei F vom genauen Grade ν, so folgt $\alpha^\nu \equiv 1$, also ist α höchstens ν–deutig festgelegt, und β dann eindeutig falls $\nu > 1$ ist; es gibt also für jedes nichtlineare F höchstens n solche Substitutionen, für lineares $F \not\equiv 0$ dagegen p, und für $F \equiv 0$ sogar $p(p-1)$. Läßt man die sowieso trivialen linearen F aus der Summe fort und summiert im übrigen nur über nicht–äquivalente F, so erhält man eine Abschätzung

$$\begin{aligned} \frac{p(p-1)}{n} \sum_F{}^* |S(F)|^{2n} &= \mathfrak{O}(p^{2n}), \\ \sum_F{}^* |S(F)|^{2n} &= \mathfrak{O}(p^{2n-2}), \\ |S(F)| &= \mathfrak{O}(p^{1-\frac{1}{n}}). \end{aligned}$$

Das ist das Resultat von Mordell. Es ist nicht besser, als das Resultat der Weylschen Methode.

Bemerkung 1. Die Mordellsche Methode gibt in ihrer ersten Hälfte eine genaue Formel für den Mittelwert:

$$\frac{1}{p^n} \sum_F |S(F)|^{2k} = N\Big(T_k^{(\nu)} \equiv U_k^{(\nu)}\Big)_{(\nu=1,\ldots,n)}$$

bei beliebigem k. Sie reduziert das Studium der *einen* Kongruenz $F(t) \equiv a$ mit *einer* Variablen aber n Parametern $a_1, \ldots, a_n$ auf das Studium eines Systems von n Kongruenzen mit $2k$ Variablen aber *ohne* Parameter. — Nimmt

man an, daß *alle* $S(F)$ genau von derselben Größenordnung sind, so muß dieses die des Mittelwerts sein, und für $k = n$ folgt dann:

$$|S(F)|^{2n} = \mathfrak{O}(p^n)$$

$\big($die Lösungszahl ist genau $n!p^n + \mathfrak{O}(p^{n-1})\big)$, d. h.

$$|S(F)| = \mathfrak{O}(p^{\frac{1}{2}}).$$

Die Schwierigkeit des Problems liegt aber gerade darin, daß man nicht genug Automorphismen hat, um alle $S(F)$ als von gleicher Größenordnung zu erkennen. In F stecken n Parameter $a_1, \ldots, a_n$, aber nur 2 von ihnen können durch die $\mathfrak{O}(p^2)$ Automorphismen eliminiert werden, es bleiben also $n-2$ unabhängige Parameter. In allen verwendeten Problemen erhält man die „wahre“ Abschätzung nur dann, wenn es gelingt *alle* Parameter durch Automorphismen zu eliminieren.

Bemerkung 2. Kleinere k liefern schlechtere Resultate. Man könnte aber daran denken, mit größeren k, ja mit $k \to \infty$ nach dem Prinzip der Graeffeschen Näherungsmethode zu arbeiten. Dabei tritt ein Umstand ins Gewicht, der bei $k = n$ gerade noch harmlos ist, nämlich das Glied mit $F = 0$ links, mit $S(0) = p$. Es liefert zu dem Mittelwert $\frac{1}{p^n} \sum\limits_F |S(F)|^{2k}$ den Beitrag p^{2k-n}, der gerade dem Hauptglied der Lösungsanzahl rechts entspricht (n Kongruenzen für $2k$ Unbekannte). Für $k = n$ ist die Summe der übrigen Glieder links (wenn $S(F) = \mathfrak{O}(p^{\frac{1}{2}})$ genau richtig ist) noch von derselben Ordnung: $\frac{1}{p^n}(p^n - 1)\mathfrak{O}(p^n) = \mathfrak{O}(p^n)$. Für $k > n$ wird dagegen diese Summe von kleinerer Ordnung: $\frac{1}{p^n}(p^n - 1)\mathfrak{O}(p^k) = \mathfrak{O}(p^k)$, und die Abschätzung läuft auf die *Restabschätzung* der Kongruenzlösungsanzahl des Systems $T_k^{(\nu)} \equiv U_k^{(\nu)}$ hinaus. Diese ist aber keineswegs einfach. Um auf $S(F) = \mathfrak{O}(p^{\frac{1}{2}})$ schließen zu können, müßte man diese Restabschätzung mit der Genauigkeit

$$N(T_k^{(\nu)} \equiv U_k^{(\nu)}) = p^{2k-n} + \mathfrak{O}(p^{k+r(n)})$$

machen, wo $r(n)$ nicht von k abhängt. Dann folgte in der Tat für $k \to \infty$ jedenfalls:

$$S(F) = \mathfrak{O}(p^{\frac{1}{2}+\varepsilon}) \quad \text{für jedes} \quad \varepsilon > 0.$$

Man kommt aber bis heute auf diesem Wege nicht durch.

Es gibt einige Fälle, von den parameterfreien Gaußschen Summen abgesehen, wo man jedenfalls bessere Resultate als das Mordellsche $S(F) = \mathcal{O}(p^{1-\frac{1}{n}})$ hat.

Zunächst hat im Falle $n = 3$ Davenport durch Eingehen auf die algebraische Struktur der kubischen Polynome bewiesen:

$$S(F) = \mathcal{O}(p^{\frac{5}{8}}) \quad \text{für} \quad n = 3.$$

Mordell's Resultat gibt hier nur $\mathcal{O}(p^{\frac{2}{3}})$.

Ferner hat Davenport das Mordellsche Resultat allgemein etwas verschärft:

$$S(F) = \mathcal{O}(p^{1-\frac{1}{n_0}}), \qquad \begin{array}{l}\text{wenn } n_0 \text{ die größte Zahl einer der For-}\\ \text{men } 2^\nu, 3.2^\nu \text{ ist, die } \leqq n \text{ ist.}\end{array}$$

Schließlich hat Mordell noch die Abschätzung bewiesen:

$$S(F) = \mathcal{O}(p^{1-\frac{1}{2r}}), \qquad \begin{array}{l}\text{wenn } r \text{ die genaue Anzahl der in } F \text{ wirklich}\\ \text{vorkommenden nicht–konstanten Glieder ist.}\end{array}$$

Diese ist unter Umständen besser als die vorher hergeleitete allgemeine Abschätzung.

Dies letztere Mordellsche Resultat gilt auch, wenn man für die Glieder von F negative Exponenten zuläßt. Dann fällt die betr. Summe unter den allgemeinen Typus

$$S(\mathsf{R}) = \sum_t{}' e\big(\mathsf{R}(t)\big),$$

wo $\mathsf{R}(t)$ eine beliebige rationale Funktion über P_p ist, und die Summation natürlich die Nullstellen des Nenners zu vermeiden hat. Hier hat man zwar $\mathcal{O}(p^3)$ Automorphismen $t' \equiv \frac{\alpha t+\beta}{\gamma t+\delta}$, aber die Mordellsche Methode der Summation über die Koeffizienten von F überträgt sich nicht ohne weiteres auf R. Ansätze mittels Partialbruchzerlegung von $\mathsf{R}(t)$ stoßen auf Schwierigkeiten. Immerhin dürfte dies Problem mit einigem Geschick zu einem Resultat der Form $\mathcal{O}(p^{1-\frac{1}{N}})$ durchführbar sein, wo N von der algebraischen Struktur von R abhängt. Das wird durch Davenportsche Untersuchungen für niedrigere Gradzahlen bestätigt.

Besonders bemerkenswert ist noch der Spezialfall der Kloostermanschen Summen:

$$\mathsf{R}(t) \equiv at + bt^{-1},$$

die mit der Verteilung der Reziproken mod p zu tun haben. Für sie liefert das angeführte Mordellsche Resultat ($r = 2$) sofort:

$$S(\mathsf{R}) = \mathcal{O}(p^{\frac{3}{4}}).$$

Das hatte schon Kloosterman bewiesen; der bei verfeinerter Untersuchung des quadratischen quaternären Darstellungsproblems nach der Hardy–Littlewoodschen Methode auf diese Summen gestoßen war. Neuerdings haben Davenport und Salié unabhängig voneinander

$$S(\mathsf{R}) = \mathcal{O}(p^{\frac{2}{3}})$$

bewiesen. Natürlich vermutet man auch hier, wie überhaupt für die allgemeinste rationale Funktion R

$$S(\mathsf{R}) = \mathcal{O}(p^{\frac{1}{2}}).$$

Das Mordellsche Hauptresultat

$$S(F) = \mathcal{O}(p^{1-\frac{1}{n}})$$

überträgt sich leicht auf den Fall eines beliebigen endlichen Körpers P_q statt P_p. Hier handelt es sich um die Summe

$$S(F) = \sum_t e\big(\operatorname{Sp} F(t)\big),$$

wo jetzt $F(t)$ ein beliebiges Polynom über P_q ist, t den Körper P_q durchläuft, und Sp die Spur in P_q bezeichnet:

$$\operatorname{Sp} a \equiv a + a^p + \cdots + a^{\frac{q}{p}}.$$

Hier hat man nur die folgende Tatsache zu beachten:

$$\operatorname{Sp} uv \equiv 0 \quad \text{für alle } v \longleftrightarrow u \equiv 0,$$

die ohne weiteres aus der Tatsache folgt, daß P_q über P_p die „Diskriminante“ 1 hat, d. h. $|v_i^{p^\nu}| \not\equiv 0$ $(i, \nu = 0, \ldots, n-1)$ für eine Basis v_i von P_q. Mittels dieser Tatsache sieht man zunächst ein, daß wieder

$$S(F) = \sum_a N_a e(\operatorname{Sp} a),$$

also ein Mittelwert der Kongruenzlösungszahlen

$$N_a = N\big(F(t) \equiv a\big)$$

ist (alle Summationen etz. jetzt in P_q verstanden!). Ferner liefert auf Grund dieser Tatsache die Mordellsche Methode fast ohne Änderung das Resultat:

$$S(F) = \mathfrak{O}(q^{1-\frac{1}{n}}),$$

wenn F vom Grade n.

Es scheint mir ohne Zweifel — wenn ich es auch noch nicht explizit durchgeführt habe —, daß auch alle genannten Verschärfungen des Mordellschen Hauptresultats sich in gleicher einfacher Weise auf P_q übertragen.

3.) Ich will jetzt noch auf den Fall der Kongruenzen in 2 Variablen eingehen, der für die Artinschen und F. K. Schmidtschen Zetafunktionen wichtig ist.

Sei $F(t,x)$ ein irreduzibles Polynom in x,t über P_p. Dann kommt es zum Nachweis der Riemannschen Vermutung für jene Funktionen auf den Nachweis der Tatsache an:

$$\text{in } \mathsf{P}_p: \qquad N\big(F(t,x) \equiv 0\big) = p + \mathfrak{O}(p^{\frac{1}{2}+\varepsilon}) \qquad \text{für jedes } \varepsilon > 0,$$

und allgemeiner

$$\text{in } \mathsf{P}_q: \qquad N\big(F(t,x) \equiv 0\big) = q + \mathfrak{O}(q^{\frac{1}{2}+\varepsilon}) \qquad \text{“} \qquad \text{“} \qquad \text{“}\,.$$

In dieser Richtung weiß man nun bis heute sehr wenig. Für den Fall eines *quadratischen* Polynoms $F(x,t)$ weiß man durch Untersuchungen von Jacobsthal, die schon bei Gauß vorbereitet sind, daß sogar

$$N = p, p+1 \quad \text{oder} \quad p-1$$

ist (und entsprechend in P_q). Aber dies ist für unsere Zwecke uninteressant, weil hier bei Reduktion auf den Typus $D(t) \equiv x^2$ das Polynom $D(t)$ den Grad $n = 1$ bekommt, also gar keine nicht–trivialen Nullstellen von $\zeta_D(s)$ vorliegen.

Ferner weiß man hier ein schönes Resultat von Mordell für den Fall eines *kubischen* Polynoms $F(t,x)$, nämlich

$$\text{in } \mathsf{P}_p: \qquad N\big(F(t,x) \equiv 0\big) = p + \mathfrak{O}(p^{\frac{2}{3}}).$$

Auch dieses Mordellsche Resultat läßt sich nach den oben genannten Prinzipien sofort auf P_q übertragen:

$$\text{in } \mathsf{P}_q: \qquad N\big(F(t,x) \equiv 0\big) = q + \mathcal{O}(q^{\frac{2}{3}}),$$

sodaß dann also bewiesen ist, daß die Nullstellen der betr. ζ–Funktionen alle im Streifen $\frac{1}{3} \leqq \Re(s) \leqq \frac{2}{3}$ liegen.

Weitere Resultate in der genannten Richtung kennt man durch Mordell und Davenport in dem bei Artin betrachteten *hyperelliptischen* Fall $F(t,x) \equiv D(t) - x^2$, wo wir wieder $D(t)$ ohne Einschränkung als quadratfrei und von ungeradem Grad $n \geqq 3$ annehmen dürfen:

(NB. Für $n = 1$ gilt ohne weiteres $q + \mathcal{O}(q^{\frac{1}{2}})$ — Gaußsche Summen — also die Riemannsche Verm.)

$$\begin{array}{lcccll} N\big(D(t) \equiv x^2\big) - q & = & \mathcal{O}(q^{\frac{2}{3}}) & \text{für} & n = 3 & \text{(Mordell)} \\ & = & \mathcal{O}(q^{\frac{7}{8}}) & \shortparallel & n = 5 & \text{(Mordell)} \\ & = & \mathcal{O}(q^{\frac{19}{20}}) & \shortparallel & n = 7 & \text{(Davenport)} \\ & & \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & & \end{array}$$

und allgemein in Fortführung dieser Resultate:

$$= \mathcal{O}\left(q^{1 - \frac{1}{(n+3)2^{\frac{n-5}{2}}}}\right) \qquad \text{(Davenport)}$$

Die Folgerungen hieraus für die ζ–Funktionsnullstellen liegen auf der Hand nach dem schon Gesagten.

Für die beiden letztgenannten Resultate ist allerdings noch eine algebraische Eliminationsschwierigkeit zu überwinden, sowie die Übertragung auf den Fall P_q zu kontrollieren — bei Mordell und Davenport wird immer nur der Fall P_p behandelt. Die Mordellschen Anfangsresultate ergeben sich nach einer weitgehend analogen Methode zu der oben auseinandergesetzten Mordellschen Methode für die Kongruenzlösungsanzahlen in einer Variablen. Für die höheren Davenportschen Resultate ist eine Weiterbildung der Mordellschen Methode erforderlich, die in sukzessivem Quadrieren und Anwendung quadratischer Substitutionen besteht.

Mordell und Davenport haben dann auch noch den allgemeineren Fall $D(t) \equiv x^m$ untersucht, wo ohne Einschränkung m als Teiler von $p - 1$ ange-

nommen werden darf. Hier ist das am meisten hervorstechende Resultat:

$$N\big(D(t) \equiv x^3\big) = q + \mathfrak{O}(q^{\frac{1}{2}}) \qquad \text{(Mordell)}, \quad \text{wenn} \quad n = 3.$$

Davenport konnte sogar die Lösungszahl genau ausdrücken, als Funktion der Koordinaten a, b in $p = a^2 + ab + b^2$.

> Für diesen Fall ist also das Analogon der Riemannschen Vermutung bestätigt.

Außerdem haben Mordell und Davenport noch eine Reihe weiterer Resultate in dieser Richtung gefunden, die ich aber hier nicht alle aufzählen will.

1.13 Marburg 1933 I

Über die Nullstellen der Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen.

Vortrag Marburg, Februar 1933.

1.) P_p beliebiger endlicher Körper, p Elementzahl (Potenz einer Primzahl p_0)

$\mathsf{P}_p(x)$ Körper der rationalen Funktionen einer Unbestimmten x über P_p.

Weitgehende Analogie zur gewöhnlichen Zahlentheorie im Körper der rationalen Zahlen:

Ganze Zahlen	Integritätsbereich $\mathsf{P}_p[x]$ der Polynome in x über P_p.
Primzahlen	Primpolynome $P(x)$
absoluter Betrag	p^{Grad}
Einheiten (± 1)	Elemente $\neq 0$ aus P_p

Artin hat nun in seiner Dissertation die Theorie der quadratischen Körper $\mathsf{K} = \mathsf{P}_p(x, \sqrt{F(x)})$ über $\mathsf{P}_p(x)$ in weitgehender Analogie zur Theorie der gewöhnlichen quadratischen Körper entwickelt. Und F. K. Schmidt hat in seiner Dissertation dann auch die allgemeine Theorie der algebraischen Erweiterungskörper K endlichen Grades von $\mathsf{P}_p(x)$ durchgeführt. Außer der bereits genannten Analogie zur Zahlentheorie steht bei F.K. Schmidt eine zweite Analogie im Vordergrund: Eine algebraische Erweiterung K endlichen Grades über $\mathsf{P}_p(x)$ wird nämlich definiert durch Adjunktion einer Nullstelle eines Polynoms $F(x, y)$ über $\mathsf{P}_p[x]$, und kann daher als „Körper algebraischer Funktionen über P_p“ aufgefaßt und in Analogie zur gewöhnlichen Theorie der algebraischen Funktionen über dem Körper der komplexen Zahlen behandelt werden. Bei dieser Auffassung verliert die unabhängige Variable x ihre ausgezeichnete Bedeutung, sie kann durch jedes über P_p transzendente Element u ersetzt werden, und K dann in der Form $\mathsf{P}_p(u, v)$ mit über $\mathsf{P}_p(u)$ algebraischem v dargestellt werden (birationale Transformation).

Artin und F.K. Schmidt haben beide ihre algebraisch–arithmetische Theorie durch Einführung des Analogons zur Dedekindschen ζ–Funktion und Entwicklung einer analogen Theorie von Residuum bei $s = 1$, Funktionalgleichung und Nullstellenproblem ergänzt. Über diese analytische Theorie will ich nachstehend berichten, und zwar insbesondere über das Nullstellenproblem. Dieses ist zwar unendlich viel einfacher, als das Nullstellenproblem

der Riemannschen und der Dedekindschen ζ–Funktionen, hauptsächlich deshalb, weil die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen periodisch im imaginären Teil t von $s = \sigma + it$ (mit der Periode $\frac{2\pi}{\log p}$) sind, während die Riemannsche und die Dedekindschen ζ–Funktionen nur fastperiodisch in t sind. Aber es bleibt noch immer ein tiefliegendes mathematisches Problem, das bis heute nur in Spezialfällen befriedigend gelöst ist. Immerhin zeigen schon diese Spezialfälle, und weitere in Richtung des Analogons zur Riemannschen Vermutung liegenden Teilresultate, daß für die Artinschen und F.K. Schmidtschen ζ–Funktionen das Nullstellenproblem mit den heutigen Hilfsmitteln „angreifbar“ ist, während es bei der Riemannschen und den Dedekindschen ζ–Funktionen heute völlig „unangreifbar“ erscheint.

Ich werde mich hier sofort an die allgemeine F.K. Schmidtsche Definition der ζ–Funktion $\zeta_{\mathsf{K}}(s)$ eines Körpers K der oben beschriebenen Art halten. Diese ist nicht nur durch die Allgemeinheit von der Artinschen unterschieden — Artin behandelt nur quadratische Körper K über $\mathsf{P}_p(x)$ —, sondern auch dadurch, daß F.K. Schmidt von vornherein den birational invarianten Standpunkt der algebraischen Funktionentheorie einnimmt, bei dem der Körper $\mathsf{P}_p(x)$ und folglich auch der Grad $[\mathsf{K} : \mathsf{P}_p(x)]$ gar keine invariante Bedeutung hat, und eine birational invariante Funktion $\zeta_{\mathsf{K}}(s)$ definiert. Der Übergang zu der nicht–invarianten Artinschen Funktion im Artinschen Spezialfall, der invariant als der „hyperelliptische“ Fall charakterisiert ist, kann dann leicht vollzogen werden (Abspaltung endlich vieler trivialer Faktoren), interessiert aber nicht weiter.

2.) Die F.K. Schmidtsche Definition der Funktion $\zeta_{\mathsf{K}}(s)$ beruht auf dem Begriff der Primstelle und des Primdivisors von K, die in voller Analogie zur Theorie der gewöhnlichen algebraischen Funktionen einführbar sind. Man muß zur Herstellung der Analogie nur nicht von der geometrisch–anschaulichen Definition der Riemannschen Fläche und ihrer Stellen ausgehen, sondern von der arithmetisch–abstrakten. Am besten kommt das in der Sprechweise der Bewertungstheorie zum Ausdruck.

Unter einer *Primstelle* $\mathfrak{P}$ von K versteht man eine Bewertung von K. Es stellt sich heraus, daß jede Bewertung von K diskret ist, d. h. es gibt ein Element Π größten Wertes < 1, und jedes Element $\mathsf{A} \neq 0$ von K ist dann eindeutig in der Form

$$\mathsf{A} = \mathsf{E}\,\Pi^a$$

darstellbar, wo a ganz–rational ist und E den Wert 1 hat, sodaß

$$|\mathsf{A}|_{\mathfrak{P}} = |\Pi|_{\mathfrak{P}}^{a}$$

der Wert von A für $\mathfrak{P}$ ist. a heißt die *Ordnung von* A *für* $\mathfrak{P}$. A heißt *ganz für* $\mathfrak{P}$, wenn $a \geqq 0$, *durch* $\mathfrak{P}^b$ *teilbar*, wenn $a \geqq b$. Hiernach ist klar, was *Restklasse* mod $\mathfrak{P}^b$ (im Bereich der für $\mathfrak{P}$ ganzen A) heißt. Die Restklassen mod $\mathfrak{P}$ bilden einen Körper. Dieser erweist sich als endlich, sein Grad f über P_p heißt der (*absolute*) *Grad von* $\mathfrak{P}$, seine Elementzahl p^f heißt die (*absolute*) *Norm von* $\mathfrak{P}$, Bezeichnung $\mathfrak{N}\mathfrak{P} = p^f$.

Dabei ist hier wie durchweg im folgenden P_p bei gegebenem K als der *größte* endliche Teilkörper von K zu verstehen. Dann ist also *jedes* nicht zu P_p gehörige Element x aus K über P_p transzendent und kann zum algebraischen Aufbau von K von $\mathsf{P}_p(x)$ aus verwendet werden.

Eine Übersicht über alle Primstellen $\mathfrak{P}$ von K werden wir gleich entwickeln. Sie ergibt insbesondere, daß es nur abzählbar viele solche gibt. Die ζ–Funktion von K ist dann definiert durch:

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{\mathfrak{N}\mathfrak{P}^s}} \,.$$

Indem man formal beliebige Potenzprodukte je endlich vieler $\mathfrak{P}$:

$$\mathfrak{A} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_r^{a_r}$$

mit ganz–rationalen Exponenten als *Divisoren* einführt (die $\mathfrak{P}$ heißen daher dann auch Primdivisoren) und die *ganzen Divisoren* als solche mit Exponenten $a_i \geqq 0$ erklärt, erhält man (vorbehaltlich des Konvergenznachweises) die andere Darstellung:

$$\zeta_{\mathsf{K}}(s) = \sum_{\mathfrak{A}} \frac{1}{\mathfrak{N}\mathfrak{A}^s} \,,$$

wo über alle ganzen Divisoren $\mathfrak{A}$ von K summiert ist und

$$\mathfrak{N}\mathfrak{A} = \mathfrak{N}\mathfrak{P}_1^{a_1} \cdots \mathfrak{N}\mathfrak{P}_r^{a_r}$$

gesetzt ist.

Die sämtlichen Primstellen $\mathfrak{P}$ von K kann man durch Einführung einer Darstellung

$$\mathsf{K} = \mathsf{P}_p(x, y)$$

von $\mathsf{P}_p(x)$ aus durch algebraische Erweiterung übersehen. Jede Bewertung $\mathfrak{P}$ von K entsteht nämlich durch Fortsetzung einer Bewertung $\mathfrak{p}$ von $\mathsf{P}_p(x)$, und umgekehrt läßt sich jede Bewertung $\mathfrak{p}$ von $\mathsf{P}_p(x)$ auf endlich viele Arten zu Bewertungen $\mathfrak{P}$ von K fortsetzen. Genauer gilt dabei: Sind $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ die zu $\mathfrak{p}$ gehörigen Primstellen von K und $e_1, \ldots, e_r$ ihre *Relativordnungen* (ein Primelement π für $\mathfrak{p}$ hat die Ordnung e_i für $\mathfrak{P}_i$), $f_1, \ldots, f_r$ ihre *Relativgrade* (der Restklassenkörper mod $\mathfrak{P}_i$ hat über dem mod $\mathfrak{p}$ den Relativgrade f_i), so ist

$$\sum_{i=1}^{r} e_i f_i = n_x$$

der Grad von K über $\mathsf{P}_p(x)$. Man schreibt dann auch:

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad N(\mathfrak{P}_i) = \mathfrak{p}^{f_i}.$$

(So kann dann auch die *Relativnorm* beliebiger Divisoren in bezug auf $\mathsf{P}_p(x)$ erklärt werden, doch brauchen wir das nicht.) Ist f_0 der Absolutgrad von $\mathfrak{p}$, so sind $f_0 f_i$ die Absolutgrade der $\mathfrak{P}_i$. Die Aufgabe, alle Primdivisoren $\mathfrak{P}$ von K zu ermitteln reduziert sich dann auf zwei Punkte:

a.) alle Primdivisoren $\mathfrak{p}$ von $\mathsf{P}_p(x)$ zu ermitteln,

b.) die Zerlegung der $\mathfrak{p}$ in K zu ermitteln.

Die letztere Aufgabe ist das Analogon zur Herleitung des Zerlegungsgesetzes in der algebraischen Zahlentheorie. Für über $\mathsf{P}_p(x)$ abelsche K hat F. K. Schmidt sie in voller Analogie dazu durch Übertragung der gesamten Klassenkörpertheorie gelöst. Wir brauchen das hier nicht, sind ja auch nicht bloß mit dem abelschen Spezialfall beschäftigt; für den Artinschen Spezialfall liegt natürlich gerade ein solcher abelscher Fall vor. Wir brauchen hier im wesentlichen nur den schon angegebenen allgemeinen Typ des Zerlegungsgesetzes.

Die erstere Aufgabe ist leicht gelöst. An Bewertungen $\mathfrak{p}$ von $\mathsf{P}_p(x)$ gibt es genau die folgenden: Für jede (normierte) Primfunktion $P(x)$ eine, nämlich nach der Teilbarkeit durch $P(x)$, $\pi = P(x)$, $f_0 =$ Grad von $P(x)$; und außerdem eine unendliche Primstelle $\mathfrak{p}_\infty$, der „absoluten“ Bewertung von $\mathsf{P}_p(x)$ (nach dem Grad) entsprechend, $\pi = \frac{1}{x}$.

Aus dieser Übersicht über die Primdivisoren und damit alle Divisoren von K ergibt sich die Konvergenz und Gültigkeit obiger beiden Darstellungen von $\zeta_{\mathsf{K}}(s)$ dort.

Die Artinsche ζ–Funktion würde entstehen, wenn man die endlich vielen $\mathfrak{P}/\mathfrak{p}_\infty$ ausläßt. Wir wollen das nicht weiter verfolgen.

3.) Um nun zu tieferliegenden Einsichten in die Struktur von $\zeta_\mathsf{K}(s)$ zu gelangen, braucht man ein ziemlich tief liegendes Theorem über die Divisoren von K, nämlich das Analogon des Riemann–Rochschen Satzes. Für die additive Darstellung der Funktion $\zeta_\mathsf{K}(s)$ kommt es nämlich nur darauf an zu wissen, wieviel ganze Divisoren $\mathfrak{A}$ mit gegebener $\mathfrak{N}\mathfrak{A} = p^n$ es in K gibt. Ich nenne n auch den *Grad* des Divisors $\mathfrak{A}$. Jeder durch ein Element $\mathsf{A} \neq 0$ aus K gelieferte Divisor hat den Grad 0 und legt das Element A bis auf eine Einheit (Element aus P_p) eindeutig fest. Diese Divisoren sind (bis auf den den Einheiten entsprechenden Divisor 1) sämtlich gebrochen, treten also in $\zeta_\mathsf{K}(s)$ nicht direkt in Erscheinung. Wohl aber indirekt so: Mit $\mathfrak{A}$ haben auch alle Divisoren $\mathfrak{A}\mathsf{A}$ den Grad n. Diese bilden die *Klasse* des Divisors $\mathfrak{A}$. Für die Funktion $\zeta_\mathsf{K}(s)$ kommt es also nur darauf an:

a.) Die Divisorenklassen zu übersehen,

b.) Die Anzahl der ganzen Divisoren einer Klasse zu kennen.

Das letztere, und dann auch das erstere, leistet der Riemann–Rochsche Satz, und zwar das letztere genau nach dem Schema der algebraischen Zahlentheorie:

Ist C eine Klasse, $\mathfrak{C}$ fest aus C^{-1}, so entsprechen die ganzen Divisoren $\mathfrak{A}$ aus C auf Grund von

$$\mathfrak{A} = \frac{\mathsf{A}}{\mathfrak{C}}$$

umkehrbar eindeutig bis auf den willkürlichen Einheitsfaktor den ganzen Multipla $\mathsf{A} \neq 0$ von $\mathfrak{C}$. Genauer ist d die Anzahl der bzgl. P_p linear unabhängigen ganzen Multipla von $\mathfrak{C}$, so ist d unabhängig von der Auswahl des festen Divisors $\mathfrak{C}$ aus C (Dimension von C, Bezeichnung $\{C\}$), und dann $\frac{p^d-1}{p-1}$ die Anzahl aller ganzen Divisoren von C. Das Analogon des Riemann–Rochschen Satzes macht nun eine Aussage über die Dimension $\{C\}$. Ganz analog wie in der algebraischen Zahlentheorie kann man nämlich zu jeder Klasse C eine komplementäre Klasse C' definieren. Man stützt sich dazu auf ein festes x (so, daß K über $\mathsf{P}_p(x)$ von 1. Art ist, was stets erreichbar), und betrachtet zunächst den Divisor

$$\mathfrak{Z}_x = \frac{\mathfrak{D}_x}{\mathfrak{N}_x^2},$$

wo $\mathfrak{D}_x$ der *Differentendivisor* von K über $\mathsf{P}_p(x)$ ist (in üblicher Weise erklärt) und $\mathfrak{N}_x$ der Nennerdivisor von x. Die Klasse W dieses Divisors erweist sich als eine Invariante (Analogon der Differentialklasse der algebraischen Funktionentheorie), insbesondere also auch sein Grad, den man als $2g-2$ bezeichnet. Es ist dann g das Analogon des *Geschlechts*, das sich (gerade durch den Riemann–Rochschen Satz) als ganzzahlig $\geqq 0$ erweist, und das man aus den Graden d_x und n_x von $\mathfrak{D}_x$ und $\mathfrak{N}_x$ also so berechnet:

$$2g-2 = d_x - 2n_x, \qquad g = \frac{d_x}{2} - n_x + 1.$$

Zwei Klassen C, C' heißen komplementär, wenn

$$CC' = W$$

ist. Und das Analogon des Riemann–Rochschen Satzes sagt aus:

$$\{C\} = \{C'\} + n - (g-1)$$

und somit

$$\{C\} - \frac{n}{2} = \{C'\} - \frac{n'}{2},$$

wenn n, n' die Grade von C und C' sind. Das ergibt insbesondere die Ganzzahligkeit von g, und (für $n = 2g-1$) auch $g \geqq 0$. Für $n > 2g-2$ ist $n' < 0$ also sicher $\{C'\} = 0$, d. h.

$$\{C\} = n - (g-1) \quad \text{für} \quad n > 2g-2.$$

Mittels des Analogons des Riemann–Rochschen Satzes ergibt sich dann ferner, daß es für jeden Grad n nur endlich viele, und zwar gleich viele Divisorenklassen gibt. Diese Anzahl h, eine wichtige Invariante von K, heißt die *Klassenzahl von* K.

h ist *nicht* das genaue Analogon der gewöhnlichen Klassenzahl algebraischer Zahlkörper. Dieses kommt vielmehr erst heraus, wenn man ein Element x auszeichnet und zu den Idealen des Integritätsbereichs $\mathfrak{I}_x$ der in x ganzen Elemente übergeht (Auslassung der endlich vielen Primdivisoren $\mathfrak{P}/\mathfrak{p}_\infty = \frac{1}{x}$, Artinscher Standpunkt). Man findet:

$$h = \frac{h_x \mathsf{R}_x}{u_x},$$

wo

h_x die Idealklassenzahl in $\mathfrak{I}_x$
R_x der Regulator von $\mathfrak{I}_x$
u_x der gr. gem. Teiler der Grade der $\mathfrak{P}/\mathfrak{p}_\infty = \frac{1}{x}$.]

Daß es wirklich für *jeden* Grad n Divisoren in K gibt, ist allerdings erst eine Folge aus der analytischen Theorie $\big($Residuum von $\zeta_{\mathsf{K}}(s)\big)$. Ich stelle diese Tatsache hier, wo es sich nur um einen Tatsachenbericht nicht um Beweise handelt, voran, um die Formeln nicht mit einem Parameter n_0 (gr. gem. Teiler der Grade aller Primdivisoren — kleinster positiver Divisorengrad) zu belasten, der sich dann doch nachträglich als 1 herausstellt.

Ferner ergibt sich dann auch noch, daß man x stets so wählen kann, daß $[\mathsf{K} : \mathsf{P}_p(x)] = g+1$ ist (für $n = g+1$ ist $\{C\} \geqq 2$, was die Existenz eines nicht zu P_p gehörigen Hauptdivisors x mit Zähler und Nenner vom Grade $g+1$ ergibt). Für $g = 0$ folgt speziell, daß K als $\mathsf{P}_p(x)$ selbst darstellbar ist.

4.) Aus dem Vorstehenden ergibt sich unmittelbar folgende Entwicklung für $\zeta_{\mathsf{K}}(s)$:

$$\zeta_{\mathsf{K}}(s) = \sum_{n=0}^{\infty} \sum_{i=1}^{h} \frac{p^{\{C_n^{(i)}\}} - 1}{p-1} \cdot \frac{1}{p^{ns}},$$

wo $C_n^{(i)}$ jeweils die h Klassen des Grades n durchläuft, und dann weiter:

$$\zeta_{\mathsf{K}}(s) = \sum_{n=0}^{2g-2} \sum_{i=1}^{h} \frac{p^{\{C_n^{(i)}\}} - 1}{p-1} \cdot \frac{1}{p^{ns}} + h \cdot \sum_{n=2g-1}^{\infty} \frac{p^{n-(g-1)} - 1}{p-1} \cdot \frac{1}{p^{ns}}$$

(auch für $g = 0$, weil dann der formal eingeführte Summand mit $n = -1$ in der zweiten Summe Null ist, während die erste Summe ja leer ist). Für $g = 0$ (also $h = 1$) ergibt sich so als Analogon der gewöhnlichen Riemannschen ζ–Funktion:

$$\begin{aligned} \zeta(s) &= \frac{1}{p-1} \left[\frac{p}{1 - \frac{p}{p^s}} - \frac{1}{1 - \frac{1}{p^s}} \right] \\ &= \frac{1}{1 - \frac{p}{p^s}} \cdot \frac{1}{1 - \frac{1}{p^s}} \\ &= \frac{p^s}{p-1} \left[1 + \frac{p^{1-s}}{1 - p^{1-s}} + \frac{p^s}{1 - p^s} \right]. \end{aligned}$$

Für $g > 0$ kann man ferner so schreiben:

$$\zeta_{\mathsf{K}}(s) = \frac{1}{p-1}\sum_{n=0}^{2g-2}\sum_{i=1}^{h}\frac{p^{\{C_n^{(i)}\}}}{p^{ns}} + \frac{h}{p-1}\,\frac{1}{p^{(g-1)s}}\left[\frac{p^{g(1-s)}}{1-p^{1-s}} + \frac{p^{gs}}{1-p^{s}}\right].$$

Hieraus liest man ab:

I.) $\zeta_{\mathsf{K}}(s)$ *ist periodisch mit der Periode* $\frac{2\pi i}{\log p}$ *und regulär in der ganzen Ebene bis auf Pole 1. Ordnung bei* $s = 0, s = 1$ *und den homologen Stellen mit den Residuen*

$$-\frac{h}{p-1}\cdot\frac{1}{\log p}\,, \qquad \frac{1}{p^{g-1}}\cdot\frac{h}{p-1}\cdot\frac{1}{\log p}\,.$$

Ferner folgert man leicht:

II.) $\zeta_{\mathsf{K}}(s)$ *genügt der Funktionalgleichung*:

$$p^{(g-1)s}\zeta_{\mathsf{K}}(s) = p^{(g-1)(1-s)}\zeta_{\mathsf{K}}(1-s).$$

Für die Polglieder ist das aus obiger Schreibweise ersichtlich: sie tauschen sich bei $s \to 1-s$ aus. Das tun auch die Glieder der ersten Summe, die man nach Abspaltung des Faktors $\frac{1}{p-1}\cdot\frac{1}{p^{(g-1)s}}$ ja so schreiben kann:

$$\begin{aligned} p^{(g-1)s}\sum_{n=0}^{2g-2}\sum_{C_n}\frac{p^{\{C_n\}}}{p^{ns}} &= p^{\frac{g-1}{2}}\sum_{n=0}^{2g-2}\sum_{C_n}\frac{p^{\{C_n\}-\frac{n}{2}}}{p^{(n-(g-1))(s-\frac{1}{2})}} \\ &= p^{\frac{g-1}{2}}\sum_{n=0}^{2g-2}\sum_{C_n}\frac{p^{\{C_n\}-\frac{n}{2}}}{p^{(\{C_n\}-\{C'_{n'}\})(s-\frac{1}{2})}}\,; \end{aligned}$$

hier sind $\{C_n\} - \frac{n}{2}$ und $\{C_n\} - \{C'_{n'}\}$ symmetrisch bzw. antisymmetrisch in den komplementären Klassen $C_n, C'_{n'}$ (ersteres nach dem Analogon des Riemann–Rochschen Satzes), und der Summationsbereich wird durch $C_n \to C'_{n'}$ in sich abgebildet. —

In der üblichen, von der gewöhnlichen Riemannschen ζ–Funktion bekannten Weise folgert man aus der Produktentwicklung und dem Pol bei $s = 1$ ferner:

III.) $\zeta_{\mathsf{K}}(s) \neq 0$ *für* $\sigma = 1$*; daher liegen die ev. Nullstellen von* $\zeta_{\mathsf{K}}(s)$ *sämtlich in* $0 < \sigma < 1$.

Ferner:

IV.) *Es ist*

$$\frac{\zeta_{\mathsf{K}}(s)}{\zeta(s)} = 1 + \frac{\sigma_1}{p^s} + \cdots + \frac{\sigma_{2g}}{p^{2gs}} = P(z)$$

ein Polynom vom Grade $2g$ *in* $z = \frac{1}{p^s}$ *. Hierin ist*

$$\sigma_1 = N_1 - (p+1),$$

wo N_1 *die Anzahl der ganzen (Prim–)Divisoren vom Grade* 1 *in* K *ist, und*

$$\sigma_{2g} = p^g.$$

$\zeta_{\mathsf{K}}(s)$ *hat also für* $g > 0$ *wirklich Nullstellen, nämlich genau* $2g$ *im Periodenstreifen.*

Zum Beweis betrachte man $\zeta_{\mathsf{K}}(s)$ und $\zeta(s)$ als rationale Funktionen von $z = \frac{1}{p^s}$. Im Endlichen haben beide Pole genau bei $z = 1$ und $z = \frac{1}{p}$, und zwar von der 1. Ordnung. Also ist der Quotient $\frac{\zeta_{\mathsf{K}}(s)}{\zeta(s)}$ ein Polynom in z, da ja $\zeta(s)$ keine Nullstellen hat. Grad und höchster Koeffizient ergeben sich ohne weiteres durch Betrachtung der höchsten Glieder in z bei $\zeta_{\mathsf{K}}(s)$ und $\zeta(s)$:

$$\{C^{(i)}_{2g-2}\} = \begin{cases} g-1 & \text{für} \quad C^{(i)}_{2g-2} \neq W, \\ g & \text{für} \quad C^{(i)}_{2g-2} = W. \end{cases}$$

$$\begin{array}{lcl} \zeta_{\mathsf{K}}(s) & : & z^{2g-2}\left(\frac{(h-1)p^{g-1}+p^g}{p-1} - \frac{hp^{g-1}}{p-1}\right) = z^{2g-2}p^{g-1} \\ \zeta(s) & : & z^{-2}p^{-1} \end{array}$$

$$\zeta_{\mathsf{K}}(s) \quad : \quad z^{2g}p^g\,, \quad \text{also Grad } 2g, \quad \sigma_{2g} = p^g.$$

Der Koeffizient von z ergibt sich einfach aus:

$$\begin{array}{lcl} \zeta_{\mathsf{K}}(s) & = & 1 + \frac{N_1}{p^s} + \cdots \\ \zeta(s) & = & 1 + \frac{p+1}{p^s} + \cdots\,, \end{array}$$

letzteres, da in $\mathsf{P}_p(x)$ genau $p+1$ Primdivisoren vom Grad 1 vorhanden sind, entsprechend den p linearen Primfunktionen $x - a$, nebst dem unendlichen Primdivisor $\mathfrak{p}_\infty = \frac{1}{x}$. —

5.) Für die Behandlung der Nullstellen von $\zeta_{\mathsf{K}}(s)$ ist es bequemer, $z = p^s$ zu setzen und

$$p^{2gs}\frac{\zeta_{\mathsf{K}}(s)}{\zeta(s)} = P(z) = z^{2g} + \sigma_1 z^{2g-1} + \cdots + \sigma_{2g}$$
$$= z^{2g} + \big(N_1 - (p+1)\big)z^{2g-1} + \cdots + p^g$$

zu schreiben. Seien $\rho_1, \ldots, \rho_{2g}$ die Nullstellen und

$$\beta_i = p^{\rho_i}$$

die ihnen entsprechenden z–Werte, also

$$p^{2gs}\frac{\zeta_{\mathsf{K}}(s)}{\zeta(s)} = P(z) = (z-\beta_1)\cdots(z-\beta_{2g}).$$

Dann liegen also die β_i alle im Kreisring

$$1 < |\beta_i| < p.$$

Das **Analogon der Riemannschen Vermutung** besagt:

$$|\beta_i| = p^{\frac{1}{2}} = \sqrt{p}$$

NB. Die Residuen bei $s = 0$ und $s = 1$ liefern dann übrigens folgende Klassenzahlformeln:

$$h = (1-\beta_1)\cdots(1-\beta_{2g}) = P(1)$$
$$h = p^{-g}(p-\beta_1)\cdots(p-\beta_{2g}) = p^{-g}P(p)$$

die durch die Funktionalgleichung zusammenhängen:

$$z^{-g}P(z) = \left(\tfrac{p}{z}\right)^{-g} P\left(\tfrac{p}{z}\right).$$

Eine erste Annäherung daran kann man durch direkte Berechnung des Koeffizienten

$$\sigma_1 = N_1 - (p+1) = -(\beta_1 + \cdots + \beta_{2g})$$

erhalten. Um an die β_i selbst heranzukommen, ist es aber unbequem, auch die weiteren *Koeffizienten* von $P(z)$ durch die Anzahlen der Divisoren höherer Grade auszudrücken. Man kann vielmehr eleganter und wirksamer stattdessen mit den höheren *Potenzsummen* der Wurzeln β_i operieren, die einer Deutung in unserer analytischen Theorie fähig sind. Es gilt nämlich:

V.) *Entsteht* K_r *aus* K *durch (die!) Erweiterung* r*–ten Grades des Koeffizientenkörpers* P_p *zu* P_{p^r}*, so ist*

$$\zeta_{\mathsf{K}_r}(s) = \prod_{\rho=0}^{r-1} \zeta_{\mathsf{K}}\left(s - \frac{2\pi i}{\log p} \cdot \frac{\rho}{r}\right)$$
$$\zeta_r(s) = \prod_{\rho=0}^{r-1} \zeta\left(s - \frac{2\pi i}{\log p} \cdot \frac{\rho}{r}\right)$$

also

$$p^{2grs}\frac{\zeta_{\mathsf{K}_r}(s)}{\zeta_r(s)} = P_r(z^r) = \prod_{\rho=0}^{r-1}\left(z - e^{\frac{2\pi i\rho}{r}}\beta_1\right)\cdots\left(z - e^{\frac{2\pi i\rho}{r}}\beta_{2g}\right)$$
$$= (z^r - \beta_1^r)\cdots(z^r - \beta_{2g}^r),$$

NB. Es tritt $z^r = p^{rs}$ an Stelle von z.
und somit

$$\sigma_1^{(r)} = N_1^{(r)} - (p^r + 1) = -(\beta_1^r + \cdots + \beta_{2g}^r).$$

Das folgt einfach aus der Produktentwicklung

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{\mathfrak{N}\mathfrak{P}^s}}, \qquad \zeta(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}\mathfrak{p}^s}}$$

und dem leicht herleitbaren Zerlegungsgesetz bei Übergang von K zu K_r bzw. $\mathsf{P}_p(x)$ zu $\mathsf{P}_{p^r}(x)$ (Kreiskörper der (p^r-1)–ten E. W.!):

$$\mathfrak{P} = \mathfrak{P}_1^{(r)}\cdots\mathfrak{P}_j^{(r)}, \quad N\mathfrak{P}_i^{(r)} = \mathfrak{P}^k; \qquad \mathfrak{p} = \mathfrak{p}_1^{(r)}\cdots\mathfrak{p}_{j_0}^{(r)}, \quad N\mathfrak{p}_i^{(r)} = \mathfrak{p}^{k_0},$$
$$jk = r,\ j_0k_0 = r$$

wenn k, k_0 die frühesten Exponenten sind, für die

$$\mathfrak{N}\mathfrak{P}^k \equiv 1 \mod p^r - 1, \quad \mathfrak{N}\mathfrak{p}^{k_0} \equiv 1 \mod p^r - 1,$$

d. h. wenn

$$\mathfrak{N}\mathfrak{P} = p^n, \qquad \mathfrak{N}\mathfrak{p} = p^{n_0}$$

ist, für die

$$kn \equiv 0 \mod r, \qquad k_0n_0 \equiv 0 \mod r$$

ist. Es ist formal genau dasselbe, wie die Aufspaltung der gewöhnlichen Dedekindschen ζ–Funktion des Klassenkörpers in die L–Reihen der Charaktere der zugeordneten Klasseneinteilung des Grundkörpers. Hier sind eben $\mathsf{K}_r, \mathsf{P}_{p^r}(x)$ Klassenkörper zu den Gruppen

$$\mathfrak{M}\mathfrak{A} \equiv 1 \mod p^r - 1, \qquad \mathfrak{N}\mathfrak{a} \equiv 1 \mod p^r - 1$$

in $\mathsf{K}, \mathsf{P}_p(x)$. —

6.) Zur vollen Beherrschung der β_i genügt es daher, die Anzahlen $N_1^{(r)}$ in den K_r zu studieren. Diese hängen nun mit den Lösungsanzahlen $N^{(r)}$ einer K definierenden Gleichung

$$F(x, y) = 0$$

in den endlichen Koeffizientenkörpern P_{p^r} zusammen.

NB. $F(x, y)$ ist so normiert angenommen, daß es Polynom in $\mathsf{P}_p[x]$ mit höchstem Koeffizienten 1 in y ist.

In der Tat entspricht jedenfalls jedem $\mathfrak{P}$ vom Grad 1 in K, von den $\mathfrak{P}/\mathfrak{p}_\infty = \frac{1}{x}$ abgesehen, eine Lösung a, b von $F(x, y)$ in P_p. Denn mod $\mathfrak{P}$ sind alle Restklassen in P_p vertretbar und

$$F(a, b) \equiv 0 \mod \mathfrak{P} \longleftrightarrow F(a, b) = 0.$$

Umgekehrt entspricht jeder Lösung a, b mindestens ein $\mathfrak{P}$ vom Grade 1, nämlich $\mathfrak{P} \mid \mathfrak{p} = x - a$. Es kann allerdings sein, daß einer u. derselben Lösung a, b mehrere $\mathfrak{P}$ entsprechen (die sich erst durch Betrachtung der Grundgleichung $F(x, y) = 0$ nach höheren Potenzen von $\mathfrak{p} = x - a$ als Modul voneinander trennen). Dies tritt aber, wie in der algebraischen Zahlentheorie, nur für außerwesentliche Diskriminantenteiler $\mathfrak{p}$ ein, d. h. für solche Teiler der Diskriminante $D(x)$ von $F(x, y)$ in bezug auf y, die in der Diskriminante $\mathfrak{d}_x = N(\mathfrak{D}_x)$ von $\mathfrak{I}_x$ nicht ebensohoch aufgehen. Da sie dann im Quadrat in $D(x)$ aufgehen, muß für sie $D(x)$ die Doppelwurzel a haben.

Hat also $D(x)$ keine Doppelwurzel in P_p, so ist die Anzahl der *endlichen* $\mathfrak{P}$ vom Grade 1 genau gleich der Lösungszahl N, und ganz entsprechend auch für die $\mathfrak{P}^{(r)}$ und $N^{(r)}$, wenn $D(x)$ *überhaupt* keine Doppelwurzel hat. Allgemein zeigt F. K. Schmidt, daß die Differenz zwischen beiden Anzahlen $\leqq \frac{\overline{d}_x n_x}{2}$ ist, wenn $\overline{d}_x$ den Grad von $D(x)$ in x angibt;

N. B. $\overline{d}_x$ ist $\geqq d_x$, wo d_x die obige Bedeutung (S. 8▶) hat.

denn den höchstens $\frac{\overline{d}_x}{2}$ Doppelwurzeln können immer höchstens n_x Lösungen und Primteiler $\mathfrak{P}$ entsprechen. Berücksichtigt man noch die höchstens n_x unendlichen $\mathfrak{P}/\mathfrak{p}_\infty = \frac{1}{x}$ vom Grad 1, so folgt also stets:

$$|N_1^{(r)} - N^{(r)}| \leqq \left(\frac{\overline{d}_x}{2} + 1\right) n_x.$$

Wesentlich ist, daß die rechte Seite von r und auch von den Koeffizienten von F unabhängig ist, sondern nur von den durch F definierten Gradzahlen $\overline{d}_x$ und n_x abhängt. In *diesem* Sinne sei im folgenden stets das auf $r \to \infty$ bezügliche Landausche $\mathfrak{O}(\cdots)$ verstanden, also hier:

$$N_1^{(r)} = N^{(r)} + \mathfrak{O}(1).$$

Wir wollen jetzt annehmen, es sei

(A) $$N^{(r)} - p = \mathfrak{O}(p^{\vartheta r})$$

mit einem ϑ im Intervall $\frac{1}{2} \leqq \vartheta < 1$ bewiesen, das *nicht* von r abhängt. Dann folgt nach dem Prinzip des Graeffeschen Näherungsverfahrens, weil ja dann auch

$$N_1^{(r)} - (p+1) = -(\beta_1^{(r)} + \cdots + \beta_{2g}^{(r)}) = \mathfrak{O}(p^{\vartheta r})$$

ist, daß jedes

$$|\beta_i| \leqq p^{\vartheta}$$

ist. (Hier wird wesentlich die Gleichmäßigkeit der $\mathfrak{O}$ in r benutzt.) Das ist dann also ein Resultat in Richtung der Riemannschen Vermutung für die Funktion $\zeta_{\mathsf{K}}(s)$, und für $\vartheta = \frac{1}{2}$ sie selbst. Überdies folgt automatisch die genauere Abschätzung

$$|N_1^{(r)} - (p+1)| \leqq 2gp^{\vartheta r},$$

und daraus

$$|N^{(r)} - p| \leqq 2gp^{\vartheta r} + 1 + \left(\frac{\overline{d}_x}{2} + 1\right) n_x,$$

statt der zunächst nur angenommenen rohen Abschätzungen.

Alles kommt also auf die Herleitung einer Abschätzung vom Typus (A) an.

7.) Ich beschäftige mich jetzt mit dem *hyperelliptischen Spezialfall*, wo also K durch eine Gleichung

$$F(x,y) = y^2 - F(x) = 0 \qquad \big(F(x) \text{ Polynom über } \mathsf{P}_p\big)$$

definiert ist:

$$\mathsf{K} = \mathsf{P}_p\big(x, \sqrt{F(x)}\,\big).$$

NB. Ist $F(x)$ nicht konstant, so ist dabei in der Tat auch P_p der größte in K enthaltene absolut–abelsche Körper.

In diesem Fall haben die englischen Mathematiker *Mordell* und *Davenport* neuerdings Abschätzungen vom Typus (A) hergeleitet, allerdings nur für den Fall, daß p Primzahl ist, wo es sich dann also um die Lösungsanzahl einer Kongruenz des obigen Typus mit ganz–rationalen Zahlkoeffizienten nach einem Primzahlmodul p handelt. Der allgemeine Fall (p Primzahlpotenz), der in dieser Sprechweise der Kongruenzlösungsanzahl nach einem Primidealmodul eines algebraischen Zahlkörpers entspricht, läßt sich aber, wie ich zeigen konnte, mit denselben Methoden durch Hinzufügung einer einzigen neuen Idee behandeln. Das will ich nachstehend auseinandersetzen.

Wir setzen zunächst $p \neq 2$ voraus. Für $p = 2$ ist nämlich K von 2. Art über $\mathsf{P}_p(x)$, also — Irreduzibilität — von 1. Art über $\mathsf{P}_p(y)$, und wegen $\mathsf{P}_p(y) \cong \mathsf{P}_p(y^2)$ ist $g = 0$. Das interessiert also nicht.

Wir setzen ferner voraus, daß $F(x)$ keine Doppelwurzel hat (weder in P_p noch in irgendeinem P_{p^k}). Denn sonst reduziert sich die Aufgabe über einem geeigneten P_{p^k} auf eine Gleichung $y^2 - \Phi(x) = 0$ mit Φ von niedrigerem Grade als F, und für unsere Aufgabe kommt es doch nur auf die Behandlung in einer Serie „aufsteigender“ P_{p^r} an, gleichgültig, ob man bei P_p selbst oder bei einem P_{p^k} anfängt.

Unter diesen Voraussetzungen ist für den Körper K:

$$n_x = 2, \quad d_x = 2n, \quad \text{wenn } F \text{ vom Grade } 2n-1 \text{ oder } 2n \text{ ist,}$$

also

$$g = \frac{d_x}{2} - n_x + 1 = n - 1$$

Daher können wir auch noch den Fall $n = 1$ eines linearen oder quadratischen F ausschließen, der ja wieder auf $g = 0$ führt.

Die Lösungsanzahl $N = N(F)$ von $F(x) = y^2$ in P_p läßt sich nun mittels des quadratischen Charakters χ von P_p folgendermaßen ausdrücken:

$$N(F) = \sum_x \big(1 + \chi\big(F(x)\big)\big) = p + \sum_x \chi\big(F(x)\big),$$

wo x den Körper P_p durchläuft; denn $1+\chi(b)$ ist die Lösungszahl von $y^2=b$ in P_p.

Nun gilt für den Charakter χ die folgende Darstellung: Es sei

$$e(u)=e^{\frac{2\pi i \operatorname{Sp} u}{p}}, \quad \text{wo } \operatorname{Sp} u = u+u^{p_0}+\cdots+u^{p_0^{r_0-1}} \text{ die Spur in } \mathsf{P}_p \text{ ist } (p=p_0^{r_0}).$$

Dann ist

$$\sum_t \chi(t)e(tb)=\chi(b)\sum_t \chi(t)e(t),$$

da tb für $b\neq 0$ mit t den Körper P_p durchläuft, während für $b=0$ beide Seiten 0 sind. Hier ist bekanntlich

$$\sum_t \chi(t)e(t)=G(\chi)=\pm\sqrt{\chi(-1)p} \quad \text{(Gaußsche Summe; auf das Vorzeichen kommt es hier nicht an).}$$

Daraus folgt die angekündigte Darstellung:

$$\chi(b)=\frac{1}{G(\chi)}\sum_t \chi(t)e(tb)=\frac{\pm\sqrt{\chi(-1)}}{\sqrt{p}}\sum_t \chi(t)e(tb).$$

Damit erhält man für die zu bestimmende Anzahlfunktion:

$$N(F)-p=\frac{\pm\sqrt{\chi(-1)}}{\sqrt{p}}\sum_{x,t}\chi(t)e\big(tF(x)\big).$$

Das erheben wir in die $2n+2$ –te Potenz:

$$\big(N(F)-p\big)^{2n+2}=\frac{\chi(-1)^{n+1}}{p^{n+1}}\sum_{x_\nu,t_\nu}\chi(t_1\cdots t_{2n+2})e\big(t_1F(x_1)+\cdots \\ \cdots+t_{2n+2}F(x_{2n+2})\big),$$

und summieren dann über *alle* p^{2n+1} Polynome F in P_p, deren Grad $\leqq 2n$ ist (ohne Rücksicht auf die oben geforderten Einschränkungen für F — die uns interessierenden F kommen ja dabei sicher alle vor!). Rechts ziehen wir die Summation über die Koeffizienten c_ν von

$$F(x)=c_0+c_1x+\cdots+c_{2n}x^{2n}$$

nach innen. Dann entsteht:

$$\begin{aligned}\sum_F \big(N(F)-p\big)^{2n+2} &= \frac{\chi(-1)^{n+1}}{p^{n+1}} \sum_{x_\nu,t_\nu} \chi(t_1,\dots,t_{2n+2}) \sum_{c_\nu} e(c_0S_0+\cdots \\ &\qquad \cdots + c_{2n}S_{2n}) \\ &= \frac{\chi(-1)^{n+1}}{p^{n+1}} \sum_{x_\nu,t_\nu} \chi(t_1,\dots,t_{2n+2}) \sum_{c_0} e(c_0S_0)\cdots \\ &\qquad \cdots \sum_{c_{2n}} e(c_{2n}S_{2n}),\end{aligned}$$

wo zur Abkürzung gesetzt ist:

$$\begin{aligned} S_0 &= t_1+\cdots+t_{2n+2} \\ S_1 &= t_1x_1+\cdots+t_{2n+2}x_{2n+2} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ S_{2n} &= t_1x_1^{2n}+\cdots+t_{2n+2}x_{2n+2}^{2n}.\end{aligned}$$

Nun gilt

$$\sum_c e(cu) = \begin{cases} p & \text{für} \quad u=0 \\ 0 & \text{für} \quad u\neq 0 \end{cases}$$

Ersteres ist klar. Um letzteres einzusehen, stelle man c durch eine Basis $w_1,\dots,w_{r_0}$ von P_p dar:

$$c=\gamma_1w_1+\cdots+\gamma_{r_0}w_{r_0}, \quad \gamma_i \quad \text{in} \quad \mathsf{P}_{p_0}.$$

Dann wird

$$\sum_c e(cu) = \sum_{\gamma_1} e(\gamma_1w_1u)\cdots\sum_{\gamma_{r_0}} e(\gamma_{r_0}w_{r_0}u).$$

Hier ist nun

$$\sum_\gamma e(\gamma wu) = \sum_\gamma e^{\frac{2\pi i\gamma \mathrm{Sp}(wu)}{p}} = \begin{cases} p & \text{für} \quad \mathrm{Sp}(wu)=0 \\ 0 & \text{||} \quad \mathrm{Sp}(wu)\neq 0. \end{cases}$$

Wäre nun durchweg

$$\mathrm{Sp}(w_iu)=0 \qquad (i=1,\dots,r_0),$$

so folgte wegen

$$|w_i^{p_0^k}| \neq 0$$

notwendig

$$u = 0.$$

Somit ist für $u \neq 0$ mindestens eine $\mathrm{Sp}(w_i u) \neq 0$, d. h. die entsprechende $\sum_{\gamma_i} e(\gamma_i w_i u) = 0$, und daher auch $\sum_c e(cu) = 0$.

Für unsere Anzahlfunktion folgt daraus:

$$\sum_F \big(N(F) - p\big)^{2n+2} = \frac{\chi(-1)^{n+1}}{p^{n+1}} \cdot p^{2n+1} \cdot \sum_{\substack{x_\nu, t_\nu \\ \text{erfüllen} \\ \text{(G)}}} \chi(t_1 \cdots t_{2n+2}),$$

wo über die Lösungen x_ν, t_ν des Gleichungssystems

$$\text{(G)} \qquad \begin{cases} t_1 + \cdots + t_{2n+2} &= 0 \\ t_1 x_1 + \cdots + t_{2n+2} x_{2n+2} &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ t_1 x_1^{2n} + \cdots + t_{2n+2} x_{2n+2}^{2n} &= 0 \end{cases}$$

zu summieren ist. Es genügt, über diejenigen Lösungen zu summieren, für die alle $t_\nu \neq 0$ sind, wegen $\chi(0) = 0$.

(G) ist bei festen x_ν linear homogen in den t_ν und enthält $2n+1$ Gleichungen für $2n+2$ Unbekannte. Werden nun die x_ν zunächst *alle untereinander verschieden* vorgeschrieben, so ist der Rang gleich $2n+1$, also die t_ν bis auf einen Proportionalitätsfaktor *eindeutig* bestimmt, und zwar

$$t_1 : t_2 : \cdots : t_{2n+2} = \Delta_1 : -\Delta_2 : \cdots\cdots : -\Delta_{2n+2},$$

wo $\Delta_1, \ldots, \Delta_{2n+2}$ die $2n+1$ –reihigen Unterdeterminanten der Matrix

$$\begin{pmatrix} 1 & \cdots\cdots\cdots & 1 \\ x_1 & \cdots\cdots\cdots & x_{2n+2} \\ \cdots\cdots\cdots\cdots\cdots\cdots & & \\ x_1^{2n-1} & \cdots\cdots\cdots & x_{2n+2}^{2n-1} \\ x_1^{2n} & \cdots\cdots\cdots & x_{2n+2}^{2n} \end{pmatrix}$$

sind (Δ_ν entsteht durch Streichung der ν–ten Spalte), also

$$\Delta_\nu = \prod_{\substack{i>k \\ i,k \neq \nu}} (x_i - x_k).$$

Da bei der gemachten Voraussetzung *alle* $\Delta_\nu \neq 0$ sind, sind für die Lösung auch wirklich alle $t_\nu \neq 0$, wenn nur der Proportionalitätsfaktor nicht 0 ist, und es ist (weil $2n+2$ gerade ist)

$$\chi(t_1 \cdots t_{2n+2}) = \chi(-1)^{n+1}\chi(\Delta_1 \cdots \Delta_{2n+2}).$$

In $\Delta_1 \cdots \Delta_{2n+2}$ kommt aber jede feste Differenz $x_i - x_k$ $(i > k)$ genau $2n$–mal vor (nämlich für alle ν außer i und k). Daher ist $\Delta_1 \cdots \Delta_{2n+2}$ ein Quadrat, und somit $\chi(\Delta_1 \cdots \Delta_{2n+2}) = 1$, also

$$\chi(t_1 \cdots t_{2n+2}) = \chi(-1)^{n+1}.$$

Da es $p(p-1)\cdots\big(p-(2n+1)\big)$ Systeme durchweg verschiedener x_ν gibt und jedem $p-1$ Lösungen $t_\nu \neq 0$ entsprechen, ergibt sich hiernach:

$$\begin{aligned}\sum_F \big(N(F)-p\big)^{2n+2} &= p^n \cdot p(p-1)\cdots\big(p-(2n+1)\big)\cdot(p-1)+ \\ &\quad + \chi(-1)^{n+1}p^n \sum_{(\mathrm{G})}{}' \chi(t_1 \cdots t_{2n+2}) \\ &= p^{3n+3} + \mathfrak{O}(p^{3n+2}) + \chi(-1)^{n+1}p^n \sum_{(\mathrm{G})}{}' \chi(t_1 \cdots t_{2n+2}),\end{aligned}$$

wo die Restsumme nur noch über die Lösungen mit nicht durchweg verschiedenen x_ν zu erstrecken ist. $\mathfrak{O}$ bezieht sich auf $p \to \infty$, was im Sinne unserer Anwendung liegt — Ersetzung von p durch p^r mit $r \to \infty$.

Es seien jetzt unter den x_ν genau $s < 2n+2$ verschiedene, die in Gruppen von je $\nu_1, \ldots, \nu_s$ gleichen auftreten. Faßt man die Glieder dieser Gruppen in (G) zusammen, so entsteht ein System linearer homogener Gleichungen in der Anzahl $2n+1$ für $s \leqq 2n+1$ Unbekannte, nämlich die den Gruppen entsprechenden Summen aus den t_ν. Hierbei haben die ersten s Gleichungen eine von 0 verschiedene Determinante, legen also jene t_ν–Summen zu 0 fest, und die übrigen Gleichungen bestehen dann von selbst.

NB. Das wird nicht gebraucht! ⟵ [Ist also auch nur ein $\nu_i = 1$, so wird das entsprechende $t_{\nu_i} = 0$, und die Lösung fällt für uns aus.]

Allgemein gibt es $p(p-1)\cdots\big(p-(s-1)\big)$ Möglichkeiten für die Werte der s verschiedenen x_ν, und wenn man noch die Verteilung auf die $2n+2$ Plätze berücksichtigt, jedenfalls nur $\mathfrak{O}(p^s)$ Systeme der betrachteten Art. Jedem solchen System entsprechen genau $p^{(\nu_1-1)+\cdots+(\nu_s-1)} = p^{2n+2-s}$ Systeme t_ν (ohne

Rücksicht auf $t_\nu \neq 0$). Schätzt man also für alle diese Lösungen $\chi(t_1 \cdots t_{2n+2})$ noch durch 1 ab, so wird jedenfalls

$$\sum_{(G)}{}' \chi(t_1 \cdots t_{2n}) = \mathfrak{O}(p^{2n+2}),$$

und damit endlich:

$$\sum_F \big(N(F) - p\big)^{2n+2} = p^{3n+3} + \mathfrak{O}(p^{3n+2}).$$

Wir haben uns nunmehr mit der linken Seite zu befassen und dort das Äquivalent des „Hauptgliedes“ p^{3n+3} rechts zu suchen. Dies Äquivalent wird von denjenigen F geliefert, für die eine Zerfällung der Form

$$F = cF_0^2$$

in P_p besteht. Den Fall $F = 0$ können wir außer Acht lassen, da ersichtlich $N(0) = p$ ist. Ist nun $F = cF_0^2$ mit $c \neq 0, F_0 \neq 0$, so bestimmt sich die Anzahl $N(F)$ so:

a.) $\chi(c) = +1$, also $c = c_0^2$ in P_p. Dann reduziert sich die Forderung $F(x) = y^2$ auf eine der beiden Forderungen:

$$c_0 F_0(x) = y, \qquad c_0 F_0(x) = -y.$$

Jede einzelne dieser Forderungen hat genau p Lösungen. Bei der Zusammenfügung sind genau diejenigen n_0 Lösungen nur einmal zu zählen, für die $y = 0$ also $F_0(x) = 0$ ist; das sind höchstens n. Also:

$$N(F) = 2p - n_0, \qquad N(F) - p = p - n_0, \quad \text{wo} \quad 0 \leqq n_0 \leqq n$$

b.) $\chi(c) = -1$. Dann muß notwendig $F_0(x) = 0, y = 0$ sein, was genau n_0 Lösungen ergibt:

$$N(F) = n_0, \qquad N(F) - p = n_0 - p.$$

Für die betrachteten $F = c_0 F_0^2 \neq 0$ wird also

$$|N(F) - p| = p + \mathfrak{O}(1).$$

Solche F gibt es nun genau $p^{n+1} - 1$. Denn $F_0 \neq 0$ gibt es $p^{n+1} - 1$, $c \neq 0$ gibt es $p - 1$, und $cF_0^2 = c' F_0'^2$ ist dann und nur dann der Fall, wenn $F_0' =$

kF_0 mit $k \neq 0$ (und dann $c' = \frac{c}{k^2}$) ist, was je $p-1$ Darstellungen von F zusammenfallen läßt.

Somit ist

$$\sum_{F=cF_0^2} \big(N(F)-p\big)^{2n+2} = (p^{n+1}-1)\big(p^{2n+2}+\mathfrak{O}(p^{2n+1})\big)$$
$$= p^{3n+3}+\mathfrak{O}(p^{3n+2}).$$

In der Tat liefern also diese F das Hauptglied p^{3n+3}. Läßt man sie aus, so folgt also

$$\sum_{F\neq cF_0^2} \big(N(F)-p\big)^{2n+2} = \mathfrak{O}(p^{3n+2}).$$

Wir betrachten nunmehr die linear gebrochenen Substitutionen

$$x' = \frac{ax+b}{cx+d}, \qquad ad-bc \neq 0.$$

Setzt man

$$y' = \frac{y}{(cx+d)^n},$$

so geht $y'^2 = F(x')$ dabei über in eine Gleichung [1]

$$y'^2 = F'(x),$$

wo auch

$$F'(x) = (cx+d)^{2n} F\left(\frac{ax+b}{cx+d}\right)$$

wieder ein Polynom vom Grade $\leqq 2n$ ist. Da diese Substitutionen umkehrbar eindeutig sind, ist dabei $N(F') = N(F)+\mathfrak{O}(1)$ (letzteres wegen des Unendlichen!). Ferner ist die Beschränkung auf $F \neq cF_0^2$ bei diesen Substitutionen invariant, und auch die gleich einzuführende Doppelwurzelfreiheit und die Eigenschaft, genau vom Grade $2n-1$ oder $2n$ zu sein, sind invariant.

Gehen wir von einem doppelwurzelfreien F vom Grade $2n-1$ oder $2n$ aus, und führt eine Substitution der betrachteten Art F in sich über, so sind ihre Koeffizienten a, b, c, d durch die Übergänge (man beachte $2n-1 \geqq 3$ wegen $n > 1$!) dreier solcher Wurzeln in irgendeins der $\binom{2n}{3}$ Systeme von

1. vielleicht auch $y^2 = F'(x)$

drei Wurzeln von F bis auf einen Proportionalitätsfaktor k festgelegt, und dieser Faktor (der sich F' als k^{2n} mitteilt) ist selbst höchstens $2n$–deutig festgelegt. Solcher Substitutionen gibt es also höchstens $2n \cdot \binom{2n}{3} = \mathfrak{O}(1)$. Es gibt also auch nur $\mathfrak{O}(1)$ Substitutionen, die F in dasselbe F' überführen.

Wir gehen jetzt von einem festen doppelwurzelfreien F vom Grade $2n-1$ oder $2n$ aus — wie zu Beginn — und haben dann jedenfalls nach obigem

$$\sum_{F' \sim F}{}' \big(N(F') - p\big)^{2n+2} = \mathfrak{O}(p^{3n+2}),$$

wo über alle zu F in der genannten Weise äquivalenten, untereinander verschiedenen F' zu summieren ist. Läßt man die Bedingung der Verschiedenheit der F' fallen, so ist also jedes F' jetzt $\mathfrak{O}(1)$–mal statt 1–mal als Summand zu setzen, was nichts ausmacht:

$$\sum_{F' \sim F} \big(N(F') - p\big)^{2n+2} = \mathfrak{O}(p^{3n+2}).$$

Links steht jetzt so oft ein Summand der Form $\big(N(F) + \mathfrak{O}(1) - p\big)^{2n+2}$, als es Substitutionen der betrachteten Art gibt, d. h. $p^4 + \mathfrak{O}(p^3)$ mal.

Daher folgt:

$$\begin{aligned} \big(p^4 + \mathfrak{O}(p^3)\big)\big(N(F) + \mathfrak{O}(1) - p\big)^{2n+2} &= \mathfrak{O}(p^{3n+2}), \\ \big(N(F) + \mathfrak{O}(1) - p\big)^{2n+2} &= \mathfrak{O}(p^{3n-2}) \\ N(F) + \mathfrak{O}(1) - p &= \mathfrak{O}\left(p^{\frac{3n-2}{2n+2}}\right). \end{aligned}$$

Leider gibt das nur für die beiden Anfangswerte $n = 2$ und $n = 3$ nicht–triviale Resultate, nämlich:

$$\begin{aligned} \boldsymbol{N(F) - p = \mathfrak{O}(p^{\frac{2}{3}})} \quad & \textbf{für} \quad \boldsymbol{n = 2} \\ \boldsymbol{N(F) - p = \mathfrak{O}(p^{\frac{7}{8}})} \quad & \textbf{für} \quad \boldsymbol{n = 3.} \end{aligned}$$

Das sind die beiden Resultate von *Mordell* (in Verallgemeinerung auf beliebige P_p).

Davenport hat durch feinere Methoden auch für beliebiges n ein Resultat dieser Art erhalten, das allerdings nicht so scharf ist. Auch dieses verallgemeinert sich in gleicher Weise auf beliebige P_p. Es lautet:

$$N(F) - p = \mathfrak{O}\left(p^{1 - \frac{1}{(2n+2)2^{n-3}}}\right).$$

Allerdings ist der Davenportsche Beweis bisher nur bis $n = 5$ komplett. Im allgemeinen Fall ist noch eine algebraische Eliminationsschwierigkeit zu überwinden, was aber wohl in endlicher Zeit geschehen wird.

Für die Nullstellen der (in diesem Falle Artinschen) ζ–Funktionen folgt also:

Im hyperelliptischen Fall $y^2 = F(x)$ *mit doppelwurzelfreiem* $F(x)$ *vom Grade* $2n-1$ *oder* $2n$ *liegen alle Nullstellen von* $\zeta_{\mathsf{K}}(s)$ *im Streifen* $\frac{1}{3} \leqq \sigma \leqq \frac{2}{3}$ $(n = 2)$, $\frac{1}{8} \leqq \sigma \leqq \frac{7}{8}$ $(n = 3)$, $\frac{1}{(2n+2)2^{n-3}} \leqq \sigma \leqq 1 - \frac{1}{(2n+2)2^{n-3}}$ *(allgemein)*

Schließlich möchte ich noch anführen, das die englischen Mathematiker auch Gleichungen der Art

$$y^m = F_n(x), \quad F_n(x) \text{ vom Grade } n$$

in entsprechender Weise für spezielle Werte von m und n behandelt haben. Hier ist das am meisten hervorstechende Resultat (*Mordell*):

$$N\big(y^3 = F_3(x)\big) - p = \mathcal{O}(p^{\frac{1}{2}}).$$

Auch dies überträgt sich wieder auf beliebige P_p in analoger Weise. *Für diesen Fall ist damit also die Riemannsche Vermutung bestätigt.* Es ist der einzige bisher bekannte Fall, in dem man solch ein scharfes Resultat hat, von den Artinschen rechnerisch hergeleiteten Bestätigungen für kleine Primzahlen p abgesehen.

Übrigens konnte *Davenport* hier sogar die Lösungszahl bis auf ein Glied $\mathcal{O}(1)$ genau ausdrücken, als Funktion der Koordinaten a, b in $p = a^2 + ab + b^2$ (der Fall $p \equiv -1 \mod 3$ ist natürlich trivial).

1.14 Marburg 1933 II

Riemannsche Vermutung für Kongruenzzetafunktionen im elliptischen Fall.

Vortrag Marburg, Mai 1933.

1. Rekapitulation aus Februarvortrag.▸

E_q endlicher Körper ($q = p^f$). K algebraischer Funktionenkörper über E_q, erzeugt durch $F(x, y) = 0$ oder beliebige birationale Transformierte. E_q als größter in K enthaltener Konstantenkörper vorausgesetzt.

Zwei wichtige Invarianten: Geschlecht g ($\geqq 0$), Klassenanzahl h (der Divisoren jedes festen Grades).

F. K. Schmidtsche ζ–Funktion von K:

$$\zeta_K(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P})^s}} = \sum_{\mathfrak{A}} \frac{1}{\mathfrak{N}(\mathfrak{A})^s}.$$

Wird trivial für $g = 0$:

$$\zeta(s) = \frac{1}{1 - \frac{1}{q^s}} \cdot \frac{1}{1 - \frac{q}{q^s}}.$$

Eigenschaften:

I. Periodisch mit $\frac{2\pi i}{\log q}$. Regulär bis auf Pole 1. Ordnung bei $0, 1$ und homologen Stellen mit Residuen

$$-\frac{h}{q-1}\,\frac{1}{\log q}, \qquad \frac{1}{q^g - 1}\,\frac{h}{q-1}\,\frac{1}{\log q}.$$

II. Funktionalgleichung:

$$q^{(g-1)s}\zeta_K(s) \quad \text{bei} \quad s \to 1 - s \quad \text{invariant.}$$

III. $\zeta_K(s) \neq 0$ für $\Re(s) = 1$. Nullstellen also allein in $0 < \Re(s) < 1$.

IV. Wesentlich Polynom $2g$–ten Grades in $z = q^s$:

$$z^{2g}\frac{\zeta_K(s)}{\zeta(s)} = \mathsf{P}(z) = z^{2g} + \sigma_1 z^{2g-1} + \cdots + \sigma_{2g}$$

$\sigma_1 = N_1 - (q+1)$, N_1 Anzahl der ganzen (Prim–)Divisoren 1. Grades in K. Ungefähr Anzahl der Lösungen von $F(x,y) = 0$ in E_q; aber im Gegensatz dazu birational invariant.

Also wirklich genau $2g$ Nullstellen ρ_i

$$\mathsf{P}(z) = \prod_{i=1}^{2g}(z - \beta_i), \qquad \beta_i = q^{\rho_i}.$$

Analogon der Riemannschen Vermutung:

$$|\beta_i| = q^{\frac{1}{2}}.$$

V. Bei Übergang zu $K^{(1)}$ über E_{q^r} entsprechendes Polynom:

$$z^{2g}\frac{\zeta_K^{(r)}(s)}{\zeta^{(r)}(s)} = \mathsf{P}^{(r)}(z) = \prod_{i=1}^{2g}(z - \beta_i^r), \qquad z = q^{rs}.$$

Es genügt also, Riemannsche Vermutung für geeignete Erweiterung $K^{(r)}$ zu bestätigen.

Elliptischer Spezialfall, $g = 1$. $\zeta_K(s)$ allein durch h bestimmt:

$$\zeta_K(s) = \frac{q+h-1}{q-1} + \frac{h}{q-1}\left(\frac{q^s}{1-q^s} + \frac{q^{1-s}}{1-q^{1-s}}\right).$$

$$z^2\frac{\zeta_K(s)}{\zeta(s)} = \mathsf{P}(z) = z^2 + \sigma_1 z + \sigma_2 = (z-\beta)(z-\overline{\beta}).$$

$\sigma_1 = N_1 - (q+1) = h - (q+1)$ (also $N_1 = h$)

$\sigma_2 = q$.

$\beta, \overline{\beta}$ entweder konjugiert–komplex (dann stimmt Riemannsche Vermutung)
oder reell verschieden (dann nicht).

Nachweis der Riemannschen Vermutung läuft auf

$$|N_1 - (q+1)| \leqq 2q^{\frac{1}{2}}$$

hinaus, also auf Abschätzung des Faktors der Anzahl N_1 gegenüber ihrem Mittelwert $q+1$.

Durch Anwendung des Übergangs zu $K^{(r)}$ genügt es allgemein, $N_1^{(r)} - (q^r + 1) = \mathfrak{O}(q^{\frac{n}{2}})$ für $r \to \infty$ zu beweisen. Ist $\mathfrak{O}\left(q^{r(\frac{1}{2}+\vartheta)}\right)$ für ein ϑ bekannt, so folgt, daß die Nullstellen $\Re(\rho) \leqq \frac{1}{2}+\vartheta$ haben. Durch Übertragung elementar–analytischer Abschätzungen von Mordell und Davenport von E_p auf E_{q^r} so Teilreduktion erreichbar für hyperelliptische Fälle.

2. Darstellung des elliptischen Körpers K in Weierstrassscher Normalform.

Für $p \neq 2, 3$ ist K in der Form erzeugbar

$$y^2 = 4x^3 - c_2 x - c_3, \quad \text{mit} \quad \partial = c_2^3 - 27c_3^2 \neq 0.$$

Im folgenden Spezialfälle $c_2 = 0$ oder $c_3 = 0$ beiseite gelassen. Analoger Behandlung fähig, aber mit unliebsamen Modifikationen. Mühe dafür unnütz, da elementar völlig behandelbar (Davenport, Methoden von ihm und Mordell).

Charakteristische Invarianten von K:

$$k = \frac{(12c_2)^3}{\partial} \quad \text{und} \quad \chi_2(c_3).$$

Aus ihnen abgeleitete weitere wichtige Invarianten:

$$\widehat{k} = k - 12^3 = \frac{(216c_3)^2}{\partial} \quad \text{und} \quad \chi_4(c_2), \chi_6(c_3), \chi_{12}(\partial).$$

Wegen $c_2 \neq 0, c_3 \neq 0$ dabei hier immer $k, \widehat{k} \neq 0$.

Normalform, die allein Invarianten enthält, nur irrational möglich:

$$\xi = \frac{12c_2 \cdot 216c_3}{\partial} \cdot 12x, \qquad \eta = \frac{y}{\sqrt[4]{\partial}}$$

führt zu

$$2^4 3^3 k \sqrt{\widehat{k}}^3 \eta^2 = \xi^3 - 3k\widehat{k}\xi - 2k\widehat{k}^2.$$

Das erzeugt also $K^{(\delta)}$ über E_{q^δ}, wo δ die Ordnung von $\sqrt[4]{\partial}$ und $\sqrt{\widehat{k}}$ durch $\sqrt[4]{\partial}$ normiert.

Im folgenden wird $N_1^{(\delta)}$ für $K^{(\delta)}$ bestimmt:

$$N_1^{(\delta)} = N^{(\delta)} + 1,$$

wo $N^{(\delta)}$ die gewöhnliche Lösungszahl der Gleichung zwischen ξ, η in E_{q^δ}. Die zusätzliche 1 repräsentiert die eine unendliche Lösung.

3. Uniformisierung durch elliptische Funktionen.

Weierstrasssche Normalform:

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3, \qquad \Delta = g_2^3 - 27g_3^2 \neq 0.$$

Dabei $\wp = \wp(u, \mathfrak{w})$, $g_2 = g_2(\mathfrak{w})$, $g_3 = g_3(\mathfrak{w})$. Geht durch analoge Transformation

$$\tau = \frac{12g_2 \cdot 216g_3}{\Delta} \cdot 12\wp, \qquad \widehat{\tau} = \frac{\wp'}{\sqrt[4]{\Delta}}$$

über in

$$2^4 3^3 j \sqrt{\widehat{j}}^{\,3}\, \widehat{\tau}^2 = \tau^3 - 3j\,\widehat{j}\,\tau - 2j\,\widehat{j}^{\,2}.$$

Dabei

$$j = \frac{(12g_2)^3}{\Delta}, \qquad \widehat{j} = j - 12^3 = \frac{(216g_3)^2}{\Delta}.$$

$\tau, \widehat{\tau}, j, \widehat{j}$ Funktionen 0. Dimension.

„Singuläre“ Werte dieser Funktionen für

$\mathfrak{w} = \mathfrak{a}$ (Modul aus imaginär quadratischem Körper $\Omega = \mathsf{P}(\sqrt{d})$)
$u = \rho$ (Zahl aus Ω)

sind durchweg algebraisch und erzeugen abelsche Körper über Ω, die nach den Methoden der Klassenkörpertheorie durch Idealgruppen in Ω charakterisierbar.

Prinzip meiner Methode: Darstellung der Koeffizienten der gegebenen Gleichung, also wesentlich k, als Kongruenzwerte der entsprechenden Modulfunktionen für geeignetes singuläres Argument $\mathfrak{a}$ nach Primteiler $\mathfrak{P}$ von p. Erzeugung des ganzen E_{q^δ} durch Kongruenzwerte von $\tau(\rho, \mathfrak{a})$ für geeignete Argumente ρ als volles Restsystem nach Primteiler $\mathfrak{P}^*$ von $\mathfrak{P}$. Untersuchung,

ob die zugehörigen Kongruenzwerte von $\widehat{\tau}(\rho, \mathfrak{a})$ auch noch mod $\mathfrak{P}^*$ rational sind, durch Untersuchung des Zerlegungsgesetzes für $\mathfrak{P}^*$ bei weiterer Adjunktion von $\widehat{\tau}(\rho, \mathfrak{a})$. Kurz: Darstellung der Gleichung in E_{q^δ} durch Kongruenzbetrachtung einer Zahlen*gleichung*.

□□□

Fundamentales Uniformisierungstheorem.

k Element *ungeraden* Grades f_0 über E_p, also erzeugt E_{q_0} ($q_0 = p^{f_0}$) von ungeradem Grade. Es existiert imaginär–quadratischer Modul $\mathfrak{a}$ derart, daß p im Körper $\mathsf{K}_0 = \Omega\big(j(\mathfrak{a})\big)$ (Ω Körper von $\mathfrak{a}$) in Primideale $\mathfrak{P}_0$ vom Grade f_0 zerfällt — also der Restklassenkörper mod $\mathfrak{P}_0$ zu E_{q_0} isomorph ist, und bei einer isomorphen Abbildung

$$j(\mathfrak{a}) \equiv k \mod \mathfrak{P}_0, \quad \text{also auch} \quad \widehat{j}(\mathfrak{a}) \equiv \widehat{k} \mod \mathfrak{P}_0$$

gilt.

K_0 Ringklassenkörper mod m über Ω, wenn $\mathfrak{a}$ Moduldiskriminante $D = m^2 d$ hat, wo d Diskriminante von Ω ist; also Klassenkörper zur Gruppe aller Hauptideale (λ) aus Ω, mit $\lambda \equiv$ rat. zu m primer Zahl mod m. Nach Zerlegungsgesetz für K_0 gilt dabei

$$q_0 = p^{f_0} = \pi_0 \overline{\pi}_0 \quad \text{im Ring mod } m, \text{ mit} \quad (\pi_0) = \mathfrak{p}^{f_0},\ (\overline{\pi}_0) = \overline{\mathfrak{p}}^{f_0},$$

wo $\mathfrak{p}, \overline{\mathfrak{p}}$ die beiden gleichen oder verschiedenen Primteiler von p in Ω; insbesondere also $\left(\frac{d}{p}\right) = 0$ [1] oder 1 (für $\left(\frac{d}{-p}\right) = -1$ wird Grad der Primteiler gerade). Ferner wird m prim zu p. Dabei ist Ω, d. h. d, in jedem Falle eindeutig bestimmt, ebenso die Faktoren $\pi_0, \overline{\pi}_0$ bis aufs Vorzeichen, und im allgemeinen auch $\mathfrak{a}$, d. h. insbesondere D oder m; nur im Spezialfall $d = -p$ ($p \equiv -1 \mod 4$) kommen ev. zwei $\mathfrak{a}$ mit $D = -p$ und $D = -4p$ in Frage.

Wegen $k, \widehat{k} \neq 0$ wird noch $d \neq -4, -3$, d. h. die ausgearteten Fälle der elliptischen und Modulfunktionen und die Ω mit höheren Einheitswurzeln kommen bei dieser Voraussetzung nicht vor; sie entsprechen eben den ausgearteten Fällen $c_3 = 0$, $c_2 = 0$.

Natürlich besteht erst recht Zerlegung

$$q = p^f = \pi_1 \overline{\pi}_1 \quad \text{im Ring mod } m,$$

1. undeutlich

wenn k (nicht notw. primitives) Element aus E_q, und der Restklassenkörper mod $\mathfrak{P}_0$ ist als Teilkörper von E_q darstellbar.

Um Koeffizienten der Normalform zu erfassen, Übergang zu Ringklassenkörper $\mathsf{K} = \Omega\left(\sqrt{\widehat{j}(\mathfrak{a})}\right)$, mod m oder $2m$, je nachdem $2 \nmid D$ oder $2 \mid D$. Sei $\mathfrak{P}$ Primteiler von $\mathfrak{P}_0$ darin, so zeigt sich: Der Restklassenkörper mod $\mathfrak{P}$ ist als Teilkörper von E_{q^δ} darstellbar, es gilt

$$q^\delta = p^{f\delta} = \pi\overline{\pi} \quad \text{im Ring mod } zm \quad \big(z = (2, D)\big),$$

und

$$j(\mathfrak{a}) \equiv k, \quad \widehat{j}(\mathfrak{a}) \equiv \widehat{k}, \quad \sqrt{\widehat{j}(\mathfrak{a})} \equiv \sqrt{\widehat{k}} \mod \mathfrak{P},$$

bei richtiger Normierung der $\sqrt{\widehat{j}(\mathfrak{a})}$. Damit *Koeffizienten* der Normalform uniformisiert.

Uniformisierung leider bisher nur für ungeraden Grad der Invariante k durchführbar, also z. B. sicher, wenn E_q ungeraden Grad f hat, insbesondere für $E_q = E_p$.

4. Uniformisierung der Variablen. Geschieht durch die Funktionswerte

$$\tau\left(\frac{\alpha}{\pi - 1}, \mathfrak{a}\right) \quad \text{und} \quad \tau\left(\frac{\alpha}{\pi + 1}, \mathfrak{a}\right),$$

wo α die Zahlen aus $\mathfrak{a}$ durchläuft; und zwar lassen wir α so laufen, daß gerade jedesmal ein volles Periodenparallelogramm (ohne Nullpunkt) durchlaufen wird: $(\pi \mp 1)$–te Teilwerte. Durch Adjunktion zum Koeffizientenkörper K entsteht über Ω abelscher Körper K^*. Sei $\mathfrak{P}^*$ Primteiler von $\mathfrak{P}$ in K^*, und π unter $\pi, \overline{\pi}$ so gewählt, daß $\mathfrak{P}^*$ Primteiler von $\mathfrak{p}$ in Ω. Dann zeigt sich aus komplexer Multiplikation:

$\mathfrak{P}^*$ hat genau Grad $f\delta$, d. h. Restklassenkörper mod $\mathfrak{P}^*$ ist zu E_{q^δ} isomorph. Die obigen Teilwerte, von denen insgesamt immer genau zwei entgegengesetzte einander gleich sind (zweite Teilwerte in beiden Serien auftretend!) sind sämtlich mod $\mathfrak{P}^*$ ganz und inkongruent, soweit verschieden, bilden also genau zweimal den Körper E_{q^δ}.

Bemerkung. Ersetzt man q^δ durch beliebige Potenz $q^{\delta r}$, also π durch π^r, so gilt ganz Entsprechendes. Somit Uniformisierung von $K^{(\infty)}$ (bei $\mathsf{K}^{(\delta)}$ anfangend) durch Teilwerte von τ und $\widehat{\tau}$. Unsere Aufgabe, bei *festem* E_{q^δ} zu untersuchen, wieviele entsprechende Werte von $\widehat{\tau}$ in E_{q^δ} liegen. —

Antwort durch Zerlegungsgesetz für $\mathfrak{P}^*$ in den einzelnen über Ω abelschen Körpern $\mathsf{K}^*\left(\widehat{\tau}\left(\frac{\alpha}{\pi\mp1},\mathfrak{a}\right)\right)$. Ergibt: bei richtiger Normierung von π unter $\pm\pi$ sind genau die $\widehat{\tau}\left(\frac{\alpha}{\pi-1},\mathfrak{a}\right)$ in E_{q^δ}, die $\widehat{\tau}\left(\frac{\alpha}{\pi+1},\mathfrak{a}\right)$, soweit nicht zweite Teilwerte, d. h. auch in der ersten Serie vertreten, nicht in E_{q^δ}.

Anzahl der $\widehat{\tau}\left(\frac{\alpha}{\pi-1},\mathfrak{a}\right)$ ist $\mathfrak{N}(\pi-1)-1=\mathfrak{N}(\pi)-\mathfrak{S}(\pi)=q^\delta-(\pi+\overline{\pi})$.[2]

Jedem nicht–zweiten Teilwert darunter entsprechen
= zweiten = = =

zwei Lösungen (da $\widehat{\tau}$ dann $\neq 0$)
eine = (da $\widehat{\tau}$ dann 0).

Die ersteren kommen aber zweimal, die letzteren einmal vor. Daher Anzahl der Lösungen einfach

$$N^{(\delta)}=q^\delta-(\pi+\overline{\pi}),\qquad N_1^{(\delta)}=h=q^\delta+1-(\pi+\overline{\pi})$$

Folglich wegen $\pi\overline{\pi}=q^\delta$ sind also einfach π und $\overline{\pi}$ die Wurzeln des Polynoms

$$\mathsf{P}(z)=z^2-(q^\delta+1-N_1^{(\delta)})z+q^\delta,$$

das zur Funktion $\zeta_K^{(\delta)}(s)$ gehört:

$$\beta^\delta=\pi,\qquad \overline{\beta}^\delta=\overline{\pi}.$$

Das beweist Riemannsche Vermutung, da $\pi,\overline{\pi}$ konjugiert–komplex oder reell gleich sind.

Ferner folgt

$$\beta=\pi_1,\qquad \overline{\beta}=\overline{\pi}_1,$$

wo $\pi_1,\overline{\pi}_1$ die im Vorzeichen richtig normierten Faktoren von

$$q=p^f=\pi\overline{\pi}\quad\text{in}\quad\Omega;\qquad(\pi)=\mathfrak{p}^f,\quad(\overline{\pi})=\overline{\mathfrak{p}}^f$$

sind.

Die richtige Normierung von π unter $\pm\pi$ und π_1 unter $\pm\pi_1$ läßt sich in einigen Fällen noch durch Kongruenzen mod 4 angeben; leider bisher nicht allgemein.

2. Das hier als $\mathfrak{S}$ wiedergegebene Zeichen ist schwer zu lesen.

Für die Fälle $c_2 = 0, c_3 = 0$ $(d = -3, -4)$ gilt ganz Entsprechendes. Hier nur Normierung komplizierter, da mehr Einheitswurzeln, aber voll angebbar.

Analogie zu Siegels Behandlung der Transzendenzprobleme und Diophantischer Gleichungen. Höheres Geschlecht entsprechend verknüpft mit abelschen Funktionen. Ev. auch A. Weils Methoden allein schon ausreichend, zusammen mit algebraisch gefaßtem Abelschem Theorem.

Wurzeln von $\zeta_K(s)$ erscheinen als transzendent bestimmt: Wesentlich gegeben bei Kenntnis von Ω, als Faktoren von q in Ω. Bestimmung von Ω eindeutig durch Lösung des Uniformisierungsproblems

$$j(\mathfrak{a}) \equiv k \mod \mathfrak{P}_0.$$

Zur rein algebraischen Erfassung wäre also diese Uniformisierung losgelöst von Theorie der elliptischen Funktionen zu leisten, insbesondere also transzendentes Argument $\mathfrak{a}$ der Modulfunktion zu gewinnen. Dazu führt vielleicht eine abstrakt aufgebaute Theorie der Modulfunktionen und elliptischen Funktionen über unendlichem Galoisfeld E_∞. Addition der Perioden algebraisch erfaßbar durch Additionstheorem.

5. Anhang. Illustration der Methode an trivialem Problem $y^2 = 1 - x^2$

Uniformisierung:

$$x = c(u), \qquad y = s(u),$$

wo

$$c(u) = \cos 2\pi u, \qquad s(u) = \sin 2\pi u.$$

Koeffizientenuniformisierung tritt nicht auf, da hier Geschlecht 0, kein Parameter.
Uniformisierung der Variablen:

$$c\left(\frac{u}{p-1}\right), \quad c\left(\frac{v}{p+1}\right) \qquad \mu = 0, \ldots, p-2; \quad \nu = 0, \ldots, p.$$

Das sind $2p$ Werte. Je zwei einander gleich (zweite Teilwerte in beiden Serien gemeinsam, entsprechen trivialen Lösungen $\pm 1, 0$). Also genau p verschiedene Werte. Erzeugen zusammen das Kompositum K der reellen Teilkörper des Körpers der $(p-1)$–ten und des Körpers der $(p+1)$–ten Einheitswurzeln. In K zerfällt p in Primideale $\mathfrak{p}$ vom 1. Grade, da $p \equiv 1 \mod p-1$ und $p \equiv -1 \mod p+1$. Die verschiedenen unter den Teilwerten sind inkongruent mod

p. Dies folgt entweder durch Theorie der Multiplikations– oder Teilungsgleichung $c(u)$, indem man nachweist

$$\prod_{\mu}\left(t-c\left(\frac{\mu}{p-1}\right)\right)\prod_{\nu}\left(t-c\left(\frac{\nu}{p+1}\right)\right)\equiv(t^p-t)^2 \mod p,$$

oder durch Darstellung des Differenzenprodukts der verschiedenen Teilwerte durch Einheitswurzeln mittels Additionstheorem 2. Art der Funktion $c(u)$ und Erkenntnis, daß es prim zu p ist.

Erstere Methode führt bei $j(\mathfrak{w})$ zum Uniformisierungsproblem, letztere für $\tau(u,\mathfrak{w})$ zur Konstruktion des Restsystems.

Entscheidung über Lösbarkeit durch Adjunktion eines Wertes $s\left(\frac{\mu}{p-1}\right)$ oder $s\left(\frac{\nu}{p+1}\right)$. Dieser erzeugt jeweils vollen Kreiskörper der d–ten Einheitswurzeln über K, wenn d reduzierter Nenner des Teilpunkts. In ihm zerfällt $\mathfrak{p}$ dann und nur dann, wenn $p\equiv+1 \mod d$. Von den zweiten Teilpunkten abgesehen ist das nur der Fall für Serie $\frac{\mu}{p-1}$, für Serie $\frac{\mu}{p+1}$ ist $p\equiv-1 \mod d$, also auch $p\equiv+1 \mod d$ nur für $d=1,2$. so kommen

$2\frac{p-1-2}{2}$	$=$	$p-3$	Lösungen	für	die	nicht–zweiten Teilwerte
		1	Lösung	$1,0$	für	ersten Teilwert
		1	Lösung	$-1,0$	"	zweiten Teilwert
		.....				
insgesamt		$p-1$	Lösungen			

1.15 Würzburg 1933

Die Riemannsche Vermutung bei den F.K. Schmidtschen Kongruenzzetafunktionen.

Vortrag Würzburg, September 1933.

1. Problemstellung.

Mordellsches Problem: Gegeben endlicher Körper E_q ($q = p^f$; — bei Mordell nur $q = p$) und Polynom $F(x, y)$ in E_q, absolut–irreduzibel (d. h. bei beliebiger algebr. Erweiterung von E_q zu E_{q^r} irreduzibel). Gesucht möglichst genaue Bestimmung der Anzahl N der Lösungen von $F(x, y) = 0$ in E_q.

Da für die q^2 Wertsysteme x, y q Funktionswerte $F(x, y)$ zur Verfügung stehen, ist zu erwarten, daß N ungefähr q ist. Man fragt dann nach der Größe von $N - q$. Ist speziell $F(x, y) = y - F(x)$, so ist trivialerweise genau $N = q$. Allgemein sucht man eine Abschätzung vom Typus:

$$|N - q| \leqq Cq^{\vartheta}, \qquad \text{(kurz: } (\vartheta, C)\text{–Abschätzung)},$$

wo $\vartheta < 1$ und $C > 0$ Konstanten sind, die nur von den algebraischen Eigenschaften von $F(x, y)$ abhängen, etwa bei Betrachtung aller Polynome eines festen Grades in x, y nur von diesem Grad, nicht von q und den Koeffizienten. Die genaue Präzisierung des zu erwartenden und in gewissen Fällen bewiesenen Resultats lautet allerdings etwas anders.

Dazu führt das Studium des durch $F(x, y)$ erzeugten algebraischen Gebildes über E_q. Dies ist ein Körper K algebraischer Funktionen über E_q. Umgekehrt wird jeder solche durch eine Relation $F(x, y) = 0$ erzeugt. Der absoluten Irreduzibilität von $F(x, y)$ entspricht dabei die Tatsache, daß E_q der umfassendste in K enthaltende absolut–algebraische Körper (Konstantenkörper) ist.

x, y sind nicht ausgezeichnet innerhalb K, birationale Transformation. Daher auch $F(x, y)$ und Lösungsanzahl N keine Invarianten von K. F. K. Schmidt hat aber birational invarianten Punktbegriff des Gebildes eingeführt: Punkt = Primdivisor P von K, definiert durch Bewertung von K = homomorphe Abbildung von K auf einen Konstantenkörper E_{q^r}, r Grad von P. Dabei entsprechen insbesondere die Primdivisoren P_1 vom Grade 1 wesentlich eineindeutig den Lösungen a, b von $F(x, y) = 0$ in E_q, abgesehen

von endlich vielen nicht birational invarianten Ausnahmeprimdivisoren (außerwesentliche Diskriminantenteiler von $F(x,y)$, Nennerteiler von x,y). Die Anzahl N_1 der P_1 ist das birational invariante Äquivalent für N. Die Aufgabe ist also, eine (ϑ, C)–Abschätzung für $N_1 - (q+1)$ zu finden ($q+1$ mit Rücksicht auf das Unendliche theoretisch richtiger als q). Daraus ist dann in jedem Falle durch genaues Studium von $N_1 - N$ (stets $\geqq 0$) der Übergang zu der ursprünglichen Mordellschen Aufgabe betr. $N - q$ möglich.

Die Punkte P von höherem Grade r entsprechen ebenso wesentlich eineindeutig den Serien konjugierter Lösungen α, β in E_{q^r}, und sie lösen sich in $K^{(r)} = E_{q^r}(x,y)$ in r Punkte vom Grade 1 auf. Betrachtet man also das „algebraisch abgeschlossene“ Gebilde $\overline{K} = \overline{E}(x,y)$, wo $\overline{E}$ der algebraisch abgeschlossene absolut–algebraische Körper der Charakteristik p ist, so entsprechen dessen Punkte $\overline{P}$ im wesentlichen eineindeutig der Gesamtheit aller algebraischen Lösungen von $F(x,y) = 0$. Eine grundlegende Invariante von $\overline{K}$ (und damit von K) ist das Geschlecht g, das von F. K. Schmidt in formaler Analogie zur gewöhnlichen algebraischen Funktionentheorie eingeführt ist (Verzweigungstheorie). $g = 0$ ist gleichbedeutend mit der linearen Erzeugbarkeit von K, $y = F(x)$, Beweis allerdings bisher nur analytisch.

Die Bestimmung von N_1 kann hiernach in folgende zwei Teilaufgaben zerlegt werden:

a.) Übersicht über alle algebraischen Punkte des Gebildes.

b.) Aussonderung der in E_q rationalen Punkte.

2. Zusammenhang mit der Riemannschen Vermutung.

Auf Grund seines birational invarianten Divisorenbegriffs definiert F. K. Schmidt die K invariant zugeordnete Zetafunktion:

$$\zeta_K(s) = \prod_P \frac{1}{1 - \frac{1}{N(P)^s}}, \quad \text{wo} \quad N(P) = q^r,$$

eine mit der Periode $\frac{2\pi i}{\log q}$ periodische Funktion von s. Speziell für $g = 0$, also $K = k = E_q(x)$, ist diese Funktion trivial:

$$\zeta_K(s) = \prod_p \frac{1}{1 - \frac{1}{N(p)^s}} = \frac{1}{1 - \frac{q}{q^s}} \, \frac{1}{1 - \frac{1}{q^s}}.$$

Sie hat keine Nullstellen, und die Pole 1. Ordnung

$$s = \frac{2\pi i v}{\log q}, \quad 1 + \frac{2\pi i v}{\log q}.$$

Diese treten als einzige Pole von $\zeta_K(s)$ auf, nämlich

$$\frac{\zeta_K(s)}{\zeta_k(s)} = 1 + \frac{N_1 - (q+1)}{q^s} + \cdots + \frac{q}{q^{2gs}}$$

ist ein Polynom in $\frac{1}{q^s}$ vom Grade $2g$. Es gibt ferner daher genau $2g$ Serien von Nullstellen von $\zeta_K(s)$, wegen der Produktdarstellung und der von F. K. Schmidt bewiesenen Funktionalgleichung jedenfalls im „kritischen Streifen“ (inkl. Rand) gelegen, im folgenden beschrieben durch die zugehörigen $2g$ Nullstellen β_i in $z = q^s$ des z–Polynoms

$$z^{2g}\frac{\zeta_K(s)}{\zeta_k(s)} = z^{2g} + \big(N_1 - (q+1)\big)z^{2g-1} + \cdots + q,$$

dessen Koeffizienten sich als ganz–rational erweisen; insbesondere ist der zweithöchste gerade die zu untersuchende Differenz, und diese also dargestellt als die negative Summe der Nullstellen β_i:

$$N_1 - (q+1) = -\sum_{i=1}^{2g} \beta_i.$$

Die Nullstellen liegen jedenfalls im „kritischen“ Kreisring $1 \leqq z \leqq q$, und die Riemannsche Vermutung für $\zeta_K(s)$ besagt:

$$|\beta_i| = q^{\frac{1}{2}}.$$

Sie impliziert hiernach:

$$|N_1 - (q+1)| \leqq 2gq^{\frac{1}{2}},$$

also eine $(\frac{1}{2}, 2g)$–Abschätzung. Das ist die oben in Aussicht gestellte Präzisierung des zu erwartenden Resultats. Jedes rohere Resultat $|\beta_i| \leqq cq^{\vartheta}$ $(\frac{1}{2} < \vartheta < 1)$ impliziert ebenso eine rohere Abschätzung, nämlich eine $(\vartheta, 2gc)$–Abschätzung.

Dieser Zusammenhang ist umkehrbar (Artin) durch simultane Betrachtung der zu den $K^{(r)} = E_{q^r}(x,y)$ gehörigen Anzahlen $N_1^{(r)}$. Für diese gilt nämlich:

$$N_1^{(r)} - (q^r + 1) = -\sum_{i=1}^{2g} \beta_i^r$$

Eine (ϑ, C)–Abschätzung aller $N_1^{(r)}$ mit von r unabhängigem C impliziert also $|\beta_i| \leqq q^{\vartheta}$ und führt überdies zur (ev.) Verbesserung des ursprünglichen C in $2g$. Insbesondere folgt aus einer $(\frac{1}{2}, C)$–Abschätzung für alle $N_1^{(r)} - (q^r + 1)$ die Riemannsche Vermutung.

3. Elliptischer Fall, $g = 1$.

Nächsteinfacher Fall nach dem trivialen $g = 0$.

Sei $p \neq 2, 3$. Dann K durch Weierstraßsche Normalform

$$y^2 = 4x^3 - c_2 x - c_3 \quad \text{mit} \quad \partial = c_2^3 - 27c_3^2 \neq 0$$

erzeugbar. Die Spezialfälle $c_2 = 0, c_3 = 0$ seien ausgeschlossen.

Übergang zu von Dimension 0 homogener Normalform

$$\eta^2 = 4\xi^3 - \kappa_2 \xi - \kappa_3 \quad \text{mit} \quad \kappa_2^3 - 27\kappa_3^2 = 1$$

durch Multiplikationstransformation

$$\eta = \frac{y}{\sqrt[4]{\partial}},\ \xi = \frac{x}{\sqrt[6]{\partial}}\,; \qquad \kappa_2 = \frac{c_2}{\sqrt[3]{\partial}},\ \kappa_3 = \frac{c_3}{\sqrt[2]{\partial}}\,.$$

Ist verbunden mit Erweiterung zu $K^{(t)} = E_{q^t}(x,y)$, wo $t \mid 12$, was nicht wesentlich ist.

Teilaufgabe a.) Übersicht über alle algebraischen Punkte des Gebildes; wird bewerkstelligt durch Uniformisierung mittels elliptischer Funktionen. Diese selbst zur Uniformisierung nicht geeignet, da in einem Zahlkörper (Char. 0) verlaufend. Übergang zu Körper der Char. p wird erreicht, durch Übergang zu den Restklassen nach einem Primidealteiler von p in einem algebraischen Zahlkörper, dem die zu betrachtenden Funktionswerte angehören (Komplexe Multiplikation). Diese Uniformisierung ist mir bisher in allen Fällen gelungen, wo der Grad der Invariante $\kappa_2^3 = \frac{c_2^3}{\partial}$ über E_p ungerade ist, speziell also, wenn ursprünglich E_p selbst als Grundkörper gegeben war.

Uniformisierungstheorem.

I. Koeffizienten. Es existiert ein eindeutig (in einem Spezialfall zweideutig) b. a. prop. bestimmter Modul $a = [\alpha_1, \alpha_2]$ in einem imaginär–quadratischen Zahlkörper $\Omega = \mathsf{P}(\sqrt{d})$, der reguläres Ringideal mod m für ein zu p primes m ist, derart, daß

1.) $p = p\overline{p}$ in Ω ($\overline{p} = p$ oder $\overline{p} \neq p$),

$p^f = (\varpi)$, $\overline{p}^f = (\overline{\varpi})$, $\varpi\overline{\varpi} = p^f = q$;

2.) für einen Primteiler P von p in dem durch die Modulfunktionswerte

$$\gamma_2(\mathfrak{a}) = \frac{g_2(\mathfrak{a})}{\sqrt[3]{\Delta(\mathfrak{a})}}, \qquad \gamma_3(\mathfrak{a}) = \frac{g_3(\mathfrak{a})}{\sqrt[2]{\Delta(\mathfrak{a})}}$$

über Ω bestimmten Ringklassenkörper K der Restklassenkörper mod P isomorph in E_{q^t} enthalten ist und dabei gilt:

$$\gamma_2(a) \equiv \kappa_2, \qquad \gamma_3(a) \equiv \kappa_3 \mod P.$$

Damit ist die zu untersuchende Relation dargestellt als realisiert durch Betrachtung der Identität

$$\widehat{\pi}(u, \mathfrak{a})^2 = 4\pi(u, \mathfrak{a})^3 - \gamma_2(\mathfrak{a})\pi(u, \mathfrak{a}) - \gamma_3(\mathfrak{a}),$$

wo

$$\pi(u, \mathfrak{a}) = \frac{\wp(u, \mathfrak{a})}{\sqrt[6]{\Delta(\mathfrak{a})}}, \qquad \widehat{\pi}(u, \mathfrak{a}) = \frac{\wp'(u, \mathfrak{a})}{\sqrt[4]{\Delta(\mathfrak{a})}},$$

als Kongruenz mod P.

II. Variable. Läßt man u alle rationalen Teilpunkte $\frac{\alpha}{n}$ (α in a) mit zu p primem Nenner n des Periodenmoduls a durchlaufen, und bezeichnet $\overline{P}$ einen Primteiler von P in dem durch alle zugehörigen Teilwerte der Funktionen $\pi(u, a)$, $\widehat{\pi}(u, a)$ erzeugten unendlichen algebraischen Zahlkörper $\overline{\mathsf{K}}$ über K, so erhält man genau alle Punkte des algebraisch–abgeschlossenen Gebildes $\overline{K}$.

Damit ist die Teilaufgabe a.) gelöst.

Teilaufgabe b.) Aussonderung der in E_{q^t} rationalen Punkte; erfordert geeignete Auswahl unter den sämtlichen Teilpunkten $\frac{\alpha}{n}$. Zunächst durchläuft für die Teilpunkte $\frac{\alpha}{\varpi^t \pm 1}$ der Funktionswert $\pi(u, a) \mod \overline{P}$ genau

zweimal den Körper E_{q^t} (in isomorpher Abbildung). Dann zeigt das Zerlegungsgesetz für die durch die zugehörigen Funktionswerte $\widehat{\pi}(u,a)$ erzeugten Strahlklassenkörper, daß genau für die eine der beiden Teilpunktserien, bei passender Normierung etwa die Serie $\frac{\alpha}{\varpi^t-1}$, auch der Funktionswert $\widehat{\pi}(u,a)$ in E_{q^t} liegt.

Damit ist die Uniformisierung auch unter Beschränkung auf das ursprüngliche Gebilde K, oder vielmehr auf $K^{(t)}$, geleistet. Die fragliche Anzahl $N_1^{(t)}$ ist sogar genau bestimmt:

$$N_1^{(t)} = (q^t+1) - (\varpi^t + \overline{\varpi}^t),$$

und daraus folgt weiter durch den Artinschen Rückschluß auf K selbst: Bei richtiger Normierung der beiden konjugierten Faktoren $\varpi, \overline{\varpi}$ von q in Ω sind diese die Nullstellen des zu $\zeta_K(s)$ gehörigen Polynoms, und es ist

$$N_1 = (q+1) - (\varpi + \overline{\varpi}), \quad \text{also} \quad |N_1 - (q+1)| \leqq 2q^{\frac{1}{2}}.$$

Die Riemannsche Vermutung stimmt, da $\varpi, \overline{\varpi}$ konjugiert–komplex sind.

Bemerkung. Die Bestimmung von $\Omega, m, a, \varpi, \overline{\varpi}$ zu K ist vorläufig nur auf dem transzendenten Wege über die Theorie der elliptischen Modulfunktionen gegeben. Ich möchte vermuten, daß man auf Grund des Additionstheorems der $\wp$–Funktion in seiner rationalen Gestalt zu einer abstrakten Theorie der Modul– und elliptischen Funktionen der Char. p kommen kann, die dann den Schlüssel zur algebraischen Bestimmung der Nullstellen der Zetafunktion liefert.

Für höheres Geschlecht g hätte man dasselbe mit der allgemeinen Theorie der abelschen Funktionen zu machen. Das scheint im Hinblick auf die Erfolge Siegels mit dieser Theorie für die Behandlung des Problems der Lösungsanzahl diophantischer Gleichungen hoffnungsvoll.

4. Weitere Fälle.

a.) Ausnahmefälle $c_2 = 0, c_3 = 0$ subsumieren sich durch bir. Transf. unter allgemeinen Fall

$$F(x,y) = ax^m + by^n - c \quad \text{in} \quad E_q, \qquad (a,b,c \neq 0)$$

wo oBdA $m, n \mid q-1$ angenommen werden darf. In diesem Falle Bestimmung der Nullstellen von $\zeta_K(s)$, und damit von N_1 und N, elementar ausführbar

(Davenport–Hasse; Publikation demnächst). Nullstellenanzahl nach allgemeiner Theorie:

$$2g = (m-1)(n-1) - (d-1), \quad \text{wo} \quad d = (m,n).$$

Methode:

$$K = E_q(x,y) = k\left(\sqrt[m]{\frac{ct}{a}}, \sqrt[n]{\frac{c(1-t)}{b}}\right) \quad \text{über } k = E_q(t) \text{ vom Geschlecht } 0,$$

$$\text{wo} \quad t = ax^m = 1 - by^n.$$

$$\zeta_K(s) = \prod_{\chi,\psi} L_k(s, X\Psi),$$

wo

$$X(\mathfrak{a}) = \left(\frac{\frac{ct}{a}}{\mathfrak{a}}\right)_m^{\mu}, \quad \Psi(\mathfrak{a}) = \left(\frac{\frac{c(1-t)}{b}}{\mathfrak{a}}\right)_n^{\nu} \qquad (\mu = 0,\dots,m-1;\ \nu = 0,\dots,n-1)$$

Charaktere (Legendre–Symbole) nach Teilkörpern $k\left(\sqrt[m]{\frac{ct}{a}}\right), k\left(\sqrt[n]{\frac{c(1-t)}{b}}\right)$ durchlaufen. Auf Grund der Klassenkörpertheorie (Reziprozitätsgesetz, Dedekind) dieser beiden Körper findet man:

$$\begin{aligned} L_k(s, X\Psi) &= \zeta_k(s) && \text{für} \quad \chi = 1,\ \psi = 1 \\ &= 1 && \text{für} \quad \chi = 1 \quad \text{oder} \quad \psi = 1 \\ & && \text{oder} \quad \chi\psi = 1 \quad \text{sonst} \\ &= 1 + \frac{1}{q^s}\,\frac{\tau_a(\chi)\tau_b(\chi)}{\tau_c(\chi\psi)} && \text{für} \quad \chi \neq 1,\ \psi \neq 1,\ \chi\psi \neq 1. \end{aligned}$$

Dabei χ, ψ die in bestimmter Weise X, Ψ zugeordneten Charaktere in E_q, und

$$\tau_a(\chi) = \sum_{x \text{ in } E_q} \chi(x) e^{\frac{2\pi i a}{p}\mathrm{Sp}(x)} \qquad (a\text{–te Gausssche Summe zu } \chi)$$

Also sind die $(m-1)(n-1) - (d-1)$ Grössen

$$\varpi(\chi,\psi) = -\frac{\tau_a(\chi)\tau_b(\psi)}{\tau_c(\chi\psi)} \qquad (\text{Faktorensystem der Gaussschen Summen})$$

die Nullstellen des zu $\zeta_K(s)$ gehörigen Polynoms (Bestätigung des Geschlechts) und die Riemannsche Vermutung stimmt (Betrag der Gaussschen Summe ist $q^{\frac{1}{2}}$). Durch Verallgemeinerung der Kummerschen Resultate über Primidealzerlegung der Gaussschen Summen lassen sich die Nullstellen $\varpi(\chi, \psi)$ arithmetisch genau charakterisieren, nämlich als bestimmte Potenzprodukte der Primidealteiler von p im Körper der $(q-1)$–ten E. W. mit bestimmten Kongruenzeigenschaften. Übrigens noch merkwürdige bisher unbekannte Relationen zwischen Gaussschen Summen:

$$\prod_{\chi^n=\varphi} \tau(\chi) = \varphi(n)\tau(\varphi) \prod_{\substack{\psi^n=1 \\ \psi\neq 1}} \tau(\psi).$$

Beweis durch Koeffizientenvergleich in

$$L_{\overline{k}}(s, \overline{X}) = \prod_{\Psi} L_k(s, X\Psi) \qquad (\text{für } x^m + y^n = 1)$$

für $\overline{k} = k(y)$, $K = k(\sqrt[m]{1-y^n})$ und den X entspr. Charakter $\overline{X}$ in $\overline{k}$.

Übrigens subsumiert sich auch allererster Fall mit bew. Riemannscher Vermutung, nämlich Mordellscher Fall $y^3 = F_3(x)$ (kub. Pol.) dem eben betr. allgem. Fall durch birat. Transf. (ell. Fall mit $c_2 = 0$).

b.) Hyperelliptische Fälle.

$$y^n = F(x) \qquad (\text{oBdA } F(x) \text{ Pol., } n \mid q-1)$$

Riemannsche Vermutung dafür äquivalent mit $(\frac{1}{2}, C)$–Abschätzung der Mordellschen *Charaktersummen*

$$S(\chi) = \sum_{x \text{ in } E_q} \chi\big(F(x)\big), \qquad (\chi \ n\text{–ter Potenzcharakter in } E_q),$$

also Problem aus der Verteilung des n–ten Potenzcharakters in E_q.

Im elliptischen Falle ($p \neq 2, 3$) wie gesagt, durch meine Uniformisierungstheorie bestätigt. Allgemein Teilresultate von Davenport und Mordell (gewisse $\vartheta > \frac{1}{2}$).

c.) Zyklische Körper vom Grad *p*. Artinsche Gleichungen

$$y^p - y = F(x) \qquad (\text{rat. Funkt.}).$$

Hängt völlig analog zusammen mit Mordellschen *Exponentialsummen*

$$S_\nu = \sum_{x \text{ in } E_q}{}' e^{\frac{2\pi i\nu}{p}\mathrm{Sp}(F(x))} \qquad (x \text{ keine Nennernullstelle, aber ev. } \infty)$$

Ich konnte nämlich in Ergänzung von F. K. Schmidt zeigen, dass hier K [1] Klassenkörper ist nach Klasseneinteilung durch Charakter

$$X(\mathfrak{a}) = \left[\frac{F(x)}{\mathfrak{a}}\right]_p = e^{\frac{2\pi i}{p}(\mathrm{Sp}(F(x))} \quad (\text{Spur mod } \mathfrak{a}) \qquad \Big\| \text{ Insbes. Artinsches Rez. Ges. für diesen } p\text{–ten Charakter!}$$

dessen zugeordneter additiver Charakter in E_q ist:

$$\chi(a) = e^{\frac{2\pi i a}{p}}, \quad \text{also} \quad S(\chi) = \sum_{x \text{ in } E_q}{}' \chi\big(F(x)\big) = S_1.$$

Riemannsche Vermutung äquivalent mit $(\frac{1}{2}, C)$–Abschätzung der S_ν.

Bis auf triviale Spezialfälle (s. u.) bisher nur Teilresultate von Mordell und Davenport (gewisse $\vartheta > \frac{1}{2}$).

Erledigter Spezialfall:

$$y^p - y = x^m. \qquad 2g = (m-1)(p-1)$$

Führt ganz analog wie oben durch Betrachtung von $K = k\left(\sqrt[m]{t}, \sqrt[p]{t}\right)$ über $k = E_q(t)$ $(t = y^p - y = x^m)$ zu

$$\zeta_K(s) = \zeta_k(s) \prod_{\chi \neq 1} \prod_{\nu \neq 0} L_k(s, \chi, \nu) \quad \text{mit} \quad L_k(s, \chi, \nu) = 1 + \frac{1}{q^s}\tau_\nu(\chi).$$

Also sind die Nullstellen einfach die $-\tau_\nu(\chi)$, neue Deutung der Gaussschen Summen.

Nach Geschlecht gemessen ($2g = (v-2)(p-1)$, wo v = Grad des Führers, aus Nenner von $F(x)$ bestimmt) sind niedrigste Fälle:

a.) $F(x)$ kub. Pol. (Davenport: $\vartheta = \frac{5}{8}$)

b.) $F(x)$ Quot. zweier quadr. Pol. (äquiv. mit Klostermannschen Summen; Davenport–Salié: $\vartheta = \frac{2}{3}$).

1. undeutlich

Ich hoffe, gerade in diesen beiden Fällen durch Uniformisierung mittels elliptischer Transformationsgleichungen höherer Stufe zu $\vartheta = \frac{1}{2}$ und exakten Nullstellen zu kommen.

4. Weitere Fälle.

Die Ausnahmefälle, wo $c_2 = 0$ oder $c_3 = 0$, subsumieren sich (durch birationale Transformation) unter den allgemeinen Fall:

$$F(x, y) = ax^m + by^n - 1 \quad \text{in} \quad E_q,$$

wo oBdA $m, n \mid q - 1$ angenommen werden darf. In diesem Fall läßt sich die Bestimmung der Nullstellen der Zetafunktion und damit der fraglichen Anzahl N_1 (und auch N) leicht elementar ausführen, wie Davenport und ich gezeigt haben (Veröffentlichung demnächst). Die Nullstellenanzahl ist

$$2g = (m-1)(n-1) - (d-1), \quad \text{wo} \quad d = (m, n).$$

Man findet durch Ausrechnen der Lösungsanzahl mittels der m–ten und n–ten Potenzcharaktere χ und ψ in E_q:

$$N_1 - (q+1) = \sum_{\chi,\psi,\chi\psi\neq 1} \chi(a)\psi(b)\frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)} = \sum_{\chi,\psi,\chi\psi\neq 1} \varpi(\chi, \psi),$$

und $N = N_1 - N$, wo N die sofort angebbare Anzahl der Lösungen von $z^d = -\frac{a}{b}$ in E_q ist. $\tau(\chi)$ bedeutet die Gaußsche Summe zum Charakter χ:

$$\tau(\chi) = \sum_{x \text{ in } E_q} \chi^{-1}(x) e^{\frac{2\pi i}{p}\mathrm{Sp}(x)}.$$

Der Hauptschluß besteht in dem Nachweis, daß bei Übergang zu E_{q^r} die Summanden $\varpi(\chi, \psi)$ rechts sich einfach mit r potenzieren, also einem interessanten Theorem über Gaußsche Summen in endlichen Körpern. Daraus folgt unmittelbar, daß diese $\varpi(\chi, \psi)$ gerade die gesuchten Nullstellen sind; die Anzahl ist in der Tat gerade $2g$. Ihr Betrag ist nach der bekannten Tatsache über Gaußsche Summen wirklich $q^{\frac{1}{2}}$, Riemannsche Vermutung.

Durch Verallgemeinerung der Kummerschen Resultate über die Primidealzerlegung der Gaußschen Summen kann man ferner hier die fraglichen Nullstellen arithmetisch genau charakterisieren, nämlich als bestimmte Potenzprodukte der Primidealteiler von p im Körper der $q-1$–ten Einheitswurzeln mit bestimmten Kongruenzeigenschaften. Übrigens wird man dabei

noch zu merkwürdigen Relationen zwischen den Gaußschen Summen geführt, nämlich

$$\prod_{\chi^n=X} \tau(\chi) = X(n)\tau(X) \prod_{\substack{\psi^n=1 \\ \psi\neq 1}} \tau(\psi).$$

Es sei bemerkt, daß sowohl die Ausdrücke $\varpi(\chi,\psi)$, als auch diese Relation sich mittels hyperkomplexer Faktorensysteme deuten lassen. Vielleicht liegt hier die algebraische Quelle für diese Relationen.

Übrigens subsumiert sich auch der allererste Fall, in dem die Riemannsche Vermutung festgestellt wurde, nämlich der von Mordell erledigte Fall

$$y^3 = F_3(x) \qquad \text{(kubisches Polynom)},$$

dem oben betrachteten allgemeinen Fall durch geeignete birationale Transformation (elliptischer Fall mit $c_2 = 0$).

5. Charaktersummen und Exponentialsummen.

Mordell hat im Zusammenhang mit den Lösungsanzahlen N zwei Sorten von Summen studiert.

a.) Charaktersummen:

$$S(\chi) = \sum_{x \text{ in } E_q} \chi\big(F(x)\big),$$

wo $F(x)$ eine rationale Funktion über E_q (oBdA ein Polynom) und χ ein m–ter Potenzcharakter in E_q mit oBdA $m \mid q-1$ ist. Deren Untersuchung ist äquivalent mit der Untersuchung der Lösungszahl N im hyperelliptischen Falle

$$y^m = F(x).$$

Die Riemannsche Vermutung für dieses Gebilde ist äquivalent mit:

$$|S(\chi)| \leqq C q^{\frac{1}{2}},$$

wo C eine mit dem Geschlecht des Gebildes zusammenhängende leicht angebbare Konstante ist. Im elliptischen Falle (und $p \neq 2, 3$) ist das, wie ich oben ausführte, bestätigt. Allgemein liegen jedenfalls Teilresultate von Davenport und Mordell vor (mit gewissen $\vartheta > \frac{1}{2}$).

b.) Exponentialsummen:

$$S_\nu = \sum_{x \text{ in } E_q}{}' e^{\frac{2\pi i\nu}{p}\mathrm{Sp}(F(x))} \qquad (x \text{ keine Nennernullstelle})$$

Ich konnte zeigen, daß diese Summen in ganz analoger Weise mit denjenigen Gebilden verknüpft sind, die durch eine zyklische Gleichung vom Grade p über $E_q(x)$ erzeugt werden, also eine Gleichung vom Artinschen Typus:

$$y^p - y = F(x),$$

wo die rationale Funktion $F(x)$ über E_q jetzt nicht mehr einfach als Polynom angenommen werden darf. Anders gesagt, können also die Exponentialsummen aufgefaßt werden als Charaktersummen für die Charaktere, die der Bildung $y^p - y$ statt der m–ten Potenz y^m entsprechen.

Die Riemannsche Vermutung für das genannte Gebilde ist äquivalent mit:

$$|S_\nu| \leqq (v-2)q^{\frac{1}{2}},$$

wo v der Grad desjenigen Divisors ist, der entsteht, wenn man die Exponenten der Nennerprimteiler von $F(x)$ um 1 erhöht; es ist $2g = (p-1)(v-2)$. Der fragliche Divisor vom Grade v ist der Führer des Körpers K im Sinne der Klassenkörpertheorie. Diese Klassenkörpertheorie war bei F. K. Schmidt anders als in den Fällen mit durch p unteilbarem Grade noch nicht entwickelt. Ich konnte dies tun, und insbesondere das Artinsche Reziprozitätsgesetz für diese zyklischen Körper vom Grade p beweisen, woraus sich dann der eben angeführte Zusammenhang ergab.

Die Riemannsche Vermutung ist für diese Exponentialsummen noch in keinem Falle bestätigt. Aber es liegen wieder Teilresultate von Davenport und Mordell mit $\vartheta > \frac{1}{2}$ vor.

Das Geschlecht, d. h. die darin steckende Zahl v gibt ein gewisses Maß für die Höhe des betr. Problems. Der in diesem Sinne niedrigste Typus, $v-2=2$ ($=1$ ist trivial) liegt vor, wenn

α.) $F(x)$ ein kubisches Polynom ist (Davenport: $\vartheta = \frac{5}{8}$),

β.) $F(x)$ Quotient zweier quadratischer Polynome ist (äquivalent mit sogen. Klostermanschen Summen; Davenport, Salié: $\vartheta = \frac{2}{3}$).

In diesen beiden Fällen hoffe ich bis zur vollen Wahrheit, der Riemannschen Vermutung vordringen zu können durch Uniformisierung mittels Transformationsgleichungen höherer Stufe der elliptischen Funktionen.

1.16 Göttingen 1933 II

Quaternionenkörper und Darstellungstheorie der quadratischen Formen.

Vortrag Göttingen, Dezember 1933.

Gewöhnliche Quaternionen.

System der Größen

$$\xi = w + xi + yj + zij$$

mit Zahlkoordinaten w, x, y, z, gebildet aus 4 hyperkomplexen Einheiten $1, i, j, ij$ mit den Rechenvorschriften

$$i^2 = -1, \qquad j^2 = -1, \qquad ij = -ji.$$

Die Zahlkoordinaten w, x, y, z nimmt man gewöhnlich als *reelle* Zahlen. Dann gelten alle Rechengesetze bis auf das komm. Gesetz der Multiplikation. Insbesondere ist die Division durch $\xi \neq 0$ stets möglich, weil der dabei in den Koordinaten auftretende Nenner

$$N(\xi) = \xi\xi' = w^2 + x^2 + y^2 + z^2$$

nicht Null ist. Dieser Nenner ist das Produkt von ξ mit den konjugierten

$$\xi' = w - xi - yj - zij,$$

und die Division $\frac{\eta}{\xi}$ vollzieht sich nach dem Schema $\dfrac{\eta\xi'}{N(\xi)}$. Alles dies gilt a fortiori bei Beschränkung auf *rationale* Koordinaten. Im folgenden *stets* so.

Verallgemeinerte Quaternionen.

System der Größen

$$\xi = w + x\alpha + y\beta + z\alpha\beta$$

mit *rationalen Zahlkoordinaten* w, x, y, z, gebildet aus 4 hyperkomplexen Einheiten $1, \alpha, \beta, \alpha\beta$ mit den Rechenvorschriften

$$\alpha^2 = a, \qquad \beta^2 = b, \qquad \alpha\beta = -\beta\alpha.$$

Dabei a, b gegebene rationale Zahlen $\neq 0$. Es gelten wieder die Gesetze der Addition, Subtraktion und Multiplikation bis auf das komm. Gesetz der Multiplikation. Die Division muß untersucht werden. Rechnet man wieder

$$\xi' = w - x\alpha - y\beta - z\alpha\beta$$

als das konjugierte zu ξ, so ist hier

$$N(\xi) = \xi\xi' = w^2 - ax^2 - by^2 + abz^2,$$

und für die Division kommt es genau wie oben darauf an, ob diese quadr. Form nicht-identische Nulldarstellungen hat. (*Nullform*!), und zwar entsprechend unserer Grundvoraussetzung mit *rationalen* w, x, y, z.

Ich bezeichne das verallgemeinerte hyperkomplexe Quaternionensystem mit den Koeffizienten a, b durch (a, b). In diesem Sinne sind die gewöhnlichen Quaternionen $(-1, -1)$.

1. Hauptfrage. *Wann ist* (a, b) *ein Nullsystem*? Bezeichnung: $(a, b) \sim 1$. Gleichbedeutend mit der Frage: *Wann ist die quaternäre quadratische Form*

$$F = w^2 - ax^2 - by^2 + abz^2$$

Nullform? Oder auch: *Wann ist die ternäre quadratische Form*

$$f = w^2 - ax^2 - by^2$$

Nullform?

Ist nämlich F Nullform, so a fortiori auch F. Ist umgekehrt F Nullform,

$$(w_0^2 - ax_0^2) - b(y_0^2 - az_0^2) = 0,$$

so entweder a Quadrat und f trivialerweise Nullform; oder a kein Quadrat, dann

$$y_0^2 - az_0^2 \neq 0$$

und

$$\frac{w_0^2 - ax_0^2}{y_0^2 - az_0^2} = \frac{N(w_0 + \alpha x_0)}{N(y_0 + \alpha z_0)} = N\left(\frac{w_0 + \alpha x_0}{y_0 + \alpha z_0}\right) = N(u_0 + av_0) = u_0^2 - av_0^2 = b,$$

also wieder f Nullform. –

2. Hauptfrage. *Äquivalenz.* Durch Ausübung einer nicht-singulären Basistransformation T auf $1, \alpha, \beta, \alpha\beta$ kann man neue Basis $\omega_1, \omega_2, \omega_3, \omega_4$ herleiten. Dabei erfahren die Koordinaten w, x, y, z die kontragrediente Transformation T'^{-1}, und F geht in eine äquivalente quadratische Form F' über. Im allgemeinen wird das Multiplikationsschema der neuen Basis $\omega_1, \omega_2, \omega_3, \omega_4$ nicht wieder von derselben einfachen Art sein, wie für $1, \alpha, \beta, \alpha\beta$, und dementsprechend F' nicht von derselben einfachen Art wie F. Es kann jedoch sein, daß T eine neue Basis der Form $1, \alpha', \beta', \alpha'\beta'$ mit

$$\alpha'^2 = a', \qquad \beta'^2 = b', \qquad \alpha'\beta' = -\beta'\alpha'$$

liefert, und demgemäß

$$F' = w'^2 - a'x'^2 - b'y'^2 + a'b'z'^2$$

wird. Man sieht auch leicht, daß umgekehrt, wenn F' diese Form bekommt, die neue Basis das genannte einfache Multiplikationsschema hat. Wir schreiben dann $(a', b') = (a, b)$. Die notwendige und hinreichende Bedingung dafür ist die *Äquivalenz* $F' \sim F$. Die Transformationskoeffizienten sind dabei, wie alle vorkommenden Zahlen, als rationale Zahlen gedacht.

Z.B. ist so stets $(aa_0^2, bb_0^2) = (a, b)$ für beliebige $a_0, b_0 \neq 0$, d.h. es kommt für die a, b nicht auf quadratische Faktoren an, sie können stets als ganze quadratfreie Zahlen angenommen werden. Ferner ist z.B. stets

$$(a, b) = (a, b'), \qquad \text{wenn} \quad \left(a, \frac{b}{b'}\right) \sim 1, \quad \text{d.h.} \quad \frac{b}{b'} = u_0^2 - av_0^2.$$

Denn dann

$$F = (w^2 - ax^2) - b(y^2 - az^2) = (w^2 - ax^2) - b'(u_0^2 - av_0^2)(y^2 - az^2) = \\ = (w^2 - ax^2) - b'(y'^2 - az'^2).$$

Die 2. Hauptfrage lautet also: *Wann ist* $(a', b') = (a, b)$? Gleichbedeutend mit: *Wann ist* $F' \sim F$?

Wir wollen uns hier hauptsächlich mit der Lösung der 1. Hauptfrage beschäftigen. Daraus kann man dann, wie ich anschließend skizzieren werde, auch zu einer Lösung der 2. Hauptfrage kommen. Die Lösung wird uns überdies einen Einblick in zentrale Fragestellungen und Theorien der modernen Algebra und Arithmetik vermitteln.

Lösung der 1. Hauptfrage. Dafür kommt es nicht auf die Unterscheidung verschiedener Erzeugungsarten (a, b), (a', b') desselben Systems, d.h. auf die Unterscheidung äquivalenter F, F' an. Die Lösung beruht auf einem *Fundamentalsatz über quadratische Formen*, den ich in den Mittelpunkt dieses Vortrags stellen will. Dieser findet sich schon als beherrschendes Prinzip in der klassischen Theorie der quadratischen Formen, wie sie in den berühmten Disqu. Arbeiten von Gauß entwickelt ist, allerdings in etwas anderer Einkleidung. Und er hat sich in näherer Zeit als leitendes Grundprinzip für viele zahlentheoretische Fragestellungen erwiesen.

Auf dies Prinzip führt folgende Überlegung: Ist die Form

$$f = w^2 - ax^2 - by^2$$

(a, b ganz rational quadratfrei) Nullform, so ist sie sicher auch *Nullform mod* m für jede ganze Zahl $m > 0$, d.h. sie kann teilbar durch m gemacht werden und zwar so, daß w, x, y mit m keinen gemeinsamen Teiler haben. Denn die Zahl 0 ist teilbar durch jedes m. Nun ist aber die 0 durch diese Eigenschaft auch unter *allen* ganzen Zahlen charakterisiert. Also sollte man annehmen, daß eine Form f, welche Nullform für jedes $m > 0$ ist, auch Nullform schlechthin ist. Das ist natürlich so nicht unmittelbar einsichtig, denn die Variablenwerte, welche f teilbar durch m machen, werden i.a. mit m variieren. Der Fundamentalsatz behauptet nun:

Ist f Nullform mod m für jedes ganze $m > 0$ und zudem Nullform im reellen Zahlbereich, so ist f rationale Nullform; und umgekehrt (trivial).

Die Forderung, f solle auch Nullform im reellen Zahlbereich sein, ist durchaus einsichtig. Sie verlangt, daß a, b nicht beide negativ sind.

Beweis. Wir setzen wie gesagt, a, b als ganz quadratfrei voraus, und setzen voraus, daß f Nullform mod m für alle $m > 0$ und reelle Nullform ist. Wir verwenden vollständige Induktion nach der absoluten Größe der Koeffizienten a, b, und zwar denken wir uns diese (o.B.d.A.) immer so geordnet: $|a| \leqq |b|$, und schließen dann induktiv in der Rangordnung

$$(1,1);\ (1,2),(2,2);\ (1,3),(2,3),(3,3);\ \ldots$$

für die absoluten Beträge $|a|, |b|$.

Für $|a| = |b| = 1$ stimmt die Behauptung. Denn da f reelle Nullform, ist notwendig a oder $b = +1$, und daher f ersichtlich rationale Nullform.

Sei nun $(|a|, |b|)$ in der Rangordnung höher als $(1, 1)$, und sei angenommen, die Behauptung sei bereits für alle in der Rangordnung vorangehenden (die Nullformvoraussetzungen erfüllenden) Formen bewiesen. □□□

Wir benutzen, daß nach Voraussetzung f sicher Nullform mod b^2 ist:

$$w_0^2 - ax_0^2 - by_0^2 \equiv 0 \bmod b^2, \quad \text{mit} \quad (w_0, x_0, y_0, b) = 1.$$

Dabei ist sicher x_0 prim zu b. Denn wäre p ein gemeinsamer Primteiler, so wäre p^2 in w_0^2, x_0^2 enthalten, ferner in b, also in by_0^2, und wegen der Quadratfreiheit von b also auch in y_0^2, gegen die obige Zusatztatsache. Betrachtet man also die Kongruenz nur mod $|b|$ und dividiert durch die prime Restklasse von x_0, so erhält man eine Lösung u_0 der Kongruenz:

$$a \equiv u_0^2 \bmod |b| \qquad \left(u_0 \equiv \frac{w_0}{x_0} \bmod |b|\right).$$

Dies u_0 kann im absolut-kleinsten Restsystem mod $|b|$ gewählt werden:

$$|u_0| \leqq \frac{|b|}{2}.$$

Wir setzen:

$$u_0^2 - a = bb', \qquad \text{wo also } b' \text{ ganz.}$$

Ist hier $b' = 0$, so ist a Quadrat und f ersichtlich Nullform. Ist aber $b' \neq 0$ (Hauptfall), so ist der oben angewandte Schluß anwendbar, da $\frac{b}{b'} = \left(\frac{u_0}{b'}\right)^2 - \left(\frac{1}{b'}\right)^2$, und es resultiert $(a, b) = (a, b')$. Hierbei ist

$$|b'| = \left|\frac{u_0^2}{b} - \frac{a}{b}\right| \leqq \frac{|b|^2}{4|b|} + \frac{|a|}{|b|} \leqq \frac{|b|}{4} + 1 < |b|, \quad \text{da} \quad |b| > 1.$$

Folglich geht $(a, b') = (b', a)$ in der Rangordnung voran, d.h. $(a, b') \sim 1$ nach Induktionsannahme, also auch $(a, b) \sim 1$, d.h. f rationale Nullform.

Damit ist der Fundamentalsatz durch vollständige Induktion bewiesen.

Weitere Reduktion der Lösung der 1. Hauptfrage.

Durch den Fundamentalsatz wird die Lösung des in der 1. Hauptfrage liegenden rein *algebraischen* Problems auf die Lösung eines *arithmetischen* Problems zurückgeführt, nämlich die Frage, ob

$$f = w^2 - ax^2 - by^2 \equiv 0 \bmod m \qquad \text{mit} \quad (w, x, y, m) = 1$$

lösbar ist. Dies kann man nun nach elementaren arithmetischen Methoden weiter behandeln.

Zunächst sieht man leicht, daß es genügt, für m alle *Primzahlpotenzen* p^ν zugrundezulegen. Denn aus Lösungen für eine Reihe von Primzahlpotenzen läßt sich eine Lösung für ihr Produkt zusammenbauen (und trivialerweise umgekehrt).

Ferner kann man dann zeigen, daß es (bei quadratfreien ganzen a, b) sogar genügt, die Potenzen 2^3 oder 2^4 und p oder p^2 ($p \neq 2$) zugrundezulegen, indem aus einer Lösung für sie nach einem einfachen zahlentheoretischen Schluß Lösungen für die höheren Potenzen konstruiert werden können.

Schließlich kann man dann die Lösbarkeitsbedingungen für diese Potenzen nach der Theorie der quadratischen Reste explizit aufstellen.

Ich will hier nur das Resultat dieser arithmetischen Untersuchung angeben und dann daran weitere Beobachtungen knüpfen.

Sei zunächst $p \neq 2$ und r_p eine primitive Wurzel mod p. Dann lassen sich die Zahlen a, b so darstellen:

$$a \equiv p^\alpha r_p^{\alpha'} \bmod p^{\alpha+1}$$
$$b \equiv p^\beta r_p^{\beta'} \bmod p^{\beta+1}.$$

(Hierzu brauchen a, b nicht einmal quadratfrei, und bei geeignetem Kongruenzbegriff auch nicht einmal ganz normiert zu sein; sind sie ganz quadratfrei, so ist der Modul entweder p oder p^2). Es stellt sich dann heraus, daß f Nullform für alle Potenzen p^ν dann und nur dann ist, wenn die Einheit

$$\left(\frac{a, b}{p}\right) = (-1)^{\frac{p-1}{2}\alpha\beta+\alpha\beta'+\alpha'\beta}$$

den Wert $+1$ hat. Insbesondere ist dies also stets der Fall, wenn $\alpha, \beta = 0$ sind, d.h. es sind von vornherein nur die *endlich vielen* Primteiler p der Koeffizienten a, b kritisch.

Für $p = 2$ lassen sich a, b so darstellen:

$$a \equiv 2^\alpha (-1)^{\alpha'} 5^{\alpha''} \bmod 2^{\alpha+3}$$
$$b \equiv 2^\beta (-1)^{\beta'} 5^{\beta''} \bmod 2^{\beta+3}$$

(Der Modul ist für quadratfreie a, b entweder 2^3 oder 2^4). Und f ist Nullform für alle Potenzen 2^ν dann und nur dann, wenn die Einheit

$$\left(\frac{a, b}{2}\right) = (-1)^{\alpha\beta''+\alpha'\beta'+\alpha''\beta}$$

gleich +1 ist.

Schließlich läßt sich auch noch die Bedingung, daß f reelle Nullform sei, auf diese Form bringen. Stellt man nämlich a, b in der Form

$$\begin{aligned} a &= (-1)^{\alpha} a_0 \\ b &= (-1)^{\beta} b_0 \qquad (a_0, b_0 > 0) \end{aligned}$$

dar, wo also das Positivsein jetzt die Rolle des kongruent 1 Seins des Restfaktors bekommen hat, so lautet die Bedingung so, daß die Einheit

$$\left(\frac{a,b}{p_\infty}\right) = (-1)^{\alpha\beta}$$

den Wert +1 haben muß (p_∞ soll symbolisch die Betrachtung dem Vorzeichen nach andeuten).

So ist also jeder quadratischen Form $f = w^2 - ax^2 - by^2$ und mittelbar also auch jedem Quaternionensystem (a, b) ein System von Einheiten

$$c_p = \left(\frac{a,b}{p}\right) = \pm 1$$

zugeordnet, und zwar für jede Primzahl p eine und zudem noch für das Symbol p_∞ (die Betrachtung dem Vorzeichen nach) eine solche Einheit. Von diesen Einheiten sind von vornherein nur *endlich viele* gleich -1, nämlich höchstens für $2, p_\infty$ und die ungeraden Primteiler p der ganz quadratfrei normierten Koeffizienten.

Dies System von Einheiten c_p entscheidet darüber ob f Nullform, d.h. ob $(a, b) \sim 1$ ist, und zwar so:

$$f \text{ Nullform} \leftrightarrow F \text{ Nullform} \leftrightarrow (a,b) \sim 1 \leftrightarrow$$
$$\leftrightarrow c_p = \left(\frac{a,b}{p}\right) = +1 \quad \text{für } \textit{alle } p.$$

Bei Gauß tritt dieser Satz (in anderer Terminologie – quadr. Restsymbol statt unserer Formeln für das Symbol $c_p = \left(\frac{a,b}{p}\right)$) im Zusammenhang mit dem *quadratischen Reziprozitätsgesetz, seinem* theorema fundamentale auf. Es stellt sich nämlich heraus, daß auf Grund dieses berühmten Gesetzes:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\left(\frac{q-1}{2}\right)} \qquad \text{für verschiedene ungerade Primzahlen } p, q$$

und seiner Ergänzungssätze

$$\left.\begin{array}{rcl}\left(\dfrac{-1}{p}\right) & = & (-1)^{\frac{p-1}{2}} \\ \left(\dfrac{2}{p}\right) & = & (-1)^{\frac{\pm p-1}{4}} \quad (\pm p \equiv 1 \bmod 4)\end{array}\right\} \text{ für ungerade Primzahlen } p$$

zwischen den einzelnen Einheiten $c_p = \left(\frac{a,b}{p}\right)$ eine Abhängigkeit besteht, nämlich

$$\prod_p c_p = \prod_p \left(\frac{a,b}{p}\right) = +1,$$

d.h. die Anzahl der endlich vielen *kritischen* p (p mit Symbolwert -1) ist stets gerade. Daher in dem obigen Fundamentalsatz *eine* Bedingung, z.B. die auf die Vorzeichen bezügliche, entbehrlich.

Wir wollen das eine Hauptgesetz bestätigen. Dazu betrachten wir das Quaternionensystem (p, q), d.h. die Form

$$f = w^2 - px^2 - qy^2$$

für zwei verschiedene ungerade Primzahlen p, q. Die Einheiten sind von vornherein $+1$ außer für $2, p, q$. Für p lauten die Darstellungen:

$$\begin{gathered} p = p^1 \\ q \equiv r_p^{\beta'} \bmod p, \end{gathered}$$

wo β' gerade oder ungerade, je nachdem $\left(\frac{q}{p}\right) = +1$ oder -1.
Also:

$$c_p = \left(\frac{p,q}{p}\right) = (-1)^{\beta'} = \left(\frac{q}{p}\right).$$

Ebenso:

$$c_q = \left(\frac{p,q}{q}\right) = \left(\frac{p}{q}\right).$$

Für 2 lauten die Darstellungen:

$$\begin{aligned} p &\equiv (-1)^{\alpha'} 5^{\alpha''} \bmod 8 \\ q &\equiv (-1)^{\beta'} 5^{\beta''} \bmod 8, \end{aligned}$$

$$c_2 = \left(\frac{p,q}{2}\right) = (-1)^{\alpha'\beta'}.$$

Es kommt also nur auf die Exponenten α', β' an, die bereits durch

$$\begin{aligned} p &\equiv (-1)^{\alpha'} \bmod 4 \\ q &\equiv (-1)^{\beta'} \bmod 4 \end{aligned}$$

charakterisiert sind, und zwar offenbar

$$\begin{aligned} \alpha' &\equiv \frac{p-1}{2} \bmod 2 \\ \beta' &\equiv \frac{q-1}{2} \bmod 2. \end{aligned}$$

Also:

$$c_2 = \left(\frac{p,q}{2}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

In der Tat ist also nach dem Reziprozitätsgesetz $c_2 c_p c_q = 1$.

Entsprechend bestätigt man auf Grund auch der Ergänzungssätze, daß *allgemein* das obige Produkttheorem gilt. Man muß dabei nur beachten, daß wegen der Linearität und Homogenität der Exponenten von -1 in der Definition von $\left(\frac{a,b}{p}\right)$ in den Exponenten von a und b die *Zerlegungssätze* gelten:

$$\left(\frac{a,b_1b_2}{p}\right) = \left(\frac{a,b_1}{p}\right)\left(\frac{a,b_2}{p}\right), \qquad \left(\frac{a_1a_2,b}{p}\right) = \left(\frac{a_1,b}{p}\right)\left(\frac{a_2,b}{p}\right).$$

Dadurch reduziert sich der Beweis auf die Fälle, wo a und b entweder eine ungerade Primzahl q oder die Primzahl 2 oder die Einheit -1 ist. Man hat dann alle wesentlich verschiedenen (7) Kombinationen dieser Fälle in gleicher Weise wie eben durchzugehen.

Das obige Produkttheorem ist hiernach eine einheitliche Formulierung des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze. Es ist zuerst von Hilbert in dieser Form ausgesprochen worden. Gauß hat umgekehrt den aufgedeckten Zusammenhang mit der Theorie der ternären Form $f = w^2 - ax^2 - by^2$ dazu benutzt um einen *Beweis* des Reziprozitätsgesetzes zu geben, das er mit Recht für so grundlegend hielt, daß er dafür 6 auf den verschiedensten Grundlagen aufgebaute Beweise gab.

Lösung der 2. Hauptfrage (Skizze).

Die gewonnenen Einheiten $c_p = \left(\frac{a,b}{p}\right)$ vermitteln ohne weiteres auch die Lösung der 2. Hauptfrage. Es gilt nämlich der Satz:

$$\left.\begin{aligned} (a,b) &= (a',b') \\ \text{d.h.}\quad F &\sim F' \end{aligned}\right\} \leftrightarrow \left(\frac{a,b}{p}\right) = \left(\frac{a',b'}{p}\right) \quad \text{für } \textit{alle } p.$$

Auch das Äquivalenzproblem ist hierdurch auf arithmetischem Wege gelöst. Auf den Beweis kann ich hier nicht im einzelnen eingehen. Ich will nur soviel andeuten. Es genügt zu zeigen, daß unter der angegebenen Bedingung die Formen

$$ax^2 + by^2 - abz^2 \qquad \text{und} \qquad a'x'^2 + b'y'^2 - a'b'z'^2$$

äquivalent sind. Denkt man sich hier für x, y, z die linearen Formen in x', y', z' eingesetzt und setzt $x' = 1$, y', $z' = 0$, so entsteht eine Darstellung von a' durch die erste Form. Man beweist nun zunächst, daß eine solche jedenfalls besteht. Das kommt homogen geschrieben auf eine Relation

$$ax_0^2 + by_0^2 = abz_0^2 + a'u_0^2 \qquad (u_0 \neq 0)$$

hinaus, oder also auf die Existenz einer Hilfszahl h, so daß gleichzeitig

$$ax^2 + by^2 - h\,[\ldots]^2 \qquad \text{und} \qquad abz^2 + a'u^2 - ht^2$$

Nullformen sind. Nun hat man ja nach dem obigen das Kriterium, wann eine ternäre Form Nullform ist (daß ein Koeffizient 1 ist, kann man natürlich stets durch Division der Form durch einen der Koeffizienten erreichen). Man muß dann also nur prüfen, ob man ein h so wählen kann, daß beide Formen gleichzeitig Nullformen sind. Es zeigt sich nun, daß das stets geht. Dazu braucht man den berühmten Dirichletschen Satz von der arithmetischen Progression, daß es in jeder teilerfremden arithmetischen Progression Primzahlen gibt. Die Nullformkriterien führen nämlich auf bestimmte arithmetische Progressionen für h, die zwar Teiler haben, aber nach Abspaltung dieser durch eine Primzahl p erfüllt werden können. Dann stimmen die Nullformkriterien für alle Primzahlen bis auf ev. dies p. Für dieses müssen sie dann auch stimmen nach dem Produktgesetz.

Daß man stets auch noch $u_0 \neq 2$ erreichen kann, zeigt man durch direkte Umformung einer Relation mit $u_0 = 0$ in eine solche mit $u_0 \neq 0$.

Hat man so erst einmal den „Anfang“ der Transformation, indem man a' durch die erste Form dargestellt hat, so kann man die Transformation ohne weiteres so ausbauen, daß eine Form

$$a'x''^2 + b''y''^2 - a'b''z''^2$$

mit einem gewissen b'' entsteht (der letzte Koeffizient regelt sich durch die Invarianz des Diskriminantenkerns bei Transformationen). Diese Form hat

dann auch dieselben Einheiten wie $a'x'^2 + b'y'^2 - a'b'z'^2$, d.h.

$$\left(\frac{a', b''}{p}\right) = \left(\frac{a', b'}{p}\right) \qquad \text{für alle } p,$$

also

$$\left(\frac{a', \frac{b''}{b'}}{p}\right) = 1 \qquad \text{für alle } p,$$

Dann ist aber, wie wir bewiesen haben, $\left(a', \frac{b''}{b'}\right) \sim 1$, also $(a', b'') = (a', b')$, was zu beweisen war. –

Nach diesem Äquivalenzsatz bilden die Einheiten $c_p = \left(\frac{a,b}{p}\right)$ ein *vollständiges Invariantensystem* für die Quaternionensysteme (a, b) oder auch für die quadratischen Formen $F = w^2 - ax^2 - by^2 + abz^2$ bzgl. rationaler Transformation. Dies System gestattet die beiden algebraischen Hauptfragen nach *Nullsystem* (Nullform) und *Identität* (Äquivalenz) zu entscheiden. Zudem vermittelt es eine Übersicht über *alle verschiedenen* Quaternionensysteme (Formenklassen). Diese entsprechen eineindeutig den möglichen Verteilungen von Einheiten $c_p = \pm 1$ auf die „Stellen“ p mit den beiden Einschränkungen:

(1.) nur endlich viele $c_p \neq +1$

(2.) $\prod_p c_p = +1$

Es gilt nämlich in Abrundung der bewiesenen Tatsachen der *Existenzsatz*:
Zu jedem System c_p, das den Bedingungen (1.), (2.) genügt, existiert wirklich ein Quaternionensystem (a, b) mit $c_p = \left(\frac{a,b}{p}\right)$, d.h. (1.) und (2.) sind auch die einzigen Einschränkungen.
Z.B. hat das gewöhnliche Quaternionensystem $(-1, -1)$ die Invarianten $c_2 = -1$, $c_{p_\infty} = -1$, sonst $c_p = +1$.

Weitere Ausblicke.

I. *Theorie der allgemeinen hyperkomplexen Systeme (mit rationalen Koeffizienten).*

Die weiteste Verallgemeinerung des Begriffs der Quaternionensysteme ist so:
Gegeben n hyperkomplexe Einheiten $\varepsilon_1, \ldots, \varepsilon_n$ mit linear-homogenen Multiplikationsregeln

$$\varepsilon_i \varepsilon_j = \sum_{\ell=1}^{n} a_{ij\ell} \varepsilon_\ell$$

Man betrachtet das System $\mathfrak{S}$ der hyperkomplexen Zahlen

$$\xi = x_1\varepsilon_1 + \cdots + x_n\varepsilon_n.$$

Ganz willkürlich wird man aber dabei die $a_{ij\ell}$, das Analogon der obigen a, b, nicht wählen, sondern jedenfalls so, daß die Multiplikation *assoziativ* ist:

$$(\varepsilon_i\varepsilon_j)\varepsilon_k = \varepsilon_i(\varepsilon_j\varepsilon_k).$$

Das gibt eine Reihe von bilinearen Bedingungsgleichungen zwischen den $a_{ij\ell}$, die bei den Quaternionen erfüllt sind (dort sind die $a_{ij\ell} = a, b, 0, \pm 1$). Außerdem ist es vernünftig sich auf Systeme $\mathfrak{S}$ zu beschränken, für die eine gewisse Determinante aus den $a_{ij\ell}$, die sog. *Diskriminante* des Systems, nicht 0 ist; auch das ist bei den Quaternionensystemen erfüllt.

Es gelten dann ganz entsprechende Tatsachen. Wieder existiert ein arithmetisch definiertes Invariantensystem in Zuordnung zu den einzelnen Primzahlen p (inkl. p_∞), nur mit 2 Unterschieden gegen obigen Spezialfall:

a.) Für jedes p hat man eine feste Zahl $c_p^{(1)}, \ldots c_p^{(r)}$ von Einheiten.

b.) Diese Einheiten sind jetzt allgemeiner Einheitswurzeln fester Exponenten $m_1, \ldots m_r$. Wieder wird das *Identitätsproblem* gelöst durch das Übereinstimmen *aller* dieser Einheiten. Und wieder bestehen die beiden *Einschränkungen*; und zwar als *einzige*:

(1.) für jedes ϱ sind nur endlich viele $c_p^{(\varrho)} \neq 1$

(2.) für jedes ϱ ist $\prod_p c_p^{(\varrho)} = 1$.

Die letztere ist die einheitliche Formulierung der höheren Reziprozitätsgesetze. Man kann dann auch von hier aus, analog zu Gauß, zu einem *Beweis* dieser höheren Reziprozitätsgesetze kommen, der sich vor allen anderen durch seine Natürlichkeit und gedankliche Einfachheit auszeichnet.

II. Allgemeine Theorie der quadratischen Formen.

Man kann die speziellen Erkenntnisse über ternäre und quaternäre Formen ausnutzen, um allgemein über das Äquivalenzproblem der quadratischen Formen mit rationalen Koeffizienten von beliebig vielen Variablen zu entscheiden.

Eine solche ist ein Ausdruck: [1]

$$F(x_i) = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{i<k} a_{ik}x_ix_k = \sum_{i,k=1}^{n} a_{ik}x_ix_k \qquad (a_{ik} = a_{ki})$$

1. Index i unklar

Vernünftigerweise nimmt man die Form nicht-singulär an, d.h. ihre *Diskriminante*

$$D = |a_{ik}| \neq 0.$$

Man kann elementar (rational) f auf eine *reine* Form

$$f = \sum_{i=1}^{n} a_i x_i^2$$

transformieren, wie sie ja auch in unseren obigen Überlegungen nur vorkommen.

Invarianten sind dann:

a.) die Variablenzahl n

b.) der quadratische Kern d der Diskriminante D.

c.) der Trägheitsindex I, d.h. die Anzahl der negativen a_i

d.) ein System von Einheiten $C_p = \pm 1$ mit denselben beiden Einschränkungen wie in unseren obigen Spezialfällen (Endlichkeits- und Produktbedingung). Und zwar ist explizit:

$$C_p = \prod_{i \leqq k} \left(\frac{a_i, a_k}{p} \right).$$

Bei unseren obigen Formen F reduziert sich das leicht auf unsere obigen Einheiten c_p; die Invariante n ist natürlich da fest $= 4$, ferner d fest $= 1$, und I wird da schon völlig durch c_{p_∞} beschrieben.

Das Fundamentaltheorem besagt nun, daß die genannten Invarianten ein *vollständiges Invariantensystem* für rationale Äquivalenz bilden. Wieder ist also ein rein algebraisches Problem dadurch arithmetisch gelöst. Ferner existiert wieder zu jedem Invariantensystem auch wirklich eine Formenklasse (allerdings muß man dabei noch einige weitere Einschränkungen berücksichtigen, nämlich Bindungen zwischen d, I und C_{p_∞}).

Die Zurückführung des Äquivalenzproblems auf die einzelnen „Stellen“ p spricht sich inhaltlich in dem Fundamentalprinzip aus:

Zwei quadratische Formen F und F' sind rational äquivalent dann und nur dann, wenn sie mod m äquivalent sind für jedes $m > 0$ und zudem reell-äquivalent.

Mithilfe der Invarianten kann man wieder speziell auch die Nullformfrage allgemein lösen, d.h. Kriterien dafür angeben, wann eine Form F Nullform ist. Und noch allgemeiner auch Kriterien dafür, ob eine rationale Zahl a rational durch F darstellbar ist. In beiden Fällen zerfallen die Kriterien wieder in solche für die einzelnen p, und diese sind gerade die Kriterien für die betr. Frage mod p^ν, sodaß auch hier wieder das Fundamentalprinzip gilt:

Eine quadratische Form F stellt eine rationale Zahl a (im Falle $a = 0$ nicht-identisch) dann und nur dann dar, wenn dies mod m für jedes $m > 0$ und reell der Fall ist.

Diese Theorie der quadratischen Formen erledigt zwar eine große Reihe von Fragestellungen, ist aber doch noch nicht tief genug, um die von Gauß in den Mittelpunkt der Theorie gestellten Fragen anzugreifen. Diese Fragen legen nämlich anstatt des Bereichs *aller* rationalen Zahlen nur den Bereich aller *ganzen* rationalen Zahlen zugrunde, und sogar dementsprechend nach *ganzzahliger Äquivalenz*, *ganzzahligen Darstellbarkeit*, also z.B. die klassischen Fragen nach der Darstellbarkeit einer ganzen rationalen Zahl $a > 0$ als Summe von $2, 3, 4, \ldots$ Quadraten. Im Bereich der ganzzahligen Formen liefert unsere Betrachtung nur eine verhältnismäßig *grobe* Klasseneinteilung. Diese läßt sich mit den angegebenen Hilfsmitteln noch etwas verfeinern, indem man statt der *rationalen Äquivalenz* die *quasiganze Äquivalenz* fordert. Hierfür spricht sich das Fundamentaltheorem so aus:

Nat. Äquiv.	$\leftrightarrow$	Äquivalenz nach jedem $m > 0$ und reelle Äquiv.
Quasiganze Äquiv.	$\leftrightarrow$	ganze Äquiv. nach jedem $m > 0$ und reelle Äquiv.

(beliebig normierbare [2] Nenner) ([...] Geschlechtes)

Weiter kommt man jedoch mit dieser Methode *nicht*. Das Problem der *ganzzahligen* Äquivalenz gestattet *nicht* mehr eine Aufspaltung nach den einzelnen Stellen p. Dies liefert nur *notwendige* Bedingungen, nicht immer hinreichend. Entsprechend für die *Darstellbarkeitsprobleme*.

Die Theorie der Quaternionen öffnet aber auch den Weg zu solchen ganzz. Problemen. Z.B. liefert sie sehr elegant den Satz, daß jede positive ganze Zahl sich als Summe von vier Quadratzahlen darstellen läßt.

1.17 Königsberg 1936

Ein Hauptsatz über quadratische Formen mit rationalen Koeffizienten

Vortrag in Königsberg, 13. May 1936.

Eine für die Theorie der quadratischen Formen mit rationalen Koeffizienten und überhaupt für einen großen Fragenkomplex aus der Zahlentheorie grundlegende Frage ist, unter welchen Bedingungen eine ternäre quadratische Form der Gestalt

$$f_{a,b} \;=\; f_{a,b}(x,\,y,\,z) \;=\; x^2 - ay^2 - bz^2\,,$$

wo $a,\,b$ von Null verschiedene rationale Zahlen sind, *rationale Nullform* ist, d. h. die Null mit nicht sämtlich verschwindenden rationalen Werten von $x,\,y,\,z$ darstellt. Die Antwort wurde zuerst von Legendre gegeben, und zwar mittels eines von Lagrange stammenden Reduktionsverfahrens.

Da man etwaige quadratische Faktoren der rationalen Zahlen $a,\,b$ in die Variablen $y,\,z$ ziehen kann, ist es keine Beschränkung, wenn man $a,\,b$ *als ganze quadratfreie* Zahlen voraussetzt. Legendre führt überdies noch die einschränkende Voraussetzung ein, daß *a und b teilerfremd* seien. Sein Resultat lautet dann:

$f_{a,b}$ ist rationale Nullform dann und nur dann, wenn

(1.) *a und b nicht beide negativ sind,*

und

(2.) *a qu. Rest* mod. *b und b qu. Rest* mod. *a ist.*

Die Bedingung **(2.)** kann in bekannter Weise auch aufgespalten werden in:

(2'.) $\left(\frac{a}{p}\right) = 1$ *für alle ungeraden Primzahlen* $p \mid b$

und

$\left(\frac{b}{p}\right) = 1$ *für alle ungeraden Primzahlen* $p \mid a$.

Man sieht leicht, daß diese Bedingungen *notwendig* sind. **(1.)** ist notwendig, weil für negative $a,\,b$ eine Summe von drei nicht sämtlich verschwindenden positiven Zahlen vorliegt. Um **(2.)** als notwendig zu erkennen, bemerken wir, daß in einer rationalen Nulldarstellung $x,\,y,\,z$ als ganze teilerfremde Zahlen angenommen werden dürfen (*primitive Nulldarstellung*). Ist dann $p \mid b$,

so ist notwendig $p \nmid y$, weil aus $p \mid y$ folgte $p \mid x$, $p^2 \mid x^2 - ay^2$, $p^2 \mid bz^2$, also wegen der Quadratfreiheit von b auch $p \mid z$. Somit folgt

$$x^2 - ay^2 \equiv 0 \text{ mod. } p \qquad \text{mit} \quad y \not\equiv 0 \text{ mod. } p,$$

und daraus

$$a \equiv u^2 \text{ mod. } p \qquad (\text{mit } u \text{ aus } yu \equiv x \mod p).$$

Daß die Bedingungen *hinreichend* sind, liegt tiefer. Ich will hier eine moderne Umgestaltung des klassischen Beweises von Lagrange–Legendre geben, die zugleich tiefer in die Bedeutung des Legendreschen Resultats hineinblicken läßt.

Die obigen notwendigen Bedingungen kommen dadurch zustande, daß man die Gleichung $x^2 - ay^2 - bz^2 = 0$ in rationalen (ohne Einschränkung ganzen teilerfremden) Zahlen einerseits als Gleichung in reellen Zahlen, andererseits als Kongruenz nach gewissen Primzahlen als Modul auffaßt. Führt man diesen Gedanken systematisch durch, so wird man darauf geführt, nicht nur *gewisse* Primzahlen (die ungeraden Primteiler von a und b), sondern gleich *alle* Primzahlen und weiter auch alle Primzahlpotenzen als Betrachtungsmoduln einzuführen (eigentlich auch alle zusammengesetzten ganzen Zahlen, aber die Kongruenzen nach ihnen lassen sich ja in bekannter Weise auf Kongruenzen nach den darinsteckenden Primzahlpotenzen zurückführen).

Wir wollen dementsprechend die folgenden Begriffe einführen (dabei a, b ganze Zahlen, aber nicht notwendig quadratfrei):

$f_{a,b}$ heißt reelle Nullform, wenn die Gleichung $x^2 - ay^2 - bz^2 = 0$ durch reelle nicht sämtlich verschwindende x, y, z lösbar ist.

$f_{a,b}$ heißt Nullform für eine Primzahl p, wenn die Gleichung $x^2 - ay^2 - bz^2 = 0$ durch ganze für p teilerfremde x, y, z lösbar ist.

Die Kernaussage des Legendreschen Satzes ist dann die folgende grundlegende Tatsache, die ich in den Mittelpunkt meines heutigen Vortrages stellen möchte:

Hauptsatz. *Damit $f_{a,b}$ rationale Nullform ist, ist notwendig und hinreichend, daß $f_{a,b}$ Nullform für jede Primzahl p und reelle Nullform ist.*

Daß die Bedingungen notwendig sind, ist nach dem Gesagten klar. Ich werde hier ausführlich beweisen, daß sie hinreichend sind. Damit ist dann zunächst noch nicht das explizite Kriterium von Legendre bewiesen, sondern erst eine Vorstufe dazu. Diese Vorstufe stellt aber eine wesentliche Reduktion

des Problems dar. Denn die Untersuchung, wann $f_{a,b}$ Nullform für ein einzelnes p ist, ist erheblich einfacher als die ursprüngliche Frage, sie kann mit den Hilfsmitteln der Theorie der quadratischen Reste leicht erledigt werden. Und wann $f_{a,b}$ reelle Nullform ist, ist schon oben in trivialer Weise explizit entschieden.

Die genannte Vorstufe ist aber auch an sich von hohem theoretischem Interesse. Sie ist der einfachste Fall eines die gesamte moderne Zahlentheorie beherrschenden Prinzips, nämlich der Zurückführung von Eigenschaften im *Großen* (für rationale Zahlen) auf Eigenschaften im *Kleinen* oder *lokale* Eigenschaften (Verhalten als Kongruenz nach den einzelnen Primzahlpotenzen, Verhalten im Reellen), ganz analog wie man in der komplexen Funktionentheorie das Prinzip hat: Eine Funktion ist dann und nur dann rational, wenn sie an jeder endlichen Stelle und im Unendlichen rationalen Charakter hat. Die einzelnen rationalen Primzahlen entsprechen den endlichen Stellen $z = a$ der komplexen Ebene (die zugehörigen Linearfaktoren $z - a$ sind die Primfunktionen, aus denen sich die rationalen Funktionen zusammensetzen), und das Reelle entspricht der unendlichen Stelle (auf der Kugel). Aus diesem auch noch tiefer verfolgbaren Analogiegrunde wollen wir für *reelle Nullform* auch die formale Ausdrucksweise *Nullform für* p_∞ einführen, und wollen die Tatsache, daß eine rationale Zahl a das Vorzeichen ± 1 hat, auch formal als Kongruenz $a \equiv \pm 1 \bmod. p_\infty$ schreiben.

Übrigens ist der hier behandelte Spezialfall des genannten zahlentheoretischen Prinzips der einzige bekannte, wo der Beweis ohne analytische Hilfsmittel, mit elementar–zahlentheoretischen Mitteln durchführbar ist; daher sein besonderes Interesse.

Dem Beweis des Hauptsatzes stellen wir einige Vorbetrachtungen voran.

Wir wollen zwei Formen $f_{a,b}$ und $f_{c,d}$ *äquivalent (im engeren Sinne)* nennen, wenn $f_{a,b}(x, y, z)$ durch eine lineare Substitution

$$\begin{array}{rcccccc} x & = & a_{11}\overline{x} & + & a_{12}\overline{y} & + & a_{13}\overline{z} \\ y & = & a_{21}\overline{x} & + & a_{22}\overline{y} & + & a_{23}\overline{z} \\ z & = & a_{31}\overline{x} & + & a_{32}\overline{y} & + & a_{33}\overline{z} \end{array}$$

mit rationalen Koeffizienten und nicht verschwindender Determinante, die also in der gleichen Form umkehrbar ist, in $f_{c,d}(\overline{x}, \overline{y}, \overline{z})$ übergeht:

$$f_{a,b}(x, y, z) \;=\; f_{c,d}(\overline{x}, \overline{y}, \overline{z})\,, \quad \text{kurz} \quad f_{a,b} \simeq f_{c,d}\,.$$

$f_{a,b}$ und $f_{c,d}$ sollen *äquivalent (im weiteren Sinne)* heißen, wenn ebenso mit einem unbestimmten rationalen Faktor r $(\neq 0)$ gilt:

$$f_{a,b}(x,\, y,\, z) \;=\; r \cdot f_{c,d}(\overline{x},\, \overline{y},\, \overline{z})\,, \quad \text{kurz} \quad f_{a,b} \sim f_{c,d}\,.$$

Dann ist zunächst ohne weiteres klar:

Ist $f_{a,b} \sim f_{c,d}$, so sind $f_{a,b}$ und $f_{c,d}$ gleichzeitig rationale Nullformen oder nicht.

Ferner auch:

Ist $f_{a,b} \sim f_{c,d}$, so sind $f_{a,b}$ und $f_{c,d}$ gleichzeitig reelle Nullformen oder nicht. Denn die rationalen (reellen) $x,\, y,\, z \neq 0,\, 0,\, 0$ entsprechen bei der Substitution eineindeutig den rationalen (reellen) $\overline{x},\, \overline{y},\, \overline{z} \neq 0,\, 0,\, 0$.

Es gilt aber auch (dabei $a,\, b$ ganz vorausgesetzt):

Ist $f_{a,b} \sim f_{c,d}$, so sind $f_{a,b}$ und $f_{c,d}$ gleichzeitig Nullformen für p oder nicht.

Sei nämlich $f_{a,b}(x,\, y,\, z) \equiv 0 \bmod p^n$ mit $(x,\, y,\, z,\, p\,) = 1$, so ist jedenfalls

$$r \cdot f_{c,d}(\overline{x},\, \overline{y},\, \overline{z}) \equiv 0 \bmod p^n\,,$$

aber dabei sind $\overline{x},\, \overline{y},\, \overline{z}$ möglicherweise gebrochen. Sei nun die Transformation kurz mit $(x,\, y,\, z) = A\,(\overline{x},\, \overline{y},\, \overline{z})$ bezeichnet, ihre Umkehrung entsprechend mit $(\overline{x},\, \overline{y},\, \overline{z}) = \overline{A}\,(x,\, y,\, z)$, und seien $g,\, \overline{g}$ die Generalnenner der Transformationskoeffizienten von $A,\, \overline{A}$. Dann sind

$$\overline{gx},\, \overline{gy},\, \overline{gz} \;=\; \overline{g}\,\overline{A}\,(x,\, y,\, z)$$

ganz; sei p^δ die ihnen gemeinsame Potenz von p, also

$$\overline{gx},\, \overline{gy},\, \overline{gz} \;=\; p^\delta x',\, p^\delta y',\, p^\delta z'\,, \quad \text{mit} \quad (x',\, y',\, z',\, p\,) = 1\,.$$

Dann hat man

$$f_{a,b}(x,\, y,\, z) \;=\; r \cdot f_{c,d}(\overline{x},\, \overline{y},\, \overline{z}) \;=\; r\,\frac{p^{2\delta}}{\overline{g}^2}\, f_{c,d}(x',\, y',\, z'\,) \equiv 0 \bmod p^n.$$

Wegen $g\,\overline{g}(x,\, y,\, z) = g\,A\,(\overline{g}(\overline{x},\, \overline{y},\, \overline{z}))$ ist dabei $p^\delta \mid g\overline{g}$, und daher folgt aus der genannten Kongruenz durch Multiplikation mit der ganzen Zahl $g^2\overline{g}^2 p^{-2\delta}$ erst recht $rg^2 f_{c,d}(x',\, y',\, z'\,) \equiv 0 \bmod p^n$. Bezeichnen also $p^\varrho,\, p^\gamma$ die in $r,\, g$ steckenden Potenzen von p, so ergibt sich, jedenfalls soweit $n > h = \varrho + 2\gamma$ ist,

$$f_{c,d}(x',\, y',\, z'\,) \equiv 0 \bmod p^{n-h} \quad \text{mit} \quad (x',\, y',\, z'\,p\,) = 1\,.$$

Da h fest ist (d. h. von n und damit von x, y, z unabhängig), durchläuft $n-h$ alle positiven Exponenten, wenn n alle Exponenten $> h$ durchläuft. Daher ist dann $f_{c,d}$ in der Tat Nullform für p. Wegen der Symmetrie kann natürlich auch rückwärts von $f_{c,d}$ auf $f_{a,b}$ geschlossen werden.

Wir haben damit bewiesen:

Hilfssatz 1. *Ist $f_{a,b} \sim f_{c,d}$, so sind $f_{a,b}$ und $f_{c,d}$ gleichzeitig rationale Nullform, reelle Nullform, Nullform für p, oder nicht.*

Bemerkung. Der Beweis für p wird hier deshalb formal komplizierter als der Beweis für rationale und reelle Zahlen, weil die Restklassen mod. p^n (für $n > 1$) nur einen *Ring* bilden, während die rationalen Zahlen und die reellen Zahlen *Körper* bilden. Nun hat aber Hensel erkannt, daß sich das Studium des Verhaltens der rationalen Zahlen für alle Potenzen p^n einer festen Primzahl p als Modul durch einen Erweiterungskörper R_p des rationalen Zahlkörpers R beschreiben läßt, den Körper der sogen. *p–adischen Zahlen*. Diese Körper R_p treten gleichberechtigt zur Seite der Erweiterung des Körpers R zum Körper der reellen Zahlen, der in diesem Zusammenhang mit R_{p_∞} bezeichnet sei. Nullform für p bedeutet, wie sich zeigt, gerade Nullform im Körper R_p, ebenso wie reelle Nullform bedeutet Nullform im Körper R_{p_∞}. Auf dieser Grundlage wird also der Beweis für p von derselben formalen Einfachheit wie für die rationalen und reellen Zahlen. Das gilt auch für die gesamte in diesem Vortrag behandelte Theorie: Ihre endgültige und glatte Form erhält sie erst durch Einführung der einzelnen p–adischen Zahlkörper R_p neben dem reellen Zahlkörper R_{p_∞}. Ich wollte jedoch hier die Theorie der p–adischen Zahlen nicht als bekannt voraussetzen.

Wir beweisen weiter:

Hilfssatz 2. *Ist die rationale Zahl $c \neq 0$ in der Form*

$$c \;=\; u^2 - av^2$$

rational darstellbar, so gilt

$$f_{a,b} \sim f_{a,bc}\,.$$

Denn die Transformation

$$\begin{array}{rcl} x &=& u\cdot\overline{x} \;+\; av\cdot\overline{y} \\ y &=& v\cdot\overline{x} \;+\; u\cdot\overline{y} \\ z &=& c\cdot\overline{z} \end{array}$$

mit der Determinante $(u^2 - av^2)c = c^2 \neq 0$

liefert ersichtlich

$$f_{a,b}(x,\,y,\,z) \;=\; x^2 - ay^2 - bz^2 \;=\; c\overline{x}^2 - ac\overline{y}^2 - bc^2\overline{z}^2 \;=\; c\cdot f_{a,bc}(\overline{x},\,\overline{y},\,\overline{z})\,.$$

Wir können Hilfssatz 2 auch in der Form aussprechen:
Es ist

$$f_{a,b} \sim f_{a,b'} ,$$

wenn bb' *in der Form* $u^2 - av^2$ *rational darstellbar ist.*
Denn dann ist auch

$$\frac{b'}{b} \;=\; \left(\frac{u}{b}\right)^2 - a\left(\frac{v}{b}\right)^2 \;=\; \overline{u}^2 - a\,\overline{v}^2 .$$

Für zwei Formen $f_{a,b}$ und $f_{a,b'}$ mit $bb' = u^2 - av^2$ können wir also sagen, daß beide gleichzeitig rationale Nullform, reelle Nullform, Nullform für p sind, oder nicht. In dieser Form werden wir die Hilfssätze anwenden.

Beweis des Hauptsatzes.
Voraussetzung: $f_{a,b}$ ist Nullform für jedes p und für p_∞ .
Behauptung: $f_{a,b}$ ist rationale Nullform.

Dabei seien, wie gesagt, a, b als ganze rationale Zahlen vorausgesetzt; die Quadratfreiheit soll aus technischen Gründen für den Beweis nicht gefordert werden.

Der Satz ist richtig für die kleinsten Absolutwerte der Koeffizienten:

$$|a| \;=\; 1 , \qquad |b| \;=\; 1 .$$

Denn von den vier Formen $x^2 \pm y^2 \pm z^2$ wird $x^2 + y^2 + z^2$ durch die Voraussetzung für p_∞ ausgeschlossen, die drei übrigen sind ersichtlich rationale Nullformen.

Sei demgemäß $f_{a,b}$ jetzt eine Form mit $|a| > 1$ oder $|b| > 1$, und sei angenommen, der Satz sei bereits bewiesen für alle Formen $f_{c,d}$, für die die Absolutwerte der Koeffizienten kleiner sind, in dem genaueren Sinne, daß

$$|c| \le |a| , \qquad |d| < |b|$$

bei geeigneter Reihenfolge von a, b und c, d ist. Wir zeigen dann, daß der Satz auch für $f_{a,b}$ gilt. Dann folgt seine Allgemeingültigkeit durch vollständige Induktion. Dies ist der Kern des auch von Legendre benutzten Lagrangeschen Reduktionsverfahrens.

Sei dazu etwa

$$1 \le |a| \le |b| , \quad \text{also dann sicher} \quad |b| > 1 .$$

1.) Ist a ein rationales Quadrat, $a = u^2$, so ist $f_{a,b}$ trivialerweise rationale Nullform:

$$u^2 - a \cdot 1^2 - b \cdot 0^2 \;=\; 0\,.$$

2.) Ist b nicht quadratfrei, $b = g^2 b'$ mit $|g| > 1$, so ist ersichtlich

$$f_{a,b'} \simeq f_{a,b} \quad \text{und} \quad |a| = |a|\,, \quad |b'| < |b|\,.$$

Daher hat man das Schlußschema:

$$\begin{array}{ccc} \text{Vor. für } f_{a,b} & & \text{Beh. für } f_{a,b} \\ \downarrow \text{(Hilfss. 1)} & & \uparrow \text{(Hilfss. 1)} \\ \text{Vor. für } f_{a,b'} & \underset{\text{(Ind. Ann.)}}{\longrightarrow} & \text{Beh. für } f_{a,b'} \end{array}$$

$$\begin{array}{ccc} \text{Vor. für } f_{a,b} & & \text{Beh. für } f_{a,b} \\ \Big\downarrow \text{(Hilfss. 1)} & & \Big\uparrow \text{(Hilfss. 1)} \\ \text{Vor. für } f_{a,b'} & \underset{\text{(Ind. Ann.)}}{\longrightarrow} & \text{Beh. für } f_{a,b'} \end{array}$$

3.) Ist a kein rationales Quadrat und b quadratfrei, so konstruieren wir eine ganze Zahl $b' \neq 0$ mit den beiden Eigenschaften:

(1.) $bb' = u^2 - a = u^2 - a \cdot 1^2$ mit (ganzem) rationalem u,

(2.) $|b'| < |b|$.

Dann ist nach Hilfssatz 2

$$f_{a,b'} \sim f_{a,b} \quad \text{und dabei wieder} \quad |a| = |a|\,,\ |b'| < |b|\,,$$

und also hat man nach Hilfssatz 1 und Induktionsannahme wieder genau das obige Schlußschema.

Um b' zu konstruieren, nutzen wir die Voraussetzung für die Primzahlen $p_i \mid b$ aus, und zwar die Nullformeigenschaft mod. p_i^2:

$$x_i^2 - a y_i^2 - b z_i^2 \;\equiv\; 0 \bmod p_i^2\,, \quad (x_i,\, y_i,\, z_i) = 1\,.$$

Dabei ist dann notwendig nach einem ganz analogen Schluß wie oben in der Einleitung $y_i \not\equiv 0 \bmod p_i$, und man hat daher

$$a \equiv u_i^2 \bmod p_i \quad (\text{mit } u_i \text{ aus } y_i u_i \equiv x_i \bmod p_i\,).$$

Durch Zusammensetzung dieser Kongruenzlösungen u_i für die sämtlichen Primteiler p_i des quadratfreien $|b| = p_1 \dots p_r$ ergibt sich eine Lösung u von

$$a \equiv u^2 \text{ mod. } |b| \,,$$

und diese kann im absolut–kleinsten Restsystem mod. $|b|$ gewählt werden:

$$|u| \leq \frac{|b|}{2} \,.$$

Dann hat man also einerseits

$$u^2 - a \;=\; bb' \,, \quad b' \quad \text{ganz}, \quad b' \neq 0 \quad (\text{da } a \text{ kein rat. Quadrat}) \,,$$

andererseits

$$|b'| \;=\; |\frac{u^2 - a}{b}| < |\frac{u^2}{b}| + |\frac{a}{b}| < \frac{|b|}{4} + 1 < |b| \quad (\text{da } |b| > 1) \,,$$

d. h. die angeführten Eigenschaften (1.) und (2.).

Das vollendet den Beweis des Hauptsatzes.

Im folgenden will ich ohne Beweis noch eine Reihe von weiteren Tatsachen anführen, die teils die explizite Legendresche Formulierung des Nullformkriteriums ergeben, teils die Bedeutung des ganzen Fragenkomplexes beleuchten sollen.

Durch den Hauptsatz ist, wie gesagt, die Bestimmung des rationalen Nullformcharakters von $f_{a,b}$ zurückgeführt auf die Bestimmung des Nullformcharakters für die einzelnen p. Dieser hängt nur von dem Kongruenzverhalten von a und b nach Potenzen von p als Modul ab, und zwar, wie sich genauer zeigt, nicht nach beliebig hohen Potenzen, sondern nur nach den Potenzen

$$\begin{array}{llll} p^{\alpha+1} & \text{und} & p^{\beta+1} & \text{für ungerade Primzahlen } p \,, \\ 2^{\alpha+3} & \text{und} & 2^{\beta+3} & \text{für} \quad p = 2 \,, \end{array}$$

wo α und β die genauen Exponenten bezeichnen, zu denen p in a und b aufgeht. Dementsprechend kommt es auf die folgenden eindeutigen Darstellungen von a und b nach diesen p–Potenzen als Moduln an:

a.) *p ungerade Primzahl; w primitive Wurzel mod. p.*

$$\begin{aligned} a &\equiv p^{\alpha} w^{\alpha'} \text{ mod. } p^{\alpha+1}\,; \quad \alpha \text{ ganz}\,, \quad \alpha' \text{ mod. } p-1\,, \\ b &\equiv p^{\beta} w^{\beta'} \text{ mod. } p^{\beta+1}\,; \quad \beta \text{ ganz}\,, \quad \beta' \text{ mod. } p-1\,. \end{aligned}$$

b.) $p = 2$.

$$\begin{aligned} a &\equiv 2^{\alpha}(-1)^{\alpha'} 5^{\alpha''}\,; \quad \alpha \text{ ganz}\,, \quad \alpha', \alpha'' \text{ mod. } 2\,, \\ b &\equiv 2^{\beta}(-1)^{\beta'} 5^{\beta''}\,; \quad \beta \text{ ganz}\,, \quad \beta', \beta'' \text{ mod. } 2\,. \end{aligned}$$

c.) $p = p_{\infty}$.

$$\begin{aligned} a &\equiv (-1)^{\alpha}\,; \quad \alpha \text{ mod. } 2\,, \\ b &\equiv (-1)^{\beta}\,; \quad \beta \text{ mod. } 2\,. \end{aligned}$$

Es zeigt sich dann genauer, daß der Nullformcharakter für p nur von dem Kongruenzwert mod. 2 der Exponenten in diesen eindeutigen Basisdarstellungen abhängt (entsprechend der Tatsache, daß es auf a und b nur bis auf quadratische Faktoren ankommt), und daß er in folgender Form gegeben ist:

$$f_{a,b} \quad \text{Nullform für } p \longleftrightarrow \left(\frac{a,\, b}{p}\right) = 1\,,$$

wo $\left(\text{—}\right)$, das berühmte Hilbertsche (Normenrest–) Symbol, in folgender Weise explizit definiert ist:

a.) $\left(\frac{a,b}{p}\right) = (-1)^{\frac{p-1}{2}\alpha\beta+\alpha'\beta+\alpha\beta'}$

b.) $\left(\frac{a,b}{2}\right) = (-1)^{\alpha\beta''+\alpha'\beta'+\alpha''\beta}$

c.) $\left(\frac{a,b}{p_{\infty}}\right) = (-1)^{\alpha\beta}$.

Der Beweis für dieses explizite Nullformkriterium beruht auf der Theorie der quadratischen Reste.

Das Hilbertsche Symbol hat, wie man leicht aus seiner Definition abliest, die folgenden Eigenschaften:

$$\left(\frac{a,\, b_1 b_2}{p}\right) = \left(\frac{a,\, b_1}{p}\right)\left(\frac{a,\, b_2}{p}\right), \quad \left(\frac{a_1 a_2,\, b}{p}\right) = \left(\frac{a_1,\, b}{p}\right)\left(\frac{a_2,\, b}{p}\right)$$

$$\left(\frac{a,\, b}{p}\right) = \left(\frac{b,\, a}{p}\right),$$

ferner

$$\left(\frac{a,\,b}{p}\right) = 1 \qquad \text{stets, wenn } p \text{ eine ungerade Primzahl ist, die nicht in } a \text{ und } b \text{ aufgeht (also } = -1 \text{ höchstens für endlich viele } p\text{)},$$

$$\left(\frac{a,\,b}{p}\right) = \left(\frac{a}{p}\right), \qquad \text{wenn } p \text{ eine ungerade Primzahl ist, die nicht in } a \text{ aufgeht; allgemeiner gilt dasselbe, wenn } p \text{ links oben durch eine genau durch } p^1 \text{ teilbare Zahl ersetzt wird},$$

$$\left(\frac{a,\,-1}{2}\right) = (-1)^{\frac{a-1}{2}}, \qquad \text{wenn 2 nicht in } a \text{ aufgeht},$$

$$\left(\frac{a,\,2}{2}\right) = (-1)^{\frac{a^2-1}{8}}, \qquad \text{wenn 2 nicht in } a \text{ aufgeht},$$

$$\left(\frac{a,\,b}{2}\right) = (-1)^{\frac{a-1}{2}\,\frac{b-1}{2}}, \qquad \text{wenn 2 nicht in } a \text{ und } b \text{ aufgeht}.$$

Aus allen diesen Eigenschaften ergibt sich nun (durch Zerlegung von a und b in Faktoren -1, 2 und ungerade p) nach dem quadratischen Reziprozitätsgesetz und seinen beiden Ergänzungssätzen die grundlegende *Hilbertsche Produktformel:*

$$\prod_p \left(\frac{a,\,b}{p}\right) = 1, \qquad \text{für beliebige rationale } a,\, b \neq 0,$$

wo p alle Primzahlen und die unendliche Stelle p_∞ durchläuft. Diese Produktformel kann geradezu als eine einheitliche und elegante Zusammenfassung des quadratischen Reziprozitätsgesetzes und seiner beiden Ergänzungssätze aufgefaßt werden. Sie sagt aus, daß die nach dem schon vorher Gesagten jedenfalls endliche Anzahl der p, für die das Hilbertsche Symbol (mit festen a, b) den Wert -1 hat, stets eine gerade Zahl ist. Sie kann auch als ein zahlentheoretisches Analogon zu dem bekannten Residuensatz der Funktionentheorie angesehen werden, der aussagt, daß ein rationales Differential nur an endlich vielen Stellen der komplexen Zahlenkugel von 0 verschiedene Residuen hat, und daß deren Summe stets 0 ist.

Nach unserem Hauptsatz ist nun $f_{a,b}$ dann und nur dann rationale Nullform, wenn

$$\left(\frac{a,\, b}{p}\right) \;=\; 1 \quad \text{für alle } p$$

ist. Nach der Produktformel kann dabei ein p, etwa $p = p_\infty$ oder besser $p = 2$ außer Acht gelassen werden. Ferner können jedesmal auch alle diejenigen unendlichvielen ungeraden p außer Acht gelassen werden, die nicht in a oder b aufgehen. Es bleiben dann nur noch p_∞ und die ungeraden Primteiler von a und b zu betrachten. So ergibt sich die oben angeführte Legendresche explizite Formulierung des rationalen Nullformkriteriums:

p_∞ ergibt die Bedingung: a und b nicht beide negativ;

die ungeraden $p \mid a$ ergeben: $\left(\frac{b}{p}\right) = 1$, also b qu. Rest mod. a;

die ungeraden $p \mid b$ ergeben: $\left(\frac{a}{p}\right) = 1$, also a qu. Rest mod. b.

Dabei sind die Legendreschen Voraussetzungen gemacht:
a und b quadratfrei und teilerfremd.

Die Symbole $\left(\frac{a,b}{p}\right)$ für die einzelnen p sind nach Hilfssatz 1 Invarianten gegen rationale Äquivalenz im weiteren Sinne der Form $f_{a,b}$. Es läßt sich nun durch einen ziemlich tiefliegenden Schluß, nämlich durch Anwendung des berühmten Dirichletschen Satzes von den Primzahlen in einer arithmetischen Progression, zeigen, daß das Übereinstimmen dieser Invarianten für alle p nicht nur notwendig, sondern auch hinreichend für die rationale Äquivalenz im weiteren Sinne ist, also:

$$f_{a,b} \sim f_{c,d} \;\longleftrightarrow\; \left(\frac{a,\, b}{p}\right) \;=\; \left(\frac{c,\, d}{p}\right) \quad \text{für alle } p\,.$$

Auch läßt sich mittels des Hilbertschen Symbols ganz allgemein eine vollständige Invariantentheorie der rationalen Äquivalenz (im engeren oder auch weiteren Sinne) quadratischer Formen $f(x_1, \ldots, x_n)$ von n Variablen geben. Ich will das Resultat für die Äquivalenz im engeren Sinne angeben, an der man vornehmlich interessiert ist; die Äquivalenz im weiteren Sinne hat nur

untergeordnete Bedeutung, sie kam oben durch die Beschränkung auf Formen mit erstem Koeffizienten 1 herein.

Ohne Einschränkung kann man f als *reine* Form, d. h. in der Gestalt

$$f \;=\; a_1 x_1^2 + \cdots + a_n x_n^2 \qquad \text{mit rationalen} \quad a_i \neq 0$$

annehmen. Dann hat f als Invarianten gegen rationale Äquivalenz im engeren Sinne:

1.) den quadratfreien Kern d der Diskriminante $a_1 \ldots a_n$,

2.) die Charaktere $\prod_{i \geq j} \left(\frac{a_i, a_j}{p}\right)$ für alle p,

3.) den Trägheitsindex J, d. h. die Anzahl der negativen a_i.

Dies Invariantensystem ist ein vollständiges Invariantensystem für die rationale Äquivalenz im engeren Sinne, d. h. zwei Formen sind dann und nur dann im engeren Sinne rational äquivalent, wenn sie in diesen Invarianten übereinstimmen.

Auch lassen sich mit diesen Invarianten notwendige und hinreichende Kriterien dafür angeben, daß f rationale Nullform ist oder eine gegebene rationale Zahl $a \neq 0$ rational darstellt.

Siehe zu alledem meine Arbeiten in Crelle 152, 153, 172, sowie auch eine demnächst in Crelle 176 erscheinende Arbeit von E. Witt.

Die entsprechende Äquivalenztheorie und Darstellbarkeitstheorie bei durchgängiger Beschränkung auf *ganzzahlige* Koeffizienten und Variablenwerte liegt viel tiefer. Man kennt für sie kein vollständiges Invariantensystem.

Es gibt jedoch eine Zwischenstufe zwischen beiden Theorien, nämlich die der *quasiganzen* Äquivalenz und Darstellbarkeit, ein von E. Artin eingeführter Begriff, der besagt, daß man bei der rationalen Äquivalenz oder Darstellung jeden vorgegebenen Primzahlnenner in den Substitutionskoeffizienten bzw. darstellenden Variablen vermeiden kann, daß man also den evtl. unvermeidbaren Nenner von beliebigen Primstellen wegschieben kann. Diese Theorie wird ebenfalls durch ein arithmetisches Invariantensystem aus der Theorie der quadratischen Reste beherrscht, das eine Verfeinerung des obigen Invariantensystems für rationale Äquivalenz darstellt. Die zugehörige Klasseneinteilung der ganzzahligen quadratischen Formen ist unter dem Namen *Geschlechtereinteilung* in der Literatur bekannt. In seinen kürzlich in den Annals of Mathematics erschienenen tiefen Arbeiten zur Theorie der quadratischen Formen hat Siegel mein rein qualitatives Übertragungsprinzip von

den einzelnen Stellen aufs Große durch eine quantitative Relation unterbaut, die formal denselben Charakter hat wie die Hilbertsche Produktformel. Sie sagt aus, daß die geeignet definierte Dichte der quasiganzen Darstellungen durch eine ganzzahlige quadratische Form gleich dem Produkt der geeignet definierten Darstellungsdichten für die einzelnen p ist.

1.18 Baden–Baden 1938

Bericht über neuere Untersuchungen und Fragestellungen in der arithmetischen Theorie der algebraischen Funktionenkörper.

Vortrag Baden–Baden, September 1938.

Im *19. Jahrhundert* entwickelte sich ein großes, heute im wesentlichen abgeschlossenes Gebiet der Zahlentheorie, die Theorie der *algebraischen Zahlkörper* (algebraische Gleichungen in einer Unbestimmten). Zu Beginn des 19. Jahrhunderts wurden große Entdeckungen auf diesem Gebiet gemacht, man sah aber das Gebiet noch nicht in seiner heutigen, abgerundeten Form vor sich. Vieles, was wir heute an wohlbestimmter Stelle in die algebraische Zahlentheorie eingegliedert haben, stand damals noch zusammenhangslos nebeneinander.

Im *20. Jahrhundert* haben wir eine ähnliche Sachlage für die Theorie der *algebraischen Funktionenkörper über algebraischen Zahlkörpern* (algebraische Gleichungen in zwei Unbestimmten). Wir haben eine Reihe von wichtigen Einzelergebnissen, ohne daß diese im Bewußtsein der Forscher schon ihren wohlbestimmten Platz in einer abgerundeten Theorie haben.

Ich gebe im folgenden einen Überblick darüber, wie ich dieses neue Gebiet als Ganzes sehe und wie sich die bereits vorhandenen Ergebnisse und die noch offenen Fragen einordnen. Ich benutze diese Gelegenheit gleichzeitig, um den neuesten Stand der Arbeit an den verschiedenen Einzelfragen zu schildern.

Ich glaube, daß es für den Forscher notwendig ist, sich gelegentlich einmal auf die Zusammenhänge *im Großen* seines Arbeitsgebiets zu besinnen, und sich nicht völlig in die Einzelarbeit *im Kleinen* zu verlieren. Sonst wird ihm schnell der Boden unter den Füßen verschwinden, und er wird die unmittelbare Berührung mit der Welt des Greifbaren und Wirklichen in seinem Gebiet verlieren. In diesem Sinne möge man schon die Tatsache, daß ich die im folgenden zu besprechenden Einzelfragen in den Rahmen eines Vortrags einordne und sie von einem einheitlichen Gesichtspunkt aus sehe, als einen Versuch ansehen, an der Verschmelzung dieser Gedankenkreise zu einer abgerundeten Theorie nach besten Kräften mitzuwirken.

Allgemeines.

Die Theorie der algebraischen Funktionenkörper als solche gehört eigentlich nicht zur Zahlentheorie. In ihrer klassischen Form (Konstantenkörper der komplexe Zahlkörper) gehört sie zur Funktionentheorie, oder wenn der Nachdruck auf der Kurvendeutung der algebraischen Funktionen liegt, zur algebraischen Geometrie. In ihrer modernen Form (Konstantenkörper ein beliebiger Körper) gehört sie zur Algebra. Die Zahlentheorie ist vornehmlich an dem Fall interessiert, daß der Konstantenkörper ein algebraischer Zahlkörper ist. Sie darf von der Behandlung dieses Falles einmal eine Befruchtung gewisser Fragestellungen der algebraischen Zahlentheorie erwarten, dann aber auch wesentliche neue Fragestellungen und Ergebnisse.

Schon in der algebraischen Zahlentheorie selbst zieht man nun aber neben den eigentlich interessierenden algebraischen Zahlkörpern auch andere Körper heran, die nicht aus Zahlen im klassischen Sinne bestehen, nämlich einmal die endlichen Körper, die als Restklassenkörper nach Primidealen der algebr. Zahlkörper auftreten, und dann die $\wp$–adischen Körper, die als perfekte Hüllen zu den Bewertungen der algebraischen Zahlkörper auftreten. Daher ist die rein algebraische Theorie der algebraischen Funktionenkörper (Konstantenkörper beliebig) auch für die Zwecke des Zahlentheoretikers wichtig.

Wir betrachten demgemäß zunächst einen algebraischen Funktionenkörper (einer Unbestimmten) K über einem beliebigen Konstantenkörper Ω. Für den Fall, daß Ω Primzahlcharakteristik hat, setzen wir voraus, daß K/Ω *separabel erzeugbar* ist:

$$\mathsf{K} = \Omega(u, v) \quad \text{mit} \quad g(u, v) = 0$$

wo $g(u, v)$ ein absolut–irreduzibles Polynom über Ω ist, das in u oder v separabel ist. Wir wollen ferner durchweg voraussetzen, daß K/Ω *aufgeschlossen* ist, d. h. mindestens einen Primdivisor ersten Grades enthält; das kann stets durch endlich–algebraische Erweiterung von Ω erreicht werden. Durch Übergang zur algebraisch–abgeschlossenen Hülle $\overline{\Omega}$ von Ω entsteht der zu K gehörige *abgeschlossene* Funktionenkörper

$$\overline{\mathsf{K}} = \overline{\Omega}(u, v) \quad \text{mit} \quad g(u, v) = 0,$$

für den alle Primdivisoren vom ersten Grade sind. Wir zeichnen einen festen Primdivisor ersten Grades $\mathfrak{o}$ von K als *Bezugsprimdivisor* aus. K besitzt dann eine durch $\mathfrak{o}$ bis auf elementare Transformationen eindeutig festliegende *Normalerzeugung*:

$$\mathsf{K} = \Omega(x; y_1, \ldots, y_n)$$

mit Multiplikationsschema

(M) $$y_i y_j = \sum_{k=1}^{n} f_{ijk}(x) y_k.$$

Dabei ist:

> x Element mit möglichst niedriger $\mathfrak{o}$–Potenz $\mathfrak{o}^n$ im Nenner $[\mathsf{K} : \Omega(x)] = n$; es ist stets $n \leqq g+1$, wo g das Geschlecht von K.
> $y_1, \ldots, y_n$ Basis der in x ganzalgebraischen Elemente aus K in bezug auf die in x ganzalgebraischen Elemente aus $\Omega(x)$ (Polynome in x).

In einfachen Fällen kann $y_1, \ldots, y_n$ in der Form $1, y, \ldots, y^{n-1}$ gewählt werden; dann reduziert sich (M) auf eine einzige Gleichung

$$f(x, y) = 0,$$

die absolut–irreduzibel, in y separabel, und vom höchsten Koeff. 1 in y ist. Ist z. B. $g = 1$ und Char. $\Omega \neq 2, 3$, so hat man die Weierstrasssche Normalform

$$y^2 = 4x^3 - g_2 x - g_3, \qquad g_2^3 - 27 g_3^2 \neq 0.$$

Den trivialen Fall $g = 0$ (wo $n = 1$, $y_1 = 1$), lassen wir in der Folge durchweg beiseite. Der Einfachheit halber schreiben wir die Normalerzeugung kurz (auch allgemein kurz) in der Form

$$\mathsf{K} = \Omega(x, y) \quad \text{mit} \quad f(x, y) = 0$$

und nennen $f(x, y) = 0$ die Grundgleichung; im allgemeinen ist dabei also y ein n–gliedriges System und $f(x, y) = 0$ ein Multiplikationsschema.

Primdivisoren $\mathfrak{p} \neq \mathfrak{o}$ von K	$\longleftrightarrow$	über Ω algebr. nicht konj. Lösungen (a, b) von $f(x, y) = 0$
$\mathfrak{o}$	$\longleftrightarrow$	Lösung (∞, ∞)
Primdivisoren ersten Grades $\mathfrak{p} \neq \mathfrak{o}$ von K (*rationale Punkte*)	$\longleftrightarrow$	Lösungen (a, b) in Ω von $f(x, y) = 0$
Primdivisoren $\overline{\mathfrak{p}}$ von $\overline{\mathsf{K}}$ (*Punkte*)	$\longleftrightarrow$	Lösungen $(\overline{a}, \overline{b})$ in $\overline{\Omega}$ von $f(x, y) = 0$

Ungenaue Beschreibung durch Lös. von $g(u, v) = 0$.

Von besonderer Bedeutung für alle zu behandelnden Fragen ist die *Divisorenklassengruppe nullten Grades* von K; sie sei im folgenden mit D_{K} bezeichnet. Die Divisorenklassen nullten Grades lassen sich in der Form repräsentieren:

$$\frac{\mathfrak{g}}{\mathfrak{o}^g}, \quad \mathfrak{g} \text{ ganzer Divisor } g\text{–ten Grades von } \mathsf{K}.$$

Die ganzen Divisoren g–ten Grades entsprechen vermöge

$$\mathfrak{g} = \overline{\mathfrak{p}}_1 \cdots \overline{\mathfrak{p}}_g \quad \text{in} \quad \overline{\mathsf{K}}, \quad \overline{\mathfrak{p}}_i \longleftrightarrow (\overline{a}_i, \overline{b}_i) \quad \text{in} \quad \overline{\Omega} \quad (\textit{Koord. System} \text{ von } \mathfrak{g})$$

umkehrbar eindeutig den g–gliedrigen Systemen $(\overline{a}_i, \overline{b}_i)$ von über Ω algebraischen Grundgleichungslösungen, deren symm. Funktionen in Ω liegen (rationale *g–gliedrige Punktgruppen*).

Die Repräsentation ist (für $g > 1$) nicht immer eindeutig; vielmehr tritt eine Ausnahmemannigfaltigkeit von höchstens $g-1$ Dimensionen in der g–dimensionalen Mannigfaltigkeit aller $\mathfrak{g}$ auf, für die je unendlich viele $\mathfrak{g}$ dieselbe Klasse bestimmen. Man kann sie aber so eindeutig machen:

$$\frac{\mathfrak{g}_\gamma \mathfrak{o}^{g-\gamma}}{\mathfrak{o}^g} = \frac{\mathfrak{g}_\gamma}{\mathfrak{o}^\gamma} \qquad (0 \leqq \gamma \leqq g)$$

wo $\mathfrak{g}_\gamma$ alle ganzen, nicht durch $\mathfrak{o}$ teilbaren Divisoren mit $\dim \mathfrak{g}_\gamma = 1$ durchläuft; für deren Grade γ gilt von selbst die angegebene Ungleichung. Wir denken uns dies (oder irgendein) eindeutiges Repräsentantensystem für die $\mathfrak{g}$ zugrundegelegt. Dann stellt sich das Rechnen in D_{K} durch das Rechnen mit diesen Repräsentanten dar:

$$\frac{\mathfrak{g}}{\mathfrak{o}^g} \frac{\mathfrak{g}'}{\mathfrak{o}^g} \sim \frac{\mathfrak{g}''}{\mathfrak{o}^g}.$$

Dafür schreiben wir kurz additiv:

$$\mathfrak{g} + \mathfrak{g}' \sim \mathfrak{g}''.$$

In dieser Relation steckt natürlich $\mathfrak{o}$ als Bezugsprimdivisor. Dieser Darstellung des Rechnens in D_{K} liegen rationale Formeln für die Koordinaten $(\overline{a}_i, \overline{b}_i)$, $(\overline{a}'_i, \overline{b}'_i)$, $(\overline{a}''_i, \overline{b}''_i)$ von $\mathfrak{g}, \mathfrak{g}', \mathfrak{g}''$ zugrunde; die Koordinaten von $\mathfrak{g}''$ bestimmen sich durch Auflösung algebraischer Gleichungen g–ten Grades aus denen von $\mathfrak{g}, \mathfrak{g}'$.

Im klassischen Falle (Ω der komplexe Zahlkörper) ist die Struktur von D_{K} bekannt. Nach Abelschem Theorem und Jacobischen Umkehrsatz stellt sich

D_{K} isomorph durch das additive Rechnen mit dem g–gliedrigen Vektor

$$\mathfrak{u} \equiv \int_{\mathfrak{o}^g}^{\mathfrak{g}} d\mathfrak{u} \mod \mathsf{Per}$$

der Integrale 1. Gattung mit Reduktion nach dem komplex–g–dimensionalen Periodenparallelotop dar; dabei durchläuft $\mathfrak{u}$ alle g–gliedrigen Vektoren aus komplexen Zahlen.

I. Der Satz von A. Weil

Sei Ω ein algebraischer Zahlkörper. Welche Struktur hat D_{K} dann? Der Satz von A. Weil besagt, daß dann D_{K} von *endlichem Rang* r ist. Als abelsche Gruppe von endlichem Rang besitzt D_{K} dann eine Basis. Da die Elemente endlicher Ordnung ein Teilgitter des $2g$–dimensionalen Periodengitters bilden, sieht diese Basisdarstellung so aus:

$$\mathfrak{g} \sim \mu_1\mathfrak{a}_1 + \cdots + \mu_{2g}\mathfrak{a}_{2g} + \nu_1\mathfrak{b}_1 + \cdots + \nu_r\mathfrak{b}_r \quad \left\{ \begin{array}{c} \mu_i \mod m_i \\ \nu_i \text{ ganzrational} \end{array} \right\}.$$

Dabei sind die $\mathfrak{a}_i, \mathfrak{b}_i$ feste ganze Divisoren g–ten Grades. Also: Herleitung aller „rationalen“ g–gliedrigen Punktgruppen aus endlich vielen durch die Additionsrelation (und die darauf gestützte Multiplikation).

□□□

Weil beweist seinen Satz auf analytischem Wege, nämlich durch Heranziehung der zum Periodenparallelotop gehörigen Abelschen Funktionen (Thetafunktionen). Es ist uns in meinem Seminar gelungen, diesen Beweis im Falle $g = 1$ rein algebraisch durchzuführen. Dadurch gewinnt er erheblich an Einfachheit und Durchsichtigkeit. Gleichzeitig ergibt sich ein interessanter Ausblick auf eine Verallgemeinerung der Klassenkörpertheorie. Für $g > 1$ wollen wir dasselbe im nächsten Seminar durchführen.

Ich skizziere nachstehend kurz den Gedankengang des rein algebraischen Beweises für $g = 1$. Es wird zunächst die Weilsche Distributionslehre entwickelt; auch deren Begründung können wir gegenüber Weil stark vereinfachen. Dabei kann g noch beliebig sein.

Durchläuft $\mathfrak{p}$ die Primdivisoren von K und $\Omega_{\mathfrak{p}}$ die zugehörigen Restklassenkörper von K — endlich–algebraische Erweiterungen von Ω, deren Grade

$f_\mathfrak{p}$ die Grade der $\mathfrak{p}$ sind — so versteht man unter einer Distribution $\mathfrak{a}_\mathfrak{p}$ von K eine Funktion der $\mathfrak{p}$, deren Werte Ideale aus den $\Omega_\mathfrak{p}$ sind. Zwei Distributionen heißen gleich

$$\mathfrak{a}_\mathfrak{p} \doteq \mathfrak{a}'_{\mathfrak{p}'},$$

wenn zwei von $\mathfrak{p}$ unabhängige Ideale $\mathfrak{u}, \mathfrak{u}'$ aus Ω existieren derart, daß

$$\mathfrak{u}\mathfrak{a}_\mathfrak{p} = \mathfrak{u}'\mathfrak{a}'_\mathfrak{p} \quad \text{für alle} \quad \mathfrak{p}$$

ist. Es kommt also für die Distributionen auf „beschränkte“ Faktoren nicht an.

Jedem Element $a \neq 0$ entspricht eine Hauptdistribution $a(\mathfrak{p})$, geliefert durch die Hauptideale der Reste $a \mod \mathfrak{p}$ in $\Omega_\mathfrak{p}$; auf die endlich vielen $\mathfrak{p}$ mit $a(\mathfrak{p}) = \infty$ kommt es im Sinne $\doteq$ nicht an. $a(\mathfrak{p})$ hängt nur von a als Hauptdivisor ab. Der Weilsche Hauptsatz über die Distributionen lautet nun:

> Jedem Divisor $\mathfrak{a}$ von K entspricht eindeutig eine Distribution $\mathfrak{a}(\mathfrak{p})$ derart, daß Multipl., Division, gr. gem. Teilerbild. sich isomorph übertragen und für Hauptdivisoren die angegebenen Hauptdistributionen vorliegen. Insbesondere entsprechen ganzen Divisoren ganze Distributionen (beschr. Nenner).

Ein erster rein algebraischer Teil des Weilschen Endlichkeitsbeweises stellt fest, daß der Index $[D_\mathsf{K} : nD_\mathsf{K}]$ endlich ist für jedes natürliche n. Dies beweist man für $g = 1$ so. Ohne Einschränkung sei Ω so groß, daß die n^2 Klassen vom Exponenten n von $\overline{\mathsf{K}}$ bereits zu K gehören. Sie bilden eine abelsche Gruppe vom Typus (n, n), repräsentiert durch die Primdivisoren ersten Grades $\mathfrak{u}$ mit $n\mathfrak{u} \sim \mathfrak{o}$. Man betrachtet dann den durch n–Multiplikation entstehenden zu K isomorphen Teilkörper $\mathsf{K}n$.

$\mathsf{K}/\mathsf{K}n$ ist abelsch vom Typus (n, n); die Galoisgruppe wird durch die den $\mathfrak{u}$ entsprechenden Translationsautomorphismen $\sigma_\mathfrak{u}$ geliefert. Das Zerlegungsgesetz lautet:

$$\mathfrak{p}n = \prod_{\overline{\mathfrak{q}}} \overline{\mathfrak{q}} \quad \text{mit} \quad n\overline{\mathfrak{q}} \sim \mathfrak{p}.$$

Dabei ist $\mathfrak{p}$ ein Primdivisor ersten Grades von K, $\mathfrak{p}n$ sein isomorphes Bild in $\mathsf{K}n$. Die $\overline{\mathfrak{q}}$ entstehen aus einem durch die $\sigma_\mathfrak{u}$:

$$\sigma_\mathfrak{u}\overline{\mathfrak{q}} \sim \overline{\mathfrak{q}} + \mathfrak{u}.$$

Insbesondere ist $\mathsf{K}/\mathsf{K}n$ unverzweigt. Voll zerlegt in K sind genau *die* Primdivisoren ersten Grades $\mathfrak{p}n$ von $\mathsf{K}n$, für die $\mathfrak{p}$ eine Klasse aus nD_{K} repräsentiert.

Es sei nun

$$\mathsf{K} = \mathsf{K}n(\sqrt[n]{z_1 n},\ \sqrt[n]{z_2 n})$$

eine Kummersche Erzeugung von $\mathsf{K}/\mathsf{K}n$. Man erhält sie in der Form

$$z_1 \cong \frac{\mathfrak{u}_1^n}{\mathfrak{o}^n}\,, \qquad z_2 \cong \frac{\mathfrak{u}_2^n}{\mathfrak{o}^n}\,,$$

wo $\mathfrak{u}_1, \mathfrak{u}_2$ eine Basis der Klassen vom Exponenten n sind. Dann wird der Restklassenkörper $\Omega_{\overline{\mathfrak{q}}}$ für die Primdivisoren $\overline{\mathfrak{q}}$ durch

$$z_1(n\overline{\mathfrak{q}}) = z_1(\mathfrak{p}), \qquad z_2(n\overline{\mathfrak{q}}) = z_2(\mathfrak{p})$$

erzeugt:

$$\Omega_{\overline{\mathfrak{q}}} = \Omega(\sqrt[n]{z_1(\mathfrak{p})},\ \sqrt[n]{z_2(\mathfrak{p})}).$$

Dieser Restklassenkörper ist als Verschärfung des Grades der Primdivisoren bei der Zerlegung anzusehen; für nicht–endliche Restklassenkörper ist die Zerlegung nicht allein durch den Grad gekennzeichnet. Es gilt nun das Zerlegungsgesetz:

> *Die Multiplikationsgruppe der* $z_1(\mathfrak{p}), z_2(\mathfrak{p})$ *im Sinne* $\underset{n}{=}$ (*Kummer–Erzeugung*) *ist isomorph zur Klassengruppe* $D_{\mathsf{K}}/nD_{\mathsf{K}}$ *bei der Repräsentation durch die* $\mathfrak{p}$.

In diesem Sinne kann $\mathsf{K}/\mathsf{K}n$ (besser $\mathsf{K}n^{-1}/\mathsf{K}$) als Klassenkörper zu $D_{\mathsf{K}}/nD_{\mathsf{K}}$ bezeichnet werden.

Aus der Distributionenlehre entnimmt man nun leicht, daß die Gruppe der $z_1(\mathfrak{p}), z_2(\mathfrak{p})$ im Sinne $\underset{n}{=}$ endlich ist. Daraus folgt dann die Endlichkeit von $D_{\mathsf{K}}/nD_{\mathsf{K}}$.

Der zweite Teil des Weilschen Endlichkeitsbeweises geht so vor sich: Sei n fest gewählt (Weil nimmt $n = 2$), und sei $\mathfrak{R}$ ein Repräsentantensystem der Klassen von $D_{\mathsf{K}}/nD_{\mathsf{K}}$. Dann hat man für jeden Primdivisor $\mathfrak{p}$ ersten Grades von K eine Reduktion:

$$\mathfrak{p} \sim \mathfrak{r} + n\mathfrak{q}\,, \quad \mathfrak{r} \quad \text{in} \quad \mathfrak{R}$$

auf einen weiteren Primdivisor $\mathfrak{q}$ ersten Grades von K. Man zeigt, daß bei hinreichend häufiger Fortsetzung dieses Verfahrens man auf einen endlichen

Wertevorrat für den Restprimdivisor kommt. Dazu hat man die Koordinaten von $\mathfrak{q}$ durch die von $\mathfrak{p}$ abzuschätzen (descente infinie). Man nimmt dazu zweckmäßig die Koordinaten nicht für eine Normalerzeugung, sondern folgendermaßen: Die n^2 Elemente

$$x_{\mathfrak{u}} \cong \frac{\mathfrak{u}n}{\mathfrak{o}^{n^2}} = \frac{\mathfrak{x}\mathfrak{u}}{\mathfrak{o}^{n^2}}$$

bilden eine Basis des Moduls $\left(\frac{1}{\mathfrak{o}^{n^2}}\right)$. Man zeigt leicht, daß dann die Kummer–Erzeugung von $\mathsf{K}/\mathsf{K}n$ in der folgenden Form geschrieben werden kann

$$x_{\mathfrak{u}}^{n^2} = t^{n^2} \sum_{\mathfrak{v}} a_{\mathfrak{u}\mathfrak{v}} \cdot (x_{\mathfrak{v}} n), \qquad t \cong \frac{\mathfrak{o}n}{\mathfrak{o}^{n^2}}\,.$$

Ist einfach $\mathfrak{p} \sim n\mathfrak{q}$, so hat man

$$x_{\mathfrak{u}}(\mathfrak{q})^{n^2} = t(\mathfrak{q})^{n^2} \sum_{\mathfrak{v}} a_{\mathfrak{u}\mathfrak{v}} x_{\mathfrak{v}}(\mathfrak{p}).$$

Nun kann man *eine* Distribution $\mathfrak{o}(\mathfrak{q})$ als Hauptideale normieren; dann werden auch die daran durch Hauptdivisorbeziehungen gekoppelten Distributionen Hauptideale

$$x_{\mathfrak{v}}(\mathfrak{p}) = \frac{\mathfrak{x}(\mathfrak{p})}{\mathfrak{o}(\mathfrak{p})^{n^2}},$$

und obige Formeln stellen sich für die Zähler so dar:

$$\mathfrak{x}\mathfrak{u}(\mathfrak{q})^{n^2} \doteq \sum_{\mathfrak{v}} a_{\mathfrak{u}\mathfrak{v}} \mathfrak{x}_{\mathfrak{v}}(\mathfrak{p}).$$

Dabei haben die $\mathfrak{x}_{\mathfrak{v}}(\mathfrak{p})$, $\mathfrak{x}\mathfrak{u}(\mathfrak{q})$ als ganze Distributionen beschränkte Nenner und können in den letzten Formeln im Sinne $\doteq$ auch durch ganzalgebraische Zahlen ersetzt werden. Für das Maximum der absoluten Beträge (bei sämtlichen arch. Bewertungen von Ω) erhält man so die Abschätzung:

$$X(\mathfrak{q}) \leqq C \cdot X(\mathfrak{p})^{\frac{1}{n^2}}.$$

Nimmt man noch die Addition des Repräsentanten $\mathfrak{r}$ aus $\mathfrak{R}$ hinzu, so folgt ähnlich:

$$X(\mathfrak{q}) \leqq C X(\mathfrak{p})^{\frac{2}{n^2}}.$$

Hieraus folgt durch Iteration, wegen $n^2 > 2$, daß die $\mathfrak{q}$ schließlich einem endlichen Wertevorrat angehören, weil die $X(\overline{\mathfrak{q}})$ schließlich beschränkt sind.

Zur Verallgemeinerung dieses Beweises auf $g > 1$ muß die Weilsche Distributionenlehre auf den zu K gehörigen Abelschen Funktionenkörper (Transzendenzgrad g) verallgemeinert werden. Weil hat das mit algebraisch–geometrischen Methoden gemacht, jedoch ist gerade dieser Teil seines Beweises am wenigsten durchsichtig. Ansätze dazu, die sich auf die Krullsche Theorie der Zerlegung der Primideale niedrigster Dimension (Stellen) stützen, haben wir bereits, und wir hoffen im Wintersem. damit durchzukommen.

Im Anschluß an den Weilschen Satz erhebt sich natürlich die Frage, wie sich der Rang r von D aus den arithm. Eigenschaften des Zahlkörpers Ω und den K kennzeichnenden Invarianten (Moduln) bestimmt. Dies ist meiner Ansicht nach das allerwichtigste Problem der neuen Theorie. Man weiß bisher in dieser Richtung so gut wie nichts. Nagell und Billing haben Abschätzungen von r im Falle $g = 1$ gegeben, wo K durch einen Modul j gekennzeichnet ist. Dabei spielen Klassenzahlen und Einheiten von Ω eine Rolle (oder vielmehr von $\Omega(\theta)$, wo θ Nullstelle des Polynoms $4x^3 - g_2x - g_3$ ist). Ferner ist aus Beispielen bekannt, daß $r \geqq 1$ sein kann.

Interessant wäre z. B. die Frage nach dem Wert von r für den mit dem Fermatproblem verbundenen Funktionenkörper

$$\mathsf{K} = \mathsf{P}(x, y) \quad \text{mit} \quad x^p + y^p = 1$$

vom Geschlecht

$$g = \frac{(p-1)(p-2)}{2},$$

der von keinem Koeffizientenparameter abhängt.

Allgemein liefert jede Aussage über r einen tiefliegenden Satz über Diophantische Gleichungen.

II. Der Satz von C. Siegel.

Dieser Satz entspringt der Frage nach den Lösungen einer beliebigen Gleichung $g(u, v) = 0$ über Ω vom Geschlecht $g \geqq 1$ in ganzalgebraischen Zahlen u, v aus Ω. Er sagt aus, daß es nur endlich viele solche Lösungen gibt, und auch nur endlich viele Lösungen mit ganzem u. Er kann so ausgesprochen werden:

> Ist u ein nicht–konstantes Element aus K, so gibt es höchstens endlich viele Primdivisoren ersten Grades $\mathfrak{p}$ von K, für die $u(\mathfrak{p})$ ganzalgebraisch ist, oder auch nur: für die $u(\mathfrak{p})$ beschränkten Nenner hat.

Mittels der Weilschen Distributionenlehre reduziert er sich auf den folgenden Satz:

> Ist $\mathfrak{u}$ ein Primdivisor ersten Grades von K, so ist die Distribution $\mathfrak{u}(\mathfrak{p}) \neq 1$ für jede unendliche Menge von Primdivisoren ersten Grades $\mathfrak{p}$ von K.

Zum Beweis leitet man aus der gegenteiligen Annahme eine Approximationsaussage von folgender Art her: ein g–gliedriges System $\alpha_1, \ldots, \alpha_g$ über Ω algebraischer Zahlen wird sehr scharf durch Zahlbrüche $\frac{\xi_1}{\xi_0}, \ldots, \frac{\xi_g}{\xi_0}$ aus Ω approximiert.
Das widerspricht dann einer Verallgemeinerung des Thue–Siegelschen Satzes.

Zur Herleitung dieser Approximationsaussage verwendet Siegel wieder die Thetafunktionen. Es ist uns in meinem Seminar gelungen, den Beweis für $g = 1$ rein algebraisch durchzuführen; für $g > 1$ wollen wir das im Wintersem. durchführen.

Der Grundgedanke für die Herleitung der Approximationsaussage ist wieder die Verwendung der n–Multiplikation, diesmal aber nicht mit festem n sondern mit $n \to \infty$.

Aus der Annahme, daß $\mathfrak{u}(\mathfrak{p}) \doteq 1$ für unendlich viele $\mathfrak{p}$ ist, folgt für $g = 1$ nach dem Weilschen Satz, daß dies auch für unendlich viele $\mathfrak{p}$ der Fall ist, die — bei geeignetem Bezugsprimdivisor $\mathfrak{o}$ — von der Form $\mathfrak{p} \sim n\mathfrak{q}$ sind. Dann ist aber $(\mathfrak{u}n)(\mathfrak{q}) \doteq 1$ für unendlich viele $\mathfrak{q}$, und man hat jetzt einen ganzen Divisor $\mathfrak{u}n$ vom Grade n^2 mit lauter verschiedenen Primteilern, statt des Primdivisors $\mathfrak{u}$. Man zeigt dann, daß hieraus folgt, daß die x–Koordinate α eines Primteilers von $\mathfrak{u}n$ sehr stark durch die x–Koordinaten $\frac{\xi_{[\ldots]}}{\xi_0}$ der $\mathfrak{q}$ approximiert wird, und zwar nach einer ähnlichen Methode wie oben im Beweis des Weilschen Satzes, mittels der Distributionen.

Für $g > 1$ hat man ganze Divisoren g–ten Grades statt der Primdivisoren ersten Grades als Vertreter der Klassen; man beginnt formal mit $\mathfrak{p}^g$, erhält dann aber durch die n–Teilung nicht etwa $\mathfrak{q}^g$, sondern einen allgemeinen ganzen Divisor g–ten Grades $\mathfrak{g}$. So kommt man hier zu einer simultanen Approximation.

Die fragliche Verallgemeinerung des Thue–Siegelschen Satzes ist in der Siegelschen Arbeit mit der Anwendung auf die dort auftretenden Thetafunktionen verschmolzen. Wir haben folgenden eleganten Approximationssatz herausgearbeitet:

Ω algebr. Zahlkörper vom Grade k

$\alpha_1, \ldots, \alpha_g$ algebraische Zahlen, deren Körper $\Omega(\alpha_1, \ldots, \alpha_g)$ über Ω den Relativgrad r hat, und deren lin. Unabhängigkeitsmaß über Ω den Wert d hat (die Potenzprod. bis zur Dimension d hin sind noch lin. unabh. über Ω).

Wenn dann die Ungleichungen

$$\left|\frac{\xi_i}{\xi_0} - \alpha_i\right| \leqq C.\, N(X)^{-e} \qquad (i = 1, \ldots, g)$$

$$\left\{ \begin{array}{c} C \text{ pos. Konstante} \\ X = \operatorname{Max}\big(|\xi_0|, |\xi_1|, \ldots, |\xi_g|\big) \end{array} \right\}$$

unendlich viele Lösungen $\frac{\xi_1}{\xi_0}, \ldots, \frac{\xi_g}{\xi_0}$ in ganzen $\xi_0, \xi_1, \ldots, \xi_g$ aus Ω haben, so ist notwendig

$$e \leqq \operatorname*{Min}_{\delta=0,1,\ldots,d} \left(\delta + \frac{kr}{\binom{g+\delta}{g}} \right)$$

$\binom{g+\delta}{g}$ ist die Anzahl der Potenzprodukte bis zur Dimension δ hin. Für $g = 1$ wird $d = r - 1$ und

$$e \leqq \operatorname*{Min}_{\rho=0,1,\ldots,r-1} \left(\rho + \frac{kr}{\rho + 1} \right).$$

Das ist genau der Thue–Siegelsche Satz.

III. Der Satz von E. Lutz.

Für die genauere Untersuchung von D_{K} wird man wichtige Hilfsmittel bekommen, wenn man analog zur Theorie der quadratischen Formen und der Algebren die entsprechende Frage im Kleinen stellt.

Für $g = 1$ hat E. Lutz diese Frage erschöpfend beantwortet. Ist Ω ein $\wp$–adischer Zahlkörper, so ist D_{K} sogar eine Operatorgruppe mit den ganzen $\wp$–adischen Zahlen aus Ω als Operatorenbereich und hat als solche den *Rang* 1. Man hat daher eine eindeutige Basisdarstellung der Form:

$$\mathfrak{p} \sim \mu_1 \mathfrak{a}_1 + \mu_2 \mathfrak{a}_2 + \nu \mathfrak{b} \qquad \left\{ \begin{array}{c} \mu_i \mod m_i \\ \nu \text{ ganz } \wp\text{–adisch aus } \Omega \end{array} \right\}.$$

Hieran anschließend erheben sich die Fragen: Wie steht es mit den ganzzahligen $\wp$–adischen Lösungen einer beliebigen Gleichung $g(u,v) = 0$ vom Geschlecht 1?

Wie lautet die Verallgemeinerung des Satzes von Frl. Lutz für $g > 1$?

Besteht ein Zusammenhang zwischen D_{K} für einen algebr. Zahlkörper Ω und den $D_{\mathsf{K}_\wp}$ für seine $\wp$–adischen Erweiterungen $\Omega_\wp$ nach Analogie der Siegelschen Produktformel für die Lösungsdichten bei quadr. Formen?

Über diese Fragen ist nichts bekannt. Besonders die letzte Frage scheint mir der Schlüssel zu genaueren Aussagen über D_{K} zu sein.

IV. Der Satz von H. Hasse.

Anstatt bei einem algebraischen Zahlkörper Ω zu den $\wp$–adischen Erweiterungen $\Omega_\wp$ überzugehen, kann man auch erst einmal nur zur Kongruenz mod $\wp$ übergehen. Für fast alle $\wp$ entsteht dabei ein algebraischer Funktionenkörper K mit endlichem Konstantenkörper Ω von gleichem Geschlecht g und mit der sich durch Restbildung ergebenden Normalerzeugung.

Die Theorie der Funktionenkörper K mit endlichem Konstantenkörper Ω hat auch großes selbständiges Interesse, abgesehen von der Bedeutung, die die so entstehenden Kongruenzfunktionenkörper für die Untersuchung eines Funktionenkörpers mit algebraischem Zahlkörper als Konstantenkörper haben. Denn es bestehen weitgehende Analogien zwischen den Kongruenzfunktionenkörpern und den algebraischen Zahlkörpern. Die Kongruenzfunktionenkörper sind sogar einfacher als die algebraischen Zahlkörper, weil bei ihnen alle Bewertungen diskret sind, während bei den algebraischen Zahlkörpern endlich viele Kontinuierliche Bewertungen auftreten. Anstelle der durch diese kontinuierlichen Bewertungen bedingten Approximationsaussagen (Minkowskische Diskriminantenabschätzung) treten für die Kongruenzfunktionenkörper genaue Aussagen (Riemann–Rochscher Satz).

Diese größere Einfachheit äußert sich insbesondere für die Zetafunktion von K:

$$\zeta(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}}$$

wo $\mathfrak{N}(\mathfrak{p}) = q^{\mathfrak{f}_\mathfrak{p}}$ die Elementanzahl des endlichen Restklassenkörpers $\Omega_\mathfrak{p}$ von K mod $\mathfrak{p}$ bezeichnet; q bezeichnet die Elementanzahl von Ω. Diese Funktion

ist nämlich wesentlich ein Polynom in $\frac{1}{q^s}$:

$$\zeta(s) = \zeta_0(s)L(s)$$
$$\zeta_0(s) = \frac{1}{1-\frac{1}{q^s}}\,\frac{1}{1-\frac{q}{q^s}}$$
$$L(s) = 1 + \frac{N_1-(q+1)}{q^s} + \cdots + \frac{q^g}{q^{2gs}},$$

und zwar vom Grade $2g$, mit höchstem Koeffizienten q^g und Koeffizienten $N_1-(q+1)$ des linearen Gliedes. Dabei bezeichnet N_1 die Anzahl der Primdivisoren ersten Grades von K. $N_1-(q+1)$ ist die Abweichung von N_1 gegenüber seinem wahrscheinlichen Wert $q+1$; N_1 ist ja die Anzahl der Lösungen von $f(x,y)=0$ in Ω (inkl. ∞).

Die Riemannsche Vermutung für diese Zetafunktion ist gleichwertig mit der Aussage

$$|N_1-(q+1)| \leqq 2gq^{\frac{1}{2}}$$

(für Ω und alle endlichen Erweiterungskörper in der Rolle von Ω). Es ist mir gelungen, diese Riemannsche Vermutung für $g=1$ zu beweisen, und zwar nicht etwa durch Bestätigung der Abschätzung, sondern als eine Strukturaussage über D_{K}. Für $g=1$ ist $N_1=h$ die Ordnung von D_{K} (Klassenzahl von K).

Um diese Strukturaussage auszusprechen und zu beweisen, braucht man ein weiteres rein algebraisches Rüstzeug, die Theorie der Korrespondenzen und des Multiplikatorenrings von K, die kürzlich von Deuring für beliebigen Konstantenkörper in einer für die arithmetischen Anwendungen brauchbaren Form entwickelt wurde. In der Sprache der algebraischen Geometrie findet sie sich schon in den Arbeiten der italienischen Schule entwickelt, insbesondere bei Severi.

Eine Primkorrespondenz von K zu sich entspringt aus einer Lösung ξ,η von $f(x,y)=0$ in der algebraisch–abgeschlossenen Hülle $\overline{\overline{\mathsf{K}}}$ von K. Sie bewirkt einen Homomorphismus von $D_{\overline{\mathsf{K}}}$ in sich. Zusammengesetzte Korrespondenzen werden durch formale Homomorphismenaddition erklärt. So ist K eindeutig ein (nur von $\overline{\mathsf{K}}$ abhängiger) nichtkommutativer Operatorenring M von $D_{\overline{\mathsf{K}}}$ zugeordnet, der Multiplikatorenring von K. Im klassischen Falle stellt sich dieser Ring M durch die komplexen Multiplikationen der Periodenmatrix der Integrale 1. Gattung von K dar.

Jedem solchen Multiplikator $\mu \neq 0$ ist eine natürliche Zahl $N(\mu)$ zugeordnet, der Grad von $\mathsf{K}(\xi,\eta)/\Omega(\xi,\eta)$. Man kann zeigen, daß $N(\mu)$ (von Inseparabilitätsausnahmen abgesehen) der Index $[D : \mu D]$ ist. M hat ferner stets die Charakteristik 0, auch wenn Ω Primzahlcharakteristik hat. M enthält also den Ring Γ der ganzrationalen Zahlen, entsprechend der schon oben benutzten natürlichen Multiplikation.

M besitzt einen involutorischen Antiautomorphismus $\mu \longrightarrow \overline{\mu}$, entsprechend der Umkehrung der Korrespondenzrichtung.

Für endlichen Körper Ω liefert

$$(\xi,\eta) = (x^q, y^q)$$

eine Korrespondenz π mit $N(\pi) = q^g$. Die Anwendung von π auf einen ganzen Divisor g–ten Grades $\mathfrak{g}$ von K stellt sich als q–Potenzierung seiner Koordinaten und also auch ihrer symmetr. Grundfunktionen dar. So folgt, daß D_{K} innerhalb $D_{\overline{\mathsf{K}}}$ durch $\pi\overline{\mathfrak{g}} \sim \overline{\mathfrak{g}}$ oder also $(\pi-1)\overline{\mathfrak{g}} \sim \mathfrak{o}$ gekennzeichnet ist $\big((\pi-1)$–te Teilwerte$\big)$. Es ist daher

$$N(\pi - 1) = h.$$

Für $g = 1$ zeigt man nun leicht, daß $N(\mu) = \mu\overline{\mu}$ ist und auch $\mu + \overline{\mu}$ zu Γ gehört. Daher genügt jedes μ zusammen mit $\overline{\mu}$ einer quadratischen Gleichung über Γ, und zwar wegen $N(\mu) > 0$ einer solchen mit konjugiert komplexen Wurzeln. Für endlichen Körper Ω hat π die Gleichung

$$\pi^2 + v\pi + q = 0,$$

wo v wegen $N(\pi - 1) = h = N_1$ den Wert

$$v = N_1 - (q+1)$$

hat. Daher ist diese Gleichung wesentlich das Polynom

$$q^{2s}L(s) = q^{2s} + \big(N_1 - (q+1)\big)q^s + q,$$

d. h. π ist zusammen mit $\overline{\pi}$ formal das Wurzelpaar der Zetafunktion. Als Multiplikatoren sind $\pi, \overline{\pi}$ konjugiert–komplex, und dies bedeutet

$$|N_1 - (q+1)| \leqq 2q^{\frac{1}{2}}$$

d. h. die Riemannsche Vermutung für $g = 1$.

Für $g > 1$ bleibt noch zu zeigen, daß die Elemente μ aus M algebraischen Gleichungen vom Grade $2g$ über Γ genügen, und daß dabei $\mu \longrightarrow \overline{\mu}$ formal der Übergang zum konj. kompl. ist. Und zwar ist genauer zu zeigen, daß μ und $\overline{\mu}$ Wurzeln derj. Gleichung sind, die sich aus

$$N(t - \mu) = f(t)$$

ergibt, wenn man die ganze Zahl t als Unbestimmte auffaßt. Daß dies wirklich ein Polynom vom Grade $2g$ liefert, ist nicht auf der Hand liegend. Ist dies bewiesen, so folgt die Identität mit dem L–Polynom nach einem Identitätssatz von Rohrbach. Darüber hinaus ist dann aber noch zu zeigen, daß $\mu \longrightarrow \overline{\mu}$ für dieses Polynom den Übergang zum konj. komplexen bedeuten.

Als Aussage über D_{K} kann die Riem. Vermutung so ausgesprochen werden: D_{K} ist innerhalb $D_{\overline{\mathsf{K}}}$ als die durch den Operator $\pi - 1$ annullierte Untergruppe $\big((\pi-1)$–te Teilwerte$\big)$ gekennzeichnet, und dabei ist π formal eine der beiden Nullstellen der Zetafunktion in q^s.

Grob gesagt ist die Riemannsche Vermutung für Kongruenzfunktionenkörper im Falle $g = 1$ das Äquivalent zu der Tatsache, daß im klassischen Falle der Periodenquotient $\frac{\omega_2}{\omega_1}$ von Null verschiedenen Imaginärteil hat. Für $g > 1$ ist die Verallgemeinerung hierzu im klassischen Falle, daß für die Periodenmatrix (Ω_1, Ω_2) der Quotient $\Omega_1^{-1}\Omega_2$ eine (g–reihige) Matrix ist, deren Imaginärteil eine definite quadr. Form hat. Das Äquivalent hierzu ist die Riemannsche Vermutung für Kongruenzfunktionenkörper im Falle $g > 1$. Das zum Beweis noch zu leistende besteht darin, im klassischen Falle hierfür eine rein algebraische Deutung zu geben.

V. Der Satz von M. Deuring.

Deuring hat für den Fall $g = 1$ die Hauptsätze der komplexen Multiplikation rein algebraisch gedeutet und bewiesen.

In analytischer Formulierung lauten diese Hauptsätze so: Es sei k ein imaginär–quadratischer Zahlkörper und ω_1, ω_2 eine Ganzheitsbasis von k, ferner $j(\omega_1, \omega_2)$ der Wert der normierten Modulfunktion für sie. Dann ist $k\big(j(\omega_1, \omega_2)\big)$ der absolute Klassenkörper zu k. Es sei ferner $\tau(u; \omega_1, \omega_2)$ die aus der Weierstrassschen $\wp$–Funktion durch Normierung entspringende Webersche Funktion. Ist dann $\mathfrak{m}$ ein ganzes Ideal von k und $\rho \cong \frac{\mathfrak{r}}{\mathfrak{m}}$ ein reduzierter

Idealbruch vom Nenner $\mathfrak{m}$. Dann ist $k\big(j(\omega_1,\omega_2),\tau(\rho;\omega_1,\omega_2)\big)$ der Strahlklassenkörper mod $\mathfrak{m}$ zu k.

□□□

Zur algebraischen Formulierung dieser beiden Hauptsätze der komplexen Multiplikation betrachtet Deuring zunächst den Multiplikatorenring M eines algebr. Funktionenkörpers K vom Geschlecht $g = 1$ über irgendeinem Konstantenkörper Ω. Dann hängt M nur vom zugehörigen abgeschlossenen Funktionenkörper $\overline{\mathsf{K}}$ ab. Es gibt einen kleinsten Konstantenkörper Ω_0 derart, daß die Multiplikatoren von $\overline{\mathsf{K}}$ sich bereits im Koeffizientenbereich Ω_0 rational darstellen, also Multiplikatoren der zugehörigen Konstantenerweiterung K_0 sind.

M hat notwendig einen der drei folgenden Typen:

a.) $\mathsf{M} = \Gamma$

b.) M Ordnung in einem imag. quadr. Zahlkörper k

c.) M Ordnung in einer imag. quadr. Divisionsalgebra.

Die beiden letzten Typen kommen höchstens dann vor, wenn Ω_0 absolut–algebraisch ist, der letzte nur für Ω_0 von Primzahlcharakteristik.

Es sei nun Ω ein algebraischer Zahlkörper; dann kommt nur der erste (reguläre) und der zweite (singuläre) Typus vor. Sei vorausgesetzt, daß der singuläre Typus vorliegt, und — der Einfachheit halber — daß M die Hauptordnung seines imaginär–quadratischen Quotientenkörpers k ist. Dann lautet der erste Hauptsatz in rein–algebraischer Formulierung einfach so:

> Der zugehörige kleinste Konstantenkörper Ω_0 ist der absolute Klassenkörper zu k.

Ist nämlich $y^2 = 4x^3 - g_2x - g_3$ die Normalerzeugung, so liegen g_2, g_3 in Ω_0, also auch $j = \frac{12^3 g_2^3}{g_2^3 - 27g_3^2}$. Ferner ist auch k isomorph in Ω_0 vertreten, vermöge der Anwendung der Multiplikatoren μ auf das ganze Differential $\frac{dx}{y}$:

$$\frac{d(x\mu)}{y\mu} = c_\mu \frac{dx}{y}\,.$$

Es zeigt sich dann, daß Ω_0 durch diese Repräsentation von k und durch j erzeugt ist.

Zum rein–algebraischen Beweis ist natürlich erheblich mehr zu tun, als bloß diese formale Zurückführung auf den analytisch formulierten Satz zu geben. Deuring gibt einen reinalgebraischen Beweis, indem er für den Körper Ω_0 das Klassenkörperzerlegungsgesetz bestätigt. Dieses ergibt sich durch die von mir gegebene Kennzeichnung von $D_{\mathsf{K}_0 \mod \wp}$ für die Primideale $\wp$ von Ω_0 durch die Multiplikatoren von $\overline{\mathsf{K}} \mod \wp$. Deurings Beweis ist so ein Beispiel für die Beherrschung von K_0 durch die zugehörigen Kongruenzfunktionenkörper mod $\wp$.

Der zweite Hauptsatz lautet in rein–algebraischer Formulierung so:

> Es sei $\mathfrak{m}$ ein beliebiges ganzes Ideal von k und $\overline{\mathfrak{p}}$ ein Primdivisor von $\overline{\mathsf{K}}$ mit der Eigenschaft
>
> $$\mu\overline{\mathfrak{p}} \sim \mathfrak{o} \quad \text{genau für} \quad \mu \equiv 0 \mod \mathfrak{m}.$$

Die durch $\overline{\mathfrak{p}}$ bestimmte Klasse kann in diesem Sinne als $\mathfrak{m}$–ter Teilwert bezeichnet werden. Genauer sei $\overline{\mathfrak{p}}$ ein primitiver $\mathfrak{m}$–ter Teilwert, d. h. $\mathfrak{m}$ kann nicht durch einen echten Teiler ersetzt werden. Ferner sei K_0^* derjenige Teilkörper von K_0, der bei den Einheitsoperatoren aus M invariant ist $\big($im allgem. sind das nur $\varepsilon = \pm 1$, und es ist $\mathsf{K}_0^* = \Omega_0(x)\big)$. Dann ist $\mathsf{K}_0^* \mod \overline{\mathfrak{p}}$ der Strahlklassenkörper mod $\mathfrak{m}$ von k.

Diese Deuringschen Sätze lassen die Frage offen, welche imag. quadr. Körper k als Quotientenkörper von Multiplikatorenringen M auftreten, derart daß M die Hauptordnung von k ist. Analytisch weiß man, daß *alle* imag.–quadr. Körper auftreten. Ein rein–algebr. Beweis hierfür dürfte sehr schwierig sein. Erst damit wären die Hauptsätze der komplexen Multiplikation in ihrem vollen Umfang rein algebraisch bewiesen.

Allgemein kann man die auftretende Frage für beliebiges Geschlecht g stellen: Welche Ringe M treten als Multiplikatorenringe algebr. Funktionenkörper auf?

Von der Periodenmatrix ausgehend wird diese Frage in den Arbeiten von Albert behandelt. Diese Untersuchungen gehen aber gar nicht auf den tiefliegenden Unterschied zwischen Periodenmatrizen überhaupt und Periodenmatrizen algebraischer Funktionenkörper ein, auf den es hier gerade ankommt.

Abgesehen von dieser sehr tiefliegenden Frage besitzt Deuring auch die Verallgemeinerung seiner rein algebraischen Formulierungen auf beliebiges

Geschlecht g. Wie sie lauten, hat er allerdings noch nicht mitgeteilt. Jedenfalls ist man damit der Lösung des Hilbertschen Problems der Klassenkörperkonstruktion durch Abelsche Funktionen ein gutes Stück näher gekommen. Es sieht so aus, als ob die rein algebraische Behandlung im Rahmen der in diesem Vortrag entwickelten Theorie erheblich bessere Aussichten auf die endgültige Lösung hat, als die mit viel unnötigem Ballast beladene Lösung auf funktionentheoretischem Wege. Das ist im Falle $g = 1$ (elliptische Funktionen) ganz klar zu erkennen. Es liegt das vor allem daran, daß man bei der rein algebraischen Behandlung sofort den ganzen Körper charakterisiert, während man ihn bei der funktionentheoretischen Behandlung durch einen bestimmten Funktionswert als primitives Element erzeugt.

1.19 Helsinki, Djursholm 1938

Neuere Untersuchungen und Fragestellungen in der arithmetischen Theorie der algebraischen Funktionenkörper.

Vortrag Helsinki, Djursholm. September 1938.

Einleitung.

Zwei Richtungen in neuerer Zahlentheorie, unterschieden durch Fragestellung:

Wie groß ist etwas?	Wie ist etwas gebaut?
z. B. bei quadratischen Formen:	
Anzahl der Darstellungen?	Gesetze für die Darstellbarkeit?
Anzahl der Klassen?	Zusammenhänge zwischen den Klassen?
Im allgemeinen:	
Fragestellungen sehr einfach, Methoden in keinem Verhältnis dazu. (Hardy–Littlewood)	Fragestellungen und Methoden erwachsen organisch aus einander. (Hilbert, Artin)
Antworten sind:	
Gesetze des Zufalls.	Organische Gesetze.
Trennung nach Nationalitäten im Großen gesehen:	
englisch (russisch)	deutsch (französisch, italienisch).

Die folgenden Betrachtungen fallen unter die zweite Kategorie. Sie betreffen ein Gebiet der Zahlentheorie, das noch ganz jung ist, nämlich die Zahlentheorie der algebraischen Gleichungen in zwei Variablen.

Im *19. Jahrhundert* entwickelte sich ein großes, heute im wesentlichen abgeschlossenes Gebiet der Zahlentheorie, die algebraische Zahlentheorie. Sie kann als die *Zahlentheorie der algebraischen Gleichungen in einer Variablen* beschrieben werden. Zu Beginn des 19. Jahrhunderts wurden große Entdeckungen auf diesem Gebiete gemacht. Man sah aber das Gebiet noch nicht in seiner heutigen abgerundeten Form vor sich. Vieles, was wir heute an wohlbestimmter Stelle in die algebraische Zahlentheorie eingegliedert haben, stand damals noch zusammenhangslos nebeneinander.

Im *20. Jahrhundert* haben wir eine ähnliche Sachlage für die *Zahlentheorie der algebraischen Gleichungen in zwei Variablen*. Wir haben eine Reihe

von wichtigen Einzelergebnissen, ohne daß im Bewußtsein der Forscher diese Tatsachen schon ihren wohlbestimmten Platz in einer abgerundeten Theorie haben.

Ich gebe im folgenden einen Überblick darüber, wie ich diese Theorie sehe und wie sich die bereits vorhandenen Ergebnisse und die noch offenen Fragen einordnen.

I. Die Grundbegriffe.

In der zu betrachtenden Theorie handelt es sich um algebraische Gleichung in zwei Variablen mit algebraischen Koeffizienten:

$$f(x, y) = 0$$

Ohne Einschränkung:

$f(x, y)$ absolut–irreduzibel (nicht in ebensolche Faktoren zerlegbar),

$f(x, y)$ ganzalgebraische Koeffizienten.

Ähnlich wie bei algebraischen Gleichungen in einer Variablen betrachtet man hier gleich den Körper K aller rationalen Funktionen von x, y mit Koeffizienten aus einem gegebenen endlich–algebraischen Zahlkörper Ω, der die Koeffizienten von $f(x, y)$ enthält:

$$\mathsf{K} = \Omega(x, y) \quad \text{mit} \quad f(x, y) = 0$$

heißt algebraischer Funktionenkörper einer Variablen über Ω als Konstantenkörper. Es zeigt sich, daß man zu glatten Begriffen und Tatsachen nur kommt, wenn man diesen Körper als den eigentlich zu behandelnden Gegenstand ansieht, und die Gleichung als eine unter unendlich vielen Möglichkeiten seiner Erzeugung (Körperinvarianz, birationale Transformation).

In der klassischen Theorie der algebraischen Funktionen nimmt man statt eines endlich–algebraischen Zahlkörpers Ω den Körper aller komplexen Zahlen als Konstantenkörper. Ich darf die Begriffsbildungen und Hauptsätze dieser klassischen Theorie hier als in großen Zügen bekannt voraussetzen. Man verwendet dabei weitgehend die Theorie der analytischen Funktionen einer komplexen Variablen, selbst wenn man sich der Analogie mit der Zahlentheorie und ihrer Ausdrucksweise bedient (Hensel–Landsberg). Ein Weg zum Aufbau der Theorie für einen endlich–algebraischen Zahlkörper Ω ergibt sich, indem man Ω als Teilkörper des komplexen Zahlkörpers ansieht und aus den

klassischen Sätzen solche über den Körper K durch diese Einbettung (Beschränkung der Koeffizienten auf Ω) herleitet. Das ist aber einerseits nicht methodenrein; andrerseits ist es für den Aufbau der Theorie, wie ich ihn mir denke, unerläßlich, eine von analytischen Methoden freie Begründung zu geben. Wie wir noch genauer sehen werden, braucht man nämlich die entsprechende Theorie auch für Körper Ω als Konstantenkörper, die nicht im Körper der komplexen Zahlen enthalten sind.

Es gibt nun in der Tat eine von analytischen Methoden ganz freie Begründung der arithmetischen Theorie der algebraischen Funktionenkörper K über einem beliebigen Konstantenkörper Ω:

$$\mathsf{K} = \Omega(x, y) \quad \text{mit} \quad f(x, y) = 0$$

> $f(x, y)$ absolut–irreduzibel über Ω, d. h. nicht in Faktoren mit über Ω algebraischen Koeffizienten zerlegbar.
> Für den Fall, daß Ω Primzahlcharakteristik p hat, ist noch zu fordern, daß $f(x, y)$ etwa in y separabel ist.

ich gebe nachstehend eine Übersicht über die Grundbegriffe dieser Theorie, und zwar erläutere ich diese Grundbegriffe durch Gegenüberstellung der entsprechenden Begriffe der klassischen Theorie.

Ω beliebiger Körper	Ω Körper der komplexen Zahlen
Primdivisoren $\mathfrak{p}$ von K, definiert durch Bewertungen $w_{\mathfrak{p}}(z)$ von K/Ω oder durch formale Potenzreihen–entwicklungen. Restbildung mod $\mathfrak{p}$ bildet die Ele–mente z von K auf Elemente $z(\mathfrak{p})$ einer endlich–algebraischen Erweiterung $\Omega_{\mathfrak{p}}$ von Ω ab (inkl. ∞). Deren Grad $\mathfrak{f}_{\mathfrak{p}}$ heißt der Grad von $\mathfrak{p}$. Man erhält alle Primdivisoren $\mathfrak{p}$ von K auch, indem man alle solchen Abbildungen von K nimmt. Dabei entspricht über Ω konjugierten Abbildungen	Punkte $\mathfrak{p}$ der Riemannschen Fläche $\mathfrak{R}$ zu K. K besteht aus den auf $\mathfrak{R}$ im Kleinen analytischen, im Großen eindeutigen Funktionen. Wert $z(\mathfrak{p})$ an der Stelle $\mathfrak{p}$ von $\mathfrak{R}$, $\Omega_{\mathfrak{p}} = \Omega, \quad \mathfrak{f}_{\mathfrak{p}} = 1.$

(Fortsetzung auf der nächsten Seite)

Ω beliebiger Körper	Ω Körper der komplexen Zahlen
derselbe Primdivisor $\mathfrak{p}$.	
Entsprechend einer Erzeugung $\mathsf{K} = \Omega(x, y)$ mit $f(x, y) = 0$ können die Primdivisoren $\mathfrak{p}$ bis auf endlich viele Ausnahmen auch durch die Lösungen $x(\mathfrak{p}) = a, y(\mathfrak{p}) = b$ von $f(x, y) = 0$ in über Ω algebraischen Elementen a, b gekennzeichnet werden, wobei über Ω konju– gierten Lösungen derselbe Primdivisor entspricht.	Die Stellen $\mathfrak{p}$ von $\mathfrak{R}$ sind bis auf endlich viele Ausnahmen durch die Lösungen $x(\mathfrak{p}) = a, y(\mathfrak{p}) = b$ von $f(x, y) = 0$ in komplexen Zahlen gekennzeichnet.
Jeder Primdivisor $\mathfrak{p}$ vom Grade $\mathfrak{f}_\mathfrak{p}$ zerfällt—der Unterscheidung der $\mathfrak{f}_\mathfrak{p}$ Konjugierten entsprechend— in $\mathfrak{f}_\mathfrak{p}$ Primdivisoren ersten Grades $\overline{\mathfrak{p}}_i$ des Körpers $\overline{\mathsf{K}}$, der durch Erweiterung des Konstantenkörpers auf seine algebraisch–abgeschlossene Hülle $\overline{\Omega}$ entsteht.	Ist Ω endlich–algebraisch, so entsprechen die Primdivisoren von $\overline{\mathsf{K}}$ umkehrbar eindeutig denjenigen Punkten von $\mathfrak{R}$, für die alle Funktionen z aus K über Ω algebraische Werte haben. Die Primdivisoren von K entstehen daraus, indem jeweils die bezgl. Ω konjugierten Primdivisoren von $\overline{\mathsf{K}}$ zusammengefaßt werden.
Wir setzen (durch endl. alg. Erw. von Ω) voraus, daß K auf– geschlossen ist, d. h. mindestens einen Primdivisor ersten Grades $\mathfrak{o}$ enthält. Ein solcher sei als Bezugs– primdivisor ausgezeichnet. Dann übersieht man alle Primdivisoren $\mathfrak{p} \neq \mathfrak{o}$ von K (ausnahmslos) auf Grund einer zu $\mathfrak{o}$ gehörigen Nor– malerzeugung: x Element, das nur bei $\mathfrak{o}$ unendlich wird, von möglichst niedriger Ordnung n (liegt durch $\mathfrak{o}$ bis auf ganze lineare Substitu– tionen fest). $\mathsf{K}/\Omega(x)$ vom Grade n $y_1, \ldots, y_n$ Basis der von x ganzalg. abhängigen Elemente aus K	Auszeichnung eines bestimmten Elements aus K als unabhängige Variable: x Funktion aus K mit einzigem Pol in gegebenem Punkt $\mathfrak{o}$ von $\mathfrak{R}$, von möglichst niedriger Ordnung n. Zugehörige Darstellung der (abstrakten) Fläche $\mathfrak{R}$ als n–blättr. Fläche über der x–Kugel. $y_1, \ldots, y_n$ Basis derj. Funktionen aus K, die $\mathfrak{o}$ als einzigen Pol haben; sie ist nicht notwendig von der Form $1, y, \ldots, y^{n-1}$.
$\mathsf{K} = \Omega(x; y_1, \ldots, y_n)$ mit Multiplikationstafel	$\mathfrak{o}$ wird bei der gewonnenen Reali– sierung von $\mathfrak{R}$ das Unendliche; dieses

(Fortsetzung auf der nächsten Seite)

Ω beliebiger Körper	Ω Körper der komplexen Zahlen
(M) $y_i y_j = \sum_{k=1}^{n} f_{ijk}(x) y_k,\ f_{ijk}(x)$ Polyn. über Ω. (Verallgemeinerung einer Erzeugung durch Grundgleichung).	ist dabei Verzweigungspunkt der Ordnung n.
Primdivisoren $\mathfrak{p} \neq \mathfrak{o}$ von K entsprechen jetzt umkehrbar eindeutig den über Ω algebraischen nicht konjugierten Lösungen $x(\mathfrak{p}) = a; y_1(\mathfrak{p}) = b_1, \ldots, y_n(\mathfrak{p}) = b_n$ von (M). Bei Unterscheidung der Konjugierten erhält man die Prim–Divisoren $\overline{\mathfrak{p}}_i$ von $\overline{\mathsf{K}}$. Die Primdivisoren ersten Grades $\mathfrak{p} \neq \mathfrak{o}$ von K entsprechen umkehrbar eindeutig den Lösungen von (M) in Ω.	Die endlichen Stellen $\mathfrak{p} \neq \mathfrak{o}$ von $\mathfrak{R}$ werden jetzt umkehrbar eindeutig durch die zugeordneten Wertsysteme $x(\mathfrak{p}) = a; y_1(\mathfrak{p}) = b_1, \ldots, y_n(\mathfrak{p}) = b_n$ beschrieben.
Divisoren von K: $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}}$	Vorgabe von Nullstellen und Polen mit vorgeschriebenen Ordnungen;
($\alpha_\mathfrak{p}$ ganzrat. nur endl. viele $\alpha_\mathfrak{p} \neq 0$)	Endlichkeitsbedingung
Hauptdivisoren: $z \cong \prod_{\mathfrak{p}} \mathfrak{p}^{w_\mathfrak{p}(z)},\ \sum_{\mathfrak{p}} \mathfrak{f}_\mathfrak{p} w_\mathfrak{p}(z) = 0$	Elemente von K erfüllen
z durch seinen Hauptcharakter eindeutig bis auf Konstante $\neq 0$ als Faktor festgelegt.	neben der Endlichkeitsbedingung noch die Summenformel: $\sum_{\mathfrak{p}} w_\mathfrak{p}(z) = 0$ für die funktionentheoretischen Ordnungszahlen $w_\mathfrak{p}(z)$ an den einzelnen Stellen $\mathfrak{p}$ von $\mathfrak{R}$. Durch Angabe der Nullstellen und Pole mit Ordnungszahlen liegt eine Funktion des Körpers bis auf Konstante $\neq 0$ als Faktor fest.
Grad $\mathfrak{f}_\mathfrak{a} = \sum_{\mathfrak{p}} \mathfrak{f}_\mathfrak{p} \alpha_\mathfrak{p}$	
Hauptdivisoren $\mathfrak{a} \cong z$ haben $\mathfrak{f}_\mathfrak{a} = 0$	
Divisorengruppe	
Divisorengruppe nullten Grades	
Divisorenklassengruppe	

(Fortsetzung auf der nächsten Seite)

Ω beliebiger Körper	Ω Körper der komplexen Zahlen
Divisorenklassengruppe nullten Grades (für alles Folgende wichtigster Begriff).	
Differentiale wdz, zugeordneter Differentialdivisor.	Integralfunktionen auf $\mathfrak{R}$ (im Kleinen analytisch bis auf logar. [...]stellen, im Großen Perioden)
Ganze Differentiale, solche mit ganzem zugeordneten Divisor.	Integrale 1. Gattung (im Kleinen regulär, im Großen Perioden).
Geschlecht g = Anzahl der linear unabh. ganzen Differentiale.	g fällt mit topologischem Geschlecht von $\mathfrak{R}$ zusammen.
$g = 0$ ist (für aufgeschlossene K) gleichbedeutend damit, daß $\mathsf{K} = \Omega(t)$ rational ist. Im folgenden sei durchweg $g \geqq 1$ vorausgesetzt.	Dann bestimmen die Integrale 1. Gattung durch kanonische Zerschneidung von $\mathfrak{R}$ ein Periodenparallelotop von g komplexen Dimensionen.
Nach Riemann–Rochschem Satz gibt es in jeder Divisorenklasse nullten Grades mindestens einen Vertreter der Form $\frac{\mathfrak{g}}{\mathfrak{o}^g}$, wo $\mathfrak{g}$ ganzer Divisor vom Grade g, und mit Ausnahme einer Mannigfaltigkeit niederer Dimension (im algebr. Sinne) für $\mathfrak{g}$ auch nur einen solchen Vertreter. Das Rechnen in der Klassengruppe nullten Grades stellt sich dann durch diese Vertreter so dar: $\frac{\mathfrak{g}_1}{\mathfrak{o}^g} \cdot \frac{\mathfrak{g}_2}{\mathfrak{o}^g} \sim \frac{\mathfrak{g}}{\mathfrak{o}^g}$. Dafür schreiben wir kurz: $\mathfrak{g}_1 + \mathfrak{g}_2 \sim \mathfrak{g}\ (\mathfrak{o})$ Daß dabei die Vertreter $\mathfrak{g}$ nicht immer eindeutig bestimmt sind, schadet nichts. Man rechne mit irgendeinem vollen Vertretersystem.	Die Struktur der Klassengruppe nullten Grades wird durch das Abelsche Theorem und den Jacobischen Umkehrsatz vollständig gegeben. Diese beiden Sätze sagen zusammen aus, daß die Klassengruppe nullten Grades von K isomorph ist zur Additionsgruppe der g–gliedrigen Vektoren aus komplexen Zahlen, wobei mit den Vektoren nach dem Periodenparallelotop als Modul gerechnet wird; und zwar wird dieser Isomorphismus gegeben durch $\mathfrak{u} \equiv \int_{\mathfrak{o}^g}^{\mathfrak{g}} d\mathfrak{u} \mod \mathsf{P}\mathfrak{a}$

(Fortsetzung auf der nächsten Seite)

Ω beliebiger Körper	Ω Körper der komplexen Zahlen
Für $g = 1$ sind sie immer eindeutig bestimmt.	wo $\mathfrak{u}$ ein Basisvektor der Integrale 1. Gattung von K ist, und $\int_{\mathfrak{o}^g}^{\mathfrak{g}} = \int_{\mathfrak{o}}^{\mathfrak{p}_1} + \cdots + \int_{\mathfrak{o}}^{\mathfrak{p}_g}$ für $\mathfrak{g} = \mathfrak{p}_1 \cdots \mathfrak{p}_g$.
Die Vertreter $\mathfrak{g}$ entsprechen umkehrbar eindeutig den g–gliedrigen Lösungssystemen von (M) in über Ω algebraischen Elementen, deren symmetr. Funktionen in Ω liegen; dabei ist $\mathfrak{o}$ formal die unend–liche Lösung zuzuordnen.	$\mathfrak{u}$ durchläuft alle g–gliedrigen kom–plexen Vektoren mod $\mathsf{P}\mathfrak{a}$. Zwei $\mathfrak{g}$ gehören dann und nur dann zur selben Klasse, wenn die $\mathfrak{u}$ mod $\mathsf{P}\mathfrak{a}$ kongr. sind, und der Klassen–multiplikation entspricht die Addition der $\mathfrak{u}$ mod $\mathsf{P}\mathfrak{a}$.
Das oben erklärte additive Rechnen mit den $\mathfrak{g}$ im Sinne $\sim (\mathfrak{o})$ ist als das algebraische Äquivalent zum Rechnen im Periodenparallelotop anzusehen. Es kann durch rationale Formeln ausgedrückt werden.	Die Vertreter $\mathfrak{g}$ sind genau die g–gliedrigen Punktgruppen auf $\mathfrak{R}$.
Als den zu K gehörigen Körper Abelscher Funktionen bezeichnet man den Körper $\mathfrak{K} = \Omega\{\mathfrak{x}_1, \ldots, \mathfrak{x}_g\}$ der rationalen symmetrischen Funktionen mit Koeffizienten aus Ω von g algebraisch–unabhängigen Lösungssystemen $\mathfrak{x}_i = (x_i; y_{i1}, \ldots, y_{in})$ von (M), also sozusagen von g unabhängigen variablen Primdivisoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_g$ von K, die man dann auch zu einem variablen ganzen Divisor $\mathfrak{x} = \mathfrak{x}_1 \cdots \mathfrak{x}_g$ vom Grade g zusammenfassen kann. □□□	Der so rein algebraisch definierte Abelsche Funktionenkörper $\mathfrak{K}$ besteht aus der Gesamtheit der zum Periodenparallelotop gehörigen analytischen Funktionen eines g–gliedrigen komplexen Vektors $\mathfrak{u}$.

Gekürzte Einleitung. [1]

1. Hasses Seitenzählung beginnt hier erneut bei -1-

Im Werden begriffene neue Theorie: *Zahlentheorie der algebraischen Gleichungen in zwei Variablen*

Vergleich mit Zahlentheorie der algebraischen Gleichungen in einer Variablen im vorigen Jahrhundert.

Zweck dieses Vortrags ist: Bisherige Hauptergebnisse der neuen Theorie in einheitlichem Rahmen auszusprechen und den Weg für weitere Forschung zu weisen. Dadurch mitzuhelfen an dem Zustandekommen einer einheitlichen und geschlossenen Theorie.

Grundbegriffe.

Ω beliebiger Körper; Hauptanwendung auf algebraische Zahlkörper; doch braucht man dazu als Hilfsmittel auch abstrakte Körper.

$\mathsf{K} = \Omega(x, y)$ mit $f(x, y) = 0$ (abs. irr.)

Prinzip der Körperinvarianz (birationale Invarianz)

Erster wichtiger Grundbegriff: *Punkt* oder *Prindivisor* von K.
Im klassischen Fall: Punkt der zugehörigen Riemannschen Fläche.

Allgemein roh gesagt: Über Ω algebraische Lösung der Grundgleichung.
Dazu Ergänzungen hinsichtlich ∞ und Verzweigungspunkten. Besonders wichtig: *Primdivisoren 1. Grades*, entsprechen Grundgleichungslösungen in Ω selbst. Dadurch Anknüpfung an klassisches Problem der Zahlentheorie: Lösungen diophantischer Gleichungen.

Zur scharfen Fassung des Punktbegriffs *Normalerzeugung*. Ohne Einschränkung Ω so groß (endl. alg. Erw.), daß ursprüngliche Grundgleichung eine Lösung in Ω hat, d. h. daß K einen Primdivisor 1. Grades hat. Ein solcher als *Bezugsprimdivisor* $\mathfrak{o}$ zugrundegelegt.

x Element aus K, das nur $\mathfrak{o}$ im Nenner hat, und zu möglichst niedrigem Exponenten n. Dann x bis auf ganze lineare Substitution $x \longrightarrow \alpha x + \beta$ festgelegt. $[\mathsf{K} : \Omega(x)] = n$. Ferner dann $y_1, \ldots, y_n$ Basis der von x ganzalgebr. abh. Elemente aus K in bezug auf Polynombereich $\Omega[x]$. Dann K bestimmt durch *Multiplikationsschema*

$$y_i y_j = \sum_{k=1}^{n} f_{ijk}(x) y_k \qquad \text{(M)}$$

Es übernimmt Rolle der Grundgleichung; Raumkurve in $n+1$ Dimensionen, statt 2–dimensionaler Kurve. Basis $y_1, \ldots, y_n$ liegt bis auf leicht angebbare

Substitutionen fest. Somit liegt Normalerzeugung wesentlich eindeutig durch $\mathfrak{o}$ fest.

Geschlecht g. Im klassischen Falle das topologische Geschlecht der Riemannschen Fläche. Die Riemannsche Formel hat rein algebraischen Charakter und überträgt sich auf beliebigen Konstantenkörper Ω. $g = 0 \longleftrightarrow \mathsf{K} = \Omega(x)$ (bei geeignetem x); dieser Fall sei durchweg ausgeschlossen. Also $g \geqq 1$. Für $g = 1$ ist Normalerzeugung [2]

$$y^2 = 4x^3 - g_2 x - g_3\,, \qquad g_2^3 - 27 g_3^2 \neq 0$$

(vorausgesetzt, daß $\operatorname{Char}\Omega \neq 2, 3$; sonst auch leicht angebbar).

Stets ist $n \leqq g + 1$ (nach Riemann–Rochschem Satz).

Primdivisoren $\neq \mathfrak{o} \longleftrightarrow$ über Ω algebr., nicht konj. Lösungen von (M)

$\mathfrak{o} \longleftrightarrow$ Lösung $(\infty; \infty, \ldots, \infty)$.

Unterscheidet man die konj., so erhält man die Primdiv. (1. Grades) von $\overline{\mathsf{K}}$, entspr. Übergang zu algebr.–abgeschl. Hülle $\overline{\Omega}$.

Primdivisoren 1. Grades $\neq \mathfrak{o} \longleftrightarrow$ Lösungen von (M) in Ω.

Die $\alpha; \beta_1, \ldots, \beta_n$ zu Punkt $\mathfrak{p}$ heißen seine Koordinaten (bezgl. der Normalerz.) entsprechen den Funktionswerten bei $\mathfrak{p}$ im klassischen Fall.

Zweiter wichtiger Grundbegriff: *Rechnen mit den g–gliedrigen Punktgruppen* (*ganzen Divisoren g–ten Grades*):

$$\mathfrak{g} = \mathfrak{p}_1 \cdots \mathfrak{p}_g$$

Dabei $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ Punkte von $\overline{\mathsf{K}}$ derart, daß die symm. Funktionen der Koordinaten in Ω liegen (die $\mathfrak{p}_i = 0$ nicht mitzurechnen).

$\mathfrak{g} \sim \mathfrak{g}'$, wenn $\frac{\mathfrak{g}}{\mathfrak{g}'}$ ein El. aus Ω entspricht (nach Nullst. u. Polen).

Verknüpfungsrelation:

$$\frac{\mathfrak{g}}{\mathfrak{o}^g} \cdot \frac{\mathfrak{g}'}{\mathfrak{o}^g} \sim \frac{\mathfrak{g}''}{\mathfrak{o}^g}\,, \quad \text{kurz} \quad \mathfrak{g} + \mathfrak{g}' \sim \mathfrak{g}'' \ (\mathfrak{o}).$$

$\mathfrak{g}''$ existiert nach Riemann–Rochschem Satz immer, und im allgemeinen auch eindeutig. Wir denken ein volles Repr. System für die $\mathfrak{g}$ im Sinne $\sim$ gewählt.

2. Relationszeichen der zweiten der beiden folgenden Relationen undeutlich

Dann ist die Verkn. eindeutig und unbeschränkt und liefert eine abelsche Gruppe, die *Divisorenklasssengruppe nullten Grades* D_{K} von K; sie ist sogar unabhängig von $\mathfrak{o}$, also Invariante von K. Um sie handelt es sich wesentlich. Grob gesagt handelt es sich bei D_{K} um ein bestimmtes Rechnen mit den g–gliedrigen Lösungssystemen einer Grundgleichung $f(x,y)=0$ (oder schärfer eines Mult. Schemas (M)), deren symm. Funktionen in Ω liegen. Für $g=1$ wird das Rechnen durch die Koord. so beschrieben:

$$\begin{vmatrix} 1 & \alpha & \beta \\ 1 & \alpha' & \beta' \\ 1 & \alpha'' & \beta'' \end{vmatrix} = 0$$

(Add. Th. der ell. Funkt.). Für $g>1$ hat man eine entspr. Determinanten–Darst. des Rechnens mit den g–gliedr. Punktgr.)

Im klassischen Falle (Ω der kompl. Zahlkörper) stellt sich das Rechnen in D_{K} transzendent so dar:

$d\mathfrak{u}$ g–gliedriger Basisvektor der Diff. 1. Gattung (ganzen Diff.)

$$\mathfrak{u} \equiv \int_{\mathfrak{o}^g}^{\mathfrak{g}} d\mathfrak{u} \equiv \sum_{i=1}^{g} \int_{\mathfrak{o}}^{\mathfrak{p}_i} d\mathfrak{u} \mod \mathsf{P}\mathfrak{a}.$$

liefert Vektor $\mathfrak{u}$ aus kompl. Zahlen mod $\mathsf{P}\mathfrak{a}$. (Parallelotop von g komplexen Dimensionen).

Nach Abelschem Theorem: $\mathfrak{g} \sim \mathfrak{g}' \longleftrightarrow \mathfrak{u} \equiv \mathfrak{u}' \mod \mathsf{P}\mathfrak{a}$.

Nach Jacobischem Theorem: $\mathfrak{u}$ durchl. *alle* kompl. Vektoren.

Daher

$D_{\mathsf{K}} \cong$ Rechnen mit g–gliedrigen kompl. Vekt. mod $\mathsf{P}\mathfrak{a}$.

II. Der Satz von A. Weil.

Es sei jetzt wie zu Beginn Ω ein endlichalgebraischer Zahlkörper. Der Satz von A. Weil macht eine allgemeine Aussage über die Struktur der Divisorenklassengruppe nullten Grades von K. Er sagt aus, daß diese Gruppe *endlichen Rang* r hat. Als abelsche Gruppe besitzt sie dann eine Basisdarstellung der Form:

$$\mathfrak{g} \sim \mu_1\mathfrak{a}_1 + \cdots + \mu_{2g}\mathfrak{a}_{2g} + \nu_1\mathfrak{b}_1 + \cdots + \nu_r\mathfrak{b}_r \ (\mathfrak{o}) \left\{ \begin{array}{c} \mu_i \bmod m_i \\ \nu_i \text{ ganzrational} \end{array} \right\}.$$

$(\mathfrak{g}; \mathfrak{a}_1, \ldots, \mathfrak{a}_{2g}; \mathfrak{b}_1, \ldots, \mathfrak{b}_r$ ganze Divisoren g–ten Grades).

Die Anzahl der Basiselemente endlicher Ordnung ist notwendig $\leqq 2g$, entsprechend dem Periodenparallelotop.

Weil hat diesen Satz mit analytischen Hilfsmitteln bewiesen. Er benutzt die Darstellung der zu K gehörigen Abelschen Funktionen durch Thetafunktionen. Für $g = 1$ wurde der Satz schon vorher durch Mordell bewiesen, und zwar entsprechend unter Benutzung der Darstellung der Funktionen aus K als elliptische Funktionen. Es ist uns in meinem Seminar gelungen, den Beweis für $g = 1$ rein arithmetisch zu führen. Für $g > 1$ haben wir dazu ebenfalls einen Ansatz und wollen ihn im nächsten Semester durchführen. Der Beweis gewinnt dadurch an Einfachheit und Durchsichtigkeit.

Wir wollen uns die Bedeutung des Satzes von Weil am Spezialfall $g = 1$ (Mordell) klarmachen. Eine Normalerzeugung von K kann in der Weierstrassschen Normalform angenommen werden:

$$y^2 = 4x^3 - g_2 x - g_3 \qquad (g_2^3 - 27g_3^2 \neq 0).$$

Die Klassen nullten Grades entsprechen hier umkehrbar eindeutig den Primdivisoren ersten Grades, also einfach den Lösungen a, b dieser Gleichung in Ω, wobei der Bezugsprimdivisor $\mathfrak{o}$ der unendlichen Lösung entspricht. Die Additionsrelation

$$\mathfrak{p}_1 + \mathfrak{p}_2 \sim \mathfrak{p} \ (\mathfrak{o})$$

in der Klassengruppe nullten Grades wird rational durch die Formeln des Additionstheorems der Weierstrassschen Funktionen

$$x = \wp(u), \qquad y = \wp'(u)$$

dargestellt. Diese Formeln liefern aus Lösungen in Ω wieder Lösungen in Ω. Der Satz von Mordell sagt aus, daß man alle Lösungen in Ω aus endlich vielen durch wiederholte Addition und Subtraktion im Sinne des Additionstheorems herleiten kann. Analytisch kann er auch so formuliert werden: die Punkte u im Periodenparallelogramm, für die $\wp(u), \wp'(u)$ in Ω liegen, werden in eindeutiger Basisdarstellung in folgender Form gegeben:

$$u \equiv \mu_1\alpha_1 + \mu_2\alpha_2 + \nu_1\beta_1 + \cdots + \nu_r\beta_r \mod \mathsf{Pa}. \left\{ \begin{array}{c} \mu_i \bmod m_i \\ \nu_i \text{ ganzrational} \end{array} \right\}$$

Im allgemeinen Falle (Weil) treten an Stelle der Lösungen der Grundgleichung in Ω die g–gliedrigen Lösungssysteme des Multiplikationsschemas

(M) einer Normalerzeugung von K, deren symmetrische Funktionen in Ω liegen, und anstelle der $u, \alpha_1, \alpha_2, \beta_1, \ldots, \beta_r$ g–gliedrige Vektoren im Periodenparallelotop. Grob gesagt handelt es sich um einen Endlichkeitssatz für die g–gliedrigen Lösungssysteme einer beliebigen Grundgleichung $f(x, y) = 0$, deren symmetrische Funktionen in Ω liegen.

An den Satz von Weil schließt sich naturgemäß die tiefere Frage an, wie die Invarianten m_i und r der Klassengruppe nullten Grades von K bestimmt sind. Darüber ist noch recht wenig bekannt. Für $g = 1$ hat man obere Abschätzungen von Nagell und Billing, die eng mit arithmetischen Eigenschaften von Ω oder einer algebr. Erweiterung von Ω (Einheiten, Klassenzahl) verknüpft sind. Man hat für $g = 1$ Beispiele dafür, daß $r > 0$ sein kann, daß also die durch die komplexe Multiplikation gelieferten algebraischen Teilwerte der elliptischen Funktionen keineswegs die einzigen algebraischen Werte sind.

Ich möchte es als eine Hauptaufgabe der hier besprochenen Theorie hinstellen, genaue Aussagen über die Bestimmung der Invarianten m_i, r aus den arithmetischen Eigenschaften von Ω und aus den Invarianten (Moduln) von K zu gewinnen.

Hinsichtlich des Fermatproblems wäre es z. B. interessant, diese Aufgabe für den (parameterfreien) Funktionenkörper mit der Grundgleichung

$$x^p + y^p = 1$$

vom Geschlecht

$$g = \frac{(p-1)(p-2)}{2}$$

in Angriff zu nehmen.

III. Der Satz von C. Siegel.

Eine tieferliegende Frage ist die nach den Lösungen von $f(x, y) = 0$ in ganzalgebraischen Zahlen aus Ω. Hier hat C. Siegel den tiefliegenden Endlichkeitssatz bewiesen, daß die Anzahl dieser Lösungen für $g \geqq 1$ *endlich* ist. Siegel zeigt genauer: Ist x ein nicht–konstantes Element aus K, so ist $x(\mathfrak{p})$ höchstens für endlich viele Primdivisoren ersten Grades $\mathfrak{p}$ von K ganzalgebraisch (in Ω).

Der Beweis erfolgt bei Siegel unter Ausnutzung des Satzes und der analytischen Methoden von Weil. Es ist uns auch hier gelungen, den Beweis für

$g = 1$ rein arithmetisch zu führen. Im allgemeinen Falle wollen wir diese Aufgabe im nächsten Semester angreifen. Allgemeinste descente infinie.

Der Siegelsche Beweis erfolgt so: aus der Annahme, $x(\mathfrak{p})$ sei ganz für unendlich viele Primdivisoren ersten Grades von K wird eine scharfe Approximation eines Systems über Ω algebraischer Zahlen $\alpha_1, \ldots, \alpha_g$ durch Zahlen $\frac{\xi_1}{\xi_0}, \ldots, \frac{\xi_g}{\xi_0}$ aus Ω konstruiert. Diese steht im Widerspruch zu einer Verallgemeinerung des Thue–Siegelschen Satzes. Diese Verallgemeinerung wird allerdings in der Siegelschen Arbeit nicht explizit ausgesprochen; sie ist dort in den recht komplizierten Beweis mittels der Thetafunktionen verwoben. Wir haben sie wie folgt herausgearbeitet:

> Ω algebraischer Zahlkörper vom Grade k
>
> $\alpha_1, \ldots, \alpha_g$ algebraische Zahlen, deren Körper $\Omega(\alpha_1, \ldots, \alpha_g)$ über Ω den Relativgrad r hat, und deren lineares Unabhängigkeitsmaß in bezug auf Ω gleich d ist (die Potenzprodukte bis zur Dimension d hin noch lin. unabh. über Ω).
>
> Wenn dann die Ungleichungen
>
> $$\left|\frac{\xi_i}{\xi_0} - \alpha_i\right| \leqq C \cdot N(X)^{-e} \left\{ \begin{array}{c} C \text{ positive Konstante} \\ X = \operatorname{Max}(|\xi_0|, |\xi_1|, \ldots, |\xi_g|) \end{array} \right\}$$
>
> unendlich viele Lösungen $\frac{\xi_1}{\xi_0}, \ldots, \frac{\xi_g}{\xi_0}$ in ganzen $\xi_0, \xi_1, \ldots, \xi_g$ aus Ω haben, so ist notwendig
>
> $$e \leqq \operatorname*{Min}_{\delta=0,1,\ldots,d} \left(\delta + \frac{kr}{\binom{g+\delta}{g}} \right).$$
>
> Für $g = 1$ wird $d = r - 1$ und
>
> $$e \leqq \operatorname*{Min}_{\rho=0,1,\ldots,r-1} \left(\rho + \frac{kr}{\rho + 1} \right).$$
>
> Das ist genau der Thue–Siegelsche Satz.

IV. Der Satz von E. Lutz.

Motivierung der Fragestellung: Zusammenhang zwischen Lösungsanzahl im Großen und Lösungsanzahlen im Kleinen bei quadratischen Gleichungen:

über Ω , über den $\wp$–adischen Erweiterungen $\Omega_\wp$, die den Primidealen und unendlichen Primstellen von Ω entsprechen

Entsprechend bei Frage der Zerfällung von Algebren.

Daher liegt es nahe, auch bei algebraischen Funktionenkörpern nach einem Zusammenhang zu fragen zwischen der Divisorenklassengruppe nullten Grades von

$$\mathsf{K} = \Omega(x, y) \quad \text{mit} \quad f(x, y) = 0,$$

und den Divisorenklassengruppen nullten Grades der $\wp$–adischen Erweiterungen

$$\mathsf{K}_\wp = \Omega_\wp(x, y) \quad \text{mit} \quad f(x, y) = 0.$$

In dieser Richtung ist bisher noch gar nichts bekannt. Ich sehe aber gerade in dieser Richtung den Zugang zu der erwünschten genaueren Einsicht in den Aufbau der Divisorenklassengruppe nullten Grades von K.

Als ersten Punkt eines Vorstoßes in dieser Richtung hat man die Divisorenklassengruppe einer einzelnen $\wp$–adischen Erweiterung $\mathsf{K}_\wp$ zu untersuchen. Das tut Frl. Lutz. Sie bestimmt die Struktur der Divisorenklassengruppe nullten Grades für einen algebraischen Funktionenkörper

$$\mathsf{K}_\wp = \Omega_\wp(x, y) \quad \text{mit} \quad f(x, y) = 0$$

über einem $\wp$–adischen Zahlkörper ($\wp$ Primideal von Ω) vom Geschlecht $g = 1$. Es stellt sich heraus, daß die Divisorenklassengruppe nullten Grades hier neben den ganzrationalen Zahlen auch die ganzen $\wp$–adischen Zahlen (aus $\Omega_\wp$) als Operatoren zuläßt, und daß sie als solche Operatorgruppe den *Rang* 1 hat. Man hat also eine eindeutige Basisdarstellung der Form

$$\mathfrak{p} \sim \mu_1\mathfrak{a}_1 + \mu_2\mathfrak{a}_2 + \nu\mathfrak{b} \ (\mathfrak{o}) \ \left\{ \begin{array}{c} \mu_i \bmod m_i \\ \nu \text{ ganz } \wp \text{ adisch, in } \Omega_\wp \end{array} \right\}.$$

Es erhebt sich weiter die Frage nach den Primdivisoren ersten Grades $\mathfrak{p}$, für die eine $\wp$–adisch ganzzahlige Weierstraßsche Normalerzeugung $y^2 = 4x^3 - g_2x - g_3$ ganzzahlige $\wp$–adische Lösungen hat. Darüber ist noch nichts bekannt.

Ebenso ist nicht bekannt, wie sich der Satz von Frl. Lutz auf beliebiges Geschlecht g verallgemeinert.

V. Der Satz von H. Hasse.

Eine noch gröbere Fragestellung ergibt sich, wenn man nur die Näherungswerte mod $\wp$ der $\wp$–adischen Zahlen betrachtet. Diese Untersuchung

spielt in der vorschwebenden Theorie dieselbe Rolle, wie die Kongruenztheorie der algebraischen Zahlen nach einer Primzahl. Man hat es dabei mit einem algebraischen Funktionenkörper

$$\mathsf{K} = \Omega(x, y) \quad \text{mit} \quad f(x, y) = 0$$

zu tun, dessen Konstantenkörper Ω ein endlicher Körper ist. Diese Theorie ist, auch abgesehen von der eben gegebenen Einordnung in die hier vorschwebende Theorie, interessant. Denn diese Körper K sind selbst weitgehend analog zu den algebraischen Zahlkörpern. Sie sind sogar einfacher als diese, weil für sie alle Bewertungen diskret sind, während bei den algebraischen Zahlkörpern endlich viele nicht–diskrete Bewertungen (unendliche Primstellen) auftreten. Anstelle der durch diese nicht–diskreten Bewertungen bedingten analytischen Approximationsaussagen (Minkowskische Diskriminantenabschätzungen u. s. w.) treten für die Körper K genaue Aussagen (Riemann–Rochscher Satz).

Diese größere Einfachheit äußert sich insbesondere in der Zetafunktion von K:

$$\zeta(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}} \,,$$

wo $\mathfrak{N}(\mathfrak{p}) = q^{f_\mathfrak{p}}$ die Elementanzahl des endlichen Restklassenkörpers $\Omega_\mathfrak{p}$ von K mod $\mathfrak{p}$ bezeichnet; q ist die Elementanzahl von Ω. Diese Funktion ist nämlich wesentlich ein Polynom in $\frac{1}{q^s}$:

$$\begin{aligned} \zeta(s) &= \zeta_0(s) L(s) \\ \zeta_0(s) &= \frac{1}{1 - \frac{1}{q^s}} \frac{1}{1 - \frac{q}{q^s}} \\ L(s) &= 1 + \frac{N_1 - (q+1)}{q^s} + \cdots + \frac{q^g}{q^{2gs}} \,, \end{aligned}$$

und zwar vom Grade $2g$. Der höchste Koeffizient ist q^g, der Koeffizient des linearen Gliedes $N_1 - (q+1)$, wo N_1 die Anzahl der Primdivisoren ersten Grades von K ist.

Die Riemannsche Vermutung für diese Zetafunktion ist gleichwertig mit der Aussage

$$|N_1 - (q+1)| \leqq 2g q^{\frac{1}{2}}$$

(für Ω und alle endlichen Erweiterungskörper in der Rolle von Ω). N_1 ist wesentlich die Anzahl der Lösungen von $f(x, y) = 0$ im endlichen Körper Ω, der

unter Hinzunahme des ebenfalls zu betrachtenden ∞ die Elementanzahl $q+1$ hat; $q+1$ ist also der wahrscheinliche Wert für N_1, und die Riemannsche Vermutung ist gleichwertig mit der angegebenen Abschätzung der Abweichung zwischen N_1 und seinem wahrscheinlichen Wert $q+1$.

Es ist mir gelungen, diese Riemannsche Vermutung für $g = 1$ zu beweisen, und zwar nicht etwa durch Bestätigung der Abschätzung sondern als eine Strukturaussage. Für $g = 1$ ist $N_1 = h$ die Anzahl der Divisorenklassen nullten Grades von K, und mein Satz kann als eine genaue Bestimmung dieser Anzahl angesehen werden; so ordnet er sich den Sätzen von A. Weil, C. Siegel, E. Lutz zur Seite, die ja sämtlich Aussagen über die Divisorenklassengruppe nullten Grades sind.

Diese Deutung der Riemannschen Vermutung und mein Beweis stützen sich auf die allgemeine Theorie der Korrespondenzen in algebraischen Funktionenkörpern, die kürzlich von M. Deuring in einer für den vorliegenden Zweck brauchbaren rein algebraischen Form entwickelt wurde.

Funktionentheoretisch gesagt ist eine Korrespondenz von K eine konforme Abbildung einer Überlagerungsfläche von $\mathfrak{R}$ auf eine andere solche (je mit endlicher Überlagerungszahl). Sie bewirkt eine Operation vom Typus einer Multiplikation im Perioden–Parallelotop (komplexe Multiplikation) und damit eine abstrakte Operatormultiplikation in der Divisorenklassengruppe nullten Grades von K. Deuring hat gezeigt, wie man diese Operationen bei beliebigem Konstantenkörper rein algebraisch einführen kann.

Man erhält so zu jedem algebraischen Funktionenkörper $\overline{\mathsf{K}}$ einen abstrakten Ring M, den *Multiplikatorenring* von $\overline{\mathsf{K}}$, der aus Operationen μ vom Typus einer Multiplikation in der Divisorenklassengruppe nullten Grades von $\overline{\mathsf{K}}$ besteht. Durch den Querstrich haben wir angedeutet, daß zur Definition dieses Ringes M der Konstantenkörper Ω durch seine algebraisch–abgeschlossene Hülle $\overline{\Omega}$ ersetzt wird. Für $g = 1$ im klassischen Falle ist dieser Ring M das algebraische Äquivalent derjenigen Multiplikationen μu, die für u als Element des Periodenparallelogramms eindeutig erklärt sind (komplexe Multiplikation im klassischen Sinne).

Im allgemeinen ist M nicht kommutativ. M besitzt einen involutorischen Antiautomorphismus, der Umkehrung der Korrespondenzrichtung entsprechend. M hat ferner stets die Charakteristik 0, enthält also den Ring Γ der ganzrationalen Zahlen (natürliche Multiplikation, wie sie vorher schon mehrfach in der Divisorenklassengruppe nullten Grades auftrat). Die Elemente μ von M stellen sich rein algebraisch dar als die Substitutionen einer Normalerzeugung

$x; y_1, \ldots, y_n$ von K mit Multiplikationsschema (M) in Systeme $\xi; \eta_1, \ldots, \eta_n$ die (M) befriedigen und von $x; y_1, \ldots, y_n$ algebraisch (mit Koeffizienten aus $\overline{\Omega}$) abhängen; man nennt solche Substitutionen *Meromorphismen.*

Für $g = 1$ kann man zeigen, daß jedes Element μ aus M zusammen mit $\overline{\mu}$ einer quadratischen Gleichung mit Koeffizienten aus Γ genügt, und daß $\mu\overline{\mu} = N(\mu)$ (für $\mu \neq 0$) ein gewisser Körpergrad ist und daher stets positiv ist. Daraus folgt, daß sich $\mu, \overline{\mu}$ formal wie konjugiert–komplexe Zahlen verhalten.

Im Falle eines endlichen Körpers Ω ist nun

$$(x, y) \longrightarrow (x^q, y^q)$$

ein Meromorphismus π von $\overline{\mathsf{K}}$, weil dabei die Grundgleichung $f(x, y)$ erhalten bleibt. Der fragliche Körpergrad ist hier $N(\pi) = q$. Die Wirkung von π in der Divisorenklassengruppe nullten Grades von $\overline{\mathsf{K}}$ stellt sich so dar:

$$\overline{\mathfrak{p}} \longleftrightarrow (\overline{a}, \overline{b}) \ , \qquad \pi\overline{\mathfrak{p}} \longleftrightarrow (a^q, b^q).$$

Es ist also $(\pi - 1)\overline{\mathfrak{p}} \sim \mathfrak{o}$ dann und nur dann, wenn $\overline{\mathfrak{p}} = \mathfrak{p}$ ein Primdivisor ersten Grades von K selbst ist, d. h. die $N_1 = h$ Primdivisoren ersten Grades $\mathfrak{p}$ von K sind innerhalb aller $\overline{\mathfrak{p}}$ von $\overline{\mathsf{K}}$ durch $(\pi - 1)\overline{\mathfrak{p}} \sim \mathfrak{o}$ gekennzeichnet $\big((\pi - 1)$–te Teilwerte!$\big)$. Daraus folgert man $N(\pi - 1) = N_1 = h$.

Zusammengenommen bestimmt sich damit die quadratische Gleichung für π so:

$$\pi^2 + \big(N_1 - (q + 1)\big)\pi + q = 0.$$

Vergleich mit dem Polynom

$$q^{2s}L(s) = q^{2s} + \big(N_1 - (q + 1)\big)q^s + q$$

zeigt, daß dieses Polynom konjugiert–komplexe Wurzeln hat. Dies besagt

$$|N_1 - (q + 1)| \leqq 2gq^{\frac{1}{2}},$$

also die Riemannsche Vermutung.

Als Aussage über die Divisorenklassengruppe nullten Grades von K kann diese Riemannsche Vermutung so ausgesprochen werden: diese Gruppe ist die in der Divisorenklassengruppe nullten Grades von $\overline{\mathsf{K}}$ durch den Operator $\pi - 1$ annullierte Gruppe, und dabei ist π formal eine der beiden Nullstellen der Zetafunktion.

Ein umfangreicher Teil dieses Beweises läßt sich auf $g > 1$ übertragen. Ich kann aber für $g > 1$ bisher nicht zeigen, daß die Operatoren μ algebraische Gleichungen vom Grade $2g$ mit Koeffizienten aus Γ genügen und daß dabei $\mu \longrightarrow \overline{\mu}$ formal der Übergang zum Konjugiert–komplexen ist.

Grob gesagt ist die Riemannsche Vermutung für Kongruenzfunktionenkörper im Falle $g = 1$ das Äquivalent zu der Tatsache, daß im klassischen Falle der Periodenquotient $\frac{\omega_2}{\omega_1}$ von Null verschiedenen Imaginärteil hat. Für $g > 1$ ist die Verallgemeinerung dazu im klassischen Falle, daß für die Periodenmatrix (W_1, W_2) der Quotient $W_1^{-1}W_2$ eine Matrix ist, deren Imaginärteil eine definite quadr. Form hat. Das Äquivalent hierzu ist die Riemannsche Vermutung für Kongruenzfunktionenkörper im Falle $g > 1$. Das zum Beweis noch zu leistende Kunststück besteht darin, für diese Tatsache im klassischen Falle eine rein algebraische Deutung zu geben.

VI. Der Satz von M. Deuring.

Ist k ein imaginär–quadratischer Zahlkörper und ω_1, ω_2 eine Basis der ganzen Zahlen (oder eines Ideals) von k, so entsteht aus k durch Adjunktion von $j(\omega_1, \omega_2)$ bekanntlich der absolute Klassenkörper K von k.

Deuring hat diesem 1. Hauptsatz der komplexen Multiplikation durch seine rein–algebraische Theorie des Multiplikatorenrings eine neue Beleuchtung und gleichzeitig einen rein–algebraischen Beweis gegeben. In derselben Weise hat er auch den 2. Hauptsatz der komplexen Multiplikation, der die Strahlklassenkörper betrifft, rein algebraisch bewiesen. Seine Methode besteht in der Herstellung eines Zusammenhangs zwischen dem Multiplikatorenring von K bei endlich–algebraischem Konstantenkörper Ω und dem Multiplikatorenring eines Kongruenzfunktionenkörpers $\mathsf{K}_\wp$ der sich durch Übergang zu einem Restklassenkörper $\Omega_\wp$ nach einem Primideal $\wp$ von Ω ergibt.

Deuring besitzt ferner Ansätze zur Verallgemeinerung dieser Beweise auf beliebiges Geschlecht $g \geqq 1$. Die Durchführung zielt hier auf die Lösung des Hilbertschen Problems der Klassenkörperkonstruktion durch automorphe Funktionen ab. Dabei werden aber diese automorphen Funktionen rein algebraisch gefaßt. Deuring hofft so die Schwierigkeiten zu überwinden, die sich bisher der Lösung dieses Problems auf analytischem Wege entgegengestellt haben.

Deurings Ergebnisse sind insofern noch unvollständig, als sie von einem gegebenen Funktionenkörper und seinem Multiplikatorenring ausgehen. Es entsteht die sehr tiefliegende Frage, welche Ringe M als Multiplikatorenringe

auftreten, also die Frage der Existenz eines algebraischen Funktionenkörpers zu vorgegebenem Multiplikatorenring.

Schluß.

Der hauptsächliche Zweck dieses Vortrages war, einmal die verschiedenen mehr oder weniger kurz berührten Sätze und Fragestellungen in einem einheitlichen Rahmen auszusprechen und gegenüberzustellen. Wie schon in der Einleitung gesagt, ist es meine Überzeugung, daß diese und manche andere hier nicht berührten Gedankengänge im Laufe der nächsten Zukunft immer mehr zu einem einheitlichen von organischen Sätzen beherrschten Gebiet der Zahlentheorie verschmelzen werden. Ich glaube, daß es für den Forscher gut ist, sich gelegentlich einmal auf die Zusammenhänge *im Großen* seines Arbeitsgebiets zu besinnen, und sich nicht völlig in die Einzelarbeit *im Kleinen* zu verlieren. Sonst wird ihm schnell der Boden unter den Füßen verschwinden, und er wird den Kontakt mit der Welt des Wirklichen und Greifbaren in seinem Gebiet verlieren.

1.20 HU Berlin 1953

(Vortrag 1. Math. Inst. Humboldt Univ. Berlin) 3. März 1953

Riemannsche Vermutung in Kongruenzfunktionenkörpern.

(*Nach P. Roquette*)

I. Arithmetische Formulierung.

Ω_1 endlicher Körper von q Elementen

K_1/Ω_1 algebr. Funktionenkörper über Ω_1 als Konstantenkörper, Erzeugung $f(t,u)=0$, abs. irr. über Ω_1
Geschlecht g.

$$\zeta_{\mathsf{K}_1}(s)=\sum_{\mathfrak{g}\text{ ganz}}\frac{1}{\mathfrak{N}(\mathfrak{g})^s}=\sum_{n=0}^{\infty}\frac{N_n}{q^{ns}}=\sum_{n=0}^{\infty}\frac{N_n}{z^n}=\mathsf{Z}_{\mathsf{K}_1}(z)\qquad(q^s=z)$$

wo $N_n=$ Anzahl der gz. Div. n–ten Grades von K_1/Ω_1,
speziell $N_1=$ Anzahl der Primdiv. 1–ten Grades von K_1/Ω_1

Speziell für $g=0$, also $\mathsf{K}_1=\mathsf{P}_1=\Omega_1(t)$ ist $N_n=\frac{q^{n+1}-1}{q-1}$, und daher

$$\zeta_{\mathsf{P}_1}(s)=\frac{1}{1-\frac{1}{q^s}}\,\frac{1}{1-\frac{q}{q^s}}=\frac{1}{1-\frac{1}{z}}\,\frac{1}{1-\frac{q}{z}}=\mathsf{Z}_{\mathsf{P}_1}(z)$$

Nach R. R. Satz erkennt man

$$\ell_{\mathsf{K}_1}(s)=\frac{\zeta_{\mathsf{K}_1}(s)}{\zeta_{\mathsf{P}_1}(s)}=1+\frac{N_1-(q+1)}{z}+\cdots+\frac{q^g}{z^{2g}}=L_{\mathsf{K}_1}(z),$$

also

$z^{2g}L_{\mathsf{K}_1}(z)$ normiertes Polynom in $z=q^s$ vom Grad $2g$

mit

$$\text{Nullstellensumme}=(q+1)-N_1=$$
$$=\text{Fehlerglied der Anzahl } N_1 \text{ gegen Mittelwert } q+1$$

Riem. Verm. besagt (im Falle $g \geqq 1$) für die $2g$ Nullstellen:

$$\mathfrak{R}(s) = \frac{1}{2} \longleftrightarrow |q^s| = q^{\frac{1}{2}},$$

also Fehlerabschätzung

$$|(q+1) - N_1| \leqq 2g\, q^{\frac{1}{2}}.$$

Ähnlich wie bei gew. Riem. Verm. und Primzahlsatz ist auch hier diese Fehlerabschätzung *äquivalent* mit Riem. Vermutung, wenn man sie für *alle* endl. Körper Ω_1 hat. Bei Übergang zu endl. Konst. Erw. K_r/Ω_r vom Grade r gilt nämlich:

$$\mathsf{Z}_{\mathsf{K}_r}(z^r) = \prod_{\zeta^r=1} \mathsf{Z}_{\mathsf{K}_1}(\zeta z)$$

$$L_{\mathsf{K}_r}(z^r) = \prod_{\zeta^r=1} L_{\mathsf{K}_1}(\zeta z)$$

Nullstellen in $z^r = q^{rs}$ von $z^{2gr} L_{\mathsf{K}_r}(z^r) = r$–te Potenzen der Nullstellen in $z = q^s$ von $z^{2g} L_{\mathsf{K}_1}(z)$.

Nullstellensumme $= (q^r + 1) - N_1^{(r)}$

Weiß man

$$|(q^r + 1) - N_1^{(r)}| \leqq 2g\, q^{\frac{r}{2}}$$

für alle r, so folgt Riem. Verm. für die Nullstellen von $z^{2g} L_{\mathsf{K}_1}(z)$.

II. Hilfsmittel zum Roquetteschen Beweis.

Betrachte algebr. abgeschl. Konstantenerweiterung K/Ω von K_1/Ω_1. Jeder Primdivisor n–ten Grades $\mathfrak{o}_1$ von K_1/Ω_1 zerfällt in n verschiedene Primdivisoren 1–ten Grades von K/Ω (sogar schon von K_n/Ω_n). Primdivisoren 1. Grades $\mathfrak{o}_1$ von K_1/Ω_1 sind dadurch gekennzeichnet, daß sie in K/Ω unzerlegt bleiben. Dies äußert sich in ihrem Restklassenkörper dadurch, daß die $\mathfrak{o}_1$–ganzen Elemente aus K_1 Reste in Ω_1 haben.

Bilde den Doppelkörper (zunächst mit *irgendzwei* K/Ω, K'/Ω)

$$\Delta = \mathsf{K} \times \mathsf{K}' = \Omega(t, u; t', u') \quad \text{mit} \quad \left\{ \begin{array}{c} f(t,u) = 0 \\ f'(t',u') = 0 \end{array} \right\}$$

(t', u') von (t, u) algebr. unabh.

Primdivisoren von Δ/Ω entstehen aus den Primpolynomen des rationalen Doppelkörpers

$$\Delta_0 = \mathsf{P} \times \mathsf{P}' = \Omega(t, t')$$

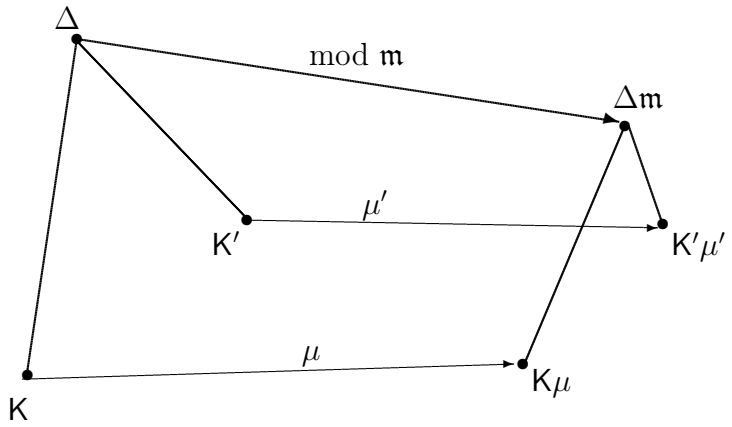
durch Bew. Forts. bei endl. algebr. Erw. Entsprechend den drei Primpolynomsorten

$$p(t), \quad p(t'), \quad p(t, t')(\textit{binär})$$

gibt es drei Primdivisorsorten

$$\mathfrak{p} \text{ schon von } \mathsf{K}/\Omega, \quad \mathfrak{p}' \text{ schon von } \mathsf{K}'/\Omega, \quad \mathfrak{m} \textit{ binär.}$$

Binäre Primdiv. $\mathfrak{m}$ entsprechen umkehrbar eindeutig den durch Restklassenbildung mod $\mathfrak{m}$ gelieferten Isomorphismenpaaren μ, μ' von K/Ω, K'/Ω nach folgendem Schema:



$$gr_{\Delta/\mathsf{K}'}(\mathfrak{m}) = [\Delta\mathfrak{m} : \mathsf{K}\mu]\,,$$
$$gr_{\Delta/\mathsf{K}}(\mathfrak{m}) = [\Delta\mathfrak{m} : \mathsf{K}'\mu']\,.$$

Dabei μ, μ' nur bis auf willk. ([...]) Isomorphismen der gew. alg. Fkt. Kp. $\Delta\mathfrak{m}/\Omega$ bestimmt. Man kann normieren:

$$\mu' = 1, \qquad \mathsf{K}'\mu' = \mathsf{K}'.$$

Dann die μ als Isom. von K/Ω in endl. alg. Erw. von K' bestimmt, wobei es auf die Unterscheidung K'–konj. μ, d. h. K'–konj. Bildkörper $\mathsf{K}\mu$ nicht ankommt.

Formale Zusammensetzung der Primdivisoren liefert die volle Divisorengruppe von Δ/Ω.

Darin Klassenbildung nach

$$\left\{ \begin{array}{c} \text{Hauptdivisoren (\textit{gew.} Klassen)} \\ \text{Hauptdiv. u. Div. von } \mathsf{K}/\Omega,\ \mathsf{K}'/\Omega \text{ (\textit{gröbere} Kl.)} \end{array} \right\}.$$

Bei letzteren kokmmt es nur auf den linearen Bestandteil an.
Schreibweise der Divisoren *additiv*.

Roquette definiert nun für je zwei zueinander prime Divisoren $\mathfrak{a}, \mathfrak{b}$ von Δ/Ω ein

$$\textit{Restprodukt} \qquad \langle \mathfrak{a}, \mathfrak{b} \rangle = \langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathsf{K}} + \langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathsf{K}'}$$

als direkte Summe zweier Divisoren von $\mathsf{K}/\Omega, \mathsf{K}'/\Omega$ mit folgenden Eigenschaften:

$$\begin{aligned} \langle \mathfrak{a}, \mathfrak{b} \rangle &\quad \text{bilinear in } \mathfrak{a}, \mathfrak{b}, \\ \langle \mathfrak{a}, \mathfrak{b} \rangle &\quad \text{symmetrisch in } \mathfrak{a}, \mathfrak{b}, \\ \langle \mathfrak{a}, \mathfrak{b} \rangle &\quad \text{klasseninvariant für gew. Div. Klassen,} \\ gr\, \langle \mathfrak{a}, \mathfrak{b} \rangle &= gr_{\mathsf{K}/\Omega}\, \langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathsf{K}} = gr_{\mathsf{K}'/\Omega}\, \langle \mathfrak{a}, \mathfrak{b} \rangle_{\mathsf{K}'} \end{aligned}$$

Die Definition stützt sich auf eine Theorie der Divisorrestbildung:

$\mathfrak{a}\mathfrak{n}$ = Divisor von $\Delta\mathfrak{n}/\Omega$, der durch lokale g. g. T.–Bildung aus den Resten $a\mathfrak{n}$ für die Elemente a eines lokalen Vielfachenideals zu $\mathfrak{a}$ erhalten wird.

Man setzt dann (für binäre Primdivisoren $\mathfrak{n}$):

$$\begin{aligned} \langle \mathfrak{a}, \mathfrak{n} \rangle &= N_{\Delta\mathfrak{n}/\mathsf{K}\nu}(\mathfrak{a}\mathfrak{n})\nu^{-1} + N_{\Delta\mathfrak{n}/\mathsf{K}'\nu'}(\mathfrak{a}\mathfrak{n})\nu'^{-1} \\ &= \langle \mathfrak{a}, \mathfrak{n} \rangle_{\mathsf{K}} + \langle \mathfrak{a}, \mathfrak{n} \rangle_{\mathsf{K}'} \end{aligned}$$

und in den ausgearteten Fällen sinngemäß.

Die *Symmetrie* des Restprodukts beruht auf einer anderen Darstellung, die auch als Definition genommen werden kann. Für zwei verschiedene binäre Primdivisoren $\mathfrak{m}, \mathfrak{n}$ ist nämlich bei K–Normierung:

$$\mathfrak{m}\mathfrak{n} = \sum_{\mu} \mathfrak{D}_{\mu,\nu}$$

$$\langle \mathfrak{m}, \mathfrak{n} \rangle_{\mathsf{K}'} = \mathfrak{R}_{\underline{\mu},\underline{\nu}} = \sum_{\mu,\nu} \mathfrak{D}_{\mu,\nu}\ ,$$

wo $\underline{\mu}, \underline{\nu}$ die vollen Systeme K'–konj. Isom. μ, ν zu $\mathfrak{m}, \mathfrak{n}$ durchlaufen und $\mathfrak{D}_{\mu,\nu}$ die *Differente* des Isomorphismenpaares μ, ν bedeutet, letztere nach dem Schema der gewöhnlichen lokalen Differententheorie definiert; $\mathfrak{R}_{\underline{\mu},\underline{\nu}}$ dann die *Resultante* der Is. Systeme $\underline{\mu}, \underline{\nu}$.

Die *Klasseninvarianz* des Restprodukts erlaubt es, für die gewöhnlichen Divisorenklassen A, B von Δ/Ω einschränkungslos ein *Klassenrestprodukt*

$$\langle A, B\rangle = \langle A, B\rangle_{\mathsf{K}} + \langle A, B\rangle_{\mathsf{K}'}$$

zu definieren, als direkte Summe zweier Klassen von $\mathsf{K}/\Omega, \mathsf{K}'/\Omega$. Insbesondere findet sich dabei für eine Klasse M, die einem binären Primdivisor $\mathfrak{m}$ vom K'–Grad 1 entspringt, die Formel

$$\langle M, M\rangle = -\langle W, M\rangle = -gr_{\Delta/\mathsf{K}}(\mathfrak{m})W - W\mu,$$

wo W die Diff. Klasse von K/Ω (als solche von Δ/K').

Aus diesem Klassenrestprodukt entspringt eine invariante ganzrationalwertige Metrik

$$gr\,\langle A, B\rangle = gr_{\mathsf{K}/\Omega}\,\langle A, B\rangle_{\mathsf{K}} = gr_{\mathsf{K}/\Omega}\,\langle A, B\rangle_{\mathsf{K}'}$$

in der gew. Div. Klassengruppe von Δ/Ω, wobei kurz

$$\textit{Metrik} = \text{bilineare, symmetr. Zahlfunktion.}$$

Grob gesagt handelt es sich um die Metrik aus den *Schnittpunktzahlen* der durch die Divisoren $\mathfrak{a}, \mathfrak{b}$ definierten *Kurven* auf der durch den Doppelkörper $\Delta = \mathsf{K} \times \mathsf{K}'$ definierten *zylindrischen Fläche* des vierdimensionalen Raums, genauer Schnittpunktszahlen der Kurven*klassen*, so daß auch Schnittpunkte einer Kurve mit sich selbst (Doppelpunkte!) vernünftig definiert.

Dieser *nichttrivialen* Metrik steht eine *triviale* Metrik zur Seite, nämlich

$$gr\{A, B\} = gr_{\Delta/\mathsf{K}}(A)gr_{\Delta/\mathsf{K}'}(B) + gr_{\Delta/\mathsf{K}'}(A)gr_{\Delta/\mathsf{K}}(B).$$

Im Falle eines rationalen Doppelkörpers stimmen die beiden Metriken überein. Im nicht–rationalen Falle ist die von *A. Weil* eingeführte Differenzmetrik

$$\delta(A, B) = gr\{A, B\} - gr\,\langle A, B\rangle$$

von grundlegender Bedeutung. Sie mißt, um wieviel geringer (oder größer) die Schnittpunktzahl im algebraischen Falle gegenüber dem rationalen Fall

ist, ähnlich wie das Geschlecht angibt, um wieviel geringer die wahre Doppelpunktanzahl gegenüber der dem Grade nach zu erwartende Doppelpunktanzahl ist.

Diese Metrik ist *klasseninvariant im gröberen Sinne.*

Durch eine auf den R. R. Satz gestützte genaue Abschätzung des Grades der Diskriminante

$$\mathfrak{d}_{\underline{\mu}} = \sum_{\mu \neq \mu'} \mathfrak{D}_{\mu,\mu'}$$

für ein volles Isomorphismensystem $\underline{\mu}$ von K/Ω in $\overline{\mathsf{K}}'/\Omega$ zu einem Primdivisor $\mathfrak{m}$ oder allg. ganzen Divisor $\mathfrak{a}$ von $\overline{\Delta}/\Omega$ beweist nun Roquette die grundlegende Tatsache, daß die *Weilsche Metrik positiv–definit* ist:

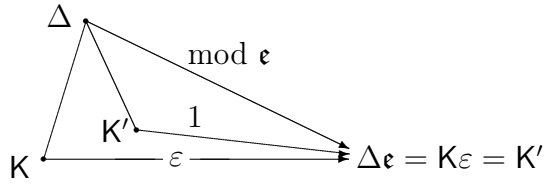
$$\delta(A, A) > 0 \quad \text{für} \quad A \not\approx 0.$$

III. Skizze des Roquetteschen Beweises.

Jetzt wird K'/Ω als zweites, algebr. unabh. Exemplar von K/Ω angenommen. Dann hat man also einen

$$\text{Isom. } \varepsilon \text{ von } \mathsf{K}/\Omega \text{ auf } \mathsf{K}'/\Omega, \text{ def. durch } (t, u)\varepsilon = (t', u').$$

Er definiert Primdivisor $\mathfrak{e}$ von Δ/Ω nach dem Schema:



mit

$$\begin{array}{lll} gr_{\Delta/\mathsf{K}}(\mathfrak{e}) = 1, \quad gr_{\Delta/\mathsf{K}'}(\mathfrak{e}) = 1, & gr\{E, E\} & = \quad 2 \\ \langle E, E\rangle = -W - W\varepsilon, & gr\,\langle E, E\rangle & = \quad -2g + 2 \\ & \hline \delta(E, E) & = \quad 2g \end{array}$$

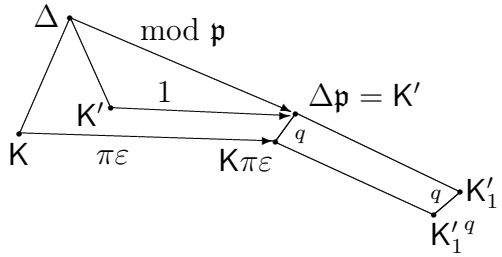
Ferner besitzt K/Ω einen Isomorphismus π in sich, def. durch

$$\mathsf{K}\pi = \mathsf{K}^q, \quad \text{explizit} \quad (t, u)\pi = (t^q, u^q).$$

Dann

$$\mathsf{K}\pi\varepsilon = \mathsf{K}'^q, \quad \text{explizit} \quad (t, u)\pi\varepsilon = (t'^q, u'^q)$$

ein Isom. $\pi\varepsilon$ von K/Ω in K'/Ω. Er definiert Primdivisor $\mathfrak{p}$ von Δ/Ω nach dem Schema:



mit

$$\begin{aligned} gr_{\Delta/\mathsf{K}}(\mathfrak{p}) = q, \quad gr_{\Delta/\mathsf{K}'}(\mathfrak{p}) = 1, \quad gr\{P,P\} &= 2q \\ \langle P,P\rangle = -gr_{\Delta/\mathsf{K}}(\mathfrak{p})W - W\pi\varepsilon, \quad gr\,\langle P,P\rangle &= -q(2g-2) \\ \hline \delta(P,P) &= 2qg \end{aligned}$$

Es interessiert dann noch das Restprodukt $\langle \mathfrak{e},\mathfrak{p}\rangle = \langle E,P\rangle$. Da beide $\mathfrak{e},\mathfrak{p}$ vom Grad 1 über K', ist einfach die Komp.

$$\langle \mathfrak{e},\mathfrak{p}\rangle_{\mathsf{K}'} = \mathfrak{D}_{\varepsilon,\pi\varepsilon} = \mathfrak{D}_{1,\pi}\varepsilon.$$

Nun

$$\begin{aligned} \mathfrak{o} \mid \mathfrak{D}_{1,\pi} \longleftrightarrow\ & a \equiv a\pi \mod \mathfrak{o} \text{ für alle } \mathfrak{o}\text{–ganzen } a \text{ aus } \mathsf{K} \\ \text{d. h.}\quad & a_1 \equiv a_1^q \mod \mathfrak{o} \text{ für alle } \mathfrak{o}\text{–ganzen } a_1 \text{ aus } \mathsf{K}_1 \\ \text{d. h.}\quad & \text{Restkl. Kp. mod } \mathfrak{o} \text{ von } \mathsf{K}_1/\Omega \text{ fällt mit } \Omega \text{ zusammen} \\ \text{d. h.}\quad & \mathfrak{o} = \mathfrak{o}_1 \text{ Primdiv. ersten Grades von } \mathsf{K}_1/\Omega \\ & \text{(wie sie für Riem. Verm. in } N_1 \text{ zu zählen).} \end{aligned}$$

Genauer für einen solchen die $a_1 - a_1\pi = a_1 - a_1^q$ gemeinsam nur einfach durch $\mathfrak{o}$ teilbar, also

$$\mathfrak{D}_{1,\pi} = \sum_{\mathfrak{o}_1} \mathfrak{o}_1\,, \qquad gr_{\mathsf{K}/\Omega}(\mathfrak{D}_{1,\pi}) = N_1.$$

Damit

$$\begin{aligned} gr\{\mathfrak{o},\mathfrak{p}\} &= q+1 \\ gr\,\langle \mathfrak{o},\mathfrak{p}\rangle &= N_1 \\ \hline \delta(E,P) &= q+1-N_1 \\ &= \text{abzuschätzendes Fehlerglied.} \end{aligned}$$

Nun wird Hauptsatz über die Weilsche Metrik ausgenutzt. Bei einer pos. def. Metrik $\delta(A,B)$ (sogar schon bei pos. semidef.) gilt:

$$G(m,n) = \delta(mA+nB, mA+nB) \geqq 0 \quad \text{für alle ganzen } m,n,$$

also Schwarzsche Ungleichung

$$\begin{vmatrix} \delta(A,A) & \delta(A,B) \\ \delta(A,B) & \delta(B,B) \end{vmatrix} \geqq 0.$$

Hier

$$0 \leqq \begin{vmatrix} \delta(E,E) & \delta(E,P) \\ \delta(E,P) & \delta(P,P) \end{vmatrix} = \begin{vmatrix} 2g & (q+1)-N_1 \\ (q+1)-N_1 & 2qg \end{vmatrix}$$
$$= (2g)^2 q - \big((q+1)-N_1\big)^2,$$

w. z. b. w.

1.21 Akad. Berlin 1953

5. März 1953

Riemannsche Vermutung für Funktionenkörper.

Vortrag Deutsche Akad. d. Wiss. Berlin

1. Gewöhnliche Riemannsche Vermutung.

Verteilung der Primzahlen in der Folge der natürlichen Zahlen.

Gauss: Vermutete auf Grund experimenteller Auszählung, daß Dichte der Primzahlen in der Umgebung einer Stelle x (d. h. auf Intervall der Länge 1 bezogenen Anzahl) ungefähr $\frac{1}{\log x}$ ist, und daher Gesamtanzahl der Primzahlen unter x ungefähr

$$\pi(x) \sim \int_0^x \frac{dx}{\log x} = \mathrm{Li}(x) \qquad \text{(Integrallogarithmus)}.$$

Hadamard–de Vallée Poussin: Bewiesen das strenge, und zwar in dem Sinne, daß

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1.$$

Blieb die Frage, wie genau die Annäherung von $\mathrm{Li}(x)$ an $\pi(x)$ ist, d. h. wie groß der Fehler

$$\pi(x) - \mathrm{Li}(x)$$

höchstens werden kann.

Riemann: Hatte schon vorher gezeigt, daß dies Problem aufs Engste mit den Nullstellen der Zetafunktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

als Funktion der komplexen Variablen s zusammenhängt. Seine Vermutung war, daß diese Nullstellen (von trivialen negativen abgesehen) alle auf der Geraden

$$s = \frac{1}{2} + it$$

liegen. Diese berühmte *Riemannsche Vermutung* hat bisher allen Beweisversuchen getrotzt. Ist wohl das schwerste unter den zahlreichen noch ungelösten Problemen der modernen Mathematik.

Man weiß aber heute, daß die Riemannsche Vermutung völlig äquivalent ist mit der folgenden genauen Abschätzung des obigen „Fehlers“ bei der Primzahlverteilung

$$|\pi(x) - \mathrm{Li}(x)| \leqq c\sqrt{x}\log\, x, \quad \text{kurz} \quad \mathfrak{O}(\sqrt{x}\log\, x)$$

Das ist genau die Größenordnung des Fehlers, die man nach dem „Gesetz der großen Zahlen“ aus der Statistik zu erwarten hat, wenn die Verteilung der Primzahlen eine völlig regellose, zufällige ist.

So ist die Riemannsche Vermutung mit dem statistischen Problem äquivalent, die völlige Regellosigkeit der Verteilung der Primzahlen streng nachzuweisen.

2. Riemannsche Vermutung in Funktionenkörpern.

Nun gibt es andere zahlentheoretische Probleme, die ebenfalls von solcher statistischer Natur sind, und die etwas leichter angreifbar erscheinen.

Ich will hier über ein solches Problem sprechen, das in ganz analoger Weise mit einer Zetafunktion und Riemannschen Vermutung verknüpft ist, und bei dem man in der letzten Zeit die vollständige Lösung gefunden hat.

Gegeben sei eine *ganzzahlige algebraische Gleichung*

$$f(x, y) = 0$$

in zwei Variablen x, y. Genauer: es sei $f(x, y)$ ein Polynom, das aus Gliedern der Gestalt

$$a_{\mu\nu}x^{\mu}y^{\nu} \qquad (\mu = 0, \ldots, m; \nu = 0, \ldots, n)$$

aufgebaut ist, und dabei seien die Koeffizienten $a_{\mu\nu}$ ganze rationale Zahlen.

Ferner sei irgendeine Primzahl p gegeben. Man rechne nun nicht mit der gewöhnlichen Gleichheit $f(x, y) = 0$, sondern mit der *Kongruenz* mod p, d. h. der Gleichheit der Reste bei der Division durch p, also etwa für $p = 2$ mit den beiden Resten $0, 1$ als Repräsentanten der Alternative gerade–ungerade:

$$f(x, y) \equiv 0 \mod p.$$

Dann kann man die Variablen x, y auf die je p Werte $0, 1, \ldots, p-1$ beschränken.

Man interessiert sich dann für die *Anzahl N der Lösungen dieser Kongruenz* mod p.

Man setzt dabei zweckmäßig voraus, daß das Polynom $f(x, y)$ *irreduzibel* ist, d. h. nicht in „kleinere“ Polynome aufgespalten werden kann. Seine „Schwierigkeitsstufe“ wird dann durch eine bestimmte ganze Zahl g gemessen, die man das *Geschlecht* des Polynoms nennt, und die sich grob gesagt aus der Anzahl der Doppelpunkte der Kurve $f(x, y) = 0$ bestimmt.

Ferner ist es zweckmäßig auch die in bestimmter Weise (projektive Geometrie) definierten *unendlichen Lösungen* mitzuzählen, also für die Variablen x, y auch noch das Symbol ∞ zuzulassen.

Jede der Variablen x, y durchläuft dann $p + 1$ Werte $0, 1, \ldots, p - 1, \infty$. Die geforderte Kongruenz

$$f(x, y) \equiv 0 \mod p$$

legt aber durchschnittlich zu jedem Wert von x einen Wert von y fest, genauer natürlich für manche x kein y, dafür für andere x mehrere y. Roh geschätzt hat man daher $p + 1$ Lösungen zu erwarten. Die genaue Lösungsanzahl N wird davon abweichen, und die Frage ist, wie groß dieser Fehler

$$N - (p + 1)$$

sein kann.

Man kann sich nun, wie gesagt, auch zu diesem Problem eine Zetafunktion konstruieren und zeigen, daß ein ganz entsprechender Zusammenhang zwischen der Größe des genannten Fehlers und der Lage der Nullstellen dieser Zetafunktion besteht, wie im Falle der Primzahlverteilung und der gewöhnlichen Riemannschen Vermutung. Dieses Analogon zur Riemannschen Vermutung ist völlig äquivalent mit der Fehlerabschätzung

$$|N - (p + 1)| \leqq 2g\sqrt{p}.$$

Denkt man sich ein u. dasselbe Polynom $f(x, y)$ nacheinander für *alle* unendlich vielen Primzahlen p betrachtet, so ist das wieder eine Fehlerabschätzung von der Größenordnung $\mathcal{O}(\sqrt{p})$, wie sie nach dem statistischen Gesetz der großen Zahlen zu erwarten ist, wenn die Verteilung der Lösungen eine völlig regellose, zufällige ist.

3. Methoden zum Beweis der Riemannschen Vermutung.

Dies Problem wurde zuerst von *Artin* 1921 in seiner Dissertation aufgeworfen, dort allerdings nur im einfachsten (nichttrivialen) Spezialfall des Geschlechtes $g = 1$, dann einige Jahre später allgemein von *F. K. Schmidt*. In dem Artinschen Spezialfall $g = 1$ gelang mir 1934 die Lösung mittels der Theorie der *elliptischen Funktionen*.

Während des Krieges fand *A. Weil* die Lösung für den allgemeinen Fall. Diese hat er nach dem Kriege in einer großen Abhandlung publiziert. Sie stützt sich auf die von ihm entwickelte neue Begründung der *algebraischen Geometrie in abstrakten Körpern*, die er kurz zuvor in einem noch umfangreicheren Buch publiziert hatte.

Ganz abgesehen davon, daß der A. Weilsche Weg zu dem grundlegenden Resultat sehr lang und mühevoll ist, ist auch die benutzte Methodik vom Standpunkt des Arithmetikers aus dem Problem nicht recht angemessen, und überdies genügt sein Beweis nicht den Ansprüchen an Finitheit und Konstruktivität der einzelnen Definitionen und Beweisschritte, die sich in der modernen Arithmetik im Anschluß an *Kronecker* immer mehr durchsetzen.

So habe ich 1949 meinem Schüler *Roquette* die Anregung gegeben, einen kürzeren, eleganteren und den genannten methodischen Ansprüchen genügenden Beweis aufzufinden, und diese Aufgabe hat er dann 1951 in seiner Hamburger Dissertation in ausgezeichneter Weise gelöst.

Ich will hier nur noch ein paar Worte über die von ihm geschaffene und benutzte Methode sagen, deren Bedeutung weit über das zum Ausgang genommene Problem hinausreicht.

Man betrachtet zwei Exemplare der gegebenen Kurve:

$$f(x, y) = 0\,, \qquad f(x', y') = 0$$

in zwei getrennten Koordinatenebenen (x, y) und (x', y'). Diese beiden Koordinatenebenen bestimmen zusammen einen vierdimensionalen Raum (x, y, x', y'), und die beiden Kurven bestimmen in diesem vierdimensionalen Raum eine *zweidimensionale, zylindrische Fläche*. Die Aufgabe erweist sich dann äquivalent mit einer Aussage über die *Schnittpunktzahlen* von Kurven A, B dieser zylindrischen Fläche, nämlich damit, zunächst einmal diese Schnittpunktzahlen präzise zu definieren, unter Berücksichtigung aller Komplikationen, die durch mehrfache Punkte der Kurven auftreten können, und dann zu zeigen, daß die Schnittpunktzahlen (A, B) eine *positiv–definite Metrik* im System der *Kurvenscharen* auf der Fläche festlegen.

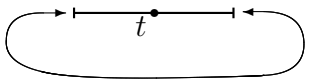
Da es sich um eine Fläche im *vier*dimensionalen Raum handelt, versagt die Anschauung völlig. Man kann sich aber in folgender Weise doch ein an-

schauliches Bild machen, das die wesentlichen Züge der Situation darstellt.

Als Kurve nehme man etwa den Kreis

$$x^2 + y^2 - r^2 = 0.$$

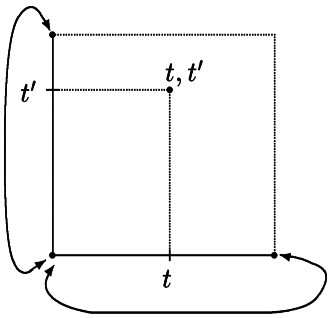
Man denke sich diese zweidimensionale Kurve künstlich eindimensional gemacht, indem man sie auf einer Geraden abrollen läßt. Dann erhält man eine Strecke



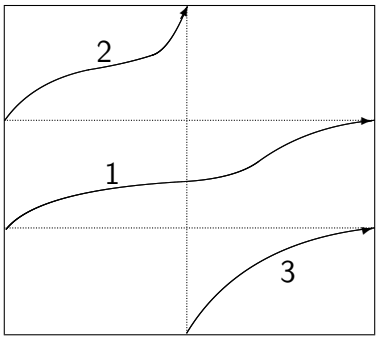
bei der Anfangs– und Endpunkt zu identifizieren sind. Den anderen Kreis

$$x'^2 + y'^2 - r^2 = 0$$

denke man dann auf einer zu der ersten senkrechten Geraden abgerollt:

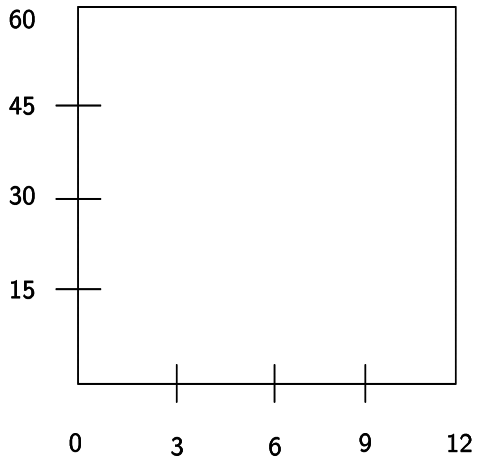


An die Stelle der Fläche im vierdimensionalen Raum tritt dann eine nur zweidimensionale Quadratfläche, deren Punkte (t, t') den Paaren von Punkten t und t' der beiden Kreise genau entsprechen. Dabei sind jeweils die gegenüberliegenden Begrenzungsgeraden des Quadrats zu identifizieren, d. h. wenn man in dem Quadrat spazieren geht und an den Rand kommt, soll man seinen Weg im gegenüberliegenden Randpunkt fortsetzen:

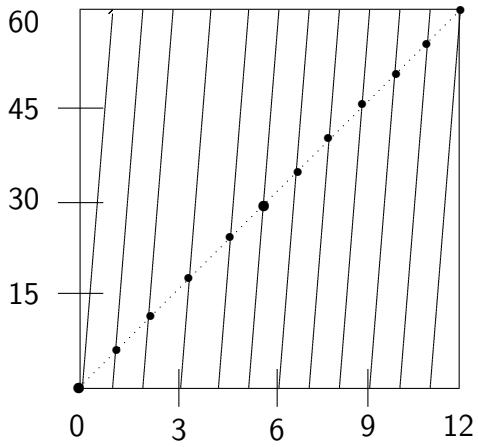


Darstellung einer geschlossenen Kurve
auf der Fläche.

Man denke sich nun die beiden Kreise etwa durch die Stellungen der beiden Zeiger einer Uhr realisiert:



Sind beide Zeiger frei beweglich, so erhält man als Bilder ihrer möglichen Stellungen alle Punkte des Quadrats.
In Wirklichkeit aber sind die beiden Zeiger so gekoppelt, daß der große 12–mal so schnell läuft wie der kleine. Das Bild des Laufens der Uhr gibt demnach die folgende Kurve auf der Fläche:



Das sind die *wirklichen* Zeigerstellungen bei einer Uhr.

Eine andere Kurve wird etwa definiert durch zwei gleichschnell laufende Zeiger. Sie läuft diagonal durch das Quadrat.

Beide Kurven schneiden sich in genau 11 Punkten. Es sind das diejenigen Zeigerstellungen, bei denen sich die beiden Zeiger decken.

Dies ist eine anschauliche Darstellung der Schnittpunkte zweier Kurven auf der zylindrischen Fläche im vierdimensionalen Raum, die durch zwei Kreise erzeugt wird.

Roquette hat nun gezeigt, wie man ganz allgemein bei einer *beliebigen* algebraischen Kurve $f(x, y) = 0$ eine präzise Behandlung der Schnittpunktzahlen von *irgendwelchen* Kurven A, B auf der zylindrischen Fläche erreichen kann. Durch den Nachweis, daß die durch diese Schnittpunktzahlen (A, B) gelieferte Metrik positiv–definit ist, hat er den obigen arithmetischen Satz über die Lösungszahlen von Kongruenzen

$$f(x, y) \equiv 0 \mod p$$

auf eine sehr elegante und durchsichtige Art erneut bewiesen und durch diese Beweismethode den Grundstein zu vielen interessanten weiteren Anwendungen auf arithmetische und algebraische Probleme gelegt.

1.22 Bonn 1953

Zetafunktion und L–Funktionen eines arithmetischen Funktionenkörpers vom Fermatschen Typus.

Vortrag Bonn, 3. 7. 1953.

§1. Arithmetische Funktionenkörper.

Es gibt zwei Klassen von Körpern, in denen sich eine Arithmetik entwickeln läßt, die weitgehend zur Arithmetik im rationalen Zahlkörper P analog ist, nämlich:

A. Die *algebraischen Zahlkörper*, d. h. die endlich–algebraischen Erweiterungskörper K/P des rationalen Zahlkörpers P.

B. Die *Kongruenzfunktionenkörper*, d. h. die endlich–algebraischen Erweiterungskörper $\mathsf{K}/\Omega(t)$ des rationalen Funktionenkörpers $\Omega(t)$ einer Unbestimmten t über einem endlichen Körper Ω.

Der Aufbau der Arithmetik in diesen beiden Körperklassen erfolgt, wenn man die Analogie hervortreten lassen will, auf der Grundlage der *Bewertungstheorie*. Die Arithmetik fußt wesentlich auf den folgenden Endlichkeitseigenschaften des *vollständigen Systems nicht–archimedischer Bewertungen* von K bzw. von K/Ω:

I. Die *Bewertungen* $w_{\mathfrak{p}}$ sind sämtlich *diskret*; Primdivisoren $\mathfrak{p}$ von K bzw. K/Ω zugeordnet.

II. Für jedes Element $a \neq 0$ aus K sind *nur endlich viele Werte* $w_{\mathfrak{p}}(a) \neq 0$; in a stecken nur endlich viele $\mathfrak{p}$.

III. Die *Restklassenkörper* $\mathsf{K}_{\mathfrak{p}}$ sind *endlich*.

Hat ein Körper K/P bzw. ein nicht–algebraischer Körper K/Ω diese Eigenschaften, so ist er ein algebraischer Zahlkörper bzw. ein Kongruenzfunktionenkörper.

Siehe zu alledem meine „Zahlentheorie“ §20.

In Körpern, die nicht einer dieser beiden Klassen angehören, hat man daher, wenn sich überhaupt eine Arithmetik auf bewertungstheoretischer Grundlage aufbauen läßt, Abweichungen in den Gesetzlichkeiten über

Primdivisorzerlegung, Ganzheit, Einheiten, Kongruenzen

zu erwarten.

Nun werden in den beiden hervorgehobenen, arithmetisch einfachsten Klassen von Körpern K die nicht–archimedischen Bewertungen $w_{\mathfrak{p}}$, oder also die ihnen zugeordneten Primdivisoren $\mathfrak{p}$, nach folgendem Schema erhalten. Man geht aus von dem Teilkörper

P	$\Omega(t)$
In ihm entsprechen die Bewertungen $w_{\mathfrak{p}}$ eindeutig den	
Primzahlen p	Primpolynomen $p = p(t)$.
Für die endlich–algebraische Erweiterung	
K/P	$\mathsf{K}/\Omega(t)$

entwickelt man dann eine Fortsetzungstheorie der Bewertungen, oder also eine Zerlegungstheorie der Primdivisoren. So erhält man dann jedem p zugeordnet endlich viele $w_{\mathfrak{p}}, \mathfrak{p}$ mit bestimmten Verzweigungsordnungen und Restklassengraden.

Als nächst einfachere Klasse von Körpern bietet sich eine solche dar, bei der Primdivisoren jedes dieser beiden Typen

$\mathfrak{p}$ zu Primzahl p $\qquad$ $\mathfrak{p}$ zu Primpolynom $p(t)$

vorkommen. Grundtypus einer solchen Körperklasse ist der Körper

$\mathsf{R} = \mathsf{P}(t)$ der rationalen Funktionen einer Unbestimmten t über dem rationalen Zahlkörper.

In ihm hat man eindeutige Primelementzerlegung mit den Primelementen

Primzahlen p $\qquad$ ganzzahlige primitive Primpolynome $P(t)$

und den zugeordneten Restklassenkörpern

$\mathsf{R}_p = \mathsf{P}_p(t)$	$\mathsf{R}_P = \mathsf{P}(\omega) \quad \text{mit} \quad P(\omega) = 0$
(einfachster Kongruenz–Funktionenkörper)	(allgemeinster algebraischer Zahlkörper)

Durch endlich–algebraische Erweiterung erhält man hieraus die Klasse der Körper

$$K \quad \text{endlich–algebraischer Erweiterungskörper von } \mathsf{R} = \mathsf{P}(t),$$

oder also

$$K = \mathsf{P}(t, u) \quad \text{mit irreduzibler Gleichung } F(t, u) = 0 \text{ über } \mathsf{P},$$

d. h. der algebraischen Funktionenkörper einer Unbestimmten mit dem rationalen Zahlkörper als Koeffizientenkörper. Diese Körper K seien *arithmetische Funktionenkörper* genannt.

Die vorgenommene endlich–algebraische Erweiterung zerfällt im allgemeinen in einen ersten Schritt, der nur P zu einem bestimmten algebraischen Zahlkörper K erweitert (Grundgleichung von t unabhängig) und einen zweiten Schritt, bei dem keine weiteren absolut–algebraischen Elemente hinzukommen (Grundgleichung in t, u absolut–irreduzibel). Man nennt dann K den *Konstantenkörper* von K und schreibt die Erzeugung in der Form:

K endlich–algebraischer Erweiterungskörper von $\mathsf{R} = \mathsf{K}(t)$ mit genauem Konstantenkörper K,

oder also

$$K = \mathsf{K}(t, u) \text{ mit absolut–irreduzibler Grundgleichung } F(t, u) = 0 \text{ über } \mathsf{K},$$

d. h.

K/K algebraischer Funktionenkörper einer Unbestimmten mit einem algebraischen Zahlkörper K als Konstantenkörper.

Die Arithmetik in einem solchen arithmetischen Funktionenkörper K wird dadurch bestimmt, daß man sowohl im Konstantenkörper K einen Ganzheitsbegriff hat, nämlich den der ganzen algebraischen Zahl, als auch im Funktionenkörper K/K, nämlich den der Ganzheit in der Unbestimmten t. Letzterer

liegt allerdings erst nach Auszeichnung einer Unbestimmten t fest, ist also nicht birational–invariant; die Bewertungstheorie ermöglicht aber einen birational–äquivalenten Aufbau der Arithmetik von K/K $\big($Hinzunahme von $\frac{1}{t}$ zu den $P(t)\big)$.

Die Schwierigkeiten für den Aufbau einer Arithmetik von K selbst liegen darin, daß diese bekannte Arithmetik von K/K mit der Arithmetik von K kombiniert werden soll. Was das bedeutet, kann man sich am besten klarmachen, indem man den algebraischen Konstantenkörper K mit seiner aus den Primzahlen p entspringenden Arithmetik durch einen algebraischen Funktionenkörper K/Ω einer Unbestimmten x mit seiner aus den Primpolynomen $p(x)$ über $\Omega(x)$ entspringenden Arithmetik ersetzt denkt. Man hat dann einen Körper vom Typus:

> K endlich–algebraischer Erweiterungskörper des rationalen Funktionenkörpers $\Omega(x,t)$ von zwei unabhängigen Unbestimmten t, x über irgendeinem Körper Ω,

d. h. einen algebraischen Funktionenkörper K/Ω von zwei Unbestimmten. Man weiß, daß hier der geläufige bewertungstheoretische Aufbau der Arithmetik versagt, daß vielmehr viel kompliziertere arithmetische Verhältnisse vorliegen. Komplikationen der gleichen Art liegen auch bei den arithmetischen Funktionenkörpern K vor. Genau wie dort ist auch hier ein birational–invarianter Aufbau der Arithmetik in K bisher nicht möglich. Während für die Relativarithmetik von K/K keine Auszeichnung einer Unbestimmten t erforderlich ist, muß man eine solche Auszeichnung zugrundelegen, wenn man die Arithmetik von K selbst aufbauen will.

§2. Primdivisoren, Punkte.

1. Nach dem Vorbild der Arithmetik in algebraischen Zahlkörpern und Kongruenzfunktionenkörpern (allgemeiner auch der Relativarithmetik in algebraischen Funktionenkörpern K/K einer Unbestimmten mit beliebigem Konstantenkörper K) wird man für den Aufbau der Arithmetik in einem arithmetischen Funktionenkörper K zunächst nach den *Primdivisoren von* K fragen. Man erhält diese durch Betrachtung der nicht–archimedischen Bewertungen von K, und zwar der Bewertungen im gewöhnlichen Sinne, d. h. mit einer Wertgruppe aus reellen Zahlen.

Diese Bewertungen zerfallen in zwei Sorten, je nachdem der Konstantenkörper K identisch oder nicht–identisch bewertet wird.

Den Bewertungen der ersten Sorte, also denen von K/K, entsprechen die Primdivisoren $\mathfrak{P}$ der bekannten Relativarithmetik von K/K. Sie seien die *algebraischen Primdivisoren von* K genannt. Bei einem zweistufigen Aufbau [1]

$$\mathsf{R} = \mathsf{K}(t) \quad \text{rein–transzendent}, \qquad K/\mathsf{R} \quad \text{endlich–algebraisch}$$

entspringen diese algebraischen Primdivisoren $\mathfrak{P}$ aus den Primpolynomen $P(t)$ (nebst $\frac{1}{t}$) über K durch Primzerlegung der zugeordneten Primdivisoren von R/K in K/R. Ihre *Restklassenkörper* $K_{\mathfrak{P}}$ sind endlich–algebraische Erweiterungen des Konstantenkörpers K, also *algebraische Zahlkörper*.

Den Bewertungen der zweiten Sorte entsprechen zunächst Primdivisoren $\mathfrak{p}$ von K, und es handelt sich um deren Fortsetzungen zunächst auf die rein–transzendente Erweiterung R/K, dann auf die endlich–algebraische Erweiterung K/K.

Für den ersten Schritt R/K stehen unendlich viele, schwer übersehbare Möglichkeiten zur Verfügung. Unter ihnen hebt sich aber, wenn man nicht nur den rationalen Teilkörper $\mathsf{R} = \mathsf{K}(t)$, sondern schärfer dessen erzeugende Unbestimmte t auszeichnet, jeweils eine durch den Primdivisor $\mathfrak{p}$ von K eindeutig bestimmte Möglichkeit hervor, nämlich die Fortsetzung von $\mathfrak{p}$ als sogen. *t–Funktionalprimdivisor von* R:

$$\begin{aligned}
\mathfrak{p}\text{–Potenz in Polynom } F(t) \text{ über } \mathsf{K} \quad &= \quad \text{höchste } \mathfrak{p}\text{–Potenz in den Koeffizienten von } F(t), \\
\mathfrak{p}\text{–Potenz in } \frac{F(t)}{G(t)} \quad &= \quad \frac{\mathfrak{p}\text{–Potenz in } F(t)}{\mathfrak{p}\text{–Potenz in } G(t)}\,, \\
F(t) \text{ ganz für } \mathfrak{p} \quad &\longleftrightarrow \quad \text{Koeffizienten von } F(t) \text{ ganz für } \mathfrak{p}, \\
F(t) \text{ Einheit für } \mathfrak{p} \quad &\longleftrightarrow \quad \text{Koeffizienten von } F(t) \text{ ganz und teilerfrei für } \mathfrak{p} \ \big(F(t) \text{ primitiv für } \mathfrak{p}\big), \\
F(t) \equiv G(t) \mod \mathfrak{p} \quad &\longleftrightarrow \quad \text{koeffizientenweise Kongruenz mod } \mathfrak{p}.
\end{aligned}$$

Begrifflich sind diese t–Funktionalprimdivisoren $\mathfrak{p}$ von R unter allen möglichen Fortsetzungen auf R der Primdivisoren $\mathfrak{p}$ von K am einfachsten durch die Forderung gekennzeichnet, daß die Transzendenzeigenschaft der Unbestimmten t über K, nämlich

$$1, t, t^2, \ldots \qquad \text{sind linear–unabhängig über } \mathsf{K},$$

1. Ob es sich im Folgenden um zwei verschiedene 'R' handelt, etwa R und R, ist optisch schwer zu entscheiden.

auch bei Übergang zu den Resten mod $\mathfrak{p}$ erhalten bleiben soll, also

$$1, t, t^2, \ldots \mod \mathfrak{p} \text{ sind linear–unabhängig über } \mathsf{K}_\mathfrak{p}\,.$$

Es ist dann also der Restklassenkörper

$$\mathsf{R}_\mathfrak{p} = \mathsf{K}_\mathfrak{p}(t)$$

der rationale Kongruenzfunktionenkörper in t über dem endlichen Restklassenkörper $\mathsf{K}_\mathfrak{p}$.

Für den zweiten Schritt K/R gilt die gewöhnliche Theorie der Primzerlegung. Sie liefert für jeden t–Funktionalprimdivisor $\mathfrak{p}$ von R eine Zerlegung in endlich viele *t–Funktionalprimdivisoren $\mathfrak{p}$ von K*, mit bestimmten Restklassengraden und Verzweigungsordnungen. Diese t–Funktionalprimdivisoren $\mathfrak{p}$ von K seien auch die *arithmetischen Primdivisoren von K* genannt. Ihre *Restklassenkörper* $K_\mathfrak{p}$ sind endlich–algebraische Erweiterungen der eben genannten rationalen Kongruenzfunktionenkörper $\mathsf{R}_\mathfrak{p}$, also wieder *Kongruenzfunktionenkörper*.

Schematisch zusammengestellt:

$$\text{Arithm. Fkt. Kp. } K \left\{ \begin{array}{l} \text{mod. algebr. Primdiv. } \mathfrak{P} \longrightarrow \text{algebr. Zahlkp. } K_\mathfrak{P} \text{ über } \mathsf{K} \\ \text{mod. arithm. Primdiv. } \mathfrak{p} \longrightarrow \text{Kongr. Fkt. Kp. } K_\mathfrak{p} \text{ über } \mathsf{K}_\mathfrak{p} \end{array} \right\}$$

Das so bei Auszeichnung einer Unbestimmten t festgelegte Primdivisorsystem $\mathfrak{P}, \mathfrak{p}$ von K besteht zwar nicht aus allen überhaupt vorhandenen Primdivisoren von K — die arithmetischen $\mathfrak{p}$ sind ja durch eine sehr einengende Auswahlvorschrift festgelegt —, reicht aber zu einer Beschreibung der arithmetischen Eigenschaften von K aus. Für den Grundtypus $\mathsf{R} = \mathsf{P}(t)$ entspricht es genau den Primzahlen p und primitiven Primpolynomen $P(t)$ über P, also den sämtlichen Primelementen der eindeutigen Primelementzerlegung, wobei zu den $P(t)$ noch der $\frac{1}{t}$ entsprechende Primdivisor hinzuzunehmen ist (Beseitigung der Auszeichnung von t für die algebraischen Primdivisoren!).

Eine der Grundaufgaben für den Aufbau der Arithmetik in K ist die Herleitung des genauen *Zerlegungsgesetzes* für die t–Funktionalprimdivisoren von R in solche von K. In dieser Richtung hat *Deuring* 1942 folgendes bewiesen. Fast alle $\mathfrak{p}$ von R bleiben in K unzerlegt und unverzweigt, d. h. erhöhen nur ihren Restklassenkörper von $\mathsf{R}_\mathfrak{p} = \mathsf{K}_\mathfrak{p}(t)$ auf die endlich–algebraische Erweiterung $K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}$. Für fast alle $\mathfrak{p}$ ist ferner $\mathsf{K}_\mathfrak{p}$ der genaue Konstantenkörper des Kongruenzfunktionenkörpers $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$, bleibt nämlich eine Erzeugung

$$K = \mathsf{K}(t, u) \quad \text{mit absolut–irreduziblem } F(t, u) = 0 \text{ über } \mathsf{K}$$

auch mod $\mathfrak{p}$ absolut–irreduzibel über $\mathsf{K}_\mathfrak{p}$. Für fast alle $\mathfrak{p}$ bleibt schließlich das Geschlecht $\mathfrak{p}$ von K/K auch das Geschlecht $g_\mathfrak{p}$ des Kongruenzfunktionenkörpers $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$.

Für einen leistungsfähigen und voll befriedigenden Aufbau der Arithmetik in K wird man aber über die Feststellung hinaus, daß sich fast alle $\mathfrak{p}$ von R in diesem Sinne *regulär* verhalten, auch das genaue Verhalten der endlich vielen *irregulären* $\mathfrak{p}$ von R benötigen. Eine allgemeine Untersuchung über das Zerlegungsgesetz für die t–Funktionalprimdivisoren erscheint mir als eine lohnende Aufgabe.

2. Ebenso wie man in der Theorie der algebraischen Funktionenkörper von zwei Unbestimmten

$$K \text{ endlich–algebraisch über } \Omega(x,t), \text{ also über } \mathsf{K}(t) \text{ mit } \mathsf{K} = \Omega(x)$$

mit den Primdivisoren allein nicht auskommt, sondern wesentlich auch die Punkte braucht, so wird man auch in der Theorie der arithmetischen Funktionenkörper einer Unbestimmten

$$K \text{ endlich–algebraisch über } \mathsf{K}(t) \text{ mit } \mathsf{K} \text{ algebraisch über } \mathsf{P}$$

mit den vorstehend festgelegten algebraischen und arithmetischen Primdivisoren $\mathfrak{P}, \mathfrak{p}$ allein nicht auskommen, sondern ein Analogon zu den *Punkten* brauchen.

Zum besseren Verständnis sei die Analogie der beiden eben genannten Körpertypen zunächst für die Primdivisoren durchgeführt.

Im algebraischen *Falle* $K/\Omega(x,t)$ entspringt ein ausreichendes System von Primdivisoren durch Primzerlegung aus den Primpolynomen $P(x,t)$ (einschl. $\frac{1}{x}, \frac{1}{t}$) des rationalen Teilkörpers $\Omega(x,t)$. Setzt man $\Omega(x,t) = \mathsf{K}(t)$ mit $\mathsf{K} = \Omega(x)$, so erhält man das Analogon der

> algebraischen Primdivisoren aus den $P(x,t)$, die t wirklich enthalten (einschl. $\frac{1}{t}$),
> arithmetischen Primdivisoren aus den $P(x)$, die t nicht enthalten (einschl. $\frac{1}{x}$).

Diese Einteilung der Primdivisoren trägt nicht der Tatsache Rechnung, daß man die Rollen der beiden Unbestimmten x, t vertauschen kann. Will man diese Symmetrie mehren, so muß man aus den algebraischen Primdivisoren noch diejenigen abspalten, die aus den $P(t)$ (einschl. $\frac{1}{t}$) entspringen, die also

bei dem Ansatz $\Omega(x,t) = \mathsf{K}'(x)$ mit $\mathsf{K}' = \Omega(t)$ arithmetische Primdivisoren sind.

Im arithmetischen *Falle* $K/\mathsf{K}(t)$ *mit* K/P *algebraisch* besteht keine derartige Symmetrie: man kann nicht die Rollen von t und K/P als Erzeugende je einer Arithmetik vertauschen, hat vielmehr eine echte Stufung $\mathsf{K}/\mathsf{P}, K/\mathsf{K}$.

Diese Unsymmetrie macht sich auch geltend, wenn man den Punktbegriff im arithmetischen Falle $K/\mathsf{K}(t)$ in Analogie zum algebraischen Falle $K/\Omega(x,t)$ aufbauen will.

Im *algebraischen Falle* $K/\Omega(x,t)$ werden die Punkte in der algebraischen Geometrie folgendermaßen definiert. Man betrachte, unter Auszeichnung der Transzendenzbasis x,t, zunächst den rationalen Teilkörper

$$\mathsf{R} = \Omega(x,t)$$

Bei ihm liefert jede Einsetzung

$$x \longrightarrow \xi,\ t \longrightarrow \tau \quad \text{mit über } \Omega \text{ algebraischen } \xi,\tau \text{ (einschl. } \infty)$$

einen Homomorphismus von R/Ω auf eine endlich–algebraische Erweiterung $\Omega(\xi,\tau)$ von Ω (bei dem neben den bestimmt abgebildeten Elementen auch solche ohne bestimmtes Bildelement vorkommen). Jeder solche Homomorphismus setzt sich — in Analogie zur Primzerlegung — auf endlich viele verschiedene Weisen zu Homomorphismen von K/Ω auf (ξ,τ enthaltende) endlich–algebraische Erweiterungen von Ω fort. Die Gesamtheit der so entstehenden Homomorphismen von K/Ω auf endlich–algebraische Erweiterungen von Ω nennt man die Punkte von K/Ω in bezug auf die zugrundegelegte Transzendenzbasis x,t.

Für die Analogisierung muß man dies in x,t symmetrische Definitionsschema der Punkte von K/Ω zunächst unsymmetrisch machen, nämlich von dem zweistufigen Aufbau

$$K/\mathsf{R} \quad \text{mit} \quad \mathsf{R} = \mathsf{K}(t), \quad \mathsf{K} = \Omega(x)$$

ausgehend beschreiben. Hierzu stützt man sich auf die Tatsache, daß bei einem algebraischen Funktionenkörper einer Unbestimmten sich die

> Homomorphismen auf endlich–algebraische Erweiterungen des Konstantenkörpers

und die

Primdivisoren

umkehrbar eindeutig entsprechen, indem die Homomorphismen jeweils die Restabbildungen nach den Primdivisoren sind. Danach kann man die Punkte folgendermaßen durch Primdivisoren beschreiben.

Der Einsetzung $x \longrightarrow \xi$ entspricht in $\mathsf{K} = \Omega(x)$ das Primpolynom $P(x)$ über Ω mit $P(\xi) = 0$, und damit in $\mathsf{R} = \mathsf{K}(t)$ ein t–Funktionalprimdivisor, sowie weiter auch in K ein t–Funktionalprimdivisor $\mathfrak{p}$ derart, daß der durch $x \longrightarrow \xi$ erzeugte Homomorphismus von K/Ω gerade die Restabbildung mod $\mathfrak{p}$ von K auf den Restklassenkörper $K_\mathfrak{p}$ ist. Dieser Restklassenkörper $K_\mathfrak{p}$ ist eine endlich–algebraische Erweiterung des für R vorliegenden Restklassenkörpers $\mathsf{R}_\mathfrak{p} = \Omega(\xi, t) = \Omega_\mathfrak{p}(t)$ mit $\Omega_\mathfrak{p} = \Omega(\xi)$, also ein algebraischer Funktionenkörper einer Unbestimmten

$K_\mathfrak{p}$ endlich–algebraisch über $\Omega_\mathfrak{p}(t)$.

Der Einsetzung $t \longrightarrow \tau$ entspricht dann in $K_\mathfrak{p}$ ein Primdivisor $\mathfrak{P}_\mathfrak{p}$ von $K_\mathfrak{p}/\Omega_\mathfrak{p}$, der durch Primzerlegung aus dem Primpolynom $P(t)$ über Ω mit $P(\tau) = 0$ entspringt, derart, daß der durch $t \longrightarrow \tau$ erzeugte Homomorphismus von $K_\mathfrak{p}/\Omega_\mathfrak{p}$ gerade die Restabbildung mod $\mathfrak{P}_\mathfrak{p}$ von $K_\mathfrak{p}$ auf den Restklassenkörper $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ ist. Dieser Restklassenkörper $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ ist eine endlich–algebraische Erweiterung von $\Omega_\mathfrak{p} = \Omega(\xi)$, die auch τ, also $\Omega(\xi, \tau)$ enthält.

Zusammengenommen hat man damit folgendes Entstehungsschema der Punkte:

$\mathfrak{p}$ ein t–Funktionalprimdivisor von K/Ω, Restklassenkörper $K_\mathfrak{p}/\Omega_\mathfrak{p}$ (alg. Fkt. Kp. einer Unbest.),
$\mathfrak{P}_\mathfrak{p}$ ein Primdivisor von $K_\mathfrak{p}/\Omega_\mathfrak{p}$, Restklassenkörper $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}/\Omega_\mathfrak{p}$ (endl. algebr.),

$$K \xrightarrow[\text{mod } \mathfrak{p}]{} K_\mathfrak{p} \xrightarrow[\text{mod } \mathfrak{P}_\mathfrak{p}]{} K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}.$$

Im *arithmetischen Falle* $K/\mathsf{K}(t)$ *mit* K/P *algebraisch* läßt sich das letztere stufenweise Entstehungsschema der Punkte ohne weiteres analogisieren:

$\mathfrak{p}$ ein t–Funktionalprimdivisor von K, Restklassenkörper $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ (Kongr. Fkt. Kp.),
$\mathfrak{P}_\mathfrak{p}$ ein Primdivisor von $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$, Restklassenkörper $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}/\mathsf{K}_\mathfrak{p}$ (endlich),

$$K \xrightarrow[\text{mod } \mathfrak{p}]{} K_\mathfrak{p} \xrightarrow[\text{mod } \mathfrak{P}_\mathfrak{p}]{} K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}.$$

Die so definierten zweistufigen Restabbildungen von K seien die *Punkte von* K in bezug auf die zugrundegelegte Unbestimmte t genannt. Diese Punkte von K können ihrer Definition nach kurz durch $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ bezeichnet werden. Bei der Restabbildung mod $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ werden (zum mindesten) die $\mathfrak{p}$–ganzen Elemente aus K bestimmt abgebildet, nämlich auf endliche Elemente aus $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ oder ∞, je nachdem das Bildelement mod $\mathfrak{p}$ in $K_\mathfrak{p}$ ganz für $\mathfrak{P}_\mathfrak{p}$ ist oder nicht.

Nach einer brieflichen Ankündigung (Mitteilung) von *Roquette* lassen sich die so festgelegten Punkte $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ von K auch auf bewertungstheoretischer Grundlage definieren, nämlich mittels der von *Krull* 1931 untersuchten *allgemeinen* nicht–archimedischen Bewertungen von K, deren Wertgruppe nicht–archimedisch ist. Der Zweistufigkeit von K entsprechend hat man es dabei im vorliegenden Fall mit einer zweistufig nicht–archimedischen Wertgruppe zu tun, deren Werte also reelle Zahlpaare in lexikographischer Anordnung sind.

§3. Die Zetafunktion.

In einem algebraischen Zahlkörper K hat man für die Zetafunktion $\zeta_\mathsf{K}(s)$ zwei Definitionen, als Dirichletsche Reihe und als Eulersches Produkt, die auf Grund der eindeutigen Primdivisorzerlegung in K miteinander identisch sind:

$$\text{Dirichletsche Reihe} \quad \zeta_\mathsf{K}(s) = \sum_\mathfrak{g} \frac{1}{\mathfrak{N}(\mathfrak{g})^s}\,,$$

$$\text{Eulersches Produkt} \quad \zeta_\mathsf{K}(s) = \prod_\mathfrak{p} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}}\,.$$

Dabei durchläuft $\mathfrak{g}$ alle ganzen Divisoren, $\mathfrak{p}$ alle Primdivisoren von K, und $\mathfrak{N}$ bezeichnet die Absolutnorm, definiert als die Restklassenanzahl mod $\mathfrak{g}$ bzw. mod $\mathfrak{p}$ in K.

In einem arithmetischen Funktionenkörper K sind nun für die *Primdivisoren* die Restklassenanzahlen unendlich:

algebraische $\mathfrak{P}$, Restklassenkörper $K_\mathfrak{P}$ = algebr. Zahlkörper,
arithmetische $\mathfrak{p}$, Restklassenkörper $K_\mathfrak{p}$ = Kongr. Funktionenkörper.

Daher läßt sich die obige Definition der Zetafunktion von K jedenfalls nicht mittels der Primdivisoren von K analogisieren.

Dagegen haben die Punkte $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ von K endliche Restklassenanzahlen

Punkte $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$. Restklassenkörper $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ endlich.

Daher lässt sich die Produktdefinition der Zetafunktion von K mittels der *Punkte* von K analogisieren:

$$\text{Eulersches Produkt} \qquad \zeta_K(s) = \prod_{(\mathfrak{p},\mathfrak{P}_\mathfrak{p})} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p},\mathfrak{P}_\mathfrak{p})^s}},$$

wo $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ alle Punkte von K (in bezug auf eine feste Unbestimmte t) durchläuft und $\mathfrak{N}(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ jeweils die Elementanzahl von $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ bezeichnet.

Eine entsprechende *Analogisierung der Reihendefinition der Zetafunktion* von K erscheint nicht möglich, weil man in K zwar eine eindeutige Primdivisorzerlegung, nicht aber eine eindeutige Punktzerlegung hat.

Man kann jedoch in dieser Richtung einen ersten Schritt tun, indem man die eindeutige Primdivisorzerlegung in $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ anwendet. Es ist zunächst

$$\mathfrak{N}(\mathfrak{p}, \mathfrak{P}_\mathfrak{p}) = \mathfrak{N}(\mathfrak{P}_\mathfrak{p}),$$

weil $K_{\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ als der Restklassenkörper des Primdivisors $\mathfrak{P}_\mathfrak{p}$ von $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ zustandekommt. Daher hat man

$$\zeta_K(s) = \prod_\mathfrak{p} \prod_{\mathfrak{P}_\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P}_\mathfrak{p})^s}}.$$

Hier ist aber das innere Produkt nichts anderes als die Zetafunktion des Kongruenzfunktionenkörpers $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ in ihrer Eulerschen Produktdarstellung:

$$\zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) = \prod_{\mathfrak{P}_\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P}_\mathfrak{p})^s}}.$$

Für diese Zetafunktion hat man aber auch die Dirichletsche Reihendarstellung

$$\zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) = \sum_{\mathfrak{G}_\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{G}_\mathfrak{p})^s},$$

wo $\mathfrak{G}_\mathfrak{p}$ alle ganzen Divisoren von $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ durchläuft. Für die zu untersuchende Zetafunktion

$$\zeta_K(s) = \prod_\mathfrak{p} \zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s)$$

hat man daher neben der zur Definition genommenen Darstellung als Doppelprodukt auch die Darstellung

$$\zeta_K(s) = \prod_{\mathfrak{p}} \sum_{\mathfrak{G}_\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{G}_\mathfrak{p})^s}$$

als einfaches Produkt Dirichletscher Reihen.

Der zweite Schritt zur Herleitung der Dirichletschen Reihendarstellung würde die Ausmultiplikation dieser unendlich vielen Dirichletschen Reihen erfordern. Formal kann man das natürlich tun; Ziel müßte jedoch sein, zu einem einfachen Bildungsgesetz der Koeffizienten der Produktreihe zu gelangen, das in der Arithmetik von K wurzelt. Vielleicht könnte hierzu die von *Deuring* und neuerdings allgemeiner von *Roquette* entwickelte Theorie des Übergangs von den ganzen Divisoren $\mathfrak{G}$ von K/K zu ihren Resten mod $\mathfrak{p}$ dienlich sein; diese Reste sind ja ganze Divisoren von $K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$.

Wie das zugrundegelegte Punktsystem $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ erscheint auch die mit seiner Hilfe definierte Zetafunktion $\zeta_K(s)$ zunächst abhängig von der ausgezeichneten Unbestimmten t aus K. Es ist zu vermuten, daß diese Abhängigkeit in Wahrheit nicht vorhanden ist, daß also $\zeta_K(s)$ eine *birationale Invariante von* K ist, ähnlich wie etwa das Geschlecht g von K/K, dessen Definition

$$2g - 2 = \text{Grad } \frac{\text{Differente von } K/\mathsf{K}(t)}{\text{Nennerquadrat von } t}$$

ja auch zunächst von der Wahl der Unbestimmten t abhängt. Zu diesem Invarianzbeweis wird wahrscheinlich die von *Roquette* in Aussicht gestellte invariante Kennzeichnung des Punktsystems $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ mittels der allgemeinen Krullschen Bewertungen führen.

Ich habe schon 1938 vermutet, daß die wie angegeben definierte *Zetafunktion von K eine „vernünftige“ Zetafunktion* ist, nämlich analoge funktionentheoretische und arithmetische Eigenschaften hat, wie die Zetafunktion von K. Anlaß zu dieser Vermutung waren folgende beiden Bemerkungen.

1.) Im Spezialfall, daß $\mathsf{R} = \mathsf{K}(t)$ ein *rationaler Funktionenkörper* ist, sind auch die $\mathsf{R}_\mathfrak{p} = \mathsf{K}_\mathfrak{p}(t)$ rationale Kongruenzfunktionenkörper. Für diese ist aber einfach

$$\zeta_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) = \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}} \frac{1}{1 - \frac{\mathfrak{N}(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}}$$

Daraus folgt durch Produktbildung die explizite Darstellung

$$\zeta_{\mathsf{R}}(s) = \zeta_{\mathsf{K}}(s)\zeta_{\mathsf{K}}(s-1)$$

der Zetafunktion von R durch die von K. Entsprechend der Zweistufigkeit des Punktsystems $(\mathfrak{p}, \mathfrak{P}_{\mathfrak{p}})$ tritt hier das Argumentpaar $s, s-1$ auf, demzufolge $\zeta_{\mathsf{R}}(s)$ nicht nur bei $s = 1$ sondern auch noch bei $s = 2$ einen Pol erster Ordnung hat. Diese Darstellung läßt übrigens die Invarianz von $\zeta_{\mathsf{R}}(s)$ hervortreten.

2.) Im *allgemeinen Falle* hat die Zetafunktion von $K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}$ bekanntlich folgende Struktur. Es ist

$$\zeta_{K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}}(s) = \zeta_{\mathsf{R}_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}}(s) L_{K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}}(s)$$

mit einem Polynom

$$L_{K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}}(s) = 1 - \frac{N_1(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s} + \cdots + \frac{\mathfrak{N}(\mathfrak{p})^{g_{\mathfrak{p}}}}{\mathfrak{N}(\mathfrak{p})^{2g_{\mathfrak{p}}s}}$$

vom Grade $2g_{\mathfrak{p}}$ in $\frac{1}{\mathfrak{N}(\mathfrak{p})^s}$, wo $g_{\mathfrak{p}}$ das Geschlecht von $K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}$ und $N_1(g)$ die Anzahl der Primdivisoren ersten Grades von $K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}$ ist. Setzt man für dies Polynom die Linearfaktorenzerlegung

$$L_{K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}}(s) = \prod_{i=1}^{2g_{\mathfrak{p}}} \left(1 - \frac{\omega_i(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right)$$

an, so haben nach dem von *A. Weil* allgemein bewiesenen Analogon zur Riemannschen Vermutung die Nullstellen $\omega_i(\mathfrak{p})$ sämtlich den absoluten Betrag

$$|\omega_i(\mathfrak{p})| = \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}}.$$

Für fast alle $\mathfrak{p}$ ist nun nach *Deuring* $g_{\mathfrak{p}} = g$ einfach das Geschlecht von K/K, für die restlichen endlich vielen $\mathfrak{p}$ jedenfalls $g_{\mathfrak{p}} < g$. Rechnet man für die letzteren $\mathfrak{p}$ die fehlenden Nullstellen $\omega_i(\mathfrak{p}) = 0$ und ordnet dann für die einzelnen $\mathfrak{p}$ die $2g$ Nullstellen $\omega_i(\mathfrak{p})$ irgendwie einander zu, so kann man die Produktbildung unter Benutzung des obigen Ergebnisses für $\zeta_{\mathsf{R}_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}}(s)$ folgendermaßen durchführen:

$$\zeta_K(s) = \zeta_{\mathsf{K}}(s)\zeta_{\mathsf{K}}(s-1) \cdot \prod_{i=1}^{2g} \prod_{\mathfrak{p}} \left(1 - \frac{\omega_i(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right).$$

Hier konvergiert auf Grund der Riemannschen Vermutung jedes der $2g$ inneren Produkte für $\Re(s) > \frac{3}{2}$. Demnach ist $\zeta_K(s)$ jedenfalls für $\Re(s) > \frac{3}{2}$ analytisch und u. A. d. R. V. nullstellenfrei, mit einzigem Pol erster Ordnung bei $s = 2$.

Für den *allgemeinen Fall* ist das bis heute alles, was man weiß. Dagegen hat sich meine Vermutung im Spezialfall der *arithmetischen Funktionenkörper K vom Fermatschen Typus* durch eine kürzlich erschienene Arbeit von *A. Weil* in vollem Umfange bestätigt, desgleichen nach einer Mitteilung von *Deuring* auch für diejenigen *elliptischen arithmetischen Funktionenkörper* ($\mathfrak{p} = 1$)*, die eine komplexe Multiplikation besitzen.*

Nachstehend soll noch skizziert werden, wie die Verhältnisse in dem Weilschen Spezialfall der arithmetischen Funktionenkörper vom Fermatschen Typus liegen, und zwar nur für die einfachsten solchen Körper, bei denen der Kern der Sache ungetrübt durch zusätzliche algebraische und arithmetische Komplikationen hervortritt.

§4. Arithmetische Funktionenkörper vom Fermatschen Typus.

Die von *A. Weil* behandelten *arithmetischen Funktionenkörper vom Fermatschen Typus* sind folgende:

$$\mathsf{K} \text{ beliebiger algebraischer Zahlkörper}$$
$$K = \mathsf{K}(u_1, u_2) \quad \text{mit} \quad \frac{u_1^{m_1}}{\gamma_1} + \frac{u_2^{m_2}}{\gamma_2} = 1,$$

wo $\gamma_1, \gamma_2 \neq 0$ Zahlen aus K und m_1, m_2 natürliche Zahlen bedeuten. Wählt man

$$t = \frac{u_1^{m_1}}{\gamma_1} = 1 - \frac{u_2^{m_2}}{\gamma_2}$$

als ausgezeichnete Unbestimmte, legt also der Erzeugung den rationalen Funktionenkörper

$$\mathsf{R} = \mathsf{K}(t)$$

zugrunde, so hat man umgekehrt

$$u_1^{m_1} = \gamma_1 t, \qquad u_2^{m_2} = \gamma_2(1-t),$$

so daß sich die Erzeugung von K/R in der Form

$$K = \mathsf{R}\left(\sqrt[m_1]{\gamma_1 t},\ \sqrt[m_2]{\gamma_2(1-t)}\right)$$

darstellt.

Hier werde nur der folgende *Kernfall* behandelt:

$$\begin{aligned} &m = \ell \quad \text{Primzahl}(\neq 2),\\ &\mathsf{K} \quad \text{Körper der } \ell\text{–ten Einheitswurzeln},\\ &K = \mathsf{K}(u_1, u_2) \quad \text{mit} \quad u_1^\ell + u_2^\ell = 1,\\ &K = \mathsf{R}\left(\sqrt[\ell]{t}, \sqrt[\ell]{1-t}\right), \end{aligned}$$

also der Fall der *gewöhnlichen Fermatschen Gleichung*. Hier ist K/R aus zwei zueinander fremden zyklischen Körpern vom Primzahlgrade ℓ über R komponiert. Für das doppelte Geschlecht von K/K findet sich

$$2g = (\ell - 1)(\ell - 2) \quad (> 0).$$

Als erste Aufgabe habe ich für diesen gewöhnlichen Fermatschen Fall das *Zerlegungsgesetz der Primdivisoren* $\mathfrak{p}$ von K, aufgefaßt als *t–Funktionalprimdivisoren von* $\mathsf{R} = \mathsf{K}(t)$, im Körper $K = \mathsf{R}\left(\sqrt[\ell]{t}, \sqrt[\ell]{1-t}\right)$ in Angriff genommen, mit folgendem Ergebnis:

$$\begin{aligned} &\text{a.)} \quad \mathfrak{p} \nmid \ell, \mathfrak{p} \text{ in } K \text{ träge}, && K_\mathfrak{p} = \mathsf{R}_\mathfrak{p}\left(\sqrt[\ell]{t}, \sqrt[\ell]{1-t}\right), && g_\mathfrak{p} = g,\\ &\text{b.)} \quad \mathfrak{l} \mid \ell, \mathfrak{l} = \bar{\mathfrak{l}}^\ell \text{ in } K \left\{ \begin{array}{c} \text{träge} \\ \text{unverzweigt} \end{array} \right\}, && K_{\bar{\mathfrak{l}}} = \mathsf{R}_\mathfrak{l}\left(\sqrt[\ell]{t}\right), && g_{\bar{\mathfrak{l}}} = 0. \end{aligned}$$

Es verhalten sich also alle Primdivisoren $\mathfrak{p} \nmid \ell$ regulär; irregulär ist nur der eine Primdivisor $\mathfrak{l} \mid \ell$, mit $\mathfrak{l}^{\ell-1} \cong \ell$, gegeben durch $\mathfrak{l} \cong 1 - \zeta$, wo ζ eine primitive ℓ–te Einheitswurzel (aus K).

Mit Aufwand einiger Mühe konnte ich ein entsprechendes Zerlegungsgesetz auch für den folgenden allgemeineren Fall herleiten:

$$\begin{aligned} &\gamma_1, \gamma_2 = 1, \qquad m_1, m_2 \quad \text{beliebig},\\ &\mathsf{K} \quad \text{Körper der } [m_1, m_2]\text{–ten Einheitswurzeln}. \end{aligned}$$

Dagegen bin ich im allgemeinsten Falle vom Fermatschen Typus, wo $\gamma_1, \gamma_2 \neq 0$ aus K beliebig sind und K ein beliebiger Erweiterungskörper des Körpers der $[m_1, m_2]$–ten Einheitswurzeln oder gar ein ganz beliebiger algebraischer Zahlkörper ist, noch nicht durchgekommen. Die Herleitung des fraglichen Zerlegungsgesetzes ist in diesen allgemeineren Fällen eine sehr kniffliche arithmetische Aufgabe.

Weiter sind nun im gewöhnlichen Fermatschen Falle (und entsprechend auch in dem vorher genannten allgemeineren Falle) die *Nullstellen* $\omega_i(\mathfrak{p})$ $(i = 1, \ldots, 2g_\mathfrak{p})$ *der Kongruenzzetafunktionen* $\zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s)$ durch *Davenport–Hasse* (1934) bekannt. Es sind nämlich die sogenannten *Jacobischen Summen* zu den Charakteren der Ordnung ℓ in den endlichen Körpern $\mathsf{K}_\mathfrak{p}$ von $\mathfrak{N}(\mathfrak{p})$ Elementen.

Für $\mathfrak{p} \nmid \ell$ ist $\mathfrak{N}(\mathfrak{p}) \equiv 1 \mod \ell$, und es gibt ℓ Charaktere vom Exponenten ℓ in $\mathsf{K}_\mathfrak{p}^\times$. Die Nullstellen $\omega_i(\mathfrak{p})$ sind dann den Paaren χ_1, χ_2 solcher Charaktere mit $\chi_1 \neq 1, \chi_2 \neq 1, \chi_1\chi_2 \neq 1$ zugeordnet, die ja gerade in der richtigen Anzahl $2g_\mathfrak{p} = 2g = (\ell - 1)(\ell - 2)$ vorhanden sind. Sie lauten explizit:

$$\omega(\chi_1, \chi_2|\mathfrak{p}) = \sum_{\substack{x_1, x_2 \text{ in } \mathsf{K}_\mathfrak{p} \\ x_1 + x_2 \equiv 1 \mod \mathfrak{p}}} \chi_1(x_1)\chi_2(x_2) \qquad (\chi_1, \chi_2, \chi_1\chi_2 \neq 1).$$

Für $\mathfrak{l} \mid \ell$ ist $\mathfrak{N}(\mathfrak{l}) = \ell$, und es gibt keine Charaktere der Ordnung ℓ in $\mathsf{K}_y^\times = \mathsf{P}_\ell^\times$. Dementsprechend ist ja hier auch $2g_\mathfrak{p} = 0$.

Man hat demgemäß explizit:

$$\zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) = \zeta_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) \prod_{\chi_1, \chi_2, \chi_1\chi_2 \neq 1} \left(1 - \frac{\omega(\chi_1, \chi_2|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right) \qquad (\mathfrak{p} \nmid \ell),$$

$$\zeta_{K_\mathfrak{l}/\mathsf{K}_\mathfrak{l}}(s) = \zeta_{\mathsf{R}_\mathfrak{l}/\mathsf{K}_\mathfrak{l}}(s).$$

Diese explizite Darstellung der Kongruenzzetafunktionen $\zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s)$ ergibt sich aus der klassenkörpertheoretischen Zerlegung

$$\zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) = \prod_{\tilde{\mathfrak{l}}_\mathfrak{p}} L_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s|\chi_\mathfrak{p})$$

in L–Funktionen über $\mathsf{R}_\mathfrak{p} = \mathsf{K}_\mathfrak{p}(t)$, wo $\chi_\mathfrak{p}$ die Charaktere der Galoisgruppe $\mathfrak{G}_\mathfrak{p}$ von $K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}$ durchläuft.

Für $\mathfrak{p} \nmid \ell$ erscheinen nämlich die Charakterpaare χ_1, χ_2 mit $\chi_1, \chi_2, \chi_1\chi_2 \neq 1$ vermöge des Artinschen Reziprozitätsgesetzes isomorph zugeordnet den Charakteren $\chi_\mathfrak{p}$ (der Galoisgruppe $\mathfrak{G}_\mathfrak{p}$) von $K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}$ mit der Eigenschaft:

$\chi_\mathfrak{p}$ ist nicht schon Charakter von $\mathsf{R}\left(\sqrt[\ell]{t}\right), \mathsf{R}_\mathfrak{p}\left(\sqrt[\ell]{1-t}\right)$,
$\mathsf{R}_\mathfrak{p}\left(\sqrt[\ell]{\frac{1-t}{t}}\right)$; kurz $\chi_\mathfrak{p} \not\sim 1$.

Die Zuordnungsvorschrift dabei ist folgende:

Elemente aus $\mathfrak{G}_\mathfrak{p}$ isomorph dargestellt durch das Artin–Symbol $\left(\frac{K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}}{\mathfrak{A}_\mathfrak{p}}\right)$ für zu $t, 1-t$ prime Divisoren $\mathfrak{A}_\mathfrak{p}$ von $\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$, genauer durch die Kongruenzklassen dieser Divisoren nach dem Führer von $K/\mathsf{K}_\mathfrak{p}$.

Erzeugende Charaktere von $\mathfrak{G}_\mathfrak{p}$ dargestellt durch die Wirkung dieses Artin–Symbols auf die beiden Radikale $\sqrt[\ell]{t}, \sqrt[\ell]{1-t}$ aus $K_\mathfrak{p}$, also durch die beiden ℓ–ten Potenzrestsymbole

$$\left(\frac{t}{\mathfrak{A}_\mathfrak{p}}\right)_\ell, \quad \left(\frac{1-t}{\mathfrak{A}_\mathfrak{p}}\right)_\ell \quad \text{in} \quad \mathsf{R}_\mathfrak{p}\,.$$

Für Primdivisoren ersten Grades $\mathfrak{P}_\mathfrak{p}$ von $\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ (prim zu t bzw. $1-t$), den Primpolynomen $t-x$ mit x aus $\mathsf{K}_\mathfrak{p}$ ($\not\equiv 0$ bzw. $1 \mod \mathfrak{p}$) zugeordnet, berechnen sich diese ℓ–ten Potenzrestsymbole in $\mathsf{R}_\mathfrak{p}$ als

$$\left(\frac{t}{\mathfrak{P}_\mathfrak{p}}\right)_\ell = \left(\frac{x}{\mathfrak{p}}\right)_\ell, \qquad \left(\frac{1-t}{\mathfrak{P}_\mathfrak{p}}\right)_\ell = \left(\frac{1-x}{\mathfrak{p}}\right)_\ell,$$

also als ℓ–te Potenzrestsymbole nach $\mathfrak{p}$ in K. Das ℓ–te Potenzrestsymbol nach $\mathfrak{p}$ in K ist aber ein *erzeugender Charakter der Ordnung ℓ von $\mathsf{K}_\mathfrak{p}$.*

Aus dieser Zuordnung für die Erzeugenden ergibt sich ein *bestimmter Isomorphismus* zwischen einerseits

den Charakteren $\chi_\mathfrak{p}$ von $\mathfrak{G}_\mathfrak{p}$,

andrerseits

den Charakterpaaren χ_1, χ_2 mit dem Exponenten ℓ von $\mathsf{K}_\mathfrak{p}$.

Der Bedingung $\chi_1, \chi_2, \chi_1\chi_2 \neq 1$ entspricht dabei gerade die oben genannte Bedingung $\chi_\mathfrak{p} \not\sim 1$.
Bei diesem Isomorphismus findet sich dann gerade:

$$\begin{aligned}
L_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s|\chi_\mathfrak{p}) &= 1 - \frac{\omega(\chi_1, \chi_2|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s} && \text{für} \quad \chi_\mathfrak{p} \not\sim 1,\\
L_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s|\chi_\mathfrak{p}) &= 1 && \text{für} \quad \chi_\mathfrak{p} \sim 1, \chi_\mathfrak{p} \neq 1,\\
L_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s|\chi_\mathfrak{p}) &= \zeta_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) && \text{für} \quad \chi_\mathfrak{p} = 1.
\end{aligned}$$

Dementsprechend werden fortan die Nullstellen

$$\omega(\chi_\mathfrak{p}|\mathfrak{p}) = \omega(\chi_1, \chi_2|\mathfrak{p})$$

als den Charakteren $\chi_\mathfrak{p}$ von $\mathfrak{G}_\mathfrak{p}$ zugeordnet aufgefaßt.

Für $\mathfrak{l} \mid \ell$ artet der analoge Isomorphismus aus. Einerseits ist $\mathfrak{G}_\mathfrak{l}$ als Galoisgruppe von $K_\mathfrak{l} = \mathsf{R}_\mathfrak{l}(\sqrt[\ell]{t}\,)$ über $\mathsf{R}_\mathfrak{l}$ nur zyklisch von der Ordnung $\mathfrak{l}$. Andrerseits sind das ℓ–te Potenzrestsymbol $\left(\frac{t}{\mathfrak{P}_\mathfrak{l}}\right)_\ell$ in $\mathsf{R}_\mathfrak{p}$ und $\left(\frac{x}{\mathfrak{l}}\right)_\ell$ in K beide identisch 1, weil die Restklassenkörper mod $\mathfrak{P}_\mathfrak{l}$ und mod $\mathfrak{l}$ endliche Körper der Charakteristik ℓ sind. Dementsprechend hat man hier durchweg $\chi_\mathfrak{p} \sim 1$ zu rechnen, und dann gelten die obigen Formeln für die L–Funktionen formal unverändert (nur die beiden letzten kommen vor).

Man kann nun die Galoisgruppe $\mathfrak{G}_\mathfrak{p}$ von $K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}$ im Falle $\mathfrak{p} \nmid \ell$ als isomorphes, im Falle $\mathfrak{l} \mid \ell$ als homomorphes Bild der Galoisgruppe $\mathfrak{G}$ von K/R auffassen, weil ja bei der Restabbildung mod $\mathfrak{p}$ im ersteren Falle die algebraische Struktur erhalten bleibt:

$$K = \mathsf{R}\left(\sqrt[\ell]{t}, \sqrt[\ell]{1-t}\,\right) \xrightarrow[\text{mod}\,\mathfrak{p}]{} K_\mathfrak{p} = \mathsf{R}_\mathfrak{p}\left(\sqrt[\ell]{t}, \sqrt[\ell]{1-t}\,\right),$$

während im letzteren Falle

$$K = \mathsf{R}\left(\sqrt[\ell]{t}, \sqrt[\ell]{1-t}\,\right) \xrightarrow[\text{mod}\,\mathfrak{l}]{} K_\mathfrak{l} = \mathsf{R}_\mathfrak{l}\left(\sqrt[\ell]{t}\,\right)$$

das zweite Radikal $\sqrt[\ell]{1-t} \equiv 1 - \sqrt[\ell]{t} \mod \mathfrak{l}$ wird, also sich auf das erste reduziert. Genauer gesagt handelt es sich hierbei im nicht–trivialen Falle $\mathfrak{p} \nmid \ell$ um einen festen, unabhängig von $\mathfrak{p}$ definierten Isomorphismus von $\mathfrak{G}$ auf $\mathfrak{G}_\mathfrak{p}$, dadurch gegeben, daß die Einheitswurzelfaktoren ζ aus K an den Radikalen unverändert als $\zeta \mod \mathfrak{p}$ aus $\mathsf{K}_\mathfrak{p}$ übertragen werden; man hat sich dabei $\mathsf{K}_\mathfrak{p}$ konkret als $\mathsf{K} \mod \mathfrak{p}$ gegeben vorzustellen. Dabei $\chi_\mathfrak{p} \not\sim 1$ invariant!

Legt man diese Auffassung zugrunde, geht man also von den Charakteren χ von $\mathfrak{G}$ aus und schreibt demgemäß die Nullstellen (Jacobischen Summen) einfacher in der Form

$$\omega(\chi|\mathfrak{p}) = \omega(\chi_\mathfrak{p}|\mathfrak{p}) = \omega(\chi_1, \chi_2|\mathfrak{p}),$$

so liegt es nahe, die für die Zetafunktion

$$\zeta_K(s) = \prod_\mathfrak{p} \zeta_{K_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s) = \prod_\mathfrak{p} \prod_{\chi_\mathfrak{p}} L_{\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}(s|\chi_\mathfrak{p})$$

vorzunehmende Produktbildung über alle Primdivisoren $\mathfrak{p}$ von K bereits in den einfacher gebauten L–Funktionen vorzunehmen, also mit der Produktbildung über die Charaktere $\chi_\mathfrak{p}$ von $\mathfrak{G}_\mathfrak{p}$ zu vertauschen. So wird man auf folgende neue Bildungen geführt, die sinngemäß als *L–Funktionen zu den Charakteren* χ (der Galoisgruppe $\mathfrak{G}$) von K/R zu bezeichnen sind:

$$\begin{aligned} L_\mathsf{R}(s|\chi) &= \prod_{\mathfrak{p}\nmid\ell}\left(1-\frac{\omega(\chi|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right) \quad \text{für} \quad \chi \not\sim 1, \\ L_\mathsf{R}(s|\chi) &= 1 \qquad\qquad\qquad\qquad \text{für} \quad \chi \sim 1, \chi \neq 1, \\ L_\mathsf{R}(s|\chi) &= \zeta_\mathsf{K}(s)\zeta_\mathsf{K}(s-1) \qquad \text{für} \quad \chi = 1. \end{aligned}$$

Bei dieser Definition hat man dann formal das Analogon der Klassenkörpertheoretischen Zerlegung:

$$\zeta_K(s) = \prod_\chi L_\mathsf{R}(s|\chi).$$

Die Frage, ob $\zeta_K(s)$ eine „vernünftige“ Zetafunktion ist, reduziert sich damit auf die Frage, ob die $L_\mathsf{R}(s|\chi)$ „vernünftige“ L–Funktionen sind.

Hierzu sei zunächst folgendes bemerkt. Im nicht–trivialen Fall $\chi \not\sim 1, \mathfrak{p} \nmid \ell$ hat man nach dem Gesagten, wenn man von den Gruppenelementen zu den Kongruenzdivisorenklassen als $\chi_\mathfrak{p}$–Argument übergeht:

$$\chi_\mathfrak{p}(\mathfrak{P}_\mathfrak{p}) = \left(\frac{t}{\mathfrak{P}_\mathfrak{p}}\right)_\ell^\nu \left(\frac{1-t}{\mathfrak{P}_\mathfrak{p}}\right)_\ell^{\nu'} \quad \text{mit} \quad \nu, \nu', \nu+\nu' \not\equiv 0 \mod \ell,$$

und damit

$$\omega(\chi|\mathfrak{p}) = \sum_{\mathfrak{N}(\mathfrak{P}_\mathfrak{p})=\mathfrak{N}(\mathfrak{p})} \left(\frac{t}{\mathfrak{P}_\mathfrak{p}}\right)_\ell^\nu \left(\frac{1-t}{\mathfrak{P}_\mathfrak{p}}\right)^{\nu'}$$

(wobei für Führerteiler $\mathfrak{P}_\mathfrak{p}$ die Potenzrestsymbole als 0 zu rechnen sind, ebenso wie ja in $\mathsf{K}_\mathfrak{p}$ die Charakterwerte für die Nullklasse mod $\mathfrak{p}$ als 0 gerechnet werden, sofern es sich nicht um den Hauptcharakter handelt). Man kann nun, analog zu dem eben durchgeführten Rückgang von $\mathfrak{G}_\mathfrak{p}$ zu $\mathfrak{G}$, also von $K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}$ zu K/R, auch hier die *Potenzrestsymbole* nach den Primdivisoren ersten Grades $\mathfrak{P}_\mathfrak{p}$ von $\mathsf{R}_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ als solche *nach den Punkten* $\mathfrak{p}, \mathfrak{P}_\mathfrak{p}$ *ersten Grades von* R auffassen. Die eingeführten L–Funktionen $L_\mathsf{R}(s|\chi)$ sind so mit einer *Klasseneinteilung der Punkte ersten Grades* $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ *des rationalen Funktionenkörpers* $\mathsf{R} = \mathsf{K}(t)$ verknüpft, ähnlich wie die Dirichletschen L–Funktionen

$L_{\mathsf{P}}(s|\chi)$ mit einer Klasseneinteilung der Primzahlen p des rationalen Zahlkörpers verknüpft sind. Ob es sinnvoll ist, diesem Gedanken nachzugehen, muß die weitere Entwicklung der noch in ihren Anfängen stehenden Theorie lehren.

Das jetzt zu besprechende Ergebnis von *A. Weil*, durch das meine Vermutung von 1938 über die „Vernünftigkeit“ der Bildungen $\zeta_K(s), L_{\mathsf{R}}(s|\chi)$ bestätigt wird, geht in der Tat nicht diesem Gedanken nach, die *Jacobischen Summen* $\omega(\chi|\mathfrak{p})$ als Kongruenzcharaktere der Punkte $(\mathfrak{p}, \mathfrak{P}_{\mathfrak{p}})$ von K aufzufassen, betrachtet vielmehr diese Summen einfacher *als Funktionen der Primdivisoren* $\mathfrak{p}$ *von* K.

A. Weil beweist, was im hier behandelten Falle der gewöhnlichen Fermatschen Gleichung besonders einfach geht, daß die $\omega(\chi|\mathfrak{p})$ die Werte eines *Heckeschen Größencharakters in* K *vom Führer* $\mathfrak{l}^2$ *oder* $\mathfrak{l}$ für die Primdivisoren $\mathfrak{p} \nmid \ell$ von K sind. Es läuft dies auf folgende Feststellung hinaus. Man definiere formal

$$\omega(\chi|\mathfrak{a}) = \prod_{\mathfrak{p}} \omega(\chi|\mathfrak{p})^{w_{\mathfrak{p}}(\mathfrak{a})}$$

für beliebige zu $\mathfrak{l}$ prime Divisoren $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{w_{\mathfrak{p}}(\mathfrak{a})}$ von K. Diese Bildung hat folgende drei bekannten Eigenschaften:

(1.) *Automorphieverhalten* $\quad \omega(\chi^r|\mathfrak{a}) = \omega(\chi|\mathfrak{a})^{\sigma_r^{-1}}$,
wo $\quad \sigma_r^{-1} = (\zeta \longrightarrow \zeta^r) \qquad (r \text{ prim zu } \ell)$

(2.) *Absoluter Betrag* $\quad |\omega(\chi|\mathfrak{a})| = \mathfrak{N}(\mathfrak{a})^{\frac{1}{2}}$.

(3.) *Primdivisorzerlegung* $\quad \omega(\chi, \mathfrak{a}) \cong \mathfrak{a}^{\sum_r \delta(\chi^r)\sigma_r}$,
wo $\quad \delta(\chi^r) = 0$ oder 1 und
r die primen Restkl. mod ℓ durchl.

Und zwar ist $\delta(\chi^r)$ durch Zurückgehen auf die obigen Exponenten ν, ν' mod ℓ von χ (also die Darstellung von χ durch Potenzrestsymbole) folgendermaßen bestimmt:

$\delta(\chi^r) =$ Übertragungszahl bei der Addition der kleinsten positiven Reste $\nu, \nu' \mod \ell$.

Aus diesen Eigenschaften folgert man nach dem Prinzip der arithmetischen Kennzeichnung algebraischer Zahlen aus Davenport–Hasse fast unmittelbar die folgende vierte Eigenschaft:

(4.) *Führereigenschaft* $\omega(\chi|\alpha) = 1$ für Zahlen $\alpha \equiv 1 \mod \mathfrak{l}^2$ aus K,

bei gewissen χ unter Umständen sogar für $\alpha \equiv 1 \mod \mathfrak{l}$, aber jedenfalls nicht für alle zu $\mathfrak{l}$ primen Zahlen α aus K.

Die Eigenschaften (3.), (4.) besagen, daß $\omega(\chi|\mathfrak{a})$ unter die Definition der Heckeschen Größencharaktere fällt; als Charakter sei er mit $\omega(\chi)$ bezeichnet.

Über den Führer konnte ich noch genauer folgende interessante Regel beweisen. Für denjenigen Charakter χ, der den Potenzrestsymbolen entspricht (Exponenten $\nu, \nu' \equiv 1 \mod \ell$), und seine Potenzen χ^r gilt:

> *$\omega(\chi)$ hat den Führer $\mathfrak{l}$ genau dann, wenn $\frac{2^\ell - 2}{\ell} \equiv 0 \mod \ell$ ist, wenn also ℓ eine Wieferichsche Primzahl ist.*

Dieser Zusammenhang des Größencharakters $\omega(\chi)$ mit einem Kriterium zur Fermatschen Vermutung zeigt, daß die entwickelte Theorie ev. Beiträge zu dieser Vermutung liefern kann, wie das ja auch schon daraus klar ist, daß die Zetafunktion $\zeta_K(s)$ mittels der Punkte $(\mathfrak{p}, \mathfrak{P}_\mathfrak{p})$ von K definiert ist und sicher etwas mit den algebraischen Primdivisoren $\mathfrak{P}$ von K, insbesondere denen ersten Grades, also den Lösungen in K der Fermatschen Gleichung zu tun hat.

Der Größencharakter $\omega(\chi)$ in K ist noch nicht, wie bei Hecke, auf (Normbeitrag 1, hier) (absoluten Betrag 1) normiert. Nach der Eigenschaft (2.) ergibt sich als zugehöriger normierter Größencharakter

$$\lambda(\chi|\mathfrak{a}) = \frac{\omega(\chi|\mathfrak{a})}{|\omega(\chi|\mathfrak{a})|} = \frac{\omega(\chi|\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^{\frac{1}{2}}}\,.$$

Schreibt man nun die obigen L–Funktionen in R mittels dieses normierten Größencharakters:

$$L_\mathsf{R}(s|\chi) = \prod_{\mathfrak{p}\nmid\ell} \left(1 - \frac{\lambda(\chi|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^{s-\frac{1}{2}}}\right) \quad \text{für} \quad \chi \not\sim 1,$$

so steht rechts gerade das Reziproke der Eulerschen Produktdarstellung der *Heckeschen L–Funktion* zu dem normierten Größencharakter $\lambda(\chi)$ in K.

Man hat demnach

$$\begin{aligned} L_{\mathsf{R}}(s|\chi) &= L_{\mathsf{K}}\left(s-\tfrac{1}{2}|\lambda(\chi)\right)^{-1} && \text{für} \quad \chi \not\sim 1, \\ L_{\mathsf{R}}(s|\chi) &= 1 && \text{für} \quad \chi \sim 1, \chi \neq 1, \\ L_{\mathsf{R}}(s|\chi) &= \zeta_{\mathsf{K}}(s)\zeta_{\mathsf{K}}(s-1) && \text{für} \quad \chi = 1, \end{aligned}$$

und somit

$$\zeta_K(s) = \zeta_{\mathsf{K}}(s)\zeta_{\mathsf{K}}(s-1)\prod_{\chi\not\sim 1} L_{\mathsf{K}}\left(s-\tfrac{1}{2}\Big|\lambda(\chi)\right)^{-1}.$$

Da die Heckeschen L–Funktionen $L_{\mathsf{K}}(s|\lambda)$ „vernünftige“ L–Funktionen sind, d. h. ganze Funktionen mit Funktionalgleichung des bekannten Typus bei $\left\{\begin{array}{c} s \longrightarrow 1-s \\ \lambda \longrightarrow \overline{\lambda} \end{array}\right\}$, ergibt sich, daß auch die neu eingeführten Funktionen $L_{\mathsf{R}}(s|\chi)$, $\zeta_K(s)$ „vernünftig“ sind, nämlich jedenfalls *meromorph* und mit *Funktionalgleichung* des bekannten Typus bei $\left\{\begin{array}{c} s \longrightarrow 2-s \\ \lambda \longrightarrow \overline{\lambda} \end{array}\right\}$.

$\zeta_K(s)$ hat Pole erster Ordnung bei $s=1, s=2$, ferner bei den nicht–trivialen Nullstellen der $L_{\mathsf{K}}\left(s-\frac{1}{2}|\lambda(\chi)\right)$, also vermutlich auf der hier kritischen Geraden $\Re(s)=1$ und nicht–triviale Nullstellen auf den beiden hier ebenfalls kritischen Geraden $\Re(s)=\frac{1}{2}, \frac{3}{2}$.

1.23 Mainz 1953

Zetafunktion arithmetischer Funktionenkörper.

Vortrag auf DMV–Tagung Mainz, 24. 9. 53

Gliederung.

I. Allgemeine Grundlagen.

§1. Arithmetische Funktionenkörper.

Arithmetischer Funktionenkörper (vom Transzendenzgrad 1):

K algebraischer Funktionenkörper (vom Transzendenzgrad 1) über einem endlich–algebraischen Zahlkörper K als Konstantenkörper.

Erzeugung durch Transzendente t in folgenden beiden Schritten:

K	endlich–algebraischer Zahlkörper,
$\mathsf{R} = \mathsf{K}(t)$	rationaler Funktionenkörper vom Transzendenzgrad 1 über K,
K/R	endlich–algebraische Erweiterung, fremd zu absolut–algebraischen Erweiterungen.

Analogie zu algebraischem Funktionenkörper K vom Transzendenzgrad 2 über beliebigem Körper Ω; dabei

$\mathsf{K} = \Omega(x)$	rationaler Funktionenkörper vom Transzendenzgrad 1,
$\mathsf{R} = \Omega(x,t)$	rationaler Funktionenkörper vom Transzendenzgrad 2,
K/R	endlich–algebraische Erweiterung.

Zur Analogie oben besser P statt K; und K dann als genauen Konst. Kp. einführen.

Aber in diesem *algebraischen* Fall ist Symmetrie in x, t vorhanden, im *arithmetischen* Fall besteht zwischen K und t als Erzeugenden je einer Arithmetik keine Symmetrie, sondern echte Stufung.

§2. Primdivisoren, Punkte.

Aufgabe ist, die bekannte Relativarithmetik in K/K durch die Arithmetik in K zu unterbauen. Dies geschieht auf der Grundlage der Theorie der Exponentenbewertungen folgendermaßen:

a.) Relativarithmetik in K/K entspringt aus denjenigen Bewertungen von K, bei denen K identisch bewertet; liefert die *algebraischen Primdivisoren* $\mathfrak{P}$ von K.

b.) Arithmetik von K entspringt aus den nicht–identischen Bewertungen von K; liefert die Primdivisoren $\mathfrak{p}$ von K. Es handelt sich um deren sämtliche Fortsetzungen auf K. Diese schwer zu übersehen; es genügt jedoch hinreichend große Teilmenge. Dazu zeichne man eine Transzendente t aus K aus. Für den rationalen Teilkörper $\mathsf{R} = \mathsf{K}(t)$ heben sich die eindeutigen Fortsetzungen der $\mathfrak{p}$ als *t–Funktionalprimdivisoren* von R hervor:

$$1, t, t^2, \ldots \text{ sind ganz für } \mathfrak{p} \text{ und bleiben mod } \mathfrak{p} \text{ linear unabhängig.}$$

Diese $\mathfrak{p}$ setzen sich in bekannter Weise auf je endlich viele Weisen von R auf die endlich–algebraische Erweiterung K fort; mit bestimmten Zerlegungsanzahlen, Restklassengraden, Verzweigungsordnungen. So entsteht ein ausreichendes System von *arithmetischen Primdivisoren* $\mathfrak{p}$ von K.

Ausreichend in dem Sinne, daß durch die Bewertungen zu den $\mathfrak{P}, \mathfrak{p}$ die Elemente von K eindeutig bis auf Einheiten von K gekennzeichnet. *Restklassenkörper*:

$$\begin{aligned} &\text{algebraische } \mathfrak{P} \longrightarrow K_{\mathfrak{P}} \text{ endl.–alg. Erw. von } \mathsf{K} \text{ (alg. Zahlkp.)} \\ &\text{arithmetische } \mathfrak{p} \longrightarrow K_{\mathfrak{p}} \text{ endl.–alg. Erw. von } \mathsf{K}_{\mathfrak{p}} \text{ (Kongr. Funkt. Kp.)} \end{aligned}$$

Zerlegungsgesetz für die t–Funktionalprimdivisoren von $\mathsf{R} = \mathsf{K}(t)$ in arithmetische Primdivisoren von K. Nach Deuring gilt jedenfalls für *fast* alle $\mathfrak{p}$ von K:

1.) $\mathfrak{p}$ in K unzerlegt und unverzweigt, vielmehr nur träge mit separablem Restklassenkörper $K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}$.

2.) $\mathsf{K}_{\mathfrak{p}}$ der genaue Konstantenkörper von $K_{\mathfrak{p}}$.

3.) Geschlecht $g_{\mathfrak{p}}$ von $K_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}}$ stimmt überein mit Geschlecht g von K/K.

□□□

Diese arithmetischen $\mathfrak{p}$ von R mögen *regulär* heißen. Für die Theorie der Zetafunktion von K wird aber, wenn man sie nicht nur bis auf endlich viele $\mathfrak{p}$ genau haben will, auch das *Zerlegungsverhalten der irregulären* $\mathfrak{p}$ *von* R gebraucht. Dies allgemein anzupacken, erscheint als ein sehr schwieriges Problem.

Neben dem Primdivisorsystem $\mathfrak{P}, \mathfrak{p}$ von K wird — in Analogie zur Theorie der algebr. Funkt. Kp. vom Transzendenzgrad 2 — auch ein ausreichendes System von *Punkten* von K gebraucht. Durch Verfolgung der Analogie erhält man folgende Vorschrift zur Definition eines solchen Punktsystems.

Betrachte zweistufige Homomorphismen von K:

$$K \xrightarrow[\bmod \mathfrak{p}]{} K_{\mathfrak{p}} \xrightarrow[\bmod \mathfrak{P}_{\mathfrak{p}}]{} K_{\mathfrak{p},\mathfrak{P}_{\mathfrak{p}}}$$

$\mathfrak{p}$ arithm. Primdiv. von K, $\quad$ $\mathfrak{P}_{\mathfrak{p}}$ Primdiv. von $K_{\mathfrak{p}}$

Punkte $(\mathfrak{p}, \mathfrak{P}_{\mathfrak{p}})$ liefern Restabbildung auf endliche Körper $K_{\mathfrak{p},\mathfrak{P}_{\mathfrak{p}}}$; deren Elementanzahl ist $\mathfrak{N}(\mathfrak{P}_{\mathfrak{p}})$, eine gewisse Potenz von $\mathfrak{N}(\mathfrak{p})$.

□□□

Definition der Punkte nach Mitteilung von *Roquette* auch mittels der allgemeinen Krullschen Bewertungen (mit zweistufig nicht–archimedischer Wertgruppe) möglich.

§3. Die Zetafunktion.

Definition

$$\zeta_K(s) = \prod_{\mathfrak{p},\mathfrak{P}_{\mathfrak{p}}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P}_{\mathfrak{p}})^s}} \quad \Big[\mathfrak{N}(\mathfrak{p}, \mathfrak{P}_{\mathfrak{p}}) = \mathfrak{N}(\mathfrak{P}_{\mathfrak{p}})\Big],$$

wo $\mathfrak{p}$ alle arithmetischen Primdivisoren von K (in bezug auf eine feste Transzendente t) und $\mathfrak{P}_{\mathfrak{p}}$ jeweils alle Primdivisoren des Restklassenkörpers $K_{\mathfrak{p}}$ durchläuft.

Frage der Unabhängigkeit von t, d. h. birationalen Invarianz.

Vermutung erscheint gewagt; jedoch Analogie zu Geschlecht.

Ausmultiplikation über die $\mathfrak{P}_\mathfrak{p}$ liefert:

$$\zeta_K(s) = \prod_\mathfrak{p} \zeta_{K_\mathfrak{p}}(s),$$

d. h. Darstellung der Zetafunktion von K als Produkt der Zetafunktionen der zugeordneten Kongruenzfunktionenkörper $K_\mathfrak{p}$.

Definition analogisiert das Eulersche Produkt. Es entsteht Frage nach der Dirichletschen Reihe. Dazu hätte man die Dirichletschen Reihen für die $\zeta_{K_\mathfrak{p}}(s)$ auszumultiplizieren und ein Koeffizientengesetz zu suchen, das in der Arithmetik von K wurzelt. Vielleicht hilft hierzu die von *Roquette* in Aussicht gestellte Definition der Punkte mittels der allgemeinen Krullschen Bewertungen.

Meine Vermutung aus den dreißiger Jahren: $\zeta_K(s)$ ist meromorphe Funktion mit Funktionalgleichung und entsprechenden Eigenschaften wie $\zeta_\mathsf{K}(s)$.

Neuerdings von *A. Weil* bestätigt für arithmetische Funktionenkörper vom *Fermatschen Typus*:

$$K = \mathsf{K}(u_1, u_2) \quad \text{mit} \quad \frac{u_1^{m_1}}{\gamma_1} + \frac{u_2^{m_2}}{\gamma_2} = 1$$

K bel. alg. Zahlkp.,
m_1, m_2 bel. nat. Zahlen,
$\gamma_1, \gamma_2 \neq 0$ bel. Zahlen aus K,

Ausgezeichnete Unbestimmte

$$t = \frac{u_1^{m_1}}{\gamma_1}, \qquad 1 - t = \frac{u_2^{m_2}}{\gamma_2}, \qquad \mathsf{R} = \mathsf{K}(t)$$
$$K = \mathsf{R}\left(\sqrt[m_1]{\gamma_1 t},\ \sqrt[m_2]{\gamma_2(1-t)}\right).$$

Von *Deuring*, gestützt auf abstrakte Begründung der komplexen Multiplikation und im Grunde auf frühere Formel von mir zum Zerlegungsgesetz, auch bestätigt für elliptische Funktionenkörper mit komplexem Multiplikatorenring.

Sowohl bei *Weil* als auch bei *Deuring* $\zeta_K(s)$ jeweils nur bis auf die endlich vielen irregulären $\mathfrak{p}$ in Betracht gezogen.

Zwei Grundlagen für meine Vermutung:

a.) Für *rationalen* Funktionenkörper $\mathsf{R} = \mathsf{K}(t)$ wird

$$\zeta_{\mathsf{R}_\mathfrak{p}}(s) = \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}} \quad \frac{1}{1 - \frac{\mathfrak{N}(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}} ,$$

also

$$\zeta_{\mathsf{R}}(s) = \zeta_{\mathsf{K}}(s) \quad \zeta_{\mathsf{K}}(s-1),$$

insbesondere *unabhängig von der Wahl der Transzendenten* t aus R unter *allen* $\frac{\alpha t+\beta}{\gamma t+\delta}$, nicht nur den ganzen unimodularen, bei denen die t–Funktionalprimdivisoren invariant sind.

$\zeta_{\mathsf{R}}(s)$ ist in der Tat meromorph und genügt einer Funktionalgleichung des bekannten Typus bei $s \longrightarrow 2 - s$.

b.) Für *beliebigen* arithmetischen Funktionenkörper K kann man aus den oben erwähnten Resultaten von *Deuring* über das Zerlegungsverhalten der t–Funktionalprimdivisoren von R in K schließen, daß von den endlich vielen Beiträgen der irregulären $\mathfrak{p}$ abgesehen gilt:

$$\zeta_K(s) \sim \zeta_{\mathsf{K}}(s)\zeta_{\mathsf{K}}(s-1) \prod_{i=1}^{2g} \prod_{\mathfrak{p}} \left(1 - \frac{\omega_i(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right),$$

wo jeweils $\omega_i(\mathfrak{p})$ die $2g$ Nullstellen von $\zeta_{K_\mathfrak{p}}(s)$ (in $\mathfrak{N}(\mathfrak{p})^s$ gemessen) durchläuft. Nach der von *A. Weil* bewiesenen Riemannschen Vermutung in Kongruenzfunktionenkörpern sind nun die Beträge

$$|\omega_i(\mathfrak{p})| = \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}}.$$

Daraus liest man ab, daß $\zeta_K(s)$ jedenfalls für $\Re(s) > \frac{3}{2}$ analytisch ist, mit einzigem Pol erster Ordnung bei $s = 2$.

II. Der Spezialfall vom Fermatschen Typus.

§4. Das Zerlegungsgesetz für die arithmetischen Primdivisoren.

Allgemeiner Fermatscher Typus:

$$K = \mathsf{K}(u_1, u_2) \quad \text{mit} \quad \frac{u_1^{m_1}}{\gamma_1} + \frac{u_2^{m_2}}{\gamma_2} = 1,$$

K bel. alg. Zahlkp.,
m_1, m_2 bel. nat. Zahlen,
$\gamma_1, \gamma_2 \neq 0$ bel. Zahlen aus K,

$$t = \frac{u_1^{m_1}}{\gamma_1}, \quad 1 - t = \frac{u_2^{m_2}}{\gamma_2}, \quad \mathsf{R} = \mathsf{K}(t)$$
$$K = \mathsf{R}\left(\sqrt[m_1]{\gamma_1 t}\ \sqrt[m_2]{\gamma_2(1-t)} \right)$$

Bei Betrachtung eines festen arithmetischen Primdivisors $\mathfrak{p}$ von R kann man γ_1, γ_2 ganz für $\mathfrak{p}$ und frei von m_1–ten, m_2–ten Potenzen für $\mathfrak{p}$ normieren und erhält so für jedes $\mathfrak{p}$ eine besondere Normierung von u_1, u_2, während ausgezeichnete Transzendente t fest ist.

Geschlecht:	$2g = (m_1 - 1)(m_2 - 1) - (m_0 - 1), \quad m_0 = (m_1, m_2)$
Regulär:	alle $\mathfrak{p}$, die nicht in m_1, m_2 und nicht in den m_1, m_2–Kernen von γ_1, γ_2 stecken.

Für die irregulären $\mathfrak{p}$ wird Zerlegungsgesetz sehr kompliziert; viele Fallunterscheidungen.

Spezieller Fermatscher Typus:

K enthält die m–ten Einheitswurzeln, $m = [m_1, m_2]$
$\gamma_1, \gamma_2 = 1$, also $u_1^{m_1} + u_2^{m_2} = 1$.

Dann K bizyklisch vom Typus $\{m_1, m_2\}$.

$$K = \mathsf{R}_1\mathsf{R}_2 \quad \text{mit} \quad \mathsf{R}_1 = \mathsf{R}\left(\sqrt[m_1]{t}\right),\ \mathsf{R}_2 = \mathsf{R}\left(\sqrt[m_2]{1-t}\right).$$

Zerlegungsgesetz lautet dann:

$\mathfrak{p}$ *stets unzerlegt, also nur einen einzigen Primteiler*

Regulärer Fall $\mathfrak{p} \nmid m$ (Spezialfall):

$$K_\mathfrak{p} = \mathsf{R}_\mathfrak{p}\left(\sqrt[m_1]{t},\ \sqrt[m_2]{1-t} \right), \quad g_\mathfrak{p} = g.$$

Irregulärer Fall $\mathfrak{p} \mid m$ (allgemeiner Fall):

$$K_\mathfrak{p} = \mathsf{R}'_\mathfrak{p}\left(\sqrt[m'_1]{t'},\ \sqrt[m'_2]{1-t'} \right) \quad \text{mit} \quad \mathsf{R}'_\mathfrak{p} = \mathsf{R}_\mathfrak{p}(t') = \mathsf{R}_\mathfrak{p}^{\frac{1}{qq'_0}}, \quad t'^{q_0 q'_0} \equiv t \mod \mathfrak{p},$$
$$2g_\mathfrak{p} = (m'_1 - 1)(m'_2 - 1) - (m'_0 - 1),$$

wo m_1', m_2', m_0' die zu p primen Bestandteile von m_1, m_2, m_0 und q, q_0 die p–Potenzen in m, m_0, sowie q_0' nicht näher bestimmter Teiler von q_0.

In jedem Falle läßt sich ein eindeutig bestimmter *Restklassenhomomorphismus* der Galoisgruppe $\mathfrak{G}$ von K/R auf die Galoisgruppe $\mathfrak{G}_\mathfrak{p}$ von $K_\mathfrak{p}/\mathsf{R}_\mathfrak{p}$ definieren, nämlich durch Anwendung der S aus $\mathfrak{G}$ auf die erzeugenden Radikale und Übertragung der Einheitswurzelfaktoren ζ aus K als $\zeta \mod \mathfrak{p}$ aus $\mathsf{K}_\mathfrak{p}$. Im regulären Falle ist das sogar ein Isomorphismus.

Dabei werden die Charaktere χ von $\mathfrak{G}$ homomorph abgebildet auf die Charaktere $\chi_\mathfrak{p}$ von $\mathfrak{G}_\mathfrak{p}$ und diese weiter nach dem Artinschen Reziprozitätsgesetz isomorph auf die Charakterpaare χ_1, χ_2 der Exponenten m_1, m_2 von $\mathsf{K}_\mathfrak{p}$, nämlich mittels der Potenzrestsymbole:

$\mathfrak{G}_\mathfrak{p}$ dargestellt durch das Artinsymbol $\left(\frac{K/\mathsf{R}}{\mathfrak{P}_\mathfrak{p}}\right)$, wo $\mathfrak{P}_\mathfrak{p}$ die Primdiv. ersten Grades von $\mathsf{R}_\mathfrak{p}$ durchläuft, gegeben durch $t - \xi \cong \frac{\mathfrak{P}_\mathfrak{p}}{[\ldots]}$, $\xi \mod \mathfrak{p}$, ξ in K.

Anwendung von $\left(\frac{K/\mathsf{R}}{\mathfrak{P}_\mathfrak{p}}\right)$ auf Radikale $\sqrt[m_1]{t}$, $\sqrt[m_2]{1-t}$ liefert Charaktere von $\mathfrak{G}_\mathfrak{p}$. Diese Anwendung stellt sich so dar:

$$\left(\frac{t}{\mathfrak{P}_\mathfrak{p}}\right)_{m_1} = \left(\frac{\xi}{\mathfrak{p}}\right)_{m_1}, \quad \left(\frac{1-t}{\mathfrak{P}_\mathfrak{p}}\right)_{m_2} = \left(\frac{1-\xi}{\mathfrak{p}}\right)_{m_2}$$

mit Potenzrestsymbolen in $\mathsf{R}_\mathfrak{p}$ bzw. $\mathsf{K}_\mathfrak{p}$.

Im folgenden interessieren diejenigen Charakterpaare χ_1, χ_2 von $\mathsf{K}_\mathfrak{p}$, für welche

$$\chi_1 \neq 1, \quad \chi_2 \neq 1, \quad \chi_1\chi_2 \neq 1 \qquad \text{kurz} \quad (\chi_1, \chi_2) \not\sim 1$$

ist.Ihnen sind als Urbilder isomorph zugeordnet diejenigen Charaktere $\chi_\mathfrak{p}$ von $\mathfrak{G}_\mathfrak{p}$, für welche

$\chi_\mathfrak{p}$ nicht schon Charakter eines der Teilkörper

$$\mathsf{R}_\mathfrak{p}\left(\sqrt[m_1]{t}\right), \mathsf{R}_\mathfrak{p}\left(\sqrt[m_2]{1-t}\right), \mathsf{R}_\mathfrak{p}\left(\sqrt[m_0]{\frac{t}{1-t}}\right)$$

ist, kurz $\chi_\mathfrak{p} \not\sim 1$.

Diesen wieder entspringen homomorph aus denjenigen Charakteren χ von $\mathfrak{G}$, für welche

χ nicht schon Charakter eines der Teilkörper

$$\mathsf{R}\left(\sqrt[m_1]{t}\right), \mathsf{R}\left(\sqrt[m_2]{1-t}\right), \mathsf{R}\left(\sqrt[m_0]{\frac{t}{1-t}}\right),$$

ist, kurz $\chi \not\sim 1$.

Es gilt also

$$\chi \sim 1 \longrightarrow \chi_{\mathfrak{p}} \sim 1, \qquad \chi \not\sim 1 \longleftarrow \chi_{\mathfrak{p}} \not\sim 1,$$

aber nicht notwendig umgekehrt.

§5. Aufspaltung der Kongruenzzetafunktion in Kongruenz–*L*–Funktionen.

Nach *Davenport–Hasse* hat man die klassenkörpertheoretische Zerlegung

$$\zeta_{K_{\mathfrak{p}}}(s) = \zeta_{\mathsf{R}_{\mathfrak{p}}}(s) \prod_{\chi_{\mathfrak{p}} \not\sim 1} L(s|\chi_{\mathfrak{p}})$$

mit den *Kongruenz–L–Funktionen*

$$L(s|\chi_{\mathfrak{p}}) = 1 - \frac{\omega(\chi_1, \chi_2)}{\mathfrak{N}(\mathfrak{p})^s}, \qquad \chi_{\mathfrak{p}} \longleftrightarrow (\chi_1, \chi_2)$$

wo

$$= \sum_{\substack{\xi_1, \xi_2 \bmod \mathfrak{p} \\ \xi_1 + \xi_2 \equiv 1 \bmod \mathfrak{p}}} \chi_1(\xi_1)\chi_2(\xi_2)$$

die sogen. *Jacobischen Summen.*

Diese können nach dem eben Gesagten als den Charakteren χ von $\mathfrak{G}$ zugeordnet angesehen werden, und zwar sei festgesetzt:

$$\omega(\chi|\mathfrak{p}) = \omega(\chi_1, \chi_2), \quad \text{wenn} \quad \chi_{\mathfrak{p}} \not\sim 1, \quad \chi_{\mathfrak{p}} \longleftrightarrow (\chi_1, \chi_2)$$
$$\omega(\chi|\mathfrak{p}) = 0, \quad \text{wenn} \quad \chi_{\mathfrak{p}} \sim 1.$$

Dann hat man

$$\zeta_{K_{\mathfrak{p}}}(s) = \zeta_{\mathsf{R}_{\mathfrak{p}}}(s) \prod_{\chi \not\sim 1} \left(1 - \frac{\omega(\chi|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right).$$

Durch Multiplikation über alle $\mathfrak{p}$ erhält man:

$$\zeta_K(s) = \zeta_{\mathsf{R}}(s) \prod_{\chi \not\sim 1} L_{\mathsf{R}}(s|\chi)$$

mit

$$L_{\mathsf{R}}(s|\chi) = \prod_{\mathfrak{p}} L_{\mathsf{R}_\mathfrak{p}}(s|\chi_\mathfrak{p}) = \prod_{\mathfrak{p}} \left(1 - \frac{\omega(\chi|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right) \quad \text{für} \quad \chi \not\sim 1.$$

Diese Bildung kann als L–Funktion zu einer Kongruenzklasseneinteilung der *Punkte ersten Grades* $(\mathfrak{p},\ \mathfrak{P}_\mathfrak{p})$ in R angesehen werden, entsprechend der Schreibweise: [1]

$$L_{\mathsf{R}}(s|\chi) = \prod_{\mathfrak{p}} \prod_{\mathfrak{P}_\mathfrak{p}} \frac{1}{1 - \frac{\chi_\mathfrak{p}(\mathfrak{P}_\mathfrak{p})}{\mathfrak{N}(\mathfrak{P}_\mathfrak{p})^s}} = \prod_{\mathfrak{p}} L_{\mathsf{R}_\mathfrak{p}}(s|\chi_\mathfrak{p}).$$

§6. Die Jacobischen Summen als Größencharaktere.

Es handelt sich jetzt um die Abhängigkeit der Jacobischen Summen $\omega(\chi|\mathfrak{p})$ von dem Primdivisor $\mathfrak{p}$ von K.

A. Weil hat allgemein gezeigt, daß die $\omega(\chi|\mathfrak{p})$ für *reguläre* $\mathfrak{p}$ die Primdivisorwerte eines *Heckeschen Größencharakters* $\omega(\chi|\mathfrak{a})$ von K sind, dessen Führer jedenfalls ein Teiler von m^2 ist.

Da meine Untersuchungen zur Einbeziehung auch der *irregulären* $\mathfrak{p}$ für beliebige Exponenten m_1, m_2 und beliebigen Körper K (der die m–ten E. W. enthält) noch nicht abgeschlossen sind, beschränke ich mich fortan auf den Spezialfall:

$$m_1 = m_2 = m_0 = m = \ell \neq 2 \quad \textit{Primzahl}$$

der gewöhnlichen Fermatschen Gleichung $u_1^\ell + u_2^\ell = 1$ über dem Körper

$$\mathsf{K} = \mathsf{P}(\zeta), \quad \zeta = \sqrt[\ell]{1}\,, \quad \text{der } \ell\text{–ten Einheitswurzeln.}$$

Hier läßt sich das Weilsche Resultat ganz einfach aus den Ergebnissen von *Davenport–Hasse* folgern.

1. teilweise undeutlich

Setze

$$\omega(\chi|\mathfrak{a}) = \prod_{\mathfrak{p}} \omega(\chi|\mathfrak{p})^{w_{\mathfrak{p}}(\mathfrak{a})}$$

für beliebige Divisoren $\mathfrak{a}$ von K, die zu dem einzigen irregulären Primdivisor $\mathfrak{l}|\ell$ mit $\mathfrak{l}^{\ell-1} \cong \ell$ prim sind. Dann bestehen nach *Davenport–Hasse* folgende Eigenschaften:

(1.) *Automorphieverhalten* $\omega(\chi^r|\mathfrak{a}) = \omega(\chi|\mathfrak{a})^{\sigma_r}$ wo $\sigma_r^{-1} = (\zeta \longrightarrow \zeta^r)$ (r prim zu ℓ).

(2.) *Absoluter Betrag* $\omega(\chi|\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^{\frac{1}{2}}$.

(3.) *Primdivisorzerlegung* $\omega(\chi|\mathfrak{a}) \cong \mathfrak{a}^{\sum_r \delta(\chi^r)\sigma_r}$ (r prim zu ℓ),

wo $\delta(\chi^r) = 0$ oder 1 die Übertragungszahl bei der Addition der kleinsten positiven Reste $r\mu_1, r\mu_2 \mod \ell$ ist, die den Exponenten $\mu_1, \mu_2 \mod \ell$ von χ bei der Darstellung durch Potenzrestsymbole entsprechen.

Aus diesen Eigenschaften folgert man nach dem Prinzip der arithmetischen Kennzeichnung fast unmittelbar, schärfer als bei Weil:

(4.) *Führereigenschaft* $\omega(\chi|\alpha) = 1$ für Zahlen $\alpha \equiv 1 \bmod \mathfrak{l}^2$ aus K,

bei gewissen χ unter Umständen sogar für $\alpha \equiv 1 \mod \mathfrak{l}$, aber sicher nicht für alle zu $\mathfrak{l}$ primen α.

Die Eigenschaften (3.), (4.) besagen, daß $\omega(\chi|\mathfrak{a})$ unter die Definitionsforderungen der Heckeschen Größencharaktere fällt; dieser Größencharakter werde kurz mit $\omega(\chi)$ bezeichnet.

Normierter Größencharakter $\lambda(\chi)$

Über die Alternative, ob der Führer $\mathfrak{l}^2$ oder $\mathfrak{l}$ ist, konnte ich noch genauer folgende interessante Regel beweisen. Für diejenigen Charaktere χ^r, die aus χ mit den Exponenten $1, 1 \mod \ell$ entspringen, gilt:

$\omega(\chi^r)$ hat den Führer $\mathfrak{l}$ genau dann, wenn $\frac{2^\ell-2}{\ell} \equiv 0 \mod \ell$ ist, wenn also ℓ eine Wieferichsche Primzahl ist.

Allgemeiner bei $1, \mu$ tritt Frage nach $\sum_{(\mu+1)r \leqq \ell} \frac{1}{r} \mod \ell$ auf.

Meine Ansätze erscheinen auch zur Behandlung des allgemeineren Falles beliebiger Exponenten m_1, m_2 geeignet. So konnte ich zum Beispiel auch im Falle $m_1 = m_2 = m_0 = m = 2^2$ durchkommen und fand abweichend von Weil

$$\omega(\chi) \text{ hat } \begin{cases} \text{Führer } 4 & \text{für Exponenten} & (\mu_1, \mu_2) \equiv \pm(1,1) & \bmod 4 \\ \text{Führer } 2\mathfrak{l} & \text{für Exponenten} & (\mu_1, \mu_2) \equiv \pm(1,2), \pm(2,1) & \bmod 4. \end{cases}$$

§7. Aufspaltung der Zetafunktion in *L*–Funktionen.

Durch Ausführung der Multiplikation über alle Primdivisoren $\mathfrak{p}$ von K ergibt sich für die Zetafunktion von K die Aufspaltung

$$\zeta_K(s) = \zeta_{\mathsf{R}}(s) \prod_{\chi \not\sim 1} L_{\mathsf{R}}(s|\chi) = \zeta_{\mathsf{K}}(s)\zeta_{\mathsf{K}}(s-1) \prod_{\chi \not\sim 1} L_{\mathsf{K}}\Big(s - \frac{1}{2}\Big|\omega(\chi)\Big)^{-1}$$

mit

$$L_{\mathsf{K}}\Big(s - \frac{1}{2}\Big|\omega(\chi)\Big) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\omega(\chi|\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\lambda(\chi,\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^{s-\frac{1}{2}}}} \ ,$$

wo der Tatsache $|\omega(\chi, \mathfrak{p})| = \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}}$ entsprechend der zugeordnete auf Betrag 1 normierte Heckesche Größencharakter durch

$$\omega(\chi, \mathfrak{p}) = \frac{\lambda(\chi, \mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^{\frac{1}{2}}}$$

definiert ist.

Demnach ist $\zeta_K(s)$ eine meromorphe Funktion mit einer Funktionalgleichung bei $s \longrightarrow 2 - s$, und mit Polen erster Ordnung bei $s = 1, s = 2$ sowie bei den nicht–trivialen Nullstellen der $L_{\mathsf{K}}\Big(s - \frac{1}{2}\Big|\omega(\chi)\Big)$.

Für *beliebige Exponenten* m_1, m_2 gilt Entsprechendes, wenn es noch gelingt zu zeigen, daß alle Primteiler $\mathfrak{p}$ von m wirklich im Führer von $\omega(\chi)$ aufgehen, was nicht schwierig erscheint.

Für *echte Erweiterungskörper* K des m–ten Einheitswurzelkörpers Z erweist sich ganz einfach $\omega(\chi)$ als derjenige Größencharakter von K, der durch Normbildung mit dem wie vorstehend definierten von Z zusammenhängt.

Wie gesagt:

Grundlage für neue arithmetische Theorie, an einfachem, bis ins letzte Detail durchsichtigen Beispiel erläutert, als Richtlinie für weitere Ausgestaltung der Theorie im allgemeinen Fall.

Es erheben sich nach Analogie der Zahlkörpertheorie mannigfache Fragen, so z. B. nach Herausarbeiten der entsprechenden Dichtigkeitssätze über

diophantische Gleichungen, wo ja gerade der behandelte Spezialfall besonders interessant wäre.

Vor allem aber nach einer Einsicht in den klassenkörpertheoretischen Mechanismus, nach dem gerade die Heckeschen L–Funktionen bei den arithmetischen Funktionenkörpern auftreten.

1.24 Istanbul 1955

Über das Analogon zur Riemannschen Vermutung in Kongruenzfunktionenkörpern.

Vortrag Istanbul, 26. 3. 1955

§1. Gewöhnliche Riemannsche Vermutung und Primzahlsatz.

Die Theorie der Verteilung der Primzahlen fragt nach einem expliziten Ausdruck für die Anzahlfunktion

$$\pi_0(x) = \sum_{p \leqq x} 1$$

der Primzahlen p unter einer gegebenen (reell–positiven) Schranke x, und zwar soll der explizite Ausdruck so beschaffen sein, daß man aus ihm eine möglichst gute elementare Annäherungsfunktion ablesen und die Größenordnung des Fehlerglieds bei $x \longrightarrow \infty$ abschätzen kann. Es ist das eine Aufgabe über eine statistische Verteilung, wobei als Grundereignis die Eigenschaft einer natürlichen Zahl n auftritt, eine Primzahl p zu sein.

1. *Riemann* hat zur Behandlung dieser Aufgabe analytische Methoden herangezogen, deren Grundgedanken bereits auf *Euler* und *Dirichlet* zurückgehen. Er betrachtet die über alle natürlichen Zahlen n erstreckte Dirichletsche Reihe

$$\zeta(s) = \sum_n \frac{1}{n^s},$$

und zwar als Funktion einer komplexen Variablen s. Als solche konvergiert sie für $\Re(s) > 1$. Sie erweist sich durch das Schleifenintegral

$$\frac{1}{2\pi i} \int_{\leftarrow\circ} \frac{z^s}{e^{-z}-1} \frac{dz}{z} = \frac{\sin \pi s}{\pi} \Gamma(s)\zeta(s) = \frac{1}{\Gamma(1-s)} \zeta(s)$$

in die ganze s–Ebene analytisch fortsetzbar mit einzigem

Pol 1. Ordnung bei $s = 1$, Residuum 1.

Ihr Zusammenhang mit den Primzahlen p wird geliefert durch die Eulersche Identität

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}} ,$$

gültig im Konvergenzgebiet $\Re(s) > 1$ der zum Ausgang genommenen Dirichletschen Reihe.

2. Die analytische Behandlung des Primzahlproblems beruht darauf, daß sich vermöge dieser Eulerschen Identität eine mit $\pi_0(x)$ eng verwandte Anzahlfunktion $\pi(x)$ ausdrücken läßt. Die Dirichletsche Reihe

$$-\log\zeta(s) = \sum_p \sum_\nu \frac{1}{\nu}\frac{1}{p^{\nu s}} \qquad \big(\Re(s) > 1\big)$$

hat nämlich die Koeffizientenpartialsumme

$$\pi(x) = \sum_{p^\nu \leqq x} \frac{1}{\nu} = \pi_0(x) + \frac{1}{2}\pi_0(x^{\frac{1}{2}}) + \frac{1}{3}\pi_0(x^{\frac{1}{3}}) + \cdots$$

Für die analytische Behandlung ist es zweckmäßig, diese abgerundete Anzahlfunktion $\pi(x)$ zugrundezulegen, bei der nicht nur die Primzahlen p selbst, sondern auch ihre Potenzen p^ν gezählt werden, und zwar mit den Gewichten $\frac{1}{\nu}$. Außerdem soll für ganzzahliges x, wenn speziell $x = p^\nu$ ist, diese letzte Primzahlpotenz nur halb, also mit dem Gewicht $\frac{1}{2\nu}$, gezählt werden. Die Abrundung von $\pi_0(x)$ zu $\pi(x)$ ist so, daß ihr Effekt von dem nachher anzugebenden Restglied in der Primzahlformel verschluckt wird.

3. Man kann die analytische Behandlung noch etwas einfacher gestalten, indem man zur logarithmischen Ableitung übergeht:

$$-\frac{d}{ds}\log\zeta(s) = -\frac{\zeta'(s)}{\zeta(s)} = \sum_p \sum_\nu \frac{\log p}{p^{\nu s}} \qquad \big(\Re(s) > 1\big).$$

Deren Koeffizientenpartialsumme

$$\psi(x) = \sum_{p^\nu \leqq x} \log p = \psi_0(x) + \psi_0(x^{\frac{1}{2}}) + \psi_0(x^{\frac{1}{3}}) + \cdots$$

zählt die Primzahlpotenzen p^ν mit den (von ν unabhängigen) Gewichten $\log p$, wobei wieder für ganzzahliges x, wenn speziell $x = p^\nu$ ist, diese Primzahlpotenz nur halb, also mit dem Gewicht $\frac{1}{2}\log p$, gezählt werden soll. Sie

entspringt aus der weniger organischen Anzahlfunktion

$$\psi_0(x) = \sum_{p \leqq x} \log p$$

durch Abrundung auf Primzahlpotenzen. Kennt man eine $\psi(x)$ entsprechende Annäherungsfunktion und das dabei auftretende Restglied, so ergeben sich Annäherungsfunktion und Restglied für $\pi(x)$ durch eine elementare Umrechnung, und auch umgekehrt; kurz die Problemstellungen für $\pi(x)$ und $\psi(x)$ sind miteinander äquivalent.

4. Die Anzahlfunktionen $\pi(x), \psi(x)$ sind unstetig, nämlich sogenannte Treppenfunktionen. Aus der Theorie der Fourierschen Reihen ist bekannt, daß man auch derartige Funktionen explizit durch unendliche Reihen stetiger Funktionen darstellen kann. Es ist das Verdienst von Riemann, eine solche explizite, analytische Darstellung für die Primzahlfunktion $\pi(x)$ angegeben zu haben. Es mag hier genügen, die entsprechende explizite, analytische Darstellung für die modifizierte Primzahlfunktion $\psi(x)$ anzugeben. Sie entsteht durch Auswertung des Integrals

$$\frac{1}{2\pi i} \int_{\boxed{\dot{0}}\uparrow} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) x^s \frac{ds}{s}$$

über ein nach oben und links ins Unendliche rückendes Rechteck, ein formaler Integrationsprozeß für Dirichletsche Reihen, analog dem Cauchyschen Integrationsprozeß zur Heraushebung der Koeffizienten einer Potenzreihe. Die Auswertung nach dem Residuensatz liefert nach Ausführung des Grenzübergangs mit dem Integrationsweg die folgende explizite Formel:

$$\psi(x) = x - \log 2\pi - \frac{1}{2} \log \sqrt{1 - \frac{1}{x^2}} - \sum_{\rho} \frac{x^\rho}{\rho} \ ,$$

wo die restliche Summe über die *nicht–trivialen Nullstellen* ρ der Zetafunktion $\zeta(s)$ — oder also die nicht–trivialen Pole der logarithmischen Ableitung $-\frac{\zeta'(s)}{\zeta(s)}$ — erstreckt ist.

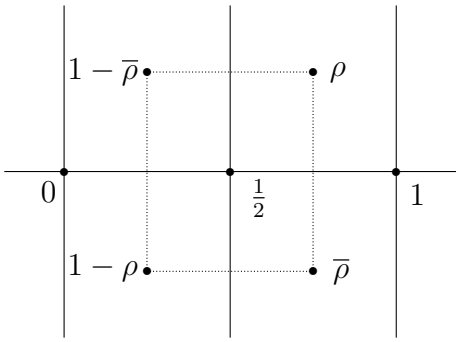
5. Über diese nicht–trivialen Nullstellen ist folgendes zu sagen. Die oben angegebene, in der ganzen s–Ebene gültige Darstellung von $\frac{1}{\Gamma(s-1)}\zeta(s)$ als

Schleifenintegral gestattet zu folgern, daß die Zetafunktion der *Funktionalgleichung* genügt:

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) \quad \text{ist bei } s \longrightarrow 1-s \text{ invariant,}$$

die eine Spiegelsymmetrie am Punkte $s = \frac{1}{2}$ der angegebenen Bildung bedeutet. Nun ist aus der Eulerschen Produktdarstellung klar, daß $\zeta(s)$ in der rechten Halbebene $\Re(s) > 1$ keine Nullstellen hat, und man kann auch noch zeigen, daß auf dem Rande $\Re(s) = 1$ keine Nullstellen liegen. Die Funktionalgleichung ergibt dann, daß $\zeta(s)$ in der linken Halbebene $\Re(s) \leqq 0$ nur die *trivialen* (durch den Γ–Zusatzfaktor bedingten) *Nullstellen* $-2m$ hat. *Nicht–triviale Nullstellen* ρ können demnach nur im *kritischen Streifen*

$$0 < \Re(s) < 1$$



liegen, und zwar gruppieren sich solche im Hinblick auf die Spiegelung an $\frac{1}{2}$ (durch die Funktionalgleichung) und die Spiegelung an der reellen Achse $\big($durch den Übergang zum konjugiert–komplexen $\overline{\zeta(s)} = \zeta(\overline{s})\big)$ in Rechtecken der angegebenen Art.

Daß es wirklich unendlich viele nicht–triviale Nullstellen ρ gibt, beweist man durch Anwendung des Hauptsatzes der Hadamardschen Theorie der ganzen Funktionen auf die ganze, bei $s \longrightarrow 1-s$ invariante Funktion

$$s(1-s)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

bei der die trivialen Nullstellen $-2m$ durch den Faktor $\Gamma\left(\frac{s}{2}\right)$ und die beiden Pole $0, 1$ durch den Faktor $s(1-s)$ eliminiert sind. Man erkennt übrigens auch noch leicht, daß diese nicht–trivialen Nullstellen nicht auf der reellen

Symmetrielinie $0 < s < 1$ des kritischen Streifens liegen, weil nämlich die Reihe

$$\left(1 - \frac{2}{2^s}\right)\zeta(s) = \frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

sogar für $\Re(s) > 0$ noch bedingt konvergiert und im Intervall $0 < s < 1$ ersichtlich positiv ist. Die nicht–trivialen Nullstellen ρ von $\zeta(s)$ sind also echt komplex.

Mittels der logarithmischen Residuenformel hat man für ihre Anzahl $\mathsf{N}(\mathsf{T})$ im Rechteck

$$0 < \Re(s) < 1\,, \qquad |\Im(s)| < 2\pi\mathsf{T}$$

die asymptotische Form

$$\mathsf{N}(\mathsf{T}) = \mathsf{T}\log\mathsf{T} - \mathsf{T} + \mathcal{O}(\log\mathsf{T})$$

bewiesen.

6. Alle diese Aussagen über $\zeta(s)$ hat *Riemann* in seiner berühmten Arbeit „Über die Anzahl der Primzahlen unter einer gegebenen Grenze“ (1859) teils bewiesen, teils vermutet und plausibel gemacht, und andere (*Hadamard*, *v. Mangoldt*) haben die exakten Beweise erbracht. Nur eine der von Riemann ausgesprochenen Vermutungen ist bis heute unbewiesen geblieben und hat allen Anstrengungen der bedeutendsten Mathematiker des inzwischen vergangenen Jahrhunderts getrotzt. Sie ist heute unter dem Namen „*die Riemannsche Vermutung*“ bekannt und berühmt. Sie lautet:

> *Die nicht–trivialen Nullstellen ρ von $\zeta(s)$ liegen sämtlich auf der imaginären Symmetrielinie $\Re(s) = \frac{1}{2}$ des kritischen Streifens.*

Wenn diese Riemannsche Vermutung zutrifft, folgt aus der vorher angegebenen expliziten Formel für die modifizierte Primzahlfunktion leicht

$$\psi(x) = x + \mathcal{O}(\sqrt{x}\log^2 x)$$

und damit für die von Riemann betrachtete Primzahlfunktion dann

$$\pi(x) = \int_0^x \frac{du}{\log u} + \mathcal{O}(\sqrt{x}\log x),$$

wobei jeweils das erste Glied rechts die Annäherungsfunktion ist das zweite die Größenordnung des Fehlergliedes angibt. Diese Formeln gelten, wie gesagt, auch für die ursprünglichen Anzahlfunktionen $\psi_0(x), \pi_0(x)$ bei denen

nur die Primzahlen p selbst (nicht auch ihre Potenzen) mit den Gewichten $\log p$ bzw. 1 gezählt werden.

Könnte man wenigstens beweisen, daß alle Realteile $\Re(\rho) < \theta$ mit einem festen $\theta < 1$ sind, so würden sich die obigen Formeln mit x^θ statt $\sqrt{x} = x^{\frac{1}{2}}$ ergeben. Bis heute hat man aber nicht einmal das beweisen können. Daher mußte man sich für das Primzahlproblem mit einer viel gröberen Abschätzung des Fehlergliedes begnügen, bei der die Größenordnung nur „unendlich wenig“ unter der Größenordnung x bzw. $\frac{x}{\log x}$ des Hauptgliedes liegt:

$$\psi(x) = x + \mathcal{O}\left(\frac{x}{e^{a\sqrt{\log x \log\log x}}}\right),$$
$$\pi(x) = \int_0^x \frac{du}{\log u} + \mathcal{O}\left(\frac{x}{e^{a\sqrt{\log x \log\log x}}}\right),$$

mit einer positiven Konstante a. Diese als *Primzahlsatz mit Restabschätzung* bekannten, bisher wirklich bewiesenen Ergebnisse haben aber im Hinblick auf die große Plausibilität der Riemannschen Vermutung nur provisorischen Charakter.

Unter Annahme der Riemannschen Vermutung hat man schließlich zeigen können, daß die Größenordnungen

$$\mathcal{O}\left(\sqrt{x}\log^2 x\right) \quad \text{bzw.} \quad \mathcal{O}\left(\sqrt{x}\log x\right)$$

ziemlich genau an den bisher unbekannten wahren Größenordnungen liegen, daß nämlich die unteren Abschätzungen bestehen:

$$\psi(x) - x = \Omega^{\pm}(\sqrt{x}\log\log\log x),$$
$$\pi(x) - \int_0^x \frac{du}{\log u} = \Omega^{\pm}\left(\frac{\sqrt{x}}{\log x}\log\log\log x\right),$$

d. h. das Restglied wird immer mal wieder größer als eine feste Konstante mal dem $\Omega^{\pm}$–Argument, und zwar sowohl positiv als auch negativ. Zwischen den oberen und unteren Abschätzungen klafft demnach „nur“ eine Lücke von der Größenordnung

$$\frac{\log^2 x}{\log\log\log x}\,.$$

§2. Verteilungsprobleme und Zetafunktionen für Kongruenzfunktionenkörper.

Wir haben gesehen, daß die endgültige Lösung des Primzahlverteilungsproblems von dem Beweis der Riemannschen Vermutung über die nicht–trivialen Nullstellen der Riemannschen Zetafunktion abhängt. Nun gibt es in der höheren Zahlentheorie einen Typus von statistischen Verteilungsproblemen, denen ebenfalls eine Art von Zetafunktionen zugeordnet sind, und wo die Lösung ebenfalls darauf hinausläuft, für diese Zetafunktionen das Analogon zur Riemannschen Vermutung zu beweisen. Dabei ist aber die Sachlage sehr viel einfacher als bei der gewöhnlichen Zetafunktion. Man hat hier den Beweis des Analogons zur Riemannschen Vermutung tatsächlich erbringen können und hat damit die genaue Größenordnung des Restgliedes für die in Rede stehenden statistischen Verteilungsprobleme bestimmt.

1. Die größere Einfachheit liegt daran, daß es sich bei den neuartigen Zetafunktionen um Dirichletsche Reihen handelt, die nicht nach *allen* natürlichen Zahlen n, sondern nur nach Potenzen p^ν einer *festen Primzahl* p fortschreiten:

$$\zeta(s) = \sum_{\nu=0}^{\infty} \frac{a_\nu}{p^{\nu s}} \qquad \big(\Re(s) > 1\big).$$

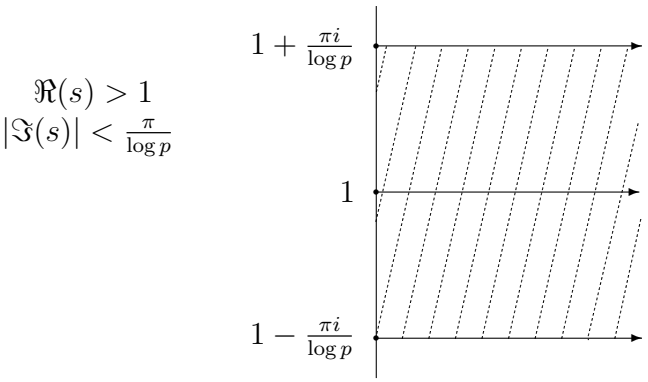
Eine solche Dirichletsche Reihe kann durch die Variablensubstitution

$$z = \frac{1}{p^s}$$

in eine Potenzreihe

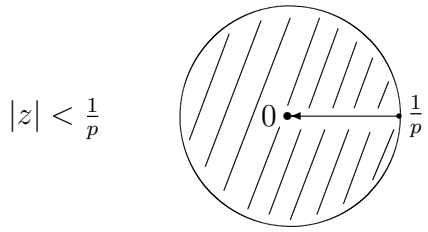
$$\mathsf{Z}(z) = \sum_{\nu=0}^{\infty} a_\nu z^\nu \qquad \big(|z| < \frac{1}{p}\big)$$

transformiert werden. Die Funktion $\zeta(s)$ ist periodisch mit der Grundperiode $\frac{2\pi i}{\log p}$, und der Übergang zu $\mathsf{Z}(z)$ bedeutet, daß man den Grundperiodenstreifen:



s–Ebene

umkehrbar eindeutig konform auf das Kreisinnere:



z–Ebene

abbildet. Dadurch werden dann ev. Nullstellen ρ von $\zeta(s)$ zu Serien homologer

$$\rho_k = \rho_0 + \frac{2\pi i k}{\log p} \quad (k \text{ bel. ganz}), \text{ kurz} \quad \rho \bmod \frac{2\pi i}{\log p}\,,$$

zusammengefaßt. Jeder solchen Serie homologer Nullstellen von $\zeta(s)$ entspricht eineindeutig eine einzige Nullstelle

$$\omega = \frac{1}{p^\rho}$$

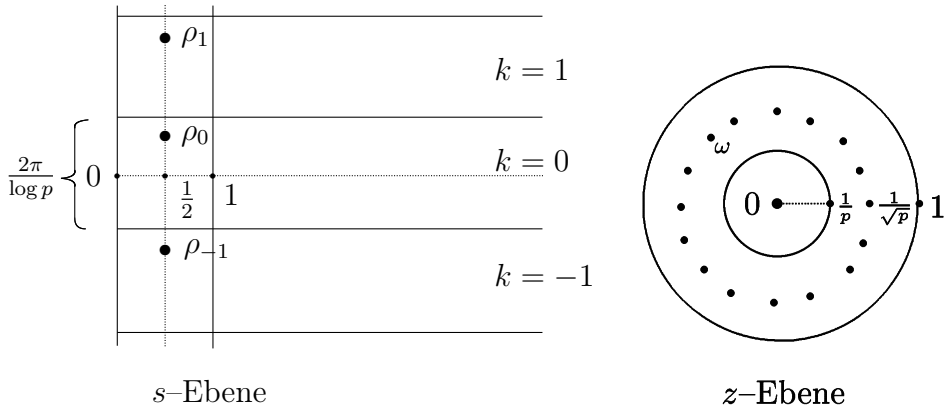
von $\mathsf{Z}(z)$. Daß bei analytischer Fortsetzung die Nullstellen $\rho \mod \frac{2\pi i}{\log p}$ von $\zeta(s)$ sämtlich auf der

> (arithm.) Mittellinie $\Re(s) = \frac{1}{2}$ des kritischen Streifens $0 < \Re(s) < 1$

liegen, übersetzt sich darin, daß bei analytischer Fortsetzung die Nullstellen ω von $\mathsf{Z}(z)$ sämtlich auf dem

(geom.) Mittelkreis $|z| = \frac{1}{\sqrt{p}}$ des kritischen Kreisrings $1 > |z| > \frac{1}{p}$

liegen:



s–Ebene z–Ebene

Bei den in Rede stehenden statistischen Verteilungsproblemen ist nun die Funktion $\zeta(s)$ so beschaffen, daß die transformierte Funktion $\mathsf{Z}(z)$ nur *endlich viele* Nullstellen ω besitzt, also $\zeta(s)$ selbst nur endlich viele Serien homologer Nullstellen $\rho \mod \frac{2\pi i}{\log p}$ hat.

Es sollen jetzt die in Rede stehenden statistischen Verteilungsprobleme und die ihnen zugeordneten Zetafunktionen genauer beschrieben werden.

2. Ausgangspunkt dafür ist der *rationale Kongruenzfunktionenkörper* R zu einer gegebenen Primzahl p, als Analogon des rationalen Zahlkörpers P.

Bekanntlich erhält man für jede Primzahl p einen endlichen Körper Ω von genau p Elementen, indem man mit den gewöhnlichen ganzen Zahlen nur mod p rechnet, d. h. beim Rechnen nicht auf die genaue Größe der Zahlen sondern nur auf ihren Divisionsrest mod p achtet.

Beispiel $p = 2$:

Rechenelemente $\left\{ \begin{array}{l} 0 \mod 2 = \text{gerade Zahlen; Symbol çift} \\ 1 \mod 2 = \text{ungerade Zahlen; Symbol tek} \end{array} \right\}$

çift + çift	=	çift	çift × çift	=	çift
çift + tek	=	tek	çift × tek	=	çift
tek + tek	=	çift	tek × tek	=	tek.

Man betrachtet nun die Gesamtheit der Polynome in einer Unbestimmten x über einem solchen endlichen Körper Ω, also

$$A = A(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \qquad (\alpha_\nu \text{ in } \Omega).$$

Sie bilden einen Integritätsbereich $\mathsf{G} = \Omega[x]$. Dieser kann mit dem Integritätsbereich Γ der gewöhnlichen ganzen Zahlen, oder vielmehr mit dem Halbintegritätsbereich Γ^+ der nicht–negativen ganzen Zahlen a folgendermaßen gegenübergestellt werden:

Elementgesamtheit (*Gleichheitsrelation*)	
$a = \alpha_0\alpha_1\alpha_2\cdots\alpha_n$ im p–adischen Ziffernsystem geschrieben	$A = \alpha_0\alpha_1\alpha_2\cdots\alpha_n$ als Koeff. System eines Polynoms σ über Ω aufgefaßt.
Rechenoperationen (*Addition, Multiplikation*)	
nach geläufigem Schema	
mit Ziffernübertragung	*ohne* Ziffernübertragung.

Von diesem Integritätsbereich $\mathfrak{I} = \Omega[x]$ bildet man weiter den Quotientenkörper $\mathsf{G} = \Omega(x)$, bestehend aus allen Polynomquotienten

$$\frac{A(x)}{B(x)} \quad \text{mit Nenner} \quad B(x) \neq 0.$$

Er ist bei dem angegebenen modifizierten Rechenschema das Analogon des rationalen Zahlkörpers P.

$$\ast \textit{ Im folgenden durchweg } \left\{ \begin{array}{ccc} \mathsf{G} & \textit{statt} & \Omega[x] \\ \mathsf{R} & = & \Omega(x) \end{array} \right\} \textit{ schreiben!}$$

Die Polynome $A \neq 0$ aus $\Omega[x]$ (und damit auch die Polynomquotienten aus $\Omega(x)$) setzen sich eindeutig aus Primpolynomen P und einer Konstanten $\alpha \neq 0$ aus Ω zusammen, analog zu der eindeutigen Zusammensetzung der Zahlen $a \neq 0$ aus Γ (und damit auch der aus P) aus Primzahlen p und einem Einheitsfaktor ± 1. Der Normierung $p > 0$ der Primzahlen entspricht hierbei die Normierung der Primpolynome P auf höchsten Koeffizienten 1; in der Tat sind die Konstanten $\alpha \neq 0$ aus Ω gerade die Einheiten in $\Omega[x]$.

Die Polynome A sind zwar keine Zahlen im gewöhnlichen Sinne, sondern nur solche in dem angegebenen modifizierten Sinne. Man kann aber dennoch ihre „Größe“ in vernünftiger Weise durch gewöhnliche Zahlen messen. Für

eine gewöhnliche positive ganze Zahl a ist ja ihre „Größe“ auch deutbar als die Anzahl der Restklassen mod a. Hat nun A als Polynom in x den genauen Grad n (oben $\alpha_n \neq 0$), so besteht das reduzierte Restsystem mod A in $\Omega[x]$ aus allen Polynomen über Ω, deren Grad $< n$ ist. Solche Polynome gibt es genau p^n. Man definiert demgemäß die Größenmaßzahl von A als

$$\mathfrak{N}(A) = p^n, \quad \text{wo} \quad n = \operatorname{Grad} A$$

und nennt diese Bildung die *Absolutnorm* von A.

3. Im rationalen Zahlkörper P war nun die Zetafunktion dadurch definiert, daß man die Bildung $\frac{1}{a^s}$ über alle *positiven ganzen* Zahlen a summiert. Im Körper $\Omega(x)$ entsprechen den *ganzen* Zahlen die Polynome A aus dem Integritätsbereich $\Omega[x]$, und der Beschränkung auf positive Zahlen entspricht die Normierung auf höchsten Koeffizienten 1. Als Analogon in $\Omega(x)$ der Zetafunktion wird man demgemäß die folgende Bildung anzusehen haben:

$$\zeta_0(s) = \sum_{\substack{A \text{ in } \Omega[x] \\ \text{höchster Koeff. } 1}} \frac{1}{\mathfrak{N}(A)^s} = \sum_{n=0}^{\infty} \sum_{\mathfrak{N}(A)=p^n} \frac{1}{p^{ns}} \qquad \big(\Re(s) > 1\big).$$

Diese Dirichletsche Reihe von dem zuvor besprochenen Typus läßt sich elementar summieren. Die Anzahl der normierten Polynome A in $\Omega[x]$ vom Grade n ist ja einfach p^n, und daher hat man

$$\zeta_0(s) = \sum_{n=0}^{\infty} \frac{p^n}{p^{ns}} = \frac{1}{1 - \frac{p}{p^s}} \quad \left[= \frac{1}{1 - pz} = \mathsf{Z}_0(z)\right]$$

Hierdurch wird $\zeta_0(s)$ über die ganze s–Ebene fortgesetzt. An *Polen* tritt lediglich *eine* Serie homologer bei $s \equiv 1 \mod \frac{2\pi i}{\log p}$ von der Ordn. 1 auf. Dagegen besitzt diese Zetafunktion *überhaupt keine Nullstellen.*

Auf Grund der eindeutigen Primpolynomzerlegung besteht auch hier das Analogon der Eulerschen Produktformel:

$$\zeta_0(s) = \prod_P \frac{1}{1 - \frac{1}{\mathfrak{N}(P)^s}} \qquad \big(\Re(s) > 1\big).$$

Man kann mit dieser Zetafunktion das Analogon der gewöhnlichen Primzahlverteilungslehre entwickeln, nämlich die Anzahlfunktion

$$\pi_0(x) = \sum_{\mathfrak{N}(P) \leqq x} 1 \quad \text{oder besser} \quad \pi(x) = \sum_{\mathfrak{N}(P^\nu) \leqq x} 1$$

(mit zweckmäßig $x = p^{\mathsf{N}}$, also: $\operatorname{Grad} P \leqq \mathsf{N}$ bzw. $\operatorname{Grad} P^{\nu} \leqq \mathsf{N}$) explizit bestimmen und für $x \longrightarrow \infty$ ($\mathsf{N} \longrightarrow \infty$) durch eine Annäherungsfunktion nebst Restglied darstellen. Es ist aber nicht dieses Verteilungsproblem, auf das wir hier abzielen. Vielmehr ist dies Verteilungsproblem ziemlich trivial. Eine explizite Formel für $\pi_0(x)$ bzw. $\pi(x)$ kann man schon auf elementar–algebraischem Wege mittels der Möbiusschen Umkehrformeln gewinnen. Es wäre nur eine ganz reizvolle Übungsaufgabe zur Algebra, den ganzen komplizierten Gedankengang der gewöhnlichen Primzahlverteilungslehre einmal für diesen viel einfacher gelagerten Fall in formal analoger Weise durchzuführen und so die gewöhnliche analytische Theorie in formaler, fast rein–algebraischer Weise zu beleuchten.

Analytisch äußert sich die Trivialität dieses Verteilungsproblems in dem schon erwähnten Umstand, daß die Zetafunktion $\zeta_0(s)$ keine Nullstellen hat. Bei den hier herauszuarbeitenden Verteilungsproblemen nicht–trivialer Art wird die Zetafunktion Nullstellen haben, die zu den nicht–trivialen Nullstellen der Riemannschen Zetafunktion analog sind — triviale Nullstellen werden hier nicht auftreten —, und die Lösung des Verteilungsproblems wird auf den Beweis des Analogons der Riemannschen Vermutung für diese Nullstellen hinauslaufen.

4. Ehe wir an die Formulierung dieses Typus von Verteilungsproblemen gehen können, müssen wir noch die zuvor definierte Zetafunktion $\zeta_0(s)$ zu einer mehr organischen Zetafunktion $\zeta(s)$ abrunden, nämlich zu einer solchen die bei den Automorphismen $x \longrightarrow \frac{\alpha x+\beta}{\gamma x+\delta}$ ($\alpha, \beta, \gamma, \delta$ aus Ω, $\alpha\delta - \beta\gamma \neq 0$) invariant ist. Es geschieht das durch eine Umdeutung der Primpolynome P zu *Primdivisoren* $\mathfrak{P}$ oder *Punkten* im Sinne der projektiven algebraischen Geometrie. Wie wir schon zur Definition des Größenmaßes $\mathfrak{N}(P)$ die Restklassenbildung mod P in $\Omega[x]$ herangezogen haben, so soll das jetzt auch für die zu gebende Umdeutung der P geschehen.

Wir betrachten zunächst die einfachsten Primpolynome P, nämlich die vom *ersten Grade*:

$$P(x) = x - \alpha \qquad (\alpha \text{ in } \Omega).$$

Sie entsprechen eineindeutig den p Elementen α aus dem Konstantenkörper Ω. Das volle Restsystem mod P besteht nur aus den $\mathfrak{N}(P) = p$ Konstanten aus Ω, und zwar erhält man den konstanten Rest mod P eines A aus $\Omega[x]$ einfach nach dem Schema

$$A(x) \equiv A(\alpha) \mod P,$$

also durch Bildung des Funktionswertes $A(\alpha)$. Die Restklassenabbildung mod P ist ein Homomorphismus des Integritätsbereichs $\Omega[x]$ auf den Konstantenkörper Ω, der durch die Zuordnung (Einsetzung) $x \longrightarrow \alpha$ völlig beschrieben wird. Sie setzt sich nach dem Schema

$$\frac{A(x)}{B(x)} \longrightarrow \frac{A(\alpha)}{B(\alpha)}$$

eindeutig auf den vollen Körper $\Omega(x)$ fort, wenn man nur noch formal festsetzt, daß im Falle $B(\alpha) = 0$ (bei reduzierter Bruchdarstellung $\frac{A}{B}$) der Rest ∞ sein soll, analog zur Einbeziehung des *Funktionswerts* ∞ in der komplexen Funktionentheorie. Und analog zur Einbeziehung des Arguments ∞ in der komplexen Funktionentheorie wollen wir auch hier noch ∞ zum Konstantenkörper Ω hinzugefügt denken und dementsprechend auch noch den Restklassenhomomorphismus $x \longrightarrow \infty$ von $\Omega(x)$ auf Ω mit in Betracht ziehen; er liefert in der geläufigen Weise $\left(\frac{1}{x} \longrightarrow 0\right)$ für alle diejenigen $\frac{A}{B}$ endliche Werte, für welche Grad $A \leqq$ Grad B ist, speziell den Wert 0, wenn Grad $A <$ Grad B ist.

Es zeigt sich nun, daß die vorstehend aufgeführten $p + 1$ Restklassenhomomorphismen von $\Omega(x)$ auf Ω überhaupt *alle möglichen Homomorphismen von* $\Omega(x)$ *auf* Ω sind, wobei „Homomorphismus“ in der angegebenen Weise unter Einbeziehung von ∞ zu verstehen ist. Diesen $p + 1$ Homomorphismen denken wir Symbole $\mathfrak{P}$ zugeordnet, die wir *Primdivisoren ersten Grades* oder *rationale Punkte* von $\Omega(x)$ nennen. Man beachte, daß diese Definition nur vom Körper $\Omega(x)$, nicht von der Erzeugenden x abhängt, also bei den Automorphismen $x \longrightarrow \frac{\alpha x+\beta}{\gamma x+\delta}$ von $\Omega(x)$ invariant ist.

Für ein Primpolynom P *höheren Grades* n liefert die Restabbildung mod P von $\Omega(x)$, wie aus den Grundlagen der höheren Algebra bekannt, gerade den algebraischen Erweiterungskörper

$$\Omega^{(n)} = \Omega(\xi) \quad \text{mit} \quad P(\xi) = 0$$

vom Grade n des Konstantenkörpers. Es ist das ein endlicher Körper von p^n Elementen — in amerikanischer Bezeichnung $\mathrm{GF}(p^n)$ —, der nur von dem Grade n von P (nicht von den Koeffizienten von P) abhängt. Diesen Primpolynomen P ordnen wir demgemäß Symbole $\mathfrak{P}$ zu, die *Homomorphismen von* $\Omega(x)$ *auf endliche Erweiterungen von* Ω bedeuten und *Primdivisoren höheren Grades* genannt werden.

Wir setzen allgemein die Absolutnorm

$$\mathfrak{N}(\mathfrak{P}) = p^n,$$

wo n der Grad des Restklassenkörpers $\Omega^{(n)}$ bei $\mathfrak{P}$ ist.

Denkt man den Konstantenkörper Ω algebraisch–abgeschlossen, also alle $\Omega^{(n)}$ in ihn einbezogen, so lösen sich die Primdivisoren n–ten Grades in n Primdivisoren ersten Grades auf, entsprechend der jetzt notwendig werdenden Unterscheidung der n konjugierten $\xi^{(\nu)}$ zu dem obigen abstrakt–algebraischen $\xi = (x \bmod P)$. Die Gesamtheit dieser bei algebraischem Abschluß von Ω entstehenden Primdivisoren — sämtlich ersten Grades — nennt man auch die *algebraischen Punkte* von $\Omega(x)$, weil sie den sämtlichen über Ω algebraischen Einsetzungen $x \longrightarrow \xi$, unter Unterscheidung konjugierter, eineindeutig entsprechen, während bei den Primdivisoren über Ω selbst die konjugierten Einsetzungen nicht unterschieden werden.

Für die Zetafunktion von $\Omega(x)$ ergibt diese Tieferlegung des Fundaments zunächst eine Auffüllung des Eulerschen Produkts um einen Faktor $\frac{1}{1-\frac{1}{p^s}}$, entsprechend dem hinzugekommenen Homomorphismus $x \longrightarrow \infty$, und dann eine veränderte, nämlich invariante Schreibweise. Die endgültige Zetafunktion ist in der Eulerschen Produktdarstellung gegeben durch:

$$\zeta(s) = \prod_{\mathfrak{P}} \frac{1}{1-\frac{1}{\mathfrak{N}(\mathfrak{P})^s}} = \frac{1}{1-\frac{p}{p^s}}\,\frac{1}{1-\frac{1}{p^s}} = \frac{1}{1-pz}\,\frac{1}{1-z} = \mathsf{Z}(z).$$

Um auch die ursprüngliche Definition als Dirichletsche Reihe in dieser neuen, invarianten Weise schreiben zu können, bildet man die aus den Primdivisoren $\mathfrak{P}$ erzeugte freie abelsche Gruppe:

$$\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{\nu_{\mathfrak{P}}} \qquad \text{(nur endlich viele } \nu_{\mathfrak{P}} \neq 0\text{)}.$$

Ihre Elemente nennt man die *Divisoren* von $\Omega(x)$, speziell die mit durchweg $\nu_{\mathfrak{P}} \geqq 0$ die *ganzen* Divisoren. Man hat dann, jedenfalls formal:

$$\zeta(s) = \sum_{\mathfrak{A}\text{ ganz}} \frac{1}{\mathfrak{N}(\mathfrak{A})^s},$$

wo $\mathfrak{N}(\mathfrak{A}) = \prod_{\mathfrak{P}} \mathfrak{N}(\mathfrak{P})^{\nu_{\mathfrak{P}}}$ gesetzt ist. Auf die inhaltliche Bedeutung dieser Divisoren $\mathfrak{A}$, nämlich ihre Beziehung zu den Elementen A aus $\Omega(x)$ soll hier nicht weiter eingegangen werden.

5. Der herauszuarbeitende Typus von Verteilungsproblemen hängt mit den *endlich–algebraischen Erweiterungen* K des rationalen Funktionenkörpers $\mathsf{R} = \Omega(x)$ über einem endlichen Körper Ω zusammen.

Wir haben bisher Ω immer als endlichen Körper mit einer *Primzahl* p als Elementanzahl, kurz als den *Primkörper* zu einer Primzahl p vorausgesetzt. Jetzt, wo wir endlich–algebraische Erweiterungen betrachten, ist es vernünftig, von vornherein für Ω auch endlich–algebraische Erweiterungen des Primkörpers zuzulassen. Das sind endliche Körper mit einer Potenz $q = p^r$ als Elementanzahl, und man lehrt in der Algebra, daß es für jede Primzahlpotenz $q = p^r$ genau einen solchen Körpertypus gibt; er ist algebraisch vom Grade r über dem Primkörper zu p. Alles Vorhergehende gilt auch für solche allgemeineren endlichen Körper $\big($in amerikanischer Terminologie $\mathrm{GF}(p^r)\big)$; denn davon, daß p Primzahl ist, wurde nur insoweit Gebrauch gemacht, daß eben die Restklassen mod p einen (endlichen) Körper bilden.

Eine endlich–algebraische Erweiterung K von $\mathsf{R} = \Omega(x)$ ist gegeben durch eine Erzeugung

$$\mathsf{K} = \mathsf{R}(y) = \Omega(x, y) \quad \text{mit} \quad F(y) = f(x, y) = 0$$

wo F ein irreduzibles Polynom in y mit Koeffizienten aus R ist. Man kann diese Koeffizienten durch einen Faktor $\neq 0$ aus R — eindeutig bis auf eine Konstante $\neq 0$ aus Ω — so normieren, daß sie ganz, d. h. Polynome in x, und ohne gemeinsamen Teiler sind. Dadurch wird F zu einem irreduziblen Polynom f in x, y über Ω.

Man kann ferner ohne Einschränkung voraussetzen, daß dies Polynom f sogar *absolut–irreduzibel* in x, y ist, d. h. auch bei beliebiger algebraischer Erweiterung von Ω irreduzibel bleibt. Man erreicht das nämlich, indem man bei Vorhandensein einer Zerlegung von f über einer algebraischen Erweiterung von Ω, die notwendig in algebraisch–konjugierte Faktoren erfolgt, die Koeffizienten dieser Faktoren zu Ω adjungiert, so daß sich dann f auf einen (beliebig wählbaren) dieser konjugierten Faktoren reduziert.

Wird diese Erweiterung von Ω als bereits vollzogen, also f als absolut–irreduzibel vorausgesetzt, so heißt Ω der *genaue Konstantenkörper* von K, weil sich zeigt, daß dann Ω schon mit der Gesamtheit aller *Konstanten*, d. h. über Ω algebraischen Elemente aus K zusammenfällt.

Sei jetzt K ein solcher algebraischer Funktionenkörper mit dem Konstantenkörper Ω von q $(= p^r)$ Elementen. Dann läßt sich eine Theorie der *Primdivisoren* $\mathfrak{P}$ von K/Ω analog zu der in R entwickeln.

Die *Primdivisoren* $\mathfrak{P}$ *vom ersten Grade* oder *rationalen Punkte* von K/Ω sind gekennzeichnet durch die *Homomorphismen von* K/Ω *auf den Konstantenkörper* Ω *einschl.* ∞. Sie werden explizit beschrieben durch die Ersetzungen

$$(x, y) \longrightarrow (\alpha, \beta) \quad \text{mit} \quad \alpha, \beta \quad \text{in} \quad \Omega, \quad f(\alpha, \beta) = 0,$$

kurz durch die *Lösungen* α, β *in* Ω *der Grundgleichung* $f(x, y) = 0$. Dabei muß man allerdings diese Lösungen mit Vielfachheiten im Sinne der algebraischen Geometrie zählen, und projektiv, d. h. unter Einbeziehung von ∞. Eine algebraische Präzisierung dieser Zählung ergibt sich, indem man x so wählt, daß im Unendlichen nur ein einziger Punkt liegt und dann anstelle der einen weiteren Erzeugenden y eine *Ganzheitsbasis* $y_1, \ldots, y_n$ des Integritätsbereichs $\mathfrak{I}$ der in x ganzen Elemente aus K über dem Integritätsbereich $\mathsf{G} = \Omega[x]$ der in x ganzen Elemente aus $\mathsf{R} = \Omega(x)$ setzt; anstelle der einen Grundgleichung $f(x, y) = 0$ tritt dabei das Multiplikationsschema der Basis $y_1, \ldots, y_n$. Algebraisch–geometrisch bedeutet das: Ersetzung der „Kurve“ $f(x, y) = 0$ im zweidimensionalen Raum durch ein *singularitätenfreies Modell* im $(n + 1)$–dimensionalen Raum.

Allgemein sind die *Primdivisoren* $\mathfrak{P}$ *höheren Grades* m gekennzeichnet durch die *Homomorphismen von* K/Ω *auf die algebraische Erweiterung* m*–ten Grades* $\Omega^{(m)}/\Omega$ *einschl.* ∞ ohne Unterscheidung konjugierter. Sie werden explizit beschrieben durch die Ersetzungen

$$(x, y) \longrightarrow (\alpha, \beta) \quad \text{mit} \quad \alpha, \beta \quad \text{in} \quad \Omega^{(m)}, \quad f(\alpha, \beta) = 0,$$

kurz durch die *vom Grade* m *über* Ω *algebraischen Lösungen der Grundgleichung* $f(x, y) = 0$, wobei jedem System konjugierter Lösungen ein einziger Primdivisor $\mathfrak{P}$ entspricht. Man setzt dann wieder die *Absolutnorm*

$$\mathfrak{N}(\mathfrak{P}) = q^m,$$

weil dies als Elementanzahl von $\Omega^{(m)}$ gerade die Restklassenanzahl mod $\mathfrak{P}$ in K ist.

Wie vorher sind hierbei die Lösungen wieder mit Vielfachheiten im Sinne der algebraischen Geometrie zu zählen. Unterscheidet man die über Ω konjugierten Lösungen, so zerfällt jeder Primdivisor m–ten Grades in m konj. *algebraische Punkte* m*–ten Grades*; diese können auch als Primdivisoren ersten Grades der *Konstantenerweiterung* $\mathsf{K}^{(m)}/\Omega^{(m)}$ von K/Ω gedeutet werden.

In der komplexen Funktionentheorie treten bei den Riemannschen Flächen solche Punkte höheren Grades nicht auf, weil dort der Konstantenkörper Ω algebraisch–abgeschlossen, nämlich der komplexe Zahlkörper ist. Ihr Auftreten hier ist einer der wesentlich neuen Züge der arithmetischen Theorie der algebraischen Funktionenkörper mit endlichem Konstantenkörper.

6. Wir definieren nun die *Zetafunktion von* K *als das Eulersche Produkt*:

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P})^s}} \qquad \big(\Re(s) > 1\big),$$

erstreckt über alle Primdivisoren $\mathfrak{P}$ von K. Führt man wieder formal die zusammengesetzten Divisoren

$$\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{\nu_{\mathfrak{P}}} \qquad \text{(nur endlich viele } \nu_{\mathfrak{P}} \neq 0)$$

und ihre Absolutnormen

$$\mathfrak{N}(\mathfrak{A}) = \prod_{\mathfrak{P}} \mathfrak{N}(\mathfrak{P})^{\nu_{\mathfrak{P}}}$$

ein, so stellt sich die Zetafunktion von K formal auch dar als die Dirichletsche Reihe:

$$\zeta_{\mathsf{K}}(s) = \sum_{\mathfrak{A}\text{ ganz}} \frac{1}{\mathfrak{N}(\mathfrak{A})^s} \qquad \big(\Re(s) > 1\big)$$

erstreckt über alle ganzen Divisoren $\mathfrak{A}$ von K (alle $\nu_{\mathfrak{P}} \geqq 0$).

Für die Herleitung der wesentlichen Eigenschaften dieser Zetafunktion von K hat man näher auf die inhaltliche Bedeutung der zusammengesetzten Divisoren $\mathfrak{A}$ von K, nämlich ihre Beziehungen zu den Elementen a von K einzugehen. Wegen der Knappheit der zur Verfügung stehenden Zeit kann das hier nicht geschehen. Es sei hier lediglich bemerkt, daß diese Beziehungen dazu führen, neben der aus der Absolutnorm entspringenden additiven Bildung

$$\operatorname{Grad} \mathfrak{A} = m, \quad \text{wenn} \quad \mathfrak{N}(\mathfrak{A}) = q^m$$

1.25 Hamburg 1963

Die algebraischen und zahlentheoretischen Arbeiten von Emil Artin (1898-1962)

Vortrag in der Mathematischen Gesellschaft

Hamburg, 13. Juni 1963

I. Funktionenkörper

II. Zetafunktionen, L-Reihen, Frobenius-Struktur

III. Allgemeines Reziprozitätsgesetz

IV. Explizite Reziprozitätsformeln

V. Ringe und hyperkomplexe Zahlsysteme

VI. Allgemeines zur algebraischen Zahlentheorie

VII. Klassenzahl

VIII. Bücher

IX. Dissertationen

I. Funktionenkörper

2. Quadratische Körper im Gebiete der höheren Kongruenzen I, II. Math. Zeitschr. **19** (1924), 153-246 (*Dissertation*)

Aufbau eines Analogons zur arithmetischen Theorie der quadratischen Zahlkörper in der arithmetischen Theorie der hyperelliptischen Funktionenkörper mit dem Primkörper der Charakteristik p als Konstantenkörper:

K Körper der rationalen Funktionen von t mit Koeffizienten mod. p,
Ω $= \mathsf{K}(\sqrt{\mathsf{D}})$, wo D eine oBdA quadratfreie solche ganze rationale Funktion.

Man kann K auch als Rechnen im p-adischen Ziffernsystem ohne jede Ziffernübertragung beschreiben. Dadurch entstehen einfachere Verhältnisse. Das Analogon wirft so auf im Zahlenkörperfall schwierige Verhältnisse neues Licht.

Artin muß, da nichts vorlag, zunächst die gesamte elementare Algebra und Arithmetik der quadratischen Zahlkörper auf diesen Fall übertragen. Es gelingt ihm bis zum Beweis des quadratischen Reziprozitätsgesetzes aus der Theorie der Idealklassen quadratischer Körper vorzustoßen.

Diese arithmetische Theorie wurde kurz darauf 1925 von *F.K. Schmidt* auf beliebige algebraische Funktionenkörper mit endlichem Konstantenkörper verallgemeinert, angeregt durch die Artinschen Untersuchungen.

I. Funktionenkörper

Das Hauptgewicht der Artinschen Arbeit liegt aber zweifellos in ihrem analytischen Teil. Dort wird die Theorie der Zetafunktion auf die betrachteten Körper Ω übertragen, und es werden die Probleme der analytischen Zahlentheorie damit angepackt. Bei Artin erscheinen die Formeln dadurch noch nicht in der heute geläufigen Gestalt, daß er nicht birational-invariant arbeitet, nämlich die unendliche Primstelle des rationalen Funktionenkörpers K nicht mit in die arithmetischen Bildungen einbezieht. In heutiger birational-invarianter Gestalt hat man

$$\frac{\mathsf{Z}_\Omega(s)}{\mathsf{Z}_\mathsf{K}(s)} = \mathsf{L}_\Omega(s) = 1 + \frac{\mathsf{N}_1 - (p+1)}{p^s} + \cdots + \frac{p^g}{p^{2gs}}.$$

Das Polynom $\mathsf{L}_\Omega(s)$ hat $2g$ Nullstellen ω_ν in $z = p^s$ und es ist

$$h = \prod_{\nu=1}^{2g}(1-\omega_\nu), \qquad \mathsf{N}_1 - (p+1) = -\sum_{\nu=1}^{2g}\omega_\nu.$$

Die Riemannsche Vermutung besagt, daß alle $|\omega_\nu| = \sqrt{p}$ sind. Artins Arbeit enthält Tafeln, in denen er diese Vermutung für etwa vierzig hyperelliptische Körper bestätigt.

Allgemein wurde sie für den elliptischen Spezialfall durch mich 1933 und dann allgemein durch *A. Weil* 1948 bewiesen. *Roquette* gab 1953 einen rein arithmetischen Beweis.

II. Zetafunktionen, *L*-Reihen, Frobenius-Struktur

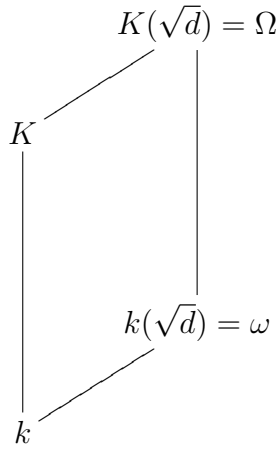
1. Über die Zetafunktion gewisser algebraischer Zahlkörper.
Math. Ann. **89** (1923), 147-156.

Erstes Eindringen in eigenartige Relationen zwischen den Zetafunktionen der Teilkörper eines relativ-galoisschen Zahlkörpers für gewisse Spezialfälle (metazyklische Körper von Primzahlpotenzgrad, Ikosaederkörper).

In seiner späteren Arbeit 3 wird er diesen Relationen auf den Grund gehen und die Sachlage völlig aufhellen.

Beispiel einer solchen Relation:

K/k kubisch, nicht-zyklisch, Diskriminante d



$$\begin{aligned} \zeta_K^2 \zeta_\omega &= \zeta_\Omega \zeta_k^2 \\ \left(\frac{\zeta_K}{\zeta_k}\right)^2 &= \frac{\zeta_\Omega}{\zeta_\omega} = \prod_{\chi \neq 1} \mathsf{L}_\chi = \mathsf{L}_\chi \mathsf{L}_{\overline{\chi}} \end{aligned}$$

II. Zetafunktionen, *L*-Reihen, Frobenius-Stuktur

3. Über eine neue Art von L-Reihen – Hmb. Abh. **3** (1924), 89-109 (*Habilitationsschrift*)

Sei K/k ein relativ-galoisscher Zahlkörper mit der Gruppe $\mathfrak{G}$. Den Frobeniussschen Charakteren χ von $\mathfrak{G}$ werden L-Reihen über k zugeordnet, die folgendermaßen erklärt sind:

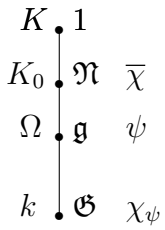
$$\mathsf{L}_k(s, \chi) = \prod_{\mathfrak{p}} \frac{1}{|I - N(\mathfrak{p})^{-s} \mathsf{A}_\chi(\sigma_\mathfrak{P})|},$$

wo $\mathfrak{p}$ alle Primdivisoren von k durchläuft, die nicht in der Relativdiskriminante von K aufgehen, und jeweils

$\mathfrak{P}$	einen Primdivisor von $\mathfrak{p}$ in K,
$\sigma_{\mathfrak{P}}$	seinen Frobenius-Automorphismus: $\mathsf{A}^{\sigma_{\mathfrak{P}}} \equiv \mathsf{A}^{N(\mathfrak{p})} \bmod \mathfrak{P}$,
$\mathsf{A}_\chi(\sigma_{\mathfrak{P}})$	die ihm entsprechende Matrix aus einer Darstellung der durch χ charakterisierten Klasse.
	$L_k(s, \chi_1 + \chi_2) = L_k(s, \chi_1) L_k(s, \chi_2)$, $L_k(s, \overline{\chi}) = L_k(s, \chi)$
	($\overline{\chi}$ Char. von gal. Teilkp. K_0/k,
	χ seine Aufblähung auf K/k)

Für einen Teilkörper Ω von K/k gilt die wichtige *Induktionsregel*:

$$\mathsf{L}_\Omega(s, \psi) = \mathsf{L}_k(s, \chi_\psi).$$



Hiernach hat die Zetafunktion von Ω die Aufspaltung

$$\zeta_\Omega(s) = \prod_{i=1}^{r} \mathsf{L}_k(s, \chi_i)^{g_i},$$

wenn der durch den Hauptcharakter von $\mathfrak{g}$ induzierte Charakter von $\mathfrak{G}$ die Zerlegung

$$\chi_\Omega = \sum_{i=1}^{r} g_i \chi_i$$

in irreduzible Charaktere χ_i von $\mathfrak{G}$ hat.

II. Zetafunktionen, *L*-Reihen, Frobenius-Struktur

Diese Parameterdarstellung der Zetafunktionen durch Artinsche L-Reihen setzt, wenn man die Aufspaltung bis auf den rationalen Zahlkörper zurückführt, sämtliche Relationen zwischen den Zetafunktionen in Evidenz.

Die Frage, ob die Artinschen L-Reihen im Spezialfall abelscher Charaktere χ mit den aus der Klassenkörpertheorie geläufigen L-Reihen zu Kongruenzcharakteren übereinstimmen, läuft auf das Artinsche Reziprozitätsgesetz zurück, das Artin in *diesem* Zusammenhang erschau`[...]` und dann in seiner späteren Arbeit 16 allgemein bewiesen hat.

Aus dieser Übereinstimmung ergibt sich der funktionentheoretische Charakter der Artinschen L-Reihen. Unter Vorwegnahme eines wichtigen Satzes von *R. Brauer* über die Frobeniusschen Charaktere handelt es sich um *meromorphe* Funktionen mit einer *Funktionalgleichung* vom geläufigen Typus.

Die von Artin aufgeworfene Frage, ob diese Funktionen sogar *ganz* sind, ist jedoch bisher nur im Analogiefalle der Funktionenkörper bejahend entschieden (*A. Weil* 1948).

II. Zetafunktionen, *L*-Reihen, Frobenius-Struktur

19. Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren. Hamb. Abh. **8** (1931), 292-306.

Die frühere L-Reihen-Arbeit wird in dreierlei Hinsicht abgerundet:

1.) *Einbeziehung der Beiträge der Diskriminantenprimteiler.* Das kann ohne Schwierigkeit durch Einbeziehung der höheren Verzweigungsgruppen in den gruppentheoretischen Ansatz geschehen.

2.) *Explizite Angabe der Funktionalgleichung* bis auf einen konstanten Faktor vom Betrage 1, der dann später *R. Brauer* 1947, *Hasse* 1954 und *Dwork* 1955 genau bestimmt und auf seine gruppentheoretische und arithmetische Struktur untersucht wurde.

3.) *Deutung der Gammafaktoren als Beiträge der unendlichen Primstellen.* – Dadurch wird die gruppentheoretische Struktur der Funktionalgleichung erst wirklich organisch.

In der Funktionalgleichung treten die gruppentheoretisch definierten *Artinschen Führer* $f_k(\chi)$ zum betrachteten relativ-galoisschen Zahlkörper K/k auf, die in der nachfolgenden Arbeit 20 eingeführt werden und dort den Schlüssel zur Beherrschung der Diskriminantenstruktur liefern.

II. Zetafunktionen, *L*-Reihen, Frobenius-Struktur

20. Gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper. – Crelle **164** (1931), 1-11.

K/k relativ-galoisscher Zahlkörper, Ω Zwischenkörper.

χ durchläuft die Charaktere der Galoisgruppe $\mathfrak{G}$.

Analogie:

$$\begin{array}{rcl} L_k(s,\chi) & \longleftrightarrow & f_k(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{\frac{1}{v_0}\sum\limits_{\nu\geqq 0}\left(v_\nu \chi(1)-\chi(\mathfrak{V}_\nu)\right)} \\ & & \mathfrak{V}_\nu \quad \text{die Verzweigungsgruppen} \\ & & v_\nu \quad \text{ihre Ordnungen} \\ & & f_k(\chi) \quad \text{ist ganzer Divisor von } k. \\ \zeta_\Omega(s) & \longleftrightarrow & \mathfrak{D}_\Omega \quad \text{Diskriminante von } \Omega/k \end{array}$$

Parameterdarstellung:

$$\zeta_\Omega(s) = \prod_{i=1}^{r} \mathsf{L}_k(s,\chi_i)^{g_i} \longleftrightarrow \mathfrak{D}_\Omega = \prod_{i=1}^{r} f_k(\chi_i)^{g_i},$$

wenn

$$\chi_\Omega = \sum_{i=1}^{r} g_i \chi_i$$

(Durch den Hauptcharakter der Invariantengruppe von Ω induzierter Charakter von $\mathfrak{G}$).

$f_k(\chi)$ stimmt für abelsche Charaktere χ mit dem Führer der durch χ gekennzeichneten Kongruenzklasseneinteilung überein. Begriffliche Bedeutung im allgemein-galoisschen Fall noch unbekannt. Eine algebrentheoretische Deutung gab *Cahit Arf* 1940.

III. Allgemeines Reziprozitätsgesetz

16. Beweis des allgemeinen Reziprozitätsgesetzes.
Hmb. Abh. **5** (1927), 353-363.

Angeregt durch ein Überschneidungsverfahren von *Tschebotareff*, durch das dieser den Frobeniusschen Dichtigkeitssatz von den Abteilungen auf die Klassen konjugierter Elemente verallgemeinern konnte, gelingt Artin hier der Beweis des allgemeinen Reziprozitätsgesetzes in der ihm durch seine L-Reihen-Arbeit suggerierten eigenartigen Gestalt:

Sei K/k ein relativ-abelscher Zahlkörper, Klassenkörper zur Kongruenzklassengruppe D/H. Die nach der Takagischen Klassenkörpertheorie bestehende Isomorphie zwischen D/H und der Galoisgruppe $\mathfrak{G}$ von K/k wird in kanonischer Weise realisiert durch die Zuordnung:

$$\text{Klasse von } \mathfrak{p} \text{ nach } \mathsf{H} \quad \longrightarrow \quad \begin{array}{l}\text{Frobenius-Automorphismus } \sigma_{\mathfrak{p}} \\ \text{(für alle } \mathfrak{P}/\mathfrak{p} \text{ gleichzeitig)}\end{array}$$

Man schreibt heute für diesen Frobenius-Automorphismus (im abelschen Falle) einfach $\left(\frac{K/k}{\mathfrak{p}}\right)$ und nennt das das *Artin-Symbol*.

Übergang zur klassischen Form des Reziprozitätsgesetzes durch Betrachtung von $K = k(\sqrt[n]{\alpha})$ und Anwendung (wo k die n-ten Einheitswurzeln enthält)

III. Allgemeines Reziprozitätsgesetz

Des Artin-Symbols auf $\sqrt[n]{\alpha}$:

$$\sqrt[n]{\alpha}^{\left(\frac{k(\sqrt[n]{\alpha})}{\mathfrak{p}}\right)} = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha},$$

woe die n-te Einheitswurzel $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ durch das Eulersche Kriterium

$$\alpha^{\frac{\mathfrak{N}(\mathfrak{p})-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{p}$$

als das n-te Potenzrestsymbol gekennzeichnet ist. Dieses hängt hiernach nur von der Kongruenzklasse ab, in der $\mathfrak{p}$ bei der $k(\sqrt[n]{\alpha})$ zugeordneten Klasseneinteilung in k liegt.

Von dieser Formulierung kommt man unter Anwendung von Sätzen der Klassenkörpertheorie leicht zu der eigentlichen Reziprozitätsformel:

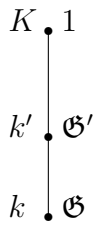
$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\beta}{\alpha}\right)_n,$$

wenn α, β zueinander und zu n prim und eines von ihnen n-primär.

III. Allgemeines Reziprozitätsgesetz

18. Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz. – Hmb. Abh. **7** (1930), 46-51.

Artin zeigt, wie man mittels seines Reziprozitätsgesetzes Aussagen darüber machen kann, in welche Kongruenzklassen eines Erweiterungskörpers die Divisoren des Grundkörpers fallen. Es geschieht das, indem man diese Klassenfrage vermöge des Artinsymbols in die Galoisgruppe verlagert. Diese Fragestellung überschreitet aber wesentlich den Bereich der abelschen Zahlkörper, weil man dazu die Galoisgruppe eines metabelschen Zahlkörpers braucht:



Die Divisoren von k werden hinsichtlich ihres Klassenverhaltens bei der K/k' entsprechenden Einteilung in k' durch Elemente der Galoisgruppe $\mathfrak{G}'$ von K/k' dargestellt, die sich durch *gruppentheoretische Verlagerung* von $\mathfrak{G}$ nach $\mathfrak{G}'$ ergeben.

Ist k'/k der maximale abelsche Teilkörper von K, der Kommutatorgruppe $\mathfrak{G}'$ von $\mathfrak{G}$ zugeordnet, so ergibt diese Verlagerung nach einer Arbeit von *Furtwängler* durchweg 1. Dadurch wird dann insbesondere (gewöhnliche Klasseneinteilung) der Hilbertsche *Hauptidealsatz* bewiesen. Eine wesentliche Vereinfachung des Furtwänglerschen Beweises gab neuerdings *E. Witt* 1954.

IV. Explizite Reziprozitätsformeln

6. Über den zweiten Ergänzungssatz zum Reziprozitätsgesetz der ℓ-ten Potenzreste im Körper k_ζ der ℓ-ten Einheitswurzeln und in Oberkörpern von k_ζ. – Crelle **154** (1925), 143-148, gemeinsam mit *H. Hasse.*

Beweis der Reziprozitätsformeln:

$$\left(\frac{\lambda}{\alpha}\right)_\ell = \zeta^{\mathrm{S}\left(\frac{\zeta \log \alpha}{\ell\lambda}\right)}, \qquad \left(\frac{\ell}{\alpha}\right)_\ell = \zeta^{-\mathrm{S}\left(\frac{\log \alpha}{\lambda^\ell}\right)}$$

für $\alpha \equiv 1 \bmod \lambda$.

IV. Explizite Reziprozitätsformeln

17. Die beiden Ergänzungssätze zum Reziprozitätsgesetz der ℓ^n-ten Potenzreste im Körper der ℓ^n-ten Einheitswurzeln. – Hmb. Abh. **6** (1928), 146-162, gemeinsam mit *H. Hasse.*

Beweis der expliziten Reziprozitätsformeln:

$$\left(\frac{\zeta_n}{\alpha}\right)_{\ell^n} = \left((-1)^{\ell-1}\zeta_n\right)^{\frac{1}{\ell^n}\mathfrak{S}_n(\log\alpha)} \qquad (n \geqq 2 \text{ für } \ell = 2)$$

$$\left(\frac{\lambda_n}{\alpha}\right)_{\ell^n} = \zeta_n^{\frac{1}{\ell^n}\mathfrak{S}_n\left(-\frac{\zeta_n}{\lambda_n}\log\alpha\right)}$$

für $\alpha \equiv 1 \bmod \lambda_n$.

Während die erste Formel eine einfache Umgestaltung des definitionsgemäßen Exponenten $\dfrac{\mathfrak{N}_n(\alpha)-1}{\ell^n}$ in Spurform ist, liegt dem Beweis der zweiten Formel eine einigermaßen komplizierte Rechnung zugrunde, die durch Einführung eines neuen quasilogarithmischen Kalküls gebändigt wird.

V. Ringe und hyperkomplexe Zahlsysteme

9. Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Körpererweiterungen. – Gött. Nachr. 1926, 23-27, gemeinsam mit *B.L. v.d. Waerden*.

Den bekannten fünf Axiomen von *E. Noether* für eindeutige Primidealzerlegung wird zur Erfassung inseparabler Erweiterungen ein sechstes hinzugefügt:

Endlichkeit des Wurzelrings $R^{\frac{1}{p}}$ bezüglich R bei Charakteristik p.

Dann wird das Erhaltenbleiben des Axiomensystems bei beliebigen (auch inseparabler) algebraischer Erweiterung gezeigt.

V. Ringe und hyperkomplexe Zahlsysteme

13. Über einen Satz von Herrn J.H. Maclagan Wedderburn. – Hmb. Abh. **5** (1927), 245-250.

Gedanklich sehr einfacher, eleganter Beweis des Satzes, daß ein endlicher Schiefkörper notwendig kommutativ ist. Der Satz wird in der Form bewiesen, daß ein endlicher Schiefkörper notwendig mit seinem Zentrum zusammenfällt.

Einen noch einfacheren, wesentlich gruppentheoretischen Beweis gab *E. Witt* 1931.

V. Ringe und hyperkomplexe Zahlsysteme

14. Zur Theorie der hyperkomplexen Zahlen. – Hmb. Abh. **5** (1927), 251-260

Neue, vereinfachte Begründung der Wedderburnschen Strukturtheorie der Algebren, wobei die Grundlegung gleich so verallgemeinert wird, daß neben den Algebren auch allgemeiner Ringe mit Doppelkettensatz erfaßt werden.

In der späteren Buch-Veröffentlichung 4 wird dann sogar nur der Vielfachenkettensatz (minimum condition) beibehalten.

V. Ringe und hyperkomplexe Zahlsysteme

15. Zur Arithmetik hyperkomplexer Zahlen. – Hmb. Abh. **5** (1927), 261-289

Neue, einfachere Begründung, Weiterführung und Vertiefung der von *A. Speiser* 1926 im Anschluß an das Dicksonsche Buch über Algebren entwickelten Arithmetik in Algebren über dem rationalen Zahlkörper.

Behandelt werden:

Maximalordnungen, Ideale, Rechtsideale, Primideale, Rechtsidealklassen, Typen von Maximalordnungen, Brandtsches Gruppoid der Ideale.

VI. Allgemeines zur algebraischen Zahlentheorie

21. Über die Einheiten relativ galoisscher Zahlkörper. – Crelle **167** (1932), 153-156.

Vereinfachter bewertungstheoretischer Beweis des Minkowskischen Einheitensatzes für galoissche Zahlkörper und der Herbrandschen Verallgemeinerung auf relativ-galoissche Zahlkörper.

VI. Allgemeines zur algebraischen Zahlentheorie

22. Über die Bewertungen algebraischer Zahlkörper. – Crelle **167** (1932), 157-159.

Vereinfachungen der die arithmetischen Bewertungen betreffenden Schlüsse in der Grundlegung der Bewertungstheorie.

VI. Allgemeines zur algebraischen Zahlentheorie

27. Axiomatic characterisation of fields by the product formula for valuations. – Bull. Amer. Math. Soc. **51** (1945), 469-492, gemeinsam mit *G. Whaples.*

$$\text{Kennzeichnung der} \left\{ \begin{array}{c} \text{algebraischen Zahlkörper} \\ \text{algebraischen Funktionenkörper mit endlichem} \\ \text{Konstantenkörper} \end{array} \right\}$$

Durch das Bestehen der Produktformel:

$$\prod_{\mathfrak{p}} |a|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = 1 \qquad \text{bzw.} \qquad \prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = 1$$

nebst der ihr zugrundeliegenden Endlichkeitseigenschaft:

$$|a|_{\mathfrak{p}} \neq 1 \quad \text{nur für endlich viele } \mathfrak{p}.$$

Dabei muß aber zusätzlich noch gefordert werden, daß mindestens eine Bewertung entweder diskret mit endlichem Restklassenkörper oder arithmetisch ist. Dagegen braucht nicht gefordert zu werden, daß es sich um das volle Bewertungssystem handelt.

Mir erscheint diese Kennzeichnung weniger glatt und weniger zweckmäßig als die in meiner „Zahlentheorie“ gegebene durch bloße Endlichkeitseigenschaften.

28. A note on axiomatic characterisation of fields. – Bull. Amer. Math. Soc. **52** (1946), 245-247, gemeinsam mit *G. Whaples.*

Noch schwächere Forderung: Produkt aller Bewertungen konvergiert gegen 1.

VI. Allgemeines zur algebraischen Zahlentheorie

44. Representatives of the connected component of the idele class group. – Proc. Internat. Sympos. on Algebraic Number Theory, Tokyo 1956, 51-54.

A. Weil 1951 hat die Zusammenhangskomponente von 1 der Idelklassengruppe eines algebraischen Zahlkörpers nur durch ihr duales Gegenstück beschrieben. Artin gibt hier eine einfache Beschreibung dieser Zusammenhangskomponente selbst durch die Idelkomponenten eines total-positiven Grundeinheitensystems.

VII. Klassenzahl

39. The class-number of real quadratic fields. – Proc. Nat. Acad. Sci. U.S.A. **37** (1951), 524-525, gemeinsam mit *N.C. Ankeny* und *S. Chowla*.

40. The class-number of real quadratic number fields. – Ann. of Math. (2) **56** (1932), 479-493, gemeinsam mit *N.C. Ankeny* und *S. Chowla*.

Kongruenzen nach ungeraden Primteilern p der Diskriminante d eines reell-quadratischen Zahlkörpers für den Ausdruck $-2h\frac{v}{u}$, wo h die Klassenzahl und $\frac{u+v\sqrt{d}}{2}$ die Grundeinheit des Körpers sind.

Diese Kongruenzen sind als erster Vorstoß in ein wissenschaftliches Neuland zu werten, das neuerdings durch *H.W. Leopoldt*s Theorie der p-adischen Klassenzahlformel abelscher Zahlkörper systematisch erschlossen wurde.

VIII. Bücher

5. Algebraic numbers and algebraic functions I. – Princeton-New York 1951, 1-345

Bewertungen
Vollständige Körper
Die lokalen Grade e, f, n
Verzweigungstheorie
Differente
Vorbereitungen zur lokalen Klassenkörpertheorie
Erste und zweite Ungleichung
Normsymbol
Existenzsatz
Anwendungen und Illustrationen
Vorbereitungen zur globalen Theorie
Kennzeichnung von Körpern durch die Produktformel
Differentiale in Produktformelkörpern
Riemann-Rochscher Satz
Konstantenkörpererweiterungen
Anwendungen des Riemann-Rochschen Satzes
Differentiale in Funktionenkörpern

9. Class Field Theory. – Havard 1961, 1-259, gemeinsam mit *J. Tate*

Erste fundamentale Ungleichung
Zweite fundamentale Ungleichung
Reziprozitätsgesetz
Existenzsatz
Zusammenhangskomponente der Idelklassengruppe
Grunwald-Wangscher Satz
Höhere Verzweigungstheorie
Explizite Reziprozitätsformeln
Gruppenerweiterungen
Abstrakte Klassenkörpertheorie
Weilsche Gruppen

IX. Dissertationen

1. Hey, Käthe, *Analytische Zahlentheorie in Systemen hyperkomplexer Zahlen.* – Hamburg 1927.

Berühmt geworden durch Anwendbarkeit auf kurzen analytischen Beweis des Hauptsatzes der Algebrentheorie (*Zorn* 1933) und damit Begründung der Klassenkörpertheorie (*Hasse* 1933).

3. Henke, Karl, *Zur arithmetischen Idealtheorie hyperkomplexer Zahlen.* – Hamburg 1931. – Hmb. Abh. **11** (1935), 311-332.

Axiomatische Begründung der Idealtheorie auf *E. Noether*scher Grundlage.

4. Beller, Josef, *Beiträge zur Arithmetik der dreidimensionalen Vektoren.* – Hamburg 1933. – Mitt. Math. Ges. Hamburg **7** (1934), 213-231.

5. Nehrkorn, Harald, *Über absolute Idealklassengruppen und Einheiten in algebraischen Zahlkörpern.* – Hamburg 1932. – Hmb. Abh. **9** (1933), 318-334.

Einbettung der Idealklassen für Teilkörper eines relativ-galoisschen Zahlkörpers K/k wird nach gruppentheoretischem Schema untersucht, entsprechend auch für Einheiten. –

Untersuchungen dieser Art finden heute in den Arbeiten von *H.W. Leopoldt* ihren systematischen Ausbau.

6. Rothgiesser, Hans, *Zum Reziprozitätsgesetz für ℓ^n.* – Hamburg 1934. – Hmb. Abh. **11** (1936), 1-16.

Beweis einer interessanten Formel für das allgemeine Reziprozitätsgesetz der ℓ^n-ten Potenzreste, in die ein Differentialoperator D und ein ℓ-Potenzierungsoperator P eingehen.

9. Söhngen, Heinz, *Zur komplexen Multiplikation.* – Hamburg 1934. – Math. Ann. **111** (1935), 302-328.

Übertragung einer Begründung der Strahlklassenkörpererzeugung von der Hauptordnung auf eine beliebige Ordnung des imaginär-quadratischen Grundkörpers.

IX. Dissertationen

10. Weissinger, Johannes, *Theorie der Divisorenkongruenzen.* – Hamburg 1937. – Hmb. Abh. **12** (1938), 115-126.

Verallgemeinerung des Riemann-Rochschen Satzes für Kongruenzklassen und Herleitung der Funktionalgleichung der zugehörigen L-Funktionen. – Letztere war schon 1934 von mir vermutet und 1936 von *E. Witt* bewiesen worden, wovon allerdings Verf. keine Kenntnis hatte.

Außerdem 16 in den Vereinigten Staaten angeregte Dissertationen algebraisch-zahlentheoretischen Inhalts, darunter die von *Shapiro*, *Mills*, *Ankeny*, *O'Meara*, *Wang*, *Tate*, *S. Lang*, *Ramanathan.*

Man kann von Artin schon heute sagen, daß er der Mathematik unseres Jahrhunderts seinen Stempel aufgedrückt hat. Seine Art, mathematische Sachverhalte zu sehen, zu durchdringen und in größter Eleganz und Klarheit zu gestalten, lebt fort in seinen Schülern und allen den zahlreichen Fachgenossen, die er durch sein Wirken mitgerissen hat. Dazu dürfen wir uns wohl alle zählen. Er wird uns also auch überhaupt der mathematischen Nachwelt unvergeßlich bleiben.

Kapitel 2

Register