1 08.11.1932, Hasse to Artin

Mathematisches Seminar der Universität

Marburg-Lahn, den 8. November 1932

Lieber Herr Artin!

Nach einigem weiteren Nachdenken habe ich eine halbwegs befriedigende Lösung meiner Frage über die Klassenkörperbeweise gefunden. Ich möchte sie Ihnen auf alle Fälle vorlegen. Vielleicht können Sie es noch einfacher machen.

Ich vermeide auf jeden Fall den vorherigen Beweis des „exakten" Zerlegungsgesetzes, zeige vielmehr zuerst die Gültigkeit des Artinschen Reziprozitätsgesetzes (ARG) für zyklische Körper, dann damit die Gültigkeit des „statistischen" Zerlegungsgesetzes für beliebige Klassenkörper, und daraus schließlich die Gültigkeit des ARG für beliebige Klassenkörper.

Zunächst ein

Hilfssatz: Ist K beliebig abelsch, so nimmt das Artin-Symbol $\left(\frac{K}{a}\right)$ jeden Wert S aus der Gruppe G von K an.

Beweis: Man setze K aus unabhängigen Körpern K_i von Primzahlpotenzgraden $l_i^{v_i}$ zusammen. Die K_i sind Klassenkörper zu Gruppen H_i, deren direkter Durchschnitt die K zugeordnete Idealgruppe H ist. Nach dem Satz von der arithmetischen Progression kann man Primideale p_i wählen, die in allen H_j $(j \neq i)$ liegen, während sie nicht in der H_i enthaltenden Gruppe $\overline{H}_i$ vom Primzahlindex l_i liegen. Dabei kann man noch diejenigen ev. Ausnahmen der Dichte 0 vermeiden, für die aus der Zugehörigkeit zu H_j nicht das volle Zerfallen in K_j folgt. Die p_i zerfallen dann also voll in den K_j $(j \neq i)$, dagegen bleiben sie unzerlegt in den in den K_i enthaltenen Körpern $\overline{K}_i$ vom Primzahlgrad l_i (weil sie sonst in $\overline{H}_i$ liegen müßten). Sie bleiben dann auch unzerlegt in den K_i. Daher sind die Artin-Symbole $\left(\frac{K}{p_i}\right) = S_i$ ein volles System von Erzeugenden der Gruppen G_i der K_i, und durch Zusammensetzung von Idealen a aus den p_i kann jeder Wert S des Artin-Symbols $\left(\frac{K}{a}\right)$ erzeugt werden. –

Ich beweise ferner:

I. Ist K zyklisch und S ein erzeugendes Element der Gruppe G von K, so existiert ein Ideal c derart, daß $\left(\frac{K}{c}\right) = S$ ist und daß aus $\left(\frac{K}{a}\right) = S^x$ folgt $a \sim c^x$ (H).

Bemerkung: Insbesondere also:

Aus $\left(\frac{K}{a}\right) = 1$ folgt a in H.

Das ist aber (auch für beliebige Klassenkörper K) fast unmittelbar äquivalent mit dem ARG.

Beweis: Es genügt, den Fall eines Primideals $a = p$ zu behandeln. Methode: Überschneidung der Klasseneinteilung nach der K zugeordneten Idealgruppe H mit der nach zwei Gruppen Q und Q', die zu zwei zyklischen Kreiskörpern C und C' gehören, und zwar derart, daß Q zum Vergleich von c^x mit einem zu wählenden Hilfsideal r und Q' zum Vergleich von p mit demselben r dient. (Anordnung nach Chevalley.)

Im einzelnen so:

1. C unabhängig von K so, daß Grad q Multiplum des Grades n von K. Sei T Erzeugende der Gruppe von C, und K_0 der Inv. Körper von ST in KC. In K_0 nach Hilfssatz ein c_0 so, daß

$$\left(\frac{KC}{c_0}\right) = ST. \text{ Sei } c = N(c_0).$$

C' unabhängig von KC so, daß p in Klasse von durch n teilbarer Ordnung nach Q'; dann sicher auch Grad q' von C' Multiplum von n. Es ist

$$\left(\frac{KC'}{p}\right) = S^x T' \quad \text{mit } T' \text{ aus der Gruppe von } C'.$$

Im Inv. Körper K_0' von $S^x T'$ in KC' ist dann p voll zerlegt. Für einen der Primteiler p_0' gilt dann

$$\left(\frac{KC'}{p_0'}\right) = S^x T' \qquad \text{und} \qquad p = N(p_0').$$

Im Inv. Körper $\overline{K}_0'$ von $S^x T^x T'$ innerhalb KCC' wählen wir $\overline{r}_0$ so, daß

$$\left(\frac{KCC'}{\overline{r}_0}\right) = S^x T^x T'. \text{ Sei } r = N(\overline{r}_0).$$

Das sei unser Vergleichshilfsideal.

2. Wie man aus den Invarianzgruppen abliest, gilt:

$$\overline{K}_0 \geqq K_0 \quad \text{und} \quad \overline{K}_0 \geqq K_0'.$$

Sei dementsprechend

$$r_0 = N_{\overline{K}_0|K_0}(\overline{r}_0) \qquad \text{und} \qquad r_0' = N_{\overline{K}_0|K_0'}(\overline{r}_0).$$

Dann ist auch

$$\left(\frac{KCC'}{r_0}\right) = S^x T^x T' \qquad \text{und} \qquad \left(\frac{KCC'}{r_0'}\right) = S^x T^x T'.$$

Ferner sieht man aus den Gradbedingungen, nach denen T und T' durch n teilbare Ordnungen haben, daß gilt:

$$KC = K_0 C \qquad \text{und} \qquad KC' = K_0' C'.$$

Hiernach sind KC und KC' zyklische Kreiskörper über K_0 bzw. K_0'.

3. Für diese Körper gilt also das ARG. Daher folgt aus der Beziehung zwischen den Artin-Symbolen von KC nach r_0 und nach c_0, daß r_0 und c_0^x in derselben Klasse der zu KC über K_0 gehörigen Einteilung liegen. Durch Normbildung folgt daraus nach dem Verschiebungssatz, daß r und c^x in derselben Klasse der zu KC über dem Grundkörper k gehörigen Klasseneinteilung liegen, insbesondere also in derselben Klasse der zu K über k gehörigen Klasseneinteilung, der nach H.

Entsprechend folgt aus der Beziehung zwischen den Artin-Symbolen von KC' nach r_0 und p_0', daß diese beiden Ideale in derselben Klasse der zu KC' über K_0' gehörigen Klasseneinteilung liegen, also ihre Normen r und p wieder in derselben Klasse nach KC' über k, somit insbesondere nach H.

Zusammengenommen also: $p \sim c^x(H)$.

II. Zerlegungsgesetz für fast alle Primideale bei beliebigem Klassenkörper K.

Beweis: Durch vollständige Induktion nach dem Körpergrad.

1. Für Primzahlgrad richtig, da dann K zyklisch, also das ARG bereits bewiesen.

2. Angenommen, es sei bei niedrigerem Körpergrad als der von K (und beliebigem Grundkörper) bereits bewiesen.

a. Für diejenigen Primideale p_L, die in einem Körper L mit $k < L \leqq K$ voll zerfallen, ist nach dem Verschiebungssatz die Ordnung f in bezug auf H gleich der Ordnung ihrer Primteiler q_L in L in bezug auf die L zugeordnete Idealgruppe J. Nach Induktionsannahme zerfallen fast alle diese q_L in K in Primteiler f-ten Grades. Wegen $p_L = N(q_L)$ bleibt das „fast alle“ beim Übergang zu den p_L erhalten, und also zerfallen auch fast alle diese p_L in K in Primteiler vom Grade f.

Das „fast alle“ bleibt auch erhalten, wenn man die endlich vielen Körper L, die obiger Bedingung genügen, durchgeht.

b. Es bleiben also nur noch diejenigen Primideale p übrig, die in keinem solchen L voll zerfallen. Diese sind aber unzerlegt in K – das ist also nur bei zyklischem K möglich – und dann ist wieder bereits das ARG bewiesen.

III. Hilfssatz: Ist K Klassenkörper zu H und $H' > H$, so existiert zu H' ein Klassenkörper K' $(< K)$.

Beweis: Wie im Göttinger Vortrag, indem man zum Aufbau von H' aus H nur solche Primideale verwendet, die nicht zu den ev. Ausnahmen im statistischen Zerlegungsgesetz für K gehören. – Das geht wieder nach dem Satz von der arithmetischen Progression.

IV. Artinsches Reziprozitätsgesetz für beliebige Klassenkörper K.

Beweis: Basisdarstellung der Klassengruppe nach H, Definition der Gruppen H_i und Körper K_i (auf Grund des Hilfssatzes) wie im Göttinger Vortrag.

Dann
$$\left(\frac{K}{a}\right) = \prod \left(\frac{K_i}{a}\right) \quad \text{in direkter Zerlegung.}$$
Ist also $\left(\frac{K}{a}\right) = 1$, so sind alle $\left(\frac{K_i}{a}\right) = 1$, also nach I a in allen H_i, und somit a im Durchschnitt der H_i, d.h. a in H.

Damit ist wieder die Grundtatsache des ARG festgestellt, also das Gesetz bewiesen. –

Jetzt folgt natürlich die volle Gültigkeit des Zerlegungssatzes, sowie der Isomorphiesatz.

2 undatiert, Beweisskizze des Umkehrsatzes, von Hasse

Skizze des Beweises des Umkehrsatzes.

K/k zyklisch vom Grad n, S erzeugender Automorphismus

$f_\mathfrak{p}$ $\mathfrak{p}$-Führer von K/k, d.h. früheste $\mathfrak{p}$-Potenz, für die aus $\alpha \equiv N(\mathsf{A}) \bmod f_\mathfrak{p}$ mit A aus K folgt $\alpha = N(\mathsf{A}_\mathfrak{p})$ mit $\mathsf{A}_\mathfrak{p}$ aus $K_\mathfrak{p}$.

$f = \prod_\mathfrak{p} f_\mathfrak{p}$ Führer von K/k (definitorisch).

m beliebiges Multiplum von f.

Zu berechnen ist der Index $h = (A_m : H_m)$ der K/k mod m zugeordneten Idealgruppe H_m in der Gruppe A_m aller zu m primen Ideale aus k.

Ich lasse nun zunächst eine durchgängige Modifikation des Idealbegriffs eintreten, die kurz gesagt dahin geht, daß Primteiler von m als 1 gerechnet werden, NB. also einfach eine Faktorgruppenbildung! Während also die gewöhnlichen Ideale in der Vorgabe eines Systems von Ordnungszahlen für *alle* endlichen Primstellen bestehen (nur endlich viele Ordnungszahlen $\neq 0$), sollen jetzt die Ideale in der Vorgabe eines Systems von Ordnungszahlen (nur endlich viele $\neq 0$) für *alle nicht in m vorkommenden* endlichen Primstellen bestehen, während für die Primteiler von m (und natürlich die unendlichen Primstellen) keinerlei Vorschrift gemacht wird. Entsprechend wird der Begriff der Einheit modifiziert: Eine Einheit ist jetzt eine Zahl, die höchstens Primteiler von m enthält. Im folgenden sind durchweg diese modifizierten Begriffe genannt.

Man sieht sofort, daß der obige Index h dann auch erklärbar ist als der Index der K/k mod m zugeordneten Idealgruppe H in der Gruppe A *aller* Ideale aus k. (Man beachte, daß „Idealgruppe“ jetzt eine modifizierte Bedeutung hat!)

In Gruppenstenographie:

$$h = \left[\mathfrak{a} : \mathfrak{A}^N(\nu)\right], \qquad \left\{\begin{array}{l} \mathfrak{a} \text{ beliebige Ideale aus } k, \\ \mathfrak{A} \text{ beliebige Ideale aus } K, \\ N = 1 + S + \cdots + S^{n-1}, \\ \nu \text{ Normenreste (\textit{nicht} nur zu } m \text{ prime!)} \\ \text{von } K \bmod m. \end{array}\right.$$

Gerade diese Befreiung der *Grundbegriffe* der Klassenkörpertheorie von der lästigen Voraussetzung „prim zu m" scheint mir methodisch wichtig und vorteilhaft zu sein. Das Ganze bewegt sich in einem Ideenkreis, der vom Riemann-Rochschen Satz her geläufig ist, und in der Tat ist ja die zu machende Berechnung als Analogon des Riemann-Rochschen Satzes anzusehen.

Neben dem Index h führe ich von vornherein den Index

$$a = \left[\nu \cap \mathfrak{A}^N : \mathsf{A}^N\right], \qquad \begin{cases} \cap & \text{Zeichen für Durchschnitt,} \\ \mathsf{A} & \text{beliebige Zahlen aus } K, \end{cases}$$

ein, der ersichtlich die Abweichung von der Gültigkeit des Normensatzes mißt ($a = 1$ bedeutet, daß jeder Normenrest ν mod m, der Idealnorm ist, auch Zahlnorm ist. Da m Multiplum von f ist, ist für die nicht in m aufgehenden $\mathfrak{p}$ $f_{\mathfrak{p}} = \mathfrak{p}^0$, also die in „Idealnorm" geforderte Ordnungszahlbedingung schon hinreichend für „$\mathfrak{p}$-adische Zahlnorm". Daher sagt $a = 1$ in der Tat: Wenn ν für jedes $\mathfrak{p}$ $\mathfrak{p}$-adische Norm ist, ist, ν Zahlnorm; und umgekehrt hat dieser Normensatz ersichtlich $a = 1$ zur Folge.)

Ich gehe nun von vornherein auf die Berechnung des Indexquotienten

$$q = \frac{h}{a} = \frac{[\mathfrak{a} : \mathfrak{A}^N(\nu)]}{[\nu \cap \mathfrak{A}^N : \mathsf{A}^N]}$$

aus, und habe $q = n$ zu beweisen.

Erste Umformungsserie (Abspaltung der Klassenkörpertheorie im Kleinen).

$$
\begin{aligned}
q &= \frac{[\mathfrak{a} : \mathfrak{A}^N(\nu)]}{[\nu \cap \mathfrak{A}^N : \mathsf{A}^N]} = \frac{[\mathfrak{a} : \mathfrak{A}^N(\nu)][\mathfrak{A}^N(\nu) : (\nu)]}{[\nu \cap \mathfrak{A}^N : \mathsf{A}^N][\mathfrak{A}^N(\nu) : (\nu)]} \\
&= \frac{[\mathfrak{a} : (\nu)]}{[(\nu) \cap \mathfrak{A}^N : (\mathsf{A}^N)][\varepsilon \cap \nu : \eta][\mathfrak{A}^N : (\nu) \cap \mathfrak{A}^N]} \\
&= \frac{[\mathfrak{a} : (\nu)]}{[\mathfrak{A}^N : (\mathsf{A})^N][\varepsilon \cap \nu : \eta]}\,, \qquad \left\{ \begin{array}{ll} \varepsilon & \text{beliebige Einheiten aus } k, \\ \eta & \text{Einheiten aus } k \text{, die} \\ & \text{Zahlnormen aus } K \text{ sind,} \end{array} \right. \\
&= \frac{[\mathfrak{a} : (\alpha)][(\alpha) : (\nu)]}{[\mathfrak{A}^N : (\mathsf{A})^N][\varepsilon \cap \nu : \eta]} \\
&= \frac{[\mathfrak{a} : (\alpha)][\alpha : \nu]}{[\mathfrak{A}^N : (\mathsf{A})^N][\varepsilon \cap \nu : \eta][\varepsilon : \varepsilon \cap \nu]}\,, \qquad \alpha \text{ beliebige Zahlen aus } k, \\
&= \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{A}^N : (\mathsf{A})^N][\varepsilon : \eta]} \cdot [\alpha : \nu] \\
&= q_0 \cdot \prod_{\mathfrak{p} | m} n_{\mathfrak{p}}\,, \qquad n_{\mathfrak{p}} \text{ Grad von } K_{\mathfrak{p}}/k_{\mathfrak{p}},
\end{aligned}
$$

(Hauptergebnis der Klassenkörpertheorie im Kleinen)

Es bleibt zu berechnen der Indexquotient

$$q_0 = \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{A}^N : (\mathsf{A})^N][\varepsilon : \eta]}.$$

Zweite Umformungsserie (Theorie des Hauptgeschlechts und der ambigen Klassen).

$$[\mathfrak{A}^N : (\mathsf{A})^N] = \frac{[\mathfrak{A} : (\mathsf{A})]}{[\mathfrak{A}^{1-s} : (\theta)]}\,,$$

θ Zahlen aus K mit $(\theta)^N = 1$, für die also $\theta^N = \eta$ Einheit ist; das sind dann gerade die obigen η. – Es wurde ferner angewandt, daß Ideale mit Norm 1 stets $1-s$–te Idealpotenzen sind und umgekehrt.

$$= \frac{[\mathfrak{A} : (\mathsf{A})]}{[\mathfrak{A} : \mathfrak{B}]}\,,$$

$\mathfrak{B}$ Ideale aus K, für die $\mathfrak{B}^{1-s} = (\theta)$ Hauptideal ist; das sind dann (wieder nach dem eben genannten Normensatz) gerade die obigen θ.

$$= [\mathfrak{B} : (\mathsf{A})].$$

Dritte Umformungsserie (Reduktion auf Einheitenhauptgeschlecht).

$$\begin{aligned} q_0 &= \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{A}^N : (\mathsf{A})^N][\varepsilon : \eta]} = \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{B} : (\mathsf{A})][\varepsilon : \eta]} \\ &= \frac{[\mathfrak{a} : (\alpha)]}{[(\theta) : (\mathsf{A})^{1-s}][\mathfrak{a} : (\mathsf{B})][\varepsilon : \eta]}, \end{aligned}$$

B Zahlen aus K, für die $(\mathsf{B})^{1-s} = 1$, d.h. B^{1-s} Einheit ist. – Man beachte, daß wegen des modifizierten Idealbegriffs die Ideale aus k die *einzigen* ambigen (bei $1-s$ 1-werdenden) Ideale sind; gerade in diesem Punkt besteht die *sachliche* Kürzung bei dieser neuen Methode!

$$= \frac{[(\mathsf{B}) : (\alpha)]}{[(\theta) : (\mathsf{A})^{1-s}][\varepsilon : \eta]}$$

$$= \frac{[\mathsf{B} : \alpha\mathsf{E}]}{[\theta : \mathsf{A}^{1-s}\mathsf{E}][\varepsilon : \eta]},$$

E beliebige Einheiten aus K,

$$= \frac{[\mathsf{H} : \mathsf{E}^{1-s}]}{[\theta : \mathsf{A}^{1-s}\mathsf{E}][\varepsilon : \eta]},$$

H Einheiten aus K mit $\mathsf{H}^N = 1$, für die also $\mathsf{H} = \mathsf{B}^{1-s}$ ist; das sind dann gerade die obigen B.

$$= \frac{[\mathsf{H} : \mathsf{E}^{1-s}]}{[\eta : \mathsf{E}^N][\varepsilon : \eta]}$$

$$= \frac{[\mathsf{H} : \mathsf{E}^{1-s}]}{[\varepsilon : \mathsf{E}^N]}.$$

$$\textbf{Ergebnis:}\ \frac{h}{a} = q = q_0 \cdot \prod_{\mathfrak{p}|m} n_{\mathfrak{p}} = \frac{[\mathsf{H} : \mathsf{E}^{1-s}]}{[\varepsilon : \mathsf{E}^N]} \cdot \prod_{\mathfrak{p}|m} n_{\mathfrak{p}}.$$

Nun hat man durch leichte Modifikation der Herbrandschen Methode (Einbeziehung der endlichen $\mathfrak{p}|m$), also durch Konstruktion eines Systems unabhängiger modifizierter Einheiten, nur den Indexquotienten

$$\frac{[\mathsf{H} : \mathsf{E}^{1-s}]}{[\varepsilon : \mathsf{E}^N]} = \frac{n}{\prod_{\mathfrak{p}|m} n_{\mathfrak{p}}}$$

nachzuweisen. Das geht, wie Artin mir schrieb, ganz ebenso einfach, wie bisher. Darum kommt:

$$q = n, \quad \text{also} \quad h = a \cdot n.$$