Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1937
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0176
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0176

LOG Id: LOG_0025
LOG Titel: Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren.
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren.

Von *Martin Eichler* in Halle.

1. Die neuere Entwicklung in der Algebrentheorie hat gezeigt, daß sich diese Theorie von der der Zahlkörper durch viel größere Einfachheit auszeichnet. Eine besonders schwierige Aufgabe ist es bekanntlich, die Idealklassenzahl eines Zahlkörpers zu berechnen, und diese darf keineswegs als allgemein gelöst betrachtet werden. Die Frage nach der Idealklassenzahl im Hyperkomplexen wird wiederum i. a. durch sehr einfache Sätze beantwortet, die im folgenden bewiesen werden sollen.

Satz 1. *Es bezeichne* $\mathfrak{A}$ *eine normale einfache Algebra vom Grad* n *über dem algebraischen Zahlkörper* K *und* $\mathfrak{u}$ *das Produkt aller unendlichen Primstellen von* K, *an denen* $\mathfrak{A}$ *verzweigt ist. Ist* $n > 2$ *oder umfaßt* $\mathfrak{u}$ *nicht alle unendlichen Primstellen von* K, *so sind die und nur die Ideale von* $\mathfrak{A}$ *Hauptideale, deren Normen* [1]) *zum Strahl* mod $\mathfrak{u}$ *gehören.*

Dieser Satz sagt einzig über Quaternionenalgebren über einem totalreellen algebraischen Zahlkörper nichts aus, welche totalpositive Normenformen haben. Solche Quaternionenalgebren sind andererseits dadurch unter allen normalen einfachen Algebren ausgezeichnet, daß sich sämtliche Einheiten jeder ihrer Ordnungen als Produkte von endlich vielen mit Zentrumseinheiten darstellen lassen; dies läßt sich mühelos aus dem Dirichletschen Einheitensatze folgern. Es ist zu erwarten, daß sich hier die Idealklassenzahl so wenigstens größenordnungsmäßig auf analytischem Wege bestimmen läßt, wie es für rationales Zentrum möglich ist [2]).

Der Satz 1 ist mit folgendem gleichbedeutend:

Satz 2. *Ist* $n > 2$ *oder umfaßt* $\mathfrak{u}$ *nicht alle unendlichen Primstellen von* K, *so ist die Idealklassenzahl in* $\mathfrak{A}$ *gleich der Strahlklassenzahl* mod $\mathfrak{u}$ *in* K.

Wenn $\mathfrak{A}$ eine Matrixalgebra ist, so sind die behaupteten Sätze schon bekannt und in der Dissertation von Herrn Schilling bewiesen worden [3]). Für den Fall, daß $\mathfrak{A}$ eine indefinite Quaternionenalgebra über dem rationalen Zahlkörper ist, machte mich Herr Brandt auf ihre Gültigkeit aufmerksam. Einen Beweis könnte man hier auf den Satz von A. Mayer stützen, daß i. a. zwei indefinite ternäre quadratische Formen desselben Geschlechts mit rationalen Koeffizienten äquivalent sind [4]). Einen Hinweis auf die

[1]) Die Normen $n(\mu)$, $n\mathfrak{M}$ von Zahlen μ und Idealen $\mathfrak{M}$ sind stets in reduziertem Sinne zu verstehen.

[2]) H. Brandt, Idealtheorie in Quaternionenalgebren, Math. Ann. **99** (1928), S. 1, § 67.
K. Hey, Analytische Zahlentheorie in Systemen hyperkomplexer Zahlen, Diss. Hamburg 1929.

[3]) O. Schilling, Über gewisse Beziehungen zwischen der Arithmetik hyperkomplexer Zahlsysteme und algebraischer Zahlkörper, Math. Ann. **111** (1935), S. 372, § 3.

[4]) Vgl. L. E. Dickson, Studies in the theory of Numbers, Chicago 1930; dort finden sich weitere Literaturangaben.

Zusatz bei der Korrektur: Zu meinem Satz 1 vgl. auch C. G. Latimer, On ideals in generalized quaternion algebras, Transactions Amer. Math. Soc. **38** (1935), p. 436, und J. H. Teller, A class of quaternion algebras, Duke Mathematical Journal **2** (1936), p. 280.

Gültigkeit dieser Sätze stellt auch das Ergebnis dar, daß fast jede an allen unendlichen Verzweigungsprimstellen einer normalen Divisionsalgebra $\mathfrak{A}$ positive Zahl Norm einer Zahl aus $\mathfrak{A}$ ist [5]).

Wie in den beiden genannten Spezialfällen gelingt der Beweis unter den allgemeinsten Bedingungen im wesentlichen auf arithmetischem Wege. Analytische Sätze spielen eine untergeordnete Rolle, man braucht von solchen nur den Satz von der arithmetischen Progression und den hiermit verwandten Dichtigkeitssatz von Tschebotarew. Herrn C. Chevalley verdanke ich wesentliche Vereinfachungen meines Beweises und ebenso den Hinweis darauf, daß die behaupteten Sätze in der Regel auch für $n = 2$ gültig bleiben; mir war diese Tatsache ursprünglich nur in dem Spezialfalle $\mathfrak{u} = (1)$ bekannt.

2. Einige Hilfssätze werden vorausgeschickt.

Hilfssatz 1. *Es sei* $\mathfrak{p}$ *ein Primideal von* K *und* $\mathsf{K}_\mathfrak{p}$ *die* $\mathfrak{p}$*-adische Erweiterung von* K. $f(x)$ *sei ein irreduzibles Polynom in* $\mathsf{K}_\mathfrak{p}$. *Dann existiert ein Exponent* h *derart, daß jedes Polynom* $g(x)$ *mit Koeffizienten aus* K, *welches der Kongruenz*

$$g(x) \equiv f(x) \pmod{\mathfrak{p}^h}$$

genügt, ebenfalls in $\mathsf{K}_\mathfrak{p}$ *irreduzibel ist.*

Beweis. Ist $f(x)$ in dem Ring der Restklassen der ganzen Größen von $\mathsf{K}_\mathfrak{p}$ mod $\mathfrak{p}^h$ irreduzibel oder, kurz gesagt: ist $f(x)$ mod $\mathfrak{p}^h$ irreduzibel, so gilt dasselbe für $g(x)$, und $g(x)$ ist auch in $\mathsf{K}_\mathfrak{p}$ irreduzibel. Es braucht somit nur ein Exponent h gefunden zu werden, für welchen $f(x)$ mod $\mathfrak{p}^h$ irreduzibel ist.

Wäre für jedes h

$$f(x) \equiv p_h(x) q_h(x) \pmod{\mathfrak{p}^h},$$

so gälte auch

$$f(x) \equiv p_h(x) q_h(x) \pmod{\mathfrak{p}}.$$

$f(x)$ kann mod $\mathfrak{p}$ aber nur auf endlich viele Arten zerlegt werden, und daher wird es zwei Polynome $p^{(1)}(x)$, $q^{(1)}(x)$ derart geben, daß für eine unendliche Menge H_1 von Exponenten h

$$p_h(x) \equiv p^{(1)}(x) \pmod{\mathfrak{p}}, \quad q_h(x) \equiv q^{(1)}(x) \pmod{\mathfrak{p}}$$

gilt. Es werde als bewiesen angenommen, daß es zwei Folgen von Polynomen $p^{(i)}(x)$, $q^{(i)}(x)$ $(i = 1, 2, \ldots, t)$ so gibt, daß für jeden Exponenten h aus einer unendlichen Teilmenge H_i von H_1

$$p_h(x) \equiv p^{(i)}(x) \pmod{\mathfrak{p}^i}, \quad q_h(x) \equiv q^{(i)}(x) \pmod{\mathfrak{p}^i}$$

und ferner

$$p^{(i)}(x) \equiv p^{(i-1)}(x) \pmod{\mathfrak{p}^{i-1}}, \quad q^{(i)}(x) \equiv q^{(i-1)}(x) \pmod{\mathfrak{p}^{i-1}}$$

gilt.

$f(x)$ kann nun auch mod $\mathfrak{p}^{t+1}$ nur auf endlich viele Arten zerlegt werden, daher wird es in den Restklassen von $p^{(t)}(x)$ und $q^{(t)}(x)$ mod $\mathfrak{p}^t$ zwei Polynome $p^{(t+1)}(x)$ und $q^{(t+1)}(x)$ so geben, daß für eine unendliche Teilmenge H_{t+1} von H_t

$$p_h(x) \equiv p^{(t+1)}(x) \pmod{\mathfrak{p}^{t+1}}, \quad q_h(x) \equiv q^{(t+1)}(x) \pmod{\mathfrak{p}^{t+1}}$$

gilt. Die Folgen $p^{(i)}(x)$, $q^{(i)}(x)$ konvergieren $\mathfrak{p}$-adisch gegen zwei Grenzfunktionen $p(x)$, $q(x)$, und es wird

$$f(x) = p(x)\, q(x),$$

im Widerspruch zur Voraussetzung.

---

[5]) H. Hasse und O. Schilling, Die Normen aus einer normalen Divisionsalgebra über einem algebraischen Zahlkörper, dieses Journ. **174** (1935), S. 248.

Hilfssatz 2. *Es sei* $\mathfrak{J}$ *eine Maximalordnung einer normalen einfachen Algebra* $\mathfrak{A}$ *vom Grad* n *über* K *und* $\mathfrak{p}$ *ein Primideal aus* K. $\alpha_\mathfrak{p}$ *sei eine Zahl aus* $\mathfrak{J}_\mathfrak{p}$ *mit der Eigenschaft, daß* $\mathsf{K}_\mathfrak{p}(\alpha_\mathfrak{p})$ *eine Erweiterung* n*-ten Grades von* $\mathsf{K}_\mathfrak{p}$ *ist. Dann gibt es einen solchen Exponenten* h*, daß für jede Zahl* α *aus* $\mathfrak{J}$*, die der Kongruenz*

$$\alpha \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{p}^h\mathfrak{J}_\mathfrak{p}}$$

genügt, auch $\mathsf{K}_\mathfrak{p}(\alpha)$ *eine Erweiterung* n*-ten Grades von* $\mathsf{K}_\mathfrak{p}$ *ist.*

Beweis. Ist

$$\alpha \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{p}^h\mathfrak{J}_\mathfrak{p}},$$

so sind die Hauptgleichungen von $\alpha_\mathfrak{p}$ und $\alpha \bmod \mathfrak{p}^h$ kongruent. Die Hauptgleichung von $\alpha_\mathfrak{p}$ ist nach Voraussetzung in $\mathsf{K}_\mathfrak{p}$ irreduzibel. Wird jetzt h nach Hilfssatz 1 so groß gewählt, daß auch die Hauptgleichung von α in $\mathsf{K}_\mathfrak{p}$ irreduzibel ist, so ist $\mathsf{K}_\mathfrak{p}(\alpha)$ eine Erweiterung n-ten Grades von $\mathsf{K}_\mathfrak{p}$.

Im folgenden werden jetzt kommutative Systeme $\mathsf{K}(\xi)$ betrachtet, die durch Zahlen ξ aus einer Maximalordnung $\mathfrak{J}$ und deren Potenzen über K erzeugt werden. Dann und nur dann, wenn $\mathsf{K}(\xi)$ halbeinfach ist, läßt sich von der Ordnung aller ganzen Größen von $\mathsf{K}(\xi)$ in sinnvoller Weise reden; diese Ordnung sei mit $\mathfrak{R}(\xi)$ bezeichnet. $\mathfrak{F}_\xi$ bedeute den Führer der Ordnung $\mathfrak{R}(\xi) \cap \mathfrak{J}$ bezüglich $\mathfrak{R}(\xi)$, d. h. es sei in Dedekindscher Schreibweise

$$\mathfrak{F}_\xi = \frac{\mathfrak{R}(\xi) \cap \mathfrak{J}}{\mathfrak{R}(\xi)}.$$

Besitzt $\mathsf{K}(\xi)$ ein von 0 verschiedenes Radikal, so werde symbolisch

$$\mathfrak{F}_\xi = 0$$

geschrieben. Wenn ξ ganz und $\mathfrak{F}_\xi = (1)$ ist, so bedeutet das, daß ξ in $\mathfrak{J}$ enthalten und $\mathsf{K}(\xi)$ halbeinfach ist. Die Bezogenheit von $\mathfrak{F}_\xi$ auf $\mathfrak{J}$ braucht nicht zum Ausdruck gebracht zu werden, ohne daß Mißverständnisse zu befürchten sind. Ist $\mathfrak{p}$ ein Primideal von K, $\xi_\mathfrak{p}$ eine Zahl aus $\mathfrak{J}_\mathfrak{p}$, so wird an Stelle von $\mathfrak{R}(\xi)$, $\mathfrak{F}_\xi$ jetzt $\mathfrak{R}_\mathfrak{p}(\xi_\mathfrak{p})$, $\mathfrak{F}_{\xi_\mathfrak{p},\mathfrak{p}}$ zu schreiben sein, wobei diese Ausdrücke natürlich von den $\mathfrak{p}$-Komponenten von $\mathfrak{R}(\xi)$ und $\mathfrak{F}_\xi$ zu unterscheiden sind.

Hilfssatz 3. *Ist* $\alpha_\mathfrak{p}$ *eine Zahl aus* $\mathfrak{J}_\mathfrak{p}$*, für die* $\mathfrak{F}_{\alpha_\mathfrak{p},\mathfrak{p}} = (1)$ *ist, so gibt es einen Exponenten* r *derart, daß für jede der Kongruenz*

$$\alpha \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{p}^r\mathfrak{J}_\mathfrak{p}}$$

genügende Zahl α *aus* $\mathfrak{J}$ *auch* $\mathfrak{F}_{\alpha,\mathfrak{p}} = (1)$ *ist.*

Beweis. Ist $\varrho_0, \varrho_1, \ldots, \varrho_{n-1}$ eine Basis von $\mathfrak{R}_\mathfrak{p}(\alpha_\mathfrak{p})$ in bezug auf $\mathsf{K}_\mathfrak{p}$, so besteht ein System linearer Gleichungen

$$\alpha_\mathfrak{p}^k = \sum_{i=0}^{n-1} a_{ik}\varrho_i \qquad (k = 0, 1, \ldots, n-1)$$

mit ganzen a_{ik} aus $\mathsf{K}_\mathfrak{p}$. Die Determinante $|a_{ik}|$ ist von 0 verschieden, sie möge $\mathfrak{p}$ gerade in der Potenz $\mathfrak{p}^{r_1}$ enthalten. Ist jetzt

$$\alpha \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{p}^{r_1+1}\mathfrak{J}_\mathfrak{p}},$$

so sind die Ordnungen $[1, \alpha, \ldots, \alpha^{n-1}]$ und $[1, \alpha_\mathfrak{p}, \ldots, \alpha_\mathfrak{p}^{n-1}]$ mod $\mathfrak{p}^{r_1+1}$ isomorph, und daher geht erstere durch die lineare Substitution $(a_{ik})^{-1}$ in eine Ordnung $\mathfrak{R}_\mathfrak{p}(\alpha)$ über, welche in $\mathfrak{J}_\mathfrak{p}$ enthalten ist und welche der Ordnung $\mathfrak{R}_\mathfrak{p}(\alpha_\mathfrak{p})$ mod $\mathfrak{p}$ isomorph ist. Nun läßt sich $\mathfrak{R}_\mathfrak{p}(\alpha_\mathfrak{p})$ nicht zu einer größeren Ordnung erweitern, und dasselbe gilt dann auch

für $\mathfrak{R}_\mathfrak{p}(\alpha)$. Es ist also $\mathfrak{R}_\mathfrak{p}(\alpha)$ maximal und deshalb die $\mathfrak{p}$-Komponente von $\mathfrak{F}_\alpha$ gleich (1). Man sieht somit, daß der Exponent $r = r_1 + 1$ die erforderliche Eigenschaft besitzt.

Hilfssatz 4 [6]). *Es sei* Z *ein Relativkörper endlichen Grades über* K *und* $\mathfrak{a}$ *ein ganzes Ideal in* K. *Für jeden Primteiler* $\mathfrak{p}$ *von* $\mathfrak{a}$ *sei in* $\mathfrak{J}_\mathfrak{p}$ *eine Zahl* $\alpha_\mathfrak{p}$ *gegeben, die entweder Einheit ist oder für welche* $\mathfrak{F}_{\alpha_\mathfrak{p},\mathfrak{p}} = (1)$ *gilt. Dann gibt es in* $\mathfrak{J}$ *eine Zahl* α, *die erstens für alle diese* $\mathfrak{p}$ *den Kongruenzen*

$$\alpha \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{a}_\mathfrak{p}\mathfrak{J}_\mathfrak{p}}$$

genügt, für die zweitens α *zu* $\mathfrak{F}_\alpha$ *teilerfremd und drittens* $\mathsf{K}(\alpha)$ *eine Erweiterung n-ten Grades von* K *mit* $\mathsf{K}(\alpha) \cap \mathsf{Z} = \mathsf{K}$ *ist.*

Beweis. Es sei zunächst $\mathfrak{q}$ ein zu $\mathfrak{a}$ primes und in Z völlig zerlegtes Primideal von K und $\alpha_\mathfrak{q}$ eine solche Zahl aus $\mathfrak{J}_\mathfrak{q}$, daß $\mathsf{K}_\mathfrak{q}(\alpha_\mathfrak{q})$ eine Erweiterung n-ten Grades von $\mathsf{K}_\mathfrak{q}$ ist. Dann sei α_1 eine Zahl aus $\mathfrak{J}$, welche die Kongruenzen

$$\alpha_1 \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{a}_\mathfrak{p}^{r_\mathfrak{p}}\mathfrak{J}_\mathfrak{p}}, \qquad \alpha_1 \equiv \alpha_\mathfrak{q} \pmod{\mathfrak{q}^h\mathfrak{J}_\mathfrak{q}}$$

befriedigt, wobei h und die $r_\mathfrak{p}$ die nach den Hilfssätzen 2 und 3 existierenden Exponenten sind, so daß erstens $\mathsf{K}_\mathfrak{q}(\alpha_1)$ eine Erweiterung n-ten Grades von $\mathsf{K}_\mathfrak{q}$ ist und zweitens $\mathfrak{F}_{\alpha_1,\mathfrak{p}} = (1)$ gilt, falls $\mathfrak{F}_{\alpha_\mathfrak{p},\mathfrak{p}} = (1)$ ist. $\mathsf{K}(\alpha_1)$ ist dann auch eine Erweiterung n-ten Grades von K, und weil $\mathfrak{q}$ in Z völlig zerlegt, dagegen in $\mathsf{K}(\alpha_1)$ höchstens in gleiche Primfaktoren zerspalten wird (denn sonst könnte $\mathsf{K}_\mathfrak{q}(\alpha_1)$ nicht eine Erweiterung n-ten Grades von $\mathsf{K}_\mathfrak{q}$ sein), so haben $\mathsf{K}(\alpha_1)$ und Z außer den Zahlen von K keine weiteren gemeinsam.

Jetzt zerlegen wir den Führer $\mathfrak{F}_{\alpha_1}$ von $\mathfrak{R}(\alpha_1) \cap \mathfrak{J}$ in ein Produkt

$$\mathfrak{F}_{\alpha_1} = \mathfrak{F}_1\mathfrak{F}_2,$$

wobei alle Primteiler von $\mathfrak{F}_1$ in $\mathfrak{a}$ aufgehen, dagegen $\mathfrak{F}_2$ zu $\mathfrak{a}$ teilerfremd ist. Weiterhin seien f_1, f_2 zwei Zahlen aus K, deren erste in $\mathfrak{a}n\mathfrak{F}_1$, und deren zweite in $n\mathfrak{F}_2$ enthalten ist, und für die

$$f_1 + f_2 = 1$$

gilt. Wird nun

$$\alpha = \alpha_1 f_2 + f_1$$

gesetzt, so ist α die Zahl, deren Existenz zu zeigen ist: Es ist nämlich erstens für alle $\mathfrak{p}$, die $\mathfrak{a}$ teilen,

$$\alpha \equiv \alpha_1 \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{a}_\mathfrak{p}\mathfrak{J}_\mathfrak{p}}.$$

Zweitens ist $\mathsf{K}(\alpha) = \mathsf{K}(\alpha_1)$, also auch $\mathfrak{F}_\alpha = \mathfrak{F}_{\alpha_1}$. Ein etwa vorhandener gemeinsamer Primteiler $\mathfrak{P}$ von α und $\mathfrak{F}_\alpha$ könnte offenbar nicht in $\mathfrak{F}_2$ aufgehen. Ginge $\mathfrak{P}$ aber in $\mathfrak{F}_1$ auf, so auch in $\mathfrak{a}$; und bezeichnet $\mathfrak{p}$ das durch $\mathfrak{P}$ teilbare Primideal von K, so könnte wegen

$$\alpha = \alpha_1 f_2 + f_1 \equiv \alpha_1 \equiv \alpha_\mathfrak{p} \pmod{\mathfrak{a}_\mathfrak{p}\mathfrak{J}_\mathfrak{p}}$$

$\alpha_\mathfrak{p}$ keine Einheit sein. Dann wäre aber voraussetzungsgemäß $\mathfrak{F}_{\alpha_\mathfrak{p},\mathfrak{p}} = (1)$, und, wie schon oben für diesen Fall festgestellt wurde, $\mathfrak{F}_{\alpha,\mathfrak{p}} = \mathfrak{F}_{\alpha_1,\mathfrak{p}} = (1)$. Folglich können α und $\mathfrak{F}_\alpha$ keinen gemeinsamen Primteiler besitzen. Drittens ist

$$\mathsf{K}(\alpha) \cap \mathsf{Z} = \mathsf{K}(\alpha_1) \cap \mathsf{Z} = \mathsf{K},$$

und damit ist der Hilfssatz 4 bewiesen.

---

[6]) Auf diesen Hilfssatz und seine Eignung zum Beweise des behaupteten Klassenzahltheorems hat mich Herr Chevalley hingewiesen.

Hilfssatz 5. *Ist* $\mathfrak{M}$ *ein ganzes Ideal der Linksordnung* $\mathfrak{J}$, *das zur Diskriminante* $\mathfrak{d}$ *von* $\mathfrak{J}$ *teilerfremd ist, so kann man für jeden Primteiler* $\mathfrak{p}$ *von* $n\mathfrak{M}$ *ein Element* $\mu_\mathfrak{p}$ *in* $\mathfrak{J}_\mathfrak{p}$ *derart finden, daß erstens*

$$\mathfrak{M}_\mathfrak{p} = \mathfrak{J}\mu_\mathfrak{p},$$

zweitens $\mathsf{K}_\mathfrak{p}(\mu_\mathfrak{p})$ *direkte Summe von* n *einfachen Systemen und drittens* $\mathfrak{F}_{\mu_\mathfrak{p},\mathfrak{p}} = (1)$ *ist.*

Beweis. Unter der Voraussetzung, daß $\mathfrak{p}$ die Diskriminante $\mathfrak{d}$ von $\mathfrak{J}$ nicht teilt, kann man $\mathfrak{J}_\mathfrak{p}$ bekanntlich als die Ordnung aller n-reihigen Matrizen mit ganzen Koeffizienten aus $\mathsf{K}_\mathfrak{p}$ darstellen. Alle Ideale sind Hauptideale, es ist also

$$\mathfrak{M}_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\mu,$$

wobei μ eine Matrix aus $\mathfrak{J}_\mathfrak{p}$ ist. Jetzt gibt es zwei Einheiten ε, η in $\mathfrak{J}_\mathfrak{p}$ derart [7]), daß

$$\eta\mu\varepsilon = \begin{pmatrix} m_1 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & m_n \end{pmatrix}$$

eine Diagonalmatrix ist, wobei alle m_i voneinander verschieden sind, und dann gilt

$$\mathfrak{M}_\mathfrak{p}\varepsilon = \mathfrak{J}_\mathfrak{p} \begin{pmatrix} m_1 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & m_n \end{pmatrix}$$

und

$$\mathfrak{M}_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\varepsilon \begin{pmatrix} m_1 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & m_n \end{pmatrix} \varepsilon^{-1}.$$

Wird

$$\mu_\mathfrak{p} = \varepsilon \begin{pmatrix} m_1 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & m_n \end{pmatrix} \varepsilon^{-1}, \quad \nu = \begin{pmatrix} m_1 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & m_n \end{pmatrix}$$

gesetzt, so sind $\mathsf{K}_\mathfrak{p}(\mu_\mathfrak{p})$ und $\mathsf{K}_\mathfrak{p}(\nu)$ isomorph. Letzteres System ist die direkte Summe von n einfachen Systemen, dasselbe gilt daher auch für $\mathsf{K}_\mathfrak{p}(\mu_\mathfrak{p})$. Nun ist $\mathfrak{R}_\mathfrak{p}(\nu)$ in $\mathfrak{J}_\mathfrak{p}$ enthalten, und weil ε Einheit ist, ist auch

$$\mathfrak{R}_\mathfrak{p}(\mu_\mathfrak{p}) = \varepsilon\mathfrak{R}_\mathfrak{p}(\nu)\varepsilon^{-1}$$

in $\mathfrak{J}_\mathfrak{p}$ enthalten. Daher ist $\mathfrak{F}_{\mu_\mathfrak{p},\mathfrak{p}} = (1)$, was zu beweisen war.

Hilfssatz 6. *Es sei* $\mathfrak{p} = (p)$ *ein Hauptprimideal von* K, *welches die Diskriminante* $\mathfrak{d}$ *von* $\mathfrak{J}$ *nicht teilt. Sind* $\mathfrak{P}$ *und* $\mathfrak{P}'$ *zwei ganze Ideale der Linksordnung* $\mathfrak{J}$ *und derselben Norm*

$$n\mathfrak{P} = n\mathfrak{P}' = \mathfrak{p},$$

so gibt es in $\mathfrak{J}$ *eine solche Zahl* τ, *daß*

$$\mathfrak{P}_\mathfrak{p} = \tau^{-1}\mathfrak{P}'_\mathfrak{p}\tau$$

und p *modulo jeder Potenz von* $(n(\tau))$ *ein* n*-ter Potenzrest ist.*

Beweis. Es sei nach Hilfssatz 5

$$\mathfrak{P}'_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\pi'_\mathfrak{p},$$

wobei $\mathsf{K}_\mathfrak{p}(\pi'_\mathfrak{p})$ direkte Summe von n einfachen Systemen ist. Bekanntlich gibt es eine Einheit ε in $\mathfrak{J}_\mathfrak{p}$, für welche

$$\mathfrak{P}_\mathfrak{p} = \varepsilon^{-1}\mathfrak{P}'_\mathfrak{p}\varepsilon$$

[7]) Vgl. hierzu H. Hasse, Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Math. Ann. **104** (1931), S. 495, besonders S. 524.

gilt [7]). $n(\varepsilon)$ ist eine Einheit von $\mathsf{K}_\mathfrak{p}$ und daher die Norm einer Einheit ϑ von $\mathsf{K}_\mathfrak{p}(\pi_\mathfrak{p}')$; dann ist $n(\vartheta^{-1}\varepsilon) = 1$ und

$$\mathfrak{P}_\mathfrak{p} = (\vartheta^{-1}\varepsilon)^{-1}\mathfrak{P}_\mathfrak{p}'(\vartheta^{-1}\varepsilon).$$

Es macht deshalb nichts aus, wenn gleich von vornherein $n(\varepsilon) = 1$ angenommen wird.

Jetzt bezeichne Z den kleinsten relativgaloisschen durch $\sqrt[n]{p}$ über K erzeugten Zahlkörper und $\mathfrak{h}$ den Führer des größten relativabelschen Unterkörpers Z' von Z. Ferner durchlaufe $\mathfrak{r}$ alle von $\mathfrak{p}$ verschiedenen Primteiler von $\mathfrak{h}$. Dann existiert nach Hilfssatz 4 eine den Kongruenzen

$$\sigma \equiv \varepsilon \pmod{\mathfrak{p}\mathfrak{h}_\mathfrak{p}\mathfrak{F}_\mathfrak{p}}, \quad \sigma \equiv 1 \pmod{\mathfrak{h}_\mathfrak{r}\mathfrak{F}_\mathfrak{r}}$$

genügende Zahl σ in $\mathfrak{F}$ mit den Eigenschaften

$$(\mathsf{K}(\sigma) : \mathsf{K}) = n, \quad \mathsf{K}(\sigma) \cap \mathsf{Z} = \mathsf{K}, \quad (\sigma, \mathfrak{F}_\sigma) = (1).$$

Es ist wegen $n(\varepsilon) = 1$

$$n(\sigma) \equiv 1 \pmod{\mathfrak{h}},$$

daher gehört $(n(\sigma))$ zu der Idealgruppe, für die Z' Klassenkörper ist, und wegen $\mathsf{K}(\sigma) \cap \mathsf{Z} = \mathsf{K}$ gehört (σ) zu der Idealgruppe von $\mathsf{K}(\sigma)$, für welche $\mathsf{K}(\sigma)\mathsf{Z}'$ Klassenkörper ist. Wir betrachten nun die Strahlklassen in $\mathsf{K}(\sigma)$ mod $\mathfrak{F}_\sigma\mathfrak{h}\mathfrak{p}$: Es sei Γ der Strahlklassenkörper zu diesem Führer, er umfaßt $\mathsf{K}(\sigma)\mathsf{Z}'$, und Γ ist Klassenkörper zu einer Idealgruppe H in $\mathsf{K}(\sigma)\mathsf{Z}'$, die mod $\mathfrak{F}_\sigma\mathfrak{h}\mathfrak{p}$ erklärbar ist. Jetzt ist

$$\mathsf{K}(\sigma)\mathsf{Z} \cap \Gamma = \mathsf{K}(\sigma)\mathsf{Z}',$$

daher ist die Gruppe von $\mathsf{K}(\sigma)\mathsf{Z}\Gamma/\mathsf{K}(\sigma)\mathsf{Z}'$ gleich dem direkten Produkt der Gruppen von $\mathsf{K}(\sigma)\mathsf{Z}/\mathsf{K}(\sigma)\mathsf{Z}'$ und $\Gamma/\mathsf{K}(\sigma)\mathsf{Z}'$. Bezeichnet K irgendeine Idealklasse von $\mathsf{K}(\sigma)\mathsf{Z}'$ mod H und $\varkappa$ die im Sinne der Klassenkörpertheorie zu K gehörige Substitution der galoisschen Gruppe von $\Gamma/\mathsf{K}(\sigma)\mathsf{Z}'$, so gibt es nach dem Existenzsatze von Tschebotarew unendlich viele Primideale ersten Grades, deren Artinsymbol für die Gruppe von $\mathsf{K}(\sigma)\mathsf{Z}\Gamma/\mathsf{K}(\sigma)\mathsf{Z}'$ gleich der durch $\varkappa$ erzeugten Klasse $\langle\varkappa\rangle$ ausfällt. Weil die Gruppe von $\mathsf{K}(\sigma)\mathsf{Z}\Gamma/\mathsf{K}(\sigma)\mathsf{Z}'$ gleich dem direkten Produkt der Gruppen von $\Gamma/\mathsf{K}(\sigma)\mathsf{Z}'$ und $\mathsf{K}(\sigma)\mathsf{Z}/\mathsf{K}(\sigma)\mathsf{Z}'$ ist, müssen diese Primideale in der Klasse K enthalten sein und in $\mathsf{K}(\sigma)\mathsf{Z}/\mathsf{K}(\sigma)\mathsf{Z}'$ völlig zerlegt werden.

Es sei jetzt (σ') ein Primideal aus $\mathsf{K}(\sigma)$, das der Kongruenz

$$\sigma' \equiv \sigma \pmod{\mathfrak{F}_\sigma\mathfrak{h}\mathfrak{p}}$$

genügt. Es ist zu $\mathfrak{h}$ prim und gehört wie (σ) zu der Idealgruppe, für die $\mathsf{K}(\sigma)\mathsf{Z}'$ Klassenkörper ist, deshalb wird (σ') in $\mathsf{K}(\sigma)\mathsf{Z}'/\mathsf{K}(\sigma)$ völlig zerlegt. $\mathfrak{S}$ sei ein Primteiler von (σ') in $\mathsf{K}(\sigma)\mathsf{Z}'$. Dann gibt es nach dem oben Bemerkten ein Primideal $\mathfrak{T}$ ersten Grades, das derselben Idealklasse mod H wie $\mathfrak{S}$ angehört, und das in $\mathsf{K}(\sigma)\mathsf{Z}/\mathsf{K}(\sigma)\mathsf{Z}'$ völlig zerlegt wird. Die Norm von $\mathfrak{T}$ in Bezug auf $\mathsf{K}(\sigma)$ gehört zu derselben Strahlklasse mod $\mathfrak{F}_\sigma\mathfrak{h}\mathfrak{p}$ wie die von $\mathfrak{S}$, sie ergibt also ein Hauptideal (τ) mit $\tau \equiv \sigma' \equiv \sigma \pmod{\mathfrak{F}_\mathfrak{p}\mathfrak{h}\mathfrak{p}}$. Da $\mathfrak{T}$ Primideal ersten Grades sein sollte, so sind auch (τ) bzw. $(n(\tau))$ Primideale ersten Grades in $\mathsf{K}(\sigma)$ bzw. K, und weil (τ) in $\mathsf{K}(\sigma)\mathsf{Z}/\mathsf{K}(\sigma)$ völlig zerlegt wird, wird auch $(n(\tau))$ in Z/K völlig zerlegt, und dann ist p mod $(n(\tau))$ ein n-ter Potenzrest. Wird nun $\mathfrak{T}$ und damit auch $(n(\tau))$ zu p und n prim angenommen, was nach Obigem die Allgemeinheit nicht beeinträchtigt, so ist p auch modulo jeder Potenz von $(n(\tau))$ ein n-ter Potenzrest.

Andererseits ist $\mathsf{K}(\tau) = \mathsf{K}(\sigma)$, also $\mathfrak{R}(\tau) = \mathfrak{R}(\sigma)$ und $\mathfrak{F}_\tau = \mathfrak{F}_\sigma$, und es gilt

$$\tau \equiv \sigma \pmod{\mathfrak{F}_\tau};$$

τ ist daher, ebenso wie σ, in $\mathfrak{R}(\tau) \cap \mathfrak{F}$, also in $\mathfrak{F}$ enthalten. Weiterhin gilt

$$\tau \equiv \sigma \equiv \varepsilon \pmod{\mathfrak{p}\mathfrak{F}_\mathfrak{p}},$$

und aus dem Grunde ist

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

Der Hilfssatz 6 ist damit bewiesen.

3. Nunmehr kann zu dem Beweis des Satzes 1 geschritten werden. Wir zeigen zunächst, daß die in ihm genannte Bedingung notwendig ist.

Ist nämlich

$$\mathfrak{M} = \mathfrak{J}\mu$$

ein Hauptideal, und genügt μ in K einer irreduziblen Gleichung n-ten Grades, so ist $K(\mu)$ ein Zerfällungskörper von $\mathfrak{A}$, und aus dem Grunde ist

$$n(\mu) \equiv 1 \pmod{\mathfrak{u}}.$$

$n\mathfrak{M}$ gehört also zum Strahl mod $\mathfrak{u}$. Genügt aber μ nicht einer irreduziblen Gleichung n-ten Grades in K, so gilt

$$n(\mu) \equiv 1 \pmod{\mathfrak{u}}$$

trotzdem. Denn ist $\alpha_1, \alpha_2, \ldots, \alpha_m$ eine K-Basis von $\mathfrak{A}$, so kann man nach dem Irreduzibilitätssatze von Hilbert den unabhängigen Variablen $x_1, x_2, \ldots, x_m$ solche Werte in K erteilen, daß die Hauptgleichungen von

$$\xi = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m \quad \text{und} \quad \mu\xi$$

in K irreduzibel sind, und dann gilt nach Obigem

$$n(\mu) \equiv n(\mu\xi) \equiv 1 \pmod{\mathfrak{u}}.$$

4. Es sei jetzt $\mathfrak{M}$ ein ganzes Ideal von $\mathfrak{A}$ mit der Linksordnung $\mathfrak{J}$, dessen Norm zum Strahl mod $\mathfrak{u}$ gehört:

$$n\mathfrak{M} = (m), \qquad m \equiv 1 \pmod{\mathfrak{u}}.$$

Wenn bewiesen werden soll, daß $\mathfrak{M}$ Hauptideal ist, braucht dasselbe nur für irgendein Ideal

$$\mathfrak{P} = \mu\mathfrak{M}^{-1}$$

gezeigt zu werden. Diese Tatsache gestattet es uns, den Beweis für die Hauptidealeigenschaft auf einen einfachen Spezialfall zu reduzieren.

$\mathfrak{J} = \mathfrak{J}_1, \mathfrak{J}_2, \ldots, \mathfrak{J}_h$ sei ein Repräsentantensystem aller Typen von Maximalordnungen. Es sei speziell so ausgewählt, daß die Distanzideale $(\mathfrak{J} \times \mathfrak{J}_i)^{-1}$ zu $n\mathfrak{M} = (m)$ und zur Diskriminante $\mathfrak{d}$ von $\mathfrak{J}$ prime Normen haben; diese Bedingung kann deshalb stets erfüllt werden, weil bekanntlich jede Idealklasse Ideale enthält, deren Normen zu einem gegebenen Zentrumsideal teilerfremd sind. Nun gibt es eine zu (m) und zu $\mathfrak{d}$ prime Zahl a in K, die durch die Normen aller Distanzen $(\mathfrak{J} \times \mathfrak{J}_i)^{-1}$ teilbar ist, und sie hat die Eigenschaft, daß für jedes $i = 1, 2, \ldots, h$

$$a\mathfrak{J}_i < \mathfrak{J}$$

gilt. Weiterhin sei $\mu_\mathfrak{p}$ für jeden Primteiler $\mathfrak{p}$ von $n\mathfrak{M}$ eine Zahl mit den im Hilfssatz 5 angegebenen Eigenschaften, und für jeden Primteiler $\mathfrak{p}$ von a sei

$$\mu_\mathfrak{p} = \begin{pmatrix} 1 & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & 1 \\ 0 & & & m \end{pmatrix},$$

wenn $\mathfrak{J}_\mathfrak{p}$ als die Ordnung aller n-reihigen Matrizen mit ganzen Koeffizienten aus $K_\mathfrak{p}$ dargestellt wird.

Wird nun $\mathfrak{a} = (m^2 a^n)$ gesetzt, so sind alle Bedingungen des Hilfssatzes 4 erfüllt, und es gibt daher in $\mathfrak{J}$ eine Zahl μ_1, die in K einer irreduziblen Gleichung n-ten Grades genügt, und für die

$$\mu_1 \equiv \mu_\mathfrak{p} \pmod{\mathfrak{a}_\mathfrak{p}\mathfrak{J}_\mathfrak{p}}, \quad (\mu_1, \mathfrak{F}_{\mu_1}) = (1)$$

gilt. Es ist $\frac{n(\mu_1)}{n\mathfrak{M}}$ ganz und zu $an\mathfrak{M}$ prim, daher wird (μ_1) in $K(\mu_1)$ in ein Produkt zweier Ideale zerlegt:

$$(\mu_1) = \mathfrak{M}_1\mathfrak{N}_1,$$

wobei $n\mathfrak{M}_1 = n\mathfrak{M}$ und $\mathfrak{N}_1$ zu $\mathfrak{F}_{\mu_1} an\mathfrak{M}$ prim ist. Nun werde in $K(\mu_1)$ nach dem Satz von der arithmetischen Progression ein zu $\mathfrak{d}$ teilerfremdes Primideal $\mathfrak{P}_1$ ersten Grades bestimmt, welches die Kongruenz

$$\mathfrak{P}_1 \equiv \mathfrak{N}_1 \pmod{\mathfrak{F}_{\mu_1} a^n n\mathfrak{M}}$$

befriedigt. Es ist

$$\mathfrak{M}_1\mathfrak{P}_1 = (\mu)$$

und

$$\mu \equiv \mu_1 \pmod{\mathfrak{F}_{\mu_1} a^n n\mathfrak{M}}.$$

Insbesondere ist $\mu \equiv \mu_1 \pmod{\mathfrak{F}_{\mu_1}}$, deswegen liegt μ, ebenso wie μ_1, in $\mathfrak{J}$ und wegen $\mu \equiv \mu_1 \pmod{n\mathfrak{M}}$ sogar in $\mathfrak{M}$. Daher ist

$$\mathfrak{P} = \mu\mathfrak{M}^{-1}$$

ein ganzes Ideal, seine Norm ist

$$n\mathfrak{P} = n\mathfrak{P}_1 = (p) = \left(\frac{n(\mu)}{m}\right).$$

Nach **3** gehört sie wie $n\mathfrak{M}$ zum Strahl mod $\mathfrak{u}$. (p) ist Primideal ersten Grades, weil $\mathfrak{P}_1$ ein Primideal ersten Grades ist. Und schließlich gilt für jedes in a aufgehende Primideal $\mathfrak{p}$

$$p = \frac{n(\mu)}{m} \equiv \frac{n(\mu_1)}{m} \equiv \frac{n(\mu_\mathfrak{p})}{m} = 1 \pmod{a_\mathfrak{p}^n},$$

also

$$p \equiv 1 \pmod{a^n}.$$

Das so konstruierte Ideal $\mathfrak{P}$ kann nun als Hauptideal nachgewiesen werden; es werde dazu $\mathfrak{M}$ durch $\mathfrak{P}$ ersetzt. Die Maximalordnungen $\mathfrak{J} = \mathfrak{J}_1, \mathfrak{J}_2, \ldots, \mathfrak{J}_h$ und die Zahl a mögen die oben erklärte Bedeutung behalten. Ferner seien $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \ldots$ alle Ideale der Norm (p) und der Linksordnung $\mathfrak{J}$:

$$n\mathfrak{P} = n\mathfrak{P}' = n\mathfrak{P}'' = \cdots = (p) = \mathfrak{p}$$

und $\tau', \tau'', \ldots$ solche nach Hilfssatz 6 existierenden Zahlen aus $\mathfrak{J}$, daß

$$\mathfrak{P}_\mathfrak{p} = \tau'^{-1}\mathfrak{P}'_\mathfrak{p}\tau' = \tau''^{-1}\mathfrak{P}''_\mathfrak{p}\tau'' = \cdots$$

gilt, und daß p modulo jeder Potenz von $(n(\tau'))$, $(n(\tau''))$, $\ldots$ ein n-ter Potenzrest wird. Es werde

$$n(\tau')n(\tau'')\cdots = b, \quad ab = c$$

geschrieben. Dann ist p ein n-ter Potenzrest mod c^n, d. h. es gibt eine ganze Zahl t in K, welche die Kongruenz

$$p \equiv t^n \pmod{c^n}$$

befriedigt.

Da p zu $\mathfrak{d}$ prim ist, ist p für jeden Primteiler $\mathfrak{q}$ von $\mathfrak{d}$ die Norm einer ganzen Zahl aus dem unverzweigten Relativkörper n-ten Grades über $K_\mathfrak{q}$; infolgedessen gibt es für jedes dieser $\mathfrak{q}$ ein Polynom

$$g_\mathfrak{q}(x) = x^n + a_{1,\mathfrak{q}}x^{n-1} + \cdots + a_{n-1,\mathfrak{q}}x + (-1)^n p$$

mit ganzen Koeffizienten aus $K_\mathfrak{q}$, welches in $K_\mathfrak{q}$ irreduzibel ist. $h_\mathfrak{q}$ bezeichne solche nach Hilfssatz 1 existierenden Exponenten, daß jedes Polynom, welches $g_\mathfrak{q}(x)$ mod $\mathfrak{q}^{h_\mathfrak{q}}$ kongruent ist, in $K_\mathfrak{q}$ ebenfalls irreduzibel ist.

Nun kann man ein Polynom

$$g(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + (-1)^n p$$

mit ganzen Koeffizienten aus K konstruieren, welches den Kongruenzen

$$g(x) \equiv g_\mathfrak{q}(x) \pmod{\mathfrak{q}^{h_\mathfrak{q}}} \quad \text{für alle } \mathfrak{q} \mid \mathfrak{d},$$

$$g(x) \equiv (x - t)^n \pmod{c^n}$$

genügt.

Wenn $\mathfrak{u} = (1)$ ist, d. h. wenn $\mathfrak{A}$ keine unendlichen Verzweigungsprimstellen besitzt, so erzeugt jetzt eine Wurzel von $g(x) = 0$ einen Zerfällungskörper von $\mathfrak{A}$. Infolgedessen [8]) enthält $\mathfrak{A}$ eine Wurzel π von $g(x) = 0$. Nun ist $\frac{\pi - t}{c}$ eine ganze Zahl; ohne Beschränkung der Allgemeinheit darf vorausgesetzt werden, daß sie in einer der Maximalordnungen $\mathfrak{J}_1, \mathfrak{J}_2, \ldots, \mathfrak{J}_n$ liegt. Dann ist $a\frac{\pi - t}{c} = \frac{\pi - t}{b} = \nu$ und mithin auch π in $\mathfrak{J}$ enthalten. Wegen $n(\pi) = p$ ist jetzt $\mathfrak{J}\pi$ ein ganzes Ideal der Norm (p). Wäre $\mathfrak{J}\pi = \mathfrak{P}$, so wäre $\mathfrak{P}$ bereits als Hauptideal nachgewiesen. Sonst ist jedenfalls $\mathfrak{J}\pi$ einem der Ideale $\mathfrak{P}', \mathfrak{P}'', \ldots$ gleich, es sei etwa $\mathfrak{J}\pi = \mathfrak{P}'$. Dann ist

$$\mathfrak{P}_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\tau'^{-1}\pi\tau'.$$

Es ist aber

$$\tau'^{-1}\pi\tau' = b\tau'^{-1}\nu\tau' + t,$$

und weil b durch $n(\tau')$ teilbar ist und τ' und ν in $\mathfrak{J}$ enthalten sind, liegt auch $\tau'^{-1}\pi\tau'$ in $\mathfrak{J}$. Dann ist aber

$$\mathfrak{P} = \mathfrak{J}\tau'^{-1}\pi\tau',$$

und der Beweis des Satzes 1 ist erbracht.

Ist aber $\mathfrak{u} \neq (1)$, und das kann nur für gerades n eintreten, so müssen die Fälle $n > 2$ und $n = 2$ getrennt behandelt werden. Es werde zunächst $n > 2$ angenommen. Dann ist $g(x)$ wegen $p = (-1)^n p \equiv 1 \pmod{\mathfrak{u}}$ für grosse negative und positive x sowie für $x = 0$ positiv an allen zu $\mathfrak{u}$ gehörigen unendlichen Primstellen. Man kann nun eine ganze und rationale Zahl A, die durch alle $\mathfrak{q}^{h_\mathfrak{q}}$ und durch c^n teilbar ist, derart bestimmen, daß

$$g_1(x) = g(x) + Ax^2$$

für alle reellen x positiv an allen zu $\mathfrak{u}$ gehörigen unendlichen Primstellen wird. Dann erzeugt eine Wurzel von $g_1(x) = 0$ einen Zerfällungskörper von $\mathfrak{A}$, und man kann jetzt den Beweis dadurch zu Ende führen, daß man $g(x)$ durch $g_1(x)$ ersetzt.

---

[8]) H. Hasse, Theory of cyclic algebras over an algebraic number field, Transactions Amer. Math. Soc. **34** (1932), S. 171, Satz (II. 2).

5. Ist zweitens $n = 2$,

$$g(x) = x^2 + ex + p,$$

und kann man eine ganze Zahl e_1 in K derart finden, daß

$$e_1 \equiv e \pmod{\mathfrak{q}^{h_\mathfrak{q}}} \quad \text{für alle } \mathfrak{q} \mid \mathfrak{d},$$
$$e_1 \equiv e \pmod{c^n}$$

gilt, und daß $e_1^2 - 4p$ an allen zu u gehörigen unendlichen Primstellen negativ wird, so liefert eine Wurzel von

$$g_1(x) = x^2 + e_1 x + p = 0$$

einen Zerfällungskörper von $\mathfrak{A}$, und man braucht oben nur $g(x)$ durch $g_1(x)$ zu ersetzen, um den Beweis zu Ende zu führen.

Wenn u nicht alle unendlichen Primstellen von K umfaßt, so kann eine Zahl e_1 mit den genannten Eigenschaften in der Tat gefunden werden. Um dies zu zeigen, seien die Konjugierten zu einer Zahl z aus K mit $z^{(1)}, z^{(2)}, \ldots, z^{(m)}$ bezeichnet, und zwar mit $z^{(1)}, z^{(2)}, \ldots, z^{(k)}$ speziell diejenigen, die zu den unendlichen Verzweigungsprimstellen von $\mathfrak{A}$ gehören. Wird unter A schließlich eine ganze und rationale, durch alle $\mathfrak{q}^{h_\mathfrak{q}}$ und durch c^n teilbare Zahl verstanden, so kann man die Existenz einer solchen Zahl e_1 aus dem nachstehenden Hilfssatz entnehmen:

Hilfssatz 7. *e sei irgendeine Zahl aus* K *und* $A > 0$ *eine rationale*; $e^{(1)}, e^{(2)}, \ldots, e^{(k)}$ *seien zu e konjugierte Zahlen, die in reellen zu* K *konjugierten Körpern liegen mögen. Ausgenommen in dem Falle, wo k gleich dem Grad m des Körpers* K *ist, gibt es ganze Zahlen y in* K *derart, daß die Beträge der Differenzen* $e_1^{(i)} = e^{(i)} - Ay^{(i)}$ $(i = 1, 2, \ldots, k)$ *unter beliebig vorgegebenen Schranken* ε_i *liegen*:

$$|e^{(i)} - Ay^{(i)}| < \varepsilon_i.$$

Beweis. Es gibt in K gewiß eine ganze Zahl w, für die $|w^{(1)}|$ kleiner als $\frac{\varepsilon_1}{A}$ angenommen werden darf. Dann ist

$$\left| e^{(1)} - A\left[\frac{e^{(1)}}{Aw^{(1)}}\right] w^{(1)} \right| = |e^{(1)} - Ay^{(1)}| < \varepsilon_1,$$

der Hilfssatz 7 gilt mithin für $k = 1$ [9]). Er werde bereits für $k - 1$ als richtig angenommen. Dann gibt es eine ganze Zahl z in K, die den Ungleichungen

$$|e^{(i)} - Az^{(i)}| < \frac{\varepsilon_i}{2} \qquad (i = 1, 2, \ldots, k-1)$$

genügt. Ist nun $\left[\frac{e^{(k)} - Az^{(k)}}{\varepsilon_k}\right] = 0$, so ist auch schon

$$|e^{(k)} - Az^{(k)}| < \varepsilon_k,$$

und es hat z die erforderliche Eigenschaft; sonst ist für jede reelle Zahl $T \geqq 1$ auch

$$\left[T\frac{e^{(k)} - Az^{(k)}}{\varepsilon_k}\right] \neq 0.$$

Jetzt existiert nach dem Hilfssatz von Minkowski über homogene Linearformen eine ganze Zahl v in K, die den Ungleichungen

---

[9]) Für positives reelles T bedeute $[T]$ die größte natürliche Zahl, die kleiner oder gleich T ist, und es gelte $[-T] = -[T]$.

$$|v^{(i)}| < \frac{\varepsilon_i}{2A} \frac{1}{\left[|\sqrt{D}| \frac{e^{(k)} - Az^{(k)}}{\varepsilon_k}\right]} = \eta_i \quad (i = 1, 2, \ldots, k-1),$$

$$|v^{(k)}| < \frac{\varepsilon_k}{A} = \eta_k,$$

$$|v^{(i)}| < \eta_i \qquad (i = k+1, \ldots, m)$$

genügt, wenn D die Diskriminante von K bezeichnet und die $\eta_{k+1}, \ldots, \eta_m$ so angenommen werden, daß

$$\prod_{i=1}^{m} \eta_i = |\sqrt{D}|$$

ist (für konjugiert komplexe $v^{(i)}$ müssen die Schranken η_i gleich sein). Es ist $1 \leqq \prod_{i=1}^{m} |v^{(i)}|$,

$$|v^{(k)}| \geqq \left| \frac{1}{v^{(1)} \ldots v^{(k-1)} v^{(k+1)} \ldots v^{(m)}} \right| > \frac{1}{\eta_1 \ldots \eta_{k-1} \eta_{k+1} \ldots \eta_m} = \frac{\eta_k}{|\sqrt{D}|} = \frac{\varepsilon_k}{A|\sqrt{D}|}.$$

Die Zahl

$$y = z + \left[\frac{e^{(k)} - Az^{(k)}}{Av^{(k)}}\right] v$$

besitzt nun die geforderte Eigenschaft: y ist ganz, ferner ist für $i = 1, 2, \ldots, k-1$

$$|e^{(i)} - Ay^{(i)}| \leqq |e^{(i)} - Az^{(i)}| + A\left|\left[\frac{e^{(k)} - Az^{(k)}}{Av^{(k)}}\right] v^{(i)}\right| < \frac{\varepsilon_i}{2} + A\left|\left[|\sqrt{D}| \frac{e^{(k)} - Az^{(k)}}{\varepsilon_k}\right] v^{(i)}\right| < \varepsilon_i$$

und

$$|e^{(k)} - Ay^{(k)}| = \left| e^{(k)} - Az^{(k)} - A\left[\frac{e^{(k)} - Az^{(k)}}{Av^{(k)}}\right] v^{(k)} \right| < \varepsilon_k.$$

Damit ist der Hilfssatz 7 bewiesen.

Eingegangen 30. Mai 1936.