BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

SITZUNGSBERICHTE

JAHRGANG

1956

MÜNCHEN 1956

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN

In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung München

Über ein Fundamentalproblem der Theorie der Einheiten algebraischer Zahlkörper

Von Heinrich-Wolfgang Leopoldt in Erlangen

Vorgelegt von Herrn Otto Haupt am 4. Mai 1956

1. Einleitung: Zur Abrundung der Theorie der Einheiten algebraischer Zahlkörper K ist es notwendig, ein systematisches Verfahren anzugeben, welches ein Grundeinheitensystem *effektiv-rational* – d. h. durch eine beschränkte Anzahl rationaler Operationen, angewandt etwa auf eine Ganzheitsbasis des Körpers – zu bestimmen gestattet. Die vorliegende Note entwickelt ein solches Verfahren für diejenigen Zahlkörper K, welche über dem rationalen Zahlkörper P normal sind mit abelscher Galoisgruppe $\mathfrak{G}_K$. Die Hauptpunkte des Verfahrens werden durch zwei *Endlichkeitssätze* bezeichnet. Wir beschränken uns hier auf einen kurzen zusammenfassenden Bericht. Eine ausführliche Darstellung der Beweise sowie spezieller Ergebnisse für bestimmte Körpertypen wird bei anderer Gelegenheit erfolgen.

2. Reduktion der Aufgabe: Es genügt, reelle Körper K zu betrachten. Die Strukturtheorie der Einheitengruppe E_K (als $\mathfrak{G}_K$-Operatorgruppe) eines solchen Körpers K wurde vom Verfasser in einer früheren Arbeit weitgehend entwickelt (Leopoldt [2]).[1] Sie erlaubt eine weitere Reduktion der Aufgabe. Entscheidend dafür ist der Begriff der *Relativeinheit*[2] eines zyklischen Körpers Z; das sind jene Einheiten von Z, deren Relativnormen in bezug auf alle echten Teilkörper von Z den Wert ± 1 haben. Ist insbesondere der Grad von Z eine Primzahl, so fällt die Relativeinheitengruppe E_Z^* von Z mit der vollen Einheitengruppe E_Z von Z zusammen. Für einen beliebigen abelschen Körper K ist das über

[1] Siehe Lit.-Verz.

[2] Auf die Unterscheidung von eigentlichen und uneigentlichen Relativeinheiten gehen wir hier nicht ein. Auch ist die Bezeichnungsweise gegenüber [2] vereinfacht.

alle zyklischen Teilkörper Z von K erstreckte Produkt E^{K} der E_{Z}^{*} über $\{\pm 1\}$ direkt,

$$E^{\mathsf{K}} = \operatorname*{dir}_{\pm 1} \prod_{\mathsf{Z} \leq \mathsf{K}} E_{\mathsf{Z}}^{*}, \tag{1}$$

und von endlichem Index Q_{K} in der vollen Einheitengruppe E_{K} von K. Für die Faktorgruppe $E_{\mathsf{K}}/E^{\mathsf{K}}$ kommen nur beschränkt viele, vom Typus von $\mathfrak{G}_{\mathsf{K}}$ abhängende Möglichkeiten in Betracht: Ihr Exponent ist ein Teiler des Körpergrades $g = (\mathsf{K} : \mathsf{P})$, ihre Ordnung ein Teiler von g^{g}. Daher und wegen (1) genügt es, zur Erreichung des Ziels dieser Note ein systematisches Verfahren zur effektiv-rationalen Bestimmung eines *Relativgrundeinheitensystems*, also einer Basis von E_{Z}^{*} für zyklische Körper Z anzugeben.

3. **Endlichkeitssätze:** Wir setzen daher für das Weitere voraus: K sei ein reeller zyklischer Zahlkörper vom Grade $(\mathsf{K} : \mathsf{P}) = g$ (und zwar ohne Einschränkung $g \geq 3$). Eine Erzeugende seiner Galoisgruppe $\mathfrak{G}_{\mathsf{K}}$ sei mit σ_1 bezeichnet. Ferner setzen wir mit der Eulerschen Funktion $\varphi(g) = 2k$. Bedeutet $\phi(x)$ das g-te Kreisteilungspolynom, so sind die Relativeinheiten H von K auch gekennzeichnet durch die Beziehung

$$\mathsf{H}^{\phi(\sigma_1)} = \pm 1, \tag{2}$$

d. h. man darf hier mit σ_1 wie mit einer primitiven g-ten Einheitswurzel rechnen, da es uns auf das Vorzeichen in (2) nicht ankommt. Die Relativeinheitengruppe E_{K}^{*} von K liefert eine ganzzahlige rational-irreduzible treue Darstellung von $\mathfrak{G}_{\mathsf{K}}$, ist also operatorisomorph zu einem Ideal des Körpers P_g der g-ten Einheitswurzeln und hat insbesondere den Rang $\varphi(g) = 2k$. Jede Relativeinheit $\mathsf{H} \neq \pm 1$ von K erzeugt mit (-1) und ihren Konjugierten H^{σ} $(\sigma \in \mathfrak{G}_{\mathsf{K}})$ eine mit $\{\mathsf{H}\}$ bezeichnete Untergruppe von endlichem Index in E_{K}^{*}. Eine solche Gruppe nennen wir $\mathfrak{G}_{\mathsf{K}}$-*zyklisch*, ihren Index nenen wir die *Höhe* von H, und H selbst eine *erzeugende Einheit* dieser Gruppe. Ist $\mathsf{H} \neq \pm 1$ eine feste und E irgendeine andere Relativeinheit von K, so gibt es eine natürliche Zahl m und ein ganzzahliges Polynom $P(x)$ derart, daß mit passendem Vorzeichen

$$\mathsf{E}^{m} = \pm \mathsf{H}^{P(\sigma_1)} \tag{3}$$

gilt. Fordert man, daß $P(x)$ einen Grad $\leq 2k-1$ hat, und daß der Koeffiziententeiler von $P(x)$ prim zu m ist, so ist dieses *Exponentenpaar* $(m, P(x))$ *von* E *bez.* H durch diese Einheiten eindeutig bestimmt.

Der Ausdruck

$$s(\mathsf{H}) = \text{Spur}(\mathsf{H}^2 + \mathsf{H}^{-2}) \tag{4}$$

ist für $\mathsf{H} \in E_K^*$ stets eine natürliche Zahl und liefert eine „Anordnung" der Relativeinheiten von K. Für jedes positive t gibt es höchstens endlich viele Relativeinheiten H von K mit $s(\mathsf{H}) \leq t$. Die in dieser Anordnung kleinsten Relativeinheiten sind die Einheitswurzeln ± 1 von K; sie gehören zum Wert $s(\pm 1) = 2g$. Jede in dieser Anordnung auf ± 1 unmittelbar folgende Relativeinheit von K wollen wir *s-minimal* nennen. Für gerades g vereinfacht sich die Funktion $s(\mathsf{H})$ zu

$$s(\mathsf{H}) = 2 \cdot \text{Spur}(\mathsf{H}^2), \qquad (\text{für } 2|g) \tag{4'}$$

da dann H^{-2} unter den Konjugierten von H^2 vorkommt.

Eine s-minimale Relativeinheit $\mathsf{H} = \mathsf{E}_0$ von K läßt sich effektiv-rational bestimmen. Eine Schranke für $s_0 = s(\mathsf{E}_0)$ wird z. B. mit Hilfe der Relativkreiseinheit von K erhalten. Der folgende *erste Endlichkeitssatz* gibt Auskunft über den nächsten Schritt:

Satz 1:

Es existiert (und läßt sich effektiv-rational bestimmen) ein endliches, nur von g abhängiges System $\mathfrak{S} = (m_\varrho, P_\varrho(x))_{\varrho=1\ldots r}$ *von Exponentenpaaren mit folgender Eigenschaft:*

In jeder maximalen $\mathfrak{G}_K$*-zyklischen Relativeinheitengruppe eines reellen zyklischen Körpers* K *vom Grade g, welche eine beliebig vorgegebene s-minimale Relativeinheit* E_0 *von* K *enthält, gibt es eine Relativeinheit* E*, welche diese Gruppe erzeugt (also eine Relativeinheit von minimaler Höhe) und deren Exponentenpaar in bezug auf* E_0 *zum System* $\mathfrak{S}$ *gehört.*

Zur Berechnung einer solchen Einheit E aus E_0 hat man also für die endlich vielen Einheiten $\mathsf{E}_0^{P_\varrho(\sigma_1)}$, $\varrho = 1, \ldots r$, zu ent-

scheiden, ob sie jeweils m_ϱ-te Potenzen in K sind oder nicht. Auch dies ist effektiv-rational durchführbar.

Ist nun die Relativeinheitengruppe E_K^* selbst $\mathfrak{G}_\mathsf{K}$-zyklisch, so ist $E_\mathsf{K}^* = \{\mathsf{E}\}$ und man ist fertig. Diese Voraussetzung ist z. B. für alle zyklischen Körper K eines Grades $g \leq 22$ erfüllt. Denn für diese g hat P_g die Klassenzahl 1, so daß E_K^* operatorisomorph zu einem Hauptideal von P_g wird. Ist diese Voraussetzung nicht erfüllt, oder über ihre Gültigkeit nichts bekannt, so setzt der folgende *zweite Endlichkeitssatz* das Verfahren fort:

Satz 2:

Es existiert (und läßt sich effektiv-rational bestimmen) eine endliche, nur von g abhängige Matrix $\mathfrak{M} = (m_{\varkappa\lambda}, P_{\varkappa\lambda}(x))_{\substack{\varkappa = 1,\ldots 2k \\ \lambda = 1,\ldots l}}$ *von Exponentenpaaren mit folgender Eigenschaft: Besitzt die Relativeinheit* E *eines reellen zyklischen Körpers vom Grade g minimale Höhe, so ist genau eine Spalte von* $\mathfrak{M}$ *das Exponentenpaarsystem bezüglich* E *eines Relativgrundeinheitensystems dieses Körpers.*

Um auf dem angegebenen Weg ein Relativgrundeinheitensystem effektiv-rational bestimmen zu können, muß nur ein System $\mathfrak{S}$ und gegebenenfalls eine Matrix $\mathfrak{M}$ bekannt sein. Der folgende Abschnitt zeigt, wie man $\mathfrak{S}$ und $\mathfrak{M}$ erhält.

4. Zur Beweismethode: Wir betrachten den g-dimensionalen reellen Vektorraum $\mathfrak{L}$ mit den Vektoren $\mathfrak{x} = (\ldots x_\sigma \ldots)$, $\sigma \in \mathfrak{G}_\mathsf{K}$. Dort bilden die den Relativeinheiten H von K entsprechenden Vektoren $\mathfrak{x}_\mathsf{H}$ mit den Koordinaten

$$x_\sigma = \log |\mathsf{H}^\sigma| \qquad (\sigma \in \mathfrak{G}_\mathsf{K})$$

ein Gitter $\mathbf{\Gamma}_\mathsf{K}^*$, welches einen $\varphi(g)$-dimensionalen Teilraum $\mathfrak{L}^*$von $\mathfrak{L}$ aufspannt. Setzt man $\mathfrak{x} \cdot \tau = (\ldots x_{\sigma\tau} \ldots)$ für $\tau \in \mathfrak{G}_\mathsf{K}$, so sind nach (2) die $\mathfrak{x} \in \mathfrak{L}^*$ durch

$$(2') \qquad \mathfrak{x} \cdot \phi(\sigma_1) = 0$$

gekennzeichnet. Die Exponentialreihe liefert uns eine Entwicklung

$$(5) \qquad s(\mathsf{H}) = 2 \cdot \sum_{n \geq 0} \frac{2^{2n}}{(2n)!} D_{2n}(\mathfrak{x}_\mathsf{H})^{2n}$$

der anordnenden Funktion s (H) nach den Distanzfunktionen

$$D_{2n}(\mathfrak{x}) = \left(\sum_{\sigma} x_{\sigma}^{2n}\right)^{\frac{1}{2n}}$$

des Raumes $\mathfrak{x}$ bzw. $\mathfrak{x}^*$. Letztere lassen sich durch die einfach zu behandelnde euklidische Länge $D_2(\mathfrak{x}) = \|\mathfrak{x}\|$ abschätzen; es gilt mit $c_n = g^{\frac{1}{2}\left(\frac{1}{n}-1\right)}$ für $\mathfrak{x} \neq \mathfrak{o}$ aus $\mathfrak{x}^*$ und $n > 1$ die Ungleichung

$$c_n \cdot \|\mathfrak{x}\| \leq D_{2n}(\mathfrak{x}) < \sqrt{2k} \cdot c_n \cdot \|\mathfrak{x}\|. \tag{6}$$

Nach (2′) sind die ganzen Elemente von P_g als ganzzahlige Polynome in σ_1 höchstens $(2k-1)$ten Grades eindeutig als Operatoren von $\mathfrak{x}^*$ bzw. Γ_{K}^* erklärbar. Zwei Vektoren $\mathfrak{x}$, $\mathfrak{y}$ aus $\mathfrak{x}^*$ wollen wir *assoziiert* nennen, wenn sie mit einer Einheit ε von P_g in einer Beziehung $\mathfrak{x} = \mathfrak{y} \cdot \varepsilon$ stehen.

Für $k = 1$, also für imaginär-quadratisches P_g, hat jeder Vektor $\mathfrak{x}$ aus $\mathfrak{x}^*$ nur endlich viele Assoziierte. In diesem Falle $k = 1$, oder also $g = 3, 4$ bzw. 6, genügt (6) bereits zum Beweis des scharfen Resultats:

Satz 3:

In einem reellen zyklischen Körper K *vom Grade* $g = 3, 4$ *oder* 6 *wird die Relativeinheitengruppe* E_{K}^* *von* K *von einer Relativeinheit* E, *ihren Konjugierten und* (-1) *erzeugt.* E *ist s-minimal und als Erzeugende durch diese Eigenschaft gekennzeichnet.*

Einen äquivalenten Satz für $g = 3, 4$ benützte H. Hasse zur Relativgrundeinheitenberechnung in diesen Fällen (Hasse [1]).

Wir dürfen weiterhin $k \geq 2$ voraussetzen. Selbst wenn Γ_{K}^* dann $\mathfrak{G}_{\mathsf{K}}$-zyklisch ist, gilt Satz 3 in dieser scharfen Fassung sicher nicht mehr, denn in der Anordnung durch s (H) gibt es beliebig große erzeugende Relativeinheiten. Wir nennen einen Vektor $\mathfrak{x}$ aus $\mathfrak{x}^*$ *reduziert*, wenn er unter Assoziierten minimale Länge besitzt, oder also wenn $\mathfrak{x}$ die unendlich vielen, den Einheiten ε von P_g zugeordneten Ungleichungen

$$\|\mathfrak{x}\| \leq \|\mathfrak{x} \cdot \varepsilon\| \tag{7}$$

befriedigt. Dann gilt das

Lemma: *Es existiert (und läßt sich effektiv-rational bestimmen) eine nur von g abhängige Konstante c mit folgender Eigenschaft: Ist* $\mathfrak{x}$ *aus* $\mathfrak{L}^*$ *reduziert und* α *aus* P_g *ganz, so gilt die Ungleichung:*

$$\|\mathfrak{x}\,\alpha\| > \sqrt[2k]{\frac{N(\alpha)}{c}} \cdot \|\mathfrak{x}\|. \tag{8}$$

Dabei bedeutet $N(\alpha)$ die Norm von α im Körper P_g. Die untere Grenze aller c, welche (8) für alle reduzierten $\mathfrak{x}$ aus $\mathfrak{L}^*$ und alle ganzen α aus P_g erfüllen, sei mit c^* bezeichnet.

Zum allgemeinen Beweis von Satz 1 gehe man aus von dem einer s-minimalen Relativeinheit E_0 zugeordneten Gittervektor $\mathfrak{x}_0$. Weiter sei $\{\mathsf{E}\}$ eine maximale, $\{\mathsf{E}_0\}$ umfassende $\mathfrak{S}_\mathsf{K}$-zyklische Untergruppe von E_K^*. Der E zugeordnete Gittervektor $\mathfrak{x}$ darf als reduzierter Vektor vorausgesetzt werden. Dann ist $\mathfrak{x}_0 = \mathfrak{x} \cdot \gamma$ mit ganzem γ aus P_g, und aus (6) und (8) folgt die Ungleichungskette

$$D_{2n}(\mathfrak{x}\gamma) \geq c_n \|\mathfrak{x}\gamma\| > \sqrt[2k]{\frac{N(\gamma)}{c}}\, c_n \|\mathfrak{x}\| > \sqrt[2k]{\frac{N(\gamma)}{c}} \cdot \frac{1}{\sqrt{2k}}\, D_{2n}(\mathfrak{x}).$$

Für $N(\gamma) \geq c\,(2k)^k$ würde nach (5) daraus $s(\mathsf{E}_0) > s(\mathsf{E})$ folgen im Widerspruch zur Minimaleigenschaft von E_0. Mithin ist zunächst die Norm von γ in P_g beschränkt durch

$$N(\gamma) < c \cdot (2k)^k. \tag{9}$$

Assoziierten Zahlen γ entsprechen assoziierte Vektoren $\mathfrak{x}\,\gamma$ und damit dasselbe $\mathfrak{S}_\mathsf{K}$-zyklische Teilgitter. Durchläuft also γ_ϱ, $\varrho = 1, \ldots r$ ein vollständiges System nicht-assoziierter ganzer Zahlen mit gemäß (9) beschränkter Norm, so erhält man die Exponentenpaare des Systems $\mathfrak{S}$ aus Satz 1 jeweils aus der Darstellung

$$\gamma_\varrho^{-1} = \frac{1}{m_\varrho} \cdot P_\varrho(\sigma_1), \qquad (\varrho = 1, \ldots r). \tag{10}$$

Zum Beweis von Satz 2 sei E eine Relativeinheit von K mit minimaler Höhe, also $\{\mathsf{E}\}$ eine maximale $\mathfrak{S}_\mathsf{K}$-zyklische Untergruppe von E_K^*. Ist $\mathfrak{x}$ der E zugeordnete Gittervektor, so hat das volle Gitter Γ_K^* die Gestalt

$$\Gamma_\mathsf{K}^* = \mathfrak{x} \cdot \left(\frac{1}{\mathfrak{m}}\right). \tag{11}$$

Dabei bezeichnet $\left(\frac{1}{\mathfrak{m}}\right)$ das Vielfachenideal des Reziproken eines ganzen Divisors $\mathfrak{m}$ von P_g. Auf Grund der Minimaleigenschaft von E besitzt $\mathfrak{m}$ die kleinste Norm in seiner Divisorenklasse. Durchläuft nun $\mathfrak{m}_\lambda$, $\lambda = 1, \ldots l$, die endlich vielen Divisoren von P_g mit diesen Eigenschaften, und ist weiter $\mu_{\varkappa\lambda}$, $\varkappa = 1, \ldots 2k$ jeweils eine Modulbasis von $\left(\frac{1}{\mathfrak{m}_\lambda}\right)$, so erhält man die Exponentenpaare der Matrix $\mathfrak{M}$ von Satz 2 aus den Darstellungen

$$\mu_{\varkappa\lambda} = \frac{1}{m_{\varkappa\lambda}} \cdot P_{\varkappa\lambda}(\sigma_1). \tag{12}$$

Hiernach ist klar, wie man ein System $\mathfrak{S}$ und eine Matrix $\mathfrak{M}$ für eine feste Gradzahl g erhält: Mit den Kreiseinheiten von P_g ist ein unabhängiges Einheitensystem vom Höchstrang von P_g bekannt. Mit dessen Hilfe läßt sich einerseits das System der Divisoren $\mathfrak{m}$ und damit die Matrix $\mathfrak{M}$, andererseits eine (8) erfüllende Konstante c und damit ein System $\mathfrak{S}$ effektiv-rational bestimmen.

5. **Schlußbemerkung und Beispiel:** Um den Umfang der Rechnungen im konkreten Fall herabdrücken zu können, wäre es nützlich, die Konstante c^* – die untere Grenze aller (8) erfüllenden Konstanten c – zu bestimmen. Diese Aufgabe erfordert jedoch die Kenntnis des Kegels $\mathfrak{R}^*$ der reduzierten Vektoren von $\mathfrak{L}^*$, oder also die Auflösung des Ungleichungssystems (7). Für $k = 2$ ergibt sich leicht eine solche geschlossene Auflösung und damit für c^* der Wert

$$c^* = \left(\frac{\sqrt{|\varepsilon_1|} + \sqrt{|\varepsilon_1|}^{-1}}{2}\right)^4, \tag{13}$$

wobei ε_1 die Grundeinheit von P_g bezeichnet. Dieser Wert liefert für die einfachsten, von Satz 3 nicht erfaßten Körpertypen – nämlich für die reellen zyklischen Körper vom Grade $g = 5, 8, 10$ oder 12 – praktisch brauchbare Ergebnisse. Wie schon gesagt, ist die Aufstellung der Matrix $\mathfrak{M}$ hier entbehrlich. Das mit (13) gewonnene System $\mathfrak{S}$ besteht z. B. für $g = 5$ aus den sechs Exponentenpaaren:

$(1, 1)$, $(5, (1 - x)^3)$,
$(11, 2 + x)$, $(11, 2 + x^2)$,
$(11, 2 + x^3)$, $(11, -1 + x + x^2 + x^3)$,

von denen vermutlich die letzten vier noch fortgelassen werden dürfen.

Literatur:

[1] H. Hasse: Rein arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen, kubischen und biquadratischen Zahlkörpern. Berlin 1950. Abh. d. Dt. Akad. d. Wissensch., Berlin, Math.Nat.-Kl., Jahrg. 1948, No. 2.

[2] H. W. Leopoldt: Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper. Berlin 1954. Abh. d. Dt. Akad. d. Wissensch., Berlin, Math. Nat. Kl., Jahrgang 1953, No. 2.