Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 28 (1954)

Artikel: Relativquadratische Zahlkörper, deren Klassenzahl durch eine vorgegebene ungerade Primzahl teilbar ist.
Autor: Gut, Max
DOI: https://doi.org/10.5169/seals-22622

Relativquadratische Zahlkörper, deren Klassenzahl durch eine vorgegebene ungerade Primzahl teilbar ist

von Max Gut, Zürich

Herrn Paul Finsler zum sechzigsten Geburtstage gewidmet

Es bedeute p eine beliebige ungerade Primzahl und ζ die p-te Einheitswurzel $\zeta = e^{\frac{2\pi i}{p}}$. Es sei ferner k ein algebraischer Zahlkörper von endlichem Grade, der ζ enthält, und in welchem wenigstens ein p teilendes Primideal $\mathfrak{p}$ von k den absoluten Grad 1 hat. Dies ist jedenfalls für den Körper der p-ten Einheitswurzeln der Fall, denn für $\lambda = 1 - \zeta$ ist in diesem Körper $p = (\lambda)^{p-1}$, wo das Primideal (λ) vom 1. Grade ist.

In der vorliegenden Arbeit beweisen wir den

Satz: Es gibt unter den beiden über k gemachten Voraussetzungen unendlich viele in bezug auf k relativquadratische Zahlkörper K, deren Klassenzahl durch p teilbar ist.

Wir werden jedoch wesentlich nicht nur zeigen, daß unendlich viele solche Körper K existieren, sondern geben in jedem Falle explizite eine algebraische Zahl vom Relativgrade $2p$ in bezug auf k an, deren Adjunktion zu K ein Stück des Hilbertschen Klassenkörpers von K liefert, das in bezug auf K den Relativgrad p hat.

Ein Polynom heiße *normiert*, wenn der Koeffizient der höchsten Potenz gleich 1 ist.

Es sei z eine freie Variable und

$$x = z + \frac{1}{z}. \tag{1}$$

Ist dann n eine beliebige natürliche Zahl, so ist identisch in z:

$$z^n + \frac{1}{z^n} = G_n(x),$$

wo $G_n(x)$ ein wohlbestimmtes, normiertes, ganzrationalzahliges Polynom

vom Grade n in x ist, dessen Koeffizienten uns hier übrigens nicht weiter interessieren. Es ist also, um möglichst klar zu sein:

$$z + \frac{1}{z} = G_1(x) = x\,,$$

$$z^2 + \frac{1}{z^2} = G_2(x) = x^2 - 2\,,$$

$$z^3 + \frac{1}{z^3} = G_3(x) = x^3 - 3x$$

usf.

Setzt man $z = 1$, so wird $x = 2$, und man erkennt, daß für jede natürliche Zahl n:

$$2 = G_n(2)\,. \tag{2}$$

Wir beweisen zunächst folgenden

Hilfssatz: Für $n \geqq 3$ und $k = 1, 2, \ldots, n-1$ gilt die Formel:

$$\frac{G_n^{(k)}(2)}{(k-1)!\,n} = \binom{n+k-1}{2k-1} = \binom{n+k-1}{n-k}\,. \tag{3}$$

Beweis: Es ist gemäß (1):

$$\frac{dx}{dz} = 1 - \frac{1}{z^2} = \frac{z^2-1}{z^2}\,,$$

also

$$\frac{dz}{dx} = \frac{z^2}{z^2-1}\,.$$

Folglich ist für $n \geqq 3$:

$$\begin{aligned}\frac{G_n'(x)}{n} - \frac{G_{n-2}'(x)}{n-2} &= \frac{d}{dz}\left[\frac{1}{n}\left(z^n + \frac{1}{z^n}\right) - \frac{1}{n-2}\left(z^{n-2} + \frac{1}{z^{n-2}}\right)\right] \cdot \frac{dz}{dx} \\ &= \left[z^{n-1} - \frac{1}{z^{n+1}} - z^{n-3} + \frac{1}{z^{n-1}}\right]\frac{z^2}{z^2-1} \\ &= \left[z^{n-3}(z^2-1) + \frac{1}{z^{n+1}}(z^2-1)\right]\frac{z^2}{z^2-1} \\ &= z^{n-1} + \frac{1}{z^{n-1}} = G_{n-1}(x)\,,\end{aligned}$$

also

$$\frac{G_n'(x)}{n} = \frac{G_{n-2}'(x)}{n-2} + G_{n-1}(x)\,.$$

Mithin wird für $k = 1, 2, \ldots, n-1$, falls unter $G_n^{(0)}(x) \equiv G_n(x)$ verstanden wird:

$$\frac{G_n^{(k)}(x)}{n} = \frac{G_{n-2}^{(k)}(x)}{n-2} + G_{n-1}^{(k-1)}(x) .$$

Es folgt

$$\frac{G_{n-2}^{(k)}(x)}{n-2} = \frac{G_{n-4}^{(k)}(x)}{n-4} + G_{n-3}^{(k-1)}(x)$$

usf. ...

Falls n *ungerade*, ist schließlich

$$\frac{G_3^{(k)}(x)}{3} = \frac{G_1^{(k)}(x)}{1} + G_2^{(k-1)}(x) .$$

Daher ist für *ungerades* n, wie sich durch Addition dieser $\frac{n-1}{2}$ Gleichungen ergibt

$$\frac{G_n^{(k)}(x)}{n} = G_1^{(k)}(x) + \left\{ G_{n-1}^{(k-1)}(x) + G_{n-3}^{(k-1)}(x) + G_{n-5}^{(k-1)}(x) + \cdots + G_2^{(k-1)}(x) \right\}.$$

Falls n *gerade* ist, ist schließlich:

$$\frac{G_4^{(k)}(x)}{4} = \frac{G_2^{(k)}(x)}{2} + G_3^{(k-1)}(x)$$

und

$$\frac{G_2^{(k)}(x)}{2} = G_1^{(k-1)}(x) .$$

Folglich ist für *gerades* n, wie sich durch Addition dieser $\frac{n}{2}$ Gleichungen ergibt:

$$\frac{G_n^{(k)}(x)}{n} = \left\{ G_{n-1}^{(k-1)}(x) + G_{n-3}^{(k-1)}(x) + G_{n-5}^{(k-1)}(x) + \ldots + G_1^{(k-1)}(x) \right\} .$$

Insbesondere ist mithin für *ungerades* n:

$$\frac{G_n^{(k)}(2)}{n} = G_1^{(k)}(2) + \sum_{r=0}^{\frac{n-3}{2}} G_{n-1-2r}^{(k-1)}(2) \tag{4}$$

und für *gerades* n:

$$\frac{G_n^{(k)}(2)}{n} = \sum_{r=0}^{\frac{n-2}{2}} G_{n-1-2r}^{(k-1)}(2) . \tag{5}$$

Wir beweisen die Formel (3) für $k = 1$. Ist n ungerade, so ist gemäß (4) und (2):

$$\frac{G_n'(2)}{n} = 1 + \sum_{r=0}^{\frac{n-3}{2}} 2 = 1 + \frac{n-1}{2} \cdot 2 = n .$$

Ist n gerade, so ist gemäß (5) und (2):

$$\frac{G_n'(2)}{n} = \sum_{r=0}^{\frac{n-2}{2}} 2 = 2 \cdot \frac{n}{2} = n \,.$$

Die Formel (3) ist mithin richtig für $k = 1$.

Für festgehaltenes n nehmen wir an, die Formel (3) sei richtig für k, wo $1 \leqq k \leqq n-2$ ist, und zeigen, daß sie richtig ist für $k+1$.

Für *ungerades* n wird gemäß (4), da $G_1^{(k+1)}(2) = 0$ ist:

$$\frac{G_n^{(k+1)}(2)}{n} = \sum_{r=0}^{\frac{n-3}{2}} G_{n-1-2r}^{(k)}(2) = \sum_{r=0}^{\left[\frac{n-2}{2}\right]} G_{n-1-2r}^{(k)}(2) \,.$$

Für *gerades* n wird gemäß (5):

$$\frac{G_n^{(k+1)}(2)}{n} = \sum_{r=0}^{\left[\frac{n-2}{2}\right]} G_{n-1-2r}^{(k)}(2) \,.$$

Mithin ist für jedes $n \geqq 3$ nach Induktionsvoraussetzung:

$$\begin{aligned}
\frac{G_n^{(k+1)}(2)}{n} &= (k-1)! \sum_{r=0}^{\left[\frac{n-2}{2}\right]} (n-1-2r) \binom{n+k-2-2r}{2k-1} \\
&= k! \sum_{r=0}^{\left[\frac{n-2}{2}\right]} \frac{(n+k-1-2r)-k}{k} \binom{n+k-2-2r}{2k-1} \\
&= k! \sum_{r=0}^{\left[\frac{n-2}{2}\right]} \left\{ 2\binom{n+k-1-2r}{2k} - \binom{n+k-2-2r}{2k-1} \right\} \\
&= k! \sum_{r=0}^{\left[\frac{n-2}{2}\right]} \left\{ \binom{n+k-1-2r}{2k} + \binom{n+k-2-2r}{2k} \right\} \\
&= k! \sum_{s=1}^{n-k} \binom{n+k-s}{2k} = k! \binom{n+k}{2k+1} ,
\end{aligned}$$

womit unser Hilfssatz bewiesen ist.

Insbesondere folgt für jede ungerade Primzahl p:

$$\frac{G_p^{(k)}(2)}{k!} = \frac{p}{k}\binom{p+k-1}{2k-1} = \frac{p}{k}\binom{p+k-1}{p-k}, \; k = 1, 2, \ldots, p-1. \quad (6)$$

Da $G_p(x)$ ein normiertes ganzrationalzahliges Polynom p-ten Grades ist, sind die Größen (6) ganz rational.

Wir wenden uns zum Beweise des Hauptsatzes.

Es sei γ eine beliebige *ganze* Zahl von k, die zu $2p$ teilerfremd und quadratischer Rest mod. p ist:

$$\gamma \equiv c^2 \not\equiv 0 \pmod{\mathfrak{p}}, \tag{7}$$

wo c ganz rational ist, und wir betrachten das normierte Polynom vom ungeraden Primzahlgrade p

$$G_p(x) - \lambda^{2p}\gamma - 2, \tag{8}$$

dessen Koeffizienten ganze Zahlen von k sind. Wir setzen

$$x = 2 + \lambda^2 y$$

und zur Abkürzung:

$$f(y) = y^p + \sum_{k=p-1}^{1} \frac{G_p^{(k)}(2)}{k!\,\lambda^{2(p-k)}}\, y^k - \gamma\,. \tag{9}$$

Beachten wir, daß $G_p(2) = 2$ gemäß (2), so sehen wir, daß

$$G_p(x) - \lambda^{2p}\gamma - 2 = G_p\big(2 + (x-2)\big) - \lambda^{2p}\gamma - 2 =$$

$$= (x-2)^p + \sum_{k=p-1}^{1} \frac{G_p^{(k)}(2)}{k!}\,(x-2)^k - \lambda^{2p}\gamma = \lambda^{2p}\cdot f(y)\,.$$

Da $p = -\lambda^{p-1}\varepsilon$ ist, wo ε eine Einheit des Körpers der p-ten Einheitswurzeln ist, für welche

$$\varepsilon \equiv 1 \big(\mathrm{mod.}\,(\lambda)\big),$$

so folgt aus (6):

Die auf den linken Seiten der folgenden vier Kongruenzen stehenden Zahlen sind *ganze* Zahlen des Körpers der p-ten Einheitswurzeln und

1. für $k = p-1, p-2, \cdots, \dfrac{p+3}{2}$ ist:

$$\frac{G_p^{(k)}(2)}{k!\,\lambda^{2(p-k)}} \equiv 0 \big(\mathrm{mod.}\,(\lambda)\big)$$

2. für $k = \dfrac{p+1}{2}$ ist:

$$\frac{G_p^{\left(\frac{p+1}{2}\right)}(2)}{\left(\frac{p+1}{2}\right)!\,\lambda^{p-1}} \equiv -2 \big(\mathrm{mod.}\,(\lambda)\big)$$

3. für $k = \frac{p-1}{2}, \frac{p-3}{2}, \cdots, 2$ ist:

$$\frac{G_p^{(k)}(2)}{k!\,\lambda^{2(p-k)}} \equiv 0 \,(\mathrm{mod.}\,(\lambda))$$

4. Für $k = 1$ ist:

$$\frac{G_p'(2)}{1!\,\lambda^{2(p-1)}} \equiv 1 \,(\mathrm{mod.}\,(\lambda)) .$$

Mithin wird gemäß (9) und (7)

$$f(y) \equiv y^p - 2y^{\frac{p+1}{2}} + y - c^2 \equiv y(y^{\frac{p-1}{2}} - 1)^2 - c^2 \pmod{\mathfrak{p}}. \qquad (10)$$

Das Polynom $f(y)$ hat mod. $\mathfrak{p}$ weder einen Linearfaktor noch ein mod. $\mathfrak{p}$ irreduzibles Polynom 2. Grades als Faktor. Denn betrachtet man die Kongruenz (10) als eine Gleichung im Galoisfeld $GF(p^2)$, wobei dann c eine von 0 verschiedene Größe des Unterkörpers $GF(p)$, d. h. des Primkörpers der Charakteristik p ist, so besitzt das Polynom (10) im $GF(p^2)$ keinen Linearfaktor. In der Tat folgt aus

$$y(y^{\frac{p-1}{2}} - 1)^2 = c^2,$$

daß y gleich dem Quadrat eines Elementes des $GF(p^2)$ sein muß, $y = \eta^2 \neq 0$, und dann folgt

$$\eta(\eta^{p-1} - 1) = \eta^p - \eta = \pm c .$$

Wendet man auf die letzte Gleichung den von der Identität verschiedenen Automorphismus des $GF(p^2)$ an, so folgt

$$\eta^{p^2} - \eta^p = \eta - \eta^p = \pm c ,$$

und die Addition der beiden letzten Gleichungen führt zum Widerspruch, daß $c = 0$ sein müßte.

Eine beliebige Nullstelle der Gleichung

$$G_p(x) - \lambda^{2p}\gamma - 2 = 0 \qquad (11)$$

legt daher einen Körper fest, der in bezug auf k mindestens vom dritten Relativgrad ist.

Es sei jetzt γ ein Produkt von endlich vielen voneinander verschiedenen rationalen ungeraden Primzahlen, das zur Körperdiskriminanten von k teilerfremd und quadratischer Rest mod. p ist. Insbesondere darf das Produkt auch aus nur einem einzigen Faktor bestehen.

Wir setzen in der Gleichung (11) die Größe $x = z + \frac{1}{z}$. Dadurch geht sie über in die Gleichung

$$z^{2p} - (\lambda^{2p}\gamma + 2)\, z^p + 1 = 0\,. \tag{12}$$

Setzt man

$$z^p = u\,, \tag{13}$$

so wird

$$u^2 - (\lambda^{2p}\gamma + 2)\, u + 1 = 0\,. \tag{14}$$

Die Diskriminante D dieser Gleichung ist

$$D = \lambda^{2p}\gamma \cdot (\lambda^{2p}\gamma + 4)\,.$$

D ist keine Quadratzahl von k. Denn jedes Primideal von k, welches ein Teiler des Hauptideales (D) von k ist, müßte in einer *geraden* Potenz in (D) als Faktor enthalten sein. Das ist aber nicht möglich, denn γ ist zu $\lambda^{2p}\gamma + 4$ teilerfremd, und jeder Primidealteiler der ganzen rationalen Zahl γ ist in k unverzweigt. Mithin ist der Relativgrad von $K = k(u)$ in bezug auf k gleich 2. Übrigens ist die Relativdiskriminante von K in bezug auf k zu p teilerfremd. Denn K kann aus k auch erhalten werden durch Adjunktion von v, wo

$$v = \frac{u - 1}{\lambda^p}\,.$$

Für $u = 1 + \lambda^p v$ geht aber (14) über in die Gleichung

$$v^2 - \lambda^p \gamma v - \gamma = 0\,.$$

v ist mithin algebraisch ganz, und die Diskriminante dieser Gleichung ist

$$\gamma(\lambda^{2p}\gamma + 4) = \frac{D}{\lambda^{2p}}\,,$$

also zu p teilerfremd.

Ist z_1 eine willkürlich aber fest gewählte Nullstelle der Gleichung (12), so werden alle $2p$ Nullstellen von (12) durch die $2p$ algebraischen Einheiten

$$z_t = \zeta^{t-1} z_1,\ z_{p+t} = \frac{\zeta^{1-t}}{z_1},\ t = 1, 2, \ldots, p\,,$$

gegeben und gemäß (13) und (14) hangen sowohl K wie $K(z_1) = K(z)$ nicht ab von der Wahl von z_1. Die p Nullstellen des Polynoms (11) werden gegeben durch

$$x_t = z_t + \frac{1}{z_t} = \zeta^{t-1} z_1 + \frac{\zeta^{1-t}}{z_1},\ t = 1, 2, \ldots, p\,.$$

Der Körper $K(z_1)$ hat in bezug auf K den Relativgrad p oder den Relativgrad 1. Aber das letztere ist nicht möglich, denn sonst hätte z_1 in bezug auf k den Relativgrad 2. Mithin müßte auch

$$x_1 = z_1 + \frac{1}{z_1}$$

in bezug auf k den Relativgrad 2 oder 1 haben. Aber oben haben wir gezeigt, daß x_1 in bezug auf k mindestens vom dritten Relativgrade ist.

Gemäß (13) und (14) gilt für die algebraische Einheit z_1:

$$z_1^p = \tfrac{1}{2}\left(\lambda^{2p}\gamma + 2 \pm \sqrt{D}\right),$$

also

$$z_1^p \equiv 1 \equiv 1^p \left(\text{mod. } (\lambda)^p\right),$$

und daher[1]) ist $K(z_1)$ ein Unterkörper des Hilbertschen (absoluten) Klassenkörpers von K, der in bezug auf K den Relativgrad p hat. Folglich ist die Klassenzahl von K durch p teilbar.

Hat man durch geeignete Wahl von $\gamma_1, \gamma_2, \ldots, \gamma_s$ so schon s voneinander verschiedene in bezug auf k relativquadratische Körper

$$K_1, K_2, \ldots, K_s,$$

deren Klassenzahl je durch p teilbar ist, konstruiert – für $s = 1$ ist dies ja der Fall – so hat man γ_{s+1} nur so zu wählen, daß die in γ_{s+1} aufgehende oder aufgehenden ungeraden rationalen Primzahlen zur Diskriminanten von k, zu $\gamma_1, \gamma_2, \ldots, \gamma_s$ und zu $\lambda^{2p}\gamma_1 + 4, \lambda^{2p}\gamma_2 + 4, \ldots, \lambda^{2p}\gamma_s + 4$ (bzw. den absoluten Normen dieser s Zahlen, genommen im Körper der p-ten Einheitswurzeln) teilerfremd sind, und γ_{s+1} quadratischer Rest mod. p ist. Dann ist K_{s+1} ein von den Körpern $K_1, K_2, \ldots K_s$ verschiedener Körper mit den verlangten Eigenschaften. Es gibt mithin unendlich viele solche Körper K_s.

(Eingegangen den 5. April 1954)

---

[1]) Vgl. z. B. *Hecke, Erich:* Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923, § 39, p. 148–154.