Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Klasse

der

Bayerischen Akademie der Wissenschaften zu München

Jahrgang 1953

München 1954

Verlag der Bayerischen Akademie der Wissenschaften

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

Zur Quadratsummendarstellung in relativquadratischen Zahlkörpern

Von **Hanfried Lenz** in München

Vorgelegt von Herrn Oskar Perron am 4. Dezember 1953

Nach Artin[1] läßt sich jede totalpositive Zahl eines Körpers K als Quadratsumme darstellen. Für den Fall, daß K quadratisch über einem algebraischen Zahlkörper G ist, beweisen wir nach einem Ansatz von Otto Meißner[2] den

Satz: *Ist γ eine totalpositive Zahl einer quadratischen Erweiterung K eines algebraischen Zahlkörpers G, so gibt es eine Darstellung*

$$\gamma = \alpha^2 + a_1^2 + a_2^2 + \ldots\ldots + a_m^2, \tag{1}$$

wobei α dem Körper K und alle a_k dem Grundkörper G angehören.

Bemerkungen: Setzt man den tiefliegenden und im Gegensatz zu dem erwähnten Artinschen Satz nur mit Methoden der algebraischen Zahlentheorie zu beweisenden Siegelschen Satz[3] von der Zerlegbarkeit der totalpositiven Zahlen aus G in *vier* Quadrate voraus, so genügt es, in (1) $m = 4$ zu nehmen.

Ist G der rationale Zahlkörper P und $K = G(\sqrt{d})$ mit ganzrationalem und quadratfreiem d, so kommt man mit $m = 3$ aus, falls $d \not\equiv 1 \pmod 8$ ist, dagegen nicht, falls $d \equiv 1 \pmod 8$ ist.

Beweis: **1.** G sei algebraisch vom n-ten Grade über dem rationalen Primkörper P. $\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_n$ sei eine Basis von G über P. G kann dann bekanntlich als n-dimensionaler Vektorraum $\mathfrak{G}$ über

[1] Emil Artin, Über die Zerlegung definiter Funktionen in Quadrate. Abh. math. Sem. Hamburg 5 (1927) S. 100–15.

[2] Otto Meißner, Über die Darstellung der Zahlen einiger algebraischer Zahlkörper als Summen von Quadratzahlen des Körpers. Arch. d. Math. u. Phys. (3) 7 (1904) S. 266–68; 9 (1905) S. 202–03.

[3] Carl Ludwig Siegel, Darstellung totalpositiver Zahlen durch Quadrate. Math. Zeitschr. 11 (1921) S. 246–75.

P aufgefaßt werden. G läßt sich in die n-dimensonalen Vektorräume $\mathfrak{R}$ bzw. $\mathfrak{C}$ über den Körpern R bzw. C der reellen bzw. komplexen Zahlen mit denselben Basisvektoren einbetten. Definiert man die Multiplikation von Punkten aus $\mathfrak{C}$ mit Hilfe der in G erklärten Multiplikation der Basisvektoren $i_1, \ldots, i_n$ und der distributiven Gesetze, so werden $\mathfrak{G}$, $\mathfrak{R}$ und $\mathfrak{C}$ bekanntlich zu *hyperkomplexen Systemen* oder *Vektorringen* über G, R bzw. C. (Die übliche Bezeichnung „Algebren" soll in dieser Note vermieden werden.)

Die Elemente von G, und damit auch die Punkte aus $\mathfrak{G}$, lassen sich bekanntlich auf n verschiedene Weisen als komplexe Zahlen deuten. Ist x ein willkürliches Element des abstrakten Körpers G, so bezeichne $w_\mu(x)$ ($\mu = 1, 2, \ldots, n$) diese n isomorphen Abbildungen von G in C. Wir nehmen an, daß die Werte $w_\mu(x)$ für $\mu = 1, 2, \ldots, r$ für alle x aus G reell seien, während für $\mu > r$ $w_\mu(x)$ bei mindestens einem $x \in G$ komplex werde und $w_{r+2h-1}(x)$ zu $w_{r+2h}(x)$ konjugiert komplex ausfalle (für $h = 1, 2, \ldots, s = (n - r)/2$).

Wir ordnen nicht nur den Elementen von G, sondern auch den Punkten $\mathfrak{x}$ aus $\mathfrak{G}$, $\mathfrak{R}$ und $\mathfrak{C}$ je n komplexe Werte $w_\mu(\mathfrak{x})$ zu mittels der Vorschrift

$$(2) \qquad \text{wenn} \qquad w_\mu(\mathfrak{x}) = \sum_{i=1}^{n} x_i w_\mu(i_i), \qquad \mathfrak{x} = \sum_{i=1}^{n} x_i i_i$$

die Komponentenzerlegung von $\mathfrak{x}$ ist.

Man verifiziert leicht die Rechenregeln

$$(3) \qquad w_\mu(\mathfrak{x} + \mathfrak{y}) = w_\mu(\mathfrak{x}) + w_\mu(\mathfrak{y}),$$

$$(4) \qquad w_\mu(c\mathfrak{x}) = c\, w_\mu(\mathfrak{x}),$$

$$(5) \qquad w_\mu(\mathfrak{x}\mathfrak{y}) = w_\mu(\mathfrak{x})\, w_\mu(\mathfrak{y})$$

für $c \in C$, $\mathfrak{x} \in \mathfrak{C}$, $\mathfrak{y} \in \mathfrak{C}$.

Konvergiert eine Punktfolge $\mathfrak{x}_h$ aus $\mathfrak{C}$ gegen einen Punkt $\mathfrak{x}$, so konvergieren alle $w_\mu(\mathfrak{x}_h)$ gegen $w_\mu(\mathfrak{x})$.

Ein Element von G ist totalpositiv, wenn und nur wenn die ersten r Werte $w_\mu(\mathfrak{x})$ des zugeordneten Vektors $\mathfrak{x}$ positiv sind.

2. Hilfssatz 1: *n beliebig vorgegebene komplexe Zahlen w_μ ($\mu = 1, \ldots, n$) bestimmen eindeutig einen Vektor $\mathfrak{x} \in \mathfrak{C}$, für den $w_\mu(\mathfrak{x}) = w_\mu$ ist. Sind die Zahlen $w_1, \ldots, w_r$ reell und die darauf folgenden Paare $w_{r+1}, w_{r+2}; \ldots; w_{r+2s-1}, w_{r+2s}$ konjugiert komplex, so ist $\mathfrak{x} \in \mathfrak{R}$.*

Beweis des Hilfssatzes 1: Die Determinante Δ des Gleichungssystems

$$w_\mu(\mathfrak{x}) = \sum_{k=1}^{n} x_k w_\mu(\mathfrak{i}_k) = w_\mu \tag{6}$$

ist von Null verschieden, denn ihr Quadrat ist nichts anderes als die Diskriminante der Basis $\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_n$. Die ersten r Zeilen der Koeffizientenmatrix sind (unter der zusätzlichen Voraussetzung der zweiten Hälfte des Hilfssatzes) reell, die folgenden paarweise konjugiert komplex. Vertauscht man daher in den Zähler- und Nennerdeterminanten der nach der Cramerschen Regel erhaltenen Auflösungsformel

$$x_k = \frac{\Delta_k}{\Delta}$$

des Gleichungssystems (6) je die $(r + 2h - 1)$-te und $(r + 2h)$-te Zeile (für $h = 1, \ldots, s$), so gehen sie in ihre konjugiert komplexen Werte über und multiplizieren sich andererseits mit $(-1)^s$. Daraus folgt, daß die x_k ihren konjugiert komplexen Werten gleich, also reell sind, w. z. b. w.

3. $\mathfrak{P}$ sei die Menge der Punkte aus $\mathfrak{G}$, die totalpositiven Elementen von G entsprechen. Ihre abgeschlossene Hülle $\overline{\mathfrak{P}} \subseteq \mathfrak{R}$ ist der Durchschnitt der r Halbräume $w_\mu(\mathfrak{x}) \geqq 0$ ($\mu = 1, \ldots, r$) des Raumes $\mathfrak{R}$. $\mathfrak{Q}$ sei die Menge der Punkte aus $\mathfrak{G}$, die Quadratzahlen aus G darstellen.

Hilfssatz 2: *$\mathfrak{Q}$ ist dicht in $\overline{\mathfrak{P}}$.*

Beweis des Hilfssatzes 2: Es sei $\mathfrak{y}$ ein Punkt aus $\overline{\mathfrak{P}}$. Dann ist $w_\mu(\mathfrak{y}) \geqq 0$ für $\mu = 1, \ldots, r$. Folglich sind die n rein quadratischen Gleichungen (mit den Unbekannten $w_1, \ldots, w_n$)

$$w_\mu^2 = w_\mu(\mathfrak{y})$$

so lösbar, daß die w_μ für $\mu \leqq r$ reell und für $\mu > r$ paarweise kon-

jugiert komplex werden. Nach Hilfssatz 1 gibt es also einen Punkt $\mathfrak{x}$ aus $\mathfrak{R}$, so daß für alle $\mu = 1, \ldots, n$

oder
$$w_\mu(\mathfrak{x}) = w_\mu$$
$$w_\mu(\mathfrak{x})^2 = w_\mu(\mathfrak{x}^2) = w_\mu(\mathfrak{y})$$

wird. Da nach Hilfssatz 1 jeder Punkt aus $\mathfrak{C}$ durch seine n Werte eindeutig bestimmt ist, folgt

$$\mathfrak{y} = \mathfrak{x}^2. \tag{7}$$

$\mathfrak{x}$ ist Häufungspunkt von Punkten aus $\mathfrak{G}$, $\mathfrak{y}$ wegen der Stetigkeit der durch (7) vermittelten Abbildung von $\mathfrak{C}$ in sich also Häufungspunkt von Punkten aus $\mathfrak{Q}$, w. z. b. w.

4. Wir denken uns nun die ersten r Einbettungen von G in C (also in R) so numeriert, daß $w_\mu(d)$ für $\mu \leqq h$ positiv, für $h < \mu \leqq r$ negativ wird. $\gamma = a + b\sqrt{d}$ sei total positiv in $K = G(\sqrt{d})$. Es gilt die Identität

$$a + b\sqrt{d} = \left(c + \frac{b\sqrt{d}}{2c}\right)^2 + a - c^2 - \frac{db^2}{4c^2}.$$

Unser Satz ist bewiesen, wenn wir zeigen können, daß sich $c \in G$ so wählen läßt, daß die Zahl

$$f = a - c^2 - \frac{db^2}{4c^2}$$

totalpositiv wird. Das ist dann und nur dann der Fall, wenn für $\mu \leqq r$

$$w_\mu(f) = w_\mu(a) - w_\mu(c^2) - w_\mu\left(\frac{db^2}{4c^2}\right) > 0 \tag{8}$$

wird.

Für $r \geqq \mu > h$ ist $w_\mu(d) < 0$ und (8) ist sicher erfüllt, wenn die positive Zahl $w_\mu(c^2)$ hinreichend klein, etwa für geeignete rationale $\alpha_\mu > 0$

$$0 < w(c^2) < \alpha_\mu \tag{9}$$

wird. (Denn $-w_\mu\left(\frac{db^2}{4c^2}\right)$ wird dann beliebig groß).

Für $\mu \leqq h$ können wir die isomorphe Abbildung von G in R so auf den quadratischen Erweiterungskörper K fortsetzen, daß

$$w_\mu(\sqrt{d}) = \sqrt{w_\mu(d)} > 0$$

wird.

Dann kann man schreiben

$$w_\mu(f) = w_\mu(a) - |w_\mu(b\sqrt{d})| - \left[w_\mu(c^2) - \left|w_\mu\left(\frac{b}{2}\sqrt{d}\right)\right|\right] - \tag{10}$$
$$- \left[w_\mu\left(\frac{db^2}{4c^2}\right) - \left|w_\mu\left(\frac{b}{2}\sqrt{d}\right)\right|\right].$$

Wir wählen nun einen Punkt $\mathfrak{y} \in \mathfrak{C}$ aus, der den folgenden Gleichungen und Ungleichungen genügt:

$$w_\mu(\mathfrak{y}) = \left|w_\mu\left(\frac{b}{2}\sqrt{d}\right)\right| > 0 \qquad \text{für } \mu \leqq h,$$
$$0 < w_\mu(\mathfrak{y}) < \alpha_\mu \qquad \text{für } h < \mu \leqq r,$$
$$w_{r+2k-1}(\mathfrak{y}) = \overline{w_{r+2k}(\mathfrak{y})} \qquad \text{für } k = 1, \ldots, s.$$

Nach Hilfssatz 1 ist das möglich und $\mathfrak{y}$ liegt in $\overline{\mathfrak{P}}$. Nach Hilfssatz 2 ist $\mathfrak{y}$ also Häufungspunkt von Punkten aus $\mathfrak{Q}$, d. h. es gibt eine Folge von Quadraten c_k^2 aus G, so daß für $\mu \leqq h$

$$\lim_{k\to\infty}\left[w_\mu(c_k^2) - \left|w_\mu\left(\frac{b}{2}\sqrt{d}\right)\right|\right] = 0, \tag{11}$$
$$\lim_{k\to\infty}\left[w_\mu\left(\frac{db^2}{4c_k^2}\right) - \left|w_\mu\left(\frac{b}{2}\sqrt{d}\right)\right|\right] = 0,$$

und außerdem für hinreichend großes k und $h < \mu \leqq r$

$$0 < w_\mu(c_k^2) < \alpha_\mu \tag{12}$$

wird. $\gamma = a + b\sqrt{d}$ ist totalpositiv, also

$$w_\mu(a) - |w_\mu(b\sqrt{d})| > 0 \qquad \text{für } \mu \leqq h.$$

Daraus und aus (10), (11), (9) und (12) folgt für hinreichend großes k, wenn man $c = c_k$ setzt:

$$w_\mu(f) > 0 \quad \text{für alle } \mu = 1, 2, \ldots, r,$$

womit unser Satz bewiesen ist.

5. Es bleibt noch die anfangs gemachte Bemerkung über den Fall zu beweisen, daß G der rationale Primkörper ist. Wir benötigen dazu den bekannten Satz, daß eine natürliche Zahl dann

und nur dann als Summe dreier ganzrationaler Quadrate dargestellt werden kann, wenn ihr quadratfreier Bestandteil mod 8 einen von 7 verschiedenen Rest besitzt.[1]

Daraus schließt man mühelos: Eine rationale Zahl ist Summe dreier rationaler Quadrate, wenn und nur wenn sie erstens positiv ist und zweitens der quadratfreie Bestandteil des Produkts aus Zähler und Nenner mod 8 einen von 7 verschiedenen Rest besitzt.

Es sei also nun $G = P$, $d \not\equiv 1 \pmod 8$. Ohne Beschränkung der Allgemeinheit dürfen wir $a > 0$ und b als ganzrational, d als ganzrational und quadratfrei annehmen. Die oben eingeführte Zahl c sei als gekürzter Bruch $\frac{p}{q}$ geschrieben. Die Zahl f ist Summe dreier rationaler Quadrate, wenn und nur wenn die ganze Zahl

$$z = 4ap^2q^2 - 4p^4 - db^2q^4$$

positiv und nicht von der Form $4^e(8m + 7)$ ist.

Es sei $b = 2^g u$ mit ungeradem u. Dann kann man q ungerade und p durch eine so hohe Potenz von 2 teilbar wählen, daß die ganze Zahl

$$z \cdot 2^{-2g} \not\equiv 0, 4, 7 \pmod 8$$

wird. Man kann im Fall $d > 0$ außerdem noch erreichen, daß $c = \frac{p}{q}$ beliebig nahe an $\sqrt[4]{\frac{db^2}{4}}$ liegt, und damit, daß z positiv, also Summe dreier Quadrate wird. Im Fall $d < 0$ genügt es, c hinreichend klein zu wählen.

6. Ist dagegen $d \equiv 1 \pmod 8$, so sei wieder $\gamma = a + b\sqrt{d}$ total-positiv, ferner seien a und b ungerade ganze Zahlen. Die oben eingeführte Zahl $z = 4ap^2q^2 - 4p^4 - db^2q^4$ läßt für ungerades q den Rest 7 (mod 8). Für gerades $q = 2q_0$ muß p ungerade sein, also wird

$$\frac{z}{4} = 4ap^2q_0^2 - 4db^2q_0^4 - p^4 \equiv 7 \pmod 8,$$

gleichgültig, ob q_0 gerade ist oder nicht. z kann daher für kein rationales $c = \frac{p}{q}$ in drei Quadrate zerlegt werden, f also auch nicht.

[1] Vgl. etwa Enz. d. math. Wiss. I C 2 S. 619 oder Burton W. Jones, The arithmetic theory of quadratic forms. The Carus Mathematical Monographs 10 (1950) S. 187.