Darstellung total positiver Zahlen durch Quadrate.

Von

Carl Siegel in Göttingen.

Für den Hilbertschen Satz: „Jede total positive Zahl eines algebraischen Zahlkörpers läßt sich als Summe von vier Quadratzahlen desselben Körpers darstellen“ ist bisher kein Beweis publiziert worden. Es sind nur spezielle Fälle des Satzes erledigt; und andererseits weiß man einiges über die Darstellbarkeit total positiver Zahlen durch Quadrate von Körperzahlen überhaupt. Mir sind bekannt geworden die beiden unten zitierten Notizen von O. Meißner, in denen quadratische und kubische Zahlkörper betrachtet werden, und eine von Landau veröffentlichte Bemerkung von I. Schur, der den Hilbertschen Satz für die total positive Zahl -1 in einem Kreiskörper beweist. Außerdem hat Landau den Hilbertschen Satz für quadratische Körper, sowie die Darstellbarkeit der total positiven Zahlen durch endlich viele Quadrate bewiesen.

Ich betrachte den Satz als spezielles Ergebnis einer allgemeinen Theorie der quadratischen Formen, deren Koeffizienten und Variable in einem algebraischen Zahlkörper liegen. Dementsprechend werden in § 1 die wichtigsten Begriffe der Arithmetik quadratischer Formen aus dem Gebiete der rationalen Zahlen auf Zahlkörper übertragen; §§ 2, 3 enthalten den eigentlichen Beweis der Hilbertschen Behauptung. Eine unmittelbare Folgerung ist die Lösung einer Verallgemeinerung des Waringschen Problems auf Zahlkörper; § 4 gibt einige weitere Anwendungen. In § 5 entwickle ich die notwendigen und hinreichenden Bedingungen für Darstellbarkeit durch 2 oder 3 Quadrate.

Die Frage, ob bei der Darstellung einer *ganzen* total positiven Zahl als Summe von 4 Quadraten die Nenner in den Basen stets aus einem nur vom Körper abhängigen endlichen Wertevorrat gewählt werden können, bzw. in welchen Körpern dies zutrifft, kann ich nicht entscheiden. Ich kann nur zeigen (in § 6), und zwar mit ganz elementarer Methode, daß

beschränkte Nenner im Fall eines *total reellen* Körpers bei der Zerlegung in endlich viele (anstatt in 4) Quadrate gefordert werden können.

Zur Erleichterung stelle ich hier für den Leser die wichtigen Sätze der höheren Arithmetik zusammen, die im folgenden gebraucht werden:

I. Hilbert-Furtwänglersches quadratisches Reziprozitätsgesetz:

Sind μ und ν zwei ganze Zahlen eines algebraischen Zahlkörpers K, so ist

$$\prod_{\mathfrak{w}} \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1,$$

wo das Produkt über alle Primideale $\mathfrak{w}$ aus K und die Symbole $1^{(i)}$ zu erstrecken ist.

II. Sind μ und ν zwei ganze Zahlen aus K und ist $\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1$, wo $\mathfrak{w}$ alle Primideale in K und die Symbole $1^{(i)}$ durchläuft, so ist ν Relativnorm einer Zahl des Körpers $K(\sqrt{\mu})$. Dann hat also auch die Diophantische Gleichung

$$\mu x^2 + \nu y^2 = z^2$$

eine Lösung in ganzen Zahlen x, y, z aus K, die nicht alle 0 sind.

III. Wenn $\mathfrak{q}$ ein Primideal des Körpers K ist, das nicht in der Relativdiskriminante des relativquadratischen Körpers $K(\sqrt{\mu})$ aufgeht, so ist jede zu $\mathfrak{q}$ prime Zahl in K Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{q}$.

Geht dagegen $\mathfrak{q}$ in der Relativdiskriminante von $K(\sqrt{\mu})$ auf, so bedeute e im Falle $\mathfrak{q}+2$ einen beliebigen positiven Exponenten, im Falle $\mathfrak{q}\,2$, wenn $\mathfrak{q}$ in 2 zu genau k-ter Potenz aufgeht, einen beliebigen Exponenten $> 2k$; dann sind von allen vorhandenen zu $\mathfrak{q}$ primen und nach $\mathfrak{q}^e$ inkongruenten Zahlen in K genau die Hälfte Normenreste des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{q}$.

IV. Es sei $\mathfrak{p}$ ein zu 2 primes Primideal des Körpers K. Geht $\mathfrak{p}$ in der Zahl μ genau zur a-ten Potenz auf, so ist die Relativdiskriminante von $K(\sqrt{\mu})$ durch $\mathfrak{p}$ teilbar oder nicht, je nachdem a ungerade oder gerade ist.

Es sei $\mathfrak{l}$ ein Primideal von K, das in 2 aufgeht und zwar zu genau k-ter Potenz; ferner gehe $\mathfrak{l}$ in μ genau zur a-ten Potenz auf. Die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ ist durch $\mathfrak{l}$ teilbar oder nicht, je nachdem die Kongruenz $x^2 \equiv \mu \pmod{\mathfrak{l}^{2k+a}}$ in K unlösbar oder lösbar ist.

V. Dirichlet-Heckescher Satz:

Es seien $\mathfrak{f}$ und $\mathfrak{a}$ zwei teilerfremde Ideale aus K. Es gibt unendlich viele Primideale $\mathfrak{p}$ und ganze total positive zu $\mathfrak{f}$ teilerfremde Zahlen α, β des Körpers K, so daß

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{p}, \qquad \alpha \equiv \beta \pmod{\mathfrak{f}}$$

ist.

Für die Sätze I bis IV vergleiche man die Arbeiten: D. Hilbert, Über die Theorie des relativquadratischen Zahlkörpers; Mathematische Annalen **51** (1898), S. 1—127. Ph. Furtwängler, Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern; Mathematische Annalen, Erster Teil, **67** (1909), S. 1—31; Zweiter Teil, **72** (1912), S. 346—386; Dritter Teil, **74** (1914), S. 413—429.

Satz V steht bei E. Hecke, Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper; Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, Jahrgang 1917, S. 299—318. E. Landau, Über Ideale und Primideale in Idealklassen; Mathematische Zeitschrift **2** (1918), S. 52—154.

In einer späteren Arbeit hoffe ich die Theorie der quadratischen Formen in algebraischen Zahlkörpern weiter entwickeln zu können. Herrn D. Hilbert danke ich für seine freundliche Erlaubnis, meinen Beweis vor dem seinigen veröffentlichen zu dürfen.

§ 1.

Es bedeute $f(x) = f(x_1, x_2, x_3) = \sum_{i,k=1}^{3} \alpha_{ik} x_i x_k$ eine ternäre quadratische Form mit ganzen algebraischen Koeffizienten $\alpha_{ik} = \alpha_{ki}$ aus einem Körper K. Die Determinante $|\alpha_{ik}| = d$ sei im folgenden stets $\neq 0$. Ich setze $d(\alpha_{ik})^{-1} = (A_{ik})$ und nenne die ternäre quadratische Form $F(X) = F(X_1, X_2, X_3) = \sum_{i,k=1}^{3} A_{ik} X_i X_k$ die zu $f(x)$ *adjungierte* Form. Ihre Koeffizienten $A_{ik} = A_{ki}$ sind ganze algebraische Zahlen aus K; ihre Determinante ist $|A_{ik}| = d^2 \neq 0$. Die größten gemeinsamen Teiler der Koeffizienten von $f(x)$ und $F(X)$ seien $(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}) = \mathfrak{a}$, $(A_{11}, A_{12}, \ldots, A_{33}) = \mathfrak{A}$; dann ist $\mathfrak{a}^2 | \mathfrak{A} = \mathfrak{a}^2 \mathfrak{D}$. Ferner ist nach der Fundamentaleigenschaft der Elementarteiler $\frac{\mathfrak{A}}{\mathfrak{a}} | \frac{(d)}{\mathfrak{A}}$, $\frac{\mathfrak{a}(d)}{\mathfrak{A}^2} = \frac{(d)}{\mathfrak{a}^3 \mathfrak{D}^2}$ ganz, also $(d) = \mathfrak{a}^3 \mathfrak{D}^2 \mathfrak{d}$ und $(|A_{ik}|) = (d^2) = (\mathfrak{a}^2 \mathfrak{D})^3 \mathfrak{D} \mathfrak{d}^2 = \mathfrak{A}^3 \mathfrak{d}^2 \mathfrak{D}$.

Es gelten folgende zwei Identitäten, deren Richtigkeit man z. B. durch Vergleichung der Koeffizienten sofort erkennt:

$$(1) \quad f(x_1, x_2, x_3) f(y_1, y_2, y_3) = \Big(\sum_{i,k=1}^{3} \alpha_{ik} x_i y_k\Big)^2 + F\left(\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}, \begin{vmatrix} x_3 & x_1 \\ y_3 & y_1 \end{vmatrix}, \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}\right),$$

$$(2) \quad F(X_1, X_2, X_3) F(Z_1, Z_2, Z_3) = \Big(\sum_{i,k=1}^{3} A_{ik} X_i Z_k\Big)^2 + d f\left(\begin{vmatrix} Z_2 & Z_3 \\ X_2 & X_3 \end{vmatrix}, \begin{vmatrix} Z_3 & Z_1 \\ X_3 & X_1 \end{vmatrix}, \begin{vmatrix} Z_1 & Z_2 \\ X_1 & X_2 \end{vmatrix}\right).$$

Hierin mögen X_ν und Z_ν $(\nu = 1,2,3)$ die Unterdeterminanten von x_ν und z_ν in der Matrix $\begin{pmatrix} x_1 x_2 x_3 \\ y_1 y_2 y_3 \\ z_1 z_2 z_3 \end{pmatrix}$ bedeuten. Dann sind die in (2) auftretenden Größen $\begin{vmatrix} Z_2 Z_3 \\ X_2 X_3 \end{vmatrix}, \ldots$ die Unterdeterminanten von Y_ν $(\nu = 1,2,3)$ in der Matrix $\begin{pmatrix} X_1 X_2 X_3 \\ Y_1 Y_2 Y_3 \\ Z_1 Z_2 Z_3 \end{pmatrix}$, haben also die Werte $(x_1 X_1 + x_2 X_2 + x_3 X_3) y_\nu$; und da f homogen ist, so folgt aus (1) und (2)

$$F(X) f(x) f(y)$$

$$= F(X) \Big(\sum_{i,k=1}^{3} a_{ik} x_i y_k \Big)^2 + \Big(\sum_{i,k=1}^{3} A_{ik} X_i Z_k \Big)^2 + d f(y) \Big(\sum_{\nu=1}^{3} x_\nu X_\nu \Big)^2 .$$

Es sei $\beta_1, \beta_2, \beta_3$ ein ganzzahliges Wertsystem der y, für welches $f(\beta_1, \beta_2, \beta_3) = m \neq 0$ ist. Ferner seien die ganzzahligen Werte $z_\nu = \gamma_\nu$ so beschaffen, daß für die zugehörigen $X_\nu = A_\nu$ auch die Zahl $F(A_1, A_2, A_3) = M \neq 0$ ist. Dann gilt

$$M m f(x) = M U^2 + V^2 + d m W^2 , \tag{3}$$

wo

$$U = \sum_{i,k=1}^{3} a_{ik} \beta_i x_k , \qquad V = \sum_{i,k=1}^{3} A_{ik} A_i Z_k , \qquad W = \sum_{\nu=1}^{3} A_\nu x_\nu$$

gesetzt ist. U, V, W sind homogene lineare Funktionen von x_1, x_2, x_3; die Determinante dieser Substitution sei S. Bildet man von der quadratischen Form (3) beiderseits die Determinante, so folgt

$$(M m)^3 d = M \cdot 1 \cdot d m \cdot S^2 , \quad \text{also} \quad S = \pm M m \neq 0 .$$

Ist der Körper K reell, so kann $f(x)$ definit oder indefinit sein. Nach dem Trägheitsgesetz der quadratischen Formen ist $f(x)$ dann und nur dann definit, wenn in (3) die Koeffizienten von U^2, V^2, W^2 gleiche Vorzeichen haben. Der Koeffizient von V^2 ist $1 > 0$, also ist für definite $f(x)$ gleichzeitig $M > 0$, $d m > 0$; für indefinite $f(x)$ ist mindestens eine der beiden Zahlen $M, d m < 0$. Es seien $K^{(1)}, \ldots, K^{(s)}$ sämtliche zu K konjugierten reellen Körper, wenn solche vorhanden sind. Es gehe $f^{(i)}$ aus f dadurch hervor, daß die Koeffizienten a_{ik} durch ihre Konjugierten aus $K^{(i)}$ ersetzt werden. Dann ist, wie soeben gezeigt wurde, die Form $f^{(i)}$ definit oder indefinit, je nachdem $\left(\frac{-M, -d m}{1^{(i)}}\right) = -1$ oder $= +1$ ist[1]).

[1]) Das Hilbertsche Symbol $\left(\frac{\nu, \mu}{1^{(i)}}\right)$ hat folgende Definition: Es seien μ, ν zwei von 0 verschiedene Zahlen aus K und i eine Zahl der Reihe 1 bis s. Ist dann zugleich $\mu^{(i)} < 0$, $\nu^{(i)} < 0$, so bedeutet $\left(\frac{\nu, \mu}{1^{(i)}}\right)$ die Zahl -1; in jedem andern Fall bedeutet $\left(\frac{\nu, \mu}{1^{(i)}}\right)$ die Zahl $+1$.

Zwei Zahlen, die wie m und M in der Form $m = f(\beta_1, \beta_2, \beta_3)$, $M = F(\beta_2\gamma_3 - \beta_3\gamma_2,\ \beta_3\gamma_1 - \beta_1\gamma_3,\ \beta_1\gamma_2 - \beta_2\gamma_1)$ darstellbar sind, sollen *simultan* durch f und F darstellbar genannt werden. Das Symbol $\left(\frac{-M,-dm}{1^{(i)}}\right)$ hat also für zwei beliebige durch f und F simultan darstellbare Zahlen $m \neq 0$ und $M \neq 0$ denselben Wert; dieser hängt also nur von f, nicht von der besonderen Wahl von m und M ab. Es verdient hervorgehoben zu werden, daß durch das Vorzeichen von $d^{(i)}$ und den Wert von $\left(\frac{-M,-dm}{1^{(i)}}\right)$ der Trägheitsindex von $f^{(i)}$ eindeutig festgelegt ist.

Es sei $\mathfrak{w}$ ein Primideal aus K und r eine natürliche Zahl. Ich betrachte bei festen $m \neq 0$ und $M \neq 0$ die Kongruenz

$$(4) \qquad M U_0^2 + V_0^2 + dm W_0^2 \equiv 0 \pmod{\mathfrak{w}^{2r}}$$

in den Unbekannten U_0, V_0, W_0. Ist sie für jedes r in ganzen U_0, V_0, W_0 aus K lösbar, welche nicht sämtlich durch $\mathfrak{w}$ teilbar sind, so hat das Normenrestsymbol $\left(\frac{-M,-dm}{\mathfrak{w}}\right)$ den Wert $+1$. Gibt es dagegen ein r, für das sie nicht in solchen U_0, V_0, W_0 lösbar ist, so ist $\left(\frac{-M,-dm}{\mathfrak{w}}\right) = -1$. Die höchste Potenz von $\mathfrak{w}$, die in Mm aufgeht, sei $\mathfrak{w}^{r_0}$ $(r_0 \geqq 0)$. Es sei $\left(\frac{-M,-dm}{\mathfrak{w}}\right) = +1$ und $r > r_0$. Die Kongruenz (4) hat dann eine Lösung U_0, V_0, W_0 mit $(U_0, V_0, W_0, \mathfrak{w}^r) = \mathfrak{w}^{r_0}$. Die Determinante $S = \pm Mm$ der in bezug auf x_1, x_2, x_3 linearen Kongruenzen

$$(5) \qquad U \equiv U_0, \qquad V \equiv V_0, \qquad W \equiv W_0 \pmod{\mathfrak{w}^r}$$

ist genau durch $\mathfrak{w}^{r_0}$ teilbar; und da $\mathfrak{w}^{r_0}$ auch in den rechten Seiten aufgeht, so werden sie durch drei ganze Zahlen x_1, x_2, x_3 befriedigt, die nicht alle $\equiv 0 \pmod{\mathfrak{w}}$ sind. Dann ist nach (3), (4), (5)

$$Mm f(x) \equiv 0 \pmod{\mathfrak{w}^{2r}},$$

$$f(x) \equiv 0 \pmod{\mathfrak{w}^{2r-r_0}}, \qquad f(x) \equiv 0 \pmod{\mathfrak{w}^r}.$$

Ist also $\left(\frac{-M,-dm}{\mathfrak{w}}\right) = +1$, so ist $f(x) \equiv 0 \pmod{\mathfrak{w}^r}$ für jedes r lösbar, und zwar in solchen x_1, x_2, x_3, die nicht alle durch $\mathfrak{w}$ teilbar sind.

Umgekehrt sei $f(x) \equiv 0 \pmod{\mathfrak{w}^r}$ für jedes r in derartigen x_1, x_2, x_3 lösbar. Dann ist auch $f(x) \equiv 0 \pmod{\mathfrak{w}^{2r-r_0}}$, also $Mm f(x) \equiv 0 \pmod{\mathfrak{w}^{2r}}$ lösbar. Wegen $\mathfrak{w}^{r_0+1} \nmid Mm = \pm S$ ist für ein solches Wertsystem x eine der Zahlen U, V, W nicht durch $\mathfrak{w}^{r_0+1}$ teilbar; da nun

$$MU^2 + V^2 + dmW^2 \equiv 0 \pmod{\mathfrak{w}^{2r}}$$

gilt, so ist auch

$$M U_0^2 + V_0^2 + d m W_0^2 \equiv 0 \pmod{\mathfrak{w}^{2r-2r_0}},$$

also auch (4) für jedes r mit der Bedingung $(U_0, V_0, W_0, \mathfrak{w}) = \mathfrak{o}$ lösbar.

Daraus folgt: Ist $f(x) \equiv 0 \pmod{\mathfrak{w}^r}$ für jedes r lösbar (mit $(x_1, x_2, x_3, \mathfrak{w}) = \mathfrak{o}$), so ist $\left(\frac{-M, -dm}{\mathfrak{w}}\right) = +1$; ist dagegen $f(x) \equiv 0 \pmod{\mathfrak{w}^r}$ nicht für jedes r lösbar, so ist $\left(\frac{-M, -dm}{\mathfrak{w}}\right) = -1$. Der Wert des Symboles $\left(\frac{-M, -dm}{\mathfrak{w}}\right)$ hängt also nur von f, nicht von der besonderen Wahl des simultan dargestellten Zahlen m und M ab.

Ich setze noch $(a_{11}, a_{22}, a_{33}, 2a_{23}, 2a_{31}, 2a_{12}) = \mathfrak{a}\mathfrak{d}$, $(A_{11}, A_{22}, A_{33}, 2A_{23}, 2A_{31}, 2A_{12}) = \mathfrak{A}\mathfrak{S}$; dann ist $\mathfrak{d} \mid 2, \mathfrak{S} \mid 2$. Zwei ternäre quadratische Formen mit ganzen Koeffizienten aus K heißen von gleicher *Ordnung*, wenn sie in den Idealen $\mathfrak{d}, \mathfrak{s}, \mathfrak{D}, \mathfrak{S}$ und der Zahl d übereinstimmen. Alle Formen derselben Ordnung, die in den Werten von $\left(\frac{-M, -dm}{\mathfrak{w}}\right)$ für alle $\mathfrak{w}$ (d. h. für $\mathfrak{w}$ = Primideal und $\mathfrak{w} = 1$[4]) übereinstimmen[2]), bilden ein *Geschlecht*.

§ 2.

In diesem Paragraphen mache ich folgende drei Voraussetzungen:

1. ξ sei eine ganze *total positive*[3]) Zahl aus K.

2. -1 und $-\xi$ seien nicht gleich dem Quadrat einer Zahl des Körpers K.

3. Jeder Primidealteiler von 2 gehe in der Relativdiskriminante des relativquadratischen Körpers $K(\sqrt{-\xi})$ auf.

Ich betrachte fortan nur die spezielle ternäre Form

$$f(x_1, x_2, x_3) = \xi x_1^2 - x_2^2 - x_3^2.$$

In den Bezeichnungen von § 1 ist dann

$$F(X_1, X_2, X_3) = X_1^2 - \xi X_2^2 - \xi X_3^2, \qquad d = \xi \neq 0,$$
$$\mathfrak{a} = \mathfrak{A} = \mathfrak{D} = \mathfrak{s} = \mathfrak{S} = \mathfrak{o}, \qquad \mathfrak{d} = (\xi).$$

Setzt man für β und γ die Zahlentripel 0, 1, 0 und 0, 0, 1, so wird $A_1 = 1$, $A_2 = A_3 = 0$; und es sind $m = -1 \neq 0$ und $M = +1 \neq 0$ simultan darstellbar, so daß sich das Geschlecht von $f(x)$ durch die Werte der Symbole $\left(\frac{-1, \xi}{\mathfrak{w}}\right) = \varepsilon_{\mathfrak{w}}$ bestimmt.

[2]) Dies sind in Wirklichkeit nur endlich viele Bedingungen, da für ein Primideal $\mathfrak{w} \nmid 2\alpha\beta$ stets $\left(\frac{\alpha, \beta}{\mathfrak{w}}\right) = +1$ ist.

[3]) d. h. $\xi^{(i)} > 0$ für $i = 1, \ldots, s$. Bezeichnung (nach Landau): $\xi \gg 0$.

Hilfssatz 1. Das Geschlecht von $f(x)$ enthält eine Form der Gestalt $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -M_1 & N_1 \\ 0 & N_1 & -M_1' \end{pmatrix}$, wo M_1 eine nicht in 2ξ aufgehende total positive Primzahl aus K bedeutet.

Beweis. 1. Es sei t_1 irgendeine total positive Zahl aus K. Dann ist

$$\left(\frac{t_1, -\xi}{1^{(i)}}\right) = \left(\frac{-1, \xi}{1^{(i)}}\right) = +1.$$

2. Es sei $\mathfrak{p}$ ein Primfaktor der Relativdiskriminante von $K(\sqrt{-\xi})$, der nicht in 2 aufgeht. Nach Satz IV der Einleitung teilt dann $\mathfrak{p}$ auch die Relativdiskriminante von $K(\sqrt{+\xi})$, und umgekehrt. Nach Satz III der Einleitung gibt es dann in K eine ganze nicht durch $\mathfrak{p}$ teilbare Zahl t_2, so daß $\left(\frac{t_2, -\xi}{\mathfrak{p}}\right)$ den vorgeschriebenen Wert $\varepsilon_\mathfrak{p}$ hat.

3. Es sei $\mathfrak{l}$ ein Primteiler von 2. Dann geht nach der Voraussetzung 3. dieses Paragraphen das Primideal $\mathfrak{l}$ auch in der Relativdiskriminante des relativquadratischen Körpers $K(\sqrt{-\xi})$ auf. Nach Satz III der Einleitung gibt es also ein ganzes t_3 mit $\mathfrak{l} \nmid t_3$ derart, daß $\left(\frac{t_3, -\xi}{\mathfrak{l}}\right) = \varepsilon_\mathfrak{l}$ ist.

Damit eine Zahl t aus K die Eigenschaften der in den drei vorhergehenden Abschnitten betrachteten Zahlen t_1, t_2, t_3 besitzt, reicht es hin, daß $t \succ 0$ ist und die Kongruenzen

(6) $\quad t \equiv t_2 \pmod{\mathfrak{p}}$ für alle bei 2. in Betracht kommenden $\mathfrak{p}$,

(7) $\quad t \equiv t_3 \pmod{\mathfrak{l}^{2k+1}}$ für alle $\mathfrak{l} \mid 2$, wenn genau $\mathfrak{l}^k$ in 2 aufgeht,

erfüllt sind. (6) und (7) sind kompatibel und lassen sich durch *eine* Kongruenz

$$t \equiv t_0 \pmod{\mathfrak{n}}$$

ersetzen, wo das Ideal $\mathfrak{n}$ sich aus den verschiedenen Primidealen $\mathfrak{p}$ und $\mathfrak{l}$ zusammensetzt und zu t_0 teilerfremd ist. Nach Satz V der Einleitung gibt es unendlich viele nicht assoziierte total positive Primzahlen t, welche $\equiv t_0 \pmod{\mathfrak{n}}$ sind. Unter diesen wähle ich eine, die in 2ξ nicht aufgeht, und nenne sie M_1.

Nach Satz I der Einleitung ist nun

$$\prod_\mathfrak{w} \varepsilon_\mathfrak{w} = \prod_\mathfrak{w} \left(\frac{-1, \xi}{\mathfrak{w}}\right) = +1,$$

wo über alle $\mathfrak{w} \nmid 2\xi$ und $\mathfrak{w} = 1^{(i)}$ zu multiplizieren ist; ebenso ist

$$\left(\frac{M_1, -\xi}{(M_1)}\right) \prod_\mathfrak{w} \left(\frac{M_1, -\xi}{\mathfrak{w}}\right) = +1,$$

wo dieselben $\mathfrak{w}$ zu nehmen sind. Andererseits ist nach Konstruktion

$$\left(\frac{M_1, -\xi}{\mathfrak{w}}\right) = \varepsilon_{\mathfrak{w}},$$

so daß aus den drei letzten Gleichungen folgt

$$\left(\frac{M_1, -\xi}{(M_1)}\right) = +1;$$

d. h. die Kongruenz

$$-\xi \equiv x^2 \pmod{M_1}$$

ist lösbar. Es gibt daher in K zwei ganze Zahlen M_1' und N_1, so daß

$$-\xi = N_1^2 - M_1 M_1' \tag{8}$$

gilt. Nun setze ich

$$f_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -M_1 & N_1 \\ 0 & N_1 & -M_1' \end{pmatrix},$$

dann ist wegen (8) die adjungierte Form

$$F_1 = \begin{pmatrix} \xi & 0 & 0 \\ 0 & -M_1' & -N_1 \\ 0 & -N_1 & -M_1 \end{pmatrix}.$$

Ferner ist $f_1(1,0,0) = 1$, $f_1(0,1,0) = -M_1$, $F_1(0,0,1) = -M_1$, so daß die Zahlen 1 und $-M_1$ durch f_1 und F_1 simultan dargestellt werden. Daher besitzt f_1 die Geschlechtscharaktere $\left(\frac{M_1, -\xi}{\mathfrak{w}}\right) = \varepsilon_{\mathfrak{w}}$; gehört also dem Geschlecht von f an, da offenbar f_1 und F_1 *eigentlich primitive* Formen sind, d. h. die Invarianten $\mathfrak{a} = \mathfrak{A} = \mathfrak{s} = \mathfrak{S} = \mathfrak{o}$ besitzen. Damit ist Hilfssatz 1 bewiesen.

Hilfssatz 2. Es gibt eine Substitution von der Determinante ± 1 mit (ganzen oder gebrochenen) Koeffizienten aus K, welche die Form

$$f = \begin{pmatrix} \xi & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

in die Form

$$f_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -M_1 & N_1 \\ 0 & N_1 & -M_1' \end{pmatrix}$$

des Hilfssatzes 1 transformiert.

Beweis. Das nach Hilfssatz 1 gemeinsame Geschlecht von f und f_1 wird durch die Werte der Symbole $\left(\frac{-1, \xi}{\mathfrak{w}}\right) = \left(\frac{M_1, -\xi}{\mathfrak{w}}\right)$ bestimmt. Hierbei kommen für $\mathfrak{w}$ alle in $2 M_1 \xi$ aufgehenden Primideale sowie die Zeichen $1^{(\mathfrak{o})}$

in Betracht. Ich werde jetzt zeigen, daß es in K eine ganze Zahl ζ_0 gibt, welche für alle diese $\mathfrak{w}$ die Gleichungen

$$\left(\frac{-1,\zeta_0}{\mathfrak{w}}\right)=+1,\qquad \left(\frac{M_1,-\zeta_0}{\mathfrak{w}}\right)=+1 \tag{9}$$

erfüllt.

1. Es sei $\mathfrak{w}=1^{(6)}$. Dann wird (9) wegen $M_1>0$ für jedes $\zeta_0>0$ erfüllt.

2. Es sei $\mathfrak{w}=(M_1)+2$. Dann ist für jedes nicht durch M_1 teilbare ζ_1 das Symbol $\left(\frac{-1,\zeta_1}{(M_1)}\right)=+1$; und unter allen diesen ζ_1 gibt es sicher auch solche, für welche $\left(\frac{M_1,-\zeta_1}{(M_1)}\right)=+1$ gilt; z. B. hat $\zeta_1=-1$ diese Eigenschaft.

3. Es sei $\mathfrak{w}\mid\xi$, $\mathfrak{w}+2$ [4]). Wegen $(M_1,\xi)=0$ gilt dann (9) für jedes ζ_0, das nicht durch $\mathfrak{w}$ teilbar ist.

4. Es sei $\mathfrak{w}=\mathfrak{l}\mid 2$. Es gehe $\mathfrak{l}$ zu genau k-ter Potenz in 2 auf, und man betrachte ein System von $\varphi(\mathfrak{l}^{2k+1})$ inkongruenten nicht durch $\mathfrak{l}$ teilbaren Zahlen ζ_2 modulo $\mathfrak{l}^{2k+1}$. Nach Satz III der Einleitung genügen von diesen mindestens die Hälfte der Gleichung $\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)=+1$, und gleichfalls mindestens die Hälfte der Gleichung $\left(\frac{M_1,-\zeta_2}{\mathfrak{l}}\right)=+1$. Diese beiden Gleichungen lassen sich also dann und nur dann nicht durch dasselbe ζ_2 erfüllen, wenn für jedes ζ_2 mit $\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)=+1$ die Relation $\left(\frac{M_1,-\zeta_2}{\mathfrak{l}}\right)=-1$, mit $\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)=-1$ die Relation $\left(\frac{M_1,-\zeta_2}{\mathfrak{l}}\right)=+1$ erfüllt ist; d. h. für alle ζ_2 müßte

$$\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)\left(\frac{M_1,-\zeta_2}{\mathfrak{l}}\right)=-1$$

gelten. Hieraus folgte durch Zerlegung der Normenrestsymbole

$$\left(\frac{-1,-1}{\mathfrak{l}}\right)\left(\frac{-1,-\zeta_2}{\mathfrak{l}}\right)\left(\frac{M_1,-\zeta_2}{\mathfrak{l}}\right)=-1,$$

$$\left(\frac{-M_1,-\zeta_2}{\mathfrak{l}}\right)=-\left(\frac{-1,-1}{\mathfrak{l}}\right),\qquad \text{also konstant}=+1,$$

denn die linke Seite ist jedenfalls $+1$ für $\zeta_2=-1$. Daher wäre auch

$$\left(\frac{-1,-1}{\mathfrak{l}}\right)=-1. \tag{10}$$

Ich setze jetzt $\zeta_3=\xi\zeta_2$; dann wird

$$\left(\frac{-1,\zeta_3}{\mathfrak{l}}\right)=\left(\frac{-1,\xi}{\mathfrak{l}}\right)\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right),\qquad \left(\frac{M_1,-\zeta_3}{\mathfrak{l}}\right)=\left(\frac{M_1,-\xi}{\mathfrak{l}}\right)\left(\frac{M_1,\zeta_2}{\mathfrak{l}}\right). \tag{11}$$

[4]) Falls es solche $\mathfrak{w}$ gibt.

Hierin haben die beiden rechten Seiten den gleichen Wert; denn es ist $\left(\frac{-1,\xi}{\mathfrak{l}}\right)=\left(\frac{M_1,-\xi}{\mathfrak{l}}\right)$ und $\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)\left(\frac{M_1,\zeta_2}{\mathfrak{l}}\right)=\left(\frac{-M_1,\zeta_2}{\mathfrak{l}}\right)=+1$, da $\left(\frac{-M_1,-\zeta_2}{\mathfrak{l}}\right)$ für alle zu $\mathfrak{l}$ primen ζ_2, also auch für $-\zeta_2$, den Wert $+1$ hat. Damit also die linken Seiten von (11) beide den Wert $+1$ haben, genügt es, daß die Gleichung $\left(\frac{-1,\xi}{\mathfrak{l}}\right)=\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)$ erfüllt ist. Diese Gleichung ist aber sicher lösbar, mag nun $\left(\frac{-1,\xi}{\mathfrak{l}}\right)=+1$ oder $=-1$ sein, denn $\left(\frac{-1,\zeta_2}{\mathfrak{l}}\right)$ ist $=+1$ für $\zeta_2=+1$ und nach (10) $=-1$ für $\zeta_2=-1$. Ist $\mathfrak{l}^{k_0}$ die höchste Potenz von $\mathfrak{l}$, die in ξ aufgeht, so gilt dann

$$\left(\frac{-1,\zeta_4}{\mathfrak{l}}\right)=+1 \quad \text{und} \quad \left(\frac{M_1,-\zeta_4}{\mathfrak{l}}\right)=+1$$

für alle $\zeta_4\equiv\xi\zeta_2^2 \pmod{\mathfrak{l}^{2k+k_0+1}}$.

Damit ist festgestellt: Zu jedem Primideal $\mathfrak{w}\,|\,2M_1\xi$ gibt es eine ganze Zahl $\zeta_\mathfrak{w}$ von folgenden Eigenschaften:

I. Ist $\mathfrak{w}+2$, so sind für jedes $\zeta_0\equiv\zeta_\mathfrak{w} \pmod{\mathfrak{w}}$ die beiden Gleichungen (9) erfüllt; $\zeta_\mathfrak{w}$ ist nicht durch $\mathfrak{w}$ teilbar;

II. Ist $\mathfrak{w}=\mathfrak{l}\,|\,2$, so sind für jedes $\zeta_0\equiv\zeta_\mathfrak{w} \pmod{\mathfrak{w}^{k'}}$ die beiden Gleichungen (9) erfüllt. Hierin ist entweder $k'=2k+1$ und $\mathfrak{l}+\zeta_\mathfrak{w}$; oder $\zeta_\mathfrak{w}$ und ξ enthalten genau dieselbe Potenz $\mathfrak{l}^k$ von $\mathfrak{l}$, und es ist $k'=2k+k_0+1$.

Die den verschiedenen $\mathfrak{w}$ entsprechenden Kongruenzen lassen sich nun gleichzeitig durch eine Zahl ζ_0 befriedigen, und zwar darf man dabei fordern, daß ζ_0 total positiv ist und mit $2M_1\xi$ höchstens solche Primteiler gemeinsam hat, die auch in 2 aufgehen, und zwar in keiner höheren Potenz, als sie in ξ auftreten. Dieses ζ_0 genügt sämtlichen Gleichungen (9). Dieselbe Eigenschaft hat jede total positive Zahl $\zeta\equiv\zeta_0 \pmod{8M_1\xi}$. Von dem Ideal (ζ_0) spalte ich den größten zu 2 relativ primen Faktor $\mathfrak{b}$ ab. Dann ist auch $(\mathfrak{b},8M_1\xi)=\mathfrak{o}$; $\mathfrak{b}$ ist also Repräsentant einer Idealklasse modulo $8M_1\xi$. Nach Satz V der Einleitung enthält diese Idealklasse ein Primideal $\mathfrak{z}$. Dann ist $\frac{(\zeta_0)}{\mathfrak{b}}\mathfrak{z}$ ein Hauptideal (ζ) mit $\zeta\equiv\zeta_0 \pmod{8M_1\xi}$ und $\frac{\zeta}{\zeta_0}\succ 0$, so daß wegen $\zeta_0\succ 0$ auch $\zeta\succ 0$ ist. Die Zahl ζ erfüllt also die Bedingungen (9) und hat außer etwaigen in 2 aufgehenden Primfaktoren nur den Primteiler $\mathfrak{z}$, der nicht in $8M_1\xi$ enthalten ist. Aus dem Reziprozitätsgesetz (Satz I der Einleitung) folgt nun genau wie beim Beweise von Hilfssatz 1, daß auch

$$\left(\frac{-1,\zeta}{\mathfrak{z}}\right)=+1 \quad \text{und} \quad \left(\frac{M_1,-\zeta}{\mathfrak{z}}\right)=+1$$

gilt. Mit Rücksicht auf (9) gelten also die Gleichungen

$$\left(\frac{-1,\zeta}{\mathfrak{w}'}\right)=+1,\quad \left(\frac{M_1,-\zeta}{\mathfrak{w}'}\right)=+1 \tag{12}$$

für *alle* Primideale $\mathfrak{w}'$ und für $\mathfrak{w}'=1^{(i)}$. Nach Satz II der Einleitung sind also die beiden Diophantischen Gleichungen

$$\zeta u^2-v^2=w^2 \quad \text{und} \quad -\zeta u_1^2+M_1 v_1^2=w_1^2 \tag{13}$$

in ganzen Zahlen u, v, w und u_1, v_1, w_1 aus K lösbar, die nicht alle Null sind. Da -1, $\pm\zeta$, M_1, $\frac{M_1}{\zeta}$ keine Quadratzahlen des Körpers K sind (vgl. Voraussetzung 1 dieses Paragraphen), so sind alle sechs Zahlen $u, \ldots, w_1$ von 0 verschieden; insbesondere ist $u\neq 0$, $u_1\neq 0$. Aus (13) folgt

$$-\zeta u^2=f(0,w,v),\quad -\zeta u_1^2=f_1(w_1,v_1,0). \tag{14}$$

Nach Satz V der Einleitung gibt es unendlich viele nicht assoziierte Primzahlen $Z\equiv 1 \pmod{8\xi\zeta}$. Dann ist aber

$$\left(\frac{Z,\xi\zeta}{\mathfrak{w}}\right)=+1 \tag{15}$$

für alle $\mathfrak{w}\,|\,2\xi\zeta$ und $\mathfrak{w}=1^{(i)}$ [5]), also gilt (15) nach Satz I der Einleitung auch für $\mathfrak{w}=(Z)$ und folglich für jedes $\mathfrak{w}$. Nach Satz II ist daher die Gleichung

$$ZU^2+\xi\zeta V^2=W^2 \tag{16}$$

in nicht sämtlich verschwindenden ganzen Zahlen U, V, W aus K lösbar; und da $\xi\zeta$ nicht das Quadrat einer Körperzahl ist, so ist $U\neq 0$.

Ferner folgt aus (12) und (15) für jedes $\mathfrak{w}$

$$\left(\frac{Z,\xi\zeta}{\mathfrak{w}}\right)\left(\frac{-1,\zeta}{\mathfrak{w}}\right)\left(\frac{-1,\xi}{\mathfrak{w}}\right)\left(\frac{M_1,-\xi}{\mathfrak{w}}\right)\left(\frac{M_1,-\zeta}{\mathfrak{w}}\right)=+1\cdot+1\cdot\varepsilon_{\mathfrak{w}}\cdot\varepsilon_{\mathfrak{w}}\cdot+1=+1,$$

andererseits hat die linke Seite dieser Gleichung nach Zusammensetzung den Wert $\left(\frac{-M_1 Z,\xi\zeta}{\mathfrak{w}}\right)$, so daß mit Rücksicht auf Satz II die Gleichung

$$-M_1 Z U_1^2+\xi\zeta V_1^2=W_1^2 \tag{17}$$

mit $U_1\neq 0$ lösbar ist.

Aus (13) und (16) folgt

$$\begin{aligned} Z(uU)^2&=(uW)^2-\xi\zeta(uV)^2=(uW)^2-\xi(vV)^2-\xi(wV)^2\\ &=F(uW,vV,-wV), \end{aligned} \tag{18}$$

---

[5]) Man braucht an dieser Stelle nicht die Landausche Verschärfung des Heckeschen Satzes, da wegen $\xi\zeta>0$ das Symbol $\left(\frac{\alpha,\xi\zeta}{1^{(i)}}\right)=+1$ für jedes $\alpha\neq 0$ ist.

und aus (8), (13) und (17)

$$(19)\quad Z(u_1 U_1 M_1)^2 = -M_1 u_1^2 W_1^2 + \xi\zeta M_1 u_1^2 V_1^2 = -M_1 u_1^2 W_1^2 - \xi w_1^2 M_1 V_1^2$$
$$+\xi M_1^2 v_1^2 V_1^2 = \xi(v_1 V_1 M_1)^2 - M_1'(w_1 V_1 M_1)^2 - M_1(u_1 W_1)^2$$
$$+N_1^2 M_1(w_1 V_1)^2 = \xi(v_1 V_1 M_1)^2 - M_1'(w_1 V_1 M_1)^2 - M_1(u_1 W_1 + w_1 V_1 N_1)^2$$
$$+2N_1(w_1 V_1 M_1)(u_1 W_1 + w_1 V_1 N_1) = F_1(v_1 V_1 M_1, -w_1 V_1 M_1, u_1 W_1 + w_1 V_1 N_1).$$

Wegen der Homogenität von (16) kann $W = wW'$ durch w teilbar angenommen werden. Setze ich dann $\beta_1 = -V$, $\beta_2 = 0$, $\beta_3 = -uW'$, $\gamma_1 = 0$, $\gamma_2 = w$, $\gamma_3 = v$, so ist $\beta_2\gamma_3 - \beta_3\gamma_2 = uW$, $\beta_3\gamma_1 - \beta_1\gamma_3 = vV$, $\beta_1\gamma_2 - \beta_2\gamma_1 = -wV$. Folglich sind wegen (14) und (18) die Zahlen $-\zeta u^2$ und $Z(uU)^2$ durch f und F simultan darstellbar. Ferner mache ich die Annahme $w_1 | W_1 = w_1 W_1'$ und setze $\beta_1 = 0$, $\beta_2 = -u_1 W_1' - V_1 N_1$, $\beta_3 = -V_1 M_1$, $\gamma_1 = w_1$, $\gamma_2 = v_1$, $\gamma_3 = 0$; dann ist $\beta_2\gamma_3 - \beta_3\gamma_2 = v_1 V_1 M_1$, $\beta_3\gamma_1 - \beta_1\gamma_3 = -w_1 V_1 M_1$, $\beta_1\gamma_2 - \beta_2\gamma_1 = u_1 W_1 + w_1 V_1 N_1$, so daß nach (14) und (19) die Zahlen $-\zeta u_1^2$ und $Z(u_1 U_1 M_1)^2$ durch f_1 und F_1 simultan darstellbar sind.

Folglich gilt wegen (3) eine Identität

$$f(x) = \frac{P^2}{-\zeta} + \frac{Q^2}{-\zeta Z} + \xi\frac{R^2}{Z},$$

wo P, Q, R aus x_1, x_2, x_3 durch eine lineare umkehrbare Substitution S mit Koeffizienten aus dem Körper K hervorgehen. Ebenso gilt

$$f_1(x) = \frac{P_1^2}{-\zeta} + \frac{Q_1^2}{-\zeta Z} + \xi\frac{R_1^2}{Z},$$

wo P_1, Q_1, R_1 aus x_1, x_2, x_3 ebenfalls durch eine lineare in K rationale Substitution S_1 hervorgehen. Daher besitzt die Substitution $S^{-1}S_1 = T$ Koeffizienten aus K und führt die Form f in f_1 über; und da f und f_1 dieselbe Determinante ξ haben, so ist offenbar $T| = \pm 1$. Damit ist Hilfssatz 2. bewiesen.

§ 3.

Hilfssatz 3. ξ sei eine ganze total positive Zahl des Körpers K. $-\xi$ sei nicht das Quadrat einer Körperzahl, so daß $K(\sqrt{-\xi})$ nicht mit K identisch ist. Ist dann die Relativdiskriminante von $K(\sqrt{-\xi})$ durch jeden Primfaktor von 2 teilbar, so läßt sich ξ als Summe von drei Quadraten von Körperzahlen darstellen.

Beweis. 1. Die Zahl -1 sei in K als Summe von zwei Quadraten darstellbar:

$$-1 = a^2 + b^2.$$

Dann ist sogar identisch in ξ

$$\xi = \left(\frac{\xi+1}{2}\right)^2 + \left(a\frac{\xi-1}{2}\right)^2 + \left(b\frac{\xi-1}{2}\right)^2. \tag{20}$$

2. Die Zahl -1 sei nicht Summe von zwei Quadraten. Die drei Voraussetzungen des vorigen Paragraphen sind erfüllt. Nach Hilfssatz 2 kann f rational in f_1 transformiert werden, und da f_1 die Zahl $f_1(1,0,0)=1$ darstellt, so gibt es insbesondere drei Zahlen t_1, t_2, t_3 aus K, so daß

$$f(t_1, t_2, t_3) = \xi t_1^2 - t_2^2 - t_3^2 = 1$$

ist. Da hierin $t_1 \neq 0$ ist, so folgt die gesuchte Darstellung

$$\xi = \left(\frac{1}{t_1}\right)^2 + \left(\frac{t_2}{t_1}\right)^2 + \left(\frac{t_3}{t_1}\right)^2.$$

Hilfssatz 4. Es sei $\mathfrak{l}$ ein Primfaktor von 2. Es gibt eine ganze Zahl ϱ des Körpers K, die als Summe von vier Quadraten darstellbar ist und von den Teilern der 2 nur das Primideal $\mathfrak{l}$, und zwar genau in erster Potenz enthält.

Beweis. 1. $\mathfrak{l}$ gehe in 2 zu ungerader Potenz auf. Dann läßt sich setzen:

$$2 = \varkappa\alpha^2,$$

wo $\varkappa$ eine ganze Zahl aus K bedeutet, die jeden Primfaktor von 2 enthält, von diesen aber das Primideal $\mathfrak{l}$ nur in erster Potenz. Bedeutet nun μ irgendeine ganze Zahl mit $(\mu, 2)=\mathfrak{l}$, so ist

$$\varrho = \varkappa + \mu^2 = \left(\frac{1}{\alpha}\right)^2 + \left(\frac{1}{\alpha}\right)^2 + \mu^2 + 0^2$$

als Summe von vier Quadraten darstellbar, und es gilt $(\varrho, 4)=\mathfrak{l}$.

2. $\mathfrak{l}$ gehe in 2 in gerader Potenz auf. Dann setze ich

$$2 = \nu\beta^2,$$

wo ν eine ganze nicht durch $\mathfrak{l}$ teilbare Zahl bedeutet. Es sei λ eine ganze Zahl, in der genau die erste Potenz von $\mathfrak{l}$ aufgeht; dann gibt es zwei ganze Zahlen γ_1 und γ_2 mit $\mathfrak{l}\nmid\gamma_1$, so daß

$$\nu \equiv \gamma_1 + \gamma_2\lambda \pmod{\mathfrak{l}^2}$$

gilt. Durchläuft δ ein System zu $\mathfrak{l}$ primer modulo $\mathfrak{l}$ inkongruenter Zahlen, so sind auch die Zahlen δ^2 alle modulo $\mathfrak{l}$ verschieden; denn aus $\delta^2 \equiv \delta'^2 \pmod{\mathfrak{l}}$ folgt $\delta \equiv \pm\delta' \equiv \delta' \pmod{\mathfrak{l}}$. Jedes δ ist also quadratischer Rest nach $\mathfrak{l}$. Man kann daher

$$\gamma_1 \equiv \delta_1^2 \pmod{\mathfrak{l}}, \qquad \nu \equiv \delta_1^2 + \gamma_2'\lambda \pmod{\mathfrak{l}^2}$$

setzen. Ist nun hierin $\mathfrak{l}\mid\gamma_2'$, so folgt $\nu \equiv \delta_1^2 \pmod{\mathfrak{l}^2}$; ist aber $\mathfrak{l}\nmid\gamma_2'$, so gibt es ein δ_2 derart, daß $\gamma_2' \equiv \delta_2^2 \pmod{\mathfrak{l}}$, also $\nu \equiv \delta_1^2 + \delta_2^2\lambda \pmod{\mathfrak{l}^2}$

ist. Es bedeute $\mathfrak{l}^k$ die in 2 aufgehende Potenz von $\mathfrak{l}$; dann ist im ersteren Fall $2 \equiv (\delta_1\beta)^2 \pmod{\mathfrak{l}^{k+2}}$. Setze ich

$$\varrho_1 = 1^2 + (1+\lambda)^2 + (\delta_1\beta)^2 + \lambda^2, \tag{21}$$

so gilt in diesem ersteren Fall wegen $\mathfrak{l}^{k+2} \mid 4$

$$\varrho_1 = 2 + 2\lambda + 2\lambda^2 + (\delta_1\beta)^2 \equiv 4 + 2\lambda + 2\lambda^2 \equiv \lambda(\delta_1\beta)^2 \pmod{\mathfrak{l}^{k+2}}.$$

Im letzteren Fall ist $2 \equiv (\delta_1\beta)^2 + \lambda(\delta_2\beta)^2 \pmod{\mathfrak{l}^{k+2}}$; dann setze ich

$$\varrho_2 = 1^2 + 1^2 + (\delta_1\beta)^2 + 0^2, \tag{22}$$

und es wird

$$\varrho_2 \equiv 2(\delta_1\beta)^2 + \lambda(\delta_2\beta)^2 \equiv \lambda(\delta_2\beta)^2 \pmod{\mathfrak{l}^{k+2}}.$$

Man setze nun $\varrho_3 = \frac{\varrho_n}{(\delta_n\beta)^2}$ mit $n=1$ im ersten, $n=2$ im letzten Fall. Dann ist nach (21) und (22) die Zahl ϱ_3 als Summe von vier Quadraten darstellbar und enthält, in gekürzter Form geschrieben, im Nenner das Primideal $\mathfrak{l}$ überhaupt nicht, im Zähler dagegen genau in erster Potenz. Also gibt es auch eine ganze Zahl ϱ_4 von dieser Eigenschaft:

$$\varrho_4 = \sum_{\nu=1}^{4} \eta_\nu^2, \qquad (\varrho_4, \mathfrak{l}^2) = \mathfrak{l}.$$

Nun sei τ eine ganze Zahl, die durch jeden etwaigen von $\mathfrak{l}$ verschiedenen Primteiler $\mathfrak{l}'$ von 2, aber nicht durch $\mathfrak{l}$ selbst teilbar ist; ferner soll im Nenner von $\tau\eta_1$ kein $\mathfrak{l}'$ aufgehen. Endlich werde eine ganze Zahl τ' so bestimmt, daß $\mathfrak{l} \mid \tau'$, $\mathfrak{l}' \nmid \tau'$ und $\tau\tau'\eta_1$ eine ganze Zahl ist. Setze ich dann

$$\varrho = (\eta_1\tau + \tau')^2 + \sum_{\nu=2}^{4} (\eta_\nu\tau)^2,$$

so ist $\varrho = \varrho_4\tau^2 + 2\tau\tau'\eta_1 + \tau'^2$ eine ganze Zahl und

$$\varrho \equiv \varrho_4\tau^2 \pmod{\mathfrak{l}^2}, \qquad \varrho \equiv \tau'^2 \not\equiv 0 \pmod{\mathfrak{l}'}, \qquad \text{also} \qquad (\varrho, 4) = \mathfrak{l};$$

ϱ erfüllt also die Forderungen des Hilfssatzes.

Hauptsatz (Satz 1). Jede total positive Zahl aus K läßt sich als Summe von vier Quadratzahlen aus K darstellen.

Beweis. Es sei ϑ irgendeine total positive Zahl $\neq 0$ aus K. Ich wähle eine ganze Zahl $\vartheta_1 \neq 0$ derart, daß $\vartheta\vartheta_1^2$ ganz ist, und setze $4\vartheta\vartheta_1^2 = \vartheta_2$; dann ist $\vartheta_2 \succ 0$. Die verschiedenen Primfaktoren $\mathfrak{l}, \mathfrak{l}', \ldots$ von 2 mögen in ϑ_2 genau in den Potenzen $\mathfrak{l}^c, \mathfrak{l}'^{c'}, \ldots$ auftreten. Hierbei sind wegen $4 \mid \vartheta_2$ die Exponenten $c, c', \ldots > 0$. Es mögen $\varrho, \varrho', \ldots$ die zu $\mathfrak{l}, \mathfrak{l}', \ldots$ gehörende Bedeutung des ϱ von Hilfssatz 4 haben. Dann läßt sich die

Zahl $\frac{\vartheta_2}{\varrho^{c-1}\varrho'^{c'-1}\dots}$ in der Form $\frac{\vartheta_3}{\vartheta_4}$ schreiben, wo ϑ_3, ϑ_4 ganz sind, ϑ_4 zu 2 teilerfremd ist und ϑ_3 jedes der Primideale $\mathfrak{l}, \mathfrak{l}', \dots$ in genau erster Potenz enthält. Nun setze ich

$$\vartheta_3 \vartheta_4 = \xi.$$

Dann ist $\xi \succ 0$, weil $\vartheta_2, \varrho, \varrho', \dots$ sämtlich $\succ 0$ sind. Ferner ist $(\xi, 4) = \mathfrak{l}\mathfrak{l}' \dots$; $-\xi$ ist also keine Quadratzahl, und jedes der Primideale $\mathfrak{l}, \mathfrak{l}', \dots$ teilt nach Satz IV der Einleitung die Relativdiskriminante des relativquadratischen Körpers $K(\sqrt{-\xi})$. Folglich läßt sich nach Hilfssatz 3 die ganze Zahl ξ als Summe von drei Quadraten, also a fortiori als Summe von vier Quadraten darstellen. Nun ist aber

$$\vartheta = \frac{\xi}{(2\vartheta_1\vartheta_4)^2} \varrho^{c-1}\varrho'^{c'-1} \dots;$$

und hierin sind nach Hilfssatz 4 die Zahlen $\varrho, \varrho', \dots$ als Summen von vier Quadraten darstellbar. Nach der bekannten Identität von Lagrange läßt sich also auch das Produkt $\xi\varrho^{c-1}\varrho'^{c'-1}\dots$ in vier Quadrate zerlegen, also auch die gegebene Zahl $\vartheta \neq 0$.

Für $\vartheta = 0$ aber ist der Satz trivial.

Anmerkungen. 1. In der Zerlegung $\vartheta = \sum_{\nu=1}^{4} \eta_\nu^2$ einer total positiven *ganzen* Zahl ϑ in vier Quadrate können die Basen η_ν nicht immer ganzzahlig gewählt werden. Liegt z. B. ein quadratischer Zahlkörper $K(\sqrt{m})$ mit quadratfreiem $m \equiv 3 \pmod 4$ vor, so hat bekanntlich jede ganze Zahl desselben die Form $\eta_\nu = a_\nu + b_\nu\sqrt{m}$ mit ganzen rationalen a_ν, b_ν; dann ist aber in $\sum_{\nu=1}^{4} \eta_\nu^2$ der Koeffizient von $\sqrt{m}$ durch 2 teilbar, was natürlich nicht für jedes ϑ der Fall ist. Es dürfte recht schwierig sein, zu entscheiden, ob in allen Zahlkörpern die bei der Zerlegung der total positiven Zahlen in vier Quadrate auftretenden Nenner oder auch nur deren Primidealteiler aus einem endlichen Wertevorrat gewählt werden können oder nicht (vgl. § 6).

2. Es gibt Körper, in denen jede Zahl in zwei Quadrate zerlegt werden kann; z. B. hat jeder Körper diese Eigenschaft, welcher $\sqrt{-1}$ enthält.

Hilfssatz 5. Es sei $\xi \succ 0$. Es sei m eine natürliche Zahl, a_1 und a_2 zwei rationale Zahlen, $0 \leqq a_1 < a_2$. Dann gibt es eine total positive Zahl α des Körpers K von ξ, so daß $a_1 \prec \alpha^m \xi \prec a_2$ [6]) ist.

---

[6]) Dies bedeutet: $a_2 - \alpha^m\xi \succ 0$, $\alpha^m\xi - a_1 \succ 0$.

Beweis. Es seien $K(\xi^{(1)}), \ldots, K(\xi^{(r)})$ sämtliche reellen konjugierten Körper ($r \geqq 1$, da sonst nichts zu beweisen wäre). Es gibt ein reellzahliges Polynom $P(x)$ vom Grade $\leqq r-1$, das für $x = \xi^{(\nu)}$ $(\nu = 1, \ldots, r)$ den Wert $\sqrt[m]{\frac{a_1+a_2}{2\,\xi^{(\nu)}}}$ hat, wo die Wurzel positiv zu nehmen ist. Dann ist

$$P(\xi^{(\nu)})^m \xi^{(\nu)} = \frac{a_1+a_2}{2},$$

also $< a_2$ und $> a_1$. Ich kann nun die Koeffizienten von $P(x)$ durch benachbarte rationale Zahlen ersetzen, so daß für ein so entstehendes rationalzahliges Polynom $R(x)$ auch noch

$$a_1 < R(\xi^{(\nu)})^m \xi^{(\nu)} < a_2, \qquad R(\xi^{(\nu)}) > 0 \qquad (\nu = 1, \ldots, r)$$

gilt; dann erfüllt $R(\xi) = \alpha$ die Forderung des Hilfssatzes.

Satz 2. Es sei m eine natürliche Zahl. Jede total positive Zahl eines algebraischen Zahlkörpers K läßt sich als Summe einer *festen* nur von m und nicht von K abhängigen Anzahl m-ter Potenzen von *total positiven* Zahlen des Körpers darstellen.

Beweis. Hilbert hat folgende Vermutung von Hurwitz bewiesen: Es seien m und r zwei natürliche Zahlen. Dann gibt es eine natürliche Zahl N, rationale Zahlen $a_{1\lambda}, \ldots, a_{r\lambda}$ $(\lambda = 1, \ldots, N)$ und positive rationale Zahlen $\varrho_1, \ldots, \varrho_N$, die nur von m und r abhängen, so daß identisch in $x_1, \ldots, x_r$ gilt

$$(23) \qquad (x_1^2 + \ldots + x_r^2)^m = \sum_{\lambda=1}^{N} \varrho_\lambda (a_{1\lambda} x_1 + \ldots + a_{r\lambda} x_r)^{2m}\ ^{7}).$$

Hierin sei speziell $r = 5$. Man ersetze in (23) die Zahl m durch $m+1$ und differentiiere zweimal nach x_1; dann wird

$$(24) \qquad (x_1^2 + \ldots + x_5^2)^m + 2m x_1^2 (x_1^2 + \ldots + x_5^2)^{m-1} = \sum_{\lambda=1}^{N} (2m+1) \varrho_\lambda a_{1\lambda}^2 (a_{1\lambda} x_1 + \ldots + a_{5\lambda} x_5)^{2m}.$$

Nun führe man an Stelle der x neue vier Reihen von Variablen $x^{(\varkappa)}$ $(\varkappa = 1, \ldots, 4)$ ein, die der Bedingung

$$(25) \qquad x_1^{(\varkappa)2} + \ldots + x_5^{(\varkappa)2} = 1$$

genügen sollen. Dann liefert (24) durch Addition der vier entsprechenden Identitäten

$$2 + m \sum_{\varkappa=1}^{4} x_1^{(\varkappa)2} = \sum_{\varkappa=1}^{4} \sum_{\lambda=1}^{N} \frac{2m+1}{2} \varrho_\lambda a_{1\lambda}^2 (a_{1\lambda} x_1^{(\varkappa)} + \ldots + a_{5\lambda} x_5^{(\varkappa)})^{2m}.$$

---

[7]) Der einfachste elementare Beweis der Existenz einer solchen Identität findet sich in der unten zitierten Arbeit von Stridsberg.

Bedeutet q den Hauptnenner der N rationalen Zahlen $\frac{2m+1}{2}\varrho_\lambda a_{1\lambda}^2$, so ist $\frac{2m+1}{2}\varrho_\lambda a_{1\lambda}^2 q^{2m}$ ganz rational und $\geqq 0$. Folglich gilt

$$2+m\sum_{\varkappa=1}^{4} x_1^{(\varkappa)2} = \sum_{\nu=1}^{N'} X_\nu^{2m}, \tag{26}$$

wo X_ν eine lineare rationalzahlige Funktion von $x_1^{(\varkappa)},\ldots,x_5^{(\varkappa)}$ $(\varkappa=1,\ldots,4)$ bedeutet und $N'=2(2m+1)Nq^{2m}\max\limits_{\lambda=1,\ldots,N}(\varrho_\lambda a_{1\lambda}^2)$ ist. N' hängt nur von m ab.

Nun sei ξ eine total positive Zahl aus K. Nach Hilfssatz 5 gibt es ein $\alpha>0$, so daß $2<\alpha^m\xi<3$ ist; dann ist also die Zahl $\frac{\alpha^m\xi-2}{m}>0$ und <1. Da sie >0 ist, so läßt sie nach dem Hauptsatz eine Zerlegung in vier Quadrate zu; es seien $x_1^{(\varkappa)}$ $(\varkappa=1,\ldots,4)$ die Basen dieser Quadrate:

$$\frac{\alpha^m\xi-2}{m}=\sum_{\varkappa=1}^{4} x_1^{(\varkappa)2}. \tag{27}$$

Da sie <1 ist, so ist jede der vier Zahlen $1-x_1^{(\varkappa)2}>0$; es gibt daher nach dem Hauptsatz für jedes $\varkappa$ vier Zahlen $x_2^{(\varkappa)}$, $x_3^{(\varkappa)}$, $x_4^{(\varkappa)}$, $x_5^{(\varkappa)}$ des Körpers, welche (25) Genüge leisten. Aus (26) und (27) folgt aber

$$\xi=\sum_{\nu=1}^{N'}\left(\frac{X_\nu^2}{\alpha}\right)^m \quad \text{mit} \quad \frac{X_\nu^2}{\alpha}>0,$$

q. e. d.

Anmerkungen. 1. Satz 2 ist für $m=2$ nicht im Hauptsatz enthalten, da dort die Basen der Quadrate nicht total positiv zu sein brauchen.

2. Daß die Hilbertsche Methode zur Lösung des Waringschen Problems, wie sie beim Beweise von Satz 2 benutzt wurde, sich abkürzen ließ, liegt natürlich daran, daß Ganzzahligkeit nicht gefordert wird. Aus demselben Grunde erklärt sich die sonderbare Tatsache, daß der Satz für $m=3$ ganz leicht und auf dem elementarsten Wege bewiesen werden kann. Nach Le Besgue gilt nämlich folgende Identität:

$$p=\left(\frac{p}{6q^2}\right)^3\{(2-a)^3-a^3(b-1)^3+b^3(c-1)^3+c^3\}, \tag{28}$$

wo $a=1+\frac{6q^3}{p}$, $b=2-\frac{3}{1+a^3}$, $c=2-\frac{3}{1+b^3}$ gesetzt ist. Hierin sind die Kuben positiv für $c>1$, $b>1$, $a<2$, und diese Bedingungen liefern sukzessive

$$b>\sqrt[3]{2},\qquad a>\sqrt[3]{\frac{1+\sqrt[3]{2}}{2-\sqrt[3]{2}}},\qquad \sqrt[3]{\frac{1-\sqrt[3]{2}}{2-\sqrt[3]{2}}}<1+\frac{6q^3}{p}<2; \tag{29}$$

und in der letzten Ungleichung ist $\sqrt[3]{\frac{1+\sqrt[3]{2}}{2-\sqrt[3]{2}}} < 2$ [8]). Ist nun $p \neq 0$ eine total positive Zahl des Körpers K, so wähle man nach Hilfssatz 5 eine total positive Zahl q aus K derart, daß $r < q^3 \frac{6}{p} < 1$ ist, wo r einen echten rationalen Bruch $> \sqrt[3]{\frac{1+\sqrt[3]{2}}{2-\sqrt[3]{2}}} - 1$ bedeutet. Für dieses q gelten die Ungleichungen (29); und (28) liefert eine Zerlegung von p in vier total positive Kuben.

3. Landau hat auf elementare Art bewiesen, daß jede total positive Zahl als Summe von Quadratzahlen des Körpers dargestellt werden kann. Dies läßt sich für den Fall eines total reellen Körpers fast unmittelbar in Evidenz setzen. Ist nämlich ξ total reell und total positiv, so sind in der irreduziblen Gleichung für ξ

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - + \ldots + (-1)^n a_n = 0$$

die rationalen Zahlen $a_1, \ldots, a_n$ sämtlich > 0. Nun ist

$$\xi(a_{n-1} + a_{n-3}\xi^2 + \ldots) = a_n + a_{n-2}\xi^2 - a_{n-4}\xi^4 + \ldots;$$

oder, wenn $a_{n-1} + a_{n-3}\xi^2 - \ldots = \nu$ gesetzt wird,

$$\xi = \frac{1}{\nu^2}(a_{n-1} - a_{n-3}\xi^2 + \ldots)(a_n - a_{n-2}\xi^2 + \ldots) = \frac{1}{\nu^2}(b_0 + b_1\xi^2 + b_2\xi^4 + \ldots),$$

wo die Zahlen $b_0, b_1, b_2, \ldots$ positiv rational sind. Ihre Anzahl ist, da $\xi^{2(n-1)}$ die höchste rechts auftretende Potenz von ξ^2 ist, genau n; jede von ihnen zerfällt nach dem Satz von Lagrange in vier Quadrate; folglich läßt sich ξ in $4n$ Quadrate zerlegen.

§ 4.

Aus dem Hauptsatz hat Hilbert gefolgert, daß jedes rationalzahlige positiv definite Polynom sich als Quotient von Quadratsummen rationalzahliger Polynome darstellen läßt; und Landau hat sogar gezeigt, daß man jedes solche Polynom als Summe von acht Quadraten rationalzahliger Polynome schreiben kann. Es ist leicht, diesen Satz auf trigonometrische Polynome zu übertragen.

---

[8]) Es ist $54 < 125$, $3\sqrt[3]{2} < 5$, $1 + \sqrt[3]{2} < 8(2 - \sqrt[3]{2})$, $\sqrt[3]{\frac{1+\sqrt[3]{2}}{2-\sqrt[3]{2}}} < 2$.

Satz 3. Es sei

$$f(\varphi) = \sum_{\nu=0}^{n} a_\nu \cos \nu\varphi + b_\nu \sin \nu\varphi$$

ein trigonometrisches Polynom mit rationalen Koeffizienten a_ν, b_ν. $f(\varphi)$ sei nicht-negativ definit, d. h. für alle reellen φ sei $f(\varphi) \geqq 0$. Dann gibt es eine Darstellung von $f(\varphi)$ als Summe von acht Quadraten rationalzahliger trigonometrischer Polynome in $\frac{\varphi}{2}$:

$$(30) \quad f(\varphi) = \sum_{\lambda=1}^{8} g_\lambda\left(\frac{\varphi}{2}\right)^2, \qquad g_\lambda\left(\frac{\varphi}{2}\right) = \sum_{\nu=0}^{n} c_\nu^{(\lambda)} \cos \nu \frac{\varphi}{2} + d_\nu^{(\lambda)} \sin \nu \frac{\varphi}{2}.$$

Beweis. Ich setze $\operatorname{tg} \frac{\varphi}{2} = x$, dann ist $\cos\varphi = \frac{1-x^2}{1+x^2}$, $\sin\varphi = \frac{2x}{1+x^2}$, und $f(\varphi)(1+x^2)^n$ geht über in ein rationalzahliges Polynom vom Grade $2n$, das für keinen reellen Wert seiner Variablen x negativ ist. Nach dem erwähnten Landauschen Satze ist daher

$$f(\varphi)(1+x^2)^n = \sum_{\lambda=1}^{8} h_\lambda(x)^2,$$

wo $h_\lambda(x)$ ein rationalzahliges Polynom n-ten Grades in x bedeutet. Nun ist aber $\frac{1}{1+x^2} = \cos^2 \frac{\varphi}{2}$, also $f(\varphi) = \sum_{\lambda=1}^{8} \left\{\cos^n \frac{\varphi}{2} h_\lambda\left(\operatorname{tg} \frac{\varphi}{2}\right)\right\}^2$. Die Funktion $\cos^n \frac{\varphi}{2} h_\lambda\left(\operatorname{tg} \frac{\varphi}{2}\right)$ ist ein homogenes Polynom n-ten Grades in $\cos \frac{\varphi}{2}$ und $\sin \frac{\varphi}{2}$, das die Form $g_\lambda\left(\frac{\varphi}{2}\right)$ aus (30) erhält, wenn jedes Produkt $\cos^\varkappa \frac{\varphi}{2} \sin^{n-\varkappa} \frac{\varphi}{2}$ $(\varkappa = 0, \ldots, n)$ linear und rationalzahlig durch $\cos \nu \frac{\varphi}{2}$ und $\sin \nu \frac{\varphi}{2}$ $(\nu = 0, \ldots, n)$ ausgedrückt wird, was bekanntlich möglich ist.

Nach den oben genannten Sätzen von Hilbert und Landau kann man jedes definite Polynom in eine solche Form setzen, daß seine charakteristische Eigenschaft ausgedrückt wird. Etwas Analoges läßt sich für Polynome bewirken, die für alle positiven Werte der Variablen selbst positiv sind.

Satz 4. Es sei $f(x)$ ein rationalzahliges Polynom n-ten Grades, das für alle positiven x selbst positiv ist. Dann gilt eine Darstellung

$$(31) \quad f(x) = c \frac{\prod_{\nu=1}^{n_1} (x + q_\nu(x))}{\prod_{\nu=1}^{n_2} (x + q_\nu^*(x))},$$

wo c eine rationale Zahl >0, $q_\nu(x)$ und $q_\nu^*(x)$ Summen von vier Quadraten rationalzahliger Polynome in x bedeuten. Deren Grade, sowie die Zahlen n_1 und n_2 hängen nur von n ab.

Beweis. Jeder irreduzible Faktor von $f(x)$ ist >0 für $x>0$; ferner hat das Produkt zweier Ausdrücke von der Form der rechten Seite von (31) wieder diese Form. Ich darf daher $f(x)$ als irreduzibel voraussetzen. Es sei $f(\xi)=0$; dann ist nach Voraussetzung $-\xi$ total positiv. Nach dem Hauptsatze gibt es also vier rationalzahlige Polynome $g_\nu(x)$ $(\nu=1,\ldots,4)$ vom Grade $n-1$, so daß $-\xi=\sum_{\nu=1}^{4} g_\nu(\xi)^2$ ist. Daraus folgt

$$x+\sum_{\nu=1}^{4} g_\nu(x)^2 = f(x)f_1(x), \tag{32}$$

wo $f_1(x)$ ein rationalzahliges Polynom ist, und zwar vom Grade $n-2$ für $n\geqq 2$, vom Grade 0 für $n=1$. $f_1(x)$ hat also kleineren Grad als $f(x)$; ferner ist nach (32) $f_1(x)>0$ für $x>0$. Ist nun $f_1(x)$ nicht konstant, also $n>2$, so wende man auf jeden der endlich vielen irreduziblen Faktoren von $f_1(x)$ dieselben Schlüsse an. So ergibt sich mit Rücksicht auf (32) nach endlich vielen Schritten für $f(x)$ ein Ausdruck der Form (31).

Für eine weitere Anwendung des Hauptsatzes gebrauche ich einen Hilfssatz, der an und für sich Interesse besitzt und mit gewissen Sätzen von Laguerre zusammenhängt. Ein Beweis desselben, der von E. Meißner gegeben worden ist, wird durch geometrische Betrachtungen erschwert; daher möchte ich ihn hier rein algebraisch beweisen[9]). Der Satz lautet:

Hilfssatz 6. Jedes reellzahlige Polynom $f(x)$, das für alle positiven x positiv ist, ist Quotient zweier positivzahliger[10]) Polynome.

Beweis. Es gilt eine Zerlegung

$$f(x)=a\prod_{\nu=1}^{r_1}(x-x_\nu)\prod_{\nu=1}^{r_2}\varphi_\nu(x);$$

hierin bedeutet a eine Zahl >0, r_1 die Anzahl der reellen Wurzeln von $f(x)$, $x_1,\ldots,x_{r_1}$ diese Wurzeln selbst, $2r_2$ die Anzahl der imaginären Wurzeln von $f(x)$, $\varphi_\nu(x)$ ein reellzahliges definites quadratisches Polynom der Form $x^2-\alpha_\nu x+\beta_\nu$. r_1 oder r_2 können auch 0 sein; dann fallen die entsprechenden Faktoren eben fort. Nach Voraussetzung ist $f(x)>0$,

[9]) Der Satz ist in allgemeineren Resultaten von Curtiss oder Fekete und Pólya enthalten, deren Beweise jedoch schwieriger sind.

[10]) D. h. alle Koeffizienten sind ≥ 0.

also $\neq 0$, für $x > 0$; demnach sind die Zahlen $x_1, \ldots, x_{r_1} \leqq 0$. Daher ist $a\prod_{\nu=1}^{r_1}(x - x_\nu)$ ein positivzahliges Polynom. Nun ist das Produkt zweier positivzahliger Polynome wieder positivzahlig; der Satz braucht also nur für das definite Polynom $\varphi_\nu(x)$ bewiesen zu werden. Von den beiden reellen Zahlen $-\alpha_\nu$ und β_ν ist $\beta_\nu > 0$; ist auch $-\alpha_\nu > 0$ oder $= 0$, so ist $\varphi_\nu(x)$ selbst positivzahlig. Daher bleibt nur noch der Fall zu behandeln, daß $\alpha_\nu > 0$ ist. Es sei $\varphi_\nu(x) = \varphi(x)$, $\alpha_\nu = \alpha$, $\beta_\nu = \beta$.

Unter n verstehe ich eine später näher zu fixierende Zahl und setze

$$\psi(x) = (x^2 + \beta)^{2n} - (\alpha x)^{2n}.$$

Die Koeffizienten von $\psi(x)$ sind alle $\geqq 0$ mit etwaiger Ausnahme des Koeffizienten von x^{2n}, welcher den Wert $c_n = \binom{2n}{n}\beta^n - \alpha^{2n}$ besitzt. Da $\varphi(x)$ definit ist, so ist die Diskriminante $\alpha^2 - 4\beta < 0$, also die positive Zahl $q = \frac{\alpha^2}{4\beta} < 1$. Es gilt

$$\frac{\sqrt{n}\, c_n}{(4\beta)^n} = \frac{\sqrt{n}}{2^{2n}}\binom{2n}{n} - \sqrt{n}\, q^n; \tag{33}$$

da nun nach der Stirlingschen Formel

$$\frac{\sqrt{n}}{2^{2n}}\binom{2n}{n} = \frac{\sqrt{n}}{2^{2n}}\frac{(2n)!}{(n!)^2} \sim \frac{n^{\frac{1}{2}}}{2^{2n}}\frac{(2n)^{2n+\frac{1}{2}}e^{-2n}\sqrt{2\pi}}{(n^{n+\frac{1}{2}}e^{-n}\sqrt{2\pi})^2} = \frac{1}{\sqrt{\pi}}$$

ist und $\sqrt{n}\, q^n$ mit wachsendem n gegen 0 strebt, so läßt sich ein $n = n(q)$ derart wählen, daß die linke Seite von (33), also auch c_n, > 0 ist. Bei dieser Wahl von n ist das Polynom $\psi(x)$ positivzahlig. Dann ist

$$\varphi(x) = x^2 - \alpha x + \beta = \frac{(x^2+\beta)^{2n} - (\alpha x)^{2n}}{\sum_{\lambda=0}^{2n-1}(x^2+\beta)^{2n-1-\lambda}(\alpha x)^\lambda} = \frac{\psi(x)}{\chi(x)}$$

Quotient zweier positivzahliger Polynome $\psi(x)$ und $\chi(x)$.

Zusatz. Die Darstellung kann so gewählt werden, daß die Koeffizienten von Zähler und Nenner dem Körper der Koeffizienten von $f(x)$ angehören.

Beweis. Ohne Beschränkung der Allgemeinheit sei $f(x)$ nicht durch x teilbar. Es sei $f(x) = \frac{g_1(x)}{h_1(x)}$ eine Darstellung von $f(x)$ als Quotient positivzahliger Polynome. Ein etwaiger gemeinsamer Faktor x in g_1 und h_1 könnte fortdividiert werden, ohne die Art der Darstellung zu ändern; daher kann

$$g_1(x) = a + \ldots + bx^m$$

(nach steigenden Potenzen von x geordnet) mit $a > 0$, $b > 0$, $m \geqq 1$ angenommen werden. Ich setze nun

$$g_2(x) = (1 + x + \ldots + x^{m-1}) g_1(x);$$

dann hat für *jedes* ν der Reihe $0, 1, \ldots, 2m-1$ der Koeffizient von x^ν in $g_2(x)$ einen *positiven* Wert. Da aber $g_2(x) = (1 + x + \ldots + x^{m-1}) f(x) h_1(x)$ eine stetige Funktion der Koeffizienten von $h_1(x)$ ist, so kann man diese Koeffizienten durch benachbarte nicht negative *rationale* Zahlen derart ersetzen, daß, wenn auf diese Weise das Polynom $(1 + x + \ldots + x^{m-1}) h_1(x)$ in $h(x)$ übergeht, die Koeffizienten von $h(x) f(x) = g(x)$ auch noch positiv sind. Nun ist $h(x)$ rationalzahlig; die Koeffizienten von $g(x)$ liegen daher im Körper der Koeffizienten von $f(x)$, und $f(x) = \frac{g(x)}{h(x)}$ ist die gesuchte Darstellung.

Satz 5. Eine total positive Zahl α erzeuge den algebraischen Zahlkörper K. Dann gibt es zu jeder total positiven Zahl $\xi \neq 0$ aus K zwei Polynome $g(x)$ und $h(x)$ mit *positiven* rationalen Koeffizienten, so daß

$$\xi = \frac{g(\alpha)}{h(\alpha)} \tag{34}$$

ist[11]).

Beweis. Nach dem Hauptsatze gibt es vier rationalzahlige Polynome $f_\nu(x)$ $(\nu = 1, \ldots, 4)$ derart, daß $\xi = \sum_{\nu=1}^{4} f_\nu(\alpha)^2$ ist; dabei darf angenommen werden, daß die Grade dieser Polynome kleiner als der Grad von K sind. Haben sie also einen gemeinsamen Teiler $x - \lambda$, so ist λ von den Konjugierten zu α verschieden. Die Bezeichnung sei so gewählt, daß $f_1(x)$ nicht identisch 0 ist; ferner sei $f(x) = 0$ die irreduzible Gleichung für α. Dann gibt es eine natürliche Zahl m, so daß $f_1(x)$ und $f_2(x) + m f(x)$ teilerfremd sind. Da nun $f_2(\alpha) + f(\alpha) = f_2(\alpha)$ ist, so darf man annehmen, daß $f_1(x), \ldots, f_4(x)$ teilerfremd sind, wenn man die Beschränkung über ihren Grad aufhebt. Dann ist das Polynom $\sum_{\nu=1}^{4} f_\nu(x)^2 = \varphi(x)$ positiv definit, also a fortiori > 0 für $x > 0$. Nach Hilfssatz 6 und Zusatz gibt es daher zwei Polynome $g(x)$ und $h(x)$ mit positiven rationalen Koeffizienten, so daß $\varphi(x) = \frac{g(x)}{h(x)}$ ist. Dabei darf ich $h(\alpha) \neq 0$ annehmen, da ich sonst nur die Koeffizienten von $g(x)$ und $h(x)$ durch benachbarte zu ersetzen brauche (vgl. die Überlegung beim Beweis des Zusatzes). Daher gilt (34).

[11]) Daß umgekehrt jede Zahl ξ der Form (34) > 0 ist, ist trivial.

Anmerkungen. 1. Beim Beweise von Satz 5 ist nirgends davon Gebrauch gemacht worden, daß α total positiv ist; der Satz gilt also für jedes algebraische α.

2. An Stelle des Hauptsatzes kann beim Beweise der oben (Satz 2, Anm. 3) erwähnte (elementar beweisbare) Landausche Satz über die Zerlegung total positiver Zahlen in Quadrate benutzt werden.

3. In (34) kann der Nenner $h(\alpha)$ nicht entbehrt werden. Ist z. B. α reell und eine der Konjugierten α' ebenfalls reell und $> \alpha$, so ist $g(\alpha') > g(\alpha)$ für jedes positivzahlige Polynom $g(x)$. Nun gibt es sicher Körperzahlen ξ mit $\xi' < \xi$, und ein solches ξ kann daher nicht die Form $g(\alpha)$ haben.

§ 5.

Es gibt Körper, in denen nicht *jede* total positive Zahl als Summe von *weniger* als vier Quadraten sich darstellen läßt; z. B. gilt dies für den Körper der rationalen Zahlen. Ich stelle im folgenden die notwendigen und hinreichenden Bedingungen dafür auf, daß eine total positive ganze Zahl ξ als Summe von zwei oder drei Quadraten dargestellt werden kann.

Satz 6. Eine total positive ganze Zahl ξ läßt sich dann und nur dann als Summe von zwei Quadratzahlen schreiben, wenn für alle Primideale $\mathfrak{w} \mid 2\xi$ das Symbol $\left(\frac{\xi, -1}{\mathfrak{w}}\right)$ den Wert $+1$ hat.

Beweis. Damit ξ Summe von zwei Quadraten ist, ist notwendig und hinreichend, daß die Diophantische Gleichung

$$\xi x^2 - y^2 = z^2 \tag{35}$$

im Körper von ξ lösbar ist (ohne daß x, y, z alle drei 0 sind). Ist nämlich dabei $x = 0$, so ist $-1 = i^2$ Quadratzahl des Körpers, und dann gilt $\xi = \left(\frac{\xi+1}{2}\right)^2 + \left(i\frac{\xi-1}{2}\right)^2$. (35) läßt sich aber nach Satz II der Einleitung dann und nur dann lösen, wenn für alle Primideale $\mathfrak{w} \mid 2\xi$ das Symbol $\left(\frac{\xi, -1}{\mathfrak{w}}\right) = +1$ ist; die Gleichung $\left(\frac{\xi, -1}{1^{(i)}}\right) = +1$ gilt nämlich für alle $\xi > 0$.

Satz 7. Eine total positive ganze Zahl ξ läßt sich dann und nur dann als Summe von drei Quadratzahlen schreiben, wenn für alle Primideale $\mathfrak{l} \mid 2$ die Gleichung $\left(\frac{x, -\xi}{\mathfrak{l}}\right) = \left(\frac{-1, -1}{\mathfrak{l}}\right)$ eine Lösung x hat.

Beweis. Damit ξ Summe von drei Quadraten ist, ist notwendig und hinreichend, daß die Diophantische Gleichung

$$\xi x_1^2 - y_1^2 - z_1^2 = t_1^2 \tag{36}$$

im Körper von ξ in nicht sämtlich verschwindenden ganzen Zahlen

x_1, y_1, z_1, t_1 lösbar ist. Ist nämlich dabei $x_1 = 0$, so ist -1 Summe von zwei Quadraten, und nach (20) jedes ξ des Körpers in drei Quadrate zerlegbar. Ist (36) lösbar, so kann dabei $t_1 \neq 0$ angenommen werden. Es bedeute f die in (36) links stehende ternäre Form und F ihre Adjungierte. Es sei $x \neq 0$ eine simultan mit t_1^2 durch F dargestellte Zahl. Dann gilt, da auch -1 und $+1$ durch f und F simultan darstellbar sind, nach dem Ergebnis von § 1 für alle $\mathfrak{w}$ (d. h. $\mathfrak{w}$ = Primideal und $\mathfrak{w} = 1^{(2)}$)

$$\left(\frac{-1, \xi}{\mathfrak{w}}\right) = \left(\frac{-x, -\xi t_1^2}{\mathfrak{w}}\right);$$

also

$$\left(\frac{-1, -1}{\mathfrak{w}}\right)\left(\frac{-1, -\xi}{\mathfrak{w}}\right) = \left(\frac{-x, t_1^2}{\mathfrak{w}}\right)\left(\frac{-x, -\xi}{\mathfrak{w}}\right), \qquad \left(\frac{x, -\xi}{\mathfrak{w}}\right) = \left(\frac{-1, -1}{\mathfrak{w}}\right),$$

und letztere Gleichung gilt speziell für $\mathfrak{w} = 1$. Ist umgekehrt diese Gleichung für x lösbar, wenn $\mathfrak{w} = 1$ ist, so ist sie für beliebiges $\mathfrak{w}$ lösbar da für alle Primideale $\mathfrak{w} \neq 2$ das Symbol $\left(\frac{-1, -1}{\mathfrak{w}}\right) = +1$ ist. Aus den Überlegungen von § 2 ergibt sich dann die Lösbarkeit von (36).

Anmerkungen. 1. Die Sätze 6 und 7 liefern natürlich für den Körper der rationalen Zahlen die bekannten Resultate:

Ist $\xi = n$ eine natürliche Zahl und geht die Primzahl $p \neq 2$ in n zu gerader Potenz auf, so ist $\left(\frac{n, -1}{p}\right) = +1$, geht sie in ungerader Potenz auf, so ist $\left(\frac{n, -1}{p}\right) = (-1)^{\frac{p-1}{2}}$; es ergibt sich also die Bedingung $p \equiv 1 \pmod 4$ für jede Primzahl p, die in n zu ungerader Potenz aufgeht. Ist diese Bedingung erfüllt, so ist n Summe von zwei Quadraten.

Ich setze $n = 2^r n'(2 + n';\ r \geqq 0)$, $x = 2^s x'(2 + x';\ s \geqq 0)$; dann ist

$$\left(\frac{x, -n}{2}\right) = \left(\frac{2^s x', -2^r n'}{2}\right) = \left(\frac{x', 2}{2}\right)^r \left(\frac{n', 2}{2}\right)^s \left(\frac{x', -n'}{2}\right)$$
$$= (-1)^{\frac{x'^2-1}{8} r + \frac{n'^2-1}{8} s + \frac{n'+1}{2}\frac{x'-1}{2}}.$$

Damit die rechte Seite den Wert $\left(\frac{-1, -1}{2}\right) = -1$ hat, muß der Exponent ungerade sein, also

$$\frac{x'^2-1}{8} r + \frac{n'^2-1}{8} s + \frac{n'+1}{2}\frac{x'-1}{2} \equiv 1 \pmod 2;$$

und diese Kongruenz läßt sich nur dann durch kein Zahlenpaar s, x' befriedigen, wenn r gerade, $\frac{n'^2-1}{8} \equiv \frac{n'+1}{2} \equiv 0 \pmod 2$, $n' \equiv 7 \pmod 8$ ist, also n von der Form $4^k(8m + 7)$ ist. In jedem anderen Fall ist daher n in drei Quadrate zerlegbar.

2. Von Interesse für die Darstellung definiter Polynome durch Quadrate ist der Fall $\xi = -1$ in einem total imaginären Körper. Nach Satz 7 lautet für dieses ξ die Bedingung für Darstellbarkeit durch drei Quadrate $\left(\frac{x,1}{l}\right) = \left(\frac{-1,-1}{l}\right)$, also $\left(\frac{-1,-1}{l}\right) = +1$ für jedes $l \mid 2$. Dies ist aber nach Satz 6 die Bedingung für Darstellbarkeit durch zwei Quadrate. Läßt sich also -1 als Summe von drei Quadraten darstellen, so läßt es sich auch in zwei Quadrate zerlegen; und dies ist dann und nur dann der Fall, wenn die Kongruenz $1 + u^2 + v^2 \equiv 0 \pmod 8$ im Körper lösbar ist. Dann ist aber nach (20) jede Zahl des Körpers in drei Quadrate zerlegbar. Damit also die Zahlen eines total imaginären Körpers sämtlich Summen von drei Quadraten sind, ist notwendig und hinreichend, daß die Zahl -1 Summe von zwei Quadraten ist, oder, anders ausgedrückt, daß die Gleichung $x^2 + y^2 + z^2 = 0$ eine von der trivialen verschiedene Lösung besitzt.

§ 6.

Wie ich bereits oben (Satz 1, Anm. 1) bemerkt habe, weiß man nichts über die Beschaffenheit der Nenner bei der Zerlegung einer ganzen total positiven Zahl in vier Quadrate. Auch die Landausche Methode zur Zerlegung in Quadrate überhaupt liefert darüber nichts. Ich behandle das Problem in diesem Schlußparagraphen mit vollkommen elementaren Mitteln, muß aber die wesentliche Einschränkung machen, daß der Körper *total reell* ist.

Satz 8. Es sei K ein total reeller Körper. Ich bezeichne seine total positiven Einheiten in irgendeiner Reihenfolge mit $\varepsilon_1, \varepsilon_2, \ldots$. Dann gibt es eine nur von K abhängige natürliche Zahl d derart, daß jede total positive ganze Zahl ξ des Körpers in der Form

$$\xi = \frac{x_1 \varepsilon_1 + x_2 \varepsilon_2 + \cdots}{d} \tag{37}$$

mit ganzen rationalen *nicht negativen* x_ν $(\nu = 1, 2, \ldots)$ darstellbar ist. $d\xi$ läßt sich also als Summe von total positiven Einheiten schreiben.

Beweis. Der Satz ist trivial für den Körper der rationalen Zahlen; der Grad von K sei also $n \geqq 2$. K ist total reell, besitzt also ein System von $n-1$ total positiven Grundeinheiten $\eta_1, \ldots, \eta_{n-1}$. Die $n-1$ linearen Gleichungen

$$\mu_1 \log \eta_1^{(\lambda)} + \ldots + \mu_{n-1} \log \eta_{n-1}^{(\lambda)} = \log \frac{\xi^{(\lambda)}}{\sqrt[n]{N\xi}} \quad [12]) \qquad (\lambda = 1, \ldots, n-1) \tag{38}$$

[12]) Die Zeichen N und S bedeuten Norm und Spur.

sind eindeutig nach $\mu_1, \ldots, \mu_{n-1}$ auflösbar; und (38) gilt auch noch für $\lambda = n$. Ich setze $m_1 = [\mu_1], \ldots, m_{n-1} = [\mu_{n-1}]$, $H = \eta_1^{m_1} \ldots \eta_{n-1}^{m_{n-1}}$, $\frac{\xi}{H} = \xi_1$; dann ist die Einheit $H > 0$, also $\xi_1 > 0$, und $N\xi_1 = N\xi$. Der Wahl der Zahlen $m_1, \ldots, m_{n-1}$ zufolge gibt es mit Rücksicht auf (38) zwei positive rationale Zahlen a und A $(0 < a < 1 < A)$, die nur vom Körper abhängen, so daß die Ungleichung

$$a\sqrt[n]{N\xi_1} < \xi_1^{(\lambda)} < A\sqrt[n]{N\xi_1} \tag{39}$$

für jedes $\lambda = 1, \ldots, n$ gilt. Ich unterscheide nun zwei Fälle:

1. $SH \geqq n\frac{A}{a}$ [12]. Dann setze ich

$$\xi_2 = \xi_1 - [a\sqrt[n]{N\xi_1}];$$

dies ist wegen (39) eine total positive ganze Zahl. Ferner ist nach (39)

$$a\sqrt[n]{N\xi_1} = \frac{a}{A} \cdot A\sqrt[n]{N\xi_1} > \frac{a}{An} S\xi_1,$$

$$S\xi_2 \leqq S\xi_1 - n\left[\frac{a}{An} S\xi_1\right] < \left(1 - \frac{a}{A}\right) S\xi_1 + n. \tag{40}$$

Aus der Ungleichung

$$S\xi = S(H\xi_1) > a\sqrt[n]{N\xi_1}\, SH \geqq nA\sqrt[n]{N\xi_1} \geqq S\xi_1$$

folgt dann mit (40)

$$S\xi_2 < \left(1 - \frac{a}{A}\right) S\xi + n.$$

2. $SH < n\frac{A}{a}$. Dann ist a fortiori $H < n\frac{A}{a}$, und aus $NH = 1$ folgt $H > \frac{1}{\left(n\frac{A}{a}\right)^{n-1}}$. Nach (39) ist

$$\frac{a\sqrt[n]{N\xi}}{\left(n\frac{A}{a}\right)^{n-1}} < \xi^{(\lambda)} < n\frac{A^2}{a}\sqrt[n]{N\xi}. \tag{41}$$

Ich setze in diesem Falle 2.

$$\xi_2 = \xi - \left[\frac{a^n}{(An)^{n-1}}\sqrt[n]{N\xi}\right];$$

dies ist wegen (41) eine total positive ganze Zahl. Ferner ist nach (41)

$$\frac{a^n}{(An)^{n-1}}\sqrt[n]{N\xi} = n\left(\frac{a}{An}\right)^{n+1} \cdot n\frac{A^2}{a}\sqrt[n]{N\xi} > \left(\frac{a}{An}\right)^{n+1} S\xi,$$

$$S\xi_2 \leqq S\xi - n\left[\left(\frac{a}{An}\right)^{n+1} S\xi\right] < \left(1 - n\left(\frac{a}{An}\right)^{n+1}\right) S\xi + n. \tag{42}$$

Nun sei $q = n\left(\frac{a}{An}\right)^{n+1}$; dann ist $0 < q < \frac{a}{A} < 1$, und nach (40) und (42) in jedem der Fälle 1., 2.

$$S\xi_2 < (1-q) S\xi + n, \qquad \xi_2 > 0 \text{ und ganz;} \tag{43}$$

ferner ist

$$\xi = H\xi_1 = [a\sqrt[n]{N\xi}]\,H + \xi_2 H, \quad \text{resp.} \quad \xi = \left[\frac{a^n}{(An)^{n-1}}\sqrt[n]{N\xi}\right] + \xi_2.$$

Jetzt verfahre ich mit ξ_2 genau so wie vorhin mit ξ; es ergibt sich analog zu (43)

$$S\xi_4 < (1-q)S\xi_2 + n, \qquad \xi_4 > 0 \text{ und ganz},$$

mit

$$\xi_2 = H_2\xi_3 = [a\sqrt[n]{N\xi_2}]\,H_2 + \xi_4 H_2, \quad \text{resp.} \quad \xi_2 = \left[\frac{a^n}{(An)^{n-1}}\sqrt[n]{N\xi_2}\right] + \xi_4;$$

und ebenso erhält man allgemein für $k = 1, 2, 3, \ldots$, wenn $H_0 = H$, $\xi_0 = \xi$ gesetzt wird,

$$(44) \qquad S\xi_{2k} < (1-q)S\xi_{2k-2} + n, \qquad \xi_{2k} > 0 \text{ und ganz},$$

$$(45) \qquad \xi_{2k-2} = H_{2k-2}\xi_{2k-1} = [a\sqrt[n]{N\xi_{2k-2}}]\,H_{2k-2} + \xi_{2k}H_{2k-2},$$

$$\text{resp.} \quad \xi_{2k-2} = \left[\frac{a^n}{(An)^{n-1}}\sqrt[n]{N\xi_{2k-2}}\right] + \xi_{2k},$$

wobei ξ_{2k-2}, ξ_{2k-1}, ξ_{2k}, H_{2k-2} den Zahlen ξ, ξ_1, ξ_2, H entsprechen.

Ist nun bereits $S\xi < \frac{2n}{q}$, so wende man das eben geschilderte Verfahren überhaupt nicht an. Ist aber $S\xi \geqq \frac{2n}{q}$, so ist nach (44)

$$S\xi_2 < (1-q)S\xi + \frac{q}{2}S\xi = \left(1-\frac{q}{2}\right)S\xi < S\xi.$$

Ist auch noch $S\xi_2 \geqq \frac{2n}{q}$, so ist ebenso

$$S\xi_4 < \left(1-\frac{q}{2}\right)S\xi_2 < \left(1-\frac{q}{2}\right)^2 S\xi;$$

allgemein folgt also aus $S\xi_{2k-2} \geqq \frac{2n}{q}$ nach (44) die Ungleichung

$$S\xi_{2k} < \left(1-\frac{q}{2}\right)^k S\xi.$$

Da nun $\left(1-\frac{q}{2}\right)^k$ mit wachsendem k gegen 0 strebt, so gibt es ein k der Reihe 0, 1, 2, ... derart, daß $S\xi_{2k} < \frac{2n}{q}$ ist. Dann gehört aber die total positive ganze Zahl ξ_{2k} einem *endlichen* Wertevorrat an; und ferner gilt wegen (45) eine Zerlegung

$$(46) \qquad \xi = a_1 E_1 + \ldots + a_k E_k + \xi_{2k} E,$$

wo $E_1, \ldots, E_k, E$ total positive Einheiten und $a_1, \ldots, a_k$ *nicht negative* ganze rationale Zahlen bedeuten.

Ich brauche also den Satz nur für die endlich vielen total positiven ganzen Zahlen ζ mit $S\zeta < \frac{2n}{q}$ zu beweisen. Nun sei $Q = Q(\zeta)$ die natürliche Zahl

$$(47) \qquad Q = \left[n! \left(\frac{A}{a}\right)^{n-1} \frac{S\zeta}{\min(\zeta^{(1)}, \ldots, \zeta^{(n)})} \right] > n! \left(\frac{A}{a}\right)^{n-1},$$

mit den Zahlen a und A aus (39). Für jedes $\lambda = 1, \ldots, n$ gibt es eine total positive Einheit ε_λ derart, daß $\varepsilon_\lambda^{(\varkappa)} < 1$ für $\varkappa \neq \lambda$, aber $Q < \varepsilon_\lambda^{(\lambda)} < \frac{A}{a} Q$ ist. In der Determinante $|\varepsilon_\lambda^{(\varkappa)}|$ $(\varkappa = 1, \ldots, n;\ \lambda = 1, \ldots, n)$ sind also die Elemente der Hauptdiagonale zwischen Q und $\frac{A}{a} Q$ gelegen, alle andern aber zwischen 0 und 1. Daher ist nach (47)

$$|\varepsilon_\lambda^{(\varkappa)}| > Q^n - (n! - 1)\left(\frac{A}{a} Q\right)^{n-1} > Q^{n-1}\left\{Q - n!\left(\frac{A}{a}\right)^{n-1}\right\} > 0.$$

Bedeutet ferner $E_{\varkappa\lambda}$ die Unterdeterminante von $\varepsilon_\lambda^{(\varkappa)}$, so ist

$$E_{\varkappa\varkappa} > Q^{n-1} - ((n-1)! - 1)\left(\frac{A}{a} Q\right)^{n-2},$$

$$E_{\varkappa\lambda} > -(n-1)!\left(\frac{A}{a} Q\right)^{n-2}.$$

Ich setze nun

$$\zeta^{(\varkappa)} = \sum_{\lambda=1}^{n}{}' z_\lambda \varepsilon_\lambda^{(\varkappa)} \qquad (\varkappa = 1, \ldots, n);$$

dann ist

$$\varepsilon_\lambda^{(\varkappa)} z_\lambda = \sum_{\varkappa=1}^{n}{}' E_{\varkappa\lambda} \zeta^{(\varkappa)} > Q^{n-1} \zeta^{(\lambda)} - (n-1)!\left(\frac{A}{a} Q\right)^{n-2} S\zeta$$

$$= Q^{n-2} \zeta^{(\lambda)} \left\{ Q - (n-1)! \left(\frac{A}{a}\right)^{n-2} \frac{S\zeta}{\zeta^{(\lambda)}} \right\},$$

also nach (47) $z_\lambda > 0$. Außerdem sind die z_λ rational. Folglich gibt es *natürliche* Zahlen $y_1, \ldots, y_n, d$, so daß $\zeta = \frac{y_1 \varepsilon_1 + \ldots + y_n \varepsilon_n}{d}$ ist; und da nur endlich viele ζ in Frage kommen, läßt sich für alle dasselbe d wählen. Dann ist zugleich für jedes total positive ganze ξ die Zahl $d\xi$ nach (46) als Summe von total positiven Einheiten darstellbar.

Anmerkung. Auf der rechten Seite von (37) sind wegen $dS\xi = \Sigma x_\nu S\varepsilon_\nu \geqq n \Sigma x_\nu$ höchstens $\left[\frac{dS\xi}{n}\right]$ von den x_ν von 0 verschieden. Da es (für $n > 1$) beliebig kleine ganze total reelle total positive Zahlen gibt, kann offenbar keine endliche Basis der Form (37) existieren.

Satz 9. Es sei K ein total reeller algebraischer Zahlkörper. Es gibt eine nur von K abhängige natürliche Zahl t derart, daß jede ganze total positive Zahl ξ des Körpers K in der Form

$$\xi = \left(\frac{\vartheta_1}{t}\right)^2 + \left(\frac{\vartheta_2}{t}\right)^2 + \dots \tag{48}$$

mit *ganzen* $\vartheta_1, \vartheta_2, \dots$ aus K dargestellt werden kann.

Beweis. Nach Satz 8 gibt es ein natürliches $d = d(K)$ und gewisse total positive Einheiten $E_1, E_2, \dots$ (unter denen auch gleiche vorkommen können), so daß

$$\xi = \frac{E_1}{d^2} + \frac{E_2}{d^2} + \dots$$

ist. Jede Einheit E kann nun in die Form $E_0 \bar{E}^2$ gesetzt werden, wo E_0 eine Einheitswurzel oder das Produkt aus einer Einheitswurzel mit einer oder mehreren *verschiedenen Grund*einheiten bedeutet und, wie auch $\bar{E}$, in K liegt. E_0 gehört also einem endlichen Wertevorrat an. Ist $E > 0$, so ist auch $E_0 > 0$. Dann läßt sich, wie in der Anmerkung 3 zu Satz 2 elementar bewiesen wurde, E_0 im Körper K in Quadrate zerlegen. Für jede der endlich vielen Möglichkeiten für E_0 denke ich mir eine solche Zerlegung gebildet; darauf wähle ich eine natürliche Zahl d', die durch jeden Nenner der hierbei auftretenden endlich vielen Quadratbasen teilbar ist. Dann lassen sich also die Zahlen $d'^2 E_0$ als Summen von ganzzahligen Quadraten darstellen, und das gleiche gilt von $d'^2 E = (d'\bar{E})^2 E_0$. Ich nehme jetzt für E speziell die total positiven Einheiten $E_1, E_2, \dots$ und erhalte eine Darstellung von $(dd')^2 \xi$ als Summe von *ganzen* Quadratzahlen aus K, so daß die Konstante t des Satzes $= dd'$ gewählt werden kann.

Anmerkung. Für die Anzahl der Summanden auf der rechten Seite von (48) ergibt sich auf diesem Wege keine von ξ oder gar von K freie Schranke. Aus (48) läßt sich nur entnehmen, daß diese Anzahl $\leqq \left[\frac{t^2 S\xi}{n}\right]$ ist, wo n den Grad von K bedeutet.

Literaturverzeichnis[13]).

Curtiss, D. R., The degree of a Cartesian multiplier. Bulletin of the American Mathematical Society, Ser. 2, **20** (1913), S. 19–26.

— An extension of Descartes' rule of signs. Mathematische Annalen **73** (1913), S. 424–435.

[13]) Während der Korrektur erschien die Arbeit: L. J. Mordell, On the representation of algebraic numbers as a sum of four squares. Proceedings of the Cambridge Philosophical Society, vol. XX (1921), S. 250—256. Hierin wird der Hilbertsche Satz für kubische Zahlkörper bewiesen.

Fekete, M., und Pólya, G., Über ein Problem von Laguerre. Rendiconti del Circolo Matematico di Palermo **34** (1912), S. 89–120.

Fujiwara, M, Über die Darstellung binärer Formen als Potenzsummen. The science reports of the Tôhoku Imperial University **2** (1913), S. 55–62.

Hilbert, D., Grundlagen der Geometrie. 1. Aufl. enthalten in: Festschrift zur Feier der Enthüllung des Gauß-Weber-Denkmals in Göttingen. Leipzig (B. G. Teubner), 1899, S. 80–85; 2. Aufl. 1903, S. 78–79; 3. Aufl. 1909, S. 113–115; 4. Aufl. 1913, S. 104–107.

— The Foundations of Geometry. Authorized Translation by E. J. Townsend. Chicago (The Open Court Publishing Company), 1902, S. 116–121.

— Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). Mathematische Annalen **67** (1909), S. 281–300.

Landau, E., Über die Darstellung definiter binärer Formen durch Quadrate. Mathematische Annalen **57** (1903), S. 53–64.

— Über die Darstellung definiter Funktionen durch Quadrate. Mathematische Annalen **62** (1906), S. 272–285.

— Über die Zerlegung total positiver Zahlen in Quadrate. Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, Jahrgang 1919, S. 392–396.

Le Besgue, V. A., Exercices d'analyse numérique. Paris (Leiber et Faraguet), 1859, S. 147–151.

Meißner, E., Über positive Darstellungen von Polynomen. Mathematische Annalen **70** (1911), S. 223–235.

Meißner, O, Über die Darstellung der Zahlen einiger algebraischer Zahlkörper als Summen von Quadratzahlen des Körpers. Archiv der Mathematik und Physik, 3. Reihe, **7** (1904), S. 266–268.

— Über die Darstellbarkeit der Zahlen quadratischer und kubischer Zahlkörper als Quadratsummen. Archiv der Mathematik und Physik, 3. Reihe, **9** (1905), S. 202–203.

Stridsberg, E., Några elementära undersökningar rörande fakulteter och deras aritmetiska egenskaper. Arkiv för Matematik, Astronomi och Fysik **11** (1916/1917), Nr. 25, 52 S.

Göttingen, 27. September 1920.

(Eingegangen am 28. September 1920.)