Werk

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

LOG Id: LOG_0008
LOG Titel: Theorie der quadratischen Formen in beliebigen Körpern.
LOG Typ: article

Übergeordnetes Werk

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

Contact

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

Theorie der quadratischen Formen in beliebigen Körpern.

Von *Ernst Witt* in Göttingen.

Die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten rational ineinander transformiert werden können, sind zuerst von *Minkowski* (5) aufgestellt worden [1]). Aufbauend auf seine Theorie der ganzzahligen quadratischen Formen zeigte er, daß sich aus einer Form f für jede Primzahl p in gewisser Weise eine *Einheit* $C_p(f) = \pm 1$ herstellen läßt, die bei allen Transformationen der Form ungeändert bleibt; und er sprach den Satz aus, daß zwei Formen mit gleicher Diskriminante, gleichem Sylvesterschen Trägheitsindex und gleichen Einheiten C_p immer rational ineinander transformiert werden können. Er löste auch die Frage, unter welchen Umständen eine Form die Null rational darstellen kann, und er gab an, bei welchen Zusammenstellungen der Invarianten es zugehörige quadratische Formen wirklich gibt.

In einer Reihe von Arbeiten hat dann *Hasse* (3) die Sätze von Minkowski mit einer übersichtlichen, von Hensel eingeführten Behandlungsweise (*Schluß vom Kleinen aufs Große*) hergeleitet; er hat diese Sätze auch für ganz beliebige Zahlkörper verallgemeinert. Die Minkowskischen Einheiten C_p konnten durch *Hilbertsche Normrestsymbole* $\left(\frac{a, b}{p}\right)$ ersetzt werden, dadurch wurden die Beweise unabhängig von der weitläufigen Theorie der ganzzahligen Formen.

Da aus der neueren Theorie der Algebren bekannt ist, daß eine Algebra (a, b) im wesentlichen dasselbe ist wie ein System von Normrestsymbolen, hat *Artin* in einer Vorlesung die quadratischen Formen von vornherein auf dieser Grundlage behandelt. Er ordnete jeder *Form*

$$f = \sum_1^n a_i x_i^2$$

die *Algebra*

$$S(f) = \prod_{i \leqq k} (a_i, a_k)$$

zu. Die Invarianz dieser Algebra bei allen Transformationen war allerdings nicht ganz leicht einzusehen, und so erhob sich die Forderung, ein anderes hyperkomplexes System ausfindig zu machen, für welches die Invarianz direkt ersichtlich ist, und aus welchem sich die Algebra $S(f)$ in einfacher Weise gewinnen läßt. Dies geschieht in dieser Arbeit durch Angabe des **Systems** $C(f)$ *vom Rang* 2^n *mit den Erzeugenden* $u_1, \ldots, u_n$ *und den definierenden Relationen* $u_i^2 = a_i$, $u_i u_k = -u_k u_i$ $(i \neq k)$. Historisch ist zu bemerken, daß diese hyperkomplexen Zahlen für den Fall $a_i = -1$ bereits von *Clifford* (2) als Verallgemeinerung der Quaternionen betrachtet wurden.

[1]) Die eingeklammerten Zahlen in Fettdruck verweisen auf die entsprechende Arbeit im Literaturverzeichnis auf S. 44.

In ganz beliebigen Körpern (der Charakteristik $\neq 2$) liefert die Algebra $S(f)$ zusammen mit der Diskriminante für $n = 1, 2, 3$ ein volles Invariantensystem bezüglich der Äquivalenz der quadratischen Formen, und für $n = 1, 2, 3, 4$ lassen sich allgemeingültige Bedingungen dafür angeben, wann eine Form die Null darstellt (vgl. die Tabelle auf S. 39). Nach einer einfachen Bemerkung von Hensel (4) folgen daraus sofort Kriterien dafür, wann irgendeine Zahl $m \neq 0$ von einer Form dargestellt wird (für $n = 1, 2, 3$).

Im Anfang der Arbeit werden bei beliebigen Körpern allgemeine Theoreme über quadratische Formen hergeleitet, die zwar mit den einfachsten Mitteln beweisbar sind, dennoch bisher wohl unbekannt waren, wie z. B. der Satz, daß aus der Äquivalenz von $f + g$ mit $f + h$ die andere Äquivalenz von g mit h folgt. In dieser Theorie spielen diejenigen Formen, welche die Null nicht darstellen, eine wichtige Rolle. Bei geeigneter Komposition bilden sie die Elemente eines **Ringes** (ebenso, wie in der Algebrentheorie die Schiefkörper Elemente einer Gruppe sind).

Indem wir uns auf diese allgemeinen Sätze stützen, können wir in vielen Körpern, in denen die Algebrentheorie schon erforscht ist, alle diejenigen Fragen lösen, welche von Minkowski und Hasse für den Fall eines Zahlkörpers untersucht worden sind. Die Hauptsätze über quadratische Formen mit Koeffizienten aus einem Zahlkörper werden hier noch einmal kurz als Anwendung der allgemeinen Theorie dargestellt (vgl. die Tabelle auf S. 42). Für viele interessante Spezialfälle der Hauptsätze, die hier nicht aufgenommen sind, verweisen wir auf die Arbeiten von Hasse (3).

Als letztes Beispiel werden quadratische Formen in einem reellen Funktionenkörper vollständig behandelt. Hier wird z. B. die Äquivalenz durch unendlich viele Trägheitsindizes geregelt.

I. Metrische Räume.

Einführung. Es sei ein fester Koeffizientenkörper K zugrundegelegt, die Charakteristik sei $\neq 2$.

Mit Hilfe einer quadratischen Form (Metrik)

$$f = \sum_{i,k} a_{ik} x_i x_k \qquad (a_{ik} = a_{ki};\ i, k = 1, \ldots, n)$$

machen wir den n-dimensionalen Vektorraum

$$\mathfrak{R} = \langle K\mathfrak{u}_1, \ldots, K\mathfrak{u}_n \rangle$$

zu einem metrischen Raum, indem wir in ihm ein (inneres) Produkt zweier Vektoren erklären durch

$$\sum_i x_i \mathfrak{u}_i \cdot \sum_k y_k \mathfrak{u}_k = \sum_{i,k} a_{ik} x_i y_k .$$

Eine Basisänderung entspricht dem Übergang zu einer äquivalenten quadratischen Form. Die Diskriminante $|\mathfrak{u}_i \mathfrak{u}_k| = |a_{ik}|$ multipliziert sich dabei stets mit einer Quadratzahl $\neq 0$ aus dem Körper K. Diese bis auf Quadratzahlen festgelegte Zahl $|\mathfrak{u}_i \mathfrak{u}_k|$ bezeichnen wir mit $|\mathfrak{R}|$ oder mit $d(f)$.

Besteht zwischen zwei Räumen eine additions- und multiplikationstreue Zuordnung, so sollen sie isomorph heißen. Äquivalente Formen $f_1 \cong f_2$ bestimmen also isomorphe Räume $\mathfrak{R}_1 \cong \mathfrak{R}_2$, und umgekehrt. Eindimensionale Räume sind schon durch die Diskriminante $|\mathfrak{R}|$ bis auf Isomorphie festgelegt.

Wenn $\mathfrak{u}\mathfrak{v} = 0$ ist, sagen wir, die Vektoren $\mathfrak{u}$ und $\mathfrak{v}$ stehen senkrecht aufeinander. Mit $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2$ bezeichnen wir die Zerlegung in senkrechte Teilräume.

Untersuchung. Diejenigen Vektoren $\sum_i x_i \mathfrak{u}_i$, welche auf *allen* Vektoren von $\mathfrak{R}$ senkrecht stehen, bilden einen Teilraum $\mathfrak{R}_0$, das **Radikal** von $\mathfrak{R}$. Da sich der Wert eines

Vektorproduktes nicht ändert, wenn die Faktoren mod. $\mathfrak{R}_0$ abgeändert werden, ist es sinnvoll, von einem Raume $\mathfrak{R}/\mathfrak{R}_0$ zu reden. Wegen

$$\mathfrak{R} \cong \mathfrak{R}_0 + \mathfrak{R}/\mathfrak{R}_0$$

hängt die Beschaffenheit des Raumes $\mathfrak{R}$ nur von der Struktur des durch $\mathfrak{R}$ eindeutig bestimmten Raumes $\mathfrak{R}/\mathfrak{R}_0$ ab; dieser Raum $\mathfrak{R}/\mathfrak{R}_0$ hat kein Radikal mehr.

Es genügt daher, *von jetzt ab einen Raum $\mathfrak{R}$ ohne Radikal* zu untersuchen. Das Fehlen des Radikals ist gleichbedeutend mit der Unlösbarkeit des Gleichungssystems $\sum_i x_i u_i u_k = 0$ $(k = 1, \ldots, n)$, d. h. *die Diskriminante $|\mathfrak{R}|$ darf nicht verschwinden.*

Die Grundlage zu einer übersichtlichen Strukturuntersuchung der metrischen Räume ohne Radikal liefert

Satz 1. *$\mathfrak{r}$ sei ein Teilraum von $\mathfrak{R}$, und $\mathfrak{r}^*$ sei der zu $\mathfrak{r}$ senkrechte Teilraum. Dann gilt*

$$\dim \mathfrak{r} + \dim \mathfrak{r}^* = \dim \mathfrak{R}, \tag{1}$$

$$\mathfrak{r}^{**} = \mathfrak{r}. \tag{2}$$

Wenn $|\mathfrak{r}| \neq 0$ ist, so ist auch $|\mathfrak{r}^*| \neq 0$, und es gilt

$$\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^*, \tag{3}$$

$$|\mathfrak{R}| = |\mathfrak{r}| \cdot |\mathfrak{r}^*|. \tag{4}$$

Beweis. Wir dürfen $\mathfrak{r} = \langle u_1, \ldots, u_r \rangle$ annehmen. $\mathfrak{r}^*$ besteht aus allen Vektoren $\sum_i x_i u_i$ mit $\sum_i x_i u_i u_k = 0$ $(k = 1, \ldots, r)$. Wegen $|\mathfrak{R}| \neq 0$ hat dieses Gleichungssystem den Rang r und damit $n - r$ linear unabhängige Lösungen. — Aus (1) folgt $\dim \mathfrak{r}^{**} = \dim \mathfrak{r}$, andererseits ist logisch klar, daß $\mathfrak{r}^{**} \geqq \mathfrak{r}$ gilt; damit ist (2) bewiesen. — Wenn $\mathfrak{r}$ kein Radikal hat, gilt $\mathfrak{r} \cap \mathfrak{r}^* = 0$. Wegen (1) folgt jetzt (3). Wir dürfen $\mathfrak{r}^* = \langle u_{r+1}, \ldots, u_n \rangle$ annehmen, daraus ist die Gültigkeit von (4) ersichtlich, und aus (4) folgt $|\mathfrak{r}^*| \neq 0$.

Die bekannte Tatsache, daß es zu jeder quadratischen Form eine äquivalente Diagonalform gibt, in der eine beliebige durch die Form darstellbare Zahl $a \neq 0$ als erster Koeffizient erscheint, ist eine unmittelbare Folge von Satz 1. Wir sprechen sie nur in einer anderen, aber gleichwertigen Form aus:

Satz 2. *Ist $\mathfrak{v}_1$ ein beliebiger Vektor, dessen Quadrat nicht verschwindet, so gibt es eine orthogonale Zerlegung*

$$\mathfrak{R} = \langle \mathfrak{v}_1 \rangle + \cdots + \langle \mathfrak{v}_n \rangle.$$

Beweis durch Induktion. Wegen $|\mathfrak{R}| \neq 0$ verschwinden nicht alle Vektorprodukte, und wegen $4\mathfrak{u}\mathfrak{v} = (\mathfrak{u} + \mathfrak{v})^2 - (\mathfrak{u} - \mathfrak{v})^2$ auch nicht alle Vektorquadrate (Charakteristik $\neq 2$!). Es sei $\mathfrak{v}_1^2 \neq 0$. Nach Satz 1 folgt eine Zerlegung $\mathfrak{R} = \langle \mathfrak{v}_1 \rangle + \langle \mathfrak{v}_1 \rangle^*$. Für den Teilraum $\langle \mathfrak{v}_1 \rangle^*$ dürfen wir aber schon eine Zerlegung $\langle \mathfrak{v}_1 \rangle^* = \langle \mathfrak{v}_2 \rangle + \cdots + \langle \mathfrak{v}_n \rangle$ ansetzen.

In besonderen Fällen läßt sich zu einer quadratischen Form eine zugehörige Diagonalform explizit angeben:

Satz 3. *Sind alle Teildeterminanten*

$$d_r = \begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix} \neq 0 \quad \text{für} \quad r = 1, \ldots, n,$$

so ist

$$\sum_{i,k} a_{ik} x_i x_k \cong \sum_i \frac{d_i}{d_{i-1}} y_i^2 \qquad (d_0 = 1).$$

Beweis durch Induktion. Für den Teilraum $\mathfrak{r} = \langle \mathfrak{u}_1, \ldots, \mathfrak{u}_{n-1} \rangle$ dürfen wir eine Zerlegung $\mathfrak{r} = \langle \mathfrak{v}_1 \rangle + \cdots + \langle \mathfrak{v}_{n-1} \rangle$ ansetzen mit $\mathfrak{v}_i^2 = \frac{d_i}{d_{i-1}}$. Nach Satz 1 ist $\mathfrak{R} = \mathfrak{r} + \langle \mathfrak{v}_n \rangle$ und $\mathfrak{v}_n^2 \cong \frac{d_n}{d_{n-1}}$. (Dabei bedeute $a \cong b$, daß $\frac{a}{b}$ eine Quadratzahl ist.)

Für die weitere Entwicklung brauchen wir einen

Hilfssatz. *Alle binären Formen $ax^2 + 2bxy + cy^2$, welche die Null (in nicht trivialer Weise) darstellen, sind untereinander äquivalent.*

Beweis. Die Nulldarstellung bedeutet: Es gibt in $\mathfrak{R}$ einen Vektor $\mathfrak{u} \neq 0$ mit $\mathfrak{u}^2 = 0$. Wegen $|\mathfrak{R}| \neq 0$ gibt es einen Vektor $\mathfrak{w}$ mit $\mathfrak{u}\mathfrak{w} = 1$. Es sei $\mathfrak{v} = 2\mathfrak{w} - \mathfrak{w}^2\mathfrak{u}$. Für $\mathfrak{u}, \mathfrak{v}$ lautet die Produkttafel $\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$. Folglich ist die gegebene Form mit der festen Form $4xy$ äquivalent. — Eine andere Normalform ist z. B. $x^2 - y^2$.

Nun sind wir in der Lage, einen wichtigen Kürzungssatz zu beweisen.

Satz 4. *Aus $\mathfrak{R}_1 + \mathfrak{R}_3 \cong \mathfrak{R}_2 + \mathfrak{R}_3$ darf $\mathfrak{R}_1 \cong \mathfrak{R}_2$ geschlossen werden.*

Beweis. Da $\mathfrak{R}_3$ entsprechend Satz 2 zerlegt werden kann, genügt es, $\mathfrak{R}_3$ als eindimensional anzunehmen. Setzen wir $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_3$, so können wir die Behauptung auch folgendermaßen formulieren: Aus $\mathfrak{u}^2 = \mathfrak{v}^2 \neq 0$ folgt $\langle \mathfrak{u} \rangle^* \cong \langle \mathfrak{v} \rangle^*$.

Wenn $\langle \mathfrak{u}, \mathfrak{v} \rangle$ eindimensional ist, so ist sogar $\langle \mathfrak{u} \rangle^* = \langle \mathfrak{v} \rangle^*$. Es sei jetzt $\langle \mathfrak{u}, \mathfrak{v} \rangle$ zweidimensional.

Wenn die Diskriminante $|\mathfrak{u}, \mathfrak{v}| \neq 0$ ist, so gilt nach Satz 1

$$\mathfrak{R} = \langle \mathfrak{u}, \mathfrak{v} \rangle + \langle \mathfrak{u}, \mathfrak{v} \rangle^* \quad \text{und} \quad \langle \mathfrak{u}, \mathfrak{v} \rangle = \langle \mathfrak{u} \rangle + \mathfrak{U} = \langle \mathfrak{v} \rangle + \mathfrak{V};$$

dabei müssen $\mathfrak{U}$ und $\mathfrak{V}$ als eindimensionale Räume mit gleicher Diskriminante äquivalent sein. Also ist

$$\langle \mathfrak{u} \rangle^* = \mathfrak{U} + \langle \mathfrak{u}, \mathfrak{v} \rangle^* \cong \mathfrak{V} + \langle \mathfrak{u}, \mathfrak{v} \rangle^* = \langle \mathfrak{v} \rangle^*.$$

Ist endlich $|\mathfrak{u}, \mathfrak{v}| = 0$, so läßt sich eine neue Basis $\mathfrak{u}_0, \mathfrak{u}_1$ mit der Produkttafel $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$ angeben ($a \neq 0$). Da $\mathfrak{R}$ kein Radikal besitzt, gibt es einen Vektor $\mathfrak{u}_2$ mit $\mathfrak{u}_0\mathfrak{u}_2 = 1$. Für $\mathfrak{u}_0, \mathfrak{u}_1, \mathfrak{u}_2$ lautet die Produkttafel $\begin{pmatrix} 0 & 0 & 1 \\ 0 & a & * \\ 1 & * & * \end{pmatrix}$, diese Vektoren spannen also einen dreidimensionalen Raum $\mathfrak{r}$ mit $|\mathfrak{r}| \neq 0$ auf. Es gilt

$$\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^* \quad \text{und} \quad \mathfrak{r} = \langle \mathfrak{u} \rangle + \mathfrak{U} = \langle \mathfrak{v} \rangle + \mathfrak{V}.$$

Dabei enthalten $\mathfrak{U}$ und $\mathfrak{V}$ beide den Vektor $\mathfrak{u}_0$ mit $\mathfrak{u}_0^2 = 0$, sind also nach dem Hilfssatz isomorphe Räume. Nun folgt

$$\langle \mathfrak{u} \rangle^* = \mathfrak{U} + \mathfrak{r}^* \cong \mathfrak{V} + \mathfrak{r}^* = \langle \mathfrak{v} \rangle^*, \text{ w. z. b. w.}$$

Anmerkung. Aus Satz 4 können leicht folgende Tatsachen erschlossen werden: Jede Lösung ω_{i1} der Gleichung $\sum_i a_i x_i^2 = a_1$ läßt sich zu einer Substitution $x_i = \sum_k \omega_{ik} y_k$ ergänzen, die die Form $\sum_i a_i x_i^2$ festläßt. Ebenfalls jede Lösung ω_{i1}, ω_{i2} des Gleichungssystems

$$\sum_i a_i x_{i1}^2 = a_1, \quad \sum_i a_i x_{i2}^2 = a_2, \quad \sum_i a_i x_{i1} x_{i2} = 0. \quad \text{Usw.}$$

Sind f und g zwei quadratische Formen, und sind die Variablen der einen Form unabhängig von den Variablen der anderen, so bilden wir die Summe $f + g$. Satz 4 können wir dann auch so aussprechen:

Aus $f_1 + f_3 \cong f_2 + f_3$ *darf* $f_1 \cong f_2$ *geschlossen werden.*

Für die Klassifikation der quadratischen Formen lehrt der folgende Satz, daß es nur auf die Kenntnis derjenigen Formen ankommt, welche die Null nicht darstellen (Grundformen). Angewandt auf den Körper P der reellen Zahlen ergibt sich beispielsweise sofort, daß der Trägheitsindex einer quadratischen Form invariant bleibt bei allen Transformationen.

Satz 5. *Stellt f die Null dar, so kann f auf die Gestalt $x^2 - y^2 + f'$ transformiert werden. Die Form f' ist (nach Satz 4) durch f bis auf Äquivalenz eindeutig bestimmt.*

Beweis. Es sei $\mathfrak{u}^2 = 0$, $\mathfrak{u} \neq 0$. Da $\mathfrak{R}$ kein Radikal besitzt, gibt es einen Vektor $\mathfrak{v}$ mit $\mathfrak{u}\mathfrak{v} = 1$. Für $\mathfrak{u}$, $\mathfrak{v}$ lautet die Produkttafel $\begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}$, diese Vektoren spannen also einen zweidimensionalen Raum $\mathfrak{r}$ mit $|\mathfrak{r}| \neq 0$ auf. Es gilt $\mathfrak{R} = \mathfrak{r} + \mathfrak{r}^*$, dabei hat $\mathfrak{r}$ nach dem Hilfssatz die Metrik $x^2 - y^2$.

Möglicherweise stellt auch f' die Null dar, dann ist

$$f' \cong x'^2 - y'^2 + f'', \qquad f \cong (x^2 - y^2) + (x'^2 - y'^2) + f''.$$

Auch die Form f'' ist durch f bis auf Äquivalenz eindeutig festgelegt.

Spalten wir von f möglichst oft Formen der Gestalt $X^2 - Y^2$ ab, so gelangen wir entweder zur leeren Form 0 oder zu einer Form, die nicht mehr die Null darstellt. Diese Form nennen wir die **Grundform** von f. Sie ist bis auf Äquivalenz durch f eindeutig bestimmt.

Zur Aufstellung aller Klassen äquivalenter Formen genügt daher die Angabe aller Klassen äquivalenter Grundformen.

Wenn f und g äquivalente Grundformen haben, so sagen wir, f und g sind **ähnlich**, $f \sim g$. Haben die Diagonalformen f und g die Koeffizienten a_i bzw. b_k, so erklären wir die **Summe** $f + g$ und das **Produkt** $f \cdot g$ durch die Diagonalformen mit den Koeffizienten a_i, b_k bzw. $a_i b_k$.

Es gilt $f - f \sim 0$, denn diese Form hat die Koeffizienten a_i, $-a_i$, und nach dem Hilfssatz kann jedes Paar a_i, $-a_i$ durch 1, -1 ersetzt werden. Wie jetzt leicht zu sehen ist, gilt

Satz 6. *Die Klassen ähnlicher Formen bilden einen Ring.*

Merkwürdig ist die Parallele zwischen quadratischen Formen und den normalen einfachen Algebren. Die Grundformen entsprechen den Schiefkörpern. In beiden Fällen führt die Einteilung in „ähnliche" Objekte zu einer Gruppe. Vermutlich besteht die Analogie noch in einem weiteren Umfange; so wäre es wünschenswert, zu beweisen, *daß eine Grundform auch in jedem Oberkörper von ungeradem Grad m die Null nicht darstellen kann.*

Ist bei festem Oberkörper $\overline{K}$ diese Vermutung für alle Formen mit $n \leqq m$ richtig, so läßt sie sich auch für jede Form f mit $n > m$ beweisen: Die Grundform f gehöre zum Raum $\mathfrak{R}$. Durch Erweiterung des Koeffizientenbereichs zu $\overline{K}$ entstehe der Raum $\overline{\mathfrak{R}}$. Ist $f = 0$ in $\overline{K}$ lösbar, so gibt es in $\overline{\mathfrak{R}}$ einen Vektor $\bar{\mathfrak{u}} \neq 0$ mit $\bar{\mathfrak{u}}^2 = 0$. Wegen $n > m$ ist $\bar{\mathfrak{u}}\mathfrak{v} = 0$ mit $\mathfrak{v} \neq 0$ aus $\mathfrak{R}$ lösbar. Da f Grundform ist, folgt $\mathfrak{v}^2 \neq 0$; $\bar{\mathfrak{u}}$ liegt im $(n-1)$-dimensionalen Raum $\overline{\langle \mathfrak{v} \rangle^*}$. Dies ist aber ein Widerspruch, wenn die Vermutung schon bis $n-1$ bewiesen ist.

Aus den allgemeinen Kriterien der Nulldarstellbarkeit (Abschnitt II) folgt die *Richtigkeit der Vermutung für*

$$n = 1, 2, 3, 4 \text{ und jedes ungerade } m,$$

nach der soeben gemachten Bemerkung folgt die Gültigkeit außerdem für

$$m = 3 \text{ und jedes } n.$$

Zum Nachweis, daß irgendein Ausdruck, der von den Koeffizienten einer Diagonalform $f = \Sigma a_i x_i^2$ abhängt, bei jeder Transformation (in andere Diagonalformen) invariant

bleibt, kann der Satz 7 dienlich sein. Wird eine binäre Teilform $a_i x_i^2 + a_k x_k^2$ in $a_i' x_i'^2 + a_k' x_k'^2$ transformiert, so ist damit auch eine Umformung von f in eine Diagonalform f' gegeben.

Satz 7. *Zwei äquivalente Diagonalformen f und g lassen sich immer derartig durch mehrmalige binäre Transformation ineinander überführen, daß jeweils die Diagonalgestalt bestehen bleibt.*

Beweis. Erstens sei f eine Grundform. Bekanntlich läßt sich jede Transformation aus Elementartransformationen zusammensetzen. D. h. jede Form läßt sich in eine äquivalente Form dadurch überführen, daß auf die Matrix der Form die folgenden Operationen wiederholt angewandt werden:

a) Vertauschung zweier benachbarter Zeilen,

b) Multiplikation einer Zeile mit einer Zahl,

c) Addition einer vervielfachten Zeile zu einer späteren,

jedesmal verbunden mit einer entsprechenden Umformung auf die Spalten. Bei einer derartigen allmählichen Transformation von f in g mögen die Matrizen $A_1, \ldots, A_s$ auftreten; dabei brauchen nur A_1 und A_s Diagonalmatrizen zu sein. Da f nicht die Null darstellt, läßt sich Satz 2 auf jede Matrix A_j anwenden, und wir gelangen dadurch zu einer äquivalenten Diagonalform f_j. A_j und A_{j+1} unterscheiden sich höchstens in einer der Teildeterminanten des Satzes 2, f_j und f_{j+1} unterscheiden sich daher höchstens in zwei Koeffizienten. Nach Satz 4 läßt sich f_j schon durch Transformation einer binären Teilform in f_{j+1} überführen. Wegen $f_1 = f$, $f_s = g$ ist die Behauptung für Grundformen bewiesen.

Zweitens stelle f die Null dar. f habe die Koeffizienten $a_1, a_2, a_3, \ldots$. Nach Satz 5 kann f in eine Form h mit den Koeffizienten $1, -1, c_3, \ldots$ transformiert werden. Wegen Satz 3 kann h binär in $a_1, -a_1, c_3, \ldots$ verwandelt werden. Die Behauptung sei schon für Formen mit weniger Variablen bewiesen. Nach Satz 4 ist $-a_1, c_3, \ldots \cong a_2, a_3, \ldots$, die Überführung kann durch mehrmalige binäre Transformation geschehen. Daher läßt sich f und ebenso g in der gewünschten Weise in h überführen. Damit ist die ganze Behauptung bewiesen.

Zu einem festen quadratischen Oberkörper K_2/K können *hermitesche Formen*

$$\sum_{i,k} a_{ik} x_i \bar{x}_k \qquad (a_{ik} = \overline{a_{ki}} \text{ aus } K_2)$$

eingeführt werden. *Alle Sätze dieses Abschnittes lassen sich* ohne Schwierigkeit auch *auf hermitesche Formen übertragen.* (Die Diskriminante $|a_{ik}|$ multipliziert sich hier bei Transformation mit der Norm einer Zahl aus K_2).

II. Die Systeminvariante $S(f)$ einer quadratischen Form.

Weitere Ergebnisse über quadratische Formen $f = \sum_{i=1}^{n} a_i x_i^2$ aus einem beliebigen Grundkörper K können wir gewinnen, wenn wir jeder solchen Form ein gewisses assoziatives hyperkomplexes System zuordnen.

Das Cliffordsche Zahlsystem $C(f)$ hat die Basis

$$u_1^{\nu_1} u_2^{\nu_2} \cdots u_n^{\nu_n} \qquad (\nu_i = 0, 1)$$

vom Rang 2^n und die Rechentafel

$$u_i^2 = a_i, \quad u_i u_k = -u_k u_i \qquad (i \neq k).$$

Die Rechenvorschrift können wir auch in eine einzige Regel zusammenfassen:

$$(\Sigma x_i u_i)^2 = \Sigma a_i x_i^2 = f.$$

Satz 8. *Zu äquivalenten Diagonalformen gehören isomorphe Cliffordsche Zahlsysteme.*

Beweis. f werde durch die Substitution $x_\alpha = \Sigma p_{\alpha\beta}\overline{x}_\beta$ in eine andere Diagonalform $\overline{f} = \Sigma \overline{a}_i \overline{x}_i^2$ übergeführt. $C(f)$ wird auch durch die Größen $\overline{u}_\beta = \Sigma u_\alpha p_{\alpha\beta}$ erzeugt. Wegen $\Sigma \overline{x}_i \overline{u}_i = \Sigma x_i u_i$ und $\Sigma a_i x_i^2 = \Sigma \overline{a}_i \overline{x}_i^2$ gilt

$$(\Sigma \overline{x}_i \overline{u}_i)^2 = \Sigma \overline{a}_i \overline{x}_i^2 = \overline{f}.$$

Da diese Gleichung genau so aussieht, wie die Rechenvorschrift für das System $C(\overline{f})$, ist $C(f) \cong C(\overline{f})$.

Das System $C(a_1 x_1^2 + a_2 x_2^2)$ wird in der Algebrentheorie gewöhnlich mit (a_1, a_2) bezeichnet; es ist einfach und hat den Grundkörper K als Zentrum. Für eine Form f mit ungerader Variablenzahl braucht das Cliffordsche System nicht mehr einfach zu sein. Aus diesem Grunde werden wir jetzt jeder Form f ein anderes invariantes System $S(f)$ zuordnen; dabei wird $S(f)$ direktes Produkt von mehreren Systemen der Gestalt (a, b) sein, also auch selbst einfach und normal sein.

Wir setzen $S(f) = C(F_n)$, wobei $F_n = f - \sum_{i=1}^{n} x_{-i}^2$ eine Form mit $2n$ Variablen ist, so daß $S(f)$ den Rang 4^n hat. Es ist nach Satz 8 klar, daß sich $S(f)$ nicht ändert bei Transformationen von f. Wir beweisen nun

Satz 9. $S(f) = \prod_{k=1}^{n} (d_k, a_k), \quad d_k = a_1 \cdots a_k.$

$C(F_n)$ wird von den Größen $u_1, u_{-1}, \ldots, u_n, u_{-n}$ erzeugt. Wegen $u_i^2 = a_i \neq 0$ sind dies keine Nullteiler. Wir setzen

$$v_1 = (u_1 u_{-1})(u_2 u_{-2}) \cdots (u_{n-1} u_{1-n})(u_n), \qquad v_2 = u_n u_{-n}.$$

Es ist $v_2 = a_n$. Um v_1^2 zu berechnen, beachten wir, daß die einzelnen Klammern, aus denen v_1 zusammengesetzt ist, untereinander vertauschbar sind. So folgt $v_1^2 = a_1 a_2 \cdots a_n = d_n$, ferner gilt $v_1 v_2 = -v_2 v_1$. v_1, v_2 erzeugen also ein Untersystem (d_n, a_n) vom Rang 4. Die mit v_1 und v_2 vertauschbaren Größen $u_1, u_{-1}, \ldots, u_{n-1}, u_{1-n}$ erzeugen ein anderes Untersystem $C(F_{n-1})$ vom Rang 4^{n-1}. Beide Systeme erzeugen zusammen $C(F_n)$. Mithin ist $C(F_n) = C(F_{n-1}) \times (d_n, a_n)$, aus dieser Rekursionsformel ergibt sich die behauptete Zerlegung von $S(f)$.

Bemerkung. Das Cliffordsche Zahlsystem $C(f)$ läßt sich für eine quadratische Form $\Sigma a_{ik} x_i x_k$ auch dann invariant definieren, wenn die Matrix a_{ik} nicht Diagonalgestalt hat: $u_1, \ldots, u_n$ seien assoziative, unvertauschbare Unbestimmte mit der definierenden Relation

$$(\Sigma x_i u_i)(\Sigma y_k u_k) = \Sigma a_{ik} x_i y_k,$$

d. h.

$$u_i u_k + u_k u_i = 2 a_{ik}.$$

Werden die 2^n linear unabhängigen Produkte der u_i mit U_I bezeichnet, so sind die Komponenten P_{IK}^L der Multiplikationstafel $U_I U_K = \sum_L P_{IK}^L U_L$ Polynome in den Koeffizienten a_{ik}.

Ähnlich wie in Satz 9 läßt sich auch $C(f)$ in Faktoren zerlegen, und zwar spaltet sich bei geradem n ein Faktor vom Rang 4, bei ungeradem n einer vom Rang 2 ab. Diese Faktoren sind jedoch komplizierter gebaut, überdies haben wir nachgeprüft, daß $C(f)$

schon von $S(f)$ und der Diskrimante d abhängt, so daß ein näheres Eingehen auf das System $C(f)$ unnötig ist.

Im Sinne der Algebrenähnlichkeit gelten, wie bekannt, folgende Regeln:

$$(a, c)\,(b, c) \sim (ab, c), \quad (b, a) \sim (a, b), \quad (a, -a) \sim 1 \quad \text{(Zerfall)}.$$

Auf Grund dieser Regeln finden wir für $S(f)$ die Zerlegungen

$$S(f) \sim \prod_{i \leqq k} (a_i, a_k) \sim \prod_k (-d_{k-1}, d_k).$$

Nach einer kleinen Rechnung folgt

Satz 10. *Es gilt*

$$S(mf) \sim (m, (-1)^{\frac{n(n+1)}{2}} d^{n+1})\, S(f),$$
$$S(f+g) \sim (d(f), d(g))\, S(f)\, S(g).$$

Aus $d(f+g) \cong d(f+h)$ *und* $S(f+g) \sim S(f+h)$ *folgt* $d(g) \cong d(h)$ *und* $S(g) \sim S(h)$.

Im allgemeinen bilden d und S kein vollständiges Invariantensystem für die Äquivalenz quadratischer Formen. Z. B. haben für $n = 4$ die beiden Formen f und $-df$ stets gleiche Invarianten d und S, und trotzdem brauchen f und $-df$ nicht äquivalent zu sein, man betrachte etwa $f = \sum_1^4 x_i^2$ im Körper der reellen Zahlen.

Satz 11. *Für* $n = 1, 2, 3$ *sind* d *und* S *ein vollständiges Invariantensystem für Äquivalenz quadratischer Formen.*

Beweis. Für $n = 1$ ist d die einzige Invariante.

Für $n = 2$ seien $f = a x^2 + b y^2$ und $\bar{f} = \bar{a}\bar{x}^2 + \bar{b}\bar{y}^2$ zwei Formen mit gleichen Invarianten d und S. Wegen $S(f) \sim (-1, d)\,(a, b)$ und $S(\bar{f}) \sim (-1, d)\,(\bar{a}, \bar{b})$ ist $(a, b) \cong (\bar{a}, \bar{b})$, daher sind die Normenformen dieser Algebren

$$z_0^2 - a z_1^2 - b z_2^2 + ab z_3^2 \quad \text{und} \quad \bar{z}_0^2 - \bar{a}\bar{z}_1^2 - \bar{b}\bar{z}_2^2 + \bar{a}\bar{b}\bar{z}_3^2 \qquad (ab = \bar{a}\bar{b} = d)$$

einander äquivalent. Nach Satz 4 folgt daraus die Äquivalenz von f mit $\bar{f}$.

Für $n = 3$ seien $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2$ und $\bar{f}$ zwei Formen mit gleichen Invarianten d und S. Eine leichte Rechnung ergibt

$$s(f) = (-a_1 a_2, -a_1 a_3) \sim (-1, -1)\, S(f) \qquad (\text{für } n = 3).$$

Es ist also $(-a_1 a_2, -a_1 a_3) \cong (-\bar{a}_1\bar{a}_2, -\bar{a}_1\bar{a}_3)$, daher sind die mit $d = a_1 a_2 a_3 = \bar{a}_1\bar{a}_2\bar{a}_3$ multiplizierten Normenformen dieser Algebren

$$d z_0^2 + a_3 z_1^2 + a_2 z_2^2 + a_1 z_3^2 \quad \text{und} \quad d\bar{z}_0^2 + \bar{a}_3\bar{z}_1^2 + \bar{a}_2\bar{z}_2^2 + \bar{a}_1\bar{z}_3^2$$

einander äquivalent. Nach Satz 4 folgt daraus wieder $f \cong \bar{f}$.

Anwendung *auf solche Körper* k, *in denen jede Algebra* (a, b) *zerfällt.* **Beispiele** sind:

Ein Galoisfeld (nach dem Satz von Wedderburn);

ein algebraischer *Funktionenkörper* einer Variablen *mit algebraisch abgeschlossenem Konstantenkörper* (nach Tsen (6));

der reelle Funktionenkörper $\mathrm{P}(x, \sqrt{-1 - x^2})$ und dessen endliche Erweiterungen (Witt (8)).

Satz 12. *In solchen Körpern* K *sind* n *und* d *die einzigen Invarianten für die Äquivalenz quadratischer Formen.*

Beweis. Die Behauptung stimmt für $n = 1$ und nach Satz 11 auch für $n = 2$. Es sei $n > 2$ und die Behauptung bis $n - 1$ bewiesen. Dann ist

$$a_1, a_2, a_3, \ldots, a_n \cong 1, a_1 a_2, a_3, \ldots, a_n \cong 1, 1, 1, \ldots, d.$$

K sei wieder ein beliebiger Körper. Nach Satz 5 kann jede die Null darstellende Form f auf die Gestalt $x^2 - y^2 - dz^2$ gebracht werden, es folgt $s(f) \sim 1$. Aus Satz 11 folgt, daß umgekehrt eine Form f mit $s(f) \sim 1$ in $x^2 - y^2 - dz^2$ transformiert werden kann, mithin $f = 0$ lösbar ist:

Satz 13. *Für die Lösbarkeit von* $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$ *ist die Bedingung* $(-1, -1)\, S(f) \sim (-a_1 a_2, -a_1 a_3) \sim 1$ *notwendig und auch hinreichend.*

Für $n = 4$ beweisen wir

Satz 14. *Für die Lösbarkeit von* $f = a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + a_4 x_4^2 = 0$ *ist notwendig und auch hinreichend, daß die Algebra* $(-a_1 a_2, -a_1 a_4)$ *im Oberkörper* $K(\sqrt{d})$ *zerfällt.*

Wir setzen $-a_1 a_2 = a$, $-a_1 a_3 = b$, $a_1 a_2 a_3 = c$, $a_1 a_2 a_3 a_4 = d$. Im Oberkörper $K(\sqrt{d})$ wird $d \cong 1$, also wird

$$cf \cong dx_4^2 - ax_3^2 - bx_2^2 + abx_1^2$$

Normenform der Algebra (a, b). $f = 0$ in $K(\sqrt{d})$ ist daher gleichbedeutend mit $(a, b) \sim 1$ in $K(\sqrt{d})$. Aus $f = 0$ in K folgt erst recht $f = 0$ in $K(\sqrt{d})$, aber es ist auch der umgekehrte Schluß richtig: Sei $K(\sqrt{d}) > K$, d. h. $d \neq 1$ in K. Wenn dann $K(\sqrt{d})$ Zerfällungskörper von (a, b) ist, muß nach der allgemeinen Algebrentheorie ein zu $K(\sqrt{d})$ isomorpher Körper in (a, b) vorkommen, d muß also das Quadrat eines Elements $x_0 + x_3 u + x_2 v + x_1 uv$ aus (a, b) sein. Daraus folgt $x_0 = 0$ und $d = ax_3^2 + bx_2^2 - abx_1^2$, mithin ist $cf = 0$ auch in K lösbar. Satz 14 ist damit bewiesen.

In K braucht (a, b) keine Invariante von f zu sein, dagegen folgt nach leichter Rechnung die Invarianz im Oberkörper $K(\sqrt{d})$ wegen

$$(-a_1 a_2, -a_1 a_3) \sim (-1, -1)\, S(f) \text{ in } K(\sqrt{d}) \qquad (\text{für } n = 4),$$

indem wieder $d \cong 1$ in $K(\sqrt{d})$ beachtet wird.

Den Inhalt der Sätze 11, 13, 14 stellen wir in einer Tabelle zusammen:

n	Volles Invariantensystem für Äquivalenz	Bedingung für die Darstellbarkeit der Null
1	d	unmöglich
2	d und S	$d \cong -1$
3	d und S	$S \sim (-1, -1)$
4	?	$S \sim (-1, -1)$ in $K(\sqrt{d})$

Bemerkung (vgl. (4)). K enthalte mehr als 5 Elemente. Es seien $a, b, x \neq 0$, dann läßt sich t so wählen, daß $bt^2 \neq \pm a, 0$ wird, und es folgt

$$a \cdot x^2 + b \cdot 0^2 = a\left(x \frac{bt^2 - a}{bt^2 + a}\right)^2 + b\left(\frac{2axt}{bt^2 + a}\right)^2,$$

worin die neuen Quadrate nicht verschwinden. Durch Wiederholung dieses Verfahrens kann eine Lösung $x_1, \ldots, x_n$ von $f = 0$ (nicht alle $x_i = 0$) stets durch eine andere Lösung $y_1, \ldots, y_n$ ersetzt werden, in der sogar *alle* $y_i \neq 0$ sind.

Satz 15. *Darstellbarkeit einer Zahl* $m \neq 0$ *durch eine Form* f *ist gleichwertig mit der Lösbarkeit von* $f - mx^2 = 0$.

Denn jede Lösung von $f = m$ liefert eine Lösung von $f - mx^2 = 0$; ist umgekehrt $f - mx^2 = 0$ lösbar, so gibt es auch eine Lösung mit $x \neq 0$, sogar mit $x = 1$, also ist $f = m$ lösbar. Dasselbe gilt auch in den Körpern von 3 oder 5 Elementen, da für $n > 1$ jede Form f sämtliche Zahlen $m \neq 0$ darstellt.

Anwendung auf einen $\mathfrak{p}$-adischen Zahlkörper ($\mathfrak{p}$ endlich):

Satz 16. *In einem $\mathfrak{p}$-adischen Zahlkörper stellt jede quinäre quadratische Form die Null dar (also auch jede Form mit $n \geqq 5$).*

Zum Beweis werde angenommen, daß $f = 0$ unlösbar ist. Dies trifft dann auch zu für die Teilform a_1, a_2, a_3, a_4 von $df = a_1, a_2, a_3, a_4, a_5$. Nach Satz 14 ist $K(\sqrt{a_1a_2a_3a_4})$ kein Zerfällungskörper von $(-a_1a_2, -a_1a_3)$. Im $\mathfrak{p}$-adischen wird bekanntlich eine Algebra (a, b) von jedem quadratischen Oberkörper zerfällt, also ist $a_1a_2a_3a_4 \cong 1$ oder $a_5 \cong 1$. Entsprechend folgt $a_i \cong 1$, also $df \cong \sum_1^5 x_i^2$. Weiter ist $(-a_1a_2, -a_1a_3) = (-1, -1) \dotplus 1$, das ergibt $\mathfrak{p} \mid 2$. In diesem Fall liegt $\sqrt{-7}$ in K und es ist $1^2 + 1^2 + 1^2 + 2^2 + \sqrt{-7}^2 = 0$, $df = 0$ ist doch lösbar, w. z. b. w.

Anwendung *auf solche Körper K, in denen jede quinäre quadratische Form die Null darstellt.* **Beispiele** sind:

Ein $\mathfrak{p}$-adischer Zahlkörper für endliches $\mathfrak{p}$ (Satz 16);

ein algebraischer *Funktionenkörper* einer Variablen *mit endlich vielen Konstanten* (nach Chevalley (**1**) (**7**) und Tsen (**6**));

ein algebraischer *Funktionenkörper in zwei Variablen mit algebraisch abgeschlossenem Konstantenkörper* (Tsen (**6**)).

Satz 17. *In solchen Körpern K sind n, d und S ein volles Invariantensystem für die Äquivalenz von quadratischen Formen.*

Beweis. Für $n = 1, 2, 3$ war das schon gezeigt. Es sei $n > 3$ und die Behauptung bis $n - 1$ bewiesen. f und $\bar{f}$ seien zwei Formen mit gleichen Invarianten d und S. Wir setzen $f = ax^2 + h$. Nach Voraussetzung ist $\bar{f} = a$ lösbar, daher kann nach Satz 1 die Form $\bar{f}$ auf die Gestalt $a\bar{x}^2 + \bar{h}$ gebracht werden. Aus Satz 10 folgt $d(h) \cong d(\bar{h})$ und $S(h) \sim S(\bar{h})$. Wegen der Induktion ist $h \cong \bar{h}$, folglich $f \cong \bar{f}$.

Es wird jetzt noch gezeigt, welche Algebren S auftreten können als Invarianten von quadratischen Formen f mit vorgegebener Variablenanzahl $n > 1$ und vorgegebener Diskriminante d.

Satz 18. *Für $n = 2$ und vorgegebenem d treten genau diejenigen S auf, für die $S \sim (-1, -1)$ in $K(\sqrt{-d})$ ist.*

Wird über den Körper K die einschränkende Voraussetzung gemacht, daß alle Algebren (a, b) eine Gruppe bilden, so treten die Invarianten $n \geqq 3$, d und $S \sim (a, b)$ in beliebiger Zusammenstellung wirklich auf.

Beweis. Für die Form $ax^2 + by^2$ ist $(-1, -1)S \sim (-a, -d)$, also $S \sim (-1, -1)$ in $K(\sqrt{-d})$. Wird dies umgekehrt über S vorausgesetzt, so läßt sich $(-1, -1)S$ in der Gestalt $(-a, -d)$ schreiben, und die Form $ax^2 + ady^2$ hat die Invarianten d und S. $n \geqq 3$, d und (a, b) seien vorgelegt. Nach Voraussetzung dürfen wir $(-1, -1)(a, b) \sim (p, q)$ setzen. Für

$$g = dpqx_1^2 - dqx_2^2 - dpx_3^2$$

ist dann $s(g) = (p, q)$, also $S(g) \sim (a, b)$. $f = g + \sum_{i=4}^{n} x_i^2$ ist also eine Form mit den Invarianten n, d und $S \sim (a, b)$.

Beispiele *von Körpern, in denen die Algebren (a, b) eine Gruppe bilden:*

Zahlkörper,

$\mathfrak{p}$-adische Körper,

algebraische Funktionenkörper einer Variablen mit endlich vielen Konstanten.

III. Quadratische Formen in speziellen Körpern.

Für einen *$\mathfrak{p}$-adischen Körper* ($\mathfrak{p}$ endlich) oder einen
algebraischen Funktionenkörper über einem Galoisfeld
geben die Sätze 17 und 18 eine klare Übersicht über die Klassen äquivalenter Formen: n, d und S sind ein vollständiges Invariantensystem, und für $n \geqq 3$ sind d und S unabhängig. Im Falle $n \geqq 5$ stellt jede Form die Null dar, für $n = 1, 2, 3, 4$ ist die Bedingung für die Lösbarkeit von $f = 0$ auf der allgemeingültigen Tabelle auf S. 39 angegeben.

Im Falle des *Körpers der reellen Zahlen* sind der Rang n und der Trägheitsindex j (Anzahl der negativen Quadrate) ein vollständiges Invariantensystem, und zwischen ihnen besteht die einzige Relation $0 \leqq j \leqq n$. Die Bedingung für die Lösbarkeit von $f = 0$ lautet: $0 < j < n$.

Das Ziel in diesem Abschnitt ist, eine entsprechende Übersicht zu gewinnen für
1. *Zahlkörper*,
2. *reelle Funktionenkörper einer Variablen.*

1. Zahlkörper.

Aus der Zahlkörpertheorie sind für uns folgende Tatsachen grundlegend:

(1) Wenn eine Zahl an allen Primstellen $\mathfrak{p}$ (d. h. in allen $\mathfrak{p}$-adischen Oberkörpern) Quadratzahl ist, so ist sie schlechthin (d. h. im Zahlkörper K) Quadratzahl.

(2) Wenn eine Algebra (a, b) an allen Primstellen zerfällt, so zerfällt (a, b) schlechthin.

(3) Die Anzahl der Stellen, an denen (a, b) nicht zerfällt, ist gerade.

(4) Die Algebren (a, b) bilden eine Gruppe.

Für den Beweis des nachfolgenden Satzes bemerken wir:

(5) Im Falle einer ternären Form ist $f = 0$ an einer geraden Anzahl von Stellen unlösbar. Dies folgt aus (3) und Satz 13.

(6) Ist $\mathfrak{p}$ endlich und kein Teiler von 2, und sind mindestens drei Koeffizienten einer Diagonalform f prim zu $\mathfrak{p}$, so stellt f an der Stelle $\mathfrak{p}$ die Null dar. Denn die Theorie der $\mathfrak{p}$-adischen Körper lehrt, daß an solchen Stellen $\mathfrak{p}$ eine Algebra (a, b) zerfällt, sobald $\mathfrak{p}$ prim ist zu a und b; nach Satz 13 enthält die Form f also eine ternäre Teilform, welche die Null darstellt.

Satz 19. *Wenn $f = 0$ an allen Stellen lösbar ist, so auch im Zahlkörper K.*

Beweis. Für $n = 1, 2, 3, 4$ folgt die Nulldarstellbarkeit in K aus der Tabelle auf S. 39 in Verbindung mit (1) und (2).

Nun sei $n \geqq 5$. Wir setzen $f = \varphi - \psi$, wobei φ $n - 2$ und ψ zwei Variable enthält. $\mathfrak{p}_i$ durchlaufe erstens alle Primideale, die in den Koeffizienten von f vorkommen, zweitens alle Primfaktoren von 2, drittens alle unendlichen Stellen. Bei der Nulldarstellung von f in $k_{\mathfrak{p}_i}$ mögen φ und ψ den Wert μ_i annehmen. Sollte $\mu_i = 0$ sein, so stellen φ und ψ alle Zahlen dar, wir dürfen daher $\mu_i \neq 0$ annehmen. In folgender Weise approximieren wir jetzt die endlich vielen μ_i durch ein einziges μ aus dem Zahlkörper K:

In $\mathfrak{p}_i^e$ werde der Exponent e so hoch gewählt, daß der Strahl mod $\mathfrak{p}_i^e$ aus lauter $\mathfrak{p}_i$-adischen Quadratzahlen besteht. Ist $\mathfrak{p}_i^{a_i}$ der genaue Beitrag zu μ_i an der endlichen Stelle $\mathfrak{p}_i$, so wählen wir eine Hilfszahl ϱ mit

$$(\varrho) = \mathfrak{a} \prod_{\text{endl.}} \mathfrak{p}_i^{a_i}, \quad (\mathfrak{a}, \mathfrak{p}_i) = 1.$$

Nach dem Satz von der arithmetischen Progression gibt es ein Primideal $\mathfrak{q}$ mit

$$\mathfrak{q} = \mathfrak{a}\xi, \quad \xi \equiv \frac{\mu_i}{\varrho} \bmod \mathfrak{p}_i^e.$$

Wird jetzt $\mu = \varrho\xi$ gesetzt, so folgt

$$(\mu) = \mathfrak{q} \prod_{\text{endl.}} \mathfrak{p}_i^{a_i}, \qquad \mu \equiv \mu_i \bmod \mathfrak{p}_i^{e}.$$

Wir zeigen jetzt, daß die Formen φ und ψ an allen Stellen die Zahl μ darstellen. Für $\mathfrak{p} = \mathfrak{p}_i$ ist dies der Fall, da an diesen Stellen $\mu \cong \mu_i$ ist.

Wegen (6) stellt die Form $\varphi - \mu x^2$ an den Stellen $\mathfrak{p} \neq \mathfrak{p}_i$, und falls außerdem $\mathfrak{p} \neq \mathfrak{q}$ ist, auch die Form $\psi - \mu y^2$ die Null dar. Für die restliche Stelle $\mathfrak{q}$ muß $\psi - \mu y^2 = 0$ nach (5) lösbar sein.

Da die Formen $\varphi - \mu x^2$ und $\psi - \mu y^2$ weniger als n Variablen enthalten, und an allen Stellen die Null darstellen, dürfen wir für sie die Nulldarstellbarkeit in K schon annehmen. Wenn aber φ und ψ beide in K die Zahl μ darstellen, so ist $f = \varphi - \psi = 0$ in K lösbar, q. e. d.

Satz 20. *Wenn an allen Stellen $f \sim 0$ ist oder wenn überall $f \cong g$ ist, so gilt das entsprechende schlechthin im Körper K.*

Beweis durch Induktion nach n. Es sei $n > 0$, und überall $f \sim 0$. Nach Satz 19 ist $f = 0$ in K lösbar, d. h. nach Satz 5 ist $f \sim f'$ in K $(n' < n)$. Weil an allen Stellen $f' \sim 0$ ist, gilt im Körper K: $f' \sim 0$ und damit $f \sim 0$. — Wenn f und g gleichviel Variable enthalten, so ist die Aussage $f \cong g$ gleichwertig mit $f - g \sim 0$.

Die Sätze 19 und 20 ermöglichen uns, die Theorie der quadratischen Formen im Großen (d. h. im Zahlkörper K) zurückzuführen auf die schon hergeleitete Theorie im Kleinen (d. h. in den $\mathfrak{p}$-adischen Körpern, Sätze 16 und 17).

Mit j_ν bezeichnen wir den Trägheitsindex einer Form f an der reellen unendlichen Erweiterung K_ν. Werden die neuen Ergebnisse in die Tabelle auf S. 39 aufgenommen, so erhalten wir die beiden ersten Spalten der folgenden

Tabelle für einen Zahlkörper K.

n	Volles Invariantensystem für Äquivalenz	Bedingungen für die Darstellbarkeit der Null	Einzige Relationen zwischen den angegebenen Invarianten
1	d	unmöglich	keine
2	d und S	$d \cong -1$	$S \sim (-1, -1)$ in $K(\sqrt{-d})$
3	d und S	$S \sim (-1, -1)$	keine
4	d, S, j_ν	$S \cong (-1, -1)$ in $K(\sqrt{d})$	$d \cong (-1)^{j_\nu}$ und $S \sim (-1, -1)^{\frac{j_\nu(j_\nu+1)}{2}}$ in K_ν $(0 \leqq j_\nu \leqq n)$.
5, 6, usw.	d, S, j_ν	$0 < j_\nu < n$	

Es ist noch die letzte Tabellenspalte nachzuprüfen: Für $n = 2, 3$ ist Satz 18 maßgebend. Wie ferner eine leichte Rechnung ergibt, gelten die Relationen

$$(n) \qquad d \cong (-1)^{j_\nu} \quad \text{und} \quad S \sim (-1, -1)^{\frac{j_\nu(j_\nu+1)}{2}} \quad \text{in } K_\nu \qquad (0 \leqq j_\nu \leqq n)$$

sicher für jedes n. Für $n = 3$ folgt allein aus diesen Relationen, daß j_ν nur von d und S abhängt.

Es sei $n \geqq 4$. Wir beweisen jetzt induktiv, daß außer den Relationen (n) keine weiteren bestehen zwischen den Invarianten d, S, j_ν, indem wir zeigen:

Satz 21. *Wenn zwischen gegebenen d, S, j_ν die Relationen (n) bestehen, so gibt es eine quadratische Form f mit diesen Invarianten $(n \geqq 4)$.*

Zu diesem Zweck werde

$$\iota_\nu = \begin{cases} 0 & \text{falls } j_\nu \neq n \\ 1 & \text{falls } j_\nu = n \end{cases}$$

eingeführt. In K werde eine Zahl δ mit dem K_ν-Vorzeichen $(-1)^{\iota_\nu}$ bestimmt. Aus den angenommenen Relationen (n) für n, d, S, j_ν folgen nach leichter Umformung die entsprechenden Relationen $(n-1)$ für die Größen

$$d' = d\delta, \quad S' = S \cdot (\delta, d), \quad j'_\nu = j_\nu - \iota_\nu.$$

Im Fall $n - 1 = 3$ sei f' eine Form mit den Invarianten d' und S'. Wie schon gesagt, hat dann f' von selbst die Trägheitsindizes j_ν. Falls $n - 1 > 3$, gibt es nach Induktionsvoraussetzung eine Form f' zu d', S', j'_ν.

Aus Satz 9 folgt jetzt, daß die Form $f = \delta x^2 + f'$ in n Variablen gerade die Invarianten d, S, j_ν hat, w. z. b. w.

2. Reeller Funktionenkörper.

Durch die Gleichung $F(x, y) = 0$ mit reellen Koeffizienten sei der reelle algebraische Funktionenkörper K definiert. Diejenigen Punkte $\mathfrak{p}$ auf der Riemannschen Fläche des Oberkörpers $K(i)$, in welchen sämtliche Funktionen α des Körpers K reelle Werte $\alpha(\mathfrak{p})$ annehmen, bilden eine Reihe von geschlossenen Kurven, die sich nicht schneiden. Diese „reellen Kurven" spielen eine entscheidende Rolle für die Untersuchung der Algebren über K. Aus der Arbeit (8) entnehmen wir die folgenden Tatsachen:

(1) Eine Algebra (α, β) zerfällt genau dann, wenn für fast alle Kurvenpunkte $\mathfrak{p}$ die Algebra $(\alpha(\mathfrak{p}), \beta(\mathfrak{p}))$ (über dem reellen Konstantenkörper) zerfällt, d. h. wenn fast nirgends α und β zugleich negativ werden.

(2) Wird jede Kurve in eine endliche Anzahl von Intervallen eingeteilt, und werden zu diesen Intervallen willkürliche Vorzeichen gewählt, so gibt es Funktionen, die in fast allen Kurvenpunkten genau das verlangte Vorzeichen annehmen.

Hierauf fußend behaupten wir folgende Sätze.

Satz 22. *Wenn für fast alle Kurvenpunkte* $\mathfrak{p}$ *die reelle quadratische Form* $f(\mathfrak{p}) = \sum_1^n \alpha_i(\mathfrak{p})\, x_i^2$ *indefinit ist, so stellt die Form* $f = \sum_1^n \alpha_i x_i^2$ *im Körper* K *die Null dar* $(n \geqq 3)$.

Beweis. Für $n = 3$ folgt die Behauptung aus Satz 13 in Verbindung mit (1). Für $n > 3$ wenden wir Induktion an. Wir setzen $f = \varphi - \psi$, wobei φ wieder $n - 2$ und ψ zwei Variable enthält. Nach (2) können wir eine Funktion μ wählen, die in fast allen Punkten positive Werte annimmt, in welchen entweder φ oder ψ positiv definit wird; dagegen soll μ in fast allen übrigen Kurvenpunkten negativ werden. Weil f in fast allen Punkten indefinit ist, sind nach dieser Wahl von μ auch die beiden Formen $\varphi - \mu x^2$ und $\psi - \mu y^2$ in fast allen Punkten indefinit, sie stellen mithin nach Induktion beide im Körper K die Null dar. Wenn aber φ und ψ beide die Zahl μ darstellen, ist $f = \varphi - \psi = 0$ in K lösbar.

Den Trägheitsindex von $f(\mathfrak{p}) = \Sigma \alpha_i(\mathfrak{p}) x_i^2$ nennen wir den Trägheitsindex von $f = \Sigma \alpha_i x_i^2$ im reellen Kurvenpunkt $\mathfrak{p}$. Der Trägheitsindex werde jedoch nicht erklärt für die Nullstellen und Pole der α_i, er ist also nur in fast allen Punkten festgelegt.

Satz 23. *Wenn die Formen* f *und* g *in* n *Variablen dieselbe Diskriminante und in fast allen Kurvenpunkten gleichen Trägheitsindex haben, so sind* f *und* g *äquivalente Formen.*

Beweis. Die Form $h = f - g$ in $2n$ Variablen hat die Diskriminante $(-1)^n$ und den Trägheitsindex n. Durch Induktion zeigen wir die (mit $f \cong g$ gleichwertige) Behauptung $h \sim 0$:

Für $n = 1$ ist klar, daß $h = 0$ lösbar ist, und für $n > 1$ folgt die Nulldarstellbarkeit aus Satz 22. Nach Satz 5 ist $h \cong x^2 - y^2 + h'$, wo also h' eine Form in $2n - 2$ Variablen mit der Diskriminante $(-1)^{n-1}$ ist, die an fast allen Punkten den Trägheitsindex $n - 1$ hat. Folglich ist $h' \sim 0$ und damit auch $h \sim 0$.

Für die Diskriminante einer Form gilt an fast allen Kurvenpunkten $\operatorname{sign} d = (-1)^j$, wo j den Trägheitsindex in diesem Punkt bedeutet ($0 \leqq j \leqq n$).

Der folgende Satz lehrt, daß außer diesen angegebenen Relationen keine weiteren zwischen den Invarianten n, d, j bestehen.

Satz 24. *Man teile die reellen Kurven in endlich viele Intervalle* $[\nu]$ *ein und gebe* j_ν ($0 \leqq j_\nu \leqq n$) *und* d *aus* K *so vor, daß* $\operatorname{sign}_\nu d = (-1)^{j_\nu}$ *in fast allen Punkten gilt. Dann gibt es eine quadratische Form* f *in* n *Variablen mit der Diskriminante* d, *die in fast allen Punkten des Intervalls* $[\nu]$ *den Trägheitsindex* j_ν *besitzt.*

Beweis. Wir bestimmen nach (2) n Funktionen α so, daß im Intervall $[\nu]$

$$\alpha_1, \ldots, \alpha_{j_\nu} < 0 \quad \text{und} \quad \alpha_{j_\nu+1}, \ldots, \alpha_n > 0$$

ist. Dann hat

$$f = d\alpha_2 \cdots \alpha_n x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_n x_n^2$$

die vorgeschriebenen Invarianten.

Göttingen, den 25. 1. 1936.

Literaturverzeichnis.

(1) C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Sem. Hamburg **11** (1935), S. 73.

(2) W. K. Clifford, Applications of Graßmann's extensive algebra, Math. Papers, p. 271 = Am. Journ. of Math. **1** (1878), p. 350.

(3) H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Crelle **152** (1923), S. 129.

—, Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen, Crelle **152** (1923), S. 205.

—, Symmetrische Matrizen im Körper der rationalen Zahlen, Crelle **153** (1924), S. 12.

—, Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, Crelle **153** (1924), S. 113.

—, Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, Crelle **153** (1924), S. 158.

(4) K. Hensel, Zahlentheorie (1913), S. 308.

(5) H. Minkowski, Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten rational ineinander transformiert werden können, Ges. Abh. **1** (1914), S. 219.

(6) Ch. C. Tsen, Divisionsalgebren über Funktionenkörpern, Gött. Nachr. 1933, S. 335.

—, Algebren über Funktionenkörpern, Diss. Göttingen 1934.

(7) E. Warning, Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, Abh. Math. Sem. Hamburg **11** (1935), S. 76.

(8) E. Witt, Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper, Crelle **171** (1934), S. 4.

Eingegangen 2. Mai 1936.