Sonderabdruck aus „Mathematische Zeitschrift", Band 51, Heft 2
Springer-Verlag Berlin und Göttingen

Quadratische Formen über quadratischen Körpern.

Von

H. Maaß in Heidelberg.

Es sei K ein total reeller algebraischer Zahlkörper, I der Bereich der ganzen Zahlen in K. Eine quadratische Form über K

$$v = \sum_{i,k=1}^{n} \alpha_{ik}\xi_i\xi_k \qquad (\alpha_{ik} = \alpha_{ki} \subset I) \tag{1}$$

heißt gerade und positiv, wenn für beliebige, nicht sämtlich verschwindende $\xi_i \subset I$

$$v \equiv 0\,(2) \text{ und } v \gg 0. \tag{2}$$

Es wird hier nur von solchen positiven geraden Formen (1) die Rede sein, deren Determinante eine Einheit ε ist:

$$|\alpha_{ik}| = \varepsilon. \tag{3}$$

Quadratische Formen, welche durch eine unimodulare lineare Transformation der Variablen mit Koeffizienten aus I ineinander übergeführt werden können, werden äquivalent genannt. Eine nicht erweiterungsfähige Menge von untereinander äquivalenten Formen heißt eine Klasse.

Im rationalen Zahlkörper R sind folgende Sätze bekannt. Eine positive gerade Form von n Variablen mit der Determinante 1 existiert dann und nur dann, wenn $n \equiv 0\,(8)$. Minkowski[1]) hat als erster eine solche Form von 8 Variablen angegeben. Nach Mordell[2]) gibt es nur eine Klasse von geraden Formen zu $n = 8$, nach Witt[3]) genau zwei Klassen zu $n = 16$. Analoge Sätze sind auch für den quadratischen Körper $R(\sqrt{5})$ bewiesen worden[4]). Für diesen Körper lautet das Existenzkriterium: $n \equiv 0\,(4)$, $\varepsilon =$ Quadrat einer Einheit. Zu $n = 4$ gibt es genau eine Formenklasse, zu $n = 8$ genau zwei.

In der vorliegenden Arbeit wird für einen beliebigen quadratischen Körper $K = R(\sqrt{a})$ (a quadratfreie natürliche Zahl) die Frage beantwortet, wann es eine positive gerade Form über $R(\sqrt{a})$ von n

[1]) H. Minkowski, Gesammelte Abhandlungen I (1911).

[2]) L. J. Mordell, The definite quadratic forms in eight variables with determinant unity, Journal de Mathématiques pures et appliquées 17 (1938), S. 41—46.

[3]) E. Witt, Eine Identität zwischen Modulformen zweiten Grades, Abhandl. aus d. Math. Seminar d. Hansischen Universität 14 (1941), S. 323—337.

[4]) H. Maass, Modulformen und quadratische Formen über dem quadratischen Zahlkörper $R(\sqrt{5})$, Math. Annalen 118 (1941), S. 65—84.

Variablen mit der Determinante ε gibt. Es zeigt sich, daß eine solche Form dann und nur dann existiert, wenn

(4) $$\varepsilon \gg 0; \ n \equiv 0\,(2),\ (-1)^{\frac{n}{2}}\,\varepsilon \equiv \alpha^2\,(4),\ \alpha \subset I.$$

Darüber hinaus ist es in den Fällen $a \not\equiv 1\,(8)$ stets möglich, gerade Formen unter der Voraussetzung (4) nach einem Verfahren von Witt [3]) zu konstruieren, welchem folgender Gedanke zugrunde liegt. Im Rationalen entspricht jeder Klasse positiver Formen von n Variablen nach Minkowski [1]) ein n-dimensionales Raumgitter. Solche Raumgitter lassen sich übersichtlich durch lineare Kongruenzen definieren und stellen damit ein ausgezeichnetes Hilfsmittel dar, die arithmetischen Eigenschaften quadratischer Formen zu studieren. Bei dem Versuch, gerade Formen über $R(\sqrt{a})$ $(a \not\equiv 1\,(8))$ auf die angegebene Art zu konstruieren, bin ich in Anlehnung an die Wittsche Untersuchung auf folgendes System von Kongruenzen in $R(\sqrt{a})$ geführt worden:

(5) $$\begin{cases} (5')\ \ x_i \equiv 0\,(\mathfrak{p}^{-1}) & (i = 1, 2, \ldots, n), \\ (5'')\ \ x_k \equiv \alpha_1 x_n\,(1) & (k = 1, 2, \ldots, n-1), \\ (5''')\ \ \sum\limits_{k=1}^{n-1} x_k + \alpha_1 x_n \equiv 0\,(\mathfrak{p}). \end{cases}$$

Dabei ist $\mathfrak{p}$ das Primideal, welches 2 teilt, und

(6) $$\alpha_1 = \begin{cases} \sqrt{a}\,\alpha, \text{ wenn } a \equiv 5\,(8),\ n \equiv 4, 6\,(8), \\ \quad \alpha \text{ sonst.} \end{cases}$$

α ist aus (4) zu entnehmen. Zur Bestimmung von α ist im Falle $a \equiv 5\,(8)$ noch ein Zusatz nötig. Aus dem Bestehen der zweiten Kongruenz unter (4) kann unter der Voraussetzung $a \equiv 5\,(8)$ gefolgert werden, daß auch

(7) $$(-1)^{\frac{n}{2}}\,\varepsilon \equiv \alpha^{*2}\,(8),\ \ \alpha^* \subset I$$

lösbar ist. Es soll dann $\alpha = \alpha^*$ angenommen werden.

Im einzelnen wird nun folgendes bewiesen: Die Menge der Lösungsvektoren

$$\mathfrak{x} = \{x_1, x_2, \ldots, x_n\}$$

des Systems (5) stellt einen I-Modul M mit n-gliedriger Basis, etwa $\mathfrak{x}_i\,(i = 1, 2, \ldots, n)$, dar:

(8) $$M = I\mathfrak{x}_1 + I\mathfrak{x}_2 + \cdots + I\mathfrak{x}_n.$$

Das ist eine nicht-triviale Aussage, wenn die Idealklassenzahl von $R(\sqrt{a})$ größer als 1 ist. Wir üben auf jeden Vektor $\mathfrak{x} \subset M$ die Abbildung

(9) $$\mathfrak{x} = \{x_1, x_2, \ldots, x_n\} \to \mathfrak{y} = \{x_1, \ldots, x_{n-1}, x_n\sqrt{\varepsilon}\}$$

aus. Dabei gehe $\mathfrak{x}_i$ in $\mathfrak{y}_i$ und M in

(10) $$N = I\mathfrak{y}_1 + I\mathfrak{y}_2 + \cdots + I\mathfrak{y}_n$$

über. Es ist nun leicht zu sehen, daß $\mathfrak{y}^2 \equiv 0\,(2)$ für $\mathfrak{y} \subset N$ und folglich

$$\mathfrak{y}\mathfrak{y}^* = \tfrac{1}{2}\{(\mathfrak{y}+\mathfrak{y}^*)^2 - \mathfrak{y}^2 - \mathfrak{y}^{*2}\} \equiv 0\,(1) \text{ für } \mathfrak{y}, \mathfrak{y}^* \subset N.$$

Die quadratische Form

$$(11) \qquad \left(\sum_{i=1}^{n} \mathfrak{y}_i \xi_i\right)^2 = \sum_{i,k=1}^{n} a_{ik} \xi_i \xi_k,$$

die wir kurz mit $\mathfrak{Q}$ bezeichnen, ist daher gerade und positiv und hat bei geeigneter Normierung der Basisvektoren $\mathfrak{y}_i$ die Determinante

$$(12) \qquad |\mathfrak{y}_i \mathfrak{y}_k| = |a_{ik}| = \varepsilon.$$

ε_0 sei eine Grundeinheit von $R(\sqrt{a})$. Da in der Klasse von $\mathfrak{Q}$ immer ein Repräsentant mit der Determinante 1 oder ε_0 aufgefunden werden kann, so bedeutet es keine Einschränkung, wenn im folgenden $\varepsilon = 1$ oder ε_0 angenommen wird.

Die Vektoren $\mathfrak{a} \subset N$, für welche $\mathfrak{a}^2 = 2$ oder $2\varepsilon_0$, fassen wir zu einem Vektordiagramm L zusammen. Die Kenntnis von L ist an sich von Interesse, darüber hinaus aber auch zur Bestimmung der Automorphismengruppe von $\mathfrak{Q}$ bzw. N [3]) und zur Beantwortung der Frage von Nutzen, wann die Formen $\mathfrak{Q}$ und $\varepsilon_0\mathfrak{Q}$ äquivalent sind. Die Automorphismengruppe $\mathfrak{G}$ von N besteht aus den orthogonalen Transformationen von N in sich; unter diesen kommen insbesondere die Spiegelungen an den Normalebenen zu den Vektoren $\mathfrak{a} \subset L$ vor, wie aus der Darstellung einer solchen Spiegelung

$$(13) \qquad \mathfrak{y} \to \mathfrak{y} - \varepsilon_0^{-m}(\mathfrak{a}\mathfrak{y})\,\mathfrak{a}, \quad \mathfrak{a}^2 = 2\varepsilon_0^m, \quad \mathfrak{a} \subset L$$

unmittelbar hervorgeht. $\mathfrak{G}$ enthält also die zu L gehörige Spiegelungsgruppe $\mathfrak{S}$, die aus sämtlichen Spiegelungen (13) erzeugt wird. Die nicht in $\mathfrak{S}$ gelegenen Automorphismen von N können nun auf Grund der von Witt angegebenen Resultate über Spiegelungsgruppen [5]) von Fall zu Fall leicht berechnet werden. Zur Äquivalenz der Formen $\mathfrak{Q}$ und $\varepsilon_0\mathfrak{Q}$ ist offenbar notwendig, daß L gleich viele Vektoren der Längen $\sqrt{2}$ und $\sqrt{2\varepsilon_0}$ enthält. Das ist der Fall, wenn

$$(14) \qquad \begin{array}{lll} n = 2, & \varepsilon = \varepsilon_0 & \text{oder} \\ n = 2, & \varepsilon = 1, \quad \zeta^2 = 2\varepsilon_0 & \text{oder} \\ n = 4, & \varepsilon = 1, \quad \zeta^2 = 2\varepsilon_0 & (\zeta \subset I). \end{array}$$

Diese Bedingungen sind aber auch hinreichend für die Äquivalenz der Formen. Es verdient noch hervorgehoben zu werden, daß $2\varepsilon_0$ durch $\mathfrak{Q}$ dann und nur dann dargestellt wird, wenn entweder $\zeta^2 = 2\varepsilon_0$ oder $a \equiv 5\,(8)$, $n = 2$, $\varepsilon = \varepsilon_0$, $\zeta^2 = 7\varepsilon_0$.

Der Ausschluß der Körper $R(\sqrt{a})$ mit $a \equiv 1\,(8)$ scheint eine notwendige Maßnahme zu sein. Es kann nämlich passieren, daß über diesen Körpern keine positiven geraden Formen von n Variablen mit

[5]) E. Witt, Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe, Abhandl. aus d. Math. Seminar d. Hansischen Universität 14 (1941), S. 289—322.

der Determinante ε durch Kongruenzen nach beliebigen Idealmoduln zu definieren sind, obgleich die für die Existenz hinreichenden Bedingungen (4) erfüllt sind. Dieser Fall liegt z. B. vor im Körper $R(\sqrt{33})$ für $n = 2$, $\varepsilon = \varepsilon_0 = 23 + 4\sqrt{33}$, wie auf Grund bekannter arithmetischer Sätze leicht festgestellt wird.

Wenn $n \equiv 0\,(8)$, so wird durch das System

$$(15) \qquad x_i \equiv 0\,(\tfrac{1}{2}),\ x_i \equiv x_n\,(1)\ \ (i = 1, 2, \ldots, n),\ \sum_{i=1}^{n} x_i \equiv 0\,(2)$$

eine Klasse von positiven geraden Formen definiert, welche nach Witt[3]) einen rationalen Repräsentanten $\mathfrak{Q}^*$ mit der Determinante 1 enthält. Für $a \equiv 2, 3\,(4)$ ist diese Formenklasse verschieden von der Formenklasse zu $\mathfrak{Q}$ (mit $\varepsilon = 1$, $\alpha_1 = 1$), da die zugehörigen Automorphismengruppen verschiedene Ordnungen haben. Die Formen $\mathfrak{Q}$ und $\varepsilon_0 \mathfrak{Q}$ haben offenbar dieselben Automorphismengruppen, was auch für $\mathfrak{Q}^*$ und $\varepsilon_0 \mathfrak{Q}^*$ gilt. $\mathfrak{Q}^*$ und $\varepsilon_0 \mathfrak{Q}^*$ gehören verschiedenen Klassen an, da 2, aber nicht $2\,\varepsilon_0$ durch $\mathfrak{Q}^*$ dargestellt wird. Infolgedessen repräsentieren die Formen

$$\mathfrak{Q},\ \varepsilon_0 \mathfrak{Q},\ \mathfrak{Q}^*,\ \varepsilon_0 \mathfrak{Q}^* \qquad (n \equiv 0\,(8),\ \varepsilon = \alpha = 1)$$

vier verschiedene Klassen über $R(\sqrt{a})$, wenn $a \equiv 2, 3\,(4)$.

§ 1.

Das Existenzkriterium. Konstruktion von Formen.

Sei (α_{ik}) das Koeffizientenschema einer gegebenen positiven geraden Form über $R(\sqrt{a})$ mit der Determinante ε. Dann läßt sich eine ganzzahlige Matrix U mit der Determinante 1 und Koeffizienten aus I derart bestimmen, daß $U'(\alpha_{ik})\,U$ einer Kästchenmatrix

$$(16) \qquad \begin{pmatrix} \beta_1 & \gamma_1 & & & \\ \gamma_1 & \delta_1 & & & \\ & & \beta_2 & \gamma_2 & \\ & & \gamma_2 & \delta_2 & \\ & & & & \ddots \end{pmatrix}$$

mod 4 kongruent ist. Außerhalb der quadratischen zweireihigen Kästchen stehen Nullen, und die Diagonalelemente β_i, δ_i sind sämtlich durch 2 teilbar. Die Transformation der Matrix (α_{ik}) mod 4 auf eine Matrix vom Typus (16) kann so vorgenommen werden, daß man zunächst die ersten beiden Zeilen und Spalten von (α_{ik}) reduziert, darauf die nächsten beiden usf. Aus dem Verfahren geht hervor, daß die Variablenzahl n notwendig gerade ist. Determinantenbildung ergibt dann

$$\varepsilon = |\alpha_{ik}| \equiv \prod_{j=1}^{\frac{n}{2}} (-\gamma_j^2) \equiv (-1)^{\frac{n}{2}} \alpha^2\,(4).$$

Damit ist gezeigt, daß die Bedingungen (4) für die Existenz der Formen notwendig sind. Wir nehmen jetzt umgekehrt an, daß die Bedingungen (4) erfüllt sind und beweisen daraus die Existenz einer zugehörigen positiven geraden Form. Offenbar können wir uns auf $n = 2$ und 4 beschränken, da man sich durch Komposition dieser speziellen Formen solche von beliebiger zulässiger Variablenzahl n verschaffen kann.

1. $n = 2$. Da $-\varepsilon \equiv \alpha^2 (4)$, so kann β ganzzahlig aus $4\beta = \alpha^2 + \varepsilon$ bestimmt werden. Die Form mit den Koeffizienten

$$(17) \qquad \begin{pmatrix} 2 & \alpha \\ \alpha & 2\beta \end{pmatrix}$$

hat die gewünschte Eigenschaft.

2. $n = 4$. Für das Koeffizientenschema der gesuchten Form machen wir den Ansatz

$$(18) \qquad A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2\beta & \gamma & 0 \\ 0 & \gamma & 2\delta & \alpha \\ 0 & 0 & \alpha & 2 \end{pmatrix}.$$

Darin soll β so bestimmt werden, daß

$$(19) \qquad 4\beta - 1 = q$$

eine Primzahl wird. Da $|A| = q(4\delta - \alpha^2) - 4\gamma^2$, so ist also

$$(20) \qquad 4q\delta = 4\gamma^2 + q\alpha^2 + \varepsilon$$

zu fordern. Wenn (19) und (20) befriedigt sind, ist die zu A gehörige Form überdies positiv, da

$$\begin{vmatrix} 2 & 1 \\ 1 & 2\beta \end{vmatrix} = q, \qquad \begin{vmatrix} 2 & 1 & 0 \\ 1 & 2\beta & \gamma \\ 0 & \gamma & 2\delta \end{vmatrix} = \frac{\varepsilon + q\alpha^2}{2}$$

total positive Zahlen sind. Die Bedingungen (19) und (20) sind zur Definition von β und δ geeignet, wenn

$$(21) \qquad q \equiv -1\,(4), \quad 4\gamma^2 + \varepsilon \equiv 0\,(q), \quad \varepsilon \equiv \alpha^2\,(4).$$

Die letzte der drei Kongruenzen kann nach Voraussetzung als erfüllt angesehen werden. Die Primzahl q sei nun so bestimmt, daß

$$(22) \qquad \left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right) = -1 \quad \text{und} \quad \varepsilon \not\equiv 1\,(q).$$

Die erste Kongruenz von (21) ist dann befriedigt; außerdem bleibt das Ideal (q) in $R(\sqrt{a})$ unzerlegt, ist also ein Primideal $\mathfrak{q}$. Es braucht dann nur noch gezeigt zu werden, daß $-\varepsilon$ quadratischer Rest mod $\mathfrak{q}$ ist oder damit gleichwertig, daß $\mathfrak{q}$ im Körper $R(\sqrt{a}, \sqrt{-\varepsilon})$ vollständig zerfällt. $R(\sqrt{a}, \sqrt{-\varepsilon})$ enthält die imaginär quadratischen Körper $R(\sqrt{b})$ und $R(\sqrt{ab})$, wobei $\sqrt{b} = \sqrt{-\varepsilon} + \frac{1}{\sqrt{-\varepsilon}}$. In einem dieser Körper zerfällt das Ideal (q), da die Restsymbole $\left(\frac{b}{q}\right)$ und $\left(\frac{ab}{q}\right)$ verschiedene Werte haben (q/b ist durch $\varepsilon \not\equiv 1\,(q)$ ausgeschlossen). $\mathfrak{q} = (q)$ muß also auch in $R(\sqrt{a}, \sqrt{-\varepsilon})$ zerfallen, q. e. d. Wir formulieren das Ergebnis in

Satz 1. *Notwendig und hinreichend für die Existenz einer positiven geraden Form über $R(\sqrt{a})$ von n Variablen mit der Determinante ε sind die Forderungen* (4).

Wir stellen nun eine Reihe von Sätzen zusammen, die ihrer Natur nach elementar aber im Zusammenhang mit den hier behandelten Fragen von Interesse sind. Um eine kurze Ausdrucksweise anzustreben, verwenden wir folgende Termini. Eine zu 2 prime Zahl aus I heißt primär bzw. hyperprimär, wenn sie quadratischer Rest mod 4 bzw. mod 8 ist. Mit $\mathbf{N}\alpha\,(\alpha \subset R(\sqrt{a}))$ bezeichnen wir die Norm von α.

Satz 2: *Die Zahl -1 ist in $R(\sqrt{a})$ dann und nur dann primär, wenn $a \equiv 3\,(4)$.*

Satz 3. *In $R(\sqrt{a})$ mit $a \equiv 3\,(4)$ sei ε_0 (und damit auch $-\varepsilon_0$) primär; dann ist das Primideal $\mathfrak{p}$, welches 2 teilt, kein Hauptideal.*

Satz 4. *In $R(\sqrt{a})$ mit $a \equiv 1\,(4)$ ist eine der beiden Grundeinheiten ε_0 und $-\varepsilon_0$ dann und nur dann primär, wenn $\mathbf{N}\varepsilon_0 = 1$.*

Satz 5. *Wenn in $R(\sqrt{a})$ mit $a \equiv 5\,(8)$ eine der Einheiten ε_0* und $-\varepsilon_0$ *primär ist, dann ist dieselbe auch hyperprimär.*

Der Beweis von Satz 2 darf übergangen werden. Satz 3 ergibt sich aus folgender Bemerkung: Wenn $(2) = \mathfrak{p}^2$, $\mathfrak{p} = (\zeta)$, so ist etwa $\zeta^2 = 2\varepsilon_0$ und dann $\zeta^2 \equiv 2\sqrt{a}\,(4)$, also $\varepsilon_0 \equiv \sqrt{a}\,(2)$. $\sqrt{a}$ ist aber kein quadratischer Rest mod 2. Zum Beweis der letzten beiden Sätze wählt man zweckmäßig in I folgende Minimalbasis:

$$\omega_1 = \frac{1+\sqrt{a}}{2}, \quad \omega_2 = \frac{1-\sqrt{a}}{2}.$$

Sei nun $\varepsilon_0 = u\,\omega_1 + v\,\omega_2$, $\alpha = x\,\omega_1 + y\,\omega_2$. Die Kongruenz $\pm\,\varepsilon_0 \equiv \alpha^2\,(2^m)$ bedeutet dann

$$\begin{aligned} \pm\, u &\equiv x^2 + l(x-y)^2, \\ \pm\, v &\equiv y^2 + l(x-y)^2 \end{aligned} \quad (2^m) \qquad \left(l = \frac{a-1}{4}\right).$$

Man überzeugt sich leicht von der Auflösbarkeit dieses Systems in den Fällen $a \equiv 1\,(8)$, $m = 2$ und $a \equiv 5\,(8)$, $m = 3$ unter der Voraussetzung $\mathbf{N}\varepsilon_0 = uv - l(u-v)^2 = 1$.

Wir befassen uns nun mit dem Kongruenzensystem (5).

Satz 6. *Der für $a \not\equiv 1\,(8)$ durch das System* (5) *oben erklärte I-Modul M hat folgende Eigenschaften:*

1. *Für $\mathfrak{y} \subset N$ ist $\mathfrak{y}^2 \equiv 0\,(2)$.*

2. *Es gibt in N eine I-Basis $\mathfrak{y}_1, \mathfrak{y}_2, \ldots, \mathfrak{y}_n$ derart, daß die mit den Vektoren $\mathfrak{y}_i$ gebildete Determinante den Wert $\sqrt{\varepsilon}$ hat.*

N definiert also eine Klasse von positiven geraden Formen, welche durch die Form

$$\sum_{i,k=1}^{n} \mathfrak{y}_i \mathfrak{y}_k \xi_i \xi_k \tag{23}$$

mit der Determinante ε repräsentiert wird.

Beweis. 1. Aus (5″) und (5‴) folgt

$$x_i = \alpha_1 x_n + \gamma_i \quad (i = 1, 2, \ldots, n-1), \quad \gamma_i \subset I,$$
$$\sum_{i=1}^{n-1} \gamma_i \equiv -n \alpha_1 x_n (\mathfrak{p}),$$

also

$$\begin{aligned} \mathfrak{y}^2 = \sum_{i=1}^{n-1} x_i^2 + \varepsilon x_n^2 &\equiv [(n-1)\alpha_1^2 + \varepsilon] x_n^2 + 2\alpha_1 x_n \sum_{i=1}^{n-1} \gamma_i + \left(\sum_{i=1}^{n-1} \gamma_i\right)^2 \\ &\equiv [(n-1)\alpha_1^2 + \varepsilon] x_n^2 - 2n\alpha_1^2 x_n^2 + n^2 \alpha_1^2 x_n^2 \equiv [(n-1)\alpha_1^2 + \varepsilon] x_n^2. \end{aligned} \quad (2)$$

Auf Grund der Voraussetzung (4) und unserer Festsetzung (6) α_1 betreffend ergibt sich nun $\mathfrak{y}^2 \equiv 0\,(2)$.

2. In $R(\sqrt{a})$ sollen Zahlen $\beta, \gamma_1, \gamma_2$ so bestimmt werden, daß die n Vektoren

$$\begin{aligned} \mathfrak{x}_1 &= \{1, -1, 0, \ldots, 0, \quad 0, \quad 0\}, \\ \mathfrak{x}_2 &= \{0, -1, 1, \ldots, 0, \quad 0, \quad 0\}, \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathfrak{x}_{n-2} &= \{0, 0, \quad 0, \ldots, -1, 1, \quad 0\}, \\ \mathfrak{x}_{n-1} &= \{0, 0, \quad 0, \ldots, 0, \quad 1, -\beta\}, \\ \mathfrak{x}_n &= \{\gamma_1, -\gamma_1, \gamma_1, \ldots, -\gamma_1, \gamma_1, \gamma_2\} \end{aligned} \tag{24}$$

Lösungsvektoren des Systems (5) darstellen, und die aus ihnen gebildete Determinante den Wert $(-1)^{\frac{n}{2}}$ hat. Es sind also folgende Bedingungen zu befriedigen:

$$\begin{gathered} \beta \equiv 0\,(1), \quad \gamma_1 \equiv 0\,(\mathfrak{p}^{-1}), \quad \gamma_2 \equiv 0\,(\mathfrak{p}^{-1}) \\ 1 - \alpha_1 \beta \equiv 0\,(\mathfrak{p}), \quad \gamma_1 + \alpha_1 \gamma_2 \equiv 0\,(\mathfrak{p}), \\ \gamma_1 \beta + \gamma_2 = -1. \end{gathered} \tag{25}$$

Die letzte Gleichung benutzen wir zur Definition von γ_2. Für β und γ_1 verbleiben die Forderungen:

$$\begin{gathered} \beta \equiv 0\,(1), \quad \gamma_1 \equiv 0\,(\mathfrak{p}^{-1}), \\ 1 - \alpha_1 \beta \equiv 0\,(\mathfrak{p}), \quad \gamma_1 (1 - \alpha_1 \beta) \equiv \alpha_1\,(\mathfrak{p}), \end{gathered} \tag{26}$$

die ersichtlich erfüllt werden können. Es ist nun leicht zu sehen, daß die Vektoren (24) eine Basis für den Lösungsmodul M bilden. Setzen wir für $\mathfrak{x} \subset M$:

$$\mathfrak{x} = \sum_{i=1}^{n} \xi_i \mathfrak{x}_i,$$

so ist zu beweisen, daß die Koeffizienten ξ_i in I liegen. Für die Komponenten x_i von $\mathfrak{x}$ folgt zunächst

$$\sum_{i=1}^{n-1} x_i \beta + x_n = -\xi_n,$$

also nach (5‴) und (25)

$$\xi_n \equiv (\alpha_1 \beta - 1) x_n \equiv 0\,(1).$$

Der Vektor $\mathfrak{x}^* = \mathfrak{x} - \xi_n \mathfrak{x}_n = \{x_1^*, x_2^*, \ldots, x_n^*\}$ liegt demnach in M und für seine Komponenten besteht die Beziehung

$$\sum_{i=1}^{n-1} x_i^* \beta + x_n^* = 0.$$

Nach (25) und (5) ist nun zu schließen, daß

$$x_n^* = \left(\sum_{i=1}^{n-1} x_i \gamma_2 - x_n \gamma_1\right) \beta \equiv \left(\sum_{i=1}^{n-1} x_i + \alpha_1 x_n\right) \gamma_2 \beta \equiv 0\,(1).$$

Zufolge (5″) ist dann auch $x_i^* \equiv 0\,(1)$, und $\mathfrak{x}^*$ kann somit als ganzzahlige Linearkombination der Vektoren $\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_{n-1}$ bestimmt werden. Damit ist die Basiseigenschaft der $\mathfrak{x}_i$ für M bewiesen. Die zu den Vektoren $\mathfrak{x}_i$ nach (9) berechneten Bildvektoren $\mathfrak{y}_i$ haben die in Satz 6 formulierten Eigenschaften, q. e. d.

Es ist übrigens leicht zu beweisen, daß die im Körper zu (23) konjugierte quadratische Form in derselben Formenklasse liegt.

In den nun folgenden Paragraphen beschränken wir uns auf $\varepsilon = 1$ und ε_0. $\mathbf{N}$ und $\mathbf{S}$ werden als Norm- und Spurzeichen in $R(\sqrt{a})$ verwendet. Die zu einer Körperzahl ξ konjugierte bezeichnen wir mit ξ'.

§ 2.

Berechnung des Vektordiagramms L für $a \equiv 5\,(8)$.

Wir wählen in $R(\sqrt{a})$ für $a \equiv 5\,(8)$ die feste Minimalbasis

(27) $$\omega_1 = \frac{1+\sqrt{a}}{2}, \quad \omega_2 = \frac{1-\sqrt{a}}{2} \qquad \left(l = \frac{a-1}{4} \equiv 1\,(2)\right)$$

und bezeichnen mit $\mathfrak{e}_1, \mathfrak{e}_2, \ldots, \mathfrak{e}_n$ die Einheitsvektoren des n-dimensionalen Raumes. Ein Lösungsvektor

(28) $$\mathfrak{x} = \{x_1, x_2, \ldots, x_n\} = \sum_{i=1}^{n} x_i \mathfrak{e}_i$$

des Systems (5) gestattet dann die Darstellung

(29) $$\mathfrak{x} = \mathfrak{u}\,\omega_1 + \mathfrak{v}\,\omega_2$$

mit rationalen Vektoren

(30) $$\begin{aligned} \mathfrak{u} &= \{u_1, u_2, \ldots, u_n\} = \mathfrak{u}^* + u_n \mathfrak{e}_n, \\ \mathfrak{v} &= \{v_1, v_2, \ldots, v_n\} = \mathfrak{v}^* + v_n \mathfrak{e}_n. \end{aligned}$$

Aus (29) folgt

$$(31)\qquad \mathfrak{x}^2 = [\mathfrak{u}^2 + l(\mathfrak{u}-\mathfrak{v})^2]\,\omega_1 + [\mathfrak{v}^2 + l(\mathfrak{u}-\mathfrak{v})^2]\,\omega_2,$$

$$(32)\qquad \mathbf{N}\,\mathfrak{x}^2 = [\mathfrak{u}\mathfrak{v} - l(\mathfrak{u}-\mathfrak{v})^2]^2 + a[\mathfrak{u}^2\mathfrak{v}^2 - (\mathfrak{u}\mathfrak{v})^2],$$

und für $\mathfrak{y} = \{x_1, \ldots, x_{n-1}, x_n\sqrt{\varepsilon}\}$ gilt ähnlich

$$(33)\qquad \mathfrak{y} = \mathfrak{u}^*\omega_1 + \mathfrak{v}^*\omega_2 + x_n\sqrt{\varepsilon}\,\mathfrak{e}_n,$$

$$(34)\qquad \mathfrak{y}^2 = [\mathfrak{u}^{*2} + l(\mathfrak{u}^*-\mathfrak{v}^*)^2]\,\omega_1 + [\mathfrak{v}^{*2} + l(\mathfrak{u}^*-\mathfrak{v}^*)^2]\,\omega_2 + x_n^2\varepsilon,$$

$$(35)\qquad \begin{aligned}\mathbf{N}\,\mathfrak{y}^2 = {} & [\mathfrak{u}^*\mathfrak{v}^* - l(\mathfrak{u}^*-\mathfrak{v}^*)^2]^2 + a[\mathfrak{u}^{*2}\mathfrak{v}^{*2} - (\mathfrak{u}^*\mathfrak{v}^*)^2] \\ & + [u_n v_n - l(u_n - v_n)^2]^2 + \mathbf{S}\Big(\sum_{i=1}^{n-1} x_i^2 x_n'^2\,\varepsilon'\Big),\end{aligned}$$

$$(36)\qquad \mathbf{S}\,\mathfrak{y}^2 = \mathfrak{u}^{*2} + \mathfrak{v}^{*2} + 2l(\mathfrak{u}^*-\mathfrak{v}^*)^2 + \mathbf{S}\,x_n^2\varepsilon.$$

Wir behandeln nun nacheinander die Fälle $\varepsilon = 1$ und ε_0.

1. $\varepsilon = 1$. Es ist dann $\mathfrak{y} = \mathfrak{x}$, $n \equiv 0\,(4)$, $\alpha = 1$, $\alpha_1 \equiv \alpha\,(2)$, und damit geht (5″) über in $x_i \equiv x_n\,(1)$ für $i = 1, 2, \ldots, n$. Die Komponenten von $\mathfrak{u}$ und ebenso die von $\mathfrak{v}$ sind also durchweg ganz- oder halbzahlig, so daß wegen $n \equiv 0\,(4)$ die Kongruenzen

$$(37)\qquad \mathfrak{u}^2 \equiv \mathfrak{v}^2 \equiv 0\,(1),\quad \mathfrak{u}\mathfrak{v} \equiv 0\,(\tfrac{1}{2})$$

bestehen.

11. Wir beweisen zunächst, daß $2\,\varepsilon_0$ durch $\mathfrak{Q}$ nicht dargestellt wird. Das ist richtig für $a \equiv 5, 13$, da in diesen beiden Körpern $\mathbf{N}\,\varepsilon_0 = -1$, so daß wir $a \geqq 21$ voraussetzen können. Wir nehmen $\mathbf{N}\,\mathfrak{x}^2 = 4$ an. Aus (32) folgt dann nach einer im folgenden häufig anzuwendenden Schlußweise die lineare Abhängigkeit der Vektoren $\mathfrak{u}$ und $\mathfrak{v}$. Das ist ein Ergebnis der Cauchy-Schwarzschen Ungleichung, die in der zweiten eckigen Klammer auf der rechten Seite von (32) wirksam wird; dabei ist zu beachten, daß dieser Klammerausdruck zufolge (37) höchstens den Nenner 4 hat. Wir entnehmen aus (32) weiter, daß $\mathfrak{u} \neq 0$ und $\mathfrak{v} \neq 0$ und schließen nun:

$$\mathfrak{v} = \frac{r}{s}\,\mathfrak{u},\quad (r, s) = 1,\quad s > 0$$

sowie nach (32):

$$\frac{\mathfrak{u}^2}{s^2}\,[s\,r - l(s-r)] = \pm 2.$$

Der Klammerausdruck ist nicht durch 2 teilbar; $\frac{\mathfrak{u}^2}{s^2}$ ist nach (37) ganzzahlig, also ist $\frac{\mathfrak{u}^2}{s^2} \equiv 0\,(2)$, und aus $\mathfrak{x}^2 = \frac{\mathfrak{u}^2}{s^2}\,(s\,\omega_1 + r\,\omega_2)^2$ folgt $\mathfrak{x}^2 = 2\,\varepsilon_0^{2m}$, q. e. d.

Wir bestimmen nun die Lösungen von

12. $\mathfrak{x}^2 = 2$. Die Gleichung (31) zerfällt in das rationale System

$$\mathfrak{u}^2 + l(\mathfrak{u}-\mathfrak{v})^2 = 2,$$
$$\mathfrak{v}^2 + l(\mathfrak{u}-\mathfrak{v})^2 = 2.$$

Wenn $\mathfrak{u} \neq \mathfrak{v}$, dann ist notwendig $\mathfrak{u}^2 = \mathfrak{v}^2 = 1$, $l = 1$, $(\mathfrak{u}-\mathfrak{v})^2 = 1$, also $a = 5$, $\mathfrak{u}\mathfrak{v} = \frac{1}{2}$. Da entweder $\mathfrak{u}$ oder $\mathfrak{v}$ halbzahlig ist, so ist $\mathfrak{u}^2 = \mathfrak{v}^2 = 1$ nur mit $n = 4$ verträglich und es kommen folgende Vektoren als Lösungen in Frage ($\sigma_i = \pm 1$):

$$\begin{cases} \mathfrak{u} = \sigma_i \mathfrak{e}_i \\ \mathfrak{v} = \frac{1}{2}\sum\limits_{k=1}^{4} \sigma_k \mathfrak{e}_k \end{cases} \qquad \begin{cases} \mathfrak{u} = \frac{1}{2}\sum\limits_{k=1}^{4} \sigma_k \mathfrak{e}_k \\ \mathfrak{v} = \sigma_i \mathfrak{e}_i \end{cases} \qquad \begin{cases} \mathfrak{u} = \frac{1}{2}\sum\limits_{k=1}^{4} \sigma_k \mathfrak{e}_k \\ \mathfrak{v} = \frac{1}{2}\sum\limits_{k=1}^{4} \sigma_k \mathfrak{e}_k - \sigma_i \mathfrak{e}_i. \end{cases}$$

Die Bedingungen, die sich aus dem System (5) ergeben, sind am besten zu übersehen, wenn man das System (5) auf $\mathfrak{u}$ und $\mathfrak{v}$ umschreibt ($\alpha_1 = \sqrt{a}$):

$$(38) \qquad \left.\begin{aligned} u_i &\equiv 0\,(\tfrac{1}{2}), \quad u_i \equiv \tfrac{1}{2}\sum_{k=1}^{n} v_k \quad (1), \\ v_i &\equiv 0\,(\tfrac{1}{2}), \quad v_i \equiv \tfrac{1}{2}\sum_{k=1}^{n} (u_k + v_k)\,(1) \end{aligned}\right\} \text{ für } \quad n \equiv 4\,(8).$$

Es ergeben sich dann folgende Lösungsvektoren

$$(39) \qquad \left.\begin{aligned} &\sigma_i \frac{3+\sqrt{5}}{4}\mathfrak{e}_i + \frac{1-\sqrt{5}}{4}\sum_{k \neq i} \sigma_k \mathfrak{e}_k, \quad \prod_{k=1}^{4} \sigma_k = 1, \\ &\sigma_i \frac{3-\sqrt{5}}{4}\mathfrak{e}_i + \frac{1+\sqrt{5}}{4}\sum_{k \neq i} \sigma_k \mathfrak{e}_k, \quad \prod_{k=1}^{4} \sigma_k = -1, \\ &\sigma_i \frac{\sqrt{5}}{2}\mathfrak{e}_i + \frac{1}{2}\sum_{k \neq i} \sigma_k \mathfrak{e}_k, \quad \prod_{k=1}^{4} \sigma_k = 1 \end{aligned}\right\} \text{ für } a = 5,\ n = 4.$$

Es bleibt noch $\mathfrak{u} = \mathfrak{v}$ zu diskutieren. In diesem Fall ist $\mathfrak{u}^2 = \mathfrak{v}^2 = 2$. Halbzahlige Lösungen liegen nur für $n = 8$ vor; es ist dann $\alpha_1 = 1$, und die Lösungsvektoren lauten

$$(40) \qquad \tfrac{1}{2}\sum_{k=1}^{8} \sigma_k \mathfrak{e}_k, \quad \prod_{k=1}^{8} \sigma_k = 1 \quad \text{für} \quad n = 8.$$

Die ganzzahligen Lösungen haben die Gestalt

$$(41) \qquad \pm \mathfrak{e}_i \pm \mathfrak{e}_k, \quad i < k.$$

2. $\varepsilon = \varepsilon_0$. Es handelt sich um die Körper $R(\sqrt{a})$ mit $\mathbf{N}\varepsilon_0 = 1$, also ist $a = 21$ oder $a \geqq 69$ und entsprechend $l = 5$ oder $l \geqq 17$. Nach (5″) sind die Komponenten von $\mathfrak{u}^*$ und ebenso die von $\mathfrak{v}^*$ durchweg ganz- oder halbzahlig.

21. $\mathfrak{y}^2 = 2$. Der Fall $\mathfrak{u}^* \neq \mathfrak{v}^*$ liegt zufolge (36) nur vor, wenn $l = 5$, $(\mathfrak{u}^* - \mathfrak{v}^*)^2 = \frac{1}{4}$, also $n = 2$. Für $a = 21$ ist $\varepsilon_0 = 3\,\omega_1 + 2\,\omega_2$ und $-\varepsilon_0 \equiv \omega_2^2(8)$. Aus der Spurrelation (36) ergibt sich dann $u_1 = 0$, $v_1 = \frac{\sigma_1}{2}$ oder $u_1 = \frac{\sigma_1}{2}$, $v_1 = 0$. Dazu berechnet man nach (34) die

Komponente $x_2 = \frac{\sigma_2}{2}$ bzw. $x_2 = \frac{\sigma_2}{2}\varepsilon_0'$. In beiden Fällen wird (5) befriedigt, wenn $\sigma_1\sigma_2 = -1$. Wir erhalten vier Lösungsvektoren:

$$(42)\qquad \left.\begin{aligned} &\pm\frac{1}{2}\left(\frac{1-\sqrt{21}}{2}\,\mathfrak{e}_1 - \sqrt{\frac{5+\sqrt{21}}{2}}\,\mathfrak{e}_2\right) \\ &\pm\frac{1}{2}\left(\frac{1+\sqrt{21}}{2}\,\mathfrak{e}_1 - \sqrt{\frac{5-\sqrt{21}}{2}}\,\mathfrak{e}_2\right)\end{aligned}\right\}\quad \text{für}\quad a = 21,\ n = 2.$$

Wenn $\mathfrak{u}^* = \mathfrak{v}^*$, so ist nach (34) $2 = \mathfrak{u}^{*2} + x_n^2\varepsilon_0$. Für halbzahliges $\mathfrak{u}^*$ ist zu schließen, daß $x_i = u_i = \frac{\sigma_i}{2}$ für $i < n$ und daher $\frac{9-n}{4} = \frac{p}{4} = x_n^2\varepsilon_0$. Es kommen also nur die Variablenzahlen $n = 2, 4, 6$ in Frage; für diese n ist $p = 9 - n$ eine Primzahl, welche a teilen muß. Sei $\zeta^2 = p\,\varepsilon_0$, dann können wir uns $\alpha_1 = \zeta$ gewählt denken. Mit $x_n = \frac{\sigma_n}{2}|\zeta'|$ erhält man zufolge (5''') die Bedingung $\sum\limits_{i=1}^{n-1}\sigma_i \equiv (n-1)\,\sigma_n \operatorname{sgn}\zeta\,(4)$, aus der sich folgende Lösungsvektoren ergeben:

$$(43)\quad \tfrac{1}{2}\left(\sum_{i=1}^{n-1}\sigma_i\mathfrak{e}_i + \sigma_n\sqrt{p}\,\mathfrak{e}_n\right),\quad \prod_{i=1}^{n}\sigma_i = \operatorname{sgn}\zeta \begin{cases}\text{für}\quad n = 2, 4, 6,\\ p = 9-n,\\ \zeta^2 = p\,\varepsilon_0\quad(\alpha_1 = \zeta).\end{cases}$$

Für ganzzahliges $\mathfrak{u}^*$ ist notwendig $x_n = 0$. Man erhält damit die Lösungsvektoren

$$(44)\qquad \pm\,\mathfrak{e}_i \pm \mathfrak{e}_k,\quad i < k < n.$$

22. $\mathfrak{y}^2 = 2\,\varepsilon_0$. Wir beweisen zunächst, daß $\mathfrak{u}^*$ und $\mathfrak{v}^*$ linear abhängig sind. Aus der Unabhängigkeit der Vektoren würde nämlich nach (35) folgen, daß $a = 21$ und $\mathfrak{u}^*, \mathfrak{v}^*$ beide halbzahlig wären. (36) ergibt dann einen Widerspruch. Nach (34) ist

$$|x_n| \leqq \sqrt{2},\quad |x_n'| \leqq \sqrt{2}.$$

Für irrationales x_n werden diese Ungleichungen nur befriedigt, wenn $a = 21$ und

$$x_n = \frac{\sigma_n}{2}\,\frac{1+\sqrt{21}}{2}\quad\text{oder}\quad x_n = \frac{\sigma_n}{2}\,\frac{1-\sqrt{21}}{2}.$$

Im ersten Fall resultiert aus (36) $\mathfrak{u}^* = \mathfrak{v}^*$, $\mathfrak{u}^{*2} = \frac{1}{4}$, $n = 2$, also $x_1 = \frac{\sigma_1}{2}$. $\sigma_1\sigma_2 = 1$ wird durch (5''') gefordert. Im zweiten Fall ist (34) äquivalent mit

$$\begin{aligned}\tfrac{7}{2} &= \mathfrak{u}^{*2} + 5\,(\mathfrak{u}^* - \mathfrak{v}^*)^2,\\ \tfrac{9}{4} &= \mathfrak{v}^{*2} + 5\,(\mathfrak{u}^* - \mathfrak{v}^*)^2.\end{aligned}$$

Aus diesem System ist zu ersehen, daß $\mathfrak{u}^*, \mathfrak{v}^*$ nicht beide halbzahlig, dann aber, daß $\mathfrak{u}^*$ halbzahlig und $\mathfrak{v}^*$ ganzzahlig sind. Man erhält somit $(\mathfrak{u}^* - \mathfrak{v}^*)^2 = \frac{1}{4}$, $\mathfrak{v}^{*2} = 1$, $\mathfrak{u}^{*2} = \frac{9}{4}$, also $n = 2$ und $u_1 = \frac{3}{2}\sigma_1$,

$v_1 = 0$. Wie oben ist auch hier $\sigma_1 \sigma_2 = 1$. Die vier Lösungsvektoren lauten:

$$(45)\quad \left.\begin{array}{l} \pm \frac{1}{2}\left(\mathfrak{e}_1 + \frac{1+\sqrt{21}}{2}\sqrt{\frac{5+\sqrt{21}}{2}}\,\mathfrak{e}_2\right) \\ \pm \frac{1}{2}\left(\frac{5+\sqrt{21}}{2}\,\mathfrak{e}_1 + \frac{1-\sqrt{21}}{2}\sqrt{\frac{5+\sqrt{21}}{2}}\,\mathfrak{e}_2\right) \end{array}\right\} \text{ für } \quad a = 21,\ n = 2.$$

Wir diskutieren den Fall rationaler x_n. Die lineare Abhängigkeit von $\mathfrak{u}^*$ und $\mathfrak{v}^*$ besagt, daß

$$\mathfrak{u}^* = s\,\mathfrak{w}, \quad \mathfrak{v}^* = r\,\mathfrak{w}, \quad (r, s) = 1,$$

und führt über (34) zu

$$2\,\varepsilon_0 = \mathfrak{w}^2 (s\,\omega_1 + r\,\omega_2)^2 + x_n^2\,\varepsilon_0 .$$

Mit x_n wären auch $\mathfrak{u}^*$, $\mathfrak{v}^*$ und damit $\mathfrak{w}$ ganzzahlig, da der Nenner von $\mathfrak{w}$ sowohl r als auch s teilen würde. Das führt zu einem Widerspruch mit der letzten Gleichung. Mögliche halbzahlige Werte von x_n sind $x_n = \frac{\sigma_n}{2}$. Da $2\,\mathfrak{w}$ ganzzahlig ist, so folgt aus $7\,\varepsilon_0 = (2\,\mathfrak{w})^2 \zeta^2$, $\zeta = s\,\omega_1 + r\,\omega_2$, daß $\mathfrak{w} = \frac{\sigma_i}{2}\,\mathfrak{e}_i$, $i < n$, also $n = 2$ und $\zeta^2 = 7\,\varepsilon_0$. Wie bei der Herleitung von (43) ergeben sich jetzt die Lösungsvektoren

$$(46)\quad \frac{\sqrt{\varepsilon_0}}{2}\,(\sigma_1 \sqrt{7}\,\mathfrak{e}_1 + \sigma_2\,\mathfrak{e}_2), \quad \sigma_1\sigma_2 = -\operatorname{sgn}\zeta \quad \begin{cases} \text{für} \quad n = 2, \\ \zeta^2 = 7\,\varepsilon_0 \quad (\alpha_1 = \zeta). \end{cases}$$

Die Vektordiagramme L sind im allgemeinen irreduzibel, d. h. nicht in zwei zu einander orthogonale Teilmengen zerlegbar, und stimmen bis auf eine Ähnlichkeitstransformation mit den von WITT[5]) aufgestellten Diagrammen überein. Wir behalten für diese die WITTsche Bezeichnung A_n^*, B_n^*, ... bei. Die Relation $L \sim L^*$ bedeute die Ähnlichkeit der Diagramme L und L^*. Zusammenfassend stellen wir dann fest:

Satz 7: *Für $a \equiv 5\,(8)$ setzt sich L aus folgenden Vektoren zusammen:*

1. $\varepsilon = 1,\ n = 4,\ a = 5$:	$(39) + (41)$	$\sim G_4^*$
2. $\varepsilon = 1,\ n = 8$:	$(40) + (41)$	$\sim E_8^*$
3. $\varepsilon = \varepsilon_0,\ n = 2,\ a = 21$:	$(42) + (43) + (45) + (46)$	$\sim D_{(6)}^*\ (\lambda < 1)$
4. $\varepsilon = \varepsilon_0,\ n = 2,\ a > 21,\ \zeta^2 = 7\,\varepsilon_0$:	$(43) + (46)$	$\sim D_{(2)}^*\ (\lambda < 1)$
5. $\varepsilon = \varepsilon_0,\ n = 4,\ \zeta^2 = 5\,\varepsilon_0$:	$(43) + (44)$	$\sim A_4^*$
6. $\varepsilon = \varepsilon_0,\ n = 6,\ \zeta^2 = 3\,\varepsilon_0$:	$(43) + (44)$	$\sim E_6^*$
7. $\varepsilon = 1$ *in allen übrigen Fällen*:	(41)	$\sim B_n^*$
8. $\varepsilon = \varepsilon_0$ „ „ „ „ :	(44)	$\sim B_{n-1}^*$

(dabei ist B_1^* leer, $B_2^* \sim D_{(2)}^*(\lambda = 1)$, $B_3^* \sim A_3^*$).

Die Zahl 2 wird durch die Form $\mathfrak{Q}$ entsprechend den acht Fällen 120, 240, 6, 2, 20, 72, $2n(n-1)$, $2(n-1)(n-2)$ *mal dargestellt;* $2\varepsilon_0$ *wird im 3. Fall 6 mal, im 4. Fall 2 mal und sonst nicht dargestellt.*

§ 3.

Berechnung des Vektordiagramms L für $a \equiv 2, 3\,(4)$.

Das Formelsystem (27) bis (36) ist jetzt entsprechend der Wahl von $1, \sqrt{a}$ als Minimalbasis in $R(\sqrt{a})$ mit $a \equiv 2, 3\,(4)$ zu modifizieren:

$$\mathfrak{x} = \mathfrak{u} + \mathfrak{v}\sqrt{a}, \tag{47}$$

$$\begin{aligned} \mathfrak{u} &= \{u_1, u_2, \ldots, u_n\} = \mathfrak{u}^* + u_n \mathfrak{e}_n, \\ \mathfrak{v} &= \{v_1, v_2, \ldots, v_n\} = \mathfrak{v}^* + v_n \mathfrak{e}_n. \end{aligned} \tag{48}$$

$$\mathfrak{x}^2 = \mathfrak{u}^2 + a\mathfrak{v}^2 + 2\mathfrak{u}\mathfrak{v}\sqrt{a}, \tag{49}$$

$$\mathbf{N}\mathfrak{x}^2 = (\mathfrak{u}^2 - a\mathfrak{v}^2)^2 + 4a[\mathfrak{u}^2\mathfrak{v}^2 - (\mathfrak{u}\mathfrak{v})^2], \tag{50}$$

$$\mathfrak{y} = \{x_1, \ldots, x_{n-1}, x_n\sqrt{\varepsilon}\} = \mathfrak{u}^* + \mathfrak{v}^*\sqrt{a} + x_n\sqrt{\varepsilon}\,\mathfrak{e}_n, \tag{51}$$

$$\mathfrak{y}^2 = \mathfrak{u}^{*2} + a\mathfrak{v}^{*2} + 2\mathfrak{u}^*\mathfrak{v}^*\sqrt{a} + x_n^2\varepsilon, \tag{52}$$

$$\begin{aligned} \mathbf{N}\mathfrak{y}^2 = {} & (\mathfrak{u}^{*2} - a\mathfrak{v}^{*2})^2 + 4a[\mathfrak{u}^{*2}\mathfrak{v}^{*2} - (\mathfrak{u}^*\mathfrak{v}^*)^2] \\ & + (u_n^2 - a v_n)^2 + \mathbf{S}\left(\sum_{i=1}^{n-1} x_i^2 x_n'^2 \varepsilon'\right), \end{aligned} \tag{53}$$

$$\mathbf{S}\,\mathfrak{y}^2 = 2(\mathfrak{u}^{*2} + a\mathfrak{v}^{*2}) + \mathbf{S}\,x_n^2\varepsilon. \tag{54}$$

Da $\alpha_1 = \alpha \equiv 1\,(\mathfrak{p})$, so sind nach (5″) die Komponenten von $\mathfrak{u}$ und $\mathfrak{v}$ durchweg ganzzahlig oder halbzahlig, woraus

$$\mathfrak{u}^2 \equiv \mathfrak{v}^2 \equiv \mathfrak{u}\mathfrak{v} \equiv 0\,(\tfrac{1}{2})$$

zu schließen ist. Wir bestimmen nun die Darstellungen $\mathfrak{y}^2 = 2$ und $\mathfrak{y}^2 = 2\varepsilon_0$.

1. $\varepsilon = 1$. Es ist dann $\mathfrak{y} = \mathfrak{x}$.

11. $\mathfrak{x}^2 = 2$. Die Gleichung (49) zerfällt in

$$2 = \mathfrak{u}^2 + a\mathfrak{v}^2, \quad \mathfrak{u}\mathfrak{v} = 0. \tag{55}$$

Wenn $\mathfrak{v} \neq 0$, so ist $a = 2$ oder 3. Für $a = 2$ kommt nur $n \equiv 0\,(4)$ in Frage, so daß $\mathfrak{u}^2 \equiv \mathfrak{v}^2 \equiv 0\,(1)$ und zufolge (55) $\mathfrak{u} = 0$, $\mathfrak{v}^2 = 1$. Die Lösungsvektoren mit halbzahligem $\mathfrak{v}$ lauten daher:

$$\frac{1}{\sqrt{2}}(\pm\mathfrak{e}_1 \pm \mathfrak{e}_2 \pm \mathfrak{e}_3 \pm \mathfrak{e}_4) \quad \text{für} \quad n = 4,\ a = 2 \tag{56}$$

und die mit ganzzahligem $\mathfrak{v}$:

$$\pm\sqrt{2}\,\mathfrak{e}_i \quad \text{für} \quad a = 2. \tag{57}$$

Für $a = 3$ erhält man $\mathfrak{u}^2 = \mathfrak{v}^2 = \frac{1}{2}$, $\mathfrak{u}\mathfrak{v} = 0$ und damit die Lösungsvektoren

(58) $$\pm \frac{1+\sigma\sqrt{3}}{2}\,\mathfrak{e}_1 \pm \frac{1-\sigma\sqrt{3}}{2}\,\mathfrak{e}_2,\quad \sigma = \pm 1,\quad \text{für}\quad n = 2,\ a = 3.$$

$\mathfrak{v} = 0$ liefert nur die ganzzahligen Lösungsvektoren

(59) $$\pm\,\mathfrak{e}_i \pm \mathfrak{e}_k,\ i < k.$$

12. $\mathfrak{x}^2 = 2\varepsilon_0$. Aus der linearen Unabhängigkeit von $\mathfrak{u}$ und $\mathfrak{v}$ folgt nach (50), daß $a = 3$ (in $R(\sqrt{2})$ ist $\mathbf{N}\varepsilon_0 = -1$) und $\mathfrak{u}, \mathfrak{v}$ beide halbzahlig sind. Mit $\varepsilon_0 = 2 + \sqrt{3}$ geht (49) über in

$$4 = \mathfrak{u}^2 + 3\mathfrak{v}^2,\quad 1 = \mathfrak{u}\mathfrak{v}.$$

Da $\mathfrak{u}, \mathfrak{v}$ unabhängig und halbzahlig sind, so ist $n = 2$. Man findet dann leicht die Lösungsvektoren

(60) $$\left.\begin{array}{l} \pm \frac{1+\sqrt{3}}{2}\,\mathfrak{e}_1 \pm \frac{3+\sqrt{3}}{2}\,\mathfrak{e}_2 \\ \pm \frac{3+\sqrt{3}}{2}\,\mathfrak{e}_1 \pm \frac{1+\sqrt{3}}{2}\,\mathfrak{e}_2 \end{array}\right\}\quad \text{für}\quad n = 2;\ a = 3.$$

Wir können nun voraussetzen, daß $\mathfrak{u}$ und $\mathfrak{v}$ linear abhängig sind:

$$\mathfrak{v} = r\mathfrak{w},\quad \mathfrak{u} = s\mathfrak{w},\quad (r, s) = 1.$$

$2\mathfrak{w}^2$ ist offenbar ganzzahlig. Nach (50) ist $\pm 2 = \mathfrak{w}^2(s^2 - a r^2)$. Da 4 kein Teiler von $s^2 - a r^2$ ist, so ist $\mathfrak{w}^2$ ganzzahlig. Nach (50) ergibt sich dann $\mathfrak{w}^2 = 1$ und $\xi^2 = 2\varepsilon_0$ mit $\xi = s + r\sqrt{a}$, d. h. daß das Primideal $\mathfrak{p}$, welches 2 teilt, ein Hauptideal ist. Die ganzzahligen $\mathfrak{w} = \pm\,\mathfrak{e}_i$ ergeben die Lösungsvektoren

(61) $$\pm\,\xi\,\mathfrak{e}_i \quad \text{für}\quad \xi^2 = 2\varepsilon_0$$

und die halbzahligen $\mathfrak{w} = \frac{1}{2}(\pm\,\mathfrak{e}_1 \pm \mathfrak{e}_2 \pm \mathfrak{e}_3 \pm \mathfrak{e}_4)$ für $n = 4$ ergeben

(62) $$\frac{\xi}{2}(\pm\,\mathfrak{e}_1 \pm \mathfrak{e}_2 \pm \mathfrak{e}_3 \pm \mathfrak{e}_4) \quad \text{für}\quad n = 4,\ \xi^2 = 2\varepsilon_0.$$

2. $\varepsilon = \varepsilon_0$. Es ist dann $a = 6$ oder 14 oder $a \geqq 22$.

21. $\mathfrak{y}^2 = 2$. Nach (54) ist $\mathfrak{v}^* \neq 0$ nur mit $a = 6$, $n = 2$, $\mathfrak{v}^{*2} = \frac{1}{4}$ verträglich. Da für gerade a der Vektor $\mathfrak{u}$ ganzzahlig ist, so ist nach (54) $\mathfrak{u}^* = 0$ und nach (52) $x_2 = \pm\frac{2-\sqrt{6}}{2}$, dazu kommt $x_1 = \pm\frac{\sqrt{6}}{2}$. Es ergeben sich somit die Lösungsvektoren

(63) $$\pm\sqrt{\frac{3}{2}}\,\mathfrak{e}_1 \pm \frac{1}{\sqrt{2}}\,\mathfrak{e}_2 \quad \text{für}\quad n = 2,\ a = 6.$$

Wenn $\mathfrak{v}^* = 0$, dann sind $\mathfrak{u}, x_n$ ganzzahlig und aus $2 = \mathfrak{u}^{*2} + x_n^2\varepsilon_0$ leitet man sofort die Lösungsvektoren

(64) $$\pm\sqrt{2}\,\mathfrak{e}_n \quad \text{für}\quad \xi^2 = 2\varepsilon_0$$

und

(65) $$\pm \mathfrak{e}_i \pm \mathfrak{e}_k,\quad i < k < n$$

ab.

22. $\mathfrak{y}^2 = 2\varepsilon_0$. Wären $\mathfrak{u}^*$ und $\mathfrak{v}^*$ linear unabhängig, so würde nach (53) $a = 6$ oder 14 folgen. Da aber für gerade a der Vektor $\mathfrak{u}$ ganzzahlig ist, so kommen zufolge (53) auch $a = 6$ und 14 nicht vor, und wir können $\mathfrak{v}^* = r\mathfrak{w}$, $\mathfrak{u}^* = s\mathfrak{w}$, $(r, s) = 1$ annehmen. Nach (52) ist mit $\zeta = s + r\sqrt{a}$:

(66) $$2\varepsilon_0 = \mathfrak{w}^2\zeta^2 + x_n'^2\varepsilon_0,$$

woraus insbesondere $|x_n| \leqq \sqrt{2}$, $|x_n'| \leqq \sqrt{2}$ folgt. Diese Ungleichungen sind für irrationales x_n nur erfüllt, wenn $a = 6$ und $x_n = \pm\frac{\sqrt{6}}{2}$. Da $2\mathfrak{w}$ ganzzahlig, so ergibt (66) $\mathfrak{w}^2 = \frac{1}{4}$, $\zeta^2 = 2\varepsilon_0$. Also ist $n = 2$, $\mathfrak{w} = \pm\frac{1}{2}\mathfrak{e}_1$, $x_1 = \pm\frac{2+\sqrt{6}}{2}$, $x_2 = \pm\frac{\sqrt{6}}{2}$, woraus die Lösungsvektoren

(67) $$\frac{2+\sqrt{6}}{2}(\pm\mathfrak{e}_1 \pm \sqrt{3}\,\mathfrak{e}_2) \quad \text{für} \quad n = 2,\ a = 6$$

abgeleitet werden. Wenn x_n rational, dann ist x_n und folglich $\mathfrak{u}^*$, $\mathfrak{v}^*$ und $\mathfrak{w}$ ganzzahlig, also nach (66) $x_n = 0$. Man erhält somit die Lösungsvektoren

(68) $$\pm\zeta\mathfrak{e}_i,\ i < n \quad \text{für} \quad \zeta^2 = 2\varepsilon_0.$$

Wir fassen die Ergebnisse zusammen in

Satz 8. *Für $a \equiv 2, 3\ (4)$ setzt sich L aus folgenden Vektoren zusammen:*

1. $\varepsilon = 1,\ n = 2,\ a = 3$:	(58)+(59)+(60)+(61)	$\sim D^*_{(12)}\ (\lambda < 1)$
2. $\varepsilon = 1,\ n = 2,\ a > 3,\ \zeta^2 = 2\varepsilon_0$:	(59)+(61)	$\sim D^*_{(4)}\ (\lambda < 1)$
3. $\varepsilon = 1,\ n = 4,\ a = 2$:	(56)+(57)+(59)	$\sim F^*_4\ (\lambda = \sqrt{2})$
4. $\varepsilon = 1,\ n = 4,\ \zeta^2 = 2\varepsilon_0$:	(59)+(61)+(62)	$\sim F^*_4\ (\lambda < \sqrt{2})$
5. $\varepsilon = 1,\ n > 4,\ a = 2$:	(57)+(59)	$\sim C^*_n\ (\lambda = \sqrt{2})$
6. $\varepsilon = 1,\ n > 4,\ \zeta^2 = 2\varepsilon_0$:	(59)+(61)	$\sim C^*_n\ (\lambda \neq \sqrt{2})$
7. $\varepsilon = \varepsilon_0,\ n = 2,\ a = 6$:	(63)+(64)+(67)+(68)	$\sim D^*_{(6)}\ (\lambda < 1)$
8. $\varepsilon = \varepsilon_0,\ n = 2,\ a > 6,\ \zeta^2 = 2\varepsilon_0$:	(64)+(68)	$\sim D^*_{(2)}\ (\lambda < 1)$
9. $\varepsilon = \varepsilon_0,\ n > 2,\ \zeta^2 = 2\varepsilon_0$:	(64)+(65)+(68)	$\sim C^*_{n-1} + A^*_1\ (\lambda \neq \sqrt{2})$
10. $\varepsilon = 1$ *in allen übrigen Fällen*:	(59)	$\sim B^*_n$
11. $\varepsilon = \varepsilon_0$ „ „ „ „ :	(65)	$\sim B^*_{n-1}$

(dabei ist B^*_1 leer, $B^*_2 \sim D^*_{(2)}\ (\lambda = 1)$, $B^*_3 \sim A^*_3$).

Die Zahl 2 wird durch die Form $\mathfrak{Q}$ entsprechend den elf Fällen 12, 4, 48, 24, $2n^2$, $2n(n-1)$, 6, 2, $2(n-1)(n-2)+2$, $2n(n-1)$, $2(n-1)(n-2)$ mal und die Zahl $2\varepsilon_0$ entsprechend 12, 4, 0, 24, 0, $2n$, 6, 2, $2(n-1)$, 0, 0 mal dargestellt.

§ 4.

Berechnung der Automorphismengruppe $\mathfrak{G}$ für N.

Unter einer Transformation soll stets eine orthogonale Transformation verstanden werden. Reduziert man alle Vektoren in L auf gleiche Länge, so gehe das Vektordiagramm L in $\overline{L}$ über. Es bedeute

$$
(69)\qquad
\begin{array}{l}
\mathfrak{S} \text{ die Spiegelungsgruppe von } L,\\
\mathfrak{G} \text{ die Gruppe aller Transformationen von } N \text{ in sich},\\
\mathfrak{H} \quad ,, \qquad ,, \qquad ,, \qquad\qquad ,, \qquad L \;,, \;\; ,, \;;\\
\overline{\mathfrak{H}} \quad ,, \qquad ,, \qquad ,, \qquad\qquad ,, \qquad \overline{L} \;,, \;\; ,, \;.
\end{array}
$$

Offenbar ist

$$
(70)\qquad \mathfrak{S} \subset \mathfrak{G} \subset \mathfrak{H} \subset \overline{\mathfrak{H}}.
$$

Mit L^* bezeichnen wir irgend eines der Wittschen Vektordiagramme $A_n^*, B_n^*, \ldots$. Das Diagramm $\overline{L}^*$ entstehe aus L^*, wenn man in L^* alle Vektoren auf gleiche Länge reduziert. Analog zu (69) sei

$$
(71)\qquad
\begin{array}{l}
\mathfrak{S}^* \text{ die Spiegelungsgruppe von } L^*,\\
\mathfrak{H}^* \text{ die Gruppe aller Transformationen von } L^* \text{ in sich},\\
\overline{\mathfrak{H}}^* \quad ,, \qquad ,, \qquad ,, \qquad\qquad ,, \qquad \overline{L}^* \;,, \;\; ,, \;.
\end{array}
$$

Wenn L und L^* ähnlich sind, dann sind die Gruppen $\mathfrak{S}, \mathfrak{H}$ bzw. $\overline{\mathfrak{H}}$ zu $\mathfrak{S}^*, \mathfrak{H}^*$ bzw. $\overline{\mathfrak{H}}^*$ isomorph. Nach Witt[5]) ist

$$
(72)\qquad (\overline{\mathfrak{H}}^* : \mathfrak{S}^*) = \begin{cases} 1 & \text{für } L^* = A_1^*,\ C_n^*\,(n \neq 2),\ E_8^*,\ G_4^*,\\ 2 & \;,, \quad L^* = A_n^*\,(n > 1),\ B_n^*\,(n \neq 4),\ D_{(m)}^*,\ E_6^*,\ F_4^*,\\ 6 & \;,, \quad L^* = B_4^*. \end{cases}
$$

Die Ordnungen der im Verlauf dieses Paragraphen auftretenden Spiegelungsgruppen $\mathfrak{S}^*$ haben nach Witt[5]) Satz 10 folgende Werte:

(73)

L^*	A_n^*	B_n^*	C_n^*	$D_{(m)}^*$	E_6^*	E_8^*	F_4^*	G_4^*
$(\mathfrak{S}^* : 1)$	$(n+1)!$	$2^{n-1}\,n!$	$2^n\,n!$	$2\,m$	$72 \cdot 6!$	$192 \cdot 10!$	$2^7 \cdot 3^2$	$5!^2$

Dabei ist der Wert für $L^* = E_6^*$ bereits korrigiert. Bestimmt man in E_6^* alle zu einem festen Vektor des Diagramms E_6^* orthogonalen Vektoren, so erhält man ein 5-dimensionales irreduzibles Vektordiagramm von 30 Vektoren. Es handelt sich hierbei um A_5^* und nicht, wie Witt angibt, um B_5^*. Die Buchstaben $S, S_1, S_2, \ldots$ mögen orthogonale Transformationen des n-dimensionalen Raumes in sich bezeichnen. D entstehe aus der n-reihigen Einheitsmatrix, wenn man die letzte 1 in der Hauptdiagonale durch $\sqrt{\varepsilon}$ ersetzt. Einer Transformation

$$
(74)\qquad \tilde{\mathfrak{y}} = S\mathfrak{y}, \quad S \subset \mathfrak{G}
$$

entspricht dann vermöge $\mathfrak{y} = D\mathfrak{x}$ eine Abbildung

$$
(75)\qquad \tilde{\mathfrak{x}} = D^{-1} S D \mathfrak{x}
$$

des Lösungsmoduls M des Kongruenzensystems (5).

Um die Ordnung der Gruppe $\mathfrak{G}$ zu bestimmen, genügt es im wesentlichen, den Index $(\mathfrak{G}:\mathfrak{S})$ zu berechnen. In den Fällen $L \sim C_n^* (n \neq 2)$, E_8^*, G_4^* ist zufolge (70) und (72) sofort $(\mathfrak{G}:\mathfrak{S}) = 1$ zu schließen. Wir diskutieren der Reihe nach die übrigen Fälle.

1. $L \sim A_4^*$. Wir brauchen dann nur Satz 7, 5. Fall zu betrachten. $\mathfrak{S}$ enthält die Spiegelungsgruppe $\mathfrak{S}_1$ zum Diagramm $\pm \mathfrak{e}_i \pm \mathfrak{e}_k$, $i < k < 4$ $(\sim A_3^*)$. Die Transformation S, definiert durch

$$S\mathfrak{e}_1 = \mathfrak{e}_1, \quad S\mathfrak{e}_2 = \mathfrak{e}_2, \quad S\mathfrak{e}_3 = -\mathfrak{e}_3, \quad S\mathfrak{e}_4 = -\mathfrak{e}_4,$$

ist nicht in $\mathfrak{S}_1$ enthalten, aber mit $\mathfrak{S}_1$ vertauschbar. Da $(\mathfrak{S}:\mathfrak{S}_1) = 5$, so liegt S auch nicht in $\mathfrak{S}$, so daß $\mathfrak{H} = \mathfrak{S} + \mathfrak{S}S = \mathfrak{G}$; denn $D^{-1}SD = S$ führt (5) in sich über.

2. $L \sim B_n^* (n \neq 4)$. Es ist dann stets $L = B_n^*$. Die Transformation

$$S\mathfrak{e}_1 = -\mathfrak{e}_1, \quad S\mathfrak{e}_i = \mathfrak{e}_i \quad \text{für} \quad i > 1$$

führt zwar L in sich über, liegt aber nicht in $\mathfrak{S}$, so daß $\mathfrak{H} = \mathfrak{S} + \mathfrak{S}S$. $D^{-1}SD = S$ führt (5) in sich über, wenn $a \equiv 2, 3\,(4)$, für $a \equiv 5\,(8)$ dagegen nicht, so daß

$$\mathfrak{G} = \begin{cases} \mathfrak{S} & \text{für} \quad a \equiv 5\,(8), \\ \mathfrak{S} + \mathfrak{S}S & \quad ,, \quad a \equiv 2, 3\,(4). \end{cases}$$

3. $L \sim B_{n-1}^* (n > 2)$. Auch hier ist $L = B_{n-1}^*$. Eine Transformation aus $\mathfrak{H}$ permutiert notwendig die Vektoren $\pm \mathfrak{e}_n$ unter sich, da der zu L orthogonale lineare Raum aus den Vielfachen von $\mathfrak{e}_n$ besteht. $\mathfrak{S}$ hat in der Gruppe der Transformationen von L in sich, welche $\mathfrak{e}_n$ festlassen, den Index 2. Definieren wir S_1 und S_2 durch

$$\begin{aligned} S_1\mathfrak{e}_1 &= -\mathfrak{e}_1, \quad S_1\mathfrak{e}_i = \mathfrak{e}_i \quad \text{für} \quad i > 1, \\ S_2\mathfrak{e}_k &= \mathfrak{e}_k, \quad\;\; S_2\mathfrak{e}_n = -\mathfrak{e}_n \quad ,, \quad k < n, \end{aligned}$$

so ist leicht zu sehen, daß

$$\mathfrak{H} = \mathfrak{S} + \mathfrak{S}S_1 + \mathfrak{S}S_2 + \mathfrak{S}S_1S_2.$$

Das System (5) ist bezüglich $D^{-1}S_iD = S_i\,(i = 1, 2)$ invariant, wenn $a \equiv 2, 3\,(4)$, aber nicht für $a \equiv 5\,(8)$. Damit erhält man

$$\mathfrak{G} = \begin{cases} \mathfrak{S} & \text{für} \quad a \equiv 5\,(8), \\ \mathfrak{S} + \mathfrak{S}S_1 + \mathfrak{S}S_2 + \mathfrak{S}S_1S_2 & \quad ,, \quad a \equiv 2, 3\,(4). \end{cases}$$

4. $L \sim B_4^*$. Dann ist $L = B_4^*$ und $\varepsilon = 1$. Es sei

$$S_1\mathfrak{e}_1 = -\mathfrak{e}_1, \quad S_1\mathfrak{e}_i = \mathfrak{e}_i \quad \text{für} \quad i > 1$$

und S_2 die Spiegelung an der Normalebene zu $\frac{1}{\sqrt{2}}(\mathfrak{e}_1 + \mathfrak{e}_2 + \mathfrak{e}_3 + \mathfrak{e}_4)$:

$$S_2\mathfrak{e}_i = \tfrac{1}{2}(\mathfrak{e}_i - \sum_{k \neq i} \mathfrak{e}_k).$$

Beide Transformationen führen L in sich über. Mit Hilfe der Matrizendarstellungen für S_i errechnet man die Relationen

$$S_3 = S_1 S_2, \quad S_1^2 = S_3^3 = E, \quad S_1 S_3 = S_3^2 S_1.$$

Ein Potenzprodukt $S_1^\mu S_3^\nu$ liegt also nur dann in $\mathfrak{S}$, wenn $\mu \equiv 0\,(2)$, $\nu \equiv 0\,(3)$, so daß

$$\mathfrak{H} = \sum_{\mu,\,\nu} \mathfrak{S} S_1^\mu S_3^\nu \quad (\mu = 0, 1; \quad \nu = 0, 1, 2).$$

Die Transformation S_3 vermittelt die Abbildung

$$\begin{aligned}
\tilde{x}_1 &= \tfrac{1}{2}(-x_1 + x_2 + x_3 + x_4),\\
\tilde{x}_2 &= \tfrac{1}{2}(-x_1 + x_2 - x_3 - x_4),\\
\tilde{x}_3 &= \tfrac{1}{2}(-x_1 - x_2 + x_3 - x_4),\\
\tilde{x}_4 &= \tfrac{1}{2}(-x_1 - x_2 - x_3 + x_4).
\end{aligned}$$

Aus dieser expliziten Darstellung folgt nach kurzer Rechnung die Invarianz von (5) bezüglich S_3. S_1 läßt (5) nur invariant für $a \equiv 2, 3\,(4)$, dagegen nicht für $a \equiv 5\,(8)$. Man erhält daher folgendes Resultat:

$$\mathfrak{G} = \begin{cases} \mathfrak{S} + \mathfrak{S} S_3 + \mathfrak{S} S_3^2 & \text{für} \quad a \equiv 5\,(8),\\ \mathfrak{S} + \mathfrak{S} S_3 + \mathfrak{S} S_3^2 + \mathfrak{S} S_1 + \mathfrak{S} S_1 S_3 + \mathfrak{S} S_1 S_3^2 & \,„ \quad a \equiv 2, 3\,(4). \end{cases}$$

5. $L \sim D^*_{(m)}\,(\lambda < 1)$. Da L Vektoren verschiedener Länge enthält, ist offenbar $(\overline{\mathfrak{H}} : \mathfrak{H}) = 2$, also $\mathfrak{G} = \mathfrak{S}$.

6. $L \sim E_6^*$. Es handelt sich um Satz 7, 6. Fall. Ähnlich wie im Fall $L \sim A_4^*$ schließt man, daß die Transformation S, definiert durch

$$S\mathfrak{e}_i = \mathfrak{e}_i \quad \text{für} \quad i < 5, \quad S\mathfrak{e}_5 = -\mathfrak{e}_5, \; S\mathfrak{e}_6 = -\mathfrak{e}_6,$$

mit der Spiegelungsgruppe $\mathfrak{S}_1$ zum Diagramm $\pm\mathfrak{e}_i \pm \mathfrak{e}_k$, $i < k < 6\,(\sim B_5^*)$ vertauschbar ist und weder in $\mathfrak{S}_1$ noch in $\mathfrak{S}$ enthalten ist; denn es ist $(\mathfrak{S} : \mathfrak{S}_1) = 3^3$. S läßt das System (5) invariant, so daß

$$\mathfrak{G} = \mathfrak{H} = \mathfrak{S} + \mathfrak{S} S.$$

7. $L \sim F_4^*$. Das Diagramm $\overline{L}$ setzt sich aus den beiden Systemen

$$(76) \qquad \pm\mathfrak{e}_i \pm \mathfrak{e}_k \; (i < k)$$

und

$$(77) \qquad \frac{1}{\sqrt{2}}(\pm\mathfrak{e}_1 \pm \mathfrak{e}_2 \pm \mathfrak{e}_3 \pm \mathfrak{e}_4), \; \pm\sqrt{2}\,\mathfrak{e}_i$$

zusammen. Diese werden durch die Transformation S, definiert durch

$$S\mathfrak{e}_1 = \frac{1}{\sqrt{2}}(\mathfrak{e}_1 - \mathfrak{e}_2), \quad S\mathfrak{e}_3 = \frac{1}{\sqrt{2}}(\mathfrak{e}_3 - \mathfrak{e}_4),$$
$$S\mathfrak{e}_2 = \frac{1}{\sqrt{2}}(\mathfrak{e}_1 + \mathfrak{e}_2), \quad S\mathfrak{e}_4 = \frac{1}{\sqrt{2}}(\mathfrak{e}_3 + \mathfrak{e}_4)$$

miteinander vertauscht. Da die Matrizen der Transformationen aus $\mathfrak{S}$ rationale Koeffizienten haben, so liegt S nicht in $\mathfrak{S}$, sodaß $\overline{\mathfrak{H}} = \mathfrak{S} + \mathfrak{S} S$. Wenn L Vektoren verschiedener Länge enthält, dann wird das System (76) durch die Transformationen aus $\mathfrak{H}$ in sich übergeführt. Es kann also S nicht in $\mathfrak{H}$ liegen und muß $\mathfrak{G} = \mathfrak{S}$ gelten. Enthält L nur

Vektoren der Länge $\sqrt{2}$, so ist $a = 2$ und die Transformation S läßt (5) invariant, mithin ist jetzt $\mathfrak{G} = \mathfrak{S} + \mathfrak{S}S$.

8. $L \sim C^*_{n-1} + A^*_1 (n > 2)$. L setzt sich zusammen aus den beiden orthogonalen Diagrammen C^*_{n-1} und $\pm\sqrt{2}\,e_n$, welche durch eine beliebige Transformation aus $\overline{\mathfrak{H}}$ in sich übergeführt werden. Da die Spiegelungsgruppe von L gleich dem direkten Produkt der Spiegelungsgruppen $\mathfrak{S}_1$ und $\mathfrak{S}_2$ zu C^*_{n-1} bzw. $\pm\sqrt{2}\,e_n$, so ist also $\overline{\mathfrak{H}} = \mathfrak{S}$ und $\mathfrak{G} = \mathfrak{S}_1 \times \mathfrak{S}_2$.

9. L ist leer. Dann ist $n = 2$ und $\varepsilon = \varepsilon_0$. Es sei

$$S = \begin{pmatrix} \beta_{11} & \frac{\beta_{12}}{\sqrt{\varepsilon_0}} \\ \sqrt{\varepsilon_0}\,\beta_{21} & \beta_{22} \end{pmatrix} = \begin{pmatrix} \sigma\cos\varphi & \sin\varphi \\ -\sigma\sin\varphi & \cos\varphi \end{pmatrix} \quad (\sigma = \pm 1)$$

eine Transformation aus $\mathfrak{G}$. Sie vermittelt die Abbildung

$$\begin{aligned} \tilde{x}_1 &= \beta_{11} x_1 + \beta_{12} x_2, \\ \tilde{x}_2 &= \beta_{21} x_1 + \beta_{22} x_2 \end{aligned} \tag{78}$$

des Lösungsmoduls M des Systems (5) in sich, woraus man ersieht, daß die Koeffizienten β_{ik} Körperzahlen mit der Eigenschaft $\beta_{ik} \equiv 0\,(\mathfrak{p}^{-2})$ sind. Für die β_{ik} bestehen die Beziehungen

$$\beta_{11}^2 + \beta_{12}^2 \varepsilon_0' = 1, \quad \beta_{21} = \pm\beta_{12}\varepsilon_0', \quad \beta_{22} = \pm\beta_{11}.$$
$$|\beta_{11}| \leqq 1, \quad |\beta_{11}'| \leqq 1.$$

Den Ungleichungen zufolge muß β_{11} rational sein; denn der Nenner von β_{11} ist beschränkt, und für $a \equiv 5\,(8)$ ist von vornherein $a > 64$ anzusetzen. Wir betrachten zunächst den Fall $a \equiv 2, 3\,(4)$. $\beta_{11} = \pm 1$ liefert die Vierergruppe, erzeugt von

$$S_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{79}$$

Für $\beta_{11} = \pm\frac{1}{2}$ ist $(2\beta_{12})^2 = 3\varepsilon_0$, d. h. $3/a$ und das Primideal, welches 3 teilt, ist Hauptideal. Wir bezeichnen mit ξ eine Erzeugende dieses Ideals, sodaß $\xi^2 = 3\varepsilon_0$. Offenbar ist $\alpha_1 = \xi$ zu wählen. Man erhält die acht zulässigen Transformationen

$$\begin{pmatrix} \frac{\sigma_1}{2} & \frac{\sigma_2}{2}\sqrt{3} \\ -\frac{\sigma_3}{2}\sqrt{3} & \frac{\sigma_4}{2} \end{pmatrix}, \quad \prod_{i=1}^{4}\sigma_i = 1. \tag{80}$$

Die zugehörigen Abbildungen (78) führen das System (5) in sich über, was eine einfache Rechnung erkennen läßt. S_3 sei die spezielle Transformation, die man für $\sigma_i = 1$ erhält. S_1 und S_3 erzeugen $\mathfrak{G}$, wenn $\xi^2 = 3\varepsilon_0$. Es bestehen die Relationen

$$S_1^2 = S_3^6 = (S_1 S_3)^2 = E.$$

Für $a \equiv 5\,(8)$ und $\beta_{11} = \pm 1, \pm \frac{1}{2}$ wird man auf dieselben Transformationen geführt. $\beta_{11} = \pm \frac{1}{4}, \pm \frac{3}{4}$ liefert nur noch Transformationen, welche (5) nicht invariant lassen. S_1 und S_2 lassen (5) nicht invariant, wohl aber $S_1 \cdot S_2$ und S_3. Es ergibt sich damit folgendes Resultat

$$
\mathfrak{G} = \begin{cases} \{S_3\} & \text{für} \quad a \equiv 5\,(8), \quad \zeta^2 = 3\,\varepsilon_0, \\ \{S_1 \cdot S_2\} & \text{„} \quad a \equiv 5\,(8) \quad \text{sonst}, \\ \{S_1, S_3\} & \text{„} \quad a \equiv 2, 3\,(4), \quad \zeta^2 = 3\,\varepsilon_0, \\ \{S_1, S_2\} & \text{„} \quad a \equiv 2, 3\,(4) \quad \text{sonst}. \end{cases} \tag{81}
$$

Die mit Hilfe der Tabelle (73) zu bestimmenden Ordnungen der Gruppe $\mathfrak{G}$ stellen wir zur Übersicht zusammen.

Satz 9. *Die Ordnung der Automorphismengruppe $\mathfrak{G}$ von N hat in Abhängigkeit von L folgenden Wert:*

$L \sim$	$(\mathfrak{G} : 1)$		$L \sim$	$(\mathfrak{G} : 1)$
A_4^*	$2 \cdot 5!$		E_8^*	$192 \cdot 10!$
B_4^*	$4!^2$	*für* $a \equiv 5\,(8)$	$F_4^*(\lambda < \sqrt{2})$	$2 \cdot 4!$
	$2 \cdot 4!^2$	„ $a \equiv 2,3\,(4)$	$F_4^*(\lambda = \sqrt{2})$	$4 \cdot 4!$
$B_{n-1}^*(n > 2)$	$2^{n-2}(n-1)!$	„ $a \equiv 5\,(8)$	G_4^*	$5!^2$
	$2^n(n-1)!$	„ $a \equiv 2,3\,(4)$	$C_{n-1}^* + A_1^*(n > 2)$	$2^n\,(n-1)!$
$B_n^*(n \neq 4)$	$2^{n-1}\,n!$	„ $a \equiv 5\,(8)$	*leer*	6 *für* $a \equiv 5(8)$, $\zeta^2 = 3\,\varepsilon_0$
	$2^n\,n!$	„ $a \equiv 2,3\,(4)$		2 „ $a \equiv 5(8)$ *sonst*
$C_n^*(n > 2)$	$2^n\,n!$			12 „ $a \equiv 2,3(4)$, $\zeta^2 = 3\,\varepsilon_0$
$D_{(m)}^*(\lambda < 1)$	$2\,m$			4 „ $a \equiv 2,3(4)$ *sont.*
E_6^*	$12^2 \cdot 6!$			

§ 5.

Betrachtungen zur Äquivalenz quadratischer Formen.

Die vorangehenden Untersuchungen der Eigenschaften von $\mathfrak{Q}$ sind so ausführlich dargestellt, daß die analogen Aussagen für die durch das System (15) definierte quadratische Form $\mathfrak{Q}^*$, die nach demselben Verfahren zu ermitteln sind, ohne Beweis mitgeteilt werden können. Dabei unterliegt der quadratische Körper $R(\sqrt{a})$ keinen Einschränkungen. Mit M^* bezeichnen wir den I-Modul der Lösungsvektoren $\mathfrak{x} = \{x_1, x_2, \ldots, x_n\}$ des Systems (15). L^* sei das Vektordiagramm in M^*, das alle Vektoren aus M^* der Längen $\sqrt{2}$ und $\sqrt{2\,\varepsilon_0}$ ($\varepsilon_0 \gg 0$ voraussgesetzt) enthält; L^* besteht aus folgenden Vektoren:

$$
\begin{gathered} \pm\,\mathfrak{e}_i \pm \mathfrak{e}_k \quad (i < k), \\ \tfrac{1}{2}\Big(\sum_{i=1}^{8} \sigma_i \mathfrak{e}_i\Big), \quad \prod_{i=1}^{8} \sigma_i = 1, \quad \text{zusätzlich für} \quad n = 8. \end{gathered} \tag{82}
$$

Daraus ist zu entnehmen, daß $2\varepsilon_0$ durch $\mathfrak{Q}^*$ nicht dargestellt wird. Die Automorphismengruppe $\mathfrak{G}^*$ von M^* ist mit der Spiegelungsgruppe zum Diagramm L^* identisch, sodaß auf Grund der Angaben des vorigen Paragraphen

$$(\mathfrak{G}^* : 1) = \begin{cases} 192 \cdot 10! & \text{für} \quad n = 8, \\ 2^{n-1} n! & \quad ,, \quad n > 8. \end{cases}$$

Für $a \equiv 2, 3\,(4)$, $n \equiv 0\,(8)$, $\varepsilon = 1$ zeigt nun die eingangs beschriebene Schlußweise, daß die Formen $\mathfrak{Q}$, $\varepsilon_0\mathfrak{Q}$, $\mathfrak{Q}^*$, $\varepsilon_0\mathfrak{Q}^*$ verschiedene Klassen repräsentieren; denn nach Satz (8) stellt $\mathfrak{Q}$ die Zahlen 2 und $2\varepsilon_0$ nicht gleich oft dar und nach Satz 9 ist $(\mathfrak{G} : 1) \neq (\mathfrak{G}^* : 1)$.

Wir können nun auch allgemein die Frage beantworten, wann $\mathfrak{Q}$ und $\varepsilon_0\mathfrak{Q}$ in derselben Klasse liegen. Notwendig dafür ist, daß die Zahlen 2 und $2\varepsilon_0$ durch $\mathfrak{Q}$ gleich oft dargestellt werden. Den Sätzen 7 und 8 entnehmen wir, daß dies nur in den drei unter (14) aufgeführten Fällen zutrifft. Für diese beweisen wir die Äquivalenz von $\mathfrak{Q}$ und $\varepsilon_0\mathfrak{Q}$.

1. $n = 2$, $\varepsilon = \varepsilon_0$. Mit $\mathfrak{x} = \{x_1, x_2\}$ ist auch $\mathfrak{x}^* = \{-x_2, x_1\varepsilon_0'\}$ ein Lösungsvektor von (5). Die zugeordneten nach der Vorschrift (9) zu berechnenden Vektoren in N lauten $\mathfrak{y} = \{x_1, x_2\sqrt{\varepsilon_0}\}$ und $\mathfrak{y}^* = \sqrt{\varepsilon_0'}\{-x_2\sqrt{\varepsilon_0}, x_1\}$. Wir wählen eine beliebige Basis $\mathfrak{y}_1, \mathfrak{y}_2$ in N; das zugeordnete Vektorpaar $\mathfrak{y}_1^*, \mathfrak{y}_2^*$ stellt ebenfalls eine Basis von N dar. Es ist dann

$$(\mathfrak{y}_i\mathfrak{y}_k) = \varepsilon_0(\mathfrak{y}_i^*\mathfrak{y}_k^*) \sim \varepsilon_0(\mathfrak{y}_i\mathfrak{y}_k)\,{}^{6)}, \quad \text{q. e. d.}$$

2. $n = 2$, $\varepsilon = 1$, $\xi^2 = 2\varepsilon_0$. Dann ist $a \equiv 3\,(4)$ und etwa $\alpha = \sqrt{a}$. Die Vektorpaare

$$\{1, -1\},\ \left\{\frac{1+\sqrt{a}}{2}, \frac{1-\sqrt{a}}{2}\right\} \quad \text{und} \quad \{\xi, 0\},\ \left\{\frac{\sqrt{a}}{\xi}, \frac{1}{\xi}\right\}$$

stellen Basen von N dar. Die mit diesen Basen gebildeten quadratischen Formen sind äquivalent. Das hat zur Folge

$$\begin{pmatrix} 2 & \sqrt{a} \\ \sqrt{a} & \frac{a+1}{2} \end{pmatrix} \sim \begin{pmatrix} \xi^2 & \sqrt{a} \\ \sqrt{a} & \frac{a+1}{\xi^2} \end{pmatrix} \sim \begin{pmatrix} \xi^2 & \sqrt{a}\,\varepsilon_0 \\ \sqrt{a}\,\varepsilon_0 & \frac{a+1}{\xi^2}\varepsilon_0^2 \end{pmatrix} = \varepsilon_0 \begin{pmatrix} 2 & \sqrt{a} \\ \sqrt{a} & \frac{a+1}{2} \end{pmatrix},$$

q. e. d.

3. $n = 4$, $\varepsilon = 1$, $\xi^2 = 2\varepsilon_0$. Die Zeilen der Matrix

$$A' = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & \xi & 0 \\ \frac{1}{\xi} & \frac{1}{\xi} & \frac{1}{\xi} & \frac{1}{\xi} \end{pmatrix}$$

---

[6]) Für zwei symmetrische Matrizen A und B möge $A \sim B$ bedeuten, daß die mit den Koeffizienten von A und B gebildeten quadratischen Formen äquivalent sind.

bilden ein System von Basisvektoren für N. Zu der mit dem Koeffizientenschema $A'A$ gebildeten quadratischen Form $\mathfrak{Q}$ findet man $\varepsilon_0 \mathfrak{Q}$ als äquivalente Form wie folgt:

$$A'A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & \zeta & 0 \\ 0 & \zeta & \zeta^2 & 1 \\ 0 & 0 & 1 & \frac{4}{\zeta^2} \end{pmatrix} \sim \begin{pmatrix} \frac{4}{\zeta^2} & 1 & 0 & 0 \\ 1 & \zeta^2 & \zeta & 0 \\ 0 & \zeta & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} \frac{4}{\zeta^2}\varepsilon_0^2 & \varepsilon_0 & 0 & 0 \\ \varepsilon_0 & \zeta^2 & \zeta\varepsilon_0 & 0 \\ 0 & \zeta\varepsilon_0 & 2\varepsilon_0^2 & \varepsilon_0 \\ 0 & 0 & \varepsilon_0 & 2 \end{pmatrix} = \varepsilon_0 A'A.$$

Damit ist bewiesen

Satz 10. *Notwendig und hinreichend für die Äquivalenz der quadratischen Formen $\mathfrak{Q}$ und $\varepsilon_0 \mathfrak{Q}$ ist die Bedingung* (14).

Zum Schluß soll gezeigt werden, daß im Körper $R(\sqrt{33})$ mit der Grundeinheit $\varepsilon_0 = 23 + 4\sqrt{33}$ eine positive gerade Form von 2 Variablen mit der Determinante ε_0 nicht durch Kongruenzen definiert werden kann, wie es sich oben für die Körper $R(\sqrt{a})$ mit $a \not\equiv 1\,(8)$ als möglich erwiesen hat, wenn die Bedingung (4) für $\varepsilon = \varepsilon_0$ erfüllt ist. Sei

$$\begin{pmatrix} A & B \\ B & C \end{pmatrix}$$

das Koeffizientenschema einer solchen Form, also

$$A \equiv C \equiv 0\,(2), \quad AC - B^2 = \varepsilon_0,$$

und

$$A = \alpha^2 + \varepsilon_0\beta^2, \quad B = \alpha\gamma + \varepsilon_0\beta\delta, \quad C = \gamma^2 + \varepsilon_0\delta^2$$

aus einer hypothetischen Darstellung der Form durch Kongruenzen nach einem beliebigen Modul gewonnen. Dann ist ein Widerspruch aufzudecken. Da $B^2 \equiv 1\,(4)$, so gilt auch $B^2 \equiv 1\,(8)$, also $AC \equiv \varepsilon_0 + 1 \equiv 4\,(8)$. $\frac{1}{2}A$ ist demnach teilerfremd zu 2. Die Primzahl 2 zerfällt vollständig in $K = R(\sqrt{33})$: $(2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$. Dagegen bleiben die Primideale $\mathfrak{p}_i$ im Körper $Z = K(\sqrt{-\varepsilon_0})$ unzerlegt. Z enthält nämlich den quadratischen Körper $R(\sqrt{-3})$, in welchem die Primzahl 2 unzerlegt bleibt. Die Zahl A erscheint als Relativnorm $\mathbf{N}_{Z/K}(\alpha + \sqrt{-\varepsilon_0}\,\beta)$ und müßte daher als gerade Zahl mindestens durch 4 teilbar sein, was nicht der Fall ist.

(Eingegangen am 25. August 1944.)