Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 36 (1961-1962)

Artikel: Über die Reduktion und die Darstellungen positiver quaternärer quadratischer Formen.
Autor: Weber, Oskar
DOI: https://doi.org/10.5169/seals-515624

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 15.04.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Über die Reduktion und die Darstellungen positiver quaternärer quadratischer Formen

von Oskar Weber, Zürich

Einleitung

Die Zahlentheorie ganz rationaler quaternärer Formen ist immer noch in den Anfängen.

Im 3. Band der «History of the theory of numbers» von Dickson [2], orientiert das zehnte Kapitel über die Untersuchungen und Ergebnisse auf diesem Gebiet bis um 1920.

Ich erwähne vor allem die zahlreichen Arbeiten Liouvilles, die er in den Jahren 1860–1865 in seinem Journal publiziert hat. Die von ihm behandelten positiven quaternären Formen lassen sich alle als Summe von binären Formen auffassen; sie sind vornehmlich vom Typus

$$f(x, y, z, w) = ax^2 + by^2 + cz^2 + dw^2 .$$

Diese Auswahl entspricht der verwendeten Beweismethode; die gegebene Zahl n wird in zwei Summanden zerlegt und jeder Summand durch die binäre Teilform dargestellt, wobei die bekannten Darstellungsgesetze binärer Formen verwendet werden können, also:

$$f(x, y, z, w) = f'(x, y) + f''(z, w) = n' + n'' = n .$$

Zur Bewältigung dieses Kalküls hat Liouville eigene Zerlegungsformeln, seine «formules générales qui peuvent être utiles dans la théorie des nombres» gefunden. Leider aber hat er die meisten Resultate, insbesondere diese Formeln, ohne Beweise veröffentlicht. Einerseits erwähnt er, daß alle seine Formeln aus der Theorie der elliptischen Funktionen abgeleitet werden können, anderseits betont er ausdrücklich, daß man zum Beweis nur die elementarsten Prinzipien der Algebra zu verwenden habe.

Tatsächlich hat man seither die meisten dieser Formeln elementar beweisen können. Auch hat Pepin [5], mittels dieser Formeln viele Resultate Liouvilles nachträglich abgeleitet. Andere Ergebnisse konnten nur mit der Theorie elliptischer Funktionen erhalten werden. Dazu gehört das Darstellungsgesetz der Form

$$F = x^2 + y^2 + z^2 + 5w^2 ,$$

welches in meiner Arbeit verwendet wird. Chapelon [1] beweist dieses Gesetz im Anschluß an die Untersuchung der Transformationsformeln 5. Ordnung der Thetafunktionen[1]).

[1]) Seine in [1] auf S. 102 publizierte Formel (92) ist, nach leichten Umrechnungen, mit der Liouvilleschen Formel identisch.

Erst später wurde die Reduktionstheorie der positiven quaternären Formen (MINKOWSKI, JULIA) entwickelt, welche eine systematische zahlentheoretische Untersuchung gestattet. Der allgemeinen Reduktionstheorie positiver quadratischer Formen ist die Arbeit [7] meines verehrten Lehrers gewidmet; deren Studium ist die Grundlage der vorliegenden Arbeit geworden.

Im ersten Kapitel werden die Methoden der Reduktionstheorie auf den quaternären Fall spezialisiert. Das Darstellungsproblem wird durch den Begriff des Gitters geometrisiert. Von großer Bedeutung ist im quaternären Fall, mit Ausnahme der einzigen Formenklasse mit Diskriminante $D = 4$, die Möglichkeit der Reduktion nach sukzessiven Minima, d.h. nach kleinstmöglichen Basisvektoren im Sinne der durch die Formenklasse im Gitter induzierten euklidischen Metrik.

Ferner enthält das Kapitel die notwendigen und hinreichenden Bedingungen für Diskriminantenzahlen.

Im zweiten Kapitel werden die Methoden des ersten Kapitels auf die Formen mit Diskriminante $D = 5$ angewendet, der kleinsten Diskriminante, die keine Quadratzahl ist. (Denn im Falle einer Quadratzahl, aber auch nur dann, kann die Formenklasse durch Anwendung der Idealtheorie auf verallgemeinerte Quaternionenalgebren untersucht werden.[2])

Diese Anwendung führt mühelos zu den reduzierten Formen und zur Kenntnis aller Transformationen, welche reduzierte in reduzierte Formen überführen. Es zeigt sich, daß zu $D = 5$ eine einzige, zweiseitige Klasse existiert.

Im dritten Kapitel wird das Darstellungsproblem für die Formenklasse $D = 5$ gelöst. Dabei ergeben sich einfache Darstellungssätze sowohl für beliebige wie auch für teilerfremde Darstellungen; im ersten Fall tritt eine gewisse Teilersumme, im zweiten Fall ein gewisses Primzahlprodukt auf. Beide Funktionen, die durch EISENSTEIN und LIOUVILLE gefunden wurden, können sukzessive ineinander umgeformt werden. Zum Beweis der Darstellungssätze wird über die Summe von Quadraten eine Relation zur LIOUVILLEschen Form F hergestellt.

In den Ergänzungen werden noch andere Beispiele einklassiger Diskriminanten erwähnt. Man darf vermuten, daß dabei im Darstellungsgesetz stets eine gewisse, von der Diskriminante abhängige Teilersumme auftritt; diese Funktion steht in Beziehung zur Theorie der quadratischen Reste modulo der Diskriminante D.

---

[2]) H. GROSS, Darstellungsanzahlen von quaternären quadratischen Stammformen mit quadratischer Diskriminante. Comment. Math. Helv. 34 (1960), 198–221.

1. KAPITEL

Grundlagen

Der reelle, vierdimensionale Vektorraum E_4 mit Basisvektoren $\vec{e}_1, \vec{e}_2, \vec{e}_3, \vec{e}_4$ kann mittels einer positiv definiten, quaternären quadratischen Form f *metrisiert* werden. Eine solche Form wird in dieser Arbeit kurz als positive quaternäre Form bezeichnet; sie hat die Gestalt

$$f = f(x_1, x_2, x_3, x_4) = \sum_{i,k=1}^{4} g_{ik} x_i x_k$$

mit Variabeln x_i und reellen, symmetrischen Koeffizienten $g_{ik} = g_{ki}$. Ich schreibe dafür auch

$$f = f(x, y, z, w) = ax^2 + by^2 + cz^2 + dw^2 + exy + fxz + gxw + hyz + kyw + lzw\,, \tag{1}$$

indem offenbar in dieser nicht-symmetrischen Darstellung die Variabeln mit x, y, z, w bezeichnet sind und

$g_{11} = a, g_{22} = b, g_{33} = c, g_{44} = d, 2g_{12} = e, 2g_{13} = f, 2g_{14} = g, 2g_{23} = h, 2g_{24} = k, 2g_{34} = l$ gesetzt wird.

Ist nun $\vec{a} = \sum_i a_i \vec{e}_i$ ein beliebiger Vektor des E_4, so definiert man die *Norm* von $\vec{a}$: $N(\vec{a}) = f(a_1, a_2, a_3, a_4) \geq 0$ und die *Länge* von $\vec{a}$: $|\vec{a}| = \sqrt{N(\vec{a})}$.

Mit der f zugeordneten Bilinearform $f(x_i, y_i) = \sum_{i,k=1}^{4} g_{ik} x_i y_k$ erklärt man das *Skalarprodukt* zweier Vektoren $\vec{a} = \sum_i a_i \vec{e}_i$, $\vec{b} = \sum_i b_i \vec{e}_i$:

$$(\vec{a}\,, \vec{b}) = \sum_{i,k} g_{ik} a_i b_k .$$

Bezeichnet ferner $G = (g_{ik})$ die Koeffizientenmatrix von f, $|G|$ ihre Determinante, so heiße die reelle Zahl

$$D = 16 \cdot |G|$$

Diskriminante der Form f.

Bilden die Vektoren $\vec{e}_i'$ eine neue Basis des E_4, so bestehen die Transformationsgleichungen:

$$\vec{e}_k' = \sum_i t_{ik} \vec{e}_i \qquad (k = 1 \ldots 4) \tag{2}$$

$T = (t_{ik})$ = Transformationsmatrix mit $|T| \neq 0$.

Dabei transformieren sich die Vektorkomponenten nach den Gleichungen:

$$x_i = \sum_k t_{ik} x'_k \quad (i = 1 \ldots 4) . \tag{3}$$

Fordert man die *Invarianz der Norm* gegenüber Basistransformationen, so induziert jede solche Transformation vermöge der Gleichungen (3) eine Transformation der Form $f(x_1, x_2, x_3, x_4)$ in eine neue Form $f'(x_1', x_2', x_3', x_4')$.

Um die Änderung der quaternären Form bei solchen Transformationen zu überblicken, kann man die Matrizenrechnung verwenden. Bildet man die Komponentenmatrizen

$$X = \begin{pmatrix} x_1 & 0 & 0 & 0 \\ x_2 & \cdot & \cdot & 0 \\ x_3 & \cdot & \cdot & 0 \\ x_4 & \cdot & \cdot & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} x_1' & 0 & 0 & 0 \\ x_2' & \cdot & \cdot & 0 \\ x_3' & \cdot & \cdot & 0 \\ x_4' & \cdot & \cdot & 0 \end{pmatrix}$$

so sind die Gleichungen (3) äquivalent zur Matrizengleichung:

$$X = T \cdot Y . \tag{4}$$

Bedeutet ferner $\bar{A}$ allgemein die transponierte Matrix von A, so gilt $\overline{A \cdot B} = \bar{B} \cdot \bar{A}$.

Ordnet man nun jeder quaternären Form f die Matrix $\bar{X} G X$ mit $G = (g_{ik}) = \bar{G}$ zu, welche als Element der 1. Zeile und 1. Spalte $\Sigma g_{ik} x_i x_k$ und sonst lauter Nullen enthält, so folgt bei Basistransformation nach (4):

$$f' \longleftrightarrow (\overline{T\,Y})\, G\, (T\,Y) = \bar{Y} (\bar{T}\, G\, T)\, Y .$$

Also hat die transformierte Form als Koeffizientenmatrix:

$$G' = \bar{T}\, G\, T .$$

Die Diskriminante der neuen Form ist

$$D' = 16 \mid G' \mid = 16 \mid \bar{T}\, G\, T \mid = \mid T \mid^2 \cdot 16 \cdot \mid G \mid = \mid T \mid^2 \cdot D , \tag{5}$$

d.h. sie entsteht aus der ursprünglichen Diskriminante durch Multiplikation mit einer Quadratzahl.

Unter den Basistransformationen ist die folgende JACOBI*sche Transformation* von besonderer Wichtigkeit. Sie beruht, nach dem Prinzip der quadratischen Ergänzung, auf der Identität:

$$f(x, y, z, w) \equiv \alpha(x + \alpha_1 y + \alpha_2 z + \alpha_3 w)^2 + \beta(y + \beta_1 z + \beta_2 w)^2 + \gamma(z + \gamma_1 w)^2 + \delta w^2 .$$

Offenbar ist die Form f dann und nur dann *positiv definit*, wenn hierin α, β, γ, δ positive Zahlen sind.

Also existiert die JACOBIsche Transformation

$$\begin{aligned} \xi_1 &= \sqrt{\alpha}\cdot(x + \alpha_1 y + \alpha_2 z + \alpha_3 w) \\ \xi_2 &= \sqrt{\beta}\cdot(y + \beta_1 z + \beta_2 w) \\ \xi_3 &= \sqrt{\gamma}\,(z + \gamma_1 w) \\ \xi_4 &= \sqrt{\delta}\cdot w\,, \end{aligned} \tag{6}$$

welche die Form f in die Form $f' = \xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2$ überführt.

Damit ist gezeigt:

Satz 1: *Jede positive quaternäre Form definiert im E_4 eine euklidische Metrik. Die ξ_i heißen deshalb rechtwinklige Vektorkomponenten.*

Ferner gilt nach (6) für die JACOBIsche Transformation T:

$$|T^{-1}| = |T|^{-1} = \sqrt{\alpha\cdot\beta\cdot\gamma\cdot\delta} \quad \text{und somit nach (5):} \quad D = 16\cdot\alpha\beta\gamma\delta\,,$$

d.h. die Diskriminante D ist notwendig eine positive Zahl. Setzen wir für alles folgende voraus, daß in der Darstellung (1): $f = f(x, y, z, w)$ die Koeffizienten $a, b, \ldots, l$ ganze Zahlen sind (ganzzahlige quaternäre Form), so ist auch ihre Diskriminante

$$D = \begin{vmatrix} 2a & e & f & g \\ e & 2b & h & k \\ f & h & 2c & l \\ g & k & l & 2d \end{vmatrix} \tag{7}$$

stets eine ganze Zahl.

Berechnet man D nach (7) und schreibt man den Ausdruck modulo 4, so folgt die Kongruenz:

$$D \equiv (el + fk + gh)^2 \bmod 4\,, \text{ d.h.}$$

Satz 2. *Die Diskriminante D einer ganzzahligen positiven quaternären Form ist eine positive ganze Zahl, die modulo 4 kongruent 0 oder 1 ist.*

Hievon gilt auch die Umkehrung

Satz 3. *Zu jeder positiven ganzen Zahl $D > 1$, welche kongruent 0 oder 1 modulo 4 ist, existiert stets eine ganzzahlige positive quaternäre Form.*

Zum *Beweis* zeige ich die Existenz einer positiven quaternären Form, in der mindestens die Koeffizienten f und g Null sind, also

$$\begin{aligned} &ax^2 + by^2 + cz^2 + dw^2 + exy + hyz + kyw + lzw \\ &= \alpha(x + \alpha_1 y)^2 + \beta(y + \beta_1 z + \beta_2 w)^2 + \gamma(z + \gamma_1 w)^2 + \delta w^2\,. \end{aligned}$$

Ihre Diskriminante hat, wie leicht zu verifizieren, die Gestalt

$$D = (4ab - e^2)\cdot(4cd - l^2) - 4a(dh^2 - lhk + ck^2) \tag{8}$$

und die Koeffizienten $\alpha, \beta, \gamma, \delta$ haben die Werte

$$\alpha = a \quad \beta = \frac{4ab - e^2}{4a} \qquad \gamma = \frac{(4ab - e^2)\,c - ah^2}{4ab - e^2}$$

$$\delta = \frac{D}{4\,[(4ab - e^2)\,c - ah^2]}$$

Also ist diese Form genau dann positiv, wenn die Bedingungen

$$a > 0\,, \quad 4ab - e^2 > 0\,, \quad (4ab - e^2)c - ah^2 > 0 \tag{9}$$

erfüllt sind.

Somit ist zu zeigen, daß jede zulässige Zahl D unter Berücksichtigung der Bedingungen (9) auf die Gestalt (8) gebracht werden kann.

1) *D gerade*

Als Spezialfälle von (8) erhält man für
$a = b = c = 1,\ e = 1,\ l = 0,\ h = 1,\ k = 0 : D = 8d$, also
$x^2 + y^2 + z^2 + dw^2 + xy + yz = (x + \frac{1}{2}y)^2 + \frac{3}{4}(y + \frac{2}{3}z)^2 + \frac{2}{3}z^2 + dw^2$
und für
$a = b = c = 1,\ e = 1,\ l = 0,\ h = 1,\ k = 1 : D = 8d - 4$,
also
$x^2 + y^2 + z^2 + dw^2 + xy + yz + yw = (x + \frac{1}{2}y)^2 + \frac{3}{4}(y + \frac{2}{3}z + \frac{2}{3}w)^2$
$+ \frac{2}{3}(z - \frac{1}{2}w)^2 + (d - \frac{1}{2})w^2$.
Somit gibt es zu $D \equiv 0 \bmod 4$ stets positive quaternäre Formen.

2) *D ungerade*

Aus (8) wird für

$$a = b = c = 1,\ e = 1,\ l = 1,\ h = 1,\ k = 0 : D = 8d - 3,$$

also

$$x^2 + y^2 + z^2 + dw^2 + xy + yz + zw =$$
$$(x + \tfrac{1}{2}y)^2 + \tfrac{3}{4}(y + \tfrac{2}{3}z)^2 + \tfrac{2}{3}(z + \tfrac{3}{4}w)^2 + (d - \tfrac{3}{8})w^2\,. \tag{10}$$

Während damit das Problem bei $D \equiv 5 \bmod 8$ gelöst ist, finde ich keine solche Formel bei $D \equiv 1 \bmod 8$.

Um den Satz allgemein bei ungeradem D zu beweisen, unterscheide ich folgende drei Fälle:

1. Fall. D besitzt eine Zerlegung vom Typus $D = A \cdot B$ mit $A \equiv B \equiv 3$ modulo 4.

Jetzt ist D in der Form $D = (4ab - e^2)\,(4cd - l^2)$ darstellbar, d.h. es existiert eine positive quaternäre Form, welche die Summe zweier binärer Formen ist. Man vergleiche Formel (8) bei $h = 0,\ k = 0$.

Beispiel: $D = 33 = 3 \cdot 11 = (4 \cdot 1 - 1)(4 \cdot 3 - 1)$.

$f = x^2 + y^2 + xy + z^2 + 3w^2 + zw$.

2. Fall. D besitzt keine Zerlegung vom Typus $D = A \cdot B$ mit $A \equiv B \equiv 3$ modulo 4 und ist keine Quadratzahl.

Nach der Theorie der quadratischen Reste gibt es eine Primzahl $p \equiv 3$ mod 4, so daß das JACOBI-Symbol

$$\left(\frac{-D}{p}\right) = +1, \text{ d.h. } (-D) \text{ quadratischer Rest mod } p \text{ ist.}$$

Denn nach Voraussetzung ist $D = N^2 \cdot E$, wo E quadratfrei ist. Sei q ein Primfaktor von E und $E = B \cdot q$, wobei q und alle Primzahlen von B kongruent 1 modulo 4 sind. Dann gibt es ein m mit

$$\left(\frac{m}{q}\right) = -1;\ m \equiv 1 \bmod B;\ m \equiv 3 \bmod 4.$$

In derselben Restklasse (mod $4 \cdot E$) existiert eine Primzahl p, die nicht in N aufgeht.

Nun folgt unter Verwendung des quadratischen Reziprozitätsgesetzes

$$\left(\frac{-D}{p}\right) = \left(\frac{-E}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{B}{p}\right)\left(\frac{q}{p}\right) = -\left(\frac{p}{B}\right)\left(\frac{p}{q}\right) = -\left(\frac{m}{B}\right)\left(\frac{m}{q}\right) = +1.$$

Damit ist die Kongruenz $D + t^2 \equiv 0 \bmod p$ lösbar; unter den Lösungen gibt es sicher eine gerade $t = 2 \cdot A$, so daß eine Darstellung

$$D + 4 \cdot A^2 = (4b - e^2)(4d - l^2)$$

möglich ist. Diese Darstellung entspricht Formel (8), wenn man dort $a = c = 1$, $h = 0$, $k = A$ setzt, wobei offenbar (9) erfüllt werden kann q.e.d.

Beispiel: $D = 1009 \cdot p = 11$; die Kongruenz $D + t^2 \equiv 0 \bmod 11$ hat die Lösung $t = 6 = 2 \cdot A$.

Aus $1009 + 36 = 11 \cdot 95$ folgt

$f = x^2 + 3y^2 + z^2 + 24w^2 + xy + 3yw + zw$.

3. Fall. D besitzt keine Zerlegung vom Typus $D = A \cdot B$ mit $A \equiv B \equiv 3$ modulo 4, ist aber eine Quadratzahl.

Es ist $D = u^{2v}$, wobei $u \equiv 1 \bmod 4$ und keine Quadratzahl ist. Somit ist, wie soeben beim 2. Fall gezeigt wurde, die Zahl u^{2v-1} wie folgt darstellbar:

$$u^{2v-1} + 4 \cdot A^2 = (4b - e^2)(4r - s^2).$$

Daraus folgt

$$u^{2v} \equiv (u^{2v-1} + 4 \cdot A^2)u - 4 \cdot A^2 u = (4b - e^2)(4r - s^2)u - 4 \cdot A^2 u,$$

wobei sowohl $4b - e^2 \equiv 3 \bmod 4$ als auch $(4r - s^2)\,u \equiv 3 \bmod 4$ sind.

Nun gibt es eine binäre Form

$$f(h, k) = dh^2 - lhk + uk^2$$

mit Diskriminante $4ud - l^2 = (4r - s^2)u$, was damit identisch ist, daß $f(h, k)$ die Zahl u darstellt. Man setze nämlich für die zu bestimmenden Zahlen l, d:

$$l = u,\ d = \frac{4r - s^2 + u}{4} = \text{ganze Zahl wegen } s \text{ ungerade, } u \equiv 1 \text{ modulo } 4.$$

Daraus folgt

$$u^{2v} = (4b - e^2)(4ud - l^2) - 4 \cdot A^2 u\,,$$

also die Darstellung (8) bei $a = 1, c = u, h = 0, k = A$ q.e.d.

Beispiel: $D = 289 = 17^2$. $u = 17, p = 3$; die Kongruenz $u + t^2 \equiv 0 \bmod 3$ hat die Lösung $t = 2 = 2 \cdot A$. $D = (17 + 4) \cdot 17 - 4 \cdot 17 = 3 \cdot 7 \cdot 17 - 4 \cdot 17$. Also $l = 17$, $d = 6$, d.h.

$f(h, k) = 6h^2 - 17hk + 17k^2$ und

$f = x^2 + y^2 + 17z^2 + 6w^2 + xy + yw + 17zw$.

Die zahlentheoretische Untersuchung einer positiven quaternären Form wird geometrisiert durch den Begriff des *Gitters*, d.h. der Gesamtheit aller ganzzahligen Linearkombinationen von vier linear unabhängigen Vektoren $\vec{e}_i$ des E_4.

Die ganzzahlige positive Form f definiert im Gitter eine euklidische Metrik mit ganzzahligen Normen. Die Existenz eines Gittervektors

$$\vec{s} = x\vec{e}_1 + y\vec{e}_2 + z\vec{e}_3 + w\vec{e}_4$$

mit Norm $N \geq 0$ bedeutet, daß die Zahl N durch die Form f dargestellt wird. Bei eigentlicher Darstellung, $ggT(x, y, z, w) = 1$, heißt der Gittervektor *primitiv*.

Für das folgende betrachten wir nur noch jene Basistransformationen, bei denen die neuen Basisvektoren wieder eine Gitterbasis bilden. Es gilt:

Die Transformation $T = (t_{ik})$ ist dann und nur dann eine Transformation der Gitterbasis, wenn T eine *unimodulare Substitution* ist, d.h. die

t_{ik} ganze Zahlen sind und $|T| = +1$ oder -1 ist.

Die durch eine solche Matrix T nach (3) transformierte Form f' heißt zur ursprünglichen Form f *äquivalent*. Bei der feineren Einteilung nach *eigentlicher Äquivalenz* wird nur die Transformierbarkeit mit $|T| = +1$ zugelassen.

Weil die Relation «f' äquivalent f» reflexiv, symmetrisch und transitiv ist, definiert sie eine Einteilung der positiven quaternären Formen in *Klassen äquivalenter Formen*. Dabei ist nach (5) die Gleichheit der Diskriminante eine notwendige Bedingung der Äquivalenz.

Um für diese Klasseneinteilung ein Repräsentantensystem zu erhalten, definiert man die *reduzierte* Form.

Eine positive quaternäre Form heißt reduziert, wenn die unendlich vielen Ungleichungen

$$f_{kk} \leq f(s_1, s_2, s_3, s_4) \quad k = 1 \ldots 4 \tag{11}$$

für alle Systeme ganzer Zahlen s_i mit $ggT(s_k \ldots, s_4) = 1$ erfüllt sind.

Der reduzierten Form entspricht in geometrischer Formulierung die *reduzierte Gitterbasis*.

Gehört nämlich zur Gitterbasis $\vec{e}_i$ als metrische Grundform die reduzierte Form f, so heißt die Basis reduziert. Nach (11) besagt dies:

$$f_{kk} = N(\vec{e}_k) \leq f(s_1, s_2, s_3, s_4) = N(\vec{s}) \text{ mit } ggT(s_k, \ldots, s_4) = 1$$

d.h. die Gitterbasis $\vec{e}_i$ ist, geometrisch formuliert, reduziert, wenn

a) $\vec{e}_1$ kürzester primitiver Gittervektor,

b) $\vec{e}_2$ kürzester unter allen Gittervektoren $\vec{s} = \sum_{i=1}^{4} s_i \cdot \vec{e}_i$ mit $ggT(s_2, s_3, s_4) = 1$,

c) $\vec{e}_3$ kürzester unter allen Gittervektoren $\vec{s} = \sum_{i=1}^{4} s_i \cdot \vec{e}_i$ mit $ggT(s_3, s_4) = 1$,

d) $\vec{e}_4$ kürzester unter allen Gittervektoren $\vec{s} = \sum_{i=1}^{4} s_i \cdot \vec{e}_i$ mit $s_4 = \pm 1$ ist. (12)

Die Existenz einer reduzierten Gitterbasis ist aus folgenden zwei Gründen gesichert:

1) In jeder nicht leeren Menge von Gittervektoren, deren Normen ja eine Teilmenge der natürlichen Zahlen bilden, gibt es (mindestens) einen kürzesten Vektor.

2) Jedes System von Gittervektoren, das zu einer Gitterbasis ergänzt werden kann, heißt *primitives Vektorsystem*. Nun gilt folgender Hilfssatz[3]):

Der Gittervektor $\vec{s} = \sum_{i=1}^{4} s_i \vec{e}_i$ bildet mit den Gittervektoren $\vec{e}_1, \ldots, \vec{e}_{k-1}$ dann und nur dann ein primitives Vektorsystem, wenn der $ggT(s_k, \ldots, s_4) = 1$ ist.

Weil somit jedes Gitter in bezug auf jede gegebene Metrik eine reduzierte Gitterbasis besitzt, hat jede quaternäre Form eine äquivalente reduzierte Form.

Die arithmetischen Bedingungen (11) für eine reduzierte Form werden wesentlich vereinfacht durch den von MINKOWSKI bewiesenen

---

[3]) Für die Begründung aller hier nicht bewiesenen Sätze sei nochmals auf die Arbeit von B. L. VAN DER WAERDEN [7]: «Die Reduktionstheorie der positiven quadratischen Formen» verwiesen.

Satz 4. (Erster Endlichkeitssatz): *Die unendlich vielen Ungleichungen* (11) *sind bereits erfüllt, wenn man unter ihnen nur jene endlich vielen berücksichtigt, die man erhält, wenn man für s_i die Zahlen* $0, +1, -1$ *einsetzt.*

Damit erhält man für die quaternäre Form (1) folgende *endlich viele Reduktionsbedingungen:*

$$\begin{gathered} a \leq b \leq c \leq d \\ |e| \leq a\,,\ |f| \leq a\,,\ |g| \leq a\,, \\ |h| \leq b\,,\ |k| \leq b\,, \\ |l| \leq c \end{gathered} \tag{13}$$

$$\begin{array}{llll} -e-f-h \leq a+b & & -e-g-k \leq a+b \\ -e+f+h \leq a+b & & -e+g+k \leq a+b \\ +e-f+h \leq a+b & & +e-g+k \leq a+b \\ +e+f-h \leq a+b & & +e+g-k \leq a+b \end{array}$$

$$\begin{array}{llll} -f-g-l \leq a+c & & -h-k-l \leq b+c \\ -f+g+l \leq a+c & & -h+k+l \leq b+c \\ +f-g+l \leq a+c & & +h-k+l \leq b+c \\ +f+g-l \leq a+c & & +h+k-l \leq b+c \end{array}$$

$$\begin{array}{l} -e-f-g-h-k-l \leq a+b+c \\ -e+f-g+h-k+l \leq a+b+c \\ -e+f+g+h+k-l \leq a+b+c \\ -e-f+g-h+k+l \leq a+b+c \\ +e-f-g+h+k-l \leq a+b+c \\ +e+f-g-h+k+l \leq a+b+c \\ +e+f+g-h-k-l \leq a+b+c \\ +e-f+g+h-k+l \leq a+b+c \end{array}$$

Die quaternäre Form heißt *eigentlich reduziert*, wenn in allen diesen Ungleichungen nur das Zeichen $<$ steht.

Ferner entnehme ich der Theorie der positiven quadratischen Formen die *fundamentale Ungleichung* der Reduktionstheorie, welche speziell für quaternäre Formen besagt:

Satz 5. *Ist f eine reduzierte quaternäre Form mit Diskriminante D, so besteht zwischen ihren Diagonalkoeffizienten a, b, c, d und D die Ungleichung:*

$$4\,a\,b\,c\,d \leqq D$$

(Bei ganzzahligen Koeff. ist also $D \geq 4$)

Als wichtige *Folgerung* erhält man, wenn man noch die Reduktionsbedingungen Satz 4 (13) berücksichtigt:

Zu gegebener, fester Diskriminante D gibt es nur endlich viele Klassen; ihre Anzahl heißt *Klassenzahl* zu dieser Diskriminante.

Denn bei festem D sind alle ganzzahligen Koeffizienten von f beschränkt.

In derselben Formenklasse können mehrere, jedoch nur endlich viele reduzierte Formen auftreten. Damit stellt sich das Problem,
alle jene unimodularen Substitutionen T zu bestimmen, welche eine reduzierte in eine äquivalente reduzierte Form transformieren. Ist dabei die transformierte mit der ursprünglichen Form identisch, so heißt die Substitution *automorph*.

Dazu beweist man in der allgemeinen Theorie:

Satz 6. (Zweiter Endlichkeitssatz): *Es gibt nur endlich viele unimodulare Substitutionen, welche eine reduzierte quaternäre Form in eine äquivalente reduzierte Form überführen.*

Zu diesen Transformationen gehören stets die $2^4 = 16$ *Umkehrtransformationen*

$$x_i' = \pm x_i \quad (i = 1 \ldots 4) .$$

Bei einer eigentlich reduzierten Form sind dies alle Transformationen, weil jeder Basisvektor der reduzierten Basis bis auf $\pm$ eindeutig bestimmt ist.

Bei einer uneigentlich reduzierten Form (d.h. in gewissen Reduktionsbedingungen gilt das Gleichheitszeichen) gibt es außer den Umkehrtransformationen mindestens noch eine weitere Transformation T, welche f in eine äquivalente reduzierte Form überführt.

Ist z.B. $a = b = c = d$, so existieren außerdem die $4! = 24$ *Vertauschungstransformationen*, bei denen die Transformation nur in einer Permutation der Variabeln besteht.

Für meine Arbeit ist von besonderer Wichtigkeit, daß bei positiven quaternären Formen der Begriff der reduzierten Gitterbasis etwas weiter als (12) gefaßt werden kann. Im vierdimensionalen Gitter mit metrischer Grundform f versteht man unter *sukzessiven Minimalvektoren*
vier Gittervektoren $\vec{s}_1, \vec{s}_2, \vec{s}_3, \vec{s}_4$ mit folgenden Eigenschaften:

a′) $\vec{s}_1$ ist ein kürzester Gittervektor $\neq \vec{0}$,

b′) $\vec{s}_2$ ist ein kürzester, von $\vec{s}_1$ linear unabhängiger Gittervektor,

c′) $\vec{s}_3$ ist ein kürzester, von $\vec{s}_1$, $\vec{s}_2$ linear unabhängiger Gittervektor,

d′) $\vec{s}_4$ ist ein kürzester, von $\vec{s}_1$, $\vec{s}_2$, $\vec{s}_3$ linear unabhängiger Gittervektor.

Obschon mehrere Systeme sukzessiver Minimalvektoren bestehen, sind ihre Normen N_1, N_2, N_3, N_4, die sogenannten
sukzessiven Minima, eindeutig bestimmt.

Während bei positiven quadratischen Formen in mehr als vier Variabeln, wo diese Begriffe ganz analog gebildet werden, die sukzessiven Minimalvektoren wohl eine Raumbasis, aber keine Gitterbasis bilden, gilt im quaternären Falle mit Ausnahme der einzigen Formenklasse mit Diskriminante $D = 4$:

Satz 7. *In jedem vierdimensionalen Gitter mit Diskriminante $D > 4$ bildet jedes System von vier sukzessiven Minimalvektoren eine reduzierte Gitterbasis. In der zu dieser Basis gehörenden reduzierten quaternären Form f gilt*

$$N_k = f_{kk} \quad (k = 1 \ldots 4) .$$

2. KAPITEL

Die Formenklasse mit Diskriminante $D = 5$

In dieser Arbeit wird der Fall der Diskriminante $D = 5$ eingehend behandelt. Das Ziel dieses Kapitels besteht im Nachweis, daß zu dieser Diskriminante eine einzige *zweiseitige Formenklasse* existiert, deren Formen also zugleich eigentlich und uneigentlich äquivalent sind. Dabei werden die allgemeinen Methoden des 1. Kapitels, insbesondere Satz 7, angewendet.

Nach Formel (10) findet man für $d = 1$ als *reduzierte* Form mit $D = 5$:

$$x^2 + y^2 + z^2 + w^2 + xy + yz + zw .$$

Um für alles folgende möglichst einfache Verhältnisse zu haben, verwende ich jene Form, die daraus durch die gerade Permutation $P = \begin{pmatrix} x\,y\,z\,w \\ y\,z\,x\,w \end{pmatrix}$ entsteht:

$$\begin{aligned} f &= x^2 + y^2 + z^2 + w^2 + xz + xw + yz \\ &\equiv (x + \tfrac{1}{2}z + \tfrac{1}{2}w)^2 + (y + \tfrac{1}{2}z)^2 + \tfrac{1}{2}(z - \tfrac{1}{2}w)^2 + \tfrac{5}{8}w^2 . \end{aligned} \qquad (14)$$

Gleichzeitig betrachte ich f als metrische Grundform des Gitters mit (reduzierter) Basis

$$\vec{e}_1 = (1, 0, 0, 0) \quad \vec{e}_2 = (0, 1, 0, 0) \quad \vec{e}_3 = (0, 0, 1, 0) \quad \vec{e}_4 = (0, 0, 0, 1).$$

Neben den Komponenten in bezug auf die Basis $\vec{e}_i$ verwende ich die durch die JACOBIsche Transformation (14) gelieferten *rechtwinkligen Komponenten:*

$$\xi_1 = x + \tfrac{1}{2}z + \tfrac{1}{2}w \quad \xi_2 = y + \tfrac{1}{2}z \quad \xi_3 = \frac{\sqrt{2}}{2}(z - \tfrac{1}{2}w) \quad \xi_4 = \frac{\sqrt{10}}{4}w .$$

Vektorkomponenten bezüglich der $\vec{e}_i$ werden in runden, rechtwinklige Komponenten in geschweiften Klammern geschrieben, also z.B.:

$$\vec{e}_1 = (1, 0, 0, 0) = \{1, 0, 0, 0\}$$
$$\vec{e}_2 = (0, 1, 0, 0) = \{0, 1, 0, 0\}$$
$$\vec{e}_3 = (0, 0, 1, 0) = \left\{\tfrac{1}{2}, \tfrac{1}{2}, \frac{\sqrt{2}}{2}, 0\right\}$$
$$\vec{e}_4 = (0, 0, 0, 1) = \left\{\tfrac{1}{2}, 0, \frac{-\sqrt{2}}{2}, \frac{\sqrt{10}}{4}\right\}$$

Wegen $a = b = c = d = 1$ haben alle sukzessiven Minima den Wert eins:

$$N_1 = N_2 = N_3 = N_4 = 1 .$$

Man erhält deshalb die Gesamtheit der Minimalvektoren

$$\vec{s} = x\vec{e}_1 + y\vec{e}_2 + z\vec{e}_3 + w\vec{e}_4$$

als ganzzahlige Lösungen der Gleichung Norm $\vec{s} = f(x, y, z, w) = 1$. Die JACOBIsche Darstellung (14) liefert dafür die Bedingung:

$$8f = 2(2x + z + w)^2 + 2(2y + z)^2 + (2z - w)^2 + 5w^2 = 8 .$$

Danach besitzt das Gitter die folgenden *20 Minimalvektoren*, alle mit Länge eins:

$$1) \pm(1, 0, 0, 0) = \pm\{1, 0, 0, 0\}$$
$$2) \pm(0, 1, 0, 0) = \pm\{0, 1, 0, 0\}$$
$$3) \pm(-1, 0, 1, 1) = \pm\left\{0, \tfrac{1}{2}, \frac{\sqrt{2}}{4}, \frac{\sqrt{10}}{4}\right\}$$
$$4) \pm(1, 1,-1,-1) = \pm\left\{0, \tfrac{1}{2}, \frac{-\sqrt{2}}{4}, \frac{-\sqrt{10}}{4}\right\}$$
$$5) \pm(0, 0, 0, 1) = \pm\left\{\tfrac{1}{2}, 0, \frac{-\sqrt{2}}{4}, \frac{\sqrt{10}}{4}\right\}$$
$$6) \pm(1, 0, 0,-1) = \pm\left\{\tfrac{1}{2}, 0, \frac{\sqrt{2}}{4}, \frac{-\sqrt{10}}{4}\right\}$$
$$7) \pm(0, 0, 1, 0) = \pm\left\{\tfrac{1}{2}, \tfrac{1}{2}, \frac{\sqrt{2}}{2}, 0\right\}$$
$$8) \pm(0,-1, 1, 0) = \pm\left\{\tfrac{1}{2},-\tfrac{1}{2}, \frac{\sqrt{2}}{2}, 0\right\}$$
$$9) \pm(1, 1,-1, 0) = \pm\left\{\tfrac{1}{2}, \tfrac{1}{2}, \frac{-\sqrt{2}}{2}, 0\right\}$$
$$10) \pm(1, 0,-1, 0) = \pm\left\{\tfrac{1}{2},-\tfrac{1}{2}, \frac{-\sqrt{2}}{2}, 0\right\}$$

Die *Skalarprodukte* zweier verschiedener Minimalvektoren sind in der nachstehenden Tabelle zusammengestellt. Dabei bedeutet z.B.

12 das Skalarprodukt des +Vektors 1) mit dem +Vektor 2).

s = *Skalarprodukt*

	s		s		s		s		s
1 2	0	2 1	0	3 1	0	4 1	0	5 1	$\frac{1}{2}$
1 3	0	2 3	$\frac{1}{2}$	3 2	$\frac{1}{2}$	4 2	$\frac{1}{2}$	5 2	0
1 4	0	2 4	$\frac{1}{2}$	3 4	$-\frac{1}{2}$	4 3	$-\frac{1}{2}$	5 3	$\frac{1}{2}$
1 5	$\frac{1}{2}$	2 5	0	3 5	$\frac{1}{2}$	4 5	$-\frac{1}{2}$	5 4	$-\frac{1}{2}$
1 6	$\frac{1}{2}$	2 6	0	3 6	$-\frac{1}{2}$	4 6	$\frac{1}{2}$	5 6	$-\frac{1}{2}$
1 7	$\frac{1}{2}$	2 7	$\frac{1}{2}$	3 7	$\frac{1}{2}$	4 7	0	5 7	0
1 8	$\frac{1}{2}$	2 8	$-\frac{1}{2}$	3 8	0	4 8	$-\frac{1}{2}$	5 8	0
1 9	$\frac{1}{2}$	2 9	$\frac{1}{2}$	3 9	0	4 9	$\frac{1}{2}$	5 9	$\frac{1}{2}$
1 10	$\frac{1}{2}$	2 10	$-\frac{1}{2}$	3 10	$-\frac{1}{2}$	4 10	0	5 10	$\frac{1}{2}$

(15)

	s		s		s		s		s
6 1	$\frac{1}{2}$	7 1	$\frac{1}{2}$	8 1	$\frac{1}{2}$	9 1	$\frac{1}{2}$	10 1	$\frac{1}{2}$
6 2	0	7 2	$\frac{1}{2}$	8 2	$-\frac{1}{2}$	9 2	$\frac{1}{2}$	10 2	$-\frac{1}{2}$
6 3	$-\frac{1}{2}$	7 3	$\frac{1}{2}$	8 3	0	9 3	0	10 3	$-\frac{1}{2}$
6 4	$\frac{1}{2}$	7 4	0	8 4	$-\frac{1}{2}$	9 4	$\frac{1}{2}$	10 4	0
6 5	$-\frac{1}{2}$	7 5	0	8 5	0	9 5	$\frac{1}{2}$	10 5	$\frac{1}{2}$
6 7	$\frac{1}{2}$	7 6	$\frac{1}{2}$	8 6	$\frac{1}{2}$	9 6	0	10 6	0
6 8	$\frac{1}{2}$	7 8	$\frac{1}{2}$	8 7	$\frac{1}{2}$	9 7	0	10 7	$-\frac{1}{2}$
6 9	0	7 9	0	8 9	$-\frac{1}{2}$	9 8	$-\frac{1}{2}$	10 8	0
6 10	0	7 10	$-\frac{1}{2}$	8 10	0	9 10	$\frac{1}{2}$	10 9	$\frac{1}{2}$

Die Kenntnis der Minimalvektoren gestattet nach Satz 7 (Kap. 1) folgendes elementares *Verfahren:*

Je vier linear unabhängige Minimalvektoren bilden eine reduzierte Gitterbasis, und umgekehrt besteht jede reduzierte Basis aus je vier lin. unabh. Minimalvektoren. Die zur reduzierten Basis gehörende metrische Fundamentalform f' ist

reduziert und zur Form f äquivalent.

Gleichzeitig liefert die Transformationsmatrix eine unimodulare Transformation T, welche die Form f in die äquivalente Form f' transformiert.

Dabei bestehen zwei Fälle:

1) $f' = f$. *T ist eine automorphe Substitution.*

2) $f' \neq f$. *f' ist eine weitere reduzierte Form derselben Formenklasse.*

In Übereinstimmung mit Satz 6 gibt es nur endlich viele Transformationen T der beschriebenen Art.

1) *Automorphe Substitutionen*

Die Gesamtheit der automorphen Substitutionen bildet eine *endliche Gruppe*, weil offenbar das Produkt zweier solcher Substitutionen wieder automorph ist.

Von den *Umkehrtransformationen* sind einzig E = Einheitstransformation und $-E$ automorph; von den *Vertauschungstransformationen* ist außer E die Transformation V, welche die Basisvektoren 1, 3 und die Basisvektoren 2, 4 vertauscht, automorph:

$$\begin{aligned} x' &= z \\ y' &= w \\ z' &= x \\ w' &= y \end{aligned} \qquad V = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad \begin{aligned} |V| &= +1 \\ V^2 &= E \\ V(f) &= f\,. \end{aligned}$$

Jede automorphe Substitution A gibt Anlaß zu den folgenden vier automorphen Substitutionen, wobei die Gesamtheit der Basisvektoren unverändert bleibt:

$$E\,A = A\,, \quad -E\,A = -A\,, \quad A\,V\,, \quad -A\,V\,. \tag{16}$$

Im allgemeinen ergeben je vier Minimalvektoren $\vec{s}_1$, $\vec{s}_2$, $\vec{s}_3$, $\vec{s}_4$ mit den Skalarprodukten

$$\vec{s}_1\vec{s}_2 = 0\,, \quad \vec{s}_1\vec{s}_3 = \vec{s}_1\vec{s}_4 = \tfrac{1}{2}\,, \quad \vec{s}_2\vec{s}_3 = \tfrac{1}{2}\,, \quad \vec{s}_2\vec{s}_4 = 0\,, \quad \vec{s}_3\vec{s}_4 = 0\,,$$

eine automorphe Substitution.

Beispiel: Nach Tabelle (15) ist dies für die Minimalvektoren 7, 9, 1, 3 der Fall. Die neue Gitterbasis ist

$$\begin{aligned} \vec{e}_1' &= (\ 0,\ 0,\ \ 1,\ 0) \\ \vec{e}_2' &= (\ 1,\ 1,-1,\ 0) \\ \vec{e}_3' &= (\ 1,\ 0,\ \ 0,\ 0) \\ \vec{e}_4' &= (-1,\ 0,\ \ 1,\ 1) \end{aligned}$$

Die Transformationsmatrix $T = (t_{ik})$ enthält nach (2) in der $k$ten Spalte die Komponenten von $\vec{e}_k'$ in bezug auf die Basis $\vec{e}_i$ und hat deshalb die Gestalt:

$$T = \begin{pmatrix} 0 & 1 & 1 & -1 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{aligned} x' &= y + z - w \\ y' &= y \\ z' &= x - y + w \\ w' &= w \end{aligned}$$

In der Tat ist

$$f(x', y', z', w') = x^2 + y^2 + z^2 + w^2 + xz + xw + yz = f\,.$$

Weil die Determinante $|T|$ den Wert -1 hat, folgt, daß die durch f definierte Formenklasse *zweiseitig* ist. Denn ist f' eine quaternäre Form, die aus f durch unimodulare Transformation G entsteht:

$$f' = G(f), \text{ so gilt auch } f' = GT(f);$$

von den beiden Transformationen ist die eine eigentlich, die andere uneigentlich unimodular.

Ferner gilt $T^2 = E$; die Zerlegung der automorphen Gruppe in Restklassen nach der Untergruppe $\{T, T^2 = E\}$ zeigt, daß in der Gruppe *gleich viele* eigentlich als auch uneigentlich automorphe Substitutionen existieren.

Die Transformation T werde symbolisch mit (7, 9, 1, 3) bezeichnet, d.h. die Spaltenvektoren ihrer Matrix sind die Minimalvektoren $+7, +9, +1, +3$ der Tabelle (15). Wenn ich mich derselben symbolischen Schreibweise bediene, besitzt die Form f[4]) folgende automorphe Substitutionen, wobei von den vier Substitutionen (16) nur eine notiert wird:

$(1, 2, 7, 5) = E$	$(7, 9, 1, 3) = T$	(1, 3, 5, 8)	(1, −4, 5, 7)
(1, −3, 6, 9)	(1, 4, 6, 10)	(1, −2, 8, 5)	(1, −4, 8, 10)
(1, 2, 9, 6)	(1, 4, 9, 7)	(1, −2, 10, 6)	(1, −3, 10, 8)
(2, −6, 3, 9)	(2, 5, 3, −8)	(2, −5, 4, 7)	(2, 6, 4, −10)
(2, 1, 7, 4)	(2, 6, 7, 9)	(2, −1, −8, 3)	(2, −6, −8, −10)
(2, 1, 9, 3)	(2, 5, 9, 7)	(2, −1, −10, 4)	(2, −5, −10, −8)
(3, 8, −4, −10)	(3, −9, −4, 7)	(3, 1, 5 2)	(3, 9, 5, 7)
(3, −1, −6, 2)	(3, −8, −6, −10)	(3, 1, 7, −4)	(3, 8, 7, 5)
(3, −1, −10, −4)	(3, −9, −10, −6)	(4, −1, −5, 2)	(4, −10, −5, −8)
(4, 1, 6, 2)	(4, 7, 6, 9)	(4, −1, −8, −3)	(4, −7, −8, −5)
(4, 1, 9, −3)	(4, 10, 9, 6)	(5, −7, −6, 9)	(5, −8, −6, 10)
(5, 2, 9, −6)	(5, −8, 9, 3)	(5, −2, 10, −6)	(5, −7, 10, −4)
(6, 2, 7, −5)	(6, −10, 7, 4)	(6, −2, 8, −5)	(6, −9, 8, −3)
(7, −4, 8, −10)	(7, −9, 8, 3)	(7, −5, −10, 8)	(7, −9, −10, 6)
(8, −5, −9, 7)	(8, −10, −9, 6)	(9, −3, 10, −8)	(9, −7, 10, 4)

Total = 240 automorphe Substitutionen.
Zusammenfassend gilt

Satz 8. Die Formenklasse $\{f\}$ besitzt eine Gruppe von 240 *automorphen Substitutionen*, von denen die eine Hälfte eigentlich, die andere Hälfte uneigentlich unimodular ist.

Die Formenklasse ist somit *zweiseitig*.

---

[4]) Ist T für die Form f automorph, so gilt für $f' = G(f)$: $GTG^{-1}(f') = f'$, das heißt die automorphen Substitutionen von f und f' entsprechen sich eineindeutig.

2. *Reduzierte Formen*

Die aus vier linear unabhängigen Minimalvektoren gebildeten reduzierten Gitterbasen, welche nicht zu automorphen Substitutionen führen, haben als metrische Grundformen neue reduzierte Formen derselben Klasse.

Reduzierte Formen, die durch Umkehr- und Vertauschungstransformationen gebildet werden können und nach Satz 8 zu f in jedem Falle eigentlich äquivalent sind, können in derselben Teilmenge vereinigt werden.

Zur Abkürzung werde $x^2 + y^2 + z^2 + w^2 = Q$ gesetzt.

Teilmenge 1:

Aus der gegebenen Form f entstehen durch Umkehrung und Vertauschung:

$$
\begin{array}{llllllll}
Q & \pm & xz & \pm & xw & \pm & yz & \\
Q & \pm & xz & \pm & yw & \pm & zw & \\
Q & \pm & xz & \pm & yz & \pm & yw & \\
Q & \pm & xz & \pm & xw & \pm & yw & \text{Weil alle acht Vor-} \\
Q & \pm & xw & \pm & yz & \pm & zw & \text{zeichenkombinationen} \quad (17) \\
Q & \pm & xw & \pm & yz & \pm & yw & \text{zulässig sind, besteht} \\
Q & \pm & xy & \pm & yw & \pm & zw & \text{die Teilmenge aus} \\
Q & \pm & xy & \pm & yz & \pm & zw & \\
Q & \pm & xy & \pm & xw & \pm & zw & 12.8 = \textit{96 reduzierten Formen.} \\
Q & \pm & xy & \pm & xw & \pm & yz & \\
Q & \pm & xy & \pm & xz & \pm & zw & \\
Q & \pm & xy & \pm & xz & \pm & yw &
\end{array}
$$

Teilmenge 2:

Zur Gitterbasis (7, 9, 1, 6) gehört nach Tabelle (15) die neue reduzierte Form

$$
\begin{aligned}
f_2 &= x^2 + y^2 + z^2 + w^2 + xz + xw + yz + zw \\
&= (x + \tfrac{1}{2}z + \tfrac{1}{2}w)^2 + (y + \tfrac{1}{2}z)^2 + \tfrac{1}{2}(z + \tfrac{1}{2}w)^2 + \tfrac{5}{8}w^2 .
\end{aligned}
$$

Die eigentlich unimodulare Transformation T, welche f in f_2 transformiert, ist

$$
T = (7, 9, 1, 6) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \qquad \begin{aligned} x' &= y + z + w \\ y' &= y \\ z' &= x - y \\ w' &= -w \end{aligned}
$$

Durch die Umkehrtransformationen, von denen zwei automorph sind, entstehen acht Formen:

$$
\begin{array}{cccccccccc}
Q & + & xz & + & xw & + & yz & + & zw \\
Q & + & xz & - & xw & + & yz & - & zw \\
Q & - & xz & + & xw & - & yz & - & zw \\
Q & + & xz & + & xw & - & yz & + & zw \\
Q & - & xz & - & xw & + & yz & + & zw \\
Q & - & xz & - & xw & - & yz & + & zw \\
Q & + & xz & - & xw & - & yz & - & zw \\
Q & - & xz & + & xw & + & yz & - & zw\,.
\end{array} \tag{18}
$$

Die übrigen Vorzeichenkombinationen sind wegen den Reduktionsbedingungen nicht zulässig; die ausgeschlossenen Formen sind indefinit, z.B.

$$
\begin{gathered}
Q + xz + xw - yz - zw \\
= (x + \tfrac{1}{2}z + \tfrac{1}{2}w)^2 + (y - \tfrac{1}{2}z)^2 + \tfrac{1}{2}(z - \tfrac{3}{2}w)^2 - \tfrac{3}{8}w^2\,, \quad D = -3\,.
\end{gathered}
$$

Durch die Vertauschungstransformationen, von denen zwei automorph sind, entstehen zwölf Kombinationen der Variabeln; zu jeder dieser Kombinationen sind die obigen acht Anordnungen der Vorzeichen möglich. Somit besteht die Teilmenge 2 aus

$$12.8 = 96 \textit{ reduzierten Formen}.$$

Teilmenge 3:

Zur Gitterbasis (1, 10, 9, 5) gehört nach Tabelle (15) die neue reduzierte Form

$$
\begin{gathered}
f_3 = x^2 + y^2 + z^2 + w^2 + xy + xz + xw + yz + yw + zw \\
= (x + \tfrac{1}{2}y + \tfrac{1}{2}z + \tfrac{1}{2}w)^2 + \tfrac{3}{4}(y + \tfrac{1}{3}z + \tfrac{1}{3}w)^2 + \tfrac{2}{3}(z + \tfrac{1}{4}w)^2 + \tfrac{5}{8}w^2\,.
\end{gathered}
$$

Die eigentlich unimodulare Transformation, welche f in f_3 transformiert, ist

$$
T = (1, 10, 9, 5) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{aligned} x' &= x + y + z \\ y' &= z \\ z' &= -y - z \\ w' &= w \end{aligned}
$$

Durch die Umkehrtransformationen entstehen die acht Formen:

$$
\begin{array}{cccccccccccc}
Q & + & xy & + & xz & + & xw & + & yz & + & yw & + & zw \\
Q & + & xy & + & xz & - & xw & + & yz & - & yw & - & zw \\
Q & + & xy & - & xz & + & xw & - & yz & + & yw & - & zw \\
Q & - & xy & + & xz & + & xw & - & yz & - & yw & + & zw \\
Q & - & xy & - & xz & - & xw & + & yz & + & yw & + & zw \\
Q & + & xy & - & xz & - & xw & - & yz & - & yw & + & zw \\
Q & - & xy & + & xz & - & xw & - & yz & + & yw & - & zw \\
Q & - & xy & - & xz & + & xw & + & yz & - & yw & - & zw
\end{array} \tag{19}
$$

Von den 64 Vorzeichenkombinationen werden die übrigen, welche auf indefinite Formen führen, durch die Reduktionsbedingungen ausgeschlossen.

Weil die Vertauschungstransformationen zu den automorphen Substitutionen von f_3 gehören, besteht die Teilmenge 3 aus *8 reduzierten Formen.*

Damit enthält die Formenklasse $\{f\}$ insgesamt

200 reduzierte Formen.

Fordert man nach MINKOWSKI bei einer reduzierten Form außerdem, daß die gemischten Koeffizienten $f_{ik} (i \neq k)$ alle positiv oder Null sind, so existieren nur *25 normierte reduzierte Formen.*

Nun soll noch, wie eingangs des Kapitels erwähnt wurde, bewiesen werden, daß damit nicht nur die reduzierten Formen der Klasse $\{f\}$, sondern überhaupt alle reduzierten Formen mit Diskriminante $D = 5$ aufgestellt sind.

Um das zu zeigen, benutze ich die fundamentale Ungleichung des Satzes 5:

$$4\,a\,b\,c\,d \leq D = 5\,.$$

Also kommen für jede *reduzierte Form* mit $D = 5$ nur die Werte $a = b = c = d = 1$ in Frage, d.h. in einem Gitter, das durch eine solche Form metrisiert ist, haben alle Minimalvektoren die Länge eins und je vier linear unabhängige bilden eine Gitterbasis.

Nach den Reduktionsbedingungen (13) können die gemischten Koeffizienten $e \ldots l$ nur die Werte $0, +1, -1$ haben. Die Klassenzahl zu $D = 5$ kann also bestimmt werden, wenn man alle reduzierten Formen mit

$$a = b = c = d = 1\,,\ e \text{ bis } l = 0, +1, -1$$

bildet. Denn in dieser Menge sind alle Klassen mit $D = 5$ vertreten.

Die dazu erforderliche Rechenarbeit wird abgekürzt, wenn man

$$\text{Satz 2:}\quad D \equiv (e\,l + f\,k + g\,h)^2 \bmod 4$$

benutzt, weil damit sofort die Parität der Diskriminante entschieden werden kann.

Beachtet man neben Satz 2 die Tatsache, daß man bei Vertauschung der Variabeln stets in derselben Klasse bleibt, so erhält man nur noch die folgenden Fälle:

a) Nur die Koeffizienten g und h sind ungerade; die andern Koeffizienten sind gerade: $D \equiv 1 \bmod 4$.

$$x^2 + y^2 + z^2 + w^2 \pm x\,w \pm y\,z =$$
$$= (x \pm \tfrac{1}{2}w)^2 + (y \pm \tfrac{1}{2}z)^2 + \tfrac{3}{4}z^2 + \tfrac{3}{4}w^2\,,\ \text{also}\ D = 9\,.$$

b) Nur die Koeffizienten f, g und h sind ungerade; die andern Koeffizienten sind gerade: $D \equiv 1 \bmod 4$.

Alle Formen sind reduziert und haben $D = 5$; offenbar erhält man genau die reduzierten Formen der Teilmenge 1 (17).

c) Nur die Koeffizienten f, g, h und l sind ungerade; die andern Koeffizienten sind gerade: $D \equiv 1 \bmod 4$.

Alle Formen, die reduziert sind, haben $D = 5$. Man erhält die Teilmenge 2 (18).

d) Alle sechs Koeffizienten e, f, g, h, k, l sind ungerade: $D \equiv 1 \bmod 4$.

Alle Formen, die reduziert sind, haben $D = 5$. Man erhält die Teilmenge 3 (19).

Damit ist endgültig bewiesen:

Satz 9. Zur Diskriminante $D = 5$ existiert eine einzige zweiseitige Formenklasse.

Die Klasse enthält 200 reduzierte Formen, jedoch nur 25 normierte reduzierte Formen.

3. KAPITEL

Darstellungen durch die Formenklasse mit Diskriminante $D = 5$

In diesem Kapitel werden die Darstellungen durch die Formenklasse $D = 5$ untersucht.

Zu diesem Zwecke genügt es, einen Repräsentanten dieser Klasse zu betrachten, also die ganzzahligen Lösungen der Gleichung

$$f(x, y, z, w) = x^2 + y^2 + z^2 + w^2 + xz + xw + yz = n$$

zu bestimmen, wobei n eine beliebig vorgegebene natürliche Zahl ist.

Gesucht werden *Gesetze* für die Anzahl der Lösungen $f = n$; diese Anzahl werde in diesem Kapitel mit

a) $f(n)$ bezeichnet, wenn *beliebige Darstellungen*, die also einen $ggT > 1$ haben dürfen, zugelassen sind,

b) $f_e(n)$ bezeichnet, wenn nur *eigentliche*, d.h. teilerfremde Darstellungen gezählt werden.

In jedem Falle heißen zwei Darstellungen $f(x, y, z, w) = n$, $f(x', y', z', w') = n$ dann und nur dann *gleich*, wenn $x = x'$, $y = y'$, $z = z'$, $w = w'$ ist.

Ist f die metrische Grundform eines Gitters, so werden im Falle

a) die verschiedenen Gittervektoren mit Norm $= n$,

im Falle

b) die verschiedenen primitiven Gittervektoren mit Norm $= n$ gezählt.

Durch Auflösung der zu $f = n$ gleichwertigen Gleichung

$$2(2x + z + w)^2 + 2(2y + z)^2 + (2z - w)^2 + 5w^2 = 8f \qquad (20)$$

habe ich auf induktivem Wege für die eigentlichen Darstellungen der Zahl n folgende *Regeln* gefunden:

1. Jede natürliche Zahl n wird eigentlich dargestellt.

2. n = Primzahl $\neq 5$. Die Darstellungszahl hängt außer n von der Restklasse mod 5 ab, in der n liegt.
   a) $n = p \equiv 2, 3 \bmod 5$, d.h. p ist (quadratischer) Nichtrest mod 5.
   $f_e(p) = 30 \cdot (p - 1)$
   Die Regel gilt auch für $p = 2 : f_e(2) = 30$, so daß die Primzahl 2 keine besondere Stellung einnimmt.
   b) $n = q \equiv 1, 4 \bmod 5$, d.h. q ist (quadratischer) Rest mod 5.
   $f_e(q) = 20 \cdot (q + 1)$

3. n = natürliche, zu 5 teilerfremde Zahl, also
   $n = \prod_{k=1}^{r} p_k^{u_k} \cdot \prod_{k=1}^{s} q_k^{v_k}$ $\qquad p_k$ = Nichtreste mod 5, q_k = Reste mod 5.
   a) $n \equiv 2, 3 \bmod 5$.
   $$f_e(n) = 30\, n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right) \cdot \prod_{k=1}^{s} \left(1 + \frac{1}{q_k}\right)$$
   b) $n \equiv 1, 4 \bmod 5$.
   $$f_e(n) = 20\, n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right) \cdot \prod_{k=1}^{s} \left(1 + \frac{1}{q_k}\right)$$
   Der Fall 2) ist in 3) als Spezialfall enthalten.

4. n = natürliche, durch 5 teilbare Zahl, also
   $n = 5^u \cdot \prod_{k=1}^{r} p_k^{u_k} \cdot \prod_{k=1}^{s} q_k^{v_k}$ mit $u > 0$.
   a) $n \equiv 10, 15 \bmod 25$, d.h. $n/5 \equiv 2, 3 \bmod 5$.
   $$f_e(n) = 26\, n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right) \cdot \prod_{k=1}^{s} \left(1 + \frac{1}{q_k}\right)$$
   b) $n \equiv 0, 5, 20 \bmod 25$, d.h. $n/5 \equiv 0, 1, 4 \bmod 5$.
   $$f_e(n) = 24\, n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right) \cdot \prod_{k=1}^{s} \left(1 + \frac{1}{q_k}\right)$$

Die in diesen Formeln auftretende Funktion

$$n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right) \cdot \prod_{k=1}^{s} \left(1 + \frac{1}{q_k}\right)$$

kann allgemein als zahlentheoretische Funktion $P(n)$ definiert werden.

Ist nämlich $n = \Pi t^e$ die Primzahlzerlegung der beliebigen natürlichen Zahl n und verwendet man das JACOBI-Symbol

$$\left(\frac{a}{5}\right) = +1, \text{ falls } a \text{ Rest mod } 5$$

$$\left(\frac{a}{5}\right) = -1, \text{ falls } a \text{ Nichtrest mod } 5$$

$$\left(\frac{a}{5}\right) = 0, \quad \text{falls } a \equiv 0 \text{ mod } 5,$$

so kann die in Rede stehende Funktion wie folgt dargestellt werden:

$$P(n) = n \cdot \Pi\left[1 + \left(\frac{t}{5}\right) t^{-1}\right] = \Pi\left[t^e + \left(\frac{t}{5}\right) t^{e-1}\right] \tag{21}$$

$$\text{für } n > 1;\ P(1) = 1.$$

$P(n)$ ist also stets eine natürliche Zahl.

Zusammenfassend gilt bei den eigentlichen Darstellungen durch die Formenklasse $D = 5$:

Satz 10:

1.	$n \equiv 2, 3$	mod 5	$f_e(n) = 30 \cdot P(n)$
2.	$n \equiv 1, 4$	mod 5	$f_e(n) = 20 \cdot P(n)$
3.	$n \equiv 10, 15$	mod 25	$f_e(n) = 26 \cdot P(n)$
4.	$n \equiv 0, 5, 20$	mod 25	$f_e(n) = 24 \cdot P(n)$

Die folgenden Ausführungen enthalten den Beweis dieses Satzes sowie das entsprechende Gesetz für beliebige Darstellungen $f(n)$.

Zuerst einige *Beispiele* zu Satz 10:
$f_e(1) = 20$, d.h. es gibt 20 Minimalvektoren, siehe Kapitel 2.

$$f_e(4n) = \begin{cases} 4 \cdot f_e(n), & \text{falls } n \text{ gerade} \\ 2 \cdot f_e(n), & \text{falls } n \text{ ungerade}, \end{cases}$$

denn $4n$ und n haben mod 5 dasselbe quadratische Restverhalten.

$$f_e(6) = 40, f_e(7) = 180, f_e(8) = 120, f_e(9) = 120.$$

$$f_e(5) = 120, f_e(10) = 130, f_e(15) = 260, f_e(20) = 240, f_e(25) = 600.$$

Um Satz 10 zu beweisen, wird ein gerades Vielfaches einer reduzierten Form f (der Klasse $D = 5$) als quaternäre Form mit nur rein quadratischen Gliedern dargestellt:

$$k \cdot f(x, y, z, w) = a X^2 + b Y^2 + c Z^2 + d W^2$$

wobei $X = \alpha_1 x + \alpha_2 y + \alpha_3 z + \alpha_4 w$
$Y = \beta_1 x + \beta_2 y + \beta_3 z + \beta_4 w$
$Z = \gamma_1 x + \gamma_2 y + \gamma_3 z + \gamma_4 w$
$W = \delta_1 x + \delta_2 y + \delta_3 z + \delta_4 w$

$k =$ gerade, natürliche Zahl;
$a, b, c, d > 0$;
alle Koeffizienten ganze Zahlen.

Die Möglichkeit einer solchen Darstellung wird bei der JACOBIschen Transformation verwendet; ein Beispiel mit
$k = 8$ liefert Gleichung (20):

$$8 \cdot f = 2\,X^2 + 2\,Y^2 + Z^2 + 5\,W^2 .$$

Dabei ist $8 \cdot f$ bereits das kleinste Vielfache einer reduzierten Form f der Klasse $D = 5$, das so umgeformt werden kann.

Die Gleichung (20) führt, wenn man die Identität

$$2\,X^2 + 2\,Y^2 = (X + Y)^2 + (X - Y)^2$$

verwendet, auf die besonders einfache Gestalt

$$\begin{gathered} f = x^2 + y^2 + z^2 + w^2 + xz + xw + yz , \\ 8\,f = (2x + 2y + 2z + w)^2 + (2x - 2y + w)^2 + (2z - w)^2 + 5w^2 . \end{gathered} \tag{22}$$

Also kann jeder Darstellung $f(x, y, z, w) = n$ vermöge der Formeln

$$\begin{aligned} A &= 2x + 2y + 2z + w , & B &= -(2x - 2y + w) \\ C &= -(2z - w) , & D &= -w , \end{aligned} \tag{22*}$$

eindeutig eine Darstellung

$$A^2 + B^2 + C^2 + 5\,D^2 = 8\,n$$

zugeordnet werden.

Damit ist der Zusammenhang mit der von LIOUVILLE (siehe Einleitung) behandelten Form

$$F(X, Y, Z, W) = X^2 + Y^2 + Z^2 + 5W^2$$

hergestellt.

Für alles Folgende beziehen sich große Buchstaben auf diese Form F, kleine Buchstaben auf die obige Form f.

Die Umkehrung der Formeln (22*) ergibt:

$$\begin{aligned} x &= \frac{A - B + C + 3D}{4} & y &= \frac{A + B + C + D}{4} \\ z &= -\frac{C + D}{2} & w &= -D \end{aligned} \tag{23}$$

Somit stellt sich zuerst die Frage, ob auch jeder ganzzahligen Lösung $F = 8\,n$ vermöge (23) eine ganzzahlige Lösung $f = n$ entspricht.

Aus $A^2 + B^2 + C^2 + 5D^2 = 8n$ folgt modulo 4:

$$A^2 + B^2 + C^2 + D^2 \equiv 0 \mod 4 .$$

Daraus erhält man die Folgerungen:

1. In jeder Lösung $F = 8n$ sind die Zahlen A, B, C, D *entweder alle gerade oder alle ungerade.*

2. In den Formeln (23) sind z, w stets ganze Zahlen.

3. Die Zahlen $(A - B + C + 3D)$ und $(A + B + C + D)$, siehe Formeln (23), liegen in derselben Restklasse mod 4, denn diese Aussage ist mit $B \equiv D \mod 2$ gleichwertig.

Es bleibt also noch zu untersuchen, wann x und y in den Formeln (23) ganze Zahlen sind.

a) *A, B, C, D sind gerade Zahlen.*

Mit $A = 2A', B = 2B', C = 2C', D = 2D'$ gilt $A'^2 + B'^2 + C'^2 + 5D'^2 = 2n$, also

$$A'^2 + B'^2 + C'^2 + D'^2 \equiv A' + B' + C' + D' \equiv 0 \mod 2 .$$

Somit ist y und wegen Folgerung 3. auch x eine ganze Zahl, d.h.
jeder geraden Lösung $F = 8n$ entspricht umgekehrt eine ganzzahlige Lösung $f = n$.

b) *A, B, C, D sind ungerade Zahlen.*

Mit A, B, C, D betrachten wir alle Lösungen $\pm A, \pm B, \pm C, \pm D$ von $F = 8n$, insgesamt 16 Lösungen.

Weil modulo 2: $\pm A \pm B \pm C \pm D \equiv 1 + 1 + 1 + 1 \equiv 0$ ist, gilt

$$\pm A \pm B \pm C \pm D \equiv 0 \text{ oder } 2 \text{ modulo } 4 .$$

Von den 16 Möglichkeiten führen, wie man leicht verifiziert, genau je acht zu den Restklassen 0 oder 2 modulo 4, d.h.
bei ungerader Darstellung $F = 8n$ liefert nur die Hälfte nach (23) Darstellungen von $f = n$.

Nach a) und b) besteht, wenn man mit $f(n)$ bzw. $F(n)$ die Anzahl beliebiger Darstellungen $f = n$ bzw. $F = n$ bezeichnet, die Anzahl $f(n)$ aus allen geraden Lösungen $F = 8n$ und der Hälfte aller ungeraden Lösungen $F = 8n$.

Weil offenbar die Anzahl der geraden Lösungen $F = 8n : F(2n)$ beträgt, gilt

$$f(n) = \frac{F(8n) - F(2n)}{2} + F(2n) \text{ d.h.}$$

$$f(n) = \frac{F(8n) + F(2n)}{2} . \tag{24}$$

Damit ist das Darstellungsgesetz der Form f, d.h. der Formenklasse $D = 5$, auf das entsprechende Gesetz der Form F zurückgeführt.

Nach LIOUVILLE[5]) wird nun die natürliche, gerade Zahl N durch die Form

$$F = X^2 + Y^2 + Z^2 + 5W^2$$

in folgender Anzahl dargestellt:

$$N = 2^\alpha \cdot 5^\beta \cdot m \text{ mit } \alpha > 0,\ ggT(m, 10) = 1\,,$$

$$F(N) = \tfrac{1}{3}\left[5^{\beta+1} + (-1)^\alpha\left(\frac{m}{5}\right)\right] \cdot \left[2^{\alpha+1} - (-1)^\alpha \cdot 5\right] \cdot \sum_{\delta \cdot d = m}\left(\frac{\delta}{5}\right)d \qquad (25)$$

$\left(\frac{5}{m}\right), \left(\frac{\delta}{5}\right)$ = quadratische Restsymbole, δ = zu d konjugierter Teiler von m.

Der wesentliche Bestandteil der Formel ist die Funktion

$$S(n) = \sum_{\delta \cdot d = n}\left(\frac{\delta}{5}\right) \qquad \text{Summation über alle Teiler } d \text{ von } n, \qquad (26)$$

welche allgemein als zahlentheoretische Funktion definiert werden kann und bei beliebigen Darstellungen an die Stelle der früher definierten Funktion $P(n)$, (21), tritt.

Bei $n \equiv \pm 1 \bmod 5$, $\left(\frac{n}{5}\right) = 1$ gilt $\left(\frac{\delta}{5}\right) = \left(\frac{d}{5}\right)$,

bei $n \equiv \pm 2 \bmod 5$, $\left(\frac{n}{5}\right) = -1$ gilt $\left(\frac{\delta}{5}\right) = -\left(\frac{d}{5}\right)$, so daß $S(n)$

bei $\left(\frac{n}{5}\right) = +1$ den Überschuß der Teilersumme $5k \pm 1$ über die Teilersumme $5k \pm 2$,

bei $\left(\frac{n}{5}\right) = -1$ den Überschuß der Teilersumme $5k \pm 2$ über die Teilersumme $5k \pm 1$ bedeutet.

Wie LIOUVILLE erwähnt (l.c. Seite 4), kann $S(n)$ als Produkt dargestellt werden.

Ist nämlich

$$\mathrm{n} = \Pi\, t^e \text{ die Primzahlzerlegung von } n,$$

so gilt:

$$S(n) = \Pi\left[t^e + \left(\frac{t}{5}\right)t^{e-1} + t^{e-2} + \left(\frac{t}{5}\right)t^{e-3} + \ldots\right] \qquad (27)$$

Dabei ist jeder Faktor eine geometrische Reihe, welche bei geradem Exponenten mit $+1$, bei ungeradem Exponenten mit $+1$ oder -1 endet, je nachdem die Primzahl quadratischer Rest oder quadratischer Nichtrest modulo 5 ist.

---

[5]) Journal de Mathématiques, Jahrgang 1864, S. 1–12, vgl. die Bemerkungen der Einleitung.

Beweis: Es ist $n = a^u \cdot q$ mit $ggT(a, q) = 1$.

$$S(n) = \sum_{\substack{\delta_1 d_1 = a^u \\ \delta_2 d_2 = q}} \left(\frac{\delta_1 \delta_2}{5}\right) d_1 d_2 = \Sigma \left(\frac{\delta_1}{5}\right)\left(\frac{\delta_2}{5}\right) d_1 d_2 = S(a^u) \cdot S(q);$$

die Funktion $S(n)$ ist also distributiv.

Nun ist $S(a^u) = \sum_{p=0}^{u} \left(\frac{a^p}{5}\right) a^{u-p} = \sum_{p=0}^{u} \left(\frac{a}{5}\right)^p a^{u-p} = a^u + \left(\frac{a}{5}\right) a^{u-1} + a^{u-2}$

$+ \left(\frac{a}{5}\right) a^{u-3} + \ldots,$

womit gleichzeitig die Behauptung bewiesen ist, falls n nur eine Primzahl enthält. Nimmt man also an, der Satz sei für $(k-1)$-Primzahlen schon bewiesen, so gilt er auch für k-Primzahlen q.e.d.

Korollar. Aus der Gestalt der Faktoren, d.h. der geometrischen Reihen folgt sofort, daß die Funktion $S(n)$ stets *positiv*, also eine natürliche Zahl ist.

Wir bestimmen nun zu gegebener Zahl $n = 2^\varepsilon \cdot 5^\beta \cdot m$ die Funktion $f(n)$ auf Grund der Gleichungen (24) und (25).

$$2 \cdot f(n) = F(2^{\varepsilon+3} \cdot 5^\beta \cdot m) + F(2^{\varepsilon+1} \cdot 5^\beta \cdot m) = 1/3 \cdot \left[5^{\beta+1} - (-1)^\varepsilon \cdot \left(\frac{m}{5}\right)\right]$$

$$\cdot \left[2^{\varepsilon+4} + (-1)^\varepsilon \cdot 5\right] \cdot S(m) + 1/3 \cdot \left[5^{\beta+1} - (-1)^\varepsilon \cdot \left(\frac{m}{5}\right)\right] \cdot \left[2^{\varepsilon+2} + (-1)^\varepsilon \cdot 5\right]$$

$$\cdot S(m) = 1/3 \cdot \left[5^{\beta+1} - (-1)^\varepsilon \cdot \left(\frac{m}{5}\right)\right] \cdot \left[10 \cdot 2^{\varepsilon+1} + 10 \cdot (-1)^\varepsilon\right] \cdot S(m);$$

also

$$f(n) = 5/3 \cdot \left[5^{\beta+1} - (-1)^\varepsilon \cdot \left(\frac{m}{5}\right)\right] \cdot \left[2^{\varepsilon+1} + (-1)^\varepsilon\right] \cdot S(m) \qquad (28)$$

Weil bei der Formenklasse $D = 5$ die Primzahl 2 keine besondere Stellung einnimmt, muß sich dies auch formelmäßig ausdrücken lassen. Um das zu zeigen, setze ich

$$n = 5^\beta \cdot n' \text{ mit } n' = 2^\varepsilon \cdot m$$

und betrachte statt $S(m)$ die Funktion $S(n')$.

Unter Benutzung der Produktdarstellung (27) folgt:

$$S(n') = \{2^\varepsilon - 2^{\varepsilon-1} + 2^{\varepsilon+2} - + \ldots\} \cdot S(m) =$$

$$= \frac{2^\varepsilon \cdot [1 - (-\frac{1}{2})^{\varepsilon+1}]}{3/2} \cdot S(m) =$$

$$= 1/3 \cdot [2^{\varepsilon+1} + (-1)^\varepsilon] \cdot S(m).$$

Setzt man den letzten Ausdruck in (28) ein und beachtet man

$$(-1)^e \cdot \left(\frac{m}{5}\right) = \left(\frac{2^e \cdot m}{5}\right) = \left(\frac{n'}{5}\right),$$

so folgt abschließend das Darstellungsgesetz für beliebige Darstellungen durch die Formenklasse $D = 5$:

Satz 11. Die natürliche Zahl $n = 5^\beta \cdot n'$ mit $ggT(n', 5) = 1$ wird durch die Formenklasse $D = 5$ in folgender Anzahl dargestellt:

$$f(n) = 5 \cdot \left[5^{\beta+1} - \left(\frac{n'}{5}\right)\right] \cdot S(n') .$$

Zum Beispiel gilt bei $\beta = 0$, also $n = n'$ und

$$n \equiv \pm 1 \bmod 5 : f(n) = 20 \cdot S(n)$$
$$n \equiv \pm 2 \bmod 5 : f(n) = 30 \cdot S(n) .$$

Satz 10 kann auf Satz 11 zurückgeführt werden; dabei ist zu zeigen, wie beim Übergang von beliebigen zu eigentlichen Darstellungen die Funktion (26)

$$S(n') = \sum_{\delta d = n'} \left(\frac{\delta}{5}\right) d$$

durch die Funktion (21)

$$P(n') = \Pi\left[t^e + \left(\frac{t}{5}\right) t^{e-1}\right]$$

zu ersetzen ist.

Satz 11 kann abkürzend durch

$$f(n) = \lambda \cdot S(n') , \; n = 5^\beta \cdot n' ,$$

bezeichnet werden. Dabei ist $\lambda = \lambda\left[\beta, \left(\frac{n'}{5}\right)\right]$

ein Faktor, der vom Exponenten β und vom quadratischen Restverhalten n' mod 5 abhängt.

Wir befassen uns vorerst nur noch mit jenen Darstellungen, die außer der Primzahl 5 keinen gemeinsamen Teiler > 1 besitzen, d.h. bei denen der ggT höchstens noch Diskriminantenteiler enthält. Es gilt der

Hilfssatz. Die Anzahl der Lösungen $f(x, y, z, w) = n$ mit ggT $(x, y, z, w) = 5^u$, $u \geq 0$ wird bei gleichbleibendem λ durch die Formel

$$g(n) = \lambda \cdot P(n')$$

gegeben.

Beweis: Wir verwenden die bereits bewiesene Produktdarstellung (27) von $S(n')$ und denken uns in $f(n) = \lambda \cdot S(n')$ die Funktion $S(n')$ in dieser Weise dargestellt.

Es sei nun $n = 5^\beta \cdot n'$ und $n' = p^k \cdot n''$, wobei n'' den Primfaktor p nicht mehr enthält.

1. *Schritt:* Wir subtrahieren von $f(n)$ alle Darstellungen, welche den gemeinsamen Teiler p enthalten; ihre Anzahl ist offenbar $f\left(\frac{n}{p^2}\right)$, falls $k \geq 2$ ist. [Falls $k < 2$ ist, gibt es gar keine solchen Darstellungen; dann aber hat $S(n')$ in bezug auf p schon die Form von $P(n')$. Analoges gilt für die folgenden Schritte.]

Der 1. Rest besteht aus Darstellungen, deren ggT zu p teilerfremd ist:

$$
\begin{aligned}
& f(n) - f\left(\frac{n}{p^2}\right) = \\
& = \lambda \cdot \left[p^k + \left(\frac{p}{5}\right) p^{k-1} + p^{k-2} + \ldots \right] \cdot S(n'') \\
& - \lambda \cdot \left[p^{k-2} + \left(\frac{p}{5}\right) p^{k-3} + p^{k-4} + \ldots \right] \cdot S(n'') \\
& = \lambda \cdot \left[p^k + \left(\frac{p}{5}\right) p^{k-1} \right] \cdot S(n'') \\
& = \lambda \cdot P(p^k) \cdot S(n'') \,.
\end{aligned}
$$

Der Wert von λ bleibt dabei erhalten, weil β fest ist und zwei Zahlen, die sich um eine Quadratzahl unterscheiden, dasselbe quadratische Restverhalten haben.

Auf Grund der nach dem 1. Schritt erzielten Gleichung ist es naheliegend, folgendes Korollar zu beweisen:

Korollar. Es sei $n' = u \cdot v$, wobei der Faktor u nur die Primfaktoren $p_1, \ldots, p_m$ enthält.

Ist nun $f(n) = \lambda \cdot S(n')$ die Anzahl beliebiger Darstellungen durch die Formenklasse $D = 5$, so ist

$$g_m(n) = \lambda \cdot P(u) \cdot S(v)$$

die Anzahl jener Darstellungen von n, deren ggT zu den m in ihr enthaltenen Primzahlen $p_1, \ldots, p_m$ teilerfremd ist. Ist insbesondere m die Anzahl der in n' enthaltenen Primzahlen, also $v = 1$ und $S(1) = 1$, so ist das Korollar mit dem Hilfssatz identisch.

Der behandelte 1. Schritt besagt, daß das Korollar für $m = 1$ richtig ist. Nach der Methode der vollständigen Induktion dürfen wir die Gültigkeit des

Korollars nach *m-Schritten*, d. h. für m-Primzahlen, die in einer beliebigen natürlichen Zahl N enthalten sind, annehmen.

Bei $N = n$ sei also

$$g_m(n) = \lambda \cdot P(u) \cdot S(v) .$$

Um das Korollar auch bei $(m + 1)$-Primzahlen zu beweisen, sei $v = q^t \cdot w$, wobei w die Primzahl $p_{m+1} = q$ nicht mehr enthalte.

Jetzt sind noch die Darstellungen mit gemeinsamem Teiler q zu eliminieren. Weil man die Darstellungen mit gemeinsamem Teiler $p_1, \ldots, p_m$ bereits subtrahiert hat, besteht die zu eliminierende Anzahl aus den Darstellungen der Zahl $\left(\frac{n}{q^2}\right)$, die zu $p_1, \ldots, p_m$ teilerfremd sind.

Nach Induktionsvoraussetzung bei $N = \frac{n}{q^2}$ ist diese Anzahl

$$= \lambda \cdot P(u) \cdot S(q^{t-2} \cdot w) .$$

Somit erhält man nach $(m + 1)$-Schritten den Rest

$$\begin{aligned} &\lambda \cdot P(u) \cdot S(q^t \cdot w) - \lambda \cdot P(u) \cdot S(q^{t-2} \cdot w) = \\ &= \lambda \cdot P(u) \cdot S(w) \cdot [S(q^t) - S(q^{t-2})] = \\ &= \lambda \cdot P(u \cdot q^t) \cdot S(w) , \text{ womit das Korollar bewiesen ist.} \end{aligned}$$

Es besteht also ein *sukzessiver Übergang*, der von Satz 11 über das Korollar zum Hilfssatz und von diesem, wie jetzt noch zu zeigen ist, nach Satz 10 führt, wenn man die Darstellungen mit gemeinsamem Teiler 5 eliminiert.

Ich unterscheide fünf Fälle; in den ersten vier Fällen ist offenbar die Funktion $g(n)$ des Hilfssatzes bereits mit $f_e(n)$, der Anzahl eigentlicher Darstellungen, identisch.

1. Fall: $\beta = 0$, $n = n'$, $n =$ Nichtrest mod 5 .

$$f_e(n) = g(n) = 5 \cdot \left[5 - \left(\frac{n}{5}\right) \right] \cdot P(n) = 30 \cdot P(n)$$

2. Fall: $\beta = 0$, $n = n'$, $n =$ Rest mod 5.

$$f_e(n) = g(n) = 5 \cdot \left[5 - \left(\frac{n}{5}\right) \right] \cdot P(n) = 20 \cdot P(n)$$

3. Fall: $\beta = 1$, $n = 5 \cdot n'$, $n' =$ Nichtrest mod 5.

$$f_e(n) = g(n) = 5 \cdot \left[25 - \left(\frac{n'}{5}\right) \right] \cdot P(n') = 26 \cdot P(n)$$

wegen $5 \cdot P(n') = P(n)$.

4. Fall: $\beta = 1$, $n = 5 \cdot n'$, $n' =$ Rest mod 5.

$$f_e(n) = g(n) = 5 \cdot \left[25 - \left(\frac{n'}{5}\right) \right] \cdot P(n') = 24 \cdot P(n)$$

wegen $5 \cdot P(n') = P(n)$.

5. Fall: $\beta \geq 2$, $n = 5^\beta n'$.

Jetzt sind in $g(n)$ noch alle jene Darstellungen enthalten, die den gemeinsamen Teiler 5 besitzen, ihre Anzahl ist aber

$$= g(5^{\beta-2} \cdot n') \text{ . Somit:}$$

$$f_e(n) = g(5^\beta \cdot n') - g(5^{\beta-2} \cdot n') =$$

$$= 5 \cdot \left[5^{\beta+1} - \left(\frac{n'}{5}\right) \right] \cdot P(n') - 5 \cdot \left[5^{\beta-1} - \left(\frac{n'}{5}\right) \right] \cdot P(n') = 24 \cdot 5^\beta \cdot P(n') = 24 \cdot P(n)$$

wegen $5^\beta \cdot P(n') = P(n)$.

Mittels der LIOUVILLEschen Formel (25), welche sich auf die Form

$$F = X^2 + Y^2 + Z^2 + 5 \cdot W^2$$

bezieht, ist somit das Darstellungsproblem der Klasse $D = 5$ vollständig gelöst und bewiesen.

4. Ergänzungen

Gewisse Betrachtungen dieser Arbeit können auch in anderen Fällen durchgeführt werden.

a) Der untersuchten Form

$$f = x^2 + y^2 + z^2 + w^2 + xz + xw + yz \text{ mit } D = 5$$

entspricht allgemein die für jede natürliche Zahl d reduzierte Form

$$f_d = x^2 + y^2 + z^2 + dw^2 + xz + xw + yz$$

mit der JACOBIschen Darstellung

$$f_d = (x + \tfrac{1}{2}z + \tfrac{1}{2}w)^2 + (y + \tfrac{1}{2}z)^2 + \tfrac{1}{2}(z - \tfrac{1}{2}w)^2 + (d - \tfrac{3}{8})w^2 ,$$

also der Diskriminante $D = 8\,d - 3$.

Der Formel (22) entspricht die Identität

$$8 \cdot f_d = (2x + 2y + 2z + w)^2 + (2x - 2y + w)^2 + (2z - w)^2 + Dw^2 ,$$

so daß das Darstellungsgesetz der durch f_d repräsentierten Klasse über die ganz analog zu beweisende Formel (24):

$$f(n) = \frac{F(8n) + F(2n)}{2}$$

auf die Form

$$F = X^2 + Y^2 + Z^2 + D \cdot W^2$$

zurückgeführt werden kann.

Beispiel: $d = 2$.

$$f = x^2 + y^2 + z^2 + 2 \cdot w^2 + xz + xw + yz\,,\ D = 13\,.$$

Zu $D = 13$ existiert nur eine zweiseitige Klasse, wie man nach dem bei $D = 5$ benutzten Verfahren beweist.

Auf empirischem Wege finde ich für beliebige Darstellungen durch die Formenklasse $D = 13$ folgendes Gesetz bestätigt, jedoch ohne Beweis:

$$n = 13^{\beta} \cdot n' \text{ mit } \mathrm{ggT}\,(13, n') = 1$$

$$f(n) = \left[13^{\beta+1} - \left(\frac{n'}{13}\right)\right] \cdot \sum_{\substack{d \mid n' \\ \delta d = n'}} \left(\frac{\delta}{13}\right) d$$

b) Um gewisse Analogien der Darstellungsgesetze besonders hervorzuheben, sei noch die Untersuchung der quaternären Formen mit $D = 8$ kurz mitgeteilt.

Reduzierte Formen:

$$\begin{aligned} f &= x^2 + y^2 + z^2 + w^2 + xz + yz \\ &= (x + \tfrac{1}{2}z)^2 + (y + \tfrac{1}{2}z)^2 + \tfrac{1}{2}z^2 + w^2\,. \\ g &= x^2 + y^2 + z^2 + w^2 + xz + xw + zw \\ &= (x + \tfrac{1}{2}z + \tfrac{1}{2}w)^2 + y^2 + \tfrac{3}{4}(z + \tfrac{1}{3}w)^2 + \tfrac{2}{3}w^2\,. \end{aligned}$$

Die Form g ist zu f eigentlich äquivalent vermöge der Transformation

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad \begin{aligned} x' &= x \\ y' &= -z \\ z' &= y \\ w' &= z + w \end{aligned} \qquad |T| = +1.$$

Die Klasse f ist zweiseitig, weil f z.B. die automorphe Substitution

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

mit Determinante $|A| = -1$ besitzt.

Außer den durch Umkehr- und Vertauschungstransformationen entstehenden Formen gibt es keine weiteren reduzierten Formen mit $D = 8$, so daß zu $D = 8$ wieder nur *eine einzige zweiseitige Klasse* existiert.

Nun besteht die Identität:

$$2 \cdot f = (x + y + z)^2 + (x - y)^2 + z^2 + 2 \cdot w^2 ,$$

womit die Form f auf die Form

$$F = X^2 + Y^2 + Z^2 + 2 \cdot W^2$$

bezogen werden kann. Auf Grund der Zuordnungen

$$A = x + y + z , \; B = x - y , \; C = z , \; D = w;$$

$$x = \frac{A + B - C}{2} , \; y = \frac{A - B - C}{2} , \; z = C , \; w = D$$

entsprechen sich die ganzzahligen Lösungen $f(x, y, z, w) = n$ und $F(A, B, C, D) = 2n$ eineindeutig, d.h.
die natürliche Zahl n wird durch die Form f in gleicher Anzahl dargestellt wie die Zahl $2n$ durch die Form F.

Die Form F wurde von LIOUVILLE (J. Math. Pures Appl. 1861, S. 225f.) vollständig behandelt und seine Resultate wurden von PEPIN bewiesen[6]). Damit lautet das Gesetz für beliebige Darstellungen durch die Formenklasse $D = 8$:

Satz 12. *Die natürliche Zahl $n = 2^u \cdot n'$, n' ungerade, wird durch die Formenklasse mit Diskriminante $D = 8$ wie folgt dargestellt:*

$$f(n) = 2 \cdot \left[2^{u+3} - \left(\frac{2}{n'}\right) \right] \cdot \sum_{\delta d = n'} \left(\frac{2}{\delta}\right) d$$

Das zugehörige Gesetz für eigentliche Darstellungen kann wie beim Übergang von Satz 11 zu Satz 10 bewiesen werden; dabei tritt an die Stelle der Funktion

$$S(n) = \sum_{\delta d = n} \left(\frac{2}{\delta}\right) d \qquad \text{wieder} \quad P(n) = \Pi \left[t^e + \left(\frac{2}{t}\right) t^{e-1} \right] .$$

Man darf also annehmen, daß bei einklassigen Diskriminanten D im Gesetz für beliebige Darstellungen die Funktion

$$S = \Sigma \left(\frac{D}{\delta}\right) d,$$

im Gesetz für eigentliche Darstellungen die Funktion

$$P = \Pi \left[t^e + \left(\frac{D}{t}\right) \cdot t^{e-1} \right]$$

eine wesentliche Rolle spielt[7]).

---

[6]) [5] PEPIN.

[7]) Bei $D \equiv 1 \bmod 4$ ist $\left(\frac{D}{t}\right) = \left(\frac{t}{D}\right)$.

LITERATURVERZEICHNIS

[1] J. CHAPELON, *Sur les relations entre les nombres des classes de formes quadratiques binaires.* Ecole Polytech., 19 (1915).

[2] L. E. DICKSON, *History of the Theory of Numbers.* Band III: Quadratic and higher forms, Washington, 1923.

[3] J. LIOUVILLE, *Sur la forme* $x^2 + y^2 + z^2 + 5t^2$. J. Math. Pures Appl. (2), 9 (1864), 1–16.

[4] H. MINKOWSKI, *Geometrie der Zahlen.* Neudruck New York, 1953.

[5] T. PEPIN, *Sur quelques formes quadratiques quaternaires.* J. Math. Pures Appl. (4), 6 (1890), 5–67.

[6] SCHOLZ und SCHOENEBERG, *Einführung in die Zahlentheorie.* Sammlung Göschen, Band 1131.

[7] B. L. VAN DER WAERDEN, *Die Reduktionstheorie der positiven quadratischen Formen.* Acta math. 96 1956), 265f.

(Eingegangen den 3. März 1961)