

# DIE REDUKTIONSTHEORIE DER POSITIVEN QUADRATISCHEN FORMEN

VON

B. L. VAN DER WAERDEN

in Zürich

„Obschon die rationalen quadratischen Formen zu den ältesten Gebieten der Zahlentheorie überhaupt gehören, haben sie doch bisher nur im binären Fall eine einigermaßen abschliessende Behandlung erfahren. Was darüber hinaus angeboten wird, befindet sich in einem chaotischen unbefriedigenden Zustand, wie die enzyklopädische Darstellung von Bachmann deutlich erkennen lässt. Nirgends bemerkt man, dass leitende Gesichtspunkte in den Vordergrund gestellt und nebensächliche ihnen untergeordnet werden.“

H. BRANDT, Über Stammformen. *Ber. Verh. sächs. Akad. Leipzig*, 100 (1952), S. 3.

## Einleitung

Seit Brandt die eben zitierten Worte geschrieben hat, ist das Buch von Eichler, *Quadratische Formen und orthogonale Gruppen* (Springer 1952), erschienen, in dem wirklich leitende Gesichtspunkte in den Vordergrund gestellt sind. Jedoch ist damit erst ein Anfang gemacht, denn vieles Wichtige ist bei Eichler nicht ausgeführt und im Ganzen ist die Theorie nach wie vor, wie Brandt ganz richtig sagt, in einem chaotischen Zustand.

Fragen wir z. B. ganz konkret: Was wissen wir von den Darstellungen gegebener Zahlen durch quaternäre Formen? so finden wir in der Literatur einerseits die allgemeine Maßformel von Siegel<sup>1</sup>, andererseits eine Reihe von zerstreuten Untersuchungen mit ganz verschiedenen Methoden über spezielle Formen wie

$$f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2. \quad (\text{A})$$

---

<sup>1</sup> C. L. SIEGEL, Analytische Theorie der quadratischen Formen I. *Annals of Math.*, 40, 52. Dazu Kap. 5 des Buches von EICHLER.

Von einer systematischen Herleitung dieser Ergebnisse aus einer allgemeinen Methode sind wir noch weit entfernt. Zwar hat Hurwitz den Zusammenhang mit den Quaternionen hergestellt, aber er hat seine Methode nur auf die eine Form (A) angewandt.

Um hier weiter zu kommen, müsste man einerseits die allgemeine Maßformel auf quaternäre Formen spezialisieren und die in ihr vorkommenden Faktoren explizit auswerten, andererseits die Hurwitzsche Zahlentheorie der Quaternionen und die Gauss'sche Theorie der binären Formen verallgemeinern. Indem man nach Hilberts bewährtem Rezept von den ganz einfachen Beispielen ausgeht und dabei doch die allgemeinen Gesichtspunkte im Auge behält, muss es möglich sein, eine befriedigende Theorie aufzubauen.

Ein Hilfsmittel wird man dabei jedenfalls brauchen, nämlich die *Reduktionstheorie*. Man wird nämlich in konkreten Fällen untersuchen müssen, welche Formenklassen gegebener Diskriminante es gibt. Das geeignete Hilfsmittel dazu ist, wie im binären Fall, die Reduktionstheorie.

Eine positive binäre Form<sup>1</sup>

$$f(x_1, x_2) = f_{11} x_1^2 + f_{12} x_1 x_2 + f_{22} x_2^2$$

heißt nach Lagrange (siehe Literaturverzeichnis am Schluss der Abhandlung) *reduziert*, wenn die Koeffizienten die Bedingungen

$$|f_{12}| \leq f_{11} \leq f_{22} \tag{B}$$

erfüllen. Jede positive Form  $f$  ist äquivalent einer reduzierten Form.

Die Bedingungen (B) sind, wie man leicht sieht, gleichbedeutend mit der Forderung, dass  $f_{11} = f(1,0) = f(\mathbf{e}_1)$  das erste und  $f_{22} = f(0,1) = f(\mathbf{e}_2)$  das zweite Minimum der Form  $f$  ist, d. h.  $f_{11}$  ist das Minimum von  $f(\mathbf{s})$  für Gittervektoren  $\mathbf{s} \neq 0$  und  $f_{22}$  ist das Minimum von  $f(\mathbf{s})$  für Gittervektoren  $\mathbf{s}$ , die von  $\mathbf{e}_1 = (1,0)$  linear unabhängig sind.

In ähnlicher Weise kann man nach Seeber und Dirichlet auch bei ternären Formen fordern, dass  $f_{11}$ ,  $f_{22}$  und  $f_{33}$  das erste, zweite und dritte Minimum sein sollen.

Für  $n$ -äre Formen ist jedoch diese *Reduktion nach sukzessiven Minima* nicht durchführbar, weil die sukzessiven Minimumvektoren im allgemeinen keine Basis des vorgelegten Gitters bilden. Anders ausgedrückt: es gibt nicht in jeder Formenklasse eine reduzierte Form im Sinne von Dirichlet. Ein Beispiel für  $n = 5$  wird man in § 7 finden.

Aus diesem Grunde hat Hermite den Begriff der reduzierten Form anders definiert. Eine positive quadratische Form

---

<sup>1</sup> Ich folge SEEBER und BRANDT, indem ich den Koeffizienten von  $x_1 x_2$  nicht, wie GAUSS,  $2b$  oder  $2f_{12}$ , sondern  $f_{12}$  nenne. Die arithmetische Theorie wird dadurch, wie BRANDT am Beispiel der ternären Formen gezeigt hat, sehr viel einfacher. Die Koeffizienten  $f_{ik}$  sind in dieser Arbeit immer reelle Zahlen.

$$f(x_1, \dots, x_n) = f_{11}x_1^2 + f_{12}x_1x_2 + \dots + f_{nn}x_n^2 \quad (\text{C})$$

heisst nach Hermite reduziert, wenn  $f_{11}$  der kleinstmögliche Wert des ersten Koeffizienten für alle zu  $f$  äquivalenten Formen ist,  $f_{22}$  der kleinstmögliche Wert des zweiten Diagonalkoeffizienten für alle äquivalenten Formen mit dem gleichen Koeffizienten  $f_{11}$ , ebenso  $f_{33}$  minimal bei gegebenen  $f_{11}$  und  $f_{22}$ , etc. bis  $f_{nn}$ .

Minkowski hat eine etwas einfachere Definition gegeben. Eine Form  $f$  heisst nach Minkowski reduziert, wenn folgende Ungleichungen gelten:

$$f_{kk} \leq f(s_1, \dots, s_n) \quad \text{für alle ganzen Zahlen } s_1, \dots, s_n \quad \text{mit} \quad (s_1, \dots, s_n) = 1 \quad (\text{D})$$

Ist eine Form im Sinne von Hermite reduziert, so auch im Sinne von Minkowski; das folgt leicht aus den Sätzen des nachfolgenden § 1. Ob das Umgekehrte auch gilt, weiss ich nicht.

Der Vollständigkeit halber möge hier auch noch der Reduktionsbegriff von Selling erwähnt werden. Siehe darüber den neuen Enzyklopädieartikel von O. H. Keller, *Geometrie der Zahlen*, S. 56.

Die vorliegende Arbeit besteht aus 3 Hauptteilen. Ich gebe zunächst eine Übersicht über den Inhalt der 3 Teile.

### Teil I (§ 1–10)

Die Bedingungen (D) haben die Form von linearen Ungleichungen in den Koeffizienten  $f_{ij}$ . Es gelang Minkowski, zu beweisen, dass alle Bedingungen (D) aus endlich vielen unter ihnen folgen. Ferner bewies Minkowski eine fundamentale Ungleichung für die Diskriminante  $D_n$  einer reduzierten Form, nämlich

$$\lambda_n f_{11} f_{22} \dots f_{nn} \leq D_n. \quad (\text{E})$$

Für  $n = 2$  und  $3$  hatten bereits Gauss und Seeber solche Ungleichungen (mit  $\lambda_2 = \frac{3}{4}$  und  $\lambda_3 = \frac{1}{2}$ ) erhalten.

In seiner *Geometrie der Zahlen* hatte Minkowski eine ähnliche Ungleichung für die sukzessiven Minima  $N_1, N_2, \dots$  einer positiven Form  $f$  hergeleitet, nämlich

$$N_1 N_2 \dots N_n \leq \mu_n D_n. \quad (\text{F})$$

Nach einer gut begründeten Vermutung von H. Weyl hatte Minkowski die Absicht, seine *Geometrie der Zahlen* für die Reduktionstheorie nutzbar zu machen und insbesondere (E) aus (F) herzuleiten. Er hat aber anscheinend die Brücke zwischen (F) und (E) nicht gefunden; denn in seiner grossen Abhandlung [2] über die Reduktionstheorie, die 9 Jahre nach der „*Geometrie der Zahlen*“ erschien, macht er von seinen eigenen geometrischen

Methoden keinerlei Gebrauch. Der Beweis der Ungleichung (E) ist bei Minkowski in komplizierter Weise verknüpft mit dem Endlichkeitsbeweis für die Reduktionsbedingungen (D).

Eine Vereinfachung dieses Endlichkeitsbeweises gelang Bieberbach und Schur. Sie spalteten den Endlichkeitssatz in zwei Teilsätze auf (Satz 8 und Satz 9 im folgenden § 8), von denen der zweite sagt, dass nur in endlich vielen Bedingungen (D) für reduzierte Formen das Gleichheitszeichen gelten kann, und der erste, dass aus diesen Bedingungen die übrigen folgen.

Die Ungleichung (E) wurde von Remak 1938 neu bewiesen und verschärft. Im gleichen Jahr gelang Mahler der Übergang von (F) zu (E) in einer sehr einfachen Weise, indem er eine Ungleichung

$$f_{kk} \leq \delta_k N_k \quad (\text{G})$$

bewies. Die Ungleichung (G) wurde 1940 von Weyl wiederentdeckt. In § 6–7 wird sich zeigen, dass die Ungleichung (G) durch Anwendung der Remakschen Schätzungsmethode ohne Mühe so verschärft werden kann, dass die Ungleichung (E) mit dem von Remak angegebenen Koeffizienten  $\lambda_n$  herauskommt. Die gleiche Schätzungsmethode führt dann in § 8 auf dem von Bieberbach–Schur und Weyl gezeigten Weg zum Beweis des Endlichkeitssatzes für die Bedingungen (D).

Mit derselben Methode, unter Anwendung eines zahlentheoretischen Kunstgriffes, ergibt sich in § 10 ein sehr einfacher Beweis für den „zweiten Endlichkeitssatz“, der besagt, dass nur endlich viele ganzzahlige Transformationen reduzierte Formen in reduzierte Formen überführen können.

Um die Darstellung leicht verständlich zu machen, werden in § 1–5 die Grundbegriffe von Anfang an entwickelt. § 1 handelt von den Basen eines Gitters und den primitiven Systemen von Vektoren  $\mathbf{e}_1, \dots, \mathbf{e}_k$ , die sich zu einer Basis ergänzen lassen. In § 2 wird eine quadratische Metrik eingeführt und die dazu gehörige Form  $f$  als Summe von Quadraten geschrieben; im Anschluss daran wird gezeigt, dass die Diskriminante  $D_n$  der Form  $f$  das Quadrat des Volumens der Gittermasche ist. In § 3 wird bewiesen, dass es in jeder Klasse von positiven Formen eine reduzierte im Sinne von Minkowski gibt. § 4 handelt von den Ungleichungen von Gauss und Seeber für binäre und ternäre reduzierte Formen

$$D_2 \geq \frac{3}{4} f_{11} f_{22} \text{ und } D_3 \geq \frac{1}{2} f_{11} f_{22} f_{33}. \quad (\text{H})$$

In § 5 werden die sukzessiven Minima  $N_1, N_2, \dots$  eingeführt und die Ungleichung von Minkowski (F) bewiesen.

Beim Beweis der Ungleichung von Mahler (G) in § 6 ergibt sich gleichzeitig, dass für  $k \leq 4$  die Gleichung

$$f_{kk} = N_k \quad (k = 1, 2, 3, 4) \quad (\text{I})$$

gilt. Daraus folgt, dass die reduzierten Formen in höchstens 4 Variablen auch im Sinne der sukzessiven Minima reduziert sind. Dieses Ergebnis stammt von Julia, der auch die einzige quaternäre Form bestimmt hat, deren erste 4 Minimumvektoren nicht notwendig eine Basis des Gitters bilden (§ 7).

In § 8 wird der Endlichkeitssatz für die Reduktionsbedingungen (D) nach Bieberbach-Schur mit der Vereinfachung von Weyl bewiesen. Die Schätzungsmethode von Remak führt zu recht scharfen Schranken für die in (D) auftretenden ganzen Zahlen  $s_1, \dots, s_n$ .

In § 9 werden die Reduktionsbedingungen für binäre, ternäre und quaternäre Formen vollständig ausgeschrieben. Es ist zu erwarten, dass in einer künftigen Theorie der quaternären Formen diese Reduktionsbedingungen und die von Mahler [3] zuerst formulierte Ungleichung

$$D_4 \geq \frac{1}{4} f_{11} f_{22} f_{33} f_{44} \quad (\text{K})$$

eine ähnliche Rolle spielen werden wie die Bedingungen (B) und die Ungleichung (H) in der Gaußschen Theorie der binären Formen.

In § 10 wird der „zweite Endlichkeitssatz“ bewiesen. Die bisherigen Beweise, unter denen der von Siegel hervorgehoben zu werden verdient, benutzen recht komplizierte Abschätzungen. Man kommt aber mit den gleichen Beweismethoden aus, die beim ersten Endlichkeitssatz zum Ziel führten, indem man zunächst mittels eines zahlentheoretischen Kunstgriffes die Koordinaten der sukzessiven Minimumvektoren  $\mathbf{s}_1, \dots, \mathbf{s}_n$  abschätzt und dann die Übergangsmatrix, die von einer reduzierten Gitterbasis  $(\mathbf{e}_1, \dots, \mathbf{e}_n)$  zu einer anderen  $(\mathbf{e}'_1, \dots, \mathbf{e}'_n)$  führt, als Produkt  $S'S^{-1}$  darstellt, wobei  $S$  von den  $\mathbf{s}_j$  zu den  $\mathbf{e}_i$  und  $S'$  von den  $\mathbf{s}_j$  zu den  $\mathbf{e}'_i$  führt.

## Teil II (§ 11–13)

Die positiven quadratischen Formen bilden ein Gebiet  $G$  im  $N$ -dimensionalen Raum aller quadratischen Formen. Die reduzierten Formen bilden in dieser offenen Menge eine „Zelle“  $Z$ , die durch endlich viele ebene „Wände“ begrenzt wird. Eine unimodulare Transformation  $T$  der Variablen  $x_1, \dots, x_n$  transformiert  $Z$  in eine Zelle  $TZ$ , die in  $2^n$  trivialen Fällen mit  $Z$  zusammenfällt, sonst aber mit  $Z$  höchstens Randpunkte gemeinsam hat. Die Zellen  $TZ$  überdecken zusammen das ganze Gebiet  $G$ , jeder Punkt von  $G$  gehört nur endlich vielen Zellen an und die Zellen häufen sich nur gegen den Rand von  $G$ . Von jeder Zelle  $T_0 Z$  aus kann man jede andere  $TZ$  erreichen durch Übergang zu Nachbarzellen  $T_1 Z, T_2 Z, \dots, TZ$ , von denen je zwei aufeinanderfolgende ein  $(N-1)$ -dimensionales

Wandstück gemeinsam haben. Das alles hat Weyl auf Grund seiner Abschätzungen streng bewiesen. Man braucht die Abschätzungen aber nicht, sondern man kann topologische Schlüsse benutzen, die im wesentlichen darauf beruhen, dass ein  $N$ -dimensionales Gebiet durch einen linearen Raum von weniger als  $N - 1$  Dimensionen nicht zerlegt wird. Diese Schlüsse lassen sich auch in anderen Fällen anwenden, in denen keine expliziten Abschätzungen verfügbar sind.

Der Teil der Zelle  $Z$ , der durch

$$f_{k, k+1} \geq 0 \quad (k = 1, 2, \dots, n - 1) \quad (\text{L})$$

bestimmt wird, ist nach Minkowski ein Fundamentalbereich für die Gruppe der Transformationen  $T$  im Gebiet der positiven Formen.

Wenn die Formen  $f$  durch  $f_{11} + \dots + f_{nn} = 1$  normiert werden, so wird aus der Zelle  $Z$  ein beschränktes Polyeder im  $(N - 1)$ -dimensionalen Raum. Im Fall  $n = 2$  ist dieses Polyeder ein Dreieck. Man kann es in den bekannten Fundamentalbereich der Modulgruppe transformieren (§ 13).

### Teil III (§ 14–16)

Die Ungleichung (F) hängt unmittelbar mit dem Problem der dichtesten gitterförmigen Kugelpackung im  $n$ -dimensionalen Raum zusammen. Aus (F) folgt nämlich

$$N_1^n \leq \mu_n D_n. \quad (\text{M})$$

Dabei ist  $N_1$  das erste Minimum der Form  $f$ , d. h. das Quadrat des Abstandes von 0 zum nächsten Gitterpunkt und  $D_n$  das Quadrat des Volumens der Gittermasche. Umgekehrt folgt auch (F) aus (M).

In § 14 wird zunächst nach Minkowski gezeigt, dass  $\sqrt[n]{D_n}$  eine konkave Funktion der Koeffizienten  $f_{ij}$  ist. Daraus folgt, dass das Minimum von  $D_n$  bei gegebenem  $f_{11} = N_1$  nur von einer „Kantenform“ auf einer eindimensionalen Kante der Zelle  $Z$  geliefert werden kann. Um das Minimum effektiv zu bestimmen, hat man nach Korkine und Zolotareff zunächst alle *Extremformen* aufzustellen. Eine Form  $f$  heisst extrem, wenn bei jeder kleinen Änderung, bei der das erste Minimum  $N_1$  gleich bleibt, die Diskriminante  $D_n$  zunimmt.

Die Minimumvektoren  $\mathbf{s}$  einer Extremform  $f$  werden, wenn  $N_1 = 1$  normiert wird, durch

$$f(\mathbf{s}) = 1 \quad (\text{N})$$

definiert. Es gibt für jede Form  $f$  nur endlich viele Gittervektoren  $\mathbf{s}$  mit der Eigenschaft (N). Unter den endlich vielen Gleichungen (N) gibt es  $N$  linear unabhängige, welche die

Koeffizienten  $f_{ij}$  vollständig bestimmen (§ 15, Satz 21). Dieser Satz von Korkine und Zolotareff folgt fast unmittelbar aus der Konkavität der Funktion  $\sqrt[n]{D_n}$ .

In § 16 werden zunächst auf Grund eines weiteren Satzes von Korkine und Zolotareff die ternären und quaternären Extremformen bestimmt. Für  $n = 3$  gibt es nur eine Extremform, die zu der bekannten dichtesten gitterförmigen Kugelpackung führt. Für  $n = 4$  gibt es 2 Extremformen mit verschiedenen Diskriminanten, von denen eine das Minimum  $D_4 = \frac{1}{4} N_1^4$  liefert. Am Schluss wird noch eine Übersicht über die Untersuchungen von Korkine, Zolotareff, Hofreiter und Coxeter gegeben, die zur Bestimmung der quinären und senären Extremformen geführt haben.

## TEIL I

### § 1. Primitive Vektorsysteme in einem Gitter

**DEFINITION.** Ein Gitter  $G_n$  besteht aus allen ganzzahligen Linearkombinationen  $\mathbf{y} = \mathbf{e}_1 y_1 + \dots + \mathbf{e}_n y_n$  von  $n$  linear unabhängigen Vektoren  $\mathbf{e}_1, \dots, \mathbf{e}_n$ . Diese  $n$  Vektoren bilden eine *Basis* des Gitters.

**DEFINITION.** Irgend  $k$  linear unabhängige Gittervektoren  $\mathbf{s}_1, \dots, \mathbf{s}_k$  bilden für das gegebene Gitter ein *primitives System*, wenn es in dem von ihnen aufgespannten linearen Raum keine Gittervektoren ausser ganzzahligen Linearkombinationen  $\mathbf{s}_1 g_1 + \dots + \mathbf{s}_k g_k$  gibt. Besteht das System nur aus einem Vektor  $\mathbf{s}$ , so heisst dieser ein *primitiver Vektor* des Gitters.

**SATZ 1.** Ein primitiver Vektor  $\mathbf{s}$  kann zu einer Basis des Gitters ergänzt werden.

*Beweis:* Sei  $\mathbf{s} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_n s_n$ . Wir können annehmen, dass die  $s_i$  nicht negativ sind (sonst würde man  $-\mathbf{e}_i$  statt  $\mathbf{e}_i$  als Basisvektor nehmen) und dass  $s_1$  der kleinste von Null verschiedene Koeffizient ist. Ist nun etwa  $s_2 \neq 0$ , also  $s_2 \geq s_1$ , so kann man den Ausdruck für  $\mathbf{s}$  so umformen

$$\mathbf{s} = (\mathbf{e}_1 + \mathbf{e}_2 q) s_1 + \mathbf{e}_2 (s_2 - q s_1) + \mathbf{e}_3 s_3 + \dots + \mathbf{e}_n s_n = \mathbf{e}'_1 s_1 + \mathbf{e}_2 s'_2 + \mathbf{e}_3 s_3 + \dots + \mathbf{e}_n s_n$$

mit  $s'_2 = s_2 - q s_1$ . Wählt man  $q$  so, dass  $s'_2$  positiv oder Null, aber  $< s_1$  wird und verkleinert man in der gleichen Weise die übrigen Koeffizienten, so erhält man entweder die Koeffizientenreihe  $(s_1, 0, \dots, 0)$  oder man erhält einen positiven Koeffizienten  $s'_i < s_1$ . In diesem Fall bringt man den kleinsten positiven Koeffizienten durch Vertauschung der Basisvektoren wieder an die erste Stelle und setzt das Verfahren fort. So erhält man nach endlich vielen Schritten eine neue Basis  $(\mathbf{e}_1^*, \dots, \mathbf{e}_n^*)$  und einen Ausdruck für  $\mathbf{s}$  von der Form

$$\mathbf{s} = \mathbf{e}_1^* m \quad (m > 0).$$

Wenn nun  $\mathbf{s}$  primitiv ist, muss  $m = 1$  sein. Man erhält also  $\mathbf{s} = \mathbf{e}_1^*$  und der Satz ist bewiesen.

**KORROLAR 1.** Ein Gittervektor  $\mathbf{s} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_n s_n$  ist dann und nur dann primitiv, wenn der GGT der Koeffizienten Eins ist. Diese Eigenschaft bleibt nämlich bei Koeffiziententransformationen  $s'_2 = s_2 - q s_1$  erhalten.

**SATZ 2.** Ein primitives System  $\mathbf{s}_1, \dots, \mathbf{s}_k$  kann zu einer Basis des Gitters ergänzt werden.

*Beweis:* Für  $k = 1$  haben wir Satz 1. Wir können also eine Induktion nach  $k$  ansetzen. Ein primitives System  $\mathbf{s}_1, \dots, \mathbf{s}_{k+1}$  sei gegeben. Nach der Induktionsvoraussetzung können wir eine Basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  so wählen, dass  $\mathbf{s}_1 = \mathbf{e}_1, \dots, \mathbf{s}_k = \mathbf{e}_k$  wird. Wir setzen nun

$$\mathbf{s}_{k+1} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_k s_k + \mathbf{e}_{k+1} s_{k+1} \dots + \mathbf{e}_n s_n$$

an. Die Koeffizienten  $s_{k+1}, \dots, s_n$  sind nicht alle Null, denn sonst wären  $\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{s}_{k+1}$  linear abhängig. Wir formen nun die Zahlenreihe  $s_{k+1}, \dots, s_n$  genau so um wie beim Beweis von Satz 1 und erhalten.

$$\mathbf{s}_{k+1} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_k s_k + \mathbf{e}_{k+1}^* m \quad (m > 0). \quad (1)$$

Der Vektor  $\mathbf{e}_{k+1}^*$  ist Gittervektor und liegt in dem linearen Raum, der von  $\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{s}_{k+1}$  aufgespannt wird, muss also eine ganzzahlige Linearkombination dieser Vektoren sein. Daraus folgt  $m = 1$ . Man kann nun  $\mathbf{e}_{k+1}^*$  als Basisvektor durch

$$\mathbf{s}_{k+1} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_k s_k + \mathbf{e}_{k+1}^*$$

ersetzen. Damit ist der Satz bewiesen.

**KORROLAR 2.** Ein Vektor  $\mathbf{s} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_n s_n$  bildet mit  $\mathbf{e}_1, \dots, \mathbf{e}_k$  dann und nur dann ein primitives System, wenn die Koeffizienten  $s_{k+1}, \dots, s_n$  nicht alle Null sind und ihr GGT Eins ist.

**KORROLAR 3.** Sind  $\mathbf{e}_1, \dots, \mathbf{e}_k, \mathbf{s}_{k+1}$  linear unabhängig, so kann man unter Beibehaltung der Basisvektoren  $\mathbf{e}_1, \dots, \mathbf{e}_k$ , den nächsten Basisvektor  $\mathbf{e}_{k+1}^*$  so wählen, dass (1) gilt.

## § 2. Quadratische Metrik

Ist eine Basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  des reellen Vektorraums  $E_n$  gegeben und drückt man jeden Vektor  $\mathbf{x}$  durch die Basis aus:

$$\mathbf{x} = \mathbf{e}_1 x_1 + \dots + \mathbf{e}_n x_n,$$

so definiert jede positive reelle quadratische Form



$$f(x) = \sum_i f_{ii} x_i^2 + \sum_{i < k} f_{ik} x_i x_k \tag{2}$$

eine *quadratische Metrik*. Die reelle, nicht negative Zahl  $f(x)$  heisst auch *Norm* des Vektors  $\mathbf{x}$ , ihre Quadratwurzel ist die Länge  $|\mathbf{x}|$ :

$$N \mathbf{x} = |\mathbf{x}|^2 = f(x).$$

Mit der Norm ist das Skalarprodukt

$$(\mathbf{x}, \mathbf{y}) = \sum_i f_{ii} x_i y_i + \frac{1}{2} \sum_{i < k} f_{ik} (x_i y_k + x_k y_i)$$

invariant verknüpft. Ist  $(\mathbf{x}, \mathbf{y}) = 0$ , so heissen  $\mathbf{x}$  und  $\mathbf{y}$  *orthogonal* oder *senkrecht*.

Man kann die Form (2) so schreiben:

$$f(x) = f_{11}(x_1 + \frac{1}{2} f_{11}^{-1} f_{12} x_2 + \dots + \frac{1}{2} f_{11}^{-1} f_{1n} x_n)^2 + g(x_2, \dots, x_n).$$

Wiederholt man das Verfahren, so erhält man schliesslich die *Jacobische Darstellung*

$$f(x) = \xi_1^2 + \dots + \xi_n^2 \tag{3}$$

mit

$$\left. \begin{aligned} \xi_1 &= h_1(x_1 + \beta_{12} x_2 + \dots + \beta_{1n} x_n), \\ \xi_2 &= \quad \quad h_2(x_2 + \dots + \beta_{2n} x_n), \\ &\dots \dots \dots \dots \dots \dots \dots \dots \\ \xi_n &= \quad \quad \quad \quad \quad \quad \quad \quad h_n x_n. \end{aligned} \right\} \tag{4}$$

Die Diskriminante der Form (2) sei  $D_n$ . Die Diskriminante der transformierten Form (3) ist 1. Die Determinante der Übergangssubstitution (4) ist  $h_1 h_2 \dots h_n$ . Also ist

$$D_n = (h_1 \dots h_n)^2. \tag{5}$$

Die  $\xi_i$  heissen *rechtwinklige Koordinaten* des Vektors  $\mathbf{x}$ . Setzt man in (4) speziell  $x_k = 1$  und die übrigen  $x_j = 0$ , so erhält man die rechtwinkligen Koordinaten des Basisvektors  $\mathbf{e}_k$ :

$$\left. \begin{aligned} \varepsilon_{jk} &= h_j \beta_{jk} & (j < k) \\ \varepsilon_{kk} &= h_k \\ \varepsilon_{jk} &= 0 & (j > k) \end{aligned} \right\} \tag{6}$$

Die Norm des Basisvektors  $\mathbf{e}_k$  ist nach (3) die Quadratsumme der rechtwinkligen Koordinaten

$$f_{kk} = N \mathbf{e}_k = h_1^2 \beta_{1k}^2 + h_2^2 \beta_{2k}^2 + \dots + h_k^2. \tag{7}$$

Aus (7) folgt unmittelbar die Ungleichung

$$h_k^2 \leq f_{kk}. \tag{8}$$

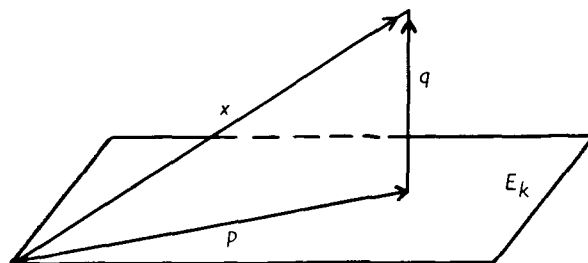


Fig. 1.

Aus (3) sieht man, dass die Form  $f$  eine gewöhnliche Euklidische Metrik definiert. Wir können also die uns vertrauten geometrischen Begriffe anwenden. Statt „Vektor“ werden wir häufig „Punkt“ sagen. Die Länge  $|\mathbf{x} - \mathbf{y}|$  heisst der *Abstand* zwischen den Punkten  $\mathbf{x}$  und  $\mathbf{y}$ .

Ist  $E_k$  der von  $\mathbf{e}_1, \dots, \mathbf{e}_k$  aufgespannte Teilraum des Vektorraumes, so kann man jeden Vektor  $\mathbf{x}$  aufspalten in eine *Projektion*  $\mathbf{p}$  in  $E_k$  und eine Komponente  $\mathbf{q}$  senkrecht dazu:

$$\mathbf{x} = \mathbf{p} + \mathbf{q}, \quad \mathbf{p} \text{ in } E_k, \quad \mathbf{q} \perp E_k.$$

Sind  $\xi_1, \dots, \xi_n$  die rechtwinkligen Koordinaten von  $\mathbf{x}$ , so haben  $\mathbf{p}$  und  $\mathbf{q}$  die Koordinaten  $(\xi_1, \dots, \xi_k, 0, \dots, 0)$  und  $(0, \dots, 0, \xi_{k+1}, \dots, \xi_n)$ . Die Zerlegung

$$\xi_1^2 + \dots + \xi_n^2 = (\xi_1^2 + \dots + \xi_k^2) + (\xi_{k+1}^2 + \dots + \xi_n^2)$$

ergibt direkt den „Pythagoras“

$$N\mathbf{x} = N\mathbf{p} + N\mathbf{q}.$$

Die Vektoren  $\mathbf{y}$ , die sich ganzzahlig durch die Basisvektoren  $\mathbf{e}_1, \dots, \mathbf{e}_n$  ausdrücken:

$$\mathbf{y} = \mathbf{e}_1 y_1 + \dots + \mathbf{e}_n y_n$$

heissen *Gitterpunkte* oder *Gittervektoren*. Wir bezeichnen mit  $\mathbf{x}, \mathbf{p}, \mathbf{q}, \dots$  beliebige Punkte des Raumes, mit  $\mathbf{y}, \mathbf{s}, \dots$  Gitterpunkte.

Das Volumen  $V_n$  der *Gittermasche*, d. h. des von  $\mathbf{e}_1, \dots, \mathbf{e}_n$  aufgespannten Parallelotops, ist die Determinante der rechtwinkligen Koordinaten (6) der Vektoren  $\mathbf{e}_k$ . Da in dieser Determinante unterhalb der Hauptdiagonale lauter Nullen stehen, erhält man

$$V_n = h_1 h_2 \dots h_n. \quad (9)$$

Das Volumen der  $(n-1)$ -dimensionalen Gittermasche, die von  $\mathbf{e}_1, \dots, \mathbf{e}_{n-1}$  im Teilraum  $E_{n-1}$  aufgespannt wird, ist ebenso

$$V_{n-1} = h_1 h_2 \dots h_{n-1}. \quad (10)$$

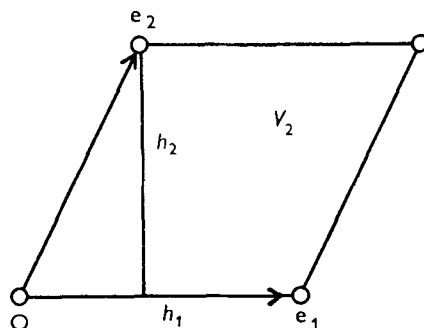


Fig. 2.

Aus (9) und (10) folgt  $V_n = V_{n-1}h_n$ , wie es nach der Elementargeometrie auch sein soll; denn  $V_{n-1}$  ist die Basis und  $h_n$  die Höhe der Gittermasche  $V_n$ . Aus (5) und (9) folgt ferner

$$D_n = (h_1 \dots h_n)^2 = V_n^2 \quad (11)$$

und ebenso für jedes  $k$

$$D_k = (h_1 \dots h_k)^2 = V_k^2. \quad (12)$$

### § 3. Reduktion

**SATZ 3.** In jeder nicht leeren Menge von Gittervektoren gibt es einen kürzesten.

*Beweis:* Sei  $\mathbf{y}'$  ein Gittervektor in der Menge. Wir betrachten alle Gittervektoren  $\mathbf{y}$  der Menge, die gleich lang oder kürzer als  $\mathbf{y}'$  sind:

$$|\mathbf{y}| \leq |\mathbf{y}'| = R.$$

Die Quadratsumme der rechtwinkligen Koordinaten  $\eta_1, \dots, \eta_n$  von  $\mathbf{y}$  ist  $\leq R^2$ , also ist jede Koordinate dem Betrage nach höchstens gleich  $R$ . Die Gitterkoordinaten  $y_1, \dots, y_n$  sind nach (4) lineare Funktionen der  $\eta_i$ ; also sind auch sie dem Betrage nach beschränkt. Da die  $y_j$  ganze Zahlen sein müssen, gibt es für jede von ihnen nur endlich viele Möglichkeiten, also kommen nur endlich viele Vektoren  $\mathbf{y}$  in Betracht. Unter diesen kann man einen kürzesten aussuchen.

**DEFINITION.** Die Gitterbasis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  heisst *reduziert* in Bezug auf die Metrik, wenn folgende Bedingungen erfüllt sind:

- 1)  $\mathbf{e}_1$  ist der kürzeste unter allen primitiven Gittervektoren;
- 2)  $\mathbf{e}_k$  ist der kürzeste unter allen Gittervektoren, die mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System bilden ( $k = 2, 3, \dots, n$ ).

Dass es in jedem Gitter eine reduzierte Basis gibt, ist leicht einzusehen. Nach Satz 3 gibt es nämlich einen kürzesten primitiven Gittervektor  $\mathbf{e}_1$ . Nach Satz 1 kann man dazu

einen Gittervektor  $\mathbf{e}_2$  finden, der mit  $\mathbf{e}_1$  ein primitives Paar bildet. Nach Satz 3 gibt es unter diesen  $\mathbf{e}_2$  einen kürzesten. Nach Satz 2 kann man zu  $\mathbf{e}_1$  und  $\mathbf{e}_2$  ein  $\mathbf{e}_3$  finden, etc.

Das Ergebnis gilt nicht nur für quadratische, sondern für beliebige definite Metriken mit beschränktem Eichkörper.

Nach Korollar 1 und 2 (§ 1) kann man die Bedingungen 1) und 2) auch so formulieren:

- 1)  $\mathbf{e}_1$  ist der kürzeste unter den Vektoren  $\mathbf{s} = \mathbf{e}_1 s_1 + \dots + \mathbf{e}_n s_n$  mit  $(s_1, \dots, s_n) = 1$ ,
- 2)  $\mathbf{e}_k$  ist der kürzeste unter den Vektoren  $\mathbf{s}$  mit  $(s_k, \dots, s_n) = 1$  ( $k = 2, 3, \dots, n$ ).

Die Bedingung  $(s_k, \dots, s_n) = 1$  schliesst natürlich ein, dass die  $s_k, \dots, s_n$  nicht alle Null sind.

Quadriert man die Längen der Vektoren  $\mathbf{s}$  und führt die Form  $f(\mathbf{s}) = N\mathbf{s}$  ein, so kann man die Bedingungen auch so formulieren:

$$f(\mathbf{e}_k) \leq f(\mathbf{s}) \text{ für alle Gittervektoren } \mathbf{s} \text{ mit } (s_k, \dots, s_n) = 1,$$

oder ganz arithmetisch:

$$f_{kk} \leq f(s_1, \dots, s_n) \text{ für alle ganzen Zahlen } s_1, \dots, s_n \text{ mit } (s_k, \dots, s_n) = 1. \quad (13)$$

Eine quadratische Form  $f$ , die alle Bedingungen (13) erfüllt, heisst nach Minkowski *reduziert*. Wir sehen also: *Wenn die Gitterbasis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  in Bezug auf die durch  $f$  definierte Metrik reduziert ist, so ist die Form  $f$  reduziert und umgekehrt.*

Minkowski verlangt von einer reduzierten Form auch noch die Normierung

$$f_{k,k+1} \geq 0,$$

aber davon wollen wir vorläufig absehen.

Geht man von der Gitterbasis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  auf eine neue Basis desselben Gitters über:

$$\mathbf{e}'_k = \sum \mathbf{e}_j t_{jk},$$

so transformieren die Gitterkoordinaten  $x_1, \dots, x_n$  eines Vektors  $\mathbf{x}$  sich nach einer ganzzahligen, ganzzahlig umkehrbaren Transformation

$$x_j = \sum t_{jk} x'_k \quad (14)$$

und die Form  $f(x)$  wird in eine äquivalente Form  $f'(x')$  transformiert:

$$f(x) = f'(x').$$

Unter einer *Transformation*  $T$  verstehen wir im folgenden immer eine ganzzahlige, ganzzahlig umkehrbare Transformation (14). Die Matrix  $(t_{jk})$  bezeichnen wir ebenfalls mit  $T$ . Ihre Determinante ist  $\pm 1$ .

Wir haben gesehen, dass es zu jeder Gitterbasis  $(\mathbf{e}_1, \dots, \mathbf{e}_n)$  eine reduzierte Basis  $(\mathbf{e}'_1, \dots, \mathbf{e}'_n)$  desselben Gitters gibt. Also gibt es zu jeder positiven Form  $f$  eine äquivalente reduzierte Form  $f'$ . Damit haben wir den

**SATZ 4.** *In jeder Klasse von äquivalenten positiven Formen gibt es reduzierte Formen.*

Die Reduktionsbedingungen (13) sind lineare homogene Ungleichungen für die Koeffizienten  $f_{jk}$ . Einige von diesen Ungleichungen wollen wir gleich aufschreiben. Setzt man in (13) ein  $s_j$  gleich Eins und die übrigen Null, so erhält man

$$f_{11} \leq f_{22} \leq \dots \leq f_{nn}. \quad (15a)$$

Setzt man andererseits  $s_j$  und  $s_k$  gleich  $\pm 1$  und die übrigen Null, so erhält man

$$f_{kk} \leq f_{jj} \pm f_{jk} + f_{jk} \quad (j < k)$$

oder

$$\pm f_{jk} \leq f_{jj} \quad (j < k)$$

bei jeder Wahl des Vorzeichens. Man kann dafür auch schreiben

$$|f_{jk}| \leq f_{jj} \quad \text{für } j < k. \quad (15b)$$

#### § 4. Ungleichungen für binäre, ternäre und quaternäre reduzierte Formen

Für binäre Formen kann man die Ungleichungen (15 a–b) so schreiben

$$|f_{12}| \leq f_{11} \leq f_{22}.$$

Daraus erhält man sofort eine untere Schranke für die Diskriminante  $D_2$ , nämlich

$$D_2 = f_{11} f_{22} - \frac{1}{4} f_{12}^2 \geq f_{11} f_{22} - \frac{1}{4} f_{11}^2.$$

Vergrößert man die Abschätzung, indem man  $f_{11}^2$  durch  $f_{11} f_{22}$  ersetzt, so erhält man die bekannte Ungleichung

$$D_2 \geq \frac{3}{4} f_{11} f_{22}. \quad (16)$$

Eine ähnliche Ungleichung für ternäre reduzierte Formen hat Seeber experimentell gefunden und Gauss bewiesen. Sie lautet

$$D_3 \geq \frac{1}{2} f_{11} f_{22} f_{33}. \quad (17)$$

Weitere Beweise gaben Dirichlet (*Werke* II, S. 29), Hermite (*Œuvres* I, S. 94), Korkine und Zolotareff (*Œuvres de Zolotareff* I, S. 125), Selling (*J. f. d. reine u. ang. Math.* 77, S. 143), Minkowski (*Ges. Abh.* II, S. 27) und Mahler [2].

Für reduzierte quaternäre Formen gilt die Ungleichung

$$D_4 \geq \frac{1}{4} f_{11} f_{22} f_{33} f_{44}, \quad (18)$$

die K. Mahler [3] zuerst ausdrücklich formuliert und bewiesen hat. Wir werden sie später aus allgemeinen Sätzen neu herleiten.

Für beliebige  $n$  gilt eine ähnliche Ungleichung: die „fundamentale Ungleichung der Reduktionstheorie“ (§ 7).

### § 5. Sukzessive Minima

$N_1$  sei die Norm eines kürzesten von Null verschiedenen Gittervektors  $\mathbf{s}_1$ . Ebenso sei  $N_2$  die Norm eines kürzesten von  $\mathbf{s}_1$  linear unabhängigen Gittervektors  $\mathbf{s}_2$ . Allgemein sei  $N_k$  rekursiv definiert als Norm eines kürzesten von  $\mathbf{s}_1, \dots, \mathbf{s}_{k-1}$  linear unabhängigen Gittervektors.

Man nennt  $N_1, N_2, N_3, \dots$  die *sukzessiven Minima* der Form  $f$ .

Man kann die Minima  $N_1, N_2, \dots$  auch unabhängig von der Wahl der Vektoren  $\mathbf{s}_1, \mathbf{s}_2, \dots$  definieren, nämlich so:

$N_k$  ist die kleinste reelle Zahl  $N'$ , für die es  $k$  linear unabhängige Gittervektoren mit Normen  $\leq N'$  gibt.

Diese Definition ist offensichtlich mit der vorigen äquivalent.

Die  $\mathbf{s}_k$  brauchen keine Basis für das ganze Gitter zu bilden. Für  $n = 1, 2$  und  $3$  sind sie es wohl, aber für  $n = 4$  gibt es eine Ausnahme, wie wir später sehen werden. Für  $n > 4$  bilden die Minimalvektoren  $\mathbf{s}_k$  in der Regel keine Gitterbasis.

Für das erste Minimum  $N_1 = f_{11}$  gilt eine von Hermite herrührende, von Minkowski und Blichfeldt verschärfte Ungleichung<sup>1</sup>

$$N_1^n \leq \mu_n D_n. \quad (19)$$

*Beweis* (nach Minkowski): Der kleinste Abstand zwischen zwei Gitterpunkten ist  $d = \sqrt{N_1}$ . Beschreibt man um jeden Gitterpunkt eine Kugel mit Radius  $r = \frac{1}{2} d$ , so haben diese Kugeln nur Randpunkte gemeinsam. Von der Kugel um den Nullpunkt liegt ein

---

<sup>1</sup> Für Literatur siehe etwa den Enzyklopädieartikel von O.-H. KELLER. Die genauen Minimalwerte von  $\mu_n$  kennt man nur für  $n \leq 10$ :

$$\mu_2 = \frac{4}{3}, \mu_3 = 2, \mu_4 = 4, \mu_5 = 8, \mu_6 = \frac{64}{3}, \mu_7 = 64, \mu_8 = 256, \mu_9 = 512, \mu_{10} = \frac{4096}{3}.$$

$\mu_2$  wurde von HERMITE bestimmt, aber  $\mu_2$  und  $\mu_3$  waren vorher schon GAUSS bekannt, denn die Ungleichung (19) folgt für  $n = 2$  aus (16) und für  $n = 3$  aus (17). Für  $\mu_4$  und  $\mu_5$  siehe KORKINE-ZOLOTAREFF [1] und [3]. Für  $\mu_6, \mu_7$  und  $\mu_8$  siehe BLICHFELDT [4], [5], [6] und [7], für  $\mu_9$  und  $\mu_{10}$  T. W. CHAUNDY. Die Beweise von CHAUNDY scheinen aber nicht ganz vollständig zu sein (siehe das Referat von Coxeter in *Math. Rev.*, 8 (1947), 137).

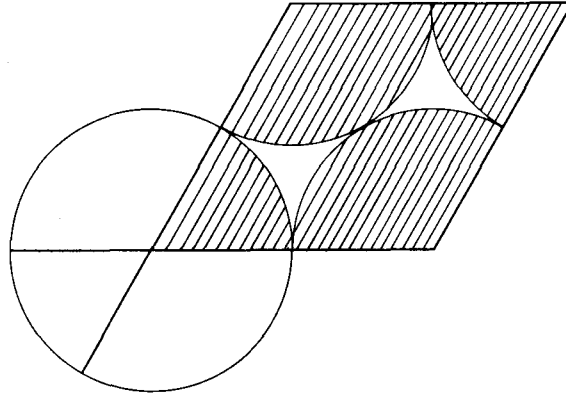


Fig. 3.

Teil in der Gittermasche  $0 \leq x_i < 1$ , die übrigen Teile in verschobenen Gittermaschen  $s_i \leq x_i < s_i + 1$ . Verschiebt man nun alle Teile in die Gittermasche  $0 \leq x_i < 1$  hinein, so haben die verschobenen Teile nur Randpunkte gemeinsam. Der Inhalt der Kugel ist gleich der Summe der Inhalte der Teile, also höchstens gleich dem Inhalt der Gittermasche  $V_n$ . Rechnet man den Kugelinhalt aus, so erhält man eine Ungleichung (19) mit

$$\mu_n = \left(\frac{4}{\pi}\right)^n \left\{ \Gamma\left(\frac{n}{2} + 1\right) \right\}^2.$$

Blichfeldt [1] hat diese Schranke zu

$$\mu_n = \left(\frac{2}{\pi}\right)^n \left\{ \Gamma\left(2 + \frac{n}{2}\right) \right\}^2$$

verbessert. Eine Vereinfachung des Blichfeldtschen Beweises gab Remak [1]. Für weitere Verschärfungen siehe Blichfeldt [2] und [3].

Mordell hat bewiesen  $\mu_n \leq \mu_{n-1}^{n/(n-1)}$  mit Gleichheit für  $n=4$  und  $8$ .

Aus (19) folgt die *Ungleichung von Minkowski*

$$N_1 N_2 \dots N_n \leq \mu_n D_n. \quad (20)$$

*Beweis* (nach H. Minkowski, *Geometrie der Zahlen*, § 51): Es seien  $\mathbf{s}_1, \dots, \mathbf{s}_n$  linear unabhängige Gittervektoren mit Normen  $N_{\mathbf{s}_k} = N_k$ . Jeder Vektor  $\mathbf{z}$  des Raumes  $E_n$  kann als Linearkombination von  $\mathbf{s}_1, \dots, \mathbf{s}_n$  dargestellt werden:

$$\mathbf{z} = \mathbf{s}_1 z_1 + \dots + \mathbf{s}_n z_n.$$

Die Norm von  $\mathbf{z}$  ist eine quadratische Form in den  $z_i$ , die wieder als Quadratsumme geschrieben werden kann:

$$N\mathbf{z} = g(z_1, \dots, z_n) = \zeta_1^2 + \dots + \zeta_n^2,$$

wobei  $\zeta_k, \dots, \zeta_n$  Funktionen von  $z_k, \dots, z_n$  allein sind. Wir bilden nun die neue Form

$$f'(x_1, \dots, x_n) = g'(z_1, \dots, z_n) = N_1^{-1} \cdot \zeta_1^2 + \dots + N_n^{-1} \cdot \zeta_n^2.$$

In der neuen, durch  $f'(x)$  definierten Metrik hat kein Gittervektor ausser dem Nullvektor eine Norm  $< 1$ . Ist nämlich  $\mathbf{z}$  ein Gittervektor  $\neq 0$  und ist  $\zeta_k$  die letzte von Null verschiedene unter den  $\zeta_1, \dots, \zeta_n$ , so ist der Vektor  $\mathbf{z}$  von  $\mathbf{s}_1, \dots, \mathbf{s}_{k-1}$  linear unabhängig; sonst wären nämlich  $z_k, \dots, z_n$  Null und daher  $\zeta_k, \dots, \zeta_n$  auch. Somit hat  $\mathbf{z}$  in der ursprünglichen Metrik eine Norm  $\geq N_k$ . Daraus folgt aber

$$f'(x) = g'(z) = N_1^{-1} \cdot \zeta_1^2 + \dots + N_k^{-1} \cdot \zeta_k^2 \geq N_k^{-1} \cdot (\zeta_1^2 + \dots + \zeta_k^2) \geq 1.$$

Die Diskriminante der Form  $f'(x)$  ist  $N_1^{-1} \dots N_n^{-1} D_n$ . Also ergibt (19)

$$1 \leq \mu_n N_1^{-1} \dots N_n^{-1} D_n.$$

Damit ist (20) bewiesen.

Der Koeffizient  $\mu_n$  in (20) ist derselbe wie in (19). Jede Verschärfung von  $\mu_n$  beim Problem der dichtesten gitterförmigen Kugelpackung führt also automatisch zu einer Verschärfung der Minkowskischen Ungleichung (und umgekehrt).

## § 6. Die Ungleichung von Mahler und Weyl

Zwischen den Diagonalkoeffizienten  $f_{kk}$  einer reduzierten Form  $f$  und den sukzessiven Minima  $N_k$  derselben Form  $f$  besteht immer die Beziehung

$$N_k \leq f_{kk}.$$

Das folgt unmittelbar aus der zweiten Definition von  $N_k$ , weil die Basisvektoren  $\mathbf{e}_1, \dots, \mathbf{e}_k$  linear unabhängig sind und Normen  $\leq f_{kk}$  haben.

Wir wollen nun eine Ungleichung der Form

$$f_{kk} \leq \delta_k N_k$$

herleiten, die von Mahler [1] gefunden und von Weyl [1] wiederentdeckt wurde. Dabei soll die Mahler-Weylsche Schranke  $\delta_k$  verschärft werden. Die Verschärfung gilt allerdings nur in einer quadratischen Metrik, während die Mahler-Weylsche Abschätzung in einer beliebigen Metrik gilt.

Zwei Vektoren  $\mathbf{x}$  und  $\mathbf{x}'$  heissen *kongruent* (nach dem von  $\mathbf{e}_1, \dots, \mathbf{e}_n$  aufgespannten Gitter), wenn ihre Differenz  $\mathbf{x} - \mathbf{x}' = \mathbf{y}$  ein Gittervektor ist.

Aus den Formeln (4) § 2 ergibt sich fast unmittelbar



SATZ 5. Zu jedem Vektor  $\mathbf{x}$  gibt es einen kongruenten Vektor  $\mathbf{x}' = \mathbf{x} - \mathbf{y}$ , so dass die rechtwinkligen Koordinaten  $\xi'_i$  von  $\mathbf{x}'$  dem Betrage nach höchstens gleich  $\frac{1}{2} h_i$  sind:

$$|\xi'_i| = |\xi_i - \eta_i| \leq \frac{1}{2} h_i. \quad (21)$$

Zum Beweis fängt man mit der letzten Gleichung (4) an:

$$\xi'_n = \xi_n - \eta_n = h_n(x_n - y_n),$$

und bestimmt  $y_n$  als ganze Zahl so, dass

$$-\frac{1}{2} h_n < \xi'_n \leq \frac{1}{2} h_n$$

wird. Dann bestimmt man  $y_{n-1}$  aus der vorletzten Gleichung so, dass

$$-\frac{1}{2} h_{n-1} < \xi'_{n-1} \leq \frac{1}{2} h_{n-1}$$

wird, etc. bis  $y_1$ . So ergeben sich nacheinander alle Ungleichungen (21).

Aus (21) folgt

$$N(\mathbf{x} - \mathbf{y}) = N\mathbf{x}' \leq \frac{1}{4}(h_1^2 + \dots + h_n^2). \quad (22)$$

Damit haben wir

SATZ 6. Es gibt zu jedem Punkte  $\mathbf{x}$  in  $E_n$  einen Gitterpunkt  $\mathbf{y}$  im Abstand

$$|\mathbf{x} - \mathbf{y}| \leq \frac{1}{2} \sqrt{h_1^2 + \dots + h_n^2}.$$

Diesen Hilfssatz haben auch Remak und Weyl verschiedentlich angewandt. Wir benutzen ihn zur Herleitung und Verschärfung der Ungleichung von Mahler und Weyl.

SATZ 7. Ist  $f_{kk}$  der Koeffizient von  $x_k^2$  in einer reduzierten quadratischen Form  $f$  und sind  $N_1, N_2, \dots, N_n$  die sukzessiven Minima der gleichen Form, so gilt

$$f_{kk} \leq \delta_k N_k. \quad (23)$$

Dabei werden die  $\delta_k$  durch die Rekursionsformeln

$$\delta_1 = 1, \quad \delta_k = \text{Max.} (1, \frac{1}{4} \delta_1 + \dots + \frac{1}{4} \delta_{k-1} + \frac{1}{4}) \quad (24)$$

definiert.

*Beweis:* Für  $k = 1$  ist selbstverständlich  $f_{11} = N_1$ . Es sei also  $k > 1$ . Wir betrachten das von  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  aufgespannte Gitter im linearen Raum  $E_{k-1}$ . Nach Definition von  $N_k$  gibt es  $k$  linear unabhängige Gittervektoren  $\mathbf{s}_1, \dots, \mathbf{s}_k$  mit Normen  $\leq N_k$ . Einer von diesen Vektoren, nennen wir ihn  $\mathbf{s}$ , liegt nicht in  $E_{k-1}$ . Nach Korollar 3 (§ 1) gibt es ein primitives System  $(\mathbf{e}_1, \dots, \mathbf{e}_{k-1}, \mathbf{e}^*)$  so, dass eine Gleichung der Form (1) gilt:

$$\mathbf{s} = (\mathbf{e}_1 s_1 + \dots + \mathbf{e}_{k-1} s_{k-1}) + \mathbf{e}^* m \quad (m > 0). \quad (25)$$

Soweit sind wir Weyl [1] gefolgt; jetzt geht es nach Remak [2] weiter.

Wenn  $m = 1$  ist, so bildet  $\mathbf{s}$  selbst mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System. Da  $N\mathbf{s} \leq N_k$  ist, hat auch der kürzeste Vektor, der mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System bildet, eine Norm  $\leq N_k$ . Daher hat man in diesem Fall

$$f_{kk} \leq N_k \leq \delta_k N_k. \quad (26)$$

Ist aber  $m > 1$ , so ist  $m \geq 2$ . Wir zerlegen  $\mathbf{e}^*$  in eine Komponente  $\mathbf{p}$  in  $E_{k-1}$  und eine Komponente  $\mathbf{q}$  senkrecht dazu:

$$\mathbf{e}^* = \mathbf{p} + \mathbf{q}. \quad (27)$$

Setzt man (27) in (25) ein, so erhält man eine Komponentenzerlegung von  $\mathbf{s}$ :

$$\mathbf{s} = (\mathbf{e}_1 s_1 + \dots + \mathbf{e}_{k-1} s_{k-1} + \mathbf{p} m) + \mathbf{q} m.$$

Nach Pythagoras ist

$$N\mathbf{s} \geq N(\mathbf{q} m) = m^2 N\mathbf{q} \geq 4 N\mathbf{q},$$

also

$$N\mathbf{q} \leq \frac{1}{4} N\mathbf{s} \leq \frac{1}{4} N_k.$$

In der Darstellung (25) steckt eine gewisse Willkür. Man kann nämlich, wenn  $\mathbf{y}$  ein beliebiger Gitterpunkt in  $E_{k-1}$  ist,  $\mathbf{e}^*$  durch

$$\mathbf{e}^* - \mathbf{y} = (\mathbf{p} - \mathbf{y}) + \mathbf{q} \quad (28)$$

ersetzen. Diese Willkür benutzen wir, um  $N(\mathbf{p} - \mathbf{y})$  klein zu machen. Nach Satz 6 kann man  $\mathbf{y}$  so wählen, dass

$$N(\mathbf{p} - \mathbf{y}) \leq \frac{1}{4} (h_1^2 + \dots + h_{k-1}^2) \quad (29)$$

wird. Jetzt sind in (28) beide Komponenten abgeschätzt. Nach Pythagoras wird

$$N(\mathbf{e}^* - \mathbf{y}) = N(\mathbf{p} - \mathbf{y}) + N\mathbf{q} \leq \frac{1}{4} (h_1^2 + \dots + h_{k-1}^2) + \frac{1}{4} N_k. \quad (30)$$

Der Vektor  $\mathbf{e}^* - \mathbf{y} = \mathbf{e}^* - (y_1 \mathbf{e}_1 + \dots + y_{k-1} \mathbf{e}_{k-1})$  bildet mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System, also folgt aus (30)

$$f_{kk} \leq \frac{1}{4} (h_1^2 + \dots + h_{k-1}^2) + \frac{1}{4} N_k. \quad (31)$$

Wegen (8) ist jedes  $h_j^2 \leq f_{jj}$ . Also folgt

$$f_{kk} \leq \frac{1}{4} (f_{11} + \dots + f_{k-1, k-1}) + \frac{1}{4} N_k. \quad (32)$$

Geht man nun rekursiv vor und setzt für  $f_{jj}$  mit  $j < k$  die Abschätzung (23) voraus, so folgt

$$\begin{aligned} f_{kk} &\leq \frac{1}{4} (\delta_1 N_1 + \dots + \delta_{k-1} N_{k-1}) + \frac{1}{4} N_k \\ &\leq \left( \frac{1}{4} \delta_1 + \dots + \frac{1}{4} \delta_{k-1} + \frac{1}{4} \right) N_k \leq \delta_k N_k. \end{aligned} \quad (33)$$

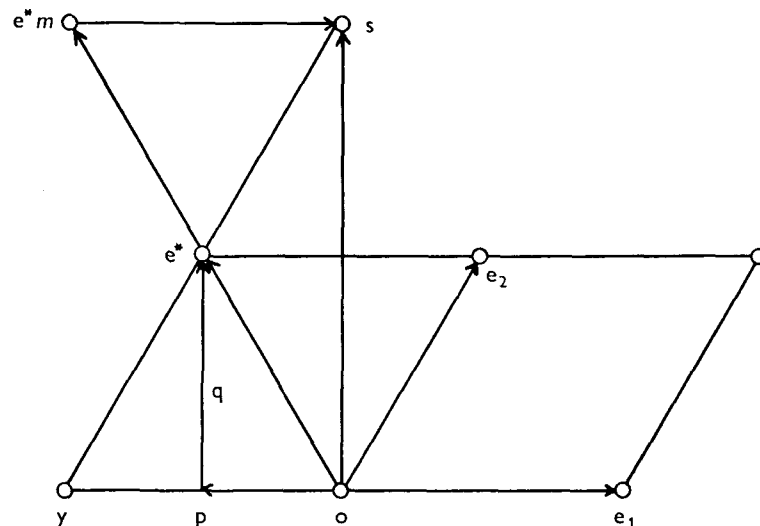


Fig. 4.

Damit ist (23) sowohl für  $m = 1$  als auch für  $m > 1$  bewiesen.

Der Grundgedanke der vorstehenden Rechnung lässt sich geometrisch so formulieren. Da  $\mathbf{s}$  einer von den Minimumvektoren  $\mathbf{s}_1, \dots, \mathbf{s}_k$  ist, ist  $N\mathbf{s}$  klein. Also ist auch die Komponente von  $\mathbf{s}$  senkrecht zu  $E_{k-1}$  klein. Die senkrechte Komponente von  $\mathbf{s}$  ist nach (25) gleich der senkrechten Komponente von  $\mathbf{e}^*$  mal  $m$ , also ist auch die senkrechte Komponente von  $\mathbf{e}^*$  klein. Die Komponente von  $\mathbf{e}^*$  in  $E_{k-1}$  ist  $\mathbf{p}$ . In der Nähe des Punktes  $\mathbf{p}$  liegt ein Gitterpunkt  $\mathbf{y}$ . Also hat  $\mathbf{e}^* - \mathbf{y}$  kleine Komponenten sowohl in  $E_{k-1}$  als senkrecht dazu; also ist  $N(\mathbf{e}^* - \mathbf{y})$  klein. Der Basisvektor  $\mathbf{e}_k$  aber hat von allen Vektoren, die mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System bilden, die kleinstmögliche Norm. Also ist  $f_{kk} \leq N(\mathbf{e}^* - \mathbf{y})$  und daraus ergibt sich die Abschätzung (31).

Die gleiche Methode, die hier auf den Vektor  $\mathbf{e}^*$  angewandt wurde, ergibt, auf irgend einen Gittervektor  $\mathbf{s}$  angewandt, folgendes:

*Es sei  $j < k$ . Wenn ein Gittervektor  $\mathbf{s} = \mathbf{p} + \mathbf{q}$  mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System bildet, wobei  $\mathbf{p}$  in  $E_j$  liegt und  $\mathbf{q}$  senkrecht dazu ist, so gilt:*

$$\begin{aligned} f_{kk} &\leq \frac{1}{4}(h_1^2 + \dots + h_j^2) + N\mathbf{q} \\ &\leq \frac{1}{4}(f_{11} + \dots + f_{j-1, j-1} + h_j^2) + N\mathbf{q}. \end{aligned}$$

Addiert man zu beiden Seiten  $N\mathbf{p}$  und subtrahiert  $f_{kk}$ , so erhält man

$$\begin{aligned} N\mathbf{p} &\leq \frac{1}{4}(f_{11} + \dots + f_{j-1, j-1} + h_j^2) + (N\mathbf{s} - f_{kk}) \\ &\leq \frac{1}{4}(\delta_1 N_1 + \dots + \delta_{j-1} N_{j-1} + h_j^2) + (N\mathbf{s} - f_{kk}). \end{aligned}$$

Sind  $\sigma_1, \dots, \sigma_n$  die rechtwinkligen Koordinaten des Vektors  $\mathbf{s}$ , so ist  $N\mathbf{p} = \sigma_1^2 + \dots + \sigma_j^2$  und man erhält

$$\begin{aligned} \sigma_1^2 + \dots + \sigma_j^2 &\leq \frac{1}{4}(f_{11} + \dots + f_{j-1, j-1} + h_j^2) + (N\mathbf{s} - f_{kk}) \\ &\leq \frac{1}{4}(\delta_1 + \dots + \delta_{j-1})N_j + \frac{1}{4}h_j^2 + (N\mathbf{s} - f_{kk}). \end{aligned} \quad (34)$$

Wegen

$$f_{11} + \dots + f_{j-1, j-1} \leq (j-1)f_{jj}$$

und

$$\frac{1}{4}\delta_1 + \dots + \frac{1}{4}\delta_{j-1} \leq \delta_j - \frac{1}{4}$$

erhält man schliesslich

$$\sigma_1^2 + \dots + \sigma_j^2 \leq \frac{j-1}{4}f_{jj} + \frac{1}{4}h_j^2 + (N\mathbf{s} - f_{kk}) \quad (35)$$

und

$$\sigma_1^2 + \dots + \sigma_j^2 \leq (\delta_j - \frac{1}{4})N_j + \frac{1}{4}h_j^2 + (N\mathbf{s} - f_{kk}) \quad (36)$$

Für  $j \leq 4$  werden wir (35) verwenden, für  $j > 4$  ist (36) etwas besser.

Die Ungleichungen (35) und (36) liefern besonders dann scharfe Schranken für  $\sigma_1, \dots, \sigma_j$ , wenn  $N\mathbf{s}$  den Minimalwert  $f_{kk}$  hat. Das letzte Glied rechts fällt dann weg und man erhält für jedes  $\sigma_j^2$  eine Schätzung von der Grössenordnung  $f_{jj}$ . Diese Schätzungsmethode stammt von Remak [2]. Wir werden sie in § 8 wieder anwenden.

## § 7. Die fundamentale Ungleichung der Reduktionstheorie

Aus der Ungleichung von Mahler folgt

$$f_{11}f_{22} \dots f_{nn} \leq \delta_1\delta_2 \dots \delta_n \cdot N_1N_2 \dots N_n. \quad (37)$$

Nach (20) war aber

$$N_1N_2 \dots N_n \leq \mu_n D_n. \quad (38)$$

Aus (37) und (38) folgt die *fundamentale Ungleichung*

$$\lambda_n f_{11}f_{22} \dots f_{nn} \leq D_n \quad (39)$$

mit

$$\lambda_n = \frac{1}{\delta_1 \delta_2 \dots \delta_n \mu_n}. \quad (40)$$

Die fundamentale Ungleichung (39) gilt natürlich auch für das von  $\mathbf{e}_1, \dots, \mathbf{e}_k$  aufgespannte  $k$ -dimensionale Gitter:

$$\lambda_k f_{11} \dots f_{kk} \leq D_k. \quad (41)$$

Wie der Beweis zeigt, gilt (41) sogar dann noch, wenn der letzte Faktor  $f_{kk}$  durch  $\delta_k N_k$  ersetzt wird:

$$\lambda_k f_{11} \cdots f_{k-1, k-1} \delta_k N_k \leq D_k. \quad (42)$$

Eine Abschätzung von  $D_k$  nach oben ergibt sich unmittelbar aus (8):

$$D_k = h_1^2 h_2^2 \cdots h_k^2 \leq f_{11} f_{22} \cdots f_{kk}. \quad (43)$$

Aus (42) und (43) folgt weiter

$$h_k^2 = \frac{D_k}{D_{k-1}} \geq \frac{\lambda_k f_{11} \cdots f_{k-1, k-1} \delta_k N_k}{f_{11} \cdots f_{k-1, k-1}} = \lambda_k \delta_k N_k.$$

Wir haben also für  $h_k^2$  die Schranken

$$\lambda_k f_{kk} \leq \lambda_k \delta_k N_k \leq h_k^2 \leq f_{kk} \leq \delta_k N_k. \quad (44)$$

Wir berechnen nun die  $\delta_k$  und  $\lambda_k$  für die niedrigsten Werte von  $k$ .

Für  $k = 1, 2, 3$  oder  $4$  erhält man aus (24) jedesmal  $\delta_k = 1$ , d. h.  $f_{kk} \leq N_k$ . Da auch  $N_k \leq f_{kk}$  war, so folgt

$$f_{kk} = N_k \quad \text{für } k \leq 4.$$

Für  $k \geq 4$  vereinfacht sich (24) zu

$$4 \delta_k = \delta_1 + \cdots + \delta_{k-1} + 1.$$

Daraus folgt, wenn beiderseits  $\delta_k$  addiert wird,

$$5 \delta_k = \delta_1 + \cdots + \delta_k + 1 = 4 \delta_{k+1},$$

also

$$\delta_k = \left(\frac{5}{4}\right)^{k-4} \quad \text{für } k \geq 4. \quad (45)$$

Für das Produkt  $\delta_1 \delta_2 \cdots \delta_k$  erhält man aus (45)

$$\delta_1 \delta_2 \cdots \delta_k = \begin{cases} 1 & \text{für } k \leq 4, \\ \left(\frac{5}{4}\right)^{\frac{1}{2}(k-3)(k-4)} & \text{für } k > 4. \end{cases} \quad (46)$$

Somit wird nach (40)

$$\lambda_n = \begin{cases} \mu_n^{-1} & \text{für } n \leq 4, \\ \mu_n^{-1} \left(\frac{5}{4}\right)^{\frac{1}{2}(n-3)(n-4)} & \text{für } n > 4. \end{cases} \quad (47)$$

Diese Schranken stammen von Remak [2].

Für  $n = 2, 3, 4$  erhält man aus (47) die bestmöglichen Schranken

$$\lambda_2 = \frac{3}{4}, \quad \lambda_3 = \frac{1}{2}, \quad \lambda_4 = \frac{1}{4}.$$

Die Extremformen, für die in (39) das Gleichheitszeichen gilt, sind äquivalent zu den folgenden reduzierten Formen (vgl. § 4 und § 16):

$$(n = 2) \quad g_2 = x_1^2 + x_2^2 + x_1 x_2,$$

$$(n = 3) \quad g_3 = x_1^2 + x_2^2 + x_3^2 + (x_1 + x_2)x_3,$$

$$(n = 4) \quad g_4 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1 + x_2 + x_3)x_4.$$

Im Beweis des Satzes 7 wurde eine Zahl  $m$  eingeführt. Nun zeigt sich, dass für  $k = 1, 2$  oder  $3$  notwendig  $m = 1$  sein muss; im Fall  $m > 1$  würde man nämlich aus (33)  $f_{kk} < N_k$  erhalten.

Für  $k = 4$  ist auch  $m = 2$  möglich, aber nur dann, wenn in allen Abschätzungen, die im Beweis benutzt wurden, das Gleichheitszeichen gilt. Es muss also  $h_1^2 = f_{11}$ ,  $h_2^2 = f_{22}$  und  $h_3^2 = f_{33}$  sein, d. h. das Gitter in  $E_3$  ist rechtwinklig. Ferner muss  $N_1 = N_2 = N_3 = N_4$  sein, d. h. das Gitter in  $E_3$  ist kubisch und der vierte Basisvektor  $\mathbf{e}_4$  hat die gleiche Länge wie die ersten drei. Sodann muss  $\mathbf{p} - \mathbf{y}$  der Vektor von einer Würfecke zum Würfelmittelpunkt sein, damit in (29) das Gleichheitszeichen gilt. So erhält man das folgende vierdimensionale Gitter (in rechtwinkligen Koordinaten)

$$\mathbf{e}_1 = (1, 0, 0, 0)$$

$$\mathbf{e}_2 = (0, 1, 0, 0)$$

$$\mathbf{e}_3 = (0, 0, 1, 0)$$

$$\mathbf{e}_4 = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

Diese 4 Basisvektoren haben die Länge 1. Es gibt aber in dem von ihnen aufgespannten Gitter noch einen Vektor  $\mathbf{s}$  der Länge Eins, der mit  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$  kein primitives System bildet, nämlich

$$\mathbf{s} = -\mathbf{e}_1 - \mathbf{e}_2 - \mathbf{e}_3 + 2\mathbf{e}_4 = (0, 0, 0, 1).$$

Die zu diesem Gitter gehörige Form ist die vorhin schon erwähnte

$$g_4 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1 + x_2 + x_3)x_4.$$

Das ist der einzige Ausnahmefall für  $k \leq 4$ , wie Julia bereits erkannt hat. *In allen andern Fällen bilden die ersten zwei, drei oder vier sukzessiven Minimumvektoren  $\mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3, \mathbf{s}_4$  automatisch ein primitives System.*

Für  $k = 5$  erhält man  $\delta_5 = \frac{5}{4}$ , also

$$f_{55} \leq \frac{5}{4} N_5.$$

Auch hier ist das Gleichheitszeichen möglich, nämlich im folgenden Fall

$$\mathbf{e}_1 = (1, 0, 0, 0, 0)$$

$$\mathbf{e}_2 = (0, 1, 0, 0, 0)$$

$$\mathbf{e}_3 = (0, 0, 1, 0, 0)$$

$$\mathbf{e}_4 = (0, 0, 0, 1, 0)$$

$$\mathbf{e}_5 = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

Die Koeffizienten der Form  $f$  sind die Skalarprodukte dieser 5 Basisvektoren. Die Form ist also

$$f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1 + x_2 + x_3 + x_4)x_5 + \frac{5}{4}x_5^2.$$

Die ersten 5 Minima sind  $N_1 = N_2 = N_3 = N_4 = N_5 = 1$ . Die Minimumvektoren  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4$  und  $\mathbf{s} = -\mathbf{e}_1 - \mathbf{e}_2 - \mathbf{e}_3 - \mathbf{e}_4 + 2\mathbf{e}_5$  bilden aber kein primitives System.

### § 8. Die Reduktionsbedingungen

Die Bedingungen für reduzierte Formen lauten nach (13):

$$f_{kk} \leq f(s_1, \dots, s_n) \quad (48)$$

für alle ganzzahligen  $s_j$  mit  $(s_1, \dots, s_n) = 1$ .

Setzt man  $s_k$  gleich 1 oder  $-1$  und alle anderen  $s$  gleich Null, so erhält man eine triviale Bedingung  $f_{kk} \leq f_{kk}$ , in der immer das Zeichen  $=$  steht. Diese trivialen Bedingungen lassen wir weg. Wenn in allen übrigen Bedingungen das Zeichen  $<$  steht, heisst die Form  $f$  *eigentlich reduziert*. Ein Beispiel ist die Form  $\sum kx_k^2$ . Im Raum der positiven Formen bilden die reduzierten Formen eine abgeschlossene Menge, die eigentlich reduzierten Formen aber eine offene Menge, wie man leicht beweist.

Eine Bedingung (48) wird gegeben durch eine Zahl  $k$  und ein System  $s$  von ganzen Zahlen  $s_1, \dots, s_n$ . Die Bedingung heisse  $B_{ks}$ . Wenn es eine reduzierte Form  $f$  gibt, für welche in der Bedingung  $B_{ks}$  das Zeichen  $=$  gilt, so wollen wir diese Bedingung *mit dem Gleichheitszeichen erfüllbar* oder kurz *erfüllbar* nennen.

Nach Bieberbach und Schur gelten die folgenden zwei Sätze:

SATZ 8. *Von allen Bedingungen  $B_{ks}$  braucht man nur die erfüllbaren zu berücksichtigen: alle übrigen folgen aus ihnen.*

SATZ 9. *Es gibt nur endlich viele erfüllbare Bedingungen  $B_{ks}$ .*

Zum Beweis des Satzes 8 dient eine topologische Überlegung, die Weyl sehr einfach dargestellt hat.

Es sei  $f_0$  eine eigentlich reduzierte Form. Gesetzt, es gäbe eine Form  $f_1$ , die alle erfüllbaren Bedingungen erfüllt und doch nicht reduziert ist. Dann verbinden wir  $f_0$  mit  $f_1$  durch eine Formenschar

$$f_t = (1 - t)f_0 + tf_1 \quad (0 \leq t \leq 1).$$

Die obere Grenze aller  $t$ , für welche die Form  $f_t$  reduziert ist, sei  $u$ . Die zu diesem Wert  $u$  gehörige Form  $f_u$  ist reduziert, weil die Menge der reduzierten Formen abgeschlossen ist. Also ist  $u < 1$ . Die Form  $f_u$  ist aber nicht eigentlich reduziert, denn sonst wäre  $f_{u+\epsilon}$  auch noch eigentlich reduziert. Also gibt es eine Bedingung  $B_{ks}$ , in der für  $f_u$  das Gleichheitszeichen steht. Diese Bedingung  $B_{ks}$  ist erfüllbar, weil die Form  $f_u$  sie mit dem Gleichheitszeichen erfüllt. Wir können die Bedingung  $B_{ks}$  als

$$L(f) \geq 0$$

schreiben, wobei  $L$  eine Linearform in den Koeffizienten der Form  $f$  ist. In dieser Bedingung  $B_{ks}$  gilt für  $f_0$  das Zeichen  $>$  und für  $f_1$  das Zeichen  $\geq$ . Nun ist

$$L(f_u) = (1 - u)L(f_0) + uL(f_1),$$

also folgt  $L(f_u) > 0$ . Früher fanden wir aber  $L(f_u) = 0$ . Wir erhalten also einen Widerspruch.

*Beweis von Satz 9:* Es sei  $B_{ks}$  eine erfüllbare Bedingung. Dann gibt es also eine reduzierte Form  $f$  mit

$$f_{kk} = f(s_1, \dots, s_n) = Ns.$$

Dafür kann man auch schreiben, wenn  $\sigma_1, \dots, \sigma_n$  die rechtwinkligen Koordinaten des Vektors  $\mathbf{s}$  sind,

$$f_{kk} = \sigma_1^2 + \dots + \sigma_n^2.$$

Daraus folgt für jedes  $j$  die Ungleichung

$$\sigma_j^2 \leq f_{kk}. \quad (49)$$

Für  $j \geq k$  folgt daraus weiter

$$\sigma_j^2 \leq f_{jj} \quad (j \geq k). \quad (50)$$

Man überzeugt sich leicht, dass für  $j = k$  die Ungleichung (50) zu

$$\sigma_k^2 < f_{kk} \quad (51)$$

verschärft werden kann.

Für  $j < k$  gilt die Ungleichung (49) zwar auch, aber sie ist nicht scharf genug, weil  $f_{kk}$  möglicherweise gross gegen  $f_{jj}$  ist. Um zu einer schärferen Ungleichung zu kommen, wenden wir (35) oder (36) an, was erlaubt ist, da  $\mathbf{s}$  mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System



bildet. Wegen  $Ns = f_{kk}$  fällt das letzte Glied rechts in (35) oder (36) weg und man erhält

$$\sigma_j^2 \leq \frac{j-1}{4} f_{jj} + \frac{1}{4} h_j^2 \quad (j < k), \quad (52)$$

$$\sigma_j^2 \leq (\delta_j - \frac{1}{4}) N_j + \frac{1}{4} h_j^2 \quad (j < k). \quad (53)$$

In den Formeln (50)–(53) können  $f_{jj}$  und  $N_j$  nach (44) durch  $\lambda_j^{-1} h_j^2$  bzw.  $(\lambda_j \delta_j)^{-1} h_j^2$  abgeschätzt werden. So erhält man

$$\sigma_j^2 \leq f_{jj} \leq \lambda_j^{-1} h_j^2 \quad (j \geq k) \quad (54)$$

$$\sigma_j^2 < \lambda_j^{-1} h_j^2 \quad (j = k) \quad (55)$$

$$\sigma_j^2 \leq \left( \frac{j-1}{4} \lambda_j^{-1} + \frac{1}{4} \right) h_j^2 \quad (j < k) \quad (56)$$

$$\sigma_j^2 \leq \left( \frac{1}{\lambda_j} - \frac{1}{4 \delta_j \lambda_j} + \frac{1}{4} \right) h_j^2 < \lambda_j^{-1} h_j^2 \quad (j < k) \quad (57)$$

Man kann (54)–(57) abschwächen zu einer einzigen Schätzung, die für beliebige  $j$  gilt:

$$\sigma_j^2 \leq \lambda_j^{-1} h_j^2 \quad (58)$$

mit dem Zeichen  $<$  für  $j \leq k$ . Setzt man noch

$$\frac{\sigma_j}{h_j} = \tau_j \quad \text{und} \quad C_j = \lambda_j^{-\frac{1}{2}}, \quad (59)$$

so kann man für (58) schreiben

$$|\tau_j| \leq C_j \quad (\text{mit } < \text{ für } j \leq k). \quad (60)$$

Will man feiner abschätzen, so verwendet man für  $j < k$  die genaueren Formeln (56) und (57). Sie ergeben (mit neuen Konstanten  $c_j$ )

$$|\tau_j| \leq c_j \quad (j < k). \quad (61)$$

Für  $j = 1, 2, 3, 4$  findet man aus (56)

$$c_1^2 = \frac{1}{4}, \quad c_2^2 = \frac{7}{12}, \quad c_3^2 = \frac{5}{4}, \quad c_4^2 = \frac{13}{4}.$$

Vom Vektor  $\mathbf{s}$  wurde nur  $f_{kk} = Ns$  vorausgesetzt. Diese Gleichung gilt aber auch für  $\mathbf{s} = \mathbf{e}_k$ . Also kann man unsere Schätzungen auch auf  $\mathbf{e}_k$  anwenden. Die rechtwinkligen Koordinaten  $\varepsilon_{jk}$  von  $\mathbf{e}_k$  sind nach (6) für  $j < k$  gleich  $h_j \beta_{jk}$ . Dividiert man sie durch  $h_j$  und wendet (61) an, so erhält man nach Remak [2]

$$|\beta_{jk}| \leq c_j. \quad (62)$$

Die Transformation von Gitterkoordinaten  $s_1, \dots, s_n$  auf rechtwinklige Koordinaten  $\sigma_j = h_j \tau_j$  ist durch (4) gegeben. Dividiert man in (4) beide Seiten durch  $h_j$ , so erhält man

$$\left. \begin{array}{l} \tau_1 = s_1 + \beta_{12} s_2 + \dots + \beta_{1n} s_n \\ \tau_2 = \quad \quad \quad s_2 + \dots + \beta_{2n} s_n \\ \dots \dots \dots \dots \dots \dots \dots \\ \tau_n = \quad \quad \quad \quad \quad \quad \quad s_n \end{array} \right\} \quad (63)$$

Die linken Seiten dieser Transformationsformeln sind nach (61) numerisch beschränkt, die Koeffizienten rechts nach (62) ebenfalls, also erhält man ohne Mühe numerische Schranken für  $|s_1|, \dots, |s_n|$ . Folglich gibt es für  $s_1, \dots, s_n$  nur endlich viele Möglichkeiten. Damit ist Satz 9 bewiesen.

Aus den Sätzen 8 und 9 folgt der *erste Endlichkeitssatz*:

SATZ 10. Die Reduktionsbedingungen (48) folgen alle aus endlich vielen unter ihnen.

### § 9. Binäre, ternäre und quaternäre Formen

Der Beweis des Satzes 10 gibt uns zugleich ein Mittel, die Schranken für die  $|s_j|$  auszurechnen und so die endlich vielen Reduktionsbedingungen  $B_{ks}$  für eine gegebene Variablenzahl  $n$  wirklich aufzuschreiben. In den Fällen  $n = 2, 3$  und  $4$  kommt man aber schneller zum Ziel, indem man nach Minkowski direkt beweist, dass für  $n \leq 4$  in den Reduktionsbedingungen

$$f_{kk} \leq f(s_1, \dots, s_n) \quad \text{für } (s_k, \dots, s_n) = 1$$

nur die Werte  $s_i = 0$  und  $\pm 1$  in Betracht zu ziehen sind. Für den Beweis siehe Minkowski, *Ges. Abh.* II, S. 78.

Für *binäre Formen* ( $n = 2$ ) erhält man die bekannten Reduktionsbedingungen

$$\left. \begin{array}{l} f_{11} \leq f_{22} \quad \quad (s_1 = 0, \quad s_2 = 1), \\ f_{22} \leq f_{11} - f_{12} + f_{22} \quad (s_1 = -1, \quad s_2 = 1), \\ f_{22} \leq f_{11} + f_{12} + f_{22} \quad (s_1 = 1, \quad s_2 = 1), \end{array} \right\} \quad (64)$$

die man zu  $|f_{12}| \leq f_{11} \leq f_{22}$  (65)

zusammenfassen kann.

Für *ternäre Formen* ( $n = 3$ ) kommen noch 9 Bedingungen mit  $s_3 = 1$  hinzu. Sie lauten

$$\left. \begin{aligned} f_{22} &\leq f_{33}, \\ |f_{13}| &\leq f_{11}, \\ |f_{23}| &\leq f_{22}, \\ -f_{12} - f_{13} - f_{23} &\leq f_{11} + f_{22}, \\ -f_{12} + f_{13} + f_{23} &\leq f_{11} + f_{22}, \\ f_{12} - f_{13} + f_{23} &\leq f_{11} + f_{22}, \\ f_{12} + f_{13} - f_{23} &\leq f_{11} + f_{22}. \end{aligned} \right\} \quad (66)$$

Für quaternäre Formen kommen zu den 3 + 9 Bedingungen (65) und (66) noch 27 Bedingungen

$$\left. \begin{aligned} f_{33} &\leq f_{44} \\ f_{44} &\leq f(s_1, s_2, s_3, 1) \quad \text{mit} \quad s_1, s_2, s_3 = 0 \quad \text{oder} \quad \pm 1 \end{aligned} \right\} \quad (67)$$

hinzu

Für Formen in 5 und 6 Variablen hat Minkowski (*Ges. Abh.* I, S. 154 und 218) ohne Beweis die in Frage kommenden Werte der  $s_j$  angegeben.

### § 10. Der zweite Endlichkeitssatz

Der zweite Endlichkeitssatz besagt, dass es nur endlich viele ganzzahlige Transformationen gibt, die im Stande sind, eine reduzierte positive Form in eine ebensolche überzuführen.

Zu den sukzessiven Minima  $N_1, N_2, \dots, N_n$  einer positiven Form  $f$  seien  $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_n$  Minimumvektoren:

$$N \mathbf{s}_k = N_k.$$

Man kann alle Vektoren des Raumes sowohl durch die  $\mathbf{s}_k$  als durch die  $\mathbf{e}_j$  ausdrücken:

$$\mathbf{x} = \sum \mathbf{s}_k z_k = \sum (\sum \mathbf{e}_j s_{jk}) z_k = \sum \mathbf{e}_j x_j, \quad (68)$$

$$x_j = \sum s_{jk} z_k, \quad (69)$$

$$N \mathbf{x} = f(x_1, \dots, x_n) = g(z_1, \dots, z_n). \quad (70)$$

Ist  $d$  die Determinante der Matrix  $(s_{jk})$ , so ist die Diskriminante der Form  $g$  gleich  $d^2 D_n$ . Man hat also nach der Ungleichung von Minkowski

$$d^2 D_n \leq N_1 N_2 \dots N_n \leq \mu_n D_n.$$

Daraus folgt

$$d^2 \leq \mu_n. \quad (71)$$

Die Umkehrung der Transformation (69) kann so geschrieben werden:

$$z_k = \sum \frac{d_{kj}}{d} x_j. \quad (72)$$

Wir betrachten nun den Vektor  $\mathbf{s} = \mathbf{s}_k$ . Seine orthogonalen Koordinaten seien  $\sigma_1, \dots, \sigma_n$ . Wir wollen Schranken für  $\sigma_j$  herleiten.

Zunächst haben wir wieder

$$\sigma_j^2 \leq \sigma_1^2 + \dots + \sigma_n^2 = N\mathbf{s} = N_k \leq f_{kk}. \quad (73)$$

Für  $j < k$  brauchen wir schärfere Schranken. Die Methode ist die gleiche, die in § 8 schon angewandt wurde. Wir vergleichen den Vektor  $\mathbf{s}$  mit

$$\mathbf{s}^* = \mathbf{s} - \mathbf{y}m, \quad (74)$$

wobei  $\mathbf{y}$  als Gittervektor in  $E_j$  gewählt wird:

$$\mathbf{y} = \mathbf{e}_1 y_1 + \dots + \mathbf{e}_j y_j. \quad (75)$$

Die natürliche Zahl  $m$  wählen wir so gross, dass  $m^2 > \mu_n$  ist. Dann folgt aus (71)  $d^2 < m^2$ .

Ich behaupte, dass der Vektor  $\mathbf{s}^*$  immer linear unabhängig von  $\mathbf{s}_1, \dots, \mathbf{s}_{k-1}$  ist, wie auch  $y_1, \dots, y_j$  gewählt werden. Um das zu zeigen, genügt es, die  $k$ -te Koordinate  $z_k^*$  des Vektors  $\mathbf{s}^* = \mathbf{s} - \mathbf{y}m$  in Bezug auf  $\mathbf{s}_1, \dots, \mathbf{s}_n$  als Koordinatenvektoren auszurechnen. Man erhält aus (72)

$$z_k^* = 1 - m \sum \frac{d_{kj}}{d} y_j. \quad (76)$$

Wäre  $z_k^* = 0$ , so hätte man

$$d = m \sum d_{kj} y_j.$$

Das ist aber unmöglich, da  $d$  nicht durch  $m$  teilbar sein kann. Also ist  $\mathbf{s}^*$  in der Tat linear unabhängig von  $\mathbf{s}_1, \dots, \mathbf{s}_{k-1}$ .

Daraus folgt wegen der Minimumeigenschaft von  $N_k = N\mathbf{s}$

$$N\mathbf{s}^* \geq N\mathbf{s}. \quad (77)$$

Wir zerlegen nun  $\mathbf{s}$  in eine Komponente  $\mathbf{p}$  in  $E_j$  und eine Komponente  $\mathbf{q}$  senkrecht dazu:

$$\mathbf{s} = \mathbf{p} + \mathbf{q},$$

$$N\mathbf{s} = N\mathbf{p} + N\mathbf{q}.$$

Die entsprechende Zerlegung für  $\mathbf{s}^*$  lautet

$$\begin{aligned}\mathbf{s}^* &= (\mathbf{p} - \mathbf{y}m) + \mathbf{q}, \\ N\mathbf{s}^* &= N(\mathbf{p} - \mathbf{y}m) + N\mathbf{q}.\end{aligned}$$

Die Ungleichung (77) ergibt nun

$$N(\mathbf{p} - \mathbf{y}m) \geq N\mathbf{p}. \quad (78)$$

Nach Satz 6 kann man  $\mathbf{y}$  so wählen, dass

$$N(\mathbf{p}m^{-1} - \mathbf{y}) \leq \frac{1}{4}(h_1^2 + \dots + h_j^2)$$

oder

$$N(\mathbf{p} - \mathbf{y}m) \leq \frac{m^2}{4}(h_1^2 + \dots + h_j^2) \quad (79)$$

wird. Aus (78) und (79) folgt

$$\begin{aligned}N\mathbf{p} &\leq \frac{m^2}{4}(h_1^2 + \dots + h_j^2), \\ &\leq \frac{m^2}{4}(f_{11} + \dots + f_{jj}) \leq \frac{m^2 j}{4}f_{jj}.\end{aligned} \quad (80)$$

Aus (73) folgt

$$\sigma_j^2 \geq f_{kk} \quad (j \geq k) \quad (81)$$

und aus (80)

$$\sigma_j^2 \leq \frac{m^2 j}{4}f_{jj} \quad (j < k). \quad (82)$$

Damit haben wir die gewünschten Schranken gefunden. Aus ihnen erhält man, genau wie im Beweis von Satz 9, Schranken für  $|s_{1k}|, \dots, |s_{nk}|$ . Also folgt:

**SATZ 11.** *Es gibt nur endlich viele Möglichkeiten für die Matrix  $S = (s_{jk})$ .*

Aus Satz 11 folgt fast unmittelbar der zweite *Endlichkeitssatz*:

**SATZ 12.** *Wenn eine Transformation  $T$  eine reduzierte Form  $f$  in eine reduzierte Form  $f'$  überführt, so gibt es für ihre Matrix  $T$  nur endlich viele Möglichkeiten.*

*Beweis:* Die lineare Transformation  $T$  möge die reduzierte Gitterbasis  $(\mathbf{e}_1, \dots, \mathbf{e}_n)$  in die reduzierte Basis  $(\mathbf{e}'_1, \dots, \mathbf{e}'_n)$  überführen. Die Koordinaten eines Vektors  $\mathbf{x}$  in Bezug auf die Basen  $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ ,  $(\mathbf{s}_1, \dots, \mathbf{s}_n)$  und  $(\mathbf{e}'_1, \dots, \mathbf{e}'_n)$  seien  $x_i, z_k$  und  $x'_j$ . Dann ist

$$\begin{aligned}x_i &= \sum s_{ik} z_k, \\ x'_j &= \sum s'_{jk} z_k.\end{aligned}$$

Die Matrix der Transformation  $T$  ist also  $S'S^{-1}$ . Nach Satz 11 gibt es dafür nur endlich viele Möglichkeiten.

## TEIL II

## § 11. Der Bereich der reduzierten Formen

Bisher haben wir uns auf positive Formen  $f$  beschränkt. Jetzt betrachten wir beliebige quadratische Formen  $f$  und beweisen zunächst

**SATZ 13.** *Jede Form  $f$ , welche die Reduktionsbedingungen  $B_{ks}$  erfüllt, ist positiv definit oder halbdefinit. Für positive reduzierte Formen ist  $f_{11} > 0$ , für halbdefinite  $f_{11} = 0$ .*

Zum Beweis kann die gleiche topologische Überlegung dienen, die im Beweis des Satzes 8 schon verwendet wurde. Es sei  $f_0$  eine eigentlich reduzierte positive Form und  $f_1$  eine Form, die alle Bedingungen  $B_{ks}$  erfüllt. Die obere Grenze aller  $t \leq 1$ , für welche die Form

$$f_t = (1-t)f_0 + tf_1$$

positiv und reduziert ist, sei  $u$ . Die Form  $f_u$  ist als Limes von positiven Formen zumindest halbdefinit. Ferner erfüllt sie alle Reduktionsbedingungen, insbesondere die Bedingung  $f_{11} \geq 0$ . Wenn  $u < 1$  ist, so gilt in allen diesen Bedingungen sogar das Zeichen  $>$ ; insbesondere ist dann  $f_{11} > 0$ .

Wir unterscheiden nun 2 Fälle:

*Fall 1.*  $f_{11} = 0$ . Dann ist nach dem eben Gesagten  $u = 1$  und die Form  $f_1 = f_u$  ist halbdefinit.

*Fall 2.*  $f_{11} > 0$ . Die Ungleichung (19):

$$f_{11}^n \leq \mu_n D_n$$

gilt für die positiven reduzierten Formen  $f_t$ , also auch im Limes für  $t = u$ . Daraus folgt  $D_n > 0$ , also ist die Form  $f_u$  positiv. Wäre  $u < 1$ , so wäre die Form  $f_u$  eigentlich reduziert; dann wäre aber  $f_{u+\varepsilon}$  für genügend kleine  $\varepsilon$  auch noch positiv und reduziert, was der Definition von  $u$  als oberer Grenze widerspricht. Also ist  $u = 1$  und die Form  $f_1 = f_u$  ist positiv.

Damit ist Satz 13 bewiesen.

Alle Formen, welche die Bedingungen  $B_{ks}$  erfüllen, nennen wir *reduziert*. Die quadratischen Formen bilden einen linearen Raum von der Dimension  $N = \frac{n(n+1)}{2}$ . Die reduzierten Formen bilden in diesem Raum eine Zelle  $Z$ , die sich vom Nullpunkt aus kegelförmig ins Unendliche erstreckt. Sie wird nach Satz 10 durch endlich viele Ungleichungen

$$L_1(f) \geq 0, \dots, L_r(f) \geq 0 \tag{83}$$

definiert.

Die Zelle  $Z$  geht in ein beschränktes Polyeder  $P$  über, wenn die Formen  $f$  durch

$$f_{11} + f_{22} + \cdots + f_{nn} = 1$$

normiert werden. Bei dieser Normierung werden nämlich wegen den Reduktionsbedingungen

$$|f_{jk}| \leq f_{kk} \leq f_{11} + \cdots + f_{nn}$$

alle Koeffizienten einer reduzierten Form beschränkt. Das Polyeder  $P$  liegt in dem  $(N-1)$ -dimensionalen Teilraum  $f_{11} + \cdots + f_{nn} = 1$ . Durch Projektion des Polyeders  $P$  vom Nullpunkt aus erhält man wieder die Zelle  $Z$ .

Eine *Seite* der Zelle  $Z$  erhält man, wenn man in einigen Ungleichungen (83) das Zeichen  $\geq$  durch  $=$  ersetzt. Die Dimension einer solchen Seite kann von 1 bis  $N-1$  variieren. Die eindimensionalen Seiten heissen *Kanten*; sie entsprechen den Ecken des Polyeders  $P$ . Die  $(N-1)$ -dimensionalen Seiten heissen *Wände*.

Auf einer Wand  $W_i$  kann nur eine einzige Gleichung  $L_i(f) = 0$  gelten. Wir numerieren diese Wandgleichungen  $L_i(f) = 0$  und die entsprechenden Ungleichungen  $L_i(f) \geq 0$  sowie die Wände  $W_i$ , zu denen sie gehören, von 1 bis  $q$ . Die übrigen Ungleichungen (83) erhalten dann Nummern von  $q+1$  bis  $r$ .

Nun ist leicht zu sehen, dass die Ungleichung  $L_{q+1}(f) \geq 0$  entbehrlich ist: sie ist eine Folge der übrigen. Sonst würde es nämlich eine Form  $f_1$  geben, welche die Ungleichung  $L_{q+1} \geq 0$  nicht erfüllt, wohl aber alle übrigen. Die Gleichung  $L_{q+1} = 0$  definiert, zusammen mit den Ungleichungen (83), eine Seite  $S_d$  von  $Z$  von einer Dimension  $d < N-1$ . Wir wählen nun eine eigentlich reduzierte Form  $f_0$  so, dass die Strecke

$$f_t = (1-t)f_0 + tf_1 \quad (0 \leq t \leq 1) \quad (84)$$

die Seite  $S_d$  nicht trifft, was wegen  $d < N-1$  immer möglich ist. Nun wäre  $L_{q+1}(f_0) > 0$  und  $L_{q+1}(f_1) < 0$ , also gäbe es ein  $t$  zwischen 0 und 1 mit  $L_{q+1}(f_t) = 0$ , also würde die Strecke (84) die Seite  $S_d$  doch treffen.

Nachdem man die Ungleichung  $L_{q+1} \geq 0$  aus (83) weggelassen hat, kann man auch die nächste  $L_{q+2} \geq 0$  streichen, usw., bis nur noch die Wandgleichungen

$$L_1(f) \geq 0, \dots, L_q(f) \geq 0 \quad (85)$$

übrig bleiben.

Für einen Randpunkt  $f$  der Zelle  $Z$  gilt in mindestens einer Ungleichung (85) das Gleichheitszeichen. Würde nämlich überall das Grösserzeichen gelten, so würde in einer Umgebung von  $f$  auch noch das Grösserzeichen gelten und  $f$  wäre innerer Punkt. Also haben wir

SATZ 14. Die Wandungleichungen (85) definieren die Zelle  $Z$ . Jeder Randpunkt von  $Z$  liegt auf mindestens einer Wand.

## § 12. Die transformierten Zellen $TZ$

Eine ganzzahlige Transformation  $T$  führt die Zelle  $Z$  in eine transformierte Zelle  $TZ$  über, die mit  $Z$  positive Formen gemeinsam haben kann. Ist etwa  $f$  eine solche positive Form, die zu  $Z$  und zu  $TZ$  gehört, so ist  $f = Tg$ , wobei  $g$  wieder zu  $Z$  gehört. Die Transformation  $T$  führt dann die reduzierte positive Form  $g$  in die reduzierte positive Form  $f$  über. Umgekehrt, wenn eine Transformation  $T$  diese Eigenschaft hat, so haben  $Z$  und  $TZ$  die Form  $f = Tg$  gemeinsam. Die Frage nach den transformierten Zellen  $TZ$ , die mit  $Z$  Punkte gemeinsam haben, ist also gleichbedeutend mit der Frage nach den Transformationen  $T$ , die mindestens eine reduzierte positive Form in eine ebensolche Form überführen.

Nach Satz 12 gibt es nur endlich viele solche Transformationen  $T$ . Unter ihnen sind zunächst die  $2^n$  Umkehrtransformationen

$$x'_k = \pm x_k$$

hervorzuheben, welche die Zelle  $Z$  auf sich selbst abbilden.

Andere Transformationen als die Umkehrtransformationen können niemals eine eigentlich reduzierte Form  $f$  in eine reduzierte Form überführen. Bei einer eigentlich reduzierten Form sind nämlich die Vektoren  $\mathbf{e}_1, \dots, \mathbf{e}_n$  der Reihe nach bis auf Faktoren  $\pm 1$  eindeutig bestimmt, da es ausser  $\mathbf{e}_k$  und  $-\mathbf{e}_k$  keine Vektoren gleicher Länge gibt, die mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System bilden. Also gilt

SATZ 15. Ist  $T$  eine Umkehrtransformation, so fällt  $TZ$  mit  $Z$  zusammen. In allen anderen Fällen haben  $Z$  und  $TZ$  nur Randpunkte gemeinsam. Es gibt nur endlich viele transformierte Zellen  $TZ$ , die mit  $Z$  positive Formen  $f$  gemeinsam haben.

KORROLAR 1. Es gibt nur endlich viele transformierte Zellen  $TZ$ , die mit einer gegebenen transformierten Zelle  $T_0Z$  positive Formen gemeinsam haben.

Hat nämlich  $TZ$  mit  $T_0Z$  eine positive Form  $f$  gemeinsam, so hat  $T_0^{-1}TZ$  mit  $Z$  die Form  $T_0^{-1}f$  gemeinsam.

KORROLAR 2. Eine positive Form  $f$  gehört nur endlich vielen transformierten Zellen an.

Beweis: Nach Satz 4 ist  $f = T_0g$ , wobei  $g$  reduziert ist. Also gehört  $f$  der transformierten Zelle  $T_0Z$  an. Jetzt folgt die Behauptung aus Korrolar 1.

SATZ 16. Jeder Randpunkt von  $Z$  gehört mindestens einer weiteren Zelle  $TZ$  an.



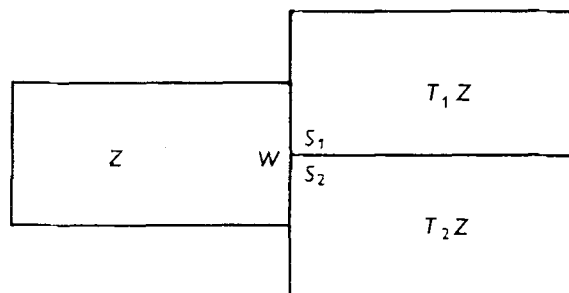


Fig. 5.

*Beweis:* Ist  $f$  ein Randpunkt von  $Z$ , so gilt in mindestens einer nicht trivialen Bedingung  $B_{ks}$  das Gleichheitszeichen:

$$f_{kk} = f(s_1, \dots, s_n).$$

Das bedeutet, dass es ausser  $\mathbf{e}_k$  und  $-\mathbf{e}_k$  noch mindestens einen weiteren Vektor kleinster Länge  $\mathbf{e}'_k$  gibt, der mit  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  ein primitives System bildet. Von  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}, \mathbf{e}'_k$  ausgehend, kann man eine reduzierte Basis  $(\mathbf{e}_1, \dots, \mathbf{e}_{k-1}, \mathbf{e}'_k, \dots, \mathbf{e}'_n)$  konstruieren, die aus  $\mathbf{e}_1, \dots, \mathbf{e}_n$  nicht nur durch eine Umkehrtransformation hervorgeht. Die Transformation  $T$ , die  $\mathbf{e}_1, \dots, \mathbf{e}_n$  in diese neue Basis überführt, führt  $f$  in eine reduzierte Form  $Tf = g$  über. Nun ist  $f = T^{-1}g$ , also gehört  $f$  dem Bereiche  $T^{-1}Z$  an. Damit ist Satz 16 bewiesen.

Wir betrachten nun eine Wand  $W$  der Zelle  $Z$ . Es gibt ausser  $Z$  selbst nur endlich viele Zellen  $T_1Z, \dots, T_rZ$ , die mit  $W$  Punkte gemeinsam haben. Die Punkte von  $W$ , die gleichzeitig zu  $T_iZ$  gehören, bilden auf  $W$  eine konvexe, abgeschlossene Menge  $M_i$ . Diese Mengen  $M_i$  überdecken  $W$  nach Satz 16.

Die  $(N-1)$ -dimensionalen unter den konvexen Mengen  $M_i$  nennen wir *Wandstücke* oder Stücke  $S_i$  der Wand  $W$ . Wenn ein Punkt  $f$  von  $W$  keinem solchen Wandstück angehören würde, wäre auch eine volle Umgebung  $U$  von  $f$  auf  $W$  zu allen Wandstücken fremd, da die Wandstücke ja abgeschlossene Mengen sind. In  $U$  könnte man einen Punkt  $g$  wählen, der keiner weniger als  $(N-1)$ -dimensionalen Menge  $M_j$  angehört. Der Punkt  $g$  würde dann überhaupt keiner Menge  $M_i$  angehören, was nicht geht. Also liegt jeder Punkt der Wand in mindestens einem Wandstück  $S_i$ .

Ein solches Stück  $S_i$  ist Teil einer Wand von  $Z$ , aber auch Teil einer Wand von  $T_iZ$ . Die Gleichung der Hyperebene, in der das Stück  $S_i$  liegt, sei  $L(f) = 0$ . Dann gehört  $L(f) \geq 0$  zu den definierenden Gleichungen von  $Z$  und  $-L(f) \geq 0$  zu den definierenden Gleichungen von  $T_iZ$ . In einer genügend kleinen Umgebung eines inneren Punktes von  $S_i$  gehören alle Punkte mit  $L(f) \geq 0$  zu  $Z$  und alle mit  $L(f) \leq 0$  zu  $T_iZ$ . Für weitere transformierte Zellen, die an  $S_i$  anstossen, ist kein Platz mehr. Also gilt

SATZ 17. Die  $(N - 1)$ -dimensionalen Wandstücke  $S_i$  überdecken die ganze Wand  $W$ . Jedes Wandstück  $S_i$  gehört genau zwei Zellen  $Z$  und  $T_i Z$  an. Alle Punkte in einer genügend kleinen Umgebung eines inneren Punktes von  $S_i$  liegen in  $Z$  oder in  $T_i Z$ .

Was für die Zelle  $Z$  gilt, gilt selbstverständlich auch für jede transformierte Zelle  $TZ$ . Auch hier stösst an jedes Wandstück genau eine weitere Zelle an.

Alle diese Sätze sind anschaulich einleuchtend. Das gleiche gilt für den folgenden

SATZ 18. Ist  $f$  eine positive Form, so überdecken die endlich vielen transformierten Zellen  $T_i Z$ , die  $f$  enthalten, eine volle Umgebung von  $f$ .

*Beweis:* Die  $f$  nicht enthaltenden Seiten der Zellen  $T_j Z$  haben eine abgeschlossene Vereinigungsmenge  $V$ . Wir wählen eine konvexe Umgebung  $U$  von  $f$ , die zu  $V$  fremd ist und nur aus positiven Formen besteht. Nun wird behauptet, dass jede Form  $f_1$  in  $U$  mindestens einer Zelle  $T Z$  angehört.

Wir wählen in  $U$  eine Form  $f_0$ , die dem Innern eines Bereiches  $T_j Z$  angehört. Wir verbinden  $f_0$  mit  $f_1$  innerhalb  $U$  durch eine Strecke

$$f_t = (1 - t)f_0 + tf_1.$$

Man kann  $f_0$  so wählen, dass die Strecke keine von den weniger als  $(N - 1)$ -dimensionalen Seiten der Zelle  $T_j Z$  trifft. Es sei  $u$  die obere Grenze der  $t$ , für welche  $f_t$  wenigstens einer der Zellen  $T_j Z$  angehört. Dann gehört  $f_u$  auch noch einer Zelle  $T_j Z$  an. Wäre  $u < 1$ , so müsste  $f_u$  einer Wand von  $T_j Z$  angehören, und zwar, da die weniger als  $(N - 1)$ -dimensionalen Seiten nicht in Betracht kommen, einem Wandstück  $S_i$ . An  $S_i$  stossen nach Satz 17 genau zwei Zellen  $T_j Z$  und  $T'_j$  an und eine volle Umgebung des Punktes  $f_u$  liegt in der Vereinigung dieser zwei Zellen. Dann wäre aber  $u$  nicht die obere Grenze. Also muss  $u = 1$  sein und der Punkt  $f_1$  gehört der Zelle  $T_j Z$  an.

Man kann Satz 18 auch so formulieren:

*Die Zellen  $TZ$  überdecken das Gebiet der positiven Formen, aber sie häufen sich nicht gegen die Punkte dieses Gebietes, sondern nur gegen den Rand, d.h. gegen die halbdefiniten Formen.*

Diesen Satz hat H. Weyl [1] durch direkte Abschätzung der Matrixelemente der Transformationen  $T$  bewiesen. Die hier befolgte Methode erscheint lehrreicher, weil sie auch bei anderen eigentlich diskontinuierlichen Transformationsgruppen angewandt werden kann. Für die hier geführten Beweise genügt es, anzunehmen, dass die Ausgangszelle  $Z$  durch vernünftige Ränder begrenzt wird, derart dass jedes  $(N - 1)$ -dimensionale Wandstück genau zwei Zellen  $Z$  und  $TZ$  voneinander trennt, während die Randteile von weniger als  $N - 1$  Dimensionen durch geeignete Verbindungswege umgangen

werden können. Diese Voraussetzungen sind in vielen Fällen erfüllt, auch wenn die Wände nicht eben sind.

**KORROLAR ZU SATZ 18.** *Eine kompakte Menge  $M$  im Gebiet der positiven Formen wird von endlich vielen Zellen  $TZ$  überdeckt.*

*Beweis:* Zu jedem Punkt von  $M$  gibt es nach Satz 18 eine Umgebung, die von endlich vielen transformierten Zellen überdeckt wird. Endlich viele von diesen Umgebungen überdecken  $M$ .

**SATZ 19.** *Jede Zelle  $TZ$  kann von  $Z$  aus erreicht werden durch eine endliche Folge von transformierten Zellen, von denen je zwei aufeinanderfolgende ein Wandstück gemeinsam haben<sup>1</sup>.*

*Beweis:* Es sei  $f$  ein innerer Punkt von  $Z$  und  $f_1$  ein innerer Punkt von  $TZ$ . Wir verbinden  $f_1$  durch Strecken mit allen Punkten einer kompakten Umgebung von  $f$ . Die Vereinigungsmenge dieser Verbindungsstrecken ist eine kompakte Menge  $M$ , die von endlich vielen Zellen  $T_iZ$  überdeckt wird. In der gewählten Umgebung von  $f$  wählen wir einen Punkt  $f_0$  derart, dass die Strecke

$$f_t = (1-t)f_0 + tf_1$$

die Seiten der  $T_iZ$  von weniger als  $(N-1)$  Dimensionen nicht trifft. Die Wände der Zellen  $T_iZ$  zerlegen dann die Strecke in endlich viele Teilstrecken, von denen jede in einer bestimmten Zelle  $T_iZ$  liegt. Daraus folgt die Behauptung.

### § 13. Der binäre Fall. Der Fundamentalbereich von Minkowski

Die Art und Weise, wie die Zellen  $TZ$  sich zu einer Parkettierung des Gebietes  $G$  der positiven Formen aneinanderschliessen, kann man sich am Beispiel der binären Formen anschaulich klarmachen. Um das Gebiet  $G$  ganz ins Endliche zu bringen, normieren wir die Formen durch

$$f_{11} + f_{22} = 1.$$

Das Gebiet  $G$  ist durch

$$f_{11}f_{22} - \frac{1}{4}f_{12}^2 > 0$$

oder

$$f_{12}^2 + (f_{22} - f_{11})^2 < (f_{11} + f_{22})^2$$

definiert. Trägt man also

$$X = f_{12} \quad \text{und} \quad Y = f_{22} - f_{11}$$

<sup>1</sup> WEYL beweist Satz 19 in [1] durch eine komplizierte vollständige Induktion.

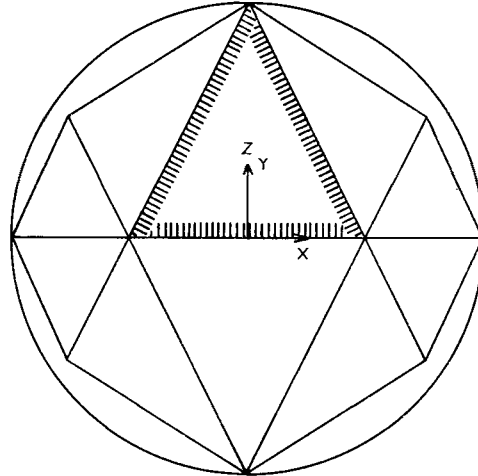


Fig. 6.

als rechtwinklige Koordinaten auf, so wird  $G$  das Innere eines Kreises

$$X^2 + Y^2 < 1.$$

Die Zelle  $Z$  wird durch die drei Geraden

$$f_{11} = f_{22}, \quad f_{12} = f_{11}, \quad -f_{12} = f_{11}$$

oder

$$Y = 0, \quad Y + 2X = 1, \quad Y - 2X = 1$$

begrenzt. Die obere Ecke ( $X = 0, Y = 1$ ) stellt die halbdefinite Form  $x_2^2$  dar, die unteren Ecken die zwei Formen

$$\frac{1}{2}(x_1^2 \pm x_1 x_2 + x_2^2).$$

Die Zelle  $Z$  ist ein Fundamentalbereich für die Gruppe der ganzzahligen Transformationen mit Determinante  $+1$ . Ein Fundamentalbereich für die Gruppe der Transformationen  $T$  mit Determinante  $\pm 1$  ist die durch  $f_{12} \geq 0$  definierte rechte Hälfte des Dreiecks.

Analog muss man im  $n$ -ären Fall, um einen Fundamentalbereich für die Gruppe aller durch ganzzahlige Transformationen induzierten Formentransformationen  $f' = Tf$  zu erhalten, die reduzierten Formen nach Minkowski durch

$$f_{k, k+1} \geq 0 \quad (k = 1, \dots, n-1)$$

normieren. Zu einem inneren Punkt des so erhaltenen Bereichs gibt es dann keine äquivalenten Punkte im Bereich mehr.

Im binären Fall kann das Dreieck  $Z$  durch eine bekannte Abbildung (Übergang vom Kleinschen zum Poincaréschen Modell der ebenen hyperbolischen Geometrie) in den

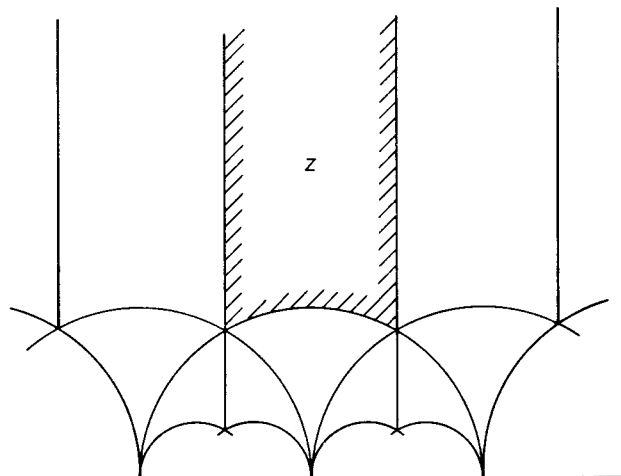


Fig. 7.

Fundamentalebene der Modulgruppe übergeführt werden. Vom Gitter ausgehend, kann man den Übergang z.B. so vollziehen: man führt nach § 2 rechtwinklige Koordinaten  $\xi_1, \xi_2$  ein und setzt

$$z = \xi_1 + i \xi_2. \quad (86)$$

Die Basisvektoren  $e_1$  und  $e_2$  des Gitters werden dann durch komplexe Zahlen  $\omega_1$  und  $\omega_2$  dargestellt. Nun bildet man den Quotienten

$$\tau = \frac{\omega_2}{\omega_1}. \quad (87)$$

Man kann immer annehmen, dass der Imaginärteil von  $\tau$  positiv ist. Der Punkt  $\tau$  liegt dann in der oberen Halbebene und durchläuft, wenn  $f$  alle reduzierten Formen durchläuft, den Fundamentalebene der Modulgruppe.

### TEIL III

#### § 14. Kantenformen und dichteste Kugelpackungen

Nach Minkowski ist die  $n$ -te Wurzel aus der Diskriminante im Gebiet der positiven Formen  $f$  eine konkave Funktion von  $f$ , d. h. wenn  $f$  und  $g$  positive Formen sind, so gilt für positive  $\lambda$  und  $\mu$

$$\sqrt[n]{D_n(\lambda f + \mu g)} \geq \lambda \sqrt[n]{D_n(f)} + \mu \sqrt[n]{D_n(g)}. \quad (88)$$

Zum Beweis transformiert Minkowski die Formen  $f$  und  $g$  gleichzeitig in Quadratsummen mit positiven Koeffizienten:

$$f = a_1 \xi_1^2 + \dots + a_n \xi_n^2, \quad g = b_1 \xi_1^2 + \dots + b_n \xi_n^2$$

und wendet die bekannte Ungleichung von Brunn-Minkowski an:

$$\sqrt[n]{(\lambda a_1 + \mu b_1)(\lambda a_2 + \mu b_2) \dots} \geq \lambda \sqrt[n]{a_1 a_2 \dots} + \mu \sqrt[n]{b_1 b_2 \dots}$$

Das Gleichheitszeichen gilt in (88) nur für  $f = cg$ .

Diesen Satz kann man anwenden um bei gegebenem Minimum  $N_1$  das Minimum der Diskriminante  $D_n$  zu bestimmen, mit anderen Worten, um in der Ungleichung (19) die schärfste Schranke  $\mu_n$  zu finden. Man kann dabei  $N_1 = 1$  annehmen. Das Problem ist gleichwertig mit dem Problem der dichtesten gitterförmigen Kugelpackung im  $n$ -dimensionalen Raum; denn wenn in einem Gitter  $N_1 \geq 1$  ist, so kann man in jedem Gitterpunkt eine Kugel mit Radius  $\frac{1}{2}$  anbringen, ohne dass die Kugeln sich durchdringen, und umgekehrt.

Um das Minimum von  $D_n$  bei  $N_1 = 1$  zu finden, genügt es offenbar, sich auf reduzierte Formen zu beschränken; denn jede positive Form ist äquivalent einer reduzierten. Man hat dann  $f_{11} = N_1 = 1$ . Es handelt sich also darum, das Minimum von  $D_n$  für reduzierte Formen mit  $f_{11} = 1$  zu bestimmen.

Unter *Kantenformen* versteht Minkowski die Formen auf den Kanten der Zelle  $Z$ . Normiert man die Kantenformen durch  $f_{11} = 1$ , so gibt es nur endlich viele Kantenformen. Nun gilt nach Minkowski

SATZ 20. *Das Minimum von  $D_n$  für reduzierte Formen mit  $f_{11} = 1$  kann nur durch eine Kantenform geliefert werden.*

*Beweis:* Gesetzt,  $D_n(f)$  wäre das Minimum und  $f$  wäre keine Kantenform. Dann wäre  $f$  innerer Punkt einer Strecke

$$f_t = (1-t)f_0 + tf_1,$$

wobei  $f_0$  und  $f_1$  beide reduziert sind und durch  $f_{11} = 1$  normiert werden können. Wir hätten dann, da  $f_0$  und  $f_1$  nicht proportional sind, in der Ungleichung (88) für  $f = f_t$  das Zeichen  $>$ :

$$\sqrt[n]{D_n(f)} > (1-t) \sqrt[n]{D_n(f_0)} + t \sqrt[n]{D_n(f_1)}.$$

Die rechte Seite wäre aber, da  $D_n(f)$  das Minimum sein sollte,  $\geq \sqrt[n]{D_n(f)}$ . Das ist ein Widerspruch.

Wegen der fundamentalen Ungleichung (39) wächst  $D_n$  ins Unendliche, sobald  $f_{nn}$  ins Unendliche wächst. Wir können uns also bei der Bestimmung des Minimums von  $D_n$  auf

einen beschränkten Teil  $f_{nn} \leq M$  der Zelle  $Z$  beschränken. In diesem beschränkten Teil hat  $D_n$  ein Minimum. Man braucht also, um das Minimum von  $D_n$  bei  $N_1 = 1$  zu finden, nur alle Kantenformen der Zelle  $Z$  mit  $f_{11} = 1$  zu durchmustern.

Jedoch nicht alle Kantenformen kommen als Extrema von  $D_n$  in Betracht, sondern nur die *Extremformen* im Sinne von Korkine und Zolotareff. Diesen wenden wir uns jetzt zu.

### § 15. Extremformen

Eine positive Form heisst *extrem*, wenn bei jeder kleinen Änderung, welche die Diskriminante  $D_n$  ungeändert lässt, das erste Minimum  $N_1$  abnimmt. Gleichwertig damit ist die Forderung, dass bei jeder kleinen Änderung, bei der  $N_1$  gleich bleibt,  $D_n$  zunimmt.

Es sei  $f$  eine Extremform mit  $N_1 = 1$ . Es seien  $\mathbf{s}^{(1)}, \mathbf{s}^{(2)}, \dots$  die endlich vielen Gittervektoren, für welche die Form ihr Minimum 1 annimmt. Dann gelten die Gleichungen

$$f(\mathbf{s}^{(1)}) = 1, f(\mathbf{s}^{(2)}) = 1, \dots \quad (89)$$

Alle diese Gleichungen sind linear in den Formenkoeffizienten. Sie definieren einen linearen Teilraum im Raum aller Formen. Nun gilt (nach Korkine und Zolotareff):

**SATZ 21.** *Wenn  $f$  extrem ist, so besteht der durch (89) definierte lineare Raum nur aus der einen Form  $f$ , d. h. unter den Gleichungen (89) kommen  $N$  linear unabhängige vor, die die Form  $f$  vollständig bestimmen.*

Formen  $f$  mit dieser Eigenschaft heissen nach Voronoï *perfekt*.

*Beweis:* Wäre  $f$  innerer Punkt einer Strecke

$$f_t = (1-t)f_0 + tf_1,$$

wobei alle Formen  $f_t$  die Gleichungen (89) erfüllen, so würde man genau wie im Beweis von Satz 20 einen Widerspruch erhalten.

Aus Satz 21 folgt leicht, dass es unter den Vektoren  $\mathbf{s}^{(1)}, \mathbf{s}^{(2)}, \dots, \mathbf{s}^{(n)}$  linear unabhängige gibt. Also sind die sukzessiven Minima  $N_1, N_2, \dots$  für eine Extremform alle gleich.

Eine Extremform  $f$  kann immer als reduzierte Form angenommen werden. Ist  $f$  reduziert und  $N_1 = 1$ , so ist nach der Ungleichung (23) von Mahler und Weyl

$$f_{kk} \leq \delta_k, \quad (90)$$

insbesondere

$$f_{11} = f_{22} = f_{33} = f_{44} = 1. \quad (91)$$

Werden die reduzierten Formen durch  $f_{11} = 1$  normiert, so geht die Zelle  $Z$  in ein Polyeder  $P'$  des  $(N-1)$ -dimensionalen Raumes über, das sich allerdings (im Gegensatz zum früher betrachteten Polyeder  $P$ ) ins Unendliche erstreckt. Den Kanten von  $Z$  (soweit sie nicht aus lauter halbdefiniten Formen mit  $f_{11} = 0$  bestehen) entsprechen Ecken von

$P'$ . Eine Extremform  $f$  mit  $f_{11} = 1$  ist nach Satz 20 eine Ecke von  $P'$ . Für die reduzierten Transformierten  $Tf$  gilt dasselbe. Ferner muss auf jeder von  $f$  ausgehenden Kante von  $P'$

$$f_t = (1 - t)f + tf_1$$

die Ableitung der Diskriminante  $D_n(f_t)$  nach  $t$  für  $t = 0$  positiv sein. Dasselbe muss für alle reduzierten Transformierten von  $f$  gelten.

Sind umgekehrt alle reduzierten Transformierten  $Tf$  Ecken von  $P'$  und ist auf allen von ihnen ausgehenden Kanten die Ableitung von  $D_n(f)$  positiv, so ist  $f$  eine Extremform, wie Minkowski (*Ges. Abh.* II, S. 77) bewiesen hat. Um alle Extremformen zu erhalten, genügt es also, die Ecken des Polyeders  $P'$  zu durchmustern und zu sehen, welche von ihnen die eben genannten Bedingungen erfüllen.

Zu jeder Form  $f(x_1, \dots, x_n)$  gehört eine *reziproke Form*  $f^*(u_1, \dots, u_n)$ , deren Matrix die Inverse zur Matrix der Form  $f$  ist. Zu jedem Minimumvektor  $s^{(\alpha)}$  gehört eine Linearform  $(s^{(\alpha)}u)$  in  $u_1, \dots, u_n$ , deren Koeffizienten die Koordinaten von  $s^{(\alpha)}$  sind. Wenn die Form  $f^*(u)$  sich als Summe von Quadraten dieser Linearformen mit positiven Koeffizienten  $\varrho_\alpha$  darstellen lässt:

$$f^*(u) = \sum \varrho_\alpha (s^{(\alpha)}u)^2,$$

so heisst die Form  $f$  nach Coxeter *eutaktisch*.

Nach Satz 21 ist jede Extremform perfekt. Nach Voronoï [1] ist jede Extremform ausserdem eutaktisch. Umgekehrt gilt: *Jede perfekte eutaktische Form ist extrem*. Für diesen Satz von Voronoï hat Coxeter [2] einen einfachen Beweis gegeben.

## § 16. Extremformen und dichteste Kugelpackungen in 3, 4, 5 und 6 Dimensionen

Korkine und Zolotareff [3] haben alle Extremformen in 3, 4 und 5 Dimensionen aufgestellt. Ihr Verfahren lässt sich folgendermassen beschreiben.

Es sei wieder  $N_1 = 1$ . Man stelle zuerst alle ganzzahligen Vektoren  $\mathbf{s} = (s_1, \dots, s_n)$  auf, für welche eine Gleichung

$$f(s_1, \dots, s_n) = 1 \tag{92}$$

gelten kann, wobei  $f$  eine reduzierte Form mit  $f_{11} = 1$  ist. Für eine Extremform müssen  $N = \frac{1}{2}n(n+1)$  linear unabhängige Gleichungen (92) gelten. Durch Einführung von neuen Basisvektoren  $\mathbf{e}'_1, \dots, \mathbf{e}'_n$  werden nun die Gleichungen (92) möglichst vereinfacht. Schliesslich werden die Koeffizienten der Form  $f$  aus den  $N$  unabhängigen linearen Gleichungen berechnet.

Bei der Durchführung ist der folgende Satz sehr nützlich:



SATZ 22. Wenn alle Determinanten, die man aus je  $n$  Vektoren  $\mathbf{s}$  mit Norm 1 bilden kann, gleich 0 oder  $\pm 1$  sind, dann gibt es genau  $n(n+1)$  solche Vektoren und die Form kann in

$$u_n = \sum_i x_i^2 + \sum_{i < k} x_i x_k \quad (93)$$

transformiert werden. Die Vektoren  $\mathbf{s}$  sind dann die  $2n$  Vektoren  $\pm \mathbf{e}_k$  und die  $n(n-1)$  Differenzen  $\mathbf{e}_j - \mathbf{e}_k$ .

Für den Beweis möge auf die zitierte Arbeit von Korkine und Zolotareff [3] verwiesen werden.

Wie nützlich dieser Satz ist, sieht man aus den folgenden Beispielen.

1. *Ternäre Extremformen.* In § 7 haben wir gesehen, dass je 3 linear unabhängige Minimumvektoren  $\mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3$  automatisch ein primitives System bilden, d. h. dass ihre Determinante gleich  $\pm 1$  ist. Nach Satz 22 folgt daraus, dass es nur eine extreme Formenklasse gibt, nämlich die Klasse der Form

$$u_3 = \sum x_i^2 + x_1 x_2 + x_1 x_3 + x_2 x_3. \quad (94)$$

Die drei Basisvektoren  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$  haben in dieser Metrik die Längen 1 und die Skalarprodukte  $\frac{1}{2}$ , d. h. sie schliessen Winkel von  $60^\circ$  miteinander ein. Das Gitter ist *rhomboidisch*. Die zugehörige Kugelpackung besteht aus hexagonalen ebenen Schichten: in jeder Schicht sind die Kugelmittelpunkte in gleichseitigen Dreiecken angeordnet und in der nächsten Schicht liegt ein Kugelmittelpunkt immer senkrecht über einem Dreiecksmittelpunkt der ersten Schicht. Ob die Kugelpackung eine dichteste ist, weiss man nicht<sup>1</sup>, aber jedenfalls ist sie die dichteste *gitterförmige* Kugelpackung im dreidimensionalen Raum.

Die Diskriminante der Form  $u_3$  ist  $\frac{1}{2}$ . In den Ungleichungen (19) und (20) ist also  $\mu_3 = 2$  der bestmögliche Faktor, ebenso in (39)  $\lambda_3 = \frac{1}{2}$ , was Seeber und Gauss ja auch schon wussten.

2. *Quaternäre Extremformen.* Hier gibt es nach § 7 zwei Fälle:

*Fall A.* Die Form ist äquivalent der Form

$$g_4 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1 + x_2 + x_3) x_4. \quad (95)$$

In diesem Falle gibt es 4 linear unabhängige Minimalvektoren von der Länge Eins, die kein primitives System bilden. Sie sind paarweise senkrecht und spannen ein einfaches kubisches Gitter auf. Das ursprüngliche Gitter ist kubisch raumzentriert; der vierte

---

<sup>1</sup> Siehe über diese Frage L. FEJES TÓTH, *Lagerungen in der Ebene, auf der Kugel und im Raum*, Kap. 7 (Springer-Verlag 1953).

Basisvektor  $\mathbf{e}_4$  hat die rechtwinkligen Koordinaten  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  und geht von einer Ecke zur Mitte des vierdimensionalen Würfels. Die Diskriminante der Form ist  $\frac{1}{4}$ ; es gibt 24 Gittervektoren mit Norm 1.

*Fall B.* In allen anderen Fällen bilden je 4 linear unabhängige Minimalvektoren automatisch ein primitives System. Die Determinante aus je 4 Minimalvektoren ist also immer 0 oder  $\pm 1$ . Nach Satz 22 gibt es unter dieser Voraussetzung nur eine Extremform, nämlich

$$u_4 = \sum_i x_i^2 + \sum_{i < k} x_i x_k. \quad (96)$$

Die Diskriminante dieser Form ist  $\frac{5}{16}$ . Es gibt  $n(n+1) = 20$  Vektoren mit Norm Eins. Die Basisvektoren  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4$  haben die Länge Eins und ihre Skalarprodukte sind  $\frac{1}{2}$ , wie beim rhomboedrigen Gitter in 3 Dimensionen.

Die kleinstmögliche Diskriminante, nämlich  $\frac{1}{4}$ , ergibt sich im Fall A. Also ist  $\mu_4 = 4$  der bestmögliche Faktor in (19) und (20), und  $\lambda_4 = \frac{1}{4}$  der bestmögliche Faktor in der fundamentalen Ungleichung für reduzierte quaternäre Formen

$$D_4 \geq \frac{1}{4} f_{11} f_{22} f_{33} f_{44}. \quad (97)$$

Für  $n = 5$  sind die Extremformen nach Korkine und Zolotareff [3]:

$$\begin{aligned} u_5 &= \sum x_i^2 + \sum_{i < k} x_i x_k, \\ z_5 &= \sum x_i^2 - \frac{1}{2} x_1 x_2 - \frac{1}{2} x_1 x_3 - \frac{1}{2} x_1 x_4 - \frac{1}{2} x_1 x_5 + \frac{1}{2} x_2 x_3 + \frac{1}{2} x_2 x_4 - x_2 x_5 + \frac{1}{2} x_3 x_4 - x_3 x_5 - x_4 x_5, \\ v_5 &= u_5 - x_1 x_2. \end{aligned}$$

Ihre Diskriminanten sind  $\frac{3}{16}$ ,  $\frac{81}{512}$  und  $\frac{1}{8}$ . Die dichteste Kugelpackung und der beste Wert von  $\mu_5$  werden durch die Form  $v_5$  geliefert.

Coxeter [2] hat diese Formen zur Theorie der einfachen Liegruppen in Beziehung gesetzt. Er ersetzt die Formen  $u_n$  und  $v_n = u_n - x_1 x_2$  durch die äquivalenten Formen

$$\begin{aligned} A_n &= \sum x_i^2 - \sum x_i x_{i+1} \\ D_n &= A_{n-1} - x_{n-2} x_n + x_n^2 \end{aligned}$$

die zu den von Cartan ebenso bezeichneten Liegruppen gehören. Diese Formen sind für jedes  $n$  extrem. Dieselbe gilt (mit wenigen Ausnahmen) für die ähnlich definierten Formen  $A_n^r$ ,  $D_n^2$ ,  $E_6$  und  $E_6^3$  die ebenfalls zu einfachen Liegruppen gehören. Die letzten beiden sind so definiert:

$$\begin{aligned} E_6 &= A_5 - x_3 x_6 + x_6^2 \\ E_6^3 &= A_6 - \frac{1}{3} x_5^2. \end{aligned}$$

Die früher betrachteten Formen  $g_3$  und  $g_4$  sind äquivalent zu  $v_3$  und  $v_4$  oder zu  $D_3$  und  $D_4$ . Die quaternären Extremformen sind also  $u_4$  und  $v_4$  oder (wenn man will)  $A_4$  und  $D_4$ .

Die Form  $z_5$  ist äquivalent zu

$$A_5^3 = A_4 - x_2 x_5 + \frac{2}{3} x_5^2.$$

Die quinären Extremformen  $u_5$ ,  $z_5$ ,  $v_5$  können also durch  $A_5$ ,  $A_5^3$  und  $D_5$  ersetzt werden.

Die Extremformen in 6 Veränderlichen hat N. Hofreiter [1], [2] bestimmt, jedoch hat Coxeter [2] einen Fehler in seiner Arbeit gefunden. Hofreiters Form  $F_4$  mit Diskriminante  $2^{-14} \cdot 3^3 \cdot 53$  ist nicht extrem. Dafür hat Coxeter die Extremform  $E_6^3$  entdeckt, die mit den 27 Geraden auf einer kubischen Fläche zusammenhängt und die Diskriminante  $2^{-12} \cdot 3^5$  hat.

Ausser  $E_6^3$  gibt es noch 3 senäre Extremformen  $A_6$ ,  $D_6$  und  $E_6$  mit Diskriminanten  $\frac{7}{64}$ ,  $\frac{3}{64}$  und  $\frac{1}{16}$ . Die grösste Diskriminante  $\frac{7}{64}$  hat  $A_6$  oder die äquivalente Form

$$u_6 = \sum x_i^2 + \sum_{i < k} x_i x_k.$$

Die kleinste Diskriminante  $\frac{3}{64}$  hat die Form  $D_6$  oder die äquivalente

$$v_6 = u_6 - x_1 x_2.$$

Die dichteste Kugelpackung in 6 Dimensionen wird durch  $v_6$  geliefert; die zugehörige Konstante  $\mu_6$  ist  $\frac{6^4}{3}$ .

Die Methode von Hofreiter besteht darin, dass er zunächst untersucht, wie viele und welche Gitterpunkte in dem Parallelepiped liegen können, das von den ersten 6 Minimumvektoren  $s_1, \dots, s_6$  aufgespannt wird. Er findet 6 Möglichkeiten:

- 1) Nur die Ecken sind Gitterpunkte.
- 2) In drei vierdimensionalen Seiten sind die Mittelpunkte Gitterpunkte. Diese Gitterpunkte sind

$$\frac{1}{2}(s_1 + s_2 + s_3 + s_4), \quad \frac{1}{2}(s_1 + s_2 + s_5 + s_6), \quad \frac{1}{2}(s_3 + s_4 + s_5 + s_6).$$

- 3) In einer vierdimensionalen Seite ist der Mittelpunkt  $\frac{1}{2}(s_1 + s_2 + s_3 + s_4)$  Gitterpunkt.
- 4) In einer fünfdimensionalen Wand ist der Mittelpunkt  $\frac{1}{2}(s_1 + s_2 + s_3 + s_4 + s_5)$  Gitterpunkt.
- 5) Der Mittelpunkt der Gittermasche  $\frac{1}{2} \sum s_j$  ist Gitterpunkt.
- 6) Im Innern der Gittermasche liegen 2 Gitterpunkte  $\frac{1}{3} \sum s_j$  und  $\frac{2}{3} \sum s_j$ .

Wenn bei jeder Wahl der linear unabhängigen Minimumvektoren  $s_j$  der Fall 1) eintritt, kann man Satz 22 anwenden und findet nur die Form  $u_6$ . In den anderen Fällen werden jeweils die  $N$  Gleichungen (92) aufgestellt, die ausdrücken, dass gewisse Gittervektoren die Norm 1 haben. Diese linearen Gleichungen bestimmen die Koeffizienten der Extremform. Für die Durchführung sei auf die Arbeiten von Hofreiter verwiesen.

## Literatur

### Teil I und II

- J. L. LAGRANGE, *Œuvres* III, 695.  
 L. A. SEEBER, *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen*. Freiburg, 1831.  
 C. F. GAUSS, Besprechung des Buches von SEEBER, *Werke* II, 188.  
 P. G. LEJEUNE DIRICHLET, *J. f. d. reine u. ang. Math.*, 40 (1850), 209.  
 CH. HERMITE, *J. f. d. reine u. ang. Math.*, 40 (1850), 261–315. = *Œuvres I*, 94–164.  
 H. MINKOWSKI, [1] *Geometrie der Zahlen*. Leipzig 1896 und 1910, unveränderter Nachdruck 1925. [2] Diskontinuitätsbereich für arithmetische Äquivalenz. *J. f. d. reine u. ang. Math.*, 129 (1905), 220. = *Ges. Abh.* II, 53.  
 H. F. BLICHFELDT, [1] A new principle in the geometry of numbers. *Trans. Amer. Math. Soc.*, 15 (1914), 227. [2] A further reduction of the known maximum limit to the least value of quadratic forms. *Bull. Amer. Math. Soc.*, 23 (1917), 401. [3] The minimum value of quadratic forms and the closest packing of spheres. *Math. Ann.*, 101, (1929), 605. Für weitere Arbeiten von BLICHFELDT siehe Lit. zu Teil III.  
 G. JULIA, *Comptes rendus Acad. Paris*, 162 (1916), 320 und 498.  
 L. BIEBERBACH und I. SCHUR, Über die Minkowskische Reduktionstheorie. *Sitzungsber. Preuss. Akad. Berlin* 1928, 510; Berichtigung 1929, 508.  
 R. REMAK [1] Vereinfachung eines Blichfeldtschen Beweises aus der Geometrie der Zahlen. *Math. Z.*, 26 (1927), 694. [2] Über die Minkowskische Reduktion. *Compositio math.*, 5 (1938), 368.  
 K. MAHLER, [1] On Minkowski's theory of reduction. *Quarterly J. Math.*, 9 (1938), 259. [2] On reduced positive definite ternary quadratic forms. *J. London Math. Soc.*, 15 (1940), 193. [3] On reduced definite quaternary quadratic forms. *Nieuw Archief Wiskunde* (2), 22 (1946), 207.  
 C. L. SIEGEL, Einheiten quadratischer Formen. *Abh. Math. Sem. Hamburg*, 13 (1939), 209.  
 H. WEYL, [1] Theory of reduction for arithmetical equivalence. *Trans. Amer. Math. Soc.*, 48 (1940), 126. [2] Part II. *Ibid.*, 51 (1942), 203. [3] On Geometry of Numbers. *Proc. London Math. Soc.*, 47 (1942), 268.  
 L. J. MORDELL, Observation on the minimum of a positive quadratic form in eight variables. *J. London Math. Soc.*, 19 (1944), 3.  
 O. H. KELLER, Geometrie der Zahlen. *Enz. der Math. Wiss.*, 2. Aufl., Band I, Art. 27, 36–39 und 54–61. Dort weitere Literatur.  
 T. W. CHAUNDY, The arithmetic minima of pos. quadr. forms. *Quart. J. Math.* (Oxford ser.), 17 (1946), 166.

**Teil III**

- A. KORKINE und G. ZOLOTAREFF, [1] Sur les formes quadratiques positives quaternaires. *Math. Ann.*, 5 (1872), 581. [2] Sur les formes quadratiques. *Ibid.*, 6 (1873), 366. [3] Sur les formes quadratiques positives. *Ibid.*, (1877), 242.
- G. VORONŌI, [1] Propriétés des formes quadratiques positives parfaites. *J. f. d. reine u. ang. Math.*, 133 (1908), 97. [2] Sur les paralléloèdres primitifs. *Ibid.*, 134 (1908), 198.
- H. F. Blichfeldt, [4] Note on quadratic forms. *Bull. Amer. Math. Soc.*, 29 (1923), 194. [5] On the minimum value of positive real quadratic forms in 6 variables. *Ibid.*, 31 (1925), 386. [6] The minimum value of positive quadratic forms in seven variables. *Ibid.*, 32 (1926), 99. [7] The minimum values of positive quadratic forms in six, seven and eight variables. *Math. Z.*, 39 (1934), 1.
- N. Hofreiter, [1] Über Extremformen. *Monatshefte Math. Phys.*, 40 (1933), 129. [2] Zur Geometrie der Zahlen. I. *Ibid.*, 40 (1933), 181. [3] II. *Ibid.*, 42 (1935), 101.
- L. J. MORDELL, Thoughts on number theory. *J. London Math. Soc.*, 21 (1946), 58.
- H. S. M. COXETER, [1] Extreme forms. *Proc. Int. Congr. Math.* (1950), Vol. 1, 294. [2] Extreme forms. *Canadian J. of Math.*, 3 (1951), 391.