THEORY OF REDUCTION FOR ARITHMETICAL EQUIVALENCE

BY

HERMANN WEYL

INTRODUCTION

Minkowski's *Geometrie der Zahlen* as it was published in 1896 led up to two fundamental inequalities concerning a symmetric convex body in relationship to a lattice; in his notation

$$M^n V \leqq 2^n \tag{1}$$

and

$$S_1 \cdots S_n V \leqq 2^n. \tag{2}$$

The second inequality, which generalizes the first, is a decisive step towards a theory of reduction of arbitrary gauge functions under arithmetical equivalence. In fact the problem of reduction for quadratic forms of n variables (ellipsoids) was the starting point of Minkowski's investigations. But he must have found that the new instrument which he invented and of which he made so many beautiful applications in other directions was not quite adequate to the goal for which it had originally been devised. For 14 years later he came out with a paper on "Diskontinuitätsbereich für arithmetische Aequivalenz" [1] which makes no use whatsoever of his own geometric methods. This was probably due to two difficulties: he failed to see a way of passing from pseudo-reduction to true reduction for an arbitrary convex body, and in the special case of ellipsoids he found the inequality of true reduction tied up with the selection of a finite number among the linear inequalities which characterize a reduced form. The latter knot was unraveled by a kind of topological argument in a joint paper by L. Bieberbach and I. Schur [2] while K. Mahler in 1938 made an almost trivial remark which removed the first difficulty [3]. In a general overhauling of the geometry of numbers [4], to which the author was led by preparing an introductory talk for a seminar on the subject, he generalized (2) in such a way as to make the approach to that inequality more natural [5], rediscovered Mahler's observation, substituted a simpler argument for that used by Bieberbach and Schur and finally extended Minkowski's second theorem of finiteness. Without this extension certain primitive questions about the topological pattern of equivalent cells would be unanswerable. In a previous paper R. Remak had considerably shortened and sharpened Minkowski's estimate for the coefficients β_{ij} which appear in

Presented to the Society, February 24, 1940; received by the editors February 16, 1940.

the Jacobi transformation of a reduced quadratic form [6]. The author found that a considerable part of the theory of reduction could be carried through along the lines of Mahler's approach for arbitrary convex bodies and that this more general procedure results in stronger rather than weaker estimates for the quantities on which the question of finiteness depends.

The present paper sets forth the whole theory *ab ovo*, and hence is partly of a didactic nature; as far as possible it follows the geometric approach dealing with arbitrary convex bodies. In order to prevent it from becoming too dull reading, I have extended the theory to vectors and lattices and forms in which complex numbers or quaternions take the place of real numbers. Chapter I deals with the general theory, Chapter II with the special case of quadratic, Hermitian and "Hamiltonian" forms(1).

Chapter I. General theory of reduction

A. The real case

1. **Known facts about lattices.** In the n-dimensional vector space E_n whose elements are the n-uples $\mathfrak{x}=(x_1, \cdots, x_n)$ of real numbers we consider the *lattice* $\mathfrak{L}$ of the vectors with integral components x_i. The n unit vectors $\mathfrak{e}_k=(\delta_1^k, \cdots, \delta_n^k)$ form a basis of, or span, this lattice in the sense that the lattice vectors appear as sums $\sum_i x_i\mathfrak{e}_i$ with integral coefficients. Here δ_i^k are the Kronecker δ's. Any basis $\mathfrak{s}_k=(s_1^k, \cdots, s_n^k)$ of the lattice arises from the absolute basis $\mathfrak{e}_k$ by a *unimodular transformation* $S=\|s_i^k\|$:

$$\mathfrak{s}_k = \sum_i s_i^k \mathfrak{e}_i.$$

The corresponding coordinates, x_i and x_i', $\mathfrak{x}=\sum_i x_i\mathfrak{e}_i=\sum_k x_k'\mathfrak{s}_k$, are linked by the equations(2)

$$x_i = \sum_k x_k' s_i^k \text{ or briefly, } x=x'S.$$

The coefficients s_i^k are integers and their determinant is ± 1. The substitutions S with these properties form a group $\{S\}$, the *modular group*. Our viewpoint is that the vector space is endowed with the lattice, but that the choice of the lattice basis is arbitrary.

(1) A brief and masterly treatment of the reduction of quadratic forms along purely arithmetical lines is to be found in a recent paper by C. L. Siegel, Abhandlungen aus dem mathematischen Seminar der Hansischen Universität, vol. 13 (1939), pp. 209–239, of which I received a reprint on March 20, 1940. (The number of the journal itself has not yet reached Princeton.) But even against Siegel's highly simplified arithmetical treatment, the geometrical approach retains the advantage of yielding sharper estimates. Siegel has a generalization of the second theorem of finiteness, different from ours, which leads to important applications in the domain of rational indefinite forms. (Added March 25, 1940.)

(2) In preparation for a later generalization to quaternions we take good care to put factors in their proper order.

Any k linearly independent vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ $(0 \leqq k \leqq n)$ span a k-dimensional subspace

$$E_k = E = [\mathfrak{d}_1, \cdots, \mathfrak{d}_k].$$

If they are lattice vectors, then E is a *lattice subspace.* E_0 consists of the vector zero only.

A vector $\mathfrak{a}$ not in E may be adjoined to E and then gives rise to the $(k+1)$-dimensional manifold $E' = [E, \mathfrak{a}]$ consisting of all sums

$$\mathfrak{x}' = \mathfrak{x} + x\mathfrak{a} \tag{3}$$

with $\mathfrak{x}$ in E, x a number. If E is a lattice subspace and $\mathfrak{a}$ a lattice vector, the adjunction is said to be *primitive* provided every lattice vector (3) in E' has an integral coefficient x (and hence a lattice component $\mathfrak{x}$ in E).

Suppose $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ are k linearly independent lattice vectors spanning the lattice subspace $E = [\mathfrak{d}_1, \cdots, \mathfrak{d}_k]$.

LEMMA 1. *There exists a positive integer M such that every lattice vector in E is of the form*

$$\frac{y_1}{M}\mathfrak{d}_1 + \cdots + \frac{y_k}{M}\mathfrak{d}_k$$

where the y's are integers.

There are two essentially different proofs of this fact, one resting on divisibility and determinants, the other on considerations of magnitude. The first proof runs as follows. We can select $n-k$ among the unit vectors $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$, say $\mathfrak{e}_1', \cdots, \mathfrak{e}_{n-k}'$, such that

$$\mathfrak{d}_1, \cdots, \mathfrak{d}_k, \mathfrak{e}_1', \cdots, \mathfrak{e}_{n-k}' \tag{4}$$

are linearly independent. The determinant of the components of (4) is nonzero; denote its absolute value by M. Writing down the equation

$$\mathfrak{x} = y_1\mathfrak{d}_1 + \cdots + y_k\mathfrak{d}_k + x_1'\mathfrak{e}_1' + \cdots + x_{n-k}'\mathfrak{e}_{n-k}' \tag{5}$$

for any lattice vector $\mathfrak{x}$ in terms of absolute components, one finds the coefficients y and x' to be fractions with the common denominator M. This applies in particular to the lattice vectors in E for which $x_1' = \cdots = x_{n-k}' = 0$.

The other proof compares $\mathfrak{L} \cap E = \mathfrak{L}_k$, "the lattice in E," with the coarser lattice $\mathfrak{L}_k^0$ consisting of all integral combinations of $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$,

$$y_1\mathfrak{d}_1 + \cdots + y_k\mathfrak{d}_k \qquad (y_1, \cdots, y_k \text{ integers}). \tag{6}$$

We maintain that there is only a finite number M of vectors in $\mathfrak{L}_k$ which are incongruent modulo $\mathfrak{L}_k^0$. For every vector $\mathfrak{x}$ in E their exists a reduced one

$$\mathfrak{x}^* \equiv \mathfrak{x} \pmod{\mathfrak{L}_k^0}, \qquad \mathfrak{x}^* = y_1^*\mathfrak{d}_1 + \cdots + y_k^*\mathfrak{d}_k, \tag{7}$$

which satisfies the inequalities

$$(8) \qquad |y_1^*| \leqq \tfrac{1}{2}, \cdots, |y_k^*| \leqq \tfrac{1}{2}.$$

Using again the absolute components one readily derives from (8) upper bounds for the $|x_i^*|$ of any reduced vector $\mathfrak{x}^* = (x_1^*, \cdots, x_n^*)$. Hence if the x_i^* are required to be integers, which is the case when $\mathfrak{x}$ and thus $\mathfrak{x}^*$ is a lattice vector, one finds oneself restricted to a finite number of possibilities. Our result states that the additive Abelian group $\mathfrak{L}_k/\mathfrak{L}_k^0$ is of finite order M, and therefore every vector $\mathfrak{x}$ of $\mathfrak{L}_k$ satisfies the congruence $M\mathfrak{x} \equiv 0$ $(\mathfrak{L}_k^0)$, which was to be proved.

The vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ form a lattice basis of E if $\mathfrak{L}_k$ coincides with $\mathfrak{L}_k^0$, that is to say, if every lattice vector in E is of the form (6).

The vector $\mathfrak{s}_k$ of any basis $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ of $\mathfrak{L}$ evidently is a primitive adjunction to $[\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}]$. More generally, we have

LEMMA 2. *Suppose $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ constitute a basis of $\mathfrak{L}$. The vector*

$$\mathfrak{a} = a_1\mathfrak{s}_1 + \cdots + a_n\mathfrak{s}_n$$

is a primitive adjunction to $E = [\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}]$ if and only if $a_1, \cdots, a_n$ are integers and $a_k, \cdots, a_n$ are without common divisor.

Proof. 1. If $(a_k, \cdots, a_n)$ have a common divisor $d > 1$, then

$$(9) \qquad \frac{1}{d}(a_k\mathfrak{s}_k + \cdots + a_n\mathfrak{s}_n).$$

evidently is a vector $\mathfrak{x}'$ in $E' = [E, \mathfrak{a}]$ for which the x in (3) is $1/d$ and thus not an integer.

2. If one denotes by x_i' the components of $\mathfrak{x}'$ in (3) with respect to the basis $\mathfrak{s}_i$, one has

$$(10) \qquad x_k' = xa_k, \cdots, x_n' = xa_n.$$

Hence (10) must be integers for any lattice vector $\mathfrak{x}'$ in E'. However if $a_k, \cdots, a_n$ are without common divisor one can ascertain integers $l_k, \cdots, l_n$ satisfying the equation

$$a_kl_k + \cdots + a_nl_n = 1.$$

The integrity of (10) then results in the integrity of

$$x = x_k'l_k + \cdots + x_n'l_n$$

itself.

LEMMA 3. *Suppose E' is a given lattice subspace and $\mathfrak{d}$ a lattice vector outside E'. Then one can pass from E' to $E = [E', \mathfrak{d}]$ by a primitive adjunction $\mathfrak{s}$.*

Proof. Let E be spanned by the $k-1$ linearly independent lattice vectors

$\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}$ and use the notations $\mathfrak{L}_k$, $\mathfrak{L}_k^0$ with respect to the basis $(\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}, \mathfrak{d})$ of E. We write each vector $\mathfrak{x}$ of $\mathfrak{L}_k$ in the form (3),

$$\mathfrak{x} = x\mathfrak{d} + \mathfrak{x}' \qquad (\mathfrak{x}' \text{ in } E'). \tag{11}$$

If M is the order of the additive Abelian group $\mathfrak{L}_k/\mathfrak{L}_k^0$, we know that

$$Mx = y \tag{12}$$

is an integer. Select a full system of residues

$$\mathfrak{x}^{(0)} = 0, \mathfrak{x}^{(1)}, \cdots, \mathfrak{x}^{(M-1)}$$

of $\mathfrak{L}_k$ modulo $\mathfrak{L}_k^0$ and denote by $y^{(0)}=0, y^{(1)}, \cdots, y^{(M-1)}$ the corresponding numbers y as defined by (11), (12). The integers $M, y^{(1)}, \cdots, y^{(M-1)}$ have a greatest common divisor (G.C.D.) m^*, namely a common divisor expressible as a linear combination

$$lM + l^{(1)}y^{(1)} + \cdots + l^{(M-1)}y^{(M-1)}$$

with integral coefficients l. By forming the corresponding combination

$$\mathfrak{s} = l\mathfrak{d} + l^{(1)}\mathfrak{x}^{(1)} + \cdots + l^{(M-1)}\mathfrak{x}^{(M-1)}$$

we obtain a vector $\mathfrak{s}$ of $\mathfrak{L}_k$,

$$\mathfrak{s} = (m^*/M)\mathfrak{d} + \mathfrak{s}' \qquad (\mathfrak{s}' \text{ in } E'),$$

such that for every $\mathfrak{x}$ in $\mathfrak{L}_k$ the coefficient y is divisible by m^*. This $\mathfrak{s}$ evidently satisfies our lemma.

Since m^* is a divisor of M, $M=mm^*$, we have

$$\mathfrak{s} = (1/m)\mathfrak{d} + t_1\mathfrak{s}_1 + \cdots + t_{k-1}\mathfrak{s}_{k-1}. \tag{13}$$

m is a positive integer. Moreover one can assume

$$|t_1| \leqq \tfrac{1}{2}, \cdots, |t_{k-1}| \leqq \tfrac{1}{2}. \tag{14}$$

In the special case $m=1$ one may simply take $\mathfrak{s}=\mathfrak{d}$.

We shall use our lemma only for the case when $\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}$ constitute a lattice basis of E'. Then the lemma makes possible, by induction with respect to k, the construction of a lattice basis for any given lattice subspace.

All these simple facts about lattices are well known to the mathematician and the crystallographer. We had to restate them for later use and generalizations.

2. **Gauge functions. Minkowski's inequality.** According to Minkowski, a real-valued continuous function $f(\mathfrak{x})=f(x_1, \cdots, x_n)$ in vector space is said to be a *gauge function* under the following three conditions:

(i) $f(x_1, \cdots, x_n)>0$, except for $x_1= \cdots =x_n=0$;

(ii) $f(tx_1, \cdots, tx_n)=|t| \cdot f(x_1, \cdots, x_n)$ for any real factor t;

(iii) $f(x_1+x_1', \cdots, x_n+x_n') \leqq f(x_1, \cdots, x_n)+f(x_1', \cdots, x_n')$.

One may use this function to endow the n-dimensional affine point space with a *metric* by ascribing the distance $f(\overrightarrow{pp'})$ to any two points p, p'. The gauge body $\mathfrak{K}$ defined by $f(\mathfrak{x})<1$ is an open convex bounded set surrounding the origin $\mathfrak{x}=0$. (Boundedness follows from the fact that $f(x_1, \cdots, x_n)$ has a positive minimum on the sphere $x_1^2+\cdots+x_n^2=1$.) $\mathfrak{K}$ has a Jordan volume V.

Equation (13), together with (14) and $m\geqq 1$, results in the inequality

$$f(\mathfrak{s}) \leqq f(\mathfrak{d}) + \tfrac{1}{2}\{f(\mathfrak{s}_1) + \cdots + f(\mathfrak{s}_{k-1})\}. \tag{15}$$

If one makes the distinction $m=1$ or $m\geqq 2$ one finds that $f(\mathfrak{s})$ cannot exceed both numbers

$$f(\mathfrak{d}), \qquad \tfrac{1}{2}f(\mathfrak{d}) + \tfrac{1}{2}f(\mathfrak{s}_1) + \cdots + \tfrac{1}{2}f(\mathfrak{s}_{k-1}).$$

Therefore we may state this

SUPPLEMENT TO LEMMA 3. *The vector* $\mathfrak{s}$ *may be chosen so that* (15) *holds, or even so that*

$$f(\mathfrak{s}) \leqq \max\{f(\mathfrak{d}), \tfrac{1}{2}f(\mathfrak{d}) + \tfrac{1}{2}f(\mathfrak{s}_1) + \cdots + \tfrac{1}{2}f(\mathfrak{s}_{k-1})\}. \tag{16}$$

Minkowski determines a sequence of lattice vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$ and lattice subspaces $E_0, E_1, \cdots, E_n$ starting with the zero-space E_0 by the following induction with respect to k.

Among all lattice vectors $\mathfrak{a}$ outside E_{k-1}, one chooses one, $\mathfrak{d}_k$, for which $f(\mathfrak{a})$ takes on the least possible value, so that $f(\mathfrak{a})\geqq f(\mathfrak{d}_k)$ for every $\mathfrak{a}$ outside E_{k-1}. The space E_k arises from E_{k-1} by the adjunction of $\mathfrak{d}_k$, $E_k=[E_{k-1}, \mathfrak{d}_k]$.

We put $f(\mathfrak{d}_k)=M_k$. Evidently

$$M_1 \leqq M_2 \leqq \cdots \leqq M_n.$$

Consider the continuous series of homothetic solids

$$\mathfrak{K}(q): \quad f(\mathfrak{x}) < q$$

increasing with the positive parameter q. Our M_k can be described thus: $\mathfrak{K}(q)$ contains less than k linearly independent lattice vectors as long as $q\leqq M_k$, but at least k such vectors if $q>M_k$. Hence $M_1, \cdots, M_n$ are uniquely determined. About these consecutive minima Minkowski proved the fundamental inequality:

THEOREM 1.

$$M_1 \cdots M_n V \leqq 2^n. \tag{2}$$

For later purposes we repeat this proposition in the following slightly modified form: Suppose $M_1', \cdots, M_n'$ are given positive numbers such that the number of linearly independent lattice vectors $\mathfrak{x}$ for which $f(\mathfrak{x})<M_k'$ is less than k. Then

$$M_1' \cdots M_n' V \leqq 2^n. \tag{17}$$

While $M_1, \cdots, M_n$ are uniquely determined, there may be a certain amount of free play in the choice of $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$. The most one can say about it in general terms is this:

THEOREM 2. *If $\mathfrak{d}_1', \cdots, \mathfrak{d}_n'$ are a second set of lattice vectors determined just like $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$, and if, for a certain k, $M_k < M_{k+1}$, then $\mathfrak{d}_1', \cdots, \mathfrak{d}_k'$ are linear combinations of $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ only.*

Proof. Suppose one of the vectors $\mathfrak{d}_1', \cdots, \mathfrak{d}_k'$, say $\mathfrak{d}_i'$, is not a linear combination of $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$. Then $\mathfrak{d}_1, \cdots, \mathfrak{d}_k, \mathfrak{d}_i'$ are linearly independent, and hence not all the $k+1$ numbers

$$f(\mathfrak{d}_1) = M_1, \cdots, f(\mathfrak{d}_k) = M_k, f(\mathfrak{d}_i') = M_i$$

can be less than M_{k+1}. This contradicts the assumption $M_k < M_{k+1}$.

The problem of reduction consists in constructing a basis for the lattice $\mathfrak{L}$ in terms of the given gauge function f. The vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$ do not yet solve the problem because in general they do not span the whole lattice $\mathfrak{L}$. Our next task will be to pass from this pseudo-reduction to true reduction, a step well prepared by the considerations of §1.

3. **Reduction.** The only modification needed in the definition of $\mathfrak{d}_k$ is the insertion at its proper place of the word "primitive." The new inductive definition of lattice vectors $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ and lattice subspaces $E_0, E_1, \cdots, E_n$ runs as follows:

Among all primitive adjunctions $\mathfrak{a}$ to E_{k-1}, we choose one, $\mathfrak{d}_k$, for which $f(\mathfrak{a})$ assumes the least possible value, so that

$$f(\mathfrak{a}) \geqq f(\mathfrak{s}_k)$$

for every primitive adjunction $\mathfrak{a}$ to E_{k-1}. Moreover

$$E_k = [E_{k-1}, \mathfrak{s}_k].$$

Lemma 3 guarantees the existence of primitive adjunctions $\mathfrak{a}$ to E_{k-1}. We realize by induction that $\mathfrak{s}_1, \cdots, \mathfrak{s}_k$ is a lattice basis for E_k, hence $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ for the whole space. We put $f(\mathfrak{s}_k) = L_k$. Taking Lemma 2 into account, we can give our definition of a reduced basis $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ the following turn:

An n-uple of integers $(x_1, \cdots, x_n)$ is said to belong to X_k if $x_k, \cdots, x_n$ are without common divisor. *The basis $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ of $\mathfrak{L}$ is reduced with respect to f, if for every $k = 1, \cdots, n$ and every $(x_1, \cdots, x_n)$ of X_k the inequality*

$$f(x_1\mathfrak{s}_1 + \cdots + x_n\mathfrak{s}_n) \geqq f(\mathfrak{s}_k) \tag{18}$$

holds [7]. Our procedure has led up to this result:

THEOREM 3. *For every gauge function f there exists a reduced basis $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ of the lattice.*

Relation (18) implies

$$f(\mathfrak{s}_{k+1}) \geqq f(\mathfrak{s}_k)$$

or

$$L_1 \leqq L_2 \leqq \cdots \leqq L_n. \tag{19}$$

The following proposition ties up pseudo-reduction with the reduction just defined [8]:

THEOREM 4 (Mahler's theorem). *One has*

$$L_k \leqq \theta_k M_k \tag{20}$$

where θ_k is a constant independent of the gauge function f.

An immediate corollary derived from it by Minkowski's inequality (2) is

THEOREM 5. *The relation*

$$L_1 \cdots L_n V \leqq \mu_n \tag{21}$$

holds with $\mu_n = 2^n \cdot \theta_1\theta_2 \cdots \theta_n$.

Proof. After we have ascertained $\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}$ we determine a primitive adjunction $\mathfrak{s}$ to $E' = [\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}]$ by the construction of Lemma 3, choosing $\mathfrak{d}$ in this particular fashion: One of the k linearly independent vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ occurring in Minkowski's construction, say $\mathfrak{d}_i$, lies outside E'. We take $\mathfrak{d} = \mathfrak{d}_i$ and then find a primitive adjunction $\mathfrak{s}$ to E' such that $[E', \mathfrak{s}] = [E', \mathfrak{d}]$. By the supplement to Lemma 3 one will have

$$f(\mathfrak{s}) \leqq f(\mathfrak{d}) + \tfrac{1}{2}\{f(\mathfrak{s}_1) + \cdots + f(\mathfrak{s}_{k-1})\}.$$

Since $f(\mathfrak{d})$ is one of the numbers $M_1, \cdots, M_k$ and hence is less than or equal to M_k, and since by definition $L_k \leqq f(\mathfrak{s})$, we find

$$L_k \leqq M_k + \tfrac{1}{2}(L_1 + \cdots + L_{k-1}),$$

which under the assumption of the inequalities

$$L_1 \leqq \theta_1 M_1, \cdots, L_{k-1} \leqq \theta_{k-1} M_{k-1}$$

leads on to

$$L_k \leqq \theta_k M_k$$

with

$$\theta_k = 1 + \tfrac{1}{2}(\theta_1 + \cdots + \theta_{k-1}). \tag{22}$$

Hence Theorem 4 is proved inductively, and, by the recursive relations (22) or

$$\theta_1 = 1; \qquad \theta_{k+1} = 1 + \tfrac{1}{2}(\theta_1 + \cdots + \theta_{k-1} + \theta_k) = \theta_k + \tfrac{1}{2}\theta_k = \tfrac{3}{2}\theta_k,$$

we find the following explicit expressions for θ_k and μ_n:

$$\theta_k = (\tfrac{3}{2})^{k-1}, \qquad \mu_n = (\tfrac{3}{2})^{n(n-1)/2}.$$

Suppose $p_0, p_1, \cdots, p_n$ are given numbers satisfying the following conditions:

$$1 = p_0 \leqq p_1 \leqq \cdots \leqq p_n. \tag{23}$$

A basis $\mathfrak{s}_1', \cdots, \mathfrak{s}_n'$ of $\mathfrak{L}$ is said to have the property $B(p_1, \cdots, p_n)$ if the inequality

$$f(x_1\mathfrak{s}_1' + \cdots + x_n\mathfrak{s}_n') \geqq (1/p_k)f(\mathfrak{s}_k)$$

holds whenever $(x_1, \cdots, x_n)$ is an n-uple in X_k and k one of the indices $1, \cdots, n$. By exploiting our method to the full we arrive at the following [9] generalization of Theorem 4:

THEOREM 6. *If the lattice basis $\mathfrak{s}_k'$ has the property $B(p_1, \cdots, p_n)$, then the values $f(\mathfrak{s}_k') = L_k'$ satisfy the inequalities*

$$L_k' \geqq \frac{1}{p_i} L_i' \qquad (\textit{for } k > i) \tag{24}$$

and

$$L_k' \leqq \theta_k(p) \cdot M_k \qquad (k = 1, \cdots, n) \tag{25}$$

with a constant $\theta_k(p)$ depending on $p_1, \cdots, p_k$ but not on f.

Relation (24) is a consequence of the fact that $(\delta_1^k, \cdots, \delta_n^k)$ is an n-uple in X_i if $k > i$. Otherwise the proof follows the same road as before. (22) gives place to this recursive equation:

$$\theta_k(p)/p_k = 1 + \tfrac{1}{2}(\theta_1(p) + \cdots + \theta_{k-1}(p))$$

which in the same manner readily leads to

$$\theta_k(p) = p_k \cdot \prod_{i=1}^{k-1} (1 + \tfrac{1}{2}p_i).$$

One sees that $\theta_k(p)/p_k$ increases with k, and therefore (23) implies

$$1 = \theta_0(p) \leqq \theta_1(p) \leqq \cdots \leqq \theta_n(p). \tag{26}$$

One can repeat our whole argument after replacing (15) by the sharper and slightly more complex inequality (16). One then obtains this

SUPPLEMENT TO THEOREMS 4–6. *One may choose*

$$\theta_k = (\tfrac{3}{2})^{k-1}, \qquad \mu_n = (\tfrac{3}{2})^{n(n-1)/2}, \qquad \theta_k(p) = p_k \cdot \prod_{i=1}^{k-1} (1 + \tfrac{1}{2}p_i), \tag{27}$$

or, with a slight improvement,

$$\theta_1 = 1, \qquad \theta_k = (\tfrac{3}{2})^{k-2} \quad (\textit{for } k \geqq 2); \qquad \mu_n = (\tfrac{3}{2})^{(n-1)(n-2)/2};$$

$$\theta_1(p) = p_1, \ \theta_k(p) = p_k \cdot \frac{1+p_1}{2} \cdot \prod_{i=2}^{k-1} (1 + \tfrac{1}{2}p_i) \qquad (\textit{for } k \geqq 2). \tag{28}$$

Shifting the accent, *we call a gauge function* $f(x_1, \cdots, x_n)$ *reduced if it satisfies the inequalities*

$$f(x_1, \cdots, x_n) \geqq f(\overset{k}{\delta}_1, \cdots, \overset{k}{\delta}_n)$$

for any vector $(x_1, \cdots, x_n)$ *in* X_k *and* $k = 1, \cdots, n$. This means that the unit vectors $\mathfrak{e}_k = (\overset{k}{\delta}_1, \cdots, \overset{k}{\delta}_n)$ form a reduced lattice basis with respect to f. The inequalities (20) then hold for $L_k = f(\mathfrak{e}_k)$. If $f(\mathfrak{x})$ is any gauge function and $\mathfrak{z}_1, \cdots, \mathfrak{z}_n$ a reduced lattice basis with respect to f, we may set

$$f(x_1\mathfrak{z}_1 + \cdots + x_n\mathfrak{z}_n) = f^*(x_1, \cdots, x_n).$$

Then $f^*(x_1, \cdots, x_n)$ is a reduced gauge function, and we see that any gauge function f can be carried over into a reduced one by a unimodular transformation S of its variables. We shall adopt this terminology in Chapter II while at present we stick to talking in terms of reduced bases rather than gauge functions.

4. **The question of uniqueness.** Denote by X_k^* the set X_k after excluding the two n-uples

$$(x_1, \cdots, x_n) = \pm (\overset{k}{\delta}_1, \cdots, \overset{k}{\delta}_n).$$

The lattice basis $\mathfrak{z}_1, \cdots, \mathfrak{z}_n$ is said to be *properly reduced* when for every $k = 1, \cdots, n$ and for every $(x_1, \cdots, x_n)$ in X_k^* the inequality (18) holds with the $>$ sign.

The 2^n diagonal transformations of the modular group,

$$J: \ \mathfrak{z}_1' = \pm \mathfrak{z}_1, \cdots, \mathfrak{z}_n' = \pm \mathfrak{z}_n$$

(all possible combinations of signs admitted) form a finite Abelian subgroup $\{J\}$ of order 2^n. Its generators are the involutions $J_1, \cdots, J_n$ which change one sign at a time:

$$J_k: \mathfrak{z}_k' = -\mathfrak{z}_k \text{ and } \mathfrak{z}_j' = \mathfrak{z}_j \text{ for all } j \neq k.$$

Clearly the J carry a reduced basis $(\mathfrak{z}_1, \cdots, \mathfrak{z}_n)$ into a reduced one. The first result concerning the question of uniqueness is that this exhausts the possibilities, provided $(\mathfrak{z}_1, \cdots, \mathfrak{z}_n)$ is *properly* reduced [10]. Of two lattice bases $(\mathfrak{z}_1, \cdots, \mathfrak{z}_n)$ and $(\mathfrak{z}_1', \cdots, \mathfrak{z}_n')$, the first is called *lower* than the second provided the first nonvanishing difference

$$f(\mathfrak{z}_1') - f(\mathfrak{z}_1), \cdots, f(\mathfrak{z}_n') - f(\mathfrak{z}_n)$$

happens to be positive (which includes the case for which they are all zero).

THEOREM 7. *Let* $(\mathfrak{s}_1', \cdots, \mathfrak{s}_n')$ *be any lattice basis and* $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ *be a properly reduced lattice basis. In these circumstances* $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ *is lower than* $(\mathfrak{s}_1', \cdots, \mathfrak{s}_n')$, *and the equations*

$$f(\mathfrak{s}_1') = f(\mathfrak{s}_1), \cdots, f(\mathfrak{s}_k') = f(\mathfrak{s}_k)$$

imply

$$\mathfrak{s}_1' = \pm \mathfrak{s}_1, \cdots, \mathfrak{s}_k' = \pm \mathfrak{s}_k.$$

If $(\mathfrak{s}_1', \cdots, \mathfrak{s}_n')$ *is reduced and* $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ *is properly reduced, then*

$$\mathfrak{s}_1' = \pm \mathfrak{s}_1, \cdots, \mathfrak{s}_n' = \pm \mathfrak{s}_n.$$

Proof. Under the hypothesis that $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ is properly reduced, we have to show that

$$\mathfrak{s}_1' = \pm \mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}' = \pm \mathfrak{s}_{k-1} \tag{29}$$

imply $f(\mathfrak{s}_k') \geqq f(\mathfrak{s}_k)$, and even $f(\mathfrak{s}_k') > f(\mathfrak{s}_k)$ unless $\mathfrak{s}_k' = \pm \mathfrak{s}_k$.

Because of (29), $\mathfrak{s}_k'$ is a primitive adjunction to

$$[\mathfrak{s}_1', \cdots, \mathfrak{s}_{k-1}'] = [\mathfrak{s}_1, \cdots, \mathfrak{s}_{k-1}],$$

and hence

$$f(\mathfrak{s}_k') \geqq f(\mathfrak{s}_k). \tag{30}$$

As $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ is properly reduced, the equality sign in (30) will hold only if $\mathfrak{s}_k' = \pm \mathfrak{s}_k$.

Suppose $\mathfrak{s}_1', \cdots, \mathfrak{s}_n'$ is reduced and (29) holds. Since $\mathfrak{s}_k$ is a primitive adjunction to $[\mathfrak{s}_1', \cdots, \mathfrak{s}_{k-1}']$, we must have $f(\mathfrak{s}_k) \geqq f(\mathfrak{s}_k')$ in addition to (30), and hence $f(\mathfrak{s}_k') = f(\mathfrak{s}_k)$, an equation which we have just found impossible unless $\mathfrak{s}_k' = \pm \mathfrak{s}_k$. This establishes the full content of our theorem.

Much less can be said if the reduced basis $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ is not properly reduced.

THEOREM 8. *If*

$$\mathfrak{s}_1, \cdots, \mathfrak{s}_n; \qquad \mathfrak{s}_1', \cdots, \mathfrak{s}_n'$$

are two reduced bases, then

$$L_k = f(\mathfrak{s}_k), \qquad L_k' = f(\mathfrak{s}_k')$$

satisfy the inequalities

$$\theta_k L_k \geqq L_k', \qquad \theta_k L_k' \geqq L_k. \tag{31}$$

(This proposition indicates how far the uniqueness of the M_k survives for the L_k.)

Proof. Because there are k linearly independent lattice vectors $\mathfrak{x}=\mathfrak{s}_1, \cdots, \mathfrak{s}_k$ for which $f(\mathfrak{x})\leqq L_k$, L_k cannot be smaller than M_k. Hence

$$(32)\qquad \begin{aligned} M_k &\leqq L_k, & L_k &\leqq \theta_k M_k;\\ M_k &\leqq L_k', & L_k' &\leqq \theta_k M_k. \end{aligned}$$

Elimination of M_k leads to the two inequalities (31).

The case when $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ is reduced while the basis $(\mathfrak{s}_1', \cdots, \mathfrak{s}_n')$ has the property $B(p_1, \cdots, p_n)$ will also be needed later. The k linearly independent vectors $\mathfrak{s}_1', \cdots, \mathfrak{s}_{k-1}', \mathfrak{s}_k'$ impart values to f which are less than or equal to

$$p_1L_k', \cdots, p_{k-1}L_k', L_k'$$

respectively. Hence

$$M_k \leqq p_{k-1}L_k', \qquad L_k' \leqq \theta_k(p)\cdot M_k.$$

Substituting these inequalities for the second line of (32) and again eliminating M_k we find:

THEOREM 8_p. *For a reduced basis* $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ *and a basis* $(\mathfrak{s}_1', \cdots, \mathfrak{s}_n')$ *of the property*

$$B(p_1, \cdots, p_n) \qquad (1 = p_0 \leqq p_1 \leqq \cdots \leqq p_n)$$

the values

$$L_k = f(\mathfrak{s}_k), \qquad L_k' = f(\mathfrak{s}_k')$$

satisfy the inequalities

$$(33)\qquad L_k' \leqq \theta_k(p)\cdot L_k, \qquad L_k \leqq \theta_k p_{k-1}\cdot L_k'.$$

With the same effort one could have established similar relations for two bases of the properties $B(p_1, \cdots, p_n)$ and $B(p_1', \cdots, p_n')$ respectively. The present generality, however, is sufficient for our purposes.

THEOREM 9_p. *If, for a certain* $k=1, \cdots, n-1$,

$$(34)\qquad \theta_k(p)\theta_{k+1}\cdot L_k < L_{k+1},$$

then $\mathfrak{s}_1', \cdots, \mathfrak{s}_k'$ *are linear combinations of the vectors* $\mathfrak{s}_1, \cdots, \mathfrak{s}_k$ *only and thus arise from them by a unimodular transformation of degree* k.

Proof. Suppose that in one of the vectors $\mathfrak{s}_1', \cdots, \mathfrak{s}_k'$, say

$$\mathfrak{s}_i' = \overset{i}{s_1}\mathfrak{s}_1 + \cdots + \overset{i}{s_n}\mathfrak{s}_n,$$

not all the components s_i^j, $(j=k+1, \cdots, n)$, vanish. Then $\mathfrak{s}_1, \cdots, \mathfrak{s}_k, \mathfrak{s}_i'$ are linearly independent and hence the maximum of the $k+1$ numbers

$$L_1 = f(\mathfrak{s}_1), \cdots, L_k = f(\mathfrak{s}_k), L_i' = f(\mathfrak{s}_i')$$

must be greater than or equal to M_{k+1}. If on the contrary

$$L_1, \cdots, L_k; \qquad L_1', \cdots, L_k' \tag{35}$$

are all less than M_{k+1}, then the $\mathfrak{s}_1', \cdots, \mathfrak{s}_k'$ are linear combinations of $\mathfrak{s}_1, \cdots, \mathfrak{s}_k$ only. Now

$$L_i' \leqq \theta_i(p) \cdot L_i \qquad (i = 1, \cdots, k),$$

and owing to

$$L_1 \leqq \cdots \leqq L_k, \qquad 1 \leqq \theta_1(p) \leqq \cdots \leqq \theta_k(p)$$

all our requirements concerning (35) can be met by the one condition

$$\theta_k(p) \cdot L_k < M_{k+1}$$

which in its turn is a consequence of

$$\theta_k(p) \cdot L_k < L_{k+1}/\theta_{k+1}$$

because $L_{k+1} \leqq \theta_{k+1} M_{k+1}$.

In the particular case where $(\mathfrak{s}_1', \cdots, \mathfrak{s}_n')$ is likewise reduced $(p_1 = \cdots = p_n = 1)$, we have the following close parallel to Theorem 2:

THEOREM 9. *Let $\mathfrak{s}_1, \cdots, \mathfrak{s}_n$ and $\mathfrak{s}_1', \cdots, \mathfrak{s}_n'$ be two reduced bases of $\mathfrak{L}$, and $f(\mathfrak{s}_k) = L_k$. Suppose that moreover, for some $k \leqq n-1$,*

$$\theta_k \theta_{k+1} L_k < L_{k+1}.$$

Then the first k vectors $\mathfrak{s}_1', \cdots, \mathfrak{s}_k'$ are linear combinations of $\mathfrak{s}_1, \cdots, \mathfrak{s}_k$ only.

B. THE IMAGINARY AND QUATERNION CASES

5. **Integers and Minkowski's inequality in the complex field.** *Complex numbers $\xi = x_0 + ix_1$* have two real components x_0, x_1. We denote the conjugate by $\bar{\xi} = x_0 - ix_1$. Trace and norm:

$$\operatorname{tr} \xi = \xi + \bar{\xi} = 2x_0, \qquad \mathrm{N}\xi = \xi\bar{\xi} = |\xi|^2 = x_0^2 + x_1^2$$

are real and the coefficients of a quadratic equation satisfied by ξ:

$$\xi^2 - \xi \cdot \operatorname{tr} \xi + \mathrm{N}\xi = 0. \tag{36}$$

Let ω be a non-real number. $1, \omega$ span a lattice $\mathfrak{J}$ in the Gaussian plane consisting of all numbers

$$\xi = y_0 + y_1\omega \qquad (y_0, y_1 \text{ integers}). \tag{37}$$

If $\mathfrak{J}$ is closed with respect to multiplication and the operation $\xi \to \bar{\xi}$, then $\mathfrak{J}$ is a self-conjugate ring, and we agree to call the elements of $\mathfrak{J}$ *integers*. Owing to the choice of 1 as an element of the lattice basis $1, \omega$, the only real integers (with $y_1 = 0$) are the common rational integers. Trace and norm of an integer ξ are rational integers. Hence the quadratic equation (36) for $\xi = \omega$ shows that ω

is of the form $\frac{1}{2}(c+id^{1/2})$ where c and d are rational integers and either

$$c \equiv 0 \ (2), \quad d \equiv 0 \ (4), \quad \text{or} \quad c \equiv 1 \ (2), \quad d \equiv 1 \ (4).$$

The lattice $\mathfrak{J}$ is rectangular in the first, rhombic in the second case. The density of the lattice $\mathfrak{J}$, that is to say, the area of its fundamental parallelogram spanned by $1, \omega$, is $\frac{1}{2}d^{1/2}$.

The numbers of the form (37) with rational coefficients y_0, y_1 form the embedding *field* $\mathfrak{J}_0$. Indeed if $\xi \neq 0$ is in $\mathfrak{J}_0$ so is

$$\xi^{-1} = \bar{\xi}/\mathrm{N}\xi.$$

$\mathfrak{J}_0$ is the quadratic field over the rational field determined by $(-d)^{1/2}$. The x_0, x_1 and y_0, y_1, formula (37), are always spoken of as the x- and y-components of a complex number $\xi = x_0 + ix_1$.

We ask for the least radius r such that the circles of radius r around all integers cover the whole ξ-plane. One readily finds in the rectangular case,

$$r = \tfrac{1}{2}(1 + \tfrac{1}{4}d)^{1/2},$$

and in the rhombic case

$$r = \frac{1+d}{4d^{1/2}}.$$

If ξ is any complex number, one can always ascertain an integer α such that

$$\mathrm{N}(\xi - \alpha) \leqq r^2.$$

Another constant which will crop up later is the least norm e^2 of an integer $\alpha \neq 0$ which is not a unit (i.e. for which $1/\alpha$ is no integer); e is either $2^{1/2}$, $3^{1/2}$ or 2.

We operate in a vector space E_n of $2n$ real dimensions whose vectors $\mathfrak{x} = (\xi_1, \cdots, \xi_n)$ have arbitrary complex coordinates ξ_i. The lattice $\mathfrak{L}$ consists of all vectors whose coordinates ξ_i are integers (elements of $\mathfrak{J}$). The notion of a lattice basis needs no explanation. The modular group $\{S\}$ consists of all unimodular transformations S,

$$\xi_i = \sum_k \xi_k' \sigma_i^k$$

with integral coefficients σ_i^k whose determinant is a unit ϵ.

A *gauge function* is a real-valued continuous function $f(\xi_1, \cdots, \xi_n)$ with the following three properties:

(i) $f(\xi_1, \cdots, \xi_n) > 0$ except for $(\xi_1, \cdots, \xi_n) = (0, \cdots, 0)$;

(ii) $f(\tau\xi_1, \cdots, \tau\xi_n) = |\tau| \cdot f(\xi_1, \cdots, \xi_n)$;

(iii) $f(\xi_1 + \xi_1', \cdots, \xi_n + \xi_n') \leqq f(\xi_1, \cdots, \xi_n) + f(\xi_1', \cdots, \xi_n')$.

We introduce real coordinates x_{k0}, x_{k1} by $\xi_k = x_{k0} + ix_{k1}$ and use them in defin-

ing the volumes of solids in our space. In particular V denotes the volume of the gauge body

$$\mathfrak{K}: \quad f(\xi_1, \cdots, \xi_n) < 1.$$

We carry out Minkowski's construction according to the same recipe as in the real case and thus determine n lattice vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$ and consecutive minima $M_k = f(\mathfrak{d}_k)$. Our first concern is the analogue of Minkowski's inequality:

THEOREM 1*.

$$M_1^2 \cdots M_n^2 V \leqq (2d^{1/2})^n. \tag{38}$$

We resort to Minkowski's original inequality in the form (17). But under the present circumstances we deal with $2n$ real coordinates x_{k0}, x_{k1} and with a lattice which is the direct product of n two-dimensional lattices of density $\frac{1}{2}d^{1/2}$ rather than 1. Hence the right side in (17) is to be replaced by

$$2^{2n}(\tfrac{1}{2}d^{1/2})^n = (2d^{1/2})^n.$$

The only lattice vectors $\mathfrak{x}$ for which $f(\mathfrak{x}) < M_k$ are linear combinations of $\mathfrak{d}_1, \cdots, \mathfrak{d}_{k-1}$ with complex coefficients. Hence there are at most $2(k-1)$ vectors satisfying this inequality which are linearly independent in the real sense. Consequently we may take

$$M'_{2k-1} = M'_{2k} = M_k,$$

and in this way the inequality

$$M'_1 \cdots M'_{2n} \cdot V \leqq (2d^{1/2})^n$$

results in (38).

6. **The same for quaternions.** A *quaternion* ξ has four real components (x_0, x_1, x_2, x_3). The conjugate is $\bar{\xi} = (x_0, -x_1, -x_2, -x_3)$. The quaternions $(x, 0, 0, 0)$ can be identified with the real numbers x. Both trace and norm:

$$\operatorname{tr} \xi = \xi + \bar{\xi} = 2x_0, \qquad \mathrm{N}\xi = \xi\bar{\xi} = |\xi|^2 = x_0^2 + x_1^2 + x_2^2 + x_3^2,$$

are such real numbers. Every quaternion $\xi \neq 0$ has its reciprocal

$$\xi^{-1} = \bar{\xi}/\mathrm{N}\xi; \tag{39}$$

but since multiplication is noncommutative we have to do with a division algebra rather than a field. Each quaternion ξ satisfies the quadratic equation (36) with real coefficients.

Any lattice $\mathfrak{J}$ in the four-dimensional space with the real coordinates x_0, x_1, x_2, x_3 which is spanned by four linearly independent quaternions including 1,

$$\omega_0 = 1, \quad \omega_1, \quad \omega_2, \quad \omega_3, \tag{40}$$

may serve to define the integral quaternions as those of the form

$$\xi = y_0\omega_0 + y_1\omega_1 + y_2\omega_2 + y_3\omega_3 \tag{41}$$

with ordinary integral coefficients y, provided $\mathfrak{J}$ is closed with respect to multiplication and the operation $\xi \to \bar{\xi}$. Then trace and norm of a quaternion integer are rational integers. As (39) shows, the quaternions (41) with rational y form the embedding field $\mathfrak{J}_0$. We denote by $\frac{1}{4}d$ the density of the lattice $\mathfrak{J}$, and maintain that d is a rational integer. Although this fact is of little importance to us I shall briefly indicate its proof.

With (41) we form

$$\mathrm{N}\xi = \sum_{i,k=0}^{3} a_{ik}y_iy_k \ (= x_0^2 + x_1^2 + x_2^2 + x_3^2). \tag{42}$$

The coefficients

$$a_{ii} \text{ and } 2a_{ik} \text{ for } i \equiv k \tag{43}$$

are rational integers. According to the transformation theory of quadratic forms the discriminant of (42) is $(\frac{1}{4}d)^2$ and hence, because of (43), d^2 is a rational integer. On the other side let us study the *field* $\mathfrak{J}_0$ and any basis $\omega_0 = 1, \omega_1, \omega_2, \omega_3$ of the field. Starting with (40) we may first subtract from ω_1 and ω_2 half their traces and thus provide for the conditions

$$\bar{\omega}_1 = -\omega_1, \qquad \bar{\omega}_2 = -\omega_2.$$

Then $\omega_1\omega_2 + \omega_2\omega_1$ is the trace of $\omega_1\omega_2$ and hence a real rational number $2c$. Replacing ω_2 by $\omega_2 + c\omega_1$, one gets

$$\omega_2\omega_1 = -\omega_1\omega_2.$$

$\omega_1\omega_2$ is in the field. Choosing it as ω_3 the form (42) becomes

$$y_0^2 + ay_1^2 + by_2^2 + aby_3^2$$

which shows that its discriminant is the square of a rational number. This property persists for any basis of $\mathfrak{J}_0$. Hence d^2 is the square of a rational number d, and, as d^2 is integral, so is d itself [11].

r and e have the same significance as before.

The vectors $\mathfrak{x} = (\xi_1, \cdots, \xi_n)$ which we now consider have arbitrary quaternions ξ_k for their components,

$$\begin{aligned} \xi_k &= (x_{k0}, x_{k1}, x_{k2}, x_{k3}) \\ &= y_{k0}\omega_0 + y_{k1}\omega_1 + y_{k2}\omega_2 + y_{k3}\omega_3. \end{aligned}$$

The definition of lattice vectors remains unchanged. The modular group con-

sists of all pairs of mutually inverse transformations

$$\xi_i = \sum_k \xi_k' \sigma_i^k, \qquad \xi_i' = \sum_k \xi_k \tau_i^k$$

with integral coefficients σ_i^k, τ_i^k. (This modification of the definition is forced upon us because a quaternion matrix $\|\sigma_i^k\|$ has no determinant.) One has to observe carefully the position of the factors. Our convention is that the subspace spanned by k linearly independent vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ consists of the vectors $\eta_1\mathfrak{d}_1 + \cdots + \eta_k\mathfrak{d}_k$ with the coefficients η in front of the vectors.

The description of a gauge function by the three properties (i), (ii), (iii) stays unaltered, with the factor τ in front of the variables $\xi_1, \cdots, \xi_n$ in (ii). Minkowski's inequality assumes the form

$$M_1^4 \cdots M_n^4 \cdot V \leqq 2^{4n}(\tfrac{1}{4}d)^n,$$

which we put down as

THEOREM 1**.

$$M_1^2 \cdots M_n^2 \cdot V^{1/2} \leqq (2d^{1/2})^n. \tag{44}$$

7. **Reduction.** What remains will be done simultaneously for the imaginary and the quaternion cases in such language as applies literally to the more complex of the two. We have to check Lemmas 1–3 of §1 as to their validity under the new circumstances.

Both proofs of Lemma 1 go through with the following precautions. (5) is to be written down in terms of the $4n$ integral y-components of the vectors and coefficients concerned, and the positive rational integer M is the absolute value of the determinant of the linear equations with $4n$ unknowns thus obtained. The inequalities (8) for a reduced vector (7),

$$\mathfrak{x}^* = \eta_1^*\mathfrak{d}_1 + \cdots + \eta_k^*\mathfrak{d}_k,$$

must be replaced by

$$\mathrm{N}\eta_1^* \leqq r^2, \cdots, \mathrm{N}\eta_k^* \leqq r^2.$$

In order to secure the validity of Lemmas 2 and 3 an essentially new assumption has to be made:

HYPOTHESIS P. *Every left or right ideal in the ring $\mathfrak{J}$ is a principal ideal.*

As far as left ideals are concerned it requires: Any integers

$$(\alpha_1, \cdots, \alpha_h) \neq (0, \cdots, 0)$$

have a left common divisor δ,

$$\alpha_1 = \delta\cdot\beta_1, \cdots, \alpha_h = \delta\cdot\beta_h \qquad (\beta_1, \cdots, \beta_h \text{ integers}),$$

which can be written as a linear combination

$$\alpha_1\lambda_1 + \cdots + \alpha_h\lambda_h \tag{45}$$

with integral coefficients λ_i. This divisor δ, which up to a right unit factor is uniquely determined, is called the left G.C.D. of $\alpha_1, \cdots, \alpha_h$. (The integers represented by (45) if the λ_i range independently over all integers coincide with the values of $\delta\cdot\mu$ for all possible integral values of μ. It is sufficient to make the requirement for two integers α_1, α_2.)

Lemma 2, in which the last words "*without common divisor*" must be changed into "*without left common divisor*," is true under the hypothesis P for *left* ideals (P_l). Change the Roman into Greek letters and define d, or rather δ, as the left G.C.D. of $\alpha_k, \cdots, \alpha_n$. The alternative 1 occurs if δ is not a unit, the alternative 2 if $\alpha_k, \cdots, \alpha_n$ are without left common divisor (which means, of course, that they have no left common divisors except units).

One has merely to glance through the proof of Lemma 3 in order to realize that it depends on the hypothesis P for *right* ideals. We obtain the primitive adjunction in the form

$$\mathfrak{s} = (1/\mu)\mathfrak{d} + \tau_1\mathfrak{s}_1 + \cdots + \tau_{k-1}\mathfrak{s}_{k-1}$$

where μ is a nonzero integer and the τ satisfy the inequalities

$$N\tau_1 \leqq r^2, \cdots, N\tau_{k-1} \leqq r^2.$$

If μ is a unit one may take

$$\mathfrak{s} = \mathfrak{d}, \text{ i.e.,} \quad \mu = 1, \quad \tau_1 = \cdots = \tau_{k-1} = 0.$$

As $N\mu \geqq 1$ for any integer $\mu \neq 0$, the inequality (15) is turned over into

$$f(\mathfrak{s}) \leqq f(\mathfrak{d}) + r\{f(\mathfrak{s}_1) + \cdots + f(\mathfrak{s}_{k-1})\}$$

while in (16) the smallest norm $e^2 > 1$ of integers makes its appearance:

$$f(\mathfrak{s}) \leqq \max\{f(\mathfrak{d}), (1/e)f(\mathfrak{d}) + r(f(\mathfrak{s}_1) + \cdots + f(\mathfrak{s}_{k-1}))\}.$$

Incidentally hypotheses P_l and P_r are fulfilled if $r<1$. For then Euclid's algorithm for the G.C.D. goes through. In the complex field this happens for the rectangular lattices $\mathfrak{J}$ with $d=4$ (Gaussian field) and $d=8$, and for the rhombic lattices $\mathfrak{J}$ with $d=3, 7, 11$. The most important example for quaternions is the classical case first treated by A. Hurwitz [12]: he declares a quaternion (x_0, x_1, x_2, x_3) to be integral when $2x_0, 2x_1, 2x_2, 2x_3$ are rational integers either congruent to $(0, 0, 0, 0)$ or to $(1, 1, 1, 1)$ modulo 2. One realizes at once that here $r<1$; the exact value is $r=1/3^{1/2}$.

The whole theory of reduction of §§3 and 4 will now go through, practically without alterations. We indicate the few changes to be made. X_k is the set of all n-uples $(\xi_1, \cdots, \xi_n)$ for which $\xi_1, \cdots, \xi_n$ are integral and $\xi_k, \cdots, \xi_n$

without *left* common divisor. X_k^* arises from X_k by excluding the following n-uples:

$$\epsilon(\overset{k}{\delta}_1, \cdots, \overset{k}{\delta}_n) \qquad (\epsilon \text{ a unit}).$$

$\{J\}$ consists of the diagonal transformations

$$J: \quad \mathfrak{z}_1' = \epsilon_1\mathfrak{z}_1, \cdots, \mathfrak{z}_n' = \epsilon_n\mathfrak{z}_n, \quad \text{or} \quad \xi_1 = \xi_1'\epsilon_1, \cdots, \xi_n = \xi_n'\epsilon_n$$

where $\epsilon_1, \cdots, \epsilon_n$ are units. This group is the direct product of n factors each of which is isomorphic with the group of units. The most essential point concerns the values of the constants θ_k, $\theta_k(p)$ and μ_n.

Instead of the recursive formula (22) we get $\theta_k = 1 + r(\theta_1 + \cdots + \theta_{k-1})$ leading to

$$\theta_k = (1 + r)^{k-1}.$$

Similarly

$$\theta_k(p) = p_k \cdot \prod_{i=1}^{k-1} (1 + rp_i).$$

THEOREM 5**. *The inequality*

$$\overset{2}{L}_1 \cdots \overset{2}{L}_n \cdot V^{2/\kappa} \leqq \overset{2}{\mu}_n$$

holds, where $\kappa = 1, 2, 4$ *characterize the real, imaginary and quaternion cases respectively and*

$$\overset{2}{\mu}_n = \left\{2d^{1/2} \cdot (1 + r)^{n-1}\right\}^n.$$

(*In the real case* $d = 4$, $r = \frac{1}{2}$.)

The same trick as used before, compare formulas (27) and (28), allows us to improve to some extent these values of θ_k, $\theta_k(p)$ and μ_n.

CHAPTER II. REDUCTION OF QUADRATIC, HERMITIAN AND HAMILTONIAN FORMS

8. **Jacobi transformation.** A *quadratic form*

$$f(\mathfrak{x}) = \sum g_{ij}x_ix_j \qquad (i, j = 1, \cdots, n) \tag{46}$$

of n variables $(x_1, \cdots, x_n) = \mathfrak{x}$ is characterized by its real symmetric coefficients $g_{ij} = g_{ji}$ and may thus be denoted by $f = \{g_{ij}\}$. All quadratic forms constitute a linear space R of $N = \frac{1}{2}n(n+1)$ dimensions. In the imaginary and the quaternion cases the analogues are the *Hermitian* and "*Hamiltonian*" *forms* respectively,

$$f(\xi_1, \cdots, \xi_n) = \sum_{i,j} \xi_i\gamma_{ij}\bar{\xi}_j \tag{47}$$

whose complex or quaternion coefficients satisfy the symmetry condition

$$\gamma_{ji} = \bar{\gamma}_{ij}. \tag{48}$$

The conjugate of a product is the product of the conjugates in inverted order. This rule at once shows that the value of f is real, $\bar{f}=f$. In the quaternion case one has to watch out for the order of the factors on the right side of (47). The substitution $x_i \to tx_i$ multiplies the quadratic form (46) with $t^2 = |t|^2 = \mathrm{N}t$, while $\xi_i \to \tau\xi_i$ changes (47) into $\tau f \bar{\tau}$, or since f is real, into

$$\tau\bar{\tau}\cdot f = \mathrm{N}\tau\cdot f.$$

The diagonal coefficients γ_{ii} are real while the skew coefficients γ_{ij} on one side of the diagonal, $i<j$, may be chosen arbitrarily and then determine the coefficients γ_{ji} on the other side by (48). Hence the quadratic, Hermitian and Hamiltonian forms f constitute linear spaces of

$$N = n + \kappa\cdot\frac{n(n-1)}{2}$$

or of

$$N = \tfrac{1}{2}n(n+1), \qquad n^2, \qquad n(2n-1)$$

dimensions respectively. The form f is said to be *positive* if $f(\mathfrak{x})>0$ except for $\mathfrak{x}=0$. According to our remarks above, $f^{1/2}$ may then serve as gauge function in the real, imaginary or quaternion vector spaces.

Jacobi's transformation is a uniquely determined linear transformation of recursive character of a positive quadratic form into a square sum. It is nothing else than the method of "completing the square" which, probably some 4000 years ago, was invented for the solution of quadratic equations. It no less applies to Hermitian and Hamiltonian forms, though in the latter case we have to bear in mind that there are no determinants. Thus we had better disregard this formal tool altogether. The discriminant of the form will be defined by recursion in the course of our construction. Its general explicit expression in terms of the coefficients γ_{ij} is a task about which we need not bother here [13]. I now give the description of the process for positive Hamiltonian forms f.

If f is positive, then γ_{11} is real and greater than 0, $\gamma_{11}=q_1$. We form

$$\zeta_1 = \xi_1 + \xi_2\frac{\gamma_{21}}{\gamma_{11}} + \cdots + \xi_n\frac{\gamma_{n1}}{\gamma_{11}}$$

which implies

$$\bar{\zeta}_1 = \bar{\xi}_1 + \frac{\gamma_{12}}{\gamma_{11}}\bar{\xi}_2 + \cdots + \frac{\gamma_{1n}}{\gamma_{11}}\bar{\xi}_n$$

and find

$$f(\xi_1, \cdots, \xi_n) = q_1\zeta_1\bar{\zeta}_1 + f^*(\xi_2, \cdots, \xi_n) \tag{49}$$

where the remainder f^* depends on the variables $\xi_2, \cdots, \xi_n$ only. Incidentally its coefficients are given by

$$\overset{*}{\gamma}_{ij} = \gamma_{ij} - \frac{\gamma_{i1}\gamma_{1j}}{\gamma_{11}}. \tag{50}$$

f^* is positive; for if $\xi_2, \cdots, \xi_n$ are any given values we may determine ξ_1 by the equation

$$\xi_1 + \xi_2\frac{\gamma_{21}}{\gamma_{11}} + \cdots + \xi_n\frac{\gamma_{n1}}{\gamma_{11}} = 0$$

and then

$$f^*(\xi_2, \cdots, \xi_n) = f(\xi_1, \xi_2, \cdots, \xi_n) > 0$$

except for $\xi_2 = \cdots = \xi_n = 0$. Iteration of the splitting (49), therefore, leads to an expression

$$f(\mathfrak{x}) = q_1|\zeta_1|^2 + \cdots + q_n|\zeta_n|^2 \tag{51}$$

(Jacobi's transform) where the q are positive numbers and ζ_i linear forms of the recursive type

$$\zeta_i = \xi_i + \sum_{(j>i)} \xi_j\beta_{ji}. \tag{52}$$

The product $q_1 \cdots q_n = D = D_n$ is called the discriminant of f.

Break the sum (51) into two parts according to

$$f(\mathfrak{x}) = (q_1|\zeta_1|^2 + \cdots + q_{k-1}|\zeta_{k-1}|^2) + (q_k|\zeta_k|^2 + \cdots + q_n|\zeta_n|^2)$$

and substitute $\mathfrak{x} = \mathfrak{e}_k$. The value of the whole form is γ_{kk} while the value of the second summand is q_k. Hence

$$q_k \leqq \gamma_{kk}, \tag{53}$$

$$D \leqq \gamma_{11} \cdots \gamma_{nn}. \tag{54}$$

The Jacobi transformation of the positive form

$$f^{(k)} = f(\xi_1, \cdots, \xi_k, 0, \cdots, 0)$$

of k variables is obtained from (51) by setting $\xi_{k+1} = \cdots = \xi_n = 0$. Consequently its discriminant is $D_k = q_1 \cdots q_k$ and thus

$$q_k = D_k/D_{k-1} \qquad (k = 1, \cdots, n; D_0 = 1).$$

The first step (49) goes through under the sole assumption $\gamma_{11} = q_1 > 0$. If, in carrying the process further for a given form f, we find $q_2 > 0, \cdots, q_n > 0$

at the following steps, then the formula (51) itself reveals that f is positive.

By (50) the inequality $q_2 > 0$ amounts to

$$|\gamma_{21}|^2 = |\gamma_{12}|^2 < \gamma_{11}\cdot\gamma_{22}.$$

More generally we must have

$$|\gamma_{ij}|^2 < \gamma_{ii}\cdot\gamma_{jj} \qquad (i \neq j)$$

for any positive form f.

Next we compute the volume V of the $4n$-dimensional ellipsoid $f(\mathfrak{x}) < 1$. Denote by ω_n the volume of the sphere

$$x_1^2 + \cdots + x_n^2 < 1$$

in the n-dimensional real vector space. When in the recursive substitution (52) we replace each of the quaternions ξ and ζ by its 4 real x-components, we again obtain a recursive substitution, this time in $4n$ variables, whose coefficient matrix has 1's along the principal diagonal and hence is of determinant 1. Thus the volume V is the same as that of the Jacobi transform $\sum_i q_i|\xi_i|^2 < 1$ or in real x-components

$$\sum_{i=1}^{n}\sum_{\alpha=0}^{3}(q_i^{1/2}x_{i\alpha})^2 < 1.$$

Consequently

$$V = \frac{\omega_{4n}}{(q_1^{1/2}\cdots q_n^{1/2})^4} = \frac{\pi^{2n}}{(2n)!}\,\frac{1}{q_1^2\cdots q_n^2} = \frac{\pi^{2n}}{(2n)!}\cdot\frac{1}{D^2}. \tag{55}$$

In the real and the imaginary case one finds

$$V = \frac{\omega_n}{D^{1/2}}, \qquad V = \frac{\omega_{2n}}{D} = \frac{\pi^n}{n!}\cdot\frac{1}{D} \tag{56}$$

instead. Incidentally these formulas prove that, although our recursive definition refers to a definite arrangement, the discriminant of f is not changed by arranging the variables $\xi_1, \cdots, \xi_n$ in a different order.

From here on we limit ourselves to real quadratic forms, because the adjustments to the two other cases are sufficiently trivial; only an occasional glance will be cast upon them.

9. **Some simple topological considerations.** Within the N-dimensional linear space R of all quadratic forms $f = \{g_{ij}\}$ the positive ones form a convex subset G which is a cone with the origin $f = 0$ as vertex. The relative clause means that dilatation, $f \to tf$, at any positive rate t carries G into itself. G is an open set. Indeed the quantities emerging at the first step of Jacobi's transformation,

$$q_1 = g_{11}, \quad b_{i1} = \frac{g_{i1}}{g_{11}}, \quad \overset{*}{g}_{ij} = g_{ij} - \frac{g_{i1}g_{1j}}{g_{11}} \qquad (i, j = 2, \cdots, n),$$

all depend continuously on f. [We now use corresponding Roman instead of Greek letters throughout, so that the transformation (52) reads

$$z_i = x_i + \sum_{(j>i)} x_j b_{ji}. \tag{52'}$$]

Hence $q_1, \cdots, q_n$; b_{ji} $(j>i)$ depend continuously on f at a given point f^0 of G, and all forms f in a certain neighborhood U of f^0 will satisfy the conditions

$$q_1 \geqq \tfrac{1}{2}\overset{0}{q}_1, \cdots, q_n \geqq \tfrac{1}{2}\overset{0}{q}_n$$

and thus be positive.

Jacobi's transformation shows quite explicitly that for a given positive form f and a given number A the inequality $f(\mathfrak{x}) \leqq A$ entails upper bounds for the $|x_i|$ of $\mathfrak{x} = (x_1, \cdots, x_n)$. In fact, one first obtains upper bounds for $|z_1|, \cdots, |z_n|$ and then, going in backward direction, from the relations (52′) upper bounds for $|x_n|, |x_{n-1}|, \cdots, |x_1|$. One can make this estimate uniform throughout a sufficiently small neighborhood of a given form. Hence this

LEMMA 4. *Let $A(f)$ be a real function depending on a variable point f in G and continuous at the given point f^0. We can fix a neighborhood U of f^0 such that nearly every lattice vector $\mathfrak{x} = (x_1, \cdots, x_n)$ has the property of satisfying the inequality*

$$f(\mathfrak{x}) > A(f)$$

for all f in U.

("Nearly every" means that only a finite number lack the property in question.)

Proof. We fix the neighborhood U so that

$$q_k(f) \geqq \tfrac{1}{2}\overset{0}{q}_k, \qquad A(f) \leqq 1 + A(\overset{0}{f}), \qquad |b_{ji}(f)| \leqq 1 + |\overset{0}{b}_{ji}|.$$

If $\mathfrak{x}$ is a vector such that there is an f in U for which $f(\mathfrak{x}) \leqq A(f)$, then (51) yields upper bounds for $|z_k|$ which are universal in that they do not depend on the specific f in U, and (52′) yields universal bounds for $|x_n|, \cdots, |x_1|$.

From now on up to the end of §12, f without or with accent or index always indicates a point of G. All topological notions are to be interpreted relative to G; e.g., a subset of G is said to be open or closed whenever it is open or closed relative to G.

Before going on we specialize some of our previous definitions concerning gauge functions to gauge functions of the type $f^{1/2}$ now under consideration. *A positive quadratic form f is said to be reduced if it satisfies the inequality*

$$f(x_1, \cdots, x_n) \geqq g_{kk}$$

for any vector $(x_1, \cdots, x_n)$ *in* X_k *and for* $k=1, \cdots, n$. *This implies*

$$(0 <) g_{11} \leqq g_{22} \leqq \cdots \leqq g_{nn}.$$

Two forms f, f' are called equivalent and counted in the same class if one proceeds from the other by a substitution

$$x_i = \sum_k x_k' s_i^k$$

of the modular group. Every point f in G is equivalent to a reduced one.

To each index k and vector $\mathfrak{x}=(x_1, \cdots, x_n)$ in X_k there corresponds a linear form of the coordinates g_{ij} in R,

$$f(\mathfrak{x}) - g_{kk} = \sum_{i,j} x_i x_j g_{ij} - g_{kk} = \sum_{i,j} \alpha_{ij} g_{ij},$$

which we denote by $\alpha_k(\mathfrak{x})$; its coefficients are

$$\alpha_{ij} = x_i x_j - \delta_i^k \delta_j^k.$$

The relations for the variable point $\{g_{ij}\}$,

$$\sum \alpha_{ij} g_{ij} = 0, \qquad \geqq 0, \qquad > 0$$

are referred to as the *equation*, the *inequality* and the *strict inequality* $\alpha_k(\mathfrak{x})$ respectively. Except for $\mathfrak{x} = \pm \mathfrak{e}_k$, i.e., for every vector $\mathfrak{x}$ in X_k^*, the inequality and equation $\alpha_k(\mathfrak{x})$ define a half-space and its bounding $(N-1)$-dimensional plane in R. Now f is properly reduced provided the strict inequality $\alpha_k(\mathfrak{x})$ is satisfied for every $\mathfrak{x}$ in X_k^* and every k. Examples of properly reduced forms are ready at hand; the simplest are the diagonal forms

$$g_1 x_1^2 + \cdots + g_n x_n^2 \qquad \text{with } 0 < g_1 < g_2 < \cdots < g_n.$$

The reduced points form a closed convex subset Z of G which again is a cone and will be called the (basic) *cell*. A properly reduced f is said to belong to the *core* of Z. An inner point of Z belongs to its core. Each unimodular substitution S carries Z into an equivalent cell Z_S. The substitutions of the subgroup $\{J\}$ leave Z unchanged, but if S is not in $\{J\}$ then no point of the core of Z can be in Z_S (Theorem 7). Hence the equivalent cells Z_S cover G without gaps and overlappings; two different cells have none but boundary points in common. Here two substitutions like S and JS which are left equivalent modulo $\{J\}$ are to be identified because they have the same effect on Z. Our aim is first to study the individual cell Z and then the whole pattern of the division of G into equivalent cells.

We start with the observation that *a point* f^0 *belonging to the core of* Z *is*

an inner point of Z. Indeed according to Lemma 4, nearly every lattice vector $\mathfrak{x}$ satisfies the inequalities $f(\mathfrak{x}) > g_{kk}$ for $k = 1, \cdots, n$ and for all forms f in a certain neighborhood U of f^0. Therefore among the infinitely many inequalities

$$\alpha_k(\mathfrak{x}) \qquad (\mathfrak{x} \text{ in } X_k^*;\ k = 1, \cdots, n) \tag{57}$$

there are only a finite number, say $\alpha', \alpha'', \cdots$, which are not a priori sure to hold throughout U. But if the *strict* inequalities $\alpha', \alpha'', \cdots$ hold for f^0 then they hold also in a sufficiently small neighborhood U' of f^0; and the neighborhood $U \cap U'$ of f^0 lies in Z.

Denote by T_k the subset of X_k to which $\mathfrak{x}$ belongs if there are reduced forms f satisfying the equation $f(\mathfrak{x}) = g_{kk}$. The two vectors $\pm \mathfrak{e}_k$ belong to T_k, and again T_k^* designates what is left of T_k after these two vectors have been removed. The planes $\alpha_k(\mathfrak{x}) = 0$ corresponding to the $\mathfrak{x}$ in T_k^* graze the cell Z. Our last result asserts that every boundary point of Z lies in one of these grazing planes

$$\alpha_k(\mathfrak{x}) = 0 \qquad (\mathfrak{x} \text{ in } T_k^*,\ k = 1, \cdots, n). \tag{58}$$

Hence from a general topological principle which we shall presently prove for our special situation there follows

THEOREM 10. *In the definition of Z as the set consisting of all points f of G which satisfy the inequalities*

$$\alpha_k(\mathfrak{x}) \qquad \textit{for every } \mathfrak{x} \textit{ in } X_k \textit{ and } k = 1, \cdots, n, \tag{59}$$

the vector set X_k may be replaced by T_k^*.

Proof. Choose one of the points f^0 belonging to the core of Z as the center of Z and suppose f is any point (of G) outside Z. Join f^0 with f by a straight segment. Somewhere, at a point f', it will cross the border of Z; the part f^0f' of the segment, including f', belongs to Z while the points beyond f' are outside Z. The point f' satisfies one of the equations (58), say

$$\sum \alpha_{ij} g_{ij} = 0. \tag{60}$$

The left member of (60) is greater than 0 at f^0, equals 0 at f', and hence is less than 0 at f. Consequently a point f which satisfies all inequalities

$$\alpha_k(\mathfrak{x}) \geqq 0 \qquad (\mathfrak{x} \text{ in } T_k^*,\ k = 1, \cdots, n)$$

cannot lie outside Z [14].

We denote by X_k^0 the set of lattice vectors $(x_1, \cdots, x_n)$ for which

$$x_k = 1, \qquad x_{k+1} = \cdots = x_n = 0.$$

X_k^0 is a subset of X_k. Let ρ be any number greater than 1 and σ a positive

number. Later on we shall have occasion to study the part $G(\rho, \sigma)$ of G defined by the following simultaneous inequalities:

$$(61_1) \qquad f(x_1, \cdots, x_n) \geqq \frac{1}{\rho^2} \cdot g_{kk} \qquad \text{for every vector } (x_1, \cdots, x_n) \text{ in } X_k,$$

$$(61_2) \qquad f(x_1, \cdots, x_n) \geqq g_{kk} - \sigma g_{11} \qquad \text{for every vector } (x_1, \cdots, x_n) \text{ in } X_k^0$$

$$[k = 1, \cdots, n].$$

$G(\rho, \sigma)$ is a closed convex part of G which increases with increasing ρ and σ. A point f of G satisfying all these inequalities (61) with the $>$ sign is an inner point of $G(\rho, \sigma)$, as follows by the argument previously applied to Z. The domain $G(\rho, \sigma)$ contains the cell Z in its interior. I propose to show that with $\rho \uparrow \infty$, $\sigma \uparrow \infty$ it exhausts the whole G. Let f be any point of G. All lattice vectors $(x_1, \cdots, x_n)$ except those of a certain finite set Σ satisfy the inequalities

$$f(x_1, \cdots, x_n) > g_{kk} \qquad (k = 1, \cdots, n)$$

and hence (61), whatever the values $\rho > 1$ and $\sigma > 0$. When $(x_1, \cdots, x_n)$ varies over the finite set $X_k \cap \Sigma$, $f(x_1, \cdots, x_n)$ will assume a least (positive) value g_{kk}/ρ_k^2. Thus all the inequalities (61_1), with the $>$ sign and for $k = 1, \cdots, n$, will hold as soon as $\rho > \rho_1, \rho_2, \cdots, \rho_n$. In the same manner one sees that, for a sufficiently high σ, f satisfies all relations (61_2) with the $>$ sign for $k = 1, \cdots, n$.

10. **The first theorem of finiteness.** We now resume the algebraic study of reduced forms, first specializing Theorem 5 for the gauge function $f^{1/2}$:

THEOREM 11. *Any reduced form $f = \{g_{ij}\}$ satisfies the inequality*

$$(62) \qquad \lambda_n g_{11} \cdots g_{nn} \leqq D$$

where $\lambda_n = (\omega_n/\mu_n)^2$.

About the constant μ_n see the Supplement to Theorems 4–6 in §3. We use the formulas (55) and (56) for the volumes of our ellipsoidal gauge bodies and thus obtain a corresponding inequality

$$\lambda_n \gamma_{11} \cdots \gamma_{nn} \leqq D$$

for reduced Hermitian and Hamiltonian forms, with

$$\lambda_n = \frac{\pi^n}{n!} \cdot \frac{1}{\mu_n^2}, \qquad \lambda_n = \frac{\pi^n}{[(2n)!]^{1/2}} \cdot \frac{1}{\mu_n^2}$$

and the values of μ_n^2 given by Theorem 5**. The resulting values of λ_n are certainly not optimal, but fairly good.

In passing we mention the following relations:

$$(63) \qquad |g_{ij}| \leqq \tfrac{1}{2}g_{ii}, \qquad |\gamma_{ij}| \leqq r\gamma_{ii},$$

which hold for reduced forms and for $i<j$. Choose two different indices, say 2 and 5. The two vectors for which $x_2=\pm 1$, $x_5=1$ and all other x_i vanish belong to X_5; hence

$$g_{22} \pm 2g_{25} + g_{55} \geqq g_{55}$$

or

$$2|g_{25}| \leqq g_{22}.$$

In the imaginary and quaternion cases the procedure is as follows. Let η range over all integers. We take $\xi_5=1$ and $\xi_2=-\eta$ while all other ξ_i vanish. The resulting inequality reads

$$\gamma_{22}\eta\bar{\eta} - \eta\gamma_{25} - \gamma_{52}\bar{\eta} \geqq 0$$

which for $\gamma=\gamma_{52}/\gamma_{22}$ yields

$$|\gamma - \eta|^2 \geqq |\gamma|^2.$$

This means that, in the lattice of integers, γ is not farther from zero than from any other integer. Hence this distance $|\gamma|$ cannot exceed r.

If $f(x_1, \cdots, x_n)$ is a reduced form of n variables, then

$$f^{(k)} = f(x_1, \cdots, x_k, 0, \cdots, 0)$$

is one of k variables, therefore

$$D_k \geqq \lambda_k g_{11} \cdots g_{kk}.$$

Combining this with (54) for $f^{(k-1)}$, $D_{k-1} \leqq g_{11} \cdots g_{k-1,k-1}$, *we find the important inequality*

$$q_k \geqq \lambda_k g_{kk} \qquad (k = 1, \cdots, n)$$

holding for reduced forms f.

We are now sufficiently prepared to prove the first theorem of finiteness:

THEOREM 12. *The set T_k of lattice vectors is finite.*

Hence by Theorem 10 we have succeeded in sifting from the infinitely many inequalities (59) a finite number on which all others are consequent and therefore redundant. In proving our proposition we shall give fairly explicit upper bounds of $|x_1|, \cdots, |x_n|$ for the vectors $\mathfrak{x}=(x_1, x_2, \cdots, x_n)$ in T_k.

Proof. Suppose $\mathfrak{x}$ is in T_k and f a reduced form for which $f(\mathfrak{x})=g_{kk}$. In particular $\mathfrak{x}=\mathfrak{e}_k$ fulfills this demand. We apply Jacobi's transformation to f and then find for the vector in question

$$q_1 z_1^2 + \cdots + q_n z_n^2 = g_{kk};$$

a fortiori

$$\sum_{j=k}^{n} q_j z_j^2 \leqq g_{kk}.$$

In the last sum $q_j \geqq \lambda_j g_{jj} \geqq \lambda_j g_{kk}$ $(j \geqq k)$, and thus the inequality

$$\sum_{j=k}^{n} \lambda_j z_j^2 \leqq 1$$

results which yields universal upper bounds for $|z_k|, \cdots, |z_n|$:

$$|z_j|^2 \leqq 1/\lambda_j \qquad (j = k, \cdots, n). \tag{64}$$

To find universal bounds for $|z_1|, \cdots, |z_{k-1}|$ is a slightly more intricate job. Let h be a given index less than k. Without altering $x_n, \cdots, x_{h+1}$ we may replace $x_h, \cdots, x_1$ by such integers $x_h^*, \cdots, x_1^*$ in succession that the corresponding $z_h^*, \cdots, z_1^*$ satisfy

$$|z_h^*| \leqq \tfrac{1}{2}, \cdots, |z_1^*| \leqq \tfrac{1}{2}.$$

Since the new vector $(x_1^*, \cdots, x_h^*, x_{h+1}, \cdots, x_n)$ also is in X_k, we must have

$$f(x_1^*, \cdots, x_h^*, x_{h+1}, \cdots, x_n) \geqq g_{kk},$$

consequently

$$(q_1 z_1^{*2} + \cdots + q_h z_h^{*2}) + (q_{h+1} z_{h+1}^2 + \cdots + q_n z_n^2)$$
$$\geqq g_{kk} = (q_1 z_1^2 + \cdots + q_h z_h^2) + (q_{h+1} z_{h+1}^2 + \cdots + q_n z_n^2)$$

or

$$q_1 z_1^{*2} + \cdots + q_h z_h^{*2} \geqq q_1 z_1^2 + \cdots + q_h z_h^2.$$

The left member is less than or equal to

$$r^2(q_1 + \cdots + q_h) \leqq r^2(g_{11} + \cdots + g_{hh}) \leqq r^2 h g_{hh} \qquad (r = \tfrac{1}{2}).$$

Hence

$$r^2 h g_{hh} \geqq q_h z_h^2 \geqq \lambda_h g_{hh} z_h^2 \quad \text{or}$$

$$z_h^2 \leqq r^2 h/\lambda_h \qquad (h = 1, \cdots, k-1). \tag{65}$$

(The notation r is used in order to cover also the imaginary and quaternion cases.)

Applying (65) to $\mathfrak{x} = \mathfrak{e}_k$, one gets

$$b_{kh}^2 \leqq r^2 h/\lambda_h \qquad (\text{for } h < k). \tag{66}$$

The universal upper bounds for $|z_n|, \cdots, |z_1|$ together with the universal bounds for the moduli of the coefficients b_{kh} in the recursive equations (52′) result in universal upper bounds for $|x_n|, \cdots, |x_1|$.

This argument is chiefly due to Minkowski and is in my view the backbone of his theory of reduction. The simple remark leading from (65) to (66) was first made by Remak [15]. It dispenses with the necessity of making use of the explicit expression of b_{kh} as Minkowski did, which is the more fortunate as it would have been quite cumbersome to follow his procedure in the quaternion case.

11. **The second theorem of finiteness. Generators of the modular group.** We prove now the following theorem.

THEOREM 13. *The set $G(\rho, \sigma)$ has points in common with not more than a finite number of cells Z_S.*

We must show that there is only a finite number of unimodular substitutions S capable of carrying an (unspecified) point f of Z into a point f' of $G(\rho, \sigma)$,

$$f(y_1\mathfrak{s}_1 + \cdots + y_n\mathfrak{s}_n) = f'(y_1, \cdots, y_n).$$

Here $(\mathfrak{s}_1, \cdots, \mathfrak{s}_n)$ is a lattice basis of the property $B(\rho, \cdots, \rho)$ with respect to $f^{1/2}$. Consider the two series of subspaces

$$E_0, \quad E_1 = [\mathfrak{e}_1], \quad E_2 = [\mathfrak{e}_1, \mathfrak{e}_2], \cdots, E_n;$$
$$E_0', \quad E_1' = [\mathfrak{s}_1], \quad E_2' = [\mathfrak{s}_1, \mathfrak{s}_2], \cdots, E_n'.$$

$E_0 = E_0'$ is the zero space, $E_n = E_n'$ the full vector space. Let l be the highest of the indices $1, \cdots, n$ for which

$$E_{l-1}' = E_{l-1}. \tag{67}$$

The decision whether or not $E_k' = E_k$ depends merely on checking whether some integers are zero. For l there exist the possibilities $l = 1, \cdots, n$. We propose to consider the S with a definite l.

First we focus our attention on the vectors

$$\mathfrak{s}_k \qquad (k = l, \cdots, n). \tag{68}$$

For the moment let $\mathfrak{x} = (x_1, \cdots, x_n)$ denote the vector $\mathfrak{s}_k$; then

$$f(\mathfrak{x}) = q_1 z_1^2 + \cdots + q_n z_n^2 = g_{kk}'. \tag{69}$$

Put

$$\theta_i' = \theta_i(p) \qquad \text{for } p_1 = \cdots = p_i = \rho.$$

Because of the significance of l and Theorem 9_p we have

$$(\theta_i' \theta_{i+1})^2 g_{ii} \geqq g_{i+1,i+1}$$

for $i \geqq l$. Therefore and because f is reduced,

$$
\begin{aligned}
q_l z_l^2 + \cdots + q_n z_n^2 &\geqq \lambda_l g_{ll} z_l^2 + \cdots + \lambda_n g_{nn} z_n^2 \\
&\geqq g_{kk}\Big\{\lambda_n z_n^2 + \cdots + \lambda_k z_k^2 + \frac{\lambda_{k-1}}{(\theta'_{k-1}\theta_k)^2} z_{k-1}^2 + \cdots \\
&\qquad + \frac{\lambda_l}{(\theta'_{k-1}\cdots\theta'_l\cdot\theta_k\cdots\theta_{l+1})^2} z_l^2\Big\},
\end{aligned}
\tag{70}
$$

while by Theorem 8_p

$$
g'_{kk} \leqq (\theta'_k)^2 g_{kk}. \tag{71}
$$

Combining the two inequalities (70) and (71) with (69), we get hold of universal upper bounds for $|z_l|, \cdots, |z_n|$, namely

$$
|z_k| \leqq \frac{\theta'_k}{\lambda_k^{1/2}}, \cdots, |z_n| \leqq \frac{\theta'_k}{\lambda_n^{1/2}},
$$

$$
|z_{k-1}| \leqq \frac{\theta'_{k-1}\theta'_k\cdot\theta_k}{\lambda_{k-1}^{1/2}}, \cdots, |z_l| \leqq \frac{\theta'_l\cdots\theta'_k\cdot\theta_{l+1}\cdots\theta_k}{\lambda_l^{1/2}}.
$$

So far we have used merely the first set (61_1) of inequalities for f'.

The second set yields universal bounds for $|z_1|, \cdots, |z_{l-1}|$. Suppose $y_1, \cdots, y_{l-1}$ to be any integers; we have

$$
f'(y_1, \cdots, y_{l-1}, \overset{k}{\delta_l}, \cdots, \overset{k}{\delta_n}) \geqq f'(\overset{k}{\delta_1}, \cdots, \overset{k}{\delta_n}) - \sigma g'_{11}
$$

which is equivalent to

$$
f(y_1\mathfrak{s}_1 + \cdots + y_{l-1}\mathfrak{s}_{l-1} + \mathfrak{s}_k) \geqq f(\mathfrak{s}_k) - \sigma g'_{11}
$$

or

$$
f(x_1^*, \cdots, x_{l-1}^*, x_l, \cdots, x_n) \geqq f(x_1, \cdots, x_n) - \sigma g'_{11} \tag{72}
$$

where $(x_1, \cdots, x_n)$ again is the vector $\mathfrak{s}_k$ and $x_1^*, \cdots, x_{l-1}^*$ denote any integers. In fact

$$
x_1^* = x_1 + x'_1, \cdots, x_{l-1}^* = x_{l-1} + x'_{l-1}
$$

with

$$
y_1\mathfrak{s}_1 + \cdots + y_{l-1}\mathfrak{s}_{l-1} = x'_1\mathfrak{e}_1 + \cdots + x'_{l-1}\mathfrak{e}_{l-1}.
$$

Observe that $\mathfrak{s}_1, \cdots, \mathfrak{s}_{l-1}$ span the lattice in E_{l-1} so that $x'_1, \cdots, x'_{l-1}$ and therefore $x_1^*, \cdots, x_{l-1}^*$ range independently over all integers while $y_1, \cdots, y_{l-1}$ do so. Let h be one of the indices $1, \cdots, l-1$, and choose $x_i^* = x_i$ for $i > h$, but $x_h^*, \cdots, x_1^*$ such that

$$|z_h^*| \leqq r, \cdots, |z_1^*| \leqq r \qquad (r = \tfrac{1}{2}).$$

Then (72) yields

$$\sigma g_{11}' + (q_1 z_1^{*2} + \cdots + q_h z_h^{*2}) \geqq q_1 z_1^2 + \cdots + q_h z_h^2 \geqq q_h z_h^2 \geqq \lambda_h g_{hh} z_h^2.$$

The left member is less than or equal to

$$\sigma\rho^2 g_{11} + r^2(g_{11} + \cdots + g_{hh}) \leqq (\sigma\rho^2 + r^2 h) g_{hh};$$

thus

$$\lambda_h z_h^2 \leqq \sigma\rho^2 + r^2 h \qquad (h = 1, \cdots, l-1).$$

Hence we have obtained universal bounds for all $|z_i|$ and by means of (66) also for all $|x_i|$. In other words, for each of the lattice vectors (68) we find ourselves limited to a finite set from which to choose.

If $l=1$ nothing remains to be said. In the opposite case the same situation prevails for the "cut" forms

$$f(x_1, \cdots, x_{l-1}, 0, \cdots, 0), \qquad f'(x_1, \cdots, x_{l-1}, 0, \cdots, 0)$$

of $l-1<n$ variables in E_{l-1} as for the full forms f and f' in n dimensions which we started with. Thus the proof is complete by induction.

The main idea of the proof is again borrowed from Minkowski—with two essential modifications:

(1) Where Minkowski uses estimates based upon Jacobi's transformation of quadratic forms, we have availed ourselves of the general Theorems 8 and 9 holding for any gauge function whatsoever; in spite of their far greater generality these estimates are sharper than Minkowski's.

(2) Minkowski has our proposition only for

$$\rho = 1, \qquad \sigma = 0, \qquad G(\rho, \sigma) = Z,$$

in which case it asserts that Z borders on not more than a finite number of equivalent cells Z_S. However, we should know that every boundary point of Z is on the common boundary of Z and a different cell Z_S, or that the cells Z_S cluster only towards the border of G, which means that into any sufficiently small neighborhood of a point of G, or into any compact subset of G, there penetrate only a finite number of cells Z_S. Our theorem goes beyond this because $G(\rho, \sigma)$ exhausts G if $\rho \uparrow \infty, \sigma \uparrow \infty$, but is not compact. About this finer point refer to §13. Here is an application of the fact that the cells do not cluster in the interior of G:

LEMMA 5. *Any cell $Z' = Z_S$ may be reached from the basic cell Z by a chain*

$$Z = Z_1, Z_2, \cdots, Z_\nu = Z' \tag{73}$$

in which any two consecutive members are in contact, i.e., have points in common.

Proof. The center f^0 of Z goes by the substitution S into an inner point f_S^0 of $Z_S = Z'$. Join f^0 with f_S^0 by a straight segment τ. Determine $\rho > 1$ and $\sigma > 0$ so that f_S^0 is an inner point of $G(\rho, \sigma)$. Then the whole segment τ lies in $G(\rho, \sigma)$. Since the number of cells Z_S having points in common with $G(\rho, \sigma)$ is finite, the same is true a fortiori for the cells Z_S which are met by the segment τ. On the other hand every point of τ belongs to a certain cell Z_S, and the points which τ and Z_S have in common form a (closed) interval on τ. Hence τ is covered by a finite number of subintervals of which we can select a chain connecting f^0 with f_S^0. What we obtain in this manner is a chain of cells (73) in which any two consecutive members have a contact point on τ.

Those substitutions of the modular group which effect transition from Z to cells in contact with Z form a finite set $[Z]$. If S is in $[Z]$, so is the "(two-sided) congruent" substitution

$$S^* = JSJ' \qquad (J, J' \text{ any two elements of } \{J\})$$

as one readily verifies by performing the substitution J' on the two contacting cells Z and $Z_{JS} = Z_S$. Hence $[Z]$ breaks up into a number of complete sets of congruent substitutions; we choose a representative out of each set: $S', S'', \cdots$.

THEOREM 14. *The substitutions of $\{S\}$ which carry Z into cells bordering on Z, or rather a complete system of modulo $\{J\}$ incongruent representatives $S', S'', \cdots$ among them, combined with $\{J\}$, generate the whole modular group $\{S\}$.*

Proof. Let S be any element of the modular group and determine a chain (73) leading from Z to $Z_S = Z'$. A certain unimodular S_i^{-1} will carry Z_i into Z and Z_{i+1} into a cell contacting Z which therefore arises from Z by an element $S^{(i)}$ of $[Z]$. The substitution $S^{(i)}S_i$ carries Z into Z_{i+1} and thus can and shall be adopted as S_{i+1}. If this inductive definition of S_i is started off with S_1 the identity, then $S^{(\nu-1)} \cdots S^{(1)}$ carries Z into Z_S, and therefore

$$S = JS^{(\nu-1)} \cdots S^{(1)} \qquad (J \text{ in } \{J\}).$$

12. **Faces and walls.** The main body of the theory of reduction is now complete; what follows are accessories of minor importance. In this section we discuss the consequences upon the cell configuration of the fact that any boundary point of a convex solid polyhedron lies on one of its faces. Engaging in this kind of general topological argument, we prefer the notation $y_1, \cdots, y_N$ instead of g_{ij} for the coordinates in our N-dimensional space R. A *face* of the cell would be described by one of the *equations*

$$\alpha_k(\mathfrak{x}) \qquad (\mathfrak{x} \text{ in } X_k^*,\ k = 1, \cdots, n), \tag{57}$$

which hold for $N-1$ linearly independent points of Z. Taking it for granted that each boundary point of Z lies on a face, we infer from the proof of

Theorem 10 that the corresponding inequalities suffice to define Z as a part of G: those planes (57) which do not share an $(N-1)$-dimensional convex face with Z may be discarded. It is clear that on account of their "extreme" character the remaining inequalities are truly indispensable.

As to the configuration of all equivalent cells Z_S, it seems clear that any point on the boundary of Z lies on a "wall" separating Z from an "adjacent" cell Z_S. By these words "wall" and "adjacent" we wish to indicate that Z and Z_S have $N-1$ linearly independent points in common. The points which two cells have in common, if any, form a convex cone of 1 or 2 or $\cdots$ or $N-1$ dimensions. We speak of a contact of order $1, 2, \cdots, N-1$ respectively. The unimodular S carrying Z into adjacent cells form a finite set $[[Z]]$ narrower than $[Z]$. Again it decomposes into subsets of congruent substitutions. Theorem 14 remains true if $S', S'', \cdots$ denote representatives of these sets. We can dispense with none of these more restricted generators.

The ultimate goal of all such considerations should be to show that the pattern of our cells which mutually border on each other is a *complex* in the combinatorial topological sense, of such particular structure as to form the skeleton of a manifold.

It is clear that the walls of Z are parts of its faces. This simple observation establishes a close relationship between the first and Minkowski's special case of the second theorem of finiteness.

I shall try to give the most convenient arrangement of the proofs. First the faces of Z.

LEMMA 6. *Any boundary point of Z lies on a face of Z.*

We know that Z as a part of G is characterized by inequalities

$$\alpha(y) = \alpha_1 y_1 + \cdots + \alpha_N y_N \geqq 0 \tag{74}$$

corresponding to a finite set $\Sigma = \Sigma_0$ of linear forms $\alpha(y)$. Let f^1 be a point (of G) on the boundary of Z; it will satisfy at least one of the inequalities of Σ with the $=$ sign. After an appropriate linear transformation of the coordinates y_i we may assume

$$f^1 = e^1 = (1, 0, 0, \cdots, 0). \tag{75}$$

Σ_1 is the non-empty subset of Σ to which a linear form $\alpha(y)$ belongs if nullified by e^1. Their first coefficient α_1 vanishes, so that they may be looked upon as forms of $N-1$ variables. For the linear forms $\alpha(y)$ in the complementary subset $\bar{\Sigma}_0$ the first coefficient α_1 is positive. We describe the νth step of this process of selection. Suppose the subset Σ_ν of those linear forms of Σ in which the variables $y_1, \cdots, y_\nu$ are absent is not empty. The corresponding inequalities

$$\alpha_{\nu+1} y_{\nu+1} + \cdots + \alpha_N y_N \geqq 0$$

of Σ_ν define a convex pyramid Z^ν in the $(N-\nu)$-dimensional space R^ν with

the coordinates $y_{\nu+1}, \cdots, y_N$. As long as $N-\nu \geqq 2$, we can find a point $f^{\nu+1} \neq 0$ on the boundary of that pyramid, and by a suitable affine transformation of the coordinates $y_{\nu+1}, \cdots, y_N$ we can provide for $f^{\nu+1}$ having the coordinates

$$(y_{\nu+1}, \cdots, y_N) = (1, 0, \cdots, 0).$$

Σ_ν breaks up into the subsets $\Sigma_{\nu+1}$ and $\overline{\Sigma}_\nu$ whose members have their first coefficient $\alpha_{\nu+1}=0$ and >0 respectively. $\Sigma_{\nu+1}$ is not empty.

The existence of $f^{\nu+1}$ follows in this way. Denote by $f^0=(y_1^0, \cdots, y_N^0)$ the center of the cell Z. All linear forms $\alpha(y)$ belonging to Σ_ν have the property $\alpha(f^0)>0$ for

$$f^0 = (\overset{0}{y}_{\nu+1}, \cdots, \overset{0}{y}_N), \tag{76}$$

or (76) is an inner point of Z^ν. Operating in the $(N-\nu)$-dimensional space R^ν we choose one of the forms of Σ_ν, say $\alpha'(y)$, and a point $f \neq 0$ in the plane $\alpha'(y)$. (As long as R^ν has at least two dimensions, a plane $\alpha'(y)=0$ through the origin O certainly contains points $f \neq 0$.) We join f^0 with f by a straight segment, which will not contain the origin O. Traveling along the segment from f^0 to f we encounter a first point f^* where one of the forms of Σ_ν ceases to be positive. (If not before this will happen for f.) All forms of Σ_ν are greater than or equal to 0 for f^* and at least one equals 0. We take $f^{\nu+1}=f^*$.

We end up with a non-empty set Σ_{N-1} consisting of linear forms $\alpha_N y_N$ in the 1-dimensional space R^{N-1} with the single coordinate y_N. They are positive for $y_N=y_N^0$. We take one of them as the coordinate y_N; then the coefficients α_N of the others are greater than 0 and $y_N \geqq 0$ is the pyramid Z^{N-1} in R^{N-1}. At the same time we have arrived at a complete normalization of the affine system of coordinates $y_1, \cdots, y_N$.

By construction the pyramid $Z^{\nu-1}$ in $R^{\nu-1}$ contains the point

$$(y_\nu, \cdots, y_N) = (1, 0, \cdots, 0).$$

The system $\Sigma_{\nu-1}$ of linear forms

$$\alpha_\nu y_\nu + \cdots + \alpha_N y_N$$

splits into Σ_ν and $\overline{\Sigma}_{\nu-1}$ according to the condition $\alpha_\nu=0$ or $\alpha_\nu>0$. It is therefore easy to ascertain a positive constant $\epsilon_\nu \leqq 1$ such that $(1, y_{\nu+1}, \cdots, y_N)$ lies in $Z^{\nu-1}$ provided $(y_{\nu+1}, \cdots, y_N)$ lies in Z^ν and

$$|y_{\nu+1}| \leqq \epsilon_\nu, \cdots, |y_N| \leqq \epsilon_\nu.$$

This is true even at the first step $\nu=1$ when $R^0=R$ is restricted to G, because for a sufficiently small ϵ the neighborhood of (75) described by

$$y_1 = 1, \ |y_2| \leqq \epsilon, \cdots, |y_N| \leqq \epsilon$$

lies in G.

Starting with the point $y_N=0$ in Z^{N-1} and following this rule for the tran-

sition $Z^\nu \to Z^{\nu-1}$ backwards from Z^{N-1} to Z, we find that the following $N-1$ points

$$\begin{aligned}
&(1,\ 0,\ 0,\ \ 0, \cdots, 0),\\
&(1,\ \epsilon_1,\ 0,\ \ 0, \cdots, 0),\\
&(1,\ \epsilon_1,\ \epsilon_1\epsilon_2,\ 0, \cdots, 0),\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

belong to Z. Thus the plane $y_N = 0$ belongs to Σ_{N-1}, hence to Σ, is a face and contains the point f^1.

LEMMA 7. *Any cell $Z' = Z_S$ may be reached from the basic cell Z by a chain whose consecutive members are adjacent.*

The inner reason for this lemma is obvious: because the region G is *convex*, the cell complex into which it has been divided is *connected*.

We start with the chain described in Lemma 5. Any two of its consecutive members have a common point f situated on the segment τ; but in general their contact will be one of order 1 only. We must insert further cells between them to make the chain proceed by contacts of order $N-1$.

The point f, being common to two cells, is not an inner point of a cell. I shall try to describe the situation intuitively in the plane section $g_{nn} = 1$ of G. The cells to which f belongs cover an entire neighborhood U of f, each of them participating in it by an $(N-1)$-dimensional pyramid with vertex f. Hence we obtain a division of the $(N-1)$-dimensional space R^1 into a finite number of convex pyramids radiating from the vertex f, and our task is to prove that this complex is connected. We thus face the same problem as before, but in one dimension less, and hence induction with respect to N will lead to the desired result. Let us now repeat the argument in detail, again using the notation $y_1, \cdots, y_N$ instead of g_{ij} for the coordinates in R.

Not more than a finite number of cells Z_S penetrate into a neighborhood U of f which lies in $G(\rho, \sigma)$. If one of these cells does not contain f, then U may be shrunk so as to have its intersection with the closed Z_S empty. Hence we find a smaller neighborhood of f, again called U, into which none but cells Z_f containing f will penetrate. We choose the coordinates y_i such that $f = (1, 0, 0, \cdots, 0)$. A cell Z_f is defined by a finite set Σ of inequalities (74) which as before is divided into the subsets Σ_1 and $\overline{\Sigma}_0$; and as has been shown above, any point $(1, y_2, \cdots, y_N)$ sufficiently near to f, if it satisfies merely the inequalities Σ_1, will lie in Z_f. The inequalities Σ_1 define a convex pyramid $Z_f^{(1)}$ in the $(N-1)$-dimensional space R^1 with the coordinates $y_2, \cdots, y_N$. The center $(y_1^0, \cdots, y_N^0)$ of Z_f gives rise to a center $(y_2^0, \cdots, y_N^0)$ of $Z_f^{(1)}$. Thus the Z_f determine a division of R^1 into a finite number of pyramids $Z_f^{(1)}$, and our aim is to prove the connectivity of that assemblage. Let us formulate this assertion as a lemma for N instead of $N-1$ dimensions.

LEMMA 8_N. *Suppose the N-dimensional space R divided into a finite number of convex pyramids* Π *with their common vertex at the origin O. Each of them is supposed to contain inner points. Then any two of them can be joined by a chain whose consecutive members have contacts of order* $N-1$.

The argument employed to reduce Lemma 7 to 8_{N-1} may be used equally well to reduce 8_N to 8_{N-1} and thus to prove 8_N by induction. The case is somewhat simpler because we now deal with a finite set of cells from the beginning. There is a slight complication, however, in so far as the Euclidean N-dimensional space robbed of the point O is not convex, but it is still *connected* as long as $N \geqq 2$, and that is what counts. Indeed the centers of any two of our pyramids can be joined by a line consisting of *one or two* straight segments without passing through O.

As a consequence of Lemma 7, Theorem 14 is sharpened to

THEOREM 15. *A complete system of modulo* $\{J\}$ *incongruent substitutions S which carry Z into adjacent cells generates the whole modular group when one combines them with a system of generators for* $\{J\}$.

13. **Concluding remarks.** Observe that a reduced form f satisfies the inequality

$$f(x_1, \cdots, x_n) \geqq g_{11} \tag{77}$$

not only for integers $x_1, \cdots, x_n$ without a (left) common divisor, but for any integers $(x_1, \cdots, x_n) \neq (0, \cdots, 0)$ whatsoever. This is nothing else than the equation $L_1 = M_1$.

In this final section we are going to study the cell Z of reduced forms relatively to the whole N-dimensional space R rather than G.

The cell Z as a subset of R is not (necessarily) closed; boundary points f which do not belong to G will be semi-definite forms in the sense that $f(\mathfrak{x}) \geqq 0$ for every vector $\mathfrak{x}$, but $f(\mathfrak{x}) = 0$ for certain vectors $\mathfrak{x} \neq 0$. Such a form can be written as a square sum

$$z_1^2 + \cdots + z_m^2$$

of $m < n$ linear forms $z_1, \cdots, z_m$ of the coordinates x_i with real coefficients. Now if ϵ is any pre-assigned positive number we can ascertain a lattice vector $(x_1, \cdots, x_n) \neq (0, \cdots, 0)$ for which

$$|z_1| \leqq \epsilon, \cdots, |z_m| \leqq \epsilon$$

and thus

$$f \leqq m\epsilon^2. \tag{78}$$

This is accomplished either by Minkowski's inequality (1) for a parallelotope or by an easy application of Dirichlet's principle concerning the distribu-

tion of $\nu+1$ objects in ν boxes. But (78) contradicts (77) unless

$$g_{11} = 0.$$

Because of the relations (63),

$$|g_{12}| \leqq rg_{11}, \cdots, |g_{1n}| \leqq rg_{11},$$

which will extend from the forms in Z to those on the boundary of Z, the latter will satisfy the n equations

$$g_{11} = g_{12} = \cdots = g_{1n} = 0. \tag{79}$$

(Even an appeal to the inequality $g_{1i}^2 \leqq g_{11} \cdot g_{ii}$ valid for all positive forms would have sufficed here.)

The closure $\overline{Z}$ of Z in R has each of its boundary points either on one of the planes formerly assembled in the finite set Σ or on the plane $g_{11}=0$. Hence $\overline{Z}$ as a part of R is completely described by the inequalities Σ together with $g_{11} \geqq 0$ and therefore is a pyramid. For $n=1$, the set Σ is empty and we have the one inequality $g_{11} \geqq 0$. We may safely ignore this trivial case. For $n \geqq 2$, $\overline{Z}$ reaches the boundary of G only along the "edge" (79) of n dimensions less; hence $g_{11}=0$ is no face of $\overline{Z}$, and the inequality $g_{11} \geqq 0$ is redundant. Therefore:

THEOREM 16. *The same finite set of inequalities which defines Z in G defines $\overline{Z}$ in R. The boundary points of $\overline{Z}$ which do not belong to Z lie on the edge* (79).

The vertices of $\overline{Z}$ are the so-called extreme forms; every reduced form is a linear combination of them with non-negative coefficients, but some of the extreme forms will be semi-definite.

We can now more fully appreciate the fine points in our two theorems of finiteness. By excluding from Z an arbitrarily small neighborhood

$$V_\epsilon: \quad g_{11} < \epsilon g_{nn}$$

of the "edge" we obtain a compact subset Z_ϵ of G(3). The fact that the boundary points of Z which lie outside this neighborhood V_ϵ belong to a finite number of plane faces is considerably less deep than our first theorem of finiteness, and so is its proof. When one excludes V_ϵ, one could have used the region $G(\rho)$ defined by the first set of inequalities (61) alone instead of $G(\rho, \sigma)$, and could have shown that $G(\rho)$ possesses not more than a finite number of plane faces outside V_ϵ, while this is not true for $G(\rho)$ or $G(\rho, \sigma)$ as a whole. And the second theorem of finiteness could have been replaced by the less profound and more easily accessible assertion that there is only a finite number of S capable of carrying a point of Z outside of V_ϵ into a point of $G(\rho)$ outside V_ϵ. These statements would have sufficed for the topological analysis

(3) Compact under the convention that proportional forms like f and tf $(t>0)$ are identified.

in §12. Our two theorems of finiteness include the approach to the "edge" and thus reveal finer features which are of great interest to the algebraist, though perhaps of less important from the topological standpoint.

Up to now positive quadratic forms have been the object of investigation. Instead one can study arbitrary *affine coordinate systems* [16] in an n-dimensional vector space, consisting of n linearly independent vectors $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$; these new objects form an n^2-dimensional space $\mathfrak{A}$. Two such systems $(\mathfrak{a}_1, \cdots, \mathfrak{a}_n)$ and $(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ are said to be (arithmetically) equivalent if connected by a unimodular transformation S,

$$\mathfrak{b}_i = \sum_k \overset{i}{s_k}\mathfrak{a}_k \qquad (\overset{i}{s_k} \text{ integers, } \det(\overset{i}{s_k}) = \pm 1).$$

For any vector $\mathfrak{x} = (x_1, \cdots, x_n)$ we introduce its square

$$\mathfrak{x}^2 = \overset{2}{x_1} + \cdots + \overset{2}{x_n}$$

(in accordance with Euclidean metric geometry) and associate the positive form

$$f(x_1, \cdots, x_n) = (x_1\mathfrak{a}_1 + \cdots + x_n\mathfrak{a}_n)^2 \tag{80}$$

with the coordinate system $(\mathfrak{a}_1, \cdots, \mathfrak{a}_n)$(4). The latter is said to be reduced and to belong to the "cell" $\mathfrak{Z}$ of $\mathfrak{A}$ provided the associated form f is reduced. $\mathfrak{Z}$ is a fundamental domain for the group $\{S\}$ in $\mathfrak{A}$, and we could interpret our whole theory in terms of the new objects. The quadratic forms are then merely a tool for the study of coordinate systems under the rule of unimodular equivalence. We have thus returned to the approach of Chapter I: What we now call a reduced system $(\mathfrak{a}_1, \cdots, \mathfrak{a}_n)$ was there termed a reduced system with respect to the gauge function

$$(\overset{2}{x_1} + \cdots + \overset{2}{x_n})^{1/2}.$$

A similar shift of viewpoint is applicable to the imaginary and the quaternion cases.

Bibliography

1. Journal für die reine und angewandte Mathematik, vol. 129 (1905), pp. 220–274; also *Gesammelte Abhandlungen* II, Leipzig, 1911, pp. 53–100. Cited as M with the page number in the *Gesammelte Abhandlungen*.

2. Sitzungsberichte der Preussischen Akademie der Wissenschaften, 1928, pp. 510–535; 1929, p. 508.

3. Quarterly Journal of Mathematics, vol. 9 (1938), pp. 259–262.

4. H. Weyl, *On geometry of numbers*, soon to appear in the Proceedings of the London Mathematical Society. On the whole subject see H. Hancock, *Development of the Minkowski Geometry of Numbers*, New York, 1939.

(4) The inequality (54), $g_{11} \cdots g_{nn} \geqq D$, for (80) reads in this interpretation as follows: The volume of a parallelotope cannot exceed the product of the lengths of the vectors by which it is spanned.

5. Another short proof by H. Davenport, Quarterly Journal of Mathematics, vol. 10 (1939), pp. 119–121.

6. Compositio Mathematica, vol. 5 (1938), pp. 368–391.

7. Cf. Minkowski's definition in M, p. 59.

8. See Mahler, loc. cit. (3 above), and the author, loc. cit. (4 above), Theorem V.

9. Weyl, loc. cit. (4 above), "Generalized Theorem V."

10. See M, pp. 56–58.

11. For more details see L. E. Dickson, *Algebren und ihre Zahlentheorie*, Zürich, 1927, chap. 9; C. G. Latimer, American Journal of Mathematics, vol. 48 (1926), pp. 57–66; M. Deuring, *Algebren*, Ergebnisse der Mathematik, vol. 4, no. 1, Berlin, 1935, chap. 6.

12. *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, 1919.

13. The larger part of E. H. Moore's "Algebra of Matrices" (*General Analysis*, Part I, Memoirs of the American Philosophical Society, Philadelphia, 1935) deals with the formalism of "Hamiltonian" forms.

14. Cf. Weyl, loc. cit. (4 above), §8, and the more complicated argument in Bieberbach-Schur, loc. cit. (2 above), pp. 521–523.

15. Loc. cit. (6 above), equation (25).

16. See M, p. 53.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.