Institute for Advanced Study Princeton, N.J., 1949

Seminar on

Geometry of Numbers.

(Weyl, Siegel and Mahler)

Preliminary plan:

1) Historical remarks; general results on the relations between lattices and point sets.

2) Minkowski's theorem on the successive minima of a convex body: proof by Davenport.

3) The Minkowski-Hlawka theorem: proofs by Weyl and by Rogers.

4) The identity by Siegel.

5) Reduction of quadratic forms

6) Rogers' theorem on the successive minima of an arbitrary point set.

7) Results by Macbeath.

8) Dyson's theorem on the product of 4 linear polynomials.

9) Hajós' theorem on the densest packing of parallel epipeds.

10) Blichfeldt's method.

etc.

Books: H. Minkowski, Geometrie der Zahlen
Diophantische Approximationen
H. Hancock, The Minkowski Geometry of Numbers
A. Châtelet, Théorie des nombres.
Hardy-Wright, Theory of numbers.
J.H. Koksma, Diophantische Approximationen

Classical papers by:

Blichfeldt, Voronoy, Remak and newer authors.

Introduction

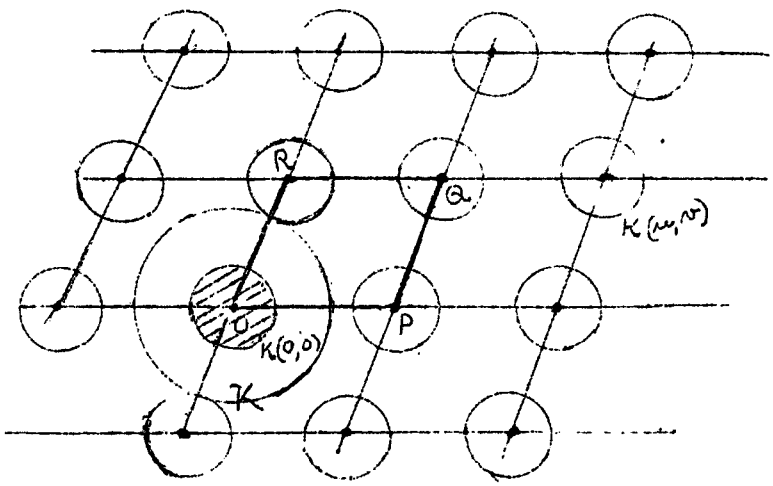
The geometry of numbers arose from the problem of finding solutions in integers of the problem of making one or more functions in several variables as small as possible. The first general method was given by Ch.Hermite. By means of his method of continuous variables, he showed how to make a positive definite quadratic form in n variables small, and from this result he deduced similar inequalities for indefinite quadratic forms and also for forms of higher degree. The bounds found by him were very large when the number of variables was so, and his method sometimes involved a lot of arithmetic.

In his desire to simplify Hermite's work, Minkowski was lead to a very simple, but powerful, method, based on geometrical instead of analytical ideas, and he called the new theory the Geometry of Numbers. This theory is based on the two concepts of

1) the point lattice, and

2) the convex domain.

It will be convenient to explain his ideas in the two dimensional case, before beginning with a more modern and general n-dimensional theory.



Let $\alpha, \beta, \gamma, \delta$ be four real numbers such that

$$\alpha\delta - \beta\gamma \neq 0$$

The points

$$\Lambda: \quad (\alpha u + \beta v,\ \gamma u + \delta v)$$

$$(u, v = 0, \pm 1, \pm 2, \ldots)$$

are then said to form a point lattice Λ; it contains among

others, the origin

$$O = (0, 0)$$

and the points

$$P = (\alpha, \gamma), \quad Q = (\alpha+\beta, \gamma+\delta), \quad R = (\beta, \delta)$$

and these four points

$$O\ P\ Q\ R$$

form the vertices of a parallelogram, evidently of area

$$d(\Lambda) = |\alpha\delta - \beta\gamma| > 0;$$

$d(\Lambda)$ is called the determinant of the lattice and gives a measure for its fineness.

Let next K be a convex region with centre at O; it is thus a set with the properties,

1) if (x_1,y_1) and (x_2,y_2) belong to K, so does every point of the line segment

   $(t\,x_1+(1-t)x_2,\ t\,y_1+(1-t)y_2)$, where $0 < t < 1$,

   joining these two points;

2) if (x,y) belongs to K, so does the symmetrical point $(-x, -y)$;

3) $O = (0,0)$ belongs to K; and

4) K is a bounded closed set.

Assume K is of area J. The similar convex region $K(0,0)$ consisting of all points $(\frac{1}{2}x, \frac{1}{2}y)$ where (x, y) belongs to K, is then of area $\frac{J}{4}$ since it has linear dimensions just half as large as those of K.

Next denote by $K(u,v)$, where u,v run over all integers, the set of all points

$$(\tfrac{1}{2}x + \alpha u + \beta v,\ \tfrac{1}{2}y + \gamma u + \delta v), \text{ where } (x,y) \text{ belongs to K;}$$

Hence $K(u,v)$ is congruent to $K(0,0)$, and similarly situated, but has its centre at the point $(\alpha u + \beta v, \gamma u + \delta v)$ of Λ; also $K(u,v)$ is therefore of area $\frac{J}{4}$.

The set K contains the origin 0 as an inner point. It is easily shown that K contains another point $(\alpha u + \beta v, \gamma u + \delta v)$ $(u,v \neq 0,0)$ of Λ if and only if the two congruent sets

$$K(0,0) \quad \text{and} \quad K(u,v)$$

have at least one point in common; moreover the lattice point is an inner point of K if and only if the point common to $K(0,0)$ and $K(u,v)$ is an inner point of both.

Hence if no point of Λ different from 0 is an inner point of K, then no two of the sets

$$K(u,v), \quad \text{where } u, v = 0, \pm 1, \pm 2, \ldots,$$

can overlap, as 0 can be moved into every other lattice point by a translation of the plane which leaves the configuration of all sets $K(u,v)$ unchanged. Assume this.

Denote now by ω a large positive integer. There are $(2\omega + 1)^2$ lattice points of Λ such that

$$|u| \leq \omega, \quad |v| \leq \omega,$$

and the sets $K(u,v)$ belonging to these fill an area just equal to

$$(2\omega + 1)^2 \ \frac{J}{4}.$$

Since K is bounded, there is a constant $c > 0$ such that every point (x,y) belonging to one of these sets $K(u,v)$ is of the form

$$(\alpha u' + \beta v', \gamma u' + \delta v')$$

where

$$|u'| \leq \omega + c, \quad |v'| \leq \omega + c.$$

But the totality of these points form a parallelogram similar to O P Q R and increased in the ratio

$$\mathfrak{I} : 2(\omega + c),$$

hence of area

$$4(\omega + c)^2 \, d(\Lambda) .$$

Hence

$$(2\omega + 1)^2 \frac{J}{4} \leqq 4(\omega + c)^2 \, d(\Lambda).$$

On dividing by ω^2 and allowing ω to tend to infinity, we get

$$\boxed{J \leqq 4 \, d(\Lambda)}$$

as a necessary condition that no lattice point $\neq 0$ is an inner point of K. One usually takes for Λ the lattice of all points (u,v) with integral coordinates, thus of determinant $d(\Lambda) = 1$; then $J \leqq 4$ is the necessary condition that no point of Λ except 0 is an inner point of K.

The whole proof can immediately be extended to n dimensions. We can further ask whether the constant 4 may be replaced by a smaller one. While this is not possible for all convex sets, it can be shown that better results hold if K is neither a parallelogram nor a convex hexagon, and Minkowski showed already how to obtain the best possible inequality for the case of 2 or 3 dimensions.

In the two books by Minkowski already given and in his coll. works, Minkowski made many applications to continued fractions and the theory of algebraic numbers. But in this seminar we shall restrict the discussion to questions in the geometry of numbers, and I shall now begin with general results on lattices and point sets which have proved of importance in the modern study of the subject.

Notation

Let R_n be the Euclidean space of all points

$$X = (x_1, x_2, \ldots, x_n), \qquad Y = (y_1, y_2, \ldots, y_n), \text{ etc.},$$

with real coordinates. We use the standard vector notation and write

$$| X | = + \sqrt{x_1^2 + x_2^2 + \ldots + x_n^2}$$

for the distance of X from the origin

$$0 = (0, 0, \ldots, 0)$$

of the coordinate system; further $X \mp Y$ for the points

$$X \mp Y = (x_1 \mp y_1, x_2 \mp y_2, \ldots, x_n \mp y_n) ,$$

and $t X$ for the point

$$t X = (tx_1, tx_2, \ldots, tx_n)$$

where t is any real number. The points

$$X_1, X_2, \ldots, X_k$$

are independent if no relation

$$t_1 X_1 + t_2 X_2 + \ldots + t_k X_k = 0$$

with coefficients not all zero holds. At most n points

$$X_1, X_2, \ldots, X_n$$

can be independent; and these n points

$$X_k = (x_1^{(k)}, x_2^{(k)}, \ldots, x_n^{(k)})$$

are independent if and only if their determinant

$$\{X_1, X_2, \ldots, X_n\} = \begin{vmatrix} x_1^{(1)}, \ldots, x_n^{(1)} \\ \cdot \\ \cdot \\ x_n^{(n)}, \ldots, x_n^{(n)} \end{vmatrix}$$

is different from zero.

Let now

$$X_1, X_2, \ldots, X_n$$

be any n independent points. Then the set $\mathcal{L}$ of all points

$$X = u_1X_1 + u_2X_2 + \ldots + u_nX_n \qquad (u_1, u_2, \ldots, u_n = 0, \pm 1, \pm 2, \ldots)$$

is called a lattice, or more exactly a homogeneous lattice; it is the additive free Abelian group of n generators. These n generators

$$X_1, X_2, \ldots, X_n$$

are called a basis of $\mathcal{L}$, and the absolute value

$$d(\mathcal{L}) = |\{X_1, X_2, \ldots, X_n\}| > 0$$

of their determinant is called the determinant of $\mathcal{L}$. Any other n points $Y_1, Y_2, \ldots, Y_n$ of $\mathcal{L}$ form a basis of this lattice if and only if also

$$d(\mathcal{L}) = |\{Y_1, Y_2, \ldots, Y_n\}|;$$

the determinant is thus independent of the special basis; moreover necessarily

$$Y_h = \sum_{k=1}^{n} g_{hk} X_k \qquad (h = 1,2,\ldots,n)$$

with integral coefficients g_{hk} of determinant ± 1.

A further important quantity connected with $\mathcal{L}$ is the diameter $\delta(\mathcal{L})$ of this lattice; it is defined as the smallest distance between any two <u>different</u> points of $\mathcal{L}$. Evidently $\delta(\mathcal{L})$ is equal to the distance between 0 and the nearest lattice point $\neq 0$; hence $\delta(\mathcal{L}) > 0$ exists, as every finite part of space contains only a finite number of lattice points.

As a consequence of the theory of quadratic forms, we shall later prove the following result:

Every lattice $\mathcal{L}$ contains a basis $X_1, X_2, \ldots, X_n$ such that

$$|X_1|\ |X_2| \ \ldots\ |X_n| \leq \gamma_n\, d(\mathcal{L});$$

here γ_n is a positive constant depending alone on the dimension of the space R_n considered.

If Λ is any homogeneous lattice and X_o is any point, then the set of all points

$$X + X_o, \qquad \text{where } X \in \Lambda ,$$

form what we call an inhomogeneous lattice

$$L = X_o + \Lambda;$$

we call X_o; X_1, ..., X_n a basis of L, if X_1, ..., X_n form one of Λ. The first element X_o of such a basis can evidently be replaced by any point $X_o + X$ where $X \in \Lambda$, without changing L.

The determinant and the diameter of L are the same as those of Λ:

$$d(L) = d(\Lambda), \qquad \delta(L) = \delta(\Lambda);$$

in particular, $\delta(L)$ measures again the smallest distance between any two distinct points of L.

From Minkowski's theorem on convex bodies, and from the previous result for homogeneous lattices, it is possible to deduce that every inhomogeneous lattice L possesses a basis X_o; X_1, ..., X_n such that

$$|X_o| \leq \Gamma_n \frac{d(L)}{\delta(L)^{n-1}}, \qquad |X_1|\,|X_2| \cdots |X_n| \leq \gamma_n\, d(L);$$

here γ_n is the same constant as before, and Γ_n is a further positive number depending only on the dimension n of R_n.

Limits of lattices.

We can introduce the concept of a convergent sequence of lattices

$$\Lambda_1, \Lambda_2, \Lambda_3, \cdots$$

or more generally

$$L_1, L_2, L_3, \ldots .$$

If, say, L_r has the basis $X_0^{(r)}; X_1^{(r)}, \ldots, X_n^{(r)}$, and if there exists a lattice L of basis $X_0; X_1, \ldots, X_n$ such that

$$\lim_{r \to \infty} X_k^{(r)} = X_k \qquad (k=0, 1, \ldots, n),$$

then we say that the lattices L_r tend to L:

$$\lim_{r \to \infty} L_r = L .$$

This convergence evidently implies that

$$\lim_{r \to \infty} d(L_r) = d(L).$$

It is easily seen that, in every bounded closed part of space, the points of the lattices L_r tend just to the points of L; hence also

$$\lim_{r \to \infty} \delta(L_r) = \delta(L).$$

On putting $X_0^{(r)} = 0$, $X_0 = 0$, we get the analogous definitions and results for homogeneous lattices .

The following definition proves of great use:

Definition: An infinite sequence of homogeneous lattices $\Lambda_1, \Lambda_2, \ldots$ (or of inhomogeneous lattices $L_1, L_2, \ldots$) is called bounded if there exist two positive numbers c_1 and c_2 such that

$$d(\Lambda_r) \leqq c_1, \qquad \delta(\Lambda_r) \geqq c_2$$

(respectively

$$d(L_r) \leqq c_1 , \qquad \delta(L_r) \geqq c_2)$$

for all indices r = 1, 2, 3, ...

Basic theorems on lattices.

From the definition, the following result is obtained:

THEOREM: Let $\Lambda_1, \Lambda_2, \ldots$ ($L_1, L_2, \ldots$) be an infinite bounded sequence of homogeneous (inhomogeneous) lattices. Then there exists in it a convergent infinite subsequence

$$\Lambda_{r_1}, \Lambda_{r_2}, \ldots \qquad (L_{r_1}, L_{r_2}, \ldots)$$

where

$$r_1 < r_2 < r_3 < \ldots .$$

Proof: It will be sufficient to show the assertion for the inhomogeneous lattice sequence $L_1, L_2, \ldots$. For each lattice L_r , select a basis

$$x_o^{(r)} ; \; x_1^{(r)}, \ldots, x_n^{(r)}$$

such that

$$|x_o^{(r)}| \leq \Gamma_n \frac{d(L)}{\delta(L_r)^{n-1}}; |x_1^{(r)}| |x_2^{(r)}| \ldots |x_n^{(r)}| \leq \gamma_n d(L_r) .$$

Then from the hypothesis

$$|x_o^{(r)}| \leq \frac{\Gamma_n c_1}{c_2^{n-1}} ; \; |x_k^{(r)}| \leq \frac{\gamma_n c_1}{c_2^{n-1}} \quad \text{for } k = 1, 2, \ldots, n$$

$$d(L_r) \geq \frac{c_2^n}{\gamma_n}$$

for all r. This shows that all basis points are bounded. Hence we can select an infinite sequence of indices

$$r_1, r_2, r_3, \ldots \quad \text{with} \quad r_1 < r_2 < r_3 < \ldots$$

such that the n+1 limit points

$$X_0 = \lim_{k\to\infty} X_0^{(r_k)}; \qquad X_1 = \lim_{k\to\infty} X_1^{(r_k)}, \ \ldots, \ X_n = \lim_{k\to\infty} X_n^{(r_k)}$$

exist.

Evidently

$$\left\{X_1, X_2, \ldots, X_n\right\} = \lim_{k\to\infty} \left\{X_1^{(r_k)}, X_2^{(r_k)}, \ldots, X_n^{(r_k)}\right\},$$

whence

$$\left|\left\{X_1, X_2, \ldots, X_n\right\}\right| = \lim_{k\to\infty} \left|\left\{X_1^{(r_k)}, X_2^{(r_k)}, \ldots, X_n^{(r_k)}\right\}\right|$$

$$= \lim_{k\to\infty} d(L_{r_k}) \geq \frac{c_2^n}{\gamma_n} > 0.$$

Hence $X_0; X_1, \ldots, X_n$ is the basis of a lattice, L say, and then

$$L = \lim_{k\to\infty} L_{r_k},$$

whence the assertion.

Admissible and Critical lattices.

Minkowski studied the relation of a lattice to a convex set; let us generalize his ideas and consider the relation of a lattice to an arbitrary point set which need neither be convex nor bounded.

Let S be any point set in R_n. As usual, a point $X \in S$ will be called an inner point of S if all points of a certain neighborhood of X also belong to S, i.e., if there exists a positive ε such that

$$X \in S, \quad |X - Y| < \varepsilon, \text{ implies that also } Y \in S.$$

We introduce now the following two slightly different definitions for homogeneous, or inhomogeneous, lattices.

Definition: A homogeneous lattice Λ is called S-admissible if no point of Λ, except possibly 0, is an inner point of S.

An inhomogeneous lattice L is called S-admissible if no point of L is an inner point of S.

This distinction is justified since now 0 plays no distinctive role.

In the homogeneous case, it would be sufficient to consider only point sets symmetrical in 0. For denote by

$$S^* = S \cup (-S)$$

the set of all points X such that

$$X \in S \quad \text{or} \quad -X \in S \quad \text{or both;}$$

then Λ is clearly S-admissible if and only if it is S^*-admissible.

Together with point sets, we consider also sets Π of homogeneous lattices Λ or sets $\mathcal{M}$ of inhomogeneous lattices L. In either case, we call the set closed if with every convergent sequence of lattices it contains the limiting lattice.

Definition 1. Let M be a fixed closed set of homogeneous lattices Λ, and let S be a point set. Then we say that S is of the infinite type w.r. to M if no lattice in M is S-admissible, and we call S of the finite type if at least one lattice in M is S-admissible. In the first case put

$$\Delta(S \mid M) = \infty ,$$

and in the second case denote by $\Delta(S \mid M)$ the lower bound

$$\Delta(S \mid M) = \text{l.b. } d(\Lambda)$$

extended over all S-admissible lattices in M. Hence in the second case

$$0 \leq \Delta(S \mid M) < \infty .$$

Definition 2. Let $\mathcal{M}$ be a fixed closed set of inhomogeneous lattices L, and let S be a point set. Then we say that S is of the infinite type w. r. to $\mathcal{M}$ if no lattice in $\mathcal{M}$ is S-admissible, and otherwise call S of the finite type. In the first case put

$$D(S \mid \mathcal{M}) = \infty ,$$

in the second case denote by $D(S \mid \mathcal{M})$ t he lower bound

$$D(S \mid \mathcal{M}) = \text{l. b. } d(L)$$

extended over all S-admissible lattices in $\mathcal{M}$. Hence in the second case,

$$0 \leq D(S \mid \mathcal{M}) < \infty .$$

In the definitions of $\Delta(S \mid M)$ and $D(S \mid \mathcal{M})$, it is not essential that M and $\mathcal{M}$ are closed sets of lattices. This restriction becomes, however, fundamental for the applications of previous results.

Definition 3: The lattice Λ is called a critical lattice of S w. r. to M if

1) Λ is S-admissible, and

2) $d(\Lambda) = \Delta(S \mid M)$

Definition 4. The lattice L is called a critical lattice of S w. r. to $\mathcal{M}$ if

1) L is S-admissible, and

2) $d(\Lambda) = D(S \mid \mathcal{M})$

The existence of critical lattices.

The first problem is to decide which sets have critical lattices. naturally not every set has this property. A trivial reason for having no critical lattice is given if

$$\triangle(S \mid M) = 0 \text{ or } \infty ,$$

respectively if

$$D(S \mid \mathcal{M}) = 0 \text{ or } \infty .$$

For if one of these two functions is ∞, then no critical lattices exist since there are no admissibles ones; and if the functions are 0, then again no critical lattice exists since every homogeneous or inhomogeneous lattice is of positive determinant.

In the case

$$0 < \triangle(S \mid M) < \infty ,$$

respectively

$$0 < D(S \mid \mathcal{M}) < \infty ,$$

the position is different. Then a necessary and sufficient condition for the existence of critical lattices is given by the following theorems:

THEOREME 1: Assume $0 < \triangle(S \mid M) < \infty$. Then S has at least one critical lattice w. r. to M if and only if there exists an infinite bounded sequence of S-admissible lattices

$$\Lambda_1, \Lambda_2, \Lambda_3, \ldots$$

in M such that

$$\lim_{r \to \infty} d(\Lambda_r) = \triangle(S \mid M) .$$

THEOREME 2: Assume $0 < D(S \mid \mathcal{M}) < \infty$. Then S has at least one critical lattice w. r. to $\mathcal{M}$ if and only if there exists an infinite bounded sequence of S-admissible lattices

$$L_1, L_2, L_3, \ldots$$

in $\mathcal{M}$ such that

$$\lim_{r\to\infty} d(L_r) = D(S \mid \mathcal{M}).$$

It will be sufficient to prove Theorem 1, since Theorem 2 can be proved in exactly the same way.

(α) The condition is necessary. For if Λ_o is a critical lattice, then the sequence

$$\Lambda_o, \Lambda_o, \Lambda_o, \ldots$$

has the asserted properties.

(β) The condition is also sufficient. For let $\Lambda_1, \Lambda_2, \Lambda_3, \ldots$ be a sequence as described in the Theorem. Since this sequence is bounded, an infinite subsequence

$$\Lambda_{\nu_1}, \Lambda_{\nu_2}, \Lambda_{\nu_3}, \ldots \quad (\nu_1 < \nu_2 < \nu_3 < \ldots)$$

exists which tends to a lattice Λ ; and Λ belongs to M since M is assumed closed. We assert that Λ is the wanted critical lattice.

For, firstly,

$$d(\Lambda) = \lim_{k\to\infty} d(\Lambda_{\nu_k}) = \lim_{r\to\infty} d(\Lambda_r) = \Delta(S \mid M).$$

Secondly Λ is S-admissible. If not, there exists a point $X \neq 0$ of Λ which is an inner point of S. But we can select in each lattice Λ_{r_k} a point P_{r_k} such that $\lim_{k\to\infty} P_{r_k}$ exists and is $= P$.

Therefore, for sufficiently large k, P_{r_k} is an inner point of S, contrary to the assumption that Λ_{r_k} is S-admissible.

For the application of this result, the most interesting cases are that $\mathfrak{U}$ is the set of all homogeneous, or $\mathfrak{M}$ the set of all inhomogeneous lattices; and in these cases we write simpler

$$\triangle(S) \text{ and } D(S) .$$

But before studying these functions, I shall mention the case of lattices over algebraic fields where it is important to have the more general theorems above.

Lattices over an algebraic field.

Denote by

$$f(t) = t^n + \tau_1 t^{n-1} + \dots + \tau_n$$

a fixed polynomial with integral coefficients which is irreducible in the field of all rational numbers. We denote by K^* the set of all polynomials in t with real coefficients with the convention that any two such polynomials are considered as identical if their difference is divisible by f(t); and we denote by K the set of all such polynomials with rational coefficients. Then K is a finite algebraic field of degree n over the rational number field, and K^* is a ring containing K. From the definition, it is clear how to define the four operations in K and K^*.

Next let

$$n = n N$$

where N is any positive integer. We define the space $R_n(K)$ as the set of all points

$$X = (x_1, x_2, \dots, x_N)$$

where the coordinates $x_1, x_2, \ldots x_N$ are in K^*. The sum or difference of such points is defined as usual, and if x is any element of K^*, then x X denotes the point

$$x\,X = (x\,x_1,\ x\,x_2,\ \ldots,\ x\,x_N)\ .$$

Every element x of K^* can be written in a unique way in the reduced form

$$x = x^{(o)} + x^{(1)}t + \ldots + x^{(M-1)}t^{M-1}\ ,$$

thus every point X of $R_N(K)$ in the reduced form

$$X = (x_1^{(o)} + x_1^{(1)}t + \ldots + x_1^{(M-1)}t^{M-1},\ \ldots,\ x_N^{(o)} + x_N^{(1)}t + \ldots + x_N^{(M-1)}t^{M-1}).$$

Let now

$$X_1,\ X_2,\ \ldots,\ X_N$$

be any N points of $R_N(K)$; we then define as the determinant

$$\langle X_1,\ X_2,\ \ldots,\ X_N \rangle$$

of these points the ordinary n-th order determinant in which the rows are given by the "reduced coefficients"

$$x_1^{(o)},\ x_1^{(1)},\ \ldots,\ x_1^{(M-1)},\ \ldots,\ x_N^{(o)},\ x_N^{(1)},\ \ldots,\ x_N^{(M-1)}$$

belonging to the n points

$$X_1,\ t\,X_1,\ \ldots,\ t^{M-1}X_1,\ \ldots,\ X_N,\ t\,X_N,\ \ldots,\ t^{M-1}X_N\ .$$

If this determinant is not zero, then the set of all points

$$X = x_1X_1 + x_2X_2 + \ldots + x_NX_N\ ,$$

where the coefficients

$$x_h = x_h^{(o)} + x_h^{(1)}t + \ldots + x_h^{(M-1)}t^{M-1} \qquad (h = 1,2,\ldots,N)$$

run over all elements of K with integral coefficients

$$x_h^{(0)}, x_h^{(1)}, \ldots, x_h^{(N-1)} \qquad (h = 1,2,\ldots,N),$$

is called a lattice Λ over K, and its determinant is defined by

$$d(\Lambda) = \left| \langle X_1, X_2, \ldots, X_N \rangle \right| > 0.$$

If we map the point X in $R_N(K)$ on the point

$$(x_1^{(0)}, x_1^{(1)}, \ldots, x_1^{(N-1)}, \ldots, x_N^{(0)}, x_N^{(1)}, \ldots x_N^{(N-1)})$$

in ordinary space R_n, then Λ evidently corresponds to a lattice in this space of the same determinant. But this lattice in R_n will be specialized and not the most general one. (Inhomogeneous lattices can be defined analogously).

There is no difficulty in defining convergence of lattices in $R_N(K)$ and to apply now the theorems 1 and 2 to such lattices, since the set of all lattices over K is closed.

Examples of the existence theorems.

The theory of inhomogeneous lattices is much less developped than that of homogenous ones. From now on, I shall then restrict myself to the consideration of homogeneous lattice point problems in R_n.

From Theorem 1, it is immediately clear that every point set S has critical lattices if it satisfies the following two conditions:

1) $\Delta(S) < \infty$;

2) 0 is an inner point of S.

While the first condition is natural, the same cannot be said for 2).

Another, even simpler, consequence of Theorem 1 is that S has a critical lattice if it has the following two properties:

1) $\Delta(S) > 0$;

2) S is a bounded set.

Again 1) is a natural condition, but not 2).

It may be best to give a number of examples for the case of two dimensions.

1) Remove from the plane R_2 all circle areas of radius $\frac{1}{6}$ with their centres at the points with integral coordinates. For the resulting open set S, the lattice Λ of all points with integral coordinates is clearly admissible, hence also every sublattice of Λ. But no other lattice is admissible; hence $\Delta(S) = 1$, Λ is the only critical lattice, and the set of all admissible lattices is enumerable.

The last example is distinguished by the fact that the S-admissible lattice Λ consists of points all of which have distance $\frac{1}{6}$ from Λ. It is thus not at all necessary for a critical lattice to have points arbitrarily near to its set.

2) One can show that the set

$$S : \quad 0 \leq xy \leq 1$$

is of determinant $\Delta(S) = 1$, and that it has an infinity of critical lattices, namely all lattices of the form

$$\Lambda_t : \quad P = u(t,0) + v(0,\tfrac{1}{t}) \qquad (u,v = 0, \pm 1, \pm 2, \ldots)$$

where t is an arbitrary positive number. Denote now by S_r the subset of all points in S which lie at a distance not greater than $r > 0$ from the origin. Then it is easily shown that

$$\Delta(S_r) = 0 .$$

Thus although, for $r \longrightarrow \infty$, S_r tends to S, it is not true that $\Delta(S_r)$ tends

to $\Delta(S)$. The functional $\Delta(S)$ is thus not always continuous.

3) The set S just considered is a proper subset of the set

$$S^*: \quad 0 \leq xy \leq 1 + \frac{1}{x^2+y^2} .$$

If (α,β), $\alpha > 0$, $\beta > 0$, is any point on the boundary of S^*, then the lattice $\Lambda_{\alpha\beta}$ of all points

$$u(\alpha,0) + v(0,\beta) \qquad (u,v = 0, \pm 1, \pm 2, \ldots)$$

is S^*-admissible, and it had the determinant

$$d(\Lambda_{\alpha\beta}) = \alpha\beta > 1 .$$

On making $\alpha^2+\beta^2$ sufficiently large, we can evidently make the difference $\alpha\beta - 1$ as small as we like, but never equal to 1. Hence

$$\Delta(S^*) = 1 ,$$

and while S^* has a continuous infinity of admissible lattices, it has no critical lattices.

By a more complicated method, one can obtain an (unbounded) point set with an enumerable set of admissible but no critical lattices.

4) Denote by θ any number such that $0 < \theta < 1$, and by Q_θ the square ring

$$\theta \leq \max(|x|,|y|) \leq 1 .$$

It is easily seen that

$$\Delta(Q_\theta) = \begin{cases} 1 & \text{if } \theta < \frac{1}{2}, \\ \frac{1}{4} & \text{if } \theta = \frac{1}{2}. \end{cases}$$

Hence even for bounded sets $\Delta(S)$ is not necessarily a continuous functional of S.

5) A star domain is defined as a closed but not necessarily bounded point set with the following properties:

α) $0 = (0,0)$ is an inner point, and S is symmetrical in 0.

β) If X belongs to S, so does t X if $0 \leq t \leq 1$.

γ) The boundary of S is a continuous curve which is cut by every line from 0 in at most one point.

A simpler definition of a star domain is by means of a distance function $F(X) = F(x,y)$, i.e., a function with t he following properties

α) $F(0) = 0$, $F(X) \geq 0$ for all X

β) $F(t\,X) = |t|\,F(X)$ for all X and real t

γ) F(X) is a continuous function of X

Thus

$$F(X) = |xy|^{\frac{1}{2}} \quad \text{and} \quad F(X) = |x^2y|^{\frac{1}{3}}$$

are examples of distance functions. Of the corresponding star domains

$$|xy| \leq 1 \quad \text{and} \quad |x^2y| \leq 1,$$

the first is of the finite, the second one of the infinite type.

For star domains, $\triangle(S)$ has certain continuity properties. In particular, let S_r be again by the set of all X in S for which $|X| \leq r$. Then, if S is a star domain, then

$$\triangle(S) = \lim_{r \to \infty} \triangle(S_r).$$

This proof, and many other one, all use the compactness property of the set of all lattices.

The points of a critical lattice on the boundary of S.

We saw that a critical lattice of an arbitrary set need not have points arbitrarily near to the boundary of S. On the other hand, it is trivial that if $S : F(X) \leq 1$ is a star domain of the finite type, then, for $\varepsilon > 0$, there exists at least one lattice point P of every critical lattice

such that

$$1 \leq F(X) < 1 + \varepsilon .$$

Here the equality sign need not hold, as the example of the set

$$S^*: (x^2 + y^2)\, y^2 \leq 1$$

with $\Delta(S^*) = \sqrt{5}$ shows; for this is a subset of

$$S : |xy| \leq 1$$

with $\Delta(S) = \sqrt{5}$. Every critical lattice of S is also critical w. r. to S^*, but has clearly no point on the boundary of $S^* \subset S$.

Outlook.

The functional $\Delta(S)$ is easily seen to be an affine invariant just as the area $V(S)$ of S. It has therefore interest to study relations between $\Delta(S)$ and $V(S)$. For convex domains, Minkowski's theorem gives

$$4\,\Delta(S) \geq V(S) ,$$

while for star domains the Hlanka-Minkowski theorem states that

$$V(S) \geq 2\,\zeta(2)\,\Delta(S) ;$$

analogous inequalities with 2^n instead of 4 and $2\zeta(n)$ instead of $2\zeta(2)$ hold in R_n .

Other important inequality relations are given by Minkowski's theorem on the successive minima of a convex body, and its recent analogue for arbitrary set by C.A.Rogers. All such results and still undiscovered ones form the subject of the Geometry of numbers.

The successive Minima of a Bounded Star Body.

We intend to prove Minkowski's theorem on the successive minima of a bounded convex body (symmetrical in the origin), but we can define the successive minima for any bounded star body. Recall that a bounded star body is a set consisting of those points X in n-dimensional real Euclidean space R_n such that $F(X) \leq 1$, where $F(X)$ is a continuous function such that $F(0) = 0$, $F(X) > 0$ for $X \neq 0$, and $F(tX) = |t| F(X)$ for real t and all X.

THEOREM. To every bounded star body K: $F(X) \leq 1$ and to every lattice Λ, there exist n independent points $P_1, P_2, \ldots, P_n$ of Λ and n positive numbers $p_1, p_2, \ldots, p_n$ with the following properties:

(a) $F(P_1) = p_1$, $F(P_2) = p_2, \ldots, F(P_n) = p_n$,

(b) $p_1 \leq p_2 \leq \ldots \leq p_n$,

(c) if $1 \leq m \leq n$ and $P \neq 0$ is linearly independent of $P_1, P_2, \ldots, P_{m-1}$, then $F(P) \geq p_m$.

Proof: For every $\sigma > 0$ the star body σK: $F(X) \leq \sigma$ is bounded and so contains at most a finite number of points of Λ. Hence there exists a positive number p_1 such that $F(P) < p_1$, is satisfied by no lattice point $P \neq 0$, but that $F(P_1) = p_1$ for at least one non-zero lattice point P_1. Assume now that for $2 \leq m \leq n$ the lattice points $P_1, P_2, \ldots, P_{m-1}$ and the constants $p_1, p_2, \ldots, p_{m-1}$ have already been found. Then there exist lattice points linearly independent of $P_1, P_2, \ldots, P_{m-1}$; hence there also exists a constant $p_m > 0$ such that $F(P) < p_m$ is satisfied for no lattice point $P \neq 0$ linearly independent of $P_1, P_2, \ldots, P_{m-1}$, but that $F(P_m) = p_m$ for at least one lattice point P_m linearly independent of $P_1, P_2, \ldots, P_{m-1}$. This proves (a) and (c). The inequalities (b) hold since the successive p's are the

minima of F(P) on smaller and smaller sets of lattice points.

Definition: The constants $p_1, p_2, \ldots, p_n$ in the preceding theorem are called the successive minima of K: $F(X) \leq 1$ in Λ.

THEOREM: The successive minima depend only on K and Λ and are otherwise uniquely determined.

Proof: Suppose that the independent lattice points $P_1, P_2, \ldots, P_n$ with the constants $p_1, p_2, \ldots, p_n$ and the independent lattice points $Q_1, Q_2, \ldots, Q_n$ with the constants $q_1, q_2, \ldots, q_n$ both satisfy the conditions (a), (b), (c) of the preceding theorem. We claim then that $p_1 = q_1, p_2 = q_2, \ldots, p_n = q_n$. Clearly $p_1 = q_1$, since both must be the minimum of F(P) on the set of all non-zero lattice points. Assume now that for some m ($2 \leq m \leq n$) we have

$$p_1 = q_1, p_2 = q_2, \ldots, p_{m-1} = q_{m-1}, p_m \neq q_m,$$

say

$$p_m > q_m.$$

Now the m-1 points $P_1, P_2, \ldots, P_{m-1}$ and also the m points $Q_1, Q_2, \ldots, Q_m$ are linearly independent. Hence there is an index μ, $1 \leq \mu \leq m$, such that Q_μ is linearly independent of $P_1, P_2, \ldots, P_{m-1}$. But then

$$F(Q_\mu) = q_\mu \leq q_m < p_m,$$

contrary to the property (c).

Definition: Any set of n independent points $Q_1, Q_2, \ldots, Q_n$ of Λ satisfying

$$F(Q_1) = p_1, F(Q_2) = p_2, \ldots, F(Q_n) = p_n,$$

where $p_1, p_2, \ldots, p_n$ are the succesive minima of K: $F(X) \leq 1$ in Λ, is called a system of successive minimum points of K in Λ.

Thus a system of successive minimum points is any set of n independent points satisfying the property (a) of the first theorem of this

section, where $p_1, p_2, \ldots, p_n$ are the established successive minima. We now show that a system of successive minimum points automatically has property (c).

THEOREM: If $Q_1, Q_2, \ldots, Q_n$ is any system of successive minimum points of K in Λ and if $P \neq 0$ is any point of Λ linearly independent of $Q_1, Q_2, \ldots, Q_{m-1}$ $(1 \leq m \leq n)$, then $F(P) \geq p_m$.

Proof. The assertion is true for $m = 1$, since $F(P) \geq p_1$, if $P \neq 0$. Assume that for some index m with $2 \leq m \leq n$ there is a non-zero lattice point P linearly independent of $Q_1, Q_2, \ldots, Q_{m-1}$ satisfying $F(P) < p_m$. Then $p_1 < p_m$, since no non-zero lattice point satisfies $F(P) < p_1$. Thus there is a uniquely determined index $\mu \geq 2$ such that

$$p_{\mu-1} < p_\mu = p_{\mu+1} = \cdots = p_m.$$

The lattice point P is also linearly independent of $Q_1, Q_2, \ldots, Q_{\mu-1}$ and satisfies

$$F(P) < p_\mu .$$

Further from the definition of the Q's we have

$$F(Q_1) = p_1 < p_\mu, \quad F(Q_2) = p_2 < p_\mu, \ldots, F(Q_{\mu-1}) = p_{\mu-1} < p_\mu .$$

By the definition of p_μ this requires that all μ points

$$P, Q_1, Q_2, \ldots, Q_{\mu-1}$$

are linearly dependent on $P_1, P_2, \ldots, P_{\mu-1}$, where $P_1, P_2, \ldots, P_n$ are the points of the first theorem of this section. Hence $P, Q_1, Q_2, \ldots, Q_{\mu-1}$ are linearly dependent. Since $Q_1, Q_2, \ldots, Q_{\mu-1}$ are linearly independent, this implies that P is linearly dependent on $Q_1, Q_2, \ldots, Q_{\mu-1}$. This contradiction completes the proof.

These basic theorems on the existence of successive minima are true for an arbitrary bounded star body. For the special case of a bounded convex body, i.e., a bounded star body K: $F(X) \leq 1$ whose distance function $F(X)$ satisfies

the additional condition

$$F(X + Y) \leq F(X) + F(Y) ,$$

Minkowski proved the inequality

$$P_1 P_2 \cdots P_n \, V(K) \leq 2^n \, d(\Lambda),$$

where $d(\Lambda)$ is the determinant of the lattice Λ. This is sometimes called Minkowski's second theorem. His first theorem, namely that $\Delta(K) \geq 2^{-n} V(K)$ for a bounded convex body K, follows from his second; for if Λ is K-admissible, then $p_1 \geq 1$ and hence $d(\Lambda) \geq 2^{-n} V(K)$. Before proving Minkowski's second theorem, we need some additional preparations.

A Basis Determined by n Independent Lattice Points.

If $P_1, P_2, \ldots, P_n$ are n linearly independent points of the lattice Λ, they do not in general form a basis for Λ. However the following theorem shows that it is possible to find a basis $Z_1, Z_2, \ldots, Z_n$ for the lattice such that for any m, $1 \leq m \leq n$, linear dependence of a point in R_n on $P_1, P_2, \ldots, P_m$ is equivalent to linear dependence on $Z_1, Z_2, \ldots, Z_m$.

THEOREM: If $P_1, P_2, \ldots, P_n$ are any n linearly independent points of a lattice Λ, we can find a basis $Z_1, Z_2, \ldots, Z_n$ for the lattice such that

$$P_h = \sum_{k=1}^{h} s_{hk} Z_k \qquad (h = 1, \ldots, n),$$

where each s_{hk} is integral $(1 \leq k \leq h \leq n)$ and $s_{hh} \geq 1$, $h = 1, \ldots, n$.

Proof. For $m = 1, 2, \ldots, n$ denote by W_m the set of all points

$$Z = t_1 P_1 + \cdots + t_m P_m, \quad 0 \leq t_1 \leq 1, \ldots, 0 \leq t_{m-1} \leq 1, \quad 0 < t_m \leq 1 .$$

If

$$Z' = t_1' P_1 + \cdots + t_m' P_m, \quad 0 \leq t_1' \leq 1, \ldots, 0 \leq t_{m-1}' \leq 1, \quad 0 < t_m' \leq 1 ,$$

is a second point of W_m, then Z is called lower than Z' if the first non-vanishing one of the differences

$$t_m - t_m', \; t_{m-1} - t_{m-1}', \; \ldots, \; t_1 - t_1'$$

is negative.

Since the set W_m is bounded, it contains at most a finite number of points of the lattice Λ; and it does contain such points, for example the point P_m. Hence W_m contains a lowest lattice point, say the point

$$Z_m = \tau_{m1}P_1 + \ldots + \tau_{mm}P_m, \; 0 \leq \tau_{m1} \leq 1, \; \ldots, \; 0 \leq \tau_{m,m-1} \leq 1, \; 0 < \tau_{mm} \leq 1.$$

We claim that $Z_1, Z_2, \ldots, Z_n$ as just defined form a basis for Λ. (To get a basis it is not essential that Z_m be the lowest point of Λ in W_m, but only a point of Λ in W_m with minimal t_m. However the above choice gives a unique character to the process).

Clearly the n points $Z_1, Z_2, \ldots, Z_n$ are linearly independent and so every point X in the space R_n can be written in the form

$$X = t_1Z_1 + \ldots + t_nZ_n$$

with real coefficients. We must show that if X is in Λ, then $t_1, t_2, \ldots, t_n$ are integers.

Let this assertion be false and suppose that t_m is fractional, while $t_{m+1}, t_{m+2}, \ldots, t_n$ are integral $(1 \leq m \leq n)$. Then the assertion is also false for

$$X - ([t_m] Z_m + t_{m+1}Z_{m+1} + \ldots + t_nZ_n),$$

where [x] denotes the greatest integer not exceeding the real number x. There is therefore no loss of generality in assuming that

$$0 < t_m < 1,\ t_{m+1} = t_{m+2} = \dots = t_n = 0,$$

so that X is of the form

$$X = t_1 Z_1 + t_2 Z_2 + \dots + t_m Z_m,\ 0 < t_m < 1.$$

By expressing $Z_1, Z_2, \dots, Z_m$ in terms of $P_1, P_2, \dots, P_m$ we get

$$X = t_1(\tau_{11} P_1) + t_2(\tau_{21} P_1 + \tau_{22} P_2) + \dots + t_m(\tau_{m1} P_1 + \dots + \tau_{mm} P_m)$$

$$= u_1 P_1 + u_2 P_2 + \dots + u_m P_m ,$$

where

$$u_1 = t_1 \tau_{11} + t_2 \tau_{21} + \dots + t_m \tau_{m1}, \dots, u_{m-1} = t_{m-1} \tau_{m-1,m-1} + t_m \tau_{m,m-1}, u_m = t_m \tau_{mm}.$$

In particular, since $0 < t_m < 1$, we have

$$0 < u_m < \tau_{mm} .$$

Therefore the point

$$X^* = (u_1 - [u])\, P_1 + \dots + (u_{m-1} - [u_{m-1}])\, P_{m-1} + u_m P_m$$

belongs to both Λ and W_m and is lower than Z_m. This contradiction shows that if X is in Λ and

$$X = t_1 X_1 + \dots + t_n Z_n,$$

then $t_1, t_2, \dots, t_n$ are integers. Thus $Z_1, Z_2, \dots, Z_n$ form a basis for Λ.

Since P_m can obviously be expressed as a linear combination of $Z_1, Z_2, \dots, Z_m$ with real coefficients $(1 \leq m \leq n)$, it follows that actually

$$P_1 = s_{11} Z_1, P_2 = s_{21} Z_1 + s_{22} Z_2, \dots, P_n = s_{n1} Z_1 + \dots + s_{nn} Z_n$$

with integral s_{hk}, $1 \leq k \leq h \leq n$. In particular

$$s_{11} = \frac{1}{\tau_{11}} \geq 1 , \dots, s_{nn} = \frac{1}{\tau_{nn}} \geq 1 .$$

A General Theorem on Bounded Point Sets.

The following theorem provides the simplest proof of Minkowski's first theorem and will be crucial in proving his second theorem.

THEOREM: Let S be a bounded set of volume V(S) and let Λ be a lattice of determinant $d(\Lambda)$. If $V(S) > d(\Lambda)$, then S contains two distinct points X_1 and X_2 such that $X_1 - X_2 \neq 0$ lies in Λ.

Minkowski's first theorem follows from this by observing that if the volume of a bounded convex body K: $F(X) \leq 1$ exceeds $2^n d(\Lambda) = d(2\Lambda)$, then K contains two distinct points X_1 and X_2 such that $X_1 - X_2 \neq 0$ lies in 2Λ. Then $\frac{1}{2}(X_1 - X_2) \neq 0$ lies in Λ and is a point of K by convexity and symmetry.

To prove the above theorem let $Z_1, \ldots, Z_n$ be a basis for Λ and denote by D the parallelopiped of all points

$$X = x_1 Z_1 + \ldots + x_n Z_n, \quad 0 \leq x_1 < 1, \ldots, 0 \leq x_n < 1.$$

To every point X of S belongs a unique point $Q = Q(X)$ of Λ such that $X^* = X - Q(X)$ belongs to D. Since S is bounded, Q(X) is one of a finite number of lattice points, say $Q_1, \ldots, Q_r$. Denote by S_ς, for $\varsigma = 1, \ldots, r$, the set of all points X for which $Q(X) = Q_\varsigma$ and denote by $T_\varsigma = S_\varsigma - Q_\varsigma$ the congruent set in D. No two of the sets S_ς have points in common; also $V(S_\varsigma)$ exists, since S_ς is the intersection of S and a certain parallelopiped. Therefore

$$V(S) = \sum_{\varsigma=1}^{r} V(S_\varsigma) .$$

Evidently $V(T_\varsigma) = V(S_\varsigma)$ and hence

$$V(S) = \sum_{\varsigma=1}^{r} V(T_\varsigma).$$

Now if no two of the sets T_ς have a point in common, we have

$$V(S) = \sum_{\varsigma=1}^{r} V(T_\varsigma) = V(\bigcup_{\varsigma=1}^{r} T_\varsigma) \leq V(D) = d(\Lambda).$$

But we are assuming that $V(S) > d(\Lambda)$. Hence two of the sets T_ς, say T_1 and T_2, have a point X^* in common. Thus there are points X_1 and X_2 in S such that

$$X_1 - Q_1 = X^* = X_2 - Q_2 .$$

Then $X_1 - X_2 = Q_1 - Q_2$ is a non-zero point of Λ, which proves the theorem.

Obviously the result of the theorem is true in fact for an unbounded point set in R_n of volume greater than $d(\Lambda)$, for such a set must contain a bounded subset of volume greater than $d(\Lambda)$.

Davenport's Proof of Minkowski's Second Theorem.

The theorem is as follows.

THEOREM. Let $K: F(X) \leq 1$ be a bounded convex body of volume $V(K)$, Λ a lattice of determinant $d(\Lambda)$, and $p_1, p_2, \ldots, p_n$ the successive minima of K in Λ. Then

$$p_1 p_2 \cdots p_n V(K) \leq 2^n d(\Lambda).$$

We first give Davenport's proof. Suppose $P_1, P_2, \ldots, P_n$ are a system of successive minimum points of K in Λ. Then we can find a basis $Z_1, Z_2, \ldots, Z_n$ of Λ such that

$$P_h = \sum_{k=1}^{h} s_{hk} Z_k \qquad (h = 1,2,\ldots,n)$$

with integral coefficients $s_{hk} (1 \leq k \leq h \leq n)$ and $s_{hh} \geq 1$ $(h = 1,2,\ldots,n)$. Every point X in the space R_n can be written in a unique way as

$$X = x_1 Z_1 + x_2 Z_2 + \cdots x_n Z_n = [x_1, x_2, \ldots, x_n]$$

with real coefficients $x_1, x_2, \ldots, x_n$; and X belongs to Λ if and only if these coefficients are integers. We shall call $x_1, x_2, \ldots, x_n$ the coordinates of X.

Clearly if a set S has a volume it is given by

$$V(S) = d(\Lambda) \int\int \cdots \int dx_1 dx_2 \cdots dx_n,$$

where the integration extends over all points $X = [x_1, x_2, \ldots, x_n]$ in S.

Denote by K_h the set defined by $F(X) < p_h$. From our general theory of successive minima for bounded star bodies it follows that if a lattice point X is in K_h, then X is linearly dependent on $P_1, P_2, \ldots, P_{h-1}$, hence X is linearly dependent on $Z_1, Z_2, \ldots, Z_{h-1}$, and hence $x_h = x_{h+1} = \cdots = x_n = 0$.

Now we remark that in order to prove our theorem it would suffice to construct point sets K_h^* (not necessarily convex) with the following three

properties:

(a) $K_h^* \subset K_h$

(b) if $X^{(h+1)}$ and $Y^{(h+1)}$ are two points of K_{h+1}^* with the same last n-h coordinates ($1 \leq h \leq n-1$), then there exist two points $X^{(h)}$ and $Y^{(h)}$ in K_h^* such that $X^{(h)} - Y^{(h)} = X^{(h+1)} - Y^{(h+1)}$.

(c) $V(K_n^*) \geq p_1 p_2 \cdots p_n V(K)$.

For suppose that we can construct such sets and suppose

$$p_1 p_2 \cdots p_n V(K) > 2^n d(\Lambda).$$

Then

$$V(K_n^*) > 2^n d(\Lambda) = d(2\Lambda)$$

and hence there exist two distinct points $X^{(n)}$ and $Y^{(n)}$ in K_n^* such that $X^{(n)} - Y^{(n)}$ lies in 2Λ. Thus $\frac{1}{2}(X^{(n)} - Y^{(n)})$ is in Λ and K_n, since K_n is convex and symmetrical, and hence the last coordinate of $\frac{1}{2}(X^{(n)} - Y^{(n)})$ is zero, i.e., $x_n^{(n)} = y_n^{(n)}$. Then by (b) there exist points $X^{(n-1)}$ and $Y^{(n-1)}$ in K_{n-1}^* such that

$$X^{(n-1)} - Y^{(n-1)} = X^{(n)} - Y^{(n)}.$$

Since $\frac{1}{2}(X^{(n-1)} - Y^{(n-1)})$ is in Λ and K_{n-1}, its last two coordinates must be zero, i.e., $x_n^{(n-1)} = y_n^{(n-1)}$ and $x_{n-1}^{(n-1)} = y_{n-1}^{(n-1)}$. Continuing in this way we finally get two distinct points $X^{(1)}$ and $Y^{(1)}$ in K_1^* such that

$$X^{(n)} - Y^{(n)} = X^{(n-1)} - Y^{(n-1)} = \cdots = X^{(2)} - Y^{(2)} = X^{(1)} - Y^{(1)}.$$

Then $\frac{1}{2}(X^{(1)} - Y^{(1)})$ is a non-zero lattice point in K_1, a contradiction.

Thus the construction of sets K_h^* with properties (a), (b), and (c) would give Minkowski's second theorem. Actually the sets K_h^* which we shall

define will have the property

$$\text{(d)} \qquad V(K_1^*) = p_1^n V(K), \quad V(K_{h+1}^*) = \left(\frac{p_{h+1}}{p_h}\right)^{n-h} V(K_h^*) \qquad (h = 1,\dots,n-1),$$

which of course implies (c).

The construction is as follows. We define $K_1^* = K_1$. We suppose now that K_h^* has been defined and proceed to define K_{h+1}^*. To do this we find h continuous real-valued functions $\phi_1(x_{h+1},\dots,x_n),\dots, \phi_h(x_{h+1},\dots,x_n)$ with domain the projection of K_h on the space spanned by $Z_{h+1},\dots,Z_n$ and ranges such that the point $[\phi_1,\dots,\phi_h,x_{h+1},\dots,x_n]$ lies in K_h. That such functions exist is intuitively quite plausible. However, for Davenport's proof to be completely satisfactory this should be proved. We shall merely indicate one possible method of establishing this existence. Denote by $K_h[c_{h+1},\dots,c_n]$ the set of points of K_h with

$$x_{h+1} = c_{h+1}, \dots, x_n = c_n .$$

Then we could define

$$\phi_1(c_{h+1},\dots,c_n),\dots, \phi_h(c_{h+1},\dots,c_n)$$

as those real numbers such that the point

$$[\phi_1,\dots,\phi_h, c_{h+1},\dots,c_n]$$

is the centroid of $K_h[c_{h+1},\dots,c_n]$, i.e.,

$$\phi_k(c_{h+1},\dots,c_n) = \frac{\int\int\cdots\int_{K_h[c_{h+1},\dots,c_n]} x_k \, dx_1 dx_2 \dots dx_h}{\int\int\cdots\int_{K_h[c_{h+1},\dots,c_n]} dx_1 dx_2 \dots dx_h} \qquad (k = 1,2,\dots,h).$$

It can be proved that with this definition the point

$$[\phi_1,\ldots,\phi_h, c_{h+1},\ldots,c_n]$$

lies in K_h and that $\phi_k(c_{h+1},\ldots,c_n)$ is a continuous function of $c_{h+1},\ldots,c_n$ for $k = 1,2,\ldots,h$. However we shall do this, since we shall subsequently give Minkowski's more elementary proof of his second theorem. not

Now if $X = [x_1,x_2,\ldots,x_n]$ is a point of K_h we put

$$\underline{\Phi}(X) = [\phi_1(x_{h+1},\ldots,x_n),\ldots,\phi_h(x_{h+1},\ldots,x_n),x_{h+1},\ldots,x_n].$$

Thus $\underline{\Phi}(X)$ lies in K_h and actually depends only upon the last n-h coordinates of X. If $X = [x_1,x_2,\ldots,x_n]$ runs through all the points of K_h^*, we now define K_{h+1}^* as the set of points $X' = [x_1', x_2', \ldots, x_n']$ given by

$$X' = X + \left(\frac{p_{h+1}}{p_h} - 1\right) \underline{\Phi}(X) = \underline{\Psi}(X)$$

or, more explicitly, by

$$x_1' = x_1 + \left(\frac{p_{h+1}}{p_h} - 1\right) \phi_1(x_{h+1},\ldots,x_n)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x_h' = x_h + \left(\frac{p_{h+1}}{p_h} - 1\right) \phi_h(x_{h+1},\ldots,x_n)$$

$$x_{h+1}' = x_{h+1} + \left(\frac{p_{h+1}}{p_h} - 1\right) x_{h+1} = \frac{p_{h+1}}{p_h}\, x_{h+1}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x_n' = x_n + \left(\frac{p_{h+1}}{p_h} - 1\right) x_n = \frac{p_{h+1}}{p_n}\, x_n .$$

It is easy to see that the function $\underline{\Psi}(X)$ is in fact a one-to-one mapping of K_h^* onto K_{h+1}.

Moreover $\underline{\Psi}$ has the property that if X' and Y' are two points of

K_{h+1}^* with the same last n - h coordinates and if X and Y are the corresponding points in K_h^* under the inverse mapping, i.e., if

$$X = \Psi^{-1}(X') , \qquad Y = \Psi^{-1}(Y') ,$$

then

$$X - Y = X' - Y' .$$

Thus the one-to-one mapping Ψ^{-1} from K_{h+1}^* to K_h^* has the property needed to give (b).

To prove property (a) we naturally proceed by induction and assume that $K_h^* \subset K_h$. Then if X' is in K_{h+1}^*, we have

$$X' = X + \left(\frac{p_{h+1}}{p_h} - 1\right) \Phi(X),$$

where $X \in K_h^* \subset K_h$ and $\Phi(X) \subset K_h$. Hence

$$F(X') \leq F(X) + \left(\frac{p_{h+1}}{p_h} - 1\right) F(\Phi(X))$$

$$< p_h + \left(\frac{p_{h+1}}{p_h} - 1\right) p_h = p_{h+1},$$

so that $X' \in K_{h+1}$. Thus $K_{h+1}^* \subset K_{h+1}$ and (a) is proved.

Finally the first part of (d) follows from the fact that $K_1^* = K_1$ is given by $F(X) < p_1$. Since the cross-section

$$x_{h+1} = c_{h+1}, \ldots, x_n = c_n$$

of K_h^* has the same h-dimensional volume as the cross section

$$x_{h+1}' = \frac{p_{h+1}}{p_h} c_{h+1}, \ldots, x_n' = \frac{p_{h+1}}{p_h} c_n$$

of K_{h+1}^*, the second part of (d) follows. (We see this by integrating first with respect to $x_1, \ldots, x_h$ and then with respect to $x_{h+1}, \ldots, x_n$ for the two bodies K_h^* and K_{h+1}^*; of course both integrals must be multiplied by $d(\Lambda)$ to give the actual volumes). However (d) implies (c), and thus Minkowski's second theorem is proved.

Minkowski's Proof.

As in Davenport's proof we find a basis $Z_1, Z_2, \ldots, Z_n$ of the lattice Λ such that

$$P_h = \sum_{k=1}^{h} s_{hk} Z_k, \quad s_{hk} = \text{integer}, \quad s_{hh} \geq 1 \qquad (h = 1,2,\ldots,n),$$

where $P_1, P_2, \ldots, P_n$ is a system of successive minimum points of K in Λ. Also we represent each point X in R_n in the form

$$X = x_1 Z_1 + x_2 Z_2 + \ldots + x_n Z_n = \{x_1, x_2, \ldots, x_n\},$$

where we call $x_1, x_2, \ldots, x_n$ the coordinates of X. Again volumes are found by integrating with respect to $x_1, x_2, \ldots, x_n$ and then multiplying by $d(\Lambda)$.

As earlier let D denote the fundamental parallelopiped consisting of all points of the form

$$X = x_1 Z_1 + x_2 Z_2 + \ldots + x_n Z_n, \quad 0 \leq x_1 < 1, \; 0 \leq x_2 < 1, \ldots, 0 \leq x_n < 1 .$$

For any point set S let us denote by $\bar{S}$ the set of points X in D such that $X + Q$ is in S for some Q in Λ. That is, $\bar{S}$ is the point set obtained from S by replacing all the coordinates of all points in S by their fractional parts. We observe that the arguments on pp.28-29 show that if S is a bounded point set of volume V(S) and if S does not contain two distinct points X_1 and X_2 such that $X_1 - X_2$ lies in Λ, then $V(S) = V(\bar{S})$.

We consider the n point sets

$$H_i: \quad F(X) < \tfrac{1}{2} p_i \qquad (i = 1,\ldots,n),$$

Since obviously

$$H_1 \subset H_2 \subset \ldots \subset H_n,$$

we have

$$\bar{H}_1 \subset \bar{H}_2 \subset \ldots \subset \bar{H}_n$$

and hence

$$V(\bar{H}_1) \leq V(\bar{H}_2) \leq \ldots \leq V(\bar{H}_n) \leq d(\Lambda).$$

Clearly H_1 does not contain two points X_1 and X_2 such that $X_1 - X_2$ is in Λ. For otherwise

$$2H_1 : F(X) < p_1$$

would contain two points $Y_1 = 2X_1$ and $Y_2 = 2X_2$ such that $Y_1 - Y_2$ is in 2Λ; then $\frac{1}{2}(Y_1 - Y_2)$ would belong to $2H_1$, a contradiction to the definition of p_1. Hence

$$V(\bar{H}_1) = V(H_1) = (\tfrac{1}{2}p_1)^n \cdot V(K).$$

The bulk of the proof consists now of showing that

$$(A) \qquad V(\bar{H}_{i+1}) \geq \left(\frac{p_{i+1}}{p_i}\right)^{n-i} V(\bar{H}_i) \qquad (i = 1,\ldots,n-1).$$

From (A) Minkowski's second theorem follows at once, for we have

$$V(\bar{H}_2)\ldots V(\bar{H}_n) \geq V(\bar{H}_1)\ldots V(\bar{H}_{n-1}) \left(\frac{p_2}{p_1}\right)^{n-1} \left(\frac{p_3}{p_2}\right)^{n-2} \cdots \frac{p_n}{p_{n-1}}$$

and hence

$$d(\Lambda) \geq V(\bar{H}_n) \geq V(\bar{H}_1) \frac{p_2 p_3 \cdots p_n}{p_1^{n-1}} = \frac{V(K) p_1 p_2 \cdots p_n}{2^n}.$$

Now (A) is trivial if $p_{i+1} = p_i$, so suppose that $p_i < p_{i+1}$. If X_1 and X_2 are two points of H_{i+1} such that $X_1 - X_2$ is in Λ, then the last n-i coordinates of $X_1 - X_2$ must be zero; for otherwise $X_1 - X_2 = \frac{1}{2}(2X_1 - 2X_2)$ would be a point of Λ which is in

$$2H_{i+1} : \; F(X) < p_{i+1}$$

and which is linearly independent of $P_1, P_2, \ldots, P_i$, a contradiction to the definition of p_{i+1}. Let $M^{(i)}$ denote the set obtained from the point set M by replacing the first i coordinates of each point of M by their fractional

parts. (Thus $M^{(n)} = \bar{M}$). Then by what has just been said the set $H_{i+1}^{(i)}$ contains no two distinct points X_1 and X_2 such that $X_1 - X_2$ is in Λ. Similarly for $H_i^{(i)} \subset H_{i+1}^{(i)}$. Thus

$$V(H_i^{(i)}) = V(\overline{H_i^{(i)}}) = V(\bar{H}_i)$$

$$V(H_{i+1}^{(i)}) = V(\overline{H_{i+1}^{(i)}}) = V(\overline{H_{i+1}}),$$

so that to prove (A) it suffices to prove

$$(B) \qquad V(H_{i+1}^{(i)}) \geq \left(\frac{p_{i+1}}{p_i}\right)^{n-i} V(H_i^{(i)}).$$

Let us define a body $H_{i,i+1}$ as follows:

If $[x_1, x_2, \ldots, x_n]$ runs through the points of H_i, then

$$\left[\frac{p_{i+1}}{p_i} x_1, \ldots, \frac{p_{i+1}}{p_i} x_i, x_{i+1}, \ldots, x_n\right]$$

runs through all the points of $H_{i,i+1}$. Thus if $[x_1, x_2, \ldots, x_n]$ runs through all the points of $H_{i,i+1}$, then

$$\left[x_1, \ldots, x_i, \frac{p_{i+1}}{p_i} x_{i+1}, \ldots, \frac{p_{i+1}}{p_i} x_n\right]$$

runs through all the points of H_{i+1}. We claim that

$$(C) \qquad V(H_{i,i+1}^{(i)}) \geq V(H_i^{(i)})$$

and

$$(D) \qquad V(H_{i+1}^{(i)}) = \left(\frac{p_{i+1}}{p_i}\right)^{n-i} V(H_{i,i+1}^{(i)}).$$

These two give (B), hence (A), and thus Minkowski's theorem.

To prove (C) we need the following lemma.

LEMMA. If G is a convex point set in R_n and $t \geq 1$, then

$$V(\bar{G}) \leq V(\overline{t\,G}).$$

This is proved by observing that if P is some point in G, then

$$G - P \subset t(G - P) = t\,G - t\,P,$$

where G - P means the set obtained from G by subtracting the vector P from each vector of G (and similarly for t G - t P). Hence

$$V(\bar{G}) = V(\overline{G - P}) \leq V(\overline{t\,G - t\,P}) = V(\overline{t\,G}).$$

Let now $H_i[c_{i+1},\ldots,c_n]$ or $H_{i,i+1}[c_{i+1},\ldots,c_n]$ be the set of points of H_i or $H_{i,i+1}$ with

$$x_{i+1} = c_{i+1},\ldots,x_n = c_n.$$

Then by the lemma (applied to the space spanned by $Z_1,Z_2,\ldots,Z_i$, i.e., with i in place of n) we see that the i-dimensional volume of $H_i[c_{i+1},\ldots,c_n]^{(i)}$ does not exceed the i-dimensional volume of $H_{i,i+1}[c_{i+1},\ldots,c_n]^{(i)}$. Therefore by integration with respect to $c_{i+1},\ldots,c_n$ we get the inequality (C).

The points of $H_{i+1}^{(i)}$ come from the points of $H_{i,i+1}^{(i)}$ by multiplying each of the last n-i coordinates of each point of $H_{i,i+1}$ by p_{i+1}/p_i. Hence (D) follows. Thus Minkowski's second theorem is proved.

Reduction of a convex body.

Let $f(x_1,\dots,x_n) = \sum_{i,j=1}^{n} a_{ij}\, x_i\, x_j$ be a positive definite quadratic form with real coefficients. Minkowski called $f(x_1,\dots,x_n)$ reduced if for every n-tuple of integers $(g_1,\dots,g_n)$ such that $(g_k,g_{k+1},\dots,g_n)$ have no common factor

$$f(g_1,\dots,g_n) \geq a_{kk} \qquad (k=1,\dots,n)$$

and if

$$a_{kk+1} \geq 0 \qquad (k=1,\dots,n-1).$$

From this definition he proved that for a reduced form

$$a_{11} \leq a_{22} \leq \dots \leq a_{nn}$$

$$\pm 2a_{jk} \leq a_{kk} \qquad (j < k)$$

$$a_{11}\, a_{22} \cdots a_{nn} \leq \gamma_n D ,$$

and where γ_n is a constant depending on n and not on $f(x_1,\dots,x_n)$, and D is the determinant of the matrix $||a_{ij}||$ of the form.

This reduction can be carried over without much difficulty to the case of an arbitrary convex body, as we shall show.

Let R_n be Euclidean space of n dimensions. We shall consider a lattice Λ in R_n generated by n independent vectors $X_1,\dots,X_n$.

Let $f(X) = f(x_1,\dots,x_n)$ be a real valued function of the elements of the vector X and satisfying

i) $f(X) > 0$ except when $X = 0$, $f(0) = 0$,

ii) $f(tX) = |t|\, f(X)$, t real,

iii) $f(X+Y) \leq f(X) + f(Y)$.

Let G_k be the set of lattice points

$$a_1X_1 + a_2X_2 + \dots + a_nX_n \qquad (a_1,\dots,a_n \text{ integral})$$

such that

$$(a_k, a_{k+1}, \dots, a_n) = 1.$$

We make the following definition:

f(X) is reduced with regard to the basis $X_1, X_2, \dots, X_n$ if for every k and for every $Y \in G_k$

$$f(Y) \geq f(X_k).$$

We shall prove the following result.

THEOREM: For every function f(X) satisfying the conditions i), ii), iii) there exists a basis $X_1,\dots,X_n$ for which the body (or the function) f(X) is reduced.

Proof: Let $Y_1,\dots,Y_n$ be any basis of the lattice. Then any other basis $X_1,\dots,X_n$ is obtained by a unimodular substitution, viz.

$$(X_1,\dots,X_n) = (Y_1,\dots,Y_n)\ U\ ,$$

where U is a unimodular matrix (with integral elements and determinant ± 1).

Let $U = (u_1u_2\dots u_n)$ where u_k denotes the k^{th} column of U. Consider now the first column u_1 of all the unimodular matrices U. Choose now u_1 in such a way that

$$L_1 = f(X_1) = f(Yu_1)$$

is a minimum. This minimum exists (from definition of convex body).

Consider now all unimodular matrices U whose first column is u_1 and choose the second column u_2 so that

$$L_2 = f(X_2) = f(Yu_2)$$

is the smallest possible. It is obvious that

$$L_1 \leq L_2 \ .$$

This process can be continued and we finally obtain a matrix $U = ||u_1 \ u_2 \ \dots \ u_n||$ in such a way that

$$(X_1, \dots, X_n) = (Y_1, \dots, Y_n)\, U$$

and

$$f(Yu_1) \leq f(Yu_2) \leq \dots f(Yu_n).$$

$(X_1, \dots, X_n)$ is obviously a basis of the lattice since $Y_1, \dots, Y_n$ is one. Further if v_k is any column of a unimodular matrix such that v_k is linearly independent of $u_1, \dots, u_{k-1}$, then

$$f(Y.v_k) \geq f(Y.u_k).$$

Let now U_{k-1} be a unimodular matrix whose first k-1 columns coincide with those of U. Then

$$U_{k-1} = U \begin{pmatrix} E & A \\ 0 & B \end{pmatrix}, \qquad E = E_{k-1},$$

where B is an integral unimodular matrix. Consider now the k^{th} column of U_{k-1}. Let it be v_k and let the k^{th} column of

$$\begin{pmatrix} E & A \\ 0 & B \end{pmatrix}$$

be $\eta_k = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$. Since B is unimodular $(q_k, q_{k+1}, \dots, q_n) = 1$.

Furthermore

$$v_k = U\, \eta_k \ ,$$

Hence

$$f(Y.u_k) \leq f(Y.v_k) = f(Y.U.\eta_k) = f(X.\eta_k)$$

$$= f(X_1q_1 + X_2q_2 + \ldots + X_nq_n).$$

Now $X_1q_1 + \ldots + X_nq_n$ is in G_k and we thus obtain

$$f(X.\eta_k) \geq f(Y.u_k) = L_k \quad .$$

It is obvious from Gauss' theorem, that η_k can be quite arbitrary so long as $(q_k, q_{k+1}, \ldots, q_n) = 1$. We thus obtain from any basis $Y_1, \ldots, Y_n$ a reduced basis $X_1, \ldots, X_n$.

Thus if $X_1, \ldots, X_n$ is a reduced basis

$$f(X_1) \leq f(X_2) \leq \ldots \leq f(X_n).$$

We shall now prove the following result.

THEOREM: (Weyl - Mahler). If $f(X) \leq 1$ is reduced with regard to the basis $X_1, \ldots, X_n$ then

$$f(X_1)\, f(X_2) \ldots f(X_n) \leq 2^n \left(\frac{3}{2}\right)^{\frac{1}{2}(n-1)(n-2)} \frac{d}{V}$$

where d is the determinant of the lattice and V the volume of the convex body $f(X) \leq 1$.

Proof: Let $P_1, \ldots, P_n$ be the successive minimum points and $M_1, \ldots, M_n$ the successive minimum values of the convex body $f(X) \leq 1$, so that

$$f(P_k) = M_k \qquad (k = 1, \ldots, n)$$

and $P_1, \ldots, P_n$ are linearly independent.

Since $P_1, \ldots, P_n$ are lattice points we have

$$\left\{\begin{array}{l} P_1 = a_{11}X_1 + a_{12}X_2 + \dots + a_{1n}X_n \\ \dots\dots\dots\dots\dots\dots \\ P_k = a_{k1}X_1 + a_{k2}X_2 + \dots + a_{kn}X_n \\ \dots\dots\dots\dots\dots\dots \\ P_n = a_{n1}X_1 + a_{n2}X_2 + \dots + a_{nn}X_n \end{array}\right.$$

Now $P_1,\dots,P_n$ are linearly independent and hence there is a j, $1 \leq j \leq k$ such that

$$a_{jk}, a_{jk+1},\dots,a_{jn}$$

are not all zero (since otherwise $P_1,\dots,P_k$ would be linearly dependent)

So let for some j, $1 \leq j \leq k$

$$(a_{jk}, a_{jk+1},\dots,a_{jn}) = d > 0 .$$

If $d = 1$ then $P_j \in G_k$ and hence

$$L_k \leq f(P_j) = M_j \leq M_k .$$

If $d > 1$ let us put

$$a_{jr} + g_r \equiv 0 \pmod{d}, \quad |g_r| \leq \frac{d}{2} \quad (r = 1,2,\dots,k-1).$$

Consider now the point

$$Q = \frac{1}{d}(P_j + g_1X_1 + g_2X_2 + \dots + g_{k-1}X_{k-1}).$$

This is obviously a lattice point and what is more it is an element in G_k.

Hence

$$L_k \leq f(Q) \leq \frac{1}{d} f(P_j) + \frac{g_1}{d} L_1 + \dots + \frac{g_{k-1}}{d} L_{k-1}$$

$$\leq \frac{M_k}{2} + \frac{L_1 + L_2 + \dots + L_{k-1}}{2} .$$

We shall prove now that

$$L_k \leq \theta_k M_k \qquad (k = 1,\ldots,n)$$

where θ_k does not depend on $f(x)$.

Obviously $L_1 = M_1$ so that $\theta_1 = 1$.

Let us assume that

$$L_1 \leq \theta_1 M_1 \, , \; L_2 \leq \theta_2 M_2 , \; \ldots \, , \; L_{k-1} \leq \theta_{k-1} M_{k-1} \, .$$

Then if $d > 1$ we have

$$L_k \leq \frac{M_k}{2} + \frac{\theta_1 M_1 + \theta_2 M_2 + \ldots + \theta_{k-1} M_{k-1}}{2}$$

$$\leq \left(\frac{1 + \theta_1 + \theta_2 + \ldots + \theta_{k-1}}{2} \right) M_k$$

(from the property $M_1 \leq M_2 \leq \ldots \leq M_n$).

Hence in this case

$$\theta_k \leq \left(\frac{1 + \theta_1 + \theta_2 + \ldots + \theta_{k-1}}{2} \right) .$$

Thus in general we have

$$\theta_k \leq \max \left(1, \frac{1 + \theta_1 + \theta_2 + \ldots + \theta_{k-1}}{2} \right) ,$$

so that

$$\theta_1 = 1, \; \theta_2 = 1 \ldots \theta_k = \left(\frac{3}{2}\right)^{k-2} , \; \ldots\ldots .$$

We have thus shown that

$$L_k \leq \theta_k M_k \, , \qquad \theta_k = \left(\frac{3}{2} \right)^{k-2} , \; \theta_1 = \theta_2 = 1 \, ,$$

and therefore

$$L_1 L_2 \ldots L_n \leq \mu_n M_1 M_2 \ldots M_n \, ,$$

$$\mu_n = \left(\frac{3}{2} \right)^{1+2+\ldots+n-2} = \left(\frac{3}{2} \right)^{\frac{1}{2}(n-1)(n-2)} .$$

Minkowski's fundamental inequality on successive minima gives

$$M_1 M_2 \cdots M_n \leq \frac{2^n d}{V} .$$

Using the last two inequalities we prove the theorem.

In case $f(X)^2 = f(x_1,\ldots,x_n)^2$ is a quadratic form we can give more precise results.

Let

$$f^2(X) = f^2(x_1,\ldots,x_n) = \left(\sum_{i,j} a_{ij} x_i x_j \right)$$

be a reduced quadratic form; then applying the theorem (Weyl-Mahler)

$$a_{11}\, a_{22} \cdots a_{nn} \leq 2^{2n} \left(\frac{3}{2} \right)^{(n-1)(n-2)} \frac{1}{V^2} ,$$

where V is now the volume of the Ellipsoid $\sum a_{ij} x_i x_j \leq 1$.

$$V^2 = \frac{\Gamma(\frac{1}{2})^{2n}}{\Gamma(1+\frac{1}{2}n)^2} \frac{1}{D} = \frac{\pi^n}{\Gamma(1+\frac{n}{2})^2} D^{-1} .$$

Hence

$$a_{11}\, a_{22} \cdots a_{nn} \leq 2^{2n} \left(\frac{3}{2} \right)^{(n-1)(n-2)} \frac{(1+\frac{1}{2}n)^2 D}{\pi^n}$$

where D is the determinant of $\| a_{ij} \|$.

The Minkowski-Hlawka Theorem.

Suppose we have a bounded open set K in n-space, whose volume is V(K). Minkowski's Fundamental Theorem gives a lower bound for $\Delta(K)$ in terms of V(K) if K is convex. Hlawka's Theorem is an inequality in the reverse direction for a less restricted class of K.

THEOREM: For any open set K in n-space, $n \geq 2$, we have

(i) $\Delta \leq V$,

(ii) if K is symmetric in the origin $\Delta \leq \frac{1}{2} V$,

(iii) if K is a star body $\Delta \leq \frac{V}{\zeta(n)}$,

(iv) if K is a symmetric star body $\Delta \leq \frac{V}{2\zeta(n)}$.

The last statement is the Minkowski conjecture first proved by E. Hlawka [Math.Zeit.49(1944)pp.285-312]. Further proofs were given by H.Weyl (unpublished), C.L.Siegel [Ann.of Math.46(1945)pp.340-347] and C.A.Rogers [Ann.of Math.48(1947)pp.994 - as well as another unpublished proof]. The proofs of Weyl and Rogers are of a very elementary nature and the exposition here follows mainly Roger's unpublished proof (which is very similar to Weyl's).

Notation: Summations will be over integers or lattice-points according to context. $\sum'$ means exclusion of the origin from lattice-points or zero from the integers. $\sum^*$ is a sum over all primitive lattice-points. (A point P of a lattice Λ is called primitive if P is in Λ but not in $k\Lambda$ for any $k > 1$.)

Integrations will be over the whole space, but since we shall be dealing with functions which vanish except in a bounded region, no questions of convergence will arise.

LEMMA 1. Let $f(\xi)$ be a real valued continuous function of position in n-space, vanishing outside some sphere. Then, given $\epsilon > 0$, there exists a lattice Λ such that

$$d(\Lambda) = 1, \quad \sum{}' f(X) < \int f(\xi)\,d\xi + \epsilon .$$

For the moment we assume this lemma. The proof will be given later.

LEMMA 2. Let $\varphi(\xi)$ be a real-valued non-negative continuous function in n-space, vanishing outside a large sphere. Then, given $\epsilon > 0$, there exists a lattice Λ such that

$$d(\Lambda) = 1, \quad \sum{}^{*} \varphi(X) < \frac{1}{\varphi(n)} \int \varphi(\xi)\,d\xi + \epsilon .$$

Proof: This lemma follows formally from lemma 1 on writing $f(\xi) = \sum_{\nu > 0} \mu(\nu)\varphi(\nu\xi)$, where μ is the Möbius function. Difficulties of convergence arise, so we define $\mu_N(m)$ by the relation

$$\prod_{p \le N} (1 - p^{-s}) = \sum_{\nu > 0} \mu_N(\nu)\nu^{-s} = \frac{1}{\zeta_N(s)} .$$

It can easily be shown (e.g. by multiplying by $\zeta(s)$ and comparing coefficients) that

$$\sum_{d|m} \mu_N(d) = \begin{cases} 1 & \text{if } p|m \Rightarrow p \ge N, \text{ say } (p, N!) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Write

$$f(\xi) = \sum_{\nu \ge 1} \mu_N(\nu)\varphi(\nu\xi).$$

By lemma 1 there exists a Λ such that

$$\sum{}' f(X) < \int f(\xi)\,d\xi + \epsilon .$$

Consider the two sides of this relation. Firstly

$$\sum{}'f(X) = \sum{}^{*}\sum_{j>0} f(jX) = \sum{}^{*}\sum_{j>0}\sum_{\nu>0}\mu_N(\nu)\varphi(\nu jX)$$

$$= \sum{}^{*}\sum_{m>0}\sum_{d|m}\mu_N(d)\varphi(mX) = \sum{}^{*}\sum_{\substack{(\nu,N)=1\\ \nu>0}}\varphi(\nu X) > \sum{}^{*}\varphi(X),$$

since φ is positive. Secondly

$$\int f(\xi)d\xi = \sum_{\nu>0}\mu_N(\nu)\int\varphi(\nu\xi)d\xi$$

$$= \sum\mu_N(\nu)\nu^{-n}\int\varphi(\xi)d\xi = \frac{1}{\mathfrak{S}_N(n)}\int\varphi(\xi)d\xi < \frac{1}{\mathfrak{S}(n)}\int\varphi(\xi)d\xi + \varepsilon.$$

Thus Lemma 2 follows.

Parts (iii), (iv) of our theorem are easy deductions from lemma 2. Consider a star body K: $F(\xi) < 1$ of volume $V < \mathfrak{S}(n)$; or of volume $V < 2\mathfrak{S}(n)$ if K is symmetric. Define

$$\varphi(\xi) = \begin{cases} 1 & \text{if } F(\xi) \leq 1 \\ 1 - \dfrac{F(\xi)-1}{\delta} & \text{if } 1 \leq F(\xi) \leq 1+\delta \\ 0 & \text{if } F(\xi) \geq 1+\delta\,. \end{cases}$$

Choose δ so small that the volume of the enlarged body $\varphi(\xi) > 0$ is still less than $\mathfrak{S}(n)$ (or $2\mathfrak{S}(n)$). By lemma 2 choose Λ such that

$$\sum{}^{*}\varphi(\xi) < \frac{1}{\mathfrak{S}(n)}\int\varphi(\xi)d\xi + \varepsilon < 1 \text{ (or } 2).$$

There cannot then be a lattice point other than the origin in K for this would give $\sum^{*} \geq 1$, and, if the symmetric lattice point is also in K, $\sum^{*} \geq 2$.

The results (i), (ii) for an arbitrary body follow in exactly the same way from lemma 1, on writing

$$f(\xi) = \max\left(0,\ 1 - \frac{d}{\xi}\right),$$

where d is the distance of ξ from K.

It only remains to prove lemma 2. We deduce from the following fact.

LEMMA 3. Let Λ^- be a fixed (n-1) dimensional lattice of determinant $D > 0$ in the plane $x_n = 0$. Let $\alpha > 0$. Let

$$I(\tau) = \int \cdots \int f(\xi_1, \ldots, \xi_{n-1}, \tau)\, d\xi_1 \cdots d\xi_{n-1} .$$

It is possible to find $P(g_1, \ldots, g_{n-1}, \alpha)$ such that, if Λ is the lattice generated by Λ^- and P, then

$$\sum_{\substack{x_n \neq 0 \\ X \in \Lambda}} f(X) \leq D^{-1} \sum_t I(\alpha t) .$$

Proof: We assume, without loss of generality, that Λ^- is the lattice of points X with integer coordinates and $x_n = 0$. The left-hand side of our relation is

$$S(g_1, \ldots, g_{n-1}) = \sum_{t \neq 0} \sum_{x_1 \ldots x_{n-1}} f(x_1 + tg_1, \ldots, x_{n-1} + tg_{n-1}, \alpha t)$$

where the x_i are integers.

If we integrate over all "boxes" and sum, we have

$$I(\alpha\tau) = \sum_{(x)} \int_0^1 \cdots \int_0^1 f(x_1 + u_1, \ldots, x_{n-1} + u_{n-1}, \alpha\tau)\, du_1 \cdots du_{n-1}$$

$$= \sum_{(x)} t^{n-1} \int_0^{1/t} \cdots \int_0^{1/t} f(x_1 + tg_1, \ldots, x_{n-1} + tu_{n-1}, \alpha\tau)\, dg_1 \cdots dg_{n-1}$$

$$= \int_0^1 \cdots \int_0^1 \sum_{(x)} f(x_1 + tg_1, \ldots, x_{n-1} + tg_{n-1}, \alpha\tau)\, dg_1 \cdots dg_{n-1},$$

since the integrand is periodic with period $\frac{1}{t}$ in each variable. Hence

$$\sum_{t \neq 0} I(\alpha t) = \int_0^1 S(g_1 \cdots g_{n-1})\, dg_1 \cdots dg_{n-1}$$

This relation cannot hold if S is greater than the left-hand expression for all g; so there are $g_1, \ldots, g_{n-1}$ such that

$$S \leq \sum_t{}' I(\alpha t).$$

Lemma 1 now follows easily. Let D be any large number. Choose an (n-1)-lattice $\bar{\Lambda}$ of determinant D so that $f(\xi) = 0$ at all points of $\bar{\Lambda}$ except the origin. Complete $\bar{\Lambda}$ to a lattice Λ as in lemma 3, with $\alpha = \frac{1}{D}$. Then, by the definition of the Riemann integral we have for sufficiently small α (i.e., for large D)

$$\begin{aligned}
\sum{}' f(X) &= \sum_{\substack{x_n \neq 0 \\ X}} f(X) \\
&\leq D^{-1} \sum_t{}' I(\alpha t) \\
&= \alpha \sum_t{}' I(\alpha t) \\
&< \int I(\tau)\, d\tau + \varepsilon \\
&= \int f(\xi)\, d\xi + \varepsilon .
\end{aligned}$$

Rogers' Theorem (Lecture by K.Mahler)

The problem.

If K: $F(X) \leq 1$ is a bounded star body and Λ a lattice in R_n, denote by

$$\mu_1, \mu_2, \ldots, \mu_n$$

the successive minima and by

$$P_1, P_2, \ldots, P_n$$

n successive minimum points of K in Λ. Hence

$$F(P_k) = \mu_k ,$$

and further

$$F(P) \geq \mu_1 \text{ for all } P \neq 0 \text{ in } \Lambda,$$

$F(P) \geq \mu_k$ for all P in Λ which are independent of $P_1, P_2, \ldots, P_{k-1}$.

In the special case that K is a convex body, we learned that, by a theorem of Minkowski, (V(K)volume of K)

(1): $$\mu_1 \mu_2 \cdots \mu_n V(K) \leq 2^n d(\Lambda).$$

The problem arises whether this inequality, or at least a similar one with another constant instead of 2^n, holds for arbitrary bounded star bodies. But it is easy to construct examples which show that such inequalities do not hold: take for K the interior of a sphere with centre at 0 and very large radius, from which all cones C(P) have been removed. Here P runs over all primitive points of Λ inside the sphere, and C(P) consists of all points

$$X = (1+t)P + \varepsilon t\, Y \qquad (t \geq 0)$$

where $\varepsilon > 0$ is a small constant and Y runs over the whole unit sphere. Evidently V(K) can be made arbitrarily large, while $d(\Lambda)$ is fixed and

$$\mu_1 = \mu_2 = \ldots = \mu_n = 1.$$

Since, then, (1) cannot be extended in this obvious manner, it seems reasonable to replace V(K) by another quantity of the same dimension and put the same question. The most fundamental quantity in the geometry of numbers is now $\Delta(K)$, and it is of the same dimension.

We may then put the question:

Does there exist a positive number c_n depending only on the dimension n such that

(2): $$\mu_1 \mu_2 \cdots \mu_n \Delta(K) \leq c_n \, d(\Lambda)$$

for all bounded star bodies K and all lattices K, and if so, what is the smallest allowed value for c_n ?

The first result of this kind was published by Chabauty in C.R.Acad. Sci.Paris vol,227(1948)pp.747 - 749 (October 4); he proved (2) with the constant

$$c_n = 2^{n-(1+\frac{1}{2}+\ldots+\frac{1}{n})}$$

for all star bodies and even for more general sets. Already in August last, before I knew of Chabauty's result, I had found that (2) holds for all bounded star bodies if one takes

$$c_n = n! \, .$$

When I met C.A.Rogers in London in September, I told him of my inequality, and he nearly at once recognized that he could deduce, from earlier work of his on papers by Jarnik and Knichal, that (2) holds even with the constant

$$c_n = 2^{\frac{n-1}{2}} \, ,$$

even for arbitrary point sets, provided the successive minima are defined in a sensible way; he obtained thus a better result than Chabauty's, of which,

neither of us knew at the time. I was soon able to prove that Roger's inequality is best-possible, even if one restricts one-self to bounded star bodies.

Since for every convex body

$$V(K) \leq 2^n \triangle(K),$$

Rogers's result implies then

$$\mu_1 \mu_2 \cdots \mu_n V(K) \leq 2^{n+\frac{n-1}{2}} d(\Lambda),$$

a result not quite as good as Minkowski's. Only if one could show for convex bodies that

$$\mu_1 \mu_2 \cdots \mu_n \triangle(K) \leq d(\Lambda) \tag{3}$$

would Minkowski's inequality (1) be deducible. But so far (3) is known only for $n = 2$, and it is uncertain whether it holds for $n \geq 3$.

I shall to-day prove Rogers' inequality for arbitrary n.

Definition of the minima

Let S be an arbitrary point set in R_n. We denote by μS, where $\mu > 0$, the set of all points μX where X runs over S. For $k = 1,2,\ldots,n$, the k^{th} minimum

$$\mu_k = \mu_k(S,\Lambda)$$

of S over the lattice Λ is then defined as the lower bound of all $\mu > 0$ for which the set μS contains at least k linearly independent points of Λ, and we put

$$\mu_k = +\infty$$

if no such number μ exists.

It is immediately clear from this definition that

$$0 \leq \mu_1 \leq \mu_2 \leq \dots \leq \mu_n .$$

If S is an open star body K: F(X) < 1, then the new μ's are easily seen to coincide with the minima as defined earlier. We shall prove that

$$\mu_1 \mu_2 \dots \mu_n \Delta(S) \leq 2^{\frac{n-1}{2}} d(\Lambda)$$

for all sets, if the left-hand side has a meaning.

The main lemma.

THEOREM 1. Let S be a point set and Λ a lattice in R_n. Denote by μ a positive number and by $m_1, m_2, \dots, m_n$ positive integers, and assume that

(a) $m_1 \mid m_2,\ m_2 \mid m_3,\ \dots,\ m_{n-1} \mid m_n$;

(b) $\mu m_k \leq \mu_k = \mu_k(S, \Lambda)$ for $k = 1, 2, \dots, n$.

Then

(1) $$\Delta(S) < +\infty$$

(2) $$\mu^n m_1 m_2 \dots m_n \Delta(S) \leq d(\Lambda) .$$

Proof: (1) Since $\mu_1 \geq \mu m_1 > 0$, there are numbers μ^* with $0 < \mu^* < \mu_1$. By the definition of μ_1, the set $\mu^* S$ contains no points $\neq 0$ of Λ; hence $\mu^{*-1}\Lambda$ is S-admissible, and so S is of the finite type.

(2) Let ν be any number with

$$0 < \nu < \mu .$$

We denote by L_k the linear manifold of smallest dimension containing

$$0 \text{ and the points of } \Lambda \cap \nu m_k S .$$

Hence L_k consists of all points

$$X = \xi_1 X_1 + \dots + \xi_r X_r$$

where the ξ's run over all real numbers, and $X_1, X_2, \dots, X_r$ are elements of $\Lambda \cap \nu m_k S$. By (b) and the definition of μ_k, L_k is of dimension less than k, say of dimension d_k:

$$d_k < k .$$

By (a), it is clear that if

$$P \in \Lambda \cap \nu m_k S,$$

then

$$\frac{m_{k+1}}{m_k} P \in \Lambda \cap \nu m_{k+1} S ;$$

for $\frac{m_{k+1}}{m_k}$ is an integer. Hence

$$L_k \subset L_{k+1} \quad \text{if } k = 1, 2, \dots, n-1 .$$

Hence we can select a set of lattice points

$$P_1, P_2, \dots, P_n$$

generating Λ such that

L_k is the manifold generated by

$$0, P_1, P_2, \dots, P_{d_k} \qquad (k=1,2,\dots,n).$$

Denote now by Λ' the lattice of basis

$$\frac{1}{\nu m_1} P_1, \frac{1}{\nu m_2} P_2, \dots, \frac{1}{\nu m_n} P_n$$

hence of determinant

$$d(\Lambda') = \frac{d(\Lambda)}{\nu^n m_1 m_2 \dots m_n} .$$

I assert that this lattice is S-admissible. Then let this be false and let

$$X \neq 0$$

be an inner point of $\Lambda' \cap S$. Then X can be written as

$$X = \frac{u_1}{\nu m_1} P_1 + \frac{u_2}{\nu m_2} P_2 + \dots + \frac{u_n}{\nu m_n} P_n$$

with certain integers $u_1, u_2, \ldots, u_n$ not all zero. Choose k, with $1 \leq k \leq n$, such that

$$u_k \neq 0, \text{ but } u_{k+1} = \ldots = u_n = 0 .$$

Then, by (a), the point

$$\nu m_k X = \frac{u_1 m_k}{m_1} P_1 + \ldots + \frac{u_k m_k}{m_k} P_k \in \Lambda \cap \nu m_k S .$$

But since

$$u_k \neq 0,$$

this point $\nu m_k X$ does not lie in the linear manifold generated by

$$0, P_1, \ldots, P_{k-1},$$

and so, since

$$d_k < k,$$

it does not belong to L_k, contrary to the definition of L_k.

Since then Λ' is S-admissible, we have

$$d(\Lambda') = \frac{d(\Lambda)}{\nu^n m_1 m_2 \ldots m_n} \geq \Delta(S),$$

whence the assertion.

A further lemma.

THEOREM 2: Let $\mu_1, \mu_2, \ldots, \mu_n$ be any real numbers satisfying

$$0 < \mu_1 \leq \mu_2 \leq \ldots \leq \mu_n .$$

Then there exist a positive number μ, and n positive integers $m_1, m_2, \ldots, m_n$ such that

(1) $m_1 \mid m_2, m_2 \mid m_3, \ldots, m_{n-1} \mid m_n$

(2) $\mu m_k \leq \mu_k$ for $k = 1, 2, \ldots, n$.

(3) $\mu_1 \mu_2 \ldots \mu_n \leq 2^{\frac{n-1}{2}} \mu^n m_1 m_2 \ldots m_n$.

Proof: Write

$$\delta_k = \frac{\log \mu_k}{\log 2} \text{ whence } \mu_k = 2^{\delta_k} \quad (k = 1, 2, \ldots n)$$

$$r(x) = x - [x]$$

where $[x]$ is the integer g satisfying $g \leq x < g + 1$.

Evidently

$$r(0) = 0, \qquad r(x) + r(-x) = \begin{cases} 0 \text{ if } x \text{ is an integer,} \\ 1 \text{ if } x \text{ is not an integer;} \end{cases}$$

and

$$r(x) = r(y) \text{ if } x \equiv y \pmod 1;$$

hence

$$\sum_{h=1}^{n} \sum_{k=1}^{n} r(\delta_k - \delta_h) \leq \frac{n(n-1)}{2}.$$

Hence there is an index h with $1 \leq h \leq n$ such that

$$\sum_{k=1}^{n} r(\delta_k - \delta_h) \leq \frac{n-1}{2}.$$

More generally, if

$$\delta \equiv \delta_h \pmod 1,$$

then, by the periodicity of $r(x)$,

$$\sum_{k=1}^{n} r(\delta_k - \delta) \leq \frac{n-1}{2},$$

and we can choose δ such that

$$\delta \leq \delta_1,$$

hence

$$\delta \leq \delta_1 \leq \delta_2 \leq \ldots \leq \delta_n.$$

Put

$$\left.\begin{aligned} q_k &= [\delta_k - \delta] \\ m_k &= 2^{q_k} \end{aligned}\right\} \quad (k = 1,2,\ldots,n)$$

$$\mu = 2^{\delta}.$$

Then

$$0 \leq q_1 \leq q_2 \leq \dots \leq q_n,$$

hence the m's are integers and

$$m_1 \mid m_2,\ m_2 \mid m_3,\ \dots,\ m_{n-1} \mid m_n.$$

Also

$$q_k \leq \delta_k - \delta$$

whence

$$\mu_{m_k} = 2^{\delta + q_k} = 2^{[\delta_k - \delta] + \delta} \leq 2^{\delta_k} = \mu_k.$$

Finally

$$\frac{\log\left(\dfrac{\mu_1 \mu_2 \cdots \mu_n}{\mu_{m_1 m_2 \cdots m_n}}\right)}{\log 2} = \sum_{k=1}^{n} (\delta_k - \delta - [\delta_k - \delta])$$

$$= \sum_{k=1}^{n} r(\delta_k - \delta) \leq \frac{n-1}{2}$$

whence the assertion.

Proof of Rogers's theorem

THEOREM: Let S be an arbitrary point set and Λ an arbitrary lattice.

Assume that

$$\mu_1(S, \Lambda) > 0 \text{ and } \Delta(S) > 0.$$

Then

$$\mu_n(S, \Lambda) < \infty \text{ and } \Delta(S) < \infty$$

and moreover

$$\mu_1 \mu_2 \cdots \mu_n \Delta(S) = 2^{\frac{n-1}{2}} d(\Lambda).$$

Proof: Since $\mu_1 > 0$, the lattice Λ contains no points $\neq 0$ of $\mu^* S$ if $\mu^* < \mu_1$; hence $\frac{1}{\mu^*} \Lambda$ is then S-admissible, whence $\Delta(S) < \infty$.

If further $\mu_n(S, \Lambda) = \infty$, put

$$\mu = \mu_1,\ m_1 = m_2 = \dots = m_{n-1} = 1,\ m_n = N$$

where N is an arbitrarily large integer > 0. Then, by Theorem 1,

$$\mu_1^n N \Delta(S) \leq d(\Lambda)$$

whence $\Delta(S) = 0$ contrary to hypothesis. -

Construct corresponding to $\mu_1, \ldots, \mu_n$ the numbers $\mu, m_1, \ldots, m_n$ of Theorem 2, so that

$$\mu_1 \mu_2 \cdots \mu_n \leq 2^{\frac{n-1}{2}} \mu^n m_1 \cdots m_n.$$

Since the conditions of Theorem 1 are satisfied,

$$\mu^n m_1 \cdots m_n \Delta(S) \leq d(\Lambda)$$

and so

$$\mu_1 \mu_2 \cdots \mu_n \Delta(S) \leq 2^{\frac{n-1}{2}} d(\Lambda)$$

as asserted.

A slightly improved discussion shows that " $\leq$ " can be replaced by " $<$ " in the last inequality if S is a bounded star body.

A Mean Value Theorem Implying the Minkowski-Hlawka Theorem

Preliminaries.

We shall be interested in the following groups: the group Ω of non-singular n by n real matrices Y; the normal subgroup Ω_1 of Ω consisting of the matrices of determinant unity; the unimodular group Γ, i.e., the subgroup of Ω consisting of matrices U with integral elements and determinant ± 1; and the proper unimodular group Γ_1, i.e., the subgroup of index two in Γ consisting of the matrices U of determinant 1.

Before we can even state our mean value theorem we must define in the space Ω_1 a fundamental region F with respect to right multiplication by Γ_1, i.e., a well-behaved set F in Ω_1 such that the maps FU, when U runs over Γ_1, cover Ω_1 completely but without overlapping. Note that each element A in Ω_1 defines a lattice of determinant unity in n-dimensional Euclidean space (spanned by the column vectors of A). The matrix AU, where $U \in \Gamma_1$, of course gives the same lattice. Thus F is roughly the space of all lattices of determinant unity.

In order to define F we shall have to map Ω into the space P of positive real symmetric n-rowed matrices S by mapping Y into Y'Y. Since any positive real quadratic form in n variables can be expressed as a sum of squares, it follows that this is an onto mapping. Moreover the complete inverse image of $S = Y'Y$ is the set of matrices OY, where O runs over the n by n orthogonal matrices.

To right multiplication of Y by U corresponds replacing $S = Y'Y$ by $S[U] = U'SU$. Thus we must consider equivalence classes of the S under this operation. We shall sketch the Minkowski theory of finding a fundamental region in the space P with respect to this transformation by elements of Γ.

Reduction theory of positive real symmetric matrices

For a given symmetric matrix S we choose a unimodular matrix $U = (g^{(1)}, \ldots, g^{(n)})$ so that the matrix $U'SU = S[U]$ equivalent to S has certain special properties. Among all possible first columns of unimodular matrices, i.e., among all column vectors of integers with greatest common divisor unity, we choose $g^{(1)}$ so that $\mu_1 = S[g^{(1)}] = g^{(1)'}Sg^{(1)}$ is a minimum. Then among all possible second columns of unimodular matrices having $g^{(1)}$ as first column, i.e., among all integral column vectors g such that the greatest common divisor of the two-rowed minors of $(g^{(1)}g)$ is unity, we choose $g^{(2)}$ so that $\mu_2 = S[g^{(2)}]$ is a minimum. Then among all possible third columns of unimodular matrices having $g^{(1)}$ and $g^{(2)}$ as the first two columns, i.e., among all integral column vectors g such that the greatest common divisor of the three-rowed minors of $(g^{(1)}g^{(2)}g)$ is unity, we choose $g^{(3)}$ so that $\mu_3 = S[g^{(3)}]$ is a minimum. Proceeding in this way we get a unimodular matrix $U = (g^{(1)}, \ldots, g^{(n)})$ such that $\mu_k = S[g^{(k)}] \leq S[g]$ for all possible kth columns g of unimodular matrices with $g^{(1)}, \ldots, g^{(k-1)}$ as the first $k - 1$ columns ($k = 1, \ldots, n$). Note that

$$\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n.$$

Since the element in the jth row and kth column of $U'SU = S[U]$ is $g^{(j)'}Sg^{(k)}$, it follows that changing the sign of $g^{(k)}$ changes the signs of the elements in the kth row and the kth column except for the element $\mu_k = S[g^{(k)}]$ in the main diagonal. Thus by changing the signs of $g^{(2)}, \ldots, g^{(n)}$ in turn (if necessary) we can ensure that the elements of the first row and column of U'SU are non-negative. The matrix U which we have chosen is generally unique up to replacing U by - U.

Thus we have shown that in each equivalence class of symmetric matrices with respect to transformation by unimodular U there is a matrix S with the

two properties given below. (Here $s_k = s_{kk}$ for $k = 1, \ldots, n$ and $\mathfrak{e}^{(1)}, \ldots, \mathfrak{e}^{(n)}$ are the n unit vectors). First, for all integral column vectors g such that $(\mathfrak{e}^{(1)}, \ldots, \mathfrak{e}^{(k-1)}, g)$ can be filled out to a unimodular matrix, i.e., for all g such that $(g_k, g_{k+1}, \ldots, g_n) = 1$, where $g_1, \ldots, g_n$ are the components of g, we have

$$S[g] \geq S[\mathfrak{e}^{(k)}] = s_k.$$

Secondly,

$$s_{1k} \geq 0 \qquad (k = 2, \ldots, n).$$

We shall denote by K the region defined in the space P by the above conditions. A matrix in K is sometimes called reduced.

The region K is defined by infinitely many inequalities which are homogeneous linear in the coefficients of S, i.e., it is the intersection of infinitely many half-spaces bounded by planes through the origin. Thus if S lies in K, so does λS for positive scalar λ ; and if S_1 and S_2 lie in K, so does $S_1 + S_2$. That is, K is a convex half-cone with vertex at S = O. It can be proved that the infinitely many homogeneous linear inequalities are actually consequences of finitely many, so that K is actually a convex pyramid. Moreover K contains inner points. For example for n = 2 the region K is defined by $s_2 \geq s_1 \geq 2s_{12} \geq 0$.

There is a point in K equivalent to any point in P. On the other hand if we identify U and - U it can be proved that an inner point of K is never equivalent to another point of K, although two boundary points may be equivalent. Thus the images $K[U] = U'KU$ cover P without overlapping except for boundary points. Thus K is a fundamental region for the discontinuous representation $S \longrightarrow S[U]$ of the group Γ of unimodular matrices U. Although K is not compact, it can be shown that only finitely many of its images K[U] are neighbors of K. [For more details of the reduction theory see C. L. Siegel, Einheiten quadratischer Formen, Abh. Math. Sem. Hamburgischen Universität vol.

13 (1940) pp. 209-239, §§ 1-3].

Of the infinitely many reduction conditions those obtained as follows are especially useful. In the first condition choose g as the n-rowed column vector with ± 1 in the kth row and 1 in the jth row, where $k < j$. This gives

$$s_j + s_k \pm 2s_{jk} \geq s_j$$

or

$$|s_{jk}| \leq \tfrac{1}{2}s_k.$$

A new coordinate system for the space P.

By successive completions of the square we can write a positive real quadratic form $S(x) = x'Sx = \sum s_{jk}x_jx_k$ in the form

$$\begin{aligned} S[x] = {} & t_1(x_1 + d_{12}x_2 + d_{13}x_3 + \cdots + d_{1n}x_n)^2 \\ & + t_2(x_2 + d_{23}x_3 + \cdots + d_{2n}x_n)^2 \\ & + \cdots \\ & + t_{n-1}(x_{n-1} + d_{n-1,\,n}x_n)^2 \\ & + t_nx_n^2, \end{aligned}$$

where $t_j > 0$ for $j = 1, \ldots, n$. In other words the most general positive real symmetric matrix S has the form $T[D] = D'TD$, where T is a diagonal matrix with positive elements $t_1, \ldots, t_n$ and $D = (d_{jk})$ is a triangular matrix with $d_{jk} = 0$ $(1 \leq k < j \leq n)$, $d_{jj} = 1$ $(j = 1, \ldots, n)$, d_{jk} real $(1 \leq j < k \leq n)$. This is the so-called Jacobi transformation.

Since

$$s_k = t_1d_{1k}^2 + t_2d_{2k}^2 + \cdots + t_k \geq t_k,$$

it is trivial that

$$|S| = t_1t_2 \cdots t_n \leq s_1s_2 \cdots s_n.$$

On the other hand it has been shown on page 45 of these notes that there is a constant C_n depending only on n such that

$$s_1 s_2 \cdots s_n \leq C_n \left| S \right| ,$$

provided S is in the fundamental region K.

We shall need the fact that if S is in K, then the d_{jk} $(1 \leq j < k \leq n)$ and t_1/t_2, t_2/t_3, ..., t_{n-1}/t_n are bounded. Since

$$\frac{s_1}{t_1} \frac{s_2}{t_2} \cdots \frac{s_n}{t_n} = \frac{s_1 s_2 \cdots s_n}{|S|} \leq C_n,$$

we have

$$1 \leq \frac{s_k}{t_k} \leq C_n \qquad (k = 1, \ldots, n).$$

But

$$\frac{s_k}{s_{k+1}} \leq 1 \qquad (k = 1, \ldots, n-1)$$

and hence

$$\frac{t_k}{t_{k+1}} \leq \frac{s_k}{s_{k+1}/C_n} \leq C_n.$$

To prove that the d_{jk} are bounded we proceed by induction on j. For j = 1 we have

$$\left| d_{1k} \right| = \left| \frac{s_{1k}}{s_1} \right| \leq \tfrac{1}{2} \qquad (k = 2, \ldots, n).$$

Now for $1 < j < k$ we have

$$s_{jk} = t_1 d_{1j} d_{1k} + \cdots + t_{j-1} d_{j-1,\,j} d_{j-1,\,k} + t_j d_{jk})$$

so that

$$d_{jk} = \frac{s_{jk}}{t_j} - \frac{t_1}{t_j} d_{1j} d_{1k} + \cdots + \frac{t_{j-1}}{t_j} d_{j-1,\,j} d_{j-1,\,k}.$$

Also

$$\frac{s_{jk}}{t_j} < \frac{s_{jk}}{s_j/C_n} \leq C_n, \quad \frac{t_1}{t_j} \leq C_n^{j-1}, \quad \ldots, \quad \frac{t_{j-1}}{t_j} \leq C_n.$$

Hence the boundedness of the d_{jk} follows by induction on j.

Instead of $t_1, \ldots, t_n$ we introduce the n - 1 ratios $t_j/t_{j+1} = q_j (j = 1, \ldots, n-1)$ and the determinant $q_n = t_1 \cdots t_n = \left| S \right|$. We call $q_1, \ldots, q_n$ and d_{jk} $(1 \leq j < k \leq n)$ the normal coordinates of S. It

is clear that S and λ S have the same normal coordinates with the exception of q_n, for all positive scalar factors λ. In the fundamental region K the normal coordinates, with the exception of q_n, are bounded.

Integration in Ω and Ω_1

In the space Ω we define a volume element by merely imbedding the space Ω in real Euclidean space of n^2 dimensions, i.e., we use the volume element

$$\{dY\} = \prod_{j,k=1}^{n} dy_{jk}.$$

If we make the linear transformation $Y_1 = YC$ or $Y_2 = CY$, where C is in Ω, we see that

$$\{dY_1\} = \{dY_2\} = |C|^n \{dY\}.$$

Thus $\{dY\}$ gives a volume element on Ω which is unchanged by left or right multiplication by an element of Ω_1 (although not of course by an arbitrary element of Ω).

In terms of this volume element $\{dY\}$ on Ω we define a volume element $d\omega_1$ on Ω_1 which is invariant under right and left multiplication by elements of Ω_1. Let G be a subset of Ω_1 which is measurable in the Jordan sense and denote by $\overline{G}$ the cone over the base G consisting of all matrices $Y = \lambda A$, where $0 < \lambda \leq 1$ and $A \in G$. Then

$$V(G) = \int_{\overline{G}} \{dY\}$$

is the Euclidean volume of $\overline{G}$. Since $\{dY\}$ is unchanged by multiplication by an element of Ω_1, it follows that $V(CG) = V(GC) = V(G)$ for any C in Ω_1; consequently the formula

$$V(G) = \int_G d\omega_1$$

defines an invariant volume element $d\omega_1$ on Ω_1. Now if Y is in $\overline{G}$, then $Y = \lambda A$, where $\lambda = |Y|^{1/n}$, $0 < \lambda \leq 1$, $A = |Y|^{-1/n} Y$, $A \in G$. Hence if $\psi(A)$ is a real-valued integrable function on the subset G of Ω_1, we

obtain

$$\int_G \psi(A)\, d\omega_1 = \int_{\overline{G}} \psi(|Y|^{-1/n} Y) \left\{ dY \right\} .$$

Integration in P.

We introduce in the space P of positive real symmetric matrices the Euclidean volume element $\left\{ dS \right\} = \prod_{j \leq k} ds_{jk}$. Let Q be a Jordan measurable set in P and let Q* be the complete inverse image of Q in Ω under the mapping $Y \longrightarrow Y'Y$. Suppose h(S) is a real-valued integrable function on Q. We wish to express

$$\int_{Q^*} h(Y'Y) \left\{ dY \right\}$$

in terms of an integral over Q. Now the most general positive symmetric matrix is $S = T[D] = D'TD$, where T is a diagonal matrix with positive elements $t_1, \ldots, t_n$ and D is a triangular matrix with ones in the main diagonal. If we denote by $T^{1/2}$ the diagonal matrix with the positive elements $t_1^{1/2}, \ldots, t_n^{1/2}$, we can write

$$S = (T^{1/2}D)'(T^{1/2}D).$$

The most general solution of $Y'Y = S$ is thus $Y = O(T^{1/2}D)$, where O is an orthogonal matrix. Hence to express the integral of $h(Y'Y)$ over Q* with respect to $\left\{ dY \right\}$ in terms of an integral over Q, we must merely integrate with respect to the $\frac{1}{2} n(n-1)$ parameters of the orthogonal group. This gives

$$\int_{Q^*} h(Y'Y) \left\{ dY \right\} = \int_Q h(S) j(S) \left\{ dS \right\} ,$$

where j(S) arises from the integration with respect to the orthogonal group.

We claim that $j(S) = a_n |S|^{-\frac{1}{2}}$, where a_n is a constant depending only on n. To show this take $h(S) = 1$ for all S in Q and Q as a neighborhood of S whose size tends to zero. Then

$$j(S) = \lim_{Q \longrightarrow S} \frac{\int_{Q^*} \left\{ dY \right\}}{\int_Q \left\{ dS \right\}} .$$

Now if we make the transformation $Y \longrightarrow YC$, where $C \in \Omega$, we see that $S \longrightarrow C'SC$. The Jacobians of these transformations are respectively $|C|^n$ and $|C|^{n+1}$. Hence

$$j(C'SC) = (\text{abs } C)^{-1} j(S),$$

where abs C denotes the ordinary absolute value of the determinant $|C|$ of C. Now there exists a C in Ω such that $C'SC = E$, where E is the n by n identity matrix. For this C we have

$$\text{abs } C = |S|^{-\frac{1}{2}}$$

and

$$j(S) = (\text{abs } C)j(E) = |S|^{-\frac{1}{2}} a_n,$$

where a_n depends only on n. Thus we have

$$\int_{Q^*} h(Y'Y) \{dY\} = a_n \int_{Q} h(S) |S|^{-\frac{1}{2}} \{dS\} .$$

The constant a_n in the preceding relation can be determined by taking $Q = P$, $Q^* = \Omega$, and $h(S) = \ell^{-\pi\sigma(S)}$, where $\sigma(S)$ denotes the trace of S. For

$$\int_{\Omega} \ell^{-\pi\sigma(Y'Y)} \{dY\} = \left(\int_{-\infty}^{\infty} \ell^{-\pi y^2} dy \right)^{n^2} = 1,$$

and it can be shown that [cf. C. L. Siegel, "Über die analytische Theorie der quadratischer Formen, Ann. of Math. vol. 36 (1935) pp. 527-606, Hilfssatz 37]

$$\int_{P} \ell^{-\pi\sigma(S)} |S|^{-\frac{1}{2}} \{dS\} = \prod_{k=1}^{n} \frac{\Gamma(k/2)}{\pi^{k/2}} .$$

Hence

$$a_n = \prod_{k=1}^{n} \frac{\pi^{k/2}}{\Gamma(k/2)} .$$

Integration in terms of the normal coordinates in P

In applying the formula

$$\int_{Q^*} h(Y'Y) \left\{dY\right\} = a_n \int_{Q} h(S) \left| S \right|^{-\frac{1}{2}} \left\{dS\right\}$$

we shall find it more convenient to use on the right hand side the normal coordinates for S rather than the coordinates $s_{jk}(1 \leq j \leq k \leq n)$. Thus we must compute $\left| S \right|^{-\frac{1}{2}} \left\{dS\right\}$ in terms of the normal coordinates $q_j(1 \leq j \leq n)$ and $d_{jk}(1 \leq j < k \leq n)$.

First we get $\left\{dS\right\}$ in terms of $t_j(1 \leq j \leq n)$ and $d_{jk}(1 \leq j < k \leq n)$. To compute the Jacobian let us arrange the s_{jk} in lexicographical order $s_{11}, s_{12}, \cdots, s_{1n}, s_{22}, \cdots, s_{nn}$ and the t_j and d_{jk} in the order

$$t_1, d_{12}, \cdots, d_{1n}, t_2, d_{23}, \cdots, d_{2n}, \cdots, t_{n-1}, d_{n-1,n}, t_n.$$

Then it is easily seen that the matrix of the Jacobian has zeros above the main diagonal and that the product of the elements in the main diagonal is $t_1^{n-1} t_2^{n-2} \cdots t_{n-1}$. Hence

$$\left\{dS\right\} = t_1^{n-1} t_2^{n-2} \cdots t_{n-1} \left\{dT\right\} \left\{dD\right\},$$

where $\left\{dT\right\}$ and $\left\{dD\right\}$ denote the products of the corresponding differentials.

The task of this section will be completed if we can express $t_1, \cdots, t_n$ in terms of $q_1, \cdots, q_n$. The Jacobian of $q_1, \cdots, q_n$ with respect to $t_1, \cdots, t_n$ is easily computed to be

$$n\frac{t_1}{t_n} = nq_1q_2 \cdots q_{n-1},$$

so that

$$\left\{dS\right\} = \frac{t_1^{n-1} t_2^{n-2} \cdots t_{n-1}}{nq_1q_2 \cdots q_{n-1}} dq_1 \cdots dq_n \left\{dD\right\}$$

Now $t_j = q_j \cdots q_{n-1} t_n$ and hence

$$q_n = t_1t_2 \cdots t_n = q_1q_2^2 \cdots q_{n-1}^{n-1} t_n^n,$$

$$t_n^{\,n} = q_n q_1^{-1} q_2^{-2} \cdots q_{n-1}^{-(n-1)}.$$

Further

$$t_1^{\,n-1} t_2^{\,n-2} \cdots t_{n-1}$$

$$= q_1^{\,n-1} q_2^{(n-1)+(n-2)} \cdots q_{n-1}^{(n-1)+(n-2)+\cdots+1} t_n^{\,n(n-1)/2}$$

$$= t_n^{\,n(n-1)/2} \prod_{j=1}^{n-1} q_j^{jn-j(j+1)/2}$$

$$= q_n^{(n-1)/2} \prod_{j=1}^{n-1} q_j^{jn-j(j+1)/2-j(n-1)/2}$$

$$= q_n^{(n-1)/2} \prod_{j=1}^{n-1} q_j^{j(n-j)/2}.$$

Hence finally

$$|S|^{-\frac{1}{2}} \{dS\} = \frac{1}{n} \{dD\} \; q_n^{\,n/2-1} \, dq_n \prod_{j=1}^{n-1} (q_j^{\,j(n-j)/2-1} dq_j).$$

A fundamental region for Ω_1 modulo Γ_1.

We have a fundamental region K with respect to the transformations $S \longrightarrow S[U] = U'SU$, where U runs over the unimodular group Γ and U and - U give the same transformation. In other words the images K[U] cover P exactly twice, K[U] and K[-U] being the same.

In order to get a fundamental region in Ω with respect to the transformations $Y \longrightarrow YU$, where U runs over the unimodular group Γ, we consider in Ω the complete inverse image K* of K under the mapping $Y \longrightarrow Y'Y$. Clearly the images K*U cover Ω exactly twice. Here U and - U give different transformations, but K* is symmetric (i.e., if $Y \in K^*$, then $-Y \in K^*$) and accordingly K*U and K*(-U) are the same. If we take that half of K* consisting of those Y in K* such that $\sigma(Y) \geq 0$, we get a region H which is a fundamental region in Ω with respect to right multiplication by Γ.

Now let us consider the subgroup Ω_+ of Ω made up by the matrices of positive determinant. Suppose U_1 is the fixed unimodular matrix which has zeros off the main diagonal, - 1 in the first row and first column, and 1 elsewhere on the main diagonal. Put $H = M \smile N$, where M consists of those elements of H which have positive determinant and N consists of those elements of H which have negative determinant. Then $G = M \smile NU_1$ is a fundamental region in Ω_+ with respect to right multiplication by the proper unimodular group Γ_1.

Finally $F = \Omega_1 \frown G$ is a fundamental region in Ω_1 with respect to right multiplication by Γ_1.

Let K_o be that part of K defined by $|S| \leq 1$ and let K_o^*, H_o, M_o, N_o and G_o be the parts of K^*, H, M, N, and G respectively defined by $|Y|^2 \leq 1$. Suppose h(S) is an integrable real-valued function on K_o such that $h(U_1'SU_1) = h(S)$, for example, a function depending only on the coordinates $t_1, \ldots, t_n$ of S. Then since $G_o = \overline{F}$ we have

$$\int_{\overline{F}} h(Y'Y) \left\{dY\right\} = \int_{M_o} h(Y'Y) \left\{dY\right\} + \int_{N_oU_1} h(Y'Y) \left\{dY\right\}$$

$$= \int_{M_o} h(Y'Y) \left\{dY\right\} + \int_{N_o} h(U_1'Y'YU_1) \left\{dY\right\}$$

$$= \int_{M_o} h(Y'Y) \left\{dY\right\} + \int_{N_o} h(Y'Y) \left\{dY\right\}$$

$$= \int_{H_o} h(Y'Y) \left\{dY\right\} = \tfrac{1}{2} \int_{K_o^*} h(Y'Y) \left\{dY\right\}$$

$$= \tfrac{1}{2} a_n \int_{K_o} h(S) \left|S\right|^{1/2} \left\{dS\right\}.$$

In particular for h(S) = 1 we get

$$V(F) = \int_{\overline{F}} \left\{dY\right\} = \tfrac{1}{2} a_n \int_{K_o} \left|S\right|^{-\frac{1}{2}} \left\{dS\right\}$$

Now for a matrix S in K all the normal coordinates except q_n are bounded and hence for S in K_o all the normal coordinates are bounded. Moreover in the expression for $|S|^{-\frac{1}{2}} \{dS\}$ in terms of the normal coordinates, the exponents of $q_1, \ldots, q_n$ are all greater than - 1. Hence

$$V_n = V(F) = \int_F d\omega_1$$

is finite.

Finally we define a new volume element $d\omega$ on Ω_1 as follows

$$d\omega = \frac{1}{V_n} d\omega_1.$$

Thus

$$\int_F d\omega = 1.$$

Statement of the main theorem.

We are now in a position to state our theorem. Let R be the space of n-dimensional real vectors x, where $n > 1$. Denote by $\{dx\}$ the Euclidean volume element in R. We shall prove in the sequel the following result.

THEOREM. Suppose f(x) is a real-valued function on R which is integrable in the Riemann sense and vanishes outside a bounded domain. Suppose A runs over the fundamental region F on Ω_1 with respect to right multiplication by Γ_1. If g runs over all non-zero integral vectors, then

$$\int_F \left\{ \sum_{g \neq 0} f(Ag) \right\} d\omega = \int_R f(x) \{dx\} .$$

If g runs over all primitive integral vectors, then

$$\zeta(n) \int_F \left\{ \sum_g{}^* f(Ag) \right\} d\omega = \int_R f(x) \{dx\} .$$

The asterisk denotes summation over the primitive integral vectors. By a primitive integral vector we mean an integral vector for which the greatest common divisor of the elements is unity, i.e., which is not an integral multiple of another integral vector. Also $\zeta(n)$ denotes the Riemann zeta function.

Hlawka [Math. Zeit. vol. 49 (1943) pp. 285-312, Satz 1] proved that for every positive ϵ there exists a real n-rowed matrix A of determinant $|A| = 1$ such that

$$\sum_{g \neq 0} f(Ag) \leq \int_R f(x) \left\{ dx \right\} + \epsilon .$$

However it follows from the first identity of our theorem that we can even assert that there exists a real n-rowed A with $|A| = 1$ such that

$$\sum_{g \neq 0} f(Ag) \leq \int_R f(x) \left\{ dx \right\} .$$

Thus if J is an arbitrary Jordan measurable set in R (e.g., an open set) whose volume < 1, we see by choosing f(x) as the characteristic function of J that there exists in R a lattice of determinant 1 such that J contains no non-zero lattice point [cf. Hlawka, op. cit., Satz 2]. Similarly if J is a Jordan measurable set symmetric in the origin and of volume < 2, there exists a lattice of determinant 1 such that J contains no non-zero lattice point.

The second identity of our theorem likewise implies that there exists a real n-rowed matrix A with $|A| = 1$ such that

$$\zeta(n) \sum_{g}^{*} f(Ag) \leq \int_R f(x) \left\{ dx \right\}$$

Now let B be a star domain in R, i.e., a point set which is measurable in the Jordan sense and which contains with any point x the whole segment λx, $0 < \lambda < 1$. If the volume of B is less than $\zeta(n)$, we see by choosing f(x) in the preceding inequality as the characteristic function of B that there exists in R a lattice of determinant 1 such that B contains no non-zero lattice point [cf. Hlawka, op. cit., Satz 3]. Similarly if B is a star domain symmetrical in the origin and of volume less than $2\,\zeta(n)$, there exists a lattice of determinant 1 such that B contains no non-zero lattice point [cf. Hlawka, op. cit., Satz 4]. These last two consequences of our theorem were conjectured by Minkowski but first proved by Hlawka over fifty years later.

A lemma of estimation.

With f(x) satisfying the hypothesis of our theorem consider

$$\phi(\lambda, A) = \lambda^n \sum_{g \neq 0} f(\lambda Ag), \quad \Phi(\lambda, A) = \lambda^n \sum_{g \neq 0} \text{abs } f(\lambda Ag),$$

where $0 < \lambda \leq 1$, $A \in \Omega_1$, and abs denotes ordinary absolute value. For fixed λ and A in a bounded region of Ω_1 it is not difficult to see that the sums here have a bounded number of terms; thus for fixed λ the function $\Phi(\lambda, A)$ is integrable over any bounded region in Ω_1. We shall show that $\Phi(\lambda, A)$ is actually integrable over F, which is not bounded, and that the resulting integral is uniformly convergent in λ. These statements are contained in the following lemma.

LEMMA. There exists a function m(A), independent of λ, such that m(A) is integrable over any bounded region in Ω_1, $\Phi(\lambda, A) < m(A)$ everywhere in Ω_1, and the integral $\int_F m(A) d\omega_1$ converges.

Since f(x) is Riemann integrable, it must be bounded. Also f(x) vanishes outside a certain sphere $x'x \leq r^2$. Hence it suffices to prove the assertion of the lemma for the characteristic function of this sphere, namely

$$f(x) = \begin{cases} 1 & \text{if } x'x \leq r^2 \\ 0 & \text{if } x'x > r^2 \end{cases}.$$

With this f(x) the sum $\sum f(\lambda Ag) = \sum \text{abs } f(\lambda Ag)$ is just the number of integral vectors g such that

$$r^2 \geq (\lambda Ag)'(\lambda Ag) = \lambda^2 (g'A'Ag) = \lambda^2 (g'Sg) = \lambda^2 S[g],$$

where $S = A'A$. Thus we estimate the number of integral vectors such that $S[g] \leq r^2 \lambda^{-2}$. If $S = T[D]$, where T and D are as before, and $g_1, \cdots, g_n$ are the coordinates of g, we have

$$S[g] = T[Dg] = \sum_{j=1}^{n} t_j \left(g_j + \sum_{k=j+1}^{n} d_{jk} g_k \right)^2.$$

Hence

$$|g_n| \leq \frac{r}{\lambda t_n^{\frac{1}{2}}}$$

and so g_n has at most $2r\lambda^{-1}t_n^{-\frac{1}{2}} + 1$ values. For each value of g_n the possible values of g_{n-1} lie in an interval of length $2r\lambda^{-1}t_{n-1}^{-\frac{1}{2}}$ and so are at most $2r\lambda^{-1}t_{n-1}^{-\frac{1}{2}} + 1$ in number. Proceeding in this way we see that

$$\lambda^n \sum_g f(\lambda Ag) \leq \lambda^n \prod_{j=1}^{n}\left(\frac{2r}{\lambda t_j^{\frac{1}{2}}} + 1\right)$$

$$= \prod_{j=1}^{n}\left(\frac{2r}{t_j^{\frac{1}{2}}} + \lambda\right) \leq \prod_{j=1}^{n}\left(\frac{2r}{t_j^{\frac{1}{2}}} + 1\right) = m(A),$$

where $m(A)$ depends only on r and the coordinates $t_1, \ldots, t_n$ of $S = A'A$.

Now by definition

$$\int_F m(A)d\omega_1 = \int_{\overline{F}} m(|Y|^{-1/n}Y)\left\{dY\right\}.$$

But $m(|Y|^{-1/n}Y)$ depends only on r and the coordinates $t_1, \ldots, t_n$ of $Y'Y = S$, where we are changing the meaning of S. Hence we can apply the formula from page 67 connecting integrals in and P. This gives

$$\int_F m(A)d\omega_1 = \tfrac{1}{2}a_n \int_{K_o} \prod_{j=1}^{n}\left(\frac{2rq_n^{1/(2n)}}{t_j^{1/2}} + 1\right)|S|^{-\frac{1}{2}}\left\{dS\right\}.$$

Since $t_1 \leq t_2 \leq \cdots \leq t_n$ it suffices to estimate only those terms in the expansion of the product of the form

$$\int_{K_o} \frac{\left(2rq_n^{1/(2n)}\right)^k}{\left(t_1t_2 \cdots t_k\right)^{1/2}}|S|^{-1/2}\left\{dS\right\}, \quad 1 \leq k \leq n.$$

For $k = n$ the convergence of this integral follows from the formula

$$|S|^{-1/2}\left\{dS\right\} = \frac{1}{n}\left\{dD\right\} q_n^{n/2-1}dq_n \prod_{j=1}^{n-1} q_j^{j(n-j)/2-1}dq_j.$$

For $1 \leq k \leq n-1$ we have

$$t_1 t_2 \cdots t_k = q_1 q_2^{\,2} \cdots q_k^{\,k} (q_{k+1} \cdots q_{n-1})^k \, t_n^{\,k}$$

$$= q_1 q_2^{\,2} \cdots q_k^{\,k} (q_{k+1} \cdots q_{n-1})^{\,k} \, q_n^{\,k/n} (q_1 q_2^{\,2} \cdots q_{n-1}^{\,n-1})^{-k/n} ,$$

we have

$$\frac{(2r q_n^{\,1/(2n)})^{\,k}}{(t_1 t_2 \cdots t_k)^{1/2}} \, |S|^{-1/2} \left\{dS\right\}$$

$$= \frac{(2r)^k}{n} \left\{dD\right\} \, q_n^{\,n/2-1} dq_n \prod_{j=1}^{n-1} \left(q_j^{\,j(n-j)/2+jk/(2n)-\min(j,k)/2-1} dq_j \right) .$$

Since the exponents of $q_1, \ldots, q_n$ are all greater than -1 and $q_1, \ldots, q_n$ are bounded in K_o, we see that the integral $\int_F m(A)\, d\omega_1$ must converge, as asserted.

Application of the lemma.

If we put

$$\int_R f(x) \left\{dx\right\} = \Psi ,$$

then for any A in Ω_1 we have by the definition of the Riemann integral

$$\lim_{\lambda \to o} \Phi(\lambda, A) = \lim_{\lambda \to o} \lambda^n \sum_{g \neq o} f(\lambda Ag) = \lim_{\lambda \to o} \lambda^n \sum_{g} f(\lambda Ag) = \Psi .$$

The reason for this is that the points λAg are points of a lattice of determinant λ^n and thus give a subdivision of the sphere $x'x \leq r^2$ into parallelopipeds whose maximum dimension tends to zero with λ. Moreover if A lies in a bounded region of Ω_1, this maximum dimension tends to zero uniformly in A and hence $\Phi(\lambda, A)$ tends to Ψ uniformly.

By the lemma the expression

$$\Psi(\lambda) = \int_F \Phi(\lambda, A)\, d\omega_1 = \int_F \lambda^n \sum_{g \neq o} f(\lambda Ag)\, d\omega_1$$

converges absolutely. Hence we can conclude that the order of summation and

integration can be reversed. More specifically suppose F_ϵ is a bounded subregion of F such that

$$\int_{F-F_\epsilon} m(A)\,d\omega_1 < \epsilon .$$

Then

$$\text{abs}\left\{\int_{F-F_\epsilon} \lambda^n \sum_{g\neq 0} f(\lambda Ag)\,d\omega_1\right\} < \epsilon$$

Also if the prime denotes any sum over a finite number of non-zero g we have

$$\lambda^n \sum{}' \int_{F-F_\epsilon} \text{abs } f(\lambda Ag)\,d\omega_1 = \int_{F-F_\epsilon} \lambda^n \sum{}' \text{abs } f(\lambda Ag)\,d\omega_1$$

$$< \int_{F-F_\epsilon} m(A)\,d\omega_1 < \epsilon ;$$

hence

$$\text{abs}\left\{\lambda^n \sum_{g\neq 0} \int_{F-F_\epsilon} f(\lambda Ag)\,d\omega_1\right\} < \epsilon .$$

But

$$\int_{F_\epsilon} \lambda^n \sum_{g\neq 0} f(\lambda Ag)\,d\omega_1 = \lambda^n \sum_{g\neq 0} \int_{F_\epsilon} f(\lambda Ag)\,d\omega_1,$$

since for A in F_ϵ the number of non-zero terms in the sums is bounded (for fixed λ). Hence our assertion about the interchangeability of summation and integration is justified, i.e.

$$\psi(\lambda) = \lambda^n \sum_{g\neq 0} \int_F f(\lambda Ag)\,d\omega_1 .$$

Also since

$$\lim_{\lambda\to 0} \phi(\lambda, A) = \gamma$$

uniformly in A for A in a bounded region of Ω_1, we can conclude that

$$\lim_{\lambda\to 0} \psi(\lambda) = \lim_{\lambda\to 0} \int_F \phi(\lambda, A)\,d\omega_1 = \int_F \gamma\,d\omega_1 = \gamma V_n .$$

More specifically by the uniformity property we have

$$\lim_{\lambda \to 0} \int_{F_\epsilon} \phi(\lambda, A) d\omega_1 = \int_{F_\epsilon} \lim_{\lambda \to 0} \phi(\lambda, A) d\omega_1 = \int_{F_\epsilon} \gamma \, d\omega_1.$$

Further since abs $\phi(\lambda, A) \leq m(A)$ we have

$$\int_{F-F_\epsilon} \phi(\lambda, A) d\omega_1 \leq \int_{F-F_\epsilon} m(A) d\omega_1 < \epsilon ;$$

since $\gamma = \lim_{\lambda \to 0} \phi(x, A) \leq m(A)$ we have

$$\int_{F-F_\epsilon} \gamma \, d\omega_1 \leq \int_{F-F_\epsilon} m(A) d\omega_1 < \epsilon .$$

Thus our assertion

$$\lim_{\lambda \to 0} \psi(\lambda) = \gamma \, V_n$$

is proved.

Investigation of a certain sum.

We consider the sum

$$\chi(\lambda) = \sum_g^* \int_F f(\lambda Ag) d\omega_1,$$

where the asterisk indicates summation over all primitive integral g. It will turn out to be sufficient to investigate

$$\chi(1) = \sum_g^* \int_F f(Ag) d\omega_1 = \sum_g^* \int_{\bar{F}} f(|Y|^{-1/n} Yg) \left\{dY\right\} .$$

To each primitive g let us associate a fixed proper unimodular matrix U_g with the first column g. Then

$$\chi(1) = \sum_g^* \int_{\overline{FU}_g} f(|Y|^{-1/n} YU_g^{-1} g) \left\{dY\right\}$$

$$= \sum_g^* \int_{\overline{FU}_g} f(|Y|^{-1/n} x) \left\{dY\right\} ,$$

where x denotes the first column of the variable matrix Y in the cone $\overline{FU}_g$.

The unimodular matrices of the particular form

$$U_1 = \begin{pmatrix} 1 & u' \\ 0 & U_o \end{pmatrix},$$

where u is an arbitrary (n-1)-dimensional integral vector and U_o is an arbitrary proper unimodular (n-1)-rowed matrix, constitute a subgroup Δ of Γ_1. The most general element of Γ_1 has the form $U_g U_1$, so that the left cosets of Δ in Γ_1 are $U_g \Delta$, where g runs exactly over all primitive n-dimensional integral vectors. Consequently the union of all the FU_g is a fundamental region $f(\Delta)$ in Ω_1 with respect to right multiplication by Δ. Hence

$$\chi(1) = \sum\nolimits^{*}_{FU_g} \int f(|Y|^{-1/n_x}) \{dY\} = \int_{F(\Delta)} f(|Y|^{-1/n_x}) \{dY\}.$$

To each non-zero real vector x let us associate a specific matrix W_x with determinant 1 and first column x. Then any Y in Ω_1 has the form

$$Y = W_x \begin{pmatrix} 1 & y' \\ 0 & Y_o \end{pmatrix},$$

with a real (n-1)-dimensional vector y and a real non-singular (n-1)-rowed matrix Y_o. Note that $|Y| = |Y_o|$. Moreover if we change the variables of integration from the elements of Y to the elements of x, y, and Y_o, it is not difficult to verify that the Jacobian of the transformation is unity. In other words

$$\{dY\} = \{dx\}\{dy\}\{dY_o\}.$$

In terms of these new coordinates it is simple to define a more natural fundamental region in Ω_1 with respect to right multiplication by elements of Δ. In fact right multiplication of Y by an element

$$U_1 = \begin{pmatrix} 1 & u' \\ 0 & U_o \end{pmatrix}$$

of Δ involves leaving x unchanged, replacing y by $U_o' y + u$, and replacing

Y_o by $Y_o U_o$. This holds in particular for an element $Y = A$ of Ω_1. Thus a fundamental region in Ω_1 with respect to right multiplication by Δ can be obtained by taking all A of the form

$$A = W_x \begin{pmatrix} 1 & y' \\ 0 & Y_o \end{pmatrix},$$

where x is arbitrary, the components of y all lie in the interval $(0, 1)$, and the matrix Y_o lies in the region F_o corresponding to F in $(n-1)$-dimensions. I.e., F_o is the fundamental region in the space of all $(n-1)$-rowed matrices A_o with $|A_o| = 1$ with respect to right multiplication by the group of proper unimodular $(n-1)$-rowed matrices U_o.

Since the first column x of the matrix Y is unchanged by right multiplication by an element of Δ and since Δ consists of matrices of determinant 1, our integral over $F(\Delta)$ can be replaced by the same integral over the cone spanned by our new fundamental region for Δ in Ω_1.

Hence

$$\chi(1) = \int_{F(\Delta)} f(|Y|^{-1/n} x) \{dY\} = \int_{F_o} \int_R f(|Y_o|^{-1/n} x) \{dx\} \{dY_o\}$$

$$= \int_{F_o} |Y_o| \, \gamma \{dY_o\} = \gamma L_{n-1},$$

where

$$L_{n-1} = \int_{F_o} |Y_o| \{dY_o\}.$$

Now if u is any positive scalar factor

$$\int_{uF_o} \{dY_o\} = u^{(n-1)^2} \int_{F_o} \{dY_o\} = u^{(n-1)^2} V_{n-1}.$$

Also

$$\int_{uF_o} |Y_o| \{dY_o\} = u^{n(n-1)} \int_{F_o} |Y_o| \{dY_o\} = u^{n(n-1)} L_{n-1}.$$

Hence

$$\frac{d}{du} \int_{u\overline{F}_o} |Y_o| \left\{dY_o\right\} = n(n-1)u^{n^2-n-1} L_{n-1}.$$

But

$$\frac{d}{du} \int_{u\overline{F}_o} |Y_o| \left\{dY_o\right\} = \lim_{\Delta u \to o} \frac{1}{\Delta u} \int_{(u+\Delta u)\overline{F}_o - u\overline{F}_o} |Y_o| \left\{dY_o\right\}$$

$$= u^{n-1} \lim_{\Delta u \to o} \frac{1}{\Delta u} \int_{(u+\Delta u)\overline{F}_o - u\overline{F}_o} \left\{dY_o\right\}$$

$$= u^{n-1} \lim_{\Delta u \to o} \frac{(u+\Delta u)^{(n-1)^2} - u^{(n-1)^2}}{\Delta u} V_{n-1}$$

$$= (n-1)^2 u^{n^2-n-1} V_{n-1}.$$

Consequently

$$L_{n-1} = \frac{n-1}{n} V_{n-1}.$$

This proves that

$$\chi(1) = \gamma L_{n-1} = \frac{n-1}{n} \gamma V_{n-1}.$$

Now if we replace $f(x)$ by $f(\lambda x)$ we see that γ is replaced by $\lambda^{-n} \gamma$.

Hence

$$\chi(\lambda) = \lambda^{-n} \chi(1) = \lambda^{-n} \frac{n-1}{n} \gamma V_{n-1}.$$

Proof of the mean value theorem.

If g runs over all primitive integral vectors and k over all natural numbers, then kg runs exactly over all non-zero integral vectors. Therefore

$$\psi(\lambda) = \lambda^n \sum_{k=1}^{\infty} \chi(k\lambda) = \lambda^n \sum_{k=1}^{\infty} k^{-n} \lambda^{-n} \chi(1) = \chi(1) \zeta(n),$$

so that $\psi(\lambda)$ is independent of λ. Hence

$$\gamma V_n = \lim_{\lambda \to o} \psi(\lambda) = \psi(1) = \int_F \sum_{g \neq o} f(Ag) d\omega_1$$

or

$$\gamma = \int_F \sum_{g \neq o} f(Ag)\, d\omega .$$

which is the first identity of our theorem. Also

$$\gamma V_n = \lim_{\lambda \to o} \psi(\lambda) = \zeta(n)\, \chi(1) = \zeta(n) \int_F \sum_g{}^{*} f(Ag)\, d\omega_1$$

or

$$\gamma = \zeta(n) \int_F \sum_g{}^{*} f(Ag)\, d\omega ,$$

which is the second identity of our theorem.

Auxiliary results: the volume of F and of K_o.

We have

$$\gamma V_n = \chi(1)\, \zeta(n) = \frac{n-1}{n}\, \gamma V_{n-1}\, \zeta(n)$$

or

$$nV_n = (n-1)V_{n-1}\, \zeta(n).$$

Since $V_1 = 1$ we see that the volume V_n of F is given by

$$nV_n = \prod_{k=2}^{n} \zeta(k).$$

This formula for the volume of F gives

$$\tfrac{1}{2}a_n \int_{K_o} |S|^{-1/2} \left\{dS\right\} = \frac{1}{n} \prod_{k=2}^{n} \zeta(k),$$

where K_o is the domain of reduced positive symmetric matrices with determinant ≤ 1. By a procedure analogous to that used to go from L_{n-1} to V_{n-1} we can go from the preceding to Minkowski's formula for the volume of K_o:

$$\int_{K_o} \left\{dS\right\} = \frac{2 \prod_{k=2}^{n} \zeta(k)}{(n+1)a_n} = \frac{2}{n+1} \prod_{k=2}^{n} \frac{\zeta(k)\, \Gamma(k/2)}{\Pi^{k/2}}$$

Non-homogeneous lattices in two dimensions.

Let R be an unbounded closed convex region, not the whole plane or a half-plane, and not lying inside any infinite strip (i.e. a region of the form $k \leq as + by \leq \ell$). Let X be a point of R. Define X - R to be the reflexion of R in the point X.

We shall show that the intersection $R \cap (X-R)$ is bounded; for, since R is not the whole plane it has one tac-line. Since it is not a half-plane it has a second, and since it does not lie in an infinite strip, these tac-lines are not parallel. We may choose these tac-lines as oblique axes $x = 0$, $y = 0$ and every point of R satisfies $x \geq 0$, $y \geq 0$. If X is (a, b) then X - R satisfies $x \leq 2a$, $y \leq 2b$; so $R \cap (X-R)$ lies in the parallelogram

$$0 \leq x \leq 2a;\ 0 \leq y \leq 2b$$

and so is bounded.

$R \cap (X-R)$ has thus finite area, which we call f(X). Our object is to prove

THEOREM If Λ is an arbitrary non-homogeneous lattice, there is a point X of Λ in R such that

$$f(X) < 4d(\Lambda)$$

Examples.

1.) Let R be $x \geq 0$, $y \geq 0$.

If X is the point (u, v), $f(X) = 4uv$. Hence: There is a point of Λ in the region

$$x \geq 0,\ y \geq 0,\ xy < d(\Lambda).$$

(This result is due to Davenport and Heilbronn, Journal Lond. Math. Soc. 22 (1947) 53-61. For the generalization to n dimensions see Chalk, Quarterly Journal of Math. (Oxford) 18 (1947) 215-227 and Macbeath, Journal Lond. Math. Soc. 23(1948) 141-147.)

2.) Let R be $y \geq x^2$. $f(x, y) = \frac{8}{3}(y-x^2)^{3/2}$.

There is a point of Λ in the region

$$0 \leq y - x^2 < [\tfrac{9}{4}(d(\Lambda))^2]^{1/3}$$

Example (1) shows that the theorem is best possible, i.e. the constant 4 cannot be replaced by a smaller one without affecting the truth of the theorem; however, Example (2) is not best possible, $\frac{9}{4}d^2$ can be replaced by $2d^2$.

Points at infinity

Def. 1 Let K be a closed convex region. K is said to contain the point at infinity $I(\gamma, \delta)$ if $\exists\ \alpha\ \beta$ such that the point $(\alpha + t\gamma, \beta + t\delta)$ is in K for all $t \geq 0$.

$I(\gamma, \delta)$ is the same as $I(c\gamma, c\delta)$ if $c > 0$, and we assume either γ or δ is different from zero.

Def. 2. Let (α', β') be any point. The point-set $(\alpha' + t\gamma, \beta' + t\delta)$ $t \geq 0$ is called the line-segment joining (α', β') to $I(\gamma, \delta)$.

We shall now show that, with this convention, the characteristic property of convex sets is preserved.

LEMMA 1. If a closed convex region K contains two points, of which one is a point at infinity, it contains every point of the line-segment joining them.

Proof. On applying a suitable affine transformation, assume I(1, 0) is the point at infinity, and, by a change of origin, assume (u, 0) is in K for all $u \geq 0$.

Let (a, b) be any finite point of K. We have to show (a+t, b) in K for every positive t. Let $q_n = a + nt$. $(q_n, 0)$ is in K for all $n > n_o > 0$. By convexity

$$(1 - \tfrac{1}{n})\ (a,\ b) + \tfrac{1}{n}(q_n,\ 0)$$

i.e. $(a+t,\ b-\frac{b}{n})$ is in K. Let $n \longrightarrow \infty$

$$(a+t,\ b) \in \bar{K} \subset K.$$

LEMMA 2. Any unbounded closed convex region K contains a point at infinity. Suppose, without loss of generality, that the part K_1 of K that lies in the first quadrant ($x \geq 0,\ y \geq 0$) is unbounded. Let K_1' be the region into which K_1 is mapped by the projectivity

$$x' = \frac{x}{x+y+1} \quad y' = \frac{y}{x+y+1} \quad . \tag{1}$$

(1) maps the first quadrant into the triangular region

$$x' \geq 0 \qquad y' \geq 0 \qquad x' + y' < 1. \tag{2}$$

It transforms convex subsets of the first quadrant into convex subsets of (2); for

$$(\frac{\lambda a+\mu c}{\lambda+\mu},\ \frac{\lambda b+\mu d}{\lambda+\mu}) \text{ is mapped into}$$

$$(\frac{\lambda a + \mu c}{\lambda(a+b+1) + \mu(c+d+1)},\ \frac{\lambda b + \mu d}{\lambda(a+b+1) + \mu(c+d+1)}) \ ,$$

i.e. $$(\frac{\lambda' a' + \mu' c'}{\lambda' + \mu'},\ \frac{\lambda' b' + \mu' d'}{\lambda' + \mu'})$$

where $\lambda' = \lambda(a+b+1),\ \mu' = \mu(c+d+1)$.

Thus the map preserves segments + so convexity. Hence K_1' is convex.

Since x + y is unbounded in K_1 and

$$x' + y' = \frac{(x+y)}{(x+y)+1} \ ,$$

there is a point (ξ, η) of the closure $\bar{K}_1'$ of K_1', such that $\xi + \eta = 1$. Let (α, β) be a point of K_1' so that $\alpha + \beta < 1$. $\bar{K}_1'$ is convex and so contains every point of the segment

$$(\frac{\lambda\alpha+\mu\xi}{\lambda+\mu},\ \frac{\lambda\beta+\mu\eta}{\lambda+\mu}) \ , \lambda, \mu > 0$$

Applying the inverse map of (1),

$$\left(\frac{\alpha}{1-\alpha-\beta}+\frac{\mu}{\lambda}\,\frac{\xi}{1-\alpha-\beta}\,,\ \frac{\beta}{1-\alpha-\beta}+\frac{\mu}{\lambda}\,\frac{\eta}{1-\alpha-\beta}\right)$$

is in $\overline{K}_1 \subset \overline{K} = K$ for $\mu > 0$, $\lambda > 0$. i.e. $I(\xi, \eta)$ is in K.

LEMMA 3. The 4 vertices of a parallelogram cannot all lie on the boundary of R.

Proof Suppose the contrary. Choose oblique axes so that the vertices are $(\pm a, \pm b)$. No point of the 4 regions $|x| > a$ $|y| > b$ is in R. Suppose, for example (c, d) is in R with $c > a$ $d > b$. Then (a, b) is in the interior of the triangle (-a, b); (a_1-b), (c, d), so interior to R, a contradiction.

Hence the point at infinity of R must be $I(\pm 1, 0)$ or $I(0, \pm 1)$. Suppose it is, say I(0, 1). Then there is no point (p, q) in R such that $|p| > a$; for if so (p, v) would be in R (lemma 1) for all $v > q$, contradicting what we have already proved.

This shows that R lies in the infinite strip $|x| \leq a$, a contradiction.

Def. 3 A curve B is said to cross the boundary of R at a point Q, if, for every neighbourhood v of Q, $v \cap B$ contains points in R and points not in R.

LEMMA 4. If R_1 is derived by a translation from R_2, the boundary B_1 of R_1 crosses the boundary of R_2 at not more than one point.

Proof Let T be the translation that carries R_1 into R_2. Let B_1 cross the boundary B_2 of R_2, if possible, at P, Q.

Case 1. Suppose T is not in a direction parallel to PQ. Then P, Q are on B_1, so T(P), T(Q) are on B_2.

P, Q, T(P), T(Q) are 4 vertices of a parallelogram on B_2, contrary to lemma 3.

Case 2. Suppose T is parallel to the direction PQ. Choose the x-axis in this direction, with origin at Q, so that

$$P(-a, 0) \quad Q(0, 0) \quad T: x \longrightarrow x + b.$$

We assume, without loss of generality, that $a, b > 0$. P, Q are on both B_1, B_2, so, applying T and its inverse

$$(-a-b, 0) \text{ is on } B_1$$

$$(b, 0) \text{ is on } B_2.$$

Choose oblique axis of y so that $(0, c)$ is in R_2 for some $c > 0$. Then

$$(-a-b, 0)\ (-a, 0)\ (0, 0) \text{ are on } R_1,$$

so $y = 0$, being the only line through the second point which does not separate the first from the third, is a tac-line and every point of B_1 satisfies $y \geq 0$ (3)

Again $(-a, 0)$, $(b, 0)$, $(0, c)$ are in R_2. Let $m = \min(a, b)$. By convexity the triangular region

$$\frac{|x|}{m} + \frac{y}{c} \leq 1,\ y \geq 0 \qquad (4)$$

is contained in R_2.

Let ν be the neighbourhood of Q defined by the inequality

$$\frac{|x|}{m} + \frac{|y|}{c} < 1.$$

By (3) every point of $\nu \cap B_1$ satisfies (4) and so lies in R_2. But we supposed that B_1 crossed B_2 at Q, and then, by def. 3., $\nu \cap B_1$ contains points not in R_2, a contradiction.

LEMMA 5. The boundary of R has exactly two points in common with that of P - R. The boundary of R (P-R), being finite, must contain points of the boundaries of both R and P-R. These boundaries must therefore intersect at L, L', say, where by symmetry P is the midpoint of LL'. There cannot be another such pair M, M', for then LL'MM' would be vertices of a parallelogram, contrary to lemma 3.

It follows from lemma 5 that the boundary of $R \cap (P-R)$ consists of two connected arcs LL'. One of these, which we call lower boundary, is part

of the boundary of R. The upper boundary is the reflection in P of this, and is part of the boundary of P - R.

The lower half of the region $R \cap (P-R)$ is defined to be that part of $R \cap (P-R)$ which lies on the same side of the line LL' as the lower-boundary-arc.

The functional inequality for $f(x)$.

Let P be an interior point of R. Let V be a point on the lower boundary of $R \cap (P-R)$. Let U be a point on the line-segment PV such that $PU \geq \lambda PV$, $0 \leq \lambda < 1$.

Then $f(U) \leq (1-\lambda^2) f(P)$.

Note We prove this inequality on the assumption that U is interior and that V is not at an intersection of the boundaries; but trivial modifications (or continuity arguments) will cover these cases.

Let L, L' be the intersections of the boundaries of R, P - R. Let the line PUV be called m. m meets the boundary of P - R at V', the reflexion of V in P and it meets the boundary of U - R at V", the reflexion of V in U.

I. The upper arc LL' consists of two parts LV', V'L', which lie on opposite sides of m. Since V is on the lower arc LL', V' is on the upper arc, by reflexion in P. Moreover m does not cut the upper arc at any point other than V', for it cannot cut the boundary of the convex region $R \cap (P-R)$ at more than two points. L, L' lie on opposite sides of m by symmetry, so the arcs LV', L'V' lie wholly on oppposite sides of m.

II. V' is not in U - R.

V" lies on one or other of the line-segments V'P, PV, and so in the interior of R; hence, by reflexion in U, V is an interior point of U - R.

Suppose, then, if possible that V' were in U - R. Then V" on the segment VV' would be an interior point of U - R, contrary to the definition of V".

III. At least one of the arcs LV', L'V' lies wholly outside U - R.

P - R is derived from U - R by a translation; by lemma 4 the arc LL', which forms part of the boundary of P - R, crosses the boundary of U - R at not more than one point. Hence either LV' or L'V' does not cross the boundary of U - R. Suppose LV', say, does not. Then, since V' is not in U - R, by II, neither is any point of the arc LV'.

Suppose that LV' is the arc that lies outside U - R. By I, LV' lies entirely in one of the half-planes, say Γ, bounded by the line m. Let π, ρ be the parts of $R \cap P - R$, $R \cap U - R$ lying on this same side of m:

$$\pi = \Gamma \cap R \cap P - R, \quad \rho = \Gamma \cap R \cap U - R. \tag{5}$$

π has area $\geq f(P)$ ρ area $\geq f(U)$.

IV. $\rho \subset \pi$.

From (5), it suffices to show that $\rho \subset P - R$. Suppose there is a point X of ρ not in P - R. Since U is in P - R the segment XU cuts the lower boundary of P - R at Y, say. Y is in ρ, by convexity; so Y is on the part of the boundary of P - R that lies in $\Gamma \cap R$, i.e. the arc LV'. This contradicts the choice of LV' as the arc lying wholly outside U - R.

Now let ℓ, ℓ', ℓ'' be parallel tac-lines to R, P - R, U - R at V, V', V''. Choose oblique axes with ℓ' as $x = 0$, m as $y = 0$. Choose sign so that all points of π, ρ have non-negative coordinates, ℓ, ℓ'' have equations $x = a$, $x = \lambda a$ $(a > 0)$ and every point of ρ satisfies $\lambda a \leq x \leq a$.

Let μ be the upper bound of $\frac{y}{x}$ for all points (x, y) of ρ. Since ρ is a bounded closed region there is a point $(b, \mu b)$ say, where this bound is attained.

Every point of ρ satisfies the inequalities

$$0 \leq y \leq \mu x \qquad \lambda a \leq x \leq a, \tag{6}$$

so the area is less than the area of the region defined by (6):

$$\tfrac{1}{2}f(U) \leq \tfrac{1}{2}a^2\mu(1-\lambda^2) \qquad (7)$$

Consider the triangular region

$$0 \leq y \leq \mu x \qquad 0 \leq x \leq \lambda a$$

Its vertices are V'(0, 0), V''(λa, 0) and (λa, $\lambda\mu a$). The third vertex (as well as the first two) is in Π, for (b, μ b) is in $\rho \subset \Pi$ by definition of b. Hence $b \geq \lambda a$ by (6), and (λa, $\lambda\mu a$) is on the segment joining the origin V' to (b, μ b), and so (λa, $\lambda\mu a$) is in Π by convexity.

Since the three vertices are in Π, the whole triangle is in Π by convexity. Moreover, no point of it is in ρ, for the second inequalities of (6), (8) contradict one another. Hence the region (8) lies inside $\Pi - \rho$, so

$$\tfrac{1}{2}f(P) - \tfrac{1}{2}f(U) \geq \tfrac{1}{2}\mu a^2 \lambda^2$$

Combine this with (7):

$$f(U) \leq (1-\lambda^2)f(P),$$

and the inequality is established.

LEMMA 6. R contains a point of every lattice.

Choose axes so that I(0, 1) is a point at infinity of R, and so that (0, 0) is a lattice-point. Let (a, b) (c, d) be vectors generating the lattice, where we assume, without loss of generality, $a > 0$, $b > 0$, $ad - bc > 0$. Let (α, β) be any point of R. Then there is a point (α', β' ..) of R such that $|\alpha - \alpha'| > a$; for if not R lies in the infinite strip

$$\alpha - a \leq x \leq \alpha + a,$$

contrary to definition of R.

Let $p = \min(\alpha, \alpha')$, $q = \max(\beta, \beta')$. By convexity (with I(0, 1) R contains the region

$$v \geq q, \quad p \leq a \leq p + \alpha. \qquad (9)$$

Choose a positive integer n such that

$$n \cdot \frac{ad-bc}{a} + p\frac{b}{a} \geq q$$

Then let m be an integer such that

$$p \leq ma + nc \leq p + a$$

We have $mb + nd = (ma+nc)\frac{b}{a} + n \cdot \frac{ad-bc}{a} \geq q$

Hence the lattice-point (ma+nc, mb+nd) satisfies (9) and so lies in R.

It is now easy to prove the main theorem. Choose, by lemma 6, a point X_o of Λ in R. If $f(X_o) < 4d(\Lambda)$ there is nothing to prove. If $f(X_o) \geq 4d(\Lambda)$, there is a point X_1 of Λ, other than X_o in $R \cap (X_o-R)$, by Minkowski's Fundamental Theorem. We may assume that X_1 is in the lower half of the region $R \cap (X_o-R)$ since the lattice is symmetrical about X_o. We may assume further that X_1 is at least half-way from X_o to the boundary, for if it were not one of the other lattice-points which are equally spaced along the line X_oX_1 would satisfy this.

Then $f(X_1) \leq \frac{3}{4} f(X_o)$, by the inequality for f(X) with $\lambda = \frac{1}{2}$. If again $f(X_1) \geq 4d(\Lambda)$ we can repeat the process, and after a finite number of steps we arrive at a lattice-point X_n which satisfies the theorem.