ANNALS OF MATHEMATICS
Vol. 42, No. 2, April, 1941

AN ANALOGUE TO MINKOWSKI'S GEOMETRY OF NUMBERS IN A FIELD OF SERIES

BY KURT MAHLER

(Received November 16, 1939)

Minkowski, in his "Geometrie der Zahlen" (Leipzig 1910), studied properties of a convex body in a space R_n of n dimensions with respect to the set of all lattice points. Let $F(X) = F(x_1, \cdots, x_n)$ be a distance function, i.e. a function satisfying the conditions

$$F(0) = 0, F(X) > 0 \text{ if } X \neq 0;$$

$$F(tX) = |t| F(X) \text{ for all real } t;$$

$$F(X - Y) \leqq F(X) + F(Y).$$

The inequality $F(X) \leqq 1$ defines a convex body in R_n which has its centre at the origin $X = 0$. Suppose that this body has the volume V. The well known result of Minkowski asserts that *if* $V \geqq 2^n$, *then the body contains at least one (and so at least two) lattice points different from* 0. This theorem is contained in the following deeper result of Minkowski (G.d.Z. §§50–53): "*There are* n *independent lattice points* $X^{(1)}, X^{(2)}, \cdots, X^{(n)}$ *in* R_n *with the following properties*: (1) $F(X^{(1)}) = \sigma^{(1)}$ *is the minimum of* $F(X)$ *in all lattice points* $X \neq 0$, *and for* $k \geqq 2$, $F(X^{(k)}) = \sigma^{(k)}$ *is the minimum of* $F(X)$ *in all lattice points* X *which are independent of* $X^{(1)}, \cdots, X^{(k-1)}$. (2) *The determinant* D *of the points* $X^{(1)}, \cdots, X^{(n)}$ *satisfies the inequalities*

$$1 \leqq |D| \leqq n!.$$

(3) *The numbers* $\sigma^{(k)}$ *depend only on* $F(X)$ *and not on the special choice of the lattice points* $X^{(k)}$, *and they satisfy the inequalities*

$$0 < \sigma^{(1)} \leqq \sigma^{(2)} \leqq \cdots \leqq \sigma^{(n)}, \qquad \frac{2^n}{n!} \leqq V\sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)} \leqq 2^n."$$

(A new simple proof for the last part of this theorem was given by *H. Davenport*, Quart. Journ. Math. (Oxford Ser.), Vol. 10 (1939), 119–121).

From Minkowski's theorem, properties of general classes of convex bodies can be obtained. For instance, there is a *convex body* $G(Y) \leqq 1$ *polar to* $F(X) \leqq 1$, and to this body correspond by the theorem n minima $\tau^{(1)}, \tau^{(2)}, \cdots, \tau^{(n)}$. I have proved (Časopis 68 (1939), 93–102), that *these minima are related to the* σ*'s by the inequalities*

$$1 \leqq \sigma^{(h)}\tau^{(n-h+1)} \leqq (n!)^2 \qquad (h = 1, 2, \cdots, n).$$

From this result, applications to inhomogeneous Diophantine inequalities can be made, and in particular, generalizations of *Kronecker's* theorem can be obtained.

The present paper does *not* deal with ordinary convex bodies in a real space. The n-dimensional space P_n with which we shall be concerned has its coordinates in a field $\mathfrak{R}$ with a non-*Archimedean* valuation $|\ x\ |$; a distance function is any function satisfying

$$F(0) = 0,\ F(X) > 0 \text{ if } X \neq 0,$$

$$F(tX) = |\ t\ |\, F(X) \text{ for all } t \text{ in } \mathfrak{R},$$

$$F(X - Y) \leqq \max\,(F(X), F(Y)).$$

The inequality $F(X) \leqq \tau$ then defines the convex body $C(\tau)$, if $\tau > 0$. We show that every convex body is bounded, and that it has properties similar to a parallelepiped in real space.

In particular, let $\mathfrak{R}$ be the field of all Laurent series

$$x = \alpha_f z^f + \alpha_{f-1} z^{f-1} + \alpha_{f-2} z^{f-2} + \cdots$$

with coefficients in an arbitrary field $\mathfrak{k}$; the valuation $|\ x\ |$ is defined as $|\ 0\ | = 0$, and $|\ x\ | = e^f$ if $\alpha_f \neq 0$. Further let Λ_n be the modul of all points in P_n, the coordinates of which are polynomials in z with coefficients in $\mathfrak{k}$; these points we call *lattice points.* We consider only distance functions $F(X)$ which for all $X \neq 0$ in P_n are always as integral power of e. We shall define a certain positive constant V as the volume of $C(1)$; this constant is invariant under all linear transformations of P_n with determinant 1, and the volume of $C(1)$ and that of its polar reciprocal body $C'(1)$ have the product 1. In analogy to Minkowski's theorem, the following theorem holds: "*There are n independent lattice points* $X^{(1)}, \cdots, X^{(n)}$ *in* P_n *with the following properties*: 1) $F(X^{(1)})$ *is the minimum of* $F(X)$ *in all lattice points* $X \neq 0$, *and for* $k \geqq 2$, $F(X^{(k)})$ *is the minimum of* $F(X)$ *in all lattice points* X *which are independent of* $X^{(1)}, \cdots, X^{(k-1)}$. 2) *The determinant of the points* $X^{(1)}, \cdots, X^{(n)}$ *is* 1. 3) *The numbers* $F(X^{(k)}) = \sigma^{(k)}$, *which depend only on* $F(X)$ *and not on the special choice of the lattice points* X, *satisfy the formulae*

$$0 < \sigma^{(1)} \leqq \sigma^{(2)} \leqq \cdots \leqq \sigma^{(n)}, \qquad \sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)} = \frac{1}{V}."$$

Further, we have similar minima $\tau^{(1)}, \cdots, \tau^{(n)}$ for the distance function $G(Y)$ which defines the polar body $C'(1)$; these are related with the σ's by the equations

$$\sigma^{(h)}\tau^{(n-h+1)} = 1 \qquad (h = 1, 2, \cdots, n).$$

These two results can be used to study special Diophantine problems in P_n; a few of them are considered as examples. All the proofs in this paper are based on the methods of Minkowski, and in one final paragraph I make use of ideas of C. L. Siegel.

I. Convex Domains in Non-Archimedean Spaces

1. Notation. In this chapter, we denote by

$\mathfrak{R}$ *an arbitrary field,*

$|x|$ *a non-Archimedean valuation of the elements* x *of* $\mathfrak{R}$,[1]

$\mathfrak{K}$ *the perfect extension of* $\mathfrak{R}$ *with respect to this valuation,*

P_n *the* n*-dimensional space of all points or vectors*

$$X = (x_1, \cdots, x_n),$$

where the coordinates $x_1, \cdots, x_n$ *lie in* $\mathfrak{K}$,

$|X|$ *the length of the vector* X, *viz.*

$$|X| = \max(|x_1|, \cdots, |x_n|).$$

We apply the usual notation for vectors in P_n ; thus if

$$X = (x_1, \cdots, x_n) \quad \text{and} \quad Y = (y_1, \cdots, y_n),$$

and a belongs to $\mathfrak{K}$, then we write

$$X \mp Y = (x_1 \mp y_1, \cdots, x_n \mp y_n),$$

$$aX = (ax_1, \cdots, ax_n),$$

$$XY = \sum_{h=1}^{n} x_h y_h.$$

For instance, the length $|X|$ of X has the properties:

(1) $|X| \geqq 0$, with equality if and only if $X = (0, \cdots, 0) = 0$;

(2) $|aX| = |a||X|$, if a is any element of $\mathfrak{K}$;

(3) $|X \mp Y| \leqq \max(|X|, |Y|)$;

(4) $|XY| \leqq |X||Y|$.

If $\mathfrak{D}$ is any sub-ring of $\mathfrak{K}$, and $X^{(1)}, \cdots, X^{(r)}$ are vectors in P_n, then these are called $\mathfrak{D}$-dependent, or $\mathfrak{D}$-independent, according as there exist, or do not exist elements $a_1, \cdots, a_r$ of $\mathfrak{D}$ not all zero, such that

$$a_1 X^{(1)} + \cdots + a_r X^{(r)} = 0.$$

A set of vectors of P_n is called a $\mathfrak{D}$-modul, if with X and Y it also contains $aX + bY$, where a and b are arbitrary elements of $\mathfrak{D}$; the modul has the dimen-

---

[1] This means that the function $|x|$ satisfies the conditions:

$$|0| = 0, \text{ but } |x| > 0 \text{ for } x \neq 0,$$

$$|xy| = |x||y|,$$

$$|x \mp y| \leqq \max(|x|, |y|).$$

sion m, if there are m, but not $m + 1$, $\mathfrak{D}$-independent elements in it. The dimension of a $\mathfrak{R}$-modul is at most n, while that of any other class of moduli need not be finite.

2. The distance function $F(X)$. A function $F(X)$ of the variable point X in P_n is called a general distance function, if it has the properties:

(A): $$F(X) \geqq 0;$$

(B): $$F(aX) = |a| F(X) \text{ for all } a \text{ in } \mathfrak{R}, \text{ hence } F(0) = 0;$$

(C): $$F(X \mp Y) \leqq \max (F(X), F(Y));$$

it is called a special distance function or simply a distance function, if instead of (A) it satisfies the stronger condition

(A'): $$F(X) > 0 \text{ for } X \neq 0.$$

If τ is a positive number, then the set $C(\tau)$ of all points X with

$$F(X) \leqq \tau$$

is called a convex set;[2] if $F(X)$ is a special distance function, then it is called a convex body. It is clear from the definition of $F(X)$ that a convex set $C(\tau)$ contains the origin 0, and that with X and Y also $aX + bY$ belong to it, if a and b are elements of $\mathfrak{R}$ such that $|a| \leqq 1$, $|b| \leqq 1$. Further, if

$$E^{(1)} = (1, 0, \cdots, 0), E^{(2)} = (0, 1, \cdots, 0), \cdots, E^{(n)} = (0, 0, \cdots, 1)$$

are the n unit vectors of the coordinate system, then

$$X = x_1 E^{(1)} + \cdots + x_n E^{(n)}, \quad \text{i.e.} \quad F(X) \leqq \max_{h=1,2,\cdots,n} (|x_h| F(E^{(h)})),$$

and therefore

$$F(X) \leqq \Gamma |X|, \tag{5}$$

where Γ is the positive constant

$$\Gamma = \max_{h=1,2,\cdots,n} (F(E^{(h)})).$$

$C(\tau)$ contains therefore all points of the cube

$$|X| \leqq \frac{\tau}{\Gamma}.$$

We prove now that *for special distance functions there is a* second *positive constant* γ, *such that for all points in* P_n

$$F(X) \geqq \gamma |X|. \tag{6}$$

[2] We consider only convex sets and bodies as defined; they are obviously symmetrical with respect to the origin.

PROOF: We assume that (6) is not true and show that this leads to a contradiction.

By hypothesis, there is an infinite sequence S of points

$$X^{(h)} = (x_1^{(h)}, \cdots, x_n^{(h)}) \neq 0 \qquad (h = 1, 2, 3, \cdots),$$

such that

$$\lim_{h\to\infty} \frac{F(X^{(h)})}{|X^{(h)}|} = 0.$$

Since

$$\frac{F(aX)}{|aX|} = \frac{F(X)}{|X|}$$

for all $a \neq 0$ in $\mathfrak{R}$, we may assume that for the elements of S

$$\lim_{h\to\infty} F(X^{(h)}) = 0, \qquad |X^{(h)}| = 1,$$

so that in particular the n real sequences

$$|x_k^{(1)}|, |x_k^{(2)}|, |x_k^{(2)}|, \cdots \qquad (k = 1, 2, \cdots, n)$$

are bounded.

Hence we can replace S by an infinite sub-sequence which we again call S: $X^{(1)}, X^{(2)}, X^{(3)}, \cdots$, such that the n real limits

$$a_k = \lim_{h\to\infty} |x_k^{(h)}| \qquad (k = 1, 2, \cdots, n) \tag{7}$$

exist and satisfy the equation

$$\max_{k=1,2,\cdots,n} a_k = 1.$$

We call S a sequence of rank m, if exactly m of the limits $a_1, a_2, \cdots, a_n$ do not vanish; without loss of generality, these are the m first limits $a_1, a_2, \cdots, a_n$. Obviously $1 \leqq m \leqq n$.

If the rank $m = 1$, then for large h

$$|x_1^{(h)}| = 1, \quad \text{and} \quad \frac{X^{(h)}}{x_1^{(h)}} = \left(1, \frac{x_2^{(h)}}{x_1^{(h)}}, \cdots, \frac{x_n^{(h)}}{x_1^{(h)}}\right), = E^{(1)} + X^{*(h)}$$

say, where

$$\lim_{h\to\infty} |X^{*(h)}| = 0.$$

Hence by (5)

$$F(E^{(1)}) = F\left(\frac{X^{(h)}}{x_1^{(h)}} - X^{*(h)}\right) \leqq \max\left(\frac{F(X^{(h)})}{|x_1^{(h)}|}, F(X^{*(h)})\right)$$

$$\leqq \max\,(F(X^{(h)}), \Gamma\,|X^{*(h)}|),$$

and therefore for $h \to \infty$

$$0 \leqq F(E^{(1)}) \leqq 0, \text{ i.e. } F(E^{(1)}) = 0,$$

which is not true.

Hence the rank $m \geqq 2$. Put

$$X^{(g,h)} = \frac{X^{(g)}}{x_m^{(g)}} - \frac{X^{(h)}}{x_m^{(h)}} = (x_1^{(g,h)}, \cdots, x_m^{(g,h)}).$$

Then from (7) for large g, h

$$F(X^{(g,h)} \leqq \max\left(\frac{F(X^{(g)})}{|x_m^{(g)}|}, \frac{F(X^{(h)})}{|x_m^{(h)}|}\right) \leqq \frac{2}{a_m} \max\,(F(X^{(g)}), F(X^{(h)})),$$

and therefore

$$\lim_{\substack{g\to\infty \\ h\to\infty}} F(X^{(g,h)}) = 0.$$

Two cases are now possible:

a: The limit

$$\lim_{\substack{g\to\infty \\ h\to\infty}} |X^{(g,h)}| = \lim_{\substack{g\to\infty \\ h\to\infty}} \max\,(|x_1^{(g,h)}|, \cdots, |x_n^{(g,h)}|)$$

exists and is zero. Hence the n limits in $\mathfrak{R}$

$$x_k^* = \lim_{h\to\infty} \frac{x_k^{(h)}}{x_m^{(h)}} \qquad (k = 1, 2, \cdots, n) \tag{8}$$

all exist, and in particular

$$x_m^* = \lim_{h\to\infty} 1 = 1,$$

so that

$$X^* = (x_1^*, \cdots, x_n^*) \neq 0.$$

By the continuity of $F(X)$,[3]

$$F(X^*) = \lim_{h\to\infty} F\left(\frac{X^{(h)}}{x_m^{(h)}}\right) = \frac{1}{a_m} \lim_{h\to\infty} F(X^{(h)}) = 0,$$

which is not true.

b: The limit

$$\lim_{\substack{g\to\infty \\ h\to\infty}} |X^{(g,h)}|$$

[3] If $\epsilon > 0$ is given, then there is a $\delta > 0$, such that $|F(X) - F(Y)| < \epsilon$ for $|X - Y| < \delta$, as follows easily from the properties (B), (C), and (5).

either does not exist, or exists and is different from zero. That implies that at least one of the limits (8) does not exist. Now obviously

$$\lim_{\substack{g\to\infty\\ h\to\infty}} |\, x_k^{(g,h)} \,| = 0 \qquad (k = m, m+1, \cdots, n),$$

since for large g, h

$$x_m^{(g,h)} = 0; \qquad |\, x_k^{(g,h)} \,| = \left| \frac{x_k^{(g)}}{x_m^{(g)}} - \frac{x_k^{(h)}}{x_m^{(h)}} \right| \leqq \frac{2}{a_m} \max\left(|\, x_k^{(g)} \,|, |\, x_k^{(h)} \,|\right)$$

$$(k = m+1, \cdots, n).$$

Hence the index μ of this non-existing limit (8) is $\leqq m-1$. For this index,

$$\lim_{\substack{g\to\infty\\ h\to\infty}} x_\mu^{(g,h)}$$

either does not exist or exists and is different from zero. Hence there is an infinite one-dimensional sub-sequence

$$X^{(g_i,h_i)} \qquad (i = 1, 2, 3, \cdots) \tag{9}$$

of the double sequence $X^{(g,h)}$, such that for all i

$$|\, x_\mu^{(g_i,h_i)} \,| \geqq c,$$

where c is a positive constant. Further obviously

$$\lim_{i\to\infty} F(X^{(g_i,h_i)} = 0,$$

$$\lim_{i\to\infty} |\, x_k^{(g_i,h_i)} \,| = 0 \qquad (k = m, m+1, \cdots, n),$$

and all $m-1$ first coordinates

$$x_k^{(g_i,h_i)} \qquad (k = 1, 2, \cdots, m-1)$$

are bounded for $i \to \infty$.

Let ξ_i, for every i, be the coordinate

$$x_k^{(g_i,h_i)} \qquad (k = 1, 2, \cdots, m-1)$$

of maximum value $|\, x_k^{(g_i,h_i)} \,|$; hence

$$|\, \xi_i \,| \geqq c, \qquad \text{since} \qquad |\, \xi_i \,| \geqq |\, x_\mu^{(g_i,h_i)} \,|.$$

Then there is an infinite subsequence

$$X^{(g_{i_j},h_{i_j})} \qquad (j = 1, 2, 3, \cdots)$$

of the sequence (9), such that, if

$$X'^{(j)} = \frac{X^{(g_{i_j},h_{i_j})}}{\xi_{i_j}} = (x_1'^{(j)}, \cdots, x_n'^{(j)}) \qquad (j = 1, 2, 3, \cdots),$$

then all n limits

$$\lim_{j\to\infty} |x_k'^{(j)}| = a_k' \qquad (k = 1, 2, \cdots, n)$$

exist and satisfy the equations

$$\max(a_1', \cdots, a_n') = 1, \qquad a_m = a_{m+1} = \cdots = a_n = 0,$$

and

$$0 \leqq \lim_{j\to\infty} F(X'^{(j)}) \leqq \frac{1}{c} \lim_{j\to\infty} F(X^{(g_{i_j}, h_{i_j})}) = 0, \quad \text{i.e.} \quad \lim_{j\to\infty} F(X'^{(j)}) = 0,$$

Therefore the new sequence S'

$$X'^{(1)}, X'^{(2)}, X'^{(3)}, \cdots$$

has the same properties as S, but is of lower rank. Hence by induction with respect to the rank, a contradiction follows also in this case.—

By the inequality (6), all points of the convex body $C(\tau)$ lie in the finite cube

$$|X| \leqq \frac{\tau}{\gamma};$$

a convex body is therefore bounded. Conversely, if a convex set is bounded, then it is a convex body. For if its distance function $F(X)$ is not special, then there is at least one point $X^{(0)} \neq 0$, such that $F(X^{(0)}) = 0$; hence all points of the straight line passing through $X^{(0)}$ and the origin 0 belong to the set.

3. The character of a convex body. Let $C(\tau)$ be a convex body, $F(X)$ its distance function. If $X' \neq 0$ is an arbitrary vector, then the point $X = aX'$, where a is an element of $\mathfrak{R}$, lies in $C(\tau)$ provided that $|a|$ is either sufficiently small and positive, or 0. Hence for every index $h = 1, 2, \cdots, n$, the set S_h of all points

$$X = (x_1, \cdots, x_n) \qquad \text{with} \qquad x_1 = \cdots = x_{h-1} = 0, \qquad x_h \neq 0$$

of $C(\tau)$ is not empty and contains an infinity of elements. By (6),

$$|x_h| \leqq \frac{\tau}{\gamma}$$

for the points of S_h. Therefore $|x_h|$ has a positive upper bound ξ_h in this set, and to every $\epsilon > 0$ there is a point

$$X_\epsilon^{(h)} = (x_{1\epsilon}^{(h)}, \cdots, x_{n\epsilon}^{(h)}),$$

for which

$$F(X_\epsilon^{(h)}) \leqq \tau, \qquad x_{1\epsilon}^{(h)} = \cdots = x_{h-1\epsilon}^{(h)} = 0, \qquad \frac{\xi_h}{1+\epsilon} < |x_{h\epsilon}^{(h)}| \leqq \xi_h,$$

whereas there is no point X for which

$$F(X) \leqq \tau, \qquad x_1 = \cdots = x_{h-1} = 0, \qquad |x_h| > \xi_h .$$

The system of the n points

$$X_\epsilon^{(1)}, X_\epsilon^{(2)}, \cdots, X_\epsilon^{(n)}$$

corresponding to ϵ is obviously $\mathfrak{R}$-independent, and any point X of P_n can be written as

$$X = u_{1\epsilon}X_\epsilon^{(1)} + \cdots + u_{n\epsilon}X_\epsilon^{(n)},$$

where the u's belong to $\mathfrak{R}$ and are given explicitly by

$$u_{h\epsilon} = \sum_{k=1}^{n} \alpha_{hk\epsilon} x_k \qquad (h = 1, 2, \cdots, n)$$

with a matrix

$$(\alpha_{hk\epsilon})_{h,k=1,2,\cdots,n}$$

of non-vanishing determinant and elements depending on ϵ, but not on X.

We distinguish now whether the valuation $|x|$ of $\mathfrak{R}$, is *discrete* or not.

If $|x|$ is discrete, then there is a constant $b > 1$, such that for all $x \neq 0$ in $\mathfrak{R}$ [4]

$$|x| = b^g$$

---

[4] If $|x|$ is discreet, then $F(X)$ has a similar property: *The set s of its values for X in P_n has no point of accumulation except* 0. This is clear for $n = 1$, for then all vectors are multipla of the unit vector (1). Suppose that the statement has already been proved for all spaces of $n - 1$ dimensions, but that it is not true in P_n. There is therefore an infinite sequence Σ of points

$$X^{(k)} = (x_1^{(k)}, \cdots, x_n^{(k)}) \qquad (k = 1, 2, 3, \cdots)$$

in P_n, such that all numbers

$$F(X^{(1)}), \qquad F(X^{(2)}), \qquad F(X^{(3)}), \cdots$$

are different from each other, and that the limit

$$\lim_{k\to\infty} F(X^{(k)}) = \lambda$$

exists and is positive. Write

$$X^{(k)} = x_1^{(k)} E^{(1)} + X^{(k)*} \qquad (k = 1, 2, 3, \cdots)$$

where

$$X^{(k)*} = (0, x_2^{(k)}, \cdots, x_n^{(k)}) \qquad (k = 1, 2, 3, \cdots)$$

lies in the $(n-1)$-dimensional subspace P_{n-1}: $x_1 = 0$, of P_n. By (6), $|x_1^{(k)}|$ is bounded in Σ; hence we may assume that

$$\lim_{k\to\infty} |x_1^{(k)}| = \mu,$$

with a rational integer g depending on x. In this case the set of values $|x_{h\epsilon}^{(h)}|$ satisfies the equations

$$|x_{h\epsilon}^{(h)}| = \xi_h \qquad (h = 1, 2, \cdots, n)$$

for all sufficiently small ϵ. We assume that ϵ is sufficiently small and omit the index ϵ. Put

$$\Phi_\tau(X) = \tau \max(|u_1|, \cdots, |u_n|) = \tau \max_{h=1,2,\cdots,n} \left(\left| \sum_{k=1}^{n} \alpha_{hk} x_k \right| \right).$$

Then obviously

$$F(X) \leqq \tau, \qquad \text{if} \qquad \Phi_\tau(X) \leqq \tau.$$

Conversely let X be any point in $C(\tau)$. Then

$$|x_1| \leqq \xi_1$$

and therefore

$$|u_1| = \frac{|x_1|}{|x_1^{(1)}|} \leqq 1.$$

---

since, if necessary, we can replace Σ by an infinite subsequence. If $\mu = 0$, then for all sufficiently large k

$$F(X^{(k)}) = F(X^{(k*)}),$$

so that the sequence $X^{(1)*}, X^{(2)*}, X^{(3)*}, \cdots$ has the same properties as Σ, contrary to the hypothesis on P_{n-1}.

Hence if

$$\frac{x_1^{(k+1)}}{x_1^{(k)}} = q^{(k)}, \qquad \text{then} \qquad \lim_{k\to\infty} |q^{(k)}| = 1,$$

so that for all sufficiently large k

$$|q^{(k)}| = 1.$$

Obviously

$$X^{*(k)} = X^{(k+1)} - q^{(k)}X^{(k)} = X^{(k+1)*} - q^{(k)}X^{(k)*}$$

lies in P_{n-1}, and for all large k

$$F(X^{(k)}) = F(q^{(k)}X^{(k)}) \neq F(X^{(k+1)}).$$

Hence

$$F(X^{*(k)}) = \max(F(X^{(k)}), F(X^{(k+1)})).$$

Therefore the sequence of positive numbers

$$F(X^{*(1)}), F(X^{*(2)}), F(X^{*(2)}), \cdots$$

contains an infinity of different elements and has the limit λ, so that again a contradiction is obtained.

Hence, if

$$X' = X - u_1 X^{(1)} = (0, x_2', \cdots, x_n'),$$

then

$$F(X') \leqq \max\,(F(X), \mid u_1 \mid F(X^{(1)})) \leqq \tau,$$

and so X' also belongs to $C(\tau)$. Therefore

$$\mid x_2' \mid \leqq \xi_2\,,$$

so that

$$\mid u_2 \mid = \frac{\mid x_2' \mid}{\mid x_2^{(2)} \mid} \leqq 1.$$

Continuing in this way, we obtain all inequalities

$$\mid u_1 \mid \leqq 1, \cdots, \mid u_n \mid \leqq 1,$$

i.e. we have proved

$$\Phi_\tau(X) \leqq t, \qquad \text{if} \qquad F(X) \leqq \tau.$$

The domain defined by

$$\frac{1}{\tau}\,\Phi_\tau(X) = \max_{h=1,2,\cdots,n} \left(\left| \sum_{k=1}^{n} \alpha_{hk} x_k \right| \right) \leqq 1$$

is called a parallelepiped; our result may therefore be expressed in the form:

If the valuation $\mid x \mid$ is discrete, than every convex body $C(\tau)$ is a parallelepiped.

As we have proved, the two domains

$$F(X) \leqq \tau \qquad \text{and} \qquad \Phi_\tau(X) \leqq \tau$$

are identical. In general, this does not imply the identity[5]

$$F(X) = \Phi_\tau(X)$$

for all X, and the function $\Phi_\tau(X)$ depends on τ. Suppose, however, that the set of values of $F(X)$ is the same as that of the values of $\mid x \mid$, and that τ is also an element of this set.[6] Then

$$\Phi_\tau(X) = \Phi(X)$$

becomes independent of τ, and for all X in P_n identically

$$F(X) = \Phi(X), \tag{10}$$

as follows easily from the property (B) of the distance functions.—

[5] E.g., if $\mathfrak{R} = \mathfrak{K}$ is the p-adic field ($p \geqq 3$), $n = 2$, and

$$F(X) = \max\,(\mid x_1 \mid_p\,,\ 2 \mid x_2 \mid_p)\,.$$

[6] It suffices to assume that $F(X)$ does not assume every positive value, and that the equation $F(X) = \tau$ has no solution.

Next assume that *the valuation* $|\ x\ |$ *is not discrete*, so that *its values lie everywhere dense on the positive real axis.* Now the n vectors

$$X_\epsilon^{(1)}, X_\epsilon^{(2)}, \cdots, X_\epsilon^{(n)}$$

will depend on ϵ, and so does the function

$$\Phi_{\tau\epsilon}(X) = \tau \max_{h=1,2,\cdots,n} (|\ u_{h\epsilon}\ |) = \tau \max_{h=1,2,\cdots,n} \left(\left| \sum_{k=1}^{n} \alpha_{hk\epsilon} x_k \right| \right).$$

Evidently

$$F(X) \leqq \tau, \quad \text{if} \quad \Phi_{\tau\epsilon}(X) \leqq \tau. \tag{11}$$

Conversely, suppose $F(X) \leqq \tau$. Then

$$|\ x_1\ | \leqq \xi_1$$

and therefore

$$|\ u_{1\epsilon}\ | = \frac{|\ x_1\ |}{|\ x_{1\epsilon}^{(1)}\ |} < 1 + \epsilon.$$

Hence, if

$$X_\epsilon' = X - u_{1\epsilon} X_\epsilon^{(1)} = (0, x_{2\epsilon}', \cdots, x_{u\epsilon}'),$$

then

$$F(X_\epsilon') \leqq \max\,(F(X), |\ u_{1\epsilon}\ | F(X_\epsilon^{(1)})) < (1 + \epsilon)\tau.$$

There is a number α_ϵ in $\mathfrak{R}$ such that

$$F(X_\epsilon') \leqq |\ \alpha_\epsilon\ | \tau \leqq (1 + \epsilon)\tau, \quad \text{i.e.} \quad F(\alpha_\epsilon^{-1} X_\epsilon') \leqq \tau.$$

Hence

$$|\ \alpha_\epsilon^{-1} x_{2\epsilon}'\ | \leqq \xi_2\,, \qquad |\ x_{2\epsilon}'\ | \leqq (1 + \epsilon)\xi_2\,,$$

and therefore

$$|\ u_{2\epsilon}\ | = \frac{|\ x_{2\epsilon}'\ |}{|\ x_{2\epsilon}^{(2)}\ |} < (1 + \epsilon)^2,$$

so that, if

$$X_\epsilon'' = X_\epsilon' - u_{2\epsilon} X_\epsilon^{(2)} = X - (u_{1\epsilon} X_\epsilon^{(1)} + u_{2\epsilon} X_\epsilon^{(2)}) = (0, 0, x_{3\epsilon}'', \cdots, x_{n\epsilon}''),$$

then

$$F(X_\epsilon'') \leqq \max\,(F(X_\epsilon'), |\ u_{2\epsilon}\ | F(X_\epsilon^{(2)})) < (1 + \epsilon)^2\tau.$$

Continuing in the same way, we obtain the n inequalities

$$|\ u_{h\epsilon}\ | < (1 + \epsilon)^h \qquad (h = 1, 2, \cdots, n),$$

hence

$$\Phi_{\tau\epsilon}(X) < (1 + \epsilon)^n \tau, \quad \text{if} \quad F(X) \leqq \tau. \tag{12}$$

From (11) and (12), since $\epsilon > 0$ is arbitrarily small:

If the valuation $|\ x\ |$ is everywhere dense on the positive axis, then the convex body $C(\tau)$ can be approximated arbitrarily near both from the inside and outside by means of parallelepipeds.

Take now, say $\tau = 1$ and put

$$\Phi_\epsilon(X) = \Phi_{1\epsilon}(X) = \max_{h=1,2,\cdots,n} \left(\left| \sum_{k=1}^{n} \alpha_{hk\epsilon} x_k \right| \right).$$

To every point X, there are two elements α and β of $\mathfrak{R}$, such that

$$\Phi_\epsilon(X) \leqq |\ \alpha\ | \leqq (1 + \epsilon)\Phi_\epsilon(X) \qquad \text{and} \qquad F(X) \leqq |\ \beta\ | \leqq (1 + \epsilon)F(X).$$

Hence from (11)

$$\Phi_\epsilon\left(\frac{X}{\alpha}\right) \leqq 1, \qquad F\left(\frac{X}{\alpha}\right) \leqq 1, \qquad F(X) \leqq |\ \alpha\ | \leqq (1 + \epsilon)\Phi_\epsilon(X),$$

and from (12)

$$F\left(\frac{X}{\beta}\right) \leqq 1, \quad \Phi_\epsilon\left(\frac{X}{\beta}\right) \leqq (1 + \epsilon)^n, \quad \Phi_\epsilon(X) \leqq (1 + \epsilon)^n |\ \beta\ | \leqq (1 + \epsilon)^{n+1} F(X),$$

and therefore uniformly in X

$$(1 + \epsilon)^{-(n+1)}\Phi_\epsilon(X) \leqq F(X) \leqq (1 + \epsilon)\Phi_\epsilon(X). \tag{13}$$

In general, these inequalities cannot be improved to an equation analogous to (10), e.g. if $F(X) = \tau$ has no solution.

4. The character of a convex set. If $F(X)$ is not special, then the set M of all solutions of $F(X) = 0$ contains elements other than $X = 0$. From (B) and (C), with X and Y also $aX + bY$ belongs to M, if a and b are elements of $\mathfrak{R}$. Hence M is a $\mathfrak{R}$-modul, say of dimension $n - m$. Obviously $m < n$; it is possible that $m = 0$, but then $F(X)$ vanishes identically and $C(\tau)$ is the whole space. Suppose therefore, that $1 \leqq m \leqq n - 1$, and let

$$P^{(m+1)}, P^{(m+2)}, \cdots, P^{(n)}$$

be $n - m$ $\mathfrak{R}$-independent elements of M,

$$P^{(1)}, P^{(2)}, \cdots, P^{(m)}$$

m other points of P_n, so that the system of n vectors

$$P^{(1)}, P^{(2)}, \cdots, P^{(n)}$$

is still $\mathfrak{R}$-independent. Then every point X in P_n can be written as

$$X = v_1 P^{(1)} + \cdots + v_n P^{(n)}$$

with elements $v_1, \cdots, v_n$ of $\mathfrak{R}$, viz.

$$v_h = \sum_{k=1}^{n} \beta_{hk} x_k \qquad (h = 1, 2, \cdots, n),$$

where the constant matrix in $\mathfrak{R}$

$$(\beta_{hk})_{h,k=1,2,\ldots,n}$$

has non-vanishing determinant. Since

$$F\left(\sum_{h=m+1}^{n} v_k P^{(h)}\right) = 0,$$

we have

$$F(X) = F\left(\sum_{h=1}^{m} v_h P^{(h)}\right) = \Psi(V),$$

where

$$\Psi(V) = \Psi(v_1, \cdots, v_m) = \Psi\left(\sum_{k=1}^{n} \beta_{1k} x_k, \cdots, \sum_{k=1}^{n} \beta_{nk} x_k\right)$$

is now obviously a special distance function in the m-dimensional space P_m of all points $V = (v_1, \cdots, v_m)$. Every convex set with $m > 0$ can therefore be considered as a cylinder, the basis of which is a convex body of $m < n$ dimensions.

5. The polar body of $C(\tau)$. Let $F(X)$ be the general distance function of §4, Y an arbitrary vector in P_n. Then we define a function $G(Y)$ by

(14) $G(0) = 0$; $G(Y) = \limsup (|XY|)$ *for all* X *with* $F(X) \leqq 1$, *if* $Y \neq 0$.

In order to determine this function, let

$$Q^{(1)}, Q^{(2)}, \cdots, Q^{(n)}$$

be the n points in P_n, which satisfy the equations

$$P^{(h)} Q^{(k)} = \begin{cases} 1 & \text{for } h = k, \\ 0 & \text{for } h \neq k, \end{cases}$$

and write

$$Y = w_1 Q^{(1)} + \cdots + w_n Q^{(n)};$$

then

$$w_h = \sum_{k=1}^{n} \gamma_{hk} y_k \qquad (h = 1, 2, \cdots, n),$$

where the determinant of the matrix in $\mathfrak{R}$

$$(\gamma_{hk})_{h,k=1,2,\ldots,n}$$

does not vanish. Then

$$XY = v_1 w_1 + \cdots + v_n w_n .$$

Hence obviously

$$G(Y) = \infty, \qquad \text{unless} \qquad w_{m+1} = \cdots = w_n = 0.$$

Suppose therefore that

$$w_{m+1} = w_{m+2} = \cdots = w_n = 0, \tag{15}$$

and put

$$G(Y) = \mathrm{X}(W),$$

where $W = (w_1, \cdots, w_m)$ is a vector in P_m. Then from (14),

$$\mathrm{X}(0) = 0; \quad \mathrm{X}(W) = \limsup (|\, VW \,|) \text{ for all } V \text{ with } \Psi(V) \leqq 1, \quad \text{if } W \neq 0, \tag{16}$$

so that the relation of $\mathrm{X}(W)$ to $\Psi(V)$ is the same as that of $G(Y)$ to $F(X)$. By §4, $\Psi(V)$ is a *special* distance function, and so is $\mathrm{X}(W)$, as follows easily from (16) and the properties (A'), (B), and (C) of $\Psi(V)$.

We call $G(Y)$ the *polar function to* $F(X)$; *for* $m < n$ *it is not itself a distance function*, but becomes one in the m-dimensional space (15), where it coincides with $\mathrm{X}(W)$. The set $C'(1/\tau)$: $G(Y) \leqq 1/\tau$, is further called the *polar set to* $C(\tau)$; it lies entirely in (15) and here is identical with the convex body $\mathrm{X}(W) = 1/\tau$.

Suppose now that $m = n$, i.e. both $F(X)$ and $G(Y)$ are special distance functions; then the polar set $C'(1/\tau)$ becomes a convex body. We shall prove that in this case *the relation between* $F(X)$ *and* $G(Y)$ *is reciprocal*, i.e. $F(X)$ is the polar function to $G(Y)$ and $C(\tau)$ the polar body to $C'(1/\tau)$.

This assertion is evident, if $F(X) = |\, X \,|$, for then obviously $G(Y) = |Y|$. Further let

$$\Omega = (a_{hk})_{h,k=1,2,\ldots,n}; \qquad \Omega^K = (a^K_{hk})_{h,k=1,2,\ldots,n}$$

be an arbitrary matrix in $\mathfrak{R}$ with nonvanishing determinant, and its complementary matrix, so that for all X and Y the scalar product[7]

$$\Omega X \cdot \Omega^K Y = XY.$$

Then the transformed distance functions $G'(Y) = G(\Omega^K Y)$ and $F'(X) = F(\Omega X)$ have still the property that the first one is polar to the second, since

$$G'(Y) = G(\Omega^K Y) = \limsup_{F(X) \leqq 1} (|\, X \cdot \Omega^K Y \,|)$$

$$= \limsup_{F(\Omega X) \leqq 1} (|\, \Omega X \cdot \Omega^K Y \,|) = \limsup_{F'(X) \leqq 1} (|\, XY \,|).$$

Further, if $F_1(X)$ and $F_2(X)$ are two distance functions such that for all X

$$F_1(X) \leqq F_2(X),$$

[7] The vector $X' = (x'_1, \cdots, x'_n) = \Omega X$ is defined by $x'_h = \sum_{k=1}^n a_{hk} x_k$ for $h = 1, 2, \cdots, n$.

then the polar distance functions $G_1(Y)$ and $G_2(Y)$ satisfy the inverted inequality

$$G_1(Y) \geqq G_2(Y).$$

We distinguish now the same two cases as in §3. If the valuation $|x|$ is discrete, then we showed the existence of a matrix

$$A = (\alpha_{hk})_{h,k=1,2,\ldots,n}$$

in $\mathfrak{R}$ with determinant different from zero, such that

$$F(X) = \Phi(X) = |AX|$$

identically in X. The polar function to $F(X)$ is therefore

$$G(Y) = |A^K Y|,$$

and since $(A^K)^K = A$, the statement follows at once.—In this case, the definition of $G(Y)$ can obviously be replaced by the simpler one:

$$G(Y) = \max_{X \neq 0} \frac{|XY|}{F(X)}. \tag{17}$$

Secondly, let $|x|$ be everywhere dense on the positive real axis. Then to every $\delta > 0$, there are two matrices

$$A_1 = (\alpha_{hk}^{(1)})_{h,k=1,2,\ldots,n} \quad \text{and} \quad A_2 = (\alpha_{hk}^{(2)})_{h,k=1,2,\ldots,n}$$

in $\mathfrak{R}$ with non-vanishing determinants, such that if

$$F_1(X) = |A_1 X|, \qquad F_2(X) = |A_2 X|,$$

then for all X

$$F_1(X) \leqq F(X) \leqq F_2(X) \leqq (1 + \delta)F_1(X),$$

as follows easily from (13). Hence if

$$G_1(Y) = |A_1^K Y|, \qquad G_2(Y) = |A_2^K Y|$$

are the polar functions to $F(X)$ and $F(X)$, then also

$$G_2(Y) \leqq G(Y) \leqq G_1(Y);$$

and[8]

$$G_2(Y) \leqq (1 + 2\delta)G_1(Y)$$

---

[8] There is a number α in $\mathfrak{R}$ such that

$$1 + \delta \leqq |\alpha| \leqq 1 + 2\delta.$$

Then by hypothesis

$$F_1(X) \overset{\text{polar}}{\leqq} (1 + \delta)F_2(X) \leqq F_2(\alpha X).$$

Hence

$$\frac{1}{1 + 2\delta} G_2(Y) \leqq G_2\left(\frac{Y}{\alpha}\right) \leqq G_1(Y),$$

since the polar function to $F_2(\alpha X)$ is $G_2\left(\frac{Y}{\alpha}\right)$.

for all Y. Since δ can be taken arbitrarily small, the assertion follows again for the same reason.—In this case, the definition of $G(Y)$ is easily replaced by

$$G(Y) = \limsup_{X \neq 0} \frac{|XY|}{F(X)}. \tag{17'}$$

By the proved reciprocity of $F(X)$ and $G(Y)$, the formulae (17) and (17') remain true if $G(Y)$ is replaced by $F(X)$ and vice versa.

II. "Geometry of Numbers" in a Domain of Power Series

6. Notation. We specialize now the fields $\mathfrak{R}$ and $\mathfrak{K}$ of §1, and denote by

$\mathfrak{k}$ *an arbitrary field,*

z *an indeterminate,*

$\mathfrak{T} = k[z]$ *the ring of all polynomials in z with coefficients in $\mathfrak{k}$,*

$\mathfrak{R} = k(z)$ *the quotient field of $\mathfrak{T}$,* i.e. *the field of all rational functions in z with coefficients in $\mathfrak{k}$,*

$|x|$ *the special valuation of $\mathfrak{R}$ defined by*

$$|x| = \begin{cases} 0, & \text{if } x = 0, \\ e^f, & \text{if } x \neq 0 \text{ is of order } f,\end{cases}$$

[9]

$\mathfrak{K}$ *the perfect extension of $\mathfrak{R}$ with respect to this valuation, i.e. the field of all formal Laurent series*

$$x = \alpha_f z^f + \alpha_{f-1} z^{f-1} + \alpha_{f-2} z^{f-2} + \cdots$$

with coefficients in $\mathfrak{k}$; if α_f is the non-vanishing coefficient with highest index $\gtreqless 0$, then $|x| = e^f$,

Λ_n *the set of all "lattice points" in P_n, i.e. that of all points with coordinates in $\mathfrak{T}$.*

The valuation $|x|$ is by definition a power of e with integral exponent. We assume the same for all distance functions which we consider from now onwards, and we shall consider only convex sets or bodies $C(\tau)$, where τ is an exact power of e, say $\tau = e^t$.

7. The volume V of a convex body $C(1)$. Let $F(X)$ be a special distance function, $C(e^t)$ the convex body $F(X) \leqq e^t$, where t is an arbitrary integer. It is obvious that the set $\mathfrak{m}(t)$ of all lattice points in $C(e^t)$ forms a $\mathfrak{k}$-modul. In the special case $F(X) = |X|$, this set has exactly

$$M_0(t) = n(t+1)$$

$\mathfrak{k}$-independent elements. Hence, by the inequalities (5) and (6), $\mathfrak{m}(t)$ has always a finite dimension $M(t)$, and this dimension is certainly positive for large t.

---

[9] The order of a rational function is the degree of its numerator minus the degree of its denominator.

Obviously

$$M_0(t+1) = M_0(t) + n. \tag{18}$$

Suppose that t is already so large that

$$e^{t+1} \geqq \Gamma.$$

Then a lattice point in $C(e^{t+1})$ can be written as

$$X = X_0 + zX_1,$$

where X_0 and X_1 are again lattice points, and the coordinates of X_0 lie in $\mathfrak{k}$, i.e.

$$|X_0| \leqq 1, \qquad F(X_0) \leqq \Gamma \leqq e^{t+1}.$$

Hence

$$F(zX_1) \leqq \max(F(X), F(X_0)) \leqq e^{t+1}, \qquad F(X_1) \leqq e^t,$$

so that X_1 lies in $\mathfrak{m}(t)$. Conversely, if X_1 belongs to $\mathfrak{m}(t)$, then

$$F(X) \leqq \max(F(zX_1), F(X_0)) \leqq e^{t+1}.$$

Now the two vectors X_0 and zX_1, where X_0 and X_1 are lattice points and $|x_0| \leqq 1$, are $\mathfrak{k}$-independent, and the X_0 form a $\mathfrak{k}$-modul of dimension n. Hence

$$M(t+1) = M(t) + n. \tag{19}$$

The two equations (18) and (19) show that for large t, the function $M(t) - M_0(t)$ of t is independent of t. Hence the limit

$$V = \lim_{t \to \infty} e^{M(t) - M_0(t)} \tag{20}$$

exists; it is called the *volume of the convex body* $C(1)$.[10] In particular, if $F(X) = |X|$, then obviously $V = 1$.

8. The invariance of V. Let

$$\Omega = (a_{hk})_{h,k=1,2,\ldots,n} \quad \text{and} \quad \Omega^I = (a^I_{hk})_{h,k=1,2,\ldots,n}$$

be a matrix with elements in $\mathfrak{R}$ and determinant $D \neq 0$, and its inverse matrix. The linear transformation

$$Y = \Omega X \quad \text{or} \quad X = \Omega^I Y$$

changes $F(X)$ into the new distance function

$$F'(Y) = F(X) = F(\Omega^I Y);$$

let $C'(e^t)$ be the corresponding convex body $F'(Y) \leqq e^t$, and V' the volume of $C'(1)$. *Then*

$$V' = |D| V. \tag{21}$$

[10] This definition is analogous to that of the volume of a body by means of lattice points in an ordinary real space.

PROOF: We denote by $\mathfrak{m}'(t)$ the $\mathfrak{k}$-modul of all lattice points in $C'(e^t)$, by $M'(t)$ the dimension of $\mathfrak{m}'(t)$, and prove the statement in a number of steps.

1: The elements of Ω lie in $\mathfrak{T}$, and D belongs to $\mathfrak{k}$.

The formulae $Y = \Omega X$, $X = \Omega^I Y$ establish a (1, 1)-correspondence between the elements X of $\mathfrak{m}(t)$ and Y of $\mathfrak{m}'(t)$. Obviously, this correspondence changes every linear relation

$$\alpha_1 X^{(1)} + \cdots + \alpha_r X^{(r)} = 0$$

with coefficients in $\mathfrak{k}$ into the identical relation in the Y's, and vice versa; therefore $\mathfrak{k}$-independent elements of $\mathfrak{m}(t)$ or $\mathfrak{m}'(t)$ are transformed into $\mathfrak{k}$-independent members of the other modul. Hence both moduls have the same dimension: $M(t) = M'(t)$, q.e.d.

2: Ω is a triangle matrix

$$\Omega = \begin{pmatrix} a_{11} & & & \\ a_{21} & a_{22} & & 0 \\ \vdots & \vdots & \ddots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

with elements in $\mathfrak{T}$ and determinant

$$D = a_{11}a_{22} \cdots a_{nn} \neq 0.$$

The equation $Y = \Omega X$ denotes that

$$\begin{aligned} y_1 &= a_{11}x_1 , \\ y_2 &= a_{21}x_1 + a_{22}x_2 , \\ &\cdots\cdots\cdots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n ; \end{aligned}$$

hence every lattice point Y can be written as[11]

$$Y = \Omega X^* + Y^*,$$

where X^* and Y^* are again lattice points and $Y^* = (y_1^*, \cdots, y_n^*)$ satisfies the inequalities

$$| y_1^* | < | a_{11} |, | y_2^* | < | a_{22} |, \cdots, | y_n^* | < | a_{nn} |.$$

Therefore

$$| Y^* | \leqq c_1 , \text{ i.e. } F'(Y^*) \leqq c_1\Gamma',$$

where c_1 is a positive constant depending only on Ω, and Γ' is the constant in (5) belonging to $F'(Y)$. The set of all vectors Y^* forms a $\mathfrak{k}$-modul $\mathfrak{m}^*$ of dimension d, where

$$e^d = | a_{11} || a_{22} | \cdots | a_{nn} | = | D |.$$

[11] We use the trivial lemma: "*To a and $b = 0$ in $\mathfrak{T}$ there is a q and an r in $\mathfrak{T}$, such that $a = bq + r$ and $| r | < | b |$.*

Let t be so large that

$$e^t \geqq c_1\Gamma'.$$

Then for X^* in $\mathfrak{m}(t)$

$$F'(Y) = F(\Omega^I Y) = F(X^* + \Omega^I Y^*) \leqq \max\,(F(X^*), F'(Y^*)) \leqq e^t,$$

and conversely for Y in $\mathfrak{m}'(t)$

$$F(X^* + \Omega^I Y^*) \leqq e^t, \text{ i.e. } F(X^*) \leqq \max\,(F(X^* + \Omega^I Y^*), F'(Y^*)) \leqq e^t.$$

There is therefore a (1, 1)-correspondence between the elements Y of $\mathfrak{m}'(t)$ and the pairs (X^*, Y^*) of one element X^* of $\mathfrak{m}(t)$ and one element Y^* of $\mathfrak{m}^*$. Hence $M'(t) = M(t) + d$, q.e.d.

3: The elements of Ω belong to $\mathfrak{T}$.

The result follows immediately from the two previous steps, since Ω, as is well known,[12] can be written as $\Omega = \Omega_1\Omega_2$, where the two factors are of the classes 1 and 2.

4: The elements of Ω lie in $\mathfrak{R}$.

Now $\Omega = \Omega_a\Omega_b^I$, where both Ω_a and Ω_b are of the class 3, so that the statement follows at once.

5: Ω has elements in $\mathfrak{R}$, such that

$$|D| = 1, \qquad |a_{hk}| \leqq 1 \qquad (h, k = 1, 2, \cdots, n).$$

Then the same inequalities hold for the inverse matrix Ω^I, so that for every point X

$$|\Omega X| \leqq |X|, \qquad |X| = |\Omega^I \Omega X| \leqq |\Omega X|,$$

and therefore

$$|X| = |\Omega X| = |\Omega^I X|.$$

Now to every lattice point X there is a second lattice point Y such that with a suitable point Y^*

$$\Omega X = Y + Y^*, \qquad |Y^*| < 1;$$

then conversely

$$\Omega^I Y = X + X^*, \qquad |X^*| < 1,$$

and

$$X^* = -\Omega^I Y^*, \qquad \Omega X^* = -Y^*.$$

The relation between X and Y is therefore a (1, 1)-correspondence which obviously leaves invariant the property of $\mathfrak{k}$-independence. Suppose that

$$e^t \geqq \Gamma.$$

[12] This can be proved, e.g. by a method analogous to Minkowki's "adaptation" of a lattice; Geometrie der Zahlen §46.

Then for X in $\mathfrak{m}(t)$

$$F(X^*) < \Gamma \leqq e^t,$$

and therefore

$$F'(Y) = F(\Omega^I Y) = F(X + X^*) \leqq \max\,(F(X), F(X^*)) \leqq e^t,$$

so that Y lies in $\mathfrak{m}'(t)$; conversely, if Y belongs to $\mathfrak{m}'(t)$. then X is an element of $\mathfrak{m}(t)$. Hence $M(t) = M'(t)$, q.e.d.

6: Finally, let Ω have elements in $\mathfrak{R}$. Then it can be split into

$$\Omega = \Omega_4 + \Omega^*$$

where Ω_4 is of the class 4, while the elements of Ω^* lie in $\mathfrak{R}$ and have so small values that

$$\Omega_5 = \Omega_4^I \Omega$$

is of the class 5. Then the result follows at once, since $\Omega = \Omega_4 \Omega_5$.

Two conclusions are immediate from (21). The convex body $C(e^t)$, i.e. $F(z^{-t}X') \leqq 1$, is obtained from $C(1)$ by the transformation $X' = z^t X$; hence it has the volume $V(e^t) = e^{nt}V$. Secondly, *let $G(Y)$ be the polar distance function to $F(X)$, and V' the volume of the convex body $C'(1)$*, i.e. $G(Y) \leqq 1$. *Then V and V' are related by the equation*

$$VV' = 1. \tag{22}$$

For by §5, there is a matrix A with non-vanishing determinant, such that

$$F(X) = |\,\mathrm{A}X\,| \quad \text{and} \quad G(Y) = |\,\mathrm{A}^K Y\,|,$$

hence

$$V = (|\,\mathrm{A}\,|)^{-1} \quad \text{and} \quad V' = (|\,\mathrm{A}^k\,|)^{-1} = |\,\mathrm{A}\,|;$$

the statement is therefore obvious.

9. The minima of $F(X)$. To the distance function $F(X)$, there exist n $\mathfrak{R}$-independent lattice points

$$X^{(k)} = (x_1^{(k)}, \cdots, x_n^{(k)}) \qquad (k = 1, 2, \cdots, n),$$

such that

$F(X^{(1)}) = \sigma^{(1)} = e^{g_1}$ *is the minimum of $F(X)$ in all lattice points $X \neq 0$,*

$F(X^{(2)}) = \sigma^{(2)} = e^{g_2}$ *is the minimum of $F(X)$ in all lattice points X which are $\mathfrak{R}$-independent of $X^{(1)}$*, etc., and finally

$F(X^{(n)}) = \sigma^{(n)} = e^{g_n}$ *is the minimum of $F(X)$ in all lattice points X which are $\mathfrak{R}$-independent of $X^{(1)}, X^{(2)}, \cdots, X^{(n-1)}$.*

The numbers $\sigma^{(1)}, \sigma^{(2)}, \cdots, \sigma^{(n)}$ are called *the n successive minima of $F(X)$*. By this construction, the determinant

$$D = |\,x_h^{(k)}\,|_{h,k=1,2,\cdots,n}$$

lies in $\mathfrak{T}$ and does not vanish; further obviously

$$0 < \sigma^{(1)} \leqq \sigma^{(2)} \leqq \cdots \leqq \sigma^{(n)} \quad \text{and} \quad g_1 \leqq g_2 \leqq \cdots \leqq g_n . \tag{23}$$

We shall prove the two equations

$$|D| = 1, \tag{24}$$

$$\sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)} = \frac{1}{V}; \tag{25}$$

in the second one, V is again the volume of $C(1)$. Thus, in particular, D *is an element of* $\mathfrak{k}$, *and may obviously be taken as equal to* 1.

A: Proof of (24). Every point X in P_n can be written as

$$X = y_1X^{(1)} + \cdots + y_nX^{(n)},$$

where the y's are elements of $\mathfrak{R}$. Then the coordinates x_h of X are linear functions with determinant D of the coordinates y_h of $Y = (y_1, \cdots, y_n)$. We define a new distance function $\Pi(X)$ by

$$\Pi(X) = |Y|.$$

By (21), the convex body $\Pi(X) \leqq 1$ has the volume $|D|$; we determine it in the following way:

If X is a lattice point, then Y also has its coordinates y_h in $\mathfrak{T}$. For since with Y also X is obviously a lattice point, we may assume without loss of generality that

$$\Pi(X) = |Y| < 1, \tag{26}$$

and have to show that no lattice point $X \neq 0$ satisfies this inequality. Let m, where $1 \leqq m \leqq n$, be the greatest index for which $y_m \neq 0$. Then

$$X = \sum_{h=1}^{m} y_hX^{(h)}, \qquad X^{(1)}, \cdots, X^{(m-1)}$$

are $\mathfrak{R}$-independent lattice points, and by (26)

$$F(X) \leqq \max (|y_1|F(X^{(1)}), \cdots, |y_m|F(X^{(m)})) < \sigma^{(m)},$$

in contradiction to the minimum property of $\sigma^{(m)}$.

Hence there are exactly $M_1(t) = n(t + 1)$ $\mathfrak{k}$-independent lattice points such that $\Pi(X) \leqq e^t$, viz. all points corresponding to a basis of $\mathfrak{k}$-independent points Y with $|Y| \leqq e^t$. Therefore

$$|D| = \lim_{t\to\infty} e^{M_1(t)-M_0(t)} = 1, \qquad \text{q.e.d.}$$

B: Proof of (25). Now we use the fact that every point X in P_n can be written as

$$X = y_1z^{-g_1}X^{(1)} + \cdots + y_nz^{-g_n}X^{(n)},$$

where the y's belong to $\mathfrak{R}$. Let $\Sigma(X)$ be the distance function given by

$$\Sigma(X) = |Y|.$$

Since

$$F(z^{-\varrho_h}X^{(h)}) = 1 \qquad (h = 1, 2, \cdots, n),$$

obviously

$$F(X) \leqq 1, \quad \text{if} \quad \Sigma(X) \leqq 1.$$

But the converse is also true: If

$$F(X) \leqq 1, \quad \text{then} \quad \Sigma(X) \leqq 1,$$

and therefore evidently

$$F(X) = \Sigma(X) = |Y|,$$

identically in X.

For suppose that on the contrary for a certain point X in P_n

$$F(X) \leqq 1, \quad \text{but} \quad \Sigma(X) > 1.$$

Then let m with $1 \leqq m \leqq n$ be the greatest index for which $|y_m| > 1$; hence if $m < n$

$$|y_{m+1}| \leqq 1, \cdots, |y_n| \leqq 1.$$

Write

$$y_h = zy_h^* + y_h^{**} \qquad (h = 1, 2, \cdots, n),$$

where the y_h^* are elements of $\mathfrak{T}$, the y_h^{**} elements of $\mathfrak{R}$, and

$$y_m^* \neq 0, \qquad y_{m+1}^* = \cdots = y_n^* = 0, \qquad |y_1^{**}| \leqq 1, \cdots, |y_n^{**}| \leqq 1,$$

and put

$$Y^* = (y_1^*, \cdots, y_n^*), \qquad Y^{**} = (y_1^{**}, \cdots, y_n^{**}),$$

so that

$$Y = zY^* + Y^{**}.$$

Obviously, Y^* is a lattice point, Y^{**} a point such that $|Y^{**}| \leqq 1$. Also write

$$X^* = \sum_{h=1}^{n} y_h^* z^{-\varrho_h} X^{(h)} = \sum_{h=1}^{m} y_h^* z^{-\varrho_h} X^{(h)}, \qquad X^{**} = \sum_{h=1}^{n} y_h^{**} z^{-\varrho_h} X^{(h)},$$

so that

$$X = zX^* + X^{**}.$$

Then from $\Sigma(X^{**}) = |Y^{**}| \leqq 1$,

$$F(X^{**}) \leqq 1.$$

Hence

$$F(zX^*) \leqq \max\,(F(X), F(X^{**})) \leqq 1, \qquad F(X^*) < 1,$$

and

$$F(X^0) < \sigma^{(m)},$$

where $X^0 = z^{\varrho_m} X^*$. This inequality, however, is impossible, since the m lattice points

$$X^0 = \sum_{h=1}^{m} y_h^* z^{\varrho_m - \varrho_h} X^{(h)}, \qquad X^{(1)}, \cdots, X^{(m-1)}$$

are $\mathfrak{R}$-independent, so that by the minimum property of $\sigma^{(m)}$

$$F(X^{(0)}) \geqq \sigma^{(m)}.$$

Therefore (27) is true, so that by the invariance theorem of §8

$$V = \frac{|D|}{\sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)}} = (\sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)})^{-1},$$

since the transformation of X into Y has the determinant

$$Dz^{-(\varrho_1+\varrho_2+\cdots+\varrho_n)}.$$

The equation (25) is therefore proved.

From this equation and from (23) in particular

$$\sigma^{(1)} \leqq V^{-1/n};$$

i.e. *to every distance function* $F(X)$ *there is a lattice point* $X \neq 0$ *such that*

$$F(X) \leqq \frac{1}{\sqrt[n]{V}}.$$

Here equality holds if and only if all minima

$$\sigma^{(1)} = \sigma^{(2)} = \cdots = \sigma^{(n)},$$

thus certainly not, if V is not an integral power of e^n.

10. The relations between the minima of $F(X)$ and $G(Y)$. To the n lattice points $X^{(1)}, X^{(2)}, \cdots, X^{(n)}$ defined in the last paragraph, we construct n points $Y^{(1)}, Y^{(2)}, \cdots, Y^{(n)}$ satisfying

$$X^{(h)} Y^{(n-k+1)} = \begin{cases} 1 & \text{for } h = k, \\ 0 & \text{for } h \neq k; \end{cases} \tag{27}$$

since $|D| = 1$, these points are lattice points. We further define n positive numbers

$$\tau^{(h)} = \frac{1}{\sigma^{(n-h+1)}} = e^{\vartheta_h} \qquad (h = 1, 2, \cdots, n), \tag{28}$$

so that

$$0 < \tau^{(1)} \leqq \tau^{(2)} \leqq \cdots \leqq \tau^{(n)} \quad \text{and} \quad j_1 \leqq j_2 \leqq \cdots \leqq j_n . \tag{29}$$

Then $F(X)$ and the polar function $G(Y)$ can be written as

$$F(X) = \max_{h=1,2,\cdots,n} (\sigma^{(h)} \mid XY^{(n-h+1)} \mid), \tag{30}$$

$$G(Y) = \max_{h=1,2,\cdots,n} (\tau^{(h)} \mid YX^{(n-h+1)} \mid), \tag{31}$$

thus in an entirely symmetrical way. For we proved in the preceding paragraph that if X is written as

$$X = \sum_{h=1}^{n} y_h z^{-g_h} X^{(h)}, \tag{32}$$

then

$$F(X) = \mid Y \mid, \qquad Y = (y_1, y_2, \cdots, y_n).$$

But by multiplying (32) scalar with $Y^{(n)}, \cdots, Y^{(1)}$, we get by (27)

$$y_h = z^{g_h} \cdot (XY^{(n-h+1)}) \qquad (h = 1, 2, \cdots, n)$$

and therefore (30). The formula (31) is a consequence of (30) by the results in §5.[13]

From (27) and (31)

$$G(Y^{(h)}) = \tau^{(h)} = e^{j_h}. \tag{33}$$

We prove now that these numbers $\tau^{(h)}$ in their natural order are the n successive minima of $G(Y)$ in Λ_n. Obviously it suffices to show that *if*

$$Z^{(1)}, Z^{(2)}, \cdots, Z^{(n)}.$$

are any n $\mathfrak{R}$-independent lattice points, such that

$$G(Z^{(1)}) \leqq G(Z^{(2)}) \leqq \cdots \leqq G(Z^{(n)}),$$

---

[13] We can prove (31) directly in the following way: Obviously

$$X = \sum_{h=1}^{n} (XY^{(n-h+1)}) X^{(h)},$$

where the brackets are again the scalar products. Hence from (14)

$$G(Y) = \max (\mid XY \mid) = \max \left(\left| \sum_{h=1}^{n} (XY^{(n-h+1)})(X^{(h)}Y) \right| \right),$$

where the maximum extends over all points X of $C(1)$, i.e. for which

$$\mid XY^{(n-h+1)} \mid \leqq \frac{1}{\sigma^{(h)}} = \tau^{(n-h+1)} \qquad (h = 1, 2, \cdots, n).$$

By choosing X such that there is equality in one of these conditions, but that all other scalar products $XY^{(n-h+1)}$ vanish, the assertion follows after replacing h by $n - h + 1$.

then[14]

$$G(Z^{(h)} \geqq G(Y^{(h)}) = \tau^{(h)}.$$

Consider the $n + 1$ vectors

$$X^{(1)}, X^{(2)}, \cdots, X^{(n-h+1)}, \qquad Z^{(1)}, Z^{(2)}, \cdots, Z^{(h)}.$$

At most n of these are $\mathfrak{R}$-independent; hence the scalar products

$$X^{(i)}Z^{(j)} \qquad \begin{pmatrix} i = 1, 2, \cdots, n - h + 1 \\ j = 1, 2, \cdots, \quad h \end{pmatrix}$$

do not all vanish simultaneously, and at least one of them, say $X^{(i)}Z^{(j)}$, is different from zero. Since it is an element of $\mathfrak{T}$, therefore

$$| X^{(i)}Z^{(j)} | \geqq 1.$$

Now by (17)

$$| XY | \leqq F(X)G(Y),$$

for all points X and Y. Therefore

$$1 \leqq | X^{(i)}Z^{(j)} | \leqq F(X^{(i)})G(Z^{(j)}) \leqq F(X^{(n-h+1)})G(Z^{(h)}) = \frac{1}{\tau^{(h)}} G(Z^{(h)}),$$

as was to be proved.

From (28) and (29) in particular

$$\sigma^{(1)} \leqq \left(\frac{\tau^{(1)}}{V}\right)^{1/n-1} \quad \text{and} \quad \tau^{(1)} \leqq (\sigma^{(1)}V)^{1/n-1}, \tag{34}$$

so that if the minimum of $F(X)$ in $\mathfrak{T}$ is small, then the same is true for that of $G(Y)$, and vice versa.

11. The relation between the homogeneous and the inhomogeneous problem. The reciprocity formulae of the preceding paragraph can be applied to inhomogeneous problems. Let P be an arbitrary point in P_n which is not necessarily a lattice point; it can be written as

$$P = p_1X^{(1)} + \cdots + p_nX^{(n)}$$

where the p's lie in $\mathfrak{R}$. Put

$$p_h = -x_h + r_h \qquad (h = 1, 2, \cdots, n),$$

where x_h is an element of $\mathfrak{T}$ and

$$| r_h | \leqq \frac{1}{e} \qquad (h = 1, 2, \cdots, n).$$

[14] The minima $\sigma^{(h)}$ of $F(X)$ have the analogous property.

Then the lattice point $X = (x_1, \cdots, x_n)$ satisfies the inequality

$$F(P + X) = F\left(\sum_{h=1}^{n} r_h X^{(h)}\right) \leqq \frac{\sigma^{(n)}}{e},$$

or by (28)

$$F(P + X) \leqq \frac{1}{e\tau^{(1)}}. \tag{35}$$

This inequality cannot in general be improved, since

$$F\left(\frac{1}{z} X^{(n)} + X\right) \geqq \frac{1}{e\tau^{(1)}} \tag{36}$$

for all lattice points X, as follows immediately from the $\mathfrak{R}$-independence of the n vectors

$$X^{(1)}, X^{(2)}, \cdots, X^{(n-1)}, X^{(n)} + zX.$$

These two inequalities (35) *and* (36) *relate the inhomogeneous F-problem to the homogeneous G-problem,* in analogy with similar relations in many parts of mathematics.

As an application, consider the two polar distance functions

$$F(X) = \max\left(|\, \alpha_1 x_n - x_1 \,|, \cdots, |\, \alpha_{n-1} x_n - x_{n-1} \,|, e^{-t} |\, x_n \,|\right),$$

$$G(Y) = \max\left(|\, y_1 \,|, \cdots, |\, y_{n-1} \,|, e^{t} |\, \alpha_1 y_1 + \cdots + \alpha_{n-1} y_{n-1} + y_n \,|\right),$$

where t is a positive integer. Assume that the numbers $1, \alpha_1, \cdots, \alpha_{n-1}$ are $\mathfrak{R}$-independent, so that for all lattice points $Y = (y_1, \cdots, y_n) \neq 0$

$$\alpha_1 y_1 + \cdots + \alpha_{n-1} y_{n-1} + y_n \neq 0.$$

Then, as $t \to \infty$, the first minimum $\tau^{(1)}$ of $G(Y)$

$$\tau^{(1)} \to \infty.$$

Hence by (35), *for every* $\epsilon > 0$ *and for every point* $P = (p_1, \cdots, p_n)$ *there is a lattice point* $X = (x_1, \cdots, x_n)$ *satisfying the inequalities*

$$|\, \alpha_1 x_n - x_1 + p_1 \,| < \epsilon, \cdots, |\, \alpha_{n-1} x_n - x_{n-1} + p_{n-1} \,| < \epsilon.$$

Thus we have established a result analogous to *Kronecker's* theorem.

12. A property of matrices. *Let*

$$\Omega = (a_{hk})_{h,k=1,2,\cdots,n}$$

be a matrix in $\mathfrak{R}$ *with determinant* 1; *then there is a matrix*

$$U = (u_{hk})_{h,k=1,2,\cdots,n}$$

with elements in $\mathfrak{T}$ *and determinant* 1, *such that the product matrix*

$$\Omega U = \Omega^* = (a_{hk}^*)_{h,k=1,2,\cdots,n}$$

satisfies the equation

$$\prod_{h=1}^{n} \max_{k=1,2,\cdots,n} (|\, a_{hk}^* \,|) = 1.$$

PROOF:[15] To the convex body $C(1)$ belonging to the distance function

$$F(X) = \max_{h=1,2,\cdots,n} \left(\left| \sum_{k=1}^{n} a_{hk} x_k \right| \right),$$

there are n lattice points $X^{(1)}, X^{(2)}, \cdots, X^{(n)}$ of determinant $D = 1$, such that the n minima

$$F(X^{(h)}) = \sigma^{(h)} \qquad (h = 1, 2, \cdots, n)$$

satisfy

$$0 < \sigma^{(1)} \leqq \sigma^{(2)} \leqq \cdots \leqq \sigma^{(n)}, \qquad \sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)} = 1.$$

Let $X^{(k)} = (x_1^{(k)}, \cdots, x_n^{(k)})$, and X be the matrix

$$\mathrm{X} = (x_h^{(k)})_{h,k=1,2,\cdots,n}$$

with elements in $\mathfrak{T}$ and determinant 1. We introduce new coordinates $y_1, \cdots, y_n$ by putting

$$X = y_1 X^{(1)} + \cdots + y_n X^{(n)}, \text{ i.e., } x_h = \sum_{k=1}^{n} x_h^{(k)} x_k \qquad (h = 1, 2, \cdots, n);$$

then $F(X)$ changes into

$$F(X) = F'(Y) = \max_{h=1,2,\cdots,n} \left(\left| \sum_{k=1}^{n} a'_{hk} y_k \right| \right),$$

where

$$\Omega' = (a'_{hk})_{h,k=1,2,\cdots,n} = \Omega \mathrm{X}.$$

The n points $X = X^{(h)}$ are transformed into $Y = E^{(h)}$ $(h = 1, 2, \cdots, n)$; hence

$$F'(E^{(h)}) = \sigma^{(h)} \qquad (h = 1, 2, \cdots, n),$$

that is

$$\max_{h=1,2,\cdots,n} (|\, a'_{hk} \,|) = \sigma^{(k)} \qquad (k = 1, 2, \cdots, n). \tag{37}$$

[15] An analogous theorem in the real field was proved some time ago by C. L. Siegel in a letter to L. J. Mordell. The present proof and theorem, though not stated in Siegel's paper, are obtained from it with only slight changes by making use of the results in §9.

Hence every minor Δ_m of order m formed from the m first columns and m arbitrary rows of Ω' satisfies the inequality

$$|\Delta| \leqq \sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(m)}. \tag{38}$$

On the other hand, any determinant Δ of order m can be written as

$$\Delta = \sum_{h=1}^{n} a_h \delta_h,$$

where the a_h are the elements of its last column, and the δ_h their cofactors; therefore

$$\max_{h=1,2,\cdots,n} (|\delta_h|) \geqq |\Delta| \{ \max_{h=1,2,\cdots,n} (|a_h|) \}^{-1}.$$

We apply this inequality repeatedly to the determinant

$$\Delta_n = 1 = \sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n)}$$

of Ω' and use (37) and (38); then it follows that *there exists*

an $(n-1)^{\text{th}}$ *order minor* Δ_{n-1} *of* Δ_n *formed from the* $n-1$ *first columns of* Ω' *and satisfying*

$$|\Delta_{n-1}| = \sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n-1)};$$

an $(n-2)^{\text{th}}$ *order minor* Δ_{n-2} *of* Δ_{n-1} *formed from the* $n-2$ *first columns of* Ω' *and satisfying*

$$|\Delta_{n-2}| = \sigma^{(1)}\sigma^{(2)} \cdots \sigma^{(n-2)};$$

etc.; *a second order minor* Δ_2 *of* Δ_3 *formed from the two first columns of* Ω' *and satisfying*

$$|\Delta_2| = \sigma^{(1)}\sigma^{(2)};$$

and finally an element Δ_1 *of* Δ_2 *lying in the first column of* Ω' *and satisfying*

$$|\Delta_1| = \sigma^{(1)}.$$

Without loss of generality, we may assume that the determinants so constructed are exactly the principle determinants

$$\Delta_r = |a'_{hk}|_{h,k=1,2,\cdots,r} \qquad (r = 1, 2, \cdots, n).$$

We shall now construct a set of matrices of order n

$$U_m = \begin{pmatrix} 1 & 0 & \cdots & 0 & g_1^{(m)} & 0 & \cdots & 0 \\ & 1 & \cdots & 0 & g_2^{(m)} & 0 & \cdots & 0 \\ & & \ddots & \vdots & \vdots & \vdots & & \vdots \\ & & & 1 & g_{m-1}^{(m)} & 0 & \cdots & 0 \\ & & & & 1 & 0 & \cdots & 0 \\ & O & & & & 1 & \cdots & 0 \\ & & & & & & \ddots & \vdots \\ & & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \} m \text{ rows} \\ \\ \\ \} n - m \text{ rows} \end{matrix} \qquad (m = 1, 2, \cdots, n),$$

where the g's lie in $\mathfrak{T}$, and U_1 is the unit matrix. If

$$\Omega_m = \Omega' U_1 U_2 \cdots U_m = (a_{hk}^{(m)})_{h,k=1,2,\cdots,m} \qquad (m = 1, 2, \cdots, n),$$

then $\Omega_1 = \Omega'$, and for $h, k = 1, 2, \cdots, n$

$$a_{hk}^{(m)} = a_{hk}^{(m-1)} \text{ if } k \neq m, \text{ and } a_{hm}^{(m)} = g_1^{(m)} a_{h1}^{(m-1)} + \cdots + g_{m-1}^{(m)} a_{hm-1}^{(m-1)} + a_{hm}^{(m-1)}.$$

The n principal determinants of Ω_m :

$$\Delta_r = |\, a_{hk}^{(m)} \,|_{h,k=1,2,\cdots,r} \qquad (r = 1, 2, \cdots, n)$$

are therefore equal to the corresponding ones of Ω_{m-1} and so of Ω'.

By construction, the elements of Ω_1 satisfy the inequalities

$$|\, a_{hk}^{(1)} \,| \leqq \sigma^{(k)} \qquad (h, k = 1, 2, \cdots, n),$$

and therefore also the inequalities

$$|\, a_{h1}^{(1)} \,| \leqq \sigma^{(h)} \qquad (h = 1, 2, \cdots, n).$$

Assume now that $U_1, \cdots, U_{m-1}$ were determined such that

$$(39) \qquad \begin{aligned} &|\, a_{hk}^{(m-1)} \,| \leqq \sigma^{(k)} && (h, k = 1, 2, \cdots, n); \\ &|\, a_{hk}^{(m-1)} \,| \leqq \sigma^{(h)} && \text{for } h = 1, 2, \cdots, n;\ k = 1, 2, \cdots, m-1. \end{aligned}$$

Then U_m, as we shall prove now, can be constructed such that Ω_m satisfies the stronger inequalities

$$(40) \qquad \begin{aligned} &|\, a_{hk}^{(m)} \,| \leqq \sigma^{(k)} && (h, k = 1, 2, \cdots, n); \\ &|\, a_{hk}^{(m)} \,| \leqq \sigma^{(h)} && \text{for } h = 1, 2, \cdots, n;\ k = 1, 2, \cdots, m. \end{aligned}$$

To this purpose put

$$a_{h1}^{(m-1)} \gamma_1 + \cdots + a_{hm-1}^{(m-1)} \gamma_{m-1} + a_{hm}^{(m-1)} = t_h(\gamma_1, \cdots, \gamma_{m-1}) = t_h \quad (h = 1, 2, \cdots, n),$$

and determine elements $\gamma_1, \gamma_2, \cdots, \gamma_{m-1}$ of $\mathfrak{R}$ such that

$$t_1 = t_2 = \cdots = t_{m-1} = 0.$$

This system of linear equations has the determinant Δ_{m-1}. On solving,

$$\Delta_{m-1} \gamma_r = \mp \Delta_{m-1,r} \qquad (r = 1, 2, \cdots, m-1),$$

where $\Delta_{m-1,r}$ is the $(m-1)^{\text{th}}$ order minor of Δ_m obtained by omitting the m^{th} row and the r^{th} column. Hence from (37),

$$|\, \gamma_r \,| = \left| \frac{\Delta_{m-1,r}}{\Delta_{m-1}} \right| \leqq \frac{\sigma^{(1)} \cdots \sigma^{(m)}}{\sigma^{(r)}} : (\sigma^{(1)} \cdots \sigma^{(m-1)}) = \frac{\sigma^{(m)}}{\sigma^{(r)}} \geqq 1.$$

Let the element $g_r^{(m)}$ of U_m now be the number in $\mathfrak{T}$ satisfying the inequality

$$|\, g_r^{(m)} - \gamma_r \,| < 1 \qquad (r = 1, 2, \cdots, m-1),$$

so that

$$| g_r^{(m)} | = \frac{\sigma^{(m)}}{\sigma^{(r)}}.$$

Then from the first system of inequalities (39) for $h = 1, 2, \cdots, n$

$$| a_{hm}^{(m)} | = | t_h(g_1^{(m)}, \cdots, g_{m-1}^{(m)}) | = | g_1^{(m)} a_{h1}^{(m-1)} + \cdots + g_{m-1}^{(m)} a_{hm-1}^{(m-1)} + a_{hm}^{(m-1)} |$$
$$\leqq \max\left(\frac{\sigma^{(m)}}{\sigma^{(1)}} \cdot \sigma^{(1)}, \cdots, \frac{\sigma^{(m)}}{\sigma^{(m-1)}} \cdot \sigma^{(m-1)}, \sigma^{(m)}\right) = \sigma^{(m)},$$

and from the second system for $h = 1, 2, \cdots, m$

$$| a_{hm}^{(m)} | = | t_h(g_1^{(m)}, \cdots, g_{m-1}^{(m)}) |$$
$$= | (g_1^{(m)} - \gamma_1) a_{h1}^{(m-1)} + \cdots + (g_{m-1}^{(m)} - \gamma_{m-1}) a_{hm-1}^{(m-1)} | < 1 \cdot \sigma^{(h)} = \sigma^{(h)}.$$

Since the remaining inequalities (40) are contained in (39), the matrix U_m has the required property. Hence if

$$U = XU_1U_2 \cdots U_n,$$

then this matrix satisfies the statement of our theorem.

13. A property of the product of n inhomogeneous linear polynomials in n variables. Let $\Omega = (a_{hk})_{h,k=1,2,\cdots,n}$ be again a matrix with elements in $\mathfrak{R}$ of determinant 1. We form the distance function

ce
$$F(X \mid f) = \max_{h=1,2,\cdots,n} (e^{f_h} \mid a_{h1}x_1 + a_{h2}x_2 + \cdots + a_{hn}x_n \mid),$$

where $f_1, f_2, \cdots, f_n$ are n integers such that $f_1 + \cdots + f_n = 0$. By the theorem of last paragraph, there is a matrix U with elements in $\mathfrak{T}$ and determinant 1, such that the product matrix

$$\Omega^* = \Omega U = (a_{hk}^*)$$

satisfies the equation

$$\prod_{h=1}^{n} \max_{k=1,2,\cdots,n} (| a_{hk}^* |) = 1.$$

Let us choose the integers f_h^0 such that

$$e^{-f_h^0} = \max_{k=1,2,\cdots,n} (| a_{hk}^* |) \qquad (h = 1, 2, \cdots, n) \tag{41}$$

and put

$$a_{hk}^{**} = z^{f_h^0} a_{hk}^* \qquad (h, k = 1, 2, \cdots, n).$$

Then by the transformation $X = UY$, $F(X) \mid f^0)$ changes into a new distance function

$$F(X \mid f^0) = F'(Y) = \max_{h=1,2,\cdots,n} (| a_{h1}^{**} y_1 + \cdots + a_{hn}^{**} y_n |),$$

where now all coefficients a_{hk}^{**} satisfy the inequalities $|a_{hk}| \leqq 1$, and their determinant is still 1. Obviously, for all n $\mathfrak{R}$-independent vectors $Y^{(1)} = E^{(1)}$, $Y^{(2)} = E^{(2)}, \cdots, Y^{(n)} = E^{(n)}$, the value of this function

$$F'(Y^{(h)}) \leqq 1 \qquad (h = 1, 2, \cdots, n).$$

Therefore by the equation (25), necessarily

$$F'(Y^{(1)}) = F'(Y^{(2)}) = \cdots = F'(Y^{(n)}) = 1,$$

and so all minima of $F(X \mid f^0)$, where the f^0's are given by (41), have the same value 1, and in particular, the first minimum of $F(X \mid f^0)$ has the exact value $\frac{1}{\sqrt[n]{V}}$, where $V = 1$ is the volume of $F(X \mid f^0) \leqq 1$.

As an application, let $a_1, a_2, \cdots, a_n$ be any n elements of $\mathfrak{R}$, and $\eta_1, \eta_2, \cdots, \eta_n$ n elements of $\mathfrak{R}$ satisfying the equations

$$a_{h1}^{*}\eta_1 + \cdots + a_{hn}^{*}\eta_h + a_h = 0 \qquad (h = 1, 2, \cdots, n).$$

If $y_1, y_2, \cdots, y_n$ are the elements of $\mathfrak{T}$ for which

$$|y_h - \eta_h| \leqq \frac{1}{e} \qquad (h = 1, 2, \cdots, n),$$

then obviously

$$|a_{h1}^{*}y_1 + \cdots + a_{hn}^{*}y_n + a_h| \leqq e^{-f_h^0-1} \quad (h = 1, 2, \cdots, n).$$

Hence the lattice point $X = (x_1, x_2, \cdots, x_n) = U^I Y$ *satisfies the inequalities*

$$|a_{h1}x_1 + \cdots + a_{hn}x_n + a_h| \leqq e^{-f_h^0-1} \quad (h = 1, 2, \cdots, n),$$

and therefore the inequality

$$\prod_{h=1}^{n} |a_{h1}x_1 + \cdots + a_{hn}x_n + a_h| \leqq e^{-n}.$$

Here the constant e^{-n} on the right-hand side is the best possible, as is clear if, e.g. Ω is the unit matrix and all $a_h = 1/z$.

14. Distance functions in $\mathfrak{R}_\mathfrak{p}$. The field $\mathfrak{R}$ of all rational functions with coefficients in $\mathfrak{k}$ has valuations different from the "infinite" valuation $|x|$, which expresses the behavior of x at the point $z = \infty$.

Let ζ be any element of $\mathfrak{k}$, and $\mathfrak{p}$ the "finite" point $z = \zeta$. Then we define a valuation $|x|_\mathfrak{p}$ by putting for $x \neq 0$

$$|x|_\mathfrak{p} = e^{-f_\mathfrak{p}},$$

where $f_\mathfrak{p}$ is that integer, for which neither the numerator nor the denominator of the simplified fraction $(z - \zeta)^{-f_\mathfrak{p}}x$ are divisible by $z - \zeta$; we denote by $\mathfrak{R}_\mathfrak{p}$

the perfect extension of $\mathfrak{R}$ with respect to this valuation; it consists of all formal Laurent series

$$x = \alpha_f(z - \zeta)^f + \alpha_{f+1}(z - \zeta)^{f+1} + \alpha_{f+2}(z - \zeta)^{f+2} + \cdots$$

with coefficients in $\mathfrak{k}$, and if $\alpha_f \neq 0$, then $| x |_\mathfrak{p} = e^{-f}$.

Let now $F(X)$ be any special distance function of $\mathfrak{R}$; we use it as the measure for the size of X. Further let $F(X \mid \mathfrak{p})$ be a general distance function of $\mathfrak{R}_f$. Since

$$F((z - \zeta)^f X \mid \mathfrak{p}) = e^{-f} F(X \mid \mathfrak{p}),$$

this distance function may assume arbitrarily small values, if X lies in the modul Λ_n of all lattice points. By (5), there is a constant $\Gamma_\mathfrak{p} > 0$ such that

$$F(X \mid \mathfrak{p}) \leqq \Gamma_\mathfrak{p} \mid X \mid_\mathfrak{p};$$

here for $X = (x_1, \cdots, x_n)$

$$| X |_\mathfrak{p} = \max (| x_1 |_\mathfrak{p}, \cdots, | x_n |_\mathfrak{p}).$$

Hence

$$F(X \mid \mathfrak{p}) \leqq \Gamma_\mathfrak{p} \text{ for all lattice points } X.$$

Let t be an integer such that

$$e^{-t} \leqq \Gamma_\mathfrak{p}, \quad \text{i.e.} \quad t \geqq \log\left(\frac{1}{\Gamma_\mathfrak{p}}\right),$$

and $C(e^{-t} \mid \mathfrak{p})$ the convex set of all points X in P_n for which

$$F(X \mid \mathfrak{p}) \leqq e^{-t}.$$

Then the set $\mathfrak{m}(-t \mid \mathfrak{p})$ of all lattice points in $C(e^{-t} \mid \mathfrak{p})$ contains with X and Y also $aX + bY$, when a and b lie in $\mathfrak{T}$; it is therefore an $\mathfrak{T}$-modul. By the general theory of polynomial ideals,[16] this modul has a basis of n lattice points

$$P^{(k)} = (p_1^{(k)}, \cdots, p_n^{(k)}) \qquad (k = 1, 2, \cdots, n),$$

such that every point X in Λ_n belongs to $\mathfrak{m}(-t \mid \mathfrak{p})$, if and only it can be written as

$$X = y_1 P^{(1)} + \cdots + y_n P^{(n)} \quad \text{with } y_1, \cdots, y_n \text{ in } \mathfrak{T}.$$

The determinant

$$D(-t) = | p_h^{(k)} |_{h,k=1,2,\cdots,n} \neq 0,$$

and therefore the number

$$\Delta(-t) = | D(-t) |$$

is positive.

---

[16] Compare the basis theorem in §80 of van der Waerden's "Moderne Algebra", Vol. II, 1st ed.

The function $F(X)$ changes into a new distance function

$$F'(Y) = F(X) = F(\Omega Y), \qquad \Omega = (p_h^{(k)})_{h,k=1,2,\cdots,n}$$

by the transformation (42). The convex body $F'(Y) \leqq 1$ has the volume

$$V' = \Delta(-t)^{-1}V,$$

where V denotes the volume of $F(X) \leqq 1$. By the results in §9, there are n lattice points $Y^{(1)}, \cdots, Y^{(n)}$ with determinant 1, such that

$$F'(Y^{(1)}) \cdots F(Y^{(n)}) = \frac{\Delta(-t)}{V}.$$

The transformed lattice points $X^{(1)}, \cdots, X^{(n)}$ given by

$$X^{(k)} = \Omega Y^{(k)} = (x_1^{(k)}, \cdots, x_n^{(k)}) \qquad (k = 1, 2, \cdots, n)$$

have the determinant

$$D(-t) = |\, x_h^{(k)} \,|_{h,k=1,2,\cdots,n},$$

and satisfy the relations

$$F(X^{(1)}) \cdots F(X^{(n)}) = \frac{\Delta(-t)}{V}, \qquad F(X^{(k)} \mid \mathfrak{p}) \leqq e^{-t} \qquad (k = 1, 2, \cdots, n).$$

It is not difficult to prove that for large t

$$\Delta(-t) = O(e^{nt}), \qquad |\, D(-t) \,|_{\mathfrak{p}} = O(e^{-t}).$$

In the following case, sharper results are obtained. Let

$$F(X \mid \mathfrak{p}) = \max_{h=1,2,\cdots,m} (|\, a_{h1}x_1 + \cdots + a_{hn-m}x_{n-m} + x_{n-m+h} \,|_{\mathfrak{p}}),$$

where the a's are elements in $\mathfrak{R}_{\mathfrak{p}}$ such that

$$|\, a_{hk} \,|_{\mathfrak{p}} \leqq 1 \qquad \begin{pmatrix} h = 1, 2, \cdots, m \\ k = 1, 2, \cdots, n \end{pmatrix}.$$

Then to every positive integer t there are elements A_{hk} in $\mathfrak{T}$ satisfying

$$|\, a_{hk} - A_{hk} \,|_{\mathfrak{p}} \leqq e^{-t} \qquad \begin{pmatrix} h = 1, 2, \cdots, m \\ k = 1, 2, \cdots, n \end{pmatrix}.$$

Hence, if $y_1, \cdots, y_n$ belong to $\mathfrak{T}$, and $x_1, \cdots, x_n$ are defined by

$$x_1 = y_1, \cdots, x_{n-m} = y_{n-m};$$

$$x_{n-m+h} = (z - \zeta)^t y_{n-m+h} - (A_{h1}y_1 + \cdots + A_{hn-m}y_{n-m}), \qquad (h = 1, 2, \cdots, m), \tag{42}$$

then $F(X \mid \mathfrak{p}) \leqq e^{-t}$. Let $F'(Y) = F(X)$ be the special distance function in $\mathfrak{R}$ derived from $F(X)$ by the transformation (42). Then $F'(Y) \leqq 1$ has the

volume $|(z-\zeta)^{-mt}|V = e^{-mt}V$. Hence there are n $\mathfrak{R}$-independent lattice points $Y^{(1)}, \cdots, Y^{(n)}$ of determinant 1 such that

$$F'(Y^{(1)}) \cdots F'Y^{(n)}) = \frac{e^{mt}}{V}.$$

The n lattice points $X^{(1)}, \cdots, X^{(n)}$ derived from these by (42) have the determinant $(z-\zeta)^{mt}$ and satisfy the conditions

$$F(X^{(1)}) \cdots F(X^{(n)}) = \frac{e^{mt}}{V}, \qquad F(X^{(k)}|\mathfrak{p}) \leqq e^{-t} \qquad (k = 1, 2, \cdots, n).$$

MANCHESTER, ENGLAND.