A LECTURE ON THE GEOMETRY OF NUMBERS OF CONVEX BODIES

BY

KURT MAHLER

Reprinted from the
BULLETIN OF THE AMERICAN MATHEMATICAL SOCIETY
May, 1971, Vol. 77, No. 3
Pp. 319-325

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 77, Number 3, May 1971

A LECTURE ON THE GEOMETRY OF NUMBERS OF CONVEX BODIES

BY KURT MAHLER

Before I can explain the subject of my talk, let me introduce the notation to be used: R^n denotes the n-dimensional space of all points, $\mathbf{x}=(x_1, \cdots, x_n)$, $\mathbf{y}=(y_1, \cdots, y_n)$, $\mathbf{0}=(0, \cdots, 0)$, etc., with real coordinates, $\mathbf{0}$ being called the *origin*. Such points will be treated as vectors, and we put

$$\mathbf{x}+\mathbf{y}=(x_1+y_1, \cdots, x_n+y_n), \qquad C\mathbf{x}=(Cx_1, \cdots, Cx_n)$$

where C is any real number. We also use the inner product

$$\mathbf{xy}=x_1y_1+\cdots+x_ny_n$$

of two points and the determinant

$$(\mathbf{x}^{(1)}, \cdots, \mathbf{x}^{(n)})=\begin{vmatrix} x_{11} & \cdots & x_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ x_{n1} & \cdots & x_{nn} \end{vmatrix}$$

of n points

$$\mathbf{x}^{(h)}=(x_{h1}, \cdots, x_{hn}) \qquad (h=1, 2, \cdots, n).$$

This determinant is $\neq 0$ if and only if the n points are linearly independent over R. Points with integral coordinates are called *lattice points*, and we use Λ to denote the lattice of all such lattice points. Λ is an Abelian group with n independent generators under addition. Every bounded set contains at most finitely many lattice points.

We shall be concerned with the relation between Λ and convex bodies. Here a convex body K is to mean a bounded closed convex set in R^n which contains the origin as an interior point and is symmetric in $\mathbf{0}$. Important examples are the "cube" $|x_1| \leqq 1, \cdots, |x_n| \leqq 1$, the "octahedron" $|x_1|+\cdots+|x_n| \leqq 1$, and the "sphere" $x_1^2+\cdots+x_n^2 \leqq 1$. The volume of a convex body K is defined by

---

An invited address delivered to the 674th meeting of the Society in Madison, Wisconsin on April 17, 1970.

AMS 1969 *subject classifications*. Primary 5230, 1025.

Key words and phrases. Convex bodies, lattices, successive minima, polar convex bodies, compound convex bodies, transfer theorems.

$$V(K) = \int_K \cdots \int dx_1 \cdots dx_n,$$

an integral which always exists. To every convex body there exists a unique convex distance function

$$F(\mathbf{x}) = F(x_1, \cdots, x_n)$$

with the following properties:

(1) $F(\mathbf{0}) = 0$, $F(x) > 0$ if $\mathbf{x} \neq \mathbf{0}$.

(2) $F(t\mathbf{x}) = |t| F(\mathbf{x})$ for all points $\mathbf{x}$ and all real t.

(3) $F(\mathbf{x}+\mathbf{y}) \leqq F(\mathbf{x}) + F(\mathbf{y})$.

(4) K consists exactly of all points $\mathbf{x}$ satisfying $F(\mathbf{x}) \leqq 1$.

We can further associate with K a tac-function

$$G(\mathbf{y}) = G(y_1, \cdots, y_n)$$

which has the properties (1), (2), (3), but for which (4) is replaced by the following property:

(4*) K consist exactly of all points $\mathbf{x}$ with the property $|\mathbf{xy}| \leqq G(\mathbf{y})$ for all points $\mathbf{y}$.

We can form the second convex body K^* consisting of all points $\mathbf{y}$ for which $G(\mathbf{y}) \leqq 1$. This body has the distance function $G(\mathbf{y})$, and the tac-function $F(\mathbf{x})$. Thus the relation between K and K^* is symmetrical. If $F(\mathbf{x})$ is given, $G(\mathbf{y})$ can be formed from

$$G(\mathbf{y}) = \sup_{\mathbf{x} \neq \mathbf{0}} \frac{|\mathbf{xy}|}{F(\mathbf{x})} = \sup_{F(\mathbf{x})=1} |\mathbf{xy}|,$$

and an analogous formula gives $F(\mathbf{x})$ again in terms of $G(\mathbf{y})$.

Let now $K: F(\mathbf{x}) \leqq 1$ be an arbitrary convex body, of volume $V(K)$. The geometry of numbers began with Minkowski's discovery of the following theorem.

THEOREM 1. *If $V(K) \geqq 2^n$, then K contains at least one lattice point $\neq \mathbf{0}$.*

The power of this theorem was shown by Minkowski in its many applications, in particular to the theory of algebraic number fields. By means of Theorem 1, Minkowski was the first to prove that every finite number field distinct from the rational field $\mathcal{Q}$ has a discriminant $\neq \mp 1$. Since his time, many other applications of Theorem 1 have been made.

However, Theorem 1 is not Minkowski's main theorem. In an amazing chapter of his *Geometry der Zahlen*, he established a much deeper and more powerful result of which Theorem 1 is an immediate

consequence. This result depends on the following construction of the *successive minima*. There evidently exists a lattice point $\mathbf{x}^{(1)} \neq 0$ for which

$$F(\mathbf{x}^{(1)}) = m_1, \quad \text{say},$$

is a minimum. For every convex body $F(x) \leqq C$ is bounded and therefore contains at most finitely many lattice points. There next, for the same reason, exists a lattice point $\mathbf{x}^{(2)}$ linearly independent of $\mathbf{x}^{(1)}$ such that

$$F(\mathbf{x}^{(2)}) = m_2, \quad \text{say},$$

is a minimum. Generally, if $k = 2, 3, \cdots, n$, and if $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \cdots, \mathbf{x}^{(k-1)}$ and $m_1, m_2, \cdots, m_{k-1}$ have already been defined, there evidently exists a lattice point $\mathbf{x}^{(k)}$ linearly independent of $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \cdots, \mathbf{x}^{(k-1)}$ such that also

$$F(\mathbf{x}^{(k)}) = m_k, \quad \text{say},$$

is a minimum.

By this construction, we obtain n linearly independent lattice points

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

and n positive numbers

$$F(\mathbf{x}^{(k)}) = m_k \qquad (k = 1, 2, \cdots, n)$$

which are easily seen to satisfy $0 < m_1 \leqq m_2 \leqq \cdots \leqq m_n$ and are called the *successive minima* of $F(\mathbf{x})$ or of K. Although the lattice points $\mathbf{x}^{(k)}$ can always be chosen in more than one way, the minima m_k are uniquely determined. In fact, let $\boldsymbol{X}^{(1)}, \cdots, \boldsymbol{X}^{(n)}$ be any n independent lattice points in R^n arranged such that

$$F(\boldsymbol{X}^{(1)}) \leqq F(\boldsymbol{X}^{(2)}) \leqq \cdots \leqq F(\boldsymbol{X}^{(n)}).$$

Then it can be shown that

$$m_k \equiv F(\mathbf{x}^{(k)}) \leqq F(\boldsymbol{X}^{(n)}) \qquad (k = 1, 2, \cdots, n)$$

a result due to Minkowski.

Minkowski's main theorem is now as follows.

THEOREM 2. $2^n/n! \leqq V(K)m_1m_2 \cdots m_n \leqq 2^n$.

By way of example, if $V(K) \geqq 2^n$, then $m_1 \leqq 1$, and so the lattice point $\mathbf{x}^{(1)}$ constructed above lies in $K: F(x) \leqq 1$. This is Theorem 1.

Minkowski himself applied Theorem 2 only to the study of the

approximation of algebraic numbers. However, Theorem 2 allows many other applications obtained in more recent years. By way of example, let me mention just one such application.

Every algebraic number field of finite degree, n say, over $\mathbb{Q}$ and of discriminant Δ, has an integral basis $\omega_1, \cdots, \omega_n$, such that

$$\max_{h,k=1,2,\cdots,n} |\omega_h^{(k)}| \leqq C_n |\Delta|^{1/2},$$

where $\omega_h^{(k)}$ are the conjugates of ω_h, and $C_n > 0$ depends only on n and is not large for small values of n, say for $n \leqq 5$.

One application of Theorem 2 concerns inhomogeneous problems. Let $\mathfrak{x}^{(1)}, \cdots, \mathfrak{x}^{(n)}$ be again n independent lattice points at which the successive minima $m_1, \cdots, m_n$ are attained, and let $\mathfrak{x}$ be an arbitrary point in R^n. There exist then real numbers $t_1, \cdots, t_n$ such that

$$\mathfrak{x} = t_1\mathfrak{x}^{(1)} + \cdots + t_n\mathfrak{x}^{(n)}$$

and integers $g_1, \cdots, g_n$ such that

$$|t_k - g_k| \leqq \tfrac{1}{2} \qquad (k = 1, 2, \cdots, n).$$

On putting

$$\mathfrak{x}^{(0)} = g_1\mathfrak{x}^{(1)} + \cdots + g_n\mathfrak{x}^{(n)},$$

$\mathfrak{x}^{(0)}$ is a lattice point,

$$\mathfrak{x} - \mathfrak{x}^{(0)} = (t_1 - g_1)\mathfrak{x}^{(1)} + \cdots + (t_n - g_n)\mathfrak{x}^{(n)},$$

and therefore

$$F(\mathfrak{x} - \mathfrak{x}^{(0)}) \leqq \tfrac{1}{2}F(\mathfrak{x}^{(1)}) + \cdots + \tfrac{1}{2}F(\mathfrak{x}^{(n)}) \leqq \frac{m_1 + \cdots + m_n}{2} \leqq \frac{n}{2} m_n.$$

On the other hand, the lattice point

$$2(\tfrac{1}{2}\mathfrak{x}^{(n)} - \mathfrak{x}^{(0)}) = -2g_1\mathfrak{x}^{(1)} - \cdots - 2g_{n-1}\mathfrak{x}^{(n-1)} + (1 - 2g_n)\mathfrak{x}^{(n)}$$

is for all choices of the integers $g_1, \cdots, g_n$ linearly independent of $\mathfrak{x}^{(1)}, \cdots, \mathfrak{x}^{(n-1)}$, and hence $F(2(\tfrac{1}{2}\mathfrak{x}^{(n)} - \mathfrak{x}^{(0)})) \geqq m_n$, $F(\tfrac{1}{2}\mathfrak{x}^{(n)} - \mathfrak{x}^{(0)}) \geqq m_n/2$. Thus for every point $\mathfrak{x}$ there is a lattice point $\mathfrak{x}^{(0)}$ such that

$$F(\mathfrak{x} - \mathfrak{x}^{(0)}) \leqq \frac{n}{2} m_n,$$

while for $\mathfrak{x} = \tfrac{1}{2}\mathfrak{x}^{(n)}$ the value of $F(\mathfrak{x} - \mathfrak{x}^{(0)})$ cannot be less than $\tfrac{1}{2}m_n$. Thus the nth successive minimum m_n gives us, up to constant factors, a measure for the distance of any point to the nearest lattice

point. Also

$$V(K)m_1^{n-1}m_n \leqq V(K)m_1m_2 \cdots m_n \leqq 2^n$$

and therefore

$$m_n \leqq \frac{2^n}{V(K)m_1^{n-1}}.$$

Thus the inhomogeneous problem has a good solution if the homogeneous problem has only bad ones, i.e., if m_1 is not too small.

What I have said so far was all known to Minkowski or implied in his work. Many more properties have become established since his time, and I shall discuss some of these. They are of the form of *transfer theorems*, i.e., they deal with connections between the successive minima of several convex bodies.

The simplest such theorem concerns the successive minima

$$m_k = F(\mathbf{x}^{(k)}) \quad \text{and} \quad m_k^* = G(\mathbf{y}^{(k)})$$

of a convex body K and the reciprocal body K^* as defined earlier. By Theorem 2,

$$(*)\quad \frac{2^n}{n!} \leqq V(K)m_1 \cdots m_n \leqq 2^n \text{ and also } \frac{2^n}{n!} \leqq V(K^*)m_1^* \cdots m_n^* \leqq 2^n.$$

It is not difficult to prove that

$$(*)\quad \frac{4^n}{(n!)^2} \leqq V(K)V(K^*) \leqq 4^n.$$

If further $\mathbf{x}$ and $\mathbf{y}$ are any two lattice points such that the inner product $\mathbf{x}\cdot\mathbf{y} \neq 0$ and therefore $|\mathbf{x}\cdot\mathbf{y}| \geqq 1$, then from the definition of $G(\mathbf{y})$,

$$(*)\quad F(\mathbf{x})G(\mathbf{y}) \geqq |\mathbf{x}\mathbf{y}| \geqq 1.$$

In particular, for every k not all products

(*) $\mathbf{x}^{(i)}\mathbf{y}^{(j)}$, where $i = 1, 2, \cdots, k; j = 1, 2, \cdots, n+1-k$, vanish simultaneously.

On combining the properties (*), we obtain now easily the law:

THEOREM 3. $1 \leqq m_k m_{n-k+1}^* \leqq (n!)^2$ $(k = 1, 2, \cdots, n)$.

This reciprocity theorem has many applications in Diophantine analysis of both real and p-adic numbers.

There are many other such transfer theorems. For reasons of time

I shall quote only two more closely connected ones which are special cases of a more general result.

If $2 \leqq p \leqq n-1$, and $\mathfrak{x}^{(h)} = (x_{hp}, \cdots, x_{hn})$ $(h = 1, 2, \cdots, p)$ are any p points in K, we can form the matrix

$$\begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ x_{p1} & \cdots & x_{pn} \end{bmatrix}$$

and all its $p \times p$ minors

$$\begin{vmatrix} x_{1i_1} & \cdots & x_{1i_p} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ x_{pi_1} & \cdots & x_{pi_p} \end{vmatrix} \quad \text{where } 1 \leqq i_1 < i_2 < \cdots < i_p \leqq n.$$

Denote by N the number of these minors, and by $\xi_1, \cdots, \xi_N$ these minors arranged, say lexicographically. We can then associate with the set of p points $\mathfrak{x}^{(1)}, \cdots, \mathfrak{x}^{(p)}$ in R^n the compound point

$$\xi = (\xi_1, \cdots, \xi_N)$$

in the space R^N. This point lies on a certain fixed algebraic manifold in R^N, the Grassmann manifold G.

Let now $K_1, \cdots, K_p$ be any p convex bodies just as K and K^* in R^n. We allow $\mathfrak{x}^{(1)}, \cdots, \mathfrak{x}^{(p)}$ to run independently over $K_1, \cdots, K_p$, respectively. Then the compound point ξ describes a certain point set Σ on the Grassmann manifold; in general, Σ is not itself a convex body in R^N. We therefore form the convex closure

$$\tilde{K} = [K_1, \cdots, K_p]$$

of Σ in R^N; this is again a convex body with the usual properties, but lies in a space of N dimensions where N will in general be much larger than n.

If the p bodies $K_1, \cdots, K_p$ are distinct, it can be proved that

$$V(\tilde{K})\{V(K_1) \cdots V(K_p)\}^{-N/n} \geqq 2^{-(p-1)N} N! - 1;$$

but this expression has no finite upper bound. Let

$$m_{h1}, \cdots, m_{hn} \quad \text{and} \quad \mu_1, \cdots, \mu_N$$

be the successive minima of K_h and $\tilde{K}$, respectively. Denote by $M_1, \cdots, M_N$ the products

$$m_{1i_1} m_{2i_2} \cdots m_{pi_p} \qquad (1 \leqq i_1 < i_2 < \cdots < i_p \leqq n)$$

arranged in increasing order. Then

THEOREM 4. $\mu_l \leqq M_l$ $(l=1, 2, \cdots, N)$.

There are no analogous lower bounds for the μ's.

Assume, however, that

$$K_1 = \cdots = K_p = K, \quad \text{say,}$$

and denote now again by $m_1, \cdots, m_n$ the successive minima of K. Firstly, it can now be proved that constants $C_1>0$ and $C_2>0$ depending only on n and p exist such that

$$C_1 \leqq V(\tilde{K})V(K)^{-\binom{n-1}{p-1}} \leqq C_2.$$

And secondly, there is now also a constant $C_3>0$ depending only on n and p such that

THEOREM 5. $C_3 M_l \leqq \mu_l \leqq M_l$ $(l=1, 2, \cdots, N)$.

Thus the successive minima of the compound body are given in terms of those of the original body, except for a factor which is independent of K and bounded in both directions.

In this short talk, I have discussed a few general laws of the geometry of numbers of convex bodies. The basic Theorems 1 and 2 were due to Minkowski, while the others are more recent. Naturally this is only a fraction of what is known today, and I refer for a more complete and detailed account to the recent book[1] by C. G. Lekkerkerker. This book has a very full bibliography of both the older and the recent work. It deals not only with convex bodies, but with more general point sets, a subject which I had to exclude.

OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210

---

[1] C. G. Lekkerkerker, *Geometry of numbers*, Bibliotheca Mathematica, vol. VIII, Walters-Noordhoff, Groningen: North-Holland, Amsterdam, 1969.