ON MINKOWSKI'S THEORY OF REDUCTION OF POSITIVE DEFINITE QUADRATIC FORMS

By K. MAHLER (*Manchester*)

[Received 8 June 1938]

MINKOWSKI* called a positive definite quadratic form in n variables

$$F(x) = \sum_{h,k=1}^{n} a_{hk} x_h x_k$$

reduced, if, for $h = 1, 2, \ldots, n$ and for all systems of n integers $x_1, \ldots, x_n$,

$$F(x) \geqslant a_{hh},$$

when the greatest common divisor

$$\text{g.c.d.}\ (x_h, x_{h+1}, \ldots, x_n) = 1,$$

and if certain $n-1$ other unimportant inequalities were satisfied. He proved that, for reduced forms of discriminant D,

$$\lambda_n a_{11} a_{22} \ldots a_{nn} \leqslant D,$$

where $\lambda_n > 0$ depends only on n. L. Bieberbach and I. Schur† showed that

$$\lambda_n \geqslant (\tfrac{48}{125})^{\frac{1}{6}(n^3-n)},$$

and R. Remak‡ in a recent paper improved this to

$$\lambda_n \geqslant \gamma_n (\tfrac{4}{5})^{\frac{1}{2}(n-3)(n-4)}$$

where γ_n is Hermite's constant, for which $D \geqslant \gamma_n a_{nn}^n$.§

As Remak's proof is rather long, I give here a very short and simple proof (which I had obtained before the paper of Remak appeared) for the slightly weaker inequality (since $\frac{4}{9} < \frac{4}{5}$)

$$\lambda_n \geqslant 2^{-2n} (\tfrac{4}{9})^{\frac{1}{2}(n-1)(n-2)} \frac{\{\Gamma(\frac{1}{2})\}^{2n}}{\{\Gamma(1+\frac{1}{2}n)\}^2}.$$

My proof is valid for the reduction of arbitrary convex bodies; it employs Minkowski's theorem on the successive minima of a convex body.‖

* *Gesammelte Abhandlungen*, Bd. 2, 53–100.

† *Sitzungsber. Preussische Akad. Wiss., phys.-math. Kl.* (1928), 510–35.

‡ *Compositio Math.* 5 (1938), 368–91.

§ See J. F. Koksma, 'Diophantische Approximationen', *Erg. d. Math.* IV 4, Kap. II, § 6. The best known result for large n is

$$\gamma_n \geqslant \frac{\pi^n}{2^n \Gamma(2+\frac{1}{2}n)^2},$$

due to Blichfeldt.

‖ *Geometrie der Zahlen*, 218.

1. Let $f(x) = f(x_1,\ldots,x_n)$ be a real function of n real variables $x_1,\ldots, x_n$ $(n \geqslant 2)$ with the following properties:

(i) $f(0,\ldots,0) = 0, \quad f(x_1,\ldots,x_n) > 0$ for $\sum_{h=1}^{n} x_h^2 > 0$;

(ii) $f(tx_1,\ldots,tx_n) = |t| f(x_1,\ldots,x_n)$ for real t;

(iii) $f(x_1+y_1,\ldots,x_n+y_n) \leqslant f(x_1,\ldots,x_n)+f(y_1,\ldots,y_n)$.

Then, for $t > 0$, the inequality $f(x) \leqslant t$ defines a convex body $K(t)$ in n dimensions, of volume $J(t) = Jt^n$, where J denotes the volume of the body $K(1)$, say K.

For every $t > 0$, since $K(t)$ contains only a finite number of lattice points, it is possible to apply Minkowski's method of reduction* to the function $f(x)$. Let M_h $(h = 1,\ldots,n)$ be the set of all lattice points $(x_1,\ldots,x_n)$ whose last $n-h+1$ coordinates x_h, $x_{h+1},\ldots,x_n$ are relatively prime, and let

$$a_h = f(\delta_{h1}, \delta_{h2},\ldots, \delta_{hn}) = f(\delta_h) \quad (h = 1, 2,\ldots, n),$$

where δ_{hk} is Kronecker's symbol:

$$\delta_{hh} = 1, \quad \text{but} \quad \delta_{hk} = 0 \text{ for } h \neq k \quad (h, k = 1, 2,\ldots, n).$$

DEFINITION. *The function $f(x)$ and the corresponding convex body K are called 'reduced', if for each $h = 1,\ldots, n$ and for all lattice points (x) in M_h*

$$f(x) \geqslant a_h.$$

As in Minkowski's paper, it is easily proved that $f(x)$ can be reduced by applying a suitable unimodular linear transformation

$$x_h \to \sum_{k=1}^{n} a_{hk} x_k \quad (h = 1, 2,\ldots, n)$$

with integer coefficients.

2. THEOREM. *For reduced functions $f(x)$*

$$a_1 a_2 \ldots a_n \leqslant \frac{2^n (\frac{3}{2})^{\frac{1}{2}(n-1)(n-2)}}{J}.$$

Proof. Minkowski† proved that there are n independent lattice points

$$(p_h) = (p_{h1},\ldots, p_{hn}) \quad (h = 1, 2,\ldots, n)$$

such that, if

$$S_h = f(p_h) = f(p_{h1},\ldots, p_{hn}) \quad (h = 1, 2,\ldots, n),$$

then

$$S_1 \leqslant S_2 \leqslant \ldots \leqslant S_n, \qquad S_1 S_2 \ldots S_n \leqslant \frac{2^n}{J},$$

* *Gesammelte Abhandlungen*, Bd. 2, 53–100.

† *Geometrie der Zahlen*, 218.

and
$$f(x) \geqslant S_h$$
for all lattice points (x) which are linearly independent of (p_1), $(p_2),\ldots, (p_{h-1})$.

Obviously, (p_1) belongs to M_1; hence
$$a_1 \leqslant S_1. \tag{1}$$
(More exactly $a_1 = S_1$, but we do not need this.)

Suppose that we have already obtained $m-1$ positive absolute constants
$$\gamma_1, \gamma_2, \ldots, \gamma_{m-1},$$
such that
$$a_h \leqslant \gamma_h S_h \quad (h = 1, 2, \ldots, m-1). \tag{2}$$
By (1) in particular
$$\gamma_1 = 1,$$
and we now find a similar constant γ_m for which
$$a_m \leqslant \gamma_m S_m. \tag{3}$$

The m lattice points $(p_1),\ldots, (p_m)$ are independent. Hence at least one of them, say $(p_i) = (p_{i1},\ldots, p_{im})$ ($i = 1$ or 2 or...or m), has its last $n-m+1$ coordinates $p_{im}, p_{i,m+1},\ldots, p_{in}$ not all zero. Therefore the greatest common divisor
$$\text{g.c.d.}\,(p_{im}, p_{i,m+1},\ldots, p_{in}) = d_m \neq 0.$$
If $d_m = 1$, then (p_i) belongs to M_m, and therefore $a_m \leqslant S_i$, i.e.
$$a_m \leqslant S_m. \tag{4}$$
Suppose, however, that $d_m \geqslant 2$. Then we can find $m-1$ integers $g_1, g_2,\ldots, g_{m-1}$, such that
$$p_{ih}+g_h \equiv 0 \pmod{d_m} \quad \text{and} \quad |g_h| \leqslant \tfrac{1}{2}d_m \quad (h = 1, 2,\ldots, m-1).$$
Hence, writing the left-hand side in vector form,
$$\left(\frac{p_{i1}+g_1}{d_m},\ldots, \frac{p_{i,m-1}+g_{m-1}}{d_m}, \frac{p_{im}}{d_m},\ldots, \frac{p_{in}}{d_m}\right) = \frac{1}{d_m}\left\{\sum_{k=1}^{m-1} g_h(\delta_h)+(p_i)\right\}$$
is a lattice point of the set M_m. Therefore, from (ii) and (iii), since $d_m \geqslant 2$,
$$a_m \leqslant \frac{1}{d_m}\left\{\sum_{h=1}^{m-1} |g_h| a_h + S_i\right\} \leqslant \frac{1}{2}\left\{\sum_{h=1}^{m-1} \gamma_h S_h + S_m\right\},$$
i.e.
$$a_m \leqslant \frac{\gamma_1+\gamma_2+\ldots+\gamma_{m-1}+1}{2} S_m. \tag{5}$$

Put
$$\gamma_m = \max\left(1, \frac{\gamma_1+\gamma_2+\ldots+\gamma_{m-1}+1}{2}\right).$$
Then, from (4), (5), we see that (3) is satisfied.

Now

$$\gamma_1 = 1, \qquad \gamma_2 = \max\left(1, \frac{1+1}{2}\right) = 1,$$

$$\gamma_3 = \max\left(1, \frac{1+1+1}{2}\right) = \tfrac{3}{2},$$

$$\gamma_4 = \max\left(1, \frac{1+1+\frac{3}{2}+1}{2}\right) = \tfrac{9}{4} = (\tfrac{3}{2})^2.$$

Suppose, then, that

$$\gamma_h = (\tfrac{3}{2})^{h-2} \quad \text{for} \quad h = 2, 3, \dots, m-1. \tag{6}$$

Then

$$\gamma_m = \max\left(1, \frac{3+(\frac{3}{2})^1+(\frac{3}{2})^2+\dots+(\frac{3}{2})^{m-3}}{2}\right) = \frac{1}{2}\left\{3+\frac{(\frac{3}{2})^{m-2}-(\frac{3}{2})^1}{\frac{3}{2}-1}\right\} = (\tfrac{3}{2})^{m-2},$$

and so (6) holds for $h = m$.

On multiplying the inequalities

$$a_1 \leqslant S_1 \quad \text{and} \quad a_h \leqslant (\tfrac{3}{2})^{h-2} S_h \quad \text{for} \quad h = 2, 3, \dots, n,$$

we have

$$a_1 a_2 \dots a_n \leqslant (\tfrac{3}{2})^{1+2+\dots+(n-2)} S_1 S_2 \dots S_n \leqslant \frac{2^n (\frac{3}{2})^{\frac{1}{2}(n-1)(n-2)}}{J},$$

as was to be proved.

Suppose in particular that

$$\{f(x)\}^2 = F(x) = \sum_{h,k=1}^{n} a_{hk} x_h x_k$$

is a reduced positive definite quadratic form of determinant D. Then

$$J = \frac{\{\Gamma(\frac{1}{2})\}^n}{\Gamma(1+\frac{1}{2}n)} \frac{1}{\sqrt{D}}$$

is the volume of the convex body $f(x) \leqslant 1$, and so by our theorem

$$a_{11} a_{22} \dots a_{nn} \leqslant 2^{2n} (\tfrac{3}{2})^{(n-1)(n-2)} \frac{\{\Gamma(1+\frac{1}{2}n)\}^2}{\{\Gamma(\frac{1}{2})\}^{2n}} D,$$

since

$$a_{hh} = a_h^2 \quad (h = 1, 2, \dots, n).$$