MINKOWSKI'S THEOREM ON THE FIELD DISCRIMINANT

EDMUND LANDAU

(Presented at the Meeting on July 28, 1922)

**Theorem 1.** The absolute value of the discriminant $\Delta$ of every algebraic number field of degree $n > 1$ is $> 1$.

The arithmetic proofs for this famous theorem due to Minkowski are all based on his theorem on $n$ real linear forms

$$L_r = \sum_{s=1}^{n} a_{rs} x_s \quad (r = 1, \ldots, n)$$

with $|\det(a_{rs})| = D > 0$ and $n > 1$:

For given $\lambda_r > 0$ with $\prod_r \lambda_r = D$ there exists a lattice point $(x_1, \ldots, x_r) \neq (0, \ldots, 0)$ with $|L_1| \leq \lambda_1$ and $|L_r| < \lambda_r$ for $r > 1$.

The arithmetic proof of this last theorem is given first for rational values of $a_{rs}$, and then by taking limits for real $a_{rs}$, with $\leq$ in all $n$ inequalities, and by taking limits once more we obtain the theorem in the form given above.

The following new proof reaches its goal in one step, by avoiding the general theorem on linear forms and by modifying the application of Dirichlet’s classical box principle. The theorem on linear forms is only needed in the special case $a_{rs} = 0$ for $s > r$, and I prove this Lemma 2 with, if I may say so, moving instead of fixed boxes (Lemma 1). In no. 38 of his *Geometrie der Zahlen* (1896), Minkowski had remarked, concerning a special case (Satz A) of his theorem on linear forms, that the method of Dirichlet’s box principle only succeeds if $t \geq 1$. In §4 of Chap. 1 of his *Diophantische Approximationen* (1907) he proved Satz A for $n = 2$ using moving boxes for each $t \geq 1$, in §5, however, for $n \geq 3$ only for integral $t \geq 1$ and using fixed boxes. (As is well known, Minkowski derived the general theorem on linear forms using geometric considerations.) Going from Lemma 3 to the final theorem is of course done as usual.

**Lemma 1.** Let $\lambda > 0$ and real $z_1, \ldots, z_t$ for $t > \gamma > 0$ be given. Then there is a system of more than $\gamma \lambda$ pairs of integers $m, g$ such that any pair of numbers $z_m + b$ has distance $< \lambda$.

**Proof.** Choose the integer $h$ in such a way that $t|h\lambda| > \gamma h \lambda$. The number of solutions of $0 \leq z_m + g < h \lambda$ is at least $t|h\lambda| > \gamma h \lambda$. Thus at least one of the $h$ intervals $(j\lambda, (j + 1)\lambda]$ of length $\lambda$ for $j = 0, 1, \ldots, h - 1$ contains more than $\gamma \lambda$ solutions.

**Lemma 2.** Minkowski’s Theorem on Linear Forms with $a_{rs} = 0$ for $s > r$.

**Proof.** Without loss of generality assume that $a_{rr} = 1$, hence $\prod_r \lambda_r = 1$. I set $u_1 = 1, \ldots, [\lambda_1] + 1$. Applying Lemma 1 with $\lambda = \lambda_2$, $t = [\lambda_1] + 1$, $z_m = a_{21} m$
and $\gamma = \lambda$ we find that there exists a system of more than $\lambda_1 \lambda_2$ pairs of integers $u_1, u_2$ such that each pair of $L_1 = u_1$ and $L_2 = a_{21} u_1 + u_2$ have distance $\leq \lambda_1$ and $< \lambda_2$, respectively. Etc. Finally: After having found more than $\lambda_1, \ldots, \lambda_{n-1}$ systems $u_1, \ldots, u_{n-1}$ with the property that any two $L_i$ have distance $\leq \lambda_1$ and $< \lambda_2$, respectively. Etc. Finally: After having found more than $\lambda_1, \ldots, \lambda_{n-1}$ systems $u_1, \ldots, u_{n-1}$ with the property that any two $L_i$ have distance $\leq \lambda_1$ and $< \lambda_2$, respectively. Etc. Finally: After having found more than $\lambda_1, \ldots, \lambda_{n-1}$ systems $u_1, \ldots, u_{n-1}$ with the property that any two $L_i$ have distance $\leq \lambda_1$ and $< \lambda_2$, respectively.

**Lemma 3.** Let $n > 1$, $\Lambda = \sum_{s=1}^{n} a_{rs} x_s$ ($r = 1, \ldots, n$) linear form with complex coefficients $a_{rs}$ such that $|\det a_{rs}| = D > 0$, and assume that with every linear form, its complex-conjugate also occurs. Then there exists a lattice point $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ such that

$$\prod_{r=1}^{n} |\Lambda_r| < D.$$  

**Proof.** The quadratic form

$$\sum_{t=1}^{n} \Lambda_t x_t = \sum_{r} \alpha_{tr} x_r \sum_{s} \alpha_{ts} x_s$$

is definite, hence can be written in the form $\sum_{r=1}^{n} L_r^2$, where $L_r = \sum_s a_{rs} x_s$ with real $a_{rs}$ and $a_{rs} = 0$ for $s > r$. Since

$$\sum_{t} \alpha_{tr} \bar{\alpha}_{ts} + \sum_{t} \alpha_{ts} \bar{\alpha}_{tr} = 2 \sum_{t} \alpha_{tr} \bar{\alpha}_{ts} = 2 \sum_{t} a_{tr} a_{ts}$$

we have

$$D^2 = \det(\alpha_{rs}) \det(\bar{\alpha}_{rs}) = \det(a_{tr}) \det(a_{ts}),$$

$$\det(a_{rs}) = \pm D$$

By Lemma 2 there is a lattice point $\neq (0, \ldots, 0)$ with

$$|L_1| \leq \sqrt{D}, \quad |L_r| < \sqrt{D} \quad \text{for } r > 1;$$

for this lattice point we have

$$\prod_{r} |\Lambda_r|^2 \leq \left( \frac{1}{n} \sum_{r} |\Lambda_r|^2 \right)^n = \left( \frac{1}{n} \sum_{r} L_r^2 \right)^n < D^2.$$  

This completes the proof.

**Proof of Minkowski’s Theorem.** Let $\omega_1, \ldots, \omega_n$ denote a basis of the number field, and let $\omega_s^{(r)}$ denote their conjugates. Applying Lemma 3 to $\Lambda_r = \sum_s \omega_s^{(r)}$ with $D = \sqrt{\Delta}$ and choosing $\beta = \sum_s \omega_s x_s$ we obtain

$$1 \leq |N\beta|^2 = \prod_{r} |\Lambda_r|^2 < |\Delta|.$$