COLLOQUIUM MATHEMATICUM

VOL. XXXVIII 1978 FASC. 2

MINKOWSKI'S THEOREMS IN COMPLETIONS OF A-FIELDS OF NON-ZERO CHARACTERISTIC

BY

M. DUGGAL AND I. S. LUTHAR (CHANDIGARH)

In 1941, Mahler [2] developed an analogue of Minkowski's geometry of numbers, where the roles of Z, Q, and R were played by $F_q[T]$, $F_q(T)$, and $F_q\{T\}$, respectively; here F_q is a finite field with q elements, T is an indeterminate and $F_q\{T\}$ denotes the field of series

$$\xi = a_\nu T^\nu + a_{\nu-1} T^{\nu-1} + \ldots \quad (a_i \in F_q),$$

the absolute value in this field being given by

$$|\xi| = \begin{cases} 0 & \text{if } \xi = 0, \\ q^\nu & \text{if } \xi \neq 0 \text{ with } a_\nu \neq 0. \end{cases}$$

If E is the vector space of n-tuples of $F_q\{T\}$, a *convex body* in E in the sense of Mahler [2] means a set defined by an inequality of the type

$$N(x) \leqslant 1, \tag{1}$$

where N is a norm function in E. If r_∞ denotes the maximal compact subring of $F_q\{T\}$, then a body defined by inequality (1) is an open and compact r_∞-*module*, i.e. an $F_q\{T\}$-lattice in E in the sense of Weil [3]. Conversely, any $F_q\{T\}$-lattice L in E can be defined by an inequality of type (1). Namely, we just take

$$N(x) = \operatorname*{Inf}_{\xi \neq 0,\ \xi x \in L} |\xi|^{-1}; \tag{2}$$

this particular norm function is said to be *associated* with $F_q\{T\}$-lattice L. It is the only norm function taking its values in the set $\{0, q^{\pm 1}, q^{\pm 2}, \ldots\}$ and such that L is given by (1).

We notice now that $F_q\{T\}$ is the completion k_u of $k = F_q(T)$ at the place u of k for which $|T|_u > 1$, and that $F_q[T]$ is the ring $\mathfrak{o}_u$ of those elements x of k for which $\operatorname{ord}_v(x) \geqslant 0$ for every place $v \neq u$ of k. Keeping this in view, let k be an arbitrary A-field of characteristic $p \neq 0$, having F_q

as its field of constants. Let u be an arbitrary place of k and let k_u be the completion of k at u; let $\mathfrak{o}_u$ denote the ring of *u-exceptional integers*, i.e. those elements x of k such that $\mathrm{ord}_v(x) \geqslant 0$ for every place $v \neq u$ of k.

In this paper we shall extend the results of Mahler to the case where the roles of integers, rationals, and reals are played by $\mathfrak{o}_u$, k, and k_u, respectively. Our notations are exactly as in Weil [3] and we shall use them without much explanation. The Haar measure in k_u^n will be that for which r_u^n has measure 1; one may notice that, in the case considered by Mahler, this measure is the same as defined in [2]. The genus of k will be denoted by g, and the degree of the place u will be denoted by d, so that the module q_u of k_u is q^d; E will denote the space of n-tuples of elements of k, and E_v, for any place v of k, will denote the space of n-tuples of elements of k_v.

We first notice that $\mathfrak{o}_u$ is discrete in k_u. For, let U be a compact neighborhood of 0 in k_u; then $U \times \prod_{v \neq u} r_v$ is a compact neighborhood of 0 in k_A. As k is discrete in k_A, it has only finitely many points in $U \times \prod_{v \neq u} r_v$, which means that $\mathfrak{o}_u$ has only finitely many points in U, or that $\mathfrak{o}_u \cap r_u$ is the finite set F_q.

THEOREM 1 (Minkowski-Mahler). *Let L_u be a k_u-lattice ("convex body") in E_u of measure greater than $q^{n(g-1)}$. Then there is a non-zero point $x = (x_1, \ldots, x_n)$ in L_u with each x_i in $\mathfrak{o}_u$.*

Proof. Let μ denote that Haar measure on E_A for which

$$\mu\left(\prod_v \varepsilon_v\right) = 1$$

for every basis ε of E over k, and consider the coherent system of lattices $L = (L_v)_v$, where $L_v = r_v^n$ for $v \neq u$ and L_v is the given lattice L_u for $v = u$. Then

$$q^{n(g-1)} < \mathrm{meas}(L_u) = \mu\left(\prod_v L_v\right) = q^{-\delta(L)},$$

so that $-n(g-1) - \delta(L) > 0$. Thus

$$\lambda(L) = \lambda(L') - n(g-1) - \delta(L) > 0,$$

and hence there exists a non-zero element x in

$$\Lambda(L) = E \cap \prod_v L_v,$$

i.e., $x \in L_u \cap \mathfrak{o}_u^n$.

COROLLARY. *Let $\varphi_1(z), \ldots, \varphi_l(z)$ be l independent linear forms in the variables $z_1, \ldots, z_l$ with coefficients from k_u, and let Δ be the determinant of these linear forms. If $\varrho_1, \ldots, \varrho_l$ are integers such that*

$$q_u^{\varrho} > q^{l(g-1)}|\Delta|_u \quad \cdot(\varrho = \varrho_1 + \ldots + \varrho_l), \tag{3}$$

then the inequalities

$$|\varphi_\lambda(z)|_u \leqslant q_u^{\varrho_\lambda}, \qquad 1 \leqslant \lambda \leqslant l, \tag{4}$$

have a non-zero solution in $\mathfrak{o}_u^l$.

This is an immediate consequence of Theorem 1 by noticing that inequalities (4) define a k_u-lattice of measure $q_u^{\varrho}|\Delta|_u^{-1}$.

Remark. Let L_u be any k_u-lattice in E_u. It is well known that there exist l independent vectors $e_1, \ldots, e_l$ in L_u such that the vector

$$z = \varphi_1 e_1 + \ldots + \varphi_l e_l$$

is in L_u if and only if $|\varphi_\lambda|_u \leqslant 1$ for $1 \leqslant \lambda \leqslant l$. The φ_λ are linear forms $\varphi_\lambda(z)$, and thus L_u is defined by the inequalities $|\varphi_\lambda(z)|_u \leqslant 1$, $1 \leqslant \lambda \leqslant l$.

In view of this remark, the result of the Corollary is as general as the result of Theorem 1.

Let, again, L_u be a k_u-lattice in E_u and let

$$N(x) = \operatorname*{Inf}_{a \neq 0, a \cdot x \in L_u} |a|_u^{-1} \tag{5}$$

be the associated distance function. If $V = q_u^e$ denotes the measure of L_u, then the measure of the lattice $N(x) \leqslant q_u^t$ is $q_u^{nt} V$. If we choose

$$t = \left[\frac{g-1}{d} - \frac{s}{n}\right] + 1,$$

then $q_u^{nt} V > q^{n(g-1)}$, and hence, by Theorem 1, there exists a non-zero point x in $\mathfrak{o}_u^n$ satisfying

$$N(x) \leqslant q_u^t \leqslant q^{g-1+d} V^{-1/n}.$$

Thus, if

$$\sigma_1 = \operatorname*{Inf}_{0 \neq x \in \mathfrak{o}_u^n} N(x) \tag{6}$$

is the first minimum of L_u, then

$$\sigma_1 \leqslant q^{g-1+d} V^{-1/n}. \tag{7}$$

Let σ_1 be attained at a point $x^{(1)}$ of $\mathfrak{o}_u^n$ and let σ_2 be the infimum of the set

$$\{N(x)\colon x \text{ in } \mathfrak{o}_u^n \text{ and } x \text{ independent of } x^{(1)}\}.$$

Let σ_2 be attained at $x^{(2)}$ and define σ_3 to be the infimum of the set

$$\{N(x)\colon x \text{ in } \mathfrak{o}_u^n \text{ and } x \text{ independent of } x^{(1)} \text{ and } x^{(2)}\}.$$

Continuing, we obtain

$$q_u^{e_1} = \sigma_1 = N(x^{(1)}) \leqslant \ldots \leqslant q_u^{e_n} = \sigma_n = N(x^{(n)}). \tag{8}$$

We notice that the k_u-lattice $N(x) \leqslant q_u^{e_i}$ contains at least i independent points of $\mathfrak{o}_u^n$ (namely, $x^{(1)}, \ldots, x^{(i)}$) and that the k_u-lattice $N(x) \leqslant q_u^{e_i - 1}$ contains at most those points of $\mathfrak{o}_u^n$ which are dependent on $x^{(1)}, \ldots, x^{(i-1)}$ over k_u. In particular, $q_u^{e_i}$ is the least power of q_u such that $N(x) \leqslant q_u^{e_i}$ has at least i independent points of $\mathfrak{o}_u^n$. The quantities $\sigma_1, \ldots, \sigma_n$ which, in particular, depend only on L_u will be called the *successive minima* of L_u.

THEOREM 2 (Minkowski-Mahler). *Let L_u be a k_u-lattice in E_u of measure V, and let $\sigma_1, \ldots, \sigma_n$ be the successive minima of L_u. Then*

$$V^{-1} \leqslant \sigma_1 \ldots \sigma_n \leqslant q^{n(g+d-1)} V^{-1}. \tag{9}$$

Moreover, if $x^{(1)}, \ldots, x^{(n)}$ are defined as above, then

$$1 \leqslant |\det(x_j^{(i)})|_u \leqslant q^{n(g+d-1)}. \tag{10}$$

Remark. In the case considered by Mahler [2], $g = 0$, $d = 1$, and hence $\sigma_1 \ldots \sigma_n = V^{-1}$ and $|\det(x_j^{(i)})|_u = 1$, so that $\det(x_j^{(i)})$ is a non-zero element of F_q. These are Mahler's results.

Proof. Let us denote by π_u a prime element of k_u.

(a) Since $N(\pi_u^{e_i} x^{(i)}) = 1$, the k_u-lattice generated by the points $\pi_u^{e_i} x^{(i)}$, $1 \leqslant i \leqslant n$, is contained in L_u, and hence

$$\sigma_1^{-1} \ldots \sigma_n^{-1} |\det(x_j^{(i)})|_u \leqslant V. \tag{11}$$

Since $\det(x_j^{(i)})$ is a non-zero member of k, and $|\det(x_j^{(i)})|_v \leqslant 1$ for each $v \neq u$, we have, by Artin's product formula,

$$|\det(x_j^{(i)})|_u \geqslant 1, \tag{12}$$

and hence, by (11), $V^{-1} \leqslant \sigma_1 \ldots \sigma_n$. This proves the first inequality in (9) as well as the first inequality in (10).

(b) Let $E^{(0)}$ denote the zero subspace of E and, for $1 \leqslant i \leqslant n$, let $E^{(i)}$ denote the subspace of E generated by $x^{(1)}, \ldots, x^{(i)}$. Let $L = (L_v)_v$ be the coherent system of lattices belonging to E defined by

$$L_v = \begin{cases} L_u & \text{if } v = u, \\ r_v^n & \text{if } v \neq u. \end{cases} \tag{13}$$

Let π_u be a prime element of k_u and let $z = \pi_u^{-1}$; we shall also consider z as an idele (namely, $z_u = \pi_u^{-1}$, $z_v = 1$ for $v \neq u$). We put

$$U(L) = \prod_v L_v. \tag{14}$$

Then, for any integer e,

$$E \cap z^e U(L) = \{x \in \mathfrak{o}_u^n : N(x) \leqslant q_u^e\}.$$

In particular, by what has been said just before Theorem 2,

$$E \cap z^{e_i - 1} U(L) \subset E^{(i-1)},$$

and hence

$$E^{(i)} \cap z^{e_i - 1} U(L) = E^{(i-1)} \cap z^{e_i - 1} U(L). \tag{15}$$

(c) Let $M = (M_v)_v$ be a coherent system of lattices belonging to a vector space E of dimension n over k; let $\bar{E}$ be a subspace of E of dimension r, and let

$$\bar{M}_v = \bar{E}_v \cap M_v.$$

It is obvious that $\bar{M} = (\bar{M}_v)_v$ is a coherent system of lattices belonging to $\bar{E}$, and that

$$\Lambda(\bar{M}) = \bar{E} \cap \prod_v \bar{M}_v$$

is the same as $\bar{E} \cap \prod_v M_v$. We shall denote by $\bar{\lambda}(M)$ the dimension of $\Lambda(\bar{M})$ over F_q. In case $\bar{E} = E^{(i)}$, $\bar{\lambda}(M)$ will be denoted by $\lambda_i(M)$. Put

$$\bar{D}(M) = q^{-\bar{\lambda}(M)} \mu\big(U(M)\big). \tag{16}$$

In case $\bar{E} = E^{(i)}$, $\bar{D}(M)$ will be denoted by $D_i(M)$.

If z is any idele, denote by zM the coherent system $(z_v M_v)_v$; it is obvious that $\overline{zM} = z\bar{M}$.

CLAIM. *If z is such that $|z_v|_v \geqslant 1$ for all v, then*

$$\bar{D}(zM) \geqslant |z|_A^{n-r} \bar{D}(M), \tag{17}$$

where, as usual, $|z|_A$ denotes $\prod_v |z_v|_v$.

To prove (17) we apply the Riemann-Roch theorem to the coherent systems of lattices $z\bar{M}$ and $\bar{M}$ belonging to $\bar{E}$ and we get

$$\bar{\lambda}(zM) = \lambda(z\bar{M}) = \lambda\big((z\bar{M})'\big) - \delta(z\bar{M}) - r(g-1),$$

$$\bar{\lambda}(M) = \lambda(\bar{M}) = \lambda(\bar{M}') - \delta(\bar{M}) - r(g-1).$$

Since $|z_v|_v \geqslant 1$ for each v, we have $z_v \bar{M}_v \supset \bar{M}_v$, so that $(z_v \bar{M}_v)' \subset \bar{M}_v'$ for all v, and hence

$$\lambda\big((z\bar{M})'\big) \leqslant \lambda(\bar{M}').$$

Consequently,

$$q^{\bar{\lambda}(M) - \bar{\lambda}(zM)} \geqslant q^{-\delta(\bar{M}) + \delta(z\bar{M})} = \frac{\text{measure in } \bar{E}_A \text{ of } U(\bar{M})}{\text{measure in } \bar{E}_A \text{ of } U(z\bar{M})} = |z|_A^{-r}.$$

Also

$$\mu\big(U(zM)\big) = \mu\big(zU(M)\big) = |z|_A^n \mu\big(U(M)\big).$$

Multiplying the last two relations, we get (17).

If, in particular, z is such that $\mathrm{ord}_u(z_u) = -1$ and $z_v = 1$ for all $v \neq u$, then $|z|_A = q_u$, and hence

$$D_i(z^t M) \geqslant q_u^{t(n-i)} D_i(M) \quad (t \geqslant 0 \text{ any integer}). \tag{18}$$

(d) Let us now return to the coherent system (13). In view of (15),

$$\lambda_i(z^{e_i-1}L) = \lambda_{i-1}(z^{e_i-1}L),$$

and hence

$$D_i(z^{e_i-1}L) = D_{i-1}(z^{e_i-1}L), \quad 1 \leqslant i \leqslant n \tag{19}$$

$$(\mathrm{ord}_u(z_u) = -1,\ z_v = 1 \text{ for } v \neq u).$$

Finally,

$$\lambda(z^{e_n-1}L) \geqslant -\delta(z^{e_n-1}L) - n(g-1),$$

and hence

$$D_n(z^{e_n-1}L) \leqslant q^{n(g-1)}. \tag{20}$$

We can now easily complete the proof of Theorem 2. In fact, by (18), (19) and (20) we have

$$\begin{aligned}
q^{n(g-1)} &\geqslant D_n(z^{e_n-1}L) = D_{n-1}(z^{e_n-e_{n-1}}z^{e_{n-1}-1}L) \\
&\geqslant q_u^{e_n-e_{n-1}} D_{n-1}(z^{e_{n-1}-1}L) = q_u^{e_n-e_{n-1}} D_{n-2}(z^{e_{n-1}-e_{n-2}}z^{e_{n-2}-1}L) \\
&\geqslant q_u^{(e_n-e_{n-1})+2(e_{n-1}-e_{n-2})} D_{n-2}(z^{e_{n-2}-1}L) = \dots \\
&\quad \dots \\
&\geqslant q_u^{(e_n-e_{n-1})+2(e_{n-1}-e_{n-2})+\dots+(n-1)(e_2-e_1)} D_1(z^{e_1-1}L) \\
&= q_u^{e_n+\dots+e_2-(n-1)e_1}\mu\big(z^{e_1-1}U(L)\big) \\
&= q_u^{e_n+\dots+e_2-(n-1)e_1} q_u^{n(e_1-1)}\mu\big(U(L)\big) \\
&= \sigma_1 \dots \sigma_n q_u^{-n} V.
\end{aligned}$$

This proves the second inequality in (9). By (11) we get

$$|\det(x_j^{(i)})|_u \leqslant \sigma_1 \dots \sigma_n V \leqslant q^{n(g+d-1)},$$

which is the second inequality in (10), and the proof of Theorem 2 is completed.

Remark. Notice that the proof of Theorem 2 is like the first proof in [1]. It might be interesting to give proofs of that theorem similar to the second and third proofs in [1].

Successive minima of the dual lattice. Let L_u be a k_u-lattice in $E_u = k_u^n$ and let

$$L_u' = \{y \text{ in } E_u\colon |x \cdot y|_u \leqslant 1 \text{ for all } x \text{ in } L_u\}, \tag{21}$$

where $x \cdot y$ means $\sum_i x_i y_i$.

If $x^{(1)}, \ldots, x^{(n)}$ is a basis of the r_u-module L_u and if $y^{(1)}, \ldots, y^{(n)}$ are found such that

$$x^{(i)} \cdot y^{(j)} = \delta_{ij}, \quad 1 \leqslant i, j \leqslant n, \tag{22}$$

then one checks easily that L'_u is the r_u-submodule of E_u generated by $y^{(1)}, \ldots, y^{(n)}$. In particular, L'_u is a k_u-lattice which we shall call the *dual lattice* of L_u.

THEOREM 3. *Let $\sigma_1, \ldots, \sigma_n$ be the successive minima of the lattice L_u, and let $\sigma'_1, \ldots, \sigma'_n$ be those of the dual lattice L'_u. Then*

$$1 \leqslant \sigma_i \sigma'_{n-i+1} \leqslant q^{n(g+d-1)}, \quad 1 \leqslant i \leqslant n. \tag{23}$$

Proof. Let $x^{(1)}, \ldots, x^{(n)}$ be a basis of L_u as an r_u-module, and let $y^{(1)}, \ldots, y^{(n)}$ be the basis of the r_u-module L'_u given by (22). If we write any vector x as

$$x = \sum_{i=1}^{n} a_i(x) x^{(i)}, \quad x = \sum_{i=1}^{n} b_i(x) y^{(i)}, \tag{24}$$

then a_i and b_i are linear forms in x,

$$a_i(x) = \sum_j a_{ij} x_j, \quad b_i(x) = \sum_j b_{ij} x_j, \tag{25}$$

and L_u and L'_u are given by the inequalities $N(x) \leqslant 1$ and $N'(x) \leqslant 1$, respectively, where

$$N(x) = \operatorname*{Max}_i |a_i(x)|_u, \tag{26}$$

$$N'(x) = \operatorname*{Max}_i |b_i(x)|_u. \tag{26'}$$

Since, for any vectors x and y, by (22), (24), and (25) the equalities

$$\sum_i x_i y_i = x \cdot y = \sum_i a_i(x) b_i(y) = \sum_{i,j,l} a_{ij} b_{il} x_j y_l$$

hold, we have

$$\sum_i a_{ij} b_{il} = \delta_{jl},$$

and hence $B' = A^{-1}$, where $A = (a_{ij})$ and $B = (b_{ij})$.

Let now $z^{(1)}, \ldots, z^{(n)}$ be n points of $\mathfrak{o}_u^n$ which are independent over k_u and which are such that

$$N(z^{(j)}) = \sigma_j. \tag{27}$$

Let Z be the matrix whose columns are $z^{(1)}, \ldots, z^{(n)}$ and let W be the adjoint matrix of Z; write

$$W = \begin{pmatrix} w^{(1)} \\ \ldots \\ w^{(n)} \end{pmatrix} = \begin{pmatrix} w_1^{(1)}, \ldots, w_n^{(1)} \\ \ldots\ldots\ldots \\ w_1^{(n)}, \ldots, w_n^{(n)} \end{pmatrix}.$$

Then, of course, $w^{(1)}, \ldots, w^{(n)}$ are all in $\mathfrak{o}_u^n$. Now

$$(\det A)^{-1}\operatorname{adj}(AZ) = (\operatorname{adj} Z)B' = WB',$$

and hence, by (25),

$$b_j(w^{(i)}) = (\det A)^{-1}\big(i-j \text{ entry in } \operatorname{adj}(AZ)\big). \tag{28}$$

Since, by (25), $AZ = \big(a_i(z^{(j)})\big)$ and since each entry in the l-th column of AZ is not greater than σ_l in absolute value, it follows from Theorem 2 that

$$|i-j \text{ entry in } \operatorname{adj}(AZ)|_u \leqslant \prod_{l \neq i} \sigma_l \leqslant \sigma_i^{-1} q^{n(\varrho+d-1)} |\det A|_u,$$

and hence, by (28),

$$|b_j(w^{(i)})|_u \leqslant \sigma_i^{-1} q^{n(\varrho+d-1)}, \quad 1 \leqslant j \leqslant n.$$

Thus $N'(w^{(i)}) \leqslant \sigma_i^{-1} q^{n(\varrho+d-1)}$. Since $\sigma_1 \leqslant \ldots \leqslant \sigma_n$, we see that

$$N'(w^{(i)}),\ N'(w^{(i+1)}), \ldots, N'(w^{(n)})$$

are all not greater than $\sigma_i^{-1} q^{n(\varrho+d-1)}$. In other words, the k_u-lattice

$$N'(w) \leqslant \sigma_i^{-1} q^{n(\varrho+d-1)}$$

contains the $n-i+1$ independent points $w^{(i)}, \ldots, w^{(n)}$ of $\mathfrak{o}_u^n$. Consequently,

$$\sigma'_{n-i+1} \leqslant \sigma_i^{-1} q^{n(\varrho+d-1)}$$

proving the second of inequalities (23).

To prove the first of inequalities (23), choose n independent points $z'^{(1)}, \ldots, z'^{(n)}$ of $\mathfrak{o}_u^n$ such that

$$N'(z'^{(l)}) = \sigma'_l, \quad 1 \leqslant l \leqslant n. \tag{27'}$$

For any i, $1 \leqslant i \leqslant n$, the conditions

$$z'^{(l)} \cdot z = 0, \quad 1 \leqslant l \leqslant n-i+1, \tag{29}$$

define a subspace of dimension $i-1$. Hence, not all of $z^{(1)}, \ldots, z^{(i)}$ can satisfy (29) and, consequently, there exist λ and μ, $1 \leqslant \lambda \leqslant n-i+1$, $1 \leqslant \mu \leqslant i$, such that

$$z'^{(\lambda)} \cdot z^{(\mu)} \neq 0.$$

Since $z'^{(\lambda)} \cdot z^{(\mu)}$ is in $\mathfrak{o}_u$, by Artin's product formula we have

$$1 \leqslant |z'^{(\lambda)} \cdot z^{(\mu)}|_u = \Big| \sum_h a_h(z^{(\mu)}) b_h(z'^{(\lambda)}) \Big|_u \leqslant \sigma_\mu \sigma'_\lambda \leqslant \sigma_i \sigma'_{n-i+1}.$$

This completes the proof of Theorem 3.

REFERENCES

[1] R. P. Bambah, A. Woods and H. Zassenhaus, *Three proofs of Minkowski's second inequality in the geometry of numbers*, The Journal of the Australian Mathematical Society 5 (1965), p. 453-462.

[2] K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series*, Annals of Mathematics 42 (1941), p. 488-522.

[3] A. Weil, *Basic number theory*, New York 1967.

DEPARTMENT OF MATHEMATICS
PANJAB UNIVERSITY
CHANDIGARH, INDIA

Reçu par la Rédaction le 24. 3. 1976