THE GEOMETRY OF NUMBERS OVER ALGEBRAIC NUMBER FIELDS

BY

K. ROGERS[1] AND H. P. F. SWINNERTON-DYER

1. The Geometry of Numbers was founded by Minkowski in order to attack certain arithmetical problems, and is normally concerned with lattices over the rational integers. Minkowski himself, however, also treated a special problem over complex quadratic number fields [5], and a number of writers have since followed him. They were largely concerned with those fields which have class-number $h=1$; and this simplification removes many of the characteristic features of the more general case. Hermann Weyl [10] gave a thorough account of the extension of Minkowski's theory of the reduction of quadratic forms to "gauge functions" over general algebraic number fields and quaternion algebras, and we shall follow part of his developments, though our definition of a lattice is quite different.

The desirability of extending the Geometry of Numbers to general algebraic number fields was emphasized by Mahler in a seminar at Princeton. In this paper we shall carry out this program, extending the fundamental results of Mahler [4] to our more general case and applying them to specific problems. Certain new ideas are necessary, but much of this paper must be regarded as expository. In particular, when the proof of a result is essentially analogous to that for the real case we have merely given a reference to the latter.

2. Let K be an algebraic extension of the rationals of degree m. We regard K as an algebra over the rationals, which we can extend to an algebra K^* over the reals. It is well known that K^* is commutative and semi-simple (being in fact isomorphic to the direct sum of r copies of the reals and s copies of the complex numbers, where r and $2s$ are the number of real and complex conjugates of K); and the integers of K^* are just those of K. We now define the n-dimensional space K^n over K as being the set of ordered n-tuples of elements in K^*. Any $\xi\in K^*$ is of the form $\xi=x_1\omega_1+\cdots+x_m\omega_m$, where the x_i are real and $\omega_1, \cdots, \omega_m$ is an integral basis for K; and hence there is a natural map of K^n onto R^{mn} in which each component ξ is mapped onto m of the components of the point in R^{mn}, namely $x_1, \cdots, x_m$ as above. We can define a metric and a measure in K^n by means of those in R^{mn}, with the above map, and so K^n is a locally compact complete metric space.

Received by the editors November 19, 1956.

(1) The work of this author was supported in part by the Office of Ordnance Research, U. S. Army, Contract No. DA-19-020-ORD-3778.

The *integer lattice* in K^n is defined as the set of points all of whose coordinates are integers. It would be natural to define a lattice in K^n as any nonsingular linear transformation of the integer lattice, but we shall see that this could correspond to a lattice of dimension less than mn in R^{mn}. Namely, a transformation in K^n of matrix A and determinant $\delta \neq 0$ induces a transformation in R^{mn} of matrix $\Omega^{-1}\mathfrak{A}\Omega$, where $\Omega = (\omega_j^{(i)} I_n)$ $(i = 1, \cdots, m;\ j = 1, \cdots, m;\ I_n = \text{unit matrix of order } n)$ and $\mathfrak{A}$ is an mn-by-mn matrix with the conjugates $A^{(1)}, \cdots, A^{(m)}$ down the diagonal and zeroes elsewhere. Thus, extending the norm symbol from K to K^*, we see that the transformation in R^{mn} has determinant Norm δ, which may very well be zero. We therefore define a *lattice in* K^n to be any linear transformation of determinant δ of the integer lattice, such that Norm $\delta \neq 0$; in other words, any transform of the integer lattice which maps into a lattice in R^{mn} (that is, one of full dimension mn). The determinant of a lattice is defined to be the principal ideal generated by the determinant of the corresponding linear transformation. Since the automorphisms of a lattice are precisely the unimodular transformations (those with integral coefficients and determinant a unit), the determinant of a lattice does not depend on the way in which it has been generated. However, the norm of this ideal is the more natural constant of the lattice, being the measure (in R^{mn}) of the fundamental region of this discrete subgroup of the topological group K^n.

We note here the difference between Weyl's definition [10^2, §2] and ours. For him, a "lattice belonging to the principal order $\mathfrak{O}$ of integers of K" is a lattice in R^{mn} such that the corresponding set of points in K^n is mapped into itself under multiplication by any element of $\mathfrak{O}$. Our lattices satisfy a more stringent condition. In fact we have(2):

THEOREM 1. *Let* Λ *be a point-set in* K^n, *lying in no* $(n-1)$*-dimensional subspace of* K^n, *which satisfies*:

(a) *if* $P, Q \in \Lambda$ *and* $u, v \in \mathfrak{O}$, *then* $uP + vQ \in \Lambda$;

(b) Λ *is discrete.*

Then there are points $P_1, P_2, \cdots, P_n$ *in* Λ, *linearly independent over* K^*, *and a fractional ideal* $\mathfrak{a}$ *of* K *such that the points of* Λ *are just the points* $u_1P_1 + \cdots + u_nP_n$ *with* $u_1, \cdots, u_{n-1}$ *all in* $\mathfrak{O}$ *and* u_n *in* $\mathfrak{a}$. *The class of* $\mathfrak{a}$ *depends only on* Λ *and not on the choice of* $P_1, \cdots, P_n$.

For Λ to be a lattice in Weyl's sense, in addition to (a) and (b) we need only demand that its image in R^{mn} does not lie in a subspace of lower dimension; but for our definition it is necessary and sufficient that, in addition to all these conditions, the associated ideal class be the principal one. One can develop a theory for "pseudo-lattices of a given ideal class" analogous to ours for lattices, and so deduce all our main results for lattices in Weyl's

(2) For the classical case, where a discrete n-dimensional subgroup of R^n is shown to be a lattice, see Hajós [2].

sense; but it is easier in that case to prove them directly. For fields K of class-number 1, both definitions are the same.

Proof of Theorem 1. We deal first with all except the last part of the statement. Our induction really begins at the stage $n=2$, but for this we need the case $n=1$. For $n=1$, we can consider the points of Λ as elements of K^* and choose for P_1 any point of Λ other than the origin. By (a), Λ consists of complete cosets modulo $\mathfrak{O}P_1$. Thus $K^*/\mathfrak{O}P_1$ exists and is, by (b), a discrete subgroup of the compact group $K^*/\mathfrak{O}P_1$; it is therefore a finite group of order l, say. Hence every point of Λ is of the form $(\alpha/l)P_1$ for some integer α; and clearly the α form an ideal in $\mathfrak{O}$. Calling this ideal $\mathfrak{a}l$, we obtain the case $n=1$ of the theorem.

To carry on the induction we need a definition and a lemma. If P is any point of Λ, then clearly the set of numbers α in K such that $\alpha P\in\Lambda$ forms a fractional ideal. Since this ideal contains 1, it is of the form $\mathfrak{a}^{-1}$, where $\mathfrak{a}$ is an integral ideal. We call $\mathfrak{a}$ *the ideal associated with* P, and we say that P is primitive if it is associated with $(1)=\mathfrak{O}$.

LEMMA 1. *If* $n\geqq 2$, Λ *contains at least two independent primitive points.*

Proof. Let P_1 and P_2 be independent points of Λ. By confining our attention to the subspace generated by these points we may suppose that $n=2$, for convenience. The points $\alpha_1P_1+\alpha_2P_2$ with α_1, $\alpha_2\in\mathfrak{O}$ form a lattice subset Λ' of finite index in Λ, by the discreteness of Λ. If l denotes this index, then every point of Λ is of the form $\alpha_1P_1+\alpha_2P_2$ with $l\alpha_1$, $l\alpha_2\in\mathfrak{O}$. Let $\mathfrak{a}_1$ be the ideal associated with P_1, and let $\mathfrak{b}^{-1}$ be the ideal consisting of all α_2 such that there exists an α_1 with $\alpha_1P_1+\alpha_2P_2\in\Lambda$. Since $\mathfrak{b}^{-1}\supset\mathfrak{O}$, it follows that $\mathfrak{b}$ is integral. Replacing P_2 by $\alpha_1P_1+\alpha_2P_2$ replaces $\mathfrak{b}$ by $\alpha_2\mathfrak{b}$, which can be any ideal in the same class, since α_2 can be any member of $\mathfrak{b}^{-1}$. By Satz 74 of Hecke's *Vorlesungen über die Theorie der algebraischen Zahlen*, it follows that we can find a member of this ideal class which is prime to α_1. Now let $\mathfrak{a}$ be the ideal associated with αP_1+P_2, where $\alpha\in\mathfrak{O}$. Then $\mathfrak{a}$ is an integral ideal which depends on α, and clearly $\mathfrak{a}^{-1}\subset\mathfrak{b}^{-1}$, hence $\mathfrak{a}\,|\,\mathfrak{b}$. Let now $\mathfrak{p}$ be a prime ideal divisor of $\mathfrak{b}$. If $\mathfrak{p}\,|\,\mathfrak{a}$ for all α, then $\mathfrak{p}^{-1}\subset\mathfrak{a}^{-1}$ for all α; and hence for $\lambda\in\mathfrak{p}^{-1}$ we have $\lambda(\alpha P_1+P_2)\in\Lambda$ and $\lambda\{(\alpha+1)P_1+P_2\}\in\Lambda$, so that $\lambda P_1\in\Lambda$, that is to say $\lambda\in\mathfrak{a}_1^{-1}$. Hence this would imply that $\mathfrak{p}\,|\,\mathfrak{a}_1$, which is false, since $\mathfrak{p}$ already divides $\mathfrak{b}$ which is prime to $\mathfrak{a}_1$. Hence there exist α such that $\mathfrak{p}\nmid\mathfrak{a}$; and since, for $\lambda\in\mathfrak{p}^{-1}$, $\lambda\{(\alpha+\mathfrak{p})P_1+P_2\}\subset\Lambda$ if and only if $\lambda(\alpha P_1+P_2)\in\Lambda$, it also follows that all integers congruent to α mod $\mathfrak{p}$ will share this desired property. Since only the divisors of $\mathfrak{b}$ can divide $\mathfrak{a}$, it follows by the Chinese Remainder Theorem that there is a residue class modulo a certain product of prime ideals such that for all α in this class $\mathfrak{a}$ has no prime divisors and is therefore just (1). Since points αP_1+P_2 and $\alpha' P_1+P_2$ are independent if $\alpha\neq\alpha'$, we certainly have found two independent primitive points of Λ.

We next apply this lemma to prove Theorem 1 for $n=2$. Let now Q_1

and Q_2 denote independent primitive points of the set Λ in K^2. Write $\mathfrak{a}^{-1}$ for the ideal of α_1 such that there exists α_2 with $\alpha_1 Q_1 + \alpha_2 Q_2 \in \Lambda$, and similarly for $\mathfrak{b}^{-1}$ with the subscripts interchanged. Now $\mathfrak{a} = \mathfrak{b}$; for if $\lambda \in \mathfrak{a}$, then $\lambda \in \mathfrak{O}$, and so for each $\alpha_2 \in \mathfrak{b}^{-1}$ we take an $\alpha_1 \in \mathfrak{a}^{-1}$ such that $\alpha_1 Q_1 + \alpha_2 Q_2 \in \Lambda$, and hence $\lambda(\alpha_1 Q_1 + \alpha_2 Q_2) \in \Lambda$. Since $\lambda\alpha_1 \in \mathfrak{O}$, $\lambda\alpha_1 Q_1 \in \Lambda$, and hence $\lambda\alpha_2 Q_2 \in \Lambda$. Since Q_2 is primitive, it follows that $\lambda\alpha_2 \in \mathfrak{O}$; and this being true for all $\alpha_2 \in \mathfrak{b}^{-1}$ implies that $\lambda \in \mathfrak{b}$. The converse is proved in the same way, and hence $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$. Let a basis for $\mathfrak{a}^{-1}$ over $\mathfrak{O}$ be $(1, \alpha)$. Then $\alpha Q_1 + \beta Q_2 \in \Lambda$ implies that $\beta = u + u_0\alpha$, where u, u_0 are integers. Hence $\alpha Q_1 + u_0 \alpha Q_2 \in \Lambda$, and so any λ in $\mathfrak{a}^{-1}$ is such that $\lambda(Q_1 + u_0 Q_2) \in \Lambda$. The converse being immediate, it follows that the ideal associated with the point $Q_1 + u_0 Q_2$ is $\mathfrak{a}$. Now, if P is any point of Λ, it can be written as $P = aQ_1 + bQ_2$, where a and b belong to $\mathfrak{a}^{-1}$. Hence $P = a(Q_1 + u_0 Q_2) + (b - au_0)Q_2$, and since we know that $a(Q_1 + u_0 Q_2) \in \Lambda$, it follows that $(b - au_0)Q_2 \in \Lambda$ and therefore $b - au_0 \in \mathfrak{O}$, since Q_2 is primitive. Thus, if we write $P_1 = Q_2$ and $Q_1 + u_0 Q_2 = P_2$, we have shown that

$$\Lambda = \mathfrak{O}P_1 + \mathfrak{a}^{-1}P_2,$$

thus completing the proof of the main part of Theorem 1 for $n = 2$.

We return to the induction of the theorem. Suppose it is proved in $n-1$ dimensions, where $n \geqq 3$. Let $P_1, Q_2, \cdots, Q_n$ be linearly independent points of Λ. The general point of Λ is

$$P = \alpha_1 P_1 + \alpha_2 Q_2 + \cdots + \alpha_n Q_n. \tag{1}$$

Let Λ' be the set of all $\alpha_2 Q_2 + \cdots + \alpha_n Q_n$ such that (1) holds for some $P \in \Lambda$ and some α_1. Then in the subspace generated by $Q_2, \cdots, Q_n$, Λ' satisfies the conditions of Theorem 1, with $n-1$ in place of n. Let $P_2', \cdots, P_n', \mathfrak{a}'$ be a basis for Λ' as in the theorem; and let $P_2, \cdots, P_n$ be points of Λ of the form

$$P_i = \alpha^{(i)} P_1 + P_i', \qquad (2 \leqq i \leqq n).$$

Then each point of Λ can be written as $P = \alpha P_1 + u_2 P_2 + \cdots + u_n P_n$, where $u_2, \cdots, u_{n-1}$ are in $\mathfrak{O}$ and u_n is in $\mathfrak{a}'$. The theorem now follows when we apply the case $n = 2$ to the set of points of the form $\alpha P_1 + u P_n$, where $u \in \mathfrak{a}'$, which belong to Λ.

To prove the last statement of the theorem, suppose that the basis of Λ, according to what we have proved, is $P_1, \cdots, P_n, \mathfrak{a}$. Let $Q_1, \cdots, Q_n$ be independent points of Λ, and suppose

$$Q = \alpha_{i1} P_1 + \cdots + \alpha_{in} P_n. \tag{2}$$

Then as $Q_1, \cdots, Q_n$ vary, $\det(\alpha_{ij})$ runs through precisely the elements of $\mathfrak{a}$. Hence, if we go from one basis with associated ideal $\mathfrak{a}$ to another with associated ideal $\mathfrak{a}'$, then $\mathfrak{a}'/\mathfrak{a}$ is just the principal ideal generated by the determinant of the transformation; thus $\mathfrak{a}'$ and $\mathfrak{a}$ are in the same ideal class. This completes the proof of the theorem.

COROLLARY. *Let Λ satisfy the conditions of Theorem* 1, *and let $P_1, \cdots, P_n$ be any linearly independent points of Λ. Then a necessary and sufficient condition for Λ to be a lattice is that, if for any n points $Q_1, \cdots, Q_n$ of Λ we write $\Delta = \det(\alpha_{ij})$ with the α_{ij} given by* (2), *then for fixed P_i and varying Q_j the ideal generated by the values of Δ is principal.*

This follows at once by an argument similar to that of the last paragraph.

In the rest of this paper we have been careful to give proofs not depending on Theorem 1; for the proof of this depends heavily on the particular properties of algebraic number fields, whereas we believe that most of our results can be further generalized without much difficulty and that such generalization may be useful.

3. Let Λ be a lattice and $P_1, \cdots, P_n$ be a basis for Λ. Then if $S_1, \cdots, S_n$ are neighborhoods of $P_1, \cdots, P_n$ we define the corresponding neighborhood of Λ as the set of those lattices Λ' which have a basis $P_1', \cdots, P_n'$ with $P_i' \in S_i$. The topology thus induced corresponds also to the natural topology on the transformations introduced in the definition of a lattice. A definition of the topology, independent of a chosen basis, is the following: to each compact set H and neighborhood V of the origin corresponds a neighborhood of Λ, consisting of those lattices Λ' such that for each $y \in \Lambda \cap H$ there is an $x \in \Lambda'$ such that $x - y \in V$, and for each $x \in \Lambda' \cap H$ there is a $y \in \Lambda$ such that $x - y \in V$ (cf. C. Chabauty [1]).

If S is any open set, we say that Λ is *admissible for* S if S contains no point of Λ except possibly the origin. Since a lattice of determinant δ in K^n corresponds to one of determinant Norm δ in R^{mn}, Minkowski's convex body theorem gives us a lower bound for $|\text{Norm } \delta|$ over all lattices admissible for some fixed neighborhood of the origin.

THEOREM 2. *Let S be a neighborhood of the origin; then there is a constant $c(S)$ such that any lattice admissible for S has*

$$|\text{ Norm } \delta| \geqq c(S) > 0.$$

Moreover, if S is convex and centrally symmetric, then $c(S) \geqq 2^{-mn} V$, where V is the measure (in R^{mn}) of S.

A *distance-function* is a continuous mapping, f, from K^n to the reals such that:

(a) $f(x) \geqq 0$ for all $x \in K^n$, and $f(x) > 0$ for some x;

(b) $f(tx) = |t| f(x)$ for all points x and all real t. For any real $M > 0$ the open set defined by $f(x) < M$ is called a *star-body*. It is convex if $f(x+y) \leqq f(x) + f(y)$ for all x, y in K^n. Now let S be a bounded star-body, and write λS for the dilation of S in the ratio λ:1, where λ may be any positive number or an element of K^*. For a given lattice Λ we define the rth successive minimum of S with respect to Λ as the greatest real $\lambda = \lambda_r$ such that the points of $\lambda S \cap \Lambda$ lie in an $(r-1)$-dimensional linear space. As preliminary to the

analogue of Theorem 2 for successive minima, we prove the following lemma.

LEMMA 2. *Let the points $P_1, \cdots, P_n$ of Λ be boundary points respectively of $\lambda_1 S, \cdots, \lambda_n S$, so chosen as to be linearly independent, where S is a star body; and let Λ' be the lattice generated by $P_1, \cdots, P_n$. Then Λ/Λ' is a finite group whose order is bounded by a constant depending only on S.*

Proof. The only part needing proof is the bound on the order. Suppose that $\mu_1, \cdots, \mu_m$ is a basis for K over the rationals and so also for K^* over the reals. Multiplying them by small enough rational numbers, we may suppose that the convex closure of $\mu_i S$ is in S for all μ_i. Now consider the convex closure of the set of points $\pm\mu_i P_j$. The measure of the corresponding set of points in R^{mn} is $\mu[\Lambda:\Lambda']^m|\text{Norm } \delta|$, where $\mu>0$ depends only on the μ_i. Moreover, this region contains no point of Λ except the origin in its interior; for suppose P were such a point and choose r such that P is linearly dependent (over K) on $P_1, \cdots, P_r$ but not on $P_1, \cdots, P_{r-1}$. Then P lies in the convex closure of the $\pm\mu_i P_j$ $(j \leqq r)$ and so in the interior of $\lambda_r S$; and this contradicts the definition of λ_r.

Thus we can apply the last part of Theorem 2 to the region just defined, obtaining

$$2^{-mn}\mu[\Lambda:\Lambda']^m|\text{ Norm } \delta| \leqq |\text{ Norm } \delta|,$$

which proves that $[\Lambda:\Lambda']$ is bounded.

We now prove the *successive minima theorem.*

THEOREM 3. *Let S be a star body; then there is a constant $c(S)>0$ such that the successive minima of S with respect to any lattice Λ satisfy*

$$|\text{ Norm } \delta| \geqq c(S)(\lambda_1 \cdots \lambda_n)^m.$$

Proof. Replacing S by a smaller region if necessary, we may assume that it is a bounded convex star body. We use the notation of Lemma 2. Since $\lambda_1 \leqq \lambda_2 \leqq \cdots$, we can choose rational integers $a_1, a_2, \cdots$ such that

$$\lambda_{r+1}/\lambda_r \leqq a_r \leqq 2\lambda_{r+1}/\lambda_r.$$

We write $b_r = a_r a_{r+1} \cdots a_{n-1}$. Suppose that Λ'' is the lattice generated by the $\pm b_i P_i$, so that $[\Lambda':\Lambda''] = b_1 b_2 \cdots b_n$; then Λ'' is admissible for $\lambda_n S$. For if not, let P be a point of Λ'', other than the origin, in $\lambda_n S$, and suppose that P is linearly dependent (over K) on $P_1, \cdots, P_r$ but not on $P_1, \cdots, P_{r-1}$. Then P is linearly dependent (over $\mathfrak{O}$) on the $\pm b_i P_i$ $(i \leqq r)$, and is therefore b_r times a point of Λ', since every b_i divides all its predecessors. But since $b_r \geqq \lambda_n/\lambda_r$, this point of Λ' must be in the interior of $\lambda_r S$, which contradicts the definition of λ_r.

Applying Theorem 2 to Λ'' and $\lambda_n S$, we have

$$[\Lambda:\Lambda']^m[\Lambda':\Lambda'']^m|\text{ Norm } \delta| \geqq \lambda_n^{mn} c_1(S).$$

But $[\Lambda:\Lambda']$ is bounded, by Lemma 1, and

$$[\Lambda':\Lambda''] = b_1 \cdots b_n \leqq 2^{n(n-1)/2}\lambda_n^{n-1}/\lambda_1\lambda_2 \cdots \lambda_{n-1},$$

by the original condition on the a_r. Combining these results we obtain the theorem.

The greatest possible value of $c(S)$ in Theorem 2 is called the *lattice constant of* S, and lattices admissible for S for which $|\text{Norm } \delta|$ attains its minimum value are called *critical*. A similar terminology could be used for Theorem 3. We now prove the analogue of the Mahler compactness theorem.

THEOREM 4. *Let S be a neighborhood of the origin and $\{\Lambda_i\}$ an infinite sequence of lattices satisfying*

(a) *Λ_i is admissible for S;*

(b) *there is a constant M such that $|\text{Norm } \delta_i| \leqq M$ for all i. Then there is a subsequence of the Λ_i which converges to a limit lattice Λ, and Λ is admissible for S and satisfies $|\text{Norm } \delta| \leqq M$.*

Proof. If Λ is the limit of a sequence of Λ_i, then every point of Λ other than the origin is the limit of a sequence of points other than the origin from the Λ_i. Since S is open and the Λ_i are admissible for S, so is Λ.

In proving the remainder of the theorem we may replace S by a smaller neighborhood, and so we may assume that S is a bounded convex star body. We use the notation of Lemma 2 and Theorem 3, and superscripts indicate the λ and P relating to Λ_i. Now the upper bound on $|\text{Norm } \delta_i|$ and the lower bound on $\lambda_1^{(i)}$ imply an upper bound on $\lambda_n^{(i)}$ independent of i; thus the $P_j^{(i)}$ lie in a region bounded independently of i. By taking a subsequence, we can assume that $P_j^{(i)} \to P_j$, for each j, as $i \to \infty$. Now by Lemma 2 we can find a rational integer N such that $N\Lambda_i \subset \Lambda_i'$ for each i, whence every point in Λ_i can be written as $\sum_{j=1}^{n} (u_j/N)P_j^{(i)}$ for some integers $u_1, \cdots, u_n$ of K. Thus Λ_i is specified by the $P_j^{(i)}$ and certain vectors $(u_1, \cdots, u_n)$ of integers of K. These vectors fall into complete residue classes modulo N, and there are therefore only a finite number of possibilities for the set of all such vectors. By choosing a subsequence of the Λ_i we can assume that they all have the same set of permissible vectors $(u_1, \cdots, u_n)$. Then clearly the Λ_i converge to the lattice Λ which consists of all the points $\sum(u_j/N)P_j$, where $(u_1, \cdots, u_n)$ runs through all permissible vectors. This proves the theorem.

An alternative proof could be given by using the compactness theorem for ordinary lattices in R^{mn}; that the resulting lattice in R^{mn} gives rise to a lattice in K^n follows easily from Theorem 1 and its Corollary.

Theorem 4 does not necessarily depend on Theorem 3; for we can construct a proof along the lines of that given by Chabauty [1] for Mahler's original theorem. To prove that the resulting limit set is a lattice not merely in Weyl's sense but in ours, we may either use Theorem 1 or an argument similar to that in the proof above.

4. The proofs of Mahler's principal theorems now carry over without substantial change.

THEOREM 5. *Let S be a neighborhood of the origin. Then if S has admissible lattices it also has critical ones.*

We say that S is *automorphic* if there is a bounded region T such that to any $P \in S$ we can find an automorphism of S taking P into a point of T. As in Mahler's paper, one can deduce the following:

COROLLARY. *If S is automorphic, then among the critical lattices of S there is at least one which contains boundary points of S.*

There is an exactly analogous theory for inhomogeneous lattices (cf. Swinnerton-Dyer [9]). We shall define an exterior boundary point of S as a point P on the boundary of S such that the interval OP contains points of S arbitrarily close to P.

THEOREM 6. *Let S be automorphic and such that any line through any point of the closure of the set of exterior boundary points of S contains points of S. Then the inhomogeneous lattice constant of S is not zero; and if S has admissible lattices it also has critical lattices.*

This theorem holds a fortiori for homogeneous lattices. In the same way we can prove:

THEOREM 7. *Let S be an open set. Then a sufficient condition for S to have nonzero lattice constant is that every line through O contains points of S; and in this case S will have critical lattices whenever it has admissible ones. If S is bounded, the condition is also necessary.*

We conclude this section by considering the analogous problems for the product of successive minima. We write

$$c(S, \Lambda) = \frac{|\operatorname{Norm} \delta|}{(\lambda_1 \cdots \lambda_n)^m},$$

and call any lattice for which $c(S, \Lambda)$ attains its minimum critical. We shall write $c(S) = \operatorname{Min} c(S, \Lambda)$.

LEMMA 3. *Let S be a bounded star body. Then there is an N_0 with the following property: to any lattice Λ we can find Λ' so that $c(S, \Lambda') \leqq c(S, \Lambda)$ and $\lambda_i' \leqq N_0 \lambda_{i-1}'$ for $1 < i \leqq n$.*

Proof. We use the ideas of Lemma 2. Let $P_1, \cdots, P_n$ be linearly independent points on the boundaries respectively of $\lambda_1 S, \cdots, \lambda_n S$; and let Λ'' be the lattice generated by $P_1, \cdots, P_n$. Then by Lemma 2 we have $[\Lambda : \Lambda''] \leqq N_0 - 1$, say. Let us write $[\Lambda : \Lambda''] = N$, and suppose that $\lambda_r > (N+1)\lambda_{r-1}$. We know (as in the proof of Theorem 4) that Λ is determined by $P_1, \cdots, P_n$

and a certain set of vectors $(u_1, \cdots, u_n)$. Let Λ''' be determined from the points $(N+1)P_1, \cdots, (N+1)P_{r-1}, P_r, \cdots, P_n$ and the same set of vectors $(u_1, \cdots, u_n)$. Since the points of Λ are just the $\sum(u_j/N)P_j$, and since the u_j form complete cosets modulo N, it is clear that

$$\Lambda \supset \Lambda''' \supset (N+1)\Lambda.$$

Hence $\lambda_i \leqq \lambda_i''' \leqq (N+1)\lambda_i$; and clearly we have $\lambda_i''' = (N+1)\lambda_i$ for $i<r$. Also $\delta''' = (N+1)^{r-1}\delta$. It follows that $c(S, \Lambda''') \leqq c(S, \Lambda)$ and

$$c(S, \Lambda)\left(\frac{\lambda_n}{\lambda_1}\right)^m \geqq (N+1)^m c(S, \Lambda''')\left(\frac{\lambda_n'''}{\lambda_1'''}\right)^m.$$

Since the left side is, for all Λ, bounded below by $c(S)$, this process can only be repeated a finite number of times; and clearly the lattice Λ' which we finally obtained satisfies all the conditions of the lemma.

THEOREM 8. *If S is a bounded star body, then there exist critical lattices for the problem of successive minima with respect to S.*

Proof. In view of Lemma 3, we can find a sequence of lattices $\Lambda^{(i)}$ such that $c(S, \Lambda^{(i)}) \to c(S)$ and the ratio $\lambda_n^{(i)}/\lambda_1^{(i)}$ remains bounded. Multiplying the lattices by suitably chosen real numbers, we may assume that $|\text{Norm } \delta^{(i)}|$ is constant also. It now follows from the definition of $c(S, \Lambda)$ that $\lambda_1^{(i)}$ is bounded below by a strictly positive number; that is, there is a λ such that all the $\lambda^{(i)}$ are admissible for λS. Now by Theorem 4 there is a subsequence of the $\Lambda^{(i)}$ which tends to a limit lattice Λ, and clearly $c(S, \Lambda) = c(S)$. This proves the theorem.

The theorem, as also Lemma 3, remains true if we drop the condition of boundedness. Our proof of this, however, depends on special properties of algebraic number fields and is not suited to the view-point of the present paper.

5. We now consider the question of isolation of an admissible lattice. It is usual in this context to suppose the star body fixed and to vary the lattice. We shall, however, find it advantageous to work the opposite way; and so we must first set up a topology on the set of all star bodies. Let $f(x)$ be a distance function which vanishes only at the origin; then the set F of points defined by $f(x) = 1$ is closed and compact, and has just one point on every semi-infinite ray ending at the origin. If g_1 and g_2 are two distance functions, then we define our metric on the set of all distance functions by

$$\|g_1 - g_2\| = \operatorname*{Max}_{P \in F} |g_1(P) - g_2(P)|.$$

This gives a topology on the set of all star-bodies, of course. It is easy to verify that this topology does not depend on f, though the original metric does. Moreover, if S is any star-body and $\mathfrak{S}$ the set of star-bodies obtainable

from S by linear transformations (whose image transformation in R^{mn} is nonsingular), the restriction of our given topology to $\mathfrak{S}$ is the same as the topology induced on $\mathfrak{S}$ by the natural topology on the linear transformations. In particular, $\mathfrak{S}$ is locally compact.

We now set up a partial ordering in the set of all star-bodies, saying that S_1 majorizes S_2, written $S_1 \succ S_2$, if there is a $\lambda > 0$ such that $\lambda S_1 \supset S_2$. This clearly implies that the distance function of S_2 can vanish only at points where the distance function of S_1 vanishes.

Now let S be a star-body, Λ a lattice admissible for S, and $\mathfrak{S}$ any set of star-bodies containing S. (In all cases of interest, $\mathfrak{S}$ will be invariant under linear transformations and locally compact: for the usual definition of "isolated," $\mathfrak{S}$ is to be taken as the set of all permissible linear transforms of S.) We say that Λ is *an isolated admissible lattice of* S (*relative to* $\mathfrak{S}$) if there is a neighborhood of S in $\mathfrak{S}$ and a $\lambda > 1$ such that the only bodies in the neighborhood of S for which $\lambda\Lambda$ is admissible are those majorized by S. Similarly, we say that Λ is a *strongly isolated* admissible lattice of S with respect to $\mathfrak{S}$ if for every $\lambda > 1$ there is a neighborhood with the property as before. This is the most we can demand([3]); for if $S > S_1$ and Λ is admissible for S, then for some $\lambda > 0$, $\lambda\Lambda$ is admissible for S_1.

It is clear that to prove isolation we have to consider the positions of an infinity of points of Λ relative to S; and we are therefore led to consider the group G of those linear transformations which leave both Λ and S invariant.

For any positive integer n we define a distance function of degree n as the nth power of a distance function. Let f be the distance-function of degree n for S, f_1 that for some S_1 in $\mathfrak{S}$, and $g_1 = f - f_1$. The S_1 majorized by S are those for which f_1 is bounded below on the boundary of S, or for which g_1 is bounded above by a constant strictly less than 1. The following lemma is virtually trivial; at the same time it gives an effective criterion for isolation.

LEMMA 4. *Let* $\delta > 0$ *have the following property: there is a point* P *of* Λ *and a transformation* $T \in G$ *such that* $Tg_1(P) > \delta$. *Then* $\lambda\Lambda$ *is not admissible for* S_1 *if* $\lambda^n < (f(P) - \delta)^{-1}$.

COROLLARY 1. *Suppose there is a neighborhood of* S *in* $\mathfrak{S}$ *and a* $\delta > 0$ *such that: to each* S_1 *in the neighborhood not majorized by* S *we can find a* $T \in G$ *and a* $p \in \Lambda$ *with the properties* $f(P) = 1$, $Tg_1(P) > \delta$. *Then* Λ *is isolated.*

COROLLARY 2. *Suppose that to each* $\delta > 0$ *we can find a neighborhood of* S *in* $\mathfrak{S}$ *such that: to each* S_1 *in the neighborhood not majorized by* S *we can find a* $T \in G$ *and a* $P \in \Lambda$ *with the property that* $Tg_1(P) > f(P) - \delta$. *Then* Λ *is strongly isolated.*

([3]) The reader should note that, with our definition, if $\mathfrak{S}$ is the set of all bounded star bodies, then any lattice admissible for S is strongly isolated in $\mathfrak{S}$; for all bounded star bodies majorize one another. This is not the normal usage.

In practice we choose P from a finite set and rely on the choice of T to give $Tg_1(P)$ the proper value.

Suppose further that the distance function of degree n is of the form $|\text{Norm } \phi|$, where ϕ is a homogeneous function with values in K^*, for all the star bodies in $\mathfrak{S}$. Then we write $\psi=\phi-\phi_1$ and have

LEMMA 5. *Let $P_1, \cdots, P_r$ be points of Λ such that to any neighborhoods of the $\phi(P_i)$ we can find a neighborhood of S in $\mathfrak{S}$ such that: to each S_1 in the neighborhood not majorized by S we can find a T leaving ϕ and Λ invariant and P_i such that $T\psi_1(P_i)$ is in the given neighborhood of $\phi(P_i)$. Then Λ is strongly isolated.*

LEMMA 6. *Let $P_1, \cdots, P_r$ be points of Λ on the boundary of S, and suppose there are closed neighborhoods of the $\phi(P_i)$ contained in the respective open sets defined by $|\text{Norm } (\phi(P_i)-x)|<1$. Suppose that to each S_1 in a small enough neighborhood of S not majorized by S we can find a T leaving ϕ and Λ invariant and a P_i such that $T\psi_1(P_i)$ is in the given neighborhood of $\phi(P_i)$. Then Λ is isolated.*

In view of our preceding remarks, the natural body to consider in this context is that given by

$$|\text{Norm } (X_1X_2\cdots X_n)| < 1, \qquad (n>1).$$

The simple way to generate admissible lattices for this region is as follows: choose any relatively real extension L of degree n over K and take X_1 to be a linear form over K with coefficients in L which does not represent zero non-trivially. Now we take $X_2, \cdots, X_n$ to be the relative conjugates of X_1 over K. The resulting lattice or dilation thereof is admissible for the region cited. We define $\mathfrak{S}$ as the set of all star-bodies given by $|\text{Norm } \phi|<1$ where ϕ is a polynomial of degree n in the X_i. Except in the special case when $n=2$ and K is a complex quadratic field, this is the only way we have of constructing admissible lattices; and it follows easily from Lemma 3 that all such lattices are strongly isolated.

We now consider the exceptional case. We are concerned with $\phi=\alpha X_1^2+X_1X_2+\beta X_2^2$, where α and β are small; and the transformations of G are of the form $x_1\to\lambda x_1$, $x_2\to\lambda' x_2$, with Norm $\lambda\lambda'=1$, λ and λ' conjugate integers of L. The possible values of λ are powers μ^n of a particular value μ, and we shall assume $\mu\mu'=1$—at worst at the cost of increasing the number of P_i used in Lemma 4. Now Λ is isolated, if we can choose, for any small α, an integer n and a point P_i such that at P_i

$$|X_1X_2| = 1, \qquad |\alpha\mu^{2n}X_1^2+X_1X_2| < 1-\delta.$$

We can certainly do this if μ^2 is not real (and indeed with only one P_i). If μ^2 is real and negative, we have trouble with those values of α for which

$\alpha X_1/X_2$ is almost pure imaginary. Thus in this case Λ is certainly isolated if there are points P_1, P_2 of Λ on the boundary of S such that

$$X_1(P_1)\cdot X_2(P_2)/X_2(P_1)\cdot X_1(P_2)$$

is not real. Finally, suppose that μ^2 is real and positive. In this case Λ is certainly isolated if we can find $P_1, \cdots, P_r$ of Λ on the boundary of S such that any angle is strictly within $\pi/2$ of some $\arg(X_1(P_i)/X_2(P_i))$. The remaining cases we cannot handle; but we expect that Λ will usually not be isolated.

6. We now turn to bounded convex star bodies. Two points P_1, P_2 on the boundary of S are called *equivalent* if there is an integer (always a unit) α of K such that $\alpha S=S$ and $P_1=\alpha P_2$. We define an admissible lattice Λ of S to be *extremal* if all admissible lattices for S near enough to Λ to have a value for Norm(determinant) at least as large as that for Λ.

THEOREM 9. *If Λ is extremal for the convex, bounded star-body S, then there are at least $n(mn+r)/2$ inequivalent points of Λ on the boundary of S.*

Proof. We take coordinates such that Λ is the unit lattice, generated by $(1, 0, \cdots, 0), \cdots, (0, \cdots, 0, 1)$ and Λ' is a nearby lattice generated by $(1+a_{11}\delta, a_{12}\delta, \cdots, a_{1n}\delta)$, etc. Here the a_{ij} are in K^* with $a_{ij}=\bar{a}_{ji}$, and δ is real (and will be made arbitrarily small). Now

$$\text{Det } \Lambda' = \begin{vmatrix} 1+a_{11}\delta, \cdots, a_{1n}\delta \\ \cdots\cdots\cdots \\ a_{n1}\delta, \cdots, 1+a_{nn}\delta \end{vmatrix} = 1 + A\delta + B\delta^2 + \cdots,$$

where

$$A = a_{11} + a_{22} + \cdots + a_{nn}, \qquad B = \sum_{i<j} a_{ii}a_{jj} - \sum_{i<j} a_{ij}a_{ji}.$$

Let $A_1, \cdots, A_n$ be the conjugates of A; then

$$\text{Norm (Det } \Lambda') = 1 + \delta \text{ Spur } A + \delta^2\left(\sum_{i<j} A_iA_j + \text{Spur } B\right) + \cdots.$$

But

$$\begin{aligned}(\text{Spur } A)^2 &= \sum A_i^2 + 2\sum_{i<j} A_iA_j \\ &= 2\sum_{i<j} A_iA_j + 2\,\text{Spur}\sum_{i<j} a_{ii}a_{jj} + \text{Spur}\sum a_{ii}^2,\end{aligned}$$

so that

$$\sum A_iA_j + \text{Spur } B - \frac{1}{2}(\text{Spur } A)^2 = \text{Spur}\left(-\frac{1}{2}\sum a_{ii}^2 - \sum_{i<j} a_{ij}\bar{a}_{ij}\right).$$

It follows that for a suitable choice of sign δ and all small enough $|\delta|$ we have Norm (Det Λ') $\leqq$ Norm (Det Λ), with equality only when $\Lambda=\Lambda'$. If Λ is extremal, then it follows that Λ' must be inadmissible. Now let $P_1, \cdots, P_N$ be the inequivalent lattice points of Λ on the boundary of S. We impose on Λ' the further conditions that each corresponding P_i' lies on a tac-plane to S through P_i, the tac-plane being defined as usual in the image in R^{mn}, so that this gives N homogeneous equations in the real parameters (independent of δ). These N conditions must constrain Λ' to be Λ; and since Λ' has $mn(n-1)/2 + n(r+s)$ disposible real parameters, this proves the theorem.

An important special case is when K is complex quadratic and S is the sphere $X_1\overline{X}_1+ \cdots + X_n\overline{X}_n<1$; in other words the problem of the minimum of a positive definite Hermitian form. By analogy with the well-known results of Korkine and Zolotareff we show that here the lattice points of Λ on the boundary of S are enough to determine S.

We may assume the coordinates so chosen that S is $\sum x_i\bar{x}_i<1$, and we denote the points of Λ on the boundary of S by superfixes. We wish to show that the only Hermitian matrix (a_{ij}) satisfying

$$\sum a_{ij}x_i^{(r)}\bar{x}_j^{(r)} = 1, \qquad (r = 1, \cdots, N)$$

is the unit matrix. Suppose this were false; then we could find an Hermitian $(\lambda_{ij}) \neq (0)$ with

$$\sum \lambda_{ij}x_i^{(r)}\bar{x}_j^{(r)} = 0,$$

and it would follow that for small enough real δ, of either sign, Λ would be admissible for

$$\sum x_i\bar{x}_i + \delta \sum \lambda_{ij}x_i\bar{x}_j < 1.$$

But this is a positive definite Hermitian form whose determinant, for suitable choice of δ, is strictly less than 1 (by the same calculation as we performed earlier); and it follows that Λ is not extremal. In view of this contradiction, we conclude that the points of Λ on the boundary of S are enough to determine S.

One of us [8] has used this and analogues of other results of Korkine and Zolotareff [3] to prove:

THEOREM 10. *Let $f(x) = \sum_{i,j=1}^{3} a_{ij}x_i\bar{x}_j$ be a positive definite ternary Hermitian form of determinant D. Then there exist integer values of (x) in $Q(i)$, not all zero, such that*

$$f(x) \leqq (4D)^{1/3}.$$

The sign of equality is necessary only for forms equivalent to a multiple of

$$x_1\bar{x}_1 + x_2\bar{x}_2 + x_3\bar{x}_3 + \frac{1}{2}(x_2\bar{x}_3 + \bar{x}_2x_3) + \frac{1}{2}(x_3\bar{x}_1 + \bar{x}_3x_1)$$
$$+ \frac{1}{2}(1+i)x_1\bar{x}_2 + \frac{1}{2}(1-i)\bar{x}_1x_2.$$

7. We consider now the star body defined by

$$|\text{Norm } X_i| < 1, \qquad (i = 1, \cdots, N).$$

Except when K is complex quadratic, this is unbounded; we shall see however that it behaves in every way like a bounded star-body, and that for example none of its admissible lattices is isolated. We shall also give an algorithm for finding its extremal lattices in any particular case.

Let λ denote any unit of K. Then S is automorphic under the group of transformations $X_i \to \lambda X_i$; and since this transformation is simply $P \to \lambda P$ it leaves all lattices in K^n invariant. Hence there is a bounded portion of S, which we call S', such that every lattice admissible for S' is admissible for S; and if Λ is admissible for S the number of inequivalent points of Λ on the boundary of S is finite.

Now let Λ be extremal for S, and consider the effect of replacing X_1 by $X_1 + \mu_2X_2 + \cdots + \mu_nX_n$, where $\mu_2, \cdots, \mu_n$ are small numbers in K^*. If the resulting body is still to have Λ an admissible lattice we have only to consider the points of Λ on the face

$$|\text{Norm } X_1| = 1, \qquad |\text{Norm } X_r| < 1 \qquad (r = 2, \cdots, n)$$

of S. Suppose that these points are insufficient to determine X_1 uniquely in a neighborhood of its actual "value." Denoting by superfixes values at the points of Λ we are concerned with, we would deduce that the tac-planes at the origin in the μ-space to the surfaces

$$|\text{Norm } (X_1^{(i)} + \mu_2X_2^{(i)} + \cdots + \mu_nX_n^{(i)})| = |\text{Norm } X_1^{(i)}|$$

have at least a line in common. But on such a tac-plane,

$$|\text{Norm } (X_1^{(i)} + \mu_2X_2^{(i)} + \cdots + \mu_nX_n^{(i)})| < |\text{Norm } X_1^{(i)}|$$

unless

$$\mu_2X_2^{(i)} + \cdots + \mu_nX_n^{(i)} = 0.$$

It now follows that, for some t, the lattice points on any face of S lie on an $(n-t)$-dimensional space through the origin and determine X up to addition of some linear function vanishing on the $(n-t)$-dimensional space. From this we can for any particular n deduce an algorithm for finding the lattice constant of the region. Though tedious for the hand, this algorithm appears

well suited for electronic computation.

Particularly simple is the case $n=2$. Now either (i) both sides are determined by the lattice points on them, or (ii) the lattice includes a point at which $|\text{Norm } X_1| = 1$, $X_2 = 0$. We have used these results to derive simpler proofs for Minkowski's results concerning two linear forms with variables integers of either $Q(i)$ or $Q(\rho)$, where $\rho = \exp 2\pi i/3$, and have published some details for the case of $Q(i7^{1/2})$, [7]. We now give some details of the proof of the result for the field $Q(i5^{1/2})$, when $h=2$.

THEOREM 11. *Let $\xi = ax+by$, $\eta = cx+dy$, where a, b, c, d are complex numbers and $ad-bc=\Delta \neq 0$. Then there exist integers x, y of $Q(i5^{1/2})$, not both zero, such that*

$$\max(|\xi|, |\eta|) \leqq \left(\frac{2|\Delta|}{(15)^{1/2}-3}\right)^{1/2} = \mu,$$

say. The sign of equality is necessary only for forms which, apart from unimodular factors, can be reduced by unimodular transformations in $Q(i5^{1/2})$ to $\mu\xi_0$, $\mu\eta_0$, where

$$\xi_0 = i\frac{5^{1/2}-3^{1/2}}{2}x + \frac{-3+(15)^{1/2}+i(3^{1/2}-5^{1/2})}{2}y,$$

$$\eta_0 = x + \frac{-1+i3^{1/2}}{2}y.$$

Proof. The method is, of course, to use the conditions for an extremal lattice for the region S, $\max(|X_1|, |X_2|)<1$ to reduce the problem to a finite, but very tedious, process of elimination. By Minkowski's theorem we show that an admissible lattice of determinant Δ has $|\Delta|^2 > \pi^2/80$, while the upper bound 2 for $|\det(P_1, P_2)|$ gives $|\Delta| \cdot |E| \leqq 2$, where P_1, P_2 are lattice points on the boundary of S, of determinant E relative to the lattice. Hence $|E|^2 < 320/\pi^2$, giving only a finite number of values for the integer E. If we tabulate the integer pairs which give lattice-points on the boundary, we note that right-multiplication by unimodular matrices corresponds to a change of lattice basis, and hence we can reduce at least two rows of the array to a finite number of cases if we show that there is only a finite number of sub-lattices of the integer lattice of given determinant. The last statement is trivial, for $n \times n$ matrices and any field, by congruence considerations modulo the determinant, but special methods for our case give an explicit reduction process. Clearly, each integer pair generates the ideal of smallest norm in its class, that is either (1) or $(2, 1+i5^{1/2})$; and a result of one of us [6] shows not only that one row may be taken as either (1, 0) or $(2, 1+i5^{1/2})$, but also that in the second case a row which with 2, $1+i5^{1/2}$ makes a determinant E can have its first element reduced mod E while 2, $1+i5^{1/2}$ remains unchanged. In principle, we have reduced the array to a finite number of cases.

The mechanics of elimination of cases has been illustrated in the case of $Q(i7^{1/2})$, [7]. Two results which help to reduce the work are given there without proof. One is an obvious analogue ("Lemma 4") of a result of Minkowski, the other ("Lemma 5") is quite easy to verify. Using these techniques we find, after a huge amount of computation, that the critical lattice is given by taking the integer pairs (1, 0), (0, 1) and (1, 1) to make $|\eta| = 1$, $|\xi| < 1$, and the pairs $(2, 1+i5^{1/2})$, $(-1-i5^{1/2}, 1-i5^{1/2})$ and $(1-i5^{1/2}, 2)$ to make $|\xi| = 1$, $|\eta| < 1$. These give the forms ξ_0, η_0 of the theorem, of determinant of absolute value $1((15)^{1/2}-3)/2$.

References

1. C. Chabauty, *Limite d'ensembles et Géométrie des Nombres*, Bull. Soc. Math. France vol. 77 (1950) pp. 143–151.

2. G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Zeit. vol. 47 (1942) pp. 427–462.

3. A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. vol. 11 (1877) pp. 242–292.

4. K. Mahler, *On lattice-points in n-dimensional star-bodies*, Proc. Royal Soc. London. Ser. A vol. 187 (1946) pp. 151–187.

5. H. Minkowski, *Diophantische approximationen*, Leipzig, B. G. Teubner, 1907, Chapter 6.

6. K. Rogers, *On the generators of an ideal*, Amer. J. Math. vol. 77 (1955) pp. 621–627.

7. ———, *Complex homogeneous linear forms*, Proc. Cambridge Philos. Soc. vol. 52 (1955) pp. 35–38.

8. ———, Cambridge Ph.D. Thesis, 1954, Chapter III.

9. H. P. F. Swinnerton-Dyer, *Inhomogeneous lattices*, Proc. Cambridge Philos. Soc. vol. 50 (1954) pp. 20–25.

10. H. Weyl, *Theory of reduction for arithmetical equivalence*, Trans. Amer. Math. Soc. vol. 48 (1940) pp. 126–164, and vol. 51 (1942) pp. 203–231.

Harvard University,
Cambridge, Mass.
Trinity College,
Cambridge, England