A CLASS OF GEOMETRIC LATTICES

K. ROGERS AND E. G. STRAUS

Communicated by E. F. Beckenbach, December 26, 1959

1. **Introduction.** By an n-dimensional lattice Λ we mean, as usual, an additive subgroup with n linearly independent generators of the vectors in Euclidean n-space, R^n. If we denote by Z^n the lattice of vectors with integral components, then Λ is the image of Z^n under a nonsingular linear transformation:

$$\Lambda = \{Au \mid u \in Z^n\}, \qquad \det A \neq 0.$$

The matrices mapping Z^n onto Λ constitute a coset AU of the subgroup of all integral unimodular matrices, and so $\det \Lambda = |\det A|$ is well-defined. It is convenient to use the same name Λ for the point-lattice of all points P such that OP is in Λ.

Minkowski [2] showed that every lattice of determinant one contains a point other than the origin 0 in the cube

$$\{(x_1, \cdots, x_n) \mid |x_i| \leqq 1, i = 1, \cdots, n\},$$

and that the same holds if any $n-1$ of the signs are replaced by strict inequality. Those unimodular lattices, such as Z^n, which have only the origin in common with the open cube shall be called *critical*, as shall the corresponding matrices. Minkowski conjectured, and Hajos [1] proved in 1938, that a critical lattice must contain one of the points $(\delta_{i1}, \cdots, \delta_{in})$, $i = 1, \cdots, n$. If A is critical then so is any matrix obtained from it by permuting rows and post-multiplication by integral unimodular matrices: such matrices will be called *equivalent* to A. An induction argument shows that Hajos' theorem is the same as the assertion:

A is critical if and only if it is equivalent to a matrix with ones on the diagonal and all zeros above.

Siegel [3] tried to prove Minkowski's conjecture by showing that, if A is critical, then each point other than 0 of the lattice corresponding to A has at least one coordinate in Z^*, the set of nonzero integers. If we consider the set of matrices A defined by the property

(P) $\qquad u \in Z^n, \qquad u \neq 0 \Rightarrow Au$ has a component in Z^*,

then Hajos' theorem would follow from Siegel's result, if it were true that every A with property (P) has an integral row. For in that case we could prove by induction on n that A is equivalent to a triangular matrix with zeros above the diagonal and positive integers on the

diagonal. Thus if $|\det A| = 1$, then the diagonal elements must be 1.

Conversely, since every A with property (P) and $|\det A| = 1$ is clearly critical, Hajos' theorem shows that the combination of (P) with $|\det A| = 1$ does imply that A has an integral row.

Unfortunately property (P) alone does not suffice for $n \geqq 5$ as is shown by the example

$$A = \begin{pmatrix} 1/3 & 0 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 & 0 \\ 1/2 & 3/2 & 3 & 0 & 0 \\ 1 & 3/2 & 0 & 3 & 0 \\ 3/2 & 1 & 0 & 0 & 3 \end{pmatrix}.$$

Here A has property (P) but no row is integral. However we were able to show that property (P) does imply that $\det A \in Z^*$ and to obtain various generalizations of that result.

2. The special case of the main theorem enunciated at the end of the introduction, when A is rational, is included in:

THEOREM I. *Let K be an algebraic number field of class-number one, and let J be its ring of integers. If an n-by-n matrix A over K has the property*

(P) $\qquad u \in J^n, \qquad u \neq 0 \Rightarrow Au$ *has a component in* J^*,

then $\det A \in J^*$.

PROOF. If A has property (P) then $\det A \neq 0$, so we only have to show that $\det A \in J$. The theorem being trivial for $n = 1$, we use induction. Take an A with (P) and assume that $\det A$ is not in J. We shall deduce the existence of an A with (P) such that $\det A = 1/q$, where q is a prime of J; and then a contradiction follows from a pseudo-analogue of Minkowski's theorem, which we shall prove.

LEMMA 1. *If there is an A with* (P) *such that* $\det A$ *is not in J, then there exists A_1 with* (P) *such that* $\det A_1 = a/q$, *where $a \in J$ and q is a prime of J which does not divide a.*

PROOF. Since J has unique factorization into primes and since $\det A$ is not integral, we have $\det A = a/qb$, where a, b, q are in J, q is a prime element, and $(a, qb) = J$. Multiplying the first row of A by b gives a matrix A_1 with (P) such that $\det A_1 = a/q$, as required.

It is easy to remove from each row of A any common denominator prime to q without affecting (P) or the fact that the determinant has

denominator q. Thus we may assume that: (i) A has property (P), (ii) $\det A = a/q$, where q is a prime not dividing a, (iii) some power of q is a denominator for A.

LEMMA 2. *If there is an A with properties* (i), (ii) *and* (iii), *then there exists an A with* (P) *such that* $\det A = 1/q$.

PROOF. Since J has only principal ideals, we can find an integral unimodular matrix U such that AU is triangular. By the properties of A we may write the diagonal elements of the new A as $a_{ii} = a_i q^{b_i}$, $a = \prod a_i$, $\sum b_i = -1$. Multiplying a column or a row of A by a non-zero integer does not affect (P). Hence, if A' is obtained from A by multiplying the first $n-1$ columns by a_n, then A' has (P) and only powers of q occur in the denominators in A'. Since a_n is prime to q, we get a matrix A'' with (P) when we divide each row of A' by a_n. The net result is that $a''_{ij} = a_{ij}$ if $(i, j) \neq (n, n)$, $a''_{nn} = q^{b_n}$. Similarly we can multiply the first $n-2$ columns by a_{n-1} and then divide the first $n-1$ rows by a_{n-1}, and so on. We end up with the matrix

$$A^* = \begin{pmatrix} q^{b_1} & 0 & \cdots & 0 \\ a_{21} & q^{b_2} & 0 \cdots & 0 \\ a_2 a_{31} & & \cdot & \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \\ a_2 \cdots & a_{n-1} a_{n1}, & \cdots, & q^{b_n} \end{pmatrix}$$

which has property (P) and determinant $q^{\sum b_i} = q^{-1}$, as required.

Since $|\text{norm } q^{-1}| < 1$, the desired contradiction follows from the next theorem.

THEOREM II. *If A is an n-by-n matrix over K such that $0 < |\text{norm } (\det A)| < 1$, then there exists $u \neq 0$ in J^n such that Au has no component in J^*.*

PROOF. Let d_i be a common denominator for the elements of the ith row of A, and let A_1 denote the matrix obtained by multiplying each row of A by its d_i. Then

$$0 < |\text{norm } (\det A_1)| = \left| \prod_i \text{norm } d_i \cdot \text{norm } (\det A) \right|$$

$$< \left| \prod_i \text{norm } d_i \right|.$$

Hence it is sufficient to prove:

LEMMA 3. *If B is an n-by-n matrix over J such that* $0 < |\text{norm}(\det B)| < \prod \text{norm } d_i$, *where the* $d_i \in J$, *then there exists a* $\mathbf{u} \neq \mathbf{0}$ *in* J^n *such that* $B\mathbf{u} = \mathbf{v}$, *where* $v_i = 0$ *or* $d_i | v_i$, *for each* i.

PROOF. Rado [4] has given a proof of Minkowski's theorem on linear forms which can easily be generalised to prove this lemma. We may assume B has been put in the form of a triangular matrix, with zeros above the diagonal and elements $a_1, \cdots, a_n$ on the diagonal. Hence $0 < |\prod_{i=1}^{n} \text{norm } a_i| < |\prod \text{norm } d_i|$. Let α_i, δ_i run over complete sets of residues mod a_i and mod d_i, respectively. Then the number of vectors $\boldsymbol{\alpha}$ is $|\prod \text{norm } a_i|$, and the number of $\boldsymbol{\delta}$ is $|\prod \text{norm } d_i|$. Thus, there are more vectors $\boldsymbol{\delta}$ than $\boldsymbol{\alpha}$. Now we assert that for given $\boldsymbol{\delta}$ there is one and only one $\boldsymbol{\alpha}$ such that the equation

$$B\mathbf{u} = \boldsymbol{\delta} + \boldsymbol{\alpha}$$

is solvable for $\mathbf{u} \in J^n$. For $n = 1$, the equation is $a_1 u = \delta_1 + \alpha_1$; and for given δ_1 this is solvable with integral u if and only if α_1 is in a certain residue class mod a_1, hence for one and only one α_1. Assuming the assertion true for $n-1$, we know that the first $n-1$ equations are solvable, for given $\delta_1, \cdots, \delta_{n-1}$, with integral $u_1, \cdots, u_{n-1}$ for one and only one $(\alpha_1, \cdots, \alpha_{n-1})$. Finally, for given δ_n, the equation

$$(b_{n1}u_1 + \cdots + b_{n,n-1}u_{n-1}) + a_n u_n = \delta_n + \alpha_n$$

is solvable with integral u_n for one and only one α_n, as in the case $n = 1$.

Since there are more $\boldsymbol{\delta}$ than $\boldsymbol{\alpha}$, we can find distinct $\boldsymbol{\delta}$, $\boldsymbol{\delta}'$ and some $\boldsymbol{\alpha}$ such that $B\mathbf{u} = \boldsymbol{\delta} + \boldsymbol{\alpha}$ and $B\mathbf{u}' = \boldsymbol{\delta}' + \boldsymbol{\alpha}$, where $\mathbf{u}$ and $\mathbf{u}'$ are in J^n. Since $\boldsymbol{\delta} \neq \boldsymbol{\delta}'$, therefore $\mathbf{u} - \mathbf{u}' \neq \mathbf{0}$ and $B(\mathbf{u} - \mathbf{u}') = \boldsymbol{\delta} - \boldsymbol{\delta}'$. Now δ_i, δ_i' are either equal or in distinct residue classes mod d_i; hence $\delta_i - \delta_i'$ is either zero or indivisible by d_i. This proves the lemma, with $\mathbf{v} = \boldsymbol{\delta} - \boldsymbol{\delta}'$, and also completes the proofs of Theorems I and II.

3. **Generalizations.** Theorem I holds without the restriction that the elements of A lie in K.

LEMMA 4. *Let K be any field with at least n elements, and let A be an n-by-n matrix over some K-module, such that*

$(\mathrm{P}')_n$ $\qquad \mathbf{u} \in K^n, \quad \mathbf{u} \neq \mathbf{0} \Rightarrow A\mathbf{u}$ *has a component in* K^*.

Then some row of A consists of elements of K, not all zero, and A is equivalent, under interchange of rows and right-multiplication by a non-singular matrix over K, to a triangular matrix whose diagonal elements are in K^*.

PROOF. Since the lemma is true for $n=1$, take $n\geqq 2$. If we write $L_i=\{u \mid u\in K^n,\ (Au)_i\in K\}$, then L_i is a subspace of K^n, and $L_i=K^n$ if the ith row of A is zero, an a priori possibility. Condition $(P')_n$ shows that K^n is the union of the L_i which correspond to a nonzero row of A. If one of these $L_i=K^n$, then the ith row of A is nonzero and all its elements are in K. Otherwise, we must have K^n equal to a union of at most n proper subspaces. We now show that this is impossible when $\#(K)\geqq n$. Suppose we have reduced down to the case $K^n=L_1\cup L_2\cdots\cup L_m$, with $m\leqq n$ and minimal. Hence there exist u, v in K^n such that u is not in $L_2\cup L_3\cdots\cup L_n$ and v is not in L_1. By intersecting each side of the above equation with the plane $Ku+Kv$, we find that the plane equals the union of at most n lines through the origin. This is clearly false if K is an infinite field; and in the case $q=\#(K)$, the total number of points would be $q^2=m(q-1)+1$, hence $m=q+1$, in contradiction to $q\geqq n\geqq m$.

We can now switch the row whose elements are in K to the first row and then by linear combinations of columns with coefficients from K reduce A to the form

$$\begin{pmatrix} a_1 & 0\cdots 0 \\ \cdot & \\ \cdot & B \\ \cdot & \end{pmatrix}$$

where $a_1\in K^*$. Since B has property $(P')_{n-1}$ we can now proceed by induction to prove the last part of the lemma.

COROLLARY. *If the field K in Lemma 4 is an algebraic number field of class-number one, then property* (P') *implies the equivalence of A to a triangular matrix with diagonal elements in K^* by switching of rows and right-multiplication by a unimodular matrix over J, the integers of K.*

PROOF. We again switch the row with elements in K to the first row. Since the class-number is one, we can form a linear combination of the columns with coefficients in J to give a new first column such that in the new matrix a_{11} divides all terms in the first row, i.e. $a_{1i}\in a_{11}J$, $i=1, 2, \cdots, n$. Then by subtracting integral multiples of the first column from other columns we can reduce a_{1i} to 0 for $i=2, \cdots, n$. The induction proceeds as before.

LEMMA 5. *If K is the field of Theorem* I, *A an n-by-n matrix over some K-module, K_1, and A has property* (P), *then there is a matrix A' over K with property* (P) *such that* $\det A=\det A'$.

PROOF. Since (P) implies (P'), we can triangularize A, as in the

corollary. We can regard A as being over the K-module obtained by adjoining the a_{ij} to K, say K'. If $1, \xi_1, \cdots, \xi_N$ be a basis for K' over K, then

$$A = A' + A_1\xi_1 + \cdots + A_N\xi_N,$$

say, where A' and the A_i are over K, all are triangular, the A_i having all zeros on the diagonal, while A' coincides with A on the diagonal. Hence $\det A = \det A'$. Finally, since

$$Au = A'u + \sum_{i=1}^{N} \xi_i(A_i u),$$

it is clear that A' also has property (P).

We have thus proved the desired generalization:

THEOREM I'. *Theorem* I *remains valid under the hypothesis that the matrix A is over some K-module.*

In particular, if A is over the reals and transforms every nonzero integer vector into a vector with at least one component in Z^*, then $\det A$ is in Z^*.

REFERENCES

1. G. Hajos, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Z., vol. 47 (1941) pp. 427–467.

2. H. Minkowski, *Geometrie der Zahlen*, Leipzig, Teubner, 1910, §30, p. 72.

3. C. L. Siegel, *Neuer Beweis des Satzes von Minkowski über lineare Formen*, Math. Ann. vol. 87 (1922) pp. 36–38.

4. R. Rado, *A proof of Minkowski's theorem on homogeneous linear forms*, J. London Math. Soc. vol. 9 (1934) pp. 164–165.

UNIVERSITY OF CALIFORNIA, LOS ANGELES