STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1961- 13 2

A Theorem on the distribution of lattices

C.G. Lekkerkerker

Reprinted from
Proceedings of the KNAW, Series A, 64(1961)
Indagationes Mathematicae, 23(1961), p 197-210

1961

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN – AMSTERDAM
Reprinted from Proceedings, Series A, **64**, No. 2 and Indag. Math., **23**, No. 2, 1961

MATHEMATICS

A THEOREM ON THE DISTRIBUTION OF LATTICES

BY

C. G. LEKKERKERKER

(Communicated by Prof. J. POPKEN at the meeting of November 26, 1960)

1. *Introduction*

Continuing work of FURTWÄNGLER, DAVENPORT [1] proved in 1955 a general theorem dealing with simultaneous diophantine approximation to r given real numbers. An important step in the proof of his theorem was the deduction of a certain approximation property of matrices. In terms of lattices this property is given by

Theorem 1a. *If Λ is a lattice in n-dimensional space, if $\varepsilon > 0$ and N is sufficiently large, then Λ has a basis of vectors $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that*

$$\mathfrak{b}_i = N(\mathfrak{e}_i + \mathfrak{d}_i) \qquad \text{for } i = 1, 2, \ldots, n-1,$$

where $\mathfrak{e}_i$ is the i-th unit vector and the coordinates of the vectors d_i $(i = 1, 2, \ldots, n-1)$ are of the form $O(N^{-1+\varepsilon})$.

At the end of his paper DAVENPORT formulates a dual result which concerns the approximation mod 1 to zero of one homogeneous linear form in r variables. He only sketches a proof of this result. At any rate, the main step of it, if enunciated in the terminology of lattices and bases thereof, is expressed by the following analogue of Theorem 1a:

Theorem 1b. *If Λ is a lattice in n-dimensional space, if $\varepsilon > 0$ and N is sufficiently large, then Λ has a basis of vectors $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that*

$$\mathfrak{b}_1 = N^{n-1}(\mathfrak{e}_1 + \mathfrak{d}_1), \;\; \mathfrak{b}_i = (1/N)(\mathfrak{e}_i + \mathfrak{d}_i) + \theta_i \mathfrak{b}_1 \quad (i = 2, 3, \ldots, n),$$

where $\theta_2, \ldots, \theta_n$ are real numbers and the coordinates of the vectors $\mathfrak{d}_1, \ldots, \mathfrak{d}_n$ are all of the form $O(N^{-1+\varepsilon})$.

In a lecture held at a symposium on number theory at Amsterdam, a year ago, Prof. MULLENDER suggested the problem of generalizing DAVENPORT's result to the case of the simultaneous approximation to zero of r homogeneous linear forms in s variables. In trying to solve this problem I found that the main difficulty lies in the generalization of the approximation properties of lattices enunciated above. In this paper I shall give such a generalization. In a subsequent paper the application to simultaneous diophantine approximation shall be dealt with.

The generalization as mentioned is illustrated by

Theorem 2. *Let Λ be a lattice in n-dimensional space and let r, s be positive integers with $r+s=n$. Let $\varepsilon>0$ and let N, M be sufficiently large positive numbers with $N^r M^{-s}=d(\Lambda)$. Then Λ has a basis of vectors $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that*

$$(1) \quad \begin{cases} \mathfrak{b}_i = N(\mathfrak{e}_i + \mathfrak{d}_i) & \text{for } i=1, 2, \ldots, r \\ \mathfrak{b}_i = \theta_{1i}\mathfrak{b}_1 + \ldots + \theta_{ri}\mathfrak{b}_r + (1/M)(\mathfrak{e}_i + \mathfrak{d}_i) & \text{for } i=r+1, \ldots, n, \end{cases}$$

where $\theta_{hi}(h=1, \ldots, r;\ i=r+1, \ldots, n)$ are real numbers and where the coordinates d_{hi} of the vectors $\mathfrak{d}_i$ satisfy

$$(2) \quad \begin{cases} d_{hi} = O(max(N^{-1+\varepsilon}, M^{-1+\varepsilon})) & \text{for } h, i=1, \ldots, r \text{ and for} \\ & \qquad h, i=r+1, \ldots, n \\ d_{hi}=0 \quad \text{for } h=1, \ldots, r;\ i=r+1, \ldots, n. \end{cases}$$

Contrary to the case of Theorem 1a, or Theorem 1b, there is nothing asserted about the last coordinates of $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$. I was unable to get here a restriction of the same type as for the other coordinates. But, fortunately, the values of these coordinates are irrelevant for the application, as has already been remarked by Davenport in the special case of Theorem 1a. As to the last relations (2), these are easily managed in the special cases. Thus, in the case $r=r$, $s=1$ of Theorem 1a we need only to write $\mathfrak{b}_n$ as a linear combination of $\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1}, \mathfrak{e}_n$. And in the case $r=1$, $s=r$ of Theorem 1b we can obtain, by suitable minor changes of the numbers θ_i, that the coordinates $b_{12}, \ldots, b_{1n}$ vanish, while the restrictions for the other coordinates remain valid.

In a less exact form, Theorem 2 says that *Λ has a basis $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_n\}$ such that, in the first r coordinates, the vectors $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ are approximately fixed (large) multiples of $\mathfrak{e}_1, \ldots, \mathfrak{e}_r$ and that, modulo the subspace generated by these first vectors $\mathfrak{b}_i$, the last ones are fixed (small) multiples of $\mathfrak{e}_{r+1}, \ldots, \mathfrak{e}_n$.* It is convenient to state Theorem 2 in terms of matrices also. Let X denote the $r \times s$-matrix of numbers θ_{hi}. Then it reads as follows.

Theorem 2′. *Let A be any real, non-singular $n \times n$-matrix and let $n=r+s$. Then, for $\varepsilon>0$ and sufficiently large N, M with $N^r M^{-s} = |\det A|$, there exists an integral unimodular matrix P such that AP has the form*

$$(3) \qquad AP = \begin{pmatrix} N(I_r+D) & N(I_r+D)X \\ Y & YX+M^{-1}(I_s+E) \end{pmatrix},$$

where I_r, I_s are the unit matrices of order r, s respectively, the elements of D and E are all of the form $O(\max(N^{-1+\varepsilon}, M^{-1+\varepsilon}))$ and X, Y are a certain $r \times s$-matrix, c.q. $s \times r$-matrix.

In the following we always *suppose*, as we may do, *that r and s are* $\geqq 2$.

Below we shall prove Theorem 2′. Roughly speaking, the proof will run along the following lines. Let Q denote the inverse of the matrix P sought for. We shall divide the various $n \times n$-matrices occurring in the proof into four sub-matrices obtained by taking either the first r or the last s rows, and either the first r or the last s columns of the complete matrices. Thus, for instance, we shall write, without further notational explications,

$$A=\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \quad P=\begin{pmatrix} P_1 & P_3 \\ P_2 & P_4 \end{pmatrix}, \quad Q=\begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}.$$

We shall see that, without loss of generality, we may suppose that $A_3=0$.

Now suppose that, for some P, the matrix AP has the form (3). Then we have e.g. the following matrix relations:

$$A_1P_1+A_2P_2=N(I_r+D), \tag{4}$$

$$A_4P_2=Y. \tag{5}$$

Furthermore, multiplying both members of (3) to the left with

$$\begin{pmatrix} I_r & 0 \\ -N^{-1}Y(I_r+D)^{-1} & I_s \end{pmatrix},$$

we get

$$\begin{pmatrix} A_1 & A_2 \\ -N^{-1}Y(I_r+D)^{-1}A_1 & A_4-N^{-1}Y(I_r+D)^{-1}A_2 \end{pmatrix} P=\begin{pmatrix} N(I_r+D) & N(I_r+D)X \\ 0 & M^{-1}(I_s+E) \end{pmatrix}.$$

Multiplying both members to the right with Q we get the following equation for Q_4 (containing also I_r+D and Y):

$$A_4-N^{-1}Y(I_r+D)^{-1}A_2=M^{-1}(I_s+E)Q_4. \tag{6}$$

Conversely, suppose that we have determined P in such a way that (4), (5) and (6) hold. Then, by (4) and (5), the first r columns of AP constitute the matrices $N(I_r+D)$, Y, and so the last s rows of $\begin{pmatrix} I_r & 0 \\ -N^{-1}Y(I_r+D)^{-1} & I_s \end{pmatrix} AP$ constitute a matrix of the form $(0, Z)$. Hence, $ZQ_4=A_4-N^{-1}Y(I_r+D)^{-1}A_2$ and so, by (6), ZQ_4 has the form $M^{-1}(I_s+E)Q_4$. Then it follows that AP has the form (3).

In the course of the proof we shall multiply A to the right with a matrix $\begin{pmatrix} I_r & U \\ 0 & I_s \end{pmatrix}$, where U is an integral $r\times s$-matrix to be chosen suitably. The effect of this is that the submatrix A_2 is replaced by

$$A_2{}^*=A_2+A_1U. \tag{7}$$

We shall also, for a very special form of the submatrix P_2, establish sufficient conditions in order that, given P_1, P_2 and Q_4, we can complete these sub-matrices to matrices P, Q which are unimodular and, furthermore, are each others inverse.

In fact, it will appear that we can solve the problem by taking for P_2

a matrix having elements $\neq 0$ only in its last column. As a consequence, the first $r-1$ columns of A_2P_2, and also of $A_2^*P_2$ vanish, and we can determine $r-1$ columns of P_1 independently of U. Further, the matrix P_2 will be such that $Y=A_4P_2$ is approximately a matrix with only one element $\neq 0$, namely on the place (n, r). Consequently, the first $r-1$ rows of both members of (6) do not depend heavily on U (neither on A_2). So also the first $r-1$ rows of Q_4 can be determined independently of U. In the final stage of the proof we shall choose U, the last row of Q_4 and the last column of P_1 so as to satisfy (4) and (6), with A_1 replaced by A_2^*, and the conditions alluded to above.

2. *Some lemmas*

First of all, we shall make use of the basic Theorem 2 in the paper of DAVENPORT [1]). We do not only need that which is enunciated in that theorem, but also some more information afforded by the proof of it. Therefore, we enunciate it here as the following [2])

Lemma 1. *Let $\tilde{B}=(b_{ij})$ be any real $r\times(r-1)$-matrix. Then, if $\varepsilon>0$ and N is sufficiently large, there exists an integral $r\times(r-1)$-matrix $\tilde{P}_1=(p_{ij})$ with the following properties:*

1°. $|p_{ij}-Nb_{ij}|<N^{\varepsilon}$ *for* $i=1, \ldots, r$ *and* $j=1, \ldots, r-1$

2°. *the two numbers α_k and β_k given by*

$$\alpha_k=\begin{vmatrix} p_{11} & --- & p_{1k} \\ -- & -- & -- \\ p_{k1} & --- & p_{kk}\end{vmatrix}, \quad \beta_k=\begin{vmatrix} p_{21} & --- & p_{2k} \\ -- & -- & -- \\ p_{k+1,1} & -- & p_{k+1,k}\end{vmatrix}$$

are relatively prime for $k=1, \ldots, r-1$.

We draw immediately a conclusion from 2° by proving

Lemma 2. *Let $\tilde{P}_1=(p_{ij})$ be an integral $r\times(r-1)$-matrix possessing the above property 2°. Then $\tilde{P}_1$ can be written as $\tilde{P}_1=R_1\tilde{V}_1$, where R_1 is an integral $r\times r$-matrix with determinant 1 and $\tilde{V}_1=(v_{ij})$ satisfies*

$$v_{ij}=0 \text{ if } i>j,\ v_{jj}=1 \quad (i=1, \ldots, r;\ j=1, \ldots, r-1).$$

Proof. By 2°, with $k=1$, the elements p_{11} and p_{21} are coprime. So there are integers r_1, r_2 with $r_1p_{11}+r_2p_{21}=1$. Now consider the $r\times r$-matrix $R'=(r_{ij}')$, where

$$\begin{pmatrix} r_{11}' & r_{12}' \\ r_{21}' & r_{22}'\end{pmatrix} = \begin{pmatrix} r_1 & r_2 \\ -p_{21} & p_{11}\end{pmatrix} \text{ and } r_{ij}'=\delta_{ij} \text{ otherwise}$$

(δ_{ij} denoting the Kronecker delta). If we write $R'\tilde{P}_1=(p_{ij}')$, then we

1) Theorems 1*a* and 1*b* of the Introduction are corollaries of this theorem, but we shall not use this fact.

2) See DAVENPORT [1], p. 188–189.

clearly have

$$p_{11}'=1,\ \ p_{21}'=0.$$

This proves the lemma in the case $r=2$, with $R_1=R'^{-1}$.

If $r>2$, then we multiply $R'\tilde{P}_1$ by a left factor U' of the form $U'=(\delta_{ij}+\delta_{1j}\,u_i)$ so as to obtain a matrix $U'R'\tilde{P}_1=(p_{ij}'')$ with $p_{11}''=1$ and $p_{i1}''=0$ for all $i>1$. We assert that

$$\text{g.c.d.}\ \left(\begin{vmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{vmatrix}, \begin{vmatrix} p_{11} & p_{12} \\ p_{31} & p_{32} \end{vmatrix}, \begin{vmatrix} p_{21} & p_{22} \\ p_{31} & p_{32} \end{vmatrix}\right)=$$

$$=\text{g.c.d.}\ \left(\begin{vmatrix} p_{11}'' & p_{12}'' \\ p_{21}'' & p_{22}'' \end{vmatrix}, \begin{vmatrix} p_{11}'' & p_{12}'' \\ p_{31}'' & p_{32}'' \end{vmatrix}, \begin{vmatrix} p_{21}'' & p_{22}'' \\ p_{31}'' & p_{32}'' \end{vmatrix}\right).$$

By 2°, with $k=2$, the expression on the left equals 1. So, on account of $p_{11}''=1$, $p_{21}''=p_{31}''=0$, the assertion means that the elements p_{22}'', p_{32}'' are coprime. We assert more generally that the $k+1$ determinants of order k formed from the elements p_{ij}'' with $i=2, \ldots, k+2$ and $j=2, \ldots, k+1$ by omitting any of the $k+1$ rows are relatively prime, for $k=1, \ldots, r-2$. This is most rapidly seen as follows.

On account of 2°, there exists an integral quadratic matrix P' of order $k+2$, and with determinant 1, having in its first $k+1$ columns the elements p_{ij} with $i=1, \ldots, k+2$ and $j=1, \ldots, k+1$. Observing that $U'R'$ has the form $\begin{pmatrix} V_{k+2} & 0 \\ W & I_{r-k-2} \end{pmatrix}$, where V_{k+2} is of order $k+2$ and has determinant 1, we see that there is a similar relation between the (unimodular) matrix $V_{k+2}P'$ and the elements p_{ij}''. From this and $p_{i1}''=\delta_{i1}(i=1, \ldots, k+2)$ the asserted property follows.

The lemma now follows by a suitable induction process.

Corollary. *If we complete $\tilde{P}_1$ to a quadratic matrix P_1 by adding an arbitrary new integral column, then P_1 is a product of three integra matrices*:

$$P_1=R_1T_1S_1, \tag{8}$$

where T_1 is a diagonal matrix with diagonal elements $1, \ldots, 1, t_1$, *where* $t_1=\det T_1=\det P_1$, *and where S_1 is a triangular matrix $S_1=(s_{ij})$ with*

$$s_{ij}=0 \quad \textit{if}\ i>j, \quad s_{ii}=1 \qquad (i, j=1, \ldots, r).$$

For the only thing which occurs is that a new column to V_1 is added also. The last element of this column must be taken as t_1; cancelling a left factor T_1, we obtain an integral matrix S_1 of the type desired. We annotate here that the corollary gives more precise information concerning the matrix P_1 than is yielded by the theorem on the elementary divisors of a matrix.

We now turn our attention to the matrix Q_4. We apply the foregoing lemmas to the transposed of the matrix (a_{ij}), where $i=r+1, \ldots, n-1$

and $j=r+1, \ldots, n$. We then find that, if $\varepsilon>0$ and M is sufficiently large, there exists an integral $(s-1)\times s$-matrix $\tilde{Q}_4=(q_{ij})$, where $i=r+1, \ldots, n-1$ and $j=r+1, \ldots, n$, with the following properties

3°. $|Ma_{ij}-q_{ij}|<M^{\varepsilon}$ *for* $i=r+1, \ldots, n-1$ *and* $j=r+1, \ldots, n$

4°. *the matrix* $\tilde{Q}_4$ *can be written as* $\tilde{Q}_4=\tilde{V}_4R_4$, *where* R_4 *is an integral* $s\times s$-*matrix with determinant* 1 *and* $\tilde{V}_4=(v_{ij})$ *satisfies*

$$v_{ij}=0 \quad \text{if } j>i, \quad v_{ii}=1 \qquad (i=r+1, \ldots, n-1;\ j=r+1, \ldots, n).$$

Also, for any integral row $\mathfrak{q}=(q_{n,r+1}, \ldots, q_{nn})$ we can decompose the quadratic matrix $Q_4=(q_{ij})$, where $i, j=r+1, \ldots, n$, as a product

$$Q_4=S_4T_4R_4, \tag{9}$$

where all matrices are integral, T_4 is a diagonal matrix with diagonal elements $1, \ldots, 1, t_4$, where $t_4=\det T_4=\det Q_4$, and S_4 is a triangular matrix (s_{ij}) with

$$s_{ij}=0 \quad \text{if } j>i, \quad s_{ii}=1 \qquad (i, j=r+1, \ldots, n).$$

We further consider an integral $s\times r$-matrix P_2 having elements $\neq 0$ only in its last column, say $\mathfrak{p}''$. We shall prove

Lemma 3, *Let* P_1, P_2, Q_4 *be integral matrices, where* P_2 *is of the above ype and* P_1, Q_4 *are of the form* (8) *and* (9) *respectively. Suppose that the following conditions are satisfied*

1) $\det Q_4=\det P_1$, 2) $\mathfrak{p}''$ *is the last column of* R_4^{-1}.

Then P_1, P_2 *can be completed to an integral* $n\times n$-*matrix* P *and* Q_4 *to an integral* $n\times n$-*matrix* Q, *such that* P *and* Q *have determinant* 1 *and are each others inverse.*

Proof. The lemma will be true if we can determine Q_1, Q_2, Q_3 in such a way that the following relations hold

$$Q_1P_1+Q_2P_2=I_r, \quad Q_3P_1+Q_4P_2=0 \tag{10}$$

$$\det\begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}=1. \tag{11}$$

For then Q has determinant 1 and P_1, P_2 constitute the first r rows of Q^{-1}. Now the matrices R_1, S_1, R_4, S_4 occurring in (8) and (9) all have determinant 1. Hence Q is an integral matrix with determinant 1, if and only if this is true for the matrix

$$Q'=\begin{pmatrix} Q_1' & Q_2' \\ Q_3' & Q_4' \end{pmatrix}=\begin{pmatrix} S_1 & 0 \\ 0 & S_4^{-1} \end{pmatrix}\begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}\begin{pmatrix} R_1 & 0 \\ 0 & R_4^{-1} \end{pmatrix}.$$

If we use (8), then the equations (10) lead to the following equations for the Q_i':

$$Q_1'T_1S_1+Q_2'R_4P_2=S_1, \qquad Q_3'T_1S_1+Q_4'R_4P_2=0.$$

From the form of P_2 and S_1 it follows that

(12) $$P_2S_1 = P_2.$$

Hence the last equations can also be written as

(13) $$Q_1'T_1 + Q_2'R_4P_2 = I_r, \qquad Q_3'T_1 + Q_4'R_4P_2 = 0.$$

Here, by the condition 2), $R_4\mathfrak{p}''$ is an s-vector with elements $0, \dots, 0, 1$. Further,

$$Q_4' = S_4^{-1}Q_4R_4^{-1} = T_4.$$

We can solve (13) with a matrix Q' of the form

$$\varphi' = \left(\begin{array}{ccc|c|cccc} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ \hline & & & u & & & & v \\ \hline & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \\ & & & w & & & & t_4 \end{array}\right)$$

where all open places are zero. For then (13) holds, providing that the numbers u, v, w satisfy the relations

$$ut_1 + v = 1, \qquad wt_1 + t_4 = 0.$$

In view of (11) we also require that

$$ut_4 - vw = 1.$$

These three equations for u, v, w are soluble if (and only if) $t_1 = t_4$, i.e. if the condition 1) holds. We then find

$$w = -1, \quad v = 1 - t_1u, \qquad u \text{ arbitrary}.$$

We note that the above reasoning is also valid in the case that $\det Q_4 = \det P_1 = 0$. The lemma has now been proved.

Finally, we prove the following well-known

Lemma 4. *Let $\mathfrak{p}$ be any column vector and $\mathfrak{b}$ any row vector both consisting of s elements. Then*

$$\det\,(I_s + \mathfrak{p}\mathfrak{b}) = 1 + \mathfrak{b}\mathfrak{p}.$$

Proof. Let p_i, b_i $(i = 1, \dots, s)$ be the elements of $\mathfrak{p}, \mathfrak{b}$ respectively. We may suppose that $p_1 \neq 0$. Then, subtracting suitable multiples of the first row from the other rows and expanding according to the first row, we obtain

$$\det\,(I_s + \mathfrak{p}\mathfrak{b}) = p_1 \begin{vmatrix} p_1^{-1} + b_1 & b_2 & b_3 & - & - & - & b_s \\ -p_1^{-1}p_2 & 1 & 0 & - & - & - & 0 \\ -p_1^{-1}p_3 & 0 & 1 & - & - & - & 0 \\ - & - & - & - & - & - & - \\ -p_1^{-1}p_s & 0 & 0 & - & - & - & 1 \end{vmatrix}$$

$$= 1 + b_1p_1 + b_2p_2 + \dots + b_sp_s.$$

3. *Proof of Theorem 2'.*

Let $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ be given. By multiplying A to the right with a suitable integral unimodular matrix we can get any permutation of the columns of A and also arrange that the elements of a given column are multiplied by -1. Hence, without loss of generality, we may suppose that

$$\det A_1 \neq 0, \qquad \det A > 0. \tag{14}$$

Next, we note that the right hand member of (3) can be written as

$$\begin{pmatrix} I_r & 0 \\ N^{-1}Y(I_r+D)^{-1} & I_s \end{pmatrix} \cdot \begin{pmatrix} N(I_r+D) & N(I_r+D)X \\ 0 & M^{-1}(I_s+E) \end{pmatrix}.$$

Now, as to the matrix Y there are no requirements at all. Hence, if Z is any $s\times r$-matrix, the assertion of the theorem holds for A if and only if it holds for the matrix

$$\begin{pmatrix} I_r & 0 \\ Z & I_s \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} A_1 & A_2 \\ ZA_1+A_3 & ZA_2+A_4 \end{pmatrix}.$$

In particular, we may choose $Z = -A_1^{-1}A_3$. It follows that, without loss of generality, we may suppose that

$$A_3 = 0. \tag{15}$$

We now divide the proof into four parts.

3.1. *Preliminary approximation to A by a matrix $\bar{A}$*

Let us write

$$\det A_1 = \alpha, \qquad \det A_4 = \beta.$$

Then, by (14) and (15),

$$\det A = \alpha\beta > 0.$$

For given N we define M by $N^r M^{-s} = \alpha\beta$. We take N as large as is required below for the applications of lemma 1 to the matrix A_1^{-1} and the transposed of the matrix A_4.

First, we determine $s-1$ row vectors

$$\mathfrak{q}_i = (q_{i,r+1}, \ldots, q_{i,n}) \qquad (i = r+1, \ldots, n-1)$$

such that the matrix $\tilde{Q}_4 = (q_{ij})$ possesses the properties 3° and 4° given in section 2. This gives a certain matrix R_4. Then, we define $\mathfrak{p}''$ as the last column of R_4^{-1}. Further, we denote the inverse of A_1 by $B = (b_{ij})$ $(i, j = 1, \ldots, r)$ and the columns of B by

$$\mathfrak{b}^1, \ldots, \mathfrak{b}^r.$$

Applying lemma 1 to the matrix $\tilde{B}$ consisting of the columns $\mathfrak{b}^1, \ldots, \mathfrak{b}^{r-1}$

we get $r-1$ column vectors

$$\mathfrak{p}^j = \begin{pmatrix} p_{1j} \\ \vdots \\ p_{rj} \end{pmatrix} \quad (j=1, \ldots, r-1)$$

such that the properties 1° and 2° hold. After this, we determine a column vector $\mathfrak{p}'$ of r components such that the components of

$$\mathfrak{p}' + A_1{}^{-1}A_2\mathfrak{p}'' - N\mathfrak{b}^r \tag{16}$$

are all $\leqq \frac{1}{2}$ in absolute value.

We are now ready for introducing the matrix D occurring in the theorem. For this purpose we apply the matrix A_1 to the column vectors $\mathfrak{p}^j - N\mathfrak{b}^j (j=1, \ldots, r-1)$ and to the vector (16). Then the components of the resulting vectors are all of the form $O(N^\varepsilon)$ [1]. Further, the vectors $A_1\mathfrak{b}^j$ $(j=1, \ldots, r)$ constitute the unit matrix I_r. Hence, if we denote by $I_r + D$ the matrix with columns

$$N^{-1}A_1\mathfrak{p}^j \ (j=1, \ldots, r-1), \qquad N^{-1}(A_1\mathfrak{p}' + A_2\mathfrak{p}''),$$

then the elements of D are all of the form $O(N^{-1+\varepsilon})$ and so D is of the type desired in the theorem.

We also make a beginning with the determination of the matrix E. Let $\mathfrak{a}_n$ be the last row of A_4 and let η be a real number. We now multiply the vectors $\mathfrak{q}_i$ to the right with the matrix $A_4{}^{-1}$. Then, we denote by $I_s + E_1$ the matrix with rows

$$M^{-1}\mathfrak{q}_iA_4{}^{-1} \ (i=r+1, \ldots, n-1), \ (1+\eta)\mathfrak{a}_nA_4{}^{-1}$$

(the last row has elements $0, \ldots, 0, 1+\eta$), where η is determined in such a way that

$$\det(I_s + E_1) = \det(I_r + D). \tag{17}$$

Then, by the choice of the $\mathfrak{q}_i$, the elements in the first $s-1$ rows of E_1 are all of the form $O(M^{-1+\varepsilon})$. It follows from (17) that η is of the form

$$\eta = O\,(\max(N^{-1+\varepsilon}, M^{-1+\varepsilon})). \tag{18}$$

The matrices D and E_1 being chosen we define the matrix $\bar{A}$ in the following way

$$\bar{A} = \begin{pmatrix} \bar{A}_1 & \bar{A}_2 \\ 0 & \bar{A}_4 \end{pmatrix} = \begin{pmatrix} (I_r+D)^{-1} & 0 \\ 0 & I_s+E_1 \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ 0 & A_4 \end{pmatrix}. \tag{19}$$

Then we have the following relations

$$\bar{A}_1\mathfrak{p}^j = N\bar{\mathfrak{e}}^j \qquad (j=1, \ldots, r-1) \tag{20}$$

$$\bar{A}_1\mathfrak{p}' + \bar{A}_2\mathfrak{p}'' = N\bar{\mathfrak{e}}^r \tag{21}$$

$$M\bar{\mathfrak{a}}_i = \mathfrak{q}_i \qquad (i=r+1, \ldots, n-1). \tag{22}$$

Here $\bar{\mathfrak{e}}^j$ denotes the j-th column of I_r and $\bar{\mathfrak{a}}_i$ the i-th row of $\bar{A}_4$.

---

[1] It is clear that the constant in the O-symbol only depends on the matrix A.

3.2. *Some computations*

Let us write

$$\det \bar{A}_1 = \bar{\alpha}, \ \det \bar{A}_4 = \bar{\beta}.$$

Then, on account of (17) and (19), we have

$$\bar{\alpha}\bar{\beta} = \alpha\beta. \tag{23}$$

We now define the matrix P_2 as in section 2 (see lemma 3), and then compute the matrix $\bar{Y} = \bar{A}_4 P_2$ (compare the relation (5)). First of all, the s-vector $R_4 \mathfrak{p}''$ has components $0, \ldots, 0, 1$. It follows therefore from the property 4°, in particular from the form of $\tilde{V}_4$, that $\tilde{Q}_4 \mathfrak{p}'' = \tilde{V}_4 R_4 \mathfrak{p}''$ is the zero vector. In other words, by (22),

$$\bar{\mathfrak{a}}_i \mathfrak{p}'' = 0 \qquad (i = r+1, \ldots, n-1). \tag{24}$$

Next, we complete the matrix $\tilde{Q}_4$ to a $s \times s$-matrix C_4 by adding the (not necessarily integral) row $M\bar{\mathfrak{a}}_n$, and write $C_4 R_4^{-1} = V_4$. Then we have

$$C_4 \mathfrak{p}'' = V_4 R_4 \mathfrak{p}'',$$

hence, by the form of V_4 and $R_4 \mathfrak{p}''$,

$$M\bar{\mathfrak{a}}_n \mathfrak{p}'' = \det V_4 = \det C_4,$$

and so

$$\bar{y}_{nr} = \bar{\mathfrak{a}}_n \mathfrak{p}'' = M^{-1} \det C_4 = M^{s-1} \bar{\beta}. \tag{25}$$

So we find that *all elements of* $\bar{Y} = \bar{A}_4 P_2$ *are zero, except for the element* $\bar{y}_{nr}$ in its last row and column which is given by (25).

We also compute some determinants. Let $\bar{\mathfrak{a}}_r'$ and $\bar{\mathfrak{a}}_r''$ denote the last rows of $\bar{A}_1$ and $\bar{A}_2$ respectively and, for brevity, write

$$\bar{\mathfrak{a}}_r'' \mathfrak{p}'' = \theta. \tag{26}$$

Then we have, using (20), (21) and an obvious notation for the matrix which has given vectors as columns,

$$\begin{aligned} \det(\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \mathfrak{p}') &= \bar{\alpha}^{-1} \det(\bar{A}_1 \mathfrak{p}^1, \ldots, \bar{A}_1 \mathfrak{p}^{r-1}, \bar{A}_1 \mathfrak{p}') \\ &= \bar{\alpha}^{-1} \det(N I_r - \bar{A}_2 P_2) = \bar{\alpha}^{-1} N^r (1 - N^{-1}\theta). \end{aligned}$$

On account of $N^r M^{-s} = \alpha\beta$ and (23) we then have

$$\det(\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \mathfrak{p}') = M^s \bar{\beta}(1 - N^{-1}\theta).$$

Next, by lemma 4,

$$\begin{aligned} \det M(\bar{A}_4 - N^{-1}\bar{Y}\bar{A}_2) &= \det M\bar{A}_4 \cdot \det(I_s - N^{-1} P_2 \bar{A}_2) \\ &= \det M\bar{A}_4 \cdot \det(I_s - N^{-1} \mathfrak{p}'' \bar{\mathfrak{a}}_r'') \\ &= M^s \bar{\beta}(1 - N^{-1} \bar{\mathfrak{a}}_r'' \mathfrak{p}'') = M^s \bar{\beta}(1 - N^{-1}\theta). \end{aligned}$$

We thus have found the important relation

$$\det(\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \mathfrak{p}') = \det M(\bar{A}_4 - N^{-1}\bar{Y}\bar{A}_2). \tag{27}$$

It is this relation which will enable us hereafter to apply lemma 3. One should compare it with the relation (6) in the Introduction and also note the words "and only if" at the end of the proof of lemma 3. Or course, the adjustment of the last row of the matrix E_1 such that (17) holds plays a rôle here.

A by-product of the proof of (27) is that the number k defined by

$$k = \det M(\bar{A}_4 - N^{-1}\bar{Y}\bar{A}_2) = M^s\bar{\beta}(1 - N^{-1}\theta) \tag{28}$$

is an integer.

There is another way of computing the right hand member of (27). The matrix occurring there has $s-1$ rows $M\bar{\mathfrak{a}}_i = \mathfrak{q}_i$, whereas the last row is given by

$$\mathfrak{z}^\circ = M(\bar{\mathfrak{a}}_n - N^{-1}\bar{y}_{nr}\bar{\mathfrak{a}}_r''). \tag{29}$$

Following the deduction of (25), with the last row of C_4 replaced by $\mathfrak{z}^\circ$, we get

$$\det M(\bar{A}_4 - N^{-1}\bar{Y}\bar{A}_2) = \mathfrak{z}^\circ\mathfrak{p}''. \tag{30}$$

We further show that

$$N^{-1}M^s\bar{\beta}\bar{\mathfrak{a}}_r' = \mathfrak{c}, \tag{31}$$

say, is a primitive integral vector. To this end, we choose an arbitrary integral r-vector $\bar{\mathfrak{p}}$ thus that the matrix $\bar{P}$ with columns $\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \bar{\mathfrak{p}}$ has determinant 1; this is possible because of the property 2°, with $k = r-1$. Then, on the one hand, $\det \bar{A}_1\bar{P} = \bar{\alpha}$. On the other hand, by (20), the matrix $\bar{A}_1\bar{P}$ has the form

$$\bar{A}_1\bar{P} = \begin{pmatrix} N & & \times \\ & \ddots & \vdots \\ & N & \times \\ & & \bar{\mathfrak{a}}_r'\,\bar{\mathfrak{p}} \end{pmatrix},$$

where the elements on the open places are all zero. Therefore

$$\bar{\alpha} = N^{r-1}\bar{\mathfrak{a}}_r'\bar{\mathfrak{p}}, \text{ or } \mathfrak{c}\bar{\mathfrak{p}} = 1.$$

Hence, by the form of $\bar{A}_1\bar{P}$,

$$\mathfrak{c}\bar{P} = (0, \ldots, 0, 1), \text{ or } \mathfrak{c} = \bar{P}^{-1}\ (0, \ldots, 0, 1).$$

Since $\bar{P}$ is integral and unimodular, this proves that the vector $\mathfrak{c}$ is integral and primitive.

3.3. *Introduction of the matrix U and the lattice $\bar{\Lambda}$.*

Let us multiply $\bar{A}$ to the right with a matrix $\begin{pmatrix} I_r & U \\ 0 & I_s \end{pmatrix}$, where U is an integral $r\times s$-matrix to be determined below. This has the effect (see (7)) that $\bar{A}_2$ is replaced by

$$A_2^* = \bar{A}_2 + \bar{A}_1 U.$$

In particular, $\bar{\mathfrak{a}}_r''$ is replaced by

$$\mathfrak{a}_r^* = \bar{\mathfrak{a}}_r'' + \bar{\mathfrak{a}}_r' U. \tag{32}$$

Next, we have

$$\bar{A}_1 \mathfrak{p}' + \bar{A}_2 \mathfrak{p}'' = \bar{A}_1 \mathfrak{p}^* + A_2^* \mathfrak{p}'', \tag{33}$$

if we take

$$\mathfrak{p}^* = \mathfrak{p}' - U\mathfrak{p}''. \tag{34}$$

The foregoing computations remain valid if we replace $\bar{A}_2$, $\bar{\mathfrak{a}}_r''$, $\mathfrak{p}'$ by A_2^*, $\mathfrak{a}_r^*$, $\mathfrak{p}^*$ respecrively (θ also changes). In particular, we have

$$\det(\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \mathfrak{p}^*) = \det M(\bar{A}_4 - N^{-1}\bar{Y} A_2^*) = \mathfrak{z}\mathfrak{p}'', \tag{35}$$

if $\mathfrak{z}$ is the last row of $M(\bar{A}_4 - N^{-1}\bar{Y} A_2^*)$. Clearly, $\mathfrak{p}^*$ is integral.

At the end of the proof we shall also consider a matrix A_4^* obtained by modifying the last column $\bar{\mathfrak{a}}_n$ of $\bar{A}_4$ in a suitable manner. Let us write

$$\det A_4^* = (1-\delta) \det \bar{A}_4, \quad Y^* = A_4^* P_2.$$

Then, by writing $A_4^* = A_4^* \bar{A}_4^{-1} \cdot \bar{A}_4$, we get

$$\det M(A_4^* - N^{-1} Y^* A_2^*) = (1-\delta) \det M(\bar{A}_4 - N^{-1}\bar{Y} A_2^*). \tag{36}$$

Let us again consider the matrix $M(\bar{A}_4 - N^{-1}\bar{Y} A_2^*)$. It has $s-1$ rows $\mathfrak{q}_i$ and one row $\mathfrak{z}$ given by (see (32), (29), (25) and (31))

$$\mathfrak{z} = M\bar{\mathfrak{a}}_n - N^{-1} M \bar{y}_{nr} \mathfrak{a}_r^* = \mathfrak{z}^\circ - \mathfrak{c}U. \tag{37}$$

By (35) and (28), its determinant is equal to

$$\mathfrak{z}\mathfrak{p}'' = \mathfrak{z}^\circ \mathfrak{p}'' - \mathfrak{c}U\mathfrak{p}'' = k - \mathfrak{c}U\mathfrak{p}''.$$

Here $\mathfrak{c}$ as well as $\mathfrak{p}''$ are primitive integral vectors. This has two consequences. Firstly, if we write

$$\mathfrak{r} = \mathfrak{c}U, \tag{38}$$

then $\mathfrak{r}$ runs through all lattice points in s-dimensional space if U runs through all integral $r \times s$-matrices. Secondly, the product $\mathfrak{c}U\mathfrak{p}'' = \mathfrak{r}\mathfrak{p}''$ takes on all integral values. Then, since k is an integer, there are matrices U such that $\mathfrak{z}\mathfrak{p}'' = 0$.

We consider $\mathfrak{z}$ as a point in an s-dimensional space. Then $\mathfrak{z}^\circ$ is the point obtained by putting $U=0$, and we have

$$\mathfrak{z} = \mathfrak{z}^\circ - \mathfrak{r}, \quad \mathfrak{z}^\circ \mathfrak{p}'' = k.$$

We denote by H the hyperplane of points $\mathfrak{x}$ with $\mathfrak{x}\mathfrak{p}'' = 0$. The point $\mathfrak{z}$

belongs to H if $\mathfrak{x} = \mathfrak{c}U$ is chosen in such a way that $\mathfrak{x}\mathfrak{p}'' = k$:

$$\mathfrak{z} = \mathfrak{z}^\circ - \mathfrak{x} \in H \quad \text{if} \quad \mathfrak{x}\mathfrak{p}'' = k. \tag{39}$$

These points $\mathfrak{z}$ constitute a certain (not necessarily homogeneous) $(s-1)$-dimensional lattice in H. We denote this lattice by $\bar{\Lambda}$. The determinant of $\bar{\Lambda}$ is rather large.

3.4. *End of the proof*

We will return to our procedure in 3.1, where we have chosen preliminarily the r columns $\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \mathfrak{p}'$ of P_1 and $s-1$ rows $\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_{n-1}$ of Q_4. We have also replaced A by $\bar{A}$. Now, according to our remarks in the Introduction we wish to approximate the matrix $M(\bar{A}_4 - N^{-1}\bar{Y}\bar{A}_2)$ by a matrix Q_4. Further, we wish to do this in such a way that $\det Q_4 = \det P_1$ so that, by (27),

$$\det Q_4 = \det M(\bar{A}_4 - N^{-1}\bar{Y}\bar{A}_2).$$

We recall that the above matrix has rows $\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_{n-1}, \mathfrak{z}^\circ$. So we wish to approximate $\mathfrak{z}^\circ$ in a certain sense by a row $\mathfrak{q}_n$, in such a way that the determinant is not altered. However, such rows $\mathfrak{q}_n$ are distributed scarcely. But the difficulty which thus arises can be overcome by operating with the matrix U.

It is convenient to work in the linear subspace H. We reason as follows:

Let $\mathfrak{z}^1$ be a particular point of the lattice $\bar{\Lambda}$ introduced above, e.g. a point $\neq \mathfrak{o}$ with minimal distance to the origin $\mathfrak{o}$. Let K be the cylinder consisting of the points $\mathfrak{x}$ with [1])

$$\min |\lambda\mathfrak{z}^1 - \mathfrak{x}| \leqq 1 \qquad (\lambda \text{ real}).$$

Applying MINKOWSKI's theorem to a suitable portion of K and the homogeneous lattice $\Lambda = \bar{\Lambda} - \mathfrak{z}^1$ we get some point $\mathfrak{s}$ of Λ in K. We may even determine $\mathfrak{s}$ in such a way that

$$|\mathfrak{s}| \geqq M|\mathfrak{z}^1|$$

(we do not require that $\mathfrak{s}$ be a primitive point of Λ).

The point $\mathfrak{z}^1 + \mathfrak{s}$ belongs to $\bar{\Lambda}$. We determine the matrix U in such a way that the vector (37) is equal to $\mathfrak{z} = \mathfrak{z}^1 + \mathfrak{s}$, and we write

$$\mathfrak{y} = \mathfrak{z} - M\bar{\mathfrak{a}}_n.$$

Further, we decompose $\mathfrak{s}$ as follows

$$\mathfrak{s} = (1-\delta)\mathfrak{z} + M\mathfrak{d} \qquad (\delta \text{ real}),$$

such that $\mathfrak{d}$ is orthogonal to $\mathfrak{z}$. It is easily verified that $|M\mathfrak{d}| \leqq 1$ and that $|\delta| \leqq (M-1)^{-1}$.

[1]) $|\mathfrak{y}|$ denotes the length of $\mathfrak{y}$.

We introduce now a new row $\mathfrak{a}_n^*$ by

$$M\mathfrak{a}_n^* + (1-\delta)\mathfrak{y} = \hat{\mathfrak{z}} \tag{40}$$

and write

$$A_4^* = (I_s + E_2)\bar{A}_4, \quad Y^* = A_4^* P_2, \tag{41}$$

where A_4^* is the matrix with rows $\bar{\mathfrak{a}}_{r+1}, \ldots, \bar{\mathfrak{a}}_{n-1}, (1-\delta)\bar{\mathfrak{a}}_n + \mathfrak{d}$. Then the elements of E_2 are all of the form $O(M^{-1})$. Further, we have

$$M\mathfrak{a}_n^* = \hat{\mathfrak{z}} - (1-\delta)\mathfrak{z} + (1-\delta)M\bar{\mathfrak{a}}_n = M\mathfrak{d} + (1-\delta)M\bar{\mathfrak{a}}_n.$$

Here, $M\mathfrak{d}$ belongs to H, and so $\mathfrak{d}\mathfrak{p}'' = 0$. Hence, the last row of $M(A_4^* - N^{-1}Y^*A_2)$ is equal to

$$\begin{aligned} &M\mathfrak{a}_n^* - N^{-1}M\mathfrak{a}_n^* P_2 A_2^* \\ &= M\mathfrak{d} + (1-\delta)M\bar{\mathfrak{a}}_n - N^{-1}(1-\delta)M\bar{\mathfrak{a}}_n P_2 A_2^* \\ &= M\mathfrak{d} + (1-\delta)\mathfrak{z} = \hat{\mathfrak{z}}. \end{aligned} \tag{42}$$

The other rows are simply $M\bar{\mathfrak{a}}_i = \mathfrak{q}_i$ $(i = r+1, \ldots, n-1)$.

Next, we define Q_4 as the matrix with rows $\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_{n-1}, \hat{\mathfrak{z}}$ and P_1 as the matrix with columns $\mathfrak{p}^1, \ldots, \mathfrak{p}^{r-1}, \mathfrak{p}^*$ where $\mathfrak{p}^*$ is given by (34). We recall that $\mathfrak{p}''$ and P_2 are determined by R_4, and so by the rows $\mathfrak{q}_i$. By virtue of (20), (21) and (33) we have

$$\bar{A}_1 P_1 + A_2^* P_2 = N I_r.$$

By (22) and (42),

$$A_4^* - N^{-1}Y^*A_2^* = M^{-1}Q_4, \text{ with } Y^* = A_4^* P_2.$$

On account of (35), (36) and $\mathfrak{z} = \mathfrak{z}^1 + \hat{\mathfrak{z}} \in H$ the last matrix has determinant 0, so that $\det Q_4 = 0$. Again, by (35), $\det P_1 = 0$. Then, by the choice of $\mathfrak{p}''$, the conditions of lemma 3 are satisfied. And so, by that lemma, we can complete P_1, P_2, Q_4 to full matrices P, Q. Hence it follows (see the Introduction) that the theorem holds for the matrix

$$\begin{pmatrix} \bar{A}_1 & A_2^* \\ 0 & A_4^* \end{pmatrix} = \begin{pmatrix} (I_r + D)^{-1} & 0 \\ 0 & (I_s + E_2)(I_s + E_1) \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ 0 & A_4 \end{pmatrix} \begin{pmatrix} I_r & U \\ 0 & I_s \end{pmatrix}$$

Then it also holds for the matrix $\begin{pmatrix} A_1 & A_2 \\ 0 & A_4 \end{pmatrix}$. The theorem is now proved.

Mathematisch Centrum, Amsterdam

REFERENCE

[1]. Davenport, H. On a theorem of Furtwängler, J. London Math. Society **30**, 186–195 (1955).