COMPOSITIO MATHEMATICA

WOLFGANG M. SCHMIDT

The subspace theorem in diophantine approximations

Compositio Mathematica, tome 69, n° 2 (1989), p. 121-173
<http://www.numdam.org/item?id=CM_1989__69_2_121_0>

Compositio Mathematica 69: 121–173 (1989)

The subspace theorem in diophantine approximations

WOLFGANG M. SCHMIDT*
Department of Mathematics, University of Colorado, Box 426, Boulder, CO 80309, USA

Received 1 February 1988; accepted 24 May 1988

1. Introduction

It is well known that the method of Thue–Siegel–Roth does not provide bounds for the *sizes* of good rational approximations of algebraic numbers. But it does give explicit bounds for the *number* of such approximations. Thus if α is algebraic of degree $d \geqq 2$ and if $\delta > 0$, the number of rational approximations x/y with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}} \tag{1.1}$$

is under some bound which depends on d, δ and on the height $H_0 = H_0(\alpha)$, which is the maximum modulus of the coefficients of the minimal defining polynomial of α over $\mathbb{Z}$. Explicit estimates were given by Davenport and Roth [5]. More recently, Bombieri and Van der Poorten [2] used a theorem of Esnault and Viehweg [6] to obtain significantly better such estimates.

Note that (1.1) may be written as $|L_1(\mathbf{x})L_2(\mathbf{x})| < y^{-\delta}$ where $\mathbf{x} = (x, y)$, $L_1(\mathbf{x}) = y$, $L_2(\mathbf{x}) = \alpha y - x$. This is closely related to $|L_1(\mathbf{x})L_2(\mathbf{x})| < |\mathbf{x}|^{-\delta}$ where $|\mathbf{x}| = (x^2 + y^2)^{1/2}$. More generally, let $L_1, \ldots, L_n$ be linearly independent linear forms in n variables, with real or complex algebraic coefficients. The *Subspace Theorem* ([11]; see also [N]) says that the integer solutions $\mathbf{x} = (x_1, \ldots, x_n) \neq \mathbf{0}$ of

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\mathbf{x}|^{-\delta}$$

where $|\mathbf{x}| = (x_1^2 + \cdots + x_n^2)^{1/2}$, lie in a finite number of proper rational subspaces of $\mathbb{R}^n$. In particular, they lie in a finite number of subspaces of dimension $n - 1$; in what follows, the word *subspace* will always designate a rational subspace of dimension $n - 1$.

* Supported in part by NSF grant DMS-8603093.

Our goal here will be to derive a bound for the required number of subspaces. Given linear forms $L_1, \ldots, L_n$ in n variables, let $\det(L_1, \ldots, L_n)$ denote the modulus of the determinant of their coefficient matrix. We will suppose throughout that $n > 1$.

THEOREM: *Let $L_1, \ldots, L_n$ be linearly independent linear forms with coefficients in a real or complex algebraic number field K of degree d. Consider the inequality*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n)|\mathbf{x}|^{-\delta} \tag{1.2}$$

where $0 < \delta < 1$. There are proper subspaces $S_1, \ldots, S_t$ of $\mathbb{R}^n$ with

$$t = [(2d)^{2^{26n\delta^{-2}}}] \tag{1.3}$$

(and with [ ] denoting integer parts), such that every integer solution $\mathbf{x}$ of (1.2) either lies in one of these subspaces, or has norm

$$|\mathbf{x}| < \max((n!)^{8/\delta}, H(L_1), \ldots, H(L_n)), \tag{1.4}$$

where the $H(L_i)$ are suitably defined heights.

Our definition of heights is the same as in Bombieri and Vaaler [1], and had already been discussed in [10]. Given a number field K, let $M(K)$ be an indexing set for the absolute values of K; for $w \in M(K)$, the absolute value $|\lambda|_w$ defined for $\lambda \in K$ will be an extension of the standard absolute value of $\mathbb{Q}$ or of a p-adic absolute value of $\mathbb{Q}$. Let n_w be the local degree, i.e. the degree of K_w over $\mathbb{Q}_w$, where K_w is the w-adic completion of K and $\mathbb{Q}_w$ the completion of $\mathbb{Q}$ (so that $\mathbb{Q}_w$ is $\mathbb{R}$ or $\mathbb{Q}_p$). Then the product formula

$$\prod_{w \in M(K)} |\lambda|_w^{n_w} = 1$$

holds for $\lambda \neq 0$ in K. It will be convenient to introduce a set $M'(K)$ of symbols v, such that to each $w \in M(K)$ there correspond n_w symbols v in $M'(K)$, and for such v put $|\lambda|_v = |\lambda|_w$. The product formula may be rewritten as

$$\prod_{v \in M'(K)} |\lambda|_v = 1.$$

We will suppose that K is embedded in $\mathbb{C}$, and then the standard absolute value $|\lambda|$ equals one of the archimedean absolute values $|\lambda|_v$; say the one with $v = v^*$.

Given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K^n$, put

$$|\boldsymbol{\alpha}|_v = \begin{cases} (|\alpha_1|_v^2 + \cdots + |\alpha_n|_v^2)^{1/2} & \text{for } v \text{ archimedean,} \\ \max(|\alpha_1|_v, \ldots, |\alpha_n|_v) & \text{for } v \text{ non-archimedean.} \end{cases}$$

For $\boldsymbol{\alpha} \neq \mathbf{0}$ set

$$H_K(\boldsymbol{\alpha}) = \prod_v |\boldsymbol{\alpha}|_v. \tag{1.5}$$

Here and below, the product is over $v \in M'(K)$. For $\lambda \neq 0$, $\lambda \in K$, we have $H_K(\lambda\boldsymbol{\alpha}) = H_K(\boldsymbol{\alpha})$ by the product formula. It also follows that $H_K(\boldsymbol{\alpha}) \geqq 1$. In contrast to the "field height" H_K, the "absolute height", given by

$$H(\boldsymbol{\alpha}) = H_K(\boldsymbol{\alpha})^{1/d} \tag{1.6}$$

where d is the degree of K, is independent of K. That is, if the components of $\boldsymbol{\alpha}$ lie in a field K, and also in a field K', then $H(\boldsymbol{\alpha})$ is the same whether computed in terms of K or of K'. Now when $L = \alpha_1 X_1 + \cdots + \alpha_n X_n$ is a nonzero linear form with algebraic coefficients, we put

$$H(L) = H(\boldsymbol{\alpha}).$$

In what follows, H will denote $\max(H(L_1), \ldots, H(L_n))$, or more generally will be any quantity with

$$H \geqq \max(H(L_1), \ldots, H(L_n)). \tag{1.7}$$

The inequality (1.4) may then be replaced by

$$|\mathbf{x}| < \max((n!)^{8/\delta}, H). \tag{1.8}$$

There are only finitely many integer points with (1.8), and one can give various estimates for the number of proper subspaces which contain all the solutions of (1.2), (1.8). For this see Section 4. But such estimates involve not only n, d, δ, but also H. It may be seen[†] that the number of solutions of (1.1), or the number of subspaces containing all the solutions of (1.2), cannot be estimated independently of heights. But see the remark at the end of Section 4.

[†] See e.g. J. Mueller and W. M. Schmidt, On the number of good rational approximations to algebraic numbers. *Proc. A.M.S.* (to appear).

As was pointed out above, recent results of Esnault and Viehweg may be used to estimate the number of solutions of (1.1). A conjectured generalization of their work, which would be relevant for simultaneous approximations, has so far not been established. Therefore we have to appeal to the more classical "Roth's Lemma". A generalization of the work of Esnault and Viehweg would lead to a significant improvement of our estimates. Another reason why the general estimates are so much worse than for approximation to a single algebraic number is that for simultaneous approximations we have to use certain "transference principles" from the Geometry of Numbers. The number 26 in the definition of t in (1.3) is somewhat arbitrary and could easily be reduced.

Often one would like to estimate the number of solutions of (1.2), and not just the number of subspaces containing them. But there is a difficulty here. We cannot estimate the number of subspaces independently of H, and in fact we would be quite happy to get an estimate for the number of solutions of (1.2) involving H. But the dependency on H is deadly in a possible induction argument: we would have to estimate the number of solutions of (1.2) with $\mathbf{x}$ in a subspace S, say a subspace of dimension $n - 1$. The integer points in S are of the type $\mathbf{x} = T\mathbf{y}$, where T is a linear map $\mathbb{R}^{n-1} \to S$, and where $\mathbf{y}$ runs through $\mathbb{Z}^{n-1}$. Now (1.2) leads to an estimate for $|L_1'(\mathbf{y}) \cdots L_n'(\mathbf{y})|$ with $L_i'(\mathbf{y}) = L_i(T(\mathbf{y}))$. Moreover, if, say, $|L_1'(\mathbf{y})| \leqq \cdots \leqq |L_n'(\mathbf{y})|$, it is usually possible to obtain an upper bound for

$$|L_1'(\mathbf{y}) \cdots L_{n-1}'(\mathbf{y})|$$

which is analogous to (1.2). An application of the case $n - 1$ of our Theorem gives a bounded number of proper subspaces of $\mathbb{R}^{n-1}$, as well as possible solutions $\mathbf{y}$ whose norm $|\mathbf{y}|$ is bounded by the analogue of (1.4). But since we don't known anything about S, we don't have any estimates on the heights of the forms L_i', so that ultimately we have no estimate for $|\mathbf{y}|$ in terms of the given data, and therefore no estimate for the number of solutions $\mathbf{y}$.

The situation is different again when it comes to diophantine equations which may be treated by diophantine approximation methods. It has been known since Evertse's work [7] that the number of solutions of a Thue equation $F(x, y) = h$ may be bounded in terms of h and the degree of F, but independently of the coefficients of F, i.e., independently of the "height" of F. In forthcoming work [12] we will use the present main theorem to reach a similar conclusion for norm form equations. In fact, this application is the main motivation for the present paper.

Basically, our task here will be to make the arguments as presented in [N] more explicit. Wherever possible we will refer back to this earlier work. We

will try to strike a balance between being too brief and being too repetitive of [N]. One difference is that now we will make a more systematic use of heights. We will collect preparatory material in Sections 2–8, and will begin with the main arguments in Section 9.

We will use symbols such as X, X_1, X_2, . . . for variables, and x, x_1, x_2, . . . for rational integers. Linear forms are of the type

$$L(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_n X_n = \boldsymbol{\alpha}\mathbf{X}$$

with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\mathbf{X} = (X_1, \ldots, X_n)$. For $\boldsymbol{\alpha}, \boldsymbol{\beta}$ in $\mathbb{R}^n$ we put $\boldsymbol{\alpha}\boldsymbol{\beta} = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$. Also, $|\boldsymbol{\alpha}| = (\boldsymbol{\alpha}, \boldsymbol{\alpha})^{1/2}$. Hence in the special case when $\boldsymbol{\alpha}$ has components in a real number field K, we have $|\boldsymbol{\alpha}| = |\boldsymbol{\alpha}|_{v^*}$ in the notation introduced above.

We will quote my 1980 Lecture Notes as [N], and [N, X] will denote chapter X of [N], etc.

I wish to thank H.P. Schlickewei for pointing out a number of inaccuracies and obscurities in my original manuscript.

2. Reduction to the case of real coefficients

PROPOSITION A: *Let $L_1, \ldots, L_n$ be linear forms with real algebraic coefficients and nonvanishing determinant. The solutions of* (1.2) *with*

$$|\mathbf{x}| \geqq \max((n!)^{4/\delta}, \tfrac{1}{2}H^{1/2}) \tag{2.1}$$

(*where, as always, H is a quantity with* (1.7)), *lie in at most t_0 subspaces, where*

$$t_0 = [(4d)^{2^{24n}\delta^{-2}}].$$

We are going to deduce the Theorem. So let $L_1, \ldots, L_n$ be linearly independent linear forms with coefficients in a real or complex algebraic number field K of degree d. Let $\bar{K}$ be the field obtained from K by complex conjugation, and K' the compositum of K, $\bar{K}$ and $\mathbb{Q}(i)$. It has degree $d' = dd_1$ with $d_1 < 2d$. Since the Theorem is invariant under replacing the linear forms by nonzero multiples, we may suppose that each L_i has some coefficient equal to 1. Write $L_n = L_n' + iL_n''$ where L_n', L_n'' have real coefficients. Either $\det(L_1, \ldots, L_{n-1}, L_n')$ or $\det(L_1, \ldots, L_{n-1}, L_n'')$ is $\geqq \frac{1}{2}\det(L_1, \ldots, L_{n-1}, L_n)$. Say the former is. Then since $|L_n'(\mathbf{x})| \leqq |L_n(\mathbf{x})|$, (1.2) yields $|L_1(\mathbf{x}) \cdots L_{n-1}(\mathbf{x})L_n'(\mathbf{x})| < 2\det(L_1, \ldots, L_{n-1}, L_n')|\mathbf{x}|^{-\delta}$. In a

similar manner we may replace each of $L_1, \ldots, L_n$, to obtain real forms $L_1', \ldots, L_n'$ with $|L_1'(\mathbf{x}) \cdots L_n'(\mathbf{x})| < 2^n \det(L_1', \ldots, L_n')|\mathbf{x}|^{-\delta}$. Now in the Theorem it will suffice to consider points with $|\mathbf{x}| \geqq (n!)^{8/\delta}$, so that $|\mathbf{x}|^{\delta/2} > 2^n$, and

$$|L_1'(\mathbf{x}) \cdots L_n'(\mathbf{x})| < \det(L_1', \ldots, L_n')|\mathbf{x}|^{-\delta/2}.$$

We will apply Proposition A to $L_1', \ldots, L_n', d'$, and with $\delta/2$ in place of δ. To do so we have to estimate the heights $H(L_i')$.

Say L_n' is the real part of L_n, so that when $L_n(\mathbf{X}) = \boldsymbol{\alpha}\mathbf{X}$, we have $L_n'(\mathbf{X}) = \frac{1}{2}(\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}})\mathbf{X}$. Thus

$$H_{K'}(L_n') = H_{K'}(\tfrac{1}{2}(\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}})) = H_{K'}(\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}}) = \prod_{v \in M'(K')} |\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}}|_v.$$

Since $\boldsymbol{\alpha}$ (and $\bar{\boldsymbol{\alpha}}$) has a component equal to 1, we have $|\boldsymbol{\alpha}|_v \geqq 1$, $|\bar{\boldsymbol{\alpha}}|_v \geqq 1$ for each v. Thus

$$|\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}}|_v \leqq \max(|\boldsymbol{\alpha}|_v, |\bar{\boldsymbol{\alpha}}|_v) \leqq |\boldsymbol{\alpha}|_v |\bar{\boldsymbol{\alpha}}|_v$$

when v is nonarchimedean, and

$$|\boldsymbol{\alpha} + \bar{\boldsymbol{\alpha}}|_v \leqq 2 \max(|\boldsymbol{\alpha}|_v, |\bar{\boldsymbol{\alpha}}_v|) \leqq 2|\boldsymbol{\alpha}|_v |\bar{\boldsymbol{\alpha}}|_v$$

when v is archimedean. Therefore

$$H_{K'}(L_n') \leqq 2^{d'} \prod_{v \in M'(K')} |\boldsymbol{\alpha}|_v |\bar{\boldsymbol{\alpha}}|_v$$

$$= 2^{d'} H_{K'}(\boldsymbol{\alpha}) H_{K'}(\bar{\boldsymbol{\alpha}}) = 2^{d'} H_{K'}(L_n)^2,$$

and $H(L_n') \leqq 2H^2(L_n) \leqq 2H^2$. The situation is similar when L_n' is the imaginary part of L_n. More generally, the quantity $H' = \max(H(L_1'), \ldots, H(L_n'))$ has $H' \leqq 2H^2$.

The points $\mathbf{x}$ violating (1.8) have

$$|\mathbf{x}| \geqq \max((n!)^{8/\delta}, H) \geqq \max((n!)^{4/(\delta/2)}, \tfrac{1}{2}H'^{1/2}).$$

Thus by Proposition A, the integer points $\mathbf{x}$ with (1.2) but not (1.8) lie in not more than

$$[(4d')^{2^{24n} \cdot 4\delta^{-2}}] \leqq [(2d)^{12 \cdot 2^{24n}\delta^{-2}}] \leqq t$$

subspaces.

3. The gap principle

Consider rational approximations x/y to a real number α with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{Py^2} \tag{3.1}$$

where $P \geqq 4$. If x/y and x'/y' are two distinct such approximations in their lowest terms with $0 < y \leqq y'$, then

$$\frac{1}{yy'} \leqq \left|\frac{x}{y} - \frac{x'}{y'}\right| \leqq \left|\alpha - \frac{x}{y}\right| + \left|\alpha - \frac{x'}{y'}\right| < \frac{2}{Py^2},$$

so that we have the "gap principle" that $y' > (P/2)y$. Therefore if $x_1/y_1, \ldots, x_v/y_v$ are distinct approximations with (3.1) and with $0 < y_1 \leqq \cdots \leqq y_v \leqq B$, then $y_j \geqq (P/2)^{j-1}$ $(j = 1, \ldots, v)$, so that $(P/2)^{v-1} \leqq B$ and

$$v \leqq 1 + (\log B)/(\log (P/2)) \leqq 1 + 2(\log B)/(\log P).$$

The following lemma is (except for the values of some constants) a generalization of these facts.

LEMMA 3.1: *Let $L_1, \ldots, L_n$ be linearly independent linear forms in* n *variables and with real coefficients. Suppose that*

$$(n!)^4 \leqq P \leqq B, \tag{3.2}$$

and put $Q = (\log B)/(\log P)$. Then the integer points $\mathbf{x}$ *in the ball*

$$|\mathbf{x}| \leqslant B \tag{3.3}$$

and satisfying

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n)P^{-1} \tag{3.4}$$

lie in the union of not more than

$$n^{3n}Q^{n-1}$$

proper subspaces.

Proof: Given linear forms $L = \alpha_1 X_1 + \cdots + \alpha_n X_n = \boldsymbol{\alpha}\mathbf{X}$ and $M = \boldsymbol{\beta}\mathbf{X}$, put $(L, M) = \boldsymbol{\alpha}\boldsymbol{\beta}$. Also put $|L| = (L, L)^{1/2}$ (so that in the case when L has coefficients in a number field K, then $|L| = |L|_{v^*}$ in the notation of the introduction). We will reduce the problem to a situation where $L_1, \ldots, L_n$ are pairwise orthogonal, i.e., $(L_i, L_j) = 0$ for $i \neq j$.

Write $L_i = \boldsymbol{\alpha}_i\mathbf{X}$ $(i = 1, \ldots, n)$ and form the exterior products

$$\hat{\boldsymbol{\alpha}}_i = (-1)^{i-1}\boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_{i-1} \wedge \boldsymbol{\alpha}_{i+1} \wedge \cdots \wedge \boldsymbol{\alpha}_n.$$

(For a definition of such products see [N, IV, Section 6].) Then

$$\boldsymbol{\alpha}_i\hat{\boldsymbol{\alpha}}_j = \delta_{ij} \det(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n),$$

where δ_{ij} is the Kronecker symbol. Now (3.4) is invariant under replacing L_i by $\lambda_i L_i$ $(i = 1, \ldots, n)$ with nonzero $\lambda_1, \ldots, \lambda_n$. If we take $\lambda_i = |\hat{\boldsymbol{\alpha}}_i|/(|\hat{\boldsymbol{\alpha}}_1| \cdots |\hat{\boldsymbol{\alpha}}_n|)^{1/(n-1)}$, then $\boldsymbol{\alpha}_1$ is replaced by $\lambda_i\boldsymbol{\alpha}_i$, and $\hat{\boldsymbol{\alpha}}_i$ is replaced by $\lambda_1 \cdots \lambda_{i-1}\lambda_{i+1} \cdots \lambda_n\hat{\boldsymbol{\alpha}}_i = |\hat{\boldsymbol{\alpha}}_i|^{-1}\hat{\boldsymbol{\alpha}}_i$. We may thus suppose that $|\hat{\boldsymbol{\alpha}}_1| = \cdots = |\hat{\boldsymbol{\alpha}}_n| = 1$.

By symmetry it will suffice to consider solutions of (3.3), (3.4) with

$$|L_n(\mathbf{x})| = \max(|L_1(\mathbf{x})|, \ldots, |L_n(\mathbf{x})|), \tag{3.5}$$

and to prove that they are contained in not more than $n^{-1} \cdot n^{3n} Q^{n-1}$ subspaces. We may write $\hat{\boldsymbol{\alpha}}_n$ as

$$\hat{\boldsymbol{\alpha}}_n = c_1\boldsymbol{\alpha}_1 + \cdots + c_n\boldsymbol{\alpha}_n.$$

Taking the inner product with $\hat{\boldsymbol{\alpha}}_j$ we obtain

$$\hat{\boldsymbol{\alpha}}_n\hat{\boldsymbol{\alpha}}_j = c_j \det(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n) \quad (j = 1, \ldots, n).$$

Since $|\hat{\boldsymbol{\alpha}}_n\hat{\boldsymbol{\alpha}}_j| \leqq |\hat{\boldsymbol{\alpha}}_n||\hat{\boldsymbol{\alpha}}_j| = 1$, with equality for $j = n$, we have $|c_j| \leqq |c_n|$ $(j = 1, \ldots, n)$. Thus $\boldsymbol{\alpha}_n' = c_n^{-1}\hat{\boldsymbol{\alpha}}_n$ has

$$\boldsymbol{\alpha}_n' = c_1'\boldsymbol{\alpha}_1 + \cdots + c_{n-1}'\boldsymbol{\alpha}_{n-1} + \boldsymbol{\alpha}_n$$

with $|c_i'| \leqq 1$, and $\boldsymbol{\alpha}_n'$ is orthogonal to $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{n-1}$. Set $L_n' = \boldsymbol{\alpha}_n'\mathbf{X} = c_1'L_1 + \cdots + c_{n-1}'L_{n-1} + L_n$. Then $\det(L_1, \ldots, L_{n-1}, L_n') = \det(L_1, \ldots, L_{n-1}, L_n)$, moreover L_n' is orthogonal to $L_1, \ldots, L_{n-1}$, and $|L_n'(\mathbf{x})| \leqq nL_n(\mathbf{x})$ by (3.5). Thus we see: *it will suffice to show that when* L_n *is*

orthogonal to $L_1, \ldots L_{n-1}$, *then the points* $\mathbf{x}$ *in* (3.3) *with*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n) n P^{-1} \tag{3.6}$$

lie in at most $n^{-1} \cdot n^{3n} Q^{n-1}$ *subspaces.*

Starting with these new forms $L_1, \ldots, L_{n-1}, L_n$, where L_n is orthogonal to $L_1, \ldots, L_{n-1}$, we repeat the process. Again we may suppose that $|\hat{\boldsymbol{\alpha}}_1| = \cdots = |\hat{\boldsymbol{\alpha}}_n| = 1$. It will suffice to show that the solutions of (3.3), (3.6) with

$$|L_{n-1}(\mathbf{x})| = \max(|L_1(\mathbf{x})|, \ldots, |L_{n-1}(\mathbf{x})|)$$

lie in at most $n^{-1}(n-1)^{-1} n^{3n} Q^{n-1}$ subspaces. Now $\hat{\boldsymbol{\alpha}}_{n-1}$ is orthogonal to $\boldsymbol{\alpha}_n$, hence is spanned by $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{n-1}$:

$$\hat{\boldsymbol{\alpha}}_{n-1} = c_1 \boldsymbol{\alpha}_1 + \cdots + c_{n-1} \boldsymbol{\alpha}_{n-1}.$$

Here $|c_j| \leqq |c_{n-1}|$ $(j = 1, \ldots, n-1)$. We set $L'_{n-1} = \boldsymbol{\alpha}'_{n-1} \mathbf{X}$ with $\boldsymbol{\alpha}'_{n-1} = c_{n-1}^{-1} \hat{\boldsymbol{\alpha}}_{n-1}$. Then L'_{n-1} is orthogonal to $L_1, \ldots, L_{n-2}$ and $|L'_{n-1}(\mathbf{x})| \leqq (n-1)|L_{n-1}(\mathbf{x})|$. We see: *It will suffice to show that when* L_n *is orthogonal to* $L_1, \ldots, L_{n-1}$, *and* L_{n-1} *orthogonal to* $L_1, \ldots L_{n-2}$, *then the solutions of* (3.3) *and*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n) n(n-1) P^{-1}$$

lie in at most $n^{-1}(n-1)^{-1} n^{3n} Q^{n-1}$ *subspaces.*

Continuing in this way we finally see that *it will be enough to prove that for pairwise orthogonal forms* $L_1, \ldots, L_n$, *the points in the ball* (3.3) *with*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n) n! P^{-1} \tag{3.7}$$

lie in not more than $(2n^2)^{n-1} Q^{n-1} \leqq (n!)^{-1} n^{3n} Q^{n-1}$ *subspaces.*

Replacing $L_1, \ldots, L_n$ by multiples, we may finally suppose that $(L_i, L_j) = \delta_{ij}$ and $\det(L_1, \ldots, L_n) = 1$. Then (3.3) yields

$$|L_i(\mathbf{x})| \leqq B \quad (i = 1, \ldots, n). \tag{3.8}$$

With $C = (P/(n!)^2)^{1/(n-1)}$, (3.7) may be rewritten as

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \frac{1}{n! C^{n-1}}. \tag{3.9}$$

Write

$$R = (\log (n!B^n))/\log C.$$

Our solutions satisfy either

$$|L_i(\mathbf{x})| < BC^{-R} = \frac{1}{n!} B^{1-n} \tag{3.10}$$

for some i in $1 \leqq i \leqq n-1$, or

$$C^{-p_i-1}B < |L_i(\mathbf{x})| \leqq C^{-p_i}B \quad (i = 1, \ldots, n-1) \tag{3.11}$$

for certain integers $p_1, \ldots, p_{n-1}$ in $0 \leqq p_i \leqq R$ $(i = 1, \ldots, n-1)$.

Any n points $\mathbf{x}_1, \ldots, \mathbf{x}_n$ satisfying (3.3) and (3.10) for a given i, have by $\det(L_1, \ldots, L_n) = 1$ and by (3.8),

$$|\det(\mathbf{x}_1, \ldots, \mathbf{x}_n)| = |\det(L_i(\mathbf{x}_j))| < n!B^{n-1} \cdot \frac{1}{n!} B^{1-n} = 1,$$

so that in fact $\det(\mathbf{x}_1, \ldots, \mathbf{x}_n) = 0$. Therefore at most $n-1$ such points can be linearly independent, so that these points lie in a fixed proper subspace. On the other hand when $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are satisfying (3.9), as well as (3.11) for given values of $p_1, \ldots, p_{n-1}$, then

$$|L_n(\mathbf{x}_i)| < \frac{1}{n!} B^{1-n} C^{p_1 + \cdots + p_{n-1}},$$

so that

$$|\det(\mathbf{x}_1, \ldots, \mathbf{x}_n)| = |\det(L_i(\mathbf{x}_j))|$$

$$< n! \left(\prod_{i=1}^{n-1} C^{-p_i} B \right) \cdot \frac{1}{n!} B^{1-n} C^{p_1 + \cdots + p_{n-1}} = 1.$$

Again such solutions lie in a proper subspace. The total number of our subspaces is

$$\leqq n - 1 + (R+1)^{n-1}.$$

Now from (3.2) we have $C \geqq P^{1/2(n-1)}$ and $n!B^n < B^{n+1}$, so that

$$R < (\log B^{n+1})/(\log P^{1/2(n-1)}) = (2n^2 - 2)Q.$$

The number of subspaces is

$$\leqq n - 1 + ((2n^2 - 1)Q)^{n-1} \leqq (2n^2Q)^{n-1}.$$

We now briefly return to rational approximations to a real number. This time we consider approximations with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}}. \tag{3.12}$$

If x/y and x'/y' are two distinct such approximations in their lowest terms and with $4^{1/\delta} \leqq y \leqq y'$, then

$$\frac{1}{yy'} < \frac{2}{y^{2+\delta}},$$

so that $y' > \frac{1}{2}y^{1+\delta} \geqq y^{1+(\delta/2)}$, and this is a second "gap principle". Therefore if $x_1/y_1, \ldots, x_v/y_v$ are distinct approximations with (3.12) and with $4^{1/\delta} \leqq y_1 \leqq \cdots \leqq y_v \leqq B$, then

$$4^{(1/\delta)(1+\delta/2)^{v-1}} \leqq B.$$

When $0 < \delta < 1$, then $(1 + \delta/2)^{v-1} < \log B$ and $v < 1 + (\log\log B)/\log(1 + \delta/2)) < 1 + (4/\delta)\log\log B$. When $B > 4$, this is $< (50/\delta)\log\log B$.

A generalization is as follows.

LEMMA 3.2: *Suppose that* $0 < \delta < 1$ *and* $(n!)^{4/\delta} \leqq A < B$. *Then the points* $\mathbf{x}$ *in* $A < |\mathbf{x}| \leqq B$ *with*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n)|\mathbf{x}|^{-\delta} \tag{3.13}$$

lie in

$$< e^n n^{3n} \delta^{1-n}(1 + \log(\log B/\log A))$$

subspaces.

Proof: Initially we consider the case where $B = A^e$. Solutions of (3.13) have

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < P^{-1}|\det(L_1, \ldots, L_n)| \tag{3.14}$$

with $P = A^\delta \geqq n!^4$. By Lemma 3.1, the points $\mathbf{x}$ with (3.14) and $|\mathbf{x}| \leqq B$ lie in

$$\leqq n^{3n}(\log B/\log P)^{n-1} = n^{3n}(e/\delta)^{n-1} < (en^3)^n\delta^{1-n}$$

subspaces.

In general, the interval $A < \xi \leqq B$ is contained in the union of the intervals $A^{e^\nu} < \xi \leqq A^{e^{\nu+1}}$ with $0 \leqq \nu \leqq \log(\log B/\log A)$, so that the number of these intervals is $\leqq 1 + \log(\log B/\log A)$. The Lemma follows.

4. Applications of the gap principle

(*i*) *A reduction*

PROPOSITION B: *Let $L_1, \ldots, L_n$ be independent forms with coefficients in a real number field K of degree d. The points* $\mathbf{x}$ *with*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |L_1| \cdots |L_n||\mathbf{x}|^{-\delta} \tag{4.1}$$

and with

$$|\mathbf{x}| > (2H)^{e^{t_1}}, \tag{4.2}$$

where $0 < \delta < 1$, H satisfies (1.7), *and where*

$$t_1 = [(2d)^{2^{24n}\delta^{-2}}], \tag{4.3}$$

lie in the union of t_1 subspaces.

We will deduce Proposition A. First we observe that (1.2) implies (4.1) (but the difference is not too great by (5.3) below). We still have to consider solutions of (1.2) with $A < |\mathbf{x}| \leqq B$, where $A = \max((n!)^{4/\delta}, \frac{1}{2}H^{1/2})$ and $B = (2H)^{e^{t_1}}$. We observe that

$$A \geqq ((n!)^{4/\delta} \cdot \tfrac{1}{2}H^{1/2})^{1/2} > (2H)^{1/4}$$

and $\log B/\log A < 4e^{t_1} < e^{(3/2)t_1}$, and

$$1 + \log(\log B/\log A) < 1 + (3/2)t_1 < 2t_1.$$

Thus when $B > A$, Lemma 3.2 tells us that the solutions of (1.2) in question lie in

$$< 2t_1(en^3\delta^{-1})^n < e^{3n^4\delta^{-1}}t_1$$

subspaces. By Proposition B, the integer points with (1.2), (2.1) lie in not more than

$$t_1 + e^{3n^4\delta^{-1}}t_1 \leqq t_0$$

subspaces.

It will be convenient to use forms whose coefficients do not necessarily lie in our number field K, but which are proportional to forms with coefficients in K. Such a form will be said to be *defined over* K. Similarly, if $\boldsymbol{\beta} \neq \mathbf{0}$ is proportional to a vector in K^n, we will say that it is defined over K. If $\boldsymbol{\beta}$ is proportional to $\boldsymbol{\alpha}$ in K^n, we put $H(\boldsymbol{\beta}) = H(\boldsymbol{\alpha})$; since $H(\lambda\boldsymbol{\alpha}) = H(\boldsymbol{\alpha})$ for $\lambda \neq 0$ in K, this causes no ambiguity. Similarly we define $H(M)$ when M is a form defined over K. If L has coefficients in K, then $M(\mathbf{X}) = |L|^{-1}L(\mathbf{X})$ is defined over K and *is normalized* in the sense that $|M| = 1$. Clearly it will suffice to prove Proposition B for normalized forms $M_1, \ldots, M_n$ defined over K. The inequality (4.1) then becomes

$$|M_1(\mathbf{x}) \cdots M_n(\mathbf{x})| < |\mathbf{x}|^{-\delta}. \tag{4.4}$$

We will write $M_i(\mathbf{X}) = \boldsymbol{\beta}_i\mathbf{X}$ with $|\boldsymbol{\beta}_i| = 1$ and $H(\boldsymbol{\beta}_i) = H(M_i)$ $(i = 1, \ldots, n)$. The relation (1.7) may be written as

$$H \geqq \max(H(\boldsymbol{\beta}_1), \ldots, H(\boldsymbol{\beta}_n)), \tag{4.5}$$

and (4.4) becomes

$$|\boldsymbol{\beta}_1\mathbf{x}| \cdots |\boldsymbol{\beta}_n\mathbf{x}| < |\mathbf{x}|^{-\delta} \tag{4.6}$$

(*ii*) *Very small solutions*

Suppose that $H > (n!)^{8/\delta}$ and consider solutions of (1.2) with

$$(n!)^{8/\delta} < |\mathbf{x}| \leqq H. \tag{4.7}$$

If $L_1, \ldots L_n$ are complex, we can use the procedure of Section 2 to obtain real forms $L_1', \ldots, L_n'$ such that (1.2), (4.7) yield

$$|L_1'(\mathbf{x}) \cdots L_n'(\mathbf{x})| < 2^n \det(L_1', \ldots, L_n')|\mathbf{x}|^{-\delta} < \det(L_1', \ldots, L_n')|\mathbf{x}|^{-\delta/2}.$$

By Lemma 3.2 with $A = (n!)^{8/\delta}$, $B = H$, and $\delta/2$ in place of δ, so that

$$1 + \log(\log B/\log A) < 1 + \log\log H < 2\log\log H,$$

the integer points in question lie in the union of

$$< 2e^n n^{3n}(\delta/2)^{1-n} \log\log H = (2en^3)^n \delta^{1-n} \log\log H$$

subspaces.

There remain possible solutions with $|\mathbf{x}| \leqq (n!)^{8/\delta}$. There are less than $(2n! + 1)^{8n/\delta}$ such points.

Incidentally, when (1.2) is replaced by

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \det(L_1, \ldots, L_n)H^{-\eta}|\mathbf{x}|^{-\delta}$$

with $\eta > 0$, the integer solutions will lie in t^* subspaces, where t^* may be bounded in terms of n, d, δ, η, but independently of H.

5. On heights

We shall have occasion to use general exterior products. Recall that when $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_p$ lie in $\mathbb{R}^n$ with $1 \leqq p \leqq n$, the exterior product $\boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_p$ lies in $\mathbb{R}^l$ with

$$l = \binom{n}{p}.$$

(See [N, IV, §6].) In particular, $\boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_{n-1}$ lies in $\mathbb{R}^n$ and is orthogonal to each of $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{n-1}$.

LEMMA 5.1: *Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_p$ be linearly independent in K^n where K is an algebraic number field. Then*

$$\boldsymbol{\gamma} = \boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_p$$

has

$$H(\gamma) \leqq H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_p). \tag{5.1}$$

Proof: For every $v \in M'(K)$ we have

$$|\gamma|_v \leqq |\boldsymbol{\alpha}_1|_v \cdots |\boldsymbol{\alpha}_p|_v.$$

This follows from the definition of the exterior product when v is non-archimedean, and is well known when v is archimedean. The assertion now follows from the definition of H_K as a product over $v \in M'(K)$.

LEMMA 5.2: *Again let* $\gamma = \boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_p$, *where* $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_p$ *are linearly independent in* K^n. *Suppose* K *is of degree* d. *Then*

$$|\gamma| H(\gamma)^{-d} \geqq |\boldsymbol{\alpha}_1| \cdots |\boldsymbol{\alpha}_p| (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_p))^{-d}. \tag{5.2}$$

In the case when $p = n$, *we note that* $|\boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_n| = |\det(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n)|$, *so that*

$$|\det(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n)| \geqq |\boldsymbol{\alpha}_1| \cdots |\boldsymbol{\alpha}_n| (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_n))^{-d}. \tag{5.3}$$

Proof: We have $|\gamma|_v \leqq |\boldsymbol{\alpha}_1|_v \cdots |\boldsymbol{\alpha}_p|_v$ for each v. Therefore

$$\begin{aligned} H_K(\gamma) &= \prod_v |\gamma|_v = |\gamma| \prod_{v \neq v^*} |\gamma|_v \leqq |\gamma| \prod_{v \neq v^*} (|\boldsymbol{\alpha}_1|_v \cdots |\boldsymbol{\alpha}_p|_v) \\ &= |\gamma| |\boldsymbol{\alpha}_1|^{-1} \cdots |\boldsymbol{\alpha}_p|^{-1} H_K(\boldsymbol{\alpha}_1) \cdots H_K(\boldsymbol{\alpha}_p). \end{aligned}$$

The lemma follows.

LEMMA 5.3: *Suppose* $\boldsymbol{\alpha}$ *has components in a field* K *of degree* d, *and* $\mathbf{g}$ *is an integer point with* $\boldsymbol{\alpha}\mathbf{g} \neq 0$. *Then*

$$|\boldsymbol{\alpha}\mathbf{g}| \geqq |\boldsymbol{\alpha}| H(\boldsymbol{\alpha})^{-d} |\mathbf{g}|^{1-d}. \tag{5.4}$$

Proof: We have

$$|\boldsymbol{\alpha}\mathbf{g}|_v \leqq |\boldsymbol{\alpha}|_v \qquad \text{for } v \text{ nonarchimedean,}$$

$$|\boldsymbol{\alpha}\mathbf{g}|_v \leqq |\boldsymbol{\alpha}|_v |\mathbf{g}| \quad \text{for } v \text{ archimedean.}$$

The absolute value $|\boldsymbol{\alpha}| = |\boldsymbol{\alpha}|_{v^*}$ is one of the archimedean absolute values. Further there are precisely d elements $v \in M'(K)$ with $|\ldots|_v$ archimedean. By the product formula,

$$\begin{aligned} 1 &= \prod_v |\boldsymbol{\alpha}\mathbf{g}|_v = |\boldsymbol{\alpha}\mathbf{g}| \prod_{v \neq v^*} |\boldsymbol{\alpha}\mathbf{g}|_v \\ &\leqq |\boldsymbol{\alpha}\mathbf{g}| \cdot |\mathbf{g}|^{d-1} \left(\prod_v |\boldsymbol{\alpha}|_v \right) |\boldsymbol{\alpha}|_{v^*}^{-1} \\ &= |\boldsymbol{\alpha}\mathbf{g}| \cdot |\mathbf{g}|^{d-1} H_K(\boldsymbol{\alpha}) |\boldsymbol{\alpha}|^{-1}. \end{aligned}$$

The lemma follows.

LEMMA 5.4: *Let* $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{n-1}$ *be linearly independent in* K^n, *and put* $\boldsymbol{\gamma} = \boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_{n-1}$. *Let* $\mathbf{g}$ *be an integer point with* $\boldsymbol{\gamma}\mathbf{g} \neq 0$. *Then*

$$|\boldsymbol{\gamma}\mathbf{g}| \geqq |\boldsymbol{\alpha}_1| \cdots |\boldsymbol{\alpha}_{n-1}| (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_{n-1}))^{-d} |\mathbf{g}|^{1-d}. \tag{5.5}$$

Remark: Lemmas 5.1, 5.3 together yield the somewhat weaker estimate $|\boldsymbol{\gamma}\mathbf{g}| \geqq |\boldsymbol{\gamma}| (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_{n-1}))^{-d} |\mathbf{g}|^{1-d}$.

Proof: $\boldsymbol{\gamma}\mathbf{g} = \det(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{n-1}, \mathbf{g})$, so that for each v,

$$|\boldsymbol{\gamma}\mathbf{g}|_v \leqq |\boldsymbol{\alpha}_1|_v \cdots |\boldsymbol{\alpha}_{n-1}|_v |\mathbf{g}|_v.$$

Here $|\mathbf{g}|_v = |\mathbf{g}|$ when v is archimedean, and $|\mathbf{g}|_v \leqq 1$ otherwise. By the product formula,

$$\begin{aligned} 1 &= \prod_v |\boldsymbol{\gamma}\mathbf{g}|_v = |\boldsymbol{\gamma}\mathbf{g}| \prod_{v \neq v^*} |\boldsymbol{\gamma}\mathbf{g}|_v \\ &\leqq |\boldsymbol{\gamma}\mathbf{g}| \prod_{v \neq v^*} (|\boldsymbol{\alpha}_1|_v \cdots |\boldsymbol{\alpha}_{n-1}|_v |\mathbf{g}|_v) \\ &\leqq |\boldsymbol{\gamma}\mathbf{g}| |\mathbf{g}|^{d-1} H_K(\boldsymbol{\alpha}_1) \cdots H_K(\boldsymbol{\alpha}_{n-1}) |\boldsymbol{\alpha}_1|^{-1} \cdots |\boldsymbol{\alpha}_{n-1}|^{-1}. \end{aligned}$$

The lemma follows.

LEMMA 5.5: *Let* $A = (\alpha_{ij})$ $(1 \leqq i, j \leqq n)$ *be a nonsingular matrix with entries in* K, *and let* $C = (\gamma_{ij})$ *be its inverse. Let* $\boldsymbol{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{in})$ $(i = 1, \ldots, n)$

be the rows of A, *and* $\boldsymbol{\gamma}_j = (\gamma_{1j}, \ldots, \gamma_{nj})$ $(j = 1, \ldots, n)$ *the "columns" of* C. *Then*

$$|\boldsymbol{\alpha}_i||\boldsymbol{\gamma}_i| \leqq (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_n))^d \quad (i = 1, \ldots, n). \tag{5.6}$$

Proof: Up to a $\pm$sign, $\boldsymbol{\gamma}_i$ equals

$$(\det A)^{-1} \cdot \boldsymbol{\alpha}_1 \wedge \cdots \wedge \boldsymbol{\alpha}_{i-1} \wedge \boldsymbol{\alpha}_{i+1} \wedge \cdots \wedge \boldsymbol{\alpha}_n.$$

Thus by Lemma 5.2,

$$|\boldsymbol{\alpha}_i||\boldsymbol{\gamma}_i| \leqq |\det A|^{-1}|\boldsymbol{\alpha}_1| \cdots |\boldsymbol{\alpha}_n| \leqq (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_n))^d.$$

LEMMA 5.6: *Let* $L_1, \ldots, L_n$ *be linearly independent linear forms with coefficients in* K. *The variables* X_i *may uniquely be expressed as linear combinations*:

$$X_i = \gamma_{i1}L_1 + \cdots + \gamma_{in}L_n \quad (i = 1, \ldots, n).$$

Then

$$|\gamma_{ij}||L_j| \leqq (H(L_1) \cdots H(L_n))^d \quad (1 \leqq i, j \leqq n). \tag{5.7}$$

Proof: Let $L_i = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n = \boldsymbol{\alpha}_i\mathbf{X}$. The matrices $A = (\alpha_{ij})$ and $C = (\gamma_{ij})$ are inverses of each other. By the preceding lemma,

$$|\gamma_{ij}||L_j| = |\gamma_{ij}||\boldsymbol{\alpha}_j| \leqq |\boldsymbol{\gamma}_j||\boldsymbol{\alpha}_j| \leqq (H(\boldsymbol{\alpha}_1) \cdots H(\boldsymbol{\alpha}_n))^d.$$

LEMMA 5.7: *Let* $L_0, L_1, \ldots, L_k$ *be nonzero forms with coefficients in* K, *and heights* $H(L_i) \leqq H$ $(i = 0, \ldots, k)$. *Suppose* L_0 *is a linear combination of* $L_1, \ldots, L_k$. *Then the normalized forms* $M_i = |L_i|^{-1}L_i$ $(i = 0, \ldots, k)$ *satisfy a relation*

$$M_0 = c_1M_1 + \cdots + c_kM_k \tag{5.8}$$

with $|c_i| \leqq H^{(k+1)d}$ $(i = 1, \ldots, k)$.

This lemma, which fits well in the present context, will only be needed in the subsequent paper [12].

Proof: By throwing out some of the forms $L_1, \ldots, L_k$, we may suppose that L_0 is not a linear combination of a proper subset of $L_1, \ldots, L_k$.

Then any k among $L_0, L_1, \ldots, L_k$ are linearly independent. Write $L_i = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n = \boldsymbol{\alpha}_i\mathbf{X}$ and $L_i' = \alpha_{i1}X_1 + \cdots + \alpha_{ik}X_k = \boldsymbol{\alpha}_i'\mathbf{X}$ $(i = 0, \ldots, k)$. We may suppose that $L_1', \ldots, L_k'$ are linearly independent. There is a relation

$$\lambda_0 L_0 + \lambda_1 L_1 + \cdots + \lambda_k L_k = 0 \tag{5.9}$$

where up to signs, $\lambda_i = \det(L_0', \ldots, L_{i-1}', L_{i+1}', \ldots, L_k')$. Here $\lambda_0 \neq 0$ by the independence of $L_1', \ldots, L_k'$, and hence also $\lambda_1 \neq 0, \ldots, \lambda_k \neq 0$, since any k of the forms in (5.9) are linearly independent. We have $H(L_i') \leqq H(L_i) \leqq H$ and therefore

$$H^{-kd}|L_0'| \cdots |L_k'| \leqq |L_i'||\lambda_i| \leqq |L_0'| \cdots |L_k'|$$

by (5.3). Now

$$H^d \geqq H_K(L_i) = H_K(\boldsymbol{\alpha}_i') \prod_v (|\boldsymbol{\alpha}_i|_v/|\boldsymbol{\alpha}_i'|_v) \geqq |\boldsymbol{\alpha}_i|/|\boldsymbol{\alpha}_i'| = |L_i|/|L_i'|,$$

so that

$$H^{-kd}|L_0'| \cdots |L_k'| \leqq |L_i||\lambda_i| \leqq H^d|L_0'| \cdots |L_k'| \quad (i = 0, \ldots, k). \tag{5.10}$$

From (5.9) we get (5.8) with

$$c_i = -\frac{\lambda_i|L_i|}{\lambda_0|L_0|}.$$

Now (5.10) yields the desired bound $|c_i| \leqq H^{(k+1)d}$.

LEMMA 5.8. *Let $L_1, \ldots, L_m$ be nonzero linear forms in n variables and with coefficients in a number field K of degree d. Then if $md < n$, the system of equations*

$$L_i(\mathbf{x}) = 0 \quad (i = 1, \ldots, m)$$

has a nontrivial solution $\mathbf{x} \in \mathbb{Z}^n$ with

$$\boxed{\mathbf{x}} \leqq (H(L_1) \cdots H(L_m))^{d/(n-md)} \tag{5.11}$$

where

$$\boxed{\mathbf{x}} = \max(|x_1|, \ldots, |x_n|).$$

Proof: This follows from Theorem 12 and Corollary 13 in [1]. In that theorem it suffices to consider the special case when $k = \mathbb{Q}$ and $M_i = 1$, and to observe that the smallest solution $\mathbf{x}$ has $|\mathbf{x}|^{n-md} \leqq |\mathbf{x}_1| \cdots |\mathbf{x}_{n-md}|$, when $\mathbf{x}_1, \ldots, \mathbf{x}_{n-md}$ are any linearly independent solutions.

LEMMA 5.9: *Let $\gamma_1, \ldots, \gamma_k$ be vectors in K^n. Suppose we know that there is a $\mathbf{h} \neq \mathbf{0}$ in $\mathbb{Q}^n$ with*

$$\gamma_i \mathbf{h} = 0 \quad (i = 1, \ldots, k). \tag{5.12}$$

Then there is a $\mathbf{h} \neq \mathbf{0}$ in $\mathbb{Z}^n$ with (5.12) *and with*

$$|\mathbf{h}| \leqq H_1^{n-1},$$

where $H_1 = \max(H(\gamma_1), \ldots, H(\gamma_k))$.

Proof: There is a solution $\mathbf{h} \in \mathbb{Q}^n \backslash \mathbf{0}$ of (5.12) with the least possible number of nonzero components, say l nonzero components. Say $\mathbf{h} = (h_1, \ldots, h_l, 0, \ldots, 0)$ with $h_1 h_2 \cdots h_l \neq 0$. Thus $\mathbf{h}$ lies in a coordinate-plane of dimension l. We may replace $\gamma_1, \ldots, \gamma_k$ by their projections $\gamma_1', \ldots, \gamma_k'$ on this coordinate plane, and restrict our attention to this hyperplane, on noting that $H(\gamma_i') \leqq H(\gamma_i)$ $(i = 1, \ldots, k)$.

We therefore may suppose without loss of generality that every solution $\mathbf{h} \in \mathbb{Q}^n \backslash \mathbf{0}$ of (5.12) has all its coordinates nonzero. Thus $\mathbf{h}$ is uniquely determined up to a factor. Let $\sigma_1, \ldots, \sigma_d$ be the embeddings of K into $\mathbb{C}$, and write $\alpha^{(j)} = \sigma_j(\alpha)$ for $\alpha \in K$. Define $K^{(j)} = \sigma_j(K)$, and $\boldsymbol{\alpha}^{(j)} = \sigma_j(\boldsymbol{\alpha})$ (in an obvious notation) for $\boldsymbol{\alpha} \in K^n$. Now $\gamma_i \mathbf{h} = 0$ implies that $\gamma_i^{(j)} \mathbf{h} = 0$ for $j = 1, \ldots, d$, and since we know a solution to (5.12) to exist, the $(kd \times n)$-matrix with rows $\gamma_i^{(j)}$ $(1 \leqq i \leqq k, 1 \leqq j \leqq d)$ has rank $\leqq n - 1$. *We claim that its rank is* $n - 1$: for denote its rank by $m - 1$, so that $1 \leqq m \leqq n$. We may suppose that the first $m - 1$ columns of the matrix with rows $\gamma_i^{(j)}$ have rank $m - 1$; then also the first m columns constitute a matrix of rank $m - 1$. This $(kd \times m)$-matrix has rows $\gamma_i'^{(j)}$ $(1 \leqq i \leqq k, 1 \leqq j \leqq d)$, where $\gamma_i'^{(j)} \in \mathbb{C}^m$ is the projection of $\gamma_i^{(j)}$ on the first m coordinates. There is by linear algebra a vector $\mathbf{h}' \neq \mathbf{0}$ in $\mathbb{C}^m$, unique up to a factor, with $\gamma_i'^{(j)} \mathbf{h}' = 0$ $(1 \leqq i \leqq k, 1 \leqq j \leqq d)$. We may choose $\mathbf{h}'$ to have its components in the compositum E of the conjugate fields $K^{(1)}, \ldots, K^{(d)}$. Now E is normal, and for ϕ in the Galois group of $E/\mathbb{Q}$, we have

$$\phi(\gamma_i^{(j)}) \cdot \phi(\mathbf{h}') = 0 \quad (1 \leqq i \leqq k, 1 \leqq j \leqq d).$$

But $\phi(\gamma_i^{(j)}) = \phi\sigma_j(\gamma_i)$, and $\phi\sigma_1, \ldots, \phi\sigma_d$ is just a permutation of $\sigma_1, \ldots, \sigma_d$. Thus

$$\boldsymbol{\gamma}_i^{(j)} \cdot \phi(\mathbf{h}') = 0 \quad (1 \leqq i \leqq k,\ 1 \leqq j \leqq d).$$

Thus up to a factor, $\phi(\mathbf{h}')$ is the same as $\mathbf{h}'$. If, as we may, we choose $\mathbf{h}'$ with some nonzero rational coordinate, then in fact $\phi(\mathbf{h}') = \mathbf{h}'$ for every ϕ in the Galois group, so that $\mathbf{h}' \in \mathbb{Q}^m$. This yields a rational solution of (5.12) with at most m nonzero coordinates, and by the supposition made at the beginning, this shows that $m = n$.

Thus the matrix with rows $\gamma_i^{(j)}$ $(1 \leqq i \leqq k,\ 1 \leqq j \leqq d)$ has rank $n - 1$. Let $\boldsymbol{\delta}_1, \ldots, \boldsymbol{\delta}_{n-1}$ be any $n - 1$ linearly independent rows among these kd rows. Then $\boldsymbol{\delta} = \boldsymbol{\delta}_1 \wedge \cdots \wedge \boldsymbol{\delta}_{n-1}$ has $\gamma_i^{(j)}\boldsymbol{\delta} = 0$ $(1 \leqq i \leqq k,\ 1 \leqq j \leqq d)$, and $\boldsymbol{\delta}$ is proportional to $\mathbf{h}$. Thus by Lemma 5.1,

$$H(\mathbf{h}) = H(\boldsymbol{\delta}) \leqq H(\boldsymbol{\delta}_1) \cdots H(\boldsymbol{\delta}_{n-1}) \leqq H_1^{n-1}.$$

We may choose $\mathbf{h}$ to have coprime components in $\mathbb{Z}$. Then

$$|\mathbf{h}| = H(\mathbf{h}) \leqq H_1^{n-1}.$$

6. Geometry of numbers

We will collect some results from this area. Throughout, $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ will be linearly independent vectors in $\mathbb{R}^n$ with a determinant of modulus B^{-1}. The inequalities

$$|\boldsymbol{\beta}_i \mathbf{x}| \leqq 1 \quad (i = 1, \ldots, n) \tag{6.1}$$

define a parallelepiped Π of volume $2^n B$. Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of Π, so that λ_j is the least number λ such that there are j linearly independent integer points in $\lambda\Pi$, i.e., in the set with $|\boldsymbol{\beta}_i \mathbf{x}| \leqq \lambda$ $(i = 1, \ldots, n)$. We have $0 < \lambda_1 \leqq \cdots \leqq \lambda_n < \infty$ and, according to Minkowski,

$$(n!B)^{-1} \leqq \lambda_1 \cdots \lambda_n \leqq B^{-1}. \tag{6.2}$$

(See e.g., Cassels [3], Th. V on p. 218). Fix linearly independent integer points $\mathbf{g}_1, \ldots, \mathbf{g}_n$ with

$$\mathbf{g}_j \in \lambda_j \Pi \quad (j = 1, \ldots, n). \tag{6.3}$$

Then

$$|\det(\mathbf{g}_1, \ldots, \mathbf{g}_n)| \leqq n!. \tag{6.4}$$

(See Cassels [3], Corollary on p. 219, or [N, IV, (1.9)] where we had wasted a factor $n!$ by using a weak form of Minkowski's inequality.)

LEMMA 6.1: *Let* $\varrho_1, \ldots, \varrho_n$ *be reals with*

$$\varrho_1 \geqq \varrho_2 \geqq \cdots \geqq \varrho_n > 0, \tag{6.5}$$

$$\varrho_1 \lambda_1 \leqq \cdots \leqq \varrho_n \lambda_n, \tag{6.6}$$

$$\varrho_1 \varrho_2 \cdots \varrho_n = 1. \tag{6.7}$$

Then there is a permutation of $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *such that after this permutation, the new parallelepiped* Π' *defined by*

$$|\varrho_i \boldsymbol{\beta}_i \mathbf{x}| \leqq 1 \quad (i = 1, \ldots, n)$$

has successive minima $\lambda_1', \ldots, \lambda_n'$ *with*

$$2^{-n} \varrho_i \lambda_i \leqq \lambda_i' \leqq 4^{n^2} \varrho_i \lambda_i \quad (i = 1, \ldots, n).$$

Moreover, every integer point $\mathbf{x}$ *not in the subspace* S_{i-1} spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_{i-1}$ (with $\mathbf{g}_1, \ldots, \mathbf{g}_n$ the points in (6.3)) has

$$\max(|\varrho_1 \boldsymbol{\beta}_1 \mathbf{x}|, \ldots, |\varrho_n \boldsymbol{\beta}_n \mathbf{x}|) \geqq 2^{-n} \varrho_i \lambda_i.$$

For a proof of this lemma, which is essentially due to Davenport [4], see [N, IV, Theorem 3A].

Given linearly independent $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$, let $\boldsymbol{\beta}_1^*, \ldots, \boldsymbol{\beta}_n^*$ be the *reciprocal* basis, i.e., let $\boldsymbol{\beta}_i^*$ $(1 \leqq i \leqq n)$ be the vector with $\boldsymbol{\beta}_i^* \boldsymbol{\beta}_j = \delta_{ij}$, the Kronecker symbol $(1 \leqq i, j \leqq n)$. The parallelepiped Π^* given by

$$|\boldsymbol{\beta}_i^* \mathbf{x}| \leqq 1 \quad (i = 1, \ldots, n)$$

is the *reciprocal* parallelepiped to the parallelepiped given by (6.1). Denote the successive minima of Π^* by $\lambda_1^*, \ldots, \lambda_n^*$.

Now if again $\mathbf{g}_1, \ldots, \mathbf{g}_n$ are the integer points in (6.3), let $\mathbf{g}_1^*, \ldots, \mathbf{g}_n^*$ be the reciprocal basis, and put

$$\hat{\mathbf{g}}_i = \mathbf{g}_1 \wedge \cdots \wedge \mathbf{g}_{i-1} \wedge \mathbf{g}_{i+1} \wedge \cdots \wedge \mathbf{g}_n \quad (i = 1, \ldots, n), \tag{6.8}$$

so that $\hat{\mathbf{g}}_1, \ldots, \hat{\mathbf{g}}_n$ lie in $\mathbb{Z}^n$. We have $\mathbf{g}_i \hat{\mathbf{g}}_j = \pm \delta_{ij} \det(\mathbf{g}_1, \ldots, \mathbf{g}_n)$ and therefore

$$\hat{\mathbf{g}}_j = \pm \det(\mathbf{g}_1, \ldots, \mathbf{g}_n) \mathbf{g}_j^* \quad (1 \leqq j \leqq n). \tag{6.9}$$

LEMMA 6.2: *We have*

$$n^{-1} \leqq \lambda_i^* \lambda_{n+1-i} \leqq (n-1)! \quad (1 \leqq i \leqq n) \tag{6.10}$$

and

$$|\boldsymbol{\beta}_i^* \hat{\mathbf{g}}_j| \leqq (n-1)! \lambda_j^{-1} \quad (1 \leqq i, j \leqq n). \tag{6.11}$$

This is due to Mahler [8].

Proof: For (6.11) we just have to compute the constants in the proof of [N, IV, Theorem 4A]. On page 94 of this work we obtain $|A_{ij}| \leqq (n-1)! \lambda_1 \cdots \lambda_{j-1} \lambda_{j+1} \cdots \lambda_n$, and thus

$$\begin{aligned} |\boldsymbol{\beta}_i^* \mathbf{g}_j^*| &\leqq (n-1)! \lambda_1 \cdots \lambda_n \lambda_j^{-1} |\det(\boldsymbol{\beta}_l \mathbf{g}_m)|^{-1} \\ &= (n-1)! \lambda_1 \cdots \lambda_n \lambda_j^{-1} B |\det(\mathbf{g}_1, \ldots, \mathbf{g}_n)|^{-1} \\ &\leqq (n-1)! \lambda_j^{-1} |\det(\mathbf{g}_1, \ldots, \mathbf{g}_n)|^{-1} \end{aligned}$$

by (6.2). Combining this with (6.9) we obtain (6.11). But (6.11) yields $\lambda_i^* \lambda_{n+1-i} \leqq (n-1)!$ and the right hand inequality in (6.10).

Put

$$F(\mathbf{x}) = \max_i |\boldsymbol{\beta}_i \mathbf{x}|, \quad F^*(\mathbf{x}) = \max_i |\boldsymbol{\beta}_i^* \mathbf{x}|,$$

$$\bar{F}(\mathbf{x}) = \sum_{i=1}^{n} |\boldsymbol{\beta}_i^* \mathbf{x}|.$$

Then F, $\bar{F}$ are "distance functions" which are polar to each other (Cassels [3], VIII.5). Thus if $\bar{\lambda}_1, \ldots, \bar{\lambda}_n$ are the successive minima of the set of $\mathbf{x}$ with $\bar{F}(\mathbf{x}) \leqq 1$, we have $\bar{\lambda}_i \lambda_{n+1-i} \geqq 1$ $(i = 1, \ldots, n)$ (loc. cit., Theorem VI). But now $\bar{F}(\mathbf{x}) \leqq nF^*(\mathbf{x})$, and since $\lambda_1^*, \ldots, \lambda_n^*$ are the successive minima of the set of $\mathbf{x}$ with $F^*(\mathbf{x}) \leqq 1$, we have $\bar{\lambda}_i \leqq n\lambda_i^*$, and the first inequality in (6.10).

Suppose now that $1 \leqq p \leqq n$ and $l = \binom{n}{p}$. Let $C(n, p)$ be the set of p-tuples $\sigma = \{i_1 < \cdots < i_p\}$ of integers i in $1 \leqq i \leqq n$; the cardinality of this set is l. If $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are a basis of $\mathbb{R}^n$ with $|\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)| = B^{-1}$, put

$$\boldsymbol{\beta}_\sigma = \boldsymbol{\beta}_{i_1} \wedge \cdots \wedge \boldsymbol{\beta}_{i_p} \tag{6.12}$$

for $\sigma \in C(n, p)$. The vectors $\boldsymbol{\beta}_\sigma$ with $\sigma \in C(n, p)$ are a basis of $\mathbb{R}^l$, and the determinant of this basis is of modulus $B^{-lp/n}$ (see [N, VI, §6]). The inequalities

$$|\boldsymbol{\beta}_\sigma \mathbf{X}^{(p)}| \leqq 1 \quad (\sigma \in C(n, p)),$$

where $\mathbf{X}^{(p)}$ stands for a vector in $\mathbb{R}^l$, define a parallelepiped in $\mathbb{R}^l$ of volume $2^l B^{lp/n}$ called the *pth pseudocompound* of Π (see [N, VI, §7]).

Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of Π, and for $\tau \in C(n, p)$ put

$$\lambda_\tau = \prod_{i \in \tau} \lambda_i.$$

There is an ordering $\tau_1, \ldots, \tau_l$ of the elements of $C(n, p)$ such that

$$\lambda_{\tau_1} \leqq \cdots \leqq \lambda_{\tau_l}.$$

Let $\mathbf{g}_1, \ldots, \mathbf{g}_n$ be independent integer points with $\mathbf{g}_j \in \lambda_j \Pi$, i.e., with $|\boldsymbol{\beta}_i \mathbf{g}_j| \leqq \lambda_j$ $(1 \leqq i, j \leqq n)$. For $\tau = \{j_1 < \cdots < j_p\}$ in $C(n, p)$, put

$$\mathbf{G}_\tau = \mathbf{g}_{j_1} \wedge \cdots \wedge \mathbf{g}_{j_p}.$$

By Laplace's identity,

$$|\boldsymbol{\beta}_\sigma \mathbf{G}_\tau| \leqq p! \lambda_\tau \quad (\sigma, \tau \in C(n, p)). \tag{6.13}$$

(See [N, IV, (7.4)].)

LEMMA 6.3: (Mahler [9]). *The successive minima $v_1, \ldots, v_l$ of the pseudocompound have*

$$\frac{1}{l!(p!)^{l-1}} \lambda_{\tau_i} \leqq v_i \leqq p! \lambda_{\tau_i} \quad (i = 1, \ldots, l). \tag{6.14}$$

Proof: The upper bound follows from (6.13). Now (6.2) yields

$$(n!B)^{-lp/n} \leqq \lambda_{\tau_1} \cdots \lambda_{\tau_l} \leqq B^{-lp/n},$$

and the analogue of (6.2) in $\mathbb{R}^l$ is

$$\frac{1}{l!} B^{-lp/n} \leqq v_1 \cdots v_l \leqq B^{-lp/n}.$$

Thus

$$(l!)^{-1} \leqq \prod_{i=1}^{l} (v_i/\lambda_{\tau_i}) \leqq (n!)^{lp/n},$$

and the upper bound in (6.14) implies the lower bound.

LEMMA 6.4: *Define the points* $\mathbf{G}_\tau$ *and* $\tau_1, \ldots, \tau_l$ *as above. Once the span of* $\mathbf{G}_{\tau_1}, \ldots, \mathbf{G}_{\tau_{l-1}}$ *in* $\mathbb{R}^l$ *is determined, the span of* $\mathbf{g}_1, \ldots, \mathbf{g}_{n-p}$ *in* $\mathbb{R}^n$ *is determined.*

Proof: Denote the span of $\mathbf{G}_{\tau_1}, \ldots, \mathbf{G}_{\tau_{l-1}}$ by $S^{(p)}$. It is an $(l-1)$-dimensional subspace of $\mathbb{R}^l$. Now if $(\mathbf{G}_{\tau_1})^*, \ldots, (\mathbf{G}_{\tau_l})^*$ is reciprocal to $\mathbf{G}_{\tau_1}, \ldots, \mathbf{G}_{\tau_l}$, then $(\mathbf{G}_{\tau_l})^*$ lies in the orthogonal complement of $S^{(p)}$. On the other hand if $\mathbf{g}_1^*, \ldots, \mathbf{g}_n^*$ is reciprocal to $\mathbf{g}_1, \ldots, \mathbf{g}_n$ in $\mathbb{R}^n$, and if $(\mathbf{G}^*)_\tau = \mathbf{g}_{j_1}^* \wedge \cdots \wedge \mathbf{g}_{j_p}^*$ for $\tau = \{j_1 < \cdots < j_p\}$, then $(\mathbf{G}_{\tau_l})^* = (\mathbf{G}^*)_{\tau_l}$ (see [N, IV, (6.12)]). Thus $(\mathbf{G}^*)_{\tau_l}$ lies in the orthogonal complement of $S^{(p)}$. Now clearly $\tau_l = \{n-p+1, n-p+2, \ldots, n\}$, so that $\mathbf{g}_{n-p+1}^* \wedge \cdots \wedge \mathbf{g}_n^*$ lies in the orthogonal complement of $S^{(p)}$. But once the direction of $\mathbf{g}_{n-p+1}^* \wedge \cdots \wedge \mathbf{g}_n^*$ in $\mathbb{R}^l$ is given, the span T of $\mathbf{g}_{n-p+1}^*, \ldots, \mathbf{g}_n^*$ in $\mathbb{R}^n$ is determined. (See [N, IV, Lemma 6C].) Then the span of $\mathbf{g}_1, \ldots, \mathbf{g}_{n-p}$ is the orthogonal complement of T.

7. Geometry of numbers continued

Again $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ will be linearly independent vectors of $\mathbb{R}^n$ with determinant of modulus B^{-1}. We will make the additional assumption that they are *normalized*, i.e., that

$$|\boldsymbol{\beta}_1| = \cdots = |\boldsymbol{\beta}_n| = 1.$$

Throughout, $c_1, \ldots, c_n$ will be reals with $|c_i| \leqq 1$ $(i = 1, \ldots, n)$ and with

$$c_1 + \cdots + c_n = 0. \tag{7.1}$$

Given $Q > 1$, let $\Pi = \Pi(Q)$ be the parallelepiped

$$|\boldsymbol{\beta}_i \mathbf{x}| \leqq Q^{c_i} \quad (i = 1, \ldots, n). \tag{7.2}$$

This is the same as $|\boldsymbol{\beta}_i' \mathbf{x}| \leqq 1$ $(i = 1, \ldots, n)$ with $\boldsymbol{\beta}_i' = Q^{-c_i}\boldsymbol{\beta}_i$, and the theory of the last section applies. We define minima $\lambda_j = \lambda_j(Q)$ with respect

to $\Pi(Q)$, and again we have points $\mathbf{g}_1, \ldots, \mathbf{g}_n$ with (6.3). The reciprocal parallelepiped $\Pi^* = \Pi^*(Q)$ is given by $|\boldsymbol{\beta}_i^* \mathbf{x}| \leqq Q^{-c_i}$ $(i = 1, \ldots, n)$.

LEMMA 7.1: *The point* $\hat{\mathbf{g}}_n = \mathbf{g}_1 \wedge \cdots \wedge \mathbf{g}_{n-1}$ *has*

$$|\hat{\mathbf{g}}_n| < n! B \lambda_1 \cdots \lambda_{n-1} Q. \tag{7.3}$$

Proof: Write $\hat{\boldsymbol{\beta}}_i = \boldsymbol{\beta}_1 \wedge \cdots \wedge \boldsymbol{\beta}_{i-1} \wedge \boldsymbol{\beta}_{i+1} \wedge \cdots \wedge \boldsymbol{\beta}_n$, so that in analogy to (6.9), $\hat{\boldsymbol{\beta}}_i = \pm B^{-1} \boldsymbol{\beta}_i^*$ $(i = 1, \ldots, n)$. By Laplace's identity

$$\begin{aligned} |\hat{\boldsymbol{\beta}}_i \hat{\mathbf{g}}_n| &\leqq (n-1)! \lambda_1 \cdots \lambda_{n-1} Q^{c_1 + \cdots + c_{i-1} + c_{i+1} + \cdots + c_n} \\ &= (n-1)! \lambda_1 \cdots \lambda_{n-1} Q^{-c_i}, \end{aligned} \tag{7.4}$$

and thus

$$|\boldsymbol{\beta}_i^* \hat{\mathbf{g}}_n| \leqq B(n-1)! \lambda_1 \cdots \lambda_{n-1} Q^{-c_i} \quad (i = 1, \ldots, n). \tag{7.5}$$

If we write $\hat{\mathbf{g}}_n$ as $\hat{\mathbf{g}}_n = u_1 \boldsymbol{\beta}_1 + \cdots + u_n \boldsymbol{\beta}_n$, this says that $|u_i| \leqq B(n-1)! \lambda_1 \cdots \lambda_{n-1} Q^{-c_i}$, and therefore

$$|\hat{\mathbf{g}}_n| < n! B \lambda_1 \cdots \lambda_{n-1} Q.$$

Lemma 5.2 remains true for vectors defined over K. In particular, if $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are independent and normalized, we have

$$1 \leqq B = |\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|^{-1} \leqq (H(\boldsymbol{\beta}_1) \cdots H(\boldsymbol{\beta}_n))^d.$$

From now on, H will be a quantity with (4.5), and we obtain

$$1 \leqq B = |\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|^{-1} \leqq H^{nd}. \tag{7.6}$$

The estimate (7.3) yields

$$|\hat{\mathbf{g}}_n| < n! \lambda_1 \cdots \lambda_{n-1} H^{nd} Q. \tag{7.7}$$

LEMMA 7.2: *Let* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *be linearly independent and normalized vectors defined over* K. *Let* $\Pi(Q)$ *be given by* (7.2), *and let* $\mathbf{g}_1, \ldots, \mathbf{g}_n$, *as well as* $\hat{\mathbf{g}}_n$, *be as above. Then for every subscript* i *with*

$$\boldsymbol{\beta}_i^* \hat{\mathbf{g}}_n \neq 0 \tag{7.8}$$

we have

$$|\hat{\mathbf{g}}_n| > \frac{1}{n!H^n}\left(\frac{Q^{c_i}}{\lambda_1 \cdots \lambda_{n-1}}\right)^{1/d}.$$

Proof: Lemma 5.4 remains true for vectors defined over K. In particular, since $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are normalized, since $\hat{\boldsymbol{\beta}}_i = \boldsymbol{\beta}_1 \wedge \cdots \wedge \boldsymbol{\beta}_{i-1} \wedge \boldsymbol{\beta}_{i+1} \wedge \cdots \wedge \boldsymbol{\beta}_n$, and since $\hat{\boldsymbol{\beta}}_i \hat{\mathbf{g}}_n \neq 0$, we have

$$|\hat{\boldsymbol{\beta}}_i \hat{\mathbf{g}}_n| \geqq (H(\boldsymbol{\beta}_1) \cdots H(\boldsymbol{\beta}_{i-1})H(\boldsymbol{\beta}_{i+1}) \cdots H(\boldsymbol{\beta}_n))^{-d}|\hat{\mathbf{g}}_n|^{1-d}.$$

On the other hand we have (7.4), so that

$$|\hat{\mathbf{g}}_n|^d \geqq |\hat{\mathbf{g}}_n|^{d-1} > \frac{1}{n!H^{nd}}\left(\frac{Q^{c_i}}{\lambda_1 \cdots \lambda_{n-1}}\right).$$

There is a linear form $V = V(\mathbf{X}) = v_1\mathbf{X}_1 + \cdots + v_n\mathbf{X}_n$ with coprime integer coefficients vanishing on $\mathbf{g}_1, \ldots, \mathbf{g}_{n-1}$. This form is unique up to a factor ± 1. Write

$$\boxed{V} = \max(|v_1|, \ldots, |v_n|) = \boxed{\mathbf{v}}.$$

We will write

$$q = n - 1. \tag{7.9}$$

Also, $\mathfrak{S}$ will denote the set of subscripts i with

$$c_i > 0.$$

LEMMA 7.3: *Suppose* $\delta > 0$,

$$\lambda_q = \lambda_q(Q) \leqq Q^{-\delta} \tag{7.10}$$

and

$$Q^{q\delta} \geqq (n!)^{6d}H^{2nd}. \tag{7.11}$$

Suppose there is an $i \in \mathfrak{S}$ *with* $\boldsymbol{\beta}_i^* \hat{\mathbf{g}}_n \neq 0$, *i.e., with* (7.8). *Then*

$$Q^{q\delta/2d} < \boxed{V} < Q. \tag{7.12}$$

Proof: Clearly $\hat{\mathbf{g}}_n$ is a multiple of the coefficient vector $\mathbf{v}$ of V, say $\hat{\mathbf{g}}_n = m\mathbf{v}$. In view of (6.4), the g.c.d. of the components of $\hat{\mathbf{g}}_n$ is $\leqq n!$, so that $1 \leqq m \leqq n!$.

Now (7.7), (7.10) yield

$$\boxed{V} = \boxed{\mathbf{v}} \leqq |\hat{\mathbf{g}}_n| < n!H^{nd}Q^{-q\delta}Q,$$

and the second inequality in (7.12) follows from (7.11). On the other hand, Lemma 7.2 with $c_i > 0$ yields

$$\boxed{V} = \boxed{\mathbf{v}} \geqq n^{-1}|\mathbf{v}| \geqq (n!)^{-2}|\hat{\mathbf{g}}_n|$$

$$> \frac{1}{(n!)^3 H^n} Q^{q\delta/d} \geqq Q^{q\delta/2d}$$

by (7.10), (7.11).

LEMMA 7.4: *Again let* $\Pi = \Pi(Q)$ *be the parallelepiped* (7.2), *where* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *in* $\mathbb{R}^n$ *are normalized and have determinant of modulus* B^{-1}. *Suppose that*

$$n!B\lambda_q^n < 1, \tag{7.13}$$

and that there is an integer point $\mathbf{h} \neq \mathbf{0}$ *with*

$$\boldsymbol{\beta}_i^*\mathbf{h} = 0 \quad \textit{for every } i \textit{ with } nB|\mathbf{h}|\lambda_q Q^{c_i} \geqq 1. \tag{7.14}$$

Then

$$\mathbf{g}_i\mathbf{h} = 0 \quad \text{for} \quad i = 1, 2, \ldots, q. \tag{7.15}$$

Proof: The inequality (6.10) is valid for Π and its reciprocal Π^*. In particular, for i with $nB|\mathbf{h}|\lambda_q Q^{c_i} < 1$, we have

$$\lambda_2^* \geqq 1/(n\lambda_{n-1}) = 1/(n\lambda_q) > B|\mathbf{h}|Q^{c_i}.$$

Since $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are normalized we have $|\boldsymbol{\beta}_i^*| \leqq B$, and thus

$$|\boldsymbol{\beta}_i^*\mathbf{h}| \leqq B|\mathbf{h}| < \lambda_2^* Q^{-c_i}$$

for such i. Since (7.14) holds for the other values of i, it follows that $\mathbf{h}$ lies in the interior of $\lambda_2^*\Pi^*$.

On the other hand, we observe (7.5); and since $1 \leqq n\lambda_2^* \lambda_{n-1}$, we obtain

$$|\boldsymbol{\beta}_i^* \hat{\mathbf{g}}_n| \leqq n!B\lambda_1 \cdots \lambda_{n-2}\lambda_{n-1}^2 \lambda_2^* Q^{-c_i}$$

$$\leqq n!B\lambda_q^n \lambda_2^* Q^{-c_i}$$

$$< \lambda_2^* Q^{-c_i} \quad (i = 1, \ldots, n).$$

Thus $\hat{\mathbf{g}}_n$ also lies in the interior of $\lambda_2^* \Pi^*$. Since any two integer points in the interior of $\lambda_2^* \Pi^*$ are proportional, we see that $\mathbf{h}$, $\hat{\mathbf{g}}_n$ are proportional. Now $\hat{\mathbf{g}}_n$ is orthogonal to $\mathbf{g}_1, \ldots, \mathbf{g}_{n-1}$, and hence so is $\mathbf{h}$, and (7.15) is established.

LEMMA 7.5: *Let* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *be linearly independent, normalized vectors defined over K. Suppose there is an integer point* $\mathbf{h} \neq \mathbf{0}$ *with*

$$\boldsymbol{\beta}_i^* \mathbf{h} = 0 \tag{7.16}$$

for $i \in \mathfrak{S}$, *i.e., for every i with* $c_i > 0$. *In fact, let* $\mathbf{h}$ *be an integer point with this property having smallest possible norm* $|\mathbf{h}|$. *Suppose that* (7.10) *holds, i.e., that* $\lambda_q \leqq Q^{-\delta}$ *with* $\delta > 0$, *and that*

$$Q^{\delta} > n!H^{n(n+d-1)}. \tag{7.17}$$

Then (7.15) *holds, i.e.* $\mathbf{g}_1\mathbf{h} = \cdots = \mathbf{g}_q\mathbf{h} = 0$.

Proof: It will suffice to check the conditions (7.13), (7.14) of the preceding lemma. Now

$$n!B\lambda_q^n < n!H^{nd}Q^{-\delta} < 1$$

by (7.6), (7.17). On the other hand, by Lemmas 5.9, 5.1,

$$|\mathbf{h}| \leqq \max_{i \in \mathfrak{S}} H(\boldsymbol{\beta}_i^*)^{n-1} = \max_{i \in \mathfrak{S}} H(\hat{\boldsymbol{\beta}}_i)^{n-1}$$

$$\leqq \max_{t} H(\hat{\boldsymbol{\beta}}_t)^{n-1} \leqq H^{n^2-n}.$$

Therefore $nB|\mathbf{h}|\lambda_q Q^{c_i} \geqq 1$ implies that

$$nH^{n(d+n-1)}Q^{-\delta}Q^{c_i} \geqq 1,$$

so that $Q^{c_i} > 1$ by (7.17). We may conclude that $i \in \mathfrak{S}$, so that $\boldsymbol{\beta}_i^* \mathbf{h} = 0$ by (7.16). But this is (7.14).

LEMMA 7.6: *Let again* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *be normalized and independent, and defined over* K. *Let* $\Pi(Q)$ *be given by* (7.2), *and let* $S = S(Q)$ *be the subspace spanned by* $\mathbf{g}_1, \ldots, \mathbf{g}_q$. *Suppose that*

$$0 < \delta < 1.$$

Then the values of Q *with* $\lambda_q = \lambda_q(Q) < Q^{-\delta}$, *and lying in an interval*

$$Q_0 < Q \leqq Q_0^E \tag{7.18}$$

where $E > 1$ *and*

$$Q_0^{n\delta/2} > n! H^{nd} \tag{7.19}$$

give rise to not more than

$$1 + 4\delta^{-1} \log E$$

distinct subspaces $S(Q)$.

Proof: The argument will be similar to the one in Section 3. Consider an interval of the type

$$Q_0 < Q \leqq Q_0^{1+(\delta/2)} \tag{7.20}$$

with (7.19). Let $Q_1, \ldots, Q_n$ be any values of Q in (7.20) with $\lambda_q(Q) < Q^{-\delta}$. For $1 \leqq j \leqq n$, let $\mathbf{h}_j$ be one of the points $\mathbf{g}_1(Q_j), \ldots, \mathbf{g}_q(Q_j)$. Then

$$|\boldsymbol{\beta}_i \mathbf{h}_j| \leqq \lambda_q(Q_j) Q_j^{c_i} \leqq Q_j^{c_i - \delta} \quad (1 \leqq i, j \leqq n).$$

Now

$$|\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)| = B|\det(\boldsymbol{\beta}_i \mathbf{h}_j)| \leqq n! B \max_{j_1, \ldots, j_n} Q_{j_1}^{c_1 - \delta} \cdots Q_{j_n}^{c_n - \delta},$$

where the maximum is over permutations $j_1, \ldots, j_n$ of $1, \ldots, n$. For i with $c_i - \delta < 0$ we have

$$Q_{j_i}^{c_i - \delta} < Q_0^{c_i - \delta},$$

whereas for i with $c_i - \delta \geqq 0$ we have

$$Q_{l_i}^{c_i-\delta} \leqq Q_0^{(c_i-\delta)(1+(\delta/2))}.$$

We obtain (on observing (7.1))

$$|\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)| \leqq n!BQ_0^{-n\delta+(\delta/2)\Sigma},$$

where Σ is the sum of $c_i - \delta$ over i with $c_i - \delta \geqq 0$, so that $\Sigma < n$. Thus

$$|\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)| < n!BQ_0^{-n\delta/2} \leqq n!H^{nd}Q_0^{-n\delta/2} < 1$$

by (7.19). We may conclude that $\det(\mathbf{h}_1, \ldots, \mathbf{h}_n) = 0$, so that $\mathbf{h}_1, \ldots, \mathbf{h}_n$ are linearly dependent. In fact, any vectors $\mathbf{h}_1, \ldots, \mathbf{h}_n$ with $\mathbf{h}_i \in S(Q_i)$ are linearly dependent. Therefore $S(Q_1) = \cdots = S(Q_n)$, and for Q in (7.20) with (7.10), the subspace $S(Q)$ is always the same.

The given interval (7.18) is contained in the union of not more than

$$1 + (\log E/\log(1 + (\delta/2))) < 1 + 4\delta^{-1}\log E$$

intervals of the type (7.20).

8. The index

The ring of polynomials

$$P = P(X_{11}, \ldots, X_{1n}; \ldots; X_{m1}, \ldots, X_{mn})$$

in nm variables and with integer coefficients will be denoted $\mathfrak{R}$. Given an m-tuple

$$\mathbf{r} = (r_1, \ldots, r_m)$$

of natural numbers, $\mathfrak{R}'$ will denote the set of polynomials in $\mathfrak{R}$ which are homogeneous of degree $\mathfrak{I}_h$ in the block of variables $X_{h1}, \ldots, X_{hn}$ $(1 \leqq h \leqq m)$. The symbol will denote nm-tuples of nonnegative integers

$$(i_{11}, \ldots, i_{1n}; \ldots; i_{m1}, \ldots, i_{mn}),$$

and we will use the notation

$$(\mathfrak{I}/\mathbf{r}) = \sum_{h=1}^{m} \frac{i_{h1} + \cdots + i_{hn}}{r_h}.$$

We put

$$P^{\mathfrak{I}} = \frac{1}{i_{11}! \cdots i_{mn}!} \frac{\partial^{i_{11} + \cdots + i_{mn}}}{\partial X_{11}^{i_{11}} \cdots \partial X_{mn}^{i_{mn}}} P.$$

With $\sqcap$ denoting the maximum modulus of coefficients of a polynomial, we have for $P \in \mathfrak{R}'$ that

$$\sqcap P^{\mathfrak{I}} \sqcap \leqq 2^r \sqcap P \sqcap \tag{8.1}$$

with

$$r = r_1 + \cdots + r_m. \tag{8.2}$$

(See [N, VI, Lemma 5A].)

Let $L_1, \ldots, L_m$ be nonzero linear forms, where L_h is a form in the variables $X_{h1}, \ldots, X_{hm}$, so that $L_h = \alpha_{h1} X_{h1} + \cdots + \alpha_{hn} X_{hn}$ $(h = 1, \ldots, m)$. Let T be the subspace of $\mathbb{R}^{mn}$ defined by $L_1 = \cdots = L_m = 0$. In view of lemmas 4B, 4C of [N, VI], the *index* of a polynomial $P \in \mathfrak{R}$ with respect to $(L_1, \ldots, L_m; \mathbf{r})$ could be defined as follows. When $P = 0$, set Ind $P = \infty$. When $P \neq 0$, *the index is the least value of* c *such that there is an* $\mathfrak{I}$ *with* $(\mathfrak{I}/\mathbf{r}) = c$, *such that* $P^{\mathfrak{I}}$ *is not identically zero on* T. Furthermore, if $\alpha_{h1} \neq 0$ for $h = 1, \ldots, m$, *then there is an*

$$\mathfrak{I} = (i_1, 0, \ldots, 0; \ldots; i_m, 0, \ldots, 0) \tag{8.3}$$

with $(\mathfrak{I}/r) \neq 0$ *and with* $P^{\mathfrak{I}}$ *not identically zero on* T.

We now quote a version of Roth's Lemma from [N, VI, Theorem 10 B].

LEMMA 8.1: *Suppose that* $0 < \theta < 1/12$, *that* m *is a positive integer, and*

$$\omega = 24 \cdot 2^{-m} (\theta/12)^{2m-1}. \tag{8.4}$$

Let $r_1, \ldots, r_m$ *be positive integers with*

$$\omega r_h \geqq r_{h+1} \quad (1 \leqq h \leqq m). \tag{8.5}$$

Let $V_1, \ldots V_m$ be nonzero linear forms in n variables with coprime rational integer coefficients where V_h is a polynomial in $X_{h1}, \ldots, X_{hn}$. Suppose that $0 < \Gamma \leqq q = n - 1$, and that

$$\boxed{V_h}^{r_h} \geqq \boxed{V_1}^{r_1\Gamma} \quad (2 \leqq h \leqq m),^{\dagger} \tag{8.6}$$

$$\boxed{V_h}^{\omega\Gamma} \geqq 2^{3mq^2} \quad (1 \leqq h \leqq m). \tag{8.7}$$

Let $P \in \mathfrak{R}'$ be nonzero, and with

$$\boxed{P}^{q^2} \leqq \boxed{V_1}^{\omega r_1 \Gamma}. \tag{8.8}$$

Then the index of P with respect to $(V_1, \ldots, V_m; \mathbf{r})$ is $\leqq \theta$.

9. The index theorem and the polynomial theorem

$\mathfrak{R}'$ *consists of polynomials*

$$P = \sum c(j_{11}, \ldots, j_{mn}) X_{11}^{j_{11}} \cdots X_{mn}^{j_{mn}}, \tag{9.1}$$

where the sum is over nonnegative integers $j_{11}, \ldots, j_{mn}$ with $j_{h1} + \cdots + j_{hn} = r_h$ for $h = 1, \ldots, m$. Given h, the number of such $j_{h1}, \ldots, j_{hn}$ is $\binom{r_h + n - 1}{n - 1}$, so that the number N of summands in (9.1) is

$$N = \binom{r_1 + n - 1}{n - 1} \cdots \binom{r_m + n - 1}{n - 1} \leqq 2^{(r_1+n-1)+\cdots+(r_m+n-1)} < 2^{mn+r}, \tag{9.4}$$

with r given by (8.2). Thus there are N coefficients $c(j_{11}, \ldots, j_{mn})$, and $\mathfrak{R}'$ is a free $\mathbb{Z}$-module of rank N.

LEMMA 9.1: *Suppose $L = \alpha_1 X_1 + \cdots + \alpha_n X_n \neq 0$ has coefficients in a field K of degree d. With P given by* (9.1), *construct a polynomial P* in the nm–m variables*

$$X_{12}, \ldots, X_{1n}; \ldots; X_{m2}, \ldots, X_{mn}$$

---

† The condition (10.3) in [N, VI, Theorem 10B] should be $2 \leqq h \leqq m$.

by setting

$$P^* = P^{\mathfrak{I}}(-\alpha_2 X_{12} - \cdots - \alpha_n X_{1n}, \alpha_1 X_{12}, \ldots, \alpha_1 X_{1n}; \ldots;$$

$$- \alpha_2 X_{m2} - \cdots - \alpha_n X_{mn}, \alpha_1 X_{m2}, \ldots, \alpha_1 X_{mn}),$$

where $\mathfrak{I}$ *is of the type* (8.3):

$$\mathfrak{I} = (i_1, 0, \ldots, 0; \ldots; i_m, 0, \ldots, 0). \tag{9.3}$$

Then every coefficient γ *of* P^* *is a linear form* $\gamma = \mathfrak{L}_\gamma((c(j_{11}, \ldots, j_{mn})))$ *in the* N *coefficients* $c(j_{11}, \ldots, j_{mn})$ *of* P, *and every such form* $\mathfrak{L}_\gamma \neq 0$ *has*

$$H(\mathfrak{L}_\gamma) < 2^{mn}(3n^{1/2}H(L))^r. \tag{9.4}$$

Proof: Only the inequality (9.4) needs to be shown. Now P^* is the sum of N summands

$$\pm c(j_{11}, \ldots, j_{mn}) \binom{j_{11}}{i_1} \cdots \binom{j_{mn}}{i_m}$$

$$\times (\alpha_2 X_{12} + \cdots + \alpha_n X_{1n})^{j_{11}-i_1}(\alpha_1 X_{12})^{j_{12}} \cdots (\alpha_1 X_{1n})^{j_{1n}}$$

$$\cdots (\alpha_2 X_{m2} + \cdots + \alpha_n X_{mn})^{j_{m1}-i_m}(\alpha_1 X_{m2})^{j_{m2}} \cdots (\alpha_1 X_{mn})^{j_{mn}}$$

$$= \pm c(j_{11}, \ldots, j_{mn}) P_1 P_2 \ldots P_m,$$

where for $1 \leqq h \leqq m$,

$$P_h = \binom{j_{h1}}{i_h} (\alpha_2 X_{h2} + \cdots + \alpha_n X_{hn})^{j_{h1}-i_h}(\alpha_1 X_{h2})^{j_{h2}} \cdots (\alpha_1 X_{hn})^{j_{hn}}.$$

If η_h denotes a typical coefficient of P_h, then for archimedean v,

$$|\eta_h|_v \leqq \binom{j_{h1}}{i_h} |\alpha_1|_v^{j_{h2}+\cdots+j_{hn}}(|\alpha_2|_v + \cdots + |\alpha_n|_v)^{j_{h1}-i_h}$$

$$\leqq 2^{r_h}(|\alpha_1|_v + \cdots + |\alpha_n|_v)^{j_{h1}+\cdots+j_{hn}-i_h}$$

$$= 2^{r_h}(|\alpha_1|_v + \cdots + |\alpha_n|_v)^{r_h - i_h}$$

$$\leqq 2^{r_h}(n(|\alpha_1|_v^2 + \cdots + |\alpha_n|_v^2))^{(1/2)(r_h - i_h)}$$

$$\leqq (2n^{1/2})^{r_h}|\boldsymbol{\alpha}|_v^{r_h - i_h}.$$

Thus every coefficient η of $P_1 P_2 \cdots P_m$ has

$$|\eta|_v \leqq (2n^{1/2})^r |\boldsymbol{\alpha}|_v^t$$

with $t = r - i_1 - \cdots - i_m$. On the other hand for nonarchimedean v we have

$$|\eta_h|_v \leqq |\boldsymbol{\alpha}|_v^{j_{h1} + \cdots + j_{hn} - i_h} = |\boldsymbol{\alpha}|_v^{r_h - i_h}$$

and therefore

$$|\eta|_v \leqq |\boldsymbol{\alpha}|_v^t.$$

Let $\boldsymbol{\beta}_\gamma$ be the coefficient vector of $\mathfrak{L}_\gamma$. Then $\boldsymbol{\beta}_\gamma$ has N components, and each component is a coefficient η of the type considered above. Therefore

$$|\boldsymbol{\beta}_\gamma|_v \leqq N^{1/2}(2n^{1/2})^r |\boldsymbol{\alpha}|_v^t < 2^{nm}(3n^{1/2})^r |\boldsymbol{\alpha}|_v^t$$

when v is archimedean, and

$$|\boldsymbol{\beta}_\gamma|_v \leqq |\boldsymbol{\alpha}|_v^t$$

when v is nonarchimedean, so that

$$H_K(\mathfrak{L}_\gamma) = H_K(\boldsymbol{\beta}_\gamma) < (2^{nm}(3n^{1/2})^r)^d H_K(\boldsymbol{\alpha})^t,$$

where d is the degree of K. The assertion (9.4) follows on extracting dth roots and noting that $t \leqq r$.

Given a linear form $L = \alpha_1 X_1 + \cdots + \alpha_n X_n$, we make m forms out of it by setting $L^{[h]} = \alpha_1 X_{h1} + \cdots + \alpha_n X_{hn}$ $(h = 1, \ldots, m)$. The index *with respect to* $(L; \mathbf{r})$ is defined as the index with respect to $(L^{[1]}, \ldots, L^{[m]}; \mathbf{r})$.

INDEX THEOREM: *Suppose $L_1, \ldots, L_s$ are nonzero linear forms with coefficients in a field of degree d. Suppose*

$$H(L_i) \leqq H \quad (i = 1, \ldots, s). \tag{9.5}$$

Suppose that $\varepsilon > 0$ *and*

$$m > 4\varepsilon^{-2} \log (2sd). \tag{9.6}$$

Then given $\mathbf{r} = (r_1, \ldots, r_m)$, *there exists a nonzero polynomial* $P \in \mathfrak{R}'$ *with*
(i) $\operatorname{Ind} P \geqq ((1/n) - \varepsilon)m$ *with respect to* $(L_i; \mathbf{r})$ $(i = 1, \ldots, s)$,
(ii) $\boxed{P} < 2^{mn} (3n^{1/2}H)^r$.

This is Theorem 6A of [N, VI], but with a more explicit estimate for $\boxed{P}$.

Proof: Write P in the form (9.1); the number N of available coefficients is given by (9.2). Let us deal with condition (i) for a particular $(L_i; \mathbf{r})$. Write $L_i = \alpha_1 X_1 + \cdots + \alpha_n X_n$; we may suppose without loss of generality that $\alpha_1 \neq 0$. In view of what we said in the last section, the index condition will be satisfied if every $P^{\mathfrak{I}}$ with $\mathfrak{I}$ of the type (8.3) with $(\mathfrak{I}/\mathbf{r}) < (n^{-1} - \varepsilon)m$ vanishes on the subspace T_i given by $L_i^{[1]} = \cdots = L_i^{[m]} = 0$.

Keep i and $\mathfrak{I}$ fixed at the moment. The condition then is that P^* as defined in Lemma 9.1 vanishes identically. Now P^* is homogeneous in $X_{h2}, \ldots, X_{hn}$ of degree $r_h - i_h$ $(h = 1, \ldots m)$, hence has

$$\binom{r_1 - i_1 + n - 2}{n - 2} \cdots \binom{r_m - i_m + n - 2}{n - 2} = f_1(i_1) \cdots f_m(i_m),$$

say, potential coefficients. Each coefficient γ is a linear form $\gamma = \mathfrak{L}_\gamma$ in the coefficients $c(j_{11}, \ldots j_{mn})$. Each of the $f_1(i_1) \cdots f_m(i_m)$ potential coefficients has to be set equal to zero. This gives $f_1(i_1) \cdots f_m(i_m)$ linear equations in the $c(j_{11}, \ldots, j_{mn})$. Summing over i from 1 to s, and summing over $\mathfrak{I}$, we obtain

$$M = s \sum f_1(i_1) \cdots f_m(i_m)$$

equations, where the sum Σ is over nonnegative $i_1, \ldots, i_m$ with $(i_1/r_1) + \cdots + (i_m/r_m) < (n^{-1} - \varepsilon)m$. By an estimnate in [N, p. 179],

$$M \leqq s \binom{r_1 + n - 1}{r_1} \cdots \binom{r_m + n - 1}{r_m} e^{-\varepsilon^2 m/4} = sNe^{-\varepsilon^2 m/4},$$

so that $M \leqq N/2d$ by (9.6). Each linear equation is given in terms of a linear form $\mathfrak{L}_\gamma$ whose height may be estimated by (9.4). We now apply Lemma 5.8

with N, M in place of n, m. We obtain a nonzero polynomial P with

$$\begin{aligned}|P| &\leqq \max_{\gamma} (H(\mathfrak{L}_\gamma))^{Md/(N-Md)} \\ &\leqq \max_{\gamma} H(\mathfrak{L}_\gamma) \\ &< 2^{mn}(3n^{1/2}H)^r.\end{aligned}$$

Let $L_1, \ldots, L_n$ be linearly independent forms with coefficients in a field of degree d, and let $M_1, \ldots, M_n$ be their normalizations, i.e.,

$$M_i = |L_i|^{-1} L_i \quad (i = 1, \ldots, n).$$

We may write $X_1, \ldots, X_n$ as linear combinations of $M_1, \ldots, M_n$, and $X_{h1}, \ldots, X_{hn}$ as linear combinations of $M_1^{[h]}, \ldots, M_n^{[h]}$ $(h = 1, \ldots, m)$. Now if (9.6) holds with $s = n$, let P be the polynomial of the Index Theorem. Given an mn-tuple $\mathfrak{J}$, we may write $P^{\mathfrak{J}}$ uniquely as

$$P^{\mathfrak{J}} = \sum_{j_{11}, \ldots, j_{mn}} d^{\mathfrak{J}}(j_{11}, \ldots j_{mn}) M_1^{[1]j_{11}} \cdots M_n^{[1]j_{1n}} \cdots M_1^{[m]j_{m1}} \cdots M_n^{[m]j_{mn}}. \tag{9.7}$$

Here the summation may be restricted to $j_{h1} + \cdots + j_{hn} \leqq r_h$ $(h = 1, \ldots, m)$.

POLYNOMIAL THEOREM:
(i) *When* $(\mathfrak{J}/\mathbf{r}) \leqq 2\varepsilon m$, *then* $d^{\mathfrak{J}}(j_{11}, \ldots, j_{mn}) = 0$ *unless*

$$\left| \left(\sum_{h=1}^{m} \frac{j_{hk}}{r_h} \right) - \frac{m}{n} \right| < 3mn\varepsilon \quad (1 \leqq k \leqq n).$$

(ii) *Each coefficient* $d^{\mathfrak{J}}$ *has*

$$|d^{\mathfrak{J}}(j_{11}, \ldots, j_{mn})| < 2^{mn}(6n^{3/2}H^{nd+1})^r.$$

Except for the more explicit estimate for $|d^{\mathfrak{J}}|$, this is Theorem 7A of [N, VI].

Proof: (i) is exactly as in [N]. So let us turn to (ii). Writing $X_i = \eta_{i1}M_1 + \cdots + \eta_{in}M_n$ we have $|\eta_{ij}| \leqq H^{nd}$ by Lemma 5.6. A typical monomial $X_{11}^{j_{11}} \ldots X_{mn}^{j_{mn}}$ may be written as

$$X_{11}^{j_{11}} \cdots X_{mn}^{j_{mn}} = \left(\sum_{k=1}^{n} \eta_{1k} M_k^{[1]} \right)^{j_{11}} \cdots \left(\sum_{k=1}^{n} \eta_{nk} M_k^{[m]} \right)^{j_{mn}},$$

and this is a polynomial in the forms $M_k^{[h]}$ with coefficients of modulus

$$\leqq (nH^{nd})^{j_{11}+\cdots+j_{mn}} \leqq (nH^{nd})^r.$$

Since $\boxed{P^{\mathfrak{J}}} \leqq 2^r\boxed{P}$, we obtain

$$|d^{\mathfrak{J}}(j_{11}, \ldots, j_{mn})| \leqq (2nH^{nd})^r\boxed{P}$$
$$< 2^{mn}(6n^{3/2}H^{nd+1})^r.$$

10. The index of P with respect to certain rational linear forms

Let $L_i(\mathbf{X}) = \boldsymbol{\alpha}_i\mathbf{X}$ $(i = 1, \ldots, n)$ be linearly independent linear forms with coefficients in K and with (9.5), and let $M_i(\mathbf{X}) = \boldsymbol{\beta}_i\mathbf{X}$ $(i = 1, \ldots, n)$ be their respective normalizations. We will suppose that $\varepsilon > 0$ and $m > 4\varepsilon^{-2}\log(2nd)$, and that P is the polynomial of the Index and Polynomial Theorems. As in section 7, $c_1, \ldots, c_n$ will be reals of modulus $\leqq 1$ satisfying (7.1), and $\Pi(Q)$ will be the parallelepiped (7.2). Given Q, we have minima $\lambda_1 = \lambda_1(Q), \ldots, \lambda_n = \lambda_n(Q)$, and we have certain points $\mathbf{g}_1 = \mathbf{g}_1(Q), \ldots, \mathbf{g}_n = \mathbf{g}_n(Q)$. Again, $V = V(Q)$ will be the linear form with coprime integer coefficients and vanishing on $\mathbf{g}_1, \ldots, \mathbf{g}_q$ where $q = n - 1$. If $V = v_1X_1 + \cdots + v_nX_n$ write $V^{[h]} = v_1X_{h1} + \cdots + v_nX_{hn}$ $(h = 1, \ldots, m)$.

LEMMA 10.1: *Suppose that* $0 < \delta < 1$ *and* $0 < \varepsilon \leqq \delta/15n^2$. *Let* $Q_1, \ldots, Q_m$ *satisfy*

$$r_1 \log Q_1 \leqq r_h \log Q_h \leqq (1 + \varepsilon)r_1 \log Q_1 \quad (h = 1, \ldots, m), \tag{10.1}$$

$$\lambda_q(Q_h) \leqq Q_h^{-\delta} \quad (h = 1, \ldots, m), \tag{10.2}$$

and

$$Q_h^{\delta} > 2^{24n}\varepsilon^{-4}H^{8nd} \quad (h = 1, \ldots, m). \tag{10.3}$$

Then P *has index* $\geqq m\varepsilon$ *with respect to* $(V^{[1]}(Q_1), \ldots, V^{[m]}(Q_m); \mathbf{r})$.

This corresponds to Theorem 9A in [N, VI].

Proof: Let T be the subspace of $\mathbb{R}^{mn}$ where $V^{[1]}(Q_1), \ldots, V^{[m]}(Q_m)$ vanish. It will suffice to show that $P^{\mathfrak{J}} = 0$ on T whenever $(\mathfrak{J}/\mathbf{r}) < \varepsilon m$. Let Γ_h

($h = 1, \ldots, m$) be the "grid" consisting of points

$$\mathbf{u} = u_1\mathbf{g}_1(Q_h) + \cdots + u_q\mathbf{g}_q(Q_h),$$

where $u_1, \ldots, u_q$ run through the integers in $1 \leqq u_i \leqq [\varepsilon^{-1}] + 1$. Just as in [N, page 189], it will suffice to show that

$$P^{\mathfrak{Z}}(\mathbf{u}_1, \ldots, \mathbf{u}_m) = 0 \tag{10.4}$$

when $(\mathfrak{Z}/\mathbf{r}) < 2\varepsilon m$ and $\mathbf{u}_h \in \Gamma_h$ ($h = 1, \ldots, m$).

Now

$$P^{\mathfrak{Z}}(\mathbf{u}_1, \ldots, \mathbf{u}_m) = \sum_{j_{11}, \ldots, j_{mn}} d^{\mathfrak{Z}}(j_{11}, \ldots, j_{mn}) M_1(\mathbf{u}_1)^{j_{11}} \cdots M_n(\mathbf{u}_m)^{j_{mn}}. \tag{10.5}$$

Here

$$|M_k(\mathbf{u}_h)| \leqq n(\varepsilon^{-1} + 1)\lambda_q(Q_h)Q_h^{c_k} < (2n/\varepsilon)Q_h^{c_k - \delta} \quad (1 \leqq k \leqq n, 1 \leqq h \leqq m),$$

so that

$$|M_k(\mathbf{u}_1)^{j_{1k}} \cdots M_k(\mathbf{u}_m)^{j_{mk}}| < (2n/\varepsilon)^{j_{1k} + \cdots + j_{mk}} (Q_1^{j_{1k}} \cdots Q_m^{j_{mk}})^{c_k - \delta}.$$

By assertion (ii) of the Polynomial Theorem we have $d^{\mathfrak{Z}}(j_{11}, \ldots, j_{mn}) = 0$ unless

$$\sum_{h=1}^{m} j_{hk} \log Q_h \geqq r_1 \log Q_1 \cdot \sum_{h=1}^{m} \frac{j_{hk}}{r_h} \geqq r_1 \log Q_1 \cdot \left(\frac{1}{n} - 3n\varepsilon\right) m,$$

$$\sum_{h=1}^{m} j_{hk} \log Q_h \leqq (1 + \varepsilon) r_1 \log Q_1 \cdot \sum_{h=1}^{m} \frac{j_{hk}}{r_h} \leqq r_1 \log Q_1 \cdot (1 + \varepsilon)\left(\frac{1}{n} + 3n\varepsilon\right) m,$$

so that for $k = 1, \ldots, n$, in view of $(1 + \varepsilon)((1/n) + 3n\varepsilon) < (1/n) + (7/2)n\varepsilon$,

$$\left|\left(\sum_{h=1}^{m} j_{hk} \log Q_h\right) - (r_1 \log Q_1) \cdot \frac{m}{n}\right|$$

$$\leqq r_1 \log Q_1 \cdot (7/2)nm\varepsilon < r_1 \log Q_1 \cdot \delta m/(4n).$$

We may infer that

$$|M_k(\mathbf{u}_1)^{j_{1k}} \cdots M_k(\mathbf{u}_m)^{j_{mk}}| < (2n/\varepsilon)^{j_{1k} + \cdots + j_{mk}} Q_1^{r_1(m/n)(c_k - \delta)} Q_1^{r_1(\delta m/4n)|c_k - \delta|}.$$

By assertion (ii) of the Polynomial Theorem, and since $c_1 + \cdots + c_n = 0$, and each $|c_k - \delta| \leqq 2$, every summand in (10.5) has modulus

$$< 2^{mn}(6n^{3/2}H^{2nd})^r(2n/\varepsilon)^r Q_1^{-r_1 m\delta/2}$$

$$< (2^{5n}\varepsilon^{-1}H^{2nd})^r(Q_1^{-r_1}\cdots Q_m^{-r_m})^{\delta/2(1+\varepsilon)}$$

by (10.1). The number of summands in (10.5) is $\leqq 2^{n(r_1+\cdots+r_m)} = 2^{nr}$, so that

$$|P^{\mathfrak{Z}}(\mathbf{u}_1, \ldots, \mathbf{u}_m)| < \prod_{h=1}^{m} (2^{6n}\varepsilon^{-1}H^{2nd}Q_h^{-\delta/4})^{r_h} < 1$$

by (10.3). We may conclude that $P^{\mathfrak{Z}}(\mathbf{u}_1, \ldots, \mathbf{u}_m) = 0$.

11. The next to last minimum

LEMMA 11.1: *Suppose that* $0 < \delta < 1$ *and*

$$m > 900n^4\delta^{-2}\log 2nd. \tag{11.1}$$

Put

$$E = \tfrac{1}{12}2^m(180)^{2m-1}. \tag{11.2}$$

Let $\Pi(Q)$ *be the parallelepiped* (7.2), *where* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *are independent and normalized vectors defined over a field of degree* d, *and with heights* $H(\boldsymbol{\beta}_i) \leqq H$ $(i = 1, \ldots, n)$. *Suppose there is no integer point* $\mathbf{h} \neq \mathbf{0}$ *with* (7.16) *for every* $i \in \mathfrak{S}$. *Then the numbers* Q *with*

$$\lambda_q(Q) < Q^{-\delta} \tag{11.3}$$

and with

$$Q^{\delta^2} > (2^{4n}H)^{4d^2mE} \tag{11.4}$$

lie in at most $m - 1$ *intervals of the type*

$$Q_h < Q \leqq Q_h^E \quad (h = 1, \ldots, m-1). \tag{11.5}$$

Proof: We first remark that $m > (\log 2)^{-1}(\log 2n^2d) + 1$ by (11.1), so that $2^{m-1} > 2n^2d$ and

$$E > e^{4n^2d} > n^{4nd}. \tag{11.6}$$

This yields

$$Q^{\delta} > Q^{\delta^2} > (2^{4n}H)^{1000\delta^{-2}n^{4nd}} > 2^{24n}(15n^2)^4\delta^{-4}H^{8nd} = 2^{24n}\varepsilon^{-4}H^{8nd} \tag{11.7}$$

and thus (10.3) if we set

$$\varepsilon = \delta/15n^2. \tag{11.8}$$

Suppose the lemma were false. Let Q_1 be the infimum of the values of Q with (11.3) and (11.4). Then Q with (11.3), (11.4) will have $Q > Q_1$. If all the values of Q with (11.3), (11.4) were in the interval $Q_1 < Q \leqq Q_1^E$, the lemma would be correct. So there are $Q \geqq Q_1^E$ with (11.3); let Q_2 be their infimum. And so forth. Continuing in this way we find $Q_1, \ldots, Q_m$ with $\lambda_q(Q_h) \leqq Q_h^{-\delta}$ $(h = 1, \ldots, m)$ and

$$Q_{h+1} \geqq Q_h^E \quad (h = 1, \ldots, m-1). \tag{11.9}$$

Let r_1 be so large that

$$r_1 > \varepsilon^{-1} \log Q_m/\log Q_1.$$

For $h = 2, \ldots, m$ put

$$r_h = [r_1 \log Q_1/\log Q_h] + 1.$$

Then for $h = 1, \ldots, m$,

$$r_1 \log Q_1 \leqq r_h \log Q_h \leqq r_1 \log Q_1 + \log Q_h < (1+\varepsilon)r_1 \log Q_1, \tag{11.10}$$

and (10.1) holds. By (11.1) and (11.8), m satisfies (9.6) (with $s = n$) of the Index Theorem. Let P be the polynomial of the Index and Polynomial Theorems. Since (10.1), (10.2), (10.3) are satisfied, we see that P has index $\geqq m\varepsilon$ with respect to $(V^{[1]}(Q_1), \ldots, V^{[m]}(Q_m); \mathbf{r})$.

Now with $\theta = 1/15$ and with ω given by (8.4), we have $E = 2/\omega$, so that

$$\omega r_h \geqq \omega \frac{r_{h+1} \log Q_{h+1}}{(1 + \varepsilon) \log Q_h} = \frac{2r_{h+1}}{(1 + \varepsilon)E} \frac{\log Q_{h+1}}{\log Q_h} \geqq r_{h+1}$$

by (11.10), (11.9). Thus (8.5) is satisfied.

Since there is no $\mathbf{h}$ with (7.16) for every $i \in \mathfrak{S}$, there is for each Q_h an $i \in \mathfrak{S}$ with $\boldsymbol{\beta}_i^* \hat{\mathbf{g}}_n \neq 0$ where $\hat{\mathbf{g}}_n = \hat{\mathbf{g}}_n(Q_h)$, so that by Lemma 7.3 (on noting that (11.4) implies (7.11)),

$$Q_h^{\Gamma} < |V_h| < Q_h$$

with

$$\Gamma = q\delta/2d, \tag{11.11}$$

where $V_h = V(Q_h)$. We obtain

$$|V_h|^{r_h} > Q_h^{r_h \Gamma} \geqq Q_1^{r_1 \Gamma} > |V_1|^{r_1 \Gamma} \quad (h = 1, \ldots, m),$$

i.e., (8.6). Furthermore, by (11.11), and since $E = 2/\omega$,

$$|V_h|^{\omega\Gamma} > Q_h^{\omega\Gamma^2} = Q_h^{2\Gamma^2/E} = Q_h^{q^2\delta^2/(2d^2E)} > 2^{3mq^2},$$

in view of (11.4). Thus (8.7) holds. Finally, from the Index Theorem,

$$|P| < 2^{mn}(3n^{1/2}H)^r < (2^{4n}H)^{r_1 m},$$

and therefore

$$|P|^{q^2} < (2^{4n}H)^{r_1 q^2 m} < (2^{4n}H)^{r_1 q^2 m E \omega}$$

$$= (2^{4n}H)^{r_1 \omega \Gamma^2 m E \cdot 4d^2/\delta^2} < Q_h^{r_1 \omega \Gamma^2} < |V_h|^{r_1 \omega \Gamma}$$

by (11.4); thus also (8.8) holds.

By Roth's Lemma, the index of P with respect to $(V_1, \ldots, V_m; r)$ is $\leqq \theta$. Since $\theta = 1/15 < m\delta/15n^2 = m\varepsilon$, this contradicts the lower bound given above.

LEMMA 11.2: *Let δ, m, E be as in Lemma 11.1, and $\Pi(Q)$ the parallelepiped* (7.2), *where $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are independent and normalized, defined over a field of degree d and with heights $\leqq H$. Given Q, let $S = S(Q)$ be the subspace spanned by $\mathbf{g}_1 = \mathbf{g}_1(Q), \ldots, \mathbf{g}_q(Q)$ (so that S is the zero set of the linear form $V = V(Q)$).*

Then as Q ranges over values with (11.3) *and* (11.4), *$S(Q)$ ranges over less than*

$$m(1 + 4\delta^{-1} \log E)$$

distinct subspaces.

Proof: Suppose at first that there is an integer point $\mathbf{h} \neq \mathbf{0}$ with (7.16) for $i \in \mathfrak{S}$. Let $\mathbf{h}$ be a point with this property with smallest possible norm. Then since (11.4) implies (7.17), Lemma 7.5 shows that $S(Q)$ consists of $\mathbf{x}$ with $\mathbf{hx} = 0$, and hence is fixed.

If there is no such integer point $\mathbf{h}$, we may apply Lemma 11.1. Then since (11.4) implies (7.19), Lemma 7.6 shows that for Q in a particular interval (11.5), $S(Q)$ will run through not more than $1 + 4\delta^{-1} \log E$ distinct subshapes. Summation over h in $1 \leqq h < m$ gives the desired result.

We have to give another version of the lemma just proved.

LEMMA 11.3: *Suppose that* $0 < \delta < \frac{1}{2}$,[†]

$$m > 3600n^4\delta^{-2} \log 2nd, \tag{11.12}$$

and that E is given by (11.2). *Given positive reals $A_1, \ldots, A_n$ with*

$$A_1 \ldots A_n = 1, \tag{11.13}$$

let $\Pi = \Pi(A_1, \ldots, A_n)$ be the parallelepiped

$$|\boldsymbol{\beta}_i \mathbf{x}| \leqq A_i \quad (i = 1, \ldots, n), \tag{11.14}$$

where $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are as in Lemma 11.2. Let $\lambda_j(A_1, \ldots, A_n)$ for $j = 1, \ldots, n$ be the successive minima of $\Pi(A_1, \ldots, A_n)$, let $\mathbf{g}_j = \mathbf{g}_j(A_1, \ldots, A_n)$ be corresponding integer points, and $S(A_1, \ldots, A_n)$ the subspace spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_q$.

[†] Here and in the lemmas below, the upper bounds for δ are unnecessarily small and could be increased.

Then for values of $A_1, \ldots, A_n, Q$ *with*

$$Q^{\delta^2} > (2^{4n}H)^{16d^2mE}, \tag{11.15}$$

$$Q \geqq \max(A_1, \ldots, A_n, A_1^{-1}, \ldots, A_n^{-1}) \tag{11.16}$$

and

$$\lambda_q(A_1, \ldots, A_n) < Q^{-\delta}, \tag{11.17}$$

$S(A_1, \ldots, A_n)$ *is among not more than*

$$m(6/\delta)^n(1 + 8\delta^{-1} \log E)$$

fixed subspaces.

Proof: Writing $A_i = Q^{\eta_i}$ $(i = 1, \ldots, n)$, we have $-1 \leqq \eta_i \leqq 1$ and $\eta_1 + \cdots + \eta_n = 0$. Let v be the least integer $\geqq 2/\delta$, and $\xi_l = -1 + (l/v)$ $(l = 0, 1, \ldots, 2v)$. We claim that it is possible to pick integers $l_1, \ldots, l_n$ in $0 \leqq l \leqq 2v$ with

$$|\eta_i - \xi_{l_i}| < v^{-1} \quad (i = 1, \ldots, n) \tag{11.18}$$

and

$$|(\eta_1 - \xi_{l_1}) + \cdots + (\eta_i - \xi_{l_i})| < v^{-1} \quad (i = 1, \ldots, n). \tag{11.19}$$

Choose l_1 with $|\eta_1 - \xi_{l_1}| \leqq (2v)^{-1}$. If $l_1, \ldots, l_{j-1}$ have been chosen with (11.18), (11.19) valid for $i = 1, \ldots, j-1$, and if

$$(\eta_1 - \xi_{l_1}) + \cdots + (\eta_{j-1} - \xi_{l_{j-1}}) > 0 \quad (\text{or } \leqq 0),$$

pick l_j with $|\eta_j - \xi_{l_j}| < v^{-1}$ and $\eta_j - \xi_{l_j} \leqq 0$ (or $\geqq 0$, respectively); then (11.18), (11.9) are valid also for $i = j$.

Note that (11.19) for $i = n$ gives $|\xi_{l_1} + \cdots + \xi_{l_n}| < v^{-1}$ and thus $\xi_{l_1} + \cdots + \xi_{l_n} = 0$.

Let us initially restrict ourselves to values of $A_1, \ldots, A_n$ with fixed $l_1, \ldots, l_n$, and put $c_i = \xi_{l_i}$. Then $|c_i| \leqq 1$ and (7.1) holds. Now

$$\begin{aligned} \Pi(A_1, \ldots, A_n) &= \Pi(Q^{\eta_1}, \ldots, Q^{\eta_n}) \subseteq Q^{1/v}\Pi(Q^{c_1}, \ldots, Q^{c_n}) \\ &= Q^{1/v}\Pi(Q), \end{aligned}$$

with $\Pi(Q)$ given by (7.2). Further (11.17), together with the definition of v, yields

$$\lambda_q(Q) < Q^{(1/v)-\delta} \leqq Q^{-\delta/2}. \tag{11.20}$$

By this, and since (11.12) and (11.15) are (11.1) and (11.4) with $\delta/2$ in place of δ, the number of possibilities for $S(Q)$ is

$$\leqq m(1 + 8\delta^{-1} \log E) \tag{11.21}$$

by the preceding lemma.

The vectors $\mathbf{g}_i = \mathbf{g}_i(A_1, \ldots, A_n)$ for $1 \leqq i \leqq q$ lie in $Q^{-\delta/2}\Pi(Q)$. On the other hand, since by Minkowski and by (7.6),

$$\lambda_1(Q) \cdots \lambda_n(Q) \geqq (n!B)^{-1} \geqq (n!)^{-1}H^{-nd} > Q^{-\delta},$$

we have $\lambda_n(Q) > Q^{-\delta/2}$. Therefore $S(Q)$ is spanned by the $\mathbf{g}_i(A_1, \ldots, A_n)$ for $i = 1, \ldots, q$, and $S(Q) = S(A_1, \ldots, A_n)$. The number of possibilities of $S(A_1, \ldots, A_n)$ is bounded by (11.21).

It remains for us to take account of the possible values of $l_1, \ldots, l_n$. This introduces a factor

$$\leqq (2v + 1)^n < ((4/\delta) + 3)^n < (6/\delta)^n.$$

12. The last two minima

LEMMA 12.1: *Suppose that* $0 < \delta < n$ *and*

$$m > 6 \cdot 10^4 n^6 \delta^{-2} \log 2nd. \tag{12.1}$$

Let E *be given by* (11.2), *and let* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n, H, A_1, \ldots, A_n, \Pi(A_1, \ldots, A_n)$, *etc., be as in the last section. Then for values of* $A_1, \ldots, A_n, Q$ *with*

$$Q^{\delta^2/8n^2} > (2^{4n}H)^{16d^2mE}, \tag{12.2}$$

$$Q \geqq \max(A_1, \ldots, A_n, A_1^{-1}, \ldots, A_n^{-1}), \tag{12.3}$$

and

$$\lambda_q(A_1, \ldots, A_n) < Q^{-\delta}\lambda_n(A_1, \ldots, A_n), \tag{12.4}$$

$S(A_1, \ldots, A_n)$ is among not more than

$$m(24n/\delta)^n(1 + 32n\delta^{-1} \log E) \tag{12.5}$$

subspaces.

Proof: From (7.6), the modulus B^{-1} of the determinant of $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ has

$$1 \leqq B \leqq H^{nd}.$$

Moreover, as in the proof of the Polynomial Theorem, we have $X_i = \eta_{i1}(\boldsymbol{\beta}_1\mathbf{X}) + \cdots + \eta_{in}(\boldsymbol{\beta}_n\mathbf{X})$ $(i = 1, \ldots, n)$ with $|\eta_{ij}| \leqq H^{nd}$, so that

$$|\mathbf{x}| \leqq nH^{nd} \max(|\boldsymbol{\beta}_1\mathbf{x}|, \ldots, |\boldsymbol{\beta}_n\mathbf{x}|).$$

Writing $\lambda_i = \lambda_i(A_1, \ldots, A_n)$ we have (6.2) and therefore

$$(n!H^{nd})^{-1} \leqq \lambda_1 \cdots \lambda_n \leqq 1. \tag{12.6}$$

The basis vectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$ have $|\boldsymbol{\beta}_i\mathbf{e}_j| \leqq 1 \leqq A_iQ$, so that $\lambda_n \leqq Q$. On the other hand, integer points $\mathbf{x} \neq \mathbf{0}$ have

$$\max(A_1^{-1}|\boldsymbol{\beta}_1\mathbf{x}|, \ldots, A_1^{-1}|\boldsymbol{\beta}_n\mathbf{x}|) \geqq Q^{-1} \max(|\boldsymbol{\beta}_1\mathbf{x}|, \ldots, |\boldsymbol{\beta}_n\mathbf{x}|)$$

$$\geqq (nH^{nd}Q)^{-1}|\mathbf{x}| \geqq (nH^{nd}Q)^{-1},$$

so that $\lambda_1 \geqq (nH^{nd}Q)^{-1}$.

Put

$$\varrho_0 = (\lambda_1 \cdots \lambda_{n-2}\lambda_{n-1}^2)^{1/n},$$

$$\varrho_1 = \varrho_0/\lambda_1, \ldots, \varrho_{n-1} = \varrho_0/\lambda_{n-1}, \text{ but } \varrho_n = \varrho_{n-1} = \varrho_0/\lambda_{n-1}.$$

The relations (6.5), (6.6), (6.7) of Lemma 6.1 are satisfied. Thus there is a permutation $t_1, \ldots, t_n$ of $1, \ldots, n$ such that the successive minima $\lambda_1', \ldots, \lambda_n'$ of the parallelepiped Π' given by

$$|\boldsymbol{\beta}_i\mathbf{x}| \leqq A_i\varrho_{t_i}^{-1} \ (= A_i', \text{ say}) \quad (i = 1, \ldots, n) \tag{12.7}$$

satisfy

$$2^{-n}\varrho_j\lambda_j \leqq \lambda_j' \leqq 4^{n^2}\varrho_j\lambda_j \quad (j = 1, \ldots, n).$$

Now

$$\varrho_0 = (\lambda_1 \cdots \lambda_n(\lambda_q/\lambda_n))^{1/n} \leqq (\lambda_q/\lambda_n)^{1/n} < Q^{-\delta/n},$$

by (12.4), so that

$$\lambda_q' \leqq 4^{n^2}\lambda_{n-1}\varrho_{n-1} = 4^{n^2}\varrho_0 < 4^{n^2}Q^{-\delta/n} < Q^{-\delta/2n} \tag{12.8}$$

since $Q^{\delta/2n} > 4^{n^2}$ by (12.2) and (11.6). We have

$$\varrho_1 = \lambda_1^{-1}\varrho_0 < \lambda_1^{-1}Q^{-\delta/n} \leqq nH^{nd}QQ^{-\delta/n} < Q,$$

$$\varrho_n = \lambda_{n-1}^{-1}\varrho_0 = (\lambda_1 \cdots \lambda_n)^{1/n}\lambda_n^{-1}(\lambda_n/\lambda_{n-1})^{1-(1/n)}$$

$$> (nH^d)^{-1}Q^{-1}Q^{\delta(1-(1/n))} > Q^{-1}$$

by (12.4), (12.2). Therefore

$$Q^{-1} < \varrho_n \leqq \varrho_{n-1} \leqq \cdots \leqq \varrho_1 < Q$$

and $Q^{-2} < A_i\varrho_{t_i}^{-1} = A_i' < Q^2$. In view of (12.1), (12.2), (12.8) we see that the conditions (11.12), (11.15), (11.16), (11.17) of Lemma 11.3 are satisfied with $A_1', \ldots, A_n', Q^2, \delta/4n$ in place of $A_1, \ldots, A_n, Q, \delta$. So if $S(A_1', \ldots, A_n')$ is the subspace belonging to the parallelepiped $\Pi' = \Pi'(A_1', \ldots, A_n')$ given by (12.7), we see that it has not more than (12.5) possibilities. (This is the bound of Lemma 11.3 with $\delta/4n$ in place of δ.)

By the last assertion of Lemma 6.1, for every integer point $\mathbf{g} \notin S(A_1, \ldots, A_n)$ we have

$$\max_i (|\boldsymbol{\beta}_i\mathbf{g}|\varrho_{t_i}A_i^{-1}) = \max_i (|\boldsymbol{\beta}_i\mathbf{g}|A_i'^{-1})$$

$$\geqq 2^{-n}\varrho_n\lambda_n > 4^{-2n^2}\lambda_n' \geqq 4^{-2n^2}(\lambda_1' \cdots \lambda_n')^{1/n}$$

$$\geqq 4^{-2n^2}(nH^d)^{-1} > Q^{-\delta/2n}$$

by (12.2), while on the other hand $\lambda_{n-1}' < Q^{-\delta/2n}$ by (12.8). Therefore such $\mathbf{g}$ cannot lie in $S(A_1', \ldots, A_n')$. Thus $S(A_1, \ldots, A_n) = S(A_1', \ldots, A_n')$, and the number of possibilities for $S(A_1, \ldots, A_n)$ again is restricted by (12.5).

13. Two adjacent minima

LEMMA 13.1: *Let* $\boldsymbol{\beta}_1, \ldots \boldsymbol{\beta}_n$, H, $A_1, \ldots, A_n$, $\Pi = \Pi(A_1, \ldots, A_n)$, $\lambda_i = \lambda_i(A_1, \ldots, A_n)$ *and* $\mathbf{g}_i = \mathbf{g}_i(A_1, \ldots, A_n)$ *be as before. Let* $1 \leqq s < n$, *and* $S_s = S_s(A_1, \ldots, A_n)$ *the subspace spanned by* $\mathbf{g}_1, \ldots, \mathbf{g}_s$. *Put*

$$l = \binom{n}{s},$$

suppose that $0 < \delta < l$,

$$m > 24 \cdot 10^4 n^2 l^6 \delta^{-2} \log 2ld, \tag{13.1}$$

and put

$$E = \tfrac{1}{12} 2^m (180)^{2^{m-1}}. \tag{13.2}$$

Then for values of $A_1, \ldots, A_n$, Q *with*

$$Q^{\delta^2} > (2^{4l} H)^{2^9 d^2 m n^2 l^2 E}, \tag{13.3}$$

$$Q \geqq \max(A_1, \ldots, A_n, A_1^{-1}, \ldots, A_n^{-1}) \tag{13.4}$$

and

$$\lambda_s < Q^{-\delta} \lambda_{s+1}, \tag{13.5}$$

$S_s(A_1, \ldots, A_n)$ *is among not more than*

$$m(48ln/\delta)^l (1 + 64ln\delta^{-1} \log E) \tag{13.6}$$

s-dimensional subspaces.

Proof: Put $p = n - s$, recall from section 6 that $C(n, p)$ is the set of p-tuples $\sigma = \{i_1 < \cdots < i_p\}$ of integers in $1 \leqq i \leqq n$, and define $\boldsymbol{\beta}_\sigma$ by (6.12). Also write

$$A_\sigma = \prod_{i \in \sigma} A_i.$$

We will apply Lemma 6.3 with $\boldsymbol{\beta}_i A_i^{-1}$ in place of $\boldsymbol{\beta}_i$. The parallelepiped $\Pi^{(p)}$ given by

$$|\boldsymbol{\beta}_\sigma \mathbf{X}^{(p)}| \leqq A_\sigma \quad (\sigma \in C(n, p))$$

is the pth pseudocompound of Π. Denote its successive minima by $v_1, \ldots, v_l$. It is clear that in Lemma 6.3 we may take

$$\tau_l = \{n - p + 1, n - p + 2, \ldots, n\} = \{s + 1, s + 2, \ldots, n\},$$

$$\tau_{l-1} = \{n - p, n - p + 2, \ldots, n\} = \{s, s + 2, \ldots, n\}.$$

Thus Lemma 6.3 in conjunction with (13.5) and (13.3) gives

$$v_{l-1} < p!^l l! Q^{-\delta} v_l < Q^{-3\delta/4} v_l. \tag{13.7}$$

We have

$$H^{-pd} \leqq |\boldsymbol{\beta}_\sigma| \leqq 1$$

by (5.2). We introduce the normalized vectors $\boldsymbol{\gamma}_\sigma = |\boldsymbol{\beta}_\sigma|^{-1} \boldsymbol{\beta}_\sigma$ and the parallelepiped $N^{(p)}$ defined by

$$|\boldsymbol{\gamma}_\sigma \mathbf{X}^{(p)}| \leqq A_\sigma \quad (\sigma \in C(n, p)),$$

whose successive minima we denote by $v_1', \ldots, v_l'$. Now $H^{-pd}\Pi^{(p)} \subset N^{(p)} \subset \Pi^{(p)}$, and therefore

$$v_i \leqq v_i' \leqq H^{pd} v_i \quad (i = 1, \ldots, l).$$

Together with (13.7) and (13.3) this yields

$$v_{l-1}' < H^{pd} Q^{-3\delta/4} v_l' < Q^{-\delta/2} v_l'. \tag{13.8}$$

Note that $H(\boldsymbol{\beta}_\sigma) \leqq H^p$ by Lemma 5.1, and thus also $H(\boldsymbol{\gamma}_\sigma) = H(\boldsymbol{\beta}_\sigma) \leqq H^p$. We have

$$Q^{-p} \leqq A_\sigma \leqq Q^p \quad (\sigma \in C(n, p)). \tag{13.9}$$

We now apply Lemma 12.1 with n, δ, $\boldsymbol{\beta}_i$, H, Q replaced respectively by l, $\delta/2p$, $\boldsymbol{\gamma}_\sigma$, H^p, Q^p. The conditions (12.1), (12.2), (12.3), (12.4) are replaced

respectively by (13.1), (13.3), (13.9), (13.8). The conclusion is that the subspace $S^{(p)}$ of $\mathbb{R}^l$ spanned by the first $l-1$ minimal points of $N^{(p)}$ is among a set of not more than (13.6) subspaces of $\mathbb{R}^l$.

Let again $\mathbf{g}_1, \ldots, \mathbf{g}_n$ be independent points with $\mathbf{g}_i \in \lambda_i \Pi$ $(i = 1, \ldots, n)$. By (6.13), the points $\mathbf{G}_{\tau_1}, \ldots, \mathbf{G}_{\tau_{l-1}}$ lie in

$$p!\lambda_{\tau_{l-1}} \Pi^{(p)} \subset p!\lambda_{\tau_{l-1}} H^{pd} N^{(p)}.$$

But

$$\begin{aligned} p!\lambda_{\tau_{l-1}} H^{pd} &< p!H^{pd} Q^{-\delta} \lambda_{\tau_l} \leqslant (p!)^l l! \cdot H^{pd} Q^{-\delta} v_l \\ &< v_l \leqq v_l' \end{aligned}$$

by (13.5), (6.14) and (13.3). Thus $\mathbf{G}_{\tau_1}, \ldots, \mathbf{G}_{\tau_{l-1}}$ span $S^{(p)}$. Therefore there are not more than (13.6) possibilities for the span of $\mathbf{G}_{\tau_1}, \ldots, \mathbf{G}_{\tau_{l-1}}$ in $\mathbb{R}^l$. By Lemma 6.4, there are not more than (13.6) possibilities for the span of $\mathbf{g}_1, \ldots, \mathbf{g}_s$ in $\mathbb{R}^n$, i.e., for S_s.

14. Proof of Proposition B, and hence the Theorem

We will adopt the notation of section 4. We will introduce a new parameter $\mu > 0$: Initially we will study solutions of (4.6) with

$$|\boldsymbol{\beta}_i \mathbf{x}| > H^{-\mu} |\mathbf{x}|^{1-\mu} \quad (i = 1, \ldots, n). \tag{14.1}$$

Writing $A_i = A_i(\mathbf{x}) = |\boldsymbol{\beta}_i \mathbf{x}| / (|\boldsymbol{\beta}_1 \mathbf{x}| \cdots |\boldsymbol{\beta}_n \mathbf{x}|)^{1/n}$ we have $A_1 A_2 \cdots A_n = 1$. In view of $|\boldsymbol{\beta}_i \mathbf{x}| \leqq |\mathbf{x}|$ we have

$$(H|\mathbf{x}|)^{-\mu} \leqq A_i \leqq (H|\mathbf{x}|)^{\mu} \quad (i = 1, \ldots, n).$$

Thus with $Q = (H|\mathbf{x}|)^{\mu}$ we have $Q^{-1} \leqq A_i \leqq Q$. Furthermore, when $|\mathbf{x}| > H$ we have $Q = (H|\mathbf{x}|)^{\mu} < |\mathbf{x}|^{2\mu}$, and (4.6) yields $|\boldsymbol{\beta}_1 \mathbf{x}| \cdots |\boldsymbol{\beta}_n \mathbf{x}| < Q^{-\delta/2\mu}$ and

$$|\boldsymbol{\beta}_i \mathbf{x}| = A_i (|\boldsymbol{\beta}_1 \mathbf{x}| \cdots |\boldsymbol{\beta}_n \mathbf{x}|)^{1/n} < A_i Q^{-\delta/2n\mu}. \tag{14.2}$$

Thus if $\Pi = \Pi(A_1, \ldots, A_n)$ is the parallelepiped (11.14), then $\mathbf{x}$ lies in $Q^{-\delta/2n\mu} \Pi$, and $\lambda_1 < Q^{-\delta/2n\mu}$. On the other hand we have $\lambda_n > (nH^d)^{-1}$ from (6.2) and (7.6), and if we suppose that

$$|\mathbf{x}|^{\delta} > (nH^d)^{6n} \tag{14.3}$$

then

$$\lambda_n > |\mathbf{x}|^{-\delta/6n} \geqq Q^{-\delta/6n\mu}. \tag{14.4}$$

Thus $\mathbf{x}$ lies in the subspace $S = S(A_1, \ldots, A_n)$ spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_q$, where again $\mathbf{g}_i = \mathbf{g}_i(A_1, \ldots, A_n)$. Let k be minimal such that $\mathbf{x}$ lies in the k-dimensional subspace S_k spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_k$; then $1 \leqq k \leqq q$. By (14.2), $\lambda_k < Q^{-\delta/2n\mu}$. There is by (14.4) an s in $k \leqq s \leqq q$ with

$$\lambda_s < Q^{-\delta/3n^2\mu}\lambda_{s+1}. \tag{14.5}$$

The idea now is to use Lemma 13.1 with $\delta/3n^2\mu$ in place of δ. Since $l = \binom{n}{s} \leqq 2^{n-1}$ and

$$\log(2ld) \leqq \log(2^n d) \leqq \log(2^n d^n) = n \log 2d,$$

the condition (13.1) will certainly be true if

$$m > 4 \cdot 10^4 \mu^2 \delta^{-2} n^7 2^{6n} \log 3d. \tag{14.6}$$

With E given by (13.2), the condition (13.3) (with $\delta/3n^2\mu$ in place of δ) will hold if

$$Q^{\delta^2} > (2^{4l}H)^{2^{13}d^2mn^6l^2\mu^2E}.$$

Since $Q \geqq |\mathbf{x}|^{\mu}$, this will certainly be true when

$$|\mathbf{x}|^{\delta^2} > (2^{2^{n+1}}H)^{2^{11}D^2mn^6 2^{2n}\mu E}. \tag{14.7}$$

When $0 < \delta < 3n^2\mu$ (so that $\delta/3n^2\mu < 1$), we may apply Lemma 13.1 to conclude that $S_s(A_1, \ldots, A_n)$ is among not more than

$$m(144ln^3\mu/\delta)^l(1 + 192ln^3(\mu/\delta) \log E) \tag{14.8}$$

subspaces, so that $\mathbf{x}$ itself lies in a collection of not more than this many subspaces. Summing over s in $1 \leqq s < n$, we see that $\mathbf{x}$ with (4.6), (14.1), (14.7), lies in a collection of not more than

$$t_2 = nm(400 \cdot 2^{2n}\mu/\delta)^{2n} \log E \tag{14.9}$$

subspaces.

Points $\mathbf{x}$ with $\boldsymbol{\beta}_i\mathbf{x} = 0$ for some $\boldsymbol{\beta}_i$ lie in n subspaces. For other integer points $\mathbf{x}$, (14.1) holds with $\mu = d$ by Lemma 5.3. However, if we substitute $\mu = d$ into (14.6), then m, and as a consequence E, will grow rather rapidly with d. In order to obtain a better dependency on d, we now proceed as follows.

Integer points lying in a coordnate plane $x_i = 0$ or satisfying $\boldsymbol{\beta}_i\mathbf{x} = 0$ for some i are contained in $2n$ subspaces. We will disregard such points for the time being. Let $\boldsymbol{\beta}$ be one of the vectors $\boldsymbol{\beta}_i$; then $|\boldsymbol{\beta}\mathbf{x}| \geqq |\mathbf{x}|^{1-d}H^{-d}$ by Lemma 5.3. Suppose now that

$$10n < \mu \leqq d \tag{14.10}$$

and consider points $\mathbf{x}$ with

$$|\mathbf{x}|^{1-\mu}H^{-\mu} \leqq |\boldsymbol{\beta}\mathbf{x}| < |\mathbf{x}|^{1-(\mu/e)}H^{-\mu/e}. \tag{14.11}$$

Suppose that, say, $\boldsymbol{\beta}, \mathbf{e}_2, \ldots, \mathbf{e}_n$ are linearly independent, where $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are the coordinate basis vectors. We have

$$|\boldsymbol{\beta}\mathbf{x}||\mathbf{e}_2\mathbf{x}| \cdots |\mathbf{e}_n\mathbf{x}| < |\mathbf{x}|^{n-\mu/e} = |\mathbf{x}|^{-\delta}$$

with $\delta = (\mu/e) - n$. Since $\delta < 3n^2\mu$, we may apply what we said above to $\boldsymbol{\beta}, \mathbf{e}_2, \ldots, \mathbf{e}_n$, and we see that points $\mathbf{x}$ with (14.7), (14.11) lie in a collection of not more than t_2 subspaces. But $\delta/\mu = (1/e) - (n/\mu) > 1/4$, so that $\mu/\delta < 4$, and we obtain less than

$$t_3 = nm(1600 \cdot 2^{2n})^{2^n} \log E$$

subspaces. With our present values of μ, δ, the relations (14.6), (14.7) will hold if

$$m > 64 \cdot 10^4 n^7 2^{6n} \log 3d, \tag{14.12}$$

$$|\mathbf{x}| > (2^{2^{n+1}}H)^{2^{13}d^2mn^6 2^{2n}E}. \tag{14.13}$$

Now if $10n < d$ and we carry this out with $\mu = \mu_1, \ldots, \mu_w$ where $\mu_i = de^{1-i}$ and $w = [\log (d/10n)]$, we see that points $\mathbf{x}$ with

$$|\boldsymbol{\beta}\mathbf{x}| < |\mathbf{x}|^{1-(\mu_w/e)}H^{-\mu_w/e}$$

and (14.13) lie in not more than wt_3 subspaces.

We now return to (4.6). We treat each $\boldsymbol{\beta}_i$ in the way just described and see that if we exclude not more than nwt_3 subspaces, then (14.1) holds with $\mu = \mu_w/e \leqq de(10n/d) = 10en$, hence holds with $\mu = 10en$. This was when $10n < d$; but when $d \leqq 10n$, then (14.1) holds with $\mu = 10en$ anyhow. We now may apply what we said at the beginning with $\mu = 10en$, and we obtain

$$t_2 < nm(11000n2^{2n}/\delta)^{2^n} \log E$$

subspaces. With our present value of μ, the conditions (14.6), (14.7) will hold if

$$m > 35 \cdot 10^6 n^9 2^{6n} \delta^{-2} \log 3d, \tag{14.14}$$

$$|\mathbf{x}| > (2^{2^{n+1}} H)^{2^{16} d^2 mn^7 2^{2n} \delta^{-2} E}. \tag{14.15}$$

Recalling the $2n$ subspaces excluded at the beginning, we have not more than

$$\begin{aligned} &2n + nwt_3 + t_2 \\ &\quad < 2n + n^2 wm(1600 \cdot 2^{2n})^{2^n} \log E + nm(11{,}000n2^{2n}/\delta)^{2^n} \log E \\ &\quad < n^2 m(\log 2d)(2^{14} n 2^{2n}/\delta)^{2^n} \log E \end{aligned} \tag{14.16}$$

subspaces. We now choose m minimal with (14.14). Then also (14.12) holds since $0 < \delta < 1$. We have

$$2^m < (2d)^{2^{26} n^9 2^{6n} \delta^{-2}},$$

$$\log E < 10 \cdot (2d)^{2^{26} n^9 2^{6n} \delta^{-2}},$$

and in view of (14.16), the number of subspaces will be

$$< (2d)^{2^{27} n^9 2^{6n} \delta^{-2}} \leqq [(2d)^{2^{24n} \delta^{-2}}] = t_1.$$

Since $2^{17} d^2 mn^7 2^{3n} \delta^{-2} E < e^{t_1}$, the condition (14.15) (and also the weaker condition (14.13)) will hold true if $|\mathbf{x}| > (2H)^{e^{t_1}}$.

Proposition B, and hence the Theorem, follow.

References

1. E. Bombieri and J. Vaaler, On Siegel's lemma. *Invent. Math.* 73 (1983) 11–32.
2. E. Bombieri and A.J. Van der Poorten, Some quantitative results related to Roth's Theorem. *MacQuarie Math. Reports*, Report No. 87-0005, February 1987.
3. J.W.S. Cassels, *An Introduction to the Geometry of Numbers.* Springer Grundlehren 99 (1959).
4. H. Davenport, Note on a result of Siegel. *Acta Arith.* 2 (1937) 262–265.
5. H. Davenport and K.F. Roth, Rational approximation to algebraic numbers. *Mathematika* 2 (1955) 160–167.
6. H. Esnault and E. Viehweg, Dyson's Lemma for polynomials in several variables (and the theorem of Roth). *Invent. Math.* 78 (1984) 445–490.
7. J.H. Evertse, Upper bounds for the number of solutions of Diophantine equations. *Math. Centrum*, Amsterdam (1983) 1–127.
8. K. Mahler, Ein Übertragungsprinzip für konvexe Körper. Časopis Pěst. Mat. Fys. (1939) 93–102.
9. K. Mahler, On compound convex bodies I. *Proc. Lon. Math. Soc.* (3) 5, 358–379.
10. W.M. Schmidt, On heights of algebraic subspaces and diophantine approximations. *Annals of Math.* 83 (1967) 430–472.
11. W.M. Schmidt, Norm form equations. *Annals of Math.* 96 (1972) 526–551.
12. W.M. Schmidt, The number of solutions of norm form equations. *Transactions A.M.S.* (to appear).
13. W.M. Schmidt, Diophantine approximation. *Springer Lecture Notes in Math.* 785, Berlin, Heidelberg, New York (1980).