Compositio Mathematica

Hans Peter Schlickewei

The quantitative subspace theorem for number fields

Compositio Mathematica, tome 82, nº 3 (1992), p. 245-273

<http://www.numdam.org/item?id=CM_1992__82_3_245_0>

© Foundation Compositio Mathematica, 1992, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http://http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Compositio Mathematica **82**: 245–273, 1992.
© 1992 *Kluwer Academic Publishers. Printed in the Netherlands.*

The quantitative Subspace Theorem for number fields

HANS PETER SCHLICKEWEI
Abt. für Mathematik, Universität Ulm, Oberer Eselsberg, D-7900 Ulm, Germany

Received 22 February 1990; accepted 19 September 1991

1. Introduction

Roth's theorem [7] says that given an algebraic number α of degree $d \geqslant 2$ and given $\delta > 0$ there are only a finite number of rational approximations $\frac{x}{y}$ of α satisfying

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

It is well known that here the method of proof is ineffective, i.e. the proof does not give bounds for $|x|$ and $|y|$. However it does provide bounds for the *number* of solutions x, y of (1.1) (cf. the papers of Davenport and Roth [4], Bombieri and van der Poorten [1] and Luckhardt [5]).

The analogue of (1.1) for n dimensions is Schmidt's Subspace Theorem [13], [14].

Suppose that $L_1, \ldots, L_n$ are linearly independent linear forms with algebraic coefficients in n variables. Let $\delta > 0$. Then the subspace theorem says that there are a finite number of proper subspaces of $\mathbb{Q}^n$ containing all rational integral solutions $\mathbf{x} = (x_1, \ldots, x_n) \neq 0$ of the inequality

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

where $|\mathbf{x}| = (x_1^2 + \cdots + x_n^2)^{1/2}$.

This result was extended by Schlickewei [8] to include p-adic valuations.

In a recent paper W.M. Schmidt proved a quantitative version of his Subspace Theorem [16] in which he derived an explicit upper bound for the number of subspaces containing all solutions of an inequality as (1.2). This in turn was generalized by Schlickewei [10] to the case of archimedean as well as nonarchimedean absolute values.

Let $S = \{\infty, p_2, \ldots, p_s\}$, where $p_2, \ldots, p_s$ are rational primes. For $v \in S$ denote by $|\ |_v$ the v-adic absolute value on $\mathbb{Q}$ (i.e. $|\ |_\infty$ is the standard absolute value, whereas $|\ |_{p_j}$ is the p_j-adic absolute value with $|p_j|_{p_j} = p_j^{-1}$). Let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ with respect to $|\ |_v$ and let Ω_v be the algebraic closure of $\mathbb{Q}_v$. Each absolute value $|\ |_v$ has a unique extension to Ω_v, again denoted by $|\ |_v$. Let K be an algebraic number field. Each extension of $|\ |_v$ to K is given by an embedding φ_v of K over $\mathbb{Q}$ into Ω_v. The result of [10] reads as follows.

Let $[K:\mathbb{Q}] = d$. Suppose that for each $v \in S$ we are given n linearly independent linear forms $L_1^{(v)}, \ldots, L_n^{(v)}$ in n variables with coefficients in K. Consider the inequality

$$\prod_{v\in S} |L_1^{(v)}(\mathbf{x}) \cdots L_n^{(v)}(\mathbf{x})|_v < \left(\prod_{v\in S} |\det(L_1^{(v)}, \ldots, L_n^{(v)})|_v\right) |\mathbf{x}|^{-\delta} \tag{1.3}$$

where $0 < \delta < 1$ and where $\det(L_1^{(v)}, \ldots, L_n^{(v)})$ denotes the determinant of the coefficient matrix of $L_1^{(v)}, \ldots, L_n^{(v)}$.

Then there are proper subspaces $T_1, \ldots, T_r$ of $\mathbb{Q}^n$ with

$$r = [(8sd!)^{2^{26n}s^6\delta^{-2}}] \tag{1.4}$$

such that every rational integral solution $\mathbf{x}$ of (1.3) either lies in one of these subspaces, or has norm

$$|\mathbf{x}| < \max\{(n!)^{8/\delta}, H(L_i^{(v)})(v \in S, i = 1, \ldots, n)\} \tag{1.5}$$

where the $H(L_i^{(v)})$ are heights which will be defined below.

Schmidt in [16] pioneered the case $S = \{\infty\}$ of this result. Actually Schmidt obtains a better bound in (1.4) with $d!$ replaced by d. But, as was shown in a remark in [10], the term $d!$ in (1.4) may be replaced by d if we suppose that $K/\mathbf{Q}$ is a normal extension.

The quantitative version of his Subspace Theorem was used by Schmidt [17] to deduce upper bounds for the number of solutions of norm form equations. The most interesting feature in these bounds consists in the fact that the bounds derived there depend only upon the number of variables and upon the degree but do not depend upon the particular coefficients of the equation under consideration. Similar remarks apply to the results about S-unit equations [11], [12] derived by Schlickewei from the p-adic quantitative Subspace Theorem. However, for many applications we require the variables not to be restricted to $\mathbb{Z}^n$, but to be integers in a number field. For such applications we need the quantitative version of the Subspace Theorem with the variables being algebraic integers.

In a qualitative sense the Subspace Theorem for number fields was proved by Schmidt [15] for archimedean valuations and later on by Schlickewei [9] in the more general setting where also nonarchimedean valuations come in.

It is the goal of this paper to derive a result of this type which is quantitative in the sense of (1.4), (1.5). Let K be a number field of degree d. Let $M(K)$ be the set of places of K. For $v \in M(K)$ denote by $|\ |_v$ be corresponding absolute value normalized such that for $a \in \mathbb{Q}$, $|a|_v = |a|_\infty$ if v lies above the archimedean prime of $\mathbb{Q}$ and $|p|_v = p^{-1}$ if v lies above the rational prime p. Let K_v be the completion of K with respect to $|\ |_v$ and put $d_v = [K_v : \mathbb{Q}_v]$ for the local degree. For $\alpha \in K$ write

$$\|\alpha\|_v = |\alpha|_v^{d_v/d}. \tag{1.6}$$

Given a vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K^n$ and $v \in M(K)$ we put

$$|\boldsymbol{\alpha}|_v = \begin{cases} (|\alpha_1|_v^2 + \cdots + |\alpha_n|_v^2)^{1/2} & \text{if } v \text{ is archimedean} \\ \max_{1 \leqslant i \leqslant n} |\alpha_i|_v & \text{if } v \text{ is nonarchimedean} \end{cases} \tag{1.7}$$

and $\|\boldsymbol{\alpha}\|_v = |\boldsymbol{\alpha}|_v^{d_v/d}$. We define the height of $\boldsymbol{\alpha}$ by

$$H(\boldsymbol{\alpha}) = \prod_{v \in M(K)} \|\boldsymbol{\alpha}\|_v. \tag{1.8}$$

Given a linear form $L(\mathbf{x}) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ with coefficients $\alpha_i \in K$ and $v \in M(K)$ write $\|L\|_v = \|\boldsymbol{\alpha}\|_v$, and $H(L) = H(\boldsymbol{\alpha})$ for the height of L.

THEOREM. *Let K be a normal extension of $\mathbb{Q}$ of degree d. Let S be a finite subset of $M(K)$ of cardinality s. Suppose that for each $v \in S$ we are given n linearly independent linear forms $L_1^{(v)}, \ldots, L_n^{(v)}$ in n variables with coefficients in K. Let* $0 < \delta < 1$. *Consider the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} \frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} < H(\boldsymbol{\beta})^{-n-\delta}. \tag{1.9}$$

There exists proper subspaces $S_1, \ldots, S_t$ of K^n with

$$t = [(8sd)^{2^{34nd} s^6 \delta^{-2}}] \tag{1.10}$$

such that every solution $\boldsymbol{\beta} \in K^n$ either lies in $\bigcup_{i=1}^t S_i$ or satisfies

$$H(\boldsymbol{\beta}) < \max\{(n!)^{9/\delta}, H(L_i^{(v)})^{9dns/\delta}\ (v \in S,\ i = 1, \ldots, n)\}. \tag{1.11}$$

Notice that the hypothesis in (1.3) differs somewhat from the hypothesis in (1.9). This is the reason for the slight change in (1.11) as compared to (1.5). For the applications however this is no serious disadvantage. What is significant in our Theorem is that the assertion does not involve the field discriminant of K. Such a dependence would cause serious problems in the applications and would destroy uniformity results we are able to derive from the present version.

We shall prove our Theorem by using an integral basis for K over $\mathbb{Q}$ and replacing the solution vectors $\boldsymbol{\beta} \in K^n$ in (1.9) by a vector $\mathbf{x} \in \mathbb{Q}^{nd}$ and then applying the quantitative Subspace Theorem for $\mathbb{Q}$ [10] as quoted above. In fact this method was already useful in proving the qualitative results in Schmidt [15] or in Schlickewei [9] by means of the previous results with rational solutions as in [13], or [8], respectively. However for our quantitative version we have to be much more careful as a straightforward application of this method would yield results implying the discriminant as well as the regulator of K and we definitely want to avoid such a dependence.

2. Intermediate fields

Given a vector $\boldsymbol{\beta} \in K^n$ and a field F with $K \supset F \supset \mathbb{Q}$, we say that $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ *defines* F if F is generated over $\mathbb{Q}$ by the quotients β_i/β_j $(1 \leqslant i, j \leqslant n)$ with $\beta_j \neq 0$.

If a solution $\boldsymbol{\beta} \in K^n$ of (1.9) defines an intermediate field F, then by homogeneity we may in fact suppose that $\beta_1, \ldots, \beta_n \in F$.

PROPOSITION 2.1. *Let K be a normal extension of $\mathbb{Q}$ of degree d. Let F with $K \supset F \supset \mathbb{Q}$ be an intermediate field of degree f over $\mathbb{Q}$. Suppose that R is a finite subset of $M(F)$ of cardinality r. For each $v \in R$ let $L_1^{(v)}, \ldots, L_n^{(v)}$ be linearly independent linear forms in n variables with coefficients in K. Assume that for each $v \in R$, we have an extension of $|\ |_v$ to K, again denoted by $|\ |_v$. Let $0 < \delta < 1$. Consider the solutions $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in F^n$ of the inequality*

$$\prod_{v \in R} \prod_{i=1}^{n} \frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} < H(\boldsymbol{\beta})^{-n-\delta} \tag{2.1}$$

with the additional property

$$\boldsymbol{\beta} \text{ defines } F \text{ over } \mathbb{Q}. \tag{2.2}$$

Then the following assertion holds true. There exists proper linear subspaces $T_1, \ldots, T_{t_1}$ of F^n with

$$t_1 = [(8rd)^{2^{33nd} r^6 \delta^{-2}}] \tag{2.3}$$

such that every $\boldsymbol{\beta} \in F^n$ with (2.1) and (2.2) either lies in the union of these subspaces or satisfies

$$H(\boldsymbol{\beta}) < \max\{(n!)^{9/\delta}, H(L_i^{(v)})^{9nrd/\delta}\ (i = 1, \ldots, n;\ r \in R)\}. \tag{2.4}$$

We proceed to show that Proposition 2.1 implies the Theorem. In fact, it is clear that there are not more than

$$2^d \tag{2.5}$$

intermediate fields $K \supset F \supset \mathbb{Q}$. We divide the set of solutions $\boldsymbol{\beta}$ of (1.9) into classes $\mathfrak{C}$ as follows. Two solutions $\boldsymbol{\beta}$ and $\boldsymbol{\beta}'$ belong to the same class $\mathfrak{C}$ if they define the same intermediate field F over $\mathbb{Q}$. As we said above, here we may assume moreover that $\boldsymbol{\beta} \in F^n$ and $\boldsymbol{\beta}' \in F^n$.

We will show that the solutions of (1.9) in a fixed class $\mathfrak{C} = \mathfrak{C}(F)$ that do not satisfy (1.11) lie in the union of not more than

$$t_2 = d^s \cdot [(8sd)^{2^{33nd}s^6\delta^{-2}}] \tag{2.6}$$

proper subspaces of F^n (and hence also of K^n). In view of (2.5), (2.6), (1.10) and since $2^d t_2 \leqslant [(8sd)^{2^{34nd}s^6\delta^{-2}}] = t$, this will imply the theorem.

Given an absolute value $v' \in M(F)$ and an absolute value $v \in M(K)$ the symbol $v \mid v'$ means that v extends v' to K. We have the relation

$$\sum_{\substack{v \in M(K) \\ v \mid v'}} d_v = [K:F] f_{v'},$$

where d_v is the local degree $[K_v : \mathbb{Q}_v]$ and $f_{v'}$ is the local degree $[F_{v'} : \mathbb{Q}_{v'}]$.

Let $R \subset M(F)$ be the set of absolute values $v' \in M(F)$ for which there exists $v \in S$ with $v \mid v'$. Then we get for each $v' \in R$

$$\sum_{\substack{v \in S \\ v \mid v'}} d_v \leqslant [K:F] f_{v'} \tag{2.7}$$

Since $d = [K:\mathbb{Q}] = [K:F][F:\mathbb{Q}]$ and $[F:\mathbb{Q}] = f$, (2.7) implies

$$\sum_{\substack{v \in S \\ v \mid v'}} \frac{d_v}{d} \leqslant \frac{f_{v'}}{f} \tag{2.8}$$

Let us study the term

$$\prod_{\substack{v \in S \\ v \mid v'}} \prod_{i=1}^{n} \frac{\| L_i^{(v)}(\boldsymbol{\beta}) \|_v}{\| L_i^{(v)} \|_v \| \boldsymbol{\beta} \|_v} = \prod_{\substack{v \in S \\ v \mid v'}} \prod_{i=1}^{n} \left(\frac{| L_i^{(v)}(\boldsymbol{\beta}) |_v}{| L_i^{(v)} |_v | \boldsymbol{\beta} |_v} \right)^{d_v/d}$$

in (1.9). Given a solution $\boldsymbol{\beta} \in F^n$ of (1.9) and $v' \in R$ define $w' = w'(v') \in S$ by

$$\prod_{i=1}^{n} \frac{| L_i^{(w')}(\boldsymbol{\beta}) |_{w'}}{| L_i^{(w')} |_{w'} | \boldsymbol{\beta} |_{w'}} = \min_{\substack{v \in S \\ v \mid v'}} \prod_{i=1}^{n} \frac{| L_i^{(v)}(\boldsymbol{\beta}) |_v}{| L_i^{(v)} |_v | \boldsymbol{\beta} |_v}. \tag{2.9}$$

Choose the extension of v' to K such that $|\;|_{v'}$ and $|\;|_{w'}$ coincide on K. Then combination of (2.8), (2.9) yields (using for $v' \in R$ the notation $\|\;\|_{v'} = |\;|_{v'}^{f_{v'}/f}$)

$$\prod_{i=1}^{n} \frac{\|L_i^{(w')}(\boldsymbol{\beta})\|_{v'}}{\|L_i^{(w')}\|_{v'}\|\boldsymbol{\beta}\|_{v'}} = \prod_{i=1}^{n}\left(\frac{|L_i^{(w')}(\boldsymbol{\beta})|_{w'}}{|L_i^{(w')}|_{w'}|\boldsymbol{\beta}|_{v'}}\right)^{f_{v'}/f} \leqslant \prod_{i=1}^{n}\left(\frac{|L_i^{(w')}(\boldsymbol{\beta})|_{v'}}{|L_i^{(w')}|_{v'}|\boldsymbol{\beta}|_{v'}}\right)^{\Sigma_{v\in S, v|v'} d_v/d}$$

$$\leqslant \prod_{\substack{v\in S\\ v|v'}}\left(\prod_{i=1}^{n}\frac{|L_i^{(v)}(\boldsymbol{\beta})|_v}{|L_i^{(v)}|_v|\boldsymbol{\beta}|_v}\right)^{d_v/d} = \prod_{\substack{v\in S\\ v|v'}}\prod_{i=1}^{n}\frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v\|\boldsymbol{\beta}\|_v}.$$

Therefore, each solution $\boldsymbol{\beta} \in F^n$ also satisfies an inequality

$$\prod_{v'\in R}\prod_{i=1}^{n}\frac{\|L_i^{(w')}(\boldsymbol{\beta})\|_{v'}}{\|L_i^{(w')}\|_{v'}\|\boldsymbol{\beta}\|_{v'}} < H(\boldsymbol{\beta})^{-n-\delta} \tag{2.10}$$

Divide the solutions $\boldsymbol{\beta}$ of a class $\mathfrak{C}$ into subclasses $\mathscr{D}$, such that $\boldsymbol{\beta}$ and $\boldsymbol{\beta}'$ belong to the same subclass $\mathscr{D}$ if they satisfy (2.9) for the same tuple $(w'(v'))_{v'\in R}$. Since for any $v' \in R$ there are at most $d/f \leqslant d$ possible choices for $w'(v')$ and since the cardinality of R is bounded above by the cardinality of S, each class $\mathfrak{C}$ splits into not more than

$$d^s \tag{2.11}$$

subclasses $\mathscr{D}$.

Solutions $\boldsymbol{\beta}$ of (1.9) in the same subclass satisfy (2.2) and (2.10). So we may apply Proposition 2.1. However if a solution does not satisfy (1.11), then it does not satisfy (2.4) either. Thus by (2.3) and since $r \leqslant s$ such solutions are contained in the union of not more than

$$t_1 \leqslant (8sd)^{2^{33nd}s^6\delta^{-2}}$$

proper subspaces of K^n. Allowing the factor d^s from (2.11) for the number of subclasses of the class $\mathfrak{C}$ we see in fact, that the solutions $\boldsymbol{\beta} \in \mathfrak{C}$ that do not satisfy (1.11) are contained in the union of not more than

$$d^s \cdot [(8sd)^{2^{33nd}s^6\delta^{-2}}] = t_2$$

proper subspaces of K^n as claimed in (2.6).

The remainder of the paper deals with the proof of Proposition 2.1.

3. Heights

LEMMA 3.1. *Let F be an algebraic number field of degree f. Let $\boldsymbol{\beta} \in F^n$, $\boldsymbol{\beta} \neq \mathbf{0}$.*

Denote by $D_{F/\mathbb{Q}}$ *the absolute value of the discriminant of* F. *Write* $M(F) = M_\infty(F) \cup M_0(F)$, *where* $M_\infty(F)$ *and* $M_0(F)$ *are the set of archimedean and nonarchimedean absolute values in* $M(F)$ *respectively. There exists an integral vector* $\boldsymbol{\beta}' = \lambda\boldsymbol{\beta}$ *with* $\lambda \in F$, $\lambda \neq 0$ *having*

$$H(\boldsymbol{\beta}') \geqslant D_{F/\mathbb{Q}}^{-1/2f} \prod_{v \in M_\infty(F)} \|\boldsymbol{\beta}'\|_v. \tag{3.1}$$

Proof. Recall the definition

$$H(\boldsymbol{\beta}) = \prod_{v \in M(F)} \|\boldsymbol{\beta}\|_v. \tag{3.2}$$

It is well known that

$$\prod_{v \in M_0(F)} \|\boldsymbol{\beta}\|_v = \mathfrak{N}(\mathfrak{B})^{-1/f} \tag{3.3}$$

where $\mathfrak{B}$ is the fractional ideal in F generated by the components $\beta_1, \ldots, \beta_n$ of $\boldsymbol{\beta}$. Now in the ideal class of $\mathfrak{B}$ there is an integral ideal $\mathfrak{B}'$ having

$$\mathfrak{N}(\mathfrak{B}') \leqslant D_{F/\mathbb{Q}}^{1/2}. \tag{3.4}$$

Combining (3.2), (3.3) and (3.4) we find a $\lambda \in F$, $\lambda \neq 0$ such that in fact $\boldsymbol{\beta}' = \lambda\boldsymbol{\beta}$ satisfies the assertion of the lemma.

For $\boldsymbol{\beta} \in F^n$ we define $\overline{|\boldsymbol{\beta}|} = \max\{|\beta_1^{(1)}|, \ldots, |\beta_n^{(1)}|, \ldots, |\beta_1^{(f)}|, \ldots, |\beta_n^{(f)}|\}$, where for $\beta \in F$, $\beta^{(1)}, \ldots, \beta^{(f)}$ are the conjugates of β.

For a number field F of degree f we denote by $M(F)$ the set of its prime divisors. Let $M'(F)$ be a set of symbols v, such that with every $v \in M'(F)$ there is associated an absolute value $|\ |_v$ of F, and moreover every absolute value $|\ |_w$ of F is obtained in this way for precisely f_w elements v of $M'(F)$. Here f_w denotes the local degree, i.e. the degree of F_w over $\mathbb{Q}_w$, where F_w is the w-adic completion of F and $\mathbb{Q}_w$ the completion of $\mathbb{Q}$.

In other words $M'(F)$ is the set of absolute values of F with multiplicities, so that a given $|\ |_w$ occurs f_w times.

Given a prime divisor $w \in M(\mathbb{Q})$ there exists f elements $v_1, \ldots, v_f$ in $M'(F)$ lying above w. (We use for this again the symbol $v_i \mid w$.)

LEMMA 3.2. *Given* $\boldsymbol{\beta} \in F^n$, $\boldsymbol{\beta} \neq 0$, *there exists an integer* $\lambda \in F$, $\lambda \neq 0$ *with the following properties*:

$$|N_{F/\mathbb{Q}}(\lambda)| \leqslant D_{F/\mathbb{Q}}^{1/2} \tag{3.5}$$

and

$$\overline{|\lambda\boldsymbol{\beta}|} \leqslant D_{F/\mathbb{Q}}^{1/2f}\Bigl(\prod_{v\in M'_\infty(F)}|\boldsymbol{\beta}|_v\Bigr)^{1/f}. \tag{3.6}$$

Proof. Consider the set of inequalities

$$|\lambda|_w \leqslant \mu\frac{(\prod_{v\in M'_\infty(F)}|\boldsymbol{\beta}|_v)^{1/f}}{|\boldsymbol{\beta}|_w} \quad \text{if } w\in M'_\infty(F) \tag{3.7}$$

$$|\lambda|_w \leqslant 1 \quad \text{if } w\in M'_0(F) \tag{3.8}$$

with μ yet to be determined.

Here $M'_\infty(F)$ and $M'_0(F)$ are defined in the same way with respect to $M_\infty(F)$ and $M_0(F)$ as $M'(F)$ with respect to $M(F)$. According to the generalization of Minkowski's lattice point theorem to number fields (cf. Bombieri and Vaaler [2], Theorem 3) the system (3.7), (3.8) has a nontrivial solution $\lambda\in F$ with

$$\mu = D_{F/\mathbb{Q}}^{1/2f} \tag{3.9}$$

Now (3.8) implies that λ may be chosen as an integer in F. Moreover with μ chosen as in (3.9), (3.5) follows from (3.7).

Another consequence of (3.7) and (3.9) is that

$$\overline{|\lambda\boldsymbol{\beta}|} = \max_{w\in M_\infty(F)}|\lambda\boldsymbol{\beta}|_w \leqslant D_{F/\mathbb{Q}}^{1/2f}\Bigl(\prod_{v\in M_\infty(F)}|\boldsymbol{\beta}|_v\Bigr)^{1/f}$$

and (3.6) is proved.

LEMMA 3.3. *Suppose K is a number field of degree d. Let $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_n\in K^n$ be linearly independent. Then for each $v\in M(K)$ we have*

$$|\boldsymbol{\alpha}_1|_v\cdots|\boldsymbol{\alpha}_n|_v \leqslant |\det(\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_n)|_v(H(\boldsymbol{\alpha}_1)\cdots H(\boldsymbol{\alpha}_n))^d. \tag{3.10}$$

This is Lemma 5.2 of Schmidt [16].

4. Integral bases and discriminants

For our proof of Proposition 2.1, an essential ingredient will be a lower bound for the height of solutions in terms of the discriminant. Such a result is given by

LEMMA 4.1. *Let F be a number field of degree $f > 1$. Denote by $D = D_{F/\mathbb{Q}}$ the* *absolute value of the discriminant of F. Let* $\boldsymbol{\beta}=(\beta_1,\ldots,\beta_n)\in F^n$ *be such that* $\boldsymbol{\beta}$ *defines F over* $\mathbb{Q}$. *Then*

$$H(\boldsymbol{\beta}) \geqq (f^{-f}D)^{1/2f(f-1)} \tag{4.1}$$

This is a special case of Silverman [18] (Theorem 2).

Using an integral basis of F we shall reduce the assertion of Proposition 2.1 to the case when the variables lie in $\mathbb{Q}$. To do this successfully, we need an integral basis $\gamma_1,\ldots,\gamma_f$ of F such that $H(\boldsymbol{\gamma})=H(\gamma_1,\ldots,\gamma_f)$ is not too large as compared with the discriminant $D_{F/\mathbb{Q}}$. Let $\sigma_1,\ldots,\sigma_f$ be the embeddings of F into $\bar{\mathbb{Q}}$. For $\gamma\in F$ put $\sigma_i(\gamma)=\gamma^{(i)}$ $(1\leqslant i\leqslant f)$.

LEMMA 4.2. *There exists an integral basis* $\gamma_1,\ldots,\gamma_f$ *of F having*

$$D_{F/\mathbb{Q}} \leqslant H(\boldsymbol{\gamma})^{2f} \tag{4.2}$$

and

$$H(\boldsymbol{\gamma}) \leqslant f!f^{1/2}\cdot 2^f V(f)^{-1}D_{F/\mathbb{Q}}^{1/2} \tag{4.3}$$

$$\max_{1\leqslant i,j\leqslant f} |\gamma_j^{(i)}| \leqslant f!2^f V(f)^{-1}D_{F/\mathbb{Q}}^{1/2}, \tag{4.4}$$

where $V(f)$ *denotes the volume of the f-dimensional unit ball.*

Proof. Let $\hat{\gamma}_1,\ldots,\hat{\gamma}_f$ be any integral basis of F over $\mathbb{Q}$. Recall that

$$D_{F/\mathbb{Q}} = \begin{vmatrix} \hat{\gamma}_1^{(1)},\ldots,\hat{\gamma}_f^{(n)} \\ \vdots \qquad \vdots \\ \hat{\gamma}_1^{(f)},\ldots,\hat{\gamma}_f^{(f)} \end{vmatrix}^2. \tag{4.5}$$

Moreover, we have

$$\prod_{\substack{v\in M(F)\\ v\nmid\infty}} \|\hat{\boldsymbol{\gamma}}\|_v = \mathfrak{N}(\hat{\gamma}_1,\ldots,\hat{\gamma}_f)^{-1} = 1.$$

Therefore

$$H(\hat{\boldsymbol{\gamma}}) = \prod_{i=1}^{f} (|\hat{\gamma}_1^{(i)}|^2+\cdots+|\hat{\gamma}_f^{(i)}|^2)^{1/2f} \tag{4.6}$$

and (4.2) is an immediate consequence of Hadamard's inequality. The more interesting part of Lemma 4.2 is (4.3), (4.4). The method of proof here is similar to the one applied by Schmidt [17] (Lemma 2).

We consider the column vectors

$$\hat{\gamma}_i = \begin{pmatrix} \hat{\gamma}_i^{(1)} \\ \vdots \\ \hat{\gamma}_i^{(f)} \end{pmatrix} \quad (i = 1, \dots, f)$$

in (4.5). $\hat{\gamma}_1, \dots, \hat{\gamma}_f$ generate a $\mathbb{Z}$-module Λ^* of rank f in $\mathbb{C}^f$. Suppose that the embeddings $\sigma_1, \dots, \sigma_f$ are ordered such that $\sigma_1, \dots, \sigma_r$ are real and $\sigma_{r+1}, \sigma_{r+2}, \dots, \sigma_{f-1}, \sigma_f$ are complex conjugate in pairs. For vectors $\mathbf{z}, \mathbf{z}' \in \mathbb{C}^f$ let $(\mathbf{z}, \mathbf{z}')$ be the inner product $z_1\bar{z}'_1 + \cdots + z_f\bar{z}'_f$. Thus for points $\mathbf{z}, \mathbf{z}' \in \Lambda^*$ we have

$$(\mathbf{z}, \mathbf{z}') = z_1 z'_1 + \cdots + z_r z'_r + z_{r+1}\bar{z}'_{r+1} + \cdots + z_f \bar{z}'_f .$$

Consider the map $\varphi: \Lambda^* \to \mathbb{R}^f$ defined by

$$\varphi(\mathbf{z}) = \varphi \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ z_{r+1} \\ z_{r+2} \\ \vdots \\ z_{f-1} \\ z_f \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ \sqrt{2}\,\mathrm{Re}\, z_{r+1} \\ \sqrt{2}\,\mathrm{Im}\, z_{r+1} \\ \vdots \\ \sqrt{2}\,\mathrm{Re}\, z_{f-1} \\ \sqrt{2}\,\mathrm{Im}\, z_{f-1} \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_r \\ w_{r+1} \\ w_{r+2} \\ \vdots \\ w_{f-1} \\ w_f \end{pmatrix}.$$

Then, given $\mathbf{z}, \mathbf{z}' \in \Lambda^*$ an easy computation shows that $(\varphi(\mathbf{z}), \varphi(\mathbf{z}')) = (\mathbf{z}, \mathbf{z}')$, which means that φ preserves inner products. Put $\varphi(\Lambda^*) = \Lambda$, so that Λ is a lattice of rank f in $\mathbb{R}^f$ and φ induces a bijection between Λ^* and Λ. Moreover, since φ preserves inner products, we have

$$|\det((\hat{\gamma}_i, \hat{\gamma}_j))| = |\det(\varphi(\hat{\gamma}_i), \varphi(\hat{\gamma}_j))| = (\det \Lambda)^2 = D_{F/\mathbb{Q}} . \tag{4.7}$$

Let $\lambda_1, \dots, \lambda_f$ be the successive minima of the d-dimensional unit ball with respect to Λ. Then by Minkowski (cf. Cassels [3], Theorem V, p. 218)

$$\lambda_1 \cdots \lambda_f V(f) \leqq 2^f \det \Lambda . \tag{4.8}$$

There exists a basis $\mathbf{w}_1, \dots, \mathbf{w}_f$ of Λ having

$$|\mathbf{w}_i| \leqslant i\lambda_i \quad (i = 1, \dots, f) \tag{4.9}$$

(cf. Cassels [3], Lemma 8, p. 135). Combining (4.8) and (4.9) we obtain

$$|\mathbf{w}_1| \cdots |\mathbf{w}_f| \leqslant f!\lambda_1 \cdots \lambda_f \leqslant \frac{f!2^f \det \Lambda}{V(f)} . \tag{4.10}$$

Let $\mathbf{z}_i = \varphi^{-1}(\mathbf{w}_i)$ be the corresponding basis of Λ^*. Then (4.10) and (4.7) imply that

$$|\mathbf{z}_1| \cdots |\mathbf{z}_f| \leqslant f!2^f V(f)^{-1} D_{F/\mathbb{Q}}^{1/2}. \tag{4.11}$$

Let us study more in detail the points $\mathbf{z}_1, \ldots, \mathbf{z}_f$. We have $\mathbf{z}_i = x_{i1}\hat{\boldsymbol{\gamma}}_1 + \cdots + x_{if}\hat{\boldsymbol{\gamma}}_f$ with suitable integers $x_{i1}, \ldots, x_{if}$. Since $\mathbf{z}_1, \ldots, \mathbf{z}_f$ are a basis of Λ^* we may infer that the elements $\gamma_i = x_{i1}\hat{\gamma}_1 + \cdots + x_{if}\hat{\gamma}_f$ $(i = 1, \ldots, f)$ form an integral basis of F. Let $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_f)$. Then in view of (4.6) we get

$$H(\boldsymbol{\gamma}) = \prod_{i=1}^{f} (|\gamma_1^{(i)}|^2 + \cdots + |\gamma_f^{(i)}|^2)^{1/2f} \leqslant f^{1/2} \max_{i \leqslant i,j \leqslant f} |\gamma_j^{(i)}|. \tag{4.12}$$

Notice that the components of $\mathbf{z}_j$ are the f conjugates of the algebraic integer γ_j. We may conclude that

$$|\mathbf{z}_j| \geqslant 1 \quad \text{for each } j \quad (1 \leqslant j \leqslant f). \tag{4.13}$$

Suppose without loss of generality that the maximum in (4.12) is assumed for $j = 1$. Then (4.12) says that

$$f^{-1/2} H(\boldsymbol{\gamma}) \leqq \max_{1 \leqslant i \leqslant f} |\gamma_1^{(i)}| \leqslant |\mathbf{z}_1|. \tag{4.14}$$

Combination of (4.11), (4.13), (4.14) yields

$$f^{-1/2} H(\boldsymbol{\gamma}) \leqslant f!2^f V(f)^{-1} D_{F/\mathbb{Q}}^{1/2}$$

and

$$\max_{1 \leqslant i,j \leqslant f} |\gamma_j^{(i)}| \leqslant f!2^f V(f)^{-1} D_{F/\mathbb{Q}}^{1/2},$$

which proves (4.3) and (4.4).

5. A gap principle

The following lemma will be crucial for us to deal with comparatively small solutions. It appears implicitly already in Mahler [6] (p. 710f).

LEMMA 5.1. *Suppose* $0 < \gamma < 1$ *and* $q \in \mathbb{N}$ *are given. Then there is a subset* M *of cardinality* $\leqslant 2^{q/(1-\gamma)}$ *of the set*

$$\{(\Gamma_1, \ldots, \Gamma_q) \mid \Gamma_1 + \cdots + \Gamma_q = \gamma, \Gamma_i \geqslant 0 \ (i = 1, \ldots, q)\}$$

with the following property: For every point $\mathbf{x}=(x_1,\ldots,x_q)$ *in* $\mathbb{R}^q$ *having* $x_i \geqslant 0$ *for each* i $(i=1,\ldots,q)$ *there exists a point* $\mathbf{\Gamma}=(\Gamma_1,\ldots,\Gamma_q)\in M$ *such that for each* i $(i=1,\ldots,q)$

$$x_i \geqslant \Gamma_i(x_1+\cdots+x_q)$$

holds true.

Proof. In the case $x_1=\cdots=x_q=0$ any $(\Gamma_1,\ldots,\Gamma_q)$ will satisfy the assertion. Thus we may assume that $x_1+\cdots+x_q>0$. By homogeneity we may suppose that

$$x_1+x_2+\cdots+x_q=1. \tag{5.1}$$

Define λ by

$$\frac{1}{1+\lambda}=\gamma. \tag{5.2}$$

Let v be the smallest integer such that

$$\lambda v \geqslant q. \tag{5.3}$$

Moreover define nonnegative integers g_i by

$$g_i=[v(1+\lambda)x_i] \quad (i=1,\ldots,q). \tag{5.4}$$

Now (5.4) implies that there exists real numbers ρ_i $(i=1,\ldots,q)$ with

$$(1+\lambda)x_i=\frac{g_i}{v}+\rho_i \quad \text{and} \quad 0\leqslant \rho_i<\frac{1}{v}. \tag{5.5}$$

Combination of (5.3) and (5.5) yields

$$0\leqslant \sum_{i=1}^{q}\rho_i<\lambda \tag{5.6}$$

On the other hand we infer from (5.1), (5.5), (5.6) that

$$\sum_{i=1}^{q}\frac{g_i}{v}=(1+\lambda)\sum_{i=1}^{q}x_i-\sum_{i=1}^{q}\rho_i>(1+\lambda)-\lambda=1$$

and therefore

$$\sum_{i=1}^{q} g_i > v.$$

We now replace the integers g_i in (5.4) by integers f_i satisfying

$$0 \leqslant f_i \leqslant g_i, \qquad f_1 + \cdots + f_q = v. \tag{5.7}$$

Then, using (5.1), (5.2), (5.5), we get

$$x_i \geqslant \frac{f_i}{v} \cdot \frac{1}{1+\lambda} + \frac{\rho_i}{1+\lambda} = \frac{f_i}{v}\gamma + \rho_i\gamma \geqslant \frac{f_i}{v}\gamma(x_1 + \cdots + x_q) \tag{5.8}$$

So given γ, we may choose $\Gamma_i = f_i\gamma/v$ with v defined by (5.3) and f_i satisfying (5.7). Notice that by (5.7) we have $\Gamma_1 + \cdots + \Gamma_q = \gamma$.

Given v the number of choices for $f_1, \ldots, f_q$ with (5.7) is bounded by

$$\binom{v+q-1}{q-1} \leqslant 2^{v+q-1}. \tag{5.9}$$

On the other hand the definition of v in (5.3) implies that

$$v \leqslant \frac{q}{\lambda} + 1. \tag{5.10}$$

Combining (5.9) and (5.10) we see that

$$\leqslant 2^{q/\lambda + q} = 2^{q/(1-\gamma)}$$

tuples $(\Gamma_1, \ldots, \Gamma_q)$ will suffice.

Let $L_i^{(v)}$ be the forms in our Theorem. We put

$$H = \max\{H(L_i^{(v)})\ (i = 1, \ldots, n;\ v \in S)\}.$$

LEMMA 5.2. *Let K, S, δ, $L_1^{(v)}, \ldots, L_n^{(v)} (v \in S)$ be as in the Theorem. Suppose A and B are positive real numbers satisfying*

$$A < B \quad \text{and} \quad A > (n!H^{nsd})^{48/11\delta}. \tag{5.11}$$

Then the solutions $\boldsymbol{\beta} \in K^n$ *of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} \frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} < H(\boldsymbol{\beta})^{-n-\delta} \tag{5.12}$$

with

$$A \leqslant H(\boldsymbol{\beta}) \leqslant B \tag{5.13}$$

lie in the union of not more than

$$2^{8n^2 s/\delta}\left(1 + \log \frac{\log B}{\log A}\right) \tag{5.14}$$

proper subspaces of K^n.

Proof. Since $\frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} \leqslant 1$ for each pair (v, i) with $v \in S$, $i = 1, \dots, n$ and for any $\boldsymbol{\beta} \in K^n \backslash \{0\}$, we see that for each solution $\boldsymbol{\beta}$ of (5.12) there exists an $n \cdot s$-tuple of nonnegative real numbers x_{vi} ($v \in S$, $i = 1, \dots, n$) such that

$$\sum_{v \in S} (x_{vi} + \cdots + x_{vn}) = 1$$

and

$$\frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} \leqslant H(\boldsymbol{\beta})^{-(n+\delta)x_{vi}} \tag{5.15}$$

holds true, and for at least one pair (v, i) we have strict inequality in (5.15).

We now apply Lemma 5.1 with

$$\gamma = 1 - \frac{\delta}{4(n+1)} \tag{5.16}$$

and

$$q = n \cdot s \tag{5.17}$$

Accordingly there is a set M of cardinality $\leqslant 2^{ns/(1-\gamma)}$ of tuples $\boldsymbol{\Gamma} = (\Gamma_{vi})$ such that each solution of (5.15) satisfies

$$\frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} \leqslant H(\boldsymbol{\beta})^{-(n+\delta)\Gamma_{vi}} \quad (v \in S,\ i = 1, \dots, n) \tag{5.18}$$

for a suitable tuple $\mathbf{\Gamma}$, and again for at least one pair (v, i) we have strict inequality in (5.18). We now subdivide the solutions $\boldsymbol{\beta}$ into classes C_{Γ} and we say that $\boldsymbol{\beta}$ belongs to C_{Γ} if it satisfies (5.18) for $\mathbf{\Gamma}$. Remember that we have not more than

$$2^{ns/(1-\gamma)} \tag{5.19}$$

classes C_{Γ}.

We next restrict ourselves to solutions $\boldsymbol{\beta}$ belonging to a fixed class C_{Γ}. We claim that for any E with

$$A \leqslant E \tag{5.20}$$

there exists a proper subspace of K^n containing the solutions $\boldsymbol{\beta} \in C_{\Gamma}$ having

$$E \leqslant H(\boldsymbol{\beta}) \leqslant E^{1+\delta/2n} \tag{5.21}$$

Suppose for the moment our claim to be proved. Notice that the interval $A \leqslant x < B$ may be covered by

$$\leqslant 1 + \frac{4n}{\delta} \log \frac{\log B}{\log A}$$

intervals of type (5.21). Therefore the solutions $\boldsymbol{\beta} \in C_{\Gamma}$ are contained in the union of

$$\leqslant 1 + \frac{4n}{\delta} \log \frac{\log B}{\log A}$$

proper subspaces of K^n. Allowing a factor $2^{ns/(1-\gamma)}$ for the number of classes (cf. (5.19)) we see that the solutions of (5.12), (5.13) are contained in the union of not more than

$$2^{8n^2s/\delta}\left(1 + \log \frac{\log B}{\log A}\right)$$

and (5.14) follows.

It remains to prove our claim concerning (5.21), (5.20).

Let $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ be any solutions in C_{Γ} satisfying (5.21). We may suppose that

$$H(\boldsymbol{\beta}_1) \leqslant H(\boldsymbol{\beta}_2) \leqslant \cdots \leqslant H(\boldsymbol{\beta}_n) \tag{5.22}$$

holds true. We are going to prove that

$$\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n) = 0.$$

In view of the product formula for K this will certainly be true if we can show that

$$\prod_{v \in M'(K)} |\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|_v < 1. \tag{5.23}$$

Recall the definition of $\| \ \|_v$ in (1.6). Now (5.18) and (5.22) imply that we have for each $v \in S$

$$\frac{|L_i^{(v)}(\boldsymbol{\beta}_j)|_v}{|L_i^{(v)}|_v |\boldsymbol{\beta}|_v} \leqslant H(\boldsymbol{\beta}_1)^{-d(n+\delta)\Gamma_{vi}/d_v} \quad (i = 1, \ldots, n; j = 1, \ldots, n). \tag{5.24}$$

We infer from (5.24) that

$$|\det((L_i^{(v)}(\boldsymbol{\beta}_j))_{i,j})|_v \leqslant \prod_{i=1}^{n} (|L_i^{(v)}|_v |\boldsymbol{\beta}_i|_v) H(\boldsymbol{\beta}_1)^{-d(n+\delta)(\Sigma_{i=1}^n \Gamma_{vi})/d_v} \tag{5.25}$$

for $v \in S$, v nonarchimedean, and

$$|\det((L_i^{(v)}(\boldsymbol{\beta}_j))_{i,j})|_v \leqslant n! \prod_{i=1}^{n} (|L_i^{(v)}|_v |\boldsymbol{\beta}_i|_v) H(\boldsymbol{\beta}_1)^{-d(n+\delta)(\Sigma_{i=1}^n \Gamma_{vi})/d_v} \tag{5.26}$$

for $v \in S$, v archimedean.

We apply Lemma 3.3 and thus we may replace the term

$$\prod_{i=1}^{n} |L_i^{(v)}|_v$$

on the right-hand side of (5.25) and of (5.26) by $|\det(L_i^{(v)}, \ldots, L_n^{(v)})|_v \cdot H^{nd}$ where H is a quantity with $H \geqslant \max\{H(L_i^{(v)}) \ (v \in S, i = 1, \ldots, n)\}$. Then we get cancelling $|\det(L_1^{(v)}, \ldots, L_n^{(v)})|$ on both sides

$$|\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|_v \leqslant H^{nd} \prod_{i=1}^{n} |\boldsymbol{\beta}_i|_v \cdot H(\boldsymbol{\beta}_1)^{-d(n+\delta)(\Sigma_{i=1}^n \Gamma_{vi})/d_v} \tag{5.27}$$

for $v \in S$, v nonarchimedean, and

$$|\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|_v \leqslant n! H^{nd} \prod_{i=1}^{n} |\beta_i|_v H(\boldsymbol{\beta}_1)^{-d(n+\delta)(\Sigma_{i=1}^n \Gamma_{vi})/d_v} \tag{5.28}$$

for $v \in S$, v archimedean.

We next treat $v \notin S$. Here we obtain

$$|\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|_v \leqslant \prod_{i=1}^{n} |\boldsymbol{\beta}_i|_v \quad \text{for each } v \notin S. \tag{5.29}$$

Combination of (5.27), (5.28), (5.29) yields (noting that $d_v \leqslant d$)

$$\prod_{v \in M(K)} \|\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)\|_v < n! H^{nds} H(\boldsymbol{\beta}_1) \cdots H(\boldsymbol{\beta}_n) \cdot H(\boldsymbol{\beta}_1)^{-(n+\delta)\gamma}. \tag{5.30}$$

Recall the definition of γ in (5.16). Remember that $H(\boldsymbol{\beta}_1)$ satisfies (5.13). Therefore

$$n! H^{nds} < H(\boldsymbol{\beta}_1)^{\frac{11}{12} \cdot \frac{\delta}{4}} < H(\boldsymbol{\beta}_1)^{\delta(1-\delta/4(n+1))/4} = H(\boldsymbol{\beta}_1)^{\gamma\delta/4} \tag{5.31}$$

Moreover, by (5.21) we have

$$H(\boldsymbol{\beta}_1)^{(n+3\delta/4)\gamma} > H(\boldsymbol{\beta}_1)^{n+\delta/2} > H(\boldsymbol{\beta}_1) \cdots H(\boldsymbol{\beta}_n). \tag{5.32}$$

Combination of (5.30), (5.31), (5.32) implies

$$\prod_{v \in M(K)} \|\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)\|_v < 1.$$

Therefore our claim is proved and the lemma follows.

6. Application of the gap principle

LEMMA 6.1. *Let K, F, R, δ, $L_1^{(v)}, \ldots, L_n^{(v)}$* ($v \in R$) be as in Proposition 2.1. *Put* $H = \max\{H(L_i^{(v)})\ (i = 1, \ldots, n;\ v \in R)\}$. *Then the solutions $\boldsymbol{\beta} \in F^n$ of* (2.1) *such that*

$$\boldsymbol{\beta} \textit{ defines } F \text{ over } \mathbb{Q} \tag{6.1}$$

(*i.e. with* (2.2)) *and such that moreover*

$$C \leqslant H(\boldsymbol{\beta}) \leqslant (2HD_{F/\mathbb{Q}}^{1/6d^2})^{E^2} \tag{6.2}$$

with

$$C = \max\{(n!)^{9/\delta}, H^{9nrd/\delta}\} \tag{6.3}$$

$$E = [(8rd)^{2^{26nd} \cdot 8192 r^6 \delta^{-2}}] \tag{6.4}$$

are contained in the union of not more than

$$t_3 = 3 \cdot 2^{8n^2r/\delta} \log E \tag{6.5}$$

proper subspaces of F^n.

Proof. We remark that condition (6.1) is crucial to get in (6.5) a result that does not depend upon the discriminant of F. In fact Lemma 4.1 says that $\boldsymbol{\beta}$ with (6.1) has for $F \neq \mathbb{Q}$

$$H(\boldsymbol{\beta}) \geqslant (D_{F/\mathbb{Q}} \cdot f^{-f})^{1/2f(f-1)}.$$

Thus we may suppose that

$$H(\boldsymbol{\beta}) \geqslant \frac{1}{2} \cdot (D_{F/\mathbb{Q}})^{1/2d^2}. \tag{6.6}$$

Combining (6.3) and (6.6) we have only to study those $\boldsymbol{\beta}$ for which

$$H(\boldsymbol{\beta}) \geqslant \max\left\{(n!)^{9/\delta},\ H^{9nrd/\delta},\ \frac{1}{2} D_{F/\mathbb{Q}}^{1/2d^2}\right\}.$$

We want to apply Lemma 5.2 with

$$A = \max\left\{(n!)^{9/\delta},\ H^{9nrd/\delta},\ \frac{1}{2} D_{F/\mathbb{Q}}^{1/2d^2}\right\} \tag{6.7}$$

and with S replaced by R. Here we get $A \geqslant (n!)^{9/2\delta} H^{9nrd/2\delta} \geqslant (n! H^{nrd})^{48/11\delta}$. Thus, in our context the second inequality in (5.11) is satisfied.

Moreover, by (6.7)

$$A \geqslant (n!)^{3/\delta} H^{3nrd/\delta} 2^{-1/3} D_{F/\mathbb{Q}}^{1/6d^2} > 2HD_{F/\mathbb{Q}}^{1/6d^2}. \tag{6.8}$$

Put $B = (2HD_{F/\mathbb{Q}}^{1/6d^2})^{E^2}$. Then, using (6.8) we see that

$$\frac{\log B}{\log A} \leqslant E^2$$

and by (5.14) the solutions in question are contained in the union of not more than

$$2^{8n^2r/\delta}(1 + 2 \log E) \leqslant 3 \log E \cdot 2^{8n^2r/\delta}$$

proper subspaces of F^n.

7. Rational integral variables

Let $\gamma_1, \ldots, \gamma_f$ be the integral basis of F over $\mathbb{Q}$ constructed in Section 4. Put $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_f)$. Denote by O_F the ring of integers in F.

LEMMA 7.1. *Suppose* $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ *lies on* O_F^n. *Then writing*

$$\beta_i = x_{i1}\gamma_1 + \cdots + x_{if}\gamma_f \quad (i = 1, \ldots, n) \tag{7.1}$$

with $\mathbf{x} = (x_{11}, \ldots, x_{1f}, \ldots, x_{n1}, \ldots, x_{nf}) \in \mathbb{Z}^{nf}$ *we have*

$$|\mathbf{x}| \leqslant \sqrt{nf}\, f!D_{F/\mathbb{Q}}^{-1/2}\overline{|\boldsymbol{\gamma}|}^{f-1}\overline{|\boldsymbol{\beta}|} \tag{7.2}$$

$$\overline{|\boldsymbol{\beta}|} \leqslant |\bar{\gamma}|\,|\mathbf{x}|. \tag{7.3}$$

Proof. Let $\sigma_1, \ldots, \sigma_f$ be the embeddings of F over $\mathbb{Q}$ into an algebraically closed field. For $\gamma \in F$ we put $\gamma^{(j)} = \sigma_j(\gamma)$ $(j = 1, \ldots, f)$. Then (7.1) yields the system of equations

$$\begin{matrix} \beta_i^{(1)} = x_{i1}\gamma_1^{(1)} + \cdots + x_{if}\gamma_f^{(1)} \\ \vdots \qquad \vdots \qquad\qquad \vdots \\ \beta_i^{(f)} = x_{i1}\gamma_1^{(f)} + \cdots + x_{if}\gamma_f^{(f)} \end{matrix} \quad (i = 1, \ldots, n). \tag{7.4}$$

Applying Cramer's rule to (7.4) we get immediately

$$|x_{ij}| \leqslant D_{F/\mathbb{Q}}^{-1/2}(f-1)!\overline{|\boldsymbol{\gamma}|}^{f-1}\overline{|\boldsymbol{\beta}|}f = f!D_{F/\mathbb{Q}}^{-1/2}\overline{|\boldsymbol{\gamma}|}^{f-1}\overline{|\boldsymbol{\beta}|}$$

and (7.2) follows. (7.3) also is an obvious consequence of (7.4).

LEMMA 7.2. *Let* $L(\boldsymbol{\beta}) = \lambda_1\beta_1 + \cdots + \lambda_n\beta_n$ *be a linear form with coefficients in* K. *Suppose* $\boldsymbol{\beta} \in O_F^n$. *If we replace* $\boldsymbol{\beta}$ *by the vector* $\mathbf{x} = (x_{11}, \ldots, x_{nf})$ *defined in* (7.1) *and if we put* $L(\boldsymbol{\beta}) = M(\mathbf{x})$, *then the height of the linear form* M *satisfies*

$$H(M) = H(\boldsymbol{\gamma})H(L). \tag{7.5}$$

Proof. We have

$$\lambda_1\beta_1 + \cdots + \lambda_n\beta_n = \lambda_1\gamma_1x_{11} + \cdots + \lambda_1\gamma_fx_{1f} + \cdots + \lambda_n\gamma_1x_{n1} + \cdots + \lambda_n\gamma_fx_{nf}.$$

Thus the coefficient vector $(\lambda_1\gamma_1, \ldots, \lambda_1\gamma_f, \ldots, \lambda_n\gamma_1, \ldots, \lambda_n\gamma_f)$ of M has

$$|M|_v = |\boldsymbol{\gamma}|_v|L|_v$$

for any $v \in M(K)$. In view of the definition of the height in (1.8) assertion (7.5) follows.

LEMMA 7.3. *Let $w \in M(\mathbb{Q})$. Suppose that for each $v_i \in M'(F)$ with $v_i | w$ $(i = 1, \ldots, f)$ we are given linearly independent linear forms $L_1^{(v_i)}, \ldots, L_n^{(v_i)}$ with coefficients in K in the variables $\boldsymbol{\beta}^{(i)} = (\beta_1^{(i)}, \ldots, \beta_n^{(i)}) \in (\sigma_i(O_F))^n$ (with $\beta_j^{(i)}$ defined as in (7.4)). Then, if we replace $\beta_j^{(i)}$ by $x_{j1}, \ldots, x_{jf}$ in $\mathbb{Z}$ as in (7.4) we get new forms $M_1^{(v_1)}, \ldots, M_n^{(v_1)}, \ldots, M_1^{(v_f)}, \ldots, M_n^{(v_f)}$ with coefficients in K in $\mathbf{x} = (x_{11}, \ldots, x_{1f}, \ldots, x_{n1}, \ldots, x_{nf}) \in \mathbb{Z}^{nf}$ and we have*

$$\prod_{\substack{v \in M'(F) \\ v | w}} |\det(L_1^{(v)}, \ldots, L_n^{(v)})|_v = |D_{F/\mathbb{Q}}|_w^{-f/2} |\det(M_1^{(v_1)}, \ldots, M_n^{(v_f)})|_w.$$

Proof. Let Ω_w be the algebraic closure of $\mathbb{Q}_w$. The absolute value $|\ |_w$ has a unique extension to Ω_w which we denote again by $|\ |_w$.

Now the extensions $v_1, \ldots, v_f$ of w onto F may be obtained via the embeddings $\sigma_1, \ldots, \sigma_f$ of F over $\mathbb{Q}$ into Ω_w (in fact since K is normal these are even embeddings into K) by putting for $\alpha \in F, |\alpha|_{v_i} = |\sigma_i(\alpha)|_w$. If we extend the embeddings σ_i to embeddings of K into Ω_w we may understand our forms $L_1^{(v_1)}, \ldots, L_n^{(v_1)}, \ldots, L_1^{(v_f)}, \ldots, L_n^{(v_f)}$ as a system of nf forms in the variables $(\boldsymbol{\beta}^{(1)}, \ldots, \boldsymbol{\beta}^{(f)})$ such that in fact the forms $L_1^{(v_i)}, \ldots, L_n^{(v_i)}$ depend only upon the i-th block of variables $\boldsymbol{\beta}^{(i)}$. So we have

$$|\det(L_1^{(v_1)}, \ldots, L_n^{(v_1)}, \ldots, L_1^{(v_f)}, \ldots, L_n^{(v_f)})|_w = \prod_{i=1}^{f} |\det(L_1^{(v_i)}, \ldots, L_n^{(v_i)})|_{v_i}.$$

On the other hand it is clear that the determinant of the transformation

$$\begin{aligned} \sigma_1(\beta_i) &= x_{i1}\sigma_1(\gamma_1) + \cdots + x_{if}\sigma_1(\gamma_f) \\ &\vdots \qquad\qquad (i = 1, \ldots, n) \\ \sigma_f(\beta_i) &= x_{i1}\sigma_f(\gamma_1) + \cdots + x_{if}\sigma_f(\gamma_f) \end{aligned}$$

has w-adic absolute value $|D_{F/\mathbb{Q}}|_w^{f/2}$. This proves the assertion of the Lemma.

8. Rational integral variables continued

Let $R \subset M(F)$ be as in Proposition 2.1. Let R_1 be the smallest subset of $M(F)$ with the following properties:

$$R_1 \supset R \tag{8.1}$$

$$R_1 \supset M_\infty(F) \tag{8.2}$$

for each $w \in M(\mathbb{Q})$ such that there exists $v \in R$ with $v | w$, R_1 contains all extensions of w onto F. (8.3)

We call R_1 the saturation of R in $M(F)$. Let r_1 be the cardinality of R_1. Then (8.2) and (8.3) imply that

$$r \leqslant r_1 \leqslant (r+1)f \tag{8.4}$$

Thus the difference between R and R_1 is not too dramatic. However, for the solutions of (2.1) which have a comparatively large height it is convenient in the proof of Proposition 2.1, to replace R by R_1. Since the factors on the left-hand side of (2.1) are all bounded above by 1, this will do no harm. In fact the bound (2.3), we shall obtain, will still be in terms of the parameter r and not in terms of r_1.

LEMMA 8.1. *Let K be a normal extension of $\mathbb{Q}$ of degree d. Let F with $K \supset F \supset \mathbb{Q}$ be an intermediate field of degree f over $\mathbb{Q}$. Suppose that R is a finite subset of $M(F)$ of cardinality r and that R_1 is its saturation. For each $v \in R_1$ let $L_1^{(v)}, \ldots, L_n^{(v)}$ be linearly independent linear forms in n variables with coefficients in K. Assume that for each $v \in R_1$, $| \ |_v$ is extended to K. Let $0 < \delta < 1$. Then for each solution $\boldsymbol{\beta} \in F^n$ of the inequality*

$$\prod_{v \in R_1} \prod_{i=1}^{n} \frac{\|L_i^{(v)}(\boldsymbol{\beta})\|_v}{\|L_i^{(v)}\|_v \|\boldsymbol{\beta}\|_v} < H(\boldsymbol{\beta})^{-n-\delta} \tag{8.5}$$

with

$$H(\boldsymbol{\beta}) \geqslant H^{2nd(r+1)f/\delta} D_{F/\mathbb{Q}}^{(n+2)/\delta} \cdot n^{1/2} \tag{8.6}$$

where $H = \max\{H(L_i^{(v)}), (v \in R_1, i = 1, \ldots, n)\}$ there exists a nonzero vector $\boldsymbol{\beta}' \in O_F^n$ that is proportional to $\boldsymbol{\beta}$ and satisfies

$$\prod_{v \in R_1'} |L_1^{(v)}(\boldsymbol{\beta}') \cdots L_n^{(v)}(\boldsymbol{\beta}')|_v < \left(\prod_{v \in R_1'} |\det(L_1^{(v)}, \ldots, L_n^{(v)})|_v \right) \overline{|\boldsymbol{\beta}'|}^{-\delta/2} \tag{8.7}$$

where R_1' is R_1 'with multiplicities' as introduced in Section 3.

Proof. Notice that (8.5) is invariant under replacing $\boldsymbol{\beta}$ by $\lambda\boldsymbol{\beta}$ with $\lambda \in L$, $\lambda \neq 0$. Using Lemma 3.1 we find an element $\lambda \in L$, $\lambda \neq 0$ such that $\lambda\boldsymbol{\beta} \in O_F^n$ and such that (3.1) holds true for $\lambda\boldsymbol{\beta}$. Since R_1 is saturated, we may infer from (8.5) and (3.1) that

$$\begin{aligned}\prod_{v \in R_1} \prod_{i=1}^{n} \|L_i^{(v)}(\lambda\boldsymbol{\beta})\|_v &< \left(\prod_{v \in R_1} \prod_{i=1}^{n} \|L_i^{(v)}\|_v \right) \prod_{v \in R_1} \|\lambda\boldsymbol{\beta}\|_v^n H(\lambda\boldsymbol{\beta})^{-n-\delta} \\ &\leqslant \left(\prod_{v \in R_1} \prod_{i=1}^{n} \|L_i^{(v)}\|_v \right) D_{F/\mathbb{Q}}^{n/2f} H(\lambda\boldsymbol{\beta})^{-\delta}. \end{aligned} \tag{8.8}$$

Applying again (3.1) to (8.8) we get since $\delta < 1$

$$\prod_{v\in R_1}\prod_{i=1}^{n}\|L_i^{(v)}(\lambda\boldsymbol{\beta})\|_v < \left(\prod_{v\in R_1}\prod_{i=1}^{n}\|L_i^{(v)}\|_v\right) D_{F/\mathbb{Q}}^{(n+1)/2f} \prod_{v\in M_\infty(F)}\|\lambda\boldsymbol{\beta}\|^{-\delta}$$

Raising this to the f-th power gives

$$\prod_{v\in R_1'}\prod_{i=1}^{n}|L_i^{(v)}(\lambda\boldsymbol{\beta})|_v < \left(\prod_{v\in R_1'}\prod_{i=1}^{n}|L_i^{(v)}|_v\right) D_{F/\mathbb{Q}}^{(n+1)/2} \prod_{v\in M_\infty'(F)}|\lambda\boldsymbol{\beta}|^{-\delta}. \tag{8.9}$$

To replace the first factor on the right-hand side of (8.9) we use Lemma 3.3 and get in view of (8.4) with $H = \max_{v\in R_1}\{H(L_1^{(v)}),\ldots,H(L_n^{(v)})\}$

$$\prod_{v\in R_1'}\prod_{i=1}^{n}|L_i^{(v)}(\lambda\boldsymbol{\beta})|_v < \left(\prod_{v\in R_1'}|\det(L_1^{(v)},\ldots,L_n^{(v)})|_v\right) H^{nd(r+1)f} D_{F/\mathbb{Q}}^{(n+1)/2} \prod_{v\in M_\infty'(F)}|\lambda\boldsymbol{\beta}|^{-\delta}. \tag{8.10}$$

Put $\lambda\boldsymbol{\beta} = \boldsymbol{\beta}''$. Given $\boldsymbol{\beta}''$, choose $\lambda' \in O_F$ according to Lemma 3.2. If we replace $\boldsymbol{\beta}''$ in (8.10) by $\lambda'\boldsymbol{\beta}'' = \boldsymbol{\beta}'$ say, then (3.5), (3.6) and the fact that R_1 is saturated imply

$$\prod_{v\in R_1'}\prod_{i=1}^{n}|L_i^{(v)}(\boldsymbol{\beta}')|_v < \left(\prod_{v\in R_1'}|\det(L_1^{(v)},\ldots,L_n^{(v)})|_v\right) H^{nd(r+1)f} D_{F/\mathbb{Q}}^{(n+1)/2} D_{F/\mathbb{Q}}^{\delta/2}\,\overline{|\boldsymbol{\beta}'|}^{\,-f\delta}$$

and since $\delta < 1$

$$\prod_{v\in R_1'}\prod_{i=1}^{n}|L_i^{(v)}(\boldsymbol{\beta}')|_v < \left(\prod_{v\in R_1'}|\det(L_1^{(v)},\ldots,L_n^{(v)})|_v\right) H^{nd(r+1)f} D_{F/\mathbb{Q}}^{(n+2)/2}\,\overline{|\boldsymbol{\beta}'|}^{\,-\delta}. \tag{8.11}$$

Since $\boldsymbol{\beta}' \in O_F^n$ the definition of heights in (1.8) shows that

$$\overline{|\boldsymbol{\beta}'|} \geqslant \sqrt{n}^{\,-1}H(\boldsymbol{\beta}') = \sqrt{n}^{\,-1}H(\boldsymbol{\beta}).$$

Thus, applying (8.6) the assertion of the Lemma follows from (8.11).

9. The Subspace Theorem with rational integral solutions

PROPOSITION 9.1. *Let S' be a finite subset of $M(\mathbb{Q})$ of cardinality s' containing the archimedean prime. Let K be a normal extension of $\mathbb{Q}$ of degree d. For each $v \in S'$ let $M_1^{(v)},\ldots,M_m^{(v)}$ be linearly independent linear forms in m variables with coefficients in K. Suppose that for each $v \in S'$ the absolute value $|\;|_v$ is extended from*

$\mathbb{Q}$ to K. Suppose $0 < \eta < 1$. Then there exists proper subspaces $T_1, \ldots, T_{t_4}$ of $\mathbb{Q}^m$ with

$$t_4 = [(8s'd)^{2^{26m}s'^6\eta^{-2}}] \tag{9.1}$$

such that any solution $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ of the inequality

$$\prod_{v \in S'} \prod_{i=1}^{m} |M_1^{(v)}(\mathbf{x}) \cdots M_m^{(v)}(\mathbf{x})|_v < \left(\prod_{v \in S'} |\det(M_1^{(v)}, \ldots, M_m^{(v)})|_v \right) |\mathbf{x}|^{-\eta} \tag{9.2}$$

satisfying

$$|\mathbf{x}| \geqslant \max\{(m!)^{8/\eta}, H(M_i^{(v)}) \ (i = 1, \ldots, m;\ v \in S')\} \tag{9.3}$$

is contained in the union $\bigcup_{i=1}^{t_4} T_i$.

This is the main result of Schlickewei [10]. Notice that the theorem in [10] treats the more general case, where K is an arbitrary extension of $\mathbb{Q}$ of degree d. In that case one would have to replace in (9.1) d by $d!$. However, as is shown in a remark in [10], if K is normal, then in fact (9.1) holds with d.

Again let F with $K \supset F \supset \mathbb{Q}$ the intermediate field of Proposition 2.1 of degree f. Let $\gamma_1, \ldots, \gamma_f$ be the integral basis of F constructed in Section 4. Given $\boldsymbol{\beta} \in O_F^n$ there exists a unique representation of the shape

$$\beta_i = x_{i1}\gamma_1 + \cdots + x_{if}\gamma_f \quad (i = 1, \ldots, n) \tag{9.4}$$

with rational integers x_{ij} $(i = 1, \ldots, n;\ j = 1, \ldots, f)$.

LEMMA 9.2. *Let K and F be as above. Let R and R_1 be as in Lemma 8.1. Suppose that for each $v \in R_1$ we are given linearly independent linear forms $L_1^{(v)}, \ldots, L_n^{(v)}$ in n variables with coefficients in K. Let $0 < \varepsilon < 1$. Put $H = \max\{H(L_i^{(v)}) \ (i = 1, \ldots, n;\ v \in R_1)\}$. Consider the inequality*

$$\prod_{v \in R_1'} |L_1^{(v)}(\boldsymbol{\beta}) \cdots L_n^{(v)}(\boldsymbol{\beta})|_v < \left(\prod_{v \in R_1'} |\det(L_1^{(v)}, \ldots, L_n^{(v)})|_v \right) \overline{|\boldsymbol{\beta}|}^{-\varepsilon}. \tag{9.5}$$

Then there exists proper subspaces $U_1, \ldots, U_{t_5}$ of $\mathbb{Q}^{nf}$ with

$$t_5 = [(8rd)^{2^{26nd} \cdot 512 r^6 \varepsilon^{-2}}] \tag{9.6}$$

such that for any solution $\boldsymbol{\beta} \in O_F^n$ of (9.5) with

$$H(\boldsymbol{\beta}) \geqslant \max\{(nf)!^{17/\varepsilon} \overline{|\boldsymbol{\gamma}|}^{2f}, (nf)!^{3/2} 2^{4f} \overline{|\boldsymbol{\gamma}|} D_{F/\mathbb{Q}}^{1/2} H\} \tag{9.7}$$

the vector $\mathbf{x} = (x_{11}, \ldots, x_{1f}, \ldots, x_{n1}, \ldots, x_{nf}) \in \mathbb{Z}^{nf}$ *corresponding to* $\boldsymbol{\beta}$ *according to* (9.4) *is contained in the union* $\bigcup_{i=1}^{t_5} U_i$.

Proof. Remember that R_1 is saturated. Therefore, if we replace $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ by $\mathbf{x} = (x_{11}, \ldots, x_{1f}, \ldots, x_{n1}, \ldots, x_{nf})$ we get for each tuple $v_1, \ldots, v_f \in R_1'$, which lies above the same element $w \in M(\mathbb{Q})$ $n \cdot f$ linearly independent linear forms $M_1^{(w)}, \ldots, M_{nf}^{(w)}$ in $\mathbf{x}$ with coefficients in K. Let S' be the set of primes in $M(\mathbb{Q})$ lying below R_1. Then S' has cardinality $s' \leqslant r+1$ where r is the cardinality of R.

We apply Lemma 7.1 and Lemma 7.3 to (9.5) and get

$$\prod_{w \in S'} |M_1^{(w)}(\mathbf{x}) \cdots M_{nf}^{(w)}(\mathbf{x})|_w$$
$$< \prod_{w \in S'} (|D_{F/\mathbb{Q}}|_w^{-f/2} |\det(M_1^{(w)}, \ldots, M_{nf}^{(w)})|_w)(\sqrt{nf}\, f!\, D_{F/\mathbb{Q}}^{-1/2} \overline{|\gamma|}^{f-1})^{\varepsilon} \cdot |\mathbf{x}|^{-\varepsilon}. \tag{9.8}$$

Combining (7.3) and (9.7) we see that

$$|\mathbf{x}| \geqslant \overline{|\gamma|}^{-1} \overline{|\boldsymbol{\beta}|} \geqslant n^{-1/2} \overline{|\gamma|}^{-1} H(\boldsymbol{\beta}) \geqslant nf \cdot (f!)^2 \overline{|\gamma|}^{2f-2}$$

and we obtain from (9.8)

$$\prod_{w \in S'} |M_1^{(w)}(\mathbf{x}) \cdots M_{nf}^{(w)}(\mathbf{x})|_w < \left(\prod_{w \in S'} |\det(M_1^{(w)}, \ldots, M_{nf}^{(w)})|_w \right) |\mathbf{x}|^{-\varepsilon/2}. \tag{9.9}$$

We want to apply Proposition 9.1 with $\eta = \varepsilon/2$ and $m = nf$. For this purpose we still have to check condition (9.3).

Now Lemma 7.2 says that for each j $(j = 1, \ldots, nf)$ we have

$$H(M_j^{(w)}) \leqslant H(\gamma) \cdot H.$$

Combining this with (4.3) of Lemma 4.2 and using $\dfrac{1}{(f!)^{1/2} V(f)} < (2\pi)^{f/2}$ we get

$$\begin{aligned} H(M_j^{(w)}) &\leqslant f! f^{1/2} 2^f V(f)^{-1} D_{F/\mathbb{Q}}^{1/2} \cdot H \\ &< (f!)^{3/2} 2^{2f} (2\pi)^{f/2} D_{F/\mathbb{Q}}^{1/2} \cdot H. \end{aligned}$$

Therefore, in view of (9.7) we obtain with (7.3)

$$|\mathbf{x}| \geqslant \overline{|\gamma|}^{-1} \overline{|\boldsymbol{\beta}|} \geqslant n^{-1/2} \overline{|\gamma|}^{-1} H(\boldsymbol{\beta}) > \max\{(nf)!^{16/\varepsilon}, H(M_j^{(w)})\ (j = 1, \ldots, nf;\ w \in S')\}.$$

We now may infer from Proposition 9.1 that our rational integral solutions $\mathbf{x}$ in question lie in the union of not more than

$$(8(r+1)d)^{2^{26nf}(r+1)^6 4\varepsilon^{-2}} \leqslant (8rd)^{2^{26nf}\cdot 512r^6\varepsilon^{-2}} \leqslant (8rd)^{2^{26nd}\cdot 512r^6\varepsilon^{-2}}$$

proper subspaces of $\mathbb{Q}^{nf}$.

10. Back to solutions in F^n

LEMMA 10.1. *There exist proper subspaces $T_1, \ldots, T_{t_6}$ of F^n with*

$$t_6 = [(8rd)^{2^{26nd}\cdot 8192r^6\delta^{-2}}] \tag{10.1}$$

such that any solution $\boldsymbol{\beta} \in O_F^n$ of (2.1) with

$$H(\boldsymbol{\beta}) > \max\{H^{4nd^2r/\delta} D_{F/\mathbb{Q}}^{2n/\delta} \cdot n,\ (dt_6)^{6nd^2/\delta} D_{F/\mathbb{Q}}^{3nd/\delta} H\} \tag{10.2}$$

is contained in the union $\bigcup_{i=1}^{t_6} T_i$.

Proof. In view of Lemma 8.1 it suffices to study solutions $\boldsymbol{\beta} \in O_F^n$ satisfying (8.7) provided that (8.6), i.e.

$$H(\boldsymbol{\beta}) > n^{1/2} H^{2nd(r+1)f/\delta} D_{F/\mathbb{Q}}^{(n+2)/\delta} \tag{10.3}$$

holds true. But because of (10.2), this is amply satisfied. Therefore we may apply Lemma 9.2 for all values of ε with

$$\varepsilon \leqslant \frac{\delta}{2}. \tag{10.4}$$

Notice that t_6 is the value in (9.6) with $\varepsilon = \delta/4$. Put

$$h = f \cdot t_6 \tag{10.5}$$

and consider the $(h \times f)$-Vandermonde-matrix

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{f-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & h & h^2 & \cdots & h^{f-1} \end{pmatrix}.$$

Again let $\gamma_1, \dots, \gamma_f$ be the integral basis of F over $\mathbb{Q}$ from Section 4. Define elements $\lambda_1, \dots, \lambda_h$ in O_F by

$$\lambda_j = \gamma_1 + j\gamma_2 + \cdots + j^{f-1}\gamma_f \quad (j = 1, \dots, h). \tag{10.6}$$

It is clear that any f different elements among the λ_j are linearly independent over $\mathbb{Q}$. To estimate λ_j we may apply (4.4) of Lemma 4.2 and we get for each j $(1 \leqslant j \leqslant h)$ and for $v \in M(F)$, $|\lambda_j|_v \leqslant fh^{f-1} f! 2^f V(f)^{-1} D_{F/\mathbb{Q}}^{1/2}$ for v archimedean. Since $\dfrac{1}{(f!)^{1/2} V(f)} \leqslant (2\pi)^{f/2}$ and since $f \leqslant d$, the definition of t_6 in (10.1) and of h in (10.5) implies

$$|\lambda_j|_v \leqslant h^f D_{F/\mathbb{Q}}^{1/2} \quad \text{for } v \text{ archimedean.} \tag{10.7}$$

From $|N_{F/\mathbb{Q}}(\lambda_j)| \geqslant 1$ and (10.7) we may infer that

$$|\lambda_j|_v \geqslant h^{-f^2+f} D_{F/\mathbb{Q}}^{-f/2} \quad \text{for } v \text{ archimedean.} \tag{10.8}$$

Moreover we have

$$|\lambda_j|_v \leqslant 1 \quad \text{for } v \text{ nonarchimedean.} \tag{10.9}$$

Now let $\boldsymbol{\beta}$ be a solution of (9.5) with $\varepsilon = \dfrac{\delta}{2}$. Using the estimates (10.7), (10.9) we conclude that for each j $(1 \leqslant j \leqslant h)$ $\lambda_j \boldsymbol{\beta}$ satisfies

$$\prod_{v \in R_1'} \prod_{i=1}^{n} |L_i^{(v)}(\lambda_j \boldsymbol{\beta})|_v < \left(\prod_{v \in R_1'} |\det(L_1^{(v)}, \dots, L_n^{(v)})|_v \right) h^{nf^2} D_{F/\mathbb{Q}}^{nf/2} h^{f/2} D_{F/\mathbb{Q}}^{1/4} \overline{|\lambda_j \boldsymbol{\beta}|}^{\,-\delta/2} \tag{10.10}$$

In view of (10.8) and (10.2) we obtain

$$\begin{aligned} \overline{|\lambda_j \boldsymbol{\beta}|} &\geqslant h^{-f^2+f} D_{F/\mathbb{Q}}^{-f/2}\, \overline{|\boldsymbol{\beta}|} \geqslant h^{-f^2+f} D_{F/\mathbb{Q}}^{-f/2} h^{-1/2} H(\boldsymbol{\beta}) \\ &\geqslant (h^{nf^2+f/2} D_{F/\mathbb{Q}}^{nf/2+1/4})^{4/\delta} \end{aligned}$$

Thus if $\boldsymbol{\beta}$ is a solution in O_F^n of (9.5) with $\varepsilon = \dfrac{\delta}{2}$, then (10.10) implies that $\lambda_j \boldsymbol{\beta}$ is a solution $\boldsymbol{\beta}'$ of

$$\prod_{v \in R_1'} \prod_{i=1}^{n} |L_i^{(v)}(\boldsymbol{\beta}')|_v < \left(\prod_{v \in R_1'} |\det(L_1^{(v)}, \dots, L_n^{(v)})|_v \right) \overline{|\boldsymbol{\beta}'|}^{\,-\delta/4} \tag{10.11}$$

To apply Lemma 9.2 we still have to check (9.7) with $\varepsilon = \delta/4$. But it is easily seen that the lower bound in (10.2) by far exceeds the lower bound in (9.7). (We recall in that context that the vector $\boldsymbol{\gamma}$ in (9.7) satisfies (4.4).)

Now Lemma 9.2 says that the rational integral points $\mathbf{x}^{(j)} = (x_{11}^{(j)}, \ldots, x_{1f}^{(j)}, \ldots, x_{n1}^{(j)}, \ldots, x_{nf}^{(j)})$ corresponding to our solutions $\lambda_j \boldsymbol{\beta}$ of (10.11) lie in the union of proper subspaces $U_1, \ldots, U_{t_6}$ of $\mathbb{Q}^{nf}$. We may assume that these subspaces are each of dimension $nf - 1$. Thus U_k is defined by a nontrivial equation

$$a_{11}^{(k)} x_{11} + \cdots + a_{1f}^{(k)} x_{1f} + \cdots + a_{n1}^{(k)} x_{n1} + \cdots + a_{nf}^{(k)} x_{nf} = 0 \tag{10.12}$$

with coefficients $a_{il}^{(k)}$ in $\mathbb{Q}$. Since each $\mathbf{x}^{(j)}$ is a solution of an equation (10.12) for a suitable k, we see that each vector $\lambda_j \boldsymbol{\beta} = (\lambda_j \beta_1, \ldots, \lambda_j \beta_n)$ satisfies a nontrivial equation with coefficients in K

$$\lambda_j^{(1)}(c_{k11}\beta_1^{(1)} + \cdots + c_{k1n}\beta_n^{(1)}) + \cdots + \lambda_j^{(f)}(c_{kf1}\beta_1^{(f)} + \cdots + c_{kfn}\beta_n^{(f)}) = 0 \tag{10.13}$$

for some k with $1 \leqslant k \leqslant t_6$. Since $h = ft_6$, there exists a k_0 in $1 \leqslant k \leqslant t_6$ for which (10.13) is satisfied for at least f values of j. Suppose for simplicity, that it is satisfied for $j = 1, \ldots, f$. Since $\lambda_1, \ldots, \lambda_f$ are linearly independent over $\mathbb{Q}$, the matrix $(\lambda_i^{(j)})_{1 \leqslant i,j \leqslant f}$ is nonsingular. We have a system and we may infer that

$$c_{k_0 j 1}\beta_1^{(j)} + \cdots + c_{k_0 j n}\beta_n^{(j)} = 0 \quad (j = 1, \ldots, f). \tag{10.14}$$

Since Eq. (10.13) is nontrivial, we see that there exists a $j_0 = j_0(k_0)$ for which (10.14) is a nontrivial equation. (We may choose j_0 minimal with this property and obtain in this way a bijection between Eqs. (10.12) and (10.14).)

Notice that the coefficients $c_{k_0 j_0 1}, \ldots, c_{k_0 j_0 n}$ of our equation lie in the large field K. However, since the intersection of a hyperplane in K^n with $(\sigma_{j_0}(F))^n$ is a proper linear subspace of $(\sigma_{j_0}(F))^n$, we may infer that there exists elements $d_{k_0 1}^{(j_0)}, \ldots, d_{k_0 n}^{(j_0)}$ in $\sigma_{j_0}(F)$ not all zero, that depend only upon $c_{k_0 j_0 1}, \ldots, c_{k_0 j_0 n}$ such that

$$d_{k_0 1}^{(j_0)} \beta_1^{(j_0)} + \cdots + d_{k_0 n}^{(j_0)} \beta_n^{(j_0)} = 0.$$

But this implies that $\boldsymbol{\beta}$ satisfies a nontrivial relation

$$e_{k_0 1}\beta_1 + \cdots + e_{k_0 n}\beta_n = 0 \tag{10.15}$$

with coefficients $e_{k_0 1}, \ldots, e_{k_0 n}$ in F that depend only upon k_0.

We conclude that every solution $\boldsymbol{\beta} \in O_F^n$ of (2.1) that satisfies (10.2) is in fact contained in the union of our subspaces $T_1, \ldots, T_{t_6}$ and Lemma 10.1 follows.

11. Conclusion

The proof of Proposition 2.1 is now easily finished. Lemma 6.1 covers the solutions $\boldsymbol{\beta}$ of (2.1) with small height, whereas Lemma 10.1 deals with the large solutions.

Notice that the constant E in (6.4) is nothing else than t_6 in (10.1). Using this fact it is easily seen that the upper bound in (6.2) for $H(\boldsymbol{\beta})$ by far exceeds the lower bound for $H(\boldsymbol{\beta})$ in (10.2). Thus the two lemmata deal with all solutions $\boldsymbol{\beta}$ of (2.1) having

$$H(\boldsymbol{\beta}) \geqslant \max\{(n!)^{9/\delta}, H^{9nrd/\delta}\}$$

Therefore, the number of subspaces needed does not exceed

$$t_3 + t_6 = 3 \cdot 2^{8n^2 r/\delta} \log t_6 + t_6 \leqslant 2t_6$$

since

$$t_6 = [(8rd)^{2^{26nd} \cdot 8192 r^6 \delta^{-2}}].$$

But

$$2t_6 < [(8rd)^{2^{33nd} r^6 \delta^{-2}}] = t_1,$$

and Proposition 2.1 follows.

References

[1] E. Bombieri and A.J. van der Poorten: Some quantitative results related to Roth's theorem, *J. Austral. Math. Soc.* (series A), 45 (1988), 233–248.

[2] E. Bombieri and J. Vaaler: On Siegel's lemma, *Invent. Math.* 73 (1983), 11–32.

[3] J.W.S. Cassels: An introduction to the geometry of numbers, Springer Grundlehren 99 (1959).

[4] H. Davenport and K.F. Roth: Rational approximation to algebraic numbers, *Mathematika* 2 (1955), 160–167.

[5] H. Luckhardt: Herbrand-Analysen zweier Beweise des Satzes von Roth; polynomiale Anzahlschranken, *J. of Symb. Logic* 54 (1989), 234–263.

[6] K. Mahler: Zur Approximation algebraischer Zahlen I. (Über den größten Primteiler binärer Formen), *Math. Ann.* 107 (1933), 691–730.

[7] K.F. Roth: Rational approximations to algebraic numbers, *Mathematika* 2 (1955), 1–20.

[8] H.P. Schlickewei: On products of special linear forms with algebraic coefficients, *Acta Arith.* 31 (1976), 389–398.

[9] H.P. Schlickewei: The p-adic Thue-Siegel-Roth-Schmidt theorem, *Arch. Math.* 29 (1977), 267–270.

[10] H.P. Schlickewei: The number of subspaces occurring in the p-adic subspace theorem in diophantine approximation, *J. Reine Angew. Math.* 406 (1990), 44–108.

[11] H.P. Schlickewei: An explicit upper bound for the number of solutions of the S-unit equation, *J. Reine Angew. Math.* 406 (1990), 109–120.
[12] H.P. Schlickewei: Linear equations in integers with bounded sum of digits, *J. Number Th.* 35 (1990), 335–344.
[13] W.M. Schmidt: Norm form equations, *Annals of Math.* 96 (1972), 526–551.
[14] W.M. Schmidt: Diophantine approximation, *Springer Lecture Notes in Math.* 785 (1980).
[15] W.M. Schmidt: Simultaneous approximation to algebraic numbers by elements of a number field, *Monatsh. Math.* 79 (1975), 55–66.
[16] W.M. Schmidt: The subspace theorem in diophantine approximations, *Comp. Math.* 69 (1989), 121–173.
[17] W.M. Schmidt: The number of solutions of norm form equations, *Trans. Amer. Math. Soc.* 317 (1990), 197–227.
[18] J.H. Silverman: Lower bounds for height functions, *Duke Math. J.* 51 (1984), 395–403.