

ADDITIVE RELATIONS IN FIELDS

A. J. VAN DER POORTEN and H. P. SCHLICKEWEI

(Received 11 October 1989)

Communicated by J. H. Loxton

Abstract

This paper is the first part of a long delayed revision of the manuscript ‘The growth conditions for recurrence sequences’ (circulated in 1982) in which the authors outlined a proof of the now well known theorem on the finiteness of the number of solutions of S -unit equations. The argument lifting the result from number fields to arbitrary fields of characteristic zero has original features.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 J 25, 11 D 72.

The present paper was conceived in conversation between the authors at an Oberwolfach meeting early last decade. Some of its results were announced at a lecture by one of us at the János Bolyai Number Theory Colloquium in Budapest in 1981 and much of this paper appeared as a locally published preprint in 1982. We allude to subsequent developments both in our principal arguments below and in the second part of this note which deals with basic applications of the main result.

The results below are now mostly well known, with the possible exception of the lifting argument at Section 5–6. On the other hand, our draft report [11] has been extensively quoted and it seems undesirable that it not be put into the public domain proper.

The research of the first author was partially supported by the Australian Research Council.
© 1991 Australian Mathematical Society 0263-6115/91 \$A2.00 + 0.00

1. Introduction

In 1933 Mahler [7] proved that if S_0, S_1, S_2 are disjoint nonempty finite sets of rational primes then an equation

$$z_0 + z_1 + z_2 = 0,$$

where z_i is only divisible by primes in S_i ($i = 0, 1, 2$), has only finitely many solutions $(z_0, z_1, z_2) \in \mathbb{Z}^3$. Independently, Dubois and Rhin [3] and Schlickewei [14] extended this result to equations

$$(1) \quad z_0 + z_1 + \cdots + z_n = 0,$$

($n \geq 2$). In fact they proved a little more: let S_0, \dots, S_n be pairwise disjoint finite sets of rational primes. Let $\varepsilon > 0$ and $c > 0$ be given. Then (1) has only finitely many solutions in rational integers z_i satisfying

$$(2) \quad \prod_{i=1}^n \left(|z_i| \prod_{p \in S_i} |z_i|_p \right) \leq c |z|^{1-\varepsilon},$$

where $|z| = \max\{|z_0|, \dots, |z_n|\}$. In the present paper we apply the p -adic subspace theorem of Schlickewei [15] to extend this result in two ways. First, we eliminate the requirement that the sets be pairwise disjoint by asking for primitive solutions of (1); that is, solutions with their $\gcd(z_0, \dots, z_n) = 1$. Secondly, we generalise the result to algebraic number fields (and, ultimately, to arbitrary fields of characteristic zero).

In that context we must, of course, identify projectively equivalent solutions of (1) in elements z_i of an algebraic number field \mathbb{K} ; that is, if we presume $z_0 \neq 0$, as we may, we identify solutions (z_0, \dots, z_n) and (z'_0, \dots, z'_n) if

$$(z_1/z_0, \dots, z_n/z_0) = (z'_1/z'_0, \dots, z'_n/z'_0).$$

Thus we lose no generality in assuming from the outset that the z_i yielding a solution be elements of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the number field \mathbb{K} .

Let p be a prime of \mathbb{Q} (where p may be the archimedean prime as usual denoted by ∞), and denote by $|\cdot|_p$ the usual normalised absolute value associated with p . Write \mathbb{Q}_p for the completion of \mathbb{Q} with respect to $|\cdot|_p$ (so $\mathbb{R} = \mathbb{Q}_{\infty}$), and denote by $\overline{\mathbb{Q}}_p$ its algebraic closure. Then $|\cdot|_p$ has a unique extension to $\overline{\mathbb{Q}}_p$ which we may continue to denote by $|\cdot|_p$.

Suppose \mathbb{K} has degree r over \mathbb{Q} . Then there are r distinct isomorphic embeddings $\sigma_p : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}_p$. Denote this set by G_p and with $\alpha \in \mathbb{K}$ write α_p^σ for the image of α under the embedding $\sigma_p \in G_p$.

We may define a height for a point of \mathbb{K}^{n+1} just by setting

$$\|\alpha\| = \max_{\sigma} |\alpha_{\infty}^{\sigma}|_{\infty}$$

and then, for $\mathbf{z} = (z_0, z_1, \dots, z_n) \in \mathbb{K}^{n+1}$ writing

$$\|\mathbf{z}\| = \max_{0 \leq i \leq n} \|z_i\|.$$

If so, we can insist on the following normalisation of solutions to (1). A point is said to be *quasi-primitive* if

$$(3) \quad \prod_{p \neq \infty} \prod_{\sigma} \max(|z_{0,p}^{\sigma}|_p, \dots, |z_{n,p}^{\sigma}|_p) \gg 1$$

with some explicit implied constant depending only on the field \mathbb{K} . (If $\mathcal{O}_{\mathbb{K}}$ has class number 1 then in (3) we are just asking for a point with relatively prime co-ordinates. In general it is well-known that any point of $\mathcal{O}_{\mathbb{K}}^{n+1}$ is projectively equivalent to a quasi-primitive point.) Moreover, since we may normalise by a unit of $\mathcal{O}_{\mathbb{K}}$ we may restrict solutions to those that are quasi-primitive and that satisfy

$$(4) \quad \max_{\sigma} (|z_{0,\infty}^{\sigma}|_{\infty}, \dots, |z_{n,\infty}^{\sigma}|_{\infty}) \gg \ll \|\mathbf{z}\|$$

with the implied constants again depending only on \mathbb{K} .

It is equivalent, and may be preferable, to directly acknowledge that we seek to study points of the projective space $\mathbb{P}^n(\mathbb{K})$. Then it is appropriate to define the absolute homogeneous height $H(\mathbf{z})$ of a point $\mathbf{z} \in \mathbb{P}^n(\mathbb{K})$ by setting (recall that $r = [\mathbb{K} : \mathbb{Q}]$)

$$\log H(\mathbf{z}) = r^{-1} \sum_p \sum_{\sigma} \max(\log |z_{0,p}^{\sigma}|_p, \dots, \log |z_{n,p}^{\sigma}|_p).$$

It is the product formula for $\alpha \in \mathbb{K}^{\times}$, namely

$$\sum_p \sum_{\sigma} \log |\alpha_p^{\sigma}|_p = 0,$$

that entails that $H(\mathbf{z})$ is well-defined for a projective point. (Above, the summations are over all places p of \mathbb{Q} , including ∞ , and all embeddings σ of \mathbb{K} into \mathbb{C} .) Furthermore, the normalisation by $r = [\mathbb{K} : \mathbb{Q}]$ guarantees that $H(\mathbf{z})$ does not depend on whether \mathbf{z} is deemed to be defined over \mathbb{K} or over some extension field of \mathbb{K} . The notation automatically incorporates the various normalisations we imposed on \mathbf{z} in the preceding paragraphs, and with \mathbf{z} so normalised we have

$$H(\mathbf{z}) \gg \ll \|\mathbf{z}\|,$$

with the implied constants depending only on \mathbb{K} . (For this remark see, say, [16].) In a context of ineffective results the two notations are essentially interchangeable.

Let \mathcal{N} denote the norm from \mathbb{K} to \mathbb{Q} . Our generalisation of the result quoted at (2) is

THEOREM 1. *Let $\varepsilon > 0$ and $C > 0$ be given, and let S be a finite set of nonarchimedean primes of \mathbb{Q} . Then the equation*

$$z_0 + z_1 + \dots + z_n = 0$$

has only finitely many solutions $\mathbf{z} \in \mathfrak{O}_{\mathbb{K}}^{n+1}$ normalised so as to satisfy (3) and (4) and moreover satisfying the following two conditions:

- (i) *no proper subsum of the z_i vanishes; and*
- (ii)

$$\prod_{i=0}^n \prod_{p \in S \cup \{\infty\}} |\mathcal{N}(z_i)|_p \leq C \|\mathbf{z}\|^{r-\varepsilon}.$$

Alternatively, the cited equation has only finitely many solutions $\mathbf{z} \in \mathbb{P}^n(\mathbb{K})$ satisfying the two conditions (i) and

(ii)' there is a representative of \mathbf{z} such that $(\mathcal{N}(z_0), \mathcal{N}(z_1), \dots, \mathcal{N}(z_n))$ is a vector of S -integers and

$$\prod_{i=0}^n \prod_{p \in S \cup \{\infty\}} |\mathcal{N}(z_i)|_p \leq C(\mathbf{H}(\mathbf{z}))^{r-\varepsilon}.$$

This result was proved independently by Evertse [4]. Indeed, we have chosen to incorporate his refinements in this long-delayed revision of our draft [11]. (Because our primary motive was to produce inequalities for the growth of recurrence sequences it seems we strived to obtain a marginally weaker result by combining various inequalities in the argument in a rather unnatural manner. It would be absurd to duplicate that part of the argument and, indeed, it now seems almost impossible to do so.)

Theorem 1 yields important inequalities for recurrence sequences and more generalised power sums; see subsequent parts of the present note and the applications proved by Evertse [4]. Since wide classes of diophantine problems reduce to equations in a sum of generalised units in a number field, Theorem 1 yields results on generalised integer points on certain varieties; see, for example, Vojta [18]. Moreover we can lift the essential features of Theorem 1 to arbitrary fields of characteristic zero.

THEOREM 2. *Let \mathbf{F} be a field of characteristic zero and let G be a finitely generated subgroup of \mathbf{F}^\times . Let (a_0, a_1, \dots, a_n) be an $(n + 1)$ -tuple of*

nonzero elements of F . Then there are only finitely many projectively distinct relations

$$a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$$

with (u_0, u_1, \dots, u_n) in G^{n+1} and for which no proper subsum of $a_0u_0 + a_1u_1 + \dots + a_nu_n$ vanishes.

2. Preliminaries

The proof of Theorem 1 consists of an application of Schlickewei’s p -adic generalisation [13] of W. M. Schmidt’s Subspace Theorem [17, page 153] and its generalisation to algebraic number fields [17, pages 272–75]. We quote here a version of [13, Theorem 2.1] suitable for our present purposes.

LEMMA 1. Let $\eta > 0$. For each pair (p, σ) , with $p \in S \cup \{\infty\}$ and $\sigma \in G_p$, let

$$L_{1,\sigma,p}, \dots, L_{m,\sigma,p}$$

be m linearly independent linear forms in m variables and with coefficients algebraic over \mathbb{Q} in $\overline{\mathbb{Q}}_p$. For a point $\mathbf{x} = (x_1, \dots, x_m) \in \mathcal{D}_{\mathbb{K}}^m$ denote by \mathbf{x}_p^σ the point $(x_{1,p}^\sigma, \dots, x_{m,p}^\sigma)$. Then there are finitely many proper subspaces $t \subset \mathbb{K}^m$ containing all solutions $\mathbf{x} \in \mathcal{D}_{\mathbb{K}}^m$, $\mathbf{x} \neq 0$, of the inequality

$$(5) \quad \prod_{p \in S \cup \{\infty\}} \prod_{\sigma} \prod_{i=1}^m |L_{i,\sigma,p}(\mathbf{x}_p^\sigma)|_p \leq \|\mathbf{x}\|^{-\eta}.$$

As noted above, we may replace $\|\mathbf{x}\|$ by $H(\mathbf{x})$ in this result.

3. Proof of Theorem 1

We are given

$$(1) \quad z_0 + z_1 + \dots + z_n = 0,$$

with $\mathbf{z} \in \mathbb{P}^n(\mathbb{K})$.

For each pair (p, σ) with $p \in S \cup \{\infty\}$ we then have

$$(6) \quad z_{0,p}^\sigma + z_{1,p}^\sigma + \dots + z_{n,p}^\sigma = 0,$$

and if (I_1, I_2) is a partition of $\{0, 1, \dots, n\}$ then

$$\left| \sum_{i \in I_1} z_{i,p}^\sigma \right|_p = \left| \sum_{i \in I_2} z_{i,p}^\sigma \right|_p,$$

so

$$(7) \quad \max_{i \in I_1} |z_{i,p}^\sigma|_p \gg \left| \sum_{i \in I_2} z_{i,p}^\sigma \right|_p.$$

Setting

$$\mathbf{z}' = (z_1, \dots, z_n) \in \mathbb{K}^n,$$

we define for each pair (p, σ) a set of $n + 1$ linear forms

$$(8) \quad L_{i,\sigma,p}(\mathbf{z}'^\sigma) = z_{i,p}^\sigma \quad (1 \leq i \leq n)$$

and

$$L_{0,\sigma,p}(\mathbf{z}'^\sigma) = - \sum_{i=1}^n L_{i,\sigma,p}(\mathbf{z}'^\sigma).$$

Notice that for each (p, σ) any n of these $n + 1$ linear forms are linearly independent. Further, by (6)

$$(9) \quad L_{0,\sigma,p}(\mathbf{z}'^\sigma) = z_{0,p}^\sigma.$$

By (7) we have

$$(10) \quad \|\mathbf{z}\| \gg \ll \|\mathbf{z}'\|,$$

and we note that for each $p \in S \cup \{\infty\}$,

$$\prod_{\sigma} |L_{i,\sigma,p}(\mathbf{z}'^\sigma)|_p = |\mathcal{N}(z_i)|_p, \quad (0 \leq i \leq n).$$

Consider the product

$$(11) \quad F(\mathbf{z}) = \left(\prod_{p \in S \cup \{\infty\}} \prod_{\sigma} \max_{0 \leq j \leq n} |z_{j,p}^\sigma|_p \right)^{-1} \prod_{p \in S \cup \{\infty\}} \prod_{i=0}^n |\mathcal{N}(z_i)|_p,$$

noting that for each pair (p, σ) it contains a product of n linearly independent forms selected from the $n + 1$ forms (8) and (9). Let $\eta > 0$. Suppose first that every solution $\mathbf{z} \in \mathfrak{D}_{\mathbb{K}}^{n+1}$ satisfying condition (i), but not necessarily condition (ii), of Theorem 1, has

$$(12) \quad F(\mathbf{z}) \gg \|\mathbf{z}'\|^{-\eta}.$$

Then (10) implies that every solution satisfying (3) and (4) has

$$(13) \quad \prod_{i=0}^n \prod_{p \in S \cup \{\infty\}} |\mathcal{N}(z_i)|_p \gg \|\mathbf{z}\|^{r-\eta}.$$

With $\|z\|$ sufficiently large and $\eta < \varepsilon$ this inequality is opposite to that of (ii) of Theorem 1. Hence it suffices to prove (12) for all solutions z satisfying the given conditions, and this we do by induction on n , noting that the case $n = 1$ is trivial since it is implied by the product formula in \mathbb{K} . Accordingly, suppose $n > 1$ and

$$(14) \quad F(z) < \|z'\|^{-\eta}.$$

Lemma 1 applies to the product $F(z)$. For example, if one considers all solutions z such that

$$|z_{i(p, \sigma), p}|_p = \max_{0 \leq j \leq n} |z_{j, p}^\sigma|_p$$

for certain fixed subscripts $i(p, \sigma) \in \{0, 1, \dots, n\}$ with $p \in S \cup \{\infty\}$ and $\sigma \in G_p$, then $F(z)$ can be seen just to be

$$\prod_{p \in S \cup \{\infty\}} \prod_{\sigma} \prod_{i \neq i(p, \sigma)} |L_{i, \sigma, p}(z_p^\sigma)|_p.$$

So there are finitely many proper subspaces T_1, \dots, T_H of \mathbb{K}^n containing all solutions $(z_1, \dots, z_n) \in \mathfrak{D}_{\mathbb{K}}^n$ of (14). Without loss of generality each subspace T_h has codimension 1 and is defined by an equation

$$(15) \quad \gamma_{h1}z_1 + \dots + \gamma_{hn}z_n = 0$$

with the γ_{hi} in $\mathfrak{D}_{\mathbb{K}}$. Fix h for the following remarks. Consider the $\gamma_{hi}z_i$ ($1 \leq i \leq n$) as new variables. Then (15) is of the same shape as (1) but in fewer variables. If some proper subsum of (15) were to vanish we could simplify and deal with yet fewer variables, say with an equation

$$(16) \quad \gamma_m z_m + \dots + \gamma_n z_n = 0,$$

where $1 \leq m \leq n$. Then the sum (16) satisfies condition (i) of the theorem. Because the γ_i are nonzero constants (and $\|z\|$ is ‘sufficiently large’) they do not make an essential contribution to $|\gamma_{i,p}^\sigma z_{i,p}^\sigma|_p$. So the induction hypothesis applied to (16) implies, say,

$$(17) \quad \left(\prod_{p \in S \cup \{\infty\}} \prod_{\sigma} \max_{m \leq j \leq n} |z_{j, p}^\sigma|_p \right)^{-1} \prod_{p \in S \cup \{\infty\}} \prod_{i=m}^n |\mathcal{N}(z_i)|_p \gg \|z\|^{-\eta/3}.$$

With

$$(18) \quad z_m + \dots + z_n = z_{-1},$$

the original equation (1) becomes

$$(19) \quad z_{-1} + \dots + z_{m-1} = 0$$

and again the induction hypothesis yields, from (7), that

$$(20) \quad \left(\prod_{p \in S \cup \{\infty\}} \prod_{\sigma} \max_{0 \leq j < m} |z_{j,p}^{\sigma}|_p \right)^{-1} \prod_{p \in S \cup \{\infty\}} \prod_{i=-1}^{m-1} |\mathcal{N}(z_i)|_p \gg \|z\|^{-\eta/3}.$$

We now combine (17) and (20) with (14) to obtain

$$(21) \quad \left(\prod_{p \in S \cup \{\infty\}} |\mathcal{N}(z_{-1})|_p^{-1} \right) \left\{ \prod_{p \in S \cup \{\infty\}} \prod_{\sigma} \left(\max_{0 \leq i \leq n} |z_{i,p}^{\sigma}|_p \right)^{-1} \right. \\ \left. \times \left(\max_{0 \leq j \leq m-1} |z_{j,p}^{\sigma}|_p \right) \left(\max_{m \leq k \leq n} |z_{k,p}^{\sigma}|_p \right) \right\} \ll \|z\|^{-\eta/3}.$$

But the terms

$$\left(\max_{0 \leq i \leq n} |z_{i,p}^{\sigma}|_p \right)^{-1}$$

cancel with just one of either

$$\left(\max_{0 \leq j \leq m-1} |z_{j,p}^{\sigma}|_p \right) \text{ or } \left(\max_{m \leq k \leq n} |z_{k,p}^{\sigma}|_p \right);$$

and for each pair (p, σ) by (18) and (19),

$$|z_{-1,p}^{\sigma}|_p \ll \min \left(\max_{0 \leq j \leq m-1} |z_{j,p}^{\sigma}|_p, \max_{m \leq k \leq n} |z_{k,p}^{\sigma}|_p \right).$$

Thus in (21) the left hand side is $\gg 1$. Since $\eta > 0$, this yields a contradiction once $\|z\|$ is large relative to the implied constants. This yields Theorem 1. Its alternative formulation is equivalent: it suffices to recall our earlier remarks and to notice that for any nonzero s in \mathbb{K} such that $\mathcal{N}(s)$ is a rational composed solely of the primes of S (thus an S -unit of \mathbb{Q}), one has

$$\prod_{i=0}^n \prod_{p \in S \cup \{\infty\}} |\mathcal{N}(s z_i)|_p = \prod_{i=0}^n \prod_{p \in S \cup \{\infty\}} |\mathcal{N}(z_i)|_p. \quad \square$$

4. Inequalities for sums of generalised units

The following by-product of Theorem 1 is a generalisation of the result that motivated the present work. Indeed, it required a remark by Birch, made to one of us at Budapest, 1981 (apropos the lecture [10]) for us to notice the reformulation that became Theorems 1 and 2.

It is convenient to adopt a more conventional notation than heretofore.

THEOREM 3. *Let \mathbb{K} be a number field and T a finite subset of its places. Denote by S a finite set of primes of \mathbb{Q} including those lying below the nonarchimedean places of T . Let $H(\mathbf{z})$ denote the (absolute homogeneous) height of points $(z_0 : z_1 : \dots : z_n) \in \mathbb{P}^n(\mathbb{K})$. Then, for every $\varepsilon > 0$, the inequality*

$$\prod_{\nu \in T} |z_1 + \dots + z_n|_{\nu} > \left(\prod_{p \in S \cup \{\infty\}} \prod_{i=1}^n |\mathcal{N}(z_i)|_p \right)^{-1} \prod_{\nu \in T} \max_{1 \leq i \leq n} |z_i|_{\nu} H(\mathbf{z})^{-\varepsilon}$$

holds for all but at most finitely many \mathbf{z} in $\mathbb{P}^n(\mathbb{K})$ for which

(i) neither the sum $z_1 + \dots + z_n$ nor any of its proper subsums vanishes; and

(ii) the representative of \mathbf{z} is such that $(\mathcal{N}(z_1), \dots, \mathcal{N}(z_n))$ is a vector of S -integers of \mathbb{Q} .

Note. In practice one selects S so as to validate the second condition.

PROOF. Set $z_0 = -z_1 - z_2 - \dots - z_n$, and denote by T' the places above $S \cup \{\infty\}$ and not in T . Since, of course, (presuming that appropriate normalisations have been selected for the values)

$$\prod_{\nu \in T'} |z_0|_{\nu} \prod_{\nu \in T} |z_0|_{\nu} = \prod_{p \in S \cup \{\infty\}} |\mathcal{N}(z_0)|_p,$$

and, plainly,

$$\prod_{\nu \in T'} |z_0|_{\nu} \left(\prod_{\nu \in T'} \max_{0 \leq j \leq n} |z_j|_{\nu} \right)^{-1} \leq 1,$$

we see on applying (12) that Theorem 3 is entailed by a reformulation of Theorem 1. \square

5. Specialisation

The following discussion is preliminary to deriving Theorem 2 from Theorem 1. Our initial remarks arise from a suggestion of Cassels [2] and constitute the first step in a p -adic embedding argument; a summary of that argument appears in [12]

Let F be a field finitely generated over \mathbb{Q} and let $\mathbf{x} = (x_1, \dots, x_r)$ be a transcendence basis for F over \mathbb{Q} . Then $F = \mathbb{Q}(\mathbf{x})[y]$, with y algebraic over $\mathbb{Q}(\mathbf{x})$. Denote the defining polynomial of y over $\mathbb{Z}[\mathbf{x}]$ by $F[\mathbf{x}](Y)$, and suppose that it is of degree r .

Each element ϕ of the field $F = \mathbb{Q}(\mathbf{x})[y]$ has a representation

$$\phi = U_{\phi}(y; \mathbf{x})/V_{\phi}(\mathbf{x}),$$

with $U_\phi \in \mathbb{Z}[y; \mathbf{x}]$ of degree less than r in y and $V_\phi \in \mathbb{Z}[\mathbf{x}]$. Clearly, we may choose both U_ϕ so that its set of coefficients as a polynomial in y are relatively prime and choose V_ϕ relatively prime to that set of coefficients of U_ϕ and with its set of coefficients relatively prime over \mathbb{Z} . We may then refer to $V_\phi \in \mathbb{Z}[\mathbf{x}]$ as *the denominator of ϕ* .

Cassels' idea is to introduce a suitable finite set Γ of elements of \mathbb{F} with the property that whenever $\gamma \in \Gamma$ and $\gamma \neq 0$ then also $\gamma^{-1} \in \Gamma$. Having chosen Γ , we set

$$V_\Gamma(\mathbf{x}) = \prod_{\gamma \in \Gamma} V_\gamma(\mathbf{x}).$$

It will always be convenient to require that Γ contains the discriminant and the leading and trailing coefficients of $F[\mathbf{x}](Y)$; we assume this implicitly below.

Denote by

$$\mathbf{c} = (c_1, c_2, \dots, c_t)$$

t -tuples of rational integers. It is easy to see, by induction on t , that there are infinitely many such t -tuples \mathbf{c} so that $V_\Gamma(\mathbf{c}) \neq 0$. Whenever $V_\Gamma(\mathbf{c}) \neq 0$, we refer to a map $\mathbf{x} \mapsto \mathbf{c}$, together with an induced map $y = y(\mathbf{x}) \mapsto y(\mathbf{c})$ with $y(\mathbf{c})$ some zero of $F[\mathbf{c}](Y)$, as a Γ -specialisation of \mathbb{F} . (This is an abuse of language; we specialise only the elements of a subring $\mathbb{Q}[\gamma : \gamma \in \Gamma]$.)

Clearly, for $\gamma \in \Gamma$ we have $V_\gamma(\mathbf{c}) \neq 0$. If $\gamma \neq 0$ then $\gamma^{-1} \in \Gamma$, so also $V_{\gamma^{-1}}(\mathbf{c}) \neq 0$.

We allege that if $\gamma = \gamma(y(\mathbf{x}); \mathbf{x}) \in \Gamma$, its Γ -specialisation $\gamma(y(\mathbf{c}); \mathbf{c})$ is an element of an algebraic number field $\mathbb{K} = \mathbb{Q}(\mathbf{c})[y(\mathbf{c})]$ of degree at most r over \mathbb{Q} . But this is clear. Trivially, $\mathbb{Q}(\mathbf{c}) = \mathbb{Q}$ and $y(\mathbf{c})$ is a zero of a polynomial $F[\mathbf{c}](Y)$ of degree r over \mathbb{Q} . Moreover, if $\gamma \neq 0$, the specialisation of γ is nonzero. For, by the definition of Γ , the element γ^{-1} also belongs to Γ and thus also has an image in \mathbb{K} under the specialisation.

Now let R be a subring of \mathbb{F} finitely generated over \mathbb{Z} (thus of *finite type*). We select the finite set Γ as above so that *inter alia* Γ contains the generators of R . Then a Γ -specialisation of \mathbb{F} maps $R \subset \mathbb{F}$ into the number field \mathbb{K} of degree at most r over \mathbb{Q} .

Moreover, by augmenting the set Γ controlling the admissible specialisations, we may arrange that a given element of R does not map to a root of unity. To see this, suppose $\rho \in R$ is not a root of unity in \mathbb{F} . Thus $\rho^k - 1$ is nonzero for all $k = 1, 2, \dots$. We recall that a root of unity in a number field of degree r over \mathbb{Q} has order at most r' , where $\phi(r') \leq r$. Noting only that $\phi(r') \rightarrow \infty$ as $r' \rightarrow \infty$ (in fact r' is of order $r \log \log r$) we see that r' is bounded in terms of r . Then, augmenting Γ with the finitely many nonzero elements $\rho^k - 1$ ($k = 1, \dots, r'$), to obtain a new controlling set

Γ' , guarantees that those elements are not sent to zero by a Γ' -specialisation and entails that ρ is not specialised to a root of unity.

6. Proof of Theorem 2

Fix an $(n + 1)$ -tuple (a_0, a_1, \dots, a_n) of nonzero elements of \mathbf{F} and suppose that, throughout the sequel, $(n + 1)$ -tuples \mathbf{u} and \mathbf{u}' belong to G^{n+1} , with G a given finitely generated multiplicative subgroup of \mathbf{F}^\times , and satisfy

$$a_0u_0 + a_1u_1 + \dots + a_nu_n = 0 \quad \text{and} \quad a_0u'_0 + a_1u'_1 + \dots + a_nu'_n = 0.$$

6.1 Weak equivalence. Each relation $a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$ is associated with one or more partitions $\mathcal{T} = (T_0, T_1, \dots, T_m)$ of $\{0, 1, \dots, n\}$ according as, for each j , $\sum_{i \in T_j} a_iu_i = 0$, but, for any proper subset T of T_j , $\sum_{i \in T} a_iu_i \neq 0$.

Suppose $a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$ and $a_0u'_0 + a_1u'_1 + \dots + a_nu'_n = 0$ have associated partitions \mathcal{T} and \mathcal{T}' respectively. Then we say that the pairs $(\mathbf{u}, \mathcal{T})$ and $(\mathbf{u}', \mathcal{T}')$ are *weakly equivalent*, and write $(\mathbf{u}, \mathcal{T}) \sim (\mathbf{u}', \mathcal{T}')$ if $\mathcal{T} = \mathcal{T}'$ and, for each $T_j \in \mathcal{T}$, there is an element v_j of G such that $u'_i = v_ju_i$ for each $i \in T_j$.

We are forced to define the equivalence relation on pairs (u, \mathcal{T}) in order to ensure the transitivity of the relation. To see this, say that a relation is *primitive* if its associated partition \mathcal{T} is trivial, that is, if $\mathcal{T} = (\{0, 1, \dots, n\})$. Now notice that imprimitive relations may arise from shorter primitive relations in a variety of ways.

Conversely, given a partition $\mathcal{T} = (T_0, T_1, \dots, T_m)$ fix maps $T_j \rightarrow T_j : i \mapsto j(i)$ constant on the subsets T_j of $\{0, 1, \dots, n\}$. Then triples, consisting of pairs of $(n + 1)$ -tuples \mathbf{u} and \mathbf{u}' in G^{n+1} and a partition \mathcal{T} , determine $n + 1$ elements τ_i of G by

$$\tau_i(\mathbf{u}, \mathbf{u}', \mathcal{T}) = u_iu'_{j(i)}u_i^{-1}u_{j(i)}^{-1} \quad (i = 0, 1, \dots, n).$$

Plainly, if $a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$ and $a_0u'_0 + a_1u'_1 + \dots + a_nu'_n = 0$ have the same associated partition \mathcal{T} , then

$$(\mathbf{u}, \mathcal{T}) \sim (\mathbf{u}', \mathcal{T}) \Leftrightarrow \tau_i(\mathbf{u}, \mathbf{u}', \mathcal{T}) = 1 \quad \text{for all } i \text{ in } \{0, 1, \dots, n\}.$$

6.2 Admissible specialisations. We describe a specialisation of \mathbf{F} as *admissible* if the finite set Γ , defining the subring of \mathbf{F} actually specialised, contains the given coefficients a_0, \dots, a_n and a generating set of the multiplicative subgroup G .

Let f be an admissible specialisation f of \mathbf{F} controlled by the finite subset Γ of \mathbf{F} . Now f restricted to G , $f|_G$, is a group homomorphism $G \rightarrow f(G)$, with $f(G)$ a finitely generated subgroup of some number field \mathbb{K} of degree at most r over \mathbb{Q} . Let K denote the torsion-hull of the kernel of this map, that is, those elements of G sent to a root of unity in \mathbb{K} . We shall show that there we may choose f so that it preserves the multiplicative independence of multiplicatively independent elements, and thus so that K is just the torsion subgroup of G .

LEMMA 2. *Let g_1, g_2, \dots, g_s be multiplicatively independent elements of G . Then there is an admissible specialisation f of \mathbf{F} so that $f(g_1), f(g_2), \dots, f(g_s)$ are multiplicatively independent elements of a number field of degree at most r over \mathbb{Q} .*

PROOF. Given H sufficiently large relative to the data, consider the specialisations of \mathbf{F} induced by $\mathbf{x} \mapsto \mathbf{c} = (c_1, \dots, c_t)$, with each rational integer c_i satisfying $|c_i| < H$. Select an admissible such specialisation (there are $O(H^t)$ such) and denote the image of g_j by \bar{g}_j ; the \bar{g}_j will be elements of some number field \mathbb{K} of degree r over \mathbb{Q} . We have $\log H(\bar{g}_j) \ll \log H$, with the implied constant depending only on the data and not on the selected specialisation. By a result of Loxton and van der Poorten [6] if the \bar{g}_j are multiplicatively dependent then there is a multiplicative relation

$$\bar{g}_1^{a_1} \dots \bar{g}_s^{a_s} = 1,$$

in integers a_j , not all zero, with the $|a_j| \ll (\log H)^{s-1}$. Accordingly, we augment the controlling set with the elements

$$g_1^{b_1} \dots g_s^{b_s} - 1 \text{ for all integer vectors } \mathbf{b} \text{ with } |b_j| \ll (\log H)^{s-1},$$

and obtain a new controlling set Γ , say. The construction prevents the g_j from specialising to multiplicatively dependent elements under any Γ -specialisation induced by $\mathbf{x} \mapsto \mathbf{c}$ with each c_i satisfying $|c_i| < H$. Only $\ll H^{t-1}(\log H)^{s^2-1}$ of the original $O(H^t)$ specialisations induced by $\mathbf{x} \mapsto \mathbf{c}$ fail to yield an admissible specialisation with respect to Γ . So if H is large enough relative to the data this leaves a plentitude of specialisations to spare.

6.3 Strong equivalence. Let f be a specialisation, selected according to the lemma and fixed from hereon. Set $f(u_i) = w_i$ ($i = 0, 1, \dots, n$). On applying f to the relation

$$a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$$

we obtain a relation

$$f(a_0)w_0 + f(a_1)w_1 + \dots + f(a_n)w_n = 0$$

in some number field \mathbb{K} of degree at most r over \mathbb{Q} . Let \mathcal{T}_f be a partition associated with this relation.

Similarly, the relation

$$a_0u'_0 + a_1u'_1 + \dots + a_nu'_n = 0$$

specialises to

$$f(a_0)w'_0 + f(a_1)w'_1 + \dots + f(a_n)w'_n = 0$$

in \mathbb{K} , say with an associated partition \mathcal{T}'_f .

Once each relation $a_0w_0 + a_1w_1 + \dots + a_nw_n = 0$ is associated with some partition once for all, we may say that \mathbf{u} and \mathbf{u}' are strongly equivalent—relative to the given specialisation and the choice of associated partitions, and write $\mathbf{u} \approx \mathbf{u}'$, if

$$(\mathbf{w}, \mathcal{T}_f) \sim (\mathbf{w}', \mathcal{T}'_f).$$

Since weak equivalence is an equivalence relation on the pairs $(\mathbf{u}, \mathcal{T})$ it readily follows that strong equivalence is an equivalence relation on the \mathbf{u} .

6.4 Counting equivalence classes. In Theorem 1 we deal with primitive relations over number fields and *inter alia* prove that, given the $(n + 1)$ -tuple $(f(a_0), \dots, f(a_n))$ and a finitely generated subgroup $f(G) \in \mathbb{K}^\times$, there are just finitely many weak equivalence classes of pairs $(\mathbf{w}, \{0, 1, \dots, n\})$ over a number field \mathbb{K} . *A fortiori*, the same holds for weak equivalence classes arising from given relations of length shorter than n . Because there are just a finite number of partitions of $\{0, 1, \dots, n\}$, it follows readily that a given $(f(a_0), \dots, f(a_n))$ and a finitely generated subgroup $f(G) \in \mathbb{K}^\times$ yield only finitely many weak equivalence classes $(\mathbf{w}, \mathcal{T}_f)$ in a number field \mathbb{K} .

Thus there are only finitely many strong equivalence classes of $(n + 1)$ -tuples $\mathbf{u} \in G^{n+1}$ with $a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$.

Hence, to prove Theorem 2, it suffices to show that each strong equivalence class comprises only finitely many weak equivalence classes.

6.5 The inductive step. Suppose that $u \approx u'$. Then, by the choice of the specialisation f ,

$$f(\tau_i(\mathbf{u}, \mathbf{u}', \mathcal{T}_f)) = 1$$

entails that

$$\tau_i(\mathbf{u}, \mathbf{u}', \mathcal{T}_f) = 1 \quad \text{for } i = 0, 1, \dots, n.$$

Hence there is an $(m + 1)$ -tuple (v_0, v_1, \dots, v_m) of elements of G so that

$$u'_i = v_j u_i \quad \text{for each } i \in T_j \text{ and each } T_j \in \mathcal{T}_f.$$

Thus, with $b_j = \sum_{i \in T_j} a_i u_i$ for $j = 0, 1, \dots, m$, there is an $(m + 1)$ -tuple

(v_0, v_1, \dots, v_m) in G^{m+1} satisfying the relation

$$b_0v_0 + b_1v_1 + \dots + b_mv_m = 0.$$

The point is that $m < n$, so this new relation is shorter than the ones with which we began. We therefore assume that each of the b_j is nonzero. In the contrary case, we have a relation

$$b_j = \sum_{i \in T_j} a_i u_i = 0$$

with $|T_j| < n$, and we work with it as a new shorter relation in the argument below.

We remark, in passing, that if $a_0u_0 + a_1u_1 + \dots + a_nu_n = 0$ is a primitive relation then, both, none of the b_j can vanish and the new relation itself is primitive.

6.6 The main argument. Theorem 2 is obvious for $n = 1$ and, as induction assumption, we may have assumed its truth for relations on fewer than $n + 1$ summands. In particular we may take as further induction assumption that, when $m < n$, a given $(m + 1)$ -tuple (b_0, b_1, \dots, b_m) of nonzero elements of F yields only finitely many weak equivalence classes of pairs $(\mathbf{v}, \mathcal{T})$ of $(m + 1)$ -tuples $\mathbf{v} \in G^{m+1}$ satisfying the relation $b_0v_0 + b_1v_1 + \dots + b_mv_m = 0$ with associated partition \mathcal{T} of $\{0, 1, \dots, m\}$.

We have shown that each \mathbf{u}' strongly equivalent to \mathbf{u} either yields an $(m + 1)$ -tuple $\mathbf{v} \in G^{m+1}$ satisfying the relation $b_0v_0 + b_1v_1 + \dots + b_mv_m = 0$ with the b_j nonzero, or $\sum_{i \in T_j} a_i u_i = 0$, some j .

In the former case there are just finitely many weak equivalence classes $(\mathbf{v}, \mathcal{T})$ by the induction assumption; so the \mathbf{u}' arise from only finitely many weak equivalence classes. That makes plain that each strong equivalence class comprises only finitely many weak equivalence classes, completing the proof. In the latter case, we have a shorter relation on the u_i to begin with and, again, induction completes our argument.

6.7 Remarks. The principal argument is an *in extenso* rendition of the argument which appears as a 'one line' remark in our original manuscript [11]; Evertse (in a conversation with one of us at Leiden in 1982) pointed out that a few more words might well be needed. Robert Rumely (ARGS visiting fellow at Macquarie University in 1985) suggested the notions of weak and strong equivalence. Lemma 2, for which we originally had rather more dubious arguments, is implicit in work of Masser [9] (and independently came to the attention of each of us during 1985).

6.8 The referee’s suggestion. Actually, it suffices to prove the following result:

THEOREM 2’. *Let \mathbf{F} be a field of characteristic zero and let c_1, c_2, \dots, c_n be nonzero elements of \mathbf{F} . Denote by G_1, G_2, \dots, G_n finitely generated subgroups of \mathbf{F}^\times . Then the equation*

$$(22) \quad c_1u_1 + c_2u_2 + \dots + c_nu_n = 1$$

has only finitely many solutions in elements $u_i \in G_i$ ($1 \leq i \leq n$) for which no proper subsum of $c_1u_1 + c_2u_2 + \dots + c_nu_n$ vanishes.

PROOF. We refer to a solution $\mathbf{u} = (u_1, u_2, \dots, u_n)$ of (22) as *admissible* if it satisfies the conditions of the theorem. We proceed by induction on $M = \sum_{i=1}^n \text{rank } G_i$, where the rank of an abelian group is defined as the rank of its torsion-free part. Our induction assumption is the truth of the theorem if the sum of the ranks is less than M . If $M = 0$ then the groups G_i are finite and there is nothing to prove. Nor is it any restriction to suppose that each G_i has rank at least 1, for otherwise (22) is readily transformed into finitely many similar equations involving fewer than n summands, and we prove each of these to have only finitely many admissible solutions.

Accordingly we may select, for each i , a $g_i \in G_i$ not a root of unity. Next, as described in Section 5, we construct a finite set Γ so that specialisations f controlled by Γ have the property that no element of the groups G_i is sent to zero, that the $f(c_i)$ are nonzero and none of the $f(g_i)$ are a root of unity. Furthermore, the $f(c_i)$ and the multiplicative subgroups $f(G_i)$ are contained in some number field \mathbb{K} . Set

$$H_i = \{g \in G_i : f(g) \text{ is a root of unity}\} \quad (1 \leq i \leq n).$$

Then for each i we have $\text{rank } H_i < \text{rank } G_i$. To see this, notice that if $\text{rank } H_i = \text{rank } G_i$ then H_i has finite index, say m , in G_i whence $g^m \in H_i$ for every $g \in G_i$. But that is a contradiction because, by the construction, $f(g_i)$ is not a root of unity.

Then a solution \mathbf{u} of (22) yields a solution $f(\mathbf{u}) = \mathbf{w} = (w_1, w_2, \dots, w_n)$ of

$$f(c_1)w_1 + f(c_2)w_2 + \dots + f(c_n)w_n = 1$$

with $w_i \in f(G_i)$ for $1 \leq i \leq n$; and there is a subset $I \subseteq \{1, 2, \dots, n\}$ such that $\sum_{i \in I} f(c_i)w_i = 1$ and $\sum_{i \in K} f(c_i)w_i \neq 0$ for $\emptyset \neq K \subsetneq I$.

By Theorem 1 there is a finite subset \mathcal{S} of \mathbb{K} , depending only on the $f(a_i)$, the $f(G_i)$ and n (and thence only on the a_i , the G_i and n) such that each $w_i \in \mathcal{S}$. This is to say, for each solution \mathbf{u} of (22) and each $i \in \{1, 2, \dots, n\}$, there is an $s \in \mathcal{S}$ such that $f(u_i) = s$.

We take $i = n$ and complete the inductive step by showing that (22) has only finitely many admissible solutions \mathbf{u} with $f(u_n) = s$. Indeed, let \mathbf{u} and \mathbf{v} be solutions with $f(u_n) = s$ and $f(v_n) = s$ respectively. Then $f(u_n/v_n) = 1$, so $u_n/v_n \in H_n$. Thus, on writing $c'_n = c_n v_n$ and $u'_n = u_n/v_n$, we have

$$(23) \quad c_1 u_1 + c_2 u_2 + \dots + c'_n u'_n = 1$$

with $u_i \in G_i$ for $i = 1, 2, \dots, n-1$ and $u'_n \in H_n$, whilst each proper subsum on the left is nonzero.

But, according to the induction hypothesis, (23) has only finitely many admissible solutions $(u_1, u_2, \dots, u_{n-1}, u'_n)$, so (22) has only finitely many admissible solutions \mathbf{u} with $f(u_n) = s$.

We are grateful to the referee for allowing us to incorporate this argument in the present manuscript.

7. Generalisations to function fields

There are now other generalisations of Theorem 1. Denote by \mathbf{L} an arbitrary field of characteristic zero and let \mathbf{F} be a function field over \mathbf{L} of genus g . Then, sharpening results of Mason [8], Brownawell and Masser [1] show that every solution \mathbf{u} in $\mathbb{P}^n(\mathbf{F})$ of

$$u_0 + u_1 + \dots + u_n = 0,$$

such that no proper subset of the u_i is linearly dependent over \mathbf{L} , has projective height bounded explicitly in terms of g and the numbers $m(v)$ of elements amongst the u_i which are units at the respective values v of \mathbf{F} . A relevant corollary is that if the u_i all are S -units for some finite set S of values, with S of cardinality $|S|$, then the height of a solution is bounded by

$$\frac{1}{2}n(n-1)(|S| + 2g - 2).$$

This result is skew to those above in that it neither includes nor is included in ours. Nonetheless, it seems clear that on taking the base field of finite transcendence degree over \mathbb{Q} , and using Theorem 1 as the base of an induction on both the transcendence degree t of \mathbf{F} over \mathbb{Q} and on n , one may derive Theorem 2 by an argument which Masser has described as “... ‘specialising’, except that one does not actually need to specialise at all” (conversation with one of us at IAS, Princeton, 1986). The task has recently been carried out by Evertse and Györy [5, Appendix], and is indeed quite straightforward as predicted.

References

- [1] W. D. Brownawell and D. W. Masser, 'Vanishing sums in function fields', *Math. Proc. Cambridge Phil. Soc.* **100** (1986), 427–434.
- [2] J. W. S. Cassels, 'An embedding theorem for fields', *Bull. Austral. Math. Soc.* **14** (1976) 193–198; Addendum, *ibid.* **14** (1976) 479–480.
- [3] E. Dubois and G. Rhin, 'Sur la majoration de formes linéaires à coefficients algébriques réels et p -adiques (Démonstration d'une conjecture de K. Mahler)', *C. R. Acad. Sci. Paris A282* (1976), 1211.
- [4] Jan-Hendrik Evertse, 'On sums of S -units and linear recurrences', *Compositio Math.* **53** (1984), 225–244.
- [5] J.-H. Evertse and K. Györy, 'On the number of solutions of weighted unit equations', *Compositio Math.* **66** (1988), 329–354.
- [6] J. H. Loxton and A. J. van der Poorten, 'Multiplicative dependence in number fields', *Acta Arith.* **42** (1983), 291–302.
- [7] K. Mahler, 'Zur Approximation algebraischer Zahlen I (Über den größten Primteiler binärer Formen)', *Math. Ann.* **107** (1933), 691–730.
- [8] R. C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Notes 96, Cambridge University Press (1984).
- [9] D. W. Masser, 'Linear relations on algebraic groups' in Alan Baker, (Ed.), *New Advances in Transcendence Theory*, Cambridge University Press (1988), 248–262.
- [10] A. J. van der Poorten, 'Some problems of recurrent interest', *Colloq. Math. Soc. János Bolyai* (Budapest, 1981) **34**, *Topics in Number Theory*, North-Holland (1984), 1265–1294.
- [11] A. J. van der Poorten and H. P. Schlickewei, 'The growth conditions for recurrence sequences', *Macquarie Math. Reports* 82-0041 (August, 1982), Macquarie University, Australia 2109.
- [12] A. J. van der Poorten, 'Some facts that should be better known; especially about rational functions', in R. A. Mollin (Ed.), *Number Theory and Applications*, (NATO–Advanced Study Institute, Banff 1988), Kluwer Academic Publishers, Dordrecht (1989), 497–528.
- [13] H. P. Schlickewei, 'Linearformen mit algebraischen Koeffizienten', *Manuscripta Math.* **18** (1976), 147–185.
- [14] H. P. Schlickewei, 'Über die diophantische Gleichung $x_1 + x_2 + \dots + x_n = 0$ ', *Acta Arith.* **33** (1977), 183–185.
- [15] H. P. Schlickewei, 'The p -adic Thue-Siegel-Roth-Schmidt theorem', *Arch. Mat.* **29** (1977), 267–270.
- [16] W. M. Schmidt, 'Simultaneous approximation to algebraic numbers by elements of a number field', *Monatsh. Math.* **79** (1975), 55–66.
- [17] W. M. Schmidt, *Diophantine approximation*, Lecture Notes in Math. 785, Springer-Verlag (1980).
- [18] P. A. Vojta, *Integral points on varieties*, PhD Thesis, Harvard University (1983).

School of Mathematics, Physics,
Computing and Electronics
Macquarie University, NSW 2109
Australia

Abteilung für Mathematik
Universität Ulm
Oberer Eselsberg, Postfach 4066
D-7900 Ulm
Germany