10

DECOMPOSABLE FORM EQUATIONS

J.-H. Evertse and K. Győry[1]

Let $F(\underline{x}) = F(x_1, \ldots, x_m)$ be a form (homogeneous polynomial) in $m \geq 2$ variables with coefficients in $\mathbb{Z}$. Suppose that F is *decomposable* (that is that F factorizes into linear factors over the field $\overline{\mathbb{Q}}$ of algebraic numbers). For $m = 2$ every form is decomposable, but for $m > 2$ this is not always the case. Let $b \in \mathbb{Z} \setminus \{0\}$ and consider the *decomposable form equation*

$$F(\underline{x}) = F(x_1, \ldots, x_m) = b \tag{1}$$

in $\underline{x} = (x_1, \ldots, x_m) \in R^m$ where R is a subring of $\mathbb{Q}$ finitely generated over $\mathbb{Z}$. Equations of this type are of basic importance in the theory of Diophantine equations and have many applications to algebraic number theory. Important classes of such equations are *Thue equations*, when $m = 2$, *norm form equations*, *discriminant form equations* and *index form equations*. In the last twenty years much progress has been made in the study of decomposable form equations. By means of the Thue-Siegel-Roth-Schmidt method general finiteness criteria have been established which guarantee, under the most general conditions possible for F and R, the finiteness of the numbers of solutions for every b. These criteria do not provide, however, any procedure to solve the equations in question or decide the solvability and hence are *ineffective*. *Effective* finiteness theorems have been obtained for a restricted class of decomposable form equations, including Thue equations, discriminant form equations, index form equations and a class of norm form equations. By using Baker's method concerning linear forms in logarithms of algebraic numbers, explicit upper bounds have been derived for the absolute values (heights) of the solutions. These bounds make it possible, at least in principle, to determine all solutions. Finally, for the restricted class of decomposable form equations mentioned above, explicit upper bounds have been given for the numbers of solutions which are independent of the coefficients of the decomposable forms involved. The most important theorems have

[1] Research supported in part by the Hungarian National Foundation for Scientific Research, grant 273

been generalized to the case that the ground ring (cf. §1) is an arbitrary finitely generated integral domain over $\mathbf{Z}$, and analogous results have been established over function fields. It turns out that the theory of decomposable form equations is in fact equivalent to the theory of unit equations (see [15], and [16] in this volume) and this close connection has proved very useful for decomposable form equations. The most general ineffective and effective finiteness results concerning decomposable form equations have been obtained via unit equations.

In §1, we shall give a historical survey on the advances in the study of decomposable form equations and their applications. We shall state results only over finitely generated subrings of $\mathbf{Q}$ and indicate extensions to the case of more general ground rings finitely generated over $\mathbf{Z}$. Results over function fields will be discussed in Mason's paper in this volume. For the methods which have been used, related results, further applications and references we refer to [62], [10], [7], [4], [56], [28], [33], [67], [44], [58], [16].

In §2, two new results, Theorems 1′ and 2′, will be presented. Theorem 1′ is an effective finiteness result for a wide class of decomposable form equations over finitely generated subrings of algebraic number fields. Theorem 2′ provides, for the same class of equations, an explicit upper bound for the numbers of solutions which is independent of the coefficients of the decomposable forms involved. Theorems 1′ and 2′ are extensions of the previous results to a slightly larger class of equations. The proofs of Theorems 1′ and 2′ are given in §3.

§1. Historical Survey

In this section, we first give a brief survey of results obtained for decomposable form equations in two unknowns (Thue equations), and then discuss to what extent these results have been generalized to norm form equations, discriminant form and index form equations and in general to decomposable form equations in more than two unknowns. In the sequel, $C_1, C_2, \ldots$ will denote effectively computable positive numbers which depend only on appropriate parameters of the equations under consideration. Unless otherwise stated, explicit expressions for these numbers have been given in the papers to which we shall refer.

Thue equations

Consider the equation

$$F(x_1, x_2) = b \tag{2}$$

in $x_1, x_2 \in \mathbf{Z}$ where $F \in \mathbf{Z}[X_1, X_2]$ is a binary form and $b \in \mathbf{Z} \setminus \{0\}$. If $n = \deg(F) \leq 2$, (2) may have infinitely many solutions and all these can be described. In 1909 Thue [70] proved the following.

Theorem A (Thue [70]). *If $F \in \mathbf{Z}[X_1, X_2]$ is an irreducible binary form of degree $n \geq 3$ then (2) has only finitely many solutions in $x_1, x_2 \in \mathbf{Z}$.*

After Thue, equations of this type are named *Thue equations*. It is easy to see that in Thue's theorem the "irreducibility" condition can be replaced by the weaker assumption that F is not a constant multiple of a linear form or of an irreducible quadratic form with positive discriminant.

Thue deduced his finiteness result from his approximation theorem. Theorem A was later improved and generalized by several authors. Siegel [60] gave a general finiteness criterion for polynomial Diophantine equations in two unknowns. In 1933, Mahler [46] extended Thue's theorem to the equation

$$F(x_1, x_2) = b p_1^{z_1} \dots p_s^{z_s} \text{ in } x_1, x_2, z_1 \dots, z_s \in \mathbf{Z} \text{ with } (x_1, x_2) = 1 \tag{3}$$

where $p_1, \dots, p_s$ $(s \geq 0)$ are distinct primes.

Theorem B (Mahler [46]). *Let $F \in \mathbf{Z}[X_1, X_2]$ be a binary form having at least three pairwise linearly independent linear factors in its factorization over $\overline{\mathbf{Q}}$. Then equation (3) has only finitely many solutions.*

Equations of the type (3) are called *Thue-Mahler equations*. An equivalent formulation of Mahler's theorem is that equation (2) has only finitely many solutions x_1, x_2 in the ring $\mathbf{Z}\left[\frac{1}{p_1}, \dots, \frac{1}{p_s}\right]$. Since every subring of $\mathbf{Q}$ which is finitely generated over $\mathbf{Z}$ can be written in this form (with finitely many appropriate primes), Mahler's result implies that (2) has finitely many solutions in every finitely generated subring of $\mathbf{Q}$. We note that these results of Mahler do not remain valid in general if F has at most two pairwise linearly independent linear factors over $\overline{\mathbf{Q}}$.

Siegel [59], [60], Parry [48] extended the above-mentioned results of Thue and Mahler, respectively, to the so-called *relative case* when the ground ring (that is, the ring containing b, the coefficients of F and the values assumed by the unknowns) is the ring of integers of an arbitrary algebraic number field. Finally, Lang [44] gave a further generalization

to the case of arbitrary finitely generated ground rings over $\mathbf{Z}$. By a recent result of Faltings [17] (see also [18]), even the number of "rational" solutions is finite, provided the degree $n \geq 4$. All these results are, however, *ineffective*, that is, their proofs do not provide an algorithm for deciding the solvability or determining the solutions.

The first general *effective* result on the Thue equations was proved by Baker [1] in 1968. By using his fundamental effective inequalities concerning linear forms in the logarithms of algebraic numbers, he showed the following.

Theorem C (Baker [1]). *If $F \in \mathbf{Z}[X_1, X_2]$ is an irreducible binary form of degree $n \geq 3$ then all solutions $x_1, x_2 \in \mathbf{Z}$ of (2) satisfy*

$$\max(|x_1|, |x_2|) < \exp\{n^{v^2} H^{vn^3} + (\log |b|)^{2n+2}\}$$

where $v = 128n(n+1)$ and H denotes the maximum absolute value of the coefficients of F.

This made it possible, at least in principle, to solve Thue's equations. Baker's estimate was later improved by Feldman [19], Sprindžuk [65], Stark [68], Baker [3] and others. The best known upper bound, due to Győry and Papp [37] is of the form

$$\max(|x_1|, |x_2|) < (H \cdot |b|)^{(C_1 n)^{C_2 n} (R_K \log R_K^*)^2},$$

where C_1 and C_2 are effectively computable positive absolute constants, R_K is the regulator of the field K generated by a root of $F(X, 1) = 0$ and $R_K^* = \max(R_K, 3)$. The above bounds led to effective improvements of Liouville's approximation theorem (cf. [1], [19], [37]).

By proving and using a p-adic analogue of Baker's inequality concerning linear forms in logarithms, Coates [8], [9] made effective Mahler's theorem for irreducible binary forms F. Coates' estimate for the solutions was improved and generalized by Sprindžuk [63], [64], [66] and Shorey, van der Poorten, Tijdeman and Schinzel [57]. In [57] the authors gave an effective version of Mahler's theorem in full generality. The results of Baker, Coates and Shorey, van der Poorten, Tijdeman and Schinzel were later extended to the relative case by Baker [2], Kotov [39] and Győry [24], [26], respectively. Further extensions to the case of arbitrary finitely generated ground rings over $\mathbf{Z}$ were recently obtained by Győry [31], [33].

Several authors derived upper bounds for the numbers of solutions of the Thue and Thue-Mahler equations; for references see e.g. [11], [12].

In 1983, Evertse [11], [12] was the first to obtain (without any additional restriction concerning F or b) bounds for the numbers of solutions of (2) and (3) which are independent of the coefficients F. Let $\omega(b)$ denote the number of distinct prime factors of b.

Theorem D (Evertse [12]). *Under the assumption of Theorem B, equation* (3) *has at most*

$$2 \times 7^{n^3(2s+2\omega(b)+3)}$$

solutions.

Evertse [12] proved his theorem in a more general form, in the relative case, by using a modification of a method of Thue and Siegel. For further generalizations to equations over arbitrary finitely generated domains over $\mathbf{Z}$ see Evertse and Győry [14].

It follows from Theorem D that (2) has at most $2 \times 7^{n^3(2s+2\omega(b)+3)}$ solutions x_1, x_2 in the ring $\mathbf{Z}[\frac{1}{p_1}, \ldots, \frac{1}{p_s}]$. By restricting themselves to solutions x_1, x_2 in $\mathbf{Z}$ with $(x_1, x_2) = 1$, Bombieri and Schmidt [6] have recently improved this upper bound to $C_3 \times n^{\omega(b)+1}$, where C_3 is an absolute constant (which was not explicitly computed but smaller than 215 for n sufficiently large). For further recent related results we refer to the paper of Schmidt in this volume.

Norm form equations

Let K be an algebraic number field of degree $n \geq 2$ with $\mathbf{Q}$-isomorphisms $\sigma_1, \ldots, \sigma_n$ in $\mathbf{C}$. Put $\alpha^{(i)} = \sigma_i(\alpha)$ for any $\alpha \in K$. Let $\alpha_1 = 1$, $\alpha_2, \ldots \alpha_m$, $m \geq 2$, be linearly independent elements of K over $\mathbf{Q}$, (i.e. $m \leq n$) and suppose, for simplicity, that $K = \mathbf{Q}(\alpha_1, \ldots, \alpha_m)$. Put

$$L^{(i)}(\underline{X}) = \alpha_1^{(i)} X_1 + \ldots + \alpha_m^{(i)} X_m \qquad \text{for } i = 1, \ldots, n. \tag{4}$$

Then

$$N(\underline{X}) = N(\alpha_1 X_1 + \ldots + \alpha_m X_m) = \prod_{i=1}^{n} L^{(i)}(\underline{X})$$

is a decomposable form with coefficients in $\mathbf{Q}$ which is called a *norm form*. In what follows, let[1] $b \in \mathbf{Q}^*$. An equation of the type

$$N(\underline{x}) = b \tag{5}$$

[1] K^* will denote the set of non-zero elements of a field K. In general, for any integral domain R, R^+ and R^* will denote the additive group and the unit group (that is, the multiplicative group of invertible elements of R).

in $\underline{x} \in \mathbf{Z}^m$ is called *norm form equation* (over $\mathbf{Z}$). If in particular $m = 2$ and $n \geq 3$, then (5) is just a Thue equation.

For $m = n$, (5) is a generalization of the Pell-equation and then (5) can be completely solved (cf. [7]). For $m < n$, the problem is much more difficult. Let V denote the $\mathbf{Q}$-vector space generated by $\alpha_1, \ldots, \alpha_m$. By means of his powerful subspace theorem Schmidt [53] proved in 1971 the following general finiteness criterion.

Theorem E (Schmidt [53]). *The following two statements are equivalent:*

(i) *V has no subspace of the form $\mu K'$ where $\mu \in K^*$ and K' is a subfield of K different from $\mathbf{Q}$ and the imaginary quadratic fields;*

(ii) (5) *has finitely many solutions $\underline{x}$ in $\mathbf{Z}^m$ for all $b \in \mathbf{Q}^*$.*

For $m = 2$, Schmidt's theorem reduces to Thue's theorem. Later Schmidt [54] proved a more general theorem by showing that all solutions of an arbitrary norm form equation over $\mathbf{Z}$ belong to finitely many so-called families of solutions. In 1977, Schlickewei [51] generalized certain weaker versions of the results of Mahler and Schmidt. His results imply that if V has no subspace of the form $\mu K'$ with $\mu \in K^*$ and a subfield K' of K such that $K' \neq \mathbf{Q}$ then (5) has only finitely many solutions in every finitely generated subring of $\mathbf{Q}$. A further generalization has been recently obtained by Laurent [45] to the case when the ground ring is an arbitrary finitely generated integral domain over $\mathbf{Z}$.

The above-mentioned finiteness results concerning norm form equations are all ineffective. In 1978, Győry and Papp [35] succeeded in obtaining, as an immediate consequence of a more general result (cf. [35], Theorem 3), the following effective finiteness theorem for norm form equations. They used Baker's method concerning linear forms in logarithms of algebraic numbers.

Theorem F (Győry and Papp [35]). *Suppose that in* (5) (i′) *α_{j+1} has degree ≥ 3 over $\mathbf{Q}(\alpha_1, \ldots, \alpha_j)$ for $j = 1, \ldots, m-1$. Then all solutions $\underline{x} = (x_1, \ldots, x_m) \in \mathbf{Z}^m$ of* (5) *satisfy $\max(|x_1|, \ldots, |x_m|) \leq C_4$, where C_4 is an effectively computable number.*

For $m = 2$, Theorem F (with the explicit C_4) reduces to Baker's Theorem B with another bound. In (i′), the lower bound 3 for the degrees cannot be diminished in general. Condition (i′) is, however, stronger than (i) in Theorem E, that is Theorem F did not make Schmidt's result effective. By a recent conjecture of Mignotte, Schmidt's theorem cannot be made effective in full generality.

Later another effective result on norm form equations was obtained independently by Kotov [41], [42] and Győry [29] which is not implied, even in ineffective form, by Schmidt's theorem.

Theorem G (Győry [29], Kotov[2] [42]). *Suppose that in* (5) α_m *is of degree* ≥ 3 *over* $\mathbf{Q}(\alpha_1, \ldots, \alpha_{m-1})$. *Then all solutions* $\underline{x} = (x_1, \ldots, x_m) \in \mathbf{Z}^m$ *of* (5) *with* $x_m \neq 0$ *satisfy* $\max(|x_1|, \ldots, |x_m|) \leq C_5$, *where* C_5 *is an effectively computable number.*

The restriction $x_m \neq 0$ and the condition concerning the degree of α_m cannot be dropped in general. We remark that Theorem F can be deduced from Theorem G.

Theorems F and G were established in [35], [29], [41] in the relative case. For generalizations to the case of finitely generated ground rings in number fields see Győry [27], [30] and Kotov [40], [41], and in arbitrary finitely generated extensions of $\mathbf{Q}$ see Győry [31], [33]. Under the assumptions of Theorems F and G, respectively, upper bounds for the numbers of solutions, independent of $\alpha_1, \ldots, \alpha_m$, were derived by Evertse and Győry [14].

Discriminant form and index form equations

We shall use the same notation as before. In particular, $L(\underline{X}) = \alpha_1 X_1 + \ldots + \alpha_m X_m$ and $L^{(1)}(\underline{X}), \ldots, L^{(n)}(\underline{X})$ are defined by (4). Here we do not assume, however, that $m \geq 2$ and $\alpha_1 = 1$. Then

$$D(\underline{X}) = D(\alpha_1 X_1 + \ldots + \alpha_m X_m) = \prod_{1 \leq i < j \leq m} (L^{(i)}(\underline{X}) - L^{(j)}(\underline{X}))^2$$

is a decomposable form of degree $n(n-1)$ with coefficients in $\mathbf{Q}$ which is called *discriminant form* (cf. Kronecker [43], Hensel [38]). The equations of the type

$$D(\underline{x}) = b \tag{6}$$

in $\underline{x} \in \mathbf{Z}^m$, named *discriminant form equations* (over $\mathbf{Z}$), play an important rôle in algebraic number theory. After several special results, in 1976 the following general and effective finiteness criterion was established by Győry [21].

Theorem H (Győry [21]). *The following two statements are equivalent:*

[2] Kotov [42] made the stronger hypothesis that α_m is of degree ≥ 5 over $\mathbf{Q}(\alpha_1 \ldots, \alpha_{m-1})$.

(i) $1, \alpha_1, \ldots, \alpha_m$ *are linearly independent over* $\mathbb{Q}$;

(ii) *(6) has only finitely many solutions in* $\underline{x} \in \mathbb{Z}^m$ *for every* $b \in \mathbb{Q}^*$.

Further, if (i) *holds, then all solutions* $\underline{x} = (x_1 \ldots, x_m) \in \mathbb{Z}^m$ *of* (6) *satisfy* $\max(|x_1|, \ldots, |x_m|) \leq C_6$, *where* C_6 *effectively computable.*

In fact, in [21] a more general result was proved which asserts that all solutions of (6) belong to finitely many so-called families of solutions and all these can be effectively found.

Of particular importance is the special case when $m = n - 1$ and $\{\alpha_0 = 1, \alpha_1, \ldots, \alpha_{n-1}\}$ is a $\mathbb{Z}$-basis of O_K, the ring of integers of K. Then Theorem H implies that up to the obvious translation by elements of $\mathbb{Z}$, the equation

$$D(\alpha) = b \quad \text{in } \alpha \in O_K$$

has only finitely many solutions and all these can be effectively determined. This finiteness assertion was earlier proved by Birch and Merriman [5] in a non-effective form and, independently, by Győry [20] in an effective form.

If $\alpha \in O_K$ and if $\alpha = x_0 + x_1\alpha_1 + \ldots + x_{n-1}\alpha_{n-1}$ is the representation of α with $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ then it is easy to verify that

$$D(\alpha_1 x_1 + \ldots + \alpha_{n-1}x_{n-1}) = I^2(x_1, \ldots, x_{n-1})D_K \tag{7}$$

where D_K denotes the discriminant of K and $I(X_1, \ldots, X_{n-1})$ is a decomposable form of degree $n(n-1)/2$ with coefficients in $\mathbb{Z}$. Further, the index of α in O_K, defined by

$$I(\alpha) = \left[O_K^+ : (\mathbb{Z}[\alpha])^+\right] \quad \text{is equal to } \left|I(x_1, \ldots, x_{n-1})\right|,$$

see for example [28]. For that reason, $I(X_1, \ldots, X_{n-1})$ is called the *index form* of the integral basis $\{\alpha_0, \ldots, \alpha_{n-1}\}$ in question, and the equations of the type

$$I(x_1, \ldots x_{n-1}) = \pm b \quad \text{in } x_1, \ldots, x_{n-1} \in \mathbb{Z} \tag{8}$$

are called *index form equations.* For cubic number fields, index form equations were earlier extensively studied by Nagell [47], Delone and Faddeev [10] and others. For further references, see [28]. In view of (7), (8) can be reduced to a discriminant form equation. As a consequence of his Theorem H, Győry obtained, in 1976, the following result.

Theorem I (Győry [21]). *All solutions* $\underline{x} = (x_1, \ldots, x_{n-1}) \in \mathbb{Z}^{n-1}$ *of* (8) *satisfy* $\max(|x_1|, \ldots, |x_{n-1}|) \leq C_7$, *where* C_7 *is effectively computable.*

Of particular interest is the special case $b = \pm 1$ when (8) is equivalent to the equation

$$I(\alpha) = 1 \quad (\alpha \in O_K) \iff O_K = \mathbf{Z}[\alpha] \iff \{1, \alpha, \ldots, \alpha^{n-1}\} \text{ is an integral basis.} \tag{9}$$

The existence of such a power integral basis considerably facilitates the calculation in O_K and the study of arithmetical properties of O_K. It is known that, for example, quadratic and cyclotomic fields have such integral bases, but this is not the case in general. If α is a solution of (9), then so is $\alpha + a$ for all $a \in \mathbf{Z}$. It follows from Theorem I that, up to translation by elements of $\mathbf{Z}$, (9) has only finitely many solutions and all these can be effectively determined; cf. Győry [21].

For further applications of Theorems H and I see Győry [28]. Theorems H, I and their consequences mentioned above were later extended by Győry [22], [23], Trelina [71], [72] and Győry and Papp [36] to the relative and p-adic case, and recently by Győry [31], [33], [34] to the case of arbitrary finitely generated ground domains.

We derived in [14] explicit upper bounds for the numbers of solutions of (6) and (8) which are independent of the coefficients of the forms involved. As a consequence we showed that up to the translation by elements of $\mathbf{Z}$, the number of solutions of (9) is at most $2(4 \times 7^{3g})^{n-2}$ where g denotes the degree of the normal closure of $K/\mathbf{Q}$ (hence $n \leq g \leq n!$).

Decomposable form equations of general type

We return now to the general decomposable form equation (1). Under various restrictive conditions made for F, Schmidt [53], [55], [56] and Schlickewei [50], [52] obtained ineffective finiteness results for certain other special types of decomposable form equations. A system of linear forms with coefficients in $\overline{\mathbf{Q}}$ is called *symmetric* (cf. [53]) if every form in the system occurs as often among the forms as its complex conjugate. In (1) the system of linear factors of F over $\overline{\mathbf{Q}}$ can be chosen to be symmetric. The following theorem can be deduced from a more general result of Schmidt (cf. [53], Satz 1).

Theorem J (Schmidt [53]). *Suppose that* $F(\underline{x}) \neq 0$ *for all* $\underline{0} \neq \underline{x} \in \mathbf{Z}^m$. *Then the following two statements are equivalent*:

(i) *For every subspace V of $\mathbb{Q}^m$ of dimension $d \geq 1$ and for every symmetric subsystem φ of the linear factors of F over $\overline{\mathbb{Q}}$, the rank of φ on V is greater than*

$$\min\{dt/n, d-1\}$$

where $n = \deg(F)$ and t is the number of the linear forms in φ;

(ii) *For every $b \in \mathbb{Q}^*$, equation (1) has only finitely many solutions in $\underline{x} \in \mathbb{Z}^m$.*

Theorem J implies Theorem E. The condition $F(\underline{x}) \neq 0$ does not hold however for discriminant forms and index forms, hence the criterion above does not apply to decomposable form equations in full generality. This result of Schmidt was later extended by Schlickewei [52] to the case of finitely generated ground rings in $\mathbb{Q}$.

We shall now present a general finiteness criterion which guarantees the finiteness of the number of solutions of (1) for every $b \in \mathbb{Q}^*$ and every finitely generated subring R of $\mathbb{Q}$. Let G be the splitting field of F (i.e. the smallest extension of $\mathbb{Q}$ over which F factorizes into linear forms), and let $\mathcal{L}_0$ be a maximal set of pairwise linearly independent linear factors of F with coefficients in G. For every subspace V of $\mathbb{Q}^m$ of dimension ≥ 1, we denote by $r(V, \mathcal{L}_0)$ the minimum of all integers r for which there exist linear forms $L_{i_1}, \ldots, L_{i_r}$ in $\mathcal{L}_0$ whose restrictions to V are linearly dependent but pairwise linearly independent. If this minimum exists then $r(V, \mathcal{L}_0) \geq 3$. Otherwise we put $r(V, \mathcal{L}_0) = 2$. Let $\mathcal{L} \supset \mathcal{L}_0$ be a finite set of linear forms in $X_1, \ldots, X_m$ with coefficients in G. A subspace V of $\mathbb{Q}^m$ is called *$\mathcal{L}$-admissible* if no form in $\mathcal{L}$ vanishes identically on V.

Theorem K (Evertse and Győry [15]). *The following two statements are equivalent:*

(i) *For every $\mathcal{L}$-admissible subspace V of $\mathbb{Q}^m$ of dimension ≥ 2, we have $r(V, \mathcal{L}_0) \geq 3$;*

(ii) *For every $b \in \mathbb{Q}^*$ and every subring R of $\mathbb{Q}$ which is finitely generated over $\mathbb{Z}$, the equation*

$$F(\underline{x}) = b \text{ in } \underline{x} \in R^m \text{ with } L(\underline{x}) \neq 0 \text{ for all } L \in \mathcal{L} \setminus \mathcal{L}_0 \qquad (1')$$

has only finitely many solutions.

Further, we showed in [15] that for every $b \in \mathbb{Q}^*$ and for every finitely generated subring R of $\mathbb{Q}$, all solutions of (1') belong to finitely many $\mathcal{L}$-admissible subspaces V of $\mathbb{Q}^m$ with $r(V, \mathcal{L}_0) = 2$. Since every subspace

of $\mathbf{Q}^m$ of dimension 1 can contain only finitely many solutions of (1'), the implication (i) $\Longrightarrow$ (ii) in Theorem K is an immediate consequence of this latter finiteness assertion. In [15] we proved these results in a more general form, over finitely generated subrings of an arbitrary finitely generated extension of $\mathbf{Q}$.

In the special case $\mathcal{L} = \mathcal{L}_0$ equation (1') reduces to equation (1) and Theorem K provides a finiteness criterion for (1). Theorem K implies, in an ineffective form, the finiteness assertions of Theorems A, B, E, F, G, H and I (cf. [15]). The finiteness result quoted after Theorem K, and therefore the implication (i) $\Longrightarrow$ (ii) in Theorem K can be deduced from the following finiteness theorem on S-unit equations which was established independently by van der Poorten and Schlickewei [49] and Evertse [13].

Let K be an algebraic number field, Γ a finitely generated subgroup of K^*, and $m \geq 2$ an integer. Then the equation

$$u_1 + u_2 + \ldots + u_m = 1 \quad \text{in } u_1, \ldots, u_m \in \Gamma$$

has only finitely many solutions such that $\sum_{i \in I} u_i \neq 0$ for each non-empty subset I of $\{1, 2, \ldots, m\}$.

In [15] (see also [16]) it has been pointed out that the implication (i) $\Longrightarrow$ (ii) of Theorem K is in fact equivalent to the above theorem on S-unit equations. Since this latter theorem has been deduced from the Schmidt-Schlickewei subspace theorem which is ineffective, Theorem K is also ineffective. Moreover,if Mignotte's conjecture is true, then it cannot be made effective in full generality. There does exist, however, an algorithm to decide whether condition (i) in Theorem K holds (cf. [15]).

For decomposable form equations of general type the first general effective finiteness result was obtained by Győry and Papp [35] in 1978. Later, their result was improved and generalized by Győry [29], [30] to Theorem L stated below. In the remainder of this section, let R be an arbitrary but fixed finitely generated subring of $\mathbf{Q}$ over $\mathbf{Z}$. Then $R = \mathbf{Z}\left[\frac{1}{p_1}, \ldots, \frac{1}{p_s}\right]$ with appropriate rational primes $p_1, \ldots, p_s$ ($s \geq 0$). For every $a \in \mathbf{Q}$ with $a = k/l$; $k, l \in \mathbf{Z}$, $(k, l) = 1$ we put $h(a) = \max\big(|k|, |l|\big)$.

Theorem L (Győry [30]). *Suppose that*

(i) *$\mathcal{L}_0$ has rank m;*

(ii) *$\mathcal{L}_0$ can be divided into subsets $\mathcal{L}_1, \ldots, \mathcal{L}_h$ with the following properties: if $\mathrm{Card}(\mathcal{L}_j) \geq 2$ for some j, then for each r, r' with $L_r, L_{r'} \in \mathcal{L}_j$, there exists a sequence $L_r = L_{r_1}, \ldots, L_{r_t} = L_{r'}$ in*

$\mathcal{L}_j$ such that, for $q = 1, \dots, t-1$, L_{r_q}, $L_{r_{q+1}}$ has a linear combination with coefficients in G^* which belongs to $\mathcal{L}_j$;

(iii) *$\mathcal{L} = \mathcal{L}_0$ or $\mathcal{L} = \mathcal{L}_0 \cup \{X_k\}$ for some $k \in \{1, \dots, m\}$ according as $h = 1$ or $h > 1$;*

(iv) *If $h > 1$, then X_k can be expressed as a linear combination of the forms from $\mathcal{L}_j$ for every $j \in \{1, \dots, h\}$.*

Then all solutions $\underline{x} = (x_1, \dots, x_m)$ of (1′) satisfy $\max\big(h(x_1), \dots, h(x_m)\big) \leq C_8$, where C_8 is effectively computable.

If $h = 1$ (this is the case e.g. for Thue equations), conditions (iii) and (iv) can be obviously dropped and Theorem L provides an effective finiteness result for (1). The discriminant forms, binary forms considered in Theorem B, and norm forms considered in Theorem G all satisfy the conditions of Theorem L. Therefore Theorem L implies (with the explicit C_8) Theorems B, C, F, G, H and I (cf. [30]). For extensions of Theorem L to the case of arbitrary ground rings which are finitely generated over $\mathbb{Z}$ we refer to Győry [31], [33]. Apart from the forms of the bounds, these general versions imply all the above-mentioned effective finiteness results for decomposable form equations (cf. [31], [33]). The proofs involve among other things Baker's method, the analogues over function fields of the results in question and some effective specialization argument.

In [14] we have recently shown that conditions (i), (ii), (iii), (iv) of Theorem L together imply the following condition

(i*) *For every $\mathcal{L}$-admissible subspace V of $\mathbb{Q}^m$ of dimension ≥ 2 we have $r(V, \mathcal{L}_0) = 3$.*

Since the number of subspaces V under consideration is in general infinite, it is hard to decide whether condition (i*) is satisfied or not. Let again $\mathcal{L}$ be as in Theorem K. We shall show that in Theorem L conditions (i) to (iv) can be replaced by a weaker version of (i*) which involves only finitely many and effectively determinable subspaces.

Theorem 1. *There is a finite, effectively determinable set of $\mathcal{L}$-admissible subspaces V of $\mathbb{Q}^m$ of dimension ≥ 2 such that if $r(V, \mathcal{L}_0) = 3$ for all V in this set, then all solutions $\underline{x} = (x_1, \dots, x_m)$ of (1′) satisfy $\max\big(h(x_1), \dots, h(x_m)\big) \leq C_9$, where C_9 is effectively computable.*

Theorem L is a consequence of Theorem 1. Further, Theorem 1 is easier to compare with Theorem K. We should, however, remark that in the most important special cases when $\mathcal{L} = \mathcal{L}_0 \cup \{X_k\}$ for some k, we do not know any equation to which Theorem 1 can be applied but Theorem L cannot. Furthermore, it is easier to check the more explicit conditions

of Theorem L.

The proof of Theorem 1 will be based on an effective finiteness result of Győry [25] obtained for S-unit equations in two unknowns, which was proved by means of Baker's method and its p-adic analogue.

In what follows, we may suppose without loss of generality that in (1'), $b \in \mathbf{Z}\setminus\{0\}$. Under assumption (i*), we derived in [14] the bound $n(4 \times 7^{g(2s+2\omega(b)+3)})^{m-1}$ for the number of solutions of (1') where $n = \deg(F)$ and $g = [G : \mathbf{Q}]$. By using an upper bound of Evertse [12] established for the numbers of solutions of S-unit equations in two unknowns we shall here deduce almost the same bound subject to the weaker and effective assumption of Theorem 1.

Theorem 2. *There is a finite, effectively determinable set of $\mathcal{L}$-admissible subspaces V of $\mathbf{Q}^m$ of dimension ≥ 2 such that if $r(V, \mathcal{L}_0) = 3$ for all V in this set, then the number of solutions of (1') is at most*

$$n(3 \times 7^{g(2s+2\omega(b)+3)})^{m-1}.$$

We note that $g \leq n!$. From Theorem 2 one can easily obtain bounds of a similar type for the numbers of solutions of the Thue equations, Thue-Mahler equations (cf. Theorem D), discriminant form and index form equations, and the norm form equations considered in Theorems F and G.

In §§2 and 3, we shall state and prove Theorems 1 and 2 in a more precise and more general form, for equations considered over the rings of S-integers of algebraic number fields.

§2. Some new results

Let K be an algebraic number field of degree d. Denote by M_K the set of places (that is, equivalence classes of multiplicative valuations) on K. Places in M_K are called *finite* if they contain non-archimedean valuations, and *infinite* otherwise. The field K has at most d infinite places. In every place p on $\mathbf{Q}$ we choose a valuation $|\cdot|_p$ normalized in the usual way (for elementary properties of places and heights which will be used in §§2 and 3 we refer to [16], §§1, 2, in this volume). Further, in every place v on K we normalize a valuation $|\cdot|_v$ in the following way: if v lies above $p \in M_{\mathbf{Q}}$ and if $\mathbf{Q}_p$, K_v denote the completions of $\mathbf{Q}$ at p and K at v respectively, then we choose $|\cdot|_v$ such that $|\alpha|_v = |\alpha|_p^{[K_v:\mathbf{Q}_p]/d}$ for each $\alpha \in \mathbf{Q}$. The set of valuations thus normalized satisfies the product formula.

Let S be a finite subset of M_K with cardinality s which contains all infinite places. Suppose that the finite places in S lie above rational primes not exceeding $P(\geq 2)$. By O_S we shall denote the ring

$$\{\alpha \in K : |\alpha|_v \leq 1 \text{ for all } v \in M_K \setminus S\}.$$

The elements of O_S and O_S^* are called *S-integers* and *S-units*, respectively. If S consists only of the infinite places, then O_S is just the ring O_K of integers in K. We note that the ring O_S is finitely generated over $\mathbf{Z}$ and every subring R of K which is finitely generated over $\mathbf{Z}$ is a subring of such a ring O_S. Moreover, if in particular $K = \mathbf{Q}$ then $R = O_S$ for an appropriate finite subset S of $M_{\mathbf{Q}}$.

For any integer $t \geq 1$, we define the *height* of $\underline{\alpha} = (\alpha_1, \ldots, \alpha_t) \in K^t$ by

$$h(\underline{\alpha}) = \prod_{v \in M_K} \max\{1, \max_{1 \leq j \leq t} |\alpha_j|_v\}.$$

In particular,

$$h(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}$$

will denote the height of $\alpha \in K$. For every positive number C there are only finitely many $\underline{\alpha}$ in K^t with $h(\underline{\alpha}) \leq C$ and these belong to an effectively determinable subset of K^t (cf. (11), (12)). We define the height of a polynomial

$$P(X_1, \ldots, X_t) = \sum_{i_1, \ldots, i_t} a(i_1, \ldots, i_t) X_1^{i_1} \ldots X_t^{i_t} \quad \text{in } K[X_1, \ldots, X_t]$$

by

$$h(P) = \prod_{v \in M_K} \max\{1, \max_{i_1, \ldots, i_t} |a(i_1, \ldots, i_t)|_v\}.$$

The heights $h(\underline{\alpha})$, $h(\alpha)$ and $h(P)$ depend only on $\underline{\alpha}$, α and P, respectively, and not on the choice of the number field K.

Let $F(\underline{X}) = F(X_1, \ldots, X_m) \in K[X_1, \ldots, X_m]$ be a decomposable form of degree $n \geq 3$ in $m \geq 2$ variables with height $\leq A$ which factorizes into linear factors over a finite extension G of K. Let $g = [G : K]$ and let D_G denote the absolute value of the discriminant of G (over $\mathbf{Q}$). Let $\mathcal{L}_0$ be a maximal set of pairwise linearly independent linear factors of F over G and let $\mathcal{L} \supseteq \mathcal{L}_0$ be a finite set of linear forms in $G[X_1, \ldots, X_m]$. For any subspace V of K^m of dimension ≥ 1 we define $r(V, \mathcal{L}_0)$ in the

same way as in §1. Similarly, we shall say that V is *$\mathcal{L}$-admissible* if no form in $\mathcal{L}$ vanishes identically on V. For given $C \geq 1$, there are only finitely many linear forms $L \in K[X_1, \ldots, X_m]$ with $h(L) \leq C$. We shall denote by $\mathcal{W}(K, m, C)$ the collection of subspaces V of K^m of the type

$$V = \{\underline{x} \in K^m : L_1(\underline{x}) = L_2(\underline{x}) = \ldots = L_r(\underline{x}) = 0\}$$

where r can be any integer with $1 \leq r \leq m-1$, and $\{L_1, \ldots, L_r\}$ can be any set of linear forms from $K[X_1, \ldots, X_m]$ with heights $\leq C$. The set $\mathcal{W}(K, m, C)$ is finite and $K^m \in \mathcal{W}(K, m, C)$. Let $\beta \in K^*$ with height $\leq B$ and consider the equation

$$F(\underline{x}) = \beta \text{ in } \underline{x} \in O_S^m \text{ with } L(\underline{x}) \neq 0 \text{ for all } L \in \mathcal{L} \setminus \mathcal{L}_0. \qquad (10)$$

Theorem 1′. *There are effectively computable numbers C_1, C_2 depending only on d, g, D_G, s, P, n, A, m and B with the following property : if*

(i′) *$r(V, \mathcal{L}_0) = 3$ for every $\mathcal{L}$-admissible subspace V of K^m of dimension ≥ 2 which belongs to $\mathcal{W}(K, m, C_1)$,*

then all solutions $\underline{x}$ of (10) satisfy $h(\underline{x}) \leq C_2$.

Theorem 1′ implies that there are finitely many $\mathcal{L}$-admissible subspaces V of K^m of dimension ≥ 2 such that if $r(V, \mathcal{L}_0) = 3$ for all of these V then (10) has only finitely many solutions. Moreover, if K, S, β, G, n and the coefficients of F and of the linear forms in $\mathcal{L}$ are effectively given in the sense defined in [69] and [34], p. 59, then both the subspaces V in question and the solutions of (10) can be effectively determined. In the special case $K = \mathbf{Q}$, this gives Theorem 1 stated in §1.

There are only finitely many $v \in M_K \setminus S$ for which $|\beta|_v \neq 1$ or F has a coefficient with v-value > 1. In the sequel the number of these v will be denoted by $\omega_S(\beta, F)$.

Theorem 2′. *If the condition* (i′) *holds with the C_1 specified in Theorem 1′, then the number of solutions of* (10) *is at most*

$$n(3 \times 7^{g(d+2s+2\omega_S(\beta,F))})^{m-1}.$$

In the case $K = \mathbf{Q}$, Theorem 2′ gives Theorem 2 formulated in §1.

As was mentioned in §1, the conditions (i) to (iv) of Theorem L together imply the assumption (i′) of Theorems 1′ and 2′. Therefore Theorem 1′ provides, as a consequence, a generalization of Theorem

L to equations over O_S. Such a generalization was earlier proved by Győry [30] with an explicit upper bound for the heights of the solutions. It implied more general versions over O_S of Theorems C, F, G, H, I presented in §1 (cf. Győry [30]). This means that apart from the forms of the bounds, these more general versions of Theorems C, F, G, H, I can also be deduced from Theorem 1'. Similarly, Theorem 2' implies (with slightly different bounds) the results of Evertse [12] and Evertse and Győry [14] on Thue equations, discriminant form equations and index form equations over S-integers of number fields.

§3. Proofs

We shall keep the notation of §2. It is important to note that if $H(\alpha)$ denotes the maximum absolute value of the coefficients of the minimal polynomial of an algebraic number α over $\mathbf{Z}$ and if d is the degree of α, then $H(\alpha)$ and $h(\alpha)$ (called sometimes the usual and absolute height of α, respectively) are related by

$$(d+1)^{1/2}\big(h(\alpha)\big) \leq H(\alpha) \leq 2^d\big(h(\alpha)\big)^d \tag{11}$$

(cf. [44], Ch. 3, p. 54 and Theorem 2.8). Further, if $\alpha = a/b \in \mathbf{Q}$ with $a, b \in \mathbf{Z}$ and $(a,b) = 1$ then

$$h(\alpha) = H(\alpha) = \max\big(|a|, |b|\big).$$

Let M_G be the set of places on G and suppose that the valuation $|.|_w$ in $w \in M_G$ is normalized in the same way as was indicated in §2. The height function can be extended to $q \times t$ matrices with entries in G. Let $\underline{A} = (\alpha_{jk})$ be such a matrix. Put

$$h(\underline{A}) = \prod_{w \in M_G} \max\Big\{1, \max_{\substack{1 \leq j \leq q \\ 1 \leq k \leq t}} |\alpha_{jk}|_w\Big\}.$$

The following lemma states a few elementary properties of height functions. Let $\mathcal{M}_{q,t}(G)$ denote the set of $q \times t$ matrices with entries in G.

Lemma 1. (i) *If* $\underline{A} = (\alpha_{jk}) \in \mathcal{M}_{q,t}(G)$ *then*

$$\max_{j,k} h(\alpha_{jk}) \leq h(\underline{A}) \leq \prod_{j,k} h(\alpha_{jk}). \tag{12}$$

(ii) *If* $\underline{A} \in \mathcal{M}_{q,t}(G)$, $\underline{B} \in \mathcal{M}_{t,r}(G)$, $\alpha \in G^*$ *then*

$$h(\underline{A}\,\underline{B}) \leq th(\underline{A})h(\underline{B}), \quad h(\alpha\underline{A}) \leq h(\alpha)h(\underline{A}) \tag{13}$$

(iii) *If* $\underline{A} \in \mathcal{M}_{q,q}(G)$ *and* $\underline{A}$ *is invertible then*

$$h(\underline{A}^{-1}) \leq h(\det \underline{A})(q-1)!h(\underline{A})^{q-1} \leq (q!)^2 h(\underline{A})^{2q-1}. \tag{14}$$

(iv) *Let* $\omega_1, \ldots, \omega_q$ *be* K*-linearly independent elements of* G*. There exist effectively computable numbers* c_1 *and* c_2*, depending only on* q*, such that for every* $\gamma = \xi_1\omega_1 + \ldots + \xi_q\omega_q$ *with* $\xi_1, \ldots, \xi_q \in K$ *we have*

$$h(\xi_1, \ldots, \xi_q) \leq c_1\big(h(\omega_1, \ldots, \omega_q)h(\gamma)\big)^{c_2}. \tag{15}$$

Proof. (i). Straightforward consequence of the definitions of the heights.
(ii), (iii). Straightforward application of the inequality

$$|\alpha_1 + \ldots + \alpha_t|_w \leq t \max\{|\alpha_1|_w, \ldots, |\alpha_t|_w\}$$
$$\text{for } \alpha_1, \ldots, \alpha_t \in G \text{ and } w \in M_G.$$

(iv). Let $\sigma_1 \ldots, \sigma_q$ be distinct K-isomorphisms of G for which $\Omega = \big(\sigma_j(\omega_k)\big)$, with $1 \leq j, k \leq q$, is invertible. Let[3] $\underline{x} = (\xi_1, \ldots, \xi_q)^T$, $\underline{b} = \big(\sigma_1(\gamma), \ldots, \sigma_q(\gamma)\big)^T$. Then $\underline{b} = \Omega\underline{x}$. Since $h\big(\sigma_j(\omega_k)\big) = h(\omega_k)$ for $1 \leq j, k \leq q$, we have $h(\Omega) \leq h(\omega_1, \ldots, \omega_q)^{c_4}$ where $c_4 = c_4(q)$ is effectively computable in terms of q. Now (15) follows by applying first (14) to Ω and then (13) to $\underline{x} = \Omega^{-1}\underline{b}$. ∎

For every polynomial $P \in G[X_1, \ldots, X_m]$ and for every $w \in M_G$ we denote by $|P|_w$ the maximum of the w-values of the coefficients of P. It is known (cf. [44]) that if w is a finite place then for every $P, Q \in G[X_1, \ldots, X_m]$

$$|PQ|_w = |P|_w \cdot |Q|_w. \tag{16}$$

Put

$$h^*(P) = \prod_{w \in M_G} |P|_w.$$

Then, by the product formula, $h^*(\alpha P) = h^*(P)$ for any $\alpha \in G^*$ and

$$1 \leq h^*(P) \leq h(P). \tag{17}$$

[3] We denote by $\underline{B}^T$ the transposed matrix of a matrix $\underline{B}$.

Further, if at least one of the coefficients of P is equal to 1 then $h^*(P) = h(P)$.

Lemma 2. *Let $P, Q \in G[X_1, \ldots, X_m]$. Suppose that at least one of the coefficients of P is equal to 1 and that PQ has degree $\leq n$. Then*

$$h(P) \leq 4^{dg(n+1)^m} h(PQ).$$

Proof. We have

$$\begin{aligned} 4^{-dg(n+1)^m} h^*(PQ) &\leq h^*(P)h^*(Q) \\ &\leq 4^{dg(n+1)^m} h^*(PQ) \end{aligned} \tag{18}$$

(cf. [44], Ch. 3, Prop. 2.4). Now Lemma 2 follows from (17) and (18).

Let S' be the subset of M_G lying above the places in S, and let $O_{S'}$ be the ring of S'-integers in G. Then $O_{S'}$ contains as a subring the ring O_G of integers of G. We define the *S'-norm* by

$$N_{S'}(\alpha) = \Big(\prod_{w \in S'} |\alpha|_w \Big)^{dg} \qquad \text{for } \alpha \in G^*,$$

where $dg = [G : \mathbb{Q}]$. It is easily seen that the S'-norm is multiplicative. Further, if $\alpha \in O_{S'}$ then

$$1 \leq N_{S'}(\alpha) \leq \big(h(\alpha)\big)^{dg}.$$

The proof of Theorem 1′ is based on the following lemma which is an easy consequence of an effective result of Győry [25] on homogeneous S'-unit equations in three unknowns. We note that Győry [25] gave an explicit bound for the heights of the solutions. Following the arguments of the proofs below of Theorems 1′ and 2′ and using the explicit bound mentioned, it would not be difficult to derive explicit values for C_1 and C_2 in Theorems 1′ and 2′.

Lemma 3. *Let $N \geq 1$ and let $\gamma_1, \gamma_2, \gamma_3 \in O_G \setminus \{0\}$ with heights $\leq \Gamma$. Then all solutions of the equation*

$$\begin{aligned} \gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3 = 0 \ &\text{in } x_1, x_2, x_3 \in O_{S'} \setminus \{0\} \\ &\text{with } \max_{1 \leq i \leq 3} N_{S'}(x_i) \leq N \end{aligned} \tag{19}$$

satisfy $h(x_1/x_2) \leq c_5 N^{c_6}$ *where* c_5, c_6 *are effectively computable positive numbers depending only on* d, g, D_G, s, P *and* Γ.

In fact this lemma can be found, in a more explicit form, in the work [32] of Győry. Since [32] was written in Hungarian, we shall give here a complete proof.

Proof. Let $\wp_1, \ldots, \wp_{s'}$, be the prime ideals in O_G corresponding to the finite places in S'. Clearly $s' \leq g \cdot s$. Since $x_i \in O_{S'}$, the ideal (x_i) generated by x_i can be written as $v_i \wp_1^{a_{i1}} \ldots \wp_{s'}^{a_{is'}}$, where v_i is an integral ideal in G coprime with $\wp_1, \ldots, \wp_{s'}$, and $a_{i1}, \ldots, a_{is'}$ are non-negative rational integers. Obviously $N(v_i) \leq N$. Let h_G and R_G be the class number and regulator of G. Then

$$\max\{h_G, R_G\} < c_7(d, g, D_G),$$

where c_7 is effectively computable in terms of d, g, D_G (cf. [61]). Let b_{ij} be rational integers such that $b_{ij} \equiv a_{ij} (\mathrm{mod}\, h_G)$ and $0 \leq b_{ij} < h_G$ for each i and j. Then $v_i \wp_1^{b_{i1}} \ldots \wp_{s'}^{b_{is'}}$ is a principal ideal, say (y_i), with $y_i \in O_G$ and $|N_{G/\mathbb{Q}}(y_i)| \leq c_8 N$, $i = 1, 2, 3$. Here c_8 and c_9, c_{10} below denote effectively computable positive numbers depending only on d, g, D_G, s, P and Γ. We have $x_i = y_i \delta_i$ with some $\delta_i \in O_{S'}^*$, $i = 1, 2, 3$. Putting $\wp_j^{h_G} = (\pi_j)$ with appropriate $\pi_j \in O_G$ for $j = 1, \ldots, s'$, there are positive integers $b_1, \ldots, b_{s'}$ such that $\rho_i := \delta_i \pi_1^{b_i} \ldots \pi_{s'}^{b_{s'}} \in O_G \cap O_{S'}^*$ for $i = 1, 2, 3$. For $x_i' := \pi_1^{b_1} \ldots \pi_{s'}^{b_{s'}} x_i = y_i \rho_i$ we have

$$\gamma_1 x_1' + \gamma_2 x_2' + \gamma_3 x_3' = 0$$

and Lemma 6 of Győry [25] gives

$$h(x_1/x_2) = h(x_1'/x_2') \leq c_g N^{c_{10}}. \qquad \blacksquare$$

Denote by T the smallest subset of M_K containing S such that both $|\beta|_v = 1$ and the v-values of all coefficients of F are ≤ 1 for all $v \in M_K \setminus T$. Further, let T' be the subset of places of M_G lying above the places in T, $O_{T'}$ the ring of T'-integers in G and t' the cardinality of T'. Then $t' \leq g(s + \omega_S(\beta, F))$. Furthermore, we have $\beta \in O_{T'}^*$, $F \in O_{T'}[X_1, \ldots, X_m]$ and $O_S \subseteq O_{T'}$.

The main tool in the proof of Theorem 2′ will be the following result of Evertse [12].

Lemma 4. *For every* $\gamma, \delta \in G^*$ *the equation*

$$\gamma x + \delta y = 1 \qquad \text{in } x, y \in O_{T'}^*$$

has at most $3 \times 7^{dg+2t'}$ *solutions.*

Proof. This is Theorem 1 in [12].

Before proving our theorems we show that we can make certain assumptions without loss of generality. We may assume that the coefficient of X_1^n in F, say a_0, is different from zero. Indeed, there is a rational integer a with $0 \leq a \leq mn$ such that $F(1, a, \ldots, a^{m-1}) \neq 0$. On applying the linear transformation

$$X_i = a^{i-1} X_1' + X_i', \qquad i = 1, \ldots, m,$$

to F, $\mathcal{L}_0$, $\mathcal{L}$ and (10), all conditions of our theorems will be satisfied together with the assumption required.

Further, replacing the linear forms in $\mathcal{L}$ by appropriate proportional factors if necessary, we may choose the factorization

$$F(\underline{X}) = L_1(\underline{X}) \ldots L_n(\underline{X}) \tag{20}$$

of F into linear forms $L_1, \ldots, L_n$ from $G[X_1, \ldots, X_m]$ such that

$$\max_{1 \leq j \leq n} h(L_j) \leq c_{11} \tag{21}$$

where c_{11} and c_{12}, c_{13} below are effectively computable positive numbers depending only on d, g, n, A and m. Indeed, we may choose the coefficients of X_1 in $L_1, \ldots, L_n$ to be a_0, 1,..., 1, respectively. Then by Lemma 2,

$$A \geq h(F) \geq c_{12} \max\{h(L_1/a_0), h(L_2), \ldots, h(L_m)\}. \tag{22}$$

Further, a_0 is a coefficient of F so that $h(a_0) \leq h(F)$. Hence, by (13), $h(L_1) \leq h(a_0) h(L_1/a_0) \leq c_{13}$. Together with (22) this proves (21).

Finally, we show that if (10) is solvable then there are $\mu_1, \ldots, \mu_n \in G^*$ such that

$$\mu_j L_j(\underline{x}) \in O_{T'}^* \ (j = 1, \ldots, n) \quad \text{for all solutions } \underline{x} \text{ of (10)} \tag{23}$$

(see also [14]). Indeed, let $w \in M_G \setminus T'$. Then for every solution $\underline{x}$ we have

$$|L_j(\underline{x})|_w \leq |L_j|_w \quad \text{for } j = 1, \ldots, n,$$

and, by (16), $|\beta|_w = 1$ and $|F|_w \leq 1$,

$$\prod_{j=1}^{n} (|L_j(\underline{x})|_w / |L_j|_w) = |F(\underline{x})|_w / |F|_w = |\beta|_w / |F|_w \geq 1.$$

Hence

$$|L_j(\underline{x})|_w = |L_j|_w \qquad \text{for } j = 1, \ldots, n. \tag{24}$$

Let $\underline{x}_0$ be a fixed solution of (10) and put $\mu_1 = \beta L_1(\underline{x}_0)^{-1}$ and $\mu_j = L_j(\underline{x}_0)^{-1}$ for $j = 2, \ldots, n$. Then, by (24), $|\mu_j L_j(\underline{x})|_w = 1$ $(j = 1, \ldots, n)$ and (23) holds.

Both Theorem 1′ and Theorem 2′ are easy to deduce from the next lemma.

Lemma 5. *Let q be a rational integer with $0 \leq q \leq m-2$, let $C_q^* \geq 1$, and let V be an $\mathcal{L}$-admissible subspace of K^m of dimension $m-q$ with $V \in \mathcal{W}(K, m, C_q^*)$ and $r(V, \mathcal{L}_0) = 3$. Then there exists an effectively computable number C_{q+1}^* $(\geq C_q^*)$ depending only on d, g, D_G, s, P, A, n, m, B and C_q^* such that all solutions $\underline{x} \in V \cap O_S^m$ of (10) are contained in at most $3 \times 7^{dg+2t'}$ $\mathcal{L}$-admissible subspaces of V with dimension $m-q-1$ which belong to $\mathcal{W}(K, m, C_{q+1}^*)$.*

Proof. In what follows, $c_{14}, \ldots, c_{19}$ will denote effectively computable positive numbers depending only on d, g, D_G, s, P, A, n, m, B, C_q^*. Further, for convenience we put $N = 3 \times 7^{dg+2t'}$.

Suppose that (10) has a solution in $V \cap O_S^m$. Consider a fixed factorization of the form (20) of F with the property (21) and fix some $\mu_1, \ldots, \mu_n \in G^*$ for which (23) holds. In view of (11) and (12), the height of the least common multiple, say a, of the denominators of the coefficients of $L_1, \ldots, L_n$ occurring in (2) is at most c_{14}. Let $\underline{x} \in V \cap O_S^m$ be an arbitrary but fixed solution of (10). Then $aL_j(\underline{x}) \in O_{S'}$ and by (10) and (20), we have

$$a^n \beta \in O_{S'} \text{ and } aL_j(\underline{x}) \text{ divides } a^n \beta \text{ in } O_{S'} \text{ for } j = 1, \ldots, n. \tag{25}$$

By assumption, among $L_1, \ldots, L_n$ there are three linear forms, say L_1, L_2, L_3, whose restrictions to V are linearly dependent but pairwise linearly independent. Therefore there exist γ_1, γ_2, $\gamma_3 \in G^*$ such that $\gamma_1 L_1(\underline{X}) + \gamma_2 L_2(\underline{X}) + \gamma_3 L_3(\underline{X}) = 0$ identically on V. In view of $V \in \mathcal{W}(K, m, C_q^*)$, γ_1, γ_2, γ_3 can be chosen from $O_G \setminus \{0\}$ with heights at most c_{15}. For the solution $\underline{x}$ under consideration we have

$$\gamma_1 (aL_1(\underline{x})) + \gamma_2 (aL_2(\underline{x})) + \gamma_3 (aL_3(\underline{x})) = 0. \tag{26}$$

Further, by (25)

$$N_{S'}(L_j(\underline{x})) \leq N_{S'}(a^n\beta) \leq \left(h(a^n\beta)\right)^{dg} \leq c_{16}.$$

By applying now Lemma 3 to (26) we obtain

$$h(L_1(\underline{x})/L_2(\underline{x})) \leq c_{17}.$$

On the other hand, it follows from (26) that

$$\left(-\frac{\gamma_1\mu_1^{-1}}{\gamma_2\mu_2^{-1}}\right)\left(\frac{\mu_1 L_1(\underline{x})}{\mu_2 L_2(\underline{x})}\right) + \left(-\frac{\gamma_3\mu_3^{-1}}{\gamma_2\mu_2^{-1}}\right)\left(\frac{\mu_3 L_3(\underline{x})}{\mu_2 L_2(\underline{x})}\right) = 1.$$

Together with Lemma 4 and (23), this implies that $(\mu_1 L_1(\underline{x})/\mu_2 L_2(\underline{x}))$ and hence $L_1(\underline{x})/L_2(\underline{x})$ belongs to a subset of G^* of cardinality at most N which does not depend on $\underline{x}$. Consequently, there exist at most N elements $\lambda \in G^*$ with heights $\leq c_{17}$ such that every solution $\underline{x} \in V \cap O_S^m$ of (10) is a zero of at least one of the linear forms

$$L_\lambda(\underline{X}) = L_1(\underline{X}) - \lambda L_2(\underline{X}).$$

By the assumption made on L_1, L_2, none of the forms L_λ vanishes identically on V.

As is known (see e.g. [28], p. 71), O_G has an integral basis $\{\omega_1, \ldots, \omega_{dg}\}$ such that

$$\begin{aligned} h(\omega_1, \ldots, \omega_{dg}) &\leq h(\omega_1) \ldots h(\omega_{dg}) \\ &\leq \left(|\overline{\omega_1}| \ldots |\overline{\omega_{dg}}|\right)^{dg} \leq c_{18}, \end{aligned} \tag{27}$$

where $|\overline{\omega_i}|$ denotes the maximum of the absolute values of the conjugates of ω_i, $i = 1, \ldots, dg$. We may assume that $\omega_1, \ldots, \omega_g$ are K-linearly independent. Each L_λ considered above can be written as

$$L_\lambda(\underline{X}) = \sum_{j=1}^{g} \omega_j l_{\lambda,j}(\underline{X}) \tag{28}$$

with linear forms $l_{\lambda,j} \in K[X_1, \ldots, X_m]$ which do not all identically vanish on V. By using Lemma 1, (iv) and (27) we obtain from (28) that $h(l_{\lambda,j}) \leq c_{19}$ for $j = 1, \ldots, g$. Further, $l_{\lambda,j}(\underline{x}) = 0$ $(j = 1, \ldots, g)$ for every $\underline{x} \in V$ with $L_\lambda(\underline{x}) = 0$. Thus we conclude that all solutions $\underline{x} \in V \cap O_S^m$ are contained in at most N $\mathcal{L}$-admissible subspaces of V of dimension

$m-q-1$ which belong to $\mathcal{W}(K,m,C^*_{q+1})$ for $C^*_{q+1}=\max(C^*_q,c_{19})$. This completes the proof of the lemma. ∎

Proof of Theorem 1'. If assumption (i') holds with $C_1 \geq 1$ then $r(K^m,\mathcal{L}_0)=3$. Hence we can apply Lemma 5 successively with $q=0,1,\ldots,m-2$ and with $C^*_0=1$. Let $1\leq C^*_1\leq\ldots\leq C^*_{m-2}\leq C^*_{m-1}$ be the corresponding effectively computable numbers, specified in Lemma 5, which depend now only on d, g, D_G, s P, A, n, m and B. Put $C_1=C^*_{m-2}$ and suppose that $r(V,\mathcal{L}_0)=3$ for every $\mathcal{L}$-admissible subspace V of K^m of dimension ≥ 2 with $V\in\mathcal{W}(K,m,C_1)$. Then, by Lemma 5, it follows that all solutions of (10) are contained in subspaces of K^m of dimension 1 belonging to $\mathcal{W}(K,m,C^*_{m-1})$. This means that every solution $\underline{x}$ of (10) can be written in the form $\underline{x}=\kappa\underline{x}'$ with some $\kappa\in K^*$ and $\underline{x}'\in K^m$ for which $h(\underline{x}')\leq c_{20}$, where c_{20} as well as c_{21}, c_{22} introduced below are effectively computable numbers depending only on on d, g, D_G, s, P, A, n, m and B. From (10) we obtain

$$\kappa^n F(\underline{x}')=\beta.$$

Together with (12) and (13) this implies $h(\kappa)\leq c_{21}$ whence $h(\underline{x})\leq c_{22}$.

Proof of Theorem 2'. Apply again Lemma 5 successively in the same way as in the proof of Theorem 1'. Let $1=C^*_0\leq C^*_1\leq\ldots\leq C^*_{m-2}\leq C^*_{m-1}$ be as above, and suppose again that $r(V,\mathcal{L}_0)=3$ for every $\mathcal{L}$-admissible subspace V of K^m of dimension ≥ 2 which belongs to $\mathcal{W}(K,m,C_1)$ for $C_1=C^*_{m-2}$. Then Lemma 5 implies that all solutions of (10) are contained in at most N^{m-1} subspaces of K^m of dimension 1. If $\underline{x}$ and $\rho\underline{x}$ are solutions of (10) with some $\rho\in K^*$ then

$$\rho^n=F(\rho\underline{x})/F(\underline{x})=1.$$

Therefore, every subspace of K^m of dimension 1 contains at most n solutions. Hence the number of solutions of (10) is at most

$$\begin{aligned} nN^{m-1} &= n(3\times 7^{dg+2t'})^{m-1}\\ &\leq n(3\times 7^{g(d+2s+2\omega_S(\beta,F))})^{m-1}. \end{aligned}$$

∎

References

[1] A. Baker, Contributions to the theory of Diophantine equations, *Philos. Trans. Roy. Soc. London*, **A 263** (1968), 173–208.

[2] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Math. Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.

[3] A. Baker, A sharpening of the bounds for linear forms in logarithms II, *Acta Arith.* **24** (1973), 33–36.

[4] A. Baker, *Transcendental number theory*, 2nd ed., Cambridge University Press, 1979.

[5] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* **25** (1972), 385–394.

[6] E. Bombieri and W. M. Schmidt, On Thue's equation, *Invent. Math.* **88** (1987), 69–81.

[7] Z. I. Borevich and I. R. Shafarevich, *Number theory*, 2nd ed., 1967.

[8] J. Coates, An effective p-adic analogue of a theorem of Thue, *Acta Arith.* **15** (1969), 279–305.

[9] J. Coates, An effective p-adic analogue of a theorem of Thue II, The greatest prime factor of a binary form, *Acta Arith.* **16** (1970), 399–412.

[10] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, American Mathematical Society, Providence, 1964.

[11] J. H. Evertse, Upper bounds for the numbers of solutions of Diophantine equations, MC – tract 168, Amsterdam, 1983.

[12] J. H. Evertse, On equations in S-units and the Thue-Mahler equation, *Invent. Math.* **75** (1984), 561–584.

[13] J. H. Evertse, On sums of S-units and linear recurrences, *Compositio Math.* **53** (1984), 225–244.

[14] J. H. Evertse and K. Győry, On unit equations and decomposable form equations, *J. reine angew. Math.* **358** (1985), 6–19.

[15] J. H. Evertse and K. Győry, Finiteness criteria for decomposable form equations, *Acta, Arith.* to appear.

[16] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, S-unit equations and their applications, This volume.

[17] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[18] G. Faltings, G. Wüstholz et al., *Rational points*, Vieweg 1984.

[19] N. I. Feldman, An effective refinement of the exponent in Liouville's theorem (Russian), *Izv. Akad. Nauk SSSR* **35** (1971). 973–990.

[20] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, *Acta Arith.* **23** (1973), 419–426.

[21] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné III, *Publ. Math Debrecen* **23** (1976), 141–165.

[22] K. Győry, On polynomials with integer coefficients and given discriminant IV, *Publ. Math. Debrecen* **25** (1978), 155–167.

[23] K. Győry, On polynomials with integer coefficients and given discriminant V, p-adic generalizations, *Acta Math. Acad. Sci. Hungar.* **32** (1978), 175–190.

[24] K. Győry, On the greatest prime factors of decomposable forms at integer points, *Ann. Acad. Sci. Fenn. Ser. A I, Math.* **4** (1978/1979), 341–355.

[25] K. Győry, On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.* **54** (1979), 583–600.

[26] K. Győry, Explicit upper bounds for the solutions of some Diophantine equations, *Ann. Acad. Sci. Fenn., Ser. A, Math.* **5** (1980), 3–12.

[27] K. Győry, Sur certaines généralisations de l'équation de Thue-Mahler, *Enseign. Math.* **26** (1980), 247–255.

[28] K. Győry, Résultats effectifs sur la représentation des entiers par des formes décomposables, *Queen's Papers in Pure and Applied Math.*, No. 56, Kingston, Canada, 1980.

[29] K. Győry, On the representation of integers by decomposable forms in several variables, *Publ. Math. Debrecen* **28** (1981), 89–98.

[30] K. Győry, On S-integral solutions of norm form, discriminant form and index form equations, *Studia Sci. Math. Hungar.* **16** (1981), 149–161.

[31] K. Győry, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta. Math. Hungar.* **42** (1983), 45–80.

[32] K. Győry, Effective finiteness theorems for Diophantine problems and their applications (in Hungarian), Academic doctor's thesis, Debrecen, 1983.

[33] K. Győry, On norm form, discriminant form and index form equations, *Coll. Math. Soc. J. Bolyai 34.* Topics in Classical Number Theory, Budapest, 1981. North-Holland 1984, pp. 617–676.

[34] K. Győry, Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains, *J. reine angew. Math.* **346** (1984), 54–100.

[35] K. Győry and Z. Z. Papp, Effective estimates for the integer solutions of norm form and discriminant form equations, *Publ. Math. Debrecen* **25** (1978), 311–325.

[36] K. Győry and Z. Z. Papp, On discriminant form and index form equations, *Studia Sci. Math. Hungar.* **12** (1977), 47–60.

[37] K. Győry and Z. Z. Papp, Norm form equations and explicit lower bounds for linear forms with algebraic coefficients, *Studies in Pure Mathematics* (To the memory of Paul Turán), Budapest, 1983. pp. 245–257.

[38] K. Hensel, *Theorie der algebraischen Zahlen*, Leipzig und Berlin, 1908.

[39] S. V. Kotov, The Thue-Mahler equation in relative fields (Russian), *Acta Arith.* **27** (1975), 293–315.

[40] S. V. Kotov, On Diophantine equations of norm form type II (Russian), *Inst. Math. Akad. Nauk BSSR,* Preprint No. 10, Minsk, 1980.

[41] S. V. Kotov, Effective bound for a linear form with algebraic coefficients in the archimedean and p-adic metrics, *Inst. Math. Akad. Nauk BSSR,* Preprint No. 24, Minsk, 1981.

[42] S. V. Kotov, Effective bound for the values of the solutions of a class of Diophantine equations of norm form type (Russian), *Mat. Zametki* **33** (1983), 801–806.

[43] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Größen, *J. reine angew. Math.* **92** (1882), 1–122.

[44] S. Lang, *Fundamentals of Diophantine geometry*, Springer 1983.

[45] M. Laurent, Equations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299–327.

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

[47] T. Nagell, Zur Theorie der kubischen Irrationalitäten, *Acta Math.* **55** (1930), 33-65.

[48] C. J. Parry, The P-adic generalization of the Thue-Siegel theorem, *Acta Math.* **83** (1950), 1–100.

[49] A. J. van der Poorten and H-P. Schlickewei, The growth conditions for recurrence sequences, *Macquarie Univ. Math. Rep.* 82–0041, North Ryde, Australia, 1982.

[50] H-P. Schlickewei, Inequalities for decomposable forms, *Astérisque* **41–42** (1977), 267–271.

[51] H-P. Schlickewei, On norm form equations, *J. Number Theory* **9** (1977), 370–380.

[52] H-P. Schlickewei, On linear forms with algebraic coefficients and Diophantine equations, *J. Number Theory* **9** (1977), 381–392.

[53] W. M. Schmidt, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191** (1971), 1–20.

[54] W. M. Schmidt, Norm form equations, *Annals of Math.* **96** (1972), 526–551.

[55] W. M. Schmidt, Inequalities for resultants and for decomposable forms, *Proc. Conf. Diophantine approximation and its applications,* Washington, 1972. New York and London, 1973, pp. 235–253.

[56] W. M. Schmidt, *Diophantine approximation, Lecture Notes in Math.* **785**, Springer 1980.

[57] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gelfond-Baker method to Diophantine equations, Transcendence Theory: Advances and Applications,* 59–77. Academic Press, 1977.

[58] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations,* Cambridge University Press, 1986.

[59] C. L. Siegel, Approximation algebraischer Zahlen, *Math. Z.* **10** (1921), 173–213.

[60] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.* (1929), 1–41.

[61] C. L. Siegel, Abschätzung von Einheiten, *Nachr. Göttingen* (1969), 71–86.

[62] T. Skolem, *Diophantische Gleichungen*, Berlin, 1938.

[63] V. G. Sprindžuk, Rational approximations to algebraic numbers (Russian), *Izv. Akad. Nauk SSSR* **35** (1971), 991–1007.

[64] V. G. Sprindžuk, The greatest prime divisor of a binary form (Russian), *Dokl. Akad. Nauk BSSR* **15** (1971), 389–391.

[65] V. G. Sprindžuk, On an estimate for solutions of Thue's equation (Russian), *Izv. Akad. Nauk SSSR* **36** (1972), 712–741.

[66] V. G. Sprindžuk, On the structure of numbers representable by binary forms (Russian), *Dokl. Akad. Nauk BSSR* **17** (1973), 685–688.

[67] V. G. Sprindžuk, *Classical Diophantine equations in two variables* (Russian), Moscow, 1982.

[68] H. M. Stark, Effective estimates of solutions of some Diophantine equations, *Acta Arith.* **24** (1973), 251–259.

[69] K. B. Stolarsky, *Algebraic numbers and Diophantine approximation*, New York, 1974.

[70] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. reine angew. Math.* **135** (1909), 284–305.

[71] L. A. Trelina, On algebraic integers with discriminants having fixed prime factors (Russian), *Mat. Zametki* **21** (1977), 289–296.

[72] L. A. Trelina, On the greatest prime factor of an index form (Russian), *Dokl. Akad. Nauk BSSR* **21** (1977), 975–976.