On unit equations and decomposable form equations

By *J. H. Evertse* at Amsterdam and *K. Győry**) at Debrecen

§ 1. Introduction

Let K be a field of characteristic 0, Γ a finitely generated multiplicative subgroup of K^*[1]), and $\lambda, \mu \in K^*$. By using explicit results of Evertse on the number of solutions of linear equations in two S-units over algebraic number fields [2] and algebraic function fields [4], we shall derive an upper bound for the number of solutions of the *unit equation* in two variables

$$\lambda x + \mu y = 1 \quad \text{in} \quad x, y \in \Gamma$$

(cf. § 2, Theorem 1) which does not depend on λ, μ. By applying this, we shall establish upper bounds for the numbers of solutions of decomposable form equations of the form

$$F(x_1, \ldots, x_m) = \varepsilon \quad \text{in} \quad x_1, \ldots, x_m \in R, \quad \varepsilon \in R^*$$

(cf. § 3, Theorems 2, 3) where R is an arbitrary finitely generated integral domain over $\mathbb{Z}$ and where $F(X_1, \ldots, X_m)$ is a decomposable form (i.e. a form which factorizes into linear forms over some extension of the quotient field, say L, of R) satisfying certain general conditions. Here solutions $(x_1, \ldots, x_m, \varepsilon)$, $(x_1', \ldots, x_m', \varepsilon')$ are identified if $x_i' = u x_i$ for some $u \in L^*$ $(i = 1, \ldots, m)$. We note that our bounds do not depend on the coefficients of F. We shall apply our general results on decomposable form equations to Thue equations and Thue-Mahler equations over R (cf. § 4, Theorems 5, 6), to a class of norm form equations over R (cf. § 5, Theorems 7, 8), to discriminant form equations and index form equations over R (cf. § 6, Theorems 9, 10) and to power bases of integral ring extensions of R (cf. § 6, Theorem 11). We note that effective analogues of Theorems 3 and 5 to 11 were earlier proved by Győry [9], [10], [11]. Further, in the special case that L is an algebraic number field with ring of integers R, Theorems 5 and 6 on Thue equations and Thue-Mahler equations were earlier established (with slightly different bounds) by Evertse [1], [2].

---

*) The research has been done at the University of Leiden in the academic year 1983/1984.

[1]) K^* denotes the set of non-zero elements of K. In general, for any integral domain R, R^* will denote the unit group (i.e. the multiplicative group of invertible elements) of R.

Our results have interesting applications to algebraic number theory. For instance, let M be an algebraic number field of degree m with ring of integers $\mathcal{O}_M$. Call two numbers $\alpha, \beta \in \mathcal{O}_M$ $\mathbb{Z}$-equivalent if $\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$. Then $\mathcal{O}_M = \mathbb{Z}[\alpha]$ implies $\mathcal{O}_M = \mathbb{Z}[\beta]$ and conversely. It follows from Theorem 11 that the number of $\mathbb{Z}$-equivalence classes of $\alpha \in \mathcal{O}_M$ for which $\mathcal{O}_M = \mathbb{Z}[\alpha]$ can be estimated from above by an explicit constant depending only on m.

Finally, we mention that our finiteness assertions do not remain valid in general if the integral domain R is not finitely generated over $\mathbb{Z}$.

§ 2. On the numbers of solutions of unit equations in two variables

Let again K be a field of characteristic 0, let Γ be a finitely generated multiplicative subgroup of K^*, and let λ, μ be non-zero elements of K. Lang [12] (cf. also [13]) showed that the equation

$$\lambda x + \mu y = 1 \tag{1}$$

has at most finitely many solutions in $x, y \in \Gamma$. This implies for instance that if R is a subring of K which is finitely generated over $\mathbb{Z}$ then its unit group R^* is also finitely generated (cf. [17]) and hence (1) has at most finitely many solutions in $x, y \in R^*$. As mentioned above, the equations of this type are called unit equations.

Our aim is to give a quantitative version of Lang's result. To state this, we need some further notations. The group Γ can be embedded in a field of finite type over $\mathbb{Q}$. So we may suppose that K itself is an arbitrary finitely generated (but not necessarily algebraic) extension of $\mathbb{Q}$. Let $\{z_1, \ldots, z_q\}$ be a transcendence basis of K over $\mathbb{Q}$, and let $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$. Then K is a finite extension of K_0. Denote by d the degree of the extension K/K_0. The polynomial ring $\mathcal{O} = \mathbb{Z}[z_1, \ldots, z_q]$ is a unique factorization domain in which the prime elements are the rational primes and the primitive irreducible non-constant polynomials in $\mathcal{O}$. To every prime element π of $\mathcal{O}$ corresponds an (additive) valuation v_π on K_0 with the property that $v_\pi(\pi) = 1$ and $v_\pi\left(\frac{a}{b}\right) = 0$ if a, b are elements of $\mathcal{O}$ not divisible by π. Thus we have a set of pairwise inequivalent valuations on K_0 with value group $\mathbb{Z}$ which is denoted by m_{K_0}. Every valuation in m_{K_0} can be extended in at most d different ways to K. Let m_K denote the set of these extensions.

For any finite subset T of m_K we put

$$\Gamma_T = \{\alpha \in K^*: v(\alpha) = 0 \quad \text{for all} \quad v \in m_K \setminus T\}.$$

Then Γ_T is a multiplicative subgroup of K^* and one can show that it is finitely generated. Moreover, every finitely generated multiplicative subgroup Γ of K^* can be embedded in some subgroup Γ_T of K^*.

Theorem 1. *Let λ, μ be non-zero elements of K, and let T be a finite subset of m_K of cardinality t. Then the number of solutions of* (1) *in $x, y \in \Gamma_T$ is at most $4 \times 7^{3d+2t}$.*

It is a remarkable fact that our bound depends on d and t only. Unfortunately, it depends however on the special choice of the transcendence basis of K over $\mathbb{Q}$. Upper bounds of this type have been previously obtained in the special case that K is an algebraic number field (i.e. $q=0$). Let now K denote an algebraic number field of degree d and with unit rank r, and let Γ_T have the same meaning as above. In 1979, Győry [6] proved under certain additional hypotheses for λ, μ that (1) has at most $r+4t$ solutions in $x, y \in \Gamma_T$. In 1984, Silverman [24] (in case $\lambda=\mu=1$) and Evertse [2] (in full generality) derived the upper bounds $C\times 2^{20(r+t+1)}$ and $3\times 7^{d+2(r+t+1)}$, respectively. Here $r+1\leqq d$ and C denotes some constant depending only on d.

§ 3. On the numbers of solutions of decomposable form equations

Let K be a finitely generated (but not necessarily algebraic) extension field of $\mathbb{Q}$, and let R be a finitely generated subring of K over $\mathbb{Z}$. Let

$$F(\mathbf{X})=F(X_1,\ldots,X_m)\in R[X_1,\ldots,X_m]$$

be a decomposable form of degree $n\geqq 3$ in $m\geqq 2$ variables, that is, suppose that

$$F(\mathbf{X})=L_1(\mathbf{X})\cdots L_n(\mathbf{X}), \tag{2}$$

where $\mathscr{L}_0=\{L_1,\ldots,L_n\}$ is a system of linear forms with coefficients in some finite extension, say G, of K. Further, let $\mathscr{L}$ be a system of linear forms with coefficients in G such that $\mathscr{L}_0\subset\mathscr{L}$ and that there exists an $\mathbf{x}\in K^m$ with $L(\mathbf{x})\neq 0$ for every $L\in\mathscr{L}$. We shall deal with the *decomposable form equation*

$$F(\mathbf{x})=\varepsilon \quad \text{in} \quad \mathbf{x}\in R^m,\ \varepsilon\in R^* \quad \text{with} \quad L(\mathbf{x})\neq 0 \quad \text{for every} \quad L\in\mathscr{L}. \tag{3}$$

If V is some subspace of K^m, we say that the linear forms $l_1,\ldots,l_r$ with coefficients in some extension G' of K are linearly (in)dependent on V if there are (no) $c_1,\ldots,c_r\in G'$, not all zero, such that $c_1l_1+\cdots+c_rl_r$ vanishes identically on V. Let now V be a subspace of K^m, and let $\mathscr{L}_1$ be some non-empty system of linear forms with coefficients in G. By $S(V,\mathscr{L}_1)$ we denote the minimum of all integers r for which there are linear forms $l_1,\ldots,l_r\in\mathscr{L}_1$ which are linearly dependent on V and pairwise linearly independent on V. If this minimum does not exist, we put $S(V,\mathscr{L}_1)=2$.

If (3) is solvable and if R^* is infinite, then (3) has infinitely many solutions. Two solutions $(\mathbf{x}_1,\varepsilon_1)$, $(\mathbf{x}_2,\varepsilon_2)$ of (3) will be called linearly (in)dependent if the vectors $\mathbf{x}_1,\mathbf{x}_2$ are linearly (in)dependent in K^m. (3) may have infinitely many pairwise linearly independent solutions. However, one can show that the maximal number of pairwise linearly independent solutions of (3) is finite whenever $\mathscr{L}_0,\mathscr{L}$ satisfy the following condition: for every subspace V of K^m of dimension $\geqq 2$ on which none of the forms in $\mathscr{L}$ vanishes identically we have $S(V,\mathscr{L}_0)\geqq 3$. This can be proved by showing that for every subspace V of K^m with $\dim V\geqq 2$, the solutions of (3) in V are already contained in finitely many proper subspaces of V. The proof involves finiteness results on unit equations in several variables (cf. Evertse [3] and Schlickewei and van der Poorten [19]) together with some ideas of Laurent [14]. Unfortunately, we are not able to derive an upper bound for the maximal number of pairwise linearly independent solutions of (3) in full generality. We can, however, derive such an upper bound if $\mathscr{L}_0,\mathscr{L}$ satisfy the following stronger condition:

(4) *for every subspace V of K^m of dimension $\geqq 2$ on which none of the forms in $\mathscr{L}$ vanishes identically we have $S(V, \mathscr{L}_0) = 3$.*

Let $\{z_1, \ldots, z_q\}$, K_0, d, m_K have the same meaning as in § 2. Put $g = [G : K]$. Let T be the smallest subset of m_K such that $v(\alpha) \geqq 0$ for all $\alpha \in R$ and $v \in m_K \setminus T$. Then T is finite. Let t denote the cardinality of T.

Theorem 2. *Suppose $\mathscr{L}_0, \mathscr{L}$ satisfy* (4). *Then* (3) *has at most $(4 \times 7^{g(3d+2t)})^{m-1}$ pairwise linearly independent solutions.*

One can show that (4) implies $\operatorname{rank} \mathscr{L}_0 = m$. Together with $S(K^m, \mathscr{L}_0) = 3$ this yields $m < n$. In case that G is the splitting field of F over K, we have $g \leqq n!$.

Condition (4) has the disadvantage that for given systems $\mathscr{L}_0, \mathscr{L}$ of linear forms, it is hard to decide whether (4) is satisfied or not. However, the systems $\mathscr{L}_0, \mathscr{L}$ which will appear in the applications of Theorem 2 in §§ 4 to 6 also satisfy the conditions (a), (b), (c), (d) below, which do not have this disadvantage.

(a) $\mathscr{L} = \mathscr{L}_0 \cup \{X_k\}$ *for some* $k \in \{1, \ldots, m\}$;

(b) $\mathscr{L}_0$ *has* $\operatorname{rank} m$;

(c) $\mathscr{L}_0$ *can be divided into subsystems* $\mathscr{L}_1, \ldots, \mathscr{L}_h$ *such that each* $\mathscr{L}_j$ $(1 \leqq j \leqq h)$ *has the following properties: the cardinality of* $\mathscr{L}_j$ *is at least* 2 *and, for each* i, i' *with* $L_i, L_{i'} \in \mathscr{L}_j$, *there exists a sequence* $L_i = L_{i_1}, \ldots, L_{i_r} = L_{i'}$ *in* $\mathscr{L}_j$ *such that, for* $p = 1, \ldots, r-1$, *a suitable linear combination of* $L_{i_p}, L_{i_{p+1}}$ *with coefficients in* G^* *belongs to* $\mathscr{L}_j$;

(d) *for every* $j \in \{1, \ldots, h\}$, X_k *can be written as a linear combination of the forms from* $\mathscr{L}_j$.

The conditions (a), (b), (c), (d) together imply (4). Indeed, let V be a subspace of K^m of dimension $\geqq 2$ on which none of the forms in $\mathscr{L}$ vanishes identically. If, for each subsystem $\mathscr{L}_j$ $(j = 1, \ldots, h)$, all forms in $\mathscr{L}_j$ are pairwise linearly dependent on V, then, by (a) and (d), all forms in $\mathscr{L}_0$ are linearly dependent on X_k on V. Together with (b) this implies however that $\dim V = 1$, which is a contradiction. Hence at least one subsystem contains two linear forms which are linearly independent on V. But, by (c), this implies that $S(V, \mathscr{L}_0) = 3$. Consequently, Theorem 2 yields the following

Theorem 3. *If $\mathscr{L}_0, \mathscr{L}$ satisfy* (a), (b), (c) *and* (d), *then* (3) *has at most $(4 \times 7^{g(3d+2t)})^{m-1}$ pairwise linearly independent solutions.*

We note that earlier Győry [9], [11] gave an effective analogue of Theorem 3.

We shall now give some interesting consequences of Theorem 2. Theorem 3 has similar consequences. There are only finitely many $v \in m_K \setminus T$ for which $v(\beta) \neq 0$ $(\beta \in K^*)$. In the sequel the number of these v will be denoted by $\omega_T(\beta)$. Further, $F, \mathscr{L}_0, \mathscr{L}$ will have the same meaning as before, in Theorem 2.

Theorem 4. *Let $\beta \in R \setminus \{0\}$. Suppose $\mathscr{L}_0, \mathscr{L}$ satisfy* (4). *Then the number of solutions of the equation*

$$F(\mathbf{x}) = \beta \quad \text{in} \quad \mathbf{x} \in R^m \quad \text{with} \quad L(\mathbf{x}) \neq 0 \quad \text{for} \quad L \in \mathscr{L} \tag{5}$$

is at most $n(4 \times 7^{g(3d+2(t+\omega_T(\beta)))})^{m-1}$.

Theorem 4 follows easily from Theorem 2 (with $R[\beta^{-1}]$ instead of R) on noting that for every solution $\mathbf{x}$ of (5), $\delta\mathbf{x}$ (with $\delta \in K^*$) can be a solution of (5) only if

$$\delta^n = \frac{F(\delta\mathbf{x})}{F(\mathbf{x})} = 1.$$

Similarly, Theorem 3 implies that if $\mathscr{L}_0, \mathscr{L}$ satisfy (a), (b), (c) and (d), then (5) has at most $n(4 \times 7^{g(3d+2(t+\omega_T(\beta)))})^{m-1}$ solutions. For an effective version of this finiteness assertion see Győry [9], [11].

We shall now specialize Theorem 2 to the important special cases that $K = K_0$ (cf. § 2) or that K is an algebraic number field. In both cases, G will denote a finite extension of K of degree g, $F(\mathbf{X}) = F(X_1, \ldots, X_m)$ will be a decomposable form of degree $n \geqq 3$ with coefficients in K which factorizes over G in the form (2), and $m_K, \mathscr{L}_0, \mathscr{L}$ will have the same meaning as in Theorem 2.

First consider the case $K = K_0$. As in § 2, let $\mathcal{O} = \mathbb{Z}[z_1, \ldots, z_q]$, and let $\pi_1, \ldots, \pi_t$ be pairwise non-associated prime elements of $\mathcal{O}$. Since $\mathcal{O}$ is a unique factorization domain, every finite set of elements in $\mathcal{O}$ has a greatest common divisor. By applying Theorem 2 with the ring $R = \mathcal{O}[\pi_1^{-1}, \ldots, \pi_t^{-1}]$ and on noting that $-1, 1$ are the only units in $\mathcal{O}$, we obtain

Corollary 2. 1. *Suppose F has its coefficients in $\mathcal{O}$ and $\mathscr{L}_0, \mathscr{L}$ satisfy* (4). *Then the number of solutions of the equation*

$$F(\mathbf{x}) = \pi_1^{y_1} \cdots \pi_t^{y_t} \quad \text{in} \quad \mathbf{x} = (x_1, \ldots, x_m) \in \mathcal{O}^m, \quad \mathbf{y} = (y_1, \ldots, y_t) \in \mathbb{Z}^t$$
$$\text{with} \quad \gcd(x_1, \ldots, x_m) = \pm 1 \quad \text{and} \quad L(\mathbf{x}) \neq 0 \quad \text{for} \quad L \in \mathscr{L}$$

is at most $2(4 \times 7^{g(2t+3)})^{m-1}$.

Now suppose that K is an algebraic number field of degree d. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be distinct prime ideals in the ring of integers $\mathcal{O}_K$ of K. If $\alpha \in K$, then denote the ideal generated by α by (α). Let $T = \{v_1, \ldots, v_t\}$ be the set of valuations in m_K corresponding to $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, and let $\mathcal{O}_T = \{\alpha \in K: v(\alpha) \geqq 0 \text{ for all } v \in m_K \setminus T\}$ denote the ring of T-integers of K. By applying Theorem 2 with $R = \mathcal{O}_T$ we obtain

Corollary 2. 2. *Suppose F has its coefficients in $\mathcal{O}_K$ and $\mathscr{L}_0, \mathscr{L}$ satisfy* (4). *Then the maximal number of pairwise linearly independent solutions of the equation*

$$(6) \qquad (F(\mathbf{x})) = \mathfrak{p}_1^{y_1} \cdots \mathfrak{p}_t^{y_t} \quad \text{in} \quad \mathbf{x} = (x_1, \ldots, x_m) \in \mathcal{O}_K^m, \quad \mathbf{y} = (y_1, \ldots, y_t) \in \mathbb{Z}^t$$
$$\text{with} \quad L(\mathbf{x}) \neq 0 \quad \text{for} \quad L \in \mathscr{L}$$

is at most $(4 \times 7^{g(3d+2t)})^{m-1}$.

(*Solutions* $(\mathbf{x}_1, \mathbf{y}_1)$, $(\mathbf{x}_2, \mathbf{y}_2)$ *of* (6) *are called linearly (in)dependent if* $\mathbf{x}_1, \mathbf{x}_2$ *are linearly (in)dependent vectors in* K^m.)

In §§ 4 to 6 we shall discuss applications of Theorem 2 to Thue equations, Thue-Mahler equations, discriminant form equations, index form equations and a class of norm form equations. The results we shall present there have obviously similar consequences as Theorem 2 but we shall not state these corollaries explicitely. Further, we remark that all our results established in §§ 4 to 6 can be deduced from our Theorem 3, too.

§ 4. On the numbers of solutions of Thue equations and Thue-Mahler equations

Let K be a finitely generated extension field of $\mathbb{Q}$, and let R be a finitely generated subring of K over $\mathbb{Z}$. Let $F(X_1, X_2) \in R[X_1, X_2]$ be a binary form of degree $n \geqq 3$. F factorizes into linear factors over a finite extension G of K. Suppose that F is divisible by at least three pairwise non-proportional linear forms over G. Let $\{z_1, \ldots, z_q\}$, K_0, d, m_K have the same meaning as in § 2. Further, let $g = [G : K]$, let T be the smallest subset of m_K such that $v(\alpha) \geqq 0$ for all $\alpha \in R$ and $v \in m_K \setminus T$, and let t denote the cardinality of T. Then we have

Theorem 5. *The maximal number of pairwise linearly independent solutions of the equation*

$$F(x_1, x_2) = \varepsilon \quad \text{in} \quad (x_1, x_2) \in R^2, \quad \varepsilon \in R^* \tag{7}$$

is at most $4 \times 7^{g(3d+2t)}$.

(7) is in fact an equation of Thue-Mahler type. Let $\beta \in R \setminus \{0\}$, and let $\omega_T(\beta)$ have the same meaning as in Theorem 4. Then Theorem 5 yields the following consequence for the solutions $x_1, x_2 \in R$ of the Thue equation

$$F(x_1, x_2) = \beta. \tag{8}$$

Theorem 6. *The equation* (8) *has at most* $4n \times 7^{g(3d+2t+2\omega_T(\beta))}$ *solutions in*

$$(x_1, x_2) \in R^2.$$

It follows already from a theorem of Lang [12] (cf. also [13]) that (7) has only finitely many pairwise linearly independent solutions and that (8) has only finitely many solutions. Moreover, in [9], [11], Győry gave effective analogues of Theorems 5 and 6. We note that our bounds in Theorems 5 and 6 do not depend on the coefficients of F.

Consider now the special case when K is an algebraic number field of degree d. Let $\mathcal{O}_K$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, T, $\mathcal{O}_T$ have the same meaning as in Corollary 2. 2, and let

$$F(X_1, X_2) \in \mathcal{O}_K[X_1, X_2]$$

be a binary form of degree n with splitting field G over K. Suppose that F has at least three pairwise non-proportional linear factors over G and that $[G : K] = g$. Let $\beta \in \mathcal{O}_K \setminus \{0\}$, and let $\omega_T(\beta)$ have the same meaning as in Theorem 4. Then it follows from Theorems 6 and 5 that the number of solutions of the Thue equation (8) in $x_1, x_2 \in \mathcal{O}_T$ is at most $4n \times 7^{g(3d+2\omega_T(\beta))}$ and that the number of pairwise linearly independent solutions of the Thue-Mahler equation

$$(F(x_1, x_2)) = \mathfrak{p}_1^{y_1} \cdots \mathfrak{p}_t^{y_t} \quad \text{in} \quad x_1, x_2 \in \mathcal{O}_K, \quad y_1, \ldots, y_t \in \mathbb{Z} \tag{9}$$

is at most $4 \times 7^{g(3d+2t)}$. Previously, Evertse [2] (see also [1]) derived almost the same bounds for the numbers of solutions in $x_1, x_2 \in \mathcal{O}_K$ of (8) and (9) but with n^3 instead of g. We observe that $1 \leqq g \leqq n!$. In case that $n \geqq 3$ and F has non-zero discriminant, Silverman [23] independently showed that (8) has at most $n^{2n^2}(8n^3 d)^{R_F(\beta)}$ solutions in $x_1, x_2 \in \mathcal{O}_T$, however under the restriction that β is relatively n-th power free (cf. [23]) and that $|N_{K/\mathbb{Q}}(\beta)|$ is sufficiently large. Here $R_F(\beta)$ denotes the rank of $J_\beta(K)$ where J_β is the Jacobian variety of the projective plane curve $F(x_1, x_2) = \beta x_3^n$.

In the important particular case $K=\mathbb{Q}$, $R=\mathbb{Z}$, Lewis and Mahler [15] proved in 1961 that if F has non-zero discriminant, $F(1,0)\,F(0,1)\neq 0$, and if $|\beta|$ is sufficiently large, then the number of solutions of (8) in $x_1, x_2 \in \mathbb{Z}$ is less than $(c_1 n)^{\omega_T(\beta)+1}$, where c_1 is an absolute constant. Further, Mahler [16] recently showed, independently of Evertse [1], [2] and Silverman [23], that (8) has at most $32nu(\beta)$ solutions in $x_1, x_2 \in \mathbb{Z}$ with $(x_1, \beta)=(x_2, \beta)=1$, provided that F is irreducible over $\mathbb{Q}$ and that $|\beta|$ is sufficiently large. Here $u(\beta)$ denotes the number of congruence classes $u \pmod{\beta}$ in $\mathbb{Z}$ with $F(u,1)\equiv 0 \pmod{\beta}$. In Evertse [2] a similar, but slightly weaker bound was derived, however without any restriction on β.

§ 5. On the numbers of solutions of norm form equations

Let again K be a finitely generated extension field of $\mathbb{Q}$, and let R be a subring of K which is finitely generated over $\mathbb{Z}$ and which has quotient field K. Further, let M be a finite extension of K of degree $n\geqq 3$, and let G be the normal closure of M over K. There are n K-isomorphisms of M into G; if $\alpha \in M$ then we denote the images of α under these isomorphisms by $\alpha^{(1)}, \ldots, \alpha^{(n)}$. Let $\alpha_1=1, \alpha_2, \ldots, \alpha_m$ $(m\geqq 2)$ be linearly independent elements of M over K. Then

$$N(\alpha_1 X_1+\cdots+\alpha_m X_m)=\prod_{i=1}^{n}(\alpha_1^{(i)}X_1+\cdots+\alpha_m^{(i)}X_m)$$

is a norm form with coefficients in K. There is an $a_0 \in K^*$ such that the form

$$a_0 N(\alpha_1 X_1+\cdots+\alpha_m X_m)$$

has all its coefficients in R. We shall deal with the *norm form equation*

$$(10)\qquad a_0 N(\alpha_1 x_1+\cdots+\alpha_m x_m)=\varepsilon \quad \text{in} \quad x_1, \ldots, x_m \in R, \qquad \varepsilon \in R^*.$$

Let $\{z_1, \ldots, z_q\}$, K_0, d, m_K be the same as in § 2. Put $g=[G:K]$. Let T be the smallest subset of m_K such that $v(\alpha)\geqq 0$ for all $\alpha \in R$ and $v \in m_K \setminus T$, and let t denote the cardinality of T.

Theorem 7. *Suppose that α_m has degree at least 3 over $K(\alpha_1, \ldots, \alpha_{m-1})$. Then the maximal number of pairwise linearly independent solutions of* (10) *with $x_m \neq 0$ is at most $(4\times 7^{g(3d+2t)})^{m-1}$.*

In Theorem 7 the condition that $1, \alpha_2, \ldots, \alpha_m$ are linearly independent over K is necessary. Further, (10) may have infinitely many pairwise linearly independent solutions with $x_m=0$. This is the case if for example $K=\mathbb{Q}$, $R=\mathbb{Z}$, $\beta=1$ and among $1, \alpha_2, \ldots, \alpha_{m-1}$ there is an integral basis of a subfield of M of degree at least 3 over $\mathbb{Q}$.

The following theorem is a consequence of Theorems 7 and 5.

Theorem 8. *Suppose that in* (10) *α_{i+1} has degree at least 3 over $K(\alpha_1, \ldots, \alpha_i)$ for $i=1, \ldots, m-1$. Then the maximal number of pairwise linearly independent solutions of* (10) *is at most $2(4\times 7^{g(3d+2t)})^{m-1}$.*

Theorem 8 can be proved by induction on m. For $m=2$ Theorem 8 is a consequence of Theorem 5. Suppose Theorem 8 has been proved for $m=l-1$ ($l\geqq 3$). Then one can prove Theorem 8 for $m=l$ by estimating the number of solutions of (10) with $x_l=0$ from above by means of the induction hypothesis and by bounding above the number of solutions of (10) with $x_l\neq 0$ by means of Theorem 7.

As the example of Pell equations shows, our Theorems 7, 8 do not remain valid if we lower the bound 3 concerning the degrees of the α_j. Further, we note that in our bounds $3^{m-1}\leqq n$ and $g\leqq n!$.

We mention that earlier Győry [9], [11] proved effective analogues of Theorems 7 and 8. In the special case when K is an algebraic number field, there are a number of other finiteness theorems for norm form equations; for references see [20], [21], [22], [18], [7], [11].

Let V be the K-vector space generated by $1, \alpha_2, \ldots, \alpha_m$. Using the general result on decomposable form equations mentioned in § 3, one can show that (10) has only finitely many pairwise linearly independent solutions if there are no $\mu\in M^*$ and a subfield M' of M with $M'\subsetneqq K$ such that $\mu M'\subset V$. If this condition is not valid, then there are rings R which have quotient field K and which are finitely generated over $\mathbb{Z}$ such that (10) has infinitely many pairwise linearly independent solutions. These facts were proved by Schlickewei [18] in case that $K=\mathbb{Q}$. Earlier, W. M. Schmidt [20] proved, among other things, that in case $R=\mathbb{Z}$ (10) has only finitely many solutions if there are no $\mu\in M^*$ and a subfield M' of M which is different from $\mathbb{Q}$ and the imaginary quadratic number fields such that $\mu M'\subset V$.

§ 6. On discriminant form equations, index form equations and power bases

Let K be a finitely generated extension field of $\mathbb{Q}$, let R be a subring of K which is finitely generated over $\mathbb{Z}$ and suppose that K is the quotient field of R. Let G be a finite extension of K, and let $\mathscr{L}=\{L_1(\mathbf{X}),\ldots,L_n(\mathbf{X})\}$ be a set of distinct linear forms in $\mathbf{X}=(X_1,\ldots,X_m)$ ($m\geqq 2$) which have their coefficients in G. We suppose that $\mathscr{L}$ satisfies the following conditions:

(11) *the form* $\prod_{i=1}^{n}(Y-L_i(\mathbf{X}))$ *has its coefficients in* K;

(12) *the system* $\{X_i\}\cup\{L_i-L_j,\ 1\leqq i<j\leqq n\}$ *has* rank m *over* G *for some* $l\in\{1,\ldots,m\}$.

We notice that (12) is satisfied if rank $\mathscr{L}=m$. By (11) the so-called *discriminant form*

$$D_{\mathscr{L}}(\mathbf{X})=\prod_{1\leqq i<j\leqq n}(L_i(\mathbf{X})-L_j(\mathbf{X}))^2$$

is a decomposable form of degrees $n(n-1)$ with coefficients in K. Let $a_0\in K^*$ be an element such that $a_0D_{\mathscr{L}}(\mathbf{X})$ has its coefficients in R. We shall now deal with the discriminant form equation

$$(13)\qquad a_0D_{\mathscr{L}}(\mathbf{x})=\varepsilon \quad \text{in} \quad \mathbf{x}=(x_1,\ldots,x_m)\in R^m \quad \text{with} \quad x_l=0, \quad \varepsilon\in R^*.$$

Let $\{z_1, \ldots, z_q\}$, K_0, d, m_K have the same meaning as in § 2. Put $g = [G : K]$. Let T be the smallest subset of m_K such that $v(\alpha) \geqq 0$ for all $\alpha \in R$ and $v \in m_K \setminus T$, and let t denote the cardinality of T. Then we have

Theorem 9. *The maximal number of pairwise linearly independent solutions of* (13) *is at most* $(4 \times 7^{g(3d+2t)})^{m-2}$.

Theorem 9 is of particular interest in the following two special cases: (A) $n = m$, $\mathscr{L} = \{X_1, \ldots, X_m\}$ and $l = 1$; and (B) M is a finite extension of K of degree $n \geqq 3$ with normal closure G over K, $1, \alpha_2, \ldots, \alpha_m$ are linearly independent elements of M over K such that $M = K(\alpha_2, \ldots, \alpha_m)$, $l = 1$ and $\mathscr{L} = \{X_1 + \alpha_2^{(i)} X_2 + \cdots + \alpha_m^{(i)} X_m;\ i = 1, \ldots, n\}$ (where $\alpha^{(1)}, \ldots, \alpha^{(n)}$ denote, as in § 5, the images of any $\alpha \in M$ under the K-isomorphisms of M into G). It is obvious that $\mathscr{L}$ has the properties (11), (12) in both cases. Earlier, Győry [9], [11] derived an effective analogue of Theorem 9 in cases (A) and (B). We notice that in cases (A) and (B) Theorem 9 can be applied to derive upper bounds for the number of polynomials of given discriminant and for the number of integral elements of given discriminant, respectively. We shall deal with these problems in a separate joint paper. Further, in case (B), Theorem 9 implies results on index form equations and power bases. We shall now present these consequences.

Suppose now that R is integrally closed in K. Let M be a finite extension of K of degree $m \geqq 2$ in G and assume that G is the normal closure of M over K. Let R' be an integral extension ring of R in M and suppose that R' is a free R-module having a basis of the form $\{\omega_1 = 1, \omega_2, \ldots, \omega_m\}$. This assumption holds in many important cases, see e.g. [11]. Let $\mathscr{L} = \{X_1 + \omega_2^{(i)} X_2 + \cdots + \omega_m^{(i)} X_m;\ i = 1, \ldots, m\}$, and let $D(\omega_1, \ldots, \omega_m)$ be the discriminant of the basis $\{\omega_1, \ldots, \omega_m\}$ over K. Then $\mathscr{L}$ has the properties (11), (12); cf. case (B). It is easy to see that there exists a form $F(X_2, \ldots, X_m)$ with coefficients in R such that

$$D_{\mathscr{L}}(\mathbf{X}) = D(\omega_1, \ldots, \omega_m)\,[F(X_2, \ldots, X_m)]^2. \tag{14}$$

The form F is called the index form of the basis $\{\omega_1, \ldots, \omega_m\}$ over R. Consider now the *index form equation*

$$F(x_2, \ldots, x_m) = \varepsilon \quad \text{in} \quad (x_2, \ldots, x_m) \in R^{m-1}, \quad \varepsilon \in R^*. \tag{15}$$

Let d, g and t be the same as in Theorem 9. By applying Theorem 9 with the above $\mathscr{L}$ and with $a_0 = D(\omega_1, \ldots, \omega_m)^{-1}$ we obtain

Theorem 10. *The maximal number of pairwise linearly independent solutions of* (15) *is at most* $(4 \times 7^{g(3d+2t)})^{m-2}$.

In [8] Győry already showed that (15) has only finitely many pairwise linearly independent solutions and in [9], [11] he gave effective versions of this finiteness assertion.

Let R be as above, and let now R' be an arbitrary integral extension ring of R in M with quotient field M. Then $R' = R[\alpha]$ holds with some $\alpha \in R'$ if and only if $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis of R' as an R-module. Such a basis is called a power basis over R. We call two elements α, β of R' R-equivalent if there are $a \in R$, $u \in R^*$ such that $\beta = u\alpha + a$. If this is the case, then $R' = R[\alpha]$ implies $R' = R[\beta]$ and conversely. Since we want to derive an upper bound for the number of power bases, we may suppose without loss of generality that there exists an $\alpha_0 \in R'$ for which $R' = R[\alpha_0]$. Let $F(X_2, \ldots, X_m)$ be the index form of the basis $\{1, \alpha_0, \ldots, \alpha_0^{m-1}\}$ of R' as an R-module.

For any $\alpha \in R'$ there are uniquely determined elements $x_1, \ldots, x_m$ of R such that $\alpha = x_1 + x_2\alpha_0 + \cdots + x_m\alpha_0^{m-1}$. More generally, there are $x_{ij} \in R$ $(1 \leqq i, j \leqq m)$ with $x_{2j} = x_j$ for $j = 1, \ldots, m$ such that $\alpha^{i-1} = x_{i1} + x_{i2}\alpha_0 + \cdots + x_{im}\alpha_0^{m-1}$. Let $\Delta = \det(x_{ij})$. Then $R' = R[\alpha]$ if and only if $\Delta \in R^*$. This together with

$$D(1, \alpha, \ldots, \alpha^{m-1}) = \Delta^2 D(1, \alpha_0, \ldots, \alpha_0^{m-1})$$

and (14) yields the following equivalence:

$$\{1, \alpha, \ldots, \alpha^{m-1}\} \text{ is a basis of } R' \text{ as an } R\text{-module} \Leftrightarrow F(x_2, \ldots, x_m) \in R^*.$$

Further, putting $\beta = y_1 + y_2\alpha_0 + \cdots + y_m\alpha_0^{m-1}$ with $y_1, \ldots, y_m \in R$, α and β are R-equivalent if and only if the vectors $(x_2, \ldots, x_m)$, $(y_2, \ldots, y_m)$ are linearly dependent in K^{m-1} and $F(x_2, \ldots, x_m)/F(y_2, \ldots, y_m) \in R^*$. Hence by Theorem 10 we have

Theorem 11. *Those elements α of R' for which $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis of R' as an R-module belong to at most $(4 \times 7^{g(3d+2t)})^{m-2}$ R-equivalence classes.*

If in particular K is an algebraic number field and if R is its ring of integers, then $t = 0$. In this special case Theorem 11 gives

Corollary 11. 1. *Let K be an algebraic number field of degree d, let M be a finite extension of K of degree $m \geqq 2$, let G be the normal closure of M over K, let $g = [G : K]$, and let $\mathcal{O}_K$, $\mathcal{O}_M$ denote the rings of integers of K and M, respectively. Then those elements $a \in \mathcal{O}_M$ for which $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_M$ belong to at most $(4 \times 7^{3gd})^{m-2}$ $\mathcal{O}_K$-equivalence classes.*

We note that in Theorems 10, 11 and Corollary 11. 1 we have $g \leqq m!$.

Effective versions of Theorem 11 and Corollary 11. 1 were earlier obtained by Győry [5], [10].

§ 7. Proof of Theorem 1

In the proof of Theorem 1, K, K_0, $\{z_1, \ldots, z_q\}$, d, $\mathcal{O}$, m_K, T, t, Γ_T will have the same meaning as in § 2. Further, $\mathbb{K}$ will denote the algebraic closure of $\mathbb{Q}$ in K. We divide m_K into two subsets: $m_K^{(1)}$ will denote the set of valuations in m_K whose restrictions to $\mathcal{O}$ correspond to rational primes and, if $q > 0$, $m_K^{(2)}$ will denote the set of valuations in m_K whose restrictions to $\mathcal{O}$ correspond to primitive non-constant irreducible polynomials.

We shall also need some notations about absolute values (i.e. non-trivial multiplicative valuations). An equivalence class of absolute values on some field will be called a *prime*. If V_1, V_2 are primes on the fields K_1, K_2 respectively and if $K_1 \subset K_2$, we say that V_2 *lies above* V_1 or that V_1 *lies below* V_2 if V_1 consists of the restrictions of the absolute values in V_2 to K_1. To every valuation $v \in m_K$ corresponds a prime

$$\{C^{-v(\cdot)} \colon C \in \mathbb{R},\ C > 1\}.$$

Let $S_{\mathbb{K}}$ denote the set of primes on $\mathbb{K}$ lying below the primes on K corresponding to the valuations in $m_K^{(1)}$ and let S_K denote the set of primes on K corresponding to the valuations in $m_K^{(2)}$. Further, let $I_{\mathbb{K}}$ denote the set of primes on $\mathbb{K}$ lying above the prime on $\mathbb{Q}$ containing the ordinary absolute value. Denote by I_K the set of primes on K lying above the prime on K_0 which contains the absolute value $|.|_\infty$ defined by $|F_1/F_2|_\infty = e^{b-a}$ for every pair of non-zero polynomials $F_1, F_2 \in \mathbb{C}$ with total degrees a, b respectively. Since $[\mathbb{K}:\mathbb{Q}] \leqq d$ and $[K:K_0] \leqq d$, $I_{\mathbb{K}}$ and I_K have cardinalities at most d. Put

$$M_{\mathbb{K}} = I_{\mathbb{K}} \cup S_{\mathbb{K}}, \quad M_K = I_K \cup S_K.$$

One can show (cf. [4]) that there exist sets of absolute values $\{|.|_V\}_{V \in M_{\mathbb{K}}}$, $\{|.|_V\}_{V \in M_K}$ such that

$$\prod_{V \in M_{\mathbb{K}}} |\alpha|_V = 1 \text{ for } \alpha \in \mathbb{K}, \quad \prod_{V \in M_K} |\alpha|_V = 1 \text{ for } \alpha \in K^*.$$

Let α_1, β_1 be elements of $\mathbb{K}^*$, let α_2, β_2 be elements of K^*, and let S_1, S_2 be finite subsets of $M_{\mathbb{K}}, M_K$ respectively and of cardinalities s_1, s_2 respectively such that $I_{\mathbb{K}} \subset S_1$, $I_K \subset S_2$. Define the sets $U_{S_1}^{(1)}, U_{S_2}^{(2)}$ by

$$U_{S_1}^{(1)} = \{\alpha \in \mathbb{K}: |\alpha|_V = 1 \quad \text{for all} \quad V \in M_{\mathbb{K}} \setminus S_1\},$$
$$U_{S_2}^{(2)} = \{\alpha \in K: |\alpha|_V = 1 \quad \text{for all} \quad V \in M_K \setminus S_2\}.$$

Consider the equations

$$\alpha_1 x + \beta_1 y = 1 \quad \text{in} \quad x, y \in U_{S_1}^{(1)} \tag{16}$$

and

$$\alpha_2 x + \beta_2 y = 1 \quad \text{in} \quad x, y \in U_{S_2}^{(2)} \quad \text{with} \quad \alpha_2 x \notin \mathbb{K}, \quad \beta_2 y \notin \mathbb{K}. \tag{17}$$

Lemma 1. (i) *The equation* (16) *has at most* $3 \times 7^{d+2s_1}$ *solutions.*

(ii) *The equation* (17) *has at most* 2×7^{2s_2} *solutions.*

Proof. (i), (ii) are consequences of Theorem 1 of [2] and Theorem 2 of [4], respectively. □

Proof of Theorem 1. Let T_1 be the set of primes in $S_{\mathbb{K}}$ lying below the primes on K which correspond to the valuations in $m_K^{(1)} \cap T$. Let further T_2 be the set of primes in S_K which correspond to the valuations in $m_K^{(2)} \cap T$. Let t_i denote the cardinality of T_i for $i = 1, 2$. Then $t_1 + t_2 \leqq t$.

First of all, we shall give an upper bound for the number of solutions of (1) in $x, y \in \Gamma_T$ for which $\lambda x \in \mathbb{K}$, $\mu y \in \mathbb{K}$. Suppose that such solutions do exist and let (x_0, y_0) be such a solution. It clearly suffices to prove Theorem 1 with $\lambda' = \lambda x_0$, $\mu' = \mu y_0$ instead of λ, μ. Hence it is no restriction to assume that $\lambda, \mu \in \mathbb{K}$ and we shall do so in the sequel. Then (x, y) is a solution of (1) with $x, y \in \Gamma_T$ and $\lambda x, \mu y \in \mathbb{K}$ if and only if $x, y \in \Gamma_T \cap \mathbb{K}^*$. But we have $\Gamma_T \cap \mathbb{K}^* \subset U_{S_1}^{(1)}$, where $S_1 = I_{\mathbb{K}} \cup T_1$. By Lemma 1, (i) and since S_1 has cardinality at most $d + t_1$, the number of solutions (x, y) of (1) with $x, y \in \Gamma_T$ and $\lambda x, \mu y \in \mathbb{K}$ is at most $3 \times 7^{3d+2t_1}$.

Now we estimate the number of solutions of (1) in $x, y \in \Gamma_T$ for which $\lambda x,\ \mu y \notin \mathbb{K}$. Let $S_2 = I_K \cup T_2$. Then S_2 has cardinality at most $d + t_2$. Hence by Lemma 1, (ii) and since $\Gamma_T \subset U_{S_2}^{(2)}$, the number of solutions of (1) in $x, y \in \Gamma_T$ for which $\lambda x,\ \mu y \notin \mathbb{K}$ is at most $2 \times 7^{2d+2t_2}$. Therefore, the total number of solutions of (1) in $x, y \in \Gamma_T$ is at most

$$3 \times 7^{3d+2t_1} + 2 \times 7^{2d+2t_2} \leqq 4 \times 7^{3d+2t}. \quad \square$$

§ 8. Proofs of Theorems 2, 5, 7 and 9

K, G, $\{z_1, \ldots, z_q\}$, K_0, d, m_K, R, T, t will have the same meaning as in § 3. Let m_G and T' denote the sets of all inequivalent extensions to G of the valuations of m_K and of T, respectively. Further, let $\Gamma_{T'}$ denote the group $\{\alpha \in G\colon v(\alpha) = 0 \text{ for } v \in m_G \setminus T'\}$.

Lemma 2. *Let $\mathscr{L}_0, \mathscr{L}$ be non-empty systems of linear forms with coefficients in G in the variables $\mathbf{X} = (X_1, \ldots, X_m)$ $(m \geqq 1)$ such that $\mathscr{L}_0 \subset \mathscr{L}$ and such that for every subspace V of K^m of dimension $\geqq 2$ on which none of the forms in $\mathscr{L}$ vanishes identically we have $S(V, \mathscr{L}_0) = 3$. Let W be a subspace of K^m of dimension $p \geqq 1$. Then the maximal number of pairwise linearly independent vectors $\mathbf{x} = (x_1, \ldots, x_m) \in W$ for which*

$$(18) \qquad L(\mathbf{x}) \in \Gamma_{T'} \text{ for } L \in \mathscr{L}_0 \text{ and } L(\mathbf{x}) \neq 0 \text{ for } L \in \mathscr{L} \setminus \mathscr{L}_0$$

is at most $(4 \times 7^{g(3d+2t)})^{p-1}$.

Proof. For convenience we put $N = 4 \times 7^{g(3d+2t)}$. We shall proceed by induction on p. For $p = 1$ Lemma 2 is trivial. Suppose now that $p \geqq 2$. We shall show that W contains at most N^{p-1} pairwise linearly independent solutions of (18), provided that every subspace of W of dimension $p-1$ contains at most N^{p-2} pairwise linearly independent solutions of (18).

We assume that none of the forms in $\mathscr{L}$ vanishes identically on W which is obviously no restriction. Then $S(W, \mathscr{L}_0) = 3$. Hence there are linear forms $L_1(\mathbf{X})$, $L_2(\mathbf{X})$, $L_3(\mathbf{X}) \in \mathscr{L}_0$ as well as constants $\lambda, \mu \in G^*$ such that L_1, L_2, L_3 are pairwise linearly independent on W and $\lambda L_1(\mathbf{x}) + \mu L_2(\mathbf{x}) = L_3(\mathbf{x})$ for all $\mathbf{x} \in W$. Let $\mathbf{x} \in W$ be a solution of (18). Then $(L_1(\mathbf{x})/L_3(\mathbf{x}), L_2(\mathbf{x})/L_3(\mathbf{x}))$ is a solution of $\lambda x + \mu y = 1$ in $x, y \in \Gamma_{T'}$. Since $[G : K_0] = gd$ and T' has cardinality at most gt, this implies together with Theorem 1 that $L_1(\mathbf{x})/L_3(\mathbf{x})$ belongs to a set of cardinality at most N which does not depend on $\mathbf{x}$. But since L_1, L_3 are linearly independent on W, the vectors $\mathbf{x} \in W$ for which $L_1(\mathbf{x})/L_3(\mathbf{x})$ assumes some fixed value belong to a fixed subspace of W of dimension $p-1$. Hence the solutions of (18) which belong to W are already contained in at most N subspaces of W of dimension $p-1$. Together with the induction hypothesis this shows indeed that W contains at most N^{p-1} pairwise linearly independent solutions of (18). $\square$

Proof of Theorem 2. Let $L_1, \ldots, L_n$ be the linear forms appearing in (2), let $\mathscr{L}_0 = \{L_1, \ldots, L_n\}$ and let $\mathscr{L} \supset \mathscr{L}_0$ be the system appearing in Theorem 2. Assume that $\mathscr{L}_0, \mathscr{L}$ satisfy (4). We shall show that there are constants $c_1, \ldots, c_n \in G^*$ with $c_1 \cdots c_n = 1$ such that the forms $L_i' = c_i L_i$ $(i = 1, \ldots, n)$ have the following property: if $(\mathbf{x}, \varepsilon) \in R^m \times R^*$ is a solution of (3) then $L_i'(\mathbf{x}) \in \Gamma_{T'}$ for $i = 1, \ldots, n$. On noting that the systems

$$\mathscr{L}_0' = \{L_1', \ldots, L_n'\}, \quad \mathscr{L}' = \mathscr{L}_0' \cup (\mathscr{L} \setminus \mathscr{L}_0)$$

also satisfy (4), Theorem 2 will then follow by applying Lemma 2 to $\mathscr{L}_0', \mathscr{L}'$ with $W = K^m$.

Let $v \in m_G$. For every polynomial $P \in G[x_1, \ldots, x_m]$, denote by $v(P)$ the minimum of the v-values of the coefficients of P. Then it is known (cf. [13]) that if

$$P, Q \in G[x_1, \ldots, x_m]$$

then

$$v(PQ) = v(P) + v(Q) \quad \text{for} \quad v \in m_G. \tag{19}$$

We may obviously assume that (3) is solvable. Let $v \in m_G \setminus T'$. Then by (19) and the fact that $v(\alpha) \geqq 0$ for $\alpha \in R$ and $v(\alpha) = 0$ for $\alpha \in R^*$, we have for every solution $(\mathbf{x}, \varepsilon)$ of (3) that both

$$\sum_{i=1}^{n} \{v(L_i(\mathbf{x})) - v(L_i)\} = v(F(\mathbf{x})) - v(F) = v(\varepsilon) - v(F) \leqq 0$$

and

$$v(L_i(\mathbf{x})) - v(L_i) \geqq 0 \quad \text{for} \quad i = 1, \ldots, n.$$

Hence

$$v(L_i(\mathbf{x})) = v(L_i) \quad \text{for} \quad i = 1, \ldots, n, \quad v \in m_G \setminus T'. \tag{20}$$

Let $(\mathbf{x}_0, \varepsilon_0)$ be a fixed solution of (3). Put $c_1 = \varepsilon_0 L_1(\mathbf{x}_0)^{-1}$, $c_i = L_i(\mathbf{x}_0)^{-1}$ for $i = 2, \ldots, n$ and $L_i'(\mathbf{x}) = c_i L_i(\mathbf{x})$ $(i = 1, \ldots, n)$. Then $c_1 \cdots c_n = 1$. Moreover, we have by (20) and $R^* \subset \Gamma_{T'}$ that for every solution $(\mathbf{x}, \varepsilon)$ of (3), $v(L_i'(\mathbf{x})) = 0$ for all $v \in m_G \setminus T'$ and hence $L_i'(\mathbf{x}) \in \Gamma_{T'}$ for $i = 1, \ldots, n$. This completes the proof of Theorem 2. □

Proof of Theorem 5. Theorem 5 follows immediately from Theorem 2 by observing that for the system $\mathscr{L}_0$ of linear factors of the binary form $F(X_1, X_2)$ we have $S(K^2, \mathscr{L}_0) = 3$. □

Proof of Theorem 7. We shall use the same notations as in § 5. Further, we put $L^{(i)}(\mathbf{X}) = \alpha_1^{(i)} X_1 + \cdots + \alpha_m^{(i)} X_m$ $(i = 1, \ldots, n)$, $\mathscr{L}_0 = \{L^{(1)}, \ldots, L^{(n)}\}$, $\mathscr{L} = \mathscr{L}_0 \cup \{X_m\}$. To apply Theorem 2 to the equation (10) it suffices to show that $\mathscr{L}_0, \mathscr{L}$ satisfy (4). Let V be a subspace of K^m of dimension $\geqq 2$ on which none of the forms in $\mathscr{L}$ vanishes identically. Divide $\mathscr{L}_0$ into classes in such a way that two forms belong to the same class if and only if their coefficients of $X_1, \ldots, X_{m-1}$ are equal. Since by assumption α_m is of degree at least 3 over $K(\alpha_1, \ldots, \alpha_{m-1})$, each class contains at least three forms which are pairwise linearly independent. Further, any three linear forms in the same class are linearly dependent. At least one of the classes mentioned above must contain three forms which are pairwise linearly independent on V. For if this is not the case, then all linear forms in $\mathscr{L}_0$ are linearly dependent on X_m on V which implies, in view of rank $\mathscr{L}_0 = m$, that $\dim V = 1$. But this contradicts our assumption. Therefore, $S(V, \mathscr{L}_0) = 3$. Now Theorem 7 follows immediately from Theorem 2. □

Proof of Theorem 9. For $m = 2$ the assertion is trivial, hence we suppose that $m \geqq 3$. We shall use the same notations as in § 6. Thus $\mathscr{L} = \{L_1(\mathbf{X}), \ldots, L_n(\mathbf{X})\}$ is a system of linear forms with coefficients in G satisfying (11), (12). Denote by $L_1', \ldots, L_n'$ the forms which are obtained from $L_1, \ldots, L_n$ by putting $X_l = 0$. Let $\mathscr{L}_0$ denote the system

$$\{L_i' - L_j';\ 1 \leqq i < j \leqq n\}.$$

Then $\mathscr{L}_0$ consists of forms in $m-1$ variables and, by (12), $\mathscr{L}_0$ has rank $m-1$. Let V be a subspace of K^{m-1} of dimension $\geqq 2$ on which none of the forms in $\mathscr{L}_0$ vanishes identically. On noting that $\mathscr{L}_0$ is spanned by the linear forms $L_1' - L_j'$ $(j=2,\ldots,n)$ and that rank $\mathscr{L}_0 = m-1$, there must be two integers $i, j \in \{2,\ldots,n\}$ with $i \neq j$ such that $L_1' - L_i'$, $L_1' - L_j'$ are linearly independent on V. Since $(L_1' - L_i') - (L_1' - L_j') + (L_i' - L_j') = 0$, it follows that $S(V, \mathscr{L}_0) = 3$. Now Theorem 9 is an immediate consequence of Theorem 2. □

Acknowledgements. The second named author would like to take this opportunity to thank Professor R. Tijdeman and the University of Leiden for their hospitality during his stay in the Netherlands.

References

[1] *J. H. Evertse*, Upper bounds for the numbers of solutions of diophantine equations, MC-tract **168**, Amsterdam 1983.
[2] *J. H. Evertse*, On equations in S-units and the Thue-Mahler equation, Invent. Math. **75** (1984), 561—584.
[3] *J. H. Evertse*, On sums of S-units and linear recurrences, Comp. Math. **53** (1984), 225—244.
[4] *J. H. Evertse*, On equations in two S-units over function fields of characteristic zero, Acta Arith., to appear.
[5] *K. Győry*, On polynomials with integer coefficients and given discriminant. IV, Publ. Math. Debrecen **25** (1978), 155—167.
[6] *K. Győry*, On the number of solutions of linear equations in units of an algebraic number field, Comm. Math. Helv. **54** (1979), 583—600.
[7] *K. Győry*, Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers in Pure and Applied Math. **56**, Kingston, Canada 1980.
[8] *K. Győry*, On certain graphs associated with an integral domain and their applications to diophantine problems, Publ. Math. Debrecen **29** (1982), 79—94.
[9] *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.
[10] *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.
[11] *K. Győry*, On norm form, discriminant form and index form equations, Coll. Math. Soc. J. Bolyai **34**, Topics in Classical Number Theory, to appear.
[12] *S. Lang*, Integral points on curves, Inst. Hautes Études Sci. Publ. Math. **6** (1960), 27—43.
[13] *S. Lang*, Fundamentals of diophantine geometry, Berlin-Heidelberg-New York 1983.
[14] *M. Laurent*, Équations diophantiennes exponentielles, C. R. Acad. Sci. Paris **296** (1983), 945—947.
[15] *D. J. Lewis* and *K. Mahler*, Representation of integers by binary forms, Acta Arith. **6** (1960/61), 333—363.
[16] *K. Mahler*, On Thue's theorem, Math. Scand., to appear.
[17] *P. Roquette*, Einheiten und Divisorenklassen in endlich erzeugbaren Körpern, Jber. Deutsch. Math. Verein. **60** (1957), 1—21.
[18] *H. P. Schlickewei*, On norm form equations, J. Number Theory **9** (1977), 370—380.
[19] *H. P. Schlickewei* and *A. J. van der Poorten*, The growth conditions for recurrence sequences, to appear.
[20] *W. M. Schmidt*, Linearformen mit algebraischen Koeffizienten. II, Math. Ann. **191** (1971), 1—20.
[21] *W. M. Schmidt*, Approximation to algebraic numbers, Enseignement Math. **17** (1971), 187—253.
[22] *W. M. Schmidt*, Diophantine approximation, Lecture Notes in Math. **785**, Berlin-Heidelberg-New York 1980.
[23] *J. H. Silverman*, Representations of integers by binary forms and the rank of the Mordell-Weil group, Invent. Math. **74** (1983), 281—292.
[24] *J. H. Silverman*, Quantitative results in diophantine geometry, preprint, Cambridge, Massachusetts 1983.

Centre of Mathematics and Computer Science, PO Box 4079, 1009 AB Amsterdam, The Netherlands

Kossuth Lajos University, Mathematical Institute, 4010 Debrecen, Hungary

Eingegangen 9. März 1984, in revidierter Fassung 1. August 1984