Astérisque

KÁLMÁN GYÖRY

Some recent applications of S-unit equations

Astérisque, tome 209 (1992), p. 17-38

<http://www.numdam.org/item?id=AST_1992__209__17_0>

SOME RECENT APPLICATIONS OF S-UNIT EQUATIONS

Kálmán GYŐRY *

§ 1. Introduction

In 1988, we published with Evertse, Stewart and Tijdeman [11] a long survey article on S-unit equations and their applications. Since then much progress has been made in this fertile field. The purpose of this paper is to give a survey of some recent developments. In § 2, known finiteness theorems (cf. Theorems A, B) and some recent quantitative results (cf. Theorems 1, 2 and 3) are presented for S-unit equations. The proofs of Theorems A and 1 to 3 depend on the Thue-Siegel-Roth-Schmidt method and its p-adic generalization. §§ 3 to 6 are devoted to recent applications of the mentioned results. In § 3, finiteness theorems are established for certain arithmetic graphs (cf. Theorem 4) and irreducible polynomials of the form $g(f(X))$ (cf. Theorem 5). These are considerable improvements of earlier theorems obtained in this direction, and furnish definitive results in a sense. The results of Schinzel and the author in § 4 (cf. Theorem 6) resolve a conjecture of Posner and Rumsey [28] on common polynomial divisors of trinomials. § 5 is concerned with generalizations for decomposable form equations (cf. Theorem 7, 8) of finiteness theorems of Schmidt [34], Schlickewei [30] and Laurent [25] on families of solutions of norm form equations. Uniform upper bounds are given for the number of families of solutions. As a consequence, bounds are derived for the number of solutions, provided that this number is finite (cf. Corollary 1).

---

* Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

A further consequence is deduced in § 6 for some generalized systems of S-unit equations (cf. Theorem 9). It provides, over number fields, a quantitative version of a more general result of Laurent [25].

The results treated in §§ 2 to 6 are all ineffective. Baker's effective method and its p-adic analogue made it possible to establish an effective finiteness theorem (cf. Theorem C in § 7) for S-unit equations in two unknowns. As a recent application of Theorem C, in § 8 an effective finiteness theorem (cf. Theorem 10) of Evertse and the author is presented for decomposable forms of given discriminant. It makes effective in a more general form an ineffective theorem of Birch and Merriman [2] on binary forms. Apart from certain particular cases, no effective results are known for S-unit equations in more than two unknowns. In § 7 we state a generalization of Baker's type inequalities (cf. Proposition) whose effective resolution would imply effective versions of all results of this paper.

Theorems A, B and C were already treated in [11], while Theorems 1 to 10 have been obtained since 1988. The complete proofs of Theorems 4 to 8 and 10 will be published in Győry [18, Part II], [14, Part IV], [20], Győry and Schinzel [21] and Evertse and Győry [9], [10].

It is impossible to deal with all recent applications of unit equations within the frame of the present paper. Further applications have recently been obtained for instance to diophantine equations and irreducible polynomials of other type, modular forms, pairs of polynomials and binary forms of given resultant, recurrence sequences, group theory, algebraic number theory and transcendental number theory. Some generalizations and analogues have also been established over finitely generated domains and function fields, respectively.

§ 2. S-unit equations; ineffective results

We introduce some notation which will be used throughout this paper. Let K be an algebraic number field, O_K the ring of integers of K, and O_K^* the unit group[1] of O_K. Further, let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ be a finite set of prime ideals in O_K, and put

$$O_S = \{\alpha \in K : \ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \ \text{ for all prime ideals } \mathfrak{p} \text{ of } O_K \text{ with } \mathfrak{p} \notin S\}.$$

Then O_S is a subring of K which is called the ring of S-integers. It contains O_K as a subring. The units of O_S, i.e. the invertible elements are called S-units.

---

[1] In general, if R is an integral domain then R^* will denote its group of units; thus if R is a field then $R^* = R \setminus \{0\}$.

They form a multiplicative group which is denoted by O_S^*. Put $d = [K : \mathbb{Q}]$ and $s = r + t + 1$ where r denotes the unit rank of O_K^*. Thus $r \leq d - 1$.

Many problems of number theory can be reduced to equations of the form

$$\alpha_1 x_1 + \alpha_2 x_2 = 1 \ \text{ in } \ x_1, x_2 \in O_S^* \tag{1}$$

or, more generally,

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 1 \ \text{ in } \ x_1, \ldots, x_n \in O_S^* \tag{2}$$

where $\alpha_1, \ldots, \alpha_n$ are elements of K^*. Equation (2) is called an *S-unit equation in n unknowns*. For $n > 2$, it can happen that for a solution $x_1, \ldots, x_n$, the left hand side of (2) has a vanishing subsum. In this case the solution is called *degenerate*, otherwise *non-degenerate*. If (2) has a degenerate solution and if O_S^* is infinite then (2) has infinitely many solutions. Denote by $\mu_n(\alpha_1, \ldots, \alpha_n)$ the number of non-degenerate solutions of (2). Several results have been obtained on $\mu_n(\alpha_1, \ldots, \alpha_n)$; for references see [37] and [11]. Using the Thue-Siegel-Roth-Schmidt method, van der Poorten and Schlickewei [26] (see also [27]) and Evertse [3] proved independently of each other the following

THEOREM A. *For $n \geq 2$ we have $\mu_n(\alpha_1, \ldots, \alpha_n) < \infty$.*

The next quantitative result was established by Evertse [4].

THEOREM B. *We have*

$$\mu_2(\alpha_1, \alpha_2) \leq 3 \times 7^{d+2s}. \tag{3}$$

In 1988, we derived with Evertse [7] an upper bound for $\mu_n(\alpha_1, \ldots, \alpha_n)$ which is independent of $\alpha_1, \ldots, \alpha_n$. Recently this has been made explicit by Schlickewei [31] who proved

THEOREM 1. *For $n \geq 2$, we have*

$$\mu_n(\alpha_1, \ldots, \alpha_n) \leq \exp\{2^{36nd!} \cdot s^6 \log(4sd!)\}. \tag{4}$$

Further, if K is a normal extension of $\mathbb{Q}$ then d! can be replaced by d.

The proof is based on Schlickewei's p-adic generalization [32] of the quantitative Subspace Theorem of Schmidt [35]. Very recently Evertse (private communication) has improved (4) in terms of d to

$$(5) \qquad \mu_n(\alpha_1,\dots,\alpha_n) \le \exp\{2^{37nd} \cdot s^6 \log(8sd!)\}.$$

The dependence on d is much weaker in (4) and (5) than in (3). Probably s^6 can be improved to s.

We call two n-tuples $(\alpha_1,\dots,\alpha_n)$ and $(\alpha_1',\dots,\alpha_n')$ in $(K^*)^n$ (and the corresponding S-unit equations) *S-equivalent* if $\alpha_i'/\alpha_i \in O_S^*$ for $i=1,\dots,n$. If $(\alpha_1,\dots,\alpha_n)$ and $(\alpha_1',\dots,\alpha_n')$ are S-equivalent then $\mu_n(\alpha_1,\dots,\alpha_n) = \mu_n(\alpha_1',\dots,\alpha_n')$. We showed with Evertse, Stewart and Tijdeman [12] (see also [11]) that $\mu_2(\alpha_1,\alpha_2) \le 2$ for all but finitely many S-equivalence classes of pairs $(\alpha_1,\alpha_2) \in (K^*)^2$. Further, we pointed out that if O_S^* is infinite then there are infinitely many S-equivalence classes of pairs (α_1,α_2) for which (1) has two solutions. The proof of the above estimate depends among other things on the fact that $\mu_n := \mu_n(1,1,\dots,1)$ is finite for all $n \le 5$. Following the proof of [12] it is easy to show that apart from at most $\mu_5 + 12\mu_3 + 30\mu_2^2$ S-equivalence classes of pairs (α_1,α_2), we have $\mu_2(\alpha_1,\alpha_2) \le 2$ (see e.g. [19] or [21]). Hence, in view of Theorem 1, the above-mentioned result of [12] can be stated in the following quantitative form.

THEOREM 2. *Apart from at most*

$$\exp\{2^{180d!} \cdot s^6 \log(2(4sd!))\}$$

S-equivalence classes of pairs $(\alpha_1,\alpha_2) \in (K^*)^2$, we have $\mu_2(\alpha_1,\alpha_2) \le 2$. Further, if K is a normal extension of $\mathbb{Q}$ then $d!$ can be replaced by d.

It was shown in [12] that for $n > 2$, there can exist infinitely many S-equivalence classes of equations (2) with "many" non-degenerate solutions. Hence Theorem 2 cannot be generalized in this sense to solutions of (2). There is, however, another possibility for generalization. Denote by $\nu_n(\alpha_1,\dots,\alpha_n)$ the minimal number of $(n-1)$-dimensional linear subspaces of K^n whose union contains all solutions of (2). Theorem 1 implies an upper bound for $\nu_n(\alpha_1,\dots,\alpha_n)$. In 1988, we proved with Evertse [7] that apart from finitely many S-equivalence classes of equations (2), $\nu_n(\alpha_1,\dots,\alpha_n) < 2^{(n+1)!}$ holds. Recently, Evertse [5] improved this bound to $(n!)^{2n+2}$, and applied his estimate to decomposable form equations.

Following the proof of [7], one can derive $\mu_{(n+1)!-1}^{n-1}$ as an upper bound for the number of exceptional S-equivalence classes in question. Together with Theorem 1 this implies that the result of [7] under consideration can now be enunciated in the following quantitative form.

THEOREM 3. *Apart from at most*

$$\exp\{n2^{36(n+1)!d!}\cdot s^6\log(4sd!)\}$$

S-equivalence classes of n-tuples $(\alpha_1,\dots,\alpha_n)\in(K^*)^n$, we have $\nu_n(\alpha_1,\dots,\alpha_n)<2^{(n+1)!}$. Further, if K is a normal extension of $\mathbb{Q}$ then $d!$ can be replaced by d.

For $n=2$, $\nu_2(\alpha_1,\alpha_2)=\mu_2(\alpha_1,\alpha_2)$ holds. Thus, for $n=2$, Theorem 3 gives a weaker version of Theorem 2. The proof of Theorem 3 will be published in a joint paper with Tijdeman, together with some generalizations and further related results.

It is likely that combining the proof of [5] with Theorem 1, the bound $2^{(n+1)!}$ in Theorem 3 can be improved to $(n!)^{2n+2}$. However, this bound $(n!)^{2n+2}$ is still probably far from being best possible. Theorem 3 and its possible improvements would have applications, e.g. to decomposable form equations (cf. [5]).

§ 3. Applications to irreducible polynomials and arithmetic graphs

Let $\mathcal{A}=\{\alpha_1,\dots,\alpha_m\}$ be a finite subset of O_K. For given $N\geq 1$, we denote by $\mathcal{G}=\mathcal{G}_K(\mathcal{A},N)$ the simple graph whose vertex set is $\mathcal{A}$ and whose edges are the unordered pairs $[\alpha_i,\alpha_j]$ such that $|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i-\alpha_j)|>N$. The ordered subsets $\mathcal{A}=\{\alpha_1,\dots,\alpha_m\}$ and $\mathcal{A}'=\{\alpha'_1,\dots,\alpha'_m\}$ of O_K are called *equivalent* if $\alpha'_i=\varepsilon\alpha_i+\beta$ for some $\varepsilon\in O_K^*$ and $\beta\in O_K$, $i=1,\dots,m$. Then the graphs $\mathcal{G}_K(\mathcal{A},N)$ and $\mathcal{G}_K(\mathcal{A}',N)$ are isomorphic.

Many diophantine problems, for example related to reducibility of polynomials, pairs of polynomials of given resultant, decomposable form equations or algebraic number theory lead to the study of connectedness properties of graphs $\mathcal{G}_K(\mathcal{A},N)$ (see [17], [11], [18] and the references given there). Let $m\geq 3$. Using Theorem C of the present paper on S-unit equations in two unknowns, we proved in [17] (see also [11]) in a more precise and effective form that for all but at most finitely many equivalence classes of ordered subsets $\mathcal{A}=\{\alpha_1,\dots,\alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A},N)$ has either

(i) a connected component of order at least $m-1$,

or

(ii) two connected components of order ≥ 2 which are complete.

This result and its various other variants have been used to solve the diophantine problems mentioned.

For certain applications, for instance to irreducible polynomials (see Theorem 5 below) it is crucial to eliminate the possibility (ii) from the above statement. Recently, we have proved in [18, Part II] (see also [18, Part I]) a more precise and quantitative version of the following theorem.

THEOREM 4. *Let m be a positive integer different from 4. Then for all but at most finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \dots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ has a connected component of order at least $m-1$.*

In the case $m = 4$, we described in [18] the exceptions having property (ii). In the proof, we used the above-mentioned result of Evertse and myself [7] on S-unit equations. Further, to prove the quantitative version, we needed Theorem 1.

For given $m > 4$, we shall now sketch the proof that apart from finitely many equivalence classes of ordered subsets $\mathcal{A} = \{\alpha_1, \dots, \alpha_m\}$ of O_K, the graph $\mathcal{G}_K(\mathcal{A}, N)$ cannot have property (ii). In contrast with [18, Part II], here Theorem 2 will be used in a qualitative form. Let $\mathcal{A} = \{\alpha_1, \dots, \alpha_m\}$ be an arbitrary ordered subset of O_K for which $\mathcal{G} = \mathcal{G}_K(\mathcal{A}, N)$ has two connected components, say $\mathcal{G}_1$ and $\mathcal{G}_2$, with orders ≥ 2 such that both $\mathcal{G}_1$ and $\mathcal{G}_2$ are complete. We may assume without loss of generality that $\{\alpha_1, \dots, \alpha_k\}$ and $\{\alpha_{k+1}, \dots, \alpha_{k+l}\}$ are the vertex sets of $\mathcal{G}_1$ and $\mathcal{G}_2$, respectively. Then we have

$$\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i - \alpha_j)\right| \leq N \tag{6}$$

for each i, j with $1 \leq i \leq k$, $k+1 \leq j \leq k+l$. Denote by S the set of all prime ideals in O_K with norm at most N. Then all $\alpha_i - \alpha_j$ satisfying (6) are S-units. For distinct i, i' with $1 \leq i, i' \leq k$, we have

$$\alpha_i - \alpha_{i'} = (\alpha_i - \alpha_j) + (\alpha_j - \alpha_{i'}) \text{ for } j = k+1, \dots, k+l.$$

Now Theorem 2 implies that apart from an S-unit factor ε, $\alpha_i - \alpha_{i'}$ can assume only finitely many values, say β. But using Theorem B for fixed β, it follows from

$$\beta = (\alpha_i - \alpha_j)/\varepsilon + (\alpha_j - \alpha_{i'})/\varepsilon, \quad j = k+1, \dots, k+l$$

that $(\alpha_i - \alpha_j)/\varepsilon$ and $(\alpha_j - \alpha_{i'})/\varepsilon$ can assume only finitely many values. Hence the same holds for $(\alpha_p - \alpha_q)/\varepsilon$ for all distinct p, q with $1 \leq p, q \leq m$. Thus $\mathcal{A} = \varepsilon\mathcal{A}' + \alpha_1$ for some ordered subset $\mathcal{A}'$ of O_K whose elements can assume only finitely many values. This proves our claim.

We present now an application of Theorem 4 to irreducible polynomials. I. Schur, A. Brauer, R. Brauer, H. Hopf, I. Seres and others investigated the reducibility of polynomials of the form $f(g(X))$, where f, g are monic polynomials with coefficients in $\mathbb{Z}$, g is irreducible over $\mathbb{Q}$ and the roots of f are distinct rational integers. For a survey of results obtained in this direction, see [14]. In [14] I extended these investigations to the case when the roots of f are distinct elements of an arbitrary but fixed totally real algebraic number field K of degree d. Let $\mathcal{A} = \{\alpha_1, \dots, \alpha_m\}$ be the set of roots of such a monic polynomial $f \in \mathbb{Z}[X]$. Further, suppose that $g \in \mathbb{Z}[X]$ is an irreducible monic polynomial whose splitting field over $\mathbb{Q}$ is a CM-field, i.e. a totally imaginary quadratic extension of a totally real algebraic number field. In this case we say that $g(X)$ is of *CM-type*. If $g(f(X))$ is reducible then so are $g(f(X+a))$ for all $a \in \mathbb{Z}$. Such polynomials $f(X), f(X+a)$ are called *equivalent*. I showed that if the graph $\mathcal{G}_K(\mathcal{A}, N)$ for $N = 2^d|g(0)|^{d/\deg(g)}$ has a connected component with v vertices, then the number of irreducible factors of $g(f(X))$ over $\mathbb{Q}$ is at most $\deg(f)/v$. Further, this estimate is in general best possible (cf. [14, Part II]). Hence it is easy to deduce from Theorem 4 the following

THEOREM 5. *Let $g \in \mathbb{Z}[X]$ be an irreducible monic polynomial of CM-type. There are only finitely many pairwise inequivalent monic polynomials $f \in \mathbb{Z}[X]$ with degree greater than 4 and with distinct roots in K such that $g(f(X))$ is reducible over $\mathbb{Q}$.*

This theorem is in a certain sense a considerable refinement of Theorem 1 of [14, Part III]. We should, however, remark that this theorem of [14] was established in an effective way and over an arbitrary totally real ground field instead of $\mathbb{Q}$.

Recently, we have obtained in [14, Part IV] a more precise version of Theorem 5. There can exist infinitely many pairwise inequivalent exceptions $f(X)$ of degree 4 for which $g(f(X))$ is reducible for a suitable $g(X)$. We give in [14, Part IV] a precise description of these exceptions. Further, we show that Theorem 5 does not remain valid for any irreducible monic polynomial $g \in \mathbb{Z}[X]$ and for any number field K.

§ 4. Applications to common polynomial divisors of trinomials

Using the terminology of [28], for $i \geq 2$ we shall mean by a monic i-nomial over $\mathbb{Q}$ a polynomial of the form $X^{m_1} + a_2X^{m_2} + \cdots + a_{i-1}X^{m_{i-1}} + a_i$ over $\mathbb{Q}$ with $m_1 > m_2 > \cdots > m_{i-1} > 0$. If $p(X)$ and $s(X)$ are polynomials over $\mathbb{Q}$ with $\deg(s) \leq i-1$ such that $p(X) \mid s(X^r)$ over $\mathbb{Q}$ for some integer $r \geq 1$ then $p(X)$ divides infinitely many i-nomials over $\mathbb{Q}$. Indeed, the vector space of polynomials in $\mathbb{Q}[X]$ modulo $s(X)$ is at most $(i-1)$-dimensional, and hence $s(X)$ divides infinitely many i-nomials $T(X)$ over $\mathbb{Q}$. But then $s(X^r) \mid T(X^r)$ and so $p(X) \mid T(X^r)$ over $\mathbb{Q}$. Conversely, Posner and Rumsey [28] made in 1965 the following conjecture: *If a polynomial with rational coefficients divides* *infinitely many monic i-nomials over* $\mathbb{Q}$, *then it divides a non-zero polynomial in* $\mathbb{Q}[X]$ *with degree less than* i *in* X^r *for some* $r \geq 1$.

For $i = 2$ the conjecture is obvious. For $i = 3$, Posner and Rumsey [28] proved a weaker version of their conjecture. Recently, we have proved with Schinzel [21] that the conjecture is true for $i = 3$ and false for every $i \geq 4$. The disproof for the case $i \geq 4$ is elementary. For $i = 3$, we obtained with Schinzel the following stronger assertion.

THEOREM 6. *Let* $p \in \mathbb{Q}[X] \setminus \mathbb{Q}$, k *the number of distinct roots of* $p(X)$, K *the splitting field of* $p(X)$ *over* $\mathbb{Q}$, $d = [K : \mathbb{Q}]$, $\mathcal{S}$ *the set of places of* K *consisting of all infinite places and all valuations induced by the prime ideal divisors of the non-zero roots of* $p(X)$, *and* $s = \mathrm{Card}(\mathcal{S})$. *If* $p(X)$ *divides more than*

$$\exp\{(s^6 \cdot 2^{180d} + 8sk)\log(4sd)\}$$

monic trinomials over $\mathbb{Q}$, *then it divides a linear or quadratic polynomial in* X^r *over* $\mathbb{Q}$ *for some integer* $r \geq 1$.

The proof depends on Theorems B and 2 on S-unit equations. We sketch the basic idea of the proof. The details will be published in [21].

Let $T(X) = X^m + aX^n + b$ be a trinomial over $\mathbb{Q}$ which is divisible by $p(X)$. If $p(X)$ is divisible by X or if $ab = 0$, the assertion easily follows. Hence it suffices to deal with the case when $X \nmid p(X)$ and $ab \neq 0$. It is easy to show that $p(X)$ can be written in the form $p(X) = p_1(X) \cdot p_2^2(X)$ where p_1, p_2 are relatively prime squarefree polynomials in $\mathbb{Q}[X]$. Denote by $\xi_1, \dots, \xi_k$ the distinct roots of $p_1(x) \cdot p_2(x)$, and by S the set of all prime ideal divisors of $\xi_1 \cdots \xi_k$ in O_K. Then, for $j = 1, \dots, k$, (ξ_j^m, ξ_j^n) is a solution of the S-unit equation

$$(-1/b)x_1 + (-a/b)x_2 = 1 \quad \text{in} \quad x_1, x_2 \in O_S^*. \tag{7}$$

If (7) has at most 2 solutions, then the assertion can be proved by means of some elementary arguments from algebraic number theory. On the other hand, if $p(X)$ divides trinomials $T(X)$ over $\mathbb{Q}$ for which the corresponding equation (7) has more than 2 solutions, then one can use Theorem 2 to derive an upper bound for the number of S-equivalence classes of these equations (7). If now there are sufficiently many trinomials $T(X)$ over $\mathbb{Q}$ for which the corresponding equations (7) are S-equivalent, then one can show by means of Theorem B that there is an integer $r \geq 1$ such that ξ_j^r assumes the same value, say c, for $j = 1, \dots, k$. Here $c \in \mathbb{Q}^*$ and $p(X) \mid (X^r - c)^2$ over $\mathbb{Q}$, which proves the assertion of Theorem 6.

§ 5. Applications to decomposable form equations

In this section, we present some generalizations to decomposable form equations of well-known finiteness theorems of Schmidt, Schlickewei and Laurent concerning families of solutions of norm form equations.

Let $\mathfrak{M}$ be an O_S-lattice, i.e. a finitely generated O_S-submodule of some K-vector space. Consider a *decomposable form* $F(\mathbf{x})$ on

$$K\mathfrak{M} := \{\lambda \mathbf{x} : \lambda \in K,\ \mathbf{x} \in \mathfrak{M}\}$$

over K, i.e. a function $F\colon K\mathfrak{M} \to K$ for which there are an $\alpha \in K^*$, a finite and normal field extension G/K and K-linear functions $l_1, \dots, l_f\colon K\mathfrak{M} \to G$ such that $F(\mathbf{x}) = \alpha \prod_{i=1}^{f} l_i(\mathbf{x})$ for all $\mathbf{x} \in K\mathfrak{M}$ (for this general definition, see e.g. [9]). We may assume that G is the splitting field of F, i.e the smallest extension of K over which F factorizes into linear functions. Suppose that $n := \dim_K K\mathfrak{M} \geq 2$ and that $\{l_1, \dots, l_f\}$ contains n linearly independent functions over G. If in particular $K\mathfrak{M} = K^n$ and $\mathbf{e}_1 = (1, 0, \dots, 0)^T, \dots, \mathbf{e}_n = (0, \dots, 0, 1)^T$ is the standard basis of K^n, we identify $F(\mathbf{x})$ on K^n with the homogeneous polynomial $F(\mathbf{X}) = F(X_1\mathbf{e}_1 + \dots + X_n\mathbf{e}_n) \in K[X_1, \dots, X_n]$. This homogeneous polynomial is also called a decomposable form.

Let $\beta \in O_S \setminus \{0\}$ and consider the *decomposable form equation*

$$F(\mathbf{x}) \in \beta O_S^* \ \text{ in } \ \mathbf{x} \in \mathfrak{M}. \tag{8}$$

Put $\mathfrak{J} = \{1, \dots, f\}$. We may assume that $l_i = l_j$ if l_i and l_j are linearly dependent over G and that $\sigma(l_j) = l_{\sigma(j)}$ for all $j \in \mathfrak{J}$ and $\sigma \in \mathrm{Gal}(G/K)$, where $(\sigma(1), \dots, \sigma(f))$ is a permutation of $(1, \dots, f)$. In the special case when $F(\mathbf{x}) = \alpha \prod_{\sigma \in \mathrm{Gal}(G/K)} \sigma(l_1(\mathbf{x}))$, $F(\mathbf{x})$ is in fact a *norm form* over K, and (8) is a *norm form equation*. Denote by $\mathbf{M}$ the set of tuples $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_f) \in G^f$ for which $\lambda_i = \lambda_j$ if $l_i = l_j$, $i, j \in \mathfrak{J}$ and $\sigma(\lambda_i) = \lambda_{\sigma(i)}$ for all $i \in \mathfrak{J}$ and $\sigma \in \mathrm{Gal}(G/K)$. Defining the product of $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbf{M}$ componentwise, $\mathbf{M}$ becomes a K-subalgebra of G^f with unit element $\mathbf{1} = (1, \dots, 1)$. We denote by $\mathbf{M}^*$ the multiplicative group of invertible elements of $\mathbf{M}$, and by $N(\boldsymbol{\lambda})$ the product of components of $\boldsymbol{\lambda} \in \mathbf{M}$. This function $N\colon \mathbf{M} \to K$ is clearly multiplicative. The linear mapping $\Psi\colon K\mathfrak{M} \to G^f : \mathbf{x} \mapsto (l_1(\mathbf{x}), \dots, l_f(\mathbf{x}))$ is injective. Further, $\Psi(K\mathfrak{M})$ is contained in $\mathbf{M}$. Put $\mathcal{M} = \Psi(\mathfrak{M})$. Then $\mathcal{M}$ is an O_S-lattice in $\mathbf{M}$ and Ψ induces an isomorphism between $\mathfrak{M}$ and $\mathcal{M}$ (as well as between $K\mathfrak{M}$ and $K\mathcal{M}$). We say that $\mathcal{M}$ is *full* (in $\mathbf{M}$) if $K\mathcal{M} = \mathbf{M}$. It will be more convenient to consider (8) in the form

$$\alpha\, \mathrm{N}(\boldsymbol{\mu}) \in \beta O_S^* \ \text{ in } \ \boldsymbol{\mu} \in \mathcal{M}. \tag{9}$$

If in particular $F(\mathbf{x})$ is a norm form then (9) becomes the norm form equation

(10) $<*N_{M/i}r(/x)$ *e(30*$_s$* in /xGM,

where JVC denotes now the Os-module {/i(x) : x E 9Jl} and *M* is a suitable subfield of *G* containing *K* and lifJVC.

A partition I = {Ai,..., ^4^} of # is called symmetric if *i,j* E ***3*** belong to the same subset if *l{* = Zj, and if *a(Ai),... ,a(Ah)* is a permutation of *Ai,...,Ah* for every *a* E Gal(G/if). For a symmetric partition I = {Ai,..., *Ah}* of J, we denote by L = L(I) the subset of M consisting of those elements A = *(Xi)ieg* of M for which A; = *Xj* whenever *i* and *j* belong to the same subset in the partition I. Then L is a iT-subalgebra of M with **1.** If in particular I = {#} then we write K for L(0). Further, M = L(I_0) for the partition Io for which *ijed* belong to the same subset if and only if *li* = *lj.* The subrings of M with **1** are precisely the subalgebras L(I) where I is a svmmetric partition of fl.

Let L = L(I) with a symmetric partition I of 0, and denote by ***OS,L*** the set of those elements A = *(\i)ied* °f ^ f°^{r} which all components A^ are integral over O5. Then ***OS,L*** is a subring of L with unit element **1.** Its unit group is denoted by O J_L. Let JVC^L denote the set of all elements /x E JVC for which A • ***fx*** E *KM* for every A E L. One can show that in this case A • ***fjt*** E *KM^L,* that *M^L* is an Os-sublattice of JVC, that *M^K* = JVC, and that JVC^M = JVC if JVC is full. We say that L is *admissible* with respect to JVC or simply admissible if JVC^L fl M* 7^ 0 and if there is no subalgebra L' with **1** in M such that L ' D L and *KM$^{L>}$* = *KM^L*. We note that if JVC is full then M is admissible. For an admissible subalgebra L of M, denote by the set of those A E L for which A • ***fx*** E JVC^L for all /x E JVC^L. Then is a subring of O 5 L with **1** which contains O5 as a subring (identifying the elements A of O_s with A = (A,...,A)). Further, *KV^* = L. Denote by D^* the unit group of One can show that J $_L$•= [OJ$_L$: 2)^*] is finite. If ***fi*** E JVC^L is a solution of (9) then so is every element of //2)^*. Then the set /¿2)^*$^{'s\ ca}$lled a *family of solutions* or more precisely an (JVC, L)-famiiy *of solutions* of (9). Further, a family of solutions is called *maximal* if it is not properly contained in another family of solutions. Every solution is contained in a maximal family of solutions.

We shall state our results in a quantitative form. Hence we need some further notation. Denote by *D* the degree of the normal closure of *G* over Q. Let *m —n* or *m* = *n + 1* according as 9JT is free or not. One can show that m is the minimum of the cardinalities of the sets of generators of 93T. Assume that *F* is integral on 9JT, i.e. that for some set of generators {ai,... , a_m} of 9JT, the polynomial$<*N_{M/i}r(/x)$*e(30*$_s$*in^j'^{a}i)^ ^{as} their coefficients in O5. This notion of integrality is independent of the choice of a_x,..., a_m. For */3* E O5 \ {0}, (/3) denotes the Os-ideal generated by /3, r_m(/3) is the number of factorizations