On certain graphs associated with an integral domain and their applications to diophantine problems

By K. GYŐRY (Debrecen)

1. Introduction

In [4] and [11], we obtained effective results on certain arithmetic graphs associated with the ring of integers of a number field. The results of [11] have applications among other things to diophantine equations (see [15]) and to algebraic integers of given discriminant (cf. [16]). The purpose of the present paper is to extend, in an ineffective form, some results of [11], [15] and [16] to the case of integral domains of characteristic 0.*)

Let R be an integral domain, and Γ a non-empty subset of R. Consider the directed graph $\mathcal{G}=\mathcal{G}(R, \Gamma)$ whose vertex set is R, and whose edges are the ordered pairs $[\alpha, \beta]$ of distinct elements $\alpha, \beta \in R$ satisfying

$$\beta-\alpha \notin \Gamma.$$

$\mathcal{G}$ is in fact a Cayley graph (see e.g. [32] or [23]) of the additive group of R. Since R is a ring, it is natural to assume that Γ has some multiplicative property. From the point of view of applications, of particular importance is the case when $\Gamma=\mathcal{N}S$ where $\mathcal{N}$ is a finite non-empty subset of R, S is a finitely generated multiplicative subsemigroup of $R\setminus\{0\}$ and $-1\in S$. Many higher dimensional diophantine problems can be reduced to the study of finite induced subgraphs of such graphs $\mathcal{G}$. We remark that in these applications it is more convenient to remove the direction and regard $\mathcal{G}$ as a simple (undirected) graph.

In [11], we gave a certain characterization of finite induced subgraphs of given order of $\mathcal{G}$ in the case when R is the ring of integers of a number field. Further, we showed that the structure of these subgraphs becomes simpler whenever they have sufficiently many vertices. In the is paper we extend, in an ineffective form, these results to the case of integral domains R of characteristic 0. Our main results (Theorems 1 and 2) will be stated in Section 2.

Our Theorems 1 and 2 have a number of applications. Some of them will be presented in Sections 3, 4 and 5.

Theorem 1 enabled us to solve several higher dimensional diophantine problems which had not been attackable by the earlier methods. Generalizing certain finiteness

*) *Added in proof.* Effective versions of some results of this paper have been established in our recent works "Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains" (to appear) and "Integral elements of given discriminant over finitely generated domains" (to appear).

results of [7], [18], [31] and [12—15], in Section 3 we show that the discriminant form equations, index form equations and certain norm form equations defined over a field of finite type over $\mathbf{Q}$ have only finitely many solutions in any given integral domain finitely generated over $\mathbf{Z}$. In the terminology of Lang [21] this means that the affine varieties determined by such equations have the Siegel property.

In Section 5, general results are established on integral elements of given discriminant over finitely generated rings. These extend some finiteness results of [8], [9], [10] and [16] to this more general situation. We get as a special case that if R is an integrally closed ring of finite type over $\mathbf{Z}$ with quotient field L and K is a finite extension field of L, then, apart from the translation by elements of R, there are only finitely many integral elements over R in K with a given non-zero discriminant over L. Another consequence is that if R' is an almost finite[1]) integral extension of R then up to the obvious translation by elements of R and multiplication by invertible elements of R, there are only finitely many $\alpha \in R'$ with $R' = R[\alpha]$.

Some further applications will be published in a separate paper.

2. The main results

Let R be an integral domain of characteristic 0, S a finitely generated multiplicative subset of R (i.e. a finitely generated multiplicative subsemigroup of $R \setminus \{0\}$ containing 1), $\mathcal{N}$ a finite non-empty subset of $R \setminus \{0\}$ and $\Gamma = \mathcal{N}S$ [2]). We suppose, for convenience, that $-1 \in S$. For an arbitrary non-empty subset $\mathcal{A}$ of R, we denote by $\mathcal{G}(\mathcal{A}, \Gamma)$ the graph[3]) whose vertex set is $\mathcal{A}$, and whose edges are the unordered pairs $[\alpha, \beta]$ of distinct elements $\alpha, \beta \in \mathcal{A}$ satisfying[4])

$$\alpha - \beta \notin \Gamma. \tag{1}$$

This section is devoted to the study of finite subgraphs of $\mathcal{G}(R, \Gamma)$. Clearly it suffices to consider the induced subgraphs[5]). If $\mathcal{G}$ and $\mathcal{G}'$ are finite induced subgraphs of $\mathcal{G}(R, \Gamma)$ with vertex sets $\mathcal{A}$ and $\mathcal{A}'$ and

$$\mathcal{A}' = \varepsilon \mathcal{A} + \gamma$$

with some $\varepsilon \in S$ and $\gamma \in R$, then we shall say that $\mathcal{G}'$ comes from $\mathcal{G}$ by the translation by an element of R and multiplication by an element of S, or simply that $\mathcal{G}'$ comes

---

[1]) In other words, R' is an integral extension of R and its quotient field is a finite extension of L (see [24]).

[2]) The classical algebraic concepts used in the present work can be found e.g. in [33] and [25].

[3]) For the necessary basic concepts concerning graphs and hypergraphs we refer the reader to the books [1] and [22]. If $\mathcal{G}$ is a graph, then, as usual, $V(\mathcal{G})$ denotes the vertex set of $\mathcal{G}$, $E(\mathcal{G})$ its edge set, $|\mathcal{G}|$ its order (the number of its vertices), and $\overline{\mathcal{G}}$ its complement. A subgraph $\mathcal{G}'$ of $\mathcal{G}$ is said to be an induced one if $E(\mathcal{G}')$ consists of all edges of $\mathcal{G}$ having both their endpoints in $V(\mathcal{G}')$. In this case $\mathcal{G}'$ is called the subgraph induced by the subset $V(\mathcal{G}')$ of $V(\mathcal{G})$. If $\mathcal{G}'$ and $\mathcal{G}''$ are subgraphs of $\mathcal{G}$, $\mathcal{G}' \vee \mathcal{G}''$ will denote the subgraph induced by $V(\mathcal{G}') \cup V(\mathcal{G}'')$.

[4]) Since $-1 \in S$, (1) and $\beta - \alpha \notin \Gamma$ hold simultaneously.

[5]) We shall distinguish between two isomorphic induced subgraphs of $\mathcal{G}(R, \Gamma)$ if their vertex sets are distinct.

from $\mathcal{G}$ [6]). Further, we shall say that a subgraph of $\mathcal{G}(R, \Gamma)$ comes from the H_m defined below if it comes from a subgraph belonging to H_m.

Let $\bar{\mathcal{G}}^T$ denote the triangle hypergraph[7]) of $\bar{\mathcal{G}}$. An induced subgraph $\mathcal{H}$ of order $\geqq 2$ of $\bar{\mathcal{G}}$ will be said to be spanned by a connected component of $\bar{\mathcal{G}}^T$ if the set of endpoints of those edges of $\bar{\mathcal{G}}$ which are vertices of this component coincides with $V(\mathcal{H})$.

First we give a certain characterization of finite induced subgraphs of given order of $\mathcal{G}(R, \Gamma)$.

Theorem 1. *Given a natural number $m \geqq 2$, there is a finite subset H_m of induced subgraphs of order $\leqq m$ of $\mathcal{G}(R, \Gamma)$ with the following property. If $\mathcal{G}$ is an arbitrary induced subgraph of order m of $\mathcal{G}(R, \Gamma)$ with connected components $\mathcal{G}_1, \ldots, \mathcal{G}_l$ and $|\mathcal{G}_l| \leqq |\mathcal{G}_{l-1}| \leqq \ldots \leqq |\mathcal{G}_1|$, then at least one of the following cases holds:*

(i) *$l=1$ (i.e. $\mathcal{G}$ is connected) and, if $\mathcal{G}$ is not complete, each induced subgraph of $\mathcal{G}$ whose complement is spanned by a connected component of $\bar{\mathcal{G}}^T$ comes from H_m,*

(ii) *$l=2$, $|\mathcal{G}_2|=1$, $\bar{\mathcal{G}}_1$ is not connected and, for each connected component $\mathcal{H}$ of $\bar{\mathcal{G}}_1$, $\overline{\mathcal{H} \vee \mathcal{G}_2}$ comes from H_m,*

(iii) *$l=2$, $2 \leqq |\mathcal{G}_2| \leqq |\mathcal{G}_1|$ and both $\mathcal{G}_1$ and $\mathcal{G}_2$ are complete,*

(iv) *$\mathcal{G}$ comes from H_m.*

This theorem can be regarded as an ineffective extension of Theorem 1 of [11] to integral domains of characteristic 0.

Our theorem above shows that, apart from the translation by elements of R and multiplication by elements of S, all but a finite number of induced subgraphs of order m of $\mathcal{G}(R, \Gamma)$ are of the type (i), (ii) or (iii).

It is easy to show (see e.g. the examples given in [11]) that each of the cases (i), (ii) and (iii) really occurs. Further, any connected graph of order m can be represented (with suitable $\mathcal{N}$ and S) as an induced subgraph of $\mathcal{G}(R, \Gamma)$. In case (i) it is not possible to get a more precise but simple characterization. By means of repeated applications of Theorem 1 (see the remark below) further induced subgraphs of $\mathcal{G}$ can be obtained from a suitable finite extension of H_m.

It is clear that Theorem 1 is not true if S is not finitely generated or if $\mathcal{N}$ is infinite. Further, as the example of the graphs $\mathcal{G}(\mathcal{E}, \Gamma)$ having vertex set $\mathcal{E}=\{0, 1, 2, \varepsilon, 1+\varepsilon, 2+\varepsilon\}$, $\varepsilon \in S$, shows, Theorem 1 does not remain valid if we replace $\bar{\mathcal{G}}^T$ by that hypergraph whose vertices are the edges of $\bar{\mathcal{G}}$, and whose edges are the n-tuples ($n \geqq 4$) of edges of $\bar{\mathcal{G}}$ that form a circuit of length n.

Finally, we remark that the following repeated application of Theorem 1 to induced subgraphs of order m of $\mathcal{G}(R, \Gamma)$ can provide further information about

---

[6]) Both the translation by elements of R and the multiplication by element of S define an action on $\bar{\mathcal{G}}(R, \Gamma)$. The multiplication considered does not act in general on the edge set of $\mathcal{G}(R, \Gamma)$. However, if e.g. $\mathcal{N}=\{1\}$ and S is a group, both the translation and the multiplication act on $\mathcal{G}(R, \Gamma)$.

[7]) The triangle hypergraph $\mathcal{G}^T$ of a graph $\mathcal{G}$ is that hypergraph whose vertices are the edges of $\mathcal{G}$, and whose edges are the triples of edges of $\mathcal{G}$ that form a triangle (cf. [1], p. 440).

these subgraphs. Let $\mathcal{N}_1$ denote the finite set consisting of $\mathcal{N}$ and of the differences of the vertices (as elements of R) of the graphs belonging to $H_m=H_m(R,\Gamma)$, and put $\Gamma_1=\mathcal{N}_1 S$. Then $\Gamma\subseteq\Gamma_1$ and by Theorem 1 there exists a finite subset $H_m(R,\Gamma_1)$ of induced subgraphs of order $\leqq m$ of $\mathcal{G}(R,\Gamma_1)$ with the property specified above. It often happens that some induced subgraph of a graph $\mathcal{G}(\mathcal{A},\Gamma)$ of order m does not come from $H_m(R,\Gamma)$, but the corresponding induced subgraph of $\mathcal{G}(\mathcal{A},\Gamma_1)$ (which has the same vertex set) comes from $H_m(R,\Gamma_1)$. This observation proves useful in some applications. It is obvious that the above argument can be continued.

Our next theorem concerns finite induced subgraphs of high order of $\mathcal{G}(R,\Gamma)$. Before stating it, we introduce an important constant. In Section 6 we shall show (cf. Lemma 3) that up to the multiplication by elements of S, the equation

$$x+y+z=0 \tag{2}$$

has only finitely many solutions $(x,y,z)\in\Gamma^3$. Thus there is a finite set, T, of solutions such that every solution (x,y,z) of (2) can be written in the form $(x,y,z)=(\eta x',\eta y',\eta z')$ with some $\eta\in S$ and $(x',y',z')\in T$. The minimum cardinality of these finite sets T of solutions will be denoted by $C=C(R,\mathcal{N},S)$. We remark that C is uniquely determined by R, $\mathcal{N}$ and S.

Theorem 2. *Let $\mathcal{G}$ be an arbitrary finite induced subgraph of $\mathcal{G}(R,\Gamma)$ with $|\mathcal{G}|>3C$. Then either*

(i) *$\mathcal{G}$ is connected,*

or

(ii) *$\mathcal{G}$ has two connected components $\mathcal{G}_1$, $\mathcal{G}_2$, $|\mathcal{G}_2|\leqq|\mathcal{G}_1|$, $\mathcal{G}_2$ is complete and if $|\mathcal{G}_2|>C$ then $\mathcal{G}_1$ is also complete.*

In the case when R is the ring of integers of a number field, our Theorem 2 in [11] gives much more precise information about the structure of finite induced subgraphs of high order of $\mathcal{G}(R,\Gamma)$.

It is easy to give examples for both cases listed in Theorem 2 (cf. [11]).

There are many cases when $C=0$. If this is the case, our Theorem 1 reduces essentially to Theorem 2.

We remark that Theorem 2 is true for infinite induced subgraphs of $\mathcal{G}(R,\Gamma)$ as well. The infinite case can easily be reduced to the finite one.

3. Applications to diophantine equations

As an application of our Theorem 1, we extend now (in an ineffective form) some results of [7], [18], [31], [12], [15] and [14] to the case of fields of finite type over $\mathbf{Q}$.

Let L be a finitely generated extension field of $\mathbf{Q}$, and K an extension of L. Let

$$F(\mathbf{x})=F(x_1,\ldots,x_m)\in L[x_1,\ldots,x_m]$$

be a form of degree $n\geqq 3$ in $m\geqq 2$ variables, and suppose that F is *decomposable*, i.e. that it factors into linear factors in some finite extension, G, of L. Let R be a finitely

generated subring of K over $\mathbf{Z}$ with quotient field K', and β a non-zero element in K. We shall show that under certain conditions concerning the linear factors of F the equation

$$F(x_1, \ldots, x_m) = \beta \tag{3}$$

has only finitely many solutions $(x_1, \ldots, x_m) \in R^m$.

We may suppose without loss of generality that K contains G and that the coefficient a_0 of x_1^n in F is different from zero. Let $F(\mathbf{x}) = a_0 l_1(\mathbf{x}) \ldots l_n(\mathbf{x})$ be the factorization of F into linear factors l_i with coefficients in G. Suppose that the linear equation system

$$l_i(\mathbf{x}) = 0, \quad i = 1, \ldots, n, \tag{4}$$

has no non-trivial solution $\mathbf{x}$ in L^m and that the system $\mathscr{L}$ of linear forms $l_1, \ldots, l_n$ can be partitioned into pairwise disjoint subsystems $\mathscr{L}_1, \ldots, \mathscr{L}_k$ such that each $\mathscr{L}_h$ $(1 \leqq h \leqq k)$ is connected (that is, for any distinct i, j with $l_i, l_j \in \mathscr{L}_h$ there is a sequence $l_i = l_{j_1}, \ldots, l_{j_v} = l_j$ in $\mathscr{L}_h$ such that $\lambda'_{j_u} l_{j_u} + \lambda''_{j_{u+1}} l_{j_{u+1}} \in \mathscr{L}_h$ for each u, $1 \leqq u \leqq v-1$, with some $\lambda'_{j_u}, \lambda''_{j_{u+1}} \in G \setminus \{0\}$; in case of number fields see e.g. [15])[8]). It will be apparent from the proof that under these assumptions $m \leqq n$ holds and (4) has no non-trivial solution in any extension field of L. Further, suppose that there exists a t, $1 \leqq t \leqq m$, such that if

$$l_i(\mathbf{x}) = 0 \quad \text{for all} \quad l_i \in \mathscr{L}_h \tag{5}$$

with some $\mathbf{x} = (x_1, \ldots, x_m)$ having components from an arbitrary extension of L then $x_t = 0$ follows for each fixed h $(1 \leqq h \leqq k)$ [9]).

Theorem 3. *Under the above hypotheses, the equation* (3) *has only finitely many solutions* $(x_1, \ldots, x_m) \in R^m$ *with* $x_t \neq 0$.

Using a standard argument, from Theorem 3 we can easily deduce (in an ineffective form) the main results of [12] and [15], obtained in the case of algebraic number fields L, K'.

When $m = 2$, Theorem 3 follows from a theorem of LANG [19], [20], i.e. from a generalized version of a theorem of SIEGEL [29] concerning integral points of curves of genus $\geqq 1$.

It is evident that our Theorem 3 and its corollaries do not remain valid if K' and R are not finitely generated.

In what follows, we keep the above notations and present some consequences of Theorem 3. By a solution $\mathbf{x} \in R^m$ of (6), (7) and (9) we shall mean an $\mathbf{x} \in R^m$ satisfying

$$l_1(\mathbf{x}) \ldots l_n(\mathbf{x}) = \beta$$

where l_i are the linear factors of the corresponding decomposable form.

---

[8]) It is easily seen that if $m = 2$ then every system $\mathscr{L}$ containing at least three pairwise non-proportional linear forms satisfies these conditions with $k = 1$.

[9]) We remark that if $k = 1$ then the other hypotheses imply this assumption for each t. Thus in case $k = 1$ the restriction $x_t \neq 0$ can be omitted from Theorem 3. *Added in proof.* An equivalent formulation of the conditions concerning (4) and (5) is that *rank* $\mathscr{L} = m$ over G and, for each h, $x_t = \sum_{i, l_i \in \mathscr{L}_h} \sigma_i l_i$ with $\sigma_i \in G$.

Let M be a finite extension of degree $n \geqq 3$ of L, and let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_m$ be linearly independent elements of M over L with $m \geqq 2$ and $M = L(\alpha_2, \ldots, \alpha_m)$. We may assume without loss of generality that K contains the normal closure of M over L. We can show in the same way as in case $L = \mathbf{Q}$ (see e.g. [3]) that if $x_1, \ldots, x_m \in L$ are variables then the norm $F(\mathbf{x}) = N_{M/L}(x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m)$ is a decomposable form of degree n with coefficients in L. It is called a *norm form over* L. In this case (3) becomes a *norm form equation*

$$N_{M/L}(x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m) = \beta \tag{6}$$

over L.

Generalizing a well-know result of Schmidt [28], in the case $K' = L = \mathbf{Q}$ Schlickewei [27] gave criteria for (6) to have only finitely many solutions. In the case when L and K' are arbitrary number fields, we obtained [12], [14], [15], under certain conditions concerning $\alpha_2, \ldots, \alpha_m$, effective results on (6). We extend now (in an ineffective form) some results of [12], [14] and [15] to the above more general situation.

Corollary 3.1. *Suppose that in* (6) α_{i+1} *is of degree* $\geqq 3$ *over* $L(\alpha_1, \ldots, \alpha_i)$ *for* $i = 1, \ldots, m-1$. *Then* (6) *has only finitely many solutions* $\mathbf{x} \in R^m$.

If we restrict ourselves to the solutions $\mathbf{x} = (x_1, \ldots, x_m) \in R^m$ for which $x_m \neq 0$, the conditions of Corollary 3.1 can be relaxed.

Corollary 3.2. *Suppose that in* (6) $\alpha_1 = 1, \alpha_2, \ldots, \alpha_{m-1}$ *are linearly independent over* L *and that* α_m *is of degree* $\geqq 3$ *over* $L(\alpha_1, \ldots, \alpha_{m-1})$. *Then* (6) *has only finitely many solutions* $\mathbf{x} = (x_1, \ldots, x_m) \in R^m$ *with* $x_m \neq 0$.

Let M be as above, and let $1, \alpha_1, \ldots, \alpha_m$ be linearly independent elements of M over L such that $M = L(\alpha_1, \ldots, \alpha_m)$. If $x_0, x_1, \ldots, x_m \in L$ are variables, it is easily seen that the discriminant $D_{M/L}(\alpha_1 x_1 + \ldots + \alpha_m x_m)$ of $x_0 + \alpha_1 x_1 + \ldots + \alpha_m x_m$ over L is a decomposable form of degree $n(n-1)$ in $x_1, \ldots, x_m$ with coefficients in L. Such a form is said to be a *discriminant form over* L (in case of number fields, for this concept see e.g. [7], [18] or [13]). Taking $F(\mathbf{x}) = D_{M/L}(\alpha_1 x_1 + \ldots + \alpha_m x_m)$, (3) is a *discriminant form equation*

$$D_{M/L}(\alpha_1 x_1 + \ldots + \alpha_m x_m) = \beta \tag{7}$$

over L.

Corollary 3.3. *Under the above assumptions, the equation* (7) *has only finitely many solutions* $\mathbf{x} \in R^m$.

In the special case when L and K' are number fields, Corollary 3.3 implies (in an ineffective form) the results of Győry [7], [12], [15] and Győry and Papp [18] obtained on the finiteness of the number of solutions of discriminant form equations.

Let A be an integral domain with quotient field L, and let B be a subring of M containing A. Suppose that B, as an A-module, has a basis of the form $\{1, \omega_2, \ldots, \omega_n\}$. Then it is easily seen that

$$D_{M/L}(\omega_2 x_2 + \ldots + \omega_n x_n) = [F(x_2, \ldots, x_n)]^2 D_{M/L}(1, \omega_2, \ldots, \omega_n) \tag{8}$$

where $D_{M/L}(1, \omega_2, \ldots, \omega_n)(\in L)$ denotes the discriminant of the basis $\{1, \omega_2, \ldots, \omega_n\}$ over L and $F(x_2, \ldots, x_n) \in A[x_2, \ldots, x_n]$ is a decomposable form of degree $n(n-1)/2$. This form is called the *index form of the basis* $\{1, \omega_2, \ldots, \omega_n\}$ *of* B *over* A. When $F(\mathbf{x}) = F(x_2, \ldots, x_n)$, (3) becomes an *index form equation*

$$F(x_2, \ldots, x_n) = \beta. \tag{9}$$

In case of number fields, there is an extensive literature of index forms and index form equations (see e.g. the references given in [18] and [13]).

Corollary 3.4. *With the above notations and assumptions, the equation* (9) *has only finitely many solutions* $(x_2, \ldots, x_n) \in R^{n-1}$.

Of particular interest is the special case when L and K' are algebraic number fields, and A is the ring of integers of L. In this case the above statement was proved, in a slightly different and effective form, in our paper [15]. For certain special cases see GYŐRY [7], [12], TRELINA [31] and GYŐRY and PAPP [18].

4. Applications to polynomials of given discriminant

Let R be an integrally closed integral domain with quotient field L. Suppose that R is finitely generated over $\mathbf{Z}$. If $f \in R[x]$ and $f^*(x) = f(x+a)$ with some $a \in R$, then for their discriminants $D(f) = D(f^*) \in R$ holds. Such polynomials $f, f^* \in R[x]$ will be called *R-equivalent*.

Let δ be a non-zero element in R, S a finitely generated multiplicative subset in R, and G a finite extension of L. By applying Theorems 1 and 2 we shall prove the following

Theorem 4. *Under the above assumptions, there is a constant* c *and a finite set* $\mathscr{P}$ *of monic polynomials with coefficients in* R *and with discriminant contained in* δS *such that if* $f \in R[x]$ *is an arbitrary monic polynomial with* $D(f) \in \delta S$ *and with roots in* G, *then* $n = \deg(f) \leqq c$ *and* f *is* R*-equivalent to a polynomial of the form* $\eta^n f^*(\eta^{-1}x)$ *where* $\eta \in S$ *and* $f^* \in \mathscr{P}$.

In the case $R = \mathbf{Z}$ and $S = \{1\}$ this theorem was proved, in an effective form, in [5] and [6]. In case of arbitrary number fields L see [8], [9] and [16]. Theorem 4 can be easily extended to those monic polynomials $f \in R[x]$ of bounded degree whose monic polynomial divisor $P_f(x) \in R[x]$ of maximal degree with non-zero discriminant has the property $D(P_f) \in \delta S$ (cf. [16], Theorem 1).

An easy consequence of Theorem 4 is that up to R-equivalence there are only finitely many monic polynomials $f \in R[x]$ with roots in G and with $D(f) = \delta$. This implies e.g. that, for given $\mu \in R$, there are only finitely many monic polynomials $f \in R[x]$ with roots in G such that $D(f) = \delta$ and $f(0) = \mu$.

It is easy to see that in Theorem 4 the conditions concerning R and S are necessary.

5. Applications to integral elements of given discriminant

Let R, L, δ and S be as in the preceding section. Let K be an extension field of degree $n \geqq 2$ of L, and T the integral closure of R in K. If α is an element of T then its discriminant $D_{K/L}(\alpha)$ over L lies in R. Further, if $\alpha^* \in T$ with $\alpha - \alpha^* \in R$ then

$$D_{K/L}(\alpha) = D_{K/L}(\alpha^*).$$

Such elements of T will be called *R-equivalent*.

It is clear that if $\alpha = a + \eta\alpha^*$ with some $a \in R$, $\eta \in S$ and $\alpha^* \in T$, then we have

$$D_{K/L}(\alpha) = \eta^{n(n-1)} D_{K/L}(\alpha^*).$$

Theorem 5. *There exists a finite set $\mathscr{E}$ of elements of T with discriminant contained in δS such that any $\alpha \in T$ with $D_{K/L}(\alpha) \in \delta S$ is R-equivalent to an element of the form $\eta\alpha^*$ where $\eta \in S$ and $\alpha^* \in \mathscr{E}$.*

Our theorem generalizes (in an ineffective form) some results of ours [9], [16] obtained in case of algebraic number fields. For further references concerning earlier results see [13].

An obvious consequence of Theorem 5 is that up to translations by elements of R and multiplications by elements of S, there are only finitely many elements in T with discriminant contained in δS over L.

Corollary 5.1. *Given a non-zero element δ in R, there are only finitely many pairwise R-inequivalent elements in T with discriminant δ over L.*

This implies that for given δ and τ there are only finitely many $\alpha \in T$ with $D_{K/L}(\alpha) = \delta$ and $T_{r_{K/L}}(\alpha) = \tau$.

Let Q be another finitely generated multiplicative subset in R with $S \cap Q = \{1\}$.

Corollary 5.2. *Let δ and μ be fixed non-zero elements in R. There are only finitely many elements α in T with $D_{K/L}(\alpha) \in \delta S$ and $N_{K/L}(\alpha) \in \mu Q$.*

Let R^* and T^* denote the multiplicative group of the invertible elements of R and T, respectively. In the special case $S = \{1\}$, $Q = R^*$, $\mu = 1$ Corollary 5.2 gives the following

Corollary 5.3. *Given a non-zero element δ in R, there are only finitely many $\alpha \in T^*$ with $D_{K/L}(\alpha) = \delta$.*

Finally, we present a consequence of Theorem 5 concerning rings generated by a single element over R. Let T' be an arbitrary integral extension of R with quotient field K. If $T' = R[\alpha]$ for some $\alpha \in T'$ and $\alpha' = a + \varepsilon\alpha$ with some $a \in R$ and $\varepsilon \in R^*$, then obviously $T' = R[\alpha']$.

Corollary 5.4. *Up to the translation by elements of R and multiplication by elements of R^*, there are only finitely many $\alpha \in T'$ with $T' = R[\alpha]$.*

In the number field case Birch and Merriman [2], Győry [5—10], [16] and Trelina [30] obtained finiteness theorems on algebraic integers of given discriminant

and related questions. The results of [5—10], [16] and [30] are effective. Our above corollaries generalize, in an ineffective form, some of these results.

It is easily seen that the conditions made on R and S are necessary. Theorem 5 and its corollaries do not remain valid if R is not finitely generated. Similarly, in Theorem 5 and Corollary 5.2 it is necessary to assume S and Q finitely generated. Finally, Theorem 5 and Corollary 5.1 are not true in general when R is not integrally closed.

6. Proofs

In proving Theorems 1 and 2 we shall use the basic idea of the proofs of [11]. In place of applying Baker's method a general and deep ineffective theorem of Lang [19], [20] will be utilized.

Let R, S and Γ be as in Section 2, and let L be the quotient field of R.

Lemma 1. (S. LANG, [20].) *Let α, β, γ be non-zero elements in L, and let G be a finitely generated multiplicative subgroup of L^*. Then the equation*

$$\alpha x+\beta y=\gamma \tag{10}$$

has only finitely many solutions with $x, y\in G$.

Since the next simple assertion will be utilized several times, we state it as a separate lemma. Let $\pi_1, \ldots, \pi_s$ be a fixed system of generators of S.

Lemma 2. *Let T be any subset of S. There is a finite subset T' of T such that for any element α of T there is an element β of T' such that $\alpha=\pi_1^{a_1}\ldots\pi_s^{a_s}$ and $\beta=\pi_1^{b_1}\ldots\pi_s^{b_s}$ hold with $a_i\geqq b_i\geqq 0$, $i=1, \ldots, s$.*

PROOF. The assertion easily follows by induction on the number of generators.

Lemma 3. *Up to the multiplication by elements of S, the equation*

$$x+y+z=0 \tag{11}$$

has only finitely many solutions $(x, y, z)\in\Gamma^3$.

PROOF. Since $\Gamma=\mathcal{N}S$ and $\mathcal{N}$ is finite, from (11) we get a finite number of equations of the form

$$\alpha x+\beta y+\gamma z=0 \tag{12}$$

in $x, y, z\in S$, where the coefficients α, β, γ belong to $\mathcal{N}$. It is enough to prove the assertion for the solutions $(x, y, z)\in S^3$ of (12) with fixed α, β, γ.

Let G denote the multiplicative subgroup of L^* generated by S. S being finitely generated, G is also finitely generated. Further, from (12) we get

$$\alpha(x/z)+\beta(y/z)+\gamma=0.$$

So, by Lemma 1 x/z and y/z can take only finitely many values $x_0, y_0\in G$. Let us fix such a pair x_0, y_0. By Lemma 2 there are finitely many $(x', y', z')\in S^3$ with $x'/z'=x_0$, $y'/z'=y_0$ such that, for every $(x, y, z)\in S^3$ with $x/z=x_0$, $y/z=y_0$, we have $z'|z$ in S with some z' above. But this implies $(x, y, z)=(\eta x', \eta y', \eta z')$ with some $\eta\in S$ which completes the proof.

Lemma 4. *Let $m \geqq 2$ be a given natural number. Up to the translation by elements of R and multiplication by elements of S, there are only finitely many induced subgraphs $\mathscr{H}$ of order m of $\mathscr{G}(R, \Gamma)$ such that $\overline{\mathscr{H}}$ is spanned by a connected component of $\overline{\mathscr{H}}^T$* [10]).

PROOF. When $m=2$, the assertion follows from the finiteness of $\mathscr{N}$.

Suppose now $m \geqq 3$. Let $\mathscr{H}$ be an arbitrary induced subgraph of $\mathscr{G}(R, \Gamma)$ with vertex set $\mathscr{A}=\{\alpha_1, \ldots, \alpha_m\}$ and with the prescribed properties. If α_i, α_j and α_k form a triangle in $\overline{\mathscr{H}}$, then

$$(\alpha_i-\alpha_j)+(\alpha_j-\alpha_k)+(\alpha_k-\alpha_i)=0.$$

By Lemma 3 there is a finite subset Γ_0 of Γ (depending only on $\mathscr{N}$ and S) such that

$$\alpha_i-\alpha_j=\varepsilon\alpha_{ij}, \quad \alpha_j-\alpha_k=\varepsilon\alpha_{jk}, \quad \alpha_k-\alpha_i=\varepsilon\alpha_{ki}$$

with some $\varepsilon \in S$ and $\alpha_{ij}, \alpha_{jk}, \alpha_{ki} \in \Gamma_0$.

By hypothesis $\overline{\mathscr{H}}$ is spanned by a connected component of $\overline{\mathscr{H}}^T$. Consider those edges of $\overline{\mathscr{H}}$ which are vertices of this component. There is a numbering $i_1, \ldots, i_N$ of these edges of $\overline{\mathscr{H}}$ (with N depending only on m) such that for each u $(1 \leqq u \leqq N-1)$ the i_u-th and i_{u+1}-th edges form a triangle in $\overline{\mathscr{H}}$ together with a suitable edge of $\overline{\mathscr{H}}$. Of course, in this sequence one edge may occur several times. Denoting by β_{i_u} one of the differences of the endpoints (as elements of R) of the i_u-th edge, our above argument gives

$$\beta_{i_u} \quad \text{or} \quad -\beta_{i_u}=\varepsilon_{i_u}\gamma_{i_u} \quad \beta_{i_{u+1}}=\varepsilon_{i_u}\gamma'_{i_{u+1}} \tag{13}$$

with $\varepsilon_{i_u} \in S$ and $\gamma_{i_u}, \gamma'_{i_{u+1}} \in \Gamma_0$, $u=1, \ldots, N-1$. Since both Γ_0 and the number of possible numberings of edges is finite, it suffices to prove the assertion for those graphs $\mathscr{H}(\mathscr{A}, \Gamma)$ of order m for which N, γ_{i_u}, $\gamma'_{i_{u+1}}$ $(u=1, \ldots, N-1)$ and the signs have the same values in (13). Thus, by Lemma 2 there exists a finite number of $(\varepsilon'_{i_1}, \ldots, \varepsilon'_{i_{N-1}}) \in S^{N-1}$ satisfying (13) for some graphs considered above such that ε_{i_1} is divisible in S by at least one of these ε'_{i_1}. From this it follows that

$$\varepsilon_{i_u}=\eta\varepsilon'_{i_u}, \quad u=1, \ldots, N-1,$$

with some $\eta \in S$. Finally, we have for each numbered edge $[\alpha_u, \alpha_v]$ of $\overline{\mathscr{H}}$

$$\alpha_u-\alpha_v=\eta\alpha'_{uv} \tag{14}$$

with some $\alpha'_{uv} \in \Gamma$ belonging to a finite subset of Γ.

For every α_i and α_j there is a path of length at most m from α_i to α_j which consists of numbered edges of $\overline{\mathscr{H}}$. So, from (14) we obtain

$$\alpha_i-\alpha_j=\eta\alpha'_{ij}$$

---

[10]) It is clear that any induced subgraph of $\mathscr{G}(R, \Gamma)$ which comes from a subgraph $\mathscr{H}$ having the property specified here also has this property.

with finitely many possibilities for α'_{ij}. Writing $\alpha'_{11}=0$, there are only finitely many possibilities for each of $\alpha'_{11}, \alpha'_{21}, \ldots, \alpha'_{m1}$. This shows that there are finitely many graphs $\mathscr{H}'=\mathscr{H}'(\mathscr{A}', \Gamma)$ with vertex set $\mathscr{A}'=\{\alpha'_{11}, \alpha'_{21}, \ldots, \alpha'_{m1}\}$ such that any of these $\mathscr{H}'$ has the prescribed properties, and such that any induced subgraph $\mathscr{H}$ of order m of $\mathscr{G}(R, \Gamma)$ having the properties specified in Lemma 4 comes from one of these graphs $\mathscr{H}'$.

PROOF OF THEOREM 1. We shall use the basic idea of the proof of Theorem 1 of [11]. Let $\mathscr{A}=\{\alpha_1, \ldots, \alpha_m\}$ be the vertex set of $\mathscr{G}$. It is easily seen that if $l\geqq 3$ then both $\bar{\mathscr{G}}$ and $\bar{\mathscr{G}}^T$ are connected. So $\bar{\mathscr{G}}$ is spanned by $\bar{\mathscr{G}}^T$ and so, by Lemma 4, $\mathscr{G}$ comes from a finite subset of induced subgraphs of order m of $\mathscr{G}(R, \Gamma)$. Thus (iv) holds.

Suppose $l=2$. First assume $|\mathscr{G}_2|\geqq 2$. If both $\mathscr{G}_1$ and $\mathscr{G}_2$ are complete, (iii) follows. Suppose now that e.g. $\mathscr{G}_2$ is not complete. Let $[\alpha_u, \alpha_v]$ be an edge of $\bar{\mathscr{G}}_2$, and let $\mathscr{F}=\mathscr{F}(\mathscr{A}', \Gamma)$ denote the subgraph of $\mathscr{G}$ induced by $\mathscr{A}'=\{\alpha_u, \alpha_v\}\cup V(\mathscr{G}_1)$. Since $\bar{\mathscr{F}}$ is spanned by a connected component of $\bar{\mathscr{F}}^T$, by Lemma 4 we have for any two distinct vertices α_i, α_j of $\mathscr{F}$

$$\alpha_i-\alpha_j=\varepsilon\delta_{ij}$$

with some $\varepsilon\in S$ and with δ_{ij} belonging to a finite subset of R. Let $\mathscr{N}'$ denote the finite set consisting of $\mathscr{N}$ and of the finite subset of R mentioned above. Let $\Gamma'=\mathscr{N}'S$. We can now apply Lemma 4 to the graph $\mathscr{G}(\mathscr{A}, \Gamma')$ with Γ' in place of Γ, and for $\mathscr{G}(\mathscr{A}, \Gamma)$ (iv) follows with a suitable finite set H_m.

Assume now that $|\mathscr{G}_2|=1$. If $\bar{\mathscr{G}}_1$ is connected, by Lemma 4 $\mathscr{G}$ has the property (iv). Further, if $\bar{\mathscr{G}}_1$ is not connected and $\mathscr{H}$ is a connected component of $\bar{\mathscr{G}}_1$, by Lemma 4 (ii) holds for $\overline{\mathscr{H}\vee\mathscr{G}_2}$.

Finally, if $l=1$ and $\mathscr{G}$ is not complete, then by virtue of Lemma 4 (i) follows.

PROOF OF THEOREM 2. Let again $\mathscr{G}_1, \ldots, \mathscr{G}_l$ be the connected components of $\mathscr{G}$ with $|\mathscr{G}_l|\leqq\ldots\leqq|\mathscr{G}_1|$. In the case $l\geqq 3$, let α_i and α_j denote one vertex of $\mathscr{G}_l$ and of $\mathscr{G}_{l-1}$, respectively. Then we have

$$(\alpha_i-\alpha_j),\ (\alpha_j-\alpha_u);\ (\alpha_u-\alpha_i)\in\Gamma \tag{15}$$

and

$$(\alpha_i-\alpha_j)+(\alpha_j-\alpha_u)+(\alpha_u-\alpha_i)=0 \tag{16}$$

for each vertex α_u of $\mathscr{G}_{l-2}, \ldots, \mathscr{G}_1$. The number of these α_u is at least $|\mathscr{G}|/3$. On the other hand, since $\alpha_i-\alpha_j$ is fixed in (16), by Lemma 3 we have at most C such vertices α_u. Thus we obtain $C\geqq|\mathscr{G}|/3$ which contradicts the assumption.

Let now $l=2$. Assume that $|\mathscr{G}_2|\geqq 2$ and that $\mathscr{G}_2$ is not complete. Then (15) and (16) hold for a fixed edge $[\alpha_i, \alpha_j]$ of $\bar{\mathscr{G}}_2$ and for each vertex α_u of $\mathscr{G}_1$. Therefore, by Lemma 3 we obtain $C\geqq|\mathscr{G}|/2$ which is impossible. If $|\mathscr{G}_2|>C$ and $\mathscr{G}_1$ is not complete, we get a contradiction in a similar manner.

It remained the case $l=1$, and so our theorem is proved.

Our Theorem 3 will be deduced from Theorem 1. In deducing it, we shall use the basic idea of the proof of Theorem 1 of [15] and the following deep theorem due to ROQUETTE [26].

Lemma 5. (P. ROQUETTE, [26].) *Let R be a finitely generated integral domain over $\mathbf{Z}$. Then the invertible elements R^* of R form a finitely generated group.*

PROOF OF THEOREM 3. We may assume without loss of generality that K' contains G, and that R contains β, β^{-1}, a_0 and all the coefficients of thel inear factors $l_1, \ldots, l_n$.

Let $\mathbf{x}\in R^m$ be an arbitrary but fixed solution of (3). Put $l_j(\mathbf{x})=\beta_j$, $j=1, \ldots, n$. Since $\beta\in R^*$, we have $\beta_j\in R^*$ for each j. Let h be a fixed integer with $1\leqq h\leqq k$, and $\mathscr{I}_h$ the set of indices j satisfying $l_j\in\mathscr{L}_h$. We may suppose without loss of generality that $h\in\mathscr{I}_h$. By assumption $\mathscr{L}_h$ is connected, so if $j\in\mathscr{I}_h\setminus\{h\}$, there is a sequence $l_h=l_{j_1}, \ldots, l_{j_v}=l_j$ in $\mathscr{L}_h$ such that for each u, $1\leqq u\leqq v-1$, we have

$$\lambda'_{j_u}l_{j_u}-\lambda''_{j_{u+1}}l_{j_{u+1}}=\lambda_{j_u,u+1}l_{j_u,u+1}$$

with $l_{j_u,u+1}\in\mathscr{L}_h$ and with non-zero elements λ'_{j_u}, $\lambda''_{j_{u+1}}$, $\lambda_{j_u,u+1}$ contained in G. Since $G\subseteqq K'$ and K' is the quotient field of R, we may choose these elements λ to belong to R. Let $\mathscr{B}_h$ denote the finite subset of R consisting of 0 and $\lambda'_{j_u}\beta_{j_u}$, $\lambda''_{j_{u+1}}\beta_{j_{u+1}}$, $u=1, \ldots, v-1$, when j runs through $\mathscr{I}_h\setminus\{h\}$. The elements of $\mathscr{B}_h$ can be chosen so that Card $\mathscr{B}_h\leqq 2n$. Further, let $\mathscr{N}$ be the finite set consisting of all non-zero λ'_{j_u}, $\lambda''_{j_{u+1}}$, $\lambda_{j_u,u+1}$, $\lambda'_{j_{u+1}}-\lambda''_{j_{u+1}}$ and of the non-zero differences of λ'_{j_1} when j runs through $\mathscr{I}_h\setminus\{h\}$. Write Γ for $\mathscr{N}R^*$, where by Lemma 5 R^* is a finitely generated multiplicative group.

For fixed h and $j\in\mathscr{I}_n\setminus\{h\}$ we have now

$$\lambda'_{j_u}\beta_{j_u}-\lambda''_{j_{u+1}}\beta_{j_{u+1}}\in\Gamma,\quad u=1, \ldots, v-1,$$

and, if $\lambda'_{j_{u+1}}\neq\lambda''_{j_{u+1}}$, then

$$\lambda'_{j_{u+1}}\beta_{j_{u+1}}-\lambda''_{j_{u+1}}\beta_{j_{u+1}}\in\Gamma$$

for every u with $1\leqq u\leqq v-2$. Let us define the graph $\mathscr{G}_h=\mathscr{G}_h(\mathscr{B}_h, \Gamma)$ as in Section 2. Since both $\bar{\mathscr{G}}_h$ and $\bar{\mathscr{G}}_h^T$ are connected, by Theorem 1 we have

$$\lambda_j^*\beta_j=\eta_h\delta_j\quad\text{for all}\quad j\in\mathscr{I}_h, \tag{17}$$

where $\lambda_j^*\in\mathscr{N}$, $\eta_h\in R^*$ and δ_j can take only finitely many values. Finally, (17) holds with $\lambda_h^*=\delta_h=1$ if $\mathscr{I}_h=\{h\}$.

From (17) we get

$$\lambda_j^*l_j(\mathbf{x})=\eta_h\delta_j\quad\text{for all}\quad j\in\mathscr{I}_h. \tag{18}$$

Consider (18) as a linear equation system in $\mathbf{x}=(x_1, \ldots, x_m)$. By the hypothesis (5) x_t is uniquely determined by (18). Consequently, we have $x_t=\eta_h\varrho_h$ where there are only finitely many possibilities for ϱ_h, $h=1, \ldots, k$. Since by hypothesis $x_t\neq 0$, we obtain $\eta_h=\eta_1\varrho_1/\varrho_h$. Putting $\varrho_j=\varrho_h$ for $j\in\mathscr{I}_h$, we get

$$l_j(\mathbf{x})=\eta_1\vartheta_j,\quad j=1, \ldots, n, \tag{19}$$

where $\vartheta_j=(\varrho_1\delta_j)/(\varrho_j\lambda_j^*)$ also belong to a finite subset of K'.

In view of $F\in L[x_1, \ldots, x_m]$, $\mathscr{L}$ consists of the conjugates of l_j over L, $j=1, \ldots, n$. Since by hypothesis (4) has no non-trivial solution $\mathbf{x}$ in L^m, hence the argument of the proof of Lemma 2 of [17] applies in this more general situation as well, and it

follows that (4) has no non-trivial solution $\mathbf{x}$ in K'^m (which implies $m \leqq n$). So the $\mathbf{x}=(x_1, \ldots, x_m)\in R^m$ considered above is the only solution of (19) in K'^m. Hence we get

$$x_i = \eta_1 v_i, \quad i = 1, \ldots, m,$$

where the v_i can take only finitely many values from K'. Finally, from (3) we obtain

$$\eta_1^n F(v_1, \ldots, v_m) = \beta,$$

whence it follows that, for each fixed $(v_1, \ldots, v_m)$, η_1 also takes only finitely many values from R^*. This completes the proof of Theorem 3.

PROOF OF COROLLARY 3.1. Let $\mathbf{x}=(x_1, \ldots, x_m)\in R^m$ be an arbitrary but fixed solution of (6), and let t be the greatest integer for which $x_t \neq 0$. Since the case $t=1$ is trivial, we suppose $t \geqq 2$. Then (6) can be written in the form

$$F_t(\mathbf{x}) = \left(N_{M_t/L}(x_1+\alpha_2 x_2+\ldots+\alpha_t x_t)\right)^{n_t} = \beta$$

where $M_t=L(\alpha_2, \ldots, \alpha_t)$ and $n_t=[M:M_t]$. We can prove in the same way as in the proof of Theorem 3 of [15] that $F_t(\mathbf{x})$ satisfies all conditions of our Theorem 3, and so the assertion follows.

PROOF OF COROLLARY 3.2. It suffices to apply the above proof with $t=m$.

PROOF OF COROLLARY 3.3. The case $m=1$ being trivial, we suppose that $m \geqq 2$. Further, we may assume that $D_{M/L}(\alpha_1)\neq 0$. Indeed, if this is not the case, there are non-zero $a_2, \ldots, a_m \in R\cap L$ such that for $\alpha=\alpha_1+a_2\alpha_2+\ldots+a_m\alpha_m$ $D_{M/L}(\alpha)\neq 0$ holds. Then we can consider the equation

$$D_{M/L}(\alpha x_1^*+\alpha_2 x_2^*+\ldots+\alpha_m x_m^*) = \beta$$

in place of (7), where $x_1^*=x_1$, $x_i^*=-a_i x_1+x_i$, $i=2, \ldots, m$. This equation satisfies all conditions of Theorem 1 with $k=1$ (cf. the proof of Theorem 5 in [15]) and so the assertion is proved.

PROOF OF COROLLARY 3.4. In view of (8) every solution $\mathbf{x}\in R^{n-1}$ of (9) satisfies

$$D_{M/L}(\omega_2 x_2+\ldots+\omega_n x_n) = \beta^2 D_{M/L}(1, \omega_2, \ldots, \omega_n).$$

Since $\{1, \omega_2, \ldots, \omega_n\}$ is a basis of M/L, Corollary 3.3 applies and the assertion follows.

We shall now deduce Theorem 4 from Theorems 1 and 2. In our proof below the arguments of the proof of Theorem 1 of [16] will be utilized.

PROOF OF THEOREM 4. Let f be an arbitrary but fixed monic polynomial in $R[x]$ with $D(f)\in\delta S$ and with roots $\alpha_1, \ldots, \alpha_n$ in G. Then all α_i belong to the integral closure T of R in G. Since S is finitely generated, $D(f)$ can be written in the form $\gamma^{n(n-1)}\beta$ where $\gamma\in S$ and β belongs to a finite subset of δS. Consequently, it suffices to prove our assertion for a fixed β. Then we get

$$\prod_{1\leqq i<j\leqq n} (\alpha_j/\gamma-\alpha_i/\gamma)^2 = \beta. \tag{20}$$

Since R is finitely generated over $\mathbf{Z}$, by a well-know theorem (see e.g. [33], Ch. V, Th. 7) T is contained in a finitely generated subring of G over $\mathbf{Z}$. Thus the ring $A=T[S^{-1}, \beta^{-1}]$ generated by $\{s^{-1}|s\in S\}$ and β^{-1} over T is also contained in a ring of this type. By Lemma 5 the invertible elements of this latter ring form a finitely generated group. A^* being a subgroup of this group, it is also finitely generated.

Since $\alpha_j/\gamma-\alpha_i/\gamma\in A$ and $\beta\in A^*$, it follows from (20) that

$$\alpha_j/\gamma-\alpha_i/\gamma\in A^* \tag{21}$$

for each distinct j, i with $1\leqq j, i\leqq n$. Consider the graph $\mathscr{G}$ whose vertices are the elements $\alpha_1/\gamma, \ldots, \alpha_n/\gamma$ and whose edges are the unordered pairs $[\alpha_j/\gamma, \alpha_i/\gamma]$ not satisfying (21). Then $\mathscr{G}$ has only isolated vertices, and so, by Theorem 2, n is bounded. Further, by virtue of Theorem 1 we have

$$\alpha_j/\gamma-\alpha_i/\gamma=\varepsilon\varepsilon_{ij}, \quad 1\leqq i<j\leqq n, \tag{22}$$

with some $\varepsilon\in A^*$ and with $\varepsilon_{ij}\in A^*$ taking only finitely many values. (22) and (20) imply that for fixed β the number of these ε is also finite. Thus, we have

$$\alpha_j/\gamma-\alpha_i/\gamma=\varrho_{ji}, \quad 1\leqq i<j\leqq n, \tag{23}$$

where $\varrho_{ji}\in T[S^{-1}]$ can take only finitely many values.

For fixed β and n, let us fix now such a system of elements ϱ_{ji} $(1\leqq i<j\leqq n)$. Consider all the pairs f, γ (f with roots $\alpha_1, \ldots, \alpha_n$) satisfying (20) and (23). By Lemma 2 there are finitely many γ^* among the γ under consideration such that any of these γ can be written as $\gamma=\gamma^*\eta$ with some γ^* and $\eta\in S$. Consequently, among the pairs considered there are finitely many ones f^*, γ^* (f^* with roots $\alpha_1^*, \ldots, \alpha_n^*$) such that for every f, γ considered above

$$\frac{\alpha_j-\alpha_i}{\gamma}=\frac{\alpha_j^*-\alpha_i^*}{\gamma^*}, \quad 1\leqq i<j\leqq n, \tag{24}$$

holds with some γ^* and $\alpha_1^*, \ldots, \alpha_n^*$ such that $\gamma/\gamma^*=\eta\in S$. But $\alpha_1+\ldots+\alpha_n=a$ and $\alpha_1^*+\ldots+\alpha_n^*=a^*$ lie in R, so (24) gives

$$n(\alpha_j-\eta\alpha_j^*)=a-\eta a^*, \quad j=1, \ldots, n.$$

This implies that the element $\alpha_j-\eta\alpha_j^*$ lies in L. Further, this element is integral over R. Since by hypothesis R is integrally closed, hence $\alpha_j-\eta\alpha_j^*$ takes the same value from R for each j, and so $f(x)$ is R-equivalent to $\eta^n f^*(\eta^{-1}x)$. This completes the proof.

We deduce now Theorem 5 from Theorem 4.

Proof of Theorem 5. Let G be the normal closure of the extension K/L. Let α be an arbitrary element of T with $D_{K/L}(\alpha)\in\delta S$. Since $D_{K/L}(\alpha)\neq 0$, α is a primitive element of K/L. Denote by $f(x)$ the minimal polynomial of α over L. R being integrally closed, by a well-know theorem (cf. [33], Ch. V, Th. 4) we have $f\in R[x]$. Further, $D(f)=D_{K/L}(\alpha)$ and all roots of f lie in G. We can now apply Theorem 5 and the assertion immediately follows.

PROOF OF COROLLARY 5.2. Let α be an arbitrary element in T with $D_{K/L}(\alpha)\in\delta S$ and $N_{K/L}(\alpha)\in\mu Q$. By Theorem 5 we have

$$\alpha = a+\eta\alpha^*$$

with some $a\in R$, $\eta\in S$ and $\alpha^*\in\mathscr{E}$ (where $\mathscr{E}$ is a finite subset of T). Since Q is finitely generated, every element of μQ can be written in the form $\mu'\tau^n$ with $\tau\in Q$ and with $\mu'\in\mu Q$ which can take only finitely many values. It suffices to prove the assertion for fixed α^* and μ'. Then, if $n\geqq 3$, from Corollary 3.1 it follows that the equation

$$N_{K/L}\big((a/\tau)+(\eta/\tau)\alpha^*\big) = \mu' \tag{25}$$

has only finitely many solutions in a/τ, η/τ with a, η, τ having the properties specified above.

The multiplicative semigroup $\{S, Q\}$ generated by S and Q is finitely generated. In $\{S, Q\}$ consider all the elements $\eta\tau$ $(\eta\in S,\ \tau\in Q)$ for which η/τ has the same value. Using Lemma 2 and the hypothesis $S\cap Q=\{1\}$, we can easily see that there are only finitely many η and τ with this property. Thus, in (25) there are only finitely many possibilities for a and so, in case $n\geqq 3$, our assertion is proved.

When $n=2$, we can reduce the equation (25) to the equation (10) and we obtain then that η/τ can take only finitely many values. Then the above argument applies and this completes the proof.

PROOF OF COROLLARY 5.4. Suppose that there exists $\alpha\in T'$ with the property $T'=R[\alpha]$. Then $D_{K/L}(\alpha)=\delta$ is a non-zero element in R. Since $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of T' as an R-module, a standard argument shows (see [33] or [25]) that δ divides $D_{K/L}(\alpha')$ in R for every $\alpha'\in T'$. From this follows that if $T'=R[\alpha']$ with another $\alpha'\in T'$ then $D_{K/L}(\alpha')\in\delta R^*$. Thus Theorem 5 gives $\alpha'=a+\eta\alpha^*$ with some $a\in R$, $\eta\in R^*$ and with an α^* belonging to a finite subset of the integral closure of R in K. Because of $T'\supset R$ we have now $\alpha^*\in T'$ and $T'=R[\alpha^*]$. This proves our assertion.

References

[1] C. BERGE, Graphs and hypergraphs, *Amsterdam—London—New York*, 1973.

[2] B. J. BIRCH and J. R. MERRIMAN, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* **25** (1972), 385—394.

[3] Z. I. BOREVICH and I. R. SHAFAREVICH, Number theory, *New York and London*, 1967.

[4] K. GYŐRY, Sur l'irréductibilité d'une classe des polynômes, II. *Publ. Math. (Debrecen)* **19** (1972), 293—326.

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

[6] K. GYŐRY, Sur les polynômes à coefficients entiers et de discriminant donné, II. *Publ. Math. (Debrecen)* **21** (1974), 125—144.

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

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

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

[10] K. GYŐRY, Corps de nombres algébriques d'anneau d'entiers monogène, *Séminaire Delange—Pisot—Poitou (Théorie des nombres)*, 20e année, n° 26, 7 p, Paris (1978/1979).

[11] K. GYŐRY, On certain graphs composed of algebraic integers of a number field and their applications I. *Publ. Math. (Debrecen)*, **27** (1980), 229—242.
[12] K. GYŐRY, Explicit upper bounds for the solutions of some diophantine equations, *Ann. Acad. Sci. Fenn. Ser. A I Math.* **5** (1980), 3—12.
[13] 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.
[14] K. GYŐRY, Sur certaines généralisations de l'équation de Thue—Mahler, *Enseignement Math.* **26** (1980), 247—255.
[15] K. GYŐRY, On the representation of integers by decomposable forms in several variables, *Publ. Math. (Debrecen)*, **28** (1981), 89—98.
[16] K. GYŐRY, On discriminants and indices of integers of an algebraic number field, *J. Reine Angew. Math.* **324** (1981), 114—126.
[17] 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.
[18] K. GYŐRY and Z. Z. PAPP, On discriminant form and index form equations, *Studia Sci. Math. Hungar.* **12** (1977), 47—60.
[19] S. LANG, Integral points on curves, *Inst. Hautes Études Sci. Publ. Math.* No. **6** (1960), 27—43.
[20] S. LANG, Diophantine geometry, *New York and London*, 1962.
[21] S. LANG, Higher dimensional diophantine problems, *Bull. Amer. Math. Soc.* **80** (1974), 779—787.
[22] L. LOVÁSZ, Combinatorial problems and exercises, *Budapest*, 1979.
[23] R. C. LYNDON and P. E. SCHUPP, Combinatorial group theory, *Berlin—Heidelberg—New York*, 1977.
[24] M. NAGATA, A general theory of algebraic geometry over Dedekind domains, I. *Amer. J. Math.* **78** (1956), 78—116.
[25] L. RÉDEI, Algebra, *Budapest*, 1967.
[26] P. ROQUETTE, Einheiten und Divisorenklassen in endlich erzeugbar Körpern, *J. Deutsch. Math. Verein.* **60** (1957), 1—21.
[27] H. P. SCHLICKEWEI, On norm form equations, *J. Number Theory*, **9** (1977), 370—380.
[28] W. M. SCHMIDT, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191** (1971), 1—20.
[29] C. L. SIEGEL, Über einige Anwendungen Diophantischer Approximationen, *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.* (1929), 1—70.
[30] L. A. TRELINA, On algebraic integers with discriminant containing fixed prime divisors, *Mat. Zametki* **21** (1977), 289—296.
[31] L. A. TRELINA, On the greatest prime factor of an index form, *Dokl. Akad. Nauk BSSR* **21** (1977), 975—976.
[32] A. T. WHITE, Graphs, groups and surfaces, *Amsterdam—London—New York*, 1973.
[33] O. ZARISKI and P. SAMUEL, Commutative algebra, Vol. I., *Toronto—New York—London*, 1958.

K. GYŐRY
MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 DEBRECEN, HUNGARY

(Received December 18, 1978; revised September 29, 1980)