Acta Math. Hung.
51 (3—4) (1988), 341—362.

ON THE NUMBER OF POLYNOMIALS AND INTEGRAL ELEMENTS OF GIVEN DISCRIMINANT

J. H. EVERTSE* (Amsterdam) and K. GYŐRY* (Debrecen)

§ 1. Introduction

Let K be a field of characteristic 0, let R be a subring of K which has K as its quotient field, let G be a finite, normal extension of K and let R' be an integral extension ring of R in G. We shall suppose that either R is finitely generated over $\mathbf{Z}$ (we shall refer to this as the *absolute case*) or R is finitely generated over a field $\mathbf{k}$ of characteristic 0 which is algebraically closed in K (this will be called the *relative case*). Let $n \geqq 2$ be an integer. By $\Phi(n, R, R')$ we shall denote the set of all polynomials $f(X) \in R[X]$ of degree n which are monic and all of whose zeros are simple and belong to R'. By $\Phi(R, R')$ we denote the set $\bigcup_{n \geqq 2} \Phi(n, R, R')$. Let β be a fixed, non-zero element of R. We shall study the sets of polynomials $f(X) \in \Phi(R, R')$ satisfying

$$D(f) = \beta \tag{1}$$

or more generally

$$D(f) \in \beta R^*.[1] \tag{2}$$

Here $D(f)$ denotes the discriminant of f, i.e. if $f(X) = (X - \alpha_1)\dots(X - \alpha_n)$, then

$$D(f) = \prod_{1 \leqq i < j \leqq n} (\alpha_i - \alpha_j)^2.$$

We call two polynomials $f(X)$, $g(X) \in R[X]$ *R-equivalent* if $g(X) = f(X + a)$ for some $a \in R$ and *weakly R-equivalent* if $g(X) = u^{\deg f} f(X/u + a)$ for some $u \in R^*$ and $a \in R$. The corresponding equivalence classes will be called R-equivalence classes and weak R-equivalence classes, respectively. If two polynomials f, g are R-equivalent then $D(f) = D(g)$ whereas if f, g are weakly R-equivalent then $D(f) = \varepsilon D(g)$ with some $\varepsilon \in R^*$.

In the absolute case Győry [6], [7] proved that if R is integrally closed in K then the polynomials $f(X) \in \Phi(R, R')$ which satisfy (1) belong to at most finitely many R-equivalence classes and the polynomials $f(X) \in \Phi(R, R')$ satisfying (2) belong to at most finitely many weak R-equivalence classes. Further, in [8] he showed that these equivalence classes can be determined effectively provided that R, K, G, R' and β are given explicitly in a certain well-defined sense (cf. [8], § 2.1). As consequences, in [8] (cf. also [9]) he obtained effective finiteness theorems for integral elements with

* The research was done at the University of Leiden in the academic year 1983/1984.
[1,2] If R is a ring, then R^* denotes its group of units and R^+ its additive group.

given discriminant (or which is the same, for irreducible polynomials with given discriminant) and for power bases over R. In [8], he also established effective results in the relative case by giving an effective bound for the Degree (cf. [8], § 2.1) of an appropriate representative of an arbitrary equivalence class. However, these assertions do not lead to finiteness results. For other historical remarks on (1), (2) and for further references, we refer to [4] and [9].

If R is integrally closed in K then $R'\cap K=R$. In the present paper our results will be established in the more general case when R^{+} [2] is a subgroup of finite index in $(R'\cap K)^{+}$. We shall derive both in the absolute and in the relative case explicit upper bounds for the number of R-equivalence classes of polynomials $f\in\Phi(R, R')$ satisfying (1) and for the number of weak R-equivalence classes of polynomials $f\in\Phi(R, R')$ satisfying (2). However, in the relative case we have to restrict ourselves to non-special polynomials (cf. §§ 3, 5). In both cases, we have attempted to give bounds which depend minimally on K, R, G, R' and β. For example, if in particular K is an algebraic number field with degree d and R is its ring of integers then our bounds depend only on d, $[G\colon K]$ and the number of distinct prime ideal divisors of β.

Our results concerning polynomials will be formulated in § 3. In § 4 we shall deduce similar quantitative finiteness results on integral elements over R with given discriminant and shall point out that our finiteness assertions do not remain valid if the factor group $(R'\cap K)^{+}/R^{+}$ is infinite. As a consequence, we shall give there among other things a generalisation of a result obtained on power bases in [3], which states that for every algebraic number field K of degree d the maximal number of pairwise weakly $\mathbf{Z}$-inequivalent algebraic integers $\alpha\in K$ for which $\{1, \alpha, \dots, \alpha^{d-1}\}$ is an integral basis of K is bounded above by a constant depending on d only. Here $\alpha, \beta\in K$ are called weakly $\mathbf{Z}$-equivalent if $\beta=\pm\alpha+a$ with some $a\in\mathbf{Z}$.

Our theorems will be proved in §§ 5 to 9. The proofs are based on some recent quantitative finiteness results on unit equations, due to Evertse [2] and Evertse and Győry [3].

§ 2. Preliminaries and notations

Let R_0 be either $\mathbf{Z}$ (the absolute case) or a field $\mathbf{k}$ of characteristic 0 (the relative case) and let K_0 denote the quotient field of R_0. (Thus $K_0=\mathbf{Q}$ if $R_0=\mathbf{Z}$ and $K_0=\mathbf{k}$ if $R_0=\mathbf{k}$). Let K be a finitely generated extension field of K_0. In case $R_0=\mathbf{k}$ we suppose that $\mathbf{k}$ is algebraically closed in K. The field K has a finite transcendence basis over K_0, $\{z_1, \dots, z_q\}$ say, where $q\geqq 0$. Put $K_1=K_0(z_1, \dots, z_q)$ and $R_1=R_0[z_1, \dots, z_q]$. Then K is a finite extension of K_1. Put $d=[K\colon K_1]$. We have the following diagram:

$$\begin{array}{ccccc} & & & & K \\ & & & & \cup \\ R_1 & = & R_0[z_1, \dots, z_q] & \subset & K_1 = K_0(z_1, \dots, z_q) \\ & & \cup & & \cup \\ & & R_0 & \subset & K_0 \end{array}$$

We note that R_1 is a unique factorisation domain with unit group $R_0^*=\{1, -1\}$ if $R_0=\mathbf{Z}$ and $R_0^*=\mathbf{k}^*$ if $R_0=\mathbf{k}$. Let I denote a maximal set of pairwise non-associated irreducible elements of R_1. To every $\pi \in I$ there corresponds a valuation[3] v_π on K_1 which is defined by $v_\pi(\pi)=1$ and $v_\pi(a/b)=0$ for any $a, b \in R_1$ not divisible by π. Note that for every $\alpha \in K_1^*$ there are at most finitely many $\pi \in I$ with $v_\pi(\alpha) \neq 0$. Every valuation v_π with $\pi \in I$ can be extended in at most d pairwise inequivalent ways to K. By replacing these extensions by equivalent valuations if necessary we obtain a set of valuations m_K on K with the following properties:

(3) every $V \in m_K$ has value group $\mathbf{Z}$;

(4) if $\alpha \in K^*$ then $V(\alpha)=0$ for all but finitely many $V \in m_K$;

(5) if $\alpha \in R_1$ then $V(\alpha) \geqq 0$ for all $V \in m_K$;

(6) if $\alpha \in R_0^*$ then $V(\alpha)=0$ for all $V \in m_K$.

In the sequel we shall use the following notations. If T is a subset of m_K, then we denote by $\mathcal{O}_T$ the ring $\{\alpha \in K : V(\alpha) \geqq 0$ for all $V \in m_K \setminus T\}$. Note that $\mathcal{O}_T^* = \{\alpha \in K : V(\alpha)=0$ for all $V \in m_K \setminus T\}$.

If L/K is a finite extension, of degree p say, then one can construct in a similar way as above a set of valuations m_L on L with value group $\mathbf{Z}$. If we choose the same transcendence basis $\{z_1, \ldots, z_q\}$ for L, these valuations are, up to equivalence, just the extensions of the valuations in m_K to L. If $V \in m_K$, $W \in m_L$ and if W is equivalent to an extension of V to L then we say that W lies above V. For every $V \in m_K$ there are at most p valuations $W \in m_L$ lying above V.

The elements of the abelian group generated by m_K will be called *divisors*. Thus every divisor $\mathfrak{h}$ can be expressed as

$$\mathfrak{h} = \sum_{V \in m_K} V(\mathfrak{h}) V,$$

where the $V(\mathfrak{h})$ are integers of which at most finitely many are non-zero. If $\alpha \in K^*$ then the divisor (α) is defined by $(\alpha) = \sum_{V \in m_K} V(\alpha) V$. If K is an algebraic number field then there exists an isomorphism $\mathfrak{C}_K$ of the additive group of divisors of K onto the multiplicative group of fractional ideals in K which is defined by $\mathfrak{C}_K(\mathfrak{h}) = \{\alpha \in K : V(\alpha) \geqq V(\mathfrak{h})$ for all $V \in m_K\}$. $\mathfrak{C}_K$ maps m_K onto the set of prime ideals in K.

Let L/K be a finite extension of degree p in a fixed, finite, normal extension G of K. Let $\sigma_1, \ldots, \sigma_p$ denote the distinct K-isomorphisms of L in G and if $\alpha \in L$ put $\sigma_i(\alpha) = \alpha^{(i)}$. If $\mathbf{x} = (x_1, \ldots, x_p) \in L^p$ then

$$D(\mathbf{x}) = [\det(x_j^{(i)})_{\substack{i=1,\ldots,p \\ j=1,\ldots,p}}]^2$$

denotes the discriminant of $\mathbf{x}$ with respect to L/K. It is known that $D(\mathbf{x}) \neq 0$ if and only if $x_1, \ldots, x_p$ are linearly independent over K. If $\mathbf{x} = (1, \alpha, \ldots, \alpha^{p-1})$ for some $\alpha \in L$ then we put $D_{L/K}(\alpha) = D(\mathbf{x})$. Then we have

(7) $$D_{L/K}(\alpha) = \prod_{1 \leqq i < j \leqq p} (\alpha^{(i)} - \alpha^{(j)})^2.$$

[3] By a valuation we shall always mean an additive, non-trivial, discrete valuation. By an absolute value we shall mean a non-trivial multiplicative valuation.

Finally, if $\mathbf{x}=(x_1, \ldots, x_p)$, $\mathbf{y}=(y_1, \ldots, y_p)\in L^p$ are vectors such that $y_i=\sum_{j=1}^{p} \xi_{ij}x_j$ for certain $\xi_{ij}\in K$, then

$$D(\mathbf{y}) = [\det (\xi_{ij})_{\substack{i=1,\ldots,p\\ j=1,\ldots,p}}]^2 D(\mathbf{x}). \tag{8}$$

Let R' be a subring of L having L as its quotient field. We define the *discriminant divisor* $\mathfrak{D}_K(R')$ of R' over K by

$$V(\mathfrak{D}_K(R')) = \max\{0, \min_{\mathbf{x}\in R'^p} V(D(\mathbf{x}))\} \quad \text{for all} \quad V\in m_K.$$

By (4) this is indeed a divisor. If K is an algebraic number field and if R' is the ring of integers of L then the ideal $\mathfrak{C}_K(\mathfrak{D}_K(R'))$ is just the discriminant of L over K.

Let R be a subring of K and suppose that R' is an integral extension ring of R in L and that R' is a free R-module with basis $\mathbf{w}=(\omega_1, \ldots, \omega_p)$ say. Let T be a subset of m_K such that $R\subset\mathcal{O}_T$. If $\mathbf{w}'$ is an arbitrary vector in R'^p then, by (8),

$$D(\mathbf{w}')\in D(\mathbf{w})R. \tag{9}$$

Hence

$$V(\mathfrak{D}_K(R')) = V(D(\mathbf{w})) \quad \text{for all} \quad V\in m_K\setminus T. \tag{10}$$

§ 3. On polynomials with given discriminant

Let K, R_0, K_0, $\{z_1, \ldots, z_q\}$, R_1, K_1, d, m_K have the same meaning as in § 2. Thus R_0 is either $\mathbf{Z}$ (the absolute case) or a field $\mathbf{k}$ of characteristic 0 which is algebraically closed in K (the relative case). Let G/K be a finite, normal extension of degree g. Let $\overline{K}_0=K_0(=\mathbf{Q})$ if $R_0=\mathbf{Z}$ and let $\overline{K}_0$ be the algebraic closure of $K_0(=\mathbf{k})$ in G in the relative case. Let R be a subring of K which is finitely generated over R_0 and which has K as its quotient field. Further, let R' be an integral extension ring of R in G such that

$$\mathscr{I} := (R'\cap K^+)\colon R^+] < \infty. \tag{11}$$

We note that if R is integrally closed in K then $\mathscr{I}=1$. Further, in the relative case (11) implies that $\mathscr{I}=1$, i.e. $R'\cap K=R$. Indeed, if (in the relative case) $R'\cap K\neq R$ and $a\in(R'\cap K)\setminus R$ then the elements in $a\mathbf{k}$ are contained in distinct cosets of $(R'\cap K)^+/R^+$. Hence $\mathscr{I}=\infty$.

Let β be a fixed, non-zero element of R and let T, T' be the smallest subsets of m_K such that $R\subset\mathcal{O}_T$, $R[\beta^{-1}]\subset\mathcal{O}_{T'}$. Then, by (4), T, T' have finite cardinalities, t, t' respectively, say.

Before stating our results we have to introduce the notion of *special* polynomials. In the absolute case, every polynomial $f(X)\in R[X]$ is called non-special. In the relative case, a polynomial $f(X)$ is called *special* in $R[X]$ if $f(X)\in R[X]$ and if

$$f(X) = \mu^r h((X+a)^{n_0}/\mu)(X+a)^{\delta}, \tag{12}$$

where r, n_0, δ are integers with $r>0$, $n_0>0$, $\delta\in\{0, 1\}$, $rn_0+\delta\geqq 3$ and $\delta=0$ if $n_0=1$, where $a\in R$, where $\mu\in K^*$ is integral over R and where $h(X)\in\mathbf{k}[X]$ is a monic poly nomial of degree r with non-zero discriminant[4] which has its zeros in $\bar{K}_0$ and $h(0)\neq 0$ if $n_0>1$. The polynomial $f\in R[X]$ is called non-special if it is not of the type (12). We notice that all polynomials which are weakly R-equivalent to a special polynomial in $R[X]$ must be special in $R[X]$ themselves.

As in § 1, $\Phi(n, R, R')(n\geqq 2)$ denotes the set of all monic polynomials of degree n with coefficients in R and with only simple zeros belonging to R'. Further, we put $\Phi(R, R')=\bigcup_{n\geqq 2} \Phi(n, R, R')$. By $N_1(R, R', \beta)$, $N_1(n, R, R', \beta)$ we shall denote the number of R-equivalence classes of *non-special* polynomials $f\in\Phi(R, R')$ and $f\in\Phi(n, R, R')$ respectively, which satisfy

$$D(f)=\beta, \tag{1}$$

whereas by $N_2(R, R', \beta)$, $N_2(n, R, R', \beta)$ we shall denote the number of weak R-equivalence classes of *non-special* polynomials $f\in\Phi(R, R')$ and $f\in\Phi(n, R, R')$ respectively, which satisfy

$$D(f)\in\beta R^*. \tag{2}$$

THEOREM 1. *Let n be an integer with $n\geqq 2$. Both in the absolute and in the relative case we have*

$$N_1(n, R, R', \beta)\leqq n(n-1)\frac{(4\cdot 7^{g(3d+2t')})^{n-2}}{(n-2)!}\mathscr{I},$$

$$N_2(n, R, R', \beta)\leqq \{n(n-1)\}^{[\bar{K}_0:\,K_0](d+t)}\frac{(4\cdot 7^{g(3d+2t')})^{n-2}}{(n-2)!}\mathscr{I}.$$

Let $\mathscr{W}_1$ be the set of special polynomials in $\Phi(n, R, R')$ satisfying (1) and let $\mathscr{W}_2$ be the set of special polynomials in $\Phi(n, R, R')$ satisfying (2) ($n\geqq 3$). We shall prove in § 5 that in the relative case $\mathscr{W}_2$ contains infinitely many weak R-equivalence classes, provided that $R'\supset\bar{K}_0$ and that $\mathscr{W}_2$ contains a special polynomial with $r\geqq 2$. We shall also show that $\mathscr{W}_1$ contains infinitely many R-equivalence classes in case $\mathbf{k}$ is algebraically closed and $\mathscr{W}_1$ contains a special polynomial with $r\geqq 2$.

We shall now present some consequences of Theorem 1.

COROLLARY 1. *Both in the absolute and in the relative case we have*

$$N_1(R, R', \beta)\leqq\mathscr{I}\exp\{8\cdot 7^{g(3d+2t')}\},$$

$$N_2(R, R', \beta)\leqq\mathscr{I}\exp\{8[\bar{K}_0:K_0](d+t)\cdot 7^{g(3d+2t')}\}.$$

PROOF. For $A=4\cdot 7^{g(3d+2t')}$ and for $p\in\mathbf{Z}$, $p\geqq 1$, we have, since $\{(k+2)(k+1)\}^p\leqq 2(p+1)^{2p+k-2}$ for $k\geqq 0$,

$$\sum_{k=0}^{\infty}\{(k+2)(k+1)\}^p\frac{A^k}{k!}\mathscr{I}\leqq 2(p+1)^{2p-2}\mathscr{I}\sum_{k=0}^{\infty}\frac{\{(p+1)A\}^k}{k!}=$$

$$=2(p+1)^{2p-2}\mathscr{I}e^{pA}\leqq\mathscr{I}e^{2pA}.$$

Hence our assertion follows from Theorem 1.

[4] For a linear polynomial $h(X)$, we put $D(h)=1$.

COROLLARY 2. *Let* $\gamma \in R$. *Then both in the absolute and in the relative case*
(i) *for every* $n \geqq 2$ *the number of non-special polynomials* $f \in \Phi(n, R, R')$ *which satisfy* (1) *and* $f(0)=\gamma$ *is at most*

$$n^2(n-1)\frac{(4 \cdot 7^{g(3d+2t')})^{n-2}}{(n-2)!},$$

(ii) *the number of non-special polynomials* $f \in \Phi(R, R')$ *which satisfy* (1) *and* $f(0)=\gamma$ *is at most*

$$\exp\{8 \cdot 7^{g(3d+2t')}\}.$$

PROOF. The ring $\tilde{R}=R' \cap K$ is finitely generated over R_0 (cf. [11], [12]). In the relative case (11) implies $\tilde{R}=R$. Further, both in the absolute and the relative case $\tilde{R} \subset \mathcal{O}_T$, $\tilde{R}[\beta^{-1}] \subset \mathcal{O}_{T'}$. Since $\Phi(n, R, R') \subset \Phi(n, \tilde{R}, R')$ and $\Phi(R, R') \subset \Phi(\tilde{R}, R')$, it suffices to prove our assertion with $\tilde{R}$ instead of R. The first part of Corollary 2 follows now immediately from Theorem 1, on noting that all polynomials in a fixed $\tilde{R}$-equivalence class are of the type $f(X)=f_0(X+a)$, where $a \in \tilde{R}$ and f_0 is a fixed representative of this class, and that there are at most n values of a for which $f_0(a)=\gamma$. The second part of Corollary 2 follows at once from the first part, on noting that for $A=4 \cdot 7^{g(3d+2t')}$,

$$\sum_{k=0}^{\infty} (k+2)^2(k+1)\frac{A^k}{k!} = (A^3+8A^2+14A+4)e^A \leqq e^{2A}.$$

Corollary 1 already shows that a polynomial $f \in \Phi(R, R')$ which is non-special and which satisfies (2) must have bounded degree. More explicitly we have

THEOREM 2. *Both in the absolute and the relative case, every non-special polynomial* $f \in \Phi(R, R')$ *which satisfies* (2) *has degree at most*

$$2+4 \cdot 7^{g(3d+2t')}.$$

In the absolute case, the finiteness assertions of Theorems 1, 2 and their corollaries above were earlier proved by Győry [6] (cf. also Győry [7]) under the restriction that R is integrally closed in K. Effective versions of these results were later obtained by Győry [8]. Further, he established in [8] certain effective analogues also in the relative case.

We shall now specialise our results above to the case of algebraic number fields. Let K be an algebraic number field of degree d with ring of integers $\mathcal{O}_K$ and let G/K be a normal extension of degree g. Let $\mathcal{O}_G$ be the ring of integers of G. Let $\beta \in \mathcal{O}_K \setminus \{0\}$ and let $S=\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a (possibly empty) set of prime ideals in K. Let t' denote the number of prime ideals which belong to S or divide $\langle\beta\rangle$.[5] We call two polynomials $f(X), g(X) \in \mathcal{O}_K[X]$ *weakly S-equivalent* if there are $a, b, c \in \mathcal{O}_K$ such that $\langle b\rangle$, $\langle c\rangle$ are solely composed of prime ideals from S (b, c are units if $t=0$) and such that

$$g(X) = \left(\frac{b}{c}\right)^{\deg f} f\left(\frac{cX+a}{b}\right).$$

[5] $\langle\alpha\rangle$ denotes the ideal in $\mathcal{O}_K$ generated by α.

COROLLARY 3. *Let n be an integer with $n \geqq 2$. Then the polynomials $f(X) \in \Phi(n, \mathcal{O}_K, \mathcal{O}_G)$ with the property*

$$(13) \qquad \langle D(f) \rangle = \langle \beta \rangle \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_t^{k_t}$$

for certain rational integers $k_1, \dots, k_t$ belong to at most

$$\{n(n-1)\}^{d+t} \frac{(4 \cdot 7^{g(3d+2t')})^{n-2}}{(n-2)!}$$

weak S-equivalence classes.

For an effective finiteness result concerning the polynomials $f \in \Phi(n, \mathcal{O}_K, \mathcal{O}_G)$ which satisfy (13), see Győry [5].

PROOF OF COROLLARY 3. Let $\mathfrak{C}_K$ be the isomorphism of the group of divisors of K onto the group of fractional ideals in K (cf. § 2) and let $T = \mathfrak{C}_K^{-1}(S)$. Now Corollary 3 follows at once from Theorem 1 on noting that every polynomial $f(X) \in \Phi(n, \mathcal{O}_K, \mathcal{O}_G)$ which satisfies (13) also satisfies $D(f) \in \beta \mathcal{O}_T^*$ and that two polynomials $f(X), g(X) \in \Phi(n, \mathcal{O}_K, \mathcal{O}_G)$ are weakly S-equivalent if and only if they are weakly $\mathcal{O}_T$-equivalent.

§ 4. On integral elements with given discriminant

Let K, R_0, K_0, $\{z_1, \dots, z_q\}$, R_1, K_1, d, m_K have the same meaning as in § 2. Let L/K be a finite extension of degree $m \geqq 2$ and let G denote the normal closure of L over K. Put $[G: K] = g$. In the relative case (when $R_0 = \mathbf{k}$) we assume something stronger than in § 2, namely that $\mathbf{k}$ is algebraically closed in G. Let $\sigma_1, \dots, \sigma_m$ denote the distinct K-isomorphisms of L in G. If $\alpha \in L$ then we put $\alpha^{(i)} = \sigma_i(\alpha)$, $i = 1, \dots, m$. Let R be a subring of K which is finitely generated over R_0 and let $R' \subset L$ be an integral extension ring of R with quotient field L such that

$$(11) \qquad \mathscr{I} = [(R' \cap K)^+ : R^+] < \infty.$$

If $\alpha \in R'$, then by (7) the discriminant $D_{L/K}(\alpha)$ of α is equal to $\prod_{1 \leqq i < j \leqq d} (\alpha^{(i)} - \alpha^{(j)})^2$. Hence if $L = K(\alpha)$ then $D_{L/K}(\alpha)$ is equal to the discriminant of the minimal polynomial of α over K. For that reason we call two elements $\alpha_1, \alpha_2 \in R'$ *R-equivalent* if $\alpha_2 = \alpha_1 + a$ for some $a \in R$ and *weakly R-equivalent* if $\alpha_2 = u\alpha_1 + a$ for some $a \in R$, $u \in R^*$. As usual, the corresponding equivalence classes will be called R-equivalence classes and weak R-equivalence classes, respectively. If $\alpha_1, \alpha_2 \in R'$ are R-equivalent then $D_{L/K}(\alpha_1) = D_{L/K}(\alpha_2)$ while if $\alpha_1, \alpha_2 \in R'$ are weakly R-equivalent then $D_{L/K}(\alpha_1) = \varepsilon D_{L/K}(\alpha_2)$ with some $\varepsilon \in R^*$.

Let T be the smallest subset of m_K such that $R \subset \mathcal{O}_T$. Let $\mathfrak{D}_K(R')$ be the discriminant divisor of R' over K and let β be a fixed element of K^*. Let T'' be the smallest subset of m_K such that $R \subset \mathcal{O}_{T''}$ and $V(\beta) = V(\mathfrak{D}_K(R'))$ for all $V \in m_K \setminus T''$. The sets T, T'' have finite cardinalities t, t'' respectively, say. Let $M_1(R, R', \beta)$ denote the number of R-equivalence classes of $\alpha \in R'$ satisfying

$$(14) \qquad D_{L/K}(\alpha) = \beta$$

and let $M_2(R, R', \beta)$ denote the number of weak R-equivalence classes of $\alpha \in R'$ satisfying

$$D_{L/K}(\alpha) \in \beta R^*. \tag{15}$$

THEOREM 3. *Both in the absolute and the relative case we have*

$$M_1(R, R', \beta) \leqq m(m-1)(4 \cdot 7^{g(3d+2t'')})^{m-2} \cdot \mathscr{I},$$

$$M_2(R, R', \beta) \leqq \{m(m(-1)\}^{d+t}(4 \cdot 7^{g(3d+2t'')})^{m-2} \cdot \mathscr{I}.$$

We note that $g \leqq m!$. Notice that we have also a finiteness result (without exclusion of "special" integral elements) in the relative case. It is not clear whether such a finiteness result holds if $\mathbf{k}$ is not algebraically closed in G. Finally, we remark that if $\mathscr{I} = \infty$ and if there is an $\alpha \in R'$ satisfying (14) (resp. (15)) then $M_1(R, R', \beta)$ (resp. $M_2(R, R', \beta)$) is infinite. Indeed, in this case the (weak) $(R' \cap K)$-equivalence class of α in question splits into infinitely many (weak) R-equivalence classes.

Let $N_{L/K}$ denote the norm with respect to L/K. Then every $(R' \cap K)$-equivalence class of elements of R' contains at most m elements α for which $N_{L/K}(\alpha)$ assumes some fixed value. Thus, applying Theorem 3 to $M_1(R' \cap K, R', \beta)$ we have

COROLLARY 4. *Let $\gamma \in K$. Then the number of $\alpha \in R'$ with $D_{L/K}(\alpha) = \beta$ and $N_{L/K}(\alpha) = \gamma$ is at most*

$$m^2(m-1)(4 \cdot 7^{g(3d+2t'')})^{m-2}.$$

The above argument shows that Corollary 4 is true without assuming $\mathscr{I} < \infty$.

Let $\alpha \in R'$. We call $\{1, \alpha, \ldots, \alpha^{m-1}\}$ a *power basis* if $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis of R' as a free R-module. If this is the case and if $\alpha' \in R'$ is weakly R-equivalent to α then $\{1, \alpha', \ldots, \alpha'^{m-1}\}$ is also an R-basis of R'. From Theorem 3 it follows

COROLLARY 5. *Those $\alpha \in R'$ for which $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is an R-basis of R' belong to at most*

$$\{m(m-1)\}^{d+t}(4 \cdot 7^{g(3d+2t)})^{m-2} \cdot \mathscr{I}$$

weak R-equivalence classes.

In [3] (cf. Theorem 11) we derived the bound $(4 \cdot 7^{g(3d+2t)})^{m-2}$ in case $R_0 = \mathbf{Z}$ and R is integrally closed in K. If $R_0 = \mathbf{k}$ and R is integrally closed in K then it is also possible to get rid of the factor $\{m(m-1)\}^{d+t}$ but we shall not work this out here.

In the absolute case, Győry [6] (cf. also Győry [7]) proved earlier the finiteness assertions of Theorem 3 and its corollaries above under the assumption that R is integrally closed in K. Later he obtained [8], [9] effective versions of these results. In [8], certain effective analogues have been established also in the relative case.

PROOF OF COROLLARY 5. Suppose that R' has an R-basis of the form $\{1, \alpha_0, \ldots, \alpha_0^{m-1}\}$. This is clearly no restriction. In view of (9), $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is an R-basis of R' only if

$$D_{L/K}(\alpha) \in D_{L/K}(\alpha_0) R^*. \tag{16}$$

By (10), $V(\mathfrak{D}_K(R')) = V(D_{L/K}(\alpha_0))$ for all $V \in m_K \setminus T$. Now Corollary 5 follows immediately from (16) and Theorem 3 with $\beta = D_{L/K}(\alpha_0)$.

Let K, L be algebraic number fields with rings of integers $\mathcal{O}_K$, $\mathcal{O}_L$ respectively, where $K \subset L$, $[K: \mathbf{Q}]=d$ and $[L: K]=m$. Let G denote the normal closure of L over K and put $g=[G:K]$. Let $\mathfrak{D}_{L/K}$ denote the discriminant of L over K. For every $\alpha \in \mathcal{O}_L$ with $D_{L/K}(\alpha) \neq 0$ the ideal $\langle D_{L/K}(\alpha)\rangle \mathfrak{D}_{L/K}^{-1}$ is the square of an integral ideal, $\mathfrak{I}(\alpha)$ say, which is called the *index* of α with respect to L/K. Let $\mathfrak{a}$ be a fixed ideal in $\mathcal{O}_K$ and let $S=\{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ be a finite (possibly empty) set of prime ideals in $\mathcal{O}_K$. We shall now deal with the set of $\alpha \in \mathcal{O}_L$ satisfying

$$\mathfrak{I}(\alpha) = \mathfrak{a}\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_t^{k_t} \quad \text{for certain} \quad k_1, \dots, k_t \in \mathbf{Z}. \tag{17}$$

We call $\alpha_1, \alpha_2 \in \mathcal{O}_L$ weakly S-equivalent if there are $a, b, c \in \mathcal{O}_K$ with $\langle b\rangle$, $\langle c\rangle$ solely composed of prime ideals from S, such that

$$\alpha_2 = \frac{b\alpha_1 + a}{c}.$$

If α satisfies (17) then all elements of $\mathcal{O}_L$ which are S-equivalent to α also satisfy (17). Let t'' denote the number of prime ideals which divide $\mathfrak{a}$ or belong to S. Then we have

COROLLARY 6. *The numbers* $\alpha \in \mathcal{O}_L$ *which satisfy* (17) *belong to at most*

$$\{m(m-1)\}^{d+t}(4 \cdot 7^{g(3d+2t'')})^{m-2}$$

weak S*-equivalence classes.*

An effective finiteness result concerning the elements $\alpha \in \mathcal{O}_L$ satisfying (17) can be found in Győry [5].

PROOF OF COROLLARY 6. Let $T=\mathfrak{C}_K^{-1}(S)$ (cf. § 2 and the proof of Corollary 3 in § 3). Suppose that (17) is solvable. Let α_0 be a solution of (17) and put $D_{L/K}(\alpha_0)=\beta$. Then every solution $\alpha \in \mathcal{O}_L$ of (17) satisfies $D_{L/K}(\alpha) \in \beta \mathcal{O}_T^*$ and two elements $\alpha_1, \alpha_2 \in \mathcal{O}_L$ are S-equivalent if and only if they are $\mathcal{O}_T$-equivalent. Now Corollary 6 follows easily from Theorem 3.

§ 5. On special polynomials

Let $\mathbf{k}$ be a field of characteristic 0, let K be a field which is finitely generated over $\mathbf{k}$ and let G/K be a finite, normal extension. As in § 2, we suppose that $\mathbf{k}$ is algebraically closed in K. The algebraic closure of $\mathbf{k}$ in G is denoted by $\overline{K}_0$. Let R be a subring of K which has K as its quotient field (and which is now not necessarily finitely generated over $\mathbf{k}$). We extend the concept of special polynomials defined in § 3 by calling a polynomial $f(X)$ *special* in $R[X]$ if $f(X) \in R[X]$ and if

$$f(X) = \mu^r h((X+a)^{n_0}/\mu)(X+a)^{\delta}, \tag{12}$$

where r, n_0, δ are integers with $r>0$, $n_0>0$, $\delta \in \{0, 1\}$, $rn_0+\delta \geqq 3$ and $\delta=0$ if $n_0=1$, where $a \in R$, where $\mu \in K^*$ is integral over R and where $h(X)$ is a monic polynomial of degree r with coefficients in $\mathbf{k}$ and zeros in $\overline{K}_0$ such that $D(h)\neq 0$ and $h(0)\neq 0$ if $n_0>1$. If f satisfies (12) then $\deg f = rn_0+\delta \geqq 3$ and

$$D(f) = (-1)^{rn_0(n_0-1)/2} n_0^{rn_0} \mu^{r(rn_0-1+2\delta)} h(0)^{n_0-1+2\delta} D(h)^{n_0} \neq 0 \tag{18}$$

(with the convention that $h(0)^{n_0-1+2\delta}=1$ if $n_0=1$ and $h(0)=0$).

LEMMA 1. *Let $n\geqq 3$ be an integer and let $f(X)\in R[X]$ be a polynomial of degree n with zeros $\alpha_1, \dots, \alpha_n \in G$. Then the following statements are equivalent:*

(i) *f is special in $R[X]$;*

(ii) *there are $a\in R$, $\lambda\in G^*$ and $c_1, \dots, c_n \in \overline{K}_0$ such that $\alpha_i = c_i\lambda - a$ $(i=1, \dots, n)$;*

(iii) *there are integers $i, j\in\{1, \dots, n\}$ with $i\neq j$ such that for all $k\in\{1, \dots, n\}$ we have $(\alpha_i-\alpha_k)/(\alpha_i-\alpha_j)\in\overline{K}_0$.*

PROOF. (i)⇒(ii). Suppose that f satisfies (12). Let $\Theta_1, \dots, \Theta_r$ be the zeros of $h(X)$ in $\overline{K}_0$ and suppose that $\Theta_1\neq 0$. Then f can be written as

$$f(X) = \prod_{i=1}^{r} \{(X+a)^{n_0} - \Theta_i \mu\}(X+a)^{\delta}.$$

Choose $\lambda\in G^*$ such that $\lambda^{n_0} = \Theta_1\mu$. Then there are $c_1, \dots, c_n\in\overline{K}_0$ such that

$$f(X) = \prod_{i=1}^{n} (X+a-c_i\lambda).$$

This clearly proves (ii).

(ii)⇒(iii). If $\alpha_i = c_i\lambda - a$ for $i=1, \dots, n$, where $a\in R$, $\lambda\in G^*$ and $c_1, \dots, c_n\in\overline{K}_0$, then we have for all triples (i, j, k) with $1\leqq i, j, k\leqq n$ and $i\neq j$ that

$$\frac{\alpha_i-\alpha_k}{\alpha_i-\alpha_j} = \frac{c_i-c_k}{c_i-c_j} \in \overline{K}_0.$$

(iii)⇒(ii). Put $\lambda = \alpha_i - \alpha_j$. Then we have for $k, l\in\{1, \dots, n\}$

$$\frac{\alpha_k-\alpha_l}{\alpha_i-\alpha_j} = \frac{\alpha_i-\alpha_l}{\alpha_i-\alpha_j} - \frac{\alpha_i-\alpha_k}{\alpha_i-\alpha_j} \in \overline{K}_0,$$

hence

$$\alpha_k - \alpha_l = c_{kl}\lambda \tag{19}$$

for some $c_{kl}\in\overline{K}_0$. Put $a = -(\alpha_1+\dots+\alpha_n)/n$ and $c_k = (c_{k1}+\dots+c_{kn})/n$. Then $c_k\in\overline{K}_0$ and $a\in R$, in view of the facts that $f(X)\in R[X]$ and $n^{-1}\in\mathbf{k}\subset R$. Therefore, by (19), on taking the sum over all l, we have

$$\alpha_k = c_k\lambda - a \quad \text{for} \quad k = 1, \dots, n.$$

This proves (ii).

(ii)⇒(i). Let $g(X) = f(X-a) = \prod_{i=1}^{n} (X - c_i\lambda)$. Then $g(X)\in R[X]$. Let A be the set of rational integers m such that $\lambda^m = c\zeta$ for some $c\in\overline{K}_0$ and $\zeta\in K$. It is easy to show that A is an ideal in $\mathbf{Z}$. Since at least one coefficient of g is non-zero, A contains non-zero integers. Let n_0 be a positive integer which generates A. Let r, δ be integers with $n=rn_0+\delta$ and $0\leqq\delta<n_0$. Then $g(X)$ can be written as

$$g(X) = X^n+d_1X^{n-n_0}\lambda^{n_0}+\ldots+d_rX^\delta\lambda^{rn_0}, \tag{20}$$

where $d_1, \ldots, d_r\in\overline{K}_0$. Note that $D(g)=D(f)\neq 0$, whence $\delta\in\{0, 1\}$. Choose $c\in\overline{K}_0$ such that $\lambda^{n_0}=c\mu$ where $\mu\in K$. Then μ is integral over R. Put $h_i=d_ic^i$ $(i=1, \ldots, r)$, $h(X)=X^r+h_1X^{r-1}+\ldots+h_r$. Since $d_i\lambda^{in_0}=h_i\mu^i$ for $i=1, \ldots, r$ and $g(X)\in R[X]$ we have $h(X)\in\mathbf{k}[X]$. By (20) we obtain

$$g(X) = \mu^r h(X^{n_0}/\mu)X^\delta \quad (r>0,\ n_0>0,\ \delta\in\{0, 1\},\ rn_0+\delta = n). \tag{21}$$

The zeros of h obviously belong to $\overline{K}_0$. It is also clear, by our choice of r, δ, that $\delta=0$ if $n_0=1$ and $h(0)\neq 0$ if $n_0>1$. Now (i) follows immediately from (21) and $f(X)=g(X+a)$.

Let R be a finitely generated subring of K over $\mathbf{k}$ which has K as its quotient field, and let R' be an integral extension ring of R in G such that $R'\cap K=R$. In the lemma below we shall state some results about the sets of polynomials

$$\mathscr{V}_1 = \{f(X)\in\Phi(n, R, R'): f \text{ is special in } R[X] \text{ with } r\geqq 2 \text{ and } D(f)=\beta\},$$

$$\mathscr{V}_2 = \{f(X)\in\Phi(n, R, R'): f \text{ is special in } R[X] \text{ with } r\geqq 2 \text{ and } D(f)\in\beta R^*\},$$

where β is an element of $R\setminus\{0\}$ and $n\geqq 3$ is an integer.

LEMMA 2. (i) *Suppose that* $\overline{K}_0\subset R'$. *If* $\mathscr{V}_2$ *is non-empty then it contains infinitely many weak* R*-equivalence classes of polynomials.*

(ii) *Suppose that* $\mathbf{k}$ *is algebraically closed. If* $\mathscr{V}_1$ *is non-empty then it contains infinitely many* R*-equivalence classes of polynomials.*

PROOF. If $\overline{K}_0\subset R'$ (which is also the case if $\mathbf{k}$ is algebraically closed) then for every polynomial $f(X)\in\Phi(n, R, R')$ satisfying (12) we have $\mu\in R$. Indeed, there exists a $c\in\overline{K}_0^*$ such that $c\mu$ is the product of certain zeros of f. Therefore $c\mu\in R'$ and hence $\mu\in R'\cap K=R$. Let n_0, r, δ be integers with $n=rn_0+\delta$, $r>0$, $n_0>0$, $\delta\in\{0, 1\}$, $\delta=0$ if $n_0=1$. Let $\mu\in R\setminus\{0\}$. Put $h_m(X)=(X-1)(X-2)(X-6m)\times(X-8m)\ldots(X-2rm)$ if $r\geqq 3$ and $h_m(X)=(X-1)(X-m)$ if $r=2$ $(m=1, 2, \ldots)$. Let

$$\mathscr{S}=\mathscr{S}(n_0, r, \delta, \mu) = \{\mu^r h_m(X^{n_0}/\mu)X^\delta\colon m = 1, 2, \ldots\}.$$

We shall show that the polynomials in $\mathscr{S}$ are pairwise R-inequivalent. Let $f_p(X)=\mu^r h_p(X^{n_0}/\mu)X^\delta$, $f_q(X)=\mu^r h_q(X^{n_0}/\mu)X^\delta$ be polynomials in $\mathscr{S}$ which are weakly R-equivalent. Then there are $a\in R$ and $u\in R^*$ such that

$$\mu^r h_q(X^{n_0}/\mu)X^\delta = \mu^r u^n h_p\left(\left(\frac{X+a}{u}\right)^{n_0}\Big/\mu\right)\left(\frac{X+a}{u}\right)^\delta = \tag{22}$$

$$= (\mu u^{n_0})^r h_p\left(\frac{(X+a)^{n_0}}{\mu u^{n_0}}\right)(X+a)^\delta.$$

First suppose that $n_0>1$. Then the left-hand side of (22) can be written as $X^n+\gamma_1X^{n-n_0}+\ldots$, whereas the right-hand side of (22) can be written in the form

$(X+a)^n+\varrho_1(X+a)^{n-n_0}+\ldots=X^n+naX^{n-1}+\ldots$ with some γ_1, $\delta_1\in K$. Hence $a=0$. Therefore, by (22) we have

$$\mu^r h_q(X^{n_0}/\mu)X^\delta = (\mu u^{n_0})^r h_p(X^{n_0}/\mu u^{n_0})X^\delta$$

which implies that $h_q(X)=u^{n_0r}h_p(X/u^{n_0})$. Thus the zeros of $h_q(X)$ are just equal to the zeros of $h_p(X)$ multiplied by u^{n_0}. But then $u^{n_0}=1$, $p=q$. Hence $f_p(X)=f_q(X)$.

Now suppose that $n_0=1$. Then $\delta=0$ and $r=n\geqq 3$. Hence, by (22),

$$\mu^n h_q(X/\mu) = (\mu u)^n h_p\left(\frac{X+a}{\mu u}\right).$$

This in turn implies that

$$h_q(X) = u^r h_p\left(\frac{X}{u}+\frac{a}{\mu u}\right). \tag{23}$$

Let $\alpha_1, \ldots, \alpha_r$ be the zeros of $h_p(X)$. By (23) there is an $\alpha\in K$ such that $u\alpha_i+\alpha$ $(i=1, \ldots, r)$ are just the zeros of $h_q(X)$. But since $r\geqq 3$, it follows that $u=1$, $\alpha=0$. Hence $p=q$.

Suppose that $\mathcal{V}_2$ is non-empty and let $f(X)=\mu^r h((X+a)^{n_0}/\mu)X^\delta$ $(rn_0+\delta=n$ and μ, a, h are as in (12)) be an element of $\mathcal{V}_2$. Note that $\mu\in R\setminus\{0\}$. By (18), $\mu^{r(rn_0-1+2\delta)}\in\in\beta R^*$. By (18) we have also $\mathcal{S}=\mathcal{S}(n_0, r, \delta, \mu)\subseteqq\mathcal{V}_2$. But $\mathcal{S}$ contains infinitely many polynomials which are pairwise weakly R-inequivalent. This proves (i).

Suppose that $\mathcal{V}_1$ is non-empty and let $f(X)=\mu^r h((X+a)^{n_0}/\mu)X^\delta\in\mathcal{V}_2$ $(r, n_0, \delta, \mu, h$ have the same meaning as in the proof of (i)). Then (18) implies that

$$c\mu^{r(rn_0-1+2\delta)}(-1)^{rn_0(n_0-1)/2}n_0^{rn_0} = \beta, \quad \text{where} \quad c = h(0)^{n_0-1+2\delta}D(h)^{n_0}\neq 0.$$

Put

$$\alpha = \alpha(H) = \left[\frac{c}{H(0)^{n_0-1+2\delta}D(H)^{n_0}}\right]^{1/(r(rn_0+2\delta-1))}, \quad H^*(X) = \alpha^r H(X/\alpha)$$

for every monic polynomial $H(X)\in\mathbf{k}[X]$ of degree r with $D(H)\neq 0$ and $H(0)\neq 0$. Since $\mathbf{k}$ is algebraically closed, $H^*(X)$ is also a monic polynomial of degree r with coefficients in $\mathbf{k}$. Further, $H^*(0)^{n_0-1+2\delta}D(H^*)^{n_0}=c$. Hence the set

$$\mathcal{S}^* = \{\mu^r h_m^*(X^{n_0}/\mu)X^\delta\colon m = 1, 2, \ldots\}$$

is contained in $\mathcal{V}_1$. But it is easy to check that all these polynomials are pairwise R-inequivalent. This proves (ii).

REMARK. The question whether the set $\mathcal{V}_1$ contains infinitely many R-equivalence classes of polynomials in case $\mathbf{k}$ is not algebraically closed seems to be far more difficult to answer. Moreover, if (1) (resp. (2)) can only be satisfied by special polynomials with $r=1$ then it is possible that there are only finitely many (weak) R-equivalence classes of special polynomials satisfying (1) (resp. (2)).

§ 6. On units and unit equations

Let K, R_0, K_0, $\{z_1, \ldots, z_q\}$, R_1, K_1, d, m_K have the same meaning as in § 2. Let T be a finite subset of m_K of cardinality $t \geqq 0$. In this section we shall state some properties of the group $\mathcal{O}_T^* = \{\alpha \in K: V(\alpha) = 0 \text{ for all } V \in m_K \setminus T\}$.

LEMMA 3. (i) *If* $R_0 = \mathbf{Z}$ *then* $\mathcal{O}_T^* \cong W \times \mathbf{Z}^p$, *where* W *is the finite group of roots of unity in* K *and* $0 \leqq p \leqq d + t - 1$.

(ii) *If* $R_0 = \mathbf{k}$ *and* $\mathbf{k}$ *is algebraically closed in* K *then* $\mathcal{O}_T^*/\mathbf{k}^* \cong \mathbf{Z}^p$ *where* $0 \leqq p \leqq d + t - 1$.

PROOF. First of all we shall prove (ii). There exists a set of pairwise inequivalent absolute values $\{|\,.\,|_v\}_{v \in M_K}$ on K with the following properties (cf. [2], § 3.):

(24) If $\alpha \in K^*$ then $|\alpha|_v = 1$ for all but finitely many $v \in M_K$ and $\prod_{v \in M_K} |\alpha|_v = 1$.

$$M_K = I_K \cup P_K, \quad \text{where} \quad I_K \cap P_K = \emptyset, \tag{25}$$

where the valuations in the set $\{-\log |\,.\,|_v: v \in P_K\}$ are, up to equivalence, equal to the valuations in m_K and where the valuations in the set $\{-\log |\,.\,|_v: v \in I_K\}$ are, up to equivalence, equal to the extensions of the valuation V_∞ on $K_1 = \mathbf{k}(z_1, \ldots, z_q)$. Here V_∞ is defined by $V_\infty(F/G) = b - a$ for all polynomials $F, G \in R_1 \setminus \{0\}$ of total degrees a, b respectively.

$$\{\alpha \in K: |\alpha|_v = 1 \quad \text{for all} \quad v \in M_K\} = \mathbf{k}^*. \tag{26}$$

Let $S \subset M_K$ be the set containing the $v \in I_K$ and the $v \in P_K$ for which $-\log |\,.\,|_v$ is equivalent to a valuation in T. Let $S = \{v_1, v_2, \ldots, v_s\}$. Since I_K has cardinality $\leqq d$, we have $s \leqq d + t$. Let $\mathfrak{h}$ be the homomorphism from $\mathcal{O}_T^*$ to $\mathbf{R}^s$ defined by

$$\mathfrak{h}(\alpha) = (\log |\alpha|_{v_1}, \ldots, \log |\alpha|_{v_s}).$$

The elements α of $\mathcal{O}_T^*$ satisfy $|\alpha|_v = 1$ for $v \in M_K \setminus S$ and $\sum_{i=1}^{s} \log |\alpha|_{v_i} = 0$ (cf. (24)). Hence $\ker \mathfrak{h} = \mathbf{k}^*$ and the image of $\mathfrak{h}$ is a discrete group of rank $\leqq s - 1$. Thus $\mathcal{O}_T^*/\mathbf{k}^* \cong \mathbf{Z}^p$ for some integer p with $0 \leqq p \leqq d + t - 1$.

We now prove (i). Let $\mathbf{k}_0$ denote the algebraic closure of $\mathbf{Q}$ in K. Put $d_1 = [\mathbf{k}_0 : \mathbf{Q}]$, $d_2 = [K : \mathbf{k}_0(z_1, \ldots, z_q)]$. Then $d_1 d_2 = d$. Let $m_K^{(1)}$ be the set of valuations in m_K whose restriction to $\mathbf{k}_0$ is non-trivial and let $m_K^{(2)} = m_K \setminus m_K^{(1)}$. Let $T_i = T \cap m_K^{(i)}$ $(i = 1, 2)$ and let t_i denote the cardinality of T_i $(i = 1, 2)$. There exists a one-to-one correspondence between the valuations in $m_K^{(1)}$ and the prime ideals in $\mathbf{k}_0$ (cf. § 2). Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{t_1}$ be the prime ideals corresponding to the valuations in T_1. Then $\mathcal{O}_T^* \cap \mathbf{k}_0^* = \{\alpha \in \mathbf{k}_0^* : \langle \alpha \rangle = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_{t_1}^{k_{t_1}}$ for certain $k_1, \ldots, k_{t_1} \in \mathbf{Z}\}$. By Lang [10], Ch. 5, $\mathcal{O}_T^* \cap \mathbf{k}_0^* \cong W \times \mathbf{Z}^{r + t_1}$, where W is the group of roots of unity in $\mathbf{k}_0$ and r is the rank of the group of units in the ring of integers of $\mathbf{k}_0$. The valuations in $m_K^{(2)}$ lie above the valuations on $\mathbf{k}_0(z_1, \ldots, z_q)$ which correspond to irreducible polynomials of degree $\geqq 1$ in $\mathbf{k}_0[z_1, \ldots, z_q]$. Hence there exists a set of absolute values $\{|\,.\,|_v\}_{v \in M_K}$ satisfying the properties (24) to (26) with $\mathbf{k}_0$, $m_K^{(2)}$ instead of $\mathbf{k}$, m_K, respectively. Hence by (ii), $\mathcal{O}_T^*/\mathcal{O}_T^*\cap\mathbf{k}_0^*\cong\mathbf{Z}^{p_2}$ where p_2 is an integer with $0\leqq p_2\leqq d_2+t_2-1$. This is true since $\mathcal{O}_T^*/\mathcal{O}_T^*\cap\mathbf{k}_0^*\subset\mathcal{O}_{T_2}^*/\mathbf{k}_0^*$. But this shows that

$$\mathcal{O}_T^* \cong W\times\mathbf{Z}^{r+t_1+p_2} = W\times\mathbf{Z}^p$$

say, where $0\leqq p\leqq d_1+t_1-1+d_2+t_2-1\leqq d+t-1$.

Let λ, $\mu\in K^*$. We shall now deal with the equation

$$\lambda x+\mu y = 1 \quad \text{in} \quad x, y\in\mathcal{O}_T^*. \tag{27}$$

LEMMA 4. (i) *In the absolute case* (27) *has at most* $4\cdot 7^{3d+2t}$ *solutions.*
(ii) *In the relative case* (27) *has at most* $2\cdot 7^{2d+2t}$ *solutions with* $\lambda x\notin\mathbf{k}$, $\mu y\notin\mathbf{k}$.

PROOF. (i) is exactly Theorem 1 of [3]. In the proof of (ii) we shall use the set of absolute values $\{|\,.\,|_v\}_{v\in M_K}$ with properties (24) to (26). Let $S\subset M_K$ be the set of $v\in M_K$ for which either $v\in I_K$ or $v\in P_K$ and $-\log|\,.\,|_v$ is equivalent to a valuation in T. Let s denote the cardinality of S. Note that $|\alpha|_v=1$ for all $\alpha\in\mathcal{O}_T^*$ and $v\in M_K\setminus S$. By Theorem 2 of [2], (27) has at most $2\cdot 7^{2s}$ solutions with $\lambda x/\mu y\notin\mathbf{k}$. Since $s\leqq d+t$, this proves (ii).

§ 7. Preliminaries to the proofs of Theorem 1, 2, 3

Let K, R_0, K_0, $\{z_1, \dots, z_q\}$, d, m_K have the same meaning as in § 2. Let G/K be a finite, normal extension of degree g. Let $\bar{K}_0=K_0=\mathbf{Q}$ if $R_0=\mathbf{Z}$ and let $\bar{K}_0$ be the algebraic closure of K_0 in G if $R_0=\mathbf{k}$. Let R be a subring of K which has K as its quotient field and which is finitely generated over R_0. Let $R_1, \dots, R_n$ $(n\geqq 2)$ be integral extensions of R in G and let $\tilde{R}=R_1\cap R_2\cap\ldots\cap R_n\cap K$. In this section we shall deal with the set $\mathscr{C}$ of tuples $\boldsymbol{\alpha}=(\alpha_1, \dots, \alpha_n)$ with the following properties:

$$\alpha_i\in R_i \ \text{ for } \ i = 1, \dots, n;\ f(\boldsymbol{\alpha}; X) := \prod_{i=1}^{n}(X-\alpha_i)\in K[X];\ \alpha_i\neq\alpha_j \ \text{ for } \ 1\leqq i<j\leqq n.$$

We shall call the tuples $\boldsymbol{\alpha}'=(\alpha_1', \dots, \alpha_n')$, $\boldsymbol{\alpha}''=(\alpha_1'', \dots, \alpha_n'')\in\mathscr{C}$ *R-equivalent* if $\alpha_i''=\alpha_i'+a$ for some $a\in R$ $(i=1, \dots, n)$ and *weakly R-equivalent* if $\alpha_i''=u\alpha_i'+a$ for some $a\in R$, $u\in R^*$. The corresponding equivalente classes will be called R-equivalence classes and weak R-equivalence classes, respectively. In the absolute case, every $\boldsymbol{\alpha}\in\mathscr{C}$ will be called *non-special.* In the relative case, $\boldsymbol{\alpha}\in\mathscr{C}$ will be called *special* if $f(\boldsymbol{\alpha}; X)$ is special in $K[X]$ (in the general sense defined in § 5) and *non-special* otherwise. If in the relative case $\boldsymbol{\alpha}=(\alpha_1, \dots, \alpha_n)$ is non-special with $n\geqq 3$, then by Lemma 1 we may suppose that

$$\frac{\alpha_1-\alpha_i}{\alpha_1-\alpha_2}\notin\bar{K}_0 \quad \text{for some} \quad i\in\{3, \dots, n\}. \tag{28}$$

Lemmas 5 and 6 below will be used in the proofs of Theorems 1 and 3.

LEMMA 5. *Let* $U \geqq 1$ *and let* $n \geqq 2$ *be an integer. Let* $\mathscr{C}_1 \subset \mathscr{C}$ *be a set of non-special tuples* $\boldsymbol{\alpha}=(\alpha_1, \ldots, \alpha_n)$ *such that for all triples of integers* (i, j, k) *with* $1 \leqq i, j, k \leqq n$, $i \neq k$, *the set*

$$\left\{\frac{\alpha_i-\alpha_j}{\alpha_i-\alpha_k} : \boldsymbol{\alpha} \in \mathscr{C}_1, \quad \text{if} \quad R_0 = \mathbf{k} \quad \text{then} \quad \frac{\alpha_i-\alpha_j}{\alpha_i-\alpha_k} \notin \bar{K}_0\right\}$$

has cardinality at most U. Then the set of tuples

$$\left\{\left(\frac{\alpha_i-\alpha_j}{\alpha_1-\alpha_2}\right)_{1 \leqq i, j \leqq n} : \boldsymbol{\alpha} \in \mathscr{C}_1\right\}$$

has cardinality at most U^{n-2} *if* $R_0=\mathbf{Z}$ *and at most* $\max(1, 2^{n-2}-1)U^{n-2}$ *if* $R_0=\mathbf{k}$.

PROOF. Lemma 5 is obvious if $n=2$, so we shall assume that $n \geqq 3$. We notice that $\alpha_i-\alpha_j=(\alpha_1-\alpha_j)-(\alpha_1-\alpha_i)$, whence the tuple $[(\alpha_i-\alpha_j)/(\alpha_1-\alpha_2)]_{1 \leqq i, j \leqq n}$ is completely determined by the numbers $(\alpha_1-\alpha_k)/(\alpha_1-\alpha_2)$ $(k=3, \ldots, n)$. This proves Lemma 5 in the case $R_0=\mathbf{Z}$.

Now suppose that $R_0=\mathbf{k}$. Let $\mathscr{S}$ be a non-empty subset of $\{3, \ldots, n\}$ and let l denote the smallest element of $\mathscr{S}$. Let $\mathscr{C}_1(\mathscr{S})$ denote the set of tuples $(\alpha_1, \ldots, \alpha_n) \in \mathscr{C}_1$ such that $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2) \notin \bar{K}_0$ if and only if $i \in \mathscr{S}$. By (28), $\mathscr{C}_1$ is the union of all sets $\mathscr{C}_1(\mathscr{S})$, with $\mathscr{S}$ being a non-empty subset of $\{3, \ldots, n\}$. For all $\boldsymbol{\alpha}=(\alpha_1, \ldots, \alpha_n) \in \mathscr{C}_1(\mathscr{S})$ we thus have that $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2) \notin \bar{K}_0$ for $i \in \mathscr{S}$ and $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_l) \notin \bar{K}_0$ for $i \in \{3, \ldots, n\} \setminus \mathscr{S}$. Since $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)=[(\alpha_1-\alpha_i)/(\alpha_1-\alpha_l)][(\alpha_1-\alpha_l)/(\alpha_1-\alpha_2)]$, each tuple $((\alpha_i-\alpha_j)/(\alpha_1-\alpha_2))_{1 \leqq i, j \leqq n}$ is completely determined by the numbers $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)$ $(i \in \mathscr{S})$, $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_l)$ $(i \in \{3, \ldots, n\} \setminus \mathscr{S})$. This shows that the set of tuples

$$\left\{\left(\frac{\alpha_i-\alpha_j}{\alpha_1-\alpha_2}\right)_{1 \leqq i, j \leqq n} : (\alpha_1, \ldots, \alpha_n) \in \mathscr{C}_1(\mathscr{S})\right\}$$

has cardinality at most U^{n-2}. But since $\{3, \ldots, n\}$ has only $2^{n-2}-1$ non-empty subsets, this proves Lemma 5 also in the relative case.

Let $\beta \in K^*$ and let γ_{ij} $(1 \leqq i, j \leqq n)$ be elements of G. We shall consider the sets

$$\mathscr{C}_2 = \left\{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathscr{C} : \frac{\alpha_i-\alpha_j}{\alpha_1-\alpha_2} = \gamma_{ij} \quad \text{for} \quad 1 \leqq i < j \leqq n, \quad \prod_{1 \leqq i < j \leqq n} (\alpha_i-\alpha_j)^2 = \beta\right\},$$

and

$$\mathscr{C}_3 = \left\{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathscr{C} : \frac{\alpha_i-\alpha_j}{\alpha_1-\alpha_2} = \gamma_{ij} \quad \text{for} \quad 1 \leqq i < j \leqq n, \quad \prod_{1 \leqq i < j \leqq n} (\alpha_i-\alpha_j)^2 \in \beta R^*\right\}.$$

Let T be the smallest subset of m_K such that $R \subset \mathcal{O}_T$, and let t denote the cardinality of T.

LEMMA 6. *If* $\mathscr{I} := [\tilde{R}^+ : R^+] < \infty$ *then both in the absolute and the relative case* (i) $\mathscr{C}_2$ *is contained in at most* $n(n-1)\mathscr{I}$ *R-equivalence classes and* (ii) $\mathscr{C}_3$ *is contained in at most* $\{n(n-1)\}^{[K_0:K_0](d+t)} \cdot \mathscr{I}$ *weak R-equivalence classes.*

PROOF. We shall call two tuples $\boldsymbol{\alpha}'=(\alpha_1', \ldots, \alpha_n')$, $\boldsymbol{\alpha}''=(\alpha_1'', \ldots, \alpha_n'')\in\mathscr{C}$ $\tilde{R}$-e alent if $\alpha_i''=\alpha_i'+a$ for some $a\in\tilde{R}$ $(i=1, \ldots, n)$ and weakly $(R, \tilde{R})$-equivale $\alpha_i''=u\alpha_i'+a$ for some $u\in R^*$ and $a\in\tilde{R}$ $(i=1, \ldots, n)$. The corresponding equival classes will becalled $\tilde{R}$-equivalence classes and weak $(R, \tilde{R})$-equivalence cla respectively. It is easy to check that every $\tilde{R}$-equivalence class is contained in at $\mathscr{I}$ R-equivalence classes, and every weak $(T, \tilde{R})$-equivalence class is contained most $\mathscr{I}$ weak R-equivalence classes. Therefore it suffices to show the following:

(29) $\mathscr{C}_2$ is contained in at most $n(n-1)$ $\tilde{R}$-equivalence classes,

(30) $\mathscr{C}_3$ is contained in at most $\{n(n-1)\}^{[K_0:K_0](d+t)}$ weak $(R, \tilde{R})$-equivalence cla

For every $\boldsymbol{\alpha}=(\alpha_1, \ldots, \alpha_n)\in\mathscr{C}_3$, put $\psi(\boldsymbol{\alpha})=\alpha_1-\alpha_2$, $S(\boldsymbol{\alpha})=(\alpha_1+\ldots+\alpha_n)/n$. $\psi(\boldsymbol{\alpha})\in G^*$, $S(\boldsymbol{\alpha})\in K$. Further, put $\beta_0:=\beta/(\prod_{1\le i<j\le n}\gamma_{ij}^2)$. Let $\boldsymbol{\alpha}'=(\alpha_1', \ldots, \alpha_n')$ $\boldsymbol{\alpha}''=(\alpha_1'', \ldots, \alpha_n'')\in\mathscr{C}_3$. Then

$$\frac{\psi(\boldsymbol{\alpha}')}{\psi(\boldsymbol{\alpha}'')}=\frac{\alpha_i'-\alpha_j'}{\alpha_i''-\alpha_j''} \quad \text{for} \quad 1\le i<j\le n. \tag{31}$$

Hence

$$\frac{\psi(\boldsymbol{\alpha}')}{\psi(\boldsymbol{\alpha}'')}=\frac{\alpha_i'-S(\boldsymbol{\alpha}')}{\alpha_i''-S(\boldsymbol{\alpha}'')} \quad \text{for} \quad i=1, \ldots, n. \tag{32}$$

By (32), $\alpha_i'-\{\psi(\boldsymbol{\alpha}')/(\psi(\boldsymbol{\alpha}'')\}\alpha_i''$ does not depend on i. Since $\tilde{R}=R_1\cap\ldots\cap R_n\cap K$ we infer that $\psi(\boldsymbol{\alpha}')/\psi(\boldsymbol{\alpha}'')\in R^*$ if and only if $\boldsymbol{\alpha}'$, $\boldsymbol{\alpha}''$ are weakly $(R, \tilde{R})$-equivalent $\alpha_i''=u\alpha_i'+a$ for some $u\in R^*$, $a\in\tilde{R}$ with $u=\psi(\boldsymbol{\alpha}')/\psi(\boldsymbol{\alpha}'')$. Thus we have the follow equivalences

(33) $\psi(\boldsymbol{\alpha}')=\psi(\boldsymbol{\alpha}'')\Leftrightarrow\boldsymbol{\alpha}'$ and $\boldsymbol{\alpha}''$ are $\tilde{R}$-equivalent;

(34) $\psi(\boldsymbol{\alpha}')/\psi(\boldsymbol{\alpha}'')\in R^*\Leftrightarrow\boldsymbol{\alpha}'$ and $\boldsymbol{\alpha}''$ are weakly $(R, \tilde{R})$-equivalent.

(29) is an immediate consequence of (33), on noting that for every $\boldsymbol{\alpha}\in\mathscr{C}_2$ have $\psi(\boldsymbol{\alpha})^{n(n-1)}=\beta_0$, whence $\psi(\boldsymbol{\alpha})$ can assume at most $n(n-1)$ values.

In the proof of (30) we shall need some further notations. In the absolute c we put $\bar{K}=K$, $\bar{K}_1=K_1$, $\bar{R}=R$. In the relative case, choose $\zeta\in G$ such that $\bar{K}$ $=\bar{K}_0(\zeta)=\mathbf{k}(\zeta)$ and put $\bar{K}=K(\zeta)$, $\bar{K}_1=K_1(\zeta)$, $\bar{R}=R[\zeta]$. Then $\bar{R}\cap K=R$. Let Δ $=\{1\}$ if $R_0=\mathbf{Z}$ and $\Delta_0=\bar{K}_0^*$ if $R_0=\mathbf{k}$. Both in the absolute and in the relat case, let $\Gamma=\{u\in G^*: u^{n(n-1)}\in\bar{R}^*\}$ and let $\bar{T}$ be the set of valuations in $m_{\bar{K}}$ lying ab the valuations in T. Then $\bar{R}^*\subset\Gamma\subset\mathcal{O}_{\bar{T}}^*=\{\Theta\in\bar{K}: V(\Theta)=0$ for all $V\in m_{\bar{K}}\setminus\bar{T}\}$. $p=[\bar{K}_0:K_0]$. Then $[\bar{K}:K]=p$. Hence $\bar{T}$ has cardinality at most pt. Together w $[\bar{K}:\bar{K}_1]\le d$ and Lemma 3, this shows that Γ/Δ_0 is the direct product of at most $d+$ multiplicative cyclic groups, at most one of which is finite. Using also that Δ $\subset\bar{R}^*\subset\Gamma$ and $(\Gamma/\Delta_0)^{n(n-1)}\subset\bar{R}^*/\Delta_0\subset\Gamma/\Delta_0$, we obtain

$$[\Gamma: \bar{R}^*]=[\Gamma/\Delta_0: \bar{R}^*/\Delta_0]\le[\Gamma/\Delta_0: (\Gamma/\Delta_0)^{n(n-1)}]\le\{n(n-1)\}^{d+pt}. \tag{35}$$

We notice that $\bar{K}/K$ is a normal extension of degree p. Let $\sigma_1, \ldots, \sigma_p$ denote t distinct K-automorphisms of $\bar{K}$, where σ_1 is the identity. For every $\Theta\in G$, $\mathrm{Tr}(\Theta)$ $=\mathrm{Tr}_{G/\bar{K}}\setminus\bar{T}(\Theta)$ denotes the trace of Θ over $\bar{K}$ and for every $\Theta\in G^*$, $\bar{\Theta}$ denotes t coset of Θ in the factor group $G^*/\bar{R}^*$.

We define the mapping $\mathfrak{h}: \mathscr{C}_3 \to G^*/\bar{R}^* \times \{1, \ldots, n\}^p$ by

$$\mathfrak{h}(\boldsymbol{\alpha}) = (\overline{\psi(\boldsymbol{\alpha})}, i_1, \ldots, i_p),$$

where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathscr{C}_3$ and where i_j is the smallest integer $k_j \in \{1, \ldots, n\}$ such that $\sigma_j(\mathrm{Tr}(\alpha_1)) = \mathrm{Tr}(\alpha_{k_j})$ for $j = 1, \ldots, p$. (It is easily seen that such integers k_j exist). If $\boldsymbol{\tau} \in \mathscr{C}_3$ then $\overline{\psi(\boldsymbol{\tau})}^{n(n-1)} = \bar{\beta}_0$. Further, the number of cosets $\bar{\varrho} \in G^*/\bar{R}^*$ with $\bar{\varrho}^{n(n-1)} = \bar{\beta}_0$ is at most $[\Gamma: \bar{R}^*]$. Together with (35) and the fact that $i_1 = 1$ for every $\boldsymbol{\tau} \in \mathscr{C}_3$, this shows that the range of $\mathfrak{h}$ has cardinality at most

$$n^{p-1}\{n(n-1)\}^{d+pt} \leqq \{n(n-1)\}^{p(d+t)}. \tag{36}$$

We shall now show that for $\boldsymbol{\alpha}', \boldsymbol{\alpha}'' \in \mathscr{C}_3$ with $\mathfrak{h}(\boldsymbol{\alpha}') = \mathfrak{h}(\boldsymbol{\alpha}'')$ we have $\psi(\boldsymbol{\alpha}')/\psi(\boldsymbol{\alpha}'') \in R^*$. Together with (34) and (36) this proves (30). Let $\boldsymbol{\alpha}' = (\alpha_1', \ldots, \alpha_n')$, $\boldsymbol{\alpha}'' = (\alpha_1'', \ldots, \alpha_n'') \in \mathscr{C}_3$ with $\mathfrak{h}(\boldsymbol{\alpha}') = \mathfrak{h}(\boldsymbol{\alpha}'')$. Put $u = \psi(\boldsymbol{\alpha}')/\psi(\boldsymbol{\alpha}'')$. Then $u \in \bar{R}^*$. Moreover, by (32)

$$u = \frac{\mathrm{Tr}(\alpha_k') - gS(\boldsymbol{\alpha}')/p}{\mathrm{Tr}(\alpha_k'') - gS(\boldsymbol{\alpha}'')/p} \quad \text{for} \quad k = 1, \ldots, n. \tag{37}$$

Let $\sigma \in \{\sigma_1, \ldots, \sigma_p\}$ and let k denote the smallest integer in $\{1, \ldots, n\}$ such that $\sigma(\mathrm{Tr}(\alpha_1')) = \mathrm{Tr}(\alpha_k')$, $\sigma(\mathrm{Tr}(\alpha_1'')) = \mathrm{Tr}(\alpha_k'')$. Then (37) implies that $\sigma(u) = u$. From this it follows that $u \in \bar{R}^* \cap K = R^*$.

§ 8. Proofs of Theorems 1 and 2

Let K, R_0, K_0, $\{z_1, \ldots, z_q\}$, d, m_K be the same as in § 2. Let G/K be a normal extension of finite degree g. Let R be a subring of K which is finitely generated over R_0 and which has K as its quotient field and let R' be an integral extension ring of R in G such that $\mathscr{I} = [(R' \cap K)^+ : R^+] < \infty$. Let $\beta \in R \setminus \{0\}$ and let T, T' be the smallest subsets of m_K such that $R \subset \mathscr{O}_T$, $R[\beta^{-1}] \subset \mathscr{O}_{T'}$, respectively. Let t, t' denote the cardinalities of T, T', respectively. Let $\bar{T}'$ be the set of valuations in m_G lying above the valuations in T'. Let $\bar{K}_0 = K_0 = \mathbf{Q}$ if $R_0 = \mathbf{Z}$ and let $\bar{K}_0$ denote the algebraic closure of $\mathbf{k}$ in G if $R_0 = \mathbf{k}$. We shall use frequently that [6]

$$[G: \bar{K}_0(z_1, \ldots, z_q)] \leqq gd, \quad \#(\bar{T}') \leqq gt. \tag{38}$$

We shall now apply the results of § 7 with $R_1 = \ldots = R_n = R'$, where $n \geqq 2$. Define the sets

$$\mathscr{C}_4 = \{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathscr{C}: f(\boldsymbol{\alpha}; X) \in \Phi(n, R, R'),\ f(\boldsymbol{\alpha}; X) \text{ is non-special in } K[X],$$
$$D(f(\boldsymbol{\alpha}; X)) = \beta\},$$

$$\mathscr{C}_5 = \{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathscr{C}: f(\boldsymbol{\alpha}; X) \in \Phi(n, R, R'), f(\boldsymbol{\alpha}; X) \text{ is non-special in } K[X],$$
$$D(f(\boldsymbol{\alpha}; X)) \in \beta R^*\},$$

[6] For any finite set H, $\#(H)$ will denote the number of elements of H.

where $\mathscr{C}$ has the same meaning as in § 7, but with $R_1=\ldots=R_n=R'$. We note that if $\boldsymbol{\alpha}'$, $\boldsymbol{\alpha}''$ are (weakly) R-equivalent tuples in $\mathscr{C}_5$ then $f(\boldsymbol{\alpha}'; X)$, $f(\boldsymbol{\alpha}''; X)$ are (weakly) R-equivalent polynomials in $\Phi(n, R, R')$. Let N_1 denote the number of R-equivalence classes of tuples in $\mathscr{C}_4$, while N_2 denotes the number of weak R-equivalence classes of tuples in $\mathscr{C}_5$. Let $N_1(n, R, R', \beta)$, $N_2(n, R, R', \beta)$ be the same as in Theorem 1. Then

$$(39) \qquad N_1(n, R, R', \beta) \leqq \frac{N_1}{(n-2)!}, \quad N_2(n, R, R', \beta) \leqq \frac{N_2}{(n-2)!}.$$

For $n=2$ this is obvious. If $n\geqq 3$, then (39) follows immediately from the fact that for every polynomial $f(X)\in\Phi(n, R, R')$ there are at least $(n-2)!$ pairwise weakly R-inequalent $\boldsymbol{\alpha}\in\mathscr{C}$ with $f(X)=f(\boldsymbol{\alpha}; X)$. Indeed, let $\alpha_1, \ldots, \alpha_n$ be the zeros of f in R'. Let σ, τ be two distinct permutations of $(3, \ldots, n)$ and let $\boldsymbol{\alpha}'=(\alpha_1, \alpha_2, \alpha_{\sigma(3)}, \ldots, \alpha_{\sigma(n)})$, $\boldsymbol{\alpha}''=(\alpha_1, \alpha_2, \alpha_{\tau(3)}, \ldots, \alpha_{\tau(n)})$. Then the tuples $((\alpha_1-\alpha_{\sigma(i)})/(\alpha_1-\alpha_2))_{i=3,\ldots,n}$, $((\alpha_1-\alpha_{\tau(i)})/(\alpha_1-\alpha_2))_{i=3,\ldots,n}$ are distinct which easily implies that $\boldsymbol{\alpha}'$, $\boldsymbol{\alpha}''$ are not weakly R-equivalent.

In view of (39), Theorem 1 is an immediate consequence of the following proposition.

PROPOSITION 1. *We have*

$$N_1\leqq n(n-1)(4\cdot 7^{g(3d+2t')})^{n-2}\cdot\mathscr{I} \quad \textit{and} \quad N_2\leqq (n(n-1))^{[K_0:K_0](d+t)}(4\cdot 7^{g(3d+2t')})^{n-2}\cdot\mathscr{I}.$$

PROOF. Since R' is an integral extension of R, all tuples $\boldsymbol{\alpha}=(\alpha_1, \ldots, \alpha_n)\in\mathscr{C}_5$ have the property that $\alpha_i-\alpha_j\in\mathscr{O}^*_{T'}=\{\alpha\in G: V(\alpha)=0 \text{ for all } V\in m_G\setminus\overline{T}'\}$ for all $i, j\in\{1, \ldots, n\}$ with $i\neq j$. Together with (38), Lemma 4 and the relations

$$\frac{\alpha_i-\alpha_j}{\alpha_i-\alpha_k}+\frac{\alpha_j-\alpha_k}{\alpha_i-\alpha_k}=1,$$

this shows that for each triple (i, j, k) with $1\leqq i, j, k\leqq n$ and $i\neq k$, the set

$$\left\{\frac{\alpha_i-\alpha_j}{\alpha_i-\alpha_k}: (\alpha_1, \ldots, \alpha_n)\in\mathscr{C}_5, \frac{\alpha_i-\alpha_j}{\alpha_i-\alpha_k}\notin\overline{K}_0 \text{ if } R_0=\mathbf{k}\right\}$$

has cardinality most A if $R_0=\mathbf{Z}$ and at most $A/2$ if $R_0=\mathbf{k}$, where $A=4\cdot 7^{g(3d+2t')}$. But this in turn implies, together with Lemma 5, that both in the absolute and the relative case the set

$$\left\{\left(\frac{\alpha_i-\alpha_j}{\alpha_1-\alpha_2}\right)_{1\leqq i, j\leqq n}: (\alpha_1, \ldots, \alpha_n)\in\mathscr{C}_5\right\}$$

has cardinality at most A^{n-2}. Now Proposition 1 follows immediately from Lemma 6.

PROOF OF THEOREM 2. Let $f(X)\in\Phi(R, R')$ be a non-special polynomial in $R[X]$ which satisfies (2). Suppose that f has degree $n\geqq 3$ and zeros $\alpha_1, \ldots, \alpha_n\in R'$. We shall use that

$$(40) \qquad \alpha_i-\alpha_j\in\mathscr{O}^*_{T'} \quad \text{for} \quad i, j\in\{1, \ldots, n\} \quad \text{with} \quad i\neq j.$$

First of all suppose that $R_0=\mathbf{Z}$. Note that

$$\frac{\alpha_1-\alpha_i}{\alpha_1-\alpha_2}+\frac{\alpha_i-\alpha_2}{\alpha_1-\alpha_2}=1 \quad \text{for} \quad i=3, \ldots, n,$$

and that the numbers $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)$ $(i=3, \ldots, n)$ are pairwise distinct. Hence by Lemma 4, (38) and (40) we have

$$n-2 \leqq 4 \cdot 7^{g(3d+2t')}.$$

Now suppose that $R_0=\mathbf{k}$. Further, we assume that $(\alpha_1-\alpha_3)/(\alpha_1-\alpha_2)\notin \bar{K}_0$ (where $\bar{K}_0$ is the algebraic closure of $\mathbf{k}$ in G), which is by Lemma 1 no restriction. Let $\mathscr{S}$ be the subset of $\{3, \ldots, n\}$ consisting of those i for which $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_2)\notin \bar{K}_0$. By (38), (40), (41) and Lemma 4 we have

$$\#(\mathscr{S}) \leqq 2 \cdot 7^{g(3d+2t')}.$$

If $i\in\{3, \ldots, n\}\setminus\mathscr{S}$, then $(\alpha_1-\alpha_i)/(\alpha_1-\alpha_3)\notin \bar{K}_0$. Hence by (40), the identities

$$\frac{\alpha_1-\alpha_i}{\alpha_1-\alpha_3}+\frac{\alpha_i-\alpha_3}{\alpha_1-\alpha_3}=1 \quad (i\in\{3, \ldots, n\}\setminus\mathscr{S}),$$

(38) and Lemma 4, we have also

$$\#(\{3, \ldots, n\}\setminus\mathscr{S}) \leqq 2 \cdot 7^{g(3d+2t')}.$$

Together with (42) this shows that also in the relative case

$$n-2 \leqq 4 \cdot 7^{g(3d+2t')}.$$

§ 9. Proof of of Theorem 3

Suppose that K, R_0, K_0, $\{z_1, \ldots, z_q\}$, R_1, K_1, d, m_K have the same meaning as in § 2. Let L be a finite extension of K of degree $m\geqq 2$ and let G denote the normal closure of L over K. Put $g=[G\colon K]$. In the relative case we assume that $\mathbf{k}$ is algebraically closed in G. Let R be a subring of K which is finitely generated over R_0 and which has K as its quotient field. Let $R'\subset L$ be an integral extension of R having L as its quotient field and suppose that $\mathscr{I}=[(R'\cap K)^+\colon R^+]<\infty$. Let $\sigma_1, \ldots, \sigma_m$ be the K-isomorphisms of L in G. For $\alpha\in L$, put $\alpha^{(i)}=\sigma_i(\alpha)$ $(i=1, \ldots, m)$. Let $\mathfrak{D}_K(R')$ be the discriminant divisor of R' over K. Let T be the smallest subset of m_K such that $R\subset\mathcal{O}_T$ and let t denote the cardinality of T. Let $\beta\in K^*$ and let T'' be the smallest subset of m_K such that $T\subset T''$ and $V(\beta)=V(\mathfrak{D}_K(R'))$ for all $V\in m_K\setminus T''$. Let t'' be the cardinality of T''. Further, let $\bar{T}''$ be the set of valuations in m_G lying above the valuations in T''. We shall use frequently that

$$[G\colon K_1] \leqq gd, \quad \#(\bar{T}'') \leqq gt''. \tag{43}$$

If $\alpha\in L$, $\boldsymbol{\alpha}$ will denote the tuple $(\alpha^{(1)}, \ldots, \alpha^{(n)})$. We shall use the same notations as in § 7, however with $n=m$, $R_i=\sigma_i(R')$ for $i=1, \ldots, m$ and $\tilde{R}=R'\cap K$. We shall deal with the sets of tuples

$$\mathscr{C}_6=\{\boldsymbol{\alpha}\colon \alpha\in R', D_{L/K}(\alpha)=\beta\}, \quad \mathscr{C}_7=\{\boldsymbol{\alpha}\colon \alpha\in R', D_{L/K}(\alpha)\in\beta R^*\}.$$

We assert that if $\mathscr{C}_7$ is non-empty then $V(\beta)\geqq V(\mathfrak{D}_K(R'))$ for every $V\in m_K\setminus T$. Indeed, let $\alpha\in R'$ such that $\boldsymbol{\alpha}\in\mathscr{C}_7$. Since $D_{L/K}(\alpha)$ is integral over R, hence $V(\beta)=$ $=V(D_{L/K}(\alpha))\geqq 0$ for all $V\in m_K\setminus T$. Together with (7) and the definition of $\mathfrak{D}_K(R')$ this proves our assertion.

LEMMA 7. *Let $\alpha_1, \alpha_2\in R'$ such that $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2\in\mathscr{C}_7$. Then for $i\neq j$ with $1\leqq i,\ j\leqq m$*

$$\frac{\alpha_1^{(i)}-\alpha_1^{(j)}}{\alpha_2^{(i)}-\alpha_2^{(j)}}\in\mathcal{O}^*_{\overline{T}''} = \{\alpha\in G^*\colon V(\alpha)=0 \quad \textit{for all} \quad V\in m_G\setminus\overline{T}''\}.$$

PROOF. Let V be a fixed valuation in $m_G\setminus\overline{T}''$ and let $\alpha_1, \alpha_2\in R'$ such that $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2\in\mathscr{C}_7$. Then $D_{L/K}(\alpha_1)\neq 0$, hence $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a K-basis of L. We infer that there are $\xi_1, \ldots, \xi_m\in K$ such that $\alpha_2=\sum_{j=1}^m \xi_j\alpha_1^{j-1}$. For $i\in\{1, \ldots, m\}$, let $\mathbf{y}_i=$ $=(1, \alpha_1, \ldots, \alpha_1^{i-1}, \alpha_2, \alpha_1^{i+1}, \ldots, \alpha_1^{m-1})$. Then we have by (8) that

$$D(\mathbf{y}_i)=\det{}^2\begin{pmatrix}1 & & & & 0\\ & \ddots & & & \\ \xi_1 & & \xi_i & & \xi_m\\ & & & \ddots & \\ 0 & & & & 1\end{pmatrix}D_{L/K}(\alpha_1)=\xi_i^2 D_{L/K}(\alpha_1)\quad\text{for}\quad i=1, \ldots, m. \tag{44}$$

But by the definition of T'' we have $W(D_{L/K}(\alpha_1))=W(\beta)=W(\mathfrak{D}_K(R'))$ for all $W\in m_K\setminus T''$ and by the definition of $\mathfrak{D}_K(R')$ we have $W(D(\mathbf{y}_i))\geqq W(\mathfrak{D}_K(R'))$ for all $W\in m_K\setminus T''$. Together with (44) this shows that $V(\xi_i)\geqq 0$ for $i=1, \ldots, m$. But then we have, since $V(\alpha_1^{(i)})\geqq 0$ for $i=1, \ldots, m$,

$$V\left(\frac{\alpha_2^{(i)}-\alpha_2^{(j)}}{\alpha_1^{(i)}-\alpha_1^{(j)}}\right)=V\left(\sum_{k=2}^m \xi_k\frac{(\alpha_1^{(i)})^{k-1}-(\alpha_1^{(j)})^{k-1}}{\alpha_1^{(i)}-\alpha_1^{(j)}}\right)=V\left(\sum_{k=2}^m\sum_{l=0}^{k-2}\xi_k(\alpha_1^{(i)})^{k-2-l}(\alpha_1^{(j)})^l\right)\geqq 0.$$

We can show in a similar way, by interchanging α_1, α_2, that $V((\alpha_1^{(i)}-\alpha_1^{(j)})/(\alpha_2^{(i)}-\alpha_2^{(j)}))\geqq$ $\geqq 0$. Hence $V((\alpha_1^{(i)}-\alpha_1^{(j)})/(\alpha_2^{(i)}-\alpha_2^{(j)}))=0$. This proves Lemma 7.

We shall now prove Theorem 3. We remark that two numbers $\alpha_1, \alpha_2\in R'$ are (weakly) R-equivalent if and only if the tuples $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2$ are (weakly) R-equivalent. Hence in view of Lemma 6 it suffices to prove the following proposition:

PROPOSITION 2. *The set of tuples $\mathscr{V}=\left\{\left(\frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(1)}-\alpha^{(2)}}\right)_{1\leqq i,j\leqq n}\colon \boldsymbol{\alpha}\in\mathscr{C}_7\right\}$ has cardinality at most*

$$(4\cdot 7^{g(3d+2t'')})^{m-2}.$$

PROOF. For convenience we put $B=4\cdot 7^{g(3d+2t'')}$. Let $\boldsymbol{\alpha}_0$ be a fixed element of $\mathscr{C}_7$. We put $\lambda_{ij}=\alpha_0^{(i)}-\alpha_0^{(j)}$ for $1\leqq i, j\leqq m$ with $i\neq j$. Further, for every $\alpha\in R'$ we put $X_{ij}(\alpha)=(\alpha^{(i)}-\alpha^{(j)})/\lambda_{ij}$ for $1\leqq i, j\leqq m$ with $i\neq j$. Then for every $\boldsymbol{\alpha}\in\mathscr{C}_7$ we have by Lemma 7 that $X_{ij}(\alpha)\in\mathcal{O}^*_{T''}$. By Lemma 4, (43) and the relations

$$\frac{\lambda_{ij}}{\lambda_{ik}}\cdot\frac{X_{ij}(\alpha)}{X_{ik}(\alpha)}+\frac{\lambda_{jk}}{\lambda_{ik}}\cdot\frac{X_{jk}(\alpha)}{X_{ik}(\alpha)}=1\quad (i, j, k\in\{1, \ldots, m\},\ i\neq k),$$

we have that for each triple (i, j, k) with $1 \leqq i, j, k \leqq m$, $i \neq k$, the set

$$\left\{\frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(i)}-\alpha^{(k)}}\colon\ \boldsymbol{\alpha}\in\mathscr{C}_7,\ \frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(i)}-\alpha^{(k)}}\notin\mathbf{k}\quad\text{if}\quad R_0=\mathbf{k}\right\}$$

has cardinality at most B if $R_0=\mathbf{Z}$ and at most $\frac{1}{2}B$ if $R_0=\mathbf{k}$. In the absolute case, Proposition 2 is an immediate consequence of Lemma 5. In the relative case we infer that $\mathscr{V}$ contains at most $\max(1, 2^{m-2}-1)(B/2)^{m-2}$ tuples for which $\boldsymbol{\alpha}$ is non-special (i.e. $f(\boldsymbol{\alpha}; X)$ is non-special in $K[X]$). We shall now estimate the number of tuples in $\mathscr{V}$ for which $\boldsymbol{\alpha}$ is special.

Let $\boldsymbol{\alpha}\in\mathscr{C}_7$ such that $\boldsymbol{\alpha}$ is special or, which is the same, the minimal polynomial $f(X)$ of α is special in $K[X]$. Then $m\geqq 3$. Further, there are integers r, n_0, δ with $r>0$, $n_0>0$, $\delta\in\{0, 1\}$, $rn_0+\delta=m$ and $\delta=0$ if $n_0=1$, and there are $a\in K$, $\mu\in K^*$ and a monic polynomial $h(X)\in\mathbf{k}[X]$ of degree r with $D(h)\neq 0$ such that

$$f(X) = \mu^r h\big((X+a)^{n_0}/\mu\big)(X+a)^{\delta}.$$

But since f is irreducible we have that $\delta=0$ and h is irreducible. Furthermore, h has its zeros in G and $\mathbf{k}$ is algebraically closed in G. Hence $r=1$. Therefore there exists a $\mu'\in K^*$ such that

$$f(X) = (X+a)^m-\mu'.$$

Let ϱ be a fixed, primitive m-th root of unity and let Θ be a fixed m-th root of μ'. Then $\alpha^{(i)}=\varrho^{k_i}\theta-a$ for $i=1, \dots, m$, where $(k_1, \dots, k_m)$ is a permutation of $(1, \dots, m)$. Hence the tuple

$$\left(\frac{\alpha^{(i)}-\alpha^{(j)}}{\alpha^{(1)}-\alpha^{(2)}}\right)_{1\leqq i, j\leqq m} = \left(\frac{\varrho^{k_i}-\varrho^{k_j}}{\varrho^{k_1}-\varrho^{k_2}}\right)_{1\leqq i, j\leqq m}$$

belongs to a set of cardinality at most $m!$. But this shows that the number of tuples in $\mathscr{V}$ for which $\boldsymbol{\alpha}$ is special is, in view of $m\leqq g$, at most

$$m! \leqq 2\cdot 7^{3m(m-2)} \leqq (B/2)^{m-2}.$$

Therefore, the total number of tuples in $\mathscr{V}$ is also in the relative case at most B^{m-2}.

REMARK. We notice that a weaker version of Theorem 3 can be deduced also from Theorem 1.

References

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

[2] J. H. Evertse, On equations in two S-units over function fields of characteristic zero, *Acta Arith.*, **47** (1986), 233—253.

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

[4] K. Győry, *Résultats effectifs sur la représentation des entires par des formes décomposables*, Queen' s Papers in Pure and Applied Mathematics 56 (Kingston, Canada, 1980).

[5] K. Győry, On discriminants and indices of integers of an algebraic number field, *J. Reine angew. Math.*, **324** (1981), 114—126.

[6] K. Győry, On certain graphs associated with an integral domain and their applications to diophantine problems, *Publ. Math. Debrecen*, **29** (1982), 79—94.

[7] K. Győry, Polynomials of given discriminant and integral elements of given discriminant over integral domains, *C. R. Math. Rep. Acad. Sci. Canada*, **4** (1982), 75—80.

[8] 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.

[9] K. Győry, Sur les générateurs des ordres monogènes des corps de nombres algébriques, *Séminaire de Théorie des Nombres*, 1983—1984, Univ. Bordeaux, No. 32, pp. 12 (1984).

[10] S. Lang, *Algebraic Number Theory* (Addison-Wesley, 1970).

[11] S. Lang, *Diophantine Geometry*, Interscience Publ. (New York—London, 1962).

[12] O. Zariski and P. Samuel, *Commutative Algebra, Vol. I*, van Nostrand (1958).

(Received December 28, 1985)

CENTRE FOR MATHEMATICS AND COMPUTER SCIENCE
KRUISLAAN 413
P. O. BOX 4079
1009 AB AMSTERDAM
THE NETHERLANDS

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 DEBRECEN
HUNGARY