

Inhomogeneous discriminant form equations and integral elements with given discriminant over finitely generated integral domains

By I. GAÁL (Debrecen)

1. Introduction

In our previous paper [3] we gave effective upper bounds for the solutions of certain inhomogeneous discriminant form and index form equations over the ring of integers of an algebraic number field. Our results generalized some previous theorems of GYÖRY [6], [7] and GYÖRY and PAPP [21], [22] on discriminant form and index form equations. We also extended to the inhomogeneous case some results of GYÖRY [6], [8] on algebraic integers of given degree and of given discriminant or given index. Our proof was based on a theorem of GYÖRY [8] concerning the homogeneous case (i.e. algebraic integers of given degree and of given discriminant). Recently GYÖRY [19] generalized his results to the case when the ground ring is an arbitrary integral domain, finitely generated over $\mathbb{Z}$. As a consequence of these theorems GYÖRY [19] proved that there are only finitely many pairwise inequivalent S -integral algebraic numbers with given degree and given discriminant. The proof of these deep effective theorems involve among others Baker's famous method (see e.g. [1]) and a so called graph-method of GYÖRY (cf. [11], [17]). These general theorems of Györy enable us to extend the results of [3] to the above mentioned more general cases. In this paper we deal only with inhomogeneous discriminant form equations and integral elements with given discriminant, since the corresponding results concerning inhomogeneous index form equations and integral elements with given index can be easily obtained from these theorems (cf. [3]).

Our Theorem 1 gives effective bounds for the solutions of certain inhomogeneous discriminant form equations over finitely generated integral domains. An immediate consequence of this theorem is that such equations have only finitely many solutions and these can be effectively determined. This theorem extends to the inhomogeneous case a result of GYÖRY [18]. In Theorem 2 we show that if α and λ are integral elements (in a fixed field) over a finitely generated integral domain such that the discriminant of $\alpha + \lambda$ is given and λ is in a certain sense "small" compared to α , then α is equivalent to an element of an effectively determinable finite set. This theorem generalizes the corresponding "homogeneous" result of GYÖRY [19]. The statement of Theorem 3 and Theorem 4 corresponds to that special case of Theorem 1 and Theorem 2, respectively, when the ground ring is the ring of S -integers of an algebraic number field. The method of our proofs will be similar to that of [3].

2. Notation concerning finitely generated integral domains

We follow the notation of GYÖRÝ [19] (see also GYÖRÝ [18]). We also give a relative formulation of our results (cf. [19] or [18]).

Let us denote by K_0 the ring $\mathbf{Z}$ of rational integers (absolute case) or a field of characteristic 0 (relative case). Denote by K'_0 the quotient field of K_0 (i.e. $K'_0 = \mathbf{Q}$ in the absolute case and $K'_0 = K_0$ in the relative case). Let R be a finitely generated integral domain over K_0 , that is

$$(1) \quad R = K_0[x_1, \dots, x_q, y_1, \dots, y_t]$$

where $\{x_1, \dots, x_q\}$ is a maximal algebraically independent subset of the set of generators of R and $y_1, \dots, y_t$ are algebraic over $K'_0(x_1, \dots, x_q)$. We shall suppose that R is integrally closed. Let a be an element of the polynomial ring $K_0[x_1, \dots, x_q]$ such that ay_i is integral over $K_0[x_1, \dots, x_q]$, $i=1, \dots, t$. Denote by K the quotient field of R . Then we have

$$(2) \quad K = K'_0(x_1, \dots, x_q, y_0)$$

where $\{x_1, \dots, x_q\}$ is a transcendence basis of K over K'_0 and y_0 is integral over the polynomial ring $K_0[x_1, \dots, x_q]$. Such a set $\{x_1, \dots, x_q, y_0\}$ of generators is called a generating set over K'_0 (cf. [19] or [18]).

Let L and G be finite extension fields of K , such that $L \subseteq G$. Denote by n the degree of L over K . Let z_0 be a primitive element of L over K that is

$$(3) \quad L = K(z_0).$$

Further, we may suppose without loss of generality that G is normal over $K'_0(x_1, \dots, x_q)$. Let

$$(4) \quad G = K'_0(x_1, \dots, x_q, y)$$

where y is integral over $K_0[x_1, \dots, x_q]$. Let $g = [G : K'_0(x_1, \dots, x_q)]$, let $F(X) = X^g + F_1X^{g-1} + \dots + F_g$ be the minimal polynomial of y over $K'_0(x_1, \dots, x_q)$ and denote by D_F the discriminant of $F(X)$. Since $K_0[x_1, \dots, x_q]$ is integrally closed, hence $D_F, F_1, \dots, F_g$ belong to $K_0[x_1, \dots, x_q]$.

We shall denote by capitalized $\text{Deg}(P)$ the total degree in $x_1, \dots, x_q$ of an element P (as a polynomial in $x_1, \dots, x_q$) in $K_0[x_1, \dots, x_q]$. In the absolute case $L(P)$ denotes the length of $P \in \mathbf{Z}[x_1, \dots, x_q]$, i.e. the sum of absolute values of the coefficients of P (as a polynomial).

Assume that $\max_i \text{Deg}(F_i) \leq F$ and, in the absolute case $\max_i L(F_i) \leq \mathcal{F}$ ($\mathcal{F} \geq 2$). In the absolute case $r(\geq 0)$ will denote the number of distinct rational prime factors of aD_F and P the greatest of these prime factors (if $r=0$, let $P=1$ and $\log P=1$). Further, denote by $\mathcal{P}$ the maximum length of the non-constant irreducible factors of aD_F in $\mathbf{Z}[x_1, \dots, x_q]$ (if $aD_F \in \mathbf{Z}$, let $\mathcal{P}=2$).

Any element $x \in G$ can be uniquely represented (up to unit factors of K_0) in the form

$$(5) \quad \alpha = \frac{P_0 + P_1y + \dots + P_{g-1}y^{g-1}}{Q}$$

where $P_0, \dots, P_{g-1}, Q$ are relatively prime polynomials in $K_0[x_1, \dots, x_g]$. Let us define the Degree of α (with respect to the generating set $\{x_1, \dots, x_g, y\}$ of G over K'_0) by

$$\text{Deg}(\alpha) = \max \{ \text{Deg}(P_0), \dots, \text{Deg}(P_{g-1}), \text{Deg}(Q) \}.$$

For any $\alpha_1, \dots, \alpha_m \in G$ we have (see [19])

$$(6) \quad \text{Deg}(\alpha_1 + \dots + \alpha_m) \leq \text{Deg}(\alpha_1) + \dots + \text{Deg}(\alpha_m)$$

and

$$(7) \quad \text{Deg}(\alpha_1 \dots \alpha_m) \leq \text{Deg}(\alpha_1) + \dots + \text{Deg}(\alpha_m) + (m-1)(g-1)F.$$

Let us denote by $y = y^{(1)}, \dots, y^{(g)}$ the roots of $F(X)$ in G and let $\alpha = \alpha^{(1)}, \dots, \alpha^{(g)}$ be the conjugates of any $\alpha \in G$, corresponding to the conjugates $y^{(1)}, \dots, y^{(g)}$ of y . By Lemma 6 of GYÖRY [19] we obtain

$$(8) \quad \max_i \text{Deg}(\alpha^{(i)}) \leq g \text{Deg}(\alpha) + g_1 F$$

where g_1 (and in the following $g_2, g_3, \dots$) denotes effectively computable positive constants depending only on g . Further (7), (8) and the definition of $\text{Deg}(\alpha)$ implies that for any $\alpha, \beta \in G, \beta \neq 0$ we have

$$(9) \quad \text{Deg}\left(\frac{\alpha}{\beta}\right) \leq \text{Deg}(\alpha) + g^2 \text{Deg}(\beta) + g_2 F.$$

In the absolute case, the size of any non-zero¹⁾ $\alpha \in G$ (with respect to the generating set $\{x_1, \dots, x_g, y\}$ of G) is defined by

$$s(\alpha) = \max \{ s(P_0), \dots, s(P_{g-1}), s(Q) \}$$

where $P_0, \dots, P_{g-1}, Q \in \mathbb{Z}[x_1, \dots, x_g]$ are the polynomials appearing in the representation (5) of α and

$$s(P) = \max \{ \log H(P), 1 + \max_i \deg_{x_i} P \}$$

denotes the size of a polynomial $P \in \mathbb{Z}[x_1, \dots, x_g]$. ($H(P)$ denotes the height of P , that is the maximum absolute value of its coefficients.) Since there are only finitely many elements in G with bounded size, in this general situation this concept may be used instead of the usual size of algebraic numbers. For any non-zero $\alpha_1, \dots, \alpha_m \in G$ we have (see [19])

$$(10) \quad s(\alpha_1 + \dots + \alpha_m) \leq c_1(s(\alpha_1) + \dots + s(\alpha_m)) + c_2$$

and

$$(11) \quad s(\alpha_1 \dots \alpha_m) \leq c_1(s(\alpha_1) + \dots + s(\alpha_m)) + c_2$$

where $c_1 = (g+1)^2$ and $c_2 = 2g^2m(g+1)^2 \max \{ \log \mathcal{F}, 1+F \}$. By Lemma 6 of GYÖRY [19], we get for any $0 \neq \alpha \in G$

$$(12) \quad \max_i s(\alpha^{(i)}) \leq (g+1)^3 [gs(\alpha) + g_3 c_3]$$

¹⁾ For $\alpha=0$ we may put $\text{Deg}(\alpha)=0$ and $s(\alpha)=0$.

with $c_3 = (g!g^2F)^{2q+1} + \log \mathcal{F}$. Further, (11), (12), (2.10) of [19] and the definition of $s(\alpha)$ imply that for any non-zero $\alpha, \beta \in G$ we have

$$(13) \quad s\left(\frac{\alpha}{\beta}\right) \leq (q+1)^3 s(\alpha) + (q+1)^6 g^2 s(\beta) + (q+1)^6 g_4 c_3.$$

In our main result (Theorem 1) we shall give effective upper bounds for the Degrees, and in the absolute case, for the sizes of the solutions of inhomogeneous discriminant form equations. In the absolute case our estimates imply the finiteness of the number of solutions. The parameters involved depend on the generating set $\{x_1, \dots, x_q, y\}$ of G and on $y_1, \dots, y_t$. Some important remarks on the effectiveness of the results of this type can be found in GYÖRÝ [19] (see also [18] or [20]). We recall only that our results will be effective only if R, K, L and G are given in the form (1), (2), (3) and (4) respectively, in the absolute case g and the coefficients $F_1, \dots, F_g \in \mathbb{Z}[x_1, \dots, x_q]$ of $F(X)$ are given, and $y_1, \dots, y_t, y_0$ and z_0 are given in the form (5); in the relative case upper bounds are given for g and for the Degrees of $F_1, \dots, F_g, y_1, \dots, y_t, y_0$ and z_0 .

3. Inhomogeneous discriminant form equations over finitely generated integral domains

Using the notation of paragraph 2, suppose that $[L:K] = n \geq 2$. Let us denote by R_L the ring of those elements of L which are integral over R . Let $\alpha_0 = 1, \alpha_1, \dots, \alpha_k$ be elements in R_L , linearly independent over K such that $L = K(\alpha_1, \dots, \alpha_k)$. Assume that $\max_i \text{Deg}(\alpha_i) \leq A$ and in the absolute case $\max_i s(\alpha_i) \leq \mathcal{A}$. Further let D_0 be a non-zero element in G with Degree $\leq D$ and in the absolute case with size $\leq \mathcal{D}$. Under the above conditions consider the discriminant form equation

$$(14) \quad D_{L/K}(\alpha_1 x_1 + \dots + \alpha_k x_k) = D_0$$

with variables $x_1, \dots, x_k \in R$. GYÖRÝ [17] proved in an ineffective form that equation (14) has only finitely many solutions. Further, GYÖRÝ [18] gave bounds for the Degrees and in the absolute case for the sizes²⁾ of all solutions of (14). This theorem includes all previous effective results on discriminant form equations.

As an inhomogeneous generalization of equation (14) let us consider equation

$$(15) \quad D_{L/K}(\alpha_1 x_1 + \dots + \alpha_k x_k + \lambda) = D_0$$

where the variables are $x_1, \dots, x_k \in R$ and $\lambda \in R_L$. Here $x_1, \dots, x_k$ are called dominating variables and λ is a non-dominating variable, which is supposed to be in a

²⁾ In [18] Györy used the length $L(\alpha)$ instead of $s(\alpha)$ for $\alpha \in G$. If α is represented in the form (5) then $L(\alpha) = \max \{L(P_0), \dots, L(P_{g-1}), L(Q)\}$ where $L(P)$ denotes the length of $P \in \mathbb{Z}[x_1, \dots, x_q]$. As is remarked in footnote 1 of [19], $L(\alpha) \leq \exp \{(q+1)s(\alpha)\}$ and

$$\exp \{s(\alpha)\} \leq \max \{L(\alpha), \exp(1 + \text{Deg}(\alpha))\}.$$

certain sense "small" compared to the dominating variables. For the formulation of our Theorem 1 let

$$C_1 = 21400(g^2 g!)^2(F + D + \text{Deg}(a) + 1)$$

and

$$C_2 = n[g_5(r+1)^{2g!+11}(((2qg+1)C_1)^{q((qg+1)C_1)^q} \mathcal{F})^{qg!} \log P]^{rg!+10} P^{g!} (\mathcal{D} + n^4 \log \mathcal{P}).$$

Our main result is as follows:

Theorem 1. Suppose that $x_1, \dots, x_k \in R$ and $\lambda \in R_L$ are solutions of equation (15). If $\text{Deg}(\lambda) < \varepsilon_1 \max_i \text{Deg}(x_i)$ then

$$(16) \quad \max_i \text{Deg}(x_i) < 2k!qC_1 + 8kk!g^3A + g_6F.$$

Further, in the absolute case, if $s(\lambda) < \varepsilon_2 \max_i s(x_i)$ then

$$(17) \quad \max_i s(x_i) < 2k!(q+1)^9C_2 + 8kk!g^3(q+1)^{15}\mathcal{A} + (q+1)^{15}g_7c_3$$

where $\varepsilon_1 = (4gk!)^{-1}$ and $\varepsilon_2 = (4gk!(q+1)^{12})^{-1}$.

Our theorem implies that in the absolute case equation (15) has only finitely many solutions and these can be effectively determined. We remark that in general it is possible to decide, whether or not, an $\alpha \in G$ is in R , only if the elements of R can be represented in a well utilizable form (cf. [19], [18] or [20]).

In the special case $\lambda=0$ our Theorem 1 includes Theorem 5 of GYÖRY [18] (with different estimate). Further, our theorem implies the ineffective Corollary 3.3 of GYÖRY [17].

4. Integral elements of given discriminant over finitely generated integral domains

In this paragraph we use the notation of paragraphs 2 and 3.

The elements $\alpha, \alpha^* \in R_L$ are called R -equivalent, if $\alpha - \alpha^* \in R$. In this case $D_{L/K}(\alpha) = D_{L/K}(\alpha^*)$. In [17] Györy proved that in the absolute case there are only finitely many pairwise inequivalent elements in R_L with given discriminant. Further, GYÖRY [19] showed that such a system of pairwise inequivalent elements in R_L can be effectively determined. Now we extend these results to the inhomogeneous case. We prove in an effective form that there are only finitely many pairwise R -inequivalent $\alpha \in R_L$ such that the discriminant of $\alpha + \lambda$ is given with some $\lambda \in R_L$ which is in a certain sense "small" compared to α .

Let D_0 be as in Theorem 1 and let $[L:K] = n \geq 2$.

Theorem 2. Suppose³⁾ $\frac{1}{n} \in R$. Let $\alpha, \lambda \in R_L$ with

$$(18) \quad D_{L/K}(\alpha + \lambda) = D_0.$$

³⁾ This condition automatically holds in the relative case.

If $\text{Deg}(\lambda) < \varepsilon_3 \text{Deg}, \text{Deg}(D_{K(\alpha)/K}(\alpha))$ then α is R -equivalent to an element $\alpha^* \in R_L$ satisfying

$$(19) \quad \text{Deg}(\alpha^*) < 2nqC_1 + g_8F.$$

Further, in the absolute case, if $s(\lambda) < \varepsilon_4, s(D_{K(\alpha)/K}(\alpha))$ then for the above α^* we have

$$(20) \quad s(\alpha^*) < 3n(q+1)^4C_2 + (q+1)^2g_9c_3$$

where $\varepsilon_3 = (4gn^2)^{-1}$ and $\varepsilon_4 = (4gn^2(q+1)^7)^{-1}$.

In the special case $\lambda=0$ our Theorem 2 includes Theorem 10 of GYÖRY [19] (with another estimate). Further, Theorem 2 implies Corollary 5.1 of GYÖRY [17].

5. S -integral solutions of inhomogeneous discriminant form equations over number fields

Let $K \subset L$ be algebraic number fields with $[L:K] = n \geq 2$. Let $\alpha_0 = 1, \alpha_1, \dots, \alpha_k$ be algebraic integers in L , linearly independent over K , such that $L = K(\alpha_1, \dots, \alpha_k)$. Denote by δ a non-zero integer in K . Let us consider the discriminant form equation

$$(21) \quad D_{L/K}(\alpha_1x_1 + \dots + \alpha_kx_k) = \delta$$

with variables⁴⁾ $x_1, \dots, x_k \in \mathbf{Z}_K$. Effective bounds for all solutions of equation (21) were given by GYÖRY [6], [7], [13] and GYÖRY and PAPP [21], [22]. These theorems were extended to the so called p -adic case by GYÖRY and PAPP [21] and GYÖRY [10], [12], [14]. Further, GYÖRY [15] obtained effective bounds also for the S -integral solutions of equation (21). We remark that the general theorems of GYÖRY [18], [20] concerning equation (14) include the above mentioned results as a special case.

In our previous paper [3] we considered inhomogeneous discriminant form equations of type

$$(22) \quad D_{L/K}(\alpha_1x_1 + \dots + \alpha_kx_k + \lambda) = \delta$$

where $x_1, \dots, x_k \in \mathbf{Z}_K$ are dominating variables and $\lambda \in \mathbf{Z}_L$ is a non-dominating variable, such that⁵⁾ $|\lambda| < \varepsilon_5 \cdot \max_i |x_i|$ with a given small positive constant ε_5 .

Under this assumption we gave effective bounds for the sizes of all solutions of equation (22). Our result generalized some earlier theorems of GYÖRY [6], [7], [13] and GYÖRY and PAPP [21], [22] concerning equation (21).

Our purpose is to deduce effective bounds for the heights of all solutions of equation (22) in the more general case when the variables $x_1, \dots, x_k, \lambda$ are S -integral numbers. To formulate our result we need some further notation.

Let G be the smallest normal extension of $\mathbf{Q}$, containing L . Denote by g the degree of G over $\mathbf{Q}$ and let y be a primitive integral element of G over $\mathbf{Q}$ with height⁶⁾

⁴⁾ $\mathbf{Z}_K$ denotes the ring of integers of an algebraic number field K .

⁵⁾ $|\alpha|$ denotes the size of an algebraic number α , that is the maximum of the absolute values of its conjugates.

⁶⁾ The height $H(\alpha)$ of an algebraic number α is the maximum absolute value of the coefficients of the minimal defining polynomial of α over $\mathbf{Z}$.

not exceeding $\mathcal{H}$. Let q be the number of distinct prime factors of the discriminant of y over $\mathbf{Q}$, and let Q be the maximum of these primes.

Denote by D_K , R_K and h_K the discriminant, regulator and class number of K , respectively. Let S be a finite set of (additive) valuations⁷⁾ of K . Denote by r (≥ 0) the number of the rational primes corresponding to the valuations induced on $\mathbf{Q}$ by the elements of S , and let P denote the maximum of these primes. (In the case $r=0$ put $P=1$ and $\log P=1$.) Denote by O_S the ring of S -integers⁸⁾ of K . In the case $S=\emptyset$, O_S coincides with $\mathbf{Z}_K$.

Let us denote by $O_{S,L}$ the ring of those elements of L which are integral over O_S . We suppose that in equation (22) $\alpha_1, \dots, \alpha_k \in O_{S,L}$ with $\max_i H(\alpha_i) \leq A$ ($A > 2$), such that $\alpha_0=1, \alpha_1, \dots, \alpha_k$ are linearly independent over K and $L=K(\alpha_1, \dots, \alpha_k)$ and that $\delta \in O_S$ with height d_0 ($d_0 \geq 2$). Finally, let⁹⁾

$$C_3 = \exp \{ g_{10} n^{10} \max(R_K, h_K) [g_{11} (r+q+1)^{2g+11} H^{gg+1} \log(P+Q)]^{(r+q)g+12} \cdot (P+Q)^{g+1} (\log(d_0 |D_K|)) \}.$$

Under the above conditions we have the following theorem:

Theorem 3. *If $x_1, \dots, x_k \in O_S$ and $\lambda \in O_{S,L}$ are solutions of equation (22) and $H(\lambda) < (\max_i H(x_i))^{e_6}$ then*

$$(23) \quad \max_i H(x_i) < \exp [64k! g^4 (\log C_3 + 6k \log A)] = C_4,$$

where $e_6 = (64k! g^4)^{-1}$.

In the special case $\lambda=0$ our Theorem 3 gives effective bounds for the S -integral solutions of equation (21), that is, Theorem 3 includes Corollary 4.1 of GYÖRY [15] (with different estimate).

In the special case $S=\emptyset$ Theorem 3 implies the following corollary:

Corollary 3.1. *If $x_1, \dots, x_k \in \mathbf{Z}_K$ and $\lambda \in \mathbf{Z}_L$ are solutions of equation (21) and $|\lambda| < \frac{1}{4} (\max_i |x_i|)^{e_7}$ then*

$$(24) \quad \max_i |x_i| < 2C_4$$

where $e_7 = e_6 g^{-1}$.

In the special case $\lambda=0$ Corollary 3.1 implies e.g. Theorem 4 of GYÖRY and PAPP [22] and Theorem 2 of GYÖRY and PAPP [21] (with another bound).

In the above corollary the assumption concerning λ is stronger than the condition $|\lambda| < e_5 \max_i |x_i|$ hence it gives a weaker result than Theorem 1 of [3].

We remark that in the case of homogeneous equations as (21) there is a close connection between the S -integral solutions and the solutions of the corresponding

⁷⁾ For valuations we use the terminology of Borevich and Shafarevich [2].

⁸⁾ $\alpha \in K$ is said to be an S -integer if $v(\alpha) \geq 0$ for all valuations $v \notin S$.

⁹⁾ As in the previous paragraphs, $g_{10}, g_{11}, \dots$ denote effectively computable positive constants, depending only on g .

p -adic equation. In the inhomogeneous case there is not such connection because the restricting conditions concerning λ do not remain valid for the non-dominating variable of the corresponding p -adic equation. This is the reason why we cannot deduce, as a consequence of Theorem 3, effective bounds for the solutions of p -adic inhomogeneous discriminant form equations.

6. S -integral algebraic numbers with given discriminant

In this paragraph we use the notation of paragraph 5. Two numbers, α and α^* in $\mathcal{O}_{S,L}$ are called $\mathcal{O}_S$ -equivalent, if $\alpha - \alpha^* \in \mathcal{O}_S$. In this case $D_{L/K}(\alpha) = D_{L/K}(\alpha^*)$.

In the case $S = \emptyset$, in a series of papers GYÖRÝ [4], [5], [6], [7], [8] obtained effective finiteness theorems concerning polynomials with algebraic integer coefficients and given discriminant. As a consequence of these results he proved that there are only finitely many pairwise inequivalent algebraic integers with given degree and given discriminant, and such a system can be effectively determined. GYÖRÝ [9], [16] extended these results also to the p -adic case, and to the case of an arbitrary finite valuation set S (see [19]). The general theorems of [19], mentioned in paragraph 4, include all the above quoted results.

In the case $S = \emptyset$, in [3] we gave an inhomogeneous version of a theorem of GYÖRÝ [8] concerning algebraic integers of given degree and given discriminant. Now we formulate a similar result for an arbitrary finite valuation set S :

Theorem 4. *Let $\alpha, \lambda \in \mathcal{O}_{S,L}$. If*

$$(25) \quad D_{L/K}(\alpha + \lambda) = \delta$$

and $H(\lambda) < [H(D_{K(\alpha)/K}(\alpha))]^{\varepsilon_8}$ then α is $\mathcal{O}_S$ -equivalent to an $\alpha^ \in \mathcal{O}_{S,L}$ with height*

$$(26) \quad H(\alpha^*) < \exp(5g \log C_3),$$

where $\varepsilon_8 = (16g^2n^2)^{-1}$.

In the special case $\lambda = 0$ our theorem gives Theorem 15 of GYÖRÝ [19] (with another estimate). Further, in the special case $S = \emptyset$ Theorem 4 implies a result similar to Theorem 3 of [3], but only with a stronger condition concerning λ .

7. Proofs

The proofs of Theorem 1 and Theorem 2 are based on the following results of GYÖRÝ [19] (see Theorem 1 and Theorem 10 of GYÖRÝ [19]). We use the notation of our Theorem 1. Let $\alpha = \alpha^{(1)}, \dots, \alpha^{(g)}$ denote the conjugates of any non-zero $\alpha \in G$ over $K'_0(x_1, \dots, x_q)$ (i.e. the images of α under the distinct $K'_0(x_1, \dots, x_q)$ -automorphisms of G).

Theorem A. *Let $\alpha \in R_L$ with $D_{L/K}(\alpha) = D_0$. Then*

$$(27) \quad \max_{i,j} \text{Deg}(\alpha^{(i)} - \alpha^{(j)}) \leq qC_1$$

and in the absolute case

$$(28) \quad \max_{i,j} s(\alpha^{(i)} - \alpha^{(j)}) \leq C_2.$$

Further, if $\frac{1}{n} \in R$ then α is R -equivalent to an element $\alpha^* \in R_L$ satisfying

$$(29) \quad \text{Deg}(\alpha^*) \leq nqC_1$$

and in the absolute case

$$(30) \quad s(\alpha^*) \leq 2n(q+1)^2C_2$$

with the constants C_1, C_2 occurring in Theorem 1.

In our proofs of Theorem 1 and Theorem 2 we combine this deep effective result with the method used in [3] and we utilize the inequalities (6)–(9) and (10)–(13).

PROOF OF THEOREM 1. Let $x_1, \dots, x_k \in R$ and $\lambda \in R_L$ be a solution of equation (15), such that $\text{Deg}(\lambda) < \varepsilon_1 X_D$ and in the absolute case $s(\lambda) < \varepsilon_2 X_s$ where $X_D = \max_i \text{Deg}(x_i)$ and $X_s = \max_i s(x_i)$. Put $l(\underline{x}) = \alpha_1 x_1 + \dots + \alpha_k x_k$, $\varrho = l(\underline{x}) + \lambda$ and denote by $\gamma^{(1)}, \dots, \gamma^{(n)}$ the conjugates of any $\gamma \in L$ over K (i.e. the images of γ under the distinct K -isomorphisms of L in G). Further, let $l_{ij}(\underline{x}) = l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$, $\lambda_{ij} = \lambda^{(i)} - \lambda^{(j)}$ and $\varrho_{ij} = \varrho^{(i)} - \varrho^{(j)}$ for any $i \neq j$, $1 \leq i, j \leq n$. Applying Theorem A to equation (15), by 27) we get

$$\max_{1 \leq i, j \leq n} \text{Deg}(\varrho_{ij}) \leq qC_1$$

and in the absolute case, by (28),

$$\max_{1 \leq i, j \leq n} s(\varrho_{ij}) \leq C_2.$$

These inequalities imply

$$(31) \quad \max_{1 \leq i, j \leq n} \text{Deg}(\varrho_{ij} - \lambda_{ij}) \leq qC_1 + 2g \text{Deg}(\lambda) + g_{12}F$$

and in the absolute case

$$(32) \quad \max_{1 \leq i, j \leq n} s(\varrho_{ij} - \lambda_{ij}) \leq (q+1)^2 C_2 + 2g(q+1)^5 s(\lambda) + g_{13}(q+1)^5 c_3.$$

By our assumptions $\alpha_0 = 1, \alpha_1, \dots, \alpha_k$ are linearly independent over K , hence the equation system

$$l_{ij}(\underline{x}) = \varrho_{ij} - \lambda_{ij} \quad (1 \leq i, j \leq n)$$

has a unique solution $x_1, \dots, x_k$. Solving this equation system by Cramer's rule, we get

$$x_i = \frac{v_i}{v}, \quad i = 1, \dots, k$$

where v_i ($i = 1, \dots, k$) and v denote the corresponding determinants. Using (31) we obtain

$$\max_i \text{Deg}(v_i) \leq k!qC_1 + 2gk! \text{Deg}(\lambda) + 2kk!gA + g_{14}F$$

and

$$\text{Deg}(v) \leq 2kk!gA + g_{15}F,$$

that is

$$(33) \quad X_D = \max_i \text{Deg}(x_i) \leq k!qC_1 + 2gk! \text{Deg}(\lambda) + 4kk!g^3A + g_{16}F.$$

Since by our condition concerning λ we have $2gk! \text{Deg}(\lambda) < \frac{1}{2} X_D$, hence (16) follows from (33). Similarly, in the absolute case, by (32) we obtain

$$\max_i s(v_i) \leq k!(q+1)^6 C_2 + 2gk!(q+1)^9 s(\lambda) + 2kk!(q+1)^9 g\mathcal{A} + (q+1)^9 g_{17} c_3$$

and

$$s(v) \leq 2kk!g(q+1)^9 \mathcal{A} + (q+1)^9 g_{18} c_3,$$

whence

$$(34) \quad X_s = \max_i s(x_i) \leq \\ \leq k!(q+1)^9 C_2 + 2gk!(q+1)^{12} s(\lambda) + 4kk!g^3(q+1)^{15} \mathcal{A} + (q+1)^{15} g_{19} c_3.$$

By our assumption on λ we have $2gk!(q+1)^{12} s(\lambda) < \frac{1}{2} X_s$, and thus (34) implies (17).

PROOF OF THEOREM 2. Let us denote the conjugates of any $\gamma \in L$ over K as in the proof Theorem 1. Put $\alpha_{ij} = \alpha^{(i)} - \alpha^{(j)}$, $\lambda_{ij} = \lambda^{(i)} - \lambda^{(j)}$ and $\varrho_{ij} = \alpha_{ij} + \lambda_{ij}$ for any $i \neq j$, $1 \leq i, j \leq n$. Applying Theorem A to (18), by (27) we have

$$(35) \quad \max_{1 \leq i, j \leq n} \text{Deg}(\varrho_{ij}) \leq qC_1$$

and in the absolute case, by (28), we get

$$(36) \quad \max_{1 \leq i, j \leq n} s(\varrho_{ij}) \leq C_2.$$

Let us choose the indices i, j so that

$$\text{Deg}(\alpha_{ij}) = \max_{1 \leq i', j' \leq n} \text{Deg}(\alpha_{i'j'})$$

and similarly, in the absolute case let

$$s(\alpha_{ij}) = \max_{1 \leq i', j' \leq n} s(\alpha_{i'j'}).$$

Since $\alpha \in R_L$, hence $[K(\alpha):K] \leq [L:K] = n$ and thus our assumption concerning λ implies

$$(37) \quad \text{Deg}(\lambda) \leq \varepsilon_3 [n^2 \text{Deg}(\alpha_{ij}) + n^2(g-1)F]$$

and in the absolute case

$$(38) \quad s(\lambda) \leq \varepsilon_4 [(q+1)^2 n^2 s(\alpha_{ij}) + 2g^2 n^2 (q+1)^2 \max \{\log \mathcal{F}, 1+F\}].$$

Using (35) and (37) we obtain

$$\begin{aligned} \text{Deg}(\alpha_{ij}) &= \text{Deg}(\varrho_{ij} - \lambda_{ij}) \leq qC_1 + 2g \text{Deg}(\lambda) + g_{20} F \leq \\ &\leq qC_1 + 2gn^2 \varepsilon_3 \text{Deg}(\alpha_{ij}) + g_{21} F. \end{aligned}$$

By the definition of ε_3 we have $2gn^2 \varepsilon_3 = \frac{1}{2}$ and thus we get a bound for $\text{Deg}(\alpha_{ij})$.

Writing this bound in place of $\text{Deg}(\alpha_{ij})$ in (37), we have

$$(39) \quad \text{Deg}(\lambda) \leq qC_1 + g_{22} F.$$

In the absolute case let us use (36) and (38) to get

$$\begin{aligned} s(\alpha_{ij}) = s(\varrho_{ij} - \lambda_{ij}) &\leq (q+1)^2 C_2 + 2g(q+1)^5 s(\lambda) + (q+1)^5 g_{23} c_3 \leq \\ &\leq (q+1)^2 C_2 + 2gn^2(q+1)^7 \varepsilon_4 s(\alpha_{ij}) + (q+1)^5 g_{24} c_3, \end{aligned}$$

which, by the definition of ε_4 , implies a bound for $s(\alpha_{ij})$. Thus, again by (38), we obtain

$$(40) \quad s(\lambda) < C_2 + g_{25} c_3.$$

Applying the second part of Theorem A to (18) we get

$$\alpha + \lambda = \alpha' + a$$

where $\alpha' \in R_L$ and $a \in R$. By (29)

$$(41) \quad \text{Deg}(\alpha') \leq nqC_1$$

and, in the absolute case, by (30)

$$(42) \quad s(\alpha') \leq 2n(q+1)^2 C_2.$$

Now let $\alpha^* = \alpha' - \lambda$, then α is R -equivalent to α^* , by (39) and (41) we get (19) and in the absolute case (40) and (42) implies (20).

Now we turn to the proofs of Theorem 3 and Theorem 4. In the following we shall use the notation of paragraph 5. Theorem 3 and Theorem 4 could be deduced from Theorem 1 and Theorem 2, respectively, but our conditions concerning λ will be weaker if we prove Theorem 3 and Theorem 4 by applying the following result of GYÖRNY [19] (see Theorem 15 in [19]):

Theorem B. *If $\alpha \in \mathcal{O}_{S,L}$ with $D_{L/K}(\alpha) = \delta$ then α is $\mathcal{O}_S$ -equivalent to an $\alpha^* \in \mathcal{O}_{S,L}$ of height*

$$(43) \quad H(\alpha^*) \leq C_3$$

with the constant C_3 of Theorem 3.

This theorem is in fact a consequence of Theorem A. Using the well-known properties of the heights of algebraic numbers, one can easily prove that for any non-zero $\alpha_1, \dots, \alpha_m$ in G we have

$$\log H(\alpha_1 + \dots + \alpha_m) \leq (m+1)g + 2g(\log H(\alpha_1) + \dots + \log H(\alpha_m))$$

and

$$\log H(\alpha_1 \dots \alpha_m) \leq (m+1)g + 2g(\log H(\alpha_1) + \dots + \log H(\alpha_m))$$

(cf. e. g. [23], p. 31).

In the proofs of Theorem 3 and Theorem 4 we shall utilize these inequalities.

PROOF OF THEOREM 3. Let $x_1, \dots, x_k \in \mathcal{O}_S$ and $\lambda \in \mathcal{O}_{S,L}$ be a solution of equation (22) with $H(\lambda) < X_H^{\varepsilon_6}$ where $X_H = \max_i H(x_i)$. Let again $\gamma^{(1)}, \dots, \gamma^{(n)}$ denote the conjugates of any $\gamma \in L$ over K , and let $l(x) = \alpha_1 x_1 + \dots + \alpha_k x_k$. Applying Theorem B to equation (22) we obtain

$$(44) \quad l(x) + \lambda = \varrho + a$$

where $\varrho \in \mathcal{O}_{S,L}$, $a \in \mathcal{O}_S$ and by (43) $H(\varrho) < C_3$. Let $l_{ij}(\underline{x}) = l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$, $\lambda_{ij} = \lambda^{(i)} - \lambda^{(j)}$ and $\varrho_{ij} = \varrho^{(i)} - \varrho^{(j)}$ for any $i \neq j$, $1 \leq i, j \leq n$. (44) gives

$$(45) \quad l_{ij}(\underline{x}) = \varrho_{ij} - \lambda_{ij} \quad (1 \leq i, j \leq n)$$

where

$$(46) \quad \max_{1 \leq i, j \leq n} \log H(\varrho_{ij} - \lambda_{ij}) \leq 5g + 4g \log C_3 + 4g \log H(\lambda).$$

By our assumptions concerning $\alpha_1, \dots, \alpha_k$, equation system (45) has a unique solution $x_1, \dots, x_k$ and by Cramer's rule we have

$$x_i = \frac{v_i}{v}, \quad i = 1, \dots, k$$

where v_i ($i=1, \dots, k$) and v denote the determinants corresponding to x_i . By (46) we get

$$\max_i \log H(v_i) < k!g^3(16 \log C_3 + 16 \log H(\lambda) + 54k \log A)$$

and

$$\log H(v) < 34g^3kk! \log A,$$

whence

$$(47) \quad \log X_H = \max_i \log H(x_i) <$$

$$< k!g^4(32 \log C_3 + 32 \log H(\lambda) + 179k \log A).$$

Our condition concerning λ implies $32k!g^4 \log H(\lambda) < \frac{1}{2} \log X_H$, that is (23) follows from (47).

PROOF OF COROLLARY 3.1. One can easily see that if $|\bar{\lambda}| < \frac{1}{4} (\max_i |x_i|)^{e_7}$ then λ satisfies the condition of Theorem 3 concerning λ and (23) implies (24).

PROOF OF THEOREM 4. Denote the conjugates of any $\gamma \in L$ over K as in the proof of Theorem 3. Applying Theorem B to (25) we obtain

$$(48) \quad \alpha + \lambda = \varrho + a$$

where $\varrho \in \mathcal{O}_{S,L}$, $a \in \mathcal{O}_S$ and by (43) $H(\varrho) < C_3$. Let $\alpha_{ij} = \alpha^{(i)} - \alpha^{(j)}$, $\lambda_{ij} = \lambda^{(i)} - \lambda^{(j)}$ and $\varrho_{ij} = \varrho^{(i)} - \varrho^{(j)}$ for any $i \neq j$, $1 \leq i, j \leq n$. Let us fix the indices i, j so that

$$H(\alpha_{ij}) = \max_{1 \leq i', j' \leq n} H(\alpha_{i'j'}).$$

As in the proof of Theorem 2 we have $[K(\alpha):K] \leq [L:K] = n$ since $\alpha \in \mathcal{O}_{S,L}$. The condition of Theorem 4 concerning λ implies

$$(49) \quad \log H(\alpha) < \varepsilon_8 n^2 g(1 + 2 \log H(\alpha_{ij})).$$

Further, using (48) and (49) we have

$$\begin{aligned}\log H(\alpha_{ij}) &= \log H(\varrho_{ij} - \lambda_{ij}) \equiv 5g + 4g \log C_3 + 4g \log H(\lambda) < \\ &< 6g + 4g \log C_3 + 8n^2 g^2 \varepsilon_8 \log H(\alpha_{ij}),\end{aligned}$$

whence, by the definition of ε_8 we get a bound for $\log H(\alpha_{ij})$. In view of (49) this bound gives

$$(50) \quad \log H(\lambda) < \log C_3 + 2.$$

Put $\alpha^* = \varrho - \lambda$, then α^* is $\mathcal{O}_S$ -equivalent to α and in view of $H(\varrho) < C_3$ and (50) we get (26).

References

- [1] A. BAKER, Transcendental number theory, 2nd ed., *Cambridge*, 1979.
- [2] Z. I. BOREVICH and I. R. SHAFAREVICH, Number theory, 2nd ed., *Academic Press, New York and London*, 1967.
- [3] I. GAÁL, Inhomogeneous discriminant form and index form equations and their applications, *Publ. Math. (Debrecen)* **33** (1986), 21–27.
- [4] K. GYÖRY, Sur les polynômes à coefficients entiers et de discriminant donné, *Acta Arith.* **23** (1973), 419–426.
- [5] K. GYÖRY, Sur les polynômes à coefficients entiers et de discriminant donné, II., *Publ. Math. (Debrecen)* **21** (1974), 125–144.
- [6] K. GYÖRY, Sur les polynômes à coefficients entiers et de discriminant donné, III., *Publ. Math. (Debrecen)* **23** (1976), 141–165.
- [7] K. GYÖRY, Polynomials with given discriminant, *Coll. Math. Soc. János Bolyai*, **13** (Debrecen, 1974). Topics in Number Theory (Edited by P. Turán), *North-Holland Publ. Comp. (Amsterdam—Oxford—New York, 1976)*, 65–78.
- [8] K. GYÖRY, On polynomials with integer coefficients and given discriminant, IV., *Publ. Math. (Debrecen)* **25** (1978), 155–167.
- [9] K. GYÖRY, On polynomials with integer coefficients and given discriminant, V., p -adic generalizations, *Acta Math. Acad. Sci. Hungar.* **32** (1978), 175–190.
- [10] K. GYÖRY, On the greatest prime factors of decomposable forms at integer points, *Ann. Acad. Sci. Fenn. Ser. A, I*, **4** (1978/1979), 341–355.
- [11] K. GYÖRY, On certain graphs composed of algebraic integers of a number field and their applications I., *Publ. Math. (Debrecen)* **27** (1980), 229–242.
- [12] K. GYÖRY, Explicit upper bounds for the solutions of some diophantine equations, *Ann. Acad. Sci. Fenn. Ser. A, I*, **5** (1980), 3–12.
- [13] K. GYÖRY, 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. GYÖRY, On the representation of integers by decomposable forms in several variables, *Publ. Math. (Debrecen)* **28** (1981), 89–98.
- [15] K. GYÖRY, On S -integral solutions of norm form, discriminant form and index form equations, *Studia Sci. Math. Hungar.*, **16** (1981), 149–161.
- [16] K. GYÖRY, On discriminants and indices of integers of an algebraic number field, *J. Reine Angew. Math.*, **324** (1981), 114–126.
- [17] K. GYÖRY, On certain graphs associated with an integral domain and their applications to diophantine problems, *Publ. Math. (Debrecen)* **29** (1982), 79–94.
- [18] K. GYÖRY, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta Math. Hungar.* **42** (1983), 45–80.
- [19] K. GYÖRY, 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.
- [20] K. GYÖRY, On norm form, discriminant form and index form equations, *Coll. Math. Soc. János Bolyai*, **34** (Budapest, 1981). Topics in Classical Number Theory, *North-Holland Publ. Comp., Amsterdam*, (1984), 617–676.

- [21] K. GYÖRY and Z. Z. PAPP, On discriminant form and index form equations, *Studia Sci. Math. Hungar.*, **12** (1977), 47—60.
- [22] K. GYÖRY and Z. Z. PAPP, Effective estimates for the integer solutions of norm form and discriminant form equations, *Publ. Math. (Debrecen)* **25** (1978), 311—325.
- [23] V. G. SPRINDŽUK, Classical diophantine equations in two variables (in Russian), *Izd. Nauka, Moskva*, 1982.

KOSSUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
4010 DEBRECEN, HUNGARY

(Received April 3, 1985)