Publ. Math. Debrecen
69/**4** (2006), 473–499

Polynomials and binary forms with given discriminant

By GYŐRY KÁLMÁN (Debrecen)

Dedicated to Professor W. M. Schmidt

Abstract. There is an extensive literature of monic polynomials and binary forms with given discriminant. The first part of our paper gives a brief survey of the most important results over $\mathbb{Z}$ on such polynomials and binary forms as well as on their various applications. In the second part we improve some earlier general effective and quantitative results over number fields. As an application we obtain some new information about the arithmetical properties of discriminants of polynomials and binary forms.

1. Introduction

Many number-theoretic problems lead to discriminant equations of the form

$$D(F) = D \qquad \text{in } F, \tag{1}$$

where D is a given non-zero integer, F is a monic polynomial, a binary form or a decomposable form with coefficients in $\mathbb{Z}$ (or in a more general domain), and $D(F)$ denotes the discriminant of F. There are several finiteness theorems on such equations, which have important applications

Mathematics Subject Classification: 11R09, 11R04, 11E76, 11D85, 11D61, 11J86.
Key words and phrases: polynomials, binary forms, algebraic numbers, discriminants, diophantine equations, effective and quantitative finiteness results.
Research supported in part by the Hungarian Academy of Sciences and by Grants 38225 and 42985 from the Hungarian National Foundation for Scientific Research.

in algebraic number theory and in the theory of Diophantine equations. In Sections 2 and 3 we give a brief survey of these theorems and some of their applications. All these results were proved by reducing (1) to finitely many unit equations in two unknowns and then applying various finiteness theorems on unit equations. Using some recent improved bounds of Yu and the author [36] on the solutions of S-unit equations, we improve in Sections 4 and 5 several general effective and quantitative results from [26], [29], [32], [34] and [16] concerning monic polynomials and binary forms with given discriminant.

The survey Sections 2 and 3 are devoted to monic polynomials and binary forms, respectively. As will be pointed out in Sections 3 and 4, the results concerning equivalence classes of monic polynomials can be reformulated in terms of *strong* equivalence classes of monic binary forms. However, it should be remarked that the general effective results traited in Sections 3 and 4 on binary forms do not imply effective results on strong equivalence classes of monic binary forms and, consequently, on equivalence classes of monic polynomials.

For simplicity, the earlier results will be presented over $\mathbb{Z}$ only, and references will be given to more general versions. For latter applications, we formulate and prove our new results in more general forms, over the rings of S-integers of number fields.

In Sections 2 and 3 some important related topics will not be discussed and many references will be left out owing to lack of space. For instance, we shall not deal with numerical results and decomposable forms in more than two variables. These might be the subject of another survey paper.

2. Monic polynomials

Two monic polynomials $F, F^* \in \mathbb{Z}[x]$ are called *equivalent* if $F^*(x) = F(x+b)$ for some $b \in \mathbb{Z}$. In this case they have the same discriminant.

In 1930, Delone [8] and Nagell [43] proved independently of each other that up to equivalence, there are only finitely many irreducible monic polynomials $F \in \mathbb{Z}[x]$ with degree 3 for which (1) holds. In the quartic case, the same assertion was proved later by Nagell [44], [45]. Their proofs were ineffective.

Delone [8] (see also [9]) determined a great number of cubic monic polynomials $F \in Z[x]$ with given negative discriminant, including all F with $-172 \leq D(F) < 0$. In their book [9], Delone and Faddeev posed in 1940 the problem of giving an algorithm for finding all cubic monic polynomials with integral coefficients and given non-zero discriminant.

2.1. General effective finiteness results. By reducing (1) to unit equations and using Baker's theory of linear forms in logarithms, the present author proved in 1973 the following general theorem.

Theorem A (Győry [22]). *Up to equivalence, there are only finitely many monic polynomials $F \in Z[x]$ with a given non-zero discriminant, and all these F can be effectively determined.*

Since 1974, various *quantitative* versions have been estabilished by the author; cf. [23]–[26], [29], [32], [34]. In [23] it was proved that if $F \in Z[x]$ is a monic polynomial of degree n with discriminant $D \neq 0$ then

$$n \leq 2 + 2(\log |D|)/\log 3 \tag{2}$$

and this estimate is already sharp. Hence it suffices to consider (1) for polynomials F of fixed degree.

Denote by $H(F)$ the maximum absolute value of the coefficients of a polynomial F with integral coefficients. By the splitting field of F (over $\mathbb{Q}$) we mean the smallest finite extension of $\mathbb{Q}$ over which F can be factored into linear factors. The best known quantitative version of Theorem A which involves the splitting field is the following.

Theorem B (Győry [34]). *Let $F \in Z[x]$ be a monic polynomial of degree n with discriminant $D \neq 0$. Then F is equivalent to a polynomial F^* for which*

$$H(F^*) \leq c_1|D|^{c_2} \tag{3}$$

with effectively computable positive constants c_1, c_2 which depend only on n and the regulator of the splitting field of F.

The constants c_1 and c_2 are given explicitely in [34]. From the explicit version of (3) it is easy to deduce that

$$H(F^*) \leq \exp\{c_3(|D| \log^2 |D|)^m\}, \tag{4}$$

where c_3 is an effectively computable positive constant depending only on n, and m denotes the degree of the splitting field of F. We note that $1 \leq m \leq n!$.

For polynomials of fixed degree, Theorems A and B have been *generalized* and *extended* in several directions.

- Effective finiteness theorems were proved for equation (1) with D replaced by $p_1^{z_1} \dots p_s^{z_s}$, where $p_1, \dots, p_s$ are fixed primes and $z_1, \dots, z_s$ are unknown non-negative integers; cf. [26], [29], [32], [34] and Section 4 of the present paper.
- Generalizations were given for not necessarily monic polynomials with bounded leading coefficient; cf. [24].
- Various generalizations were established for the number field case when the ground ring is the ring of integers or, more generally, the ring of S-integers of a number field; cf. [25], [26], [29], [32], [34] and Section 4 of this paper.
- The results were extended to the case when $D(F)$ is not necessarily different from zero. Then one considers the equation $D(F_0) = D$ for fixed $D \neq 0$, where F_0 is the maximal square-free divisor of F in $\mathbb{Z}[x]$; cf. [25], [29], [34].
- In [30] and [32] further generalizations were obtained for the case when the ground ring is an arbitrary finitely generated integral domain over $\mathbb{Z}$ which may contain transcendental elements too.

The proofs of the afore-mentioned effective results were reduced to unit or S-unit equations and then some effective results of [27], [7] or [34] were applied to these equations; see also Section 5.

Analogous results over function fields were proved by Győry [32], Gaál [21] and Shlapentokh [50].

Theorems A, B as well as their various versions and generalizations led to several *applications*. We present only some applications in qualitative form and over $\mathbb{Z}$; for more general and quantitative versions and other related results we refer to [23]–[26], [29], [32], [34], [35] and [28].

- Up to translation of the type $\alpha \to \alpha + b$ with $b \in \mathbb{Z}$, there are only finitely many algebraic integers $\alpha \in \overline{\mathbb{Q}}$ with given discriminant, and all these α can be effectively determined. This was proved by Birch and Merriman [4] in a non-effective form and independently, as a consequence of Theorem A, by the present author [22] in an effective form.

- Let K be an algebraic number field with ring of integers O_K. There are only finitely many units in O_K with a given non-zero discriminant, and all these can be effectively determined; cf. [24]
- Up to translation by elements of $\mathbb{Z}$, there are only finitely many $\alpha \in O_K$ with a given index, and all these α can be effectively determined; cf. [24].
- Up to translation by elements of $\mathbb{Z}$, there are only finitely many $\alpha \in O_K$ with $O_K = \mathbb{Z}[\alpha]$ and all these α can be effectively determined; cf. [24]. This provides an algorithm which makes it possible, at least in principle, to find all power integral bases $\{1, \alpha, \ldots, \alpha^{n-1}\}$ in O_K, where n denotes the degree of K over $\mathbb{Q}$.
- Some information was obtained in [26] and [29] on the arithmetical properties of discriminants and indices of elements of O_K. In number fields of unit rank 1, certain improvements were later obtained by Pethő [47].
- Kovács [40] used the above-mentioned result on power integral bases to give a general algorithm for determining all canonical number systems in O_K.
- Some applications to irreducible polynomials were given in [24] and [31].
- Effective upper bounds were deduced for the solutions of discriminant form and index form equations; cf. [24], [37] and [55]. For "inhomogeneous" generalizations, see Gaál [20].
- Effective upper bounds were derived in [48] and [56] for the solutions of elliptic and superelliptic equations, and for m in the equation $f(x) = y^m$; see [6], [39] and [38].

2.2. Bounds for the number of equivalence classes. Evertse and the author [15] derived explicit upper bounds for the number of equivalence classes of monic polynomials with integral coefficients and given non-zero discriminant. We denote by $\omega(D)$ the number of distinct prime factors of a non-zero integer D.

Theorem C (Evertse and Győry [15]). *Let $n \geq 2$ be an integer. Then the monic polynomials $F \in \mathbb{Z}[x]$ of degree n with discriminant $D \neq 0$ and with splitting field M belong to at most*

$$c_4\Big(4 \cdot 7^{m(2\omega+3)}\Big)^{n-2} \tag{5}$$

equivalence classes, where $c_4 = n(n-1)/(n-2)!$, $m = [M : \mathbb{Q}]$ and $\omega = \omega(D)$.

Further, it was proved in [15] that for the polynomials F in Theorem C

$$n \leq 2 + 4 \cdot 7^{m(2\omega+3)} \tag{6}$$

holds. When $|D|$ is large compared with m and ω, (6) gives a better bound for n than (2).

In the proofs of (5) and (6) equation (1) was reduced to unit equations and then a result of Evertse [10] was utilized on the number of solutions of such equations.

In [14], [12], [18], [2] and [35] there are quantitative results which imply bounds for the number of equivalence classes of irreducible monic polynomials with given discriminant. These results give better estimates than (5) if m is large with respect to the degree n. Theorem C, (6) and the results of [14], [12] and [18] were proved in more *general* forms, over the rings of S-integers of a number field or, more generally, over an arbitrary finitely generated integral domain over $\mathbb{Z}$.

Theorem C from [15] and the results of [14], [12] and [18] have several *applications*. We mention some of them in their simplest form; more general and quantitative versions can be found in [14] and [15].

– Let K be an algebraic number field of degree n with ring of integers O_K. Then, up to translation by elements of $\mathbb{Z}$, the number of $\alpha \in O_K$ with a non-zero discriminant can be bounded above by an expression of the form (5); cf. [14], [15]. When m is large compared with n, better bounds follow from the results of [12] and [18]. Further improvements have been given in [35] and [2] in the particular case when the Galois group of the normal closure M of K over $\mathbb{Q}$ is triply transitive. We note that the results of [14], [12], [18], [35] and [2] are formulated in terms of decomposable form equations or, in particular, of discriminant form and index form equations.

- Theorem C and the above-mentioned results of [14], [15], [12], [18], [35] and [2] concerning algebraic integers have further applications to elements $\alpha \in O$ with given index and to power integral bases, where O is an order in K. For example, it was proved in [14] that, up to $\mathbb{Z}$-equivalence, there are at most

  $$\left(4 \cdot 7^{3m}\right)^{n-2} \tag{7}$$

  $\alpha \in O$ with $O = \mathbb{Z}[\alpha]$. Further, in the particular case when $O = O_K$ and $\mathrm{Gal}(M/\mathbb{Q})$ is triply transitive, this was proved in [35] with $2^{4n(n-1)+9}$ in place of (7). We do not know whether the best possible upper bound is exponential or polynomial in terms of n.

3. Binary forms

Every binary form $F(x, y) \in \mathbb{Z}[x, y]$ of degree $n \geq 2$ can be factored over $\overline{\mathbb{Q}}$ as $\prod_{i=1}^{n} (\alpha_i x + \beta_i y)$. The *discriminant* of F is defined by

$$D(F) = \prod_{1 \leq i < j \leq n} (\alpha_i \beta_j - \alpha_j \beta_i)^2 .$$

This is a rational integer and is independent of the choice of the factorization of F into linear forms. For $\lambda \in \mathbb{Q}^*$ and for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}$,

$$D(\lambda F) = \lambda^{2n-2} D(F), \quad D(F_A) = (\det A)^{n(n-1)} D(F),$$

where $F_A(x, y) = F(ax + by, cx + dy)$.

Two binary forms F, $F^* \in \mathbb{Z}[x, y]$ are called *equivalent* if $F^* = F_A$ for some $A \in GL_2(\mathbb{Z})$ (i.e. A has entries in $\mathbb{Z}$ and determinant ± 1). In this case F and F^* have the same discriminant. Two equivalent binary forms F, $F^* \in \mathbb{Z}[x, y]$ are said to be *strongly equivalent* if $F^* = F_A$ for some $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b \in \mathbb{Z}$. Using the correspondence between the binary forms $F(x, y)$ and polynomials $F(x, 1)$, all the results presented in Section 2 on monic polynomials can be reformulated in an obvious way for strongly equivalent *monic* binary forms, that is for forms $F(x,y)$ with $F(1,0)=1$.

By classical results of Lagrange (1773, case $n=2$) and Hermite (1851, case $n=3$), every binary form $F\in\mathbb{Z}[x,y]$ with degree $n\le 3$ and discriminant $D\ne 0$ is equivalent to a form F^* for which

$$H(F^*)\le c_5|D|$$

with an effectively computable absolute constant c_5.

In 1972, Birch and Merriman proved the following.

Theorem D (Birch and Merriman [4]). *For $n\ge 4$, there are only finitely many equivalence classes of binary forms in $\mathbb{Z}[x,y]$ of degree n with a given non-zero discriminant.*

The proof of Birch and Merriman is *non-effective.*

3.1. General effective finiteness results. Theorems A, B and (2), (4) imply in a quantitative form that there are only finitely many *strong* equivalence classes of *monic* binary forms $F\in\mathbb{Z}[x,y]$ with a given non-zero discriminant, and a full set of representatives of these classes can be effectively determined.

For *general* (i.e. not necessarily monic) binary forms $F\in\mathbb{Z}[x,y]$ of degree n and discriminant $D\ne 0$, the author [23] proved in 1974 the estimate

$$n\le 3+2\left(\log|D|\right)/\log 3 \tag{8}$$

which is already sharp. In 1991 we showed with Evertse [16] that if F is square-free then

$$n\le 3\Big(7^{m(2\omega+3)}+1\Big),$$

where $\omega=\omega(D)$ and m denotes the degree of the splitting field of F. Further, we proved the following general effective theorem.

Theorem E (Evertse and Győry [16]). *Every binary form $F\in\mathbb{Z}[x,y]$ of degree $n\ge 2$ with discriminant $D\ne 0$ is equivalent to a form F^* for which*[1]

$$H(F^*)\le\exp\left\{(c_6n)^{c_7n^4}|D|^{8n^3}\right\}, \tag{9}$$

where c_6, c_7 are effectively computable positive absolute constants.

[1] *Added in proof.* Recently we have improved the exponent of $|D|$ to $6n$.

In [16] it was also proved another version of Theorem E which implies

$$H(F^*) \leq c_8|D|^{c_9} \tag{10}$$

in place of (9), where c_8, c_9 are effectively computable positive constants which depend only on n and the discriminant of the splitting field of F over $\mathbb{Q}$.

The main tool in the proof of (10) and Theorem E is an effective result of the author [27] on S-unit equations. The proof is, however, more complicated than in the monic case because in the general situation the factorization of F into linear factors over $\overline{\mathbb{Q}}$ is unique only up to proportional factors.

Together with (8), Theorem E provides immediately the following.

Corollary. *There are only finitely many equivalence classes of binary forms $F \in \mathbb{Z}[x, y]$ with a given non-zero discriminant, and a full set of representatives of these classes can be effectively determined.*

We mention that the above general effective results concerning binary forms do not imply effective finiteness results on strong equivalence classes of monic binary forms. In other words, Theorem E and its Corollary do not provide the effective results presented in Section 2 on monic polynomials of given discriminant (see [16], p. 171).

Theorem E was proved in [16] in a more general form, over the rings of S-integers of number fields; cf. Section 4. Further, Theorem E and (8) were later generalized for decomposable forms in more than two variables; cf. [17], [33].

In [16] several *applications* of Theorem E, (10) and their more general versions were given to

- algebraic numbers of given discriminant,
- arithmetical properties of discriminants of binary forms,
- discriminant form inequalities,
- minimal non-zero values of binary forms at integral points.

Some of these applications are improved in Section 4. Further applications of (8), (9), (10) have been obtained by Brindza, Evertse and Győry [6], Stewart [53], Thunder [54], Brindza [5] to Thue-equations and

Thue-inequalities, and by Ribenboim [49] to binary forms with given discriminant and additional appropriate conditions on the coefficients. In [49] certain results are also established under the assumption that the ABC conjecture is true.

In (10), the constants c_8, c_9 are effective and c_9 can be expressed as a polynomial of the discriminant of the splitting field of F. In 1993, Evertse proved the following partially ineffective improvement of (10).

Theorem F (Evertse [11]). *Every binary form $F \in \mathbb{Z}[x,y]$ of degree $n \geq 2$ with discriminant $D \neq 0$ is equivalent to a form F^* for which*

$$H(F^*) \leq c_{10}|D|^{\frac{21}{n-1}}, \tag{11}$$

where c_{10} is a constant which depends only on n and the discriminant of the splitting field of F.

This theorem is proved [11] in a more general form, over the rings of S-integers of number fields. Its proof is based on Roth's theorem over number fields, hence c_{10} in (11) is ineffective. The exponent in (11) is already best possible up to an absolute constant factor. It would have great interest to prove Theorem F with an effective constant c_{10} and to find out whether the dependence on the splitting field is needed.

3.2. Bounds for the number of equivalence classes. Let

$$F(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n$$

be an irreducible binary form with integral coefficients. Let α be a zero of $F(x,1)$, and let $K = \mathbb{Q}(\alpha)$ with ring of integers O_K. Then

$$O_F = \left\{1, a_0\alpha, a_0\alpha^2 + a_1\alpha, \ldots, a_0\alpha^{n-1} + \cdots + a_{n-2}\alpha\right\}$$

is a $\mathbb{Z}$-module of rank n in O_K which is closed under multiplication. Thus O_F is an order. It is determined by F up to conjugation. Further, it has the following important properties (cf. [46], [51]):

- $O_{F_A} = O_F$ for every $A \in GL_2(\mathbb{Z})$, hence O_F is called the *invariant order* of F;
- The discriminant $D(O_F)$ of O_F coincides with the discriminant $D(F)$ of F;

- $D(F) = I^2 D_K$, where $I = [O_K : O_F]$. If in particular F is monic, then $O_F = \mathbb{Z}[\alpha]$.

An immediate consequence of Theorem E is that if O is a given order of some number field, then the irreducible binary forms $F \in \mathbb{Z}[x, y]$ with $O_F = O$ lie in finitely many equivalence classes, and a full set of representatives of these classes can be effectively determined.

For $n = 3$, it follows from a result of Delone and Faddeev [9] that for every cubic order O there is precisely one equivalence class of irreducible binary forms $F \in \mathbb{Z}[x, y]$ with degree n and invariant order $O_F = O$. For $n > 3$ this is no longer true: Simon [51] gave examples of number fields K of degree 4 and of arbitrary large degree whose ring of integers O_K cannot be represented as O_F for any irreducible binary form F.

If O is an order of a number field of degree $n \geq 4$, then (7) implies an explicit upper bound for the number of strong equivalence classes of monic irreducible binary forms $F \in \mathbb{Z}[x, y]$ with $O_F = O$. Recently, the following has been established in [3] for not necessarily monic binary forms.

Theorem G (Bérczes, Evertse and Győry [3]). *Let O be an order with quotient field of degree $n \geq 4$ over $\mathbb{Q}$. Then the number of equivalence classes of irreducible binary forms $F \in \mathbb{Z}[x, y]$ with $O_F = O$ is at most*

$$2^{24n^3}.$$

The proof of Theorem G involved among other things a theorem of Beukers and Schlickewei [1] on the number of solutions of the equation $x + y = 1$ in a finitely generated multiplicative group.

Theorem G was used in [3] to derive upper bounds for the number of equivalence classes of binary forms with given discriminant. For given integers $a, k \geq 1$ denote by $d_k(a)$ the number of tuples of positive integers $d_1, \ldots, d_k$ such that $d_1 \ldots d_k | a$.

Theorem H (Bérczes, Evertse and Győry [3]). *Let K be a number field of degree $n \geq 3$ over $\mathbb{Q}$ with discriminant D_K, and let I be a positive integer. The irreducible binary forms $F \in \mathbb{Z}[x, y]$ for which $K = \mathbb{Q}(\alpha)$ for some zero α of $F(x, 1)$ and $D(F) = I^2 D_K$ lie in at most*

$$2^{24n^3(\omega(I)+1)} d_{n(n-1)/2}\left(I^2\right) \left(\sum_{d^{n(n-1)/2} | I} d \right)$$

equivalence classes.

Let $K_1, \dots, K_q$ be not necessarily distinct number fields with respective degrees $n_1 \geq 3, n_2, \dots n_q$, and discriminants $D_{K_1}, \dots, D_{K_q}$. Denote by $\mathcal{F}(K_1, \dots, K_q)$ the set of binary forms $F \in \mathbb{Z}[x, y]$ such that

$$F = F_1 \dots F_q$$

with irreducible forms $F_i \in \mathbb{Z}[x, y]$ for which $K_i = \mathbb{Q}(\alpha_i)$ for some zero α_i of $F_i(x, 1)$, $i = 1, \dots, q$. Then one can show that

$$D(F) = I^2 D_{K_1} \dots D_{K_q} \tag{12}$$

for some positive integer I. The next theorem was deduced in [3] from Theorem H above and from a result obtained in [3] on resultant equations.

Theorem I (Bérczes, Evertse and Győry [3]). *For given I and $\varepsilon > 0$, the number of equivalence classes of binary forms $F \in \mathcal{F}(K_1, \dots, K_q)$ with* (12) *is at most*

$$cI^{2/n(n-1)+\varepsilon},$$

where $n = n_1 + \dots + n_q$ and $c = c(n_1, \dots, n_q, \varepsilon)$ is a positive constant.

The bound is almost best possible in terms of I, the exponent cannot be replaced by an expression $< 2/n(n-1)$. In the monic case, Theorems H and I can be compared with Theorem C in Section 2.

4. Improvement of some earlier effective and quantitative results

In this section we improve some general effective and quantitative results of the author [26], [29], [32], [34] on monic polynomials, and Evertse and the author [16] on binary forms of given discriminant. The results concerning monic polynomials will be formulated in terms of monic binary forms.

Before stating our results, we recall some definitions and adopt some notation from [29], [32], [34] and [16]. Let K be an algebraic number field with ring of integers O_K, and let S be a finite set of places on K, including the set S_∞ of infinite places. Let O_S and O_S^* denote the ring of S-integers and the group of S-units in K, respetively.

By an O_S-ideal we mean a finitely generated O_S-submodule of K and by an integral O_S-ideal, an O_S-ideal that is contained in O_S. The O_S-ideal generated by $\alpha_1, \dots, \alpha_k$ is denoted by $(\alpha_1, \dots, \alpha_k)_S$. If $F \in K[x, y]$ then $(F)_S$ denotes the O_S-ideal generated by the coefficients of F. If $\mathbf{a}$ is an O_S-ideal, and $\mathbf{a}^*$ is the O_K-ideal composed of prime ideals outside S such that $\mathbf{a} = \mathbf{a}^* O_S$, then the S-norm of $\mathbf{a}$, denoted by $N_S(\mathbf{a})$, is defined as $N_{K/\mathbb{Q}}(\mathbf{a}^*)$. The *$S$-discriminant* of a square-free binary form $F \in K[x, y]$ of degree n is defined as the O_S-ideal

$$\mathbf{d}_S(F) = \frac{(D(F))_S}{(F)_S^{2(n-1)}}.$$

This is an integral O_S-ideal.

Two binary forms $F, F^* \in K[x, y]$ are called *weakly O_S-equivalent* if there is an $A \in GL_2(O_S)$ and a $\lambda \in K^*$ such that

$$F^* = \lambda F_A.$$

We remark that this concept was defined in [16] with A contained in $SL_2(O_S)$. Following the arguments of [16], p. 173, it is easily seen that if $F, F^* \in K[x, y]$ are weakly O_S-equivalent in the present sense then they have the same S-discriminant.

In the results presented below the following notation is used: $d = [K : \mathbb{Q}]$, M is a finite normal extension of K with $[M : K] = m$, D_L is the discriminant of an arbitrary number field L, $\mathbf{p_1}, \dots, \mathbf{p_t}$ are the prime ideals in O_K associated to the finite places of S, and

$$P = \max_i N(\mathbf{p_i}), \ W = \log N(\mathbf{p_1}) \dots \log N(\mathbf{p_t})$$

if $t > 0$, and $P = W = 1$ if $t = 0$. We denote by $h(\alpha)$ the absolute height, or briefly the *height*, of an algebraic number α (cf. Section 5), while $h(F)$ (resp. $h(A)$) denotes the maximum of the heights of the coefficients (resp. of the entries) of a polynomial F (resp. of a matrix A) with coefficients (resp. with entries) in $\overline{\mathbb{Q}}$. We write

$$\log^* a \text{ for } \max\{\log a, 1\}.$$

Further, c_{11} to c_{14} and c_{17} to c_{20} will denote effectively computable positive numbers which depend only on d, m, $|D_M|$ and the degree, n, of the binary forms F involved.

Theorem 1. *Let $F \in K[x,y]$ be a square-free binary form of degree $n \geq 3$ with $d_S(F) = \mathbf{d}$ and with splitting field M over K. Then F is weakly O_S-equivalent to a form F^* in $O_S[x,y]$ for which*

$$h(F^*) \leq \exp\{c_{11} \cdot c_{12}^t \, (PW)^m \log^* N_S(\mathbf{d})\}. \tag{13}$$

For monic binary forms $F \in O_S[x,y]$ we have $\mathbf{d}_S(F) = (D(F))_S$. In this case Theorem 2 gives a stronger result.

Two binary forms $F, F^* \in O_S[x,y]$ are called *O_S-equivalent* if $F^* = F_A$ for some $A \in GL_2(O_S)$. If in particular A is of the form $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with $b \in O_S$, $d \in O_S^*$, then F and F^* are said to be *strongly O_S-equivalent.* In this case F and F^* are at the same time monic or non-monic.

We say that F is a *general* binary form if it is not necessarily monic. For general binary forms, we deduce from Theorem 1 the following theorem. For monic binary forms, Theorem 2 is new in this form.

It will be more convenient to state our results concerning the general and monic cases in a single theorem. However, these two cases will be proved separately. The result obtained on general binary forms does not imply the corresponding statement established in the monic case.

Theorem 2. *Let $\delta \in O_S \setminus \{0\}$, and let $F \in O_S[x,y]$ be a general (resp. monic) binary form of degree $n \geq 3$ with $D(F) \in \delta O_S^*$ and with splitting field M over K. Then F is O_S-equivalent (resp. strongly O_S-equivalent) to a form F^* for which*

$$h(F^*) \leq \exp\{c_{13} \cdot c_{14}^t \, (PW)^m \log^* N_S(\delta)\}. \tag{14}$$

In the general case, for large t, Theorems 1 and 2 improve upon Theorems 2' and 3' of [16]. In the upper bounds occurring in these theorems of [16] there is a factor of the form t^t which is replaced in our theorems above by c^t with an appropriate constant c. This improvement will be crucial for our Corollaries 1 to 4.

It should be remarked that in [16] weak O_S-equivalence and O_S-equivalence are defined with $SL_2(O_S)$ in place of $GL_2(O_S)$. However, it is easy to show that in the general case each of Theorems 1, 2 and Theorems 2', 3' of [16] has two equivalent formulations, according as $SL_2(O_S)$ or $GL_2(O_S)$ is involved in the definition of (weak) O_S-equivalence. These two formulations can be easily deduced from each other with bounds of the same form on $h(F^*)$ in which only the constants c are different.

Every binary form $F \in K[x,y]$ can be factored as $\lambda F_1(x,y)\dots F_q(x,y)$, where $\lambda \in K^*$ and $F_1,\dots,F_q$ are irreducible forms in $K[x,y]$. For $j = 1,\dots,q$, let $M_j = K(\alpha_j)$, where α_j is one of the zeros of $F_j(x,1)$, and $M_j = K$ if $F_j = y$. $(M_1,\dots,M_q)$ is called a *system of fields* associated to F, and it is determined by F up to conjugation over K.

In [16] the authors proved their Theorems 2' and 3' for binary forms F associated to a fixed system of fields $(M_1,\dots,M_q)$. Their upper bounds depend on $|D_{M_1}\dots D_{M_q}|$ instead of $|D_M|$. However, as is shown in the proof of our Theorem 1,

$$|D_M|^{1/m(d+1)} \le |D_{M_1}\dots D_{M_q}| \le |D_M|^n$$

where $n = \deg F$.

For applications to algebraic numbers, we give a more explicit version of Theorem 1 in the special case $S = S_\infty$. In this case we write $\mathbf{d}(F)$ for $\mathbf{d}_{S_\infty}(F)$.

Theorem 3. *Let $F \in K[x,y]$ be a square-free binary form of degree $n \ge 3$ with $\mathbf{d}(F) = \mathbf{d}$, and suppose that F is associated to the system of fields $(M_1,\dots,M_q)$. Put $D = |D_{M_1}\dots D_{M_q}|$. Then F is weakly O_K-equivalent to a form F^* in $O_K[x,y]$ for which*[2]

$$h(F^*) \le \exp\{(c_{15}dn)^{c_{16}dn^4} D^{2n^3}(D^{2n^3} + \log N_{K/\mathbb{Q}}(\mathbf{d}))\},$$

where c_{15}, c_{16} are effectively computable absolute constants.

In terms of D this is an improvement of the case $S = S_\infty$ of Theorem 2' of [16]. In the monic case similar results were obtained in [34] with a stronger notion of equivalence; see Corollary 4 and (in the irreducible case) Corollary 6 of [34].

For fixed $D(F)$ we deduce from Theorem 2 the following.

[2] *Added in proof.* Recently we have improved the first and second exponents of D to $4n$ and $2(n-1)$, respectively.

Corollary 1. *Let $\delta \in O_S\backslash\{0\}$, and let $F \in O_S[x,y]$ be a general (resp. monic) binary form of degree $n \geq 3$ with $D(F) = \delta$ and with splitting field M over K. Then there is a $U \in SL_2(O_S)$ (of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ if F is monic) such that*

$$h(F_U) \leq \exp\{c_{17} \cdot c_{18}^t \, (PW)^m \log^* h(\delta)\}. \tag{15}$$

In the monic case, this is a considerable improvement of Theorem 3 of [34] in terms of t.

Let $\mathcal{S} = O_K \cap O_S^*$.

Corollary 2. *Let $\delta \in O_K \setminus \{0\}$, and let $F \in O_K[x,y]$ be a monic binary form of degree $n \geq 3$ with $D(F) \in \delta\,\mathcal{S}$ and with splitting field M over K. Then there is an $A = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with $b \in O_K$, $d \in \mathcal{S}$ and an $F^* \in O_K[x,y]$ such that $F = F_A^*$ and*

$$h(F^*) \leq \exp\{c_{19} \cdot c_{20}^t \, (PW)^m \log^* |N_{K/\mathbb{Q}}(\delta)|\}. \tag{16}$$

For large t, this is a significant improvement of Corollary 4 of [34].

In [26], [29], [34] and [16] the authors derived from their above-mentioned results similar, but weaker estimates for $h(F^*)$ without fixing the splitting field M or the fields $M_1, \ldots, M_q$. From our Theorems 1 to 3 and their Corollaries 1,2 one can deduce in the same way bounds for $h(F^*)$ when neither M nor $M_1, \ldots, M_q$ are fixed.

The following two corollaries are concerned with arithmetical properties of discriminants of binary forms. Suppose that F is a binary form in $K[x,y]$ and that

$$\mathbf{d}_S(F) = \mathbf{q}_1^{k_1} \ldots \mathbf{q}_w^{k_w} O_S,$$

where $\mathbf{q}_1, \ldots, \mathbf{q}_w$ are prime ideals outside S and $k_1, \ldots, k_w$ are positive integers. Put

$$P_S(F) = \max_{1 \leq i \leq w} N_{K/\mathbb{Q}}(\mathbf{q}_i) \quad \text{and} \quad w_S(F) = w$$

with the convention that $P_S(F) = 1$ if $w = 0$. In general $N_S(\mathbf{d}_S(F))$ cannot be estimated from above in terms of K, S and $P_S(F)$. However, this is possible when F has *minimal* S-discriminant, that is if

$$N_S(\mathbf{d}_S(F)) \leq N_S(\mathbf{d}_S(G))$$

for every binary form G that is weakly O_T-equivalent to F for $T = S \cup \{\mathbf{q}_1, \dots, \mathbf{q}_w\}$.

Denote by $\log_i$ the i-th iterated logarithm. Corollary 3 is a consequence of Theorem 1. Below $c_{21}, \dots, c_{28}$ will denote effectively computable positive numbers which depend at most on K, S, M and n.

Corollary 3. *Let $F \in K[x,y]$ be a binary form of degree $n \geq 3$ with splitting field M over K and with minimal S-discriminant. Then*

$$P(\log P)^w \geq c_{21}(\log N)^{c_{22}} \tag{17}$$

and

$$P > \begin{cases} c_{23}(\log N)^{c_{24}} & \text{\textit{if}} \quad w \leq \log P/\log_2 P \\ c_{25}(\log_2 N)(\log_3 N)/(log_4 N) & \text{\textit{otherwise,}} \end{cases} \tag{18}$$

provided that $\log_4 N > 1$, *where* $P = P_S(F)$, $w = w_S(F)$ *and* $N = N_S(\mathbf{d}_S(F))$.

This can be compared with Corollary 4 of [16] where $C_S(F) = N_{K/\mathbb{Q}}(\mathbf{q}_1 \dots \mathbf{q}_\omega)$ is used in place of $P_S(F)$. We note that in terms of $P_S(F)$ the results of [16] give only

$$P_S(F) > c_{26} \log_2 N_S(\mathbf{d}_S(F))$$

which is weaker than (17) and (18), especially when $\omega_S(F)$ is small.

Our Corollary 3 motivates the following.

Conjecture 1. *Under the assumptions of Corollary 3,*

$$P_S(F) > c_{27}(\log N_S(\mathbf{d}_S(F)))^{c_{28}}$$

holds.

By virtue of (18) it would be enough to prove the conjecture for the case

$$\frac{\log P_S(F)}{\log_2 P_S(F)} < \omega_S(F) < c_{29} \frac{P_S(F)}{\log P_S(F)},$$

where c_{29} can be given explicitly in terms of K.

For monic binary forms $F \in O_K[x,y]$ a stronger result can be deduced from Corollary 2. In this case the S_∞-discriminant $\mathbf{d}(F)$ is just the O_K-

ideal $(D(F))$. Denote by $\omega(F)$ the number of distinct prime ideal divisors of $D(F)$, and by $P(F)$ the maximum norm of these prime ideals. In general $|N_{K/\mathbb{Q}}(D(F))|$ can not be bounded above in terms of K and $P(F)$. We say that a square-free monic binary form $F \in O_K[x,y]$ has *minimal* discriminant in *monic sense* if for every binary form $G \in O_K[x,y]$ for which $F = G_A$ with some $A = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with $b \in O_K$, $d \in O_K \setminus \{0\}$,

$$|N_{K/\mathbb{Q}}(D(F))| \leq |N_{K/\mathbb{Q}}(D(G))|$$

holds.

We denote by $c_{30}, \dots, c_{36}$ effectively computable positive numbers which depend at most on K, M and n.

Corollary 4. *Let $F \in O_K[x,y]$ be a square-free monic binary form of degree $n \geq 3$ with splitting field M over K and with minimal discriminant in monic sense. Then*

$$P(\log^* P)^w \geq c_{30}(\log N)^{c_{31}} \tag{19}$$

and

$$P > \begin{cases} c_{32}(\log N)^{c_{33}} & \text{if } w \leq \log P / \log_2 P, \\ c_{34}(\log_2 N)(\log_3 N)/(\log_4 N) & \text{otherwise,} \end{cases} \tag{20}$$

provided that $\log_4 N > 1$, where $P = P(F)$, $w = w(F)$ and
$N = |N_{K/\mathbb{Q}}(D(F))|$.

For irreducible monic binary forms $F \in O_K[x,y]$ a weaker version was proved in [29] in terms of algebraic integers.

Conjecture 2. *Under the assumptions of Corollary 4,*

$$P(F) > c_{35}(\log |N_{K/\mathbb{Q}}(D(F))|)^{c_{36}}$$

holds.

In [29], [32], [34] and [16], the earlier weaker versions of our above results were applied to algebraic numbers and algebraic integers, respectively. Restricting ourselves to irreducible binary forms and following the corresponding arguments of [29], [32], [34] and [16], it is easy to deduce improved versions of the former effective estimates concerning algebraic numbers. We present such a consequence of Theorem 3.

Two algebraic numbers α, α^* are called *O_K-equivalent* if there is a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(O_K)$ such that $\alpha^* = (a\alpha + b)(c\alpha + d)^{-1}$. To every algebraic number α of degree n over K we associate the binary form

$$F_\alpha(x,y) = \prod_{i=1}^{n} \left(x - \alpha^{(i)} y \right),$$

where $\alpha^{(1)} = \alpha$, $\alpha^{(2)}, \dots, \alpha^{(n)}$ denote the conjugates of α over K. It is easy to check that α, α^* are O_K-equivalent if and only if F_α and F_{α^*} are weakly O_K-equivalent. The *O_K-discriminant* of α is defined by $\mathbf{d}(\alpha) = \mathbf{d}(F_\alpha)$. Thus, O_K-equivalent numbers have the same O_K-discriminant (cf. [16], Section 3).

The next corollary follows immediately from Theorem 3 with the choice $q = 1$, using Lemma 1, (vi) of [16].

Corollary 5. *Let L/K be a finite extension of degree $n \geq 3$. Then every α with $L = K(\alpha)$ and $\mathbf{d}(\alpha) = \mathbf{d}$ is O_K-equivalent to an α^* for which*[3]

$$h(\alpha^*) \leq \exp\left\{ (c_{37} dn)^{c_{38} dn^4} |D_L|^{2n^3} \left(|D_L|^{2n^3} + \log N_{K/\mathbb{Q}}(\mathbf{d}) \right) \right\}, \qquad (21)$$

where c_{37}, c_{38} are effectively computable positive absolute constants.

This is an improvement of the case $S = S_\infty$ of Corollary 6, (ii) in [16]. For algebraic integers α, Corollary 6 in [34] gives a stronger result. It implies that there are $a \in O_K^*$ and $b \in O_K$ such that the height of $\alpha^* = a\alpha + b$ is bounded above by an expression which is of similar shape but better than that in (21). For $K = \mathbb{Q}$, an even better bound is given in Corollary 1 of [35].

Our Corollary 5 has been recently applied by Evertse [13] to distances between the conjugates of an algebraic number. We note that in [29], [32], [34] and [16] there are other consequences and applications as well of the earlier versions of our Theorems 1, 2 and 3, e.g. to the minimal non-zero values of binary forms at integral points. These results can also be improved by means of our theorems.

[3] *Added in proof.* Recently we have improved the first and second exponents of $|D_L|$ to $4n$ and $2(n-1)$, respectively.

5. Proofs

Keeping the notation of the preceding section, let again K denote an algebraic number field with degree d, and denote by M_K the set of places on K. For every place v we choose a valuation $|\cdot|_v$ in the usual way: if v is infinite and corresponds to $\sigma : K \to \mathbb{C}$, then we put, for $\alpha \in K$, $|\alpha|_v = |\sigma(\alpha)|^{d_v}$, where $d_v = 1$ or 2 according as $\sigma(K)$ is contained in $\mathbb{R}$ or not; if v is a finite place corresponding to the prime ideal $\mathbf{p}$ in K, then we put $|\alpha|_v = N(\mathbf{p})^{\mathrm{ord}_{\mathbf{p}}\alpha}$ for $\alpha \in K \setminus \{0\}$, and $|0|_v = 0$. Here, for $\alpha \neq 0$, $\mathrm{ord}_{\mathbf{p}}\alpha$ denotes the exponent to which $\mathbf{p}$ divides the principal fractional ideal (α). The absolute height $h(\alpha)$ of $\alpha \in K$ is defined by

$$h(\alpha) = \prod_{v \in M_K} \max\left(1, |\alpha|_v^{1/d}\right).$$

It depends only on α, and not on the choice of the number field K containing α. We note that if α is an algebraic number of degree n then

$$2^{1-n} H(\alpha) \leq (h(\alpha))^n \leq \sqrt{n+1} H(\alpha),$$

where $H(\alpha)$ denotes the ordinary height of α, that is the height of the minimal polynomial of α over $\mathbb{Z}$. For this and other properties of the height $h(\alpha)$, we refer to [19].

The first lemma plays a crucial role in our proofs.

Lemma 1. *Let $N > 1$, and let x_1, x_2, x_3 be non-zero S-integers in K such that*

$$x_1 + x_2 + x_3 = 0 \tag{22}$$

and $N_S(x_i) \leq N$ for $i = 1, 2, 3$. Then

$$\max_{i,j} h\left(x_i / x_j\right) \leq \exp\left\{c_{39} c_{40}^t P W\left(\log^* N\right)\right\},$$

where c_{39} and c_{40} are effectively computable positive constants which depend only on d and D_K.

This is a significant improvement in terms of t of Lemma 6 in [27] and the Corollary in [7].

Denote by h_K and R_K the class number and regulator of K, respectively.

Proof of Lemma 1. The lemma is an immediate consequence of Corollary 1 in Győry and Yu [36]. Its proof depends on recent estimates of Matveev [42] and Yu [41] concerning linear forms in logarithms of algebraic numbers. In [36], the corresponding constants c_{39}, c_{40} depend on d, h_K and R_K, but as is well-known (see e.g. Lemma 8 in [16] and the references given there),

$$\max\{h_K, R_K\} \leq c_{41}|D_K|^{1/2} \left(\log^* |D_K|\right)^{d-1}, \tag{23}$$

where c_{41} is an effectively computable positive absolute constant. □

Proof of Theorem 1. We follow the proof of Theorem 2′ of [16] with the following modifications. We replace Lemma 11 in [16] by our Lemma 1 above. Further, in our Theorem 1 only the splitting field M of F is fixed, while in [16] F is associated to a system of fields $(M_1, \dots, M_q)$. In [16], the corresponding bound obtained for $h(F^*)$ depends on $|D_{M_1} \dots D_{M_q}|$. However, $D_{M_i}|D_M$ for each i. Hence, in view of $q \leq n$, we infer that

$$|D_{M_1} \dots D_{M_q}| \leq |D_M|^n. \tag{24}$$

We note that conversely, by a result of Stark [52] we have

$$|D_M| \leq |D_K|^m |D_{M_1} \dots D_{M_q}|^{md}.$$

Following now the arguments of [16] and using (24), the estimate (13) follows. □

We now turn to the proof of Theorem 2. $C_1, \dots, C_{10}$ will denote expressions of the same form as the upper bound in Theorem 2, but with other effectively computable numbers instead of c_{13}, c_{14}.

Proof of Theorem 2. Consider first the general case when $F \in O_S[x, y]$ is any binary form with $D(F) \in \delta O_S^*$ and with splitting field M over K. Then (14) can be deduced from our Theorem 1 in a similar way as Theorem 3′ was derived from Theorem 2′ in [16]. We have to make in the proof of Theorem 3′ of [16] the following modifications only. We proceed now with a matrix U which is contained in $GL_2(O_S)$, and not necessarily in $SL_2(O_S)$. In the last step of the proof we infer that $G_U = \varepsilon F$, where $\varepsilon \in O_S^*$ and $h(G) \leq C_1$. By Lemma 10 of [16] we can write $\varepsilon = \varepsilon_1 \varepsilon_2^n$

with $\varepsilon_1, \varepsilon_2 \in O_S^*$ such that $h(\varepsilon_1) \leq C_2$. Putting now $F^* = \varepsilon_1^{-1} G$ and $A = \varepsilon_2 U^{-1}$ we obtain that $A \in GL_2(O_S)$, $F^* = F_A$ and $h(F^*) \leq C_3$ which proves Theorem 2 in the general case.

Consider now the monic case. There is no direct proof in the literature for this case even with weaker bound for $h(F^*)$. Hence we shall outline the proof of (14).

By assumption $D(F) \in \delta O_S^*$, hence $N_S(D(F)) = N_S(\delta)$. Using again Lemma 10 of [16], we infer that there is an $\varepsilon \in O_S^*$ such that $h\left(\varepsilon^{n(n-1)} D(F)\right) \leq C_4$. Putting

$$G(x, y) = F(x, \varepsilon y),$$

we have

$$h(D(G)) \leq C_5. \tag{25}$$

Let $\gamma_1, \ldots, \gamma_n$ be the zeros of $G(x, 1)$, and T the set of places on M lying above the places of S. Then it follows from

$$D(G) = \prod_{1 \leq i < j \leq n} (\gamma_i - \gamma_j)^2 \tag{26}$$

that

$$N_T(\gamma_i - \gamma_j) \leq N_T(\delta)^{1/2} = N_S(\delta)^{n/2}$$

for each distinct i, j. Further,

$$(\gamma_i - \gamma_j) + (\gamma_j - \gamma_k) + (\gamma_k - \gamma_i) = 0$$

for any distinct i, j, k. By applying now Lemma 1 it follows that

$$h\left(\frac{\gamma_1 - \gamma_i}{\gamma_1 - \gamma_2}\right) \leq C_6, \quad h\left(\frac{\gamma_1 - \gamma_j}{\gamma_1 - \gamma_2}\right) \leq C_6$$

for $i \neq j$. This implies that

$$h\left(\frac{\gamma_i - \gamma_j}{\gamma_1 - \gamma_2}\right) \leq C_7 \tag{27}$$

for every distinct i, j, whence, in view of (26), $h(\gamma_1 - \gamma_2) \leq C_8$ follows. Finally, together with (27) this gives

$$h(\gamma_i - \gamma_j) \leq C_9$$

for each distinct i, j. Write $x_i = \gamma_i - \gamma_1$ for $i = 1, \ldots, n$. Following the arguments of the second part of the proof of Theorem 3 in [34] and using the fact that D_K divides D_M, we deduce again that $h\left(F^*\right) \leq C_{10}$. □

To prove Theorem 3, we need a more explicit version of Lemma 1 in the special case $S = S_\infty$.

Lemma 2. *Let $N > 1$, and let x_1, x_2, x_3 be non-zero integers in K with $|N_{K/\mathbb{Q}}(x_i)| \leq N$ for $i = 1, 2, 3$, which satisfy* (22). *Then*

$$\max_{i,j} h\left(x_i/x_j\right) \leq \exp\left\{(c_{42}d)^{c_{43}d} R_K \left(\log^* R_K\right)\left(R_K + \log N\right)\right\},$$

where c_{42}, c_{43} are effectively computable positive absolute constants.

Proof. This is an immediate consequence of the Corollary in [7], where c_{42}, c_{43} are given explicitly. For the best known values of c_{42} and c_{43}, see [36]. □

We shall use the following consequence of Lemma 2.

Lemma 3. *Let x_1, x_2, x_3 be as in Lemma 2, and let $\varepsilon > 0$. Then*

$$\max_{i,j} h\left(x_i/x_j\right) \leq \exp\left\{(c_{44}d/\varepsilon)^{c_{45}d} |D_K|^{1/2+\varepsilon}\left(|D_K|^{1/2} + \log N\right)\right\},$$

with effectively computable positive absolute constants c_{44}, c_{45}.

Proof. Lemma 3 follows from Lemma 2 and (23) in the same way as Lemma 11 was deduced in [16] from Lemma 6 of [27] and (23) above. □

Proof of Theorem 3. In the proof of Theorem $2'$ of [16] it is enough to replace Lemma 11 of [16] by our Lemma 3, and the assertion follows as in [16]. □

Proof of Corollary 1. $C_{11}, \ldots, C_{13}$ will denote expressions of the same form as the upper bound in (15), but with other effectively computable numbers instead of c_{17}, c_{18}. By assumption $D(F) = \delta$. Further, $N_S(\delta) \leq h(\delta)$. Thus, by Theorem 2, $G_A = F$ for some $A \in GL_2(O_S)$ and $G \in O_S[x, y]$ with $h(G) \leq C_{11}$. It follows from $D(G)\,(\det A)^{n(n-1)} = \delta$ that $h(\det A) \leq C_{12}$. Now Lemma 7 of [16] implies that there is a $U \in SL_2(O_S)$ such that $h(AU) \leq C_{13}$. Then, for $F_U = G_{AU}$, (15) follows.

Suppose now that F is monic. Then the above A is of the form $\begin{pmatrix} 1 & -b \\ 0 & d \end{pmatrix}$ with some $b \in O_S$, $d \in O_S^*$. Further, the above argument gives that $F = G(x+by, dy)$, $h(G) \leq C_{11}$ and $h(d) \leq C_{12}$. Putting $U = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, we infer that $h(AU) \leq C_{13}$ and we obtain again (15) for $F_U = G_{AU}$. □

Proof of Corollary 2. Corollary 2 follows from Corollary 1 in the same way as in [34] Corollary 4 was deduced from Theorem 3. The bound so obtained for $h(F^*)$ depends also on the regulator and class number of M, but the use of (23) completes the proof. □

Proof of Corollary 3. $c_{46}, \dots, c_{51}$ denote effectively computable positive numbers which depend at most on K, S, M and n. Let $F \in K[x, y]$ and T, P, ω, N have the same meaning as in the statement of Corollary 3. Note that $\mathbf{d}_T(F) = (1)_T$. By Theorem 1, F is weakly O_T-equivalent to a binary form $F^* \in K[x, y]$ for which

$$h(F^*) \leq \exp\left\{c_{46}^{\omega+1} P^m \left(\log^* P\right)^{\omega m}\right\} \leq \exp\left\{c_{47} \left(P \left(\log^* P\right)^{\omega}\right)^{c_{48}}\right\}.$$

But, by Lemma 3 of [16] we have $N_S\left(\mathbf{d}_S\left(F^*\right)\right) \leq c_{49} h(F^*)^{c_{50}}$. Further, by assumption F has minimal S-discriminant, hence $N_S\left(\mathbf{d}_S\left(F\right)\right) \leq N_S\left(\mathbf{d}_S\left(F^*\right)\right)$ and (17) follows.

For $\omega \leq \log P / \log_2 P$, (18) is an immediate consequence of (17). In the remaining case we use $\omega \leq c_{51} P / \log P$ and (17) implies again the corresponding inequality in (18). □

Proof of Corollary 4. Let F, N, P and ω be as in Corollary 4. Denote by $\mathbf{p_1}, \dots, \mathbf{p}_\omega$ the distinct prime ideal divisors of $D(F)$ in O_K, and let $S = S_\infty \cup \{\mathbf{p_1}, \dots, \mathbf{p}_\omega\}$, $\mathcal{S} = O_K \cap O_S^*$. By Corollary 2, there are $F^* \in O_K[x, y]$ and $A = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with $b \in O_K$, $d \in \mathcal{S}$ such that $F = F_A^*$ and (16) hold with the choice $\delta = 1$ and $t = \omega$. The form F has, by assumption, minimal discriminant in monic sense, hence we obtain that

$$|N_{K/\mathbb{Q}}(D(F))| \leq |N_{K/\mathbb{Q}}(D(F^*))|. \tag{28}$$

Further, we have

$$|N_{K/\mathbb{Q}}(D(F^*))| \leq c_{52} h(F^*)^{c_{53}} \tag{29}$$

with effectively computable c_{52}, c_{53} which depend only n. Now (16), (28) and (29) imply (19). The estimates in (20) easily follow from (19). □

References

[1] F. Beukers and H. P. Schlickewei, The equation $x+y=1$ in finitely generated groups, *Acta. Arith.* **78** (1996), 189–199.

[2] A. Bérczes, On the number of solutions of index form equations, *Publ. Math. Debrecen* **56** (2000), 251–262.

[3] A. Bérczes, J. H. Evertse and K. Győry, On the number of equivalence classes of binary forms of given degree and given discriminant, *Acta. Arith.* **113** (2004), 363–399.

[4] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given disriminant, *Proc. London Math. Soc.* **24** (1972), 385–394.

[5] B. Brindza, On large values of binary forms, *Rocky Mountain J. Math.* **26** (1996), 839–845.

[6] B. Brindza, J. H. Evertse and K. Győry, Bounds for the solutions of some diophantine equations in terms of discriminants, *J. Austral. Math. Soc. Ser. A* **51** (1991), 8–26.

[7] Y. Bugeaud and K. Győry, Bounds for the solutions of unit equations, *Acta Arith.* **74** (1996), 67–80.

[8] B. N. Delone (Delaunay), Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante, *Math. Z.* **31** (1930), 1–26.

[9] B. N. Delone and D. K. Faddeev, The theory of irrationalities of the third degree, *Amer. Math. Soc., Providence* (1964), (translated from the Russian (1940) edn.).

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

[11] J. H. Evertse, Estimates for reduced binary forms, *J. Reine Angew. Math.* **434** (1993), 159–190.

[12] J. H. Evertse, The number of solutions of decomposable form equations, *Invent. Math.* **122** (1995), 559–601.

[13] J. H. Evertse, Distances between the conjugates of an algebraic number, *Publ. Math. Debrecen* **65** (2004), 323–340.

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

[15] J. H. Evertse and K. Győry, On the number of polynomials and integral elements of given discriminant, *Acta. Math. Hung.* **51** (1988), 341–362.

[16] J. H. Evertse and K. Győry, Effective finiteness results for binary forms with given discriminant, *Compositio Math.* **79** (1991), 169–204.

[17] J. H. Evertse and K. Győry, Effective finiteness theorems for decomposable forms of given discriminant, *Acta. Arith.* **60** (1992), 233–277.

[18] J. H. Evertse and K. Győry, The number of families of solutions of decomposable form equations, *Acta. Arith.* **80** (1997), 367–394.

[19] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, S-unit equations and their applications, in: New Advances in Transcendence Theory, (A. Baker, ed.), *Cambridge*, 1988, 110–174.

[20] I. Gaál, Inhomogeneous discriminant form and index form equations and their applications, *Publ. Math. Debrecen* **33** (1986), 1–12.

[21] I. Gaál, Integral elements with given discriminant over function fields, *Acta. Math. Hung.* **52** (1988), 133–146.

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

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

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

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

[26] K. Győry, On polynomials with integer coefficients and given discriminant V, $\mathfrak{p}$-adic generalizations, *Acta Math. Acad. Sci. Hung.* **32** (1978), 175–190.

[27] K. Győry, On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.* **54** (1979), 583–600.

[28] K. Győry, Résultats effectifs sur la représentation des entiers par des formes désomposables, Queen's Papers in Pure and Applied Math., No. 56, *Kingston, Canada*, 1980.

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

[30] 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.

[31] K. Győry, On the irreducibility of a class of polynomials III, *J. Number Theory* **15** (1982), 164–181.

[32] 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.

[33] K. Győry, Upper bounds for the degrees of decomposable forms of given discriminant, *Acta. Arith.* **66** (1994), 261–268.

[34] K. Győry, Bounds for the solutions of decomposable form equations, *Publ. Math. Debrecen* **52** (1998), 1–31.

[35] K. Győry, Discriminant form and index form equations, In "Algebraic Number Theory and Diophantine Analysis", *Walter de Gruyter, Berlin – New York*, 2000, 191–214.

[36] K. Győry and Kunrui Yu, Bounds for the solutions of unit equations and decomposable form equations, *Acta Arith.* **123** (2006), 9–41.

[37] K. Győry and Z. Z. Papp, On discriminant form and index form equations, *Studia Sci. Math. Hungar.* **12** (1977), 47–60.

[38] K. Győry, I. Pink and Á. Pintér, Power values of polynomials and binomial Thue–Mahler equations, *Publ. Math. Debrecen* **65** (2004), 342–362.

[39] J. Haristoy, Équations diophantiennes exponentielles, Thèse de docteur, *Strasbourg*, 2003.

[40] B. Kovács, Canonical number systems in algebraic number fields, *Acta Math. Acad. Sci. Hungar.* **37** (1981), 405–407.

[41] Kunrui Yu, p-adic logarithmic forms and group varieties III (*to appear*).

[42] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II, *Izvestiya: Mathematics* **64** (2000), 1217–1269.

[43] T. Nagell, Zur Theorie der kubischen Irrationalitäten, *Acta Math.* **55** (1930), 33–65.

[44] T. Nagell, Sur les discriminants des nombres algébriques, *Arkiv för Mat.* **7** (1967), 265–282.

[45] T. Nagell, Quelques propriétés des nombres algébriques du quatrième degré, *Arkiv för Mat.* **7** (1968), 517–525.

[46] J. Nakagawa, Binary forms and orders of algebraic number fields, *Invent. Math.* **97** (1989), 219–235.

[47] A. Pethő, On the greatest prime factor and divisibility properties of linear recursive sequences, *Indag. Math. (N.S.)* **1** (1990), 85–93.

[48] Á. Pintér, On the magnitude of integer points on elliptic curves, *Bull. Austral. Math. Soc.* **52** (1995), 195–199.

[49] P. Ribenboim, Finite sets of binary forms, *Publ. Math. Debrecen* **68** (2006), 261–282.

[50] A. Shlapentokh, Polynomials with a given discriminant over fields of algebraic functions of positive characteristic, *Pacific J. Math.* **173** (1996), 533–555.

[51] D. Simon, The index of nonmonic polynomials, *Indag. Math. (N.S)* **12** (2001), 505–517.

[52] H. M. Stark, Some effective cases of the Brauer–Siegel theorem, *Invent. Math.* **23** (1974), 135–152.

[53] C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations, *J. Amer. Math. Soc.* **4** (1991), 793–835.

[54] J. L. Thunder, On Thue ineuqalities and a conjecture of Schmidt, *J. Number Theory* **52** (1995), 319–328.

[55] L. A. Trelina, On the greatest prime factor of an index form, *Dokl. Akad. Nauk BSSR* **21** (1977), 975–976.

[56] L. A. Trelina, Representation of powers by polynomials in algebraic number fields, *Dokl. Akad. Nauk BSSR* **29** (1985), 5–8 (in *Russian*).

KÁLMÁN GYŐRY
UNIVERSITY OF DEBRECEN
INSTITUTE OF MATHEMATICS
NUMBER THEORY RESEARCH GROUP OF THE
HUNGARIAN ACADEMY OF SCIENCES
H-4010, DEBRECEN, P. O. BOX 12
HUNGARY

E-mail: gyory@math.klte.hu

(Received April 12, 2006)