COMPOSITIO MATHEMATICA

J. H. EVERTSE
K. GYÖRY

Lower bounds for resultants, I

Compositio Mathematica, tome 88, nº 1 (1993), p. 1-23
<http://www.numdam.org/item?id=CM_1993__88_1_1_0>

Compositio Mathematica **88**: 1–23, 1993.

Lower bounds for resultants, I

J. H. EVERTSE[1] and K. GYŐRY[2]

To Professor P. Erdős on his 80th birthday

[1]*Department of Mathematics and Computer Science, University of Leiden, P.O. Box 9512, 2300 RA Leiden, The Netherlands;* [2]*Mathematical Institute, Kossuth Lajos University, 4010 Debrecen, Hungary*

Received 3 August 1992; accepted 25 February 1993

1. Introduction

The *resultant* of two binary forms $F(X, Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$ and $G(X, Y) = b_0X^s + b_1X^{s-1}Y + \cdots + b_sY^s$ is defined by the determinant

$$R(F, G) = \begin{vmatrix} a_0 & \cdots & a_r & & & \mathbf{0} \\ & a_0 & \cdots & a_r & & \\ \mathbf{0} & & \ddots & & \ddots & \\ & & & a_0 & \cdots & a_r \\ b_0 & b_1 & \cdots & b_s & \mathbf{0} & \\ \mathbf{0} & \ddots & & & \ddots & \\ & & b_0 & b_1 & \cdots & b_s\,. \end{vmatrix}$$

where the first s rows consist of coefficients of F, and the last r rows of coefficients of G. If

$$F(X, Y) = \prod_{i=1}^{r} (\alpha_i X - \beta_i Y), \qquad G(X, Y) = \prod_{j=1}^{s} (\gamma_j X - \delta_j Y)$$

then

$$R(F, G) = \prod_{i=1}^{r} \prod_{j=1}^{s} (\alpha_i \delta_j - \beta_i \gamma_j). \tag{1.1}$$

[1]Research made possible by a fellowship of the Royal Netherlands Academy of Arts and Sciences (K.N.A.W.).
[2]Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

For a matrix $U=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, put $F_U(X, Y)=F(aX+bY, cX+dY)$ and define G_U similarly. The following properties of resultants are well-known:

$$\left.\begin{aligned}
&R(\lambda F, \mu G)=\lambda^s\mu^r R(F, G);\ R(F_U, G_U)=(\det U)^{rs}R(F, G);\\
&R(F_1F_2, G)=R(F_1, G)R(F_2, G) \text{ for binary forms } F_1, F_2, G;\\
&R(G, F)=(-1)^{rs}R(F, G);\\
&R(F, G+HF)=R(F, G) \quad \text{if } r \leqslant s \text{ and } H \text{ is a binary form}\\
&\qquad\qquad\qquad\qquad\qquad \text{with } \deg H=s-r.
\end{aligned}\right\} \tag{1.2}$$

The discriminant of $F(X, Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r = \Pi_{i=1}^r(\alpha_iX-\beta_iY)$ is equal to

$$D(F) = \prod_{1\leqslant i<j\leqslant r} (\alpha_i\beta_j-\alpha_j\beta_i)^2. \tag{1.3}$$

$D(F)$ is a homogeneous polynomial of degree $2r-2$ in $\mathbb{Z}[a_0, \ldots, a_r]$. From (1.3) it follows that for every $\lambda \neq 0$ and non-singular matrix $U=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$D(\lambda F)=\lambda^{2r-2}D(F), \qquad D(F_U)=(\det U)^{r(r-1)}D(F). \tag{1.4}$$

In this paper we derive, for binary forms $F, G \in \mathbb{Z}[X, Y]$, lower bounds for $|R(F, G)|$ in terms of $|D(F)|$ and $|D(G)|$. If $F(X, Y)$ is a binary form with coefficients in a field K, then the *splitting field* of F over K is the smallest extension of K over which F can be factored into linear forms. We call F *square-free* if it is not divisible by the square of a linear form over its splitting field. Hence F is square-free if and only if it has non-zero discriminant. By $C_i^{\text{ineff}}(\ldots)$ we denote positive numbers, depending only on the parameters between the parentheses, which cannot be computed effectively from our method of proof.

THEOREM 1. *Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $r \geqslant 3$ and $G \in \mathbb{Z}[X, Y]$ a binary form of degree $s \geqslant 3$ such that FG has splitting field L over $\mathbb{Q}$, and FG is square-free. Then for every $\varepsilon > 0$ we have*

$$|R(F, G)| \geqslant C_1^{\text{ineff}}(r, s, L, \varepsilon)(|D(F)|^{s/(r-1)}|D(G)|^{r/(s-1)})^{1/17-\varepsilon}.$$

The exponent 1/17 is probably far from best possible. Since $R(F, G)$ has degree s in the coefficients of F and degree r in the coefficients of G, whereas $D(F)$ has degree $2r-2$ in the coefficients of F and $D(G)$ has degree $2s-2$ in the coefficients of G, 1/17 cannot be replaced by a number larger than 1/2. In case that both F

and G are *monic*, i.e. $F(1,0)=1$, $G(1,0)=1$, we can obtain a better lower bound for $|R(F, G)|$. Also, in this case the proof is easier.

THEOREM 2. *Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $r \geqslant 2$ and $G \in \mathbb{Z}[X, Y]$ a binary form of degree $s \geqslant 3$ such that $F \cdot G$ has splitting field L over $\mathbb{Q}$, FG is square-free and $F(1,0)=1$, $G(1,0)=1$. Then for every $\varepsilon > 0$ we have*

$$|R(F, G)| \geqslant C_2^{\text{ineff}}(r, s, L, \varepsilon)\{\max(|D(F)|^{s/(r-1)}, |D(G)|^{r/(s-1)})\}^{1/6-\varepsilon}.$$

In Section 2 we shall show that the dependence of C_1, C_2 on the splitting field L and the conditions concerning r and s in Theorems 1 and 2 are necessary.

We shall get Theorems 1 and 2 as special cases of more general results (cf. Theorems 1A and 2A in Section 2) concerning binary forms with coefficients in the ring of S-integers of an arbitrary algebraic number field. In Section 3 we state and prove some applications of our main results. Namely, we derive a semi-quantitative version (cf. Corollaries 3, 4) of a result of Evertse and Győry ([4], Theorem 2(i)) on Thue-Mahler equations. Further, we deduce some extensions and generalizations (cf. Corollaries 1, 2) of a result of Győry ([9], Theorem 7, algebraic number field case) on resultant equations. We note that recently Győry [10] has obtained some other generalizations as well as a quantitative version of our Corollary 2 on monic binary forms.

Our main results are proved in Sections 4 and 5. The main tools in our arguments are some results (cf. Lemma 2) of Evertse [3] and Laurent [11] whose proofs are based on Schlickewei's p-adic generalization [12] of the Subspace Theorem of Schmidt (see e.g. [14]). Therefore, our inequalities are not completely effective, but 'semi-effective', in the sense that they include ineffective constants.

2. Main results

We now state our generalizations over number fields. We first introduce normalized absolute values. Let K be an algebraic number field of degree d. Denote by $\sigma_1, \ldots, \sigma_{r_1}$ the embeddings $K \hookrightarrow \mathbb{R}$ and by $\{\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}\}, \ldots, \{\sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}\}$ the pairs of complex conjugate embeddings $K \hookrightarrow \mathbb{C}$. If v is the infinite place corresponding to σ_i $(i = 1, \ldots, r_1)$ then put

$$|x|_v = |\sigma_i(x)|^{1/d} \quad \text{for } x \in K;$$

if v is the infinite place corresponding to $\{\sigma_i, \bar{\sigma}_i\}$ $(i = r_1+1, \ldots, r_1+r_2)$ then put

$$|x|_v = |\sigma_i(x)|^{2/d} \quad \text{for } x \in K;$$

and if v is the finite place corresponding to the prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K then put

$$|x|_v = (N(\mathfrak{p}))^{-\mathrm{ord}_{\mathfrak{p}}(x)/d} \quad \text{if } x \neq 0; \ |0|_v = 0,$$

where $N(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p})$ is the norm of $\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(x)$ is the exponent of $\mathfrak{p}$ in the unique prime ideal decomposition of the ideal generated by x. Denote by $\mathbb{M}_K$ the set of all infinite and finite places of K. The set of absolute values $\{|\,.\,|_v : v \in \mathbb{M}_K\}$ just defined satisfies the *Product Formula*

$$\prod_{v \in \mathbb{M}_K} |x|_v = 1 \quad \text{for } x \in K^*$$

and the *Extension Formulas*

$$\prod_{w|v} |x|_w = |N_{L/K}(x)|_v^{1/[L:K]} \text{ for } x \in L, \quad \prod_{w|v} |x|_w = |x|_v \text{ for } x \in K,$$

where $v \in \mathbb{M}_K$, L is a finite extension of K, and w runs through the places on L lying above v.

Each finite subset of $\mathbb{M}_K$ we consider contains by convention all infinite places on K. Let S be such a finite set of places. Define the ring of S-integers and the group of S-units by

$$\mathcal{O}_S = \{x \in K : |x|_v \leqslant 1 \text{ for all } v \in \mathbb{M}_K \backslash S\}$$

and

$$\mathcal{O}_S^* = \{x \in K : |x|_v = 1 \text{ for all } v \in \mathbb{M}_K \backslash S\},$$

respectively. For $x \in K$ we put

$$|x|_S := \prod_{v \in S} |x|_v.$$

Note that $|x|_S \geqslant 1$ if $x \in \mathcal{O}_S \backslash \{0\}$ and $|x|_S = 1$ if $x \in \mathcal{O}_S^*$. If L is a finite extension of K and T is the set of places on L lying above those in S, then $\mathcal{O}_T$ is the integral closure of $\mathcal{O}_S$ in L. Further, $|\,.\,|_T$ is defined similarly as $|\,.\,|_S$ and by the Extension Formulas we have

$$|x|_T = |N_{L/K}(x)|_S^{1/[L:K]} \quad \text{for } x \in L; \qquad |x|_T = |x|_S \quad \text{for } x \in K. \tag{2.1}$$

We can now state the generalizations of Theorems 1 and 2.

THEOREM 1A. *Let $F, G \in \mathcal{O}_S[X, Y]$ be binary forms such that*

$$\begin{array}{l}\deg F = r \geqslant 3, \deg G = s \geqslant 3, \\ FG \textit{ has splitting field } L \textit{ over } K, \textit{ and } FG \textit{ is square-free.}\end{array} \tag{2.2}$$

Then for every $\varepsilon > 0$ we have

$$|R(F, G)|_S \geqslant C_3^{\text{ineff}}(r, s, S, L, \varepsilon)(|D(F)|_S^{s/(r-1)} |D(G)|_S^{r/(s-1)})^{1/17-\varepsilon}. \tag{2.3}$$

THEOREM 2A. *Let $F, G \in \mathcal{O}_S[X, Y]$ be binary forms such that*

$$\begin{array}{l}\deg F = r \geqslant 2, \deg G = s \geqslant 3, F(1, 0) = 1, G(1, 0) = 1, \\ FG \textit{ has splitting field } L \textit{ over } K, \textit{ and } FG \textit{ is square-free}\end{array} \tag{2.4}$$

Then for every $\varepsilon > 0$ we have

$$|R(F, G)|_S \geqslant C_4^{\text{ineff}}(r, s, S, L, \varepsilon)\{\max(|D(F)|_S^{s/(r-1)}, |D(G)|_S^{r/(s-1)})\}^{1/6-\varepsilon}.$$

Theorems 1 and 2 follow at once from Theorems 1A and 2A, respectively, by taking $K = \mathbb{Q}$, and for S the only infinite place on $\mathbb{Q}$.

REMARK 1. The dependence on L of C_1, C_2, C_3 and C_4 is necessary. Indeed, let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a monic binary form of degree r, suppose that $s \geqslant r$, and put $G(X, Y) = F(X, Y)X^{s-r} + Y^s$. We can choose F with $|D(F)|$ arbitrarily large such that $F \cdot G$ is square-free. On the other hand, from (1.2) it follows that

$$\begin{aligned} R(F, G) &= R(F, FX^{s-r} + Y^s) = R(F, Y^s) = R(F, Y)^s \\ &= R(X^r + Y(\ldots), Y)^s = R(X, Y)^{rs} = 1. \end{aligned}$$

REMARK 2. The conditions $r \geqslant 3$, $s \geqslant 3$ in Theorems 1 and 1A are necessary. For instance, take $F(X, Y) = XY$. Let θ be an algebraic unit, put $M = \mathbb{Q}(\theta)$, and denote by $\theta_1, \ldots, \theta_s$ the conjugates of θ over $\mathbb{Q}$. Put $G_n(X, Y) = (X - \theta_1^n Y) \cdots (X - \theta_s^n Y)$ for $n \in \mathbb{Z}$. Thus, FG_n is square-free and has splitting field $\mathbb{Q}(\theta_1, \ldots, \theta_s)$. Further,

$$\begin{aligned} |R(F, G_n)| &= |R(X, G_n) R(Y, G_n)| \\ &= |G_n(0, 1) G_n(1, 0)| = |N_{M/\mathbb{Q}}(\theta)|^n = 1 \end{aligned}$$

for $n \in \mathbb{Z}$. But it follows from Győry ([7], Corollaire 1) that $\lim_{n \to \infty} |D(G_n)| = \infty$.

REMARK 3. The conditions $r \geqslant 2$, $s \geqslant 3$ in Theorems 2 and 2A are necessary.

For instance, let d be a positive integer which is not a square. For all $u, v \in \mathbb{Z}$ with $u^2 - dv^2 = 1$, define $F_u(X, Y) = X^2 - u^2Y^2$, $G_v(X, Y) = X^2 - dv^2Y^2$. Then $R(F_u, G_v) = (u^2 - dv^2)^2 = 1$, F_uG_v is square-free, F_uG_v has splitting field $\mathbb{Q}(\sqrt{d})$, $D(F_u) = 4u^2$, $D(G_v) = 4dv^2$, and hence $|D(F_u)|$, $|D(G_v)|$ can be arbitrarily large.

REMARK 4. For certain applications, the following technical variation on Theorem 1A might be useful.

By an $\mathcal{O}_S$-ideal we mean a finitely generated $\mathcal{O}_S$-submodule of K and by an integral $\mathcal{O}_S$-ideal, an $\mathcal{O}_S$-ideal contained in $\mathcal{O}_S$. The $\mathcal{O}_S$-ideal generated by $x_1, \ldots, x_k$ is denoted by $(x_1, \ldots, x_k)_S$. If $P \in K[X_1, \ldots, X_m]$ then $(P)_S$ denotes the $\mathcal{O}_S$-ideal generated by the coefficients of P. For $x \in K^*$, there is a unique $\mathcal{O}_K$-ideal $\mathfrak{a}^*$ composed of $\mathcal{O}_K$-prime ideals outside S, such that $(x)_S = \mathfrak{a}^*\mathcal{O}_S$. Then we have (see e.g. [4] or [5]) $|x|_S = |(x)_S|_S = N(\mathfrak{a}^*)^{1/d}$. More generally, if $\mathfrak{a}$ is an $\mathcal{O}_S$-ideal and $\mathfrak{a}^*$ is the $\mathcal{O}_K$-ideal composed of prime ideals outside S such that $\mathfrak{a} = \mathfrak{a}^*\mathcal{O}_S$, we put $|\mathfrak{a}|_S = N(\mathfrak{a}^*)^{1/d}$. For a binary form $F \in K[X, Y]$ of degree r we define the *discriminant $\mathcal{O}_S$-ideal* (cf. [5]) by

$$\mathscr{D}_S(F) = (D(F))_S/(F)_S^{2r-2},$$

and for binary forms $F, G \in K[X, Y]$ of degrees r, s, respectively, we define the *resultant $\mathcal{O}_S$-ideal* by

$$\mathscr{R}_S(F, G) = (R(F, G))_S/(F)_S^s(G)_S^r.$$

Note that $\mathscr{D}_S(F)$, $\mathscr{R}_S(F, G)$ are integral $\mathcal{O}_S$-ideals. Further, by (1.2), (1.4), $\mathscr{D}_S(\lambda F) = \mathscr{D}_S(F)$, $\mathscr{R}_S(\lambda F, \mu G) = \mathscr{R}_S(F, G)$ for λ, $\mu \in K^*$. Now suppose that $F, G \in K[X, Y]$ are binary forms satisfying (2.2). Then for all $\varepsilon > 0$,

$$|\mathscr{R}_S(F, G)|_S \geqslant C_S^{\text{ineff}}(r, s, S, L, \varepsilon)(|\mathscr{D}_S(F)|_S^{s/(r-1)} \cdot |\mathscr{D}_S(G)|_S^{r/(s-1)})^{1/17-\varepsilon}. \tag{2.5}$$

This can be derived from (2.3) as follows. We can choose $\lambda, \mu \in K^*$ with

$$\lambda \in (F)_S^{-1}, \quad |\lambda|_S \leqslant C_K|(F)_S^{-1}|_S$$

and

$$\mu \in (G)_S^{-1}, \quad |\mu|_S \leqslant C_K|(G)_S^{-1}|_S,$$

where C_K is some constant depending only on K (cf. [5], Lemma 4). Put $F' = \lambda F$, $G' = \mu G$. Then $F', G' \in \mathcal{O}_S[X, Y]$. Further, $1 \leqslant |(F')_S|_S$, $|(G')_S|_S \leqslant C_K$ (see [4], Section 4). Therefore,

$$|\mathscr{R}_S(F, G)|_S = |\mathscr{R}_S(F', G')|_S \geqslant C_K^{-r-s}|R(F', G')|_S$$

and

$$|\mathscr{D}_S(F)|_S = |\mathscr{D}_S(F')|_S \leqslant |D(F')|_S, \ |\mathscr{D}_S(G)|_S \leqslant |D(G')|_S.$$

Together with (2.3), applied to F', G', this implies (2.5). □

3. Applications

Let K be an algebraic number field and S a finite set of places on K. We consider the *resultant inequality*

$$0 < |R(F, G)|_S \leqslant A \tag{3.1}$$

in square-free binary forms $F, G \in \mathcal{O}_S[X, Y]$ where $A \geqslant 1$ is fixed. For the moment, we fix G and let only F vary. Note that if F is a solution of (3.1) then so is εF for all $\varepsilon \in \mathcal{O}_S^*$. We need the following lemma to derive our corollaries from Theorems 1A and 2A.

LEMMA 1. *Let G be a fixed square-free binary form of degree $s \geqslant 3$ and L a fixed finite normal extension of K containing the splitting field of G. Then up to multiplication by S-units, there are only finitely many non-constant square-free binary forms $F \in \mathcal{O}_S[X, Y]$ with splitting field contained in L that satisfy* (3.1). *Further, each of these binary forms F has degree at most $C_6(L, S, A)$, where $C_6(L, S, A)$ is a number depending only on L, S and A.*

Proof. Let H be the Hilbert class field of $L/\mathbb{Q}$ and T be the set of places on H lying above those in S. Note that H, T depend only on L, S. Denote by $\mathcal{O}_T$ the ring of T-integers in H. Let $F \in \mathcal{O}_S[X, Y]$ be a non-constant square-free binary form with splitting field contained in L that satisfies (3.1). Since H is the Hilbert class field of $L/\mathbb{Q}$, F and G can be factored as

$$F(X, Y) = \prod_{i=1}^{r} (\alpha_i X - \beta_i Y), \quad G(X, Y) = \prod_{j=1}^{s} (\gamma_j X - \delta_j Y)$$

with $\alpha_i, \beta_i, \gamma_j, \delta_j \in \mathcal{O}_T$. Here the γ_j, δ_j are fixed, and the α_i, β_i unknowns. There are non-zero elements $\sigma_j \in H, j = 1, 2, 3$, such that

$$\sigma_1(\gamma_1 X - \delta_1 Y) + \sigma_2(\gamma_2 X - \delta_2 Y) + \sigma_3(\gamma_3 X - \delta_3 Y) = 0.$$

Put $\Delta_{ij} = \alpha_i \delta_j - \beta_i \gamma_j$ for $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Then

$$\sigma_1 \Delta_{i1} + \sigma_2 \Delta_{i2} + \sigma_3 \Delta_{i3} = 0 \quad \text{for } i = 1, \ldots, r. \tag{3.2}$$

Each number Δ_{ij} divides $R(F,G)$ in $\mathcal{O}_T$. From (2.1) and (3.1) it follows that $|R(F,G)|_T \leqslant A$. Hence $|\Delta_{ij}|_T \leqslant A$ for $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. There is a finite set $\mathscr{C}_1$, depending only on H, T and A, hence only on L, S and A, such that every $x \in \mathcal{O}_T$ with $|x|_T \leqslant A$ can be expressed as $a\eta$ with $a \in \mathscr{C}_1$ and $\eta \in \mathcal{O}_T^*$ (see e.g. Lemma 1 in [4]). Therefore, we have $\Delta_{ik} = a_{ik}\eta_{ik}$ with $a_{ik} \in \mathscr{C}_1$ and $\eta_{ik} \in \mathcal{O}_T^*$. By (3.2), the pair $(\eta_{i1}/\eta_{i3}, \eta_{i2}/\eta_{i3})$ is a solution of the unit equation

$$\sigma_1 a_{i1} x + \sigma_2 a_{i2} y + \sigma_3 a_{i3} = 0 \quad \text{in } x,\, y \in \mathcal{O}_T^*.$$

By Theorem 1 of Evertse [2], the number of solutions of each such unit equation is bounded above by a number N depending only on H and T. This implies that there is a set $\mathscr{C}_2$ of cardinality $\leqslant N \cdot (\#\mathscr{C}_1)^3 \leqslant C_6(L,S,A)$, such that $(\Delta_{i1}, \Delta_{i2}, \Delta_{i3})$ can be expressed as $\rho_i(x_i, y_i, z_i)$ with $\rho_i \in \mathcal{O}_T^*$ and $(x_i, y_i, z_i) \in \mathscr{C}_2$ for $i = 1, \ldots, r$. It follows now that there is a set $\mathscr{C}_3$ of cardinality $\leqslant C_6(L,S,A)$ such that for $i = 1, \ldots, r$ we have $(\alpha_i, \beta_i) = \rho_i(u_i, v_i)$ with $\rho_i \in \mathcal{O}_T^*$ and $(u_i, v_i) \in \mathscr{C}_3$. Since F is square-free, the pairs $(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)$ are pairwise non-proportional, and hence $r \leqslant C_6(L,S,A)$. Further, it follows easily that up to multiplication by S-units, there are only finitely many square-free binary forms $F \in \mathcal{O}_S[X,Y]$ satisfying (3.1). □

REMARK 5. Now fix G, but not the splitting field of F. If $G(X,Y) = \prod_{j=1}^{s}(\gamma_j X - \delta_j Y)$, then $R(F,G) = \prod_{j=1}^{s} F(\delta_j, \gamma_j)$ is a product of linear forms in the coefficients of F, i.e. a *decomposable form.* Hence for fixed G, (3.1) is a special case of a decomposable form inequality. Wirsing [15] proved that if $G \in \mathbb{Z}[X,Y]$ has degree $s \geqslant 3$ and is square-free and if

$$r \geqslant 1, \quad 2r\left(1 + \frac{1}{3} + \cdots + \frac{1}{2r-1}\right) < s, \tag{3.3}$$

then there are only finitely many binary forms $F \in \mathbb{Z}[X,Y]$ of degree r satisfying $|R(F,G)| \leqslant A$. Schmidt [13] proved the same result with $r \geqslant 1$, $2r < s$ instead of (3.3), but under the additional condition that G is not divisible by a non-constant binary form in $\mathbb{Z}[X,Y]$ of degree $\leqslant r$.

Győry ([9], Theorem 7) was the first to consider (3.1) where both F, G are unknowns. Call two pairs of binary forms (F,G), (F',G') *S-equivalent* if

$$F' = \varepsilon F_U, \quad G' = \eta G_U$$

with some $\varepsilon, \eta \in \mathcal{O}_S^*$ and $U \in SL_2(\mathcal{O}_S)$ $\left(= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathcal{O}_S,\ ad - bc = 1\right\}\right)$. (1.2) implies that if (F,G) is a solution of (3.1) then so is (F',G') for every pair (F',G') S-equivalent to F. Győry [9] considered (3.1) for monic F, G. We extend his result to non-monic F, G. Fix a finite normal extension L of K and put

$$V_1(L) := \left\{ \begin{array}{l} (F,G): F, G \text{ are binary forms of degree} \geqslant 3 \text{ in } \mathcal{O}_S[X,Y], \\ FG \text{ is square-free, } FG \text{ has splitting field } L. \end{array} \right\}.$$

COROLLARY 1. *Up to S-equivalence,* (3.1) *has only finitely many solutions* $(F,G) \in V_1(L)$.

Proof. C_7, C_8 will denote constants depending only on S, L and A. Let $(F,G) \in V_1(L)$ be a pair satisfying (3.1). By Lemma 1 we have $\deg F =: r \leqslant C_7$, $\deg G =: s \leqslant C_7$. Together with Theorem 1A and $|R(F,G)|_S \leqslant A$ this implies that

$$|D(G)|_S \leqslant C_8. \tag{3.4}$$

By Theorem 3 of [5], there is a finite set $\mathscr{C}$ of binary forms $\tilde{G} \in \mathcal{O}_S[X,Y]$, depending only on K, S and C_8 and hence only on L, S and A, such that

$$G = \eta \tilde{G}_U \quad \text{for some } \tilde{G} \in \mathscr{C},\ \eta \in \mathcal{O}_S^*,\ U \in SL_2(\mathcal{O}_S).$$

Theorem 3 of [5] was proved effectively but in its ineffective and qualitative form that we need here, it is only a slight generalization of Theorem 2 of Birch and Merriman [1]. Note that

$$0 < |R(F_{U^{-1}}, \tilde{G})|_S = |R(F,G)|_S \leqslant A.$$

Together with Lemma 1 this implies that there is a finite set $\mathscr{C}'$ of binary forms $\tilde{F} \in \mathcal{O}_S[X,Y]$, depending only on L, S and A, such that $F_{U^{-1}} = \varepsilon \tilde{F}$ with $\tilde{F} \in \mathscr{C}'$, $\varepsilon \in \mathcal{O}_S^*$. This implies that $F = \varepsilon \tilde{F}_U$, $G = \eta \tilde{G}_U$ with $\tilde{F} \in \mathscr{C}'$, $\tilde{G} \in \mathscr{C}$ which proves Corollary 1. □

Győry's result in [9] was concerned with the set

$$V_2(L) := \left\{ \begin{array}{l} (F,G): F, G \text{ are binary forms in } \mathcal{O}_S[X,Y] \text{ with degrees} \\ \text{at least 2 and at least 3, respectively, such} \\ \text{that } F(1,0)=1,\ G(1,0)=1,\ FG \text{ is square-free,} \\ FG \text{ has splitting field } L. \end{array} \right\}$$

It follows from Theorem 7 of [9] (which was established more generally over arbitrary integrally closed and finitely generated domains over $\mathbb{Z}$) that up to equivalence defined by $(F,G) \sim (F_U, G_U)$ with $U = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $b \in \mathcal{O}_S$, there are only finitely many $(F,G) \in V_2(L)$ with a given non-zero resultant. We call the pairs

(F, G), (F', G') in $V_2(L)$ *strongly S-equivalent* if there are $\varepsilon \in \mathcal{O}_S^*$, $a \in \mathcal{O}_S$ such that

$$F' = \varepsilon^{-\deg F} F(\varepsilon x + aY, Y), \quad G' = \varepsilon^{-\deg G} G(\varepsilon x + aY, Y).$$

The next corollary is a consequence of Theorem 2A.

COROLLARY 2. *Up to strong S-equivalence,* (3.1) *has only finitely many solutions* $(F, G) \in V_2(L)$.

Corollary 2 has recently been generalized in [10] by the second author to the case when the ground ring is an arbitrary finitely generated and integrally closed ring with 1 in a finitely generated extension of $\mathbb{Q}$.

Proof. C_9, C_{10} will denote constants depending only on S, L and A. Let $(F, G) \in V_2(L)$ be a pair satisfying (3.1). Note that $R(\hat{F}, G) = R(F, G)$, where $\hat{F}(X, Y) = F(X, Y)Y$. By applying Lemma 1 to $\hat{F}$, G, we infer that $\deg F =: r \leqslant C_9$, $\deg G =: s \leqslant C_9$. Together with Theorem 2A and (3.1), this implies that $|D(G)|_S \leqslant C_{10}$. Since G is monic, we have by Theorem 1 of [8] that there is a finite set $\mathscr{C}$ of monic binary forms $\tilde{G} \in \mathcal{O}_S[X, Y]$, depending only on S, L and A, such that $G = \varepsilon^{-\deg G} \tilde{G}(\varepsilon x + aY, Y)$ for some $\tilde{G} \in \mathscr{C}$, $\varepsilon \in \mathcal{O}_S^*$, $a \in \mathcal{O}_S$. Now the proof of Corollary 2 is completed in the same way as that of Corollary 1. We have to notice that in Lemma 1, a monic binary form that is determined up to multiplication by an S-unit, is uniquely determined. □

We now consider the Thue-Mahler inequality

$$0 < |F(x, y)|_S \leqslant A \quad \text{in } x, y \in \mathcal{O}_S, \tag{3.5}$$

where $F(X, Y) \in \mathcal{O}_S[X, Y]$ is a square-free binary form of degree at least 3, and $A \geqslant 1$. Two solutions (x_1, y_1), (x_2, y_2) of (3.5) are called *proportional* if $(x_2, y_2) = \lambda(x_1, y_1)$ for some $\lambda \in K^*$. As a special case of Corollary 1 we get Theorem 2(i) of [4].

COROLLARY 3. *For every* $A \geqslant 1$ *and for any finite normal extension L of K, there are only finitely many S-equivalence classes of square-free binary forms* $F \in \mathcal{O}_S[X, Y]$ *of degree at least* 3 *and splitting field L over K for which* (3.5) *has more than two pairwise non-proportional solutions.*

Proof. Let F be an arbitrary but fixed binary form with the properties specified in Corollary 3, and suppose that (3.5) has three pairwise non-proportional solutions (x_1, y_1), (x_2, y_2), (x_3, y_3). Let

$$G(X, Y) = (y_1 X - x_1 Y)(y_2 X - x_2 Y)(y_3 X - x_3 Y).$$

Then

$$0 < |R(F, G)|_S = |F(x_1, y_1)F(x_2, y_2)F(x_3, y_3)|_S \leqslant A^3.$$

Further, FG is square-free and has splitting field L. By applying now Corollary 1 to F and G we get that indeed there are only finitely many possibilities for F up to S-equivalence. □

Using Theorem 1A, we can prove the following:

COROLLARY 4. *Let $A \geqslant 1$, and let $F \in \mathcal{O}_S[X, Y]$ be a square-free binary form of degree $r \geqslant 3$ with splitting field L such that*

$$|D(F)|_S \geqslant C_{11}^{\mathrm{ineff}}(r, L, S)A^{18(r-1)}. \tag{3.6}$$

Then (3.5) *has at most two pairwise non-proportional solutions.*

By Theorem 3 of [5] there are only finitely many S-equivalence classes of square-free binary forms $F \in \mathcal{O}_S[X, Y]$ for which $|D(F)|_S$ is bounded. Hence Corollary 4 can be regarded as a "semi-quantitative" version of Corollary 3.

Proof. Suppose that (3.5) has three pairwise non-proportional solutions $(x_1, y_1), (x_2, y_2), (x_3, y_3)$. Take G as in the proof of Corollary 3. Then by Theorem 1A we have

$$\begin{aligned} A^3 &\geqslant |F(x_1, y_1)F(x_2, y_2)F(x_3, y_3)|_S = |R(F, G)|_S \\ &\geqslant C_{12}^{\mathrm{ineff}}(r, L, S)(|D(F)|_S^{3/(r-1)})^{1/18} \end{aligned}$$

which contradicts (3.6) for sufficiently large C_{11}. □

4. Proof of Theorem 2A

Let K be an algebraic number field of degree d, and S a finite set of places on K. For $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$, put

$$|\mathbf{x}|_v = |x_1, \ldots, x_n|_v := \max(|x_1|_v, \ldots, |x_n|_v) \quad \text{for } v \in \mathbb{M}_K,$$

and

$$H_S(\mathbf{x}) = H_S(x_1, \ldots, x_n) := \prod_{v \in S} \max(|x_1|_v, \ldots, |x_n|_v). \tag{4.1}$$

For $v \in \mathbb{M}_K$, put $s(v) = 1/d$ if v corresponds to an embedding $\sigma: K \hookrightarrow \mathbb{R}$, put

$s(v) = 2/d$ if v corresponds to a pair of complex conjugate embeddings $\sigma, \bar{\sigma}: K \hookrightarrow \mathbb{C}$, and put $s(v) = 0$ if v is finite. Thus $\Sigma_{v \in S} s(v) = 1$, and

$$|x_1 + \cdots + x_n|_v \leqslant n^{s(v)} |x_1, \ldots, x_n|_v \quad \text{for } v \in \mathbb{M}_K,\ x_1, \ldots, x_n \in K.$$

Therefore,

$$|x_1 + \cdots + x_n|_S \leqslant n H_S(x_1, \ldots, x_n) \quad \text{for } x_1, \ldots, x_n \in K. \tag{4.2}$$

The following lemma is our basic tool.

LEMMA 2. *Let $x_1, \ldots, x_n$ be elements of $\mathcal{O}_S$ with*

$$\begin{cases} x_1 + \cdots + x_n = 0, \\ \Sigma_{i \in I} x_i \neq 0 \text{ for each proper non-empty subset } I \text{ of } \{1, \ldots, n\}. \end{cases} \tag{4.3}$$

Then for all $\varepsilon > 0$ we have

$$H_S(x_1, \ldots, x_n) \leqslant C_{13}^{\text{ineff}}(K, S, \varepsilon) \left| \prod_{i=1}^{n} x_i \right|_S^{1+\varepsilon}. \tag{4.4}$$

Proof. This is Lemma 6 of Laurent [11]. Laurent was, in his paper [11], the first to use results of this type to derive "semi-effective" estimates for certain Diophantine problems. Laurent's Lemma 6 is an easy consequence of Theorem 2 of Evertse [3], and the latter was derived from Schlickewei's p-adic generalization of the Subspace Theorem [12]. The constant in (4.4) is ineffective since the Subspace Theorem is ineffective.

We derive Theorem 2A from a result on pairs of monic quadratic forms. A pair of monic quadratic forms

$$F(X, Y) = X^2 + b_1 XY + c_1 Y^2, \qquad G(X, Y) = X^2 + b_2 XY + c_2 Y^2$$

is said to be *related* if $b_1 = b_2$, and *unrelated* if $b_1 \neq b_2$.

LEMMA 3. *Let $F \in \mathcal{O}_S[X, Y]$, $G \in \mathcal{O}_S[X, Y]$ be quadratic forms with*

$$\begin{cases} F(1, 0) = 1,\ G(1, 0) = 1, \\ FG \text{ is square-free, } FG \text{ has splitting field } K \text{ over } K. \end{cases} \tag{4.5}$$

Then for all $\varepsilon > 0$ *we have*

$$|D(F)|_S \leqslant C_{14}^{\text{ineff}}(K, S, \varepsilon)|R(F, G)|_S^{2(1+\varepsilon)} \quad \textit{if } F, G \textit{ are unrelated,} \tag{4.6}$$

$$|D(F)|_S \leqslant C_{15}^{\text{ineff}}(K, S, \varepsilon)(|R(F, G)|_S|D(G)|_S)^{1+\varepsilon} \quad \textit{if } F, G \textit{ are related.} \tag{4.7}$$

Proof. We may assume that

$$F(X, Y) = (X - \beta_1 Y)(X - \beta_2 Y),$$
$$G(X, Y) = (X - \delta_1 Y)(X - \delta_2 Y),$$

where β_1, β_2, δ_1, δ_2 are distinct elements of $\mathcal{O}_S$. Take $\varepsilon > 0$. The constants implied by $\ll$ are ineffective and depend only on K, S and ε.

First assume that F, G are unrelated. Then $\beta_1 + \beta_2 \neq \delta_1 + \delta_2$. We apply Lemma 2 to

$$(\beta_1 - \delta_1) - (\beta_1 - \delta_2) - (\beta_2 - \delta_1) + (\beta_2 - \delta_2) = 0. \tag{4.8}$$

Note that each sum formed from a proper non-empty subset of

$$\{(\beta_1 - \delta_1),\ -(\beta_1 - \delta_2),\ -(\beta_2 - \delta_1),\ (\beta_2 - \delta_2)\}$$

is different from 0. Further, by (1.3), (1.1), respectively, we have

$$D(F) = (\beta_1 - \beta_2)^2,$$
$$R(F, G) = (\beta_1 - \delta_1)(\beta_1 - \delta_2)(\beta_2 - \delta_1)(\beta_2 - \delta_2).$$

Hence, by (4.2) and (4.4), applied to (4.8),

$$\begin{aligned} |D(F)|_S^{1/2} &= |\beta_1 - \beta_2|_S = |(\beta_1 - \delta_1) - (\beta_2 - \delta_1)|_S \\ &\leqslant 2H_S(\beta_1 - \delta_1,\ \beta_2 - \delta_1) \\ &\leqslant 2H_S(\beta_1 - \delta_1,\ -(\beta_1 - \delta_2),\ -(\beta_2 - \delta_1),\ \beta_2 - \delta_2) \\ &\ll |(\beta_1 - \delta_1)(\beta_1 - \delta_2)(\beta_2 - \delta_1)(\beta_2 - \delta_2)|_S^{1+\varepsilon} = |R(F, G)|_S^{1+\varepsilon} \end{aligned}$$

which implies (4.6).

Now assume that F and G are related. Then $\beta_1 + \beta_2 = \delta_1 + \delta_2$. Therefore,

$$\beta_1 - \beta_2 = \delta_1 + \delta_2 - 2\beta_2 = (\delta_1 - \beta_2) + (\delta_2 - \beta_2).$$

We apply Lemma 2 to the identity

$$(\delta_1-\beta_2)-(\delta_2-\beta_2)-(\delta_1-\delta_2)=0$$

and obtain, using again (4.2),

$$\begin{aligned}|D(F)|_S^{1/2} &= |\beta_1-\beta_2|_S = |(\delta_1-\beta_2)+(\delta_2-\beta_2)|_S\\ &\leqslant 2H_S(\delta_1-\beta_2,\ \delta_2-\beta_2)\\ &\leqslant 2H_S(\delta_1-\beta_2,\ -(\delta_2-\beta_2),\ -(\delta_1-\delta_2))\\ &\ll |(\delta_1-\beta_2)(\delta_2-\beta_2)(\delta_1-\delta_2)|_S^{1+\varepsilon}\\ &= (|(\delta_1-\beta_2)(\delta_2-\beta_2)|_S |D(G)|_S^{1/2})^{1+\varepsilon}.\end{aligned}$$

Similarly,

$$|D(F)|_S^{1/2} \ll (|(\delta_1-\beta_1)(\delta_2-\beta_1)|_S |D(G)|_S^{1/2})^{1+\varepsilon}.$$

Thus we get

$$\begin{aligned}|D(F)|_S &\ll (|(\delta_1-\beta_1)(\delta_1-\beta_2)(\delta_2-\beta_1)(\delta_2-\beta_2)|_S |D(G)|_S)^{1+\varepsilon}\\ &= (|R(F,\ G)|_S |D(G)|_S)^{1+\varepsilon}\end{aligned}$$

which is just (4.7). □

Proof of Theorem 2*A*. Let $F(X, Y)$, $G[X, Y) \in \mathcal{O}_S[X, Y]$ be binary forms of degrees $r \geqslant 2$, $s \geqslant 3$, respectively, such that $F(1,0)=G(1,0)=1$, FG is square-free, and FG has splitting field L over K. Denote by T the set of places on L lying above those in S. Then

$$F(X,\ Y) = \prod_{i=1}^{r} (X-\beta_i Y), \qquad G(X,\ Y) = \prod_{j=1}^{s} (X-\delta_j Y)$$

with $\beta_i, \delta_j \in \mathcal{O}_T$ for $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Let $\varepsilon > 0$ with $\varepsilon < 1/6$ and put $\delta = \varepsilon/100$. The constants implied by $\ll$ depend only on L, S and ε. Finally, put

$$\begin{aligned}&F_{pq}(X,\ Y)=(X-\beta_p Y)(X-\beta_q Y) \quad \text{for } p,\ q\in\{1,\dots,r\},\ p<q,\\ &G_{ij}(X,\ Y)=(X-\delta_i Y)(X-\delta_j Y) \quad \text{for } i, j\in\{1,\dots,s\},\ i<j.\end{aligned}$$

Pick $p, q \in \{1,\dots,r\}$ with $p<q$. Let I be the collection of pairs (i,j) with $1 \leqslant i < j \leqslant s$ such that G_{ij} is related to F_{pq}. Then I consists of the pairs (i,j) with $\delta_i+\delta_j=\beta_p+\beta_q$. Since $\delta_1,\dots,\delta_s$ are distinct, the pairs in I must be pairwise disjoint. Therefore, since $s \geqslant 3$,

$$\# I \leqslant \left[\frac{s}{2}\right] \leqslant \frac{1}{3}\binom{s}{2}. \tag{4.9}$$

By Lemma 3 (with L, T instead of K, S) we have

$$|D(F_{pq})|_T \ll |R(F_{pq}, G_{ij})|_T^{2(1+\delta)} \quad \text{for } (i, j) \notin I. \tag{4.10}$$

But, by (1.1) and (1.2) we have

$$\prod_{1 \leqslant i<j \leqslant s} R(F_{pq}, G_{ij}) = R(F_{pq}, G)^{s-1}. \tag{4.11}$$

Together with (4.9) and (4.10) this implies

$$\begin{aligned} |D(F_{pq})|_T &\ll \Bigg(\prod_{\substack{1 \leqslant i<j \leqslant s \\ (i,j) \notin I}} |R(F_{pq}, G_{ij})|_T^2 \Bigg)^{(1+\delta)/(\binom{s}{2} - \# I)} \\ &\leqslant \Bigg(\prod_{1 \leqslant i<j \leqslant s} |R(F_{pq}, G_{ij})|_T \Bigg)^{3(1+\delta)/\binom{s}{2}} \\ &= |R(F_{pq}, G)|_T^{6(1+\delta)/s}. \end{aligned} \tag{4.12}$$

By Lemma 3, (4.10), (4.11) and (4.12) we get

$$\begin{aligned} |D(G)|_T &= \prod_{1 \leqslant i<j \leqslant s} |D(G_{ij})|_T = \prod_{\substack{1 \leqslant i<j \leqslant s \\ (i,j) \notin I}} |D(G_{ij})|_T \cdot \prod_{(i,j) \in I} |D(G_{ij})|_T \\ &\ll \Bigg(\prod_{1 \leqslant i<j \leqslant s} |R(F_{pq}, G_{ij})|_T^2 \prod_{(i,j) \in I} |D(F_{pq})|_T \Bigg)^{1+\delta} \\ &= (|R(F_{pq}, G)|_T^{2(s-1)} |D(F_{pq})|_T^{\# I})^{1+\delta} \\ &\leqslant (|R(F_{pq}, G)|_T^{2(s-1)} \cdot |R(F_{pq}, G)|_T^{(\# I) \cdot 6/s})^{(1+\delta)^2}, \end{aligned}$$

which gives, together with (4.9),

$$|D(G)|_T \ll |R(F_{pq}, G)|_T^{3(s-1)(1+\delta)^2}. \tag{4.13}$$

Finally, from (4.12), (4.13), and the relations

$$\prod_{1 \leqslant p<q \leqslant r} R(F_{pq}, G) = R(F, G)^{r-1}$$

and

$$6(1+\delta) < 6(1+\delta)^2 < \left(\frac{1}{6} - \varepsilon\right)^{-1}$$

it follows that

$$\begin{aligned}|D(F)|_T &= \prod_{1 \leqslant p < q \leqslant r} |D(F_{pq})|_T \ll \left(\prod_{1 \leqslant p < q \leqslant r} |R(F_{pq}, G)|_T \right)^{6(1+\delta)/s} \\ &= |R(F, G)|_T^{6(r-1)(1+\delta)/s} \ll |R(F, G)|_T^{(r-1)(1/6-\varepsilon)^{-1}/s}\end{aligned}$$

and

$$\begin{aligned}|D(G)|_T &\ll \left(\prod_{1 \leqslant p < q \leqslant r} |R(F_{pq}, G)|_T \right)^{3(s-1)(1+\delta)^2/\binom{r}{2}} \\ &= |R(F, G)|_T^{6(s-1)(1+\delta)^2/r} \ll |R(F, G)|_T^{(s-1)(1/6-\varepsilon)^{-1}/r}.\end{aligned}$$

This implies Theorem 2A, since $|x|_T = |x|_S$ for $x \in K$. □

5. Proof of Theorem 1A

Let again K be an algebraic number field and S a finite set of places on K. We first prove a special case of Theorem 1A.

LEMMA 4. *Let $F, G \in \mathcal{O}_S[X, Y]$ be binary forms such that*

$$\begin{aligned}&F(X, Y) = \textstyle\prod_{i=1}^3 (\alpha_i X - \beta_i Y) \quad \textit{with } \alpha_i, \beta_i \in \mathcal{O}_S \textit{ for } i = 1, 2, 3, \\ &G(X, Y) = \textstyle\prod_{j=1}^3 (\gamma_j x - \delta_j Y) \quad \textit{with } \gamma_j, \delta_j \in \mathcal{O}_S \textit{ for } j = 1, 2, 3, \\ &F \cdot G \textit{ is square-free.}\end{aligned} \tag{5.1}$$

Then for all $\varepsilon > 0$ we have

$$|R(F, G)|_S \geqslant C_{16}^{\text{ineff}}(K, S, \varepsilon)(|D(F)D(G)|_S)^{3/34-\varepsilon}. \tag{5.2}$$

Proof. We use an idea from [6]. Put

$$\begin{aligned}&\Delta_{ij} = \alpha_i \delta_j - \beta_i \gamma_j \quad \text{for } i, j = 1, 2, 3, \\ &A_{ij} = \alpha_i \beta_j - \alpha_j \beta_i,\ B_{ij} = \gamma_i \delta_j - \gamma_j \delta_i \quad \text{for } i, j = 1, 2, 3,\ i \neq j.\end{aligned}$$

It is easy to check that

$$\det\begin{pmatrix}\Delta_{11} & \Delta_{12} & \Delta_{13}\\ \Delta_{21} & \Delta_{22} & \Delta_{23}\\ \Delta_{31} & \Delta_{32} & \Delta_{33}\end{pmatrix} = 0$$

or, by expanding the determinant,

$$u_1+u_2+u_3+u_4+u_5+u_6 = 0, \tag{5.3}$$

where

$$\begin{aligned} &u_1=\Delta_{11}\Delta_{22}\Delta_{33}, \quad u_3=\Delta_{12}\Delta_{23}\Delta_{31}, \quad u_5=\Delta_{13}\Delta_{21}\Delta_{32},\\ &u_2=-\Delta_{11}\Delta_{23}\Delta_{32}, \quad u_4=-\Delta_{12}\Delta_{21}\Delta_{33}, \quad u_6=-\Delta_{13}\Delta_{22}\Delta_{31}. \end{aligned} \tag{5.4}$$

Take $i,\ j,\ k,\ l\in\{1,2,3\}$ with $i\neq j,\ k\neq l$ and choose h, m such that $\{i,j,h\}=\{k,l,m\}=\{1,2,3\}$. Then from the product rule for determinants it follows that

$$A_{ij}B_{kl} = \Delta_{ik}\Delta_{jl}-\Delta_{il}\Delta_{jk}.$$

From (5.4) it follows that there are p, q with $1\leqslant p<q\leqslant 6$, $p\not\equiv q \pmod 2$ such that $\Delta_{ik}\Delta_{jl}\Delta_{hm} = \pm u_p$, $\Delta_{il}\Delta_{jk}\Delta_{hm} = \mp u_q$. Hence

$$A_{ij}B_{kl} = \pm\Delta_{hm}^{-1}(u_p+u_q). \tag{5.5}$$

Here h, m, p and q are uniquely determined by the sets $\{i,j\}$, $\{k,l\}$ and vice versa. Hence if $\{i,j\}$, $\{k,l\}$ run through the subsets of $\{1,2,3\}$ of cardinality 2, then (h,m) runs through the ordered pairs from $\{1,2,3\}$ and (p,q) runs through the pairs with $1\leqslant p<q\leqslant 6$, $p\not\equiv q \pmod 2$. Hence, by taking the product over all sets $\{i,j\}$, $\{k,l\}$ and using the fact that

$$R(F,\ G) = \prod_{i=1}^{3}\prod_{j=1}^{3}\Delta_{ij},\ D(F)=(A_{12}A_{23}A_{13})^2,\ D(G)=(B_{12}B_{23}B_{13})^2, \tag{5.6}$$

we get

$$(D(F)D(G))^{3/2} = \pm R(F,\ G)^{-1}\prod_{\substack{1\leqslant p<q\leqslant 6\\ p\not\equiv q \pmod 2}}(u_p+u_q). \tag{5.7}$$

From (4.2) we infer that $|u_p+u_q|_S \leqslant 2H_S(u_p, u_q)$. By inserting this into (5.7) we get

$$|D(F)D(G)|_S^{3/2} \leqslant 2^9|R(F, G)|_S^{-1} \prod_{\substack{1\leqslant p<q\leqslant 6 \\ p\not\equiv q(\mathrm{mod}\,2)}} H_S(u_p, u_q). \tag{5.8}$$

Put $R := R(F, G)$. Then $R \neq 0$. We recall that

$$u_1+u_2+u_3+u_4+u_5+u_6 = 0. \tag{5.3}$$

Further, by (5.7),

$$u_p+u_q \neq 0 \quad \text{for } 1 \leqslant p < q \leqslant 6 \quad \text{with } p \not\equiv q\,(\mathrm{mod}\,2). \tag{5.9}$$

Finally, by (5.4),

$$u_1u_3u_5 = -u_2u_4u_6 = R. \tag{5.10}$$

Let U be the set of vectors $\mathbf{u} = (u_1, \ldots, u_6) \in \mathcal{O}_S^6$ satisfying (5.3), (5.9) and (5.10). Lemma 4 follows at once from (5.8) and

LEMMA 5. *For every* $\mathbf{u} = (u_1, \ldots, u_6) \in U$ *and every* $\varepsilon > 0$ *we have*

$$\prod_{\substack{1\leqslant p<q\leqslant 6 \\ p\not\equiv q(\mathrm{mod}\,2)}} H_S(u_p, u_q) \leqslant C_{17}^{\mathrm{ineff}}(K, S, \varepsilon)|R|_S^{18+\varepsilon}. \tag{5.11}$$

Proof. Put $\delta = \varepsilon/100$. The constants implied by $\ll$ depend only on K, S and ε. The idea is to consider all partitions of (5.3) into minimal vanishing subsums and to apply Lemma 2 to these subsums. We can reduce the number of cases to be considered by using (5.9) and the following symmetric property of U:

$$\begin{cases} \text{for every } \mathbf{u} = (u_1, \ldots, u_6) \in U \text{ and each permutation } \sigma \text{ of } (1, \ldots, 6) \\ \text{with } \sigma(i) - \sigma(j) \equiv i - j\,(\mathrm{mod}\,2) \text{ for } i, j \in \{1, \ldots, 6\}, \\ \text{there is an } a \in \{0, 1\} \text{ with } (-1)^a(u_{\sigma(1)}, \ldots, u_{\sigma(6)}) \in U. \end{cases} \tag{5.12}$$

Take $(u_1, \ldots, u_6) \in U$ and put

$$A = \prod_{\substack{1\leqslant p<q\leqslant 6 \\ p\not\equiv q(\mathrm{mod}\,2)}} H_S(u_p, u_q).$$

Because of (5.9), (5.12), it suffices to derive the upper bound for A in each of the four following cases:

(i) $u_1+u_2+u_3+u_4+u_5+u_6=0$, $\Sigma_{i\in I}u_i \neq 0$ for each proper non-empty subset I of $\{1,\dots,6\}$.

(ii) $u_1+u_3=0$, $u_2+u_4+u_5+u_6=0$, $\Sigma_{i\in I}u_i \neq 0$ for each proper non-empty subset I of $\{2,4,5,6\}$.

(iii) $u_1+u_2+u_3=0$, $u_4+u_5+u_6=0$.

(iv) $u_1+u_3+u_5=0$, $u_2+u_4+u_6=0$.

We shall frequently use the following obvious properties of H_S:

$$\begin{cases} H_S(\lambda\mathbf{x})=|\lambda|_S H_S(\mathbf{x}) \quad \text{for } \lambda\in K,\ \mathbf{x}\in K^n; \\ H_S(x_1y_1,\dots,x_ny_n)\leqslant H_S(x_1,\dots,x_n)H_S(y_1,\dots,y_n) \quad \text{for } x_1,\dots,y_n\in K; \\ H_S(x_1^m,\dots,x_n^m)=\{H_S(x_1,\dots,x_n)\}^m \quad \text{for } x_1,\dots,x_n\in K,\ m\in\mathbb{N}. \end{cases} \tag{5.13}$$

Case i. For p, $q\in\{1,\dots,6\}$ with $p\not\equiv q \pmod 2$ we have, by Lemma 2 and (5.10),

$$H_S(u_p,u_q)\leqslant H_S(u_1,\dots,u_6)\ll |u_1\cdots u_6|_S^{1+\delta}=|R|_S^{2+2\delta},$$

whence

$$A\ll |R|_S^{18+18\delta}\ll |R|_S^{18+\varepsilon}.$$

Case ii. For $(p,q)=(2,5)$, $(4,5)$, $(5,6)$ we have, by Lemma 2 and (5.10),

$$\begin{aligned} H_S(u_p,\ u_q) &\leqslant H_S(u_2,\ u_4,\ u_5,\ u_6)\ll |u_2u_4u_5u_6|_S^{1+\delta} \\ &\leqslant |u_1\cdots u_6|_S^{1+\delta}\ll |R|_S^{2+2\delta}. \end{aligned} \tag{5.14}$$

By (5.10) and $u_3 = -u_1$, we have

$$(u_1^2,\ u_2^2) = (u_2/u_5)(u_4u_6,\ u_2u_5).$$

By applying (5.13), Lemma 2 and (5.10) we get

$$\begin{aligned} H_S(u_1,u_2)^2 &\leqslant |(u_2/u_5)|_S H_S(u_4,\ u_2)H_S(u_6,\ u_5) \\ &\leqslant |(u_2/u_5)|_S H_S(u_2,\ u_4,\ u_5,\ u_6)^2 \ll |(u_2/u_5)|_S |u_2u_4u_5u_6|_S^{2+2\delta} \\ &\leqslant |u_2/(u_1u_3u_5)|_S |u_1\cdots u_6|_S^{2+2\delta} = |u_2|_S |R|_S^{3+4\delta}\leqslant |R|_S^{4+4\delta}. \end{aligned}$$

Hence

$$H_S(u_1,\ u_2)\ll |R|_S^{2+2\delta}.$$

Similarly, we obtain that also $H_S(u_p, u_q) \ll |R|_S^{2+2\delta}$ for $(p, q) = (1, 4), (1, 6), (2, 3), (3, 4), (3, 6)$. Together with (5.14) this implies

$$A \ll |R|_S^{18+18\delta} \ll |R|_S^{18+\varepsilon}.$$

Case iii. This is the most difficult case. For $(p, q) = (1, 2), (2, 3)$ we have, by Lemma 2,

$$H_S(u_p, u_q) \leqslant H_S(u_1, u_2, u_3) \ll |u_1 u_2 u_3|_S^{1+\delta}.$$

Similarly, for $(p, q) = (4, 5), (5, 6)$ we have $H_S(u_p, u_q) \ll |u_4 u_5 u_6|_S^{1+\delta}$. Together with (5.10) this implies

$$\begin{aligned} &H_S(u_1, u_2)H_S(u_2, u_3)H_S(u_4, u_5)H_5(u_5, u_6) \\ &\quad \ll |u_1 \cdots u_6|_S^{2+2\delta} = |R|_S^{4+4\delta}. \end{aligned} \tag{5.15}$$

By (5.10) we have

$$(u_1, u_4) = (u_1 u_4 / R)(-u_2 u_6, u_3 u_5).$$

Together with (5.13), Lemma 2 and again (5.10), this implies

$$\begin{aligned} H_S(u_1, u_4) &\leqslant |u_1 u_4|_S |R|_S^{-1} H_S(u_2, u_3) H_S(u_6, u_5) \\ &\leqslant |u_1 u_4|_S |R|_S^{-1} H_S(u_1, u_2, u_3) H_S(u_4, u_5, u_6) \\ &\ll |u_1 u_4|_S |R|_S^{-1} |u_1 u_2 u_3|_S^{1+\delta} |u_4 u_5 u_6|_S^{1+\delta} = |u_1 u_4|_S |R|_S^{1+2\delta}. \end{aligned}$$

By a similar argument, we get $H_S(u_p, u_q) \ll |u_p u_q|_S |R|_S^{1+2\delta}$ for $(p, q) = (1, 6), (3, 4), (3, 6)$. Hence, by (5.10) we obtain

$$\begin{aligned} &H_S(u_1, u_4)H_S(u_1, u_6)H_S(u_3, u_4)H_S(u_3, u_6) \\ &\quad \ll |u_1 u_4 \cdot u_1 u_6 \cdot u_3 u_4 \cdot u_3 u_6|_S |R|_S^{4+8\delta} \\ &\quad \leqslant |u_1 \cdots u_6|_S^2 |R|_S^{4+8\delta} = |R|_S^{8+8\delta}. \end{aligned} \tag{5.16}$$

Finally, by (5.10) we have

$$(u_2, u_5) = R^{-1}(-u_2^2 u_4 u_6, u_1 u_3 u_5^2).$$

Together with (5.13), Lemma 2 and (5.10), this gives

$$\begin{aligned} H_S(u_2, u_5) &\leqslant |R|_S^{-1} H_S(u_2, u_1) H_S(u_2, u_3) H_S(u_4, u_5) H_S(u_6, u_5) \\ &\leqslant |R|_S^{-1} H_S(u_1, u_2, u_3)^2 H_S(u_4, u_5, u_6)^2 \\ &\ll |R|_S^{-1} |u_1 \cdots u_6|_S^{2+2\delta} = |R|_S^{3+4\delta}. \end{aligned}$$

By combining this with (5.15) and (5.16), we obtain

$$A \ll |R|_S^{15+16\delta} \ll |R|_S^{18+\varepsilon}.$$

Case iv. By (5.10) we have

$$(u_1^3, u_2^3) = (u_1 u_2 / R)(-u_1^2 u_4 u_6, u_2^2 u_3 u_5).$$

Together with (5.13), $|u_1 u_2|_S \leqslant |R|_S^2$, Lemma 2 and (5.10) this implies

$$\begin{aligned} H_S(u_1, u_2)^3 &\leqslant |u_1 u_2 R^{-1}|_S H_S(u_1, u_3) H_S(u_1, u_5) H_S(u_4, u_2) H_S(u_6, u_2) \\ &\leqslant |R|_S H_S(u_1, u_3, u_5)^2 H_S(u_2, u_4, u_6)^2 \\ &\ll |R|_S (|u_1 u_3 u_5|_S |u_2 u_4 u_6|_S)^{2+2\delta} = |R|_S^{5+4\delta}. \end{aligned}$$

Therefore,

$$H_S(u_1, u_2) \ll |R|_S^{(5+4\delta)/3}.$$

Similarly, we obtain that $H_S(u_p, u_q) \ll |R|_S^{(5+4\delta)/3}$ for all pairs (p, q) with $1 \leqslant p < q \leqslant 6$, $p \not\equiv q \pmod 2$. Hence

$$A \ll |R|_S^{15+12\delta} \ll |R|_S^{18+\varepsilon}.$$

This completes the proof of Lemma 5 and hence that of Lemma 4. □

Proof of Theorem 1A. Let $F, G \in \mathcal{O}_S[X, Y]$ be binary forms of degrees $r \geqslant 3$, $s \geqslant 3$, respectively, such that FG is square-free, and FG has splitting field L over K. Denote by H the Hilbert class field of $L/\mathbb{Q}$ and by T the set of places on H lying above those in S. Note again that H and T depend only on L and S. Let $\varepsilon > 0$. The constants implied by $\gg$ depend only on r, s, L, S and ε.

We have

$$F(X, Y) = \prod_{i=1}^{r} (\alpha_i X - \beta_i Y), \qquad G(X, Y) = \prod_{j=1}^{s} (\gamma_j X - \delta_j Y)$$

with $\alpha_i, \beta_i, \gamma_j, \delta_j \in \mathcal{O}_T$ for $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Put

$$F_{npq}(X, Y) = (\alpha_n X - \beta_n Y)(\alpha_p X - \beta_p Y)(\alpha_q X - \beta_q Y) \quad \text{for } 1 \leqslant n < p < q \leqslant r,$$

and

$$G_{ijk}(X, Y) = (\gamma_i X - \delta_i Y)(\gamma_j X - \delta_j Y)(\gamma_k X - \delta_k Y) \quad \text{for } 1 \leqslant i < j < k \leqslant s.$$

From Lemma 4 it follows with H, T instead of K, S that for $1 \leqslant n < p < q \leqslant r$, $1 \leqslant i < j < k \leqslant s$,

$$|R(F_{npq}, G_{ijk})|_T \gg (|D(F_{npq})D(G_{ijk})|_T)^{3/34 - 3\varepsilon/2}. \tag{5.17}$$

Further,

$$\prod_{1 \leqslant n < p < q \leqslant r} \prod_{1 \leqslant i < j < k \leqslant s} R(F_{npq}, G_{ijk}) = R(F, G)^{\binom{r-1}{2}\binom{s-1}{2}},$$

$$\prod_{1 \leqslant n < p < q \leqslant r} D(F_{npq}) = D(F)^{r-2}, \quad \prod_{1 \leqslant i < j < k \leqslant s} D(G_{ijk}) = D(G)^{s-2}.$$

Hence, by (5.17), we have

$$\begin{aligned}
|R(F, G)|_T &= \left\{ \prod_{1 \leqslant n < p < q \leqslant r} \prod_{1 \leqslant i < j < k \leqslant s} |R(F_{npq}, G_{ijk})|_T \right\}^{1/\binom{r-1}{2}\binom{s-1}{2}} \\
&\gg \left\{ \left(\prod_{1 \leqslant i < j < k \leqslant s} \prod_{1 \leqslant n < p < q \leqslant r} |D(F_{npq})|_T \right) \right. \\
&\qquad \left. \cdot \left(\prod_{1 \leqslant n < p < q \leqslant r} \prod_{1 \leqslant i < j < k \leqslant s} |D(G_{ijk})|_T \right) \right\}^{(3/34 - 3\varepsilon/2)/\binom{r-1}{2}\binom{s-1}{2}} \\
&= \left\{ |D(F)|_T^{(r-2)\binom{s}{3}} |D(G)|_T^{(s-2)\binom{r}{3}} \right\}^{(3/34 - 3\varepsilon/2)/\binom{r-1}{2}\binom{s-1}{2}} \\
&= \left(|D(F)|_T^{s/(r-1)} |D(G)|_T^{r/(s-1)} \right)^{1/17 - \varepsilon}.
\end{aligned}$$

Since $|x|_T = |x|_S$ for $x \in K$, this implies Theorem 1A.

Acknowledgements

The authors are indebted to the referee for his helpful criticism.

References

[1] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc.* 25 (1972) 385–394.

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

[3] J. H. Evertse, On sums of *S*-units and linear recurrences, *Compositio Math.* 53 (1984) 225–244.

[4] J. H. Evertse and K. Győry, Thue-Mahler equations with a small number of solutions, *J. Reine Angew. Math.* 399 (1989) 60–80.

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

[6] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, On *S*-unit equations in two unknowns, *Invent. Math.* 92 (1988), 461–477.

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

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

[9] K. Győry, On arithmetic graphs associated with integral domains, in: *A Tribute to Paul Erdős* (eds. A. Baker, B. Bollobás, A. Hajnal), pp. 207–222. Cambridge University Press, 1990.

[10] K. Győry, On the number of pairs of polynomials with given resultant or given semi-resultant, to appear.

[11] M. Laurent, Equations diophantiennes exponentielles, *Invent. Math.* 78 (1984) 299–327.

[12] H. P. Schlickewei, The p-adic Thue-Siegel-Roth-Schmidt theorem, *Archiv der Math.* 29 (1977) 267–270.

[13] W. M. Schmidt, Inequalities for resultants and for decomposable forms, in: *Diophantine Approximation and its Applications* (ed. C. F. Osgood), pp. 235–253, Academic Press, New York, 1973.

[14] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Math. 785, Springer-Verlag, 1980.

[15] E. Wirsing, On approximations of algebraic numbers by algebraic numbers of bounded degree, in: *Proc. Symp. Pure Math.* 20 (1969 Number Theory Institute; ed. D. J. Lewis), pp. 213–247, Amer. Math. Soc., Providence, 1971.