Lower bounds for resultants II.

Jan-Hendrik Evertse

Abstract. Let $F(X,Y)$, $G(X,Y)$ be binary forms in $\mathbf{Z}[X,Y]$ of degrees $r \geq 3, s \geq 3$, respectively, such that FG has no multiple factors. For each matrix $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})$, define $F_U(X,Y) = F(aX + bY, cX + dY)$, and define G_U similarly. We will show that there is a matrix $U \in GL_2(\mathbf{Z})$ such that for the resultant $R(F,G)$ of F, G we have $|R(F,G)| \geq C \cdot (H(F_U)^s H(G_U)^r)^{1/718}$, where $H(F_U)$, $H(G_U)$ denote the heights (maxima of absolute values of the coefficients) of F_U, G_U, respectively, and where C is some *ineffective* constant, depending on r, s and the splitting field of FG. A slightly weaker result was announced without proof in [3] (Theorem 3). We will also prove a p-adic generalisation of the result mentioned above. As a consequence, we will obtain under certain technical restrictions a symmetric improvement of Liouville's inequality for the difference of two algebraic numbers. In our proofs we use some results from [4], [5], and the latter were proved by means of Schlickewei's p-adic generalisation of Schmidt's Subspace theorem.

1991 Mathematics Subject Classification: 11J68, 11C08.

1. Introduction.

Let $F(X,Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$, $G(X,Y) = b_0X^s + b_1X^{s-1}Y + \cdots + b_sY^s$ be two binary forms with coefficients in some field K of characteristic 0. The resultant $R(F,G)$ of F and G is defined by the determinant of order $r+s$,

$$R(F,G) = \begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_r & & & & \\ & a_0 & a_1 & \cdots & \cdots & a_r & & & \\ & & \ddots & & & & \ddots & & \\ & & & a_0 & a_1 & \cdots & \cdots & a_r & \\ b_0 & b_1 & \cdots & b_s & & & & & \\ & b_0 & b_1 & \cdots & b_s & & & & \\ & & \ddots & & & \ddots & & & \\ & & & \ddots & & & \ddots & & \\ & & & & b_0 & b_1 & \cdots & b_s & \end{vmatrix}, \tag{1.1}$$

of which the first s rows consist of coefficients of F and the last r rows of coefficients of G. Both F, G can be factored into linear forms with coefficients in the algebraic closure of K, i.e.

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

and we have

$$R(F,G)=\prod_{i=1}^{r}\prod_{j=1}^{s}(\alpha_i\delta_j-\beta_i\gamma_j)\ . \tag{1.2}$$

Hence $R(F,G)=0$ if and only if F,G have a common linear factor. Further, if for a matrix $U=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ with determinant $\det U\neq 0$ we define $F_U(X,Y):=F(aX+bY,cX+dY)$ and similarly G_U, it follows that

$$R(F_U,G_U)=(\det U)^{rs}R(F,G). \tag{1.3}$$

Now assume that F,G have their coefficients in $\mathbf{Z}$. For a polynomial P with coefficients in $\mathbf{Z}$, we define its height $H(P)$ to be the maximum of the absolute values of the coefficients of P. From (1.1) and Hadamard's inequality it follows that

$$|R(F,G)|\leq (r+1)^{s/2}(s+1)^{r/2}H(F)^sH(G)^r\ .$$

On the other hand, there are some results in the literature on lower bounds for $|R(F,G)|$ which have been obtained by applying Diophantine approximation techniques. To state these results, we need some terminology. A binary form is called *square-free* if it is not divisible by the square of any non-constant binary form. The *splitting field* over a field K of a binary form with coefficients in K is the smallest extension of K over which this binary form factors into linear forms. By $C_1^{\rm ineff}(\ )$, $C_2^{\rm ineff}(\ ),\ldots$ we denote ineffective positive constants depending only on the parameters between the parentheses.

Improving on a result of Wirsing [14], Schmidt [12] proved that if r,s are integers with $r>2s>0$ and if F is a square-free binary form of degree r in $\mathbf{Z}[X,Y]$ without irreducible factors of degree $\leq s$, then for every binary form $G\in\mathbf{Z}[X,Y]$ of degree s which is coprime with F one has

$$|R(F,G)|\geq C_1^{\rm ineff}(r,s,F,\varepsilon)H(G)^{r-2s-\varepsilon}\quad\text{for } \varepsilon>0, \tag{1.4}$$

where the dependence of C_1 on F is unspecified. From Theorem 4.1 of Ru and Wong [9] it follows that (1.4) holds true without the constraint that F have no irreducible factors of degree $\leq s$. Győry and the author ([5], Theorem 1) proved that for each pair of binary forms F,G with coefficients in $\mathbf{Z}$ such that $\deg F=r\geq 3$, $\deg G=s\geq 3$, FG has splitting field L over K and FG is square-free one has

$$|R(F,G)|\geq C_2^{\rm ineff}(r,s,L,\varepsilon)\big(|D(F)|^{\frac{s}{r-1}}|D(G)|^{\frac{r}{s-1}}\big)^{\frac{1}{17}-\varepsilon}\quad\text{for } \varepsilon>0\ , \tag{1.5}$$

where $D(F)$, $D(G)$ denote the discriminants of F,G. We recall that if $F(X,Y)=\prod_{i=1}^{r}(\alpha_iX+\beta_iY)$ then $D(F)=\prod_{1\leq i<j\leq r}(\alpha_i\beta_j-\alpha_j\beta_i)^2$. Győry and the author showed also in [5] that if $r\leq 2$ or $s\leq 2$ or if we allow the splitting field of FG to vary, then $|D(F)|$, $|D(G)|$ may grow arbitrarily large while $|R(F,G)|$ remains

bounded. For more information on lower bounds for resultants and on applications we refer to [4], [5].

Our aim is to derive instead of (1.5) a lower bound for $|R(F,G)|$ which is a function increasing in both $H(F)$ and $H(G)$. In general such a lower bound does not exist. Namely, (1.3) implies that

$$|R(F_U,G_U)| = |R(F,G)| \quad \text{for } U \in GL_2(\mathbf{Z}) \ , \tag{1.6}$$

(where $GL_2(\mathbf{Z}) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) : \ a,b,c,d \in \mathbf{Z}, ad-bc = \pm 1\}$) while $H(F_U)$, $H(G_U)$ may be arbitrarily large for varying U. However, assuming that $r \geq 3, s \geq 3$, we can show that there is an $U \in GL_2(\mathbf{Z})$ such that $|R(F,G)|$ is bounded from below by a function increasing in both $H(F_U)$, $H(G_U)$. The next result, with exponent $1/760$ instead of $1/718$, was stated without proof in [3], Theorem 3.

Theorem 1. *Let $r \geq 3, s \geq 3$, and let (F,G) be a pair of binary forms with coefficients in $\mathbf{Z}$ such that $\deg F = r$, $\deg G = s$, FG is square-free and FG has splitting field L over $\mathbf{Q}$. Then there is an $U \in GL_2(\mathbf{Z})$ such that*

$$|R(F,G)| \geq C_3^{\text{ineff}}(r,s,L)\big(H(F_U)^s H(G_U)^r\big)^{1/718} \ . \tag{1.7}$$

Remark. Similarly as for (1.5), the conditions $r \geq 3$, $s \geq 3$, as well as the dependence of C_3 on L, are necessary. Namely, the discriminant of a binary form F of degree r is a homogeneous polynomial of degree $2r-2$ in the coefficients of F, and for $U \in GL_2(\mathbf{Z})$ one has $|D(F_U)| = |D(F)|$. Therefore, there is a constant $c(r)$ such that $|D(F)| \leq c(r)\{\inf_{U \in GL_2(\mathbf{Z})} H(F_U)\}^{2r-2}$. Now, by the result from [5] mentioned above, if $r \leq 2$ or $s \leq 2$ or if we allow the splitting field of FG to vary, then $|D(F)|$, $|D(G)|$, and hence $\inf_{U \in GL_2(\mathbf{Z})} H(F_U)$, $\inf_{U \in GL_2(\mathbf{Z})} H(G_U)$ may grow arbitrarily large while $|R(F,G)|$ remains bounded.

The proof of Theorem 1 ultimately depends on Schmidt's Subspace theorem, which explains the ineffectivity of the constant C_3. It would be a remarkable breakthrough to obtain an effective lower bound for $|R(F,G)|$ which is a function increasing in both $H(F_U)$ and $H(G_U)$ for some $U \in GL_2(\mathbf{Z})$.

We also prove a p-adic generalisation of Theorem 1. To state this, we have to introduce some further terminology. Let K be an algebraic number field. Denote by $\mathcal{O}_K$ the ring of integers of K. The set of places M_K of K consists of the isomorphic embeddings $\sigma : K \hookrightarrow \mathbf{R}$ which are called real infinite places; the pairs of complex conjugate isomorphic embeddings $\{\sigma, \overline{\sigma} : K \hookrightarrow \mathbf{C}\}$ which are called complex infinite places; and the prime ideals of $\mathcal{O}_K$ which are called finite places. We define absolute values $|*|_v$ ($v \in M_K$) normalised with respect to K as follows:

$|*|_v = |\sigma(*)|^{1/[K:\mathbf{Q}]}$ if $v = \sigma$ is a real infinite place;
$|*|_v = |\sigma(*)|^{2/[K:\mathbf{Q}]} = |\overline{\sigma}(*)|^{2/[K:\mathbf{Q}]}$ if $v = \{\sigma, \overline{\sigma}\}$ is a complex infinite place;
$|*|_v = (N\wp)^{-\mathrm{ord}_\wp(*)/[K:\mathbf{Q}]}$ if $v = \wp$ is a finite place, i.e. prime ideal of $\mathcal{O}_K$,

where $N\wp = \#(\mathcal{O}_K/\wp)$ denotes the norm of $\wp$ and $\mathrm{ord}_\wp(x)$ is the exponent of $\wp$ in the prime ideal decomposition of (x), with $\mathrm{ord}_\wp(0) = \infty$. These absolute values satisfy the *Product formula*

$$\prod_{v \in M_K} |x|_v = 1 \quad \text{for } x \in K^*.$$

For any finite extension L of K, we define absolute values $|*|_w$ ($w \in M_L$) normalised with respect to L in an analogous manner. Thus, if $w \in M_L$ lies above $v \in M_K$, then the restriction of $|*|_w$ to K is equal to $|*|_v^{[L_w:K_v]/[L:K]}$, where K_v, L_w denote the completions of K at v, L at w, respectively. We will frequently use the *Extension formula*

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

so in particular

$$\prod_{w|v} |x|_w = |x|_v \quad \text{for } x \in K,\ v \in M_K,$$

where the product is taken over all places $w \in M_L$ lying above v.

Now let S be a finite set of places on K, containing all (real and complex) infinite places. The ring of S-integers and its unit group, the group of S-units, are defined by

$$\mathcal{O}_S = \{x \in K : |x|_v \le 1 \ \text{ for } v \notin S\}, \quad \mathcal{O}_S^* = \{x \in K : |x|_v = 1 \ \text{ for } v \notin S\},$$

respectively, where '$v \notin S$' means '$v \in M_K \backslash S$.' We put

$$|x|_S := \prod_{v \in S} |x|_v \quad \text{for } x \in K\ .$$

Thus,

$$|x|_S > 1 \quad \text{for } x \in \mathcal{O}_S,\ x \neq 0,\ x \notin \mathcal{O}_S^*, \qquad |x|_S = 1 \quad \text{for } x \in \mathcal{O}_S^*\ . \tag{1.8}$$

We define the truncated height H_S by

$$H_S(\mathbf{x}) = H_S(x_1, \ldots, x_n) = \prod_{v \in S} \max(|x_1|_v, \ldots, |x_n|_v) \quad \text{for } \mathbf{x} = (x_1, \ldots, x_n) \in K^n\ .$$

For a polynomial P with coefficients in K we put $H_S(P) := H_S(p_1, \ldots, p_t)$, where $p_1, \ldots, p_t$ are the coefficients of P. By (1.8) we have

$$H_S(\mathbf{x}) \ge 1 \quad \text{for } \mathbf{x} \in \mathcal{O}_S^n \backslash \{\mathbf{0}\}, \tag{1.9}$$

$$H_S(u\mathbf{x}) = H_S(\mathbf{x}) \quad \text{for } \mathbf{x} \in \mathcal{O}_S^n \backslash \{\mathbf{0}\}, \quad u \in \mathcal{O}_S^*. \tag{1.10}$$

Further, one can show that for every $A > 0$ the set of vectors $\mathbf{x} \in \mathcal{O}_S^n$ with $H_S(\mathbf{x}) \le A$ is the union of finitely many "$\mathcal{O}_S^*$-cosets" $\{u\mathbf{y} :\ u \in \mathcal{O}_S^*\}$ with $\mathbf{y} \in \mathcal{O}_S^n$ fixed.

(1.3) and (1.8) imply that for binary forms F, G with coefficients in $\mathcal{O}_S$ we have

$$|R(F_U, G_U)|_S = |R(F, G)|_S \quad \text{for } U \in GL_2(\mathcal{O}_S)\ , \tag{1.11}$$

where $GL_2(\mathcal{O}_S) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathcal{O}_S, ad - bc \in \mathcal{O}_S^*\}$. We prove the following generalisation of Theorem 1:

Theorem 2. *Let $r \geq 3, s \geq 3$, and let (F, G) be a pair of binary forms with coefficients in $\mathcal{O}_S$ such that $\deg F = r$, $\deg G = s$, FG is square-free and FG has splitting field L over K. Then there is an $U \in GL_2(\mathcal{O}_S)$ such that*

$$|R(F, G)|_S \geq C_4^{\text{ineff}}(r, s, S, L)\big(H_S(F_U)^s H_S(G_U)^r\big)^{1/718} \ . \tag{1.12}$$

In the proof of Theorem 2 we use a lower bound for resultants in terms of discriminants from [5] which has been proved by means of Schlickewei's p-adic generalisation [10] of Schmidt's Subspace theorem [11], a lower bound for discriminants in terms of heights from [4] which follows from Lang's p-adic generalisation [6] (Chap. 7, Thm. 1.1) of Roth's theorem [8], and also a 'semi-effective' result on Thue-Mahler equations, stated below, which follows also from the p-adic generalisation of Roth's theorem.

Theorem 3. *Let $F(X, Y) \in \mathcal{O}_S[X, Y]$ be a square-free binary form of degree $r \geq 3$ with splitting field M over K and let $A \geq 1$. Then every solution $(x, y) \in \mathcal{O}_S^2$ of*

$$|F(x, y)|_S = A \tag{1.13}$$

satisfies

$$H_S(x, y) \leq C_5^{\text{ineff}}(r, S, M, \varepsilon) \cdot (H_S(F) \cdot A)^{\frac{3}{r}+\varepsilon} \quad \textit{for every } \varepsilon > 0 \ . \tag{1.14}$$

Using the techniques from the paper of Bombieri and van der Poorten [1] it is probably possible to derive instead of (1.14) an upper bound

$$H_S(x, y) \leq C_6^{\text{ineff}}(r, S, M, \varepsilon) \cdot H_S(F)^{c(r,\varepsilon)} A^{\frac{1}{r-2}+\varepsilon} \quad \text{for every } \varepsilon > 0 \ ,$$

where $c(r, \varepsilon)$ is a function increasing in r, ε^{-1}.

We derive from Theorem 2 a symmetric improvement of Liouville's inequality. The (absolute) height of an algebraic number ξ is defined by

$$h(\xi) = \prod_{v \in M_K} \max(1, |\xi|_v),$$

where K is any number field containing ξ. By the Extension formula, this height is independent of the choice of K.

Let K be an algebraic number field and ξ, η numbers algebraic over K with $\xi \neq \eta$. Put $L = K(\xi, \eta)$. Further, let T be a finite set of places on L (not necessarily containing all infinite places). By the Product formula we have

$$\prod_{w \in T} \frac{|\xi - \eta|_w}{\max(1, |\xi|_w) \max(1, |\eta|_w)} = \Big(\prod_{w \notin T} \frac{\max(1, |\xi|_w) \max(1, |\eta|_w)}{|\xi - \eta|_w}\Big) h(\xi)^{-1} h(\eta)^{-1}$$

$$\geq \frac{1}{2}\big(h(\xi)h(\eta)\big)^{-1} , \tag{1.15}$$

where as usual, the absolute values $|*|_w$ are normalised with respect to L. The latter is known as Liouville's inequality. Under certain hypotheses we can improve upon the exponent -1. Assume that

$$\left.\begin{array}{l} L = K(\xi,\eta); \\ [K(\xi):K] \geq 3,\ [K(\eta):K] \geq 3; \\ [L:K] = [K(\xi):K][K(\eta):K], \end{array}\right\} \tag{1.16}$$

i.e. $K(\xi),\ K(\eta)$ are linearly disjoint over K. Further, let T be a finite set of places on L such that if S is the set of places on K lying below those in T then

$$W := \max_{v\in S} \frac{1}{[L:K]} \sum_{\substack{w\in T\\ w|v}} [L_w : K_v] < \frac{1}{3} , \tag{1.17}$$

where for each place $v \in S$, the sum is taken over those places $w \in T$ that lie above v.

Theorem 4. *Assuming that ξ,η,L,T satisfy (1.16), (1.17) we have*

$$\prod_{w\in T} \frac{|\xi-\eta|_w}{\max(1,|\xi|_w)\max(1,|\eta|_w)} \geq C_7^{\text{ineff}}(L,T)\cdot\big(h(\xi)h(\eta)\big)^{-1+\delta} \tag{1.18}$$

$$\textit{with}\quad \delta = \frac{1}{718}\cdot\frac{1-3W}{1+3W} .$$

For instance, suppose that L,ξ,η satisfy (1.16) with $K=\mathbf{Q}$ and that T is a subset of the set of infinite places on L, satisfying (1.17) with $K=\mathbf{Q}$ and with S consisting of the only infinite place of $\mathbf{Q}$. Inequality (1.18) has been stated in terms of absolute values normalised with respect to L and we will "renormalise" these to $\mathbf{Q}$. Each $w\in T$ is either an isomorphic embedding of L into $\mathbf{R}$ and then $L_w=\mathbf{R}$; or a pair of complex conjugate embeddings of L into $\mathbf{C}$ and then $L_w=\mathbf{C}$. Therefore, the union of all places $w\in T$ is a collection Σ of isomorphic embeddings of L into $\mathbf{C}$ such that with an isomorphic embedding also its complex conjugate belongs to Σ and moreover, the quantity W of (1.17) is precisely $\#\Sigma/[L:\mathbf{Q}]$. We recall that if $w=\sigma$ is real then $|*|_w = |\sigma(*)|^{1/[L:\mathbf{Q}]}$ while if $w=\{\sigma,\overline{\sigma}\}$ is complex then $|*|_w = (|\sigma(*)|\cdot|\overline{\sigma}(*)|)^{1/[L:\mathbf{Q}]}$. This implies that the left-hand side of (1.18) equals $\prod_{\sigma\in\Sigma}\big(|\sigma(\xi-\eta)|/\max(1,|\sigma(\xi)|)\max(1,|\sigma(\eta)|)\big)^{1/[L:\mathbf{Q}]}$. For an algebraic number ξ, we define $\tilde{H}(\xi)$ to be the maximum of the absolute values of the coefficients of the minimal polynomial of ξ over $\mathbf{Z}$. Then $h(\xi)^{\deg\xi} \leq c\tilde{H}(\xi)$ where c depends only on the degree of ξ (cf. [6], Chap. 3, §2, Prop. 2.5). Thus, Theorem 4 implies the following:

Corollary. *Let ξ, η be algebraic numbers of degrees $r\geq 3$, $s\geq 3$, respectively, such that the field $L=\mathbf{Q}(\xi,\eta)$ has degree rs. Further, let Σ be a collection of isomorphic embeddings of L into $\mathbf{C}$ such that if $\sigma\in\Sigma$ then also $\overline{\sigma}\in\Sigma$, and such* *that* $W := \#\Sigma/[L:\mathbf{Q}] < \frac{1}{3}$. *Put* $\delta = \frac{1}{718}\frac{1-3W}{1+3W}$. *Then*

$$\prod_{\sigma\in\Sigma} \frac{|\sigma(\xi-\eta)|}{\max(1,|\sigma(\xi)|)\max(1,|\sigma(\eta)|)} \geq C_8^{\mathrm{ineff}}(L)\cdot\left(\tilde{H}(\xi)^{-s}\tilde{H}(\eta)^{-r}\right)^{1-\delta}. \tag{1.19}$$

For instance, assume that $L\subset\mathbf{R}$ and take $\Sigma=\{\text{identity}\}$. Then $[L:\mathbf{Q}] = rs \geq 9$ and hence $W\leq\frac{1}{9}$. So by (1.19) we have

$$\frac{|\xi-\eta|_w}{\max(1,|\xi|_w)\max(1,|\eta|_w)} \geq C_9^{\mathrm{ineff}}(L)\cdot\left(\tilde{H}(\xi)^{-s}\tilde{H}(\eta)^{-r}\right)^{\frac{1435}{1436}}. \tag{1.20}$$

If $L\subset\mathbf{C}$, $L\not\subset\mathbf{R}$ then with $\Sigma=\{\text{identity, complex conjugation}\}$ we have $W\leq\frac{2}{9}$ and so (1.19) gives

$$\left(\frac{|\xi-\eta|_w}{\max(1,|\xi|_w)\max(1,|\eta|_w)}\right)^2 \geq C_{10}^{\mathrm{ineff}}(L)\cdot\left(\tilde{H}(\xi)^{-s}\tilde{H}(\eta)^{-r}\right)^{\frac{3589}{3590}}. \tag{1.21}$$

Results similar to (1.20), (1.21) with better exponents were derived in [3] (Corollary 3, (i)).

For an inequality of type (1.18) with $\delta>0$ to hold it is certainly necessary to impose some conditions on ξ,η,L,T but (1.16), (1.17) are probably far too strong. Using for instance geometry of numbers over the adeles of a number field one may prove a generalisation of Dirichlet's theorem of the sort that for a number field M, a number η of degree 2 over M and a finite set of places T on $L:=M(\eta)$ satisfying some mild conditions, there is a constant $c=c(\eta,M,T)$ such that the inequality

$$\prod_{w\in T}\frac{|\xi-\eta|_w}{\max(1,|\xi|_w)} \leq ch(\xi)^{-1}$$

has infinitely many solutions in $\xi\in M$. Thus, for an inequality of type (1.18) to hold it is probably necessary to assume that $[L:K(\xi)]\geq 3$, $[L:K(\eta)]\geq 3$.

The following example shows that the condition $W<1$ is necessary. Assume that $W=1$. Then there is a place v on K such that T contains all places on L lying above v. Fix two elements ξ_0, η_0 of L such that $L=K(\xi_0,\eta_0)$, $[K(\xi_0):K]\geq 3$, $[K(\eta_0):K]\geq 3$ and $[L:K]=[K(\xi_0):K][K(\eta_0):K]$. Let $\gamma_1,\gamma_2,\ldots$ be a sequence of elements from K such that $\lim_{i\to\infty}|\gamma_i|_v=\infty$. By the strong approximation theorem, there exists for every i an $\alpha_i\in K$ such that $|\alpha_i-\gamma_i|_v<1$ and $|\alpha_i|_{v'}\leq 1$ for every place $v'\neq v$ on K. Now put $\xi_i:=\xi_0+\alpha_i$, $\eta_i:=\eta_0+\alpha_i$ for $i=1,2,\ldots$. Then for all places $w\in M_L$ lying outside a finite collection depending only on ξ_0, η_0 we have $|\xi_i|_w\leq 1$, $|\eta_i|_w\leq 1$, while for the remaining places on L not lying above v we have $|\xi_i|_w\ll 1$, $|\eta_i|_w\ll 1$ for $i=1,2\ldots$, where the constants implied by $\ll$, $\gg$ depend only on ξ_0, η_0. Further, for $w\in M_L$ lying above v we have $|\xi_i|_w\gg|\alpha_i|_w\gg|\gamma_i|_w$, $|\eta_i|_w\gg|\gamma_i|_w$ for i sufficiently large. Therefore, by the Extension formula, $h(\xi_i)\gg\ll\prod_{w|v}\max(1,|\xi_i|_w)\gg|\gamma_i|_v\to\infty$ for $i\to\infty$ and similarly, $h(\eta_i)\gg\ll\prod_{w|v}\max(1,|\eta_i|_w)\gg|\gamma_i|_v\to\infty$ for $i\to\infty$, where the products are taken over the places $w\in M_L$ lying above v. Moreover, since

$\xi_i - \eta_i = \xi_0 - \eta_0$ we have

$$\prod_{w\in T} \frac{|\xi_i-\eta_i|_w}{\max(1,|\xi_i|_w)\max(1,|\eta_i|_w)} \ll \prod_{w|v} \frac{|\xi_0-\eta_0|_w}{\max(1,|\xi_i|_w)\max(1,|\eta_i|_w)}$$
$$\ll \big(h(\xi_i)h(\eta_i)\big)^{-1} \quad \text{for } i=1,2,\dots\ .$$

2. Proof of Theorem 3.

As in Section 1, K is an algebraic number field and S a finite set of places on K containing all infinite places. Further, $F(X,Y)$ is a square-free binary form of degree $r \geq 3$ with coefficients in $\mathcal{O}_S$ and A a real ≥ 1. We assume that

$$F(X,Y) = \prod_{i=1}^{r}(\alpha_i X + \beta_i Y) \quad \text{with } \alpha_i, \beta_i \in \mathcal{O}_S \text{ for } i=1,\dots,r\ . \tag{2.1}$$

This is no loss of generality. Namely, suppose that F has splitting field M over K. Thus, $F(X,Y) = \prod_{i=1}^{r}(\alpha_i' X + \beta_i' Y)$ with $\alpha_i', \beta_i' \in M$. Let L be the Hilbert class field of M/K and T the set of places on L lying above those in S. Then for $i=1,\dots,r$, the fractional ideal with respect to $\mathcal{O}_T$ generated by α_i', β_i' is principal and since F has its coefficients in $\mathcal{O}_S$ this implies that F can be factored as in (2.1) but with $\alpha_i, \beta_i \in \mathcal{O}_T$. From the Extension formula it follows that for $(x,y) \in \mathcal{O}_S^2$ we have $|F(x,y)|_T = |F(x,y)|_S$, $H_T(x,y) = H_S(x,y)$ and that also $H_T(F) = H_S(F)$, where $|*|_T = \prod_{w\in T} |*|_w$, $H_T(*,\dots,*) = \prod_{w\in T}\max(|*|_w,\dots,|*|_w)$. So, if we have proved that for all $(x,y) \in \mathcal{O}_T^2$ with $|F(x,y)|_T = A$ and all $\varepsilon > 0$ we have $H_T(x,y) \leq C_{11}^{\text{ineff}}(r,T,L,\varepsilon)\big(H_T(F)A\big)^{\frac{3}{r}+\varepsilon}$, then Theorem 3 readily follows, on observing that T, L are uniquely determined by S, M.

In the proof of Theorem 3 we need some lemmas. The first lemma is fundamental for everything in this paper:

Lemma 1. *Let $x_0,\dots,x_n$ be non-zero elements of $\mathcal{O}_S$ such that*

$$x_0 + \dots + x_n = 0,$$
$$\sum_{i\in I} x_i \neq 0 \ \textit{for each proper nonempty subset } I \textit{ of } \{0,\dots,n\}.$$

Then for all $\varepsilon > 0$ we have

$$H_S(x_0,\dots,x_n) \leq C_{12}^{\text{ineff}}(K,S,\varepsilon)\cdot \Big|\prod_{i=0}^{n} x_i\Big|_S^{1+\varepsilon}.$$

Proof. Lemma 1 in this form appeared in Laurent's paper [7]. It is a reformulation of Theorem 2 of [2]. For $n=2$, Lemma 1 follows from the p-adic generalisation of Roth's theorem [6] (Chap. 7, Thm. 1.1) and for $n>2$ from Schlickewei's p-adic generalisation [10] of Schmidt's Subspace theorem [11]. The constant C_{11}

(and also each other constant in this paper) is ineffective because the Subspace theorem is ineffective. In fact, we need Lemma 1 only for $n = 2$ in which case the non-vanishing subsum condition is void. However, Lemma 1 with $n > 2$ has been used in the proof of a result from [5] which we will need in the present paper. □

For a polynomial P with coefficients in K and for $v \in M_K$ we define $|P|_v := \max(|p_1|_v, \dots, |p_t|_v)$ where $p_1, \dots, p_t$ are the coefficients of P.

Lemma 2. *Let $F(X,Y) = \prod_{i=1}^r (\alpha_i X + \beta_i Y)$ with $\alpha_i, \beta_i \in \mathcal{O}_S$ for $i = 1, \dots, r$. There is a constant c depending only on r and K such that*

$$c^{-1} \prod_{i=1}^r H_S(\alpha_i, \beta_i) \leq H_S(F) \leq c \prod_{i=1}^r H_S(\alpha_i, \beta_i) \ . \tag{2.2}$$

Proof. According to, for instance [6], Chap. 3, §2, we have for any polynomials $P_1, \dots, P_r \in K[X_1, \dots, X_n]$, $v \in M_K$ that

$$c_v^{-1} |P_1 \cdots P_r|_v \leq |P_1|_v \cdots |P_r|_v \leq c_v |P_1 \cdots P_r|_v \text{ if } v \text{ is infinite,}$$
$$|P_1 \cdots P_r|_v = |P_1|_v \cdots |P_r|_v \text{ if } v \text{ is finite,}$$

where each c_v is a constant > 1 depending only on r, n, K. Now Lemma 2 follows by applying this with $P_i(X,Y) = \alpha_i X + \beta_i Y$ for $i = 1, \dots, r$ and any $v \in S$, and then taking the product over $v \in S$. □

We complete the proof of Theorem 3. Let $F(X,Y)$ be a square-free binary form of degree $r \geq 3$ satisfying (2.1) and let $\varepsilon > 0$. Put $\varepsilon' := \varepsilon/10$. In what follows, the constants implied by $\ll$ will be ineffective and depending only on K, S, r, ε. Define

$$\Delta_{ij} := \alpha_i \beta_j - \alpha_j \beta_i \quad \text{for } i, j = 1, \dots, r \ .$$

We will use that

$$|\Delta_{ij}|_v \ll \max(|\alpha_i|_v, |\beta_i|_v) \max(|\alpha_j|_v, |\beta_j|_v) \quad \text{for } v \in M_K \tag{2.2}$$

whence, on taking the product over $v \in S$,

$$|\Delta_{ij}|_S \ll H_S(\alpha_i, \beta_i) H_S(\alpha_j, \beta_j) \ . \tag{2.3}$$

Pick three distinct indices i, j, k from $\{1, \dots, r\}$ and define the linear forms

$$A_1 = \Delta_{jk}(\alpha_i X + \beta_i Y), \ A_2 = \Delta_{ki}(\alpha_j X + \beta_j Y), \ A_3 = \Delta_{ij}(\alpha_k X + \beta_k Y).$$

Thus,

$$A_1 + A_2 + A_3 = 0. \tag{2.4}$$

Further,

$$\begin{aligned} \Delta_{ij}\Delta_{jk}\Delta_{ki} \cdot X &= \Delta_{ki}\beta_j A_1 - \Delta_{jk}\beta_i A_2, \\ \Delta_{ij}\Delta_{jk}\Delta_{ki} \cdot Y &= -\Delta_{ki}\alpha_j A_1 + \Delta_{jk}\alpha_i A_2. \end{aligned} \tag{2.5}$$

Let $(x,y)\in\mathcal{O}_S^2$ be a pair satisfying (1.13). Put $a_h := A_h(x,y)$ for $h=1,2,3$. From (2.5) and (2.2) it follows that for $v\in S$,

$$|\Delta_{ij}\Delta_{jk}\Delta_{ki}|_v\max(|x|_v,|y|_v)\ll\Big(\prod_{p\in\{i,j,k\}}\max(|\alpha_p|_v,|\beta_p|_v)\Big)\max(|a_1|_v,|a_2|_v).$$

By taking the product over $v\in S$ we get

$$|\Delta_{ij}\Delta_{jk}\Delta_{ki}|_S H_S(x,y)\ll\Big(\prod_{p\in\{i,j,k\}}H_S(\alpha_p,\beta_p)\Big)\cdot H_S(a_1,a_2)\ .$$

By Lemma 1 and (2.4) we have

$$H_S(a_1,a_2)\le H_S(a_1,a_2,a_3)\ll\Big(|\Delta_{ij}\Delta_{jk}\Delta_{ki}|_S\prod_{p\in\{i,j,k\}}|\alpha_p x+\beta_p y|_S\Big)^{1+\varepsilon'}.$$

By combining these inequalities we obtain

$$\begin{aligned}H_S(x,y)&\ll|\Delta_{ij}\Delta_{jk}\Delta_{ki}|_S^{\varepsilon'}\Big(\prod_{p\in\{i,j,k\}}H_S(\alpha_p,\beta_p)\Big)\prod_{p\in\{i,j,k\}}|\alpha_p x+\beta_p y|_S\Big)^{1+\varepsilon'}\\&\ll\Big(\prod_{p\in\{i,j,k\}}\big(H_S(\alpha_p,\beta_p)\cdot|\alpha_p x+\beta_p y|_S\big)\Big)^{1+3\varepsilon'}\quad\text{in view of (2.3).}\end{aligned}$$

By taking the product over all subsets $\{i,j,k\}$ of $\{1,\dots,r\}$ we get, using Lemma 2 and $\prod_{i=1}^r|\alpha_i x+\beta_i y|_S=A$ which is a consequence of (2.1), (1.13), that

$$\begin{aligned}H_S(x,y)^{\binom{r}{3}}&\ll\Big(\prod_{i=1}^r\big(H_S(\alpha_i,\beta_i)\cdot|\alpha_i x+\beta_i y|_S\big)\Big)^{\binom{r-1}{2}(1+3\varepsilon')}\\&\ll\big(H_S(F)\cdot A\big)^{\binom{r}{3}\cdot(\frac{3}{r}+\varepsilon)}\ .\end{aligned}$$

This proves Theorem 3. □

3. Proof of Theorem 2.

Let again K be an algebraic number field and S a finite set of places on K containing all infinite places. We recall that the discriminant of a binary form $F(X,Y)=\prod_{i=1}^r(\alpha_i X+\beta_i Y)$ is given by $D(F)=\prod_{1\le i<j\le r}(\alpha_i\beta_j-\alpha_j\beta_i)^2$. This implies that $|D(F_U)|_S=|D(F)|_S$ for $U\in GL_2(\mathcal{O}_S)$. We need some results from other papers.

Lemma 3. *Let F be a square-free binary form of degree $r\ge3$ with coefficients in $\mathcal{O}_S$ and with splitting field M over K. Then there is an $U\in GL_2(\mathcal{O}_S)$ such that*

$$|D(F)|_S\ge C_{13}^{\text{ineff}}(r,M,S)H_S(F_U)^{\frac{r-1}{21}}.$$

Proof. This follows from Theorem 2 of [4]. The proof of that theorem uses Lemma 1 mentioned above with $n = 2$ and a reduction theory for binary forms.

I would like to mention here that the reduction theory for binary forms developed in [4] is essentially a special case of a reduction theory for norm forms which was developed some years earlier by Schmidt [13] (for a totally different purpose). I apologize for having overlooked this in [4]. □

Lemma 4. *Let F, G be binary forms of degrees $r \geq 3$, $s \geq 3$, respectively, with coefficients in $\mathcal{O}_S$ such that FG is square-free and FG has splitting field L over K. Then*

$$|R(F,G)|_S \geq C_{14}^{\text{ineff}}(r,s,L,S,\varepsilon)\Big(|D(F)|_S^{\frac{s}{r-1}}|D(G)|_S^{\frac{r}{s-1}}\Big)^{\frac{1}{17}-\varepsilon} \quad \textit{for } \varepsilon > 0.$$

Proof. This is Theorem 1A of [5]. The proof of that theorem uses Lemma 1 with $n > 2$. □

We now prove Theorem 2. We assume that

$$|D(F)|_S^{\frac{s}{r-1}} \leq |D(G)|_S^{\frac{r}{s-1}} \tag{3.1}$$

which is clearly no loss of generality. Let $U \in GL_2(\mathcal{O}_S)$ be the matrix from Lemma 3. We will show that (1.12) holds with this U. Let M be the Hilbert class field of L/K, and T the set of places on M lying above those in S. Thus, we have

$$F_U(X,Y) = \prod_{i=1}^{r}(\alpha_i X + \beta_i Y), \quad G_U(X,Y) = \prod_{j=1}^{s}(\gamma_j X + \delta_j Y)$$
$$\text{with } \alpha_i, \beta_i, \gamma_j, \delta_j \in \mathcal{O}_T \text{ for } i = 1,\ldots,r,\ j = 1,\ldots,s. \tag{3.2}$$

The height H_T and the quantity $|*|_T$ are defined similarly to H_S, $|*|_S$ but with respect to the absolute values $|*|_w$ ($w \in T$). In what follows, the constants implied by $\ll$, $\gg$ will be ineffective and depending only on r, s, L, S and ε, where ε is a positive number depending only on r, s which will later be chosen sufficiently small.

Note that by Lemma 4, (3.1), our choice of U, and Lemma 3 we have

$$\begin{aligned}|R(F,G|_S &\gg \Big(|D(F)|_S^{\frac{s}{r-1}}|D(G)|_S^{\frac{s}{r-1}}\Big)^{\frac{1}{17}-\varepsilon} \gg |D(F)|_S^{\frac{s}{r-1}(\frac{2}{17}-2\varepsilon)} \\ &\gg H_S(F_U)^{s(\frac{2}{357}-\frac{2\varepsilon}{21})}\ .\end{aligned} \tag{3.3}$$

We estimate $H_S(G_U)$ from above. By (1.2), (3.2) we have

$$R(F_U, G_U) = \prod_{i=1}^{r}\prod_{j=1}^{s}(\alpha_i\delta_j - \beta_i\gamma_j) = \prod_{j=1}^{s} F_U(\delta_j, -\gamma_j)\ ,$$

and together with (1.11) and the Extension formula this implies that

$$|R(F,G)|_S = |R(F_U,G_U)|_T = \prod_{j=1}^{s} |F_U(\delta_j,-\gamma_j)|_T \ . \tag{3.4}$$

Further, using that $H_S(F_U) = H_T(F_U)$, $H_S(G_U) = H_T(G_U)$ by the Extension formula, we have

$$H_S(G_U) \ll \prod_{j=1}^{s} H_T(\gamma_j,\delta_j) \ \text{ by (3.2), Lemma 2,} \tag{3.5}$$

$$H_T(\gamma_j,\delta_j) \ll \Big(H_S(F_U)\cdot|F_U(\delta_j,-\gamma_j)|_T\Big)^{\frac{3}{r}+\varepsilon} \ \text{ for } j=1,\dots,s \ \text{ by Theorem 3,} \tag{3.6}$$

where both Lemma 2, Theorem 3 have been applied with M,T replacing K,S. Now (3.4), (3.5), (3.6) together imply

$$H_S(G_U) \ll \Big(H_S(F_U)^s|R(F,G)|_S\Big)^{\frac{3}{r}+\varepsilon}.$$

In combination with (3.3) this gives

$$\begin{aligned} H_S(F_U)^sH_S(G_U)^r &\ll H_S(F_U)^{s(4+r\varepsilon)}|R(F,G)|_S^{3+r\varepsilon} \\ &\ll |R(F,G)|_S^{(4+r\varepsilon)(\frac{2}{357}-\frac{2\varepsilon}{21})^{-1}+3+r\varepsilon} \\ &\ll |R(F,G)|_S^{718} \ \text{ for } \varepsilon \text{ sufficiently small.} \end{aligned}$$

This implies (1.12), whence completes the proof of Theorem 2. □

4. Proof of Theorem 4.

As before, let K be an algebraic number field and S a finite set of places on K containing all infinite places. For a matrix $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with entries in K we define

$$|U|_v := \max(|a|_v,|b|_v,|c|_v,|d|_v) \ \text{ for } v\in M_K \ , \quad H_S(U) = \prod_{v\in S}|U|_v.$$

We need the following elementary lemma:

Lemma 5. *Let $F(X,Y)$ be a square-free binary form of degree $r\geq 3$ with coefficients in $\mathcal{O}_S$ and $U\in GL_2(\mathcal{O}_S)$. Then for some constant c depending only on r and the splitting field of F over K we have*

$$H_S(U) \leq c\cdot\big(H_S(F)H_S(F_U)\big)^{3/r} \ . \tag{4.1}$$

Proof. We prove (4.1) only for binary forms F such that

$$F(X,Y)=\prod_{i=1}^{r}(\alpha_i X+\beta_i Y)\quad\text{with } \alpha_i,\beta_i\in\mathcal{O}_S \text{ for } i=1,\dots,r. \tag{4.2}$$

This is no restriction. Namely, in general F has a factorisation as in (4.2) with $\alpha_i,\beta_i\in\mathcal{O}_T$ where T is the set of places lying above those in S on the Hilbert class field of the splitting field of F over K. Now if we have shown that $H_T(U)\le c\cdot\big(H_T(F)H_T(F_U)\big)^{3/r}$ then (4.1) follows from the Extension formula.

From (4.2) it follows that

$$F_U(X,Y)=\prod_{i=1}^{r}(\alpha_i^* X+\beta_i^* Y)\quad\text{with } (\alpha_i^*,\beta_i^*)=(\alpha_i,\beta_i)U \text{ for } i=1,\dots,r. \tag{4.3}$$

Let $U=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$. Pick three indices i,j,k from $\{1,\dots,r\}$. Then $(a,c,b,d,-1,-1,-1)$ is a solution to the system of six linear equations

$$\begin{pmatrix}\alpha_i&\beta_i&0&0&\alpha_i^*&0&0\\0&0&\alpha_i&\beta_i&\beta_i^*&0&0\\\alpha_j&\beta_j&0&0&0&\alpha_j^*&0\\0&0&\alpha_j&\beta_j&0&\beta_j^*&0\\\alpha_k&\beta_k&0&0&0&0&\alpha_k^*\\0&0&\alpha_k&\beta_k&0&0&\beta_k^*\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\0\\0\end{pmatrix}. \tag{4.4}$$

(4.4) can be reformulated as $-x_5(\alpha_i^*,\beta_i^*)=(\alpha_i,\beta_i)X$, $-x_6(\alpha_j^*,\beta_j^*)=(\alpha_j,\beta_j)X$, $-x_7(\alpha_k^*,\beta_k^*)=(\alpha_k,\beta_k)X$, with $X=\left(\begin{smallmatrix}x_1&x_3\\x_2&x_4\end{smallmatrix}\right)$. It is well-known that up to a constant factor, there is at most one 2×2-matrix mapping three given, pairwise non-proportional vectors to scalar multiples of three given other vectors. Therefore, the solution space of system (4.4) is one-dimensional. One solution to (4.4) is given by $(\Delta_1,-\Delta_2,\dots,\Delta_7)$ where Δ_p is the determinant of the matrix obtained by removing the p-th column of the matrix at the left-hand side of (4.4). Therefore, there is a non-zero $\lambda\in K$ such that $U=\lambda\left(\begin{smallmatrix}\Delta_1&\Delta_3\\-\Delta_2&-\Delta_4\end{smallmatrix}\right)$. Note that $\Delta_1,\dots,\Delta_4$ contain the fifth, sixth, and seventh column of the matrix at the left-hand side of (4.4). Therefore, each of $\Delta_1,\dots,\Delta_4$ is a sum of terms each of which is up to sign a product of six numbers, containing one of α_p,β_p for $p=i,j,k$ and one of α_p^*,β_p^* for $p=i,j,k$. Consequently,

$$\begin{aligned}|U|_v&=|\lambda|_v\max(|\Delta_1|_v,\dots,|\Delta_4|_v)\\&\le c_v\cdot|\lambda|_v\prod_{p=i,j,k}\big(\max(|\alpha_p|_v,|\beta_p|_v)\max(|\alpha_p^*|_v,|\beta_p^*|_v)\big)\quad\text{for } v\in M_K,\end{aligned} \tag{4.5}$$

where for infinite places v, c_v is an absolute constant and for finite places v, $c_v=1$. Let $v\notin S$. Then since $U\in GL_2(\mathcal{O}_S)$ we have $|\det U|_v=1$, whence $|U|_v=1$. Further, $\alpha_p,\beta_p,\alpha_p^*,\beta_p^*\in\mathcal{O}_S$ for $p=i,j,k$, therefore, these numbers have v-adic absolute value ≤ 1. It follows that $|\lambda|_v\ge 1$ for $v\notin S$, and together with the Product formula this implies $|\lambda|_S=\prod_{v\in S}|\lambda|_v\le 1$. Now (4.5) implies, on taking the product over $v \in S$,

$$H_S(U) \le c_1 |\lambda|_S \prod_{p=i,j,k} \big(H_S(\alpha_p,\beta_p) H_S(\alpha_p^*,\beta_p^*)\big)$$
$$\le c_1 \prod_{p=i,j,k} \big(H_S(\alpha_p,\beta_p) H_S(\alpha_p^*,\beta_p^*)\big),$$

where c_1 depends only on K. By taking the product over all subsets $\{i,j,k\}$ of $\{1,\dots,r\}$, on using (4.2), (4.3), Lemma 2, we obtain

$$H_S(U)^{\binom{r}{3}} \le c_2 \big(H_S(F) H_S(F_U)\big)^{\binom{r-1}{2}},$$

where c_2 depends only on K,r. This implies (4.1). □

Lemma 6. *Let M be an extension of K of degree r and T the set of places on M lying above those in S. Denote by $x \mapsto x^{(i)}$ $(i=1,\dots,r)$ the K-isomorphisms of M.*

(i) *Let $F(X,Y) = \prod_{i=1}^r (\alpha^{(i)}X + \beta^{(i)}Y)$, where $\alpha,\beta \in \mathcal{O}_T$. Then $F \in \mathcal{O}_S[X,Y]$ and $H_S(F)^{1/r} \gg\ll H_T(\alpha,\beta)$.*
(ii) *Let $\xi \in M$ with $\xi \neq 0$. Then there are $\alpha,\beta \in \mathcal{O}_T$ such that $\xi = \alpha/\beta$ and such that for the binary form $F(X,Y) = \prod_{i=1}^r (\alpha^{(i)}X + \beta^{(i)}Y)$ we have $H_S(F)^{1/r} \gg\ll h(\xi)$.*

Here the constants implied by $\ll$, $\gg$ depend only on M.

Proof. (i) F has its coefficients in $\mathcal{O}_S$ since $\mathcal{O}_T$ is the integral closure of $\mathcal{O}_S$ in M. Let M' be the normal closure of M/K and T' the set of places on M' lying above those in T. By the Extension formula, we have $H_T(\alpha,\beta) = H_{T'}(\alpha,\beta)$. Further, by the Extension formula and Lemma 2 we have

$$H_S(F) = H_{T'}(F) \gg\ll \prod_{i=1}^r H_{T'}(\alpha^{(i)},\beta^{(i)}).$$

Now M'/K is normal, hence if $w_1,\dots,w_g$ are the places on M' lying above some $v \in M_K$ then for $i=1,\dots,r$, the tuple of absolute values $(|*^{(i)}|_{w_j} : j=1,\dots,g)$ is a permutation of $(|*|_{w_j} : j=1,\dots,g)$. Therefore, $H_{T'}(\alpha^{(i)},\beta^{(i)}) = H_{T'}(\alpha,\beta) = H_T(\alpha,\beta)$ for $i=1,\dots,r$. This implies (i).

(ii) The ideal class of $(1,\xi)$ (the fractional ideal with respect to $\mathcal{O}_M$ generated by $1,\xi$) contains an ideal, contained in $\mathcal{O}_M$, with norm $\ll 1$. This implies that there are $\alpha,\beta \in \mathcal{O}_M$ with $\xi = \alpha/\beta$ such that the ideal (α,β) has norm $\ll 1$. It follows that $\prod_{w \notin T} \max(|\alpha|_w,|\beta|_w) \gg\ll 1$. Now by the Product formula we have $h(\xi) = \prod_{w \in M_M} \max(1,|\xi|_w) = \prod_{w \in M_M} \max(|\alpha|_w,|\beta|_w)$ and so $h(\xi) \gg\ll \prod_{w \in T} \max(|\alpha|_w,|\beta|_w) = H_T(\alpha,\beta)$. Together with (i) this implies (ii). □

We now complete the proof of Theorem 4. Let $L = K(\xi,\eta)$, $r = [K(\xi):K]$, $s = [K(\eta):K]$. Then (1.16) implies that $r \ge 3$, $s \ge 3$, $[L:K] = rs$. Further, let T be a finite set of places on L such that (1.17) holds and S the set of places on K lying below those in T. We add to S all infinite places on K that do not belong to S. Thus, S contains all infinite places and the places lying below those in T. There might be places in S above which there is no place in T but then (1.17) still holds. Denote by T_1 the set of places on L lying above the places in S. Note that T is a proper subset of T_1. In what follows, the constants implied by $\ll$, $\gg$ depend only on L, S. We mention that constants depending on some subfield of L may be replaced by constants depending on L since L has only finitely many subfields.

Denote by $x \mapsto x^{(i)}$ $(i = 1, \dots, r)$ the K-isomorphisms of $K(\xi)$ and by $y \mapsto y^{(j)}$ $(j = 1, \dots, s)$ the K-isomorphisms of $K(\eta)$. From part (ii) of Lemma 6 (applied with $M = K(\xi)$, $M = K(\eta)$, respectively) it follows that there are $\alpha, \beta, \gamma, \delta$ such that $\xi = \frac{\alpha}{\beta}$, $\eta = \frac{\gamma}{\delta}$, where α, β belong to the integral closure of $\mathcal{O}_S$ in $K(\xi)$ and γ, δ to the integral closure of $\mathcal{O}_S$ in $K(\eta)$ and such that for the binary forms

$$F(X,Y) = \prod_{i=1}^{r} (\alpha^{(i)} X + \beta^{(i)} Y), \quad G(X,Y) = \prod_{j=1}^{s} (\gamma^{(j)} X + \delta^{(j)} Y) \tag{4.6}$$

we have

$$H_S(F)^{1/r} \gg\ll h(\xi), \quad H_S(G)^{1/s} \gg\ll h(\eta). \tag{4.7}$$

The forms F, G have their coefficients in $\mathcal{O}_S$, and $\deg F = r \geq 3$, $\deg G = s \geq 3$. Further, since $K(\xi)$, $K(\eta)$ are linearly disjoint over K, the numbers ξ and η are not conjugate over K and so FG is square-free. Hence all hypotheses of Theorem 2 are satisfied. The splitting field of FG is the normal closure of L over K. By Theorem 2 there is a matrix $U \in GL_2(\mathcal{O}_S)$ such that

$$|R(F,G)|_S \gg \Big(H_S(F_U)^s H_S(G_U)^r \Big)^{\frac{1}{718}}. \tag{4.8}$$

By (4.6) we have

$$F_U(X,Y) = \prod_{i=1}^{r} ((\alpha^*)^{(i)} X + (\beta^*)^{(i)} Y), \quad G_U(X,Y) = \prod_{j=1}^{s} ((\gamma^*)^{(j)} X + (\delta^*)^{(j)} Y),$$
$$\text{with } (\alpha^*, \beta^*) = (\alpha, \beta) U, \ (\gamma^*, \delta^*) = (\gamma, \delta) U \ .$$

We define the following quantities:

$$\Lambda_w := \frac{|\xi - \eta|_w}{\max(1, |\xi|_w) \max(1, |\eta|_w)} = \frac{|\alpha\delta - \beta\gamma|_w}{\max(|\alpha|_w|, |\beta|_w) \max(|\gamma|_w, |\delta|_w)} \quad \text{for } w \in T_1,$$
$$\Lambda_w^* := \frac{|\alpha^*\delta^* - \beta^*\gamma^*|_w}{\max(|\alpha^*|_w|, |\beta^*|_w) \max(|\gamma^*|_w, |\delta^*|_w)} \quad \text{for } w \in T_1,$$
$$H := H_S(F)^{1/r} H_S(G)^{1/s}, \quad H^* := H_S(F_U)^{1/r} H_S(G_U)^{1/s}.$$

Thus, (4.7) and (4.8) translate into

$$H \gg\ll h(\xi) h(\eta), \quad |R(F,G)|_S^{1/rs} \gg (H^*)^{\frac{1}{718}}. \tag{4.9}$$

Note that we have to estimate from below $\prod_{w \in T} \Lambda_w$.

For matrices $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and places w on L we put $|A|_w = \max(|a|_w, \dots, |d|_w)$. Let $v \in S$ and $w \in T_1$ a place lying above v. Using that the restriction of $|*|_w$ to K

is $|*|_v^{[L_w:K_v]/[L:K]}$ and also that $\alpha\delta-\beta\gamma=\det U^{-1}(\alpha^*\delta^*-\beta^*\gamma^*)$, $\max(|\alpha|_w,|\beta|_w)\ll |U^{-1}|_w\max(|\alpha^*|_w,|\beta^*|_w)$, $\max(|\gamma|_w,|\delta|_w)\ll|U^{-1}|_w\max(|\gamma^*|_w,|\delta^*|_w)$, we obtain

$$\Lambda_w \gg \frac{|\det U^{-1}|_w}{|U^{-1}|_w^2}\cdot\Lambda_w^* = \Big(\frac{|\det U^{-1}|_v}{|U^{-1}|_v^2}\Big)^{\frac{[L_w:K_v]}{[L:K]}}\cdot\Lambda_w^*\ .$$

Note that by Lemma 5 we have $H_S(U^{-1})\ll\big(H_S(F)H_S(F_U)\big)^{3/r}$ and $H_S(U^{-1})\ll\big(H_S(G)H_S(G_U)\big)^{3/s}$. Hence $H_S(U^{-1})\ll(H\cdot H^*)^{3/2}$. We take the product over $w\in T$. Using (1.17), $|\det U^{-1}|_v/|U^{-1}|_v^2\ll 1$ for $v\in S$ and $\det U\in\mathcal{O}_S^*$ we get

$$\prod_{v\in S}\prod_{\substack{w\in T\\ w|v}}\Big(\frac{|\det U^{-1}|_v}{|U^{-1}|_v^2}\Big)^{\frac{[L_w:K_v]}{[L:K]}} \gg \prod_{v\in S}\Big(\frac{|\det U^{-1}|_v}{|U^{-1}|_v^2}\Big)^W = \Big(\frac{|\det U^{-1}|_S}{H_S(U^{-1})^2}\Big)^W$$
$$\gg (H\cdot H^*)^{-3W}.$$

Hence

$$\prod_{w\in T}\Lambda_w \gg (H\cdot H^*)^{-3W}\prod_{w\in T}\Lambda_w^*\ . \tag{4.10}$$

We need also lower bounds for $\prod_{w\in T_1}\Lambda_w$, $\prod_{w\in T_1}\Lambda_w^*$. Note that since $[L:K]=[K(\xi):K][K(\eta):K]=rs$ we have

$$R(F,G)=\prod_{i=1}^r\prod_{j=1}^s(\alpha^{(i)}\delta^{(j)}-\beta^{(i)}\gamma^{(j)})=N_{L/K}(\alpha\delta-\beta\gamma).$$

Together with the Extension formula this implies

$$|R(F,G)|_v^{1/rs}=\prod_{w|v}|\alpha\delta-\beta\gamma|_w \quad \text{for } v\in M_K,$$

and by applying part (i) of Lemma 6 and (4.9) we obtain

$$\prod_{w\in T_1}\Lambda_w = \frac{|R(F,G)|_S^{1/rs}}{H_{T_1}(\alpha,\beta)H_{T_1}(\gamma,\delta)} \gg \Big(\frac{|R(F,G)|_S}{H_S(F)^sH_S(G)^r}\Big)^{1/rs} = \frac{|R(F,G)|_S^{1/rs}}{H}$$
$$\gg (H^*)^{\frac{1}{718}}H^{-1}. \tag{4.11}$$

Completely similarly we get, in view of (1.11),

$$\prod_{w\in T_1}\Lambda_w^* \gg \frac{|R(F_U,G_U)|_S^{1/rs}}{H^*} = \frac{|R(F,G)|_S^{1/rs}}{H^*} \gg (H^*)^{\frac{1}{718}-1}. \tag{4.12}$$

Take $\theta = \frac{1}{718(1+3W)}$. Then we obtain

$$\begin{aligned}
\prod_{w\in T} \Lambda_w &\gg (H\cdot H^*)^{-3W\theta} \prod_{w\in T}\left(\Lambda_w^{1-\theta}{\Lambda_w^*}^{\theta}\right) \quad \text{by (4.10)}\\
&\gg (H\cdot H^*)^{-3W\theta} \prod_{w\in T_1}\left(\Lambda_w^{1-\theta}{\Lambda_w^*}^{\theta}\right) \quad \text{since } \Lambda_w \ll 1,\ \Lambda_w^* \ll 1 \text{ for } w\in T_1\backslash T\\
&\gg (H\cdot H^*)^{-3W\theta}(H^*)^{(\frac{1}{718}-1)\theta}\left((H^*)^{\frac{1}{718}}H^{-1}\right)^{(1-\theta)} \quad \text{by (4.11), (4.12)}\\
&= H^{-1+(1-3W)\theta}(H^*)^{\frac{1}{718}-(1+3W)\theta} = H^{-1+\delta}\\
&\gg \left(h(\xi)h(\eta)\right)^{-1+\delta} \quad \text{by (4.9)}.
\end{aligned}$$

This completes the proof of Theorem 4. □

References

[1] E. Bombieri, A.J. van der Poorten, Some quantitative results related to Roth's theorem, J. Austral. Math. Soc. (Series A) 45 (1988), 233–248, Corrigenda, ibid. 48 (1990), 154–155.

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

[3] — Estimates for discriminants and resultants of binary forms. In: Advances in Number Theory, Proc. 3rd conf. CNTA, Kingston, 1991 (ed. by F.Q. Gouvêa, N. Yui), 367–380. Clarendon Press, Oxford 1993.

[4] — Estimates for reduced binary forms, J. reine angew. Math. 434 (1993), 159–190.

[5] J.-H. Evertse, K. Győry, Lower bounds for resultants I, Compos. Math. 88 (1993), 1–23.

[6] S. Lang, Fundamentals of Diophantine Geometry. Springer Verlag, New York, Berlin, Heidelberg, Tokyo 1983.

[7] M. Laurent, Equations diophantiennes exponentielles, Invent. math. 78 (1984), 299–327.

[8] K.F. Roth, Rational approximation to algebraic numbers, Mathematika 2 (1955), 1–20.

[9] M. Ru, P.M. Wong, Integral points of $\mathbf{P}^n\backslash\{2n+1$ hyperplanes in general position$\}$, Invent. math. 106 (1991), 195–216.

[10] H.P. Schlickewei, The $\wp$-adic Thue-Siegel-Roth-Schmidt theorem, Archiv der Math. 29 (1977), 267–270.

[11] W.M. Schmidt, Norm form equations, Ann. Math. 96 (1972), 526–551.

[12] — Inequalities for resultants and for decomposable forms. In: Diophantine approximation and its applications, Proc. conf. Washington D.C. 1972 (ed. by C.F. Osgood), 235–253. Academic Press, New York 1973.

[13] — The number of solutions of norm form equations, Trans. Am. Math. Soc. 317 (1990), 197–227.

[14] E. Wirsing, On approximations of algebraic numbers by algebraic numbers of bounded degree. In: Proc. Symp. Pure Math., 1969 Number Theory Inst. (ed. by D.J. Lewis), 213–247. Am. Math. Soc., Providence 1971.