Mathematica Pannonica
4/2 (1993), 169 – 180

ON PAIRS OF BINARY FORMS WITH GIVEN RESULTANT OR GIVEN SEMI-RESULTANT

K. **Győry***

Mathematical Institute, Kossuth Lajos University, H-4010 Debrecen, Hungary

To the memory of
E. Gesztelyi, I. Gönczi and A. Nikodémusz

Received September 1992

AMS Subject Classification: 11 E 76, 11 D 57, 11 D 85

Keywords: Binary forms, resultants, diophantine equations.

Abstract: We prove some finiteness theorems for pairs of binary forms with given semi-resultant ideal over the ring of S-integers of a number field. Our main results imply, in an ineffective form, some finiteness results of [3] on binary forms with given non-zero resultant and some finiteness theorems of [1] and [2] on binary forms with given non-zero discriminant or given non-zero discriminant ideal.

1. Introduction

In our papers [4] and [5], finiteness theorems have been established for pairs of monic polynomials with given non-zero resultant over an integrally closed and finitely generated integral domain A over $\mathbb{Z}$.

*Research partially supported by Hungarian National Foundation for Scientific Research, grant. no. 1641.

Moreover, the results of [5] have been extended to pairs of monic polynomials with given semi-resultant. In the particular case when A is the ring of S-integers O_S of a number field, explicit upper bounds have also been derived for the number of O_S-equivalence classes of pairs under consideration. On the other hand, in our joint paper [3] with Evertse lower bounds have been given for resultants of binary forms over O_S. As a consequence, we obtained in [3] a qualitative finiteness theorem for binary forms with given non-zero resultant over O_S. The purpose of the present paper is to extend this qualitative result to binary forms of given semi-resultant ideal over O_S. Since the semi-resultant ideal is a common generalization of resultant ideal and of discriminant ideal, our finiteness theorems imply both the above-mentioned qualitative finiteness result of [3] and the ineffective and qualitative versions of some finiteness theorems of [2] on binary forms with given non-zero discriminant or given non-zero discriminant ideal. It should, however, be remarked that in our proofs some results of [3] and [2] are involved. Further, in contrast with the theorems of [2] the results of the present paper are ineffective. This is a consequence of the fact that the results of [3] used in our proofs depend on the Thue-Siegel-Roth-Schmidt method and its p-adic generalization.

In Section 2, we introduce some concepts and notations and make some preliminary remarks. Our results are stated in Section 3. Finally, Section 4 is devoted to the proofs.

2. Definitions, notations and preliminary remarks

Let K be an algebraic number field with ring of integers O_K, S a finite (possibly empty) set of prime ideals in O_K, $O_S = \{\alpha \in K : : \mathrm{ord}_{\mathcal{P}}(\alpha) \geq 0$ for all prime ideals $\mathcal{P}$ of O_K with $\mathcal{P} \notin S\}$ the ring of S-integers in K, and O_S^* the group of S-units in O_S. By an O_S-ideal we mean a finitely generated O_S-submodule of K, and by an integral O_S-ideal, an O_S-ideal contained in O_S. The O_S-ideal generated by $\alpha_1, \dots, \alpha_n$ is denoted by $(\alpha_1, \dots, \alpha_n)_S$. If $F \in K[X,Y]$ then $(F)_S$ denotes the O_S-ideal generated by the coefficients of F.

If $F(\mathbf{X}) = F(X,Y)$ and $G(\mathbf{X}) = G(X,Y)$ are non-zero binary forms in $K[X,Y]$ with $\deg F = r$, $\deg G = s$, then they can be factorized as

$$F(\mathbf{X}) = \prod_{i=1}^{r} \ell_i(\mathbf{X}), \quad G(\mathbf{X}) = \prod_{j=1}^{s} \ell'_j(\mathbf{X}), \tag{1}$$

where ℓ_i, ℓ'_j are homogeneous linear polynomials with coefficients in a fixed finite extension, say L, of K. The *resultant* of F and G is defined by

$$R(F,G) = \prod_{i=1}^{r}\prod_{j=1}^{s} \det(\ell_i, \ell'_j) \tag{2}$$

where $\det(\ell_i, \ell'_j)$ denotes the coefficient determinant of $\{\ell_i, \ell'_j\}$. Here it should be remarked that for binary forms F, G with $F(1,0) \neq 0$, $G(1,0) \neq 0$, $R(F,G)$ is just the resultant of the polynomials $F(X,1)$ and $G(X,1)$. In [5] we used the concept of semi-resultant of monic polynomials in one variable which is a generalization of resultant. As far as I know, this concept of semi-resultant cannot be extended in an appropriate way to arbitrary binary forms. Instead we shall define the semi-resultant ideal of binary forms.

The *resultant* O_S*-ideal* of the binary forms $F, G \in K[X,Y]$ is defined (cf. [3]) by

$$\mathcal{R}_S(F,G) = \frac{(R(F,G))_S}{(F)_S^s (G)_S^r}. \tag{3}$$

$\mathcal{R}_S(F,G)$ is an integral O_S-ideal (see [3]). Denote by O_L the ring of integers of L, by T the set of prime ideals of O_L lying above the prime ideals in S, by O_T the ring of T-integers in L, by $(\alpha)_T$ the O_T-ideal in L generated by α, and by $(\ell_i)_T$ the O_T-ideal generated by the coefficients of the linear form ℓ_i. Further, let $I(F,G)$ denote the set of pairs $\{i,j\}$ with $\det(\ell_i, \ell'_j) \neq 0$ for $i = 1, \dots, r$, $j = 1, \dots, s$. We shall show in Section 4 that there exists a non-zero integral O_S-ideal $\mathcal{R}_S^*(F,G)$ such that

$$\mathcal{R}_S^*(F,G) = \prod_{I(F,G)} \frac{(\det(\ell_i, \ell'_j))_T}{(\ell_i)_T (\ell'_j)_T} \tag{4}$$

where the product is taken over all pairs $\{i,j\}$ in $I(F,G)$. $\mathcal{R}_S^*(F,G)$ is called the *semi-resultant* O_S*-ideal* of F and G. We note that by Gauss' lemma (see e.g. Lemma 2 in [2]), $\mathcal{R}_S^*(F,G)$ is independent of the choice of ℓ_i and ℓ'_j in (1). Further, $\mathcal{R}_S^*(F,G) = \mathcal{R}_S(F,G)$ for the case when F, G have no common linear form divisor over L. Finally, if

F is a square-free binary form in $K[X,Y]$ with degree r (i.e. F has no multiple non-constant factor over K) then

$$\mathcal{R}_S^*(F,F) = \frac{(D(F))_S}{(F)_S^{2(r-1)}} \tag{5}$$

which is just the *discriminant* O_S*-ideal* $\mathcal{D}_S(F)$ of F, as defined in [2] (see also [3]). Hence the semi-resultant O_S-ideal is a common generalization of the resultant O_S-ideal and the discriminant O_S-ideal.

It is easy to see that

$$(6)\quad \begin{cases} \mathcal{R}_S(\lambda F,\mu G) = \mathcal{R}_S(F,G) \quad \text{and} \quad \mathcal{R}_S^*(\lambda F,\mu G) = \mathcal{R}_S^*(F,G) \\ \text{for all} \quad \lambda,\mu \in K^* . \end{cases}$$

For any binary form $F \in K[X,Y]$ and for any $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(O_S)$, we put $F_U(X,Y) = F(aX+bY, cX+dY)$. Two pairs (F,G), (F',G') of binary forms in $K[X,Y]$ are called O_S*-equivalent* if $F' = \varepsilon F_U$, $G' = \eta G_U$ for some $\varepsilon,\eta \in O_S^*$ and $U \in SL_2(O_S)$, and *weakly* O_S*-equivalent* if $F' = \lambda F_U$, $G' = \mu G_U$ for some $\lambda,\mu \in K^*$ and $U \in SL_2(O_S)$. It is not difficult to show that if (F,G) and (F',G') are weakly O_S-equivalent then

$$(7)\qquad \mathcal{R}_S(F,G) = \mathcal{R}_S(F',G') \quad \text{and} \quad \mathcal{R}_S^*(F,G) = \mathcal{R}_S^*(F',G') .$$

For every O_S-ideal $\mathcal{A}$ there is a unique O_K-ideal $\mathcal{A}^*$ composed of O_K-prime ideals outside S, such that $\mathcal{A} = \mathcal{A}^* O_S$. We put

$$|\mathcal{A}|_S = N_{K/\mathbb{Q}}(\mathcal{A}^*)^{1/[K:\mathbb{Q}]} .$$

For an integral O_S-ideal $\mathcal{A}$ we have $|\mathcal{A}|_S \geq 1$. If $\mathcal{A}$ is generated by α then we put $|\alpha|_S = |\mathcal{A}|_S$.

3. Results

We keep the notation of Section 2. We shall deal with the solutions of the inequality

$$(8)\qquad |\mathcal{R}_S^*(F,G)|_S \leq M \quad \text{in binary forms} \quad F,G \in K[X,Y] ,$$

where $M \geq 1$ is an arbitrary but fixed constant.

For a binary form $F \in K[X,Y]$, let $\omega(F)$ denote the maximal number of pairwise linearly independent linear factors of F over $\overline{\mathbb{Q}}$. Further, for binary forms $F,G \in K[X,Y]$, we denote by $\omega_G(F)$ the maximal number of pairwise linearly independent linear factors of F over $\overline{\mathbb{Q}}$ which do not divide G, and we define $\omega_F(G)$ similarly. Let L be an arbitrary finite extension of K, and consider those pairs (F,G) of binary forms $F,G \in K[X,Y]$ for which

$$(9)\qquad \begin{cases} \text{(i)} & F,G \text{ factorize into linear forms over } L; \\ \text{(ii)} & \omega(F) \geq 3,\ \omega(G) \geq 3; \\ \text{(iii)} & \max\{\omega_G(F),\ \omega_F(G),\ \omega(gcd(F,G))\} \geq 3. \end{cases}$$

We note that

$$\omega_G(F) \geq 3\,, \quad \omega_F(G) \geq 3$$

imply (ii) and (iii) in (9). Further, if (F,G) satisfies (8) and (9) then so does every pair (F',G') which is weakly O_S-equivalent to (F,G).

Theorem 1. *If (F,G) is a solution of (8) with property (9) then $\omega(F)+$ $+\omega(G) \leq c_1$, where $c_1 = c_1(K,L,S,M)$ is a number depending only on K, L, S and M.*

Theorem 2. *For every $D \geq 2$, there are only finitely many weak O_S-equivalence classes of pairs (F,G) of binary forms with* $\deg F + \deg G \leq$ $\leq D$ *which satisfy* (8) *and* (9).

As Remarks 1 and 2 in [3] show, both assumptions (i) and (ii) of (9) in Ths. 1 and 2 are necessary. Recently Evertse remarked (private communication) that the condition (iii) of (9) can be replaced by the weaker assumption that either $\omega(gcd(F,G)) \geq 3$ or $\omega(F) + \omega(G) -$ $-\omega(gcd(F,G)) \geq 3$.

Consider now those solutions (F,G) of (8) for which F, G are square-free. Then (9) takes the form

$$(10)\qquad \begin{cases} \text{(i)} & F,G \ \text{ factorize into linear forms over } \ L; \\ \text{(ii)} & F,G \ \text{ are square-free;} \\ \text{(iii)} & \deg F \geq 3,\ \deg G \geq 3; \\ \text{(iv)} & \max\left\{\deg\left(\frac{F}{gcd(F,G)}\right),\ \deg\left(\frac{G}{gcd(F,G)}\right),\right. \\ & \qquad \left.\deg\left(gcd(F,G)\right)\right\} \geq 3\,. \end{cases}$$

Ths. 1 and 2 imply the following

Corollary 1. *There are only finitely many weak O_S-equivalence classes of pairs (F,G) of binary forms $F,G \in K[X,Y]$ which satisfy* (8) *and* (10).

As a further consequence, consider the solutions of the inequality

(11) $\quad 0 < |\mathcal{R}_S(F,G)|_S \leq M$ in binary forms $F, G \in K[X,Y]$.

If (F,G) is a solution of (11) then $\omega_G(F) = \omega(F)$, $\omega_F(G) = \omega(G)$ and $|\mathcal{R}_S^*(F,G)|_S = |\mathcal{R}_S(F,G)|_S$. Hence Ths. 1, 2 and Cor. 1 apply immediately to (11). For example, Cor. 1 gives

Corollary 2. *There are only finitely many weak O_S-equivalence classes of pairs (F,G) of square-free binary forms $F, G \in K[X,Y]$ of degree ≥ 3 which satisfy* (11) *and for which FG factorizes into linear factors over L.*

Next consider the solutions of the inequality

(12) $\quad 0 < |R(F,G)|_S \leq M$ in binary forms $F, G \in O_S[X,Y]$.

If (F,G) is a solution of (12) then so is every (F', G') which is O_S-equivalent to (F,G). From Cor. 2 we shall deduce the following

Corollary 3. *There are only finitely many O_S-equivalence classes of pairs (F,G) of square-free binary forms $F, G \in O_S[X,Y]$ of degree ≥ 3 which satisfy* (12) *and for which FG factorizes into linear factors over L.*

This is Cor. 1 of [3]. From Cor. 3 one can easily deduce a similar result for the solutions of the equation

(13) $\quad R(F,G) = R_0$ in binary forms $F, G \in O_S[X,Y]$,

where R_0 is a given non-zero element of O_S. It is easy to see that if (F,G) is a solution of (13) then so is $(\varepsilon F_U, \eta G_U)$ for every $U \in SL_2(O_S)$ and every $\varepsilon, \eta \in O_S^*$ with $\varepsilon^{\deg G} \cdot \eta^{\deg F} = 1$. Such pairs (F,G), $(\varepsilon F_U, \eta G_U)$ of binary forms are called *strongly O_S-equivalent.* Obviously, they are also O_S-equivalent. It follows from Cor. 3 that for every solution (F,G) of (13) for which F, G are square-free binary forms of degree ≥ 3 with splitting fields contained in L, $\deg F$ and $\deg G$ are bounded. Further, for given integers $r \geq 3$, $s \geq 3$, there are finitely many pairs (F', G') such that every solution (F,G) of (13) with $\deg F = r$, $\deg G = s$ for which FG is square-free and factorizes into linear factors over L, is O_S-equivalent to one of these (F', G'). But it is easy to prove that for such a fixed pair (F', G'), all solutions (F,G) of (13) having the properties specified above which are O_S-equivalent to (F', G') are strongly O_S-equivalent to each other. Hence we get from Cor. 3 the next corollary.

Corollary 4. *There are only finitely many strong O_S-equivalence* *classes of pairs (F,G) of square-free binary forms $F,G \in O_S[X,Y]$ of degree ≥ 3 which satisfy (13) and for which FG factorizes into linear factors over L.*

In view of (5), the above results can also be applied to the inequality

(14) $\quad 0 < |\mathcal{D}_S(F)|_S \leq M$ in square-free binary forms $F \in K[X,Y]$.

Two binary forms F, F' in $K[X,Y]$ are called *weakly O_S-equivalent* if $F' = \lambda F_U$ for some $\lambda \in K^*$ and $U \in SL_2(O_S)$. If F is a solution of (14) then so is every binary form F' which is weakly O_S-equivalent to F (see [2]). From Cor. 1 we obtain the following corollary.

Corollary 5. *There are only finitely many weak O_S-equivalence classes of square-free binary forms $F \in K[X,Y]$ of degree ≥ 3 with splitting field contained in L which satisfy (14).*

For an effective and quantitative version of Cor. 5, see Th. 2 of Evertse and the author [2]. We note that this theorem of [2] is valid for all square-free binary forms $F \in K[X,Y]$ of degree ≥ 2, without any assumption on the splitting fields of F. Using some arguments of [2], one could deduce from Cor. 5 some finiteness results for binary forms $F \in O_S[X,Y]$ with given degree and given non-zero discriminant. Finiteness theorems of this kind can be found in Birch and Merriman [1] and, in effective and quantitative forms, in [2].

4. Proofs

We adopt the notations of Sections 2 and 3. First we show that for non-zero binary forms $F,G \in K[X,Y]$, $\mathcal{R}_S^*(F,G)$ is a non-zero integral O_S-ideal in K. In the proof we shall use some arguments of [5], applied there to semi-resultants of monic polynomials. Suppose that F and G factorize into linear factors over L where L is a finite extension of K. Define T and O_T as in Section 2. There exists binary forms $F_G, G_F, P_1, \ldots, P_t$ in $K[X,Y]$ such that $P_1, \ldots, P_t$ are irreducible, F_G and G_F are relatively prime to each other and to $P_1, \ldots, P_t$ over K and

(15) $$F = F_G P_F\,, \quad G = G_F P_G\,,$$

where $P_F = P_1^{a_1} \ldots P_t^{a_t}$, $P_G = P_1^{b_1} \ldots P_t^{b_t}$ with some rational integers $a_i, b_i \geq 1$ for $i = 1, \ldots, t$. Further, $F_G, G_F, P_1, \ldots, P_t, P_F$ and P_G are uniquely determined up to multiplicative factors from K^*. In view of

(6), we may assume without loss of generality that $F_G, G_F, P_1, \dots, P_t$ are elements of $O_S[X,Y]$, that $P_i = 1$ for $i = 1, \dots, t$ if F and G are relatively prime, and that $F_G = 1$ (resp. $G_F = 1$) if F (resp. G) has no linear factor over L, not dividing G (resp. F). Consider now the representations of F and G in the form (1). By using (2), (3) and Lemma 2 of [2], one can easily verify that[1]

$$(16)\quad \begin{cases} \prod_{I(F,G)} \frac{(\det(\ell_i,\ell'_j))_T}{(\ell_i)_T(\ell'_j)_T} = \mathcal{R}_T(F_G,G_F)\mathcal{R}_T(F_G,P_G)\mathcal{R}_T(P_F,G_F)\times \\ \times \prod_{\substack{i,j=1\\ i\neq j}}^{t} (\mathcal{R}_T(P_i,P_j))^{a_ib_j} \prod_{i=1}^{t} (\mathcal{D}_T(P_i))^{a_ib_i} = \\ = \quad \Big(\mathcal{R}_S(F_G,G_F)\mathcal{R}_S(F_G,P_G)\times \\ \times\mathcal{R}_S(P_F,G_F) \prod_{\substack{i,j=1\\ i\neq j}}^{t} (\mathcal{R}_S(P_i,P_j))^{a_ib_j} \prod_{i=1}^{t} (\mathcal{D}_S(P_i))^{a_ib_i}\Big)\cdot O_T. \end{cases}$$

This implies that $\mathcal{R}_S^*(F,G)$, defined by (4), is indeed a non-zero integral O_S-ideal. Further, by (16) we have

$$(17)\quad \begin{aligned} \mathcal{R}_S^*(F,G) &= \mathcal{R}_S(F_G,G_F)\mathcal{R}_S(F_G,P_G)\mathcal{R}_S(P_F,G_F)\times \\ &\times \prod_{\substack{i,j=1\\ i\neq j}}^{t} (\mathcal{R}_S(P_i,P_j))^{a_ib_j} \cdot \prod_{i=1}^{t}(\mathcal{D}_S(P_i))^{a_ib_i}. \end{aligned}$$

Finally, we note that (17) is true for any factorizations of the form (15) of F, G (without the assumption that $F_G, G_F, P_1, \dots, P_t, P_F, P_G \in \in O_S[X,Y]$).

In the proofs below, we shall frequently use that $\omega_G(F) = \omega(F_G)$, $\omega_F(G) = \omega(G_F)$ and $\omega(gcd(F,G)) = \omega(P_1, \dots, P_t)$. Further, if F, G and H are non-zero binary forms in $K[X,Y]$ then

$$(18)\qquad \mathcal{R}_S(F,GH) = \mathcal{R}_S(F,G)\cdot\mathcal{R}_S(F,H).$$

In what follows, $c_2(\ ), \dots, c_{10}(\ )$ will denote positive numbers which depend only on the parameters occurring between the parentheses. To prove Ths. 1 and 2 we need some lemmas.

[1]For convenience, for $P = 1$ we put $\mathcal{D}_S(P) = O_S$, $\mathcal{D}_T(P) = O_T$. Further, if $Q = 1$ or if Q is a binary form in $K[X,Y]$ then let $\mathcal{R}_S(P,Q) = O_S$, $\mathcal{R}_T(P,Q) = O_T$.

Lemma 1. *Let $F, G \in K[X,Y]$ be binary forms such that $\deg F = r \geq 3$, $\deg G = s \geq 3$, FG has splitting field L over K, and FG is square-free. Then for all $\varepsilon > 0$*

$$(19) \quad |\mathcal{R}_S(F,G)|_S \geq c_2(r,s,S,L,\varepsilon) \left(|\mathcal{D}_S(F)|_S^{\frac{s}{r-1}} \cdot |\mathcal{D}_S(G)|_S^{\frac{r}{s-1}}\right)^{\frac{1}{17}-\varepsilon}.$$

Proof. This is proved in Remark 4 of [3]. ◊

Lemma 2. *Let $F, G \in K[X,Y]$ be binary forms with the properties specified in* Lemma 1. *Then*

$$(20) \qquad |\mathcal{D}_S(FG)|_S \leq c_3(r,s,S,L)|\mathcal{R}_S(F,G)|^{c_4(r,s)},$$

where $c_4(r,s) > 0$ is effectively computable.

Proof. It follows from

$$D(FG) = D(F)D(G)R^2(F,G)$$

that

$$(21) \qquad \mathcal{D}_S(FG) = \mathcal{D}_S(F)\mathcal{D}_S(G)\mathcal{R}_S^2(F,G).$$

Together with (19) this implies (20). ◊

Lemma 3. *Let $G \in K[X,Y]$ be a fixed square-free binary form of degree $s \geq 3$ and L a fixed finite normal extension of K containing the splitting field of G. Further, let $A \geq 1$ be fixed. Then up to multiplication by elements of K^*, there are only finitely many non-constant square-free binary forms $F \in K[X,Y]$ with splitting field contained in L that satisfy*

$$(22) \qquad 0 < |\mathcal{R}_S(F,G)|_S \leq A.$$

Further, each of these binary forms F has degree at most c_5, where $c_5 = c_5(K,L,S,A)$ is a number depending only on K, L, S and A.

Proof. Denote by H the Hilbert class field of L over K, by T' the set of prime ideals of O_H (the ring of integers of H) lying above the prime ideals in S, by $O_{T'}$ the ring of T' integers in H, and by $(P)_{T'}$ the $O_{T'}$-ideal generated by the coefficients of a polynomial P in $H[X,Y]$. Note that H, T depend only on K, L and S. Let $F \in K[X,Y]$ be a non-constant square-free binary form with splitting field contained in L which satisfies (22). Then there are $\lambda, \mu \in H^*$ such that $\lambda F, \mu G \in O_{T'}[X,Y]$ and $(\lambda F)_{T'} = O_{T'}$, $(\mu G)_{T'} = O_{T'}$. It follows now from (22) that

$$(23)\qquad A \geq |\mathcal{R}_{T'}(F,G)|_{T'} = |R(\lambda F, \mu G)|_{T'} > 0 .$$

Up to a multiplicative factor from $O^*_{T'}$, μ is uniquely determined. On applying now Lemma 1 of [3] to (23), we obtain that λF may assume only finitely many possibilities in $O_{T'}[X,Y]$ apart from a factor from $O^*_{T'}$. This implies that up to multiplication by elements of K^*, there are only finitely many $F \in K[X,Y]$ with the properties specified in our Lemma 3. Further, using again Lemma 1 of [3], $\deg F \leq c_6(H,T',A) \leq$ $\leq c_7(L,S,A)$ which completes the proof of the lemma. ◊

Proof of Th. 1. Let F, G be an arbitrary but fixed solution of (8) with property (9), and consider the representations of F and G in the form (15). Put $P^* = P_1 \dots P_t$. Then, by (21), we have

$$\mathcal{D}_S(P^*) = \prod_{i=1}^{t} \mathcal{D}_S(P_i) \times \prod_{\substack{i,j=1 \\ i \neq j}}^{t} \mathcal{R}_S(P_i, P_j) .$$

Together with (8) and (17) this implies that

$$(24)\qquad |\mathcal{D}_S(P^*)|_S \leq M .$$

It follows now from Th. 4 of [2] that

$$\omega(gcd(F,G)) = \omega(P^*) \leq c_8(K,L,S,M) .$$

If both $\omega(F_G)$ and $\omega(G_F)$ are less than 3 then it follows that

$$\omega(F) + \omega(G) \leq c_8 + 4 .$$

It remains the case $\max\{\omega_G(F), \omega_F(G)\} \geq 3$.

Suppose that for example $\omega_G(F) \geq 3$. Denote by F^*_G and G^*_F the maximal square-free parts of F_G and G_F, respectively. Then F^*_G and G^*_F are binary forms in $K[X,Y]$ and are uniquely determined by F and G up to non-zero proportional factors from K^*. Further, $\deg F^*_G \geq 3$. It follows from (8), (17) and (18) that

$$(25)\qquad 0 < |\mathcal{R}_S(F^*_G, P^* G^*_F)|_S \leq M .$$

By the assumption $\omega(G) \geq 3$, we have $\deg(P^* G^*_F) \geq 3$. Hence, by Lemma 3, $\deg F^*_G = \omega_G(F) \leq c_9(K,L,S,M)$ and $\deg(P^* G^*_F) =$ $= \omega(G) \leq c_9(K,L,S,M)$ and the assertion follows. One can proceed in the same way when $\omega_F(G) \geq 3$. ◊

Proof of Th. 2. In what follows $\mathcal{C}_1, \dots, \mathcal{C}_5$ denote finite sets depending at most on K, L, S, M and D. Let F, G be an arbitrary but fixed solution of (8) with $\deg F + \deg G \leq D$ and with property (9). First consider the case when $\omega_G(F) \geq 3$. Then using the notation of the proof of Th. 1, we have (25). By Lemma 2 and (25) we get

$$|\mathcal{D}_S(F_G^* P^* G_F^*)|_S \leq c_{10}(K, L, S, M, D). \tag{26}$$

But then, by Th. 2 of [2], there are a $\lambda \in K^*$ and a $U \in SL_2(O_S)$ such that $\lambda(F_G^* P^* G_F^*)_U \in \mathcal{C}_1$ for some $\mathcal{C}_1$. Since by assumption $\deg F + \deg G \leq D$, this implies that (F, G) is weakly O_S-equivalent to a pair of binary forms belonging to $\mathcal{C}_2$ for some $\mathcal{C}_2$. We can proceed in a similar way if $\omega_F(G) \geq 3$.

It remains the case when $\omega_G(F) \leq 2$ and $\omega_F(G) \leq 2$. Then, by assumption, $\omega(P^*) \geq 3$. Further, (24) holds. Now Th. 2 of [2] can be applied to (24) and we get $\lambda(P^*)_U \in \mathcal{C}_3$ for some $\lambda \in K^*$, $U \in SL_2(O_S)$ and $\mathcal{C}_3$. Further, it follows from (8), (17) and (18) that

$$|\mathcal{R}_S(F_G^* G_F^*, P^*)|_S \leq M,$$

whence

$$|\mathcal{R}_S((F_G^* G_F^*)_U, (P^*)_U)|_S \leq M.$$

But, for fixed U, $(P^*)_U$ is also fixed and, by Lemma 3, $\mu(F_G^* G_F^*)_U \in \mathcal{C}_4$ for some $\mu \in K^*$ and $\mathcal{C}_4$. Consequently, (F, G) is weakly O_S-equivalent to a pair (F', G') of binary forms with $(F', G') \in \mathcal{C}_5$ for an appropriate $\mathcal{C}_5$. $\Diamond$

Proof of Cor. 3. $\mathcal{C}_6, \ldots, \mathcal{C}_{12}$ will denote finite sets depending at most on K, L, S and M. Let (F, G) be a pair of square-free binary forms $F, G \in O_S[X, Y]$ of degree ≥ 3 which satisfy (12) and for which FG factorizes into linear factors over L. Then

$$0 < |\mathcal{R}_S(F, G)|_S \leq |R(F, G)|_S \leq M. \tag{27}$$

Hence, by Cor. 2, (F, G) is weakly O_S-equivalent to some (F', G'), where $F', G' \in \mathcal{C}_6$ for some $\mathcal{C}_6$. In other words, there are $\lambda, \mu \in K^*$ and $U \in SL_2(O_S)$ such that

$$F_U(\mathbf{X}) = \lambda F'(\mathbf{X}), \quad G_U(\mathbf{X}) = \mu G'(\mathbf{X}). \tag{28}$$

It is easy to see that this implies

$$(R(F, G))_S = (R(F', G'))_S (\lambda^s \mu^r)_S, \tag{29}$$

where $r := \deg F$, $s := \deg G$ are bounded. It follows now from (27) and (29) that $(\lambda^s \mu^s)_S \in \mathcal{C}_7$ for some $\mathcal{C}_7$. Further, we have

$$F_U^s(\mathbf{X}) G_U^r(\mathbf{X}) = (\lambda F'(\mathbf{X}))^s (\mu G'(\mathbf{X}))^r.$$

Hence we infer that $(\lambda F')_S^s (\mu G')_S^r \in \mathcal{C}_8$. But $(\lambda F')_S$ and $(\mu G')_S$ are integral O_S-ideals, hence $(\lambda F')_S, (\mu G')_S \in \mathcal{C}_9$ for suitable $\mathcal{C}_8$, $\mathcal{C}_9$. This implies that $(\lambda)_S, (\mu)_S \in \mathcal{C}_{10}$ for some $\mathcal{C}_{10}$. It follows now that there are $\lambda_0, \mu_0 \in K^*$ with $\lambda_0, \mu_0 \in \mathcal{C}_{11}$ such that $\lambda = \varepsilon\lambda_0$, $\mu = \eta\mu_0$ with some $\varepsilon, \eta \in O_S^*$. Putting now $\tilde{F} = \lambda_0 F'$, $\tilde{G} = \mu_0 G'$ we get by (28) that $F_U(\mathbf{X}) = \varepsilon\tilde{F}(\mathbf{X}), G_U(\mathbf{X}) = \eta\tilde{G}(\mathbf{X})$ and $\tilde{F}, \tilde{G} \in \mathcal{C}_{12}$. Thus we have proved that (F, G) is O_S-equivalent to $(\tilde{F}, \tilde{G})$ where $(\tilde{F}, \tilde{G})$ belong to a finite set depending only on K, L, S and M. ◊

References

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

[2] EVERTSE, J. H. and GYŐRY, K.: Effective finiteness results for binary forms with given discriminant, *Compositio Math.* **79** (1991), 169–204.

[3] EVERTSE, J. H. and GYŐRY, K.: Lower bounds for resultants, I, *Compositio Math.* **88** (1993), 1–23.

[4] GYŐRY K.: On arithmetic graphs associated with integral domains, in "A Tribute to Paul Erdős" (A. Baker, B. Bollobás, A. Hajnal, Eds.), Cambridge University Press, 1990, 207–222.

[5] GYŐRY, K.: On the number of pairs of polynomials with given resultant or given semi-resultant, *Acta Sci. Math.* **57** (1993), 515–529.