ON THE NUMBER OF EQUIVALENCE CLASSES OF BINARY FORMS OF GIVEN DEGREE AND GIVEN DISCRIMINANT

ATTILA BÉRCZES, JAN-HENDRIK EVERTSE, AND KÁLMÁN GYŐRY

To Professor Robert Tijdeman on his 60th birthday

1. Introduction

In the present paper we give explicit upper bounds for the number of equivalence classes of binary forms of given degree and discriminant, and for the number of equivalence classes of irreducible binary forms with given invariant order.

Two binary forms $F, G \in \mathbb{Z}[X, Y]$ are called equivalent if there is a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $G(X, Y) = F(aX + bY, cX + dY)$. Denote by $D(F)$ the discriminant of a binary form F, and by $\mathcal{O}_F$ the invariant order of an irreducible binary form F. We recall the definition of the invariant order of F which is less familiar. Write $F(X, Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$ and let θ_F be a zero of $F(X, 1)$. Then $\mathcal{O}_F$ is defined to be the $\mathbb{Z}$-module with basis 1, $a_0\theta_F$, $a_0\theta_F^2 + a_1\theta_F$, $a_0\theta_F^3 + a_1\theta_F^2 + a_2\theta_F$,..., $a_0\theta_F^{r-1} + a_1\theta_F^{r-2} + \cdots + a_{r-2}\theta_F$; this is indeed an order, i.e., closed under multiplication. It is well-known that two equivalent binary forms have the same discriminant. Further, two equivalent irreducible binary forms have the same invariant order. The discriminant $D(\mathcal{O}_F)$ of $\mathcal{O}_F$ is equal to $D(F)$ (see [8], [9] for a verification of these facts). Consequently, if $K = \mathbb{Q}(\theta_F)$,

2000 Mathematics Subject Classification: 11D57, 11D72, 11E76.

Keywords and Phrases: Binary forms, discriminants, invariant order, unit equations in two unknowns.

The research was supported in part by the Hungarian Academy of Sciences (A.B.,K.G.), the Netherlands Organization for Scientific Research (A.B.,J.-H.E.,K.G.), by grants F34981 (A.B), N34001 (A.B.,J.-H.E.,K.G.) T42985 (A.B., K.G.) and T38225 (A.B., K.G.) of the Hungarian National Foundation for Scientific Research and by the FKFP grant 3272-13066/201 (A.B.).

then $D(F) = c^2 D_K$, where D_K is the discriminant of K and $c = [\mathcal{O}_K : \mathcal{O}_F]$ is the index of $\mathcal{O}_F$ in the ring of integers $\mathcal{O}_K$ of K.

By classical results of Lagrange, Gauss ($r = 2$) and Hermite ($r = 3$), the binary forms $F \in \mathbb{Z}[X, Y]$ of degree $r \leq 3$ with a given discriminant $D \neq 0$ lie in finitely many equivalence classes, and these classes can be effectively determined. This finiteness theorem was generalized for the case $r \geq 4$ by Birch and Merriman [2] in an ineffective form, and later by Evertse and Győry [5] in an effective form. Moreover, the theorem remains true without fixing the degree r; see [7]. An immediate consequence is that if $\mathcal{O}$ is a given order of some number field, then the irreducible binary forms $F \in \mathbb{Z}[X, Y]$ with $\mathcal{O}_F = \mathcal{O}$ lie in finitely many equivalence classes. From a result of Delone and Faddeev [3, Chap.II, §15] it follows that for each cubic order $\mathcal{O}$ there is precisely one equivalence class of irreducible binary cubic forms $F \in \mathbb{Z}[X, Y]$ such that $\mathcal{O}_F = \mathcal{O}$. For degree larger than 3 this is no longer true: Simon [9] gave examples of number fields K of degree 4 and of arbitrarily large degree whose ring of integers $\mathcal{O}_K$ can not be represented as $\mathcal{O}_F$ for any irreducible binary form F.

In the present paper, we prove the following results:

1) Let $\mathcal{O}$ be an order whose quotient field has degree $r \geq 4$ over $\mathbb{Q}$. Then the irreducible binary forms $F \in \mathbb{Z}[X, Y]$ with $\mathcal{O}_F \cong \mathcal{O}$ lie in at most 2^{24r^3} equivalence classes.

2) Let K be an algebraic number field of degree $r \geq 3$ and let c be a positive integer. Then for every $\varepsilon > 0$ the set of irreducible binary forms $F \in \mathbb{Z}[X, Y]$ such that $K = \mathbb{Q}(\theta_F)$ for some zero θ_F of $F(X, 1)$ and such that $D(F) = c^2 D_K$ is contained in the union of at most $\alpha(r, \varepsilon) c^{\frac{2}{r(r-1)}+\varepsilon}$ equivalence classes; here $\alpha(r, \varepsilon)$ depends only on r and ε. We show that in this upper bound the exponent of c cannot be replaced by a quantity smaller than $\frac{2}{r(r-1)}$.

More generally, we prove analogues of 1) and 2) for binary forms having their coefficients in the ring of S-integers of a number field. Further, we prove a generalization of 2) for reducible binary forms. Our precise results are stated in Section 2 (Theorems 2.1, 2.2 and 2.3). Our approach is similar to that of Birch and Merriman [2], with the necessary modifications. In our

proofs we use among other things an upper bound by Beukers and Schlickewei [1, Theorem 1] for the numbers of solutions of the equation $x + y = 1$ in unknowns x, y from a multiplicative group of finite rank.

2. Statements of the results

Terminology. Before stating our results we introduce the necessary terminology. Let $F(X, Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$ be a binary form. Writing F as

$$F(X, Y) = \lambda \prod_{i=1}^{r} (\alpha_i X - \beta_i Y)$$

we may express the discriminant of F as

$$D(F) = \lambda^{2r-2} \prod_{1 \le i < j \le r} (\alpha_i\beta_j - \alpha_j\beta_i)^2 . \tag{2.1}$$

This is independent of the choice of λ and of the α_i, β_i. It is well-known that $D(F)$ is a homogeneous polynomial of degree $2r - 2$ in $\mathbb{Z}[a_0, \ldots, a_r]$. For a matrix $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we define $F_U(X, Y) := F(aX + bY, cX + dY)$. Then (2.1) gives

$$D(F_U) = (\det U)^{r(r-1)} D(F). \tag{2.2}$$

Now let R be an integral domain with quotient field of characteristic 0. Two binary forms $F, G \in R[X, Y]$ are called *R-equivalent*, notation $F \overset{R}{\sim} G$, if $G = F_U$ for some matrix $U \in \mathrm{GL}_2(R)$, i.e., with $\det U \in R^*$. (If $R = \mathbb{Z}$ we simply speak about equivalence.) It is then clear from (2.2) that for any two binary forms $F, G \in R[X, Y]$ we have

$$G \overset{R}{\sim} F \quad \Rightarrow \quad D(G) = \varepsilon D(F) \ \text{ for some } \ \varepsilon \in R^*. \tag{2.3}$$

An important invariant of an irreducible binary form $F \in R[X, Y]$ is its *invariant ring* or *invariant order* $\mathcal{O}_{F,R}$ (see Simon [9]). By an R-order of degree r (or just an order of degree r if $R = \mathbb{Z}$) we mean an integral domain $\mathcal{O}$ such that $\mathcal{O}$ is an overring of R, the domain $\mathcal{O}$ is finitely generated as an R-module, and the quotient field of $\mathcal{O}$ has degree r over the quotient field of R.

The order $\mathcal{O}_{F,R}$ (or just $\mathcal{O}_F$ if $R = \mathbb{Z}$) is defined as follows. Let $F = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$ be a binary form in $R[X,Y]$ which is irreducible over the quotient field of R. Let θ_F be a zero of $F(X,1)$. Then $\mathcal{O}_{F,R}$ is defined to be the R-module with basis

$$\begin{aligned} &\omega_1 = 1,\ \omega_2 = a_0\theta_F,\ \omega_3 = a_0\theta_F^2 + a_1\theta_F, \ldots, \\ &\qquad\qquad \omega_r = a_0\theta_F^{r-1} + a_1\theta_F^{r-2} + \cdots + a_{r-2}\theta_F. \end{aligned} \tag{2.4}$$

We recall some facts proved by Simon [9] about $\mathcal{O}_{F,R}$. First $\mathcal{O}_{F,R}$ is an R-order of degree r. Second, if G is another binary form in $R[X,Y]$ then

$$F \overset{R}{\sim} G \quad \Rightarrow \quad \mathcal{O}_{F,R} \cong \mathcal{O}_{G,R} \quad \text{(as } R\text{-algebras)}. \tag{2.5}$$

Third

$$D(\omega_1, \ldots, \omega_r) = D(F). \tag{2.6}$$

Here $D(\omega_1, \ldots, \omega_r)$ denotes the discriminant of $\omega_1, \ldots, \omega_r$, that is the determinant $\det(\mathrm{Tr}(\omega_i\omega_j)_{1\le i,j\le r})$, where Tr denotes the trace map from the quotient field of $\mathcal{O}_{F,R}$ to that of R.

Our results will be established for binary forms having their coefficients in the ring of S-integers of a number field. Therefore we recall some notions about such rings.

Let $\mathbb{k}$ be a number field, and $\{|.|_v : v \in M_{\mathbb{k}}\}$ be a maximal set of pairwise inequivalent absolute values of $\mathbb{k}$. We will refer to $M_{\mathbb{k}}$ as the set of places of $\mathbb{k}$. Let S be a finite subset of $M_{\mathbb{k}}$ containing all infinite places of $\mathbb{k}$ (i.e., the places v such that $|.|_v$ is archimedean). Then the ring of S-integers and its unit group, the group of S-units are defined by

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

respectively.

Two ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_S$ are said to belong to the same ideal class of $\mathcal{O}_S$ if there are non-zero $\lambda, \mu \in \mathcal{O}_S$ such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$. Denote by $h_m(\mathcal{O}_S)$ the number of ideal classes $\mathfrak{A}$ of $\mathcal{O}_S$ such that $\mathfrak{A}^m$ is the class of principal ideals of $\mathcal{O}_S$. For a finite extension K of $\mathbb{k}$, let $\mathfrak{d}_{K/\mathbb{k},S}$ denote the relative S-discriminant, i.e., the ideal of $\mathcal{O}_S$ generated by all discriminants $D_{K/\mathbb{k}}(\omega_1, \ldots, \omega_r)$, where $\omega_1, \ldots, \omega_r$ runs through all $\mathbb{k}$-bases of K with

$\omega_1, \ldots, \omega_r$ integral over $\mathcal{O}_S$. The absolute norm of an ideal $\mathfrak{a}$ of $\mathcal{O}_S$ is defined by $N_S(\mathfrak{a}) := \#\mathcal{O}_S/\mathfrak{a}$.

Given an irreducible binary form $F \in \mathcal{O}_S[X,Y]$ we write $\mathcal{O}_{F,S}$ for its invariant order $\mathcal{O}_{F,\mathcal{O}_S}$.

New results. Let $\Bbbk$, $\mathcal{O}_S$ be as above. From results of Birch and Merriman from 1972 [2] (ineffective) and Evertse and Győry from 1991 [5] (effective) it follows that for given $r \geq 2$ and $D \in \mathcal{O}_S$ with $D \neq 0$, the binary forms $F \in \mathcal{O}_S[X,Y]$ with degree r and with $D(F) \in D\mathcal{O}_S^*$ lie in finitely many $\mathcal{O}_S$-equivalence classes. Together with (2.6) this implies that for any given $\mathcal{O}_S$-order $\mathcal{O}$, the binary forms $F \in \mathcal{O}_S[X,Y]$ which are irreducible over $\Bbbk$ and for which $\mathcal{O}_{F,S} = \mathcal{O}$ lie in finitely many $\mathcal{O}_S$-equivalence classes. From a result of Evertse and Győry [4, Thm. 11] it can be deduced that for a given $\mathcal{O}_S$-order $\mathcal{O}$, the *monic* binary forms $F \in \mathcal{O}_S[X,Y]$ (i.e., such that $F(1,0) = 1$) with $\mathcal{O}_{F,S} = \mathcal{O}$ lie in at most $c(r)^s$ $\mathcal{O}_S$-equivalence classes, where $c(r)$ depends only on r and where $s = \#S$. Our first result extends this to non-monic binary forms.

Theorem 2.1. *Let $S \subset M_\Bbbk$ be a finite set of cardinality s, containing all infinite places. Let $\mathcal{O}$ be an $\mathcal{O}_S$-order of degree $r \geq 3$. Then there are only finitely many $\mathcal{O}_S$-equivalence classes of binary forms $F \in \mathcal{O}_S[X,Y]$ such that F is irreducible in $\Bbbk[X,Y]$ and*

$$\mathcal{O}_{F,S} \cong \mathcal{O} \quad (\textit{as } \mathcal{O}_S\textit{-algebras}). \tag{2.7}$$

The number of these classes is bounded above by

$$\begin{cases} 2^{24r^3s} & \textit{if } r \textit{ is odd,} \\ 2^{24r^3s} h_2(\mathcal{O}_S) & \textit{if } r \textit{ is even.} \end{cases} \tag{2.8}$$

In Section 9 we show that the factor $h_2(\mathcal{O}_S)$ is necessary if r is even.

In the next corollary we state the consequence for $\mathcal{O}_S = \mathbb{Z}$. Recall that in this case $\Bbbk = \mathbb{Q}$ and $\#S = 1$.

Corollary 2.1. *Let $\mathcal{O}$ be an order of degree $r \geq 3$. Then the number of equivalence classes of binary forms $F \in \mathbb{Z}[X,Y]$ such that F is irreducible*

in $\mathbb{Q}[X,Y]$ *and* $\mathcal{O}_F \cong \mathcal{O}$ *is at most*

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

We now state our second result. For an ideal $\mathfrak{a}$ of $\mathcal{O}_S$, denote by $\omega_S(\mathfrak{a})$ the number of distinct prime ideals $\mathfrak{p}$ of $\mathcal{O}_S$ with $\mathfrak{p} \mid \mathfrak{a}$ (or the number of $v \notin S$ such that $|x|_v < 1$ for every $x \in \mathfrak{a}$). Further, for an ideal $\mathfrak{a}$ of $\mathcal{O}_S$ and for $\alpha \in \mathbb{N}$, denote by $\tau_\alpha(\mathfrak{a})$ the number of tuples of ideals $(\mathfrak{d}_1, \dots, \mathfrak{d}_\alpha)$ of $\mathcal{O}_S$ such that their product $\prod_{i=1}^{\alpha} \mathfrak{d}_i$ divides $\mathfrak{a}$. In the theorems below, the ideal of $\mathcal{O}_S$ generated by a is denoted by $[a]$.

Given a finite extension K of $\mathbb{k}$, we denote by $\mathcal{F}(\mathcal{O}_S, K)$ the set of binary forms F such that $F \in \mathcal{O}_S[X,Y]$, F is irreducible in $\mathbb{k}[X,Y]$, and there is θ_F such that $F(\theta_F, 1) = 0$ and $K = \mathbb{k}(\theta_F)$. By Lemma 4.1 in Section 4, for every $F \in \mathcal{F}(\mathcal{O}_S, K)$ there is an ideal $\mathfrak{c}$ of $\mathcal{O}_S$ such that

$$[D(F)] = \mathfrak{c}^2 \cdot \mathfrak{d}_{K/\mathbb{k},S}. \tag{2.9}$$

Theorem 2.2. *Let S be as in Theorem 2.1, and let K be an extension of $\mathbb{k}$ of degree $r \geq 3$. Then for every non-zero ideal $\mathfrak{c}$ of $\mathcal{O}_S$, there are at most finitely many $\mathcal{O}_S$-equivalence classes of binary forms $F \in \mathcal{F}(\mathcal{O}_S, K)$ with (2.9). The number of these classes is at most*

$$2^{24r^3(s+\omega_S(\mathfrak{c}))} \cdot \tau_{\frac{1}{2}r(r-1)}(\mathfrak{c}^2) \left(\sum_{\mathfrak{d}^{\frac{1}{2}r(r-1)} \mid \mathfrak{c}} N_S(\mathfrak{d}) \right) \cdot h(r, \mathcal{O}_S) \tag{2.10}$$

where

$$h(r, \mathcal{O}_S) = 1 \quad \text{if } r \text{ is odd}, \qquad h(r, \mathcal{O}_S) = h_2(\mathcal{O}_S) \quad \text{if } r \text{ is even}.$$

Here the sum is taken over all ideals $\mathfrak{d}$ of $\mathcal{O}_S$ such that $\mathfrak{d}^{\frac{1}{2}r(r-1)}$ divides $\mathfrak{c}$.

We give again the consequence for $\mathcal{O}_S = \mathbb{Z}$. Given a nonzero integer a, denote by $\omega(a)$ the number of distinct primes dividing a, and for $\alpha \in \mathbb{N}$ denote by $\tau_\alpha(a)$ the number of tuples of positive integers $(d_1, \dots, d_\alpha)$ such that $\prod_{i=1}^{\alpha} d_i$ divides a.

Corollary 2.2. *Let K be a number field of degree $r \geq 3$, and let c be a positive integer. Then the irreducible binary forms $F \in \mathbb{Z}[X,Y]$, for which*

$\mathbb{Q}(\theta_F) = K$ *for some zero* θ_F *of* $F(X,1)$*, and for which*

$$D(F) = c^2 D_K$$

lie in at most

$$2^{24r^3(1+\omega(c))} \cdot \tau_{\frac{1}{2}r(r-1)}(c^2) \left(\sum_{d^{\frac{1}{2}r(r-1)} | c} d \right)$$

equivalence classes.

Theorem 2.2 will be deduced from Theorem 2.1 as follows. Let S' consist of the places in S and those places $v \notin S$ such that $|x|_v < 1$ for every $x \in \mathfrak{c}$. Then if $F \in \mathcal{F}(\mathcal{O}_S, K)$ satisfies (2.9), then $D(F) \cdot \mathcal{O}_{S'} = \mathfrak{d}_{K/\Bbbk,S'}$ and so $\mathcal{O}_{F,S'} = \mathcal{O}_{S'}$. Now Theorem 2.1 yields an upper bound for the number of $\mathcal{O}_{S'}$-equivalence classes containing the binary forms $F \in \mathcal{F}(\mathcal{O}_S, K)$ with (2.9) and from the arguments in Section 4 one obtains an upper bound for the number of $\mathcal{O}_S$-equivalence classes containing the forms lying in a single $\mathcal{O}_{S'}$-equivalence class.

We state a generalization of Theorem 2.2 for reducible forms. Let K_0, K_1,...,K_t be (not necessarily distinct) finite extensions of $\Bbbk$. Denote by $\mathcal{F}(\mathcal{O}_S, K_0, \ldots, K_t)$ the set of binary forms F with the following properties: there are binary forms $F_0, \ldots, F_t$ with $F = \prod_{i=0}^t F_i$, such that $F_i \in \mathcal{O}_S[X,Y]$, F_i is irreducible in $\Bbbk[X,Y]$, and there is a θ_{F_i} such that $F_i(\theta_{F_i}) = 0$ and $\Bbbk(\theta_{F_i}) = K_i$ $(i = 0, \ldots, t)$. By Lemma 4.1 in Section 4, for every binary form $F \in \mathcal{F}(\mathcal{O}_S, K_0, \ldots, K_t)$ there is an ideal $\mathfrak{c}$ in $\mathcal{O}_S$ such that

$$[D(F)] = \mathfrak{c}^2 \mathfrak{d}_{K_0/\Bbbk,S} \ldots \mathfrak{d}_{K_t/\Bbbk,S}. \tag{2.11}$$

Theorem 2.3. *Let* S *be as in Theorems 2.1 and 2.2, and let* $K_0, K_1, \ldots, K_t$ *be finite extensions of* $\Bbbk$*. Put* $r_i := [K_i : \Bbbk]$ $(i = 0, \ldots, t)$ *and* $r := r_0 + \cdots + r_t$*. Assume that* $r_0 \geq 3$*. Then for every non-zero ideal* $\mathfrak{c}$ *of* $\mathcal{O}_S$ *there are at most finitely many* $\mathcal{O}_S$*-equivalence classes of binary forms* $F \in \mathcal{F}(\mathcal{O}_S, K_0, \ldots, K_t)$ *with (2.11). The number of these classes is at most*

$$2^{24r^3(s+\omega_S(\mathfrak{c}))} \cdot \tau_{\frac{1}{2}r(r-1)}(\mathfrak{c}^2) \left(\sum_{\mathfrak{d}^{\frac{1}{2}r(r-1)} | \mathfrak{c}} N_S(\mathfrak{d}) \right) \cdot h(r_0, \mathcal{O}_S) \tag{2.12}$$

where

$$h(r_0, \mathcal{O}_S) = 1 \quad \text{if } r_0 \text{ is odd}, \qquad h(r_0, \mathcal{O}_S) = h_2(\mathcal{O}_S) \quad \text{if } r_0 \text{ is even}.$$

The consequence of Theorem 2.3 for $\mathcal{O}_S = \mathbb{Z}$ is as follows.

Corollary 2.3. *Let $K_0, \dots, K_t$ be number fields. Put $r_i := [K_i : \mathbb{Q}]$ $(i = 0, \dots, t)$ and $r := r_0 + \cdots + r_t$. Assume that $r_0 \geq 3$. Let c be a positive integer. Then the binary forms F for which there are irreducible binary forms $F_0, \dots, F_t \in \mathbb{Z}[X, Y]$ with $F = \prod_{i=0}^{t} F_i$ such that $K_i = \mathbb{Q}(\theta_{F_i})$ for some zero θ_{F_i} of $F_i(X, 1)$, and for which*

$$D(F) = c^2 D_{K_0} \dots D_{K_t},$$

lie in at most

$$2^{24r^3(1+\omega(c))} \cdot \tau_{\frac{1}{2}r(r-1)}(c^2) \left(\sum_{d^{\frac{1}{2}r(r-1)} | c} d \right)$$

equivalence classes.

Unfortunately, our method of proof of Theorem 2.3 requires that we have to impose some unnatural technical conditions on the binary forms F under consideration, namely that they factor into binary forms F_i with coefficients in $\mathcal{O}_S$ and that F_0 has degree $r_0 \geq 3$. If $\mathcal{O}_S$ is a principal ideal domain (for instance when $\Bbbk = \mathbb{Q}$), then the first condition is no restriction. For in that case, if a binary form $F \in \mathcal{O}_S[X, Y]$ is reducible over $\Bbbk$ its irreducible factors can always be chosen from $\mathcal{O}_S[X, Y]$. But the latter is not true if $\mathcal{O}_S$ is not a principal ideal domain.

Allowing these technical conditions, we give a relatively simple proof of Theorem 2.3 based on Theorem 2.2 and on a result on resultant equations (see Proposition 8.1 in Section 8) which may be of some independent interest. It may be possible to remove the technical conditions from Theorem 2.3 at the price of more complications.

Theorem 2.3 implies that the number of $\mathcal{O}_S$-equivalence classes of binary forms $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) is at most

$$\alpha(\Bbbk, S, r_0, \dots, r_t, \varepsilon) N_S(\mathfrak{c})^{\frac{2}{r(r-1)}+\varepsilon} \tag{2.13}$$

for every $\varepsilon > 0$, where α depends only on the parameters between the parentheses. In Section 9 we will show that the bound (2.13) is almost best possible in terms of $N_S(\mathfrak{c})$ in the following sense: for each tuple $(K_0, \dots, K_t)$ of finite extensions of $\Bbbk$, there is a sequence of ideals $\mathfrak{c}$ of $\mathcal{O}_S$ with $N_S(\mathfrak{c}) \to \infty$, such that the number of $\mathcal{O}_S$-equivalence classes of binary forms $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) is at least

$$\beta N_S(\mathfrak{c})^{\frac{2}{r(r-1)}},$$

where β is a positive constant independent of $\mathfrak{c}$.

3. Preliminaries

In our proofs it will be necessary to keep track not only of binary forms but also of their zeros. To facilitate this, we introduce below so-called augmented forms, which are tuples consisting of a binary form and of some of their zeros.

Given a field K, we define $\mathbb{P}^1(K) := K \cup \{\infty\}$. Every matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ induces a projective transformation

$$\langle A \rangle : \mathbb{P}^1(K) \to \mathbb{P}^1(K) : \xi \mapsto \frac{a\xi + b}{c\xi + d}$$

(with the usual rules $(a\xi + b)/(c\xi + d) = \infty$ if $c \neq 0$ and $\xi = -d/c$; $(a\infty + b)/(c\infty + d) = a/c$ if $c \neq 0$ and ∞ if $c = 0$). Thus, two matrices $A, B \in \mathrm{GL}_2(K)$ induce the same projective transformation if and only if $B = \lambda A$ for some $\lambda \in K^*$.

Now let $\Bbbk$ be a number field which is fixed henceforth. Let K be a finite extension of $\Bbbk$. An *augmented K-form* is a pair $F^* = (F, \theta_F)$ consisting of a binary form F which is irreducible in $\Bbbk[X, Y]$, and $\theta_F \in K$ such that $F(\theta_F, 1) = 0$ and $\Bbbk(\theta_F) = K$. We agree that $\Bbbk(\infty) = \Bbbk$ and that for every $c \in \Bbbk^*$, (cY, ∞) is an augmented $\Bbbk$-form.

Let $K_0, \dots, K_t$ be a sequence of finite extensions of $\Bbbk$. An *augmented $(K_0, \dots, K_t)$-form* is a tuple $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ with the property that there are binary forms $F_0, \dots, F_t$, such that $F = \prod_{i=0}^{t} F_i$, and $(F_i, \theta_{i,F})$ is

an augmented K_i-form for $i = 0, \dots, t$. We define the discriminant and degree of F^* by $D(F^*) := D(F)$, $\deg F^* := \deg F$, respectively. Notice that $\deg F^* = \sum_{i=0}^{t} [K_i : \Bbbk]$.

For an augmented $(K_0, \dots, K_t)$-form $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ and for $A \in \mathrm{GL}_2(\Bbbk)$, $\lambda \in \Bbbk^*$ we define

$$\lambda F_A^* := (\lambda F_A, \langle A \rangle^{-1} \theta_{0,F}, \dots, \langle A \rangle^{-1} \theta_{t,F}). \tag{3.1}$$

Clearly, λF_A^* is again an augmented $(K_0, \dots, K_t)$-form. Notice that if $G^* = \lambda F_A^*$ then $F^* = \lambda^{-1} G_{A^{-1}}^*$; further if $G^* = \lambda F_A^*$, $H^* = \mu G_B^*$ for some $A, B \in \mathrm{GL}_2(\Bbbk)$, $\lambda, \mu \in \Bbbk^*$ then $H^* = \lambda\mu F_{AB}^*$.

Let R be a subring of $\Bbbk$. Two augmented $(K_0, \dots, K_t)$-forms F^*, G^* are called *R-equivalent*, notation $F^* \overset{R}{\sim} G^*$, if $G^* = F_U^*$ for some $U \in \mathrm{GL}_2(R)$, and *weakly R-equivalent*, notation $F^* \overset{R}{\approx} G^*$, if $G^* = \lambda F_U^*$ for some $U \in \mathrm{GL}_2(R)$ and $\lambda \in R^*$.

Let

$$\mathrm{M}_2^{\mathrm{ns}}(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R,\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \right\}.$$

Then for two augmented $(K_0, \dots, K_t)$-forms F^*, G^* we write $F^* \overset{R}{\prec} G^*$ if $G^* = F_A^*$ for some $A \in \mathrm{M}_2^{\mathrm{ns}}(R)$.

In the Lemma below we have collected some simple facts.

Lemma 3.1. *Let $r := \sum_{i=0}^{t} [K_i : \Bbbk] \geq 3$ and let R be a subring of $\Bbbk$.*

(i) *Let F^* be an augmented $(K_0, \dots, K_t)$-form, $U \in GL_2(\Bbbk)$ and $\lambda \in \Bbbk^*$. Then $\lambda F_U^* = F^*$ if and only if $U = \rho \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\rho \in \Bbbk^*$ and $\rho^r = \lambda^{-1}$.*

(ii) *Let F^*, G^* be two augmented $(K_0, \dots, K_t)$-forms and suppose that $G^* = \lambda_0 F_{U_0}^*$ for some $U_0 \in GL_2(\Bbbk)$, $\lambda_0 \in \Bbbk^*$. Then for any other $U \in GL_2(\Bbbk)$, $\lambda \in \Bbbk^*$ we have $G^* = \lambda F_U^*$ if and only if $U = \rho U_0$ with $\rho \in \Bbbk^*$ and $\rho^r = \lambda_0/\lambda$.*

(iii) *Let F^*, G^*, H^* be augmented $(K_0, \dots, K_t)$-forms such that $F^* \overset{R}{\prec} G^*$, $G^* \overset{R}{\prec} H^*$. Then $F^* \overset{R}{\prec} H^*$.*

(iv) *Let F^*, G^* be two augmented $(K_0, \dots, K_t)$-forms. Then $F^* \overset{R}{\prec} G^*$, $G^* \overset{R}{\prec} F^* \iff F^* \overset{R}{\sim} G^*$.*

Proof. (i) Let $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$. For $i = 0, \dots, t$, put $r_i := [K_i : \Bbbk]$ and denote by $\theta_{i,F}^{(1)}, \dots, \theta_{i,F}^{(r_i)}$ the conjugates of $\theta_{i,F}$ over $\Bbbk$ (if $\theta_{i,F} = \infty$, then $K_i = \Bbbk$, $r_i = 1$ and $\theta_{i,F}^{(1)} = \infty$). By assumption, $\langle U \rangle^{-1} \theta_{i,F} = \theta_{i,F}$ for $i = 0, \dots, t$ and therefore, $\langle U \rangle^{-1} \theta_{i,F}^{(j)} = \theta_{i,F}^{(j)}$ for $i = 0, \dots, t$, $j = 1, \dots, r_i$. Thus, $\langle U \rangle$ has $\sum_{i=0}^{t} [K_i : \Bbbk] = r \geq 3$ fixpoints. It follows that $\langle U \rangle$ is the identity on $\mathbb{P}^1$, hence $U = \rho \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\rho \in \Bbbk^*$. Now since $\lambda F_U = F$, we have $F(X, Y) = \lambda F(\rho X, \rho Y) = \lambda \rho^r F(X, Y)$, hence $\rho^r = \lambda^{-1}$. Conversely, if $U = \rho \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\rho^r = \lambda^{-1}$, then clearly, $\lambda F_U^* = F^*$.

(ii) Let $G^* = \lambda F_U^*$. Then $(\lambda_0 \lambda^{-1}) F_{U_0 U^{-1}}^* = F^*$. Apply (i).

(iii) Obvious.

(iv) $\Leftarrow$ is clear. Assume $F^* \overset{R}{\prec} G^*$, $G^* \overset{R}{\prec} F^*$. Then there are $A, B \in \mathrm{M}_2^{\mathrm{ns}}(R)$ such that $G^* = F_A^*$, $F^* = G_B^*$. Thus $F^* = F_{AB}^*$. Hence by (i), $AB = \rho \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\rho^r = 1$. Now $\rho \in R$ and $A^{-1} = \rho^{-1} B = \rho^{r-1} B \in \mathrm{M}_2^{\mathrm{ns}}(R)$. So $A \in \mathrm{GL}_2(R)$ and $F^* \overset{R}{\sim} G^*$. □

Let again S be a finite subset of $M_\Bbbk$ containing all infinite places. For $v \notin S$ (i.e. $v \in M_\Bbbk \setminus S$) define the local ring $\mathcal{O}_v = \{x \in \Bbbk : |x|_v \leq 1\}$. We need a few probably well-known local-to-global results, relating (weak) $\mathcal{O}_v$-equivalence of augmented forms for $v \notin S$ to $\mathcal{O}_S$-equivalence. We have inserted the proofs for lack of a good reference.

Lemma 3.2. *Let F^*, G^* be two augmented $(K_0, \dots, K_t)$-forms such that F^*, G^* are $\mathcal{O}_v$-equivalent for every $v \notin S$. Then F^*, G^* are $\mathcal{O}_S$-equivalent.*

Proof. By assumption, for every $v \notin S$ there is $U_v \in \mathrm{GL}_2(\mathcal{O}_v)$ such that $G^* = F_{U_v}^*$. By Lemma 3.1, (ii) for $v \notin S$ we have $U_v = \rho_v U_0$ where U_0 is one of the matrices U_v ($v \notin S$), and $\rho_v \in \Bbbk^*$, $\rho_v^r = 1$. Then clearly, $G^* = F_{U_0}^*$ and $U_0 \in \mathrm{GL}_2(\mathcal{O}_v)$ for $v \notin S$, so $U_0 \in \mathrm{GL}_2(\mathcal{O}_S)$. Lemma 3.2 follows. □

The following result is more involved.

Lemma 3.3. *Let $\mathcal{C}^*$ be a collection of augmented $(K_0, \dots, K_t)$-forms such that for every pair $F^*, G^* \in \mathcal{C}^*$ we have that F^*, G^* are weakly $\mathcal{O}_v$-equivalent for every $v \notin S$. Let $s := \#S$. Then $\mathcal{C}^*$ is contained in the union of at most r^s $\mathcal{O}_S$-equivalence classes if r is odd, and in the union of at most $r^s h_2(\mathcal{O}_S)$ $\mathcal{O}_S$-equivalence classes if r is even.*

Before proving Lemma 3.3 we make some preparations.

If R is a domain with quotient field K, then by a fractional R-ideal, we mean a subset $\mathfrak{a} \neq \{0\}$ of K such that $\lambda\mathfrak{a}$ is an ideal of R for some $\lambda \in K^*$. For $v \notin S$, denote by $\mathfrak{p}_v$ the prime ideal of $\mathcal{O}_S$ corresponding to v, i.e., $\mathfrak{p}_v = \{x \in \mathcal{O}_S : |x|_v < 1\}$, and by ord_v the discrete valuation corresponding to v. Thus, $[x] = \prod_{v \notin S} \mathfrak{p}_v^{\mathrm{ord}_v(x)}$ for $x \in \Bbbk^*$.

Let $F^*, G^* \in \mathcal{C}^*$. Thus, for every $v \notin S$ there are $U_v \in \mathrm{GL}_2(\mathcal{O}_v)$, $\lambda_v \in \mathcal{O}_v^*$ such that $G^* = \lambda_v F^*_{U_v}$. Choose any $U \in \mathrm{GL}_2(\Bbbk)$, $\lambda \in \Bbbk^*$ such that $G^* = \lambda F^*_U$. Then by (ii) of Lemma 3.1, for each $v \notin S$ there is a $\rho_v \in \Bbbk^*$ such that

$$U_v = \rho_v U\,, \quad \lambda_v = \rho_v^{-r}\lambda\,. \tag{3.2}$$

Define the $\mathcal{O}_S$-fractional ideal

$$\mathfrak{a}(F^*, G^*) := \prod_{v \notin S} \mathfrak{p}_v^{\mathrm{ord}_v(\rho_v)}\,. \tag{3.3}$$

This is well-defined, since for all but finitely many $v \notin S$ we have $\lambda \in \mathcal{O}_v^*$, whence $\rho_v \in \mathcal{O}_v^*$, whence $\mathrm{ord}_v(\rho_v) = 0$. Let $\mathfrak{A}(F^*, G^*)$ denote the ideal class of $\mathfrak{a}(F^*, G^*)$, that is, $\{\mu \cdot \mathfrak{a}(F^*, G^*) : \mu \in \Bbbk^*\}$.

The fractional ideal $\mathfrak{a}(F^*, G^*)$ depends on the particular choice of U_v, λ_v ($v \notin S$), U, λ, but its ideal class $\mathfrak{A}(F^*, G^*)$ does not. Indeed, for $v \notin S$, choose $U'_v \in \mathrm{GL}_2(\mathcal{O}_v)$, $\lambda'_v \in \mathcal{O}_v^*$ such that $G^* = \lambda'_v F^*_{U'_v}$ and then choose $U' \in \mathrm{GL}_2(\Bbbk)$ and $\lambda' \in \Bbbk^*$ such that $G^* = \lambda' F^*_{U'}$. By (ii) of Lemma 3.1 there are $\rho'_v \in \Bbbk^*$ such that $U'_v = \rho'_v U'$, $\lambda'_v = {\rho'_v}^{-r}\lambda'$ for $v \notin S$. This gives rise to a fractional ideal $\mathfrak{a}'(F^*, G^*) = \prod_{v \notin S} \mathfrak{p}_v^{\mathrm{ord}_v(\rho'_v)}$. Again by (ii) of Lemma 3.1, there is $\mu \in \Bbbk^*$ such that $U' = \mu U$ and $\lambda' = \mu^{-r}\lambda$. This implies for $v \notin S$ that $U'_v = \rho'_v \mu \rho_v^{-1} U_v$, hence $\rho'_v \mu \rho_v^{-1} \in \mathcal{O}_v^*$, and so $\mathrm{ord}_v(\rho'_v) = \mathrm{ord}_v(\rho_v) - \mathrm{ord}_v(\mu)$. Therefore, $\mathfrak{a}'(F^*, G^*) = \mu^{-1}\mathfrak{a}(F^*, G^*)$.

Lemma 3.4. (i) *Let $F^*, G^* \in \mathcal{C}^*$. Then $\mathfrak{A}(F^*, G^*)^{\gcd(r,2)}$ is the principal ideal class.*

(ii) *Let $F^*, G^* \in \mathcal{C}^*$ and suppose that $\mathfrak{A}(F^*, G^*)$ is the principal ideal class. Then F^*, G^* are weakly $\mathcal{O}_S$-equivalent.*

(iii) *Let $F^*, G^*, H^* \in \mathcal{C}^*$. Then $\mathfrak{A}(F^*, H^*) = \mathfrak{A}(F^*, G^*) \cdot \mathfrak{A}(G^*, H^*)$.*

Proof. (i) According to (3.2) we have for $v \notin S$, that

$$\begin{aligned}\operatorname{ord}_v(\rho_v^2) &= \operatorname{ord}_v(\det U_v(\det U)^{-1}) = \operatorname{ord}_v((\det U)^{-1}\,,\\ \operatorname{ord}_v(\rho_v^r) &= \operatorname{ord}_v(\lambda\lambda_v^{-1}) = \operatorname{ord}_v(\lambda)\,,\end{aligned}$$

and so according to (3.3), $\mathfrak{a}(F^*,G^*)^2 = [\det U]^{-1}$ and $\mathfrak{a}(F^*,G^*)^r = [\lambda]$, where $[a]$ denotes the $\mathcal{O}_S$-fractional ideal generated by a. This implies (i).

(ii) Let $\mathfrak{a}(F^*,G^*)$ be given by (3.2), (3.3). Then by our assumption, $\mathfrak{a}(F^*,G^*) = [\rho]$ with $\rho \in \Bbbk^*$. This implies $\rho\rho_v^{-1} \in \mathcal{O}_v^*$ for $v \notin S$. Put $V := \rho U$, $\mu := \rho^{-r}U$. Then $G^* = \mu F_V^*$. Further, by (3.2), we have for $v \notin S$, that $U_v = \rho_v\rho^{-1}V$, $\lambda_v = (\rho_v\rho^{-1})^{-r}\mu$, which implies $V \in \mathrm{GL}_2(\mathcal{O}_v)$ and $\mu \in \mathcal{O}_v^*$. Hence $V \in \mathrm{GL}_2(\mathcal{O}_S)$ and $\mu \in \mathcal{O}_S^*$. Our assertion (ii) follows.

(iii) Straightforward computation. □

Proof of Lemma 3.3. Fix $F^* \in \mathcal{C}^*$. We subdivide $\mathcal{C}^*$ into classes such that two augmented forms $G_1^*, G_2^* \in \mathcal{C}^*$ are in the same class if and only if their corresponding ideal classes $\mathfrak{A}(F^*,G_1^*)$, $\mathfrak{A}(F^*,G_2^*)$ coincide. Let $F_1^*,\dots,F_h^*$ be a full system of representatives for these classes. Notice that by (i) of Lemma 3.4, we have $h \le 1$ if r is odd, and $h \le h_2(\mathcal{O}_S)$ if r is even.

Fix $i \in \{1,\dots,h\}$ and take any G^* from the class represented by F_i^*. According to (iii) of Lemma 3.4, we have that $\mathfrak{A}(F_i^*,G^*)$ is the principal ideal class. So by (ii) of Lemma 3.4, there are $U \in \mathrm{GL}_2(\mathcal{O}_S)$ and $\varepsilon \in \mathcal{O}_S^*$ such that $G^* = \varepsilon(F_i^*)_U$. The group $\mathcal{O}_S^*$ is the direct product of $s = \#S$ cyclic groups, with generators $\varepsilon_1,\dots,\varepsilon_s$, say. So we may write $\varepsilon = \varepsilon_1^{w_1}\cdots\varepsilon_s^{w_s}\eta^r$, with $w_1,\dots,w_r \in \{0,\dots,r-1\}$ and $\eta \in \mathcal{O}_S^*$. Consequently, $G^* = \varepsilon_1^{w_1}\cdots\varepsilon_s^{w_s}(F_i^*)_{\eta U}$.

It follows that $\mathcal{C}^*$ falls apart in at most $r^s h$ $\mathcal{O}_S$-equivalence classes, each represented by $\varepsilon_1^{w_1}\cdots\varepsilon_s^{w_s}F_i^*$ for certain $w_1,\dots,w_s \in \{0,\dots,r-1\}$, $i \in \{1,\dots,h\}$. Lemma 3.3 follows. □

4. From $\Bbbk$-equivalence classes to $\mathcal{O}_S$-equivalence classes.

We keep the notation introduced in §§2-3. Let $K_0,\dots,K_t$ be a sequence of finite extensions of $\Bbbk$. Let $\mathcal{C}^*$ be a set of augmented $(K_0,\dots,K_t)$-forms which are all $\Bbbk$-equivalent to one another, and such that every $F^* =$

$(F, \theta_{0,F}, \dots, \theta_{t,F}) \in \mathcal{C}^*$ satisfies $F \in \mathcal{O}_S[X, Y]$ and (2.11). We will show that $\mathcal{C}^*$ is contained in finitely many $\mathcal{O}_S$-equivalence classes and estimate from above the number of these classes. We first localize at a place $v \notin S$, and estimate from above the number of $\mathcal{O}_v$-equivalence classes containing $\mathcal{C}^*$. Then we use Lemma 3.2.

Let $v \in M_{\Bbbk}$ be a finite place. Denote by $\mathcal{O}_v$ the local ring of v and by $\mathfrak{p}_v$ the maximal ideal of $\mathcal{O}_v$, i.e.,

$$\mathcal{O}_v = \{x \in \Bbbk : |x|_v \leq 1\}, \quad \mathfrak{p}_v = \{x \in \Bbbk : |x|_v < 1\}.$$

Put $Nv := \#(\mathcal{O}_v/\mathfrak{p}_v)$.

Given a finite extension L of $\Bbbk$, we denote by $\mathcal{O}_{L,v}$ the integral closure of $\mathcal{O}_v$ in L. The ring $\mathcal{O}_{L,v}$ is a principal ideal domain with finitely many prime ideals. Further, it is a free $\mathcal{O}_v$-module. The v-discriminant ideal of $L/\Bbbk$ is given by the ideal of $\mathcal{O}_v$,

$$\mathfrak{d}_{L/\Bbbk,v} = D_{L/\Bbbk}(\alpha_1, \dots, \alpha_r) \cdot \mathcal{O}_v\,, \tag{4.1}$$

where $\alpha_1, \dots, \alpha_r$ is any $\mathcal{O}_v$-module basis of $\mathcal{O}_{L,v}$. This does not depend on the choice of $\alpha_1, \dots, \alpha_r$.

We will often denote the fractional $\mathcal{O}_{L,v}$-ideal generated by $a_1, \dots, a_m$ by $[a_1, \dots, a_m]$; from the context it will always be clear in which field L we are working. Given a polynomial $f \in L[X_1, \dots, X_m]$, we denote by $[f]$ the fractional $\mathcal{O}_{L,v}$-ideal generated by the coefficients of f. Then according to Gauss' Lemma,

$$[fg] = [f][g] \quad \text{for} \quad f, g \in L[X_1, \dots, X_m]. \tag{4.2}$$

Below we need some properties for resultants. The resultant of two binary forms $F = a\prod_{i=1}^{r}(X - \alpha_i Y)$, $G = b\prod_{j=1}^{s}(X - \beta_j Y)$ is given by

$$R(F, G) = a^s b^r \prod_{i=1}^{r}\prod_{j=1}^{s}(\alpha_i - \beta_j)\,. \tag{4.3}$$

The resultant $R(F, G)$ is a polynomial in the coefficients of F and G with rational integral coefficients. It is homogeneous of degree s in the coefficients of F and homogeneous of degree r in the coefficients of G. For binary forms

$F_0, \dots, F_t$ we have

$$D(F) = \left(\prod_{i=0}^{t} D(F_i) \right) \cdot \prod_{0 \le i < j \le t} R(F_i, F_j)^2. \tag{4.4}$$

Now let $K_0, \dots, K_t$ be a sequence of finite extensions of $\Bbbk$. Denote the normal closure over $\Bbbk$ of the compositum $K_0 \dots K_t$ by L. Put $r_i := [K_i : \Bbbk]$ $(i = 0, \dots, t)$ and $r := r_0 + \cdots + r_t$. For $i = 0, \dots, t$ let $\xi \mapsto \xi^{(i,j)}$ $(j = 1, \dots, r_i)$ denote the $\Bbbk$-isomorphic embeddings of K_i into L.

We prove some properties for augmented $(K_0, \dots, K_t)$-forms.

Lemma 4.1. **(i)** *Let $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ be an augmented $(K_0, \dots, K_t)$-form.*

(i) *Let $v \in M_\Bbbk$ be a finite place and suppose $F \in \mathcal{O}_v[X, Y]$. Then there is an ideal $\mathfrak{c}_v$ of $\mathcal{O}_v$ such that*

$$D(F) \cdot \mathcal{O}_v = \mathfrak{c}_v^2 \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v} \,.$$

(ii) *Suppose that $F \in \mathcal{O}_S[X, Y]$. Then there is an ideal $\mathfrak{c}$ of $\mathcal{O}_S$ such that*

$$D(F) \cdot \mathcal{O}_S = \mathfrak{c}^2 \mathfrak{d}_{K_0/\Bbbk,S} \dots \mathfrak{d}_{K_t/\Bbbk,S} \,.$$

Proof. (ii) follows by applying (i) for every $v \notin S$. We prove (i). Since $\mathcal{O}_v$ is a principal ideal domain we may write $F = F_0 F_1 \dots F_t$, where $F_i^* = (F_i, \theta_{i,F})$ is an augmented K_i-form and $F_i \in \mathcal{O}_v[X, Y]$ for $i = 0, \dots, t$. In view of (4.4) and since $R(F_i, F_j) \in \mathcal{O}_v$ for all i, j, it suffices to show that $D(F_i) \cdot \mathcal{O}_v = \mathfrak{c}_{v,i}^2 \mathfrak{d}_{K_i/\Bbbk,v}$ for some ideal $\mathfrak{c}_{v,i}$ of $\mathcal{O}_v$.

Write $F_i(X, Y) = a_0 X^{r_i} + a_1 X^{r_i - 1} Y + \cdots + a_{r_i} Y^{r_i}$, and put $\omega_1 = 1$, $\omega_2 = a_0 \theta_{i,F}$, $\omega_3 = a_0 \theta_{i,F}^2 + a_1 \theta_{i,F}$, $\dots$, $\omega_{r_i} = a_0 \theta_{i,F}^{r_i - 1} + a_1 \theta_{i,F}^{r_i - 2} + \cdots + a_{r_i - 2} \theta_{i,F}$. Let $\{\alpha_1, \dots, \alpha_{r_i}\}$ be an $\mathcal{O}_v$-basis of $\mathcal{O}_{K_i,v}$. Then since $\omega_1, \dots, \omega_{r_i} \in \mathcal{O}_{K_i,v}$ we have $\omega_i = \sum_{j=1}^{r_i} \xi_{ij} \alpha_j$ with $\xi_{ij} \in \mathcal{O}_v$. Invoking (2.6) we obtain

$$\begin{aligned} D(F_i) \cdot \mathcal{O}_v &= D_{K_i/\Bbbk}(\omega_1, \dots, \omega_{r_i}) \cdot \mathcal{O}_v \\ &= \det(\xi_{ij})^2 D_{K_i/\Bbbk}(\alpha_1, \dots, \alpha_{r_i}) \cdot \mathcal{O}_v = \det(\xi_{ij})^2 \mathfrak{d}_{K_i/\Bbbk,v}. \end{aligned}$$

Now Lemma 4.1 follows. □

Let again $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ be an augmented $(K_0, \dots, K_t)$-form. Henceforth we fix a finite place $v \in M_\Bbbk$ and assume that $F \in \mathcal{O}_v[X, Y]$. For

$i = 0, \dots, t$, choose $\alpha_{i,F}$, $\beta_{i,F}$ such that

$$\begin{aligned} &\alpha_{i,F}, \beta_{i,F} \in \mathcal{O}_{K_i,v}, \quad \frac{\alpha_{i,F}}{\beta_{i,F}} = \theta_{i,F}, \quad [\alpha_{i,F}, \beta_{i,F}] = [1] \text{ if } \theta_{i,F} \neq \infty, \\ &\alpha_{i,F} \in \mathcal{O}_v^*, \beta_{i,F} = 0 \text{ if } \theta_{i,F} = \infty; \end{aligned} \tag{4.5}$$

this is possible since $\mathcal{O}_{K_i,v}$ is a principal ideal domain. We may write

$$F = \varepsilon_F \prod_{i=0}^{t} \prod_{j=1}^{r_i} (\beta_{i,F}^{(i,j)} X - \alpha_{i,F}^{(i,j)} Y) \quad \text{with } \varepsilon_F \in \mathcal{O}_v,\ \varepsilon_F \neq 0. \tag{4.6}$$

Indeed, a priori we know only that $\varepsilon_F \in \Bbbk^*$. But by Gauss' Lemma we have

$$[F] = [\varepsilon_F] \prod_{i=0}^{t} \prod_{j=1}^{r_i} [\beta_{i,F}^{(i,j)}, \alpha_{i,F}^{(i,j)}] = [\varepsilon_F], \tag{4.7}$$

and thus $\varepsilon_F \in \mathcal{O}_v$ follows.

To pass from double to single indices we define a map

$$\begin{aligned} \varphi : 1, \dots, r \ \to &(0,1), \dots, (0, r_0), \dots \\ &\dots, (1,1), \dots, (1, r_1), \dots, (t,1), \dots, (t, r_t), \end{aligned} \tag{4.8}$$

meaning that φ maps $1, \dots, r$ to $(0,1), \dots, (t, r_t)$, respectively. We define the ideals of $\mathcal{O}_{L,v}$:

$$\mathfrak{d}_{kl}(F^*) = [\alpha_{i_1,F}^{(i_1,j_1)} \beta_{i_2,F}^{(i_2,j_2)} - \alpha_{i_2,F}^{(i_2,j_2)} \beta_{i_1,F}^{(i_1,j_1)}] \tag{4.9}$$

for $k, l = 1, \dots, r$, $k < l$, where $\varphi(k) = (i_1, j_1)$, $\varphi(l) = (i_2, j_2)$. Notice that the ideals $\mathfrak{d}_{kl}(F^*)$ are independent of the choice of $\alpha_{i,F}, \beta_{i,F}$ in (4.5). By (4.6), (2.1), we have

$$\prod_{1 \leq k < l \leq r} \mathfrak{d}_{kl}(F^*)^2 \supseteq [D(F)]. \tag{4.10}$$

Further, if G^* is an augmented $(K_0, \dots, K_t)$-form which is $\mathcal{O}_v$-equivalent to F^* then

$$\mathfrak{d}_{kl}(F^*) = \mathfrak{d}_{kl}(G^*) \text{ for } 1 \leq k < l \leq r. \tag{4.11}$$

The latter can be seen easily by taking $U \in \mathrm{GL}_2(\mathcal{O}_v)$ such that $G^* = F_U^*$ and putting $\binom{\alpha_{i,G}}{\beta_{i,G}} := U^{-1} \binom{\alpha_{i,F}}{\beta_{i,F}}$, $\theta_{i,G} := \langle U \rangle^{-1} \theta_{i,F}$ for $i = 0, \dots, t$. Then (4.5), (4.6), (4.9) hold with everywhere G, G^* in place of F, F^* and we obtain $\mathfrak{d}_{kl}(G^*) = (\det U^{-1}) \cdot \mathfrak{d}_{kl}(F^*) = \mathfrak{d}_{kl}(F^*)$ since $\det U^{-1} \in \mathcal{O}_v^*$.

Lemma 4.2. *There are ideals $\mathfrak{d}_{kl}$ of $\mathcal{O}_{L,v}$ independent of F^* such that*

$$\mathfrak{d}_{kl}(F^*) \subseteq \mathfrak{d}_{kl} \quad \textit{for} \quad 1 \le k < l \le r, \tag{4.12}$$

$$\prod_{1\le k<l\le r} \mathfrak{d}_{kl}^2 \subseteq \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v}. \tag{4.13}$$

Proof. Take $i \in \{0,\dots,t\}$ and choose an $\mathcal{O}_v$-basis $\{\alpha_{i,1},\dots,\alpha_{i,r_i}\}$ of $\mathcal{O}_{K_i,v}$. Then there is a polynomial $I_{K_i/\Bbbk} \in \mathcal{O}_v[X_1,\dots,X_{r_i}]$ (the index form of $K_i/\Bbbk$ with respect to $\alpha_{i,1},\dots,\alpha_{i,r_i}$) such that

$$\prod_{1\le j_1<j_2\le r_i} \left(\sum_{m=1}^{r_i} \alpha_{i,m}^{(i,j_1)} X_m - \sum_{m=1}^{r_i} \alpha_{i,m}^{(i,j_2)} X_m\right)^2 = D_{K_i/\Bbbk}(\alpha_{i,1},\dots,\alpha_{i,r_i}) I_{K_i/\Bbbk}^2(X_1,\dots,X_{r_i}).$$

Define the ideal of $\mathcal{O}_{L,v}$:

$$\mathfrak{b}_{i,j_1,j_2} := \left[\alpha_{i,1}^{(i,j_1)} - \alpha_{i,1}^{(i,j_2)}, \dots, \alpha_{i,r_i}^{(i,j_1)} - \alpha_{i,r_i}^{(i,j_2)}\right]. \tag{4.14}$$

Then by Gauss' Lemma

$$\prod_{1\le j_1<j_2\le r_i} \mathfrak{b}_{i,j_1,j_2}^2 \subseteq [D_{K_i/\Bbbk}(\alpha_{i,1},\dots,\alpha_{i,r_i})] = \mathfrak{d}_{K_i/\Bbbk,v}. \tag{4.15}$$

Moreover $\xi^{(i,j_1)} - \xi^{(i,j_2)} \in \mathfrak{b}_{i,j_1,j_2}$ for any $\xi \in \mathcal{O}_{K_i,v}$. Hence for the numbers $\alpha_{i,F}, \beta_{i,F}$ chosen in (4.9) we have

$$\alpha_{i,F}^{(i,j_1)} \beta_{i,F}^{(i,j_2)} - \alpha_{i,F}^{(i,j_2)} \beta_{i,F}^{(i,j_1)} \in \mathfrak{b}_{i,j_1,j_2} \quad (1 \le j_1 < j_2 \le r_i). \tag{4.16}$$

Let φ be the map from (4.8). Define $\mathfrak{d}_{kl}$ by

$$\begin{cases} \mathfrak{d}_{kl} = \mathfrak{b}_{i,j_1,j_2} & \text{if } \ \varphi(k) = (i,j_1),\ \varphi(l) = (i,j_2) \\ \mathfrak{d}_{kl} = [1] & \text{if } \ \varphi(k) = (i_1,j_1),\ \varphi(l) = (i_2,j_2) \ \text{ with } \ i_1 \ne i_2. \end{cases} \tag{4.17}$$

Then (4.12), (4.13) follow at once from (4.16), (4.17), (4.10). □

Let $\mathfrak{c}_v = \mathfrak{c}_v(F^*)$ be the ideal from (i) of Lemma 4.1. Define $\rho_v(F^*) \in \mathbb{Z}$ by $\mathfrak{c}_v = \mathfrak{p}_v^{\rho_v(F^*)}$. Thus, $[D(F)] = \mathfrak{p}_v^{2\rho_v(F^*)} \prod_{i=0}^t \mathfrak{d}_{K_i/\Bbbk,v}$.

Lemma 4.3. *Let ρ be a non-negative integer. Then as the tuple $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ runs through the collection of augmented $(K_0, \dots, K_t)$-forms with*

$$F \in \mathcal{O}_v[X, Y] \tag{4.18}$$

$$\rho_v(F^*) \le \rho\,, \tag{4.19}$$

the tuple $(\mathfrak{d}_{kl}(F^*) : 1 \le k < l \le r)$ runs through a set of cardinality at most

$$\binom{2\rho + \frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)} \tag{4.20}$$

depending only on $K_0, \dots, K_t$, v, ρ.

Proof. We define an action of the Galois group $\mathrm{Gal}(L/\Bbbk)$ on the set of subscripts $\{1, \dots, r\}$ as follows. Denote by A the set of all r-tuples $(\gamma_1, \dots, \gamma_r)$ with the property that there are $\xi_0 \in K_0$, $\xi_1 \in K_1, \dots, \xi_t \in K_t$ such that

$$(\gamma_1, \dots, \gamma_r) = (\xi_0^{(0,1)}, \dots, \xi_0^{(0,r_0)}, \dots, \xi_t^{(t,1)}, \dots, \xi_t^{(t,r_t)})\,.$$

Then there is a homomorphism $\tau \mapsto \tau^*$ from $\mathrm{Gal}(L/\Bbbk)$ to the permutation group of $\{1, \dots, r\}$, such that

$$\tau(\gamma_k) = \gamma_{\tau^*(k)} \quad \text{for} \quad (\gamma_1, \dots, \gamma_r) \in A, \quad k = 1, \dots, r. \tag{4.21}$$

Notice that if $\varphi(k) = (i, j)$, then $\varphi(\tau^*(k)) = (i, j')$ for some $j' \in \{1, \dots, r_i\}$ where φ is the map given by (4.8).

For each $k, l \in \{1, \dots, r\}$, with $k < l$, we define the subfield L_{kl} of L by

$$\mathrm{Gal}(L/L_{kl}) = \{\tau \in \mathrm{Gal}(L/\Bbbk) : \tau^*(\{k, l\}) = \{k, l\}\} \tag{4.22}$$

(i.e. $\tau^*(k) = k, \tau^*(l) = l$, or $\tau^*(k) = l, \tau^*(l) = k$). We partition the set of pairs $\{(k, l) : k, l \in \{1, \dots, r\}, k < l\}$ into orbits $C_1, \dots, C_n$ in such a way that (k_1, l_1), (k_2, l_2) belong to the same orbit if and only if $\{k_2, l_2\} = \tau^*(\{k_1, l_1\})$ for some $\tau \in \mathrm{Gal}(L/\Bbbk)$. For each $m = 1, \dots, n$ we choose a representative (k_m, l_m) of C_m. Then if (k, l) runs through C_m, the field L_{kl} runs through all conjugates over $\Bbbk$ of $L_{k_m l_m}$, and so

$$\#C_m = [L_{k_m l_m} : \Bbbk] \quad \text{for} \quad m = 1, \dots, n. \tag{4.23}$$

Now let $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ be an augmented $(K_0, \dots, K_t)$-form satisfying (4.18), (4.19). Define the ideals

$$\mathfrak{a}_{kl}(F^*) := \mathfrak{d}_{kl}(F^*)^2 \mathfrak{d}_{kl}^{-2} \quad (1 \le k < l \le r).$$

By Lemma 4.2 we have $\mathfrak{a}_{kl}(F^*) \subseteq \mathcal{O}_{L,v}$, and by (4.9), (4.14), (4.17), the ideal $\mathfrak{a}_{kl}(F^*)$ is generated by elements from the field L_{kl}. It is clear that the ideals $\mathfrak{a}_{kl}(F^*)$ determine $\mathfrak{d}_{kl}(F^*)$ $(1 \le k < l \le r)$ uniquely.

For brevity put

$$L_m := L_{k_m l_m}, \quad \mathfrak{a}_m(F^*) := \mathfrak{a}_{k_m l_m}(F^*) \cap L_m \quad (m = 1, \dots, n);$$

thus $\mathfrak{a}_m(F^*)$ is an ideal of $\mathcal{O}_{L_m,v}$. The ideals $\mathfrak{a}_1(F^*), \dots, \mathfrak{a}_n(F^*)$ determine $\mathfrak{d}_{kl}(F^*)$ $(1 \le k < l \le r)$ uniquely. Indeed, they determine the ideals $\mathfrak{a}_{k_m l_m}(F^*)$ $(m = 1, \dots, n)$ of $\mathcal{O}_{L,v}$ since the latter are generated by elements from L_m; and then by taking conjugates over $\Bbbk$ one obtains all ideals $\mathfrak{a}_{kl}(F^*)$ $(1 \le k < l \le r)$, which, as mentioned before, determine $\mathfrak{d}_{kl}(F^*)$ $(1 \le k < l \le r)$.

For $m = 1, \dots, n$ let $\mathfrak{P}_{m1}, \dots, \mathfrak{P}_{mg_m}$ be the prime ideals of $\mathcal{O}_{L_m,v}$. Thus,

$$\mathfrak{a}_m(F^*) = \mathfrak{P}_{m1}^{w_{m1}(F^*)} \dots \mathfrak{P}_{mg_m}^{w_{mg_m}(F^*)}$$

where $w_{m1}(F^*), \dots, w_{mg_m}(F^*)$ are non-negative integers since $\mathfrak{a}_m(F^*)$ is an ideal of $\mathcal{O}_{L_m,v}$. Now the tuple of integers

$$\underline{w}(F^*) := (w_{m,k}(F^*) : m = 1, \dots, n,\ k = 1, \dots, g_m)$$

determines uniquely the ideals $\mathfrak{a}_m(F^*)$ $(m = 1, \dots, n)$, hence the ideals $\mathfrak{d}_{kl}(F^*)$ $(1 \le k < l \le r)$. Therefore it suffices to show that for $\underline{w}(F^*)$ there are at most $\binom{2\rho + \frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)}$ possibilities.

Now on the one hand we have by (4.10), (4.13), (i) of Lemma 4.1, and assumption (4.19),

$$\begin{aligned} \prod_{1 \le k < l \le r} \mathfrak{a}_{kl}(F^*) &\supseteq D(F)(\mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v})^{-1} \cdot \mathcal{O}_{L,v} = \mathfrak{c}_v^2 \mathcal{O}_{L,v} \\ &\supseteq \mathfrak{p}_v^{2\rho} \cdot \mathcal{O}_{L,v}\,, \end{aligned}$$

while on the other hand,

$$\begin{aligned}\prod_{1\le k<l\le r}\mathfrak{a}_{kl}(F^*) &= \prod_{m=1}^{n}\prod_{(k,l)\in C_m}\mathfrak{a}_{kl}(F^*) = \prod_{m=1}^{n} N_{L_m/\Bbbk}(\mathfrak{a}_m(F^*))\cdot\mathcal{O}_{L,v}\\ &= \prod_{m=1}^{n}\prod_{h=1}^{g_m} N_{L_m/\Bbbk}(\mathfrak{P}_{mh})^{w_{mh}(F^*)}\cdot\mathcal{O}_{L,v}\\ &= \prod_{m=1}^{n}\prod_{h=1}^{g_m}\mathfrak{p}_v^{f_{mh}w_{mh}(F^*)}\cdot\mathcal{O}_{L,v}\\ &\subseteq \mathfrak{p}_v^{\sum_{m=1}^{n}\sum_{h=1}^{g_m}w_{mh}(F^*)}\cdot\mathcal{O}_{L,v},\end{aligned}$$

where f_{mh} is the residue class degree of $\mathfrak{P}_{mh}$ over $\mathfrak{p}_v$. Therefore,

$$\sum_{m=1}^{n}\sum_{h=1}^{g_m} w_{mh}(F^*)\le 2\rho. \tag{4.24}$$

Now $g_m\le [L_m:\Bbbk]\le \#C_m$ for $m=1,\dots,n$ in view of (4.23). Hence the number of summands on the left-hand side is at most

$$\sum_{m=1}^{n}\#C_m = \#\{(k,l): 1\le k<l\le r\} = \frac{1}{2}r(r-1).$$

By elementary combinatorics, the number of tuples of non-negative integers $\underline{w}(F^*)$ with (4.24) is at most

$$\binom{2\rho+\frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)}.$$

As observed above, this implies Lemma 4.3. □

Let $\mathcal{C}^*$ be a $\Bbbk$-equivalence class of augmented $(K_0,\dots,K_t)$-forms. Given an ideal $\mathfrak{c}_v$ of $\mathcal{O}_v$ and a tuple of ideals $\{\mathfrak{d}_{kl}: 1\le k<l\le r\}$ of $\mathcal{O}_{L,v}$, let $\mathcal{C}^*(\mathfrak{c}_v,\{\mathfrak{d}_{kl}\})$ denote the collection of augmented $(K_0,\dots,K_t)$-forms $F^* = (F,\theta_{0,F},\dots,\theta_{t,F})$ such that

$$F^*\in\mathcal{C}^*; \tag{4.25}$$

$$F\in\mathcal{O}_v[X,Y]; \tag{4.26}$$

$$[D(F)] = \mathfrak{c}_v^2\cdot\mathfrak{d}_{K_0/\Bbbk,v}\dots\mathfrak{d}_{K_t/\Bbbk,v}; \tag{4.27}$$

$$\mathfrak{d}_{kl}(F^*) = \mathfrak{d}_{kl}\quad\text{for}\quad k,l\in\{1,\dots,r\},\ 1\le k<l\le r. \tag{4.28}$$

Lemma 4.4. *Suppose* $r := \sum_{i=0}^{t}[K_i : \Bbbk] \geq 3$. *Let* $\mathfrak{c}_v$ *be an ideal of* $\mathcal{O}_v$ *and* $\{\mathfrak{d}_{kl} : 1 \leq k < l \leq r\}$ *a collection of ideals from* $\mathcal{O}_{L,v}$ *such that the set* $\mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ *is not contained in a single* $\mathcal{O}_v$*-equivalence class. Then*

$$\mathfrak{c}_v \subseteq \mathfrak{p}_v^{\frac{r(r-1)}{2}}, \quad \mathfrak{d}_{kl} \subseteq \mathfrak{p}_v\mathcal{O}_{L,v} \quad \text{for} \quad 1 \leq k < l \leq r, \tag{4.29}$$

and for every $F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ *there is an* H^* *with*

$$H^* \overset{\mathcal{O}_v}{\prec} F^*, \quad H^* \in \mathcal{C}^*(\mathfrak{p}_v^{-\frac{1}{2}r(r-1)}\mathfrak{c}_v, \{\mathfrak{p}_v^{-1}\mathfrak{d}_{kl}\}). \tag{4.30}$$

Proof. If $H^* = (H, \theta_{0,H}, \dots, \theta_{t,H})$ is an augmented form with $H \in \mathcal{O}_v[X, Y]$, then $\mathfrak{d}_{kl}(H^*)$ $(1 \leq k < l \leq r)$ are all ideals of $\mathcal{O}_{L,v}$, and by (i) of Lemma 4.1, there is an ideal $\mathfrak{c}_v' \subseteq \mathcal{O}_v$ such that $[D(H)] = \mathfrak{c}_v'^2 \cdot \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v}$. So if we have shown that there exists an H^* with (4.30), then (4.29) follows automatically.

Let $F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$. There is a $G^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ which is not $\mathcal{O}_v$-equivalent to F^*. This means that there is a matrix $A \in \mathrm{GL}_2(\Bbbk)$ with $A \notin \mathrm{GL}_2(\mathcal{O}_v)$ such that $G^* = F_A^*$. Since $\mathcal{O}_v$ is a principal ideal domain, there are matrices $U_1, U_2 \in \mathrm{GL}_2(\mathcal{O}_v)$ such that

$$A = U_1 \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} U_2$$

with

$$\alpha, \delta \in \Bbbk^*, \quad \frac{\delta}{\alpha} \in \mathcal{O}_v, \quad \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \notin \mathrm{GL}_2(\mathcal{O}_v). \tag{4.31}$$

Put $\tilde{F}^* := F_{U_1}^*$, $\tilde{G}^* := G_{U_2^{-1}}^*$. Then

$$\tilde{G}^* = \tilde{F}^*_{\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \delta \end{smallmatrix}\right)}. \tag{4.32}$$

Further, $\tilde{F}^* \overset{\mathcal{O}_v}{\sim} F^*$, $\tilde{G}^* \overset{\mathcal{O}_v}{\sim} G^*$, so by (4.11), (2.3),

$$\tilde{F}^*, \tilde{G}^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\}). \tag{4.33}$$

Clearly, in view of (iv) of Lemma 3.1, it follows that there is an H^* with (4.30) once we have proved that there is an H^* with

$$H^* \overset{\mathcal{O}_v}{\prec} \tilde{F}^*, \quad H^* \in \mathcal{C}^*(\mathfrak{p}_v^{-\frac{1}{2}r(r-1)}\mathfrak{c}_v, \{\mathfrak{p}_v^{-1}\mathfrak{d}_{kl}\}). \tag{4.34}$$

By (4.33),(4.27), (4.32), (2.2), we have

$$[D(\tilde{F})] = \mathfrak{c}_v^2 \prod_{i=0}^{t} \mathfrak{d}_{K_i/\mathbb{k},v} = [D(\tilde{G})] = [\alpha\delta]^{r(r-1)}[D(\tilde{F})]\,,$$

and together with (4.31) this implies

$$\delta \in \mathcal{O}_v, \quad \delta \notin \mathcal{O}_v^*, \quad \alpha\delta \in \mathcal{O}_v^*. \tag{4.35}$$

Write $\tilde{F}^* = (\tilde{F}, \theta_{0,\tilde{F}}, \dots, \theta_{t,\tilde{F}})$. Then by (4.32) we have

$$\tilde{G}^* = \Big(\tilde{F}_{\left(\begin{smallmatrix}\alpha & 0\\ 0 & \delta\end{smallmatrix}\right)}, \frac{\delta}{\alpha}\theta_{0,\tilde{F}}, \dots, \frac{\delta}{\alpha}\theta_{t,\tilde{F}}\Big)\,.$$

Similarly as in (4.5), choose $\alpha_{i,\tilde{F}}, \beta_{i,\tilde{F}} \in \mathcal{O}_{K_i,v}$ such that $\alpha_{i,\tilde{F}}/\beta_{i,\tilde{F}} = \theta_{i,\tilde{F}}$ and $[\alpha_{i,\tilde{F}}, \beta_{i,\tilde{F}}] = [1]$ if $\theta_{i,\tilde{F}} \neq \infty$, and $\alpha_{i,\tilde{F}} \in \mathcal{O}_v^*$, $\beta_{i,\tilde{F}} = 0$ if $\theta_{i,\tilde{F}} = \infty$. Likewise, choose $\alpha_{i,\tilde{G}}, \beta_{i,\tilde{G}} \in \mathcal{O}_{K_i,v}$ such that $\alpha_{i,\tilde{G}}/\beta_{i,\tilde{G}} = \delta\theta_{i,\tilde{F}}/\alpha$ and $[\alpha_{i,\tilde{G}}, \beta_{i,\tilde{G}}] = [1]$ if $\theta_{i,\tilde{F}} \neq \infty$, and $\alpha_{i,\tilde{G}} \in \mathcal{O}_v^*$, $\beta_{i,\tilde{G}} = 0$ if $\theta_{i,\tilde{F}} = \infty$. Then for $i = 0, \dots, t$ there is a $\lambda_i \in K_i^*$ such that

$$(\alpha_{i,\tilde{G}}, \beta_{i,\tilde{G}}) = \lambda_i(\delta\alpha_{i,\tilde{F}}, \alpha\beta_{i,\tilde{F}}) \ \text{ for } \ i = 0, \dots, t. \tag{4.36}$$

Take two pairs (i_1, j_1), (i_2, j_2) from $\{(i,j) : i = 0, \dots, t,\ j = 1, \dots, r_i\}$. Let $k, l \in \{1, \dots, r\}$ be such that $\varphi(k) = (i_1, j_1), \varphi(l) = (i_2, j_2)$, where φ is the map from (4.8). Then by (4.33), (4.36), (4.35) and again (4.33),

$$\begin{aligned}
\mathfrak{d}_{kl} =& [\alpha_{i_1,\tilde{G}}^{(i_1,j_1)}\beta_{i_2,\tilde{G}}^{(i_2,j_2)} - \alpha_{i_2,\tilde{G}}^{(i_2,j_2)}\beta_{i_1,\tilde{G}}^{(i_1,j_1)}]\\
=& [\lambda_{i_1}^{(i_1,j_1)}\lambda_{i_2}^{(i_2,j_2)}\alpha\delta(\alpha_{i_1,\tilde{F}}^{(i_1,j_1)}\beta_{i_2,\tilde{F}}^{(i_2,j_2)} - \alpha_{i_2,\tilde{F}}^{(i_2,j_2)}\beta_{i_1,\tilde{F}}^{(i_1,j_1)})]\\
=& [\lambda_{i_1}^{(i_1,j_1)}][\lambda_{i_2}^{(i_2,j_2)}]\mathfrak{d}_{kl}
\end{aligned}$$

and so $[\lambda_{i_1}^{(i_1,j_1)}][\lambda_{i_2}^{(i_2,j_2)}] = [1]$. This holds for any two distinct pairs (i_1, j_1), (i_2, j_2) from $\{(i,j) : i = 0, \dots, t,\ j = 1, \dots, r_i\}$. Taking any pair (i, j) from this set and then any two other pairs (i_1, j_1), (i_2, j_2) (which is possible since by assumption $r_0 + \cdots + r_t = r \geq 3$), we obtain

$$[\lambda_i^{(i,j)}]^2 = \frac{[\lambda_i^{(i,j)}][\lambda_{i_1}^{(i_1,j_1)}][\lambda_i^{(i,j)}][\lambda_{i_2}^{(i_2,j_2)}]}{[\lambda_{i_1}^{(i_1,j_1)}][\lambda_{i_2}^{(i_2,j_2)}]} = [1],$$

so $[\lambda_i^{(i,j)}] = [1]$ for $i = 0, \dots, t,\ j = 1, \dots, r_i$. Together with (4.36), this implies

$$[\delta\alpha_{i,\tilde{F}}, \alpha\beta_{i,\tilde{F}}] = [1] \quad \text{for } i = 0, \dots, t.$$

By (4.35) we have $\delta \in \mathfrak{p}_v$, hence $\delta\alpha_{i,\tilde{F}} \in \mathfrak{p}_v\mathcal{O}_{L,v}$ for $i = 0, \dots, t$. This implies that $\delta\alpha_{i,\tilde{F}}$ is divisible by each prime ideal of $\mathcal{O}_{L,v}$, therefore $[\alpha\beta_{i,\tilde{F}}] = [1]$ for $i = 0, \dots, t$. Since by (4.35), $[\alpha] = [\delta^{-1}] \supseteq \mathfrak{p}_v^{-1}$ we have $\beta_{i,\tilde{F}} \in \mathfrak{p}_v\mathcal{O}_{L,v}$ for $i = 0, \dots, t$. So

$$\beta_{i,\tilde{F}}^{(i,j)} \in \mathfrak{p}_v\mathcal{O}_{L,v} \quad \text{for } i = 0, \dots, t,\ j = 1, \dots, r_i. \tag{4.37}$$

We now construct an H^* with (4.34). Choose Π with $\mathfrak{p}_v = [\Pi]$ and take

$$H^* = \tilde{F}^*_{\left(\begin{smallmatrix}\Pi^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)} = (\tilde{F}_{\left(\begin{smallmatrix}\Pi^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)}, \Pi\theta_{0,\tilde{F}}, \dots, \Pi\theta_{t,\tilde{F}}).$$

Clearly,

$$H^* \overset{\mathcal{O}_v}{\prec} \tilde{F}^*. \tag{4.38}$$

Similarly as in (4.6) we may write

$$\tilde{F} = \varepsilon_{\tilde{F}} \prod_{i=0}^{t} \prod_{j=1}^{r_i} (\beta_{i,\tilde{F}}^{(i,j)} X - \alpha_{i,\tilde{F}}^{(i,j)} Y) \quad \text{with} \quad \varepsilon_{\tilde{F}} \in \mathcal{O}_v.$$

Now (4.37) implies that

$$H := \tilde{F}_{\left(\begin{smallmatrix}\Pi^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)} = \varepsilon_{\tilde{F}} \prod_{i=0}^{t} \prod_{j=1}^{r_i} (\Pi^{-1}\beta_{i,\tilde{F}}^{(i,j)} X - \alpha_{i,\tilde{F}}^{(i,j)} Y) \in \mathcal{O}_{L,v}[X, Y].$$

Since also $H \in \Bbbk[X, Y]$, we have

$$H \in \mathcal{O}_v[X, Y]. \tag{4.39}$$

Moreover, by (2.2), (4.33),

$$[D(H)] = [\Pi^{-r(r-1)} D(\tilde{F})] = (\mathfrak{p}_v^{-\frac{1}{2}r(r-1)}\mathfrak{c}_v)^2 \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v}. \tag{4.40}$$

Further, we have $\Pi\theta_{i,\tilde{F}} = \alpha_{i,\tilde{F}}/\Pi^{-1}\beta_{i,\tilde{F}}$ and $[\alpha_{i,\tilde{F}}, \Pi^{-1}\beta_{i,\tilde{F}}] = [1]$ for $i = 0, \dots, t$. The latter is true since $\alpha_{i,\tilde{F}}, \Pi^{-1}\beta_{i,\tilde{F}} \in \mathcal{O}_{L,v}$ and $[\alpha_{i,\tilde{F}}, \beta_{i,\tilde{F}}] = [1]$. So by definition (4.9) and by (4.33) we have for $1 \le k < l \le r$,

$$\begin{aligned} \mathfrak{d}_{kl}(H^*) =& [\alpha_{i_1,\tilde{F}}^{(i_1,j_1)} \Pi^{-1} \beta_{i_2,\tilde{F}}^{(i_2,j_2)} - \alpha_{i_2,\tilde{F}}^{(i_2,j_2)} \Pi^{-1} \beta_{i_1,\tilde{F}}^{(i_1,j_1)}] \\ =& [\Pi]^{-1} \mathfrak{d}_{kl}(\tilde{F}^*) = \mathfrak{p}_v^{-1} \mathfrak{d}_{kl}, \end{aligned} \tag{4.41}$$

where $\varphi(k) = (i_1, j_1), \varphi(l) = (i_2, j_2)$.

Now by collecting (4.38), (4.39), (4.40), (4.41) and the obvious fact that H^* is $\Bbbk$-equivalent to $\tilde{F}^*$ we infer that indeed H^* satisfies (4.34). This completes the proof of Lemma 4.4. □

Lemma 4.5. *Suppose* $r := \sum_{i=0}^{t}[K_i : \Bbbk] \geq 3$. *Let* $\mathfrak{c}_v, \{\mathfrak{d}_{kl} : 1 \leq k < l \leq r\}$ *be as in Lemma 4.4. Suppose that* $\mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\}) \neq \emptyset$. *Then there is an augmented* $(K_0, \ldots, K_t)$*-form* $F_0^* = (F_0, \theta_{0,F_0}, \ldots, \theta_{t,F_0})$ *such that*

$$F_0 \in \mathcal{O}_v[X, Y] \tag{4.42}$$

and

$$F_0^* \overset{\mathcal{O}_v}{\prec} F^* \quad \textit{for every} \quad F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\}). \tag{4.43}$$

Proof. We claim that there is a non-negative integer i such that

$$\mathfrak{p}_v^{-\frac{1}{2}r(r-1)i}\mathfrak{c}_v \subseteq [1], \quad \mathfrak{p}_v^{-i}\mathfrak{d}_{kl} \subseteq [1] \quad (1 \leq k < l \leq r)\,, \tag{4.44}$$

$$\mathcal{C}^*(\mathfrak{p}_v^{-\frac{1}{2}r(r-1)i}\mathfrak{c}_v, \{\mathfrak{p}_v^{-i}\mathfrak{d}_{kl}\}) \neq \emptyset\,, \tag{4.45}$$

$$\mathcal{C}^*(\mathfrak{p}_v^{-\frac{1}{2}r(r-1)i}\mathfrak{c}_v, \{\mathfrak{p}_v^{-i}\mathfrak{d}_{kl}\}) \text{ is contained in a single } \mathcal{O}_v\text{-equivalence class.} \tag{4.46}$$

Indeed, if there is no such integer i, then by inductively applying Lemma 4.1 it follows that there are arbitrarily large integers i with (4.44), (4.45). But there cannot be arbitrarily large i with (4.44).

Let i_0 be the smallest integer i with (4.44), (4.45), (4.46). Pick

$$F_0^* = (F_0, \theta_{0,F_0}, \ldots, \theta_{t,F_0}) \in \mathcal{C}^*(\mathfrak{p}_v^{-\frac{1}{2}r(r-1)i_0}\mathfrak{c}_v, \{\mathfrak{p}_v^{-i_0}\mathfrak{d}_{kl}\})\,.$$

Then $F_0[X, Y] \in \mathcal{O}_v[X, Y]$. By Lemma 4.4, for every $F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ there is a sequence

$$F_{i_0}^* \overset{\mathcal{O}_v}{\prec} F_{i_0-1}^* \overset{\mathcal{O}_v}{\prec} \ldots \overset{\mathcal{O}_v}{\prec} F_1^* \overset{\mathcal{O}_v}{\prec} F^*$$

with $F_i^* \in \mathcal{C}^*(\mathfrak{p}_v^{-\frac{1}{2}r(r-1)i}\mathfrak{c}_v, \{\mathfrak{p}_v^{-i}\mathfrak{d}_{kl}\})$ for $i = 1, \ldots, i_0$. By (4.46) we have $F_0^* \overset{\mathcal{O}_v}{\sim} F_{i_0}^*$ and then by (iv) and (iii) of Lemma 3.1, $F_0^* \overset{\mathcal{O}_v}{\prec} F_{i_0}^*$, $F_0^* \overset{\mathcal{O}_v}{\prec} F^*$. This proves Lemma 4.5. □

Lemma 4.6. *Suppose* $r := \sum_{i=0}^{t}[K_i : \Bbbk] \geq 3$. *Let* $\mathfrak{c}_v$ *be an ideal of* $\mathcal{O}_v$. *Let* ρ_v *be the non-negative integer given by* $\mathfrak{c}_v = \mathfrak{p}_v^{\rho_v}$. *Let* $\mathcal{C}^*$ *be a* $\Bbbk$*-equivalence class of augmented* $(K_0, \dots, K_t)$*-forms. Denote by* $\mathcal{C}^*(\mathfrak{c}_v)$ *the collection of augmented* $(K_0, \dots, K_t)$*-forms* $F^* = (F, \theta_{0,F}, \dots, \theta_{t,F})$ *in* $\mathcal{C}^*$ *satisfying*

$$F \in \mathcal{O}_v[X, Y], \tag{4.47}$$

$$[D(F)] = \mathfrak{c}_v^2 \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v}. \tag{4.48}$$

Then $\mathcal{C}^*(\mathfrak{c}_v)$ *is the union of at most*

$$\binom{2\rho_v + \frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)} \left(\sum_{i=0}^{[2\rho_v/r(r-1)]} (Nv)^i \right) \tag{4.49}$$

$\mathcal{O}_v$*-equivalence classes.*

Proof. By Lemma 4.3, we can express the set $\mathcal{C}^*(\mathfrak{c}_v)$ as a union of at most $\binom{2\rho_v+\frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)}$ sets $\mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ where $\mathfrak{d}_{kl}$ $(1 \leq k < l \leq r)$ are ideals of $\mathcal{O}_{L,v}$. So it suffices to show that for given ideals $\mathfrak{c}_v$ of $\mathcal{O}_v$ and $\mathfrak{d}_{kl}$ $(1 \leq k < l \leq r)$ of $\mathcal{O}_{L,v}$, the set $\mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ is the union of not more than

$$\sum_{i=0}^{[2\rho_v/r(r-1)]} (Nv)^i \tag{4.50}$$

$\mathcal{O}_v$-equivalence classes.

According to Lemma 4.5, there is a fixed augmented $(K_0, \dots, K_t)$-form $F_0^* = (F_0, \theta_{0,F}, \dots, \theta_{t,F})$ with $F_0 \in \mathcal{O}_v[X, Y]$ such that $F_0^* \overset{\mathcal{O}_v}{\prec} F^*$ for every $F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$. That is, for every $F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ there is a matrix $A \in \mathrm{M}_2^{\mathrm{ns}}(\mathcal{O}_v)$ such that $F^* = (F_0^*)_A$. By Lemma 4.1, there is an ideal $\mathfrak{c}_{v0}$ of $\mathcal{O}_v$ such that $[D(F_0)] = \mathfrak{c}_{v0}^2 \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v}$. Let $\rho_{v0} \in \mathbb{Z}_{\geq 0}$ be defined by $\mathfrak{c}_{v0} = \mathfrak{p}_v^{\rho_{v0}}$. Then by (4.48), (2.2),

$$\begin{aligned}[D(F)] &= \mathfrak{p}_v^{2\rho_v} \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v} \\ &= [\det A]^{r(r-1)}[D(F_0)] = [\det A]^{r(r-1)} \mathfrak{p}_v^{2\rho_{v0}} \mathfrak{d}_{K_0/\Bbbk,v} \dots \mathfrak{d}_{K_t/\Bbbk,v}.\end{aligned}$$

Hence

$$[\det A] = \mathfrak{p}_v^u \quad \text{with} \quad u = \frac{2(\rho_v - \rho_{v0})}{r(r-1)}. \tag{4.51}$$

Choose Π with $\mathfrak{p}_v = [\Pi]$. The ideals of $\mathcal{O}_v$ are of the shape $\mathfrak{p}_v^m$ ($m \geq 0$) and $\#\mathcal{O}_v/\mathfrak{p}_v^m$ has cardinality $(Nv)^m$. From these facts it can be deduced that every matrix $A \in \mathrm{M}_2^{\mathrm{ns}}(\mathcal{O}_v)$ with (4.51) can be expressed as

$$A = A_{ij}U \quad \text{with} \quad U \in \mathrm{GL}_2(\mathcal{O}_v), \quad A_{ij} = \begin{pmatrix} \Pi^{u-i} & 0 \\ \beta_{ij} & \Pi^i \end{pmatrix}$$

where $i \in \{0, 1, \ldots, u\}$ and where $\beta_{i1}, \ldots, \beta_{i,(Nv)^i}$ is a full system of representatives for the residue classes of $\mathcal{O}_v$ modulo $\mathfrak{p}_v^i$.

Now if $F^* \in \mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ then $F^* = (F_0^*)_A$ for some $A \in \mathrm{M}_2^{\mathrm{ns}}(\mathcal{O}_v)$ with (4.51), hence $F^* = (F_0^*)_{A_{ij}U} \overset{\mathcal{O}_v}{\sim} (F_0^*)_{A_{ij}}$ for some $i \in \{0, \ldots, u\}$, $j \in \{1, \ldots, (Nv)^i\}$. This implies that $\mathcal{C}^*(\mathfrak{c}_v, \{\mathfrak{d}_{kl}\})$ is contained in the union of

$$\sum_{i=0}^{u} (Nv)^i = \sum_{i=0}^{2(\rho_v - \rho_{v0})/r(r-1)} (Nv)^i \leq \sum_{i=0}^{[2\rho_v/r(r-1)]} (Nv)^i$$

$\mathcal{O}_v$-equivalence classes. This proves Lemma 4.6. □

We now arrive at the main result of this section. We have formulated it both for augmented forms and for ordinary binary forms.

Proposition 4.7. *Let $\mathfrak{c}$ be an ideal of $\mathcal{O}_S$. Let $r := \sum_{i=0}^{t} [K_i : \mathbb{k}] \geq 3$.*

(i) *Let $\mathcal{C}^*(\mathfrak{c})$ be a $\mathbb{k}$-equivalence class of augmented $(K_0, \ldots, K_t)$-forms such that any two elements of $\mathcal{C}^*(\mathfrak{c})$ are $\mathbb{k}$-equivalent and such that every $F^* = (F, \theta_{0,F}, \ldots, \theta_{t,F}) \in \mathcal{C}^*(\mathfrak{c})$ satisfies*

$$F \in \mathcal{O}_S[X, Y]\,, \tag{4.52}$$

$$D(F) \cdot \mathcal{O}_S = \mathfrak{c}^2 \mathfrak{d}_{K_0/\mathbb{k},S} \ldots \mathfrak{d}_{K_t/\mathbb{k},S}\,. \tag{4.53}$$

Then $\mathcal{C}^*(\mathfrak{c})$ is contained in the union of at most

$$\tau_{\frac{1}{2}r(r-1)}(\mathfrak{c}^2) \left(\sum_{\mathfrak{d}^{\frac{1}{2}r(r-1)} | \mathfrak{c}} N_S(\mathfrak{d}) \right) \tag{4.54}$$

$\mathcal{O}_S$-equivalence classes.

(ii) *Let $\mathcal{C}(\mathfrak{c})$ be a subset of $\mathcal{F}(\mathcal{O}_S, K_0, \ldots, K_t)$ such that any two binary forms in $\mathcal{C}(\mathfrak{c})$ are $\mathbb{k}$-equivalent and such that every $F \in \mathcal{C}(\mathfrak{c})$ satisfies (4.53).*

Then $\mathcal{C}(\mathfrak{c})$ is contained in the union of finitely many $\mathcal{O}_S$-equivalence classes, the number of which is bounded above by (4.54).

Proof. (i) For $v \notin S$, let $\mathfrak{p}_v$ be the prime ideal of $\mathcal{O}_S$ corresponding to v, i.e., $\mathfrak{p}_v = \{x \in \mathcal{O}_S : |x|_v < 1\}$. Then $\mathfrak{c} = \prod_{v \notin S} \mathfrak{p}_v^{\rho_v}$ with $\rho_v \in \mathbb{Z}_{\geq 0}$. According to Lemma 4.6, for each $v \notin S$ the collection $\mathcal{C}^*(\mathfrak{c})$ is contained in the union of at most

$$\begin{aligned} A_v :=& \binom{2\rho_v + \frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)} \sum_{i=0}^{[2\rho_v/r(r-1)]} (Nv)^i \\ =& \binom{2\rho_v + \frac{1}{2}r(r-1)}{\frac{1}{2}r(r-1)} \sum_{i=0}^{[2\rho_v/r(r-1)]} (N_S\mathfrak{p}_v)^i \end{aligned}$$

$\mathcal{O}_v$-equivalence classes. Lemma 3.2 implies that if $\mathcal{A}_v$ is an $\mathcal{O}_v$-equivalence class of augmented $(K_0, \dots, K_t)$-forms for $v \notin S$, then $\cap_{v \notin S} \mathcal{A}_v$ is an $\mathcal{O}_S$-equivalence class. This implies that $\mathcal{C}^*(\mathfrak{c})$ is contained in the union of at most

$$\prod_{v \notin S} A_v = \tau_{\frac{1}{2}r(r-1)}(\mathfrak{c}^2) \left(\sum_{\mathfrak{d}^{\frac{1}{2}r(r-1)} | \mathfrak{c}} N_S(\mathfrak{d}) \right)$$

$\mathcal{O}_S$-equivalence classes. This proves (i).

(ii) Fix $F_0 \in \mathcal{C}(\mathfrak{c})$. Extend F_0 to an augmented $(K_0, \dots, K_t)$-form $F_0^* = (F_0, \theta_{0,F_0}, \dots, \theta_{t,F_t})$. For every $F \in \mathcal{C}(\mathfrak{c})$, choose $A \in \mathrm{GL}_2(K)$ such that $F = (F_0)_A$ and define $F^* := (F_0^*)_A$. Clearly, the augmented forms constructed in this manner are $\Bbbk$-equivalent to one another. Now by applying (i) to the collection $\mathcal{C}^*(\mathfrak{c}) := \{F^* : F \in \mathcal{C}(\mathfrak{c})\}$, our assertion (ii) follows at once. □

5. Orders

Below, $\Bbbk$ is a number field, and K is a finite extension of $\Bbbk$ of degree $r \geq 3$. We denote by $\xi \mapsto \xi^{(i)}$ $(i = 1, \dots, r)$ the $\Bbbk$-isomorphic embeddings of K into some normal closure L of K over $\Bbbk$. As before, S is a finite subset of $M_\Bbbk$ containing all infinite places. Denote by $\mathcal{O}_{L,S}$ the integral closure of $\mathcal{O}_S$ in L. Given $a_1, \dots, a_m$, we denote by $[a_1, \dots, a_m]$ the fractional $\mathcal{O}_{L,S}$-ideal generated by $a_1, \dots, a_m$. For $f \in L[X_1, \dots, X_m]$ denote by $[f]$ the fractional $\mathcal{O}_{L,S}$-ideal generated by the coefficients of f. Given fractional $\mathcal{O}_{L,S}$-ideals

$\mathfrak{a}$, $\mathfrak{b}$ we write $\frac{\mathfrak{a}}{\mathfrak{b}}$ for $\mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{b}^{-1}$ is the inverse fractional $\mathcal{O}_{L,S}$-ideal of $\mathfrak{b}$. For a finitely generated $\mathcal{O}_S$-module $\mathcal{M} \subset K$ with $\mathcal{M} \neq (0)$ define

$$\mathfrak{d}_{ij}(\mathcal{M}) := [\xi^{(i)} - \xi^{(j)} : \xi \in \mathcal{M}] \quad (1 \leq i, j \leq r,\ i \neq j) \tag{5.1}$$

to be the fractional $\mathcal{O}_{L,S}$-ideal generated by all elements $\xi^{(i)} - \xi^{(j)}$ $(1 \leq i, j \leq r,\ i \neq j)$ with $\xi \in \mathcal{M}$ and

$$\mathfrak{D}(\mathcal{M}) := [D_{K/\Bbbk}(\omega_1, \ldots, \omega_r) : \omega_1, \ldots, \omega_r \in \mathcal{M}] \tag{5.2}$$

to be the fractional $\mathcal{O}_{L,S}$-ideal generated by all discriminants of all r-tuples $\omega_1, \ldots, \omega_r \in \mathcal{M}$.

Let $F^* = (F, \theta_F)$ be an augmented K-form. Suppose that $F \in R[X, Y]$ where R is some subring of $\Bbbk$. Then the invariant order $\mathcal{O}_{F^*,R}$ of F^* is defined to be the R-submodule of K with basis $\omega_1, \ldots, \omega_r$ given by (2.4). By Simon [9], $\mathcal{O}_{F^*,R}$ is indeed an R-order with quotient field K,

$$F^* \overset{R}{\sim} G^* \Rightarrow \mathcal{O}_{F^*,R} = \mathcal{O}_{G^*,R} \tag{5.3}$$

for any two augmented K-forms F^*, G^* (which is slightly stronger than (2.5)), and $D_{K/\Bbbk}(\omega_1, \ldots, \omega_r) = D(F^*)$. If $R = \mathcal{O}_S$ we write $\mathcal{O}_{F^*,S}$ for $\mathcal{O}_{F^*,R}$ and if $R = \mathcal{O}_v$ (local ring) we write $\mathcal{O}_{F^*,v}$ for $\mathcal{O}_{F^*,R}$. Thus if $R = \mathcal{O}_S$ we have

$$\mathfrak{D}(\mathcal{O}_{F^*,S}) = D(F^*) \cdot \mathcal{O}_S\,. \tag{5.4}$$

Lemma 5.1. *Let $F^* = (F, \theta_F)$ be an augmented K-form with $F \in \mathcal{O}_S[X, Y]$. Then*

$$\mathfrak{d}_{ij}(\mathcal{O}_{F^*,S}) = [F]\frac{[\theta_F^{(i)} - \theta_F^{(j)}]}{[1, \theta_F^{(i)}][1, \theta_F^{(j)}]} \quad (1 \leq i, j \leq r,\ i \neq j), \tag{5.5}$$

and

$$\prod_{1 \leq i < j \leq r} \mathfrak{d}_{ij}(\mathcal{O}_{F^*,S})^2 = [F]^{(r-1)(r-2)}\mathfrak{D}(\mathcal{O}_{F^*,S}). \tag{5.6}$$

Proof. We first prove (5.5). Let $i, j \in \{1, \ldots, r\}$, $i \neq j$. Write $F = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$. Then $F = a_0 \prod_{k=1}^r (X - \theta_F^{(k)}Y)$, and so by Gauss' Lemma,

$$[F] = [a_0] \prod_{k=1}^{r} [1, \theta_F^{(k)}]\,. \tag{5.7}$$

Write

$$\prod_{\substack{k=1\\k\neq i,j}}^{r}(X-\theta_F^{(k)}Y)=B_0X^{r-2}+B_1X^{r-3}Y+\cdots+B_{r-2}Y^{r-2}. \tag{5.8}$$

Then $B_0=1$, and by Gauss' Lemma and (5.7),

$$[B_0,B_1,\ldots,B_{r-2}]=\prod_{k=1}^{r}[1,\theta_F^{(k)}]=[F][a_0]^{-1}[1,\theta_F^{(i)}]^{-1}[1,\theta_F^{(j)}]^{-1}. \tag{5.9}$$

Let $\{\omega_1,\ldots,\omega_r\}$ be the basis of $\mathcal{O}_{F^*,S}$ given by (2.4). We first show that

$$\omega_m^{(i)}-\omega_m^{(j)}=a_0B_{m-2}(\theta_F^{(i)}-\theta_F^{(j)}) \quad \text{for} \quad m=2,\ldots,r. \tag{5.10}$$

Write $b_k:=a_k/a_0$ for $k=0,\ldots,r$. Then $\prod_{k=1}^{r}(X-\theta_F^{(k)}Y)=b_0X^r+b_1X^{r-1}Y+\cdots+b_rY^r$. and $a_0^{-1}\omega_m=\sum_{k=0}^{m-2}b_k\theta_F^{m-k-1}$ for $m=2,\ldots,r$. Assertion (5.10) is clear for $m=2$. Let $m\geq 3$. We have (on putting $B_{-2}=B_{-1}=0$)

$$b_k=B_k-B_{k-1}(\theta_F^{(i)}+\theta_F^{(j)})+B_{k-2}\theta_F^{(i)}\theta_F^{(j)} \quad \text{for} \quad k=0,\ldots,r,$$

and so

$$\begin{aligned}
a_0^{-1}(\omega_m^{(i)}-\omega_m^{(j)}) &= \sum_{k=0}^{m-2}b_k\left((\theta_F^{(i)})^{m-k-1}-(\theta_F^{(j)})^{m-k-1}\right)\\
&=\sum_{k=0}^{m-2}\left\{B_k-B_{k-1}(\theta_F^{(i)}+\theta_F^{(j)})+B_{k-2}\theta_F^{(i)}\theta_F^{(j)}\right\}\cdot\left\{(\theta_F^{(i)})^{m-k-1}-(\theta_F^{(j)})^{m-k-1}\right\}\\
&=\sum_{k=0}^{m-2}c_kB_k\,,
\end{aligned}$$

where

$$\begin{aligned}
c_{m-2}&=\theta_F^{(i)}-\theta_F^{(j)}\,,\\
c_{m-3}&={\theta_F^{(i)}}^2-{\theta_F^{(j)}}^2-(\theta_F^{(i)}+\theta_F^{(j)})(\theta_F^{(i)}-\theta_F^{(j)})=0\,,
\end{aligned}$$

and, if $m\geq 4$,

$$\begin{aligned}
c_k={\theta_F^{(i)}}^{m-k-1}-{\theta_F^{(j)}}^{m-k-1}&-(\theta_F^{(i)}+\theta_F^{(j)})({\theta_F^{(i)}}^{m-k-2}-{\theta_F^{(j)}}^{m-k-2})\\
&+\theta_F^{(i)}\theta_F^{(j)}({\theta_F^{(i)}}^{m-k-3}-{\theta_F^{(j)}}^{m-k-3})=0
\end{aligned}$$

for $k = 0, \dots, m-4$. This implies (5.10). By combining (5.10), (5.9) we obtain

$$\begin{aligned}\mathfrak{d}_{ij}(\mathcal{O}_{F^*,S}) &= [\omega_2^{(i)} - \omega_2^{(j)}, \dots, \omega_r^{(i)} - \omega_r^{(j)}] \\ &= [a_0] \cdot [B_0, B_1, \dots, B_{r-2}] \cdot [\theta_F^{(i)} - \theta_F^{(j)}] \\ &= [F] \frac{[\theta_F^{(i)} - \theta_F^{(j)}]}{[1, \theta_F^{(i)}][1, \theta_F^{(j)}]}\end{aligned}$$

which is (5.5).

Now from (5.4), (2.1), (5.7), (5.5) we infer

$$\begin{aligned}\mathfrak{D}(\mathcal{O}_{F^*,S})\mathcal{O}_{L,S} = [D(F)] &= [a_0^{2r-2} \prod_{1 \le i < j \le r} (\theta_F^{(i)} - \theta_F^{(j)})^2] \\ &= [F]^{2r-2} \prod_{1 \le i < j \le r} \left(\frac{[\theta_F^{(i)} - \theta_F^{(j)}]}{[1, \theta_F^{(i)}][1, \theta_F^{(j)}]} \right)^2 \\ &= [F]^{-(r-1)(r-2)} \prod_{1 \le i < j \le r} \mathfrak{d}_{ij}(\mathcal{O}_{F^*,S})^2,\end{aligned}$$

which is (5.6). □

Lemma 5.2. *Let $F^* = (F, \theta_F)$, $G^* = (G, \theta_G)$ be two augmented K-forms such that*

$$F, G \in \mathcal{O}_S[X, Y]; \tag{5.11}$$

$$\mathcal{O}_{F^*,S} = \mathcal{O}_{G^*,S}; \tag{5.12}$$

$$F^*, G^* \text{ are weakly } \Bbbk\text{-equivalent.} \tag{5.13}$$

Then F^*, G^* are weakly $\mathcal{O}_v$-equivalent for every $v \notin S$.

Proof. Take $v \notin S$. By (5.13) there are $A \in \mathrm{GL}_2(\Bbbk)$, $\lambda \in \Bbbk^*$ such that $G^* = \lambda F_A^*$. Since $\mathcal{O}_v$ is a principal ideal domain, there are matrices $U_1, U_2 \in \mathrm{GL}_2(\mathcal{O}_v)$ such that $A = U_1 \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) U_2$ with $a, d \in \Bbbk^*$. Let $\tilde{F}^* := F_{U_1}^*$, $\tilde{G}^* := G_{U_2^{-1}}^*$. Then

$$\tilde{F}^* \overset{\mathcal{O}_v}{\sim} F^*, \quad \tilde{G}^* \overset{\mathcal{O}_v}{\sim} G^*, \tag{5.14}$$

hence it suffices to show that $\tilde{F}^*, \tilde{G}^*$ are weakly $\mathcal{O}_v$-equivalent. Write $\tilde{F}^* = (\tilde{F}, \theta_{\tilde{F}})$, $\tilde{G}^* = (\tilde{G}, \theta_{\tilde{G}})$. Then $\tilde{G}^* = \lambda \tilde{F}^*_{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)}$ which means that

$$\tilde{G}(X,Y) = \lambda \tilde{F}(aX, dY), \quad \theta_{\tilde{G}} = \frac{d}{a}\theta_{\tilde{F}}. \tag{5.15}$$

Write $\tilde{F}(X,Y) = a_0X^r + a_1X^{r-1}Y + \cdots + a_rY^r$. Then $\mathcal{O}_{\tilde{F}^*,v}$ is an $\mathcal{O}_v$-module with basis

$$\omega_1 = 1, \ \omega_i = \sum_{j=0}^{i-2} a_j \theta_{\tilde{F}}^{i-j-1} \quad (i = 2, \dots, r).$$

By (5.15), $\tilde{G}(X,Y) = \lambda a_0 a^r X^r + \lambda a_1 a^{r-1} d X^{r-1}Y + \cdots + \lambda a_r d^r Y^r$ and $\mathcal{O}_{\tilde{G}^*,v}$ is an $\mathcal{O}_v$-module with basis

$$\omega_1' = 1, \ \omega_i' = \sum_{j=0}^{i-2} \lambda a_j a^{r-j} d^j \left(\frac{d}{a}\theta_{\tilde{F}}\right)^{i-j-1} = \lambda a^{r-i+1} d^{i-1} \omega_i \quad (i = 2, \dots, r).$$

By (5.14), (5.12), (5.3) we have $\mathcal{O}_{\tilde{F}^*,v} = \mathcal{O}_{\tilde{G}^*,v}$. Therefore, the matrix relating $\{\omega_1', \dots, \omega_r'\}$ to $\{\omega_1, \dots, \omega_r\}$ is in $\mathrm{GL}_2(\mathcal{O}_v)$. That is,

$$\lambda a^{r-1} d \in \mathcal{O}_v^*, \quad \lambda a^{r-2} d^2 \in \mathcal{O}_v^*, \dots, \lambda a d^{r-1} \in \mathcal{O}_v^*,$$

which implies $d = au$ with $u \in \mathcal{O}_v^*$. Further, $\lambda a^r = u^{-1} \lambda a^{r-1} d \in \mathcal{O}_v^*$. Inserting this into (5.15) we obtain

$$\tilde{G}(X,Y) = \lambda \tilde{F}(aX, auY) = \lambda a^r \tilde{F}(X, uY), \quad \theta_{\tilde{G}} = u\theta_{\tilde{F}},$$

which implies that $\tilde{F}^*, \tilde{G}^*$ are weakly $\mathcal{O}_v$-equivalent. This proves Lemma 5.2. □

We now arrive at our final result:

Proposition 5.3. *Let $\mathcal{C}^*$ be a collection of augmented K-forms such that*

$$F \in \mathcal{O}_S[X,Y] \quad \textit{for every} \quad F^* = (F, \theta_F) \in \mathcal{C}^*; \tag{5.16}$$

$$\mathcal{O}_{F^*,S} = \mathcal{O}_{G^*,S} \quad \textit{for every pair} \quad F^*, G^* \in \mathcal{C}^*; \tag{5.17}$$

the elements of $\mathcal{C}^*$ are weakly $\Bbbk$-equivalent to one onother. (5.18)

Then if r is odd, $\mathcal{C}^*$ is contained in the union of at most r^s $\mathcal{O}_S$-equivalence classes, while if r is even, $\mathcal{C}^*$ is contained in the union of at most $r^s h_2(\mathcal{O}_S)$ $\mathcal{O}_S$-equivalence classes.

Proof. Combine Lemmata 5.2 and 3.3. □

6. Proof of Theorem 2.1

Let $\Bbbk, S$ be as in Section 2; thus $\#S = s$. Let $\mathcal{O}$ be an $\mathcal{O}_S$-order of degree $r \geq 3$ and denote by K its quotient field. Let $F \in \mathcal{O}_S[X,Y]$ be a binary form which is irreducible in $\Bbbk[X,Y]$ and such that $\mathcal{O}_{F,S} \cong \mathcal{O}$ (as $\mathcal{O}_S$-algebras). Then there is a θ_F such that $F(\theta_F, 1) = 0$, $K = \Bbbk(\theta_F)$ and such that $\omega_1, \ldots, \omega_r$ given by (2.4) form an $\mathcal{O}_S$-basis of $\mathcal{O}$. Thus, $F^* := (F, \theta_F)$ is an augmented K-form with $\mathcal{O}_{F^*,S} = \mathcal{O}$. Now it is obvious that in order to prove Theorem 2.1 it suffices to prove the following:

Proposition 6.1. *Let $\#S = s$, and let K be a finite extension of $\Bbbk$ of degree $r \geq 3$. Let $\mathcal{O} \subset K$ be an $\mathcal{O}_S$-order with quotient field K. Then the set of augmented K-forms $F^* = (F, \theta_F)$ with*

$$F \in \mathcal{O}_S[X,Y], \tag{6.1}$$

$$\mathcal{O}_{F^*} = \mathcal{O} \tag{6.2}$$

is contained in the union of finitely many $\mathcal{O}_S$-equivalence classes, whose number is bounded above by

$$2^{24r^3s} \text{ if } r \text{ is odd;} \quad 2^{24r^3s} h_2(\mathcal{O}_S) \text{ if } r \text{ is even.} \tag{6.3}$$

For the moment we assume $r \geq 4$. The case $r = 3$ will be treated separately. Our main tool is a result of Beukers and Schlickewei on equations in two variables with unknowns from a multiplicative group of finite rank. Let Ω be a field of characteristic 0. We endow $(\Omega^*)^2$ with coordinatewise multiplication $(x_1, y_1) * (x_2, y_2) = (x_1x_2, y_1y_2)$; thus $(\Omega^*)^2$ becomes a group with unit element $(1,1)$. For $(x,y) \in (\Omega^*)^2$, $m \in \mathbb{Z}$ we write $(x,y)^m := (x^m, y^m)$.

Lemma 6.2. *Let $(x_1, y_1), \ldots, (x_n, y_n) \in (\Omega^*)^2$. Let*

$$\Gamma := \{(x,y) \in (\Omega^*)^2 : \exists m \in \mathbb{N}, z_1, \ldots, z_n \in \mathbb{Z} \text{ with } (x,y)^m = (x_1,y_1)^{z_1} * \cdots * (x_n,y_n)^{z_n}\}.$$

Then the equation

$$x + y = 1 \quad in \quad (x, y) \in \Gamma \tag{6.4}$$

has at most $2^{8(n+1)}$ *solutions.*

Proof. See [1, Theorem 1]. □

Let $\mathcal{O}$, K be as above. Choose a normal closure L of K over $\Bbbk$ and denote again by $\xi \mapsto \xi^{(i)}$ $(i = 1, \dots, r)$ the $\Bbbk$-isomorphic embeddings of K into L. We recall that the cross ratio of $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{P}^1(L)$ is given by

$$\{\alpha_1, \alpha_2; \alpha_3, \alpha_4\} := \frac{(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)}{(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)} \tag{6.5}$$

(with the usual adaptations if one of $\alpha_1, \dots, \alpha_4$ is ∞ or if $\alpha_1, \dots, \alpha_4$ are not all distinct). As is well-known, cross ratios are invariant under projective transformations.

For an augmented K-form $F^* = (F, \theta_F)$ with (6.1), (6.2) we define the tuple of all cross ratios of $\theta_F^{(1)}, \dots, \theta_F^{(r)}$,

$$\Delta(F^*) := (\{\theta_F^{(i)}, \theta_F^{(j)}; \theta_F^{(k)}, \theta_F^{(l)}\} : \ 1 \le i, j, k, l \le r; \quad i, j, k, l \ \text{ distinct}). \tag{6.6}$$

Lemma 6.3. *If* F^* *runs through the collection of augmented* K*-forms with (6.1), (6.2), then* $\Delta(F^*)$ *runs through a collection of cardinality at most*

$$2^{24(r^3 - r^2)s}. \tag{6.7}$$

Proof. Let $F^* = (F, \theta_F)$ be an augmented K-form with (6.1), (6.2). Let $i, j, k, l \in \{1, \dots, r\}$ be distinct. We have

$$\{\theta_F^{(i)}, \theta_F^{(j)}; \theta_F^{(k)}, \theta_F^{(l)}\} + \{\theta_F^{(i)}, \theta_F^{(l)}; \theta_F^{(k)}, \theta_F^{(j)}\} = 1. \tag{6.8}$$

Write (6.8) as $x + y = 1$. We want to apply Lemma 6.2 to (6.8) and to this end we have to find a suitable group Γ independent of F^* such that $(x, y) \in \Gamma$.

Fix θ_0 with $\Bbbk(\theta_0) = K$. For each two-element subset $\{i, j\}$ of $\{1, \dots, r\}$ define the field

$$K^{\{i,j\}} := \Bbbk(\theta_0^{(i)} + \theta_0^{(j)}, \theta_0^{(i)}\theta_0^{(j)}) \, .$$

Thus, if $P(X, Y) \in \Bbbk[X, Y]$ is a symmetric polynomial, then $P(\xi^{(i)}, \xi^{(j)}) \in K^{\{i,j\}}$ for every $\xi \in K$. Further, $[K^{\{i,j\}} : \Bbbk] \le \binom{r}{2}$. Let $t(\{i, j\})$ denote the

rank of $\mathcal{O}^*_{K^{\{i,j\}},S}$, i.e., the unit group of the integral closure of $\mathcal{O}_S$ in $K^{\{i,j\}}$. Then $t(\{i,j\})$ is equal to the number of places of $K^{\{i,j\}}$ lying above the places in S, minus 1. That is,

$$t(\{i,j\}) \le [K^{\{i,j\}} : \Bbbk]s - 1 \le \binom{r}{2}s - 1. \tag{6.9}$$

There are $\varepsilon_1^{\{i,j\}}, \dots, \varepsilon_{t(\{i,j\})}^{\{i,j\}} \in \mathcal{O}^*_{K^{\{i,j\}},S}$ such that every element of $\mathcal{O}^*_{K^{\{i,j\}},S}$ can be expressed uniquely as

$$\zeta \prod_{m=1}^{t(\{i,j\})} (\varepsilon_m^{\{i,j\}})^{w_m} \tag{6.10}$$

where $\zeta \in K^{\{i,j\}}$ is a root of unity and $w_m \in \mathbb{Z}$ for $m = 1, \dots, t(\{i,j\})$.

Let h be the least common multiple of the following integers: the class number of K; the class number of $K^{\{i,j\}}$ for each two-element subset $\{i,j\}$ of $\{1,\dots,r\}$; and the number of roots of unity in $K^{\{i,j\}}$ for each two-element subset $\{i,j\}$ of $\{1,\dots,r\}$.

We raise the identity (5.5) to the power $2h$ to obtain something useful. Let $i,j \in \{1,\dots,r\}$, $i \ne j$. First we have an identity of fractional $\mathcal{O}_{K,S}$-ideals

$$[1,\theta_F]^{2h} = [\alpha_F] \ \text{ with } \ \alpha_F \in K^* \tag{6.11}$$

since $2h$ is a multiple of the class number of K. Further, $(\theta_F^{(i)} - \theta_F^{(j)})^{2h} \in K^{\{i,j\}}$. The ideal $\mathfrak{d}_{ij}(\mathcal{O}_{F^*,S})^2$ is generated by elements $(\xi^{(i)} - \xi^{(j)})^2$ ($\xi \in \mathcal{O}_{F^*,S}$) which belong to $K^{\{i,j\}}$. By (5.6) the $\mathcal{O}_S$-ideal $[F]$ generated by the coefficients of F depends only on $\mathcal{O}_{F^*,S}$, hence by (6.2) on $\mathcal{O}$. Therefore we have an identity of fractional $\mathcal{O}_{K^{\{i,j\}},S}$-ideals

$$([F]^{-1}\mathfrak{d}_{ij}(\mathcal{O}_{F^*,S}))^{2h} = [\beta_{ij}] \ \text{ with } \ \beta_{ij} \in (K^{\{i,j\}})^*, \tag{6.12}$$

where β_{ij} depends only on $\mathcal{O}$. So in particular, β_{ij} is independent of F^*. Lastly, $\alpha_F^{(i)}\alpha_F^{(j)} \in K^{\{i,j\}}$. Now (5.5), (6.11), (6.12) yield an identity of fractional $\mathcal{O}_{K^{\{i,j\}},S}$-ideals $[\theta_F^{(i)} - \theta_F^{(j)}]^{2h} = [\alpha_F^{(i)}\alpha_F^{(j)}\beta_{ij}]$, that is, $(\theta_F^{(i)} - \theta_F^{(j)})^{2h} = \alpha_F^{(i)}\alpha_F^{(j)}\beta_{ij}\eta_{ij}$ with $\eta_{ij} \in \mathcal{O}^*_{K^{\{i,j\}},S}$. We can express η_{ij} as in (6.10). By raising

again to the power h, we can cancel the root of unity, and obtain

$$(\theta_F^{(i)}-\theta_F^{(j)})^{2h^2}=(\alpha_F^{(i)}\alpha_F^{(j)}\beta_{ij})^h\prod_{m=1}^{t(\{i,j\})}(\varepsilon_m^{\{i,j\}})^{w_m}\quad\text{with}\quad w_m\in\mathbb{Z}. \tag{6.13}$$

Taking any distinct $i,j,k,l\in\{1,\dots,r\}$, and writing again (6.8) as $x+y=1$, it follows that

$$\begin{aligned}(x,y)^{2h^2}&=(\{\theta_F^{(i)},\theta_F^{(j)};\theta_F^{(k)},\theta_F^{(l)}\},\{\theta_F^{(i)},\theta_F^{(l)};\theta_F^{(k)},\theta_F^{(j)}\})^{2h^2}\\&=\left(\frac{(\theta_F^{(i)}-\theta_F^{(j)})(\theta_F^{(k)}-\theta_F^{(l)})}{(\theta_F^{(i)}-\theta_F^{(k)})(\theta_F^{(j)}-\theta_F^{(l)})},\frac{(\theta_F^{(i)}-\theta_F^{(l)})(\theta_F^{(j)}-\theta_F^{(k)})}{(\theta_F^{(i)}-\theta_F^{(k)})(\theta_F^{(j)}-\theta_F^{(l)})}\right)^{2h^2}\\&=\left(\frac{\beta_{ij}\beta_{kl}}{\beta_{ik}\beta_{jl}},\frac{\beta_{il}\beta_{jk}}{\beta_{ik}\beta_{jl}}\right)^h*(\eta_1,\eta_2)\end{aligned}$$

where (η_1,η_2) is a product of powers of

$$\begin{gathered}(\varepsilon_m^{\{i,j\}},1)\ \ (1\le m\le t(\{i,j\}));\quad(\varepsilon_m^{\{k,l\}},1)\ \ (1\le m\le t(\{k,l\}));\\(1,\varepsilon_m^{\{i,l\}})\ \ (1\le m\le t(\{i,l\}));\quad(1,\varepsilon_m^{\{j,k\}})\ \ (1\le m\le t(\{j,k\}));\\(\varepsilon_m^{\{i,k\}},\varepsilon_m^{\{i,k\}})\ \ (1\le m\le t(\{i,k\}));\quad(\varepsilon_m^{\{j,l\}},\varepsilon_m^{\{j,l\}})\ \ (1\le m\le t(\{j,l\})).\end{gathered}$$

It is important to notice that the terms $\alpha_F^{(i)},\alpha_F^{(j)},\alpha_F^{(k)},\alpha_F^{(l)}$ are cancelled. Thus, in view of (6.9), $(x,y)^{2h^2}$ is a product of powers of

$$\begin{aligned}&1+t(\{i,j\})+t(\{k,l\})+t(\{i,l\})+t(\{j,k\})+t(\{i,k\})+t(\{j,l\})\\&\le 1+6\left(\binom{r}{2}s-1\right)=6\binom{r}{2}s-5\end{aligned}$$

terms which are independent of F^*.

Now applying Lemma 6.2 to (6.8) yields that (x,y), and so in particular $x=\{\theta_F^{(i)},\theta_F^{(j)};\theta_F^{(k)},\theta_F^{(l)}\}$, belongs to a set independent of F^* of cardinality at most

$$2^{8\{6\binom{r}{2}s-5+1\}}=2^{48\binom{r}{2}s-32}. \tag{6.14}$$

We claim that the tuple $\Delta(F^*)$ of all cross ratios is determined uniquely by the subtuple

$$\tilde{\Delta}(F^*):=(\{\theta_F^{(1)},\theta_F^{(2)};\theta_F^{(3)},\theta_F^{(l)}\}\ :\ l=4,\dots,r). \tag{6.15}$$

Indeed, let $\langle T\rangle$ be the unique projective transformation of $\mathbb{P}^1$, mapping $\theta_F^{(1)},\theta_F^{(2)},\theta_F^{(3)}$ to $1,\infty,0$, respectively. Since $\langle T\rangle$ does not alter cross ratios,

for $l = 4, \dots, r$ the image of $\theta_F^{(l)}$ under $\langle T \rangle$ is $\{\theta_F^{(1)}, \theta_F^{(2)}; \theta_F^{(3)}, \theta_F^{(l)}\}$. But then it follows that $\{\theta_F^{(i)}, \theta_F^{(j)}; \theta_F^{(k)}, \theta_F^{(l)}\}$ is equal to the cross ratio of the i-th, j-th, k-th, l-th point among $1, \infty, 0, \{\theta_F^{(1)}, \theta_F^{(2)}; \theta_F^{(3)}, \theta_F^{(4)}\}, \dots, \{\theta_F^{(1)}, \theta_F^{(2)}; \theta_F^{(3)}, \theta_F^{(r)}\}$.

So by (6.14) the total number of possibilities for $\tilde{\Delta}(F^*)$, and hence that for $\Delta(F^*)$ is at most

$$2^{\left(48\binom{r}{2}s-32\right)(r-3)} \leq 2^{24(r^3-r^2)s}.$$

This proves Lemma 6.3. □

Lemma 6.4. *Let $F^* = (F, \theta_F)$, $G^* = (G, \theta_G)$ be two augmented K-forms of degree $r \geq 3$ with (6.1), (6.2).*

(i) *If $r = 3$ then F^*, G^* are weakly $\Bbbk$-equivalent.*

(ii) *If $r \geq 4$ and moreover,*

$$\Delta(F^*) = \Delta(G^*), \tag{6.16}$$

then F^*, G^* are weakly $\Bbbk$-equivalent.

Proof. If $r \geq 4$ then by (6.16), $\{\theta_F^{(i)}, \theta_F^{(j)}; \theta_F^{(k)}, \theta_F^{(l)}\} = \{\theta_G^{(i)}, \theta_G^{(j)}; \theta_G^{(k)}, \theta_G^{(l)}\}$ for each distinct $i, j, k, l \in \{1, \dots, r\}$. This implies that there is a unique projective transformation $\langle T \rangle : \mathbb{P}^1(L) \to \mathbb{P}^1(L)$ with $\langle T \rangle(\theta_F^{(i)}) = \theta_G^{(i)}$ for $i = 1, \dots, r$. If $r = 3$ then we simply use that there is a unique projective transformation $\langle T \rangle : \mathbb{P}^1 \to \mathbb{P}^1$ defined over $\overline{\mathbb{Q}}$ with $\langle T \rangle(\theta_F^{(i)}) = \theta_G^{(i)}$ for $i = 1, 2, 3$.

In other words, both for $r = 3$ and $r \geq 4$ there is an up to a scalar factor unique matrix $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(L)$ such that

$$\theta_G^{(i)} = \frac{a\theta_F^{(i)} + b}{c\theta_F^{(i)} + d} \quad \text{for} \quad i = 1, \dots, r. \tag{6.17}$$

We choose the first non-zero element among a, b, c, d equal to 1 so that T is uniquely determined. Then for every $\tau \in \mathrm{Gal}(L/\Bbbk)$, the matrix $\tau(T) = \left(\begin{smallmatrix} \tau(a) & \tau(b) \\ \tau(c) & \tau(d) \end{smallmatrix}\right)$ also satisfies (6.17) since τ permutes both sequences $\theta_F^{(1)}, \dots, \theta_F^{(r)}$ and $\theta_G^{(1)}, \dots, \theta_G^{(r)}$ in the same manner. Hence $\tau(T) = T$ for every $\tau \in \mathrm{Gal}(L/\Bbbk)$ which implies $T \in \mathrm{GL}_2(\Bbbk)$.

Write $F = a_F \prod_{i=1}^{r}(X-\theta_F^{(i)}Y)$, $G = a_G \prod_{i=1}^{r}(X-\theta_G^{(i)}Y)$ with $a_F, a_G \in \Bbbk^*$. Thus,

$$\begin{aligned} G =& a_G \prod_{i=1}^{r}(X - \frac{a\theta_F^{(i)}+b}{c\theta_F^{(i)}+d}Y) \\ =& a_G a_F^{-1} \left\{ \prod_{i=1}^{r}(c\theta_F^{(i)}+d) \right\}^{-1} F(dX-bY, -cX+aY) \\ =& a_G a_F^{-1} \left\{ \prod_{i=1}^{r}(c\theta_F^{(i)}+d) \right\}^{-1} (ad-bc)^r F_{T^{-1}}(X,Y) = \lambda F_{T^{-1}}(X,Y) \end{aligned}$$

with $\lambda \in \Bbbk^*$, $T \in \mathrm{GL}_2(\Bbbk)$, and $\theta_G = \langle T \rangle(\theta_F)$. This implies that F^*, G^* are weakly $\Bbbk$-equivalent. □

Proof of Proposition 6.1. Let $r \geq 3$. Put $h(r, \mathcal{O}_S) := 1$ if r is odd, and $h(r, \mathcal{O}_S) := h_2(\mathcal{O}_S)$ if r is even. By Lemmata 6.3 and 6.4, the collection of augmented K-forms $F^* = (F, \theta_F)$ with (6.1), (6.2) is contained in the union of at most $2^{24(r^3-r^2)s}$ weak $\Bbbk$-equivalence classes. Together with Proposition 5.3 this implies that the collection of augmented K-forms with (6.1), (6.2) is contained in the union of at most

$$2^{24(r^3-r^2)s} \cdot r^s h(r, \mathcal{O}_S) \leq 2^{24r^3 s} h(r, \mathcal{O}_S)$$

$\mathcal{O}_S$-equivalence classes. This proves Proposition 6.1. □

7. Proof of Theorem 2.2

We keep the notation from Section 2. Thus $\Bbbk$ is a number field and S is a finite subset of $M_\Bbbk$ of cardinality s containing all infinite places. Let K be an extension of $\Bbbk$ of degree $r \geq 3$. Let $\mathfrak{c} \neq (0)$ be an ideal of $\mathcal{O}_S$ and let $S' = S \cup \{v \notin S \ : \ |x|_v < 1 \text{ for every } x \in \mathfrak{c}\}$. Notice that if $F \in \mathcal{F}(\mathcal{O}_S, K)$ satisfies (2.9), then

$$D(F) \cdot \mathcal{O}_{S'} = \mathfrak{d}_{K/\Bbbk, S'} .$$

So by (2.6), the $\mathcal{O}_{S'}$-order associated with F is $\mathcal{O}_{F,S'} = \mathcal{O}_{K,S'}$ (the integral closure of $\mathcal{O}_{S'}$ in K). On applying Theorem 2.1 with S' in place of S and with $\mathcal{O} = \mathcal{O}_{K,S'}$ we infer that the set of binary forms $F \in \mathcal{F}(\mathcal{O}_S, K)$ with

(2.9) is contained in finitely many $\mathcal{O}_{S'}$-equivalence classes, whose number is at most

$$\begin{aligned} &2^{24r^3\#S'} = 2^{24r^3(s+\omega_S(\mathfrak{c}))} \quad \text{if } r \text{ is odd,} \\ &2^{24r^3\#S'} h_2(\mathcal{O}_{S'}) \le 2^{24r^3(s+\omega_S(\mathfrak{c}))} h_2(\mathcal{O}_S) \quad \text{if } r \text{ is even,} \end{aligned} \tag{7.1}$$

where we have used $\#S' = s + \omega_S(\mathfrak{c})$ and the obvious inequality $h_2(\mathcal{O}_{S'}) \le h_2(\mathcal{O}_S)$.

In particular, the binary forms $F \in \mathcal{F}(\mathcal{O}_S, K)$ with (2.9) lie in finitely many $\Bbbk$-equivalence classes, whose number is bounded above by (7.1). By multiplying this quantity with the upper bound (4.54) from Proposition (4.7), (ii) we obtain an upper bound for the number of $\mathcal{O}_S$-equivalence classes of binary forms under consideration which is precisely the upper bound from Theorem 2.2. This completes our proof. □

8. Proof of Theorem 2.3

To prove Theorem 2.3, we need a further Proposition on resultant equations which can be regarded as a quantitative version of Lemma 1 of Evertse and Győry [6].

For the moment, let K_0, K_1 be two (not necessarily distinct) extensions of $\Bbbk$ of degrees r_0, r_1, respectively, such that $r_0 \ge 3$. Let L be a normal closure over $\Bbbk$ of the compositum of K_0, K_1. Below, by $[a_1, \dots, a_m]$ we will denote the fractional $\mathcal{O}_{L,S}$-ideal generated by $a_1, \dots, a_m$, and by $[f]$ the fractional $\mathcal{O}_{L,S}$-ideal generated by the coefficients of a given polynomial f.

Using the notation of Theorems 2.2 and 2.3, fix a binary form $F_0 \in \mathcal{F}(\mathcal{O}_S, K_0)$, and consider the binary forms $F_1 \in \mathcal{F}(\mathcal{O}_S, K_1)$.

Proposition 8.1. *Up to multiplication by S-units, there are at most*

$$2^{24r_0r_1s}$$

binary forms $F_1 \in \mathcal{F}(\mathcal{O}_S, K_1)$ which satisfy

$$R(F_0, F_1) \in \mathcal{O}_S^*. \tag{8.1}$$

Proof. Take $F_1 \in \mathcal{F}(\mathcal{O}_S, K_1)$ with (8.1). By assumption, for $i = 0, 1$ we have that $F_i \in \mathcal{O}_S[X, Y]$, F_i is irreducible over $\Bbbk$, and there is a θ_i satisfying

$F(\theta_i, 1) = 0$ and $\Bbbk(\theta_i) = K_i$. We can write

$$F_i(X, Y) = a_i \prod_{k=1}^{r_i} (X - \theta_i^{(k)} Y) \quad (i = 0, 1),$$

where $a_i \in \Bbbk^*$, and where $\theta_i^{(1)}, \dots, \theta_i^{(r_i)}$ are the conjugates of θ_i in L, for $i = 0, 1$. By Gauss' Lemma we have

$$[1] \supseteq [F_i] = [a_i] \prod_{k=1}^{r_i} [1, \theta_i^{(k)}] \quad (i = 0, 1). \tag{8.2}$$

Using (8.1) and expression (4.3) for the resultant, we get

$$\begin{aligned} [1] = [R(F_0, F_1)] &= [a_0]^{r_1} [a_1]^{r_0} \prod_{k=1}^{r_0} \prod_{l=1}^{r_1} [\theta_0^{(k)} - \theta_1^{(l)}] \\ &\subseteq \prod_{k=1}^{r_0} \prod_{l=1}^{r_1} \frac{[\theta_0^{(k)} - \theta_1^{(l)}]}{[1, \theta_0^{(k)}][1, \theta_1^{(l)}]} \,. \end{aligned}$$

In combination with the obvious inclusions $[\theta_0^{(k)} - \theta_1^{(l)}] \subseteq [1, \theta_0^{(k)}][1, \theta_1^{(l)}]$ this gives

$$[\theta_0^{(k)} - \theta_1^{(l)}] = [1, \theta_0^{(k)}][1, \theta_1^{(l)}] \text{ for } k = 1, \dots, r_0,\ l = 1, \dots, r_1. \tag{8.3}$$

Meanwhile, we have shown also that the inclusions in (8.2) are equalities, i.e.,

$$[F_i] = [a_i] \prod_{k=1}^{r_i} [1, \theta_i^{(k)}] = [1] \quad (i = 0, 1). \tag{8.4}$$

We proceed similarly as in the proof of Lemma 6.3. Define the fields $K_{i1} := \Bbbk(\theta_0^{(i)}, \theta_1) = K_0^{(i)} K_1$ $(i = 1, \dots, r_0)$. Denote by h the least common multiple of the class numbers of K_0, K_1, $K_{11}, \dots, K_{r_0,1}$ and of the numbers of roots of unity of $K_{11}, \dots, K_{r_0,1}$. By our choice of h, there are $\alpha_0 \in K_0^*$ such that $[1, \theta_0]^h = [\alpha_0]$, and $\alpha_1 \in K_1^*$ such that $[1, \theta_1]^h = [\alpha_1]$. Then by (8.3),

$$[\theta_0^{(i)} - \theta_1]^h = [\alpha_0^{(i)}][\alpha_1] \text{ for } i = 1, \dots, r_0,$$

that is

$$(\theta_0^{(i)} - \theta_1)^h = \alpha_0^{(i)} \alpha_1 \eta_i,$$

where $\eta_i \in \mathcal{O}_{K_{i1},S}^*$ (i.e., the unit group of the integral closure of $\mathcal{O}_S$ in K_{i1}). Let $\varepsilon_{i1}, \dots, \varepsilon_{is_i}$ be a system of fundamental units of $\mathcal{O}_{K_{i1},S}^*$. Then η_i is a

product of a root of unity in K_{i1} and of powers of $\varepsilon_{i1}, \dots, \varepsilon_{is_i}$ and so, by our choice of h,

$$(\theta_0^{(i)} - \theta_1)^{h^2} = (\alpha_0^{(i)})^h \alpha_1^h \varepsilon_{i1}^{w_{i1}} \dots \varepsilon_{is_i}^{w_{is_i}}$$

with $w_{i1}, \dots, w_{is_i} \in \mathbb{Z}$.

Pick distinct subscripts $i, j, k \in \{1, \dots, r_0\}$ and consider the identity

$$\frac{(\theta_0^{(i)} - \theta_0^{(j)})}{(\theta_0^{(i)} - \theta_0^{(k)})} \cdot \frac{(\theta_0^{(k)} - \theta_1)}{(\theta_0^{(j)} - \theta_1)} + \frac{(\theta_0^{(j)} - \theta_0^{(k)})}{(\theta_0^{(i)} - \theta_0^{(k)})} \cdot \frac{(\theta_0^{(i)} - \theta_1)}{(\theta_0^{(j)} - \theta_1)} = 1.$$

This can be written as $x + y = 1$, where

$$(x, y)^{h^2} = (a, b) * \prod_{q=1}^{s_k} (\varepsilon_{kq}, 1)^{w_{kq}} * \prod_{q=1}^{s_i} (1, \varepsilon_{iq})^{w_{iq}} * \prod_{q=1}^{s_j} (\varepsilon_{jq}, \varepsilon_{jq})^{-w_{jq}}$$

with

$$(a, b) = \left(\Big(\frac{(\theta_0^{(i)} - \theta_0^{(j)})}{(\theta_0^{(i)} - \theta_0^{(k)})} \Big)^{h^2} \Big(\frac{\alpha_0^{(k)}}{\alpha_0^{(j)}} \Big)^h, \Big(\frac{(\theta_0^{(j)} - \theta_0^{(k)})}{(\theta_0^{(i)} - \theta_0^{(k)})} \Big)^{h^2} \Big(\frac{\alpha_0^{(i)}}{\alpha_0^{(j)}} \Big)^h \right).$$

Notice that

$$s_i \le ([K_{i1} : \mathbb{k}]s) - 1 \le r_0 r_1 s - 1$$

and similarly for s_j and s_k. So, by Lemma 6.2 the number of possibilities for (x, y) is at most

$$2^{8(s_i + s_j + s_k + 1) + 8} \le 2^{24 r_0 r_1 s}.$$

This gives at most $2^{24 r_0 r_1 s}$ possibilities for θ_1. But, by (8.4), the ideal $[a_1]$ is uniquely determined once θ_1 is uniquely determined and moreover, $a_1 \in \mathbb{k}^*$. So a_1 is uniquely determined up to a factor from $\mathcal{O}_S^*$. We infer that up to multiplication by some factor from $\mathcal{O}_S^*$, for F_1 there are at most $2^{24 r_0 r_1 s}$ possibilities. □

Proof of Theorem 2.3. Let $K_0, K_1, \dots, K_t$ be (not necessarily distinct) extensions of $\mathbb{k}$ of degrees $r_0, r_1, \dots, r_t$, respectively, such that $r_0 \ge 3$. Let $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ be a binary form with the property (2.11). There are binary forms $F_0, \dots, F_t$ with $F = F_0 \cdots F_t$ and with $F_i \in \mathcal{F}(\mathcal{O}_S, K_i)$ for $i = 0, \dots, t$. So in particular, $F_i \in \mathcal{O}_S[X, Y]$ for $i = 0, \dots, t$. Let S' denote

the union of S and the places $v \notin S$ such that $|x|_v < 1$ for every $x \in \mathfrak{c}$. Then

$$D(F) \cdot \mathcal{O}_{S'} = \mathfrak{d}_{K_0/\Bbbk,S'} \cdots \mathfrak{d}_{K_t/\Bbbk,S'} .$$

Now by expressing $D(F)$ as in (4.4), and using $R(F_i, F_j) \in \mathcal{O}_{S'}$ $(0 \le i < j \le t)$ and the inclusions

$$D(F_i) \cdot \mathcal{O}_{S'} \subseteq \mathfrak{d}_{K_i/\Bbbk,S'} \quad (i = 0, \dots, t)$$

(which follow from (ii) of Lemma 4.1), we obtain

$$D(F_0) \cdot \mathcal{O}_{S'} = \mathfrak{d}_{K_0/\Bbbk,S'} , \tag{8.5}$$

$$R(F_0, F_i) \in \mathcal{O}_{S'}^* \quad (i = 0, \dots, t) . \tag{8.6}$$

We apply now Theorem 2.2 to (8.5) with S replaced by S'; we obtain that F_0 is contained in the union of at most

$$2^{24r_0^3(\#S')} h(r_0, \mathcal{O}_{S'}) \le 2^{24r_0^3(s+\omega_S(\mathfrak{c}))} h(r_0, \mathcal{O}_S) \tag{8.7}$$

$\mathcal{O}_{S'}$-equivalence classes. Here we have used that $\#S' = s + \omega_S(\mathfrak{c}))$ and $h(r_0, \mathcal{O}_{S'}) \le h(r_0, \mathcal{O}_S)$.

Fix one of these $\mathcal{O}_{S'}$-equivalence classes, and pick from this class a representative $F_0 \in \mathcal{F}(\mathcal{O}_S, K_0)$ with (8.5). Consider all tuples $(F_1, \dots, F_t)$ of binary forms with $F_i \in \mathcal{F}(\mathcal{O}_S, K_i)$ for $i = 1, \dots, t$ and with (8.6). Proposition 8.1 gives that for given F_0 there are, up to S'-unit factors, at most

$$2^{24r_0(r_1+\cdots+r_t)(s+\omega_S(\mathfrak{c}))}$$

such tuples $(F_1, \dots, F_t)$.

Combining this with the upper bound (8.7) for the number of $\mathcal{O}_{S'}$-equivalence classes of binary forms $F_0 \in \mathcal{F}(\mathcal{O}_S, K_0)$ with (8.5), we infer that up to $\mathcal{O}_{S'}$-equivalence, and up to an $\mathcal{O}_{S'}$-unit factor, there are at most

$$\begin{aligned} &2^{24r_0^3(s+\omega_S(\mathfrak{c}))} h(r_0, S) \cdot 2^{24r_0(r_1+\cdots+r_t)(s+\omega_S(\mathfrak{c}))} \\ &\qquad = 2^{24r_0(r_0^2+r_1+\cdots+r_t)(s+\omega_S(\mathfrak{c}))} h(r_0, \mathcal{O}_S) \end{aligned} \tag{8.8}$$

binary forms $F = F_0 \cdots F_t \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11). That is, there are binary forms $G_1, \dots, G_m \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$, with m bounded above by the quantity in (8.8), such that every binary form $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) is $\mathcal{O}_{S'}$-equivalent to εG_i for some $i \in \{1, \dots, m\}$ and $\varepsilon \in \mathcal{O}_{S'}^*$. But ε can be written in the form $\varepsilon_1^{w_1} \cdots \varepsilon_{s'}^{w_{s'}} \eta^r$, where $s' = \#S' = s + \omega_S(\mathfrak{c})$,

$\varepsilon_1, \dots, \varepsilon_{s'}$ are generators of $\mathcal{O}_{S'}^*$, $w_1, \dots, w_{s'} \in \{0, \dots, r-1\}$ and $\eta \in \mathcal{O}_{S'}^*$. Since G_i is $\mathcal{O}_{S'}$-equivalent to $\eta^r G_i = (G_i)\left(\begin{smallmatrix} \eta & 0 \\ 0 & \eta \end{smallmatrix}\right)$, we have in fact that every binary form F under consideration is $\mathcal{O}_{S'}$-equivalent to $\varepsilon_1^{w_1} \cdots \varepsilon_{s'}^{w_{s'}} G_i$, with $w_1, \dots, w_{s'} \in \{0, \dots, r-1\}$ and with $i \in \{1, \dots, m\}$. Assuming as we may in view of Theorem 2.2 that $r_1 + \cdots + r_t \geq 1$, it follows that the binary forms $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) lie in at most

$$\begin{aligned} &\left(r \cdot 2^{24r_0(r_0^2+r_1+\cdots+r_t)}\right)^{(s+\omega_S(\mathfrak{c}))} h(r_0, \mathcal{O}_S) \\ &\qquad \leq \left(r \cdot 2^{24(r-1)((r-1)^2+1)}\right)^{(s+\omega_S(\mathfrak{c}))} h(r_0, \mathcal{O}_S) \end{aligned}$$

and so in at most

$$2^{24r^3(s+\omega_S(\mathfrak{c}))} h(r_0, \mathcal{O}_S) \tag{8.9}$$

$\mathcal{O}_{S'}$-equivalence classes.

By (ii) of Proposition 4.7, the binary forms $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) lie in finitely many $\mathcal{O}_S$-equivalence classes whose product is bounded above by the product of (8.9) and of (4.54). Since this is precisely the bound of Theorem 2.3, this completes our proof. □

9. Lower bounds

We present some examples, showing that the results mentioned in Section 2 are in certain respects close to best possible.

First let K be a finite extension of $\mathbb{k}$ of even degree $r \geq 4$. Let S be a finite subset of $M_{\mathbb{k}}$ such that S contains all infinite places. We show that there are infinitely many $\mathcal{O}_S$-orders $\mathcal{O}$ with quotient field K, such that the collection of augmented K-forms $F^* = (F, \theta_F)$ with $F \in \mathcal{O}_S[X, Y]$ and $\mathcal{O}_{F^*,S} = \mathcal{O}$ cannot be contained in fewer than $h_2(\mathcal{O}_S)$ $\mathcal{O}_S$-equivalence classes. Since each binary form $F \in \mathcal{F}(\mathcal{O}_S, K)$ gives rise to at most r augmented K-forms $F^* = (F, \theta_F)$, it follows that the set of forms $F \in \mathcal{F}(\mathcal{O}_S, K)$ with $\mathcal{O}_{F,S} \cong \mathcal{O}$ cannot be contained in fewer than $r^{-1}h_2(\mathcal{O}_S)$ $\mathcal{O}_S$-equivalence classes. This shows that the factor $h_2(\mathcal{O}_S)$ in the upper bound of Theorem 2.1 is necessary.

Pick any augmented K-form $F^* = (F, \theta_F)$ with $F \in \mathcal{O}_S[X, Y]$. Let $\mathfrak{a}$ be any ideal of $\mathcal{O}_S$ such that $\mathfrak{a}^2$ is principal. The ideal $\mathfrak{a}$ can be generated by two elements, $\mathfrak{a} = [\alpha, \beta]$, say. Let $\mathfrak{a}^2 = [\lambda]$. Then there are $\xi, \eta \in \mathcal{O}_S$ such that $\xi\alpha^2 - \eta\beta^2 = \lambda$. Define

$$F^*_{\mathfrak{a}} := \lambda^{-r/2} F^*_{\left(\begin{smallmatrix} \alpha & \beta \\ \eta\beta & \xi\alpha \end{smallmatrix}\right)}.$$

We first show that $F^*_{\mathfrak{a}} = (F_{\mathfrak{a}}, \theta_{F_{\mathfrak{a}}})$ with $F_{\mathfrak{a}} \in \mathcal{O}_S[X, Y]$, and $\mathcal{O}_{F^*_{\mathfrak{a}},S} = \mathcal{O}_{F^*,S}$. Pick $v \notin S$. Then there is $\mu \in \mathcal{O}_v$ such that in $\mathcal{O}_v$ we have the identity of ideals $[\alpha, \beta] = [\mu]$. We now get

$$F_{\mathfrak{a}} = \lambda^{-r/2} F(\alpha X + \beta Y, \eta\beta X + \xi\alpha Y) = \lambda^{-r/2}\mu^r F(\frac{\alpha}{\mu}X + \frac{\beta}{\mu}Y, \frac{\eta\beta}{\mu}X + \frac{\xi\alpha}{\mu}Y).$$

Since $[\mu^2] = [\lambda]$ in $\mathcal{O}_v$ we have $\lambda^{-r/2}\mu^r \in \mathcal{O}_v^*$. Further,

$$\det \begin{pmatrix} \frac{\alpha}{\mu} & \frac{\beta}{\mu} \\ \frac{\eta\beta}{\mu} & \frac{\xi\alpha}{\mu} \end{pmatrix} = \frac{\xi\alpha^2 - \eta\beta^2}{\mu^2} = \frac{\lambda}{\mu^2} \in \mathcal{O}_v^*.$$

Hence $F^*_{\mathfrak{a}}$, F^* are weakly $\mathcal{O}_v$-equivalent. This implies $F_{\mathfrak{a}} \in \mathcal{O}_v[X, Y]$. Further by (5.3), $\mathcal{O}_{F^*_{\mathfrak{a}},v} = \mathcal{O}_{F^*,v}$ where $\mathcal{O}_{F^*_{\mathfrak{a}},v}, \mathcal{O}_{F^*,v}$ are the localizations at v of $\mathcal{O}_{F^*_{\mathfrak{a}},S}, \mathcal{O}_{F^*,S}$. This holds for every $v \notin S$. Hence $F_{\mathfrak{a}} \in \mathcal{O}_S[X, Y]$ and $\mathcal{O}_{F^*_{\mathfrak{a}},S} = \mathcal{O}_{F^*,S}$.

We now show that if $\mathfrak{a}_1$, $\mathfrak{a}_2$ are two ideals of $\mathcal{O}_S$ such that $\mathfrak{a}_1^2$, $\mathfrak{a}_2^2$ are principal and $\mathfrak{a}_1$, $\mathfrak{a}_2$ do not belong to the same ideal class, then the augmented K-forms $F^*_{\mathfrak{a}_1}, F^*_{\mathfrak{a}_2}$ constructed above are not $\mathcal{O}_S$-equivalent. Thus, the collection of augmented K-forms $F^*_{\mathfrak{a}}$ such that $\mathfrak{a}$ is an ideal of $\mathcal{O}_S$ for which $\mathfrak{a}^2$ is principal cannot be contained in fewer than $h_2(\mathcal{O}_S)$ $\mathcal{O}_S$-equivalence classes.

For $i = 1, 2$ let $\mathfrak{a}_i = [\alpha_i, \beta_i]$ be an ideal of $\mathcal{O}_S$, suppose that $\mathfrak{a}_i^2 = [\lambda_i]$ is principal, and choose $\xi_i, \eta_i \in \mathcal{O}_S$ such that $\xi_i\alpha_i^2 - \eta_i\beta_i^2 = \lambda_i$ for $i = 1, 2$. Define $F^*_{\mathfrak{a}_i} := \lambda_i^{-r/2} F^*_{\left(\begin{smallmatrix} \alpha_i & \beta_i \\ \eta_i\beta_i & \xi_i\alpha_i \end{smallmatrix}\right)}$ $(i = 1, 2)$. Suppose that $F^*_{\mathfrak{a}_2} = (F^*_{\mathfrak{a}_1})_U$ for some $U \in \mathrm{GL}_2(\mathcal{O}_S)$. Then by (ii) of Lemma 3.1, there is $\rho \in \Bbbk^*$ such that $\left(\begin{smallmatrix} \alpha_2 & \beta_2 \\ \eta_2\beta_2 & \xi_2\alpha_2 \end{smallmatrix}\right) = \rho \left(\begin{smallmatrix} \alpha_1 & \beta_1 \\ \eta_1\beta_1 & \xi_1\alpha_1 \end{smallmatrix}\right) U$, and $\rho^r = (\lambda_1\lambda_2^{-1})^{r/2}$. Hence $[\rho]^r = (\mathfrak{a}_1\mathfrak{a}_2^{-1})^r$ which implies $\mathfrak{a}_1 = \rho\mathfrak{a}_2$. So $\mathfrak{a}_1, \mathfrak{a}_2$ lie in the same ideal class. This proves our assertion.

Now let $(K_0, \dots, K_t)$ be a sequence of finite extensions of $\Bbbk$ such that $\sum_{i=0}^{t}[K_i : \Bbbk] =: r \geq 3$. We show that there are infinitely many ideals $\mathfrak{c}$ of $\mathcal{O}_S$ such that the collection of binary forms $\mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) cannot be contained in fewer than $C \times N_S(\mathfrak{c})^{2/r(r-1)}$ $\mathcal{O}_S$-equivalence classes, where C is some positive constant.

Fix $\tilde{F} \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with $D(\tilde{F}) \neq 0$. Extend this to an augmented $(K_0, \dots, K_t)$-form $\tilde{F}^* = (\tilde{F}, \theta_{0,\tilde{F}}, \dots, \theta_{t,\tilde{F}})$. Let $a \in \mathcal{O}_S$, $a \neq 0$. For $\beta \in \mathcal{O}_S$ define

$$\tilde{F}^*_\beta := \tilde{F}^*_{\left(\begin{smallmatrix}1 & \beta\\ 0 & a\end{smallmatrix}\right)} = (\tilde{F}_\beta, \theta_{0,\tilde{F}_\beta}, \dots, \theta_{t,\tilde{F}_\beta}) \ \text{ with } \ \tilde{F}_\beta = \tilde{F}(X + \beta Y, aY).$$

Now if $\beta_1, \beta_2 \in \mathcal{O}_S$ are such that $\tilde{F}^*_{\beta_1}, \tilde{F}^*_{\beta_2}$ are $\mathcal{O}_S$-equivalent, then $\tilde{F}^*_{\left(\begin{smallmatrix}1 & \beta_1\\ 0 & a\end{smallmatrix}\right)} = \tilde{F}^*_{\left(\begin{smallmatrix}1 & \beta_2\\ 0 & a\end{smallmatrix}\right)U}$ for some matrix $U \in \mathrm{GL}_2(\mathcal{O}_S)$. According to Lemma 3.1, (ii), this implies $\left(\begin{smallmatrix}1 & \beta_1\\ 0 & a\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix}1 & \beta_2\\ 0 & a\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O}_S)$ and therefore, $(\beta_1 - \beta_2)/a \in \mathcal{O}_S$.

Consequently, the augmented $(K_0, \dots, K_t)$-forms $\tilde{F}^*_\beta$ ($\beta \in \mathcal{O}_S$) cannot be contained in the union of fewer than $\#\mathcal{O}_S/[a] = N_S(a)$ $\mathcal{O}_S$-equivalence classes.

Notice that $\tilde{F}_\beta \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ for $\beta \in \mathcal{O}_S$. By (ii) of Lemma 4.1, there is an ideal $\mathfrak{c}_0$ of $\mathcal{O}_S$ such that $[D(\tilde{F})] = \mathfrak{c}_0^2\mathfrak{d}_{K_0/\Bbbk,S} \dots \mathfrak{d}_{K_t/\Bbbk,S}$. Put $\mathfrak{c} := a^{\frac{1}{2}r(r-1)}\mathfrak{c}_0$. Then by (2.2), $\tilde{F}_\beta$ satisfies (2.11) with this $\mathfrak{c}$.

Since there at most r^{t+1} different augmented forms $\tilde{F}^*_\beta$ coming from the same binary form $\tilde{F}_\beta$, it follows that for each ideal $\mathfrak{c}$ as constructed above, the set of binary forms $F \in \mathcal{F}(\mathcal{O}_S, K_0, \dots, K_t)$ with (2.11) cannot be contained in the union of fewer than

$$r^{-t-1}N_S(a) = r^{-t-1}N_S(\mathfrak{c}_0)^{\frac{-2}{r(r-1)}}N_S(\mathfrak{c})^{\frac{2}{r(r-1)}} =: C \times N_S(\mathfrak{c})^{\frac{2}{r(r-1)}}$$

$\mathcal{O}_S$-equivalence classes.

References

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

[2] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, *Proc. London Math. Soc. (3)*, **24** (1972), 385–394.

[3] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, R.I., 1964.

[4] J.-H. Evertse and K. Győry, On unit equations and decomposable form equations, *J. reine angew. Math.*, **358** (1985), 6–19.

[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 and K. Győry, Lower bounds for resultants I, *Compositio Math.*, **88** (1993), 1–23.

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

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

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

A. Bérczes
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: berczesa@math.klte.hu

J.-H. Evertse
Mathematical Institute, Universiteit Leiden
P.O. Box 9512, NL-2300 RA Leiden, The Netherlands
E-mail address: evertse@math.leidenuniv.nl

K. Győry
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: gyory@math.klte.hu