# Explicit Chevalley-Weil Theorem for Affine Plane Curves

Konstantinos Draziotis* and Dimitrios Poulakis (Thessaloniki)

**Abstract**

Let $\phi : \tilde{C} \to C$ be an unramified morphism of plane affine curves defined over a number field $K$. In this paper we obtain a quantitative version of the classical Chevalley-Weil theorem for curves giving an effective upper bound for the norm of the relative discriminant of the field $K(Q)$ over $K$ for any integral point $P \in C(K)$ and $Q \in \phi^{-1}(P)$.

## 1 Introduction and Statement of Results

In this paper we revisit the classical theorem of Chevalley-Weil for unramified maps [2], [18], [7, Theorem 8.1, page 45], [4, page 292], [14, pages 50 and 109]. This theorem has quite interesting applications to the study of integral points of algebraic curves [1], [14, Section 8.4], [6, Chapter VI] and [5, §1]. Partial quantitative versions on it have been used for the effective analysis of integral points on some families of algebraic curves [10, 12]. Note also that an interesting alternative application of the unramified maps in the study of Diophantine equations is given in [3].

Let $K$ be an algebraic number field and $O_K$ be the ring of integers. In this paper we deal with the following version derived from [14, page 109]: If $\phi : \bar{C} \to C$ is an unramified morphism of affine plane curves defined over $K$, then there exists a finite extension $L/K$ such that $\phi^{-1}(C(O_K)) \subseteq \bar{C}(L)$. More precisely, if $Q \in \phi^{-1}(P)$, where $P \in C(O_K)$, and $K(Q)$ is the field generated over $K$ by the coordinates of $Q$, then we calculate, following a new approach, an effective upper bound for the norm of the relative discriminant of $K(Q)$ over $K$, depending only on $C$, $\bar{C}$, and $\phi$.

We consider the set of standard absolute values on $\mathbb{Q}$ containing the ordinary absolute value $|\cdot|$ and for every prime $p$ the $p$-adic absolute value $|\cdot|_p$ with $|p|_p = p^{-1}$. By an absolute value of $K$ we will always understand an absolute value that is an extension to $K$ of one of the above absolute values of $\mathbb{Q}$. We denote by $M(K)$ a set of symbols $v$ such that with every $v \in M(K)$ there is precisely one associated absolute value $|\cdot|_v$ on $K$. For $v \in M_K$, we denote by $K_v$ and $\mathbb{Q}_v$ the completion of the indicated field with respect to the absolute value $|\cdot|_v$. The local degree at $v$ is given by $d_v = [K_v : \mathbb{Q}_v]$. Let $\mathbf{x} = (x_0 : \ldots : x_n)$ be a point of the projective space $\mathbb{P}^n(K)$ over $K$. We define the field height

*The research of the first author was financial supported by Hellenic State Scholarships Foundation-I.K.Y

$H_K(\mathbf{x})$ of $\mathbf{x}$ by

$$H_K(\mathbf{x}) = \prod_{v \in M(K)} \max\{|x_0|_v, \ldots, |x_n|_v\}^{d_v}.$$

Let $d$ be the degree of $K$. Then we define the absolute height $H(\mathbf{x})$ by $H(\mathbf{x}) = H_K(\mathbf{x})^{1/d}$. Furthermore, for $x \in K$ we put $H_K(x) = H_K((1:x))$ and $H(x) = H((1:x))$. If $G \in K[X_1, \ldots, X_m]$, then we define the field height $H_K(G)$ and the absolute height $H(G)$ of $G$ as the field height and the absolute height of the point whose coordinates are the coefficients of $G$ (in any order). Given $v \in M(K)$, we denote by $|G|_v$ the maximum of $|c|_v$ over all the coefficients $c$ of $G$. For an account of the properties of heights see [17, chapter VIII] or [7, chapter 3].

Let $\overline{K}$ be an algebraic closure of $K$. Recall that a morphism $\phi : \bar{C} \to C$ of algebraic curves is said to be unramified, if it is finite, $C$ is nonsingular and for every $P \in C(\overline{K})$ the number of elements of $\phi^{-1}(P)$ is equal to the degree of $\phi$ [15, page 117]. If $M$ is a finite extension of $K$, then we denote by $N_M$ and $D_{M/K}$ the norm and the relative discriminant of $M$ over $K$, respectively. For any subfield $L$ of $\overline{K}$, we denote by $L[C]$ and $L(C)$ the ring of regular functions and the function field of an affine curve $C$ over $L$, respectively.

Let $F(X,Y)$ and $\bar{F}(X,Y)$ be absolutely irreducible polynomials of $K[X,Y]$ with degrees $\deg F = N \geq 2$ and $\deg \bar{F} = \bar{N} \geq 2$, respectively. We denote by $C$ and $\bar{C}$ the affine curves defined by the equations $F(X,Y) = 0$ and $\bar{F}(X,Y) = 0$, respectively. Let $\phi : \bar{C} \to C$ be a morphism of affine curves defined over $K$ of degree $m > 1$ and $\phi_1(X,Y)$, $\phi_2(X,Y)$ be polynomials of $K[X,Y]$ such that $\phi(P) = (\phi_1(P), \phi_2(P))$ for every $P \in \bar{C}(\overline{K})$. We set $M = \max\{\deg \phi_1, \deg \phi_2\}$ and we denote by $\Phi$ a point of the projective space having as coordinates 1 and the coefficients of $\phi_i(X,Y)$ $(i = 1,2)$.

**Theorem 1.1** *Assume that $C$ is nonsingular and the morphism $\phi : \bar{C} \to C$ unramified. Then, for any $P \in C(O_K)$ and $Q \in \phi^{-1}(P)$, we have*

$$N_K(D_{K(Q)/K}) < \Omega \ (H(F)^{5\bar{N}N^3} H(\Phi)^{\bar{N}} H(\bar{F})^M)^{\omega d m^6 \bar{N}^6 N^{22}},$$

*where $\Omega$ is an effectively computable constant in terms of $N, \bar{N}, M, m, d$ and $\omega$ is an effectively computable numerical constant.*

*Remarks.* 1) By [15, Corollary 3, page 120], the curve $\bar{C}$ is nonsingular.
2) Since $m > 1$, the quantity $M$ is $> 1$.
3) Since $\bar{F}(X,Y)$ divides $F(\phi_1(X,Y), \phi_2(X,Y))$, the quantities $H(\bar{F})$ and $\bar{N}$ are bounded by constants depending only on $F$ and $\phi$. Thus, our bound can be made independent of $\bar{F}$.
4) Theorem 1.1 can be easily generalised for $S$-integral points. For simplicity we have chosen to present it only for integral points.

The proof of Theorem 1.1 relies on the construction of two primitive elements $u_1$ and $u_2$ for the field extension $K(\bar{C})/K(C)$ and polynomials $P_i(X,Y,U)$ $(i = 1,2)$ of $K[X,Y,U]$ which represent the irreducible polynomials of $u_i$ over $K(C)$ having the following property: The algebraic set defined by $F(X,Y)$ and the discriminants $D_i(X,Y)$ of $P_i(X,Y,U)$ $(i = 1,2)$ (considered as polynomial with coefficients in $K[X,Y]$) is empty. Then we obtain a Bézout identity involving $D_i(X,Y)$ $(i = 1,2)$ and $F(X,Y)$ and we deduce that when $\wp$ is a prime ideal of $O_K$ with large norm and $(a,b) \in C(O_K)$ the ideal $\wp$ cannot divide both the discriminants $D_i(a,b)$ $(i=1,2)$ and thus cannot divide the discriminat of every number field $K(Q)$, where $Q \in \phi^{-1}(a,b)$. Thus, we determine the prime ideals of $K$ which are ramified in $K(Q)$ and so we calculate a bound for the norm of the relative discriminant of $K(Q)$ over $K$. Note that the primes that potentially ramify in the various $K(Q)$ are the primes of bad reduction. In specific instances, one can have better results, the goal was to show that some bound existed and to give its shape.

The present paper is organized as follows. In Sections 2, 3, and 4 we obtain some results which are needed for the proof of Theorem 1.1. More precisely, in section 3, we determine the irreducible polynomial of an integral element over the coordinate ring of an affine irreducible plane curve, in section 3 we obtain some results on polynomials without common zero, and in section 4 we give some auxiliary lemmata. Finally, the proof of Theorem 1.1 is obtained in section 5. Thoughout this paper, we denote by $\Lambda_1(a_1,\ldots,a_s)$, $\Lambda_2(a_1,\ldots,a_s),\ldots$ effectively computable positive numbers in terms of indicated parameters.

## 2 Determination of an Irreducible Polynomial

Let $F(X,Y)$ be an absolutely irreducible polynomial in $K[X,Y]$ of degree $N \geq 2$ and $C$ be the affine curve defined by the equation $F(X,Y)=0$. Let $m>1$ and $n>1$ be the degrees of $F$ in $X$ and $Y$ respectively. Further, we denote by $x$ and $y$ the coordinate functions on $C$. In this section we prove the following proposition which will be play an important role in the proof of Theorem 1.1:

**Proposition 2.1** *Suppose that $C$ is smooth. Let $u$ be an integral element over $K[C]$ of degree $\mu > 1$ and $G(X,U)$ be a polynomial of $K[X,U]$ such that $G(x,u)=0$. Put $\gamma = \deg_X G$, $\nu = \deg_U G$. Then there is a polynomial*

$$P(X,Y,U) = U^{\mu} + p_1(X,Y)U^{\mu-1} + \cdots + p_{\mu}(X,Y),$$

*with coefficients in $K$ such that $P(x,y,U)$ is the irreducible polynomial of $u$ over $K(C)$. Furthermore, we have $\deg p_i < 5\gamma N^3$ and*

$$H(P) < \Lambda_1(N,\gamma,\nu,\mu)(H(G)H(F)^{5\gamma N^3})^{25\mu\gamma^2 N^8}.$$

Before to proceed to the proof of Proposition 2.1, we shall recall the notion of height of a polynomial over the function field $\overline{K}(C)$. Let $\Sigma$ be the set of discrete valuation rings $V$ of $\overline{K}(C)$ and $\Sigma_\infty$ be the set of $V\in\Sigma$ with $V\cap\overline{K}(X) = V_\infty$, where $V_\infty$ is the discrete valuation ring of $\overline{K}(X)$ having as elements the fractions $b(X)/c(X)$ with $\deg b \leq \deg c$. If $V\in\Sigma$ and $h\in\overline{K}(C)$, then we denote by $\mathrm{ord}_V(h)$ the order of $h$ at $V$ and by $(h)_\infty$ the divisor of poles of the function $h$. We set

$$|h|_V = \exp\{-\mathrm{ord}_V(h)\}.$$

Thus we define an ultrametric absolute value on $\overline{K}(C)$. Furthermore, if

$$A(X) = a_0X^k + \cdots + a_k$$

is a polynomial with coefficients in $\overline{K}(C)$, then we put

$$|A|_V = \max\{|a_0|_V,\ldots,|a_k|_V\}.$$

We define the *height* of $A(X)$ over $\overline{K}(C)$ by

$$H_C(A) = \prod_{V \in \Sigma} \max\{|a_0|_V, \ldots, |a_k|_V\}.$$

If $a_0 = 1$, then [7, Proposition 3.1, p. 62] gives

$$H_C(A) = \exp\{\deg(\sup_i(a_i)_\infty)\}.$$

For the proof of the Proposition 2.1 we shall need the following lemmas.

**Lemma 2.1** *Suppose that $C$ is smooth. Let $u$ be an integral element over $K[C]$ of degree $\mu > 1$ and $G(X, U)$ be a polynomial of $K[X, U]$ such that $G(x, u) = 0$. Put $\gamma = \deg_X G$. Then the irreducible polynomial of $u$ over $K(C)$ has the form*

$$P(U) = U^\mu + p_1(x, y)U^{\mu-1} + \cdots + p_\mu(x, y),$$

*where $p_i(x, y) \in K[C]$ $(i = 1, \ldots, \mu)$ with*

$$\deg(p_i(x, y))_\infty \leq 2\gamma n.$$

*Proof.* Since $C$ is smooth, it follows that the ring $K[C]$ is integrally closed. Thus the irreducible polynomial of $u$ over $K(C)$ has the form

$$P(U) = U^\mu + p_1(x, y)U^{\mu-1} + \cdots + p_\mu(x, y),$$

where $p_i(x, y) \in K[C]$ $(i = 1, \ldots, \mu)$. Write

$$G(X, U) = g_0(X)U^\nu + \cdots + g_\nu(X)$$

where $g_j(X) \in K[X]$ $(j = 0, \ldots, \nu)$ and $g_0(X) \neq 0$. Without loss of generality we may consider that the polynomials $g_j(X)$ are relatively prime. Since $G(x, u) = 0$, it follows that $P(x, y, U)$ divides $G(x, U)$. Thus, [7, Proposition 2.4, p. 57] yields

$$H_C(P(x, y, U)) \leq H_C(G(x, U)),$$

whence it follows

$$\deg(p_i(x, y))_\infty \leq \deg(\sup_{1 \leq j \leq \nu}(g_j(x)/g_0(x))_\infty).$$

Let $g_0(X) = b_0(X - b_1)^{c_1} \cdots (X - b_s)^{c_s}$ and $V_{i,j}$ $(j = 1, \ldots, r(i))$ be the rings of $\Sigma$ lying above the discrete valuation ring of $\overline{K}(X)$ defined by $X - b_i$ and $e_{i,j}$ be the ramification index of $V_{i,j}$. The divisor of poles of $g_i/g_0$ satisfies

$$\deg((g_i(x)/g_0(x))_\infty) \leq \deg(\sum_{V \in \Sigma_\infty} (\deg g_i)\mathrm{ord}_V(1/x)V + \sum_{i,j} c_i e_{i,j} V_{i,j}).$$

Thus

$$\deg(p_i(x, y))_\infty \leq 2\gamma n.$$

**Lemma 2.2** *Let $a(x, y) \in K[C]$ with $\deg(a(x, y))_\infty \leq 2\gamma n$, where $\gamma$ is a positive integer. Then there is $A(X, Y) \in K[X, Y]$ with $\deg A < 5\gamma N^3$ such that $a(x, y) = A(x, y)$.*

*Proof.* Consider the divisor

$$D = 2\gamma n \sum_{V \in \Sigma_\infty} V$$

and denote by $l(D)$ the dimension of the Riemann-Roch space $L(D)$. By [13, Theorems A2 and B2], it follows that there are polynomials $b_1(X,Y)$, …, $b_{l(D)}(X,Y)$, $q(X)$ with coefficients in $K$ and

$$\deg q \leq m(n-1), \quad \deg_Y b_i \leq n-1, \quad \deg_X b_i \leq 6\gamma n^2 + 2mn,$$

such that the functions $\phi_1, \ldots, \phi_{l(D)}$ defined by the fractions $b_1(X,Y)/q(X)$, …, $b_{l(D)}(X,Y)/q(X)$, respectively, on $C$, form a basis of $L(D)$. The leading coefficient of $q(X)$ is 1 and if $q(X) \neq 1$, then its roots are among the roots of the discriminant of $F(X,Y)$ (considered as polynomial in $Y$).

Since $a(x,y) \in K[C]$ there is $A(X,Y) \in K[X,Y]$ with $a(x,y) = A(x,y)$. Further, $a(x,y)$ is an element of $L(D)$ defined over $K$. Thus

$$a(x,y) = f(x,y)/q(x) \quad (i = 1, \ldots, \mu),$$

where $f(X,Y)$ is a linear combination of $b_1(X,Y), \ldots, b_{l(D)}(X,Y)$ with coefficients in $K$. It follows that there are polynomials $B_i(X,Y)$ $(i = 1, \ldots, \mu)$ with coefficients in $K$ such that

$$f(X,Y) = q(X)A(X,Y) + B_i(X,Y)F(X,Y) \quad (i = 1, \ldots, l(D)).$$

Let $q_h(X,Z)$ and $F_h(X,Y,Z)$ be the homogenizations of $q(X)$ and $F(X,Y)$, respectively. Since $F(X,Y)$ is absolutely irreducible, $\{F_h, q_h\}$ is a regular sequence. So, by [16, Proposition 2], it follows that we can take

$$\deg A_i, \deg B_i < 5\gamma N^3.$$

**Lemma 2.3** *Let $a_{j,s} \in K$ $(j = 1, \ldots, q,\ s = 1, \ldots, p)$. Suppose that the homogeneous linear system*

$$a_{j,1}X_1 + \cdots + a_{j,p}X_p = 0 \quad (j = 1, \ldots, q)$$

*has rank $r$. If the system has a solution $x_1, \ldots, x_p \in K$ with $x_t \neq 0$, then there is a solution $y_1, \ldots, y_p \in K$ with $y_t \neq 0$, such that for every absolute value $|\cdot|_v$ of $K$ we have*

$$|y_i|_v \leq \max\{1, |r!|_v\} (\max_{i,j}\{|a_{j,i}|_v\})^r \quad (i = 1, \ldots, p).$$

*If $a_{j,s} \in O_K$ $(j = 1, \ldots, q,\ s = 1, \ldots, p)$, then there is a solution $y_1, \ldots, y_p \in O_K$ with $y_t \neq 0$ such that for every absolute value of $K$ the above inequality holds.*

*Proof.* We may suppose, without loss of generality, that the matrix $M = (a_{i,j})_{1 \leq i,j \leq r}$ has rank $r$. Thus, the above system is equivalent to the system

$$\Delta X_i = \Delta_{i,r+1}X_{r+1} + \cdots + \Delta_{i,p}X_p \quad (i = 1, \ldots, r),$$

where $\Delta = \det M$ and $\Delta_{i,j}$ $(i = 1, \ldots, r,\ j = r+1, \ldots, p)$ are minors of order $r$ of the matrix $(a_{i,j})$. Hence, $\Delta_{i,j} \in K$ and

$$|\Delta_{i,j}|_v \leq \max\{1, |r!|_v\} (\max_{i,j}\{|a_{j,i}|_v\})^r \quad (i = 1, \ldots, r,\ j = r+1, \ldots, p).$$

Furthermore, if $a_{j,s}\in O_K$ $(j = 1,\dots,q,\ s = 1,\dots,p)$, then $\Delta_{i,j}\in O_K$ $(i = 1,\dots,r,\ j = r+1,\dots,p)$.

If $1 \le t \le r$, since there is a solution $x_1,\dots,x_p$ with $x_t \neq 0$, we obtain that there is $s\in\{r+1,\dots,p\}$ such that $\Delta_{t,s} \neq 0$. Thus, a solution of the system with the required properties is given by

$$X_s = \Delta,\ X_j = 0\ (j = r+1,\dots,p,\ j \neq s),\ X_i = \Delta_{i,s}\ (i = 1,\dots,r).$$

If $r+1 \le t \le p$, then the required solution is given by

$$X_t = \Delta,\ X_j = 0\ (j = r+1,\dots,p,\ j \neq t),\ X_i = \Delta_{i,t}\ (i = 1,\dots,r).$$

*Proof of the Proposition* 2.1. By Lemmata 2.1 and 2.2, there is a polynomial

$$P(X,Y,U) = U^\mu + p_1(X,Y)U^{\mu-1} + \cdots + p_\mu(X,Y),$$

where $p_1(X,Y),\dots,p_\mu(X,Y)\in K[X,Y]$ such that $P(x,y,U)$ is the irreducible polynomial of $u$ over $K(C)$ and

$$\deg p_i < 5\gamma N^3.$$

Put $\theta = 5\gamma N^3$. Consider $\theta N$ distinct points $(x_i,y_i)$ $(i = 1,\dots,\theta N)$ on $C$ with $x_i\in\mathbb{Z}$ and $|x_i| \le \theta N$. Since $P(x_i,y_i,U)$ divides $G(x_i,U)$, [4, Proposition B.7.3, p. 228] gives

$$H(1,p_1(x_i,y_i),\dots,p_\mu(x_i,y_i)) \le e^\nu H(g_0(x_i),\dots,g_\nu(x_i)).$$

Thus

$$H(1,p_1(x_i,y_i),\dots,p_\mu(x_i,y_i)) \le e^\nu H(G)|x_i|^\gamma(\gamma+1) \quad (i = 1,\dots,\theta N).$$

Write

$$p_r(X,Y) = \sum_{k+l<\theta} \pi_{r,k,l}X^kY^l \quad (r = 1,\dots,\mu).$$

We set $b_{r,i} = p_r(x_i,y_i)$ and consider the homogeneous linear system

$$\sum_{k+l<\theta} X_{r,k,l}x_i^ky_i^l - b_{r,i}Z = 0 \quad (r = 1,\dots,\mu,\ i = 1,\dots,\theta N).$$

A solution is given by $X_{r,k,l} = \pi_{r,k,l}$ $(r = 1,\dots,\mu,\ 0 \le k+l \le \deg p_r)$, $X_{r,k,l} = 0$ $(r = 1,\dots,\mu,\ \deg p_r < k+l \le \theta N)$, and $Z = 1$. The number of equations is $\mu\theta N$ and the number of unknowns is at most $\mu(\theta+1)\theta/2+1$. By Lemma 2.3, there is a solution of the system in $K$, $X_{r,k,l} = \rho_{r,k,l}$ and $Z = \zeta \neq 0$, such that the point $R$ of the projective space having as coordinates the elements $\rho_{r,k,l}$ and $\zeta$ satisfies

$$H(R) \le (\mu\theta N)!(H(A)H(B))^{\mu\theta N},$$

where $A$, $B$ are the points in the projective space defined as follows: the coordinates of $A$ are 1 and the elements $x_i^ky_j^l$ and the coordinates of $B$ are 1 and the elements $b_{r,j}$.

We have

$$H(A) \le H(1,x_1,\dots,x_{\theta N})^\theta H(1,y_1,\dots,y_{\theta N})^\theta \le (\theta N H(y_1)\cdots H(y_{\theta N}))^\theta$$

and using [11, Lemma 7] we obtain

$$H(A) \leq \Lambda_2(N,\gamma)H(F)^{25\gamma^2N^7}.$$

Further, we have

$$H(B) < \Lambda_3(N,\gamma,\nu)H(G)^{5\gamma N^4}.$$

Therefore

$$H(R) < \Lambda_4(N,\gamma,\nu,\mu)(H(G)H(F)^{5\gamma N^3})^{25\mu\gamma^2N^8}.$$

Write

$$Q_r(X,Y) = \sum_{k+l<\theta} (\rho_{r,k,l}/\zeta)X^kY^l.$$

Then $b_{r,i} = Q_r(x_i,y_i)$. Hence the $\theta N$ distinct points $(x_i,y_i)$ $(i = 1,\ldots,\theta N)$ of $C$ are zeros of the polynomial $\phi(X,Y) = p_r(X,Y) - q_r(X,Y)$. Since $\theta \deg F > (\deg\phi)(\deg F)$, Bézout's theorem implies that $F(X,Y)$ divides $\phi(X,Y)$ and therefore $p_r(x,y) = q_r(x,y)$. Thus, we can take $p_i(X,Y) = q_i(X,Y)$ and if $Q$ is a point of the projective space having as coordinates 1 and the coefficients of $q_r(X,Y)$, then $H(Q) = H(R)$. The lemma follows.

# 3 Polynomials with no Common Zero

Let $\phi : \bar{C} \to C$ be an unramified morphism of affine plane (irreducible) curves defined over $K$ of degree $m > 1$. Since the morphism $\phi$ is finite, the homomorphism $\phi^* : \overline{K}[C] \to \overline{K}[\bar{C}]$, defined by $\phi^*(f) = \phi \circ f$ for every $f \in \overline{K}[C]$, is injective and is extended to a field homomorphism $\phi^* : \overline{K}(C) \to \overline{K}(\bar{C})$. We also identify $\overline{K}(C)$ with its image into $\overline{K}(\bar{C})$. Let $x$, $y$ be the coordinate functions on $C$ and $\bar{x}$, $\bar{y}$ be the coordinate functions on $\bar{C}$. Suppose that the curve $C$ is defined by the polynomial $F(X,Y) \in K[X,Y]$. Let $u_\rho = \bar{y} + \rho\bar{x}$, where $\rho \in \overline{K}$, and

$$P_\rho(X,Y,U) = U^{\mu(\rho)} + p_{\rho,1}(X,Y)U^{\mu(\rho)-1} + \cdots + p_{\rho,\mu(\rho)}(X,Y)$$

is a polynomial of $K[X,Y,U]$ such that $P_\rho(x,y,U)$ is the irreducible polynomial of $u_\rho$ over $K(\rho)(C)$. We have $\mu(\rho) \leq m$. We denote by $\Pi$ the maximum of the degrees of the polynomials $p_{\rho,j}$ $(j = 1,\ldots,\mu(\rho))$ and by $R$ the degree of $P_\rho(x,y,U)$, considered as polynomial in $\rho$.

**Lemma 3.1** *Let $D_\rho(X,Y)$ be the discriminant of $P_\rho(X,Y,U)$, considered as polynomial with coefficients in $K[X,Y]$. Let $r \in \overline{K}$ such that $D_r(X,Y)$ is not a constant. Then there is a set $A \subset \overline{K}$ with $|A| \leq (2m-1)R((2m-1)N\Pi + 1)$ such that for every $t \in \overline{K} \setminus A$, with $t \neq r$, $D_t(X,Y)$ is not a constant and the polynomials $D_r(X,Y)$, $D_t(X,Y)$, and $F(X,Y)$ have no common zero.*

*Proof.* Let $V_\rho$ be the set defined by the equations

$$D_\rho(X,Y) = F(X,Y) = 0.$$

Since the polynomial $P_\rho(x,y,U)$ is irreducible, it follows that $F(X,Y)$ does not divide $D_\rho(X,Y)$ and so the set $V_\rho$ is finite. We have $\deg D_\rho(X,Y) \leq (2m-1)\Pi$ and so Bézout's theorem implies that $|V_\rho| \leq (2m-1)N\Pi$.

Let $r \in \overline{K}$. Suppose that $V_r$ is not empty and let $(\alpha_{r,j},\beta_{r,j})$ $(j = 1,\ldots,s(r))$ be all its points (hence $D_r(X,Y)$ is not a constant). Then for every $j =$

$1,\dots,s(r)$ there are $m$ distinct points $(a_{r,j,i}, b_{r,j,i})$ $(i = 1,\dots,m)$ of $\bar{C}$ with $\phi(a_{r,j,i}, b_{r,j,i}) = (\alpha_{r,j}, \beta_{r,j})$ and $\zeta_{r,j} \in \mathbb{Z}$ such that $a_{r,j,k}\zeta_{r,j} + b_{r,j,k} \neq a_{r,j,l}\zeta_{r,j} + b_{r,j,l}$, for $k \neq l$. Hence $P_{\zeta_{r,j}}(\alpha_{r,j}, \beta_{r,j}, U)$ has exactly $m$ distinct roots and so $D_{\zeta_{r,j}}(\alpha_{r,j}, \beta_{r,j}) \neq 0$. It follows that the degree in $\rho$ of $D_\rho(\alpha_{r,j}, \beta_{r,j})$ is $\geq 1$ and so we obtain that $D_\rho(x,y)$ is not independent from $\rho$.

If $D_\rho(x,y)$ is independent from $x$ and $y$, then there is $e \in \overline{K}$ such that $D_e(x,y) = 0$ and hence $P_e(x,y,U)$ divides its derivative with respect to $U$ which is a contradiction. So, $D_\rho(x,y)$ is not independent from $x$ and $y$.

The degree in $\rho$ of $D_\rho(x,y)$ is $\leq (2m-1)R$. So, for every $j = 1,\dots,s(r)$ there are at most $(2m-1)R$ integers $\rho$ with $D_\rho(\alpha_{r,j}, \beta_{r,j}) = 0$. Also, there are at most $(2m-1)R$ integers $\rho$ such that $D_\rho(x,y)$ is independent from $x$ and $y$.

Thus, there is a set $A \subset \overline{K}$ with $|A| \leq (2m-1)R((2m-1)N\Pi + 1)$ such that for every $t \in \overline{K} \setminus A$ with $t \neq r$ we have $D_t(\alpha_{r,j}, \beta_{r,j}) \neq 0$ $(j = 1,\dots,s(r)))$ and $D_t(X,Y)$ is not a constant. So, the polynomials $D_r(X,Y)$, $D_t(X,Y)$, and $F(X,Y)$ have no common zero.

**Lemma 3.2** *Let $F_j$ $(j = 1,2,3)$ be polynomials in $O_K[X_1, X_2]$, with $\deg F_j = d_j$ and $d_1 \geq d_2 \geq d_3 \geq 1$, having no common zero in $\overline{K}^2$. We denote by $\Phi$ a point in the projective space having as coordinates the coefficients of $F_j$ (in any order) and we set $\delta = \max\{d_1 d_3, d_1 + d_2 + d_3 - 2\}$. Then there are polynomials $A_j$ $(j = 1,2,3)$ in $O_K[X_1, X_2]$ and $c \in O_K \setminus \{0\}$ such that*

$$A_1 F_1 + A_2 F_2 + A_3 F_3 = c.$$

*Furthermore, $\deg A_j F_j \leq \delta$ and for every archimedean absolute value $|\cdot|_v$ of $K$ we have*

$$|A_j|_v, |c|_v \leq ((\delta+2)(\delta+1)/2)!\ |\Phi|_v^{(\delta+2)(\delta+1)/2}.$$

*Proof.* By [16, Corollary 3], there are polynomials $A_j$ of $K[X_1, X_2]$ $(j = 1,2,3)$, with $\deg A_j = e_j$, such that

$$A_1 F_1 + A_2 F_2 + A_3 F_3 = 1$$

and $\deg A_j F_j \leq \delta$. We put

$$F_j = \sum_{i_1 + i_2 \leq d_j} f_{j,i_1,i_2} X_1^{i_1} X_2^{i_2} \quad (j = 1,2,3)$$

and

$$A_j = \sum_{i_1 + i_2 \leq e_j} a_{j,i_1,i_2} X_1^{i_1} X_2^{i_2} \quad (j = 1,2,3).$$

Hence

$$\sum_{s_1 + s_2 \leq \delta} (\sum_{j=1}^{3} \sum_{k_j + p_j = s_j} f_{j,k_1,k_2} a_{j,p_1,p_2}) X_1^{s_1} X_2^{s_2} = 1.$$

Thus, the numbers $a_{j,p_1,p_2}$ and 1 is a solution of the homogeneous linear system

$$\sum_{j=1}^{3} \sum_{k_j + p_j = s_j} f_{j,k_1,k_2} X_{j,p_1,p_2} = 0 \quad (s_1 + s_2 = 1,\dots,\delta),$$

$$\sum_{j=1}^{3} f_{j,0,0}X_{j,0,0} - Z = 0.$$

The number of the equations of the above system is at most equal to $(\delta+2)(\delta+1)/2$. Lemma 2.3 implies that there is a non trivial solution $b_{j,p_1,p_2}$ and $c$ in $O_K$ with $c \neq 0$ such that for every archimedean absolute $|\cdot|_v$ of $K$ we have

$$|b_{j,p_1,p_2}|_v, |c|_v \leq ((\delta+2)(\delta+1)/2)! \ |\Phi|_v^{(\delta+2)(\delta+1)/2},$$

where $\Phi$ is a point in the projective space having as coordinates the coefficients of $F_j$ (in any order). Furthermore, the polynomials

$$B_j = \sum_{i_1+i_2 \leq e_j} b_{j,i_1,i_2} X_1^{i_1} X_2^{i_2} \quad (j = 1, 2, 3)$$

satisfy the equality

$$B_1F_1 + B_2F_2 + B_3F_3 = c.$$

**Lemma 3.3** *Let $F_j$ $(j = 1, 2)$ be polynomials in $O_K[X_1, X_2]$, with $\deg F_j \geq 1$, having no common zero in $\overline{K}^2$. Suppose that $F_1$ is absolutely irreducible and does not divide $F_2$. We denote by $\Phi$ the point in the projective space having as coordinates the coefficients of $F_1$ and $F_2$ (in any order) and put $\delta = \deg F_1 \deg F_2$. Then there are $A_j \in O_K[X_1, X_2]$ $(j = 1, 2)$, with $\deg A_jF_j \leq \delta$, and $c \in O_K \setminus \{0\}$ such that*

$$A_1F_1 + A_2F_2 = c.$$

*Furthermore, for every archimedean absolute value $|\cdot|_v$ of $K$ we have*

$$|A_j|_v, |c|_v \leq ((\delta+2)(\delta+1)/2)! \ |\Phi|_v^{(\delta+2)(\delta+1)/2}.$$

*Proof.* Let $F_{i,h}$ be the homogenization of $F_i$. Then, $F_{1,h}$ is absolutely irreducible and does not divide $F_{2,h}$. Then the class of $F_{2,h}$ is not zero in the integral domain $K[X, Y, Z]/(F_{1,h})$ and hence $\{F_{1,h}, F_{2,h}\}$ is a regular sequence. By [16, Corollary 5], there are polynomials $A_j \in K[X_1, X_2]$ $(j = 1, 2)$, with $\deg A_jF_j \leq \delta$, such that

$$A_1F_1 + A_2F_2 = 1.$$

Next, working as in the previous lemma, the result follows.

# 4 Some Auxiliary Lemmata

In this section we give some lemmata useful for the proof of Theorem 1.1.

**Lemma 4.1** *Let $a \in K$. Then there is an integer $\delta > 0$ with $\delta \leq H_K(a)$ such that $\delta a \in O_K$.*

*Proof.* Put $e = [\mathbb{Q}(a) : \mathbb{Q}]$. Then $a$ is a root of a polynomial $P(X) = c_0X^e + \cdots + c_e$ with integer pairwise prime coefficients and $c_0 > 0$. So, $c_0a$ is an algebraic integer. By [7, page 54], we have

$$H_K(a) = c_0 \prod_{i=1}^{e} \max\{1, |a_i|\},$$

where $a_1, \ldots, a_d$ are the distinct conjugates of $a$. Thus $c_0 \leq H_K(a)$.

Next lemma deals with the resultant of two polynomials. For a formal definition of the resultant see [8, Chapter V, §10]

**Lemma 4.2** *Let $P$ and $S$ be polynomials of $O_K[X_1, \ldots, X_n] \setminus K$ and $R$ be its resultant with respect to $X_n$. Put $p_i = \deg_{X_i} P$ and $s_i = \deg_{X_i} S$ $(i = 1, \ldots, n)$. Suppose that $R \neq 0$. Then $\deg_{X_i} R \leq s_n p_i + p_n s_i$ $(i = 1, \ldots, n-1)$ and*

$$H(R) \leq (p_n + s_n)!(\prod_{i=1}^{n-1}(p_i + 1))^{s_n}(\prod_{i=1}^{n-1}(s_i + 1))^{p_n} H(P)^{s_n} H(S)^{p_n}.$$

*If $\mathbf{R}$, $\mathbf{P}$, $\mathbf{S}$ are points in the projective space having as coordinates 1 and the coefficients of $R$, $P$, $S$ respectively, then the above inequality holds with the quantities $\mathbf{R}$, $\mathbf{P}$, $\mathbf{S}$ in the places of $R$, $P$, $S$ respectively.*

*Proof.* Write

$$P = \Pi_0(X_1, \ldots, X_{n-1}) X_n^{p_n} + \cdots + \Pi_{p_n}(X_1, \ldots, X_{n-1}),$$

$$S = \Sigma_0(X_1, \ldots, X_{n-1}) X_n^{s_n} + \cdots + \Sigma_{s_n}(X_1, \ldots, X_{n-1}),$$

where $\Pi_i(X_1, \ldots, X_{n-1})$ $(i = 0, \ldots, p_n)$ and $\Sigma_j(X_1, \ldots, X_{n-1})$ $(j = 0, \ldots, s_n)$ are polynomials with coefficients in $K$. The resultant $R$ is a homogeneous polynomial with integer coefficients of degree $s_n$ in $\Pi_i(X_1, \ldots, X_{n-1})$ and of degree $p_n$ in $\Sigma_j(X_1, \ldots, X_{n-1})$. Let $|\cdot|_v$ be an absolute value of $K$. If $|\cdot|_v$ is not archimedean, then

$$|R|_v \leq |P|_v^{s_n} |S|_v^{p_n}.$$

Now, suppose that $|\cdot|_v$ is archimedean. If $M(X_1, \ldots, X_{n-1})$ is a monomial of degree $s_n$ in $\Pi_i(X_1, \ldots, X_{n-1})$ and of degree $p_n$ in $\Sigma_j(X_1, \ldots, X_{n-1})$, then

$$|M|_v \leq (\prod_{i=1}^{n-1}(p_i + 1)|P|_v)^{s_n}(\prod_{i=1}^{n-1}(s_i + 1)|S|_v)^{p_n}.$$

Thus

$$|R|_v \leq (p_n + s_n)!(\prod_{i=1}^{n-1}(p_i + 1)|P|_v)^{s_n}(\prod_{i=1}^{n-1}(s_i + 1)|S|_v)^{p_n}.$$

Hence, we have the inequalities

$$H(R) \leq (p_n + s_n)!(\prod_{i=1}^{n-1}(p_i + 1))^{s_n}(\prod_{i=1}^{n-1}(s_i + 1))^{p_n} H(P)^{s_n} H(S)^{p_n},$$

and

$$H(\mathbf{R}) \leq (p_n + s_n)!(\prod_{i=1}^{n-1}(p_i + 1))^{s_n}(\prod_{i=1}^{n-1}(s_i + 1))^{p_n} H(\mathbf{P})^{s_n} H(\mathbf{S})^{p_n}.$$

Furthermore, from the definition of the resultant, we obtain that $\deg_{X_i} R \leq s_n p_i + p_n s_i$ $(i = 1, \ldots, n-1)$.

**Lemma 4.3** *Let $L$ be a finite extension of $K$ of degree $\mu$ and $\Re$ be the set of prime ideals of $O_K$ which are ramified in $L$. Then the discriminant $D_{L/K}$ of the extension $L/K$ satisfies*

$$N_K(D_{L/K}) < \prod_{\wp\in\Re} N_K(\wp)^{\mu-1}\exp(2\mu^2 d).$$

*Proof.* For every prime $p$ and every prime ideal $\wp$ of $O_K$ dividing $p$ we denote by $e_\wp$ and $f_\wp$ the ramification index and the residuel class degree of $\wp$ respectively. Furthermore, if $P$ is a prime ideal of $O_L$ dividing $\wp$, then we denote by $e(P/\wp)$ and by $f(P/\wp)$ the ramification index and the residuel class degree of $P$ over $\wp$ respectively. Finally, let $\mathrm{ord}_P$ be the discrete valuation of $L$ associated to $P$ and $\mathrm{ord}_p$ be the discrete valuation of $\mathbb{Q}$ associated to $p$.

By [9, Proposition 6.3], we get

$$D_{L/K} = \prod_{\wp\in\Re} \wp^{a_\wp},$$

where

$$a_\wp \leq \sum_{P|\wp}(e(P/\wp) - 1 + \mathrm{ord}_P(e(P/\wp)))f(P/\wp).$$

If $p > \mu$, then $\mathrm{ord}_P(e(P/\wp)) = 0$ and hence $a_p \leq \mu - 1$. Suppose that $p \leq \mu$. We have

$$\begin{aligned}\sum_{P|\wp}\mathrm{ord}_P(e(P/\wp))f(P/\wp) &= e_\wp\sum_{P|\wp}e(P/\wp)f(P/\wp)\mathrm{ord}_p(e(P/\wp))\\ &= (e_\wp/\log p)\sum_{P|\wp}e(P/\wp)f(P/\wp)\log e(P/\wp)\\ &\leq (e_\wp/\log p)\mu\log\mu.\end{aligned}$$

Thus

$$\prod_{\wp|p} N_K(\wp)^{\sum_{P|\wp}\mathrm{ord}_P(e(P/\wp))f(P/\wp)} \leq p^{(\mu\log\mu/\log p)\sum_{\wp|p} f_\wp e_\wp} = \exp(d\mu\log\mu).$$

Hence, we obtain

$$N_K(D_{L/K}) \leq \prod_{\wp\in\Re} N_K(\wp)^{\mu-1}\exp(\pi(\mu)d\mu\log\mu),$$

where $\pi(\mu)$ is the number of primes $\leq \mu$. Since $\pi(\mu) < 2\mu/\log\mu$, the result follows.

**Lemma 4.4** *Let $g_j(X,Y)$ $(j = 1,\ldots,k)$ be polynomials of $K[X,Y]$ of degree $\leq M$ and $p,q,r,s,t,u \in K$. We set*

$$G_j(U,V) = g_j(pU + qV + r, sU + tV + u), \quad (j = 1,\ldots,k)$$

*and we denote by $\Gamma$ and $\gamma$ the two points in the projective space having as coordinates the coefficients of $G_j(X,Y)$ and $g_j(X,Y)$ respectively. Then*

$$H(\Gamma) \leq 2^{M(1+2e)}(M+1)H(1,p,q,s,t)^M H(1,r,u)^M H(\gamma),$$

*where $e = 1$ if $(r,u) \neq (0,0)$ and $e = 0$ otherwise.*

*Proof.* Put $b_i(X,Y) = g_i(X+r, Y+u)$. By [4, Proposition B.7.4(e), page 234], for every absolute value $|\cdot|_v$ of $K$, we have

$$|b_i|_v \leq \max\{1, |2|_v\}^{2M} \max\{1, |r|_v, |u|_v\}^M |g_i|_v.$$

Write

$$b_i(X,Y) = \sum_{i+j \leq M} a_{i,j} X^i Y^j.$$

Since $G_i(U,V) = b_i(pU+qV, sU+tV)$ we have

$$\begin{aligned} G_i(U,V) &= \sum_{i+j\leq M} a_{i,j}(pU+qV)^i(sU+tV)^j \\ &= \sum_{i+j\leq M} a_{i,j} \sum_{\pi=0}^{i}\sum_{\rho=0}^{j} \left( \begin{array}{c} i \\ \pi \end{array} \right) \left( \begin{array}{c} j \\ \rho \end{array} \right) p^\pi q^{i-\pi} s^\rho t^{j-\rho} U^{\pi+\rho} V^{i+j-\pi-\rho}. \end{aligned}$$

The coefficient of $U^S V^T$ is

$$c_{S,T} = \sum_{i+j=S+T} a_{i,j} \sum_{\pi=0}^{i}\sum_{\rho=0}^{j} \left( \begin{array}{c} i \\ \pi \end{array} \right) \left( \begin{array}{c} j \\ \rho \end{array} \right) p^\pi q^{i-\pi} s^\rho t^{j-\rho}.$$

If $|\cdot|_v$ is an archimedean absolute value of $K$, then

$$\begin{aligned} |c_{S,T}|_v &\leq \sum_{i+j=S+T} |a_{i,j}|_v \max\{1, |p|_v, |q|_v, |s|_v, |t|_v\}^{i+j} \sum_{\pi=0}^{i} \left( \begin{array}{c} i \\ \pi \end{array} \right) \sum_{\rho=0}^{j} \left( \begin{array}{c} j \\ \rho \end{array} \right) \\ &\leq 2^{S+T} |b_i|_v (S+T+1) \max\{1, |p|_v, |q|_v, |s|_v, |t|_v\}^{S+T}. \end{aligned}$$

If $|\cdot|_v$ is a non archimedean absolute value of $K$, then $|c_{S,T}|_v \leq |b_i|_v$. Thus, for every absolute value $|\cdot|_v$ of $K$ we have

$$\begin{aligned} |G_i|_v \leq \max\{1, |2|_v\}^{M(1+2e(r))} \max\{1, |M+1|_v\} \\ \times \max\{1, |p|_v, |q|_v, |s|_v, |t|_v\}^M \max\{1, |r|_v, |u|_v\}^M |g_i|_v. \end{aligned}$$

The result follows.

# 5 Proof of Theorem 1.1

Since the morphism $\phi$ is finite, the homomorphism $\phi^* : \overline{K}[C] \to \overline{K}[\bar{C}]$, defined by $\phi^*(f) = \phi \circ f$ for every $f \in \overline{K}[C]$, is injective and so we may identify $\overline{K}[C]$ with its image into $\overline{K}[\bar{C}]$. Thus, if $x$, $y$ are the coordinate functions on $C$ and $\bar{x}$, $\bar{y}$ the coordinate functions on $\bar{C}$, then $x = \phi_1(\bar{x}, \bar{y})$ and $y = \phi_2(\bar{x}, \bar{y})$. Further, the morphism $\phi^*$ is extended to a field homomorphism $\phi^* : \overline{K}(C) \to \overline{K}(\bar{C})$. We also identify $\overline{K}(C)$ with its image into $\overline{K}(\bar{C})$. Thus, for every $\rho \in \overline{K}$ the function $u_\rho = \bar{y} + \rho\bar{x}$ is an integral element over $\overline{K}[C]$.

Consider the polynomials

$$E(W, X, \bar{X}, U) = X - \phi_1(\bar{X}, U - W\bar{X}), \quad \bar{F}_1(W, \bar{X}, U) = \bar{F}(\bar{X}, U - W\bar{X}).$$

We have

$$E(\rho, x, \bar{x}, u_\rho) = \bar{F}_1(\rho, \bar{x}, u_\rho) = 0.$$

We denote by $G(W,X,U)$ the resultant of $E(W,X,\bar{X},U)$ and $\bar{F}_1(W,\bar{X},U)$ with respect to $\bar{X}$. Then $G(\rho,x,u_\rho)=0$. If $G(W,X,U)$ is equal to zero, then $\bar{F}_1(W,\bar{X},U)$ divides $E(W,X,\bar{X},U)$ which is not the case. Therefore, $G(W,X,U)\neq 0$.

By Lemma 4.2, $\deg_X G \leq \bar{N}$, $\deg_U G \leq 2M\bar{N}$, and $\deg_W G \leq 2M\bar{N}$. For $\rho \in \overline{K}$, we put $G_\rho(X,U)=G(\rho,X,U)$, $E_\rho(X,\bar{X},U)=E(\rho,X,\bar{X},U)$ and $\bar{F}_\rho(\bar{X},U)=\bar{F}_1(\rho,\bar{X},U)$. Then Lemma 4.2 implies

$$H(G_\rho) \leq (M+\bar{N})!(1+\bar{N})^M(2(1+M))^{\bar{N}}H(E_\rho)^{\bar{N}}H(\bar{F}_\rho)^M.$$

On the other hand, Lemma 4.4 yields

$$H(\bar{F}_\rho) \leq 2^{\bar{N}}(\bar{N}+1)H(\rho)^{\bar{N}}H(\bar{F}), \quad H(E_\rho) \leq 2^M(M+1)H(\rho)^M H(\Phi),$$

where $\Phi$ is a point of the projective space having as coordinates the coefficients of $\phi_i(X,Y)$ $(i=1,2)$. Therefore

$$H(G_\rho) < (M+\bar{N}+1)^{3M+3\bar{N}}(2H(\rho))^{2\bar{N}M}H(\Phi)^{\bar{N}}H(\bar{F})^M.$$

Let $I(T)=T^s+b_1T^{s-1}+\cdots+b_s$, where $b_j{\in}\overline{K}[C]$ $(j=1,\ldots,s)$, the irreducible polynomial of $u_\rho$ over $\overline{K}(C)$. For every $\sigma{\in}\mathrm{Gal}(\overline{K}/K(\rho))$ we set $I^\sigma(T)=T^s+\sigma(b_1)T^{s-1}+\cdots+\sigma(b_s)$. Since the function $u_\rho$ is defined over $K(\rho)$, we have $I^\sigma(u_\rho)=0$ for every $\sigma{\in}\mathrm{Gal}(\overline{K}/K(\rho))$. Thus, $\sigma(b_j)=b_j$, for every $\sigma{\in}\mathrm{Gal}(\overline{K}/K(\rho))$ and hence $b_j{\in}K(\rho)[C]$. Therefore, $u_\rho$ is integral over $K(\rho)[C]$ and $[\overline{K}(C)(u_\rho):\overline{K}(C)]=[K(\rho)(C)(u_\rho):K(\rho)(C)]$. By Proposition 2.1 and the bound for the quantity $H(G_\rho)$ we obtain that there is a polynomial

$$P_\rho(X,Y,U)=U^{\mu(\rho)}+p_{\rho,1}(X,Y)U^{\mu(\rho)-1}+\cdots+p_{\rho,\mu(\rho)}(X,Y)$$

of $K(\rho)[X,Y,U]$ with $\mu(\rho)=[K(\rho)(C)(u_\rho):K(\rho)(C)]\leq m$, and

$$H(P_\rho) < \Lambda_5(N,\bar{N},M,m,\rho)\ (H(F)^{5\bar{N}N^3}H(\Phi)^{\bar{N}}H(\bar{F})^M)^{25m\bar{N}^2N^8}$$

such that $P_\rho(x,y,U)$ is the irreducible polynomial of $u_\rho$ over $K(\rho)(C)$. Moreover, we have $\deg p_{\rho,i} < 5\bar{N}N^3$ $(i=1,\ldots,\mu)$.

Let $P=(a,b)$ be a point in $C(O_K)$ and $Q\in\phi^{-1}(P)$. We consider the $\overline{K}(C)$-embedings $\sigma_1,\ldots,\sigma_m$ of $\overline{K}(\bar{C})$ into an algebraic closure of $\overline{K}(C)$. We denote by $\Gamma$ the set of integers $\rho$ with $\sigma_i(u_\rho)\neq\sigma_j(u_\rho)$ for $i\neq j$. Note that at most $m(m-1)/2$ integers do not lie in $\Gamma$. It follows that for every $\rho{\in}\Gamma$ we have $\overline{K}(\bar{C})=\overline{K}(C)(u_\rho)$ and hence for every $\rho{\in}\Gamma$ we have $m=\mu(\rho)$. Further, we similarly deduce that there are at most $m(m-1)/2$ integers $\rho\in\Gamma$ such that $K(u_\rho(Q))\neq K(Q)$. Hence, there is $r{\in}\Gamma$ with $|r|\leq m^2/2$, such that $K(u_r(Q))=K(Q)$. Since $P_\rho(x,y,U)$ divides $G_\rho(x,U)$ and $\deg_W G\leq 2M\bar{N}$, we deduce that the degree of $P_\rho(x,y,U)$, considered as polynomial in $\rho$, is $\leq 2M\bar{N}$. Thus, the degree in $\rho$ of $D_\rho(x,y)$ is $\leq 2(2m-1)M\bar{N}$.

Suppose that the polynomials $D_\rho(X,Y)$ and $F(X,Y)$ have common zeros. Thus, Lemma 3.1 implies that there is $t\in\overline{K}$ with $|t|<21m^2MN^4\bar{N}^2$ such that $D_t(X,Y)$ is not a constant, the polynomials $F(X,Y)$, $D_r(X,Y)$, $D_t(X,Y)$ have no common zero and we have $K(u_r(Q))=K(Q)=K(u_t(Q))$.

Let $D_{\rho,1}$ be a point of the projective space having as coordinates 1 and the coefficients of $D_\rho$. By Lemma 4.2, we have

$$H(D_{\rho,1}) < m^{3m-1}(9\bar{N}N^2)^{4m-2}H(P_\rho)^{2m-1}.$$

We may suppose that one of the coefficients of $F(X, Y)$ is equal to 1. By Lemma 4.1, there are positive integers $a_\rho$ and $b$ with

$$H_K(a_\rho) \leq H_K(P_\rho)^{25m\bar{N}^2N^6} \quad \text{and} \quad H_K(b) \leq H_K(F)^{2N^2}$$

such that the polynomials $a_\rho P_\rho(X, Y, U)$ and $bF(X, Y)$ have all its coefficients in $O_K$. Then the polynomial $a_\rho^{2m-2}D_\rho(X, Y)$ is in $O_K[X, Y]$. Since $F(X, Y)$, $D_r(X, Y)$, and $D_t(X, Y)$ have no common zero, Lemma 3.2 implies that there are polynomials $A_j$ $(j = 1, 2, 3)$ of $O_K[X, Y]$ and $c \in O_K$, $c \neq 0$, such that

$$A_1 a_r^{2m-1} D_r + A_2 a_t^{2m-1} D_t + A_3 bF = c.$$

Further, for every archimedean absolute value $|\cdot|_v$ of $K$ we have

$$|c|_v \leq ((\delta + 1)(\delta + 2)/2)! |\Psi|_v^{(\delta+1)(\delta+2)/2},$$

where $\delta = (2m - 1)5N^4\bar{N}$ and $\Psi$ is a point of the projective space with coordinates 1 and the coefficients of $a_r^{2m-1}D_r(X, Y)$, $a_t^{2m-1}D_t(X, Y)$ and $bF(X, Y)$. Thus

$$\begin{aligned}|N_K(c)| &\leq \\ &(100m^2\bar{N}^2N^8(H(a_r)H(a_t))^{2m-1}H(b)H(D_{r,1})H(D_{t,1})H(F))^{100dm^2\bar{N}^2N^8}.\end{aligned}$$

Using the bounds for all the quantities involved in this estimate, we obtain

$$|N_K(c)| < \Lambda_6(N, \bar{N}, M, m, d) \ (H(F)^{5\bar{N}N^3} H(\Phi)^{\bar{N}} H(\bar{F})^M)^{\lambda dm^5\bar{N}^6N^{22}},$$

where $\lambda$ is a computable numerical constant. Since $D_r(X, Y)$ and $D_t(X, Y)$ have no common zero on $C$, it follows that either $D_r(a, b) \neq 0$ or $D_t(a, b) \neq 0$. On the other hand, we have

$$A_1(a, b)a_r^{2m-1}D_r(a, b) + A_2(a, b)a_t^{2m-1}D_t(a, b) = c.$$

Let $\wp$ be a prime ideal that does not divide $c$, $O_{K,\wp}$ the local ring at $\wp$ and $\tilde{\wp} = \wp O_{K,\wp}$. We put $L = K(Q)$ and $\nu = [L : K]$. We have $L = K(u_r(Q)) = K(u_t(Q))$. We denote by $D_\wp$ the discriminant of the integral closure of $O_{K,\wp}$ in $L$ over $O_{K,\wp}$. Since $\wp$ does not divide $c$, it follows that $\tilde{\wp}$ does not divide at least one of the elements $a_r^{2m-1}D_r(a, b)$ and $a_t^{2m-1}D_t(a, b)$ (in $O_{K,\wp}$). We suppose that $\tilde{\wp}$ does not divide $a_r^{2m-1}D_r(a, b)$. Then $\tilde{\wp}$ does not divide the algebraic integers $a_r$ and $a_r^{2m-2}D_r(a, b)$. Thus, the coefficients of $a_rP_r(X, Y, U)$ lie in $O_K$ and the coefficient of the highest power of $U$, $a_r$, is a unit in $O_{K,\wp}$. Therefore, $u_r(Q)$ is an integral element over $O_{K,\wp}$ and hence $D_\wp$ divides the discriminant $D(1, u_r(Q), \ldots, u_r(Q)^{\nu-1})$ of $1, u_r(Q), \ldots, u_r(Q)^{\nu-1}$ in $O_{K,\wp}$. Further, $D(1, u_r(Q), \ldots, u_r(Q)^{\nu-1})$ divides $D_r(a, b)$. Thus, $D_\wp$ divides $D_r(a, b)$ in $O_{K,\wp}$. Since $\tilde{\wp}$ does not divide $D_r(a, b)$ (in $O_{K,\wp}$), it follows that does not divide $D_\wp$ and hence $\wp$ is not ramified in $L$. Using Lemma 4.3, we deduce

$$\begin{aligned} N_K(D_{L/K}) &< \prod_{\wp | c} N_K(\wp)^{m-1}\exp(2m^2d) \\ &< \Lambda_7(N, \bar{N}, M, m, d) \ (H(F)^{5\bar{N}N^3} H(\Phi)^{\bar{N}} H(\bar{F})^M)^{\lambda dm^6\bar{N}^6N^{22}}. \end{aligned}$$

Suppose now that $D_\rho(X, Y)$ and $F(X, Y)$ have no common zero. If $D_r(X, Y)$ is not a constant, then we work as previously (using Lemma 3.3 instead Lemma

3.2) and we obtain a sharper upper bound for $N_K(D_{L/K})$. Finally, let $D_r(X,Y) = D_r \in K - \{0\}$. If $\eta = a_r^{2m-1}D_r$, then it follows that $L$ is not ramified at every prime ideal $\wp$ of $O_K$ which is not divide $\eta a_r$ and so we deduce a sharper upper bound for $N_K(D_{L/K})$.

*Acknowledgements.* We thank Professor Marc Hindry for interesting discussions and the referee for helpful comments.

# References

[1] C. Chabauty, Démonstration de quelques lemmes de rehaussement, *C. R. Acad. Sci. Paris* 217, (1943) 413-415.

[2] C. Chevalley, Un théorème d' arithmétique sur les courbes algébriques, *C. R. Acad. Sci. Paris* 195 (1932), 570-572.

[3] K. R. Coobes and D. R. Grant, On the heterogenous Spaces, *J. London Math. Soc.* 40 (1989), 385-397.

[4] M. Hindry - J. Silverman, *Diophantine Geometry*, New-York Inc.: Springer-Verlag 2000.

[5] D. Kubert - S. Lang, Units in the Modular Function Field. I, *Math. Ann.* 218 (1975), 67-96.

[6] S. Lang, *Elliptic Curves. Diophantine Analysis,* Springer Verlag 1978.

[7] S. Lang, *Diophantine Geometry,* Springer Verlag 1983.

[8] S. Lang, *Algebra* (2nd edition), Addison-Wesley, 1984.

[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Springer and PWN 1990.

[10] D. Poulakis, Estimation effective de points entiers d' une famille de courbes algébriques, *Ann. Fac. Sci. Toulouse,* Vol. V, no 4 (1996), 691-725.

[11] D. Poulakis, Polynomial bounds for the solutions of a class of Diophantine equations, *J. Number Theory*, 66, 2 (1997), 271-281.

[12] D. Poulakis, Bounds for the size of integral solutions to $Y^m = f(X)$, *Proc. Edinburg Math. Soc.,* 42 (1999), 127-141.

[13] W. M. Schmidt, Construction and estimation of bases in function fields, *J. Number Theory* 39, 2, (1991), 181-224.

[14] J. P. Serre, *Lectures on the Mordell-Weil Theorem,* Vieweg 1989.

[15] I. Shafarevich, *Basic Algebraic Geometry*, Berlin-Heidelberg-New York: Springer Verlag 1977.

[16] B. Shiffman, Degree bounds for the division problem in polynomial ideals, *Michigan Math. J.* 36 (1989), 163-171.

[17] J. H. Silverman, *The arithmetic of elliptic curves,* Springer Verlag 1986.

[18] A. Weil, Arithmétique et géométrie sur les variétés algébriques, *Act. Sci. et Ind.* No 206, Paris: Hermann 1935.

Aristotle University of Thessaloniki,
Department of Mathematics,
54124 Thessaloniki, Greece
D. Poulakis e.mail: poulakis@math.auth.gr
K. Draziotis e.mail: drazioti@math.auth.gr