An Effective Version of Chevalley-Weil Theorem for Projective Plane Curves

Konstantinos Draziotis and Dimitrios Poulakis

Abstract

We obtain a quantitative version of the classical Chevalley-Weil theorem for curves. Let \( \phi: \tilde{C} \to C \) be an unramified morphism of non-singular plane projective curves defined over a number field \( K \). We calculate an effective upper bound for the norm of the relative discriminant of the number field \( K(Q) \) over \( K \) for any point \( P \in C(K) \) and \( Q \in \phi^{-1}(P) \).

1 Introduction

Let \( \phi: V \to W \) be an unramified covering of projective normal varieties defined over a number field \( K \). By the classical theorem of Chevalley-Weil [2, 10, 3, Theorem 8.1, page 45], [4, page 292], there exists a finite extension \( L/K \) such that \( \phi^{-1}(W(K)) \subseteq V(L) \). In [3, Theorem 1.1], we obtained a quantitative version of the Chevalley-Weil theorem in case where \( \phi: \tilde{C} \to C \) is an unramified morphism of non-singular affine plane curves defined over \( K \). More precisely, we gave, following a new approach, an effective upper bound for the relative discriminant of the minimal field of definition \( K(Q) \) of \( Q \) over \( K \) for any integral point \( P \in C(K) \) and \( Q \in \phi^{-1}(P) \). In this paper, we consider the case where \( \phi: \tilde{C} \to C \) is an unramified morphism of non-singular projective plane curves defined over \( K \) and we obtain, extending our method, an effective upper bound for the relative discriminant of \( K(Q) \) over \( K \) for any \( P \in C(K) \) and \( Q \in \phi^{-1}(P) \).

Consider the set of absolute values on \( \mathbb{Q} \) consisting of the ordinary absolute value and for every prime \( p \) the \( p \)-adic absolute value \( |\cdot|_p \) with \( |p|_p = p^{-1} \). Let \( M(K) \) be a set of symbols \( v \) such that with every \( v \in M(K) \) there is precisely one associated absolute value \( |\cdot|_v \) on \( K \) which extends one of the above absolute values of \( \mathbb{Q} \). We denote by \( d_v \) its local degree. Let \( x = (x_0: \ldots: x_n) \) be a point of the projective space \( \mathbb{P}^n(K) \) over \( K \). We define the field height \( H_K(x) \) of \( x \) by

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

Let \( d \) be the degree of \( K \). We define the absolute height \( H(x) \) by \( H(x) = H_K(x)^{1/d} \). 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 \( G \). For an account of the properties of heights see [3, chapter VIII] or [5, chapter 3].
Let $\overline{K}$ be an algebraic closure of $K$ and $O_K$ the ring of algebraic integers of $K$. If $M$ is a finite extension of $K$, then we denote by $D_{M/K}$ the relative discriminant of the extension $M/K$ and by $N_M$ the norm from $M$ to $Q$.

Let $F, \overline{F} \in K[X_1, X_2, X_3]$ be two homogeneous absolute irreducible polynomials with $N = \deg F > 1$ and $\overline{N} = \deg \overline{F} > 1$. We denote by $C$ and $\overline{C}$ the projective curves defined by $F(X_1, X_2, X_3) = 0$ and $\overline{F}(X_1, X_2, X_3) = 0$ respectively. Let $\phi : C \to \overline{C}$ be a nonconstant morphism of degree $m > 1$ defined by $\phi(X_1, X_2, X_3) = (\phi_1(X_1, X_2, X_3), \phi_2(X_1, X_2, X_3), \phi_3(X_1, X_2, X_3))$, where $\phi_i(X_1, X_2, X_3)$ $(i = 1, 2, 3)$ are relatively prime homogeneous polynomials in $K[X_1, X_2, X_3]$ of the same degree $M$. Let $\Phi$ be a point in the projective space having as coordinates the coefficients of $\phi_i$ $(i = 1, 2, 3)$.

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

$$N_K(D_{K(Q)/K}) < \Omega(H(F)^{6N^2\overline{N}}H(\Phi_1)^{\overline{N}}H(\overline{F})^M)^{\omega/dm^3M^7N^{30}\overline{N}^{13}},$$

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

**Remarks.** 1) By [3] Corollary 3, p. 120, the curve $\overline{C}$ is nonsingular.
2) Since $m > 1$, the quantity $M$ is $> 1$.
3) By Hurwitz’s formula, $\overline{C}$ and $C$ have positive genus and $\overline{N} > N > 3$.
4) Since $\overline{F}(X, Y, Z)$ divides $F(\phi_1(X, Y, Z), \phi_2(X, Y, Z), \phi_3(X, Y, Z))$, $H(\overline{F})$ and $\overline{N}$ can be bounded by constants depending only on $\overline{F}$ and $\phi$.

Let $K(C)$ and $K(\overline{C})$ be the function fields of $C$ and $\overline{C}$, respectively, over $K$, $P = (p_1: p_2: p_3)$ and $\phi^* : K(C) \to K(\overline{C})$ the field homomorphism associated to $\phi$. We denote by $\phi_{j,i}$ the function on $\overline{C}$ defined by the fraction $\phi_j/\phi_i$. The idea of the proof of Theorem 1 is as follows. For every affine view $C_i$, with $X_i = 1$ $(i = 1, 2, 3)$, of $C$ we construct two primitive elements $u_{is}$ $(s = 1, 2)$ for the field extension $K(\overline{C})/\phi^*(K(C))$ which are integral over the ring $K[\phi_{j,i}, \phi_{k,i}]$ and such that $K(u_{is}(Q)) = K(Q)$. Further, we construct polynomials $P_{is}(X, Y, U)$ $(s = 1, 2)$ representing the minimal polynomials of $u_{is}$ over $K[\phi_{j,i}, \phi_{k,i}]$ such that the discriminants $D_{is}(X, Y)$ of $P_{is}(X, Y, U)$ $(s = 1, 2)$ have no common zero on $C_i$. It follows that for every prime ideal $\mathfrak{p}$ of $O_K$ with quite large norm there is $i \in \{1, 2, 3\}$ such that $\mathfrak{p}$ cannot divide both $D_{is}(p_1/p_i, p_2/p_i)$ $(s = 1, 2)$ and hence cannot divide the discriminant of $K(Q)$. Thus, we determine the prime ideals of $K$ which are ramified in $K(Q)$ and the result follows. A totally different effective approach of Chevalley-Weil theorem is given in [1] Chapter 4.

The paper is organized as follows. In section 2 we give some auxiliary results and in section 3 we obtain the proof of Theorem 1.

**Notations.** If $C$ is a projective plane curve defined over $\overline{K}$, then we denote by $O(U)$ the ring of regular functions on an open subset $U$ of $C$ and by $\overline{K}(C)$ the function field of $C$. Let $G$ be a homogeneous polynomial of $\overline{K}[X_1, X_2, X_3]$. We denote by $D_{C}(G)$ and $V_{C}(G)$ the set of points $P \in C(\overline{K})$ with $G(P) \neq 0$ and $G(P) = 0$ respectively. Finally, throughout the paper, we denote by $A_1(a_1, \ldots, a_s), A_2(a_1, \ldots, a_s), \ldots$ effectively computable positive numbers in terms of indicated parameters.
2 Auxiliary Results

We keep the notations and the assertions of the Introduction. The restriction of \( \phi \) on \( \phi^{-1}(D_C(X_i)) \) is a finite morphism. Thus, the associated ring homomorphism \( \phi^* : O(DC(X_i)) \to O(\phi^{-1}(DC(X_i))) \), defined by \( \phi^*(f) = f \circ \phi \), for every \( f \in O(DC(X_i)) \), is surjective and the ring \( O(\phi^{-1}(DC(X_i))) \) is finite over \( \phi^*(O(DC(X_i))) \). We denote by \( x_{j,i} \) and \( x_{j,i} \) the functions defined by \( X_j/X_i \) on \( \bar{C} \) and \( C \), respectively. The function \( \phi^*(x_{j,i}) \) is defined by the fraction \( \phi_j/\phi_i \) and so \( \phi_j = \phi^*(x_{j,i}) \). Then we have \( \phi^*(O(DC(X_i))) = \mathcal{K}[\phi_j, \phi_k, i] \). Let \( \rho \) be an integer such that for every \( (z_1 : z_2 : z_3) \in V_C(X_i) \) we have \( z_k + \rho z_j \neq 0 \), where \( \{i, j, k\} = \{1, 2, 3\} \) with \( j < k \). Thus, the poles of the function \( u = x_{k,i} + \rho x_{j,i} \) are the points of \( V_C(X_i) \). Put \( \Pi_i = \phi^{-1}(DC(X_i)) \cap V_C(X_i) \).

**Proposition 1** There is a monic polynomial \( f(T) \in K[T] \) such that the function \( \bar{u} = uf(\phi_j, i) \) is integral over \( K[\phi_j, i, \phi_k, i] \). We have \( \deg f \leq \bar{N} \),

\[
H(f) < A_1(\rho, M, N, \bar{N})H(F)^{\bar{N}}H(\bar{F})^{MN}H(\bar{F})^{\bar{N}},
\]

and the roots of \( f(T) \) are the elements \( \phi_j, i, i \)(\( R \)), where \( R \in \Pi_i \). Moreover, there is a polynomial of \( K[X_j, X_k] \),

\[
P(X_j, X_k, U) = U^\mu + p_1(X_j, X_k)U^{\mu-1} + \cdots + p_\mu(X_j, X_k),
\]

such that \( P(\phi_j, i, \phi_k, i, U) \) is the minimal polynomial of \( \bar{u} \) over \( K[\phi_j, i, \phi_k, i] \). We have \( \mu \leq m \), \( \deg p_l < 11MN^4N^2 \) \( (l = 1, \ldots, \mu) \) and

\[
H(P) < A_2(\rho, M, N, \bar{N})H(\bar{F})^{6N^2\bar{N}}H(\bar{F})^{\bar{N}}H(\bar{F})^{240mM^3N^3N^{12}\bar{N}}.
\]

For the proof of Proposition 1 we shall need the following lemma.

**Lemma 1** There is a polynomial \( G(W, X, U) \in K[W, X, U] \setminus \{0\} \) such that \( G(\rho, \phi_j, i, u) = 0 \). We have \( \deg_X G \leq NN \), \( \deg_U G \leq 2MNN \), \( \deg_W G \leq 2MN\bar{N} \) and the polynomial \( G_\rho(X, U) = G(\rho, X, U) \) satisfies

\[
H(G_\rho) < A_3(\rho, M, N, \bar{N})H(F)^{\bar{N}}H(\bar{F})^{MN}H(\bar{F})^{\bar{N}}.
\]

**Proof.** We may suppose, without loss of generality, that \( j = 1, k = 2 \) and \( i = 3 \). Consider the polynomials \( \bar{F}_1(W, V, U) = \bar{F}(V, U - WV, 1) \) and

\[
E(W, X, V, U) = F(X\phi_3(V, U - WV, 1), \phi_2(V, U - WV, 1), \phi_3(V, U - WV, 1)).
\]

We have \( \bar{F}_1(\rho, \bar{x}_{1,3}, u) = \bar{F}(\rho, \phi_{1,3}, \bar{x}_{1,3}, u, \rho) = 0 \). If \( G(W, X, U) \) is the resultant of \( E(W, X, V, U) \) and \( \bar{F}_1(W, V, U) \) with respect to \( V \), then \( G(\rho, \phi_{1,3}, u) = 0 \).

Suppose that \( G(W, X, U) \) is equal to zero. Thus, since \( \bar{F}_1(W, V, U) \) is absolutely irreducible, \( \bar{F}_1(W, V, U) \) divides \( E(W, X, V, U) \). It follows that \( \bar{F}(V, U, 1) \) divides \( F(X\phi_3(V, U, 1), \phi_2(V, U, 1), \phi_3(V, U, 1)) \). Write

\[
F(X_1, X_2, X_3) = A_0(X_2, X_3)X_1^n + \cdots + A_n(X_2, X_3),
\]

where \( A_i(X_2, X_3) \) \( (i = 0, \ldots, n) \) are homogeneous polynomials with \( \deg A_i = N - n + i \). If \( P = (p_1 : p_2 : 1) \in D_C(\phi_3) \), then

\[
A_0(\phi_{2,3}(P), 1)(X_1/\phi_3(P))^n + \cdots + A_n(\phi_{2,3}(P), 1) = 0.
\]
It follows that \( A_j(\phi_{2,3}(P), 1) = 0 \) \((j = 0, \ldots, n)\) which is a contradiction since \( F(X_1, X_2, X_3) \) is absolutely irreducible. Thus \( G(W, X, U) \) is not zero.

By [3] Lemma 4.2, we have \( \deg_X G \leq N \tilde{N}, \deg_U G \leq 2MN \tilde{N} \), and \( \deg_W G \leq 2MN \tilde{N} \). Further, if \( G_p(X, U) = G(\rho, X, U) \), \( E_p(X, V, U) = E(\rho, X, V, U) \) and \( \tilde{F}_p(V, U) = \tilde{F}(\rho, V, U) \), then

\[
H(G_p) < \Lambda_4(M, N, \tilde{N}) H(E_p)^N H(\tilde{F}_p)^MN. 
\]

By [3] Lemma 4.4, we obtain

\[
H(\tilde{F}_p) < 2^N(\tilde{N} + 1) \max\{1, |\rho|\}^\tilde{N} H(\tilde{F}).
\]

Next, put \( \varphi_{\rho,l}(V, U) = \phi_l(V, U - \rho V) \) \((l = 1, 2)\). By [4] Lemma B.7.4, for every absolute value \(| \cdot |_v\) of \( K \),

\[
|E_p|_v \leq \max\{1, |2N|_v^2\}|F|_v \max_{0 \leq j \leq N} \{|\varphi_{\rho,2}^j|_v|\varphi_{\rho,3}^{N-j}|_v\}
\]

and for every positive number \( k \),

\[
|\varphi_{\rho,l}|_v \leq \max\{1, |2M|_v^2\}^k|\varphi_{\rho,l}|_v.
\]

Furthermore, the proof of [3] Lemma 4.4 gives

\[
|\varphi_{\rho,l}|_v \leq \max\{1, |\rho|_v\}^M \max\{1, |2|_v^2\}^M \max\{1, |M + 1|_v\} |\phi_l|_v, \quad (l = 1, 2).
\]

The above inequalities yield

\[
H(E_p) < \Lambda_5(\rho, M, N, \tilde{N}) H(F) H(\Phi)^N.
\]

Combining all theses estimates, the bound for \( H(G_p) \) follows.

**Proof of Proposition 1.** ByLemma 1, there is \( G_p(X, U) \in K[X, U] \) such that \( G_p(\phi_{j,i}, u) = 0 \). Write \( G_p(X, U) = g_0(X)U^\nu + \cdots + g_\nu(X) \). Thus, \( u g_0(\phi_{j,i}) \) is an integral element over \( K[\phi_{j,i}, \phi_{k,i}] \) and so \( u g_0(\phi_{j,i}) \in O(\phi^{-1}(D_C(X_i))) \).

If \( h \in \overline{K}(C) \) and \( S \in \tilde{C} \), then we denote by \( \text{ord}_S(h) \) the order of \( h \) at \( S \). Put \( B_R = \phi_{j,i}(R) \), where \( R \in \Pi_i \). Let \( m_R \) be the smallest integer such that \( (\phi_{j,i} - B_R)^{m_R} u \) is defined at \( R \). Then \( m_R \leq |\text{ord}_R(\phi)| \). Set \( f(X) = \prod_{R \in \Pi_i} (X - B_R)^{m_R} \). We have \( u f(\phi_{j,i}) \in O(\phi^{-1}(D_C(X_i))) \) and since \( |\overline{K}(C) : K(u)| = \tilde{N} \), we obtain \( \deg f = \sum_{R \in \Pi_i} m_R \leq \tilde{N} \). The elements of the Galois group \( \text{Gal}(\overline{K}/K) \) permute the elements of \( \Pi_i \) and consequently the numbers \( B_R \).

For every \( \sigma \in \text{Gal}(\overline{K}/K) \), we have \( \text{ord}_R(\phi_{j,i} - B_R) = \text{ord}_{R^\sigma}(\phi_{j,i} - B_{R^\sigma}) \) and \( \text{ord}_R(u) = \text{ord}_{R^\sigma}(u) \). It follows that \( m_R = m_{R^\sigma} \). Hence \( f(X) \in K[X] \). Since \( u g_0(\phi_{j,i}) \in O(\phi^{-1}(D_C(X_i))) \), we have \( g_0(X) = f(X)l(X) \), where \( l(X) \in K[X] \).

By [3] Proposition B.7.3, \( H(f) \leq e^{N \tilde{N}} H(G_p) \). The bound for \( H(f) \) follows.

Consider the polynomial

\[
\tilde{G}_p(X, U) = l(X)U^\nu + q_1(X)U^\nu-1 + q_2(X)f(X)U^\nu-1 + \cdots + q_\nu(X)f(X)^\nu-1.
\]

We have \( \tilde{G}_p(\phi_{j,i}, u f(\phi_{j,i}) = 0 \). The estimates for \( G_p(X, U) \) and [4] Proposition B.7.4] yield

\[
H(\tilde{G}_p) < \Lambda_7(\rho, M, N, \tilde{N}) H(F)^N H(\tilde{F})^{MN} H(\Phi)^{N \tilde{N}} 2^{MN \tilde{N}}.
\]

Using [3] Proposition 2.1] and the estimates for \( \tilde{G}_p \), we obtain the existence of polynomial \( P(X_j, X_k, U) \in K[X_j, X_k, U] \) having the required properties.
Lemma 2 Let \( P \in C(K) \) and \( Q \in C(\overline{K}) \) with \( \phi(Q) = P \). Then

\[
N_K(D_{K(Q)/K}) < (e^3(M + \bar{N}))^{dM\bar{N}}(H_K(P)H_K(\Phi))^{\bar{N}}H_K(F)^{M\bar{N}}^M.
\]

Proof. We may suppose, without loss of generality, that \( Q = (q_1 : q_2 : 1) \) and \( P = (p_1 : p_2 : 1) \). Put \( G_1(X_1, U, V) = X_1\phi_3(U, V, 1) - \phi_1(U, V, 1) \). Then \( G_1(p_1, q_1, q_2) = 0 \). We denote by \( R_1(U) \) and \( R_2(V) \) the resultants of \( F(U, V, 1) \) and \( \Gamma(U, V) = G_1(p_1, U, V) \) with respect to \( V \) and \( U \). Then \( R_1(q_1) = R_2(q_2) = 0 \). By [3, Lemma 4.2] and [4, Proposition B.7.4(b)] we obtain

\[
H(R_i) \leq (M + \bar{N})!(\bar{N} + 1)^M(M + 1)^{\bar{N}}(2H(p_1)H(\Phi))^{\bar{N}}H(F)^M.
\]

Furthermore, we have \( \deg R_i \leq 2M\bar{N} \).

Let \( B_i(T) = T^{m_i} + b_1T^{m_i-1} + \cdots + b_{m_i} \), where \( m_i \leq 2M\bar{N} \), be the irreducible polynomial of \( q_i \) over \( K \). By [3] Lemma 4.1 there is a positive integer \( \beta_i \) with \( \beta_i \leq H_K(B_i)^{m_i} \) such that \( \beta_i b_1 \cdots b_{m_i} \in O_K \). Then \( \beta_i q_i \) is an algebraic integer with minimal polynomial \( B_i(T) = T^{m_i} + \beta b_1 T^{m_i-1} + \cdots + \beta b_{m_i} \). Using [4, Proposition B.7.3] we obtain

\[
H(B_i) \leq H(B_i)\beta_i^{m_i} \leq (e^{2M\bar{N}}H(R_i))^{1+2dM\bar{N}}.
\]

Let \( \Delta(B_i) \) be the discriminant of \( B_i(T) \). By [8] Lemma 5, we have

\[
N_K(\Delta(B_i)) \leq H_K(\Delta(B_i)) \leq m_i^{3dM\bar{N}}H_K(B_i)^{2m_i-2} \leq (e^{2dM\bar{N}}H_K(R_i))^{9dM^2\bar{N}^2}.
\]

Put \( K_i = K(q_i) \). Since \( b_i q_i \) is an algebraic integer, the discriminant \( D_i \) of the extension \( K_i/K \) divides the discriminant of \( 1, b_i q_i, \ldots, (b_i q_i)^{m_i-1} \) which is equal to \( \Delta(B_i) \). Thus \( N_K(D_i) \leq |N_K(\Delta(B_i))| \). If \( I(T) \) is the irreducible polynomial of \( b_2 q_2 \) over \( K_1 \), then \( I(T) \) divides \( B_2(T) \) (in \( K_1[T] \)) and so the discriminant \( \Delta(I) \) of \( I(T) \) divides \( \Delta(B_2) \). Hence, \( D_{K(Q)/K_i} \) divides \( \Delta(B_2) \). Thus,

\[
N_K(D_{K(Q)/K}) \leq N_K(D_1)^{2M\bar{N}}N_K(D_{K(Q)/K_1}) \leq (N_K(\Delta(B_1))N_K(\Delta(B_2))^2M\bar{N}.
\]

Using the upper bounds for \( N_K(\Delta(B_i)) \) and \( H_K(R_i) \), the result follows.

3 Proof of Theorem 1

Let \( P = (a_1 : a_2 : a_3) \), \( Q \in \phi^{-1}(P) \) and \( L = K(Q) \). If \( a_j = 0 \) for some \( j \in \{1, 2, 3\} \), then [7, Lemma 4] gives \( H(P) < 2H(F) \). So Lemma 2 yields a sharper bound for \( N_K(D_{L/K}) \) than that of Theorem 1. Thus, we may suppose that \( a_j \neq 0 \) (\( j = 1, 2, 3 \)).

Let \( \Theta_i \) be the set of \( \rho \in \mathbb{Z} \) such that for every \( (z_1 : z_2 : z_3) \in V_C(X_i) \) we have \( z_k + \rho z_j = 0 \), where \( \{i, j, k\} = \{1, 2, 3\} \) with \( j < k \). Set \( u_{\rho,i} = \bar{x}_{k,i} + \rho \bar{x}_{j,i} \), where \( \rho \notin \Theta_i \). By Proposition 1, there is a monic polynomial \( f_i \in K[T] \) such that the function \( \tilde{u}_{\rho,i} = u_{\rho,i}f_i(\phi_{j,i}) \) is integral over \( K[\phi_{j,i}, \phi_{k,i}] \), \( \deg f_i \leq \bar{N} \), the roots of \( f_i \) are the elements \( \phi_{j,i}(R) \), where \( R \in \phi^{-1}(D_{C(X_i)}) \cap V_C(X_i) \) and

\[
H(f) < \Lambda_1(\rho, M, N, \bar{N})H(F)^{\bar{N}}H(F)^{MN}H(\Phi)^{N\bar{N}}.
\]

Moreover, there is a polynomial of \( K[X_j, X_k, U] \),

\[
P_{\rho,i}(X_j, X_k, U) = U^\mu + p_{\rho,i,1}(X_j, X_k)U^{\mu-1} + \cdots + p_{\rho,i,\mu}(X_j, X_k),
\]

where
such that $P_{\rho,i}(\phi_{j,i}, \phi_{k,i}, U)$ is the minimal polynomial of $\tilde{u}_{\rho,i}$ over $K[\phi_{j,i}, \phi_{k,i}]$. We have $\mu \leq m$, $\deg p_{\rho,i} < 11MN^2N^2$ ($l = 1, \ldots, \mu$), and

$$H(P) < A_2(\rho, m, N, N\tilde{N})(H(F))^6N^2\tilde{N}H(\Phi)^{\tilde{N}}H(\tilde{F})^M240mM^3N^4N^2\tilde{N}^2.$$ 

Suppose that there is $i \in \{1, 2, 3\}$ such that $f_i(a_j/a_i) = 0$. By [7, Lemma 4] and [6, Lemma 7], we have

$$H(P) \leq H(a_j/a_i)H(a_k/a_i) \leq 2(N + 1)H(F)(2H(f_i))^{N+1}.$$ 

Using the bound for $H(f_i)$, Lemma 2 gives a sharper bound for $N_K(DL/R)$ than that of Theorem 1. Next, suppose that for every $i = 1, 2, 3$ we have $f_i(a_j/a_i) \neq 0$ and so $u_{\rho,i}$ is defined at $Q$.

The monomorphism $\phi^* : O(D_C(X_i)) \to O(\phi^{-1}(D_C(X_i)))$ extends to a field homomorphism $\phi^* : \overline{K}(C) \to \overline{K}(C)$. We have $\phi^*(\overline{K}(C)) = \overline{K}(\phi_{j,i}, \phi_{k,i})$. If $\sigma_1, \ldots, \sigma_m$ are all the $\overline{K}(C)$-embeddings of $\phi^*(\overline{K}(C))$ into an algebraic closure of $\phi^*(\overline{K}(C))$, then we denote by $\Gamma_i$ the set of integers $\rho \notin \Theta_i$ with $\sigma_\rho(\tilde{u}_{\rho,i}) \neq \sigma_i(\tilde{u}_{\rho,i})$ for $p \neq q$. For every $\rho \in \Gamma_i$, we have $\overline{K}(C) = \phi^*(\overline{K}(C))(\tilde{u}_{\rho,i})$ and so $m = \mu$. Note that at most $m(m - 1)/2 + \tilde{N}$ integers $\rho$ do not lie in $\Gamma_i$. Further, there are at most $m(m - 1)/2 + \tilde{N}$ integers $\rho$ such that $K(u_{\rho,i}(Q)) \neq K(Q)$. Hence, there is $r(i) \in \mathbb{Z}$ with $r(i) \in \Gamma_i$ and $|r(i)| \leq \tilde{N} + m^2/2$ such that $K(u_{r(i),i}(Q)) = K(Q)$.

Putting $X_i = 1$ in $F(X_1, X_2, X_3)$ we obtain $F_i(X_j, X_k)$ with $j < k$. Let $D_{\rho,i}(X_j, X_k)$ be the discriminant of $P_{\rho,i}(X_j, X_k, U)$ with respect to $U$. We have $\deg D_{\rho,i} < (11(2m - 1))M^2N^4$. Since $P_{\rho,i}(\phi_{j,i}, \phi_{k,i}, U)$ is irreducible, $F_i$ does not divide $D_{\rho,i}$. We denote by $J_{r(i),i}$ the set of points $(z_1 : z_2 : z_3) \in D_C(X_i)$ with $z_i = 1$ and $D_{r(i),j}(z_j, z_k) = 0$. By Bézout’s theorem, $|J_{r(i),i}| < 11(2m - 1)M^2N^4N^2$. Thus, if $B_i = J_{r(i),i} \cup \{P\}$, then there is an integer $s(i)$ with $|s(i)| \leq 11m^2N^2N^5M$ such that $B_i = \phi(V_{C}(X_k + s(i)X_j)) = 0$.

We denote by $\tilde{F}_i(Y_1, Y_2, Y_3)$ and $\phi_{i,1}(Y_1, Y_2, Y_3)$ the polynomials obtained from $\tilde{F}(X_1, X_2, X_3)$ and $\phi_1(X_1, X_2, X_3)$, respectively, using the projective change of coordinates $\chi$ defined by $Y_j = X_j, Y_k = X_j, Y_i = X_k = s(i)X_j$. Set $\tilde{Q} = \phi(Q)$. Let $\tilde{C}_i$ be the curve defined by $\tilde{F}_i(Y_1, Y_2, Y_3) = 0$. The morphism $\psi_i : \tilde{C}_i \to C$, defined by $\psi_i(Y_1, Y_2, Y_3) = (\psi_{i,1}(Y_1, Y_2, Y_3), \psi_{i,2}(Y_1, Y_2, Y_3), \psi_{i,3}(Y_1, Y_2, Y_3))$, is unramified of degree $m$. We denote by $\Psi_i$ a point in the projective space with coordinates the coefficients of $\psi_{i,s}$ ($s = 1, 2, 3$).

Let $y_{j,i}$ be the function defined by $Y_j/Y_i$ on $\tilde{C}_i$. We set $v_{\tau,i} = \tau y_{j,i} + y_{k,i}$, where $\{i, j, k\} = \{1, 2, 3\}, j < k$ and $\tau \in \mathbb{Z}$. Further, we denote by $\psi_{j,i,k}$ the function defined on $\tilde{C}_i$ by the fraction $\psi_{i,j}/\psi_{i,k}$. By Proposition 1, there is a monic polynomial $g_i(T) \in K[T]$ such that the function $v_{\tau,i} = g_i(\psi_{i,j,i}, \psi_{i,k,i})$ is integral over $K[\psi_{i,j,i}, \psi_{i,k,i}]$, deg $g_i \leq \tilde{N}$ and

$$H(g_i) < A_1(\rho, m, N, \tilde{N})H(F)^{\tilde{N}}H(\tilde{F})^MNH(\Psi_i)^{\tilde{N}}.$$ 

The zeros of $g_i(T)$ are the elements $\psi_{i,j,i}(R)$, where $R \in \psi_{i,j,i}^{-1}(D_C(X_i)) \cap V_{\tilde{C}_i}(Y_i)$. Moreover, there is $\Pi_{\tau,i}(X_j, X_k, U) \in K[X_j, X_k, U]$ such that $\Pi_{\tau,i}(\psi_{i,j,i}, \psi_{i,k,i}, U)$ is the minimal polynomial of $\bar{v}_{\tau,i}$ over the ring $K[\psi_{i,j,i}, \psi_{i,k,i}]$. Write

$$\Pi_{\tau,i}(X_j, X_k, U) = U^{\nu} + \pi_{\tau,i,1}(X_j, X_k)U^{\nu-1} + \cdots + \pi_{\tau,i,\nu}(X_j, X_k).$$

We have $\nu \leq m$, $\deg \pi_{\tau,i,1} < 11MN^4\tilde{N}^2$ ($l = 1, \ldots, \nu$) and

$$H(\Pi_{\tau,i}) < A_2(\tau, m, N, \tilde{N})(H(F)^{6N^2\tilde{N}}H(\Psi_i)^{\tilde{N}}H(\tilde{F})^M240mM^3N^4\tilde{N}^2).$$
By [3] Lemma 4.4, $H(\bar{F}_i) < \Lambda_0(\bar{N}, s(i))H(\bar{F})$ and $H(\Psi_i) < \Lambda_0(M, s(i))H(\Psi)$. It follows that $H(g_i)$ and $H(\Pi_{\tau,i})$ satisfy inequalities as above having $H(\bar{F}_i)$ and $H(\Psi_i)$ in place of $H(\bar{F})$ and $H(\Psi_i)$ respectively.

The points $(z_1 : z_2 : z_3) \in D_{\tau}(X_i)$ with $z_i = 1$ and $g_i(z_j) = 0$ belong to $\phi(V_C(X_k + s(i)X_j))$. On the other hand, $P \in B_i$ and $B_i \cap \phi(V_C(X_k + s(i)X_j)) = \emptyset$. Hence, $g_i(a_j/a_i) \neq 0$ and so $v_{\tau,i}$ is defined at $Q (i = 1, 2, 3)$.

Let $\psi_i^* : \mathcal{K}(C) \to \mathcal{K}(\bar{C}_i)$ be the field homomorphism associated to the morphism $\psi_i$. As previously, there is a set $\Delta_i \subset \mathbb{Z}$ with $|\Delta_i| \leq m(m-1)/2 + N$ such that for every integer $\tau \notin \Delta_i$ we have $\mathcal{K}(\bar{C}_i) = \psi_i^*(\mathcal{K}(C))(\bar{v}_{\tau,i})$ (so $\nu = m$) and $K(v_{\tau,i}(Q)) = K(Q)$.

Let $\Sigma_{\tau,i}(X_j, X_k)$ be the discriminant of $\Pi_{\tau,i}(X_j, X_k, U)$ with respect to $U$. We have $deg \Sigma_{\tau,i} \leq (2m-1)11N^2N^4M$. We denote by $\Xi_i$ the set of points $(z_1 : z_2 : z_3) \in D_{\tau}(X_i)$ with $z_i = 1$, $D_{\tau(i),j}(z_j, z_k) = 0$ and $\Sigma_{\tau,i}(z_j, z_k) = 0$, for every $\tau \in \Delta_i$. Suppose that $(z_1 : z_2 : z_3) \in \Xi_i$ with $z_i = 1$. Then, for every $\tau \in \Xi_i$, $\Pi_{\tau,i}(z_j, z_k, U)$ has at most $m - 1$ distinct roots. If $g_i(z_j) \neq 0$, then there are $m$ distinct points $Q_t \in \phi_i^{-1}(z_1 : z_2 : z_3)$ ($t = 1, \ldots, m$) and $\tau_0 \in \mathbb{Z}$ such that $\bar{v}_{\tau_0,i}(Q_p) \neq \bar{v}_{\tau_0,i}(Q_q)$ for $p \neq q$. Thus, $\Pi_{\tau_0,i}(z_j, z_k, U)$ has $m$ distinct roots which is a contradiction. Hence $g_i(z_j) = 0$. Then $(z_1 : z_2 : z_3) \in \phi(V_C(X_k + s(i)X_j) \cap B_i = 0$ which is a contradiction. So, for every $(z_j, z_k) \in \mathcal{K}^2$ with $D_{\tau(i),j}(z_j, z_k) = F_i(z_j, z_k) = 0$, the polynomial in $\tau$, $\Sigma_{\tau,i}(z_j, z_k)$, is not zero.

Since $\bar{v}_{\tau,i}$ is a root of $\Pi_{\tau,i}(\psi_{i,j,i}, \psi_{i,k,i}, U)$, $\pi_{\tau,i}(\psi_{i,j,i}, \psi_{i,k,i})$, as polynomial in $\tau$, has degree at most $l$. Hence, the degree in $\tau$ of $\Sigma_{\tau,i}(\psi_{i,j,i}, \psi_{i,k,i})$ is at most $(2m - 1)m$. So, for every $(z_1, z_2, z_3) \in J_{\tau(i),i}$ with $z_i = 1$ there are at most $(2m-1)m$ integers $\tau$, such that $\Sigma_{\tau,i}(z_j, z_k) = 0$. Thus, there is $\tau(i) \in \mathbb{Z}$ with $|\tau(i)| < 22m^3MN^2N^5$, such that $\mathcal{K}(\bar{C}_i) = \psi_i^*(\mathcal{K}(C))(\bar{v}_{\tau(i),i})$ (so $\nu = m$), $K(v_{\tau(i),i}(Q)) = K(Q)$ and for every $(z_1, z_2, z_3) \in J_{\tau(i),i}$, with $z_i = 1$ we have $\Sigma_{\tau(i),i}(z_j, z_k) \neq 0$.

Let $D_{\rho,i}^1$ and $\Sigma_{\tau,i}^1$ be two points in the projective space having as coordinates and the coefficients of $D_{\rho,i}(X_j, X_k)$ and $\Sigma_{\tau,i}(X_j, X_k)$, respectively. By [3] Lemma 4.2, we have

$$H(D_{\rho,i}^1) < m^{3m-1}(11MN^4\bar{N}^2)^{4m-2}H(P_{\rho,i})^{2m-1},$$
$$H(\Sigma_{\tau,i}^1) < m^{3m-1}(11MN^4\bar{N}^2)^{4m-2}H(\Pi_{\tau,i})^{2m-1}.$$  

We may assume, without loss of generality, that one of the coefficients of $F_i$ is 1. By [3] Lemma 4.1, there are positive integers $a_{\rho,i}, b_{\rho,i}, c$ with

$$c \leq H_K(F)^{2N^2}, \quad a_{\rho,i} \leq H_K(P_{\rho,i})^{61mM^2N^4N^8}, \quad b_{\rho,i} \leq H_K(\Pi_{\tau,i})^{61mM^2N^4N^8}$$

such that $a_{\rho,i}P_{\rho,i}(X_j, X_k, U), b_{\rho,i}\Pi_{\tau,i}(X_j, X_k, U)$ and $cF_i(X_j, X_k)$ have all their coefficients in $O_K$. So, $a_{\rho,i}^{2m-2}D_{\rho,i}(X_j, X_k), b_{\rho,i}^{2m-2}\Sigma_{\tau,i}(X_j, X_k) \in O_K[X_j, X_k]$. Since $D_{\tau(i),i}(X_j, X_k), \Sigma_{\tau(i),i}(X_j, X_k)$ and $F_i(X_j, X_k)$ have no common zero, [3] Lemma 2.9 implies that there are $A_{i,s} \in O_K[X_j, X_k]$ ($s = 1, 2, 3$) and $A_i \in O_K \setminus \{0\}$ such that

$$A_{i,1}a_{\tau(i),i}^{2m-1}D_{\tau(i),i} + A_{i,2}b_{\tau(i),i}^{2m-1}\Sigma_{\tau(i),i} + A_{i,3}cF_i = A_i.$$  

Furthermore, for every archimedean absolute value $|.|_v$ of $K$ we have

$$|A_i|_v \leq (\delta + 1)(\delta + 2)/2)\|E_i\|_v^{(\delta + 1)(\delta + 2)/2},$$
where $\delta = 11MN^5\bar{N}^2$ and $E_1$ is a point of the projective space with coordinates the coefficients of $a_{r(i),i}^{2m-1} D_{r(i),i}, b_{r(i),i}^{2m-1} \Sigma_{r(i),i}$ and $c F_i$. The bounds for $a_{r(i),i}, b_{r(i),i}, c, H(D_{r(i),i}), H(\Sigma_{r(i),i}), H(P_{r(i),i})$ and $H(\Pi_{r(i),i})$ give

$$|N_K(A_i)| < \Lambda_{11}(d, m, N, N)(H(F)^{6N^2\bar{N}} H(\Phi_i)^N H(F)^M \lambda d m^2 M N^{30} \bar{N}^{13},$$

where $\lambda$ is a numerical constant.

Let $p_i = (a_j/a_i, a_k/a_i)$. Since $D_{r(i),i}(X_j, X_k), \Sigma_{r(i),i}(X_j, X_k)$ and $F_i(X_j, X_k)$ have no common zero, we have either $D_{r(i),i}(p_i) \neq 0$ or $\Sigma_{r(i),i}(p_i) \neq 0$. Let $S$ be the set of prime ideals of $O_K$ dividing $A_1A_2A_3$. Suppose that $\wp$ is a prime ideal of $O_K$ with $\wp \not\in S$. Then there is $i \in \{1, 2, 3\}$ such that $a_j/a_i, a_k/a_i \in O_{K,\wp}$. Put $L = K(Q)$ and $\xi = [L : K]$. We have $L = K(u_{r(i),i}(Q)) = K(\wp_{r(i),i}(\bar{Q}))$. We denote by $O_{K,\wp}$ the local ring at $\wp$, by $\bar{\wp}$ the prime ideal of $O_{K,\wp}$ generated by $\wp$ and by $D_\wp$ the discriminant of the integral closure of $O_{K,\wp}$ into $L$ over $O_{K,\wp}$. Since $\wp$ does not divide $A_i$, it follows that either $a_{r(i),i}^{2m-1} D_{r(i),i}(p_i)$ or $b_{r(i),i}^{2m-1} \Sigma_{r(i),i}(p_i)$ is not divisible by $\bar{\wp}$ (into $O_{K,\wp}$). If $\bar{\wp}$ does not divide $a_{r(i),i}^{2m-1} D_{r(i),i}(p_i)$, then $\bar{\wp}$ does not divide $a_{r(i),i}$ and $a_{r(i),i}^{2m-2} D_{r(i),i}(p_i)$. Thus $a_{r(i),i}$ is a unit in $O_{K,\wp}$ and so $u = u_{r(i),i}(Q)$ is integral over $O_{K,\wp}$. Then $D_\wp$ divides the discriminant $D(1, u, \ldots, u^{\xi-1})$ of $1, u, \ldots, u^{\xi-1}$ into $O_{K,\wp}$. Further, $D(1, u, \ldots, u^{\xi-1})$ divides $a_{r(i),i}^{2m-2} D_{r(i),i}(p_i)$. Since $\wp$ does not divide $a_{r(i),i}^{2m-2} D_{r(i),i}(p_i)$, $\wp$ does not divide $D_{r(i),i}$. Thus, $\wp$ is not ramified into $L$. If $\wp$ does not divide $b_{r(i),i}^{2m-1} \Sigma_{r(i),i}(p_i)$, then we have the same result. By [3] Lemma 4.3,

$$N_K(D_{L/K}) < \prod_{\wp \in S} N_K(\wp)^{m-1} \exp(2m^2 d) \leq N_K(A_1A_2A_3)^{m-1} \exp(2m^2 d).$$

Using the estimates for $N_K(A_i)$, the result follows.

References

[1] Y. Bih, Effective Analysis of Integral Points on Algebraic Curves, Ph. D. Thesis, Beer Sheva, 1993.

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

[3] K. Draziotis and D. Poulakis, An Explicit Chevalley-Weil Theorem for Affine Plane Curves, Rocky Mountain Journal of Mathematics, Rocky Mountain Journal of Mathematics, 39(1) (2009), 49-70.

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

[5] S. Lang, Diophantine Geometry, Springer Verlag 1983.

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

[7] D. Poulakis, Integer points on algebraic curves with exceptional units, J. Austral. Math. Soc. (Series A) 63 (1997), 145-164.
[8] I. Shafarevich, Basic Algebraic Geometry, Berlin-Heidelberg-New York: Springer Verlag 1977.

[9] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag 1986.

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

Dimitrios Poulakis,
Aristotle University of Thessaloniki,
Department of Mathematics,
54124 Thessaloniki, Greece
Email Address: poulakis@math.auth.gr

Konstantinos Draziotis
Kromnis 33
54454 Thessaloniki, Greece
Email Address: drazioti@math.auth.gr