ACTA ARITHMETICA
LXXXVI.1 (1998)

Bounds for the minimal solution of genus zero diophantine equations

by

Dimitrios Poulakis (Thessaloniki)

1. Introduction. In [8], Holzer proved that if the equation $aX^2+bY^2+cZ^2=0$, where $a,b,c\in\mathbb{Z}$, has a non-trivial solution in integers, then a solution (x,y,z) exists with $|x|\le|bc|^{1/2}$, $|y|\le|ac|^{1/2}$, $|z|\le|ab|^{1/2}$. Later, Mordell [12] gave a simple elementary proof of this result. Let K be an algebraic number field. In case where a,b,c are integers of K, Siegel [20] obtained a very sharp estimate for the size of the "smallest" solution of the above equation in integers of K. In this work we generalize these results. Let $F(X,Y)$ be an absolutely irreducible polynomial of $K[X,Y]$ such that the equation $F(X,Y)=0$ defines a curve C of genus 0. Suppose that C has a non-singular point defined over K. Then we calculate an explicit upper bound for the size of the "smallest" non-singular point of C over K. Furthermore, we obtain an effective parametrization of C.

A fundamental result due to Hilbert and Hurwitz [6] says that any curve of genus 0 defined over $\mathbb{Q}$ is birationally equivalent to either a line or a conic. The same result was obtained independently by Poincaré [13]. Furthermore, in [13], Poincaré proved, by another method, that any curve of genus 0 defined over $\mathbb{Q}$ is birationally equivalent to a conic. In Sections 3 and 4 we give an effective proof of these results. In Section 3, we deal with curves of genus 0 defined over K with only ordinary singular points. We prove that every curve of this class is birationally equivalent over K to a conic, giving explicit estimates on the size of the conic, the birational isomorphism and its inverse. In the case where the curve has odd degree we prove that it is birationally equivalent over K to a line giving explicit estimates for the birational isomorphism and its inverse.

A classical result asserts that any curve A is birationally equivalent to a plane curve E with at most ordinary double points as singularities. In Section 4, we give an effective proof of this result for the case of curves of

1991 *Mathematics Subject Classification*: 11G30, 14H25, 11D41.

genus 0 defined over K and we obtain explicit estimates about the size of E, the birational isomorphism and its inverse. Finally, in Section 5, Siegel's estimate for the size of the "smallest" solution of equation $aX^2+bY^2+cZ^2 = 0$ and the results of Sections 3 and 4 imply an upper bound for the size of the "smallest" solution over K of equations defining curves of genus 0 over K. Moreover, these results give an effective parametrization of curves of genus 0. Hence, if we know that a curve of genus 0 defined over K has a non-singular point over K, then we have an effective characterization of all its points over K.

2. Statement of the main results. Let K be an algebraic number field of degree d and of discriminant D_K. 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 $|\cdot|_p$. If $x = p^r a/b$, where a, b are integers not divisible by p, then by definition $|x|_p = p^{-r}$. By an absolute value of K we will always understand an absolute value that extends 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 associated precisely one absolute value $|\cdot|_v$ on K. For every $v \in M(K)$ we denote by K_v the completion of K at v and by d_v the degree of K_v over $\mathbb{Q}_v$. 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

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

and the *absolute height* $H(x)$ by $H(x) = H_K(x)^{1/d}$. Further, for $x \in K$ we define $H_K(x) = H_K((1 : x))$ and $H(x) = H((1 : x))$. Let G be a polynomial in one or several variables and with coefficients in K. We define the *field height* $H_K(G)$ and the *absolute height* $H(G)$ of G to be respectively the field height and the absolute height of the point in a projective space having as coordinates 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 [21, Chap. VIII; 10, Chap. 3].

Let us now state our main results.

THEOREM 2.1. *Let $F(X,Y)$ be an absolutely irreducible polynomial in $K[X,Y]$ of degree $N \geq 3$ such that the curve C defined by the equation $F(X,Y) = 0$ is of genus 0. Then there is a conic Γ defined over K of equation $G(X,Y) = 0$ with*

$$H(G) < (9N^{5N+4}H(F))^{13\cdot 10^4 N^{28}}$$

and a birational map $\Phi : C \to \Gamma$ given by

$$\Phi(X,Y) = \left(\frac{\phi_1(X,Y)}{\phi_3(X,Y)}, \frac{\phi_2(X,Y)}{\phi_3(X,Y)}\right),$$

where $\phi_i(X,Y) \in K[X,Y]$ $(i=1,2,3)$ *with* $\deg \phi_i < 3N^3$ *and*

$$H(\phi_i) < (9N^{5N+4}H(F))^{980N^{13}} \qquad (i=1,2,3).$$

The inverse map of Φ *is given by*

$$\Phi^{-1}(X,Y) = \left(\frac{\tau_1(X,Y)}{\tau_2(X,Y)}, \frac{\tau_3(X,Y)}{\tau_4(X,Y)}\right),$$

where $\tau_i(X,Y) \in K[X,Y]$ $(i=1,2,3,4)$ *with* $\deg \tau_i < 15N^3$ *and*

$$H(\tau_i) < \begin{cases} (9N^{5N+4}H(F))^{5355N^{16}} & (i=1,3), \\ (N+1)^{295N^{12}}H(F)^{118N^{12}} & (i=2,4). \end{cases}$$

THEOREM 2.2. *Let* $F(X,Y)$ *be an absolutely irreducible polynomial in* $K[X,Y]$ *of odd degree* $N \geq 3$ *such that the curve* C *defined by the equation* $F(X,Y)=0$ *is of genus* 0. *Then there is a birational map* $\Psi : C \to \mathbb{P}^1$ *given by*

$$\Psi(X,Y) = \frac{\psi_1(X,Y)}{\psi_2(X,Y)},$$

where $\psi_i(X,Y) \in K[X,Y]$ $(i=1,2)$ *with* $\deg \psi_i < 3N^3$ *and*

$$H(\psi_i) < (9N^{5N+4}H(F))^{980N^{13}}.$$

The inverse map of Ψ *is given by*

$$X = \frac{\sigma_1(T)}{\sigma_2(T)}, \qquad Y = \frac{\sigma_3(T)}{\sigma_4(T)},$$

where $\sigma_i(T) \in K[T]$ $(i=1,2,3,4)$ *with* $\deg \sigma_i < 8N^3$ *and*

$$H(\sigma_i) < \begin{cases} (9N^{5N+4}H(F))^{5530N^{16}} & (i=1,3), \\ (N+1)^{445N^{16}}H(F)^{180N^{16}} & (i=2,4). \end{cases}$$

THEOREM 2.3. *Let* $F(X,Y,Z)$ *be a homogeneous absolutely irreducible polynomial in* $K[X,Y,Z]$ *of degree* $N \geq 2$ *such that the curve* C *defined by the equation* $F(X,Y,Z)=0$ *is of genus* 0. *Suppose that* C *has a non-singular point defined over* K. *Then there exists a non-singular point* P *of* C *defined over* K *such that*

$$H(P) < |D_K|^{90N^3/d}(9N^{5N+4}H(F))^{18\cdot 10^6 N^{31}}.$$

Moreover, the curve $F(X,Y,1)=0$ *has a parametrization given by*

$$X = \frac{g_1(T)}{g_2(T)}, \qquad Y = \frac{g_3(T)}{g_4(T)},$$

where $g_i(T) \in K[T]$ $(i=1,2,3,4)$ *with* $\deg g_i < 30N^3$ *and*

$$H(g_i) < |D_K|^{225N^3/d}(9N^{5N+4}H(F))^{3\cdot 10^7 N^{31}}.$$

3. Curves with only ordinary singular points

3.1. *Statement of the results.* In this section we give an effective proof of the fact that a curve with only ordinary singular points is birationally equivalent to a conic. Our method develops some arguments that go back to some ideas of Poincaré [13]. Furthermore, a variant of our method gives an effective proof of the fact that a curve with only ordinary singular points and odd degree is birationally equivalent to a line. More precisely, we prove the following results:

THEOREM 3.1. *Let $F(X,Y)$ be an absolutely irreducible polynomial in $K[X,Y]$ of degree $N \geq 3$ such that the curve C defined by the equation $F(X,Y)=0$ is of genus 0. Suppose that C has only ordinary multiple points. Then there is a conic Γ defined over K of equation $G(X,Y)=0$ with*

$$H(G) < (N+1)^{40N^{12}} H(F)^{16N^{12}}$$

and a birational map $\Psi : C \to \Gamma$ defined by

$$\Psi(X,Y) = \left(\frac{\psi_1(X,Y)}{\psi_3(X,Y)}, \frac{\psi_2(X,Y)}{\psi_3(X,Y)} \right),$$

where $\psi_i(X,Y) \in K[X,Y]$ $(i=1,2,3)$ with $\deg \psi_i \leq N-1$ and

$$H(\psi_i) < (N+1)^{5N^9} H(F)^{2N^9} \qquad (i=1,2,3).$$

The inverse map of Ψ is given by

$$\Psi^{-1}(X,Y) = \left(\frac{\omega_1(X,Y)}{\omega_2(X,Y)}, \frac{\omega_3(X,Y)}{\omega_4(X,Y)} \right),$$

where $\omega_i(X,Y) \in K[X,Y]$ $(i=1,2,3,4)$ with $\deg_X \omega_i \leq N$, $\deg_Y \omega_i \leq N$ and

$$H(\omega_i) < (N+1)^{20N^{10}} H(F)^{8N^{10}}.$$

THEOREM 3.2. *Let $F(X,Y)$ be an absolutely irreducible polynomial in $K[X,Y]$ of odd degree $N \geq 3$ such that the curve C defined by the equation $F(X,Y)=0$ is of genus 0. Suppose that C has only ordinary multiple points. Then there is a birational map $\Psi : C \to \mathbb{P}^1$ defined by*

$$\Psi(X,Y) = \frac{\psi_1(X,Y)}{\psi_2(X,Y)},$$

where $\psi_i(X,Y) \in K[X,Y]$ $(i=1,2)$ with $\deg \psi_i \leq N-2$ and

$$H(\psi_i) < (N+1)^{15N^{13}} H(F)^{6N^{13}} \qquad (i=1,2).$$

The inverse map of Ψ is given by

$$X = \frac{\omega_1(T)}{\omega_2(T)}, \qquad Y = \frac{\omega_3(T)}{\omega_4(T)},$$

where $\omega_i(T) \in K[T]$ $(i = 1, 2, 3, 4)$ *with* $\deg \omega_i \le N$ *and*

$$H(\omega_i) < (N+1)^{30N^{14}} H(F)^{12N^{14}} \qquad (i = 1, 2, 3, 4).$$

3.2. *Auxiliary lemmas.* We give some lemmas which will be useful for the proof of our results. We prove only those which are not yet in the literature.

LEMMA 3.1. *Let* $F(X) = c_0 X^n + c_1 X^{n-1} + \ldots + c_n$ *be a polynomial in* $K[X] - K$ *and let* α *be one of its roots. Then*

$$H(\alpha) < 2H(F).$$

Proof. See [11; 14, Lemma 4].

LEMMA 3.2. *Let* $P(X, Y, V), Q(X, Y, W) \in K[X, Y, V, W] - K$. *Denote by* $R(X, V, W)$ *the resultant of* $P(X, Y, V)$ *and* $Q(X, Y, W)$, *considered as polynomials with coefficients in* $K[X, V, W]$. *Put* $\deg_X P = m_1$, $\deg_Y P = n_1$, $\deg_V P = r_1$ *and* $\deg_X Q = m_2$, $\deg_Y Q = n_2$, $\deg_W Q = r_2$. *Assume* $R(X, V, W) \neq 0$. *Then*

$$H(R) \le (n_1+n_2)!((r_1+1)(m_1+1))^{n_2}((r_2+1)(m_2+1))^{n_1} H(P)^{n_2} H(Q)^{n_1}.$$

Proof. Write

$$P(X, Y, V) = P_{n_1}(X, V) Y^{n_1} + \ldots + P_0(X, V),$$
$$Q(X, Y, W) = Q_{n_2}(X, W) Y^{n_2} + \ldots + Q_0(X, W),$$

where $P_i(X, V) \in K[X, V]$ $(i = 0, \ldots, n_1)$ and $Q_i(X, W) \in K[X, W]$ $(i = 0, \ldots, n_2)$. The polynomial $R(X, V, W)$ is homogeneous of degree n_2 in $P_{n_1}(X, V), \ldots, P_0(X, V)$ and of degree n_1 in $Q_{n_2}(X, W), \ldots, Q_0(X, W)$ with coefficients in $\mathbb{Z}$. If $|\cdot|_v$ is a non-archimedean absolute value, then

$$|R|_v \le |P|_v^{n_2} |Q|_v^{n_1}.$$

Let $|\cdot|_v$ be an archimedean absolute value. If $M(X, V, W)$ is a monomial of degree n_2 in $P_{n_1}(X, V), \ldots, P_0(X, V)$ and of degree n_1 in $Q_{n_2}(X, W), \ldots$ $\ldots, Q_0(X, W)$, then

$$|M(X, V, W)|_v \le ((r_1+1)(m_1+1))^{n_2}((r_2+1)(m_2+1))^{n_1} |P|_v^{n_2} |Q|_v^{n_1}.$$

Thus

$$|R|_v \le (n_1+n_2)!((r_1+1)(m_1+1))^{n_2}((r_2+1)(m_2+1))^{n_1} |P|_v^{n_2} |Q|_v^{n_1}.$$

Therefore

$$H(R) \le (n_1+n_2)!((r_1+1)(m_1+1))^{n_2}((r_2+1)(m_2+1))^{n_1} H(P)^{n_2} H(Q)^{n_1}.$$

LEMMA 3.3. *Let* f *and* g *be two polynomials of* $K[X_1, \ldots, X_m] - K$ *such that* $g(X)$ *divides* $f(X)$. *Then*

$$H(g) \le 4^{(\deg f + 1)^m} H(f).$$

P r o o f. Let h be a polynomial in $K[X_1,\dots,X_m]$ such that $gh=f$. By [10, Proposition 2.4, p. 57], we get

$$H(g)H(h)\le 4^{(\deg f+1)^m}H(f).$$

The lemma follows.

If $G(X,Y,Z)\in K[X,Y,Z]$, then by $G_{X^aY^bZ^c}(X,Y,Z)$ we denote, as usual, the (a,b,c)-partial derivative of $G(X,Y,Z)$ with respect to X,Y and Z.

LEMMA 3.4. *Let $F(X,Y,Z)$ be an irreducible homogeneous polynomial in $K[X,Y,Z]$. Let P be a singular point of the projective curve $F(X,Y,Z)=0$. Then*

$$H(P)<4(N+1)^{10N-4}H(F)^{4N-2}.$$

P r o o f. Suppose $P=(a:b:1)$. Then

$$F(a,b,1)=F_Y(a,b,1)=F_X(a,b,1)=0.$$

We denote by $R_1(X)$ the resultant of $F(X,Y,1)$ and $F_Y(X,Y,1)$ with respect to Y and by $R_2(Y)$ the resultant of $F(X,Y,1)$ and $F_X(X,Y,1)$ with respect to X. Thus $R_1(a)=R_2(b)=0$. Lemma 3.1 yields

$$H(P)\le H(a)H(b)<4H(R_1)H(R_2).$$

By Lemma 3.2,

$$H(R_i)<N^{4N-1}(N+1)^{N-1}H(F)^{2N-1}\qquad(i=1,2).$$

Hence

$$H(P)<4(N+1)^{10N-4}H(F)^{4N-2}.$$

Finally, if $P=(a:b:0)$, then $H(P)<2H(F)$. The lemma follows.

In the above proof we have used the inequality $m!<((m+1)/2)^m$, for every positive integer m (see A. Cauchy, *Exercices d'Analyse*, Vol. 4, Paris, 1847, p. 106). Throughout the paper we shall use this inequality without further mention.

LEMMA 3.5. *Let $F(X,Y)$ be a polynomial in $K[X,Y]$ of degree $m>0$ in X and $n>0$ in Y. Let $x,y\in K$ satisfy $F(x,y)=0$ and $\deg F(x,Y)=n$. Then*

$$H(y)<2(m+1)H(F)H(x)^m.$$

P r o o f. See [15, Lemma 7].

LEMMA 3.6. *Let $A_i=(a_{i1},\dots,a_{i\mu})$ $(i=1,\dots,\nu)$ be ν linearly independent vectors in $\overline{K}^\mu$ $(\nu<\mu)$ and V be the $\overline{K}$-vector space generated by A_i $(i=1,\dots,\nu)$. Let G be the Galois group of $\overline{K}$ over K. Suppose that*

$\sigma(V) = V$ for every $\sigma \in G$. Then there are $\mu - \nu$ linearly independent vectors $x_i = (x_{i1}, \dots, x_{i\mu})$ $(i = 1, \dots, \mu - \nu)$ in K such that

$$H(x_i) \le \nu! H(A_1) \dots H(A_\nu) \quad (i = 1, \dots, \mu - \nu),$$

satisfying the linear system

$$a_{i1}X_1 + \dots + a_{i\mu}X_\mu = 0 \quad (i = 1, \dots, \nu).$$

P r o o f. Let A be the matrix with rows A_i $(i = 1, \dots, \nu)$. We may suppose, without loss of generality, that the $\nu \times \nu$-matrix Δ formed by the ν first columns of A has rank ν. Thus $|\Delta| \neq 0$. We denote by $\Delta_{j,k}$ $(j = 1, \dots, \nu,\ k = \nu + 1, \dots, \mu)$ the matrix obtained from Δ by replacing the jth column by the kth column of A. Now the linear system is equivalent to

$$|\Delta| X_j = -|\Delta_{j,\nu+1}| X_{\nu+1} - \dots - |\Delta_{j,\mu}| X_\mu \quad (j = 1, \dots, \nu).$$

Taking $(X_{\nu+1}, \dots, X_\mu) = (-1, \dots, 0), \dots, (0, \dots, -1)$, we have respectively the solutions

$$x_1 = \left(\frac{|\Delta_{1,\nu+1}|}{|\Delta|}, \dots, \frac{|\Delta_{\nu,\nu+1}|}{|\Delta|}, -1, 0, \dots, 0 \right),$$

$$\vdots$$

$$x_{\mu-\nu} = \left(\frac{|\Delta_{1,\mu}|}{|\Delta|}, \dots, \frac{|\Delta_{\nu,\mu}|}{|\Delta|}, 0, \dots, 0, -1 \right)$$

which are linearly independent elements of $\overline{K}^\mu$.

Let $\sigma \in G$. Since $\sigma(V) = V$, the vectors $\sigma(A_i) = (\sigma(a_{i1}), \dots, \sigma(a_{i\mu}))$ $(i = 1, \dots, \nu)$ form a basis of V. Then there is an invertible $\nu \times \nu$-matrix B such that

$$(\sigma(A_1), \dots, \sigma(A_\nu)) = (A_1, \dots, A_\nu) B.$$

If $\sigma(\Delta)$ and $\sigma(\Delta_{j,k})$ are the matrices obtained by the action of σ on the entries of Δ and $\Delta_{j,k}$ respectively, then $\sigma(\Delta) = B^T \Delta$ and $\sigma(\Delta_{j,k}) = B^T \Delta_{j,k}$ (where B^T is the transpose of B). It follows that

$$\sigma\left(\frac{|\Delta_{j,k}|}{|\Delta|} \right) = \frac{|\sigma(\Delta_{j,k})|}{|\sigma(\Delta)|} = \frac{|B| \cdot |\Delta_{j,k}|}{|B| \cdot |\Delta|} = \frac{|\Delta_{j,k}|}{|\Delta|}.$$

Hence, $|\Delta_{j,k}|/|\Delta| \in K$ $(j = 1, \dots, \nu,\ k = \nu + 1, \dots, \mu)$, whence $x_i \in K^\mu$ $(i = 1, \dots, \mu - \nu)$.

The v-adic absolute value of a minor of A of order ν is

$$\le |A_1|_v \dots |A_\nu|_v v(\nu!),$$

where $v(\nu!) = \nu!$ if $|\cdot|_v$ is archimedean and $v(\nu!) = 1$ otherwise. Thus,

$$H(x_i) \le \nu! H(A_1) \dots H(A_\nu) \quad (i = 1, \dots, \mu - \nu).$$

LEMMA 3.7. *Let $\phi : C_1 \to C_2$ be a rational map of algebraic curves. Suppose that ϕ is defined and injective on an open subset U of C_1. Then ϕ is a birational map.*

P r o o f. Let $\widetilde{C}_i$ be a non-singular model of C_i and f_i be a birational morphism from $\widetilde{C}_i$ onto C. Then $f_2^{-1} \circ \phi \circ f_1 : \widetilde{C}_1 \to \widetilde{C}_2$ is a non-constant morphism of smooth curves and its restriction to the open set $f_1^{-1}(U)$ is injective. By [21, Proposition 2.6(b), p. 28], for all but finitely many $Q \in \widetilde{C}_2$,

$$\deg(f_2^{-1} \circ \phi \circ f_1) = \sharp(f_2^{-1} \circ \phi \circ f_1)^{-1}(Q).$$

Since the restriction of $\phi \circ f_1$ to $f_1^{-1}(U)$ is injective, we deduce that $\deg f_2^{-1} \circ \phi \circ f_1 = 1$. Thus, $f_2^{-1} \circ \phi \circ f_1$ is birational and so is ϕ.

LEMMA 3.8. *Let $C : F(X,Y) = 0$ be a plane algebraic curve defined over K of degree N. Then there is a plane model $G(X,Y) = 0$ of C defined over K with $\deg G = \deg_Y G = N$ and*

$$H(G) < N^{5N-4} H(F),$$

having N simple points at infinity.

P r o o f. Suppose that $\deg_Y F < N$ and $\deg_X F < N$. Then

$$F(X,Y) = X^a Y^b G(X,Y) + F_{N-1}(X,Y) + \ldots + F_0(X,Y),$$

where a, b are positive integers,

$$G(X,Y) = c(X + \varrho_1 Y) \ldots (X + \varrho_{N-a-b} Y)$$

with $c \in K$, $\varrho_i \in \overline{K} - \{0\}$ and $F_i(X,Y)$ is a homogeneous polynomial of degree i $(i = 0, \ldots, N-1)$. Putting $X = U + mV$ and $Y = V$, where m is a non-zero integer with $|m| < N/2$ and $G(m,1) \neq 0$, we have

$$\begin{aligned} F_1(U,V) = {} & (U+mV)^a V^b G(U+mV,V) \\ & + F_{N-1}(U+mV,V) + \ldots + F_0(U+mV,V), \end{aligned}$$

with $\deg_V F_1 = N$. The height of $F_1(U,V)$ satisfies

$$H(F_1) < (N/2)^{N-1}(N-1)!NH(F).$$

Suppose next that the curve $F_1(U,V) = 0$ does not have N points at infinity. Write

$$F_1(U,V) = f_N(U,V) + \ldots + f_0(U,V),$$

where $f_i(U,V)$ is a homogeneous polynomial of degree i $(i = 0, \ldots, N)$. Putting $U = 1/W$, we see that the curve $F_1(U,V) = 0$ is birationally equivalent to

$$F_2(W,V) = f_N(1,V) + W f_{N-1}(1,V) + \ldots + f_0(U,V) W^N = 0.$$

Let α be an integer with $|\alpha| < N^2$ such that there is no ramification above $W = \alpha$. Set $W = T + \alpha$. It follows that the curve

$$F_3(\Pi, \Xi, T) = f_N(\Pi, \Xi) + (T + \alpha\Pi)f_{N-1}(\Pi, \Xi) + \ldots + f_0(\Pi, \Xi)(T + \alpha\Pi)^N = 0$$

has N points with $T = 0$. The height of $F_3(\Pi, \Xi, T)$ satisfies

$$H(F_3) < N^{2N}N!(N+1)H(F_1) < N^{5N-4}H(F).$$

3.3. *K-rational sets*. Let $F(X, Y, Z)$ be a homogeneous absolutely irreducible polynomial in $K[X, Y, Z]$ of degree $N \geq 3$ such that the curve C defined by $F(X, Y, Z) = 0$ is of genus 0. We denote by S the set of singular points of C and for every $P \in S$ let m_P be the multiplicity of C at P. Suppose that C has no singularities other than ordinary multiple points. By Noether's formula [4, Chap. 8, p. 199; 2, Chap. III, p. 614], we have

$$\sum_{P \in S} m_P(m_P - 1) = (N-1)(N-2).$$

Let $\overline{K}$ be an algebraic closure of K. We denote by G the Galois group of $\overline{K}$ over K. A subset E of the projective plane $\mathbb{P}^2$ over $\overline{K}$ is called *K-rational* if $\sigma(E) = E$ for every $\sigma \in G$. The set S of singular points of C is determined by equations defined over K, whence S is K-rational.

Let $\nu \in \{N-1, N-2\}$ and E_ν be a K-rational subset of $C - S$ having $|E_\nu| = \varepsilon_\nu$ with $0 \leq \varepsilon_{N-2} \leq N-2$ and $0 \leq \varepsilon_{N-1} \leq 2N-2$. We denote by $W(\nu, E_\nu)$ the space of homogeneous polynomials $\psi(X, Y, Z)$ in $K[X, Y, Z]$ of degree ν such that the curve $\psi(X, Y, Z) = 0$ contains every point $P \in S$ with multiplicity $\geq m_P - 1$ and passes through the points of E_ν. Put $\delta(\nu, E_\nu) = \dim W(\nu, E_\nu)$ and $M(\nu, E_\nu) = \max\{H(Q)/Q \in S \cup E_\nu\}$. If $E_\nu = \emptyset$, then we write $W(\nu) = W(\nu, \emptyset)$, $\delta(\nu) = \delta(\nu, \emptyset)$ and $M(\nu) = M(\nu, \emptyset)$. We call, as usual, the points $(x : y : z)$ on C with $z = 0$, *points at infinity*. We denote by C_∞ the set of those points.

Lemma 3.9. *Under the above assumptions, we have*

$$\delta(\nu, E_\nu) = N\nu - (N-1)(N-2) - \varepsilon_\nu + 1$$

and there is a basis $\{\psi_1(X, Y, Z), \ldots, \psi_{\delta(\nu, E_\nu)}(X, Y, Z)\}$ *of* $W(\nu, E_\nu)$, *satisfying*

$$H(\psi_i) < N^{2N^2} M(\nu, E_\nu)^{\nu((N-1)(N-2)+2\varepsilon_\nu)/2} \quad (i = 1, \ldots, \delta(\nu, E_\nu)).$$

Proof. We can suppose, without loss of generality, that $F(0, 1, 0) \neq 0$ and that none of the points of $S \cup E_\nu$ is at infinity (if this is not the case, then we choose an appropriate projective coordinate system). Let $E(X, Y, Z)$ be a polynomial in $W(\nu)$. Denote by $R(X)$ the resultant of $E(X, Y, 1)$ and $F(X, Y, 1)$ with respect to Y. By [22, Theorem 5.3, p. 111], the multiplicity of the root a of $R(X)$ is equal to the sum of the intersection numbers of

the curves C and $E(X,Y,Z)=0$ on the line $X=a$. Let $P(i)=(\alpha_i:\beta_i:1)$ $(i=1,\dots,s)$ be the points of S. The polynomial $\Pi(X)=R(X)/\pi(X)$, where

$$\pi(X)=\prod_{i=1}^{s}(X-\alpha_i)^{m_{P(i)}(m_{P(i)}-1)},$$

is of degree $N\nu-(N-1)(N-2)$. By [4, Chap. 5, Sect. 2, p. 110] the dimension of the space $W(\nu)$ is

$$\geq \frac{(\nu+1)(\nu+2)}{2}-\frac{(N-1)(N-2)}{2}\geq N-1.$$

Thus, we can choose $E(X,Y,Z)$ such that α_i $(i=1,\dots,s)$ are not zeros of $\Pi(X)$ and the discriminant of $\Pi(X)$ has all its roots simple. Hence, $\Pi(X)$ has $N\nu-(N-1)(N-2)$ zeros pairwise distinct and different from α_i $(i=1,\dots,s)$, whence the curve $E(X,Y,Z)=0$ intersects C in $N\nu-(N-1)(N-2)$ pairwise distinct points apart from the points of S. Hence, $W(\nu)$ cuts out on C a linear series of order $N\nu-(N-1)(N-2)$ and no cycles of this series contain points of S. By [19, Chap. XII, Sect. 4, p. 379], this linear series is complete. Since C is of genus 0, [22, Chap. VI, Sect. 7, p. 187] implies that its dimension is $N\nu-(N-1)(N-2)$. It follows that $W(\nu,E_\nu)$ cuts out on C a linear series g_n^r of order $n=N\nu-(N-1)(N-2)-\varepsilon_\nu$ and dimension $r\geq N\nu-(N-1)(N-2)-\varepsilon_\nu$. By [22, Chap. VI, Theorem 2.5, p. 168], we have $r=n=N\nu-(N-1)(N-2)-\varepsilon_\nu$. Therefore $\delta(\nu,E_\nu)=N\nu-(N-1)(N-2)-\varepsilon_\nu+1$.

For every $P\in S\cup E_\nu$ we write $P=(x_P:y_P:z_P)$ with one of x_P,y_P,z_P being equal to 1. By [22, Theorem 2.4, p. 55], $W(\nu,E_\nu)$ is the space of polynomials

$$G(X,Y,Z)=\sum_{i+j=0}^{\nu}a_{ij}X^iY^jZ^{N-1-(i+j)}$$

with coefficients in K such that

$$G(x_Q,y_Q,z_Q)=0$$

for every $Q\in E_\nu$ and

$$G_{X^\alpha Y^\beta Z^\gamma}(x_P,y_P,z_P)=0$$

for every $P\in S$ and every triple of non-negative integers α,β,γ with $\alpha+\beta+\gamma=m_P-2$. Thus, we have a linear system in unknowns a_{ij}. The number of unknowns is $(\nu+1)(\nu+2)/2$. It follows that the rank ϱ of the matrix of the above system is

$$\varrho=\frac{(N-1)(N-2)}{2}+\varepsilon_\nu.$$

We consider ϱ rows of this matrix, $A_1,\dots,A_\varrho$, which are linearly independent. Since $S\cup E_\nu$ is K-rational, Lemma 3.6 implies that there exists a basis

$\{\psi_1(X,Y,Z),\dots,\psi_{\delta(\nu,E_\nu)}(X,Y,Z)\}$ of $W(\nu,E_\nu)$ satisfying

$$H(\psi_i) < \varrho! H(A_1)\dots H(A_\varrho) \quad (i=1,\dots,\delta(\nu,E_\nu)).$$

We easily deduce

$$H(A_i) < \nu! M(\nu,E_\nu)^\nu.$$

Thus

$$H(\psi_i) < \varrho!\nu! M(\nu,E_\nu)^{\nu\varrho} \quad (i=1,\dots,\delta(\nu,E_\nu)).$$

For every $\lambda=(\lambda_1,\dots,\lambda_{\delta(\nu,E_\nu)})\in K^{\delta(\nu,E_\nu)}$ we set

$$\phi_\lambda(X,Y,Z)=\lambda_1\psi_1(X,Y,Z)+\dots+\lambda_{\delta(\nu,E_\nu)}\psi_{\delta(\nu,E_\nu)}(X,Y,Z)$$

and we denote by $\kappa(\lambda)$ the curve defined by the equation $\phi_\lambda(X,Y,Z)=0$. If C_1 and C_2 are two curves in $\mathbb{P}^2$, we denote by $I(P,C_1\cap C_2)$ their intersection number at the point P of $\mathbb{P}^2$. For every positive integer r, we define $B(r)$ to be the set

$$B(r)=\{(x_1,\dots,x_{\delta(\nu,E_\nu)})\in\mathbb{Z}^{\delta(\nu,E_\nu)} \mid |x_j|\le r,\ j=1,\dots,\delta(\nu,E_\nu)\}.$$

LEMMA 3.10. *Let $\Gamma(r)$ be the set of $\delta(\nu,E_\nu)$-tuples $\lambda\in B(r)$ such that the curve $\kappa(\lambda)$ fails at least one of the following properties*:

(a) $I(P,C\cap\kappa(\lambda))=m_P(m_P-1)$ *for every* $P\in S$.
(b) $I(P,C\cap\kappa(\lambda))=1$ *for every* $P\in E_\nu$.
(c) $I(P,C\cap\kappa(\lambda))=0$ *for every* $P\in C_\infty-(S\cup E_\nu)$.
(d) *The point* $(0:1:0)$ *is not on* $\kappa(\lambda)$.

Then the number of elements of $\Gamma(r)$ is

$$\le (2r+1)^{\delta(\nu,E_\nu)-1}\Big(|S|+N+1+2\varepsilon_\nu+\sum_{P\in S}m_P\Big).$$

P r o o f. Set $n_P=m_P-1$ for every $P\in S$ and $n_P=1$ for every $P\in E_\nu$. Suppose that there is $Q\in S\cup E_\nu$ such that for every $k\in\{1,\dots,\delta(\nu,E_\nu)\}$ the curve $\psi_k(X,Y,Z)=0$ has multiplicity $>n_Q$ at Q. Consider $\delta(\nu,E_\nu)-1$ arbitrary points $Q_1,\dots,Q_{\delta(\nu,E_\nu)-1}$ on $C-(S\cup E_\nu)$ $(j=1,\dots,\delta(\nu,E_\nu)-1)$. Then there is $\mu\in K^{\delta(\nu,E_\nu)}$ such that the curve $\kappa(\mu)$ passes through the points of $S\cup E_\nu$ and $Q_1,\dots,Q_{\delta(\nu,E_\nu)-1}$. By Bezout's theorem,

$$\sum_R I(R,C\cap\kappa(\mu))=N\nu.$$

On the other hand, since the multiplicity of $\kappa(\mu)$ at Q is $>n_Q$, we have

$$\sum_R I(R,C\cap\kappa(\mu))>\sum_{P\in S}m_P(m_P-1)+\varepsilon_\nu+N\nu-(N-1)(N-2)-\varepsilon_\nu=N\nu,$$

which is a contradiction. So, for every $P\in S\cup E_\nu$ there is $j(P)\in\{1,\dots,\dots,\delta(\nu,E_\nu)\}$ such that the curve $\psi_{j(P)}(X,Y,Z)=0$ has multiplicity n_P at P.

Let $P \in S \cup E_\nu$ with $P = (x_P : y_P : 1)$. For every $j \in \{1, \dots, \delta(\nu, E_\nu)\}$ and $k \in \{0, \dots, n_P\}$ we put

$$\psi(P, j, k) = \psi_{j, X^{n_P+1-k}Y^k}(x_P, y_P, 1).$$

Then there is $j(P) \in \{1, \dots, \delta(\nu, E_\nu)\}$ and $k(P) \in \{0, \dots, n_P+1\}$ such that

$$\psi(P, j(P), k(P)) \neq 0.$$

If $P = (x_P : 1 : 0)$ or $(1 : 0 : 0)$, then we define the quantity $\psi(P, j, k)$ to be $\psi_{j, X^{n_P+1-k}Z^k}(x_P, 1, 0)$ or $\psi_{j, Y^{n_P+1-k}Z^k}(1, 0, 0)$ respectively. For every $\delta(\nu, E_\nu)$-tuple $\lambda = (\lambda_1, \dots, \lambda_{\delta(\nu,E_\nu)})$ in $K^{\delta(\nu,E_\nu)}$ we set

$$\Lambda_P(\lambda) = \lambda_1 \psi(P, 1, k(P)) + \ldots + \lambda_{\delta(\nu,E_\nu)} \psi(P, \delta(\nu, E_\nu), k(P)).$$

The number of solutions $\lambda \in B(r)$ of the equation $\Lambda_P(\lambda) = 0$ is $\leq (2r+1)^{\delta(\nu,E_\nu)-1}$. Note that if $\Lambda_P(\lambda) \neq 0$, then the multiplicity of $k(\lambda)$ at P is n_P.

If $f(X, Y) \in K[X, Y]$ and Q is a point on the curve $f(X, Y) = 0$ which is not at infinity, then we write

$$T_s(f(X, Y), Q)(\lambda, \mu) = \sum_{i=0}^{s} \frac{s!}{(s-i)!i!} f_{X^{s-i}Y^i}(Q) \lambda^{s-i} \mu^i.$$

Let $P \in S - C_\infty$. Since P is an ordinary multiple point, we have

$$T_{m_P}(F(X, Y, 1), P)(\lambda, \mu) = (\alpha_1 \lambda + \beta_1 \mu) \dots (\alpha_{m_P} \lambda + \beta_{m_P} \mu),$$

where the factors $\alpha_i \lambda + \beta_i \mu$ $(i = 1, \dots, m_P)$ are pairwise distinct. Furthermore,

$$T_{m_P-1}(\phi_\lambda(X, Y, 1), P)(-\beta_j, \alpha_j) = \sum_k \lambda_k T_{m_P-1}(\psi_k(X, Y, 1), P)(-\beta_j, \alpha_j) \qquad (j = 1, \dots, m_P).$$

For $\lambda = (\lambda_1, \dots, \lambda_{\delta(\nu,E_\nu)}) \in K^{\delta(\nu,E_\nu)}$ we write

$$L_{P,j}(\lambda) = \sum_k \lambda_k T_{m_P-1}(\psi_k(X, Y, 1), P)(-\beta_j, \alpha_j).$$

Hence, the curves C and $\kappa(\lambda)$ have distinct tangents at P if and only if

$$L_{P,j}(\lambda) \neq 0 \quad (j = 1, \dots, m_P).$$

If P is a point of S at infinity, then we consider the polynomial $F(X, 1, Z)$ or $F(1, Y, Z)$. Let now $P \in E_\nu - C_\infty$. Then P is a non-singular point of C and thus

$$T_1(F(X, Y, 1), P)(\lambda, \mu) = \zeta \lambda + \eta \mu.$$

Set

$$L_P(\lambda) = \sum_k \lambda_k T_1(\psi_k(X, Y, 1), P)(-\zeta, \eta).$$

The curves C and $\kappa(\lambda)$ have distinct tangents at P if and only if $L_P(\lambda) \neq 0$. Hence, for $P \in E_\nu$ we have the linear equation

$$L_P(\lambda) = 0$$

and for every $P \in S$ the m_P linear equations

$$L_{P,j}(\lambda) = 0 \quad (j = 1, \dots, m_P),$$

in unknowns $\lambda_1, \dots, \lambda_{\delta(\nu,E_\nu)}$. The number of solutions $\lambda \in B(r)$ of each of the above equations is $\leq (2r+1)^{\delta(\nu,E_\nu)-1}$. Note that if $P \in S$ with $L_{P,j}(\lambda) \neq 0$ $(j = 1, \dots, m_P)$ and $\Lambda_P(\lambda) \neq 0$, then $I(P, C \cap \kappa(\lambda)) = m_P(m_P - 1)$. Similarly, if $P \in E_\nu$ with $L_P(\lambda) \neq 0$ and $\Lambda_P(\lambda) \neq 0$, we get $I(P, C \cap \kappa(\lambda)) = 1$.

Let $F_N(X, Y)$ be the homogeneous part of degree N of $F(X, Y, 1)$. The points at infinity of C are $S_i = (a_i : b_i : 0)$ with $F_N(a_i, b_i) = 0$ $(i = 1, \dots, s)$. Let $\psi_{k,\nu}(X, Y)$ be the homogeneous part of degree ν of $\psi_k(X, Y, 1)$. For $\lambda = (\lambda_1, \dots, \lambda_{\delta(\nu,E_\nu)})$ in $K^{\delta(\nu,E_\nu)}$ we write

$$\Theta_i(\lambda) = \lambda_1\psi_{1,\nu}(a_i, b_i) + \dots + \lambda_{\delta(\nu,E_\nu)}\psi_{\delta(\nu,E_\nu),\nu}(a_i, b_i) \quad (i = 1, \dots, s).$$

Then $\phi_\lambda(S_i) = 0$ if and only if $\Theta_i(\lambda) = 0$. The number of solutions $\lambda \in B(r)$ of the equation $\Theta_i(\lambda) = 0$ is $\leq (2r+1)^{\delta(\nu,E_\nu)-1}$. Finally, $\phi_\lambda(0, 1, 0) \neq 0$ if and only if

$$\lambda_1\psi_{1,\nu}(0, 1) + \dots + \lambda_{\delta(\nu,E_\nu)}\psi_{\delta(\nu,E_\nu),\nu}(0, 1) \neq 0.$$

Combining the above estimates yields the lemma.

PROPOSITION 3.1. *Let Σ be a finite subset of C. Then there is $\lambda \in B(r)$, where*

$$r = \frac{1}{2}\Big(\sum_{P\in S} m_P + |\Sigma| + N^{2\delta(\nu,E_\nu)-3} + |S| + 2N + 2\varepsilon_\nu\Big) + 1,$$

such that the curve $\kappa(\lambda)$ meets C in $\delta(\nu, E_\nu) - 1$ distinct points $Q_1, \dots, Q_{\delta(\nu,E_\nu)-1}$ which are not in $S \cup E_\nu \cup \Sigma \cup C_\infty$ and satisfy

$$H(Q_i) < \Xi H(F)^{2\nu} M(\nu, E_\nu)^{\nu N((N-1)(N-2)+2\varepsilon_\nu)\delta(\nu,E_\nu)},$$

where

$$\Xi \leq N^{6N^4}(\delta(\nu, E_\nu)r)^{2N}.$$

P r o o f. Let r be a positive integer with

$$r > \frac{1}{2}\Big(|S| + N + 2\varepsilon_\nu + \sum_{P\in S} m_P\Big).$$

Then the set $\Gamma(r)$ of Lemma 3.10 is a proper subset of $B(r)$. Hence, there exists $\lambda = (\lambda_1, \dots, \lambda_{\delta(\nu,E_\nu)}) \in B(r)$ such that the curve $\kappa(\lambda) : \phi_\lambda(X, Y, Z) = 0$ has the properties (a), (b), (c) and (d) of Lemma 3.10. Let T be the set of

those points of intersection of C and $\kappa(\lambda)$ which are not contained in $S \cup E_\nu$. By (c), the points of T are not at infinity. Bezout's theorem yields

$$\sum_{Q \in T} I(Q, C \cap \kappa(\lambda)) = N\nu - \sum_{P \in S \cup E_\nu} I(P, C \cap \kappa(\lambda))$$
$$= N\nu - (N-1)(N-2) - \varepsilon_\nu = \delta(\nu, E_\nu) - 1.$$

We can suppose, without loss of generality, that $F(0,1,0) \neq 0$. Denote by $R(X)$ the resultant of $\phi_\lambda(X,Y,1)$ and $F(X,Y,1)$ with respect to Y. By [21, Theorem 5.3, p. 111], the multiplicity of the root a of $R(X)$ is equal to the sum of the intersection numbers of C and $\kappa(\lambda)$ on the line $X = a$. Let $P(i) = (a_i : b_i : 1)$ $(i = 1, \ldots, s)$ be the points of $S - C_\infty$ and $P(i) = (a_i : b_i : 1)$ $(i = s+1, \ldots, t)$ be the points of $E_\nu - C_\infty$. Put

$$\pi(X) = \prod_{i=1}^{s} (X - a_i)^{m_{P(i)}(m_{P(i)}-1)} \prod_{i=s+1}^{t} (X - a_i)$$

and consider the polynomial

$$\Pi(X) = \frac{R(X)}{\pi(X)}$$
$$= s_0(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}) X^{\delta(\nu,E_\nu)-1} + \ldots + s_{\delta(\nu,E_\nu)-1}(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}).$$

The coefficients $s_j(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)})$ are polynomials in $\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}$ of degree $\leq N$. The discriminant $\Delta_\Pi(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)})$ of $\Pi(X)$ is a polynomial in $\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}$ of degree $\leq N^{2\delta(\nu,E_\nu)-3}$. We have $|T| = \delta(\nu, E_\nu) - 1$ if and only if $\Pi(X)$ has $\delta(\nu, E_\nu) - 1$ pairwise distinct roots. Hence, $|T| = \delta(\nu, E_\nu) - 1$ if and only if $s_0(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}) \neq 0$ and $\Delta_\Pi(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}) \neq 0$. Furthermore, the number of $\delta(\nu, E_\nu)$-tuples $(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}) \in B(r)$ such that

$$\Delta_\Pi(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}) = 0 \quad \text{or} \quad s_0(\lambda_1, \ldots, \lambda_{\delta(\nu,E_\nu)}) = 0$$

is at most $(2r+1)^{\delta(\nu,E_\nu)-1}(N^{2\delta(\nu,E_\nu)-3} + N)$.

Denote by $S_1, \ldots, S_\sigma$ the elements of Σ. The number of solutions $\lambda \in B(r)$ of the equation $\phi_\lambda(S_j) = 0$ is $\leq (2r+1)^{\delta(\nu,E_\nu)-1}$. Thus, the number of $\delta(\nu, E_\nu)$-tuples $\lambda \in B(r)$ which do not have the required properties is

$$\leq (2r+1)^{\delta(\nu,E_\nu)-1} \Omega$$

where

$$\Omega = \Big(|\Sigma| + N^{2\delta(\nu,E_\nu)-3} + |S| + 2N + 1 + 2\varepsilon_\nu + \sum_{P \in S} m_P \Big).$$

Thus, if we take $r = (\Omega + 1)/2$, then there exists $\lambda \in B(r)$ such that the curve $\phi_\lambda(X,Y,Z) = 0$ intersects C in $\delta(\nu, E_\nu) - 1$ pairwise distinct points $Q_i = (x_i : y_i : 1)$ $(i = 1, \ldots, \delta(\nu, E_\nu) - 1)$ which are not in $S \cup E_\nu \cup \Sigma$.

We may assume, without loss of generality, that one of the coefficients of each ψ_j is 1. Then

$$H(\phi_\lambda) < \frac{\Omega+1}{2}\delta(\nu,E_\nu)H(\psi_1)\dots H(\psi_{\delta(\nu,E_\nu)})$$

and Lemma 3.9 yields

$$H(\phi_\lambda) < \frac{\Omega+1}{2}\delta(\nu,E_\nu)(N^{2N^2}M(\nu,E_\nu)^{\nu((N-1)(N-2)+2\varepsilon_\nu)/2})^{\delta(\nu,E_\nu)}.$$

The resultant $R(X)$ of $F(X,Y,1)$ and $\phi_\lambda(X,Y,1)$ satisfies

$$R(x_i) = 0 \quad (i = 1,\dots,\delta(\nu,E_\nu)-1).$$

Thus, Lemma 3.1 implies

$$H(x_i) < 2H(R) \quad (i = 1,\dots,\delta(\nu,E_\nu)-1).$$

By Lemma 3.2, we have

$$H(R) < (N+\nu)!(N+1)^\nu(\nu+1)^N H(F)^\nu H(\phi_\lambda)^N.$$

Thus,

$$H(x_i) < N^{4N}H(F)^\nu H(\phi_\lambda)^N.$$

Interchanging the roles of x_i and y_i we obtain the same bound for $H(y_i)$. Therefore

$$H(Q_i) < \Xi H(F)^{2\nu}M(\nu,E_\nu)^{N\nu((N-1)(N-2)+2\varepsilon_\nu)\delta(\nu,E_\nu)},$$

where

$$\Xi \le N^{6N^4}\left(\delta(\nu,E_\nu)\frac{\Omega+1}{2}\right)^{2N}.$$

Corollary 3.1. *For every positive integer ϱ there are ϱ K-rational subsets Σ_i $(i = 1,\dots,\varrho)$ of C such that $\Sigma_i \cap (S \cup E_\nu \cup C_\infty) = \emptyset$, $\Sigma_i \cap \Sigma_j = \emptyset$ for $i \ne j$, $|\Sigma_i| = \delta(\nu,E_\nu)-1$, and for every $Q \in \Sigma_i$ we have*

$$H(Q) < \Xi_i H(F)^{2\nu}M(\nu,E_\nu)^{N\nu((N-1)(N-2)+2\varepsilon_\nu)\delta(\nu,E_\nu)},$$

where

$$\Xi_i \le N^{6N^4}\delta(\nu,E_\nu)^{2N}4^{-N}$$
$$\times\Big(N^{2\delta(\nu,E_\nu)-3}+|S|+2N+2\varepsilon_\nu+\sum_{P\in S}m_P+(i-1)(\delta(\nu,E_\nu)-1)+2\Big)^{2N}.$$

Proof. For $\Sigma = \emptyset$, Proposition 3.1 implies that there is $\lambda \in B(r_1)$, where

$$r_1 = \frac{1}{2}\Big(N^{2\delta(\nu,E_\nu)-3}+|S|+2N+2\varepsilon_\nu+\sum_{P\in S}m_P\Big)+1,$$

such that the curve $\phi_\lambda(X,Y,Z)=0$ meets C in $\delta(\nu,E_\nu)-1$ pairwise distinct points $Q_1,\dots,Q_{\delta(\nu,E_\nu)-1}$ which are not in $S\cup E\cup C_\infty$ and satisfy

$$H(Q_i)<\Xi_1 H(F)^{2\nu}M(\nu,E_\nu)^{\nu N((N-1)(N-2)+2\varepsilon_\nu)\delta(\nu,E_\nu)},$$

where

$$\Xi_1\le N^{6N^4}(\delta(\nu,E_\nu)r_1)^{2N}.$$

Since $F(X,Y,Z)$ and $\phi_\lambda(X,Y,Z)$ are in $K[X,Y,Z]$, the intersection of the two curves is K-rational. In addition, $S\cup E_\nu$ is K-rational. Hence, so is $\{Q_1,\dots,Q_{\delta(\nu,E_\nu)-1}\}$.

Next, take $\Sigma_1=\{Q_1,\dots,Q_{\delta(\nu,E_\nu)-1}\}$. Proposition 3.1 implies that there exists $\mu\in B(r_2)$, where

$$r_2=\frac{1}{2}\Big(\delta(\nu,E_\nu)-1+N^{2\delta(\nu,E_\nu)-3}+|S|+2N+2\varepsilon_\nu+\sum_{P\in S}m_P\Big)+1,$$

such that the curve $\phi_\mu(X,Y,Z)=0$ meets C in $\delta(\nu,E_\nu)-1$ pairwise distinct points $S_1,\dots,S_{\delta(\nu,E_\nu)-1}$ which are not at infinity and satisfy

$$H(S_i)<\Xi_2 H(F)^{2\nu}M(\nu,E_\nu)^{N\nu((N-1)(N-2)+2\varepsilon_\nu)\delta(\nu,E_\nu)},$$

where

$$\Xi_2\le N^{6N^4}(\delta(\nu,E_\nu)r_2)^{2N}.$$

Furthermore, the points $S_1,\dots,S_{\delta(\nu,E_\nu)-1}$ are not in $S\cup E_\nu\cup\Sigma_1$. Since S, E_ν and Σ_1 are K-rational, so is $\{S_1,\dots,S_{\delta(\nu,E_\nu)-1}\}$. Repeating the above procedure yields the assertion.

3.4. *Proof of Theorem 3.1.* Take $\nu=N-2$ and $E_{N-2}=\emptyset$. Corollary 3.1 implies that there are two K-rational subsets Σ_i $(i=1,2)$ of C with $|\Sigma_i|=N-2$ and $\Sigma_1\cap\Sigma_2=\emptyset$ such that for every $Q\in\Sigma_1\cup\Sigma_1$ we have

$$H(Q)<N^{7N^4}H(F)^{2N-4}M(N-2)^{N(N-1)^2(N-2)^2}.$$

By Lemma 3.4,

$$M(N-2)<4(N+1)^{10N-4}H(F)^{4N-2}.$$

Thus, for every $Q\in\Sigma_1\cup\Sigma_2$ we have

$$H(Q)<(N+1)^{10N^6}H(F)^{4N^6}.$$

Next, let $\nu=N-1$ and $E_{N-1}=\Sigma_1\cup\Sigma_2$. Then Lemma 3.7 implies that there is a basis $\{\psi_1(X,Y,Z),\psi_2(X,Y,Z),\psi_3(X,Y,Z)\}$ of $W(N-1,\Sigma_1\cup\Sigma_2)$ such that

$$H(\psi_i)<N^{2N^2}M(N-1,E_{N-1})^{(N^3-7N+6)/2}\qquad(i=1,2,3).$$

Combining Lemma 3.4 and the above inequalities, we get

$$H(\psi_i)<(N+1)^{5N^9-30N^8}H(F)^{2N^9-12N^8}\qquad(i=1,2,3).$$

The set of common zeros of $\psi_1(X,Y,Z), \psi_2(X,Y,Z), \psi_3(X,Y,Z)$ in $\mathbb{P}^2$ is $V = \Sigma_1 \cup \Sigma_2 \cup S$. Put $U = C - V$ and consider the morphism $\psi : U \to \mathbb{P}^2$ given by

$$\psi(P) = (\psi_1(P) : \psi_2(P) : \psi_3(P)) \quad \text{for every } P \in U.$$

We denote by $\widetilde{C}$ the closure of $\psi(U)$ in $\mathbb{P}^2$. The morphism ψ defines a rational map Ψ from C to $\widetilde{C}$. First, we prove that $\widetilde{C}$ is a conic.

Consider the set $\widetilde{S}$ of singular points of $\psi(U)$. By Proposition 3.1, there is $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}^3$ such that the curve $\kappa(\lambda)$ defined by

$$\phi_\lambda(X,Y,Z) = \lambda_1\psi_1(X,Y,Z) + \lambda_2\psi_2(X,Y,Z) + \lambda_3\psi_3(X,Y,Z) = 0$$

meets C in two distinct points Γ_1, Γ_2 which are not in $S \cup E_{N-1} \cup \psi^{-1}(\widetilde{S})$. Thus, the points $\psi(\Gamma_1)$ and $\psi(\Gamma_2)$ are simple and $I(\Gamma_i, C \cap \kappa(\lambda)) = 1$ $(i = 1, 2)$. Denote by L the line in $\mathbb{P}^2$ defined by

$$\varepsilon(X,Y,Z) = \lambda_1 X + \lambda_2 Y + \lambda_3 Z = 0.$$

Put $\Delta_i = \psi(\Gamma_i)$ $(i = 1, 2)$. Then $L \cap \widetilde{S} = \{\Delta_1, \Delta_2\}$. Let $O_{\Delta_i}(\widetilde{C})$ be the local ring of $\widetilde{C}$ at Δ_i and $O_{\Gamma_i}(C)$ be the local ring of C at Γ_i $(i = 1, 2)$. The morphism ψ induces a ring monomorphism $\psi* : O_{\Delta_i}(\widetilde{C}) \to O_{\Gamma_i}(C)$ given by

$$\psi * (f) = f \circ \psi \quad \text{for every } f \in O_{\Delta_i}(\widetilde{C}).$$

Since Γ_i and Δ_i are non-singular points of C and $\widetilde{C}$ respectively, it follows that $O_{\Delta_i}(\widetilde{C})$ and $O_{\Gamma_i}(C)$ are discrete valuation rings. We denote by $\mathrm{ord}^C_{\Gamma_i}$ and $\mathrm{ord}^{\widetilde{C}}_{\Delta_i}$ the order functions defined by $O_{\Gamma_i}(C)$ and $O_{\Delta_i}(\widetilde{C})$ respectively. Then

$$\mathrm{ord}^C_{\Gamma_i}(\psi * (\varepsilon)) = \mathrm{ord}^C_{\Gamma_i}(\phi_\lambda) = I(\Gamma_i, C \cap \kappa(\lambda)) = 1.$$

Since $\mathrm{ord}^{\widetilde{C}}_{\Delta_i}(\varepsilon) \le \mathrm{ord}^C_{\Gamma_i}(\psi * (\varepsilon))$, it follows that $\mathrm{ord}^{\widetilde{C}}_{\Delta_i}(\varepsilon) = 1$, whence $I(\Delta_i, \widetilde{C} \cap L) = 1$ $(i = 1, 2)$. By Bezout's theorem, we get

$$\deg \widetilde{C} = I(\Delta_1, \widetilde{C} \cap L) + I(\Delta_2, \widetilde{C} \cap L) = 2.$$

Hence $\widetilde{C}$ is a conic.

Let $G(X,Y,Z) = 0$ be the equation defining $\widetilde{C}$. We now calculate an upper bound for $H(G)$. Let $(x, y) \in K^2$ satisfy $F(x, y, 1) = 0$ and $\psi_3(x, y, 1) \neq 0$. Put

$$\mu = \frac{\psi_1(x,y,1)}{\psi_3(x,y,1)}, \qquad \xi = \frac{\psi_2(x,y,1)}{\psi_3(x,y,1)}.$$

Then (x, y, μ) is a solution of the system

$$F(X,Y,1) = 0, \qquad \Psi_1(X,Y,M) = \psi_1(X,Y,1) - M\psi_3(X,Y,1) = 0$$

and (x, y, ξ) is a solution of the system

$$F(X,Y,1) = 0, \qquad \Psi_2(X,Y,\Xi) = \psi_2(X,Y,1) - \Xi\psi_3(X,Y,1) = 0.$$

We denote by $R_1(X,M)$ and $R_2(X,\Xi)$, respectively, the resultants of $F(X,Y,1)$, $\Psi_1(X,Y,M)$ and $F(X,Y,1)$, $\Psi_2(X,Y,\Xi)$ with respect to Y. It follows that

$$R_1(x,\mu)=0, \quad R_2(x,\xi)=0.$$

Thus, if $R(M,\Xi)$ is the resultant of $R_1(X,M)$ and $R_2(X,\Xi)$ with respect to X, then $R(\mu,\xi)=0$. We conclude that the points of $\widetilde{C}$ belong to the projective closure of the curve $R(M,\Xi)=0$. Hence $G(X,Y,1)$ divides $R(M,\Xi)$.

By Lemma 3.2, the height of R_i satisfies

$$H(R_i)<(2N-1)!(N+1)^{N-1}(2N)^N H(F)^{N-1}(H(\psi_i)H(\psi_3))^N \quad (i=1,2).$$

We deduce that

$$H(R_i)<(N+1)^{10N^{10}-50N^9}H(F)^{4N^{10}} \quad (i=1,2).$$

Further, we have $\deg_X R_i \le 2N(N-1)$ $(i=1,2)$, $\deg_M R_1 \le N$ and $\deg_\Xi R_2 \le N$. It follows that $\deg_M R \le 2N^2(N-1)$ and $\deg_\Xi R \le 2N^2(N-1)$. Lemma 3.2 yields

$$H(R)<(4N^2-4N)!(N+1)^{4N(N-1)}(H(R_1)H(R_2))^{2N(N-1)}.$$

Thus, we obtain

$$H(R)<(N+1)^{40N^{12}-39N^{11}}H(F)^{16N^{12}}.$$

Finally, Lemma 3.3 implies

$$H(G)<(N+1)^{40N^{12}}H(F)^{16N^{12}}.$$

Next, we prove that Ψ is birational. Suppose that there exist $P_1,P_2\in U$ with $P_1\neq P_2$ and $\psi(P_1)=\psi(P_2)$. If P is an arbitrary point of U with $P\neq P_1$, $P\neq P_2$ and $\psi(P)\neq\psi(P_1)$, then we consider the line in $\mathbb{P}^2$ defined by the equation $\alpha X+\beta Y+\gamma Z=0$ passing through $\psi(P_1)$ and $\psi(P)$. It follows that the curve $\kappa(\alpha,\beta,\gamma)$ meets C in the three points P,P_1,P_2 apart from the points of $S\cup\Sigma_1\cup\Sigma_2$. On the other hand, Bezout's theorem implies that C meets $\kappa(\alpha,\beta,\gamma)$ at most in two points apart from the points of $S\cup\Sigma_1\cup\Sigma_2$, which is a contradiction. Thus, $\psi(P_1)\neq\psi(P_2)$. Therefore, ψ is injective. Hence, Lemma 3.7 shows that Ψ is birational.

For every $\mu,\xi\in\overline{K}$, the curves

$$F(X,Y,1)=0, \quad \Psi_1(X,Y,\mu)=0, \quad \Psi_2(X,Y,\xi)=0$$

pass through the points of $S\cup\Sigma_1\cup\Sigma_2$ which are not in C_∞. The multiplicity of the root of $R_1(X,\mu)$ is equal to the sum of the intersection numbers of C and the curve $\Psi_1(X,Y,\mu)=0$ on the line $X=\alpha$. Let $P(i)=(\alpha_i:\beta_i:1)$ $(i=1,\dots,s)$ be the points of S, and $P(i+s)=(\alpha_{i+s}:\beta_{i+s}:1)$ $(i=1,\dots,2N-4)$ be the points of $\Sigma_1\cup\Sigma_2$ which are not in C_∞. Then for

every $\mu \in \overline{K}$ the polynomial

$$\Pi(X) = \prod_{1\le i\le s} (X-\alpha_i)^{m_P(i)(m_P(i)-1)} \prod_{1\le i\le 2N-4} (X-\alpha_{s+i})$$

divides $R_1(X,\mu)$. It follows that $\Pi(X)$ divides $R_1(X,M)$. Similarly, $\Pi(X)$ divides $R_2(X,\Xi)$. Put

$$S_1(X,M) = \frac{R_1(X,M)}{\Pi(X)}, \quad S_2(X,\Xi) = \frac{R_2(X,\Xi)}{\Pi(X)}.$$

By Bezout's theorem, the degree of the polynomials $S_1(X,\mu)$ and $S_2(X,\xi)$ is 2, whence $\deg_X S_1 = \deg_X S_2 = 2$.

Let $(\mu : \xi : 1) \in \psi(U - C_\infty)$. Since $(\mu : \xi : 1) \in \psi(U - C_\infty)$ and ψ is injective, there is exactly one pair (x_0, y_0) such that

$$F(x_0, y_0, 1) = 0, \quad \Psi_1(x_0, y_0, \mu) = 0, \quad \Psi_2(x_0, y_0, \xi) = 0.$$

Then $S_1(x_0,\mu) = S_2(x_0,\xi) = 0$. Write

$$S_1(X,M) = a_0(M)X^2 + a_1(M)X + a_2(M),$$
$$S_2(X,\Xi) = b_0(\Xi)X^2 + b_1(\Xi)X + b_2(\Xi).$$

Let $\mho$ be the set of points $(\mu : \xi : 1) \in \psi(U - C_\infty)$ such that

$$\frac{a_0(\mu)}{b_0(\xi)} = \frac{a_1(\mu)}{b_1(\xi)} = \frac{a_2(\mu)}{b_2(\xi)}.$$

Then $S_1(X,\mu)$ and $S_2(X,\xi)$ have the same roots if and only if $(\mu : \xi : 1) \in \mho$. If $(\mu : \xi : 1)$ is not in $\mho$, then $X - x_0$ is the greatest common divisor of $S_1(X,\mu)$ and $S_2(X,\xi)$.

Consider $S_1(X,M)$ and $S_2(X,\Xi)$ as elements of $K(M,\Xi)[X]$. Then there are $A(M,\Xi) \in K(M,\Xi)$ and $B(X,M,\Xi) \in K(M,\Xi)[X]$ with $\deg_X B(X,M,\Xi) = 1$ such that

$$S_1(X,M) = A(M,\Xi)S_2(X,\Xi) - B(X,M,\Xi).$$

Let $(\mu : \xi : 1)$ be a point which is not in $\mho$ and $x_0, y_0 \in \overline{K}$ with $\psi(x_0 : y_0 : 1) = (\mu : \xi : 1)$. Then $B(x_0,\mu,\xi) = 0$. Similarly, we deduce that there is $\Gamma(Y,M,\Xi) \in K(M,\Xi)[Y]$ with $\deg_Y(Y,M,\Xi) = 1$ such that $\Gamma(y_0,\mu,\xi) = 0$. Write

$$B(X,M,\Xi) = B_0(M,\Xi)X - B_1(M,\Xi),$$
$$\Gamma(Y,M,\Xi) = \Gamma_0(M,\Xi)Y - \Gamma_1(M,\Xi).$$

Thus

$$x_0 = \frac{B_1(\mu,\xi)}{B_0(\mu,\xi)} \quad \text{and} \quad y_0 = \frac{\Gamma_1(\mu,\xi)}{\Gamma_0(\mu,\xi)}.$$

Hence, the rational map Ψ^{-1} is given by the map

$$\widetilde{C} - \mho \to C, \quad (\mu,\xi) \to \left(\frac{B_1(\mu,\xi)}{B_0(\mu,\xi)}, \frac{\Gamma_1(\mu,\xi)}{\Gamma_0(\mu,\xi)}\right).$$

Finally, we calculate a bound for the heights of $B_i(M,\Xi)$, $\Gamma_i(M,\Xi)$ $(i=1,2)$. It is easily seen that

$$\frac{B_1(M,\Xi)}{B_0(M,\Xi)}=\frac{\omega_1(M,\Xi)}{\omega_2(M,\Xi)},$$

where

$$\omega_1(M,\Xi)=a_0(M)b_2(\Xi)-a_2(M)b_0(\Xi),$$
$$\omega_2(M,\Xi)=a_1(M)b_0(\Xi)-a_0(M)b_1(\Xi).$$

We have $\deg_M\omega_i\le N$, $\deg_\Xi\omega_i\le N$ $(i=1,2)$ and

$$H(\omega_i)<2H(S_1)H(S_2)\quad(i=1,2).$$

By Lemma 3.3, we get

$$H(S_j)<4^{(2N^2-N)^2}H(R_j)\quad(j=1,2).$$

Thus

$$H(S_j)<(N+1)^{10N^{10}-49N^9}H(F)^{4N^{10}}\quad(j=1,2),$$

whence

$$H(\omega_i)<(N+1)^{20N^{10}}H(F)^{8N^{10}}\quad(i=1,2).$$

Similarly, we have

$$\frac{\Gamma_1(M,\Xi)}{\Gamma_0(M,\Xi)}=\frac{\omega_3(M,\Xi)}{\omega_4(M,\Xi)}$$

with $\deg_M\omega_i\le N$, $\deg_\Xi\omega_i\le N$ $(i=3,4)$ and

$$H(\omega_i)<(N+1)^{20N^{10}}H(F)^{8N^{10}}\quad(i=3,4).$$

3.5. *Proof of Theorem 3.2.* Suppose that N is odd. At the beginning of the proof of Theorem 3.1 we have seen that there exists a K-rational subset Σ of C with $|\Sigma|=2N-4$ and $\Sigma\cap S=\emptyset$ such that for every $Q\in\Sigma$ we have

$$H(Q)<(N+1)^{10N^6}H(F)^{4N^6}.$$

Now if we take $\nu=N-1$ and $E_{N-1}=\Sigma$, Corollary 3.1 implies that there are $(N-3)/2$ K-rational subsets Σ_i $(i=1,\dots,(N-3)/2)$ of C such that $|\Sigma_i|=2$, $\Sigma_i\cap(S\cup\Sigma\cup C_\infty)=\emptyset$, $\Sigma_i\cap\Sigma_j=\emptyset$ for $i\ne j$ and for every $Q\in\Sigma_i$ we have

$$H(Q)<N^{7N^4}H(F)^{2N-2}M(N-1,\Sigma)^{3N(N^3-7N+6)}.$$

Using Lemma 3.4, we get

$$M(N-1,\Sigma)<(N+1)^{10N^6}H(F)^{4N^6}.$$

Then for every $Q\in\Sigma_i$ we obtain

$$H(Q)<(N+1)^{30N^{10}}H(F)^{12N^{10}}.$$

Next, let $\nu = N-2$ and $E_{N-2} = \Sigma_1 \cup \ldots \cup \Sigma_{(N-3)/2}$. Then Lemma 3.7 implies that there is a basis $\{\psi_1(X,Y,Z), \psi_2(X,Y,Z)\}$ of $W(N-2, E_{N-2})$ such that

$$H(\psi_i) < N^{2N^2} M(N-2, E_{N-2})^{(N^3-3N^2-2N+8)/2} \qquad (i=1,2).$$

Since

$$M(N-2, E_{N-2}) < (N+1)^{30N^{10}} H(F)^{12N^{10}},$$

we get

$$H(\psi_i) < (N+1)^{15N^{13}-40N^{12}} H(F)^{6N^{13}-16N^{12}} \qquad (i=1,2).$$

The set of common zeros of $\psi_1(X,Y,Z)$ and $\psi_2(X,Y,Z)$ in $\mathbb{P}^2$ is $E_{N-2} \cup S$. Put $U = C - (E_{N-2} \cup S)$ and consider the morphism $\psi : U \to \mathbb{P}^1$ given by

$$\psi(P) = (\psi_1(P) : \psi_2(P)) \quad \text{for every } P \in U.$$

Thus ψ defines a rational map Ψ from C to $\mathbb{P}^1$. We now prove that Ψ is a birational map and we determine Ψ^{-1}.

Put

$$\Psi_1(X,Y,M) = \psi_1(X,Y,1) - M\psi_2(X,Y,1) = 0.$$

We denote by $R_1(X,M)$ and $R_2(Y,M)$, respectively, the resultants of $F(X,Y,1)$ and $\Psi_1(X,Y,M)$ with respect to Y and X. We have $\deg_X R_1 \le 2N(N-2)$, $\deg_Y R_2 \le 2N(N-2)$ and $\deg_M R_i \le N$ $(i=1,2)$. Using Lemma 3.2, we get

$$H(R_i) < (N+1)^{30N^{14}-70N^{13}} H(F)^{12N^{14}} \qquad (i=1,2).$$

For every $\mu \in \overline{K}$, the curves $F(X,Y,1)=0$ and $\Psi_1(X,Y,\mu)=0$ pass through the points of the set $(S \cup E_{N-2}) - C_\infty$. The multiplicity of the root a of $R_1(X,\mu)$ is the sum of the intersection numbers of C and the curve $\Psi_1(X,Y,\mu)=0$ on the line $X=a$. Let $P(i) = (a_i : b_i : 1)$ $(i=1,\ldots,s)$ be the points of S and $P(i+s) = (a_{i+s} : b_{i+s} : 1)$ $(i=1,\ldots,N-3)$ be the points of E_{N-2} which are not at infinity. Then the polynomial

$$\Pi(X) = \prod_{i=1}^{s} (X-a_i)^{m_P(i)(m_P(i)-1)} \prod_{i=1}^{N-3} (X-a_{i+s})$$

divides $R_1(X,\mu)$. It follows that $\Pi(X)$ divides $R_1(X,M)$. Put

$$S_1(X,M) = \frac{R_1(X,M)}{\Pi(X)}.$$

By Bezout's theorem, $\deg S_1(X,\mu) = 1$, whence $\deg_X S_1 = 1$. Similarly, there is a polynomial $S_2(Y,M)$ dividing $R_2(Y,M)$ with $\deg_Y S_2 = 1$.

Write

$$S_1(X,M) = a_0(M)X - a_1(M), \qquad S_2(Y,M) = b_0(M)Y - b_1(M).$$

Let $(\mu : 1) \in \psi(U - C_\infty)$. Then there is a pair (x_0, y_0) such that

$$F(x_0, y_0, 1) = 0, \quad \Psi_1(x_0, y_0, \mu) = 0.$$

We have $S_1(x_0, \mu) = 0$ and $S_2(y_0, \mu) = 0$, whence

$$x_0 = \frac{a_1(\mu)}{a_0(\mu)}, \quad y_0 = \frac{b_1(\mu)}{b_0(\mu)}.$$

Hence, the rational map given by

$$X = \frac{a_1(M)}{a_0(M)}, \quad Y = \frac{b_1(M)}{b_0(M)}$$

is the inverse rational map of Ψ. Therefore, Ψ is a birational map. Since $S_1(X, M)$ divides $R_1(X, M)$ and $S_2(Y, M)$ divides $R_2(Y, M)$, Lemma 3.3 yields

$$H(a_i), H(b_i) < H(S_i) < 4^{4N^4} H(R_i) < (N+1)^{30N^{14}} H(F)^{12N^{14}} \quad (i = 1, 2).$$

4. Reduction of singularities to double ordinary points

4.1. *Statement of the results.* It is well known that every curve has a plane model having no singularities other than double ordinary points [1, Chap. VIII, Theorem 58.1; 5, Chap. IV, Corollary 3.11]. In this section we give an effective proof of this result for the case of curves of genus 0 following the main arguments of Theorem 58.1 of [1]. More precisely we prove the following result:

THEOREM 4.1. *Let $F(X, Y)$ be an absolutely irreducible polynomial in $K[X, Y]$ of degree $N \geq 3$ such that the curve C defined by the equation $F(X, Y) = 0$ is of genus 0. Then C is birational to a plane curve $\widetilde{C}$ given by $G(X, Y) = 0$, where $G(X, Y)$ is a polynomial of $K[X, Y]$ of degree N having*

$$H(G) < (9N^{5N+4} H(F))^{7810N^{16}},$$

such that $\widetilde{C}$ has no singularities other than double ordinary points. Moreover, there is a birational map $\Psi : C \to \widetilde{C}$ given by

$$\Psi(X, Y) = \left(\frac{\psi_1(X, Y)}{\psi_3(X)}, \frac{\psi_2(X, Y)}{\psi_3(X)} \right),$$

where $\psi_i(X, Y) \in K[X, Y]$ $(i = 1, 2)$ and $\psi_3(X) \in K[X]$ with $\deg_X \psi_i(X, Y) \leq 2N^2 + 4N$, $\deg_Y \psi_i < N$ $(i = 1, 2)$, $\deg \psi_3 \leq N^2$ and

$$H(\psi_i) < (9N^{5N+4} H(F))^{490N^{12}} \quad (i = 1, 2),$$
$$H(\psi_3) < (N+1)^{10N^4} H(F)^{2N^3}.$$

The inverse map of Ψ is given by

$$\Psi^{-1}(X, Y) = \left(\frac{\omega_1(X, Y)}{\omega_2(X)}, \frac{\omega_3(X, Y)}{\omega_4(X)} \right),$$

where $\omega_i(X,Y) \in K[X,Y]$ $(i = 1,2,3,4)$ *with* $\deg_X \omega_i \le 2N^2 + 4N$, $\deg_Y \omega_i < N$ $(i = 1,3)$, $\deg \omega_i \le N^2$ $(i = 2,4)$ *and*

$$H(\omega_i) < \begin{cases} (9N^{5N+4}H(F))^{5352N^{16}} & (i = 1,3), \\ (N+1)^{10N^4}H(F)^{2N^3} & (i = 2,4). \end{cases}$$

Combining Theorems 3.1, 3.2 and 4.1, we obtain Theorems 2.1 and 2.2.

4.2. *Puiseux expansions for algebraic functions.* Let $F(X,Y)$ be an irreducible polynomial in $K[X,Y]$ of degree $m > 0$ in X and $n > 0$ in Y. Write

$$F(X,Y) = A_n(X)Y^n + A_{n-1}(X)Y^{n-1} + \ldots + A_0(X).$$

Put $t_a = X - a$ if $a \in K$ and $t_a = 1/X$ if $a = \infty$. By Puiseux's theorem [1, Chap. II; 3, Chap. III; 22, Chap. IV, Sect. 3], for every $a \in K \cup \{\infty\}$ there are n distinct formal power series

$$\mathbf{y}_{i,k} = \sum_{s \ge s(i)} c_{i,s}\zeta_i^{ks} t_a^{s/e_i} \qquad (i = 1,\ldots,r;\ k = 0,\ldots,e_i - 1),$$

where $e_1,\ldots,e_r$ are positive integers with $e_1 + \ldots + e_r = n$ and ζ_i is an e_ith primitive root of 1, satisfying

$$F(X,Y) = A_n(X)\prod_{i,k}(Y - \mathbf{y}_{i,k}(X)).$$

The coefficients $c_{i,s}$ lie in a finite extension L_i of K and $c_{i,s}(i) \ne 0$ $(i = 1,\ldots,r)$. Moreover, any series $\mathbf{y}(X)$ of this form satisfying $F(X,\mathbf{y}(X)) = 0$, must be one of the series $\mathbf{y}_{i,k}(X)$ $(i = 1,\ldots,r;\ k = 0,\ldots,e_{i-1})$. The series $\mathbf{y}_{i,k}$ are known as *Puiseux expansions* at $X = a$ of the algebraic function $\mathbf{y}$ defined by $F(X,\mathbf{y}) = 0$ and $e_1,\ldots,e_r$ are called the *ramification indices* of $\mathbf{y}$ at $X = a$. Systematic methods for computing e_i and $c_{i,s}$ are known (see [1], [7], [17], [22]). If $[L_i : K] = l(i)$ and $\sigma_1,\ldots,\sigma_{l(i)}$ denote the K-isomorphisms of L_i into $\mathbb{C}$, then each of the conjugate series

$$\mathbf{y}_{i,k,\sigma_j}(X) = \sum_{s \ge s(i)} \sigma_j(c_{i,s})\zeta_i^{ks} t_a^{s/e_i} \qquad (j = 1,\ldots,l(i);\ k = 0,\ldots,e_{i-1})$$

represents one of the Puiseux expansions at $X = a$. Thus, we conclude that for every s the coefficients $c_{1,s},\ldots,c_{r,s}$ form a K-rational set. We denote by N the total degree of F and suppose that $N \ge 3$.

Denote by C the curve defined by $F(X,Y) = 0$. Let $\mathbb{U}$ be the set of discrete valuation rings V of $\overline{K}(C)$ such that $\overline{K} \subset V$. A *divisor* D on C is a formal sum

$$D = a_1V_1 + \ldots + a_sV_s,$$

where $a_1,\ldots,a_s \in \mathbb{Z}$ and $V_1,\ldots,V_s$ are pairwise distinct elements of $\mathbb{U}$. Given $f \in \overline{K}(C)$ and $V \in \mathbb{U}$, we denote by $\mathrm{ord}_V(f)$ the order of the function f at V. Let $L(D)$ be the set of functions $f \in \overline{K}(C)$ having $\mathrm{ord}_{V_i}(f) \ge -a_i$

and $\mathrm{ord}_V(f) \geq 0$ for every $V \in \mathbb{U}$, with $V \neq V_i$ $(i = 1, \ldots, s)$. Then $L(D)$ is a finite-dimensional vector space over $\overline{K}$ (see [9]). Furthermore, the *divisor of a function* $f \in \overline{K}(C)$ is defined to be the sum

$$(f) = \sum_V \mathrm{ord}_V(f)V.$$

LEMMA 4.1. *Let $D = a_1V_1 + \ldots + a_sV_s$ be a divisor on C and $\sigma_1, \ldots, \sigma_\mu$ $(\mu \geq 2)$ be a basis of $L(D)$. Let $\xi \in L(D)$ have $\mathrm{ord}_{V_j}(\xi) = -1$ $(j = 1, \ldots, s)$. Then for every $v = (v_1, \ldots, v_\mu) \in \mathbb{Z}^\mu$ the function $\eta(v) = v_1\sigma_1 + \ldots + v_\mu\sigma_\mu$ has s expansions in powers of $1/\xi$ of the form*

$$\eta_j(v) = d_{j,-1}\xi + d_{j,0} + \ldots \qquad (j = 1, \ldots, s).$$

If A is a positive integer, then there are at most $A^{\mu-1}s(s-1)/2$ μ-tuples $v = (v_1, \ldots, v_\mu) \in \mathbb{Z}^\mu$ with $|v_i| \leq A$ $(i = 1, \ldots, \mu)$ such that the leading coefficients $d_{j,-1}$ $(j = 1, \ldots, s)$ of the above expansions are not all distinct. Moreover, if $d_{j,-1}$ $(j = 1, \ldots, s)$ are pairwise distinct, then $\overline{K}(C) = \overline{K}(\xi, \eta)$.

Proof. Let t_j be a local parameter at V_j $(j = 1, \ldots, s)$. Since $\xi, \sigma_i \in L(D)$, we have

$$\sigma_i = c_{i,j,-1}t_j^{-1} + c_{i,j,0} + c_{i,j,1}t_j + \ldots, \qquad \xi = b_{j,-1}t_j^{-1} + b_{j,0} + b_{j,1}t_j + \ldots$$

Since $\mathrm{ord}_{V_j}(\xi) = -1$, it follows that $b_{j,-1} \neq 0$ $(j = 1, \ldots, s)$. Then we may write t_j as an expansion in powers of $1/\xi$ of the form

$$t_j = b_{j,-1}\xi^{-1} + \ldots \qquad (j = 1, \ldots, s).$$

Therefore, $\eta(v)$ has an expansion in powers of $1/\xi$ of the form

$$\eta(v) = d_{j,-1}\xi + d_{j,0} + \ldots,$$

where

$$d_{j,-1} = \sum_{i=1}^{\mu} v_i \frac{c_{i,j,-1}}{b_{j,-1}}.$$

Thus, we have $d_{k,-1} = d_{l,-1}$ if and only if

$$\sum_{i=1}^{\mu} v_i \left(\frac{c_{i,k,-1}}{b_{k,-1}} - \frac{c_{i,l,-1}}{b_{l,-1}} \right) = 0.$$

By [1, Corollary to Lemma 26.2, p. 74], the vectors

$$(c_{1,j,-1}, \ldots, c_{\mu,j,-1}) \qquad (j = k, l)$$

are linearly independent, whence the above linear equation is not trivial. The number of solutions $v = (v_1, \ldots, v_\mu) \in \mathbb{Z}^\mu$ with $|v_i| \leq A$ $(i = 1, \ldots, \mu)$ is at most $A^{\mu-1}$ and we have $s(s-1)/2$ such equations. It follows that there are at most $A^{\mu-1}s(s-1)/2$ μ-tuples $v = (v_1, \ldots, v_\mu) \in \mathbb{Z}^\mu$ with $|v_i| \leq A$ $(i = 1, \ldots, \mu)$ such that $d_{j,-1}$ $(j = 1, \ldots, s)$ are not all distinct.

Finally, [1, Corollary 1, p. 136] implies that if $d_{j,-1}$ $(j = 1, \dots, s)$ are pairwise distinct, then $\overline{K}(C) = \overline{K}(\xi, \eta)$.

LEMMA 4.2. *Let $D = V_1 + \dots + V_N$ be a divisor on C and $\xi, \eta \in K(C)$ be such that $K(C) = K(\xi, \eta)$. Suppose that $\xi, \eta \in L(D)$ and $\operatorname{ord}_{V_i}(\xi) = \operatorname{ord}_{V_i}(\eta) = -1$ $(i = 1, \dots, N)$. Let*

$$\xi = \frac{f_1(X,Y)}{f_0(X,Y)}, \qquad \eta = \frac{f_2(X,Y)}{f_0(X,Y)},$$

where $f_i(X,Y)$ $(i = 0, 1, 2)$ are polynomials of $K[X,Y] - K$ of degree $\le M$. Then there is an absolutely irreducible polynomial

$$G(X,Y) = Y^N + B_1(X)Y^{N-1} + \dots + B_N(X),$$

where $B_i(X) \in K[X]$ with $\deg B_i \le i$ $(i = 1, \dots, N-1)$ and $\deg B_N = N$, such that $G(\xi, \eta) = 0$. Moreover,

$$H(G) \le c(M,N) H(F)^{4NM^2} H(f_0)^{4N^2M} (H(f_1)H(f_2))^{2N^2M},$$

where

$$c(M,N) \le (N+1)^{4NM^2(M+1)} (M+1)^{4NM^2} \times 4^{2N^2M + (4N^2M+1)^2} (4MN)!(N+M)!^{4NM}.$$

Proof. Since $\xi \in L(D)$ and $\operatorname{ord}_{V_i}(\xi) = -1$ $(i = 1, \dots, N)$, we deduce that $[K(C) : K(\xi)] = N$. Let

$$G(\xi, Y) = Y^N + B_1(\xi)Y^{N-1} + \dots + B_N(\xi)$$

be the irreducible polynomial of η over $K(\xi)$. The function has no poles except those of ξ, whence $B_i(\xi) \in K[\xi]$ $(i = 1, \dots, N)$. The rings $V_1, \dots, V_N$ are all the elements of U lying above the ring of $\overline{K}(\xi)$ defined by $1/\xi$. Thus η has N conjugates over $\overline{K}(\xi)$ which are given by the Puiseux expansions of η at infinity:

$$\eta_j = \eta_{j,-1}\xi + \eta_{j,0} + \eta_{j,1}(1/\xi) + \dots \qquad (j = 1, \dots, N),$$

with $\eta_{j,-1} \neq 0$. Hence, $B_i(\xi)$ is, up to sign, the ith elementary symmetric polynomial in N quantities η_j, whence $\deg B_i(\xi) \le i$ $(i = 1, \dots, N-1)$ and $\deg B_N(\xi) = N$.

Consider the polynomials

$$\Phi_1(X,Y,\xi) = f_1(X,Y) - \xi f_0(X,Y), \qquad \Phi_2(X,Y,\eta) = f_2(X,Y) - \eta f_0(X,Y).$$

We denote by $R_1(X,\xi)$ and $R_2(X,\eta)$, respectively, the resultants of $F(X,Y)$, $\Phi_1(X,Y,\xi)$ and $F(X,Y)$, $\Phi_2(X,Y,\eta)$. We have $\deg_\xi R_1 \le N$, $\deg_\eta R_2 \le N$ and $\deg_X R_i \le 2NM$ $(i = 1, 2)$. Lemma 3.2 yields

$$H(R_i) \le (N+M)!(N+1)^M (2(M+1))^N H(F)^M H(\Phi_i)^N \qquad (i = 1, 2).$$

Let $S(\xi,\eta)$ be the resultant of $R_1(X,\xi)$ and $R_2(X,\eta)$ with respect to X. We have $\deg_\xi S \le 2N^2M$, $\deg_\eta S \le 2N^2M$ and Lemma 3.2 implies

$$H(S) \le (4NM)!(N+1)^{4NM}(H(R_1)H(R_2))^{2NM}.$$

Combining the above inequalities, we deduce

$$H(S) \le \Lambda(M,N)H(F)^{4NM^2}H(f_0)^{4N^2M}(H(f_1)H(f_2))^{2N^2M},$$

where

$$\Lambda(M,N) \le (N+1)^{4NM^2(M+1)}(M+1)^{4NM^2}16^{N^2M}(4MN)!(N+M)!^{4NM}.$$

For every $x,y \in \overline{K}$ with $f_0(x,y) \neq 0$ the elements

$$\xi(x,y) = \frac{f_1(x,y)}{f_0(x,y)} \quad \text{and} \quad \eta(x,y) = \frac{f_2(x,y)}{f_0(x,y)}$$

satisfy $G(\xi(x,y),\eta(x,y)) = 0$. On the other hand, we have $\Phi_1(x,y,\xi(x,y)) = 0$ and $\Phi_2(x,y,\eta(x,y)) = 0$, whence $S(\xi(x,y),\eta(x,y)) = 0$. So $G(X,Y)$ divides $S(X,Y)$. Then Lemma 3.3 implies that $H(G) \le 4^{(4N^2M+1)^2}H(S)$. The assertion follows.

LEMMA 4.3. *Suppose that C is of genus 0. Let $D = V_1 + \ldots + V_N$ be a divisor on C and $\{\sigma_1,\ldots,\sigma_{N+1}\}$ be a basis of $L(D)$. Let $\xi \in L(D)$ with $\mathrm{ord}_{V_j}(\xi) = -1$ $(j = 1,\ldots,N)$. For every $v = (v_1,\ldots,v_{N+1})$ in $\mathbb{Z}^{N+1}$ denote by $\Phi_v(\xi,T) = 0$ the irreducible equation of the function*

$$\eta(v) = v_1\sigma_1 + \ldots + v_{N+1}\sigma_{N+1}$$

over $\overline{K}(\xi)$ and by $D_v(\xi)$ the discriminant of $\Phi_v(\xi,T)$ considered as a polynomial with coefficients in $\overline{K}(\xi)$. Let $\Theta(\xi)$ be the product of the factors $(\xi-a)^{e_{a,i}-1}$ where $a \in \mathbb{C}$ and $e_{a,1},\ldots,e_{a,r(a)}$ are the ramification indices of $\eta(v)$ at $\xi = a$. If A is a positive integer, then there are at most $5(2A+1)^N N^2(N-1)^2$ $(N+1)$-tuples $v = (v_1,\ldots,v_{N+1}) \in \mathbb{Z}^{N+1}$ with $|v_i| \le A$ $(i = 1,\ldots,\mu)$ such that $D_v(\xi)$ is not of the form

$$D_v(\xi) = U_v(\xi)^2\Theta(\xi),$$

where $U_v(\xi) \in K[\xi]$ has pairwise distinct roots and distinct from the roots of $\Theta(\xi)$.

Proof. The function $\eta(v)$ has no poles except those of ξ and $[\overline{K}(C) : \overline{K}(\xi)] = N$. Thus, there are $B_i(\xi,v) \in \overline{K}[\xi,v]$ $(i = 1,\ldots,M \le N)$ such that

$$\Phi_v(\xi,T) = B_0(\xi,v)T^M + B_1(\xi,v)T^{M-1} + \ldots + B_M(\xi,v).$$

Since $B_i(\xi,v)$ is, up to sign, the ith elementary symmetric polynomial of the expansions of $\eta(v)$ in powers of $1/\xi$, we deduce that $\deg_\xi B_i \le i$ $(i = 1,\ldots,M)$ and the degree of $B_i(\xi,v)$ in $v_1,\ldots,v_{N+1}$ is at most i. Furthermore, note that V_i $(i = 1,\ldots,N)$ are all the rings lying above the discrete valuation ring of $\overline{K}(\xi)$ defined by $1/\xi$.

Let $a \in \overline{K}$. The conjugates of $\eta(v)$ over $\overline{K}(\xi)$ are given by the Puiseux expansions of $\eta(v)$ at $\xi = a$ which are of the form

$$h_{i,k}(\xi, v) = c_{i,0}(v) + c_{i,1}(v)\zeta_i^k(\xi - a)^{1/e_{a,i}} + \dots$$

where $i = 1, \dots, r(a)$, $k = 0, \dots, e_{a,i} - 1$. It follows that the discriminant $D_v(\xi)$ of $\Phi_v(\xi, T)$ is

$$D_v(\xi) = \prod_{(i,k)\le(j,l)} (h_{i,k}(\xi, v) - h_{j,l}(\xi, v))^2,$$

where $(i, k) \le (j, l)$ means that $i < j$ or $i = j$ and $k < l$. For every index i, there is $D_i(\xi)$ in $\overline{K}[\xi]$ such that

$$\prod_{k<l}(h_{i,k}(\xi) - h_{i,l}(\xi))^2 = (\xi - a)^{e_{a,i}-1}D_i(\xi).$$

Let Γ be the set of $a \in \mathbb{C}$ such that there is $i \in \{1, \dots, r(a)\}$ with $e_{a,i} > 1$. Hence

$$D_v(\xi) = W(\xi, v) \prod_{a\in\Gamma} (\xi - a)^{(e_{a,1}-1)+\dots+(e_{a,r(a)}-1)},$$

where $W(\xi, v) \in \overline{K}[\xi, v]$. When the coefficients $v_1, \dots, v_{N+1}$ are indeterminates with $c_{\kappa,0}(v) \ne c_{\lambda,0}(v)$ for $\kappa, \lambda \in \{1, \dots, r(a)\}$, $\kappa \ne \lambda$ and $c_{i,1}(v) \ne 0$ for $i \in \{1, \dots, r(a)\}$, then $W(\xi, v)$ does not contain factors $\xi - a$ with $a \in \Gamma$.

The Puiseux expansions of σ_j at $\xi = a$ are of the form

$$\sigma_{j,i,k}(\xi) = \tau_{j,i,0} + \tau_{j,i,1}\zeta_i^k(\xi - a)^{1/e_{a,i}} + \dots$$

where $j = 1, \dots, N+1$, $i = 1, \dots, r(a)$, $k = 0, \dots, e_{a,i}-1$. By [1, Corollary to Lemma 26.2, p. 74], any two of the vectors $(\tau_{1,i,0}, \dots, \tau_{N+1,i,0})$ are linearly independent. Thus, for $\kappa, \lambda \in \{1, \dots, r(a)\}$ and $\kappa \ne \lambda$ the equations

$$E(\kappa, \lambda)(v) = (\tau_{1,\kappa,0} - \tau_{1,\lambda,0})v_1 + \dots + (\tau_{N+1,\kappa,0} - \tau_{N+1,\lambda,0})v_{N+1} = 0$$

are non-trivial. So, $c_{\kappa,0}(v) = c_{\lambda,0}(v)$ if and only if $E(\kappa, \lambda)(v) = 0$. Furthermore, [1, Corollary to Lemma 26.2, p. 74] implies that for every $i \in \{1, \dots, r(a)\}$ the coefficients $\tau_{1,i,1}, \dots, \tau_{N+1,i,1}$ are not all zero. Thus, the equations

$$Z_i(v) = \tau_{1,i,1}v_1 + \dots + \tau_{N+1,i,1}v_{N+1} = 0 \quad (i = 1, \dots, r(a))$$

are non-trivial. Hence, $c_{i,1}(v) = 0$ if and only if $Z_i(v) = 0$. For a positive integer A the number of $v = (v_1, \dots, v_{N+1}) \in \mathbb{Z}^{N+1}$ with $|v_i| \le A$ $(i = 1, \dots, N + 1)$ such that at least one of the equations $E(\kappa, \lambda)(v) = 0$, $Z_i(v) = 0$ has a solution is at most $(2A + 1)^N(N + N(N - 1)/2)$.

Let ϱ be a zero of $W(\xi, v)$. Then ϱ must be a zero of one of the factors $h_{i,k}(\xi) - h_{j,l}(\xi)$ and each such factor occurs twice in $D_v(\xi)$. Hence the factor $\xi - \varrho$ occurs an even number of times in $D_v(\xi)$. It follows that there is

a polynomial $U(\xi, v)$ such that $W(\xi, v) = U(\xi, v)^2$. Since $\deg_\xi D_v(\xi) \le 2N(N-1)$, we get $|\Gamma| \le 2N(N-1)$. Furthermore, the degree of $U(\xi, v)$ in $v_1, \dots, v_{N+1}$ is at most $N(N-1)$. We deduce that the number of $v = (v_1, \dots, v_{N+1})$ with $v_i \in \mathbb{Z}$ and $|v_i| \le A$ $(i = 1, \dots, N+1)$ satisfying one of the equations

$$U(a, v) = 0, \quad a \in \Gamma,$$

is at most $(2A+1)^N 2N^2(N-1)^2$. Let $\Delta(v)$ be the discriminant of $U(\xi, v)$ considered as a polynomial with coefficients in $\overline{K}[v]$. Since the degree of $\Delta(v)$ in $v_1, \dots, v_{N+1}$ is at most $2N^2(N-1)^2$, the number of $v = (v_1, \dots, v_{N+1})$ with $v_i \in \mathbb{Z}$ and $|v_i| \le A$ $(i = 1, \dots, N+1)$ such that $\Delta(v) = 0$ is at most $(2A+1)^N 2N^2(N-1)^2$. Therefore, the number of $v = (v_1, \dots, v_{N+1})$ with $v_i \in \mathbb{Z}$ and $|v_i| \le A$ $(i = 1, \dots, N+1)$ such that $U(\xi, v)$ has no distinct roots or there is $a \in \Gamma$ satisfying $U(a, v) = 0$ is at most $(2A+1)^N 4N^2(N-1)^2$. Finally, there are at most $5(2A+1)^N N^2(N-1)^2$ $(N+1)$-tuples $v = (v_1, \dots, v_{N+1}) \in \mathbb{Z}^{N+1}$ with $|v_i| \le A$ $(i = 1, \dots, \mu)$ such that $D_v(\xi)$ is not of the form

$$D_v(\xi) = U(\xi, v)^2 \prod_{a \in \Gamma} (\xi - a)^{e_{a,1} + \dots + e_{a,r(a)} - r(a)},$$

with $U(\xi, v)$ having pairwise distinct roots and distinct from the elements of Γ.

LEMMA 4.4. *Let $f(X, Y) = 0$ be an irreducible curve of degree n in Y defined over $\overline{K}$. For $a \in \mathbb{C}$ denote by $e_{a,1}, \dots, e_{a,r(a)}$ the ramification indices of Y at $X = a$. Assume that the following conditions are satisfied*:

(a) *The Puiseux expansions $\mathbf{y}_i(X)$ $(i = 1, \dots, n)$ at $X = \infty$ of the algebraic function Y defined by $f(X, Y) = 0$ are*

$$\mathbf{y}_i(X) = b_{i,-1} X + b_{i,0} + b_{i,1} X^{-1} + \dots \qquad (i = 1, \dots, n)$$

with leading coefficients $b_{i,-1}$ pairwise distinct, and Y has no other poles.

(b) *The discriminant of $f(X, Y)$, considered as a polynomial with coefficients in $\overline{K}[X]$, is of the form*

$$D(X) = U(X)^2 \Theta(X)$$

where $\Theta(X)$ is the product of the factors $(X - a)^{e_{a,i} - 1}$ with $a \in \mathbb{C}$, $i = 1, \dots, r(a)$, and $U(X)$ has pairwise distinct roots and distinct from the roots of $\Theta(X)$.

Then the curve $f(X, Y) = 0$ has no singularities other than double ordinary points.

Proof. See [1, Theorem 57.1, p. 161].

4.3. *On the bases of Riemann–Roch spaces.* Let $F(X,Y,Z)$ be a homogeneous absolutely irreducible polynomial in $K[X,Y,Z]$ of degree $N \geq 3$ such that the curve C defined by $F(X,Y,Z)=0$ is of genus 0. If P is a point on C, we denote by O_P the local ring of C at P.

LEMMA 4.5. *Let $\{P_1,\dots,P_N\}$ be a K-rational subset of simple points of C. Put $D = O_{P_1}+\ldots+O_{P_N}$. Let T be the set of $a \in \overline{K}$ such that there is a ring O_{P_i} lying above $X=a$. Denote by $M(T)$ and $\Pi(T)$, respectively, the maximum and the product of $H(a)$ with $a \in T$. Then there exist polynomials $G_i(X,Y) \in K[X,Y]$ $(i=1,\dots,N+1)$ and $E(X) \in K[X]$ with $\deg_X G_i \leq 2N^2+4N$, $\deg_Y G_i < N$, $\deg E \leq N^2$ and*

$$H(G_i) < (9N^6 H(F) M(T))^{366N^{11}}, \qquad H(E) < (N+1)^{5N^3} H(F)^{2N^3} \Pi(T),$$

such that the functions ϕ_i $(i=1,\dots,N+1)$ on C defined by the fractions G_i/E $(i=1,\dots,N+1)$ form a basis of the space $L(D)$.

P r o o f. By the Riemann–Roch theorem, the space $L(D)$ has dimension $N+1$. By [18, Theorem A2], there are polynomials $E(X)$ and $G_i(X,Y)$ $(i=1,\dots,N+1)$ such that $G_i(X,Y)/E(X)$ $(i=1,\dots,N+1)$ represent a basis of $L(D)$. Since the divisor D is defined over K, [18, Theorem B2] implies that we may take the polynomials $E(X)$ and $G_i(X,Y)$ $(i=1,\dots,N+1)$ to have coefficients in K.

Let $D(X)$ be the discriminant of $F(X,Y,1)$ considered as a polynomial with coefficients in $K[X]$. We have $\deg D \leq 2N(N-1)$. By [18, Theorem A2], we get

$$\deg E \leq \frac{\deg D}{2} + N \leq N^2$$

and the roots of $E(X)$ are among the roots of $D(X)$ and the elements of T. Further, we can assume that the leading coefficient of $E(X)$ is 1. Let

$$E(X) = (X-\varrho_1)\dots(X-\varrho_r).$$

Let $R(X)$ be the resultant of $F(X,Y,1)$ and $F_Y(X,Y,1)$ with respect to Y. If ϱ_i is a root of $D(X)$, then $R(\varrho_i)=0$ and Lemma 3.1 yields $H(\varrho_i) \leq 2H(R)$. By [21, Theorem 5.9, p. 211], we have

$$H(E) \leq 2^{N^2-1} H(\varrho_1)\dots H(\varrho_r) \leq 4^{N^2} H(R)^{N^2} \Pi(T).$$

Lemma 3.2 implies

$$H(R) < (N+1)^{5N-2} H(F)^{2N-1}.$$

Hence

$$H(E) < (N+1)^{5N^3-N^2} H(F)^{2N^3} \Pi(T).$$

By [18, Theorem A2], we have

$$\deg_X G_i \leq 2N^2+4N.$$

Let $F(X,Y,1) = a_0(X)Y^n + \ldots + a_n(X)$. Following the notation of [17], we have

$$G_i(X,Y) = b_{i1}(X) + b_{i2}(X)y_2(X,Y) + \ldots + b_{in}(X)y_n(X,Y) \qquad (i = 1,\ldots,N+1),$$

where

$$y_j(X,Y) = a_0(X)Y^{j-1} + a_1(X)Y^{j-2} + \ldots + a_{j-2}(X)Y \quad (j = 2,\ldots,n)$$

and $b_{ij}(X) \in L[X]$. From [18, pp. 204, 209 and 196], we get

$$b_{ij}(X) = \delta_{ij0} + \delta_{ij1}X + \ldots + \delta_{ij\nu}X^\nu$$

with $\nu \le 2N^2 + 3N$. By [18, Lemma 26] the vector $\delta_i = \{\delta_{ijp}\}_{1\le j\le n, 0\le p\le \nu}$ has height

$$H(\delta_i) < (9N^6 H(F)M(T))^{365N^{11}}.$$

We have

$$\begin{aligned} G_i(X,Y) &= \sum_{j=1}^{n} b_{ij}(X)y_j(X,Y) \\ &= b_{i1}(X) + (b_{i2}(X)a_0(X) + \ldots + b_{in}(X)a_{n-2}(X))Y \\ &\quad + \ldots + b_{in}(X)a_0(X)Y^{n-1}. \end{aligned}$$

By the proof of Theorem C2 of [18], we can choose a vector δ_i such that one of the δ_{ijp} is 1. Further, we may suppose, without loss of generality, that one of the coefficients of $F(X,Y)$ is 1. Then we obtain

$$H(G_i) < 7N^3 H(\delta_i)H(F) < (9N^6 H(F)M(T))^{366N^{11}}.$$

LEMMA 4.6. *Let $B = \{P_1,\ldots,P_N\}$ and $\Gamma = \{Q_1,\ldots,Q_N\}$ be two K-rational subsets of simple points of C with $B \cap \Gamma = \emptyset$. Let T be the set of $a \in \overline{K}$ such that there exists a local ring O_P with $P \in B$ lying above $X = a$. Denote by $M(B)$ and $M(\Gamma)$, respectively, the maximum of $H(a)$ with $a \in T$ and the maximum of $H(Q_j)$ $(j = 1,\ldots,N)$. Then there are two polynomials $G \in K[X,Y]$, $E(X) \in K[X]$ with $\deg_X G \le 2N^2 + 4N$, $\deg_Y G < N$, $\deg E \le N^2$ and heights satisfying*

$$H(G) < (9N^6 H(F)M(B))^{655N^{13}} M(\Gamma)^{5N^4}$$

and

$$H(E) < (N+1)^{5N^3} H(F)^{2N^3} \prod_{a\in T} H(a)$$

such that the fraction G/E defines a function ϕ on C with divisor

$$(\phi) = O_{Q_1} + \ldots + O_{Q_N} - O_{P_1} - \ldots - O_{P_N}.$$

P r o o f. By Lemma 4.5, there exist polynomials $G_i(X,Y) \in K[X,Y]$ $(i=1,\dots,N+1)$ and $E(X) \in K[X]$ with $\deg_X G_i \le 2N^2+4N$, $\deg_Y G_i < N$, $\deg E \le N^2$ and

$$H(G_i) < (9N^6 H(F)M(B))^{366N^{11}},$$
$$H(E) < (N+1)^{5N^3} H(F)^{2N^3} \prod_{a\in T} H(a),$$

such that the functions ϕ_i $(i=1,\dots,N+1)$ on C defined by the fractions G_i/E $(i=1,\dots,N+1)$ form a basis of the space $L(O_{P_1}+\dots+O_{P_N})$. Let $G_{h,i}$ be the homogenization of G_i. Consider the linear system

$$G_{h,1}(Q_j)X_1 + \dots + G_{h,N+1}(Q_j)X_{N+1} = 0 \quad (j=1,\dots,N).$$

Let r be the rank of the system and suppose that the vectors

$$Z_j = (G_{h,1}(Q_j),\dots,G_{h,N+1}(Q_j)) \quad (j=1,\dots,r)$$

are linearly independent. Since Γ is a K-rational set, Lemma 3.6 implies that the system has a non-trivial solution $x_1,\dots,x_{N+1} \in K$ satisfying

$$H(x_1,\dots,x_{N+1}) \le N! H(Z_1)\dots H(Z_r).$$

We have

$$H(G_{h,i}(Q_j)) < 8N^4 H(G_i) H(Q_j)^{2N^2+5N},$$

whence

$$\begin{aligned} H(Z_j) &< H(G_{h,1}(Q_j))\dots H(G_{h,N+1}(Q_j)) \\ &< (9N^6 H(F)M(B))^{489N^{12}} M(\Gamma)^{5N^3}. \end{aligned}$$

Hence

$$H(x_1,\dots,x_{N+1}) < (9N^6 H(F)M(B))^{490N^{13}} M(\Gamma)^{5N^4}.$$

Thus, the polynomial $G = x_1G_1 + \dots + x_{N+1}G_{N+1}$ has

$$\begin{aligned} H(G) &< (N+1)H(x_1,\dots,x_{N+1})H(G_1)\dots H(G_{N+1}) \\ &< (9N^6 H(F)M(B))^{655N^{13}} M(\Gamma)^{5N^4} \end{aligned}$$

and satisfies $G(Q_j) = 0$ $(j=1,\dots,N)$. Therefore, the function ϕ on C defined by the fraction G/E has divisor

$$(\phi) = O_{Q_1} + \dots + O_{Q_N} - O_{P_1} - \dots - O_{P_N}.$$

4.4. *Proof of Theorem 4.1.* First, suppose that $\deg_Y F = N$ and C_∞ has N simple points. Since the resultant $R(X)$ of $F(X,Y)$ and $F_Y(X,Y)$ with respect to Y has degree $< 2N^2$, there is an integer a with $|a| < N^2$ such that the points $P_i = (a_i : b_i : 1)$ $(i=1,\dots,N)$ on C above $X=a$ are all simple. Put $D = O_{P_1} + \dots + O_{P_N}$. By Lemma 4.5, there exist $G_i(X,Y) \in$

$K[X,Y]$ $(i=1,\dots,N+1)$ and $E(X)\in K[X]$ with $\deg_X G_i \le 2N^2+4N$, $\deg_Y G_i < N$, $\deg E \le N^2$ and

$$H(G_i) < (9N^8H(F))^{366N^{11}}, \quad H(E) < (N+1)^{5N^3}H(F)^{2N^3},$$

such that the functions ϕ_i $(i=1,\dots,N+1)$ on C defined by the fractions G_i/E $(i=1,\dots,N+1)$ form a basis of $L(D)$.

For simplicity we denote by $\mathrm{ord}_i(f)$ the order of a function f at O_{P_i}. Suppose that there is $j\in\{1,\dots,N\}$ with $\mathrm{ord}_j(\phi_k)\ge 0$ $(k=1,\dots,N+1)$. Then $L(D)=L(D-V_j)$, which is a contradiction, because by the Riemann–Roch theorem $\dim L(D-V_j)=\dim L(D)-1$. Thus, for every $j\in\{1,\dots,N\}$ there is $k(j)\in\{1,\dots,N+1\}$ such that $\mathrm{ord}_j(\phi_{k(j)})=-1$. The Puiseux expansion of ϕ_r at O_{P_i} is of the form

$$\phi_{r,i}=c_{r,i,-1}t_i^{-1}+c_{r,i,0}+c_{r,i,1}t_i+\dots,$$

where t_i is a local parameter at O_{P_i}. The coefficients $c_{r,i,-1}$ $(r=1,\dots,N+1)$ are not all zero. For every $(N+1)$-tuple $\lambda=(\lambda_1,\dots,\lambda_{N+1})\in\mathbb{Z}^{N+1}$, put $\eta(\lambda)=\lambda_1\phi_1+\dots+\lambda_{N+1}\phi_{N+1}$. If A is a positive integer, then the number of $(N+1)$-tuples $\lambda=(\lambda_1,\dots,\lambda_{N+1})\in\mathbb{Z}^{N+1}$ with $|\lambda_j|<A$ $(j=1,\dots,N+1)$ satisfying at least one of the equations

$$\lambda_1c_{1,i,-1}+\dots+\lambda_{N+1}c_{N+1,i,-1}=0 \quad (i=1,\dots,N)$$

is at most $(2A+1)^NN$. Hence, the number of $(N+1)$-tuples $\lambda=(\lambda_1,\dots,\lambda_{N+1})\in\mathbb{Z}^{N+1}$ with $|\lambda_j|\le A$ $(j=1,\dots,N+1)$ such that $\eta(\lambda)$ has $\mathrm{ord}_{V_i}(\eta(\lambda))\ge 0$ for some $i\in\{1,\dots,N\}$, is at most $(2A+1)^NN$. Then there is $\mu=(\mu_1,\dots,\mu_{N+1})$ in $\mathbb{Z}^{N+1}$ with $|\mu_j|\le (N+1)/2$ $(j=1,\dots,N+1)$, such that the function $\xi=\eta(\mu)$ has $\mathrm{ord}_i(\xi)=-1$ $(i=1,\dots,N)$. Then ξ is defined by the fraction Ξ/E where $\Xi\in K[X,Y]$ with $\deg_X\Xi\le 2N^2+4N$, $\deg_Y\Xi<N$ and height

$$H(\Xi)<N^2(9N^8H(F))^{366N^{11}(N+1)}.$$

Lemma 4.1 implies that for every $\lambda=(\lambda_1,\dots,\lambda_{N+1})\in\mathbb{Z}^{N+1}$ the function $\eta(\lambda)$ has N expansions in powers of $1/\xi$ of the form

$$\eta_j(\lambda)=d_{j,-1}\xi+d_{j,0}+\dots \quad (j=1,\dots,N)$$

and there are at most $(2A+1)^NN(N-1)/2$ $(N+1)$-tuples $\lambda=(\lambda_1,\dots,\lambda_{N+1})\in\mathbb{Z}^{N+1}$ with $|\lambda_i|\le A$ $(i=1,\dots,N+1)$, such that the leading coefficients $d_{j,-1}$ $(j=1,\dots,N)$ of the above expansions are not all distinct. Hence, for $A\ge 1+N(N-1)/2$ there is $v=(v_1,\dots,v_{N+1})$ in $\mathbb{Z}^{N+1}$ with $|v_i|\le A$ $(i=1,\dots,N+1)$ such that the coefficients $d_{j,-1}$ $(j=1,\dots,N)$ of the expansions of $\eta(v)$ are pairwise distinct. Then Lemma 4.1 yields $K(C)=K(\xi,\eta(v))$. Since we have $\mathrm{ord}_{V_i}(\xi)=-1$ $(i=1,\dots,N)$ and ξ has no other poles, it follows that $[K(C):K(\xi)]=N$.

We denote by $\Phi_v(\xi,T)=0$ the absolutely irreducible equation satisfied by $\eta(v)$ over $K(\xi)$, and let $D_v(\xi)$ be the discriminant of $\Phi_v(\xi,T)$ considered as a polynomial with coefficients in $K(\xi)$. Let $\Theta(\xi)$ be the product of the factors $(\xi-a)^{e_{a,i}-1}$ where $a\in\mathbb{C}$ and $e_{a,1},\dots,e_{a,r(a)}$ are the ramification indices of $\eta(v)$ at $\xi=a$. By Lemma 4.3, there are at most $5(2A+1)^N N^2(N-1)^2\ (N+1)$-tuples $v=(v_1,\dots,v_{N+1})\in\mathbb{Z}^{N+1}$ with $|v_i|\le A\ (i=1,\dots,\mu)$ such that $D_v(\xi)$ is not of the form

$$D_v(\xi)=U_v(\xi)^2\Theta(\xi),$$

where $U_v(\xi)$ has pairwise distinct roots which are distinct from the roots of $\Theta(\xi)$. Then there exists $v=(v_1,\dots,v_{N+1})$ in $\mathbb{Z}^{N+1}$ with $|v_i|\le 3N^2(N-1)^2$ $(i=1,\dots,N+1)$ such that $\eta(v)$ generates $K(C)$ over $K(\xi)$, $\operatorname{ord}_{V_i}(\eta(v))=-1\ (i=1,\dots,N)$, and the discriminant $D_v(\xi)$ of the irreducible polynomial $\Phi_v(\xi,T)$ of $\eta(v)$ over $K(\xi)$ has the form

$$D_v(\xi)=U_v(\xi)^2\Theta(\xi),$$

where $U_v(\xi)$ has pairwise distinct roots which are distinct from the roots of $\Theta(\xi)$. By Lemma 4.4, the equation $\Phi_v(\xi,T)=0$ is a model of the curve C having no singularities other than double ordinary points.

Put $\eta=\eta(v)$ and $\Phi(\xi,T)=\Phi_v(\xi,T)$. The function η is defined by the fraction Θ/E where $\Theta\in K[X,Y]$ with $\deg_X\Theta\le 2N^2+4N$, $\deg_Y\Theta<N$ and height

$$H(\Theta)<3N^5(9N^8H(F))^{366N^{11}(N+1)}.$$

By Lemma 4.2,

$$H(\Phi)<4^{217N^8}(N+1)^{257N^7}H(F)^{54N^5}H(E)^{15N^4}(H(\Theta)H(\Xi))^{8N^4}.$$

Furthermore, $\deg\Phi=N$. Using the inequalities for the heights of Θ, Ξ and E we obtain

$$H(\Phi)<(9N^8H(F))^{7810N^{16}}.$$

We denote by $\Phi_h(U,V,W)$ the homogenization of the polynomial Φ. Thus, we have a birational map Ω from the plane curve $F(X,Y,Z)=0$ to $\Phi_h(U,V,W)$ defined by $\Omega(x:y:1)=(\xi(x,y):\eta(x,y):1)$.

Next, we determine the inverse map of Ω. Let $B=\{\Omega(P_1),\dots,\Omega(P_N)\}$ and $\Gamma=\Omega(C_\infty)=\{Q_1,\dots,Q_N\}$. Since we have $\operatorname{ord}_i(\xi)=\operatorname{ord}_i(\eta)=-1$ $(i=1,\dots,N)$, the points $\Omega(P_i)$ on the curve $\Phi_h(U,V,W)=0$ are at infinity. Furthermore,

$$H(Q_j)<(9N^8H(F))^{367N^{11}(N+1)}\quad(j=1,\dots,N).$$

Thus, Lemma 4.6 implies that there are $G\in K[X,Y]$ and $J(X)\in K[X]$ with $\deg_X G\le 2N^2+4N$, $\deg_Y G<N$, $\deg J\le N^2$ and heights

$$H(G)<(9N^8H(F))^{2475N^{16}},\quad H(J)<(N+1)^{5N^3}H(F)^{2N^3}$$

such that the fraction G/J defines a function ϕ on C with divisor

$$(\phi) = O_{Q_1} + \ldots + O_{Q_N} - O_{\Omega(P_1)} - \ldots - O_{\Omega(P_N)}.$$

The divisor of the function $\phi \circ \Omega$ coincides with the divisor of $x - a$, whence there is $c \in K$ such that $x - a = c\phi(\xi, \eta)$. Thus

$$x = \frac{cG(\xi, \eta) + aJ(\xi)}{J(\xi)}.$$

Suppose that $a \neq 0$. Let P_0 be a point on C with x-coordinate equal to 0. Then $H(P_0) < 2H(F)$. We have

$$H(\Omega(P_0)) < 9N^4 H(\Xi)H(\Theta)H(E)(2H(F))^{2N^2+5N}$$

and

$$H(\phi(\Omega(P_0))) < 9N^4 H(G)H(J)H(\Omega(P_0))^{2N^2+5N}.$$

Combining the above inequalities, we obtain

$$H(\phi(\Omega(P_0))) < (9N^8 H(F))^{2875N^{16}}.$$

Thus

$$H(c) \leq H(a)H(\phi(\Omega(P_0))) < (9N^8 H(F))^{2876N^{16}}.$$

So, we deduce that

$$H(cG + aJ) < 2N^2 H(c)H(G)H(J) < (9N^8 H(F))^{5352N^{16}}.$$

In the same way, we deduce a similar expression for y. Finally, Lemma 3.7 yields the assertion.

5. Rational points on conics and proof of Theorem 2.3

5.1. *Conics*. In this section we obtain an upper bound for the minimal solution of a homogeneous quadratic form in three variables. Using this result and Theorem 2.1 we prove Theorem 2.3.

Lemma 5.1. *Let*

$$G(X, Y, Z) = AX^2 + BXY + CY^2 + DXZ + EYZ + FZ^2 = 0,$$

be a (non-zero) quadratic form in X, Y, Z with $A, B, C, D, E, F \in K$. Suppose that the equation $G(X, Y, Z) = 0$ has a solution in K. Then there exist $x, y, z \in K$ such that $G(x, y, z) = 0$ and

$$H(x, y, z) \leq 45 \cdot 10^4 |D_K|^{15/(2d)} H(G)^{11}.$$

When $K = \mathbb{Q}$, we have

$$H(x, y, z) < 30H(G).$$

Proof. If a is an algebraic number and $a = a^{(1)}, \ldots, a^{(s)}$ are its conjugates, then we put $\|a\| = \max\{|a^{(1)}|, \ldots, |a^{(s)}|\}$. Consider the equation

$$aX^2 + bY^2 + cZ^2 = 0,$$

where a, b, c are integers in K, and suppose that it has a solution in integers of K. Then [20] implies that there exists a solution of the above equation in integers x, y, z of K satisfying

$$\max\{\|x/\sqrt{bc}\|, \|y/\sqrt{ac}\|, \|z/\sqrt{ab}\|\} < 6|D_K|^{2/d}.$$

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

$$\max\{|x|_v, |y|_v, |z|_v\} < 6|D_K|^{2/d} \max\{|a|_v, |b|_v, |c|_v\}.$$

It follows that

$$H(x, y, z) < 6|D_K|^{2/d} H(a, b, c, 1).$$

Consider now the conic given by the equation

$$G(X, Y, Z) = \alpha X^2 + \beta XY + \gamma Y^2 + \delta XZ + \varepsilon YZ + \zeta Z^2 = 0,$$

where $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ are integers of K, and suppose that it has a point rational over K. We have the following cases:

(i) $\beta = 0$ and $\alpha\gamma \neq 0$. Putting $X = X' + hZ'$, $Y = Y' + kZ'$ and $Z = Z'$ we take

$$G(X', Y', Z') = \alpha X'^2 + \gamma Y'^2 + (2\alpha h + \delta)X'Z' + (2\gamma k + \varepsilon)Y'Z' + G(h, k, 1)Z'^2.$$

Next, setting $h = -\delta/(2\alpha)$, $k = -\varepsilon/(2\gamma)$ and multiplying by $4\alpha\gamma$ we obtain the equation

$$\Gamma(X', Y', Z') = 4\alpha^2\gamma X'^2 + 4\alpha\gamma^2 Y'^2 + (-\delta^2\gamma - \varepsilon^2\alpha + 4\alpha\gamma\zeta)Z'^2 = 0.$$

Putting $U = 2\alpha X'$, $V = 2\gamma Y'$ and $W = Z'$, we get the equation

$$\Theta(U, V, W) = \gamma U^2 + \alpha V^2 + (-\delta^2\gamma - \varepsilon^2\alpha + 4\alpha\gamma\zeta)W^2 = 0.$$

Then the equation $\Theta(U, V, W) = 0$ has a solution in integers of K. It follows that there are integers u, v, w of K such that $\Theta(u, v, w) = 0$ and

$$H(u, v, w) < 6|D_K|^{2/d} H(\alpha, \gamma, -\delta^2\gamma - \varepsilon^2\alpha + 4\alpha\gamma\zeta, 1).$$

Thus $x = (u - \delta w)/(2\alpha)$, $y = (v - \varepsilon w)/(2\gamma)$ and $z = w$ is a solution of $G(X, Y, Z) = 0$ with

$$H(x, y, z) < 2H(u, v, w)H(\alpha, \gamma, \delta, \varepsilon, 1)^2.$$

Since

$$H(\alpha, \gamma, -\delta^2\gamma - \varepsilon^2\alpha + 4\alpha\gamma\zeta, 1) \leq 6H(\alpha, \gamma, \delta, \varepsilon, \zeta, 1)^3,$$

we deduce that

$$H(x, y, z) < 72|D_K|^{2/d} H(\alpha, \gamma, \delta, \varepsilon, \zeta, 1)^5.$$

(ii) $\beta = 0$ and $\alpha\gamma = 0$. If $\beta = \alpha = 0$, then the rational solutions of the equation $G(X, Y, Z) = 0$ over K are the triples (x, y, z) with $y, z \in K$ and $\delta x = -(\gamma y^2 + \varepsilon yz + \zeta z^2)/z$. Taking $y = 0$ and $z = 1$, we have $x = \zeta/\delta$ and the height of this solution is $H(\zeta/\delta, 0, 1) \leq H(G)$. If $\beta = \gamma = 0$, then we similarly obtain a solution of $G(X, Y, Z) = 0$ over K with height $\leq H(G)$.

(iii) $\beta \neq 0$ and $\alpha = \gamma = 0$. Putting $X = X' - Y'$, $Y = X' + Y'$ and $Z = Z'$ we have the equation

$$\Gamma(X', Y', Z') = \beta X'^2 - \beta Y'^2 + (\delta + \varepsilon)X'Z' + (\varepsilon - \delta)Y'Z' + \zeta Z'^2 = 0.$$

Furthermore, $H(\beta, \delta + \varepsilon, \varepsilon - \delta, \zeta, 1) \leq 2H(\beta, \delta, \varepsilon, \zeta, 1)$. By the case (i), there are integers u, v, w of K with

$$H(u, v, w) < 2304|D_K|^{2/d} H(\alpha, \gamma, \delta, \varepsilon, \zeta, 1)^5$$

such that $\Gamma(u, v, w) = 0$. Thus, $x = u - v$, $y = u + v$ and $z = w$ is a solution of the equation $G(X, Y, Z) = 0$ satisfying

$$H(x, y, z) < 2H(u, v, w) < 4608|D_K|^{2/d} H(\alpha, \gamma, \delta, \varepsilon, \zeta, 1)^5.$$

(iv) $\beta \neq 0$ and $\alpha \neq 0$. The transformation $X = X' - \beta Y'/(2\alpha)$, $Y = Y'$ and $Z = Z'$ gives the equation

$$\begin{aligned}\Gamma(X', Y', Z') = \alpha X'^2 + (\gamma + (-\beta^2/(4\alpha)))Y'^2 \\ + \delta X'Z' + (\varepsilon + (-\delta\beta/(2\alpha)))Y'Z' + \zeta Z'^2.\end{aligned}$$

Multiplying by 4α and putting $U = 2\alpha X'$, $V = Y'$ and $W = 2Z'$, we get the equation

$$\Theta(U, V, W) = U^2 + (4\alpha\gamma - \beta^2)V^2 + \delta UW + (2\alpha\varepsilon - \delta\beta)VW + \alpha\zeta W^2 = 0.$$

We have

$$H(1, 4\alpha\gamma - \beta^2, \delta, 2\alpha\varepsilon - \delta\beta, \alpha\zeta) \leq 5H(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, 1)^2.$$

By (i), there are integers u, v, w of K such that $\Theta(u, v, w) = 0$ and

$$H(u, v, w) < 72|D_K|^{2/d} H(1, 4\alpha\gamma - \beta^2, \delta, 2\alpha\varepsilon - \delta\beta, \alpha\zeta)^5.$$

Hence

$$H(u, v, w) < 225000|D_K|^{2/d} H(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, 1)^{10}.$$

Thus $x = (u - \beta v)/(2\alpha)$, $y = v$ and $z = w/2$ is a solution of $G(X, Y, Z) = 0$ having

$$\begin{aligned}H(x, y, z) &\leq 2H(u, v, w)H(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, 1) \\ &< 450000|D_K|^{2/d} H(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, 1)^{11}.\end{aligned}$$

(v) $\beta \neq 0$ and $\gamma \neq 0$. We obtain the same bound as in (iv).

Next, consider

$$G(X, Y, Z) = AX^2 + BXY + CY^2 + DXZ + EYZ + FZ^2 = 0$$

with $A, B, C, D, E, F \in K$. Let $A \neq 0$. By the proof of [14, Lemma 1], there is an integer Δ of K such that $\Delta B/A$, $\Delta C/A$, $\Delta D/A$, $\Delta E/A$, $\Delta F/A$ are integers of K and

$$\begin{aligned}H(1, \Delta, \Delta B/A, \Delta C/A, \Delta D/A, \Delta E/A, \Delta F/A) \\ < |D_K|^{1/(2d)} H(1, B/A, C/A, D/A, E/A, F/A).\end{aligned}$$

We put

$$g(X,Y,Z) = \alpha X^2 + \beta XY + \gamma Y^2 + \delta XZ + \varepsilon YZ + \zeta Z^2 = 0,$$

where $\alpha = \Delta$, $\beta = \Delta B/A$, $\gamma = \Delta C/A$, $\delta = \Delta D/A$, $\varepsilon = \Delta E/A$ and $\zeta = \Delta F/A$. Suppose that the equation $G(X,Y,Z) = 0$ has a solution in K. It follows that there are $x_1, x_2, x_3 \in K$ such that $g(x_1,x_2,x_3) = 0$ and

$$\begin{aligned} H(x_1,x_2,x_3) &< 450000|D_K|^{2/d} H(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta,1)^{11} \\ &< 450000|D_K|^{15/(2d)} H(G)^{11}. \end{aligned}$$

When $K = \mathbb{Q}$, [16, Theorem 1] implies that there are $x_1, x_2, x_3 \in K$ satisfying

$$H(x_1,x_2,x_3) < 30H(G).$$

Remark. In [16], there is a generalization of the result of [20] in the case of a homogeneous quadratic form in many variables. Using [16, Theorem 1] we deduce that there exist $x, y, z \in K$ such that $G(x,y,z) = 0$ and

$$H(x,y,z) \le 30|D_K|^{(3+d)/(2d)} H(G)^d.$$

Note that Lemma 5.1 gives better estimates for the exponents of $H(G)$ and $|D_K|$.

Lemma 5.2. *Let*

$$G(X,Y) = \alpha X^2 + \beta XY + \gamma Y^2 + \delta XZ + \varepsilon YZ + \zeta Z^2 = 0$$

be a (non-zero) quadratic form in X, Y with $\alpha,\beta,\gamma,\delta,\varepsilon,\zeta \in K$. Suppose that the equation $G(X,Y) = 0$ has a solution (x,y) with $x, y \in K$. Then there are polynomials $f_1(T), f_2(T), f_3(T) \in K[T]$ of degree ≤ 2 with

$$H(f_1), H(f_2) \le 3H(x,y,1)H(G), \qquad H(f_3) \le H(G)$$

such that

$$X = \frac{f_1(T)}{f_3(T)}, \qquad Y = \frac{f_2(T)}{f_3(T)}.$$

Proof. Putting $Y = y + T(X - x)$ in the equation $G(X,Y) = 0$, we get $X = f_1(T)/f_3(T)$ and $Y = f_2(T)/f_3(T)$, where

$$\begin{aligned} f_1(T) &= \alpha x T^2 - (2\alpha y + \varepsilon)T - \beta x - \gamma y, \\ f_2(T) &= (-\alpha y + \varepsilon + \gamma x)T^2 - 2\beta x T + \beta y, \\ f_3(T) &= T^2 + \gamma T + \beta. \end{aligned}$$

We easily obtain

$$H(f_1), H(f_2) \le 3H(x,y,1)H(G), \qquad H(f_3) \le H(G).$$

5.2. *Proof of Theorem 2.3.* If $N = 2$, then Lemmas 5.1 and 5.2 give the result. Thus, suppose $N \ge 3$. By Theorem 2.1, there is a conic Γ defined

over K of equation $G(X,Y)=0$ with

$$H(G) < (9N^{5N+4}H(F))^{13\cdot 10^4 N^{28}}$$

and a birational map $\Phi : C \to \Gamma$ given by

$$\Phi(X,Y) = \left(\frac{\phi_1(X,Y)}{\phi_3(X,Y)}, \frac{\phi_2(X,Y)}{\phi_3(X,Y)}\right),$$

where $\phi_i(X,Y) \in K[X,Y]$ $(i=1,2,3)$ with $\deg \phi_i < 3N^3$ and

$$H(\phi_i) < (9N^{5N+4}H(F))^{980N^{13}} \qquad (i=1,2,3).$$

The inverse map of Φ is given by

$$\Phi^{-1}(X,Y) = \left(\frac{\tau_1(X,Y)}{\tau_2(X,Y)}, \frac{\tau_3(X,Y)}{\tau_4(X,Y)}\right),$$

where $\tau_i(X,Y) \in K[X,Y]$ $(i=1,2,3,4)$ with $\deg \tau_i < 15N^3$ and

$$H(\tau_i) < \begin{cases} (9N^{5N+4}H(F))^{5355N^{16}} & (i=1,3), \\ (N+1)^{295N^{12}}H(F)^{118N^{12}} & (i=2,4). \end{cases}$$

Suppose that C has a non-singular point P defined over K which is not at infinity. If $\phi_i(P)=0$ $(i=1,2,3)$, then we choose a uniformizer $t \in K(C)$ for P and we put $\pi = \min\{\mathrm{ord}_P(\phi_1), \mathrm{ord}_P(\phi_2), \mathrm{ord}_P(\phi_3)\}$. Hence

$$\Phi(P) = ((t^{-\pi}\phi_1)(P) : (t^{-\pi}\phi_2)(P) : (t^{-\pi}\phi_3)(P))$$

is a point of Γ defined over K. If one of the $\phi_i(P)$ is non-zero, we immediately see that $\Phi(P)$ is a point of E defined over K. By Lemma 5.1, there exists a point $Q=(u:v:w)$ of E defined over K with

$$H(Q) \le 450000|D_K|^{15/(2d)}H(G)^{11}.$$

If $\mathrm{ord}_Q(\tau_1/\tau_2) < 0$ or $\mathrm{ord}_Q(\tau_3/\tau_4) < 0$, then $\Phi^{-1}(Q)$ is a point of C_∞. Next, suppose that $\mathrm{ord}_Q(\tau_1/\tau_2) \ge 0$ and $\mathrm{ord}_Q(\tau_3/\tau_4) \ge 0$. We denote by $\tau_{i,h}$ the homogenization of τ_i. Hence, $\Phi^{-1}(Q) = (\tau_{1,h}(Q)/\tau_{2,h}(Q), \tau_{3,h}(Q)/\tau_{4,h}(Q))$ is a point of $C - C_\infty$. We have

$$H(\Phi^{-1}(Q)) \le 19N^6H(Q)12N^3H(\tau_1)^2H(\tau_2)^2H(\tau_3)^2H(\tau_4)^2,$$

whence

$$H(\Phi^{-1}(Q)) < |D_K|^{90N^3/d}(9N^{5N+4}H(F))^{18\cdot 10^6 N^{31}}.$$

Furthermore, Lemma 5.2 implies that there are polynomials $f_1(T), f_2(T), f_3(T) \in K[T]$ of degree ≤ 2 with

$$H(f_1), H(f_2) \le 3H(Q)H(G), \qquad H(f_3) \le H(G),$$

such that the conic $G(X,Y)=0$ has a parametrization given by

$$X = \frac{f_1(T)}{f_3(T)}, \qquad Y = \frac{f_2(T)}{f_3(T)}.$$

Thus, the curve $F(X, Y, 1) = 0$ has a parametrization given by

$$X = \frac{g_1(T)}{g_2(T)}, \qquad Y = \frac{g_3(T)}{g_4(T)},$$

where $g_i(T) \in K[T]$ $(i = 1, 2, 3, 4)$ with $\deg g_i < 30N^3$ and

$$H(g_i) < |D_K|^{225N^3/d}(9N^{5N+4}H(F))^{3\cdot 10^7 N^{31}}.$$

Acknowledgements. I would like to thank Professor A. Schinzel for bringing to my attention the book of A. Bliss [1].

References

[1] G. A. Bliss, *Algebraic Functions*, Dover, New York, 1966.
[2] E. Brieskorn and H. Knörrer, *Plane Algebraic Curves*, Birkhäuser, 1986.
[3] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, New York, 1966.
[4] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.
[5] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.
[6] D. Hilbert und A. Hurwitz, *Über die diophantischen Gleichungen von Geschlecht Null*, Acta Math. 14 (1890), 217–224.
[7] D. L. Hilliker, *An algorithm for computing the values of the ramification index in the Puiseux series expansions of an algebraic function*, Pacific J. Math. 118 (1985), 427–435.
[8] L. Holzer, *Minimal solutions of diophantine equations*, Canad. J. Math. 2 (1950), 238–244.
[9] S. Lang, *Introduction to Algebraic and Abelian Functions*, Springer, 1982.
[10] —, *Fundamentals of Diophantine Geometry*, Springer, 1983.
[11] M. Mignotte, *An inequality on the greatest roots of a polynomial*, Elem. Math. 46 (1991), 85–86.
[12] L. J. Mordell, *On the magnitude of the integer solutions of the equation* $ax^2 + by^2 + cz^2 = 0$, J. Number Theory 1 (1969), 1–3.
[13] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, J. Math. Pures Appl. 71 (1901), 161–233.
[14] D. Poulakis, *Integer points on algebraic curves with exceptional units*, J. Austral. Math. Soc. 63 (1997), 145–164.
[15] —, *Polynomial bounds for the solutions of a class of Diophantine equations*, J. Number Theory 66 (1997), 271–281.
[16] S. Raghavan, *Bounds for minimal solutions of diophantine equations*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1975, no. 9, 109–114.
[17] W. M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. 56 (1990), 161–179.
[18] —, *Construction and estimation of bases in function fields*, J. Number Theory 39 (1991), 181–224.
[19] J. G. Semple and L. Roth, *Algebraic Geometry*, Oxford University Press, 1949.
[20] C. L. Siegel, *Normen algebraischer Zahlen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1973, no. 11, 197–215.

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
[22] R. Walker, *Algebraic Curves*, Springer, 1978.

Department of Mathematics
Aristotle University of Thessaloniki
54006 Thessaloniki, Greece
E-mail: poulakis@ccf.auth.gr

Received on 31.10.1997
and in revised form on 3.3.1998 (3288)