ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

DIMITRIOS POULAKIS

Estimation effective des points entiers d'une famille de courbes algébriques

Annales de la faculté des sciences de Toulouse 6^e série, tome 5, n° 4 (1996), p. 691-725

<http://www.numdam.org/item?id=AFST_1996_6_5_4_691_0>

© Université Paul Sabatier, 1996, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (http://picard.ups-tlse.fr/~annales/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Annales de la Faculté des Sciences de Toulouse Vol. V, n° 4, 1996

Estimation effective des points entiers d'une famille de courbes algébriques(*)

DIMITRIOS POULAKIS(1)

RÉSUMÉ. — Soit $C : F(X,Y) = 0$ une courbe algébrique, définie sur un corps de nombres K. Soient $\overline{K}$ une clôture algébrique de K et $\overline{K}(C)$ le corps des fonctions de C. Dans ce travail nous donnons des conditions suffisantes, sur la ramification de l'extension $\overline{K}(C)/\overline{K}(X)$, pour que l'équation $F(X,Y) = 0$ ne possède qu'un nombre fini de solutions en entiers de K. De plus, nous calculons un majorant explicite pour la taille des solutions de l'équation $F(X,Y) = 0$, en entiers algébriques de K.

ABSTRACT. — Let $C : F(X,Y) = 0$ be an algebraic curve, defined over an algebraic number field K. Let $\overline{K}$ be an algebraic closure of K and $\overline{K}(C)$ the function field of C. In this work we give sufficient conditions, on the ramification of the extension $\overline{K}(C)/\overline{K}(X)$, for the equation $F(X,Y) = 0$ to have only a finite number of solutions in algebraic integers of K. Also, we calculate an explicit upper bound for the size of solutions of the equation $F(X,Y) = 0$, in algebraic integers of K.

1. Introduction et énoncé du résultat

Soient K un corps de nombres, O_K son anneau des entiers et $\overline{K}$ une clôture algébrique de K. Soit $F(X,Y)$ un polynôme de $K[X\,,\,Y]$, absolument irréductible. Notons C la courbe algébrique définie par l'équation $F(X,Y) = 0$ et g son genre. Notons aussi $\overline{K}(C)$ le corps des fonctions de C. Lorsque $a \in \overline{K}$ (respectivement $a = \infty$) on désigne par Σ_a (respectivement Σ_∞) l'ensemble des anneaux de valuation discrète de $\overline{K}(C)$, qui se trouvent au-dessus de l'anneau de valuation discrète de $\overline{K}(X)$ associé à $X - a$ (respectivement $1/X$).

(*) Reçu le 31 mai 1994

(1) Université de Thessalonique, Département de Mathématiques, G-54006 Thessalonique (Grèce)

En 1929, Siegel [22] a montré le résultat suivant.

THÉORÈME .— *Il n'existe qu'un nombre fini de solutions de l'équation* $F(X,Y) = 0$, *en entiers de* K, *sauf peut-être si* $g = 0$ *et l'ensemble* Σ_∞ *possède au plus deux éléments.*

Toutefois la démonstration de Siegel ne donne pas une méthode pour déterminer de façon explicite les solutions de l'équation $F(X,Y) = 0$, en entiers de K. Dans [13] on donne une démonstration effective de ce théorème de Siegel, dans le cas où $g = 0$ et l'ensemble Σ_∞ contient au moins trois éléments. Le cas $g = 1$, a été traité de façon effective par Baker et Coates [1] et Schmidt [17]. Pour d'autres résultats effectifs on peut consulter [2], [5], [7], [11], [12], [14] et [26]. Dans [2] on donne des conditions suffisantes, sur la ramification de l'extension $\overline{K}(C)/\overline{K}(X)$, pour que l'équation $F(X,Y) = 0$ ne possède qu'un nombre fini de solutions en entiers de K. De plus, la méthode décrite dans [2], permet le calcul d'un majorant explicite pour la taille des solutions de l'équation $F(X,Y) = 0$, en entiers de K. Notons que la famille des courbes étudiée dans [2] contient les courbes C, telles que l'extension $\overline{K}(C)/\overline{K}(X)$ soit galoisienne. Le but de notre travail est d'améliorer ce résultat (théorème 1), par une autre méthode, et de le généraliser (théorème 2). Nous décrivons la méthode que nous avons employée dans la section 2.

Soit $V(\mathbb{Q})$ l'ensemble des valeurs absolues de $\mathbb{Q}$ qui contient la valeur absolue ordinaire et les valeurs absolues p-adiques $|\cdot|_p$ avec $|p|_p = p^{-1}$. Notons $V(K) = \{|\cdot|_v : v \in M(K)\}$ l'ensemble des valeurs absolues de K, qui prolongent les éléments de $V(\mathbb{Q})$. Si $v \in M(K)$, notons d_v le degré local correspondant. Soit Φ une famille finie, non vide, d'éléments de K. Si $\operatorname{card}\Phi \geq 2$, on appelle les quantités :

$$H_K(\Phi) = \prod_{v \in M(K)} \max_{x \in \Phi} |x|_v^{d_v} \quad \text{et} \quad H(\Phi) = H_K(\Phi)^{1/[K:\mathbb{Q}]}$$

"hauteur" de Φ (relativement à K) et "hauteur absolue" de Φ respectivement. Si $\Phi = \{x\}$, on pose $H_K(x) = H_K(\{1,x\})$ et $H(x) = H(\{1,x\})$. Soit $P \in K[X_1, \ldots, X_m]$; par "hauteur" $H_K(P)$ et "hauteur absolue" $H(P)$ de P nous entendrons la hauteur et la hauteur absolue de la famille des coefficients de P. Pour les propriétés des hauteurs, on peut consulter [10, chap. 3], [19, chap. 2] et [23, chap. VIII].

Soient d et D_K le degré et le discriminant de K respectivement. Posons $N = \max\{\deg_X F, \deg_Y F\}$. Notre résultat principal est le théorème suivant.

THÉORÈME 1.— *Supposons que la courbe algébrique* $C : F(X,Y) = 0$ *possède une des deux propriétés suivantes :*

(i) il existe a, $b \in \overline{K}$ *tels que les indices de ramification des anneaux de* Σ_i *sont tous divisibles par un entier* e_i, $i = a, b$, *avec* $e_a \geq 2$ *et* $e_b \geq 3$;

(ii) il existe a_1, a_2, $a_3 \in \overline{K}$ *tels que les indices de ramification des anneaux de* Σ_{a_i}, $i = 1, 2, 3$, *sont tous divisibles par* 2.

Alors si x, $y \in O_K$ *avec* $F(x,y) = 0$, *on a :*

$$\max\{H_K(x)\,,\, H_K(y)\} < \exp\left\{\Psi |D_K|^{\Psi_1} H_K(F)^{\Psi_2}\right\} \quad .$$

où

$$\Psi = N^{10^5\, d^2 N^{35}}\,, \quad \Psi_1 = 9N^{13}\,, \quad \Psi_2 = 16\, d\, 10^3 N^{35}\,.$$

COROLLAIRE 1.— *Supposons que la courbe* $C : F(X,Y) = 0$ *soit de genre* $g \geq 1$ *et l'extension* $\overline{K}(C)/\overline{K}(X)$ *galoisienne. Alors si* x, $y \in O_K$ *avec* $F(x,y) = 0$, *les quantités* $H_K(x)$, $H_K(y)$ *vérifient l'inégalité donnée dans le théorème 1.*

Dans [2], on suppose que

$$F(X,Y) = Y^n + \sum_{\substack{i=0 \\ j=0}}^{n-1,\, m} a_{ij} X^i Y^j$$

avec $a_{ij} \in O_K$. On suppose aussi que la courbe C possède une des propriétés (i), (ii) du théorème 1. Soient $\sigma_1, \ldots, \sigma_d$ les d plongements de K dans le corps des nombres complexes $\mathbb{C}$. Si $x \in O_K$, on note $\|x\| = \{|\sigma_1(x)|, \ldots, |\sigma_d(x)|\}$; les quantités $H_K(x)$ et $\|x\|$ vérifient l'inégalité $\|x\| \leq H_K(x) \leq \|x\|^d$. Aussi, on pose $H = \max_{i,j}\{\|a_{ij}\|\}$; de même les quantités $H_K(F)$ et H vérifient l'inégalité $H \leq H_K(F) \leq H^d$. Alors, si x, $y \in O_K$ avec $F(x,y) = 0$, on montre dans [2] par une autre méthode, que

$$\max\{\|x\|\,,\, \|y\|\} < \exp\left\{\Psi |D_K|^{\Psi_1} H^{\Psi_2}\right\}\,.$$

La constante Ψ ne dépend que de d et de N ; elle est effectivement calculable mais n'est pas donnée explicitement ; de plus, on a :

$$\Psi_1 = 50\, N^{12} \quad \text{et} \quad \Psi_2 = \left(N^3 d\right)^{6N^3}\,.$$

Le théorème 1 donne une valeur explicite pour Ψ et améliore sensiblement l'exposant de H, mais l'exposant de $|D_K|$ dans [2] est légèrement meilleur pour $N \geq 6$; alors, dans le cas où $K = \mathbb{Q}$, le théorème 1 améliore sensiblement le résultat de [2]. Notons aussi que dans [27], on donne une démonstration effective du théorème de Siegel, dans le cas où l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne, sans calculer un majorant explicite. La méthode employée dans [27] est différente de la méthode de [2] et de la nôtre. Enfin, dans le dernier paragraphe nous présentons des familles de courbes algébriques qui vérifient les hypothèses du théorème 1.

Rappelons qu'un diviseur sur C est un élément du groupe abélien libre engendré par les anneaux de valuation discrète W de $\overline{K}(C)$, avec $\overline{K} \subset W$ ([9]). On désigne par M le degré total de $F(X,Y)$. En combinant le théorème 1 et le théorème 2 de [14], nous obtenons le résultat plus général suivant.

THÉORÈME 2. — *Supposons que la courbe $C : F(X,Y) = 0$ soit de genre $g \geq 1$ et qu'il existe une fonction $h = \eta(X,Y)/\xi(X,Y)$ de $K(C)$, où $\eta(X,Y), \xi(X,Y) \in K[X, Y]$, telle que l'extension $\overline{K}(C)/\overline{K}(h)$ possède une des propriétés (i)-(ii) du théorème 1. Soient Φ_1 et Φ_2 deux constantes telles que $H\big(\eta(X,Y)\big)$, $H\big(\xi(X,Y)\big) < \Phi_1$ et le degré total des $\eta(X,Y)$, $\xi(X,Y)$ soit $< \Phi_2$. Soit $(h)_\infty = k_1V_1 + \cdots + k_rV_r$, où les entiers $k_1, \ldots, k_r$ sont positifs et $V_1, \ldots, V_r \in \Sigma_\infty$, le diviseur des pôles de h. Notons $\deg(h) = \delta$ et $\Xi = \max\{M, 2g+k_1, \ldots, 2g+k_r\}$. Alors si $x, y \in O_K$ avec $F(x,y) = 0$, on a :*

$$\max\big\{H_K(x), H_K(y)\big\} < \exp\Big\{\big(2\Xi\Phi_1\big)^{\Omega_1}\big|D_K\big|^{\Omega_2}H_K\big(F\big)^{\Omega_3}\Big\},$$

où

$$\Omega_1 = 3 \cdot 10^7\, d^2 n^r \Xi^{21+r} \delta^{15} g^7 2^{2g+\delta} \big(2g + 2\delta\big)^{35} \Phi_2^4$$

$$\Omega_2 = 2 \cdot 10^4\, rdn^r \Xi^r g^2 \delta^3 \big(2g + 2\delta\big)^{35}$$

$$\Omega_3 = 7 \cdot 10^6\, dn^r \delta^{11} g^7 \Xi^{16+r} 2^{2g+\delta} \big(2g + 2\delta\big)^{35} \Phi_2^2.$$

COROLLAIRE 2. — *Supposons que la courbe $C : F(X,Y) = 0$ soit de genre $g \geq 1$ et qu'il existe une fonction $h = \eta(X,Y)/\xi(X,Y)$ de $K(C)$, où $\eta(X,Y)$, $\xi(X,Y) \in K[X, Y]$, telle que l'extension $\overline{K}(C)/\overline{K}(h)$ soit galoisienne. Alors si $x, y \in O_K$ avec $F(x,y) = 0$, les quantités $H_K(x)$, $H_K(y)$ vérifient l'inégalité donnée dans le théorème 2.*

Dans [14], on étudie une famille de courbes algébriques, qui sont revêtements cycliques de la droite projective $\mathbb{P}^1$, et on calcule un majorant explicite pour la hauteur de leurs points entiers, définis sur un corps de nombres (théorème 3). Le corollaire 2 est donc une généralisation de ce résultat.

2. Principe géométrique de la démonstration

Le principe géométrique de la démonstration du théorème 1 est très bien expliqué par J.-P. Serre dans [20]. Dans ce paragraphe, nous allons le décrire d'une façon plus générale.

Soit $\mathcal{V}$ une variété affine de $\mathbb{A}^r$. Notons $x_1, \ldots, x_r$ les fonctions coordonnées de $\mathcal{V}$. Si E est un sous-ensemble de K, on désigne par $\mathcal{V}(E)$ l'ensemble des points de $\mathcal{V}$ à coordonnées dans E. On appelle un ensemble $S \subseteq \mathcal{V}(K)$, quasi-entier (relativement à O_K), s'il existe un entier rationnel non nul α, tel que pour tout $P \in S$ on a $\alpha x_i(P) \in O_K$, $i = 1, \ldots, r$. On note par $\mathcal{V}_\infty$ l'ensemble des points de la clôture projective de $\mathcal{V}$ qui se trouvent à l'infini. Par courbe algébrique on entendra une variété algébrique de dimension 1. Si C est une courbe algébrique, on désigne par $\Sigma_\infty(C)$ l'ensemble des anneaux de valuation discrète V de $\overline{K}(C)$, avec $\overline{K} \subset V$, tel que pour tout $V \in \Sigma_\infty(C)$ il existe $P \in C_\infty$ avec $V \supseteq \mathcal{O}_P(C)$, où $\mathcal{O}_P(C)$ est l'anneau local de C en P. Rappelons qu'un morphisme de courbes algébriques affines $f : C \to E$ est non ramifié si l'extension $\overline{K}(C)/\overline{K}(E)$ est non ramifiée en dehors de $\Sigma_\infty(C)$.

PROPOSITION 2.1.— *Soit $\phi : \mathcal{T} \to \mathcal{E}$ un morphisme fini de courbes affines, défini sur K.*

(a) Si $S \subseteq \mathcal{T}(K)$, alors S est quasi-entier si et seulement $\phi(S)$ est un sous-ensemble quasi-entier de $\mathcal{E}(K)$.

(b) Supposons que le morphisme ϕ est non ramifié. Alors si S est un sous-ensemble quasi-entier de $\mathcal{E}(K)$, il existe une extension finie K' de K telle que l'ensemble $\phi^{-1}(S)$ est rationnel sur K'.

On peut consulter [19, pp. 108, 109] pour une démonstration de ces résultats. Dans les énoncés correspondants de [19], on suppose aussi que le morphisme ϕ est surjectif. Ce n'est pas nécessaire, car d'après le théorème 4 de [21, p. 48], tout morphisme fini de variétés affines est surjectif. Notons aussi que la partie (b) de la proposition 2.1 est une version affine du théorème de Chevalley–Weil pour les courbes algébriques ([10, p. 44] et [19, p. 50]).

Soit $F(X,Y)$ un polynôme absolument irréductible de $K[X, Y]$. Notons C la courbe définie par l'équation $F(X,Y) = 0$. On s'intéresse à déterminer les points entiers sur C, rationnels sur K. Introduisons une courbe affine plane (irréductible) $C' : F'(X,Y) = 0$, définie sur un corps de nombres $L \supseteq K$, telle que pour tout corps de nombres $M \supseteq L$, on sait déterminer explicitement les sous-ensembles quasi-entiers de $C'(M)$.

Supposons qu'il existe un morphisme fini $f : C' \to \mathbb{A}^1$. Alors il existe un corps de nombres L', avec $L' \supseteq L$, et un polynôme $G(X,Y)$ de $L'[X, Y]$, tel que $f(x,y) = G(x,y)$, pour tout $(x,y) \in C'(\overline{K})$. Considérons une courbe $\mathcal{T}$ qui est une composante irréductible de l'ensemble algébrique défini dans l'espace affine $\mathbb{A}^4$ par les équations :

$$F(X,Y) = 0\,, \quad F'(X',Y') = 0 \quad \text{et} \quad X = G(X',Y')\,.$$

Soient x, y, x' et y' les fonctions coordonnées sur $\mathcal{T}$, engendrées par X, Y, X' et Y' respectivement. On a deux morphismes canoniques $\pi : \mathcal{T} \to C$ et $\pi' : \mathcal{T} \to C'$, définis par $\pi(Q) = \big(x(Q), y(Q)\big)$ et $\pi'(Q) = \big(x'(Q), y'(Q)\big)$. On a supposé que le morphisme f est fini; il en résulte que l'anneau $\overline{K}[x', y']$ est entier sur l'anneau $\overline{K}[G(x,y)] = \overline{K}[x]$. Par conséquent l'anneau $\overline{K}[x', y', x, y]$ est entier sur $\overline{K}[x, y]$, d'où on a que le morphisme π est fini. Comme $x = G(x', y')$, on déduit que le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathcal{T} & \xrightarrow{\pi'} & C' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle f} \\ C & \xrightarrow[x]{} & \mathbb{A}^1 \end{array}$$

Supposons maintenant que le morphisme π est non ramifié. Alors d'après la proposition 2.1(b), il existe un corps de nombres M, avec $M \supseteq L'$, tel que $\pi^{-1}\big(C(O_K)\big) \subseteq \mathcal{T}(M)$; de plus, d'après la proposition 2.1(a), on a que $\pi^{-1}\big(C(O_K)\big)$ est un sous-ensemble quasi-entier de $\mathcal{T}(M)$. Ensuite, la proposition 2.1(a) entraîne que $\pi'\big(\pi^{-1}\big(C(O_K)\big)\big)$ est un sous-ensemble quasi-entier de $C'(M)$ (qu'on sait déterminer explicitement). Si $P \in C(O_K)$, il existe $R \in \pi'\big(\pi^{-1}\big(C(O_K)\big)\big)$, tel que $x(P) = G\big(x'(R), y'(R)\big)$. Donc, dans le cas où on est muni d'une version effective de la proposition 2.1(b), on peut déterminer explicitement les éléments de $C(O_K)$.

Récapitulant, pour appliquer cette méthode on a besoin de trois choses. D'abord, d'une courbe affine plane (irréductible) C', définie sur un corps de nombres $L \supseteq K$, telle que pour tout corps de nombres $M \supseteq L$, on sait déterminer explicitement les sous-ensembles quasi-entiers de $C'(M)$.

Deuxième chose, d'un morphisme fini de courbes affines $f : C' \to \mathbb{A}^1$, défini sur un corps de nombres L, tel que morphisme fini π soit non ramifié (on définit $\mathcal{T}$, π et π' comme ci-dessus). Troisième chose, il faut connaître une vesion effective de la proposition 2.1(b), au moins dans le cas particulier auquel on s'intéresse.

À notre connaissance, on a appliqué cette méthode pour la première fois dans [8], où on l'a utilisée pour réduire le problème de déterminer les solutions entières de l'équation hyperelliptique et superelliptique, au cas de l'équation $X^3 + Y^3 = 1$. Dans [19], on considère une famille de courbes hyperelliptiques $F(X, Y) = 0$ et on utilise cette méthode pour réduire le problème de déterminer les solutions entières de l'équation $F(X, Y) = 0$, au cas d'une équation elliptique. À propos de la proposition 2.1(b), la remarque 1 de [8, p. 72], implique que si on connaît explicitement le morphisme $\phi : \mathcal{T} \to \mathcal{E}$, on peut déterminer (explicitement) l'extension finie K' de K. Toutefois, à notre connaissance, il n'existe pas dans la littérature une version effective générale de la proposition 2.1(b) (par exemple une majoration explicite du discriminant de K' en fonction des courbes $\mathcal{T}$, $\mathcal{E}$ du morphisme ϕ et de K).

Pour démontrer le théorème 1 on utilise une courbe C', adaptée aux propriétés de ramification du morphisme $p : C \to \mathbb{A}^1$, défini par $p(x, y) = x$. Dans le premier cas on utilise la courbe $S^{e_b} = R^{e_a} + (a - b)$, que l'on projette sur $\mathbb{A}^1$ par $(r, s) \to x = r^{e_a} + a = s^{e_b} + b$. Dans le deuxième cas, on utilise la courbe $R^2 = (X - a_1)(X - a_2)(X - a_3)$, que l'on projette sur $\mathbb{A}^1$ par $(x, r) \to x$. Aussi, il est bien connu qu'on sait déterminer explicitement les ensembles quasi-entiers sur les deux courbes auxiliaires. Remarquons que dans le premier cas on peut remplacer la courbe auxiliaire par les équations $R^{e_a} = X - a$ et $S^{e_a} = X - b$. Alors la proposition suivante, qui est un cas particulier effectif de la proposition 2.1(b), suffit pour la démonstration du théorème 1.

PROPOSITION 2.2.— *Soit $C : F(X, Y) = 0$ une courbe (irréductible), définie sur K. Supposons qu'il existe $a_1, \ldots, a_s \in \overline{K}$ et $e \in \mathbb{Z}$, avec $e \geq 2$, tels que les indices de ramification des anneaux de Σ_{a_i} sont tous divisibles par e, $i = 1, \ldots, s$. Notons $\mathcal{T}$ la courbe algébrique dont le corps de fonctions est le corps $\overline{K}(C)(R)$, où $R^e = (X - a_1) \cdots (X - a_s)$. Soit $\phi : \mathcal{T} \to C$ la projection définie par $\phi(x, y, r) = (x, y)$. Si x, $y \in O_K$ avec $F(x, y) = 0$, notons L le corps engendré sur $K(a_1, \ldots, a_s)$ par les éléments de l'ensemble $\phi^{-1}(x, y)$. Alors le discriminant D_L de L satisfait l'inégalité :*

$$|D_L| < |D_K|^{e^2 2^s N^{2s}} \left(N^6 H(F)\right)^{7d^2 s e^6 2^s 10^3 N^{18+2s}}.$$

Le morphisme $\phi : \mathcal{T} \to C$ est non ramifié. Alors pour démontrer la proposition 2.2, on détermine un ensemble fini S d'idéaux premiers (entiers) $\mathcal{P}$ de $K(a_1, \ldots, a_s)$, tels que pour tout $\mathcal{P} \notin S$ le morphisme $\phi : \mathcal{T} \to C$ se réduit $\mathrm{mod}\mathcal{P}$ en un morphisme de courbes affines $\phi_{\mathcal{P}} : \mathcal{T}_{\mathcal{P}} \to C_{\mathcal{P}}$ non ramifié. On en déduit que l'extension $L/K(a_1, \ldots, a_s)$ est non ramifié en dehors de S. Comme il n'existe qu'un nombre fini d'extensions d'un corps de nombres M, de degré borné, non ramifiées en dehors d'un ensemble fini d'idéaux premiers (entiers) de M, on en déduit le résultat.

Dans les sections 3, 4 et 5, nous donnons quelques résultats qui seront utiles dans la démonstration de la proposition 2.2 et des théorèmes 1 et 2.

3. Sur la ramification des courbes algébriques

Soit $F(X,Y)$ un polynôme absolument irréductible de $K[X, Y]$. Notons C la courbe algébrique définie par l'équation $F(X,Y) = 0$ et $\overline{K}(C)$ le corps des fonctions de C. Supposons que au-dessus de $X = a \in \overline{K}$ il y a de la ramification. Notons $E = K(a)$. Posons $m = \deg_X F$, $n = \deg_Y F$ et $N = \max\{m, n\}$. On considère $F(X,Y)$ comme polynôme à coefficients dans $K[X]$ et on note $D(X)$ son discriminant. Alors le degré de $D(X)$ est $\leq 2m(n-1)$. Il existe donc $\lambda_1, \ldots, \lambda_{4N^2} \in \mathbb{Z}$, avec $1 \leq \lambda_i \leq 6N^2$, $i = 1, \ldots, 4N^2$ tels qu'il n'y a pas de ramification au-dessus de $X = \lambda_1, \ldots, \lambda_{4N^2}$. Notons $V_{01}, \ldots, V_{0r}$ les éléments de Σ_a et $V_{i1}, \ldots, V_{in}$ les éléments de Σ_{λ_i}, $i = 1, \ldots, 4N^2$. Considérons le diviseur :

$$\Delta = \sum_{i,j} V_{ij} .$$

Si f est une fonction dans $\overline{K}(C)$ et W un anneau de valuation discrète de $\overline{K}(C)$, on désigne par $\mathrm{ord}_W(f)$ l'ordre de f en W. On note $L(\Delta)$ le $\overline{K}$-espace des fonctions $f \in \overline{K}(C)$, telles que $\mathrm{ord}_{V_{ij}}(f) \geq -1$, pour tout i, j et $\mathrm{ord}_W(f) \geq 0$, lorsque $W \neq V_{ij}$, pour tout i, j ; la dimension δ de $L(\Delta)$ est $\leq \deg \Delta + 1 = r + n4N^2 + 1$.

LEMME 3.1.— *Il existe une base* $\mathcal{B} = \{f_1, \ldots, f_\delta\}$ *de l'espace* $L(\Delta)$, *telle que*

$$f_i = c_i(X,Y)/q(X) , \quad i = 1, \ldots, \delta ,$$

où $c_i(X,Y) \in E[X, Y]$, $i = 1, \ldots, \delta$, *et* $q(X) \in E[X]$, *avec*

$$\deg q < 5N^3 , \quad \deg_X c_i < 21\, N^3 , \quad \deg_Y c_i < n$$

et

$$H(q) < N^{63N^4} H(F)^{10N^4}, \quad H(c_i) < N^{5030N^{12}} H(F)^{735N^{12}}.$$

De plus, pour tout i, j, il existe un indice $k(i,j) \leq \delta$, tel que la fonction $1/f_{k(i,j)}$ est une uniformisante en V_{ij}.

Démonstration. — Le théorème A2 de [16], entraîne qu'il existe des polynômes $q(X)$ et $c_i(X,Y)$ $(i = 1, \ldots, \delta)$, tels que les fractions $c_i(X,Y)/q(X)$, $i = 1, \ldots, \delta$, représentent une base de l'espace $L(\Delta)$. D'après [16, p. 186], le diviseur Δ est défini sur le corps E. Alors, le théorème B2 de [16] entraîne que $c_i(X,Y) \in E[X, Y]$ $(i = 1, \ldots, \delta)$ et $q(X) \in E[X]$.

Le théorème A2 implique que les racines de $q(X)$ sont parmi les racines $\rho_1, \ldots, \rho_\sigma$ de $D(X)$ et les entiers $\lambda_1, \ldots, \lambda_{4N^2}$; de plus on a :

$$\deg q \leq n(4N^2 + 1) + m(n-1) < 5N^3.$$

Alors le théorème 5.9 de [23, p. 211] entraîne :

$$H(q) \leq 2^{5N^3-1} \left(\max\{H(\rho_1), \ldots, H(\rho_\sigma), H(\lambda_1), \ldots, H(\lambda_{4N^2})\}\right)^{5N^3}.$$

On a $H(\lambda_i) \leq 6N^2$ $(i = 1, \ldots, 4N^2)$ et les lemmes 3 et 4 de [15] donnent :

$$H(\rho_1), \ldots, H(\rho_\sigma) < 2N^2 H(D) < N^{12N} H(F)^{2N}.$$

Donc il résulte :

$$H(q) < N^{63N^4} H(F)^{10N^4}.$$

D'après le théorème A2, on a :

$$\deg_X c_i \leq n(m + 3 + 12N^2) + \deg q + \delta - 1 + m < 21N^3.$$

Soit $F(X,Y) = a_0(X)Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$. Suivant la notation de [16], on a

$$c_i(X,Y) = X^\rho \sum_{j=1}^{n} b_{ij}(X) y_j(X,Y), \quad i = 1, \ldots, \delta,$$

où $y_j(X,Y) = a_0(X)Y^{j-1} + \cdots + a_{j-2}(X)Y$ $(j = 2, \ldots, n)$, $y_1 = 1$, ρ est un entier positif $\leq \delta$ et $b_{ij}(X)$ un polynôme de $E[X]$. On a $b_{ij}(X) =$

$\ell_2(X)d_{ij}(X)$ ([16, p. 204]) et $d_{ij}(X) = \delta_{ij0} + \delta_{ij1}X + \cdots + \delta_{ij\nu}X^\nu$ avec $\nu < 14\,N^3$ ([15, p. 209]). Le lemme 15 de [16] donne :

$$H(\ell_2) < N^{45\,N^3} H(F)^{8N^3}$$

et le lemme 26 de [16] entraîne que la hauteur du vecteur

$$\overrightarrow{\delta_i} = \{\delta_{ijp}\}_{1\le j\le \delta,\, 0\le p\le \nu}$$

satisfait l'inégalité :

$$H(\overrightarrow{\delta_i}) < N^{5024\,N^{12}} H(F)^{730\,N^{12}}.$$

On a :

$$\sum_{j=1}^{n} d_{ij}y_j = d_{i1} + (d_{i2}a_0 + \cdots + d_{in}a_{n-2})Y + \\ + (d_{i3}a_0 + \cdots + d_{in}a_{n-3})Y^2 + \cdots + d_{in}Y^{n-1}.$$

Alors on déduit :

$$H\left(\sum_{j=1}^{n} d_{ij}y_j\right) < 14\,N^3 H(\overrightarrow{\delta_i})H(F) < N^{5025\,N^{12}} H(F)^{731\,N^{12}}$$

(pour conclure cette majoration on a supposé qu'un des coefficients de $F(X,Y)$ est 1, ce qu'on peut faire sans restreindre la généralité). Enfin, la proposition 2.4 de [10, p. 57] et les majorations pour les hauteurs des polynômes ℓ_2 et $\sum_{j=1}^{n} d_{ij}y_j$ entraînent :

$$H(c_i) < N^{5030\,N^{12}} H(F)^{735\,N^{12}}.$$

Soit g le genre de la courbe C. Le degré du diviseur $\Delta - V_{ij}$ est $r + 4nN^2 - 1 > (2N)^2 \ge 2g$; alors le théorème de Riemann–Roch entraîne $\ell(\Delta) = \ell(\Delta - V_{ij}) + 1$. Par conséquent, il existe un indice $k(i,j)$ tel que $\mathrm{ord}_{V_{ij}}(f_{k(i,j)}) = -1$.

Rappelons qu'un K-système est une famille $\{A_v\}_{v\in M(K)}$ de nombres réels ≥ 1, indexée par $M(K)$, tels que $A_v = 1$ presque pour tout $v \in M(K)$ et A_v est un élément du groupe des valeurs de $|\cdot|_v$ pour tout $v \in M(K)$. On appelle "norme absolue" du K-système $\{A_v\}_{v\in M(K)}$ la quantité

$$\mathcal{N}\{A_v\} = \left(\prod_{v\in M(K)} A_v^{d_v}\right)^{1/d},$$

où d_v note le degré local qui correspond à la valeur absolue $|\cdot|_v$.

LEMME 3.2. — *Pour tout $j = 1, \ldots, r$ il existe un corps de nombres E_j avec $[E_j : E] \leq n$, un élément non nul $\beta_j \in E_j$ avec*

$$H(\beta_j) < \left(N^6 H(F)\right)^{10^3 N^{13}}$$

et une fonction $h_j \in E_j(C)$ qui appartient à l'idéal maximal de V_{0j}, tels que

$$f_{k(0,j)}^{e_j}(X - a) = \beta_j + h_j$$

où e_j est l'indice de ramification de l'anneau V_{0j}.

Démonstration. — D'après le théorème C2 de [16], le développement de la fonction $f_{k(0,j)}$ en V_{0j} est

$$f_{k(0,j)} = \sum_{s=-1}^{\infty} c_{js}(X - a)^{s/e_j};$$

les coefficients c_{js}, $s = -1, 0, \ldots$, engendrent un corps de nombres E_j sur E avec $[E_j : E] \leq n$; il existe deux E-systèmes $\{A_v\}$ et $\{B_v\}$, définis pour tout $v \in M(E)$, tels que

$$|c_{js}|_v \leq A_v^{s+4N^3} B_v, \quad s = -1, 0, \ldots,$$

avec

$$\mathcal{N}\{A_v\} < \left(2^7 N^{5+24N} H(F)^{1+4N}\right)^{9N^5}$$

et

$$\mathcal{N}\{B_v\} < \left(9\, N^{4+12N} H(F)^{1+2N}\right)^{365\, N^{11}}.$$

Alors on a

$$f_{k(0,j)}^{e_j}(X-a) = c_{j,-1}^{e_j} + h_j\,,$$

où h_j est une fonction de $E_j(C)$ qui appartient à l'idéal maximal de V_{0j}; comme la fonction $f_{k(0,j)}^{e_j}(X-a)$ est une unité dans V_{0j}, il résulte que le coefficient $c_{j,-1}$ est non nul; aussi on a :

$$H(c_{j,-1}^{e_j}) < \left(N^6 H(F)\right)^{10^3 N^{13}}.$$

4. Sur la réduction des courbes algébriques

Soit C une courbe algébrique (irréductible) définie par l'équation

$$F(X,Y) = 0\,, \quad \text{où } F(X,Y) = a_0(X)Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)\,,$$

avec $a_i(X) \in O_K[X]$, $i = 0, \ldots, n$. Considérons $F(X,Y)$ comme polynôme à coefficients dans $K[X]$ et notons $D[X]$ son discriminant.

LEMME 4.1.— *Notons S l'ensemble des idéaux premiers P de O_K tels que P divise un coefficient de $D(X)$ ou de $F(X,Y)$. Alors pour tout $P \notin S$, la réduction* mod P *du polynôme $F(X,Y)$ est un polynôme $\overline{F}(X,Y)$ absolument irréductible.*

Démonstration.— Soit P un idéal premier de O_K avec $P \notin S$. Notons $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ les fonctions algébriques (dans une clôture algébrique de $\overline{K}(X)$) telles que $F(X, \mathcal{Y}_i) = 0$, $i = 1, \ldots, n$. Soient L un corps de nombres avec $L \supseteq K$ et O_L l'anneau des entiers de L. Soit $\mathcal{P}$ un idéal premier de O_L avec $\mathcal{P} \cap O_K = P$. Notons $v_{\mathcal{P}}$ la valuation discrète de L qui est associée à $\mathcal{P}$. Si $g(X) = g_0 X^n + \cdots + g_n$ est un polynôme de $L[X]$, posons :

$$w_{\mathcal{P}}\big(g(X)\big) = \min\big\{v_{\mathcal{P}}(g_0), \ldots, v_{\mathcal{P}}(g_n)\big\}\,. \tag{4.1}$$

De cette façon on définit une valuation discrète $w_{\mathcal{P}}$ sur le corps $L(X)$; son corps résiduel est $\ell(X)$, où $\ell = O_L/\mathcal{P}$. Notons A l'anneau de valuation discrète de $L(X)$ qui est associé à $w_{\mathcal{P}}$ et $M_{\mathcal{P}}$ son idéal maximal. Notons B la fermeture intégrale de A dans le corps $\mathbb{M} = L(X)(\mathcal{Y}_1, \ldots, \mathcal{Y}_n)$ et $w_1, \ldots, w_r$ les valuations discrètes sur $\mathbb{M}$ qui prolongent $w_{\mathcal{P}}$; on note aussi $M_1, \ldots, M_r$ les idéaux maximaux de B qui se trouvent au-dessus de $M_{\mathcal{P}}$ et sont associés aux valuations $w_1, \ldots, w_r$ respectivement.

Comme $P \notin S$, on a $w_{\mathcal{P}}(a_j(X)) = 0$, $j = 0, \ldots, n$. Il en résulte que $\mathcal{Y}_i$ est un élément de B; donc $w_h(\mathcal{Y}_i) \geq 0$, $i = 1, \ldots, n$, $h = 1, \ldots, r$. Supposons que $w_h(\mathcal{Y}_i) > 0$. Alors on a :

$$0 = w_h(a_n(X)) = w_h(a_0(X)\mathcal{Y}_i^n + \cdots + a_{n-1}(X)\mathcal{Y}_i) \geq w_h(\mathcal{Y}_i) > 0\,,$$

ce qui est contradictoire. On a donc $w_h(\mathcal{Y}_i) = 0$, $i = 1, \ldots, n$, $h = 1, \ldots, r$.

Notons G le groupe de Galois de l'extension $\mathbb{M}/L(X)$ et I_i le groupe d'inertie de M_i, $i = 1, \ldots, r$. Comme $P \notin S$, on a $w_{\mathcal{P}}(D(X)) = 0$, d'où il résulte que $w_i(\mathcal{Y}_s - \mathcal{Y}_t) = 0$, pour tout (s,t) avec $s \neq t$. Supposons qu'il existe $\sigma \in I_i$ avec $\sigma \neq \mathrm{Id}$. Alors il existe un indice s tel que $\sigma(\mathcal{Y}_s) \neq \mathcal{Y}_s$ et $\sigma(\mathcal{Y}_s) - \mathcal{Y}_s \in M_i$. Donc $w_i(\sigma(\mathcal{Y}_s) - \mathcal{Y}_s) > 0$, ce qui n'est pas le cas. On en déduit $I_i = \{\mathrm{Id}\}$, $i = 1, \ldots, r$. Cela entraîne que l'idéal $M_{\mathcal{P}}$ ne se ramifie pas dans B [18, chap. I, sect. 7]. Par conséquent la valuation discrète $w_{\mathcal{P}}$ ne se ramifie pas dans $\overline{K}(C)$.

Nous allons déterminer par la suite l'anneau $E = L(C) \cap B$. Comme $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ sont toutes les fonctions algébriques avec $F(X, \mathcal{Y}_i) = 0$, il existe un indice j tel que $L(C) = L(\mathcal{Y}_j)$. On peut donc supposer, sans restreindre la généralité que $L(C) = L(\mathcal{Y}_1)$. Soit

$$z = b_0(X) + b_1(X)\mathcal{Y}_1 + \cdots + b_{n-1}(X)\mathcal{Y}_1^{n-1}\,,$$

où $b_0(X), \ldots, b_{n-1}(X) \in L(X)$, un élément de l'anneau E. Notons $\sigma_1, \ldots, \sigma_n$ les $L(X)$-plongements de $L(C)$ dans une clôture algébrique de $L(X)$. On a :

$$\sigma_i(z) = b_0(X) + b_1(X)\sigma_i(\mathcal{Y}_1) + \cdots + b_{n-1}(X)\sigma_i(\mathcal{Y}_1)^{n-1}\,, \quad i = 1, \ldots, n\,.$$

De cette façon il résulte un système linéaire qui a comme inconnues les éléments $b_0(X), \ldots, b_{n-1}(X)$. Le carré du déterminant de la matrice des inconnues est au signe près le discriminant $D(X)$ qui est une unité dans A. Aussi, les éléments $\sigma_i(z)$, $i = 1, \ldots, n$, sont entiers sur A. On en déduit que les éléments $b_0(X), \ldots, b_{n-1}(X)$ sont dans A. Donc on a $E = A[\mathcal{Y}_1]$. Notons $N_1, \ldots, N_\rho$ les idéaux maximaux de E qui se trouvent au-dessus de $M_{\mathcal{P}}$ et $v_1, \ldots, v_\rho$ les valuations discrètes correspondantes sur $L(C)$ qui prolongent $w_{\mathcal{P}}$. Alors le Lemme 4 de [18, p. 29], entraîne qu'il existe des polynômes $F_1(X,Y), \ldots, F_\rho(X,Y)$ de $L[X\,, Y]$, dont les réductions $\overline{F}_1(X,Y), \ldots, \overline{F}_\rho(X,Y) \bmod M_{\mathcal{P}}$ donnent $\overline{F}_1(X,Y) \cdots \overline{F}_\rho(X,Y) = \overline{F}(X,Y)$ et tels que $N_i = (M_{\mathcal{P}}\,, F_i(X, \mathcal{Y}_1))$, $i = 1, \ldots, \rho$. Soit π un élément de L tel que $w_{\mathcal{P}}(\pi) = 1$; alors l'idéal $M_{\mathcal{P}}$ est engendré par π.

Comme la valuation $w_{\mathcal{P}}$ ne se ramifie pas dans E, l'élément π est aussi une uniformisante pour toute valuation v_i, $i = 1, \ldots, \rho$. Par conséquent on a $F_1(X, \mathcal{Y}_1) = \pi^{\eta} G(X, \mathcal{Y}_1)$, où η est un entier positif et $G(X, \mathcal{Y}_1) \in L(X)(\mathcal{Y}_1)$, avec $v_1\big(G(X, \mathcal{Y}_1)\big) = 0$. Posons $G(X, \mathcal{Y}_1) = G'(X, \mathcal{Y}_1)/R(X)$, où $G'(X, \mathcal{Y}_1) \in E$ et $R(X) \in A$ avec $v_1\big(G'(X, \mathcal{Y}_1)\big) = 0 = w_{\mathcal{P}}\big(R(X)\big)$. Alors il existe un polynôme $J(X, Y) \in L[X, Y]$ tel que

$$R(X)F_1(X, Y) = \pi^{\eta} G'(X, Y) + J(X, Y)F(X, Y).$$

Comme $w_{\mathcal{P}}\big(R(X)\big) = 0$, la réduction $\overline{R}(X)$ de $R(X) \bmod M_{\mathcal{P}}$, est non nulle; il en résulte que la réduction $\overline{J}(X, Y)$ de $J(X, Y) \bmod M_{\mathcal{P}}$, est un élément non nul de B/N_1. On a donc :

$$\overline{R}(X)\overline{F}_1(X, Y) = \overline{J}(X, Y)\overline{F}(X, Y).$$

Cela entraîne qu'au-dessus de $M_{\mathcal{P}}$ il n'existe qu'un seul idéal premier de B et le polynôme $\overline{F}(X, Y)$ est irréductible sur le corps fini ℓ. Comme L est un corps de nombres arbitraire, avec $K \subseteq L$, on conclut que le polynôme $\overline{F}(X, Y)$ est irréductible sur toute extension finie du corps O_K/P. Alors le polynôme $\overline{F}(X, Y)$ est absolument irréductible.

Considérons un idéal premier P de O_K tel que $P \notin S$. Alors d'après la proposition 4.1, le polynôme $\overline{F}(X, Y)$ est absolument irréductible. Il définit donc une courbe algébrique sur le corps fini O_k/P que nous allons noter C_P.

Soit $a \in \overline{K}$ et (a, b_i), $i = 1, \ldots, s$ les points sur la courbe C qui se trouvent au-dessus de $X = a$. Notons $E = K(a)$ et O_E l'anneau des entiers de E. Soient V_i, $i = 1, \ldots, r$, les éléments de Σ_a et e_i $(i = 1, \ldots, r)$ leurs indices de ramification respectifs. D'après le lemme 3.1, pour tout i, il existe une uniformisante t_i en V_i, définie sur E. On a :

$$X - a = t_i^{e_i} u_i,$$

où u_i est une unité en V_i, définie sur E, $i = 1, \ldots, r$. Aussi, on a $u_i = \beta_i + h_i$, où β_i est un élément non nul de $\overline{K}$ et h_i un élément de l'idéal maximal de V_i; il existe un corps de nombres E_i, avec $E \subseteq E_i$ et $[E_i : E] \leq n$, tel que $\beta_i \in E_i$ et la fonction h_i est définie sur E_i, $i = 1, \ldots, r$. Le lemme 3.2 fournit une majoration pour la hauteur absolue de β_j. Notons ν_i le plus petit entier positif tel que $\nu_i \beta_i$ est un entier de E_i, $i = 1, \ldots, r$. On désigne par E' le composé des corps E_i, $i = 1, \ldots, r$.

Notons $L = E'(b_1, \ldots, b_s)$. Considérons l'ensemble S_a des idéaux premiers entiers $\mathcal{P}$ de O_L qui possèdent une des propriétés suivantes :

(i) $\mathcal{P}$ prolonge un élément de S,

(ii) la réduction de $a \bmod \mathcal{P}$ est l'infini (ce que l'image de a par la place de L qui correspond à $\mathcal{P}$ est l'infini),

(iii) il existe des indices j, k distincts tels que $b_j \equiv b_k \bmod \mathcal{P}$,

(iv) il existe un indice i tel que $\mathcal{P}$ divise ν_i ou $\nu_i\beta_i$.

LEMME 4.2.— *Sous les hypothèses précédentes, supposons que l'indice de ramification de tout anneau de Σ_a est divisible par un entier $e_a \geq 2$. Soit $\mathcal{P}$ un idéal premier de O_L avec $\mathcal{P} \notin S_a$. Notons $k = O_E/O_E \cap \mathcal{P}$ et $\overline{a}$ la réduction de $a \bmod \mathcal{P}$. Alors l'indice de ramification de tout anneau de valuation discrète du corps des fonctions $k(C_{\mathcal{P}})$ de la courbe $C_{\mathcal{P}}$ sur k, au-dessus de $X = \overline{a}$, est divisible par e_a.*

Démonstration.— Notons $\overline{C}$ la clôture projective de la courbe C. D'après le théorème 3 de [4, p. 179], il existe une variété projective, non singulière $\mathbb{V}$, de dimension 1, dans un espace projectif $\mathbb{P}^\sigma$ et un épimorphisme birationnel $\varphi : \mathbb{V} \to \overline{C}$. Soit $V \in \Sigma_a$. Comme la variété $\mathbb{V}$ est non singulière et birationnelle à $\overline{C}$, il résulte qu'il existe un point Q sur $\mathbb{V}$, tel que $V = \mathcal{O}_Q(\mathbb{V})$, où $\mathcal{O}_Q(\mathbb{V})$ est l'anneau local de $\mathbb{V}$ en Q. Aussi, il existe un point $P = (a, c)$ sur C, tel que V domine l'anneau local $\mathcal{O}_P(C)$ de C en P (i.e. $\mathcal{O}_P(C) \subseteq V$ et l'idéal maximal de V contient l'idéal maximal de $\mathcal{O}_P(C)$). Enfin, on a $\varphi(Q) = (a : c : 1)$.

Notons M un corps de nombres tel que $L \subseteq M$ et $\mathbb{V}$, φ et Q sont définis sur M. Notons O_M l'anneau des entiers de M, Π un idéal premier de O_M, avec $\Pi \cap O_L = \mathcal{P}$ et w_Π la valuation discrète sur M, qui est associée à Π. Considérons l'unique prolongement w de w_Π à $M(C)$ défini par (4.1). La valuation discrète w n'est pas ramifiée. Soit π un élément de O_M avec $w_\Pi(\pi) = 1$. Alors π est aussi une uniformisante pour w. Si $V = V_j$, pour simplifier la notation posons $t = t_j$, $u = u_j$, $e = e_j$, $\beta = \beta_j$ et $h = h_j$. Supposons que $w(t) = \mu \neq 0$; alors on a $w(t\pi^{-\mu}) = 0$. On peut donc supposer que $w(t) = 0$; il en résulte $w(u) = 0$. Notons $\overline{t}$ et $\overline{u}$ les réductions des fonctions t et $u \bmod \mathcal{P}$. Comme $w(t) = 0 = w(u)$, on a $\overline{t}$, $\overline{u} \neq 0, \infty$.

Soient $\overline{Q}$ et $\overline{c}$ la réduction de Q et $c \bmod \mathcal{P}$. Notons $\mathbb{V}_{\mathcal{P}}$ la réduction de la variété $\mathbb{V} \bmod \mathcal{P}$ et $\varphi_{\mathcal{P}}$ la réduction de l'application $\varphi \bmod \mathcal{P}$. Comme $\mathcal{P} \notin S_a$, l'image $\overline{a}$ de a dans k est finie, d'où il résulte que le point $(\overline{a} : \overline{c} : \overline{1})$

sur $C_{\mathcal{P}}$ est fini. Aussi on a $\varphi_{\mathcal{P}}(\overline{Q}) = (\overline{a} : \overline{c} : \overline{1})$. On en déduit que $\varphi_{\mathcal{P}}$ et $\overline{Q}$ sont définis $\bmod \mathcal{P}$. De plus, $\varphi_{\mathcal{P}}$ est une application birationnelle, donc la réduction $\mathbb{V}_{\mathcal{P}}$ de la variété $\mathbb{V}$ est un ensemble irréductible, donc une variété. On a $u = \beta + h$, où β est un élément non nul de E et h appartient à l'idéal maximal de V. Comme $\mathcal{P} \notin S_a$, la réduction $\overline{\beta}$ de $\beta \bmod \mathcal{P}$ est $\neq 0, \infty$. Si $w(h) < 0$, on a $w(u) < 0$, ce qui n'est pas le cas; si $w(h) > 0$, on a $\overline{u} = \overline{\beta} \neq 0, \infty$; si $w(h) = 0$, la réduction $\overline{h}$ de $h \bmod \mathcal{P}$ est $\neq 0, \infty$ et on a $\overline{h}(\overline{Q}) = \overline{h(Q)} = 0$, car h un élément de l'idéal maximal de V. On a donc $\overline{u}(\overline{Q}) = \overline{\beta} \neq 0, \infty$. Par conséquent $\overline{u}$ est une unité dans l'anneau local $\mathcal{O}_{\overline{Q}}(\mathbb{V}_{\mathcal{P}})$ de $\mathbb{V}_{\mathcal{P}}$ en $\overline{Q}$. Aussi, on a $\overline{t} \neq 0, \infty$ et $\overline{t}(\overline{Q}) = \overline{t(Q)} = 0$, ce qui montre que $\overline{t}$ est un élément (non nul) de l'idéal maximal de $\mathcal{O}_{\overline{Q}}(\mathbb{V}_{\mathcal{P}})$.

Soit une $\overline{k}$ clôture algébrique de k. Considérons un anneau de valuation discrète U dans $\overline{k}(C_{\mathcal{P}})$, tel que U domine $\mathcal{O}_{\overline{Q}}(\mathbb{V}_{\mathcal{P}})$ (par conséquent U se trouve au-dessus de $X = \overline{a}$). On a :

$$X - \overline{a} = \overline{t}^e \overline{u}.$$

La fonction $\overline{u}$ est une unité dans $\mathcal{O}_{\overline{Q}}(\mathbb{V}_{\mathcal{P}})$ et $\overline{t}$ un élément (non nul) de l'idéal maximal de $\mathcal{O}_{\overline{Q}}(\mathbb{V}_{\mathcal{P}})$. Il en résulte que $\overline{u}$ est une unité en U et $\overline{t}$ un élément de l'idéal maximal de U. Par conséquent l'indice de ramification de U est divisible par e_a. Les fonctions t et u sont définies sur E, d'où on conclut que l'indice de ramification de $U \cap k(C_{\mathcal{P}})$ sur $k(X)$ est divisible par e_a également.

Comme $\mathcal{P} \notin S_a$, les réductions des points (a, b_i), $i = 1, \ldots, s$, $\bmod \mathcal{P}$ sont deux à deux distinctes. Donc les points sur la courbe $C_{\mathcal{P}}$, au-dessus de $X = \overline{a}$, sont les réductions des points (a, b_i), $i = 1, \ldots, s$, $\bmod \mathcal{P}$. Il en résulte que si U est un anneau de valuation discrète dans $\overline{k}(C_{\mathcal{P}})$, au-dessus de $X = \overline{a}$, il existe un point Q sur $\mathbb{V}$, tels que U domine $\mathcal{O}_{\overline{Q}}(\mathbb{V}_{\mathcal{P}})$ (on note $\overline{Q}$ la réduction de $Q \bmod \mathcal{P}$) et on se ramène ainsi au cas précédent. On a donc que l'indice de ramification de tout anneau de valuation discrète de $k(C_{\mathcal{P}})$, au-dessus de $X = \overline{a}$, est divisible par e_a.

5. Quelques résultats quantitatifs

Soit

$$F(X, Y) = \sum_{\substack{i=0 \\ j=0}}^{m,n} a_{ij} X^i Y^j$$

un polynôme de $K[X, Y]$, absolument irréductible.

Notons $N = \max\{m, n\}$. Soit $a_{k\ell}$ un coefficient non nul de $F(X, Y)$. Notons δ le plus petit entier positif tel que les éléments $c_{ij} = \delta(a_{ij}/a_{k\ell})$, $i = 0, \ldots, m$, $j = 0, \ldots, n$, soient des entiers de O_K. Le polynôme $G(X, Y) = (\delta/a_{k\ell})F(X, Y)$ définit une courbe algébrique C sur K. On considère $G(X, Y)$ comme polynôme à coefficients dans $K[X]$ et on note $D_G(X)$ son discriminant.

Soient $a_1, \ldots, a_s \in \overline{K}$ et (a_i, b_{ij}), $j = 1, \ldots, t(i)$, les points sur C, qui se trouvent au-dessus de $X = a_i$, $i = 1, \ldots, s$. Supposons que l'extension $\overline{K}(C)/\overline{K}(X)$ est ramifiée au-dessus de $X = a_i$, $i = 1, \ldots, s$. Notons $E_i = K(a_i)$, $i = 1, \ldots, s$. Soient V_{ij}, $j = 1, \ldots, r(i)$, les éléments de Σ_{a_i} et e_{ij}, $j = 1, \ldots, r(i)$, leurs indices de ramification respectifs. D'après le lemme 3.1, pour tout i et $j \leq r(i)$ il existe une uniformisante t_{ij} en V_{ij}, définie sur E_i. On a :

$$X - a_i = t_{ij}^{e_{ij}} u_{ij} ,$$

où u_{ij} est une unité en V_{ij}, définie sur E_i, $j = 1, \ldots, r(i)$. Aussi, on a $u_{ij} = \beta_{ij} + h_{ij}$, où h_{ij} est un élément de l'idéal maximal de V_i et β_{ij} un élément non nul de $\overline{K}$. De plus, il existe un corps de nombres E_{ij}, avec $E_i \subseteq E_{ij}$ et $[E_{ij} : E_i] \leq n$, tel que h_{ij} est défini sur E_{ij} et $\beta_{ij} \in E_{ij}$. Le lemme 3.2 entraîne :

$$H(\beta_{ij}) < \left(N^6 H(F)\right)^{10^3 N^{13}}, \quad j = 1, \ldots, r(i).$$

Notons ν_{ij} le plus petit entier positif tel que $\nu_{ij}\beta_{ij}$ est un entier de E_{ij}.

Notons E' le composé des corps E_{ij}, $i = 1, \ldots, s$, $j = 1, \ldots, r(i)$, et $O_{E'}$ l'anneau des entiers de E'. On désigne par S l'ensemble des idéaux entiers premiers $\mathcal{P}$ de $E'(b_{11}, b_{12}, \ldots, b_{s\,t(s)})$ qui ont une des propriétés suivantes :

(i) $\mathcal{P}$ divise un des coefficients non nuls de $G(X, Y)$ ou de $D_G(X)$,

(ii) il existe un indice i tel que la réduction de $a_i \bmod \mathcal{P}$ est l'infini,

(iii) il existe des indices j, k distincts avec $a_j \equiv a_k \bmod \mathcal{P}$,

(iv) il existe des indices i, j, k tels que $j \neq k$ et $b_{ij} \equiv b_{ik} \bmod \mathcal{P}$,

(v) il existe des indices i, j tels que $\mathcal{P}$ divise ν_{ij} ou $\nu_{ij}\beta_{ij}$.

Posons $E = K(a_1, \ldots, a_s)$ et notons O_E l'anneau des entiers de E. On désigne par T l'ensemble des idéaux premiers P de O_E tels que $P = O_E \cap \mathcal{P}$, où $\mathcal{P} \in S$. Enfin, si L est un corps de nombres, on note N_L la norme de L sur $\mathbb{Q}$.

LEMME 5.1.— *Sous les hypothèes précédentes on a :*

$$N_E\left(\prod_{P\in T} P\right) < \left(N^6 H(F)\right)^{5sd^2 10^3 N^{18}(2N^2)^s}.$$

Démonstration. — En utilisant le théorème 5.9 de [23, p. 211] et le lemme 5.10 de [23, p. 213], on déduit :

$$\delta < \left(2H\left(\frac{a_{ij}}{a_{k\ell}}\right)\right)^{dN^2} = \left(2H(a_{ij}, a_{k\ell})\right)^{dN^2} \leq \left(2H(F)\right)^{dN^2}.$$

Alors on a :

$$\begin{aligned} N_K(c_{ij}) \leq H_K(c_{ij}) = H_K\left(\delta\left(\frac{a_{ij}}{a_{k\ell}}\right)\right) = \delta^d H_K\left(\frac{a_{ij}}{a_{k\ell}}\right) \leq \\ \leq \delta^d H_K(F) < 2^{d^2N^2} H_K(F)^{dN^2+1}. \end{aligned} \tag{5.1}$$

Soit

$$D_G(X) = c_0 X^\nu + \cdots + c_\nu,$$

où $\nu < 2N(N-1)$. La démonstration du lemme 4 de [15] entraîne :

$$N_K(c_j) \leq H_K(c_j) < N^{10\,dN} H_K(F)^{2N}. \tag{5.2}$$

Soient $P_1, \ldots, P_k$ les idéaux premiers de O_E qui divisent un des coefficients de $G(X,Y)$ ou de $D_G(X)$. Alors les inégalités (5.1) et (5.2) donnent :

$$\begin{aligned} N_E(P_1, \ldots, P_k) \leq \left(\prod_{\substack{i=0\\ j=0}}^{m,n} N_K(c_{ij}) \prod_{i=0}^{\nu} N_K(c_j)\right)^{(2N^2)^s} \\ \leq \left(N^4 H(F)\right)^{4d^2N^4(2N^2)^s}. \end{aligned} \tag{5.3}$$

Soit ε_i le plus petit entier positif tel que $\varepsilon_i a_i$ soit un entier algébrique. Le théorème 5.9 de [23, p. 211], et le lemme 5.10 de [23, p. 213], entraînent :

$$\varepsilon_i < \left(2H(a_i)\right)^{2dN(N-1)}.$$

D'autre part les lemmes 3 et 4 de [15] impliquent :

$$H(a_1)\cdots H(a_s) \leq 2N^2 H(D_G) < 2N^2 N^{10N} H(F)^{2N-1}. \tag{5.4}$$

On en déduit :

$$\varepsilon_1 \cdots \varepsilon_s < \left(2^s H(a_1)\cdots H(a_s)\right)^{2dN^2} < 4^{(s-1)dN^2}\left(N^6 H(F)\right)^{4dN^3}. \tag{5.5}$$

Soit Π le produit des idéaux premiers $\mathcal{P}$ de O_E tels que pour un indice i la réduction de $a_i \bmod \mathcal{P}$ est l'infini. Alors l'idéal Π divise l'entier $\varepsilon_1 \cdots \varepsilon_s$. Il en résulte :

$$N_E(\Pi) \leq N_E(\varepsilon_1 \cdots \varepsilon_s) < \left(4^{s-1}\left(N^6 H(F)\right)^{4N}\right)^{d^2N^2(2N^2)^s}. \tag{5.6}$$

Soit $i \neq j$. Alors on a :

$$H\left(\varepsilon_i\varepsilon_j(a_i - a_j)\right) \leq 2\varepsilon_i\varepsilon_j H(a_i)H(a_j) < \\ < \left(4H(a_i)H(a_j)\right)^{2dN^2} < \left(N^7 H(F)\right)^{4dN^3}.$$

Si P est le produit des idéaux premiers $\mathcal{P}$ de O_E, tels qu'il existe des indices k, ℓ distincts, avec $a_k \equiv a_\ell \bmod \mathcal{P}$, l'idéal P divise l'entier algébrique

$$\prod_{k<\ell} \varepsilon_k\varepsilon_\ell(a_k - a_\ell).$$

Donc, on a :

$$N_E(P) \leq \left(\prod_{k<\ell} \varepsilon_k\varepsilon_\ell(a_k - a_\ell)\right) < \prod_{k<\ell} H_E\left(\varepsilon_k\varepsilon_\ell(a_k - a_\ell)\right) < \\ < \left(N^7 H(F)\right)^{2s^2d^2N^2(2N^2)^s}. \tag{5.7}$$

On vérifie facilement que

$$H(b_{ij}) \leq N(N+1)H(F)H(a_i)^N, \quad i = 1, \ldots, s,\ j = 1, \ldots t(i),$$

Alors l'inégalité (5.4) donne :

$$H(b_{ij}) < N^{13N^2} H(F)^{2N^2}. \tag{5.8}$$

Soit ζ_{ij} le plus petit entier positif tel que $\zeta_{ij}b_{ij}$ soit un entier algébrique. Le théorème 5.9 de [23, p. 211], le lemme 5.10 de [23, p. 213] et l'inégalité (5.8) entraînent :

$$\zeta_{ij} < \big(2H(b_{ij})\big)^{2dN^3} < \big(N^7H(F)\big)^{4dN^5}, \quad i = 1, \ldots, s, \; j = 1, \ldots t(i). \tag{5.9}$$

Posons $M_{ik\ell} = E(b_{ik}, b_{i\ell})$, où $k \neq \ell$. Soit $P_{ik\ell}$ le produit des idéaux entiers premiers P de $M_{ik\ell}$ tels que $b_{ik} \equiv b_{i\ell} \bmod P$. Alors l'idéal $P_{ik\ell}$ divise l'entier algébrique $\zeta_{ik}\zeta_{i\ell}(b_{ik} - b_{i\ell})$. Les inégalités (5.8) et (5.9) donnent :

$$\begin{aligned} N_{M_{ik\ell}}\big(\zeta_{ik}\zeta_{i\ell}(b_{ik} - b_{i\ell})\big) &\leq H_{M_{ik\ell}}\big(\zeta_{ik}\zeta_{i\ell}(b_{ik} - b_{i\ell})\big) < \\ &< \big(2\zeta_{ik}\zeta_{i\ell}H(b_{ik})H(b_{i\ell})\big)^{dN^2(2N^2)^s} \\ &< \big(N^7H(F)\big)^{9d^2N^7(2N^2)^s}. \end{aligned}$$

Notons $\mathcal{P}_{ik\ell} = P_{ik\ell} \cap O_E$. On en conclut :

$$N_E\left(\prod_{i=1}^{s}\prod_{k<\ell}\mathcal{P}_{ik\ell}\right) < \big(N^7H(F)\big)^{5sd^2N^9(2N^2)^s}. \tag{5.10}$$

Le théorème 5.9 de [23, p. 211] et le Lemme 5.10 de [23, p. 213], entraînent :

$$\nu_{ij} < \big(2H(\beta_{ij})\big)^{[E_{ij}:\mathbb{Q}]} < 4^{dN^3}\big(N^6H(F)\big)^{2d10^3N^{16}},$$

d'où on a :

$$N_{E_{ij}}(\nu_{ij}\beta_{ij}) \leq H_{E_{ij}}(\nu_{ij}\beta_{ij}) = H\big(\nu_{ij}\beta_{ij}\big)^{[E_{ij}:\mathbb{Q}]} < \big(N^6H(F)\big)^{5d^210^3N^{19}}.$$

Soit P_{ij} le produit des idéaux premiers entiers de E_{ij} qui divisent ν_{ij} ou $\nu_{ij}\beta_{ij}$. Notons $\mathcal{P}_{ik} = P_{ik} \cap O_E$. Alors on a :

$$N_E\left(\prod_{i,k}\mathcal{P}_{ik}\right) < \big(N^6H(F)\big)^{4sd^210^3N^{18}(2N^2)^s}. \tag{5.11}$$

Enfin les inégalités (5.3), (5.6), (5.7), (5.10) et (5.11) donnent le résultat.

LEMME 5.2. — *Soit $C : F(X,Y) = 0$ une courbe algébrique (irréductible) définie sur K. Supposons que l'extension $\overline{K}(C)/\overline{K}(X)$ est ramifiée au-dessus des places finies $X = x_i$, $i = 1, \ldots, s$. Notons $E = K(x_1, \ldots, x_s)$. Alors le discriminant D_E de E satisfait la majoration suivante :*

$$|D_E| < N^{100\,d^2s2^sN^{5+2s}}\big|D_K\big|^{(2N(N-1))^s}H_K(F)^{16\,ds2^sN^{5+2s}}.$$

Démonstration. — On considère $F(X,Y)$ comme polynôme à coefficients dans $K[X]$ et on note $D(X)$ son discriminant. On a $\deg D(X) \leq 2N(N-1)$. Les éléments $x_1, \ldots, x_s$ sont parmi les racines de $D(X)$. Notons $x_1, \ldots, x_\mu$ ($\mu \geq s$), les racines de $D(X)$ qui sont deux à deux distinctes. Soit δ le plus petit entier positif tel que les nombres δx_i, $i = 1, \ldots, \mu$, sont des entiers algébriques. Supposons que $x_1 \notin K$; posons $K_1 = K(x_1)$ et notons D_{K_1} le discriminant du corps K_1. La formule de transitivité des discriminants donne :

$$|D_{K_1}| \leq |D_K|^{2N(N-1)} |N_K(D(P))|$$

où $D(P)$ est le discriminant du polynôme irréductible $P(X)$ de δx_1 sur K. Notons $B(X)$ le polynôme unitaire dont les racines sont les éléments $\delta x_1, \ldots, \delta x_\mu$ et D_B son discriminant. Comme $P(X)$ divise $B(X)$, on a :

$$|D_{K_1}| \leq |D_K|^{2N(N-1)} |N_K(D_B)| \leq |D_K|^{2N(N-1)} H_K(D_B).$$

On continue en procédant de cette façon et on obtient l'inégalité suivante :

$$|D_E| \leq |D_K|^{(2N(N-1))^s} H_K(D_B)^{s(2N(N-1))^{s-1}}. \tag{5.12}$$

D'autre part, le lemme 4 de [15] entraîne :

$$H_K(D) < N^{10\,dN} H_K(F)^{2N} \tag{5.13}$$

et

$$H_K(D_B) \leq N^{20\,dN^2} H_K(B)^{4N^2}. \tag{5.14}$$

Alors les inégalités (5.12) et (5.14) entraînent :

$$|D_E| \leq N^{10\,ds2^sN^{2s}} |D_K|^{(2N(N-1))^s} H_K(B)^{2s(2N^2)^s}. \tag{5.15}$$

Notons $x_1, \ldots, x_\nu$ les racines de $D(X)$ (avec multiplicité). Soit $B'(X)$ le polynôme unitaire dont les racines sont les éléments $\delta x_1, \ldots, \delta x_\nu$. Le théorème 5.9 de [23, p. 211] et le lemme 3 de [15] donnent :

$$\delta < N^{8dN^2} H_K(D)^{2N(N-1)}.$$

Alors on a :

$$H_K(B') \leq \delta^{2dN^2} H_K(D) \leq N^{16\,d^2N^4} H_K(D)^{4dN^4}.$$

En utilisant l'inégalité (5.13) il résulte :

$$H_K(B') < N^{48\,d^2N^5} H_K(F)^{8dN^5}.$$

Alors la proposition 2.4 de [10, p. 57], entraîne :

$$H_K(B) < N^{49\,d^2N^5} H_K(F)^{8dN^5}. \tag{5.16}$$

Enfin les inégalités (5.15) et (5.16) donnent le résultat.

LEMME 5.3. — *Soient E un corps nombres et O_E l'anneau des entiers de E. Soit L une extension finie galoisienne de E de degré λ. Supposons qu'il existe un ensemble fini T d'idéaux premiers de O_E tel que l'extension L/E soit non ramifiée en dehors de T. Alors le discriminant D_L de L vérifie l'inégalité :*

$$|D_L| \leq |D_E|^{\lambda} N_E \left(\prod_{P \in T} P \right)^{\lambda^3}.$$

Démonstration. — Notons $D_{L/E}$ le discriminant de L sur E. D'après la formule de transitivité des discriminants, on a :

$$|D_L| = |D_E|^{\lambda} N_E(D_{L/E}).$$

Notons $\mathcal{D}_{L/E}$ la différente de L sur E. Posons

$$\mathcal{D}_{L/E} = \mathcal{P}_1^{r_1} \cdots \mathcal{P}_k^{r_k},$$

où $r_1, \ldots, r_k \in \mathbb{Z}$ et $\mathcal{P}_1, \ldots, \mathcal{P}_k$ sont des idéaux entiers premiers de L distincts, avec $\mathcal{P}_j \cap O_E \in T$, $j = 1, \ldots, k$. D'après [18, proposition 4, p. 72, remarque 2, p. 73 et exercice 3.c, p. 79], on déduit $r_j < \lambda^2$, $j = 1, \ldots, k$. Notons $N_{L/E}$ la norme de L sur E. Alors il résulte :

$$D_{L/E} = N_{L/E}(\mathcal{D}_{L/E}) = N_{L/E}(\mathcal{P}_1^{r_1} \cdots \mathcal{P}_k^{r_k}) \supseteq \left(N_{L/E}(\mathcal{P}_1) \cdots N_{L/E}(\mathcal{P}_k)\right)^{\lambda^2}.$$

Soient $\mathcal{G}_{b_1}, \ldots, \mathcal{G}_{b_m}$ tous les idéaux entiers premiers de L au-dessus d'un même $P \in T$ et f leur degré résiduel commun. Alors on a $N_{L/E}(\mathcal{G}_{b_j}) = P^f$, $j = 1, \ldots, m$, et $mf \leq \lambda$. On en conclut :

$$|D_L| \leq |D_E|^{\lambda} N_E \left(\prod_{P \in T} P \right)^{\lambda^3}.$$

LEMME 5.4. — *Soient K et L deux corps de nombres. Notons D_K et D_L les discriminants de K et L respectivement. Alors le discriminant D_{KL} du composé KL des corps K et L satisfait l'inégalité suivante :*

$$|D_{KL}| \leq |D_K|^{[LK:K]} |D_L|^{[LK:L]} .$$

Démonstration. — Notons $\mathcal{D}_{KL}$, $\mathcal{D}_K$ et $\mathcal{D}_L$ les différentes des corps KL, K et L respectivement; notons aussi $\mathcal{D}_{KL/K}$ la différente de KL sur K. La formule de transitivité pour les différentes donne :

$$\mathcal{D}_{KL} = \mathcal{D}_{KL/K} \mathcal{D}_K .$$

La différente $\mathcal{D}_{KL/K}$ est engendrée par les éléments $f'(x)$, où x est un entier de KL et $f'(X)$ le polynôme dérivé de son polynôme minimal $f(X)$ sur K. Soit y un entier de L et $g(X)$, $h(X)$ les polynômes minimaux de y sur K et $\mathbb{Q}$ respectivement. Alors l'idéal $\mathcal{D}_{KL/K}$ contient $g'(y)$, d'où il résulte que $\mathcal{D}_{KL/K}$ contient aussi $h'(y)$. Donc on a $\mathcal{D}_L \subseteq \mathcal{D}_{KL/K}$. On en déduit :

$$\begin{aligned} |D_{KL}| = |N_{KL}(\mathcal{D}_{KL})| &= |N_{KL}(\mathcal{D}_{KL/K})||N_{KL}(\mathcal{D}_K)| \leq \\ &\leq |N_{KL}(\mathcal{D}_L)||N_K(\mathcal{D}_K)|^{[LK:K]} \leq |D_K|^{[LK:K]} |D_L|^{[LK:L]} . \end{aligned}$$

LEMME 5.5. — *Soient α un entier ≥ 2 et $a_1, \ldots, a_q \in K$, deux à deux distincts, avec $\alpha q > \alpha + q$. Notons $f(X) = a(X - a_1) \cdots (X - a_q)$. Alors si x, $y \in O_K$ avec $y^\alpha = f(x)$, on a :*

$$\max\{H_K(x), H_K(y)\} < \exp\left\{2^{150 q^3 d^2 \alpha^7} |D_K|^{8\alpha^5} H_K(f)^{35 q^2 \alpha^7}\right\} .$$

On peut consulter [12], pour une démonstration d'un résultat plus général.

LEMME 5.6. — *Soit $C : F(X,Y) = 0$ une courbe (irréductible) de genre ≥ 1. Notons M le degré total de $F(X,Y)$. Soit $h = \eta(X,Y)/\xi(X,Y)$ une fonction de $\overline{K}(C)$ avec $\eta(X,Y)$, $\xi(X,Y) \in K[X, Y]$. Soient Φ_1, Φ_2 deux constantes > 0, telles que $H(\eta)$, $H(\xi) < \Phi_1$ et le degré total des η et ξ est $< \Phi_2$. Supposons que le diviseur des pôles de h soit :*

$$(h)_\infty = k_1 V_1 + \cdots + k_r V_r ,$$

où $V_i \in \Sigma_\infty$ et $k_i > 0$, $i = 1, \ldots, r$. Notons $\deg(h)_\infty = \delta$. Alors on a :

(1) pour tout diviseur $E = \ell_1 V_1 + \cdots + \ell_r V_r$, *avec* $\ell_i \geq k_i$, $i = 1, \ldots, r$, *et* $2g + \delta \geq \deg E \geq 2g$, *tel que les entiers* δ *et* $\deg E$ *soient premiers entre eux, il existe une fonction* $f \in \overline{K}(C)$ *avec* $(f)_\infty = E$ *et* $\overline{K}(f,h) = \overline{K}(C)$;

(2) la fonction f *est définie sur un corps de nombres* L, *avec* $K \subseteq L$ *et* $[L : K] \leq n^r$; *le discriminant* D_L *de* L *satisfait l'inégalité suivante :*

$$|D_L| < \left[(2M)^{865\,dM^{21}} |D_K|^M H_K(F)^{48\,M^{11}}\right]^{rM^{r-1}} ;$$

(3) il existe un polynôme $G(X,Y)$ *à coefficients dans l'anneau des entiers* O_L *de* L, *absolument irréductible, tel que l'équation* $G(f,h) = 0$ *soit un modèle de la courbe* C *et une équation de dépendance intégrale de* f *sur l'anneau* $O_L[h]$; *notons* $\Xi = \max\{M\,,\, 2g + k_1, \ldots, 2g + k_r\}$; *alors on a* $\deg_X G = \delta$, $\deg_Y G \leq 2g + \delta - 1$ *et*

$$H_L(G) < \Omega |D_K|^{r\Xi^r \delta^3 g^2} H_K(F)^{420\,\Xi^{16+r}\delta^{11}2^{2g+\delta}g^7\Phi_2^2},$$

où

$$\Omega = \Phi_1^{8\delta^{11}g^7\Xi^5\Phi_2^2}(2\Xi)^{1\,200\,d\,\Xi^{21+r}\delta^{15}g^7 2^{2g+\delta}\Phi_2^4} ;$$

(4) la fonction h *est un élément entier sur l'anneau* $O_L[X]$;

(5) supposons qu'il existe une constante $\Phi > 0$, *telle que si* $x, y \in O_K$ *avec* $F(x,y) = 0$, *on a* $H_L(h(x,y)) < \Phi$. *Alors on a :*

$$\max\{H_L(x)\,,\, H_L(y)\} < \Psi H_K(F)^{500\,\delta^8\Xi^{17+r}2^{2g+\delta}g^5\Phi_2^2},$$

où

$$\Psi = \Phi^{\Xi^2}\Phi_1^{8\delta^8 g^5\Xi^5\Phi_2^2}(2\Xi)^{7\,000\,\delta^{12}\Xi^{21+r}dg^5 2^{2g+\delta}\Phi_2^4}.$$

C'est le théorème 2 de [14].

6. Démonstration de la proposition 2.2

Soit

$$F(X,Y) = \sum_{\substack{i=0 \\ j=0}}^{m,n} a_{ij} X^i Y^j .$$

Soit $a_{k\ell}$ un coefficient non nul de $F(X,Y)$. Si δ est le plus petit entier positif, tel que les éléments $\delta(a_{ij}/a_{k\ell})$, $i = 0, \ldots, m$, $j = 0, \ldots, n$, soient des entiers de O_K, posons $G(X,Y) = (\delta/a_{k\ell})F(X,Y)$. On note $D_G(X)$ le discriminant de $G(X,Y)$, considéré comme polynôme à coefficients dans $K[X]$. Notons $E = K(a_1, \ldots, a_s)$ et O_E l'anneau des entiers de E.

Soient (a_i, b_{ij}), $j = 1, \ldots, t(i)$, les points sur C qui se trouvent au-dessus de $X = a_i$, $i = 1, \ldots, s$. Notons $E_i = K(a_i)$, $i = 1, \ldots, s$. Soient V_{ij}, $j = 1, \ldots, r(i)$, les éléments de Σ_{a_i} et e_{ij}, $j = 1, \ldots, r(i)$, leurs indices de ramification respectifs. Le lemme 3.1 entraîne que pour tout i et $j \leq r(i)$ il existe une uniformisante t_{ij} en V_{ij}, définie sur E_i. Alors il existe une unité u_{ij} dans V_{ij}, définie sur E_i telle que :

$$X - a_i = t_{ij}^{e_{ij}} u_{ij} .$$

Aussi, on a $u_{ij} = \beta_{ij} + h_{ij}$, où $\beta_{ij} \in \overline{K}$ avec $\beta_{ij} \neq 0$ et h_{ij} appartient à l'idéal maximal de V_{ij} ; il existe un corps de nombres E_{ij}, avec $E_i \subseteq E_{ij}$ et $[E_{ij} : E_i] \leq n$, tel que $\beta_{ij} \in E_{ij}$ et la fonction h_{ij} est définie sur E_{ij}, $j = 1, \ldots, r(i)$. Le lemme 3.2 donne une majoration pour la hauteur absolue de β_{ij}. Notons ν_{ij} le plus petit entier positif tel que $\nu_{ij}\beta_{ij}$ est un entier de E_{ij}.

Soit E' le composé des corps E_{ij}, $i = 1, \ldots, s$, $j = 1, \ldots, r(i)$. On désigne par S l'ensemble des idéaux entiers premiers $\mathcal{P}$ de $\mathbb{E} = E'(b_{11}, b_{12}, \ldots, b_{s\,t(s)})$, qui ont une des propriétés suivantes :

(i) $\mathcal{P}$ divise un des coefficients de $G(X,Y)$ ou de $D_G(X)$,

(ii) il existe un indice i tel que la réduction de $a_i \bmod \mathcal{P}$ est l'infini,

(iii) il existe des indices j, k tels que $j \neq k$ et $a_j \equiv a_k \bmod \mathcal{P}$,

(iv) il existe des indices i, j, k tels que $j \neq k$ et $b_{ij} \equiv b_{ik} \bmod \mathcal{P}$,

(v) il existe des indices i, j tels que $\mathcal{P}$ divise ν_{ij} ou $\nu_{ij}\beta_{ij}$.

Posons $E = K(a_1, \ldots, a_s)$ et notons O_E l'anneau des entiers de E. On désigne par T l'ensemble des idéaux premiers P de O_E, tels que $P = O_E \cap \mathcal{P}$, où $\mathcal{P} \in S$.

Soient $x, y \in O_K$ avec $F(x,y) = 0$ et $x \neq a_i$, $i = 1, \ldots, s$. Soit $r \in \overline{K}$ avec $r^e = (x - a_1) \cdots (x - a_s)$. Alors le corps engendré sur E par les éléments de l'ensemble $\Phi^{-1}(x,y)$ est le corps $L = E(r, \zeta)$, où ζ est une racine primitive $e^{\text{ième}}$ de 1. Soit $\mathcal{P}$ un idéal entier premier de $\mathbb{E}$, qui n'est pas élément de S. Notons $\overline{x}$ et $\overline{y}$ les réductions de x et $y \bmod \mathcal{P}$ respectivement et $O_{E,P}$ le localisé de l'anneau O_E en $P = \mathcal{P} \cap O_E$. Le lemme 4.1 entraîne que la réduction $\bmod P$ du polynôme $G(X,Y)$ est un polynôme $\overline{G}(X,Y)$ absolument irréductible. Notons C_P la courbe algébrique définie par l'équation $\overline{G}(X,Y) = 0$, sur le corps fini $k = O_E/P$. Soit $\overline{a}_i$ la réduction de $a_i \bmod \mathcal{P}$, $i = 1, \ldots, s$. Comme $\mathcal{P} \notin S$, il résulte que les éléments $\overline{a}_1, \ldots, \overline{a}_s \in k$ sont deux à deux distincts. D'après le lemme 4.2, l'indice de ramification de tout anneau de valuation discrète de $k(C_P)$, au-dessus de l'anneau de $k(X)$ associé à $X - \overline{a}_i$, est divisible par e.

Notons $\left[E(r) : E\right] = \xi$. Supposons que $\overline{x} \neq \overline{a}_i$, $i = 1, \ldots, s$. Comme $\overline{a}_1, \ldots, \overline{a}_s \in k$ et $x \in O_E$, il résulte que l'élément r est entier sur $O_{E,P}$. Le discriminant $D(1, r, \ldots, r^{\xi-1})$ des éléments $1, r, \ldots, r^{\xi-1}$ divise le discriminant du polynôme $\Pi(X) = X^e - (x - a_1) \cdots (x - a_s)$, dans $O_{E,P}$, qui est égal à

$$D_\Pi = (-1)^{e-1} e^e \left[(x - a_1) \cdots (x - a_s)\right]^{e-1}.$$

On a $\overline{x} \neq \overline{a}_i$ $(i = 1, \ldots, s)$ et $\overline{a}_1, \ldots, \overline{a}_s \in k$; alors $(\overline{x} - \overline{a}_i) \cdots (\overline{x} - \overline{a}_s) \neq 0, \infty$. On en déduit que D_Π est une unité dans $O_{E,P}$, d'où on a que $D(1, r, \ldots, r^{\xi-1})$ est une unité dans $O_{E,P}$. Le discriminant Δ de la fermeture intégrale de $O_{E,P}$ dans $E(r)$ divise $D(1, r, \ldots, r^{\xi-1})$; donc Δ est une unité dans $O_{E,P}$. Cela montre que l'idéal premier P est non ramifié dans $E(r)$.

Supposons que $\overline{x} = \overline{a}_i$, $1 \leq i \leq s$. Soit V un anneau de valuation discrète de $k(C_P)$, au-dessus de l'anneau local de C_P au point $(\overline{x}, \overline{y})$. On note v l'indice de ramification de V; alors $v = eh$, où $h \in \mathbb{Z}$. Soit τ une uniformisante en V. Comme la fonction τ est définie sur k, il existe $t \in E(C)$, avec $t(x,y) \neq 0$, tel que la réduction de $t \bmod \mathcal{P}$ coïncide à τ. La fonction $D(X,Y) = (X - \overline{a}_1) \cdots (X - \overline{a}_s)/\tau^v$ est une unité en V, d'où on a $D(\overline{x}, \overline{y}) \neq 0, \infty$. Si l'élément $z = (x - a_1) \cdots (x - a_s)/t^v(x,y)$ n'est pas une unité dans $O_{E,P}$, on a $D(\overline{x}, \overline{y}) = 0$ ou ∞ : il y a donc contradiction, donc z est une unité dans $O_{E,P}$. Comme $\left(r/t(x,y)^h\right)^e = z$, il résulte que $r/t(x,y)^h$ est entier sur

$O_{E,P}$. En considérant les éléments 1, $r/t(x,y)^h$, ..., $(r/t(x,y)^h)^{\xi-1}$ et en procédant comme dans le cas précédent, on déduit que P est non ramifié dans $E(r)$.

D'après le lemme 5.1 on a :

$$N_E\left(\prod_{P\in T} P\right) < \left(N^6 H(F)\right)^{5sd^2 10^3 N^{18}(2N^2)^s}. \tag{6.1}$$

Le discriminant de l'extension $L/E(r)$ divise l'entier e^e. Alors le produit des idéaux entiers premiers de $E(r)$ qui sont ramifiés dans L divise e. Donc les idéaux premiers de O_E qui sont en dehors de S et qui ne divisent pas e sont non ramifiés dans L. Comme l'extension L/E est galoisienne, le lemme 5.3 et l'inégalité (6.1) entraînent que le discriminant D_L de L satisfait l'inégalité

$$|D_L| < |D_E|^{e^2} \left(N^6 H(F)\right)^{6e^6 sd^2 10^3 N^{18}(2N^2)^s}. \tag{6.2}$$

Enfin, le lemme 5.2 et l'inégalité (6.2) donnent :

$$|D_L| < |D_K|^{e^2 2^s N^{2s}} \left(N^6 H(F)\right)^{7d^2 se^6 2^s 10^3 N^{18+2s}}.$$

7. Démonstration du théorème 1

Soient x, $y \in O_K$ avec $F(x,y) = 0$. Considérons le premier cas. Alors il existe a, $b \in \overline{K}$ tels que les indices de ramification des anneaux de Σ_a et Σ_b sont tous divisibles par les entiers $e_a \geq 2$ et $e_b \geq 3$ respectivement. Soient r, $s \in \overline{K}$ tels que $r^{e_a} = x - a$ et $s^{e_b} = x - b$. Notons $L = K(a,b,r,s,\zeta,\eta)$, où ζ est une racine primitive $e_a^{\text{ième}}$ de 1 et η une racine primitive $e_b^{\text{ième}}$ de 1.

On désigne par ε_a et ε_b les plus petits entiers positifs, tels que les éléments $\varepsilon_a a$ et $\varepsilon_b b$ soient des entiers de $K(a,b)$. L'inégalité (5.5) donne :

$$\varepsilon_a \varepsilon_b < N^{25\,dN^3} H_K(F)^{4N^3}. \tag{7.1}$$

Posons $\varepsilon = \varepsilon_a \varepsilon_b$. On a les égalités suivantes :

$$\left(\varepsilon^{e_b} r\right)^{e_a} = \varepsilon^{e_b e_a}(x-a) \quad \text{et} \quad \left(\varepsilon^{e_a} s\right)^{e_b} = \varepsilon^{e_b e_a}(x-b).$$

On en conclut que les nombres $\varepsilon^{e_b} r$ et $\varepsilon^{e_a} s$ sont des entiers de L et vérifient l'égalité :

$$\left(\varepsilon^{e_b} r\right)^{e_a} = \left(\varepsilon^{e_a} s\right)^{e_b} + \varepsilon^{e_b e_a}(b-a).$$

Donc $(X, Y) = (\varepsilon^{e_b} r\,,\ \varepsilon^{e_a} s)$ donne une solution entière de l'équation :

$$Y^{e_b} = X^{e_a} + \varepsilon^{e_b e_a}(a - b)\,.$$

Les inégalités (5.4) et (7.1) entraînent :

$$H\big(\varepsilon^{e_b e_a}(b-a)\big) < N^{26\,dN^5} H_K(F)^{5N^5}\,. \tag{7.2}$$

La Proposition 2.2 entraîne que les discriminants D_{L_a} et D_{L_b} des corps $L_a = K(a, r, \zeta)$ et $L_b = K(b, s, \eta)$ respectivement, vérifient les inégalités :

$$\big|D_{L_i}\big| < \big|D_K\big|^{2e_i^2 N^2} \big(N^6 H(F)\big)^{14\,d^2 e_i^6 10^3 N^{20}}\,, \quad i = a,\, b\,. \tag{7.3}$$

D'après le lemme 5.4 on a :

$$|D_L| < \big|D_{L_a}\big|^{[L:L_a]} \big|D_{L_b}\big|^{[L:L_b]}\,. \tag{7.4}$$

Soit δ le p.g.c.d. des e_a et e_b ; alors on a $e_a = \delta\gamma_a$, $e_b = \delta\gamma_b$ et les entiers γ_a, γ_b sont premiers entre eux; aussi, l'entier $\delta\gamma_a\gamma_b$ divise n et $e_i \le n/2$, $i = a,\, b$. Il en résulte $[L : L_a] \le 2N^2 e_b\gamma_b$ et $[L : L_b] \le 2N^2 e_a\gamma_a$. Alors les inégalités (7.3) et (7.4) entraînent :

$$|D_L| < \big|D_K\big|^{2N^7} \big(N^6 H(F)\big)^{875\,d^2 N^{29}}\,. \tag{7.5}$$

Soit $\theta = (a-b)^{1/e_b}$. Notons $D_{L'}$ le discriminant du corps $L' = L(\theta)$ et $[L' : L] = \xi$. Le discriminant de la base $1, \varepsilon\theta, \ldots, (\varepsilon\theta)^{\xi-1}$ de l'extension L'/L est égal à l'entier algébrique $\alpha = \xi^{\xi}\big(\varepsilon^{\xi}(a-b)\big)^{\xi-1}$. Alors la formule de transitivité des discriminants donne :

$$|D_{L'}| \le \big|D_L\big|^{e_b} N_L(\alpha) \le \big|D_L\big|^{e_b} H_L(\alpha)\,.$$

Les inégalités (7.2) et (7.5) entraînent :

$$|D_{L'}| < \big|D_K\big|^{N^8} \big(N^6 H(F)\big)^{438\,d^2 N^{30}}\,. \tag{7.6}$$

Maintenant on peut utiliser le lemme 5.5 ; donc, le lemme 5.5 et les inégalités (7.2) et (7.6) donnent :

$$\max\big\{H_{L'}(\varepsilon^{e_b} r)\,,\ H_{L'}(\varepsilon^{e_a} s)\big\} < \exp\Big\{\big|D_K\big|^{N^{13}} \big(N^6 H(F)\big)^{110\,d^2 N^{35}}\Big\}\,.$$

On a :

$$x = \frac{\left(\varepsilon^{e_b} r\right)^{e_a} + \varepsilon^{e_b e_a} a}{\varepsilon^{e_b e_a}},$$

d'où il résulte :

$$H_{L'}(x) \leq 2^{[L':\mathbb{Q}]} H_{L'}\left(\varepsilon^{e_b} r\right)^{e_a} H_{L'}(a) \varepsilon^{2 e_b e_a [L':\mathbb{Q}]} ;$$

alors comme on a $H(y) \leq N(N+1) H(F) H(x)^N$, on conclut :

$$\max\left\{H_K(x)\,,\, H_K(y)\right\} < \exp\left\{|D_K|^{N^{13}} \left(N^6 H(F)\right)^{111\, d^2 N^{35}}\right\}.$$

Considérons le deuxième cas. Alors il existe a_1, a_2, $a_3 \in \overline{K}$ tels que les indices de ramification des anneaux des Σ_{a_i} $(i = 1, 2, 3)$ sont tous divisibles par 2. Soit $r \in \overline{K}$ tel que $r^2 = (x - a_1)(x - a_2)(x - a_3)$. Notons $L = K(a_1, a_2, a_3)$.

On désigne par ε_i le plus petit entier positif, tels que l'élément $\varepsilon_i a_i$ est un entier de L, $i = 1, 2, 3$. Posons $\varepsilon = \varepsilon_1 \varepsilon_2 \varepsilon_3$. L'inégalité (5.5) donne :

$$\varepsilon < N^{26\, dN^3} H_K(F)^{4N^3}. \tag{7.7}$$

Le couple $(X, R) = (\varepsilon^2 x, \varepsilon^3 r)$ est une solution entière de l'équation

$$R^2 = f(X) = (X - \varepsilon^2 a_1)(X - \varepsilon^2 a_2)(X - \varepsilon^2 a_3),$$

sur le corps L. Le théorème 5.9 de [23, p. 211], et le lemme 3 de [15] donnent :

$$\begin{aligned} H(f) &\leq 4 H(\varepsilon^2 a_1) H(\varepsilon^2 a_2) H(\varepsilon^2 a_3) < 8 N^2 \varepsilon^6 H(D) < \\ &< N^{158\, dN^3} H_K(F)^{25N^3}. \end{aligned} \tag{7.8}$$

Or la proposition 2.2 entraîne que le discriminant D_L de L satisfait l'inégalité :

$$|D_L| < |D_K|^{32\, N^6} \left(N^6 H(F)\right)^{10\,752\, d^2 10^3 N^{24}}. \tag{7.9}$$

Alors le lemme 5.5 et les inégalités (7.8) et (7.9) nous permettent d'obtenir l'inégalité :

$$\max\left\{H_K(x)\,,\, H_K(y)\right\} < \exp\left\{|D_K|^{2^{13} N^6} \left(N^6 H(F)\right)^{2^8 1\,076\, d^2 10^4 N^{24}}\right\}.$$

En utilisant la formule de Hurwitz [9, p. 26], on déduit facilement que $N \geq 3$, ce qui donne la majoration annoncée dans le théorème 1.

8. Démonstration du théorème 2

Nous allons nous ramener aux hypothèses du lemme 5.6. Notons g le genre de la courbe C. Comme $g \geq 1$, on a $\delta \geq 2$. Supposons d'abord que $\delta \geq 2g$. Alors le degré du diviseur $E = (k_1 + 1)V_1 + k_2V_2 + \cdots + k_rV_r$ est $\delta + 1$. Supposons ensuite que $\delta < 2g$. Posons

$$2g = q\,\delta + u\,,$$

où q, $u \in \mathbb{Z}$, avec $0 \leq u < \delta$. Si $u \neq 0$, 1 on a :

$$2g + \delta + 1 - u = (q+1)\,\delta + 1\,.$$

Il existe donc m, $q' \in \mathbb{Z}$, avec $0 \leq m \leq \delta - 1$, tels que

$$2g + m = q'\,\delta + 1\,,$$

d'où on conclut que les entiers $2g + m$ et δ sont premiers entre eux. Alors le degré du diviseur $E = (q'k_1 + 1)V_1 + \cdots + q'k_rV_r$ est $2g + m$ et les entiers δ et $2g + m$ sont premiers entre eux. Par conséquent il existe un diviseur $E = \ell_1V_1 + \cdots + \ell_rV_r$ avec $2g + \delta \geq \deg E \geq 2g$, tels que les entiers δ et $\deg E$ soient premiers entre eux et que pour tout i, $\ell_i \geq k_i$. Alors on peut appliquer le lemme 5.6.

Le lemme 5.6 entraîne qu'il existe une fonction $f \in \overline{K}(C)$, avec $(f)_\infty = E$ et $\overline{K}(C) = \overline{K}(f,h)$; la fonction f est définie sur un corps de nombres L avec $K \subseteq L$ et $[\,L : K\,] \leq n^r$; le discriminant D_L de L satisfait l'inégalité suivante :

$$|D_L| < (2M)^{865\,drM^{20+r}} |D_K|^{rM^r} H_K(F)^{48\,rM^{10+r}}\,.$$

Aussi, il existe un polynôme $G(X,Y)$ de $L[\,X\,,\,Y\,]$, absolument irréductible, tel que l'équation $G(f,h) = 0$ soit un modèle de la courbe C, dont le degré total est $\leq 2\delta + 2g - 1$ et dont la hauteur vérifie l'égalité :

$$H_L(G) < \Omega |D_K|^{r\Xi^r\delta^3g^2} H_K(F)^{420\,\Xi^{16+r}\delta^{11}2^{2g+\delta}g^7\Phi_2^2}\,,$$

où

$$\Omega = \Phi_1^{8\delta^{11}g^7\Xi^5\Phi_2^2} (2\Xi)^{1\,200\,d\,\Xi^{21+r}\delta^{15}g^7 2^{2g+\delta}\Phi_2^4}\,.$$

D'après le lemme 5.6. l'équation $G(f,h) = 0$ est une équation de dépendance intégrale de f sur l'anneau $O_L[h]$ et la fonction h est un élément entier sur l'anneau $O_L[X]$. Alors si $x,\ y \in O_K$, avec $F(x,y) = 0$, les éléments $f(x,y)$ et $h(x,y)$ sont des entiers de L avec $G\big(f(x,y)\,,\ h(x,y)\big) = 0$. L'extension $\overline{K}(C)/\overline{K}(h)$ vérifie les hypothèses du théorème 1. Alors, en utilisant la majoration fournie par le théorème 1, on obtient :

$$\max\big\{H_L\big(f(x,y)\big)\,,\ H_L\big(h(x,y)\big)\big\} < \exp\Big\{(2\Xi)^A \Phi_1^B |D_K|^\Gamma H_K(F)^\Delta\Big\}\,,$$

où

$$\begin{aligned}
A &= 2\cdot 10^7 d^2 n^r \Xi^{21+r} \delta^{15} g^7 2^{2g+\delta} (2g+2\delta)^{35} \Phi_2^4\,,\\
B &= 13\cdot 10^4 d n^r \delta^{11} g^7 \Xi^5 (2g+2\delta)^{35} \Phi_2^2\,,\\
\Gamma &= 16\cdot 10^3 r d n^r \Xi^r g^2 \delta^3 (2g+2\delta)^{35}\\
\Delta &= 7\cdot 10^6 d n^r \delta^{11} g^7 \Xi^{16+r} 2^{2g+\delta} (2g+2\delta)^{35} \Phi_2^2\,.
\end{aligned}$$

Enfin, en utilisant le lemme 5.6 (5), on déduit la majoration annoncée.

9. Démonstration des corollaires 1 et 2

Il suffit de démontrer que si l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne, la courbe C possède une des propriétés (i), (ii) du théorème 1. Supposons donc que l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne. Alors la formule du genre de Hurwitz [9, p. 26] donne :

$$2g-2 = -2n + \sum_{a\in\overline{K}\cup\{\infty\}} (n_a - 1)s_a\,,$$

où n_a est l'indice de la ramification au-dessus de $X = a$ et s_a le nombre des anneaux de valuation discrète de $\overline{K}(C)$ qui se trouvent dans Σ_a. Comme le genre de la courbe C est non nul, il en résulte qu'il existe au moins deux nombres algébriques a_1, a_2 tels qu'il y a de ramification au-dessus de $X = a_1,\ a_2$. S'il existe exactement deux places finies $X = a_1,\ a_2 \in \overline{K}$ ramifiées et $n_{a_1} = n_{a_2} = 2$, on a :

$$0 \le 2g-2 = -2n + \frac{n}{2} + \frac{n}{2} + (n_\infty - 1)s_\infty = -s_\infty\,,$$

ce qui est contradictoire. On en conclut que la courbe C possède une des propriétés (i), (ii) du théorème 1.

10. Exemples

Dans cette section nous allons donner des exemples de courbes algébriques qui vérifient les hypothèses du théorème 1.

1) Soient $f(X,Y)$, $g(X,Y) \in K[X,Y]$ et $h(X) \in K[X]$ trois polynômes; on suppose que $f(X,Y)$ et $g(X,Y)$ n'ont pas de zéro commun. Considérons les équations :

$$F_1(X,Y) = f(X,Y)^2 h(X) - (X-a_1)^{s_1}(X-a_2)^{s_2}(X-a_3)^{s_3} g(X,Y) = 0\,, \tag{I}$$

où a_1, a_2, $a_3 \in K$ et sont deux à deux distincts; s_1, s_2, s_3 sont des entiers positifs impairs :

$$F_2(X,Y) = f(X,Y)^{\alpha} h(X) - (X-a_1)^{t_1}(X-a_2)^{t_2} g(X,Y) = 0\,, \tag{II}$$

où a_1, $a_2 \in K$, avec $a_1 \neq a_2$; α, t_1 et t_2 sont des entiers positifs, avec $\alpha \geq 3$ et $(t_i, \alpha) = 1$, $i = 1, 2$. On suppose que les polynômes $F_i(X,Y)$, $i = 1, 2$, sont absolument irréductibles et on note C_i la courbe algébrique définie par l'équation $F_i(X,Y) = 0$, $i = 1, 2$.

Si W est un anneau de valuation discrète de $\overline{K}(C_1)$, dans Σ_{a_i}, on a :

$$2 \operatorname{ord}_W f(X,Y) = s_i \operatorname{ord}_W (X - a_i)$$

(car $h(a_i) \neq 0$ et les polynômes f et g n'ont pas de zéro commun). On en déduit que l'indice de ramification de tout anneau de valuation discrète de $\overline{K}(C_1)$, dans Σ_{a_i}, est divisible par 2, $i = 1, 2, 3$. En procédant de la même façon, on déduit que l'indice de ramification de tout anneau de valuation discrète de $\overline{K}(C_2)$, dans Σ_{a_i}, est divisible par α, $i = 1, 2$.

2) Soient $f(X,Y)$, $g(X,Y)$ deux polynômes de $K[X,Y]$, qui n'ont pas de zéro commun. Soient a, $b \in K$ avec $a \neq b$. Considérons l'équation :

$$G(X,Y) = (X-a) f(X,Y)^m - (X-b) g(X,Y)^n = 0\,,$$

où m, $n \in \mathbb{Z}$ avec $n \geq 3$ et $m \geq 2$. Aussi, on suppose que le polynôme $G(X,Y)$ est absolument irréductible. Notons C la courbe $G(X,Y) = 0$.

Soit W un anneau de valuation discrète de $\overline{K}(C)$, dans Σ_a. Alors on a :

$$\operatorname{ord}_W (X-a) = n \operatorname{ord}_W (g(X,Y))\,.$$

On en déduit que l'indice de ramification de W est divisible par n. De même, il résulte que l'indice de ramification de tout anneau de valuation discrète de $\overline{K}(C)$, dans Σ_b, est divisible par m.

Soient a, b, $c \in K$ deux à deux distincts. Considérons la courbe

$$E(X,Y) = (X-a)f(X,Y)^2 - (X-b)(X-c)g(X,Y)^n = 0\,,$$

où n est un entier positif avec $n \geq 2$. On suppose que le polynôme $E(X,Y)$ est absolument irréductible. Alors on montre comme précédemment que la courbe $E(X,Y) = 0$ vérifie les hypothèses du théorème 1.

3) Soient $C : F(X,Y) = 0$ une courbe algébrique (irréductible) définie sur K. Dans le cas où le degré de $F(X,Y)$ en Y est 3 ou 4, on peut examiner facilement si l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne. En effet, supposons que

$$F(X,Y) = Y^3 + a(X)Y^2 + b(X)Y + c(X)\,.$$

On considère $F(X,Y)$ comme polynôme à coefficients dans $K[X]$ et on note $D(X)$ son discriminant. Alors l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne si et seulement si $D(X)$ est un carré dans $\overline{K}(X)$ [24, théorème 18.2].

Supposons ensuite que

$$F(X,Y) = Y^4 + a(X)Y^3 + b(X)Y^2 + c(X)Y + d(X)\,.$$

Le polynôme

$$\begin{aligned} r(X,Y) = Y^3 - b(X)Y^2 + \big(a(X)c(X) - 4d(X)\big)Y + \\ - \big(a(X)^2 d(X) - 4b(X)\,d(X) + c(X)^2\big) \end{aligned}$$

est la résolvante cubique de $F(X,Y)$ (considéré comme polynôme à coefficients dans $\overline{K}(X)$). Notons E le corps de décomposition de $r(X,Y)$ sur $\overline{K}(X)$. Alors le théorème 1 de [6] entraîne que l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne si et seulement si on a un des cas suivants :

(i) le polynôme $r(X,Y)$ se décompose en facteurs linéaires sur $\overline{K}(X)$,

(ii) le polynôme $r(X,Y)$ possède exactement une racine t dans $\overline{K}(X)$ et le polynôme $g(Y) = \big(Y^2 - tY + d(X)\big)\big(Y^2 + a(X)Y + b(X) - t\big)$ se décompose en facteurs linéaires sur E.

Dans le cas (i) le groupe de Galois de l'extension $\overline{K}(C)/\overline{K}(X)$ est isomorphe au groupe à quatre éléments de Klein V et dans le cas (ii) est isomorphe au groupe cyclique à quatre éléments C_4.

Enfin si $F(X,Y) = Y^4 + b(X)Y^2 + d(X)$, on peut avoir un critère plus simple. Dans ce cas le théorème 3 de [6] entraîne que l'extension $\overline{K}(C)/\overline{K}(X)$ est galoisienne, de groupe de Galois V, si et seulement si $d(X) \in \overline{K}(X)^2$ et de groupe de Galois C_4, si et seulement si $d(X)\big(b(X)^2 - 4d(X)\big) \in \overline{K}(X)^2$.

Remerciements

Je remercie les Professeurs D. Bertrand, P. Dèbes et M. Hindry pour leurs remarques. Je remercie aussi le Professeur J.-P. Serre qui a bien voulu s'intéresser aux résultats de ce travail.

Références

[1] BAKER (A.) et COATES (J.) . — *Integer points on curves of genus 1*, Proc. Cambr. Philos. Soc. **67** (1970), pp. 595-602.

[2] BELOTSERKOVSKI (Y.) . — *Analyse effective d'une nouvelle classe d'équations diophantiennes* (en russe), Vestsi Akad. Navuk B.S.S.R., Ser. Fiz. Math. Navuk **6**, n° 125 (1988), pp. 34-39.

[3] COATES (J.) . — *Construction of rational functions on curves*, Proc. Camb. Phil. Soc. **68** (1970), pp. 105-123.

[4] FULTON (W.) . — *Algebraic curves*, The Benjamin I.N.C. 1969.

[5] HILLIKER (D. L.) et STRAUS (E.) . — *Determination of bounds for the solutions to those binary diophantine equations that satisfy the hypotheses of Runge's Theorem*, Trans. Amer. Math. Soc. **280** (1983), pp. 637-657.

[6] KAPPE (L. C.) et WARREN (B.) . — *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96**, n° 2 (1989), pp. 133-137.

[7] KLEIMAN (H.) . — *On the diophantine equation* $f(x,y) = 0$, J. Reine Angew. Math **286-287** (1975), pp. 124-131.

[8] KUBERT (D.) et LANG (S.) . — *Units in Modular Function Fields*, I, Math. Ann. **218** (1975), pp. 67-96.

[9] LANG (S.) . — *Introduction to algebraic and abelian Functions*, New-York – Berlin – Heidelberg, Springer-Verlag 1982.

[10] LANG (S.) . — *Fundamentals of Diophantine Geometry*, New-York – Berlin – Heidelberg – Tokyo, Springer-Verlag 1983.

[11] POULAKIS (D.) . — *Points entiers sur les courbes hyperelliptiques*, Acta Arithmetica **LXII**, n° 1 (1992), pp. 25-43.

[12] POULAKIS (D.) . — *Solutions entières de l'equation* $f(X,Y)^\alpha = h(X)g(X,Y)$, C.R. Acad. Sci. Paris **315** (1992), pp. 963-968.

[13] POULAKIS (D.) . — *Points entiers sur les courbes de genre* 0, Colloquium Math. **LXVI**, n° 1 (1993), pp. 1-7.

[14] POULAKIS (D.) . — *Points entiers et modèles de courbes algébriques*, Monatshefte für Math. **118** (1994), pp. 111-143.

[15] SCHMIDT (W. M.) . — *Eisenstein Theorem on power series expansions of algebraic functions*, Acta Arithmetica **56** (1990), pp. 161-179.

[16] SCHMIDT (W. M.) . — *Construction and Estimation of Bases in Function Fields*, J. Number. Theory **39** (1991), pp. 181-224.

[17] SCHMIDT (W. M.) . — *Integer points on curves of genus* 1, Compositio Mathematica **81** (1992), pp. 33-59.

[18] SERRE (J.-P.) . — *Corps Locaux*, Hermann, Paris 1962.

[19] SERRE (J.-P.) . — *Lectures on the Mordell–Weil Theorem*, Vieweg 1989.

[20] SERRE (J.-P.) . — *Lettre à D. Bertrand*, du 4 juin 1993.

[21] SHAFAREVICH (I. R.) . — *Basic Algebraic Geometry*, Berlin – Heidelberg – New-York, Springer-Verlag 1977.

[22] SIEGEL (C. L.) . — *Uber einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Weiss **1**, 1929.

[23] SILVERMAN (J. H.) . — *The Arithmetic of elliptic curves*, New-York – Berlin – Heidelberg, Springer-Verlag 1986.

[24] STEWART (I.) . — *Galois Theory*, Chapman and Hall, London – New-York, 1973.

[25] WALKER (R.) . — *Algebraic Curves*, New-York – Berlin – Heidelberg, Springer-verlag 1978.

[26] WALSH (P. G.) . — *A quantitative version of Runge's theorem on diophantine equations*, Acta Arith. **LXII** , n° 2 (1992), pp. 157-172.

[27] ZANNIER (U.) . — *Note on the effective solution of certain diophantine problems (Siegel's Theorem for a Galois cover)*, Prépublication.