ACTA ARITHMETICA
LXII.1 (1992)

Points entiers sur les courbes hyperelliptiques

par

Dimitrios Poulakis (Théssalonique)

1. Introduction. Soient k un corps de nombres et A son anneau des entiers. On notera $\overline{k}$ une clôture algébrique de k. Soit F un polynôme absolument irréductible de $k[X,Y]$ tel que la courbe $F(X,Y)=0$ soit de genre non nul. On sait, d'après Siegel [8], qu'il n'existe qu'un nombre fini de couples $(x,y)\in A\times A$ tels que $F(x,y)=0$. La méthode de Siegel ne permet pas de déterminer de façon effective ces couples.

Dans le cas où $\mathbb{F}\in\mathbb{Z}[X,Y]$ et le genre de la courbe $F(X,Y)=0$ est 1, Baker et Coates [1] ont donné un majorant de la hauteur $\max\{|x|,|y|\}$ des points entiers de la courbe, explicitement calculable en fonction des coefficients de F. Schmidt [4] a récemment amélioré ce résultat de Baker et Coates, et l'a étendu à un corps de nombres k quelconque.

Dans ce travail on s'intéresse aux majorations de la hauteur des points entiers sur des courbes hyperelliptiques. Rappelons qu'une courbe C sur k est dite *hyperelliptique* si son corps de fonctions $\overline{k}(C)$ contient une fonction f de degré 2 ([9]); il en résulte que $\overline{k}(C)$ possède un $\overline{k}(f)$-automorphisme τ tel que $\tau\neq\mathrm{Id}$ et $\tau^2=\mathrm{Id}$. Supposons maintenant que la courbe C définie par $F(X,Y)=0$ soit hyperelliptique de genre $g\geq 2$. Notons Σ l'ensemble des anneaux de valuation discrète de $\overline{k}(C)$ qui contiennent $\overline{k}$ et Σ_∞ l'ensemble des éléments de Σ qui se trouvent au-dessus de l'anneau de valuation discrète de $\overline{k}(X)$ définie par $1/X$.

Considérons l'ensemble $V(\mathbb{Q})$ de valeurs absolues de $\mathbb{Q}$, qui contient la valeur absolue ordinaire et pour tout premier $p\in\mathbb{Z}$ la valeur absolue $|\cdot|_p$ définie par $|p^n a/b|_p=p^{-n}$ pour $a,b\in\mathbb{Z}$ avec $(a,b)=1$. Soit $V(k)=\{|\cdot|_v : v\in M(k)\}$ l'ensemble des valeurs absolues de k qui prolongent les éléments de $V(\mathbb{Q})$. Si $\boldsymbol{x}=(x_0,\dots,x_n)$ est un point de l'espace projectif $\boldsymbol{P}^n(k)$ et $v\in M(k)$, on note $|\boldsymbol{x}|_v=\max\{|x_0|_v,\dots,|x_n|_v\}$. On appelle la quantité

$$H_k(\boldsymbol{x})=\prod_{v\in M(k)}|\boldsymbol{x}|_v^{d_v}$$

où d_v sont les degrés locaux, *hauteur* de $\boldsymbol{x}$ (relativement au corps de

nombres k) et la quantité

$$H(\boldsymbol{x}) = H_k(\boldsymbol{x})^{1/d}$$

où d est le degré de k, *hauteur absolue* de $\boldsymbol{x}$ ([7]). Si $f \in k[X_1, \ldots, X_n]$ on définit $|f|_v$, $H_k(f)$ et $H(f)$ en termes du vecteur des coefficients de f. Aussi quand $a \in k$ on note $H_k(a) = H_k((1, a))$.

Dans [7], chap. 8, J.-P. Serre montre que s'il existe $V \in \Sigma_\infty$ tel que $\tau(V) \in \Sigma_\infty$, le problème de la recherche d'un majorant effectif pour la hauteur des couples $(x, y) \in A \times A$ qui vérifient $F(x, y) = 0$ peut être réduit à l'application de la méthode de Baker. Dans ce travail on calcule un tel majorant. Plus précisément, on montre le résultat suivant :

THÉORÈME. *Soient N le degré total de F et D_k le discriminant de k. On suppose qu'il existe $V \in \Sigma_\infty$ tel que $\tau(V) \in \Sigma_\infty$. Alors si $(x, y) \in A \times A$ vérifie $F(x, y) = 0$ on a*

$$\max\{H_k(x), H_k(y)\} < \exp\{c(d, N) W^{3 \cdot 10^5 N^3 3^{2g} d^2 g^{2g+3}}\}$$

où

$$c(d, N) < (3N)^{d^3 2^{N^2} N^{5N^2}} \qquad et \qquad W = |D_k| H_k(F)^{2 \cdot 10^4 3^g N^{15}} .$$

EXEMPLES. 1. Soit F un polynôme absolument irréductible de $k[X, Y]$ tel que $F = F_{g+2} + F_{g+1} + F_g$ où F_i est un polynôme homogène de degré i et $g \geq 2$. On suppose que la courbe C définie par l'équation $F(X, Y) = 0$ n'a pas d'autres singularités que le point $(0, 0)$ qui est un point multiple ordinaire. Alors on vérifie facilement que C est une courbe hyperelliptique de genre g.

L'automorphisme τ de $\overline{k}(C)$ est donné par l'application

$$X \to -XF_g(X, Y)/(F_{g+1}(X, Y) + F_g(X, Y)) ,$$
$$Y \to -YF_g(X, Y)/(F_{g+1}(X, Y) + F_g(X, Y)) .$$

Si $F_{g+1} = 0$ on a $\tau(V) = V$ pour tout $V \in \Sigma_\infty$; aussi si les polynômes $F_{g+2}(X, 1)$, $F_{g+1}(X, 1)$ ont une racine en commun, il existe $V \in \Sigma_\infty$ tel que $\tau(V) = V$; par conséquent on peut appliquer le théorème. Dans les autres cas la condition du théorème n'est pas satisfaite.

2. Soit C la courbe définie par l'équation

$$Y^{2n+2} = a_0 X^{n+2} + a_1 X^{n+1} Y^2 + \ldots + a_n X^2 Y^{2n}$$

où $n \geq 5$, $a_i \in k$. On suppose que les racines du polynôme $a_0 X^n + a_1 X^{n-1} + \ldots + a_n$ sont deux-à-deux distinctes. L'application $X \to Y/X = W$, $Y \to X/Y^2 = T$ définit une application birationnelle de la courbe C sur la courbe définie par l'équation

$$W^2 = a_0 T^n + a_1 T^{n-1} + \ldots + a_n .$$

Donc C est une courbe hyperelliptique de genre $g = [(n-1)/2] \geq 2$. Les points à l'infini de C sont les points

$$[x,y,z] = \begin{cases} [1,0,0], [1, \pm\sqrt{a_n}, 0] & \text{si } a_n \neq 0, \\ [1,0,0], [1, \pm\sqrt{a_{n-1}}, 0], [1, \pm i\sqrt{a_{n-1}}, 0] & \text{si } a_n = 0 \end{cases}$$

(en coordonnés homogènes). Sauf $[1,0,0]$, ce sont des points non singuliers. Notons τ l'automorphisme de $\overline{k}(C)$ défini par l'application $X \to X$, $Y \to -Y$. Dans le cas où $a_n \neq 0$, notons V_+, V_- les éléments de Σ_∞ qui sont associés aux points $[1, \pm\sqrt{a_n}, 0]$; alors $\tau(V_+) = V_-$. Dans le cas où $a_n = 0$ notons V_+, V_-, V'_+, V'_- les éléments de Σ_∞ qui sont associés aux points $[1, \pm\sqrt{a_n}, 0]$, $[1, \pm i\sqrt{a_n}, 0]$ respectivement. On a $\tau(V_+) = V_-$ et $\tau(V'_+) = V'_-$. Dans tous les cas on peut donc appliquer le théorème.

Nous utilisons les résultats de [5] et [6] et le théorème de Riemann–Roch pour construire une courbe birationnelle à $F(X,Y) = 0$ d'équation $Y_1^2 = G(X_1)$ telle que les coefficients de $G(X_1)$ soient des entiers algébriques d'un corps de nombres fixé K et que les solutions de $F(X,Y) = 0$ en entiers de k soient déterminées par les solutions de $Y_1^2 = G(X_1)$ en entiers de K. Une majoration de la taille des solutions entières de l'équation hyperelliptique ([3], théorème 1) nous permet d'obtenir notre résultat.

2. Lemmes auxiliaires. Soit $u \in \Sigma$. On note $\mathrm{ord}_u(f)$ l'ordre d'une fonction $f \in \overline{k}(C)$ en u.

LEMME 1. *Soit $V \in \Sigma$. Alors*

(i) *si $\tau(V) = V$, il existe $f \in \overline{k}(C)$ tel que $\mathrm{ord}_V(f) = -2$ et $\mathrm{ord}_u(f) \geq 0$ pour tout $u \in \Sigma - \{V\}$,*

(ii) *si $\tau(V) \neq V$, il existe $f \in \overline{k}(C)$ tel que $\mathrm{ord}_V(f) = -1$, $\mathrm{ord}_{\tau(V)}(f) = -1$ et $\mathrm{ord}_u(f) \geq 0$ pour tout $u \in \Sigma - \{V, \tau(V)\}$.*

Démonstration. Soit L le sous-corps de $\overline{k}(C)$ fixé par τ. Alors il existe $h \in \overline{k}(C)$ tel que $L = \overline{k}(h)$. Si $\mathrm{ord}_V(h) \geq 0$ et si t est un paramètre local en V on a $h = a_0 + a_1 t + \ldots$ Donc $h' = h - a_0 \in V$ et h' est un paramètre local en $V \cap L$. De même si $\mathrm{ord}_V(h) < 0$, alors $h' = 1/h$ est un paramètre local en $V \cap L$. Par conséquent, si $\tau(V) = V$ on a $\mathrm{ord}_V(h') = 2$, tandis que si $\tau(V) \neq V$ on a $\mathrm{ord}_V(h') = 1$ et $\mathrm{ord}_{\tau(V)}(h') = 1$. Posons $f = 1/h'$. Comme $[\overline{k}(C) : \overline{k}(f)] = 2$, la fonction f n'a pas d'autres pôles que V et $\tau(V)$.

Soient $u_1, \ldots, u_r \in \Sigma$ et $\mu_1, \ldots, \mu_r \in \mathbb{Z}$; au diviseur $D = \sum_{i=1}^r \mu_i u_i$ est associé le $\overline{k}$-espace linéaire suivant :

$$L(D) = \{h \in \overline{k}(C) \mid \mathrm{ord}_{u_i}(h) \geq -\mu_i,\ i = 1, \ldots, r\,,\ \text{et} \\ \mathrm{ord}_u(h) \geq 0\ \forall u \in \Sigma - \{u_1, \ldots, u_r\}\}\,.$$

On note $l(D)$ sa dimension.

LEMME 2. *Posons $E = 2V$ si $V = \tau(V)$ et $E = V + \tau(V)$ si $V \neq \tau(V)$. Alors $l(\mu E) = \mu + 1$ pour $\mu = 0, 1, \ldots, g-1$.*

Démonstration. D'après le lemme 1 il existe $f \in \overline{k}(C) - \overline{k}$ tel que $f \in L(E)$. Alors les fonctions $1, f, \ldots, f^\mu \in L(\mu E)$, où $\mu \in \mathbb{N}$, $1 \leq \mu \leq g-1$, sont $\overline{k}$-linéairement indépendantes. Il en résulte que $l(\mu E) \geq \mu + 1$. En particulier $l((g-1)E) \geq g$.

D'autre part, le théorème de Riemann–Roch montre que $l((g-1)E+V) = g$. On a donc $l((g-1)E) = g$ et $L((g-1)E) = L((g-1)E + V)$. Cela entraîne que les fonctions $1, f, \ldots, f^{g-1}$ constituent une base de $L((g-1)E)$. Alors les fonctions $1, f, \ldots, f^\mu$ forment une base de $L(\mu E)$, d'où le résultat.

Soient $v \in M(k)$ et x un réel positif. Notons

$$v(x) = \begin{cases} x & \text{si } |\cdot|_v \text{ est archimédienne,} \\ 1 & \text{sinon.} \end{cases}$$

LEMME 3. *Soient $n \in \mathbb{N}$ et $u_{ij} \in k$ $(1 \leq i, j \leq n)$ avec $|u_{ij}|_v \leq A$ pour tout $v \in M(k)$. Si le système*

$$\sum_{j=1}^{n} u_{ij} X_j = 0 \qquad (i = 1, \ldots, n)$$

a une solution non triviale, alors il existe une solution $x_1, \ldots, x_n \in k$ telle que

$$|x_j|_v \leq A^{n-1} v((n-1)!) \qquad (j = 1, \ldots, n)$$

pour tout $v \in M(k)$.

Démonstration. La démonstration est la même que celle du lemme 2 de [2].

DÉFINITIONS. On appelle *k-système* 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* du k-système $\{A_v\}_{v \in M(k)}$ la quantité

$$N_k\{A_v\} = \prod_{v \in M(k)} A_v^{d_v}.$$

LEMME 4. *Soit $F(X, Y) \in k[X, Y]$ de degré n en Y et de degré total N. On suppose que F n'a pas de facteur multiple de degré positif en Y. Soit*

$$Z = a_0 + a_1 X + \ldots$$

une série telle que $F(X, Z) = 0$. Alors

(i) *Le corps $K = k(a_0, a_1, \ldots)$ engendré sur k par les coefficients de Z est un corps de nombres et $[K : k] \leq n$.*

(ii) *$K = k(a_0, a_1, \ldots, a_{2n^2})$.*

(iii) *Il existe un k-système* $\{A_v\}_{v\in M(k)}$ *tel que*

$$|a_s|_v \le A_v^{N+s} \qquad (s=0,1,2,\ldots)$$

pour tout $v\in M(k)$ *et chaque extension de* $|\cdot|_v$ *sur* K. *On a aussi*

$$N_k\{A_v\} < (2^{14}N^6)^{8N^3d}H_k(F)^{8n^2N}\,.$$

(iv) *Si* D_K *est le discriminant de* K *on a*

$$|D_K| < N^{Nd}(2^{14}N^6)^{48dN^7}|D_k|^nH_k(F)^{48n^5N^2}\,.$$

Pour une démonstration de ce résultat on peut consulter [4], §5.

3. Construction d'une équation hyperelliptique. Soient N le degré total de $F(X,Y)$ et n le degré de $F(X,Y)$ en Y. On suppose que X est une variable et Φ une fonction algébrique telle que $F(X,\Phi)=0$.

Soient $V\in\Sigma_\infty$ tel que $\tau(V)\in\Sigma_\infty$, e l'indice de ramification de V et $X_V=(1/X)^{1/e}$. Alors

$$\Phi=\sum_{s=s_0}^{\infty}a_sX_V^s\,.$$

La fonction Φ a un pôle d'ordre $\le Ne$ en V; on a donc $s_0\ge -Ne$. En ajoutant des coefficients nuls on peut poser $s_0=-Ne$.

Posons

$$\overline{\Phi}=X_V^{Ne}\Phi=a_{s_0}+a_{s_0+1}X_V+\ldots$$

Il en résulte

$$X_V^{Nen}F(X_V^{-e},X_V^{-Ne}\overline{\Phi})=0\,.$$

Le polynôme $F'(U,W)=U^{Ne(n+1)}F(U^{-e},U^{-Ne}W)$ est sans facteur multiple et de degré positif en W. Son degré en W est n et son degré total est $\le nN^2$. Alors, d'après le lemme 4, on voit que le corps engendré par les a_i, $K=k(a_{s_0},a_{s_0+1},\ldots)$, est un corps de nombres, de degré $[K:k]\le n$ et de discriminant majoré par

$$|D_K| < (2N)^{865dN^{21}}|D_k|^nH_k(F)^{48N^{11}}\,. \tag{3.1}$$

Supposons d'abord que $\tau(V)=V$. D'après le théorème de Riemann–Roch, l'espace $L((2g+1)V)$ est de dimension $g+2$. Le théorème A2 de [6] entraîne qu'il existe des entiers $\pi_1,\ldots,\pi_t\ge 0$ tels qu'une base de $L((2g+1)V)$ soit de la forme

$$X^hg_i \qquad (1\le i\le t,\ 0\le h\le\pi_i)\,.$$

Comme le diviseur $(2g+1)V$ est rationnel sur K, on déduit du théorème B2 de [6] que $g_1,\ldots,g_t\in K(X,\Phi)$. D'après le théorème C2 de [6] le

développement de g_i en V est

$$g_i = \sum_{s=-(2g+1)}^{\infty} a_{is} X_V^s$$

avec $a_{is} \in K$; de plus il existe des K-systèmes $\{A_v(V)\}$ et $\{B_v(i)\}$, définis pour tout $v \in M(K)$, tels que

$$|a_{is}|_v \le A_v(V)^{s+4N^3} B_v(i)$$

et

$$N_K\{A_v(V)\} < (2^7 N^5 H(F))^{9N^5 \deg K}\,, \tag{3.2}$$

$$N_K\{B_v(i)\} < (9N^4 H(F))^{365N^{11} \deg K}\,. \tag{3.3}$$

Notons $f_1, \dots, f_{g+2}$ la base de l'espace $L((2g+1)V)$ et écrivons

$$f_i = \sum_{s=-(2g+1)}^{\infty} b_{is} X_V^s \quad (i = 1, \dots, g+2)\,.$$

On a $b_{is} = a_{i,s+ke}$, où $k \le g+1$. Alors

$$|b_{is}|_v \le A_v(V)^{s+4N^3+(g+1)n} B_v \quad (i = 1, \dots, g+2)$$

où B_v est le produit des $B_v(i)$.

D'après le théorème de Riemann–Roch on a $l(2gV) = g+1$. Donc il existe i tel que $b_{i,-2g-1} \neq 0$. Soit $b_{1,-2g-1} \neq 0$; alors $\mathrm{ord}_V(f_1) = -2g-1$ et $\mathrm{ord}_u(f_1) \ge 0$ pour tout $u \in \Sigma - \{V\}$.

Considérons les fonctions

$$w_1 = b_{1,-2g-1} f_2 - b_{2,-2g-1} f_1,\ \dots,\ w_{g+1} = b_{1,-2g-1} f_{g+1} - b_{g+1,-2g-1} f_1\,.$$

Il est facile de vérifier que $w_1, \dots, w_{g+1}$ constituent une base de l'espace $L(2gV)$. Soient

$$w_i = \sum_{s=-2g}^{\infty} w_{is} X_V^s \quad (i = 1, \dots, g+1)\,.$$

Alors

$$|w_{is}|_v \le A_v(V)^{s+8N^3+2(g+1)n} B_v^2 v(2)\,.$$

Comme $l((2g-1)V) = g$, en utilisant le même procédé on obtient une base $\{t_1, \dots, t_g\}$ de l'espace $L((2g-1)V)$. Le développement de t_i en V est

$$t_i = \sum_{s=-2g+1}^{\infty} t_{is} X_V^s \quad (i = 1, \dots, g)$$

avec

$$|t_{is}|_v \le A_v(V)^{s+16N^3+4(g+1)n} B_v^4 v(4)\,.$$

Le lemme 2 entraîne

$$\begin{aligned}\overline{k} &= L(V) \subsetneq L(2V) = L(3V) \subsetneq \ldots \subsetneq L(2kV)\\ &= L((2k+1)V) \subsetneq \ldots \subsetneq L((2g-2)V) = L((2g-1)V)\,.\end{aligned}$$

Par suite, en utilisant successivement la méthode précédente on obtient une base $\{h_1, h_2\}$ de $L(2V)$. Le développement de h_i en V est

$$h_i = \sum_{s=-2}^{\infty} h_{is} X_V^s \qquad (i = 1, 2)$$

avec

$$|h_{is}|_v \le A_v(V)^{s+2^g(g+1)n+2^{g+2}N^3} B_v^{2^g}\, v(2^g)\,.$$

Sans restreindre la généralité on peut supposer que $h_{1,-2} \neq 0$; donc $\mathrm{ord}_V(h_1) = -2$ et $\mathrm{ord}_u(h_1) \ge 0$ pour tout $u \in \Sigma - \{V\}$.

Les fonctions

$$\begin{gathered}l_0 = 1, \quad l_1 = h_1, \quad l_2 = h_1^2, \quad \ldots, \quad l_{2g+1} = h_1^{2g+1},\\ l_{2g+2} = f_1\,, \quad l_{2g+3} = f_1^2\,, \quad l_{2g+4} = f_1 h_1\,, \quad \ldots, \quad l_{3g+3} = f_1 h_1^g\end{gathered}$$

sont des éléments de l'espace $L((4g+2)V)$ qui est de dimension $3g+3$. Donc elles sont $\overline{K}$-linéairement dépendantes.

Le développement de l_i en V est

$$l_i = \sum_{s=-4g-2}^{\infty} l_{is} X_V^s \qquad (i = 0, \ldots, 3g+3)\,.$$

Comme $(N-1)(N-2) \ge 2g$ il en résulte que $N^3 \ge 2(g+1)n$; donc

$$2^g(g+1)n + 2^{g+2}N^3 \le 9 \cdot 2^{g-1}N^3\,.$$

On obtient facilement

$$|l_{is}|_v \le A_v(V)^{s+9(2g+1)2^{g-1}N^3} B_v^{2^g(2g+1)} v(2^{g(2g+1)}(s+4g+3)^{2g})\,.$$

La dépendance linéaire des fonctions l_i $(i = 1, \ldots, 3g+4)$ entraîne que le système

$$\sum_{j=0}^{3g+3} x_j l_{jk} = 0 \qquad (-4g+2 \le k \le 0)$$

a une solution non triviale dans K. Il résulte alors du lemme 3 qu'il existe une solution du système non triviale $x_0, \ldots, x_{3g+3} \in K$ telle que

$$\begin{aligned}|x_j|_v \le A_v(V)^{27(g+1)(2g+1)2^{g-1}N^3} &B_v^{3(g+1)(2g+1)2^g}\\ &\times v(2^{3g(2g+1)(g+1)}(4g+3)^{6g(g+1)}(3g+3)!)\,.\end{aligned}$$

La fonction $\sum_{j=0}^{3g+3} x_j l_j$ n'a pas de pôles et s'annule en V; donc

$$\sum_{j=0}^{3g+3} x_j l_j = 0\,. \tag{3.4}$$

Si $x_{2g+3} = 0$, les fonctions

$$x_0 + x_1 h_1 + \ldots + x_{2g+1} h_1^{2g+1} \quad \text{et} \quad x_{2g+2} f_1 + x_{2g+4} f_1 h_1 + \ldots + x_{3g+3} f_1 h_1^g\,,$$

si elles ne sont pas nulles, ont pour valuation en V, $4g+2$ et $4g+1$ respectivement; c'est impossible. Donc $x_{2g+3} \neq 0$.

Posons

$$X' = h_1, \quad \Phi' = 2x_{2g+3} f_1 + x_{2g+2} + \sum_{j=1}^{g} x_{2g+3+j} h_1^j\,.$$

Il résulte de (3.4) que

$$\begin{aligned}\Phi'^2 = {} & x_{2g+2}^2 - 4x_{2g+3} \sum_{j=0}^{g} x_j X'^j + \sum_{j=1}^{g} x_{2g+3+j}^2 X'^{2j} \\ & + 2x_{2g+2} \sum_{j=1}^{g} x_{2g+3+j} X'^j + 2x_{2g+4} \sum_{j=2}^{g} x_{2g+3+j} X'^{j+1} \\ & + 2x_{2g+5} \sum_{j=3}^{g} x_{2g+3+j} X'^{j+2} + \ldots + 2x_{3g+2} x_{3g+3} X'^{2g-1}\,.\end{aligned}$$

Alors on a

$$\Phi'^2 = a'_{2g+1} X'^{2g+1} + a'_{2g} X'^{2g} + \ldots + a'_0$$

où

$$a'_0 = x_{2g+2}^2 - 4x_{2g+3} x_0\,,$$

$$a'_{2\lambda+1} = -4x_{2g+3} x_{2\lambda-1} + 2x_{2g+2} x_{2g+2\lambda+2} + 2 \sum_{j=\lambda}^{\mu} x_{2g+3+j} x_{2g+2\lambda+2-j}$$

avec $\mu = 2\lambda - 2$ si $2\lambda - 1 \leq g$ et $\mu = g$ si $2\lambda - 1 > g$, et

$$\begin{aligned}a'_{2\lambda} = {} & -4x_{2g+3} x_{2\lambda} + x_{2g+3+\lambda}^2 + 2x_{2g+2} x_{2g+3+2\lambda} \\ & + 2 \sum_{j=\lambda+1}^{\mu} x_{2g+3+j} x_{2g+3+2\lambda-j}\end{aligned}$$

avec $\mu = 2\lambda - 1$ si $2\lambda \leq g$ et $\mu = g$ si $2\lambda > g$ ($\lambda = 1, \ldots, g+1$).

Supposons que le polynôme

$$E(X') = a'_{2g+1} X'^{2g+1} + a'_{2g} X'^{2g} + \ldots + a'_0$$

ait une racine multiple; alors si $\varrho_1 = \varrho_2, \dots, \varrho_{2g+1}$ sont ses racines on a

$$(\Phi/(X' - \varrho_1))^2 = a'_{2g+1}(X' - \varrho_3) \dots (X' - \varrho_{2g+1}) .$$

Les fonctions $X' - \varrho_i$ $(i = 3, \dots, 2g+1)$ ont un seul pôle en V; il en résulte que $\Phi'/(X' - \varrho_1)$ possède un seul pôle en V. De plus $\operatorname{ord}_V(\Phi'/(X' - \varrho_1)) = -2g + 1$. D'après la démonstration du lemme 2 on a

$$L((2g-1)V) = L((2g-2)V) .$$

Comme $\Phi'/(X' - \varrho_1) \in L((2g-1)V)$ et $\Phi'/(X' - \varrho_1) \notin L((2g-2)V)$ on obtient une contradiction. Donc les racines de $E(X')$ sont deux-à-deux distinctes.

Les coefficients de $E(X')$: $a'_0, a'_1, \dots, a'_{2g+1}$ sont des éléments de K; on a aussi

$$|a'_0|_v, \dots, |a'_{2g+1}|_v \le A_v(V)^{54(g+1)(2g+1)2^{g-1}N^3} B_v^{6(g+1)2^g(2g+1)} v(2^{7(2g+1)^3}) .$$

Supposons maintenant que $\tau(V) \neq V$. Posons $V_1 = V$ et $V_2 = \tau(V)$. Soit e_i l'indice de ramification de V_i; notons $X_{V_i} = (1/X)^{1/e_i}$ $(i = 1, 2)$. On vérifie, sans peine, que le diviseur $(g+1)V_1 + (g+1)V_2$ est rationnel sur K. Il résulte comme précédemment qu'il existe des fonctions $f_1, \dots, f_{g+3} \in K(X, \Phi)$ qui constituent une base de l'espace $L((g+1)V_1 + (g+1)V_2)$. Le développement de f_i en V_j est

$$f_i = \sum_{s=-g-1}^{\infty} b_{isj} X_{V_j}^s \qquad (i = 1, \dots, s,\ j = 1, 2) .$$

Il y a des K-systèmes $\{A_v(V_j)\}$ et $\{B_v(i)\}$ $(j = 1, 2,\ i = 1, \dots, g+3)$ tels que

$$|b_{isj}|_v \le A_v(V_j)^{s+4N^3+(g+1)n} B_v$$

où B_v est le produit des $B_v(i)$, et

$$N_K\{A_v(V_j)\} < (2^7 N^5 H(F))^{9N^5 \deg K} , \tag{3.5}$$

$$N_K\{B_v(i)\} < (9N^4 H(F))^{365N^{11} \deg K} . \tag{3.6}$$

D'après le théorème de Riemann–Roch on a

$$l(gV_1 + (g+1)V_2) = l((g+1)V_1 + gV_2) = g + 2 .$$

Donc il existe i_1, i_2 tels que $b_{i_1,-g-1,1} \neq 0$ et $b_{i_2,-g-1,2} \neq 0$. Soit $b_{i_1,-g-1,2} = b_{i_2,-g-1,1} = 0$. Alors on a

$$\operatorname{ord}_{V_1}(f_{i_1} + f_{i_2}) = -(g+1) \quad \text{et} \quad \operatorname{ord}_{V_2}(f_{i_1} + f_{i_2}) = -(g+1) .$$

On remplace ensuite dans la base l'élément f_{i_1} par $f_{i_1} + f_{i_2}$. Alors quitte à multiplier le majorant de $|b_{isj}|_v$ par $v(2)$ on peut supposer, sans restreindre la généralité, que $b_{1,-g-1,1} \neq 0$ et $b_{1,-g-1,2} \neq 0$. Donc $\operatorname{ord}_{V_1}(f_1) = \operatorname{ord}_{V_2}(f_1) = -g - 1$ et $\operatorname{ord}_u(f_1) \ge 0$ pour tout $u \in \Sigma - \{V_1, V_2\}$.

Procédant comme dans le cas précédent et compte tenu du fait que le lemme 2 implique

$$\overline{k} = L(V_1) = L(V_2) \subsetneq L(V_1+V_2) = L(2V_1+V_2) = L(V_1+2V_2) \subsetneq \dots$$
$$\dots \subsetneq L((g-1)V_1+(g-1)V_2) = L(gV_1+(g-1)V_2) = L((g-1)V_1+gV_2)$$

on obtient une base $\{h_1, h_2\}$ de $L(V_1+V_2)$ telle que le développement de h_i en V_j soit

$$h_i = \sum_{s=-1}^{\infty} h_{isj} X_{V_j}^s$$

avec

$$|h_{isj}|_\upsilon \le A_\upsilon^{s+2^{g+1}(g+1)n+2^{g+3}N^3} B_\upsilon^{2^{g+1}} \upsilon(2^{g+2})$$

où $A_\upsilon = \max\{A_\upsilon(V_1), A_\upsilon(V_2)\}$. On peut prendre $h_{1,-1,1} \neq 0$ et $h_{1,-1,2} \neq 0$. Donc $\mathrm{ord}_{V_1}(h_1) = \mathrm{ord}_{V_2}(h_1) = -1$ et $\mathrm{ord}_u(f_1) \ge 0$ pour tout $u \in \Sigma - \{V_1, V_2\}$.

On considère les fonctions

$$l_0 = 1, \quad l_1 = h_1, \quad \dots, \quad l_{2g+2} = h_1^{2g+2}, \quad l_{2g+3} = f_1, \quad l_{2g+4} = f_1^2,$$
$$l_{2g+5} = f_1 h_1, \quad \dots, \quad l_{3g+5} = f_1 h_1^{g+1}\,.$$

Le développement de l_i en V_j est

$$l_i = \sum_{s=-2g+2}^{\infty} l_{isj} X_{V_j}^s \qquad (i = 1, \dots, 3g+5,\ j = 1, 2)$$

et on a

$$|l_{isj}| \le A_\upsilon(V_j)^{s+18(g+1)2^g N^3} B_\upsilon^{2^{g+2}(g+1)} \upsilon(4^{(g+2)^2}(s+2g+2)^{2g+1})\,.$$

Les fonctions l_i appartiennent à l'espace $L((2g+2)V_1 + (2g+2)V_2)$ dont la dimension est $l((2g+2)V_1 + (2g+2)V_2) = 3g+5$. Donc ces fonctions l_i $(i = 0, 1, \dots, 3g+5)$ sont $\overline{k}$-linéairement dépendantes. Par conséquent le système

$$\sum_{i=0}^{3g+5} x_i l_{is1} = 0\,, \qquad \sum_{i=0}^{3g+5} x_i l_{is2} = 0 \qquad (s = -2g-2, \dots, 0)$$

possède une solution non triviale dans K. Alors le lemme 3 implique qu'il existe une solution du système non triviale $x_0, x_1, \dots, x_{3g+5} \in K$ telle que

$$|x_j|_\upsilon \le A_\upsilon^{18(3g+4)(g+1)2^g N^3} B_\upsilon^{2^{g+2}(g+1)(3g+4)}$$
$$\times \upsilon(4^{(g+2)^2(3g+4)}(2g+2)^{(2g+1)(3g+4)}(3g+4)!)\,.$$

Il en résulte que $\sum_{i=0}^{3g+5} x_i l_i = 0$ avec $x_{2g+4} \neq 0$.

On pose

$$X' = h_1, \quad \Phi' = 2x_{2g+4}f_1 + x_{2g+3} + \sum_{j=1}^{g+1} x_{2g+4+j}h_1^j$$

et on obtient l'équation

$$\Phi'^2 = a'_{2g+2}X'^{2g+2} + a'_{2g+1}X'^{2g+1} + \ldots + a'_0$$

où

$$a'_0 = x_{2g+3}^2 - 4x_{2g+4}x_0\,,$$

$$a'_{2\lambda-1} = -4x_{2g+4}x_{2\lambda-1} + 2x_{2g+3}x_{2g+3+2\lambda} + 2\sum_{j=\lambda}^{\mu} x_{2g+4+j}x_{2g+4+2\lambda-j}$$

avec $\mu = 2\lambda - 2$ si $2\lambda - 1 < g+1$ et $\mu = g+1$ si $2\lambda - 1 > g+1$, et

$$a'_{2\lambda} = -4_{2g+4}x_{2\lambda} + x_{2g+4+\lambda}^2 + 2x_{2g+3}x_{2g+4+2\lambda} + 2\sum_{j=\lambda+1}^{\mu} x_{2g+4+j}x_{2g+4+2\lambda-j}$$

avec $\mu = 2\lambda - 1$ si $2\lambda \le g+1$ et $\mu = g+1$ si $2\lambda > g+1$ $(\lambda = 1, \ldots, g+1)$.

Supposons que le polynôme

$$E(X') = a'_{2g+2}X'^{2g+2} + a'_{2g+1}X'^{2g+1} + \ldots + a'_0$$

ait une racine multiple; alors si $\varrho_1 = \varrho_2$, $\varrho_3, \ldots, \varrho_{2g+2}$ sont ses racines on a

$$(\Phi'/(X' - \varrho_1))^2 = a'_{2g+2}(X' - \varrho_3)\ldots(X' - \varrho_{2g+2})\,.$$

Il en résulte que les seuls pôles de $\Phi'/(X' - \varrho_1)$ se trouvent en V_1 et V_2 et on a

$$\mathrm{ord}_{V_j}(\Phi'/(X' - \varrho_1)) = -g \quad (j = 1, 2)\,.$$

Comme $\mathrm{ord}_{V_j}(X' - \varrho_1) = -1$ $(j = 1, 2)$, $\mathrm{ord}_u(X' - \varrho_1) \ge 0$ pour tout $u \in \Sigma - \{V_1, V_2\}$ et $l(gV_1 + gV_2) = g + 1$ on en déduit que les fonctions

$$1, X' - \varrho_1, \ \ldots, \ (X' - \varrho_1)^g$$

constituent une base de l'espace $L(gV_1 + gV_2)$. Par conséquent il existe $c_0, c_1, \ldots, c_g \in \overline{k}$ tels que

$$\Phi'/(X' - \varrho_1) = c_0 + c_1(X' - \varrho_1) + \ldots + c_g(X' - \varrho_1)^g\,. \tag{3.7}$$

D'autre part, soit M le sous-espace de $L((g+1)V_1 + (g+1)V_2)$ engendré par $1, h_1, \ldots, h_1^{g+1}$. Comme $l((g+1)V_1 + (g+1)V_2) = g + 3$ il existe i tel que $f_i \notin M$. Si $i \ne 1$ on a

$$f_1 + f_i \in L((g+1)V_1 + (g+1)V_2)$$

et

$$\mathrm{ord}_{V_j}(f_1 + f_i) = -(g+1) \quad (j = 1, 2)\,,$$
$$\mathrm{ord}_u(f_1 + f_i) \ge 0 \quad \text{pour tout } u \in \Sigma - \{V_1, V_2\}\,.$$

On peut donc supposer, sans restreindre la généralité, que f_1 n'est pas une combinaison linéaire de $1, h_1, \dots, h_1^{g+1}$. La relation (3.7) entraîne que f_1 est une combinaison linéaire des $1, h_1, \dots, h_1^{g+1}$, ce qui est contradictoire. Donc les racines de $G(X')$ sont toutes simples.

Les coefficients $a'_0, a'_1, \dots, a'_{2g+2}$ de $E(X')$ sont des éléments de K; on a

$$|a'_0|_v, \dots, |a'_{2g+2}|_v \le A_v^{36(3g+4)(g+1)2^g N^3} B_v^{2^{g+3}(g+1)(3g+4)} v(2^{7(2g+1)^3}) .$$

Soit $V_1 = V_2$. Alors le degré de la fonction f_1 est $2g+1$ et le degré de h_1 est 2. Donc $[K(C) : K(f_1)] = 2g+1$ et $[K(C) : K(h_1)] = 2$. On en déduit que $K(C) = K(h_1, f_1) = K(X', \Phi')$.

Soit $V_1 \ne V_2$. Si $f_1 \in K(h_1)$ il existe $G(T), H(T) \in K[T]$ avec $\operatorname{pgcd}(G, H) = 1$ tels que $f_1 = G(h_1)/H(h_1)$.

Comme

$$[K(C) : K(f_1)] = [K(C) : K(h_1)][K(h_1) : K(f_1)]$$

on en déduit que $[K(h_1) : K(f_1)] = g+1$. Le polynôme irréductible de h_1 sur $K(f_1)$ est $G(T) - f_1 H(T)$. Donc $\max\{\deg G, \deg H\} = g+1$. D'autre part, on a

$$-(g+1) = \operatorname{ord}_{V_j}(f_1) = \operatorname{ord}_{V_1}(G(h_1)/H(h_1)) = -\deg G + \deg H .$$

Alors $\deg H = 0$. Il en résulte que f_1 est une combinaison linéaire de $1, h_1, \dots, h_1^{g+1}$, ce qui n'est pas le cas. Donc $f_1 \notin K(h_1)$ et on a $K(C) = K(f_1, h_1) = K(X', \Phi')$. Par conséquent les courbes $F(X, \Phi) = 0$ et $\Phi'^2 = F(X')$ sont birationnelles sur K.

4. Une équation satisfaite par X' sur $K[X]$. Soient $u_1, \dots, u_r$ les éléments de Σ_∞ et $e_1, \dots, e_r$ ses indices de ramification. Soient $X_{u_i} = (1/X)^{1/e_i}$ et U_i le groupe des e_i-ièmes racines de 1. Notons

$$\vartheta_{u_i\zeta} = \sum_{s=t_0(u_i)}^{\infty} \gamma_s(u_i) \zeta^s X_{u_i}^s , \tag{4.1}$$

où $\zeta \in U_i$, le développement de Puiseux de X' dans le corps des séries formelles $K((X_{u_i}\zeta))$. Alors X' est racine du polynôme

$$P(X, T) = \prod_{\substack{u_i \in \Sigma_\infty \\ \zeta \in U_i}} (T - \vartheta_{u_i\zeta}) = T^n + p_1 T^{n-1} + \dots + p_n$$

où p_i sont les polynômes élémentaires symétriques en $\vartheta_{u_i\zeta}$ à signe près. Alors $p_i \in K(X)$. Comme les pôles de X' se trouvent à l'infini on déduit que $p_i \in K[X]$.

Si $V = \tau(V)$, le seul pôle de la fonction X' se trouve en V et il est d'ordre 2; alors on a $t_0(V) = -2$ et $t_0(u) = 0$ pour $u \ne V$. Si $V \ne \tau(V)$, les seuls pôles de X' se trouvent en V et $\tau(V)$ et ils sont d'ordre 1; on a donc

$t_0(V) = -1$, $t_0(\tau(V)) = -1$ et $t_0(u) = 0$ pour $u \neq V, \tau(V)$. Par conséquent chaque p_i contient seulement des puissances de $(1/X)^\mu$ avec $\mu \geq -2$. Donc p_i est un polynôme quadratique en X. Soit

$$p_i = \sum_{s=0}^{2} \pi_{is} X^s = \sum_{s=-2}^{0} \pi_{i,-s} (1/X)^s \,.$$

On a

$$\pi_{i,-s} = (-1)^i \sum_{\substack{u_1,\zeta_1,s_1,\ldots,u_i,\zeta_i,s_i \\ s_1/e_1+\ldots+s_i/e_i=s}} \cdots \sum \gamma_{s_1}(u_1)\zeta_1^{s_1} \ldots \gamma_{s_i}(u_i)\zeta_i^{s_i} \tag{4.2}$$

où $u_1, \ldots, u_i \in \Sigma_\infty$, $\zeta_j \in U_j$ et les paires u_j, ζ_j sont deux-à-deux distinctes.

Soit $u \in \Sigma_\infty$. Etudions d'abord le cas où $\tau(V) = V$. Considérons la base $\{f_1, \ldots, f_{g+2}\}$ de l'espace $L((2g+1)V)$. Le théorème C.2 de [6] entraîne que le développement de Puiseux de f_i en u est

$$f_i = \sum_{s=-(2g+1)}^{\infty} b_{is}(u) X_u^s$$

où $b_{is}(u)$ sont des éléments d'un corps de nombres $K(u) \supseteq K$; il existe des K-systèmes $\{A_\upsilon(u)\}$ et $\{B_\upsilon(i)\}$ tels que

$$|b_{is}(u)|_\upsilon \leq A_\upsilon(u)^{s+4N^3+(g+1)n} B_\upsilon \qquad (i = 1, \ldots, g+2) \tag{4.3}$$

où B_υ est le produit des $B_\upsilon(i)$; on a aussi des relations analogues à (3.2), (3.3) le développement de Puiseux de h_i en u est

$$h_i = \sum_{s=-2}^{\infty} h_{is}(u) X_u^s$$

où $h_{is}(u) \in K(u)$ et on a

$$|h_{is}(u)|_\upsilon \leq A_\upsilon(u)^{s+2^{g-1}(g+1)n+2^{g+1}N^3} A_\upsilon(V)^{2^{g-1}(g+1)n+2^{g+1}N^3} B_\upsilon^{2^g} \upsilon(2^g) \,.$$

Comme $X' = h_2$ pour tout $\upsilon \in M(K)$ et tout prolongement de $|\cdot|_\upsilon$ à $K(u)$ on a

$$|\gamma_s(u)|_\upsilon \leq A_\upsilon(u)^{s+2^{g-2}9N^3} C_\upsilon$$

où

$$C_\upsilon = A_\upsilon(V)^{2^{g-2}9N^3} B_\upsilon^{2^g} \upsilon(2^g) \,.$$

Soit L un corps de nombres tel que $K(u_i) \subseteq L$ et $U_i \subseteq L$ $(i = 1, \ldots, r)$. Alors pour tout $\upsilon \in M(L)$ la valeur absolue de chacun des termes de la somme (4.2) est majorée par

$$A_\upsilon(u_1)^{s_1+2^{g-2}9N^3} \ldots A_\upsilon(u_i)^{s_i+2^{g-2}9N^3} C_\upsilon^i \,.$$

On a $s_j \geq -2$ si $u_j = V$ et $s_j \geq 0$ si $u_j \neq V$. Il en résulte que chaque partie de la somme $s_1/e_1 + \ldots + s_i/e_i$ est ≥ -2; alors $s_j \leq 2e_j \leq 2n$. Donc

la valeur absolue de chacun des termes de la somme (4.2) est majorée par $C_v^n D_v$ où

$$D_v = \prod_{j=1}^{r} A_v(u_j)^{2^{g-2}10N^3 e_j}\,.$$

Cela entraîne

$$|\pi_{is}|_v \le C_v^n D_v v((5n^2)^n)\,. \tag{4.4}$$

Considérons maintenant le cas où $\tau(V) \neq V$. Soit $\{f_1, \dots, f_{g+3}\}$ la base de l'espace $L((g+1)V + (g+1)\tau(V))$. Le développement de Puiseux de f_i en u est

$$f_i = \sum_{s=-g-1}^{\infty} b_{is}(u) X_u^s$$

où $b_{is}(u)$ sont des éléments d'un corps de nombres $K(u) \supseteq K$. Il existe un K-système $\{A_v(u)\}$ vérifiant des relations analogues à (4.3) et (3.5). Le développement de Puiseux de h_i en u est

$$h_i = \sum_{s=-1}^{\infty} h_{is}(u) X_u^s$$

où $h_{is}(u) \in K(u)$ et on a

$$|h_{is}(u)|_v \le A_v(u)^{s+2^g(g+1)n+2^{g+2}N^3} A_v^{2^g(g+1)n+2^{g+2}N^3} B_v^{2^{g+1}} v(2^{g+1})\,.$$

On procède comme dans le cas où $\tau(V) = V$ et on obtient

$$|\pi_{is}|_v \le C_v^n D_v v((4n^2)^n) \tag{4.5}$$

où

$$C_v = A_v^{2^{g-1}9N^3} B_v^{2^{g+1}} v(2^{g+1}) \quad \text{et} \quad D_v = \prod_{j=1}^{r} A_v(u_j)^{2^{g-1}10N^3 e_j}\,.$$

5. L'équation canonique. Supposons d'abord $\tau(V) = V$. Considérons la quantité

$$W_v = A_v(V)^{2^{g-2}9N^4+54(g+1)(2g+1)2^{g-1}N^3} B_v^{2^g N+6(g+1)(2g+1)2^g} \times \prod_{j=1}^{r} A_v(u_j)^{2^{g-2}10N^3 e_j} v(2^{7(2g+1)^3}(2^g 5n^2)^n)\,.$$

Alors $\{W_v\}$ est un K-système.

Soient $M_\infty(K)$ et $M_0(K)$ les ensembles des indices des valeurs absolues archimédiennes et non archimédiennes respectivement. Notons

$$N_{Kj}\{W_v\} = \prod_{v \in M_j(K)} W_v^{\delta_v}\,, \quad j = 0, \infty\,,$$

où δ_v est le degré local de v. Le lemme 4 de [4] entraîne qu'il existe un entier algébrique $\alpha \in K$, $\alpha \neq 0$, tel que

$$|\alpha|_v \leq W_v^{-1} \quad \text{pour tout } v \in M_0(K) \tag{5.1}$$

et

$$|\alpha|_v \leq (|D_K|^{1/2} N_{K0}\{W_v\})^{1/\deg K} \quad \text{pour tout } v \in M_\infty(K)\,. \tag{5.2}$$

Posons

$$X_1 = \alpha^2 a'_{2g+1} X'\,, \quad \Phi_1 = \alpha^{2g+1} a'^g_{2g+1} \Phi'\,.$$

Alors on a

$$\Phi_1^2 = X_1^{2g+1} + a_1 X_1^{2g} + \ldots + a_{2g+1}$$

où

$$a_i = \alpha^{2i} a'_{2g+1-i} a'^{i-1}_{2g+1} \quad (i = 1, \ldots, 2g+1)\,.$$

Comme

$$|a_i|_v = |\alpha^{2i}|_v |a'_{2g+1-i}|_v |a'^{i-1}_{2g+1}|_v \leq (W_v^{-1})^i < 1$$

pour tout $v \in M_0(K)$ il en résulte que les a_i $(i = 1, \ldots, 2g+1)$ sont des entiers algébriques de K.

Considérons le polynôme $Q(T) = \alpha^n P(T/\alpha)$. Alors $Q(\alpha X') = 0$. Les coefficients de $Q(T)$ sont des polynômes quadratiques

$$q_i(X) = \alpha^i \pi_{i0} + \alpha^i \pi_{i1} X + \alpha^i \pi_{i2} X^2\,.$$

Alors $|\alpha^i \pi_{is}|_v \leq 1$, pour tout $v \in M_0(K)$. Par conséquent $\alpha^i \pi_{is} \in O_K$, où O_K est l'anneau des entiers de K. Il en résulte que $\alpha X'$ est un élément entier sur $O_K[X]$. Comme $\alpha a'_{2g+1}$ est un entier de K, X_1 est entier sur $O_K[X]$. Par conséquent si X, Φ sont des entiers de k, alors X_1, Φ_1 sont des entiers de K.

Notons $f(X_1) = X_1^{2g+1} + a_1 X_1^{2g} + \ldots + a_{2g+1}$. Alors

$$|f|_v \leq W_v^{2g+1} (|D_K|^{1/2} N_{K0}\{W_v\})^{4g+2/\deg K}$$

pour tout $v \in M_\infty(K)$. Comme les a_i $(i = 1, \ldots, 2g+1)$ sont des entiers de K on a

$$\begin{aligned} H_K(f) &\leq \prod_{v \in M_\infty(K)} (W_v^{(2g+1)\delta_v} (|D_K|^{1/2} N_{K0}\{W_v\})^{(4g+2)\delta_v/\deg K}) \\ &\leq |D_K|^{2g+1} (N_K\{W_v\})^{4g+2}\,. \end{aligned}$$

D'autre part, on a

$$N_K\{W_v\} < c_1(d,N) H_K(F)^{6\cdot 10^3 (g+2) 2^{g-2} N^{15}} \tag{5.3}$$

où

$$c_1(d,N) < (3N)^{24\cdot 10^3 d 2^{N^2} N^{18}}\,,$$

ce qui donne

$$H_K(f) < c_2(d,N)|D_k|^{(2g+1)N} H_k(F)^{2\cdot 10^4(2g+1)(g+2)2^{g-2}N^{16}} \tag{5.4}$$

avec

$$c_2(d,N) < (3N)^{6\cdot 10^4 d 2^{N^2}N^{20}}\,.$$

Supposons maintenant $\tau(V) \neq V$. Considérons la quantité

$$W_v = A_v^{2^{g-1}9N^4+36(3g+4)(g+1)2^g N^3} B_v^{2^{g+1}N+2^{g+3}(g+1)(3g+4)} \times \prod_{j=1}^{r} A_v(u_j)^{2^{g-1}10N^3 e_j} v(2^{7(2g+1)^3}(2^{g+1}4n^2)^n)\,.$$

Alors $\{W_v\}$ est un K-système.

Comme précédemment il existe un entier algébrique $\alpha \in K$, $\alpha \neq 0$, vérifiant des relations analogues à (5.1) et (5.2). Posons

$$X_1 = a'_{2g+2}\alpha^2 X'\,, \quad \Phi_1 = (\sqrt{a'_{2g+2}})^{2g+1}\alpha^{2g+2}\Phi'\,.$$

Alors on a

$$\Phi_1^2 = X_1^{2g+2} + a_1 X^{2g+1} + \ldots + a_{2g+2}$$

où

$$a_i = a'_{2g+2-i}\alpha^{2i}a'^{i-1}_{2g+2} \quad (i = 1,\ldots,2g+2)\,.$$

Les coefficients a_i sont des entiers algébriques de K. Il résulte aussi que X_1 est entier sur $O_K[X]$. Donc si X, Φ sont des entiers de k, alors X_1, Φ_1 sont des entiers de $K' = K(\sqrt{a'_{2g+2}})$.

Notons $f(X_1) = X_1^{2g+2} + a_1 X_1^{2g+1} + \ldots + a_{2g+2}$. Alors

$$|f|_v \leq W_v^{2g+2}(|D_K|^{1/2}N_{K0}\{W_v\})^{4g+4/\deg K}$$

pour tout $v \in M_\infty(K)$. Comme les a_i $(i = 0,\ldots,2g+2)$ sont des entiers de K on a

$$\begin{aligned} H_K(f) &\leq \prod_{v\in M_\infty(K)} (W_v^{(2g+2)\delta_v}(|D_K|^{1/2}N_{K0}\{W_v\})^{(4g+4)\delta_v/\deg K}) \\ &\leq |D_K|^{2g+2}(N_K\{W_v\})^{4g+4}\,. \end{aligned}$$

On a aussi

$$N_K\{W_v\} < c_3(d,N)H_K(F)^{12\cdot 10^3 2^{g-2}(g+3)N^{15}} \tag{5.5}$$

où

$$c_3(d,N) < (3N)^{48\cdot 10^3 d 2^{N^2}N^{18}}\,.$$

On en déduit que

$$H_K(f) < c_4(d,N)|D_k|^{(2g+2)N} H_K(F)^{5\cdot 10^4 2^{g-2}(g+1)(g+3)N^{16}} \tag{5.6}$$

où

$$c_4(d,N) < (3N)^{6\cdot 10^4 d 2^{N^2} N^{20}}.$$

6. Démonstration du théorème. Nous allons utiliser le résultat suivant :

THÉORÈME A. *Soient L un corps de nombres de degré λ, B l'anneau des entiers de L et D_L son discriminant. Soit $f(X)$ un polynôme de $L[X]$ de degré n ayant au moins trois racines d'ordre impair. Alors si $(x,y) \in B \times B$ est une solution de l'équation $Y^2 = f(X)$ on a*

$$\max\{H_L(x), H_L(y)\} < \exp\{c(\lambda,n)(W_1^{n^n} W_2^{\lambda n^n}\}$$

où

$$W_1 = D_L^{12} H_L(f)^{1000\lambda^2}, \qquad W_2 = (\log^* |D_L|)^3 (\log^* H_L(f))^5$$

et

$$c(\lambda,n) < 2^{300\lambda^2 n^{2n}}$$

(*pour z réel positif on note* $\log^* z = \max(1, \log z)$).

Ceci raffine un résultat de Brindza (Acta Math. Hungar. 44 (1984), 133–139), dans lequel la dépendance de la majoration en λ, n, D_L et $H_L(f)$ n'est pas donné explicitement. On peut consulter [3] pour une démonstration du théorème A.

P r e m i e r c a s : $\tau(V) = V$. La fonction $X_1 = \alpha^2 a'_{2g+1} X'$ vérifie l'équation $R(X,T) = 0$, où $R(X,T) = (\alpha^2 a'_{2g+1})^n P(X, T/\alpha^2 a'_{2g+1})$. Les coefficients de $R(X,T)$ sont les $\pi_{is}(\alpha^2 a'_{2g+1})^i$ qui sont des entiers de K. Comme $R(X,T)$ n'a pas de facteur indépendant de X, pour tout x_1 le polynôme $R^*(X) = R(X,x_1)$ est non nul de degré ≤ 2. Alors pour tout $\upsilon \in M_\infty(K)$ on a

$$|R^*|_\upsilon \le (\max_{i,s} |\pi_{i,s}|_\upsilon |\alpha^2 a'_{2g+1}|_\upsilon^i)(\max(1, |x_1|_\upsilon^n))\upsilon(n+1).$$

Si x_1 est un entier de K alors les coefficients de R^* sont des entiers de K; on a donc

$$H_K(R^*) \le (|D_K|^{1/2} N_K\{W_\upsilon\})^{2n} H_K(x_1)^n (n+1)^{\deg K}.$$

Les majorations (3.1) et (5.3) entraînent

$$H_K(R^*) < c_5(d,N) |D_k|^{N^2} H_k(F)^{2\cdot 10^4 (g+2) 2^{g-2} N^{17}} H_K(x_1)^n$$

où

$$c_5(d,N) < (3N)^{5\cdot 10^4 d 2^{N^2} N^{19}}.$$

Soit Ω l'application birationnelle de la courbe $F(X,Y) = 0$ sur la courbe $\Phi_1^2 = f(X_1)$. Soit $(x,y) \in A \times A$ un point non singulier sur $F(X,Y) = 0$; alors $\Omega(x,y) = (x_1, y_1)$ et il en résulte que $R(x,x_1) = 0$; par conséquent on

a $R^*(x) = 0$. Le lemme 3 de [5] entraîne que $H(x) \leq 3H(R^*)$. Alors on a $(x_1, y_1) \in O_K \times O_K$ et

$$H_K(x) < 3^{dN} c_5(d,N) |D_k|^{N^2} H_k(F)^{2\cdot 10^4 (g+2) 2^{g-2} N^{17}} H_K(x_1)^n \,. \tag{6.1}$$

D'autre part, le théorème A entraîne

$$\begin{aligned} H_K(x_1) < \exp\{c_6(d,N) [D_K^{12} H_K(f)^{1000 d^2 N^2}]^{(2g+1)^{2g+1}} \\ \times [(\log^* |D_K|)^3 (\log^* H_K(f))^5]^{dN(2g+1)^{2g+1}}\} \end{aligned} \tag{6.2}$$

où

$$c(d,N) < 2^{300 d^2 N^2 N^{4N^2}} \,.$$

Alors les majorations (3.1), (5.4), (6.1) et (6.2) entraînent le résultat.

Deuxième cas : $\tau(V) \neq V$. La fonction $X_1 = a'^{2g+2}_{2g+2} \alpha^2 X'$ vérifie l'équation $R(X,T) = 0$, où $R(X,T) = (\alpha^2 a'_{2g+2})^n P(X, T/\alpha^2 a'_{2g+2})$. Les coefficients de $R(X,T)$ sont les $\pi_{is} (\alpha^2 a'_{2g+2})^i$ qui sont des entiers de K. Pour tout x_1 le polynôme $R^*(X) = R(X, x_1)$ est non nul de degré ≤ 2. Alors si x_1 est un entier de K on a

$$H_K(R^*) \leq (|D_K|^{1/2} N_K\{W_v\})^{2n} H_K(x_1)^n (n+1)^{\deg K} \,.$$

Les majorations (3.1) et (5.5) entraînent

$$H_K(R^*) < c_7(d,N) |D_k|^{N^2} H_k(F)^{3\cdot 10^4 (g+3) 2^{g-2} N^{17}} H_K(x_1)^n$$

où

$$c_7(d,N) < (3N)^{10^5 d 2^{N^2} N^{19}} \,.$$

Soit $(x,y) \in A \times A$ un point non singulier sur $F(x,y) = 0$; alors $\Omega(x,y) = (x_1, y_1)$ et il en résulte que $R(x, x_1) = 0$; donc $R^*(x) = 0$. De plus $(x_1, y_1) \in O_K \times O_{K'}$. Comme $H(x) \leq 3H(R^*)$ on conclut que

$$H_K(x) < 3^{dN} c_7(d,N) |D_k|^{N^2} H_k(F)^{3\cdot 10^4 (g+3) 2^{g-2} N^{17}} H_K(x_1)^n \,. \tag{6.3}$$

En utilisant le théorème A et les majorations (3.1), (5.6) et (6.3) on obtient le résultat.

Dans le cas où (x,y) est un point singulier de $F(X,Y) = 0$ on obtient d'une façon élémentaire une meilleure majoration.

Remerciements. Je remercie le professeur Michel Waldschmidt pour les discussions utiles que j'ai eues avec lui pendant la préparation de ce travail.

Références

[1] A. Baker and J. Coates, *Integer points on curves of genus* 1, Proc. Cambridge Philos. Soc. 67 (1970), 595–602.

[2] J. Coates, *Construction of rational functions on a curve*, ibid. 68 (1970), 105–123.
[3] D. Poulakis, *Solutions entières de l'équation* $Y^m = f(X)$, Sém. Théorie des Nombres de Bordeaux 3 (1991), 187–199.
[4] W. M. Schmidt, *Integer points on curves of genus* 1, Compositio Math. 81 (1992), 33–59.
[5] —, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. 56 (1990), 161–179.
[6] —, *Construction and estimation of bases in function fields*, J. Number Theory 39 (1991), 181–224.
[7] J. P. Serre, *Lectures on the Mordell–Weil Theorem*, Vieweg, 1989.
[8] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. 1 (1929).
[9] R. Walker, *Algebraic Curves*, Springer, 1978.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE THÉSSALONIQUE
54006 THÉSSALONIQUE, GRÈCE

Reçu le 2.4.1991 (2131)