BULL. AUSTRAL. MATH. SOC. 11G30, 11G05, 11G50
VOL. 75 (2007) [91–119]

PROBLÈMES D'EFFECTIVITÉ SUR LES QUARTIQUES DE FERMAT

ÉLIE CALI ET ALAIN KRAUS

Let K be a number field. An element $b \in K^*$ being given, let C_b be the curve defined over K by the equation $x^4 + y^4 = bz^4$. Let $C_b(K)$ be the set of the K-rational points of C_b. This paper uses Dem'janenko and Manin type methods to obtain effective criteria for $C_b(K)$ to be empty.

INTRODUCTION

Soit K un corps de nombres. Étant donné un élément b de K^*, on note C_b la courbe définie sur K d'équation

$$x^4 + y^4 = bz^4.$$

C'est une courbe lisse de genre 3. D'après les travaux de G. Faltings, l'ensemble $C_b(K)$ des points de C_b rationnels sur K est fini. On s'intéresse dans ce travail à l'effectivité de certaines méthodes globales concernant l'étude de $C_b(K)$. Soit E_b la courbe elliptique définie sur K d'équation

$$Y^2Z = X^3 - bXZ^2.$$

Les classes de K-isomorphisme de C_b et E_b ne dépendent que de la classe de b modulo K^{*4}. Il existe deux morphismes indépendants définis sur K de C_b sur E_b. En particulier, si $E_b(K)$ est de rang 0, il est facile de déterminer $C_b(K)$. Dans le cas où $E_b(K)$ est de rang 1, on obtient dans ce qui suit des critères effectifs entraînant que $C_b(K)$ est vide. Comme conséquence d'une étude des points rationnels de tordues galoisiennes de courbes sur les corps de nombres, J. Silverman a démontré en 1986 le résultat suivant ([8]).

THÉORÈME. (Silverman) *Il existe une constante absolue c_0, dépendant seulement du degré de K sur $\mathbb{Q}$, telle que l'assertion suivante soit satisfaite.*

Soient b un élément de K^* qui ne soit pas dans K^{*4} et L une extension de K obtenue en adjoignant à K une racine quatrième de b. Alors, si $E_b(K)$ est de rang 1 et si la norme de K sur $\mathbb{Q}$ du discriminant relatif de l'extension L/K est plus grande que c_0, l'ensemble $C_b(K)$ est vide.

En particulier, pour toute classe d'élément b dans K^*/K^{*4} sauf un nombre fini, si le rang de $E_b(K)$ est 1, alors $C_b(K)$ est vide.

Received 31st July, 2006

Sa démonstration repose sur la mise en œuvre d'une méthode de Dem'janenko et Manin faisant intervenir des arguments de hauteurs. Silverman a démontré l'existence d'une constante c_0 dépendant exponentiellement du degré de K sur $\mathbb{Q}$. Dans la première partie de ce travail, on se préoccupe de l'effectivité de cet énoncé en explicitant une telle constante c_0. On est confronté pour cela au problème de rendre effectif le théorème des zéros de Hilbert dans un cas particulier (appendice 1). Comme conséquence du résultat que l'on obtient à ce sujet, en notant n le degré de K sur $\mathbb{Q}$, on constate que l'on peut prendre

$$c_0 = \exp(48 + 6n).$$

Cette constante s'avère inefficace d'un point de vue pratique. Dans le cas particulier où $K = \mathbb{Q}$, on dispose du résultat optimal suivant prouvé par Dem'janenko en 1968 ([2]).

THÉORÈME. (Dem'janenko) *Soit b un entier $\geqslant 3$ sans puissances quatrièmes. Si $E_b(\mathbb{Q})$ est de rang $\leqslant 1$, alors $C_b(\mathbb{Q})$ est vide.*

On généralise dans la deuxième partie cet énoncé aux corps totalement réels, avec une constante effective qui reste utilisable en pratique dans certaines situations. On s'est inspiré pour cela d'une méthode de G. Grigorov et J. Rizov qui leur a permis d'obtenir, si $K = \mathbb{Q}$, des estimations uniformes pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur E_b, et d'en déduire une nouvelle démonstration du Théorème de Dem'janenko ([3]). On obtient le résultat suivant: le corps K étant totalement réel, de degré n sur $\mathbb{Q}$, soit $(u_1, \ldots, u_{n-1})$ un système d'unités fondamentales de l'anneau d'entiers O_K de K. Pour tout $x \in O_K$, notons $H(x)$ la hauteur de x relative à K. On a

$$H(x) = \prod_{\sigma} \operatorname{Max}\Big(1, \big|\sigma(x)\big|\Big),$$

où σ parcourt les n plongements de K dans $\mathbb{R}$. Notons par ailleurs $\mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ l'application norme de K sur $\mathbb{Q}$ et $v_{\mathfrak{P}} : K^* \to \mathbb{Z}$ la valuation sur K standard normalisée associée à un idéal premier $\mathfrak{P}$ de O_K.

THÉORÈME. *Soit b un élément non nul de O_K. Supposons que les conditions suivantes soient satisfaites.*

(1) *pour tout idéal premier $\mathfrak{P}$ de O_K, on a $v_{\mathfrak{P}}(b) < 4$.*

(2) *Le groupe $E_b(K)$ est de rang $\leqslant 1$.*

(3) *On a les inégalités*

$$\mathrm{N}_{K/\mathbb{Q}}(b) > 2^{(11n)/2} \quad \text{et} \quad \mathrm{N}_{K/\mathbb{Q}}(b) \geqslant \left(\prod_{i=1}^{n-1} H(u_i)\right)^4.$$

Alors, l'ensemble $C_b(K)$ est vide.

Pour exploiter numériquement cet énoncé, il importe évidemment de savoir démontrer que, b étant donné, le rang de $E_b(K)$ est au plus 1, si tel est le cas. On peut effectuer pour

cela une 2-descente comme il est expliqué dans [7]. Signalons à ce propos qu'il existe un programme, écrit par D. Simon, qui permet parfois de déterminer le rang d'une courbe elliptique sur un corps de nombres de degré sur $\mathbb{Q}$ assez petit ([9]).

Nous remercions vivement E. Halberstadt qui nous a communiqué le résultat qui lui est dû figurant dans l'appendice 3. Nous remercions également le referee de cet article qui nous a indiqué que les résultats obtenus dans [5], ou bien dans [1], permettaient d'améliorer les énoncés du Théorème 1 et de son corollaire. Signalons que la constante c_0 que nous obtenions préalablement était $\exp(169 + 6n)$.

I. Effectivité du Théorème de Silverman

Soient $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et K un corps de nombres contenu dans $\overline{\mathbb{Q}}$. Considérons un élément non nul b de K qui n'est pas dans K^4 et choisissons une racine quatrième α de b dans $\overline{\mathbb{Q}}$. Notons:

(a) L le corps $K(\alpha)$.

(b) d le degré de L sur K; on a $d = 4$ si et seulement si b n'est pas un carré dans K et b n'est pas dans $-4K^4$. On a $d = 2$ sinon.

(c) $D_{L/K}$ le discriminant relatif de l'extension L/K; c'est un idéal de l'anneau d'entiers de K.

(d) $\mathrm{N}_{K/\mathbb{Q}}(D_{L/K})$ la norme de K sur $\mathbb{Q}$ de $D_{L/K}$.

(e) δ_K le nombre de places archimédiennes de K. Si r_1 (respectivement $2r_2$) est le nombre de plongements réels (respectivement complexes) de K, on a $\delta_K = r_1 + r_2$.

L'énoncé que l'on obtient est le suivant.

Théorème 1. *Supposons que le rang de $E_b(K)$ soit 1. Alors, si l'on a*

$$\log \mathrm{N}_{K/\mathbb{Q}}(D_{L/K}) \geqslant (3{,}98\ (d-1) + \delta_K\ \log d)d, \tag{1}$$

l'ensemble $C_b(K)$ est vide.

En notant D_L le discriminant de L et D_K celui de K, on a

$$|D_L| = \mathrm{N}_{K/\mathbb{Q}}(D_{L/K})|D_K|^d,$$

de sorte que l'inégalité (1) peut aussi s'écrire

$$\log |D_L| \geqslant \Big(3{,}98\ (d-1) + \delta_K\ \log d + \log |D_K|\Big)d.$$

Puisque le degré n de K sur $\mathbb{Q}$ vaut $r_1 + 2r_2$, on déduit directement du théorème l'énoncé suivant signalé dans l'introduction.

Corollaire 1. *Supposons que le rang de $E_b(K)$ soit 1. Alors, si l'on a*

$$\mathrm{N}_{K/\mathbb{Q}}(D_{L/K}) \geqslant \exp(48 + 6n),$$

l'ensemble $C_b(K)$ est vide.

Démonstration du Théorème 1

1.1. Notations. Étant donné un corps de nombres k, on introduit les notations suivantes:

(a) O_k son anneau d'entiers.

(b) $v_{\mathfrak{P}} : k^* \to \mathbb{Z}$ la valuation normalisée standard associée à un idéal premier $\mathfrak{P}$ de O_k.

(c) M_k l'ensemble des places de k, c'est l'ensemble des classes d'équivalence de valeurs absolues usuelles sur k.

(d) M_k^∞ l'ensemble des places archimédiennes de k. Si $v \in M_k^\infty$ correspond à un plongement $\sigma : k \to \mathbb{C}$, la valeur absolue normalisée associée à v est définie pour tout $x \in k$ par la formule

$$|x|_v = |\sigma(x)|.$$

(e) M_k^0 l'ensemble des places non archimédiennes de k. Soit v une telle place correspondant à un idéal premier $\mathfrak{P}$ de O_k de caractéristique résiduelle p. La place v est représentée par la valeur absolue qui est définie pour tout $x \in k^*$ par la formule

$$|x|_v = p^{-v_{\mathfrak{P}}(x)/e_{\mathfrak{P}}},$$

où $e_{\mathfrak{P}} = v_{\mathfrak{P}}(p)$ est l'indice de ramification de $\mathfrak{P}$ sur p.

(f) Pour tout $v \in M_k$, on note n_v le degré local de v. Si $v \in M_k^\infty$, on a $n_v = 1$ ou $n_v = 2$. On a $n_v = 1$ si et seulement si v correspond à un plongement de k dans $\mathbb{R}$. Si $v \in M_k^0$ est associée à un idéal premier $\mathfrak{P}$ de O_k au-dessus d'un nombre premier p, on a $n_v = e_{\mathfrak{P}} f_{\mathfrak{P}}$ où $f_{\mathfrak{P}}$ est le degré de $O_k/\mathfrak{P}$ sur $\mathbb{F}_p$.

1.2. Les hauteurs h_C, h_E et $\widehat{h}_E$. Rappelons la définition de l'application hauteur absolue logarithmique $h : \mathbb{P}^2(\overline{\mathbb{Q}}) \to \mathbb{R}$ définie sur l'ensemble des points du plan projectif $\mathbb{P}^2$ à valeurs dans $\overline{\mathbb{Q}}$. Soient $P = [x, y, z]$ un point de $\mathbb{P}^2(\overline{\mathbb{Q}})$ et k un corps de nombres contenant x, y et z. La hauteur absolue logarithmique $h(P)$ de P est définie par la formule ([7, p. 215]).

$$h(P) = \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} n_v \log \operatorname{Max}\big(|x|_v, |y|_v, |z|_v\big), \tag{2}$$

où $[k : \mathbb{Q}]$ est le degré de k sur $\mathbb{Q}$. La définition de $h(P)$ ne dépend pas du choix des coordonnées de P choisies ni du corps de nombres k les contenant.

Afin de simplifier les notations, on désigne dans la suite par C et E les courbes sur $\mathbb{Q}$ d'équations

$$C : \ x^4 + y^4 = z^4 \quad \text{et} \quad E : \ Y^2Z = X^3 - XZ^2.$$

On notera:

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

(a) h_C la restriction de h à $C(\overline{\mathbb{Q}})$.

(b) h_E la hauteur sur E relative à la fonction X/Z (*loco citato*). En posant $O = [0,1,0]$, on a $h_E(O) = 0$. Pour tout point $M = [X,Y,Z] \in E(\overline{\mathbb{Q}})$ distinct de O et tout corps k contenant X et Z, on a l'égalité:

$$h_E(M) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \log \operatorname{Max}\big(|X|_v, |Z|_v\big). \tag{3}$$

Cette définition ne dépend pas du choix des coordonnées de M.

(c) $\widehat{h}_E : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ la hauteur de Néron–Tate sur E ([**7**, p. 228]). On a $2\widehat{h}_E = h_E + O(1)$ (voir *loco citato*, Theorem 9.3, p. 229). Comme nous l'a signalé le referee de cet article, les résultats qui se trouvent dans [**5**] ou [**1**] ont été implantés sur ordinateur par les auteurs. Leur programme permet d'obtenir, pour tout point $M \in E(\overline{\mathbb{Q}})$, l'inégalité:

$$\left|\widehat{h}_E(M) - \frac{1}{2} h_E(M)\right| \leqslant 0,232. \tag{4}$$

1.3. UNE MAJORATION DE HAUTEUR. On dispose de deux morphismes ϕ et ψ sur $\mathbb{Q}$ de C sur E définis pour tout point $[x,y,z]$ de C par les formules

$$\phi\big([x,y,z]\big) = [-x^2 z, xy^2, z^3] \quad \text{et} \quad \psi\big([x,y,z]\big) = [-y^2 z, x^2 y, z^3]. \tag{5}$$

On va démontrer le résultat suivant.

THÉORÈME 2. *Soit P un point de $C(\overline{\mathbb{Q}})$. Supposons que $\phi(P)$ et $\psi(P)$ dans $E(\overline{\mathbb{Q}})$ soient linéairement dépendants sur $\mathbb{Z}$. Alors, on a*

$$h_C(P) < 1,99. \tag{6}$$

DÉMONSTRATION: Indiquons d'abord le principe de la démonstration. Soit $\phi + \psi : C \to E$ le morphisme somme de ϕ et ψ relatif à loi de groupe sur E. On fournit des majorations explicites des quantités

$$\left|h_C(P) - \widehat{h}_E\big(\phi(P)\big)\right|,$$

$$\left|h_C(P) - \widehat{h}_E\big(\psi(P)\big)\right|,$$

et

$$\left|2h_C(P) - \widehat{h}_E\Big(\big(\phi+\psi\big)(P)\Big)\right|.$$

Notons $\langle\ ,\ \rangle : E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \to \mathbb{R}$ l'accouplement de Néron-Tate sur E (voir [**7**, p. 232]). On a

$$\begin{aligned}
\langle \phi(P), \phi(P) \rangle &= 2\widehat{h}_E\big(\phi(P)\big), \\
\langle \psi(P), \psi(P) \rangle &= 2\widehat{h}_E\big(\psi(P)\big), \\
\langle \phi(P), \psi(P) \rangle &= \widehat{h}_E\Big(\big(\phi+\psi\big)(P)\Big) - \widehat{h}_E\big(\phi(P)\big) - \widehat{h}_E\big(\psi(P)\big).
\end{aligned}$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Les points $\phi(P)$ et $\psi(P)$ étant linéairement dépendants dans $E(\overline{\mathbb{Q}})$, le déterminant de la matrice

$$\begin{pmatrix} \langle \phi(P), \phi(P) \rangle & \langle \phi(P), \psi(P) \rangle \\ \langle \phi(P), \psi(P) \rangle & \langle \psi(P), \psi(P) \rangle \end{pmatrix}$$

est nul. Les majorations obtenues ci-dessus permettent alors d'obtenir le résultat annoncé.

Posons $P = [x, y, z] \in C(\overline{\mathbb{Q}})$. Pour toute la suite de la démonstration, on considère un corps de nombres k contenant x, y et z. On supposera, ce qui n'est pas restrictif, que x, y et z sont dans O_k.

PROPOSITION 1. *On a l'inégalité*

$$\left| 4h_C(P) - h_E\Big((\phi + \psi)(P) \Big) \right| \leqslant \log 69. \tag{7}$$

DÉMONSTRATION: On vérifie que l'on a

$$(\phi + \psi)([x, y, z]) = [U, V, W],$$

avec $$U = (x+y)z(x^2 + xy + y^2)^2, \quad V = -xy(x^2 + xy + y^2)(2x^2 + 3yx + 2y^2),$$
$$W = (x+y)^3 z^3.$$

Vérifions l'inégalité (7) si $(x+y)z = 0$. On a dans ce cas $U = W = 0$ et $(\phi+\psi)(P) = O$, d'où $h_E\Big((\phi + \psi)(P) \Big) = 0$.

Si $z = 0$, on a $xy \neq 0$ et pour tout $v \in M_k$ on a $|x|_v = |y|_v$, ce qui conduit d'après la formule du produit à $h_C(P) = 0$ (formule (2)).

Supposons $x + y = 0$. On a alors $2x^4 = z^4$, $xyz \neq 0$ et $P = [1, -1, \beta]$, où $\beta \in \overline{\mathbb{Q}}$ vérifie l'égalité $\beta^4 = 2$. Prenons pour k le corps $\mathbb{Q}(\beta)$. On a alors $r_1 = 2$, $r_2 = 1$. Pour toute place $v \in M_k^\infty$, on a $|\beta|_v = 2^{1/4}$ où $2^{1/4}$ est la racine quatrième positive de 2 dans $\mathbb{R}$. Par ailleurs, β étant dans O_k, on a $|\beta|_v \leqslant 1$ pour toute place finie $v \in M_k^0$. Il en résulte que l'on a

$$h_C(P) = \frac{1}{4}(4 \ \log 2^{1/4}) = \frac{1}{4} \log 2.$$

Puisque $4h_C(P) = \log 2$ est plus petit que $\log 69$, l'inégalité (7) est donc vraie si $x+y = 0$. D'où notre assertion.

Supposons désormais $(x + y)z$ non nul. Dans ce cas, on a (formule (3))

$$h_E\Big((\phi + \psi)(P) \Big) = \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} n_v \ \log \mathrm{Max}\Big(\big|x^2 + xy + y^2\big|_v^2, \big|(x+y)z\big|_v^2 \Big). \tag{8}$$

Pour tout $v \in M_k^0$ on a

$$\big|x^2 + xy + y^2\big|_v \leqslant \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2$$

et

$$\big|(x+y)z\big|_v \leqslant \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2.$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Par ailleurs, pour tout $v \in M_k^\infty$ on a

$$|x^2 + xy + y^2|_v \leqslant 3 \ \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2$$

et

$$|(x+y)z|_v \leqslant 2 \ \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2.$$

On en déduit l'inégalité

$$h_E\Big((\phi+\psi)(P)\Big) \leqslant \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k^0} n_v \ \log \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^4 + \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k^\infty} n_v \ \log\Big(9 \ \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^4\Big).$$

Compte tenu du fait que

$$[k:\mathbb{Q}] = \sum_{v \in M_k^\infty} n_v,$$

il en résulte que l'on a

$$h_E\Big((\phi+\psi)(P)\Big) \leqslant \log 9 + 4h_C(P). \tag{9}$$

Inversement, démontrons que l'on a

$$4h_C(P) \leqslant \log 69 + h_E\Big((\phi+\psi)(P)\Big). \tag{10}$$

On utilise pour cela la proposition de l'appendice 1. Posons

$$g = (x^2 + xy + y^2)^2 \quad \text{et} \quad h = (x+y)^2 z^2.$$

Le point $[x, y, z]$ appartenant à $C(\overline{\mathbb{Q}})$ on a $x^4 + y^4 = z^4$. Par suite, les égalités (1) et (2) de cette proposition entraînent, avec ses notations,

$$\begin{aligned} x^{12} &= Q(x,y,z)g + R(x,y,z)h, \\ y^{12} &= Q(y,x,z)g + R(y,x,z)h, \\ z^{12} &= 2z^8 g - z^6(x+y)^2 h. \end{aligned}$$

Pour toute place finie $v \in M_k^0$, les éléments x, y et z étant dans O_k, les valeurs absolues v-adiques des éléments $Q(x,y,z)$, $R(x,y,z)$, $Q(y,x,z)$ et $R(y,x,z)$ sont inférieures à $\mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^8$. On en déduit que

$$\mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^4 \leqslant \mathrm{Max}\big(|g|_v, |h|_v\big).$$

Pour toute place $v \in M_k^\infty$ on obtient dans ce cas l'inégalité (voir les coefficients des polynômes Q et R de la proposition de l'appendice 1)

$$\mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^4 \leqslant 69 \ \mathrm{Max}\big(|g|_v, |h|_v\big).$$

L'égalité (8) entraîne alors l'inégalité (10). La proposition se déduit alors des conditions (9) et (10).

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

PROPOSITION 2. *On a les inégalités*

$$(11) \qquad \left|2h_C(P) - h_E\big(\phi(P)\big)\right| \leqslant \frac{\log 2}{2} \quad \text{et} \quad \left|2h_C(P) - h_E\big(\psi(P)\big)\right| \leqslant \frac{\log 2}{2}.$$

DÉMONSTRATION: Par symétrie par rapport à x et y, il suffit de démontrer la première inégalité de (11). Supposons $z = 0$. On a $\phi(P) = [0,1,0]$ et $h_E\big(\phi(P)\big) = 0$. Par ailleurs, on a $h_C(P) = 0$ comme on l'a déjà constaté dans la démonstration de la proposition 1. D'où le résultat dans ce cas. Supposons z non nul. D'après les formules (5), on a alors

$$h_E\big(\phi(P)\big) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \log \operatorname{Max}\big(|x|_v^2, |z|_v^2\big).$$

Posons $a = x^2$ et $b = z^2$. On a $x^4 + y^4 = z^4$. On en déduit pour tout $v \in M_k^0$ l'inégalité $|y|_v^2 \leqslant \operatorname{Max}\big(|a|_v, |b|_v\big)$. Par suite, on a dans ce cas

$$\operatorname{Max}\big(|x|_v, |y|_v, |z|_v\big)^2 \leqslant \operatorname{Max}\big(|a|_v, |b|_v\big).$$

Par ailleurs, pour tout $v \in M_k^\infty$ on a $|y|_v^2 \leqslant \sqrt{2}\operatorname{Max}\big(|a|_v, |b|_v\big)$ et l'on obtient ainsi

$$\operatorname{Max}\big(|x|_v, |y|_v, |z|_v\big)^2 \leqslant \sqrt{2}\operatorname{Max}\big(|a|_v, |b|_v\big).$$

Il en résulte l'inégalité

$$2h_C(P) \leqslant \frac{\log 2}{2} + h_E\big(\phi(P)\big).$$

Inversement, pour tout $v \in M_k$ on a

$$|a|_v, |b|_v \leqslant \operatorname{Max}\big(|x|_v, |y|_v, |z|_v\big)^2,$$

d'où $h_E\big(\phi(P)\big) \leqslant 2h_C(P)$ et le résultat.

COROLLAIRE 2. *On a les inégalités*

$$\begin{aligned} \left|h_C(P) - \widehat{h}_E\big(\phi(P)\big)\right| &\leqslant 0,406, \\ \left|h_C(P) - \widehat{h}_E\big(\psi(P)\big)\right| &\leqslant 0,406, \\ \left|2h_C(P) - \widehat{h}_E\Big(\big(\phi+\psi\big)(P)\Big)\right| &\leqslant 2,35. \end{aligned}$$

DÉMONSTRATION: C'est une conséquence directe de l'inégalité (4) ainsi que des Propositions 1 et 2.

Terminons maintenant la démonstration du Théorème 2. Posons pour cela

$$\widehat{h}_E\big(\phi(P)\big) = h_C(P) + \delta,$$

$$\widehat{h}_E\big(\psi(P)\big) = h_C(P) + \beta$$

et

$$\widehat{h}_E\Big(\big(\phi+\psi\big)(P)\Big) = 2h_C(P) + \gamma.$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

En exprimant le fait que le déterminant de la matrice

$$\begin{pmatrix} 2\big(h_C(P)+\delta\big) & \gamma-(\delta+\beta) \\ \gamma-(\delta+\beta) & 2\big(h_C(P)+\beta\big) \end{pmatrix}$$

est nul, on obtient l'égalité

$$h_C(P)^2+(\delta+\beta)h_C(P)+\delta\beta-\frac{(\gamma-(\delta+\beta))^2}{4}=0.$$

Le discriminant de cette équation est $2\delta^2+2\beta^2+\gamma^2-2\gamma(\delta+\beta)$. Il est donc majoré en valeur absolue par

$$2\delta^2+2\beta^2+\gamma^2+2\,|\gamma|\,|\delta|+2\,|\gamma|\,|\beta|\,,$$

donc, d'après le Corollaire 2, par 10. Il en résulte que l'on a

$$h_C(P)<\frac{|\delta|+|\beta|+\sqrt{10}}{2}<1,99$$

d'où le théorème.

1.4. Fin de la démonstration du Théorème 1. Rappelons que α désigne une racine quatrième de b dans $\overline{\mathbb{Q}}$. Les courbes C_b et C sont isomorphes sur $L=K(\alpha)$ via le morphisme $f_b : C_b \to C$ défini pour tout point $[x,y,z]$ de C_b par l'égalité

$$f_b\big([x,y,z]\big)=[x,y,\alpha z].$$

Le corps L est un corps minimal, au sens de l'appendice 2, sur lequel les courbes C_b et C sont isomorphes. En effet, par hypothèse b n'est pas une puissance quatrième dans K, donc C et C_b ne sont pas isomorphes sur K (on peut le vérifier en utilisant le Théorème 2.2 de [7, p. 285]). L'assertion est donc immédiate si $d=2$. Supposons $d=4$ et C_b isomorphe à C sur une extension quadratique H de K contenue dans L. Dans ce cas, b est alors une puissance quatrième dans H, ce qui conduit à une contradiction, d'où l'assertion.

Supposons que $C_b(K)$ ne soit pas vide. Considérons un point $P\in C_b(K)$. Posons $P=[x,y,z]$ (où x, y et z sont dans O_K) et $Q=f_b(P)\in C(L)$. On est dans l'un des deux cas intervenant dans l'énoncé du théorème de l'appendice 2.

Supposons que l'on soit dans le premier cas de ce théorème, c'est a dire qu'il existe σ dans le groupe de Galois de $\overline{\mathbb{Q}}$ sur K tel que ${}^{\sigma}f_b\circ f_b^{-1}$ ne soit pas l'identité de C et fixe le point Q. On a l'égalité

$${}^{\sigma}f_b\circ f_b^{-1}(Q)=\big[x,y,\sigma(\alpha)z\big],$$

ce qui conduit à $z\big(\sigma(\alpha)-\alpha\big)=0$. On a $\sigma(\alpha)\neq\alpha$ car ${}^{\sigma}f_b$ est distinct de f_b. Il en résulte que $z=0$. On en déduit que $xy\neq 0$ puis que $P=[x/y,1,0]$ où x/y est une

racine primitive huitième de l'unité. En particulier, le groupe μ_4 des racines quatrièmes de l'unité est contenu dans K. Soient i un générateur de μ_4 et $[i]$ l'automorphisme de E_b défini par

$$[i](X,Y,Z) = [-X, iY, Z].$$

Le groupe $E_b(K)$ est alors muni de la structure de $\mathbb{Z}[i]$-module définie pour tous $a, b \in \mathbb{Z}$ et $M \in E_b(K)$ par l'égalité

$$(a+ib).M = aM + b[i](M).$$

Ainsi, $E_b(K)$ modulo son sous-groupe de torsion est un $\mathbb{Z}[i]$-module libre de rang $r/2$ où r est le rang usuel de $E_b(K)$. L'entier r est donc pair ce qui contredit le fait que $r = 1$.

La condition 2 du théorème de l'appendice 2 est donc satisfaite, autrement dit on a

$$\log \mathrm{N}_{K/\mathbb{Q}} D_{L/K} \leqslant \Big(2(d-1)h_C(Q) + \delta_K \log d\Big)d. \tag{12}$$

Les morphismes ϕ et ψ étant définis par les formules (5), vérifions que les points

$$\phi(Q) \quad \text{et} \quad \psi(Q) \in E(L),$$

sont $\mathbb{Z}$-linéairement dépendants dans $E(L)$. Les courbes elliptiques E_b et E sont isomorphes sur L via le morphisme $g_b : E_b \to E$ défini pour tout point $[X,Y,Z]$ de E_b par l'égalité

$$g_b\big([X,Y,Z]\big) = \Big[\frac{X}{\alpha^2}, \frac{Y}{\alpha^3}, Z\Big].$$

Par ailleurs, on dispose de deux morphismes $\phi_b : C_b \to E_b$ et $\psi_b : C_b \to E_b$ définis sur K par les égalités

$$\phi_b\big([x,y,z]\big) = [-x^2z, xy^2, z^3]$$

et

$$\psi_b\big([x,y,z]\big) = [-y^2z, yx^2, z^3].$$

On vérifie directement que l'on a

$$g_b^{-1} \circ \phi \circ f_b = \phi_b \quad \text{et} \quad g_b^{-1} \circ \psi \circ f_b = \psi_b.$$

Il en résulte que les points

$$g_b^{-1} \circ \phi \circ f_b(P) \quad \text{et} \quad g_b^{-1} \circ \psi \circ f_b(P),$$

appartiennent à $E_b(K)$. Puisque le rang de $E_b(K)$ est 1, ces points sont donc $\mathbb{Z}$-dépendants sur $E_b(K)$. Le fait que g_b soit un isomorphisme défini sur L de E_b sur E entraîne alors notre assertion. D'après le Théorème 2, on a donc l'inégalité

$$h_C(Q) < 1,99.$$

On déduit alors de (12) que l'on a

$$\log \mathrm{N}_{K/\mathbb{Q}} D_{L/K} < \Big(3,98\ (d-1) + \delta_K \log d\Big)d,$$

ce qui contredit l'inégalité (1) du Théorème 1. Cela termine sa démonstration.

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

II. Théorème de Dem'janenko et corps totalement réels

On considère dans cette deuxième partie un corps de nombres K totalement réel, de degré n sur $\mathbb{Q}$, d'anneau d'entiers O_K. Pour tout x de O_K, notons $H(x)$ la hauteur de x relative à K. On a

$$H(x) = \prod_{\sigma} \mathrm{Max}\Big(1, |\sigma(x)|\Big),$$

où σ parcourt les n plongements de K dans $\mathbb{R}$. Le groupe des unités de O_K modulo $\{\pm 1\}$ est un $\mathbb{Z}$-module libre de rang $n-1$. Soit $(u_1, \ldots, u_{n-1})$ un système d'unités fondamentales de O_K. On a l'énoncé suivant signalé dans l'introduction.

Théorème 3. *Soit b un élément non nul de O_K. Supposons que les conditions suivantes soient satisfaites.*

(1) *pour tout idéal premier $\mathfrak{P}$ de O_K, on a $v_{\mathfrak{P}}(b) < 4$.*

(2) *Le groupe $E_b(K)$ est de rang $\leqslant 1$.*

(3) *On a les inégalités*

$$\mathrm{N}_{K/\mathbb{Q}}(b) > 2^{(11n)/2} \quad \text{et} \quad \mathrm{N}_{K/\mathbb{Q}}(b) \geqslant \left(\prod_{i=1}^{n-1} H(u_i)\right)^4. \tag{13}$$

Alors, l'ensemble $C_b(K)$ est vide.

Comme conséquence de la démonstration de ce théorème, les conditions 1 et 2 étant toujours supposées réalisées, si de plus pour tout plongement σ de K dans $\mathbb{R}$ on a $\sigma(b) \geqslant 1$, on obtient l'implication

$$\mathrm{N}_{K/\mathbb{Q}}(b) > 2^{(11n)/2} \Longrightarrow C_b(K) = \emptyset.$$

Par ailleurs, il convient de signaler que si O_K est principal, il n'y a qu'un nombre fini d'éléments de K^*/K^{*4} pour lesquels il n'existe pas de représentants satisfaisant les conditions 1 et 3 du théorème. Il n'en va pas de même si O_K n'est pas principal. Par exemple, si le nombre de classes de K est 3, on peut démontrer qu'il existe une infinité d'éléments de K^*/K^{*4} pour lesquels il n'existe pas de représentants $b \in O_K$ satisfaisant la condition 1. Le Théorème 3 est donc un cas particulier effectif du Théorème de Silverman seulement dans le cas où O_K est principal.

Démonstration du Théorème 3. On reprend les notations du paragraphe 1.1, à ceci près que pour toute place finie $v \in M_K^0$, on note ici $v : K^* \to \mathbb{Z}$ la valuation standard normalisée associée à l'idéal premier de O_K qui lui correspond. Avec cette notation, si v est de caractéristique résiduelle p, on a pour tout $x \in K^*$

$$|x|_v = p^{-v(x)/e_v}, \tag{14}$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

où e_v est l'indice de ramification de v sur p.

Soit b un élément de O_K vérifiant les deux premières conditions du Théorème 3. Il s'agit de montrer que si la norme de K sur $\mathbb{Q}$ de b est assez grande, comme il est précisé dans l'énoncé de ce théorème, l'ensemble $C_b(K)$ est vide.

2.1. RÉDUCTION SUR b. S'il existe un plongement σ de K dans $\mathbb{R}$ tel que $\sigma(b) < 0$, il est immédiat que $C_b(K)$ est vide et le théorème est démontré dans ce cas. On peut donc supposer que b est totalement positif, autrement dit que pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(b) > 0$. Compte tenu de l'appendice 3 et de la deuxième inégalité de la condition (13), il existe une unité u de O_K telle que pour tout plongement σ de K dans $\mathbb{R}$ on ait $\sigma(bu^4) \geqslant 1$. Par ailleurs, les courbes C_b et C_{bu^4} sont K-isomorphes et si l'on remplace b par bu^4 les trois conditions intervenant dans l'énoncé du Théorème 3 ne changent pas. Quitte à remplacer b par bu^4, on peut donc supposer, ce que l'on fera dans toute la suite, que la condition suivante est satisfaite:

(15) pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(b) \geqslant 1$.

2.2. LA COURBE ELLIPTIQUE E_b. Afin de simplifier les notations, on notera dans la suite E_b la courbe affine d'équation de Weierstrass

$$y^2 = x^3 - bx. \tag{16}$$

Les invariants standard c_4, c_6 et Δ associés à cette équation sont (voir [10]):

$$c_4 = 2^4.3.b, \quad c_6 = 0 \quad \text{et} \quad \Delta = 2^6.b^3. \tag{17}$$

La courbe E_b a bonne réduction en toutes les places finies $v \in M_K^0$ pour lesquelles on a $v(2b) = 0$. Son invariant modulaire est 1728, il est entier, donc E_b a partout potentiellement bonne réduction.

LEMME 1. *Soit v une place finie de K telle que $v(b) > 0$. Alors, le modèle* (16) *est minimal en v et E_b a mauvaise réduction de type additif en v.*

DÉMONSTRATION: Posons $m = v(b)$ et $e = v(2)$. D'après la condition 1 du Théorème 3, on a $m = 1, 2$ ou 3. Cela entraîne l'assertion si $e = 0$. Supposons $e \geqslant 1$. D'après (17), on a

$$v(c_4) = 4e + m \quad \text{et} \quad v(\Delta) = 6e + 3m. \tag{18}$$

Supposons que le modèle (16) ne soit pas minimal en v, autrement dit qu'il ne soit pas minimal sur le complété K_v de K en v. Dans ce cas, il existe un élément $u \in K_v$ de valuation > 0 tel que

$$\frac{c_4}{u^4}, \quad \frac{c_6}{u^6} \ (= 0) \quad \text{et} \quad \frac{\Delta}{u^{12}},$$

appartiennent à l'anneau de valuation de K_v et soient les invariants standard associés à une courbe elliptique sur K_v. En notant encore v le prolongement de v à K_v, on déduit de (18) les inégalités

$$0 < v\left(\frac{c_4}{u^4}\right) < 4e \quad \text{et} \quad v\left(\frac{c_4}{u^4}\right) \not\equiv 0 \bmod 4.$$

Cela contredit le Théorème 2 de [4] et la remarque qui le suit. D'où le résultat.

Considérons une place finie v de K telle que $v(b) > 0$. Soient K_v le complété de K en v et k_v le corps résiduel. On déduit du Lemme 1 que la courbe sur k_v déduite de la courbe elliptique E_b par réduction possède un unique point singulier qui est $(0,0)$ (voir [7, p. 173]). On désigne par $E_b^0(K_v)$ le sous-groupe de $E_b(K_v)$ formé des points de réduction non singulière sur k_v.

Lemme 2. *Supposons $v(b) > 0$. Soit $P = (x,y)$ un point de $E_b(K_v)$. Alors, P appartient à $E_b^0(K_v)$ si et seulement si $v(x) \leqslant 0$.*

Démonstration: Le modèle (16) étant minimal sur K_v, la condition annoncée est clairement nécessaire, car si $v(x) > 0$ on a aussi $v(y) > 0$. Inversement, supposons $v(x) \leqslant 0$. Posons $x = \pi^n a$, où π est une uniformisante de K_v, $n \leqslant 0$ et $v(a) = 0$. Si $n = 0$, on a $v(y) \geqslant 0$ et P ne se réduit pas en $(0,0)$. Si $n < 0$, on a $2v(y) = 3v(x)$ et P se réduit en le point $[0,1,0]$ sur la courbe projective réduite $Y^2Z = X^3$, en particulier $P \in E_b^0(K_v)$. D'où le lemme.

Pour tout point $P = (x,y) \in E_b(K)$ à distance finie, on notera désormais

$$H_x(P) = \prod_{v \in M_K} \operatorname{Max}\left(1, |x|_v\right)^{n_v/n} \tag{19}$$

et

$$h_x(P) = \log H_x(P),$$

où, comme dans le paragraphe 1.1, n_v est le degré local en v. On pose $H_x(O) = 1$, où O est le point à l'infini de E_b.

2.3. Le sous-groupe Γ de $E_b(K)$. On va maintenant définir un sous-groupe Γ d'indice fini de $E_b(K)$. Considérons pour cela le sous-ensemble G de $E_b(K)$ formé des points qui appartiennent à $E_b^0(K_v)$ pour toute place finie $v \in M_K^0$ telle que $v(b) > 0$. D'après le Lemme 2, étant donné $P = (x,y) \in E_b(K)$, on a l'équivalence

$$P \in G \Longleftrightarrow v(x) \leqslant 0 \quad \text{pour toute place } v \in M_K^0 \text{ telle que } v(b) > 0. \tag{20}$$

C'est un sous-groupe d'indice fini de $E_b(K)$ car $E_b^0(K_v)$ est lui-même un sous-groupe d'indice fini de $E_b(K_v)$ ([7, p. 359]). Pour tout plongement $\sigma : K \to \mathbb{R}$, notons $E_{\sigma(b)}$ la courbe elliptique définie sur $\mathbb{R}$ d'équation

$$y^2 = x^3 - \sigma(b)x.$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Puisque les trois abscisses des points d'ordre 2 de $E_{\sigma(b)}$ sont réelles, l'ensemble $E_{\sigma(b)}(\mathbb{R})$ possède deux composantes connexes. On désigne par I_σ la composante connexe de l'élément neutre. Compte tenu du fait que l'on a $\sigma(b) > 0$, pour tout point $M = (x, y) \in E_{\sigma(b)}(\mathbb{R})$, on a l'équivalence (en prenant la racine carrée positive)

$$M \in I_\sigma \Longleftrightarrow x \geqslant \sqrt{\sigma(b)}. \tag{21}$$

Par ailleurs, pour tout $M \in E_{\sigma(b)}(\mathbb{R})$, le point $2M$ appartient à I_σ. On définit alors Γ comme étant le sous-ensemble de G formé des points $P \in G$ tels que $\sigma(P)$ appartienne à I_σ pour tout plongement $\sigma : K \to \mathbb{R}$. C'est un sous-groupe de G et d'après l'assertion précédente, il est d'indice 2 dans G. En particulier, Γ est un sous-groupe d'indice fini de $E_b(K)$.

2.4. HAUTEURS SUR Γ. Pour tout idéal $\mathscr{I}$ de O_K, on notera dans toute la suite $\mathrm{N}(\mathscr{I})$ la norme de K sur $\mathbb{Q}$ de $\mathscr{I}$.

LEMME 3. *Soit $Q = (x, y)$ un point de $E_b(K)$. Supposons que pour tout plongement $\sigma : K \to \mathbb{R}$, le point $\sigma(Q)$ appartienne à I_σ. On a l'égalité*

$$H_x(Q)^n = \prod_{\{\mathfrak{p}\ ;\ v_\mathfrak{p}(x)>0\}} \mathrm{N}(\mathfrak{p})^{v_\mathfrak{p}(x)},$$

le produit étant indexé par l'ensemble des idéaux premiers $\mathfrak{p}$ de O_K tels que $v_\mathfrak{p}(x) > 0$.

DÉMONSTRATION: D'après (19), on a

$$H_x(P)^n = \prod_{v \in M_K^0} \mathrm{Max}\big(1, |x|_v\big)^{n_v} \prod_{v \in M_K^\infty} \mathrm{Max}\big(1, |x|_v\big)^{n_v}.$$

Soit v une place finie. La formule (14) entraîne l'égalité

$$|x|_v^{n_v} = q_v^{-v(x)},$$

où q_v est le cardinal du corps résiduel de v. Si $\mathfrak{p}$ est l'idéal premier de O_K correspondant à v, on a donc

$$|x|_v = \mathrm{N}(\mathfrak{p})^{-v_\mathfrak{p}(x)}.$$

Il en résulte que l'on a

$$\prod_{v \in M_K^0} \mathrm{Max}\big(1, |x|_v\big)^{n_v} = \prod_{\{\mathfrak{p}\ ;\ v_\mathfrak{p}(x)<0\}} \mathrm{N}(\mathfrak{p})^{-v_\mathfrak{p}(x)}. \tag{22}$$

Par ailleurs, l'hypothèse faite et les conditions (21) et (15) entraînent que pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(x) \geqslant \sqrt{\sigma(b)} \geqslant 1$. Les degrés locaux n_v étant égaux à 1 pour les places infinies, on obtient

$$\prod_{v \in M_K^\infty} \mathrm{Max}\big(1, |x|_v\big)^{n_v} = \big|N_{K/\mathbb{Q}}(x)\big| = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{v_\mathfrak{p}(x)}. \tag{23}$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Les égalités (22) et (23) entraînent alors le lemme.

Considérons maintenant un point $P = (x, y) \in E_b(K)$ tel que $2P \neq O$. L'abscisse de $2P$ est donnée par l'égalité

$$x(2P) = \frac{(x^2+b)^2}{4x(x^2-b)}. \tag{24}$$

Pour tout idéal premier $\mathfrak{p}$ de O_K posons $\alpha(\mathfrak{p}) = v_{\mathfrak{p}}(x)$. Notons A l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $\alpha(\mathfrak{p}) > 0$ et B l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $\alpha(\mathfrak{p}) < 0$. Les décompositions des idéaux fractionnaires xO_K, $(x^2+b)O_K$ et $(x^2-b)O_K$ en produit d'idéaux premiers sont de la forme:

$$xO_K = \prod_{\mathfrak{p}\in A} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathfrak{p}^{\alpha(\mathfrak{p})}, \tag{25}$$

$$(x^2+b)O_K = \prod_{\mathfrak{p}\in B} \mathfrak{p}^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathfrak{q}^{\beta(\mathfrak{q})}, \tag{26}$$

$$(x^2-b)O_K = \prod_{\mathfrak{p}\in B} \mathfrak{p}^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}, \tag{27}$$

où pour tous idéaux premiers $\mathfrak{q}$ et $\mathfrak{r}$, on pose $\beta(\mathfrak{q}) = v_{\mathfrak{q}}(x^2+b)$ et $\gamma(\mathfrak{r}) = v_{\mathfrak{r}}(x^2-b)$. Démontrons le lemme suivant:

Lemme 4. *Supposons que P appartienne à G. Il existe un idéal I de O_K qui divise $8O_K$ tel que l'on ait*

$$H_x(2P)^n = \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}e} \mathrm{N}(\mathfrak{q})^{2\beta(\mathfrak{q})} \times \frac{1}{\mathrm{N}(I)}.$$

Démonstration: D'après l'égalité (24), on a

$$x(2P)O_K = \prod_{\mathfrak{p}\in B} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in A} \mathfrak{p}^{-\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathfrak{q}^{2\beta(\mathfrak{q})} \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{-\gamma(\mathfrak{r})}\ (4O_K)^{-1}. \tag{28}$$

Soit I le plus grand commun diviseur des deux idéaux entiers

$$\prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathfrak{q}^{2\beta(\mathfrak{q})} \quad \text{et} \quad \prod_{\mathfrak{p}\in A} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathfrak{p}^{-\alpha(\mathfrak{p})} \prod_{\{\mathfrak{r}\ :\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}\ (4O_K).$$

Le point $2P$ vérifie l'hypothèse faite dans l'énoncé du Lemme 3. L'égalité (28) et le Lemme 3 entraînent alors l'égalité

$$H_x(2P)^n = \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{2\beta(\mathfrak{q})} \times \frac{1}{\mathrm{N}(I)}.$$

Tout revient donc à prouver que

$$I \text{ divise } 8O_K. \tag{29}$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Considérons pour cela un idéal premier $\mathfrak{P}$ de O_K qui divise I. Puisque $\mathfrak{P}$ divise le produit des idéaux $\mathfrak{q}^{2\beta(\mathfrak{q})}$ où $\beta(\mathfrak{q}) > 0$, on déduit de (26) que

$$\mathfrak{P} \text{ ne divise pas } \prod_{\mathfrak{p}\in B} \mathfrak{p}^{-\alpha(\mathfrak{p})}.$$

Par suite, on a $v_{\mathfrak{P}}(x) \geqslant 0$. Il en résulte que

$$v_{\mathfrak{P}}(x) = 0. \tag{30}$$

En effet, dans le cas contraire, on aurait $v_{\mathfrak{P}}(x) > 0$ et $v_{\mathfrak{P}}(x^2 + b) > 0$, d'où $v_{\mathfrak{P}}(b) > 0$, ce qui, d'après le Lemme 2, contredit le fait que P soit dans G. On en déduit que

$$I \text{ divise } \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}\ (4O_K). \tag{31}$$

En particulier, on a l'inégalité

$$v_{\mathfrak{P}}\big(4(x^2 - b)\big) > 0. \tag{32}$$

Par ailleurs, on a

$$v_{\mathfrak{P}}(x^2 + b) > 0. \tag{33}$$

Les conditions (30), (32) et (33) entraînent alors que $\mathfrak{P}$ est l'un des idéaux premiers de O_K au-dessus de 2. Il reste à démontrer que l'on a, $v_{\mathfrak{P}}(I)$ étant l'exposant de $\mathfrak{P}$ dans I,

$$v_{\mathfrak{P}}(I) \leqslant 3v_{\mathfrak{P}}(2). \tag{34}$$

Supposons pour cela que l'on ait $v_{\mathfrak{P}}(I) \geqslant 3v_{\mathfrak{P}}(2) + 1$. D'après la condition (31) et le fait que I divise le produit des idéaux $\mathfrak{q}^{2\beta(\mathfrak{q})}$ où $\beta(\mathfrak{q}) > 0$, on a

$$2v_{\mathfrak{P}}(x^2 + b) \geqslant v_{\mathfrak{P}}(I) \quad \text{et} \quad v_{\mathfrak{P}}\big(4(x^2 - b)\big) \geqslant v_{\mathfrak{P}}(I).$$

On obtient alors

$$v_{\mathfrak{P}}(x^2 + b) \geqslant \frac{3v_{\mathfrak{P}}(2) + 1}{2} \quad \text{et} \quad v_{\mathfrak{P}}\big(4(x^2 - b)\big) \geqslant 3v_{\mathfrak{P}}(2) + 1,$$

ce qui conduit aux inégalités

$$v_{\mathfrak{P}}(x^2 + b) \geqslant v_{\mathfrak{P}}(2) + 1 \quad \text{et} \quad v_{\mathfrak{P}}(x^2 - b) \geqslant v_{\mathfrak{P}}(2) + 1.$$

On en déduit que $2v_{\mathfrak{P}}(x) \geqslant 1$ et la condition (30) implique alors une contradiction. Cela prouve l'inégalité (34), puis la condition (29). D'où le résultat.

2.5. COMPARAISON ENTRE LES HAUTEURS $\widehat{h}$ ET h_x SUR Γ. Notons $\widehat{h}$ la hauteur de Néron-Tate sur E_b. On a une égalité de la forme $2\widehat{h} = h_x + O(1)$ où $h_x = \log H_x$ (formules (19)). On va maintenant effectiviser cette égalité uniformément, c'est a dire indépendamment de b, sur le groupe Γ. Démontrons le résultat suivant:

PROPOSITION 3. *Soit P un point de Γ. On a*

$$\left|2\widehat{h}(P) - h_x(P)\right| \leqslant \log 2.$$

Prouvons pour cela l'énoncé ci-dessous:

LEMME 5. *On a $\left|h_x(2P) - 4h_x(P)\right| \leqslant 3\log 2$.*

DÉMONSTRATION: Vérifions d'abord que cette inégalité est vraie si $2P = O$. Tel est le cas si $P = O$, car alors $h_x(P) = h_x(2P) = 0$. Supposons $P \neq O$. Soit $a \in \overline{\mathbb{Q}}$ tel que $b = a^2$. On a alors $P = (0,0)$ ou bien $P = \left(\pm a, 0\right)$, cette dernière éventualité ne pouvant se produire que si a est dans K. Pour tout plongement $\sigma : K \to \mathbb{R}$, le point $\sigma(P)$ étant dans I_σ, on a $P \neq (0,0)$, d'où $P = \left(\pm a, 0\right)$. Par ailleurs, P appartient à G. D'après l'équivalence (20), l'élément a est donc une unité de O_K. On obtient $H_x(P) = \left|N_{K/\mathbb{Q}}(a)\right| = 1$, d'où $h_x(P) = 0$ et notre assertion (car $h_x(2P) = 0$).

Supposons désormais $2P \neq O$ et que les décompositions des idéaux fractionnaires xO_K et $(x^2 + b)O_K$ soient données par les formules (25) et (26).

Pour tout plongement $\sigma : K \to \mathbb{R}$, le point $\sigma(P)$ étant dans I_σ, on déduit de l'équivalence (21) que l'on a

$$\mathrm{N}_{K/\mathbb{Q}}(x^2 + b) = \prod_{\sigma} \left(\sigma(x^2) + \sigma(b)\right) \leqslant \mathrm{N}_{K/\mathbb{Q}}(2x^2).$$

Il en résulte que

$$\prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \leqslant 2^n \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})},$$

d'où l'inégalité

$$\prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \leqslant 2^n \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})}.$$

On déduit alors des Lemmes 3 et 4 que l'on a

$$H_x(2P)^n \leqslant 2^{2n} \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{4\alpha(\mathfrak{p})} = 2^{2n} H_x(P)^{4n}. \tag{35}$$

Par ailleurs, b étant totalement positif, on a

$$\mathrm{N}_{K/\mathbb{Q}}(x^2 + b) \geqslant \mathrm{N}_{K/\mathbb{Q}}(x^2).$$

D'après (26), on a donc

$$\prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \geqslant \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})},$$

autrement dit,

$$\prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \geqslant \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})}.$$

Puisque l'on a $\mathrm{N}(8O_K) = 8^n$, il résulte alors des Lemmes 3 et 4 l'inégalité

$$H_x(2P)^n \geqslant \frac{1}{8^n} H_x(P)^{4n}. \tag{36}$$

D'où le lemme en prenant les logarithmes des inégalités (35) et (36).

La Proposition 3 est une conséquence directe du Lemme 5 et du résultat qui suit (voir [7, p. 228-229]):

LEMME 6. *Soit S un sous-ensemble de $E_b(K)$ stable par multiplication par 2. Supposons qu'il existe une constante $c > 0$ telle que pour tout $Q \in S$ on ait l'inégalité $|h_x(2Q) - 4h_x(Q)| \leqslant c$. Alors, pour tout $Q \in S$, on a $|2\widehat{h}(Q) - h_x(Q)| \leqslant c/3$.*

DÉMONSTRATION: Rappelons que pour tout point $M \in E_b(K)$, on a (*loco citato*):

$$\widehat{h}(M) = \frac{1}{2} \lim_{n\to+\infty} \frac{h_x(2^n M)}{4^n}.$$

Considérons un point $Q \in S$. Pour tout entier $n \geqslant 1$ on a

$$\frac{1}{4^n} h_x(2^n Q) - h_x(Q) = \sum_{j=0}^{n-1} \left(\frac{1}{4^{j+1}} h_x(2^{j+1}Q) - \frac{1}{4^j} h_x(2^j Q) \right).$$

On en déduit l'inégalité

$$\left| \frac{1}{4^n} h_x(2^n Q) - h_x(Q) \right| \leqslant \sum_{j=0}^{n-1} \frac{1}{4^{j+1}} \left| h_x(2^{j+1}Q) - 4h_x(2^j Q) \right|.$$

Par hypothèse, $2^j Q$ appartient à S. Il en résulte que l'on a

$$\left| \frac{1}{4^n} h_x(2^n Q) - h_x(Q) \right| \leqslant c \sum_{j=0}^{n-1} \frac{1}{4^{j+1}}.$$

On obtient ainsi

$$\lim_{n\to+\infty} \left| \frac{1}{4^n} h_x(2^n Q) - h_x(Q) \right| \leqslant \frac{c}{3},$$

ce qui entraîne le lemme.

Cela termine la démonstration de la Proposition 3.

2.6. HAUTEURS SUR LES IMAGES DE $C_b(K)$ DANS $E_b(K)$. Rappelons que l'on dispose de deux morphismes $\phi_b : C_b \to E_b$ et $\psi_b : C_b \to E_b$ définis sur K par les égalités

$$\phi_b([x,y,z]) = [-x^2z, xy^2, z^3]$$

et

$$\psi_b([x,y,z]) = [-y^2z, yx^2, z^3].$$

Considérons dans tout ce paragraphe un point $Q = [x,y,z] \in C_b(K)$. On a $z \neq 0$, car sinon -1 est une puissance quatrième dans K, ce qui contredit le fait que K soit totalement réel. On peut donc supposer que l'on a $z = 1$. On a ainsi l'égalité

$$x^4 + y^4 = b. \tag{37}$$

Posons $P_1 = \phi_b(Q)$ et $P_2 = \psi_b(Q)$ dans $E_b(K)$. On a dans le modèle affine (16)

$$P_1 = (-x^2, xy^2) \quad \text{et} \quad P_2 = (-y^2, yx^2). \tag{38}$$

LEMME 7. *Les points P_1 et P_2 appartiennent à G.*

DÉMONSTRATION: Soit v une place finie de K telle que $v(b) > 0$. D'après l'équivalence (20) et les égalités (38), il s'agit de démontrer que l'on a $v(x) \leqslant 0$. Supposons $v(x) > 0$. L'égalité (37) entraîne alors $v(y) > 0$ puis $v(b) \geqslant 4$, ce qui contredit la condition 1 de l'énoncé du Théorème 3. D'où notre assertion et le résultat.

PROPOSITION 4. *On a les inégalités*

$$\left|h_x(2P_1) - h_x(2P_2)\right| \leqslant 5\log 2 \qquad \text{et} \qquad \left|\widehat{h}(P_1) - \widehat{h}(P_2)\right| \leqslant \frac{7}{8}\log 2.$$

DÉMONSTRATION: (1) Prouvons la première inégalité. Elle est vraie si $xy = 0$, car dans ce cas, compte tenu de l'égalité (37), les points P_1 et P_2 sont d'ordre 2 dans $E_b(K)$. Supposons désormais xy non nul. Dans ce cas, P_1 et P_2 ne sont pas d'ordre 2 et les abscisses de $2P_1$ et $2P_2$ sont données par les égalités

$$x(2P_1) = \frac{(x^4+b)^2}{4x^2(b-x^4)} \quad \text{et} \quad x(2P_2) = \frac{(y^4+b)^2}{4y^2(b-y^4)}. \tag{39}$$

Pour tout idéal premier $\mathfrak{p}$ de O_K, posons, comme précédemment, $\alpha_\mathfrak{p} = v_\mathfrak{p}(x)$ et notons A l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $v_\mathfrak{p}(x) > 0$ et B l'ensemble des idéaux premiers tels que $v_\mathfrak{p}(x) < 0$. Les décompositions des idéaux fractionnaires xO_K et $(x^4+b)O_K$ en produit d'idéaux premiers sont de la forme:

$$xO_K = \prod_{\mathfrak{p}\in A} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathfrak{p}^{\alpha(\mathfrak{p})},$$

$$(x^4+b)O_K = \prod_{\mathfrak{p}\in B} \mathfrak{p}^{4\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathfrak{q}^{\beta(\mathfrak{q})}. \tag{40}$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Par ailleurs, pour tout idéal premier $\mathfrak{p}$ de O_K, compte tenu de (37), on a $v_\mathfrak{p}(x) < 0$ si et seulement si $v_\mathfrak{p}(y) < 0$ et dans ce cas $v_\mathfrak{p}(x) = v_\mathfrak{p}(y)$. Il en résulte que la décomposition de $(y^4 + b)O_K$ en produit d'idéaux premiers est de la forme suivante:

$$(41) \qquad (y^4 + b)O_K = \prod_{\mathfrak{p} \in B} \mathfrak{p}^{4\alpha(\mathfrak{p})} \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}.$$

D'après les Lemmes 4 et 7 et les égalités (38), il existe ainsi deux idéaux J_1 et J_2 de O_K qui divisent $8O_K$ tels que l'on ait

$$H_x(2P_1)^n = \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{2\beta(\mathfrak{q})} \times \frac{1}{\mathrm{N}(J_1)},$$

$$H_x(2P_2)^n = \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathrm{N}(\mathfrak{r})^{2\gamma(\mathfrak{r})} \times \frac{1}{\mathrm{N}(J_2)}.$$

D'après (40) et (41) on obtient donc l'égalité

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \frac{\mathrm{N}_{K/\mathbb{Q}}(x^4 + b)^2}{\mathrm{N}_{K/\mathbb{Q}}(y^4 + b)^2} \times \frac{N(J_2)}{N(J_1)}.$$

L'égalité (37) entraîne alors

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \frac{\mathrm{N}_{K/\mathbb{Q}}(2x^4 + y^4)^2}{\mathrm{N}_{K/\mathbb{Q}}(2y^4 + x^4)^2} \times \frac{N(J_2)}{N(J_1)}.$$

Posons

$$t = \frac{x^4}{y^4}.$$

On obtient

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \frac{\mathrm{N}_{K/\mathbb{Q}}(2t + 1)^2}{\mathrm{N}_{K/\mathbb{Q}}(t + 2)^2} \times \frac{N(J_2)}{N(J_1)},$$

ce qui conduit à

$$(42) \qquad \frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \mathrm{N}_{K/\mathbb{Q}}\Big(2 - \frac{3}{t+2}\Big)^2 \times \frac{N(J_2)}{N(J_1)}.$$

Pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(t) \geqslant 0$, d'où il résulte que l'on a

$$\frac{1}{2} \leqslant 2 - \frac{3}{\sigma(t) + 2} \leqslant 2.$$

On en déduit les inégalités

$$(43) \qquad \frac{1}{2^n} \leqslant \mathrm{N}_{K/\mathbb{Q}}\Big(2 - \frac{3}{t+2}\Big) \leqslant 2^n.$$

On déduit alors de (42) et (43) que l'on a

$$\frac{1}{2^{2n}} \times \frac{1}{8^n} = \frac{1}{2^{5n}} \leqslant \frac{H_x(2P_1)^n}{H_x(2P_2)^n} \leqslant 2^{2n} \times 8^n = 2^{5n}.$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

D'où la première inégalité de la proposition.

(2) En ce qui concerne la deuxième inégalité, on a

$$|\widehat{h}(P_1) - \widehat{h}(P_2)| = \frac{1}{4}|\widehat{h}(2P_1) - \widehat{h}(2P_2)|.$$

Il en résulte que

$$|\widehat{h}(P_1) - \widehat{h}(P_2)| \leqslant \frac{1}{4}\left(|\widehat{h}(2P_1) - \frac{1}{2}h_x(2P_1)| + \frac{1}{2}|h_x(2P_1) - h_x(2P_2)| + \left|\frac{1}{2}h_x(2P_2) - \widehat{h}(2P_2)\right|\right).$$

Par ailleurs, on déduit du Lemme 7 que $2P_1$ et $2P_2$ appartiennent au sous-groupe Γ de $E_b(K)$. L'inégalité déjà prouvée et la Proposition 3 entraînent alors le résultat. D'où la Proposition.

2.7. Fin de la démonstration du Théorème 3. On suppose que l'ensemble $C_b(K)$ est non vide. Il s'agit d'obtenir une contradiction. Comme on l'a constaté au début du paragraphe 2.6, il existe alors $Q = (x, y) \in C_b(K)$ dans l'ouvert affine $z = 1$, l'égalité (37) étant ainsi satisfaite. On pose comme précédemment

$$P_1 = \phi_b(Q) \quad \text{et} \quad P_2 = \psi_b(Q).$$

Vérifions que l'on a

$$P_1 + P_2 \neq O \quad \text{et} \quad P_1 - P_2 \neq O. \tag{44}$$

Supposons $P_1 = \pm P_2$. D'après (38), on a $P_1 = (-x^2, xy^2)$ et $P_2 = (-y^2, yx^2)$, d'où $x^2 = y^2$, puis $b = 2x^4$. Soit v une place finie de K telle que $v(x) \neq 0$. On a $v(2) > 0$: en effet, dans le cas contraire, on aurait $v(b) = 4v(x) > 0$ (car $b \in O_K$) ce qui contredit la condition 1 de l'énoncé du Théorème 3. Par suite, on a

$$xO_K = \prod_{\mathfrak{p}|2} \mathfrak{p}^{\alpha(\mathfrak{p})},$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de O_K au-dessus de 2 et où $\alpha(\mathfrak{p}) \in \mathbb{Z}$. Pour la même raison, l'égalité $b = 2x^4$ entraîne $\alpha(\mathfrak{p}) \leqslant 0$ pour tout $\mathfrak{p}$. On en déduit que

$$\mathrm{N}_{K/\mathbb{Q}}(b) \leqslant 2^n,$$

ce qui contredit l'inégalité $\mathrm{N}_{K/\mathbb{Q}}(b) \geqslant 2^{(11n)/2}$ intervenant dans la condition 3 de l'énoncé du théorème. D'où l'assertion (44).

On désigne par R un point de $E_b(K)$ vérifiant la condition suivante: si $E_b(K)$ est de rang 0 on a $R = O$, et si $E_b(K)$ est de rang 1 alors R est un générateur de $E_b(K)$ modulo

son sous-groupe de torsion. Il existe ainsi des entiers m, n et des points de torsion T_1, T_2 de $E_b(K)$ tels que l'on ait

$$P_1 = mR + T_1 \quad \text{et} \quad P_2 = nR + T_2.$$

Soit N un multiple des ordres de T_1 et T_2. On a $NP_1 = NmR$ et $NP_2 = NnR$. On en déduit les égalités

$$\widehat{h}(P_1) = m^2\widehat{h}(R) \quad \text{et} \quad \widehat{h}(P_2) = n^2\widehat{h}(R). \tag{45}$$

De même, on a

$$\widehat{h}(P_1 + P_2) = (m+n)^2\widehat{h}(R) \quad \text{et} \quad \widehat{h}(P_1 - P_2) = (m-n)^2\widehat{h}(R).$$

On en déduit que

$$\widehat{h}(P_1 + P_2) \leqslant |m^2 - n^2|\widehat{h}(R) \quad \text{si} \quad mn \leqslant 0, \tag{46}$$

$$\widehat{h}(P_1 - P_2) \leqslant |m^2 - n^2|\widehat{h}(R) \quad \text{si} \quad mn \geqslant 0. \tag{47}$$

Considérons alors un plongement $\sigma : K \to \mathbb{R}$. D'après (38), on a

$$\sigma\big(x(P_1)\big) \leqslant 0 \quad \text{et} \quad \sigma\big(x(P_2)\big) \leqslant 0,$$

par suite $\sigma(P_1)$ et $\sigma(P_2)$ n'appartiennent pas à la composante neutre I_σ. Par définition de la loi de groupe sur $E_{\sigma(b)}$, les points $\sigma(P_1+P_2)$ et $\sigma(P_1-P_2)$ sont donc dans I_σ. D'après le Lemme 7, il en résulte que

$$P_1 + P_2 \in \Gamma \quad \text{et} \quad P_1 - P_2 \in \Gamma.$$

D'après la Proposition 3, on obtient alors

$$\begin{aligned} h_x(P_1 + P_2) &\leqslant 2\widehat{h}(P_1 + P_2) + \log 2 \\ h_x(P_1 - P_2) &\leqslant 2\widehat{h}(P_1 - P_2) + \log 2. \end{aligned} \tag{48}$$

Compte tenu des conditions (46), (47) et (48), on a donc les inégalités

$$\begin{aligned} h_x(P_1 + P_2) &\leqslant 2|m^2 - n^2|\widehat{h}(R) + \log 2 \quad \text{si} \quad mn \leqslant 0, \\ h_x(P_1 - P_2) &\leqslant 2|m^2 - n^2|\widehat{h}(R) + \log 2 \quad \text{si} \quad mn \geqslant 0. \end{aligned}$$

Supposons $mn \leqslant 0$. Dans ce cas, les égalités (45) entraînent

$$h_x(P_1 + P_2) \leqslant 2\big|\widehat{h}(P_1) - \widehat{h}(P_2)\big| + \log 2.$$

D'après la Proposition 4, on en déduit que

$$h_x(P_1 + P_2) \leqslant \frac{11}{4}\log 2. \tag{49}$$

De même, si $mn \geqslant 0$, on obtient

$$h_x(P_1 - P_2) \leqslant \frac{11}{4}\log 2. \tag{50}$$

Démontrons maintenant que l'on a

$$nh_x(P_1 + P_2) \geqslant \frac{\log \mathrm{N}_{K/\mathbb{Q}}(b)}{2} \quad \text{et} \quad nh_x(P_1 - P_2) \geqslant \frac{\log \mathrm{N}_{K/\mathbb{Q}}(b)}{2}. \tag{51}$$

D'après (44), le point $P_1 + P_2$ est non nul. Posons $P_1 + P_2 = (u, w) \in E_b(K)$. On a

$$H_x(P_1 + P_2)^n = \prod_{v \in M_K} \mathrm{Max}\big(1, |u|_v\big)^{n_v} \geqslant \prod_{v \in M_K^\infty} \mathrm{Max}\big(1, |u|_v\big).$$

Par ailleurs, puisque $P_1 + P_2$ appartient à Γ, on a $\big|\sigma(u)\big| = \sigma(u) \geqslant \sqrt{\sigma(b)}$ pour tout plongement $\sigma : K \to \mathbb{R}$. On a ainsi

$$H_x(P_1 + P_2)^n \geqslant \prod_{\sigma} \mathrm{Max}\Big(1, \sqrt{\sigma(b)}\Big).$$

D'après la condition (15), pour tout σ on a $\sigma(b) \geqslant 1$. On en déduit que

$$H_x(P_1 + P_2)^n \geqslant \sqrt{\mathrm{N}_{K/\mathbb{Q}}(b)},$$

d'où la première inégalité de (51). La démonstration de la deuxième inégalité de (51) est la même. Les conditions (49) et (50) impliquent alors

$$\log \mathrm{N}_{K/\mathbb{Q}}(b) \leqslant \frac{11n}{2}\log 2,$$

d'où

$$\mathrm{N}_{K/\mathbb{Q}}(b) \leqslant 2^{(11n)/2}.$$

La première inégalité de (13) conduit alors à une contradiction.

Cela termine la démonstration du Théorème 3.

Appendice 1 - Exemple d'effectivité du théorème des zéros de Hilbert

On est confronté dans la démonstration de la Proposition 1 au problème de l'effectivité du théorème des zéros de Hilbert dans un cas particulier. Considérons trois indéterminées X, Y et Z. Soit I l'idéal homogène de l'anneau $\mathbb{C}[X, Y, Z]$ engendré par les polynômes F, G et H suivants:

$$F = X^4 + Y^4 - Z^4, \quad G = (X^2 + XY + Y^2)^2 \quad \text{et} \quad H = (X + Y)^2 Z^2.$$

Soit $V_p(I)$ l'ensemble algébrique projectif de $\mathbb{P}^2$ associé à I. Vérifions que $V_p(I)$ est vide. Supposons qu'il existe un point $[x, y, z] \in V_p(I)$. On a $(x+y)z = 0$. Si $z = 0$, alors $xy \neq 0$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

et il existe $\alpha \in \mathbb{C}$ tel que $x = \alpha y$ avec $\alpha^4 = -1$. L'égalité $x^2 + xy + y^2 = 0$ conduit alors à $1 + \alpha + \alpha^2 = 0$, d'où $\alpha^3 = 1$ et une contradiction. Si $x + y = 0$, l'égalité $x^2 + xy + y^2 = 0$ entraîne $x = y = 0$, d'où de nouveau une contradiction et notre assertion. D'après le théorème des zéros, il existe donc un entier $n \geqslant 1$ tel que les monômes X^n, Y^n et Z^n appartiennent à I. Il s'agit ici d'effectiviser cette condition. On a l'énoncé suivant:

PROPOSITION. *L'entier $n = 12$ convient. Posons*

$$\begin{aligned} P &= 3X^8 + 4Y^2X^6 + 4Y^4X^4 + 2Y^6X^2 + Y^8, \\ Q &= -2X^8 + 4YX^7 - 6Y^2X^6 + 4Y^3X^5 + (10Z^4 - 3Y^4)X^4 + 2Y^5X^3 \\ &\qquad -3Y^6X^2 + 2Y^7X - Y^8 + 4Z^4Y^4, \\ R &= -7Z^2X^6 - 6Z^2YX^5 - 7Z^2Y^2X^4 - 3Z^2Y^4X^2 - 2Z^2Y^5X - 3Z^2Y^6. \end{aligned}$$

On a les égalités

$$Z^6 = -Z^2F + 2Z^2G - (X+Y)^2H, \tag{1}$$

$$X^{12} = PF + QG + RH \quad \text{et} \quad Y^{12} = \tilde{P}F + \tilde{Q}G + \tilde{R}H, \tag{2}$$

où $\tilde{P}(X,Y,Z) = P(Y,X,Z)$, $\tilde{Q}(X,Y,Z) = Q(Y,X,Z)$ et $\tilde{R}(X,Y,Z) = R(Y,X,Z)$.

DÉMONSTRATION: Il est immédiat de vérifier les égalités annoncées à l'aide d'un ordinateur. On est en fait parvenu à ce résultat en partant de l'égalité

$$Z^4 + (X+Y)^4 = 2G - F. \tag{3}$$

L'égalité (1) en résulte. Par ailleurs, on déduit de (3) les deux égalités

$$\begin{aligned} G &= Z^4 + F + 2XY(X+Y)^2 - (XY)^2, \\ (XY)^2(X+Y)^4 &= -(XY)^2F + (2X^2Y^2 - Z^4)G + Z^2(X^2+Y^2)H. \end{aligned}$$

Elles entraînent que $(XY)^4$ appartient à I, puis que

$$\begin{aligned} &(XY)^4 = SF + TG + UH, \\ \text{avec} \quad &S = -(X^2+Y^2)^2, \quad T = X^4 - 2YX^3 + 3Y^2X^2 - 2Y^3X + Y^4 - 4Z^4, \\ &U = 3(XZ)^2 + 2XYZ^2 + 3(YZ)^2. \end{aligned}$$

En considérant alors l'égalité

$$X^8 + Y^8 = Z^8 + F^2 + 2Z^4F - 2(XY)^4,$$

et en multipliant ses deux membres par X^4 (respectivement Y^4) on obtient la première (respectivement la deuxième) égalité de (2).

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

Appendice 2 - Torsion galoisienne

L'objectif de cet appendice est de rappeler un résultat de Silverman concernant les tordues galoisiennes de courbes que l'on utilise dans la démonstration du Théorème 1 (voir [**6**]). Les courbes intervenant ci-dessous sont implicitement supposées projectives et lisses et plongées dans un même espace projectif $\mathbb{P}^n$. Tous les corps considérés sont par ailleurs contenus dans $\overline{\mathbb{Q}}$.

Considérons un corps de nombres K et une courbe $\mathscr{C}$ définie sur K. Soit $\mathscr{C}'$ une courbe définie sur K isomorphe à $\mathscr{C}$ sur une extension finie L de K. On suppose que L est *minimale* au sens où si M est un sous-corps strict de L, les courbes $\mathscr{C}$ et $\mathscr{C}'$ ne sont pas isomorphes sur M. Notons:

(a) G_K le groupe de Galois de $\overline{\mathbb{Q}}$ sur K.

(b) d le degré de L sur K.

(c) δ_K le nombre de places archimédiennes de K.

(d) $D_{L/K}$ le discriminant relatif de l'extension L/K.

(e) $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}$ la hauteur absolue logarithmique ([**7**, p. 215]); elle est définie par une formule analogue à celle si $n = 2$ (paragraphe 1.2).

Soit $f : \mathscr{C}' \to \mathscr{C}$ un isomorphisme défini sur L de $\mathscr{C}'$ sur $\mathscr{C}$. Pour tout $\sigma \in G_K$, on pose

$$\xi(\sigma) = {}^{\sigma}f \circ f^{-1} \in \mathrm{Aut}(\mathscr{C}).$$

Théorème. *Soit Q un point de $f\big(\mathscr{C}'(K)\big)$. On est dans l'un des cas suivants:*

(1) *il existe $\sigma \in G_K$ tel que $\xi(\sigma)$ ne soit pas l'identité de $\mathscr{C}$ et que $Q = \xi(\sigma)(Q)$.*

(2) *On a l'inégalité*

$$\log \mathrm{N}_{K/\mathbb{Q}} D_{L/K} \leqslant \Big(2(d-1)h(Q) + \delta_K \log d\Big)d. \tag{1}$$

Démonstration: On prouve d'abord le lemme suivant.

Lemme. *L'ensemble $f\big(\mathscr{C}'(K)\big)$ est formé des points $A \in \mathscr{C}(L)$ tels que, pour tout σ dans G_K, on ait ${}^{\sigma}A = \xi(\sigma)(A)$.*

Démonstration: Pour tout point $P \in \mathscr{C}'\big(\overline{\mathbb{Q}}\big)$ et tout $\sigma \in G_K$, on a

$${}^{\sigma}\big(f(P)\big) = \xi(\sigma)\big(f({}^{\sigma}P)\big). \tag{2}$$

Cela entraîne que $f\big(\mathscr{C}'(K)\big)$ satisfait la condition du lemme. Inversement, soit $A \in \mathscr{C}(L)$ tel que, pour tout σ dans G_K, on ait ${}^{\sigma}A = \xi(\sigma)(A)$. Posons $P = f^{-1}(A)$. D'après (2), on a les égalités

$$\xi(\sigma)\big(f({}^{\sigma}P)\big) = {}^{\sigma}A = \xi(\sigma)(A) = \xi(\sigma)\big(f(P)\big).$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

On en déduit que $f({}^{\sigma}P) = f(P)$, puis que $P = {}^{\sigma}P$. Il en résulte que P appartient à $\mathscr{C}'(K)$, autrement dit que A est dans $f\big(\mathscr{C}'(K)\big)$. D'où le lemme.

Le théorème se déduit comme suit. Soit $K(Q)$ le sous-corps de $\overline{\mathbb{Q}}$ engendré par K et les coordonnées de Q dans $\mathbb{P}^n\big(\overline{\mathbb{Q}}\big)$. On a l'inclusion

$$K(Q) \subseteq L. \tag{3}$$

Supposons que la condition 1 du théorème ne soit pas réalisée. Soit σ un élément de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/K(Q)\big)$. On a ${}^{\sigma}Q = Q$ et on déduit du lemme l'égalité

$$Q = \xi(\sigma)(Q).$$

D'après l'hypothèse faite, $\xi(\sigma)$ est donc l'automorphisme identité de $\mathscr{C}$, autrement dit f est définie sur $K(Q)$. Les courbes $\mathscr{C}$ et $\mathscr{C}'$ sont donc isomorphes sur $K(Q)$. D'après l'inclusion (3) et le caractère minimal de L, on a donc $L = K(Q)$. Le Théorème 2 de [**6**] entraîne alors directement l'inégalité (1). D'où le résultat.

Appendice 3 - Sur les entiers totalement positifs d'un corps totalement réel

Soit K un corps de nombres totalement réel de degré n sur $\mathbb{Q}$, d'anneau d'entiers O_K. Soient $\sigma_1, \ldots, \sigma_n$ les n plongements de K dans $\mathbb{R}$. Pour tout $x \in O_K$ on note $\mathrm{N}_{K/\mathbb{Q}}(x)$ sa norme de K sur $\mathbb{Q}$ et $H(x)$ la hauteur de x relative à K. On a

$$H(x) = \prod_{i=1}^{n} \mathrm{Max}\Big(1, \big|\sigma_i(x)\big|\Big). \tag{1}$$

On utilise dans la démonstration du Théorème 3 le résultat ci-dessous concernant les entiers totalement positifs de K.

Proposition. *Soit $(u_1, \ldots, u_{n-1})$ un système d'unités fondamentales de O_K. Soit b un élément de O_K tel que l'on ait $\sigma_j(b) > 0$ pour tout $j = 1, \ldots, n$. Supposons que b vérifie la condition suivante:*

$$\mathrm{N}_{K/\mathbb{Q}}(b) \geqslant \left(\prod_{k=1}^{n-1} H(u_k)\right)^4. \tag{2}$$

Alors, il existe une unité u de O_K telle que l'on ait

$$\sigma_j(bu^4) \geqslant 1 \quad \textit{pour} \quad j = 1, \ldots, n.$$

Démonstration: Soit $L : K^* \to \mathbb{R}^n$ le plongement logarithmique de K^*, c'est a dire l'homomorphisme de groupes défini pour tout $x \in K^*$ par

$$L(x) = \Big(\log\Big(\big|\sigma_1(x)\big|\Big), \ldots, \log\Big(\big|\sigma_n(x)\big|\Big)\Big).$$

L'image par L du groupe des unités de O_K est un réseau Λ de l'hyperplan V de $\mathbb{R}^n$ d'équation $x_1 + \cdots + x_n = 0$. Posons

$$e_k = L(u_k) \quad \text{pour} \quad k = 1, \ldots, n-1.$$

Le système $(e_1, \ldots, e_{n-1})$ est une base de Λ sur $\mathbb{Z}$ donc une base de V sur $\mathbb{R}$. Posons par ailleurs

$$\beta = L(b), \quad \beta = (\beta_1, \ldots, \beta_n) \quad \text{et} \quad S = \beta_1 + \cdots + \beta_n.$$

Puisque b est totalement positif, on a donc

$$\beta_j = \log\bigl(\sigma_j(b)\bigr) \quad \text{pour} \quad j = 1, \ldots, n. \tag{3}$$

Munissons $\mathbb{R}^n$ de la norme définie pour tout $(x_1, \ldots, x_n) \in \mathbb{R}^n$ par

$$\bigl\|(x_1, \ldots, x_n)\bigr\| = \sum_{h=1}^{n} |x_h|.$$

Vérifions que l'on a

$$S \geqslant 2 \sum_{k=1}^{n-1} \|e_k\|. \tag{4}$$

Considérons pour cela une unité a de O_K. Posons

$$P = \prod_i |\sigma_i(a)| \quad \text{et} \quad P' = \prod_j |\sigma_j(a)|,$$

où i parcourt l'ensemble des indices pour lesquels $|\sigma_i(a)| \geqslant 1$ et j parcourt l'ensemble des indices pour lesquels $|\sigma_j(a)| < 1$. On a $PP' = 1$. Il en résulte que

$$\sum_{h=1}^{n} \Bigl|\log\bigl(|\sigma_h(a)|\bigr)\Bigr| = \sum_i \log\Bigl(\bigl|\sigma_h(a)\bigr|\Bigr) - \sum_j \log\Bigl(\bigl|\sigma_h(a)\bigr|\Bigr) = \log(P) - \log(P') = 2\log(P).$$

Par ailleurs, d'après la formule (1), on a $H(a) = P$. D'après le calcul précédent, on a donc

$$\bigl\|L(a)\bigr\| = 2\log\bigl(H(a)\bigr).$$

L'inégalité (2) se traduit alors, en prenant les logarithmes, par la condition (4).

Soit M la maille du réseau Λ formée des combinaisons linéaires

$$\sum_{k=1}^{n-1} x_k e_k,$$

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

où les coefficients x_k décrivent l'intervalle $[-1/2, 1/2]$. Pour tout $i = 1, \dots, n$, soit $(e_k)_i$ la i-ème coordonnée de e_k dans la base canonique de $\mathbb{R}^n$. Pour tout $z = (z_1, \dots, z_n) \in M$, on a les inégalités

$$2|z_i| \leqslant \sum_{k=1}^{n-1} |(e_k)_i| := \ell_i. \tag{5}$$

Pour tout $i = 1, \dots, n$, le réseau Λ n'étant pas contenu dans l'hyperplan de $\mathbb{R}^n$ d'équation $x_i = 0$, on a $\ell_i > 0$. Posons alors

$$w_i = \frac{\ell_i}{\ell_1 + \cdots + \ell_n} \quad \text{et} \quad w = (w_1, \dots, w_n) \in \mathbb{R}^n.$$

Considérons le vecteur

$$y = \frac{1}{4}(Sw - \beta).$$

Par définition, y appartient à V. Il existe donc un élément $\lambda = (\lambda_1, \dots, \lambda_n) \in \Lambda$ tel que $y - \lambda$ soit dans M. On déduit alors de (5) que l'on a

$$\beta_i + 4\lambda_i \geqslant Sw_i - 2\ell_i \quad \text{pour} \quad i = 1, \dots, n. \tag{6}$$

Il existe des entiers $t_k \in \mathbb{Z}$ tels que l'on ait

$$\lambda = \sum_{k=1}^{n-1} t_k e_k.$$

Posons

$$u = \prod_{k=1}^{n-1} u_k^{t_k}.$$

Vérifions que l'unité u de O_K satisfait la conclusion de la proposition. On a $L(u) = \lambda$, d'où $\lambda_i = \log\big(|\sigma_i(u)|\big)$. Compte tenu de (3), les inégalités (6) s'écrivent donc

$$\log\big(\sigma_i(b)\big) + 4\log\Big(\big|\sigma_i(u)\big|\Big) \geqslant Sw_i - 2\ell_i,$$

autrement dit,

$$\sigma_i(bu^4) \geqslant \exp\big(Sw_i - 2\ell_i\big) \quad \text{pour} \quad i = 1, \dots, n. \tag{7}$$

Par ailleurs, on a

$$\ell_1 + \cdots + \ell_n = \sum_{k=1}^{n-1} \sum_{i=1}^{n} |(e_k)_i| = \sum_{k=1}^{n-1} \|e_k\|.$$

Il résulte alors de la condition (4) que l'on a

$$S \geqslant 2\,\mathrm{Max}\Big(\frac{\ell_1}{w_1}, \dots, \frac{\ell_n}{w_n}\Big).$$

D'après (7), on obtient ainsi que $\sigma_i(bu^4) \geqslant 1$ pour tout $i = 1, \dots, n$. D'où la proposition.

https://doi.org/10.1017/S0004972700039009 Published online by Cambridge University Press

References

[1] J.E. Cremona, M. Prickett et S. Siksek, 'Height difference bounds for elliptic curves over number fields', *J. Number Theory* **116** (2006), 42-68.

[2] V.A. Dem'janenko, 'The Indeterminate Equations $x^6 + y^6 = az^2$, $x^6 + y^6 = az^3$, $x^4 + y^4 = az^4$', *Amer. Math. Soc. Transl.* **119** (1983), 27–34.

[3] G. Grigorov et J. Rizov, 'Heights on elliptic curves and the diophantine equation $x^4 + y^4 = cz^4$', (preprint), *Sophia University* (1998).

[4] A. Kraus, 'Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique', *Acta Arith.* **54** (1989), 75–80.

[5] S. Siksek, 'Infinite descent on elliptic curves', *Rocky Mountain J. Math.* **25** (1995), 1501–1538.

[6] J.H. Silverman, 'Lower bounds for height functions', *Duke Math. J.* **51** (1984), 395–403.

[7] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106** (Springer–Verlag, New York, 1986).

[8] J.H. Silverman, Rational points on certain families of curves of genus at least 2, *Proc. London Math. Soc.* **55** (1987), 465–481.

[9] D. Simon, 'Programme de calcul du rang des courbes elliptiques dans les corps de nombres, disponible à l'adresse', `http://www.math.unicaen.fr/~simon/`.

[10] J. Tate, 'Algorithm for determining the type of a singular fiber in an elliptic pencil, dans Modular Functions of One Variable IV', *Lecture Notes in Math.* **476** (1975), 33–52.

App. 231
9 rue de Sèvres
92100 Boulogne
France
e-mail: elie.cali@wanadoo.fr

Université Pierre et Marie Curie - Paris 6
Institut de Mathématiques
UMR 7586 du CNRS
175 rue du Chevaleret
75013 Paris
France
e-mail: kraus@math.jussieu.fr