SCIREA Journal of Mathematics

http://www.scirea.org/journal/Mathematics

September 18, 2023

Volume 8, Issue 4, August 2023

https://doi.org/10.54647/mathematics110421

Points algébriques sur une courbe hyperelliptique de Nils Bruin

El Hadji SOW, Moussa FALL, Oumar SALL

Laboratoire de Mathématiques et Applications (L.M.A.) Université Assane SECK Ziguinchor, Senegal

Email: elpythasow@yahoo.fr(EL Hadji SOW), moussafalls@yahoo.fr (Moussa FALL), osall@univ-zig.sn (Oumar SALL)

Abstract : We give the set of algebraic points of degree ≤ 5 over $\mathbb{Q}$ on the hyperelliptic curve $C: y^2 = 6x(x^4 + 3)$. This result extends a previous result of Bruin of who described in [1] the set of $\mathbb{Q}$-rational points on this curve.

Keywords: Degree of algebraic points - Rational points - Algebraic extensions - Jacobian.

I. INTRODUCTION

Soit C une courbe algébrique lisse de genre $g \geq 2$ définie sur un corps de nombres K.

L'ensemble des points algébriques sur C définis sur K est noté $C(K)$ et $\bigcup_{[K:\mathbb{Q}]\leq d} C(K)$ l'ensemble des points algébriques sur C à coordonnées dans K de degrés au-plus d sur $\mathbb{Q}$. Le degré d'un point algébrique R sur $\mathbb{Q}$ est le degré de son corps de définition sur $\mathbb{Q}$ ie $\deg(R) = [\mathbb{Q}(R): \mathbb{Q}]$.

Nous nous proposons d'étudier en détail les points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur la courbe C d'équation affine $y^2 = 6x(x^4 + 3)$.

Notons $P = (0, 0)$ et ∞ le point à l'infini, les points algébriques de degré 1 sur la même courbe C décrit par Bruin dans [1] .

En utilisant le théorème d'Abel Jacobi et l'étude des systèmes linéaires sur la courbe C, nous étendons ce résultat en donnant une description des points algébriques de degrés au-plus 5 sur $\mathbb{Q}$ sur C. Notre résultat principal s'énonce comme suit:

Théorème principal:

1) L'ensemble des points algébriques de degré 2 sur C est donné par
$S = \left\{\left(\alpha, \pm\sqrt{6\alpha(\alpha^4+3)}\right), \alpha \in \mathbb{Q}^*\right\}$.

2) L'ensemble des points algébriques de degré 3 sur C est vide.

3) L'ensemble des points algébriques de degré 4 sur C est donné par $\mathcal{C}_0 \cup \mathcal{C}_1$ avec

$$\mathcal{C}_0 = \left\{\left(x, \pm\sqrt{6x(x^4+3)}\right) \mid x \in \mathbb{Q}, [\mathbb{Q}(x): \mathbb{Q} = 2]\right\};$$

$$\mathcal{C}_1 = \left\{\begin{matrix}\left(x, x(\alpha+\beta x)\right) \mid \alpha, \beta \in \mathbb{Q}^* \, et \, x \, racine \, de \\ F(x) = 6(x^4+3) - x(\alpha+\beta x)^2\end{matrix}\right\}.$$

4) L'ensemble des points algébriques de degré 5 sur C est donné par $\mathcal{D}_0 \cup \mathcal{D}_1$ avec

$$\mathcal{D}_0 = \left\{\begin{matrix}(x, \alpha+\beta x+\gamma x^2) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \, et \, x \, racine \, de \\ G(x) = (\alpha+\beta x+\gamma x^2)^2 - 6x(x^4+3)\end{matrix}\right\};$$

$$\mathcal{D}_1 = \left\{\begin{matrix}(x, \alpha x+\beta x^2+\gamma x^3) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \, et \, x \, racine \, de \\ H(x) = x(\alpha+\beta x+\gamma x^2)^2 - 6(x^4+3)\end{matrix}\right\}.$$

II. PRELIMINAIRES

Pour un diviseur D sur C nous notons $\mathcal{L}(D)$ le $\overline{\mathbb{Q}}$-espace vectoriel des fonctions rationnelles F sur C telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\overline{\mathbb{Q}}$-dimension de $\mathcal{L}(D)$. On montre dans [1] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de C est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

La courbe C est hyperelliptique de genre $g = 2$ et de rang nul d'après [1].

Soient $x\ et\ y$ les fonctions rationnelles définies sur C par :

$$x(X,Y,Z) = \frac{X}{Z}\ et\ y(X,Y,Z) = \frac{Y}{Z}$$

L'équation projective de la courbe C est :

$$C: Y^2Z^3 = 6X(X^4 + 3Z^4)$$

On désigne par J la jacobienne de C et par $j(P)$ la classe notée $[P - \infty]$ de $P - \infty$, c'est à dire que j est le plongement jacobien $C \to J(\mathbb{Q})$.

Désignons par $C^{'}.C$ le cycle d'intersection d'une courbe algébrique C' définie sur $\mathbb{Q}$ et C.

Lemme 1 :

- $div(x) = 2P - 2\infty$
- $div(y) = P + B_0 + B_1 + B_2 + B_3 - 5\infty$

Preuve :

Il s'agit d'un calcul sans difficulté du type $div(x - a) = (X - aZ = 0).C - (Z = 0).C$

Par exemple, on a $div(x) = div\left(\frac{X}{Z}\right) = (X = 0).C - (Z = 0).C.$

On a $(X = 0).C = 2P - 3\infty$ et $(Z = 0).C = 5\infty$, d'où $div(x) = 2P - 2\infty$.

Lemme 2 :

- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\ x \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \langle 1,\ x,\ x^2 \rangle$

- $\mathcal{L}(5\infty) = \langle 1,\ x,\ x^2,\ y\rangle$
- $\mathcal{L}(6\infty) = \langle 1,\ x,\ x^2,\ y,\ x^3\rangle$

Preuve : Résulte du lemme 1

Lemme 3: $\mathrm{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle 0, [(0,0) - \infty]\rangle = \{a[P - \infty],\ a \in \{0, 1\}\}$

Preuve : (Voir [1])

III. DEMONSTRATION DU THEOREME PRINCIPAL

1. Points quadratiques sur C

L'ensemble des points quadratiques sur C est donné par

$$S = \left\{\left(\alpha,\ \pm\sqrt{6\alpha(\alpha^4 + 3)}\right), \alpha \in \mathbb{Q}^*\right\}$$

Preuve :

Soit $R \in C(\overline{\mathbb{Q}})$ avec$[\mathbb{Q}(R): \mathbb{Q}] = 2$. Notons $R_1\ et\ R_2$ les conjugués de Galois de R. Travaillons avec $t = [R_1 +\ R_2 - 2\infty] \in \mathrm{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$t = [R_1 +\ R_2 - 2\infty] = aj(P) = -\ aj(P)$; $0 \leq a \leq 1$ $(*)$.

On remarque que $R \notin \{\infty,\ P\}$ et on a les deux cas suivants :

Cas $a = 0$

La relation $(*)$ devient $[R_1 +\ R_2 - 2\infty]$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 +\ R_2 - 2\infty$$

Donc $F \in \mathcal{L}(2\infty)$, d'où $F(x) = a_1 + a_2 x\ avec\ a_2 \neq 0$. Aux points R_i, on a $a_1 + a_2 x = 0$ donc $x = -\frac{a_1}{a_2} = \alpha$. En remplaçant x par α dans la relation $\mathrm{y}^2 = 6\mathrm{x}(x^4 + 3)$, on a: $y^2 = 6\alpha(\alpha^4 + 3)$

et par suite on a:

$$y = \pm\sqrt{6\alpha(\alpha^4 + 3)}$$

On a ainsi une famille de points quadratiques

$$S = \left\{\left(\alpha,\ \pm\sqrt{6\alpha(\alpha^4+3)}\right), \alpha \in \mathbb{Q}^*\right\}$$

Cas $\boldsymbol{a = 1}$

La relation $(*)$ devient $[R_1 + R_2 + P - 3\infty] = j(P) = -j(P)$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + P - 3\infty$.

Donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$ un des R_i devrait être égal à ∞ ; ce qui est absurde.

Conclusion: L'ensemble des points quadratiques sur C est donné par

$$S = \left\{\left(\alpha,\ \pm\sqrt{6\alpha(\alpha^4+3)}\right), \alpha \in \mathbb{Q}^*\right\}$$

2. Points cubiques sur C

L'ensemble des points cubiques sur C est vide.

Preuve :

Soit $R \in C(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R):\mathbb{Q}] = 3$. Notons R_1, R_2, R_3 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$t = [R_1 + R_2 + R_3 - 3\infty] = aj(P) = -aj(P)$; $0 \leq a \leq 1$ $(**)$.

On remarque que $R \notin \{\infty, P\}$ et on a les deux cas suivants:

Cas $\boldsymbol{a = 0}$

La relation $(**)$ devient $R_1 + R_2 + R_3 - 3\infty = 0$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que $div(F) = R_1 + R_2 + R_3 - 3\infty$.

Donc $F \in \mathcal{L}(3\infty)$ et comme $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, un des R_i devrait être égal à ∞ ; ce qui est absurde

Cas $\boldsymbol{a = 1}$

La relation $(**)$ devient $[R_1 + R_2 + R_3 - 3\infty] = j(P) = -j(P)$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$div(F) = R_1 + R_2 + R_3 + P - 4\infty$.

Donc $F \in \mathcal{L}(4\infty)$ d'où $F(x) = a_1 + a_2x + a_3x^2 \; avec \; a_3 \neq 0$.

Au point P, on a $F(P) = 0$ donc $a_1 = 0$ d'où $F(x) = x(a_2 + a_3x)$. Aux points R_i, on doit avoir $x(a_2 + a_3x) = 0$, donc $x \in \mathbb{Q}$ et par conséquent les R_i devraient être de degré ≤ 2.

Conclusion: L'ensemble des points cubiques sur C est vide.

3. Points quartiques sur C

L'ensemble des points quartiques sur C est donné par $\mathcal{C}_0 \cup \mathcal{C}_1$ avec

$$\mathcal{C}_0 = \left\{\left(x, \pm\sqrt{6x(x^4+3)}\right) \mid x \in \mathbb{Q}, [\mathbb{Q}(x): \mathbb{Q} = 2]\right\}$$

$$\mathcal{C}_1 = \left\{\begin{matrix}\left(x, x(\alpha + \beta x)\right) \mid \alpha, \beta \in \mathbb{Q}^* \; et \; x \; racine \; de \\ F(x) = 6(x^4+3) - x(\alpha + \beta x)^2\end{matrix}\right\}$$

Preuve :

Soit $R \in C(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R): \mathbb{Q}] = 4$. Notons R_1, R_2, R_3, R_4 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$t = [R_1 + R_2 + R_3 + R_4 - 4\infty] = aj(P) = -aj(P)$; $0 \leq a \leq 2$ ($***$).

On remarque que $R \notin \{\infty, P\}$ et on a les deux cas suivants:

Cas $a = 0$

La relation ($***$) devient $R_1 + R_2 + R_3 + R_4 - 4\infty = 0$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty$$

Donc $F \in \mathcal{L}(4\infty)$. Donc $F \in \mathcal{L}(4\infty)$ d'où $F(x) = a_1 + a_2x + a_3x^2 \; avec \; a_3 \neq 0$.

Aux points R_i , on a $a_1 + a_2x + a_3x^2 = 0$. La relation $y^2 = 6x(x^4+3)$ donne $y = \pm\sqrt{6x(x^4+3)}$.

On obtient une famille de point quartiques

$$\mathcal{C}_0 = \left\{\left(x, \pm\sqrt{6x(x^4+3)}\right) \mid x \in \mathbb{Q} \, , [\mathbb{Q}(x): \mathbb{Q}] = 2\right\}$$

Cas $a = 1$

La relation ($***$) devient $[R_1 + R_2 + R_3 + R_4 - 4\infty] = j(P) = -j(P)$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$div(F) = R_1 + R_2 + R_3 + R_4 + P - 5\infty$.

Donc $F \in \mathcal{L}(5\infty)$ d'où $F(x) = a_1 + a_2x + a_3x^2 + a_4y \; avec \; a_4 \neq 0$. Au point P , on a $F(P) = 0$ donc $a_1 = 0$ d'où $F(x) = x(a_2 + a_3x) + a_4y$. Aux points R_i, on a $x(a_2 + a_3x) + a_4y = 0$, d'où

$y = -\frac{a_2}{a_4}x - \frac{a_3}{a_4}x^2 = -\frac{a_3}{a_4}x\left(x + \frac{a_2}{a_3}\right)$. On voit que y est de la forme $y = \alpha x(x + \beta)$ avec $\alpha \; et \; \beta \in \mathbb{Q}^*$; et par suite on a $y^2 = 6x(x^4 + 3) \Leftrightarrow 6x(x^4 + 3) - \big(\alpha x(x + \beta)\big)^2 = 0$

$$x\Big(6(x^4 + 3) - x\big(\alpha(x + \beta)\big)^2\Big) = 0$$

On doit avoir $x \neq 0 \; et \; \alpha, \beta \in \mathbb{Q}^*$, on obtient une famille de points quartiques

$$\mathcal{C}_1 = \left\{ \begin{matrix} \big(x, x(\alpha + \beta x)\big) \mid \alpha, \beta \in \mathbb{Q}^* \; et \; x \; racine \; de \\ F(x) = 6(x^4 + 3) - x(\alpha + \beta x)^2 \end{matrix} \right\}$$

Conclusion: L'ensemble des points quartiques sur C est donné par $\mathcal{C}_0 \cup \mathcal{C}_1$.

4. Points quintiques sur C

L'ensemble des points quintiques sur C est donné par $\mathcal{D}_0 \cup \mathcal{D}_1$ avec

$$\mathcal{D}_0 = \left\{ \begin{matrix} (x, \alpha + \beta x + \gamma x^2) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \; et \; x \; racine \; de \\ G(x) = (\alpha + \beta x + \gamma x^2)^2 - 6x(x^4 + 3) \end{matrix} \right\}$$

Preuve :

Soit $R \in C(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R): \mathbb{Q}] = 5$. Notons R_1, R_2, R_3, R_4, R_5 les conjugués de Galois de R. Travaillons avec $t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] \in \mathrm{J}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, d'où

$t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = aj(P) = -aj(P)$; $0 \leq a \leq 1$ ($****$).

On remarque que $R \notin \{\infty, P\}$ et on a les deux cas suivants:

Cas $\boldsymbol{a = 0}$

La relation $(****)$ devient $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = 0$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty$.

Donc $F \in \mathcal{L}(5\infty)$ d'où

$F(x) = a_1 + a_2x + a_3x^2 + a_4y \; avec \; a_4 \neq 0$. Aux points R_i , on a $a_1 + a_2x + a_3x^2 + a_4y = 0$, d'où

On voit que y est de la forme $y = \alpha + \beta x + \gamma x^2$ avec $\alpha, \beta, \gamma \in \mathbb{Q}^*$; et par suite on a

$y^2 = 3x(x^4 + 3) \Leftrightarrow (\alpha + \beta x + \gamma x^2)^2 = 6x(x^4 + 3)$.

$$(\alpha + \beta x + \gamma x^2)^2 - 6x(x^4 + 3) = 0$$

On obtient une famille de points quintiques

$$\mathcal{D}_0 = \begin{Bmatrix} (x, \alpha + \beta x + \gamma x^2) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \; et \; x \; racine \; de \\ G(x) = (\alpha + \beta x + \gamma x^2)^2 - 6x(x^4 + 3) \end{Bmatrix}$$

Cas $\boldsymbol{a = 1}$

La relation $(****)$ devient $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = j(P) = -j(P)$. Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty$$

Donc $F \in \mathcal{L}(6\infty)$ d'où

$F(x) = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3 \; avec \; a_5 \neq 0$.

Au point P, on a $F(P) = 0$ donc $a_1 = 0$, d'où $F(x) = a_2x + a_3x^2 + a_4y + a_5x^3$. Ensuite aux points R_i, on a $a_2x + a_3x^2 + a_4y + a_5x^3 = 0$.

Donc on voit que y est de la forme $y = \alpha x + \beta x^2 + \gamma x^3$ avec $\alpha, \beta, \gamma \in \mathbb{Q}^*$; et par suite on a $y^2 = 6x(x^4 + 3) \Leftrightarrow (\alpha x + \beta x^2 + \gamma x^3)^2 = 6x(x^4 + 3) \Leftrightarrow$

$$x(\alpha + \beta x + \gamma x^2)^2 - 6(x^4 + 3) = 0$$

On doit avoir $x \neq 0 \; et \; \alpha, \beta, \gamma \in \mathbb{Q}^*$, on obtient une famille de points quintiques

$$\mathcal{D}_1 = \begin{Bmatrix} (x, \alpha x + \beta x^2 + \gamma x^3) \mid \alpha, \beta, \gamma \in \mathbb{Q}^* \; et \; x \; racine \; de \\ H(x) = x(\alpha + \beta x + \gamma x^2)^2 - 6(x^4 + 3) \end{Bmatrix}$$

Références

[1] N. Bruin, On powers as sums of two cubes, International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, 2000.

[2] P. A. Griffiths, Introduction to algebraic curves, Translations of mathematical monographs volume 76. American Mathematical Society, Providence, 1989.

[3] M. Hindry and J. H. Silverman, Diophantie geometry, an introduction, springer verlage,2000.

[4] J. TH. Mulholland, Elliptic curves with rational 2-torsion and related ternary Diophantine equations. ProQuest LLC. Ann Arbor, MI, 2006.

[5] E. H. Sow, M. Fall, O. Sall, Points algébriques de degrésau-plus 5 sur la courbe d'équation affine $y^2 = 4x^5 + 1$, SCIREA Journal of Mathematics, Volume 6, Issue 6, 2021.