International Journal of Mathematics and Statistics Invention (IJMSI)
E-ISSN: 2321- 4767 P-ISSN: 2321-4759
www.ijmsi.org Volume 10 Issue 1 || January, 2022 || PP 01-04

Points algébriques de degré quelconque sur la courbe d'équation affine C: $y^2 = 3(x^5 - 1)$

EL Hadji SOW [1], Pape Modou SARR [2], Moussa FALL [3], Oumar SALL [4]
Laboratoire de Mathématiques et Applications (L.M.A.)
U.F.R. des Sciences et Technologies
Université Assane SECK de Ziguinchor (SENEGAL)

Résumé. Dans ce travail, nous déterminons l'ensemble des points algébriques de degré quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ d'équation affine : $y^2 = 3(x^5 - 1)$.
L'énoncé obtenu étend un résultat de S. Siksek qui a décrit dans [3] l'ensemble des points $\mathbb{Q}$-rationnels sur cette courbe.

Abstract. In this work, we determine the set of algebraic points of given degree over $\mathbb{Q}$ on the curve $\mathcal{C}$ given by the affine equation $y^2 = 3(x^5 - 1)$.
This result extends a result of S. Siksek who described in [3] the set of rational points on this curve.

Keywords : Planes curves - Degree of algebraic points - Rationals points - Algebraic extensions - Jacobian

Mathematics Subject Classification : 14H50 - 14H40 - 11D68 - 12F05

Date of Submission: 11-01-2022 Date of Acceptance: 26-01-2022

I. INTRODUTION

Etant donnée une courbe algébrique $\mathcal{C}$ définie sur un corps de nombres K, on note $\mathcal{C}$(K) l'ensemble des points sur $\mathcal{C}$ rationnels sur K, et $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ l'ensemble des points algébriques de degré au-plus d sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$. Le degré d'un point algébrique R est le degré de son corps de définition sur $\mathbb{Q}$; en d'autres termes $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
Dans cette note, notre travail va consister en l'étude de quelques cas particuliers, où l'on peut déterminer explicitement les points algébriques de degré quelconque sur la courbe $\mathcal{C}$ d'équation affine

$$y^2 = 3(x^5 - 1) \tag{1}$$

Il semble qu'une condition indispensable est le fait que le groupe de Mordell-Weil que nous notons $J(\mathbb{Q})$ des points rationnels sur $\mathbb{Q}$ de la jacobienne J de $\mathcal{C}$ soit fini. Notons $P = (1, 0)$ et ∞ le point à l'infini. Dans [3], Siksek a donné une description des points rationnels sur $\mathbb{Q}$ sur cette courbe. Cette description s'énnonce comme suit :
Proposition. Les points $\mathbb{Q}-$rationnels sur la courbe $\mathcal{C}$ sont donnés par $\mathcal{C}(\mathbb{Q}) = \{\infty, P\}$.

Nous étendons ce résultat, en donnant une description explicite des points algébriques de degré quelconque sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$.
Nos outils essentiels sont :

- Le groupe de Mordell-Weil $J(\mathbb{Q})$ (voir [3]),
- Le théorème d'Abel Jacobi (voir [1]),
- Des systèmes linéaires sur la courbe $\mathcal{C}$.

Notre résultat principal s'énonce comme suit :

Théorème. L'ensemble des points algébriques de degré au-plus d sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par :

$$\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K) = \mathcal{F}_0 \cup \mathcal{F}_1$$

avec

avec

$$\mathcal{F}_0 = \left\{ \left(x, -\frac{\sum\limits_{i\leq\frac{n}{2}} a_i x^i}{\sum\limits_{j\leq\frac{n-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\}$$

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum\limits_{i\leq\frac{n+1}{2}} a_i x^i}{\sum\limits_{j\leq\frac{n-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ vérifiant } \sum_{i\leq\frac{n+1}{2}} a_i = 0 \text{ et } x \text{ racine de l'équation } (\mathcal{E}_1) \right\}$$

2 Résultats auxiliaires

Pour un diviseur D sur $\mathcal{C}$, nous notons $\mathcal{L}(D)$ le $\overline{\mathbb{Q}}-$ espace vectoriel des fonctions rationnelles F sur $\mathcal{C}$ telles que $F = 0$ ou $div(F) \geq -D$; $l(D)$ désigne la $\overline{Q}-$dimension de $\mathcal{L}(D)$. On montre dans [3] que le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et $\mathcal{C}$ est une courbe hyperelliptique de genre $g = 2$.
Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ par :

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

L' équation projective de la courbe $\mathcal{C}$ est :

$$\mathcal{C} : Y^2Z^3 = 3(X^5 - Z^5) \tag{2}$$

On désigne par $j(P)$ la classe notée $[P - \infty]$ de $P-\infty$, c'est- à- dire que j est le plongement jacobien $\mathcal{C} \longrightarrow J(\mathbb{Q})$.
Notons $\eta_1 = e^{i\frac{\Pi}{2}}$ et posons $A_k = (0, \sqrt{3}\eta_1^{2k+1})$ pour $k \in \{0, 1\}$.
Notons $\eta_2 = e^{i\frac{\Pi}{5}}$ et posons $B_k = (\eta_2^{2k}, 0)$ pour $k \in \{0, 1, 2, 3, 4\}$.
Désignons par $\mathcal{D}.\mathcal{C}$ le cycle d'intersection d'une courbe algébrique $\mathcal{D}$ définie sur $\mathbb{Q}$ et $\mathcal{C}$.

Lemme 1.

- $div(x - 1) = 2P - 2\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(x) = A_0 + A_1 - 2\infty$

Preuve. Il s'agit d'un simple calcul du type

$$div(x - a) = (X - aZ = 0).\mathcal{C} - (Z = 0).\mathcal{C}. \tag{3}$$

Par exemple $div(x - 1) = (X - Z = 0).\mathcal{C} - (Z = 0).\mathcal{C}$.
On a $(X - Z = 0).\mathcal{C} = 2P + 3\infty$ et $(Z = 0).\mathcal{C} = 5\infty$, d'où $div(x - 1) = 2P - 2\infty$

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 et du fait que d'après le théorème de Riemann-Rock on a $l(m\infty) = m - 1$ dès que $m \geq 3$.

Lemme 3. .
Une $\mathbb{Q}$-base de $\mathcal{L}(m\infty)$ est donné par :

$$\mathcal{B}_m = \left\{ x^i \mid i \in \mathbb{N} \text{ et } i \leq \frac{m}{2} \right\} \cup \left\{ x^j y \mid j \in \mathbb{N} \text{ et } j \leq \frac{m-5}{2} \right\}$$

Preuve. Voir [2].

Lemme 4. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle [P - \infty] \rangle = \{ a\,[P - \infty], a \in \{0, 1\} \}$.

Preuve. Voir [3].

3 Démonstration du théorème

Soit $R \in \mathcal{C}(\bar{\mathbb{Q}})$, avec $[\mathbb{Q}[R] : \mathbb{Q}] = n$. Les travaux de Siksek dans [3] nous permettent de supposer que $n \geq 2$. Notons $R_1, R_2, \ldots, R_n$ les conjugués de Galois de R.
On sait que $[R_1 + R_2 + \cdots + R_n - n\infty] \in J(\mathbb{Q})$, d'où d'après le lemme 4,
$[R_1 + R_2 + \cdots + R_n - n\infty] = a\,[P - \infty]\,,\ 0 \leq a \leq 1 \quad (*)$
Selon les valeurs de $a \in \{0, 1\}$, on a les deux cas suivants :
Premier cas : a = 0
La relation $(*)$ devient

$$[R_1 + R_2 + \cdots + R_n - n\infty] = 0$$

Le théorème d'Abel Jacobi entraine l'existence d'une fonction rationnelle F sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + R_2 + \cdots + R_n - n\infty \tag{4}$$

donc F $\in \mathcal{L}(n\infty)$, et d'après le lemme 3 on a

$$F(x, y) = \left(\sum_{i \leq \frac{n}{2}} a_i x^i \right) + \left(y \sum_{j \leq \frac{n-5}{2}} b_j x^j \right) \tag{5}$$

Aux points R_i on doit avoir

$$\left(\sum_{i \leq \frac{n}{2}} a_i x^i \right) + \left(y \sum_{j \leq \frac{n-5}{2}} b_j x^j \right) = 0 \tag{6}$$

d'où $y = -\dfrac{\sum\limits_{i \leq \frac{n}{2}} a_i x^i}{\sum\limits_{j \leq \frac{n-5}{2}} b_j x^j}$ et par suite la relation $y^2 = 3(x^5 - 1)$ donne l'équation

$$(\mathcal{E}_0) : \left(\sum_{i \leq \frac{l}{2}} a_i x^i \right)^2 = 3 \left(\sum_{j \leq \frac{n-5}{2}} b_j x^j \right)^2 (x^5 - 1)$$

On trouve ainsi une famille de points

$$\mathcal{F}_0 = \left\{ \left(x, -\frac{\sum\limits_{i \leq \frac{n}{2}} a_i x^i}{\sum\limits_{j \leq \frac{n-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ et } x \text{ racine de l'équation } (\mathcal{E}_0) \right\}$$

Deuxième cas : a = 1
La relation $(*)$ s'écrit $[R_1 + R_2 + \cdots + R_n - n\infty] = [P - \infty] = -[P - \infty]$.
Il existe alors une fonction F telle que

$$div(F) = R_1 + R_2 + \cdots + R_n + P - (n+1)\infty \tag{7}$$

donc F $\in \mathcal{L}((n+1)\infty)$, et d'après le lemme 3, on a

$$F(x,y) = \left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right) + \left(y \sum_{j\leq\frac{n-4}{2}} b_j x^j\right) \tag{8}$$

On a $F(P) = 0$ donne la relation

$$\sum_{i\leq\frac{n+1}{2}} a_i = 0$$

.

Aux points R_i on doit avoir

$$\left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right) + \left(y \sum_{j\leq\frac{n-4}{2}} b_j x^j\right) = 0 \tag{9}$$

d'où

$$y = -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_j x^j} \tag{10}$$

et par suite la relation $y^2 = 3(x^5 - 1)$ donne l'équation

$$(\mathcal{E}_1) : \left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right)^2 = 3\left(\sum_{j\leq\frac{n-4}{2}} b_j x^j\right)^2 (x^5 - 1)$$

et par suite la relation $y^2 = 3(x^5 - 1)$ donne l'équation

$$(\mathcal{E}_1) : \left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right)^2 = 3\left(\sum_{j\leq\frac{n-4}{2}} b_j x^j\right)^2 (x^5 - 1)$$

On trouve ainsi une famille de points

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \; vérifiant \sum_{i\leq\frac{n+1}{2}} a_i = 0 \; et \; x \; racine \; de \; l'équation \; (\mathcal{E}_1) \right\}$$

Références

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

[2] O. Sall, M. Fall, C. M. Coly, Points algébriques de degré donné sur la courbe d'équation affine $y^2 = x^5 + 1$, International Journal Of Development Research Vol. 06, Issue, 11, pp. 10295-10300, November, 2016.

[3] S. Siksek, Explicit Chabauty over number fields, Algebra & Number Theory, Volume 7, 2013, No. 4, page 765.