A COLLECTION OF PAPERS IN MATHEMATICS AND RELATED SCIENCES,
A FESTSCHRIFT IN HONOUR OF THE LATE GALAYE DIA
EDITORS : PROFS HAMET SEYDI, GANE SAMB LO, ABOUBAKARY DIAKHABY
SPAS-EDS (SAINT-LOUIS, CALGARY, 2018), WWW.STATPAS.ORG/SPASEDS/
IN EUCLID (WWW.PROJECTEUCLID.ORG)
DOI : 10.16929/SBS/2018.100

CHAPTER 4

Points algébriques de degré donné sur la courbe de Picard, *by Moussa FALL, Oumar SALL*

Moussa FALL. Email : moussafalls@yahoo.fr
Oumar SALL. Email : oumarsfr@yahoo.fr
Laboratoire de Mathématiques et Applications (L.M.A.), U.F.R. des Sciences et Technologies, Université Assane SECK de Ziguinchor.BP: 523 Sénégal.

Abstract. We give a parameterization of the algebraic points of given degree over $\mathbb{Q}$ on the Picard curve given by $y^3 = x^4 - 1$. This result extends a previous result of Klassen and Schaefer(1996) on the set of algebraic points of degree at most 3 over $\mathbb{Q}$ in the same curve. $\Diamond$

Keywords. Picard curve; Algebraic points of given degree; Jacobian; linear system

AMS 2010 Mathematics Subject Classification. 14H50; 14hH40; 11D68; 12FO5

Cite the chapter as :
Fall M. and Sall O.(2018). Points algébriques de degré donné sur la courbe de Picard .
In *A Collection of Papers in Mathematics and Related Sciences, a festschrift in honour of the late Galaye Dia* (Editors : Seydi H., Lo G.S. and Diakhaby A.). Spas Editions, Euclid Series Book, pp. 33 –41
Doi : 10.16929/sbs/2018.100-01-04

1. Introduction and motivations

Soit $\mathcal{C}$ la courbe algébrique définie sur $\mathbb{Q}$ par l'équation affine

$$y^3 = x^4 - 1.$$

Klassen and Schaefer (1996) ont montré que les seuls points $\mathbb{Q}$-rationnels de la courbe $\mathcal{C}$ sont

$$Q_1 = (0,\ -1,\ 1) \quad Q_2 = (-1,\ 0,\ 1) \quad Q_3 = (1,\ 0,\ 1) \quad \infty = (0,\ 1,\ 0)\,.$$

Ils ont, d'une part donné dans Klassen and Schaefer (1996), une description des points algébriques sur les extensions quadratiques et cubiques de $\mathbb{Q}$ et d'autre part, déterminé le groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de $\mathcal{C}$:

$$J(\mathbb{Q}) \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^2.$$

Dans cette note, nous déterminons les points algébriques de degré 4 et étendons ces résultats en donnant une paramétrisation des points algébriques de degré donné quelconque d ($d \geq 5$) sur $\mathbb{Q}$.

Le principe sous-jacent de la méthode utilisée est le suivant : On suppose donné un point $\infty \in \mathcal{C}(\mathbb{Q})$ et le plongement jacobien $j : \mathcal{C} \to J(\mathbb{Q})$, $P \mapsto [P - \infty]$. La méthode suppose que l'on connaisse ou détermine la structure du groupe $J(\mathbb{Q})$ et que celui-ci soit fini: $J(\mathbb{Q}) \simeq \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_s\mathbb{Z}$. On choisit alors $D_1, \ldots, D_s$ des diviseurs sur $\mathcal{C}$ définis sur $\mathbb{Q}$ tels que $j(D_i)$ soit d'ordre N_i et $j(D_1), \ldots j(D_s)$ engendrent $J(\mathbb{Q})$. Si R est un point algébrique de degré k et si on note $R_1, \ldots, R_k$ ses conjugués sous l'action de Galois, alors $j(R_1 + \ldots + R_k)$ appartient à $J(\mathbb{Q})$ et par conséquent il existe $0 \leq m_i \leq N_i - 1$ tels que $j(R_1 + \ldots + R_k) = m_1 j(D_1) + \ldots + m_s j(D_s)$. Le théorème d'Abel-Jacobi entraîne alors l'existence d'une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$R_1 + \ldots + R_k - m_1 D_1 - \ldots - m_s D_s + \sum_{i=1}^{s} (m_i \deg D_i - k)\,\infty = div(f).$$

La fonction f a donc des pôles prescrits, et si l'on sait analyser les espaces

$$\mathcal{L}(D) = \left\{ f \in \overline{\mathbb{Q}}(C) \mid div(f) + D \geq 0 \right\}$$

on en déduit des restrictions sur les R_i et même dans les bons cas une description explicite.
Nos principaux résultats sont les deux théorèmes suivants:

2. Results and proofs

THEOREM 11. *Les points algébriques sur $\mathcal{C}$, de degré 4 sur $\mathbb{Q}$, sont donnés par:*

(i) $\Gamma_1.\mathcal{C}$ *où* Γ_1 *est une droite définie sur* $\mathbb{Q}$*.*

(ii) $\Gamma_2.\mathcal{C} = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 + r\infty$ *où* Γ_2 *est une conique; avec* $n_1 \in \{0, 1, 2, 3\}$ *et* $\{n_2, n_3\} \subset \{0, 1, 2\}$, $r = 4 - n_1 - n_2 - n_3$, *et* $6 \leq 4 + n_1 + n_2 + n_3 \leq 8$*.*

(iii) $\Gamma_3.\mathcal{C} = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 + r\infty$ *où* Γ_3 *est une cubique, avec* $n_1 \in \{0, 1, 2, 3\}$ *et* $\{n_2, n_3\} \subset \{0, 1, 2\}$, $r = 8 - n_1 - n_2 - n_3$, *et* $9 \leq 4 + n_1 + n_2 + n_3 \leq 11$*.*

THEOREM 12. *Soit* $R \in \mathcal{C}\left(\overline{\mathbb{Q}}\right)$ *avec* $[\mathbb{Q}(R) : \mathbb{Q}] = d$*. Notons* $R_1, \ldots, R_d$ *les conjugués de Galois de* R*. Alors il existe une courbe* Γ_n *définie sur* $\mathbb{Q}$ *de degré* $n \leq \left[\dfrac{d+7}{3}\right]$ *telle que:*

$$\Gamma_n.\mathcal{C} = R_1 + \ldots + R_d + n_1Q_1 + n_2Q_2 + n_3Q_3 + r\infty$$

avec $r = 4n - d - n_1 - n_2 - n_3$*;* $r \geq 0$, $n_1 \in \{0, 1, 2, 3\}$ *et* $\{n_2, n_3\} \subset \{0, 1, 2\}$
La notation $[x]$ *désigne la partie entière de* x*.*

Résultats auxiliaires Pour un diviseur D sur $\mathcal{C}$, nous notons par $l(D)$ la $\overline{\mathbb{Q}}-$dimension de $\mathcal{L}(D)$ où $\mathcal{L}(D)$ est le $\overline{\mathbb{Q}}-$espace vectoriel des fonctions rationnelles définies par

$$\mathcal{L}(D) = \left\{ f \in \overline{\mathbb{Q}}(\mathcal{C})^* \;\mid\; div(f) \geq -D \right\} \cup \{ f = 0 \}.$$

Soient x et y les fonctions rationnelles définies sur $\mathcal{C}$ données par: $x(X, Y, Z) = X/Z$ et $y(X, Y, Z) = Y/Z$. On a le lemme suivant

LEMMA 5. *Soient les points*

$$Q_4 = (0, \sqrt{-1}, 1),\ Q_5 = (0, -\sqrt{-1}, 1),\ Q_6 = \left(0, \frac{1+\sqrt{-3}}{2}, 1\right),\ Q_7 = \left(0, \frac{1-\sqrt{-3}}{2}, 1\right)$$

- $div(x-1) = 3Q_3 - 3\infty$
- $div(x+1) = 3Q_2 - 3\infty$
- $div(x) = Q_1 + Q_6 + Q_7 - 3\infty$
- $div(y) = Q_2 + Q_3 + Q_4 + Q_5 - 4\infty$
- $div(y+1) = 4Q_1 - 4\infty$.

Preuve. Il s'agit d'un calcul du type $div\,(x-a) = (X - aZ = 0)\,.\mathcal{C} - (Z = 0)\,.\mathcal{C}$ Par exemple : $div\,(x-1) = (X - Z = 0)\,.\mathcal{C} - (Z = 0)\,.\mathcal{C}$. On a alors: $(X - Z = 0)\,.\mathcal{C} = 3Q_3 + \infty$ et $(Z = 0)\,.\mathcal{C} = 4\infty$. D'où $div\,(x-1) = 3Q_3 - 3\infty$. □
Soit j le plongement jacobien de $\mathcal{C} \to j(\mathbb{Q})$, la classe $[P - \infty]$ de P est notée $j(P)$. Nous déduisons du lemme 5 le résultat:

$$4j(Q_1) = 0\,, \quad 3j(Q_2) = 0 \quad et \quad 3j(Q_3) = 0. \qquad (1)$$

LEMMA 6. *i)* $J(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2 \cong \langle\, j(Q_1),\ j(Q_2),\ j(Q_3)\,\rangle$.
ii) Pour tout $x \in J\,(\mathbb{Q})$ *, il existe* $n_1 \in \{0,\ 1,\ 2,\ 3\}$ *et* $n_2,\ n_3 \in \{0,\ 1,\ 2\}$ *tels que:*

$$x = -n_1 j\,(Q_1) - n_2 j\,(Q_2) - n_3 j\,(Q_3)\,.$$

Preuve. i) Voir Klassen and Schaefer (1996).
ii) C'est une conséquence directe de i) et du résultat (1). □

LEMMA 7.
- $\mathcal{L}(\infty) = \langle 1 \rangle = \mathcal{L}(2\infty)$
- $\mathcal{L}(3\infty) = \langle 1, x \rangle$
- $\mathcal{L}(4\infty) = \langle 1, x, y \rangle = \mathcal{L}(5\infty)$
- $\mathcal{L}(6\infty) = \langle 1, x, y, x^2 \rangle$
- $\mathcal{L}(7\infty) = \langle 1, x, y, x^2, xy \rangle$
- $\mathcal{L}(8\infty) = \langle 1, x, y, x^2, xy, y^2 \rangle$
- $\mathcal{L}(9\infty) = \langle 1, x, y, x^2, xy, y^2, x^3 \rangle$
- $\mathcal{L}(10\infty) = \langle 1, x, y, x^2, xy, y^2, x^3, x^2y \rangle$
- $\mathcal{L}(11\infty) = \langle 1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2 \rangle$.
- *Plus généralement, pour* $m \geq 5$*, une base de* $\mathcal{L}(m\infty)$ *est:*

$$\mathcal{B}_m = \left\{ x^a y^b \mid a,\ b \in \mathbb{N} \text{ avec } b \leq 2 \text{ et } 3a + 4b \leq m \right\}.$$

Preuve. On a $l\,(\infty) = 1$ puisque si $l\,(point) > 1$ alors la courbe est de genre 0, ce qui n'est pas le cas avec $\mathcal{C}$.

On a $l(2\infty) = 1$, car si $l(2\infty) > 1$ alors la courbe est hyperelliptique, ce qui n'est pas le cas avec $\mathcal{C}$.

Puisque $(Z = 0).\mathcal{C} = 4\infty$ et que le genre de $\mathcal{C}$ est égal à 3, alors le diviseur canonique que l'on note $K_{\mathcal{C}}$ de $\mathcal{C}$ est égal à 4∞. Il résulte du théorème de Riemann-Roch que si l'on pose $D = m\infty$, alors $l(D) - l(K_{\mathcal{C}} - D) = degD + 1 - g$ c'est-à-dire $l(m\infty) - l(4\infty - m\infty) = m + 1 - g$, d'où $l(m\infty) = m - 2 + l(4\infty - m\infty)$ et par suite $l(3\infty) = 2$.

Puisque $K_{\mathcal{C}} = 4\infty$ est un diviseur canonique, on sait que $l(4\infty) = g = 3$. Lorsque $m \geq 5$, on obtient $l(m\infty) = m - 2$. Les éléments de $\mathcal{B}_m$ sont linéairement indépendants et appartiennent à $\mathcal{L}(m\infty)$. Posons

$$\mathcal{B}_m^0 = \left\{x^a \mid a \in \mathbb{N} \; avec \; a \leq \frac{m}{3}\right\},$$

,

$$\mathcal{B}_m^1 = \left\{x^a y \mid a \in \mathbb{N} \; avec \; a \leq \frac{m-4}{3}\right\}$$

et

$$\mathcal{B}_m^2 = \left\{x^a y^2 \mid a \in \mathbb{N} \; avec \; a \leq \frac{m-8}{3}\right\}.$$

.

Il est évident que $\mathcal{B}_m^0$, $\mathcal{B}_m^1$ et $\mathcal{B}_m^2$ constituent une partition de $\mathcal{B}_m$.

$$Card\,(\mathcal{B}_m) = Card\,(\mathcal{B}_m^0) + Card\,(\mathcal{B}_m^1) + Card\,(\mathcal{B}_m^2)$$

$$Card\,(\mathcal{B}_m) = \left(\left[\frac{m}{3}\right] + 1\right) + \left(\left[\frac{m-4}{3}\right] + 1\right) + \left(\left[\frac{m-8}{3}\right] + 1\right) = m - 2$$

donc $l\,(m\infty) = m - 2$, ce qui prouve que $\mathcal{B}_m$ est une base de $\mathcal{L}(m\infty)$. $\square$

Démonstration des théorèmes

Preuve du Théorème 11. Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = 4$. Notons $R_1, \ldots, R_4$ les conjugués de Galois de R. Nous remarquons qu'aucun des R_i n'est égal à ∞ ou un des points Q_i. Le point $[R_1 + \ldots + R_4 - \infty] \in J(\mathbb{Q})$ et d'après le Lemme 6 on a :

$$[R_1 + \ldots + R_4 - 4\infty] = -n_1 j\,(Q_1) - n_2 j\,(Q_2) - n_3 j\,(Q_3) \quad (\star)$$

avec $n_1 \in \{0, 1, 2, 3\}$ et $n_2, n_3 \in \{0, 1, 2\}$.

Notre analyse se scinde en quatre cas:

Cas 1: Supposons que $4 + n_1 + n_2 + n_3 = 4$, alors $(\star)$ devient

$$[R_1 + \ldots + R_4 - \infty] = 0$$

D'après le théorème d'Abel Jacobi(voir Griffiths (1989) page 156), il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = R_1 + \ldots + R_4 - 4\infty$$

On a donc $f \in \mathcal{L}(4\infty)$ et d'après lemme 7, il existe une droite Γ_1 définie sur $\mathbb{Q}$ telle que

$$\Gamma_1.\mathcal{C} = div f + 4\infty = R_1 + \ldots + R_4.$$

Cas 2: Supposons que $4 + n_1 + n_2 + n_3 = 5$, alors $(\star)$ devient

$$[R_1 + \ldots + R_4 + Q_i - 5\infty] = 0.$$

Il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = R_1 + \ldots + R_4 + Q_i - 5\infty.$$

On a donc $f \in \mathcal{L}(5\infty)$. Or $\mathcal{L}(5\infty) = \mathcal{L}(4\infty)$ donc un des R_i devrait être égal à ∞, ce qui est absurde.
Cas 3: Supposons que $6 \leq 4 + n_1 + n_2 + n_3 \leq 8$, alors $(\star)$ devient

$$[R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 - (4 + n_1 + n_2 + n_3)\infty] = 0.$$

Il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 - (4 + n_1 + n_2 + n_3)\infty.$$

On a donc $f \in \mathcal{L}(m\infty)$ avec $6 \leq m \leq 8$ et d'après lemme 7, il existe une conique Γ_2 définie sur $\mathbb{Q}$ telle que

$$\Gamma_2.\mathcal{C} = div f + 8\infty = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 - (4 + n_1 + n_2 + n_3)\infty + 8\infty.$$

C'est à dire

$$\Gamma_2.\mathcal{C} = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 + (4 - n_1 - n_2 - n_3)\infty.$$

Cas 4: Supposons que $7 \leq 4 + n_1 + n_2 + n_3 \leq 11$, alors $(\star)$ devient

$$[R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 - (4 + n_1 + n_2 + n_3)\infty] = 0$$

Il existe alors une fonction rationnelle f définie sur $\mathbb{Q}$ telle que

$$div(f) = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 - (4 + n_1 + n_2 + n_3)\infty.$$

On a donc $f \in \mathcal{L}(m\infty)$ avec $7 \leq m \leq 11$ et d'après lemme 7, il existe une cubique Γ_3 définie sur $\mathbb{Q}$ telle que

$$\Gamma_3.\mathcal{C} = div f + 12\infty = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 - (4 + n_1 + n_2 + n_3) + \infty + 8\infty.$$

C'est à dire

$$\Gamma_3.\mathcal{C} = R_1 + \ldots + R_4 + n_1Q_1 + n_2Q_2 + n_3Q_3 + (8 - n_1 - n_2 - n_3)\infty.$$

$\square$

Preuve du Théorème 12

Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = d$ et $R_1, \ldots, R_d$ les conjugués de Galois de R. Le cas $d \leq 3$ est traité dans Klassen and Schaefer (1996) et le cas $d = 4$ dans le théorème 11, nous pouvons donc supposer que $d \geq 5$ et en particulier qu'aucun des R_i n'est égal à ∞ ou un des points Q_i. Ainsi $[R_1 + \ldots + R_d - d\infty] \in J(\mathbb{Q})$ et d'après le Lemme 6 peut s'écrire sous la forme :

$$[R_1 + \ldots + R_d - d\infty] = -n_1 j\,(Q_1) - n_2 j\,(Q_2) - n_3 j\,(Q_3)\,,$$

avec $n_1 \in \{0,\, 1,\, 2,\, 3\}$ et $n_2,\, n_3 \in \{0,\, 1,\, 2\}$.

D'après le théorème d'Abel Jacobi(voir Griffiths (1989) page 156), il existe alors une fonction rationnelle F définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + \ldots + R_d + n_1Q_1 + n_2Q_2 + n_3Q_3 - (d + n_1 + n_2 + n_3)\,\infty$$

avec $n_1 \in \{0,\, 1,\, 2,\, 3\}$ et $n_2,\, n_3 \in \{0,\, 1,\, 2\}$.

On a donc $F \in \mathcal{L}\left((d + n_1 + n_2 + n_3)\,\infty\right)$ et le lemme 7 montre que la fonction F est un polynôme $P(x, y)$ avec $n = \deg P \leq \left[\frac{d+7}{3}\right]$ et il existe alors une courbe Γ_n définie sur $\mathbb{Q}$ d'équation $\Gamma_n : Z^n P\left(\frac{X}{Z}, \frac{Y}{Z}\right) = 0$ comme la droite $(Z = 0)$ coupe $\mathcal{C}$ en 4∞, on déduit l'égalité :

$$\Gamma_n.\mathcal{C} = R_1 + \ldots + R_d + n_1Q_1 + n_2Q_2 + n_3Q_3 + r\infty$$

avec $r = 4n - d - n_1 - n_2 - n_3$; $n_1 \in \{0,\, 1,\, 2,\, 3\}$ et $n_2,\, n_3 \in \{0,\, 1,\, 2\}$.

Ainsi pour toute fonction rationnelle définie sur $\mathbb{Q}$ telle que

$$div(F) = R_1 + \ldots + R_d + n_1Q_1 + n_2Q_2 + n_3Q_3 - m\infty$$

Si Γ_n est une courbe de degré n définie sur $\mathbb{Q}$ alors $\Gamma.\mathcal{C}$ est de degré $4n$ et on obtient

$$div(F) = \Gamma_n.\mathcal{C} - 4n\infty$$

et par suite $\Gamma_n.\mathcal{C} = R_1 + \ldots + R_d + n_1Q_1 + n_2Q_2 + n_3Q_3 + (4n - m)\,\infty$.

Ainsi la somme des conjugués $R_1 + \ldots + R_d$ est l'intersection résiduelle d'une courbe de degré n passant par les Q_i et ∞ avec les multiplicités indiquées.

□

Le théorème est explicite pour les points algébriques de petits degrés par exemple:

Corollary 5. .
Les points algébriques sur $\mathcal{C}$, de degré 5 sur $\mathbb{Q}$, sont donnés par :

(i) $\Gamma_2.\mathcal{C} = R_1 + \ldots + R_5 + n_1Q_1 + n_2Q_2 + n_3Q_3 + r\infty$ *où* Γ_2 *est une conique; avec* $n_1 \in \{0, 1, 2, 3\}$ *et* $\{n_2, n_3\} \subset \{0, 1, 2\}$, $r = 3 - n_1 - n_2 - n_3$, *et* $6 \leq 5 + n_1 + n_2 + n_3 \leq 8$.

(ii) $\Gamma_3.\mathcal{C} = R_1 + \ldots + R_5 + n_1Q_1 + n_2Q_2 + n_3Q_3 + r\infty$ *où* Γ_3 *est une cubique; avec* $n_1 \in \{0, 1, 2, 3\}$ *et* $\{n_2, n_3\} \subset \{0, 1, 2\}$, $r = 7 - n_1 - n_2 - n_3$, *et* $9 \leq 5 + n_1 + n_2 + n_3 \leq 11$.

(iii) $\Gamma_4.\mathcal{C} = R_1 + \ldots + R_5 + 3Q_1 + 2Q_2 + 2Q_3 + 4\infty$ *où* Γ_4 *est une quartique définie sur* $\mathbb{Q}$.

Bibliography

Griffiths P.A(1989) *Introduction to algebraic curves*, Translations of mathematical monographs volume 76. (1989)

M. J. Klassen and E. F. Schaefer(1996) *Arithmetic and geometry of the curve* $y^3 + 1 = x^4$, Acta Arithmetica LXXIV.3 (1996) 241-257.