



Théorie des nombres/Géométrie algébrique

Paramétrisation des points algébriques de degré donné sur la courbe d'équation affine $y^3 = x(x - 1)(x - 2)(x - 3)$

Parameterization of algebraic points of a given degree on the curve of the affine equation $y^3 = x(x - 1)(x - 2)(x - 3)$

Oumar Sall, Thiéyacine Top, Moussa Fall

Laboratoire de mathématiques et applications (L.M.A.) U.F.R. des sciences et technologies, Université de Ziguinchor, BP 523, Ziguinchor, Casamance, Sénégal

INFO ARTICLE

Historique de l'article :

Reçu le 3 octobre 2009

Accepté après révision le 18 octobre 2010

Disponible sur Internet le 3 novembre 2010

Présenté par Jean-Pierre Serre

RÉSUMÉ

Nous donnons une paramétrisation des points algébriques de degré quelconque sur \mathbb{Q} sur la courbe \mathcal{C} d'équation affine :

$$y^3 = x(x - 1)(x - 2)(x - 3)$$

L'énoncé obtenu étend un résultat de E.F. Schaefer qui a décrit dans Schaefer (1998) [1] l'ensemble des points algébriques de degré au plus 3 sur \mathbb{Q} sur cette courbe.

© 2010 Académie des sciences. Publié par Elsevier Masson SAS. Tous droits réservés.

ABSTRACT

We give a parameterization of the algebraic points of given degree over \mathbb{Q} on the curve

$$y^3 = x(x - 1)(x - 2)(x - 3)$$

This result extends a previous result of E.F. Schaefer who described in Schaefer (1998) [1] the set of algebraic points of degree ≤ 3 over \mathbb{Q} .

© 2010 Académie des sciences. Publié par Elsevier Masson SAS. Tous droits réservés.

1. Introduction

Soit \mathcal{C} une courbe algébrique de genre g définie sur un corps de nombres K . Un théorème célèbre de Faltings affirme que, si $g \geq 2$ alors l'ensemble $\mathcal{C}(K)$ des points rationnels sur K est fini. Une généralisation aux sous-variétés d'une variété abélienne permet une étude qualitative de l'ensemble des points de degré borné $\bigcup_{[L:K] \leq d} \mathcal{C}(L)$. Cette étude est équivalente à la détermination des points rationnels sur les produits symétriques de la courbe. Ces résultats sont en général ineffectifs. La situation est plus favorable dans le cas où le rang du groupe de Mordell–Weil de la jacobienne de \mathcal{C} est nul. Nous nous proposons d'étudier en détail les points algébriques de degré quelconque sur \mathbb{Q} sur la courbe \mathcal{C} d'équation affine :

$$y^3 = x(x - 1)(x - 2)(x - 3)$$

Dans [1] on a donné une description des points rationnels, quadratiques et cubiques.

Adresses e-mail : oumarsfr@yahoo.fr (O. Sall), thieyacinetop@yahoo.fr (T. Top), moussafalls@yahoo.fr (M. Fall).

Notons $P_0 = (0, 0)$, $P_1 = (1, 0)$, $P_2 = (2, 0)$, $P_3 = (3, 0)$ et ∞ le point à l'infini. Nous désignerons par $C_1.C$ le cycle intersection d'une courbe algébrique C_1 définie sur \mathbb{Q} et C .

Posons $Q_1 = (x_1, -1)$, $Q_2 = (x_2, -1)$ avec x_1 et x_2 des racines de l'équation $x^2 - 3x + 1 = 0$, et $D_0 = Q_1 + Q_2$.

La proposition donnée dans [1] s'énonce comme suit :

Proposition (Schaefer).

(i) Les points \mathbb{Q} -rationnels de la courbe C sont donnés par :

$$C(\mathbb{Q}) = \{P_0, P_1, P_2, P_3, \infty\}$$

(ii) Les points de degré 2 de la courbe C sont donnés par : Q_1 , Q_2 et $(x, 2)$ avec x racine de l'équation $(x^2 - 3x - 2)(x^2 - 3x + 4) = 0$.

(iii) Il y a douze triplets de points conjugués dans une extension cubique qui ne sont pas colinéaires. Les autres points cubiques sont donnés par l'intersection d'une droite \mathbb{Q} -rationnelle passant par l'un des points de $C(\mathbb{Q})$.

Nous étendons ces résultats en donnant une description des points de degré quelconque sur \mathbb{Q} . La description est « très explicite » en petit degré (disons $d \leq 5$), « moins explicite » pour d grand mais reste intéressante en degré quelconque.

Les outils essentiels sont :

- la détermination du groupe de Mordell-Weil de la jacobienne $J(\mathbb{Q})$ de C (faite dans [1]),
- le théorème d'Abel-Jacobi,
- l'étude des systèmes linéaires sur la courbe C .

Le résultat s'énonce comme suit :

Théorème. Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = d$. Notons R_1, \dots, R_d les conjugués de Galois de R .

Alors il existe une courbe C_1 définie sur \mathbb{Q} de degré $\delta \leq E(\frac{d}{3}) + 2$ telle que

$$C_1.C = R_1 + \dots + R_d + m_i P_i + m_j P_j + \varepsilon D_0 + r \infty$$

avec $r = 4\delta - d - m_i - m_j - 2\varepsilon$, $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$ et $\varepsilon \in \{0, 1\}$.

La notation $E(\frac{d}{3})$ désigne la partie entière de $\frac{d}{3}$.

En particulier :

(1) Les points algébriques sur C , de degré 4 sur \mathbb{Q} , sont donnés par :

(i) $C_1.C$ où C_1 est une droite définie sur \mathbb{Q} .

(ii) $C_1.C = R_1 + \dots + R_4 + m_i P_i + m_j P_j + \varepsilon D_0 + r \infty$, où C_1 est une conique ; avec $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$, $\varepsilon \in \{0, 1\}$, $r = 4 - m_i - m_j - 2\varepsilon$, et $6 \leq 4 + m_i + m_j + 2\varepsilon \leq 8$.

(iii) $C_1.C = R_1 + \dots + R_4 + m_i P_i + m_j P_j + \varepsilon D_0 + r \infty$, où C_1 est une cubique ; avec $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$, $\varepsilon \in \{0, 1\}$, $r = 8 - m_i - m_j - 2\varepsilon$, et $9 \leq 4 + m_i + m_j + 2\varepsilon \leq 12$.

(2) Les points algébriques sur C , de degré 5 sur \mathbb{Q} , sont donnés par :

(i) $C_1.C = R_1 + \dots + R_5 + m_i P_i + m_j P_j + \varepsilon D_0 + r \infty$, où C_1 est une conique ; avec $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$, $\varepsilon \in \{0, 1\}$, $r = 3 - m_i - m_j - 2\varepsilon$, et $6 \leq 5 + m_i + m_j + 2\varepsilon \leq 8$.

(ii) $C_1.C = R_1 + \dots + R_4 + R_5 + m_i P_i + m_j P_j + \varepsilon D_0 + r \infty$, où C_1 est une cubique ; avec $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$, $\varepsilon \in \{0, 1\}$, $r = 7 - m_i - m_j - 2\varepsilon$, et $9 \leq 5 + m_i + m_j + 2\varepsilon \leq 12$.

Ces résultats peuvent se traduire en termes de points \mathbb{Q} -rationnels du produit symétrique d -ième de la courbe C .

2. Résultats auxiliaires

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 $\text{div}(f) \geq -D$; $l(D)$ désigne la $\overline{\mathbb{Q}}$ -dimension de $\mathcal{L}(D)$. Soient x, y les fonctions rationnelles sur C données par

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

$$C : y^3 = x(x-1)(x-2)(x-3) \subset \mathbb{A}^2 \quad (\text{équation affine})$$

$$C : Y^3 Z = X(X-Z)(X-2Z)(X-3Z) \subset \mathbb{P}^2 \quad (\text{équation projective})$$

La classe $[P - \infty]$ de $P - \infty$ est notée $j(P)$; ainsi, j est le plongement jacobien $C \rightarrow J(\mathbb{Q})$.

Lemme 1.

(i) $\text{div}(x) = 3P_0 - 3\infty, \text{div}(x - 1) = 3P_1 - 3\infty, \text{div}(x - 2) = 3P_2 - 3\infty, \text{div}(x - 3) = 3P_3 - 3\infty, \text{div}(y) = P_0 + P_1 + P_2 + P_3 - 4\infty, \text{div}(y + 1) = 2D_0 - 4\infty.$

(ii) $\mathcal{L}(\infty) = \langle 1 \rangle = \mathcal{L}(2\infty)$
 $\mathcal{L}(3\infty) = \langle 1, x \rangle$
 $\mathcal{L}(4\infty) = \langle 1, x, y \rangle = \mathcal{L}(5\infty)$
 $\mathcal{L}(6\infty) = \langle 1, x, y, x^2 \rangle$
 $\mathcal{L}(7\infty) = \langle 1, x, y, x^2, xy \rangle$
 $\mathcal{L}(8\infty) = \langle 1, x, y, x^2, xy, y^2 \rangle$
 $\mathcal{L}(9\infty) = \langle 1, x, y, x^2, xy, y^2, x^3 \rangle$
 $\mathcal{L}(10\infty) = \langle 1, x, y, x^2, xy, y^2, x^3, x^2y \rangle$

Plus généralement, pour $m \geq 5$, une base de $\mathcal{L}(m\infty)$ est

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

Preuve. (i) Il s'agit d'un calcul sans difficulté analogue aux calculs faits dans [2]. Par exemple pour $\text{div}(x) = 3P_0 - 3\infty$, la fonction s'annule en P_0 et a pour seul pôle ∞ ; donc $\text{div}(x) = mP_0 - m\infty$, et comme $\text{ord}_{P_0}(x) = 3 \text{ ord}_{P_0}(y)$ l'entier m est multiple de 3 et comme x, y engendrent le corps de fonctions de \mathcal{C} , on a en fait $m = 3$.

(ii) On a $l(\infty) = 1$ puisque si $l(\text{point}) > 1$ 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 $(Z = 0) \cdot \mathcal{C} = 4\infty$ et que le genre de \mathcal{C} est égal à 3, alors 4∞ est un diviseur canonique de \mathcal{C} . Il résulte du théorème de Riemann–Roch que si l'on pose $K_{\mathcal{C}} = 4\infty$ et $D = m\infty$, alors

$$l(D) - l(K_{\mathcal{C}} - D) = \text{deg } D + 1 - g$$

i.e. $l(m\infty) - l(4\infty - m\infty) = m + 1 - g$, 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 $\mathcal{L}(m\infty)$ et on a

$$\begin{aligned} \text{card}(\mathcal{B}_m) &= \left(E\left(\frac{m}{3}\right) + 1 \right) + \left(E\left(\frac{m-4}{3}\right) + 1 \right) + \left(E\left(\frac{m-8}{3}\right) + 1 \right) \\ &= m - 2 = l(m\infty) \end{aligned}$$

ce qui montre que \mathcal{B}_m est une base de $\mathcal{L}(m\infty)$. \square

On a alors les résultats suivants :

(R1) Les éléments $F \in \mathcal{L}(m\infty)$ sont des polynômes de la forme $P(x, y) = \sum_{3a+4b \leq m, b \leq 2} c_{ab} x^a y^b$.

En particulier $\text{deg } P \leq \max_{3a+4b \leq m} (a + b) = E\left(\frac{m}{3}\right)$.

(R2) Nous avons les relations suivantes dans la Jacobienne : $3j(P_0) = 3j(P_1) = 3j(P_2) = 3j(P_3) = 0, j(P_0) + j(P_1) + j(P_2) + j(P_3) = 0$ et $2j(D_0) = 0$.

Lemme 2. $J(\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/2\mathbb{Z}) \cong \langle j(P_0), j(P_1), j(P_2) \rangle \oplus \langle j(D_0) \rangle$.

Preuve. Voir [1]. Notons que le point essentiel est de montrer, par une descente, que le rang du groupe de Mordell–Weil est nul. \square

Lemme 3. Pour tous m_0, m_1, m_2 , il existe $i, j \in \{0, 1, 2, 3, 4\}$ et n_i, n_j dans $\{0, 1, 2\}$ tels que

$$-m_0 j(P_0) - m_1 j(P_1) - m_2 j(P_2) = -n_i j(P_i) - n_j j(P_j).$$

Preuve. On voit que les m_k (et les n_i à construire) sont en fait des entiers modulo 3. Si l'un des m_k est nul la conclusion est immédiate et si les m_k valent 1 ou 2 alors deux d'entre eux sont égaux, par exemple $m_1 = m_2$. Dans ce cas le calcul donné fournit l'égalité

$$-m_0 j(P_0) - m_1 j(P_1) - m_2 j(P_2) = -(m_0 - m_2)j(P_0) - (-m_2)j(P_3) = -n_0 j(P_0) - n_3 j(P_3)$$

avec $n_0 \equiv (m_0 - m_2) \pmod{3}$, $n_3 \equiv (-m_2) \pmod{3}$. \square

Lemme 4. Soit $x \in J(\mathbb{Q})$ alors il existe $i, j \in \{0, 1, 2, 3, 4\}$, m_i, m_j dans $\{0, 1, 2\}$ et $\varepsilon \in \{0, 1\}$ tels que

$$x = m_i j(P_i) + m_j j(P_j) + \varepsilon j(D_0)$$

Preuve. C'est une conséquence directe du Lemme 2 et du Lemme 3. \square

3. Démonstration du théorème

Soit $R \in \mathcal{C}(\overline{\mathbb{Q}})$ avec $[\mathbb{Q}(R) : \mathbb{Q}] = d$. Notons R_1, \dots, R_d les conjugués de Galois de R .

Le cas $d \leq 3$ est traité dans [1] nous pouvons donc supposer que $d \geq 4$ et en particulier qu'aucun des R_k n'est égal à ∞ ou un des points P_i ou Q_j .

Ainsi le point $[R_1 + \dots + R_d - d\infty]$ est dans $J(\mathbb{Q})$ et d'après le Lemme 4 peut s'écrire sous la forme

$$-m_i j(P_i) - m_j j(P_j) - \varepsilon j(D_0)$$

avec $m_i \in \{0, 1, 2\}$, $\varepsilon \in \{0, 1\}$ et $D_0 = Q_1 + Q_2$.

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

$$\operatorname{div}(F) = R_1 + \dots + R_d + m_i P_i + m_j P_j + \varepsilon D_0 - (d + m_i + m_j + 2\varepsilon)\infty$$

avec $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$ et $\varepsilon \in \{0, 1\}$.

On a donc $F \in \mathcal{L}((d + m_i + m_j + 2\varepsilon)\infty)$, et (R1) montre que $F = P(x, y)$ avec $\delta = \deg P \leq E(\frac{d+6}{3})$ et il existe alors une courbe C_1 définie sur \mathbb{Q} dont l'équation est donnée par $Z^\delta P(\frac{X}{Z}, \frac{Y}{Z}) = 0$, et comme la droite $(Z = 0)$ coupe \mathcal{C} en 4∞ , on déduit l'égalité.

$$C_1 \cdot \mathcal{C} = R_1 + \dots + R_d + m_i P_i + m_j P_j + \varepsilon D_0 + r\infty$$

avec $r = 4\delta - d - m_i - m_j - 2\varepsilon$, $\{i, j\} \subset \{0, 1, 2, 3\}$, $\{m_i, m_j\} \subset \{0, 1, 2\}$ et $\varepsilon \in \{0, 1\}$.

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

$$\operatorname{div}(F) = R_1 + \dots + R_d + m_i P_i + m_j P_j + \varepsilon D_0 - m\infty$$

si C_1 est une courbe de degré δ définie sur \mathbb{Q} , alors $C_1 \cdot \mathcal{C}$ est de degré 4δ et on obtient

$$\operatorname{div}(F) = C_1 \cdot \mathcal{C} - 4\delta\infty$$

et par suite

$$C_1 \cdot \mathcal{C} = R_1 + \dots + R_d + m_i P_i + m_j P_j + \varepsilon D_0 + (4\delta - m)\infty$$

Ainsi la somme des conjugués $R_1 + \dots + R_d$ est l'intersection résiduelle d'une courbe de degré δ passant par les P_i et par D_0 avec les multiplicités indiquées.

Remerciements

Nous remercions très chaleureusement le professeur Marc Hindry de l'université Denis Diderot (Paris 7), pour nous avoir aidé à rédiger cette Note.

Nous remercions le Professeur Jean-Pierre Serre de l'Académie des Sciences de Paris pour ses remarques et ses suggestions.

Nous remercions le Ministre de l'Enseignement Supérieur, des Universités et des Centres universitaires Régionaux et de la Recherche Scientifique du Sénégal pour son appui dans le cadre des Fonds d'Impulsion pour la Recherche Scientifique et Technique (FIRST).

Références

- [1] E.F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, Math. Ann. 310 (1998) 447–471.
 [2] B. Gross, D. Rohrlich, Some results on the Mordell–Weil group of the Jacobian of the Fermat curve, Invent. Math. 44 (1978) 201–224.