

Algebraic points of degree at most 5 on the affine curve

$$y^2 = x^5 - 243$$

Abstract. In this work, we determine the set of algebraic points of degree at most 5 on the affine curve $y^2 = x^5 - 243$. This result extends a result of J.TH Mulholland who described in [2] the set of \mathbb{Q} -rational points on this curve.

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

1 Introduction

Let \mathcal{C} be a smooth algebraic curve defined over \mathbb{Q} . Let K be a numbers field. We note by $\mathcal{C}(K)$ the set of points of \mathcal{C} with coordinates in K and $\bigcup_{[K:\mathbb{Q}] \leq d} \mathcal{C}(K)$ the set of points of \mathcal{C} with coordinates in K of degree at most d over \mathbb{Q} .

The goal is to determine the set of algebraic points of given degree over \mathbb{Q} on the curve \mathcal{C} given by the affine equation

$$y^2 = x^5 - 243 \tag{1}$$

We denote by J the jacobian of \mathcal{C} and by $j(P)$ the class $[P - \infty]$ of $P - \infty$, that is to say that j is the Jacobian diving $\mathcal{C} \rightarrow J(\mathbb{Q})$. The Mordell-Weil group $J(\mathbb{Q})$ of rational points of the jacobian is a finite set (refer to [2]).

We denote by $P = (3, 0)$ et $\infty = (0, 1, 0)$. In [2], J.TH Mulholland gave a description of the rational points on \mathbb{Q} on this curve. This description is as follows :

Proposition. The rational points on \mathcal{C} are given by $\mathcal{C}(\mathbb{Q}) = \{\infty, P\}$.

In this note, we determine the set of algebraic points of degree at most five on the affine curve $y^2 = x^5 - 243$.

Our essential tools are :

- The Mordell-Weil group $J(\mathbb{Q})$ of rational points of the jacobian (refer to [2]),
- Abel Jacobi's theorem (refer to [1]),
- Linear systems on the curve \mathcal{C} .

Our main result is given by the following theorem :

Theorem.

1. The set of quadratic points on \mathcal{C} are given by

$$\mathcal{S} = \left\{ \left(\alpha, \pm \sqrt{\alpha^5 - 243} \right), \alpha \in \mathbb{Q} \right\}$$

2. The set of cubic points on \mathcal{C} is empty.

3. The set of quartic points on \mathcal{C} are given by $\mathcal{C}_1 \cup \mathcal{C}_2$ with

$$\mathcal{C}_1 = \left\{ \left(x, \pm \sqrt{\alpha^5 - 243} \right) \mid x \in \mathbb{Q}, [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ and } x \text{ root of} \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 \end{array} \right\}$$

4. The set of quintic points on \mathcal{C} are given by $\mathcal{A}_1 \cup \mathcal{A}_2$ with

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2 x + \alpha_3 x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ and } x \text{ root of} \\ B(x) = x^5 - \alpha_3^2 x^4 - 2\alpha_2 \alpha_3 x^3 - (\alpha_2^2 + 2\alpha_1 \alpha_2) x^2 - 2\alpha_1 \alpha_2 x - (\alpha_1^2 + 243) \end{array} \right\}$$

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)[n_1 + n_2(x+3) + n_3(x^2 + 3x + 9)]) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ and } x \text{ root of} \\ C(x) = (x-3)(n_1 + n_2(x+3) + n_3(x^2 + 3x + 9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}$$

2 Auxiliary results

For a divisor D on \mathcal{C} , we note $\mathcal{L}(D)$ the $\overline{\mathbb{Q}}$ -vector space of rational functions F defined on \mathbb{Q} such that $F = 0$ or $\text{div}(F) \geq -D$; $l(D)$ designates $\overline{\mathbb{Q}}$ - of $\mathcal{L}(D)$.

In [2], the Mordell-Weil group $J(\mathbb{Q})$ of \mathcal{C} is isomorph to $\mathbb{Z}/2\mathbb{Z}$ and \mathcal{C} is a hyperelliptic curve of genus $g = 2$. Let x, y be two rational functions on \mathbb{Q} defined as follow :

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

The projective equation of \mathcal{C} is

$$\mathcal{C} : Y^2 Z^3 = X^5 - 243 Z^5 = X^5 - (3Z)^5 \tag{2}$$

We denote by $\eta_1 = e^{i\frac{\pi}{2}}$ and let's put $A_k = (0, 81\sqrt{3}\eta_1^{2k+1})$ for $k \in \{0, 1\}$.

We denote by $\eta_2 = e^{i\frac{\pi}{5}}$ and let's put $B_k = (3\eta_2^{2k+1}, 0)$ for $k \in \{0, 1, 2, 3, 4\}$.

Let us designate by $\mathcal{D}.\mathcal{C}$ the intersection cycle of algebraic curve \mathcal{D} defined on \mathbb{Q} and \mathcal{C} .

Lemma 1.

- $div(x - 3) = 2P - 2\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(x) = A_0 + A_1 - 2\infty$

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

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

For $X = 3Z$, we have $Y^2 = 0$ with $Z = 1$ or $Z^3 = 0$ with $Y = 1$. We obtain the point $P = (3, 0, 1)$ with multiplicity 2 and the point $\infty = (0, 1, 0)$ with multiplicity 3. Hence $(X - 3Z = 0).\mathcal{C} = 2P + 3\infty$ (*).

Even if $Z = 0$, then $X^5 = 0$; and for $Y = 1$, we have the point $\infty = (0, 1, 0)$ with multiplicity 5. Hence $(Z = 0).\mathcal{C} = 5\infty$ (**).

The relations (*) and (**) implies that $div(x - 3) = 2P - 2\infty$.

- Similarly we show that $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$ and $div(x) = A_0 + A_1 - 2\infty$.

consequence of lemma 1 : $2j(P) = 0$.

Lemma 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 Results from lemma 1 and from the fact that according to the theorem of Riemann-Rock we have $l(m\infty) = m - 1$ as soon as $m \geq 3$.

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

Preuve Refer to [2].

3 Proof of theorem

3.1 Quadratic points on \mathcal{C}

The set of quadratic points on \mathcal{C} are given by

$$\mathcal{S} = \left\{ \left(\alpha, \pm \sqrt{\alpha^5 - 243} \right), \alpha \in \mathbb{Q} \right\}$$

Proof : Given $R \in \mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R] : \mathbb{Q}] = 2$. Note that R_1, R_2 are the Galois conjugates of R . Let's work with $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q})$, according to lemma 3 we have $t = a [P - \infty]$, $0 \leq a \leq 1$. So we have $[R_1 + R_2 - 2\infty] = a [P - \infty]$.

For $a = 0$, we have $[R_1 + R_2 - 2\infty] = 0$; then there exist a function F with coefficient in \mathbb{Q} such that $div(F) = R_1 + R_2 - 2\infty$, then $F \in \mathcal{L}(2\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x$ with $a_2 \neq 0$ otherwise one of the R_i should be ∞ .

For the points R_i , we have $a_1 + a_2x = 0$ hence $x = -\frac{a_1}{a_2} = \alpha \in \mathbb{Q}$.

By replacing x by α in (1), we have :

$$y^2 = \alpha^5 - 243 \tag{3}$$

and then we have

$$y = \pm\sqrt{\alpha^5 - 243} \tag{4}$$

So we find a family of quadratic points

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 - 243} \right), \alpha \in \mathbb{Q} \right\}$$

For $a = 1$, we have $[R_1 + R_2 + P - 3\infty] = 0$, then there exist a function F with coefficient in \mathbb{Q} such that $div(F) = R_1 + R_2 + P - 3\infty$, then $F \in \mathcal{L}(3\infty)$ and as $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ then one of the R_i should be equal to ∞ , we obtain a contradiction.

Conclusion : The set of quadratic points on \mathcal{C} are given by

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 - 243} \right), \alpha \in \mathbb{Q} \right\}$$

3.2 Cubic points on \mathcal{C}

There are no cubic points on \mathcal{C} .

Proof : Given $R \in \mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R] : \mathbb{Q}] = 3$. Note that R_1, R_2, R_3 are the Galois conjugates of R . Let's work with $t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q})$, according to lemma 3 we have $t = a[P - \infty]$, $0 \leq a \leq 1$. So we have $[R_1 + R_2 + R_3 - 3\infty] = a[P - \infty]$.

For $a = 0$, we have $[R_1 + R_2 + R_3 - 3\infty] = 0$; then there exist a function F with coefficient in \mathbb{Q} such that $div(F) = R_1 + R_2 + R_3 - 3\infty$, then $F \in \mathcal{L}(3\infty)$ and as $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ then one of the R_i should be equal to ∞ , we obtain a contradiction.

For $a = 1$, we have $[R_1 + R_2 + R_3 + P - 4\infty] = 0$, then there exist a function F with coefficient in \mathbb{Q} such that $div(F) = R_1 + R_2 + R_3 + P - 4\infty$, then $F \in \mathcal{L}(4\infty)$, then $F \in \mathcal{L}(2\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2$ with $a_3 \neq 0$ otherwise one of the R_i should be ∞ .

For the point P , we have $a_1 + 3a_2 + 9a_3 = 0$, so $a_1 = -3a_2 - 9a_3$ and replacing a_1 with its expression in $F(x, y)$ we have :

$$F(x, y) = -3a_2 - 9a_3 + a_2x + a_3x^2 \tag{5}$$

$$F(x, y) = a_2(x - 3) + a_3(x^2 - 9) \tag{6}$$

$$F(x, y) = (x - 3)[a_2 + a_3(x + 3)] \tag{7}$$

For the points R_i , we have $(x - 3)[a_2 + a_3(x + 3)] = 0$, then $x \in \mathbb{Q}$ and therefore the R_i should be of degree ≤ 2 .

Conclusion : The set of cubic points on \mathcal{C} is empty.

3.3 Quartic points on \mathcal{C}

The set of quartic points on \mathcal{C} are given by $\mathcal{C}_1 \cup \mathcal{C}_2$ with

$$\mathcal{C}_1 = \left\{ \left(x, \pm \sqrt{\alpha^5 - 243} \right) \mid x \in \mathbb{Q}, [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ and } x \text{ root of} \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 \end{array} \right\}$$

Proof : Given $R \in \mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R] : \mathbb{Q}] = 4$. Note that R_1, R_2, R_3, R_4 are the Galois conjugates of R . Let's work with $t = [R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q})$, according to lemma 3 we have $t = a[P - \infty]$, $0 \leq a \leq 1$. So we have $[R_1 + R_2 + R_3 + R_4 - 4\infty] = a[P - \infty]$. We have the following two cases :

For $a = 0$, we have $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 0$; then there exist a function F with coefficient in \mathbb{Q} such that $\text{div}(F) = R_1 + R_2 + R_3 + R_4 - 4\infty$, then $F \in \mathcal{L}(4\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2$ with $a_3 \neq 0$ otherwise one of the R_i should be ∞ .

For the points R_i , we have : $a_1 + a_2x + a_3x^2$; the relation $y^2 = x^5 - 243$ gives

$$y = \pm \sqrt{x^5 - 243}. \tag{8}$$

We find a family of quartic points

$$\mathcal{C}_1 = \left\{ \left(x, \pm \sqrt{x^5 - 243} \right) \mid x \in \mathbb{Q}, [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

For $a = 1$, we have $[R_1 + R_2 + R_3 + R_4 + P - 5\infty] = 0$; then there exist a function F with coefficient in \mathbb{Q} such that $\text{div}(F) = R_1 + R_2 + R_3 + R_4 + P - 5\infty$, then $F \in \mathcal{L}(5\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y$ with $a_4 \neq 0$.

For the point P , we have : $a_1 + 3a_2 + 9a_3 = 0$; $a_1 + 3a_2 + 9a_3 = 0$ so $a_1 = -3a_2 - 9a_3$ and replacing a_1 with its expression in $F(x, y)$ we have :

$$F(x, y) = -3a_2 - 9a_3 + a_2x + a_3x^2 + a_4y \tag{9}$$

$$F(x, y) = a_2(x-3) + a_3(x^2-9) + a_4y \tag{10}$$

$$F(x, y) = (x-3)(a_2 + a_3(x+3)) + a_4y \tag{11}$$

For the points R_i we have $(x-3)(a_2 + a_3(x+3)) + a_4y = 0$, so y is of the form $y = (x-3)(\lambda_1 + \lambda_2(x+3))$ with $\lambda_1, \lambda_2 \in \mathbb{Q}$.

The relation $y^2 = x^5 - 243 \Leftrightarrow (x-3)^2(\lambda_1 + \lambda_2(x+3))^2 = x^5 - 243$

$$(x-3)^2(\lambda_1 + \lambda_2(x+3))^2 = (x-3)(x^4 + 3x^3 + 9x^2 + 27x + 81) \tag{12}$$

Simplifying by $x-3$ and expanding we get

$$(x-3)(\lambda_1 + \lambda_2(x+1))^2 = x^4 + 3x^3 + 9x^2 + 27x + 81 \tag{13}$$

$$x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 = 0 \tag{14}$$

We find a family of quartic points

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, (x-3)(\lambda_1 + \lambda_2(x+3))) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ and } x \text{ root of} \\ A(x) = x^4 + 3x^3 + 9x^2 + 27x + 81 - (x-3)(\lambda_1 + \lambda_2(x+1))^2 \end{array} \right\}$$

Conclusion : The set of quartic points on \mathcal{C} are given by $\mathcal{C}_1 \cup \mathcal{C}_2$.

3.4 Quintic points on \mathcal{C}

The set of quintic points on \mathcal{C} are given by $\mathcal{A}_1 \cup \mathcal{A}_2$ with

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2x + \alpha_3x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ and } x \text{ root of} \\ B(x) = x^5 - \alpha_3^2x^4 - 2\alpha_2\alpha_3x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2x - (\alpha_1^2 + 243) \end{array} \right\}$$

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x-3)[n_1 + n_2(x+3) + n_3(x^2 + 3x + 9)]) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ and } x \text{ root of} \\ C(x) = (x-3)(n_1 + n_2(x+3) + n_3(x^2 + 3x + 9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}$$

Proof : Given $R \in \mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R] : \mathbb{Q}] = 5$. Note that R_1, R_2, R_3, R_4, R_5 are the Galois conjugates of R . Let's work with $t = [R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] \in J(\mathbb{Q})$, according to lemma 3 we have $t = a[P - \infty]$, $0 \leq a \leq 1$.

So we have $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = a[P - \infty]$.

We have the following two cases :

For $a = 0$, we have $[R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty] = 0$; then there exist a function F with coefficient in \mathbb{Q} such that $\text{div}(F) = R_1 + R_2 + R_3 + R_4 + R_5 - 5\infty$, then $F \in \mathcal{L}(5\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y$ with $a_4 \neq 0$.

For the points R_i , we have : $a_1 + a_2x + a_3x^2 + a_4y = 0$, so $y = \alpha_1 + \alpha_2x + \alpha_3x^2$ with $\alpha_1 = \frac{-a_1}{a_4}$, $\alpha_2 = \frac{-a_2}{a_4}$ **et** $\alpha_3 = \frac{-a_3}{a_4}$.

Replacing y by its expression in (1), we have

$$x^5 - 243 = \alpha_1^2 + \alpha_2^2x + \alpha_3^2x^4 + 2\alpha_1\alpha_2x + 2\alpha_1\alpha_3x^2 + 2\alpha_2\alpha_3x^3 \quad (15)$$

$$3x^5 - \alpha_3^2x^4 - 2\alpha_2\alpha_3x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2x - (\alpha_1^2 + 243) = 0 \quad (16)$$

We find a family of quintic points

$$\mathcal{A}_1 = \left\{ \begin{array}{l} (x, \alpha_1 + \alpha_2x + \alpha_3x^2) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}^* \text{ and } x \text{ root of} \\ B(x) = x^5 - \alpha_3^2x^4 - 2\alpha_2\alpha_3x^3 - (\alpha_2^2 + 2\alpha_1\alpha_2)x^2 - 2\alpha_1\alpha_2x - (\alpha_1^2 + 243) \end{array} \right\}$$

For $a = 1$, we have $[R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty] = 0$; then there exist a function F with coefficient in \mathbb{Q} such that $\text{div}(F) = R_1 + R_2 + R_3 + R_4 + R_5 + P - 6\infty$, then $F \in \mathcal{L}(6\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y + a_5x^3$ with $a_5 \neq 0$.

For the points R_i , we have : $a_1 + 3a_2 + 9a_3 + 27a_5 = 0$, so $a_1 = -3a_2 - 9a_3 - 27a_5$ and Replacing a_1 by its expression in $F(x, y)$, we have :

$$F(x, y) = -3a_2 - 9a_3 - 37a_5 + a_2x + a_3x^2 + a_4y + a_5x^3 \quad (17)$$

$$F(x, y) = a_2(x - 3) + a_3(x^2 - 9) + a_5(x^3 - 27) + a_4y \tag{18}$$

For the points R_i , we have : $a_2(x - 3) + a_3(x^2 - 9) + a_5(x^3 - 27) + a_4y = 0$, so y is of the form $y = n_1(x - 3) + n_2(x^2 - 9) + n_3(x^3 - 27)$ with $n_1, n_2, n_3 \in \mathbb{Q}^*$.

Finally we have :

$$y = (x - 3) (n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9)) \tag{19}$$

Replacing y by its expression in (1), we have :

$$(x - 3)^2 (n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9))^2 = x^5 - 243 \tag{20}$$

$$(x - 3)^2 (n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9))^2 = (x - 3)(x^4 + 3x^3 + 9x^2 + 27x + 81) \tag{21}$$

Simplifying by $x - 3$, we obtain

$$(x - 3) (n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) = 0 \tag{22}$$

Thus we find a family of quintic points

$$\mathcal{A}_2 = \left\{ \begin{array}{l} (x, (x - 3) [n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9)]) \mid n_1, n_2, n_3 \in \mathbb{Q}^* \text{ and } x \text{ root of} \\ C(x) = (x - 3) (n_1 + n_2(x + 3) + n_3(x^2 + 3x + 9))^2 - (x^4 + 3x^3 + 9x^2 + 27x + 81) \end{array} \right\}$$

Conclusion : The set of quintic points on \mathcal{C} are given by $\mathcal{A}_1 \cup \mathcal{A}_2$.

References

- [1] P. A. Griffiths, Introduction to algebraic curves , Translations of mathematical monographs volume 76. American Mathematical Society, Providence (1989).
- [2] J. TH. Mulholland, Elliptic curves with rational 2-torsion and related ternary Diophantine equations. ProQuest LLC. Ann Arbor, MI (2006).
- [3] O. Sall, Algebraic points on certain quotients of Fermat curves, C. R. Acad. Sci. Paris Ser. I 336 (2003) 117-120.
- [4] O. Sall, M. Fall, C. M. Coly, Algebraic points of given degree on the equation curve $y^2 = x^5 + 1$, International Journal Of Development Research Vol. 06, Issue, 11, pp. 10295-10300, November, 2016.