Alain Kraus

Quartic points on the Fermat quintic

Volume 25, n° 1 (2018), p. 199-205.

<http://ambp.cedram.org/item?id=AMBP_2018__25_1_199_0>

© Université Clermont Auvergne, Laboratoire de mathématiques Blaise Pascal, 2018, Certains droits réservés.

Cet article est mis à disposition selon les termes de la licence Creative Commons attribution – pas de modification 3.0 France.
http://creativecommons.org/licenses/by-nd/3.0/fr/

L’accès aux articles de la revue « Annales mathématiques Blaise Pascal » (http://ambp.cedram.org/), implique l’accord avec les conditions générales d’utilisation (http://ambp.cedram.org/legal/).

Publication éditée par le laboratoire de mathématiques Blaise Pascal de l’université Clermont Auvergne, UMR 6620 du CNRS
Clermont-Ferrand — France

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/
Quartic points on the Fermat quintic

Alain Kraus

Abstract

We study the algebraic points of degree 4 over $\mathbb{Q}$ on the Fermat curve $F_5/\mathbb{Q}$ of equation $x^5+y^5+z^5 = 0$. A geometrical description of these points has been given in 1997 by Klassen and Tzermias. Using their result, as well as Bruin’s work about diophantine equations of signature $(5, 5, 2)$, we give here an algebraic description of these points. In particular, we prove there is only one Galois extension of $\mathbb{Q}$ of degree 4 that arises as the field of definition of a non-trivial point of $F_5$.

1. Introduction

Let us denote by $F_5$ the quintic Fermat curve over $\mathbb{Q}$ given by the equation

$$x^5 + y^5 + z^5 = 0.$$ 

Let $P$ be a point in $F_5(\overline{\mathbb{Q}})$. The degree of $P$ is the degree of its field of definition over $\mathbb{Q}$. Write $P = (x, y, z)$ for the projective coordinates of $P$. It is said to be non-trivial if $xyz \neq 0$. Let $\zeta$ be a primitive cubic root of unity and

$$a = (0, -1, 1), \quad b = (-1, 0, 1), \quad c = (-1, 1, 0)$$

$$w = (\zeta, \zeta^2, 1), \quad \overline{w} = (\zeta^2, \zeta, 1).$$

It is well known that $F_5(\mathbb{Q}) = \{a, b, c\}$. In 1978, Gross and Rohrlich have proved that the only quadratic points of $F_5$ are $w$ and $\overline{w}$ [2, Theorem 5.1]. In 1997, by proving that the group of $\mathbb{Q}$-rational points of the Jacobian of $F_5$ is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$, and by explicit generators, Klassen and Tzermias have described geometrically all the points of $F_5$ whose degrees are less than 6 in [4, Theorem 1]. I mention that Top and Sall have

I thank D. Bernardi for his remarks during the writing of this paper, as well as the referee for his suggestions.

Keywords: Fermat quintic, number fields, rational points.

2010 Mathematics Subject Classification: 11D41, 11G30.

199
A. Kraus

pushed further this description for points of $F_5$ of degrees less than 12 in [5]. In particular, Klassen and Tzermias have proved that $F_5$ has no cubic points and they have established the following statement:

**Theorem 1.1.** The points of degree 4 of $F_5$ arise as the intersection of $F_5$ with a rational line passing through exactly one of points $a, b, c$.

Using this result, and Bruin’s work about the diophantine equations $16x^5 + y^5 = z^2$ and $4x^5 + y^5 = z^2$ [1, 3], we propose in this paper to give an algebraic description of the non-trivial quartic points of $F_5$.

2. **Statement of the results**

Let $K$ be a number field of degree 4 over $\mathbb{Q}$.

**Theorem 2.1.** Suppose that $F_5(K)$ has a non-trivial point of degree 4. One of the following conditions is satisfied:

1. the Galois closure of $K$ is a dihedral extension of $\mathbb{Q}$ of degree 8.

2. One has

\[ K = \mathbb{Q}(\alpha) \quad \text{with} \quad 31\alpha^4 - 36\alpha^3 + 26\alpha^2 - 36\alpha + 31 = 0. \]  

The extension $K/\mathbb{Q}$ is cyclic. Up to Galois conjugation and permutation, $(2, 2\alpha, -\alpha - 1)$ is the only non-trivial point in $F_5(K)$.

As a direct consequence of [2, Theorem 5.1] and the previous Theorem, we obtain:

**Corollary 2.2.** Suppose that $K$ does not satisfy one of the two conditions above. The set of non-trivial points of $F_5(K)$ is contained in $\{w, w\}$.

All that follows is devoted to the proof of Theorem 2.1.

3. **Preliminary results**

Let $P = (x, y, z) \in F_5(K)$ be a non-trivial point of degree 4. By permuting $x, y, z$ if necessary, we can suppose that $P$ belongs to a $\mathbb{Q}$-rational line $\mathcal{L}$ passing through $a = (0, -1, 1)$ (Theorem 1.1). Moreover, $P$ being non-trivial we shall assume

\[ z = 1. \]  

(3.1)
Lemma 3.1. One has $K = \mathbb{Q}(y)$. There exists $t \in \mathbb{Q}$, $t \neq -1$, such that
\[ y^4 + uy^3 + (u + 2)y^2 + uy + 1 = 0 \quad \text{with} \quad u = \frac{4t^5 - 1}{t^5 + 1}, \] (3.2)
\[ x = t(y + 1). \] (3.3)

Proof. The equation of the tangent line to $F_5$ at the point $a$ is $Y + Z = 0$. Since $x \neq 0$, it is distinct from $\mathcal{L}$. According to (3.1), it follows there exists $t \in \mathbb{Q}$ such that
\[ x = t(y + 1). \]

In particular, one has $K = \mathbb{Q}(y)$. Furthermore, one has
\[ t \neq -1. \] (3.4)

Indeed, if $t = -1$, the equalities $x + y + 1 = 0$ and $x^5 + y^5 + 1 = 0$ imply
\[ x(x + 1)(x^2 + x + 1) = 0. \]

Since $P$ is non-trivial, one has $x(x + 1) \neq 0$, so $x^2 + x + 1 = 0$. This leads to $P = w$ or $P = \overline{w}$, which contradicts the fact that $P$ is not a quadratic point, and proves (3.4).

From the equalities (3.3) and $x^5 + y^5 + 1 = 0$, as well as the condition $y \neq -1$, we then deduce the Lemma. \hfill \Box

Let $G$ be the Galois group of the Galois closure of $K$ over $\mathbb{Q}$. Let us denote by $|G|$ the order of $G$.

Lemma 3.2.

(1) One has $|G| \in \{4, 8\}$.

(2) Suppose that $|G| = 4$. One of the two following conditions is satisfied:
\[ 5(16t^5 + 1) \text{ is a square in } \mathbb{Q}. \] (3.5)
\[ (1 - 4t^5)(16t^5 + 1) \text{ is a square in } \mathbb{Q}. \] (3.6)

Proof. Let us denote
\[ f = X^4 + uX^3 + (u + 2)X^2 + uX + 1 \]

in $\mathbb{Q}[X]$. One has $f(y) = 0$ (Lemma 3.1). Let $\varepsilon \in \overline{\mathbb{Q}}$ such that
\[ \varepsilon^2 = u^2 - 4u. \]

The element $y + \frac{1}{\varepsilon}$ is a root of the polynomial $X^2 + uX + u$. So we have the inclusion
\[ \mathbb{Q}(\varepsilon) \subseteq K. \] (3.7)
Moreover, we have the equality

\[ f = \left( X^2 + \frac{u - \varepsilon}{2} X + 1 \right) \left( X^2 + \frac{u + \varepsilon}{2} X + 1 \right). \]  

(3.8)

Since \( K = \mathbb{Q}(y) \) and \([K : \mathbb{Q}] = 4\), we have

\[ [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2. \]  

(3.9)

From (3.8), we deduce that the roots of \( f \) belong to at most two quadratic extensions of \( \mathbb{Q}(\varepsilon) \). The equality (3.9) then implies \(|G| \leq 8\). Since 4 divides \(|G|\), this proves the first assertion.

Henceforth let us suppose \(|G| = 4\), i.e. the extension \( K/\mathbb{Q} \) is Galois. Let \( \Delta \) be the discriminant of \( f \). One has the equalities

\[ \Delta = -u^2(u - 4)^3(3u + 4) = 5^3 \frac{(4t^5 - 1)^2(16t^5 + 1)}{(t^5 + 1)^6}. \]  

(3.10)

Let us prove that

\[ \Delta \text{ is a square in } \mathbb{Q}(\varepsilon). \]  

(3.11)

From (3.8) and our assumption, the roots of the polynomials

\[ X^2 + \frac{u - \varepsilon}{2} X + 1 \quad \text{and} \quad X^2 + \frac{u + \varepsilon}{2} X + 1 \]

belong to \( K \), which is a quadratic extension of \( \mathbb{Q}(\varepsilon) \) ((3.7) and (3.9)). Therefore, the product of their discriminants

\[ \left( \left( \frac{u - \varepsilon}{2} \right)^2 - 4 \right) \left( \left( \frac{u + \varepsilon}{2} \right)^2 - 4 \right) \quad \text{i.e.} \quad -(u - 4)(3u + 4) \]

must be a square in \( \mathbb{Q}(\varepsilon) \). The first equality of (3.10) then implies (3.11).

Suppose that the condition (3.5) is not satisfied. From the second equality of (3.10), we deduce that \( \Delta \) is not a square in \( \mathbb{Q} \). It follows from (3.11) that we have

\[ \mathbb{Q} \left( \sqrt{\Delta} \right) = \mathbb{Q}(\varepsilon). \]

Therefore, \( \Delta(u^2 - 4u) \) is a square in \( \mathbb{Q} \), in other words, such is the case for \(-u(3u + 4)\). One has the equality

\[ -u(3u + 4) = \frac{(1 - 4t^5)(16t^5 + 1)}{(t^5 + 1)^2}. \]

This implies the condition (3.6) and proves the Lemma. \( \square \)
4. **The curve $C_1/\mathbb{Q}$**

Let us denote by $C_1/\mathbb{Q}$ the curve, of genus 2, given by the equation

$$Y^2 = 5(16X^5 + 1).$$

**Proposition 4.1.** The set $C_1(\mathbb{Q})$ is empty.

**Proof.** Suppose there exists a point $(X, Y) \in C_1(\mathbb{Q})$. Let $Z = \frac{Y}{5}$. We obtain

$$5Z^2 = 16X^5 + 1. \quad (4.1)$$

Let $a$ and $b$ be coprime integers, with $b \in \mathbb{N}$, such that

$$X = \frac{a}{b}. \quad (4.2)$$

Let us prove there exists $c \in \mathbb{N}$ such that

$$b = 5c^2. \quad (4.3)$$

For every prime number $p$, let $v_p$ be the $p$-adic valuation over $\mathbb{Q}$. If $p$ is a prime number dividing $b$, distinct from 2, 5, one has

$$2v_p(Z) = -5v_p(b),$$

consequently

$$v_p(b) \equiv 0 \mod 2. \quad (4.3)$$

Moreover, one has $v_2(X) < 0$ (5 is not a square modulo 8), so

$$4 - 5v_2(b) = 2v_2(Z).$$

In particular, one has

$$v_2(b) \equiv 0 \mod 2. \quad (4.4)$$

Let us verify the congruence

$$v_5(b) \equiv 1 \mod 2. \quad (4.5)$$

One has $v_5(X) \leq 0$. Suppose $v_5(X) = 0$. In this case, one has $X^5 \equiv \pm 1, \pm 7 \mod 25$. The equality $(4.1)$ implies $X^5 \equiv -1 \mod 25$ and $Z^2 \equiv 2 \mod 5$, which leads to a contradiction. Therefore, we have $1 + 2v_5(Z) = -5v_5(b)$, which proves $(4.5)$.

The conditions $(4.3)$, $(4.4)$ and $(4.5)$ then imply $(4.2)$.

We deduce from $(4.1)$ and $(4.2)$ the equality

$$16a^5 + b^5 = d^2 \quad \text{with} \quad d = 5^3c^5Z.$$ 

One has $ab \neq 0$. From the informations given in the Appendix of [3], this implies

$$(a, b, d) = (-1, 2, \pm 4).$$

We obtain $X = -1/2$, which is not the abscissa of a point of $C_1(\mathbb{Q})$, hence the result. \(\square\)
5. The curve $C_2/\mathbb{Q}$

Let us denote by $C_2/\mathbb{Q}$ the curve, of genus 4, given by the equation

$$Y^2 = (1 - 4X^5)(16X^5 + 1).$$

**Proposition 5.1.** One has

$$C_2(\mathbb{Q}) = \{(0, \pm 1), (-1/2, \pm 3/4)\}.$$

**Proof.** Let $(X, Y)$ be a point of $C_2(\mathbb{Q})$. Let $a$ and $b$ be coprime integers such that

$$X = \frac{a}{b}.$$

We obtain the equality

$$(Yb^5)^2 = (b^5 - 4a^5)(16a^5 + b^5). \tag{5.1}$$

Therefore, $(b^5 - 4a^5)(16a^5 + b^5)$ is the square of an integer. Moreover, $b^5 - 4a^5$ and $16a^5 + b^5$ are coprime apart from 2 and 5. So, changing $(a, b)$ by $(-a, -b)$ if necessary, there exists $d \in \mathbb{N}$ such that

$$b^5 - 4a^5 \in \{d^2, 2d^2, 5d^2, 10d^2\}.$$

Suppose $b^5 - 4a^5 \in \{2d^2, 10d^2\}$. In this case, $b$ must be even, therefore $v_2(2d^2) = 2$, which is not.

Suppose $b^5 - 4a^5 = d^2$. One has $b \neq 0$. It then comes from [3] that

$$a = 0 \quad \text{or} \quad (a, b, d) = (-1, 2, \pm 6).$$

We obtain $X = 0$ or $X = -1/2$, which leads to the announced points in the statement.

Suppose $b^5 - 4a^5 = 5d^2$. It follows from (5.1) that there exists $c \in \mathbb{N}$ such that

$$16a^5 + b^5 = 5c^2.$$ Since $a$ and $b$ are coprime, 5 does not divide $ab$. We then directly verify that the two equalities $b^5 - 4a^5 = 5d^2$ and $16a^5 + b^5 = 5c^2$ do not have simultaneously any solutions modulo 25, hence the result. \hfill $\square$

6. End of the proof of Theorem 2.1

The group $G$ is isomorphic to a subgroup of the symmetric group $S_4$ and one has $|G| = 4$ or $|G| = 8$ (Lemma 3.2). In case $|G| = 8$, $G$ is isomorphic to a 2-Sylow subgroup of $S_4$, that is dihedral.

Suppose $|G| = 4$ and let us prove the assertion 2 of the Theorem.

First, we directly verify that the extension $K/\mathbb{Q}$ defined by the condition (2.1) is cyclic of degree 4, and that the point $(2, 2\alpha, -\alpha - 1)$ belongs to $F_5(K)$.  

204
Conversely, from the Proposition 4.1, the condition (3.5) of the Lemma 3.2 is not satisfied. The condition (3.6) and the Proposition 5.1 imply that \( t = 0 \) or \( t = -1/2 \). The case \( t = 0 \) is excluded because \( P \) is non-trivial. With the condition (3.2), we obtain

\[
u = -\frac{36}{31}.
\]

Thus, necessarily \( y \) is a root of the polynomial \( 31X^4 - 36X^3 + 26X^2 - 36X + 31 \), in other words \( y \) is a conjugate over \( \mathbb{Q} \) of \( \alpha \). The equality (3.3),

\[
x = -\frac{y + 1}{2}
\]

then implies the result.

References

[1] Nils Bruin. *Chabauty methods and covering techniques applied to generalised Fermat equations*. PhD thesis, Leiden University, Nederland, 1999.

[2] Benedict H. Gross and David E. Rohrlich. Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. *Invent. Math.*, 44(3):201–224, 1978.

[3] Wilfrid Ivorra. Sur les équations \( x^p + 2\beta y^p = z^2 \) et \( x^p + 2\beta y^p = 2z^2 \). *Acta Arith.*, 108(4):327–338, 2003.

[4] Matthew Klassen and Pavlos Tzermias. Algebraic points of low degree on the Fermat quintic. *Acta Arith.*, 82(4):393–401, 1997.

[5] Thiéyacine Top and Oumar Sall. Points algébriques de degrés au plus 12 sur la quintique de Fermat. *Acta Arith.*, 169(4):385–395, 2015.