POINTS TOTALEMENT RÉELS DE LA COURBE $x^5 + y^5 + z^5 = 0$

ALAIN KRAUS

RÉSUMÉ. Soient $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et $\mathbb{Q}^{tr}$ le sous-corps de $\overline{\mathbb{Q}}$ formé de la réunion des corps de nombres totalement réels. Pour tout nombre premier $p \geq 5$, soit $F_p/\mathbb{Q}$ la courbe de Fermat d'équation $x^p + y^p + z^p = 0$. En 1996, Pop a démontré que le corps $\mathbb{Q}^{tr}$ est large. En particulier, l'ensemble $F_p(\mathbb{Q}^{tr})$ des points de F_p rationnels sur $\mathbb{Q}^{tr}$ est infini. Comment expliciter des points non triviaux ($xyz \neq 0$) de $F_p(\mathbb{Q}^{tr})$? Il semble que les seuls points déjà connus de $F_p(\mathbb{Q}^{tr})$ soient ceux de $F_p(\mathbb{Q})$ et ils sont triviaux. Dans cet article, on s'intéresse à cette question dans le cas où $p = 5$. Il n'existe pas de corps totalement réels de degré sur $\mathbb{Q}$ au plus 5 sur lesquels F_5 a des points non triviaux. On se propose ici d'expliciter une infinité de points de F_5 rationnels sur des corps totalement réels de degré 6 sur $\mathbb{Q}$.

ABSTRACT. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $\mathbb{Q}^{tr}$ be the subfield of $\overline{\mathbb{Q}}$ obtained by taking the union of all totally real number fields. For any prime $p \geq 5$, let $F_p/\mathbb{Q}$ be the Fermat curve of equation $x^p + y^p + z^p = 0$. In 1996, Pop has shown that the field $\mathbb{Q}^{tr}$ is large. In particular, the set $F_p(\mathbb{Q}^{tr})$ of the points of F_p rational over $\mathbb{Q}^{tr}$ is infinite. How to explicit non-trivial points ($xyz \neq 0$) in $F_p(\mathbb{Q}^{tr})$? It seems that the only points already known in $F_p(\mathbb{Q}^{tr})$ are those of $F_p(\mathbb{Q})$ and they are trivial. In this paper, we investigate this question in case $p = 5$. There are no totally real fields whose degree over $\mathbb{Q}$ is at most 5 over which F_5 has non-trivial points. We propose here to explicit infinitely many points of F_5 rational over totally real fields of degree 6 over $\mathbb{Q}$.

1. INTRODUCTION

Soit $p \geq 5$ un nombre premier. Notons $F_p/\mathbb{Q}$ la courbe de Fermat d'équation

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

Un point $[x, y, z]$ de $F_p(\overline{\mathbb{Q}})$ est dit non trivial si $xyz \neq 0$.

Notons $\mathbb{Q}^{tr}$ la réunion des corps de nombres totalement réels dans $\overline{\mathbb{Q}}$. Wiles a établi en 1994 que $F_p(\mathbb{Q})$ est réduit aux points triviaux ([11]). Depuis, il a été démontré, pour des familles infinies de corps K totalement réels, que $F_p(K)$ est réduit aux points triviaux si p est assez grand fonction de K (voir par exemple [3]). Cela étant, le corps $\mathbb{Q}^{tr}$ est large ([8], page 2) et $F_p(\mathbb{Q})$ n'est pas vide. Par suite, l'ensemble $F_p(\mathbb{Q}^{tr})$ est infini.

Problème. Comment expliciter des points non triviaux de $F_p(\mathbb{Q}^{tr})$?

Date: 15 janvier 2024.

2020 *Mathematics Subject Classification.* 11D41 - 11Y40 - 12F05.

Mots-clés. Équation de Fermat - Corps de nombres - Points totalement réels - Coniques.

À ma connaissance, ce problème est ouvert. Il ne semble pas qu'un point non trivial de $F_p(\mathbb{Q}^{tr})$ ait déjà été explicité.

On aborde ici ce problème dans le cas où $p = 5$. Soit ζ_3 une racine primitive cubique de l'unité. D'après les travaux de Gross et Rohrlich, les seuls points quadratiques de F_5 sont ([5], Theorem 5.1)

$$P = [\zeta_3, \zeta_3^2, 1] \quad \text{et} \quad \overline{P} = [\zeta_3^2, \zeta_3, 1]. \tag{1.1}$$

Par ailleurs, Klassen et Tzermias ont démontré qu'il n'existe pas de points cubiques sur F_5, et que les points de F_5 de degré 4 ou 5 sur $\mathbb{Q}$ s'obtiennent comme l'intersection de F_5 avec une droite définie sur $\mathbb{Q}$ ([6], Theorem 1). On en déduit, avec un résultat de [7], qu'il n'existe pas de points de F_5 dont le corps de rationalité soit totalement réel de degré 4 sur $\mathbb{Q}$. Siksek m'avait fait remarquer que l'on peut déduire directement de [6] la même conclusion pour les points de F_5 de degré 5 sur $\mathbb{Q}$. Ainsi, il n'existe pas de corps totalement réels, de degré au plus 5 sur $\mathbb{Q}$, sur lesquels F_5 a des points non triviaux. On justifie cette assertion dans l'Appendice de cet article (paragraphe 7).

On explicite ici une infinité de points de F_5 qui sont rationnels sur des corps totalement réels de degré 6 sur $\mathbb{Q}$. Pour cela, on utilise la description géométrique des points de F_5 de degré 6 faite par Klassen et Tzermias dans [6]. Ils établissent que ces points s'obtiennent comme l'intersection de F_5 avec quatre familles de coniques planes sur $\mathbb{Q}$ (*loc. cit.*, Theorem 1). On décrit dans le paragraphe 3 la famille des coniques planes sur $\mathbb{Q}$, irréductibles sur $\mathbb{Q}$, passant par P et ayant comme tangente en P celle de F_5 en P. En déterminant l'intersection de ces coniques avec F_5, on démontre qu'il existe une infinité de corps totalement réels, galoisiens sur $\mathbb{Q}$ de degré 6, de groupe de Galois isomorphe à $\mathfrak{S}_3$, sur lesquels F_5 a un point non trivial.

Tous les calculs numériques que ce travail a nécessités ont été effectués à l'aide des logiciels de calculs `Pari-gp` ([9]) et `Magma` ([1]). Il se trouve dans [4], un fichier `Magma` qui a été écrit par Nuno Freitas, ainsi qu'un fichier `Pari-gp`, permettant de vérifier ces calculs.

Je remercie vivement Nicolas Billerey et Nuno Freitas pour les remarques dont ils m'ont fait part au cours de ce travail, ainsi que pour l'aide informatique qu'ils m'ont apportée.

2. Énoncé des résultats

Dans toute la suite, la lettre t désigne un nombre rationnel distinct de 2. Posons

$$u = \frac{3t^2 - 2t + 2}{t^2 + t - 1}, \quad v = \frac{t^5 - 5t^4 + 10t^3 - 20t^2 + 15t - 7}{(t-2)(t^2 + t - 1)^2},$$

$$w = \frac{-3t^5 + 10t^4 - 20t^3 + 20t^2 - 20t + 6}{(t-2)(t^2 + t - 1)^2}.$$

Notons f_t le polynôme de $\mathbb{Q}[X]$ défini par l'égalité

$$f_t = X^6 + uX^5 + vX^4 + wX^3 + vX^2 + uX + 1. \tag{2.1}$$

Posons par ailleurs

$$s = (t^4 - 3t^3 - t^2 + 3t + 1)(t-2) \quad (\text{on a} \;\; s \neq 0),$$

$$a_0 = -\frac{(t^2+1)(t^3-t^2+2t-3)}{s}, \quad a_1 = -\frac{3t^7-9t^6+16t^5-15t^4+10t^3-11t^2+8t-7}{(t^2+t-1)s},$$

$$a_2 = \frac{2t^8-14t^7+52t^6-99t^5+100t^4-54t^3+38t^2-44t+13}{(t^2+t-1)(t-2)s},$$

$$a_3 = \frac{t^8+t^7-21t^6+65t^5-90t^4+78t^3-57t^2+32t-15}{(t^2+t-1)(t-2)s},$$

$$a_4 = -\frac{2t^5-6t^4+13t^3-14t^2+7t-5}{s}, \quad a_5 = -\frac{(t^2+t-1)(t^3-t^2+2t-3)}{s}.$$

Désignons par K_t le corps de décomposition de f_t dans $\overline{\mathbb{Q}}$. Soit $\alpha \in K_t$ une racine de f_t. On a $\alpha \neq 0$. Posons

$$\beta = \sum_{i=0}^{5} a_i \alpha^i \quad \text{et} \quad \gamma = \sum_{i=0}^{5} a_i (1/\alpha)^i. \tag{2.2}$$

Théorème 1. *Supposons $t \neq 1$.*

1) *Le polynôme $f_t \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$.*
2) *L'ensemble des six racines de f_t dans K_t est*

$$\{\alpha, \beta, \gamma, 1/\alpha, 1/\beta, 1/\gamma\}.$$

En particulier, on a $K_t = \mathbb{Q}(\alpha)$ et l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de degré 6. Son groupe de Galois sur $\mathbb{Q}$ est isomorphe à $\mathfrak{S}_3$.

3) *Les points*

$$[\alpha, \beta, 1], \quad [1/\alpha, \gamma, 1] \quad \textit{et} \quad [1/\gamma, 1/\beta, 1]$$

appartiennent à $F_5(K_t)$. Ils sont distincts et non triviaux.

Théorème 2. *Soit r le nombre réel tel que $7r^5 - 10r^4 - 20r^3 - 4 = 0$. On a $r \simeq 2,558\cdots$.*

1) *Le corps K_t est totalement réel si et seulement si on a $2 < t < r$.*
2) *Il existe une infinité de nombres rationnels t tels que $2 < t < r$ et que les corps K_t soient deux à deux distincts.*

On en déduit l'énoncé suivant :

Corollaire 1. *Il existe une infinité de corps de nombres K totalement réels, galoisiens sur $\mathbb{Q}$ de degré 6, de groupe de Galois sur $\mathbb{Q}$ isomorphe à $\mathfrak{S}_3$, tels que $F_5(K)$ possède un point non trivial.*

Exemple. Prenons $t = 5/2$. On a

$$f_t = X^6 + \frac{63}{31}X^5 - \frac{1149}{961}X^4 - \frac{4283}{961}X^3 - \frac{1149}{961}X^2 + \frac{63}{31}X + 1.$$

Le corps $\mathbb{Q}(\alpha)$ est totalement réel et on a

$$\alpha^5 + \beta^5 + 1 = 0 \quad \text{avec} \quad \beta = \frac{2821}{89}\alpha^5 + \frac{2850}{89}\alpha^4 - \frac{196815}{2759}\alpha^3 - \frac{188718}{2759}\alpha^2 + \frac{90989}{2759}\alpha + \frac{2639}{89}.$$

3. La conique $C_t/\mathbb{Q}$

Rappelons que les points P et $\overline{P}$ sont définis par les égalités (1.1). Décrivons la famille des coniques projectives planes sur $\mathbb{Q}$, irréductibles sur $\mathbb{Q}$, passant par P et ayant comme tangente en P celle de F_5 en P.

Soit $\mathcal{C}$ une conique projective plane définie sur $\mathbb{Q}$. Il existe a, b, c, d, e, f dans $\mathbb{Q}$ tels que $\mathcal{C}$ possède une équation de la forme

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$

Proposition 1. *1) Supposons que $\mathcal{C}$ soit irréductible sur $\mathbb{Q}$ et que P appartienne à $\mathcal{C}$. Alors, P est lisse.*

2) Les deux conditions suivantes sont équivalentes :

2.1) La conique $\mathcal{C}$ est irréductible sur $\mathbb{Q}$, le point P appartient à $\mathcal{C}$ et la tangente à $\mathcal{C}$ en P est celle de F_5 en P.

2.2) On a

$$a = b = c, \quad d = e = f \quad \text{et} \quad d \neq 2a. \tag{3.1}$$

Démonstration. Notons F le polynôme homogène de degré 2 définissant $\mathcal{C}$ et F_x, F_y, F_z ses polynômes dérivés par rapport à x, y et z.

1) On a les égalités

$$F_x(P) = 2a\zeta_3 + d\zeta_3^2 + e, \quad F_y(P) = 2b\zeta_3^2 + d\zeta_3 + f, \quad F_z(P) = 2c + e\zeta_3 + f\zeta_3^2. \tag{3.2}$$

Supposons que l'on ait $F_x(P) = F_y(P) = F_z(P) = 0$. En utilisant l'égalité, $\zeta_3^2 = -1 - \zeta_3$, on obtient les conditions $a = b = c$, $e = d = f$ et $d = 2a$. Par suite, on a $F = a(x + y + z)^2$, or $\mathcal{C}$ est irréductible sur $\mathbb{Q}$, d'où une contradiction et l'assertion.

2) Supposons que la condition 2.1 soit satisfaite. D'après l'assertion précédente, l'équation de la tangente à $\mathcal{C}$ en P est

$$F_x(P)x + F_y(P)y + F_z(P)z = 0.$$

L'équation de la tangente à F_5 en P est

$$\zeta_3 x + \zeta_3^2 y + z = 0.$$

D'après l'hypothèse faite, il existe donc $\lambda \in \overline{\mathbb{Q}}^*$ tel que

$$\lambda(\zeta_3, \zeta_3^2, 1) = (F_x(P), F_y(P), F_z(P)).$$

On obtient $\lambda = F_z(P)$, d'où

$$\zeta_3 F_z(P) = F_x(P) \quad \text{et} \quad \zeta_3^2 F_z(P) = F_y(P).$$

On en déduit avec (3.2) que l'on a

$$-2a + d - e + 2c = 0 \quad \text{et} \quad d - 2e + f = 0,$$

$$-d - 2c + f + 2b = 0 \quad \text{et} \quad e - 2c - f + 2b = 0.$$

La différence entre les deux dernières égalités implique la relation $e - 2f + d = 0$. Avec l'égalité $d - 2e + f = 0$, on obtient alors $e = f = d$, puis $a = b = c$. De plus, on a $d \neq 2a$, sinon $F = a(x + y + z)^2$, ce qui n'est pas, d'où la condition (3.1).

Inversement, supposons que la condition 2.2 soit satisfaite. On vérifie que $\mathcal{C}$ est irréductible sur $\overline{\mathbb{Q}}$ si et seulement si on a $(2a-d)(a+d) \neq 0$ i.e. $a+d \neq 0$ (cf. [10], Chapter III, Theorem 6.1). Par suite, si $a+d \neq 0$, alors $\mathcal{C}$ est en particulier irréductible sur $\mathbb{Q}$. Si $a+d=0$, l'équation de $\mathcal{C}$ est $x^2+y^2+z^2-(xy+xz+yz)=0$, et on constate avec [9] que $\mathcal{C}$ est irréductible sur $\mathbb{Q}$ ($\mathcal{C}$ est la réunion de deux droites définies sur $\mathbb{Q}(\zeta_3)$). Par ailleurs, on a $d \neq 2a$, donc P est un point lisse de $\mathcal{C}$ et la tangente à $\mathcal{C}$ en P est celle de F_5 en P, d'où la condition 2.1. □

Remarque 3.3. Les points P et $\overline{P}$ étant conjugués sur $\mathbb{Q}$, si la condition 2.1 est satisfaite, alors $\overline{P}$ est un point lisse de $\mathcal{C}$ et la tangente à $\mathcal{C}$ en $\overline{P}$ est celle de F_5 en $\overline{P}$.

La détermination de l'intersection de F_5 avec la famille de coniques vérifiant la condition (3.1) fournit ainsi, génériquement, des points de F_5 rationnels sur des corps de degré 6 sur $\mathbb{Q}$ ([6], Theorem 1). Afin de démontrer les résultats que l'on a en vue, on se limitera au cas où $a \neq 0$, l'équation de ces coniques étant alors de la forme $x^2+y^2+z^2+t(xy+xz+yz)=0$ avec $t \in \mathbb{Q}$ et $t \neq 2$. En fait, on constate avec la démonstration du théorème 1 que, si t est distinct de 1, ces coniques ont avec F_5 un contact d'ordre 2 en P et $\overline{P}$.

Pour tout nombre rationnel $t \neq 2$, notons désormais C_t la conique définie sur $\mathbb{Q}$ d'équation

$$x^2+y^2+z^2+t(xy+xz+yz)=0. \tag{3.4}$$

4. L'intersection $F_5 \cap C_t$

On vérifie que l'intersection de la droite d'équation $z=0$ avec $F_5 \cap C_t$ est vide. Décrivons $F_5 \cap C_t$ dans l'ouvert $z=1$.

Rappelons que, pour $t \neq 2$, le polynôme $f_t \in \mathbb{Q}[X]$ est défini par l'égalité (2.1) et que les nombres rationnels a_i (fonctions de t) ont été définis dans le paragraphe 2. La proposition qui suit n'est pas indispensable pour établir nos résultats, mais elle permet de comprendre comment l'énoncé du théorème 1 a été trouvé. On utilisera dans la suite seulement la proposition 3 ci-dessous.

Proposition 2. *Soit $[x,y,1]$ un point de $F_5 \cap C_t$, distinct de P et $\overline{P}$. On a*

$$f_t(x)=0 \quad \textit{et} \quad y=\sum_{i=0}^{5} a_i x^i. \tag{4.1}$$

Démonstration. Compte tenu de l'équation (3.4), considérons le résultant $R_t \in \mathbb{Q}[X]$ par rapport à Y des polynômes de $\mathbb{Q}[X,Y]$

$$X^5+Y^5+1 \quad \text{et} \quad X^2+Y^2+1+t(XY+X+Y).$$

On a l'égalité (cf. [9])

$$R_t=(2-t)(t^2+t-1)^2(X^2+X+1)^2 f_t.$$

Le point $[x,y,1]$ étant distinct de P et $\overline{P}$, x n'est pas ζ_3 ni ζ_3^2. On en déduit que l'on a

$$f_t(x)=0.$$

Par ailleurs, on a

$$y^2=-1-x^2-t(xy+x+y).$$

Cette égalité permet d'exprimer y^5 comme un polynôme de degré 1 en y, dont les coefficients dépendent de x et t. En utilisant les relations

$$x^5 + y^5 + 1 = 0 \quad \text{et} \quad f_t(x) = 0,$$

on constate alors que y vérifie la seconde égalité de (4.1) (voir [4]), d'où le résultat. □

Proposition 3. *Soit x un élément de $\overline{\mathbb{Q}}$ tel que $f_t(x) = 0$. Posons*

$$y = \sum_{i=0}^{5} a_i x^i.$$

Alors, on a $f_t(y) = 0$ et le point $[x, y, 1]$ appartient à $F_5 \cap C_t$.

Démonstration. On vérifie directement cet énoncé en utilisant [4]. □

5. Démonstration du Théorème 1

5.1. **Démonstration de l'assertion 1.** Supposons que f_t soit divisible par un polynôme unitaire $g \in \mathbb{Q}[X]$, irréductible sur $\mathbb{Q}$, de degré 1, 2 ou 3. Soit $x \in \overline{\mathbb{Q}}$ une racine de g. On a en particulier $f_t(x) = 0$. Posons

$$y = \sum_{i=0}^{5} a_i x^i.$$

Le point $[x, y, 1]$ appartient à F_5 (prop. 3). Son corps de rationalité est $\mathbb{Q}(x)$.

Il n'existe pas de points cubiques rationnels sur F_5 ([6], Theorem 1). Par suite, le degré de g est 1 ou 2. Si g est degré 1, vu que $F_5(\mathbb{Q})$ est réduit aux points triviaux, on a $xy = 0$. On a $f_t(x) = f_t(y) = 0$ (prop. 3) or $f_t(0) = 1$, d'où une contradiction. Ainsi, g est de degré 2. Il en résulte que $[x, y, 1]$ est P ou $\overline{P}$, et donc que x est une racine primitive cubique de l'unité ([5], Theorem 5.1). On en déduit que l'on a $g = X^2 + X + 1$. Le reste de la division euclidienne de f_t par $X^2 + X + 1$ est

$$\frac{5(t^4 - 3t^3 + 4t^2 - 2t + 1)(t-1)}{(2-t)(t^2+t-1)^2}.$$

On obtient $t = 1$, ce qui par l'hypothèse est exclu, d'où une contradiction et le résultat.

Remarque 5.1. Pour $t = 1$, on a $f_t = (X^2 + X + 1)^3$.

5.2. **Démonstration des assertions 2 et 3.** Par définition, on a $f_t(\alpha) = 0$. Le polynôme f_t est réciproque, donc $1/\alpha$ est aussi racine de f_t. Les éléments β et γ étant définis par les égalités (2.2), ce sont des racines de f_t (prop. 3) et il en est de même de $1/\beta$ et $1/\gamma$.

Il s'agit alors d'établir que ces six racines sont distinctes deux à deux. D'après l'assertion 1, on a $\alpha \neq \pm 1$ i.e. $1/\alpha \neq \alpha$. De même, on a $\beta \neq 1/\beta$ et $\gamma \neq 1/\gamma$. Vérifions que l'on a

$$\beta \neq \frac{1}{\alpha} \quad \text{et} \quad \beta \neq \alpha.$$

On peut procéder comme suit. Supposons $\alpha\beta = 1$. D'après la proposition 3, le point $[\alpha, \beta, 1]$ est dans F_5 i.e. on a $\alpha^5 + \beta^5 + 1 = 0$, d'où $\alpha^{10} + \alpha^5 + 1 = 0$ et donc $\alpha^5 = \zeta_3$ ou ζ_3^2. Par suite, α est une racine de l'unité d'ordre divisant 15, ce qui contredit le fait que α soit de degré 6 sur $\mathbb{Q}$ (assertion 1). Pour la même raison, on a $\alpha \neq \beta$ sinon $\alpha^5 = -1/2$. Ainsi, $\alpha, 1/\alpha, \beta$ et $1/\beta$ sont distincts deux à deux.

Par ailleurs, on a (cf. [4])

$$1/\alpha = \sum_{i=0}^{5} a_i\gamma^i, \quad 1/\beta = \sum_{i=0}^{5} a_i(1/\gamma)^i, \quad 1/\gamma = \sum_{i=0}^{5} a_i(1/\beta)^i. \tag{5.2}$$

La première égalité de (5.2) implique $\gamma \neq \alpha$, sinon $\beta = 1/\alpha$. De même, on a $\gamma \neq 1/\alpha$, sinon $1/\gamma = \alpha$ ce qui entraîne $1/\beta = \beta$. On a $\gamma \neq 1/\beta$, sinon $1/\gamma = 1/\alpha$ puis $\gamma = \alpha$. Il reste à établir que $\gamma \neq \beta$. Supposons $\gamma = \beta$. On a $f_t(1/\beta) = 0$, donc le système $((1/\beta)^i)_{0\leq i\leq 5}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\beta)$. On en déduit par exemple que $a_0 = 0$, d'où une contradiction et le résultat.

Démontrons que le groupe de Galois de $K_t/\mathbb{Q}$ est isomorphe à $\mathfrak{S}_3$. Il existe σ_1 et σ_2 dans $\mathrm{Gal}(K_t/\mathbb{Q})$ tels que l'on ait

$$\sigma_1(\alpha) = 1/\alpha \quad \text{et} \quad \sigma_2(\beta) = 1/\beta.$$

Les éléments σ_1 et σ_2 sont d'ordre 2. Vérifions qu'ils sont distincts, ce qui prouvera que $\mathrm{Gal}(K_t/\mathbb{Q})$ n'est pas cyclique, donc est isomorphe à $\mathfrak{S}_3$. D'après les égalités (2.2), on a

$$\sigma_1(\beta) = \sum_{i=0}^{5} a_i\sigma_1(\alpha)^i = \sum_{i=0}^{5} a_i(1/\alpha)^i = \gamma.$$

On a $\gamma \neq 1/\beta$, d'où $\sigma_1 \neq \sigma_2$ et la seconde assertion du théorème.

Vérifions la troisième assertion. Les éléments $\alpha, 1/\alpha$ et $1/\gamma$ sont des racines de f_t. D'après la proposition 3 et les égalités (2.2) et (5.2), les points $[\alpha,\beta,1]$, $[1/\alpha,\gamma,1]$ et $[1/\gamma,1/\beta,1]$ sont dans $F_5(K_t)$. Ils sont non triviaux et distincts deux à deux, d'où le résultat.

6. Démonstration du Théorème 2

6.1. **Démonstration de l'assertion 1.** D'après la remarque 5.1, on a $K_1 = \mathbb{Q}(\zeta_3)$. On peut donc supposer $t \neq 1$. L'extension $K_t/\mathbb{Q}$ étant galoisienne de groupe de Galois isomorphe à $\mathfrak{S}_3$ (th. 1), K_t contient trois corps cubiques non galoisiens sur $\mathbb{Q}$. Parce que f_t est un polynôme réciproque, l'un d'entre eux est $\mathbb{Q}(\xi)$ où $\xi = \alpha + 1/\alpha$. Le polynôme minimal de ξ sur $\mathbb{Q}$ est

$$g_t = X^3 + uX^2 + (v-3)X - 2u + w.$$

Le discriminant Δ de g_t est

$$\Delta = -\frac{5^2(t^4-3t^3-t^2+3t+1)^2(7t^5-10t^4-20t^3-4)(t-1)^2}{(t-2)^3(t^2+t-1)^6}.$$

On constate que Δ modulo $\mathbb{Q}^{*2}$ est $(2-t)(7t^5-10t^4-20t^3-4)$. Le corps K_t est donc le composé de $\mathbb{Q}(\xi)$ et du corps quadratique

$$\mathbb{Q}\left(\sqrt{(2-t)(7t^5-10t^4-20t^3-4)}\right).$$

Le polynôme g_t a trois racines réelles si et seulement si on a $\Delta > 0$. Il en résulte que K_t est totalement réel si et seulement si on a

$$(2-t)(7t^5-10t^4-20t^3-4) > 0.$$

On vérifie directement que cette condition signifie que l'on a $2 < t < r$.

Remarque 6.1. D'après le théorème 1 et la démonstration de cette assertion, l'ensemble des points rationnels sur $\mathbb{Q}$ de la courbe de genre 2 d'équation $y^2 = (2-x)(7x^5-10x^4-20x^3-4)$ est le singleton $\{(2,0)\}$. On peut aussi le constater avec [1].

6.2. **Démonstration de l'assertion 2.** Supposons qu'il n'existe qu'un nombre fini de rationnels $t \in]2, r[$ tels que les corps K_t soient deux à deux distincts. Dans ce cas, il existe un rationnel $t_0 \in]2, r[$ et une infinité de $t \in]2, r[\cap \mathbb{Q}$ tels que l'on ait $K_{t_0} = K_t$. Soit d_0 l'entier sans facteurs carrés tel que $\mathbb{Q}(\sqrt{d_0})$ soit le corps quadratique contenu dans K_{t_0}. On a constaté ci-dessus que $\mathbb{Q}\left(\sqrt{(2-t)(7t^5 - 10t^4 - 20t^3 - 4)}\right)$ est le corps quadratique contenu dans K_t. Par suite, la courbe de genre 2 d'équation

$$d_0 y^2 = (2-x)(7x^5 - 10x^4 - 20x^3 - 4)$$

possède une infinité de points rationnels sur $\mathbb{Q}$, ce qui contredit le théorème de Faltings [2] Satz 7, d'où l'assertion.

7. Appendice

Soit K un corps totalement réel de degré n sur $\mathbb{Q}$.

Proposition 4. *Supposons $n \leq 5$. Il n'existe pas de points non triviaux dans $F_5(K)$.*

Démonstration. Si on a $n \leq 3$ cela est établi, comme on l'a déjà signalé, dans [5] et [6]. Supposons $n \in \{4, 5\}$ et qu'il existe un point non trivial $[x, y, 1]$ dans $F_5(K)$. On a alors $K = \mathbb{Q}(x, y)$.

1) Supposons $n = 4$. D'après le lemme 3.1 de [7], avec ses notations, on peut supposer que l'on a $K = \mathbb{Q}(y)$ et qu'il existe $u \in \mathbb{Q}$ tel que le polynôme minimal de y sur $\mathbb{Q}$ soit

$$f = X^4 + uX^3 + (u+2)X^2 + uX + 1.$$

Par hypothèse, f possède quatre racine réelles. Il en résulte que le polynôme dérivé de f a trois racines réelles, autrement dit que son discriminant est strictement positif. On obtient

$$-8(u-4)^2(9u^2 + 16u + 8) > 0,$$

ce qui conduit à une contradiction, d'où le résultat dans ce cas.

2) Supposons $n = 5$. Quitte à permuter x et y, on déduit de [6] qu'il existe a et b dans $\mathbb{Q}$ tels que $y = ax + b$. On a donc $K = \mathbb{Q}(x)$ et le polynôme minimal de x sur $\mathbb{Q}$ est $X^5 + (aX + b)^5 + 1$. Ses racines sont réelles, par suite son polynôme dérivé possède quatre racines réelles. Il en est donc ainsi du polynôme $X^4 + a(aX + b)^4$, d'où une contradiction et le résultat. □

Références

[1] W. Bosma, J. Cannon et C. Playoust : *The Magma Algebra System I : The User Language*, J. Symb. Comp. **24** (1997), 235–265. (voir aussi http://magma.maths.usyd.edu.au/magma/) 1, 6.1

[2] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366. 6.2

[3] N. Freitas, A. Kraus et S. Siksek, *Class field theory, Diophantine analysis and the asymptotic Fermat's Last Theorem*, Adv. Math. **363** :106964, (2020). 1

[4] N. Freitas et A. Kraus, Fichiers Magma et Pari-gp de vérification des calculs, https://github.com/AlainKraus. 1, 4, 4, 5.2

[5] B. H. Gross et D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201-224. 1, 5.1, 7

[6] M. Klassen et P. Tzermias, *Algebraic points of low degree on the Fermat quintic*, Acta Arith. **82** (1997), 393-401. 1, 3, 5.1, 7

[7] A. Kraus, *Quartic points on the Fermat quintic*, Ann. Math. Blaise Pascal **25** (2018), 199-205. 1, 7

[8] F. Pop, *Embedding problems over large fields*, Ann. Math. **144** (1996), 1-34. 1

[9] The PARI Group, PARI/GP version `2.15.4`, Université de Bordeaux I, (2023). 1, 3, 4

[10] R. J. Walker *Algebraic Curves*, Springer-Verlag, 1950, 1978. 3

[11] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551. 1

Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche, UMR 7586 CNRS - Paris Diderot, 4 Place Jussieu, 75005 Paris, France

Email address: `alain.kraus@imj-prg.fr`