

## MORDELL-WEIL GROUPS OF THE JACOBIAN OF THE 5-TH FERMAT CURVE

PAVLOS TZERMIAS

(Communicated by William W. Adams)

ABSTRACT. Let  $J_5$  denote the Jacobian of the Fermat curve of exponent 5 and let  $K = \mathbb{Q}(\zeta_5)$ . We compute the groups  $J_5(K)$ ,  $J_5(K^+)$ ,  $J_5(Q)$ , where  $K^+$  is the unique quadratic subfield of  $K$ . As an application, we present a new proof that there are no  $K$ -rational points on the 5-th Fermat curve, except the so called “points at infinity”.

### 1. INTRODUCTION

Let  $F_5$  denote the complete non-singular curve over  $\mathbb{Q}$  with projective equation

$$X^5 + Y^5 + Z^5 = 0.$$

We denote by  $J_5$  the Jacobian of  $F_5$ . Let  $\zeta_5$  be a primitive 5-th root of unity in  $\overline{\mathbb{Q}}$  and let  $K = \mathbb{Q}(\zeta_5)$ . Also let  $K^+$  denote the unique quadratic subfield of  $K$ . As Faddeev ([2]) has shown, the group  $J_5(K)$  of  $K$ -rational points of  $J_5$  is finite. In this paper, we will determine the structure of this group, as well as of its subgroups  $J_5(K^+)$  and  $J_5(Q)$ .

There are 15 points  $(X, Y, Z)$  on  $F_5$  for which one of  $X, Y, Z$  is 0, namely the points  $a_j = (0, \epsilon \zeta_5^j, 1)$ ,  $b_j = (\epsilon \zeta_5^j, 0, 1)$ ,  $c_j = (\epsilon \zeta_5^j, 1, 0)$ , where  $\epsilon = e^{\pi i/5}$ ,  $\zeta_5 = \epsilon^2$  and  $0 \leq j \leq 4$ . These points will be called the points at infinity on  $F_5$ .

Let  $J_5^\infty$  be the subgroup of  $J_5$  consisting of those divisor classes of degree 0 which contain a divisor supported on the points at infinity. Rohrlich ([7]) has completely determined the structure of the group  $J_5^\infty$ . It is isomorphic to  $(\mathbb{Z}/5\mathbb{Z})^8$ .

The main result of this paper is:

**Proposition.** *In the above notation, we have  $J_5(K) = J_5^\infty$ .*

As a result of this proposition, we will also deduce:

**Corollary 1.**  *$J_5(K^+)$  is isomorphic to  $(\mathbb{Z}/5\mathbb{Z})^5$ .*

**Corollary 2.**  *$J_5(Q)$  is isomorphic to  $(\mathbb{Z}/5\mathbb{Z})^2$ .*

**Corollary 3.** *The only  $K$ -rational points on  $F_5$  are the points at infinity.*

*Remark.* It should be noted that Fermat’s Last Theorem for the exponent 5 is implied by Corollary 3.

---

Received by the editors November 5, 1994 and, in revised form, September 1, 1995.  
1991 *Mathematics Subject Classification.* Primary 14H25, 14G05; Secondary 11D41.

2. THE 5-PRIMARY PART OF  $J_5(K)$ 

In this Section, we will determine the 5-primary part of  $J_5(K)$ . Let  $\sigma, \tau$  be the automorphisms of  $F_5$  given by

$$\sigma(X, Y, Z) = (\zeta_5 X, Y, Z),$$

$$\tau(X, Y, Z) = (X, \zeta_5 Y, Z).$$

Let  $a, b$  be positive integers such that  $1 \leq a, b$ ,  $a + b \leq 4$ . Consider the quotient curve  $F_{a,b} = F_5 / \langle \sigma^b \tau^{-a} \rangle$  and let  $J_{a,b}$  be the Jacobian of  $F_{a,b}$ .

The curve  $F_{a,b}$  is defined over  $Q$  and has the affine singular equation

$$y^5 = x^a(1-x)^b.$$

It has a birational automorphism given by  $(x, y) \mapsto (x, \zeta_5 y)$ , which induces an endomorphism of  $J_{a,b}$ , which will also be called  $\zeta_5$ . Now consider the element  $\pi = \zeta_5 - 1$  of  $\text{End}(J_{a,b})$ .

In this Section, we will concentrate on  $J_{1,3}$  only and for simplicity of notation, we will write  $J = J_{1,3}$ . Let  $Q$  be a  $\pi^2$ -division point on  $J$  which is not a  $\pi$ -division point. We also assume that the complex conjugate of  $Q$  equals  $-Q$ . Then Lim ([6]) has shown that  $J_5$  is isomorphic to  $J^2 \times B$  over  $K$ , where  $B$  is the abelian variety which is the quotient of  $J$  by the subgroup generated by  $(1+3\pi)Q$ . Let  $\phi : J \rightarrow B$  be the corresponding isogeny (defined over  $K$ ), with kernel equal to  $\langle (1+3\pi)Q \rangle$ .

Now, 5 does not divide the class number of  $K^+$ ; therefore, by Greenberg's result (see [3]), the 5-primary part of  $J(K)$ , denoted by  $(J(K))_{5\text{-power}}$ , equals the kernel of the isogeny  $\pi^3$  of  $J$ . We write the kernel of  $\pi^3$  as  $J[\pi^3]$ .

So we only need to determine  $(B(K))_{5\text{-power}}$ .

We will prove the following two lemmas:

**Lemma 1.**  $(B(K))_{5\text{-power}}$  is isomorphic to  $(Z/5Z)^2$ .

**Lemma 2.**  $(J_5(K))_{5\text{-power}} = J_5^\infty$ .

We will prove both lemmas together. We proceed as follows:

Let  $D_0$  be a point in  $B(K)$  of exact order  $5^r$ , for some non-negative integer  $r$ . Let  $\sigma$  be in  $\text{Gal}(\overline{K}/K)$ . Lift to a point  $D$  in  $J$ . Since  $D_0$  is defined over  $K$ , we have  $D^\sigma - D = a(1+3\pi)Q$ , for some integer  $a$ .

Then  $\pi^2 D^\sigma - \pi^2 D = 0$ , because  $Q$  is a  $\pi^2$ -division point. Now  $\pi^\sigma = \pi$ ; therefore  $(\pi^2 D)^\sigma = \pi^2 D$ . This is true for all  $\sigma$  in  $\text{Gal}(\overline{K}/K)$ ; therefore  $\pi^2 D$  is in  $J(K)$ . Also,  $5^r D_0 = 0$ , so  $5^r D$  is in  $\langle (1+3\pi)Q \rangle$ ; hence  $5^r \pi^2 D = 0$ . Therefore,  $\pi^2 D$  is in  $(J(K))_{5\text{-power}}$ . By Greenberg's theorem ([3]), we get that  $\pi^2 D$  is killed by  $\pi^3$ ; hence  $r \leq 1$  and  $D$  is in  $J[\pi^5]$ . We have thus proved:

*Claim 1.*  $(B(K))_{5\text{-power}}$  is contained in  $\phi(J[\pi^5])$  and is annihilated by 5.

Now suppose that  $D$  is in  $J[\pi^5] - J[\pi^4]$  such that  $\phi(D)$  is in  $(B(K))_{5\text{-power}}$ . By claim 1, we get  $5\phi(D) = 0$ , so  $5D = a(1+3\pi)Q$ , for some integer  $a$ . Then  $5\pi D = aP$ , where  $P = \pi Q$ .

Observe that  $J[\pi^4] = J[5]$ ; therefore  $5\pi D = 0$ , hence  $aP = 0$ . Since  $Q$  is not a  $\pi$ -division point, we get that 5 divides  $a$ , hence  $5D = 0$ . This means that  $D$  is in  $J[\pi^4]$ , a contradiction. Therefore, we have proved:

*Claim 2.*  $(B(K))_{5\text{-power}}$  is a subgroup of  $\phi(J[\pi^4])$ .

Now suppose that  $D$  is in  $J[\pi^4] - J[\pi^3]$  such that  $\phi(D)$  is in  $(B(K))_{5\text{-power}}$ . Let  $\sigma$  be in  $\text{Gal}(\overline{K}/K)$ . Then  $D^\sigma - D = a(1 + 3\pi)Q$ , for some integer  $a$ . Therefore,  $\pi D^\sigma - \pi D = aP$ , where, again,  $P = \pi Q$ . But  $\pi D$  is in  $J[\pi^3]$ ; therefore, by [4], we have  $\pi D^\sigma = (\pi D)^\sigma = \pi D$ . Hence  $aP = 0$ , so, since  $Q$  is not a  $\pi$ -division point, we get that 5 divides  $a$ , so  $D^\sigma = D$ . This being true for all  $\sigma$  in  $\text{Gal}(\overline{K}/K)$ , we conclude that:

*Claim 3.*  $(B(K))_{5\text{-power}}$  is a subgroup of  $\phi(J[\pi^3])$ .

Claim 3, together with a cardinality argument, shows that the order of  $(B(K))_{5\text{-power}}$  divides  $5^2$ .

Therefore, since  $J_5$  and  $J^2 \times B$  are isomorphic over  $K$ , we get that  $(J(K))_{5\text{-power}}$  has order dividing  $5^8$ . On the other hand, Rohrlich ([7]) has proved that  $J_5^\infty$  is isomorphic to  $(Z/5Z)^8$ . Also, evidently,  $J_5^\infty$  is contained in  $(J(K))_{5\text{-power}}$ .

This proves Lemmas 1 and 2.

### 3. NON-EXISTENCE OF $l$ -TORSION FOR $l \neq 5$

Consider the abelian variety  $J_{a,b}$  as in Section 2. Let  $f_5(X)$  be the 5-th cyclotomic polynomial and let  $J_{a,b}^{new}$  denote the quotient of  $J_{a,b}$  by the abelian subvariety  $f_5(g)J_{a,b}$ , where  $g = \sigma^b \tau^{-a}$ . Then  $J_{a,b}^{new}$  is defined over  $Q$ .

*Claim 4.* We have  $J_{a,b}^{new} = J_{a,b}$ .

Indeed, we have  $\text{Ker}(g - 1) = 0$  and  $g^5 = 1$  on  $J_{a,b}$ ; therefore we get that  $f_5(g)J_{a,b} = 0$ , which proves the claim.

Now, using results of Coleman ([1]), we can show:

*Claim 5.* There is no  $l$ -torsion in  $J_{a,b}(K)$ , for  $l \neq 5$ .

Indeed, let  $l$  be a prime,  $l \neq 5$ . Suppose  $T$  is an  $l$ -torsion point on  $J_{a,b} = J_{a,b}^{new}$ . By Proposition 10 in [1], the field extension  $Q(T)/Q$  is ramified above  $l$  unless  $l = 2$  and  $J_{a,b}^{new}$  is ordinary at 2. However, by Corollary 13.1 in [1],  $J_{a,b}^{new}$  is not ordinary at 2 in the case of the Fermat quintic.

Therefore, we deduce that the field extension  $Q(T)/Q$  is ramified above  $l$ , whenever  $l \neq 5$  and  $T$  is an  $l$ -torsion point on  $J_{a,b}$ . Since  $K/Q$  is unramified above  $l$ , the point  $T$  can never be  $K$ -rational, so the claim follows.

Now we can show:

**Lemma 3.** *Let  $l$  be a prime,  $l \neq 5$ . Then  $J_5(K)$  has no  $l$ -torsion.*

*Proof.* We have an isogeny defined over  $Q$

$$f : J_5 \longrightarrow J_{1,1} \times J_{1,2} \times J_{1,3}.$$

Also let

$$\hat{f} : J_{1,1} \times J_{1,2} \times J_{1,3} \longrightarrow J_5$$

be the dual isogeny. Then  $\hat{f} \circ f$  equals multiplication by 5 on  $J_5$  (see for example [5]).

If  $T$  is an  $l$ -torsion point in  $J_5(K)$ , then  $f(T)$  is an  $l$ -torsion point in  $J_{1,1}(K) \times J_{1,2}(K) \times J_{1,3}(K)$ .

By Claim 5, we get  $f(T) = 0$ ; therefore  $T$  is in  $\text{Ker}(f)$ , which is contained in  $J_5[5]$ . Hence,  $T$  is also a 5-torsion point; therefore  $T = 0$ . This proves Lemma 3.

The proposition of the introduction now follows from Lemmas 2 and 3.

Finally, we will compute  $\text{Ker}(f)$ . Consider the group  $G$  of divisor classes of degree 0 on  $F_5$  which are represented by a linear combination of the divisors  $a_j - a_2$ ,  $b_j - b_2$ ,  $c_j - c_2$ , for  $j \neq 2$ ,  $0 \leq j \leq 4$ . Then:

**Lemma 4.**  $\text{Ker}(f) = G$ .

*Proof.* It is evident that  $G$  is contained in  $\text{Ker}(f)$  and it follows from the work of Rohrlich ([7]) that  $G$  has cardinality  $5^6$ .

Since  $\hat{f} \circ f = 5$  and the cardinalities of  $\text{ker}(\hat{f})$  and  $\text{ker}(f)$  are the same, the lemma follows.

#### 4. THE STRUCTURE OF $J_5(K^+)$ AND $J_5(Q)$

Now we will prove Corollaries 1 and 2 of the introduction. Recall that  $J_5^\infty$  denotes the divisor classes of degree 0 on  $J_5$  that can be represented by a divisor supported on the points at infinity.

Rohrlich ([7]) has shown that every element of  $J_5^\infty$  is represented by a linear combination of the divisors  $a_j - a_2$ ,  $b_j - b_2$ ,  $c_j - c_2$ ,  $a_2 - c_2$ ,  $b_2 - c_2$ , for  $j \neq 2$ ,  $0 \leq j \leq 4$ .

So take any divisor  $\overline{D}$  in  $J_5(K)$ . By the proposition of the introduction, we can choose a representative  $D$  of the form

$$D = s(a_2 - c_2) + t(b_2 - c_2) + \sum_{j=0}^4 (x_j(a_j - a_2) + y_j(b_j - b_2) + z_j(c_j - c_2)),$$

for integers  $x_j, y_j, z_j, s, t$ .

Now  $K = Q(\zeta_5) = Q(\epsilon)$ . Let  $\alpha$  be the generator of  $\text{Gal}(K/Q)$  given by  $\alpha(\epsilon) = \epsilon^3$ . If  $\overline{D}$  is in  $J_5(Q)$ , then we must have that  $D^\alpha - D$  is principal. But

$$D^\alpha - D = \sum_{j=0}^4 (x_j(a_{3j+1} - a_j) + y_j(b_{3j+1} - b_j) + z_j(c_{3j+1} - c_j)).$$

Now, by Corollary 1 to Theorem 2 of [7] and a tedious calculation (not presented here), we get that  $D^\alpha - D$  is principal if and only if  $D - s(a_2 - c_2) - t(b_2 - c_2)$  is a principal divisor.

This proves Corollary 1.

The proof of Corollary 2 is similar. We only need to replace the automorphism  $\alpha$  by the automorphism  $\beta$  given by  $\beta(\epsilon) = \epsilon^{-1}$ .

#### 5. THE SET $F_5(K)$

As an application of the proposition, we will now prove Corollary 3.

Consider again the curve  $F_{1,3}$  and the abelian variety  $J = J_{1,3}$ , as in Section 2. We have the quotient map

$$g : F_5 \longrightarrow F_{1,3},$$

which induces a map  $g_*$  on the divisors of degree 0 and hence a map (also denoted by  $g_*$ )

$$g_* : J_5 \longrightarrow J_{1,3}.$$

Similarly, we have the induced pullback map  $g^*$  on the divisors of degree 0 on  $F_{1,3}$  and hence a map

$$g^* : J_{1,3} \longrightarrow J_5.$$

It is easy to see that if  $D$  is a divisor of degree 0 on  $F_5$  then we have

$$g^*(g_*(D)) = \sum_{j=0}^4 (\sigma^2\tau)^j D.$$

We have the points  $P_0 = (0, 0, 1)$ ,  $P_1 = (1, 0, 1)$  and  $P_\infty = (1, 0, 0)$  on  $F_{1,3}$ . Observe that  $g(a_j) = P_0$ ,  $g(b_j) = P_1$ ,  $g(c_j) = P_\infty$ , for  $0 \leq j \leq 4$ .

Now if  $P$  is a  $K$ -rational point on  $F_5$ , which is not a point at infinity, let  $D$  be the equivalence class of the divisor  $P - c_2$ .

$D$  is in  $J_5(K)$ , so, by our proposition, we get that  $g_*(D)$  is represented by a divisor of degree 0 supported on the points  $P_0, P_1, P_\infty$ . By [4], any such divisor is linearly equivalent to a multiple of  $P_0 - P_\infty$ . Since  $g^*(P_0 - P_\infty) = \text{div}(X/Z)$ , we conclude that  $g^*(g_*(D))$  is linearly equivalent to 0. But

$$g^*(g_*(P - c_2)) = \sum_{j=0}^4 (\sigma^2\tau)^j P - \sum_{j=0}^4 c_j,$$

which cannot be principal, by Lemma 2.1 of [4] (where we take  $d = 1$  and  $u = 2$ ).

## 6. FINAL REMARKS

1. Greenberg has shown ([3]) that in the case of the quotient curves  $F_{a,b}$ , there exists a positive integer  $s$  such that the group  $J_{a,b}(K)$  equals the kernel of the isogeny  $\pi^s$  of  $J_{a,b}$ . As a result of the proposition proved in this paper, we see that this cannot be the case for the Fermat curve  $F_5$ . Indeed, the kernel of the isogeny  $\pi$  of  $J_5$  has cardinality  $5^3$ , so the kernel of  $\pi^s$  has cardinality  $5^{3s}$ , which can never equal  $5^8$ .

2. Let  $\zeta_6$  be a primitive 6-th root of unity in  $\overline{Q}$  and let  $P = (\zeta_6, \zeta_6^{-1}, 1)$  and  $\overline{P} = (\zeta_6^{-1}, \zeta_6, 1)$  on  $F_5$ . Gross and Rohrlich ([4]) have considered the divisor  $D = P + \overline{P} - a_2 - b_2$  on  $F_5$ . It is evident that  $D$  (not just the divisor class of  $D$ ) is defined over  $Q$ . Then Corollary 2 implies that the divisor class of  $D$  is a linear combination of the divisor classes of  $a_2 - c_2$  and  $b_2 - c_2$ . Indeed, a little search shows that

$$D + 2(a_2 - c_2) + 2(b_2 - c_2) = \text{div}(x + y - 1) - \text{div}(x + y),$$

where  $x = X/Z, y = Y/Z$ .

## ACKNOWLEDGMENTS

This paper will constitute part of my doctoral dissertation at Berkeley. I am indebted to Robert F. Coleman for his support and encouragement during the course of this work.

## REFERENCES

- [1] R. F. Coleman, *Torsion points on Abelian étale coverings of  $P^1 - \{0, 1, \infty\}$* , Transactions of the AMS, **311**, No. 1 (1989), 185-208. MR **90a**:11064
- [2] D. K. Faddeev, *On the divisor class groups of some algebraic curves*, Soviet Math. Dokl. **2** (1961), 67-69. MR **24**:A723
- [3] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1981), 345-359. MR **82j**:14036
- [4] B. Gross and D. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201-224. MR **58**:10911

- [5] S. Lang, *Introduction to algebraic and abelian functions*, **GTM 89**, Springer-Verlag, New York-Berlin-Heidelberg. MR **48**:6122
- [6] C. H. Lim, *The geometry of the Jacobian of the Fermat curve of exponent five*, *Journal of Number Theory* **41** (1991), 102-115. MR **93j**:14030
- [7] D. Rohrlich, *Points at infinity on the Fermat curves*, *Invent. Math.* **39** (1977), 95-127. MR **56**:367

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720

*E-mail address*: `tzermias@math.berkeley.edu`

*Current address*: Centre de Recerca Matemàtica, Institut d'Estudis Catalans, Apartat 50, E-08193 Bellaterra, Spain

*Current e-mail address*: `tzermias@crm.es`