ACTA ARITHMETICA
LXXXIV.4 (1998)

Arithmetic of cyclic quotients of the Fermat quintic

by

Pavlos Tzermias (Bellaterra)

1. Introduction. Let F denote the Fermat quintic curve over $\mathbb{Q}$ given by the projective equation

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

and let J be its Jacobian. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$ and let a and b denote the positive and negative root of the equation $X^2 - X - 1 = 0$, respectively. Let $\zeta \in \overline{\mathbb{Q}}$ be a primitive 5th root of 1 such that $a = -(\zeta^2 + \zeta^3)$. Let K be the cyclotomic field $\mathbb{Q}(\zeta)$ and denote by K^+ the maximal real subfield of K, i.e. $K^+ = \mathbb{Q}(a)$. Consider the automorphisms σ, τ and ϱ of F given by

$$\sigma(X,Y,Z) = (\zeta X, Y, Z), \quad \tau(X,Y,Z) = (X, \zeta Y, Z), \quad \varrho(X,Y,Z) = (Z, X, Y).$$

For $s = 1, 2, 3$, consider the cyclic quotient F_s of F by the group of automorphisms generated by $\sigma\tau^{-s}$. The genus of F_s equals 2. We denote by J_s the Jacobian of F_s. We have the natural projection maps (defined over $\mathbb{Q}$)

$$f_s : J \to J_s$$

and their duals (also defined over $\mathbb{Q}$)

$$f_s^* : J_s \to J.$$

It is well known ([7]) that each J_s is a simple abelian variety and that the map

$$f = \prod_{s=1}^{3} f_s : J \to \prod_{s=1}^{3} J_s$$

is an isogeny. The dual isogeny is given by

$$f^* = \sum_{s=1}^{3} f_s^* : \prod_{s=1}^{3} J_s \to J.$$

1991 *Mathematics Subject Classification*: Primary 14H25, 11G30.

In this paper, we prove some results on the arithmetic of the curves F_s. In Section 2, we recall some known results and give explicit generators for the Mordell–Weil groups $J_s(K)$. In Section 3, we give explicit generators for the kernel of f^*. We also describe the action of $\mathrm{End}(J)$ on $\mathrm{Ker}(f^*)$, by means of a result of Lim ([9]).

For an abelian variety V and an endomorphism ϕ of V, let us denote by $V[\phi]$ the kernel of ϕ. In Section 4, we give generators for the groups $J_s[5]$. It was shown by Greenberg ([5]) that the field of definition L of $J_s[5]$ is generated over K by the 5th roots of the cyclotomic units in K^+. Also, by a result of Faddeev ([3]), the groups $J_s(K)$ are finite. We show that the groups $J_s(L)$ are all infinite and we give a lower bound for their rank.

Acknowledgments. This work has been motivated by [2]. To a large extent, it is an application of Coleman's results. The author is grateful to the anonymous referee for suggesting substantial improvements on an earlier version of this paper.

2. Generators for $J_s(K)$. For $s = 1, 2, 3$, we have the well-known affine model of F_s:

$$v^5 = u^s(1-u).$$

Moreover, the projection maps $f_s : F \to F_s$ are given in affine coordinates by $(x, y, 1) \mapsto (u, v)$, where $(u, v) = (-x^5, (-1)^{s-1}x^s y)$.

Let ∞_s denote the point at infinity on F_s. We also note the affine points $(0, 0)_s$ and $(1, 0)_s$ on F_s. The curves F_1, F_2 and F_3 are isomorphic over $\mathbb{Q}$. This is explained in §2 of [1]. The following explicit formulas for these isomorphisms will be needed in the sequel.

Define a rational map $F_1 \to F_2$ given by

$$(u, v) \mapsto ((u-1)/u, v^2/u).$$

This map has a rational inverse given by

$$(u, v) \mapsto (1/(1-u), v^3/(u(u-1))).$$

Therefore, it extends to an isomorphism $g : F_1 \to F_2$. Similarly, we define an isomorphism $h : F_3 \to F_2$ extending the rational map

$$(u, v) \mapsto (1/(1-u), v^2/(u(u-1))),$$

whose rational inverse is given by

$$(u, v) \mapsto ((u-1)/u, -v^3/u^2).$$

We now have the following easy lemma:

Lemma 1. *Let notation be as above.*

(i) *We have the following equalities of maps $F \to F_2$:*

$$gf_1 = f_2\varrho^2, \qquad hf_3 = f_2\varrho.$$

(ii) *We have the following equalities of maps* $J_2 \to J$:

$$f_1^* g^{-1} = \varrho f_2^*, \qquad f_3^* h^{-1} = \varrho^2 f_2^*.$$

(iii) *Moreover*,

$$g((1,0)_1) = h(\infty_3) = (0,0)_2, \qquad g((0,0)_1) = h((1,0)_3) = \infty_2,$$
$$g(\infty_1) = h((0,0)_3) = (1,0)_2.$$

Proof. (i) is straightforward. (ii) follows from (i) and the relations $g^* = g^{-1}$, $h^* = h^{-1}$ and $\varrho^* = \varrho^2$. (iii) follows from (i) after evaluation at the points $(0,-1,1)$, $(-1,0,1)$, $(-1,1,0)$ on F.

J_s admits complex multiplication ζ induced by the map $(u,v) \mapsto (u,\zeta v)$ on F_s. We will use the same symbol π to denote the endomorphisms $\zeta - 1$ and $\tau - 1$ of J_s and J, respectively. Then it is easy to see that π commutes with f_s and f_s^*.

The following proposition is a combination of results in the literature. In fact, it is just a special case of a more general theorem concerning the Jacobians of cyclic Fermat quotients.

Proposition 1 ([1], [3], [5], [6], [8]). *For all s we have $J_s(K) = J_s[\pi^3]$ and $J_s(\mathbb{Q}) = J_s[\pi]$.*

Specifically, Faddeev showed in [3] that $J_s(K)$ is finite. In [5], Greenberg proved the equality $J_s[\pi^3] = J_s[5^\infty](K)$. Coleman showed in [1] that for all primes l such that $l \neq 5$, the l-primary part of $J_s(K)$ is trivial. The second statement of Proposition 1 follows from the work of Gross and Rohrlich ([6]). Finally, Kurihara's result ([8]) cited in Proposition 1 is not needed in the specific case we are dealing with. However, it is necessary for obtaining an analogous statement for the Jacobians of more general cyclic Fermat quotients and we include it here as a reference for the interested reader.

It should be noted that the proof of Proposition 1 does not give explicit generators for $J_s(K)$. This is done in Proposition 2 below. The only other examples besides that of Proposition 2 where explicit generators for the analogues of $J_s[\pi^3]$ or $J_s(K)$ are determined are for the Jacobians of quotients of the Fermat cubic and for the Jacobian of the Fermat quotient $v^7 = u^2(1-u)$ by Prapavessi ([10]).

We now use an observation of Coleman. One of the points in the hyperelliptic torsion packet on F_1 is $P_1 = (a,-1)$ in $F_1(K^+)$ (see [2]). Using Lemma 1, we get the points $P_2 = (b^2,-b)$ and $P_3 = (-a,-a)$ in $F_2(K^+)$ and $F_3(K^+)$, respectively. Define

$$r_s = [P_s - \infty_s] \in J_s(K^+), \quad t_s = \pi r_s \in J_s(K), \quad w_s = [(0,0) - \infty_s] \in J_s(\mathbb{Q}),$$

for $s = 1,2,3$. As in [9], we use the identification $\mathrm{End}(J_s) = \mathbb{Z}[\zeta]$. Observe that $\mathbb{Z}[\pi] = \mathbb{Z}[\zeta]$. We will now prove the following proposition:

PROPOSITION 2. *For $s = 1, 2, 3$, the Mordell–Weil group $J_s(K)$ is generated by r_s as a $\mathbb{Z}[\pi]$-module. Alternatively, the set $\{r_s, t_s, w_s\}$ is a $\mathbb{Z}/5\mathbb{Z}$-basis for $J_s(K)$.*

Proof. Fix s. By Proposition 1 and since $\pi r_s = t_s$ and $\pi w_s = 0$, the only thing we need to show is that $\pi^2 r_s \neq 0$. Suppose, on the contrary, that $\pi^2 r_s = 0$. Then πr_s is $\mathbb{Q}$-rational. In particular, it is fixed by complex conjugation. Therefore, $-\zeta^{-1}\pi r_s = \pi r_s$, hence $\zeta \pi r_s = -\pi r_s$. This implies that $0 = \pi^2 r_s = -2\pi r_s$. Therefore, by Proposition 1, r_s is $\mathbb{Q}$-rational. As the map $F_s(\overline{\mathbb{Q}}) \to J_s(\overline{\mathbb{Q}})$ defined by $R \mapsto [R - \infty_s]$ is an injection preserved by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have reached a contradiction, because P_s is not defined over $\mathbb{Q}$.

Using some of the arguments in [2] and [4], one can explicitly write down a rational function on F_s with divisor $\pi^3(P_s - \infty_s)$. We will use one of the arguments in [2] in the proof of the following lemma:

LEMMA 2. *Let notation be as above. We have*:

(i) $\pi t_2 = 2w_2$.
(ii) $g(r_1) = r_2 + 2w_2$, $g(t_1) = 2t_2 + 2w_2$ *and* $g(w_1) = 2w_2$.
(iii) $h(r_3) = r_2 - w_2$, $h(t_3) = 2t_2 + 2w_2$ *and* $h(w_3) = 2w_2$.

Proof. By [2], the following divisor on F_1 is principal:

$$\zeta^4 P_1 - \zeta^3 P_1 - \zeta^2 P_1 + \zeta P_1 - 2(1,0)_1 + 2\infty_1.$$

Applying the isomorphism $g : F_1 \to F_2$ and Lemma 1, we get

$$\pi^2[\zeta^2 P_2 + \zeta P_2 - 2\infty_2] = 2[(1,0)_2 - (0,0)_2].$$

Since $\pi^2 r_2$ is fixed by ζ, we have

$$\pi^2[\zeta^2 P_2 - \infty_2] = \pi^2[\zeta P_2 - \infty_2] = \pi^2 r_2 = \pi t_2.$$

Therefore,

$$\pi t_2 = [(1,0)_2 - (0,0)_2].$$

Now, as in [6], we have the following relations:

$$5((0,0)_2 - \infty_2) = \mathrm{div}(u), \qquad 5((0,0)_2 - (1,0)_2) = \mathrm{div}(u/(1-u)).$$

Since $v^5 = u^2(1-u)$, we get

$$5\,\mathrm{div}(v) = 2\,\mathrm{div}(u) + \mathrm{div}(1-u) = 5(2(0,0)_2 + (1,0)_2 - 3\infty_2).$$

Hence, $\mathrm{div}(v) = 2(0,0)_2 + (1,0)_2 - 3\infty_2$, which implies that

$$[(1,0)_2 - (0,0)_2] = 2w_2.$$

This proves (i). (ii) and (iii) follow from an easy computation involving the latter relation, the explicit formulas for g and h and (i).

3. Generators for $\mathrm{Ker}(f^*)$**.** Clearly, $\sharp(\mathrm{Ker}(f^*)) = 5^6$. Therefore, by Corollary 2 of [12], we have

$$\mathrm{Ker}(f^*) \subseteq \prod_{s=1}^{3} J_s(K).$$

Let a_j (resp. b_j, c_j) be the cusps on F, i.e. the points for which the first (resp. the second, the third) projective coordinate vanishes, where $j = 0, 1, \ldots, 4$. It was shown by Rohrlich ([11]) that divisor classes of degree 0 supported on these points are killed by 5 on $J(K)$. Consider three such divisor classes, namely

$$D_1 = \Big[\sum_{j=0}^{4} j(j+1)(a_j - a_0)\Big], \quad D_2 = \Big[\sum_{j=0}^{4} j(j+1)(b_j - b_0)\Big],$$

$$D_3 = \Big[\sum_{j=0}^{4} j(b_j - b_0)\Big].$$

The results in [12] imply that

$$f_2^*(J_2(K)) \subseteq \langle D_1 - 2D_2, D_3\rangle, \qquad f_2^*(J_2(K^+)) \subseteq \langle D_1 - 2D_2\rangle,$$
$$f_2^*(J_2(\mathbb{Q})) = \{0\}, \qquad \pi D_1 = 2D_3.$$

Moreover, using Corollary 1 of [11], one can show that $\varrho D_2 = -D_1 - D_2$, $\varrho D_1 = D_2$, $\varrho D_3 = D_3$. Therefore, there exists an integer m such that $f_2^*(r_2) = m(D_1 - 2D_2)$. Then $f_2^*(t_2) = 2mD_3$. By Lemmas 1 and 2 and the relations above we get

$$\begin{aligned}
f_1^*(r_1) &= \varrho f_2^* g(r_1) = \varrho f_2^*(r_2 + 2w_2) = m(2D_1 + 3D_2),\\
f_1^*(t_1) &= 4mD_3,\\
f_3^*(r_3) &= \varrho^2 f_2^* h(r_3) = \varrho^2 f_2^*(r_2 - w_2) = -m(3D_1 + D_2),\\
f_3^*(t_3) &= -mD_3.
\end{aligned}$$

Note that these relations imply that m is not divisible by 5, because

$$f^*\Big(\prod_{s=1}^{3} J_s(K)\Big) = \langle D_1, D_2, D_3\rangle,$$

as proved in [12].

Therefore, an element

$$(x_1r_1 + y_1t_1 + z_1w_1, x_2r_2 + y_2t_2 + z_2w_2, x_3r_3 + y_3t_3 + z_3w_3) \in \prod_{s=1}^{3} J_s(K)$$

lies in $\mathrm{Ker}(f^*)$ if and only if

$$(2x_1 + x_2 - 3x_3)D_1 + (3x_1 - 2x_2 - x_3)D_2 + (-y_1 + 2y_2 - y_3)D_3 = 0,$$

so we get

$$x_1 = x_2 = x_3, \quad y_1 = 2y_2 - y_3.$$

This gives a basis for $\mathrm{Ker}(f^*)$ as described in the following proposition. Our choice of basis is not the simplest possible. However, it simplifies the calculations that follow Proposition 3.

PROPOSITION 3. *A $\mathbb{Z}/5\mathbb{Z}$-basis for $\mathrm{Ker}(f^*)$ is given by the following points on $J_1 \times J_2 \times J_3$:*

$$(r_1 - w_1, r_2, r_3 + 3w_3), \quad (2t_1 - 2w_1, t_2, 0), \quad (0, -t_2, 3t_3 - 3w_3),$$
$$(3w_1, 0, 0), \quad (0, w_2, 0), \quad (0, 0, 3w_3).$$

By the work of Lim, we know the structure of the endomorphism ring of J. It turns out (see [9] for more details) that

$$\mathrm{End}(J) = \mathbb{Z}[\sigma, \tau, \varrho, W],$$

where the first three generators are the endomorphisms of J induced by the automorphisms σ, τ and ϱ of F, respectively, and the fourth generator W is an endomorphism of J which is not induced by an automorphism of F.

In [9], Lim uses the identifications $\mathrm{End}(J_s) = \mathbb{Z}[\zeta]$ to show that $\mathrm{End}(J)$ can be naturally identified with a subring of the ring $M_3(\mathbb{Z}[\zeta])$ of 3×3 matrices with entries in $\mathbb{Z}[\zeta]$. Via the latter identification, $\mathrm{End}(J)$ is the set of matrices in $M_3(\mathbb{Z}[\zeta])$ which stabilize $\mathrm{Ker}(f^*)$. We therefore get a natural action of $\mathrm{End}(J)$ on $\mathrm{Ker}(f^*)$, which we will compute below.

In order to use Lim's calculations, we will work instead with the isogeny $\widehat{\phi}$ defined by

$$\widehat{\phi} = f^*(g^{-1} \times 1 \times h^{-1}) : J_2^3 \to J$$

(see [9], §4). Clearly, $\mathrm{Ker}(\widehat{\phi})$ is isomorphic to $\mathrm{Ker}(f^*)$ via the isomorphism

$$g^{-1} \times 1 \times h^{-1} : J_2^3 \to J_1 \times J_2 \times J_3.$$

Using Lemma 2, we have the following consequence of Proposition 3:

COROLLARY 1. *The basis vectors of $\mathrm{Ker}(\widehat{\phi})$ corresponding to the basis vectors of $\mathrm{Ker}(f^*)$ given in Proposition 3 are the following points on J_2^3:*

$$e_1 = (r_2, r_2, r_2), \quad e_2 = (-t_2, t_2, 0), \quad e_3 = (0, -t_2, t_2),$$
$$e_4 = (w_2, 0, 0), \quad e_5 = (0, w_2, 0), \quad e_6 = (0, 0, w_2).$$

In §2 of [9], Lim writes down explicit matrices that describe the action of the four generators σ, τ, ϱ and W of $\mathrm{End}(J)$ on J_2^3. By Lemma 2 and a straightforward calculation we find that the action of $\mathrm{End}(J)$ on $\mathrm{Ker}(\widehat{\phi})$ is given by the following relations:

$$\sigma(e_1) = e_1 - e_2 + e_3 + e_5, \quad \sigma(e_2) = e_2 - 2e_4 + e_5, \quad \sigma(e_3) = e_3 - e_5 + 2e_6,$$
$$\tau(e_1) = e_1 + 2e_2 + e_3 + e_4, \quad \tau(e_2) = e_2 - e_4 + 2e_5, \quad \tau(e_3) = e_3 - 2e_5 + 2e_6,$$
$$\sigma(e_4) = \tau(e_4) = e_4, \quad \sigma(e_5) = \tau(e_5) = e_5, \quad \sigma(e_6) = \tau(e_6) = e_6,$$
$$\varrho(e_1) = e_1, \quad \varrho(e_2) = -e_2 - e_3, \quad \varrho(e_3) = e_2,$$
$$\varrho(e_4) = e_6, \quad \varrho(e_5) = e_4, \quad \varrho(e_6) = e_5,$$
$$W(e_1) = 0, \quad W(e_2) = -e_2 - e_3 + 3e_4 - 2e_5 - e_6,$$
$$W(e_3) = e_2 + 2e_3 - e_4 - e_5 + 2e_6, \quad W(e_4) = 3e_4 + 2e_5,$$
$$W(e_5) = -e_4 + 2e_5 - e_6, \quad W(e_6) = 3e_4 + e_5 + e_6.$$

In particular, we have the following corollary:

COROLLARY 2. *The point* $(r_1 - w_1, r_2, r_3 + 3w_3)$ *on* $J_1 \times J_2 \times J_3$ *generates* $\mathrm{Ker}(f^*)$ *as an* $\mathrm{End}(J)$*-module.*

P r o o f. By Proposition 3 and Corollary 1, it suffices to show that e_1 generates $\mathrm{Ker}(\widehat{\phi})$ as an $\mathrm{End}(J)$-module. By the relations preceding Corollary 2, we have:

$$(\varrho^2(\tau - \sigma) + (\tau - 1)(\tau + 2\sigma - 3))(2e_1) = e_3, \quad \varrho(e_3) = e_2,$$
$$(\sigma - 1)(e_1) + e_2 - e_3 = e_5, \quad \varrho(e_5) = e_4, \quad \varrho(e_4) = e_6.$$

Therefore, all the basis vectors for $\mathrm{Ker}(\widehat{\phi})$ can be successively obtained from e_1 by applying suitable elements of $\mathrm{End}(J)$. This completes the proof of Corollary 2.

4. Arithmetic over $K(J_s[5])$. The following proposition gives the hyperelliptic torsion packet on F_s, i.e. the set of points $P \in F_s(\overline{\mathbb{Q}})$ such that $[P - \infty_s]$ is a torsion point on J_s.

PROPOSITION 4 (Coleman, [2]). *The hyperelliptic torsion packets on* F_1, F_2, F_3 *are the sets*

$$T_1 = \{\infty_1, (0,0)_1, (1,0)_1, (1/2, \zeta^i/4^{1/5}), (a, -\zeta^i), (b, -\zeta^i)\},$$
$$T_2 = \{\infty_2, (0,0)_2, (1,0)_2, (-1, \zeta^i 2^{1/5}), (b^2, -\zeta^i b), (a^2, -\zeta^i a)\},$$
$$T_3 = \{\infty_3, (0,0)_3, (1,0)_3, (2, -\zeta^i 8^{1/5}), (-a, -\zeta^i a), (-b, -\zeta^i b)\},$$

respectively, where $i = 0, 1, \ldots, 4$.

Let L be the field of definition of $J_s[5]$. The field L is independent of s. In fact, it follows from a general theorem of Greenberg ([5]) that L is the number field generated over K by the 5th roots of the cyclotomic units in K^+. Fix $c \in \overline{\mathbb{Q}}$ such that $c^5 = a$. Since the group of cyclotomic units in K^+ is generated by -1 and a, it follows that $L = K(c)$. By Faddeev's work ([3]), we know that each $J_s(K)$ is finite. It makes sense to ask whether this is also true for the groups $J_s(L)$. We will prove the following proposition:

PROPOSITION 5. *For $s = 1, 2, 3$, the Mordell–Weil rank of J_s over L is a positive multiple of 4. Therefore, the Mordell–Weil rank of J over L is a positive multiple of 12.*

Proof. The second assertion follows from the first since J and J_2^3 are isogenous over $\mathbb{Q}$. Since the curves F_1, F_2, F_3 are isomorphic over $\mathbb{Q}$, it suffices to prove the first assertion for $s = 1$. Consider the point

$$R = [(\zeta^2 b, 1/c^2) - \infty_1] \in J_1(L).$$

By Proposition 4, the point R is an L-rational point of infinite order on J_1, so the rank of J_1 over L is positive. Consider the free abelian group

$$J_1(L)_{\mathrm{inf}} = J_1(L)/J_1(L)_{\mathrm{tors}}.$$

We will once again use the identification $\mathrm{End}(J_1) = \mathbb{Z}[\zeta]$. Clearly, $J_1(L)_{\mathrm{inf}}$ is a $\mathbb{Z}[\zeta]$-module. We now claim that it is a torsion-free $\mathbb{Z}[\zeta]$-module. Indeed, let P be a point of infinite order in $J_1(L)$. Suppose that for integers x_0, x_1, x_2, x_3, not all equal to 0, we have

$$x_0 P + x_1 \zeta P + x_2 \zeta^2 P + x_3 \zeta^3 P \in J_1(L)_{\mathrm{tors}}.$$

Then there exists a positive integer M such that P lies in the kernel of the endomorphism

$$Mx_0 + Mx_1\zeta + Mx_2\zeta^2 + Mx_3\zeta^3$$

of J_1. Now, since J_1 is a simple abelian variety, the latter endomorphism (which, by assumption, is non-trivial) has finite kernel. Therefore, P is a torsion point in $J_1(L)$, which is absurd, and this proves the claim.

Therefore, since $\mathbb{Z}[\zeta]$ is a principal ideal domain, it follows that $J_1(L)_{\mathrm{inf}}$ is a free $\mathbb{Z}[\zeta]$-module, hence the $\mathbb{Z}$-rank of $J_1(L)_{\mathrm{inf}}$ is a multiple of 4. This completes the proof of Proposition 5.

We conclude this paper by computing generators for the groups $J_s[5]$. In view of Proposition 2, we only need to exhibit a divisor class q_s such that $q_s \in J_s[5] - J_s(K)$. Note that $J_s[5] = J_s[\pi^4]$.

We first take $s = 1$. We will find points (u_1, v_1) and (u_2, v_2) in $F_1(\overline{\mathbb{Q}})$ such that

$$\pi[(u_1, v_1) + (u_2, v_2) - 2\infty_1] = r_1.$$

The hyperelliptic involution on F_1 is given by $(u, v) \mapsto (1-u, v)$ and acts as multiplication by -1 on J_1. Therefore, it is sufficient to find points (u_1, v_1), (u_2, v_2) as above and a rational function on F_1 whose divisor is

$$(u_1, v_1) + (1 - u_1, \zeta v_1) + (u_2, v_2) + (1 - u_2, \zeta v_2) + P_1 - 5\infty_1.$$

For a rational function of the form $u - dv^2 - ev - f$, where d, e, f are in $\overline{\mathbb{Q}}$, this means that the equation in v

$$v^5 = (dv^2 + ev + f)(1 - dv^2 - ev - f)$$

has the five roots -1, v_1, ζv_1, v_2, ζv_2, and that the corresponding values for $u = dv^2 + ev + f$ are a, u_1, $1 - u_1$, u_2, $1 - u_2$, respectively. We now make a choice of the quantities d, e, f, u_1, u_2, v_1, v_2 so that the conditions mentioned in the previous sentence are satisfied.

Let d be any element in $\overline{\mathbb{Q}}$ satisfying

$$d^5 - (5a + 5)d^3 + (15a + 10)d - (11a + 7) = 0.$$

Define e and f as follows:

$$e = (2a - 3)(d^3 - d), \qquad 2f - 1 = (5a - 8)d^5 + (9 - 6a)d^3 + (a - 1)d.$$

Also, let v_1 and v_2 be the roots in $\overline{\mathbb{Q}}$ of the equation

$$d(\zeta^2 + 1)v^2 + e(\zeta + 1)v + (2f - 1) = 0,$$

and define

$$u_1 = dv_1^2 + ev_1 + f, \qquad u_2 = dv_2^2 + ev_2 + f.$$

We claim that these choices satisfy the required conditions. Indeed, note that

$$v_1 + v_2 = \zeta^2(a - 1)(d^2 - 1), \qquad v_1 v_2 = \zeta^4((5 - 3a)d^4 + (3a - 6)d^2 + 1).$$

Then a straightforward albeit tedious computation making use of our definitions of the quantities involved shows that

$$v^5 - (dv^2 + ev + f)(1 - dv^2 - ev - f) = (v + 1)(v - v_1)(v - v_2)(v - \zeta v_1)(v - \zeta v_2).$$

Moreover, it is easy to check that $1 - u_i = d(\zeta v_i)^2 + e(\zeta v_i) + f$ for $i = 1, 2$ and $d - e + f = a$. This proves the claim.

Thus, given our choices above, we define

$$q_1 = [(u_1, v_1) + (u_2, v_2) - 2\infty_1], \qquad q_2 = g(q_1), \qquad q_3 = h^{-1}(g(q_1)).$$

Since g and $h^{-1}g$ are isomorphisms over $\mathbb{Q}$, our arguments above prove the following proposition:

PROPOSITION 6. *For $s = 1, 2, 3$, the group $J_s[5]$ is generated by q_s as a module over $\mathbb{Z}[\pi]$. Alternatively, a $\mathbb{Z}/5\mathbb{Z}$-basis for $J_s[5]$ is given by the set $\{q_s, r_s, t_s, w_s\}$.*

References

[1] R. Coleman, *Torsion points on abelian étale coverings of* $\mathbf{P}^1 - \{0, 1, \infty\}$, Trans. Amer. Math. Soc. 311 (1989), 185–208.

[2] —, *Torsion points on Fermat curves*, Compositio Math. 58 (1986), 191–208.

[3] D. Faddeev, *On the divisor class groups of some algebraic curves*, Dokl. Akad. Nauk SSSR 136 (1961), 296–298 (in Russian); English transl.: Soviet Math. Dokl. 2 (1961), 67–69.

[4] D. Grant, *A proof of quintic reciprocity using the arithmetic of* $y^2 = x^5 + 1/4$, Acta Arith. 75 (1996), 321–337.

[5] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. 42 (1981), 345–359.
[6] 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.
[7] N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of the Fermat curve*, Canad. J. Math. 30 (1978), 1183–1205.
[8] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of Z*, Compositio Math. 81 (1992), 223–236.
[9] C. Lim, *The geometry of the Jacobian of the Fermat curve of exponent five*, J. Number Theory 41 (1991), 102–115.
[10] D. Prapavessi, *On the Jacobian of the Klein curve*, Proc. Amer. Math. Soc. 122 (1994), 971–978.
[11] D. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math. 39 (1977), 95–127.
[12] P. Tzermias, *Torsion points on Fermat Jacobians*, Internat. Math. Res. Notices 1997, no. 2, 57–66.

Centre de Recerca Matemàtica
Institut d'Estudis Catalans
Apartat 50
08193 Bellaterra, Spain
E-mail: tzermias@crm.es

Received on 26.11.1996
and in revised form on 18.7.1997 (3085)