C. Hai Lim
Nagoya Math. J.
Vol. 125 (1992), 73–92

THE JACOBIAN OF A CYCLIC QUOTIENT OF A FERMAT CURVE

CHONG HAI LIM

§ 0. Introduction

Fix a positive integer m. Let F_m denote the Fermat curve over $\mathbf{Q}$ of degree m, given by the projective equation

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

Let $\mu_m \subseteq \overline{\mathbf{Q}}$ be the group of m-th roots of unity, Δ be the image of μ_m in μ_m^3 under the diagonal embedding, and let $G_m = \mu_m^3/\Delta$. Then G_m acts on F_m as follows:

$$(\xi_1, \xi_2, \xi_3) \bmod \Delta\colon (X, Y, Z) \longrightarrow (\xi_1 X, \xi_2 Y, \xi_3 Z).$$

The group ring $\mathbf{Z}[G_m]$ acts on the Jacobian J_m of F_m. Let $K = \mathbf{Q}(\mu_m)$. Then J_m/K has CM by $\mathbf{Z}[G_m]$ [4].

Let $a, b, c \in \mathbf{Z}$, with $a + b + c = 0$, $(a, b, c, m) = 1$, and none of a, b, c divisible by m. Let $\Gamma^m_{a,b,c}$ be the following subgroup of G_m:

$$\{(\xi_1, \xi_2, \xi_3) \in \mu_m^3 \mid \xi_1^a \xi_2^b \xi_3^c = 1\}/\Delta.$$

Then the quotient curve

$$F^m_{a,b,c} = \Gamma^m_{a,b,c} \backslash F_m$$

is defined over $\mathbf{Q}$, and has equation $y^m = (-1)^c x^a (1-x)^b$. Its Jacobian $J^m_{a,b,c}$ has CM by

$$\mathbf{Z}[G_m/\Gamma^m_{a,b,c}].$$

Let g be a generator of the cyclic group $G_m/\Gamma^m_{a,b,c}$, and let $f_m(x)$ denote the m-th cyclotomic polynomial. Then the sum of the images of the maps

$$J^d_{a,b,c} \longrightarrow J^m_{a,b,c}$$

induced from $F^m_{a,b,c} \to F^d_{a,b,c}$, $(x, y) \to (x, y^{m/d})$, as d varies over the set of

Received January 7, 1991.

proper divisors of m, generates the abelian subvariety $f_m(g)J^m_{a,b,c}$ of $J^m_{a,b,c}$. We define $(J^m_{a,b,c})^{\text{new}}$ to be the quotient of $J^m_{a,b,c}$ by $f_m(g)J^m_{a,b,c}$.

In [8], Koblitz-Rohrlich determined the necessary and sufficient conditions for $(J^m_{a,b,c})^{\text{new}}$ to be non-simple and its decomposition into simple factors up to isogeny in the case when $(m, 6) = 1$. Aoki [1] has solved this problem for all sufficiently large m. In § 2, we use the above mentioned results to determine the ring of rational endomorphisms of some non-simple $(J^m_{a,b,c})^{\text{new}}$.

In the rest of this paper, we let p be an odd prime, fix a cyclic quotient curve of F_p and denote its Jacobian by A. From the work of Koblitz-Rohrlich [8] and Schmidt [12], we know that A is either absolutely simple or isogeneous to a cube of an absolutely simple abelian variety over the p-th cyclotomic field $\mathbf{Q}(\mu_p)$. When A is simple, $\operatorname{End}(A)$ is isomorphic to the ring of integers in $\mathbf{Q}(\mu_p)$. In § 4, we shall completely characterize the endomorphism ring of A whenever it is non-simple. We then use this information to show in § 6 that A is in fact isomorphic over $\mathbf{Q}(\mu_p)$ to a cube of a simple abelian variety. A special case of this result ($p = 7$) is that the Jacobian $\operatorname{Jac}(C)$ of the Klein curve

$$C\colon X^3Y + Y^3Z + Z^3X = 0$$

is isomorphic to a cube of an elliptic curve [10] (in fact, the elliptic modular curve $J_0(49)$).

§ 1. Preliminaries

For the Fermat curve F_m, let $x = X/Z$ and $y = Y/Z$. Now let $r, s, t \in \mathbf{Z}$, $0 < r, s, t < m$ and $r + s + t \equiv 0 \pmod{m}$. Then

$$w_{r,s,t} = x^{r-1}y^{s-1}\frac{dx}{y^{m-1}}$$

is a differential form of the second kind on F_m. G_m is generated by $\sigma = (\zeta, 1, 1)$ and $\tau = (1, \zeta, 1)$, where ζ is a fixed primitive m-th root of unity, and the forms $w_{r,s,t}$ are eigenforms for the action of G_m: $(\sigma^j\tau^k)^*w_{r,s,t} = \zeta^{rj+sk}w_{r,s,t}$. Since the characters on $(\mathbf{Z}/m\mathbf{Z})^2$ are mutually distinct,

$$\Omega = \{w_{r,s,t} \mid 0 < r, s, t < m, r + s + t \equiv 0 \pmod{m}\}$$

is a basis of the de Rham cohomology $H^1_{\mathrm{DR}}(F_m)$. $\Omega_1 = \{w_{r,s,t} \in \Omega \mid r + s + t = m\}$ is a basis for $H^0(F_m, \Omega^1)$ in the Hodge splitting of $H^1_{\mathrm{DR}}(F_m)$.

The set of elements of Ω invariant under the action of $\Gamma^m_{a,b,c}$ descends to a basis of eigenforms for $H^1_{DR}(J^m_{a,b,c})$ under the action of $\mathbf{Z}[G_m/\Gamma^m_{a,b,c}]$. $(J^m_{a,b,c})^{\text{new}} = J^{\text{new}}$ has CM (in the sense of Shimura-Taniyama) by the ring of integers

$$\mathbf{Z}[G_m/\Gamma^m_{a,b,c}]/(f_m(g)) \approx \mathcal{O}_K$$

of $K = \mathbf{Q}(\mu_m)$, with CM type

$$H^m_{a,b,c} = \{h \in (\mathbf{Z}/m\mathbf{Z})^* \mid \langle ha\rangle + \langle hb\rangle + \langle hc\rangle = m\},$$

where $\langle h\rangle$ denotes the unique representative of h modulo m between 0 and $m-1$.

Let $\mathscr{E}$ denote the set of positive integers m which are different from each of the following numbers:

2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30,
36, 39, 40, 42, 48, 54, 60, 66, 72, 78, 84, 90, 120, 156, 180.

Then from the works of Koblitz-Rohrlich (for the cases where m is relatively prime to 6) [8] and Aoki [1], for $m \in \mathscr{E}$, J^{new} is non-simple if and only if

(1) (a, b, c) is equivalent to $(1, r, -(1+r))$, where $1 + r + r^2 \equiv 0 \pmod{m}$, or

(2) (a, b, c) is equivalent to $(1, s, -(1+s))$, where $s^2 \equiv 1 \pmod{m}$ and $s \not\equiv \pm 1 \pmod{m}$, and $s \neq m/2 + 1$ if $2^3 \mid m$, or

(3) (a, b, c) is equivalent to $(1, 1, -2)$, with $2^2 \mid m$, or

(4) (a, b, c) is equivalent to $(1, m/2+1, m/2-2)$, with $2^3 \mid m$.

In case (1), J^{new} is isogeneous to a cube of an absolutely simple abelian variety. In cases (2) and (3), J^{new} is isogeneous to a square of a simple abelian variety. Finally in case (4), J^{new} is isogeneous to X^4 for some simple abelian variety X.

We shall denote J^{new} by A and B in the first and second cases respectively.

Let ρ be the automorphism of F_m given by

$$(X, Y, Z) \longrightarrow (Z, X, Y).$$

Let Γ_A and J_A denote the $\Gamma^m_{a,b,c}$ and $J^m_{a,b,c}$ associated with A. Since

$$\rho\Gamma_A\rho^{-1} \subseteq \Gamma_A,$$

ρ induces an automorphism of G_m/Γ_A by conjugation. We note that $f_m(x^l)$

is divisible by $f_m(x)$ if l and m are relatively prime. Hence, if g is a generator of G_m/Γ_A, then

$$\rho f_m(g)J_A = f_m(\rho g \rho^{-1})J_A \subseteq f_m(g)J_A\,.$$

So ρ induces an automorphism ρ of A such that the following diagram commutes:

$$\begin{array}{ccc} J_m & \xrightarrow{\ \rho\ } & J_m \\ \downarrow & & \downarrow \\ J_A & \xrightarrow{\ \rho\ } & J_A\,. \\ \downarrow & & \downarrow \\ A & \xrightarrow{\ \rho\ } & A \end{array}$$

Let $\iota \in \mathrm{Aut}(F_m)$ be given by

$$\iota\colon (X, Y, Z) \longrightarrow (Y, X, Z)\,.$$

Then we have a similar commutative diagram to the one above with (A, ρ) replaced by (B, ι).

Since

$$H^{1,0}(J^{\text{new}}, \mathbf{C}) = \bigoplus_{h \in H^m_{a,b,c}} V(\langle ha\rangle, \langle hb\rangle, \langle hc\rangle)\,,$$

where

$$V(a, b, c) = \{\eta \in H^1(F_m, \mathbf{C}) \,|\, g^*\eta = \xi_1^a \xi_2^b \xi_3^c \eta \text{ for all } g = (\xi_1, \xi_2, \xi_3) \in G_m\}\,,$$

a basis of holomorphic differential forms for $H^0(J^{\text{new}}, \Omega^1)$ is

$$\{w_{\langle ha\rangle, \langle hb\rangle, \langle hc\rangle} \,|\, h \in H^m_{a,b,c}\}\,.$$

The following lemma shows that the abelian varieties A and B are isogeneous to

$$\prod_{l=0}^{2} A/\langle g_l\rangle \quad \text{and} \quad \prod_{l=0}^{1} B/\langle h_l\rangle$$

respectively, where g_l and h_l denote $\sigma^l \rho \sigma^{-l}$ and $\sigma^l \iota \sigma^{-l}$ respectively.

LEMMA 1.1. *$H^0(J_A, \Omega^1)^{\langle g_l\rangle}$ is spanned by*

$$g_l^*\{w_{r,s} \,|\, w_{r,s} \in H^0(J_A, \Omega^1)\}\,,$$

and $H^0(J_A, \Omega^1) = \bigoplus_{l=0}^{2} H^0(J_A, \Omega^1)^{\langle g_l\rangle}$. Similar statements hold for $H^0(J_B, \Omega^1)$, h_0 and h_1.

https://doi.org/10.1017/S0027763000003901 Published online by Cambridge University Press

Proof. Let V_l and W_l denote $(1 + g_l + g_l^2)^* H^0(J_A, \Omega^1)$ and $H^0(J_A, \Omega^1)^{\langle g_l \rangle}$ respectively. Then $V_l \subseteq W_l$ and $\dim V_l = \dim H^0(J_A, \Omega^1)/3$ by definition.

We claim that $W_j \cap (W_k + W_l) = \{0\}$ when $\{j, k, l\} = \{0, 1, 2\}$. We verify this for $j = 0$, $k = 1$ and $l = 2$. The other cases are treated similarly.

Let $w_0 = w_1 + w_2$, where $w_l \in W_l$ $(l = 0, 1, 2)$. Then $w_1 = (\sigma\rho\sigma^{-1})^* w_0 - (\sigma\rho\sigma^{-1})^* w_2 = (\sigma^{-(r+2)})^* w_0 - (\sigma^{r+2})^* w_2$. Therefore, $(\sigma^{-(r+2)} - 1)^* w_0 = (1 - \sigma^{r+2})^* w_2$. Applying $(\sigma^{r+2})^*$ to both sides of the latter equation, we obtain $(1 - \sigma^{r+2})^* (w_0 - (\sigma^{r+2})^* w_2) = 0$. In particular,

$$w_0 - (\sigma^{r+2})^* w_2 \in H^0(F_A/\langle\sigma\rangle, \Omega^1) \approx H^0(\mathbf{P}^1, \Omega^1)\,.$$

Hence, $w_0 = \rho^* w_0 = \rho^*(\sigma^{r+2})^* w_2 = (\sigma^{r+2}\rho)^* w_2 = (\sigma^2)^*(\sigma^2\rho\sigma^{-2})^* w_2 = (\sigma^2)^* w_2$, and $(\sigma^r)^* w_2 = w_2$. So, $w_2 = 0$, and $w_0 = w_1 \in W_0 \cap W_1$, which we can show to be $\{0\}$, as before. □

Let $A_l = A/\langle g_l \rangle$ and $B_l = B/\langle h_l \rangle$. Then each A_l and B_l is simple, and admits CM by the ring of integers in $L = K^{\langle r \rangle}$ and $M = K^{\langle s \rangle}$ respectively. To be precise, the endomorphisms $\sigma + \sigma^r + \sigma^{r^2}$ and $\sigma + \sigma^s$ of A and B descend to endomorphisms on A_0 and B_0 respectively. We identify the products $\prod_{l=0}^2 A_l$ and $\prod_{l=0}^1 B_l$ with $(A_0)^3$ and $(B_0)^2$ respectively through fixed isomorphisms $A_l \xrightarrow{\approx} A_0$ and $B_l \xrightarrow{\approx} B_0$.

Let us fix some terminology. (1) If R is a ring, let $\Delta_n(R)$ be the subspace of the ring of $n \times n$-matrices $M_n(R)$ with entries in R consisting of all the diagonal elements. If $\alpha_1, \cdots, \alpha_n \in R$, let $\Delta(\alpha_1, \cdots, \alpha_n)$ be the matrix $(\alpha_{i,j})$ in $\Delta_n(R)$ with $\alpha_{i,j} = \delta_{i,j}\alpha_j$.

(2) If X is an abelian variety, we associate to an endomorphism ϕ of X^n, the matrix U_ϕ in $M_n(\mathrm{End}(X))$, if on points, $\phi\colon \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} \to U_\phi \cdot \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix}$.

(3) Let $\phi\colon X \to Y$ be an isogeny of degree N. Let $\bar{\phi}\colon Y \to X$ be such that $\bar{\phi}\phi$ is multiplication by N on X. Let $F_\phi\colon \mathrm{End}^0(X) \to \mathrm{End}^0(Y)$ map α in $\mathrm{End}(X)$ to $N^{-1}(\phi\alpha\bar{\phi})$ in $\mathrm{End}^0(Y)$.

§ 2. Rational endomorphisms

Let Σ_l be a basis for $H^0(A_l, \Omega^1)$ consisting of forms of the type $(1 + g_l + g_l^2)^* w_{r,s}$. Then $\Sigma = \bigcup_{l=0}^2 \Sigma_l$ is a basis for $H^0(A, \Omega^1)$. The main result in this section is

PROPOSITION 2.1. *Let $m \in \mathscr{E}$. Then the following sequences are exact:*

$$0 \longrightarrow (f_m(\sigma)) \longrightarrow \mathbf{Q}[\sigma, \rho] \longrightarrow \mathrm{End}^0(A) \longrightarrow 0\,,$$
$$0 \longrightarrow (f_m(\sigma)) \longrightarrow \mathbf{Q}[\sigma, \iota] \longrightarrow \mathrm{End}^0(B) \longrightarrow 0\,.$$

Proof. We will prove that $F\colon \mathbf{Q}[\sigma, \rho] \to \mathrm{End}^0(A_0^3) = M_3(L)$ is surjective. Since $f_m(\sigma) \in \mathrm{Ker}\,(F)$, a dimension argument shows that the first sequence is exact. We omit the proof of exactness of the second sequence.

The matrices for $(1 + g_l + g_l^2)^*$ on $H^0(A, \Omega^1)$, with respect to the basis Σ are:

$$\begin{pmatrix} 3 & 0 & 0 \\ M_0 & 0 & 0 \\ N_0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 3 & 0 \\ 0 & M_1 & 0 \\ 0 & N_1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & M_2 \\ 0 & 0 & N_2 \end{pmatrix}$$

for $l = 0, 1, 2$ respectively.

Now $w_{1,r} \in H^0(A, \Omega^1)$ and

$$(1 + g_0 + g_0^2)^*(1 + g_1 + g_1^2)^* w_{1,r} = (1 + \zeta^{r^2+1} + \zeta^{r^2+2})(1 + g_0 + g_0^2)^* w_{1,r}\,.$$

Let $l \in (\mathbf{Z}/m\mathbf{Z})^* - \{1, (r^2 + 1)(r^2 + 2)^{-1}, (r^2 + 1)(r^2 + 2)^{-1}\}$. Since $\{\zeta^a \mid a \in (\mathbf{Z}/m\mathbf{Z})^*\}$ is a $\mathbf{Z}$-basis for $\mathcal{O}_K$, ζ^{r^2+1}, $\zeta^{(r^2+1)l}$, $\zeta^{(r^2+2)}$, $\zeta^{(r^2+2)l}$ are linearly independent over $\mathbf{Q}$. Thus $\zeta^{r^2+1} + \zeta^{r^2+2}$ is not in $\mathbf{Q}$, and $1 + \zeta^{r^2+1} + \zeta^{r^2+2} \neq 0$. This shows that the matrix M_0 is not the null matrix. In a similar way, we can prove that N_0, M_1, N_1, M_2 and N_2 are not zero. Then, in $\mathrm{End}\,(A_0^3) = M_3(\mathcal{O}_L)$, the matrices for $(1 + g_l + g_l^2)$ are:

$$\begin{pmatrix} 3 & 0 & 0 \\ \alpha_0 & 0 & 0 \\ \beta_0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 3 & 0 \\ 0 & \alpha_1 & 0 \\ 0 & \beta_1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & \alpha_2 \\ 0 & 0 & \beta_2 \end{pmatrix}$$

for $l = 0, 1, 2$ respectively, where each α_j, β_j are in $\mathcal{O}_L$.

Let $X, Y, Z \in \mathbf{Q}[\sigma]$. In the group ring $\mathbf{Q}[\sigma, \rho]$, we have the following:

$$(1 + g_l + g_l^2)(X + \rho Y + \rho^2 Z) = (1 + g_l + g_l^2)(X + Y\sigma^{l(1-r^2)} + Z\sigma^{l(1-r)})$$

by using the relations $\rho\sigma\rho^{-1} = \sigma^r$ and $\rho^{-1}\sigma\rho = \sigma^{r^2}$ in $\mathrm{Aut}\,(A)$.

The determinant of the matrix $\begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma^{1-r^2} & \sigma^{1-r} \\ 1 & \sigma^{2-2r^2} & \sigma^{2-2r} \end{pmatrix}$ is $D = f(\sigma) \in \mathbf{Q}[\sigma]$, where

$$f(x) = x^{\langle 4-r\rangle} - x^{\langle 4-r^2\rangle} + x^{\langle 1-r\rangle} - x^{\langle 1-r^2\rangle} + x^{\langle 2-2r\rangle} - x^{\langle 2-2r^2\rangle} \in \mathbf{Q}[x]\,.$$

Since $r^2 + r + 1 \equiv 0 \pmod m$, the exponents $4 - r$, $4 - r^2$, $1 - r$, $1 - r^2$, $2 - 2r$, $2 - 2r^2$ are pairwise distinct $(\mathrm{mod}\, m)$ except possibly when $m \mid 3^2$

https://doi.org/10.1017/S0027763000003901 Published online by Cambridge University Press

or $m = 13$. Hence, $D \neq 0$ (the exceptional case $m = 13$ is taken care of by inspection). In particular, there are $X, Y, Z \in \mathbf{Z}[\sigma]$ and a positive integer N such that

$$X + Y + Z = ND, \quad X + Y\sigma^{1-r^2} + Z\sigma^{1-r} = 0, \quad X + Y\sigma^{2-2r^2} + Z\sigma^{2-2r} = 0.$$

With the latter choice of X, Y and Z, let the matrix of $(X + \rho Y + \rho^2 Z)$ in $M_3(\mathcal{O}_L)$ be $(\alpha_{i,j})$. From $(1 + g_1 + g_1^2)(X + \rho Y + \rho^2 Z) = 0$, we conclude that $\alpha_{2,j} = 0$ for all j. On the other hand, $\alpha_{3,j} = 0$ for all j, follows from $(1 + g_2 + g_2^2)(X + \rho Y + \rho^2 Z) = 0$. Then the matrix of $(X + \rho Y + \rho^2 Z)(1 + g_0 + g_0^2)$ is

$$\begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 & 0 \\ \alpha_0 & 0 & 0 \\ \beta_0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \delta_0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

where $\delta_0 = 3\alpha_{1,1} + \alpha_0\alpha_{1,1} + \beta_0\alpha_{1,3} \in \mathcal{O}_L$.

Claim. $\delta_0 \neq 0$.

Suppose, on the contrary, that $\delta_0 = 0$. Then

$$N^{-1}(1 + g_0 + g_0^2)(X + \rho Y + \rho^2 Z)(1 + g_0 + g_0^2) = (1 + \rho + \rho^2)D(1 + g_0 + g_0^2) = 0.$$

We note that

$$D^*(1 + \rho + \rho^2)^* w_{1,r} = f(\zeta)w_{1,r} + f(\zeta^r)w_{r,m-r-1} + f(\zeta^{r^2})w_{m-r-1,1}$$

and if $\lambda_m = f(\zeta^r) + f(\zeta^r) + f(\zeta^{r^2})$,

$$(1 + g_0 + g_0^2)^* D^*(1 + \rho + \rho^2)^* = \lambda_m(w_{1,r} + w_{r,m-r-1} + w_{m-r-1,1}).$$

We will show that $\lambda_m \neq 0$.

First, consider the prime case $m = p$. If $\lambda_p = 0$, then the polynomial $g(x) = f(x) + f_1(x) + f_2(x)$, where $f_j(x)$ is the polynomial obtained by replacing each exponent $\langle a \rangle$ in $f(x)$ by $\langle ar^j \rangle$, has degree at most $p - 1$, and ζ as a root. We note that $4 - r$, $4 - r^2$, $1 - r$, $1 - r^2$, $2 - 2r$, $2 - 2r^2$ are distinct elements in $(\mathbf{Z}/p\mathbf{Z})^*/\{1, r, r^2\}$ for $p \neq 7, 19, 31$. Thus, with the above exceptions, $g(x) \neq 0$ and therefore, $g(x) = \pm f_p(x)$. This is a contradiction, since $g(1) = 0$ but $f_p(1) = p$. Inspection shows that $\lambda_p \neq 0$ for $p = 7, 19, 31$.

Now we treat the composite case.

Suppose that l is a prime divisor of m and $r - 4$. Then $r^2 + r + 1 \equiv 0 \pmod{l^k}$ and $r \equiv 4 \pmod{l^k}$ imply that $l^k | 21$. Thus $(m, r^2 - 4) | 21$.

Similarly $(m, r-4)|21$. However, 7 can divide at most one of the two numbers $(m, r-4)$ and $(m, r^2-4) = (m, m-r-5)$. Furthermore, it is not difficult to verify that $(1-r, m) = (1-r^2, m)|3$.

Case (1). First suppose that each of the integers $1-r$, $1-r^2$, $2-2r$, $2-2r^2$ are relatively prime to m (this is the case when $(m, 6) = 1$).

Case (1a). Both $(m, r-4)$ and (m, r^2-4) are co-prime to 7.

For $\beta \in K = \mathbf{Q}(\mu_m)$, let $\beta^{1+r+r^2} = \beta + \beta^r + \beta^{r^2}$, where $\{1, r, r^2\} \subseteq \mathrm{Gal}(K/\mathbf{Q})$. We note that if two of the integers $4-r$, $4-r^2$, $1-r$, $1-r^2$, $2-2r$, $2-2r^2$ represent the same class in $(\mathbf{Z}/m\mathbf{Z})^*/\{1, r, r^2\}$, then $m \in S$, where S is a finite set of integers whose elements can be easily found using the congruence relation $r^2 + r + 1 \equiv 0 \pmod{m}$. If $m \in S \cap \mathscr{E}$, inspection shows that $\lambda_m \neq 0$. If m is not in S, a $\mathbf{Z}$-basis for $\mathcal{O}_L$ is

$$\{\zeta^{a(1+r+r^2)} \mid a \in (\mathbf{Z}/m\mathbf{Z})^*/\{1, r, r^2\}\},$$

and we conclude that λ_m is non-zero since it is a linear combination of elements of a subset of a $\mathbf{Z}$-basis for $\mathcal{O}_L$.

Case (1b). $7 \| (m, r^2-4)$.

The elements of $\mathrm{Gal}(K/\mathbf{Q})$ which fix $\mathbf{Q}(\zeta^7)$ elementwise are the units $j \in (Z/m\mathbf{Z})^*$ such that $j \equiv 1 \pmod{m/7}$. We fix one such $j = 1 + k(m/7) \neq 1$ in $(\mathbf{Z}/m\mathbf{Z})^*$. We make the following observation: if a and bj are equal in $(\mathbf{Z}/m\mathbf{Z})^*/\{1, r, r^2\}$, then $a \equiv r^l bj \pmod{m}$ implies $a \equiv r^l b \pmod{m/7}$, and so a and b are equal in $(\mathbf{Z}/(m/7)\mathbf{Z})^*/\{1, r, r^2\}$.

The calculations for case (1a) show that $1-r$, $1-r^2$, $2-2r$, $2-2r^2$, $4-r$ are distinct in $(\mathbf{Z}/m\mathbf{Z})^*/\{1, r, r^2\}$ (hence in $(\mathbf{Z}/(m/7)\mathbf{Z})^*/\{1, r, r^2\}$), except possibly when $m/7 \in S$. For these exceptional values of m, $\lambda_m \neq 0$ by inspection. For the other values of m, the observation in the previous paragraph shows that $\bar{\lambda}_m = \lambda_m - \zeta^{(4-r^2)(1+r+r^2)}$ is such that $\bar{\lambda}_m^j \neq \bar{\lambda}_m$, since $\{\zeta^{a(1+r+r^2)} \mid a \in (\mathbf{Z}/m\mathbf{Z})^*/\{1, r, r^2\}\}$ is a $\mathbf{Z}$-basis for $\mathcal{O}_L$. Thus $\bar{\lambda}_m \notin \mathbf{Q}(\zeta^7)$, and $\lambda_m \neq 0$.

Case (1c). $7 \| (m, r-4)$.

This is case (1b), with the roles of r and r^2 reversed.

Case (2). Suppose now that $(1-r, m) = 3$. If m is odd, then we have that

$$(1-r, m) = (1-r^2, m) = (2-2r, m) = (2-2r^2, m) = 3$$
$$\text{and} \quad 9|(4-r, m)\cdot(4-r^2, m)|9.7\,.$$

We apply the arguments in case (1) applied to $(1-r)/3$, $(1-r^2)/3$, $(2-2r)/3$, $(2-2r^2)/3$, $(4-r)/3$, $(4-r^2)/3$ in $(\mathbf{Z}/(m/3)\mathbf{Z})^*/\{1, r, r^2\}$.

If m is even, we look at $(1-r)/3$, $(1-r^2)/3$, $(2-2r)/6$, $(2-2r^2)/6$, $(4-r)/3$, $(4-r^2)/3$ instead. The calculations are similar to the ones above.

This proves that $\lambda_m \neq 0$, and hence our claim that $\delta_0 \neq 0$. We have shown that $F((X+\rho Y+\rho^2 Z)(1+g_0+g_0^2)) = \Delta(\delta_0, 0, 0)$, with $\delta_0 \neq 0$. Similarly, we can show the existence of $X_l, Y_l, Z_l \in \mathbf{Z}[\sigma]$ such that $(X_l+\rho Y_l + \rho^2 Z_l)(1+g_l+g_l^2)$ are mapped onto

$$\Delta(0, \delta_1, 0) \quad \text{and} \quad \Delta(0, 0, \delta_2) \qquad \text{for } l = 1, 2 \text{ respectively.}$$

In particular, since $L \to \mathrm{End}^0(A_0^3) = M_3(L)$ (in which ζ^{1+r+r^2} is mapped to $(\sigma+\sigma^r+\sigma^{r^2})^3$) is the diagonal embedding by the theory of complex multiplication, we conclude that

$$\Delta_3(L) \subseteq \mathrm{Im}(F) \subseteq M_3(L).$$

We observe that

$$\sigma^*(\sigma(1+\rho+\rho^2)\sigma^{-1})^* w_{a,b} = (1+\rho+\rho^2)^*\sigma^* w_{a,b}, \quad \text{and}$$
$$\sigma^*(\sigma^2(1+\rho+\rho^2)\sigma^{-2})^* w_{a,b} = (\sigma(1+\rho+\rho^2)\sigma^{-1})^*\sigma^* w_{a,b}.$$

Thus the matrix for σ in $M_3(\mathcal{O}_L)$ is of the form: $\begin{pmatrix} a & b & c \\ d & 0 & 0 \\ 0 & e & 0 \end{pmatrix}$, for some a, b, c, d and e in $\mathcal{O}_L$ with $cde \in (\mathcal{O}_L)^*$ (this follows from $\det(\sigma)^m = 1$). Therefore the image of F contains the following matrices:

$$\begin{pmatrix} 0 & b & c \\ d & 0 & 0 \\ 0 & e & 0 \end{pmatrix}, \quad \begin{pmatrix} bd & ce & 0 \\ 0 & bd & cd \\ de & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b & c \\ d & 0 & 0 \\ 0 & e & 0 \end{pmatrix}^2, \quad \begin{pmatrix} 0 & ce & 0 \\ 0 & 0 & cd \\ de & 0 & 0 \end{pmatrix}.$$

This completes the proof that F is surjective. □

§ 3. Homology groups

Let $I\colon [0, 1] \to F_m(\mathbf{C})$ denote the one-simplex

$$I(t) = (t^{1/m}, (1-t)^{1/m}, \alpha), \qquad t \in [0, 1],$$

where $\alpha = -1$ if m is odd and a primitive $2m$-th root of unity if m is even. Let g be the one-cycle:

$$g = (\sigma\tau)^{(m-1)/2}(1-\sigma)(1-\tau)I \qquad \text{if } m \text{ is odd, and}$$
$$g = (1-\sigma^{-1})(1-\tau^{-1})I \qquad \text{if } m \text{ is even.}$$

https://doi.org/10.1017/S0027763000003901 Published online by Cambridge University Press

The homology group $H_1(F_m(\mathbf{C}), \mathbf{Z})$ is generated by g [11]. Moreover by the period calculations in [11], we have that $\rho(g) = g$ and $\iota(g) = -g$ [9].

PROPOSITION 3.1. *$H_1(F_m(\mathbf{C}), \mathbf{Z})$ is a cyclic $\mathbf{Z}[G_m]$-module, with g as a generator such that $\rho(g) = g$ and $\iota(g) = -g$ in homology.*

For the rest of this paper, let p be a fixed prime congruent to 1 (mod 6), let r be a fixed cube root of unity modulo p, $K = \mathbf{Q}(\mu_p)$, ζ be a fixed p-th root of unity, and A be the Jacobian variety of the curve F_A:

$$y^p = x(1-x)^r .$$

A has CM by $\mathcal{O}_K$: we fix the embedding

$$\mathcal{O}_K \longrightarrow \mathrm{End}_K(A), \qquad \zeta \longrightarrow \sigma = (\zeta, 1, 1) .$$

Let $\varphi_A\colon F_p \to F_A$ denote the canonical projection, and let I_A be the one simplex $\varphi_A I$ on F_A. Fix a base point e_0 in $F_p(\mathbf{C})$, and let x_0 be its image in $F_A(\mathbf{C})$ under φ_A. The cyclic covering φ_A gives rise to a monomorphism

$$H = \pi_1(F_p(\mathbf{C}), e_0) \longrightarrow \pi_1(F_A(\mathbf{C}), x_0) = G$$

of fundamental groups. G/H is a cyclic group of order p since φ_A has degree p. So H contains the commutator subgroup of G, and the homomorphism

$$H_1(F_p) = H_1(F_p(\mathbf{C}), \mathbf{Z}) \longrightarrow H_1(F_A(\mathbf{C}), \mathbf{Z}) = H_1(F_A)$$

factors as follows:

$$\begin{array}{ccc} H/[H, H] & \longrightarrow & G/[G, G] \\ & \nwarrow \qquad \nearrow & \\ & H/[G, G] & \end{array}$$

Thus, the index of the image T of $H_1(F_p)$ in $H_1(F_A)$ is p. T, by definition, is a cyclic $\mathbf{Z}[\sigma]$-module with $(\sigma - 1)(\sigma^r - 1)I_A$ as a generator by Proposition 3.1.

Let $\bar{T}$ be the $\mathbf{Z}[\sigma]$-submodule of $H_1(F_A)$ generated by $\alpha = (\sigma - 1)I_A$. Then $T \subseteq \bar{T} \subseteq H_1(F_A)$. We claim that $T \neq \bar{T}$, from which it follows that $H_1(F_A) = \bar{T}$.

Identifying

$$\mathbf{Q}[\sigma]/(f_p(\sigma)) \xrightarrow{\approx} K, \quad \sigma \longrightarrow \zeta ,$$

$H_1(F_A) \otimes \mathbf{Q}$ is a vector space over K. Hence the annihilator of $H_1(F_A) \otimes \mathbf{Q}$ as a $\mathbf{Q}[\sigma]$-module is $(f_p(\sigma))$, and the annihilator of $H_1(F_A)$, as a $\mathbf{Z}[\sigma]$-module is

$$(f_p(\sigma))\mathbf{Q}[\sigma] \cap \mathbf{Z}[\sigma] = (f_p(\sigma))\mathbf{Z}[\sigma] .$$

Since $H_1(F_A)$ is torsion-free over $\mathbf{Z}$, and $[H_1(F_A): \bar{T}] < \infty$, $\mathrm{Ann}_{\mathbf{Z}[\sigma]}(\bar{T}) = (f_p(\sigma))\mathbf{Z}[\sigma]$.

Suppose, on the contrary, that $T = \bar{T}$. Then $\alpha = a(\sigma)(\sigma - 1)\alpha$ for some $a(x) \in \mathbf{Z}[x]$. Therefore, $(a(\sigma)(\sigma - 1) - 1)\alpha = 0$ implies $a(x)(x - 1) - 1 = b(x)f_p(x)$ for some $b(x) \in \mathbf{Z}[x]$. Then $-1 = b(1)p$ in $\mathbf{Z}$, a contradiction. Thus, $H_1(F_A) = \bar{T}$.

Let $\bar{I} = \rho I$ and $\bar{I}_A = \varphi_A \bar{I}$. From $\rho(g) = g$ in $H_1(F_p)$, we obtain

$$(\sigma - 1)(\sigma^r - 1)I_A = \sigma^{1 + r((p+1)/2)}(\sigma^r - 1)(\sigma^{p-r-1} - 1)\bar{I}_A$$

in $H_1(F_A)$.

Let $v \in H_1(F_A)$ be such that $(\sigma^r - 1)v = 0$. Passing to $\mathcal{O}_K \subseteq \mathrm{End}_K(A)$, we have $(\zeta^r - 1)v = 0$. Then $pv = \pm N^K_{\mathbf{Q}}(\zeta^r - 1)v = 0$, and $v = 0$. Thus, we have proved

PROPOSITION 3.2. *$H_1(F_A)$ is a cyclic $\mathcal{O}_K$-module with $g_A = (1 - \sigma)I_A$ as a generator. Moreover,*

$$\rho(g_A) = \zeta^{r((p-1)/2)}\left(\frac{\zeta^r - 1}{\zeta^{r^2} - 1}\right)g_A .$$

§ 4. Endomorphisms

In the present section, we prove the following theorem. Let $\pi = \zeta - 1 \in \mathbf{Z}[\zeta] \subseteq \mathrm{End}(A)$ and $W = p^{-1}(1 + r\rho + r^2\rho^2)(\sigma - 1)^{p-3} \in \mathbf{Q}[\sigma, \rho]$.

THEOREM 4.1. *$\mathrm{End}(A) = \mathrm{Im}(\mathbf{Z}[\sigma, \rho, W])$ has group index p^3 over $\mathrm{Im}(\mathbf{Z}[\sigma, \rho])$.*

Proof. By Proposition 2.1, F: $Q[\sigma, \rho] \to \mathrm{End}^0(A)$ is surjective, and by Proposition 3.2, $H_1(F_A)$ is a cyclic $\mathbf{Z}[\zeta]$-module with a generator g_A such that $\rho(g_A) = \eta g_A$, $\rho^2(g_A) = \xi g_A$, where

$$\eta = \zeta^{r((p-1)/2)-1}\frac{(\zeta^r - 1)}{(\zeta^{r^2} - 1)} \quad \text{and} \quad \xi = \zeta^{r^2 + (p+1)/2}\frac{(\zeta^r - 1)}{(\zeta - 1)} .$$

We will use the following to determine $\mathrm{End}(A)$:

$$\mathrm{End}(A) = \{\alpha \in \mathrm{End}^0(A) \mid \alpha(H_1(F_A)) \subseteq H_1(F_A)\} .$$

Let $X, Y, Z \in K$. Then $\alpha = X + Y\rho + Z\rho^2 \in \mathrm{End}(A)$ if and only if $\alpha(\zeta^a g_A) \subseteq H_1(F_A)$ for all $a \in \mathbf{Z}$, or equivalently, for all $a \in \mathbf{Z}$,

$$X\zeta^a + Y\zeta^{ar}\eta + Z\zeta^{-a(r+1)}\xi \in \mathbf{Z}[\zeta]. \tag{4.1}$$

Let $\tilde{X} = X$, $\tilde{Y} = Y\eta$ and $\tilde{Z} = Z\xi$. Then (4.1) reads as

$$\tilde{X}\zeta^a + \tilde{Y}\zeta^{ar} + \tilde{Z}\zeta^{-a(r+1)} \in \mathbf{Z}[\zeta]. \tag{4.2}$$

Using $\tilde{X} + \tilde{Y} + \tilde{Z} \in \mathbf{Z}[\zeta]$ and (4.2) to eliminate $\tilde{X}$, we obtain for all $a \in (\mathbf{Z}/p\mathbf{Z})^*$,

$$\tilde{Y}(\zeta^{ar} - \zeta^a) + \tilde{Z}(\zeta^{-a(r+1)} - \zeta^a) \in \mathbf{Z}[\zeta]. \tag{4.3}$$

For such a, $\zeta^{ar} - \zeta^a$ and $\zeta^{-a(r+1)} - \zeta^a$ are elements of the ideal (π) of $\mathbf{Z}[\zeta]$.

Let $D_{a,b}$ be the determinant of the following matrix:

$$\begin{pmatrix} \zeta^{ar} - \zeta^a & \zeta^{-a(r+1)} - \zeta^a \\ \zeta^{br} - \zeta^b & \zeta^{-b(r+1)} - \zeta^b \end{pmatrix}.$$

Then

$$D_{a,b} = \{\zeta^{ar-b(r+1)} + \zeta^{br+a} + \zeta^{b-a(r+1)}\} - \{\zeta^{ar+b} + \zeta^{a-b(r+1)} + \zeta^{br-a(r+1)}\},$$

and (4.3) implies that

$$D_{a,b}\tilde{Y}, \qquad D_{a,b}\tilde{Z} \in (\pi) \tag{4.4}$$

for all $a, b \in (\mathbf{Z}/p\mathbf{Z})^*$.

If we set $(a, b) = (r+1, 1)$ and $(a, b) = (1, -r)$ in (4.4), we obtain, after simplification,

$$(\zeta^{3r+3} + \zeta^3 + 1 - 3\zeta^{r+2})\tilde{Z} \in (\pi) \quad \text{and} \quad (\zeta^{3r+3} + \zeta^{3r} + 1 - 3\zeta^{2r+1})\tilde{Z} \in (\pi)$$

respectively. By subtracting one from the other, we obtain

$$\zeta^3(\zeta^{r-1} - 1)^2\tilde{Z} \in (\pi).$$

Since $(p, r-1) = 1$, $\pi^2\tilde{Z} \in \mathbf{Z}[\zeta]$. By symmetry, $\pi^2\tilde{Y} \in \mathbf{Z}[\zeta]$.

We write $Y_0 = \tilde{Y}\pi^2$ and $Z_0 = \tilde{Z}\pi^2$. Then $Y_0, Z_0 \in \mathbf{Z}[\zeta]$, and (4.3) can be rewritten as

$$Y_0\frac{(\zeta^r - \zeta)^h}{(\zeta - 1)^2} + Z_0\frac{(\zeta^{-(r+1)} - \zeta)^h}{(\zeta - 1)^2} \in \mathbf{Z}[\zeta],$$

where h ranges over $H = \mathrm{Gal}(K/\mathbf{Q})$, or equivalently,

$$Y_0 + \varepsilon_h \cdot Z_0 \in (\pi) \qquad \text{for all } h \in H, \tag{4.5}$$

where

$$\varepsilon_h = \frac{(\zeta^{r^2} - \zeta)^h}{(\zeta^r - \zeta)^h} = \left(\sum_{j=0}^{r} \zeta^{j(r-1)}\right)^h \in (\mathbf{Z}[\zeta])^* .$$

Clearly, (4.5) may be rewritten as

$$Y_0 \equiv r^2 Z_0 \pmod{\pi}. \tag{4.6}$$

We have proved that $\alpha = X + Y\rho + Z\rho^2$ is in $\mathrm{End}(A)$ if and only if
($*$) $X + \eta Y + \xi Z \in \mathbf{Z}[\zeta]$, and
($**$) $Y_0 \equiv r^2 Z_0 \pmod{\pi}$, where $Y_0 = \pi^2 \eta Y$ and $Z_0 = \pi^2 \xi Z$.
We write

$$Y_0 \equiv a_0 + a_1 \pi \pmod{\pi^2}, \qquad Z_0 \equiv b_0 + b_1 \pi \pmod{\pi^2},$$

where $a_0, a_1, b_0, b_1 \in \mathbf{Z}$. By ($**$), $a_0 \equiv r^2 b_0 \pmod{p}$. Thus, we find that α is congruent to

$$b_0 \frac{1}{\pi^2}\{-(r^2+1) + r^2\eta^{-1}\rho + \xi^{-1}\rho^2\} + a_0 \frac{1}{\pi}(-1 + \eta^{-1}\rho) + b_1 \frac{1}{\pi}(-1 + \xi^{-1}\rho^2) \tag{4.7}$$

modulo $\mathrm{Im}(\mathbf{Z}[\sigma, \rho])$.

By inspection,

$$v_0 = \frac{1}{\pi^2}\{-(r^2+1) + r^2\eta^{-1}\rho + \xi^{-1}\rho^2\},$$

$$v_1 = \frac{1}{\pi}(-1 + \eta^{-1}\rho), \qquad v_2 = \frac{1}{\pi}(-1 + \xi^{-1}\rho^2)$$

satisfy ($*$) and ($**$). Hence, they are in $\mathrm{End}(A)$, and we conclude that

$$\mathrm{End}(A) = \mathrm{Im}(\mathbf{Z}[\sigma, \rho]) + Zv_0 + Zv_1 + Zv_2 . \tag{4.8}$$

From (4.8), the quotient group

$$Q = \mathrm{End}(A)/\Lambda \qquad \text{where } \Lambda = \mathrm{Im}(\mathbf{Z}[\sigma, \rho])$$

is an elementary p-abelian group. So Q is an $\mathbf{F}_p$-vector space, and $\dim_{\mathbf{F}_p}(Q) \leq 3$.

The theorem follows from the next few lemmas. □

LEMMA 4.2. *Let*

$$w = (1 + r\rho + r^2\rho^2)\frac{1}{\pi^2} = \frac{1}{\pi^2} + \frac{r}{(\zeta^r - 1)^2}\rho + \frac{r^2}{(\zeta^{r^2} - 1)^2}\rho^2 \in \mathrm{End}^0(A) .$$

https://doi.org/10.1017/S0027763000003901 Published online by Cambridge University Press

Then $w \in \mathrm{End}(A)$.

Proof. We verify (**) for w. We have $Y_0 = (r\pi^2\eta)/(\zeta^r - 1)^2$ and $Z_0 = (r^2\pi^2\xi)/(\zeta^{r^2} - 1)^2$ in the notation of the proof of Theorem 4.1. Since

$$Y_0 \equiv r\zeta^{r(p-1)/2-1}\frac{(\zeta-1)}{(\zeta^r-1)}\frac{(\zeta-1)}{(\zeta^{r^2}-1)} \equiv r \pmod{\pi}$$

and

$$Z_0 \equiv r^2\zeta^{r^2+(p+1)/2}\frac{(\zeta-1)}{(\zeta^{r^2}-1)}\frac{(\zeta^r-1)}{(\zeta^{r^2}-1)} \equiv r^2 \pmod{\pi},$$

we have $Y_0 \equiv r^2 Z_0 \pmod{\pi}$. Likewise, (*) can be verified for w. This completes the proof of the lemma. □

LEMMA 4.3. *Let* $\Sigma = \mathrm{Im}(\mathbf{Z}[\sigma, \rho, W])$. *Then* $\Sigma \subseteq \mathrm{End}(A)$, *and the following are elements of* Σ:

$$w,\ w_0 = \{1 + (r+1)\rho\}\frac{1}{\pi},\quad w_1 = (r\rho - \rho^2)\frac{1}{\pi}.$$

Proof. Let $u \in (\mathbf{Z}[\zeta])^*$ be the endomorphism of A such that $p = u\pi^{p-1}$. As an element of $\mathrm{End}^0(A)$, $W = wu^{-1}$. Hence the image of w is in Σ, and $\Sigma \subseteq \mathrm{End}(A)$.

From $w\sigma = (\sigma + r\sigma^r\rho + r^2\sigma^{r^2}\rho^2)1/\pi^2$ and $\sigma w = (\sigma + r\sigma\rho + r^2\sigma\rho^2)1/\pi^2$, we have

$$\sigma w - w\sigma \equiv (r-1)\rho\{1 + (r+1)\rho\}\frac{1}{\pi} \pmod{\Lambda}.$$

Since p does not divide $r - 1$ and $\rho \in \mathrm{Aut}(A)$, there is a $\lambda \in \mathbf{Z}$ such that

$$\{1 + (r+1)\rho\}\frac{1}{\pi} \equiv \lambda\rho^2(\sigma w - w\sigma) \pmod{\Lambda}.$$

Hence, $w_0 \in \Sigma$. Since $w_1 \equiv r\rho w_0 \pmod{\Lambda}$, we have $w_1 \in \Sigma$ also. □

LEMMA 4.4. *The mapping* f: $(\mathbf{Z}[\zeta])^3 \to \Lambda$, $(X, Y, Z) \to X + \rho Y + \rho^2 Z$ *is a right* $\mathbf{Z}[\zeta]$*-module isomorphism.*

Proof. By definition, f is surjective. By Proposition 2.1, $f \otimes 1$: $K^3 = (\mathbf{Q}(\mu_p))^3 \to \Lambda \otimes \mathbf{Q}$ is an isomorphism. Hence f is injective. □

LEMMA 4.5. *Let V be the subspace of Q spanned by* w, w_0 *and* w_1. *Then* $\dim_{\mathbf{F}_p}(V) = 3$.

Proof. Let λ, λ_0, $\lambda_1 \in \mathbf{Z}$ be such that

$$\lambda w + \lambda_0 w_0 + \lambda_1 w_1 \in \Lambda . \tag{4.9}$$

Multiplying by π on the right, $\lambda(1 + r\rho + r^2\rho^2) \in \pi\Lambda$. Using Lemma 4.4, $\lambda/\pi \in \mathbf{Z}[\zeta]$. Hence $\lambda \in (\pi) \cap \mathbf{Z} = p\mathbf{Z}$. Since $p/\pi^2 \in \mathbf{Z}[\zeta]$, we have

$$\lambda_0 w_0 + \lambda_1 w_1 \in \Lambda . \tag{4.10}$$

Another application of Lemma 4.4 to (4.10) gives λ_0, $\lambda_1 \in p\mathbf{Z}$. Therefore $\{w, w_0, w_1\}$ is an $\mathbf{F}_p$-basis for V. □

Combining Lemmas 4.3 and 4.5,

$$\dim_{\mathbf{F}_p}(\Sigma/\Lambda) \geq 3 .$$

Since $\dim_{\mathbf{F}_p}(Q) \leq 3$, we have the desired equality: $\mathrm{End}(A) = \Sigma$, and $\mathrm{End}(A)$ has group index p^3 over Λ. This completes the proof of Theorem 4.1.

COROLLARY 4.6. *A free* $\mathbf{Z}$*-basis for* $\mathrm{End}(A)$ *is given by*:

$$\{\rho^j\pi^k \mid 0 \leq j \leq 2,\ 0 \leq k \leq p-4\} \cup \{\rho\pi^{p-3}, \rho^2\pi^{p-3}, \rho\pi^{p-2}\} \cup \{w, w_0, w_1\} .$$

Proof. Let M be the $\mathbf{Z}$-submodule of $\mathrm{End}(A)$ spanned by the above elements. Inspection shows that $\Lambda \subseteq M$. By Lemma 4.5, the corollary follows. □

Remarks. Let k be a proper subfield of K, and let h be a generator of $\mathrm{Gal}(K/k) \subseteq (\mathbf{Z}/p\mathbf{Z})^*$. Then the subring of endomorphisms of A defined over k is

$$\mathrm{End}(A) = \mathrm{Im}\left(\mathbf{Z}\left[\sum_{j=1}^{t-1} \sigma^{ah^j}, \rho \,\middle|\, a \in \mathbf{Z}\right]\right),$$

where t is the order of h. $\mathrm{End}_k(A)$ is commutative if and only if k is $\mathbf{Q}$ or $L = K^{\langle r \rangle}$. In the latter cases, $\mathrm{End}_k(A)$ are contained in $\mathbf{Z} \times \mathbf{Z}[(1 + \sqrt{-3})/2]$ and $\mathcal{O}_K \times \mathcal{O}_{K(\sqrt{-3})}$ respectively.

§ 5. Action of rho on some division points

Let P_1, P_2 and P_3 be any 3 points on F_p where $X = 0$, $Y = 0$ and $Z = 0$ respectively. Recall that φ_A: $F_p \to F_A$ is the canonical projection. Set

$$\infty_2 = \varphi_A(P_1), \quad \infty_3 = \varphi_A(P_2), \quad \text{and} \quad \infty_1 = \varphi_A(P_3) .$$

Then the group of $A[\pi]$ of π-division points on A has order p, and contains all the divisor classes of degree zero supported on the set of cusps $\{\infty_1, \infty_2, \infty_3\}$ of F_A.

For each integer $a \geq 1$,

$$\pi^a \rho = \rho(\zeta^{r^2} - 1)^a = \rho \frac{\zeta^{r^2} - 1}{\zeta - 1} \pi^a$$

in $\operatorname{End}(A)$, so that ρ induces an automorphism of $A[\pi^a]$ by restriction.

LEMMA 5.1. *ρ acts on $A[\pi]$ as multiplication by r.*

Proof. Recall that the equation of F_A is $v^p = u(1-u)^r$. The divisor of the rational function v on F_A is $\infty_2 - (r+1)\infty_1 + r\infty_3$. Hence, on A, $\infty_2 - (r+1)\infty_1 + r\infty_3 = 0 = \infty_1 - (r+1)\infty_3 + r\infty_2$ (the latter equality is obtained by applying ρ to the former). In particular,

$$\rho(\infty_1 - \infty_2) = \infty_2 - \infty_3 = (r+1)(\infty_1 - \infty_3) = r(\infty_1 - \infty_2). \qquad \square$$

LEMMA 5.2. *There is an element $Q \in A[\pi^2] - A[\pi]$ such that $\rho(Q) = Q$.*

Proof. Let us fix a Q in $A[\pi^2] - A[\pi]$. Then $A[\pi^2] = \{(a + b\pi)Q \mid a, b \in \mathbf{F}_p\}$ is a vector space of dimension 2 over $\mathbf{F}_p$. Let $f(x)$ be the minimal polynomial of ρ restricted to $A[\pi^2]$. Since ρ has order 3, we have $f(x) \mid (x-1)(x-r)(x-r^2)$ in $\mathbf{F}_p[x]$. Since ρ can have at most two distinct eigenvalues, and $f(x)$ splits completely, we have $f(x) = x - \lambda_1$ or $f(x) = (x-\lambda_1)(x-\lambda_2)$, where $\lambda_1, \lambda_2 \in \{1, r, r^2\}$ and $\lambda_1 \neq \lambda_2$.

Suppose that $f(x) = x - \lambda_1$. Then $\lambda_1(\pi Q) = \rho(\pi Q) = (\zeta^r - 1)\pi Q = \lambda_1\{(\zeta^r - 1)/\pi\}\pi Q = \lambda_1\{r + (r(r-1)/2)\pi + \cdots\}\pi Q = \lambda_1 r(\pi Q)$, whence $\lambda_1 = \lambda_1 r$ and $\lambda_1 = 0$, a contradiction. Hence, $f(x) = (x-\lambda_1)(x-\lambda_2)$, and there is an $\mathbf{F}_p$-basis Q_1, Q_2 of $A[\pi^2]$ such that the matrix of ρ with respect to $\{Q_1, Q_2\}$ is $\begin{pmatrix}\lambda_1 & 0 \\ 0 & \lambda_2\end{pmatrix}$. Since at least one of Q_1, Q_2 is not in $A[\pi]$, we have found a Q in $A[\pi^2] - A[\pi]$ and a $\lambda \in \{1, r, r^2\}$ such that $\rho(Q) = \lambda Q$. By Lemma 5.1, $r(\pi Q) = \rho(\pi Q) = \lambda r(\pi Q)$, and $\lambda = 1$. This completes the proof of the lemma. $\square$

Remarks. (1) In the same way as above, we can show that there is a $Q \in A[\pi^3] - A[\pi^2]$ such that $\rho(Q) = r^2 Q$. We also remark that the annihilator, in $\operatorname{End}(A)$, of $A[\pi]$ is

$$\mathbf{Z}[\zeta]\pi + \mathbf{Z}[\zeta](\rho - r) + \mathbf{Z}[\zeta](\rho^2 - r^2) + \mathbf{Z}(1 + r\rho - (r+1)\rho^2)\frac{1}{\pi}.$$

(2) If $^-$ denotes complex conjugation, then for $Q \in A[\pi^2] - A[\pi]$, $\bar{Q} = -Q \Leftrightarrow \rho(Q) = Q$.

§ 6. The kernel of an isogeny

Let $X_j = F_A/\langle \sigma^j \rho \sigma^j \rangle$, $(j = 0, 1, 2)$, and we denote the canonical projection $F_A \to X_j$ by φ_j. Let φ be the isogeny

$$\varphi = \prod_{j=0}^{2} (\varphi_j)_* \colon A \longrightarrow \prod_{j=0}^{2} \mathrm{Jac}\,(X_j)\,.$$

LEMMA 6.1. $\mathrm{Ker}\,(\varphi) \subseteq A[\pi^2]$.

Proof. The composition $A \xrightarrow{(\varphi_j)_*} \mathrm{Jac}\,(X_j) \xrightarrow{(\varphi_j)^*} A$ is $\zeta^j(1 + \rho + \rho^2)\zeta^{-j} \in \mathrm{End}\,(A)$, so that $\mathrm{Ker}\,(\varphi_j)_* \subseteq A[\zeta^j(1 + \rho + \rho^2)\zeta^{-j}]$. Let N be $\bigcap_{j=0}^{2} A[\zeta^j(1 + \rho + \rho^2)\zeta^{-j}]$. Then

$$\mathrm{Ker}\,(\varphi) = \mathrm{Ker}\,(\varphi_0)_* \cap \mathrm{Ker}\,(\varphi_1)_* \cap \mathrm{Ker}\,(\varphi_2)_* \subseteq N\,.$$

We claim that $N \subseteq A[\pi^2]$. Let $D \in N$. Then we have

$$(1 + \rho + \rho^2)D = 0\,, \tag{6.1}$$

$$(1 + \zeta^{1-r}\rho + \zeta^{1-r^2}\rho^2)D = 0\,, \tag{6.2}$$

and

$$(1 + \zeta^{2-2r}\rho + \zeta^{2-2r^2}\rho^2)D = 0\,, \tag{6.3}$$

using the relations $\rho\sigma\rho^{-1} = \sigma^r$ and $\rho^{-1}\sigma\rho = \sigma^{r^2}$ in $\mathrm{Aut}\,(F_A)$. From (6.1) and (6.2), we obtain that

$$\{(\zeta^{1-r^2} - 1) + (\zeta^{1-r^2} - \zeta^{1-r})\rho\}D = 0\,. \tag{6.4}$$

From (6.2) and (6.3),

$$\{(\zeta^{1-r^2} - 1) + (\zeta^{2-r-r^2} - \zeta^{2-2r})\rho\}D = 0\,. \tag{6.5}$$

From (6.4) and (6.5),

$$\zeta^r(1 - \zeta^{1-r})(1 - \zeta^{2r+1})\rho D = \{(\zeta^{1-r^2} - \zeta^{1-r}) - (\zeta^{2-r-r^2} - \zeta^{2-2r})\}\rho D = 0\,.$$

Hence, $\pi^2(\rho D) = 0$ and $\rho((\zeta^{r^2} - 1)/(\zeta - 1))^2\pi^2 D = 0$. Since ρ and $(\zeta^{r^2} - 1)/(\zeta - 1)$ are in $\mathrm{Aut}\,(A)$, we have $\pi^2(D) = 0$. □

THEOREM 6.2. *Let* $N = \bigcap_{j=0}^{2} A[\zeta^j(1 + \rho + \rho^2)\zeta^{-j}]$. *Then we have* $\mathrm{Ker}\,(\varphi) = N = A[\pi]$.

https://doi.org/10.1017/S0027763000003901 Published online by Cambridge University Press

Proof. Under the canonical projection $\varphi_0\colon F_A \to X_0 = F_A/\langle\rho\rangle$, ∞_1 and ∞_2 are mapped onto the same point. Thus, $\operatorname{Ker}(\varphi_0)_*$ contains $A[\pi]$. Likewise, $A[\pi]$ is contained in $\operatorname{Ker}(\varphi_j)_*$. Thus

$$A[\pi] \subseteq \operatorname{Ker}(\varphi) \subseteq N \subseteq A[\pi^2]\,.$$

Let $D \in N$. Applying the endomorphism $w = (1 + r\rho + r^2\rho^2)1/\pi^2$ to $\pi^2 D = 0$, we get

$$(1 + r\rho + r^2\rho^2)D = 0\,.$$

Since $(1 + \rho + \rho^2)D = 0$ also, we obtain $\{(r-1)\rho + (r^2 - 1)\rho^2\}D = 0$ or $(r-1)\rho\{1 + (r+1)\rho\}D = 0$. Since D is a p-division point, $(p, r-1) = 1$ and $\rho \in \operatorname{Aut}(A)$, it follows that $\{1 + (r+1)\rho\}D = 0$ or $(r - \rho)D = r\{1 + (r+1)\rho\}D = 0$. Hence,

$$A[\pi] \subseteq \operatorname{Ker}(\varphi) \subseteq N \subseteq A[\pi^2] \cap A[\rho - r]\,.$$

By Lemmas 5.1 and 5.2, there is a $Q \in A[\pi^2] - A[\pi]$ such that $\rho(Q) = Q$ and $\rho(\pi Q) = r(\pi Q)$. Let $D = (a + b\pi)Q \in A[\rho - r]$, with $a, b \in \mathbf{F}_p$. Then $(a + b\pi)Q = (ar + br\pi)Q$, whence $a = ar$ and $a = 0$. Thus $D \in A[\pi]$ and $A[\pi^2] \cap A[\rho - r] = A[\pi]$. Hence, $\operatorname{Ker}(\varphi) = N = A[\pi]$. □

COROLLARY 6.3. *The isogeny* $\varphi\colon A \to \prod_{j=0}^{2} \operatorname{Jac}(X_j)$ *factors as*

$$\begin{array}{ccc} A & \longrightarrow & \prod_{j=0}^{2} \operatorname{Jac}(X_j) \\ {\scriptstyle \pi}\downarrow & \nearrow {\scriptstyle f} & \\ A & & \end{array},$$

where $f\colon A \to \prod_{j=0}^{2} \operatorname{Jax}(X_j)$ *is an isomorphism of abelian varieties defined over* K.

Proof. We define an isomorphism $f\colon A \to \prod_{j=0}^{2} \operatorname{Jac}(X_j)$ of abelian varieties as follows. Given $D \in \operatorname{Pic}^0(F_A)$, let E be such that $\pi E = D$. E exists since π is an isogeny. Then we define $f(D) = \varphi(E)$. f is well-defined and injective by definition. In particular, f is a birational isomorphism of abelian varieties and hence an isomorphism of abelian varieties. □

Let C be the Klein quartic curve over $\mathbf{C}$ with projective equation

$$X^3Y + Y^3Z + Z^3X = 0\,.$$

C has genus 3, $\operatorname{Aut}(C) \approx PSL(2, \mathbf{F}_7)$, and the morphism

https://doi.org/10.1017/S0027763000003901 Published online by Cambridge University Press

$$F^{7}_{1,2,4} \longrightarrow C, \quad (x, y) \longrightarrow ((x-1)/y^2, \quad -(x-1)/y^3)$$

is a birational isomorphism. Let Jac(C) be the Jacobian of C. We will denote by σ and ρ the following automorphisms of C:

$$\sigma\colon (x, y) \longrightarrow (\zeta^4 x, \zeta^5 y), \quad \rho\colon (x, y) \longrightarrow (1/y, x/y),$$

where ζ is a primitive 7-th root of unity. Then by Proposition 2.1, we have the epimorphism

$$\mathbf{Q}[\sigma, \rho] \longrightarrow \mathrm{End}^0(\mathrm{Jac}(C)).$$

By Theorem 4.1 and Corollary 6.3, we have

COROLLARY 6.4. *Let* $W = 7^{-1}(1 + r\rho + r^2\rho^2)(\sigma - 1)^4 \in \mathbf{Q}[\sigma, \rho]$, *with* $r = 2$. *Then* $\mathrm{End}(\mathrm{Jac}(C)) = \mathrm{Im}(\mathbf{Z}[\sigma, \rho, W])$ *and* Jac(C) *is isomorphic to a cube of an elliptic curve* E.

Remarks. (1) From the Weierstrass equation for E computed in [10], we see that E is $J_0(49)$.

(2) As an application of Theorem 4.1, we give a second proof of the following result due to Prapavessi [10]: Let $\infty_1 = (1, 0, 0)$, $\mu_j = \zeta^j + \zeta^{-j}$ $(j \geq 0)$ and let $P = (\mu_1, \mu_3^{-1}, 1)$. Then $D = P + \rho P - 2\infty_1$ generates the kernel of π^3 over $\mathbf{Z}[\zeta]$. Prapavessi showed ([10], Lemma 2.1) that $\pi^3(D) = 0$. It remains to show that $\pi^2(D) \neq 0$. Let $\infty_2 = (0, 1, 0)$ and $\infty_3 = (0, 0, 1)$. Suppose, on the contrary, that $\pi^2(D) = 0$. Applying the endomorphism $(1 - r^2\rho)1/\pi$ of Jac(C) we obtain $(1 - r^2\rho)\pi D = 0$, or

$$\pi D = r^2\left\{\frac{\zeta^r - 1}{\pi}\right\}\pi\rho D = r^2\left\{r + \frac{r(r-1)}{2}\pi + \cdots\right\}\pi\rho D = \pi\rho D.$$

Since the group of π-division points on Jac(C) is generated by $\infty_i - \infty_j$ $(i \neq j)$, $\pi(P - \rho^2 P) = 0$ follows from $\pi(D - \rho D) = 0$. Hence there is a non-constant rational function g on C whose divisor is $\pi(P - \rho^2 P)$. In particular, $g\colon C \to \mathbf{P}^1$ is a double covering, and C is a hyperelliptic curve, which is a contradiction. This completes the proof that $\pi^2(D) \neq 0$.

(3) Our knowledge of the endomorphism ring of A allows us to deduce a result of Greenberg [5] for $A = J^p_{1,r,-(1+r)}$. We have noted that $w = (1 + r\rho + r^2\rho^2)1/\pi^2$ is an endomorphism of A which is defined over K. Thus if $D \in A(K)$, then it follows that $w(D) \in A(K)$. Let $Q \in A[\pi^3] - A[\pi^2]$ be such that $\rho(Q) = r^2 Q$. Setting $P = \pi^2 Q$, we have $w(P) = (1 + r\rho + r^2\rho^2)(Q) = 3Q$ is an element of $A(K)$. Let $\lambda, \mu \in \mathbf{Z}$ be such that $3\mu + p\lambda$

$= 1$. Then $Q = 3\mu Q \in A(K)$. Since $A[\pi^3]$ is a cyclic $\mathbf{Z}[\zeta]$-module with Q as a generator, it follows that $A[\pi^3] \subseteq A(K)$. We also remark that the p-part of $A(K)$ is of the form $A[\pi^{3l}]$ for some $l \geq 1$.

Acknowledgements

The author would like to thank Professor R. Coleman for his encouragement and support during the course of this work.

Reference

[1] N. Aoki, Simple Factors of the Jacobian of a Fermat Curve and the Picard number of a Product of Fermat Curves, to appear in Amer. J. Math.

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

[3] R. Coleman, Lecture notes on Cyclotomy, Tokyo University (1985).

[4] R. Coleman and W. McCallum, Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. Reine Angew. Math., **385** (1988), 41–101.

[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] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. Math., **123** (1986), 43–106.

[8] N. Koblitz and D. Rohrlich, Simple Factors in the Jacobian of a Fermat curve, Canadian J. Math., **20** (1978), 1183–1205.

[9] C. H. Lim, Endomorphisms of Jacobian varieties of Fermat curves, to appear in Compositio Math.

[10] D. T. Prapavessi, On Jacobi sum Hecke Characters of Conductor a Power of 2. Ph.D. thesis, University of California, Berkeley (1988).

[11] D. Rohrlich, Appendix to "On the Periods of Abelian Integrals and a Formula of Chowla and Selberg" by B. Gross, Invent. Math., **45** (1978), 193–211.

[12] C. G. Schmidt, Der Definitions-Köper fur den Zerfall einer Abelschen Varietat mit Komplexer Multiplikation, Math. Ann., **254** (1980), 201–210.

[13] G. Shimura and Y. Taniyama, Complex multiplication of Abelian Varieties and its Applications to Number Theory, Tokyo, Math. Soc. Japan (1961).

Department of Mathematics
University of California
Berkeley
CA 94720, U.S.A.

Current address:
Department of Mathematics
Faculty of Science
National University of Singapore
Kent Ridge
Singapore 0511