COMPOSITIO MATHEMATICA

CHONG-HAI LIM

Endomorphisms of jacobian varieties of Fermat curves

Compositio Mathematica, tome 80, n° 1 (1991), p. 85-110

<http://www.numdam.org/item?id=CM_1991__80_1_85_0>

Compositio Mathematica **80**: 85–110, 1991.

Endomorphisms of Jacobian varieties of Fermat curves

CHONG-HAI LIM

*Department of Mathematics, University of California, Berkeley, CA 94720; *Department of Mathematics, National University of Singapore, 10 Kent Ridge Crescent, Singapore 0511*

Received 10 May 1990; accepted 18 December 1990

Introduction

Let m be a fixed positive integer, and let F_m denote the complete plane curve over the complex number field $\mathbf{C}$ with projective equation

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

This is called the Fermat curve of exponent m over $\mathbf{C}$. Let J_m denote the Jacobian of F_m.

The object of this paper is to give a characterization of the endomorphism ring $\mathrm{End}(J_m)$ of J_m when m is relatively prime to 6. To do this, we first determine $\mathrm{End}^0(J_m) = \mathrm{End}(J_m) \otimes \mathbf{Q}$, and the action of $\mathrm{Aut}(F_m)$ on $H_1(F_m) = H_1(F_m(\mathbf{C}), \mathbf{Z})$. Rohrlich has shown in the appendix of [9] that the latter homology group is a cyclic module over a suitable (commutative) integral group ring. $\mathrm{End}^0(J_m)$ turns out to be a quotient ring of $\mathbf{Q}[\mathrm{Aut}(F_m)]$. To prove this, we use the results of Koblitz–Rohrlich in [11]. We then use the fact that for a non-singular projective curve X over $\mathbf{C}$ with Jacobian J_X,

$$\mathrm{End}(J_X) = \{\alpha \in \mathrm{End}^0(J_X) \mid \alpha(H_1(X(\mathbf{C}), \mathbf{Z})) \subseteq H_1(X(\mathbf{C}), \mathbf{Z})\},$$

to write down necessary and sufficient conditions for an element of $\mathrm{End}^0(J_m)$ to be in $\mathrm{End}(J_m)$. In particular, we find examples of endomorphisms of J_m which are not induced from elements of the integral group ring $\mathbf{Z}[\mathrm{Aut}(F_m)]$.

Fixing a primitive m-root ζ of unity in $\bar{\mathbf{Q}}$, $G = \mathrm{Aut}(F_m)$ is generated by:

$$\sigma: (X, Y, Z) \to (\zeta X, Y, Z), \qquad \tau: (X, Y, Z) \to (X, \zeta Y, Z),$$

$$\iota: (X, Y, Z) \to (Y, X, Z), \qquad \rho: (X, Y, Z) \to (Z, X, Y).$$

The natural homomorphism $G \to \mathrm{Aut}(J_m)$ gives rise to

$$\Phi: \mathbf{Q}[G] \to \mathrm{End}^0(J_m).$$

---

*Present address of author.

For each integer $k \geqslant 0$, we let

$$I_k(T) = \sum_{j=0}^{m-1} \binom{j}{k} T^j \in \mathbf{Z}[T].$$

Let $\mathbf{T}$ be the left-sided ideal of the group ring $\mathbf{Q}[G]$ generated by the following elements: $I_0(\sigma)$, $I_0(\tau)$, $I_0(\sigma\tau)$, $I_0(\sigma^{-1}\tau)(1+\iota)$, $I_0(\sigma\tau^2)(1+\iota\rho)$, $I_0(\sigma^2\tau)(1+\iota\rho^{-1})$.

We will prove, in Sections 1 and 2,

THEOREM A. *The sequence*

$$0 \to \mathbf{T} \to \mathbf{Q}[G] \xrightarrow{\Phi} \mathrm{End}^0(J_m) \to 0$$

is exact. Moreover, $\mathrm{Ker}(\Phi) = \mathbf{T}$ *is the two-sided ideal of* $\mathbf{Q}[G]$ *generated by* $I_0(\sigma)$ *and* $I_0(\sigma^{-1}\tau)(1+\iota)$.

In Section 3, we study the singular homology group $H_1(F_m)$ and the action of G on it. Let $I\colon [0,1] \to F_m(\mathbf{C})$ denote the one-simplex

$$I\colon t \to (t^{1/m}, (1-t)^{1/m}, \alpha),$$

where the mth root is the real mth root, and $\alpha = -1$ if m is odd but α is a primitive $2m$th root of unity if m is even. Let g denote the one-cycle

$$g = (\sigma^{(m+1)/2} - \sigma^{(m-1)/2})(\tau^{(m+1)/2} - \tau^{(m-1)/2})I \quad \text{if } m \text{ is odd}$$

and

$$g = (1 - \sigma^{m-1})(1 - \tau^{m-1}) \quad \text{if } m \text{ is even.}$$

Denoting the subgroup of G generated by σ and τ by G_m, we have

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

Using Theorem A and Proposition B, we prove that:

THEOREM C. *Let* $X, Y, Z, \tilde{X}, \tilde{Y}, \tilde{Z} \in \mathbf{Q}[G_m]$. *Denoting the ideal of* $\mathbf{Q}[G_m]$ *generated by* $I_0(\sigma)$, $I_0(\tau)$ *and* $I_0(\sigma\tau)$ *by* $\mathbf{J}$, *then*

$$\Phi(X + Y\rho + Z\rho^2 + \tilde{X}\iota + \tilde{Y}\rho\iota + \tilde{Z}\rho^2\iota) \in \mathrm{End}(J_m)$$

if and only if, for all r *and* s *in* $\mathbf{Z}/m\mathbf{Z}$,

$$X\sigma^r\tau^s - \tilde{X}\sigma^s\tau^r + Y\sigma^{-s}\tau^{r-s} - \tilde{Y}\sigma^{-r}\tau^{s-r} + Z\sigma^{s-r}\tau^{-s} - \tilde{Z}\sigma^{r-s}\tau^{-r} \in \mathbf{Z}[G_m] + \mathbf{J}.$$

The next theorem shows that there are endomorphisms of J_m which are not in $\Phi(\mathbf{Z}[G])$ when m is relatively prime to 6. Let

$$W = m^{-1}\{-I_1(\sigma)I_3(\tau) + [I_1(\sigma)I_3(\tau) - I_3(\sigma)I_1(\tau)]\rho + I_3(\sigma)I_1(\tau)\rho^2\} \in \mathbf{Q}[G_m, \rho].$$

THEOREM D

$$\mathrm{End}(J_m) \cap \Phi(\mathbf{Q}[G_m, \rho]) = \Phi(\mathbf{Z}[G_m, \rho, W]) \quad \textit{and} \quad \Phi(W)$$

is not in $\Phi(\mathbf{Z}[G])$. *However,*

$$\mathrm{End}(J_m) \cap \Phi(\mathbf{Q}[G_m, \iota]) = \Phi(\mathbf{Z}[G_m, \iota]).$$

In particular, since the restriction of Φ to $\mathbf{Q}[G_m, \rho]$ is surjective when $m = 5$, we have the following theorem.

THEOREM E. *When* $m = 5$, *we have*

$$\mathrm{End}(J_5) = \Phi(\mathbf{Z}[G_m, \rho, W]).$$

1. The kernel of Φ

With the exception of Lemma 1.1, let m be relatively prime to 6. We also assume $m > 3$. In this section, we prove that the kernel of Φ is the left-sided ideal $\mathbf{T}$ of $\mathbf{Q}[G]$ defined in the Introduction. Let $A = I_0(\sigma)$, $B = I_0(\tau)$, $C = I_0(\sigma\tau)$, $D = I_0(\sigma^{-1}\tau)$, $E = I_0(\sigma\tau^2)(1+\iota\rho)$ and $F = I_0(\sigma\tau^2)(1+\iota\rho^2)$ be in $\mathbf{Q}[G]$.

LEMMA 1.1. $\mathbf{T} \subseteq \mathrm{Ker}(\Phi)$.

Proof. Since the following relations hold in $\mathbf{Q}[G]$: $\rho A\rho^{-1} = B$, $\rho B\rho^{-1} = C$, $\rho D\rho^{-1} = E$, $\rho E\rho^{-1} = F$, and $\mathrm{Ker}(\Phi)$ is a two-sided ideal in $\mathbf{Q}[G]$, it suffices to show that A and B are in $\mathrm{Ker}(\Phi)$.

Let X be the plane curve $u + v^m + 1 = 0$ and $h: F_m \to X$ be the morphism $h(x, y) = (-x^m, y)$. The induced homomorphism $h^*: J_X \to J_m$ on Jacobians is the zero map since X has genus zero. Since h is a cyclic covering with $\langle\sigma\rangle$ as Galois group, we have

$$\Phi(A)((P) - (Q)) = h^*((h(P)) - (h(Q))) = 0 \quad \text{for points } P, Q \in F_m.$$

Hence $\Phi(A) = 0$.

Next, we consider the curve $Y = F^m_{1,1,-2}$, with singular equation $y^m = x(1-x)$. It is hyperelliptic with $\iota: (x, y) \to (1-x, y)$ as its hyperelliptic involution. Let $\phi: F_m \to Y$ be the canonical projection $\varphi^m_{1,1,-2}$. Composing the homomorphisms

$$J_m \xrightarrow{\phi_*} J_Y \xrightarrow{(1+\iota)_*} J_Y \xrightarrow{\phi^*} J_m,$$

we obtain the endomorphism $\Phi(D)$ of J_m. Since $\iota_* = -1$ in $\mathrm{End}(J_Y)$, we have that $\Phi(D) = 0$. □

F_m is the Fermat curve $X^m+Y^m+Z^m=0$ defined over $\mathbf{Q}$. Let $x=X/Z$ and $y=Y/Z$. A basis for the complex vector space $H^0(F_m, \Omega^1)$ is the set

$$\left\{w_{r,s}=x^{r-1}y^{s-1}\frac{dx}{y^{m-1}}\middle| 0<r, s, r+s<m\right\}.$$

LEMMA 1.2. *Let $\alpha\in\mathbf{Z}[G_m]$ be such that $\Phi(\alpha)^*w_{r,s}=0$ for all $w_{r,s}\in H^0(F_m, \Omega^1)$. Then $\alpha\in\mathbf{J}$, where $\mathbf{J}$ is the ideal of the group ring $\mathbf{Q}[G_m]$ generated by A, B and C.*

Proof. Let $\alpha=f(\sigma, \tau)$, where $f(x, y)\in\mathbf{Z}[x, y]$. Since $(\sigma^k\tau^l)^*w_{r,s}=\zeta^{rk+sl}w_{r,s}$, $\Phi(\alpha)^*w_{r,s}=0$ for all $w_{r,s}$ implies that for $0<r, s, r+s<m$,

$$f(\zeta^r, \zeta^s)=0. \tag{1.1}$$

Let (a, b) be a pair of positive integers with $a, b<m$ and $a+b\neq m$. Let $c\in\mathbf{Z}$ be such that $0<c<m$ and $a+b+c=km$, where $k=1$ or $k=2$. If $k=1$, (1.1) holds for $(r, s)=(a, b)$. Suppose $k=2$. Then $(m-a)+(m-b)+(m-c)=m$, whence $(m-a)+(m-b)<m$. Therefore $f(\zeta^{-a}, \zeta^{-b})=0$. Applying the automorphism in $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ which sends ζ to ζ^{-1} to the latter equation, we obtain $f(\zeta^a, \zeta^b)=0$.

Let I be the ideal of $\mathbf{Q}[x, y]$ generated by $I_0(x)$, $I_0(y)$ and $I_0(xy)$. The ring $R=\mathbf{Q}[x, y]/I$ is a product of fields (hence reduced), since it is a quotient of $\mathbf{Q}[x, y]/(x^m-1, y^m-1)$. Let

$$Z(I)=\{(u, v)\in\mathscr{A}^2_{\bar{\mathbf{Q}}}\mid I_0(u)=I_0(v)=I_0(uv)=0\}.$$

Then

$$Z(I)=\{(\zeta^a, \zeta^b)\mid 0<a, b<m, a+b\neq m\}.$$

By Hilbert's Nullstellensatz, $f\in\sqrt{I.\bar{\mathbf{Q}}[x, y]}\cap\mathbf{Q}[x, y]=I$. It follows that $\alpha\in\mathbf{J}$. □

Proceeding in the same way as we did in proving Lemma 1.2, we can prove the following lemma.

LEMMA 1.3. *Let $\alpha\in\mathbf{Z}[G_m]$ be such that $\Phi(\alpha)^*w_{r,s}=0$ for all $w_{r,s}\in H^0(F_m, \Omega^1)$ with $r\neq s$, $2r+s\neq m$ and $r+2s\neq m$. Then*

$$\alpha\in\mathbf{J}+(I_0(\sigma^{-1}\tau), I_0(\sigma\tau^2), I_0(\sigma^2\tau)).$$

We devote the remaining space in this section to determine $\mathrm{Ker}(\Phi)$.

Let $U, V, W, X, Y, Z\in\mathbf{Z}[G_m]$ and

$$\varphi=U+V\rho+W\rho^2+X\iota+Y\iota\rho+Z\iota\rho^2\in\mathbf{Z}[G]$$

be such that for all $w_{r,s}\in H^0(F_m, \Omega^1)$,

$$\Phi(\varphi)^*w_{r,s}=0. \tag{1.2}$$

We choose polynomials $\tilde{U}$, $\tilde{V}$, $\tilde{W}$, $\tilde{X}$, $\tilde{Y}$, $\tilde{Z} \in \mathbf{Z}[x, y]$ such that

$$U = \tilde{U}(\sigma, \tau), \qquad V = \tilde{V}(\sigma, \tau), \qquad W = \tilde{W}(\sigma, \tau),$$
$$X = \tilde{X}(\sigma, \tau), \qquad Y = \tilde{Y}(\sigma, \tau), \qquad Z = \tilde{Z}(\sigma, \tau).$$

From (1.2), it follows that $w_{r,s}$ is annihilated by

$$\Phi(U)^* + \rho^*\Phi(V)^* + (\rho^2)^*\Phi(W)^* + \iota^*\phi(X)^* +$$
$$+ \rho^*\iota^*\Phi(Y)^* + (\rho^2)^*\iota\Phi(Z)^*,$$

or equivalently, for all $(r, s) \in \mathbf{Z}^2$ with $0 < r, s, r + s < m$,

$$\tilde{U}(\zeta^r, \zeta^s)w_{r,s} + \tilde{V}(\zeta^r, \zeta^s)w_{s,m-r-s} + \tilde{W}(\zeta^r, \zeta^s)w_{m-r-s,r} -$$
$$- \tilde{X}(\zeta^r, \zeta^s)w_{s,r} - \tilde{Y}(\zeta^r, \zeta^s)w_{r,m-r-s} - \tilde{Z}(\zeta^r, \zeta^s)w_{m-r-s,s} = 0. \tag{1.3}$$

When $r \neq s$, $r + 2s \neq m$ and $2r + s \neq m$, the set

$$\{w_{r,s}, w_{s,m-r-s}, w_{m-r-s,s}, w_{s,r}, w_{r,m-r-s}, w_{m-r-s,s}\}$$

is a linearly independent subset of $H^0(F_m, \Omega^1)$. Hence, from (1.3), $\tilde{U}$, $\tilde{V}$, $\tilde{W}$, $\tilde{X}$, $\tilde{Y}$ and $\tilde{Z}$ vanish at (ζ^r, ζ^s) whenever $0 < r, s, r + s < m$, $r \neq s$, $r + 2s \neq m$ and $2r + s \neq m$. In other words, for these pairs (r, s),

$$\Phi(U)^*w_{r,s} = \Phi(V)^*w_{r,s} = \Phi(W)^*w_{r,s} = \Phi(X)^*w_{r,s}$$
$$= \Phi(Y)^*w_{r,s} = \Phi(Z)^*w_{r,s} = 0. \tag{1.4}$$

When $r = s$, (1.3) implies that

$$(\tilde{U} - \tilde{X})(\zeta^r, \zeta^r)w_{r,r} + (\tilde{V} - \tilde{Y})(\zeta^r, \zeta^r)w_{r,m-2r} + (\tilde{W} - \tilde{Z})(\zeta^r, \zeta^r)w_{m-2r,r} = 0.$$

Since $\{w_{r,r}, w_{r,m-2r}, w_{m-2r,r}\}$ is a linearly independent subset of $H^0(F_m, \Omega^1)$ (by virtue of the fact that m is coprime to 3), we have for $0 < r \leqslant (m-1)/2$,

$$\Phi(U - X)^*w_{r,r} = \Phi(V - Y)^*w_{r,r} = \Phi(W - Z)^*w_{r,r} = 0. \tag{1.5}$$

By considering (1.3) in the cases when $r + 2s = m$ and $2r + s = m$, we obtain

$$\Phi(U - Y)^*w_{m-2r,r} = \Phi(V - Z)^*w_{m-2r,r} = \Phi(W - X)^*w_{m-2r,r} = 0 \tag{1.6}$$

for $o < r < m$, and

$$\Phi(U - Z)^*w_{r,m-2r} = \Phi(V - X)^*w_{r,m-2r} = \Phi(W - Y)^*w_{r,m-2r} = 0 \tag{1.7}$$

for $0 < r < m$, respectively.

Let $\tilde{\mathbf{J}}$ be the ideal of $\mathbf{Q}[G_m]$ generated by $I_0(\sigma)$, $I_0(\tau)$, $I_0(\sigma\tau)$, $I_0(\sigma^{-1}\tau))$, $I_0(\sigma\tau^2)$ and $I_0(\sigma^2\tau)$. We fix a basis $\{\alpha_1, \ldots, \alpha_{l_0}\}$ over $\mathbf{Q}$ for the ideal $\mathbf{J}$ generated by $I_0(\sigma)$, $I_0(\tau)$ and $I_0(\sigma\tau)$. Then we choose a basis

$$\{\beta_1 I_0(\sigma^{-1}\tau), \ldots, \beta_{l_1} I_0(\sigma^{-1}\tau)\} \cup \{\gamma_1 I_0(\sigma\tau^2), \ldots, \gamma_{l_2} I_0(\sigma\tau^2)\} \cup$$
$$\cup \{\delta_1 I_0(\sigma^2\tau), \ldots, \delta_{l_3} I_0(\sigma^2\tau)\}$$

for $\tilde{\mathbf{J}}/\mathbf{J}$, where each $\beta_i, \gamma_j, \delta_k \in G_m$. We note that

$$\{\alpha_1, \ldots, \alpha_{l_0}\} \cup \{\beta_1 I_0(\sigma^{-1}\tau), \ldots, \beta_{l_1} I_0(\sigma^{-1}\tau)\} \cup \{\gamma_1 I_0(\sigma\tau^2), \ldots, \gamma_{l_2} I_0(\sigma\tau^2)\} \cup \{\delta_1 I_0(\sigma^2\tau), \ldots, \delta_{l_3} I_0(\sigma^2\tau)\} \tag{1.8}$$

is a $\mathbf{Q}$-basis for $\tilde{\mathbf{J}}$.

Lemma 1.3 applied to (1.4) gives $U, V, W, X, Y, Z \in \tilde{\mathbf{J}}$. Using the basis in (1.8), we can write in a unique way:

$$U = \sum_{j=1}^{l_0} \lambda_{j,\alpha}\alpha_j + \sum_{j+1}^{l_1} \lambda_{j,\beta}\beta_j I_0(\sigma^{-1}\tau) + + \sum_{j=1}^{l_2} \lambda_{j,\gamma}\gamma_j I_0(\sigma\tau^2) + \sum_{j=1}^{l_3} \lambda_{j,\delta}\delta_j I_0(\sigma^2\tau),$$

where the $\lambda_{j,\alpha}$'s, $\lambda_{j,\beta}$'s, $\lambda_{j,\gamma}$'s and $\lambda_{j,\delta}$'s are in $\mathbf{Q}$. We will write

$$U_0 = \sum_{j=1}^{l_0} \lambda_{j,\alpha}\alpha_j, \quad U_1 = \sum_{j=1}^{l_1} \lambda_{j,\beta}\beta_j, \quad U_2 = \sum_{j=1}^{l_2} \lambda_{j,\lambda}\gamma_j, \quad U_3 = \sum_{j=1}^{l_3} \lambda_{j,\delta}\delta_j.$$

Thus

$$U = U_0 + U_1 I_0(\sigma^{-1}\tau) + U_2 I_0(\sigma\tau^2) + U_3 I_0(\sigma^2\tau). \tag{1.9}$$

We write similar expressions for V, W, X, Y and Z as we did for U in (1.9).

Consider

$$U - X = (U_0 - X_0) + (U_1 - X_1)I_0(\sigma^{-1}\tau) + (U_2 - X_2)I_0(\sigma\tau^2) + + (U_3 - X - 3)I_0(\sigma^2\tau).$$

By (1.5), $U - X$ annihilates $w_{r,r}$. Since each of $I_0(\sigma\tau^2)$ and $I_0(\sigma^2\tau)$ annihilates $w_{r,r}$, so does $(U_1 - X_1)I_0(\sigma^{-1}\tau)$. In addition, $I_0(\sigma^{-1}\tau)$ annihilates all $w_{r,r}$ with $r \neq s$. Thus $(U_1 - X_1)I_0(\sigma^{-1}\tau)$ annihilates all $w_{r,s} \in H^0(F_m, \Omega^1)$. By Lemma 1.2, $U_1 - X_1)I_0(\sigma^{-1}\tau) \in \mathbf{J}$. By definition of U_1 and X_1, we have $U_1 = X_1$.

We can similarly prove the following equalities: $U_2 = Y_2$, $U_3 = Z_3$, $V_1 = Y_1$, $V_2 = Z_2$, $V_3 = X_3$, $W_1 = Z_1$, $W_2 = X_2$, $W_3 = Y_3$. Therefore, φ is equal to

$$U_0 + V_0\rho + W_0\rho^2 + X_0\iota + Y_0\iota\rho + Z_0\iota\rho^2 + + U_1 I_0(\sigma^{-1}\tau)(1+\iota) + U_2 I_0(\sigma\tau^2)(1+\iota\rho) + U_3 I_0(\sigma^2\tau)(1+\iota\rho^{-1}) + + V_1 I_0(\sigma^{-1}\tau)(1+\iota)\rho + V_2 I_0(\sigma\tau^2)(1+\iota\rho)\rho + V_3 I_0(\sigma^2\tau)(1+\iota\rho^{-1})\rho + + W_1 I_0(\sigma^{-1}\tau)(1+\iota)\rho^2 + W_2 I_0(\sigma\tau^2)(1+\iota\rho)\rho^2 + W_3 I_0(\sigma^2\tau)(1+\iota\rho^{-1})\rho^2.$$

Together with Lemma 1.1 and the following relations in the group G: $\rho\sigma\rho^{-1} = \tau$, $\rho\tau\rho^{-1} = (\sigma\tau)^{-1} = \rho^{-1}\sigma\rho$, $\iota\rho\iota^{-1} = \rho^{-1}$, we have proved that $\mathbf{T} = \mathrm{Ker}(\Phi)$.

2. Isogeny classes

As before, F_m is the Fermat curve $X^m+Y^m+Z^m=0$ defined over $\mathbf{Q}$, and $x=X/Z$ and $y=Y/Z$.

Let $r, s, t \in \mathbf{Z}$ with $0<r, s, t<m$ and $r+s+t \equiv 0 \pmod m$. Then

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

is a differential form of the second kind on F_m. 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 deRham cohomology $H^1_{\mathrm{DR}}(F_m)$. In the Hodge splitting

$$H^1_{\mathrm{DR}}(F_m) \xrightarrow{\sim} H^0(F_m, \Omega^1) \oplus H^1(F_m, \mathcal{O}),$$

$H^0(F_m, \Omega^1)$ has $\Omega_1 = \{w_{r,s,t} \in \Omega \mid r+s+t=m\}$ as a basis.

We say that an abelian variety A/K has CM by a commutative ring R if there is given a homomorphism $R \to \mathrm{End}_K(A)$ such that $H^1_{\mathrm{DR}}(A)$ becomes a cyclic $R \otimes K$-module. Let $K = \mathbf{Q}(\zeta)$. Then J_m/K has CM by $\mathbf{Z}[G_m]$, with the map

$$\mathbf{Z}[G_m] \to \mathrm{End}_K(J_m)$$

induced by the inclusion $G_m \to \mathrm{Aut}_K(F_m)$.

Let $S \in S_m$ be the class of (a, b, c), where $a, b, c \in \mathbf{Z}$, $0<a, b, c<m$ and $a+b+c=m$. We first consider the case when $(m, a, b, c) = 1$. Then $F^m_{a,b,c} = F_m/\langle\sigma^b\tau^{-a}\rangle$ has irreducible equation

$$y^m = x^a(1-x)^b,$$

and

$$\Omega_S = \Omega^{\langle\sigma^b\tau^{-a}\rangle}$$

descends to a basis of eigenforms for $H^1_{\mathrm{DR}}(J^m_S)$ under the action of $\mathbf{Z}[G_m/\langle\sigma^b\tau^{-a}\rangle]$. Hence the Jacobian $J^m_S = J^m_{a,b,c}$ of $F^m_{a,b,c}$ has CM by $\mathbf{Z}[G_m/\langle\sigma^b\tau^{-a}\rangle]$.

Let $f_m(x)$ denote the mth cyclotomic polynomial over $\mathbf{Q}$, and let α be any generator of the cyclic group $G_m/\langle\sigma^b\tau^{-a}\rangle$. We define $A^m_S = (J^m_{a,b,c})^{\mathrm{new}}$ to be the abelian variety obtained as a quotient of J^m_S by the abelian subvariety $f_m(\alpha)J^m_S$.

In general, if $d=(m, a, b, c)=m/m'$, we let $a'=a/d$, $b'=b/d$, $c'=c/d$, and define

$$A^m_S = (J^m_{a',b',c'})^{\mathrm{new}}.$$

Then it is well-known that the composition

$$J_m \to \prod_{S \in S_m} J_S^m \to \prod_{S \in S_m} A_S^m$$

is an isogeny over $\mathbf{Q}$: $J_m \to \Pi_{S \in S_m} A_S^m$.

For $S_1, S_2 \in S_m$, we say that S_1 and S_2 are equivalent (written $S_1 \sim S_2$) if $A_{S_1}^m$ and $A_{S_2}^m$ are isogeneous. If $[S]$ denotes the equivalence class of $S \in S_m$, we set

$$A_{[S]}^m = \prod_{S' \in [S]} A_S^m.$$

$A_{[S]}^m$ is well-defined up to the order of the factors. Let $\lambda_{[S]}^m$ be the homomorphism

$$\mathbf{Q}[G] \to \mathrm{End}^0(A_{[S]}^m).$$

Then $\lambda_{[S]}^m$ factors through the image of

$$\mathbf{Q}[G] \to \mathrm{End}^0(J_{[S]}^m), \quad \text{where } J_{[S]}^m = \prod_{S' \in [S]} J_{S'}^m.$$

Let us fix some terminology. (1) If R is a ring, then $\Delta_n(R)$ is the subspace of the ring of $(n \times n)$-matrices $M_n(R)$ with entries in R consisting of the diagonal matrices. (2) If $r_1, \ldots, r_n \in R$, let $\Delta(r_1, \ldots, r_n)$ be the diagonal matrix $(r_{i,j}) \in \Delta_n(R)$ for which $r_{i,i} = r_i$ for all i. (3) Let I_n be the multiplicative unit of $M_n(R)$. (4) If A is a simple abelian variety, then we associate to an endomorphism ϕ of A^n the matrix $U_\phi \in M_n(\mathrm{End}(A))$ if on closed points,

$$\phi: \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} \to U_\phi \cdot \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix}.$$

(5) Let A and B be abelian varieties over a field F, and let $\varphi: A \to B$ be an isogeny of degree n. Then there is a unique isogeny $\tilde{\varphi}: B \to A$ such that $\tilde{\varphi}\varphi = n_A$ is multiplication by n on A. φ induces the canonical isomorphism $F_\varphi: \mathrm{End}^0(A) \to \mathrm{End}^0(B)$, which sends $\alpha \in \mathrm{End}(A)$ to $n^{-1}(\varphi\alpha\tilde{\varphi})$.

Case 1. A_S^m is non-simple.

In this case [11], S is the class of a permutation of $(1, w, -(1+w))$, where $w \in \mathbf{Z}/m\mathbf{Z}$ satisfies (a) $w^2 + w + 1 = 0$, or (b) $w^2 = 1$ and $w \neq \pm 1$.

In subcase (a), $A_{[S]}^m = A_{1,w,w^2}^m \times A_{1,w^2,w}^m$. Let $L = K^{\langle w \rangle}$. Then A_{1,w,w^2}^m is isogeneous to a cube of a simple abelian variety B with CM by the ring of integers $\mathcal{O}_L$, and the homomorphism

$$\Phi_1: \mathbf{Q}[\sigma, \rho] \to \mathrm{End}^0(A_{1,w,w^2}^m)$$

is surjective [13]. Since $\iota(\sigma^w \tau^{-1})\iota^{-1} = (\sigma^{w^2}\tau^{-1})^w$ in $\mathrm{Aut}(F_m)$, ι induces an isomorphism $F_{1,w^2,w}^m \to F_{1,w,w^2}^m$. Consider the isogeny f, which is the composition

$$A_{1,w,w^2}^m \times A_{1,w^2,w}^m \xrightarrow{1 \times \iota} (A_{1,w,w^2}^m)^2 \to B^6.$$

We claim that $F_f\lambda^m_{[S]}\colon \mathbf{Q}[G] \to M_6(L)$ is surjective. This is the case because $F_f\lambda^m_{[S]}$ sends ι, $I_0(\sigma\tau^{-w^2})$, $I_0(\sigma\tau^{-w})$ to

$$\begin{pmatrix} 0 & U_1 \\ U_2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & mI_3 \end{pmatrix}, \quad \begin{pmatrix} mI_3 & 0 \\ 0 & 0 \end{pmatrix}$$

respectively (where U_1 and U_2 are units in $M_3(\mathcal{O}_L)$), and Φ_1 is surjective.

In subcase (b), $A^m_{[S]} = A^m_{1,w,-(1+w)} \times A^m_{1,-(1+w),w} \times A^m_{-(1+w),1,w}$. Since

$$\Phi_2\colon \mathbf{Q}[\sigma, \iota] \to \mathrm{End}^0(A^m_{1,w,-(1+w)})$$

is surjective [13], and $\rho \in \mathrm{Aut}(F_m)$ induces the isomorphisms

$$F^m_{1,w,-(1+w)} \xrightarrow{\rho} F^m_{-(1+w),1,w} \xrightarrow{\rho} F^m_{1,-(1+w),w} \xrightarrow{\rho} F^m_{1,w,-(1+w)},$$

a proof similar to the one given above for subcase (a) shows that $\lambda^m_{[S]}$ is surjective.

We have shown that

LEMMA 2.1. *If $(m, S) = 1$ and A^m_S is non-simple, then $\lambda^m_{[S]}$ is surjective.*

Case 2. *A^m_S is simple and F^m_S is hyperelliptic.*

Here, we use the results of Coleman [2]: S is the class of a permutation of $(1, 1, -2)$. Since the 3 distinct permutations of $(1, 1, -2)$ give rise to 3 distinct classes in S_m, we have $A^m_{[S]} = A^m_{1,1,-2} \times A^m_{1,-2,1} \times A^m_{-2,1,1}$.

LEMMA 2.2. *If $(m, S) = 1$ and A^m_S is simple and F^m_S hyperelliptic, $\lambda^m_{[S]}$ is surjective.*

Proof. $\sigma \in \mathrm{Aut}(F_m)$ induce isomorphisms

$$F^m_{1,1,-2} \xrightarrow{\rho} F^m_{-2,1,1} \xrightarrow{\rho} F^m_{1,-2,1}.$$

Thus we identify $A^m_{[S]} = A^m_{1,-2,1} \times A^m_{-2,1,1} \times A^m_{1,1,-2}$ with $(A^m_{1,-2,1})^3$ via the isomorphism $(1 \times \rho \times \rho^2)$. Consider the composition

$$\lambda = F_{1\times\rho\times\rho^2}\lambda^m_{[S]}\colon \mathbf{Q}[G_m, \rho] \to M_3(K),$$

where we identify $\mathrm{End}(A^m_{1,-2,1})$ with $\mathbf{Z}[\zeta]$ by mapping σ to ζ. That λ is surjective follows from the following:

$$\lambda(\rho) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \lambda(\rho^2) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \lambda(\sigma) = \Delta(\zeta, \zeta^{-2}, \zeta),$$

$$\lambda(I_0(\sigma^2\tau)) = \Delta(m, 0, 0), \quad \lambda(I_0(\sigma\tau^2)) = \Delta(0, m, 0),$$

$$\lambda(I_0(\sigma\tau^{-1})) = \Delta(0, 0, m). \qquad \square$$

Case 3. *A^m_S is simple and F^m_S is non-hyperelliptic.*

Then S is the class of (a, b, c), where a, b and c are distinct elements in $\mathbf{Z}/m\mathbf{Z} - \{0\}$ with $a+b+c=0$, and

$$A^m_{[S]} = A^m_{a,b,c} \times A^m_{a,c,b} \times A^m_{b,a,c} \times A^m_{b,c,a} \times A^m_{c,a,b} \times A^m_{c,b,a}.$$

We identify $A^m_{[S]}$ with $(A^m_{a,b,c})^6$ via the isomorphism

$$g = 1 \times (\rho^2 \iota) \times \iota \times \rho \times \rho^2 \times (\rho \iota),$$

and fix an isomorphism $\mathrm{End}(A^m_{a,b,c}) \to \mathbf{Z}[\zeta]$. Consider the composition

$$\lambda = F_g \lambda^m_{[S]} : \mathbf{Q}[G] \to M_6(K).$$

We have

$$\lambda(I_0(\sigma^b \tau^{-a})) = \Delta(m, 0, 0, 0, 0, 0), \quad \lambda(I_0(\sigma^c \tau^{-a})) = \Delta(0, m, 0, 0, 0, 0),$$

$$\lambda(I_0(\sigma^a \tau^{-b})) = \Delta(0, 0, m, 0, 0, 0), \quad \lambda(I_0(\sigma^c \tau^{-b})) = \Delta(0, 0, 0, m, 0, 0),$$

$$\lambda(I_0(\sigma^a \tau^{-c})) = \Delta(0, 0, 0, 0, m, 0), \quad \lambda(I_0(\sigma^b \tau^{-c})) = \Delta(0, 0, 0, 0, 0, m).$$

Also, there exists an $\alpha \in G_m$ such that α has exact order m in $\mathrm{Aut}(F_m) \subseteq \mathrm{Aut}(J_m)$ since $(m, S) = 1$. Hence, $\Delta_6(K) \subseteq \mathrm{Im}(\lambda) \subseteq M_6(K)$.

Furthermore, there are units a_j and b_j in $\mathbf{Z}[\zeta]$ such that

$$\lambda(\rho) = \begin{pmatrix} 0 & 0 & 0 & a_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_2 \\ 0 & a_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_4 & 0 \\ a_5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_6 & 0 & 0 & 0 \end{pmatrix}, \quad \lambda(\iota) = \begin{pmatrix} 0 & 0 & b_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & b_2 & 0 \\ b_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b_4 \\ 0 & b_5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b_6 & 0 & 0 \end{pmatrix}.$$

Finally, we note that $M_6(K)$ is the direct sum of the subspaces

$$\Delta(K), \ \Delta(K)\lambda(\rho), \ \Delta(K)\lambda(\rho^2), \ \Delta(K)\lambda(\iota), \ \Delta(K)\lambda(\iota\rho), \ \Delta(K)\lambda(\iota\rho^2).$$

Hence, λ is surjective. □

LEMMA 2.3. *If $(m, S) = 1$, A^m_S is simple and F^m_S is non-hyperelliptic, then $\lambda^m_{[S]}$ is surjective.*

We note that for any positive divisor M of m, the morphism

$$F_m \to F_M, \ (X, Y, Z) \to (X^{m/M}, Y^{m/M}, Z^{m/M})$$

induces an isomorphism

$$F^m_{Ma,Mb,Mc} \approx F^m_{a,b,-(a+b)} \quad (\text{where } a, b, a+b \in \mathbf{Z}/M\mathbf{Z} - \{0\}).$$

Together with this observation, Lemmas 2.1, 2.2 and 2.3 imply $\lambda^m_{[S]}$ is surjective for any $S \in S_m$. In what follows, we will prove that $\Phi : \mathbf{Q}[G] \to \mathrm{End}^0(J_m)$ is surjective. The isogeny $\varphi : J_m \to \Pi_{[S] \in S_m/\sim} J^m_{[S]}$ induces an isomorphism F_φ between $\mathrm{End}^0(J_m)$ and $\Pi_{[S] \in S_m/\sim} \mathrm{End}^0(A^m_{[S]})$. Consider $F = F_\varphi \Phi = (\lambda^m_{[S]})_{[S] \in S_m/\sim}$.

For each $S' \in [S]$, let $g(S') \in G_m$ be such that $F^m_{S'} = F_m / \langle g(S') \rangle$. Then

$$\lambda^m_{[S]}\left(\sum_{S' \in [S]} I_0(g(S'))\right) = m \quad \text{but } \lambda_{[\tilde{S}]}\left(\sum_{S' \in [S]} I_0(g(S'))\right) = 0 \quad \text{for } [S] \neq [\tilde{S}].$$

Since each $\lambda^m_{[S]}$ is suriective. F is suriective.

3. The kernel of φ

Throughout this section, let $m = p$ be a prime. By Pic functoriality, we have from the canonical projection $F_p \to F_S^p$, the homomorphism $(\varphi_S^p)^*: J_S^p \to J_p$. Then $(\varphi_S^p)^*$ is the dual homomorphism to $(\varphi_S^p)_*$, and

$$\varphi = \prod_{S \in S_p} (\varphi_S^p)_*: J_p \to \prod_{S \in S_p} J_S^p \quad \text{and} \quad \hat{\varphi} = \sum_{S \in S_p} (\varphi_S^p)^*: \prod_{S \in S_p} J_S^m \to J_m$$

are dual homomorphisms by the next lemma.

LEMMA 3.1. *Let $f: A \to B$ and $g: A \to C$ be homomorphisms of abelian varieties. Then, identifying $(B \times C)\hat{}$ with $\hat{B} \times \hat{C}$, the dual of $(f, g): A \to B \times C$ is $\hat{f} + \hat{g}: \hat{B} \times \hat{C} \to \hat{A}$.*

LEMMA 3.2. *Denoting the genus of F_p by g, $\hat{\varphi}\varphi = p$ and*

$$\deg(\varphi) = \deg(\hat{\varphi}) = p^g.$$

Proof. The proof of the lemma can be found in Corollary 3.8 of [12]. □

Let $\mathscr{L}$ be a line bundle on an abelian variety A over $\mathbf{C}$. For a point x on A, let T_x be the translation by x map, and let

$$\phi_{\mathscr{L}}: A \to \hat{A},\ x \to \text{isomorphism class of } T_x^* \mathscr{L} \otimes \mathscr{L}^{-1} \text{ in } \mathrm{Pic}(A).$$

Then $\phi_{\mathscr{L}}$ is a homomorphism between A and its dual $\hat{A}$ ([14], Section 8).

Mumford ([14], Section 23) defined a skew-symmetric bihomomorphism

$$e^{\mathscr{L}}: K(\mathscr{L}) \times K(\mathscr{L}) \to \mathbf{G}_m,$$

where $K(\mathscr{L}) = \mathrm{Ker}(\phi_{\mathscr{L}})$, with the property that if

$$e_n: A[n] \times \hat{A}[n] \to \mu_n$$

is the Weil e_n-pairing on A, then

$$x \in A[n], \quad y \in n_A^{-1}(K(\mathscr{L})) = \phi_{\mathscr{L}}(A[n])$$

imply

$$e_n(x, \phi_{\mathscr{L}}(y)) = e^{\mathscr{L}^n}(x, y). \tag{3.1}$$

PROPOSITION 3.3. *Let A and B be principally polarized abelian varieties, and let $\varphi: A \to B$ be an isogeny which respects the principal polarizations of A and B. If* $\mathrm{Ker}(\varphi) \subseteq A[n]$ *and the order of $A[n]$ is the square of the order of* $\mathrm{Ker}(\varphi)$, *then* $\mathrm{Ker}(\varphi)$ *and* $\mathrm{Ker}(\hat{\varphi})$ *are maximal isotropic subgroups in regard to the respective Weil e_n-pairings.*

Proof. Let $\mathscr{M}$ be a line bundle on B associated to a theta divisor Θ_B of B, and let $\mathscr{L} = \varphi^* \mathscr{M}$. Then $\mathscr{L}$ is a line bundle on A associated to a theta divisor on A, and $\mathscr{L}^n \approx \varphi^*(\mathscr{M}^n)$. Applying the corollary to Theorem 2 in Section 23 of [14],

$$e^{\mathscr{L}^n}|_{\mathrm{Ker}(\varphi) \times \mathrm{Ker}(\varphi)} \equiv 1. \tag{3.2}$$

Since the order of $A[n]$ is the square of $\mathrm{Ker}(\varphi)$, from (3.1), (3.2) and Theorem 4 in Section 23 of [14], we conclude that $\mathrm{Ker}(\varphi)$ is a maximal isotropic subgroup of $A[n]$ with respect to the Weil e_n-pairing.

The dual $\hat{\varphi}$ of φ respects the principal polarizations of B and A, and $\mathrm{Ker}(\hat{\varphi})$ has the same order as $\mathrm{Ker}(\varphi)$. Therefore the same argument as above shows that $\mathrm{Ker}(\hat{\varphi})$ is maximal isotropic with respect to the Weil e_n-pairing on B. □

The following corollary answers a question of Rohrlich.

COROLLARY 3.4. *The kernel of* $\varphi: J_p \to \Pi_{S\in S_p} J_S^p$ *is a maximal isotropic subgroup of* $J_p[p]$ *with respect to the Weil* e_p*-pairing on* J_p*. The same result holds for the kernel of* $\hat{\varphi}$.

Proof. The homomorphism $J_p \to J^p_{1,r,-(1+r)}$ respects the principal polarizations of J_p and $J^p_{1,r,-(1+r)}$ since it is induced from the covering $F_p \to F^p_{1,r,-(1+r)}$ by Albanese functoriality. Therefore φ respects the principal polarizations of $A = J_p$ and $B = \Pi_{r=2}^{p-2} J^p_{1,r,-(1+r)}$. The corollary is then a direct application of Proposition 3.3. □

LEMMA 3.5. *Consider the homomorphism*

$$\lambda = (\lambda^p_{[S]})_{S\in S_p}: \mathbf{Q}[G] \to \mathrm{End}^0\left(\prod_{[S]\in S_p/\sim} J^p_{[S]}\right) = \prod_{[S]\in S_p/\sim} \mathrm{End}^0(J^p_{[S]}).$$

Then $p^2\,\mathrm{End}(J^p_{[S]}) \subseteq \lambda(\mathbf{Z}[G])$.

Proof. For each $[S]\in S_p$, as noted in Section 2, there is an element $\alpha_S \in \mathbf{Z}[G_p]$ for which $\lambda^p_{[S]}(\alpha_S) = p$ and $\lambda^p_{[S']}(\alpha_s) = 0$ for $[S] \neq [S']$. If we re-examine the proof to establish the surjectivity of $\lambda^p_{[S]}$, we see that $p\,\mathrm{End}(J^p_{[S]}) \subseteq \lambda^p_{[S]}(\mathbf{Z}[G])$. Hence it follows that

$$\{0\} \times \cdots \times \{0\} \times p^2\,\mathrm{End}(J^p_{[S]}) \times \{0\} \times \cdots \times \{0\} \subseteq \mathrm{Im}(\mathbf{Z}[G]).$$

This completes the proof of the lemma. □

Let $\phi: A \to B$ be an isogeny with kernel K of exponent m. Given $\alpha \in \mathrm{End}(A)$, there is a unique $\beta \in \mathrm{End}(B)$ such that $\phi \circ \alpha = n\beta \circ \phi \Leftrightarrow \alpha(n_A^{-1}(K)) \subseteq K$. Thus given $\alpha \in \mathrm{End}(A)$, there is a unique $\beta \in \mathrm{End}(B)$ for which $\phi m_A^2 \alpha = m_B \beta \phi$. Thus implies that

$$F_\phi: \mathrm{End}^0(A) \to \mathrm{End}^0(B)$$

maps $m\,\mathrm{End}(A)$ into $\mathrm{End}(B)$.

PROPOSITION 3.6. $p^2\,\mathrm{End}(J_p) \subseteq \Phi(\mathbf{Z}[G])$.

Proof. Applying Maschke's theorem ([5], Theorem 3.14) to the exact sequence in Theorem A, there is an idempotent $e \in \mathbf{Q}[G]$ such that (1) $\mathbf{T} = \mathbf{Q}[G]e$, (2) the map $f: \mathbf{Q}[G] \to \mathbf{T} \times \mathrm{End}^0(J_p)$, $X \to (Xe, \Phi(X))$ is an isomorphism. Clearly $\Sigma = \mathbf{Z}[G]e \times \mathrm{End}(J_p)$ is a $\mathbf{Z}$-order in $\Sigma \otimes \mathbf{Q}$, $f(\mathbf{Z}[G]) \subseteq \Sigma$, and with the identification f, Φ becomes the projection map $\mathbf{T} \times \mathrm{End}^0(J_p) \to \mathrm{End}^0(J_p)$,

$(X, Y) \to Y$. Since G has order $6p^2$, Σ is contained in $(6p^2)^{-1}\mathbf{Z}[G]$. Applying Φ, we obtain $\mathrm{End}(J_p) \subseteq (6p^2)^{-1}\Phi(\mathbf{Z}[G])$. Maintaining the notation of Lemma 3.5, we have $\lambda = F_\varphi \Phi$. The remarks preceding the lemma together with Lemmas 3.2 and 3.8 imply

$$F_\varphi(p^3 \,\mathrm{End}(J_p)) \subseteq p^2 \,\mathrm{End}\left(\prod_{S \in S_p} J_S^p\right) \subseteq \lambda(\mathbf{Z}[G]).$$

Hence, $p^3 \,\mathrm{End}(J_p)$ is contained in $\Phi(\mathbf{Z}[G])$. The g.c.d. of $6p^2$ and p^3 is p^2, and the proposition follows. □

4. Singular homology of Fermat curves

It is known (see the appendix in [9]) that $H_1(F_m(\mathbf{C}), \mathbf{Z})$ is a cyclic module over $\mathbf{Z}[G_m]$ with

$$(1 - \sigma)(1 - \tau)I$$

as a generator. Hence g as defined in Proposition B is also a generator.

By Lemma 1.1,

$$A, B, C \in \mathrm{Ann}_{\mathbf{Z}[G_m]}(H_1(F_m(\mathbf{C}), \mathbf{Z})),$$

where A, B, C are as defined in Section 1.

We will determine, in what follows, generators for this ideal of $\mathbf{Z}[G_m]$.

A special case of Lemmas 5.2 and 5.3 is that the ideal $\mathbf{J}$ of $\mathbf{Q}[G_m]$ generated by A, B, C has dimension $(3m-2)$ as a vector space over $\mathbf{Q}$. Fix a basis $\{A_1, \ldots, A_{3m-2}\}$ for $\mathbf{J}$ and extend it to a basis $\{A_1, \ldots, A_{3m-2}, B_1, \ldots, B_l\}$ of $\mathbf{Q}[G_m]$, where $l + 3m - 2 = m^2$. Then $\{B_1 g, \ldots, B_l g\}$ spans $H_1(F_m(\mathbf{C}, \mathbf{Q}))$ over $\mathbf{Q}$, and is therefore a basis because the genus of F_m is $l/2$. In particular, the annihilator of $H_1(F_m(\mathbf{C}), \mathbf{Q})$ over $\mathbf{Q}[G_m]$ is $\mathbf{J}$.

Let $\Delta = \Sigma' \tau^r \sigma^{-s} \in \mathbf{Q}[G_m]$, where the sum Σ' is taken over (r, s) with $0 \leqslant r, s$, $r + s \leqslant m - 2$. We note that $1 - \sigma$ is a unit in the ring $R = \mathbf{Q}[\sigma]/(I_0(\sigma))$ and that $(1 \div \sigma^{-1})\Delta = I_0(\tau) - \sigma I_0(\sigma\tau)$ in $\mathbf{Z}[G_m]$. Thus, in

$$R[\tau],\ \Delta R[\tau] \subseteq (I_0(\tau),\ I_0(\sigma\tau))R[\tau] \quad \text{and} \quad (I_0(\sigma),\ \Delta)\mathbf{Z}[G_m] \subseteq \mathbf{J} \cap \mathbf{Z}[G_m].$$

The latter inclusion induces an epimorphism

$$\mathbf{Z}[G_m]/(I_0(\sigma),\ \Delta) \to \mathbf{Z}[G_m]/(\mathbf{J} \cap \mathbf{Z}[G_m]).$$

By definition of Δ, there is a surjective mapping

$$\sum_{0 \leqslant r \leqslant m-2, 0 \leqslant s \leqslant m-3} \mathbf{Z}\sigma^r \tau^s \to \mathbf{Z}[G_m]/(\mathbf{J} \cap \mathbf{Z}[G_m])$$

between free $\mathbf{Z}$-modules of rank $2l$. Therefore, the latter map is an isomorphism and we have

PROPOSITION 4.1. *The annihilator of the* $\mathbf{Z}[G_m]$*-module* $H_1(F_m(\mathbf{C}), \mathbf{Z})$ *is the ideal of* $\mathbf{Z}[G_m]$ *generated by* $I_0(\sigma)$ *and* Δ.

It follows that $\{\sigma^r\tau^s g \mid 0 \leqslant r \leqslant m-2,\ 0 \leqslant s \leqslant m-3\}$ is a $\mathbf{Z}$-basis of $H_1(F_m(\mathbf{C}), \mathbf{Z})$.

We recall that $H^0(F_m, \Omega^1)$ is spanned by

$$w_{r,s} = x^{r-1}y^{s-1}\frac{dx}{y^{m-1}} (1 \leqslant r, s, r+s \leqslant m-1).$$

To prove that

$$\iota(g) = g \quad \text{and} \quad \rho(g) = g$$

in homology is equivalent to showing that

$$\int_{\iota(g)+g} w_{r,s} = \int_g (\iota^* w_{r,s} + w_{r,s}) = 0$$

and

$$\int_{\rho(g)-g} w_{r,s} = \int_g (\rho^* w_{r,s} - w_{r,s}) = 0$$

for all $r, s \geqslant 1$ and $r + s \leqslant m-1$, i.e. that

$$\int_g w_{s,r} = \int_g w_{r,s} \tag{4.1}$$

and

$$\int_g w_{s,m-r-s} = \int_g w_{r,s} \tag{4.2}$$

for all r, s as stated above.

If $B(u, v) = \int_0^1 t^{u-1}(1-t)^{v-1}\,dt$ is the classical beta function, we have by Rohrlich's calculations in [9] that equations (4.1) and (4.2) are equivalent to

$$\frac{B(s/m, r/m)}{m}(1-\zeta^s)(1-\zeta^r) = \frac{B(r/m, s/m)}{m}(1-\zeta^r)(1-\zeta^s) \tag{4.3}$$

and

$$\alpha^{2r+s+m}\frac{B(s/m, 1-r+s/m)}{m}(1-\zeta^s)(1-\zeta^{-r-s}) = \frac{B(r/m, s/m)}{m}(1-\zeta^r)(1-\zeta^s) \tag{4.4}$$

respectively. (4.3) is trivially true. (4.4) follows from the identity

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

5. Endomorphisms, I

Let $X, Y, Z, \tilde{X}, \tilde{Y}, \tilde{Z} \in \mathbf{Q}[G_m]$, and

$$\alpha = X + Y\rho + Z\rho^2 + \tilde{X}\iota + \tilde{Y}\rho\iota + \tilde{Z}\rho^2\iota \in \mathbf{Q}[G].$$

Then $\Phi(\alpha) \in \mathrm{End}(J_m)$ if and only if, for all $r, s \in \mathbf{Z}/m\mathbf{Z}$, $\alpha(\sigma^r\sigma^s g) \in H_1(F_m(\mathbf{C}), \mathbf{Z})$, where g is as defined in Proposition B. Since $\rho(g) = g$ and $\iota(g) = -g$, Theorem C follows.

Let $I_k(T) \in \mathbf{Z}[T]$ and $W \in \mathbf{Q}[G_m, \rho]$ be as defined in the Introduction. Let $w = \Phi(W) \in \mathrm{End}^0(J_m)$. The rest of this section is devoted to showing that w is in $\mathrm{End}(J_m)$ but not in $\Phi(\mathbf{Z}[G])$.

Since

$$I_k(T) = \frac{T^k}{k!}\frac{d^k}{dT^k}\left(\frac{1-T^m}{1-T}\right),$$

it follows, using Leibnitz's rule for derivatives and induction, that

LEMMA 5.1. *When* $0 < k < m$, $(1-T)I_k(T) = -\binom{m}{k}T^m + TI_{k-1}(T)$.

LEMMA 5.2. *Let* F *be an arbitrary field, and let* θ *be the element* $(1-\sigma)(1-\tau)(1-\sigma\tau)$ *of the group ring* $F[G_m]$. *Then* $\dim_F \mathrm{Ker}_F(\theta) = 3m-2$, *where* $\mathrm{Ker}_F(\theta)$ *is the annihilator of* θ *in* $F[G_m]$.

Proof. Let $X = \Sigma a_{r,s}\sigma^r\tau^s \in F[G_m]$. X is in $\mathrm{Ker}_F(\sigma-1)$ if and only if $a_{r,s} = a_{r+1,s}$ for all (r, s). Thus $\mathrm{Ker}_F(\sigma-1) = I_0(\sigma)F[G_m]$ has dimension m over F. The same is true if σ is replaced by τ or $\sigma\tau$. X is in $\mathrm{Ker}_F(\sigma-1)$ and $(\tau-1)F[G_m]$ if and only if $a_{r,s} = a_{r+1,s}$ for all (r, s), and $\Sigma_s a_{r,s} = 0$ for all r. For such an X, all the $a_{r,s}$'s are uniquely determined once the $a_{0,s}$'s are known for $0 < s < m-1$. So

$$\mathrm{Ker}(\sigma-1) \cap (\tau-1)F[G_m] \quad \text{and} \quad (\sigma-1)(\tau-1)F[G_m]$$

have dimensions $m-1$ and $(m^2-m)-(m-1)$ over F. Furthermore,

$$(\sigma-1)F[G_m] \cap (\tau-1)F[G_m]$$

has dimension

$$\dim(\sigma-1)F[G_m] + \dim(\tau-1)F[G_m] - \dim(\sigma-1, \tau-1)F[G_m] = (m-1)^2.$$

Therefore,

$$(\sigma-1)F[G_m] \cap (\tau-1)F[G_m]$$

is equal to

$$(\sigma-1)(\tau-1)F[G_m].$$

Finally, we note that X is in $\mathrm{Ker}(\sigma\tau-1)$ and $(\sigma-1)(\tau-1)F[G_m]$ if and only if

$a_{r,s}=a_{r+1,s+1}$ for all (r, s), and $\Sigma_r a_{r,s}=0$ for all s. For such an X, all the $a_{r,s}$'s are uniquely determined if $a_{0,s}$ $(0 \leqslant s \leqslant m-2)$ are known. Therefore

$$\mathrm{Ker}_F(\sigma-1)\cap(\sigma-1)(\tau-1)F[G_m] \quad \text{and} \quad \mathrm{Ker}_F(\theta)$$

have dimensions $m-1$ and $m^2-((m-1)^2-(m-1))=3m-2$ respectively. □

LEMMA 5.3. *Maintaining the notation of Lemma* 6.2, $\mathrm{Ker}_F(\theta)$ *is the ideal of* $F[G_m]$ *generated by* $I_0(\sigma)$, $I_0(\tau)$, $I_0(\sigma\tau)$ *and* $I_1(\sigma)I_1(\tau)$.

Proof. Let $\mathbf{J}_1$, $\mathbf{J}_2$ and $\mathbf{J}_3$ be the principal ideals of $F[G_m]$ generated by $I_0(\sigma)$, $I_0(\tau)$ and $I_0(\sigma\tau)$ respectively, and let $\mathbf{J}_F=\Sigma_{i=1}^3 \mathbf{J}_i$. We claim that $\mathbf{J}_F$ has dimension $3m-2$ and $3m-3$ depending on whether m is relatively prime to the characteristic of F or not. We fix the bases $\{\tau^r I_0(\sigma)\}$, $\{\sigma^r I_0(\tau)\}$, $\{\sigma^r I_0(\sigma\tau)\}$, where r ranges between 0 and $m-1$ inclusive in each case, for $\mathbf{J}_1$, $\mathbf{J}_2$ and $\mathbf{J}_3$ respectively. Let

$$X=\sum_{0\leqslant r\leqslant m-1} a_r\tau^r I^0(\sigma)=\sum_{0\leqslant r\leqslant m-1} b_r\sigma^r I_0(\sigma)$$

be in $\mathbf{J}_1\cap\mathbf{J}_2$, where each $a_r, b_r\in F$. By comparing the coefficients of τ^r, $a_r=a_0$ for all r. Hence, $\mathbf{J}_1\cap\mathbf{J}_2$ is $F.I_0(\sigma)I_0(\tau)$, and

$$\{\sigma^r I_0(\sigma), \tau^s I_0(\sigma) \mid 0\leqslant r\leqslant m-1,\ 0\leqslant s\leqslant m-2\}$$

is an F-basis for $(\mathbf{J}_1+\mathbf{J}_2)$.

Let a_r, b_s, $c_r\in F$ be such that

$$Y=\sum_{0\leqslant r\leqslant m-1}\sigma^r a_r I_0(\tau)+\sum_{0\leqslant s\leqslant m-2} b_s\tau^s I_0(\sigma)=\sum_{0\leqslant r\leqslant m-1} c_r\sigma^r I_0(\sigma\tau).$$

Comparing the coefficients of $\sigma^r\tau^k$ and $\sigma^r\tau^{m-1}$, where $0\leqslant k\leqslant m-2$ and $0\leqslant r\leqslant m-1$, we obtain $a_r+b_k=c_{r-k}$ and $a_r=c_{r+1}$. In particular, $c_{m-1}=a_{m-1}+b_0=c_0+b_0$. By induction, $c_{m-k}=c_0+kb_0$ for $1\leqslant k\leqslant m$. If m is prime to the characteristic of F, we conclude that $(\mathbf{J}_1+\mathbf{J}_2)\cap\mathbf{J}_3=F.I_0(\sigma)I_0(\tau)$ and $\mathbf{J}_F$ has dimension $3m-2$.

Let m be a multiple of the characteristic of F. Then, maintaining the notation of the previous paragraph, $Y=(c_0I_0(\sigma)-b_0I_1(\sigma))I_0(\sigma\tau)$, since $c_r=c_{m-(m-r)}=c_0+(m-r)b_0$. Thus,

$$(\mathbf{J}_1+\mathbf{J}_2)+\mathbf{J}_3\subseteq F.I_0(\sigma)I_0(\tau)\oplus F.I_1(\sigma)I_0(\sigma\tau).$$

Since $\mathrm{Ker}_F((\sigma-1)(\tau-1))$ and $(\mathbf{J}_1+\mathbf{J}_2)$ have the same dimension (see the proof of Lemma 5.2), and the latter is contained in the former, they are equal. By Lemma 5.1, $I_1(\sigma)I_0(\sigma\tau)$ is annihilated by $(\sigma-1)(\tau-1)$. Hence, $(\mathbf{J}_1+\mathbf{J}_2)\cap\mathbf{J}_3$ equals $F.I_0(\sigma)I_0(\tau)\oplus F.I_1(\sigma)I_0(\sigma\tau)$, $\mathbf{J}_F$ has dimension $3m-3$ and a basis

$$\{\tau^r I_0(\sigma), \sigma^s I_0(\tau), \sigma^t I_0(\sigma\tau) \mid 0\leqslant r\leqslant m-1,\ 0\leqslant s\leqslant m-2,\ 0\leqslant t\leqslant m-3\}.$$

By Lemma 5.2, θ annihilates $Z=I_1(\sigma)I_1(\tau)$. We claim that Z is not in $\mathbf{J}_F$.

Suppose, on the contrary, that

$$Z = \sum_{0 \leqslant r \leqslant m-1} a_r \tau^r I_0(\sigma) + \sum_{0 \leqslant s \leqslant m-2} b_s \sigma^s I_0(\tau) + \sum_{0 \leqslant t \leqslant m-3} c_t \sigma^t I_0(\sigma\tau).$$

Then a contradiction follows by comparing the coefficients of σ^r, τ^s, $\sigma^{m-2}\tau^{m-1}$ for $0 \leqslant r \leqslant m-1$ and $1 \leqslant s \leqslant m-1$. We omit the details of this routine calculation. □

Let A be the ring $\mathbf{Z}[G_m]/(\mathbf{J} \cap \mathbf{Z}[G_m])$. We recall (Proposition 4.1) that the ideal $\mathbf{J} \cap \mathbf{Z}[G_m]$ is generated by $I_0(\sigma)$ and $\Delta = \Sigma' \tau^r \sigma^{-s}$, where the Σ' is taken over (r, s) with $0 \leqslant r, s, r+s \leqslant m-2$. Under the homomorphism $\mathbf{Z}[G_m] \to \mathbf{Z}[\tau]$, in which $\sigma \to 1$ and $\tau \to \tau$, the elements $I_0(\sigma)$ and Δ are mapped onto m and $f(\tau)$ respectively, where

$$f(T) = \sum_{l=0}^{m-2} (m - l - 1)T^l.$$

Then

$$I_1(\tau) = -\tau f(\tau) = 0 \quad \text{in } A/(1-\sigma)A = (\mathbf{Z}/m\mathbf{Z})[\tau]/(f(\tau))$$

and

$$I_1(\tau) \in (1-\sigma)A.$$

By symmetry,

$$I_1(\sigma) \in (1-\tau)A.$$

By Lemma 5.1,

$$m = (\sigma - 1)I_1(\sigma) = (1-\tau)I_1(\tau)$$

in A. We conclude that

$$I_1(\sigma)I_1(\tau) \in m\mathbf{Z}[G_m] + \mathbf{J}.$$

LEMMA 5.4. *Let* $X \in \mathbf{Q}[G_m]$. *Then* $X \in \mathbf{Z}[G_m] + \mathbf{J}$ *if and only if* $\theta X \in \mathbf{Z}[G_m]$.

Proof. Let l be a prime. Suppose that $Y = lX \in \mathbf{Z}[G_m]$, and $\theta X \in \mathbf{Z}[G_m]$. Then $\theta Y = l(\theta X) \equiv 0 \pmod{l}$. By Lemma 5.3 and the remark before Lemma 5.4,

$$Y \in l\mathbf{Z}[G_m] + \mathbf{J} \quad \text{and} \quad X \in \mathbf{Z}[G_m] + \mathbf{J}.$$

Assume now that

$$l^n X \in \mathbf{Z}[G_m] \quad \text{and} \quad \theta X \in \mathbf{Z}[G_m].$$

Then $l^{n-1}X \in \mathbf{Z}[G_m] + \mathbf{J}$. Choose $Z \in \mathbf{J}$ such that $l^{n-1}(X - Z) \in \mathbf{Z}[G_m]$. Also $\theta(X - Z) = \theta X \in \mathbf{Z}[G_m]$. By induction hypothesis, $X - Z \in \mathbf{Z}[G_m] + \mathbf{J}$. Hence we have proved that if $l^n X \in \mathbf{Z}[G_m]$ and $\theta X \in \mathbf{Z}[G_m]$, then $X \in \mathbf{Z}[G_m] + \mathbf{J}$.

We can now prove the following statement by induction on k ($k \in \mathbf{Z}_{\geqslant 0}$): if $kX \in \mathbf{Z}[G_m]$ and $\theta X \in \mathbf{Z}[G_m]$, then $X \in \mathbf{Z}[G_m] + \mathbf{J}$, since we know it to be true for any prime power $k = l^n$. □

Applying Corollary 5.4, we obtain

COROLLARY 5.5. *Let* $X \in \mathbf{Z}[G_m]$. *Then* $X \in m\mathbf{Z}[G_m] + \mathbf{J}$ *if and only if* $\theta X \equiv 0 \pmod{m}$.

LEMMA 5.6. *Let*

$$X, Y, Z \in \mathbf{Q}[G_m].$$

Then

$$\Phi(X + Y\rho + Z\rho^2) \in \mathrm{End}(J_m)$$

if and only if

$$X\sigma^r\tau^s + Y\sigma^{-s}\tau^{r-s} + Z\sigma^{s-r}\tau^{-r} \in \mathbf{Z}[G_m] + \mathbf{J} \quad \forall (r, s) \in \mathbf{Z}^2.$$

Proof. This follows directly from Theorem C. □

PROPOSITION 5.7. $w \in \mathrm{End}(J_m)$.

Proof. Let

$$\eta_{r,s} = I_1(\sigma)I_3(\tau)(\sigma^{-s}\tau^{r-s} - \sigma^r\tau^s) + I_3(\sigma)I_1(\tau)(\sigma^{s-r}\tau^{-r} - \sigma^{-s}\tau^{r-s}).$$

In view of Corollary 5.5 and Lemma 5.6, to prove the proposition, it suffices to verify that $\theta\eta_{r,s} \in m\mathbf{Z}[G_m]$ for all $(r, s) \in \mathbf{Z}^2$.

By Lemma 5.1, and using the fact that $T^a \equiv 1 + a(T-1) \pmod{(T-1)^2}$, we have that:

$$\theta I_1(\sigma)I_3(\tau)(\sigma^{-s}\tau^{r-s} - \sigma^r\tau^s) \equiv (2s - r)I_0(\sigma)I_0(\tau) \pmod{m},$$

$$\theta I_1(\tau)I_3(\sigma)(\sigma^{s-r}\tau^{-r} - \sigma^{-s}\tau^{r-s}) \equiv (r - 2s)I_0(\sigma)I_0(\tau) \pmod{m}.$$

Therefore, $\theta\eta_{r,s} \equiv 0 \pmod{m}$, as required. □

LEMMA 5.8. *Let* $X, Y, Z \in \mathbf{Q}[G_m]$, *and let* I *be either an ideal of* $\mathbf{Q}[G_m]$ *or the subring* $\mathbf{Z}[G_m] + \mathbf{J}$. *Suppose that*

$$X\sigma^r\tau^s + Y\sigma^{-s}\tau^{r-s} + Z\sigma^{s-r}\tau^{-r} \in I, \tag{5.1}$$

for all $(r, s) \in \mathbf{Z}^2$. *Then* $(\sigma-1)^2X$, $(\sigma-1)(\tau-1)X$, $(\tau-1)^2X \in I$, *with similar statements for* Y *and* Z.

Proof. From $X + Y + Z \in I$ and (5.1), we obtain

$$Y(\sigma^{r+s}\tau^{2s-r} - 1) + Z(\sigma^{2s-r}\tau^{r+s} - 1) \in I, \tag{5.2}$$

for all $(r, s) \in \mathbf{Z}^2$. By setting

$$r \equiv -s \pmod{m}, \quad r \equiv 2s \pmod{m} \quad \text{and} \quad 2r \equiv s \pmod{m},$$

and using the hypothesis that m is coprime to 3, we obtain:

$$Y(\sigma\tau - \sigma) + Z(1 - \sigma) \in I, \tag{5.3}$$

$$Y(\sigma - 1) + Z(\sigma\tau - 1) \in I, \tag{5.4}$$

$$Y(\sigma\tau - 1) + Z(\tau - 1) \in I. \tag{5.5}$$

Setting $r = s = 1$, we get

$$Y(\sigma^2\tau - 1) + Z(\sigma\tau^2 - 1) \in I. \tag{5.6}$$

From (5.4) and (5.6), it follows that $Y(\sigma\tau - 1) + Z(\tau^2 - \tau) \in I$. Together with (5.5), the latter gives $(\tau - 1)^2 Z \in I$. By symmetry, $(\sigma - 1)^2 Z \in I$. Adding (5.3) and (5.4), we obtain $Y(\sigma\tau - 1) + Z(\sigma\tau - \sigma) \in I$. Together with (5.5), $(\sigma - 1)(\tau - 1)Z \in I$ follows. □

COROLLARY 5.9. *Let*

$$A = \Phi(\mathbf{Z}[G_m]) \quad \textit{and} \quad B = \Phi(\mathbf{Z}[G_m, \rho]).$$

Then

$$A^3 \to B,\ (X, Y, Z) \to X + Y\rho + Z\rho^2$$

is a left A-module isomorphism. In particular, $\mathrm{Ker}(\Phi|_{\mathbf{Q}[G_m,\rho]}) = \mathbf{J}\mathbf{Q}[G_m, \rho]$.

Proof. Let $\alpha = X + Y\rho + Z\rho^2 \in \mathrm{Ker}(\Phi)$, with $X, Y, Z \in \mathbf{Q}[G_m]$. Since α acts as the zero endomorphism, we have

$$X\sigma^r\tau^s + Y\sigma^{s-r}\tau^{r-s} + Z\sigma^{s-r}\tau^{-r} \in \mathbf{J} \quad \forall (r, s) \in \mathbf{Z}^2.$$

By Lemma 5.8, $(\sigma - 1)(\tau - 1)X \in \mathbf{J}$. Since $(\sigma - 1)(\tau - 1)$ is a unit in $\mathbf{Q}[G_m]/\mathbf{J}$, we have that $X \in \mathbf{J}$. Likewise, Y and Z are in $\mathbf{J}$. This proves the lemma. □

COROLLARY 5.10. $m(\mathrm{End}(J_m) \cap \Phi(\mathbf{Q}[G_m, \rho])) \subseteq \Phi(\mathbf{Z}[G_m, \rho])$.

Proof. This follows directly from Lemmas 5.7 and 5.8 (taking $I = \mathbf{Z}[G_m] + \mathbf{J}$), and the fact that there is a $y \in \mathbf{Z}[G_m]$ such that $m \equiv (\sigma - 1)(\tau - 1)y \pmod{\mathbf{J}}$. □

COROLLARY 5.11. *The element* $W \in \mathbf{Q}[G_m, \rho]$ *is not in* $\mathbf{Z}[G] + \mathrm{Ker}(\Phi)$.

Proof. Let $m \geqslant 7$, and let $\bar{\theta}$ be $\theta(\sigma^{-1} - 1)(\sigma\tau^2 - 1)(\sigma^2\tau - 1)$ in $\mathbf{Q}[G_m]$. By Theorem A, $\bar{\theta}$ annihilates $\mathrm{Ker}(\Phi)$. Suppose that $W = X + Y$, where $X \in \mathbf{Z}[G_m]$ and $Y \in \ker(\Phi)$. Then

$$\bar{\theta}W = \bar{\theta}X \in \mathbf{Z}[G_m] \quad \text{and} \quad \bar{\theta}I_1(\sigma)I_3(\tau) \in m\mathbf{Z}[G_m].$$

The coefficient of σ in $\sigma^{-1}\tau^{-3}\bar{\theta}I_1(\sigma)I_3(\tau)$ is

$$c \equiv 1 - 5\binom{m-1}{3} + 6\binom{m-2}{3} - \binom{m-3}{3} \pmod{m},$$

whence $6c$ is congruent to $12\binom{m-2}{3}$ or $-48 \pmod{m}$. In particular, c is not

divisible by m, a contradiction. This proves that W is not in $\mathbf{Z}[G]+\mathrm{Ker}(\Phi)$ for $m \geqslant 7$.

Now let $m=5$. Suppose again that $W \in \mathbf{Z}[G]+\mathrm{Ker}(\Phi)$. Then

$$w \in \Phi(\mathbf{Z}[G]) \subseteq \mathrm{End}(J_5) \quad \text{and} \quad w = x + \iota y$$

for some $x, y \in \Phi(\mathbf{Z}[G_5, \rho])$. From $I_0(\sigma^{-1}\tau)(1+\iota)=0$ in $\mathrm{End}(J_5)$, we have

$$I_0(\sigma^{-1}\tau)w = I_0(\sigma^{-1}\tau)(x - y) \in \Phi(\mathbf{Z}[G_5, \rho]).$$

By Corollary 5.9,

$$\sigma^{-1}\tau^{-3} I_0(\sigma^{-1}\tau) I_1(\sigma) I_3(\tau) \in 5\Phi(\mathbf{Z}[G_5]).$$

This is not the case by an explicit computation using the following facts

(1) $I_0(\sigma) = \Delta = 0$ in $\mathrm{End}(J_5)$,
(2) $\{\sigma^r \tau^s \mid 0 \leqslant r \leqslant 3,\ 0 \leqslant s \leqslant 2\}$ is a free $\mathbf{Z}$-basis of $\Phi(\mathbf{Z}[G_5])$.

This contradiction shows, as before, that W is not in $\mathbf{Z}[G]+\mathrm{Ker}(\Phi)$. □

6. Endomorphisms of J_m, II

Proceeding as in Proposition 5.6, we can also show that the image v of

$$V = m^{-1} I_1(\sigma) I_2(\tau)(\rho - 1) \in \mathbf{Q}[G_m, \rho]$$

under Φ is in $\mathrm{End}(J_m)$. Alternatively, we can deduce this fact as follows. Let $\bar{W} = mW$ and $\bar{V} = mV$. Then

$$(1 - \tau)^2 \bar{W} \equiv \tau^2 I_1(\sigma) I_1(\tau)(\rho - 1) \,(\mathrm{mod}(m\mathbf{Z}[G_m, \rho])),$$

$$(1 - \tau)\bar{V} \equiv \tau I_1(\sigma) I_1(\tau)(\rho - 1) \,(\mathrm{mod}(m\mathbf{Z}[G_m, \rho])).$$

Therefore

$$(1-\tau)\{\tau\bar{V} - (1 - \tau)\bar{W}\} \equiv 0 \,(\mathrm{mod}(m\mathbf{Z}[G_m, \rho])).$$

Let

$$\tau\bar{V} - (1 - \tau)\bar{W} = X + Y\rho + Z\rho^2,$$

with $X, Y, Z \in \mathbf{Z}[G_m]$. Then

$$(1 - \tau)X \equiv (1 - \tau)Y \equiv (1 - \tau)Z \equiv 0 \,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

A direct calculation shows that the annihilator of $(1-\tau)$ in $(\mathbf{Z}/m\mathbf{Z})[G_m]$ is the ideal generated by $\Sigma_{j=0}^{m-1} \tau^j$. Therefore,

$$\tau\bar{V} - (1 - \tau)\bar{W} \in m\mathbf{Z}[G_m, \rho] + \mathbf{JQ}[G_m, \rho]$$

and

$$V - \tau^{-1}(1 - \tau)W \in \mathbf{Z}[G_m, \rho] + \mathbf{JQ}[G_m, \rho].$$

We will now show that

$$\mathrm{End}(J_m) \cap \Phi(\mathbf{Z}[G_m, \rho]) = \Phi(\mathbf{Z}[G_m, \rho, W]).$$

Let

$$\alpha = X + Y\rho + Z\rho^2 \in \mathbf{Q}[G_m, \rho] \quad \text{with } X, Y, Z \in \mathbf{Q}[G_m],$$

be such that

$$\Phi(\alpha) \in \mathrm{End}(J_m).$$

By Lemma 5.6, we may assume that $X + Y + Z = 0$. By Lemma 5.8, we have that

$$(\sigma - 1)^2 X, \quad (\sigma - 1)(\tau - 1)X \quad \text{and} \quad (\tau - 1)^2 X$$

are in $\mathbf{Z}[G_m] + \mathbf{J}$, with similar statements for Y and Z.

We choose $\tilde{X}$, $\tilde{Y}$ and $\tilde{Z}$ in $\mathbf{Z}[G_m]$ such that

$$\tilde{X} \equiv mX \,(\mathrm{mod}\, \mathbf{J}), \quad \tilde{Y} \equiv mY \,(\mathrm{mod}\, \mathbf{J}), \quad \text{and} \quad \tilde{Z} \equiv mZ \,(\mathrm{mod}\, \mathbf{J}).$$

Then

$$(\sigma-1)^2\theta\tilde{X} \equiv (\sigma-1)(\tau-1)\theta\tilde{X} \equiv (\tau-1)^2\theta\tilde{X} \equiv 0\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

We wish to show that there are integers a_X, b_X and c_X such that

$$\theta\tilde{X} \equiv a_X I_0(\sigma)I_1(\tau) + b_X I_1(\sigma)I_0(\tau) + c_X I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

Let

$$\theta\tilde{X} = \sum_{0 \leqslant r,s \leqslant m-1} a_{r,s}\sigma^r\tau^s \in \mathbf{Z}[G_m],$$

and define $a_X = a_{0,1} - a_{0,0}$, $b_X = a_{1,0} - a_{0,0}$ and $c_X = a_{0,0}$.

From

$$(\sigma-1)^2\theta\tilde{X} \equiv 0\,(\mathrm{mod}(m\mathbf{Z}[G_m])), \quad (\tau-1)^2\theta\tilde{X} \equiv 0\,(\mathrm{mod}(m\mathbf{Z}[G_m]))$$

and

$$(\sigma - 1)(\tau - 1)\theta\tilde{X} \equiv 0\,(\mathrm{mod}(m\mathbf{Z}[G_m])),$$

we obtain the following congruences respectively

$$a_{r+2,s} - 2a_{r+1,s} + a_{r,s} \equiv 0\,(\mathrm{mod}\, m), \tag{6.1}$$

$$a_{r,s+2} - 2a_{r,s+1} + a_{r,s} \equiv 0\,(\mathrm{mod}\, m), \tag{6.2}$$

$$a_{r+1,s+1} + a_{r,s} \equiv a_{r,s+1} + a_{r+1,s}\,(\mathrm{mod}\, m). \tag{6.3}$$

By double induction on (r, s), we can prove that the above congruences imply that

$$a_{r,s} \equiv a_X . s + b_X . r + c_X \,(\mathrm{mod}\, m) \quad \forall (r, s) \quad \text{with } 0 \leqslant r, s \leqslant m - 1.$$

We omit the details here. We conclude that

$$\theta\tilde{X} \equiv a_X I_0(\sigma)I_1(\tau) + b_X I_1(\sigma)I_0(\tau) + c_X I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

Similarly, there are integers a_Y, a_Z, b_Y, b_Z, c_Y, c_Z such that

$$\theta\tilde{Y} \equiv a_Y I_0(\sigma)I_1(\tau) + b_Y I_1(\sigma)I_0(\tau) + c_Y I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])),$$

$$\theta\tilde{Z} \equiv a_z I_0(\sigma)I_1(\tau) + b_Z I_1(\sigma)I_0(\tau) + c_Z I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

Using Lemma 5.1,

$$a_Y I_0(\sigma)I_1(\tau)(\sigma^{r+s}\tau^{2s-r} - 1) = a_Y I_0(\sigma)I_1(\tau)(\tau^{2s-r} - 1)$$

is congruent modulo $m\mathbf{Z}[G_m]$ to

$$a_Y I_0(\sigma)I_1(\tau)\{(2s - r)(r - 1)\} \equiv a_Y(r - 2s)I_0(\sigma)I_0(\tau).$$

Similarly,

$$b_Y I_1(\sigma)I_0(\tau)(\sigma^{r+s}\tau^{2s-r} - 1) \equiv -b_Y(r + s)I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

Therefore,

$$\theta\tilde{Y}(\sigma^{r+s}\tau^{2s-r} - 1) \equiv -\{a_Y(2s-r) + b_Y(r+s)\}I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])),$$

and

$$\theta\tilde{Z}(\sigma^{2r-s}\tau^{r+s} - 1) \equiv -\{a_Z(r+s) + b_Z(2r-s)\}I_0(\sigma)I_0(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

From

$$\theta\tilde{Y}(\sigma^{r+s}\tau^{2s-r} - 1) + \theta\tilde{Z}(\sigma^{2r-s}\tau^{r+s} - 1) \equiv 0\,(\mathrm{mod}(m\mathbf{Z}[G_m])),$$

it follows that

$$a_Y(2s-r) + b_Y(r+s) + a_Z(r+s) + b_Z(2r-s) \equiv 0\,(\mathrm{mod}\ m). \tag{6.4}$$

Setting $(r, s) = (-1, 1)$ and $(r, s) = (2\lambda, \lambda)$, where $\lambda \in \mathbf{Z}$ is a solution of $3\lambda \equiv 1\,(\mathrm{mod}\ m)$, in (6.4), we obtain that

$$a_Y - b_Z \equiv 0\,(\mathrm{mod}\ m),\ b_Y + a_Z + b_Z \equiv 0\,(\mathrm{mod}\ m). \tag{6.5}$$

It is clear that (6.4) and (6.5) are equivalent.

By Lemma 5.1 again, we note that $\theta I_1(\sigma)I_3(\tau)$ and $\theta I_1(\tau)I_3(\sigma)$ are congruent to

$$I_0(\sigma)I_1(\tau) - 2I_0(\sigma)I_0(\tau) \quad \text{and} \quad I_0(\tau)I_1(\sigma) - 2I_0(\sigma)I_0(\tau) \text{ modulo } m\mathbf{Z}[G_m]$$

respectively. Let $\gamma_Z \in \mathbf{Z}$ be such that $\gamma_Z \equiv 2a_Z + 2b_Z + c_Z\ (\mathrm{mod}\ m)$. Then

$$\theta(\tilde{Z} - a_Z I_1(\sigma)I_3(\tau) - b_Z I_1(\tau)I_3(\sigma) - \gamma_Z I_1(\sigma)I_2(\tau)) \equiv 0\,(\mathrm{mod}(m\mathbf{Z}[G_m])).$$

By Corollary 5.5,

$$\tilde{Z} \equiv a_Z I_1(\sigma)I_3(\tau) + b_Z I_1(\tau)I_3(\sigma) + \gamma_Z I_1(\sigma)I_2(\tau)\,(\mathrm{mod}(m\mathbf{Z}[G_m] + \mathbf{J})).$$

Similarly, there is $\gamma_Y \in \mathbf{Z}$ such that

$$\tilde{Y} \equiv b_Z I_1(\sigma)I_3(\tau) - (a_Z + b_Z)I_1(\tau)I_3(\sigma) + \gamma_Y I_1(\sigma)I_2(\tau) (\mathrm{mod}(m\mathbf{Z}[G_m] + \mathbf{J})).$$

Since $\tilde{X} + \tilde{Y} + \tilde{Z} = 0$ (by assumption), $\tilde{X}$ is congruent modulo $m\mathbf{Z}[G_m]$ to

$$-(a_Z + b_Z)I_1(\sigma)I_3(\tau) + a_Z I_1(\tau)I_3(\sigma) - (\gamma_Y + \gamma_Z)I_1(\sigma)I_2(\tau).$$

Hence,

$$\alpha \equiv b_Z W - a_Z W\rho^2 + \gamma_Y V + \gamma_Z V(\rho + 1) (\mathrm{mod}(\mathbf{Z}[G_m, \rho] + \mathbf{JQ}[G_m, \rho])).$$

By the remarks at the beginning of this section,

$$\mathrm{End}(J_m) \cap \Phi(\mathbf{Z}[G_m, \rho]) = \Phi(\mathbf{Z}[G_m, \rho, W]).$$

This proves the first statement of Theorem D.

COROLLARY 6.1. *Let*

$$\Sigma = \Phi(\mathbf{Z}[G_m, \rho, W]) \quad \textit{and} \quad B = \Phi(\mathbf{Z}[G_m, \rho]).$$

Then the quotient group $Q = \Sigma/B$ *is a free* $\mathbf{Z}/m\mathbf{Z}$*-module of rank* 4.

Proof. We have shown that the following map is surjective

$$f: (\mathbf{Z}/m\mathbf{Z})^4 \to Q, \ (a, b, c, d) \to aw + bw\rho^2 + cv + dv\rho.$$

Let $a, b, c, d \in \mathbf{Z}$ be such that

$$aW + bW\rho^2 + cV + dV\rho \in \mathbf{Z}[G_m, \rho] + \mathbf{JQ}[G_m, \rho]. \tag{6.6}$$

By Corollary 5.9, we can collect terms in $\mathbf{Q}[G_m]$

$$-aI_1(\sigma)I_3(\tau) + b(I_1(\sigma)I_3(\tau) - I_1(\tau)I_3(\sigma)) - cI_1(\sigma)I_2(\tau) \in m\mathbf{Z}[G_m] + \mathbf{J}.$$

Multiplying throughout by $m\theta$, we get

$$(2a - 2b)I_0(\sigma)I_0(\tau) + (b - a)I_0(\sigma)I_1(\tau) - bI_0(\sigma)I_1(\tau) \in m\mathbf{Z}[G_m].$$

Comparing coefficients of τ and τ^2, we obtain $2a \equiv 2b \equiv c \ (\mathrm{mod}\ m)$. Looking at coefficients of σ and σ^2, $a \equiv 0 \ (\mathrm{mod}\ m)$.

Next we collect terms in $\mathbf{Q}[G_m]\rho$ in (6.6), and we use

$$a \equiv b \equiv c \ (\mathrm{mod}\ m),$$

to get

$$dI_1(\sigma)I_2(\tau) \in m\mathbf{Z}[G_m] + \mathbf{J}.$$

Multiplying by θ, we conclude that $d \equiv 0 \ (\mathrm{mod}\ m)$. □

We end this section by showing that, when m is odd,

$$\mathrm{End}(J_m) \cap \Phi(\mathbf{Z}[G_m, \iota]) = \Phi(\mathbf{Z}[G_m, \iota]).$$

Let X, $Y \in \mathbf{Q}[G_m]$ be such that $\Phi(X + Y_1) \in \mathrm{End}(J_m)$. Then, for all $r \in \mathbf{Z}$,

$$X\sigma^r - Y\tau^r \in \mathbf{Z}[G_m] + \mathbf{J}.$$

This is equivalent to

$$X - Y, (\sigma - \tau)X \in \mathbf{Z}[G_m] + \mathbf{J}. \tag{6.7}$$

Let M denote

$$\{Z \in \mathbf{Q}[G_m] \mid (\sigma - \tau)Z \in \mathbf{Z}[G_m] + \mathbf{J}\}.$$

We claim that

$$\mathbf{M} = \mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau).$$

Recall that

$$\Delta = \sum_{0 \leqslant r,s,r+s \leqslant m-2} \tau^r \sigma^{-s} \in \mathbf{Z}[G_m]$$

and $I_0(\sigma)$ generates the ideal $\mathbf{J} \cap \mathbf{Z}[G_m]$. Since m is odd by hypothesis, in the ring

$$\mathbf{Q}[G_m]/(I_0(\sigma), \sigma - \tau), I_0(\sigma\tau) = 0$$

and the equality

$$(1 - \sigma^{-1})\Delta = I_0(\tau) - \sigma I_0(\sigma\tau)$$

in $\mathbf{Z}[G_m]$ implies that $(1-\sigma^{-1})\Delta = 0$. Furthermore, $1-\sigma$ is a unit in $\mathbf{Q}[\sigma]/(I_0(\sigma))$ and so we have $\Delta \in (I_0(\sigma), \sigma-\tau)\mathbf{Q}[G_m]$. It then follows from

$$(I_0(\sigma))\mathbf{Q}[\sigma] \cap \mathbf{Z}[\sigma] = \mathbf{Z}.I_0(\sigma)$$

that

$$\Delta \in (I_0(\sigma), \sigma - \tau)\mathbf{Q}[G_m] \cap \mathbf{Z}[G_m] = (I_0(\sigma), \sigma - \tau)\mathbf{Z}[G_m].$$

In particular, the ring

$$R = \mathbf{Z}[G_m]/(\mathbf{J} \cap \mathbf{Z}[G_m], \sigma - \tau) = \mathbf{Z}[G_m]/(I_0(\sigma), \sigma - \tau) = \mathbf{Z}[\sigma]/(I_0(\sigma))$$

is a free $\mathbf{Z}$-module.

We define a homomorphism $\phi: M \to R$ as follows. Let $Z \in M$ be such that $(\sigma-\tau)Z = a+k$, where $a \in \mathbf{Z}[G_m]$ and $k \in \mathbf{J}$. We then define $\phi(Z) = a$. Clearly ϕ is well-defined and a homomorphism, and $\mathrm{Ker}(\phi)$ contains $\mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau)$. We wish to show that they are equal.

Let $Z \in \mathrm{Ker}(\phi)$. Write $(\sigma-\tau)Z = (\sigma-\tau)a + k$, for some $a \in \mathbf{Z}[G_m]$ and some $k \in \mathbf{J}$. Then $a = \phi(Z) = 0$ in R implies that $a = a_1 I_0(\sigma) + a_2(\sigma - \tau)$ for some a_1, $a_2 \in \mathbf{Z}[G_m]$. Then

$$(\sigma - \tau)(Z - a_2) = a_1 I_0(\sigma) + k.$$

To show that

$$Z \in \mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau)$$

is equivalent to showing that

$$Z - a_2 \in \mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau).$$

Hence, we can replace Z by $Z - a_2$, and assume that $(\sigma - \tau)Z \in \mathbf{J}$.

For $X \in \mathbf{Q}[G_m]$, let $\bar{X}$ be its image in $\mathbf{Q}[G_m]/\mathbf{J}$. Since $\mathbf{Q}[G_m]$ is a product of fields, it follows that

$$\mathrm{Ker}(\bar{\sigma} - \bar{\tau}) = (\mathrm{Ker}(\sigma - \tau) + \mathbf{J})/\mathbf{J}.$$

Therefore, $Z \in \mathrm{Ker}(\sigma - \tau) + \mathbf{J}$. Thus we have shown that the kernel of ϕ is $\mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau)$. So ϕ induces a monomorphism

$$M/(\mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau)) \to R$$

from a torsion $\mathbf{Z}$-module into a torsion-free $\mathbf{Z}$-module. This implies that $M = \mathbf{Z}[G_m] + \mathbf{J} + \mathrm{Ker}(\sigma - \tau)$, and our claim is established.

An easy calculation shows that

$$\mathrm{Ker}(\sigma - \tau) = (I_0(\sigma^{-1}\tau))\mathbf{Q}[G_m].$$

Thus

$$X + Y\iota = (X - Y) + Y(1 + \iota) \quad \text{with } Y \in \mathbf{Z}[G_m] + \mathbf{J} + (I_0(\sigma^{-1}\tau))\mathbf{Q}[G_m]$$

and

$$X - Y \in \mathbf{Z}[G_m] + \mathbf{J}.$$

By Lemma 1.6, $I_0(\sigma^{-1}\tau)(1 + \iota)$ is in $\mathrm{Ker}(\Phi)$. We conclude that

$$\Phi(X + Y\iota) \in \Phi(\mathbf{Z}[G_m, \iota]).$$

This completes the proof of Theorem D.

Acknowledgements

This paper is based on the author's Berkeley doctoral dissertation. The author wishes to thank his thesis advisor, Robert Coleman, for his encouragement and support. The author would also like to thank Hendrik Lenstra, Jr. for valuable discussions.

References

[1] G.W. Anderson, Torsion points on Fermat Jacobians, Roots of Circular Units and Relative Singular Homology, *Duke Math. Journal* 54, No. 2 (1978), 501—561.

[2] R. Coleman, Torsion Points on Abelian etale coverings of $\mathbf{P}^1 - \{0, 1, \infty\}$, *Transactions of the AMS* 311, No. 1 (1989), 185–208.
[3] R. Coleman, *Lecture notes on Cyclotomy*, Tokyo University (1977).
[4] G. Cornell and J.H. Silverman in *Arithmetic Geometry* (eds), Springer-Verlag, New York–Berlin (1986).
[5] W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. 1, John Wiley, New York (1981).
[6] P. Deligne, J.S. Milne, A. Ogus, K.-Y. Shih, *Hodge Cycles, Motives and Shimura Varieties*, Lecture Notes in Mathematics 900, Springer-Verlag, Berlin–Heidelberg–New York (1982).
[7] M.J. Greenberg and J.H. Harper, *Algebraic Topology, A First Course*, Math. Lecture Note Series, The Benjamin/Cummings Publishing Co., Mass. (1981).
[8] R. Greenberg, On the Jacobian variety of some algebraic curves, *Comp. Math.* 42 (1981), 345–359.
[9] B. Gross (with an appendix by D. Rohrlich), On the Periods of Abelian Integrals and a Formula of Chowla and Selberg, *Invent. Math.* 45 (1978), 193–211.
[10] 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.
[11] N. Koblitz and D. Rohrlich, Simple factors in the Jacobian of a Fermat curve, *Canadian J. Math.* 20 (1978), 1183–1205.
[12] S. Lang, *Introduction to Algebraic and Abelian Functions*, GTM 89 (2nd edn.), Springer-Verlag, New York–Berlin–Heidelberg.
[13] C.H. Lim, *The Jacobian of a Cyclic Quotient of a Fermat Curve*, Preprint (1990).
[14] D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford (1970).
[15] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Tokyo, Math. Soc. Japan (1961).
[16] T. Shioda, Some Observations on Jacobi Sums, *Advanced Studies in Pure Mathematics* 12, Galois Representations and Arithmetic Algebraic Geometry (1987), 119–135.