<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>The fitting ideal of $J_0(q)(F_{pn})$ over the Hecke algebra</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Ling, San</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Ling, S. (1994). The Fitting Ideal of $J_0(q)(F_{pn})$ over the Hecke Algebra. Journal of Algebra, 164(2), 563-575.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>1994</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/9861">http://hdl.handle.net/10220/9861</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 1994 Academic Press. This is the author created version of a work that has been peer reviewed and accepted for publication by Journal of Algebra, Academic Press. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<a href="http://dx.doi.org/10.1006/jabr.1994.1078">http://dx.doi.org/10.1006/jabr.1994.1078</a>].</td>
</tr>
</tbody>
</table>
The Fitting Ideal of $J_0(q)(\mathbb{F}_p)$ over the Hecke Algebra

SAN LING*

Department of Mathematics, National University of Singapore, Singapore 0511
Communicated by Walter Feit

1. INTRODUCTION

Let $q$ be a prime. Let $X_0(q)$ be the classical modular curve and let $J = J_0(q)$ be its Jacobian variety. The curve $X_0(q)$ is endowed with well known Hecke correspondences $T_n$ for all $n \geq 1$ ([8, Chap. 7]). The modular interpretation of $X_0(q)$ and the correspondence $T_n$ allows us to define these objects over $\mathbb{Q}$. Each correspondence $T_n$ of $X_0(q)$ also induces an endomorphism of $J_0(q)$ when $J_0(q)$ is regarded as (the connected component of) the Picard variety of $X_0(q)$. We denote these Hecke operators by $T_n$ again.

Let the Hecke algebra $\mathcal{T}$ be the subring of $\text{End}(J_{/\mathbb{Q}})$ generated by the Hecke operators. It is well known that $\mathcal{T}$ is a free $\mathbb{Z}$-module of finite rank. In fact, $\mathcal{T} = \text{End}(J_{/\mathbb{C}})$ ([4, II, Prop. 9.5]).

Let $p \neq q$ be another prime and consider $J_{/\mathbb{F}_p}$. Let $J(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-rational points on $J_{/\mathbb{F}_p}$ and let $\phi$ be the Frobenius endomorphism of $J_{/\mathbb{F}_p}$. Then $\phi$ induces a map $J(\mathbb{F}_p) \rightarrow J(\mathbb{F}_p)$. Considering the map $1 - \phi$ induces on $J(\overline{\mathbb{F}}_p)$ allows us to identify $\ker(1 - \phi)$ with $J(\mathbb{F}_p)$. In fact, we get the exact sequence of groups

$$0 \rightarrow J(\mathbb{F}_p) \rightarrow J(\overline{\mathbb{F}}_p) \rightarrow J(\overline{\mathbb{F}}_p) \rightarrow 0.$$  

Consequently, since $1 - \phi$ is a separable endomorphism, we have

$$\text{card}(J(\mathbb{F}_p)) = \text{card}(\ker(1 - \phi)) = \deg(1 - \phi) = P(1),$$

where $P(T) = \det_{\mathbb{Q}_l}(1 - \phi T) \in \mathbb{Q}_l[T]$ is the characteristic polynomial of $\phi$, for $l \neq p$ a prime ([5, Prop. 12.9]).

However, since

$$P(T) = N_{\mathcal{T} \otimes \mathbb{Q}_l / \mathbb{Q}_l}(\det_{\mathcal{T} \otimes \mathbb{Q}_l}(1 - \phi T))$$

* The author thanks Ken Ribet for an enlightening discussion.
and, from the Eichler–Shimura relation,
\[
\det_{T \otimes \mathbb{Q}_p}(1 - \phi) = 1 + p - T_p \in T.
\]
we have
\[
P(1) = N_{T/Z}(1 + p - T_p).
\]
In other words,
\[
\text{card}(J(F_p)) = N_{T/Z}(1 + p - T_p).
\]
From the fact
\[
\text{card}(T/(1 + p - T_p) T) = N_{T/Z}(1 + p - T_p),
\]
we deduce the equality of integers
\[
\text{card}(J(F_p)) = \text{card}(T/(1 + p - T_p) T).
\]

It is easy to verify that the group structures of $J(F_p)$ and $T/(1 + p - T_p) T$ are not necessarily identical. For example, if $q = 11$, then $J = J_0(11) \cong X_0(11)$ is an elliptic curve described by the Weierstrass equation
\[
y^2 + y = x^3 - x^2 - 10x - 20. \tag{1}
\]
In this case, we have that $T = Z$. If $p = 31$, the tables in [1] give $T_p = 7$, and hence $T/(1 + p - T_p) T = \mathbb{Z}/25\mathbb{Z}$ is cyclic. However, one verifies readily that, for example, the points $(1, 12)$ and $(0, 6)$ are points of order $5$ and generate distinct subgroups of $J_0(11)(F_{31})$. Therefore, $J_0(11)(F_{31}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is not cyclic.

The Fitting ideal (see Section 2 for definition) is a measure of the “size” of a module. It is therefore natural to ask whether $J(F_p)$ and $T/(1 + p - T_p) T$ have the same Fitting ideals over $T$. (That is, are both of the Fitting ideals equal to the ideal $(1 + p - T_p) T$?) In this paper, we answer this equation in the affirmative. In fact, we prove the following

**Theorem 1.** If $n \geq 1$ is an integer and $p \neq 2$ is an odd prime, we have
\[
F_\gamma(J(F_p)) = (1 - (\lambda_1^n + \lambda_2^n) + p^n) T,
\]
where $\lambda_1, \lambda_2 \in T \otimes_{\mathbb{Z}} \mathbb{C}$ satisfy $X^2 - T_p X + p = (X - \lambda_1)(X - \lambda_2)$.

**Note.** Clearly, $\lambda_1 + \lambda_2 = T_p \in T$ and $\lambda_1 \lambda_2 = p \in T$. Since
\[
\lambda_1^n + \lambda_2^n = (\lambda_1 + \lambda_2)(\lambda_1^{n-1} + \lambda_2^{n-1}) - \lambda_1 \lambda_2(\lambda_1^{n-2} + \lambda_2^{n-2})
\]
for \( n \geq 2 \), it follows by induction that
\[
\lambda_1^n + \lambda_2^n \in T \quad \text{for} \quad n \geq 1.
\]

The following is an immediate corollary of Theorem 1.

**Corollary 1.** For \( p \neq 2 \) an odd prime, we have the identities

(a) \( F_T(J(F_p)) = (1 + p - T_p) T \),

(b) \( F_T(J(F_{p^2})) = ((1 + p)^2 - T_{p^2}) T \).

From Theorem 1, we can also deduce the next corollary, which may be regarded as a generalisation of the fact that, given positive integers \( d \) and \( n \), \( \text{card}(J(F_{p^d})) \) divides \( \text{card}(J(F_{p^n})) \) when \( d \) divides \( n \).

**Corollary 2.** Given positive integers \( d \) and \( n \), and that \( d \) divides \( n \), \( J(F_{p^d}) \) is a \( T \)-submodule of \( J(F_{p^n}) \).

Moreover, we have the inclusion of ideals
\[
F_T(J(F_{p^d})) \subseteq F_T(J(F_{p^n})).
\]

**Proof.** The first assertion is clear.
For the second statement, suppose that \( n = dm \). Then
\[
1 - (\lambda_1^n + \lambda_2^n) + p^n = (1 - \lambda_1^d)(1 - \lambda_2^d)
\]
\[
= (1 - \lambda_1^d)(1 + \lambda_1^d + \cdots + \lambda_1^{dm-1})(1 - \lambda_2^d)
\]
\[
	imes (1 + \lambda_2^d + \cdots + \lambda_2^{dm-1})
\]
\[
= (1 - \lambda_1^d + \lambda_2^d + p^d) \left( \sum_{i=0}^{m-1} \lambda_1^d \right) \left( \sum_{j=0}^{m-1} \lambda_2^d \right)
\]
\[
= (1 - \lambda_1^d + \lambda_2^d + p^d) \left( \sum_{i,j=0}^{m-1} \lambda_1^d \lambda_2^d \right).
\]

When \( i = j \), we have \( \lambda_1^d \lambda_2^d = (\lambda_1 \lambda_2)^d = p^d \in T \).
When \( i \neq j \), say \( i = \min(i,j) \), then
\[
\lambda_1^d \lambda_2^d + \lambda_2^d \lambda_1^d = (\lambda_1 \lambda_2)^d \left( \lambda_1^{d(i-j)} + \lambda_2^{d(i-j)} \right) \in T.
\]
Therefore,
\[
(1 - (\lambda_1^n + \lambda_2^n) + p^n) T \subseteq (1 - (\lambda_1^d + \lambda_2^d) + p^d) T,
\]
i.e.,
\[
F_T(J(F_{p^d})) \subseteq F_T(J(F_{p^n})).
\]
2. Fitting Ideals

Let \( R \) be a commutative ring with 1. In this section, we define the notion of the Fitting ideal (or, in the terminology of [7], the 0th or initial Fitting invariant) of an \( R \)-module over \( R \) and describe some of its properties. For an \( R \)-homomorphism \( \alpha : R' \to R \), given by an \( s \times r \) matrix \( M \alpha \) with entries in \( R \), we determine the following

**Definition 1.** The Fitting ideal of \( \alpha \) over \( R \), denoted by \( F_R(\alpha) \), is

\[
F_R(\alpha) = \begin{cases} 
0 & \text{if } r < s, \\
\text{the } R \text{-ideal generated by the } s \times s \text{ minors of } M \alpha & \text{if } r \geq s.
\end{cases}
\]

If \( M \) is an \( R \)-module of finite representation, we have the exact sequence

\[
R' \xrightarrow{\alpha} R^s \longrightarrow M \longrightarrow 0
\]  

(2)

Since the Fitting ideal \( F_R(\alpha) \), for any \( \alpha : R' \to R \), is dependent only on the \( R \)-isomorphism class of coker \( \alpha \) ([7, Chap. III, Theorem 1]), we can define the Fitting ideal of \( M \) over \( R \), denoted by \( F_R(M) \), to be \( F_R(\alpha) \). In particular, if we have \( r = s \), then \( F_R(M) \) is simply the \( R \)-ideal generated by the determinant \( \det_R(\alpha) \) of \( \alpha \). If \( M = 0 \), then we have the trivial exact sequence

\[
R \xrightarrow{\text{id}} R \longrightarrow M \longrightarrow 0,
\]

and it follows that \( F_R(0) = R \). If \( M \) is a free \( R \)-module, then \( F_R(M) = 0 \).

If there is a surjective map \( M \to N \) of \( R \)-modules, then \( F_R(M) \subseteq F_R(N) \).

However, if \( N \) is an \( R \)-submodule of \( M \), it is not necessarily true that \( F_R(M) \subseteq F_R(N) \). An example is found in [2, VII.4, Exercise 10(g)].

Corollary 2 of Theorem 1 gives examples of \( M \) and \( N \subseteq M \) for which \( F_R(M) \subseteq F_R(N) \).

There is an intimate relationship between \( F_R(M) \) and the annihilator \( \text{Ann}_R(M) \) of \( M \). If \( M \) is of the finite presentation (2), then

\[
(\text{Ann}_R(M))^\perp \subseteq F_R(M) \subseteq \text{Ann}_R(M).
\]

In particular, if \( M \) can be generated by a single element, we have \( F_R(M) = \text{Ann}_R(M) \).

If the module \( M \) is finite, there is also a close connection between \( F_R(M) \) and the size of \( M \). For example, if

\[
R = \mathbb{Z} \quad \text{and} \quad M = \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},
\]

then we get the exact sequence

\[
\mathbb{Z}^r \xrightarrow{s} \mathbb{Z}^s \longrightarrow M \longrightarrow 0,
\]
where

\[
\text{Ma}(x) = \begin{pmatrix}
m_1 & 0 & 0 \\
0 & \ddots & 0 \\
0 & 0 & m_s
\end{pmatrix}.
\]

Hence,

\[
F_Z(M) = m_1 \cdots m_s \mathbb{Z} \quad \text{and} \quad \text{card}(M) = m_1 \cdots m_s.
\]

In fact, more generally, if \(m_1, \ldots, m_s\) are ideals of \(R\), and

\[
M = R/m_1 \oplus \cdots \oplus R/m_s,
\]

then

\[
F_R(M) = m_1 \cdots m_s.
\]

Finally, we state without proof a proposition that is of use later.

**Proposition 1** ([7, Chap. III, Theorem 3]). Let \(R\) and \(M\) be as in above. Let \(S\) be a multiplicatively closed subset of \(R\) not containing 0. Then we have

\[
F_R(M) R_S = F_{R_S}(M_S),
\]

where the right-hand side means the Fitting ideal of the \(R_S\)-module \(M_S\).

3. Proof of Theorem 1

Let \(V\) be an abelian variety over \(\overline{F}_p\) provided with an action of \(T\). Then, for any maximal ideal \(m\) of \(T\) of residue characteristic \(l\), we have

\[
V[m] \overset{\text{def}}{=} \bigcap_{x \in m} (\text{kernel of } x \text{ in } V) = \bigcap_{x \in m} (\text{kernel of } x \text{ in } V[l]).
\]

Let

\[
V_m = \lim_n V[m^n]
\]

and let \(Ta(V_m)\) be the Tate module \(\text{Hom}_{Z_l}(Q_l/Z_l, V_m)\). Then

\[
Ta(V_m) = \text{Hom}_{Z_l}(Q_l/Z_l, V_m) \\
\cong \lim_n \text{Hom}(Z/l^nZ, V_m) \\
\cong \lim_n V_m[I^n].
\]
Let

\[ T_m = \lim_{\to} T/m^n. \]

**Proposition 2.** Let \( V \) and \( W \) be abelian varieties provided with \( T \)-actions and let \( f \) be a separable isogeny \( f: V \to W \). Then, for every prime \( l \), we have the following exact sequence of \( T \otimes \mathbb{Z}_l \)-modules

\[
0 \rightarrow \text{Ta}(V_i) \overset{\text{Ta}(f)}{\rightarrow} \text{Ta}(W_i) \rightarrow (\ker f)_i \rightarrow 0,
\]

where \( \text{Ta}(V_i) \overset{\text{def}}{=} \lim_{\to} V[l^n] = \operatorname{Hom}_{\mathbb{Z}_l}(\mathbb{Q}_l/\mathbb{Z}_l, V_i) \) and similarly for \( \text{Ta}(W_i) \), and \((\ker f)_i\) denotes the \( l \)-primary part of \( \ker f \).

**Proof.** For every \( n \geq 0 \), consider the commutative diagram of \( T \)-modules

\[
\begin{array}{cccccc}
0 & \rightarrow & V[l^n] & \rightarrow & V & \rightarrow & 0 \\
& & \downarrow{f_n} & & \downarrow{f} & & \downarrow{f} \\
0 & \rightarrow & W[l^n] & \rightarrow & W & \rightarrow & 0,
\end{array}
\]

where \( f_n \) is the restriction of \( f \) to \( V[l^n] \).

Since \( f \) is surjective (It is an isogeny!) we obtain, by the Snake Lemma, the exact sequence

\[
0 \rightarrow (\ker f)[l^n] \rightarrow \ker f \overset{f_n}{\rightarrow} \ker f \rightarrow \ker f_n \rightarrow 0. \tag{3}
\]

Therefore,

\[
\ker f_n = \ker f/l^n \ker f. \tag{4}
\]

For each integer \( m \) such that \( m \geq n \geq 0 \), we deduce, from (3) and (4), a commutative diagram

\[
\begin{array}{cccccc}
0 & \rightarrow & (\ker f)[l^n] & \rightarrow & V[l^n] & \overset{f_n}{\rightarrow} & W[l^n] & \rightarrow & \ker f/l^n \ker f & \rightarrow & 0 \\
& & & & \downarrow{l^m} & & \downarrow{l^m} & & \downarrow{l^m} & & \downarrow{l^m} & & \downarrow{l^m} \\
0 & \rightarrow & (\ker f)[l^m] & \rightarrow & V[l^m] & \overset{f_m}{\rightarrow} & W[l^m] & \rightarrow & \ker f/l^m \ker f & \rightarrow & 0. \tag{5}
\end{array}
\]

The inverse system \((V[l^n]/(\ker f)[l^n], l^m-l^n)\) satisfies the Mittag-Leffler condition (cf. [3, p.191]). Upon taking inverse limits, (5) gives us the exact sequence of \( T \otimes \mathbb{Z}_l \)-modules:

\[
0 \rightarrow \text{Ta}(V_i) \overset{\text{Ta}(f)}{\rightarrow} \text{Ta}(W_i) \rightarrow (\ker f)_i \rightarrow 0. \]
Corollary 3. For every prime $l$, we have the exact sequence of $T \otimes \mathbb{Z}_l$-modules

$$0 \longrightarrow \mathcal{T}_l(J_{l/F}) \longrightarrow \mathcal{T}_l(J_{l/F}) \longrightarrow J(F_{p^r})_l \longrightarrow 0. \quad (6)$$

For any maximal ideal $m \subseteq T$ of residue characteristic $l$, the sequence of $T_m$-modules

$$0 \longrightarrow \mathcal{T}_m(J_{m}) \longrightarrow \mathcal{T}_m(J_{m}) \longrightarrow J(F_{p^r})_m \longrightarrow 0 \quad (7)$$

is also exact, where $J_m = \varprojlim_n J[m^n]$, and $J(F_{p^r})_m = J(F_{p^r}) \otimes T_m$.

Proof. The exact sequence (6) follows immediately from Proposition 2 by using $V = W = J_{l/F}$ and $f = 1 - \phi''$. The kernel of $1 - \phi''$ is $J(F_{p^r})$.

The equality $T \otimes \mathbb{Z}_l = \prod_{m|l} T_m$, where the product is taken over all maximal ideals $m \subseteq T$ containing $l$, gives rise to the decompositions $\mathcal{T}_l(J_{l/F}) = \prod_{m|l} \mathcal{T}_m(J_{m})$ and $J(F_{p^r})_l = \prod_{m|l} J(F_{p^r})_m$. The exact sequence (7) then follows immediately from these decompositions and (6).

From Proposition 1, we deduce the following

Proposition 3. We have the equalities

(a) $F_T(J(F_{p^r})) \otimes \mathbb{Z}_l = F_T \otimes \mathbb{Z}_l(J(F_{p^r})_l)$;

(b) $F_T(J(F_{p^r})_m) = F_T(J(F_{p^r})) \otimes T_m = F_T \otimes \mathbb{Z}_l(J(F_{p^r})_l) \otimes T_m$.

We next state a theorem that is an important ingredient in our proof of Theorem 1. We defer the proof of Theorem 2 until the next section. Before stating the theorem, we first define the notions of supersingular and ordinary maximal ideals in $T$, as well as those of the Eisenstein ideal and Eisenstein primes in $T$.

Definition 2. A maximal ideal $m$ of $T$ of residue characteristic $l$ is supersingular if the $l$th Hecke operator $T_l$ belongs to $m$. If $T_l \notin m$, we say that $m$ is ordinary.

Definition 3. The Eisenstein ideal $\mathfrak{E} \subseteq T$ is the ideal generated by the elements $1 + l - T_l$ (where $l \neq q$ is a prime) and by $1 - T_q$.

Definition 4. A prime ideal $\mathfrak{p} \subseteq T$ in the support of the Eisenstein ideal is called an Eisenstein prime.
Theorem 2. Let \( m \) be a maximal ideal in \( T \) of residue characteristic 1. Suppose that \( m \) is not an ordinary non-Eisenstein prime of residue characteristic 2. Then \( \text{Ta}(J_{m}) \) is free over \( T_{m} \) of rank
\[
\begin{align*}
2 & \quad \text{if } l \neq p, \\
1 & \quad \text{if } l = p, \text{ } m \text{ is ordinary,} \\
0 & \quad \text{if } l = p, \text{ } m \text{ is supersingular.}
\end{align*}
\]

Proposition 4. For all primes \( l \), we have
\[
F_{T \otimes Z_{l}}(J(F_{p^{n}})) = (1 - (\lambda_{1}^{n} + \lambda_{2}^{n}) + p^{n})(T \otimes Z_{l}),
\]
where \( \lambda_{1}, \lambda_{2} \) are the eigenvalues of the Frobenius \( \phi \), acting on \( \text{Ta}(J_{l}) \).

Proof. Case I: If \( l \neq p \). Corollary 3 says that we have an exact sequence of \( T \otimes Z_{l} \)-modules
\[
0 \rightarrow \text{Ta}(J_{l}) \xrightarrow{\text{Ta}(1 - \phi^{n})} \text{Ta}(J_{l}) \rightarrow J(F_{p^{n}})_{l} \rightarrow 0,
\]
and since \( \text{Ta}(J_{l}) \) is a free \( T \otimes Z_{l} \)-module, we have
\[
F_{T \otimes Z_{l}}(J(F_{p^{n}})) = (\det \text{Ta}(1 - \phi^{n}))(T \otimes Z_{l}) = (1 - (\lambda_{1}^{n} + \lambda_{2}^{n}) + p^{n})(T \otimes Z_{l}).
\]

Case II: If \( l = p \) and \( T_{p} \in m \) (supersingular case). From the above theorem, we have \( \text{Ta}(J_{m}) = 0 \). Therefore, by (7) in Corollary 3, we have \( J(F_{p^{n}})_{m} = 0 \).

From the definition of Fitting ideals, \( F_{T_{m}}(J(F_{p^{n}})_{m}) = T_{m} \). Since \( \lambda_{1} + \lambda_{2} = T_{p} \in m \) and \( \lambda_{1} \lambda_{2} = p \in m \), it follows by induction that \( \lambda_{1} + \lambda_{2} = (\lambda_{1} + \lambda_{2})(\lambda_{1}^{n-1} + \lambda_{2}^{n-1} - \lambda_{1} \lambda_{2} + 2 \lambda_{1}^{n-2} + 2 \lambda_{2}^{n-2}) \in m \). This implies that \( 1 - (\lambda_{1}^{n} + \lambda_{2}^{n}) + p^{n} \) is a unit in \( T_{m} \). Hence,
\[
F_{T_{m}}(J(F_{p^{n}})) = T_{m} = (1 - (\lambda_{1}^{n} + \lambda_{2}^{n}) + p^{n}) T_{m}
\]
whenever \( m \mid p \) and \( m \) is supersingular.

Case III: If \( l = p \) and \( T_{p} \notin m \) (ordinary case). By Theorem 2, \( \text{Ta}(J_{m}) \cong T_{m} \). The endomorphism \( \phi \) acts as a "unit" root \( \lambda_{1} \) in \( T_{m}^{*} \) and we have
\[
0 = \phi^{2} - T_{p} \phi + p = (\phi - \lambda_{1})(\phi - \lambda_{2}).
\]
The fact that \( \lambda_{1} \lambda_{2} = p \in mT_{m} \) implies that \( \lambda_{2} \in mT_{m} \) and \( 1 - \lambda_{2}^{n} \) is a unit in \( T_{m} \). It then follows that
\[
(1 - (\lambda_{1}^{n} + \lambda_{2}^{n}) + p^{n}) T_{m} = (1 - \lambda_{1}^{n})(1 - \lambda_{2}^{n}) T_{m} = (1 - \lambda_{1}^{n}) T_{m}.
\]
Hence,

\[ F_{\text{T}_m}(J(F_{\rho,p}))_{\text{T}_m} = \det(1 - \phi^n) \text{T}_m = (1 - \lambda_1^n) \text{T}_m = (1 - (\lambda_1^n + \lambda_2^n) + p^n) \text{T}_m. \]

Putting Cases II and III together, we obtain, if \( p = l \),

\[ F_{\text{T} \otimes Z_l}(J(F_{\rho,p})) = (1 - (\lambda_1^n + \lambda_2^n) + p^n)(\text{T} \otimes \text{Z}_l) \]

since \( \text{T} \otimes \text{Z}_l = \prod_{m \mid l} \text{T}_m \).

From Propositions 3(a) and 4, we have

**Corollary 4.** If \( p \neq 2 \), then, for all primes \( l \),

\[ F_{\text{T}}(J(F_{\rho,p})) \otimes \text{Z}_l = (1 - (\lambda_1^n + \lambda_2^n) + p^n)(\text{T} \otimes \text{Z}_l). \]

Now we are ready to prove the main theorem, which we restate.

**Theorem 1.** If \( n \geq 1 \) is an integer and \( p \neq 2 \) is an odd prime, we have

\[ F_{\text{T}}(J(F_{\rho,p})) = (1 - (\lambda_1^n + \lambda_2^n) + p^n) \text{T}, \]

where \( \lambda_1, \lambda_2 \in \text{T} \otimes \text{Z}_C \) satisfy \( X^2 - T_p X + p = (X - \lambda_1)(X - \lambda_2) \).

**Proof.** First, we prove a lemma:

**Lemma 1.** Let \( L, M, N \) be \( \text{Z} \)-lattices and, for every prime \( l \), let \( L_l \) denote \( L \otimes \text{Z}_l \) (and similarly for \( M_l \) and \( N_l \)). If \( L \subseteq N, M \subseteq N, \) and \( L_l = M_l \subseteq N_l \) for all primes \( l \), then \( L = M \).

**Proof of Lemma 1.** Let \( X = L + M \). Then \( L \subseteq X \subseteq N \) and \( L \otimes \text{Z}_l = X \otimes \text{Z}_l \). The sequence

\[ 0 \longrightarrow L \overset{\text{id}}{\longrightarrow} X \longrightarrow X/L \longrightarrow 0 \]

is exact. Tensoring with \( \text{Z}_l \), we get an exact sequence of \( \text{Z}_l \)-modules

\[ 0 \longrightarrow L \otimes \text{Z}_l \overset{\text{id} \otimes 1}{\longrightarrow} X \otimes \text{Z}_l \longrightarrow (X/L) \otimes \text{Z}_l \longrightarrow 0. \]

However, \( L \otimes \text{Z}_l = X \otimes \text{Z}_l \) for all \( l \) implies \( (X/L) \otimes \text{Z}_l = 0 \) for all primes \( l \). Therefore, \( X/L = 0 \); i.e., \( L = X = L + M \). Consequently, we have the inclusion \( M \subseteq L \). Symmetry of the argument implies that \( L = M \).

To complete the proof of Theorem 1, simply take \( L = F_{\text{T}}(J(F_{\rho,p})), M = (1 - (\lambda_1^n + \lambda_2^n) + p^n) \text{T} \) and \( N = \text{T} \).
4. Freeness of $\text{Ta}(J_m(\bar{F}_p))$

In this section, as promised earlier, we prove Theorem 2 which was stated in the last section.

From [4, II §§15.1, 15.2, 16.3, and 17.9], we see that $\text{Ta}(J_m(\bar{Q}))$ is free over $T_m$ of rank 2 and that $T_m$ is Gorenstein ([4, II §15]) under each of the following hypotheses:

1. $m$ not Eisenstein, char $T/m \neq 2$ (15.2);
2. $m$ not Eisenstein, char $T/m = 2$, $m$ supersingular (15.2);
3. $m$ Eisenstein (16.3, 17.9).

We prove Theorem 2 in the three cases in the statement of the theorem.

Case I: $m \nmid p$; i.e., char $T/m = l \neq p$. In this case,

$$J[m]_{\bar{F}_p} = \bigcap_{\alpha \in m} (\ker \text{ of } \alpha \text{ in } J_{[l], \bar{F}_p}) = \bigcap_{\alpha \in m} (\ker \text{ of } \alpha \text{ in } J[l], \bar{Q}) = J[m], \bar{Q},$$

Therefore, $\text{Ta}(J_m(\bar{F}_p)) \simeq \text{Ta}(J_m(\bar{Q}))$, and hence is free of rank 2 over $T_m$.

Case II: $m | p$, $m$ supersingular; i.e., $l = p$, $T_p \in m$. In this case, $J[m](\bar{F}_p)$ admits a Jordan–Hölder filtration whose constituents are all isomorphic to the group scheme $\alpha_p$ ([4, II §14]). In other words, the $p$-rank of $J_m(\bar{F}_p)$ is 0 ([6, p. 147]). It follows that ([6, p. 171]) $\text{Ta}(J_m(\bar{F}_p)) = 0$, i.e., $\text{Ta}(J_m(\bar{F}_p))$ is free over $T_m$ of rank 0.

Case III: $m \mid p$, $m$ ordinary; i.e., $l = p$, $T_p \notin m$. We proceed by using the proposition below:

**Proposition 5.** Let $M$ be a finitely generated module over $T_m$. Then $M$ is free of rank 1 over $T_m$ if and only if

1. $M \otimes \bar{Q}_p$ is free of rank 1 over $T_m \otimes \bar{Q}_p$, and
2. $M/mM$, as a $T/m$-module, is free of rank 1.

**Proof of Proposition 5.** ($\Rightarrow$) This direction is clear.

($\Leftarrow$) Nakayama’s lemma and Condition 2 imply that $M$ is generated over $T_m$ by an element $x$, i.e., $M = T_m x$. Let $g: T_m \rightarrow M$ be the map $g(\tau) = \tau x$, and let $H$ be the kernel of $g$. Then we have an exact sequence

$$0 \rightarrow H \rightarrow T_m \xrightarrow{g} M \rightarrow 0.$$
We can consider these as $\mathbb{Z}_p$-modules, and since $\mathbb{Q}_p$ is $\mathbb{Z}_p$-flat, the sequence of $\mathbb{Q}_p$-modules

$$0 \longrightarrow H \otimes \mathbb{Q}_p \longrightarrow T_m \otimes \mathbb{Q}_p \overset{\cdot \otimes 1}{\longrightarrow} M \otimes \mathbb{Q}_p \longrightarrow 0$$

is exact. By Condition 1, $H \otimes \mathbb{Q}_p = 0$. Since $T \cong T'$, we have $T \otimes \mathbb{Z}_p \cong T'$ and $H \subseteq T_m \subseteq T \otimes \mathbb{Z}_p \cong T'$. In particular, $H$ is $\mathbb{Z}_p$-torsion free. Therefore, $H$ can be embedded in $H \otimes \mathbb{Q}_p$ and hence $H = 0$. In other words, $M \cong T_m$, i.e., $M$ is free over $T_m$ of rank 1. This proves Proposition 5.

**Proposition 6.** Let $m \subseteq T$ be an ordinary maximal ideal of residue characteristic $p$, with the additional condition that $m$ be Eisenstein when $p = 2$. Then the $\mathbb{Z}_p$-dual of $\text{Ta}(J_m(\overline{F}_p))$ is free of rank 1 over $T_m$.

**Proof.** Let $M$ be $\text{Ta}(J_m(\overline{F}_p))$ and let $M^* = \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ be the $\mathbb{Z}_p$-dual of $\text{Ta}(J_m(\overline{F}_p))$.

By [4, II Prop. 8.5] (see also the proof of Cor. 14.11), $M^*$ and $M$ are both of rank 1 over $T_m$; i.e., $M^* \otimes \mathbb{Q}_p$ and $M \otimes \mathbb{Q}_p$ are both free of rank 1 over $T_m \otimes \mathbb{Q}_p$. Hence, Condition 1 of Proposition 5 is satisfied by $M$ and $M^*$.

We now show that Condition 2 is satisfied by $M^*/mM^*$.

**Lemma 2.** We have the isomorphism of $T/m$-modules

$$M^*/mM^* \cong \text{Hom}_{\mathbb{Z}_p}(J(\overline{F}_p)[m], \mathbb{Q}_p/\mathbb{Z}_p),$$

where $M^* = \text{Hom}_{\mathbb{Z}_p}(\text{Ta}(J_m(\overline{F}_p)), \mathbb{Z}_p)$.

(For the proof, see later.)

The module on the right-hand side of (8) is free of rank 1 over $T/m$ for $p > 2$ ([4, II Cor. 14.8]). Therefore, by Proposition 5, $M^*$ is free of rank 1 over $T_m$ for $p > 2$.

Now, let $p = 2$. We are then in the case where $m$ is Eisenstein. In this case, [4, II Cor. 14.11] implies that $M^*$ is free of rank 1 over $T_m$.

It remains, therefore, to prove Lemma 2.

Let $N$ be a $\mathbb{Z}_p$-module with $T_m$-action, of the type $F \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^n$, where $F$ is a finite abelian group and $n$ a non-negative integer. Let $N^* = \text{Hom}_{\mathbb{Z}_p}(N, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontrjagin $p$-dual of $N$.

**Lemma 3.** There is an isomorphism of $\mathbb{Z}_p$-modules $N \cong N^{**}$. The $T_m$-action on these modules is also preserved under the isomorphism.

**Proof.** Since $\text{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Z}_p$ and $\text{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Q}_p/\mathbb{Z}_p$, we have the isomorphism $N \cong N^{**}$ if $N = (\mathbb{Q}_p/\mathbb{Z}_p)^n$, for $n$ a
non-negative integer. For finite groups $F$, the isomorphism $F \cong F^{\vee}$ is well known. Hence, we obtain the isomorphism of $\mathbb{Z}_p$-modules $N \cong N^{\vee}$, where $N = F \oplus \left( \mathbb{Q}_p / \mathbb{Z}_p \right)^n$.

If $t \in T_m, f \in N^{\vee}$, and $j \in N$ (with corresponding element $j^* \in N^{\vee}$), then $t$ acts on $N^{\vee}$ by $(tf)(j) = f(tj)$. Consequently,

$$ (tj^*)(f) = j^*(tf) = (tf)(j) = f(tj) = (tj^*)(f). $$

(9)

Therefore, the $T_m$-action is preserved.

Now we prove Lemma 2.

Proof of Lemma 2. Let $N$ be $J_m(F_p)$. Then $N^{\vee} = M^*$ by [4, II §7, p.92]. From Lemma 3, we have the duality $N \cong N^{\vee}$. This duality gives rise to a one-to-one correspondence between the $T_m$-submodules $P$ of $M^*$ and the $T_m$-submodules $Q$ of $J_m(F_p)$. Indeed, given $Q \subseteq J_m(F_p)$, we get a quotient $Q^\vee$ of $N^{\vee} = M^*$. Since $Q_p / \mathbb{Z}_p$ is injective, there exists a submodule $P \subseteq M^*$ such that $M^*/P \cong Q^\vee$. Conversely, given $P \subseteq M^*$, $Q \overset{\text{def}}{=} \text{Hom}_{\mathbb{Z}_p}(M^*/P, Q_p / \mathbb{Z}_p)$ injects into $\text{Hom}_{\mathbb{Z}_p}(M^*, Q_p / \mathbb{Z}_p) = N^{\vee} \cong N$. These two directions are clearly inverse to each other. Now,

$$ mM^* \subseteq P \quad \iff \quad m \text{ annihilates } M^*/P $$

$$ \iff \quad m \text{ annihilates } \text{Hom}_{\mathbb{Z}_p}(Q, Q_p / \mathbb{Z}_p) $$

$$ \iff \quad mQ = 0 $$

$$ \iff \quad Q \subseteq J(F_p)[m]. $$

It follows then that $P = mM^*$ corresponds to $Q = J_m(F_p)[m]$ in the above correspondence, and hence

$$ M^* / mM^* \cong \text{Hom}_{\mathbb{Z}_p}(J(F_p)[m], Q_p / \mathbb{Z}_p). $$

Proposition 7 below implies that $M = \text{Ta}(J_m(F_p))$ is free of rank 1 over $T_m$ in Case III.

**Proposition 7.** Let $m \subseteq T$ be a maximal ideal of residue characteristic $p$ and let $M$ be $\text{Ta}(J_m(F_p))$. Suppose that $M^* = \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ is free of rank 1 over $T_m$. Then $M$ is also free of rank 1 over $T_m$.

**Proof.** As $J_m(F_p) \subseteq J_m(F_p)$, and $\text{Ta}(J_m(F_p))$ is a free $\mathbb{Z}_p$-module, we see that $M = \text{Ta}(Z_m(F_p))$ is also a free $\mathbb{Z}_p$-module. If the $\mathbb{Z}_p$-rank of $M$ is $s$, then $M \cong \mathbb{Z}_p^s$. Since $\text{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p^s, \mathbb{Z}_p) \cong \mathbb{Z}_p^s$, it follows that $M \cong (M^*)^*$ as $\mathbb{Z}_p$-modules. An argument parallel to the one used in (9) shows that
$M \simeq (M^*)^*$ as $T_m$-modules. Consequently, we have isomorphisms of $T_m$-modules

$$M \simeq \text{Hom}_{Z_p}(M^*, Z_p) \simeq \text{Hom}_{Z_p}(T_m, Z_p) \simeq T_m,$$

where the last isomorphism follows from the fact that $T_m$ is Gorenstein. This shows that $M$ is free of rank 1 over $T_m$. 

The proof of Theorem 2 is now complete.

REFERENCES