REDUCTION OF MODULAR JACOBIANS AT THE BAD PRIME

SREEKAR M. SHAISTRY

Abstract. The goal of these notes is to show that $\mathcal{P} \otimes \mathbb{F}_p$ is a torus and to describe the action of Frobenius on it, where $\beta$ is the Néron model over $\mathbb{Z}$ of the modular Jacobian $J_0(p)_{\mathbb{Q}}$. 

1. Integral Models of Modular Curves

1.1 Let $M_0(N)_{\mathbb{Z}[1/N]}$ be the “compactified coarse moduli scheme” associated to the problem of classifying pairs $(E,C)$ where $E$ is an elliptic curve over a $\mathbb{Z}[1/N]$-scheme and $C$ is a cyclic étale subgroup scheme of order $N$. It is a smooth proper curve over $\mathbb{Z}[1/N]$ with geometrically connected fibers. One knows that $M_0(1) \cong \mathbb{P}^1_{\mathbb{Z}}$ is “the j-line.” There is a natural map $M_0(N)_{\mathbb{Z}[1/N]} \to M_0(1)_{\mathbb{Z}[1/N]}$ gotten by forgetting the cyclic subgroup. We define $M_0(N)_{\mathbb{Z}}$ to be the normalization of $M_0(1)$ in $M_0(N)_{\mathbb{Z}[1/N]}$. Now we define $X_0(N)$ to be the minimal regular proper model of $M_0(N)$ over $\mathbb{Z}$—it is the unique scheme which is regular, proper, and flat over $\mathbb{Z}$ with generic fiber $M_0(N)_{\mathbb{Q}}$, such that for any other regular and proper scheme $\mathcal{C}$ flat over $\mathbb{Z}$ with generic fiber $M_0(N)_{\mathbb{Q}}$, the birational map $\mathcal{C} \to X_0(N)$ is a morphism; cf. [4]. See Figure 1. We will not need $X_0(N)$ in the sequel.

Henceforth we take $N$ to be a prime number $p$. We have the following description of $M_0(p)$:

1.2 Theorem. (a) $M_0(p)$ is smooth over $\mathbb{Z}$ away from the supersingular points in characteristic $p$.

(b) $M_0(p)_{\mathbb{F}_p}$ is the union of two copies of $M_0(1)_{\mathbb{F}_p} = \mathbb{P}^1_{\mathbb{F}_p}$ crossing transversally at the supersingular points. Hence $M_0(p)$ has semi-stable reduction at $p$.

(c) Let $x = j(E)$ be a supersingular point in $M_0(1)_{\mathbb{F}_p}$. Then $x$ on the first copy of $M_0(1)_{\mathbb{F}_p}$ is glued to $x^p$ on the second copy. In fact, if we let $w$ be the involution $(E,C) \mapsto (E/C, C[p]/C)$, $\Phi : M_0(1) \to M_0(p)$ be $E \mapsto (E, \ker(F : E \to E^p))$, and $c$ be the contraction map $(E,C) \mapsto c(E)$ that forgets $C$ and contracts into nodal cubics ($\neq 1$-gons) those geometric fibers of $E$ which are $n$-gons ($n > 1$), we have

\[
\begin{array}{ccc}
M_0(1)_{\mathbb{F}_p} & \Phi & M_0(1)_{\mathbb{F}_p} \\
\downarrow \quad \downarrow & \quad \downarrow & \quad \downarrow \\
M_0(p)_{\mathbb{F}_p} & \quad w\Phi & \quad M_0(p)_{\mathbb{F}_p} \\
\leftarrow \quad \downarrow c & \quad \downarrow \quad \downarrow c w & \quad \rightarrow \\
M_0(1)_{\mathbb{F}_p} & \quad M_0(1)_{\mathbb{F}_p} & \\
\end{array}
\]

with $\Phi$ and $w\Phi$ closed immersions whose images are the two irreducible components of $M_0(p)_{\mathbb{F}_p}$. 

1
(d) Let $x = j(E) \in M_0(p)(\overline{\mathbb{F}}_p)$ be a supersingular point (in fact all such are rational over $\mathbb{F}_{p^2}$; see [9], 12.5.4), and put $k := \frac{1}{2} \# \text{Aut} E$. Then $X_0(p)_{\mathbb{F}_p}$ is obtained by gluing copies of $M_0(1)_{\mathbb{F}_p}$ at corresponding supersingular points as above, and then replacing a crossing by $k - 1$ projective lines.

(e) The arithmetic genus of $M_0(p)_{\mathbb{F}_p}$ is

$$\# \{\text{supersingular } x \in M_0(1)(\overline{\mathbb{F}}_p)\} - 1.$$ 

See [5], pp. 144–148.

2. Review of the relative Picard functor

2.1 Fix $\pi : X \longrightarrow S$. Let

$$\text{Pic}_{X/S} := R^1\pi_*\mathcal{O}_X$$

with respect to the fppf topology on $S$. It is the sheafification of the functor $P_{X/S}$ which associates to an $S$-scheme $T$ the group $H^1(T, \mathcal{O}_X^\times)$. More concretely, if $\pi : X \longrightarrow S$ is proper, flat, finitely presented, has geometrically connected fibers, and we are given a section $\varepsilon : S \longrightarrow X$ then $\text{Pic}_{X/S}(T)$ is the set of isomorphism classes of pairs $(\mathcal{L}, \lambda)$ such that $\mathcal{L}$ is an invertible sheaf on $X_T$ and $\lambda : \mathcal{O}_T \longrightarrow (\varepsilon \times \text{id}_T)^*\mathcal{L}$ is an isomorphism; $\lambda$ is called a rigidification. The rigidification has the effects of killing invertible sheaves coming from $T$ and eliminating automorphisms. It turns out that the set of isomorphism classes of such pairs $(\mathcal{L}, \lambda)$ is then equal to $\text{Pic}(X_T)/\text{Pic}(T)$. See [3], p. 204.
2.2 By 2.4(b) below, if $X$ is a proper scheme over a field $k$ then $\text{Pic}_X/k$ is represented by a countable disjoint union of quasi-projective $k$-schemes; the identity component of this $k$-group is denoted $\text{Pic}^0_X/k$. It is geometrically connected.

For a general base $S$, we define the relative identity component $\text{Pic}^0_{X/S} \subset \text{Pic}_X/S$ to be the subfunctor whose $T$-points are those $\xi \in \text{Pic}_X/S(T)$ such that for all $s \in S$ and all geometric points $t \to T$ whose image is $s$, $\xi_s \in \text{Pic}^0_{X_s/k(s)}(k(t))$.

If $S$ is a proper and flat curve over a field $k$, then $\text{Pic}^0_{X/k}$ consists of all elements of $\text{Pic}_{X/k}$ whose restriction to every irreducible component of $X \otimes k$ has degree zero. See [EGA IV$_3$ 15.6.5].

The preceding is a variant of a general definition of identity components for a smooth $S$-group scheme $G$: $G^0$ is defined to be the open subscheme $\bigcup_{s \in S} G^0_s$. See [EGA IV$_3$ 15.6.5].

Before proceeding, let's give the

2.3 DEFINITION. A semi-stable curve of genus $g$ over $S$ is a proper, flat, and finitely presented morphism $f : X \longrightarrow S$ such that

(i) The fibres $X_s$ over geometric points $s$ of $S$ are reduced, connected, and one-dimensional,

(ii) $X_s$ has only ordinary double points as singularities, and

(iii) $h^1(X_s, \mathcal{O}_{X_s}) = g$.

The importance of such curves in the theory of moduli is due to the "semi-stable reduction theorem" which we will not state here. See the article by Abbes in [1] for a relatively accessible treatment.

2.4 Concerning the representability of $\text{Pic}_X/S$ we state only what we'll need later on as

THEOREM. (a) If $f : X \longrightarrow S$ is a smooth projective curve with geometrically connected fibers, then $\text{Pic}_X/S$ is represented by a separated scheme, and moreover $\text{Pic}^0_{X/S}$ is an abelian scheme.

(b) If $X$ is proper over a field $k$ then $\text{Pic}_{X/k}$ is represented by a countable disjoint union of quasi-projective $k$-schemes. If $X$ is a proper curve over $k$, then $\text{Pic}^0_{X/k}$ is a smooth $k$-group scheme.

(c) If $X$ is a semi-stable curve over $S$ then $\text{Pic}^0_{X/S}$ is represented by a smooth and separated $S$-scheme which is, moreover, semi-abelian (i.e. all of its fibers are extensions of affine tori by abelian varieties).

(d) If $p > 3$ is a prime then $\text{Pic}^0_{\text{Mod}(p)/\mathbb{Z}}$ is represented by a smooth and separated group scheme over $\mathbb{Z}$.

These are special cases of results due to Grothendieck, Murre--Oort, Deligne, and Raynaud, respectively. See [3], p. 210, p. 211, p. 232, p. 259, p. 288. For (d), also see [12]. In 4.2, we will prove the semi-abelian assertion of (c) as we will need the finer information that the proof provides.

2.5 REMARK. When $X$ is a proper curve over a field $k$, so that $\text{Pic}^0_{X/S}$ is represented by a smooth group scheme, it will also be called the Jacobian of $X$.

2.6 Finally, let's recall Weil's restriction of scalars functor. Let $f : T \longrightarrow S$ be a morphism of schemes. For a $T$-scheme $X$, we define $f_* X = \text{Res}_{T/S} X$ to be the functor on $S$-schemes

$$U \mapsto X(U \times_S T).$$
A suitable adjunction formula tells us that there is a natural morphism of functors

$$X \longrightarrow \text{Res}_{T/S}(X_T).$$

We pass over in silence all questions concerning representability. See [3], Ch. 7, §6. However, let’s mention that if $k'/k$ is a finite Galois extension of fields then for a $k'$-scheme $X$, $\text{Res}_{k'/k}X$ is the Galois descent of the $k'$-scheme

$$\prod_{\sigma \in \text{Gal}(k'/k)} X \otimes_{k} k',$$

with respect to the evident descent data.

3. **Comparison of the Picard Scheme of $M_0(p)$ and the Néron Model of the Jacobian $J_0(p)_\mathbb{Q}$**

3.1 Fix the following notations:

- $p > 3$ a prime number
- $J_0(p)_\mathbb{Q}$ the Jacobian of $M_0(p)_\mathbb{Q}$
- $P := \text{Pic}^0(M_0(p)/\mathbb{Z})$
- $P^0 := \text{Pic}^0(M_0(p)/\mathbb{Z})$
- $\mathcal{J}$ the Néron model over $\mathbb{Z}$ of $J_0(p)_\mathbb{Q}$
- $\mathcal{J}^0$ its identity component.

The Néron mapping property gives us a unique morphism $c : P^0 \longrightarrow \mathcal{J}^0$ which extends the identity map on generic fibers. The following theorem reduces the study of $P^0_{\mathbb{F}_p}$ to the study of $\mathcal{J}^0_{\mathbb{F}_p}$.

3.2 Theorem. *The map $c$ is an isomorphism.*

Proof. The statement is obvious over $\mathbb{Z}[1/p]$ as $M_0(p)$ is a smooth proper curve over $\mathbb{Z}[1/p]$. Hence, by “chasing denominators” [EGA IV$_3$, 8.10.5] we may work over $\mathbb{Z}_p$. By 1.2(b) and 4.2, $P^0_{\mathbb{F}_p}$ is a semi-abelian variety. Now use the following proposition. \qed

3.3 Proposition. *Let $R$ be a discrete valuation ring with field of fractions $K$ and residue field $k$. Let $A_K$ be an abelian variety with Néron model $A$ and let $B$ be a smooth and separated $R$-group with generic fiber $A_K$. Assume that $B_k$ is a semi-abelian variety. Then the canonical morphism $B \longrightarrow A$ is an open immersion and is an isomorphism on identity components.*

For the proof see [3], p. 182.

4. **The Toric Part of the Jacobian of a Semi-Stable Curve**

4.1 Given a semi-stable curve $X$ over a field $k$, write $S$ for the set of non-smooth points of $X \otimes \overline{k}$ and $I$ for the set of irreducible components of $X \otimes \overline{k}$. Define a graph $\Gamma(X)$ with $I$ as the set of vertices and $S$ as the set of edges: a singular point $s$ lying on the irreducible components $X_i, X_j$ ($i = j$ is allowed) defines an edge in the graph. It is a general fact in the theory of semi-stable curves that all $s \in S$ are rational over a separable extension of $k$.

4.2 Proposition. *Let $X$ be a semi-stable curve over a field $k$ with normalization $\pi : \hat{X} \longrightarrow X$. Then $\text{Pic}^0_{\hat{X}/k}$ is canonically an extension of an abelian variety by a torus:

$$1 \longrightarrow T \longrightarrow \text{Pic}^0_{\hat{X}/k} \longrightarrow \text{Pic}^0_X \longrightarrow 1.$$*
Furthermore, the rank of $T$ equals the first Betti number of the graph $\Gamma(X)$.

**Proof.** Let $X = \bigcup X_i$ be a decomposition of $X$ into irreducibles, so the normalization is

$$\hat{X} = \coprod \hat{X}_i \xrightarrow{\pi} X.$$ 

Then $\text{Pic}^0_{\hat{X}/k}$ is an abelian variety over $k$ since the $\hat{X}_i$ are proper and smooth.

We have the exact sequence of sheaves on $X_{\text{et}}$

$$1 \longrightarrow G_m/X \longrightarrow \pi_* G_m/\hat{X} \longrightarrow \mathcal{O} \longrightarrow 1.$$ 

(1) Write $S_k$ for the finite set of singular points of $X$ as a $k$-curve, so that $\mathcal{O}$ is supported on $S_k$. Fix $x \in S_k$. Naively, one expects that the pullback of (1) along $\text{Spec} k(x) \longrightarrow X$ would give rise to the sequence on $(\text{Spec} k(x))_k$

$$1 \longrightarrow G_m \longrightarrow \text{Res}_{k(\hat{x})/k(x)} G_m \times \text{Res}_{k(\hat{x}')/k(x)} G_m \longrightarrow \mathcal{O}_x \longrightarrow 1$$

where $\hat{x}, \hat{x}'$ are the two points of $\hat{X}$ lying over $x$ (see 4.3). Proceeding formally, we have that $k(x) = k(\hat{x}) = k(\hat{x}')$ by [6], p. 184, so that this sequence is just

$$1 \longrightarrow G_m \longrightarrow \text{Res}_{k(\hat{x})/k(x)} G_m \times G_m \longrightarrow \mathcal{O}_x \longrightarrow 1.$$ 

(2) Let $f : X \longrightarrow \text{Spec} k$ be the structure map. Then we have that

$$f_* \mathcal{O} \cong \prod_{x \in S_k} \text{Res}_{k(x)/k} G_m$$

is a $k$-torus of rank $\sum [k(x) : k] = \# S$. This isomorphism is not canonical as it depends on an ordering of the points $\{\hat{x}, \hat{x}'\}$ for each $x \in S_k$.

Apply $f_*$ to (1) and consider the resulting sequence of higher direct images:

$$1 \longrightarrow f_* G_m/X \longrightarrow f_* \pi_* G_m/\hat{X} \longrightarrow f_* \mathcal{O} \longrightarrow \cdots$$

$$\longrightarrow R^1 f_* G_m/X \longrightarrow (R^1 f_*) \pi_* G_m/\hat{X} \longrightarrow R^1 f_* \mathcal{O} \longrightarrow \cdots$$

Now note that:

(a) $f_* G_m/X = G_m/k$ since $X$ is proper and geometrically connected.

(b) $R^1 f_* \mathcal{O} = 0$ since the support of $\mathcal{O}$ is zero dimensional.

(c) $(R^1 f_*) \pi_* G_m/\hat{X} = \text{Pic}^0_{\hat{X}/k}$ by the conjunction of the Leray spectral sequence and the fact that if $f : X' \longrightarrow X$ is any finite morphism and $\mathcal{F}$ is an abelian sheaf on $X_0$, then $R^i f_* \mathcal{F} = 0 \forall i \geq 1$ [6], p. 32.

Hence we may rewrite the above as

$$1 \longrightarrow G_m/k \longrightarrow f_* \pi_* G_m/\hat{X} \longrightarrow f_* \mathcal{O} \longrightarrow T \longrightarrow 1$$

$$1 \longrightarrow T \longrightarrow \text{Pic}^0_{\hat{X}/k} \longrightarrow \text{Pic}^0_{\hat{X}/k} \longrightarrow 1,$$

where we have restricted to the identity component. Thus $T$, being a quotient of a torus, is a torus.

For the second assertion of the proposition, we claim that by extending scalars to $k_S$, the exact sequence (3) becomes

$$1 \longrightarrow G_m \longrightarrow \prod_{i \in I} G_m \longrightarrow \prod_{x \in S} G_m \longrightarrow 1$$

(4)
As Pic commutes with base change, the only point to be checked is that we may still label the product on the left by \( I \). This will be the case if \((\tilde{X})_{\mathit{et}} = (X_{\mathit{et}})^{\sim}\), i.e. if normalization commutes with \( \mathit{et} \) base change. This is so by [EGA IV, \( 18.12.15 \)].

By (4), the rank of \( T \) is \#\( S - \#I + 1 = \#\text{edges} - \#\text{vertices} + 1 \). This is the first Betti number of \( \Gamma(X) \) by elementary topology.

4.3 REMARK. The above proof is incomplete. The reason is as follows. Suppose we have a morphism \( f : Y \rightarrow X \) and a commutative group scheme \( G_X \) over \( X \).

As usual, we obtain a group scheme \( G_Y := G \times_X Y \) on \( Y \). Hence, by means of their functors of points, we obtain abelian sheaves again denoted \( G_X, G_Y \) on \( X_{\mathit{et}}, Y_{\mathit{et}} \), respectively. On the other hand, we also have the abelian sheaf \( f^*G_X \) on \( Y_{\mathit{et}} \). There is a canonical morphism \( \phi : f^*G_X \rightarrow G_Y \). It is not in general an isomorphism. However, it is an isomorphism if either \( f \) or \( G_X \) is \( \mathit{et} \), neither of which is the case in the above proof. For example, the sheaf \( G := \mathbb{G}_m \) on \( (\text{Spec } \mathbb{C})_{\mathit{et}} \) is isomorphic to the constant sheaf \( \mathbb{G}_m^{\infty} \) on \( (\text{Spec } \mathbb{C})_{\mathit{et}} \). If \( f : (\text{Spec } \mathbb{C}(t))_{\mathit{et}} \rightarrow (\text{Spec } \mathbb{C})_{\mathit{et}} \) is the obvious map, then \( f^*G \) is isomorphic to the constant sheaf \( \mathbb{G}_m^{\infty} \) on \( (\text{Spec } \mathbb{C}(t))_{\mathit{et}} \). This is of course not the same as \( \mathbb{G}_m \) on \( (\text{Spec } \mathbb{C}(t))_{\mathit{et}} \). See [11], pp. 68-69.

To repair the proof of 4.2, consider the divisor \( D := \sum_{P \in S_{\mathit{et}}} P \) supported on the singular locus and let \( i : D \rightarrow X \) be the inclusion. Then, for any scheme \( S \) over \( k \), one considers the following variant of (1):

\[
1 \rightarrow \mathbb{G}_m / X_S \rightarrow (\pi_S)^{\ast} \mathbb{G}_m / \tilde{X}_S \rightarrow (i_S)^{\ast} \mathbb{G}_m / D_S \rightarrow 1.
\]

One must then show that \((i_S)^{\ast} \mathbb{G}_m / D_S \) coincides with \( S_{\mathit{et}} \) with the points of a torus, compatibly as \( S \) varies through \( (\text{schemes}/k) \). We will not do this. For the details, see the notes in the margin on page 246 of Professor Conrad’s copy of [3].

4.4 Apply \( X(\cdot) := \text{Hom}_{\text{grp}}(\cdot, \mathbb{G}_m) \) to the exact sequence (2) to obtain

\[
1 \rightarrow \mathbb{Z}'(x) \rightarrow \mathbb{Z}^B \rightarrow \mathbb{Z} \rightarrow 1
\]

where \( \mathbb{Z}'(x) := X(\mathbb{Z}_x) \) and \( B_x \) is the (two element) set of analytic branches of \( X \) at \( x \). Then (4) becomes

\[
0 \rightarrow X(T) \rightarrow \bigoplus_{x \in S} \mathbb{Z}'(x) \rightarrow \bigoplus_{i \in I} \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow 0
\]

where the middle arrow sends a branch to the irreducible component containing it. The Galois action on \( X(T) \) coincides with the action induced by the natural Galois actions on the sets \( S, I \), and the \( B_x \) for \( x \in S \).

In particular, just as the proof of 4.2 shows that there is a Galois-equivariant isomorphism

\[
T_{\mathit{ks}} \simeq H^1(\Gamma(X), \mathbb{Z}) \otimes \mathbb{G}_m,
\]

we also have

\[
X(T) \simeq H_1(\Gamma(X), \mathbb{Z})
\]

compatibly with Galois actions.
4.5 Explicitly in the case of the curve $M_0(p)_{\mathbb{F}_p}$, it follows from 1.2(a) that its Jacobian is a torus, and in fact the proof of 4.2 shows that
\[
F_{\mathbb{F}_p}^0 \simeq \left( \prod_{x \in S_{\mathbb{F}_p}} \operatorname{Res}_{\mathbb{F}_p(x)/\mathbb{F}_p} G_m \right) / G_m
\]
where the $G_m$ is diagonally embedded. Moreover, the restrictions of scalars are from at worst quadratic extensions by 1.2(d).

5. The action of Frobenius

5.1 Let $S$ be a scheme of characteristic $p$, i.e. the canonical map $S \rightarrow \operatorname{Spec} \mathbb{Z}$ factors through $\operatorname{Spec} \mathbb{F}_p$. Let $F : S \rightarrow S$ be the absolute Frobenius morphism. It is defined to be the identity on the underlying topological space and the $p$-th power on $\mathcal{O}_S$. Let $X$ be a scheme over $S$. We define the relative Frobenius $F_{X/S}$, as well as $X^{(p)}$, by the diagram

\[
\begin{array}{ccc}
X & \xrightarrow{F_{X/S}} & X^{(p)} \\
\downarrow & \downarrow & \downarrow \\
S & \rightarrow & S
\end{array}
\]

For $x \in X$, we also write $x^{(p)}$ for $F_{X/S}(x)$.

5.2 Let $X$ and $X'$ be proper curves over a field $k$ of characteristic $p$. For a morphism $f : X \rightarrow X'$ over $k$, write $\operatorname{Pic}(f)$ for the induced map $\operatorname{Pic}_{X'/k}^0 \rightarrow \operatorname{Pic}_{X/k}^0$. Also, we write $F_{\mathbb{F}_p/k}$ for the relative Frobenius on $\operatorname{Pic}_{X/k}^0$.

5.3 Proposition. Let $X$ be a generically smooth, geometrically connected, and proper curve over a field $k$ of characteristic $p$. Then
\[
F_{\mathbb{F}_p/k} \circ \operatorname{Pic}(F_{X/k}) = [p]
\]
on $\operatorname{Pic}_{X/k}^0$.

Proof. We may assume without loss that $k = \mathbb{F}_p$ (cf. [5] 1.7.4). As $\operatorname{Pic}_{X/k}^0$ is smooth it suffices to check the identity on $k$-points (the $k$-points are dense; [3] p. 42). We use the fact that every invertible sheaf $\mathcal{L}$ on $X$ has the form $\mathcal{O}_X(D)$ for a Cartier divisor $D$ such that $\operatorname{supp}(D)$ is contained in the smooth locus $X^{\text{sm}}$ of $X$ (see the discussion after Theorem 7, p. 258 of [3]).

Let $\mathcal{L}$ be an invertible sheaf on $X^{(p)}$ of degree zero on each irreducible component. We may assume by additivity that $\mathcal{L}$ is of the form $\mathcal{O}_X(x_0^{(p)} - x_1^{(p)})$ where $x_0^{(p)}, x_1^{(p)} \in X^{(p)}(k)$ actually lie in the smooth locus of a common irreducible component $C^{(p)}$ of $X^{(p)}$.

Let $\iota_{x_0} : C^{\text{sm}} \rightarrow \operatorname{Pic}_{X/k}$ be the $k$-morphism $x \mapsto \mathcal{O}_X(x - x_0)$. Since $C^{\text{sm}}$ is irreducible and $\iota_{x_0}(x_0) = 0$, $\iota_{x_0}$ factors through $\operatorname{Pic}_{X/k}^0$.

Before proceeding any further, let's note that
(a) $i_{x_0}^{(p)} = i_{x_0}^{(p)}$, i.e. the following diagram commutes

For the proof, we have that

$$i_{x_0}^{(p)} : x^{(p)} \mapsto [x^{(p)} - x_0^{(p)}]$$

$$(i_{x_0})^{(p)} : x \mapsto \text{pr}^*[x - x_0]$$

where \text{pr} is as in 5.1. But $\text{pr}^*[x] = [x^{(p)}]$ so that $[x^{(p)} - x_0^{(p)}] = \text{pr}^*[x - x_0]$, as claimed.

(b) Since raising to the $p$-th power commutes with any ring map we have the commutativity of

$$
\begin{array}{ccc}
X & \xrightarrow{f} & Y \\
\text{F_{X/k}} & & \text{F_{Y/k}} \\
X^{(p)} & \xrightarrow{f^{(p)}} & Y^{(p)}
\end{array}
$$

for any morphism of $f : X \longrightarrow Y$ of schemes of characteristic $p$.

Returning to the proof of the proposition, we have

$$(\text{Fic}_{k/k} \circ \text{Pic}(F_{X/k}))(\mathcal{L}) = \text{Fic}_{k/k}(\text{Pic}^*(F_{X/k}^{(p)}(\mathcal{L})))$$

$$= \text{Fic}_{k/k}(\mathcal{O}_X(F_{X/k}^{(p)}(F_{X/k}(x) - F_{X/k}(x_0))))$$

Now using the fact that $F_{X/k}$ is finite flat and purely inseparable of degree $p$ over the smooth locus, the last term above equals $\text{Fic}_{k/k}(\mathcal{O}_X(p(x_1 - x_0)))$. Then we have

$$F_{\text{Pic}_{k/k}}(\mathcal{O}_X(p(x_1 - x_0))) = [p] \circ F_{\text{Pic}_{k/k}}(\mathcal{O}_X(x_1))$$

$$= [p] \circ F_{\text{Pic}_{k/k}}(F_{X/k}(x_1))$$

$$= [p] \circ i_{x_0}^{(p)}(x_1^{(p)})$$

$$= \mathcal{O}_X(x_1^{(p)} - x_0^{(p)})^{\otimes p}$$

as required. \hfill \Box

5.4 Put $X := M_0(p)_{F_{\mu}}$. Then by 1.2, $\Gamma(X)$ has two vertices and an edge for each geometric supersingular point. See Figure 2.

The following is Theorem A.1.1(a) of [10].
\textbf{5.5 Theorem.} $F_{\overline{F}_p}/F_p = -wp$.

\textit{Proof.} If we could show that $\text{Pic}(F_{\overline{F}_p}) = -w$ then $F_{\overline{F}_p}/F_p \circ (-w) = p$ by 5.3. The theorem would follow since $w$ is an involution.

Let $E$ be an ordinary elliptic curve over $\overline{F}_p$, so that $E[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mu_p$, and put $C := \ker(F_{\overline{F}_p}/E \rightarrow E^{(\psi)})$. $C$ is the unique connected subgroup of $E$ of order $p$; it is isomorphic to $\mu_p$. Also, $F_{\overline{F}_p}/E$ induces an isomorphism $E/C \simeq E^{(\psi)}$ and $E[p]/C$ is étale. See [5], p. 27. Hence $w(E) = w(E, C) = (E/C, E[p]/C) \simeq (E^{(\psi)}, C')$ for some étale $C' \subset E^{(\psi)}$. It now follows from 1.2(c) that $w$ exchanges the vertices of $\Gamma(X)$ and sends an edge $x$ to the edge $x^{(\psi)}$. On the other hand, $F_{\overline{F}_p}/E$ fixes the vertices and sends an edge $x$ to the edge $x^{(\psi)}$. We are done by (5). \hfill $\square$

\textbf{References}


