Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 123

Abelian subvarieties of Drinfeld Jacobians and congruences modulo the characteristic

Mihran Papikian

Saarbrücken 2005

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 123
submitted: January 11, 2005

Abelian subvarieties of Drinfeld Jacobians and congruences modulo the characteristic

Mihran Papikian

Stanford University
Department of Mathematics
CA 94305
Stanford
USA
papikan@math.stanford.edu

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

ABELIAN SUBVARIETIES OF DRINFELD JACOBIANS AND CONGRUENCES MODULO THE CHARACTERISTIC

MIHRAN PAPIKIAN

ABSTRACT. We prove a level lowering result over rational function fields, with the congruence prime being the characteristic of the field. We apply this result to show that semi-stable optimal elliptic curves are not Frobenius conjugates of other curves defined over the same field.

1. INTRODUCTION

Let $f = \sum_{n\geq 1} a_n(f)q^n$ be a (normalized) newform in $S_2(\Gamma_0(N))$, the $\mathbb{C}$-vector space of weight-2 cusp forms of level N. Fix $p \geq 3$. Let $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be the residual Galois representation attached to f by the Deligne-Serre construction. Let ℓ be a prime which strictly divides N, i.e., $N = \ell M$ with $(\ell, M) = 1$. Recall the main theorem of [18]

Theorem 1.1 (Mazur, Ribet). *Assume that ρ_f is irreducible and finite at ℓ. Assume also that either*

(1) $\ell \not\equiv 1 \pmod{p}$, *or*
(2) *N is prime to p.*

Then there is a newform $g \in S_2(\Gamma_0(M))$ and a prime ideal $\wp$ dividing p in the ring of integers of the number field generated by the Fourier coefficients of f and g such that for almost all prime numbers v the Fourier coefficients

$$a_v(f) \equiv a_v(g) \pmod{\wp}$$

are congruent modulo $\wp$.

A famous application of this deep result is the fact that Fermat's Last Theorem follows from the Shimura-Taniyama conjecture.

The aim of this paper is to discuss a certain analogue of Theorem 1.1 over function fields, when the congruence prime p is the characteristic of the field. We then apply this result to study the arithmetic of elliptic curves over rational function fields. Before stating the main result, we need to introduce some terminology and notation.

The situation which most closely resembles the classical one is when our function field $F = \mathbb{F}_q(t)$ is the field of rational functions on $\mathbb{P}^1_{\mathbb{F}_q}$. Here $\mathbb{F}_q$ is the finite field of q elements, where q is a power of the prime number p (we will not impose any restrictions on p). To get the analogue of $\mathbb{Z}$ one has to fix a closed point on $\mathbb{P}^1_{\mathbb{F}_q}$, suggestively denoted by ∞, and consider the subring of F consisting of functions regular away from ∞. We will choose ∞ to be rational, $\deg(\infty) = 1$. Without loss

Key words and phrases. Drinfeld modular curves, congruences, component groups.
Supported by a grant from the European Postdoctoral Institute.

of generality, $\infty = \frac{1}{t}$ and $\mathrm{H}^0(\mathbb{P}^1_{\mathbb{F}_q} - \infty, \mathcal{O}) = \mathbb{F}_q[t]$ is the polynomial ring in one variable over $\mathbb{F}_q$. Let $\mathfrak{n}$ be an ideal of $\mathbb{F}_q[t]$ and consider the Drinfeld modular curve $X_0(\mathfrak{n})_F$ of level $\mathfrak{n}$. This is a compactified coarse moduli scheme for pairs $(D, Z_\mathfrak{n})$ consisting of a Drinfeld $\mathbb{F}_q[t]$-module D of rank-2 over F and an $\mathfrak{n}$-cyclic subgroup $Z_\mathfrak{n}$ of D. It is a proper, smooth, geometrically connected curve over F.

Let $S(\Gamma_0(\mathfrak{n}), \mathbb{C})$ be the vector space of $\mathbb{C}$-valued cuspidal harmonic cochains invariant under the action of the Hecke congruence group $\Gamma_0(\mathfrak{n})$. We refer to §3.2 for the precise definition of this space; for now it suffices to say that $S(\Gamma_0(\mathfrak{n}), \mathbb{C})$ has an interpretation of a space of automorphic cusp forms on $\mathrm{GL}_2(\mathbb{A}_F)$ which plays a role similar to that of weight-2 cusp forms $S_2(\Gamma_0(N))$ in the classical theory. The space $S(\Gamma_0(\mathfrak{n}), \mathbb{C})$ has a canonical integral structure given by $\mathbb{Z}$-valued harmonic cochains $S(\Gamma_0(\mathfrak{n}), \mathbb{Z})$. It is known that $S(\Gamma_0(\mathfrak{n}), \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank equal to the genus of $X_0(\mathfrak{n})_F$, and $S(\Gamma_0(\mathfrak{n}), \mathbb{Z}) \otimes_\mathbb{Z} \mathbb{C} = S(\Gamma_0(\mathfrak{n}), \mathbb{C})$. The lattice $S(\Gamma_0(\mathfrak{n}), \mathbb{Z}) \subset S(\Gamma_0(\mathfrak{n}), \mathbb{C})$ is the analogue of weight-2 cusp forms having integral Fourier expansion. To simplify the notation, let $S(\mathfrak{n}) := S(\Gamma_0(\mathfrak{n}), \mathbb{C})$ and $S(\mathfrak{n}, \mathbb{Z}) := S(\Gamma_0(\mathfrak{n}), \mathbb{Z})$. There is a Hecke algebra $\mathbb{T}$ acting on $S(\mathfrak{n})$, and this action preserves $S(\mathfrak{n}, \mathbb{Z})$; see §3.3. Let $f \in S(\mathfrak{n})$ be a normalized newform. Denote by $J := J_0(\mathfrak{n})$ the Jacobian variety of $X_0(\mathfrak{n})_F$. There is a unique saturated sublattice $S_f(\mathbb{Z}) \subseteq S(\mathfrak{n}, \mathbb{Z})$ and a unique abelian subvariety $A_f \subseteq J$ which are canonically associated to f. (Saturated means $S(\mathfrak{n}, \mathbb{Z})/S_f(\mathbb{Z})$ is torsion free.) The lattice $S_f(\mathbb{Z})$ is the intersection with $S(\mathfrak{n}, \mathbb{Z})$ of the linear space spanned by f together with all of its Galois conjugates. The abelian variety A_f arises from the Shimura construction. If we let K_f be the number field generated by the Hecke eigenvalues of f then $\mathrm{rank}_\mathbb{Z}(S_f(\mathbb{Z})) = \dim_F(A_f) = [K_f : \mathbb{Q}]$.

Now suppose $\mathfrak{n} = \mathfrak{p}\mathfrak{m}$, where $\mathfrak{p}$ is a prime ideal coprime to the ideal $\mathfrak{m}$. There are two natural injective homomorphisms $S(\mathfrak{m}) \rightrightarrows S(\mathfrak{n})$. Denote the subspace generated by the images by $S(\mathfrak{n})^{\mathfrak{p}-\mathrm{old}}$, and denote the intersection $S(\mathfrak{n}, \mathbb{Z}) \cap S(\mathfrak{n})^{\mathfrak{p}-\mathrm{old}}$ by $S(\mathbb{Z})^{\mathfrak{p}-\mathrm{old}}$. It is easy to see that $S(\mathbb{Z})^{\mathfrak{p}-\mathrm{old}}$ is a saturated sublattice of $S(\mathfrak{n}, \mathbb{Z})$ which has trivial intersection with $S_f(\mathbb{Z})$. Finally, let $\Phi_{A_f,\mathfrak{p}}$ and $\Phi_{J,\mathfrak{p}}$ be the mod-$\mathfrak{p}$ component groups of the Néron models of A_f and J over $\mathbb{P}^1_{\mathbb{F}_q}$, respectively. The first main theorem of this paper is the following (see Theorem 4.4)

Theorem 1.2. *Suppose the kernel of the homomorphism $\Phi_{A_f,\mathfrak{p}} \to \Phi_{J,\mathfrak{p}}$, functorially induced from the closed immersion $A_f \hookrightarrow J$, has non-trivial p-torsion. Then $S(\mathfrak{n}, \mathbb{Z})/(S_f(\mathbb{Z}) \oplus S(\mathbb{Z})^{\mathfrak{p}-\mathrm{old}})$ has non-trivial p-torsion.*

We explain why this theorem is analogous to Theorem 1.1. First of all, it is clear that $S(\mathfrak{n}, \mathbb{Z})/(S_f(\mathbb{Z}) \oplus S(\mathbb{Z})^{\mathfrak{p}-\mathrm{old}})$ has p-torsion exactly when there is an element $\varphi \in S_f(\mathbb{Z})$ and an element $\phi \in S(\mathbb{Z})^{\mathfrak{p}-\mathrm{old}}$, neither of which is a p-multiple of some other element, and such that $\varphi - \phi \in pS(\mathfrak{n}, \mathbb{Z})$, i.e., φ and ϕ are congruent modulo p. It can be shown that a similar condition over $\mathbb{Q}$ implies the congruence between the eigenforms in Theorem 1.1; cf. [17, p.193]. The proof of this uses at one step the fact that there is a perfect pairing $S_2(N, \mathbb{Z}) \times \mathbb{T} \to \mathbb{Z}$. The analogous pairing over F is known to be perfect only after inverting p, and also the Fourier coefficients of the elements in $S(\mathfrak{n}, \mathbb{Z})$ lie in $\mathbb{Z}[p^{-1}]$; see [7, pp. 43-44]. Hence the formulation of the congruence condition as the existence of p-torsion in the quotient of $S(\mathfrak{n}, \mathbb{Z})$ seems more natural over function fields.

Next, the p-torsion subgroup schemes of abelian varieties over fields of characteristic p are not étale. Thus, instead of working with the residual Galois representations arising from such subschemes, we work directly with these finite flat group schemes. The modularity of the residual Galois representation is replaced by the requirement that the corresponding group scheme is a subgroup scheme of $J[p]$. This apparently stronger requirement of an actual inclusion $A_f[p] \subseteq J[p]$, rather than "up-to-isogeny" inclusion, is necessary since, as is easy to see, the Frobenius conjugates of A_f have increasingly large p-power torsion in their $\mathfrak{p}$-fibre component groups. The condition that $\Phi_{A_f,\mathfrak{p}}$ has p-torsion replaces the condition on ρ_f being finite at ℓ in Theorem 1.1. For example, if A_f is an elliptic curve over $\mathbb{Q}$ then $\Phi_{A_f,\ell}$ having p-torsion implies that ρ_f is finite at ℓ. Finally, the condition that some of the p-torsion of $\Phi_{A_f,\mathfrak{p}}$ lies in the kernel of $\Phi_{A_f,\mathfrak{p}} \to \Phi_{J,\mathfrak{p}}$ replaces the requirement that ρ_f is irreducible (since over $\mathbb{Q}$ the analogous condition essentially means that p is "non-Eisenstein", and hence ρ_f is irreducible, cf. [18, §5]).

Studying mod-p congruences between the elements of $S(\mathfrak{n}, \mathbb{Z})$ is interesting for several reasons. First of all, it is known that "multiplicity-one" fails for Drinfeld (rigid-analytic) cusp forms $\mathrm{H}^0(X_0(\mathfrak{n})_{F_\infty}, \Omega^1)$, that is, there might be two distinct Hecke eigenforms having the same eigenvalues, cf. [9, (9.7.4)]. The reason that this happens is exactly the existence of mod-p congruences in $S(\mathfrak{n}, \mathbb{Z})$; see [9, (6.5.1)]. This should be compared with the point of view on level lowering taken in [12], and the main theorem therein. Next, the consideration of mod-p congruences seems to arise naturally when one tries to study certain questions about Frobenius isogenies between the quotients of Drinfeld Jacobians. In fact, we were led to Theorem 1.2 in an attempt to answer the following question[1]: Is it possible for an optimal elliptic curve over F to be a Frobenius conjugate of another curve in the same F-isogeny class? It is known that an elliptic curve over F having conductor $\mathfrak{n} \cdot \infty$ and split multiplicative reduction at ∞ is a quotient of $J_0(\mathfrak{n})$ (this follows from a combination of some deep results due to Deligne, Drinfeld and Zarhin). We call such elliptic curves *modular*. The *optimal* elliptic curve in an F-isogeny class of modular elliptic curves is the unique curve E for which the quotient $J_0(\mathfrak{n}) \to E$ can be chosen to have connected and smooth kernel (equiv. E occurs as a subvariety of $J_0(\mathfrak{n})$). Combining the ideas which go into the proof of Theorem 1.2 with some additional arguments, in this paper we are able to prove the following (see Theorem 4.6)

Theorem 1.3. *Semi-stable optimal elliptic curves are not Frobenius conjugates of other curves over F.*

The theorem implies that for a semi-stable optimal E, $E(F)[p] = 1$. The next example shows that Theorem 1.3 is the best possible result, in the sense that if one allows the optimal curve to have at least one finite place of additive reduction then it can be a Frobenius conjugate.

Example 1.4. Let $F = \mathbb{F}_2(t)$. Consider the elliptic curve E given by the Weierstrass equation

$$y^2 + txy = x^3 + t^2.$$

This curve has only two places of bad reduction: t and ∞ with the reduction at t being additive and the reduction at ∞ split multiplicative. The conductor of E is $t^3 \cdot \infty$, its j-invariant is t^4. This curve is optimal, in fact one can show that

[1] This question was communicated to me by Barry Mazur.

$E = X_0(t^3)$; see [9, (9.7.3)]. Next, it is not hard to show that $E(F) \cong \mathbb{Z}/4\mathbb{Z}$ and is generated by $P = (0, t)$. Let E' be the quotient of E by the subgroup generated by P. Then $E \to E'$ is a separable isogeny of degree 4 defined over F, whose dual is Frob^2. Hence $E = (E')^{(p^2)}$.

Another optimal elliptic curve over $\mathbb{F}_2(t)$ which is a Frobenius conjugate is the following $E:\ y^2 + txy + ty = x^3$. Its conductor is $t^2(t+1)\infty$, and the j-invariant is $t^8/(t+1)^2$. It is optimal since $E = X_0(t^2(t+1))$; see [7, Ex. 4.3]. The group of rational points is $E(F) \cong \mathbb{Z}/6\mathbb{Z}$, and is generated by $P = (t, t)$. If we let $E' := E/(3P)$ then $E = (E')^{(p)}$.

Remark 1.5. The question of Frobenius conjugacy of optimal elliptic curves is related to the well-known *Szpiro's bound*. Let E be a non-isotrivial semi-stable elliptic curve over F. Denote the j-invariant of E by j_E. Define the *non-separable degree of* j_E, $\deg_{\mathrm{ns}}(j_E)$, to be the non-separable degree of the field extension $F/\mathbb{F}_q(j_E)$. In particular, $\deg_{\mathrm{ns}}(j_E)$ is equal to some power of the characteristic p. Let $\mathcal{D}_E$ be the minimal discriminant of E, and let $\mathfrak{n}_E$ be its conductor. Szpiro's bound is the following inequality

$$\deg \mathcal{D}_E \leq 6 \cdot \deg_{\mathrm{ns}}(j_E) \cdot (\deg \mathfrak{n}_E - 2).$$

This bound is the function field analogue of a famous (still open) conjecture of Szpiro which asserts a certain inequality between the discriminants and the conductors of elliptic curves over $\mathbb{Q}$. It is clear that in general there are elliptic curves over F with arbitrarily large $\deg_{\mathrm{ns}}(j)$, and the above inequality is false without $\deg_{\mathrm{ns}}(j)$ in it. More precisely, $\deg \mathcal{D}_E$ cannot be uniformly bounded only in terms of some fixed power of $\deg \mathfrak{n}_E$. (This easily can be seen by fixing a non-isotrivial elliptic curve E and considering its Frobenius conjugates $E^{(p^n)}$.)

It is an interesting question whether one could refine Szpiro's bound for arithmetically important curves, such as the optimal elliptic curves, by getting rid of $\deg_{\mathrm{ns}}(j)$. Theorem 1.3 says that this is indeed possible. Hence Szpiro's conjecture over $\mathbb{Q}$ and the provable result over $\mathbb{F}_q(t)$ take essentially the same form when we restrict the attention to optimal curves.

The organization of the paper is as follows. In Section 2 we prove two propositions about closed immersions of abelian varieties over local fields having certain reduction types. One of the propositions, Proposition 2.7, implies that the p-torsion of $\ker(\Phi_{A_f,\mathfrak{p}} \to \Phi_{J,\mathfrak{p}})$ can be "lifted" from the $\mathfrak{p}$-fibre to the generic fibre, in the sense that there is a natural injection of the Cartier dual of this étale group scheme into the connected finite flat group scheme $(A_f \cap J^{\mathfrak{p}-\mathrm{old}})^0$. Here $J^{\mathfrak{p}-\mathrm{old}}$ is the abelian subvariety of J generated by the images of $J_0(\mathfrak{m}) \rightrightarrows J$, and the scheme-theoretic intersection takes place inside of J. The second proposition, Proposition 2.9, implies that $(A_f \cap J^{\mathfrak{p}-\mathrm{old}})^0$ can be "specialized" to the ∞-fibre, in the sense that the non-triviality of $(A_f \cap J^{\mathfrak{p}-\mathrm{old}})^0$ implies mod-p congruences between the elements of the character group M_J of the connected component of the identity of the mod-∞ fibre of the Néron model of J over $\mathbb{P}^1_{\mathbb{F}_q}$. In Section 3 we show that there is a canonical $\mathbb{T}$-equivariant isomorphism $M_J \cong S(\mathfrak{n}, \mathbb{Z})$. Hence congruences in M_J translate into congruences in $S(\mathfrak{n}, \mathbb{Z})$. The reason why Theorem 1.2 currently fails to work over general function fields is exactly this last isomorphism, whose proof uses at one step a result of Gekeler and Nonnengardt [8]. (A statement similar to this result is conjecturally valid in general, cf. [9, (6.4.5)], but the proof in [8] works only over $\mathbb{F}_q(t)$.) The final Section 4 contains the proofs of the main theorems.

Notation and terminology. By a finite flat group scheme over the base scheme S we always mean a finite flat *commutative* S-group scheme. When $S = \mathrm{Spec}(L)$ with L a field, we will abbreviate this to "finite L-group scheme". If G is a finite flat group scheme over a connected base S, then the $\mathcal{O}_S$-module $\mathcal{O}_G$ is locally free of constant rank called the *order of* G and denoted $\#G$. A finite group scheme G over a field L is said to be *étale* if $G \times_{\mathrm{Spec}(L)} \mathrm{Spec}(\bar{L})$ is reduced, where $\bar{L}$ is the algebraic closure of L. As is well-known there is a one-to-one correspondence between the finite étale group schemes over L and the finite abelian groups with a continuous action of $\mathrm{Gal}(L^{\mathrm{sep}}/L)$. It is also well-known that if G over L has order coprime to the characteristic of L then G is étale. A finite flat group scheme G over S is said to be étale if the fibres G_s are étale over the corresponding residue fields for all closed points s of S. We say that a finite flat group scheme G is *multiplicative* if its Cartier dual $G^\vee$ is étale. Given an abelian variety A, its dual abelian variety will be denoted by $\hat{A}$.

Acknowledgements. This article was written while I was visiting MPIM (Bonn) and Universität des Saarlandes. I thank the staff and the members of these institutions for their hospitality. I also thank Professor E.-U. Gekeler for helpful comments on an earlier version of this article.

2. Character groups and component groups

In this section we let R be a complete discrete valuation ring, K be its field of fractions, and k be the residue field. The main results of the section are Propositions 2.7 and 2.9. Proposition 2.3, which precedes these two, plays a key role in the proofs of both.

2.1. **Néron models of abelian varieties with toric reduction.** Let A be an abelian variety over K. Denote by $\mathcal{A}$ its Néron model over R and denote by $\mathcal{A}_k^0$ the connected component of the identity of the closed fibre $\mathcal{A}_k$ of $\mathcal{A}$. We have an exact sequence

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi_A \to 0, \tag{2.1}$$

where Φ_A is a finite étale group scheme over k called the *component group of* A. We say that A has *semi-abelian reduction* if the identity component is an extension of an abelian variety A_k' by an affine algebraic torus T_k over k

$$0 \to T_k \to \mathcal{A}_k^0 \to A_k' \to 0. \tag{2.2}$$

We say that A has (*split*) *toric reduction* if $\mathcal{A}_k^0 = T_k$ is a (split) torus.

In general closed immersions of abelian varieties do not extend to closed immersions of Néron models; see [2, §7.5]. Nevertheless, under special assumptions this is true; cf. [2, Thm.7.5/4], where R is assumed to be of mixed characteristic with "small" absolute ramification index. In Proposition 2.3 we will prove a similar (slightly weaker) statement for equicharacteristic R, assuming the abelian varieties in question have toric reduction. We replace the use of Raynaud's theorem [16, Cor. 3.3.6], which is valid only in mixed characteristic, by Lemma 2.1.

Let G be a finite K-group scheme, and let $\mathcal{G}$ be a finite flat R-group scheme extending G (i.e., $\mathcal{G}_K = G$). We say that $\mathcal{G}$ is an *admissible* extension of G if the connected component $\mathcal{G}_k^0$ of the closed fibre of $\mathcal{G}$ is multiplicative (we allow $\mathcal{G}_k^0$ to be trivial).

Lemma 2.1. *Assume R is equicharacteristic. Let G be a finite group scheme over K of order equal to a power of a prime number p. Let $\mathcal{G}'$ and $\mathcal{G}''$ be two admissible extensions of G. Any map $v : \mathcal{G}' \to \mathcal{G}''$ which is an isomorphism over K is an isomorphism over R.*

Proof. If p is not the characteristic of K then any finite flat extension of G over R must be étale and is clearly unique, so we will assume p is the characteristic of K. Let $\mathcal{G}$ be any admissible extension. Consider the *connected-étale sequence* of $\mathcal{G}$

$$0 \to \mathcal{G}^0 \to \mathcal{G} \to \mathcal{G}^{\mathrm{et}} \to 0.$$

The formation of this sequence is compatible with any local base change to another henselian local ring (e.g., passage to the closed fibre $R \to k$), so

$$0 \to \mathcal{G}^0_k \to \mathcal{G}_k \to \mathcal{G}^{\mathrm{et}}_k \to 0$$

is the connected-étale sequence of $\mathcal{G}_k$. Next, we claim that the generic fibre $\mathcal{G}^0_K$ of $\mathcal{G}^0$ must be multiplicative. It is enough to show that the Cartier dual $\mathcal{H}$ of $\mathcal{G}^0$ has étale K-fibre. Since by assumption $\mathcal{G}^0_k$ is multiplicative, $\mathcal{H}_k$ is étale. This implies that $\mathcal{H}$ is étale, and in particular $\mathcal{H}_K$ is étale. Multiplicative p-power order group schemes are connected in characteristic p, so $\mathcal{G}^0_K$ is a subgroup scheme of G^0. Since $\mathcal{G}^{\mathrm{et}}_K$ is étale, we see that

$$0 \to \mathcal{G}^0_K \to \mathcal{G}_K \to \mathcal{G}^{\mathrm{et}}_K \to 0$$

is the connected-étale sequence of G. (Note that the formation of the connected-étale sequence usually does not commute with non-local base change, such as $R \to K$, so for our last conclusion the admissibility of $\mathcal{G}$ is crucial.)

Now let $\mathcal{G}'$ and $\mathcal{G}''$ be two admissible extensions of G. Let $v : \mathcal{G}' \to \mathcal{G}''$ be a morphism over R which is an isomorphism over K. There are unique maps v^0 and v^{et} between connected components and maximal étale quotients such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathcal{G}')^0 & \longrightarrow & \mathcal{G}' & \longrightarrow & (\mathcal{G}')^{\mathrm{et}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle v^0} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v^{\mathrm{et}}} & & \\ 0 & \longrightarrow & (\mathcal{G}'')^0 & \longrightarrow & \mathcal{G}'' & \longrightarrow & (\mathcal{G}'')^{\mathrm{et}} & \longrightarrow & 0. \end{array} \tag{2.3}$$

commutes. From what we proved we conclude that $(\mathcal{G}')^0$ and $(\mathcal{G}'')^0$ are two multiplicative extensions of the same multiplicative K-group scheme G^0_K. Since G^0_K has a unique such extension (for example, take the Cartier duals to get étale group schemes where this is obvious), v^0 is an isomorphism. Next, $(\mathcal{G}')^{\mathrm{et}}$ and $(\mathcal{G}'')^{\mathrm{et}}$ are étale extensions of G^{et}, hence v^{et} is also an isomorphism. We conclude that v is an isomorphism. □

Remark 2.2.

(1) The statement of the lemma is false without assuming R is equicharacteristic as the example of μ_2 over $\mathbb{Q}_2$ shows.
(2) When R has characteristic $p > 0$, G need not have any admissible extensions over R even if it is étale or multiplicative of order p. Take for example the Oort-Tate group scheme $G_{a,0}$, $a \in K$ with $0 < \mathrm{ord}_K(a) < p - 1$; see [14]. This is étale but any extension $\mathcal{G}$ has closed fibre isomorphic to $G_{0,0_{/k}} = \alpha_p$. Also, there are commutative group schemes over K killed by p and of order p^2 which do not extend over R at all; see Appendix B of Ch.3 in [13].

Proposition 2.3. *Let $f_K : A \to B$ be a closed immersion of abelian varieties over K, i.e., A is an abelian subvariety of B. Assume B has toric reduction. If R is equicharacteristic then the canonical morphism $f : \mathcal{A} \to \mathcal{B}$ extending f_K induces a closed immersion $f_k : \mathcal{A}_k \to \mathcal{B}_k$.*

Proof. If the characteristic of R is zero then in fact a stronger statement is true, cf. [2, Prop.7.5/2], so we will assume R has positive characteristic p.

By slightly modifying the argument in [2, Lem.7.4/2], one can show that A also has toric reduction. Since a monomorphism between smooth finite type group schemes over a field is necessarily a closed immersion, it suffices to show that $H := \ker f_k$ is trivial. The kernel of $f_k : \mathcal{A}_k \to \mathcal{B}_k$ is finite, as A is isogenous (in fact isomorphic) to a subvariety of B. Hence H is finite, and if we show that it has trivial ℓ-torsion for any prime ℓ, we could conclude that H is trivial. As $H[\ell] \subseteq \mathcal{A}[\ell]_k$, it is enough to show that f restricted to the quasi-finite and flat group scheme $\mathcal{A}[\ell]$ is a monomorphism. Since R is henselian, there is a unique decomposition $\mathcal{A}[\ell] = G \coprod G_0$ into disjoint subgroup schemes which are both open and closed in $\mathcal{A}[\ell]$, and such that G is finite and flat over R and G_0 has empty closed fibre; cf. [2, §7.3]. Hence it is enough to prove that f is an isomorphism when restricted to G. Let G' be the schematic image of G in $\mathcal{B}$ under f. Since f_K is a closed immersion, we have an isomorphism on generic fibres $f_K : G_K \xrightarrow{\sim} G'_K$. Since A has toric reduction, G_k^0 is multiplicative (being in the kernel of a homomorphism of tori). Similarly for G'. We conclude that G and G' are two admissible extensions of G_K, and f must be an isomorphism by Lemma 2.1. □

Let A and B be as in Proposition 2.3. Consider the commutative diagram induced by f_k:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}_k^0 & \longrightarrow & \mathcal{A}_k & \longrightarrow & \Phi_A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_k^0} & & \downarrow{\scriptstyle f_k} & & \downarrow{\scriptstyle f_\Phi} & & \\ 0 & \longrightarrow & \mathcal{B}_k^0 & \longrightarrow & \mathcal{B}_k & \longrightarrow & \Phi_B & \longrightarrow & 0. \end{array} \tag{2.4}$$

Corollary 2.4. *The morphism f_k^0 is a closed immersion and* $\ker(f_\Phi)$ *can be identified with a subgroup scheme of the quotient torus $\mathcal{B}_k^0/\mathcal{A}_k^0$. In particular, if R has characteristic $p > 0$ then* $\ker(f_\Phi)$ *has vanishing p-power torsion.*

Proof. The first sentence immediately follows from Proposition 2.3 by using the snake lemma. The second sentence is true because the p-power torsion of a torus over k is connected, whereas $\ker(f_\Phi)$ is étale. □

2.2. **Maps between component groups.** Let A be an abelian variety over K with semi-abelian reduction. The *character group*

$$M_A = \mathrm{Hom}_{\bar{k}}(T_{\bar{k}}, \mathbb{G}_{m,\bar{k}})$$

is a free abelian group contravariantly associated to A. Here T_k is as in (2.2). Let $M_{\hat{A}}$ be the analogous group associated to the dual abelian variety $\hat{A}$. In [11, §§9-10] Grothendieck defined a canonical bilinear $\mathrm{Gal}(\bar{k}/k)$-equivariant pairing,

$$u_A : M_A \times M_{\hat{A}} \to \mathbb{Z},$$

which he called the *monodromy pairing.* This pairing is uniquely characterized by the property that its extension of scalars $u_A \otimes \mathbb{Z}_\ell$, for a prime $\ell \neq \mathrm{char}(k)$, can be expressed in terms of the ℓ-adic Weil pairing on $T_\ell(A) \times T_\ell(\hat{A})$ via a formula given in [11, (9.1.2)]. We have the following key fact:

Theorem 2.5 (Grothendieck)**.** *There is a* $\mathrm{Gal}(\bar{k}/k)$*-equivariant exact sequence*

$$0 \longrightarrow M_{\hat{A}} \xrightarrow{u_A} \mathrm{Hom}(M_A, \mathbb{Z}) \longrightarrow \Phi_A \longrightarrow 0.$$

Proof. See [11, Thm. 11.5]. □

Let B be an abelian variety over K with semi-abelian reduction. We say that the abelian subvariety A of B is *maximal toric* if for any abelian subvariety D of B having toric reduction the canonical closed immersion $D \hookrightarrow B$ factors through $D \hookrightarrow A \hookrightarrow B$.

Lemma 2.6. *If an abelian subvariety A of B has toric reduction and the quotient $C := B/A$ is isomorphic to an abelian variety with good reduction (i.e., C can be extended to an abelian scheme over R) then A is maximal toric.*

Proof. This is clear. □

In this subsection we assume that A is an abelian subvariety of B satisfying the conditions of Lemma 2.6. We denote the quotient abelian variety B/A by C, so there is an exact sequence of abelian varieties

$$0 \to A \to B \to C \to 0. \tag{2.5}$$

Assume B is principally polarized, $\theta : \hat{B} \xrightarrow{\sim} B$. Taking the dual of $B \to C$ in (2.5) and using θ to identify $\hat{B}$ with B, we can identify $\hat{C}$ with a closed subvariety of B; see [3, Prop.3.3]. Since $\hat{C}$ is isogenous to C under $B \to C$, it is clear that $\hat{C} \cap A$ is a finite group scheme, where the scheme-theoretic intersection $\cap$ is taken inside of B. Let $f_K : D \hookrightarrow B$ be an abelian subvariety of B having toric reduction. Let $f_\Phi : \Phi_D \to \Phi_B$ be the homomorphism between the component groups functorially induced from f_K, cf. (2.4).

Proposition 2.7. *Assume R has characteristic $p > 0$. Let $\mathcal{H}_D := \ker(f_\Phi)[p^\infty]$ be the p-power torsion of $\ker(f_\Phi)$. There is a natural injective homomorphism $\mathcal{H}_D^\vee \hookrightarrow (D \cap \hat{C})$.*

Proof. Consider the polarization $\varphi_K : D \to \hat{D}$ obtained as the composition

$$\varphi_K : D \xrightarrow{f_K} B \xrightarrow{\hat{\theta}} \hat{B} \xrightarrow{\hat{f}_K} \hat{D}.$$

Using Theorem 2.5, we get a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M_{\hat{D}} \arrow[r, "u_D"] \arrow[d, "\varphi^*"] & \mathrm{Hom}(M_D, \mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{Hom}(\hat{\varphi}^*, \mathbb{Z})"] & \Phi_D \arrow[r] \arrow[d, "\varphi_\Phi"] & 0 \\
0 \arrow[r] & M_D \arrow[r, "u_{\hat{D}}"] & \mathrm{Hom}(M_{\hat{D}}, \mathbb{Z}) \arrow[r] & \Phi_{\hat{D}} \arrow[r] & 0.
\end{tikzcd}$$

The middle vertical arrow is injective, so $\ker(\varphi_\Phi) \hookrightarrow \mathrm{coker}(\varphi^*)$. By functoriality the map φ_Φ factors through f_Φ, and we get the injective homomorphisms

$$\mathcal{H}_D \hookrightarrow \ker(\varphi_\Phi)[p^\infty] \hookrightarrow \mathrm{coker}(\varphi^*)[p^\infty].$$

Let $\delta_k := \ker(\mathcal{D}_k^0 \to \hat{\mathcal{D}}_k^0)[p^\infty]$, so δ_k is a finite connected multiplicative group scheme over k. The Cartier dual $\delta_k^\vee$ is canonically isomorphic to $\mathrm{coker}(\varphi^*)[p^\infty]$. For any finite multiplicative k-group scheme G_k there is a unique multiplicative finite flat

R-group scheme $\widetilde{G}$ with closed fibre G_k. A moment of thought shows that we have a natural closed immersion $\widetilde{\delta}_K \hookrightarrow \ker(\varphi_K)$, cf. [3, p.762]. Let $D^\perp$ be the abelian subvariety of B which is the kernel of $\hat{f}_K \circ \hat{\theta}$, so $\ker(\varphi_K) = D \cap D^\perp$ and $\widetilde{\delta}_K \hookrightarrow (D \cap D^\perp)$. Hence $\mathcal{H}_D^\vee \hookrightarrow (D \cap D^\perp)$, and in particular $\mathcal{H}_A^\vee \hookrightarrow (A \cap \hat{C})$. We are assuming that D has toric reduction. Therefore, the closed immersion f_K factors through $D \hookrightarrow A \hookrightarrow B$. By functoriality we get the exact sequence

$$0 \to \ker(\Phi_D \to \Phi_A) \to \ker(\Phi_D \to \Phi_B) \to \ker(\Phi_A \to \Phi_B).$$

By Corollary 2.4 the map $\Phi_D \to \Phi_A$ is injective on p-torsion, so $\mathcal{H}_D \hookrightarrow \mathcal{H}_A$. Combining all the inclusions we have established so far, we get two injective homomorphisms

$$\mathcal{H}_D^\vee \hookrightarrow (A \cap \hat{C}) \quad \text{and} \quad \mathcal{H}_D^\vee \hookrightarrow (D \cap D^\perp).$$

Now note that these two injections are induced from the same map, namely from the lifting of δ_k to the toric part of the p-divisible group of B, cf. [11, Ch.5]. Hence there is an injection $\mathcal{H}_D^\vee \hookrightarrow (A \cap \hat{C} \cap D \cap D^\perp) \subseteq (D \cap \hat{C})$. □

2.3. **Maps between character groups.** In this subsection we again, as in §2.1, will primarily be dealing with abelian varieties having toric reduction. Let

$$0 \to A \xrightarrow{f_K} B \xrightarrow{\pi_K} C \to 0 \tag{2.6}$$

be an exact sequence of abelian varieties over K. Assume B has toric reduction over K, and is principally polarized: $\theta : \hat{B} \xrightarrow{\sim} B$. Since B has toric reduction, any subvariety or a quotient of B also has toric reduction. In particular, A and C have toric reduction. As we mentioned, it is well-known that optimal quotients are exactly the duals of closed immersions, i.e., $\hat{\pi}_K$ identifies $\hat{C}$ with a subvariety of $\hat{B} = B$. To simplify the notation, in this subsection we denote $\mathcal{A}_k^0$ by T_A, $\mathcal{B}_k^0$ by T_B and etc.

Consider the polarization $\varphi_K := \hat{f}_K \circ \hat{\theta} \circ f_K : A \to \hat{A}$. Let $\varphi_t : T_A \to T_{\hat{A}}$ be the induced map on the closed fibres of the Néron models. This last map is an isogeny, by functoriality, so $\ker(\varphi_t)$ is a finite multiplicative k-group scheme. Let $\widetilde{\ker(\varphi_t)}$ be the unique multiplicative finite flat R-group scheme with closed fibre $\ker(\varphi_t)$. We have a closed immersion $\widetilde{\ker(\varphi_t)}_K \hookrightarrow \ker(\varphi_K)$, and the dual quotient map $\ker(\varphi_K)^\vee \to \widetilde{\ker(\varphi_t)}_K^\vee$. Since φ_K is a polarization, there is a canonical isomorphism $\ker(\varphi_K) \cong \ker(\varphi_K)^\vee$, so we get a quotient map $\ker(\varphi_K) \to \widetilde{\ker(\varphi_t)}_K^\vee$.

Theorem 2.8. *The sequence of finite K-group schemes*

$$0 \to \widetilde{\ker(\varphi_t)}_K \to \ker(\varphi_K) \to \widetilde{\ker(\varphi_t)}_K^\vee \to 0$$

is exact.

Proof. For the proof see [3, Thm.8.6]. This is essentially an explicit version of Grothendieck's *Orthogonality Theorem* [11] in the special case of toric reduction. □

From now on we assume that R has characteristic $p > 0$. Consider the connected subgroup scheme $\ker(\varphi_K)^0$ of $\ker(\varphi_K)$. Theorem 2.8 implies that $\ker(\varphi_K)^0$ is canonically isomorphic to the Cartier dual of $\mathrm{coker}(\varphi^* : M_{\hat{A}} \to M_A)[p^\infty]$. To proceed further, we need to introduce more terminology.

The image of $M_{\hat{A}}$ in $M_{\hat{B}} \overset{\theta}{=} M_B$ under $\hat{f}^*$ need not be saturated, i.e., the quotient group $M_B/(\hat{f}^* M_{\hat{A}})$ might have torsion. We denote by

$$\overline{M}_{\hat{A}} = ((\hat{f}^* M_{\hat{A}}) \otimes \mathbb{Q}) \cap M_B \tag{2.7}$$

the *saturation* of $\hat{f}^* M_{\hat{A}}$ inside M_B, and likewise by $\overline{M}_C$ the saturation of $\pi^* M_C$ inside M_B. It is easy to see that $\overline{M}_C \cap \overline{M}_{\hat{A}} = 0$. Moreover, the abelian group $\mathcal{S}_{A,C} := M_B/(\overline{M}_C \oplus \overline{M}_{\hat{A}})$ is finite.

Let $0 \to D \to B \to X \to 0$ be an exact sequence of abelian varieties, where B is the same variety as in (2.6). Let ϕ_K be the polarization on D analogous to φ_K.

Proposition 2.9. *The finite K-group schemes* $\ker(\varphi_K)$ *and* $\ker(\phi_K)$*, considered as subgroup schemes of B, share a common non-trivial connected subgroup if and only if there is an element in M_B which maps to a non-trivial p-power torsion element both in $\mathcal{S}_{A,C}$ and in $\mathcal{S}_{D,X}$ (under the natural quotient maps).*

Proof. Denote the condition of the non-triviality of the intersection $\ker(\varphi_K)^0 \cap \ker(\phi_K)^0$ in B by $(*)$.

Define an isogeny $T_B \xrightarrow{\alpha} T_{\hat{A}} \times T_C$, where $\alpha = (\alpha_1, \alpha_2)$ with α_2 being the natural quotient map $T_B \to T_C$, and α_1 being 1 on $T_{\hat{C}}$ and φ_t on T_A. (Note that we implicitly use Corollary 2.4 to identify T_A and $T_{\hat{C}}$ with subtori of T_B.) The map α is well-defined since $\ker(\varphi_t) = T_A \cap T_{\hat{C}}$. It is easy to see that $\ker(\alpha) = \ker(\varphi_t)$. Define a similar isogeny $T_B \xrightarrow{\beta} T_{\hat{D}} \times T_X$. Using Theorem 2.8, we get that $(*)$ holds if and only if the kernel of the homomorphism

$$T_B \xrightarrow{(\alpha,\beta)} (T_{\hat{A}} \times T_C) \times (T_{\hat{D}} \times T_X)$$

has a non-trivial connected subgroup scheme. Taking the duals, this can be restated as the condition on the existence of an element in M_B which maps to a non-trivial p-power torsion element in both $M_B/(M_{\hat{A}} \oplus M_C)$ and $M_B/(M_{\hat{D}} \oplus M_X)$. (Here we omit $\hat{f}^*$, π^*, and etc. from notation.) Next, we study these finite abelian groups in more detail. Consider the sequence

$$M_{\hat{A}} \oplus M_C \to \overline{M}_{\hat{A}} \oplus \overline{M}_C \to M_B.$$

Both maps are clearly injective, so we have the short-exact sequence

$$0 \to \frac{\overline{M}_{\hat{A}}}{M_{\hat{A}}} \oplus \frac{\overline{M}_C}{M_C} \to \frac{M_B}{M_{\hat{A}} \oplus M_C} \to \frac{M_B}{\overline{M}_{\hat{A}} \oplus \overline{M}_C} \to 0.$$

We claim that the group on the left-hand side has no p-torsion. If we assume this for a moment then the proposition follows from what we have established so far.

It remains to show that $\overline{M}_C/M_C$ has no p-torsion (the argument for $\overline{M}_{\hat{A}}/M_{\hat{A}}$ is similar). Consider the commutative diagram arising from Theorem 2.5

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_B & \xrightarrow{u_B} & \mathrm{Hom}(M_B, \mathbb{Z}) & \longrightarrow & \Phi_B & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \hat{\pi}^*} & & \downarrow{\scriptstyle \mathrm{Hom}(\pi^*, \mathbb{Z})} & & \downarrow{\scriptstyle \pi_\Phi} & & \\
0 & \longrightarrow & M_{\hat{C}} & \xrightarrow{u_C} & \mathrm{Hom}(M_C, \mathbb{Z}) & \longrightarrow & \Phi_C & \longrightarrow & 0.
\end{array}$$

Since $\hat{C} \xrightarrow{\hat{\pi}} B$ is a closed immersion, the left vertical arrow is surjective by [3, Thm.8.2]. Thus, from the snake lemma

$$\#\mathrm{coker}(\pi_\Phi) = \#\mathrm{Ext}^1_{\mathbb{Z}}(M_B/\pi^* M_C, \mathbb{Z}) = \#(M_B/\pi^* M_C)_{\mathrm{tor}} = \#(\overline{M}_C/\pi^* M_C).$$

By [11, pp.5-6], $\mathrm{coker}(\pi_\Phi) \cong \mathrm{Hom}_{\mathbb{Z}}(\ker(\hat{\pi}_\Phi), \mathbb{Q}/\mathbb{Z})$. Hence the claim follows from Corollary 2.4. $\square$

Corollary 2.10. *With notation and assumptions of Proposition 2.9, also assume that $D \cap \hat{C}$ is finite. Then the order of $D \cap \hat{C}$ is divisible by p if and only if $\mathcal{S}_{D,C} := M_B/(\overline{M}_C \oplus \overline{M}_{\hat{D}})$ has p-torsion.*

Proof. Denote $G := D \cap \hat{C}$. If G is finite then $D \subseteq A$, i.e., the closed immersion $D \to B$ factors through f_K. Indeed, it is clear from (2.6) that $A \cap D$ has dimension equal to $\dim(D)$, so is dense in D. Since it is also proper, we must have $A \cap D = D$. Similarly, $\hat{C} \subseteq \hat{X}$. These two inclusions imply that $G = (A \cap \hat{C}) \cap (D \cap \hat{X})$. On the other hand, it is easy to see that $\ker(\varphi_K) = A \cap \hat{C}$ and $\ker(\phi_K) = D \cap \hat{X}$. Thus, $G = \ker(\varphi_K) \cap \ker(\phi_K)$. The group schemes on the right hand-side are self-dual, being kernels of polarizations, so G is also self-dual with respect to the Cartier duality. This implies that $\#G$ is divisible by p if and only if G^0 is non-trivial, which is also equivalent to the existence of a common non-trivial connected subgroup scheme of $\ker(\varphi_K)$ and $\ker(\phi_K)$. By Proposition 2.9 this last condition is equivalent to the existence of an element in M_B which maps to a non-trivial p-power torsion element in both $\mathcal{S}_{A,C}$ and $\mathcal{S}_{D,X}$. More explicitly, there is an element $v \in M_B$ such that $v \notin \overline{M}_C \oplus \overline{M}_{\hat{A}}$ and $v \notin \overline{M}_X \oplus \overline{M}_{\hat{D}}$, but $p^n \cdot v$ lies in both subgroups for some large enough $n \geq 1$. Since $\overline{M}_C \subseteq \overline{M}_X$ and $\overline{M}_{\hat{D}} \subseteq \overline{M}_{\hat{A}}$, we get $v \notin \overline{M}_C \oplus \overline{M}_{\hat{D}}$ and $p^n \cdot v \in \overline{M}_C \oplus \overline{M}_{\hat{D}}$. That is, $\mathcal{S}_{D,C}$ has p-power torsion. (Note that $\mathcal{S}_{D,C}$ need not be finite anymore.)

Conversely, suppose $\mathcal{S}_{D,C}$ has p-power torsion. Let v be a fixed element of M_B such that $v \notin \overline{M}_C \oplus \overline{M}_{\hat{D}}$ but $p^n \cdot v \in \overline{M}_C \oplus \overline{M}_{\hat{D}}$. Since $\overline{M}_{\hat{D}} \subseteq \overline{M}_{\hat{A}}$ and $\overline{M}_{\hat{A}} \cap \overline{M}_C = 0$, there is an exact sequence

$$0 \to \frac{\overline{M}_{\hat{A}}}{\overline{M}_{\hat{D}}} \to \frac{M_B}{\overline{M}_C \oplus \overline{M}_{\hat{D}}} \to \frac{M_B}{\overline{M}_C \oplus \overline{M}_{\hat{A}}} \to 0.$$

Since $\overline{M}_{\hat{D}}$ is saturated, $\overline{M}_{\hat{A}}/\overline{M}_{\hat{D}}$ is free. This implies that v maps to a non-trivial p-power torsion element in $\mathcal{S}_{A,C}$. Applying the same argument with the roles of C and $\hat{D}$ interchanged, we get that *the same* element v also maps to p-power torsion in $\mathcal{S}_{D,X}$. Again from Proposition 2.9 we conclude that G^0 is non-trivial. $\square$

3. Drinfeld modular curves and harmonic cochains

Let $F = \mathbb{F}_q(t)$ be the field of rational functions on $\mathbb{P}^1_{\mathbb{F}_q}$. Let $A = \mathbb{F}_q[t]$ be the subring of F consisting of functions which are regular away from $\infty := 1/t$. For a prime ideal $\mathfrak{p}$ of the Dedekind domain A we denote the completion of A at $\mathfrak{p}$ by $A_\mathfrak{p}$, the fraction field of $A_\mathfrak{p}$ by $F_\mathfrak{p}$, and the residue field $A_\mathfrak{p}/\mathfrak{p}$ by $\mathbb{F}_\mathfrak{p}$. Denote the completion of F at ∞ by K, the ring of integers in K by R, and the residue field at ∞ by k. Let the prime number p be the characteristic of F. In this section we review some facts about Drinfeld modular curves which we will need in our later discussions.

3.1. **Drinfeld modular curves.** Let $\mathfrak{n}$ be an ideal in A. The functor which associates to an A-scheme S the set of isomorphism classes of pairs $(D, Z_\mathfrak{n})$, where D is a Drinfeld module of rank 2 over S and $Z_\mathfrak{n}$ is a $\mathfrak{n}$-cyclic subgroup of D, possesses a coarse moduli scheme $M_0(\mathfrak{n})/A$ that is affine of finite type over A, and is A-flat with pure relative dimension 1. There is a canonical compactification $X_0(\mathfrak{n})$ of $M_0(\mathfrak{n})$ over $\mathrm{Spec}(A)$; see [5, §9].

Let $\Omega = \mathbb{P}^1_K - \mathbb{P}^1_K(K)$ be the *Drinfeld upper half-plane.* Ω has a natural structure of a smooth connected rigid-analytic space. Denote by $\Gamma_0(\mathfrak{n})$ the *Hecke congruence subgroup* of level $\mathfrak{n}$:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \mid c \in \mathfrak{n} \right\}.$$

In this section we assume that $\mathfrak{n}$ is fixed and, to simplify the notation, let $\Gamma = \Gamma_0(\mathfrak{n})$. The group Γ naturally acts on Ω via linear fractional transformations, and the action is *discrete* in the sense of [5, p.582]. Hence we may construct the quotient $\Gamma \setminus \Omega$ as a 1-dimensional connected smooth analytic space over K.

The following theorem can be deduced from the results in [5]:

Theorem 3.1.

(a) $X_0(\mathfrak{n})$ *is a proper, normal, flat, irreducible scheme of pure relative dimension* 1 *over* $\mathrm{Spec}(A)$.

(b) $X_0(\mathfrak{n}) \to \mathrm{Spec}A\left[\mathfrak{n}^{-1}\right]$ *is smooth.*

(c) $X_0(\mathfrak{n})_F$ *is a smooth, proper, geometrically connected curve over* F.

(d) *There is an isomorphism of rigid-analytic spaces* $\Gamma \setminus \Omega \cong M_0(\mathfrak{n})_K^{\mathrm{an}}$.

3.2. **Cuspidal harmonic cochains.** Let $\mathcal{T}$ be the *Bruhat-Tits tree* of $\mathrm{PGL}_2(K)$; see [9, §1] for the definition. We denote by $X(\mathcal{T})$ and $Y(\mathcal{T})$ the vertices and the oriented edges of $\mathcal{T}$, respectively. There is a natural action of Γ on $\mathcal{T}$ as a coset space of $\mathrm{GL}_2(K)$. This action preserves the simplicial structure of $\mathcal{T}$. For an edge $e \in Y(\mathcal{T})$ we denote by $\bar{e}$, $t(e)$, $o(e)$ the inversely oriented edge, the terminus of e, and the origin of e, respectively. For any abelian group B, let $S(\Gamma, B)$ be the group of maps $Y(\mathcal{T}) \to B$ subject to

(i) $\varphi(\bar{e}) = -\varphi(e)$ for any $e \in Y(\mathcal{T})$;

(ii) $\sum_{t(e)=v} \varphi(e) = 0$ for any $v \in X(\mathcal{T})$;

(iii) $\varphi(\gamma e) = \varphi(e)$ for any $\gamma \in \Gamma$;

(iv) φ has compact (=finite) support modulo Γ.

We call this group the *group of B-valued cuspidal harmonic cochains* for Γ, cf. [9, §3]. Using the *strong approximation theorem* for function fields, it can be shown that $S(\Gamma, \mathbb{C})$ may be interpreted as a space of automorphic cusp forms on $\mathrm{GL}_2(\mathbb{A}_F)$ which are special at ∞; see [9, §4]. This space plays a role similar to the role of weight-2 cusp forms of fixed level in the classical theory. From the definition it is easy to see that for any ring $\mathcal{O}$ contained in $\mathbb{C}$, in particular for $\mathbb{C}$ itself, there is the canonical isomorphism $S(\Gamma, \mathcal{O}) = S(\Gamma, \mathbb{Z}) \otimes \mathcal{O}$. This is the analogue of the fact that the space of weight-2 cusp forms has a basis consisting of cusp forms with integral Fourier coefficients. Thus, $S(\Gamma, \mathbb{C})$ has a canonical integral structure given by $S(\Gamma, \mathbb{Z})$.

3.3. **Hecke algebra.** Following [7, (1.10)], for any ideal $\mathfrak{m}$ of A we define a Hecke operator $T_\mathfrak{m}$ acting on $S(\Gamma, \mathbb{C})$. This is derived from a correspondence on $Y(\mathcal{T}) = \Gamma \setminus \mathrm{GL}_2(K)/\mathcal{I} \cdot Z(K)$, where $\mathcal{I}$ is the Iwahori group at ∞. Any function $\varphi \in S(\Gamma, \mathbb{C})$ can be considered as a function on $\mathrm{GL}_2(K)$. Define

$$T_\mathfrak{m}\varphi(g) = \sum \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} g\right),$$

where the sum is over $a, b, d \in A$ such that a, d are monic, the ideal (ad) is $\mathfrak{m}$, a is coprime to $\mathfrak{n}$, and $\deg b < \deg d$. We call $T_\mathfrak{m}$ the $\mathfrak{m}$*-th Hecke operator*. The Hecke operators commute with each other, and satisfy recursive relationships which allow to express each $T_\mathfrak{m}$ in terms of a polynomial with integral coefficients in $T_\mathfrak{p}$'s, where the $\mathfrak{p}$'s are the prime divisors of $\mathfrak{m}$. Let $\mathbb{T} := \mathbb{Z}[\dots, T_\mathfrak{m}, \dots]$ be the commutative $\mathbb{Z}$-algebra generated by the Hecke operators acting on $S(\Gamma, \mathbb{C})$. It is clear from the definition that $\mathbb{T}$ preserves the integral structure $S(\Gamma, \mathbb{Z})$, and since it is known that $S(\Gamma, \mathbb{Z})$ is a finitely generated free $\mathbb{Z}$-module, $\mathbb{T}$ is a finitely generated free $\mathbb{Z}$-module.

There is an equivalent "modular" definition of the $T_\mathfrak{m}$ as a correspondence on $X_0(\mathfrak{n})$ given by

$$(D, Z_\mathfrak{n}) \mapsto \sum_{Z_\mathfrak{m} \cap Z_\mathfrak{n} = 0} (D/Z_\mathfrak{m}, (Z_\mathfrak{n} + Z_\mathfrak{m})/Z_\mathfrak{m}).$$

Let $J = J_0(\mathfrak{n})$ be the Jacobian variety of $X_0(\mathfrak{n})_F$. Thus $T_\mathfrak{m}$ induces an endomorphism of J, and we can consider the commutative subalgebra $\mathbb{T} \subseteq \mathrm{End}_F(J)$ generated by the Hecke operators. Let $V_\ell(J)$ be the ℓ-adic Tate vector space of J, $\ell \neq p$. As a consequence of a theorem of Zarhin, there is a canonical isomorphism

$$\mathrm{End}_F(J) \otimes \mathbb{Q}_\ell = \mathrm{End}_{\mathrm{Gal}(F^{\mathrm{sep}}/F)}(V_\ell(J))$$

Hence $\mathbb{T}$ is naturally a subalgebra of $\mathrm{End}(V_\ell(J))$. The fundamental theorem of Drinfeld [5, Thm.2], among other things, relates the two Hecke algebras we defined:

Theorem 3.2 (Drinfeld)**.** *There is a canonical isomorphism between* $V_\ell(J)^*$ *and* $S(\Gamma, \mathbb{Q}_\ell) \otimes \mathrm{sp}(2)$ *compatible with the action of* $\mathbb{T}$*, where* $\mathrm{sp}(2)$ *is the two-dimensional special* ℓ*-adic representation of* $\mathrm{Gal}(K^{\mathrm{sep}}/K)$*, and* $V_\ell(J)^* = \mathrm{Hom}(V_\ell(J), \mathbb{Q}_\ell)$*.*

One can conclude from this theorem that the abelian subvarieties of J which are stable under the action of $\mathbb{T}$ as a subalgebra of $\mathrm{End}_F(J)$ are in one-to-one correspondence with the $\mathbb{T}$-stable subspaces of $S(\Gamma, \mathbb{Q})$.

It is well-known that the existence of the rigid-analytic uniformization in Theorem 3.1(d) implies that J has split toric reduction over K. Denote by $\mathcal{J}$ the Néron model of J over R, and let M_J be the character group of $\mathcal{J}_k^0$, cf. §2.2. By the Néron mapping property, any endomorphism of J uniquely extends to an endomorphism of $\mathcal{J}$. Specializing to the closed fibre, we get a natural homomorphism $\mathrm{End}_K(J) \to \mathrm{End}_k(\mathcal{J}_k^0)$. Since J has a toric (in particular, semi-abelian) reduction, this homomorphism is injective. On the other hand, since $\mathcal{J}_k^0$ is a split torus, there is a canonical isomorphism $\mathrm{End}_k(\mathcal{J}_k^0) \cong \mathrm{End}_\mathbb{Z}(M_J)$. Thus, we find a faithful representation $\mathbb{T} \to \mathrm{End}_\mathbb{Z}(M_J)$.

Proposition 3.3. *There is a canonical isomorphism of* $\mathbb{T}$*-modules* $M_J \xrightarrow{\cong} S(\Gamma, \mathbb{Z})$*.*

Proof. Let $\overline{\Gamma} := \Gamma^{\mathrm{ab}}/(\Gamma^{\mathrm{ab}})_{\mathrm{tor}}$. One can show, cf. [9, (3.2)], that $\overline{\Gamma}$ is a free abelian group of rank $g = $genus$(X_0(\mathfrak{n}))$. Moreover, by [8] there is a canonical isomorphism $j : \overline{\Gamma} \xrightarrow{\sim} S(\Gamma, \mathbb{Z})$. In [9, (9.3)] Gekeler and Reversat define a natural action of $\mathbb{T}$ on $\overline{\Gamma}$ and show that j is an isomorphism of $\mathbb{T}$-modules. Next, recall one of the principal results of [9], which says that there is an exact sequence

$$1 \to \overline{\Gamma} \xrightarrow{\bar{c}} \mathrm{Hom}(\overline{\Gamma}, \mathbb{G}_{m,K}^{\mathrm{an}}) \to J^{\mathrm{an}} \to 1, \tag{3.1}$$

where $\bar{c}$ is an explicit rigid-analytic period. Moreover, (3.1) is $\mathbb{T}$-equivariant in the following sense, cf. [9, (9.4)]: $T^{\mathrm{an}} := \mathrm{Hom}(\overline{\Gamma}, \mathbb{G}_{m,K}^{\mathrm{an}})$ is the universal covering space of J^{an} in the rigid-analytic category, and hence every endomorphism of J^{an} uniquely lifts to an endomorphism of the torus T^{an}. Since the endomorphisms of a split analytic torus are algebraic, $\mathrm{End}_K(T^{\mathrm{an}}) \cong \mathrm{End}_{\mathbb{Z}}(\overline{\Gamma})$. So we get two actions of $\mathbb{T}$ on $\overline{\Gamma}$, and the equivariance is expressed in the fact that these two actions are the same.

Now we recall a more abstract description of the analytic uniformization of J which brings into the picture the character group M_J. Let $\mathcal{J}^0$ be the relative connected component of the identity of $\mathcal{J}$, i.e., the largest open subscheme of $\mathcal{J}$ containing the identity section which has connected fibres. The rigidity of tori [10, Thm. 3.6] implies that the formal completion of $\mathcal{J}^0$ along its closed fibre is uniquely isomorphic to a formal split torus $\mathfrak{T} = (\mathrm{Spf}\ R\langle z, z^{-1}\rangle)^g$ respecting a choice of isomorphism $\mathcal{J}^0_k \cong \mathbb{G}^g_{m,k}$. Applying Raynaud's "generic fibre" functor, we get an open immersion of analytic groups $i : \mathfrak{T}^{\mathrm{rig}} \hookrightarrow J^{\mathrm{an}}$. We also have the analytic torus $T^{\mathrm{an}} = (\mathbb{G}^{\mathrm{an}}_{m,K})^g$ associated to $\mathfrak{T}^{\mathrm{rig}}$ and an open immersion $\mathfrak{T}^{\mathrm{rig}} \hookrightarrow T^{\mathrm{an}}$. The key fact is that i extends uniquely to a rigid-analytic group morphism $T^{\mathrm{an}} \to J^{\mathrm{an}}$, and its kernel is a lattice $\Lambda \subset (K^\times)^g$ of rank g. This induces an isomorphism of analytic groups $T^{\mathrm{an}}/\Lambda \cong J^{\mathrm{an}}$; see [1, Thm. 1.2]. This construction is compatible with respect to the action of $\mathrm{End}_K(J)$ on the groups involved. Hence the action of $\mathbb{T}$ on the tori $\mathcal{J}^0_k \to \mathfrak{T} \to \mathfrak{T}^{\mathrm{rig}} \to T^{\mathrm{an}}$ is compatible with the canonical maps between them. In particular, using the flanking terms, we see that M_J and $\overline{\Gamma}$ are canonically isomorphic $\mathbb{T}$-modules. Combining this with the isomorphism j gives the claim. □

The upshot of this proposition is that the $\mathbb{T}$-stable subvarieties of J are in one-to-one correspondence with the saturated $\mathbb{T}$-stable subgroups of M_J. Moreover, the congruences between cusp forms can be deduced from the congruences between the elements of M_J. The dictionary between $S(\Gamma, \mathbb{Z})$ and M_J goes even further. Since $S(\Gamma, \mathbb{Z})$ is a lattice in a space of automorphic forms, there is a positive definite (a priori) $\mathbb{C}$-valued pairing on this group, which comes from the Petersson inner product on the space of cusp forms. For a particular choice of the Haar measure on $Y(\Gamma \setminus \mathcal{T})$ this pairing is $\mathbb{Z}$-valued and turns out to be equal to the monodromy pairing on M_J; see [15, Prop.4.5].

4. Congruences

4.1. **Congruence primes.** We keep the notation of §3.

Definition 4.1. Let A and B be two subvarieties of $J = J_0(\mathfrak{n})$ which are stable under the action of $\mathbb{T} \subseteq \mathrm{End}(J)$. Let S_A and S_B be the unique saturated $\mathbb{T}$-stable subgroups of $S(\Gamma, \mathbb{Z})$ corresponding to A and B, which exist by Theorem 3.2. We say that a prime ℓ is a *geometric congruence prime* for A and B if $A \cap B$ is a finite F-group scheme, with the intersection taken in J, and ℓ divides $\#(A \cap B)$. We say that ℓ is an *automorphic congruence prime* for A and B if $S_A \cap S_B = 0$ and ℓ divides $\#(S(\Gamma, \mathbb{Z})/(S_A \oplus S_B))_{\mathrm{tor}}$.

Proposition 4.2. *With A and B as in Definition 4.1, the prime p is a geometric congruence prime if and only if it is an automorphic congruence prime.*

Proof. Denote by $\pi : J \to \hat{A}$ the quotient which is dual to the closed immersion of A into J. Let $M_{\hat{A}}$ be the character group of the Néron model of $\hat{A}$ over R. Let $\overline{M}_{\hat{A}}$ be the saturation of $\pi^*(M_{\hat{A}})$ in M_J, cf. (2.7). Denote by $\overline{M}_{\hat{B}}$ the similar group for

B. From the definition of the action of $\mathbb{T}$ on M_J it is clear that $\overline{M}_{\hat{A}}$ and $\overline{M}_{\hat{B}}$ are $\mathbb{T}$-stable. It is also clear that $\overline{M}_{\hat{A}}$ can be identified with S_A under the isomorphism of Proposition 3.3, and similarly for $\overline{M}_{\hat{B}}$. Moreover

$$S(\Gamma, \mathbb{Z})/(S_A \oplus S_B) = M_J/(\overline{M}_{\hat{A}} \oplus \overline{M}_{\hat{B}}). \tag{4.1}$$

Next, if $A \cap B$ is finite then $\overline{M}_{\hat{A}} \cap \overline{M}_{\hat{B}} = 0$. The easy proof of this fact is implicitly contained in the proof of Corollary 2.10. Conversely, if $A \cap B$ is not finite then it is an abelian subvariety of J, so must have toric reduction over K. In particular, $\mathcal{A}_k^0 \cap \mathcal{B}_k^0 \subseteq \mathcal{J}_k^0$ has dimension at least 1. This implies $\mathrm{rank}_{\mathbb{Z}}(\overline{M}_{\hat{A}} \cap \overline{M}_{\hat{B}}) \geq 1$. We conclude that $A \cap B$ is finite if and only if $S_A \cap S_B = 0$. Using this fact and (4.1), the proposition follows from Corollary 2.10. □

4.2. **Main theorems.** Let $\mathfrak{p}$ be a prime ideal of degree d, and let $\mathfrak{n} = \mathfrak{p}\mathfrak{m}$, with $\mathfrak{m}$ coprime to $\mathfrak{p}$. Recall the two natural degeneracy maps $\alpha, \beta : M_0(\mathfrak{n}) \rightrightarrows M_0(\mathfrak{m})$, where α, β are induced by the maps defined in terms of the moduli problem

$$\alpha : (D, Z_{\mathfrak{p}} Z_{\mathfrak{n}}) \mapsto (D, Z_{\mathfrak{n}})$$
$$\beta : (D, Z_{\mathfrak{p}} Z_{\mathfrak{n}}) \mapsto (D/Z_{\mathfrak{p}}, Z_{\mathfrak{p}} Z_{\mathfrak{n}}/Z_{\mathfrak{p}}).$$

These morphisms uniquely extend to $X_0(\mathfrak{n})$ and $X_0(\mathfrak{m})$. By the Picard functoriality we get two homomorphisms $J_0(\mathfrak{m}) \rightrightarrows J_0(\mathfrak{n})$. The subvariety of $J_0(\mathfrak{n})$ generated by the images of these homomorphisms is called *the* $\mathfrak{p}$*-old subvariety*, and is denoted by $J_0(\mathfrak{n})^{\mathfrak{p}-\mathrm{old}}$. The quotient abelian variety $J_0(\mathfrak{n})/J_0(\mathfrak{n})^{\mathfrak{p}-\mathrm{old}}$ is called *the* $\mathfrak{p}$*-new quotient* of $J_0(\mathfrak{n})$ and is denoted $J_0(\mathfrak{n})_{\mathfrak{p}-\mathrm{new}}$. Taking the dual of the quotient map $J_0(\mathfrak{n}) \to J_0(\mathfrak{n})_{\mathfrak{p}-\mathrm{new}}$ defines a subvariety of $J_0(\mathfrak{n})$, *the* $\mathfrak{p}$*-new subvariety*, and is denoted by $J_0(\mathfrak{n})^{\mathfrak{p}-\mathrm{new}}$. In this subsection we assume that $\mathfrak{p}$ and $\mathfrak{n}$ are fixed, and to simplify the notation we let $J, J^{\mathrm{old}}, J^{\mathrm{new}}$ denote the Drinfeld Jacobian $J_0(\mathfrak{n})$ and its corresponding $\mathfrak{p}$-old and $\mathfrak{p}$-new subvarieties. $J^{\mathrm{new}} \cap J^{\mathrm{old}}$ is finite, and $\mathbb{T}$ preserves both J^{old} and J^{new}. We can identify the corresponding $\mathbb{T}$-stable subgroups of $S(\Gamma_0(\mathfrak{n}), \mathbb{Z})$ as follows. There are two natural injections $S(\Gamma_0(\mathfrak{m}), \mathbb{Q}) \rightrightarrows S(\Gamma_0(\mathfrak{n}), \mathbb{Q})$. The $\mathbb{Q}$-linear subspace $S(\mathbb{Q})^{\mathfrak{p}-\mathrm{old}}$ generated by the images is the $\mathfrak{p}$*-old subspace.* The intersection $S(\mathbb{Z})^{\mathrm{old}} := S(\Gamma_0(\mathfrak{n}), \mathbb{Z}) \cap S(\mathbb{Q})^{\mathfrak{p}-\mathrm{old}}$ is the $\mathbb{T}$-stable saturated subgroup corresponding to J^{old}. The subgroup $S(\mathbb{Z})^{\mathrm{new}}$ corresponding to J^{new} is the orthogonal complement in $S(\Gamma, \mathbb{Z})$ of $S(\mathbb{Z})^{\mathrm{old}}$ with respect to the Petersson norm (equiv. with respect to the monodromy pairing on M_J, cf. §3.3).

Next, we claim that J^{new} is the maximal toric subvariety of J over $F_{\mathfrak{p}}$ in the sence of §2.2. To see this we need to recall the structure of $X_0(\mathfrak{n})$ over $A_{\mathfrak{p}}$.

A Drinfeld module D over an extension of $\mathbb{F}_{\mathfrak{p}}$ is called *supersingular* if its $\mathfrak{p}$-torsion is connected, cf. [6]. Consider $X_0(\mathfrak{m})$ over $\mathrm{Spec}(A_{\mathfrak{p}})$. It is smooth by Theorem 3.1. We will call the points of $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_{\mathfrak{p}}}$ represented by pairs $(D, Z_{\mathfrak{m}})$, with D supersingular, the *supersingular points.* There are only finitely many of these. The automorphism group $\mathrm{Aut}(D, Z_{\mathfrak{m}})$ of a pair $(D, Z_{\mathfrak{m}})$ is defined in an obvious manner. It is known that there are inclusions of groups $\mathbb{F}_q^{\times} \subseteq \mathrm{Aut}(D, Z_{\mathfrak{m}}) \subseteq \mathrm{Aut}(D) \subseteq \mathbb{F}_{q^2}^{\times}$. Let τ be the Frobenius endomorphism relative to $\mathbb{F}_q$, i.e., the map $x \mapsto x^q$. The endomorphism τ^d can be canonically identified with an involution of the set of supersingular points of $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_{\mathfrak{p}}}$. The following theorem, which is the analogue of [4, Thm. VI.6.9], describes the structure of the special fibre $X_0(\mathfrak{n})_{\overline{\mathbb{F}}_{\mathfrak{p}}}$. The proof of the theorem in case $\mathfrak{n} = \mathfrak{p}$ is carefully discussed in [6].

Theorem 4.3.

(a) *The special fibre* $X_0(\mathfrak{n})_{\overline{\mathbb{F}}_\mathfrak{p}}$ *is reduced and is a union of two copies of the smooth curve* $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_\mathfrak{p}}$*, intersecting transversally at the supersingular points. The supersingular point* x *on the first copy of* $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_\mathfrak{p}}$ *is glued to* $\tau^d(x)$ *on the second copy.*

(b) *Let* x *be a supersingular point of* $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_\mathfrak{p}}$ *defined by a pair* $(D, Z_\mathfrak{m})$*, and let* $n := \frac{1}{q-1}\#\mathrm{Aut}(D, Z_\mathfrak{m})$*. Then*

$$\widehat{\mathcal{O}^{\mathrm{sh}}_{X_0(\mathfrak{n}),x}} \cong \widehat{A^{\mathrm{sh}}_\mathfrak{p}}[\![v, w]\!]/(v \cdot w - \mathfrak{p}^n).$$

Using Theorem 4.3 and Raynaud's theorem of specializations of the Picard functor, cf. [2, Ch.9], one concludes that J^{new} has toric reduction over $F_\mathfrak{p}$ and the quotient J/J^{new} has good reduction (being isogenous to $J^{\mathrm{old}} \times J^{\mathrm{old}}$). Thus, J^{new} is the maximal toric subvariety of J over $F_\mathfrak{p}$ by Lemma 2.6.

Let A be a subvariety of J with toric reduction over $F_\mathfrak{p}$. Hence A is "new" at $\mathfrak{p}$, i.e., $A \hookrightarrow J^{\mathrm{new}}$. Denote by $\Phi_{J,\mathfrak{p}}$ and $\Phi_{A,\mathfrak{p}}$ the component groups of the Néron models of J and A over $A_\mathfrak{p}$.

Theorem 4.4 (Level lowering)**.** *Suppose that the kernel of the homomorphism* $\Phi_{A,\mathfrak{p}} \to \Phi_{J,\mathfrak{p}}$*, functorially induced from the closed immersion* $A \hookrightarrow J$*, has non-trivial* p*-power torsion. Then* p *is an automorphic congruence prime for* A *and* J^{old}*.*

Proof. If $\ker(\Phi_{A,\mathfrak{p}} \to \Phi_{J,\mathfrak{p}})$ has p-torsion, then according to Proposition 2.7 the prime p is a geometric congruence prime for A and J^{old}. Thus, the claim follows from Proposition 4.2. □

Proposition 4.5. *If* $\mathfrak{n}$ *is square-free then for any prime* $\mathfrak{p}$ *dividing* $\mathfrak{n}$ *there is the congruence* $\#\Phi_{J,\mathfrak{p}} \equiv 1 \pmod p$*. In particular,* $\Phi_{J,\mathfrak{p}}$ *has no* p*-power torsion.*

Proof. The main ingredient of the proof is a result of Raynaud reproduced in a convenient form in [2, 9.6/10, 9.6/11]. Using *loc.cit.* and Theorem 4.3, one can actually determine the structure of $\Phi_{J,\mathfrak{p}}$. Since we are only interested in the mod-p order of this group, we will take a more direct route. Let the number of supersingular points on $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_\mathfrak{p}}$ be s. Denote these points by $x_1, \dots, x_s$. Let $(D, Z_\mathfrak{m})_i$ be the pair corresponding to x_i, and let $n_i = \frac{1}{q-1}\#\mathrm{Aut}(D, Z_\mathfrak{m})_i$. Then Raynaud's result implies that

$$\#\Phi_{J,\mathfrak{p}} = \sum_{i=1}^{s} \prod_{j \neq i} n_j.$$

As we mentioned, $\mathbb{F}_q^\times \subseteq \mathrm{Aut}(D, Z_\mathfrak{m})_i \subseteq \mathbb{F}_{q^2}^\times$. Using this, one easily shows that $\mathrm{Aut}(D, Z_\mathfrak{m})_i$ is either $\mathbb{F}_q^\times$ or $\mathbb{F}_{q^2}^\times$. Thus each n_i is either 1 or $q+1$, so

$$\#\Phi_{J,\mathfrak{p}} \equiv \sum_{i=1}^{s} 1 \equiv s \pmod p. \tag{4.2}$$

By blowing-up $X_0(\mathfrak{n})_{\overline{\mathbb{F}}_\mathfrak{p}}$ at the supersingular points, one obtains two disjoint copies of the smooth curve $X_0(\mathfrak{m})_{\overline{\mathbb{F}}_\mathfrak{p}}$. A standard argument gives the formula

$$g(X_0(\mathfrak{n})_{\overline{\mathbb{F}}_\mathfrak{p}}) = s - 1 + 2g(X_0(\mathfrak{m})_{\overline{\mathbb{F}}_\mathfrak{p}}), \tag{4.3}$$

where g denotes the arithmetic genus of the corresponding curve. On the other hand, since $X_0(\mathfrak{n})$ is flat, the arithmetic genus of $X_0(\mathfrak{n})_F$ is equal to the arithmetic genus of $X_0(\mathfrak{n})_{\overline{\mathbb{F}}_\mathfrak{p}}$. Note that so far we have not used the assumption on $\mathfrak{n}$ being square-free. The assumption enters as the fact that $g(X_0(\mathfrak{n})_F) \equiv 0 \pmod p$ when $\mathfrak{n}$ is square-free. This can be easily deduced from the formula for $g(X_0(\mathfrak{n})_F)$ in [8, Cor.2.19] (in general the congruence is false if $\mathfrak{n}$ is not square-free). Since $\mathfrak{m}$ is also square-free, we also have $g(X_0(\mathfrak{m})_F) \equiv 0 \pmod p$. Therefore, from (4.3) we get $s \equiv 1$, which combined with (4.2) gives the proposition. □

Let E be a semi-stable elliptic curve over F, which has split multiplicative reduction at ∞ and conductor $\mathfrak{n} \cdot \infty$. Denote the set of proper prime ideals $\mathfrak{p}$ of A dividing $\mathfrak{n}$ by Ξ.

Theorem 4.6. *If E is optimal then there is at least one $\mathfrak{p} \in \Xi$ such that $\Phi_{E,\mathfrak{p}}$ has no p-torsion. In particular,* $\deg_{\mathrm{ns}}(j_E) = 1$.

Proof. Since we assume E is semi-stable, the ideal $\mathfrak{n}$ is square-free and E has toric reduction at every $\mathfrak{p} \in \Xi$. The curve E, by the definition of optimality, embeds into $J_0(\mathfrak{n})$, so it is new at every $\mathfrak{p} \in \Xi$. Suppose on the contrary that $\Phi_{E,\mathfrak{p}}$ has p-torsion for all $\mathfrak{p} \in \Xi$. Combining Proposition 4.5 with Proposition 2.7, we conclude that p is a geometric congruence prime for E and $J^{\mathfrak{p}-\mathrm{old}}$, $\mathfrak{p} \in \Xi$. Since E is 1-dimensional, there is a unique connected subgroup scheme of $E[p]$ of order p. Thus the same connected subgroup scheme belongs to all $E \cap J^{\mathfrak{p}-\mathrm{old}}$. The argument in the proof of Proposition 2.9, along with that of Proposition 4.2, shows that there is an element $v \in S(\Gamma_0(\mathfrak{n}), \mathbb{Z})$ such that $v \notin S_E \oplus S^{\mathfrak{p}-\mathrm{old}}$ but $p \cdot v \in S_E \oplus S^{\mathfrak{p}-\mathrm{old}}$ for all $\mathfrak{p} \in \Xi$. We get

$$p \cdot v \in \bigcap_{\mathfrak{p} \in \Xi} (S_E \oplus S^{\mathfrak{p}-\mathrm{old}}) = S_E \oplus (\bigcap_{\mathfrak{p} \in \Xi} S^{\mathfrak{p}-\mathrm{old}}).$$

The equality in the above expression holds because S_E lies in a subspace of $S(\Gamma, \mathbb{Q})$ orthogonal to any $S^{\mathfrak{p}-\mathrm{old}}$ (orthogonal with respect to the Petersson product). On the one hand, it is clear that $\bigcap_{\mathfrak{p}} S^{\mathfrak{p}-\mathrm{old}}$ is generated by the images of $S(\Gamma_0(1), \mathbb{Z})$. On the other hand, since the genus of $X_0(1) \cong \mathbb{P}^1_{\mathbb{F}_q}$ is 0, this latter group of cusp forms is 0, and we get $p \cdot v \in S_E$. This is a contradiction since by assumption $v \notin S_E$ and S_E is saturated.

To prove the second part of the theorem, assume $\deg_{\mathrm{ns}}(j_E) \neq 1$. Then for all proper prime ideals $\mathfrak{p}$ of A the valuation $\mathrm{ord}_\mathfrak{p}(j_E)$ is divisible by p. Since by *Tate's algorithm* for any $\mathfrak{p} \in \Xi$ we have $-\mathrm{ord}_\mathfrak{p}(j_E) = \#\Phi_{E,\mathfrak{p}}$, we get a contradiction. □

Remark 4.7. It is clear that Theorem 4.6 implies Theorem 1.3 in the introduction, as for any elliptic curve E there is the equality $j_{E^{(p)}} = j_E^p$.

References

1. S. Bosch and W. Lütkebohmert, *Degenerating abelian varieties*, Topology **30** (1991), 653–698.
2. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer, 1990.
3. B. Conrad and W. Stein, *Component groups of purely toric quotients*, Math. Research Letters **8** (2001), 745–766.
4. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular functions of one variable II, LNM 349, Springer (1973), 143–316.
5. V. Drinfeld, *Elliptic modules*, Math. Sbornik **94** (1974), 594–627.
6. E.-U. Gekeler, *Über Drinfeldsche Modulkurven vom Hecke-Typ*, Compositio Math. **57** (1986), 219–236.
7. ———, *Analytic construction of Weil curves over function fields*, J. Théor. Nombres Bordeaux **7** (1995), 27–49.

8. E.-U. Gekeler and U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, Internat. J. Math. **6** (1995), 689–708.
9. E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93.
10. A. Grothendieck, *Groupes de type multiplicatif: Homomorphismes dans un schéma en groupes*, SGA 3, Exposé IX, 1970.
11. ———, *Modèles de Néron et monodromie*, SGA 7, Exposé IX, 1972.
12. B. Mazur and K. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, Astérisque **196-197** (1991), 215–255.
13. J. S. Milne, *Arithmetic duality theorems*, Academic Press, 1986.
14. F. Oort and J. Tate, *Group schemes of prime order*, Ann. scient. Éc. Norm. Sup. **3** (1970), 1–21.
15. M. Papikian, *On component groups of Jacobians of Drinfeld modular curves*, Ann. Inst. Fourier, to appear.
16. M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. math. France **102** (1974), 241–280.
17. K. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), 193–205.
18. ———, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: papikian@math.stanford.edu