

ON THE TORSION OF DRINFELD MODULES OF RANK TWO

AMBRUS PÁL

October 22, 2008.

ABSTRACT. We prove that the curve $Y_0(\mathfrak{p})$ has no $\mathbb{F}_2(T)$ -rational points where $\mathfrak{p} \triangleleft \mathbb{F}_2[T]$ is a prime ideal of degree at least 3 and $Y_0(\mathfrak{p})$ is the affine Drinfeld modular curve parameterizing Drinfeld modules of rank two over $\mathbb{F}_2[T]$ of generic characteristic with Hecke-type level $\mathfrak{p}$ -structure. As a consequence we derive a conjecture of Schweizer describing completely the torsion of Drinfeld modules of rank two over $\mathbb{F}_2(T)$ implying the uniform boundedness conjecture in this particular case. We reach our results with a variant of the formal immersion method. Moreover we show that the group $\text{Aut}(X_0(\mathfrak{p}))$ has order two. As a further application of our methods we also determine the prime-to- p cuspidal torsion packet of $X_0(\mathfrak{p})$ where $\mathfrak{p} \triangleleft \mathbb{F}_q[T]$ is a prime ideal of degree at least 3 and q is a power of the prime p .

1. INTRODUCTION

Notation 1.1. Let $F = \mathbb{F}_q(T)$ denote the rational function field of transcendence degree one over a finite field $\mathbb{F}_q$ of characteristic p , where T is an indeterminate, and let $A = \mathbb{F}_q[T]$. Let $Y_0(\mathfrak{n})$ denote the Drinfeld modular curve parameterizing Drinfeld modules of rank two over $\mathbb{F}_q[T]$ of generic characteristic with Hecke-type level $\mathfrak{n}$ -structure, where $\mathfrak{n} \triangleleft \mathbb{F}_q[T]$ is a non-zero ideal. Assume now that $q = 2$. The main result of this paper is the following

Theorem 1.2. *The curve $Y_0(\mathfrak{p})$ has no F -rational points if $\mathfrak{p}$ is a prime ideal and $\deg(\mathfrak{p}) \geq 3$.*

This result is analogous to the celebrated theorem of Mazur on the isogenies of elliptic curves of prime degree defined over the field of rational numbers (proved in [14]). The basic strategy of the latter paper is to prove the formal immersion property at the cusps at every finite place. Mazur's proof of this fact is difficult to adapt to Drinfeld modular curves because of the lack of a good theory of q -expansions for Drinfeld modular forms. In fact the latter is unlikely to exist because one of its important consequences, namely multiplicity one, is probably false (see a discussion of this matter in 9.7.4 of [8] on page 90). Instead we will use a variant introduced in the papers [15] and [22] to show the formal immersion property at the special fiber of $Y_0(\mathfrak{n})$ over the place ∞ corresponding to the point at infinity on $\mathbb{P}_{\mathbb{F}_q}^1$. As a consequence in the second half of the proof we are forced to take an approach which is also different from Mazur's original method studying isogeny characters and which is rather particular to function fields (see chapter 9).

2000 *Mathematics Subject Classification.* 11G09 (primary), 11G18 (secondary).

It is possible to derive uniform bounds on the torsion of Drinfeld modules of rank two using the theorem above. In order to state this result we need to introduce some notation.

Notation 1.3. For every $\mathbb{F}_q$ -algebra B let $B\{\tau\}$ denote the skew-polynomial ring over B defined by the relation $\tau b = b^q \tau$, where b is any element of B . This ring is naturally isomorphic to the ring of $\mathbb{F}_q$ -linear endomorphisms of the group scheme $\mathbb{G}_a$ over B where the action of τ is given by the q -power map $x \mapsto x^q$ and the elements of B act by scalar multiplication. Let $\phi : A \rightarrow B\{\tau\}$ be a Drinfeld module of rank two over B where B is an A -algebra. In this special case ϕ is simply an $\mathbb{F}_q$ -algebra homomorphism with $\phi(T) = T + g\tau + \Delta\tau^2$ with some $\Delta \in B^*$. Then the additive group of B becomes an A -module via the action of A on the group scheme $\mathbb{G}_a$ induced by ϕ . Let us write $(\phi B)_{tors}$ for the torsion of this A -module.

When B is actually equal to F it is not difficult to prove that the group $(\phi F)_{tors}$ is finite, in fact we can always write it in the form $(\phi F)_{tors} = A/\mathfrak{m} \oplus A/\mathfrak{n}$ where $\mathfrak{m}$ and $\mathfrak{n}$ are non-zero ideals of A and $\mathfrak{m}$ divides $\mathfrak{n}$. For any ideal $\mathfrak{a} \triangleleft A$ let $\deg(\mathfrak{a})$ denote the degree of the unique monic polynomial generating $\mathfrak{a}$. Assume now that $q = 2$. Using the main result of this paper we will prove the following theorem which was conjectured in this precise form by A. Schweizer (see Conjecture 1 of [26] on page 601).

Theorem 1.4. *We have $\deg(\mathfrak{m}) + \deg(\mathfrak{n}) \leq 2$ for any Drinfeld module ϕ of rank two over F .*

In fact the above was conjectured by A. Schweizer for every q but we are only able to prove it for $q = 2$ at the moment. This theorem is sharp, that is every possibility allowed by the theorem above actually occurs (see the remark at the bottom of page 604 in [26]). It trivially implies the uniform boundedness conjecture made by B. Poonen in [21] (see page 572) in this particular case.

Notation 1.5. It is possible to reformulate Theorem 1.4 in an equivalent, elementary form which makes no reference to Drinfeld modules. Given a polynomial $P(t) \in F[t]$ we say that $x \in F$ is a preperiodic point for $P(t)$ if the set $\{P^{[n]}(x) | n \in \mathbb{N}\}$ is finite, where $P^{[n]}(t) = P \circ P \circ \dots \circ P(t)$ is the n -fold composition of $P(t)$ with itself. For a Drinfeld module $\phi : A \rightarrow F\{\tau\}$ the set of preperiodic points of the additive polynomial $\phi(T)$ in F is equal to $(\phi F)_{tors}$.

Assume again that $q = 2$.

Theorem 1.6. *For every polynomial $P(t) = Tt + gt^2 + \Delta t^4 \in F[t]$ the set of preperiodic points of $P(t)$ in F has cardinality at most 4.*

Proof. Note that when $F = \mathbb{F}_2(T)$ then every Drinfeld module of rank one over F is isomorphic to the Carlitz module. Because the torsion of the latter has cardinality 4 the theorem above follows immediately from Theorem 1.4. $\square$

We have another application. Let K be an algebraically closed field containing F . For every ideal $\mathfrak{n}$ as above let $X_0(\mathfrak{n})$ denote the unique geometrically irreducible smooth projective curve over F which contains $Y_0(\mathfrak{n})$ as an open subvariety. When $\deg(\mathfrak{p}) \geq 3$ the genus of $X_0(\mathfrak{p})$ is at least 2 hence the group of automorphisms $\text{Aut}(X_0(\mathfrak{p}))$ of the base change of $X_0(\mathfrak{p})$ to K is finite and it does not depend on the choice of K . Using the main result of this paper (and under the hypothesis $q = 2$) we are able to prove the following

Corollary 1.7. *The group $\text{Aut}(X_0(\mathfrak{p}))$ has order two.*

It is interesting to note that the original proof of the analogous theorem (in [16]) uses the q -expansion of modular forms in a way which is again difficult to adapt to our situation. We are able to find a different proof by heavily exploiting that F has characteristic 2.

In order to prove our main result, Theorem 1.2, we need to use the theory of the Eisenstein ideal developed in [17] and [18] to prove some facts about the Eisenstein quotient of the Jacobian of the Drinfeld modular curve $X_0(\mathfrak{p})$, the latter introduced first in [29] by Akio Tamagawa in this context. In particular we answer positively a question of Akio Tamagawa raised at the end of [29]. The latter result can be used to derive the nice application below.

Notation 1.8. For every ideal $\mathfrak{n}$ as above let $J_0(\mathfrak{n})$ denote the Jacobian of the curve $X_0(\mathfrak{n})$. For every F -rational point P_0 of $X_0(\mathfrak{p})$ we may regard $X_0(\mathfrak{p})$ as a subvariety of $J_0(\mathfrak{p})$ over F via the Albanese embedding $X_0(\mathfrak{p}) \hookrightarrow J_0(\mathfrak{p})$ which maps every closed point P to the class of the divisor $P - P_0$. We let $\mathcal{S}_{P_0}$ denote the prime-to- p torsion packet of $X_0(\mathfrak{p})$ relative to P_0 , that is, the set:

$$\mathcal{S}_{P_0} = \{P \in X_0(\mathfrak{p})(\overline{F}) \mid \exists n \in \mathbb{N} \text{ such that } n(P - P_0) = 0 \text{ in } J_0(\mathfrak{p})(\overline{F}) \text{ and } p \nmid n\},$$

where for every field K let $\overline{K}$ denote its maximal separable extension. The geometric points of the zero dimensional complement of $Y_0(\mathfrak{n})$ in $X_0(\mathfrak{n})$ are called the cusps of the curve $X_0(\mathfrak{n})$. When $\mathfrak{n} = \mathfrak{p}$ is a prime ideal then the curve $X_0(\mathfrak{p})$ has two cusps which are actually defined over F . Finally let $\tilde{F}$ denote the maximal constant field extension of F .

Theorem 1.9. *Assume that $\deg(\mathfrak{p}) \geq 3$ and P_0 is one of the two cusps of $X_0(\mathfrak{p})$. Then we have:*

$$\mathcal{S}_{P_0} = \begin{cases} X_0(\mathfrak{p})(\tilde{F}) \cup WP(\mathfrak{p}), & \text{when } \deg(\mathfrak{p}) = 3 \text{ and } p \neq 2, \\ X_0(\mathfrak{p})(\tilde{F}), & \text{when } \deg(\mathfrak{p}) = 3 \text{ and } p = 2, \\ \{\text{the two cusps}\}, & \text{otherwise,} \end{cases}$$

where $WP(\mathfrak{p})$ denotes the set of Weierstrass points of $X_0(\mathfrak{p})$.

Contents 1.10. In the next chapter we prove a useful theorem about the cokernel of maps between the connected components of Néron models of certain abelian varieties induced by functoriality, mildly generalizing a result in [19]. This theorem is first put to use in the third chapter. Here we recall the definition of the cuspidal divisor group $\mathcal{C}(\mathfrak{p})$ and the Eisenstein quotient of the Jacobian of the Drinfeld modular curve $X_0(\mathfrak{p})$, then show that the cuspidal divisor group maps isomorphically onto the Mordell-Weil group of this quotient. Moreover at the end of this chapter we prove Theorem 1.9. It is important to note that as a consequence of the results of this chapter we could use the Eisenstein quotient instead of the winding quotient if we could prove that it also has the crucial formal immersion property. But the period lattice of the Eisenstein quotient, unlike that of the winding quotient, is not explicit, this is why we work with the latter.

In the fourth chapter we recall the definition of modular symbols and some results about these objects which were proved in [18]. In the fifth chapter we construct the winding quotient of the Jacobian of the Drinfeld modular curve $X_0(\mathfrak{p})$ when $\mathfrak{p}$

is a prime ideal of degree at least 3 by describing explicitly its lattice of periods with respect to its rigid analytic uniformization at ∞ and derive its basic properties using this definition. In the sixth chapter we study the structure of quotient of the Bruhat-Tits tree by the Hecke congruence group. Although the results proved in this chapter are completely elementary, they are crucial for the proof. The aim of the following chapter is to construct a model of $X_0(\mathfrak{p})$ over the spectrum of $\mathcal{O}_\infty$, the valuation ring of the completion F_∞ of F with respect to ∞ . The key properties of this model, namely its regularity and the formal immersion property for the winding quotient, is derived with the help of the results of the previous chapter.

We study the Galois module structure of the mod $\mathfrak{p}$ torsion of a rank two Drinfeld module over F which has good reduction at every place $v \neq \infty$ of F in the eighth chapter. In the ninth chapter we actually prove Theorem 1.2 and derive Corollary 1.7 as a consequence. First we determine the set of F_∞ -rational points of $X_0(\mathfrak{p})$. When the rational point reduces to one of the cusps we follow the method used in [15] and [22]. In the remaining cases we show that the corresponding Drinfeld module has a constant j -invariant and we apply the results of the previous chapter. In the last chapter we prove Theorem 1.4 by analyzing Drinfeld modular curves of small conductor. As a consequence of the work of A. Schweizer we only need to study the Drinfeld modular curve $X_0(T^4 + T^2 + 1)$ more seriously.

Acknowledgment 1.11. I wish to thank Akio Tamagawa for some useful discussions about the proofs of Corollary 1.7 and Theorem 1.9.

2. COMPONENT GROUPS OF NÉRON MODELS OF TOTALLY SPLIT ABELIAN VARIETIES

Definition 2.1. For every algebraic group T over a field K which is a split torus let $C(T)$ denote its group of cocharacters. Then $C(T)$ is a free and finitely generated abelian group whose rank is equal to the dimension of T over K . The group $T(K)$ of K -valued points of T is canonically isomorphic to $K^* \otimes C(T)$. Let K be now a field complete with respect to a discrete valuation $v : K^* \rightarrow \mathbb{Z}$. A subgroup Λ of $T(K) = K^* \otimes C(T)$ is called a discrete lattice if the restriction of the homomorphism $v \otimes 1 : K^* \otimes C(T) \rightarrow \mathbb{Z} \otimes C(T)$ to Λ is injective and the image has finite cokernel. In this case the quotient T/Λ exists in the category of rigid analytic spaces and it is a proper rigid analytic group such that the quotient map $T \rightarrow T/\Lambda$ is a homomorphism of rigid analytic groups. Let Q be another split torus over K and let Δ be a discrete lattice in $Q(K) = K^* \otimes C(Q)$. Let $\text{Hom}(T, \Gamma; Q, \Delta)$ denote the group of homomorphisms $\phi : T \rightarrow Q$ of algebraic groups over K such that $\phi(\Gamma) \subseteq \Delta$. The operation of forming quotients induces an injective homomorphism

$$h : \text{Hom}(T, \Gamma; Q, \Delta) \rightarrow \text{Hom}(T/\Gamma, Q/\Delta)$$

where the latter is the group of rigid analytic homomorphisms from the rigid analytic group T/Γ to the rigid analytic group Q/Δ .

Theorem 2.2. *The homomorphism h is an isomorphism.*

Proof. This is essentially Satz 5 of [9], page 33, although the result there is only stated for endomorphisms, i.e. in the case when T and Q are equal. One may immediately reduce to this case by considering $\phi \oplus 0 : T \oplus Q \rightarrow T \oplus Q$. $\square$

Notation 2.3. Let $\mathcal{O}$ and $\mathbf{k}$ denote the valuation ring of K and its residue field, respectively. For every abelian variety C over K let $\Phi(C)$ denote the group of connected components of the special fiber of the Néron model of C over $\mathcal{O}$. Let A be an abelian variety defined over K and assume that the Néron model $\mathcal{A}$ of A over $\mathcal{O}$ has split multiplicative reduction. The latter means that the connected component of the identity of the special fiber of $\mathcal{A}$ is a split torus over $\mathbf{k}$. Let B be an optimal quotient of A . Let $\pi : A \rightarrow B$ be the quotient homomorphism and let $\pi_* : \Phi(A) \rightarrow \Phi(B)$ be the homomorphism induced by π .

Proposition 2.4. *The cokernel of the homomorphism $\pi_* : \Phi(A) \rightarrow \Phi(B)$ injects into the group $(\mathbf{k}^*)^{\dim(A) - \dim(B)}$. In particular its order is annihilated by the order of $\mathbf{k}^*$ when $\mathbf{k}$ is finite.*

The proposition above mildly generalizes one of the main results of [19], but our proof is much simpler and shorter.

Proof. By the uniformization theory of Gerritzen the abelian variety A has a rigid analytic uniformization by a split torus T over K . Hence the abelian variety B , as a quotient of A , has a rigid analytic uniformization by a split torus Q over K , too. Let $\Gamma \subset T(K)$ and $\Delta \subset Q(K)$ be discrete lattices such that $A = T/\Gamma$ and $B = Q/\Delta$, respectively, as rigid analytic groups. By Theorem 2.2 there is a unique homomorphism $\phi : T \rightarrow Q$ of algebraic groups over K such that $\phi(\Gamma) \subseteq \Delta$ and the homomorphism induced by ϕ via forming quotients is equal to π . Let L denote the completion of the algebraic closure of K with respect to the unique extension of the valuation of K . Because L is an algebraically closed field the homomorphism $A(L) \rightarrow B(L)$ induced by π is surjective. Hence $Q(L) = \cup_{d \in \Delta} \phi(T(L)) + d$. As a topological space $Q(L)$ is locally homeomorphic to a complete metric space. The set Δ is countable, hence by Baire's category theorem the closed set $\phi(T(L))$ contains an open ball. Therefore $\phi(T(L))$ is an open subgroup of $B(L)$ so the cokernel of the homomorphism $\phi_* : C(T) \rightarrow C(Q)$ induced by ϕ is finite.

Let S denote the scheme-theoretical reduction of the kernel of ϕ . Then S is a smooth algebraic group and it has finitely many connected components. Let R denote the connected component of the identity of S : the algebraic group R is a subtorus of T . Its group of cocharacters $C(R) \subseteq C(T)$ lies in the kernel of the homomorphism ϕ_* above. Hence the rank of $C(R)$ is at most $\dim(A) - \dim(B)$. Since the homomorphism $v \otimes 1 : R(K) = K^* \otimes C(R) \rightarrow \mathbb{Z} \otimes C(R)$ restricted to $\Gamma \cap R(K)$ is injective, the rank of $\Gamma \cap R(K)$ is at most $\dim(A) - \dim(B)$, too. The group $\Gamma \cap R(K)$ has finite index in the kernel of the restriction of $\phi : T(K) \rightarrow Q(K)$ to Γ hence the rank of the finitely generated $\mathbb{Z}$ -module $\phi(\Gamma) \subset Q(K)$ is at least $\dim(A)$. But $\phi(\Gamma)$ lies in Δ so the rank of $\phi(\Gamma)$ is exactly $\dim(A)$. In particular it is a lattice in $Q(K)$.

Let V denote the split torus which is the quotient of T by its subtorus R . Let $\phi_0 : T \rightarrow V$ denote the quotient map and let $\phi_1 : V \rightarrow Q$ be the unique homomorphism of algebraic groups such that $\phi = \phi_1 \circ \phi_0$. Let G denote the torsion of the group $\phi_0(\Gamma)$. The latter is a finite group of $V(K)$, so it injects into the group $(\mathbf{k}^*)^{\dim(A) - \dim(B)}$. Moreover its image with respect to ϕ_1 is the identity since the latter lies in $\phi(\Gamma)$, which has no torsion. Let W denote the split torus which is the quotient of V by its finite subgroup scheme G . Let $\phi_{10} : V \rightarrow W$ denote the quotient map and let $\phi_{11} : W \rightarrow Q$ be the unique homomorphism of algebraic groups such that $\phi_1 = \phi_{11} \circ \phi_{10}$. The kernel of the homomorphism ϕ_1 is a finite

group scheme, hence the same holds for ϕ_{11} as well. Therefore ϕ_{11} maps $\phi_{10} \circ \phi_0(\Gamma)$ into $\phi(\Gamma)$ injectively with finite cokernel. Hence $\phi_{10} \circ \phi_0(\Gamma)$ is a lattice in $W(K)$ by the above.

Let C denote the proper rigid analytic group $W/\phi_{10} \circ \phi_0(\Gamma)$. By construction there are homomorphisms $\pi_0 : A \rightarrow C$ and $\pi_1 : C \rightarrow B$ of rigid analytic groups such that $\pi = \pi_1 \circ \pi_0$. By a Theorem of [10] on page 338 the quotient of a split torus U by a discrete lattice $\Lambda \subset U(K)$ is isomorphic to the rigid analytic variety underlying an abelian variety over K if and only if there is a homomorphism σ from Λ to the character group $\text{Hom}(U, \mathbb{G}_m)$ of U such that the bilinear map:

$$(\alpha, \beta) \mapsto \sigma(\alpha)(\beta) : \Lambda \times \Lambda \rightarrow K^*$$

is symmetric and $v(\sigma(\alpha)(\alpha)) > 0$ whenever $1 \neq \alpha \in \Lambda$. Because Q/Δ is an abelian variety there is such a homomorphism σ from Δ to $\text{Hom}(Q, \mathbb{G}_m)$. Then the composition of $\phi_{11} : \phi_{10} \circ \phi_0(\Gamma) \rightarrow \Delta$, the homomorphism σ and the functorial homomorphism $\text{Hom}(Q, \mathbb{G}_m) \rightarrow \text{Hom}(W, \mathbb{G}_m)$ is also a homomorphism of this type from $\phi_{10} \circ \phi_0(\Gamma)$ to $\text{Hom}(W, \mathbb{G}_m)$. Therefore C is an abelian variety over K , hence, by GAGA, the homomorphisms π_0 and π_1 are algebraic. Recall that B is an optimal quotient of A if and only if for every factorization of the quotient homomorphism $\pi : A \rightarrow B$ into two homomorphisms $\pi' : A \rightarrow C'$ and $\pi'' : C' \rightarrow B$ of abelian varieties such that $\dim(C') = \dim(B)$ the homomorphism π'' is an isomorphism. Hence we get that the map $\pi_1 : C \rightarrow B$ is an isomorphism. By Theorem 2.2 the latter implies that the map $\phi_{11} : W \rightarrow Q$ is also an isomorphism.

The homomorphism $\phi_0 : T(K) \rightarrow V(K)$ is surjective. The cokernel of the homomorphism $\phi_{10} : V(K) \rightarrow W(K)$ is isomorphic non-canonically to the finite group G . By the above the map $\phi_{11} : W(K) \rightarrow Q(K)$ is an isomorphism. Hence the cokernel of the homomorphism $\phi_{10} : T(K) \rightarrow Q(K)$ is isomorphic to G . For every split torus U over K and for every discrete lattice $\Lambda \subset U(K)$ such that the quotient U/Λ is an abelian variety over K the composition of the quotient map $U(K) \rightarrow (U/\Lambda)(K)$ and the specialization map $(U/\Lambda)(K) \rightarrow \Phi(U/\Lambda)$ is surjective. Since every quotient of G is a subgroup of $(\mathbf{k}^*)^{\dim(A) - \dim(B)}$ the claim is now clear. $\square$

Assume now that A has multiplicative reduction which we do not assume to be split, that is, the connected component of the identity of the special fiber of its Néron model is a torus over $\mathbf{k}$. Let B be again an optimal quotient of A and let $\pi : A \rightarrow B$, $\pi_* : \Phi(A) \rightarrow \Phi(B)$ be the same as above.

Corollary 2.5. *The order of cokernel of the homomorphism $\pi_* : \Phi(A) \rightarrow \Phi(B)$ is relatively prime to the characteristic of $\mathbf{k}$.*

Proof. Over a finite unramified extension L of K the abelian variety A has split multiplicative reduction. Because the formation of Néron models commute with smooth base change the group of connected components of the special fiber of the Néron models of A and B over the integral closure of $\mathcal{O}$ in L are equal to $\Phi(A)$ and $\Phi(B)$, respectively, and the homomorphism induced by the base change of π to L between the group of connected components is equal to π_* . Hence by Proposition 2.4 the cokernel of the homomorphism $\pi_* : \Phi(A) \rightarrow \Phi(B)$ injects into the group $(\mathbf{l}^*)^{\dim(A) - \dim(B)}$ where $\mathbf{l}$ denotes the residue field of L . Since the multiplicative group of $\mathbf{l}$ has no finite subgroup whose order is divisible by the characteristic of $\mathbf{k}$, the claim is now obvious. $\square$

3. THE EISENSTEIN QUOTIENT

Notation 3.1. For every $f \in A$ we will let the same symbol denote the ideal generated by f when this will not cause confusion. Similarly for every prime ideal $\mathfrak{p} \triangleleft A$ we let the same symbol denote the unique valuation of F corresponding to this ideal normalized so that $\mathfrak{p}(\pi) = 1$ for every uniformizing element $\pi \in F$. There is exactly one non-trivial valuation of F (up to rescaling) that is not of this form which will be denoted by ∞ as usual. For every valuation x of F let F_x denote the completion of F with respect to x and let $\mathcal{O}_x, \mathfrak{f}_x$ denote its valuation ring and its residue field, respectively.

Definition 3.2. The cyclic group generated by the linear equivalence class of the divisor which is the difference of the two cusps of $X_0(\mathfrak{p})$ is called the cuspidal divisor group and it is denoted by $\mathcal{C}(\mathfrak{p})$. For every proper ideal $\mathfrak{m} \triangleleft A$ there is a $\mathfrak{m}$ -th Hecke correspondence on the Drinfeld modular curve $X_0(\mathfrak{p})$ which in turn induces an endomorphism of the Jacobian $J_0(\mathfrak{p})$ of the curve, called the Hecke operator $T_{\mathfrak{m}}$ (for a detailed description see for example [8].) Let $\mathbb{T}(\mathfrak{p})$ denote the algebra with unity generated by the endomorphisms $T_{\mathfrak{q}}$ of the Jacobian $J_0(\mathfrak{p})$, where $\mathfrak{q} \triangleleft A$ is any prime ideal which is relatively prime to $\mathfrak{p}$. The algebra $\mathbb{T}(\mathfrak{p})$ is known to be commutative. Let $\mathfrak{E}(\mathfrak{p})$ denote the ideal of $\mathbb{T}(\mathfrak{p})$ generated by the elements $T_{\mathfrak{q}} - q^{\deg(\mathfrak{q})} - 1$, where $\mathfrak{q}$ is any prime ideal different from $\mathfrak{p}$. The algebra $\mathbb{T}(\mathfrak{p})$ will be called the Hecke algebra and $\mathfrak{E}(\mathfrak{p})$ its Eisenstein ideal. They were already introduced in Definition 7.10 of [17] on page 160. Let γ denote the ideal $\bigcap_{n=1}^{\infty} \mathfrak{E}(\mathfrak{p})^n$ and let $E(\mathfrak{p})$ denote the quotient of $J_0(\mathfrak{p})$ by the smallest abelian sub-variety of $J_0(\mathfrak{p})$ which is left invariant under the action of $\mathbb{T}(\mathfrak{p})$ and contains the image of the endomorphism $h : J_0(\mathfrak{p}) \rightarrow J_0(\mathfrak{p})$ for every $h \in \gamma$. The abelian variety $E(\mathfrak{p})$ is naturally equipped with an action of $\mathbb{T}(\mathfrak{p})$ which makes the quotient map $J_0(\mathfrak{p}) \rightarrow E(\mathfrak{p})$ a $\mathbb{T}(\mathfrak{p})$ -equivariant homomorphism.

Let ${}^r\mathcal{E}(\mathfrak{p})$ and ${}^r\mathcal{H}(\mathfrak{p})$ denote the largest torsion subgroup of $J_0(\mathfrak{p})(\overline{F})$ and $E(\mathfrak{p})(\overline{F})$ annihilated by $\mathfrak{E}(\mathfrak{p})^r$, respectively.

Lemma 3.3. *The quotient homomorphism $\pi : J_0(\mathfrak{p}) \rightarrow E(\mathfrak{p})$ maps ${}^r\mathcal{E}(\mathfrak{p})$ isomorphically onto ${}^r\mathcal{H}(\mathfrak{p})$.*

The claim above and its proof is just a slight extension of claim (i) of Proposition 4.16 of [29] on page 234.

Proof. For every prime number l , natural number n and Galois module G let $G_l, G[l^n]$ denote the maximal l -primary submodule of G and the l^n -torsion submodule of G , respectively. Clearly we only have to show that π maps ${}^r\mathcal{E}(\mathfrak{p})_l$ isomorphically onto ${}^r\mathcal{H}(\mathfrak{p})_l$ for every prime l which divides the order of $\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})$. By Theorem 1.2 of [18] we know that l is not equal to p . Let $\mathbb{T}_l(\mathfrak{p})$ denote the tensor product $\mathbb{T}(\mathfrak{p}) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ and let $\gamma_l \triangleleft \mathbb{T}_l(\mathfrak{p})$ be the ideal generated by γ . Because $\mathbb{T}_l(\mathfrak{p})$ is finitely generated as a $\mathbb{Z}_l$ -module it has only finitely many maximal ideals $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_m$. Let $\mathbb{T}_{\mathfrak{P}_k}$ denote the completion of $\mathbb{T}_l(\mathfrak{p})$ with respect to $\mathfrak{P}_k$ and let $\pi_k : \mathbb{T}_l(\mathfrak{p}) \rightarrow \mathbb{T}_{\mathfrak{P}_k}$ be the canonical projection for every $k = 1, 2, \dots, m$. Then the direct sum $\bigoplus_k \pi_k : \mathbb{T}_l(\mathfrak{p}) \rightarrow \bigoplus_k \mathbb{T}_{\mathfrak{P}_k}$ of these projections is an isomorphism. Because the composition of the canonical inclusion $\mathbb{Z} \rightarrow \mathbb{T}(\mathfrak{p})$ and the quotient map $\mathbb{T}(\mathfrak{p}) \rightarrow \mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})$ is surjective (see Proposition 7.11 of [17] on pages 160-161), there is a unique maximal ideal of $\mathbb{T}_l(\mathfrak{p})$, say $\mathfrak{P}_1$, containing $\mathfrak{E}(\mathfrak{p})$. Let $\epsilon \in \mathbb{T}_l(\mathfrak{p})$ be the idempotent which corresponds to $(1, 0, \dots, 0) \in \bigoplus_k \mathbb{T}_{\mathfrak{P}_k}$. Then the annihilator ideal of ϵ in $\mathbb{T}_l(\mathfrak{p})$ is

exactly γ_l since the latter is the kernel of the projection π_1 onto the factor $\mathbb{T}_{\mathfrak{p}_1}$ by definition.

For every $n \in \mathbb{N}$ choose an $\epsilon_n \in \mathbb{T}(\mathfrak{p})$ such that $\epsilon_n \equiv \epsilon \pmod{l^n}$. For every $x \in J_0(\mathfrak{p})(\overline{F})[l^n]$ and for every $n \leq m \in \mathbb{N}$ we have $\epsilon_n(x) = \epsilon_m(x)$. Let $\epsilon(x)$ denote this common value: then $x \mapsto \epsilon(x)$ is an endomorphism of $J_0(\mathfrak{p})(\overline{F})_l$ which commutes with the action of $\mathbb{T}(\mathfrak{p})$. Moreover $\pi(\epsilon(x)) = \pi(x)$ because π is $\mathbb{T}(\mathfrak{p})$ -equivariant, the action of $\mathbb{T}(\mathfrak{p})$ on $E(\mathfrak{p})$ factors through γ and $\pi_1(\epsilon) = 1$ by definition. Let $x \in J_0(\mathfrak{p})(\overline{F})_l$ be a point such that $\pi(x) = 0$. Then there is a finite extension L of F , a natural number k , elements $a_1, a_2, \dots, a_k \in \gamma$ and points $y_1, y_2, \dots, y_k \in J_0(\mathfrak{p})(L)$ such that

$$x = a_1(y_1) + a_2(y_2) + \dots + a_k(y_k).$$

For every sufficiently large $n \in \mathbb{N}$ we have:

$$\epsilon(x) = \epsilon_n(x) = \epsilon_n a_1(y_1) + \epsilon_n a_2(y_2) + \dots + \epsilon_n a_k(y_k).$$

Because $\epsilon_n a_j \equiv 0 \pmod{l^n}$ for every $j = 1, 2, \dots, k$ we get that $\epsilon(x) \in l^n J_0(\mathfrak{p})(L)$ for every $n \in \mathbb{N}$. By the Mordell-Weil theorem $J_0(\mathfrak{p})(L)$ is a finitely generated $\mathbb{Z}$ -module hence $\epsilon(x)$ is torsion and its order is prime to l . But it is also l -primary torsion hence $\epsilon(x) = 0$. We get that $\epsilon(y)$ only depends on $\pi(y)$ for every $y \in J_0(\mathfrak{p})(\overline{F})_l$. Therefore the map ϵ induces a $\mathbb{T}(\mathfrak{p})$ -equivariant section of the surjective map $\pi : J_0(\mathfrak{p})(\overline{F})_l \rightarrow E(\mathfrak{p})(\overline{F})_l$. The existence of such a section guarantees that π maps ${}^r\mathcal{E}(\mathfrak{p})$ surjectively onto ${}^r\mathcal{H}(\mathfrak{p})$. Because $\epsilon \equiv 1 \pmod{\mathfrak{E}(\mathfrak{p})^r \mathbb{T}_l(\mathfrak{p})}$, we have $\epsilon(x) = x$ for every $x \in {}^r\mathcal{E}(\mathfrak{p})_l$ so π is injective on ${}^r\mathcal{E}(\mathfrak{p})_l$ as well. $\square$

Lemma 3.4. *Let B be an optimal quotient of $J_0(\mathfrak{p})$ over F . Then the Mordell-Weil group $B(F)$ has no p -torsion.*

Proof. By 5.1-5.8 of [5], pages 229-233 the curve $X_0(\mathfrak{p})$ has a semistable model over $\mathcal{O}_{\mathfrak{p}}$ such that the irreducible components of the special fiber are rational curves. Hence it has multiplicative reduction by a classical theorem of Raynaud. Moreover the order of the group of connected components of the Néron model of $J_0(\mathfrak{p})$ at $\mathcal{O}_{\mathfrak{p}}$ is relatively prime to p by Lemma 5.9 and Proposition 5.10 of [5], page 234. The abelian variety B is an optimal quotient of $J_0(\mathfrak{p})$ hence the order of the group of connected components of its Néron model at $\mathcal{O}_{\mathfrak{p}}$ is also relatively prime to p by Corollary 2.5 above. Therefore it has no F -rational p -torsion by Lemma 7.13 of [17], page 162. $\square$

Theorem 3.5. *The quotient homomorphism $\pi : J_0(\mathfrak{p}) \rightarrow E(\mathfrak{p})$ maps $\mathcal{C}(\mathfrak{p})$ isomorphically onto $E(\mathfrak{p})(F)$.*

Proof. By the lemma above $E(\mathfrak{p})(F)$ has no p -torsion. Also note that the action of $\mathbb{T}(\mathfrak{p})$ on $E(\mathfrak{p})$ satisfies the Eichler-Shimura relations because the same is true for the action of $\mathbb{T}(\mathfrak{p})$ on $J_0(\mathfrak{p})$ and $\pi : J_0(\mathfrak{p}) \rightarrow E(\mathfrak{p})$ is equivariant with respect to the action of $\mathbb{T}(\mathfrak{p})$. These two facts can be used to show that the torsion of $E(\mathfrak{p})$ is annihilated by $\mathfrak{E}(\mathfrak{p})$ the same way as we proved the same claim for $J_0(\mathfrak{p})$ in the argument of Lemma 7.16 of [17], page 163. Hence the torsion subgroup of $E(\mathfrak{p})(F)$ lies in $\mathcal{H}(\mathfrak{p})$ so it must be equal to the image of $\mathcal{C}(\mathfrak{p})$ by Lemma 3.3. The latter maps isomorphically onto its image by the lemma just quoted. Now we only have to show that $E(\mathfrak{p})(F)$ is finite.

Let $W_{\mathfrak{p}}$ denote the Atkin-Lehner involution on the curve $Y_0(\mathfrak{p})$ (for its definition and properties see [5].) The latter extends to an involution of $X_0(\mathfrak{p})$. The

automorphism of $J_0(\mathfrak{p})$ induced by this involution will be denoted by $W_{\mathfrak{p}}$ as well. It commutes with the action of $\mathbb{T}(\mathfrak{p})$ hence it leaves the kernel of the projection $\pi : J_0(\mathfrak{p}) \rightarrow E(\mathfrak{p})$ invariant. By Theorem 5.7 of [29] on page 241 we only have to show that the involution of $E(\mathfrak{p})$ induced by $W_{\mathfrak{p}}$, denoted by the same symbol by the usual abuse of notation, is multiplication by -1 . Let l be an odd prime dividing the order of $\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})$ (such a prime exists by the proof of Proposition 4.14 of [29] on page 233). Because l is automatically different from p it will be sufficient to prove that the action of $W_{\mathfrak{p}}$ on $E(\mathfrak{p})(\overline{F})_l$ is multiplication by -1 . First we are going to prove that $E(\mathfrak{p})(\overline{F})_l = \cup_{r=1}^{\infty} {}^r\mathcal{H}(\mathfrak{p})_l$. In fact the kernel of the action of $\mathbb{T}(\mathfrak{p})$ on $E(\mathfrak{p})(\overline{F})[l^n]$ contains the ideals γ and $l^n\mathbb{T}(\mathfrak{p})$. Recall that γ is the kernel of the canonical map $\mathbb{T}(\mathfrak{p}) \rightarrow \mathbb{T}_{\mathfrak{P}}$ where $\mathbb{T}_{\mathfrak{P}}$ is the completion of $\mathbb{T}(\mathfrak{p})$ with respect to the unique prime ideal $\mathfrak{P} \triangleleft \mathbb{T}(\mathfrak{p})$ over $\mathfrak{E}(\mathfrak{p})$. Hence the sum of the ideals γ and $l^n\mathbb{T}(\mathfrak{p})$ contains some r -th power of $\mathfrak{E}(\mathfrak{p})$, so $\mathfrak{E}(\mathfrak{p})^r$ annihilates $E(\mathfrak{p})(\overline{F})[l^n]$.

Note that for every involution w acting on a finite abelian group G of odd order the group G decomposes as a direct sum of eigenspaces for w with eigenvalues -1 and 1 . Using this fact it is easy to show that if G has a filtration by w -invariant subgroups $\{0\} = G_0 \subset G_1 \subset \dots \subset G_n = G$ such that the involution on G_{i+1}/G_i induced by w is multiplication by -1 for $i = 0, 1, \dots, n-1$ then the eigenspace of w for the eigenvalue 1 is trivial by induction on the length of the filtration. Now we are going to prove by induction on r that the action of $W_{\mathfrak{p}}$ on ${}^r\mathcal{H}(\mathfrak{p})_l$ is multiplication by -1 . It is sufficient to prove the same for ${}^r\mathcal{E}(\mathfrak{p})_l$ by Lemma 3.3. The claim holds for $r = 1$ by the proposition below. Now we assume that the claim has been proved for r , and let $a_1, a_2, \dots, a_m$ be a set of elements of $\mathfrak{E}(\mathfrak{p})^r$ such that their class mod $\mathfrak{E}(\mathfrak{p})^{r+1}$ generates the $\mathbb{Z}$ -module $\mathfrak{E}(\mathfrak{p})^r/\mathfrak{E}(\mathfrak{p})^{r+1}$. The map $x \mapsto a_1x \oplus \dots \oplus a_mx$ is a $W_{\mathfrak{p}}$ -invariant homomorphism ${}^{r+1}\mathcal{E}(\mathfrak{p})_l \rightarrow {}^1\mathcal{E}(\mathfrak{p})_l^m$ with kernel ${}^r\mathcal{E}(\mathfrak{p})_l$, hence the claim holds for $r+1$ as well by the remark above. $\square$

Proposition 3.6. *The action of $W_{\mathfrak{p}}$ on ${}^1\mathcal{E}(\mathfrak{p})_l$ is multiplication by -1 .*

Proof. Recall that the group ${}^1\mathcal{E}(\mathfrak{p})$ was denoted by $\mathcal{E}(\mathfrak{p})$ in the paper [17]. By Theorem 2.5 of [20] on page 327 every element of $\mathcal{E}(\mathfrak{p})$ is defined over the maximal unramified extension $\tilde{F}_{\infty}$ of F_{∞} . Therefore $\mathcal{E}(\mathfrak{p})$ has a filtration:

$$0 \rightarrow \mathcal{E}_0(\mathfrak{p}) \rightarrow \mathcal{E}(\mathfrak{p}) \rightarrow \mathcal{E}_1(\mathfrak{p}) \rightarrow 0$$

where $\mathcal{E}_0(\mathfrak{p})$ is the subgroup of all elements of $\mathcal{E}(\mathfrak{p})$ whose image with respect to the specialization map into the special fiber of the Néron model of $J_0(\mathfrak{p})$ over the valuation ring of $\tilde{F}_{\infty}$ lies in the connected component. The subgroup $\mathcal{E}_0(\mathfrak{p})$ is left invariant by $W_{\mathfrak{p}}$ because the automorphism $W_{\mathfrak{p}}$ of $J_0(\mathfrak{p})$ extends to an involution of the Néron model of the Jacobian.

We only need to show that $W_{\mathfrak{p}}$ acts on $\mathcal{E}_0(\mathfrak{p})_l$ and $\mathcal{E}_1(\mathfrak{p})_l$ as multiplication by -1 . First we are going to show this for the former. Let $l(\mathfrak{p})$ denote the largest power of l dividing $N(\mathfrak{p})$, the order of the group $\mathcal{C}(\mathfrak{p})$. By Theorem 1.2 of [18] the number $N(\mathfrak{p})$ is also the index of the Eisenstein ideal $\mathfrak{E}(\mathfrak{p})$ in the Hecke algebra $\mathbb{T}(\mathfrak{p})$. Therefore $N(\mathfrak{p})$ annihilates the l -primary group $\mathcal{E}_0(\mathfrak{p})_l$, so the latter is annihilated by $l(\mathfrak{p})$ as well. By Proposition 10.8 on pages 189-190 and Corollary 11.7 on page 194 of [17] we know that the l -torsion of $\mathcal{E}_0(\mathfrak{p})_l$ has order at most l . Hence the group $\mathcal{E}_0(\mathfrak{p})_l$ is cyclic and its order divides $l(\mathfrak{p})$. On the other hand $\mathcal{E}_0(\mathfrak{p})_l$ contains the maximal l -primary subgroup of the Shimura subgroup $\mathcal{S}(\mathfrak{p})$ (by part (i) of Proposition 8.18 in [17], pages 171-172). As the order of the latter is exactly $l(\mathfrak{p})$ (by Lemma 8.17

of [17] on page 171) the groups $\mathcal{E}_0(\mathfrak{p})_l$ and $\mathcal{S}(\mathfrak{p})_l$ are equal. Because this argument works for every prime l dividing $N(\mathfrak{p})$ we get that actually the groups $\mathcal{E}_0(\mathfrak{p})$ and $\mathcal{S}(\mathfrak{p})$ are equal.

By part (ii) of Proposition 8.18 in [17] on pages 171-172 the group $\mathcal{S}(\mathfrak{p})$ maps isomorphically onto the group of connected components of the fiber of the Néron model of $J_0(\mathfrak{p})$ at $\mathcal{O}_{\mathfrak{p}}$ via the specialization map. The same is true for the cuspidal divisor group $\mathcal{C}(\mathfrak{p})$ by 5.11 of [5] on page 235. Both maps are equivariant with respect to the action of the Atkin-Lehner operator. The latter interchanges the two cusps of $X_0(\mathfrak{p})$ hence it act as multiplication by -1 on the group $\mathcal{C}(\mathfrak{p})$, therefore on the groups $\mathcal{S}(\mathfrak{p})$ and $\mathcal{E}(\mathfrak{p})_l$ as well.

The group $\mathcal{E}_1(\mathfrak{p})_l$ injects into the l -primary group of connected components of the special fiber of the Néron model of $J_0(\mathfrak{p})$ over the valuation ring of $\tilde{F}_{\infty}$ annihilated by the Eisenstein ideal. The latter is a cyclic group by the strong multiplicity one theorem (see the proof of Proposition 7.18 of [17] on pages 163-164) so the same holds for $\mathcal{E}_1(\mathfrak{p})_l$ as well. Every involution acting on a cyclic group of odd prime power order is multiplication by ± 1 hence it will be sufficient to prove that the action of $W_{\mathfrak{p}}$ on the l -torsion $\mathcal{E}_1(\mathfrak{p})[l]$ of $\mathcal{E}_1(\mathfrak{p})_l$ is multiplication by -1 . If l does not divide $q-1$ then $\mathcal{C}(\mathfrak{p})_l$ maps isomorphically onto the group $\mathcal{E}_1(\mathfrak{p})[l]$ by Proposition 10.8 of [17] on pages 189-190, so the claim above is clear. If l does divide $q-1$ then the group $\mathcal{D}(\mathfrak{p})[l]$ of order l^2 introduced in Definition 9.17 of [17] on page 183 maps surjectively onto the group $\mathcal{E}_1(\mathfrak{p})[l]$ and the kernel is the l -torsion of the Shimura group by claim (v) Proposition 9.18 of [17] on pages 184-185. The short exact sequence of l -torsion Galois modules:

$$0 \rightarrow \mathcal{S}(\mathfrak{p})[l] \rightarrow \mathcal{D}(\mathfrak{p})[l] \rightarrow \frac{\mathcal{D}(\mathfrak{p})}{\mathcal{S}(\mathfrak{p})[l]} \rightarrow 0$$

is not split by claim (v) of the proposition just quoted above. Hence the involution $W_{\mathfrak{p}}$ must be multiplication by -1 on $\mathcal{D}(\mathfrak{p})[l]$ because $W_{\mathfrak{p}}$ commutes with the Galois action and it is multiplication by -1 on $\mathcal{S}(\mathfrak{p})[l]$. $\square$

Corollary 3.7. *The action of $W_{\mathfrak{p}}$ on $\mathcal{E}(\mathfrak{p})$ is multiplication by -1 .*

Proof. By Lemma 3.3 the étale group scheme $\mathcal{E}(\mathfrak{p})$ imbeds $W_{\mathfrak{p}}$ -equivariantly into the Eisenstein quotient $E(\mathfrak{p})$. On the other hand by the proof of Theorem 3.5 above we know that $W_{\mathfrak{p}}$ acts on $E(\mathfrak{p})$ as multiplication by -1 . $\square$

Recall that in this chapter we do not assume that $q = 2$.

Proposition 3.8. *The set $X_0(\mathfrak{p})(\tilde{F})$ lies in $\mathcal{S}_{P_0}$ when $\mathfrak{p}$ is a prime ideal of degree 3 and P_0 is a cusp.*

Proof. Let $X_{\overline{F}}$ denote the base change of every algebraic variety X defined over F to $\overline{F}$. Fix a prime l different from p and consider the l -adic representation $H^1(J_0(\mathfrak{n})_{\overline{F}}, \overline{\mathbb{Q}}_l)$ of the absolute Galois group of F where $\mathfrak{n}$ is any non-zero ideal of A . By Drinfeld's fundamental theorem (Theorem 2 of [2] on page 562) the latter decomposes as a sum of irreducible two-dimensional l -adic Galois representations over $\overline{\mathbb{Q}}_l$. The conductor of every such representation ρ is the sum of the divisors $\mathfrak{m}$ and ∞ where $\mathfrak{m}$ divides $\mathfrak{n}$. Moreover ρ appears as an irreducible component of the Galois representation $H^1(J_0(\mathfrak{m})_{\overline{F}}, \overline{\mathbb{Q}}_l)$ when $\mathfrak{m}$ is a proper divisor of $\mathfrak{n}$. The curve $X_0(1)$ has genus zero hence the degree of the conductor of every irreducible

representation ρ appearing in $H^1(J_0(\mathfrak{p})_{\overline{F}}, \overline{\mathbb{Q}}_l)$ is 4. Therefore the degree of the Grothendieck L -function $L(\rho_n, t)$ of the base change ρ_n of ρ to the field $F_n = \mathbb{F}_{q^n}(T)$ as a polynomial in t is zero by the Grothendieck-Ogg-Shafarevich formula for every $n \in \mathbb{N}$. In particular $L(\rho_n, t)$ does not vanish at q^{-n} . We get that the Mordell-Weil group $J_0(\mathfrak{p})(F_n)$ is finite by the main theorem of [24] on page 509. Hence the group $J_0(\mathfrak{p})(\tilde{F})$ is torsion. Therefore it is equal to $\mathcal{E}(\mathfrak{p})$ by Theorem 2.5 of [20] on page 327. The order of $\mathcal{E}(\mathfrak{p})$ is prime to the characteristic, hence the claim is now clear. $\square$

Proof of Theorem 1.9. Let P_0 and P_∞ denote the two cusps of $X_0(\mathfrak{p})$. Because the group $\mathcal{C}(\mathfrak{p})$ is finite and its order is prime to p both cusps are elements of $\mathcal{S}_{P_0}$. Moreover the Drinfeld modular curve $X_0(\mathfrak{p})$ is hyperelliptic when $\deg(\mathfrak{p}) = 3$ by Theorem 20 of [25] on page 343. By Theorem 20 of [25] quoted above the unique hyperelliptic involution of $X_0(\mathfrak{p})$ is the Atkin-Lehner involution $W_{\mathfrak{p}}$. Hence every Weierstrass point of $X_0(\mathfrak{p})$ is a branch point of the unique hyperelliptic covering (see Proposition 1.4 of [30] on page 286). The Atkin-Lehner involution exchanges P_0 and P_∞ so for every hyperelliptic branch point P of $X_0(\mathfrak{p})$ we have:

$$2P \sim P_\infty + P_0 \quad \text{or equivalently} \quad 2(P - P_0) \sim P_\infty - P_0,$$

where $\sim$ denotes the linear equivalence of divisors. In particular P is a $2N(\mathfrak{p})$ -torsion point with respect to the Albanese embedding $X_0(\mathfrak{p}) \hookrightarrow J_0(\mathfrak{p})$ with base point P_0 . Hence it is an element of $\mathcal{S}_{P_0}$ when p is different from 2.

Now let P be an element of $\mathcal{S}_{P_0}$ and assume that it has order $n \in \mathbb{N}$. By assumption n is relatively prime to p . Let G denote the Galois module generated by P in $J_0(\mathfrak{p})(\tilde{F})[n]$. Then G is unramified at every place of F different from $\mathfrak{p}$ and ∞ because at these places the abelian variety $J_0(\mathfrak{p})$ has good reduction. At the places $\mathfrak{p}$ and ∞ the curve $J_0(\mathfrak{p})$ has stable reduction. Hence the Galois module G is either also unramified at the places $\mathfrak{p}$ and ∞ or the curve $X_0(\mathfrak{p})$ is hyperelliptic and P is a Weierstrass point by Proposition 0.2 of [30] on page 283. The latter is only possible when $\deg(\mathfrak{p}) = 3$ by Theorem 20 of [25] quoted above and the order of $P - P_0$ is $2N(\mathfrak{p})$ in this case as we already saw above. Hence we may assume that the Galois module G is everywhere unramified. In this case P is defined over the maximal constant field extension $\tilde{F}$ of F . By Theorem 2.5 of [20] on page 327 the torsion of the group $J_0(\mathfrak{p})(\tilde{F})$ is equal to $\mathcal{E}(\mathfrak{p})$. Hence $P - P_0$ lies in $\mathcal{E}(\mathfrak{p})$, so by Corollary 3.7 we have:

$$W_{\mathfrak{p}}(P - P_0) \sim P_0 - P \quad \text{or equivalently} \quad P + W_{\mathfrak{p}}(P) \sim P_0 + P_\infty.$$

If P is different from P_0 and P_∞ the relation above implies that $X_0(\mathfrak{p})$ is hyperelliptic. In the latter case $\deg(\mathfrak{p}) = 3$, hence the claim follows from Proposition 3.8. $\square$

4. THE WINDING HOMOMORPHISM

Definition 4.1. For any graph G let $\mathcal{V}(G)$ and $\mathcal{E}(G)$ denote its set of vertices and edges, respectively. In this paper we will only consider such oriented graphs G which are equipped with an involution $\bar{\cdot} : \mathcal{E}(G) \rightarrow \mathcal{E}(G)$ such that for each edge $e \in \mathcal{E}(G)$ the original and terminal vertices of the edge $\bar{e} \in \mathcal{E}(G)$ are the terminal and original vertices of e , respectively. The edge $\bar{e}$ is called the edge e with reversed

orientation. Let R be a commutative group. A function $\phi : \mathcal{E}(G) \rightarrow R$ is called a harmonic R -valued cochain, if it satisfies the following conditions:

(i) We have:

$$\phi(e) + \phi(\bar{e}) = 0 \quad (\forall e \in \mathcal{E}(G)).$$

(ii) If for an edge e we introduce the notation $o(e)$ and $t(e)$ for its original and terminal vertex respectively,

$$\sum_{\substack{e \in \mathcal{E}(G) \\ o(e)=v}} \phi(e) = 0 \quad (\forall v \in \mathcal{V}(G)).$$

We denote by $H(G, R)$ the group of R -valued harmonic cochains on G .

Definition 4.2. Let GL_2 denote the group scheme of invertible two by two matrices and let Z denote its center. Let $\pi \in F_\infty$ be a uniformizer. We are going to recall the definition of the Bruhat-Tits tree $\mathcal{T}$ associated to the projective linear group $PGL_2(F_\infty)$. The set of vertices $\mathcal{V}(\mathcal{T})$ and edges $\mathcal{E}(\mathcal{T})$ are the cosets $GL_2(F_\infty)/GL_2(\mathcal{O}_\infty)Z(F_\infty)$ and $GL_2(F_\infty)/\Gamma_\infty Z(F_\infty)$, respectively, where Γ_∞ is the Iwahori group:

$$\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_\infty) \mid \infty(c) > 0 \right\}.$$

Since Γ_∞ is a subgroup of $GL_2(\mathcal{O}_\infty)$ there is a natural map $o : \mathcal{E}(\mathcal{T}) \rightarrow \mathcal{V}(\mathcal{T})$ which assigns to every edge its original vertex. The matrix $\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$ normalizes the Iwahori subgroup therefore the map $GL_2(F_\infty) \rightarrow GL_2(F_\infty)$ given by the rule $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$ induces a map on the coset $\mathcal{V}(\mathcal{T})$. This map is the involution which assigns to every edge e the same edge $\bar{e}$ with reversed orientation. The composition of this involution and the map o is the map $t : \mathcal{E}(\mathcal{T}) \rightarrow \mathcal{V}(\mathcal{T})$ which assigns to every edge its terminal vertex.

Definition 4.3. For every non-zero ideal $\mathfrak{n} \triangleleft A$ let $\Gamma_0(\mathfrak{n})$ denote the Hecke congruence group:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A) \mid c \equiv 0 \pmod{\mathfrak{n}} \right\}.$$

The group $GL_2(F_\infty)$ acts on itself via its left-regular action which induces an action of $GL_2(F_\infty)$ on the Bruhat-Tits tree. This action induces an action of its subgroup $\Gamma_0(\mathfrak{n})$ on $\mathcal{T}$ as well. Let $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ denote the group of $\Gamma_0(\mathfrak{n})$ -invariant R -valued cochains on $\mathcal{T}$. The group $GL_2(A)$ does not contain elements which map an edge $e \in \mathcal{E}(\mathcal{T})$ to the same edge $\bar{e}$ with reversed orientation therefore the cosets $\Gamma_0(\mathfrak{n}) \backslash \mathcal{V}(\mathcal{T})$ and $\Gamma_0(\mathfrak{n}) \backslash \mathcal{E}(\mathcal{T})$ are the vertices and edges of an oriented graph which is going to be denoted by $\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$. Every element ϕ of $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ induces an R -valued function on the edges of $\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$. If this function is zero outside of a finite set we say that ϕ is cuspidal. The R -module of cuspidal elements of $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ is denoted by $H_!(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$.

Definition 4.4. For every pair $\mathfrak{m}, \mathfrak{n} \triangleleft A$ of non-zero ideals let $H(\mathfrak{m}, \mathfrak{n})$ denote the set:

$$H(\mathfrak{m}, \mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F) \mid a, b, c, d \in A, (ad - cb) = \mathfrak{m}, \mathfrak{n} \supseteq (c), (d) + \mathfrak{n} = A \right\}.$$

The set $H(\mathfrak{m}, \mathfrak{n})$ is a double $\Gamma_0(\mathfrak{n})$ -coset and it is also the disjoint union of finitely many left $\Gamma_0(\mathfrak{n})$ -cosets. Let $R(\mathfrak{m}, \mathfrak{n})$ be a set of representatives of these cosets. For any left $\Gamma_0(\mathfrak{n})$ -invariant R -valued function $\phi : \mathcal{E}(\mathcal{T}) \rightarrow R$ define $T_{\mathfrak{m}}(\phi)$ by the formula:

$$T_{\mathfrak{m}}(\phi)(g) = \sum_{h \in R(\mathfrak{m}, \mathfrak{n})} \phi(hg), \quad \forall g \in \mathcal{E}(\mathcal{T}).$$

It is well-known and easy to check that $T_{\mathfrak{m}}(\phi)$ is independent of the choice of $R(\mathfrak{m}, \mathfrak{n})$ and it is also a left $\Gamma_0(\mathfrak{n})$ -invariant R -valued function so we have an R -linear operator $T_{\mathfrak{m}}$ acting on the R -module of left $\Gamma_0(\mathfrak{n})$ -invariant R -valued functions on $\mathcal{E}(\mathcal{T})$. It is also well-known and not too difficult to verify that $T_{\mathfrak{m}}$ leaves the submodules $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ and $H_1(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ invariant. The operator $T_{\mathfrak{m}}$ is denoted by the same symbol we use for the operators introduced in Definition 3.2, but this will not cause confusion as we will see. For the moment it is sufficient to remark that they act on different objects.

Definition 4.5. A path γ on an oriented graph G is a sequence of edges

$$\{\dots, e_1, e_2, \dots, e_n, \dots\} \in \mathcal{E}(G)$$

indexed by the set I where $I = \mathbb{Z}$, $I = \mathbb{N}$ or $I = \{0, 1, \dots, m\}$ for some $m \in \mathbb{N}$ such that $t(e_i) = o(e_{i+1})$ for every $i, i+1 \in I$. We say that γ is an infinite path, a half-infinite path or a finite path whether we are in the first, in the second or in the third case, respectively. For each edge $e \in \mathcal{E}(G)$ let $i_e : \mathcal{E}(G) \rightarrow \mathbb{Z}$ denote the unique function such that

$$i_e(f) = \begin{cases} +1, & \text{if } f = e, \\ -1, & \text{if } f = \bar{e}, \\ 0, & \text{otherwise.} \end{cases}$$

Let γ be a path $\{\dots, e_1, \dots, e_n, \dots\}$ on G such that every edge in $\mathcal{E}(G)$ is only listed finitely many times in the sequence above. Then the function $i_{\gamma} = \sum_{j \in \mathbb{Z}} i_{e_j}$ is well-defined as the sum above has only finitely many terms non-zero on e for every edge $e \in \mathcal{E}(G)$. Let us consider now the special case $G = \Gamma \backslash \mathcal{T}$ where $\Gamma = \Gamma_0(\mathfrak{n})$ is a short-hand notation introduced for convenience. Let $z(\Gamma)$ denote the cardinality of the center of Γ and Γ_e is the stabilizer of the edge $e \in \mathcal{E}(\mathcal{T})$ in Γ . (It is well-known that the latter is finite.) For every path γ on the graph $\Gamma \backslash \mathcal{T}$ such that i_{γ} is defined in the sense above we define the function $\gamma^* : \mathcal{E}(\mathcal{T}) \rightarrow \mathbb{Z}$ given by the rule $\gamma^*(e) = |\Gamma_e i_{\gamma}(\tilde{e})| / z(\Gamma)$, where $\tilde{e}$ is the image of the edge e in $\mathcal{E}(\Gamma \backslash \mathcal{T})$ and the absolute sign $|\cdot|$ denotes the cardinality of every finite set. (Since the center of Γ leaves the Bruhat-Tits tree invariant, it lies in the stabilizer Γ_e , therefore the expression above is indeed an integer.)

Definition 4.6. Next we are going to define the fundamental arch connecting two different points $a, b \in \mathbb{P}^1(F_\infty)$ on the Bruhat-Tits tree. We say that a path $\{\dots, e_1, \dots, e_n, \dots\}$ indexed by the set I on an oriented graph G is without backtracking if $\bar{e}_i \neq e_{i+1}$ for every $i, i+1 \in I$. Let $S(a, b)$ denote the set of those edges of $\mathcal{T}$ which can be represented by a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ such that the homogeneous coordinates $(\alpha : \gamma) = a$ and $(\beta : \delta) = b$. The elements of the set $S(a, b)$ can be indexed uniquely by the set of integers such that it becomes an infinite path without backtracking: this is the fundamental arch $\overline{ab}$ connecting a and b . Let $\overline{ab}$ denote the image of the fundamental arch under the canonical map $\mathcal{T} \rightarrow \Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$ as well by slight abuse of notation. Let $[a, b] : \mathcal{E}(\mathcal{T}) \rightarrow \mathbb{Z}$ denote the function $(\overline{ab})^*$ introduced in Definition 4.5 if the latter is well-defined.

Let $\mathfrak{p} \triangleleft A$ be now a proper non-zero prime ideal.

Proposition 4.7. *The following holds:*

- (i) *for every different $a, b \in \mathbb{P}^1(F)$ the function $[a, b]$ is well-defined and it is a $\mathbb{Z}$ -valued left $\Gamma_0(\mathfrak{p})$ -invariant harmonic cochain,*
- (ii) *we have $[a, b] \in H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$ for every different $a, b \in \mathbb{P}^1(F)$ which are equivalent under the Möbius action of $\Gamma_0(\mathfrak{p})$,*
- (iii) *for every proper non-zero prime ideal $\mathfrak{p} \neq \mathfrak{q} \triangleleft A$ we have*

$$(1 + q^{\deg(\mathfrak{q})} - T_{\mathfrak{q}})[0, \infty] \in (q - 1)H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}.$$

Proof. This is Proposition 5.3 of [18]. $\square$

Let r be the unique monic polynomial generating the prime ideal $\mathfrak{q}$. Let $R(\mathfrak{q}) \subset \mathbb{F}_q[T]$ denote the set of non-zero polynomials whose degree is less than $\deg(\mathfrak{q})$. The following lemma was shown during the proof of Proposition 2.7 in [18].

Lemma 4.8. *We have:*

$$(1 + q^{\deg(\mathfrak{q})} - T_{\mathfrak{q}})[0, \infty] = \sum_{0 \neq a \in R(\mathfrak{q})} [0, a/r]. \quad \square$$

Definition 4.9. Let $\widehat{\mathbb{T}}(\mathfrak{p}), \mathbb{T}(\mathfrak{p})$ denote the commutative $\mathbb{Z}$ -algebra with unity generated by the endomorphisms $T_{\mathfrak{q}}$ of the $\mathbb{Z}$ -module $H(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$ and $H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$, respectively, where $\mathfrak{q} \triangleleft A$ is any prime ideal different from $\mathfrak{p}$. Note that the latter algebra is denoted by the same symbol as the Hecke algebra introduced in Definition 3.2. Indeed the two algebras are naturally isomorphic by the Gekeler-Reversat uniformization theory (see for example Theorem 7.9 of [17] on page 159 for a convenient description of this isomorphism). By Corollary 3.13 of [18] the algebras $\widehat{\mathbb{T}}(\mathfrak{p})$ and $\mathbb{T}(\mathfrak{p})$ are sub-algebras of the endomorphism ring of a finitely generated, free $\mathbb{Z}$ -module hence they must be finitely generated, free $\mathbb{Z}$ -modules, too. Clearly $\mathbb{T}(\mathfrak{p})$ is the quotient of $\widehat{\mathbb{T}}(\mathfrak{p})$. Let $\widehat{\mathfrak{C}}(\mathfrak{p})$ denote the ideal of $\widehat{\mathbb{T}}(\mathfrak{p})$ generated by the elements $T_{\mathfrak{q}} - q^{\deg(\mathfrak{q})} - 1$, where $\mathfrak{q} \neq \mathfrak{p}$ is any prime. We have a well-defined homomorphism

$$e : \widehat{\mathfrak{C}}(\mathfrak{p}) \rightarrow H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$$

of $\widehat{\mathbb{T}}(\mathfrak{p})$ -modules given by the rule $\alpha \mapsto \alpha([0, \infty])/(q - 1)$ according to part (iii) of Proposition 4.7. This map is the analogue of the winding homomorphism introduced by Mazur.

The following claim is an immediate corollary of Theorem 5.13 of [18].

Proposition 4.10. *The image of the winding homomorphism e is non-zero.* $\square$

5. THE WINDING QUOTIENT

Definition 5.1. Recall that a finite path $\{e_0, e_2, \dots, e_n\} \in \mathcal{E}(G)$ on an oriented graph G is closed if the equality $t(e_n) = o(e_0)$ holds, too. We define $H_1(G, \mathbb{Z})$ as the abelian group of $\mathbb{Z}$ -valued functions on $\mathcal{E}(G)$ generated by the functions i_γ where γ is a closed path. We define the map

$$j_{\Gamma_0(\mathfrak{n})} : H_1(\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}, \mathbb{Z}) \rightarrow H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})},$$

as the unique homomorphism which maps i_γ to the cochain γ^* for every γ closed path, using the notations of Definition 4.5. It is easy to see that the homomorphism is well-defined, that is γ^* is indeed a harmonic cochain. By a theorem of Gekeler and Nonnengardt (Theorem 3.3 of [7], page 702) this homomorphism is in fact an isomorphism.

Definition 5.2. Let $\Gamma_0(\mathfrak{p})_{\text{ab}} = \Gamma_0(\mathfrak{p}) / [\Gamma_0(\mathfrak{p}), \Gamma_0(\mathfrak{p})]$ be the abelianization of $\Gamma_0(\mathfrak{p})$, and let $\bar{\Gamma}_0(\mathfrak{p}) = \Gamma_0(\mathfrak{p})_{\text{ab}} / (\Gamma_0(\mathfrak{p})_{\text{ab}})_{\text{tors}}$ be its maximal torsion-free quotient. For each $\gamma \in \Gamma_0(\mathfrak{p})$ let $\bar{\gamma}$ denote its image in $\bar{\Gamma}_0(\mathfrak{p})$. Fix a vertex $v_0 \in \mathcal{V}(\mathcal{T})$ and for every $\gamma \in \Gamma_0(\mathfrak{p})$ let $e_0, e_1, \dots, e_{n(\gamma)}$ be the unique geodesic path connecting v_0 with $\gamma(v_0)$, that is $v_0 = o(e_1)$ and $\gamma(v_0) = t(e_{n(\gamma)})$. Recall that a path is geodesic if it is the shortest connecting its endpoints, in this case v_0 with $\gamma(v_0)$, i.e. the number $n(\gamma)$ is the smallest possible. The image of the path $e_0, e_1, \dots$ is closed in $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$: let $i(\gamma)$ denote the corresponding element in $H_1(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}, \mathbb{Z})$. The function i induces a homomorphism $i : \bar{\Gamma}_0(\mathfrak{p}) \rightarrow H_1(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}, \mathbb{Z})$ which is independent of the choice of v_0 and it is an isomorphism. We will use this identification without further notice. In particular we equip $\bar{\Gamma}_0(\mathfrak{p})$ with an action of the Hecke operator T_q via the isomorphism i .

Notation 5.3. Let $\mathbb{C}_\infty$ denote the completion of the algebraic closure of F_∞ and let $c : \bar{\Gamma}_0(\mathfrak{p}) \rightarrow \text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ be the period map defined in Proposition 7.5 of [17] on page 159. Note that for every finitely generated, free $\mathbb{Z}$ -module $\mathcal{Y}$ the group $\text{Hom}(\mathcal{Y}, \mathbb{C}_\infty^*)$ is canonically isomorphic to the group of $\mathbb{C}_\infty$ -valued points of the unique torus $T_{\mathcal{Y}}$ whose group of characters $\text{Hom}(T_{\mathcal{Y}}, \mathbb{G}_m)$ is $\mathcal{Y}$. The image of $\bar{\Gamma}_0(\mathfrak{p})$ under c is a discrete lattice in $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$, and the rigid-analytic group variety $T_{\bar{\Gamma}_0(\mathfrak{p})} / c(\bar{\Gamma}_0(\mathfrak{p}))$ is isomorphic to the rigid-analytic variety associated to $J_0(\mathfrak{p})$ via the Abel-Jacobi map of Gekeler-Reversat. (For a description of this map using the same notation see sections 7.1-7.7 of [17] on pages 158-159.)

Definition 5.4. Let $\infty : \mathbb{C}_\infty^* \rightarrow \mathbb{Q}$ denote a valuation of $\mathbb{C}_\infty$ which induces its standard non-archimedean topology. Let $\mathcal{Y}$ be a finitely generated, free $\mathbb{Z}$ -module and let $\infty : \text{Hom}(\mathcal{Y}, \mathbb{C}_\infty^*) \rightarrow \text{Hom}(\mathcal{Y}, \mathbb{Q})$ denote also the homomorphism induced by ∞ . We will say that a submodule Λ of $\text{Hom}(\mathcal{Y}, \mathbb{C}_\infty^*)$ is a quasi-lattice if

- (i) it is a finitely generated abelian group,
- (ii) the kernel of the restriction of ∞ to Λ is finite,
- (iii) the free abelian group $\infty(\Lambda)$ spans $\text{Hom}(\mathcal{Y}, \mathbb{Q})$ as a vector space over $\mathbb{Q}$,
- (iv) the $\mathbb{Z}$ -rank of $\infty(\Lambda)$ is the same as the $\mathbb{Z}$ -rank of $\mathcal{Y}$.

When Λ is a quasi-lattice in $\text{Hom}(\mathcal{Y}, \mathbb{C}_\infty^*)$ then the quotient $T_{\mathcal{Y}} / \Lambda$ exists in the category of rigid analytic spaces, and it is a proper rigid analytic group such that the quotient map $T_{\mathcal{Y}} \rightarrow T_{\mathcal{Y}} / \Lambda$ is a homomorphism of rigid analytic groups.

Our next aim is to give a convenient description of optimal quotients of $J_0(\mathfrak{p})$, considered as an abelian variety over $\mathbb{C}_\infty$, in terms of certain period lattices. We

will say, following [19], that a subgroup Λ of $\bar{\Gamma}_0(\mathfrak{p})$ is saturated if for every $x \in \bar{\Gamma}_0(\mathfrak{p})$ we have $x \in \Lambda$ when $nx \in \Lambda$ for some positive integer n .

Proposition 5.5. *Let $\mathcal{Y}$ be a saturated $\mathbb{T}(\mathfrak{p})$ -invariant subgroup of $\bar{\Gamma}_0(\mathfrak{p})$. Then the image Λ of $\mathcal{Y}$ under the composition:*

$$\bar{\Gamma}_0(\mathfrak{p}) \xrightarrow{c} \text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*) \longrightarrow \text{Hom}(\mathcal{Y}, \mathbb{C}_\infty^*)$$

is a quasi-lattice in $\text{Hom}(\mathcal{Y}, \mathbb{C}_\infty^*)$, and the quotient $T_{\mathcal{Y}}/\Lambda$ is the rigid-analytic variety attached to a unique optimal quotient of $J_0(\mathfrak{p})$. Moreover every optimal quotient of $J_0(\mathfrak{p})$ arises this way.

Proof. This is the content of Propositions 3.11 and 3.12 of [19] on pages 2183-2184. $\square$

For every abelian variety A let $\text{End}(A)$ denote the ring of endomorphisms of A over its field of definition. The following lemma will be useful.

Lemma 5.6. *The following holds:*

- (i) *Every endomorphism of $J_0(\mathfrak{p})$ is defined over F .*
- (ii) *The algebra $\text{End}(J_0(\mathfrak{p})) \otimes \mathbb{Q}$ is the product of totally real number fields.*
- (iii) *Every finite subgroup of the group of automorphisms of the algebraic group $J_0(\mathfrak{p})$ has exponent 2.*

Proof. Claim (i) is just Theorem A.1 of [29] on page 242 whose proof is on pages 244-245. Claim (ii) is the content of Remark A.6 of [29] on page 243. The group of automorphisms of the algebraic group $J_0(\mathfrak{p})$ is a subgroup of the multiplicative group of the algebra $\text{End}(J_0(\mathfrak{p})) \otimes \mathbb{Q}$. Every finite subgroup of the latter has exponent 2 by the second claim because the maximal finite multiplicative subgroup of a totally real field is $\{\pm 1\}$. The last claim is now clear. $\square$

Proposition 5.7. *Every optimal quotient of $J_0(\mathfrak{p})$ is defined over F .*

Proof. For every abelian variety A let $A^\vee$ denote its dual. Let B an optimal quotient of $J_0(\mathfrak{p})$ and let $\pi : J_0(\mathfrak{p}) \rightarrow B$ be the quotient map. Let A be the group scheme which is the kernel of π . By our assumptions it is an abelian variety. It will be sufficient to prove that A is defined over F . Let $\pi^\vee : B^\vee \rightarrow J_0(\mathfrak{p})^\vee$ be the dual of π . Because B is an optimal quotient of $J_0(\mathfrak{p})$ the map $\pi^\vee$ is an immersion. Since $J_0(\mathfrak{p})$ is a Jacobian it has a principal polarization $\iota : J_0(\mathfrak{p}) \rightarrow J_0(\mathfrak{p})^\vee$. Let $\lambda : B \rightarrow B^\vee$ be a polarization of B . Then the composition $h = \iota^{-1} \circ \pi^\vee \circ \lambda \circ \pi$ is an endomorphism of $J_0(\mathfrak{p})$ hence it is defined over F by claim (i) of the lemma above. In particular its kernel is a group scheme defined over F . Because λ is an isogeny the reduction of the connected component of the kernel of h is A . Therefore the latter is also defined over F . $\square$

Notation 5.8. Let $\phi \in H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$ and $\psi \in H(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$ be two harmonic cochains. In this case their Petersson product is well-defined (for definition see 4.8 of [8] on page 57) and it will be denoted by $\langle \phi, \psi \rangle$. Moreover for every $\phi \in H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$ let $L(\phi, s)$ denote its L -function. (For the definition of the latter see [33].)

We are going to use the following well-known fact (see Proposition 1 of [31] on page 112):

Proposition 5.9. *For every $\phi \in H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$ we have:*

$$\langle \phi, [0, \infty] \rangle = c \cdot L(\phi, q^{-1})$$

where $c \in \mathbb{C}^*$ only depends on q . $\square$

Definition 5.10. Let $\mathfrak{I}(\mathfrak{p})$ denote the ideal:

$$\mathfrak{I}(\mathfrak{p}) = \{T \in \widehat{\mathbb{T}}(\mathfrak{p}) \mid T([0, \infty]) \in H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}\}$$

of the ring $\widehat{\mathbb{T}}(\mathfrak{p})$. Let $\Lambda(\mathfrak{p})$ denote the smallest saturated subgroup of $\overline{\Gamma}_0(\mathfrak{p})$ containing the group $\{T([0, \infty]) \mid T \in \mathfrak{I}(\mathfrak{p})\}$. Because the latter is $\mathbb{T}(\mathfrak{p})$ -invariant so is the former. Note that $\Lambda(\mathfrak{p})$ contains the image of the winding homomorphism e introduced in Definition 4.9. Let $W(\mathfrak{p})$ denote the optimal quotient of $J_0(\mathfrak{p})$ corresponding to $\Lambda(\mathfrak{p})$ under the construction described in Proposition 5.5.

For every abelian variety A defined over F let $L(A, t)$ denote its Hasse-Weil L -function.

Proposition 5.11. *The following holds:*

- (i) *the quotient $W(\mathfrak{p})$ is non-trivial,*
- (ii) *the quotient $W(\mathfrak{p})$ is actually defined over F ,*
- (iii) *the quotient $W(\mathfrak{p})$ is the largest optimal quotient of $J_0(\mathfrak{p})$ such that the Hasse-Weil L -function of $W(\mathfrak{p})$ does not vanish at q^{-1} .*

Proof. By Proposition 4.10 the group $\Lambda(\mathfrak{p})$ is non-zero so claim (i) is clear. The second claim follows from Proposition 5.7. The abelian variety $W(\mathfrak{p})$ is isogenous to the product of its absolutely simple optimal quotients, which are all defined over F by Proposition 5.7, since they are also optimal quotients of $J_0(\mathfrak{p})$. Hence it will be sufficient to prove that for every absolutely irreducible optimal quotient B of $J_0(\mathfrak{p})$ we have $L(B, q^{-1}) \neq 0$ if and only if B is also an optimal quotient of $W(\mathfrak{p})$. Now let B be an absolutely simple optimal quotient of $J_0(\mathfrak{p})$ and let $\mathcal{V} \subseteq \overline{\Gamma}_0(\mathfrak{p})$ be the corresponding saturated $\mathbb{T}(\mathfrak{p})$ -invariant subgroup. Note that B is an optimal quotient of $W(\mathfrak{p})$ if and only if $\mathcal{V} \subseteq \Lambda(\mathfrak{p})$. Because B is absolutely irreducible the $\mathbb{T}(\mathfrak{p}) \otimes \mathbb{Q}$ -module

$$\mathcal{V} \otimes \mathbb{Q} \subseteq \mathcal{H}_0(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} \otimes \mathbb{Q} = \mathcal{H}_0(\mathcal{T}, \mathbb{Q})^{\Gamma_0(\mathfrak{p})}$$

must be irreducible. Therefore the image of $\mathbb{T}(\mathfrak{p}) \otimes \mathbb{Q}$ in the endomorphism ring of the vector space $\mathcal{V} \otimes \mathbb{Q}$ is a number field K and $\mathcal{V} \otimes \mathbb{Q}$ has dimension one with respect to this K -action. In particular there is a non-zero Hecke eigenform $\phi \in \mathcal{V} \otimes K \subseteq \mathcal{H}_0(\mathcal{T}, K)^{\Gamma_0(\mathfrak{p})}$ such that we have $\mathcal{V} \subseteq \Lambda(\mathfrak{p})$ if and only if $\phi \in \Lambda(\mathfrak{p}) \otimes K$. Choose an embedding of K into $\mathbb{C}$. After this choice we may consider ϕ as an element of $\mathcal{H}_0(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$. The natural action of $\mathbb{T}(\mathfrak{p})$ on the optimal quotient B furnishes a homomorphism $K \rightarrow \text{End}(B)$. By the Eichler-Shimura isomorphism (see 8.3.8 of [8] on page 81) the L -series $Z_B(q^{-s}; K)$ of the abelian variety B with coefficients in K (in the sense of [29] on page 214) is equal to $c_\phi L(\phi, s)$ where $c_\phi \in \mathbb{C}$ is a non-zero scalar. Because $Z_B(q^{-s}; K)$ vanishes at $s = 1$ exactly when $L(B, q^{-1})$ is zero, we only have to show that for every non-zero Hecke eigenform $\phi \in \mathcal{H}_0(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$ we have $L(\phi, q^{-1}) \neq 0$ if and only if $\phi \in \Lambda(\mathfrak{p}) \otimes \mathbb{C}$. First assume the latter. Because ϕ is an eigenform there is a character $\chi : \widehat{\mathbb{T}}(\mathfrak{p}) \otimes \mathbb{C} \rightarrow \mathbb{C}$ such

that $T(\phi) = \chi(T)\phi$ for every $T \in \widehat{\mathbb{T}}(\mathfrak{p}) \otimes \mathbb{C}$. By assumption there is an operator $T \in \widehat{\mathbb{T}}(\mathfrak{p}) \otimes \mathbb{C}$ such that $\phi = T([0, \infty])$. Because the Petersson product is positive definite we get that:

$$0 < \langle \phi, \phi \rangle = \langle \phi, T([0, \infty]) \rangle = \langle T(\phi), [0, \infty] \rangle = \chi(T) \langle \phi, [0, \infty] \rangle = c\chi(T)L(\phi, q^{-1}),$$

where we also used that the action of $\widehat{\mathbb{T}}(\mathfrak{p}) \otimes \mathbb{C}$ is self-adjoint with respect to the Petersson product in the second equation. Hence $L(\phi, q^{-1})$ is non-zero as we claimed. Assume now that ϕ is not an element of $\Lambda(\mathfrak{p}) \otimes \mathbb{C}$. Because the algebra $\widehat{\mathbb{T}}(\mathfrak{p}) \otimes \mathbb{C}$ is semi-simple the vector space $\Lambda(\mathfrak{p}) \otimes \mathbb{C}$ is spanned by Hecke eigenforms. None of these is a scalar multiple of ϕ hence ϕ is orthogonal to every element of $\Lambda(\mathfrak{p}) \otimes \mathbb{C}$. In particular for every non-zero prime ideal $\mathfrak{q}$ of A different from $\mathfrak{p}$ we have:

$$\begin{aligned} 0 &= \langle \phi, (T_{\mathfrak{q}} - (q^{\deg(\mathfrak{q})} + 1))([0, \infty]) \rangle = \langle (T_{\mathfrak{q}} - (q^{\deg(\mathfrak{q})} + 1))(\phi), [0, \infty] \rangle \\ &= (\chi(T_{\mathfrak{q}}) - (q^{\deg(\mathfrak{q})} + 1)) \langle \phi, [0, \infty] \rangle \\ &= c(\chi(T_{\mathfrak{q}}) - (q^{\deg(\mathfrak{q})} + 1))L(\phi, q^{-1}), \end{aligned}$$

where we used claim (iii) of Proposition 4.7 in the first equation and the self-adjointness of $T_{\mathfrak{q}}$ in the second equation. By the Ramanujan-Petersson conjecture (proved in [2] first in this case) the number $\chi(T_{\mathfrak{q}})$ is not equal to $1 + q^{\deg(\mathfrak{q})}$ when $\deg(\mathfrak{q})$ is sufficiently large hence $L(\phi, q^{-1})$ must be zero. $\square$

Corollary 5.12. *The following holds:*

- (i) *the Mordell-Weil group $W(\mathfrak{p})(F)$ is finite,*
- (ii) *the homomorphism $J_0(\mathfrak{p})(F) \rightarrow W(\mathfrak{p})(F)$ induced by the quotient map is injective restricted to $\mathcal{C}(\mathfrak{p})$.*

Proof. The first claim follows at once from claim (iii) of Proposition 5.11 above by the main theorem of [24] on page 509. As we saw in the proof of Theorem 3.5 we have $L(E(\mathfrak{p}), q^{-1}) \neq 0$ by Theorem 5.7 of [29] on page 241. Hence the Eisenstein quotient $E(\mathfrak{p})$ is an optimal quotient of $W(\mathfrak{p})$ by claim (iii) of Proposition 5.11. Hence the quotient homomorphism $J_0(\mathfrak{p}) \rightarrow E(\mathfrak{p})$ factors through the quotient homomorphism $J_0(\mathfrak{p}) \rightarrow W(\mathfrak{p})$. Therefore the induced homomorphism $J_0(\mathfrak{p})(F) \rightarrow W(\mathfrak{p})(F)$ must be injective restricted to $\mathcal{C}(\mathfrak{p})$ by Theorem 3.5. $\square$

6. THE STRUCTURE OF THE GRAPH $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$

Some results of this chapter can be found in the paper [7] but they are not stated sufficiently explicitly for our purposes. The computations of the above quoted paper are also quite involved because they deal with a much more general situation. Hence for the sake of exposition we will use essentially the same methods to derive the necessary results.

Notation 6.1. Let v_n denote the vertex of the Bruhat-Tits tree represented by the matrix $\begin{pmatrix} T^n & 0 \\ 0 & 1 \end{pmatrix}$ for every natural number $n \in \mathbb{N}$. Let G_n denote the stabilizer of the vertex v_n in $GL_2(A)$ for every n as above. By Proposition 3 of 1.6 in [28] on pages 86-87 we have:

$$G_0 = GL_2(\mathbb{F}_q),$$

and

$$G_n = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in GL_2(A) \mid \deg(b) \leq n \right\}$$

when $n > 0$. Moreover the vertices v_n form a fundamental domain for the action of $GL_2(A)$ on the set of vertices of the Bruhat-Tits tree and the quotient graph $GL_2(A) \backslash \mathcal{T}$ is an infinite tree such that the image of v_0 has degree one and every other vertex has degree two, by the corollary following the proposition just quoted above. Here the degree of a vertex w is the number of edges with origin w .

Definition 6.2. Let u_n denote the vertex $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot v_{n+\deg(\mathfrak{p})}$ of the Bruhat-Tits tree for every natural number $n \in \mathbb{N} \cup \{-1\}$. Assume now that $\deg(\mathfrak{p})$ is even and $q = 2$. Let t be one of the two elements of A with the following properties:

- (i) we have $\deg(t) < \deg(\mathfrak{p})$,
- (ii) the reduction of t modulo $\mathfrak{p}$ generates a degree two extension over $\mathbb{F}_2 \subset \mathbf{f}_{\mathfrak{p}}$.

Let w denote the vertex $\begin{pmatrix} 0 & 1 \\ 1 & t \end{pmatrix} \cdot v_0$ of the Bruhat-Tits tree. For the sake of simple notation let Γ_v denote the stabilizer of v in $\Gamma_0(\mathfrak{p})$ for every vertex v of $\mathcal{T}$.

Proposition 6.3. Assume that $q = 2$ and let v be a vertex of $\mathcal{T}$. Then the stabilizer Γ_v of v is non-trivial if and only if v is equivalent to one of the vertices u_n, v_n (for some $n \in \mathbb{N}$) or w modulo the action of $\Gamma_0(\mathfrak{p})$.

In order to prove the claim above we will need two lemmas.

Lemma 6.4. The set

$$M(\mathfrak{p}) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \mid u \in A, \deg(u) < \deg(\mathfrak{p}) \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

is a complete set of representatives of left $\Gamma_0(\mathfrak{p})$ -cosets in $GL_2(A)$.

Proof. Let B denote the group scheme of upper-triangular two-by-two matrices and let $GL_2^0(\mathbf{f}_{\mathfrak{p}})$ and $B^0(\mathbf{f}_{\mathfrak{p}})$ denote the subgroup of those elements in $GL_2(\mathbf{f}_{\mathfrak{p}})$ and $B(\mathbf{f}_{\mathfrak{p}})$, respectively, whose determinant lies in $\mathbb{F}_q^* \subseteq \mathbf{f}_{\mathfrak{p}}^*$. Then we have:

$$[GL_2(A) : \Gamma_0(\mathfrak{p})] = [GL_2^0(\mathbf{f}_{\mathfrak{p}}) : B^0(\mathbf{f}_{\mathfrak{p}})] = [GL_2(\mathbf{f}_{\mathfrak{p}}) : B(\mathbf{f}_{\mathfrak{p}})] = q^{\deg(\mathfrak{p})} + 1,$$

because the determinant map restricted to $B(\mathbf{f}_{\mathfrak{p}})$ is a surjection onto $\mathbf{f}_{\mathfrak{p}}^*$. Hence it will be sufficient to prove that the reductions of the elements of $M(\mathfrak{p})$ modulo $\mathfrak{p}$ represent different left $B(\mathbf{f}_{\mathfrak{p}})$ -cosets. It is clear that for every $u \in A$ the matrices $\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are not in the same coset since the latter lies in $B(\mathbf{f}_{\mathfrak{p}})$, but the former does not. Now let $u, v \in A$ and assume that there are $a, b \in A^*$ and $c \in A$ such that

$$\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & v \end{pmatrix} = \begin{pmatrix} b & a + bv \\ c & cv \end{pmatrix} \pmod{\mathfrak{p}}.$$

Then $c \equiv 1 \pmod{\mathfrak{p}}$ hence $u \equiv v \pmod{\mathfrak{p}}$. Therefore we must have $u = v$ because $\deg(u)$ and $\deg(v)$ are both less than $\deg(\mathfrak{p})$. $\square$

Now we are going to assume that $q = 2$.

Lemma 6.5. *Let n be a positive integer and let $a, b \in A$ such that $\deg(a) < \deg(\mathfrak{p})$ and $\deg(b) < \deg(\mathfrak{p})$. Then the vertices $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \cdot v_n$ and $\begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix} \cdot v_n$ are equivalent modulo the action of $\Gamma_0(\mathfrak{p})$ if and only if $\deg(a - b) \leq n$.*

Proof. Assume first that $\deg(a - b) \leq n$. Then

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix} = \begin{pmatrix} -a & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix} = \begin{pmatrix} 1 & b - a \\ 0 & 1 \end{pmatrix} \in G_n$$

hence the vertices $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \cdot v_n$ and $\begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix} \cdot v_n$ are in fact equal in this case. Assume now that the vertices $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \cdot v_n$ and $\begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix} \cdot v_n$ are equivalent modulo the action of $\Gamma_0(\mathfrak{p})$. Then there is an $h \in \Gamma_0(\mathfrak{p})$ and $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in G_n$ such that

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}^{-1} \cdot h \cdot \begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix} = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

By definition the reduction of h modulo $\mathfrak{p}$ is an upper-triangular matrix, hence there are elements k, l , and $m \in \mathfrak{f}_{\mathfrak{p}}$ such that

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}^{-1} \cdot \begin{pmatrix} k & l \\ 0 & m \end{pmatrix} \cdot \begin{pmatrix} -a & 1 \\ 1 & 0 \end{pmatrix} &\equiv \begin{pmatrix} -al + m & -ak - alb + mb \\ l & k + lb \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{p}}. \end{aligned}$$

Therefore we must have $l = 0$, $k = m = 1$, and $u \equiv b - a \pmod{\mathfrak{p}}$. Because $\deg(u) \leq n$ the claim follows. $\square$

Proof of Proposition 6.3. By Lemma 6.4 the vertex v can be written in the form $h \cdot g \cdot v_n$ for some $g \in M(\mathfrak{p})$, $h \in \Gamma_0(\mathfrak{p})$ and $n \in \mathbb{N}$. Because we have $\Gamma_v = h(\Gamma_{g \cdot v_n})h^{-1}$ we may assume that $h = 1$. When g is the identity matrix then v is equal to the vertex v_n . In this case the stabilizer Γ_v is equal to the intersection $\Gamma_0(\mathfrak{p}) \cap G_n$. The latter is non-trivial for every $n \in \mathbb{N}$. Hence we may assume that $g = \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix}$ for some $u \in A$ such that $\deg(u) < \deg(\mathfrak{p})$. Assume first that $n > 0$. For every $b \in A$ we have:

$$\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & b + u \end{pmatrix} \cdot \begin{pmatrix} -u & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}.$$

In particular the matrix above is an element of $\Gamma_0(\mathfrak{p})$ if and only if $b \in \mathfrak{p}$. Hence the stabilizer $\Gamma_v = g(G_n)g^{-1} \cap \Gamma_0(\mathfrak{p})$ is non-trivial if and only if $n \geq \deg(\mathfrak{p})$. Moreover by Lemma 6.5 the vertex $v = \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \cdot v_n$ is equivalent to $u_{n-\deg(\mathfrak{p})}$ modulo the action of $\Gamma_0(\mathfrak{p})$ in this case. Assume now that $n = 0$. For every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_2)$ we have:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix}^{-1} &= \begin{pmatrix} c & d \\ a + uc & b + ud \end{pmatrix} \cdot \begin{pmatrix} -u & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -uc + d & c \\ -u^2c + u(d - a) + b & a + uc \end{pmatrix}. \end{aligned}$$

The lower left entry $-u^2c + u(d - a) + b$ must vanish modulo $\mathfrak{p}$ if the product matrix above is an element of $\Gamma_0(\mathfrak{p})$. Hence the reduction of u modulo $\mathfrak{p}$ generates an extension of degree at most two over $\mathbb{F}_2 \subset \mathbf{f}_{\mathfrak{p}}$ when the stabilizer $\Gamma_v = g(G_0)g^{-1} \cap \Gamma_0(\mathfrak{p})$ is non-trivial. Using the identity:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1+u \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and the fact that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G_0$ we may assume that u is either equal to 0 or the element t which we introduced in Definition 6.2. In the first case the vertex v is equal to v_0 because $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G_0$. In particular its stabilizer is non-trivial. In the second case the vertex v is equal to w by definition. Moreover there is a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_2)$ such that $c \neq 0$ and $g \begin{pmatrix} a & b \\ c & d \end{pmatrix} g^{-1} \in \Gamma_0(\mathfrak{p})$. Therefore the stabilizer Γ_w is non-trivial, too. $\square$

For every vertex v (or edge e) of $\mathcal{T}$ let $\tilde{v}$ (resp. $\tilde{e}$) denote the image of v (resp. e) in the factor graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$.

Lemma 6.6. *Assume that $q = 2$. Then the following holds:*

- (i) *for every $n \in \mathbb{N}$ the degrees of the vertices $\tilde{u}_n$ and $\tilde{v}_n$ are two,*
- (ii) *if $\deg(\mathfrak{p})$ is even then the degree of $\tilde{w}$ is one.*

Proof. Let f be the unique generator of the ideal $\mathfrak{p}$. The matrix $w_{\mathfrak{p}} = \begin{pmatrix} 0 & 1 \\ f & 0 \end{pmatrix} \in GL_2(F)$ normalizes the subgroup $\Gamma_0(\mathfrak{p})$, hence its action on the Bruhat-Tits tree $\mathcal{T}$ induces an automorphism of the factor graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$. The square of $w_{\mathfrak{p}}$ is a scalar matrix hence this automorphism is in fact an involution. As usual, we will call it the Atkin-Lehner involution. Note that:

$$\begin{pmatrix} 0 & 1 \\ f & 0 \end{pmatrix} \cdot \begin{pmatrix} T^n & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} T^{n+\deg(\mathfrak{p})} & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} f \cdot T^{-\deg(\mathfrak{p})} & 0 \\ 0 & 1 \end{pmatrix}.$$

Since $\begin{pmatrix} f \cdot T^{-\deg(\mathfrak{p})} & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathcal{O}_{\infty})$ we get that $\tilde{u}_n$ is the image of $\tilde{v}_n$ under the Atkin-Lehner involution. Hence it will be sufficient to verify claim (i) only for the vertex $\tilde{v}_n$. Because 3 does not divide the order of the stabilizer Γ_{v_n} the latter cannot act transitively on the set of edges with origin v_n . Hence the degree of $\tilde{v}_n$ is at least two. For every $u \in \mathbb{F}_2$ we have:

$$\begin{pmatrix} 1 & T^n u \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} T^n & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} T^n & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} u & 1 \\ 1 & 0 \end{pmatrix}.$$

By definition the product matrix in the equation above represents an edge on $\mathcal{T}$ whose origin is v_n . Because $\begin{pmatrix} 1 & T^n u \\ 0 & 1 \end{pmatrix} \in \Gamma_{v_n}$ it will be sufficient to show that these edges are different for different values of u . The latter follows from the fact that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin Z(F_{\infty})\Gamma_{\infty}.$$

The reduction of the element t introduced in Definition 6.2 modulo $\mathfrak{p}$ satisfies the equation $x^2 + x + 1$. Hence the computations of the proof of Proposition 6.3 imply that the matrix $g = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \Gamma_w$. This matrix has order 3. The group G_0 acts faithfully on the set of edges of $\mathcal{T}$ with origin v_0 . In particular every element of G_0 of order 3 acts transitively on these edges. Therefore g must act transitively on the set of edges of $\mathcal{T}$ with origin w . $\square$

Notation 6.7. We will say that a half-infinite path $\gamma = \{e_0, \dots, e_n, \dots\}$ on an oriented graph G is a half-line when for every vertex v of G there is at most one index $n \in \mathbb{N}$ such that $v = o(e_n)$. By a slight abuse of terminology we will call an oriented graph G a half-line if there is a half-line $\gamma = \{e_0, \dots, e_n, \dots\}$ on G such that for every $e \in \mathcal{E}(G)$ either e or $\bar{e}$ is listed in γ . Note that the graph G determines uniquely the half-line γ . Let H be a subgraph of the oriented graph G which is a half-line and let $\{e_0, \dots, e_n, \dots\}$ be the half-line on G which is uniquely determined by H . We will say that H is a maximal half-line if $o(e_0)$ is the only vertex of H whose degree in G is not equal to two.

Lemma 6.8. *The graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ decomposes uniquely as the edge-disjoint union of a finite graph and two maximal half-lines.*

Proof. By Theorem II.9 of [29] the graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ is the edge-disjoint union of a finite graph and finitely many half-lines. Moreover there is a bijection between the latter set of half-lines and the set $\Gamma_0(\mathfrak{p}) \backslash \mathbb{P}^1(F)$ where $\Gamma_0(\mathfrak{p})$ acts on $\mathbb{P}^1(F)$ via the Möbius action. The set $\Gamma_0(\mathfrak{p}) \backslash \mathbb{P}^1(F)$ has two elements. Hence $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ is the edge-disjoint union of a finite graph and two half-lines. The graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ has vertices whose degree is neither one nor two, for example because the group $H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$ is not trivial by Proposition 4.10. Therefore each of the two half-lines above is contained in a unique maximal half-line. $\square$

Let $\mathcal{G}(\mathfrak{p})$ denote the finite graph in the proposition above. We say that a vertex v of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ is cuspidal if it is a vertex of one of the two maximal half-lines of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ but it is not a vertex of $\mathcal{G}(\mathfrak{p})$. In the rest of this chapter we assume that $q = 2$.

Proposition 6.9. *Let v be a vertex of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$. Then v is cuspidal if and only if v is equal to one of the vertices $\tilde{u}_n$ or $\tilde{v}_n$ for some $n \in \mathbb{N}$.*

Proof. Every cuspidal vertex of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ has degree two. In particular its stabilizer is non-trivial. Hence v is equal to one of the vertices $\tilde{u}_n$ or $\tilde{v}_n$ for some $n \in \mathbb{N}$ if it is cuspidal by Proposition 6.3 and by claim (i) of Lemma 6.6. On the other hand it will be sufficient to prove the converse for the vertices $\tilde{u}_n$ only because the vertices $\tilde{v}_n$ are images of these under the Atkin-Lehner involution. Let e_n denote the edge of the Bruhat-Tits tree represented by the matrix:

$$\begin{pmatrix} T & 0 \\ 0 & T^{n+\deg(\mathfrak{p})} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ T^{n+\deg(\mathfrak{p})} & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ T & 0 \end{pmatrix}$$

for every natural number $n \in \mathbb{N}$. By definition we have that $t(e_n) = u_n$ for every $n \in \mathbb{N}$. On the other hand:

$$\begin{pmatrix} T & 0 \\ 0 & T^{n+\deg(\mathfrak{p})} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ T^{n+\deg(\mathfrak{p})-1} & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & T \\ T & 0 \end{pmatrix}.$$

Because $\begin{pmatrix} 0 & T \\ T & 0 \end{pmatrix} \in Z(F_\infty)GL_2(\mathcal{O}_\infty)$ we get that $o(e_n) = u_{n-1}$ for every $n \in \mathbb{N}$. Therefore the sequence $\{e_0, \dots, e_n, \dots\}$ is a half-infinite path. Because the vertices $o(\tilde{e}_n) = \tilde{u}_{n-1}$ are all different the sequence $\{\tilde{e}_0, \dots, \tilde{e}_n, \dots\}$ is a half-line. The claim is now clear. $\square$

Notation 6.10. Note that the stabilizer of two vertices (or edges) of $\mathcal{T}$ in $\Gamma_0(\mathfrak{p})$ which are equivalent under the action of this group are conjugate subgroups. In particular the isomorphism class of the stabilizer of a vertex v (or and edge e) only depends on the image of v (respectively e) in the quotient graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$. Therefore we may talk about the stabilizer of a vertex (or an edge) of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ being non-trivial (in the group $\Gamma_0(\mathfrak{p})$).

Proposition 6.11. *Let v be a vertex of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ which is not cuspidal and whose stabilizer is non-trivial. Then the following holds:*

- (i) *there is no vertex other than v whose stabilizer is non-trivial and which is not cuspidal,*
- (ii) *the degree of v is one,*
- (iii) *the vertex v is fixed by the Atkin-Lehner involution,*
- (iv) *the unique neighbor of v has trivial stabilizer.*

Proof. The first claim is an immediate corollary of Propositions 6.3 and 6.9. The second claim follows from claim (ii) of Lemma 6.6. By claims (i) and (ii) the vertex v is the only vertex of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ whose degree is one. Hence it must be fixed by every automorphism of this graph. Therefore claim (iii) is true. Assume that the unique neighbor w' of v has non-trivial stabilizer. Then this neighbor must be cuspidal. That means that the maximal half-line to which w' belongs to terminates in a degree one vertex. In this case the graph $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ cannot be connected which is a contradiction. Claim (iv) is now clear. $\square$

We will say that an edge e of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ is cuspidal if it is an edge of one of the two maximal half-lines of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$. For every edge $e \in \mathcal{E}(\mathcal{T})$ the stabilizer of e in $\Gamma_0(\mathfrak{p})$ is the intersection of the stabilizers of the vertices $o(e)$ and $t(e)$. Hence claim (iv) above has the following immediate

Corollary 6.12. *Let e be an edge of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ which is not cuspidal. Then the stabilizer of e is trivial. $\square$*

The next proposition will be used in the proof of the formal immersion property.

Proposition 6.13. *The following holds:*

- (i) *the unique common vertex of the graph $\mathcal{G}(\mathfrak{p})$ and the maximal half-line of $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ containing the vertices $\{\tilde{u}_n | n \in \mathbb{N}\}$ is $\tilde{u}_{-1}$,*
- (ii) *there is a harmonic cochain $\phi \in \Lambda(\mathfrak{p})$ whose reduction modulo 2, considered as a function $\phi : \mathcal{E}(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}) \rightarrow \mathbb{F}_2$, is zero on exactly one edge with origin $\tilde{u}_{-1}$.*

Proof. The unique common vertex is $o(\tilde{e}_0)$ where e_0 is the edge introduced in the proof of Proposition 6.9. Claim (i) is now clear. By Lemma 4.8 we know that:

$$(1 + q - T_{(T)})[0, \infty] = [0, 1/T] \in \Lambda(\mathfrak{p}).$$

We claim that $\phi = [0, 1/T]$ satisfies the condition in claim (ii). Let f_n denote the edge of the Bruhat-Tits tree represented by the matrix:

$$\begin{pmatrix} 0 & T^n \\ 1 & T^{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & T \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & T^n \end{pmatrix}$$

for every integer $n \in \mathbb{Z}$. Note that:

$$\begin{pmatrix} 0 & T^n \\ 1 & T^{n+1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ T & 0 \end{pmatrix} = \begin{pmatrix} 0 & T^{n+1} \\ 1 & T^{n+2} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Because $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathcal{O}_\infty)$ we get that $t(f_n) = o(f_{n+1})$ for every $n \in \mathbb{Z}$. Hence the sequence $\gamma = \{\dots, f_{-n}, \dots, f_n, f_{n+1}, \dots\}$ is an infinite path. It is clear that we have $S(0, 1/T) = \{f_n | n \in \mathbb{Z}\}$. Therefore γ is the fundamental arch $\overline{0T^{-1}}$ by definition. Since

$$\begin{pmatrix} 1 & 0 \\ 0 & T^n \end{pmatrix} = \begin{pmatrix} T^{-n} & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} T^n & 0 \\ 0 & T^n \end{pmatrix}$$

we get that $o(f_n) = \begin{pmatrix} 0 & 1 \\ 1 & T \end{pmatrix} \cdot v_{-n}$ for every negative integer n . Moreover:

$$\begin{pmatrix} 0 & T^n \\ 1 & T^{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ T & 1 \end{pmatrix} \cdot \begin{pmatrix} T^n & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathcal{O}_\infty)$ hence we have $o(f_n) = \begin{pmatrix} 1 & 0 \\ T & 1 \end{pmatrix} \cdot v_n$ for every non-negative integer n .

For the sake of simple notation let d denote $\deg(\mathfrak{p})$. From Lemmas 6.4 and 6.5 it follows that for every $g \in GL_2(A) - \Gamma_0(\mathfrak{p})$ and natural number $n \geq d-1$ the vertex $g \cdot v_n$ is equivalent to u_n under the action of $\Gamma_0(\mathfrak{p})$. Therefore we have $o(\tilde{f}_n) = \tilde{u}_{-1}$ if and only if either $n = d-1$ or $n = 1-d$, and we have $t(\tilde{f}_n) = \tilde{u}_{-1}$ if and only if either $n = d-2$ or $n = -d$. Moreover both $o(\tilde{f}_{-d})$ and $t(\tilde{f}_{d-1})$ are equal to $\tilde{u}_0$ hence the contribution of the edges $\tilde{f}_{-d}$ and $\tilde{f}_{d-1}$ to $[0, 1/T]$ cancel each other out. Now we only have to show that $t(\tilde{f}_{1-d})$ and $o(\tilde{f}_{d-2})$ are different. Let $u \in A$ be the unique element such that $\deg(u) < d$ and $uT \equiv 1 \pmod{\mathfrak{p}}$. Since we have:

$$\begin{pmatrix} 1 & 0 \\ T & 1 \end{pmatrix} = \begin{pmatrix} T^{-1} & 1 \\ 0 & T \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & T^{-1} \end{pmatrix}$$

the reductions of the matrices $\begin{pmatrix} 1 & 0 \\ T & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix}$ modulo $\mathfrak{p}$ lie in the same left $B(\mathfrak{f}_{\mathfrak{p}})$ -coset. As we saw in the proof of Lemma 6.4 the reductions of the elements of $M(\mathfrak{p})$ form a complete system of representatives for the left cosets of $B(\mathfrak{f}_{\mathfrak{p}})$ hence the matrices $\begin{pmatrix} 1 & 0 \\ T & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix}$ lie in the same left $\Gamma_0(\mathfrak{p})$ -coset. Therefore $o(\tilde{f}_{d-2})$ is equivalent to $\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \cdot v_{d-2}$ modulo the action of $\Gamma_0(\mathfrak{p})$. By Lemma 6.5 the claim now follows from the fact that $\deg(u) = d-1$. $\square$

Let h_0 and h_∞ denote the half-lines $\{e_0, \dots, e_n, \dots\}$ and $\{w_{\mathfrak{p}} \cdot e_0, \dots, w_{\mathfrak{p}} \cdot e_n, \dots\}$ on $\mathcal{T}$, respectively, where we continue to use the notation of the proofs of Lemma 6.6 and Proposition 6.9. For $i = 0, \infty$ let H_i denote the subgraph of $\mathcal{T}$ which is the half-line determined by h_i . For every $i \in \mathbb{P}^1(F)$ let Stab_i denote the subgroup of those elements of $\Gamma_0(\mathfrak{p})$ which leave i fixed where we let $\Gamma_0(\mathfrak{p})$ act on $\mathbb{P}^1(F)$ via the usual Möbius action.

Lemma 6.14. *Let i be an index such that either $i = 0$ or $i = \infty$ and let γ be an element of $\Gamma_0(\mathfrak{p})$. Then the following holds:*

- (i) *we have $\gamma(H_0) \cap H_\infty = \emptyset$,*
- (ii) *if $\gamma(H_i) \cap H_i \neq \emptyset$ then $\gamma \in \text{Stab}_i$.*

Proof. The images of H_0 and H_∞ in the quotient graph $\Gamma_0(\mathfrak{p})$ are disjoint maximal half-lines, hence claim (i) is clear. Assume now that $\gamma(H_i) \cap H_i \neq \emptyset$ for some i . Because the matrix $w_{\mathfrak{p}}$ interchanges the half-lines h_0 and h_∞ as well as the points 0 and ∞ on $\mathbb{P}^1(F)$ via its Möbius action we may assume that $i = 0$ by conjugating γ by $w_{\mathfrak{p}}$, if necessary. Let $n \in \mathbb{N} \cup \{-1\}$ be an index such that u_n lies in $\gamma(H_i) \cap H_i$. Then $u_n = \gamma(u_m)$ for some $m \in \mathbb{N} \cup \{-1\}$. Because $\tilde{u}_n$ is different from $\tilde{u}_m$ for every $m \neq n$ we must have $u_n = \gamma(u_n)$. Therefore we have:

$$\gamma \in \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} G_{n+d} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cap \Gamma_0(\mathfrak{p}) \subset \left\{ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \mid u \in \mathfrak{p} \right\} = \text{Stab}_0. \quad \square$$

7. THE REGULAR MODEL $\mathfrak{X}_0(\mathfrak{p})$

Definition 7.1. Let Ω denote the rigid analytic upper half plane, or Drinfeld's upper half plane over F_∞ . The set of ($\mathbb{C}_\infty$ -valued) points of Ω is $\mathbb{C}_\infty - F_\infty$, denoted also by Ω by abuse of notation. The group $GL_2(F_\infty)$ acts on Drinfeld's upper half plane on the left via Möbius transformations. The restriction of this action to $\Gamma_0(\mathfrak{n})$ is discrete, hence the set $\Gamma_0(\mathfrak{n}) \backslash \Omega$ has naturally the structure of a rigid analytic curve. Let $Y_0(\mathfrak{n})$ also denote the underlying rigid analytical space of the base change of $Y_0(\mathfrak{n})$ to F_∞ by abuse of notation.

Theorem 7.2. *There is a rigid-analytical isomorphism:*

$$Y_0(\mathfrak{n}) \cong \Gamma_0(\mathfrak{n}) \backslash \Omega.$$

Proof. See [2], Theorem 6.6. $\square$

Definition 7.3. Let X be a rigid analytic space over F_∞ and assume that $\mathcal{U}$ is an admissible covering of X by affinoids which is pure in the sense of [11] (for the definition of purity and the following concepts see 2.10 of [11] on page 116). We may associate a formal scheme $\mathfrak{X}$ to the data $(X, \mathcal{U})$ whose generic fiber in the sense of Raynaud is canonically isomorphic to X . The topological space underlying $\mathfrak{X}$ is the same as the topological space underlying the reduction $\overline{X}_{\mathcal{U}}$ of the rigid analytic space associated to X with respect to the cover $\mathcal{U}$. For every element U of the cover $\mathcal{U}$ let $\overline{U}$ denote its reduction in the sense used in [11]. By definition both $\overline{U}$ and $\overline{X}_{\mathcal{U}}$ are schemes over $\mathbf{f}_\infty$ and the natural map $\overline{U} \rightarrow \overline{X}_{\mathcal{U}}$ is an open immersion. Moreover for every U as above let $\mathfrak{U}$ denote the formal scheme:

$$\mathfrak{U} = \text{Spf}(\{f \in \mathcal{O}(U) \mid \|f\| \leq 1\}),$$

where $\text{Spf}(\cdot)$ denotes the formal spectrum and $\|\cdot\|$ denotes the supremum norm on $\mathcal{O}(U)$ with respect to some absolute value $|\cdot|$ on $\mathbb{C}_\infty$ corresponding to the valuation on this field. Then the topological spaces underlying $\mathfrak{U}$ and $\overline{U}$ are canonically homeomorphic. By definition the formal scheme $\mathfrak{X}$ is just the unique locally ringed space whose underlying topological space is $\overline{X}_{\mathcal{U}}$ such that the restriction of its structure sheaf $\mathcal{O}_{\mathfrak{X}}$ to the open $\overline{U}$ is the structure sheaf $\mathcal{O}_{\mathfrak{U}}$ of the formal scheme $\mathfrak{U}$ for every U as above.

Definition 7.4. Let $U(1)$ denote the rational subdomain of Ω whose underlying set of points is:

$$U(1) = \{z \in \mathbb{C}_\infty \mid |\pi| \leq |z| \leq 1, |z - c| \geq 1, |z - c\pi| \geq |\pi| \ (\forall c \in \mathbf{f}_\infty^*)\},$$

where $\pi \in F_\infty$ is a uniformizer. For every $\rho \in GL_2(F_\infty)$ and $z \in \mathbb{P}^1$ let $\rho(z)$ denote the image of z under the Möbius transformation corresponding to ρ . For every ρ as above let $U(\rho)$ denote the rational subdomain whose underlying set of points is:

$$U(\rho) = \{z \in \mathbb{C}_\infty \mid \rho^{-1}(z) \in U(1)\}.$$

The system $\mathcal{U} = \{U(\rho) \mid \rho \in GL_2(F_\infty)\}$ is a pure covering of Ω by affinoid subdomains. Let $\widehat{\Omega}$ denote the corresponding formal scheme. Because the cover $\mathcal{U}$ is invariant with respect to the Möbius action the formal scheme $\widehat{\Omega}$ is equipped with an action of $GL_2(F_\infty)$ such that for every $\rho \in GL_2(F_\infty)$ the automorphism of Ω induced by the action of ρ on $\widehat{\Omega}$ is the usual Möbius action of ρ .

Definition 7.5. By slightly extending the usual terminology we will call a scheme C defined over a field a curve if it is reduced, locally of finite type and of dimension one. A curve C is said to have normal crossings if every singular point of C is an ordinary double point in the usual sense. For any curve C with normal crossings let $\widetilde{C}$ denote its normalization, and let $\widetilde{S}(C)$ denote the pre-image of the set $S(C)$ of singular points of C . The incidence graph of C is the oriented graph whose set of vertices is the set of irreducible components of $\widetilde{C}$, and its set of edges is the set $\widetilde{S}(C)$ such that the original vertex of any edge $x \in \widetilde{S}(C)$ is the irreducible component of $\widetilde{C}$ which contains x and the terminal vertex of x is the irreducible component which contains the unique other element $\bar{x}$ of $\widetilde{S}(C)$ which maps with respect to the normalization map to the same singular point as x .

Remark 7.6. The special fiber $\widehat{\Omega}_{\mathbf{f}_\infty}$ of the formal scheme $\widehat{\Omega}$ is a curve with normal crossings over $\mathbf{f}_\infty$. The incidence graph of $\widehat{\Omega}_{\mathbf{f}_\infty}$ is canonically isomorphic to the Bruhat-Tits tree $\mathcal{T}$ in the sense that the natural action of $GL_2(F_\infty)$ on the incidence graph is the usual action of $GL_2(F_\infty)$ on the Bruhat-Tits tree under this identification. (We will give a more explicit description of this bijection in Definition 7.8 below.) We may form the quotient formal scheme $\Gamma_0(\mathfrak{n}) \backslash \widehat{\Omega}$. By the above the incidence graph of the special fiber of the latter is $\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$, which is not finite, hence the reduction of the formal scheme $\Gamma_0(\mathfrak{n}) \backslash \widehat{\Omega}$ is not even of finite type. In particular this formal scheme cannot be the formal completion of an algebraic curve over $\text{Spec}(\mathcal{O}_\infty)$ along its special fiber. Nevertheless there is a way to obtain a model from this formal scheme, using the work of Reversat in [23]. Next we will give our own account of this theory. Another possible reference is section 4.2 of [19].

Notation 7.7. Assume now that $q = 2$. For the sake of simple notation let Γ denote $\Gamma_0(\mathfrak{p})$ in the rest of this chapter. Let Γ_{tor} be the normal subgroup of Γ generated by the torsion elements, and let $\Gamma' = \Gamma / \Gamma_{tor}$. For $i = 0, \infty$ let H'_i denote the subgraph of $\mathcal{T}$ we get from H_i by removing its only vertex of degree one, where H_i is the graph which was introduced before Lemma 6.14. Moreover let G_i and G'_i denote the subgraph of $\mathcal{T}$ which is the union of the graphs $\gamma(H_i)$ and $\gamma(H'_i)$, respectively, where γ is an arbitrary element of Stab_i . If γ is an element of Γ such that $\gamma(G_i) \cap G_i \neq \emptyset$ then $\gamma \in \text{Stab}_i$ by Lemma 6.14. Similarly $\gamma(G_0) \cap G_\infty = \emptyset$ for every $\gamma \in \Gamma$.

Definition 7.8. By slight abuse of notation for every ringed space such as Ω or $\widehat{\Omega}_{\mathbf{f}_\infty}$ let the same symbol denote the underlying topological space, too. Let $\text{red}:\Omega \rightarrow \widehat{\Omega}_{\mathbf{f}_\infty}$ be the reduction map. It is a continuous $GL_2(F_\infty)$ -equivariant map between the underlying topological spaces. For every irreducible component v of $\widehat{\Omega}_{\mathbf{f}_\infty}$ let $ns(v)$ denote the topological subspace which we get from v by removing its singular points. For every edge e of the incidence graph of $\widehat{\Omega}_{\mathbf{f}_\infty}$ let $\widehat{e}$ denote the image of e under the normalization map. For every subgraph G of the incidence graph of $\widehat{\Omega}_{\mathbf{f}_\infty}$ the realization of G , denoted by $r(G)$, is the subspace of the topological space $\widehat{\Omega}_{\mathbf{f}_\infty}$ which is the union of the subspaces $ns(v)$, where v is any element of $\mathcal{V}(G)$, and the points $\widehat{e}$, where e is any element of $\mathcal{E}(G)$. For every edge e of the incidence graph of $\widehat{\Omega}_{\mathbf{f}_\infty}$ let $G(e)$ denote the subgraph whose vertices are $o(e)$ and $t(e)$ and whose edges are e and $\bar{e}$. For every $\rho \in GL_2(F_\infty)$ let $e(\rho)$ denote the edge of $\mathcal{T}$ represented by ρ . Under the identification between $\mathcal{T}$ and the incidence graph of $\widehat{\Omega}_{\mathbf{f}_\infty}$ which we mentioned in Remark 7.6 the pre-image of $r(G(e(\rho)))$ under the reduction map is the domain $U(\rho)$ for every $\rho \in GL_2(F_\infty)$.

Construction 7.9. For $i = 0, \infty$ let Ω_i and Ω'_i be the pre-image of $r(H_i)$ and $r(H'_i)$, respectively, under the reduction map. By definition Ω'_i is an open subdomain of Ω_i and these domains are invariant under the action of Stab_i . Moreover it is clear from the remark at the end of Notation 7.7 that if we have $\gamma(\Omega_i) \cap \Omega_j \neq \emptyset$ for some $\gamma \in \Gamma$ then $i = j$ and $\gamma \in \text{Stab}_i$. Hence the natural map $j_i : \text{Stab}_i \backslash \Omega_i \rightarrow \Gamma_{\text{tor}} \backslash \Omega$ is an open immersion. By Lemma 2.4 of [23] on page 384 for every i the quotient $\text{Stab}_i \backslash \Omega'_i$ is analytically isomorphic to a unit disc D_i with the origin removed. Let B_i be the rigid analytic space $\text{Stab}_i \backslash \Omega_i \cup D_i$ obtained by gluing D_i with $\text{Stab}_i \backslash \Omega_i$ along their common admissible subspace $\text{Stab}_i \backslash \Omega'_i$. For every $\gamma \in \Gamma'$ let B_i^γ be a copy of B_i . Denote by Σ the rigid analytic space

$$\Sigma = (\Gamma_{\text{tor}} \backslash \Omega) \cup \bigcup_{\gamma \in \Gamma'} B_0^\gamma \cup \bigcup_{\gamma \in \Gamma'} B_\infty^\gamma$$

obtained by gluing each B_i^γ with $\Gamma_{\text{tor}} \backslash \Omega$ along their common admissible subspace $\gamma(j_i(\text{Stab}_i \backslash \Omega_i))$. Let $f : \Omega \rightarrow \Gamma_{\text{tor}} \backslash \Omega \subset \Sigma$ be the canonical morphism of analytic spaces. By Lemma 2.6 of [23] on page 385 the system:

$$\mathcal{V} = \{f(U(\rho)) | e(\rho) \notin \mathcal{E}(G_0) \cup \mathcal{E}(G_\infty)\} \cup \{B_0^\gamma | \gamma \in \Gamma'\} \cup \{B_\infty^\gamma | \gamma \in \Gamma'\}$$

is a pure admissible covering of Σ by affinoids. Let $\widehat{\Sigma}$ denote the formal scheme associated to the data $(\Sigma, \mathcal{V})$. The natural action of the group Γ' on $\Gamma_{\text{tor}} \backslash \Omega$ extends uniquely to a discontinuous action on Σ . The group Γ' leaves the cover $\mathcal{V}$ invariant hence we may equip $\widehat{\Sigma}$ with an action of Γ' such that the induced action on Σ is the one above.

By construction the special fiber of $\Gamma \backslash \widehat{\Sigma}$ has incidence graph $\mathcal{G}(\mathfrak{p})$. In particular this graph is finite so the special fiber of $\Gamma \backslash \widehat{\Sigma}$ is proper. Hence by Grothendieck's algebraization theorem the formal scheme $\Gamma \backslash \widehat{\Sigma}$ is the formal completion of a projective curve $\mathfrak{X}_0(\mathfrak{p}) \rightarrow \text{Spec}(\mathcal{O}_\infty)$ along its special fiber. According to the main result of [23] (Theorem 2.7 on page 385):

Proposition 7.10. *The curve $\mathfrak{X}_0(\mathfrak{p})$ is a totally degenerate semi-stable model of $X_0(\mathfrak{p})$ over the spectrum of $\mathcal{O}_\infty$. $\square$*

Notation 7.11. By slight abuse of notation let the index i also denote the unique point of B_i which does not lie in $\text{Stab}_i \backslash \Omega_i$. Under the action of Γ' the corresponding points in the copies B_i^γ are all equivalent. Let i denote the common image of these points in the quotient $\Gamma' \backslash \Sigma$ as well. The identification of the rigid analytical space underlying the base change of $X_0(\mathfrak{n})$ to F_∞ and the quotient $\Gamma' \backslash \Sigma$ identifies the two cusps of $X_0(\mathfrak{p})$ and the points 0 and ∞ . We will use this identification without further notice.

Proposition 7.12. *The model $\mathfrak{X}_0(\mathfrak{p})$ is regular.*

Proof. Because $\mathfrak{X}_0(\mathfrak{p})$ is semi-stable and its base change to $\text{Spec}(F_\infty)$ is smooth, it is regular in the complement of the ordinary double points in the special fiber. The system:

$$\mathcal{V}_0 = \{f(U(\rho)) | e(\rho) \notin \mathcal{E}(G_0) \cup \mathcal{E}(G_\infty)\}$$

is a pure admissible covering by affinoids of the domain $\Sigma_0 \subset \Sigma$ it covers. Let $\widehat{\Sigma}_0$ denote the open formal subscheme of $\widehat{\Sigma}$ corresponding to the data $(\Sigma_0, \mathcal{V}_0)$. By construction Σ_0 is invariant under the action of Γ' and the open formal subscheme $\Gamma' \backslash \widehat{\Sigma}_0$ of $\mathfrak{X}_0(\mathfrak{p})$ contains every ordinary double point in the special fiber. The formal scheme $\Gamma' \backslash \widehat{\Sigma}_0$ is isomorphic to the quotient $\Gamma \backslash \widehat{\Omega}_0$ where $\widehat{\Omega}_0$ is the unique Γ -invariant open formal subscheme of $\widehat{\Omega}$ whose generic fiber in the sense of Raynaud is the domain $\Omega_0 \subset \Omega$ covered by the system:

$$\mathcal{U}_0 = \{U(\rho) | e(\rho) \notin \bigcup_{\gamma \in \Gamma} \mathcal{E}(\gamma(G_0)) \cup \bigcup_{\gamma \in \Gamma} \mathcal{E}(\gamma(G_\infty))\}.$$

By Corollary 6.12 the stabilizer of every edge of $\mathcal{G}(\mathfrak{p})$ is trivial. Hence the formal completion of the local ring at every ordinary double point v of the special fiber of $\Gamma \backslash \widehat{\Omega}_0$ is isomorphic to the formal completion of the local ring at any ordinary double point of the special fiber of $\widehat{\Omega}$ which maps to v with respect to the covering $\widehat{\Omega} \rightarrow \Gamma \backslash \widehat{\Omega}$ by the above. This completion is isomorphic to the ring $\mathcal{O}_\infty[[x, y]]/(xy - \pi)$, where π is again a uniformizer of F_∞ . As the latter is regular the claim is now clear. $\square$

Notation 7.13. Because the scheme $\mathfrak{X}_0(\mathfrak{p})$ over $\text{Spec}(\mathcal{O}_\infty)$ is projective, every F_∞ -valued point $P : \text{Spec}(F_\infty) \rightarrow X_0(\mathfrak{p})$ extends uniquely to an $\mathcal{O}_\infty$ -valued point $\text{Spec}(\mathcal{O}_\infty) \rightarrow \mathfrak{X}_0(\mathfrak{p})$ which we will denote by the same symbol by the usual abuse of notation. For every point $P \in X_0(\mathfrak{p})$ we define the reduction of P as the closed point which is the intersection of the section $P : \text{Spec}(\mathcal{O}_\infty) \rightarrow \mathfrak{X}_0(\mathfrak{p})$ and the special fiber of $\mathfrak{X}_0(\mathfrak{p})$. Let $\mathcal{J}_0(\mathfrak{p})$ and $\mathcal{W}(\mathfrak{p})$ denote the Néron model over $\mathbb{P}_{\mathbb{F}_q}^1$ of the Jacobian $J_0(\mathfrak{p})$ and the winding quotient $W(\mathfrak{p})$, respectively. By slight abuse of notation we are also going to let the same symbol denote the base change of this model to $\text{Spec}(\mathcal{O}_v)$, which is also the Néron model over this base, for every place v of F . Let $\mathfrak{X}_0^*(\mathfrak{p})$ denote the $\text{Spec}(\mathcal{O}_\infty)$ -scheme we get from $\mathfrak{X}_0(\mathfrak{p})$ by removing the ordinary double points in the special fiber. Because $\mathfrak{X}_0^*(\mathfrak{p})$ is smooth over $\text{Spec}(\mathcal{O}_\infty)$ there is a map $\mathfrak{X}_0^*(\mathfrak{p}) \rightarrow \mathcal{J}_0(\mathfrak{p})$ whose base change to $\text{Spec}(F_\infty)$ is the Albanese imbedding $X_0(\mathfrak{p}) \hookrightarrow J_0(\mathfrak{p})$ with base point 0. Let $\iota : \mathfrak{X}_0^*(\mathfrak{p}) \rightarrow \mathcal{W}(\mathfrak{p})$ denote the composition of this map and the morphism $h : \mathcal{J}_0(\mathfrak{p}) \rightarrow \mathcal{W}(\mathfrak{p})$ induced by the quotient map $J_0(\mathfrak{p}) \rightarrow W(\mathfrak{p})$.

Proposition 7.14. *The map $\iota : \mathfrak{X}_0^*(\mathfrak{p}) \rightarrow \mathcal{W}(\mathfrak{p})$ is a formal immersion at 0.*

Proof. For every scheme S over $\mathrm{Spec}(\mathcal{O}_\infty)$ let S_∞ denote its base change to $\mathrm{Spec}(\mathbf{f}_\infty)$. For any algebraic group G defined over a field K let $\mathrm{Cot}(G)$ denote the K -linear cotangent space of G at the identity element. Grothendieck duality furnishes an isomorphism:

$$\Theta : \mathrm{Cot}(\mathcal{J}_0(\mathfrak{p})_\infty) \rightarrow H^0(\mathfrak{X}_0(\mathfrak{p})_\infty, \omega)$$

where ω denotes the relative dualizing sheaf of the curve $\mathfrak{X}_0(\mathfrak{p})_\infty$ (see section e of [14] on page 140). According to section b of [1] on page 77 the sheaf ω is the sheaf of 1-forms η on the normalization of $\mathfrak{X}_0(\mathfrak{p})_\infty$ which are regular except for simple poles at the points in $\tilde{S}(\mathfrak{X}_0(\mathfrak{p})_\infty)$, and for every element e of $\tilde{S}(\mathfrak{X}_0(\mathfrak{p})_\infty)$ we have $\mathrm{Res}_e(\eta) + \mathrm{Res}_{\bar{e}}(\eta) = 0$. By the residue theorem for every $\eta \in H^0(\mathfrak{X}_0(\mathfrak{p})_\infty, \omega)$ the map $\mathrm{Res}(\eta) : \tilde{S}(\mathfrak{X}_0(\mathfrak{p})_\infty) \rightarrow \mathbf{f}_\infty$ given by the rule $e \mapsto \mathrm{Res}_e(\eta)$ is a harmonic cochain on the incidence graph $\mathcal{G}(\mathfrak{p})$ of $\mathfrak{X}_0(\mathfrak{p})_\infty$. Because $\mathfrak{X}_0(\mathfrak{p})_\infty$ is totally degenerate the homomorphism:

$$\mathrm{Res} : H^0(\mathfrak{X}_0(\mathfrak{p})_\infty, \omega) \rightarrow H(\mathcal{G}(\mathfrak{p}), \mathbf{f}_\infty)$$

given by the rule $\eta \mapsto \mathrm{Res}(\eta)$ is an isomorphism.

Let T be a split torus over the field K . Then $\mathrm{Cot}(T)$ is canonically isomorphic to $\mathrm{Hom}(T, \mathbb{G}_m) \otimes K$ where $\mathrm{Hom}(T, \mathbb{G}_m)$ is the character group of T . Let A be an abelian variety over F_∞ which has a rigid-analytical uniformization by a split torus U over F_∞ . Then the connected component of the identity of the special fiber of the Néron model of A over $\mathrm{Spec}(\mathcal{O}_\infty)$ is canonically isomorphic to the split torus U' over $\mathbf{f}_\infty$ whose group of characters is $\mathrm{Hom}(U, \mathbb{G}_m)$. Hence the cotangent space of the group variety $\mathcal{J}_0(\mathfrak{p})_\infty$ and $\mathcal{W}(\mathfrak{p})_\infty$ is isomorphic to $\bar{\Gamma}_0(\mathfrak{p}) \otimes \mathbf{f}_\infty$ and $\Lambda(\mathfrak{p}) \otimes \mathbf{f}_\infty$, respectively, and the homomorphism $h^* : \mathrm{Cot}(\mathcal{W}(\mathfrak{p})_\infty) \rightarrow \mathrm{Cot}(\mathcal{J}_0(\mathfrak{p})_\infty)$ induced by the morphism h introduced in Notation 7.13 above is $\lambda \otimes \mathrm{id}_{\mathbf{f}_\infty}$ under this identification where $\lambda : \Lambda(\mathfrak{p}) \rightarrow \bar{\Gamma}_0(\mathfrak{p})$ is the inclusion map.

For every $\eta \in H(\mathcal{G}(\mathfrak{p}), \mathbf{f}_\infty)$ let the same symbol denote the extension of η to a function $\mathcal{E}(\Gamma_0(\mathfrak{p}) \setminus \mathcal{T}) \rightarrow \mathbf{f}_\infty$ which is zero on every edge not in $\mathcal{E}(\mathcal{G}(\mathfrak{p}))$. This extension is a harmonic cochain on $\Gamma_0(\mathfrak{p}) \setminus \mathcal{T}$. The pull-back of every η as above with respect to the quotient map $\mathcal{E}(\mathcal{T}) \rightarrow \mathcal{E}(\Gamma_0(\mathfrak{p}) \setminus \mathcal{T})$ is a harmonic cochain by Corollary 6.12. Hence we may consider $H(\mathcal{G}(\mathfrak{p}), \mathbf{f}_\infty)$ as a subgroup of $H(\mathcal{T}, \mathbf{f}_\infty)^{\Gamma_0(\mathfrak{p})}$. Under this identification the map:

$$\mathrm{Res} \circ \Theta : \bar{\Gamma}_0(\mathfrak{p}) \otimes \mathbf{f}_\infty \cong \mathrm{Cot}(\mathcal{J}_0(\mathfrak{p})_\infty) \rightarrow H(\mathcal{G}(\mathfrak{p}), \mathbf{f}_\infty) \subseteq H(\mathcal{T}, \mathbf{f}_\infty)^{\Gamma_0(\mathfrak{p})}$$

is $R \otimes \mathrm{id}_{\mathbf{f}_\infty}$ where R denotes the reduction modulo 2. According to the differential condition for being a formal immersion we need to show that there is an $\eta \in H^0(\mathfrak{X}_0(\mathfrak{p})_\infty, \omega)$ in the image of the map $\Theta \circ h^*$ which does not vanish at the reduction of 0. The latter lies on the irreducible component $\tilde{u}_{-1}$. Every non-zero 1-form on the projective line $\mathbb{P}_{\mathbf{f}_\infty}^1$ which is regular except for simple poles at two closed points is actually non-zero at every point where it is regular. By the above the image of $\Theta \circ h^*$, considered as a subgroup of $H(\mathcal{T}, \mathbf{f}_\infty)^{\Gamma_0(\mathfrak{p})}$, is the reduction of $\Lambda(\mathfrak{p})$ modulo 2. The proposition now follows from claim (ii) of Proposition 6.13. $\square$

8. MOD $\mathfrak{p}$ GALOIS REPRESENTATIONS OF RANK TWO DRINFELD MODULES WITH GOOD REDUCTION EVERYWHERE

Definition 8.1. At the beginning of this chapter we will not need to assume that $q = 2$. For every Drinfeld module $\phi : A \rightarrow B\{\tau\}$, where B is an A -algebra, and for

every non-zero ideal $\mathfrak{n} \triangleleft A$ let $\phi[\mathfrak{n}]$ denote the $\mathfrak{n}$ -torsion group scheme of ϕ as usual. Recall that the latter is a finite, flat subgroup-scheme of $\mathbb{G}_a$ over $\text{Spec}(B)$. We say that an A -algebra B has characteristic $\mathfrak{p}$ if the annihilator of the A -module B contains $\mathfrak{p}$. This assumption implies that B is an $\mathbf{f}_{\mathfrak{p}}$ -algebra. Similarly we will say that a Drinfeld module $\phi : A \rightarrow B\{\tau\}$ has characteristic $\mathfrak{p}$ if B has characteristic $\mathfrak{p}$. Let $f \in \mathfrak{p}$ be a generator of the ideal $\mathfrak{p}$.

Lemma 8.2. *For every field extension $\mathbf{k}$ of $\mathbf{f}_{\mathfrak{p}}$ and for every rank two Drinfeld module $\phi : A \rightarrow \mathbf{k}\{\tau\}$ of characteristic $\mathfrak{p}$ the degree of the lowest non-zero term of the polynomial:*

$$\phi(f) = \sum_{n=0}^{2 \deg(\mathfrak{p})} a_n \tau^n \in \mathbf{k}\{\tau\}$$

is either $\deg(\mathfrak{p})$ or $2 \deg(\mathfrak{p})$.

Proof. According to the remark following Proposition 5.1 of [3], page 178 the polynomial $\phi(f)$ has no terms of degree less than $\deg(\mathfrak{p})$. Recall that the subgroup-scheme $\phi[\mathfrak{p}]$ of the additive group scheme over $\mathbf{k}$ is defined by the equation

$$\sum_{n=0}^{2 \deg(\mathfrak{p})} a_n x^{q^{n \deg(\mathfrak{p})}} = 0.$$

If the degree of the lowest non-zero term of $\phi(f)$ is not $\deg(\mathfrak{p})$ then the group scheme $\phi[\mathfrak{p}]$ is connected by Satz 5.3 of [3], page 179. Hence $\phi(f)$ has no non-zero terms of degree less than $2 \deg(\mathfrak{p})$. As the leading coefficient of $\phi(f)$ is the same as the leading coefficient of f the claim is now clear. $\square$

Definition 8.3. Let $\phi : A \rightarrow \mathcal{O}_{\mathfrak{p}}\{\tau\}$ be a Drinfeld module of rank two over $\mathcal{O}_{\mathfrak{p}}$. Let $f \in \mathfrak{p}$ be a generator of the ideal $\mathfrak{p}$ as above and let

$$\phi(f) = \sum_{n=0}^{2 \deg(\mathfrak{p})} a_n \tau^n \in \mathcal{O}_{\mathfrak{p}}\{\tau\}.$$

According to Lemma 8.2 we have:

$$\mathfrak{p}(a_i) > 0 \quad \text{for } i < d, \quad \text{and} \quad \mathfrak{p}(a_d) = 0,$$

where d is either $\deg(\mathfrak{p})$ or $2 \deg(\mathfrak{p})$, when we will say that ϕ has ordinary or supersingular reduction, respectively, following the usual terminology. For simplicity let U denote the $\text{Gal}(\overline{F}_{\mathfrak{p}}|F_{\mathfrak{p}})$ -module $\phi[\mathfrak{p}](\overline{F}_{\mathfrak{p}})$. Recall that the latter has the structure of a vector space over $\mathbf{f}_{\mathfrak{p}}$ of dimension 2 and the action of $\text{Gal}(\overline{F}_{\mathfrak{p}}|F_{\mathfrak{p}})$ is $\mathbf{f}_{\mathfrak{p}}$ -linear.

Lemma 8.4. *The Galois module U is irreducible when ϕ has supersingular reduction.*

Proof. Note that $t \in \overline{F}_{\mathfrak{p}}$ is a non-zero element of U if and only if it is a root of the polynomial:

$$g_f(x) = a_0 + a_1 x^{q-1} + \cdots + a_k x^{q^k-1} + \cdots + a_{2 \deg(\mathfrak{p})} x^{q^{2 \deg(\mathfrak{p})}-1}.$$

Therefore it will be sufficient to prove that g_f is irreducible in $F_{\mathfrak{p}}[x]$. Because $a_0 = f$ the latter follows at once from the Schönemann-Eisenstein criterion. $\square$

Proposition 8.5. *Assume that ϕ has ordinary reduction. Then the following holds:*

(i) *there is an exact sequence of Galois modules:*

$$0 \rightarrow U_0 \rightarrow U \rightarrow U_1 \rightarrow 0$$

such that the Galois module U_0 is a one-dimensional $\mathbf{f}_p$ -linear sub-vector space,

(ii) *the Galois module U_1 is unramified.*

Proof. Let $\mathfrak{p} : \overline{F}_p^* \rightarrow \mathbb{Q}$ denote the extension of the valuation $\mathfrak{p}$ to the separable closure $\overline{F}_p$, too. Because ϕ has good reduction we have $\mathfrak{p}(t) \geq 0$ for every $t \in U$. Let U_0 denote the subset:

$$\{t \in U \mid \mathfrak{p}(t) > 0\} \subseteq U.$$

Clearly $0 \in U_0$, moreover U_0 is closed under addition and left invariant by the action of the absolute Galois group of F_p . Let $g \in A$ be arbitrary. Then we have:

$$\phi(g) = \sum_{n=0}^{2 \deg(g)} b_n \tau^n$$

for some $b_n \in \mathcal{O}_p$. Hence for every $t \in U_0$ we have $\mathfrak{p}(\phi(g)(t)) > 0$ therefore U_0 is an A -module under the action of A on $\overline{F}_p$ induced by ϕ . In particular U_0 is an $\mathbf{f}_p$ -subspace of U . Let U_1 denote the quotient of U by this Galois-invariant subspace. As we already noted $t \in \overline{F}_p^*$ is an element of U if and only if it is the root of the polynomial:

$$g_f(x) = a_0 + a_1 t^{q-1} + \dots + a_k t^{q^k-1} + \dots + a_{2 \deg(\mathfrak{p})} t^{q^{2 \deg(\mathfrak{p})}-1}.$$

Let d denote $\deg(\mathfrak{p})$ for simplicity. Because ϕ has ordinary reduction we know that

$$\mathfrak{p}(a_0) = 1, \mathfrak{p}(a_k t^{q^k-1}) \geq 1 + (q^k - 1)\mathfrak{p}(t) \ (k < d), \mathfrak{p}(a_d t^{q^d-1}) = (q^d - 1)\mathfrak{p}(t), \text{ and}$$

$$\mathfrak{p}(a_k t^{q^k-1}) \geq (q^k - 1)\mathfrak{p}(t) \ (d < k \leq 2d),$$

hence by comparing valuations we get that $\mathfrak{p}(t) = (q^{\deg(\mathfrak{p})} - 1)^{-1}$, if t is an element of U_0 , and $\mathfrak{p}(t) = 0$, otherwise. Because

$$f = a_0 = \prod_{0 \neq t \in U} t,$$

we get that the cardinality of U_0 is $q^{\deg(\mathfrak{p})}$ by comparing the valuations of both sides. Claim (i) is now clear. Let $\mathfrak{M}$ and $\mathfrak{M}^+$ denote the groups

$$\mathfrak{M} = \{x \in \overline{F}_p \mid \mathfrak{p}(x) \geq 0\} \quad \text{and} \quad \mathfrak{M}^+ = \{x \in \overline{F}_p \mid \mathfrak{p}(x) > 0\},$$

respectively. The natural action of $\text{Gal}(\overline{F}_p | F_p)$ on the quotient group $V_0 = \mathfrak{M}/\mathfrak{M}^+$ is unramified by Proposition 7 of [27] on page 268. From the discussion above it is clear that the group U_1 injects into V_0 . Claim (ii) is now clear. $\square$

Definition 8.6. Recall that in Definition 4.2.1 of [12] on page 65 an A -submodule $\Lambda \subset \overline{F}_\infty$ is called an F -lattice if it satisfies the following properties:

- (i) it is finitely generated and free as an A -module,
- (ii) it is left invariant by the action of the absolute Galois group $\text{Gal}(\overline{F}_\infty|F_\infty)$,
- (iii) it is discrete, that is, its intersection with every open disk is finite.

Lemma 8.7. *Let $\Lambda \subset \overline{F}_\infty$ be an F -lattice. Then the absolute Galois group $\text{Gal}(\overline{F}_\infty|F_\infty)$ of F_∞ acts on Λ through a finite quotient.*

Proof. Because Λ is discrete and finitely generated there is an open disc D around $0 \in F_\infty$ such that the finite set $D \cap \Lambda$ generates Λ as an A -module. The absolute value on $\overline{F}_\infty$ is invariant with respect to the Galois action therefore the action of $\text{Gal}(\overline{F}_\infty|F_\infty)$ leaves $D \cap \Lambda$ invariant. Every element of $\text{Gal}(\overline{F}_\infty|F_\infty)$ fixing $D \cap \Lambda$ must act trivially on Λ , too, therefore the action of $\text{Gal}(\overline{F}_\infty|F_\infty)$ on Λ has finite image. $\square$

Let B denote the group scheme of invertible upper triangular two by two matrices.

Lemma 8.8. *Every finite subgroup of $GL_2(A)$ is either conjugate to a subgroup of $GL_2(\mathbb{F}_2) \subset GL_2(A)$ or it is a conjugate to a subgroup of $B(A) \subset GL_2(A)$.*

Proof. Let G be a finite subgroup of $GL_2(A)$. Because $GL_2(A)$ acts without inversions on the Bruhat-Tits tree $\mathcal{T}$ via its natural embedding into $GL_2(F_\infty)$, so does G . Every finite group acting on a tree without inversion has a fixed vertex. Therefore G has a fixed vertex with respect to the action above. Hence it will be conjugate to a subgroup of the stabilizer of the vertex v_n for some n . The claim now follows from Proposition 3 of 1.6 in [28] on pages 86-87. $\square$

Proposition 8.9. *Let $\phi : A \rightarrow F_\infty\{\tau\}$ be a Drinfeld module of rank two over F_∞ and fix a $\mathbf{f}_\mathfrak{p}$ -linear isomorphism $i : \phi[\mathfrak{p}] \rightarrow \mathbf{f}_\mathfrak{p}^2$. Then the image of the homomorphism $h : \text{Gal}(\overline{F}_\infty|F_\infty) \rightarrow GL_2(\mathbf{f}_\mathfrak{p})$ induced by this identification is conjugate to a subgroup of the reduction of a subgroup $G \subset GL_2(A)$ modulo $\mathfrak{p}$, where G is either $GL_2(\mathbb{F}_2)$ or $B(A)$.*

Proof. By Theorem 4.6.9 of [12] on pages 76-78 there is an F -lattice $\Lambda \subset \overline{F}_\infty$, which has rank two as an A -module, such that the Drinfeld module ϕ is uniformized by the Carlitz exponential e_Λ (defined in 4.2.3 of [12] on page 65). In particular for every ideal $\mathfrak{n} \triangleleft A$ the Galois module $\mathfrak{n}^{-1}\Lambda/\Lambda$ is isomorphic to $\phi[\mathfrak{n}]$ where $\mathfrak{n}^{-1} \subseteq F$ is the fractional ideal: $\{a \in F | ab \in A (\forall b \in \mathfrak{n})\}$. The claim is now obvious from Lemmas 8.7 and 8.8. $\square$

Assume now that $q = 2$.

Theorem 8.10. *Let $\phi : A \rightarrow F\{\tau\}$ be a Drinfeld module of rank two which has good reduction at every place of F different from ∞ . Assume that $\deg(\mathfrak{p}) \geq 3$. Then ϕ does not have a $\text{Gal}(\overline{F}|F)$ -invariant cyclic $\mathfrak{p}$ -torsion subgroup.*

Proof. Assume that the claim is false. Then there is a Drinfeld module ϕ which satisfies the condition in the claim above such that there is an exact sequence of $\text{Gal}(\overline{F}|F)$ -modules:

$$0 \rightarrow V_0 \rightarrow \phi[\mathfrak{p}] \rightarrow V_1 \rightarrow 0$$

such that the Galois modules V_0 and V_1 have dimension one as vector spaces over $\mathbf{f}_{\mathfrak{p}}$. Let $\rho_i : \text{Gal}(\overline{F}|F) \rightarrow \mathbf{f}_{\mathfrak{p}}^*$ denote the modular Galois representation corresponding to the $\text{Gal}(\overline{F}|F)$ -module V_i (where $i = 1$ or 2). For every place v of F choose a decomposition group $D_v < \text{Gal}(\overline{F}|F)$. The restriction of ρ_i to D_v is unramified when v is different from $\mathfrak{p}$ or ∞ since the Drinfeld module ϕ has good reduction at every place of F different from ∞ . We also know that the restriction of ρ_i to D_{∞} is at most tamely ramified. Because the residue field of F_{∞} has trivial multiplicative group every tamely ramified abelian representation of D_{∞} is in fact unramified by local class field theory. Hence ρ_i can be ramified only at $\mathfrak{p}$.

By Lemma 8.4 the Drinfeld module ϕ has good ordinary reduction at $\mathfrak{p}$. Hence there is an exact sequence of $D_{\mathfrak{p}}$ -modules:

$$0 \rightarrow U_0 \rightarrow \phi[\mathfrak{p}] \rightarrow U_1 \rightarrow 0$$

such that the Galois modules U_0 and U_1 have dimension one as vector spaces over $\mathbf{f}_{\mathfrak{p}}$ by Proposition 8.6. Moreover the $D_{\mathfrak{p}}$ -module U_1 is unramified by part (ii) of Proposition 8.6. It is also isomorphic to one of the $D_{\mathfrak{p}}$ -modules V_0 and V_1 . Hence either for $i = 0$ or for $i = 1$ the Galois representation ρ_i is everywhere unramified. Fix such an i . Let ϕ' denote the Drinfeld module ϕ when $i = 0$ and let ϕ' denote the Drinfeld module we get from ϕ by dividing out by the Galois-invariant $\mathfrak{p}$ -torsion subgroup V_0 when $i = 1$. In both cases the $\mathfrak{p}$ -torsion of the Drinfeld module ϕ' contains a $\text{Gal}(\overline{F}|F)$ -submodule isomorphic to V_i and ϕ' has potentially good reduction at every place of F different from ∞ .

By Proposition 8.9 the image of D_{∞} under ρ_i is a subgroup of either $B(A)$ or $GL_2(\mathbb{F}_2)$. It is also a subgroup of $\mathbf{f}_{\mathfrak{p}}^*$ hence it is a group of odd order. Every finite subgroup of $B(A)$ is a 2-group and the finite group $GL_2(\mathbb{F}_2)$ only has elements of order 1, 2 or 3. Hence the image of D_{∞} under ρ_i is either trivial or a group of order 3. The latter is only possible when 3 divides the order of $\mathbf{f}_{\mathfrak{p}}^*$. The latter holds if and only if $\deg(\mathfrak{p})$ is even. For every $n \in \mathbb{N}$ let F_n denote the constant field extension of F of degree n , that is the unique everywhere unramified extension of F of degree n . We get that the Drinfeld module ϕ' has a non-zero F_n -rational $\mathfrak{p}$ -torsion point where $n = 1$ if $\deg(\mathfrak{p})$ is odd, and $n = 3$, otherwise. In the latter case we have $\deg(\mathfrak{p}) \geq 4$. Now it is clear the theorem follows from the lemma below. $\square$

Let T denote the place of F corresponding to the prime ideal $(T) \triangleleft A$ as well.

Lemma 8.11. *Let $\phi : A \rightarrow F\{\tau\}$ be a Drinfeld module of rank two over F and let $\mathfrak{n} \triangleleft A$ be a non-zero ideal. Assume that ϕ has an F_n -rational non-zero $\mathfrak{n}$ -torsion point for some $n < \deg(\mathfrak{n})$ which is not an $\mathfrak{m}$ -torsion point for any proper divisor $\mathfrak{m}$ of $\mathfrak{n}$. Then ϕ does not have potentially good reduction at the place T .*

Proof. Assume that the claim is false and let ϕ be a Drinfeld module which is a counterexample. If we set $\phi(T) = T + g\tau + \Delta\tau^2 \in F\{\tau\}$ then the j -invariant $j(\phi) = g^3/\Delta$ of ϕ lies in $\mathcal{O}_T$ by assumption. For every $k \in F_T$ let $\phi_k : A \rightarrow F_T\{\tau\}$ denote the unique Drinfeld module with the property: $\phi_k(T) = T + kg\tau + k^3\Delta\tau^2$. Clearly ϕ_k is isomorphic to ϕ over F_T . For a suitable choice of k we have $0 \leq T(k^3\Delta) \leq 2$. Fix such a k and let $h, \Gamma \in F_T$ be such that $\phi_k(T) = T + h\tau + \Gamma\tau^2$. Let K denote the unique unramified extension of F_T of degree n . Let $\mathcal{R}$ be the valuation ring of K .

Assume first that $T(\Gamma) = 0$. Because ϕ_k is isomorphic to the base change of ϕ to F_T there is a $\mathfrak{n}$ -torsion point $y \in (\phi_k K)_{\text{tors}}$ which is not an $\mathfrak{m}$ -torsion

point for any proper divisor $\mathfrak{m}$ of $\mathfrak{n}$. By assumption $T(\Delta) \leq 3T(g)$ hence we have $T(h) = T(kg) \geq 0$. Therefore ϕ_k gives rise to a Drinfeld module over $\mathcal{O}_T$. In particular $y \in \mathcal{R}$ and the reduction map modulo the maximal ideal of $\mathcal{R}$ is injective restricted to the A -module $\{\phi_k(t)(y) | t \in A\}$. The latter has order $2^{\deg(\mathfrak{n})}$ but the cardinality of the residue field of K is 2^n . This is a contradiction.

Assume now that $T(\Gamma) \neq 0$. The separable extension L of K we get by adjoining a third root λ of the element Γ has degree 3 over K . This is a ramified extension because 3 does not divide the valuation of Γ by assumption. Hence the residue field of L is the same as the residue field of K . Let $\psi : A \rightarrow L\{\tau\}$ denote the Drinfeld module of rank two such that $\psi(T) = T + \lambda^{-1}h\tau + \tau^2$. Then ψ is isomorphic to the base change of ϕ to L hence there is a $\mathfrak{n}$ -torsion point $y \in (\psi L)_{\text{tors}}$ which is not an $\mathfrak{m}$ -torsion point for any proper divisor $\mathfrak{m}$ of $\mathfrak{n}$. On the other hand $\psi(T) \in \mathcal{O}_L\{\tau\}$, where $\mathcal{O}_L$ is the valuation ring of L , hence ψ gives rise to a Drinfeld module over $\mathcal{O}_L$. Now we may conclude the argument as above. $\square$

Proposition 8.12. *Let $\phi : A \rightarrow F\{\tau\}$ be a Drinfeld module of rank two which has j -invariant $j(\phi) = 0$. Assume that $\deg(\mathfrak{p})$ is even and at least 4. Then ϕ does not have a $\text{Gal}(\overline{F}|F)$ -invariant cyclic $\mathfrak{p}$ -torsion subgroup.*

Proof. By assumption $\phi(T) = T + k\tau^2$ for some $k \in F^*$. Let $\psi : A \rightarrow F\{\tau\}$ denote the unique Drinfeld module with the property: $\psi(T) = T + \tau^2$. Let $K = \mathbb{F}_4(T)$ be the unique everywhere unramified extension of F of degree two and let $B = \mathbb{F}_4[T]$ be the integral closure of A in K . Both ϕ and ψ can be extended uniquely to an $\mathbb{F}_4$ -algebra homomorphism $B \rightarrow K\{\tau\}$ which will be denoted by the same symbol. These homomorphisms are Drinfeld B -modules of rank one over K . If $l \in \overline{F}^*$ is a third root of k then the linear map $x \mapsto lx$ induces an isomorphism of Drinfeld B -modules from ϕ to ψ over $\overline{F}$. Now assume that the claim of the proposition is false and let $M \subset \phi[\mathfrak{p}](\overline{F})$ be a $\text{Gal}(\overline{F}|F)$ -invariant A -submodule which has dimension one as a vector space over $\mathfrak{f}_{\mathfrak{p}}$. Let $M' = lM$ denote the image of M under the linear map $x \mapsto lx$. For every $\sigma \in \text{Gal}(\overline{F}|F)$ and $x \in \overline{F}$ let x^σ denote the image of x under σ . Because $l^\sigma/l \in \mathbb{F}_4^*$ for every $\sigma \in \text{Gal}(\overline{F}|F)$ we get that

$$\bigcup_{\sigma \in \text{Gal}(\overline{F}|F)} \{x^\sigma | x \in M'\} \subseteq \bigcup_{\epsilon \in \mathbb{F}_4^*} \epsilon M'.$$

This property can be reformulated as follows. Let $\mathbb{P}$ denote the set of $\mathfrak{f}_{\mathfrak{p}}$ -linear subspaces of $\psi[\mathfrak{p}](\overline{F})$ of dimension one. Because the action of $\text{Gal}(\overline{F}|F)$ on $\psi[\mathfrak{p}](\overline{F})$ is $\mathfrak{f}_{\mathfrak{p}}$ -linear there is an induced action on $\mathbb{P}$. By the above the $\text{Gal}(\overline{F}|F)$ -orbit of M' in $\mathbb{P}$ lies in its orbit with respect to the action of $\mathbb{F}_4^*$. We will show that $\mathbb{P}$ has no such element. Because $\deg(\mathfrak{p})$ is even the prime ideal $\mathfrak{p}$ splits to the product of two different prime ideals $\mathfrak{p}_0 \triangleleft B$ and $\mathfrak{p}_1 \triangleleft B$ in B . Clearly $\psi[\mathfrak{p}](\overline{F}) = \psi[\mathfrak{p}_0](\overline{F}) \oplus \psi[\mathfrak{p}_1](\overline{F})$ and for $i = 0, 1$ the B -module $\psi[\mathfrak{p}_i](\overline{F})$ has dimension one as a vector space over $\mathfrak{f}_{\mathfrak{p}}$. Moreover $\psi[\mathfrak{p}_i](\overline{F})$ is invariant under the action of $\text{Gal}(\overline{F}|K)$. Let $\epsilon_i : \text{Gal}(\overline{F}|K) \rightarrow \mathfrak{f}_{\mathfrak{p}}^*$ denote the modular Galois representation corresponding to the $\text{Gal}(\overline{F}|K)$ -module $\psi[\mathfrak{p}_i](\overline{F})$ (where $i = 0$ or 1). The Galois representation ϵ_i is unramified at the place $\mathfrak{p}_{1-i}$ because the Drinfeld module ψ has good reduction at every place of K different from the unique place above ∞ .

We claim that the restriction of ϵ_i to the inertia group at $\mathfrak{p}_i$ is a character of

order $2^{\deg(\mathfrak{p})} - 1$. Let $f_i \in \mathfrak{p}_i$ be a monic generator. Then

$$\psi(f_i) = \sum_{j=0}^{\deg(\mathfrak{p})/2} a_{ij} \tau^j \in B\{\tau\}.$$

We have $a_{i0} = f_i$ and $a_{i \deg(\mathfrak{p})/2} = 1$ because f_i is monic. Moreover $a_{ij} \in \mathfrak{p}_i$ for $j = 0, 1, \dots, \deg(\mathfrak{p})/2 - 1$ because the base change of the finite, flat group scheme $\psi[\mathfrak{p}_i]$ to the residue field of K_i is connected where K_i denotes the completion of K with respect to $\mathfrak{p}_i$. Note that $t \in \overline{K}_i$ is a non-zero element of $\psi[\mathfrak{p}_i](\overline{K}_i)$ if and only if it is a root of the polynomial:

$$g_i(x) = a_{i0} + a_{i1}x^3 + \dots + a_{ik}x^{4^k-1} + \dots + a_{i \deg(\mathfrak{p})/2}x^{2^{\deg(\mathfrak{p})}-1}.$$

Therefore it will be sufficient to prove that g_i is irreducible in $\tilde{K}_i[x]$ where $\tilde{K}_i$ is the maximal unramified extension of K_i . The latter follows at once from the Schönemann-Eisenstein criterion.

Therefore the order of the character $\epsilon_0 \cdot \epsilon_1^{-1}$ is $2^{\deg(\mathfrak{p})} - 1$ because its order is already $2^{\deg(\mathfrak{p})} - 1$ restricted to the inertia group at $\mathfrak{p}_i$ (where $i = 0$ or 1). Hence the action of $\text{Gal}(\overline{F}|K)$ on the complement of $\{\psi[\mathfrak{p}_0](\overline{F})\} \cup \{\psi[\mathfrak{p}_1](\overline{F})\}$ in $\mathbb{P}$ is transitive. Because $2^{\deg(\mathfrak{p})} - 1 > 3$ we get that no element of this complement can have the property above. Let $\sigma \in \text{Gal}(\overline{F}|F)$ be an element whose image in the quotient group $\text{Gal}(K|F)$ is the generator. The action of σ on the places of K will interchange $\mathfrak{p}_0$ and $\mathfrak{p}_1$ so its action on $\text{Gal}(\overline{F}|K)$ via conjugation interchanges the characters ϵ_0 and ϵ_1 . Hence it must interchange the submodules $\psi[\mathfrak{p}_0](\overline{F})$ and $\psi[\mathfrak{p}_1](\overline{F})$ as well. Since these elements of $\mathbb{P}$ are fixed by the action of $\mathbb{F}_4^*$ they could not have the property either. $\square$

9. THE PROOFS OF THEOREM 1.2 AND COROLLARY 1.7

Notation 9.1. Let $\mathfrak{m} \triangleleft A$ be an arbitrary non-zero ideal. For every $(\alpha, \beta) \in (A/\mathfrak{m})^2$, and n integer let

$$W_{\mathfrak{m}}(\alpha, \beta, n) = \{0 \neq (a, b) \in A^2 \mid (a, b) \equiv (\alpha, \beta) \pmod{\mathfrak{m}}, -n = \min(\infty(a), \infty(b))\}.$$

For every (α, β) as above and N positive integer let $\epsilon_{\mathfrak{m}}(\alpha, \beta, N)(z)$ denote the function:

$$\epsilon_{\mathfrak{m}}(\alpha, \beta, N)(z) = \prod_{n \leq N} \left(\prod_{(a,b) \in W_{\mathfrak{m}}(\alpha, \beta, n)} (az + b) \cdot \prod_{(c,d) \in W_{\mathfrak{m}}(0,0,n)} (cz + d)^{-1} \right).$$

on the set Ω . The latter is clearly holomorphic in the variable z . According to Lemma 4.5 of [17] on pages 145-146 the limit

$$\epsilon_{\mathfrak{m}}(\alpha, \beta)(z) = \lim_{N \rightarrow \infty} \epsilon_{\mathfrak{m}}(\alpha, \beta, N)(z)$$

converges uniformly in z on every admissible open subdomain of Ω and defines a holomorphic function.

Definition 9.2. If $\psi : A \rightarrow \mathbb{C}_\infty\{\tau\}$ is a Drinfeld module of rank two over A , then

$$\psi(T) = T + g(\psi)\tau + \Delta(\psi)\tau^2,$$

where g and Δ are Drinfeld modular forms of weight $q-1$ and q^2-1 , respectively. Under the identification of Theorem 7.2 g and Δ are holomorphic functions on Ω and they are equal to:

$$g(z) = \sum_{(0,0) \neq (\alpha,\beta) \in (A/(T))^2} \epsilon_{(T)}(\alpha, \beta)(z), \quad \Delta(z) = \prod_{(0,0) \neq (\alpha,\beta) \in (A/(T))^2} \epsilon_{(T)}(\alpha, \beta)(z),$$

which is an immediate consequence of the uniformization theory of Drinfeld modules over $\mathbb{C}_\infty$.

Let K be an extension of F and let P be a K -valued point of $X_0(\mathfrak{p})$. Let (ϕ, G) be the Drinfeld module of rank two over K equipped with a $\text{Gal}(\overline{K}|K)$ -invariant cyclic $\mathfrak{p}$ -torsion subgroup G which corresponds to the point P . The j -invariant $j(P)$ of P is the j -invariant $j(\phi) \in K$ of the Drinfeld module ϕ by definition.

Lemma 9.3. *Assume that $q = 2$. If the reduction of the point $P \in Y_0(\mathfrak{p})(F_\infty)$ lies on the irreducible component $\tilde{w}$ then $j(P) \in \mathcal{O}_\infty$.*

Proof. Let Q be the image of P with respect to the map $Y_0(\mathfrak{p}) \rightarrow Y_0(1)$ corresponding to forgetting the level structure. By definition $j(P)$ is just the image of Q under the isomorphism $Y_0(1) \cong \mathbb{A}^1$ induced by the j -invariant. According to Theorem 7.2 the rigid-analytic space underlying $Y_0(1)$ is isomorphic to the generic fiber of the formal scheme $GL_2(A) \backslash \widehat{\Omega}$. The incidence graph of the special fiber of $GL_2(A) \backslash \widehat{\Omega}$ is canonically isomorphic to the quotient graph $GL_2(A) \backslash \mathcal{T}$. Because the vertex w of $\mathcal{T}$ is equivalent to v_0 modulo the action of $GL_2(A)$ the reduction of Q lies on the irreducible component of the special fiber of $GL_2(A) \backslash \widehat{\Omega}$ which is the image of v_0 under the quotient map $\mathcal{T} \rightarrow GL_2(A) \backslash \mathcal{T}$. Hence by Corollary 1.9 of [6] on page 186 there is a $z \in V$ whose image with respect to the uniformization in Theorem 7.2 is the point Q where V denotes the rational subdomain whose underlying set of points is:

$$V = \{z \in \mathbb{C}_\infty \mid |z - c| = 1 \ (\forall c \in \mathbf{f}_\infty)\} \subset \Omega.$$

Hence it will be sufficient to show that $|j(z)| \leq 1$ for every $z \in V$ where j is the Drinfeld modular function $j : \Omega \rightarrow \mathbb{C}_\infty$. Let $z_0 \in V$ be an element of $\mathbb{F}_4 - \mathbb{F}_2$. Then $A + Az_0 = \mathbb{F}_4[T]$ is a rank two discrete A -lattice which corresponds to a Drinfeld module $\psi : A \rightarrow \mathbb{C}_\infty\{\tau\}$ of rank two by the uniformization theory of Drinfeld modules. As explained in the proof of Theorem 2.13 of [6] on page 192 the j -invariant of ψ is zero. Hence $\psi(T) = \bar{\pi}\tau^2 + T$ for some $\bar{\pi} \in \mathbb{C}_\infty^*$. The modular unit $\epsilon_{(T)}(\alpha, \beta)(z_0)$ is a root of the additive polynomial $\bar{\pi}x^4 + Tx$ corresponding to $\psi(T)$ for every $(\alpha, \beta) \in (A/(T))^2$. Therefore $|\epsilon_{(T)}(\alpha, \beta)(z_0)| = |T/\bar{\pi}|^{1/3}$ for every non-zero (α, β) as above. The reduction of the affinoid V is irreducible hence every nowhere zero holomorphic function on V has constant absolute value. In particular $|\epsilon_{(T)}(\alpha, \beta)(z)| = |T/\bar{\pi}|^{1/3}$ for every $z \in V$ and for every non-zero (α, β) as above. We get that $|\Delta(z)| = |T/\bar{\pi}|$ and $|g(z)^3| \leq |T/\bar{\pi}|$ for every $z \in V$ using the ultrametric inequality. The claim is now clear. $\square$

Proposition 9.4. *For every place v of F the reduction map $W(\mathfrak{p})(F) \rightarrow W(\mathfrak{p})(\mathbf{f}_v)$ is injective.*

Proof. By Lemma 3.4 the order of the finite group $W(\mathfrak{p})(F)$ is not divisible by p . Hence the claim is obvious for every place v where $W(\mathfrak{p})$ has good reduction. Because $W(\mathfrak{p})$ is a quotient of $J_0(\mathfrak{p})$ this holds for every place v different from $\mathfrak{p}$ and ∞ . At the places $\mathfrak{p}$ and ∞ the Jacobian $J_0(\mathfrak{p})$ has multiplicative reduction, that is, the connected component of the identity in the fiber of its Néron model over these closed points is a torus. Therefore $W(\mathfrak{p})$ also has multiplicative reduction at these places. The claim now follows from part (i) of Lemma 7.13 of [17] on page 162 in these cases. $\square$

Notation 9.5. By Proposition 9.3 of [2] on pages 586-587 we know that for every non-zero ideal $\mathfrak{n} \triangleleft A$ the projective curve $X_0(\mathfrak{n})$ has a smooth, projective model $\overline{M}_0(\mathfrak{n})$ over $U_{\mathfrak{n}}$ where $U_{\mathfrak{n}}$ is the complement of the support of the ideal $\mathfrak{n}$ in $\text{Spec}(A)$. In the paper quoted above it is also proved that the Zariski closure of the cusps in $\overline{M}_0(\mathfrak{n})$ is a finite, étale scheme over $U_{\mathfrak{n}}$. When $\mathfrak{n} = \mathfrak{p}$ is a prime ideal Gekeler constructed a model of $X_0(\mathfrak{p})$ over $\text{Spec}(A)$ which contains $\overline{M}_0(\mathfrak{p})$ as an open subscheme. We are going to denote the latter by $\overline{M}_0(\mathfrak{p})$ as well by slight abuse of notation. For the relevant properties of this scheme see 5.1-5.8 of [5], pages 229-233.

Proof of Theorem 1.2. We are going to use again the notation which we used in chapter 7. Let $w_{\mathfrak{p}}$ denote again the matrix which was introduced in the proof of Lemma 6.6. As we already mentioned the latter normalizes the group Γ hence its Möbius action on Ω descends to the quotient $\Gamma \backslash \Omega$. Under the identification of Theorem 7.2 the corresponding automorphism of $Y_0(\mathfrak{p})$ is the Atkin-Lehner involution. Because Γ_{tor} is a characteristic subgroup of Γ the matrix $w_{\mathfrak{p}}$ normalizes this subgroup of $GL_2(F_{\infty})$, too. Hence its Möbius action on Ω descends to the quotient $\Gamma_{\text{tor}} \backslash \Omega$ as well. This action extends to Σ uniquely and leaves the cover $\mathcal{V}$ invariant. The corresponding automorphism of the formal scheme $\widehat{\Sigma}$ commutes with the action of Γ' hence we get an involutive automorphism of the $\text{Spec}(\mathcal{O}_{\infty})$ -scheme $\mathfrak{X}_0(\mathfrak{p})$ by formal GAGA. We will call the latter the Atkin-Lehner involution of the scheme $\mathfrak{X}_0(\mathfrak{p})$ and will denote it by $W_{\mathfrak{p}}$ by the usual abuse of notation. This is justified as its action of the generic fiber of $\mathfrak{X}_0(\mathfrak{p})$ is the usual Atkin-Lehner involution by the above. Moreover the action on the incidence graph $\mathcal{G}(\mathfrak{p})$ of the special fiber of $\mathfrak{X}_0(\mathfrak{p})$ induced by $W_{\mathfrak{p}}$ is the Atkin-Lehner involution which we introduced in the proof of Lemma 6.6.

Let P be an F -rational point of $X_0(\mathfrak{p})$. By Proposition 7.12 the model $\mathfrak{X}_0(\mathfrak{p})$ is regular hence the reduction of P lies in $\mathfrak{X}_0^*(\mathfrak{p})(\mathbf{f}_{\infty})$. The ordinary double points of the special fiber of $\mathfrak{X}_0(\mathfrak{p})$ are $\mathbf{f}_{\infty}$ -rational. Hence if v is an irreducible component of the special fiber of $\mathfrak{X}_0(\mathfrak{p})$ whose degree, considered as a vertex of the incidence graph, is three, then every $\mathbf{f}_{\infty}$ -rational point of v is an ordinary double point. Therefore the reduction of P must lie on the irreducible component $\tilde{u}_{-1}$, or its image with respect to the Atkin-Lehner involution, or the irreducible component $\tilde{w}$ by Propositions 6.11 and 6.13. The first two irreducible components both have degree two as a vertex of $\mathcal{G}(\mathfrak{p})$, hence they have only one $\mathbf{f}_{\infty}$ -rational point which is not an ordinary double point. These must be the reductions of the cusps 0 and ∞ , respectively. Therefore the reduction of P is either equal to the reduction of one of the cusps or $\deg(\mathfrak{p})$ is even and the reduction of P lies on the irreducible

component $\tilde{w}$.

Assume first that the reduction of P in $\mathfrak{X}_0^*(\mathfrak{p})(\mathbf{f}_\infty)$ is the same as the reduction of some cusp. By applying the Atkin-Lehner involution to P , if necessary, we may assume that this cusp is 0. In this case the image of the divisor class $P - 0$ in $W(\mathfrak{p})(F)$ with respect to the quotient map is equal to the image of the trivial divisor class in $W(\mathfrak{p})(F)$ by Proposition 9.4. Therefore we must have $P = 0$ by the formal immersion property (Proposition 7.14). Hence we may assume that $\deg(\mathfrak{p})$ is even and the reduction of P lies on the irreducible component $\tilde{w}$. By Lemma 9.3 above we know that $j(P) \in \mathcal{O}_\infty$.

We are going to show that $j(P) \in \mathcal{O}_v$ for every other place v of F . Assume that the claim is false. Because the model $\overline{M}_0(\mathfrak{p})$ is projective over $\text{Spec}(A)$ every F -valued point on $X_0(\mathfrak{p})$ has a unique extension to a section $\text{Spec}(A) \rightarrow \overline{M}_0(\mathfrak{p})$. By assumption the section extending P must intersect the section extending one of the cusps in the fiber of $\overline{M}_0(\mathfrak{p})$ at v . We may assume that P intersects the section extending ∞ as the other case can be treated exactly the same way. Then the image of the linear equivalence class of the divisor $P - \infty$ with respect to the reduction map $J_0(\mathfrak{p})(F) \rightarrow \mathcal{J}_0(\mathfrak{p})(\mathbf{f}_v)$ is zero. For every F -rational divisor D of degree zero on $X_0(\mathfrak{p})$ let $[D]$ denote the image of the linear equivalence class of D with respect to the quotient map $J_0(\mathfrak{p}) \rightarrow W(\mathfrak{p})$. By the universal property of the Néron model we get that the image of $[P - \infty]$ with respect to the reduction map $W(\mathfrak{p})(F) \rightarrow \mathcal{W}(\mathfrak{p})(\mathbf{f}_v)$ is zero. Hence $[P - \infty]$ is zero in $W(\mathfrak{p})(F)$ by Proposition 9.4. By claim (iii) of Proposition 6.11 the reduction of $W_{\mathfrak{p}}(P)$ lies on the same irreducible component as the reduction of P . Since this irreducible component is a rational curve which has only one ordinary double point the difference of these reductions is linearly equivalent to zero on the special fiber of $\mathfrak{X}_0(\mathfrak{p})$. Hence the image of the linear equivalence class of the divisor $P - W_{\mathfrak{p}}(P)$ with respect to the reduction map $J_0(\mathfrak{p})(F) \rightarrow \mathcal{J}_0(\mathfrak{p})(\mathbf{f}_\infty)$ is zero. Using the same argument as above we get from this fact that $[P - W_{\mathfrak{p}}(P)]$ is zero in $W(\mathfrak{p})(F)$ by Proposition 9.4. Therefore we may compute as follows:

$$\begin{aligned} 0 = W_{\mathfrak{p}}[P - \infty] &= [W_{\mathfrak{p}}(P) - W_{\mathfrak{p}}(\infty)] = [W_{\mathfrak{p}}(P) - P] + [P - W_{\mathfrak{p}}(\infty)] \\ &= [P - 0] = [P - \infty] + [\infty - 0] = [\infty - 0] \end{aligned}$$

where $W_{\mathfrak{p}}$ denotes the endomorphism of $W(\mathfrak{p})$ induced by the Atkin-Lehner involution, too. The linear equivalence class of the divisor $\infty - 0$ generates the group $\mathcal{C}(\mathfrak{p})$ hence the image of the latter with respect to the map $J_0(\mathfrak{p}) \rightarrow W(\mathfrak{p})$ is zero. This is a contradiction by claim (ii) of Proposition 5.12. We conclude that $j(P) \in \mathcal{O}_v$ for every place v of F . This is only possible if $j(P) \in \mathbb{F}_2$. By Proposition 8.12 we may assume that $j(P) = 1$. Every Drinfeld module ϕ of rank two over F with j -invariant $j(\phi) = 1$ is isomorphic to the Drinfeld module $\psi : A \rightarrow F\{\tau\}$ such that $\psi(T) = T + \tau + \tau^2$ over F because the latter has no non-trivial automorphisms over $\overline{F}$. The Drinfeld module ψ has good reduction at every place $v \neq \infty$ of F . This is not possible by Theorem 8.10. $\square$

Proof of Corollary 1.7. The scheme $X_0(\mathfrak{p})$ is smooth over $\text{Spec}(F)$. Hence the scheme $\mathbf{Isom}_{\text{Spec}(F)}(X_0(\mathfrak{p}), X_0(\mathfrak{p}))$ representing the functor associating to each $\text{Spec}(F)$ -scheme S the set of S -automorphisms of the scheme $X_0(\mathfrak{p}) \times_{\text{Spec}(F)} S$ is finite and unramified over $\text{Spec}(F)$ by Theorem 1.11 of [1] on pages 84-85. Therefore every automorphism u of $X_0(\mathfrak{p})$ is actually defined over the separable closure of F .

Let $\text{Aut}(J_0(\mathfrak{p})_{\overline{F}})$ denote the group of automorphism of the group scheme $J_0(\mathfrak{p})$ over $\overline{F}$. The homomorphism from $\text{Aut}(X_0(\mathfrak{p}))$ into $\text{Aut}(J_0(\mathfrak{p})_{\overline{F}})$ induced by Picard functoriality is injective. Moreover this map is also $\text{Gal}(\overline{F}|F)$ -invariant. Hence every automorphism u of $X_0(\mathfrak{p})$ is actually defined over F by claim (i) of Lemma 5.6. Therefore the image of the cusps of $X_0(\mathfrak{p})$ under u are F -rational points. By Theorem 1.2 the set $X_0(\mathfrak{p})(F)$ consists of the cusps hence every automorphism of $X_0(\mathfrak{p})$ fixes the two cusps or interchanges them. The Atkin-Lehner involution is an automorphism which interchanges the cusps. Therefore it will be sufficient to prove that every involution u of the curve $X_0(\mathfrak{p})$ fixing the cusps is the identity by claim (iii) of Lemma 5.6. Let f be a non-zero rational function on $X_0(\mathfrak{p})$ whose divisor is $N(\mathfrak{p})(\infty - 0)$. Because the automorphism u fixes the points 0 and ∞ the pull-back $u^*(f)$ of f with respect to u is also a non-zero rational function on $X_0(\mathfrak{p})$ whose divisor is $N(\mathfrak{p})(\infty - 0)$. Such a function is unique up to a non-zero scalar, so $u^*(f) = \alpha f$ for some $\alpha \in F^*$. But u is an involution so $f = u^*(u^*(f)) = \alpha^2 f$ hence $\alpha^2 = 1$. The field F has characteristic 2 so the equation $\alpha = 1$ must hold. Hence the rational function f is left invariant by the involution u . Assume now that u is not the identity. Let $X_0(\mathfrak{p})^u$ be the quotient of $X_0(\mathfrak{p})$ by u and let $\pi : X_0(\mathfrak{p}) \rightarrow X_0(\mathfrak{p})^u$ denote the quotient map. By the above there is map $g : X_0(\mathfrak{p})^u \rightarrow \mathbb{P}^1$ such that $f = g \circ \pi$. The degree of f is $N(\mathfrak{p})$ which is an odd number. On the other hand the degree of π is two. This is a contradiction. $\square$

Actually our argument works for every field $\mathbb{F}_q(T)$ of characteristic 2 under the condition that $Y_0(\mathfrak{p})$ has no $\mathbb{F}_q(T)$ -rational points.

Remark 9.6. Let B denote again the group scheme of invertible upper triangular two by two matrices. Let $h : \Gamma_0(\mathfrak{p}) \rightarrow \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$ denote the composition of the reduction map $r : \Gamma_0(\mathfrak{p}) \rightarrow B(\mathbf{A}/\mathfrak{p}) \subset GL_2(\mathbf{A}/\mathfrak{p}) \bmod \mathfrak{p}$, the upper left conner element $a : B(\mathbf{A}/\mathfrak{p}) \rightarrow (\mathbf{A}/\mathfrak{p})^*$ and the surjection $s : (\mathbf{A}/\mathfrak{p})^* \rightarrow \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$ which is unique up to isomorphism. We used that this homomorphism factors through $\overline{\Gamma}_0(\mathfrak{p})$ at a crucial point both in [17] and [18], but did not give a proof of this not entirely obvious fact. This small gap is easy to fill with some of the methods of this paper. Because $\overline{\Gamma}_0(\mathfrak{p}) = (\Gamma_0(\mathfrak{p})_{tors})^{ab}$ it will be sufficient to show that h is trivial restricted to every finite subgroup G of $\Gamma_0(\mathfrak{p})$. As we saw in the proof of Lemma 8.8 the action of G on the Bruhat-Tits tree has a fixed vertex. Hence by the results of [7] it will be conjugate to a subgroup of $B(A)$ or to a subgroup of $GL_2(\mathbb{F}_q)$, where the second case occurs only when $\deg(\mathfrak{p})$ is even. In any case every element g of G has order dividing $q^k(q-1)$ for some $k \in \mathbb{N}$, if $\deg(\mathfrak{p})$ is odd, and has order dividing $q^k(q^2-1)$ for some $k \in \mathbb{N}$, otherwise. Hence $a(r(g))$ is mapped to the identity by s .

10. THE PROOF OF THEOREM 1.4

In the next claim and its proof we are not going to assume that $q = 2$.

Proposition 10.1. *Assume that the following holds:*

- (i) *The curve $Y_1(\mathfrak{n})$ has no F -rational points if $\deg(\mathfrak{n}) \geq 3$,*
- (ii) *The curves $Y_0(T^3)$ and $Y_0(T^2(T+1))$ have no rational points.*

Then the claim of Theorem 1.5 holds for q .

The proposition above is just a slight variation of Schweizer's Lemma 4.5 of [26] on page 613.

Proof. Let $\phi : A \rightarrow F\{\tau\}$ be a Drinfeld module of rank two over F and write $(\phi F)_{tors} = A/\mathfrak{m} \oplus A/\mathfrak{n}$ where $\mathfrak{m}$ divides $\mathfrak{n}$. By assumption the latter can be written as $\mathfrak{n} = \mathfrak{m}\mathfrak{p}$ for some non-zero ideal $\mathfrak{p} \triangleleft A$. Assume that ϕ is a counterexample to the claim of Theorem 1.2. By claim (i) above the degree of the ideal $\mathfrak{n}$ is at most two. Hence $\deg(\mathfrak{m})$ is at least 1. On the other hand we have $\deg(\mathfrak{m}) \leq 1$ by Proposition 4.4 of [26] on page 613. Let $v : \phi \rightarrow \psi$ be the cyclic $\mathfrak{m}$ -isogeny whose kernel is the first component of the direct sum above. According to Lemma 4.1 of [26] on page 611, the Drinfeld module ψ over F has a cyclic $\mathfrak{m}\mathfrak{n}$ -isogeny defined over F . This Drinfeld module and isogeny give rise to an F -rational point on the Drinfeld modular curve $Y_0(\mathfrak{p}\mathfrak{m}^2)$. If the ideals $\mathfrak{p}$ and $\mathfrak{m}$ are different, then there is an automorphism of A which takes $\mathfrak{p}$ and $\mathfrak{m}$ to $(T+1)$ and (T) , respectively. On the other hand if ideals $\mathfrak{p}$ and $\mathfrak{m}$ are equal, then there is an automorphism of A which takes $\mathfrak{p} = \mathfrak{m}$ to (T) . The pull-back of $Y_0(\mathfrak{p}\mathfrak{m}^2)$ with respect to these automorphisms is either $Y_0(T^2(T+1))$ or $Y_0(T^3)$, respectively. But these curves have no rational points by claim (ii) above which is a contradiction. $\square$

Remark 10.2. In the course of the proof of Theorem 1.5 we may restrict to those $\mathfrak{n}$ ideals which has no proper divisors of degree at least three while we verify the validity of condition (i) of Proposition 10.1. In particular we may assume that either $\mathfrak{n}$ is a prime ideal of degree at least three or it is the product of irreducible polynomials of degree at most two. When $q = 2$ the only irreducible polynomials of degree 1 and 2 in $\mathbb{F}_q[T]$ are T , $T+1$ and T^2+T+1 . Moreover there is an automorphism of $\mathbb{F}_2[T]$ which maps T to $T+1$. Therefore by Theorem 1.2 and the claim above in order to prove Theorem 1.5 we have to show that the following curves have no rational points:

$$Y_0(T(T^2+T+1)), Y_0(T^3), Y_0(T^2(T+1)), Y_1(T^4+T^2+1)$$

taking into account that if the curve $Y_0(\mathfrak{n})$ has no rational points then so does $Y_1(\mathfrak{n})$. The first three cases were settled by Schweizer (Lemma 1.3 of [26] on pages 605-606).

Notation 10.3. In the rest of this section we will occupy ourselves with proving that the curve $Y_1(T^4+T^2+1)$ has no rational points. First we will collect some facts about the geometry of the curve $X_0(T^4+T^2+1)$. Let $W_{\mathfrak{n}}$ denote the full Atkin-Lehner involution of the modular curve $Y_0(\mathfrak{n})$ for every non-zero ideal $\mathfrak{n} \triangleleft A$. This map induces an involution of the curve $X_0(\mathfrak{n})$ which will be denoted by the same symbol. The index $\mathfrak{n}$ will be dropped from the notation $W_{\mathfrak{n}}$ when the ideal $\mathfrak{n}$ can be clearly identified from the context. Let $X_+(\mathfrak{n})$ denote the quotient of the curve $X_0(\mathfrak{n})$ by the involution W . Recall that the set of geometric points of $X_0(\mathfrak{n})$ in the complement of $Y_0(\mathfrak{n})$ are called its cusps.

Lemma 10.4. *The following holds:*

- (i) *the curve $X_0(T^4+T^2+1)$ has genus 2,*
- (ii) *the quotient map $X_0(T^4+T^2+1) \rightarrow X_+(T^4+T^2+1)$ is a hyperelliptic cover which has three ramification points,*
- (iii) *the latter are cusps conjugate over F .*

Proof. Claim (i) is a consequence of the formula on page 331 for the genus of Drinfeld modular curves in [25]. By formula b) of Proposition 7 on page 336 of the same paper the number of fixed points of the Atkin-Lehner involution is at most

3. Now claims (ii) and (iii) follow from the content of Example 10 of [25] on page 337 and from part (b) of Proposition 1 of the same reference on page 333. $\square$

Lemma 10.5. *The fiber of the model $\overline{M}_0(T^4 + T^2 + 1)$ over every prime ideal $\mathfrak{q} \neq (T^2 + T + 1)$ of A is an ordinary curve.*

Proof. Let $X_{\mathfrak{q}}$ denote simply the fiber of $\overline{M}_0(T^4 + T^2 + 1)$ at the prime ideal $\mathfrak{q} \neq (T^2 + T + 1)$. We know that $X_{\mathfrak{q}}$ is a smooth, projective curve over $\mathbf{f}_{\mathfrak{q}}$ whose genus is 2 by flatness. Because $\overline{M}_0(T^4 + T^2 + 1)$ is a relatively minimal model for $X_0(T^4 + T^2 + 1)$ over U_{T^2+T+1} the Atkin-Lehner involution W extends to an involution on $\overline{M}_0(T^4 + T^2 + 1)$ whose restriction to $X_{\mathfrak{q}}$ is a hyperelliptic involution. The former fixes the closure Z of the zero-dimensional subvariety of $X_0(T^4 + T^2 + 1)$ supported on the three cusps left invariant by the Atkin-Lehner involution in $\overline{M}_0(T^4 + T^2 + 1)$. As we already noted in Notation 9.5 the scheme Z is finite, étale over U_{T^2+T+1} hence the canonical hyperelliptic involution of $X_{\mathfrak{q}}$ has at least three different fixed points. Hence it will be sufficient to show that every smooth, projective curve X of genus 2 defined over a characteristic two field $\mathbf{k}$ such that the canonical hyperelliptic cover $\pi : X \rightarrow \mathbb{P}_{\mathbf{k}}^1$ has three ramification points is ordinary. We may assume without the loss of generality that $\mathbf{k}$ is algebraically closed. Let A , B and C denote the ramification points. Then the linear equivalence classes of the divisors $2B - 2A$ and $2C - 2A$ are trivial as they are the pull-backs of the divisors $\pi(B) - \pi(A)$ and $\pi(C) - \pi(A)$ with respect to π , respectively. Hence the linear equivalence classes of $B - A$ and $C - A$ are 2-torsion. If they generated the same group then they would be equal, so B would be equal to C . Hence the group generated by the linear equivalence classes of $B - A$ and $C - A$ has order four. Therefore the 2-torsion of the Jacobian of X has order four so it is an ordinary abelian variety. $\square$

Proposition 10.6. *The following holds:*

- (i) *the Mordell-Weil group $J_0(T^4 + T^2 + 1)(F)$ of the Jacobian of the Drinfeld modular curve $X_0(T^4 + T^2 + 1)$ is finite,*
- (ii) *for every prime ideal $\mathfrak{q} \neq (T^2 + T + 1)$ of A the reduction map modulo $\mathfrak{q}$ on $X_0(T^4 + T^2 + 1)(F)$ is injective.*

Proof. By the main theorem of [24] on page 509 it is enough to show that the Grothendieck L -function of the abelian variety $J_0(T^4 + T^2 + 1)$ does not vanish at q^{-1} in order to prove the first claim. We are going to use the notation which we introduced at the beginning of the proof of Proposition 3.8. Fix a prime l different from 2 and let ρ be an irreducible component of the l -adic representation $H^1(J_0(T^4 + T^2 + 1)_{\overline{F}}, \mathbb{Q}_l)$ of the absolute Galois group of F . The curves $X_0(1)$ and $X_0(T^2 + T + 1)$ have genus zero hence we get that the degree of the conductor of ρ is 5 by repeating the argument in the proof which have just mentioned above. Therefore the degree of the Grothendieck L -function $L(\rho, t)$ as a polynomial in t is one. In particular the multiplicity of the zero at q^{-1} is at most one. The Atkin-Lehner operator acts on the Jacobian of $X_0(\mathfrak{n})$ by Picard functoriality which induces an action on the cohomology group $H^1(J_0(\mathfrak{n})_{\overline{F}}, \mathbb{Q}_l)$. This action commutes with the action of the absolute Galois group of F and its restriction to every irreducible component ρ is multiplication by ± 1 . Moreover by the analogue of the classical Atkin-Lehner theory for Drinfeld modular curves (see Remark 10.7 below) the sign of the functional equation of $L(\rho, t)$ is the opposite of the sign of this multiplication.

The $+1$ -eigenspace of the action of the Atkin-Lehner operator on $H^1(J_0(T^4 + T^2 + 1)_{\overline{F}}, \overline{\mathbb{Q}}_l)$ is isomorphic to $H^1(X_+(T^4 + T^2 + 1)_{\overline{F}}, \overline{\mathbb{Q}}_l)$ which is zero by claim (ii) of Lemma 10.4. Hence the sign of the functional equation of $L(\rho, t)$ is $+1$ so the order of vanishing at q^{-1} is even. Claim (i) is now clear.

Because the curve $X_0(\mathfrak{n})$ has a smooth, projective model over U_{T^2+T+1} the Néron model of the Jacobian $J_0(T^4 + T^2 + 1)$ is an abelian scheme $\mathcal{J}$ over U_{T^2+T+1} . It will be sufficient to prove that for every prime ideal $\mathfrak{q} \neq (T^2 + T + 1)$ of A the reduction map modulo $\mathfrak{q}$ on the Mordell-Weil group $J_0(T^4 + T^2 + 1)(F)$ is injective in order to show claim (ii). The reduction map is injective restricted to the prime-to-two torsion of $J_0(T^4 + T^2 + 1)(F)$. Hence by claim (i) we only need to show that it is injective restricted to the 2-torsion as well. Let $\tilde{F}_{\mathfrak{q}}$ denote the maximal unramified extension of $F_{\mathfrak{q}}$ and let $\tilde{\mathcal{O}}_{\mathfrak{q}}, \mathbf{k}_{\mathfrak{q}}$ denote the valuation ring and the residue field of the local field $\tilde{F}_{\mathfrak{q}}$, respectively. The base change $\mathcal{J}_{\mathfrak{q}}$ of $\mathcal{J}$ to the geometric point $\text{Spec}(\mathbf{k}_{\mathfrak{q}}) \rightarrow U_{T^2+T+1}$ is ordinary by Lemma 10.5, hence its formal group is multiplicative by Lazard's theorem. The latter has no non-trivial deformations, so the formal group of the base change of $\mathcal{J}$ to the spectrum of the local ring $\tilde{\mathcal{O}}_{\mathfrak{q}}$ is also multiplicative. The group of $\tilde{F}_{\mathfrak{q}}$ -valued points of $\mathcal{J}$ which map to the identity of $\mathcal{J}_{\mathfrak{q}}$ with respect to the reduction map into the special fiber is isomorphic to the multiplicative group of those elements of $\tilde{\mathcal{O}}_{\mathfrak{q}}$ which are congruent to 1 modulo the maximal ideal of $\tilde{\mathcal{O}}_{\mathfrak{q}}$. Hence the former has no 2-torsion, so the reduction map is even injective restricted to $J_0(T^4 + T^2 + 1)(\tilde{F}_{\mathfrak{q}})[2]$. $\square$

Remark 10.7. In this paragraph we briefly indicate why the analogue of the classical Atkin-Lehner theory is true for Drinfeld modular curves (or alternatively the reader may consult the proof of Proposition 3.14 of [29] on pages 225-226). By 8.3.8 of [8] on page 81 there is an Eichler-Shimura isomorphism:

$$i_{ES} : H^1(J_0(\mathfrak{n})_{\overline{F}}, \overline{\mathbb{Q}}_l) \rightarrow H_!(\mathcal{T}, \overline{\mathbb{Q}}_l)^{\Gamma_0(\mathfrak{n})} \otimes_{\overline{\mathbb{Q}}_l} \overline{\mathbb{Q}}_l^2,$$

where $H_!(\mathcal{T}, \overline{\mathbb{Q}}_l)^{\Gamma_0(\mathfrak{n})}$ is the space of $\overline{\mathbb{Q}}_l$ -valued cuspidal cochains on the Bruhat-Tits tree $\mathcal{T}$ invariant with respect to the Hecke congruence group $\Gamma_0(\mathfrak{n})$. The Eichler-Shimura isomorphism i_{ES} is equivariant to the usual action of the Hecke algebra on these two vector spaces over $\overline{\mathbb{Q}}_l$. Moreover the map i_{ES} is equivariant with respect to the action of the Atkin-Lehner involution in the sense that under this isomorphism the operator induced by W on the cohomology group $H^1(J_0(\mathfrak{n})_{\overline{F}}, \overline{\mathbb{Q}}_l)$ corresponds to the tensor product of the identity of $\overline{\mathbb{Q}}_l^2$ and the operator on $H_!(\mathcal{T}, \overline{\mathbb{Q}}_l)^{\Gamma_0(\mathfrak{n})}$ corresponding to the product of the full Atkin-Lehner operator and the local Atkin-Lehner operator at ∞ for automorphic forms of conductor $\mathfrak{n}\infty$ where we write the product of divisors multiplicatively. Since the latter acts as multiplication by -1 on the elements of $H_!(\mathcal{T}, \overline{\mathbb{Q}}_l)^{\Gamma_0(\mathfrak{n})}$ the claim is clear.

Theorem 10.8. *The Drinfeld modular curve $Y_1(T^4 + T^2 + 1)$ has no F -rational points.*

Proof. Assume that the claim is false, and let $P \in Y_1(T^4 + T^2 + 1)(F)$ be an F -rational point. The point P maps to an F -rational point Q on $Y_0(T^4 + T^2 + 1)$ with respect to the map $Y_1(T^4 + T^2 + 1) \rightarrow Y_0(T^4 + T^2 + 1)$ of these coarse moduli induced by the forgetful functor. By claim (ii) of Proposition 10.6 the reduction of Q modulo T is different from the cusps. On the other hand the latter is not possible by Lemma 8.11. $\square$

REFERENCES

1. P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.
2. V. G. Drinfeld, *Elliptic modules*, [translation], Mat. Sbornik **23** (1974), 561–592.
3. E.-U. Gekeler, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. **262** (1983), 167–182.
4. E.-U. Gekeler, *Drinfeld modular curves*, L.N.M. 1231, Springer, Berlin-Heidelberg-New York, 1986.
5. E.-U. Gekeler, *Über Drinfeld'sche Modulcurven vom Hecke-Typ*, Comp. Math. **57** (1986), 219–236.
6. E.-U. Gekeler, *On the Drinfeld discriminant function*, Comp. Math. **106** (1997), 181–202.
7. E.-U. Gekeler and U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, Int. J. Math. **6** (1995), 689–708.
8. E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. reine angew. Math. **476** (1996), 27–93.
9. L. Gerritzen, *Über Endomorphismen nichtarchimedischer holomorpher Tori*, Invent. Math. **11** (1970), 27–36.
10. L. Gerritzen, *On non-archimedean representations of abelian varieties*, Math. Ann. **196** (1972), 323–346.
11. L. Gerritzen and M. van der Put, *Schottky groups and Mumford curves*, Lect. Notes Math. 817, Springer-Verlag, Berlin-Heidelberg-New York, 1980.
12. D. Goss, *Basic structures of function field arithmetic*, Springer-Verlag, Berlin-Heidelberg-New York, 1996.
13. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.
14. B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
15. L. Merel, *Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques*, Duke Math. J. **110** (2001), 81–119.
16. A. Ogg, *Automorphismes de courbes modulaires*, Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 7, 8 pp., Secrétariat Mathématique, Paris, 1975.
17. A. Pál, *On the torsion of the Mordell-Weil group of the Jacobian of Drinfeld modular curves*, Documenta Math **10** (2005), 131–198.
18. A. Pál, *On the Eisenstein ideal of Drinfeld modular curves*, International Journal of Number Theory **3** (2007), 557–598.
19. M. Papikian, *On component groups of Jacobians of Drinfeld modular curves*, Ann. Inst. Fourier (Grenoble) **54** (2004), 2163–2199.
20. M. Papikian, *On the torsion of optimal elliptic curves over function fields*, Math. Research Letters **13** (2006), 321–331.
21. B. Poonen, *Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture*, Math. Annalen **308** (1997), 571–586.
22. P. Parent, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$* , Compositio Math. **141** (2005), 561–572.
23. M. Reversat, *Sur les revêtements de Schottky des courbes modulaires de Drinfeld*, Arch. Math. **66** (1996), 378–387.
24. P. Schneider, *Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionen-körpern*, Math. Ann. **260** (1982), 495–510.
25. A. Schweizer, *Hyperelliptic Drinfeld modular curves*, Drinfeld modules, modular schemes and applications, World Scientific, Singapore-London-Hong Kong, 1997, pp. 330–343.
26. A. Schweizer, *On the uniform boundedness conjecture for Drinfeld modules*, Math. Z. **244** (2003), 601–614.
27. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
28. J.-P. Serre, *Trees*, Springer, Berlin-Heidelberg-New York, 1980.
29. A. Tamagawa, *The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve*, Publ. Res. Inst. Math. Sci. **31** (1995), 203–246.
30. A. Tamagawa, *Ramification of torsion points on curves with ordinary semistable Jacobian varieties*, Duke Math. **106** (2001), 281–319.

- 31. K.-S. Tan and D. Rockmore, *Computation of L -series for elliptic curves over function fields*, J. reine angew. Math. **424** (1992), 107-136.
- 32. J. Teitelbaum, *Modular symbols for $\mathbb{F}_q(T)$* , Duke Math. **68** (1992), 271-295.
- 33. A. Weil, *Dirichlet series and automorphic forms*, Springer, Berlin-Heidelberg-New York, 1971.

DEPARTMENT OF MATHEMATICS, 180 QUEEN'S GATE, IMPERIAL COLLEGE, LONDON SW7 2AZ, UNITED KINGDOM

E-mail address: `a.pal@imperial.ac.uk`