On the Torsion of the Mordell-Weil Group of the Jacobian of Drinfeld Modular Curves

Ambrus Pál

Received: September 27, 2004
Revised: February 2, 2005

Communicated by Peter Schneider

Abstract. Let $Y_0(\mathfrak{p})$ be the Drinfeld modular curve parameterizing Drinfeld modules of rank two over $\mathbb{F}_q[T]$ of general characteristic with Hecke level $\mathfrak{p}$-structure, where $\mathfrak{p} \triangleleft \mathbb{F}_q[T]$ is a prime ideal of degree d. Let $J_0(\mathfrak{p})$ denote the Jacobian of the unique smooth irreducible projective curve containing $Y_0(\mathfrak{p})$. Define $N(\mathfrak{p}) = \frac{q^d-1}{q-1}$, if d is odd, and define $N(\mathfrak{p}) = \frac{q^d-1}{q^2-1}$, otherwise. We prove that the torsion subgroup of the group of $\mathbb{F}_q(T)$-valued points of the abelian variety $J_0(\mathfrak{p})$ is the cuspidal divisor group and has order $N(\mathfrak{p})$. Similarly the maximal μ-type finite étale subgroup-scheme of the abelian variety $J_0(\mathfrak{p})$ is the Shimura group scheme and has order $N(\mathfrak{p})$. We reach our results through a study of the Eisenstein ideal $\mathfrak{E}(\mathfrak{p})$ of the Hecke algebra $\mathbb{T}(\mathfrak{p})$ of the curve $Y_0(\mathfrak{p})$. Along the way we prove that the completion of the Hecke algebra $\mathbb{T}(\mathfrak{p})$ at any maximal ideal in the support of $\mathfrak{E}(\mathfrak{p})$ is Gorenstein.

2000 Mathematics Subject Classification: Primary 11G18; Secondary 11G09.
Keywords and Phrases: Drinfeld modular curves, Eisenstein ideal.

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 $A = \mathbb{F}_q[T]$. For any non-zero ideal $\mathfrak{n}$ of A a geometrically irreducible affine algebraic curve $Y_0(\mathfrak{n})$ is defined over F, the Drinfeld modular curve parameterizing Drinfeld modules of rank two over A of general characteristic with Hecke level $\mathfrak{n}$-structure. There is a unique non-singular projective curve $X_0(\mathfrak{n})$ over F which contains $Y_0(\mathfrak{n})$ as an open subvariety. Let $J_0(\mathfrak{n})$ denote the Jacobian of the curve $X_0(\mathfrak{n})$. Let $\mathfrak{p}$ be a prime ideal of A and let d denote the degree of the residue field of $\mathfrak{p}$ over $\mathbb{F}_q$. Define $N(\mathfrak{p}) = \frac{q^d-1}{q-1}$, if d is odd, and define $N(\mathfrak{p}) = \frac{q^d-1}{q^2-1}$, otherwise.

Theorem 1.2. *The torsion subgroup $\mathcal{T}(\mathfrak{p})$ of the group of F-valued points of the abelian variety $J_0(\mathfrak{p})$ is a cyclic group of order $N(\mathfrak{p})$.*

It is possible to explicitly determine the group in the theorem above.

Definition 1.3. The geometric points of the zero dimensional complement of $Y_0(\mathfrak{n})$ in $X_0(\mathfrak{n})$ are called cusps of the curve $X_0(\mathfrak{n})$. They are actually defined over F. Since we assumed that $\mathfrak{p}$ is a prime the curve $X_0(\mathfrak{p})$ has two cusps. The cyclic group generated by the divisor which is the difference of the two cusps is called the cuspidal divisor group and it is denoted by $\mathcal{C}(\mathfrak{p})$.

Theorem 1.4. *The group $\mathcal{T}(\mathfrak{p})$ is equal to $\mathcal{C}(\mathfrak{p})$.*

Notation 1.5. The theorem above has a pair which describes the largest étale subgroup scheme of $J_0(\mathfrak{p})$ whose Cartier dual is constant. Let us introduce some additional notation in order to formulate it. Let $Y_1(\mathfrak{p})$ denote the Drinfeld modular curve parameterizing Drinfeld modules of rank two over A of general characteristic with Γ_1-type level $\mathfrak{p}$-structure. The forgetful map $Y_1(\mathfrak{p}) \to Y_0(\mathfrak{p})$ is a Galois cover defined over F with Galois group $(A/\mathfrak{p})^*/\mathbb{F}_q^*$. Let $Y_2(\mathfrak{p}) \to Y_0(\mathfrak{p})$ denote the unique covering intermediate of this covering which is a Galois covering, cyclic of order $N(\mathfrak{p})$, and let $J_2(\mathfrak{p})$ denote the Jacobian of the unique geometrically irreducible non-singular projective curve $X_2(\mathfrak{p})$ containing $Y_2(\mathfrak{p})$. The kernel of the homomorphism $J_0(\mathfrak{p}) \to J_2(\mathfrak{p})$ induced by Picard functoriality is called the Shimura group scheme and it is denoted by $\mathcal{S}(\mathfrak{p})$. For every field K let $\overline{K}$ denote the separable algebraic closure of K. We say that a finite flat subgroup scheme of $J_0(\mathfrak{p})$ is a μ-type group scheme if its Cartier dual is a constant group scheme. If this group scheme is étale, then it is uniquely determined by the group of its $\overline{F}$-valued points. The latter group actually lies in $J_0(\mathfrak{p})(\overline{\mathbb{F}}_q(T))$, where $\overline{\mathbb{F}}_q(T)$ is the maximal everywhere unramified extension of F. Let $\mathcal{M}(\mathfrak{p})$ denote the unique maximal μ-type étale subgroup scheme of $J_0(\mathfrak{p})$.

Theorem 1.6. *The group schemes $\mathcal{M}(\mathfrak{p})$ and $\mathcal{S}(\mathfrak{p})$ are equal. In particular the former is a cyclic group scheme of rank equal to $N(\mathfrak{p})$.*

These results are proved via a detailed study of the Eisenstein ideal in the Hecke algebra of the Drinfeld modular curve $Y_0(\mathfrak{p})$, defined in [18] first in this context. In particular we prove that the completion of the Hecke algebra at any prime ideal in the support of Eisenstein ideal is Gorenstein (Corollary 10.3 and Theorem 11.6). The main goal to develop such a theory in its original setting was to classify the rational torsion subgroups of elliptic curves. Some of the methods and results of this paper can be used to give a similar classification of the rational torsion subgroups of Drinfeld modules of rank two in our setting as well, whose complete proof will appear in a forthcoming paper of the author.

Contents 1.7. Of course this work is strongly influenced by [14], where Mazur proved similar theorems for elliptic modular curves, conjectured originally by Ogg. Therefore the structure of the paper is similar to [14], although there are several significant differences, too. In the next two chapters we develop the tools necessary to study congruences between automorphic forms with respect to a modulus prime to the characteristic of F: Fourier expansions and the multiplicity one theorem. Almost everything we prove is a straightforward generalization of classical results in [19]. The main idea is that the additive group of adeles of F is a pro-p group, so it is possible to do Fourier analysis for locally constant functions taking values in a ring where p is invertible. In the fourth chapter we prove an analogue of the classical Kronecker limit formula, a result of independent interest. One motivation for this result in our setting is that it connects the Eisenstein series with the geometry of the modular curve directly. We compute the Fourier coefficients of Eisenstein series in the fifth chapter and give a new, more conceptual proof of a theorem of Gekeler on the Drinfeld discriminant function. As an application of our previous results we determine the largest sub-module $\mathcal{E}_0(\mathfrak{p}, R)$ of R-valued cuspidal harmonic forms annihilated by the Eisenstein ideal in the sixth chapter, for certain rings R. The first cases of Theorem 1.4 are proved in the seventh chapter, where we connect the geometry of the modular curve to our previous observations via the uniformization theorem of Gekeler-Reversat (see [11]). With the help of a theorem of Gekeler and Nonnengardt we show that the image of the n-torsion part of $\mathcal{T}(\mathfrak{p})$, n prime to p, in the group of connected components of the Néron model of $J_0(\mathfrak{p})$ at ∞ with respect to specialization injects into $\mathcal{E}_0(\mathfrak{p}, \mathbb{Z}/n\mathbb{Z})$ without any assumptions on $t(\mathfrak{p})$, the greatest common divisor of $N(\mathfrak{p})$ and $q-1$. We also show that there is no p-torsion using a result on the reduction of $Y_0(\mathfrak{p})$ over the prime $\mathfrak{p}$, again due to Gekeler (see [6]). Then we conclude the proof of Theorem 7.19 by showing that the exponent of the kernel of the specialization map into the group of connected components at ∞ in $\mathcal{T}(\mathfrak{p})$ is only divisible by primes dividing $t(\mathfrak{p})$. We prove some important properties of the Shimura group scheme in the eight chapter. In order to do so, we first include a section on a model $M_1(\mathfrak{p})$ of $Y_1(\mathfrak{p})$ with particular emphasis on the structure of its fiber at the prime $\mathfrak{p}$ in this chapter, as the current literature on the reduction of Drinfeld modular curves is somewhat incomplete. We study an important finite étale sub-group scheme of $J_0(\mathfrak{p})$ analogous to the Dihedral subgroup of Mazur in the next chapter. The latter is an object constructed to remedy the fact that the intersection of the cuspidal and Shimura subgroups could be non-empty. Here some of the calculations overlap with the results of [5], but the author could not resist the temptation to use the methods of chapters 4 and 5 in this setting, too. The goal of the last two chapters is to fully implement Mazur's Eisenstein decent at Eisenstein primes l. The key idea here is that considerations at the prime l in Mazur's original paper should be substituted by similar arguments at the place ∞. In particular the role of the connected-étale devissage of the l-division group of the Jacobian of the classical elliptic modular curve is played by the filtration of the l-adic Tate module of $J_0(\mathfrak{p})$ defined by the monodromy-weight spectral sequence at ∞. His arguments carry over with minor modifications, but it is interesting to note that the concept of $*$-type groups is only defined for subgroups of the Jacobian $J_0(\mathfrak{p})$, unlike in the classical case considered by Mazur, where the similar concept was absolute. The main Diophantine application of the results of these chapters are Theorem 1.6 and Theorem 1.4 in the cases not taken care of by Theorem 7.19. At the end of the paper an index of notations is included for the convenience of the reader.

Acknowledgment 1.8. I wish to thank the CICMA and the CRM for their warm hospitality and the pleasant environment they created for productive research, where the most of this article was written. I also wish to thank the IHÉS for its welcoming atmosphere, where this work was completed.

2. Fourier expansion

Definition 2.1. A topological group P is a pro-p group if it is a projective limit of finite p-groups. In other words P is a compact, Haussdorf topological group which has a basis of translates of finite index subgroups and every finite quotient is a p-group. In this paper all rings are assumed to be commutative with unity. If R is a ring, we will write $1/p \in R$ if we want to say that p is invertible in R. We will call a ring R a coefficient ring if $1/p \in R$ and R is the quotient of a discrete valuation ring $\tilde{R}$ which contains p-th roots of unity. For example every algebraically closed field of characteristic different from p is a coefficient ring. Note that the image of the p-th roots of unity of $\tilde{R}$ in R are exactly the set of p-th roots of unity of R. If R is a ring, then we say that a function $f : P \to R$ is continuous, if it continuous with respect to the discrete topology on R. This is equivalent to f being a locally constant function on P.

Lemma 2.2. *There is a unique $\mathbb{Z}\langle\frac{1}{p}\rangle$-valued function μ on the open and closed subsets of P such that*
(a) for any disjoint disjoint open set U and V we have $\mu(U \cup V) = \mu(U) + \mu(V)$,
(b) for any open set U and $g \in P$ we have $\mu(U) = \mu(gU) = \mu(Ug)$,
(c) for every open subgroup U we have $\mu(U) = \frac{1}{|P:U|}$.

Proof. Existence and uniqueness immediately follows from the fact that every open and closed subset of P is a pairwise disjoint union of finitely many translates of some open subgroup U. □

Definition 2.3. The function μ will be called the normalized Haar-measure on P. If R is a ring with $1/p \in R$, then for every continuous function $f : P \to R$ we define its integral with respect to μ as

$$\int_P f(x)\mathrm{d}\mu(x) = \sum_{r \in R} r\mu(f^{-1}(r)).$$

Since all but finitely many terms of the sum above are zero, the integral is well-defined.

Definition 2.4. Assume that P is abelian. We denote the set of continuous homomorphisms $\chi : P \to R^*$ by $\widehat{P}(R)$. We define for each continuous function $f : P \to R$ and $\chi \in \widehat{P}(R)$ a homomorphism:

$$\widehat{f}(\chi) = \int_P f(x)\chi^{-1}(x)\mathrm{d}\mu(x) \in R.$$

Lemma 2.5. *Assume that R is a coefficient ring and P is p-torsion. Then for each continuous function $f : P \to R$ the function $\widehat{f} : \widehat{P}(R) \to R$ is supported on a finite set and*

$$f(x) = \sum_{\chi \in \widehat{P}} \widehat{f}(\chi)\chi(x).$$

Proof. Let $\tilde{R}$ denote a discrete valuation ring whose quotient is R, just like in Definition 2.1. Since P is compact, f takes finitely many values, so there is a continuous function $\tilde{f} : P \longrightarrow \tilde{R}$ lifting f, which means that the composition of $\tilde{f}$ and the surjection $\tilde{R} \longrightarrow R$ is f. Since P is p-torsion, all continuous homomorphisms $\chi : P \to R^*$ have a unique lift $\tilde{\chi} \in \widehat{P}(\tilde{R})$. Hence it is sufficient to prove the statement for $\tilde{f}$. There is an open subgroup $U \leq P$ such that $\tilde{f}$ is U-invariant. Then for all but finitely $\chi \in \widehat{P}(\tilde{R})$ we have $\mathrm{Ker}(\chi) \nsubseteq U$ and hence $\widehat{\tilde{f}}(\chi) = 0$. The formula is then a consequence of the similar formula for the group P/U, which is well-known. $\square$

Notation 2.6. Let F denote the function field of X, where the latter is a geometrically connected smooth projective curve defined over the finite field $\mathbb{F}_q$ of characteristic p. Let $|X|$, $\mathbb{A}$, $\mathcal{O}$ denote set of places of F, the ring of adeles of F and its maximal compact subring of $\mathbb{A}$, respectively. F is embedded canonically into $\mathbb{A}$. The group $F\backslash\mathbb{A}$ is compact, totally disconnected and it is p-torsion, hence it is a pro-p group.

Lemma 2.7. *Let R be a coefficient ring. If $\tau : F\backslash\mathbb{A} \to R^*$ is a non-trivial continuous homomorphism, then all other elements of $\widehat{F\backslash\mathbb{A}}(R)$ are of the form $x \mapsto \tau(\eta x)$ for some $\eta \in F$.*

Proof. Since $F\backslash\mathbb{A}$ is p-torsion, the image of any element of $\widehat{F\backslash\mathbb{A}}(R)$ lies in the p-th roots of unity of the ring R. This group can be identified with the subgroup of p-th roots of unity in the field of complex numbers, hence the claim follows from the same statement for complex-valued characters. $\square$

Definition 2.8. For every divisor $\mathfrak{m}$ of X let $\mathfrak{m}$ also denote the $\mathcal{O}$-module in the ring $\mathbb{A}$ generated by the ideles whose divisor is $\mathfrak{m}$, by abuse of notation. Let $\mathfrak{n}$ be an effective divisor of X. By an R-valued automorphic form over F of level $\mathfrak{n}$ we mean a locally constant function $\phi : GL_2(\mathbb{A}) \to R$ satisfying $\phi(\gamma gkz) = \phi(g)$ for all $\gamma \in GL_2(F)$, $z \in Z(\mathbb{A})$, and $k \in \mathbb{K}_0(\mathfrak{n})$, where $Z(\mathbb{A})$ is the center of $GL_2(\mathbb{A})$, and

$$\mathbb{K}_0(\mathfrak{n}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}) | c \equiv 0 \bmod \mathfrak{n}\}.$$

Moreover, if for all $g \in GL_2(\mathbb{A})$:

$$\int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g) \mathrm{d}\mu(x) = 0,$$

where $\mathrm{d}\mu(x)$ is the normalized Haar measure on $F\backslash\mathbb{A}$, we call ϕ a cusp form. Let $\mathcal{A}(\mathfrak{n}, R)$ (respectively $\mathcal{A}_0(\mathfrak{n}, R)$) denote the R-module of R-valued automorphic forms (respectively cuspidal automorphic forms) of level $\mathfrak{n}$.

Notation 2.9. Let $\mathrm{Pic}(X)$ and $\mathrm{Div}(X)$ denote the Picard group and the divisor group of the algebraic curve X, respectively. For every $y \in \mathbb{A}^*$ we denote the corresponding divisor and its class in $\mathrm{Pic}(X)$ by the same symbol by abuse of notation. For any idele or divisor y let $|y|$ and $\deg(y)$ denote its normalized absolute value and degree, respectively, related by the formula $|y| = q^{-\deg(y)}$.

Proposition 2.10. *Let R be a coefficient ring and let $\tau : F\backslash\mathbb{A} \to R^*$ be a nontrivial continuous homomorphism. Then for every $\phi \in \mathcal{A}(\mathfrak{n}, R)$ there are functions $\phi^0 : \mathrm{Pic}(X) \to R$ and $\phi^* : \mathrm{Div}(X) \to R$, the latter vanishing on non-effective divisors such that*

$$\phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}) = \phi^0(y) + \sum_{\eta \in F^*} \phi^*(\eta y \mathfrak{d}^{-1}) \tau(\eta x),$$

for all $y \in \mathbb{A}^*$ and $x \in \mathbb{A}$, where the idele $\mathfrak{d}$ is such that $\mathcal{D} = \mathfrak{d}\mathcal{O}$, where $\mathcal{D}$ is the $\mathcal{O}$-module defined as

$$\mathcal{D} = \{x \in \mathbb{A} | \tau(x\mathcal{O}) = 1\}.$$

The functions ϕ^0 and ϕ^* are called the Fourier coefficients of the automorphic form ϕ with respect to the character τ.

Proof. By the condition of Definition 2.8:

$$\phi(\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}) = \phi(\begin{pmatrix} y & x+\eta \\ 0 & 1 \end{pmatrix}) = \phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}),$$

for every $y \in \mathbb{A}^*$ and $\eta \in F$, so there is a expansion, by Lemma 2.5 and Lemma 2.7:

$$\phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}) = \sum_{\eta \in F} a(\eta, y) \tau(\eta x).$$

Since

$$\phi(\begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}) = \phi(\begin{pmatrix} \eta y & \eta x \\ 0 & 1 \end{pmatrix}) = \phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}),$$

for every $y \in \mathbb{A}^*$ and $\eta \in F^*$, we have $a(\kappa, \eta y) = a(\kappa\eta, y) = a(\kappa\eta y)$ for some function $a : \mathbb{A}^* \to R$.

For any $k \in \mathcal{O}^*$, $l \in \mathcal{O}$

$$\phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} k & l \\ 0 & 1 \end{pmatrix}) = \phi(\begin{pmatrix} yk & x+yl \\ 0 & 1 \end{pmatrix}) = \phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}),$$

again by the definition of automorphic forms, we have $a(ky)\tau(ly) = a(y)$, which implies that $a(y)$ only depends on the divisor of y and $a(y)$ is nonzero only if y is in $\mathcal{D}$. A similar argument gives the existence of ϕ^0. □

It is worth noting that this notion of Fourier coefficients coincides with the classical one when both are defined. Also note that when R contains $1/p$, then the constant Fourier coefficients $\phi^0(\cdot)$ are still defined.

Notation 2.11. For any valuation v of F we will let F_v, $\mathbf{f}_v$ and $\mathcal{O}_v$ to denote the corresponding completion of F, its constant field, or its discrete valuation ring, respectively. For any idele, adele, adele-valued matrix or function defined on the above which decomposes as an infinite product of functions defined on the individual components the subscript v will denote the v-th component. Similar convention will be applied to subsets of adeles and adele-valued matrices. Let B denote the group scheme of invertible upper triangular two by two matrices. Let P denote the group scheme of invertible upper triangular two by two matrices with 1 on the lower right corner. Let U denote the group scheme of invertible upper triangular two by two matrices with ones on the diagonal.

Lemma 2.12. *Every $\phi \in \mathcal{A}(\mathfrak{n}, R)$ is uniquely determined by its restriction to $P(\mathbb{A})$.*

Proof. It is sufficient to prove that $GL_2(F)B(\mathbb{A})$ is dense in $GL_2(\mathbb{A})$, as we can determine the values of ϕ on that set from the values of ϕ on $P(\mathbb{A})$, by Definition 2.8. This property is equivalent to the fact that $GL_2(\mathbb{A}) = GL_2(F)B(\mathbb{A})\mathbb{K}$ for every compact, open subgroup $\mathbb{K} = \prod_{v\in|X|}\mathbb{K}_v$. Take any element g of $GL_2(\mathbb{A})$. There is a finite set S of places such that if $\mathbb{K}_v$ is not $GL_2(\mathcal{O}_v)$, then $s \in S$. As the natural image of $GL_2(F)$ in $\prod_{v\in S} GL_2(F_v)$ is dense, there is a $\gamma \in GL_2(F)$ such that the v-component of $\gamma^{-1}g$ is in $\mathbb{K}_v$ for all $v \in S$. But $\gamma^{-1}g$ is in $B(F_v)\mathbb{K}_v = B(F_v)GL_2(\mathcal{O}_v)$ for all other v by the Iwasawa decomposition, so the claim above follows. □

Proposition 2.13. *If R is a coefficient ring, every $\phi \in \mathcal{A}_0(\mathfrak{n}, R)$ ($\phi \in \mathcal{A}(\mathfrak{n}, R)$) is uniquely determined by the function ϕ^* (by the functions ϕ^* and ϕ^0).*

Proof. By Lemma 2.12, ϕ is uniquely determined by its restriction to $P(\mathbb{A})$, hence it is uniquely determined by the functions ϕ^* and ϕ^0. If ϕ is a cusp form then ϕ^0 is identically zero, hence ϕ is uniquely determined by the function ϕ^* alone. □

3. Multiplicity one

Definition 3.1. Let $\mathfrak{m}$, $\mathfrak{n}$ be effective divisors of X. Define the set:

$$H(\mathfrak{m},\mathfrak{n}) = \\ \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{A}) | a,b,c,d \in \mathcal{O}, (ad-cb)=\mathfrak{m}, \mathfrak{n} \supseteq (c), (d)+\mathfrak{n}=\mathcal{O}\}.$$

The set $H(\mathfrak{m},\mathfrak{n})$ is compact and it is a double $\mathbb{K}_0(\mathfrak{n})$-coset, so it is a disjoint union of finitely many right $\mathbb{K}_0(\mathfrak{n})$-cosets. Let $R(\mathfrak{m},\mathfrak{n})$ be a set of representatives of these cosets. For any $\phi \in \mathcal{A}(\mathfrak{n},R)$ (or more generally, for any right $\mathbb{K}_0(\mathfrak{n})$-invariant R-valued function) define the function $T_{\mathfrak{m}}(\phi)$ by the formula:

$$T_{\mathfrak{m}}(\phi)(g) = \sum_{h \in R(\mathfrak{m},\mathfrak{n})} \phi(gh).$$

It is easy to check that $T_{\mathfrak{m}}(\phi)$ is independent of the choice of $R(\mathfrak{m},\mathfrak{n})$ and $T_{\mathfrak{m}}(\phi) \in \mathcal{A}(\mathfrak{n},R)$ as well. So we have an R-linear operator $T_{\mathfrak{m}} : \mathcal{A}(\mathfrak{n},R) \to \mathcal{A}(\mathfrak{n},R)$.

Lemma 3.2. *Let R be a coefficient ring. Then for every $\phi \in \mathcal{A}(\mathfrak{n},R)$ and $\mathfrak{m}$ ideal*

$$T_{\mathfrak{m}}(\phi)^*(\mathfrak{r}) = \sum_{\substack{\mathfrak{c}+\mathfrak{n}=\mathcal{O} \\ \mathfrak{r}+\mathfrak{m}\subseteq\mathfrak{c}}} \frac{|\mathfrak{c}|}{|\mathfrak{m}|}\phi^*(\frac{\mathfrak{r}\mathfrak{m}}{\mathfrak{c}^2}).$$

Proof. One particular choice of the representative system is

$$R(\mathfrak{m},\mathfrak{n}) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | (a,d) \in S,\ b \in S(a)\},$$

where S is a $\mathcal{O}^* \times \mathcal{O}^*$-representative system to all pairs $(a,d) \in \mathcal{O}\times\mathcal{O}$ such that $(ad)=\mathfrak{m}$ and $(d)+\mathfrak{n}=\mathcal{O}$, and for each $a \in \mathcal{O}$ the set $S(a)$ is a representative system of the cosets of the ideal (a) in $\mathcal{O}$. For any adele $y \in \mathcal{O}$:

$$\begin{aligned} T_{\mathfrak{m}}(\phi)^*(y) &= \int_{F\backslash\mathbb{A}} T_{\mathfrak{m}}(\phi)(\begin{pmatrix} y\mathfrak{d} & x \\ 0 & 1 \end{pmatrix})\tau(-x)\mathrm{d}\mu(x) \\ &= \sum_{\substack{(a,d)\in S \\ b\in S(a)}} \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} y\mathfrak{d}a & y\mathfrak{d}b+dx \\ 0 & d \end{pmatrix})\tau(-x)\mathrm{d}\mu(x) \\ &= \sum_{(a,d)\in S}\sum_{b\in S(a)} \tau(y\mathfrak{d}b/d)\int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} y\mathfrak{d}a/d & x \\ 0 & 1 \end{pmatrix})\tau(-x)\mathrm{d}\mu(x) \\ &= \sum_{(a,d)\in S} \phi^*(ya/d) \sum_{b\in S(a)} \tau(y\mathfrak{d}b/d). \end{aligned}$$

If $\phi^*(ya/d) \neq 0$ then $ya/d \in \mathcal{O}$ and the map $b \mapsto \tau(y\mathfrak{d}b/d)$ is an R-valued character on $\mathcal{O}/(a)$. In this case the sum $\sum_{b\in S(a)} \tau(y\mathfrak{d}b/d) = |a|^{-1}$, if $y/d \in \mathcal{O}$, and equal to 0, otherwise. Hence if we set $\mathfrak{c} = (d)$, we get:

$$T_{\mathfrak{m}}(\phi)^*(\mathfrak{r}) = \sum_{\substack{\mathfrak{c}+\mathfrak{n}=\mathcal{O}\\ \mathfrak{r}+\mathfrak{m}\subseteq\mathfrak{c}}} \frac{|\mathfrak{c}|}{|\mathfrak{m}|}\phi^*(\frac{\mathfrak{r}\mathfrak{m}}{\mathfrak{c}^2}). \ \square$$

Corollary 3.3. *Let R be a coefficient ring and assume that for each closed point $\mathfrak{p}$ of X an element $c_{\mathfrak{p}} \in R$ is given. Then the R-module of cuspidal automorphic forms $\phi \in \mathcal{A}_0(\mathfrak{n}, R)$ such that $T_{\mathfrak{p}}(\phi) = c_{\mathfrak{p}}\phi$ for each closed point $\mathfrak{p}$ of X is isomorphic to an ideal $\mathfrak{a} \lhd R$ via the map $\phi \mapsto \phi^*(1)$.*

Proof. For each effective divisor $\mathfrak{r}$ we are going to show that $\phi^*(\mathfrak{r})$ is uniquely determined by the eigenvalues $c_{\mathfrak{p}}$ and $\phi^*(1)$ by induction on the maximum $d(\mathfrak{r})$ of exponents of prime divisors of $\mathfrak{r}$. By Proposition 2.13 this implies the proposition. If $d(\mathfrak{r}) = 0$ then the claim is obvious. If $d(\mathfrak{r}) = 1$, then $\mathfrak{r} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ is the product of pair-wise different prime divisors. By Lemma 3.2 we have:

$$c_{\mathfrak{p}_1}\cdots c_{\mathfrak{p}_n}\phi^*(1) = T_{\mathfrak{p}_1}\cdots T_{\mathfrak{p}_n}(\phi)^*(1) = \frac{1}{|\mathfrak{p}_1\cdots\mathfrak{p}_n|}\phi^*(\mathfrak{p}_1\cdots\mathfrak{p}_n).$$

If $d(\mathfrak{r}) > 1$, then $\mathfrak{r} = \mathfrak{m}\mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$. The lemma above implies that we have the recursive relation:

$$c_{\mathfrak{p}}\phi^*(\mathfrak{m}\mathfrak{p}) = T_{\mathfrak{p}}(\phi)^*(\mathfrak{m}\mathfrak{p}) = \frac{1}{|\mathfrak{p}|}\phi^*(\mathfrak{m}\mathfrak{p}^2) + \phi^*(\mathfrak{m}),$$

if $\mathfrak{p}$ does not lie in the support of $\mathfrak{n}$, and

$$c_{\mathfrak{p}}\phi^*(\mathfrak{m}\mathfrak{p}) = T_{\mathfrak{p}}(\phi)^*(\mathfrak{m}\mathfrak{p}) = \frac{1}{|\mathfrak{p}|}\phi^*(\mathfrak{m}\mathfrak{p}^2),$$

otherwise. $\square$

Definition 3.4. Fix a valuation ∞ of F. We may assume that the support of divisor $\mathfrak{d}$ attached to the character τ in Proposition 2.10 does not contain ∞. Let $\mathcal{H}(\mathfrak{n}, R)$ denote the R-module of automorphic forms f of level $\mathfrak{n}\infty$ satisfying the following two identities:

$$\phi(g\begin{pmatrix} 0 & 1 \\ \upsilon & 0 \end{pmatrix}) = -\phi(g), (\forall g \in GL_2(\mathbb{A})),$$

and

$$\phi(g\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) + \sum_{\epsilon\in\mathbf{f}_\infty} \phi(g\begin{pmatrix} 1 & 0 \\ \epsilon & 1 \end{pmatrix}) = 0, (\forall g \in GL_2(\mathbb{A})),$$

where υ is a uniformizer in F_∞ and we consider $GL_2(F_\infty)$ as a subgroup of $GL_2(\mathbb{A})$ and we understand the product of their elements accordingly. Such automorphic forms are called harmonic. Let $\mathcal{H}_0(\mathfrak{n}, R)$ denote the R-module of R-valued cuspidal harmonic forms of level $\mathfrak{n}\infty$.

Lemma 3.5. *Let ϕ be an element of $\mathcal{H}(\mathfrak{n}, R)$. Then $T_\infty(\phi) = \phi$.*

Proof. For any $\epsilon \in \mathbf{f}_\infty^*$ we have the matrix identity:

$$\begin{pmatrix} 1 & 0 \\ \epsilon & 1 \end{pmatrix}\begin{pmatrix} \epsilon^{-1} & 1 \\ 0 & -\epsilon \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \upsilon & 0 \end{pmatrix} = \begin{pmatrix} \upsilon & \epsilon^{-1} \\ 0 & 1 \end{pmatrix}.$$

Hence the second identity in Definition 3.4 can be rewritten as follows:

$$\begin{aligned} 0 = & \phi(g\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) + \sum_{\epsilon \in \mathbf{f}_\infty} \phi(g\begin{pmatrix} 1 & 0 \\ \epsilon & 1 \end{pmatrix}) \\ = & -\phi(g\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \upsilon & 0 \end{pmatrix}) + \phi(g) - \sum_{\epsilon \in \mathbf{f}_\infty^*} \phi(g\begin{pmatrix} \upsilon & \epsilon^{-1} \\ 0 & 1 \end{pmatrix}) = \phi(g) - T_\infty(\phi) \end{aligned}$$

using the left $\mathbb{K}_0(\mathfrak{n}\infty)$-invariance and the first identity. □

Proposition 3.6. *Let R be a coefficient ring and assume that for each closed point $\mathfrak{p} \neq \infty$ of X an element $c_\mathfrak{p} \in R$ is given. Then the R-module of cuspidal harmonic forms $\phi \in \mathcal{H}_0(\mathfrak{n}, R)$ such that $T_\mathfrak{p}(\phi) = c_\mathfrak{p}\phi$ for each closed point $\mathfrak{p} \neq \infty$ of X is isomorphic to an ideal $\mathfrak{a} \triangleleft R$ via the map $\phi \mapsto \phi^*(1)$.*

Proof. By the lemma above ϕ is also an eigenvector for T_∞. The claim now follows from Corollary 3.3. □

Remark 3.7. The result above is the analogue of the classical (weak) multiplicity one result for mod p modular forms. In order to be useful for some of the applications we have in mind, we will need a multiplicity one result which does not require the eigenvalue of $T_\mathfrak{p}$ to be specified for every closed point $\mathfrak{p}$. We will prove such a result only in a special case. First let us introduce the following general notation: let $\mathbb{A}_f$, $\mathcal{O}_f$ denote the restricted direct products $\prod'_{x \neq \infty} F_x$ and $\prod'_{x \neq \infty} \mathcal{O}_x$, respectively. The former is also called the ring of finite adeles of F and the latter is its maximal compact subring. For the rest of the this chapter we assume that $F = \mathbb{F}_q(T)$ is the rational function field of transcendence degree one over $\mathbb{F}_q$, where T is an indeterminate, and ∞ is the point at infinity on $X = \mathbb{P}^1(F)$. Finally let $M[n]$ denote the n-torsion submodule of every abelian group M for any natural number $n \in \mathbb{N}$.

Proposition 3.8. *The map*

$$\mathcal{H}(1, R) \to R, \quad \phi \mapsto \phi^0(1)$$

is an isomorphism onto $R[q+1]$ for every coefficient ring R.

Proof. It is well-known that there is a natural bijection:

$$\iota : GL_2(\mathbb{F}_q[T]) \backslash GL_2(F_\infty)/\Gamma_\infty Z(F_\infty) \longrightarrow GL_2(F) \backslash GL_2(\mathbb{A})/\mathbb{K}_0(\infty)Z(F_\infty),$$

where $\Gamma_\infty = K_0(\infty)_\infty$ denote the Iwahori subgroup of $GL_2(F_\infty)$:

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

and ι is induced by the natural inclusion $GL_2(F_\infty) \to GL_2(\mathbb{A})$. The former double coset is the set of edges of the Bruhat-Tits tree of the local field $F_\infty = \mathbb{F}_q((\frac{1}{T}))$ factored out by $GL_2(\mathbb{F}_q[T])$. Under this bijection elements of $\mathcal{H}(1,R)$ correspond to $GL_2(\mathbb{F}_q[T])$-invariant R-valued harmonic cochains on the Bruhat-Tits tree. This correspondence is bijective, because $Z(\mathbb{A}) = Z(F)Z(\mathcal{O})Z(F_\infty)$, so every harmonic cochain is invariant with respect to this group. The reader may find the following description of the quotient graph above in Proposition 3 of 1.6 of [17], page 86-67:

Proposition 3.9. *Let Λ_n denote the vertex of the Bruhat-Tits tree represented by the matrix $\left(\begin{smallmatrix} T^n & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for every natural number $n \in \mathbb{N}$.*

- (i) *the vertices Λ_n form a fundamental domain for the action of $GL_2(\mathbb{F}_q[T])$ on the set of vertices of the Bruhat-Tits tree,*
- (ii) *the stabilizer of Λ_0 in $GL_2(\mathbb{F}_q[T])$ acts transitively on the set of edges with origin Λ_0,*
- (iii) *for every n there is an edge $\Lambda_n\Lambda_{n+1}$ with origin Λ_n and terminal vertex Λ_n,*
- (iv) *for every $n \geq 1$, the stabilizer of the edge $\Lambda_n\Lambda_{n+1}$ in $GL_2(\mathbb{F}_q[T])$ acts transitively on the set of edges with origin Λ_n distinct from $\Lambda_n\Lambda_{n+1}$.*

Proof. The second half of (i) is the corollary to the proposition quoted above on page 87 of [17]. □

Let us return to the proof of Proposition 3.8. Let α denote the value of the harmonic cochain Φ corresponding to ϕ on the edge $\Lambda_0\Lambda_1$. By (ii) of the proposition above the value of Φ is α on all other edges with origin Λ_0, so $\alpha \in R[q+1]$ by harmonicity. We are going to show that $\Phi(\Lambda_n\Lambda_{n+1}) = (-1)^n\alpha$ for all n by induction. By harmonicity $\Phi(\Lambda_n\Lambda_{n-1}) = -(-1)^{n-1}\alpha = (-1)^n\alpha$. Also note that the value of Φ is $(-1)^n\alpha$ on all edges with origin Λ_n distinct from $\Lambda_n\Lambda_{n+1}$ by (iv) of the proposition above. Hence we must have $\Phi(\Lambda_n\Lambda_{n+1}) = (-q)(-1)^n\alpha = (-1)^n\alpha$ by harmonicity, also using the fact $\alpha \in R[q+1]$. We conclude that Φ is uniquely determined by its value on the edge $\Lambda_0\Lambda_1$. For every $g \in GL_2(\mathbb{A})$ the residue of the degree of the divisor $\det(g)$ modulo 2 depends only on its class in $GL_2(F)\backslash GL_2(\mathbb{A})/\mathbb{K}_0(1)Z(\mathbb{A})$. In particular if g is equivalent to the vertex Λ_n, then $n \equiv \deg(\det(g)) \mod 2$. Hence our description of Φ can be reformulated by saying that $\phi(g) = (-1)^{\deg(\det(g))}\alpha$. Moreover

$$\phi^0(1) = \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix})\mathrm{d}\mu(x) = \int_{F\backslash\mathbb{A}} \alpha \mathrm{d}\mu(x) = \alpha,$$

because every element of the set, where the integral above is taken, has determinant 1. On the other hand for every $\alpha \in R[q+1]$ the function $H(\alpha)$, whose value is $(-1)^n\alpha$ on every edge of origin Λ_n, is clearly a harmonic cochain. The claim follows. □

Proposition 3.10. *Let R be a coefficient ring and let $\mathfrak{p} \neq \infty$ be a closed point of X. Then every harmonic form $\phi \in \mathcal{H}(\mathfrak{p}, R)$ such that $\phi^*(\mathfrak{m}) = 0$ for each effective divisor $\mathfrak{m}$ whose support does not contain $\mathfrak{p}$ and ∞ is an element of $\mathcal{H}(1, R)$.*

Proof. First note that $\phi^*(\mathfrak{m}) = 0$ even for those effective divisors $\mathfrak{m}$ whose support do not contain $\mathfrak{p}$, but may contain ∞, since for any effective divisor $\mathfrak{n}$ we have:

$$\phi^*(\mathfrak{n}) = T_\infty(\phi)^*(\mathfrak{n}) = \frac{1}{|\infty|}\phi^*(\mathfrak{n}\infty),$$

by Lemma 3.2 and Lemma 3.5, so this seemingly stronger statement follows from the condition in the claim by induction on the multiplicity of ∞ in $\mathfrak{m}$. For every $y \in \mathbb{A}^*$ and a, $x \in \mathbb{A}$ we have:

$$\begin{aligned}\phi(\begin{pmatrix} y & x \\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1\end{pmatrix}) =& \phi(\begin{pmatrix} y & x+ya \\ 0 & 1\end{pmatrix}) \\ =& \phi^0(y) + \sum_{\eta \in F^*} \phi^*(\eta y \mathfrak{d}^{-1})\tau(\eta y a)\tau(\eta x).\end{aligned}$$

If $a \in \mathfrak{p}^{-1}$, then $\phi^*(\eta y \mathfrak{d}^{-1}) = 0$ unless $\tau(\eta y a) = 1$, because $\phi^*(\eta y \mathfrak{d}^{-1}) \neq 0$ implies that $\eta y \in \mathfrak{p}\mathcal{D}$, so $\eta y a \in \mathfrak{p}\mathcal{D}\mathfrak{p}^{-1} \subset \mathrm{Ker}(\tau)$. Hence the Fourier expansion above is independent of the choice of $a \in \mathfrak{p}^{-1}$, so for every $g \in P(\mathbb{A})$ and a as above we have:

$$\phi(g\begin{pmatrix} 1 & a \\ 0 & 1\end{pmatrix}) = \phi(g).$$

In the proof of Lemma 2.12 we showed that $GL_2(F)P(\mathbb{A})Z(\mathbb{A})$ is dense in $GL_2(\mathbb{A})$, so the identity above holds for all $g \in GL_2(\mathbb{A})$ by continuity. Let $\pi \in \mathbb{A}_f^*$ be an idele such that $\pi\mathcal{O}_f = \mathfrak{p}$. We define the function $\psi : GL_2(\mathbb{A}) \to R$ by the formula:

$$\psi(g) = \phi(g\begin{pmatrix} 0 & 1 \\ \pi & 0\end{pmatrix}), \quad \forall g \in GL_2(\mathbb{A}),$$

where we consider $GL_2(\mathbb{A})$ as a $GL_2(\mathbb{A}_f)$-module and we understand the product of their elements accordingly. We claim that $\psi \in \mathcal{H}(1, R)$. It is clearly left-invariant with respect to $Z(\mathbb{A})GL_2(F)$. On the other hand we have:

$$\begin{aligned}\psi(g\begin{pmatrix} a & b \\ c & d\end{pmatrix}) = \phi(g\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} 0 & 1 \\ \pi & 0\end{pmatrix}) =& \phi(g\begin{pmatrix} 0 & 1 \\ \pi & 0\end{pmatrix}\begin{pmatrix} d & c/\pi \\ \pi b & a\end{pmatrix}) \\ =& \phi(g\begin{pmatrix} 0 & 1 \\ \pi & 0\end{pmatrix}) = \psi(g)\end{aligned}$$

for all $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathbb{K}_0(\mathfrak{p}) \cap GL_2(\mathbb{A}_f)$, upon using the identity:

$$\begin{pmatrix} 0 & 1 \\ \pi & 0\end{pmatrix}\begin{pmatrix} d & c/\pi \\ \pi b & a\end{pmatrix} = \begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} 0 & 1 \\ \pi & 0\end{pmatrix},$$

hence $\psi \in \mathcal{A}(\mathfrak{p}\infty, R)$. The same identity may be used to show that:

$$\begin{aligned}\psi(g\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix}) = \phi(g\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ \pi & 0\end{pmatrix}) &= \phi(g\begin{pmatrix}0 & 1\\ \pi & 0\end{pmatrix}\begin{pmatrix}1 & a/\pi\\ 0 & 1\end{pmatrix})\\ &= \phi(g\begin{pmatrix}0 & 1\\ \pi & 0\end{pmatrix}) = \psi(g)\end{aligned}$$

for all $a \in \mathcal{O}_f$, hence ψ is even in $\mathcal{A}(\infty, R)$. Obviously the matrix $\left(\begin{smallmatrix}0 & 1\\ \pi & 0\end{smallmatrix}\right)$ commutes with the matrices in Definition 3.4, so ψ is harmonic, too. Using the $Z(\mathbb{A})$-invariance of ψ we get:

$$\phi(g) = \psi(g\begin{pmatrix}0 & \pi^{-1}\\ 1 & 0\end{pmatrix}) = \psi(g\begin{pmatrix}0 & 1\\ \pi & 0\end{pmatrix}\begin{pmatrix}\pi^{-1} & 0\\ 0 & \pi^{-1}\end{pmatrix}) = \psi(g\begin{pmatrix}0 & 1\\ \pi & 0\end{pmatrix}),$$

the claim of the proposition follows by the lemma below and applying the same argument to ψ. □

Lemma 3.11. *For every harmonic form $\phi \in \mathcal{H}(1, R)$ we have $\phi^*(\mathfrak{m}) = 0$ for every effective divisor $\mathfrak{m}$.*

Proof. It will be sufficient to show that the function $x \mapsto \phi(\left(\begin{smallmatrix}y & x\\ 0 & 1\end{smallmatrix}\right))$ is constant on $\mathbb{A}$ for each $y \in \mathcal{O} \cap \mathbb{A}^*$. The latter follows from the fact that the determinant is constant, it is equal to y. □

Theorem 3.12. *Let R be a coefficient ring and let $\mathfrak{p} \neq \infty$ be a closed point of X. Assume that for each closed point $\mathfrak{q}$ of X, different from $\mathfrak{p}$ and ∞, an element $c_{\mathfrak{q}} \in R$ is given. Then the R-module of cuspidal harmonic forms $\phi \in \mathcal{H}_0(\mathfrak{p}, R)$ such that $T_{\mathfrak{q}}(\phi) = c_{\mathfrak{q}}\phi$ for each closed point $\mathfrak{q}$ of X, different from $\mathfrak{p}$ and ∞, is isomorphic to an ideal $\mathfrak{a} \triangleleft R$ via the map $\phi \mapsto \phi^*(1)$.*

Proof. It will be sufficient to prove that any such ϕ with $\phi^*(1) = 0$ is zero by taking the difference of any two elements of the module with the same first Fourier coefficient. The argument of Corollary 3.3 implies that $\phi^*(\mathfrak{m}) = 0$ for each effective divisor $\mathfrak{m}$ whose support does not contain $\mathfrak{p}$ and ∞ for every such ϕ. By Proposition 3.10 ϕ is in $\mathcal{H}(1, R)$, hence ϕ is an element of $\mathcal{H}_0(1, R)$, too. The latter R-module is trivial by Proposition 3.8. □

4. The Kronecker limit formula

Notation 4.1. We will adopt the convention which assigns 0 or 1 as value to the empty sum or product, respectively. For every $g \in GL_2(\mathbb{A})$ (or $g \in \mathbb{A}$, *etc.*) let g_f denote its finite component in $GL_2(\mathbb{A}_f)$. Let $|\cdot|$ denote the normalized absolute value with respect to ∞ if its argument is in F_∞. For each $(u, v) \in F_\infty^2$ let $\|(u, v)\|$, $\infty(u, v)$ denote $\max(|u|, |v|)$ and $\min(\infty(u), \infty(v))$, respectively.

Definition 4.2. Let $F^2_<$ denote the set: $F^2_< = \{(a,b) \in F^2_\infty \| |a| < |b|\}$. Let $\mathfrak{m}$ be an effective divisor on X whose support does not contain ∞. Let the same symbol also denote the ideal $\mathfrak{m} \cap \mathcal{O}_f$ by abuse of notation. For every $g \in GL_2(\mathbb{A})$, $(\alpha, \beta) \in (\mathcal{O}_f/\mathfrak{m})^2$, and n integer let

$$W_{\mathfrak{m}}(\alpha,\beta,g,n) = \{0 \neq f \in F^2 | fg_f \in (\alpha,\beta) + \mathfrak{m}\mathcal{O}_f^2, -n = \infty(fg_\infty)\}, \text{ and}$$

$$V_{\mathfrak{m}}(\alpha,\beta,g,n) = \{f \in W_{\mathfrak{m}}(\alpha,\beta,g,n) | fg_\infty \in F^2_<\}.$$

Also let

$$W_{\mathfrak{m}}(\alpha,\beta,g_f) = \bigcup_{n\in\mathbb{Z}} W_{\mathfrak{m}}(\alpha,\beta,g,n) \text{ and } V_{\mathfrak{m}}(\alpha,\beta,g) = \bigcup_{n\in\mathbb{Z}} V_{\mathfrak{m}}(\alpha,\beta,g,n).$$

Obviously the first set is well-defined. Finally let $E_{\mathfrak{m}}(\alpha,\beta,g,s)$ denote the $\mathbb{C}$-valued function:

$$E_{\mathfrak{m}}(\alpha,\beta,g,s) = |\det(g)|^s \sum_{f \in V_{\mathfrak{m}}(\alpha,\beta,g)} \|fg_\infty\|^{-2s},$$

for each complex number s and g, (α,β) as above, if the infinite sum is absolutely convergent.

Proposition 4.3. *The sum $E_{\mathfrak{m}}(\alpha,\beta,g,s)$ converges absolutely, if $\mathrm{Re}(s) > 1$, for each $g \in GL_2(\mathbb{A})$.*

Proof. The reader may find the same argument in [16]. The series $E_{\mathfrak{m}}(\alpha,\beta,g,s)$ is majorated by the series:

$$E(g,s) = |\det(g)|^s \sum_{\substack{f \in F^2 - \{0\} \\ fg \in \mathcal{O}_f^2}} \|(fg)_\infty\|^{-2s},$$

so it will be sufficient to prove that $E(g,s)$ converges absolutely for each $g \in GL_2(\mathbb{A})$ if $\mathrm{Re}(s) > 1$. For every $g \in GL_2(\mathbb{A})$ let $\mathcal{E}(g)$ denote the sheaf on X whose group of sections is for every open subset $U \subseteq X$ is

$$\mathcal{E}(g)(U) = \{f \in F^2 | fg \in \mathcal{O}_v^2, \forall v \in |U|\},$$

where we denote the set of closed points of U by $|U|$. The sheaf $\mathcal{E}(g)$ is a coherent locally free sheaf of rank two. If $\mathcal{F}_n$ denote the sheaf $\mathcal{F} \otimes \mathcal{O}_X(\infty)^n$ for every coherent sheaf $\mathcal{F}$ on X and integer n, then for every $g \in GL_2(\mathbb{A})$ and $s \in \mathbb{C}$ the series above can be rewritten as

$$E(g,s) = \sum_{n\in\mathbb{Z}} |H^0(X,\mathcal{E}(g)_n) - H^0(X,\mathcal{E}(g)_{n-1})| q^{-s\deg(\mathcal{E}(g)_n)}.$$

By the Riemann-Roch theorem for curves:

$$\dim H^0(X,\mathcal{F}) - \dim H^0(X, K_X \otimes \mathcal{F}^\vee) = 2 - 2g(X) + \deg(\mathcal{F})$$

for any coherent locally free sheaf of rank two $\mathcal{F}$ on X, where K_X, $\mathcal{F}^\vee$ and $g(X)$ is the canonical bundle on X, the dual of $\mathcal{F}$, and the genus of X, respectively. Because $\dim H^0(X,\mathcal{F}_{-n}) = 0$ for n sufficiently large depending on $\mathcal{F}$, we have that

$$|H^0(X,\mathcal{E}(g)_n)| = q^{2-2g(X)+\deg(\mathcal{E}(g))+2n\deg(\infty)} \text{ and } |H^0(X,\mathcal{E}(g)_{-n})| = 1,$$

if n is a sufficiently large positive number. Hence

$$E(g,s) = p(q^{-s}) + q^{2-2g(X)+(1-s)\deg(\mathcal{E}(g))}(1-q^{-\deg(\infty)})\sum_{n=0}^{\infty} q^{2n(1-s)\deg(\infty)},$$

where p is a polynomial. The claim now follows from the convergence of the geometric series. $\square$

Notation 4.4. Let Ω denote the rigid analytic upper half plane, or Drinfeld's upper half plane over F_∞. The set of points of Ω is $\mathbb{C}_\infty - F_\infty$, denoted also by Ω by abuse of notation, where $\mathbb{C}_\infty$ is the completion of the algebraic closure of F_∞. For the definition of its rigid analytic structure as well as the other concepts recalled below see for example [11]. For each holomorphic function $u : \Omega \longrightarrow \mathbb{C}_\infty^*$ let $r(u) : GL_2(F_\infty) \longrightarrow \mathbb{Z}$ denote the van der Put logarithmic derivative of u (see [11], page 40). If $u : GL_2(\mathbb{A}_f) \times \Omega \longrightarrow \mathbb{C}_\infty^*$ is holomorphic in the second variable for each $g \in GL_2(\mathbb{A}_f)$ then we define $r(u)$ to be the $\mathbb{Z}$-valued function on the set $GL_2(\mathbb{A}) = GL_2(\mathbb{A}_f) \times GL_2(F_\infty)$ given by the formula $r(u)(g_f, g_\infty) = r(u(g_f,\cdot))(g_\infty)$. For each $(\alpha,\beta) \in (\mathcal{O}_f/\mathfrak{m})^2$, and N positive integer let $\epsilon_{\mathfrak{m}}(\alpha,\beta,N)(g,z)$ denote the function:

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

on the set $GL_2(\mathbb{A}_f) \times \Omega$.

Lemma 4.5. *The limit*

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

converges uniformly in z on every admissible open subdomain of Ω for every fixed g and defines a function holomorphic in the second variable.

Proof. If $(\alpha,\beta)=(0,0)$ then the claim is trivial. Otherwise let (α,β) also denote an element of $W_{\mathfrak{m}}(\alpha,\beta,g_f)$ by abuse of notation. For sufficiently large N the product $\epsilon_{\mathfrak{m}}(\alpha,\beta,N)(g,z)$ can be rewritten as:

$$\epsilon_{\mathfrak{m}}(\alpha,\beta,N)(g,z)=(\alpha z+\beta)\cdot\prod_{\substack{n\leq N\\(a,b)\in W_{\mathfrak{m}}(0,0,g,n)}}\left(1+\frac{\alpha z+\beta}{az+b}\right).$$

The system of sets $\Omega(\omega)=\{z\in\mathbb{C}_\infty|1/\omega\leq|z|_i,|z|\leq\omega\}$, where $1<\omega$ is any rational number and $|z|_i=\inf_{x\in F_\infty}|z+x|$ is the imaginary absolute value of z, is a cover of Ω by admissible open subdomains. On the set $\Omega(\omega)$:

$$\left|\frac{\alpha z+\beta}{az+b}\right|\leq\frac{\max(\omega|\alpha|,|\beta|)}{\max(\omega^{-1}|a|,|b|)},$$

so it converges to zero as $\|(a,b)\|\to\infty$. The claim follows at once. $\square$

Definition 4.6. For every $\rho\in GL_2(F_\infty)$ and $z\in\mathbb{P}^1(\mathbb{C}_\infty)$ let $\rho(z)$ denote the image of z under the Möbius transformation corresponding to ρ. Let moreover $D(\rho)$ denote the open disc

$$D(\rho)=\{z\in\mathbb{P}^1(\mathbb{C}_\infty)|1<|\rho^{-1}(z)|\}.$$

Set $\delta(\rho)=-1$, if the infinite point of the projective line lies in $D(\rho)$, and let $\delta(\rho)=0$, otherwise.

Proposition 4.7. *For all $g\in GL_2(\mathbb{A})$ we have:*

$$r(\epsilon_{\mathfrak{m}}(\alpha,\beta))(g)=\delta(g_\infty)+\lim_{N\to\infty}\left(\sum_{n\leq N}|V_{\mathfrak{m}}(\alpha,\beta,g,n)|-|V_{\mathfrak{m}}(0,0,g,n)|\right).$$

Proof. The van der Put logarithmic derivative is continuous with respect to the limit of the supremum topologies on the affinoid subdomains of Ω, hence

$$r(\epsilon_{\mathfrak{m}}(\alpha,\beta))(g)=\lim_{N\to\infty}r(\epsilon_{\mathfrak{m}}(\alpha,\beta,N))(g)$$

by Lemma 4.5. More or less by definition (see [11]) for every $u\in\mathcal{O}^*(\Omega)$ rational function $r(u)(\rho)$ equals to the number of zeros z of u with $z\in D(\rho)$ counted with multiplicities minus the number of poles z of u with $z\in D(\rho)$ counted with multiplicities. If we assume that $\delta(\rho)=0$ then we can conclude that $r(az+b)(\rho)$ is 1 if and only if $(a,b)\rho\in F^2_<$ and it is 0, otherwise. Hence the claim holds for g if $\delta(g_\infty)=0$ by the additivity of the van der Put derivative. In particular the limit on the right exists in this case. Let $\Pi\in GL_2(F_\infty)$ be the matrix whose diagonal entries are zero, and its lower left and upper right entry is π and 1, respectively, where π is a uniformizer of F_∞. Clearly $F^2_\infty - \{0\} = F^2_< \coprod F^2_< \Pi$, hence

$$W_{\mathfrak{m}}(\alpha,\beta,g_f) = V_{\mathfrak{m}}(\alpha,\beta,g) \coprod V_{\mathfrak{m}}(\alpha,\beta,g\Pi)$$

for any $g \in GL_2(\mathbb{A})$. Also exactly one of the sets $D(g_\infty)$ and $D(g_\infty\Pi)$ contains the infinite point. Hence it will suffice to show that for any g and sufficiently large $N \in \mathbb{N}$ the sum

$$-1 + \sum_{n \leq N} (|W_{\mathfrak{m}}(\alpha,\beta,g,n)| - |W_{\mathfrak{m}}(0,0,g,n)|)$$

vanishes to conclude that the limit in the claim above exits in all cases. This will also imply that the expression $l(g)$ on right hand side satisfies the functional equation $l(g) + l(g\Pi) = 0$. Since the left hand side also satisfies this property the claim will follow. But the sum above vanishes because of the bijection which we already used implicitly in the proof of Lemma 4.5 when we rewrote $\epsilon_{\mathfrak{m}}(\alpha,\beta,N)(g,z)$. $\square$

Kronecker Limit Formula 4.8. *For all $g \in GL_2(\mathbb{A})$ we have:*

$$r(\epsilon_{\mathfrak{m}}(\alpha,\beta))(g) = \delta(g_\infty) + \lim_{s \to 0^+} (E_{\mathfrak{m}}(\alpha,\beta,g,s) - E_{\mathfrak{m}}(0,0,g,s)).$$

Proof. We have to show that the limit exists on the right hand side and it equals to the left hand side. For all complex s with $\mathrm{Re}(s) > 1$ we have:

$$E_{\mathfrak{m}}(\alpha,\beta,g,s) - E_{\mathfrak{m}}(0,0,g,s) = \\ |\det(g)|^s \sum_{n=-\infty}^{\infty} (|V_{\mathfrak{m}}(\alpha,\beta,g,n)| - |V_{\mathfrak{m}}(0,0,g,n)|)\,|\pi|^{2sn}.$$

According to the proof of Proposition 4.3 the cardinalities $|V_{\mathfrak{m}}(\alpha,\beta,g,n)|$ and $|V_{\mathfrak{m}}(0,0,g,n)|$ are zero if n is sufficiently small. Let (α,β) again denote an element of $W_{\mathfrak{m}}(\alpha,\beta,g_f)$ by abuse of notation as in the proof of Lemma 4.5. The map $f \mapsto (\alpha,\beta)+f$ defines a bijection between $V_{\mathfrak{m}}(0,0,g,n)$ and $V_{\mathfrak{m}}(\alpha,\beta,g,n)$ if n is sufficiently large, so the limit exists and

$$\lim_{s \to 0^+} (E_{\mathfrak{m}}(\alpha,\beta,g,s) - E_{\mathfrak{m}}(0,0,g,s)) = \\ \lim_{N \to \infty} \left(\sum_{n \leq N} |V_{\mathfrak{m}}(\alpha,\beta,g,n)| - |V_{\mathfrak{m}}(0,0,g,n)| \right).$$

The claim now follows from the previous proposition. $\square$

5. Computation of Fourier expansions

Definition 5.1. For every $\alpha \in \mathcal{O}_f/\mathfrak{m}$ and $z \in \mathbb{A}_f^*$ let

$$V_{\mathfrak{m}}(\alpha, z) = \{u \in F^* | uz \in \alpha + \mathfrak{m}\}.$$

For each α and z as above let $\zeta_{\mathfrak{m}}(\alpha, z, s)$ denote the $\mathbb{C}$-valued function

$$\zeta_{\mathfrak{m}}(\alpha, z, s) = \sum_{u \in V_{\mathfrak{m}}(\alpha, z)} |u|_{\infty}^{-s},$$

if this infinite sum is absolutely convergent. For every $\alpha \in \mathcal{O}_f/\mathfrak{m}$ define $\rho(\alpha)$ to be 1, if $\alpha = 0$, and to be 0, otherwise. Let μ be the unique Haar measure on the locally compact abelian topological group $\mathbb{A}$ such that $\mu(\mathcal{O})$ is equal to $|\mathfrak{d}|^{-1/2}$. Since this measure is left-invariant with respect to the discrete subgroup F by definition, it induces a measure on $F\backslash\mathbb{A}$ which will be denoted by the same letter by abuse of notation. By our choice of normalization $\mu(F\backslash\mathbb{A}) = 1$, so our notation is compatible with Definitions 2.3 and 2.8. Note that the former is the direct product of a Haar measure μ_f on $\mathbb{A}_f$ and a Haar measure μ_∞ on F_∞ such that $\mu_f(\mathcal{O}_f) = |\mathfrak{d}|^{-1/2}$ and $\mu_\infty(\mathcal{O}_\infty) = 1$. Finally let q_∞ be the cardinality of $\mathbf{f}_\infty$.

Proposition 5.2. *For each complex s with* $\mathrm{Re}(s) > 1$ *we have:*

$$\begin{aligned} E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^0(z) =& \rho(\alpha)|z|^s \zeta_{\mathfrak{m}}(\beta, 1, 2s) \\ &+ \frac{|\mathfrak{m}|}{|\mathfrak{d}|^{1/2}} \frac{|z|^s (q_\infty - 1)}{|z|_\infty^{2s-1}(q_\infty^{2s} - q_\infty)} \zeta_{\mathfrak{m}}(\alpha, z_f, 2s-1). \end{aligned}$$

Proof. Recall that the notion of Fourier coefficients are defined for all complex-valued automorphic forms (see [19]). The claim above should be understood in this sense. By grouping the terms in the infinite sum of Definition 4.2 we get the following identity:

$$E_{\mathfrak{m}}(\alpha, \beta, \begin{pmatrix} z & x \\ 0 & 1 \end{pmatrix}, s) = |z|^s \sum_{(0,u) \in V_{\mathfrak{m}}(\alpha, \beta, \begin{pmatrix} z & x \\ 0 & 1 \end{pmatrix})} |u|_\infty^{-2s} + |z|^s \sum_{b \in F} \sum_{\substack{a \in F^* \\ (a,0) \in V_{\mathfrak{m}}(\alpha, \beta, \begin{pmatrix} z & x+b \\ 0 & 1 \end{pmatrix})}} |a(x+b)|_\infty^{-2s}.$$

According to the Fourier inversion formula the Fourier coefficient $E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^0(z)$ is given by the formula

$$E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^0(z) = \int_{F\backslash\mathbb{A}} E_{\mathfrak{m}}(\alpha, \beta, \begin{pmatrix} z & x \\ 0 & 1 \end{pmatrix}, s) \mathrm{d}\mu(x).$$

By substituting the formula above into this integral and interchanging summation and integration we get:

$$E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^0(z) = \rho(\alpha)|z|^s \zeta_{\mathfrak{m}}(\beta, 1, 2s) + |z|^s \sum_{a \in V_{\mathfrak{m}}(\alpha, z)} |a|_\infty^{-2s} \int_{\substack{a \in V_{\mathfrak{m}}(\beta, x_f) \\ |x|_\infty > |z|_\infty}} |x|_\infty^{-2s} \mathrm{d}\mu(x).$$

Note that this computation is justified by the Lebesgue convergence theorem. The measure of the set $\{x \in \mathbb{A}_f | a \in V_{\mathfrak{m}}(\beta, x)\}$ is:

$$\begin{aligned}\mu_f(\{x \in \mathbb{A}_f | a \in V_{\mathfrak{m}}(\beta, x)\}) =& \mu_f(a_f^{-1}(\beta + \mathfrak{m})) \\ =& |a_f|^{-1}|\mathfrak{m}||\mathfrak{d}|^{-1/2} = |a|_\infty |\mathfrak{m}||\mathfrak{d}|^{-1/2}.\end{aligned}$$

On the other hand:

$$\begin{aligned}\int_{|x|_\infty > |z|_\infty} |x|_\infty^{-2s} \mathrm{d}\mu_\infty(x) =& \sum_{n=1}^{\infty} |z|_\infty^{-2s} q_\infty^{-2sn} \int_{\infty(x)=\infty(z)-n} \mathrm{d}\mu_\infty(x) \\ =& \sum_{n=1}^{\infty} |z|_\infty^{1-2s} q_\infty^{(1-2s)n} \cdot \frac{q_\infty - 1}{q_\infty},\end{aligned}$$

so the second term in the sum above is equal to:

$$|z|^s |\mathfrak{m}||\mathfrak{d}|^{-1/2} |z|_\infty^{1-2s} \cdot \frac{q_\infty - 1}{q_\infty^{2s} - q_\infty} \cdot \sum_{a \in V_{\mathfrak{m}}(\alpha, z)} |a|_\infty^{1-2s}. \ \square$$

DEFINITION 5.3. For every $\alpha \in \mathcal{O}_f/\mathfrak{m}$ and $z \in \mathbb{A}_f^*$ let

$$S_{\mathfrak{m}}(\alpha, z) = \{u \in V_{\mathfrak{m}}(\alpha, z) | u_f^{-1}\mathfrak{m}\mathcal{O}_f \subseteq \mathfrak{d}\}.$$

For each $\beta \in \mathcal{O}_f/\mathfrak{m}$ and α, z as above let $\sigma_{\mathfrak{m}}(\alpha, \beta, z, s)$ denote the finite $\mathbb{C}$-valued sum

$$\sigma_{\mathfrak{m}}(\alpha, \beta, z, s) = \sum_{u \in S_{\mathfrak{m}}(\alpha, z)} \tau(-u_f^{-1}\beta)|u|_\infty^{-s},$$

where $\beta \in \mathcal{O}_f$ also denotes a representative of the class β by abuse of notation. The expression above is well-defined because of the condition $u_f^{-1}\mathfrak{m}\mathcal{O}_f \subseteq \mathfrak{d}$.

PROPOSITION 5.4. *For each complex s with $\mathrm{Re}(s) > 1$ we have:*

$$E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^*(z\mathfrak{d}^{-1}) =$$
$$\Big(-q_\infty^{2s} + \frac{q_\infty - 1}{q_\infty} \cdot \sum_{n=0}^{\infty(z)-1} q_\infty^{n(2s-1)}\Big)|z|^s \frac{|\mathfrak{m}|}{|\mathfrak{d}|^{1/2}} \sigma_{\mathfrak{m}}(\alpha, \beta, z_f, 2s-1),$$

if $\infty(z) \geq 0$, and it is zero, otherwise.

PROOF. The first summand in the right hand side of the first equation appearing in the proof above is constant in x, so it does not contribute to the Fourier coefficient $E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^*(z\mathfrak{d}^{-1})$. Hence

$$\begin{aligned}E_{\mathfrak{m}}(\alpha, \beta, \cdot, s)^*(z\mathfrak{d}^{-1}) =& \int_{F\backslash\mathbb{A}} E_{\mathfrak{m}}(\alpha, \beta, \begin{pmatrix} z & x \\ 0 & 1 \end{pmatrix}, s)\tau(-x)\mathrm{d}\mu(x) \\ =& |z|^s \sum_{a \in V_{\mathfrak{m}}(\alpha, z)} |a|_\infty^{-2s} \int_{\substack{a \in V_{\mathfrak{m}}(\beta, x_f) \\ |x|_\infty > |z|_\infty}} |x|_\infty^{-2s} \tau(-x)\mathrm{d}\mu(x).\end{aligned}$$

interchanging summation and integration. For every $a \in V_{\mathfrak{m}}(\alpha, z)$ the integral above is a product:

$$\int\limits_{\substack{x_f \in a_f^{-1}(\beta+\mathfrak{m})\\ |x|_\infty > |z|_\infty}} |x|_\infty^{-2s}\tau(-x)\mathrm{d}\mu(x) =$$

$$\tau(-a_f^{-1}\beta) \cdot \int\limits_{a_f^{-1}\mathfrak{m}\mathcal{O}_f} \tau(-x)\mathrm{d}\mu_f(x) \cdot \int\limits_{|x|_\infty > |z|_\infty} |x|_\infty^{-2s}\tau_\infty(-x)\mathrm{d}\mu_\infty(x),$$

where τ_∞ is the restriction of the character τ to the ∞-adic component F_∞. The first integral in the product above is zero unless additive group $a_f^{-1}\mathfrak{m}\mathcal{O}_f$ lies in the kernel of τ which is equivalent to $a \in S_{\mathfrak{m}}(\alpha, z)$. In the latter case it is equal to $\mu_f(a_f^{-1}\mathfrak{m}\mathcal{O}_f) = |a|_\infty |\mathfrak{m}||\mathfrak{d}|^{-1/2}$. By assumption $\mathcal{O}_\infty$ itself is the largest $\mathcal{O}_\infty$-submodule of F_∞ such that the restriction of τ_∞ onto this submodule is trivial, hence the integral on the right above is zero if $\infty(z) < 0$, and it is equal to:

$$\int\limits_{|x|_\infty > |z|_\infty} |x|_\infty^{-2s}\tau_\infty(-x)\mathrm{d}\mu_\infty(x) = \sum_{n=-1}^{\infty(z)-1} \int\limits_{\infty(x)=n} |x|_\infty^{-2s}\tau_\infty(-x)\mathrm{d}\mu_\infty(x)$$

$$= -q_\infty^{2s} + \frac{q_\infty - 1}{q_\infty} \cdot \sum_{n=0}^{\infty(z)-1} q_\infty^{n(2s-1)}, \text{ otherwise. } \square$$

Definition 5.5. Let $A = \mathcal{O}_f \cap F$: it is a Dedekind domain. The ideals of A and the effective divisors on X with support away from ∞ are in a bijective correspondence. These two sets will be identified in all that follows. For any ideal $\mathfrak{n} \triangleleft A$ let $Y_0(\mathfrak{n})$ denote the coarse moduli for rank two Drinfeld modules of general characteristic equipped with a Hecke level-$\mathfrak{n}$ structure. It is an affine algebraic curve defined over F. The group $GL_2(F)$ acts on the product $GL_2(\mathbb{A}_f) \times \Omega$ on the left by acting on the first factor via the natural embedding and on Drinfeld's upper half plane via Möbius transformations. The group $\mathbb{K}_f(\mathfrak{n}) = \mathbb{K}_0(\mathfrak{n}) \cap GL_2(\mathcal{O}_f)$ acts on the right of this product by acting on the first factor via the regular action. Since the quotient set $GL_2(F)\backslash GL_2(\mathbb{A}_f)/\mathbb{K}_f(\mathfrak{n})$ is finite, the set

$$GL_2(F)\backslash GL_2(\mathbb{A}_f) \times \Omega/\mathbb{K}_f(\mathfrak{n})$$

is the disjoint union of finitely many sets of the form $\Gamma\backslash\Omega$, where Γ is a subgroup of $GL_2(F)$ of the form $GL_2(F) \cap g\mathbb{K}_f(\mathfrak{n})g^{-1}$ for some $g \in GL_2(\mathbb{A}_f)$. As these groups act on Ω discretely, the set above naturally has 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 5.6. *There is a rigid-analytical isomorphism:*

$$Y_0(\mathfrak{n}) \cong GL_2(F)\backslash GL_2(\mathbb{A}_f) \times \Omega/\mathbb{K}_f(\mathfrak{n}).$$

Proof. See [3], Theorem 6.6. □

Notation 5.7. From now on we make the same assumptions as we did in Remark 3.7. In this case $A = \mathbb{F}_q[T]$. If $\psi : A \longrightarrow \mathbb{C}_\infty\{\tau\}$ is a Drinfeld module of rank two over A, then

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

where Δ is the Drinfeld discriminant function. It is a Drinfeld modular form of weight q^2-1. Under the identification of Theorem 5.6 the Drinfeld discriminant function Δ is a nowhere vanishing function on $GL_2(\mathbb{A}_f) \times \Omega$ holomorphic in the second variable, and it is equal to:

$$\Delta(g,z) = \prod_{(0,0)\neq(\alpha,\beta)\in\mathcal{O}_f^2/T\mathcal{O}_f^2} \epsilon_{(T)}(\alpha,\beta)(g,z)$$

which is an immediate consequence of the uniformization theory of Drinfeld modules over $\mathbb{C}_\infty$. For every ideal $\mathfrak{n} = (n) \lhd A$ let $\Delta_{\mathfrak{n}}$ denote the modular form of weight q^2-1 given by the formula $\Delta_{\mathfrak{n}}(g,z) = \Delta(g\left(\begin{smallmatrix} n^{-1} & 0 \\ 0 & 1\end{smallmatrix}\right), z)$. As the notation indicates $\Delta_{\mathfrak{n}}$ is independent of the choice of the generator $n \in \mathfrak{n}$. Finally let $E_{\mathfrak{n}} = r(\Delta/\Delta_{\mathfrak{n}})$. Since $\Delta/\Delta_{\mathfrak{n}}$ is a modular form of weight zero, i.e. it is a modular unit, the function $E_{\mathfrak{n}}$ is a $\mathbb{Z}$-valued harmonic form of level $\mathfrak{n}\infty$.

Proposition 5.8. *If T does not divide n then we have:*

$$E^0_{\mathfrak{n}}(1) = (q-1)q(q^{\deg(\mathfrak{n})}-1) \text{ and } E^*_{\mathfrak{n}}(1) = \frac{(q^2-1)(q-1)}{q}.$$

Proof. Every $\alpha \in \mathcal{O}_f/T\mathcal{O}_f$ is represented by a unique element of the constant field $\mathbb{F}_q$, which will be denoted by the same symbol by abuse of notation. For all such α and $z \in \mathbb{F}_q[T] \subset \mathbb{A}_f^*$ with $T\not| z$ we have:

$$\zeta_{(T)}(\alpha, z^{-1}, s) = \sum_{\substack{0\neq p\in\mathbb{F}_q[T] \\ p\equiv\alpha z \bmod (zT)}} q^{-s\deg(p)}.$$

Because $p \equiv \alpha z \bmod (zT)$ holds if and only if there is a $r \in \mathbb{F}_q[T]$ with $p = \alpha z + zTr$, we have $\deg(p) = \deg(z)+1+\deg(r)$ in this case, unless $r=0$ and $p = \alpha z$. Therefore

$$\begin{aligned}\zeta_{(T)}(\alpha, z^{-1}, s) =& (1-\rho(\alpha))q^{-s\deg(z)} + \sum_{k=0}^{\infty}(q-1)q^k q^{-s(\deg(z)+1+k)} \\ =& (1-\rho(\alpha))q^{-s\deg(z)} + \frac{(q-1)q^{-s(\deg(z)+1)}}{1-q^{1-s}}.\end{aligned}$$

For every $z \in \mathbb{F}_q[T]$ let z denote the unique idele whose finite component is z and its infinite component is 1, by abuse of notation. An immediate consequence of this equation and Proposition 5.2 is that the function $E_{(T)}(\alpha,\beta,\cdot,s)^0(z^{-1})$, originally defined for $\mathrm{Re}(s) > 1$ only, has a meromorphic continuation to the whole complex plane and

$$\lim_{s\to 0} E_{(T)}(\alpha,\beta,\cdot,s)^0(z^{-1}) = -\rho(\alpha)\rho(\beta) - q^{\deg(z)}(\frac{1}{q+1} - \rho(\alpha)),$$

using the fact that divisor of $\mathfrak{d}$ is in the anticanonical class, hence its degree is two. On the other hand the Limit Formula 4.8 and the description in Notation 5.7 implies that:

$$\begin{aligned} E^0_{\mathfrak{n}}(1) = & \sum_{(0,0)\neq(\alpha,\beta)\in\mathbb{F}_q^2} \lim_{s\longrightarrow 0}(E_{(T)}(\alpha,\beta,\cdot,s)^0(1) - E_{(T)}(\alpha,\beta,\cdot,s)^0(n^{-1})) \\ & -(q^2-1)\lim_{s\longrightarrow 0}(E_{(T)}(0,0,\cdot,s)^0(1) - E_{(T)}(0,0,\cdot,s)^0(n^{-1})) \\ = & \sum_{(0,0)\neq(\alpha,\beta)\in\mathbb{F}_q^2}(q^{\deg(n)}-1)(1-\rho(\alpha)) = (q-1)q(q^{\deg(\mathfrak{n})}-1). \end{aligned}$$

By Proposition 5.4 the function $E_{(T)}(\alpha,\beta,\cdot,s)^*(1)$ is a meromorphic function and:

$$E_{(T)}(\alpha,\beta,\cdot,0)^*(1) = -\sigma_{(T)}(\alpha,\beta,\mathfrak{d},-1).$$

By choosing an appropriate character τ, we may assume that $\mathfrak{d}$ any divisor of degree two, as every such divisor is linearly equivalent to the anticanonical class. In particular we may assume that $\mathfrak{d} = T_f^2$, which is in accordance with our previous assumptions. In this case:

$$S_{(T)}(\alpha,\mathfrak{d}) = \{0 \neq p \in \mathbb{F}_q(T) | pT^2 \in \alpha + T\mathbb{F}_q[T], p^{-1} \in T\mathbb{F}_q[T]\},$$

which is the one element set $\{\alpha T^{-2}\}$, if α is non-zero, and it is $\{\gamma T^{-1} | \gamma \in \mathbb{F}_q^*\}$, otherwise. Hence:

$$\sigma_{(T)}(\alpha,\beta,\mathfrak{d},-1) = \begin{cases} \frac{1}{q^2} & \text{, if } \alpha \neq 0, \\ -\frac{1}{q} & \text{, if } \alpha = 0 \text{ and } \beta \neq 0, \\ \frac{q-1}{q} & \text{, if } \alpha = 0 \text{ and } \beta = 0, \end{cases}$$

where in the second case we used the fact that the character is non-trivial on the set of elements $\gamma^{-1}\beta T$, where $\gamma \in \mathbb{F}_q^*$. As all Fourier coefficients $E_{(T)}(\alpha,\beta,\cdot,s)^*(n^{-1})$ are zero, because the divisor n^{-1} is not effective, we get:

$$\begin{aligned} E^*_{\mathfrak{n}}(1) = & -\sum_{(0,0)\neq(\alpha,\beta)\in\mathbb{F}_q^2} \sigma_{(T)}(\alpha,\beta,\mathfrak{d},-1) + (q^2-1)\sigma_{(T)}(0,0,\mathfrak{d},-1) \\ = & \frac{(q^2-1)(q-1)}{q}. \ \square \end{aligned}$$

Remark 5.9. The modular form $\Delta_{\mathfrak{n}}$ coincides with the function defined by Gekeler (see for example [8]), which can be seen by passing from the adelic description to the usual one. The result above is also proved in [8], but the argument applied there, unlike ours, can not be easily generalized. In particular the description of the quotient of the Bruhat-Tits tree by the full modular group (Proposition 3.9) is used which has no analogue in general.

6. Cuspidal harmonic forms annihilated by the Eisenstein ideal

Definition 6.1. Let $\mathfrak{n}$ be any ideal of A and let $H \subset GL_2(\mathbb{A}_f)$ be a compact double $\mathbb{K}_f(\mathfrak{n})$-coset. It is a disjoint union of finitely many right $\mathbb{K}_f(\mathfrak{n})$-cosets. Let R be a set of representatives of these cosets. For any function $u : GL_2(\mathbb{A}_f) \times \Omega \to \mathbb{C}_\infty^*$ holomorphic in the second variable for each $g \in GL_2(\mathbb{A}_f)$, we define the function $T_H(u)$ by the formula:

$$T_H(u)(g) = \prod_{h \in R} u(gh).$$

If we assume that u is right $\mathbb{K}_f(\mathfrak{n})$-invariant then the function $T_H(u)$ is independent of the choice of R and $T_H(u)$ is holomorphic in the second variable for each $g \in GL_2(\mathbb{A}_f)$ as well. Moreover we have the identity:

$$r(T_H(u)) = T_H(r(u)),$$

where T_H also denotes the similarly defined linear operator on the set of right $\mathbb{K}_0(\mathfrak{n}\infty)$-invariant functions on $GL_2(\mathbb{A})$, slightly extending Definition 3.1. Let the symbol $T_{\mathfrak{m}}$ denote the operator T_H, if $H = H(\mathfrak{m}, \mathfrak{n}\infty) \cap GL_2(\mathbb{A}_f)$, where $\mathfrak{m} \triangleleft A$. Since we may choose the representative system $R(\mathfrak{m}, \mathfrak{n}\infty)$ to be a subset of $GL_2(\mathbb{A}_f)$, our new notation is compatible with the old one introduced in 3.1. Finally let $\mathfrak{p}$ be a prime ideal of A, and let $\pi \in \mathbb{A}_f^*$ be an idele such that $\pi \mathcal{O}_f = \mathfrak{p}$. The matrix $\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} \in GL_2(\mathbb{A}_f)$ introduced in the proof of Proposition 3.10 normalizes the subgroup $\mathbb{K}_0(\mathfrak{p}\infty)$, hence its double $\mathbb{K}_0(\mathfrak{n}\infty)$-coset as well as its double $\mathbb{K}_f(\mathfrak{n})$-coset consist of only one right coset. Let $W_{\mathfrak{p}}$ denote the corresponding operator.

The following lemma is also proved in [8], but we believe that our proof is simpler, and in a certain sense more revealing.

Lemma 6.2. *We have:*

$$W_{\mathfrak{p}}(E_{\mathfrak{p}}) = -E_{\mathfrak{p}} \text{ and } T_{\mathfrak{q}}(E_{\mathfrak{p}}) = (1 + q^{\deg(\mathfrak{q})})E_{\mathfrak{p}}$$

for every prime ideal $\mathfrak{q} \triangleleft A$ different from $\mathfrak{p}$. Moreover $E_{\mathfrak{p}}$ is an eigenvector of every Hecke operator $T_{\mathfrak{m}}$, with integral eigenvalue.

Proof. By the discussion above it is sufficient to prove the same for the modular unit $\Delta/\Delta_{\mathfrak{p}}$, up to a non-zero constant, because the van der Put derivative is zero on constant functions. Under the identification of Theorem 5.6 the modular unit $\Delta/\Delta_{\mathfrak{p}}$ corresponds to a nowhere zero rational function on the affine curve $Y_0(\mathfrak{p})$. The action of the operators $W_{\mathfrak{p}}$ and $T_{\mathfrak{m}}$ is just the usual action induced by the Atkin-Lehmer involution and the Hecke correspondence $T_{\mathfrak{m}}$, respectively. (See [6] for their definition and properties in this setting). The latter extend to correspondences on $X_0(\mathfrak{p})$, the unique non-singular projective curve which contains $Y_0(\mathfrak{p})$ as an open subvariety. The complement of $Y_0(\mathfrak{p})$ in $X_0(\mathfrak{p})$ consists of two geometric points, the cusps. These correspondences leave the group of divisors supported on the cusps invariant. In particular, the Atkin-Lehmer involution interchanges these two points, while the Hecke correspondence $T_{\mathfrak{q}}$, where $q \triangleleft A$ is a prime ideal different from $\mathfrak{p}$, maps them into themselves with multiplicity $1+q^{\deg(\mathfrak{q})}$. Since every nowhere zero rational function on the affine curve $Y_0(\mathfrak{p})$ is uniquely determined, up to a non-zero constant, by its divisor, which is of degree zero and is supported on the cusps, the claim now follows at once. □

Proposition 6.3. *A harmonic form $\phi \in \mathcal{H}(\mathfrak{p}, R)$ is cuspidal if any only if the integrals:*

$$\phi^0(1) = \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix})d\mu(x) \text{ and}$$
$$\phi^\infty(1) = \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix})d\mu(x)$$

are both zero.

Proof. The condition is clearly necessary. Also note that $\phi^\infty(1) = W_{\mathfrak{p}}(\phi)^0(1)$ for every $\phi \in \mathcal{H}(\mathfrak{p}, R)$, so the condition does not depend on the particular choice of π. In particular we may assume that all components π_v, where $v \triangleleft A$ is different from $\mathfrak{p}$, are actually equal to one. If we want to show that it is sufficient, we need to show that the integral

$$c(g, \phi) = \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g)d\mu(x)$$

is zero for every $g \in GL_2(\mathbb{A})$, if ϕ satisfies the condition of the claim. In order to do so, we first prove the lemma below. Let υ be a uniformizer in F_∞, as in Definition 3.4.

Lemma 6.4. *For every $g \in GL_2(\mathbb{A})$ and $\phi \in \mathcal{H}(\mathfrak{p}, R)$ the following holds:*

(*i*) *we have $c(g, \phi) = c(\gamma gkz, \phi)$, if $\gamma \in P(F)U(\mathbb{A})$, $k \in \mathbb{K}_0(\mathfrak{p}\infty)$ and $z \in Z(\mathbb{A})$,*

(*ii*) *we have $c(g, \phi) = -c(g\left(\begin{smallmatrix} 0 & 1 \\ \upsilon & 0 \end{smallmatrix}\right), \phi)$,*

(*iii*) *we have $c(g, \phi) = |\infty|^{-1}c(g\left(\begin{smallmatrix} \upsilon & 0 \\ 0 & 1 \end{smallmatrix}\right), \phi)$, if $g_\infty \in B(F_\infty)$.*

Proof. We first show (i). If $\gamma = \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, then:

$$\begin{aligned} c(\gamma gkz, \phi) &= \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma g) \mathrm{d}\mu(x) \\ &= \int_{F\backslash\mathbb{A}} \phi(\gamma \begin{pmatrix} 1 & \alpha^{-1}x \\ 0 & 1 \end{pmatrix} g) \mathrm{d}\mu(x) = c(g, \phi), \end{aligned}$$

using the right $\mathbb{K}_0(\mathfrak{p}\infty)Z(\mathbb{A})$-invariance and the left $GL_2(F)$-invariance of ϕ, as well as the fact that the map $x \mapsto \alpha^{-1}x$ leaves the Haar-measure μ of the group $F\backslash\mathbb{A}$ invariant for every $\alpha \in F^*$. Claim (ii) is an immediate consequence of the first condition in Definition 3.4. Assume now that $g_\infty = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. The final claim follows from the computation:

$$\begin{aligned} c(g, \phi) = c(g, T_\infty(\phi)) &= \sum_{\epsilon \in \mathbf{f}_\infty} \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \upsilon & 0 \\ 0 & 1 \end{pmatrix}) \mathrm{d}\mu(x) \\ &= \sum_{\epsilon \in \mathbf{f}_\infty} \int_{F\backslash\mathbb{A}} \phi(\begin{pmatrix} 1 & x + \frac{a}{c}\epsilon \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} \upsilon & 0 \\ 0 & 1 \end{pmatrix}) \mathrm{d}\mu(x) \\ &= \frac{1}{|\infty|} c(g \begin{pmatrix} \upsilon & 0 \\ 0 & 1 \end{pmatrix}, \phi), \end{aligned}$$

where we used Lemma 3.5. □

Let us return to the proof of Proposition 6.3. By the Iwasawa decomposition we may write g as a product bk, where $b \in B(\mathbb{A})$ and $k \in GL_2(\mathcal{O})$. We may assume that b is a diagonal matrix with 1 in the lower left corner by multiplying g by a suitable element of $U(\mathbb{A})Z(\mathbb{A})$ on the left, according to Lemma 6.4. We may also assume that k_v is the identity matrix for all $v \in |X|$, different from $\mathfrak{p}$ and ∞, by multiplying g by a suitable element of $\mathbb{K}_0(\mathfrak{p}\infty)$ on the right, using again Lemma 6.4. Since A has class number 1, the equality $F^*\mathcal{O}_f^* = \mathbb{A}_f^*$ holds, hence we may even assume that g_v is the identity matrix for all $v \in |X|$, different from $\mathfrak{p}$ and ∞, by multiplying g by a suitable diagonal element of $GL_2(F)$ on the left and of $\mathbb{K}_0(\mathfrak{p}\infty)$ on the right. Moreover $GL_2(F_\infty) = B(F_\infty)\Gamma_\infty \cup B(F_\infty) \begin{pmatrix} 0 & 1 \\ \upsilon & 0 \end{pmatrix} \Gamma_\infty$, hence claim (ii) of the lemma above implies that we may assume that g_∞ is a diagonal matrix with some power of υ in the upper right corner and 1 in the lower left corner, also repeating some of the arguments above. In this case (iii) of Lemma 6.4 can be used to reduce to the case when g_∞ is the identity matrix, too. Using the decomposition $GL_2(F_\mathfrak{p}) = B(F_\mathfrak{p})\Gamma_\mathfrak{p} \cup B(F_\mathfrak{p}) \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} \Gamma_\mathfrak{p}$, where $\Gamma_\mathfrak{p} = \mathbb{K}_0(\mathfrak{p}\infty)_\mathfrak{p}$ is the Iwahori subgroup in $GL_2(F_\mathfrak{p})$, the same logic implies that $g_\mathfrak{p}$ may be assumed to be either the identity matrix or $\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$. The proof is now complete. □

Definition 6.5. Let $\mathcal{E}_0(\mathfrak{p}, R)$ be the R-submodule of $\mathcal{H}_0(\mathfrak{p}, R)$ of those cuspidal harmonic forms ϕ such that $T_\mathfrak{q}(\phi) = (1 + q^{\deg(\mathfrak{q})})\phi$ for each closed point

$\mathfrak{q}$ of X, different from $\mathfrak{p}$ and ∞. By Theorem 3.12 the R-module $\mathcal{E}_0(\mathfrak{p},R)$ is isomorphic to an ideal $\mathfrak{a}\lhd R$ via the map $\phi\mapsto\phi^*(1)$. Let $d=\deg(\mathfrak{p})$ denote the degree of $\mathfrak{p}$.

Theorem 6.6. *For every coefficient ring R the map*

$$\mathcal{E}_0(\mathfrak{p},R)\rightarrow R,\quad \phi\mapsto\phi^*(1)$$

is an isomorphism onto $R[N(\mathfrak{p})]$, if d is odd, and is an isomorphism onto $R[2N(\mathfrak{p})]$, if d is even.

Proof. Define the harmonic form $e_\mathfrak{p}\in\mathcal{H}(\mathfrak{p},\mathbb{Z}\langle\frac{1}{q^2-1}\rangle)$ by the formula:

$$e_\mathfrak{p}=\begin{cases}\frac{E_\mathfrak{p}}{(q-1)^2} & \text{, if } d \text{ is odd,}\\ \frac{E_\mathfrak{p}}{(q-1)^2(q+1)} & \text{, if } d \text{ is even.}\end{cases}$$

For every $\alpha\in R[q+1]$ let $H(\alpha)$ again denote the unique R-valued harmonic form of level ∞ with $H(\alpha)^0(1)=\alpha$, just as in the proof of Proposition 3.8. First we are going to show the following

Lemma 6.7. *The harmonic form $e_\mathfrak{p}$ is integer-valued.*

Proof. By Proposition 5.8 we have $e^0_\mathfrak{p}(1)=N(\mathfrak{p})$ and $e^*_\mathfrak{p}(1)=\frac{q+1}{q}$, if d is odd, and $e^*_\mathfrak{p}(1)=\frac{1}{q}$, if d is even. By Lemma 6.2 the form $e_\mathfrak{p}$ is also an eigenvector for the Hecke operator $T_\mathfrak{m}$, where where $\mathfrak{m}$ is any prime ideal of A, with integral eigenvalue. Hence $e^*_\mathfrak{p}(\mathfrak{m})\in\mathbb{Z}\langle\frac{1}{q}\rangle$ for any effective divisor $\mathfrak{m}$, arguing the same way as we did in the proof of Corollary 3.3. Moreover $e^0_\mathfrak{p}(y)\in\mathbb{Z}\langle\frac{1}{q}\rangle$ for any $y\in\mathbb{A}^*$ using that $\mathrm{Pic}(X)=\mathbb{Z}$ via the degree map and part *(iii)* of Lemma 6.4. The Fourier expansion formula (Proposition 2.10) implies that we must have $e_\mathfrak{p}\in\mathcal{H}(\mathfrak{p},\mathbb{Z}\langle\frac{1}{q}\rangle)$, hence $e_\mathfrak{p}$ is an integer valued harmonic form. $\square$

Let $e_\mathfrak{p}$ denote the image of this harmonic form in $\mathcal{H}(\mathfrak{p},R)$ for any coefficient ring R with respect to the functorial homomorphism $\mathcal{H}(\mathfrak{p},\mathbb{Z})\rightarrow\mathcal{H}(\mathfrak{p},R)$, by abuse of notation.

Lemma 6.8. *For any $\alpha\in R[q+1]$ and $\beta\in R$ the harmonic form $H(\alpha)+\beta e_\mathfrak{p}$ lies in $\mathcal{E}_0(\mathfrak{p},R)$ if and only if the equations $\alpha=-\beta N(\mathfrak{p})$ and $\alpha=(-1)^d\beta N(\mathfrak{p})$ hold.*

Proof. By Lemma 6.2 the form $e_\mathfrak{p}$ is an eigenvector for the Hecke operator $T_\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal different from $\mathfrak{p}$, with $q^{\deg(\mathfrak{q})}+1$ as eigenvalue. The degree of the determinant of every element of the set $R(\mathfrak{q},\mathfrak{p}\infty)$ is $\deg(\mathfrak{q})$ for every $\mathfrak{q}$ prime of A different from $\mathfrak{p}$, hence $T_\mathfrak{q}(H(\alpha))^0(1)=(q^{\deg(\mathfrak{q})}+1)(-1)^{\deg(\mathfrak{q})}\alpha$. If $\deg(\mathfrak{q})$ is odd, then $q+1$ divides $q^{\deg(\mathfrak{q})}+1$, hence the expression above is equal to $0=(q^{\deg(\mathfrak{q})}+1)\alpha$ in this case. In particular $H(\alpha)$ is an eigenvector for the Hecke operator $T_\mathfrak{q}$ with $q^{\deg(\mathfrak{q})}+1$ as eigenvalue, too. Therefore it is sufficient to prove that $H(\alpha)+\beta e_\mathfrak{p}\in\mathcal{H}_0(\mathfrak{p},R)$ if and only if the equations hold in the claim above. Note that $H(\alpha)^{\infty}(1) = (-1)^d\alpha$, as every matrix of the form $\begin{pmatrix} \pi x & 1 \\ \pi & 0 \end{pmatrix}$ has determinant π, which has degree d. By Lemma 6.2 we have $W_{\mathfrak{p}}(e_{\mathfrak{p}}) = -e_{\mathfrak{p}}$, hence $e^{\infty}_{\mathfrak{p}}(1) = -e^0_{\mathfrak{p}}(1) = -N(\mathfrak{p})$. The claim now follows from Proposition 6.3. □

Let's start the proof proper of Theorem 6.6. First assume that d is even. In this case every $\phi \in \mathcal{E}_0(\mathfrak{p}, R)$ can be written uniquely of the form $\phi = q\phi^*(1)e_{\mathfrak{p}} + H(\alpha)$, for some $\alpha \in R[q+1]$. By Lemma 6.8 we must have $N(\mathfrak{p})\phi^*(1) = \alpha/q = -\alpha/q$, hence $2N(\mathfrak{p})\phi^*(1) = 0$. On the other hand let $\beta \in R[2N(\mathfrak{p})]$ be arbitrary. First note that $R[2] \subseteq R[q+1]$. If q is even, then 2 is invertible in R, hence $R[2] = 0$. If q is odd, then 2 divides $q+1$, hence $R[2] \subseteq R[q+1]$. Therefore $\alpha = qN(\mathfrak{p})\beta \in R[q+1]$, so $H(\alpha)$ is well-defined. By Lemma 6.8 we have $q\beta e_{\mathfrak{p}} + H(\alpha) \in \mathcal{E}_0(\mathfrak{p}, R)$, and its image under the map of the claim is β. Now assume that d is odd. Let $\tilde{R}$ be a discrete valuation ring and let $\mathfrak{a} \lhd \tilde{R}$ be an ideal such that $R = \tilde{R}/\mathfrak{a}$. Define the coefficient ring R' as the quotient $\tilde{R}/(q+1)\mathfrak{a}$. The map $R \to R'$ given by the rule $x \mapsto (q+1)x$ maps bijectively onto the ideal $(q+1) \lhd R'$. In particular for every $\phi \in \mathcal{E}_0(\mathfrak{p}, R)$ we have $(q+1)\phi \in \mathcal{E}_0(\mathfrak{p}, R')$, and the latter can be written of the form $(q+1)\phi = q\beta e_{\mathfrak{p}} + H(\alpha)$, for some $\alpha \in R'[q+1]$ and $\beta \in R'$ which maps to $\phi^*(1)$ under the canonical surjection $R' \to R$. Applying Lemma 6.8 the the coeffient ring R' we get that we must have $N(\mathfrak{p})\beta = -\alpha/q$, hence $(q+1)N(\mathfrak{p})\beta = 0$. The latter is equivalent to $\phi^*(1) \in R[N(\mathfrak{p})]$. On the other hand let $\beta \in R[N(\mathfrak{p})]$ be arbitrary. For any lift $\beta' \in R'$ with respect to the natural surjection we have $\beta' \in R'[(q+1)N(\mathfrak{p})]$. Therefore $\alpha = -qN(\mathfrak{p})\beta' \in R'[q+1]$, so $H(\alpha)$ is well-defined. By Lemma 6.8 we have $q\beta' e_{\mathfrak{p}} + H(\alpha) \in \mathcal{E}_0(\mathfrak{p}, R')$, and its image under the map of the claim is $(q+1)\beta$. If we show that all values of this harmonic form lie in the ideal $(q+1)$, then we have also shown the surjectivity of the map of the claim in case of the ring R. The latter would follow if we proved that all Fourier coefficients of this harmonic form lie in the ideal $(q+1)$, by Proposition 2.10. The constant terms are obviously zero. By Lemma 3.11 the $\mathfrak{m}$-th coefficient is equal to $q\beta' e^*_{\mathfrak{p}}(\mathfrak{m})$ which lies in $(q+1)$. □

Corollary 6.9. *For every natural number n relatively prime to p the module $\mathcal{E}_0(\mathfrak{p}, \mathbb{Z}/n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}[N(\mathfrak{p})]$, if d is odd, and it is isomorphic to $\mathbb{Z}/n\mathbb{Z}[2N(\mathfrak{p})]$, if d is even.*

Proof. Since $\mathcal{E}_0(\mathfrak{p}, \mathbb{Z}/n\mathbb{Z}) = \oplus\mathcal{E}_0(\mathfrak{p}, \mathbb{Z}/k\mathbb{Z})$, where k runs through the set of components of the primary factorization of n, we may immediately reduce to the case when n is the power of a prime l. In this case the ring $\mathbb{Z}/n\mathbb{Z}$ is still not a coefficient ring in general, but it is close to it. Let $\tilde{R}$ denote the unique unramified extension of $\mathbb{Z}_l$ we get by adjoining the p-th roots of unity. The ring $R = \tilde{R}/n\tilde{R}$ is a coefficient ring which is a free $\mathbb{Z}/n\mathbb{Z}$-module. It will be sufficient to show that the map of Theorem 6.6 maps $\mathcal{E}_0(\mathfrak{p}, \mathbb{Z}/n\mathbb{Z})$ surjectively onto $\mathbb{Z}/n\mathbb{Z}[N(\mathfrak{p})]$, if d is odd, and onto $\mathbb{Z}/n\mathbb{Z}[2N(\mathfrak{p})]$, if d is even. The latter follows from the following simple observation: for every $\beta \in R[N(\mathfrak{p})]$, if d is odd, and for every $\beta \in R[2N(\mathfrak{p})]$, if d is even, the unique form $\phi \in \mathcal{E}_0(\mathfrak{p}, R)$

with the property $\phi^*(1) = \beta$ takes values in the $\mathbb{Z}/n\mathbb{Z}$-module generated by β, which is an immediate consequence of the formula for ϕ it terms of $e_{\mathfrak{p}}$ and $H(\alpha)$ in the proof above. □

REMARK 6.10. Another interesting consequence of our analysis is the congruence:

$$\frac{E_{\mathfrak{p}}}{(q-1)^2} \equiv H(N(\mathfrak{p})) \mod (q+1),$$

which holds for every prime $\mathfrak{p}$ of odd degree. In particular the residue of the form on the left modulo $q+1$ is invariant under the full modular group.

7. THE ABEL-JACOBI MAP

DEFINITION 7.1. Let $\Gamma_0(\mathfrak{p})$ denote $GL_2(A) \cap \mathbb{K}_f(\mathfrak{p})$. This group also acts on Ω via Möbius transformations. By Theorem 5.6 the quotient curve $\Gamma_0(\mathfrak{p})\backslash\Omega$ is $Y_0(\mathfrak{p})$. Let moreover $\Gamma_0(\mathfrak{p})_{\text{ab}} = \Gamma_0(\mathfrak{p})/[\Gamma_0(\mathfrak{p}), \Gamma_0(\mathfrak{p})]$ be the abelianization of $\Gamma_0(\mathfrak{p})$, and let $\overline{\Gamma}_0(\mathfrak{p}) = \Gamma_0(\mathfrak{p})_{\text{ab}}/(\Gamma_0(\mathfrak{p})_{\text{ab}})_{\text{tors}}$ be its maximal torsion-free quotient. For each $\gamma \in \Gamma_0(\mathfrak{p})$ let $\overline{\gamma}$ denote its image in $\overline{\Gamma}_0(\mathfrak{p})$. We say that a meromorphic function θ on Ω is a theta function for $\Gamma_0(\mathfrak{p})$ with automorphy factor $\phi \in \text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$, if $\theta(\gamma z) = \phi(\overline{\gamma})\theta(z)$ for all $z \in \Omega$ and $\gamma \in \Gamma_0(\mathfrak{p})$. If $D = P_1 + \cdots + P_r - Q_1 + \cdots - Q_r \in \text{Div}_0(\Omega)$ is a divisor of degree zero on Ω, define the function

$$\theta(z; D) = \prod_{\gamma \in \Gamma_0(\mathfrak{p})} \frac{(z - \gamma P_1) \cdots (z - \gamma P_r)}{(z - \gamma Q_1) \cdots (z - \gamma Q_r)}.$$

This infinite product converges and defines a meromorphic function on Ω.

PROPOSITION 7.2. *(i) The function $\theta(z; D)$ is a theta function for $\Gamma_0(\mathfrak{p})$.*
(ii) Given $\alpha \in \Gamma_0(\mathfrak{p})$, the theta function $\theta_{\overline{\alpha}}(z) = \theta(z; (w) - (\alpha w))$ is holomorphic, does not depend on the choice of $w \in \mathbb{C}_\infty$, and depends only on the image $\overline{\alpha}$ of α in $\overline{\Gamma}_0(\mathfrak{p})$.

PROOF. See [11], pages 62-67. Part *(ii)* is *(iv)* of Theorem 5.4.1 of [11], page 65. □

NOTATION 7.3. Let ϕ_D be the automorphy factor of $\theta(z; D)$. By the above the value $c_\alpha(\beta) = \phi_{(z)-(\alpha z)}(\beta)$ does not depend on the choice of $z \in \mathbb{C}_\infty$, and depends only on the image of α and β in $\overline{\Gamma}_0(\mathfrak{p})$. Let $j : \overline{\Gamma}_0(\mathfrak{p}) \to \mathcal{H}(\mathfrak{p}, \mathbb{Z})$ denote the map which assigns $r(\theta_{\overline{\alpha}}(z))$ to $\overline{\alpha}$. It is a homomorphism by (v) of Theorem 5.4.1 of the paper quoted above.

The following result will play a crucial role.

THEOREM 7.4. *The homomorphism j is an isomorphism onto $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$.*

PROOF. By Corollary 5.6.4 of [11], page 69 the image of this map lies in $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$. The map is an isomorphism by Theorem 3.3 of [10], page 702. □

Proposition 7.5. *The assignment $\alpha \mapsto c_\alpha$ defines a map*

$$c : \overline{\Gamma}_0(\mathfrak{p}) \to \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), F_\infty^*) \subset \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*),$$

which is injective and has discrete image.

Proof. See [11], pages 67-70. □

Definition 7.6. Let

$$\Phi_{AJ} : \mathrm{Div}_0(\Omega) \to \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$$

be the map which associates to the degree zero divisor D the automorphy factor ϕ_D. Let $\overline{\Gamma}_0(\mathfrak{p})$ also denote its own image in $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ with respect to c by abuse of notation. Given a divisor D of degree zero on the curve $Y_0(\mathfrak{p})$, let $\widetilde{D}$ denote an arbitrary lift to a degree zero divisor on the Drinfeld upper half plane. The automorphy factor $\phi_{\widetilde{D}}$ depends on the choice of $\widetilde{D}$, but its image in $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)/\overline{\Gamma}_0(\mathfrak{p})$ depends only on D. Thus Φ_{AJ} induces a map $\mathrm{Div}_0(Y_0(\mathfrak{p})(\mathbb{C}_\infty)) \to \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)/\overline{\Gamma}_0(\mathfrak{p})$, which we also denote by Φ_{AJ} by abuse of notation.

Theorem 7.7. *The map*

$$\Phi_{AJ} : \mathrm{Div}_0(Y_0(\mathfrak{p})(\mathbb{C}_\infty)) \longrightarrow \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)/\overline{\Gamma}_0(\mathfrak{p})$$

defined above is trivial on the group of principal divisors of $X_0(\mathfrak{p})$, and induces a $\mathrm{Gal}(\mathbb{C}_\infty|F_\infty)$-equivariant identification of the $\mathbb{C}_\infty$-rational points of the Jacobian $J_0(\mathfrak{p})$ of $X_0(\mathfrak{p})$ with the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)/\overline{\Gamma}_0(\mathfrak{p})$.

Proof. See [11], pages 77-80. □

Definition 7.8. Recall the Hecke correspondence $T_\mathfrak{q}$ on the curve $X_0(\mathfrak{p})$ for every prime $\mathfrak{q}$ different from $\mathfrak{p}$, which we introduced in the proof of Lemma 6.2. It induces an endomorphism of the Jacobian $J_0(\mathfrak{p})$ by functoriality, which will be denoted by $T_\mathfrak{q}$ by the usual abuse of notation. Our next task is to describe this action in terms of the isomorphism of Theorem 7.7.

Theorem 7.9. *For every prime $\mathfrak{q} \lhd A$, different from $\mathfrak{p}$, there is a unique endomorphism $T_\mathfrak{q}$ of the rigid analytic torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$, which leaves the lattice $\overline{\Gamma}_0(\mathfrak{p})$ invariant, and makes the diagram:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \overline{\Gamma}_0(\mathfrak{p}) & \xrightarrow{c} & \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*) & \xrightarrow{\Phi_{AJ}} & J_0(\mathfrak{p}) & \longrightarrow & 0 \\ & & {\scriptstyle T_\mathfrak{q}}\downarrow & & {\scriptstyle T_\mathfrak{q}}\downarrow & & {\scriptstyle T_\mathfrak{q}}\downarrow & & \\ 0 & \longrightarrow & \overline{\Gamma}_0(\mathfrak{p}) & \xrightarrow{c} & \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*) & \xrightarrow{\Phi_{AJ}} & J_0(\mathfrak{p}) & \longrightarrow & 0 \end{array}$$

commutative. Moreover the map $j : \overline{\Gamma}_0(\mathfrak{p}) \to \mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$ is equivariant with respect to this action on $\overline{\Gamma}_0(\mathfrak{p})$ and the action of the Hecke operator $T_\mathfrak{q}$ on $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$.

Proof. The first claim is stated in 9.4 of [11], page 86. By definition, the action of $T_{\mathfrak{q}}$ on $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ is the adjoint of the action of $T_{\mathfrak{q}}$ on $\overline{\Gamma}_0(\mathfrak{p})$ given by the formula 9.3.1 of the same paper on page 85. On the same page Proposition 9.3.3 states that the lattice $\overline{\Gamma}_0(\mathfrak{p})$ is invariant with respect to $T_{\mathfrak{q}}$, and its action is given by this formula. The fact that Φ_{AJ} is equivariant is an immediate consequence of its construction. The second claim is the content of Lemma 9.3.2 of [11], page 85. □

Definition 7.10. Let $\mathbb{T}(\mathfrak{p})$ denote the commutative algebra with unity generated by the endomorphisms $T_{\mathfrak{q}}$ of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$, where $\mathfrak{q} \lhd A$ is again any prime ideal different from $\mathfrak{p}$. 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 $\mathfrak{q} \neq \mathfrak{p}$ is any prime. The algebra $\mathbb{T}(\mathfrak{p})$ will be called Hecke algebra and $\mathfrak{E}(\mathfrak{p})$ is its Eisenstein ideal, although these differ slightly from the usual definition, since they do not involve the Atkin-Lehmer operator. The latter will play no role in what follows. Let l be any prime ($l = p$ allowed): we define the $\mathbb{Z}_l$-algebra $\mathbb{T}_l(\mathfrak{p})$ as the tensor product $\mathbb{T}(\mathfrak{p}) \otimes \mathbb{Z}_l$. Let $\mathfrak{E}_l(\mathfrak{p})$ denote the ideal generated by the Eisenstein ideal in $\mathbb{T}_l(\mathfrak{p})$, which we will also call the Eisenstein ideal by slight abuse of terminology. We say that a prime number l is an Eisenstein prime if $l \neq p$ and the ideal $\mathfrak{E}_l(\mathfrak{p})$ is proper in $\mathbb{T}_l(\mathfrak{p})$. For any prime l different from p the l-adic Tate module of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ will be denoted by $T_l(\mathfrak{p})$: it is a $\mathbb{T}_l(\mathfrak{p})$-module.

Proposition 7.11. *The following holds:*

- (i) *the algebra $\mathbb{T}(\mathfrak{p})$ is a finitely generated, free $\mathbb{Z}$-module,*
- (ii) *the $\mathbb{T}(\mathfrak{p})$-module $\overline{\Gamma}_0(\mathfrak{p})$ is faithful,*
- (iii) *the $\mathbb{T}(\mathfrak{p})$-module $J_0(\mathfrak{p})$ is faithful,*
- (iv) *the $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$-module $\mathcal{H}_0(\mathfrak{p}, \mathbb{Q}_l)$ is free of rank one,*
- (v) *the $\mathbb{T}_l(\mathfrak{p})$-module $T_l(\mathfrak{p})$ is locally free of rank one,*
- (vi) *there is a canonical surjection $\mathbb{Z}_l/2N(\mathfrak{p})\mathbb{Z}_l \longrightarrow \mathbb{T}_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})$,*

where we also assume that $l \neq p$ in the last two claims.

Proof. Claim (i) is an immediate consequence of claim (ii), since the latter implies that $\mathbb{T}(\mathfrak{p})$ is a subalgebra of the endomorphism ring of a finitely generated, free $\mathbb{Z}$-module. The latter follows from the general fact that rigid analytic endomorphisms of algebraic tori are algebraic, so they act faithfully on any Zariski-dense invariant subset. Since Φ_{AJ} injects $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathcal{O}_\infty^*)$ into $J_0(\mathfrak{p})(F_\infty)$, the third claim also follows by the same token. By a classical theorem of Harder the elements of $\mathcal{H}_0(\mathfrak{p}, \mathbb{Q}_l)$ are supported on a finite set in $GL_2(F)\backslash GL_2(\mathbb{A})/\mathbb{K}_0(\mathfrak{p}\infty)Z(\mathbb{A})$, so the latter is a finite dimensional $\mathbb{Q}_l$-vectorspace, and $\mathcal{H}_0(\mathfrak{p}, \mathbb{Q}_l) = \mathcal{H}_0(\mathfrak{p}, \mathbb{Z}) \otimes \mathbb{Q}_l$. Therefore it is a faithful $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$-module via the map j by claim (ii). As it is well known, the action of Hecke operators on $\mathcal{H}_0(\mathfrak{p}, \mathbb{Q}_l)$ is semisimple, hence the algebra $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ itself is semisimple. By the strong multiplicity one result (Theorem 3.12) every irreducible module of $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ has multiplicity one in $\mathcal{H}_0(\mathfrak{p}, \mathbb{Q}_l)$, so this module is free of rank one, as claim (iv) states.

As we already noted in the proof of Theorem 7.9, the action of the Hecke algebra $\mathbb{T}(\mathfrak{p})$ on $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ is the adjoint of the action of $\mathbb{T}(\mathfrak{p})$ on $\overline{\Gamma}_0(\mathfrak{p}) = \mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$, so $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z}_l) = \mathcal{H}_0(\mathfrak{p}, \mathbb{Z}) \otimes \mathbb{Z}_l$ is the $\mathbb{Z}_l$-dual of $T_l(\mathfrak{p})$. In particular $T_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is a free $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$-module. Since $T_l(\mathfrak{p})$ is a finitely generated, free $\mathbb{Z}_l$-module, it is a finitely generated module over $\mathbb{T}_l(\mathfrak{p})$. Hence it will be sufficient to prove that $T_l(\mathfrak{p})/\mathfrak{m}T_l(\mathfrak{p})$ is a free module of rank one over $\mathbf{k}_\mathfrak{m} = \mathbb{T}_l(\mathfrak{p})/\mathfrak{m}$ by the Nakayama lemma, where $\mathfrak{m} \triangleleft \mathbb{T}_l(\mathfrak{p})$ is any proper maximal ideal, in order to conclude claim (v). Its dimension is at least one over $\mathbf{k}_\mathfrak{m}$, since the module $T_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is free of rank one over $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. For any ring R let $\mathcal{H}_{00}(\mathfrak{p}, R)$ denote the image of $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z}) \otimes R$ in $\mathcal{H}_0(\mathfrak{p}, R)$ with respect to the functorial map induced by the canonical homomorphism $\mathbb{Z} \to R$. Since l is an element of $\mathfrak{m}$, the $\mathbb{Z}_l$-duality between $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z}_l)$ and $T_l(\mathfrak{p})$ induces a $\mathbb{F}_l$-duality between $T_l(\mathfrak{p})/\mathfrak{m}T_l(\mathfrak{p})$ and the submodule of $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ annihilated by the ideal $\mathfrak{m}$. In general, for any ring R and faithfully flat extension R' of R the natural map $\mathcal{H}_{00}(\mathfrak{p}, R) \otimes_R R' \to \mathcal{H}_{00}(\mathfrak{p}, R')$ is an isomorphism by the theorem of Harder quoted above. This implies in particular that submodule of $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ annihilated by the ideal $\mathfrak{m}$ is a $\mathbf{k}_\mathfrak{m}$ sub-vectorspace of the space of elements of $\mathcal{H}_{00}(\mathfrak{p}, \mathbf{k}_\mathfrak{m})$ which are simultaneous eigenvectors for the operators $T_\mathfrak{q}$ with eigenvalue $T_\mathfrak{q}$ mod $\mathfrak{m}$. Let $\mathbf{l}_\mathfrak{m}$ be a finite extension of $\mathbf{k}_\mathfrak{m}$ which is also a coefficient ring. The eigenspace above tensored with $\mathbf{l}_\mathfrak{m}$ injects into the similar eigenspace of $\mathcal{H}_{00}(\mathfrak{p}, \mathbf{l}_\mathfrak{m})$, which is at most one dimensional over $\mathbf{l}_\mathfrak{m}$ by Theorem 3.12. Claim (v) is proved.

Finally let us concern ourselves with the proof of claim (vi). It is clear from the definition that every generator $T_\mathfrak{q}$ of $\mathbb{T}_l(\mathfrak{p})$ is congruent to an element of $\mathbb{Z}_l$ modulo the Eisenstein ideal, so the natural inclusion of $\mathbb{Z}_l$ in $\mathbb{T}_l(\mathfrak{p})$ induces a surjection $\mathbb{Z}_l \to \mathbb{T}_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})$. If this map is also injective, then the Eisenstein ideal generates a non-trivial ideal in $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. This implies, by claim (iv), that there is a non-zero harmonic form in $\mathcal{H}_0(\mathfrak{p}, \overline{\mathbb{Q}}_l)$ which is annihilated by the Eisenstein ideal. But this is impossible by Theorem 6.6. Therefore the map above induces an isomorphism $\mathbb{Z}_l/N\mathbb{Z}_l \to \mathbb{T}_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})$ for some non-zero $N \in \mathbb{N}$. By claim (v) the module $T_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})T_l(\mathfrak{p})$ is free of rank one over $\mathbb{Z}_l/N\mathbb{Z}_l$, therefore the $\mathbb{Z}_l$-duality between $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z}_l)$ and $T_l(\mathfrak{p})$ induces a $\mathbb{Z}_l/N\mathbb{Z}_l$-duality between $T_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})T_l(\mathfrak{p})$ and the module $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{Z}_l/N\mathbb{Z}_l) \cap \mathcal{E}_0(\mathfrak{p}, \mathbb{Z}_l/N\mathbb{Z}_l)$. The cardinality of the latter must divide $2N(\mathfrak{p})$ by Corollary 6.9, so does the cardinality of the former, because they are equal, by duality. □

An important consequence of claim (iii) above is that $\mathbb{T}(\mathfrak{p})$ may be identified with a subalgebra of the endomorphism ring of the abelian variety $J_0(\mathfrak{p})$, which we will do from now on. Also note that the factor 2 is only necessary in (vi) when $l = 2$ and d is odd.

Definition 7.12. Let $\mathbb{F}$ be local field of characteristic p and let $\mathbb{O}$, r denote its discrete valuation ring and the cardinality of its residue field, respectively. Recall that an abelian variety A defined over $\mathbb{F}$ is said to have multiplicative reduction if the connected component A_0 of the identity in the special fiber of its Néron model $\mathcal{A}$ over $\mathbb{O}$ is a torus. We also say that the abelian variety A

has totally split multiplicative reduction if it has multiplicative reduction and A_0 is a split torus.

LEMMA 7.13. *(i) If A has multiplicative reduction then the p-primary torsion subgroup $A(\mathbb{F})[p^\infty]$ injects into the group of connected components of the special fiber of $\mathcal{A}$.*
(ii) If A has totally split multiplicative reduction then the exponent of the largest torsion subgroup of $A(\mathbb{F})$ mapping into the connected component A_0 under the specialization map divides $r-1$.

PROOF. While we prove claim (i) we may take an unramified extension of $\mathbb{F}$, which will be denoted by the same letter, such that A_0 becomes a split torus, since it commutes with the formation of Néron models. In this case A has a rigid analytic uniformization by a torus $\mathbb{G}_m^n$. The subgroup of $A(\mathbb{F})$ mapping into A_0 under the specialization map is isomorphic to $(\mathbb{O}^*)^n$ in $(\mathbb{F}^*)^n = \mathbb{G}_m^n(\mathbb{F})$ via the uniformization map. Since $\mathbb{F}$ has characteristic p, the group $(\mathbb{O}^*)^n$ has no p-torsion. Claim (i) is now clear. The other half of the lemma also follows by the same reasoning as the torsion of $(\mathbb{O}^*)^n$ is $(\mathbb{F}_r^*)^n$. $\square$

Let $M_0(\mathfrak{p})$ denote the coarse moduli of Drinfeld modules over A with Hecke $\mathfrak{p}$-level structure in the sense introduced by Katz and Mazur (see Definition 3.4 of [13], page 100). It is known that $M_0(\mathfrak{p})$ is a model of $Y_0(\mathfrak{p})$ over the spectrum of A which means that its generic fiber is canonically isomorphic to $Y_0(\mathfrak{p})$.

PROPOSITION 7.14. *The model $M_0(\mathfrak{p})$ is contained in a scheme $\overline{M}_0(\mathfrak{p})$ which has the following properties:*

- (i) *the scheme $\overline{M}_0(\mathfrak{p})$ is proper and flat over Spec(A),*
- (ii) *it has good reduction over all primes $\mathfrak{q}$ different from $\mathfrak{p}$,*
- (iii) *it has stable reduction over $\mathfrak{p}$ with two components which are rational curves over $\mathbf{f}_\mathfrak{p}$ and intersect transversally in $N(\mathfrak{p})$ points,*
- (iv) *it is a model of $X_0(\mathfrak{p})$ over the spectrum of A,*
- (v) *the scheme $\overline{M}_0(\mathfrak{p})$ is either regular or has a singularity of type A_q over $\mathbf{f}_\mathfrak{p}$.*

PROOF. See 5.1-5.8 of [6], pages 229-233. $\square$

COROLLARY 7.15. *The group $J_0(\mathfrak{p})(F)$ has no p-primary torsion.*

PROOF. According to a classical theorem of Raynauld (see Proposition 1.20 of [1], page 219) the connected component of the special fiber of the Néron model over $\mathbb{O}$ of the Jacobian of any regular curve defined over $\mathbb{F}$ is isomorphic to the Picard group scheme of divisors of total degree zero of the special fiber of a regular, proper model of the curve over the spectrum of $\mathbb{O}$. If we set $\mathbb{F} = F_\mathfrak{p}$ then the curve $X_0(\mathfrak{p})$ has $\mathbb{F}$-rational points, namely the cusps. By Proposition 7.14 it has a regular, proper model over the spectrum of $\mathcal{O}_\mathfrak{p}$ such that each component in the special fiber is a rational curve and they intersect transversally. Hence $J_0(\mathfrak{p})$ has multiplicative reduction at $\mathfrak{p}$. According to Lemma 5.9 and Proposition 5.10 of [6], page 234, the order of the group of connected components of the Néron model of $J_0(\mathfrak{p})$ is $N(\mathfrak{p})$. The latter is proved the same way as the corresponding result for elliptic modular curves (see Theorem A.1 of the Appendix to [14], page 173) as it uses the description of the group of components by the intersection matrix of the special fiber, again due to Raynaud. Since $N(\mathfrak{p})$ is relatively prime to p, the claim now follows from Lemma 7.13. □

Lemma 7.16. *The torsion subgroup $\mathcal{T}(\mathfrak{p})$ of $J_0(\mathfrak{p})(F)$ is annihilated by the Eisenstein ideal $\mathfrak{E}(\mathfrak{p})$.*

Proof. For the sake of simple notation let $J_0(\mathfrak{p})$ denote the Néron model of the Jacobian over X, too. Since $J_0(\mathfrak{p})$ has good reduction over all primes $\mathfrak{q}$ different from $\mathfrak{p}$, the reduction map injects $\mathcal{T}(\mathfrak{p})$ into $J_0(\mathfrak{p})(\mathbf{f}_\mathfrak{q})$ by Corollary 7.15. Let $\mathrm{Frob}_\mathfrak{q}$ denote the Frobenius endomorphism of the abelian variety $J_0(\mathfrak{p})_{\mathbf{f}_\mathfrak{q}}$. The Hecke operator $T_\mathfrak{q}$ for each prime $\mathfrak{q}$ different from $\mathfrak{p}$ satisfies the Eichler-Shimura relation:

$$\mathrm{Frob}_\mathfrak{q}^2 - T_\mathfrak{q}\cdot\mathrm{Frob}_\mathfrak{q} + q^{\deg(\mathfrak{q})} = 0.$$

Since $\mathrm{Frob}_\mathfrak{q}$ fixes the reduction of $\mathcal{T}(\mathfrak{p})$, the endomorphism $1 - T_\mathfrak{q} + q^{\deg(\mathfrak{q})}$ annihilates this group. As the reduction map commutes with the action of the Hecke algebra, we get that $\mathfrak{E}(\mathfrak{p})$ annihilates the torsion subgroup. □

Let $t(\mathfrak{p})$ denote the greatest common divisor of $N(\mathfrak{p})$ and $q-1$.

Corollary 7.17. *If the prime l does not divide $t(\mathfrak{p})$ then the l-primary torsion subgroup of $\mathcal{T}(\mathfrak{p})$ injects into the group of connected components of the special fiber of the Néron model of $J_0(\mathfrak{p})$ at ∞ via the specialization map.*

Proof. By Corollary 7.15 we may assume that l is different from p. We may assume that l is odd, too. Otherwise $l=2$ and because it does not divide $q-1$, the number q is even, and we already covered this case. The exponent of the kernel of this map divides both $q-1$ and the cardinality of $\mathbb{T}_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})$ by (ii) of Lemma 7.13 and Lemma 7.16, respectively. The former lemma could be applied as $J_0(\mathfrak{p})$ has split multiplicative reduction at ∞ by Theorem 7.7. Since the latter quantity divides $2N(\mathfrak{p})$ by (vi) of Proposition 7.11, the claim is now clear. □

Proposition 7.18. *For every natural number n the image of $\mathcal{T}(\mathfrak{p})[n]$ with respect to the specialization map into the group of connected components of the special fiber of the Néron model of $J_0(\mathfrak{p})$ at ∞ is a subgroup of $\mathcal{E}_0(\mathfrak{p},\mathbb{Z}/n\mathbb{Z})$.*

Proof. Since $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}),\mathcal{O}_\infty^*)$ is isomorphic to the subgroup of $J_0(\mathfrak{p})(F_\infty)$ mapping into the connected component under the specialization map at ∞ via the map Φ_{AJ}, the $\mathbb{T}(\mathfrak{p})$-module $n^{-1}\overline{\Gamma}_0(\mathfrak{p})/\overline{\Gamma}_0(\mathfrak{p})$ contains the n-torsion of the group of connected components at ∞ as a submodule. The former is isomorphic to $\mathcal{H}_0(\mathfrak{p},\mathbb{Z})/n\mathcal{H}_0(\mathfrak{p},\mathbb{Z})$ by Theorem 7.4, which injects into $\mathcal{H}_0(\mathfrak{p},\mathbb{Z}/n\mathbb{Z})$. Since the specialization map is $\mathbb{T}(\mathfrak{p})$-equivariant, the image of $\mathcal{T}(\mathfrak{p})[n]$ with respect to the composition of these maps must lie in the $\mathbb{T}(\mathfrak{p})$-submodule of $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z}/n\mathbb{Z})$ annihilated by the Eisenstein ideal, according to Lemma 7.16. □

The following theorem is the main Diophantine result of this chapter, which implies Theorems 1.2 and 1.4 under the assumption $t(\mathfrak{p})$=1. The latter is automatic if $q = 2$, so we have a much simpler proof of this result in this case. In the general case we have to prove the Gorenstein property first.

Theorem 7.19. *If the prime l does not divide $t(\mathfrak{p})$ then the l-primary subgroups of $\mathcal{T}(\mathfrak{p})$ and $\mathcal{C}(\mathfrak{p})$ are equal.*

Proof. Just as in the proof of Corollary 7.17, we may assume that l is odd and different from p. This result, along with Proposition 7.18 and Corollary 6.9, also implies that the l-primary subgroup of $\mathcal{T}(\mathfrak{p})$ injects into $\mathbb{Z}_l/N(\mathfrak{p})\mathbb{Z}_l$. Since the order of $\mathcal{C}(\mathfrak{p})$ is exactly $N(\mathfrak{p})$ (see [6], Corollary 5.11 on page 235), the proof is now complete. □

8. The group scheme $\mathcal{S}(\mathfrak{p})$

Definition 8.1. 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. We will also simplify our notation by using the symbol B to denote the spectrum of any ring B. For every non-zero ideal $\mathfrak{n} \triangleleft A$ and Drinfeld module $\phi : A \to B\{\tau\}$ let $\phi[\mathfrak{n}]$ denote the finite flat group scheme of $\mathbb{G}_a$ over B which is usually called the $\mathfrak{n}$-torsion of the Drinfeld module ϕ, where B is any A-algebra. For every scheme G over any base S and any S-scheme T let $G(T)$ denote the set of sections over T, as usual. The group of sections $\phi[\mathfrak{n}](B)$ is naturally an $A/\mathfrak{n}$-module under the action of A on $\mathbb{G}_a$ defined by ϕ.
We are going to define the concept of a Γ-level structure of a Drinfeld module ϕ of rank two over an A-algebra B, where Γ is either $\Gamma(\mathfrak{n})$ or $\Gamma_1(\mathfrak{n})$. Let $N(\Gamma)$ be the abstract A-module $(A/\mathfrak{n})^2$, if $\Gamma = \Gamma(\mathfrak{n})$, and let $N(\Gamma)$ be $A/\mathfrak{n}$, if $\Gamma = \Gamma_1(\mathfrak{n})$. A homomorphism of abstract A-modules $\iota : N(\Gamma) \to \phi[\mathfrak{n}](B)$ is said to be a Γ-level structure on ϕ over B if the effective Cartier divisor D on $\mathbb{G}_a$ over B of degree $|N(\Gamma)|$ defined by $D = \sum_{a\in N(\Gamma)}[\iota(a)]$ is a subgroup scheme of $\phi[\mathfrak{n}]$. By comparing degrees one can conclude that D is actually equal to $\phi[\mathfrak{n}]$ when $\Gamma = \Gamma(\mathfrak{n})$. Hence our concept of $\Gamma(\mathfrak{n})$-level structure is the same as what is now called a Drinfeld basis of $\phi[\mathfrak{n}]$ (see 3.1.-3.2 of chapter III in [13], page 98-99).
Let (ϕ, ι) and (ψ, κ) be ordered pairs of two Drinfeld modules ϕ and ψ of rank two over B equipped with a Γ-level structure ι and κ, respectively. We say that (ϕ, ι) and (ψ, κ) are isomorphic if there is an isomorphism $j : \mathbb{G}_a \to \mathbb{G}_a$ between ϕ and ψ such that the composition $j \circ \iota$ is equal to κ. Let $\mathcal{M}(\mathfrak{n})$ and $\mathcal{M}_1(\mathfrak{n})$ denote the functor which associates to each A-algebra B the set of isomorphism classes of pairs (ϕ, ι) as above, where ι is a $\Gamma(\mathfrak{n})$-level and $\Gamma_1(\mathfrak{n})$-level structure, respectively. If $\mathfrak{n}$ and $\mathfrak{m}$ are relatively prime non-zero ideals of A, let $\mathcal{M}(\mathfrak{n}, \mathfrak{m})$ denote the fiber product of $\mathcal{M}(\mathfrak{n})$ and $\mathcal{M}_1(\mathfrak{m})$ over $\mathcal{M}(1)$. Clearly $\mathcal{M}(\mathfrak{n}, \mathfrak{m})$ is the functor which associates to each A-algebra B the set of isomorphism classes of triples (ϕ, ι, κ), where ι, κ is a $\Gamma(\mathfrak{n})$-level and $\Gamma_1(\mathfrak{m})$-level structure of the

Drinfeld module ϕ, respectively. The following result is just the Corollary to Proposition 5.4 of [3], page 577.

Theorem 8.2. *Assume that the ideal $\mathfrak{n}$ has at least two different prime factors. Then the moduli problem $\mathcal{M}(\mathfrak{n})$ is representable by a regular fine moduli scheme $M(\mathfrak{n})$.* $\square$

Remark 8.3. The natural left action of $GL_2(A/\mathfrak{n})$ on $(A/\mathfrak{n})^2$ induces a right action of $GL_2(A/\mathfrak{n})$ on $\mathcal{M}(\mathfrak{n})$, hence a right action on $M(\mathfrak{n})$, if the latter exists. Let $\Gamma(\mathfrak{n})$ denote the kernel of the natural surjection $GL_2(A/\mathfrak{n}\mathfrak{m}) \to GL_2(A/\mathfrak{n})$ for any $\mathfrak{m} \triangleleft A$ non-zero ideal, by slight abuse of notation. The pull-back of the quotients $M(\mathfrak{n}\mathfrak{m}_1)/\Gamma(\mathfrak{n})$ and $M(\mathfrak{n}\mathfrak{m}_2)/\Gamma(\mathfrak{n})$ to $X - supp(\mathfrak{m}_1\mathfrak{m}_2) - \infty$ are naturally isomorphic whenever $M(\mathfrak{n}\mathfrak{m}_1)$ and $M(\mathfrak{n}\mathfrak{m}_2)$ exist and these schemes glue together to form a coarse moduli scheme for $\mathcal{M}(\mathfrak{n})$. We let $M(\mathfrak{n})$ denote this moduli scheme. Of course this notation is compatible with the previous one.

Definition 8.4. Let G be a finite flat group scheme over the base scheme S equipped with the action of a ring R. The latter implies that there is a natural R-module structure on $G(T)$ for any S-scheme T. Let N be a finite abelian group which is also an R-module. Let $\mathrm{Hom}_R(N, G)$ denote the functor which associates to each S-scheme T the set of homomorphisms of abstract R-modules $\iota : N \to G(T)$. This functor is representable by a fine moduli scheme which will be denoted by the same symbol by the usual abuse of notation.
Let $\phi : A \to B\{\tau\}$ be a Drinfeld module over the A-algebra B, let G be the kernel of a non-zero isogeny on ϕ, and let N be a finite A-module. Note that the group scheme G is naturally an A-module under the action of A on $\mathbb{G}_a$ defined by ϕ. Let $Str_A(N, G)$ denote the sub-functor of $\mathrm{Hom}_A(N, G)$ which associates to each B-algebra C the set of those homomorphisms of abstract A-modules $\iota : N \to G(C)$ such that the effective Cartier divisor D on $\mathbb{G}_a$ over C of degree $|N|$ defined by $D = \sum_{a \in N}[\iota(a)]$ is a subgroup scheme of G.

Lemma 8.5. *The functor $Str_A(N, G)$ is represented by a closed subscheme of $\mathrm{Hom}_A(N, G)$. If G is étale then $Str_A(N, G)$ is either empty or finite, étale over every connected component of B.*

Proof. In 1.5.1 of chapter in [13], page 20-21, the concept of N-level structure was defined. By Proposition 1.6.3, Corollary 1.6.3 on page 23 of the same book the functor which associates to each B-algebra C the set of N-level structures on the $\mathfrak{n}$-torsion of the pull-back of ϕ to C is represented by a closed subscheme of $\mathrm{Hom}_{\mathbb{Z}}(N, G)$. Our functor is represented by the scheme-theoretical intersection of this scheme and $\mathrm{Hom}_A(N, G)$. The second claim follows from Proposition 1.10.12 of [13], page 46-47. $\square$

Definition 8.6. 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. We let $x^{\mathfrak{p}}$ denote $x^{q^{\deg(\mathfrak{p})}}$ for every $\mathbf{f}_{\mathfrak{p}}$-algebra B and element $x \in B$. We say that a Drinfeld module $\phi : A \to B\{\tau\}$ has characteristic $\mathfrak{p}$ if the

A-algebra B has characteristic $\mathfrak{p}$. For every Drinfeld module $\phi : A \to B\{\tau\}$ of characteristic $\mathfrak{p}$ we let $\phi^{(\mathfrak{p})} : A \to B\{\tau\}$ denote the Drinfeld module which as a homomorphism from A to $B\{\tau\}$ is the composition of ϕ and the unique homomorphism $F_{\mathfrak{p}} : B\{\tau\} \to B\{\tau\}$ such that $F_{\mathfrak{p}}(\tau) = \tau$ and $F_{\mathfrak{p}}(x) = x^{\mathfrak{p}}$ for every $x \in B$. Note that $\phi^{(\mathfrak{p})}$ is a Drinfeld module because the homomorphism $x \mapsto x^{\mathfrak{p}}$ fixes the field $\mathbf{f}_{\mathfrak{p}}$, so the composition of $\phi^{(\mathfrak{p})}$ and the derivation $\partial : B\{\tau\} \to B$ is the reduction map $A \to \mathbf{f}_{\mathfrak{p}}$ as required by definition. As obvious from the definition the endomorphism $x \mapsto x^{\mathfrak{p}}$ of the group scheme $\mathbb{G}_a$ defines an isogeny F from ϕ to $\phi^{(\mathfrak{p})}$ which will be called Frobenius. We let $\mathbf{k}_{\mathfrak{p}}$ denote the algebraic closure of the field $\mathbf{f}_{\mathfrak{p}}$.

PROPOSITION 8.7. *For every Drinfeld module $\phi : A \to B\{\tau\}$ of characteristic $\mathfrak{p}$ the kernel of the isogeny F is a sub-group scheme of $\phi[\mathfrak{p}]$.*

PROOF. Let $f \in A = \mathbb{F}_q[T]$ be a polynomial which generates $\mathfrak{p}$. We are going to prove the following stronger formulation of the statement which claims that $\phi(f) = \sum_n a_n \tau^n \in B\{\tau\}$ has no terms of degree less then $\deg(\mathfrak{p})$ in τ. This claim may be checked locally in the étale topology on B. Let $\mathfrak{n}$ be an ideal of A which is relatively prime to $\mathfrak{p}$ and has at least two different prime factors. By Lemma 8.5 the B-scheme $Str_A((A/\mathfrak{n})^2, \phi[\mathfrak{n}])$ is étale, since it is not empty over any component. The latter can be seen by noticing that the base change of ϕ to every geometric point of B has a $\Gamma(\mathfrak{n})$-level structure. Hence we may assume that ϕ is equipped with a $\Gamma(\mathfrak{n})$-level structure. By Theorem 8.2 the Drinfeld module ϕ is the pull-back of the universal Drinfeld module Φ on the fiber of the fine moduli scheme over $\mathbf{f}_{\mathfrak{p}}$. It will be sufficient to prove the claim for the latter. The fiber of the scheme $M(\mathfrak{n})$ over $\mathbf{f}_{\mathfrak{p}}$ is smooth, so we only have to show that the terms of $\Phi(f)$ of degree less then $\deg(\mathfrak{p})$ are vanishing at the geometric points of this fiber. The latter follows from the fact that the proposition holds for Drinfeld modules over $\mathbf{k}_{\mathfrak{p}}$. This last claim is the content of the remark following Proposition 5.1 of [4], page 178. □

DEFINITION 8.8. By the above $\tau^{\deg(\mathfrak{p})}$ divides $\phi(f)$ on the right in the ring $B\{\tau\}$, so there is a unique isogeny V from $\phi^{(\mathfrak{p})}$ to ϕ such that the composition $V \circ F$ is $\phi(f)$. The isogeny V will be called Verschiebung. Note that V depends on the choice of f. But the latter is unique up to a non-zero element of $\mathbb{F}_q$, so $Ker(V)$ is well-defined. Let $\mathfrak{n}$ be any ideal of A relatively prime to $\mathfrak{p}$. We let $\mathcal{I}(\mathfrak{p})$ and $\mathcal{I}(\mathfrak{n}, \mathfrak{p})$ denote the functor which associates to each $\mathbf{f}_{\mathfrak{p}}$-algebra B the set of isomorphism classes of pairs (ϕ, ι) (of triples (ϕ, ι, κ), respectively), where $\phi : A \to B\{\tau\}$ is a Drinfeld module of rank two and ι is an element of $Str_A(A/\mathfrak{p}, Ker(V))$ (and κ is a $\Gamma(\mathfrak{n})$-level structure of ϕ, respectively). We say that two pairs (ϕ, ι) and (ψ, κ) as above are isomorphic if there is an isomorphism $j : \mathbb{G}_a \to \mathbb{G}_a$ between ϕ and ψ such that the composition $j^{\mathfrak{p}} \circ \iota$ is equal to κ. (Note that the definition makes sense because $j^{\mathfrak{p}}$ is an isomorphism between $\phi^{(\mathfrak{p})}$ and $\psi^{(\mathfrak{p})}$). We define the concept of isomorphism of the triples appearing in the definition of $\mathcal{I}(\mathfrak{n}, \mathfrak{p})$ similarly.

Proposition 8.9. *Let $\psi : A \to \mathbf{k}_{\mathfrak{p}}\{\tau\}$ be a Drinfeld module of rank two. The following conditions are equivalent:*

(i) *the group scheme $\psi[\mathfrak{p}]$ is connected,*
(ii) *the group scheme $Ker(V)$ is connected,*
(iii) *the group scheme $Ker(V)$ is not étale.*

Proof. The implications $(i) \Rightarrow (ii)$ and $(ii) \Rightarrow (iii)$ are obvious. If the group scheme $Ker(V)$ is not étale then all terms of $\psi(f)$ have degree greater than $\deg(\mathfrak{p})$. The latter is equivalent to (i) by Satz 5.3 of [4], page 179. □

Definition 8.10. In complete analogy with the classical theory of elliptic curves over algebraic fields of positive characteristic, such Drinfeld modules are called supersingular. Let $\mathcal{R}_{\mathfrak{p}}$ be the maximal unramified extension of $\mathcal{O}_{\mathfrak{p}}$. By definition the residue field of the latter is $\mathbf{k}_{\mathfrak{p}}$. Let $\mathcal{C}_{\mathfrak{p}}$ denote the category whose objects are artin local $\mathcal{R}_{\mathfrak{p}}$-algebras with residue field $\mathbf{k}_{\mathfrak{p}}$ and the morphisms are local $\mathcal{R}_{\mathfrak{p}}$-homomorphisms. Let $\phi : A \to \mathbf{k}_{\mathfrak{p}}\{\tau\}$ be a Drinfeld module of rank two. We say that the Drinfeld module $\Phi : A \to \mathcal{R}_{\mathfrak{p}}[[x]]\{\tau\}$ of rank two is its universal formal deformation if the latter is the universal object over $\mathcal{R}_{\mathfrak{p}}[[x]]$ pro-representing the functor which associates to each object B of $\mathcal{C}_{\mathfrak{p}}$ the set of strict isomorphism classes of Drinfeld modules over B lifting ϕ. (Recall that two Drinfeld modules over B are strictly isomorphic if there is an isomorphism between them whose pull-back to the residue field is the identity). Under our assumption $A = \mathbb{F}_q[T]$ it is very easy to see that the universal deformation exits: up to an isomorphism $\phi(T)$ is of the form $T+\tau^2$ or $T+\tau+\Delta\tau^2$ where Δ is a non-zero element of $\mathbf{k}_{\mathfrak{p}}$. Then we may choose Φ to be the unique Drinfeld module over $\mathcal{R}_{\mathfrak{p}}[[x]]$ with $\Phi(T) = T + x\tau + \tau^2$ or $\Phi(T) = T + \tau + (\Delta + x)\tau^2$.

Proposition 8.11. *Assume that the ideal $\mathfrak{n}$ has at least two different prime factors. Then the moduli problem $\mathcal{M}(\mathfrak{n}, \mathfrak{p})$ is representable by a regular fine moduli scheme $M(\mathfrak{n}, \mathfrak{p})$.*

Proof. Let (ϕ, ι) be the universal object over the fine moduli scheme $M(\mathfrak{n})$. It is clear that the moduli problem $\mathcal{M}(\mathfrak{n}, \mathfrak{p})$ is represented by $Str_A(A/\mathfrak{p}, \phi[\mathfrak{p}])$. Now we only have to show that this scheme $M(\mathfrak{n}, \mathfrak{p})$ is regular. The group scheme $\phi[\mathfrak{p}]$ is étale over the base change of $M(\mathfrak{n})$ to $X - \mathfrak{p} - \infty$. Hence the base change of $M(\mathfrak{n}, \mathfrak{p})$ to $X - \mathfrak{p} - \infty$ is étale over $M(\mathfrak{n})$, in particular it is regular. (One may see that $Str_A(A/\mathfrak{p}, \phi[\mathfrak{p}])$ is non-empty by looking at its fibers over geometric points). Therefore we only have to show that $M(\mathfrak{n}, \mathfrak{p})$ is regular at the closed points of its special fiber over $\mathfrak{p}$. By a suitable analogue of the Deligne homogeneity principle (see Theorem 5.2.1 of [13], pages 130-134), whose proof we do not include because it is completely the same as the result quoted above, we only have to check the latter at the supersingular points. This is exactly what the next proposition claims. □

Let $\psi_0 : A \to \mathbf{k}_{\mathfrak{p}}\{\tau\}$ be a supersingular Drinfeld module of rank two, and let $\Psi : A \to \mathcal{R}_{\mathfrak{p}}[[x]]\{\tau\}$ be its universal formal deformation. Fix a $\iota_0 : (A/\mathfrak{n})^2 \to \psi_0[\mathfrak{n}]$ level structure of $\Gamma(\mathfrak{n})$-type. Let $\mathcal{M}(\mathfrak{n}, \mathfrak{p}, \Psi)$ be the functor which associates to each object B of $\mathcal{C}_{\mathfrak{p}}$ the set of isomorphism classes of triples $(\Psi|_B, \iota, \kappa)$, where $\Psi|_B$ is the pull-back of the Drinfeld module Ψ to B, and ι, κ is a $\Gamma(\mathfrak{n})$-level and $\Gamma_1(\mathfrak{p})$-level structure of the Drinfeld module $\Psi|_B$, respectively, such that the base change of ι to $\mathbf{k}_{\mathfrak{p}}$ with respect to the residue map is the level structure ι_0 above.

Proposition 8.12. *The following holds:*

- (i) *the set $\mathcal{M}(\mathfrak{n}, \mathfrak{p}, \Psi)(\mathbf{k}_{\mathfrak{p}})$ consists of one element,*
- (ii) *the functor $\mathcal{M}(\mathfrak{n}, \mathfrak{p}, \Psi)$ is pro-represented by the spectrum of a regular local ring.*

Proof. By assumption the group scheme $\psi_0[\mathfrak{p}]$ is connected, so the Drinfeld module ψ_0 has only one $\Gamma_1(\mathfrak{p})$-level structure: the identically zero map. Hence claim (i) is clear. We may apply the argument of Proposition 5.2.2 of [13], page 135, to reduce claim (ii) to the seemingly weaker claim that the functor $\mathcal{M}(\mathfrak{n}, \mathfrak{p}, \Psi)$ is pro-represented by the spectrum of a local ring whose maximal ideal is generated by two elements. The pro-representability of $\mathcal{M}(\mathfrak{n}, \mathfrak{p}, \Psi)$ by the spectrum of a ring $\mathcal{A}$ is clear since $\mathcal{M}(\mathfrak{n}, \mathfrak{p})$ itself is representable. By claim (i) this ring $\mathcal{A}$ is local. It is also a finite $\mathcal{R}_{\mathfrak{p}}[[x]]$-algebra by Lemma 8.5, so it is complete. Let $(\Psi|_{\mathcal{A}}, \alpha, \beta)$ be the universal object over $\mathcal{A}$ with respect to the moduli problem $\mathcal{M}(\mathfrak{n}, \mathfrak{p}, \Psi)$. The section $\beta(1) \in \mathbb{G}_a(\mathcal{A})$ corresponds to an element $y \in \mathcal{A}$ which lies in the maximal ideal $\mathfrak{M}$ of $\mathcal{A}$, since the reduction of $\beta(1)$ modulo $\mathfrak{M}$ lies in the connected group scheme $\psi_0[\mathfrak{p}]$. We claim that the parameter x of $\mathcal{R}_{\mathfrak{p}}[[x]]$ and y generate the maximal ideal $\mathfrak{M}$. In light of the universal property and completeness of $\mathcal{A}$ we only need to show that for every B artin local $\mathcal{R}_{\mathfrak{p}}$-algebra and $\phi : \mathcal{A} \to B$ homomorphism of local $\mathcal{R}_{\mathfrak{p}}$-algebras with $\phi(x) = \phi(y) = 0$ the map ϕ factors through the residue map $\mathcal{A} \to \mathcal{A}/\mathfrak{M} = \mathbf{k}_{\mathfrak{p}}$, which is equivalent to the rigidity assertion below. $\square$

Lemma 8.13. *If B is an artin local $\mathcal{R}_{\mathfrak{p}}$-algebra and if $\phi : \mathcal{A} \to B$ is a homomorphism of local $\mathcal{R}_{\mathfrak{p}}$-algebras with $\phi(x) = \phi(y) = 0$, then B is a $\mathbf{k}_{\mathfrak{p}}$-algebra and the induced triple $(\Psi|_B, \alpha|_B, \beta|_B)$ comes from the triple $(\psi_0, \iota_0, 0)$ by extension of scalars $\mathbf{k}_{\mathfrak{p}} \to B$.*

Proof. Let $f \in A = \mathbb{F}_q[T]$ be a polynomial which generates $\mathfrak{p}$. By assumption $\beta|_B(1) \in \mathbb{G}_a(B)$ is the zero section, hence the zero scheme of the polynomial $X^{q^{\deg(\mathfrak{p})}} \in B[X]$ is a subgroup scheme of $\Psi|_B[\mathfrak{p}]$. Hence it must divide the monic polynomial $\Psi|_B(f) = X^{2q^{\deg(\mathfrak{p})}} + \cdots + fX \in B[X]$. In particular f must be zero in B, so the latter is a $\mathbf{k}_{\mathfrak{p}}$-algebra. Since $\phi(x) = 0$ in B as well, the Drinfeld module $\Psi|_B$ must be constant in the sense that it is the pull-back of ψ_0 via the extension of scalars $\mathbf{k}_{\mathfrak{p}} \to B$. Since the group scheme $\Psi|_B[\mathfrak{n}]$ is étale, the Drinfeld module $\Psi|_B$ has exactly one $\Gamma(\mathfrak{n})$-level structure up to isomorphism whose base change to $\mathbf{k}_{\mathfrak{p}}$ with respect to residue map of the local ring B is isomorphic to the level structure ι_0 above, namely the pull-back of ι_0 via the extension of scalars. $\square$

Proposition 8.14. *Assume that the ideal $\mathfrak{n}$ has at least two different prime factors. Then the moduli problem $\mathcal{I}(\mathfrak{n},\mathfrak{p})$ is representable by a smooth affine curve $I(\mathfrak{n},\mathfrak{p})$ over $\mathbf{f}_{\mathfrak{p}}$ and the natural map $I(\mathfrak{n},\mathfrak{p}) \to M(\mathfrak{n}) \times_A \mathbf{f}_{\mathfrak{p}}$ is finite and flat.*

Proof. Let $M(\mathfrak{n})_{\mathfrak{p}}$ denote the fiber of $M(\mathfrak{n})$ over $\mathbf{f}_{\mathfrak{p}}$ and let (ϕ,ι) be the universal object over the scheme $M(\mathfrak{n})_{\mathfrak{p}}$ which is a fine moduli for Drinfeld modules of characteristic $\mathfrak{p}$ equipped with a $\Gamma(\mathfrak{n})$-level structure. It is clear that the moduli problem $\mathcal{I}(\mathfrak{n},\mathfrak{p})$ is represented by $Str_A(A/\mathfrak{p}, Ker(V))$. In particular it is finite over $M(\mathfrak{n})_{\mathfrak{p}}$. By Satz 5.9 of [4], page 181, there are only finitely many $\mathbf{k}_{\mathfrak{p}}$-valued points of $M(\mathfrak{n})_{\mathfrak{p}}$ such that the corresponding Drinfeld module is supersingular. We may reformulate this claim by saying that there is a zero-dimensional closed sub-scheme $M(\mathfrak{n})^{ss}_{\mathfrak{p}}$ of the smooth affine curve $M(\mathfrak{n})_{\mathfrak{p}}$ whose base change to $\mathbf{k}_{\mathfrak{p}}$ represents supersingular Drinfeld modules equipped with a $\Gamma(\mathfrak{n})$-level structure. Here a Drinfeld module over a $\mathbf{k}_{\mathfrak{p}}$-algebra is supersingular if its $\mathfrak{p}$-torsion group scheme is connected. By Propositions 8.7 and 8.9 we may define $M(\mathfrak{n})^{ss}_{\mathfrak{p}}$ as the zero scheme of the Hasse invariant of Gekeler, i.e. the coefficient of the term of $\phi(f)$ of degree $\deg(\mathfrak{p})$, where f is a polynomial which generates the ideal $\mathfrak{p}$. The finite, flat group scheme $Ker(V)$ over the open complement $M(\mathfrak{n})^{ord}_{\mathfrak{p}}$ of $M(\mathfrak{n})^{ss}_{\mathfrak{p}}$ is étale, because its pull-back to every $\mathbf{k}_{\mathfrak{p}}$-valued point is étale by Proposition 8.7. Hence the map $I(\mathfrak{n},\mathfrak{p}) \to M(\mathfrak{n})_{\mathfrak{p}}$ is étale over the open sub-scheme $M(\mathfrak{n})^{ord}_{\mathfrak{p}}$ by Lemma 8.5. Therefore the pre-image of $M(\mathfrak{n})^{ord}_{\mathfrak{p}}$ in $I(\mathfrak{n},\mathfrak{p})$ is a smooth curve.

Hence we only have to show that $I(\mathfrak{n},\mathfrak{p})$ is smooth of dimension one at its supersingular locus, i.e. at the pre-image of $M(\mathfrak{n})^{ss}_{\mathfrak{p}}$, because every finite, almost everywhere unramified map between smooth curves is automatically flat. It is sufficient do so after base change to $\mathbf{k}_{\mathfrak{p}}$. Our argument is very similar to the proof of Proposition 8.12. Let (ψ_0,ι_0) be a pair which corresponds to a supersingular point of $M(\mathfrak{n})$, which means that $\psi_0 : A \to \mathbf{k}_{\mathfrak{p}}\{\tau\}$ is a supersingular Drinfeld module of rank two and $\iota_0 : (A/\mathfrak{n})^2 \to \psi_0[\mathfrak{n}]$ is a $\Gamma(\mathfrak{n})$-level structure. As the group scheme $Ker(V) \subseteq \psi_0^{(\mathfrak{p})}[\mathfrak{p}]$ is connected, this point has a unique lift (ψ,ι_0,κ_0) to $I(\mathfrak{n},\mathfrak{p})$. Let $\Psi : A \to \mathbf{k}_{\mathfrak{p}}[[x]]\{\tau\}$ be the universal formal deformation of ψ_0 for local artin $\mathbf{k}_{\mathfrak{p}}$-algebras. Since the group scheme $\Psi[\mathfrak{n}]$ is étale, there is a unique level structure $\iota : (A/\mathfrak{n})^2 \to \Psi[\mathfrak{n}]$ lifting ι_0 up to strict isomorphism. The pair (Ψ,ι) is the universal object over $\mathbf{k}_{\mathfrak{p}}[[x]]$ which pro-represents the deformations of the pair (ψ_0,ι_0) over local artin $\mathbf{k}_{\mathfrak{p}}$-algebras. Let $\mathcal{A}$ be the local complete $\mathbf{k}_{\mathfrak{p}}[[x]]$-algebra whose spectrum is $Str_A(A/\mathfrak{p},\Psi[\mathfrak{p}])$: this ring is the completion of the local ring of the scheme $I(\mathfrak{n},\mathfrak{p}) \times_{\mathbf{f}_{\mathfrak{p}}} \mathbf{k}_{\mathfrak{p}}$ at the closed point (ψ,ι_0,κ_0). It will be sufficient to show that $\mathcal{A}$ is a formal power series ring over $\mathbf{k}_{\mathfrak{p}}$. We only need to find a parameter in $\mathcal{A}$ because we proved already that $\mathcal{A}$ is finite over $\mathbf{k}_{\mathfrak{p}}[[x]]$ and it has dimension one. Note that $\mathcal{A}$ pro-represents the deformations of the triple $(\psi_0,\iota_0,\kappa_0)$ over local artin $\mathbf{k}_{\mathfrak{p}}$-algebras. Let (Ψ,ι,κ) be the universal object over this ring. The section $\kappa(1) \in \mathbb{G}_a(\mathcal{A})$ corresponds to an element $y \in \mathcal{A}$ which lies in the maximal ideal $\mathfrak{M}$ of $\mathcal{A}$, since the reduction of $\kappa(1)$ modulo $\mathfrak{M}$ lies in the connected group scheme $Ker(V) \subseteq \psi_0^{(\mathfrak{p})}[\mathfrak{p}]$. We claim that y generates the maximal ideal $\mathfrak{M}$. Because of the universal property of $\mathcal{A}$ it will be sufficient to show the following rigidity assertion: if B is an artin local $\mathbf{k}_{\mathfrak{p}}$-algebra and if $\phi : \mathcal{A} \to B$ is a homomorphism of local $\mathbf{k}_{\mathfrak{p}}$-algebras with $\phi(y) = 0$, then the induced triple $(\Psi|_B, \iota|_B, \kappa|_B)$ comes from the triple $(\psi_0, \iota_0, \kappa_0)$ by extension of scalars $\mathbf{k}_{\mathfrak{p}} \to B$. Under these assumptions $Ker(V) \subseteq \Psi^{(\mathfrak{p})}|_B[\mathfrak{p}]$ is connected, hence so does $\Psi|_B[\mathfrak{p}]$, because the latter is the extension of $Ker(F)$ by $Ker(V)$. By Lemma 5.5 of [4], page 191, the scheme $M(\mathfrak{n})_{\mathfrak{p}}^{ss}$ is reduced, so the pair $(\Psi|_B, \iota|_B)$ is constant. The level structure $\kappa|_B$ is constant by assumption, so does the triple $(\Psi|_B, \iota|_B, \kappa|_B)$. □

DEFINITION 8.15. The natural left action of $GL_2(A/\mathfrak{n})$ on $(A/\mathfrak{n})^2$ induces a right action of $GL_2(A/\mathfrak{n})$ on $\mathcal{M}(\mathfrak{n}, \mathfrak{p})$, hence a right action on $M(\mathfrak{n}, \mathfrak{p})$, if the latter exists. We may glue together open pieces of the quotients $M(\mathfrak{n}, \mathfrak{p})/GL_2(A/\mathfrak{n})$ for various $\mathfrak{n}$ to form a coarse moduli scheme for $\mathcal{M}_1(\mathfrak{p})$, as in Remark 8.3. We let $M_1(\mathfrak{p})$ denote this moduli scheme. Similarly we may construct a coarse moduli scheme $I(\mathfrak{p})$ representing the functor $\mathcal{I}(\mathfrak{p})$ by gluing together open pieces of the quotients $I(\mathfrak{n}, \mathfrak{p})/GL_2(A/\mathfrak{n})$. Also note that there is a morphism $I(\mathfrak{p}) \to M_1(\mathfrak{p}) \times_A \mathbf{f}_{\mathfrak{p}}$ induced by the natural map which assigns to every pair (ϕ, ι) of the type appearing in Definition 8.8 the pair $(\phi^{(\mathfrak{p})}, \iota)$.

PROPOSITION 8.16. *The coarse moduli $M_1(\mathfrak{p})$ has the following properties:*

- (i) *it is a model of $Y_1(\mathfrak{p})$ over the spectrum of A,*
- (ii) *it is normal and affine over $Spec(A)$,*
- (iii) *the reduced scheme associated to its reduction over $\mathfrak{p}$ has two irreducible components which are smooth curves over $\mathbf{f}_{\mathfrak{p}}$ and intersect transversally in $N(\mathfrak{p})$ supersingular points.*

PROOF. We start our proof by showing the following remark: if R is a normal integral domain and G is a finite group acting on R, then the subring R^G of invariants is also integrally closed. Let Q be the quotient field of R. This field is equipped with an action of G which extends the action of the latter on R. The field Q^G of invariants clearly contains the quotient field of R^G. Any element of Q^G integral over R^G must lie in $R^G = R \cap Q^G$ because R is integrally closed. Hence the remark is true.

The first claim is obvious. Zariski-locally on $Spec(A)$ the scheme $M_1(\mathfrak{p})$ is the quotient of an affine and regular scheme by a finite group, so the second claim is also clear by the remark above. Recall that the reduction of $M_0(\mathfrak{p})$ over $\mathfrak{p}$ has two irreducible components: $M_{00}(\mathfrak{p})$ and $M_{01}(\mathfrak{p})$, whose $\mathbf{k}_{\mathfrak{p}}$-valued points correspond to pairs $(\phi, Ker(F))$ and $(\phi^{(\mathfrak{p})}, Ker(V))$, respectively, where $\phi : A \to \mathbf{k}_{\mathfrak{p}}\{\tau\}$ is any Drinfeld module of rank two over $\mathbf{k}_{\mathfrak{p}}$. Let $M_{10}(\mathfrak{p})$ and $M_{11}(\mathfrak{p})$ denote the pre-image of $M_{00}(\mathfrak{p})$ and $M_{01}(\mathfrak{p})$ via the natural map $M_1(\mathfrak{p}) \to M_0(\mathfrak{p})$, respectively. The composition of the canonical map $M_{10}(\mathfrak{p})_{red} \to M_{10}(\mathfrak{p})$ and the restriction $M_{10}(\mathfrak{p}) \to M_{00}(\mathfrak{p})$ induces a bijection between the set of $\mathbf{k}_{\mathfrak{p}}$-valued points of $M_{10}(\mathfrak{p})_{red}$ and $M_{00}(\mathfrak{p})$ because the group scheme $Ker(F)$ is always connected. By Hilbert's Nullstellensatz the compo-

sition map above must be a finite map of degree 1 between irreducible curves, in particular $M_{10}(\mathfrak{p})_{red}$ is connected. But $M_{00}(\mathfrak{p})$ is normal, so this map is an isomorphism. Hence $M_{10}(\mathfrak{p})_{red}$ is smooth, too.
For every A-algebra B of characteristic $\mathfrak{p}$ the set $\mathcal{I}(\mathfrak{p})(B)$ injects into $\mathcal{M}_1(\mathfrak{p})(B)$ under the natural map which induces the map $I(\mathfrak{p}) \to M_1(\mathfrak{p}) \times_A \mathbf{f}_\mathfrak{p}$ of Definition 8.15, so the latter is a closed immersion. Clearly $M_{11}(\mathfrak{p})$ is the image of $I(\mathfrak{p})$, so it is smooth by Proposition 8.14. The same proposition implies that the natural map $I(\mathfrak{p}) \to M(1) \times_A \mathbf{f}_\mathfrak{p}$ is a branched covering which totally ramifies over the supersingular points. The latter follows from the fact every supersingular Drinfeld module of rank two over $\mathbf{k}_\mathfrak{p}$ has a unique $\mathcal{I}(\mathfrak{p})$-structure, because its $\mathfrak{p}$-torsion group scheme is connected. Hence $M_{11}(\mathfrak{p})$ is connected, too. For the same reason we know that every supersingular point in the reduction of $M_0(\mathfrak{p})$ over $\mathfrak{p}$ has a unique lift to $M_1(\mathfrak{p})$. Claim (iii) is now fully proved. □

Lemma 8.17. *The finite group scheme $\mathcal{S}(\mathfrak{p})$ is étale and μ-type of rank $N(\mathfrak{p})$, and as a subgroup of $J_0(\mathfrak{p})(\overline{F})$ it is cyclic.*

Proof. We will gather some facts about the cover $X_1(\mathfrak{p}) \to X_0(\mathfrak{p})$, where $X_1(\mathfrak{p})$ is the unique geometrically irreducible non-singular projective curve containing $Y_1(\mathfrak{p})$, which could be also excavated from [5], section 4 of chapter V and section 5 of chapter VII, with some effort. We call a geometric point on a Drinfeld modular curve elliptic, if the automorphism group the underlying Drinfeld module of rank two is strictly larger than $\mathbb{F}_q^*$. First note that both the cover $Y_0(\mathfrak{p}) \to Y_0(1)$ and the cover $Y_1(\mathfrak{p}) \to Y_0(1)$ could ramify only over the unique elliptic point of $Y_0(1)$. Hence the cover $X_1(\mathfrak{p}) \to X_0(\mathfrak{p})$ could ramify only at elliptic points and at the cusps. By counting the latter we get that the cover is actually unramified at them. The number of elliptic points on $Y_1(\mathfrak{p})$ is $(q^{2d}-1)/(q^2-1)$. The number of elliptic points on $Y_0(\mathfrak{p})$ is $(q^d+1)/(q+1)$, if d is odd, and it is q^d+1, if d is even. Hence the cover $X_1(\mathfrak{p}) \to X_0(\mathfrak{p})$ ramifies if and only if d is even, when the ramification index is $q+1$ at each elliptic point. We get that the cover $X_2(\mathfrak{p}) \to X_0(\mathfrak{p})$ is unramified. Since it is also Galois over F with a cyclic Galois group of order $N(\mathfrak{p})$, the lemma follows immediately by the same standard argument as in the proof of Proposition 11.6 of [14], page 100. □

Proposition 8.18. *The image of $\mathcal{S}(\mathfrak{p})$ with respect to the specialization map into the the special fiber of the Néron model of $J_0(\mathfrak{p})$*

(i) *at ∞ lies in the connected component of the identity,*
(ii) *at $\mathfrak{p}$ does not intersect the connected component of the identity.*

Proof. First note that the two claims make sense because $\mathcal{S}(\mathfrak{p})$ is étale, so it has a well-defined extension into the Néron model of $J_0(\mathfrak{p})$. In this paragraph we will use the notation and results of [11] without extra notice. (Recall that $\overline{\Gamma}_0(\mathfrak{p}) = \overline{\Gamma_0(\mathfrak{p})}$ under the notation introduced by Definition 7.1). Let K_∞ be the maximal unramified extension of F_∞ and let $\mathcal{R}_\infty$ be its discrete valuation ring. Let $J_{00}(\mathfrak{p})(K_\infty)$ and $J_{20}(\mathfrak{p})(K_\infty)$ be the pre-image of the connected component under the reduction map in the Lie groups $J_0(\mathfrak{p})(K_\infty)$ and $J_2(\mathfrak{p})(K_\infty)$, respectively. In order to prove claim (i) it will be sufficient to construct a sub-group of order $N(\mathfrak{p})$ in the kernel of the map $j : J_{00}(\mathfrak{p})(K_\infty) \to J_{20}(\mathfrak{p})(K_\infty)$ induced by Picard functoriality by the previous lemma. By the definition of the Abel-Jacobi map as an automorphy factor there is a commutative diagram of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}(\overline{\Gamma_0(\mathfrak{p})}, \mathcal{R}^*_\infty) & \xrightarrow{\Phi_{AJ}} & J_{00}(\mathfrak{p})(K_\infty) & \longrightarrow & 0 \\ & & {\scriptstyle i}\downarrow & & {\scriptstyle j}\downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}(\overline{\Gamma_2(\mathfrak{p})}, \mathcal{R}^*_\infty) & \xrightarrow{\Phi_{AJ}} & J_{20}(\mathfrak{p})(K_\infty) & \longrightarrow & 0 \end{array}$$

where the first vertical map is induced by the abelianization of the canonical injection $\Gamma_2(\mathfrak{p}) \to \Gamma_0(\mathfrak{p})$. Of course $\Gamma_2(\mathfrak{p})$ is the normal arithmetic subgroup of $\Gamma_0(\mathfrak{p})$ corresponding to the cover $Y_2(\mathfrak{p}) \to Y_0(\mathfrak{p})$. By the above we only need to construct a sub-group of the kernel of the map i whose order is $N(\mathfrak{p})$. Since $\mathcal{R}^*_\infty$ contains a cyclic group of order n for any natural number n relatively prime to p, it will be sufficient to construct a surjective homomorphism $h : \Gamma_0(\mathfrak{p}) \to \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$ whose kernel contains $\Gamma_2(\mathfrak{p})$. We define h as the composition of the reduction map $r : \Gamma_0(\mathfrak{p}) \to B(A/\mathfrak{p}) \subset GL_2(A/\mathfrak{p})$, the upper left corner element $a : B(A/\mathfrak{p}) \to (A/\mathfrak{p})^*$ and the unique surjection $p : (A/\mathfrak{p})^* \to \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$.

Let's start the proof of the second claim. For every projective curve C (reduced, one-dimensional, but not necessarily irreducible projective scheme over a field) let $\mathrm{Pic}^0(C)$ denote the Picard group of divisors of total degree zero. First note that there is a projective scheme $\overline{M}_1(\mathfrak{p})$ over A which contains $M_1(\mathfrak{p})$ as a Zariski-dense open sub-scheme such that the natural map $p : M_1(\mathfrak{p}) \to M_0(\mathfrak{p})$ has an extension $\overline{p} : \overline{M}_1(\mathfrak{p}) \to \overline{M}_0(\mathfrak{p})$. We may define $\overline{M}_1(\mathfrak{p})$ as the closure of the graph of p in the product of $\overline{M}_0(\mathfrak{p})$ and any projective completion of $M_1(\mathfrak{p})$ over A. Let $r : \widetilde{M}_0(\mathfrak{p}) \to \overline{M}_0(\mathfrak{p})$ be the minimal resolution of singularities of the surface $\overline{M}_0(\mathfrak{p})$ over A. Because $\overline{M}_0(\mathfrak{p})$ is either regular or has a singularity of type A_q over $\mathbf{f}_\mathfrak{p}$ at a supersingular point, the induced map $r^* : \mathrm{Pic}^0(\overline{M}_0(\mathfrak{p}) \times_A \mathbf{k}_\mathfrak{p}) \to \mathrm{Pic}^0(\widetilde{M}_0(\mathfrak{p}) \times_A \mathbf{k}_\mathfrak{p})$ is an isomorphism. Let $\widetilde{M}_1(\mathfrak{p})$ be the minimal resolution of singularities of the fiber product $\overline{M}_1(\mathfrak{p}) \times_A \widetilde{M}_0(\mathfrak{p})$ over A. By construction there is a commutative diagram:

$$\begin{array}{ccc} \widetilde{M}_1(\mathfrak{p}) & \xrightarrow{t} & \widetilde{M}_0(\mathfrak{p}) \\ {\scriptstyle s}\downarrow & & {\scriptstyle r}\downarrow \\ \overline{M}_1(\mathfrak{p}) & \xrightarrow{\overline{p}} & \overline{M}_0(\mathfrak{p}) \end{array}$$

where the vertical maps are birational. Let $\overline{S}_1$ and $\widetilde{S}_1$ be the closure of the special fiber of $M_1(\mathfrak{p})$ over $\mathbf{k}_\mathfrak{p}$ in $\overline{M}_1(\mathfrak{p}) \times_A \mathbf{k}_\mathfrak{p}$ and its pre-image with respect to

s, respectively. By Picard functoriality we have another commutative diagram:

$$\begin{tikzcd}
\mathrm{Pic}^0((\widetilde{S}_1)_{red}) & \mathrm{Pic}^0((\widetilde{M}_1(\mathfrak{p}) \times_A \mathbf{k}_{\mathfrak{p}})_{red}) \arrow[l, "j^*"'] & \mathrm{Pic}^0(\widetilde{M}_0(\mathfrak{p}) \times_A \mathbf{k}_{\mathfrak{p}}) \arrow[l, "t^*"'] \\
\mathrm{Pic}^0((\overline{S}_1)_{red}) \arrow[u, "s|^*_{\overline{S}_1}"] & \mathrm{Pic}^0((\overline{M}_1(\mathfrak{p}) \times_A \mathbf{k}_{\mathfrak{p}})_{red}) \arrow[l, "i^*"'] \arrow[u, "s^*"] & \mathrm{Pic}^0(\overline{M}_0(\mathfrak{p}) \times_A \mathbf{k}_{\mathfrak{p}}) \arrow[l, "\overline{p}^*"'] \arrow[u, "r^*"]
\end{tikzcd}$$

By the classical theorem of Raynauld already quoted above it will be sufficient to show that the map t^* is injective in order to prove the second claim. Because r^* is bijective, trivial diagram chasing shows that we only have to prove that the composition $s|^*_{\overline{S}_1} \circ i^* \circ \overline{p}^*$ is injective. The scheme $(\overline{S}_1)_{red}$ has two irreducible components. Their image with respect to $\overline{p}$ intersect inside of the Zariski open set $M_0(\mathfrak{p})$ only, so they themselves intersect inside of the Zariski open set $M_1(\mathfrak{p})$ only. Hence Zariski's main theorem implies that the pre-image of every cross-point of $(\overline{S}_1)_{red}$ is connected in $(\widetilde{S}_1)_{red}$ as $M_1(\mathfrak{p})$ is normal. Therefore the restriction $s|^*_{\overline{S}_1}$ of the map s^* is injective on the toric part of the semi-abelian variety $\mathrm{Pic}^0((\overline{S}_1)_{red})$. On the other hand the composition of $\overline{p}^*$ and the map i^* induced by the closed immersion $i : (\overline{S}_1)_{red} \to (\overline{M}_1(\mathfrak{p}) \times_A \mathbf{k}_{\mathfrak{p}})_{red}$ is injective which can be seen by applying the argument in the proof of Proposition 11.9 of [14], pages 102-103. The semi-abelian variety $\mathrm{Pic}^0(\overline{M}_0(\mathfrak{p}) \times_A \mathbf{k}_{\mathfrak{p}})$ is a torus, so the composition $i^* \circ \overline{p}^*$ maps into the toric part of the semi-abelian variety $\mathrm{Pic}^0((\overline{S}_1)_{red})$. Therefore the homomorphism $s|^*_{\overline{S}_1} \circ i^* \circ \overline{p}^*$ is injective, as claimed. $\square$

In the next claim and its proof we let $J_0(\mathfrak{p})_l$ and $J_0(\mathfrak{p})$ denote the Galois module $J_0(\mathfrak{p})(\overline{F})$ and the Néron model of the Jacobian $J_0(\mathfrak{p})$, respectively.

Lemma 8.19. *Let l be an Eisenstein prime and let B be a subgroup of either $\mathcal{C}(\mathfrak{p})_l$ or $\mathcal{S}(\mathfrak{p})_l$. Then we have an exact sequence:*

$$0 \to B \to J_0(\mathfrak{p})_l^I \to (J_0(\mathfrak{p})_l/B)^I \to 0,$$

where the subscript denotes the module of elements fixed under the action of the inertia group I at $\mathfrak{p}$.

Proof. (Compare with Lemma 16.5 of [14], pages 125-126). What we need to show is that the map $J_0(\mathfrak{p})_l^I \to (J_0(\mathfrak{p})_l/B)^I$ is surjective. Any element of $J_0(\mathfrak{p})_l^I$ is fixed by the absolute Galois group of some finite, unramified extension K of $F_{\mathfrak{p}}$. Since the formation of Néron models commutes with unramified base change, the group $\mathcal{C}(\mathfrak{p})$ maps isomorphically onto the group of components of $J_0(\mathfrak{p})$ over K. Hence $J_0(\mathfrak{p})_l^I = J_{00}(\mathfrak{p})(\overline{\mathbf{f}}_{\mathfrak{p}})_l \times \mathcal{C}(\mathfrak{p})$, where $J_{00}(\mathfrak{p})$ is the connected component. Because $J_0(\mathfrak{p})$ has semi-stable reduction, the monodromy filtration on $J_0(\mathfrak{p})_l$ has two steps, in other words $(\gamma-1)e \in J_0(\mathfrak{p})_l^I$ for any $e \in J_0(\mathfrak{p})_l$ and $\gamma \in I$. Since $J_0(\mathfrak{p})_l$ is an l-divisible group, its image under the map $\gamma - 1$ is l-divisible, too. As l divides the order of $\mathcal{C}(\mathfrak{p})$ the l-divisible part of $J_0(\mathfrak{p})_l^I$ is the factor $J_{00}(\mathfrak{p})(\overline{\mathbf{f}}_{\mathfrak{p}})_l$ of the direct product decomposition above. We may conclude that $(\gamma-1)e$ must lie in $J_{00}(\mathfrak{p})(\overline{\mathbf{f}}_{\mathfrak{p}})$. Let $\overline{e}$ be any element of $(J_0(\mathfrak{p})_l/B)^I$ and take an element e in $J_0(\mathfrak{p})_l$ which maps to $\overline{e}$. For any $\gamma\in I$ we have $(\gamma-1)e\in B$ by definition. By the above this expression also lies in $J_{00}(\mathfrak{p})(\overline{\mathbf{f}}_{\mathfrak{p}})_l$ whose intersection with B is trivial because both $\mathcal{C}(\mathfrak{p})$ and $\mathcal{S}(\mathfrak{p})$ has trivial intersection with that group. (The former is proved in 5.11 of [6], page 235, the latter is (ii) of Proposition 8.18). Hence $e\in J_0(\mathfrak{p})_l^I$. $\square$

9. The group scheme $\mathcal{D}(\mathfrak{p})[l]$

Definition 9.1. The subgroup $B(A)$ of upper triangular matrices of $GL_2(A)$ is the stabilizer of the point ∞ on the projective line in $GL_2(A)$ with respect to the Möbius action. Also note that $B(A)$ leaves the set $\Omega_c=\{z\in\Omega|c\leq|z|_i\}$ invariant for any positive $c\in\mathbb{Q}$. If $u:\Omega\to\mathbb{C}_\infty^*$ is a $B(A)$-invariant holomorphic function then its van der Put logarithmic derivative $r(u):GL_2(F_\infty)\to\mathbb{Z}$ is also invariant with respect to the left regular action of $B(A)$. In particular the integral

$$r(u)^0=\int_{A\backslash F_\infty} r(u)\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\mathrm{d}\mu_\infty(x)$$

is well-defined, where μ_∞ is the Haar measure introduced in Definition 5.1. Let $e(z):\Omega\to\mathbb{C}_\infty^*$ denote the classical Carlitz-exponential:

$$e(z)=z\prod_{0\neq\lambda\in A}\left(1-\frac{z}{\lambda}\right)$$

and define $t(z)$ as $e(z)^{q-1}$. It is well known (see for example 2.7 of [11], page 44-45) that the function t^{-1} is $B(A)$-invariant and it is a biholomorphic map between the quotient $B(A)\backslash\Omega_c$ and a small open disc around 0 punctured at 0 for a sufficiently large c. We say that the $B(A)$-invariant holomorphic function u on Ω is meromorphic at ∞ if the composition of u and the inverse of the biholomorphic map t is meromorphic at 0 for some (and hence all) such c number. In this case we can speak about its value, order of zero or order of pole at ∞. Of course our definition is just a specialization of the general definition in [5].

Proposition 9.2. *Assume that the holomorphic function $u:\Omega\to\mathbb{C}_\infty^*$ is $B(A)$-invariant and it is meromorphic at ∞ in the sense defined above. Then its order of vanishing at ∞ is equal to $r(u)^0/(q-1)$.*

Proof. It is sufficient to prove the claim in the following two cases:

(i) the function u is non-zero at ∞,
(ii) the function u is equal to $t(z)$.

In the first case we need to show that $r(u)^0=0$. Let υ be a uniformizer of F_∞ as in Definition 3.4. Since $r(u)$ is a harmonic cochain on the Bruhat-Tits tree of $GL_2(F_\infty)$, it satisfies the identity:

$$r(u)(g)=\sum_{\epsilon\in\mathbb{F}_q} r(u)(g\begin{pmatrix}\upsilon & \epsilon\\ 0 & 1\end{pmatrix})$$

for all $g \in GL_2(F_\infty)$. By an n-fold application of this identity we get the formula:

$$\begin{aligned}\int_{A\backslash F_\infty} r(u)\begin{pmatrix} v^{-n} & x \\ 0 & 1\end{pmatrix}\mathrm{d}\mu_\infty(x) =& \sum_{\epsilon\in\mathbb{F}_q}\int_{A\backslash F_\infty} r(u)\begin{pmatrix} v^{1-n} & x+\epsilon \\ 0 & 1\end{pmatrix}\mathrm{d}\mu_\infty(x)\\ =&q\int_{A\backslash F_\infty} r(u)\begin{pmatrix} v^{1-n} & x \\ 0 & 1\end{pmatrix}\mathrm{d}\mu_\infty(x)\\ =&\ldots = q^n r(u)^0.\end{aligned}$$

Because u is non-zero at ∞, its absolute value is constant on the the set Ω_c for a sufficiently large c as the latter set maps to a small neighborhood of 0 with respect to t^{-1}. Choose the natural number n large enough such that the positive number $c = |v^{-n}|$ has the property above. For every $\rho \in GL_2(F_\infty)$ let $C(\rho)$ denote the annulus

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

By our assumptions the holomorphic function u has constant absolute value on the non-empty affinoid subdomain $C(\begin{pmatrix} v^{-n} & x \\ 0 & 1\end{pmatrix})\cap\Omega_c$ for any $x \in F_\infty$ hence either by its description in 1.7.3 of [11], page 40 as a difference of logarithms of absolute values on subdomains of this affinoid or by the results of [16], the value of $r(u)(\begin{pmatrix} v^{-n} & x \\ 0 & 1\end{pmatrix})$ is zero. Hence the integral on the left in the equation above is also zero which implies that $r(u)^0$ is zero, too.
In the second case we need to show that $r(t(z))^0 = 1-q$. By definition:

$$r(e(z))(g) = -|\{\lambda \in A|\lambda \notin D(g)\}|$$

for every $g \in GL_2(F_\infty)$ such that $\infty \in D(g)$. As

$$\infty \in D(\begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix}) = \{z \in \mathbb{P}^1(\mathbb{C}_\infty)|1 < |z-x|\}$$

for any $x \in F_\infty$, we get:

$$r(e(z))(\begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix}) = -|\{\lambda \in A||\lambda - x| \leq 1\}.$$

Since for every $x \in F_\infty$ there are exactly q elements λ of A such that $|\lambda - x| \leq 1$ holds, we get that $r(t(z)) = -(q-1)q\mu_\infty(A\backslash F_\infty) = 1-q$. □

Proposition 9.3. *(i) In $\mathcal{C}(\mathfrak{p})$ the kernel of the specialization map into the group of connected components of the special fiber of the Néron model of $J_0(\mathfrak{p})$ at ∞ is its unique cyclic group of order $t(\mathfrak{p})$.*
(ii) The intersection of $\mathcal{C}(\mathfrak{p})$ and $\mathcal{S}(\mathfrak{p})$ is their unique cyclic group of order $t(\mathfrak{p})$.

Proof. Claim (i) of the proposition above is just (i) of Theorem 5.9 in [7], page 371. The intersection of $\mathcal{C}(\mathfrak{p})$ and $\mathcal{S}(\mathfrak{p})$ is a constant and a μ-type Galois module at the same time, so it is contained in the unique cyclic group of order $t(\mathfrak{p})$ in the cuspidal divisor group. Hence it is sufficient to prove that the latter lies in the kernel of the homomorphism $J_0(\mathfrak{p}) \to J_2(\mathfrak{p})$ induced by Picard functoriality. By Corollary 3.18 of [8] on page 198 the modular unit $\Delta/\Delta_{\mathfrak{p}}$ admits an $r(\mathfrak{p})$-th root in $\mathcal{O}^*(\Omega)$, where $r(\mathfrak{p}) = (q-1)^2$, if d is odd, and $r(\mathfrak{p}) = (q-1)^2(q+1)$, if d is even. (Incidentally, the latter also follows from Lemma 6.7.) Let $D_{\mathfrak{p}}$ be such a root. By Theorem 3.20 of [8], page 199 the latter transforms under $\Gamma_0(\mathfrak{p})$ through a certain character $\omega_{\mathfrak{p}} : \Gamma_0(\mathfrak{p}) \to \mathbb{C}^*_\infty$ of order $q-1$ such that $\omega_{\mathfrak{p}}^{(q-1)/t(\mathfrak{p})}$ is trivial on $\Gamma_2(\mathfrak{p})$ using the notations of the proof of Proposition 8.18. Hence $D_{\mathfrak{p}}^{(q-1)/t(\mathfrak{p})}$ defines a rational function on $X_2(\mathfrak{p})$ whose divisor generates the pull-back of the subgroup above. $\Box$

Definition 9.4. Let l be a prime dividing $t(\mathfrak{p})$. We are going to construct a group scheme $\mathcal{D}(\mathfrak{p})[l]$ which will play a role similar to $\mathcal{S}(\mathfrak{p})[l] \oplus \mathcal{C}(\mathfrak{p})[l]$ for Eisenstein primes l not dividing $t(\mathfrak{p})$. Let $l(\mathfrak{p})$ be the largest l-power dividing $t(\mathfrak{p})$. Assume first that l divides $\frac{N(\mathfrak{p})}{l(\mathfrak{p})}$. In light of the proposition above it is clear that in this case there is an $x \in \mathcal{S}(\mathfrak{p})$ and a $y \in \mathcal{C}(\mathfrak{p})$ such that

(i) the order of x and y are both equal to $l \cdot l(\mathfrak{p})$,
(ii) we have $lx = ly \in \mathcal{S}(\mathfrak{p}) \cap \mathcal{C}(\mathfrak{p})$,
(iii) the natural topological generator Frob of the maximal constant field extension of F maps x to $(1 + \alpha l(\mathfrak{p}))x$ for some $1 \leq \alpha < l$ integer.

Property (iii) holds because the Galois module generated by x is isomorphic to $\mu_{l \cdot l(\mathfrak{p})}$ by property (i). We define $\mathcal{D}(\mathfrak{p})[l]$ as the group generated by $u = x - y$ and $v = \alpha l(\mathfrak{p})x = \alpha l(\mathfrak{p})y$.

Lemma 9.5. *The group $\mathcal{D}(\mathfrak{p})[l]$ is l-torsion, Galois-invariant and as a Galois module everywhere unramified.*

Proof. The order of u, v is l by (i) and (ii) of the preceding paragraph above, so the first claim holds. The element v is fixed by the absolute Galois group and the latter acts on u through its maximal unramified quotient. By (iii) above $\mathrm{Frob}(u) = u + v$, so the last two claims are true as well. $\Box$

Remark 9.6. By the above $\mathcal{D}(\mathfrak{p})[l]$ contains $\mathcal{S}(\mathfrak{p})[l]$ and its quotient by this subgroup is a constant Galois module of order l which will be denoted by $\mathcal{F}(\mathfrak{p})[l]$. The simple construction above does not exist when l does not divide $\frac{N(\mathfrak{p})}{l(\mathfrak{p})}$. In this case we will give another, more involved construction which will be denoted by $\mathcal{D}(\mathfrak{p})[l]$, too. Actually this case occurs, here is a little analysis. First assume that d is odd. Since $t(\mathfrak{p})$ is the greatest common divisor of d and $q-1$ in this case, we may compute as follows:

$$N(\mathfrak{p}) = \sum_{k=0}^{d-1}(1+(q-1))^k \equiv \sum_{k=0}^{d-1} 1+k(q-1) \equiv d+(q-1)\frac{d(d-1)}{2} \equiv d \mod l \cdot l(\mathfrak{p}).$$

Hence the phenomenon occurs if and only if $l \cdot l(\mathfrak{p})$ does not divide d. Now we consider the case when d is even. In this case $t(\mathfrak{p})$ is the greatest common divisor of $d/2$ and $q-1$, so we may compute as follows:

$$\begin{aligned} N(\mathfrak{p}) &= \sum_{k=0}^{d/2-1} (1+(q-1))^{2k} \\ &\equiv \sum_{k=0}^{d/2-1} 1+2k(q-1) \equiv \frac{d}{2} + (q-1)\frac{d(d-2)}{4} \equiv \frac{d}{2} \bmod l \cdot l(\mathfrak{p}). \end{aligned}$$

Hence the phenomenon occurs if and only if $l \cdot l(\mathfrak{p})$ does not divide $d/2$. Obviously these conditions can always be satisfied by choosing an appropriate d.

Notation 9.7. We start our construction by introducing a set of new notations and definitions. Every $\alpha \in \mathbf{f}_\mathfrak{p}$ is represented by a unique element of $\mathbb{F}_q[T]$ whose degree is less then $\deg(\mathfrak{p})$, which will be denoted by the same symbol by abuse of notation. Let $\Gamma(\mathfrak{p}) \triangleleft GL_2(A)$ be the principal congruence subgroup of level $\mathfrak{p}$, that is the kernel of the reduction map $GL_2(A) \to GL_2(A/\mathfrak{p})$. For every $\underline{0} \neq (\alpha, \beta) \in \mathbf{f}_\mathfrak{p}^2$ let $(\alpha : \beta)$ denote the set of points $(a : b) \in \mathbb{P}^1(F)$ where a and b are in A, they are relatively prime and $(a,b) \equiv (\alpha, \beta) \mod \mathfrak{p}$. This set is an orbit of the natural left action of $\Gamma(\mathfrak{p})$ on $\mathbb{P}^1(F)$. As the quotient $\Gamma(\mathfrak{p})\backslash\mathbb{P}^1(F)$ is the set of cusps of the Drinfeld modular curve $\Gamma(\mathfrak{p})\backslash\Omega$ parameterizing Drinfeld modules of rank two equipped with a full level $\mathfrak{p}$-structure, we may identify the set $(\alpha : \beta)$ and the cusp it represents.

Definition 9.8. Let $\pi : \mathbf{f}_\mathfrak{p}^* \to \mathbf{f}_\mathfrak{p}^*/\mathbb{F}_q^*$ be the canonical surjection and let $I \subset \mathbf{f}_\mathfrak{p}^*$ be a complete set of representatives of the cosets of the projection π. We will specify a convenient choice of I later. Let $\phi : \mathbf{f}_\mathfrak{p}^*/\mathbb{F}_q^* \to \mu_l \subseteq \mathbb{F}_q^*$ be the unique surjection onto the l-th roots of unity. For every $\alpha \in \mathbf{f}_\mathfrak{p}^*$ let $\overline{\alpha}$ denote $\phi \circ \pi(\alpha)$ and for every $d \in A$ not in $\mathfrak{p}$ let $\overline{d}$ similarly denote the value of $\phi \circ \pi$ on the reduction of d mod $\mathfrak{p}$ by slight abuse of notation. For every $x \in \mu_l$ let $C_I(x) \subset \mathbf{f}_\mathfrak{p}^*$ be the set $\{\alpha \in I | \overline{\alpha} = x\}$. For any ring R let $R[\mu_l]_0$ denote the set of all R-valued functions on μ_l whose sum over the elements of μ_l is zero. For every $D \in \mathbb{Z}[\mu_l]_0$ we define the holomorphic function $\epsilon_D : \Omega \to \mathbb{C}_\infty^*$ as the product:

$$\epsilon_D(z) = \prod_{x \in \mu_l} \prod_{\alpha \in C_I(x)} \epsilon_\mathfrak{p}(0,\alpha)(z)^{D(x)}.$$

Definition 9.9. Let $Y_{\#l}(\mathfrak{p}) \to Y_0(\mathfrak{p})$ denote the unique covering intermediate of the covering $Y_2(\mathfrak{p}) \to Y_0(\mathfrak{p})$ which is a cyclic Galois covering of order l. Let $J_{\#l}(\mathfrak{p})$ denote the Jacobian of the unique geometrically irreducible non-singular projective curve $X_{\#l}(\mathfrak{p})$ containing $Y_{\#l}(\mathfrak{p})$. The kernel of the map $J_0(\mathfrak{p}) \to J_{\#l}(\mathfrak{p})$ induced by Picard functoriality is the unique subgroup of the Shimura group of order l. The set of geometric points of $X_{\#l}(\mathfrak{p})$ in the complement of $Y_{\#l}(\mathfrak{p})$ are the cusps of $X_{\#l}(\mathfrak{p})$. The quotients $\Gamma_1(\mathfrak{p})\backslash\Omega$ and $\Gamma_{\#l}(\mathfrak{p})\backslash\Omega$ of the arithmetic subgroups

$$\begin{aligned}\Gamma_1(\mathfrak{p}) =& \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O})|c \equiv 0 \bmod \mathfrak{p}, a \equiv 1 \bmod \mathfrak{p}\} \text{ and} \\ \Gamma_{\#l}(\mathfrak{p}) =& \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O})|c \equiv 0 \bmod \mathfrak{p}, \overline{a} = 1\}\end{aligned}$$

of $GL_2(A)$ are the modular curves $Y_1(\mathfrak{p})$ and $Y_{\#l}(\mathfrak{p})$, respectively. Since for every subgroup $\Gamma \leq GL_2(A)$ the set of cusps of the modular curve $\Gamma\backslash\Omega$ is the quotient $\Gamma\backslash\mathbb{P}^1(F)$, the set

$$\{(\alpha : 0)|0 \neq \alpha \in \mathbf{f}_{\mathfrak{p}}\} \cup \{(0 : \beta)|0 \neq \beta \in \mathbf{f}_{\mathfrak{p}}\}$$

is a full set of representatives for the cusps of $Y_1(\mathfrak{p})$. It is also clear that set of sets above also represent the cusps of $Y_{\#l}(\mathfrak{p})$ and the sets $(\alpha : 0)$ and $(\beta : 0)$ (respectively $(0 : \alpha)$ and $(0 : \beta)$) represent the same cusp if and only if $\overline{\alpha} = \overline{\beta}$.

Proposition 9.10. *The function ϵ_D is a modular unit on $Y_{\#l}(\mathfrak{p})$ defined over F.*

Proof. For every $(\alpha, \beta) \in \mathbf{f}_{\mathfrak{p}}^2$ we have the following transformation law:

$$\epsilon_{\mathfrak{p}}(\alpha,\beta)\left(\frac{az+b}{cz+d}\right) = \frac{1}{cz+d}\epsilon_{\mathfrak{p}}(a\alpha + c\beta, b\alpha + d\beta)(z), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A).$$

From this formula it is clear the every holomorphic function which is the the product of functions of the form $\epsilon_{\mathfrak{p}}(\alpha,\beta)(z)/\epsilon_{\mathfrak{p}}(\alpha',\beta')(z)$, such as ϵ_D, is invariant under the action of $\Gamma(\mathfrak{p})$, so it defines a holomorphic function on the Drinfeld modular curve $Y(\mathfrak{p}) = \Gamma(\mathfrak{p})\backslash\Omega$ parameterizing Drinfeld modules with full level $\mathfrak{p}$-structure. Moreover every function on $Y(\mathfrak{p})$ arising from such a quotient is the base change to $\mathbb{C}_\infty$ of the universal modular object associating to every rank two Drinfeld module $\psi : A \to K\{\tau\}$ of general characteristic equipped with a level structure $\iota : \mathbf{f}_{\mathfrak{p}}^2 \to \psi[\mathfrak{p}]$ the fraction $\iota(\alpha,\beta)(z)/\iota(\alpha',\beta')$, so it is a modular unit defined over F. Hence we only have to show that the function ϵ_D is actually invariant under the action of $\Gamma_{\#l}(\mathfrak{p})$, too.
For every $\beta \in \mathbf{f}_{\mathfrak{p}}^*$ and $\alpha \in C_I(x)$ there is a unique $\alpha_\beta \in C_I(\overline{\beta}x)$ and a $t_\alpha(\beta) \in \mathbb{F}_q^*$ such that $\beta\alpha = t_\alpha(\beta)\alpha_\beta$. Clearly the map $C_I(x) \to C_I(\overline{\beta}x)$ given by the rule $\alpha \mapsto \alpha_\beta$ is bijective. Hence

$$\prod_{\alpha \in C_I(x)} t_\alpha(\beta) \cdot \prod_{\gamma \in C_I(\overline{\beta}x)} \gamma = \prod_{\alpha \in C_I(x)} t_\alpha(\beta)\alpha_\beta = \beta^{\frac{q^d-1}{l(q-1)}} \cdot \prod_{\alpha \in C_I(x)} \alpha.$$

Substituting the equation above into the third line of the equation below we get the following identity:

$$\begin{aligned}\epsilon_D\left(\frac{az+b}{cz+d}\right) &= \prod_{x\in\mu_l}\prod_{\alpha\in C_I(x)}\frac{1}{(cz+d)^{D(x)}}\epsilon_{\mathfrak{p}}(0,d\alpha)(z)^{D(x)}\\ &= \prod_{x\in\mu_l}(cz+d)^{-\frac{D(x)(q^d-1)}{l(q-1)}}\prod_{\alpha\in C_I(x)}\epsilon_{\mathfrak{p}}(0,t_\alpha(d)\alpha_d)(z)^{D(x)}\\ &= \prod_{x\in\mu_l}\prod_{\alpha\in C_I(x)}t_\alpha(d)^{D(x)}\cdot\prod_{y\in\mu_l}\prod_{\beta\in C_I(\overline{d}y)}\epsilon_{\mathfrak{p}}(0,\beta)(z)^{D(y)}\\ &= \prod_{\alpha\in I}\alpha^{D(\overline{\alpha})-D(\overline{d\alpha})}\cdot\epsilon_{D(\overline{d}\cdot)}(z),\quad\forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma_0(\mathfrak{p}),\end{aligned}$$

where we also used the transformation law at the start of our proof in the first equation and the simple identity $\epsilon_{\mathfrak{p}}(\gamma\alpha,\gamma\beta)(z)=\gamma\epsilon_{\mathfrak{p}}(\alpha,\beta)(z)$ valid for all $\gamma\in\mathbb{F}_q^*$ in the third equation. From this identity the claim follows immediately. $\square$

Lemma 9.11. *For any $0\neq z\in A\subset\mathbb{A}_f^*$ and $(\alpha,\beta)\in(\mathbf{f}_{\mathfrak{p}})^2$ we have:*

$$\int_{F\backslash\mathbb{A}}r(\epsilon_{\mathfrak{p}}(\alpha,\beta))(\begin{pmatrix}z^{-1}&x\\0&1\end{pmatrix})d\mu(x)=1-\rho(\alpha)\rho(\beta)-q^{1+\deg(\alpha z)-\deg(\mathfrak{p})}(1-\rho(\alpha)).$$

Proof. Recall our convention which for every $v\in\mathbb{A}_f^*$ denote the unique idele whose finite component is v and whose ∞-adic component is 1 by the symbol v as well. The equation above should be understood in this sense. By the Limit Formula 4.8 the restriction of $r(\epsilon_{\mathfrak{p}}(\alpha,\beta))$ onto $B(\mathbb{A})$ is the limit of automorphic forms, so in particular it is $B(F)$-invariant. Hence the integral on the right hand side in the equation above, which we will denote by $r(\epsilon_{\mathfrak{p}}(\alpha,\beta))^0(z^{-1})$, is well-defined. Fix an $f\in A$ generator of the ideal $\mathfrak{p}$. For all $\alpha\in\mathbf{f}_{\mathfrak{p}}$ we have:

$$\zeta_{\mathfrak{p}}(\alpha,z^{-1},s)=\sum_{\substack{0\neq u\in\mathbb{F}_q[T]\\ u\equiv\alpha z \bmod (zf)}}q^{-s\deg(u)}.$$

Applying the same argument as in the proof of Proposition 5.8, we get that:

$$\zeta_{\mathfrak{p}}(\alpha,z^{-1},s)=(1-\rho(\alpha))q^{-s\deg(\alpha z)}+\frac{(q-1)q^{-s\deg(fz)}}{1-q^{1-s}}.$$

An immediate consequence of this equation and Proposition 5.2 is that the function $E_{\mathfrak{p}}(\alpha,\beta,\cdot,s)^0(z^{-1})$, originally defined for $\mathrm{Re}(s)>1$ only, has a meromorphic continuation to the whole complex plane and

$$E_{\mathfrak{p}}(\alpha,\beta,\cdot,s)^0(z^{-1})=-\rho(\alpha)\rho(\beta)-q^{1+\deg(\alpha z)-\deg(\mathfrak{p})}(1-\rho(\alpha))+\frac{q^{1+\deg(z)}}{q+1},$$

arguing the same was as in the proof of Proposition 5.8 and using the fact that $|\mathfrak{p}|=q^{-\deg(\mathfrak{p})}$. Hence by the Limit Formula 4.8 the following equation holds:

$$\begin{aligned}r(\epsilon_{\mathfrak{p}}(\alpha,\beta))^0(z^{-1}) =& E_{\mathfrak{p}}(\alpha,\beta,\cdot,0)^0(z^{-1})-E_{\mathfrak{p}}(0,0,\cdot,0)^0(z^{-1}))\\ =&1-\rho(\alpha)\rho(\beta)-q^{1+\deg(\alpha z)-\deg(\mathfrak{p})}(1-\rho(\alpha)).\ \square\end{aligned}$$

Proposition 9.12. *For any $D \in \mathbb{Z}[\mu_l]_0$ and $\beta \in \mathbf{f}_{\mathfrak{p}}^*$ the order of vanishing of the modular unit ϵ_D at the cusp $(0:\beta)$ is zero and at the cusp $(\beta:0)$ is equal to:*

$$\frac{1}{1-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta})q^{\deg(\alpha)}.$$

Proof. Let $\mathrm{ord}_{(\alpha:\beta)}(u)$ denote the order of vanishing of any modular unit u on the curve $Y_{\#l}(\mathfrak{p})$ at the cusp $(\alpha:\beta)$. Let $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(\mathfrak{p})$ be a matrix such that $d \equiv \beta \mod \mathfrak{p}$. Then:

$$\begin{aligned}\mathrm{ord}_{(0:\beta)}\epsilon_D(z) =& \mathrm{ord}_{(0:\beta)}\epsilon_{D(\overline{\beta}^{-1}\cdot)}(\frac{az+b}{cz+d}) = \mathrm{ord}_{(0:1)}\epsilon_{D(\overline{\beta}^{-1}\cdot)}(z) = \frac{r(\epsilon_{D(\overline{\beta}^{-1}\cdot)})^0}{q-1}\\ =& \frac{1}{q^2-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta})r(\epsilon_{\mathfrak{p}}(0,\alpha))^0(1) = \frac{1}{q^2-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta}) = 0.\end{aligned}$$

Let us explain why this sequence of equalities hold. The first equation is the consequence of the transformation rule we derived at the end of the proof of Proposition 9.10. The second equation follows from the fact that the image of the cusp $(0:1)$ under the automorphism of $Y_{\#l}(\mathfrak{p})$ induced by $\begin{pmatrix} a & b \\ c & d\end{pmatrix}$ is the cusp $(0:\beta)$. The group $\Gamma_{\#l}(\mathfrak{p})$ contains $B(A)$, so the third equation is just a special case of Proposition 9.2. Note that for every $g: F\backslash\mathbb{A} \to \mathbb{C}$ continuous and $\mathcal{O}_f$-translation invariant function there is a unique $g_\infty : A\backslash F_\infty \to \mathbb{C}$ continuous function such that $g(x) = g_\infty(x)$ for every $x \in F_\infty$. Moreover

$$\int_{F\backslash\mathbb{A}} g\mathrm{d}\mu(x) = \mu_f(\mathcal{O}_f)\int_{A\backslash F_\infty} g_\infty(x)\mathrm{d}\mu_\infty(x)$$

using the notation of Definition 5.1. Hence the fourth equation follows from the relation between the usual van der Put derivative and its adelic version introduced in Notation 4.4. The fifth equation is just a special case of Lemma 9.11 and the last equation holds by definition.

For any $\begin{pmatrix} h & j \\ m & n\end{pmatrix} \in \Gamma_{\#l}(\mathfrak{p})$ we have $hn \in \mathbb{F}_q^* \subset \mathbf{f}_{\mathfrak{p}}^* \mod \mathfrak{p}$ and $\overline{h}=1$ by definition, hence the equation $\overline{n}=1$ also holds as $\mathbb{F}_q^*$ is in the kernel of $\phi\circ\pi$. Therefore the group $\Gamma_{\#l}(\mathfrak{p})$ is normalized by the matrix $\begin{pmatrix} 0 & 1 \\ f & 0\end{pmatrix}$, where $f \in A$ is again a generator of the prime ideal $\mathfrak{p}$. Hence this matrix induces an involution of the modular curve $Y_{\#l}(\mathfrak{p})$ exchanging the cusps $(0:\beta)$ and $(\beta:0)$. For every $H \in \mathbb{Z}[\mu_l]_0$ we define the holomorphic function $\widehat{\epsilon}_H : \Omega \to \mathbb{C}_\infty^*$ as the product:

$$\widehat{\epsilon}_H(z) = \prod_{x\in\mu_l}\prod_{\alpha\in C_I(x)}\epsilon_{\mathfrak{p}}(\alpha,0)(fz)^{H(x)}.$$

Then the transformation law at the start of the proof of Proposition 9.10 imply that

$$\widehat{\epsilon}_H(\frac{1}{fz}) = \epsilon_H(z),$$

in particular $\widehat{\epsilon}_H$ is also a modular unit on the curve $Y_{\# l}(\mathfrak{p})$. Therefore

$$\begin{aligned}
\mathrm{ord}_{(\beta:0)}\epsilon_D(z) =&\mathrm{ord}_{(\beta:0)}\epsilon_{D(\overline{\beta}^{-1}\cdot)}(\frac{az+b}{cz+d}) = \mathrm{ord}_{(1:0)}\epsilon_{D(\overline{\beta}^{-1}\cdot)}(z)\\
=&\mathrm{ord}_{(1:0)}\widehat{\epsilon}_{D(\overline{\beta}^{-1}\cdot)}(\frac{1}{fz}) = \mathrm{ord}_{(0:1)}\widehat{\epsilon}_{D(\overline{\beta}^{-1}\cdot)}(z) = \frac{r(\widehat{\epsilon}_{D(\overline{\beta}^{-1}\cdot)})^0}{q-1}\\
=&\frac{1}{q^2-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta}) r(\epsilon_{\mathfrak{p}}(\alpha,0)(f\cdot))^0(1)\\
=&\frac{1}{q^2-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta}) r(\epsilon_{\mathfrak{p}}(\alpha,0))^0(f^{-1})\\
=&\frac{1}{q^2-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta})(1-q^{1+\deg(\alpha)})\\
=&\frac{1}{1-q}\sum_{\alpha\in I} D(\overline{\alpha}/\overline{\beta}) q^{\deg(\alpha)}. \ \square
\end{aligned}$$

Corollary 9.13. *Let $D\in\mathbb{Z}[\mu_l]_0$ be a function such that $D(y) \bmod l$ does not depend on $y\in\mu_l$. Then the divisor of the modular unit ϵ_D is divisible by l.*

Proof. The property of D in the claim above is clearly invariant under the action of the group ring $\mathbb{Z}[\mu_l]$, hence it is sufficient to show that

$$\sum_{y\in\mu_l} D(y) \sum_{\alpha\in C_I(y)} q^{\deg(\alpha)} \equiv 0 \mod (q-1)l$$

when $D(y) = 1 + lC(y)$ for some function $C:\mu_l\to\mathbb{Z}$. We have

$$\begin{aligned}
\sum_{\alpha\in C_I(y)} q^{\deg(\alpha)} =& \sum_{\alpha\in C_I(y)} (1+(q-1))^{\deg(\alpha)}\\
\equiv& \sum_{\alpha\in C_I(y)} (1+(q-1)\deg(\alpha)) \mod (q-1)l
\end{aligned}$$

for any $y\in\mu_l$, therefore

$$\begin{aligned}
\sum_{y\in\mu_l} D(y)\sum_{\alpha\in C_I(y)} q^{\deg(\alpha)} \equiv&\frac{q^d-1}{(q-1)l}\sum_{y\in\mu_l} D(y)\\
&+(q-1)\sum_{y\in\mu_l}(1+lC(y))\sum_{\alpha\in C_I(y)}\deg(\alpha)\\
\equiv&(q-1)\sum_{\alpha\in I}\deg(\alpha) \equiv (q-1)\sum_{j=0}^{d-1} jq^j\\
\equiv&(q-1)\sum_{j=0}^{d-1} j \equiv \frac{(q-1)d(d-1)}{2} \mod (q-1)l.
\end{aligned}$$

If l is odd then 2 is invertible modulo l and l divides d. If $l = 2$ then d is even and l divides $d/2$. □

Lemma 9.14. *(i) If $M \leq \mathbb{Z}[\mu_l]_0$ is a μ_l-invariant $\mathbb{Z}$-submodule then M is either trivial or its $\mathbb{Z}$-rank is $l-1$.*
(ii) If $M_1 \lneqq M_2 \leq \mathbb{Z}_l[\mu_l]_0$ are non-trivial μ_l-invariant $\mathbb{Z}_l$-submodules and the natural μ_l-action on the quotient M_2/M_1 is trivial then M_2/M_1 is a cyclic group of order l.

Proof. The $\overline{\mathbb{Q}}$-span $M_{\overline{\mathbb{Q}}}$ of M in the $\overline{\mathbb{Q}}$-vectorspace $\overline{\mathbb{Q}}[\mu_l]_0$ has the same $\overline{\mathbb{Q}}$-rank as the $\mathbb{Z}$-rank of the free $\mathbb{Z}$-module M. Since $M_{\overline{\mathbb{Q}}}$ is also μ_l-invariant, it is the direct sum of some of the irreducible μ_l-invariant subspaces. On the other hand it is also fixed by the natural action of the absolute Galois group of $\mathbb{Q}$ on the tensor product $\overline{\mathbb{Q}}[\mu_l]_0 = \mathbb{Q}[\mu_l]_0 \otimes \overline{\mathbb{Q}}$. This action permutes the irreducible μ_l-invariant subspaces transitively, therefore $M_{\overline{\mathbb{Q}}}$ is either trivial or it is the whole $\overline{\mathbb{Q}}$-vector space.

We start the proof of the second claim by noting that the first claim also holds when the role of the ring $\mathbb{Z}$ is played by the ring $\mathbb{Z}_l$. The proof is identical. Hence for every non-trivial μ_l-invariant $\mathbb{Z}_l$-submodule $M \leq \mathbb{Z}_l[\mu_l]_0$ there is a unique natural number $n(M) \in \mathbb{N}$ such that $l^{n(M)}\mathbb{Z}_l[\mu_l]_0 \leq M$ but $l^{n(M)-1}\mathbb{Z}_l[\mu_l]_0 \not\leq M$. Let σ be a generator of μ_l. We are going to show that there is a natural number $m(M) \in \mathbb{N}$ such that M is the image of the endomorphism $x \mapsto (1-\sigma)^{m(M)}$ by induction on $n(M)$. The μ_l-invariant subgroups of the quotient $\mathbb{Z}_l[\mu_l]_0/\mathbb{Z}_l[\mu_l]_0 = \mathbb{F}_l[\mu_l]_0$ are exactly the proper ideals of the group ring $\mathbb{F}_l[\mu_l] = \mathbb{F}_l[T]/(T-1)^l$. As the latter form a chain whose Jordan-Hölder components are all isomorphic to $\mathbb{F}_l$, the claim is now obvious when $n(M) = 1$. Since the map $x \mapsto (1-\sigma)^{m(M)}$ is injective, the general case follows using induction and the same argument where the role of $\mathbb{Z}_l[\mu_l]_0$ is played by $M + l^{n(M)-1}\mathbb{Z}_l[\mu_l]_0$. Now claim (ii) follows. □

Definition 9.15. Let $\mathcal{F}_{\#l}(\mathfrak{p}) \subset J_{\#l}(\mathfrak{p})(\overline{F})$ denote the Galois module generated by the linear equivalence classes of degree zero divisors supported on the cusps of $X_{\#l}(\mathfrak{p})$ mapping to the cusp 0 of the curve $X_0(\mathfrak{p})$. Moreover let $\mathcal{F}(\mathfrak{p})[l] \subseteq \mathcal{F}_{\#l}(\mathfrak{p})$ denote subgroup of elements of l-primary order fixed by the decking transformations of the cover $X_{\#l}(\mathfrak{p}) \to X_0(\mathfrak{p})$. The next proposition partially justifies our choice of notation.

Proposition 9.16. *The group $\mathcal{F}(\mathfrak{p})[l]$ is cyclic of order l.*

Proof. Let $J \subset \mathrm{Ker}(\phi \circ \pi) \subset \mathbf{f}_{\mathfrak{p}}^*$ be a complete set of representatives of the cosets of the restriction of the projection π onto $\mathrm{Ker}(\phi \circ \pi)$. Moreover let ξ be a generator of the cyclic group $\mathbf{f}_{\mathfrak{p}}^*$. We define the set I as the union $\cup_{j=0}^{l-1}\xi^j J$. Pick a $\begin{pmatrix} h & j \\ m & n \end{pmatrix} \in \Gamma_0(\mathfrak{p})$ matrix with $n = \xi$ and let $D \in \mathbb{Z}[\mu_l]_0$ be the function with $D(1) = 1$, $D(\overline{\xi}) = -1$ and all the other values are zero. Then

$$\prod_{j=0}^{l-1} \epsilon_D(\begin{pmatrix} h & j \\ m & n \end{pmatrix}^j z) = \prod_{\alpha \in J} \frac{\epsilon_{\mathfrak{p}}(0,\alpha)(z)}{\epsilon_{\mathfrak{p}}(0,\xi\alpha)(z)} \cdot \prod_{\alpha \in J} \frac{\epsilon_{\mathfrak{p}}(0,\xi\alpha)(z)}{\epsilon_{\mathfrak{p}}(0,\xi^2\alpha)(z)} \cdots \prod_{\alpha \in J} \frac{\epsilon_{\mathfrak{p}}(0,\xi^{l-1}\alpha)(z)}{\epsilon_{\mathfrak{p}}(0,\xi^l\alpha)(z)}$$
$$= \prod_{\alpha \in J} \frac{\epsilon_{\mathfrak{p}}(0,\alpha)(z)}{\epsilon_{\mathfrak{p}}(0,\xi^l\alpha)(z)} = \prod_{\alpha \in J} t_{\xi^l}(\alpha)^{-1} = \xi^{\frac{q^d-1}{1-q}} \notin (F^*)^l$$

using the notation of the proof of Proposition 9.10. Let $\mathcal{Y}$ and $\mathcal{P}$ denote the group of degree zero divisors supported on the cusps of $X_{\#l}(\mathfrak{p})$ mapping to the cusp 0 of the curve $X_0(\mathfrak{p})$ and its subgroup of principal divisors, respectively. Let $\mathcal{U}$ denote the group of divisors of units of the form ϵ_D introduced in Definition 9.8. Fix a non-zero element $\sigma \in \mu_l$. For every $y \in \mu_l$ let $z \mapsto z^y$ denote the decking transformation of $X_{\#l}(\mathfrak{p})$ corresponding to y. It is characterized by the property that it maps the cusp $(0:1)$ to $(0:\alpha)$ where $\overline{\alpha} = y$. For every non-zero F-rational function g on the curve $X_{\#l}(\mathfrak{p})$ whose divisor lies in $\mathcal{P}$ the divisor of the product $N(g) = \prod_{y \in \mu_l} g(z^y)$ is μ_l-invariant, hence it is trivial. Therefore $N(g)$ is constant. It is also clear that its class in $F^*/(F^*)^l$ only depends on the divisor of g modulo l. We let N denote the corresponding homomorphism $\mathcal{P}/l\mathcal{P} \to F^*/(F^*)^l$ as well. It is clear from the above that this homomorphism is non-trivial restricted to $\mathcal{U}/l\mathcal{U}$. An immediate consequence is that the μ_l-invariant modules $\mathcal{P}$ and $\mathcal{U}$ are non-trivial. Hence they have $\mathbb{Z}$-rank $l-1$ by claim (i) of Lemma 9.14. In particular the group $\mathcal{F}_{\#l}(\mathfrak{p})$ is torsion. Note that the map N is μ_l-invariant, so it induces an embedding of $\mathcal{U}/(1-\sigma)\mathcal{U}$ into $F^*/(F^*)^l$. We claim that $\mathcal{U} \otimes \mathbb{Z}_l = \mathcal{P} \otimes \mathbb{Z}_l$. If this were false then there would be an element H of $\mathcal{P}$ such that $(1-\sigma)H$ lies in $\mathcal{U}$ but it does not lie in $(1-\sigma)\mathcal{U}$ by claim (ii) of Lemma 9.14. The latter can be applied as the module $\mathcal{Y} \otimes \mathbb{Z}_l$ is isomorphic to $\mathbb{Z}_l[\mu_l]_0$ as a μ_l-module. Since $N(g(z)/g(z^\sigma)) = 1$ for any F-rational function g on $X_\#(\mathfrak{p})$ whose divisor is in $\mathcal{P}$, we get a contradiction. On the other hand we claim that $\mathcal{P} \otimes \mathbb{Z}_l$ is strictly smaller than $\mathcal{Y} \otimes \mathbb{Z}_l$. By the above we only have to prove this for $\mathcal{U} \otimes \mathbb{Z}_l$. It will be enough to show that the unique smallest μ_l-invariant $\mathbb{Z}_l$-submodule of $\mathcal{U} \otimes \mathbb{Z}_l$ strictly larger than $l(\mathcal{U} \otimes \mathbb{Z}_l)$ is contained in $l(\mathcal{Y} \otimes \mathbb{Z}_l)$. But this is exactly the content of Corollary 9.13. Therefore the l-torsion of $\mathcal{F}_{\#l}(\mathfrak{p})$ is non-trivial, and the claim now follows from claim (ii) of Lemma 9.14. □

Definition 9.17. We define $\mathcal{D}(\mathfrak{p})[l] \subset J_0(\mathfrak{p})(\overline{F})$ to be the pre-image of $\mathcal{F}(\mathfrak{p})[l]$ under the map $J_0(\mathfrak{p}) \to J_{\#l}(\mathfrak{p})$ induced by Picard functoriality. In this paragraph let $\overline{S}$ denote the base change of the F-scheme S to $\overline{F}$. Since the map $X_{\#l}(\mathfrak{p}) \to X_0(\mathfrak{p})$ is a Galois covering with Galois group μ_l, there is a Hochschild-Serre spectral sequence $H^p(\mu_l, H^q(\overline{X_{\#l}(\mathfrak{p})}, \mathbb{Q}_l/\mathbb{Z}_l)) \Rightarrow H^{p+q}(\overline{X_0(\mathfrak{p})}, \mathbb{Q}_l/\mathbb{Z}_l))$ which gives rise to an exact sequence

$$H^1(\overline{X_0(\mathfrak{p})}, \mathbb{Q}_l/\mathbb{Z}_l)) \to H^1(\overline{X_{\#l}(\mathfrak{p})}, \mathbb{Q}_l/\mathbb{Z}_l)^{\mu_l} \to H^2(\mu_l, H^0(\overline{X_{\#l}(\mathfrak{p})}, \mathbb{Q}_l/\mathbb{Z}_l)) = 0$$

By definition $\mathcal{D}(\mathfrak{p})[l]$ contains $\mathcal{S}(\mathfrak{p})[l]$ and its quotient by this subgroup is isomorphic to the Galois module $\mathcal{F}(\mathfrak{p})[l]$ by the above. Also note that $\mathcal{D}(\mathfrak{p})[l]$ is

l-torsion as our choice of notation indicates. We argue as follows: the composition of the morphisms $J_0(\mathfrak{p}) \to J_{\#l}(\mathfrak{p})$ and $J_{\#l}(\mathfrak{p}) \to J_0(\mathfrak{p})$ induced by Picard and Albanese functoriality respectively is multiplication by l on $J_0(\mathfrak{p})$. On the other hand the image of every element of $\mathcal{F}(\mathfrak{p})[l]$ under the Albanese map is represented by the direct image of a divisor supported on the pre-image of the cusp 0 under the map $X_{\#l}(\mathfrak{p}) \to X_0(\mathfrak{p})$, hence it must be zero.

Proposition 9.18. *The following holds:*

(*i*) *the Galois modules $\mathcal{S}(\mathfrak{p})[l]$ and $\mathcal{F}(\mathfrak{p})[l]$ are constant of order l,*
(*ii*) *the Galois module $\mathcal{D}(\mathfrak{p})[l]$ is everywhere unramified,*
(*iii*) *both $\mathcal{S}(\mathfrak{p})[l]$ and $\mathcal{D}(\mathfrak{p})[l]$ are $\mathbb{T}(\mathfrak{p})$-invariant and annihilated by the Eisenstein ideal,*
(*iv*) *the exact sequence:*

$$0 \to \mathcal{S}(\mathfrak{p})[l] \to \mathcal{D}(\mathfrak{p})[l] \to \mathcal{F}(\mathfrak{p})[l] \to 0$$

of Galois modules does not split over F,
(*v*) *the intersection of $\mathcal{D}(\mathfrak{p})[l]$ and $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)[l]$ is $\mathcal{S}(\mathfrak{p})[l]$.*

Proof. First consider the case when l divides $N(\mathfrak{p})/l(\mathfrak{p})$. Claims (*i*) and (*ii*) are immediate consequences of Lemma 9.5. In order to show claim (*iii*) it will be sufficient to show that both $\mathcal{C}(\mathfrak{p})$ and $\mathcal{S}(\mathfrak{p})$ are $\mathbb{T}(\mathfrak{p})$-invariant and annihilated by the Eisenstein ideal, since in this case every subgroup of the sum $\mathcal{C}(\mathfrak{p})+\mathcal{S}(\mathfrak{p})$ is fixed by the Eisenstein ideal as it acts on the latter by scalar multiplication. Using the same argument again we are reduced to show that $\mathcal{T}(\mathfrak{p})$ and $\mathcal{M}(\mathfrak{p})$ are $\mathbb{T}(\mathfrak{p})$-invariant and annihilated by the Eisenstein ideal. These groups are obviously Hecke-invariant, and the annihilation by the Eisenstein ideal follows from the Eichler-Shimura relation, spelled out in Lemma 7.16 and Lemma 10.4, respectively. By the proof of Lemma 9.5 the exact sequence above is not even split over F_∞, hence claim (*iv*) holds. The the intersection of $\mathcal{D}(\mathfrak{p})[l]$ and $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)[l]$ contains $\mathcal{S}(\mathfrak{p})[l]$ by Proposition 8.18. If it were larger, then the group scheme $\mathcal{D}(\mathfrak{p})[l]$ would be μ-type over F_∞ which it is not by the above, so claim (*v*) is true.

Now consider the case when l does not divide $N(\mathfrak{p})/l(\mathfrak{p})$. The cusps of $X_{\#l}(\mathfrak{p})$ mapping to the cusp 0 of the curve $X_0(\mathfrak{p})$ are actually defined over F, so the group $\mathcal{F}(\mathfrak{p})[l]$ is constant as a Galois-module. The Galois module $\mathcal{S}(\mathfrak{p})[l]$ is μ-type of order l, so it is constant, too. This proves the first claim. Lemma 8.19 and claim (*i*) implies that $\mathcal{D}$ is unramified at $\mathfrak{p}$. Note that that $\mathcal{D}(\mathfrak{p})[l]$ is a tamely ramified Galois module. It is the extension of the constant Galois module $\mathbb{F}_l$ by itself, so there is an $\mathbb{F}_l$-basis of this module where the Galois action is given by upper triangular matrices with ones on the diagonal. So the Galois action is given by a homomorphism from the absolute Galois group of F into $\mathbb{F}_l$. That is a tame abelian extension of F. As every tamely ramified Galois module which only ramifies at ∞ is in fact everywhere unramified, we get that claim (*ii*) holds.

As we already noted the group $\mathcal{S}(\mathfrak{p})[l]$ is both $\mathbb{T}(\mathfrak{p})$-invariant and Galois-invariant. Hence the quotient module $J_0(\mathfrak{p})(\mathbb{C}^*_\infty)[l]/\mathcal{S}(\mathfrak{p})[l]$ is equipped with a commuting action of $\mathbb{T}(\mathfrak{p})$ and the absolute Galois group which also satisfies the Eichler-Shimura relations. By repeating the arguments above we get that the Galois submodule $\mathcal{F}(\mathfrak{p})[l]$ of the quotient Galois module above is $\mathbb{T}(\mathfrak{p})$-invariant. Therefore its pre-image $\mathcal{D}(\mathfrak{p})[l]$ in $J_0(\mathfrak{p})(\mathbb{C}^*_\infty)[l]$ is also $\mathbb{T}(\mathfrak{p})$-invariant. Since $\mathcal{D}(\mathfrak{p})[l]$ is the extension of a constant Galois module by a μ-type Galois module, the identity $(\mathrm{Frob}_\mathfrak{q}-1)(\mathrm{Frob}_\mathfrak{q}-q^{\deg(\mathfrak{q})})$ holds on $\mathcal{D}(\mathfrak{p})[l]$ for every $\mathfrak{q}\neq\mathfrak{p}$ prime. By subtracting this identity from the Eichler-Shimura relations we get that $\mathrm{Frob}_\mathfrak{q}(T_\mathfrak{q}-1-q^{\deg(\mathfrak{q})})=0$. Since $\mathrm{Frob}_\mathfrak{q}$ is invertible we get that $\mathcal{D}(\mathfrak{p})[l]$ is annihilated by the Eisenstein ideal. This concludes the proof of claim (iii).
We will continue to use the notation introduced in the proof of Proposition 9.16. Take an element H of $\mathcal{Y}$ which represents a non-zero element of $\mathcal{F}(\mathfrak{p})[l]$. Then $(1-\sigma)H$ lies in $\mathcal{P}$ but it does not lie in $(1-\sigma)\mathcal{P}$. Since N is μ_l-invariant, it is trivial on $(1-\sigma)(\mathcal{P}/l\mathcal{P})$, therefore $(1-\sigma)H$ is the divisor of a non-zero rational function e such that $N(e)\notin(F^*)^l$. Assume that claim (iv) is false. Then there is an F-rational divisor E on $X_0(\mathfrak{p})$ whose pull-back E^* to $X_{\#l}(\mathfrak{p})$ is linearly equivalent to H, that is there is a a non-zero F-rational function g such that $H=E^*+(g)$. Since σ fixes this pull-back E^* there is a constant $u\in F^*$ such that $e(z)=ug(z)/g(z^\sigma)$. Hence $N(e)=u^l$ which is a contradiction. Because the Galois module $\mathcal{D}(\mathfrak{p})[l]$ is unramified, it does not split over F_∞ either. Hence claim (v) follows from claim (iv), as we already saw. □

Remark 9.19. The integers $\sum_{\alpha\in C_I(y)}q^{\deg(\alpha)}$ are analogues of the Bernoulli numbers. This is more or less clear from the computations of this chapter, but we will give an alternative argument here. We continue to let f denote a generator of the prime ideal $\mathfrak{p}$. Let $\mathbb{O}$ denote the ring of integers in the extension of $\mathbb{Q}_l$ we get by adjoining the l-th roots of unity. We define the $\mathbb{O}$-valued Dirichlet character χ by requiring that $\chi(f)=0$ and $\chi(g)=\overline{g}$ for every $g\in\mathbb{F}_q[T]$ relatively prime to f, where we consider μ_l as a subset of $\mathbb{O}$. We let U denote $\mathbb{P}^1_{\mathbb{F}_q}-\{\mathfrak{p}\}$ and let $\overline{U}$ denote its base change to $\overline{\mathbb{F}}_q$. By class field theory we have a corresponding Galois representation $\chi:\widehat{\pi}_1^{ab}(U)\to\mathbb{O}^*$ which is tamely ramified at $\mathfrak{p}$ and it is totally split at ∞. More precisely the Artin L-function of χ is

$$L(\chi,t)=\prod_{\mathfrak{p}\neq x\in|\mathbb{P}^1_{\mathbb{F}_q}|}(1-\chi(\mathrm{Fr}_x)t^{\deg(x)})^{-1}=\frac{1}{(1-t)(q-1)}\sum_{f\nmid g\in\mathbb{F}_q[T]}\chi(g)t^{\deg(g)},$$

where $\mathrm{Fr}_x\in\widehat{\pi}_1^{ab}(U)$ is the arithmetic Frobenius at the place x. For every l-adic Galois representation ρ of $\widehat{\pi}_1(U,\infty)$ will use the same symbol to denote the lisse sheaf on U corresponding to ρ as well its base change to $\overline{U}$. By the Grothendieck-Verdier trace formula:

$$L(\chi,t)=\prod_{i=0}^{2}\det(1-Ft|H^1_c(\overline{U},\chi^{-1})^{(-1)^{i+1}},$$

where F is the Frobenius operator acting on the étale cohomology of χ^{-1}. Since χ as a representation of $\widehat{\pi}_1(\overline{U},\infty)$ is irreducible and non-trivial, the groups $H^0_c(\overline{U},\chi^{-1})$ and $H^2_c(\overline{U},\chi^{-1})$ are zero, and by the Ogg-Shafarevich formula the dimension of $H^1_c(\overline{U},\chi^{-1}))$ is $\deg(\mathfrak{p})-2$. Hence $L(\chi,t)$ is a polynomial of degree $\deg(\mathfrak{p})-2$ and

$$L(\chi,t)=\frac{1}{(1-t)(q-1)}\sum_{\substack{0\neq g\in\mathbb{F}_q[T]\\ \deg(g)<\deg(\mathfrak{p})}}\overline{g}\,t^{\deg(d)}=\sum_{y\in\mu_l}\frac{y}{1-t}\cdot\sum_{\alpha\in C_I(y)}t^{\deg(\alpha)}.$$

10. Mazur's Eisenstein decent at primes l not dividing $t(\mathfrak{p})$

Definition 10.1. For the rest of the paper, unless we say otherwise explicitly, we fix an Eisenstein prime l. Introduce the shorthand notation $\mathfrak{E}=\mathfrak{E}_l(\mathfrak{p})$ for the Eisenstein ideal in $\mathbb{T}_l(\mathfrak{p})$. Let $\mathfrak{P}\triangleleft\mathbb{T}_l(\mathfrak{p})$ be the unique prime ideal lying above $\mathfrak{E}$. As $\mathbb{Z}_l$ surjects onto $\mathbb{T}_l(\mathfrak{p})/\mathfrak{E}$ via its natural inclusion into $\mathbb{T}_l(\mathfrak{p})$, clearly $\mathfrak{P}=(\mathfrak{E},l)$. Hence the latter is a maximal ideal with residue field $\mathbb{F}_l$. Let $\eta_{\mathfrak{q}}$ denote the element $T_{\mathfrak{q}}-q^{\deg(\mathfrak{q})}-1\in\mathbb{T}(\mathfrak{p})$, where $\mathfrak{q}\triangleleft A$ is any prime ideal different from $\mathfrak{p}$. Let $\mathfrak{q}\triangleleft A$ be a prime ideal and let $r(T)\in A$ be the unique monic polynomial which generates $\mathfrak{q}$. We say that $\mathfrak{q}$ is a good prime if the following holds:

- (i) the prime ideal $\mathfrak{q}$ is not equal to $\mathfrak{p}$,
- (ii) the image of the reduction of the polynomial $r(T)$ modulo $\mathfrak{p}$ in the quotient $(A/\mathfrak{p})^*/\mathbb{F}_q^*$ is not an l-th power,
- (iii) if l does not divide $t(\mathfrak{p})$ then it also does not divide $q^{\deg(\mathfrak{q})}-1$,
- (iv) if l does divide $t(\mathfrak{p})$ then it does not divide $\deg(\mathfrak{q})$.

Note that every Eisenstein prime l divides $\frac{q^d-1}{q-1}$. This number is the order of the quotient group $(A/\mathfrak{p})^*/\mathbb{F}_q^*$, so the l-power map is not invertible on the latter. Hence the Chebotarev density theorem implies that there are infinitely many good primes.

For the rest of this chapter we assume that l does not divide $t(\mathfrak{p})$, unless we say otherwise explicitly. Now we can state the main result of this section:

Theorem 10.2. *The ideal $\mathfrak{P}$ is generated by l and $\eta_{\mathfrak{q}}$ for every good prime $\mathfrak{q}$.*

As explained in [14], Propositions 15.3 and 16.2, this theorem implies the following

Corollary 10.3. *The completion $\mathbb{T}_{\mathfrak{P}}$ of the Hecke algebra $\mathbb{T}_l(\mathfrak{p})$ at the prime ideal $\mathfrak{P}$ is Gorenstein.*

Before we start to prove Theorem 10.2, let us deduce its main Diophantine application from the corollary above. Let $\mathcal{E}(\mathfrak{p})$ denote the largest torsion subgroup of $J_0(\mathfrak{p})(\overline{F})$ annihilated by the Eisenstein ideal $\mathfrak{E}(\mathfrak{p})\triangleleft\mathbb{T}(\mathfrak{p})$. We will need the following preliminary result.

Lemma 10.4. *The group $\mathcal{E}(\mathfrak{p})$ contains $\mathcal{M}(\mathfrak{p})$.*

Proof. For the sake of simple notation let $J_0(\mathfrak{p})$ denote the Néron model of the Jacobian over X, too. The Cartier dual of a constant p-torsion group scheme is not étale in characteristic p, so the group scheme $\mathcal{M}(\mathfrak{p})$ has no p-torsion. Hence the reduction map injects $\mathcal{M}(\mathfrak{p})$ into $J_0(\mathfrak{p})(\overline{\mathbf{f}}_{\mathfrak{q}})$, for every prime $\mathfrak{q}$ different from $\mathfrak{p}$. The Frobenius endomorphism $\mathrm{Frob}_{\mathfrak{q}}$ of the abelian variety $J_0(\mathfrak{p})_{\mathbf{f}_{\mathfrak{q}}}$ acts as multiplication by $q^{\deg(\mathfrak{q})}$ on the reduction of $\mathcal{M}(\mathfrak{p})$. Therefore the Eichler-Shimura relation implies that the endomorphism $1 - T_{\mathfrak{q}} + q^{\deg(\mathfrak{q})}$ annihilates this group. $\square$

Theorem 10.5. *The group schemes $\mathcal{M}(\mathfrak{p})_l$ and $\mathcal{S}(\mathfrak{p})_l$ are equal for any prime l not dividing $t(\mathfrak{p})$.*

Proof. Clearly the claim only needs demonstration when l is Eisenstein. The Frobenius Frob_∞ at ∞ acts non-trivially on the l-primary subgroup of $\mathcal{M}(\mathfrak{p})$, hence the latter must lie in the torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ annihilated by the ideal $\mathfrak{E}$ according to Lemma 10.4. The latter module is dual to $T_l^\vee/\mathfrak{E}T_l^\vee$, where the subscript $^\vee$ denotes the $\mathbb{T}_l(\mathfrak{p})$-dual. As $\mathbb{T}_{\mathfrak{P}}$ is Gorenstein, the completion of the locally free $\mathbb{T}_l(\mathfrak{p})$-module T_l at $\mathfrak{P}$ is isomorphic to its dual, so the module above is isomorphic to $\mathbb{T}_{\mathfrak{P}}/\mathfrak{E}\mathbb{T}_{\mathfrak{P}}$, because $\mathfrak{E}$ is supported on $\mathfrak{P}$. The latter has the same order as $\mathbb{Z}_l/N(\mathfrak{p})\mathbb{Z}_l$, hence it has the same order as the l-primary component of $\mathcal{S}(\mathfrak{p})$. $\square$

We start our proof of Theorem 10.2 by proving a useful proposition about finite étale group schemes over the base $\mathbb{P}^1_{\mathbb{F}_q} - \{\mathfrak{p}\}$ which will function as a suitable analogue for the criteria for constancy and purity of [14] (Lemma 3.4 on page 57 and Proposition 4.5 on page 59, respectively).

Definition 10.6. In this paragraph, the next proposition and its proof l is any Eisenstein prime. We say that the group scheme G over the base S is μ-type if it is finite, flat and its Cartier dual is a constant group scheme over S. We say that the group scheme G is pure if it is the direct sum of a constant and a μ-type group scheme. Let $\mathbb{Z}/l^n\mathbb{Z}$ and μ_{l^n} denote the constant group scheme of order l^n and its Cartier dual, respectively. We say that a group scheme G is admissible if it is finite, étale and has a filtration by group schemes such that the successive quotients are pure. Clearly all these concepts make sense for the special case of finite Galois modules over fields.

Proposition 10.7. *Let G be an admissible group scheme of l-primary rank over the base $\mathbb{P}^1_{\mathbb{F}_q} - \{\mathfrak{p}\}$ and let $\mathfrak{q}$ be a good prime. Then the group scheme G is constant (resp. μ-type) if and only if it is constant (resp. μ-type) as a Galois module both over $F_{\mathfrak{q}}$ and over F_∞.*

Proof. For the sake of simple notation let U denote $\mathbb{P}^1_{\mathbb{F}_q} - \{\mathfrak{p}\}$ and let $\overline{U}$ denote its base change to $\overline{\mathbb{F}}_p$. First note that the criterion for constancy implies the other criterion by taking the Cartier-dual. In the former case clearly what we have to show is that the cardinality of the étale cohomology group $H^0_{et}(U, G)$

is the same as the rank of G. We are going to show the latter by induction on the rank of G. Since G is admissible, it contains a group scheme H isomorphic to either μ_l or $\mathbb{Z}/l\mathbb{Z}$. The group scheme H is constant as a Galois module over F_∞, hence it is isomorphic to $\mathbb{Z}/l\mathbb{Z}$. Therefore G is an extension:

$$0 \to \mathbb{Z}/l\mathbb{Z} \to G \to M \to 0.$$

The group scheme M is also admissible of l-primary rank which is constant as a Galois module both over $F_\mathfrak{q}$ and over F_∞. Hence by the induction hypothesis M is constant. Therefore it will be enough to show that the coboundary map $\delta : H^0_{et}(U, M) \to H^1_{et}(U, \mathbb{Z}/l\mathbb{Z})$ of the cohomological exact sequence of the short exact sequence above is trivial. Since G is constant as a Galois module both over $F_\mathfrak{q}$ and over F_∞, the coboundary maps $\delta : H^0(F_\mathfrak{q}, M) \to H^1(F_\mathfrak{q}, \mathbb{Z}/l\mathbb{Z})$ and $\delta : H^0(F_\infty, M) \to H^1(F_\infty, \mathbb{Z}/l\mathbb{Z})$ of the base change of the short exact sequence to the spectrum of $F_\mathfrak{q}$ and F_∞ respectively are trivial. (Of course the cohomology groups above are Galois cohomology groups.) Therefore we only have to show that the natural map $H^1_{et}(U, \mathbb{Z}/l\mathbb{Z}) \to H^1(F_\mathfrak{q}, \mathbb{Z}/l\mathbb{Z}) \oplus H^1(F_\infty, \mathbb{Z}/l\mathbb{Z})$ is injective. The cohomology group $H^1_{et}(U, \mathbb{Z}/l\mathbb{Z})$ is equal to the group cohomology $H^1(\widehat{\pi}_1^{ab}(U), \mathbb{Z}/l\mathbb{Z}) = \mathrm{Hom}(\widehat{\pi}_1^{ab}(U), \mathbb{Z}/l\mathbb{Z})$, where $\widehat{\pi}_1^{ab}(U)$ denotes the abelianization of the étale fundamental group of U. The map above is just the evaluation of the corresponding homomorphism $\widehat{\pi}_1^{ab}(U) \to \mathbb{Z}/l\mathbb{Z}$ on the Frobenius elements $\mathrm{Frob}_\mathfrak{q}$ and Frob_∞ in $\widehat{\pi}_1^{ab}(U)$. Hence we only have to prove that the image of $\mathrm{Frob}_\mathfrak{q}$ and Frob_∞ in $\widehat{\pi}_1^{ab}(U)/l\widehat{\pi}_1^{ab}(U)$ generate this group. By class field theory the latter is a consequence of (in fact it is equivalent to) the second condition in the definition of good primes. Let us give a quick proof of this fact. By class field theory the group $\widehat{\pi}_1^{ab}(U)$ is isomorphic to $F^*\backslash\mathbb{A}^*/U_\mathfrak{p}$, where $U_\mathfrak{p}$ is the direct product $\prod_{x\neq\mathfrak{p}}\mathcal{O}_x^*$. Under this identification the Frobenius elements $\mathrm{Frob}_\mathfrak{q}$ and Frob_∞ are represented by ideles $\pi_\mathfrak{q}$ and π_∞ whose divisor is $\mathfrak{q}$ and ∞, respectively, such that all components of π_v, where $v \neq \mathfrak{q}$ or ∞, which are different from $\mathfrak{q}$ or ∞, respectively, are actually equal to one. This identification also implies that there is an exact sequence

$$0 \to \mathcal{O}_\mathfrak{p}^*/(l\mathcal{O}_\mathfrak{p}^*)\mathbb{F}_q^* \to \widehat{\pi}_1^{ab}(U)/l\widehat{\pi}_1^{ab}(U) \to \mathbb{Z}/l\mathbb{Z} \to 0,$$

where the second map is the degree mod l of the divisor of any idele representing the class in $\widehat{\pi}_1^{ab}(U)/l\widehat{\pi}_1^{ab}(U)$. In particular $\widehat{\pi}_1^{ab}(U)/l\widehat{\pi}_1^{ab}(U)$ is two-dimensional as a vector space over $\mathbb{F}_l$, because l divides $\frac{q^d-1}{q-1}$. We also get that if the image of $\pi_\mathfrak{q}$ and π_∞ in $\widehat{\pi}_1^{ab}(U)/l\widehat{\pi}_1^{ab}(U)$ do not generate this group then the image of $\pi_\mathfrak{q}\pi_\infty^{-\deg(\mathfrak{q})}$ is trivial in $\widehat{\pi}_1^{ab}(U)/l\widehat{\pi}_1^{ab}(U)$. The latter can be reformulated by saying that $\pi_\mathfrak{q}\pi_\infty^{-\deg(\mathfrak{q})} = f(T)ug^l$, where $f(T) \in F^*$, $u \in U_\mathfrak{p}$ and $g \in \mathbb{A}^*$. It is clear from this equation that $f(T)$ is an l-th power in $F_\mathfrak{p}^*$. Because every degree zero divisor on $\mathbb{P}^1$ is principal, we get that $f(T) = cr(T)s(T)^l$ by comparing the divisors of the two sides of the equation above, where $c \in \mathbb{F}_q^*$ is a constant, $r(T) \in A$ is again the unique monic polynomial generating $\mathfrak{q}$ and $s(T) \in F^*$.

Looking at the $\mathfrak{p}$-adic components of the two sides of the equation above we get that $cr(T)$ is an l-th power modulo $\mathfrak{p}$. $\Box$

For any smooth group scheme G let G_l denote its maximal l-primary subgroup scheme.

Proposition 10.8. *The group $\mathcal{E}(\mathfrak{p})_l$ is the direct sum of $\mathcal{C}(\mathfrak{p})_l$ and $\mathcal{M}(\mathfrak{p})_l$.*

Proof. We first prove that $\mathcal{E}(\mathfrak{p})_l$ is admissible. The latter has a filtration by the subgroups $\mathcal{E}(\mathfrak{p})[l^n]$, where $n \in \mathbb{Z}$. The quotient $\mathcal{E}(\mathfrak{p})[l^{n+1}]/\mathcal{E}(\mathfrak{p})[l^n]$ injects into $\mathcal{E}(\mathfrak{p})[l]$ via the map $x \mapsto l^n x$, hence it will be sufficient to prove that $\mathcal{E}(\mathfrak{p})[l]$ is admissible. Let $\mathcal{W}(\mathfrak{p})$ denote the direct sum of $\mathcal{E}(\mathfrak{p})[l]$ and its Cartier dual. It is a $\mathbb{T}_l(\mathfrak{p})$-module annihilated by $\mathfrak{P}$. It is also a Galois module over F which is unramified for every prime $\mathfrak{q} \neq \mathfrak{p}$ of A such that the action of the Galois group commutes with the action of the Hecke algebra. The fact that the action of the Hecke operator $T_{\mathfrak{q}}$ on $\mathcal{W}(\mathfrak{p})$ satisfies the Eichler-Shimura relations implies that the action of the Frobenius $\mathrm{Frob}_{\mathfrak{q}}$ for any prime $\mathfrak{q} \neq \mathfrak{p}$ of A satisfies the relation
$$(\mathrm{Frob}_{\mathfrak{q}} - 1)(\mathrm{Frob}_{\mathfrak{q}} - q^{\deg(\mathfrak{q})}) = 0.$$
Hence the only eigenvalues possible for the action of $\mathrm{Frob}_{\mathfrak{q}}$ on $\mathcal{W}(\mathfrak{p})$ are 1 and $q^{\deg(\mathfrak{p})}$. Since the latter is Cartier self-dual, the multiplicities of these eigenvalues must be the same, hence the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}$ acting on $\mathcal{W}(\mathfrak{p})$ must be $(x-1)^m(x-q^{\deg(\mathfrak{q})})^m$, where $2m$ is the dimension of $\mathcal{W}(\mathfrak{p})$ as a vector space over $\mathbb{F}_l$. By the Chebotarev theorem we get that the characteristic polynomial of any element in the absolute Galois group of F acting on $\mathcal{W}(\mathfrak{p})$ is the same as the characteristic polynomial of its action on the Galois module $(\mathbb{Z}/l\mathbb{Z})^m \oplus (\mu_l)^m$. The Brauer-Nesbitt theorem implies that the semi-simplification of these modules must be equal, so $\mathcal{W}(\mathfrak{p})$, and therefore $\mathcal{E}(\mathfrak{p})_l$, are admissible.
As l does not divide $q-1$, the intersection of $\mathcal{C}(\mathfrak{p})_l$ and $\mathcal{M}(\mathfrak{p})_l$ is trivial. Now we only have to show that their direct sum is the whole l-primary subgroup of $\mathcal{E}(\mathfrak{p})$. Since $\mathcal{C}(\mathfrak{p})$ is fixed by the absolute Galois group of F, the quotient $\mathcal{H}(\mathfrak{p}) = \mathcal{E}(\mathfrak{p})/\mathcal{C}(\mathfrak{p})$ is a Galois module. This module is unramified at all places different from ∞ and $\mathfrak{p}$, because $\mathcal{E}(\mathfrak{p})$ is. The proof of Proposition 7.18 shows that the quotient of $\mathcal{E}(\mathfrak{p})_l$ by the torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ injects into $\mathbb{Z}_l/N(\mathfrak{p})\mathbb{Z}_l$. The restriction of this map onto $\mathcal{C}(\mathfrak{p})_l$ is surjective, as we already saw in the proof of Theorem 7.19. Hence $\mathcal{H}(\mathfrak{p})_l$ as a Galois module over F_∞ is isomorphic to a submodule of the torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$, in particular it is also unramified at ∞. As $\mathcal{E}(\mathfrak{p})_l$ is admissible as a Galois module over F, so does $\mathcal{H}(\mathfrak{p})_l$. Therefore the unique finite étale group scheme over $\mathbb{P}^1_{\mathbb{F}_q} - \{\mathfrak{p}\}$ prolonging $\mathcal{H}(\mathfrak{p})_l$ is also admissible. Moreover this admissible group scheme is μ-type as a Galois module over F_∞, because the l-primary torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ is. We also get that all Jordan-Hölder components of this admissible group scheme must be isomorphic to μ_l. Let $\mathfrak{q}$ be any admissible prime of A. The operator $\eta_{\mathfrak{q}}$ annihilates $\mathcal{E}(\mathfrak{p})$, so does the endomorphism $(\mathrm{Frob}_{\mathfrak{q}}-1)(\mathrm{Frob}_{\mathfrak{q}}-q^{\deg(\mathfrak{q})})$ by the Eichler-Shimura relations. By

the above $\mathrm{Frob}_{\mathfrak{q}}-1$ must be invertible on $\mathcal{H}(\mathfrak{p})_l$, so we get that $\mathrm{Frob}_{\mathfrak{q}}-q^{\deg(\mathfrak{q})}$ must annihilate this Galois module. Hence the module $\mathcal{H}(\mathfrak{p})_l$ must be μ-type by Proposition 10.7. In particular it is fixed under the action of the inertia group I at $\mathfrak{p}$. By Lemma 8.19 we get that the whole module $\mathcal{E}(\mathfrak{p})_l$ is fixed by I, too. As $\mathcal{E}(\mathfrak{p})_l$ is the direct sum of $\mathcal{C}(\mathfrak{p})_l$ and $\mathcal{E}(\mathfrak{p})_l\cap\mathrm{Hom}(\overline{\Gamma}(\mathfrak{p}),\mathbb{C}^*_\infty)_l$, where the latter is a Galois sub-module over F_∞ isomorphic to $\mathcal{H}(\mathfrak{p})_l$, the module $\mathcal{E}(\mathfrak{p})_l$ is unramified at ∞, too, so it is in fact everywhere unramified. Since it is pure as a Galois module over F_∞, it is pure as a Galois module over F, and the claim is now obvious. □

Fix a good prime $\mathfrak{q}$. For any natural number r let $\mathcal{G}_r$ denote the largest subgroup-scheme of $J_0(\mathfrak{p})_l$ annihilated by the ideal $(\mathfrak{E}\mathfrak{P}^r,\eta_{\mathfrak{q}})$.

Proposition 10.9. *The group scheme $\mathcal{G}_r$ is the direct sum of the group $\mathcal{C}(\mathfrak{p})_l$ and a μ-type group $\mathcal{M}_r$.*

Proof. We are going to prove the claim by induction on r. As $\mathcal{G}_0=\mathcal{E}(\mathfrak{p})_l$, this case has already been proved. Now we assume that the claim has been proved for $\mathcal{G}_r$, and we are going to show it for $\mathcal{G}_{r+1}$. Let $a_1,a_2,\ldots,a_m$ be a set of elements of $\mathfrak{P}^r$ such that their class mod $\mathfrak{P}^{r+1}$ is a basis of the $\mathbb{F}_l$ vector space $\mathfrak{P}^r/\mathfrak{P}^{r+1}$. The map $x\mapsto a_1x\oplus\cdots\oplus a_mx$ defines a homomorphism $\mathcal{G}_{r+1}\to\mathcal{E}(\mathfrak{p})_l^m$ with kernel $\mathcal{G}_r$, hence the quotient Galois module $\mathcal{G}_{r+1}/\mathcal{G}_r$ is pure as a submodule of a pure Galois module. Let $\mathcal{G}_{r+1}/\mathcal{G}_r=\mathcal{A}_r\oplus\mathcal{N}_r$, where $\mathcal{A}_r$, $\mathcal{N}_r$ are constant and μ-type Galois modules, respectively.
Let $\mathcal{G}$ be the pre-image of $\mathcal{A}_r$ in $\mathcal{G}_{r+1}$ and let $\overline{\mathcal{G}}$ be the quotient $\mathcal{G}/\mathcal{M}_r$ (recall that $\mathcal{M}_r$ is the μ-type component of $\mathcal{G}_r$). Clearly $\overline{\mathcal{G}}$ is a Galois module over F which is admissible, because it is the extension of the constant module $\mathcal{A}_r$ by the constant module $\mathcal{C}(p)_l$. The natural action of the Hecke algebra on the quotient Galois module $\mathcal{G}_{r+1}/\mathcal{G}_r$ commutes with the action of the Galois group, so it must preserve the eigenspace $\mathcal{A}_r$ of the latter. Therefore it leaves the Galois module $\mathcal{G}$ invariant, moreover it acts on its quotient $\overline{\mathcal{G}}$, because it leaves the module $\mathcal{M}_r$ invariant. The module $\overline{\mathcal{G}}$ injects into the quotient of $J_0(\mathfrak{p})_l$ by the l-primary torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}),\mathbb{C}^*_\infty)$. Therefore it is constant as a Galois module over F_∞. The operator $\eta_{\mathfrak{q}}$ annihilates $\overline{\mathcal{G}}$, so does the endomorphism $(\mathrm{Frob}_{\mathfrak{q}}-1)(\mathrm{Frob}_{\mathfrak{q}}-q^{\deg(\mathfrak{q})})$ by the Eichler-Shimura relations. By the above $\mathrm{Frob}_{\mathfrak{q}}-q^{\deg(\mathfrak{q})}$ must be invertible on $\overline{\mathcal{G}}$, so we get that $\mathrm{Frob}_{\mathfrak{q}}-1$ must annihilate this Galois module as well. Now we may apply Proposition 10.7 to conclude that $\overline{\mathcal{G}}$ is actually constant as a Galois module over F. As we already saw in the proof of Lemma 7.16, this fact and the Eichler-Shimura relations imply that $\overline{\mathcal{G}}$ is annihilated by the Eisenstein ideal. Hence $\overline{\mathcal{G}}=\mathcal{C}(p)_l$ according to the proof of Proposition 7.18.
We get that $\mathcal{A}_r=0$, so $\mathcal{G}_{r+1}$ is the extension of $C(\mathfrak{p})_l$ by a group scheme which the extension of the μ-type group scheme $\mathcal{N}_r$ by the μ-type group scheme $\mathcal{M}_r$. In particular the latter is admissible, and it must lie in the l-primary torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}),\mathbb{C}^*_\infty)$. Therefore the argument presented above shows that this module is μ-type over F, and the claim is now proved. □

Proof of Theorem 10.2. Let $x \in J_0(\mathfrak{p})_l$ be any element annihilated by $\eta_\mathfrak{q}$. Then x is actually annihilated by the ideal $(\eta_\mathfrak{q}, l^n)$ for some n. The latter contains $\mathfrak{E}\mathfrak{P}^r$ for some r, hence x is an element of $\mathcal{G}_r$ in this case. Since $\eta_\mathfrak{q}$ annihilates $\mathcal{E}(\mathfrak{p})_l$, we get that the group of elements $x \in J_0(\mathfrak{p})_l$ annihilated by $\eta_\mathfrak{q}$ is $\mathcal{M}(\mathfrak{p})_l \oplus \mathcal{C}(\mathfrak{p})_l$, using Propositions 10.8 and 10.9. Also note that $\eta_\mathfrak{q}$ is actually an isogeny of $J_0(\mathfrak{p})$. If it were not, then $J_0(\mathfrak{p})$ would contain an abelian subvariety such that the action of the Frobenius at $\mathfrak{q}$ on this variety would have 1 or $q^{\deg(\mathfrak{q})}$ as an eigenvalue by the Eichler-Shimura relations. The latter is impossible by Weil's theorem. Therefore $\eta_\mathfrak{q}$ is injective as an endomorphism of T_l. By dualizing we get that it is surjective as an endomorphism of $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$. Let $y \in \mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ be any element annihilated by $\eta_\mathfrak{q}$. Pick an element $x \in J_0(\mathfrak{p})_l$ whose specialization (i.e. its class in the quotient of $J_0(\mathfrak{p})_l$ by the l-primary torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)$) is y. Then $\eta_\mathfrak{q}(x) \in \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$. By the above there is a $z \in \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ such that $\eta_\mathfrak{q}(z) = \eta_\mathfrak{q}(x)$. Then the element $x - z$ is annihilated by $\eta_\mathfrak{q}$ and its specialization is y. We get that the specialization map from $C(\mathfrak{p})[l]$ into the submodule of $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ annihilated by $\eta_\mathfrak{q}$ is an isomorphism, in particular the latter is 1-dimensional as a vector space over $\mathbb{F}_l$. The latter is also dual to $T_l/(\eta_\mathfrak{q}, l)$. Since T_l is locally free of rank one as a $\mathbb{T}_l(\mathfrak{p})$-module, we get that $(\eta_\mathfrak{q}, l)$ is a prime ideal, hence the claim holds. □

11. Mazur's Eisenstein decent for primes l dividing $t(\mathfrak{p})$

Definition 11.1. For the rest of this chapter we fix a prime l dividing $t(\mathfrak{p})$. Then l is automatically an Eisenstein prime. We also introduce the shorthand notation $\mathcal{S} = \mathcal{S}(\mathfrak{p})[l]$, $\mathcal{F} = \mathcal{F}(\mathfrak{p})[l]$ and $\mathcal{D} = \mathcal{D}(\mathfrak{p})[l]$. A Galois sub-module $G \subset J_0(\mathfrak{p})_l$ is $*$-type, if

(i) it contains $\mathcal{D}$,
(ii) the intersection $G_0 = G \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ is Galois-invariant,
(iii) the Galois module G_0 is admissible,
(iv) the quotient G/G_0 is equal to $\mathcal{F}$.

In this case let $G_{00} \subseteq G_0$ denote pre-image of the largest μ-type subgroup of $G_0/\mathcal{S}$ under the quotient map. Note that under this definition $\mathcal{D}$ itself is a $*$-type group by Proposition 9.18.

Lemma 11.2. *Let $G \subset J_0(\mathfrak{p})_l$ be a $*$-type Galois module. Then G_{00} is μ-type.*

Proof. By Lemma 8.19 the Galois module G_{00} is unramified at $\mathfrak{p}$. Since every tame Galois module which only ramifies at ∞ is in fact everywhere unramified, we get that G_{00} is everywhere unramified. It is μ-type as a Galois module over F_∞, being a sub-module of G_0, hence it is μ-type as a Galois module over F, too. □

The following proposition corresponds to Lemma 17.5 of [14], pages 131-133.

Proposition 11.3. *Let $\mathfrak{q}$ be a good prime and let $G \subset H \subset J_0(\mathfrak{p})_l$ be two $\mathbb{T}(\mathfrak{p})$-invariant Galois modules annihilated by $\eta_\mathfrak{q}$ and assume that*

(i) *the Galois module G is $*$-type,*

(*ii*) *the quotient* H/G *has order* l,
(*iii*) *the quotient* $H/H \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ *is* l*-torsion.*

Then H *is* $*$*-type, too.*

PROOF. Let H_0 denote the intersection $H \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$. Since the quotient groups H/G and G/G_0 both have order l, the quotient H/G_0 must have order l^2. Hence it is either isomorphic to $\mathbb{Z}/l^2\mathbb{Z}$ or to $\mathbb{F}_l^2$ as a group. In the first case H_0 must be equal to G, since H_0/G_0 must be a proper subgroup of H/G_0 by condition (*iii*), but $\mathbb{Z}/l^2\mathbb{Z}$ has only one proper subgroup. Since G does not lie in $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$, this is a contradiction. Hence H/G_0 is l-torsion.
Because H is annihilated by the operator $\eta_\mathfrak{q}$, the Eichler-Shimura relation has the shape $(\mathrm{Frob}_\mathfrak{q} - 1)(\mathrm{Frob}_\mathfrak{q} - q^{\deg(\mathfrak{q})}) = 0$ in H for the prime $\mathfrak{q}$. The Galois module H/G is also equipped with an action of the Hecke algebra $\mathbb{T}(\mathfrak{p})$ which satisfies the Eichler-Shimura relations. Since $q \equiv 1 \mod l$ by assumption, we get that $(\mathrm{Frob}_\mathfrak{q} - 1)^2 = 0$ on H/G. Since the latter is a one-dimensional vector space over $\mathbb{F}_l$, we get that $\mathrm{Frob}_\mathfrak{q} - 1$ annihilates H/G, in other words $(\mathrm{Frob}_\mathfrak{q} - 1)(H)$ lies in G. Using the Eichler-Shimura relation for the prime $\mathfrak{q}$ in H again we get that the image of $\mathrm{Frob}_\mathfrak{q} - 1$ actually lies in the kernel M of $\mathrm{Frob}_\mathfrak{q} - q^{\deg(\mathfrak{q})}$ in G.
Note that $G/\mathcal{D}$ is μ-type as a Galois module over F_∞. Hence the image of M in this group under the quotient map is μ-type by Proposition 10.7. As the natural map $G_0/\mathcal{S} \to G/\mathcal{D}$ is an isomorphism, the image of M in $G/\mathcal{D}$ must lie in the image of G_{00} by the above. Hence M lies in the group generated by G_{00} and $\mathcal{D}$. Assume that M does not lie in G_{00}. By Lemma 11.2 the module G_{00} is μ-type, hence it is annihilated by $\mathrm{Frob}_\mathfrak{q} - q^{\deg(\mathfrak{q})}$, or in other words it is in M. This implies that M must contain $\mathcal{D}$, too. The latter is everywhere unramified, but does not split by (*ii*) and (*iv*) of Proposition 9.18. Therefore the action of $\mathrm{Frob}_\mathfrak{q}$ could not be trivial as $\mathrm{Frob}_\mathfrak{q}$ generates the maximal everywhere unramified l-torsion abelian Galois extension of F because of the condition that l does not divide $\deg(\mathfrak{q})$. This is a contradiction, so M lies in $G_{00} \subseteq G_0$. Hence we get that $\mathrm{Frob}_\mathfrak{q} - 1$ annihilates H/G_0.
Now assume that $H_0 = G_0$. In this case H/G_0 injects naturally into the quotient $J_0(\mathfrak{p})_l/\mathrm{Hom}(\overline{\Gamma}(\mathfrak{p}), \mathbb{C}^*_\infty)_l$. Hence it is trivial as a Galois module over F_∞, so it is even trivial as a Galois module over F by Proposition 10.7. The Galois module G_0 is also $\mathbb{T}(\mathfrak{p})$-invariant, so there is an induced action of the Hecke algebra $\mathbb{T}(\mathfrak{p})$ on H/G_0. The latter satisfies the Eichler-Shimura relations, so the Eisenstein ideal annihilates H/G_0 applying again the argument in the proof of Lemma 7.16. Since the inclusion of H/G_0 in $J_0(\mathfrak{p})_l/\mathrm{Hom}(\overline{\Gamma}(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ is $\mathbb{T}(\mathfrak{p})$-equivariant, we get that the former must be one-dimensional as a vector space over $\mathbb{F}_l$ by the strong multiplicity one theorem.
This is a contradiction, so H_0 is strictly larger than G_0. As we already see in the first paragraph, the group H_0/G_0 can not be equal to G/G_0, so H/G_0 has two proper subgroups invariant under the action of the absolute Galois group of F_∞. Hence H/G_0 must be trivial as a Galois module over F_∞. By repeating the argument above we get that H/G_0 is trivial as a Galois module over F. In

particular H_0/G_0 is Galois-invariant, hence H_0 is a Galois-invariant subgroup of H. Since it is the extension of $\mathbb{Z}/l\mathbb{Z}$ by the admissible Galois module G_0, it must be admissible, too. The quotient H/H_0 has order l, so it must be equal to $\mathcal{F}$. Since condition (i) of Definition 11.1 is automatic for H, the claim is now proved. $\square$

Definition 11.4. Fix a good prime $\mathfrak{q}$. Let $\mathfrak{P} = (\mathfrak{E}, l)$ be the Eisenstein prime ideal above l. For any natural number r let $\mathcal{H}(r)$ denote the largest subgroup of $J_0(\mathfrak{p})_l$ annihilated by the ideal $(l^r, \eta_{\mathfrak{q}})$. Let $\mathcal{G}(0)$ be $\mathcal{D}$, and for every positive integer r let $\mathcal{G}(r)$ be the pre-image of the largest submodule of $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ annihilated by $\eta_{\mathfrak{q}}$ in $\mathcal{H}(r)$ under the specialization map and let $\mathcal{G}_0(r)$ denote the intersection $\mathcal{G}(r) \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)_l$. Both groups are invariant under the action of $\mathbb{T}_l$ and the absolute Galois group of F_∞. What is not clear that these groups are Galois modules over F.

The following proposition corresponds to Lemma 17.7 of [14], pages 133-134.

Proposition 11.5. *The group $\mathcal{G}(r)$ is Galois-invariant, and as a Galois module it is $*$-type.*

Proof. We are going to prove the claim by induction on r. As $\mathcal{G}(0) = \mathcal{D}$, the claim is clear for $r = 0$. Now we assume that the claim is true for r and then we are going to prove it for $r+1$. If $x \in \mathcal{H}(r+1)$, then by the defining property of $\mathcal{G}(r+1)$ we have $x \in \mathcal{G}(r+1)$ if and only if $lx \in \mathcal{G}_0(r)$. (This is true even when $r = 0$ as $\mathcal{G}(1) = \mathcal{H}(1)$ is l-torsion.) We first need to show that $\sigma(x) \in \mathcal{G}(r+1)$ for any $\sigma \in \mathrm{Gal}(\overline{F}|F)$. Equivalently we have to show that $l\sigma(x) \in \mathcal{G}_0(r)$, but this is true because σ leaves $\mathcal{G}_0(r)$ stable by the induction hypothesis and $\sigma(lx) = l\sigma(x)$.
The Galois module $\mathcal{G}(r+1)$ is admissible because it is a Galois sub-module of $\mathcal{H}(r+1)$, which is admissible. The latter can be seen by noting that $\mathcal{H}(r+1)$ has a filtration by $\mathbb{T}_l$-invariant Galois submodules whose components are annihilated by the ideal $(l, \eta_{\mathfrak{q}})$, hence by some power of the Eisenstein ideal. Therefore the arguments at the start of the proof of Propositions 10.8 and 10.9 can be applied to these components to show that they are admissible.
The Galois modules $\mathcal{G}(r)$ and $\mathcal{G}(r+1)$ are both $\mathbb{T}_l$-invariant, so there is a filtration:

$$\mathcal{G}(r) = F_0 \subset F_1 \subset \ldots \subset F_j \subset \ldots \subset F_m = \mathcal{G}(r+1)$$

by $\mathbb{T}_{\mathfrak{P}}[\mathrm{Gal}(\overline{F}|F)]$-modules such that the successive quotients are irreducible modules over the group algebra $\mathbb{T}_{\mathfrak{P}}[\mathrm{Gal}(\overline{F}|F)]$, where $\mathbb{T}_{\mathfrak{P}}$ is the completion of the Hecke algebra $\mathbb{T}_l(\mathfrak{p})$ at the prime ideal $\mathfrak{P}$. These modules must be annihilated by $\mathfrak{P}$, because they are irreducible. But $\mathbb{T}_{\mathfrak{P}}/\mathfrak{P} = \mathbb{Z}/l\mathbb{Z}$, so these components are actually irreducible $\mathrm{Gal}(\overline{F}|F)$-modules. Since they are admissible, too, their order is l. Therefore it follows that F_j is $*$-type using Proposition 11.3 by induction on j: the modules F_j are $\mathbb{T}_l$-invariant by their construction, condition (i) is the induction hypothesis, condition (ii) has just been proved, and condition (iii) holds because $\mathcal{G}(r+1)/\mathcal{G}_0(r+1)$ is l-torsion by definition. $\square$

Theorem 11.6. *The ideal $\mathfrak{P}$ is generated by l and $\eta_{\mathfrak{q}}$ for every good prime $\mathfrak{q}$. In particular $\mathbb{T}_{\mathfrak{P}}$ is Gorenstein.*

Proof. Let $y \in \mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ be any element annihilated by $\eta_{\mathfrak{q}}$. Pick an element $x \in J_0(\mathfrak{p})_l$ whose specialization (i.e. its class in the quotient of $J_0(\mathfrak{p})_l$ by the l-primary torsion of the torus $\mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)$) is y. Then $\eta_{\mathfrak{q}}(x) \in \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$. Since $\eta_{\mathfrak{q}}$ is an isogeny of $J_0(\mathfrak{p})$, there is a $z \in \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ such that $\eta_{\mathfrak{q}}(z) = \eta_{\mathfrak{q}}(x)$. Then the element $u = x - z$ is annihilated by $\eta_{\mathfrak{q}}$ and its specialization is y. As u must be an element of $\mathcal{G}(r)$ for some natural number r, we get that the submodule of $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{F}_l)$ annihilated by $\eta_{\mathfrak{q}}$ is 1-dimensional as a vector space over $\mathbb{F}_l$ by Proposition 11.5. The latter is also dual to $T_l/(\eta_{\mathfrak{q}}, l)$. Since T_l is locally free of rank one as a $\mathbb{T}_l(\mathfrak{p})$-module, we get that $(\eta_{\mathfrak{q}}, l)$ is a prime ideal, hence the claim holds. □

Corollary 11.7. *The groups $\mathcal{E}(\mathfrak{p})[l]$ and $\mathcal{D}$ are equal.*

Proof. As we already noted, $\mathcal{E}(\mathfrak{p})[l]$ contains $\mathcal{D}$. By the strong multiplicity one theorem the image of the specialization of $\mathcal{E}(\mathfrak{p})[l]$ is equal to the image of the specialization of $\mathcal{D}$ (see the proof of Proposition 7.18). Because $\mathbb{T}_{\mathfrak{P}}$ is Gorenstein by Theorem 11.6, the intersection $\mathcal{E}(\mathfrak{p}) \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)[l]$ is a free $\mathbb{T}_{\mathfrak{P}}/\mathfrak{E}\mathbb{T}_{\mathfrak{P}}$ module of rank one. Hence it has the same order as $\mathcal{S}$, so they are equal, too. Since this module is the kernel of the specialization map, the claim is now obvious. □

Corollary 11.8. *The l-primary subgroups of $\mathcal{M}(\mathfrak{p})$ (resp. $\mathcal{T}(\mathfrak{p})$) and $\mathcal{S}(\mathfrak{p})$ (resp. $\mathcal{C}(\mathfrak{p})$) are equal.*

Proof. First note that the intersection $\mathcal{E}(\mathfrak{p})_l \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ is $\mathcal{S}(\mathfrak{p})_l$. This can be seen very easily by repeating the proof of Theorem 10.5 if either d is odd or $l \neq 2$. This condition is necessary to guarantee that the order of $\mathcal{E}(\mathfrak{p})_l \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_l$ is the same as the order of $\mathcal{S}(\mathfrak{p})_l$ while using claim (vi) of Proposition 7.11, which rests on Theorem 6.6. If $d = \deg(\mathfrak{p})$ is even and $l = 2$ then the same argument (and the claim quoted above) only shows that $\mathcal{S}(\mathfrak{p})_2$ is a subgroup of index at most two in the group $\mathcal{E}_2 = \mathcal{E}(\mathfrak{p}) \cap \mathrm{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}^*_\infty)_2$ as the order of the latter is the same as the index of the Eisenstein ideal $\mathfrak{E}_2(\mathfrak{p}) \triangleleft \mathbb{T}_2(\mathfrak{p})$. Note that $\mathcal{E}_2$ is the intersection of $\mathcal{E}(\mathfrak{p})$ and the union $\cup_{r \in \mathbb{N}} \mathcal{G}_0(r)$, so it is a Galois module. The quotient group $\mathcal{E}_2/\mathcal{S}(\mathfrak{p})$ is admissible of order at most two, so it must be μ-type. Hence Lemma 8.19 can be applied to show that $\mathcal{E}_2$ is unramified at $\mathfrak{p}$. By the Néron property this group has a specialization map into the group of components of $J_0(\mathfrak{p})$ at $\mathfrak{p}$. The restriction of this map to $\mathcal{S}(\mathfrak{p})$ is injective by (ii) of Proposition 8.18, so it is injective as $\mathcal{E}_2$ is a cyclic group by the strong multiplicity one theorem. The order of the maximal 2-primary subgroup of the group of components of $J_0(\mathfrak{p})$ at $\mathfrak{p}$ is the same as the order of $\mathcal{S}(\mathfrak{p})_2$, so the latter is the whole group $\mathcal{E}_2$. By reversing the logic of the argument at the start of this paragraph we get that $\mathbb{T}_l/\mathfrak{E}_l(\mathfrak{p}) = \mathbb{Z}_l/N(\mathfrak{p})\mathbb{Z}_l$ even when d is even and $l = 2$.

Let $l(\mathfrak{p})$ denote the largest power of l dividing $N(\mathfrak{p})$. If the claim above is false then there is an element x in $\mathcal{M}(\mathfrak{p})_l - \mathcal{S}(\mathfrak{p})_l$ (resp. in $\mathcal{T}(\mathfrak{p})_l - \mathcal{C}(\mathfrak{p})_l$) such that lx is in $\mathcal{S}(\mathfrak{p})_l$ (resp. in $\mathcal{C}(\mathfrak{p})_l$). The element x is annihilated by $l(\mathfrak{p})$, since it is annihilated by the Eisenstein ideal. Therefore lx is annihilated by $\frac{l(\mathfrak{p})}{l}$. Since both $\mathcal{S}(\mathfrak{p})_l$ and $\mathcal{C}(\mathfrak{p})_l$ are cyclic of order $l(\mathfrak{p})$, the element lx must have an l-root u in $\mathcal{S}(\mathfrak{p})_l$ (resp. in $\mathcal{C}(\mathfrak{p})_l$) by the above. Subtracting u from x we get that we may assume that x is l-torsion. By Corollary 11.7 we must have $x \in \mathcal{D}$. Since the Galois module $\mathcal{D}$ is not pure, we conclude that x is actually in $\mathcal{S}$. The intersection of $\mathcal{S}(\mathfrak{p})_l$ and $\mathcal{C}(\mathfrak{p})_l$ is exactly the largest constant Galois submodule of the former by Proposition 9.3, so the claim is now clear. $\square$

Remark 11.9. An interesting corollary of the proof above that the inclusion $\mathcal{H}_{00}(\mathfrak{p}, \mathbb{Z}_2/2N(\mathfrak{p})\mathbb{Z}_2) \to \mathcal{H}_0(\mathfrak{p}, \mathbb{Z}_2/2N(\mathfrak{p})\mathbb{Z}_2)$ is not surjective if $d = \deg(\mathfrak{p})$ is even, i.e. there is a cuspidal harmonic form with values in $\mathbb{Z}_2/2N(\mathfrak{p})\mathbb{Z}_2$ which cannot be lifted to an integer-valued cuspidal harmonic form. Our proof of this fact is quite involved and geometric, and wanders out of the natural algebraic universe where this question lives. It would be nice to see a more conceptual and general proof.

References

1. M. Artin, *Néron models*, Arithmetic geometry (G. Cornell, J. H. Silverman, eds.), Springer, Berlin-Heidelberg-New York, 1986, pp. 213–230.
2. P. Deligne and M. Rapoport, *Schémas de modules des courbes elliptiques*, L.N.M. 349, Springer, Berlin-Heidelberg-New York, 1973, pp. 143-316.
3. V. G. Drinfeld, *Elliptic modules*, [translation], Mat. Sbornik **23** (1974), 561–592.
4. E.-U. Gekeler, *Zur Arithmetic von Drinfeld-Monduln*, Math. Ann. **262** (1983), 167-182.
5. E.-U. Gekeler, *Drinfeld modular curves*, L.N.M. 1231, Springer, Berlin-Heidelberg-New York, 1986.
6. E.-U. Gekeler, *Über Drinfeld'sche Modulkurven von Hecke-Typ*, Comp. Math. **57** (1986), 219-236.
7. E.-U. Gekeler, *On the cuspidal divisor class group of a Drinfeld modular curve*, Doc. Math. **2** (1997), 351-374.
8. E.-U. Gekeler, *On the Drinfeld discriminant function*, Comp. Math. **106** (1997), 181-202.
9. E.-U. Gekeler, *Cuspidal divisor class groups of modular curves*, Algebraic number theory and Diophantine analysis (Graz, 1998), de Gruyter, Berlin, 2000, pp. 163–189.
10. E.-U. Gekeler and U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, Int. J. Math. **6** (1995), 689–708.
11. E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. reine angew. Math. **476** (1996), 27–93.
12. H. Jacquet and R.P. Langlands, *Automorphic forms on GL(2)*, Springer, Berlin-Heidelberg-New York, 1970.
13. N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, 1985.

14. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.
15. J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, 1980.
16. A. Pál, *The rigid analytical regulator and K_2 of Drinfeld modular curves*, submitted.
17. J.-P. Serre, *Trees*, Springer, Berlin-Heidelberg-New York, 1980.
18. A. Tamagawa, *The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve*, Publ. Res. Inst. Math. Sci. **31** (1995), 203–246.
19. A. Weil, *Dirichlet series and automorphic forms*, Springer, Berlin-Heidelberg-New York, 1971.

Index of notations

Ambrus Pál
IHÉS
Le Bois-Marie
35, Route de Chartres
F-91440
Bures-sur-Yvette, France
pal@ihes.fr