

# EXPLICIT DRINFELD MODULES WITH MAXIMAL GALOIS ACTION ON THEIR TORSION POINTS

DAVID ZYWINA

ABSTRACT. Consider a Drinfeld module over a finitely generated field with generic characteristic, and the Galois representation arising from the action on its torsion points. Recent work of Pink and Rüttsche has described the image of this representation up to commensurability. Their theorem is qualitative, and the objective of this paper is to complement this theory with a worked out example. In particular, we give examples of Drinfeld modules of rank 2 for which the Galois action on its torsion points is as large as possible. We will use the basic strategy of Serre, which he applied to semi-stable elliptic curves over  $\mathbb{Q}$  in order to give examples of his openness theorem.

## 1. INTRODUCTION

Let  $\mathbb{F}_q$  be a finite field with  $q = p^s$  elements. Let  $A$  be the ring  $\mathbb{F}_q[T]$  and let  $F$  be its fraction field  $\mathbb{F}_q(T)$ . For a given field  $K$ , let  $\bar{K}$  be an algebraic closure of  $K$  and let  $K^{\text{sep}}$  be the separable closure of  $K$  in  $\bar{K}$ . Denote by  $G_K = \text{Gal}(K^{\text{sep}}/K)$  the absolute Galois group of  $K$ .

**1.1. Drinfeld modules and Galois representations.** We now give enough background in order to state and explain our theorem. For an in-depth introduction to Drinfeld modules, see [Gos96, DH87, Dri74].

Let  $K\{\tau\}$  be the ring of skew polynomials; i.e., the ring of polynomials in the indeterminate  $\tau$  with coefficients in  $K$  satisfying the commutation rule  $\tau c = c^q \tau$  for  $c \in K$ . We can, and will, identify  $K\{\tau\}$  with the endomorphism ring  $\text{End}(\mathbb{G}_{a,K})$  by identifying  $\tau$  with the Frobenius map  $X \mapsto X^q$ . A Drinfeld  $A$ -module over  $K$  is a ring homomorphism

$$\phi: A \rightarrow K\{\tau\}, \quad a \mapsto \phi_a$$

whose image is not contained in  $K$ . A Drinfeld module  $\phi$  is determined by  $\phi_T = \sum_{i=0}^r a_i \tau^i$  with  $a_i \in K$  and  $a_r \neq 0$ ; the positive integer  $r$  is called the **rank** of  $\phi$ .

Let  $\partial_0: K\{\tau\} \rightarrow K$  be the ring homomorphism  $\sum_i a_i \tau^i \mapsto a_0$ . The **characteristic** of  $\phi$  is the kernel  $\mathfrak{p}_0$  of the homomorphism  $\partial_0 \circ \phi: A \rightarrow K$ . We say that  $\phi$  has **generic characteristic** if  $\mathfrak{p}_0 = (0)$ .

The Drinfeld module  $\phi$  endows  $K^{\text{sep}}$  with an  $A$ -module structure (i.e.,  $a \cdot x = \phi_a(x)$  for  $a \in A$  and  $x \in K^{\text{sep}}$ ); we shall write  ${}^\phi K^{\text{sep}}$  if we wish to emphasize this action. If  $\mathfrak{a}$  is a non-zero ideal of  $A$ , then the  **$\mathfrak{a}$ -torsion** of  $\phi$  is

$$\phi[\mathfrak{a}] := \{x \in {}^\phi K^{\text{sep}} : a \cdot x = 0 \text{ for all } a \in \mathfrak{a}\} = \{x \in K^{\text{sep}} : \phi_a(x) = 0 \text{ for all } a \in \mathfrak{a}\}.$$

If  $\mathfrak{a}$  is relatively prime to the characteristic  $\mathfrak{p}_0$ , then  $\phi[\mathfrak{a}]$  is a free  $A/\mathfrak{a}$ -module of rank  $r$ . For the rest of the section, assume that  $\phi$  has generic characteristic.

The absolute Galois group  $G_K$  naturally acts on  $\phi[\mathfrak{a}]$  and respects the  $A$ -module structure. This action can be re-expressed in terms of a Galois representation

$$\bar{\rho}_{\phi,\mathfrak{a}}: G_K \rightarrow \text{Aut}(\phi[\mathfrak{a}]) \cong \text{GL}_r(A/\mathfrak{a}).$$

---

*Date:* July 30, 2009.

*2000 Mathematics Subject Classification.* Primary 11G09; Secondary 11F80, 11R58.

*Key words and phrases.* Drinfeld modules, torsion points, Galois representations.

Let  $\mathfrak{p}$  be a place of  $A$ . If  $\phi$  has good reduction at  $\mathfrak{p}$  and  $\mathfrak{p} \nmid \mathfrak{a}$ , then the representation  $\bar{\rho}_{\phi, \mathfrak{a}}$  is unramified at  $\mathfrak{p}$  (one can use this as a definition of good reduction, it will agree with the later definition).

For each non-zero prime ideal  $\lambda$  of  $A$ , we have a Galois representation

$$\rho_{\phi, \lambda}: G_K \rightarrow \text{Aut} \left( \varinjlim_i \phi[\lambda^i] \right) \cong \text{GL}_r(A_\lambda)$$

where  $A_\lambda$  is the  $\lambda$ -adic completion of  $A$ . These representations satisfy analogues of the familiar  $\ell$ -adic representations. For example, if  $\phi$  has good reduction at  $\mathfrak{p} \nmid \lambda$ , then  $\det(xI - \rho_{\phi, \lambda}(\text{Frob}_{\mathfrak{p}}))$  is a polynomial with coefficients in  $A$  that does not depend on  $\lambda$ .

Combining all the representations together, we obtain a single Galois representation

$$\rho_\phi: G_K \rightarrow \text{Aut} \left( \varinjlim_{\mathfrak{a}} \phi[\mathfrak{a}] \right) \cong \text{GL}_r(\widehat{A})$$

where  $\widehat{A}$  is the profinite completion of  $A$ .

**1.2. Open image theorem.** Pink and Rüttsche have recently described the image of  $\rho_\phi$  up to commensurability [PR09a]. For simplicity we only state the version for which  $\phi$  has no non-trivial endomorphisms.

**Theorem 1.1** (Pink-Rüttsche). *Let  $\phi$  be a Drinfeld  $A$ -module of rank  $r$  over a finitely generated field  $K$  of generic characteristic. Assume that  $\text{End}_{\bar{K}}(\phi) = A$ . Then the image of*

$$\rho_\phi: G_K \rightarrow \text{GL}_r(\widehat{A})$$

*is open in  $\text{GL}_r(\widehat{A})$ . Equivalently,  $\rho_\phi(G_K)$  has finite index in  $\text{GL}_r(\widehat{A})$ .*

**1.3. Explicit example.** Theorem 1.1 is qualitative in nature; it only describes the group  $\rho_\phi(G_K)$  up to commensurability (it is unclear from the proof how feasible it is to actually compute  $\rho_\phi(G_K)$ ). Except for the rank one case, which resembles the classical theory of complex multiplication, the author is unaware of any explicit examples in the literature.

The main objective of this paper is to work out the image of  $\rho_\phi$  for an explicit example. This example will also prove the existence of Drinfeld modules of rank 2 for which the Galois action on its torsion points is maximal.

**Theorem 1.2.** *Let  $q \geq 5$  be an odd prime power. Let  $\varphi: \mathbb{F}_q[T] \rightarrow \mathbb{F}_q(T)\{\tau\}$  be the Drinfeld module of rank 2 defined by*

$$\varphi_T = T + \tau - T^{q-1}\tau^2.$$

*Then the Galois representation*

$$\rho_\varphi: G_{\mathbb{F}_q(T)} \rightarrow \text{GL}_2(\widehat{\mathbb{F}_q[T]})$$

*is surjective.*

**1.4. Elliptic curves.** It is worth mentioning the analogous theory for elliptic curves since it strongly influences the proof of Theorem 1.1 and the methods of this paper. Let  $E$  be an elliptic curve defined over a number field  $K$ . For each positive integer  $m$ , the Galois action on the  $m$ -torsion points  $E[m]$  of  $E(K^{\text{sep}})$  gives a representation

$$\bar{\rho}_{E, m}: \text{Gal}(K^{\text{sep}}/K) \rightarrow \text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Combining these representations together, we obtain a single Galois representation

$$\rho_E: \text{Gal}(K^{\text{sep}}/K) \rightarrow \text{Aut}(E_{\text{tors}}) \cong \text{GL}_2(\widehat{\mathbb{Z}}).$$

If  $\text{End}_{\bar{K}}(E) = \mathbb{Z}$ , then Serre has shown that the image of  $\rho_E$  is open in  $\text{GL}_2(\widehat{\mathbb{Z}})$ . This theorem was proved in [Ser72], and is a clear analogue of Theorem 1.1.

Earlier, Serre had showed that  $\rho_E$  has open image if  $E$  has non-integral  $j$ -invariant (cf. §3.2 of [Ser68, Chapter IV]). What makes the non-integral  $j$ -invariant case easier is that, using the theory of *Tate curves*, one can show that the image of  $\bar{\rho}_{E,\ell}: G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$  contains an element of order  $\ell$  for almost all primes  $\ell$  (cf. the proposition of [Ser68, Chapter IV Appendix A.1.5]).

Serre has given worked examples of  $\rho_E(G_K)$  for several non-CM elliptic curves over  $\mathbb{Q}$  (cf. [Ser72, §5.5]). The first example with surjective  $\rho_E$  was given recently by A. Greicius [Gre09].

**1.5. Overview.** The proof of Theorem 1.2 will be spread over three sections.

In §2, we prove that the character  $\det \circ \rho_\varphi: G_F \rightarrow \widehat{A}^\times$  is surjective. This will be accomplished by first recognizing that  $\det \circ \rho_\varphi$  is nothing but the representation  $\rho_C$  associated with the Carlitz module  $C$  (this particular Drinfeld module has been extensively studied).

In §3, we shall recall the *Tate uniformization* of a Drinfeld module (this is the analogue of the usual Tate uniformization of elliptic curves over non-archimedean local fields). We can then apply this theory to our Drinfeld module  $\varphi$  at the place ( $T$ ) where it has bad and stable reduction. The main application of the section is that for every non-zero prime ideal  $\lambda$  of  $A$ ,  $\bar{\rho}_{\varphi,\lambda}(G_F)$  contains a  $p$ -Sylow subgroup of  $\mathrm{GL}_2(A/\lambda)$ .

In the next section, we prove that  $\varphi[\lambda]$  is an irreducible  $\mathbb{F}_\lambda[G_F]$ -module for all  $\lambda$ . If  $\varphi[\lambda]$  is reducible, then we can understand the semi-simplification of  $\varphi[\lambda]$  in terms of two characters  $\chi, \chi': G_F \rightarrow \mathbb{F}_\lambda^\times$ . Using our knowledge of  $\bar{\rho}_{\varphi,\lambda}$ , we will describe the possibilities for the pair  $\{\chi, \chi'\}$ , and then derive a contradiction based upon traces of Frobenii.

Having shown that the image of  $\rho_E(G_F)$  is “large” in different contexts, we can then combine them to prove surjectivity. That the residual representations  $\bar{\rho}_{\varphi,\lambda}$  are surjective, will follow quickly. In contrast to the elliptic curve situation, it then takes some serious work to prove that these representations are independent. For elliptic curves, one makes use of the easy fact that the groups  $\mathrm{SL}_2(\mathbb{Z}_\ell)$  ( $\ell \geq 5$ ) have no common quotients; this fails miserably for the groups  $\mathrm{SL}_2(A_\lambda)$  (just consider  $\lambda$  with the same degree). The required group theory for the proof is contained in an appendix.

**Notation.** We fix throughout an odd prime power  $q = p^s \geq 5$ . We let  $A$  be the ring  $\mathbb{F}_q[T]$  and we let  $F$  be the fraction field  $\mathbb{F}_q(T)$ .

We will usually denote a non-zero prime ideal of  $A$  by  $\lambda$ , which we will also call a *finite place* of  $F$ . Since  $A = \mathbb{F}_q[T]$  is a PID, we will occasionally identify  $\lambda$  with its monic irreducible generator. We shall denote the residue field  $A/\lambda$  by  $\mathbb{F}_\lambda$ . Let  $A_\lambda$  and  $F_\lambda$  be the  $\lambda$ -adic completion of  $A$  and  $F$ , respectively. Let  $N(\mathfrak{a})$  be the cardinality of  $A/\mathfrak{a}$  for any non-zero ideal  $\mathfrak{a} \subseteq A$ .

## 2. THE DETERMINANT OF $\rho_\varphi$

**2.1. The Carlitz module.** The Carlitz module is the Drinfeld module  $C: A \rightarrow F\{\tau\}$  for which  $C_T = T + \tau$ .

**Proposition 2.1** (Hayes [Hay74]). *For every non-zero ideal  $\mathfrak{a}$  of  $A$ , the representation*

$$\bar{\rho}_{C,\mathfrak{a}}: G_F \rightarrow \mathrm{Aut}(C[\mathfrak{a}]) = (A/\mathfrak{a})^\times$$

*is surjective. The representation  $\bar{\rho}_{C,\mathfrak{a}}$  is unramified at all finite places of  $F$  not dividing  $\mathfrak{a}$ , and for each monic irreducible polynomial  $\mathfrak{p}$  of  $A$  not dividing  $\mathfrak{a}$ , we have  $\bar{\rho}_{C,\mathfrak{a}}(\mathrm{Frob}_\mathfrak{p}) \equiv \mathfrak{p} \pmod{\mathfrak{a}}$ .*

In particular, the Proposition shows that  $\rho_C: G_F \rightarrow \mathrm{GL}_1(\widehat{A}) = \widehat{A}^\times$  is surjective (this gives a rank one example of Theorem 1.1).

**2.2. The determinant.** Let  $\mathfrak{p}$  be a monic irreducible polynomial of  $A$  different from  $T$ . For any non-zero ideal  $\mathfrak{a}$  of  $A$  relatively prime to  $\mathfrak{p}$ , we know that

$$\det(xI - \bar{\rho}_{\varphi, \mathfrak{a}}(\text{Frob}_{\mathfrak{p}})) \equiv x^2 - a_{\mathfrak{p}}(\varphi)x + \epsilon_{\mathfrak{p}}(\varphi)\mathfrak{p} \pmod{\mathfrak{a}}$$

for  $a_{\mathfrak{p}}(\varphi) \in A$  and  $\epsilon_{\mathfrak{p}}(\varphi) \in \mathbb{F}_q^\times$  that do not depend on  $\mathfrak{a}$ .

We can explicitly compute  $\epsilon_{\mathfrak{p}}(\varphi)$ : Let  $\bar{T}$  be the image of  $T$  in  $\mathbb{F}_{\mathfrak{p}}$ . By Theorem 2.11 of [Gek08] (with  $L = \mathbb{F}_{\mathfrak{p}}$ ) we have

$$\epsilon_{\mathfrak{p}}(\varphi) = (-1)^{\deg \mathfrak{p}} N_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_q}(-\bar{T}^{q-1})^{-1} = (N_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_q}(\bar{T})^{q-1})^{-1} = 1.$$

(where the last equality uses that  $N_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_q}(\bar{T}) \neq 0$  since  $\mathfrak{p} \neq T$ ). Thus  $(\det \circ \bar{\rho}_{\varphi, \mathfrak{a}})(\text{Frob}_{\mathfrak{p}}) \equiv \mathfrak{p} \equiv \bar{\rho}_{C, \mathfrak{a}}(\text{Frob}_{\mathfrak{p}}) \pmod{\mathfrak{a}}$ . Using the Chebotarev density theorem, we find that the characters  $\det \circ \bar{\rho}_{\varphi, \mathfrak{a}}: G_F \rightarrow (A/\mathfrak{a})^\times$  and  $\bar{\rho}_{C, \mathfrak{a}}: G_F \rightarrow (A/\mathfrak{a})^\times$  are the same.

**Proposition 2.2.** *The representation  $\det \circ \bar{\rho}_{\varphi, \mathfrak{a}}: G_F \rightarrow (A/\mathfrak{a})^\times$  equals  $\bar{\rho}_{C, \mathfrak{a}}$ , and hence satisfies the properties of Proposition 2.1.*

*Remark 2.3.* That  $\det \circ \rho_{\varphi} = \rho_C$  is not a surprising coincidence. In the category of  $T$ -motives it makes sense to take the ‘‘determinant’’ of  $\varphi$  which gives a rank one Drinfeld  $A$ -module defined by  $T \mapsto T + T^{q-1}\tau$ , and this is isomorphic to  $C$  over  $F$ .

### 3. THE DRINFELD-TATE UNIFORMIZATION

We now fix some notation that will hold for the rest of the section. Let  $\mathcal{O}$  be a complete discrete valuation ring containing  $A$ ,  $\mathfrak{m} \subset \mathcal{O}$  the maximal ideal,  $K$  the field of fractions of  $\mathcal{O}$ , and  $K^{\text{sep}}$  a separable closure of  $K$ . Let  $v: K^\times \rightarrow \mathbb{Z}$  be the associated discrete valuation (we will also denote by  $v$  the corresponding  $\mathbb{Q}$ -valued extension of  $v$  to  $K^{\text{sep}}$ ). Let  $I_K$  be the inertia subgroup of  $G_K$  and let  $K^{\text{un}}$  be the maximally unramified extension of  $K$  in  $K^{\text{sep}}$ . We will return to our specific Drinfeld module  $\varphi$  in §3.5.

**3.1. Stable reduction.** Let  $\phi: A \rightarrow K\{\tau\}$  be a Drinfeld module of rank  $r$ . We say that  $\phi$  has **stable reduction** if there exists a Drinfeld module  $\phi': A \rightarrow \mathcal{O}\{\tau\}$  such that  $\phi'$  and  $\phi$  are isomorphic over  $K$  and the reduction of  $\phi'$  modulo  $\mathfrak{m}$  is Drinfeld module (i.e., the degree of the reduction of  $\phi'_T$  is greater than 1). We say that  $\phi$  has **stable reduction of rank  $r_1$**  if it has stable reduction and the rank of  $\phi'$  modulo  $\mathfrak{m}$  is  $r_1$ . We say that  $\phi$  has **good reduction** if it has stable reduction of rank  $r$ . Every Drinfeld  $A$ -module over  $K$  has **potentially stable reduction** (i.e., has stable reduction after possibly a finite separable extension of the field  $K$ ).

If  $\phi: A \rightarrow K\{\tau\}$  is a Drinfeld module of rank 2, then the  $j$ -invariant of  $\phi$  is defined to be  $j_\phi = g^{q+1}/\Delta$  where  $\phi_T = T + g\tau + \Delta\tau^2$ . Two Drinfeld  $A$ -modules over  $K$  of rank 2 have the same  $j$ -invariant if and only if they are isomorphic over  $\bar{K}$ . The Drinfeld module  $\phi$  has **potentially good reduction** if and only if  $v(j_\phi) \geq 0$  (cf. [Ros03, Lemma 5.2]).

### 3.2. Image of inertia at places of stable bad reduction.

**Proposition 3.1.** *Let  $\phi: A \rightarrow K\{\tau\}$  be a Drinfeld module of rank 2 of generic characteristic that has stable reduction of rank 1. Let  $\mathfrak{a}$  be a non-zero proper ideal of  $A$ .*

(i) *There is a basis of  $\phi[\mathfrak{a}]$  over  $A/\mathfrak{a}$  such that for  $\bar{\rho}_{\phi, \mathfrak{a}}: G_K \rightarrow \text{Aut}(\phi[\mathfrak{a}]) \cong \text{GL}_2(A/\mathfrak{a})$  we have*

$$\bar{\rho}_{\phi, \mathfrak{a}}(I_K) \subseteq \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} : b \in A/\mathfrak{a}, c \in \mathbb{F}_q^\times \right\}.$$

(ii) *Let  $e_\phi$  be the order of  $\frac{v(j_\phi)}{(q-1)N(\mathfrak{a})} + \mathbb{Z}$  in  $\mathbb{Q}/\mathbb{Z}$ . Then  $\bar{\rho}_{\phi, \mathfrak{a}}(I_K) \geq e_\phi$ .*

**3.3. Drinfeld-Tate uniformization.** Let  $\psi: A \rightarrow \mathcal{O}\{\tau\}$  be a Drinfeld module. A  $\psi$ -lattice is a finitely generated projective  $A$ -submodule  $\Gamma$  of  ${}^\psi K^{\text{sep}}$  that is discrete and is stable under the action of  $G_K$ . By discrete we mean that any disc of finite radius in  $K^{\text{sep}}$ , with respect to the valuation  $v$ , contains only finitely many elements of  $\Gamma$ .

**Definition 3.2.** A Tate datum over  $\mathcal{O}$  is a pair  $(\psi, \Gamma)$ , where  $\psi$  is a Drinfeld module over  $\mathcal{O}$  and  $\Gamma$  is a  $\psi$ -lattice. We say that two pairs  $(\psi, \Gamma)$  and  $(\psi', \Gamma')$  of Tate datum are isomorphic if there is an isomorphism  $f$  of  $\psi$  to  $\psi'$  such that the corresponding homomorphism  ${}^\psi K^{\text{sep}} \rightarrow {}^{\psi'} K^{\text{sep}}$  of  $A$ -modules induces an isomorphism between  $\Gamma$  and  $\Gamma'$ .

**Proposition 3.3** (Drinfeld). *Let  $r_1$  and  $r_2$  be positive integers. There is a natural bijection between the following:*

- (a) *the set of  $K$ -isomorphism classes of Drinfeld modules  $\phi: A \rightarrow K\{\tau\}$  of rank  $r := r_1 + r_2$  with stable reduction of rank  $r_1$ ;*
- (b) *the set of  $K$ -isomorphism classes of Tate datum  $(\psi, \Gamma)$  where  $\psi: A \rightarrow \mathcal{O}\{\tau\}$  is a Drinfeld module of rank  $r_1$  with good reduction and  $\Gamma$  is a  $\psi$ -module of rank  $r_2$ .*

The proposition is not very meaningful as stated; we shall now give a brief description of the implied correspondence. The correspondence is called the Drinfeld-Tate uniformization (see [Dri74, §7], and for more details see [Leh09, Chapter 4 §3]).

We start with a Drinfeld module  $\psi: A \rightarrow \mathcal{O}\{\tau\}$  of rank  $r_1$  with good reduction and a  $\psi$ -lattice  $\Gamma$  of rank  $r_2$ . Define the power series

$$e_\Gamma(X) = X \prod_{\gamma \in \Gamma, \gamma \neq 0} \left(1 - \frac{X}{\gamma}\right) \in \mathcal{O}[[X]],$$

it is  $\mathbb{F}_q$ -linear with an infinite radius of convergence and  $e_\Gamma(X) \equiv X \pmod{\mathfrak{m}}$  (the discreteness of  $\Gamma$  is key here). We may then view  $e_\Gamma$  as an element of  $\mathcal{O}\{\{\tau\}\}$ ; the (non-commutative) ring of formal power series in  $\tau$  with coefficients in  $\mathcal{O}$ . There exists a unique Drinfeld  $A$ -module  $\phi$  over  $\mathcal{O}$  such that  $e_\Gamma \psi_a = \phi_a e_\Gamma$  holds for all  $a \in A$ . This is the desired Drinfeld module  $\phi$ ; it has rank  $r_1 + r_2$  with stable reduction of rank  $r_1$ . That  $\phi$  has stable reduction of rank  $r_1$  is clear since  $\phi_T \equiv \phi_T e_\Gamma = e_\Gamma \psi_T \equiv \psi_T \pmod{\mathfrak{m}}$  and  $\psi$  has good reduction.

In the other direction, start with a Drinfeld  $A$ -module  $\phi$  of rank  $r := r_1 + r_2$  over  $K$  which has stable reduction of rank  $r_1$ . After possibly replacing  $\phi$  with a  $K$ -isomorphic Drinfeld module, we may assume that  $\phi$  takes values in  $\mathcal{O}\{\tau\}$ . There exists a unique Drinfeld module  $\psi: A \rightarrow \mathcal{O}\{\tau\}$  of rank  $r_1$  and a unique element  $u = \tau^0 + \sum_{i=1}^{\infty} a_i \tau^i \in \mathcal{O}\{\{\tau\}\}$  with  $a_i \in \mathfrak{m}$  and  $|a_i| \rightarrow 0$ , such that

$$(3.1) \quad u\psi_a = \phi_a u$$

for all  $a \in A$ . Drinfeld shows that  $u$  defines an analytic homomorphism. Let  $\Gamma$  be the kernel of  $u$ . It is a subgroup of  $K^{\text{sep}}$ , and moreover it is a  $\psi$ -lattice of rank  $r_2$ . The pair  $(\psi, \Gamma)$  is the desired Tate uniformization of  $\phi$ .

Fix an  $a \in A - \mathbb{F}_q$ . In the proof that  $\Gamma$  is a lattice, one makes use of the following  $G_K$ -equivariant short exact sequence of  $A$ -modules:

$$(3.2) \quad 1 \rightarrow \psi[a] = \psi_a^{-1}(0) \rightarrow \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\psi_a} \Gamma/a\Gamma \rightarrow 1.$$

We also have an isomorphism

$$(3.3) \quad \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\sim} \phi[a], \quad z + \Gamma \mapsto u(z)$$

of  $A[G_K]$ -modules (it is a well-defined map by (3.1)).

**3.4. Proof of Proposition 3.1.** Fix a Drinfeld module  $\phi: A \rightarrow \mathcal{O}\{\tau\}$  of rank 2 that has stable reduction of rank 1. Let  $(\psi, \Gamma)$  be the corresponding Tate uniformization as in §3.3. We have  $\mathfrak{a} = (a)$  for some  $a \in A$ . Using the isomorphism (3.3), it suffices to prove the analogous statement of the proposition for  $\psi_a^{-1}(\Gamma)/\Gamma$ . We first consider the Galois action on the pieces  $\psi[\mathfrak{a}]$  and  $\Gamma/a\Gamma$ .

The Drinfeld module  $\psi: A \rightarrow \mathcal{O}\{\tau\}$  has rank 1 and good reduction, so the Galois representation  $\bar{\rho}_{\psi, \mathfrak{a}}: G_K \rightarrow \text{Aut}(\psi[\mathfrak{a}]) = (A/\mathfrak{a})^\times$  is unramified. Choose a generator  $w$  of  $\psi[\mathfrak{a}]$  as an  $A/\mathfrak{a}$ -module; thus  $\sigma(w) = w$  for all  $\sigma \in I_K$ .

The lattice  $\Gamma$  is a free  $A$ -module of rank 1. Fix a generator  $\gamma$  of  $\Gamma$ , it is well-defined up to multiplication by an element of  $\mathbb{F}_q^\times$ . Since the lattice  $\Gamma$  is stable under the Galois action, there is a character  $\chi_\Gamma: G_K \rightarrow \mathbb{F}_q^\times$  such that  $\sigma(\gamma) = \chi_\Gamma(\sigma)\gamma$  for all  $\sigma \in G_K$ .

Choose a  $z \in K^{\text{sep}}$  for which  $\psi_a(z) = \gamma$  (this is equivalent to choosing a splitting of the short exact sequence (3.2) of  $A/\mathfrak{a}$ -modules). For any  $\sigma \in I_K$ ,

$$\psi_a(\sigma(z)) = \sigma(\psi_a(z)) = \sigma(\gamma) = \chi_\Gamma(\sigma)\gamma = \chi_\Gamma(\sigma)\psi_a(z) = \psi_a(\chi_\Gamma(\sigma)z).$$

Thus  $\sigma(z) - \chi_\Gamma(\sigma)z \in \psi[\mathfrak{a}]$ , hence there exists a unique  $b_\sigma \in A/\mathfrak{a}$  such that

$$\sigma(z) = \chi_\Gamma(\sigma)z + b_\sigma w.$$

Thus with respect to the basis  $\{w + \Gamma, z + \Gamma\}$  of  $\psi_a^{-1}(\Gamma)/\Gamma$ , an automorphism  $\sigma \in I_K$  acts via the matrix

$$\begin{pmatrix} 1 & b_\sigma \\ 0 & \chi_\Gamma(\sigma) \end{pmatrix}.$$

This proves part (i).

If  $v(z) \geq 0$ , then  $v(\gamma) = v(\psi_a(z)) \geq 0$  since  $\psi_a$  has coefficients in  $\mathcal{O}$ . However the discreteness of the lattice  $\Gamma$  implies that  $v(\gamma) < 0$ , so we must have  $v(z) < 0$ . Therefore,

$$v(\gamma) = v(\psi_a(z)) = v(z^{q^{\deg a}}) = q^{\deg a}v(z) = N(\mathfrak{a})v(z).$$

Let  $K'$  be the smallest extension of  $K^{\text{un}}$  in  $K^{\text{sep}}$  for which  $\text{Gal}(K^{\text{sep}}/K')$  acts trivially on  $\psi_a^{-1}(\Gamma)/\Gamma$ . The field  $K'$  is of course equal to  $K^{\text{un}}(\phi[\mathfrak{a}])$ , and  $\bar{\rho}_{\phi, \mathfrak{a}}(I_K) \cong \text{Gal}(K'/K)$ . Since  $\psi[\mathfrak{a}] \subseteq K^{\text{un}}$ , we find that  $K' = K^{\text{un}}(z)$ . The ramification index of the extension  $K^{\text{un}}(z)/K^{\text{un}}$  is at least the order of  $v(z) + \mathbb{Z}$  in  $\mathbb{Q}/\mathbb{Z}$ . By [Ros03, Lemma 5.3], we have  $v(\gamma) = v(j_\phi)/(q-1)$  and thus

$$v(z) = \frac{v(\gamma)}{N(\mathfrak{a})} = \frac{v(j_\phi)}{(q-1)N(\mathfrak{a})}.$$

Part (ii) now follows immediately.

**3.5. Our example.** We will now apply the above theory to our specific Drinfeld module  $\varphi: A \rightarrow F\{\tau\}$  with  $\varphi_T = T + \tau - T^{q-1}\tau^2$ .

**Proposition 3.4.** *Let  $I_T$  be an inertia subgroup of  $G_F$  at  $T$ . For any non-zero ideal  $\mathfrak{a}$  of  $A$ ,  $\bar{\rho}_{\phi, \mathfrak{a}}(I_T)$  is a  $p$ -Sylow subgroup of  $\text{Aut}(\phi[\mathfrak{a}]) \cong \text{GL}_2(A/\mathfrak{a})$ . Equivalently,  $\#\bar{\rho}_{\phi, \mathfrak{a}}(I_T) = N(\mathfrak{a})$ .*

*Proof.* The Drinfeld module  $\varphi$  has stable reduction of rank 1 at  $(T)$ . Let  $K = F((T))$  be the completion of  $F$  with respect to  $T$ , and let  $v_T$  be the corresponding valuation (normalized so that  $v_T(T) = 1$ ).

We know from Proposition 2.2 that  $\det \circ \bar{\rho}_{\varphi, \mathfrak{a}} = \bar{\rho}_{C, \mathfrak{a}}$ . Since  $C$  has good reduction at  $(T)$ , we must have  $\det(\bar{\rho}_{\varphi, \mathfrak{a}}(I_K)) = \bar{\rho}_{C, \mathfrak{a}}(I_K) = 1$ . This combined with Proposition 3.1(i) shows that  $\bar{\rho}_{\varphi, \mathfrak{a}}(I_K)$  is contained in a subgroup of  $\text{GL}_2(A/\mathfrak{a})$  of order  $N(\mathfrak{a})$ . By Proposition 3.1(ii),  $v_T(j_\phi) = -(q-1)$  implies that  $\#\bar{\rho}_{\varphi, \mathfrak{a}}(I_T) \geq N(\mathfrak{a})$ .  $\square$

#### 4. IRREDUCIBILITY

**Proposition 4.1.** *The  $\mathbb{F}_\lambda[G_F]$ -module  $\varphi[\lambda]$  is irreducible for every finite place  $\lambda$  of  $F$ .*

On the contrary, we will suppose for the rest of this section that  $\varphi[\lambda]$  is a reducible  $\mathbb{F}_\lambda[G_F]$ -module for a fixed  $\lambda$ . We shall eventually obtain a contradiction and thus prove Proposition 4.1. The strategy of this section is based on §5.4 of [Ser72].

By choosing an appropriate basis of  $\varphi[\lambda]$ , we may assume that the image of  $\bar{\rho}_{\varphi,\lambda}: G_F \rightarrow \text{Aut}(\varphi[\lambda]) \cong \text{GL}_2(\mathbb{F}_\lambda)$  lies in the group of upper triangular matrices. Moreover, there are two characters  $\chi$  and  $\chi': G_F \rightarrow \mathbb{F}_\lambda^\times$  such that  $\bar{\rho}_\lambda$  is represented in matrix form by  $\begin{pmatrix} \chi & * \\ 0 & \chi' \end{pmatrix}$ . We will now try to determine these characters.

**Lemma 4.2.** *The characters  $\chi$  and  $\chi'$  are unramified at all finite places  $\mathfrak{p} \neq \lambda$ . One of these two characters is unramified at all the finite places of  $F$ .*

*Proof.* First consider the place  $\mathfrak{p} = (T)$ . By Proposition 3.4 every element of  $\bar{\rho}_{\varphi,\lambda}(I_{\mathfrak{p}})$  has order 1 or  $p$  (where  $I_{\mathfrak{p}}$  is the inertia subgroup of  $G_F$  at  $\mathfrak{p}$ ). Therefore,  $\chi(I_{\mathfrak{p}}) = 1$  and  $\chi'(I_{\mathfrak{p}}) = 1$  since both take values in a group of cardinality relatively prime to  $p$ .

Now consider a finite place  $\mathfrak{p}$  not equal to  $\lambda$  or  $(T)$ . Since  $\varphi$  has good reduction at  $\mathfrak{p}$ , we find that  $\bar{\rho}_{\varphi,\lambda}$  is unramified at  $\mathfrak{p}$  and hence so are  $\chi'$  and  $\chi''$ .

Finally consider the case where  $\mathfrak{p} = \lambda$  and  $\mathfrak{p} \neq (T)$ . The reduction of  $\varphi$  modulo  $\mathfrak{p}$  has height 1 (if it had height 2, then [PR09b, Proposition 2.7(ii)] would imply that  $\varphi[\lambda]$  is an irreducible  $G_F$ -module). By [PR09b, Proposition 2.7],  $\bar{\rho}_{\varphi,\lambda}(I_{\mathfrak{p}})$  acts on  $\varphi[\lambda]$  via matrices of the form  $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$  with respect to an appropriate basis. Hence  $\chi(I_{\mathfrak{p}}) = 1$  or  $\chi'(I_{\mathfrak{p}}) = 1$ .  $\square$

**Lemma 4.3.** *One of the character  $\chi, \chi': G_F \rightarrow \mathbb{F}_\lambda^\times$  is of the form*

$$G_F \twoheadrightarrow \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \rightarrow \mathbb{F}_\lambda^\times$$

where the first map is restriction.

*Proof.* By Lemma 4.2 one of the characters  $\chi$  or  $\chi': G_F \rightarrow \mathbb{F}_\lambda^\times$ , without loss of generality  $\chi'$ , is unramified at all finite places of  $F$ . Thus we may view  $\chi'$  as a  $\mathbb{F}_\lambda^\times$ -valued character of the étale fundamental group of  $\mathbb{A}_{\mathbb{F}_q}^1$ . Since  $\mathbb{A}_{\mathbb{F}_q}^1$  has no non-trivial étale covers of order prime to  $p$ , we deduce that  $\chi': G_F \rightarrow \mathbb{F}_\lambda^\times$  is trivial on  $\text{Gal}(F^{\text{sep}}/\overline{\mathbb{F}}_q(T))$ . The lemma is now immediate.  $\square$

We can now express the values  $a_{\mathfrak{p}}(\varphi) \bmod \lambda$  in terms of the characters  $\chi$  and  $\chi'$ .

**Lemma 4.4.** *Let  $\lambda$  be a finite place of  $F$  for which  $\varphi[\lambda]$  is a reducible  $\mathbb{F}_\lambda[G_F]$ -module. There is a  $\zeta \in \mathbb{F}_\lambda^\times$  such that for any monic irreducible polynomial  $\mathfrak{p} \in A$  that is not  $T$  or  $\lambda$ , we have*

$$(4.1) \quad a_{\mathfrak{p}}(\varphi) \equiv \zeta^{-\deg \mathfrak{p}} \mathfrak{p} + \zeta^{\deg \mathfrak{p}} \pmod{\lambda}.$$

*Proof.* By Lemma 4.3, one of the characters  $\chi, \chi': G_F \rightarrow \mathbb{F}_\lambda^\times$ , say  $\chi'$ , factors through a character  $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \rightarrow \mathbb{F}_\lambda^\times$ . Hence there is a  $\zeta \in \mathbb{F}_\lambda^\times$  such that  $\chi'(\text{Frob}_{\mathfrak{p}}) = \zeta^{\deg \mathfrak{p}}$  for any monic irreducible polynomial  $\mathfrak{p}$  that is not  $T$  or  $\lambda$ . By Proposition 2.2, we know that  $\chi(\text{Frob}_{\mathfrak{p}})\chi'(\text{Frob}_{\mathfrak{p}}) = \det(\bar{\rho}_{\varphi,\lambda}(\text{Frob}_{\mathfrak{p}})) \equiv \mathfrak{p} \bmod \lambda$ , hence

$$\chi(\text{Frob}_{\mathfrak{p}}) \equiv \zeta^{-\deg \mathfrak{p}} \mathfrak{p} \pmod{\lambda} \quad \text{and} \quad \chi'(\text{Frob}_{\mathfrak{p}}) = \zeta^{\deg \mathfrak{p}} \pmod{\lambda}.$$

We deduce that

$$a_{\mathfrak{p}}(\varphi) \equiv \text{tr}(\bar{\rho}_{\varphi,\lambda}(\text{Frob}_{\mathfrak{p}})) = \chi(\text{Frob}_{\mathfrak{p}}) + \chi'(\text{Frob}_{\mathfrak{p}}) \equiv \zeta^{-\deg \mathfrak{p}} \mathfrak{p} + \zeta^{\deg \mathfrak{p}} \pmod{\lambda}. \quad \square$$

So by checking (4.1) for various primes  $\mathfrak{p}$ , we will be able to rule out many  $\lambda$ ; it turns out that we will only need to consider  $\mathfrak{p}$  of degree 1.

**Lemma 4.5.** *Let  $\mathfrak{p}$  be the irreducible polynomial  $T - c \in A$  with  $c \in \mathbb{F}_q^\times$ . Then  $a_{\mathfrak{p}}(\varphi) = 1$ .*

*Proof.* The image of  $T$  in  $\mathbb{F}_{\mathfrak{p}}$  is  $c$ . By Proposition 2.14(ii) of [Gek08] (with  $L = \mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$ ) we have  $a_{\mathfrak{p}}(\varphi) = -(-1/c^{q-1}) = 1$ .  $\square$

Since  $q \geq 5$ , there exist  $c_1, c_2 \in \mathbb{F}_q^\times$  such that  $\lambda, T - c_1$  and  $T - c_2$  are distinct. By Lemma 4.5 with  $\mathfrak{p} = T - c_i$ , we get

$$1 = \zeta^{-1}(T - c_i) + \zeta \pmod{\lambda}$$

This implies that  $T \equiv \zeta - \zeta^2 + c_i \pmod{\lambda}$  for distinct  $c_1, c_2 \in \mathbb{F}_q \subseteq \mathbb{F}_\lambda$ , which is impossible.

## 5. PROOF OF THEOREM 1.2

In different respects, Propositions 2.2, 3.4 and 4.1 all show that the group  $\rho_\varphi(G_F)$  is large. We now combine everything together to prove that indeed  $\rho_\varphi(G_F) = \mathrm{GL}_2(\widehat{A})$ . This will require some extra group theory which we have collected in Appendix A.

Let  $F^{\mathrm{ab}}$  be the maximal abelian extension of  $F$  in  $F^{\mathrm{sep}}$ . Note that  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) \subseteq \mathrm{SL}_2(A/\mathfrak{a})$  for each non-zero ideal  $\mathfrak{a}$  of  $A$ . We first show that the  $\lambda$ -adic representations of  $\varphi$  are surjective.

**Lemma 5.1.** *For every finite place  $\lambda$  of  $F$ , we have  $\rho_{\varphi, \lambda}(G_F) = \mathrm{GL}_2(A_\lambda)$  and  $\rho_{\varphi, \lambda}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A_\lambda)$ .*

*Proof.* By Propositions 4.1 and 3.4, the group  $\bar{\rho}_{\varphi, \lambda}(G_F) \subseteq \mathrm{GL}_2(\mathbb{F}_\lambda)$  acts irreducibly on  $\varphi[\lambda] \cong \mathbb{F}_\lambda^2$  as an  $\mathbb{F}_\lambda$ -module and it also contains a group of order  $N(\lambda)$ . From Lemma A.1, we deduce that  $\bar{\rho}_{\varphi, \lambda}(G_F) \supseteq \mathrm{SL}_2(\mathbb{F}_\lambda)$ . We have  $\bar{\rho}_{\varphi, \lambda}(G_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$  since  $\det(\bar{\rho}_{\varphi, \lambda}(G_F)) = \mathbb{F}_\lambda^\times$  by Proposition 2.2.

The group  $H := \rho_{\varphi, \lambda}(G_F)$  is closed in  $\mathrm{GL}_2(A_\lambda)$ , and satisfies  $\det(H) = A_\lambda^\times$  by Proposition 2.2. The group  $H \bmod \lambda^2 = \bar{\rho}_{\varphi, \lambda^2}(G_F)$  contains a non-scalar matrix that is congruent to the identity modulo  $\lambda$  by Proposition 3.4. We just verified that  $H \bmod \lambda = \bar{\rho}_{\varphi, \lambda}(G_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$ . Applying Lemma A.2, we deduce that  $H = \mathrm{GL}_2(A_\lambda)$ . The group  $\rho_{\varphi, \lambda}(G_{F^{\mathrm{ab}}})$  is just the commutator subgroup of  $H = \mathrm{GL}_2(A_\lambda)$  which from Lemma A.3 is  $\mathrm{SL}_2(A_\lambda)$ .  $\square$

Having surjective representations  $\rho_{\varphi, \lambda}$  is *not* enough to deduce that  $\rho_\varphi$  is surjective. There may be interdependencies between the representations. We now show that the mod  $\lambda$  representations are pairwise independent.

**Lemma 5.2.** *Let  $\lambda_1$  and  $\lambda_2$  be distinct finite places of  $F$ , and let  $\mathfrak{a} = \lambda_1 \lambda_2$  be the corresponding ideal of  $A$ . Then  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_F) = \mathrm{GL}_2(A/\mathfrak{a})$  and  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A/\mathfrak{a})$ .*

*Proof.* Define  $H := \bar{\rho}_{\varphi, \mathfrak{a}}(G_F)$  and  $H' := H \cap \mathrm{SL}_2(A/\mathfrak{a})$ . We shall verify the three conditions of Lemma A.7, which will then imply that  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_F) = \mathrm{GL}_2(A/\mathfrak{a})$ . We will then have  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A/\mathfrak{a})$  automatically since  $\mathrm{SL}_2(A/\mathfrak{a})$  is the commutator subgroup of  $\mathrm{GL}_2(A/\mathfrak{a})$  by Lemma A.3.

Condition (a) of Lemma A.7 follows from Proposition 2.2. By Lemma 5.1 we have  $\bar{\rho}_{\varphi, \lambda_i}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(\mathbb{F}_{\lambda_i})$ , so condition (b) follows since  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) \subseteq H'$ .

Take any  $c \in \mathbb{F}_q^\times$  such that  $\mathfrak{p} = T - c$  is not  $\lambda_1$  or  $\lambda_2$ . By Lemma 4.5, we have

$$\det(\bar{\rho}_{\varphi, \mathfrak{a}}(\mathrm{Frob}_{\mathfrak{p}})) / \mathrm{tr}(\bar{\rho}_{\varphi, \mathfrak{a}}(\mathrm{Frob}_{\mathfrak{p}}))^2 \equiv \mathfrak{p}/a_{\mathfrak{p}}(\varphi)^2 = \mathfrak{p} = T - c \pmod{\mathfrak{a}}.$$

One readily checks that the subring of  $A/\mathfrak{a}$  generated by the  $T - c$ , with at most two of the  $c \in \mathbb{F}_q^\times$  excluded, is all of  $A/\mathfrak{a}$ . This verifies condition (c) of Lemma A.7, and hence  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_F) = \mathrm{GL}_2(A/\mathfrak{a})$ .  $\square$

**Lemma 5.3.** *Let  $\lambda_1$  and  $\lambda_2$  be distinct finite places of  $F$ . Define*

$$\rho: G_F \rightarrow \mathrm{GL}_2(A_{\lambda_1}) \times \mathrm{GL}_2(A_{\lambda_2}), \quad \sigma \mapsto (\rho_{\varphi, \lambda_1}(\sigma), \rho_{\varphi, \lambda_2}(\sigma)).$$

*Then  $\rho(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$  and  $\rho(G_F) = \mathrm{GL}_2(A_{\lambda_1}) \times \mathrm{GL}_2(A_{\lambda_2})$ .*

*Proof.* To prove that  $\rho(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ , it suffices to show that for any positive integers  $n_1$  and  $n_2$ , we have

$$\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A/\mathfrak{a})$$

where  $\mathfrak{a} = \lambda_1^{n_1} \lambda_2^{n_2}$ . That  $\rho$  is surjective will follow from this and Proposition 2.2.

Suppose that  $H := \bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}})$  is not equal to  $\mathrm{SL}_2(A/\mathfrak{a}) = \mathrm{SL}_2(A/\lambda_1^{n_1}) \times \mathrm{SL}_2(A/\lambda_2^{n_2})$ . Let  $N_1$  and  $N_2$  be the kernels of the projections  $H \rightarrow \mathrm{SL}_2(A/\lambda_2^{n_2})$  and  $H \rightarrow \mathrm{SL}_2(A/\lambda_1^{n_1})$ , respectively. Each of these projections are surjective by Lemma 5.1. By Lemma A.4 we may view  $N_i$  as a normal subgroup of  $\mathrm{SL}_2(A/\lambda_i^{n_i})$  and the image of  $H$  in  $\mathrm{SL}_2(A/\lambda_1^{n_1})/N_1 \times \mathrm{SL}_2(A/\lambda_2^{n_2})/N_2$  is the graph of an isomorphism  $\mathrm{SL}_2(A/\lambda_1^{n_1})/N_1 \xrightarrow{\sim} \mathrm{SL}_2(A/\lambda_2^{n_2})/N_2$ .

By our assumption on  $H$ , the groups  $\mathrm{SL}_2(A/\lambda_i^{n_i})/N_i$  are non-trivial. So by Lemma A.3,  $N_i$  is a subgroup of the group of  $B \in \mathrm{SL}_2(A/\lambda_i^{n_i})$  with  $B \equiv \pm I \pmod{\lambda}$ . Therefore the image of  $H$  (equivalently, the image of  $\bar{\rho}_{\varphi, \lambda_1 \lambda_2}(G_{F^{\mathrm{ab}}})$ ) in

$$\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{\pm I\} \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$$

is the graph of an isomorphism  $\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{\pm I\} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$ . However, this contradicts Lemma 5.2 which says that  $\bar{\rho}_{\varphi, \lambda_1 \lambda_2}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$ . Therefore,  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A/\mathfrak{a})$ .  $\square$

We can now finish the proof of Theorem 1.2. Again by Proposition 2.2 we have  $\det(\rho_{\varphi}(G_F)) = \widehat{A}^{\times}$ , so it suffices to show that  $\rho_{\varphi}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(\widehat{A})$ . The equality  $\rho_{\varphi}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(\widehat{A})$  is equivalent to having

$$\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A/\mathfrak{a}) = \prod_{\lambda^n \parallel \mathfrak{a}} \mathrm{SL}_2(A/\lambda^n)$$

for every non-zero ideal  $\mathfrak{a}$  of  $A$ . By Lemma A.3, the groups  $\mathrm{SL}_2(A/\lambda^n)$  have no abelian quotients. Therefore by Lemma A.6, we need only show that  $\bar{\rho}_{\varphi, \mathfrak{a}}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(A/\mathfrak{a})$  for  $\mathfrak{a}$  of the form  $\lambda_1^{n_1} \lambda_2^{n_2}$  where  $\lambda_1$  and  $\lambda_2$  are distinct maximal ideals of  $A$ , and  $n_1$  and  $n_2$  are positive integers. This is immediate from Lemma 5.3.

## APPENDIX A. GROUP THEORY

In this appendix we collect all the group theory needed in §5 to prove our theorem. The point of that section was to show that certain closed subgroups of  $\mathrm{GL}_2(\widehat{A})$  and  $\mathrm{SL}_2(\widehat{A})$  (i.e.,  $\rho_{\varphi}(G_F)$  and  $\rho_{\varphi}(G_{F^{\mathrm{ab}}})$ , respectively) were the full groups. Note that the material in this section makes no reference to Drinfeld modules, though it will use our ongoing assumption that  $A = \mathbb{F}_q[T]$  with  $q \geq 5$  odd.

We start with the following easy generalization of [Ser68, IV-20 Lemma 2].

**Lemma A.1.** *Let  $\mathbb{F}$  be a finite field. Let  $H$  be a subgroup of  $\mathrm{GL}_2(\mathbb{F})$  such that:*

- $H$  contains a subgroup of order  $\#\mathbb{F}$ ;
- the  $\mathbb{F}[H]$ -module  $\mathbb{F}^2 = \mathbb{F} \times \mathbb{F}$  is irreducible.

*Then  $H$  contains  $\mathrm{SL}_2(\mathbb{F})$ .*

*Proof.* Let  $P_1$  be a subgroup of  $H$  of order  $\#\mathbb{F} = p^s$ ; it is a  $p$ -Sylow subgroup of  $\mathrm{GL}_2(\mathbb{F})$  and hence also of  $H$ . There is a unique one dimensional  $\mathbb{F}$ -subspace  $W_1$  of  $\mathbb{F}^2$  that is fixed by every element of  $P_1$ .

If  $P_1$  is a normal subgroup of  $H$ , then one finds that  $W_1$  is stable under the action of  $H$ , which would contradict our irreducibility assumption. Therefore, there is a second subgroup  $P_2 \neq P_1$  of  $H$  of cardinality  $\#\mathbb{F}$ . Let  $W_2$  be the unique one dimensional  $\mathbb{F}$ -subspace of  $\mathbb{F}^2$  that is fixed by every element of  $P_2$ .

With respect to a basis  $\{w_1, w_2\}$  of  $\mathbb{F}^2$  with  $w_1 \in W_1$  and  $w_2 \in W_2$ , the subgroups  $P_1$  and  $P_2$  of  $H$  become

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F} \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} : x \in \mathbb{F} \right\}$$

respectively. Now take any matrix  $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{SL}_2(\mathbb{F})$ . First suppose that  $B \neq 0$ . For  $a, b, c \in \mathbb{F}$ , we have

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 1+bc & b \\ a+c+abc & 1+ab \end{pmatrix}.$$

So setting  $b = B$  and solving  $1 + bc = A$  and  $1 + ab = D$  for  $a$  and  $c$  (recall that  $B \neq 0$ ), we find an expression for  $M$  as a product of matrices in  $P_1$  and  $P_2$  (that  $a + c + abc = C$  is automatic since our matrices have determinant 1 and  $b = B \neq 0$ ). Therefore  $M \in H$ . An analogous argument shows that  $M \in H$  when  $C \neq 0$ . Finally in the case  $B = C = 0$ , we simply note that  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ .  $\square$

The following two lemmas give some useful results about  $\text{GL}_2(A_\lambda)$  and  $\text{SL}_2(A_\lambda)$ .

**Lemma A.2.** *Let  $\lambda$  be a finite place of  $F$ , and let  $H$  be a closed subgroup of  $\text{GL}_2(A_\lambda)$ . Suppose that  $\det(H) = A_\lambda^\times$ , that  $H \bmod \lambda = \text{GL}_2(\mathbb{F}_\lambda)$ , and that  $H \bmod \lambda^2$  contains a non-scalar matrix that is congruent to the identity mod  $\lambda$ . Then  $H = \text{GL}_2(A_\lambda)$ .*

*Proof.* This is Proposition 4.1 of [PR09a] (note that  $N(\lambda) \geq q \geq 5$ ).  $\square$

**Lemma A.3.** *For each finite place  $\lambda$  of  $F$ , the group  $\text{SL}_2(A_\lambda)$  is its own commutator subgroup. The only normal subgroup of  $\text{SL}_2(A_\lambda)$  with simple quotient is the group consisting of the  $B \in \text{SL}_2(A_\lambda)$  for which  $B \equiv \pm I \bmod \lambda$ .*

*Proof.* We first prove that  $\text{SL}_2(A_\lambda)$  is its own commutator subgroup. Let  $H$  be the commutator subgroup of  $\text{SL}_2(A_\lambda)$ . It is a normal closed subgroup of  $\text{SL}_2(A_\lambda)$  and  $\text{GL}_2(A_\lambda)$ . Define  $S^0 := \text{SL}_2(A_\lambda)$ , and for each  $i \geq 1$  we let  $S^i$  be the group of  $s \in \text{SL}_2(A_\lambda)$  with  $s \equiv 1 \bmod \lambda^i$ . For  $i \geq 0$ , define  $H^i := H \cap S^i$ .

For  $i \geq 0$ , we define  $S^{[i]} := S^i/S^{i+1}$  and  $H^{[i]} := H^i/H^{i+1}$ . There is a natural inclusion  $H^{[i]} \hookrightarrow S^{[i]}$ , so it suffices to show that  $H^{[i]} = S^{[i]}$  for all  $i \geq 0$ .

Reduction modulo  $\lambda$  induces an isomorphism  $S^{[0]} \xrightarrow{\sim} \text{SL}_2(\mathbb{F}_\lambda)$  with the image of  $H^{[0]}$  being the commutator subgroup of  $\text{SL}_2(\mathbb{F}_\lambda)$ . Since  $\text{SL}_2(\mathbb{F}_\lambda)/\{\pm I\}$  is simple, we find that  $[\text{SL}_2(\mathbb{F}_\lambda) : H^{[0]}] = 1$  or 2. Since  $\text{SL}_2(\mathbb{F}_\lambda)$  is generated by elements of order  $p$  (use Lemma A.1), it has no normal subgroup of index 2. Therefore,  $H^{[0]} = S^{[0]}$ .

Now fix an  $i \geq 1$ . Let  $\mathfrak{sl}_2(\mathbb{F}_\lambda)$  be the (additive) group of matrices in  $M_2(\mathbb{F}_\lambda)$  with trace 0. We have an isomorphism

$$(A.1) \quad S^{[i]} \xrightarrow{\sim} \mathfrak{sl}_2(\mathbb{F}_\lambda), \quad [1 + \lambda^i y] \mapsto [y]$$

(where we are now viewing  $\lambda$  as a monic polynomial). Conjugation by  $\text{GL}_2(A_\lambda)$  acts on both sides of (A.1), and it factors through conjugation by  $\text{GL}_2(\mathbb{F}_\lambda)$ . By [PR09a, Proposition 2.1],  $\mathfrak{sl}_2(\mathbb{F}_\lambda)$  is an irreducible  $\text{GL}_2(\mathbb{F}_\lambda)$ -module (this uses that  $q$  is odd). Now consider  $H^{[i]} \hookrightarrow S^{[i]}$ . Since  $H$  is a normal subgroup of  $\text{GL}_2(A_\lambda)$ , we find that  $H^{[i]}$  is stable under the  $\text{GL}_2(\mathbb{F}_\lambda)$ -action. So we need only prove that  $H^{[i]} \neq 1$ .

Consider the commutator map  $S^0 \times S^i \rightarrow S^i$ ,  $(g, h) \mapsto ghg^{-1}h^{-1}$ . This induces a map  $S^{[0]} \times S^{[i]} \rightarrow S^{[i]}$  that takes values in  $H^{[i]}$ , and by using the identification  $S^{[0]} = \mathrm{SL}_2(\mathbb{F}_\lambda)$  and (A.1) it becomes

$$\mathrm{SL}_2(\mathbb{F}_\lambda) \times \mathfrak{sl}_2(\mathbb{F}_\lambda) \rightarrow \mathfrak{sl}_2(\mathbb{F}_\lambda), \quad (s, X) \mapsto sXs^{-1} - X.$$

This map is non-zero, so  $H^{[i]} \neq 1$ . Therefore,  $H = \mathrm{SL}_2(A_\lambda)$ .

Now let  $N$  be a normal subgroup of  $\mathrm{SL}_2(A_\lambda)$  for which  $\mathrm{SL}_2(A_\lambda)/N$  is simple. Since every  $p$ -group is solvable, the Jordan-Hölder factors of  $\mathrm{SL}_2(A_\lambda)$  are  $\mathrm{SL}_2(\mathbb{F}_\lambda)/\{\pm I\}$ ,  $\mathbb{Z}/2\mathbb{Z}$  and  $\mathbb{Z}/p\mathbb{Z}$ . We have just shown that  $\mathrm{SL}_2(A_\lambda)$  has no abelian quotients, so  $\mathrm{SL}_2(A_\lambda)/N \cong \mathrm{SL}_2(\mathbb{F}_\lambda)/\{\pm I\}$ . Let  $N'$  be the group consisting of  $B \in \mathrm{SL}_2(A_\lambda)$  with  $B \equiv \pm I \pmod{\lambda}$ , it is also a normal subgroup of  $\mathrm{SL}_2(A_\lambda)$  with quotient isomorphic to  $\mathrm{SL}_2(\mathbb{F}_\lambda)/\{\pm I\}$ . We must have  $N \subseteq N'$ , otherwise  $NN'/N'$  would be a non-trivial normal subgroup of  $\mathrm{SL}_2(A_\lambda)/N'$ . Similarly,  $N' \subseteq N$ .  $\square$

**Lemma A.4** (Goursat's lemma [Rib76, Lemma 5.2.1]). *Let  $B_1$  and  $B_2$  be finite groups and suppose that  $H$  is a subgroup of  $B_1 \times B_2$  for which the two projections  $p_1: H \rightarrow B_1$  and  $p_2: H \rightarrow B_2$  are surjective. Let  $N_1$  be the kernel of  $p_2$  and let  $N_2$  be the kernel of  $p_1$ . We may view  $N_1$  as a normal subgroup of  $B_1$  and  $N_2$  as a normal subgroup of  $B_2$ . Then the image of  $H$  in  $B_1/N_1 \times B_2/N_2$  is the graph of an isomorphism  $B_1/N_1 \xrightarrow{\sim} B_2/N_2$ .*

*Remark A.5.* In the setting of the above lemma, we will have  $H = B_1 \times B_2$  if and only if  $N_1 = B_1$  and  $N_2 = B_2$ .

**Lemma A.6** ([Rib76, Lemma 5.2.2]). *Let  $S_1, S_2, \dots, S_k$  be finite groups with no non-trivial abelian quotients. Let  $H$  be a subgroup of  $S_1 \times \dots \times S_k$  such that each projection  $H \rightarrow S_i \times S_j$  ( $1 \leq i < j \leq k$ ) is surjective. Then  $H = S_1 \times \dots \times S_k$ .*

The arguments in the next lemma were motivated by [Rib76, V §2].

**Lemma A.7.** *Let  $\lambda_1$  and  $\lambda_2$  be distinct maximal ideals of  $A$ , and set  $\mathfrak{a} = \lambda_1\lambda_2$ . Let  $H$  be a subgroup of  $\mathrm{GL}_2(A/\mathfrak{a})$  for which the following hold:*

- (a)  $\det(H) = (A/\mathfrak{a})^\times$ ;
- (b) the projections  $p'_1: H' \rightarrow \mathrm{SL}_2(\mathbb{F}_{\lambda_1})$  and  $p'_2: H' \rightarrow \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$  are surjective, where  $H' := H \cap \mathrm{SL}_2(A/\mathfrak{a})$ ;
- (c) the ring generated by the set

$$\mathcal{S} := \{\mathrm{tr}(h)^2/\det(h) : h \in H\} \cup \{\det(h)/\mathrm{tr}(h)^2 : h \in H \text{ with } \mathrm{tr}(h) \in (A/\mathfrak{a})^\times\}$$

is  $A/\mathfrak{a}$ .

Then  $H = \mathrm{GL}_2(A/\mathfrak{a})$ .

*Proof.* Let  $N'_1$  be the kernel of  $p'_2$  and let  $N'_2$  be the kernel of  $p'_1$ ; we may view  $N'_i$  as a normal subgroup of  $\mathrm{SL}_2(\mathbb{F}_{\lambda_i})$ . By Lemma A.4, the image of  $H'$  in  $\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/N'_1 \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/N'_2$  is the graph of a group isomorphism

$$(A.2) \quad \mathrm{SL}_2(\mathbb{F}_{\lambda_1})/N'_1 \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/N'_2.$$

If  $N'_1 = \mathrm{SL}_2(\mathbb{F}_{\lambda_1})$  (equivalently,  $N'_2 = \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$ ), then one has  $H' = \mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2}) = \mathrm{SL}_2(A/\mathfrak{a})$ . By (a), we conclude that  $H = \mathrm{GL}_2(A/\mathfrak{a})$ .

So now assume that  $N'_i$  is a proper normal subgroup of  $\mathrm{SL}_2(\mathbb{F}_{\lambda_i})$  for  $i = 1, 2$ . Using Lemma A.3, we find that  $N'_i \subseteq \{\pm I\}$ . From (A.2) and cardinality considerations, we deduce that  $N(\lambda_1) = N(\lambda_2)$  (equivalently,  $\mathbb{F}_{\lambda_1}$  and  $\mathbb{F}_{\lambda_2}$  are isomorphic fields).

For  $i \in \{1, 2\}$ , define the projection  $p_i: H \rightarrow \mathrm{GL}_2(\mathbb{F}_{\lambda_i})$ . Let  $N_1$  be the kernel of  $p_2$  and let  $N_2$  be the kernel of  $p_1$ ; we may view  $N_i$  as a normal subgroup of  $\mathrm{GL}_2(\mathbb{F}_{\lambda_i})$ . By Lemma A.4, the image of  $H$  in  $\mathrm{GL}_2(\mathbb{F}_{\lambda_1})/N_1 \times \mathrm{GL}_2(\mathbb{F}_{\lambda_2})/N_2$  is the graph of a group isomorphism

$$(A.3) \quad \mathrm{GL}_2(\mathbb{F}_{\lambda_1})/N_1 \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{F}_{\lambda_2})/N_2.$$

Since  $N_i/N'_i$  and  $N'_i$  are abelian, we find that  $N_i$  is a solvable normal subgroup of  $\mathrm{GL}_2(\mathbb{F}_{\lambda_i})$ . It is then readily checked that  $N'_i$  must be contained in the group of diagonal matrices of  $\mathrm{GL}_2(\mathbb{F}_{\lambda_i})$ . By taking further quotients, we find that the image of  $H$  in  $\mathrm{PGL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{PGL}_2(\mathbb{F}_{\lambda_2})$  is the graph of an isomorphism

$$\alpha: \mathrm{PGL}_2(\mathbb{F}_{\lambda_1}) \xrightarrow{\sim} \mathrm{PGL}_2(\mathbb{F}_{\lambda_2}).$$

By Theorem 3 of Hua's supplement in [Die80],  $\alpha$  lifts to an isomorphism

$$\tilde{\alpha}: \mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{F}_{\lambda_2}).$$

Let  $\sigma: \mathbb{F}_{\lambda_1} \xrightarrow{\sim} \mathbb{F}_{\lambda_2}$  be a field isomorphism and  $\chi: \mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \rightarrow \mathbb{F}_{\lambda_2}^\times$  a character; these define two group homomorphisms  $\mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{F}_{\lambda_2})$ :

$$(A.4) \quad A \mapsto \chi(A)A^\sigma, \quad A \mapsto \chi(A)((A^T)^{-1})^\sigma;$$

where  $B^\sigma$  represents the matrix obtained by applying  $\sigma$  coordinate-wise a matrix  $B \in \mathrm{GL}_2(\mathbb{F}_{\lambda_1})$ . By Theorem 1 of Hua's supplement in [Die80] (and using that  $\mathbb{F}_{\lambda_1} \cong \mathbb{F}_{\lambda_2}$ ), we find that there are  $\sigma$  and  $\chi$  such that  $\tilde{\alpha}$  is the composition of an inner automorphism with one of the homomorphisms of (A.4). We leave it to the reader to check that in either case, we have

$$\frac{\mathrm{tr}(\tilde{\alpha}(A))^2}{\det(\tilde{\alpha}(A))} = \sigma\left(\frac{\mathrm{tr}(A)^2}{\det(A)}\right).$$

Note that the map  $\mathrm{GL}_2(\mathbb{F}_{\lambda_i}) \rightarrow \mathbb{F}_{\lambda_i}$ ,  $A \mapsto \mathrm{tr}(A)^2/\det(A)$  factors through the projection  $\mathrm{GL}_2(\mathbb{F}_{\lambda_i}) \rightarrow \mathrm{PGL}_2(\mathbb{F}_{\lambda_i})$ . We deduce that  $\sigma(\mathrm{tr}(h_1)^2/\det(h_1)) = \mathrm{tr}(h_2)^2/\det(h_2)$  for every  $(h_1, h_2) \in H$ . Let  $W$  be the ring of  $(x_1, x_2) \in \mathbb{F}_{\lambda_1} \times \mathbb{F}_{\lambda_2} = A/\mathfrak{a}$  for which  $\sigma(x_1) = x_2$ . We have just verified that  $S \subseteq W$ . However,  $W \neq A/\mathfrak{a}$ , and this contradicts assumption (c).  $\square$

## REFERENCES

- [DH87] Pierre Deligne and Dale Husemoller, *Survey of Drinfeld modules*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), 1987, pp. 25–91. MR902591 (89f:11081) [↑1.1](#)
- [Die80] Jean Dieudonné, *On the automorphisms of the classical groups*, Memoirs of the American Mathematical Society, vol. 2, American Mathematical Society, Providence, R.I., 1980. With a supplement by Loo Keng Hua [Luo Geng Hua], Reprint of the 1951 original. MR606555 (82c:20079) [↑A, A](#)
- [Dri74] V. G. Drinfel'd, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656. MR0384707 (52 #5580) [↑1.1, 3.3](#)
- [Gek08] Ernst-Ulrich Gekeler, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721. MR2366959 (2008m:11114) [↑2.2, 4](#)
- [Gos96] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR1423131 (97i:11062) [↑1.1](#)
- [Gre09] Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, arXiv:0901.2513v1 [math.NT] (2009). [↑1.4](#)
- [Hay74] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91. [↑2.1](#)
- [Leh09] Thomas Lehmkuhl, *Compactification of the Drinfeld modular surfaces*, Mem. Amer. Math. Soc. **197** (2009), no. 921, xii+94. MR2488548 [↑3.3](#)
- [PR09a] Richard Pink and Egon Rüdtsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), no. 4, 882–907. MR2499412 [↑1.2, A, A](#)
- [PR09b] ———, *Image of the group ring of the Galois representation associated to Drinfeld modules*, J. Number Theory **129** (2009), no. 4, 866–881. MR2499411 [↑4](#)
- [Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. MR0457455 (56 #15660) [↑A.4, A.6, A](#)
- [Ros03] Michael Rosen, *Formal Drinfeld modules*, J. Number Theory **103** (2003), no. 2, 234–256. MR2020270 (2004j:11056) [↑3.1, 3.4](#)

- [Ser68] Jean-Pierre Serre, *Abelian  $l$ -adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR0263823 (41 #8422) ↑1.4, A
- [Ser72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283 (52 #8126) ↑1.4, 4

*E-mail address:* `zywina@math.upenn.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA 19104-6395, USA