DRINFELD MODULES WITH MAXIMAL GALOIS ACTION ON THEIR TORSION POINTS

DAVID ZYWINA

ABSTRACT. To each Drinfeld module over a finitely generated field with generic characteristic, one can associate a Galois representation arising from the Galois action on its torsion points. Pink and Rütsche have 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 their torsion points is as large as possible. We will follow the approach that Serre used to give explicit examples of his openness theorem for elliptic curves. Using our specific examples, we will numerically test analogues of some well-known elliptic curve conjectures.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with q elements. Let A be the ring $\mathbb{F}_q[T]$ and let F be its fraction field. For a given field extension K of $\mathbb{F}_q$, let $\overline{K}$ be an algebraic closure of K and let K^{sep} be the separable closure of K in $\overline{K}$. Denote by $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ 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 τ with coefficients in K that satisfy the commutation rule $\tau \cdot c = c^q \tau$ for $c \in K$. One can identify $K\{\tau\}$ with a subring of $\mathrm{End}(\mathbb{G}_{a,K})$ by identifying τ with the Frobenius map $X \mapsto X^q$. A Drinfeld A-module over K is a homomorphism

$$\phi \colon A \to K\{\tau\}, \quad a \mapsto \phi_a$$

of $\mathbb{F}_q$-algebras whose image is not contained in K. The Drinfeld module ϕ is determined by $\phi_T = \sum_{i=0}^r a_i \tau^i$ where $a_i \in K$ and $a_r \neq 0$; the positive integer r is called the rank of ϕ.

Let $\partial_0 \colon K\{\tau\} \to K$ be the ring homomorphism $\sum_i a_i \tau^i \mapsto a_0$. The characteristic of ϕ is the kernel $\mathfrak{p}_0$ of the homomorphism $\partial_0 \circ \phi \colon A \to K$. If $\mathfrak{p}_0$ is the zero ideal, then we say that ϕ has generic characteristic and we may then view K as an extension of F.

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

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

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

$$\bar{\rho}_{\phi,\mathfrak{a}} \colon G_K \to \mathrm{Aut}(\phi[\mathfrak{a}]) \cong \mathrm{GL}_r(A/\mathfrak{a}).$$

Let $\mathfrak{p}$ be a place of A. If ϕ 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 λ of A, we have a Galois representation

$$\rho_{\phi,\lambda} \colon G_K \to \mathrm{Aut}\left(\varinjlim_{i} \phi[\lambda^i]\right) \cong \mathrm{GL}_r(A_\lambda)$$

where A_λ is the λ-adic completion of A. These representations have properties similar to the familiar ℓ-adic representations attached to elliptic curves. For example, if ϕ has good reduction at $\mathfrak{p} \nmid \lambda$, then $P_{\phi,\mathfrak{p}}(x) := \det(xI - \rho_{\phi,\lambda}(\mathrm{Frob}_\mathfrak{p}))$ is a polynomial with coefficients in A that does not depend on λ. In particular, $a_\mathfrak{p}(\phi) := \mathrm{tr}(\rho_{\phi,\lambda}(\mathrm{Frob}_\mathfrak{p}))$ is an element of A that does not depend on λ. Combining all the representations together, we obtain a single Galois representation

$$\rho_\phi \colon G_K \to \mathrm{Aut}\left(\varinjlim_{\mathfrak{a}} \phi[\mathfrak{a}]\right) \cong \mathrm{GL}_r(\widehat{A})$$

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

1.2. **Open image theorem.** Pink and Rütsche have described the image of ρ_ϕ up to commensurability [PR09a]. For simplicity, we only state the version for which ϕ has no extra endomorphisms. Recall that the ring $\mathrm{End}_{\overline{K}}(\phi)$ of endomorphisms is the centralizer of $\phi(A)$ in $\overline{K}\{\tau\}$.

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

$$\rho_\phi \colon G_K \to \mathrm{GL}_r(\widehat{A})$$

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

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

The main objective of this paper is to compute the image of ρ_ϕ for an explicit example. This example also proves the existence of Drinfeld modules of rank 2 for which the Galois action on its torsion points is maximal. We will use our example to investigate various conjectures in §2.

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

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

Then the Galois representation

$$\rho_\varphi \colon G_{\mathbb{F}_q(T)} \to \mathrm{GL}_2\big(\widehat{\mathbb{F}_q[T]}\big)$$

is surjective. Moreover, $\rho_\varphi\big(G_{\overline{\mathbb{F}}_q(T)}\big) = \mathrm{GL}_2\big(\widehat{\mathbb{F}_q[T]}\big)$.

1.4. **Elliptic curves.** We now discuss the analogous theory of elliptic curves which 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 $E(K^{\mathrm{sep}})$ gives a representation

$$\bar{\rho}_{E,m} \colon G_K \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let $\mathfrak{p}$ be a non-zero prime ideal for which E has good reduction, then there is a unique polynomial $P_{E,\mathfrak{p}}(x) = x^2 - a_\mathfrak{p}(E)x + N(\mathfrak{p}) \in \mathbb{Z}[x]$ such that $P_{E,\mathfrak{p}}(x) \equiv \det(I - \bar{\rho}_{E,m}(\mathrm{Frob}_\mathfrak{p})) \pmod{m}$ when $\mathfrak{p} \nmid m$. Combining the representations $\bar{\rho}_{E,m}$ together, we obtain a single Galois representation

$$\rho_E \colon G_K \to \mathrm{Aut}\left(\varinjlim_m E[m]\right) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

In 1972, Serre [Ser72] showed that if $\mathrm{End}_{\overline{K}}(E) \cong \mathbb{Z}$, then ρ_E is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$; this is a clear analogue of Theorem 1.1. Earlier, Serre had shown that ρ_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 $\bar{\rho}_{E,\ell} \colon G_K \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ contains an element of order ℓ for all but finitely many primes ℓ (cf. the proposition of [Ser68, Chapter IV Appendix A.1.5]). Serre has given worked out examples of $\rho_E(G_K)$ for several non-CM elliptic curves over $K = \mathbb{Q}$ (cf. [Ser72, §5.5]). The first example with surjective ρ_E was given by A. Greicius [Gre10].

1.5. **Overview.** In §2, which is independent of the rest of the paper, we mention three well-known conjectures for elliptic curves. The heuristics and resulting predictions for these conjectures depend on the Galois action on the curve's torsion points. Having worked out the Galois image for a specific Drinfeld module of rank 2, we can now start doing numerical experiments on the analogous Drinfeld module statements.

The remainder of the paper is dedicated to the proof of Theorem 1.2.

In §3, we prove that the character $\det \circ \rho_\varphi \colon G_F \to \widehat{A}^\times$ is surjective. This will be accomplished by first recognizing that $\det \circ \rho_\varphi$ is the representation ρ_C associated with the Carlitz module C; this particular Drinfeld module has been extensively studied.

In §4, 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 φ 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 λ of A, $\bar{\rho}_{\varphi,\lambda}(G_F)$ contains a p-Sylow subgroup of $\mathrm{GL}_2(A/\lambda)$ where p is the prime dividing q.

In §5, we prove that $\varphi[\lambda]$ is an irreducible $\mathbb{F}_\lambda[G_F]$-module for all λ. If $\varphi[\lambda]$ is reducible, then we can understand the semi-simplification of the action of G_F on $\varphi[\lambda]$ in terms of two characters $\chi, \chi' \colon G_F \to \mathbb{F}_\lambda^\times$. 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 these three different contexts, we will 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 takes some serious work to prove that these representations are independent. For elliptic curves, one makes use of the easy fact that the groups $\mathrm{SL}_2(\mathbb{Z}_\ell)$ have no common quotients; this fails for the groups $\mathrm{SL}_2(A_\lambda)$ (just consider λ with the same degree). The required group theory is contained in a short appendix.

Notation. We fix throughout an odd prime power $q \geq 5$. We let A be the ring $\mathbb{F}_q[T]$ and we let F be the fraction field $\mathbb{F}_q(T)$. For a positive integer n, let $\pi_A(n)$ be the number of monic irreducible polynomials of degree n in A.

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

2. Some conjectures

Throughout this section, let E be a non-CM elliptic curve over $\mathbb{Q}$. For each prime p of good reduction, we have a finite abelian group $E(\mathbb{F}_p)$. Several number theoretic conjectures deal with the asymptotics of primes p for which $E(\mathbb{F}_p)$ has a fixed property. In §2.1, we discuss a conjecture that predicts the distribution of p for which $E(\mathbb{F}_p)$ is cyclic. In §2.2, we discuss a conjecture of Koblitz that predicts the distribution of p for which $E(\mathbb{F}_p)$ has prime cardinality. (These two conjectures are interesting in part because of public key cryptography where it is useful to have a point in $E(\mathbb{F}_p)$ that generates a group of large prime order.) Finally in §2.3, we mention a conjecture of Lang and Trotter on the number of primes p for which $a_p(E)$ takes a fixed value t. The precise Drinfeld module analogue for the Lang-Trotter conjecture is the least clear. We will not venture a full conjecture here, but hope to return to it in the future.

Before continuing, we recall a little more about the arithmetic of Drinfeld modules. For simplicity, we restrict our attention to a Drinfeld module

$$\phi\colon A \to F\{\tau\}$$

of rank 2 such that $\partial_0 \circ \phi\colon A \to F$ is the inclusion map and $\mathrm{End}_{\overline{F}}(\phi) = \phi(A)$; our numerical data will all be for the Drinfeld module φ of Theorem 1.2 with $q = 5$. Let $\mathfrak{p}$ be a non-zero prime ideal of A for which ϕ has good reduction; we will sometimes identify $\mathfrak{p}$ with its monic irreducible generator. Reduction mod $\mathfrak{p}$ induces a Drinfeld module $\phi_{\mathfrak{p}}\colon A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$ where $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}A$. We shall denote by ${}^{\phi}\mathbb{F}_{\mathfrak{p}}$, the group $\mathbb{F}_{\mathfrak{p}}$ equipped with the A-module action coming from $\phi_{\mathfrak{p}}$. Note that as an A-module, ${}^{\phi}\mathbb{F}_{\mathfrak{p}}$ need not be isomorphic to $A/\mathfrak{p}A$. For conjectures concerning the structure of the groups $E(\mathbb{F}_p)$, we will instead consider the structure of the A-modules ${}^{\phi}\mathbb{F}_{\mathfrak{p}}$. As an A-module ${}^{\phi}\mathbb{F}_{\mathfrak{p}}$ is isomorphic to

$$A/d_{\mathfrak{p}}A \times A/d_{\mathfrak{p}}e_{\mathfrak{p}}A$$

where $d_{\mathfrak{p}}$ and $e_{\mathfrak{p}}$ are unique monic polynomials in A. The Euler-Poincaré characteristic of ${}^{\phi}\mathbb{F}_{\mathfrak{p}}$ is the ideal

$$\chi_{\phi}(\mathfrak{p}) = d_{\mathfrak{p}}^2 e_{\mathfrak{p}} A.$$

We can relate the Euler characteristic to our Galois representations by noting that $\chi_{\phi}(\mathfrak{p})$ is the ideal of A generated by $P_{\phi,\mathfrak{p}}(1)$. For conjectures about the orders $|E(\mathbb{F}_p)| = P_{E,p}(1)$, the analogous object of study is $\chi_{\phi}(\mathfrak{p})$.

Let D_{ϕ} be the index of $\rho_{\phi}(G_{F\overline{\mathbb{F}}_q})$ in $\rho_{\phi}(G_F)$; it is known to be finite. By Theorem 1.2, we have $D_{\varphi} = 1$. Restriction gives an exact sequence

$$1 \to G_{F\overline{\mathbb{F}}_q} \hookrightarrow G_F \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \xrightarrow[\sim]{\mathrm{deg}} \widehat{\mathbb{Z}} \to 1$$

where $\deg(\mathrm{Frob}_{\mathfrak{p}})$ equals the degree of $\mathfrak{p}$ for irreducibles $\mathfrak{p}$ of A. For an integer n and a non-zero ideal $\mathfrak{a}$ of A, we define $\overline{\rho}_{\phi,\mathfrak{a}}(G_F)_n$ to be the image under $\overline{\rho}_{\phi,\mathfrak{a}}$ of $\{\sigma \in G_F : \deg(\sigma) \equiv n \pmod{D_{\phi}}\}$.

2.1. **Cyclicity of reductions modulo $\mathfrak{p}$.** For primes p of good reduction, the group $E(\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/d_p\mathbb{Z} \times \mathbb{Z}/d_p e_p\mathbb{Z}$ for unique positive integers d_p and e_p. It is natural to ask how often $E(\mathbb{F}_p)$ is cyclic ($d_p = 1$), that is, describe the asymptotics of the function

$$f_E(x) := \#\{p \le x : E(\mathbb{F}_p) \text{ is cyclic}\}.$$

Serre [Ser78] showed that, assuming the Generalized Riemann Hypothesis (GRH), one has

$$(2.1) \qquad\qquad f_E(x) \sim c_E \frac{x}{\log x}$$

as $x \to +\infty$, where $c_E := \sum_{m \ge 1} \mu(m)/[\mathbb{Q}(E[m]) : \mathbb{Q}]$ (see §5 of [Mur83] for a proof and §6 for an unconditional result in the CM case). If $c_E = 0$, then we interpret this as meaning that $f_E(x)$

4

is uniformly bounded. It is still unknown if (2.1) holds unconditionally. If $c_E > 0$, then Murty and Gupta [GM90] showed that $f_E(x) \gg_E x/\log^2 x$, and the constant c_E is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. For more background and progress on the conjecture, see [CM04].

The Drinfeld module analogue has been formulated and proven by W. Kuo and Y.-R. Liu [KL09]. We shall say that $^\phi\mathbb{F}_\mathfrak{p}$ is cyclic if it is isomorphic as an A-module to A/wA for some non-constant element w of A; equivalently, $d_\mathfrak{p} = 1$. For each positive integer n, we let $f_\phi(n)$ be the number of monic irreducible polynomials $\mathfrak{p}$ of degree n in A for which $^\phi\mathbb{F}_\mathfrak{p}$ is cyclic. Kuo and Liu have shown that

$$\lim_{n \to +\infty} \frac{f_\phi(n)}{\pi_A(n)} = c_\phi(n)$$

where $c_\phi(n)$ is an explicit constant whose value depends only on n modulo D_ϕ (recall that in the function field setting the analogue of GRH is known to hold). They also give a good bound on the error term, and prove a similar result for rank ≥ 3. Theorem 1.1 plays a vital role in their proof.

Let us now consider our Drinfeld module $\varphi \colon A \to F\{\tau\}$. Since $D_\varphi = 1$, we can simply write c_φ for the constant. The constant given in [KL09] is

$$c_\varphi = \sum_{m \in A \text{ monic}} \frac{\mu_q(m)}{[F(\varphi[m]) : F]}$$

where μ_q is the Möbius function for A (i.e., the multiplicative function that vanishes on polynomials with a multiple irreducible factor and is -1 for irreducible polynomials). By Theorem 1.2, we find that $\mu_q(m)/[F(\varphi[m]) : F] = \mu_q(m)/|\mathrm{GL}_2(A/mA)|$ is a multiplicative function, hence

$$c_\varphi = \prod_{\substack{\lambda \in A \\ \text{monic irreducible}}} \left(1 - \frac{1}{|\mathrm{GL}_2(A/\lambda A)|}\right) = \prod_{d=1}^{\infty} \left(1 - \frac{1}{q^d(q^d - 1)^2(q^d + 1)}\right)^{\pi_A(d)}.$$

This expression for c_φ is easy to estimate (note that $\pi_A(d)$ equals $\frac{1}{d}\sum_{e|d} \mu(e)q^{d/e}$).

For $q = 5$, we find that $c_\varphi = 0.989600049329883\ldots$. In Table 1, we see that, even for small n, the ratio $f_\varphi(n)/\pi_A(n)$ is well approximated by c_φ.

n	$f_\varphi(n)$	$\pi_A(n)$	$f_\varphi(n)/\pi_A(n)$
2	10	10	1
3	40	40	1
4	150	150	1
5	618	624	$0.99038461\ldots$
6	2554	2580	$0.98992248\ldots$
7	11069	11160	$0.99184587\ldots$
8	48270	48750	$0.99015384\ldots$
9	214807	217000	$0.98989400\ldots$
10	966135	976248	$0.98964095\ldots$
11	4392845	4438920	$0.98962022\ldots$

TABLE 1. Values of $f_\varphi(n)$ for small n where $\varphi \colon \mathbb{F}_5[T] \to \mathbb{F}_5(T)\{\tau\}$ is the Drinfeld module for which $T \mapsto T + \tau - T^4\tau^2$.

2.2. Koblitz conjecture.

Let $\mathcal{P}_E(x)$ be the number of primes $p \leq x$ of good reduction for which $|E(\mathbb{F}_p)|$ is prime. Koblitz conjectured that there is a constant C_E such that $\mathcal{P}_E(x) \sim C_E \dfrac{x}{(\log x)^2}$ as $x \to +\infty$, where $C_E \geq 0$ is an explicit constant. The constant, as revised in [Zyw11a], is

$$C_E = \lim_{m \to +\infty} \frac{|\{g \in \bar{\rho}_{E,m}(G_\mathbb{Q}) : \det(I - g) \in (\mathbb{Z}/m\mathbb{Z})^\times\}|/|\bar{\rho}_{E,m}(G_\mathbb{Q})|}{\prod_{p|m}(1 - 1/p)}$$

where m runs over positive square-free integers ordered by divisibility.

Let $\mathcal{P}_\phi(n)$ be the number of monic irreducible polynomials $\mathfrak{p}$ of degree n in A for which $\chi_\phi(\mathfrak{p})$ is a prime ideal (equivalently, $^\phi\mathbb{F}_\mathfrak{p}$ is a simple A-module). We conjecture that

(2.2) $$\mathcal{P}_\phi(n) \sim C_\phi(n)\frac{q^n}{n^2}$$

as $n \to +\infty$, where

$$C_\phi(n) = \lim_m \frac{|\{g \in \bar{\rho}_{\phi,m}(G_F)_n : \det(I - g) \in (A/mA)^\times\}|/|\bar{\rho}_{\phi,m}(G_F)_n|}{\prod_{\lambda|m,\,\lambda\,\text{prime}}(1 - 1/N(\lambda))}$$

and the m run over monic polynomials of A ordered by divisibility. The constant $C_\phi(n)$ is well-defined (one uses Theorem 1.1 to check convergence) and depends only on the value of n modulo D_ϕ. Analogues of Koblitz's conjecture for Drinfeld modules were first investigated in the Master's thesis of L. Jain [Jai08].

Let us give a crude heuristic for this conjecture. A "random" monic polynomial of degree n in A should be irreducible with probability $\pi_A(n)/q^n \approx 1/n$. So for each irreducible polynomial $\mathfrak{p}$ of degree n, we expect the degree n monic generator of $\chi_\phi(\mathfrak{p})$ to be irreducible with probability $1/n$. Thus a naive estimate for $\mathcal{P}_\phi(n)$ is $\pi_A(n)/n \approx q^n/n^2$. What this heuristic is ignoring is that the Euler characteristics $\chi_A(\mathfrak{p})$ are not random ideals when it comes to congruences. Fix a monic polynomial m in A. Then the ratio of irreducible polynomials $\mathfrak{p}$ of degree n for which m is relatively prime to $\chi_\phi(\mathfrak{p})$ is approximately $|\{g \in \bar{\rho}_{\phi,m}(G_F)_n : \det(I - g) \in (A/mA)^\times\}|/|\bar{\rho}_{\phi,m}(G_F)_n|$, while the naive ratio is $|(A/mA)^\times|/|A/mA| = \prod_{\lambda|m}(1 - 1/N(\lambda))$. So by taking into account congruences modulo m, we expect

$$\frac{|\{g \in \bar{\rho}_{\phi,m}(G_F)_n : \det(I - g) \in (A/mA)^\times\}|/|\bar{\rho}_{\phi,m}(G_F)_n|}{\prod_{\lambda|m,\,\lambda\,\text{prime}}(1 - 1/N(\lambda))}\frac{q^n}{n^2}$$

to be a better estimate for $\mathcal{P}_\phi(n)$. The conjecture (2.2) arises by letting m run over more and more divisible elements of A (it actually suffices to consider only squarefree m).

Now consider our Drinfeld module φ. Since $D_\varphi = 1$, we can simply write C_φ for the constant. Using Theorem 1.2, one can compute as in [Zyw11a] and show that

$$C_\varphi = \prod_\lambda \frac{|\{g \in \mathrm{GL}_2(A/\lambda) : \det(I - g) \in (A/\lambda A)^\times\}|/|\mathrm{GL}_2(A/\lambda A)|}{1 - 1/N(\lambda)}$$

$$= \prod_{d \geq 1}\left(1 - \frac{q^{2d} - q^d - 1}{(q^d - 1)^3(q^d + 1)}\right)^{\pi_A(d)}.$$

Taking $q = 5$, we find that $C_\varphi = 0.76075227630\ldots$. In Table 2, we numerically test our analogue of Koblitz's conjecture for small n.

n	$P_\varphi(n)$	$P_\varphi(n)/\left(\frac{5^n}{n^2}\right)$
2	5	0.8
3	10	0.72
4	41	1.0496
5	106	0.848
6	317	0.730368
7	1194	0.7488768
8	4540	0.7438336
9	18534	0.768642048
10	74724	0.76517376
11	307931	0.76308013056

TABLE 2. Numerical evidence for the Koblitz conjecture for the Drinfeld module $\varphi\colon \mathbb{F}_5[T] \to \mathbb{F}_5(T)\{\tau\}$, $T \mapsto T + \tau - T^4\tau^2$.

2.3. **Lang-Trotter.** Fix a positive integer t. In [LT76, Part I], Lang and Trotter conjectured that

$$|\{p \le x : a_p(E) = t\}| \sim C_{E,t}\frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, where $C_{E,t} \ge 0$ is an explicit constant. Again if $C_{E,t} = 0$, we interpret the asymptotic as meaning that there are only finitely many primes p such that $a_p(E) = t$. Their predicted constant is

$$C_{E,t} = \frac{2}{\pi} \lim_{m\to\infty} \frac{|\{g \in \bar\rho_{E,m}(G_\mathbb{Q}) : \operatorname{tr}(g) \equiv t \pmod{m}\}|/|\bar\rho_{E,m}(G_\mathbb{Q})|}{1/m}$$

where the limit is over positive integers m ordered by divisibility. Note that the value of $C_{E,t}$ depends only on the image of the representation $\rho_E\colon G_\mathbb{Q} \to \operatorname{GL}_2(\widehat{\mathbb{Z}})$. In particular, their conjecture implies that there are infinitely many primes p for which $a_p(E) = t$ if and only if if there are *no congruence obstructions* (i.e., for each m, there is one, and hence infinitely many, primes p of good reduction such that $a_p(E) \equiv t \pmod{m}$).

Now consider the Drinfeld module analogue. Fix an element $t \in A$. Let $\mathcal{P}_{\phi,t}(n)$ be the number of monic irreducible polynomials of degree n in A for which $a_\mathfrak{p}(\phi) = t$. We conjecture that there is a positive integer M_ϕ such that

$$(2.3) \qquad \mathcal{P}_{\phi,t}(n) \sim C_{\phi,t}(n)\frac{q^{n/2}}{n}$$

as $n \to +\infty$, where $C_{\phi,t}(n)$ are constants whose value depends only on n modulo M_ϕ. As we will see, the conjecture is in general false with $M_\phi = D_\phi$. This conjecture has been proven "on average" for $t = 0$ by C. David [Dav96], and the main theorem there suggests that $M_\phi = 2$ for a "random" ϕ.

Consider our Drinfeld module $\varphi\colon \mathbb{F}_q[T] \to \mathbb{F}_q(T)\{\tau\}$ from Theorem 1.2. The following proposition shows that when q is congruent to 1 modulo 4 and n is a sufficiently large *even* integer, we will always have $C_{\varphi,t}(n) = 0$.

Proposition 2.1. *Assume that $q \equiv 1 \pmod 4$. If n is an even integer and $\mathfrak{p} \ne (T)$ is an irreducible polynomial in A of degree n, then $a_\mathfrak{p}(t)$ has degree $n/2$.*

Proof. Let L be the field $\mathbb{F}_q[T]/\mathfrak{p}$. Since n is even, L contains a quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. By Hasse's bound, we know that $a_\mathfrak{p}(\varphi) = \sum_{i=1}^{n/2} a_i T^i$ with $a_i \in \mathbb{F}_q$. We need to check that $a_{n/2} \ne 0$.

7

By [Gek08, Proposition 2.14(i)] or [HY00, Theorem 5.1],

$$a_{n/2} = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\left(N_{L/\mathbb{F}_{q^2}}(-\overline{T}^{q-1})^{-1}\right) = \pm\,\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\left(N_{L/\mathbb{F}_{q^2}}(\overline{T}^{q-1})^{-1}\right).$$

Let $\alpha := N_{L/\mathbb{F}_{q^2}}(\overline{T}^{q-1})^{-1} \in \mathbb{F}_{q^2}^{\times}$. Assume that $a_{n/2} = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha)$ is equal to 0; we shall derive a contradiction. We have $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = (N_{L/\mathbb{F}_q}(\overline{T})^{q-1})^{-1} = 1^{-1} = 1$, so α is a root of the polynomial

$$x^2 - \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha)x + N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = x^2 + 1.$$

Since $q \equiv 1 \pmod{4}$, we deduce that $\alpha \in \mathbb{F}_q^{\times}$ and hence $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 2\alpha \neq 0$. $\qquad\square$

When $q \equiv 1 \pmod 4$, the same obstruction to $a_{\mathfrak{p}}(\varphi) = t$ does not occur when we restrict to $\mathfrak{p}$ of odd degree. Moreover, there are infinitely many $\mathfrak{p}$, with necessarily odd degree, for which $a_{\mathfrak{p}}(\varphi) = 0$ (this follows from Theorem 1.1.6 of [Bro92] with the correction mentioned in §2 of [Poo98]). In fact, it is not unreasonable to expect that $C_{\varphi,t}(n) > 0$ whenever n is odd.

What makes Proposition 2.1 surprising, at least in contrast to the elliptic curve case, is that it cannot be explained by congruence obstructions. Indeed, the elements $\rho_{\varphi}(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p}$ of *even* degree are dense in $\rho_{\varphi}\big(G_{\mathbb{F}_{q^2}(T)}\big) = \mathrm{GL}_2(\widehat{A})$, so for each non-zero ideal $\mathfrak{a}$ of A there are infinitely many $\mathfrak{p}$ of even degree for which $a_{\mathfrak{p}}(\varphi) \equiv t \pmod{\mathfrak{a}}$. The obstruction to $a_{\mathfrak{p}}(\varphi) = t$ for $\mathfrak{p}$ of large even degree arises from the infinite place!

In the elliptic curve setting, there is an archimedean component of Lang and Trotter's heuristic which is played by the Sato-Tate law of E. It is responsible for the innocuous factor $2/\pi$ occurring in the constant $C_{E,t}$, and in particular it never gives an obstruction to $a_p(E) = t$ (at least not for large enough p). J.-K. Yu has proved that there is an analogue of Sato-Tate for Drinfeld modules [Yu03], and the obstruction of Proposition 2.1 can be deduced from it. The Sato-Tate law has been described in [Zyw11b], and the author hopes to state a general Lang-Trotter conjecture in future work.

It is hard to give convincing numerical evidence for (2.3), at least compared to that supplied in §2.2 and §2.1, since $q^{n/2}/n$ grows much slower than $\pi_A(n) \approx q^n/n$. For example, some computations show that

$$\mathcal{P}_{\varphi,0}(9) = 84,\ \mathcal{P}_{\varphi,0}(11) = 359,\ \mathcal{P}_{\varphi,1}(9) = 62,\ \mathcal{P}_{\varphi,1}(11) = 272,\ \mathcal{P}_{\varphi,T}(9) = 62,\ \mathcal{P}_{\varphi,T}(11) = 259,$$

which is compatible with the conjectural asymptotic (2.3) with $M_{\varphi} = 2$ and $C_{\phi,0}(1) \approx 0.5$, $C_{\phi,1}(1) \approx 0.4$, $C_{\phi,T}(1) \approx 0.4$.

Remark 2.2. C. David and A.C. Cojocaru proved the upper bound $\mathcal{P}_{\phi,t}(n) \ll_{\phi} q^{\frac{4}{5}n}/n^{1/5}$ in [CD08] (in that paper, they were mainly considering the Drinfeld module analogue of another conjecture of Lang and Trotter). A key ingredient for their bound was the rank 2 case of Theorem 1.1. In [Zyw11b], the Sato-Tate law for ϕ is used to prove the upper bound $\mathcal{P}_{\phi,t}(n) \ll_{\phi,t} q^{\frac{3}{4}n}$.

3. The determinant of ρ_{φ}

3.1. **The Carlitz module.** The Carlitz module is the Drinfeld module $C\colon A \to F\{\tau\}$ for which $C_T = T + \tau$.

Proposition 3.1 (Hayes [Hay74])**.** *For every non-zero ideal $\mathfrak{a}$ of A, the representation*

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

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 $\bar{\rho}_{C,\mathfrak{a}}(\mathrm{Frob}_{\mathfrak{p}}) \equiv \mathfrak{p} \mod \mathfrak{a}$.

In particular, the proposition implies that $\rho_C\colon G_F \to \mathrm{GL}_1(\widehat{A}) = \widehat{A}^{\times}$ is surjective; this gives a rank one example of Theorem 1.1.

3.2. 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

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

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 $(\det \circ \bar{\rho}_{\varphi,\mathfrak{a}})(\mathrm{Frob}_{\mathfrak{p}}) \equiv \mathfrak{p} \equiv \bar{\rho}_{C,\mathfrak{a}}(\mathrm{Frob}_{\mathfrak{p}})$ mod $\mathfrak{a}$. Using the Chebotarev density theorem, we find that the characters $\det \circ \bar{\rho}_{\varphi,\mathfrak{a}} \colon G_F \to (A/\mathfrak{a})^{\times}$ and $\bar{\rho}_{C,\mathfrak{a}} \colon G_F \to (A/\mathfrak{a})^{\times}$ are the same.

Proposition 3.2. *The representation* $\det \circ \bar{\rho}_{\varphi,\mathfrak{a}} \colon G_F \to (A/\mathfrak{a})^{\times}$ *equals* $\bar{\rho}_{C,\mathfrak{a}}$, *and hence satisfies the properties of Proposition 3.1.*

Remark 3.3. 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 φ 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.

4. 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^{sep} a separable closure of K. Let $v \colon K^{\times} \twoheadrightarrow \mathbb{Z}$ be the associated discrete valuation (we will also denoted by v the corresponding $\mathbb{Q}$-valued extension of v to K^{sep}). Let I_K be the inertia subgroup of G_K and let K^{un} be the maximal unramified extension of K in K^{sep}. We will return to our specific Drinfeld module φ in §4.5.

4.1. **Stable reduction.** Let $\phi \colon A \to K\{\tau\}$ be a Drinfeld module of rank r. We say that ϕ has stable reduction if there exists a Drinfeld module $\phi' \colon A \to \mathcal{O}\{\tau\}$ such that ϕ' and ϕ are isomorphic over K and the reduction of ϕ' modulo $\mathfrak{m}$ is a Drinfeld module (equivalently, the degree of the reduction of ϕ'_T is greater that 1). We say that ϕ has stable reduction of rank r_1 if it has stable reduction and the rank of ϕ' modulo $\mathfrak{m}$ is r_1. We say that ϕ 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 replacing K by a finite separable extension).

If $\phi \colon A \to K\{\tau\}$ is a Drinfeld module of rank 2, then the j-invariant of ϕ 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 ϕ has potentially good reduction if and only if $v(j_{\phi}) \geq 0$; cf. [Ros03, Lemma 5.2].

4.2. **Image of inertia at places of stable bad reduction.**

Proposition 4.1. *Let* $\phi \colon A \to K\{\tau\}$ *be a Drinfeld module of rank 2 and 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* $\bar{\rho}_{\phi,\mathfrak{a}} \colon G_K \to \mathrm{Aut}(\phi[\mathfrak{a}]) \cong \mathrm{GL}_2(A/\mathfrak{a})$ *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_{ϕ} *be the order of* $\dfrac{v(j_{\phi})}{(q-1)N(\mathfrak{a})} + \mathbb{Z}$ *in* $\mathbb{Q}/\mathbb{Z}$. *Then* $\#\bar{\rho}_{\phi,\mathfrak{a}}(I_K) \geq e_{\phi}$.

The proof of Proposition 4.1 will be given in §4.4.

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

Definition 4.2. A Tate datum over $\mathcal{O}$ is a pair (ψ, Γ), where ψ is a Drinfeld module over $\mathcal{O}$ and Γ is a ψ-lattice. We say that two pairs (ψ, Γ) and (ψ', Γ') of Tate datum are isomorphic if there is an isomorphism from ψ to ψ' such that the corresponding homomorphism $^\psi K^{\mathrm{sep}} \to {}^{\psi'} K^{\mathrm{sep}}$ of A-modules induces an isomorphism between Γ and Γ'.

Proposition 4.3 (Drinfeld [Dri74, §7]). *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 $\phi\colon A \to K\{\tau\}$ of rank $r := r_1 + r_2$ with stable reduction of rank r_1;*

    (b) *the set of K-isomorphism classes of Tate datum (ψ, Γ) where $\psi\colon A \to \mathcal{O}\{\tau\}$ is a Drinfeld module of rank r_1 with good reduction and Γ is a ψ-module of rank r_2.*

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

We start with a Drinfeld module $\psi\colon A \to \mathcal{O}\{\tau\}$ of rank r_1 with good reduction and a ψ-lattice Γ 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 satisfies $e_\Gamma(X) \equiv X \bmod \mathfrak{m}$; the discreteness of Γ is key here. We may then view e_Γ as an element of $\mathcal{O}\{\{\tau\}\}$; the (non-commutative) ring of formal power series in τ with coefficients in $\mathcal{O}$. There exists a unique Drinfeld A-module ϕ 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 ϕ; it has rank $r_1 + r_2$ with stable reduction of rank r_1. That ϕ has stable reduction of rank r_1 is clear since $\phi_T \equiv \phi_T e_\Gamma = e_\Gamma \psi_T \equiv \psi_T \bmod \mathfrak{m}$ and ψ has good reduction.

In the other direction, start with a Drinfeld A-module ϕ of rank $r := r_1 + r_2$ over K which has stable reduction of rank r_1. After possibly replacing ϕ with a K-isomorphic Drinfeld module, we may assume that ϕ takes values in $\mathcal{O}\{\tau\}$. There exists a unique Drinfeld module $\psi\colon A \to \mathcal{O}\{\tau\}$ of 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 $|a_i| \to 0$, such that

$$(4.1) \qquad\qquad\qquad\qquad u\psi_a = \phi_a u$$

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

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

$$(4.2) \qquad\qquad 1 \to \psi[a] = \psi_a^{-1}(0) \to \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\psi_a} \Gamma/a\Gamma \to 1.$$

We also have an isomorphism

$$(4.3) \qquad\qquad \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\sim} \phi[a], \quad z + \Gamma \mapsto u(z)$$

of $A[G_K]$-modules (it is a well-defined map by (4.1)).

10

4.4. **Proof of Proposition 4.1.** Fix a Drinfeld module $\phi\colon A \to \mathcal{O}\{\tau\}$ of rank 2 that has stable reduction of rank 1. Let (ψ, Γ) be the corresponding Tate uniformization as in §4.3. We have $\mathfrak{a} = (a)$ for some $a \in A$. Using the isomorphism (4.3), 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 $\psi\colon A \to \mathcal{O}\{\tau\}$ has rank 1 and good reduction, so the Galois representation $\bar{\rho}_{\psi, \mathfrak{a}}\colon G_K \to \operatorname{Aut}(\psi[\mathfrak{a}]) = (A/\mathfrak{a})^\times$ 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 Γ is a free A-module of rank 1. Fix a generator γ of Γ, it is well-defined up to multiplication by an element of $\mathbb{F}_q^\times$. Since the lattice Γ is stable under the Galois action, there is a character $\chi_\Gamma\colon G_K \to \mathbb{F}_q^\times$ 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 (4.2) 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 ψ_a has coefficients in $\mathcal{O}$. However the discreteness of the lattice Γ 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^{un} in K^{sep} for which $\operatorname{Gal}(K^{\text{sep}}/K')$ acts trivially on $\psi_a^{-1}(\Gamma)/\Gamma$. The field K' is of course equal to $K^{\text{un}}(\phi[\mathfrak{a}])$, and $\bar{\rho}_{\phi, \mathfrak{a}}(I_K) \cong \operatorname{Gal}(K'/K^{\text{un}})$. 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.

4.5. **Our example.** We will now apply the above theory to our specific Drinfeld module $\varphi\colon A \to F\{\tau\}$ with $\varphi_T = T + \tau - T^{q-1}\tau^2$. Let p be the prime dividing q.

Proposition 4.4. *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 $\operatorname{Aut}(\phi[\mathfrak{a}]) \cong \operatorname{GL}_2(A/\mathfrak{a})$. Equivalently, $\#\bar{\rho}_{\phi, \mathfrak{a}}(I_T) = N(\mathfrak{a})$.*

Proof. The Drinfeld module φ has stable reduction of rank 1 at (T). The field $K := \mathbb{F}_q((T))$ is the completion of F with respect to T. Let v_T be the corresponding valuation normalized so that $v_T(T) = 1$.

We know from Proposition 3.2 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 4.1(i) shows that $\bar{\rho}_{\varphi, \mathfrak{a}}(I_K)$ is contained in a subgroup of $\operatorname{GL}_2(A/\mathfrak{a})$ of order $N(\mathfrak{a})$. By Proposition 4.1(ii), $v_T(j_\phi) = -(q-1)$ implies that $\#\bar{\rho}_{\varphi, \mathfrak{a}}(I_T) \geq N(\mathfrak{a})$. $\square$

5. Irreducibility

Proposition 5.1. *The $\mathbb{F}_\lambda[G_F]$-module $\varphi[\lambda]$ is irreducible for every finite place λ of F.*

We now suppose that $\varphi[\lambda]$ is a reducible $\mathbb{F}_\lambda[G_F]$-module for a fixed λ. We shall eventually obtain a contradiction and thus prove Proposition 5.1. 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 $\bar{\rho}_{\varphi,\lambda}\colon G_F \to \operatorname{Aut}(\varphi[\lambda]) \cong \operatorname{GL}_2(\mathbb{F}_\lambda)$ lies in the group of upper triangular matrices. Moreover, there are two characters χ and $\chi'\colon G_F \to \mathbb{F}_\lambda^\times$ 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 5.2. *The characters χ and χ' 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 4.4, the order of every element of $\bar{\rho}_{\varphi,\lambda}(I_\mathfrak{p})$ divides some power of q (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 q.

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

Finally consider the case where $\mathfrak{p} = \lambda$ and $\mathfrak{p} \neq (T)$. The reduction of φ 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 $\chi'(I_p) = 1$. $\qquad\square$

Lemma 5.3. *One of the characters $\chi, \chi'\colon G_F \to \mathbb{F}_\lambda^\times$ is of the form $G_F \twoheadrightarrow \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \mathbb{F}_\lambda^\times$, where the first map is restriction.*

Proof. By Lemma 5.2, one of the characters χ or $\chi'\colon G_F \to \mathbb{F}_\lambda^\times$, without loss of generality χ', is unramifed at all finite places of F. Thus we may view χ' as a $\mathbb{F}_\lambda^\times$-valued character of the étale fundamental group of $\mathbb{A}^1_{\mathbb{F}_q}$. Since $\mathbb{A}^1_{\mathbb{F}_q}$ has no non-trivial étale covers of order prime to q, we deduce that $\chi'\colon G_F \to \mathbb{F}_\lambda^\times$ is trivial on $\operatorname{Gal}(F^{\mathrm{sep}}/\overline{\mathbb{F}}_q(T))$. The lemma is now immediate. $\qquad\square$

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

Lemma 5.4. *Let λ 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 λ, we have*

$$(5.1) \qquad\qquad a_\mathfrak{p}(\varphi) \equiv \zeta^{-\deg \mathfrak{p}}\mathfrak{p} + \zeta^{\deg \mathfrak{p}} \mod \lambda.$$

Proof. By Lemma 5.3, one of the characters $\chi, \chi'\colon G_F \to \mathbb{F}_\lambda^\times$, say χ', factors through a character $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \mathbb{F}_\lambda^\times$. Hence there is a $\zeta \in \mathbb{F}_\lambda^\times$ such that $\chi'(\operatorname{Frob}_\mathfrak{p}) = \zeta^{\deg \mathfrak{p}}$ for any monic irreducible polynomial $\mathfrak{p}$ that is not T or λ. By Proposition 3.2, we know that $\chi(\operatorname{Frob}_\mathfrak{p})\chi'(\operatorname{Frob}_\mathfrak{p}) = \det(\bar{\rho}_{\varphi,\lambda}(\operatorname{Frob}_\mathfrak{p})) \equiv \mathfrak{p} \bmod \lambda$, hence

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

We deduce that

$$a_\mathfrak{p}(\varphi) \equiv \operatorname{tr}\left(\bar{\rho}_{\varphi,\lambda}(\operatorname{Frob}_\mathfrak{p})\right) = \chi(\operatorname{Frob}_\mathfrak{p}) + \chi'(\operatorname{Frob}_\mathfrak{p}) \equiv \zeta^{-\deg \mathfrak{p}}\mathfrak{p} + \zeta^{\deg \mathfrak{p}} \mod \lambda. \qquad\square$$

By checking (5.1) for various primes $\mathfrak{p}$, we will be able to rule out many λ; it turns out that we will only need to consider $\mathfrak{p}$ of degree 1.

Lemma 5.5. *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 $a_\mathfrak{p}(\varphi) = -(-1/c^{q-1}) = 1$. $\qquad\square$

Since $q \geq 5$, there exist $c_1, c_2 \in \mathbb{F}_q^\times$ such that λ, $T - c_1$ and $T - c_2$ are distinct. By Lemma 5.4 and 5.5 with $\mathfrak{p} = T - c_i$, we get

$$1 \equiv \zeta^{-1}(T - c_i) + \zeta \mod \lambda$$

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

6. Proof of Theorem 1.2

In different respects, Propositions 3.2, 4.4 and 5.1 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^{ab} be the maximal abelian extension of F in F^{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 λ-adic representations of φ are surjective.

Lemma 6.1. *For every finite place λ 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 5.1 and 4.4, 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 $N(\lambda)$. Lemma A.1 then implies 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 3.2.

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 3.2. 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 λ by Proposition 4.4. 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 $\mathrm{SL}_2(A_\lambda)$. $\qquad\square$

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

Lemma 6.2. *Let λ_1 and λ_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 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 3.2. By Lemma 6.1 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 λ_1 or λ_2. By Lemma 5.5, we have

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

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. $\qquad\square$

Lemma 6.3. *Let λ_1 and λ_2 be distinct finite places of F. Define*

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

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 ρ is surjective will follow from this and Proposition 3.2.

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 $H \to \mathrm{SL}_2(A/\lambda_2^{n_2})$ and $H \to \mathrm{SL}_2(A/\lambda_1^{n_1})$, respectively. Each of these projections are surjective by Lemma 6.1. 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 $\mathrm{SL}_2(A/\lambda_i^{n_1})/N_i$ are non-trivial. So by Lemma A.3, N_i is a subgroup of the group of $B \in \mathrm{SL}_2(A/\lambda_i^{n_1})$ with $B \equiv \pm I \bmod \lambda$. 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 6.2 which says that $\bar{\rho}_{\varphi,\lambda_1\lambda_2}(G_{F^{\mathrm{ab}}}) = \mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_1})$. 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. We first show that $\rho_{\varphi}(G_F) = \mathrm{GL}_2(\widehat{A})$. Again by Proposition 3.2 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

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

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 λ_1 and λ_2 are distinct maximal ideals of A, and n_1 and n_2 are positive integers. This is immediate from Lemma 6.3.

Finally, we show that $\rho_{\varphi}\big(G_{\overline{\mathbb{F}}_q(T)}\big) = \mathrm{GL}_2(\widehat{A})$. Since $\overline{\mathbb{F}}_q(T)/\mathbb{F}_q(T)$ is an abelian extension and the commutator subgroup of $\mathrm{GL}_2(\widehat{A})$ is $\mathrm{SL}_2(\widehat{A})$, it suffices to show that $(\det \circ \rho_{\varphi})(G_{\overline{\mathbb{F}}_q(T)}) = \widehat{A}^{\times}$. Again this is easily verified using the description of of $\det \circ \rho_{\varphi}$ in §3.1.

Acknowledgements. The calculations in §2 were performed using Magma [BCP97].

Appendix A. Group theory

In this appendix we collect all the group theory needed in §6 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 $q \geq 5$ an odd prime power.

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 with 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 $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathbb{F})$. 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 $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix} \right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix} \right) \in H$. $\square$

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

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

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

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

Proof. We first prove that $\mathrm{SL}_2(A_\lambda)$ is its own commutator subgroup. Let H be the commutator subgroup of $\mathrm{SL}_2(A_\lambda)$. It is a closed normal subgroup of $\mathrm{SL}_2(A_\lambda)$ and $\mathrm{GL}_2(A_\lambda)$. Define $S^0 := \mathrm{SL}_2(A_\lambda)$, and for each $i \geq 1$ we let S^i be the group of $s \in \mathrm{SL}_2(A_\lambda)$ 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 $H^{[i]} \hookrightarrow S^{[i]}$, and it suffices to show that $H^{[i]} = S^{[i]}$ for all $i \geq 0$.

Reduction modulo λ induces an isomorphism $S^{[0]} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_\lambda)$ with the image of $H^{[0]}$ being the commutator subgroup of $\mathrm{SL}_2(\mathbb{F}_\lambda)$. Since $\mathrm{SL}_2(\mathbb{F}_\lambda)/\{\pm I\}$ is simple, we find that $[\mathrm{SL}_2(\mathbb{F}_\lambda) : H^{[0]}] = 1$ or 2. Since $\mathrm{SL}_2(\mathbb{F}_\lambda)$ 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) $$S^{[i]} \xrightarrow{\sim} \mathfrak{sl}_2(\mathbb{F}_\lambda), \quad [1 + \lambda^i y] \mapsto [y];$$

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

15

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

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

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 $B \equiv \pm I \bmod \lambda$, 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, $N' \subseteq N$. $\qquad\square$

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 $p_1 \colon H \to B_1$ and $p_2 \colon H \to B_2$ 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 $S_1, S_2, \cdots, S_k$ be finite groups with no non-trivial abelian quotients. Let H be a subgroup of $S_1 \times \cdots \times S_k$ such that each projection $H \to S_i \times S_j$ $(1 \leq i < j \leq k)$ is surjective. Then $H = S_1 \times \cdots \times S_k$.*

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

Lemma A.7. *Let λ_1 and λ_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 $p_1' \colon H' \to \mathrm{SL}_2(\mathbb{F}_{\lambda_1})$ and $p_2' \colon H' \to \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$ 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

$$\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/N_1' \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/N_2'. \tag{A.2}$$

If $N_1' = \mathrm{SL}_2(\mathbb{F}_{\lambda_1})$ (equivalently, $N_2' = \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$), then one has $H' = \mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2}) = \mathrm{SL}_2(A/\mathfrak{a})$. Using condition (a), we deduce that $H = \mathrm{GL}_2(A/\mathfrak{a})$.

We 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 $p_i \colon H \to \mathrm{GL}_2(\mathbb{F}_{\lambda_i})$. 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

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

16

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

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

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

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

Let $\sigma \colon \mathbb{F}_{\lambda_1} \xrightarrow{\sim} \mathbb{F}_{\lambda_2}$ be a field isomorphism and $\chi \colon \mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \to \mathbb{F}_{\lambda_2}^{\times}$ 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) $$A \mapsto \chi(A)A^{\sigma}, \qquad A \mapsto \chi(A)((A^T)^{-1})^{\sigma};$$

where B^{σ} represents the matrix obtained by applying σ to each entry of 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 σ and χ such that $\widetilde{\alpha}$ 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

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

Note that the map $\mathrm{GL}_2(\mathbb{F}_{\lambda_i}) \to \mathbb{F}_{\lambda_i}$, $A \mapsto \mathrm{tr}(A)^2/\det(A)$ factors through the projection $\mathrm{GL}_2(\mathbb{F}_{\lambda_i}) \to \mathrm{PGL}_2(\mathbb{F}_{\lambda_i})$. 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 $\mathcal{S} \subseteq W$. However, $W \neq A/\mathfrak{a}$, and this contradicts assumption (c). $\qquad\square$

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑6

[Bro92] M. L. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), no. 2, 419–439. ↑2.3

[CD08] Alina Carmen Cojocaru and Chantal David, *Frobenius fields for Drinfeld modules of rank 2*, Compos. Math. **144** (2008), no. 4, 827–848. ↑2.2

[CM04] Alina Carmen Cojocaru and M. Ram Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. **330** (2004), no. 3, 601–625. ↑2.1

[Dav96] Chantal David, *Average distribution of supersingular Drinfel′d modules*, J. Number Theory **56** (1996), no. 2, 366–380. ↑2.3

[DH87] Pierre Deligne and Dale Husemoller, *Survey of Drinfel′d modules*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), 1987, pp. 25–91. ↑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. ↑A, A

[Dri74] V. G. Drinfel′d, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656. ↑1.1, 4.3

[Gek08] Ernst-Ulrich Gekeler, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721. ↑2.3, 3.2, 5

[Gos96] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 35, Springer-Verlag, Berlin, 1996. ↑1.1

[Gre10] Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507. ↑1.4

[GM90] Rajiv Gupta and M. Ram Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), no. 1, 225–235. ↑2.1

[Hay74] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91. ↑3.1

[HY00]   Liang-Chung Hsia and Jing Yu, *On characteristic polynomials of geometric Frobenius associated to Drinfeld modules*, Compositio Math. **122** (2000), no. 3, 261–280. ↑2.3

[Jai08]   Lalit Kumar Jain, *Koblitz's conjecture for the Drinfeld module*, Master's Thesis, University of Waterloo, 2008. ↑2.2

[KL09]   Wentang Kuo and Yu-Ru Liu, *Cyclicity of finite Drinfeld modules*, J. Lond. Math. Soc. (2) **80** (2009), no. 3, 567–584. ↑2.1

[LT76]   Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2-*extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in $\mathrm{G}L_2$-extensions of the rational numbers. ↑2.3

[Leh09]   Thomas Lehmkuhl, *Compactification of the Drinfeld modular surfaces*, Mem. Amer. Math. Soc. **197** (2009), no. 921, xii+94. ↑4.3

[Mur83]   M. Ram Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), no. 2, 147–168. ↑2.1

[PR09a]   Richard Pink and Egon Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), no. 4, 882–907. ↑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. ↑5

[Poo98]   Bjorn Poonen, *Drinfeld modules with no supersingular primes*, Internat. Math. Res. Notices **3** (1998), 151–159. ↑2.3

[Rib76]   Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. ↑A.4, A.6, A

[Ros03]   Michael Rosen, *Formal Drinfeld modules*, J. Number Theory **103** (2003), no. 2, 234–256. ↑4.1, 4.4

[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. ↑1.4, A

[Ser72]   _____, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1.4, 5

[Ser78]   _____, *Résumé des cours de 1977-1978*, Annuaire du Collège de France (1978), 67–70. ↑2.1

[Yu03]   Jiu-Kang Yu, *A Sato-Tate law for Drinfeld modules*, Compositio Math. **138** (2003), no. 2, 189–197. ↑2.3

[Zyw11a]   David Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769. ↑2.2, 2.2

[Zyw11b]   _____, *The Sato-Tate law for Drinfeld modules* (2011). arXiv:1110.4098. ↑2.3, 2.2

School of Mathematics, Institute for advanced study, Princeton, NJ 08540

E-mail address: `zywina@math.ias.edu`