DRINFELD MODULES WITH MAXIMAL GALOIS ACTION

DAVID ZYWINA

Abstract. With a fixed prime power $q > 1$, define the ring of polynomials $A = \mathbb{F}_q[t]$ and its fraction field $F = \mathbb{F}_q(t)$. For each pair $a = (a_1, a_2) \in A^2$ with a_2 nonzero, let $\phi(a)\colon A \to F\{\tau\}$ be the Drinfeld A-module of rank 2 satisfying $t \mapsto t + a_1\tau + a_2\tau^2$. The Galois action on the torsion of $\phi(a)$ gives rise to a Galois representation $\rho_{\phi(a)}\colon \operatorname{Gal}(F^{\rm sep}/F) \to \operatorname{GL}_2(\widehat{A})$, where $\widehat{A}$ is the profinite completion of A. We show that the image of $\rho_{\phi(a)}$ is large for random a. More precisely, for all $a \in A^2$ away from a set of density 0, we prove that the index $[\operatorname{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\operatorname{Gal}(F^{\rm sep}/F))]$ divides $q-1$ when $q > 2$ and divides 4 when $q = 2$. We also show that the representation $\rho_{\phi(a)}$ is surjective for a positive density set of $a \in A^2$.

1. Introduction

Throughout we fix a finite field $\mathbb{F}_q$ with q elements. Define the polynomial ring $A = \mathbb{F}_q[t]$ and its fraction field $F = \mathbb{F}_q(t)$.

1.1. **Background.** We now recall some notions concerning Drinfeld modules. For an introduction see [Gos96, DH87, Dri74]. Let K be an A-field, i.e., a field K with a fixed ring homomorphism $\iota\colon A \to K$. Using ι, we can view K as a field extension of $\mathbb{F}_q$.

Let $K\{\tau\}$ be the ring of skew polynomials over K, i.e., the ring of polynomials in the indeterminate τ with coefficients in K that satisfy the commutation rule $\tau c = c^q \tau$ for all $c \in K$. We can identify $K\{\tau\}$ with a subring of $\operatorname{End}(\mathbb{G}_{a,K})$ by identifying τ with the Frobenius map $X \mapsto X^q$. Let $\partial_0\colon K\{\tau\} \to K$ be the ring homomorphism $\sum_i a_i\tau^i \mapsto a_0$.

A Drinfeld A-module over K is a ring homomorphism

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

such that $\partial_0 \circ \phi = \iota$ and $\phi(A) \not\subseteq K$. The characteristic of ϕ is the kernel $\mathfrak{p}_0$ of ι; equivalently, the kernel of $\partial_0 \circ \phi\colon A \to K$. If $\mathfrak{p}_0 = (0)$, then we say that ϕ has generic characteristic and we may use ι to view K as a field extension of F. The Drinfeld module ϕ is determined by $\phi_t = \sum_{i=0}^r a_i\tau^i$ where we have $a_i \in K$ with $a_r \neq 0$; the positive integer r is called the rank of ϕ.

Fix a separable closure $K^{\rm sep}$ of K. The Drinfeld module ϕ endows $K^{\rm sep}$ with an A-module structure. More precisely, $a \cdot x := \phi_a(x)$ for $a \in A$ and $x \in K^{\rm sep}$, where we are using our identification of $K\{\tau\}$ with a subring of $\operatorname{End}(\mathbb{G}_{a,K})$. We shall write ${}^\phi K^{\rm sep}$ if we wish to emphasize $K^{\rm sep}$ with this particular A-module structure. For a nonzero ideal $\mathfrak{a}$ of A, the $\mathfrak{a}$-torsion of ϕ is the A-module

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

Suppose that $\mathfrak{a}$ is relatively prime to the characteristic $\mathfrak{p}_0$. Then $\phi[\mathfrak{a}]$ is a free $A/\mathfrak{a}$-module of rank r. The absolute Galois group $\operatorname{Gal}_K := \operatorname{Gal}(K^{\rm sep}/K)$ acts on $\phi[\mathfrak{a}]$ and respects the

2020 *Mathematics Subject Classification.* Primary 11G09; Secondary 11F80, 11R58.

A-module structure. This action can be expressed in terms of a Galois representation

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

For the rest of the section, assume that ϕ has generic characteristic. By choosing bases compatibly and taking the inverse limit, we obtain a single representation

$$\rho_\phi\colon \operatorname{Gal}_K \to \operatorname{GL}_r(\widehat{A})$$

that encodes the Galois action on the torsion submodule of ${}^{\phi}K^{\text{sep}}$, where $\widehat{A}$ is the profinite completion of A. The representation ρ_ϕ is continuous when the groups are endowed with their profinite topologies.

For a nonzero prime ideal λ of A, let $\rho_{\phi,\lambda}\colon \operatorname{Gal}_K \to \operatorname{GL}_r(A_\lambda)$ be the representation obtained by composing ρ_ϕ with the quotient map $\operatorname{GL}_r(\widehat{A}) \to \operatorname{GL}_r(A_\lambda)$, where A_λ is the inverse limit of the rings A/λ^i with $i \geq 1$. The representation $\rho_{\phi,\lambda}$ encodes the Galois action on the λ-power torsion of ϕ. We can identify ρ_ϕ with $\prod_\lambda \rho_{\phi,\lambda}$ by using the natural isomorphism $\operatorname{GL}_r(\widehat{A}) = \prod_\lambda \operatorname{GL}_r(A_\lambda)$, where the product is over the nonzero prime ideals of A.

Pink and Rütsche [PR09a] have described the image of ρ_ϕ up to commensurability when K is finitely generated. For simplicity, we only state the version for which ϕ has no extra endomorphisms. Recall that the ring $\operatorname{End}_{\overline{K}}(\phi)$ of endomorphisms is the centralizer of $\phi(A)$ in $\overline{K}\{\tau\}$, where $\overline{K} \supseteq K^{\text{sep}}$ is an algebraic closure of K.

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 $\operatorname{End}_{\overline{K}}(\phi) = \phi(A)$. Then $\rho_\phi(\operatorname{Gal}_K)$ is an open subgroup of $\operatorname{GL}_r(\widehat{A})$. Equivalently, $\rho_\phi(\operatorname{Gal}_K)$ has finite index in $\operatorname{GL}_r(\widehat{A})$.*

Theorem 1.1, especially with $r \geq 2$, is a Drinfeld module analogue of Serre's open image theorem for non-CM elliptic curves, cf. [Ser72].

In this article, we are interested in producing Galois representations ρ_ϕ with largest possible image. We shall focus our attention on the most immediate case which is $r = 2$ and $K = F$. We shall show that there are infinitely many nonisomorphic Drinfeld modules ϕ over F of rank 2 with $\rho_\phi(\operatorname{Gal}_F) = \operatorname{GL}_2(\widehat{A})$.

1.2. **Density.** For a fixed integer $n \geq 1$, we will want to talk about properties holding for "most" $a \in A^n$. To make this precise, we introduce the notion of density. For any subset $S \subseteq A^n$ and positive integer d, we let $S(d)$ be the set of $(a_1, \ldots, a_n) \in S$ with $\deg(a_i) \leq d$ for all $1 \leq i \leq n$. Define

$$\overline{\delta}(S) := \limsup_{d\to+\infty} \frac{|S(d)|}{|A^n(d)|} \quad \text{and} \quad \underline{\delta}(S) := \liminf_{d\to+\infty} \frac{|S(d)|}{|A^n(d)|};$$

these are the upper density and lower density of S, respectively. Note that $|A^n(d)| = q^{n(d+1)}$. When $\overline{\delta}(S) = \underline{\delta}(S)$, we call the common value the density of S and denote it by $\delta(S)$. Of course, $\delta(A^n) = 1$.

1.3. **Main result.** We shall always view F as an A-field via the inclusion $A \subseteq F$. For each pair $a = (a_1, a_2) \in A^2$ with $a_2 \neq 0$, let

$$\phi(a)\colon A \to F\{\tau\}, \quad \alpha \mapsto \phi(a)_\alpha$$

be the Drinfeld A-module over F for which $\phi(a)_t = t + a_1\tau + a_2\tau^2$. The Drinfeld module ϕ has rank 2 and generic characteristic. Associated to ϕ, we have a Galois representation $\rho_{\phi(a)}\colon \mathrm{Gal}_F \to \mathrm{GL}_2(\widehat{A})$ that is uniquely determined up to isomorphism.

We now define the following sets which consist of pairs $a \in A^2$ for which $\rho_{\phi(a)}$ has especially large image:

- Let S_1 be the set of $a \in A^2$ with $a_2 \neq 0$ for which $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.
- When $q \neq 2$, let S_2 be the set of $a \in A^2$ with $a_2 \neq 0$ for which $\rho_{\phi(a)}(\mathrm{Gal}_F) \supseteq \mathrm{SL}_2(\widehat{A})$ and $[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)]$ divides $q-1$.
- When $q = 2$, let S_2 be the set of $a \in A^2$ with $a_2 \neq 0$ for which $\rho_{\phi(a)}(\mathrm{Gal}_F)$ contains the commutator subgroup of $\mathrm{GL}_2(\widehat{A})$ and $[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)]$ divides 4.
- Let S_3 be the set of $a \in A^2$ with $a_2 \neq 0$ for which $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$ for all nonzero prime ideals λ of A.

Our main theorem shows that the sets S_1, S_2 and S_3 are large.

Theorem 1.2.

(i) *There is a subset of S_1 with positive density.*
(ii) *The set S_2 has density* 1.
(iii) *The set S_3 has density* 1.

Loosely, Theorem 1.2(ii) says that for a "randomly chosen" $a \in A^2$ the index of $\rho_{\phi(a)}(\mathrm{Gal}_F)$ in $\mathrm{GL}_2(\widehat{A})$ is finite and divides $q-1$ or 4 when $q \neq 2$ or $q = 2$, respectively. Theorem 1.2(i) shows that $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$ holds for many $a \in A^2$.

Remark 1.3.

(i) Assume $q \neq 2$. Take any $(a_1, a_2) \in A^2$ with a_2 monic and $\deg(a_2) \equiv 1 \pmod{q-1}$. We have $[\widehat{A}^\times : \det(\rho_{\phi(a)}(\mathrm{Gal}_F))] = q-1$ and hence $[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)] \geq q-1$, cf. Theorem 6.1. This shows that the set S_1 does not have density 1 and that the integer $q-1$ occurring in the definition of S_2 is optimal for Theorem 1.2(ii) to hold.
(ii) The commutator subgroup of $\mathrm{GL}_2(\widehat{A})$ is $\mathrm{SL}_2(\widehat{A})$ when $q \neq 2$. A group theoretic complication that arises when $q = 2$ is that the commutator subgroup of $\mathrm{GL}_2(\widehat{A})$ is a proper subgroup of $\mathrm{SL}_2(\widehat{A})$; in fact, it is a subgroup of index 4. This is the underlying reason why definition of S_2 is different when $q = 2$.
(iii) Theorem 1.2(i) gives counterexamples to [Che22a, Theorem 4.4] which would imply that $S_1 = \emptyset$ when $q = 2$. There seem to be issues when working with wildly ramified quadratic extensions of F in their proof. Also, Theorem 1.2(i) gives counterexamples to [Che22a, Theorem 5.4] which would imply that S_1 has density 0 when $q = 3$.

1.4. **Explicit examples.** For each prime power $q > 1$, we also give an example of a rank 2 Drinfeld module whose Galois representation is surjective.

Theorem 1.4. *Let $\phi\colon A \to F\{\tau\}$ be the Drinfeld module for which*

$$\phi_t = \begin{cases} t + \tau - t^{q-1}\tau^2 & \text{if } q \neq 2, \\ t + t^3\tau + (t^2+t+1)\tau^2 & \text{if } q = 2. \end{cases}$$

Then $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

1.5. **Overview.** We give a brief overview of the paper. Consider a Drinfeld module $\phi\colon A \to F\{\tau\}$ of rank 2 with $\operatorname{End}_{\overline{F}}(\phi) = \phi(A)$.

In §2, we give a criterion that will allow us to show that a subgroup of $\mathrm{GL}_2(A_\lambda)$ is equal to the full group. In §3, we give a criterion that will allow us to show that a subgroup of $\mathrm{GL}_2(\widehat{A})$ contains the commutator subgroup of $\mathrm{GL}_2(\widehat{A})$. We will try to apply these results to the subgroup $\rho_\phi(\mathrm{Gal}_F)$ of $\mathrm{GL}_2(\widehat{A})$. It is these group theoretic results that motivate the structure of the paper.

Galois representations for Drinfeld modules defined over local fields will be studied in §4. This will be used in our proofs to understand the action of inertia subgroups on the torsion of ϕ at primes for which our Drinfeld modules have semistable reduction. In particular, this will give a way to construct subgroups of $\bar{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)$ that we have some control over.

In §5, we recall that the representations $\bar{\rho}_{\phi,\mathfrak{a}}$ are compatible and give rise to Frobenius polynomials. These polynomials have coefficients in A and are computable. In §6, we recall a theorem of Gekeler that will give an explicit expression for the index of $\det(\rho_\phi(\mathrm{Gal}_F))$ in $\widehat{A}^\times$.

An important step in showing that ρ_ϕ has large image is to prove that the representations $\bar{\rho}_{\phi,\lambda}\colon \mathrm{Gal}_F \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ are irreducible for all nonzero prime ideals λ. In §7, we prove that this holds for all but finitely many λ and give an explicit bound on the norms of any possible exceptions.

In §8, we prove a version of Hilbert's irreducibility theorem. We use it to show that for a fixed nonzero ideal $\mathfrak{a}$ of A, we have $\rho_{\phi(a),\mathfrak{a}}(\mathrm{Gal}_F) = \mathrm{GL}_2(A/\mathfrak{a})$ for all $a \in A^2$ away from a set of density 0 (for future reference, we will give a version that holds for arbitrary rank $r \geq 2$). The set of density 0 will depend on $\mathfrak{a}$, so Hilbert's irreducibility theorem cannot be used by itself to prove our main theorems.

In §9, we use all the above ingredients and some careful sieving to get information on the image of $\rho_{\phi(a)}$ for all $a \in A^2$ away from a set of density 0. In particular, for all $a \in A^2$ away from a set of density 0, we show that $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$ for all nonzero prime ideals λ of A, and also show that $\rho_{\phi(a)}(\mathrm{Gal}_F)$ and $\mathrm{GL}_2(\widehat{A})$ have the same commutator subgroup. The proof of Theorem 1.2 in the case $q \neq 2$ will then be quickly proved in §9.2.

Suppose that $q = 2$. In §10, we give a condition on ϕ that ensures that the homomorphism $\mathrm{Gal}_F \to \mathrm{GL}_2(\widehat{A})/[\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$ obtained by composing ρ_ϕ with the quotient map is surjective. This is achieved by considering the ramification at the place ∞ of F. In §10.4, we prove the remaining case of Theorem 1.2.

Finally, §11 is dedicated to the computation of the Galois images of the explicit Drinfeld modules from Theorem 1.4.

1.6. **Some earlier results.** In the unpublished preprint [Zyw11] the author proved Theorem 1.4 when $q \geq 5$ is odd. This was extended to $q = 3$ and $q = 2^e \geq 4$ in [Che22a]. The original goal of this work was to reprove this in a manner that could readily generalize to most Drinfeld modules like as in Theorem 1.2. When $q = p^e$ with $p \geq 5$ and $p \equiv 1 \pmod 3$, Chen gave an example of a rank 3 Drinfeld A-module $\phi\colon A \to F\{\tau\}$ for which $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_3(\widehat{A})$, cf. [Che22b]. There are also some recent papers proving Hilbert irreducibility like results, cf. [Ray24a, Ray24b, Che24].

1.6.1. *Elliptic curves.* Let us briefly mention the analogous case of elliptic curves over a fixed number field K. Consider an elliptic curve E over K. For each integer $n \geq 1$, the Galois action on the n-torsion points of E gives rise to a continuous representation $\bar{\rho}_{E,n}\colon \mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. By choosing compatible bases, these combine to give a single Galois representation $\rho_E\colon \mathrm{Gal}_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Serre observed that for an elliptic curve over $\mathbb{Q}$, we can never have $\rho_E(\mathrm{Gal}_\mathbb{Q}) \supseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$, cf. [Ser72, Prop. 22]. One ingredient of this obstruction is that $\det\circ\rho_E\colon \mathrm{Gal}_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character and hence the fixed field in $\overline{\mathbb{Q}}$ of its kernel is the maximal abelian extension of $\mathbb{Q}$ by the Kronecker–Weber theorem. When $K \neq \mathbb{Q}$ there is no such obstruction and we have $\rho_E(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ for a "random" elliptic curve E over K, cf. [Zyw11]. Jones [Jon10] prove that we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_\mathbb{Q})] = 2$ for a "random" elliptic curve $E/\mathbb{Q}$.

1.7. **Notation.** For a nonzero ideal $\mathfrak{a}$ of A, we let $A_\mathfrak{a}$ be the inverse limit of the rings $A/\mathfrak{a}^i$ with $i \geq 1$. We have natural isomorphisms

$$A_\mathfrak{a} = \prod_{\mathfrak{p}\supseteq\mathfrak{a}} A_\mathfrak{p} \quad \text{and} \quad \widehat{A} = \prod_{\mathfrak{p}} A_\mathfrak{p},$$

where the product is over the nonzero prime ideals $\mathfrak{p}$ of A. Each ring $A_\mathfrak{p}$ is a complete discrete valuation ring.

Consider a nonzero prime ideal $\mathfrak{p}$ of A. Define the residue field $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$ and denote its cardinality by $N(\mathfrak{p})$. We let $\deg(\mathfrak{p})$ be the degree of the field extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_q$. We have $N(\mathfrak{p}) = q^{\deg(\mathfrak{p})}$ and $\deg(\mathfrak{p})$ is also the degree of any polynomial $\pi \in A$ with $\mathfrak{p} = (\pi)$. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$; it is a local field with valuation ring $A_\mathfrak{p}$. Let $v_\mathfrak{p}\colon F_\mathfrak{p}^\times \to \mathbb{Z}$ be the corresponding valuation normalized so that $v_\mathfrak{p}(F_\mathfrak{p}^\times) = \mathbb{Z}$ and we set $v_\mathfrak{p}(0) = +\infty$.

For a field K, let K^{sep} be a separable closure of K and define the absolute Galois group $\mathrm{Gal}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$.

Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld module of rank 2. The j-invariant of ϕ is $j_\phi := a_1^{q+1}/a_2 \in K$, where $\phi_t = t + a_1\tau + a_2\tau^2$.

2. Group theoretic criterion for large λ-adic image

Throughout this section, we fix a finite field $\mathbb{F}$ and define the ring of formal power series $R := \mathbb{F}[\![\pi]\!]$. The ring R is a complete discrete valuation ring with maximal ideal $\mathfrak{p}$ generated by π and has residue field $\mathbb{F}$.

The following proposition gives a criterion to check if a subgroup of $\mathrm{GL}_2(R)$ is actually the full group. Note that for a nonzero prime ideal λ of $A = \mathbb{F}_q[t]$, the ring A_λ is of the form $\mathbb{F}_\lambda[\![\pi]\!]$, cf. [Ser77, Chapter II §4 Theorem 2]. In particular, Proposition 2.1 gives a group theoretic criterion to check if $\rho_{\phi,\lambda}(\mathrm{Gal}_F)$ is equal to the full group $\mathrm{GL}_2(A_\lambda)$ for a Drinfeld A-module $\phi\colon A \to F\{\tau\}$.

Proposition 2.1. *Let G be a closed subgroup of $\mathrm{GL}_2(R)$ that satisfies the following conditions:*

(a) $\det(G) = R^\times$,
(b) *the image of G modulo $\mathfrak{p}$ is $\mathrm{GL}_2(\mathbb{F})$,*
(c) *if $|\mathbb{F}| > 2$, then there is an element $I + \pi B$ of G with $B \in M_2(R)$ so that B modulo $\mathfrak{p}$ is a nonscalar matrix in $M_2(\mathbb{F})$,*
(d) *if $|\mathbb{F}| = 2$, then the image of G modulo $\mathfrak{p}^2$ is $\mathrm{GL}_2(R/\mathfrak{p}^2)$,*
(e) *if $|\mathbb{F}| = 2$, then $G \cap \mathrm{SL}_2(R)$ contains an element whose reduction modulo $\mathfrak{p}$ in $\mathrm{SL}_2(\mathbb{F})$ has order 2.*

Then $G = \mathrm{GL}_2(R)$.

We will prove the proposition in §2.3. When $|\mathbb{F}| > 3$, Proposition 2.1 also follows from [PR09a, Proposition 4.1].

2.1. **Groups over a finite field.**

Proposition 2.2. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F})$ that acts irreducibly on $\mathbb{F}^2$ and contains a subgroup of cardinality $|\mathbb{F}|$. Then $G \supseteq \mathrm{SL}_2(\mathbb{F})$.*

Proof. Let P_1 be a subgroup of G of order $|\mathbb{F}|$; it is a p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F})$, where p is the characteristic of $\mathbb{F}$. There is a unique 1-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 G, then W_1 would be stable under the action of G which would contradict our irreducibility assumption. Therefore, there is a second subgroup $P_2 \neq P_1$ of G with cardinality $|\mathbb{F}|$. Let W_2 be the unique 1-dimensional $\mathbb{F}$-subspace of $\mathbb{F}^2$ that is fixed by every element of P_2. We have $W_1 \neq W_2$. After conjugating G in $\mathrm{GL}_2(\mathbb{F})$, we may assume that $(1,0) \in W_1$ and $(0,1) \in W_2$, and hence

$$P_1 = \{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) : x \in \mathbb{F}\} \quad \text{and} \quad P_2 = \{\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) : x \in \mathbb{F}\}.$$

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

$$\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1+bc & b \\ a+c+abc & 1+ab \end{smallmatrix}\right).$$

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 $M \in G$. An analogous argument shows that $M \in G$ when $C \neq 0$. Finally in the case $B = C = 0$, we simply note that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right) \in G$. □

Lemma 2.3.

(i) *If $|\mathbb{F}| > 3$, then the group $\mathrm{SL}_2(\mathbb{F})/\{\pm I\}$ is nonabelian and simple.*
(ii) *If $|\mathbb{F}| > 3$, then $[\mathrm{SL}_2(\mathbb{F}), \mathrm{SL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F})$, i.e., $\mathrm{SL}_2(\mathbb{F})$ is perfect.*
(iii) *If $|\mathbb{F}| > 2$, then $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F})$.*

Proof. Parts (i) and (ii) are shown in [Wil09, §3.3.2]. Part (iii) follows from (ii) when $|\mathbb{F}| > 3$ and can be checked directly when $|\mathbb{F}| = 3$. □

We define $\mathfrak{gl}_2(\mathbb{F}) := M_2(\mathbb{F})$ and we let $\mathfrak{sl}_2(\mathbb{F})$ be the subgroup consisting of matrices with trace 0. These $\mathbb{F}$-vector spaces are Lie algebras under the pairing $[x, y] = xy - yx$.

Lemma 2.4. *If $|\mathbb{F}| > 2$, then any subgroup of $\mathfrak{gl}_2(\mathbb{F})$ that is invariant under conjugation by $\mathrm{GL}_2(\mathbb{F})$ either contains $\mathfrak{sl}_2(\mathbb{F})$ or consists only of scalar matrices.*

Proof. This is Proposition 2.1 of [PR09a] when $|\mathbb{F}| \geq 4$. A direct computation shows that this also holds when $|\mathbb{F}| = 3$. □

2.2. **Filtration of a closed subgroup.**

Consider a closed subgroup G of $\mathrm{GL}_2(R)$. For each $i \geq 0$, define the open subgroup

$$G^i := \{g \in G : g \equiv I \pmod{\mathfrak{p}^i}\}$$

of G. For each $i \geq 0$, we have a quotient group $G^{[i]} := G^i/G^{i+1}$. Reduction modulo $\mathfrak{p}$ induces an injective homomorphism $\nu_0 \colon G^{[0]} \hookrightarrow \mathrm{GL}_2(\mathbb{F})$ whose image we will denote by $\overline{G}$. For $i \geq 1$, we have an injective homomorphism $\nu_i\colon G^{[i]} \hookrightarrow M_2(\mathbb{F}) = \mathfrak{gl}_2(\mathbb{F})$ that takes the coset $[1+\pi^i B]$ to B modulo $\mathfrak{p}$; we denote its image by $\mathfrak{g}_i$.

Take any $i \geq 1$. For $g = I + \pi^i B \in G^i$, we have $\det(g) \equiv 1 + \pi^i \operatorname{tr}(B) \pmod{\mathfrak{p}^{i+1}}$. So for $g \in G^i$, we have $\det(g) \equiv 1 \pmod{\mathfrak{p}^{i+1}}$ if and only if $\nu_i([g])$ lies in $\mathfrak{sl}_2(\mathbb{F})$.

Let H be the commutator subgroup of G. With notation as above, we define $\overline{H} \subseteq \mathrm{GL}_2(\mathbb{F})$ and $\mathfrak{h}_i$ for $i \geq 1$. Using that $H \subseteq \mathrm{SL}_2(R)$, we find that $\overline{H} \subseteq \mathrm{SL}_2(\mathbb{F})$ and that $\mathfrak{h}_i \subseteq \mathfrak{sl}_2(\mathbb{F})$ for all $i \geq 1$.

The vector spaces $\mathfrak{g}_i$ and $\mathfrak{h}_i$ are invariant under conjugation by $\overline{G}$; this follows by considering the conjugation action of G on G^i and H^i. The commutator map $(g,h) \mapsto ghg^{-1}h^{-1}$ induces a function $G^{[0]} \times G^{[i]} \to H^{[i]}$ that corresponds to the function

$$\overline{G} \times \mathfrak{g}_i \to \mathfrak{h}_i, \quad (g,x) \mapsto gxg^{-1} - x \tag{2.1}$$

via ν_0 and ν_i. The commutator map also induces a function $G^{[1]} \times G^{[i]} \to H^{[i+1]}$ that corresponds to the function

$$\mathfrak{g}_1 \times \mathfrak{g}_i \to \mathfrak{h}_{i+1}, \quad (x,y) \mapsto [x,y] = xy - yx \tag{2.2}$$

via ν_0, ν_i and ν_{i+1}.

Lemma 2.5. *With notation as above, assume that $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F})$ and $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F})$. Then H is the subgroup of $\mathrm{SL}_2(R)$ consists of those matrices whose image modulo λ lies in $[\overline{G},\overline{G}] \subseteq \mathrm{SL}_2(\mathbb{F})$.*

Proof. We will prove that $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ for all $i \geq 1$ by induction on i. The base case $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F})$ is true by assumption so suppose that $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ for some fixed $i \geq 1$. From the map (2.2), we find that $\mathfrak{h}_{i+1} \subseteq \mathfrak{sl}_2(\mathbb{F})$ contains the $\mathbb{F}$-subspace spanned by $[x,y]$ with $x \in \mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F})$ and $y \in \mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$. We thus have $\mathfrak{h}_{i+1} = \mathfrak{sl}_2(\mathbb{F})$ since $\mathfrak{sl}_2(\mathbb{F})$ is spanned by the vectors

$$\left[\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\right] = \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right), \quad \left[\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)\right] = -\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) \quad \text{and} \quad \left[\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\right] = \left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right).$$

Since H is a closed subgroup of $\mathrm{SL}_2(R)$ with $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ for all $i \geq 1$, we find that H contains all the $A \in \mathrm{SL}_2(R)$ with $A \equiv I \pmod{\lambda}$. The lemma is now immediate since $\overline{H} = [\overline{G},\overline{G}]$. ∎

2.3. **Proof of Proposition 2.1.** Let H be the commutator subgroup of G and fix notation as in §2.2.

Lemma 2.6. *We have $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F})$.*

Proof. The lemma holds if $|\mathbb{F}| = 2$ by (d), so we may assume that $|\mathbb{F}| > 2$. When $|\mathbb{F}| > 3$, the lemma holds from Proposition 4.1 of [PR09a] . So we may assume that $|\mathbb{F}| = 3$. Using (c), we find that $\mathfrak{g}_1$ contains a nonscalar matrix. We have $\overline{G} = \mathrm{GL}_2(\mathbb{F})$ by (b) and hence the space $\mathfrak{g}_1$ is invariant under conjugation by $\mathrm{GL}_2(\mathbb{F})$. We thus have $\mathfrak{g}_1 \supseteq \mathfrak{sl}_2(\mathbb{F})$ by Lemma 2.4.

We now suppose that $\mathfrak{g}_1 \neq \mathfrak{gl}_2(\mathbb{F})$ and hence $\mathfrak{g}_1 = \mathfrak{sl}_2(\mathbb{F})$ since $|\mathbb{F}|$ is prime. So for all $g \in G^1$, we have $\det(g) \equiv 1 \pmod{\mathfrak{p}^2}$. Let W be the subgroup of $\mathrm{GL}_2(R)$ generated by G^1 and H; it is a normal subgroup of G. Note that $\det(g) \equiv 1 \pmod{\mathfrak{p}^2}$ for all $g \in W$ since this is true for all $g \in G^1$ and we have $H \subseteq \mathrm{SL}_2(R)$. Since $\det(G) = R^\times$ by (a) and $\det(W) \subseteq 1 + \mathfrak{p}^2 R$, we find that $(R/\mathfrak{p}^2)^\times$ is a quotient of G/W.

Let $\overline{W}$ be the image of W modulo $\mathfrak{p}$. We have

$$\overline{W} = \overline{H} = [\overline{G}, \overline{G}] = [\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F}),$$

where the last equality uses Lemma 2.3(iii). Since $W \supseteq G^1$ and $\overline{W} = \mathrm{SL}_2(\mathbb{F})$, we find that the group W is normal in G and $G/W \cong \mathrm{GL}_2(\mathbb{F})/\mathrm{SL}_2(\mathbb{F}) \cong \mathbb{F}^\times$. This is a contradiction since $(R/\mathfrak{p}^2)^\times$ is a quotient of G/W and has cardinality strictly larger than $\mathbb{F}^\times = (R/\mathfrak{p})^\times$. Therefore, $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F})$. ☐

Lemma 2.7. *We have $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ for all $i \geq 1$.*

Proof. We have $\overline{G} = \mathrm{GL}_2(\mathbb{F})$ and $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F})$ by Lemma 2.6. By (2.1), $\mathfrak{h}_1 \subseteq \mathfrak{sl}_2(\mathbb{F})$ contains the $\mathbb{F}$-subspace spanned by $gxg^{-1} - x$ with $g \in \mathrm{GL}_2(\mathbb{F})$ and $x \in \mathfrak{gl}_2(\mathbb{F})$. After computing $gxg^{-1} - x$ with $g \in \{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\}$ and $x \in \{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\}$, we deduce that $\mathfrak{h}_1 \supseteq \mathfrak{sl}_2(\mathbb{F})$ and hence $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F})$.

We now prove the lemma by induction on $i \geq 1$. We have already proved the base case so suppose that $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ for some $i \geq 1$. From the map (2.2), we find that $\mathfrak{h}_{i+1} \subseteq \mathfrak{sl}_2(\mathbb{F})$ contains the $\mathbb{F}$-subspace spanned by $[x, y]$ with $x \in \mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F})$ and $y \in \mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$. We thus have $\mathfrak{h}_{i+1} = \mathfrak{sl}_2(\mathbb{F})$ since $\mathfrak{sl}_2(\mathbb{F})$ is spanned by the vectors

$$[\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)] = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \quad [\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)] = -\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad [\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)] = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$ ☐

Lemma 2.8. *The commutator subgroup H of G agrees with the subgroup of matrices in $\mathrm{SL}_2(R)$ whose image modulo $\mathfrak{p}$ lies in $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})]$. If $|\mathbb{F}| > 2$, then $H = \mathrm{SL}_2(R)$.*

Proof. Let H' be the group of matrices in $\mathrm{SL}_2(R)$ whose image modulo $\mathfrak{p}$ lies in the group $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})]$. Since $\overline{G} = \mathrm{GL}_2(\mathbb{F})$, the image of H' modulo $\mathfrak{p}$ is equal to $[\overline{G}, \overline{G}] = \overline{H}$. For each $i \geq 1$, let H'^i be the group of $g \in H'$ for which $g \equiv I \pmod{\mathfrak{p}^i}$. The inclusion $H \subseteq H'$ induces an injective homomorphism $H^i/H^{i+1} \hookrightarrow H'^i/H'^{i+1}$ that we view as an inclusion.

Suppose that $H \neq H'$. The group H' is open in $\mathrm{SL}_2(R)$ and contains H. Since H is a proper closed subgroup of H' that has the same image modulo $\mathfrak{p}$, we must have $H^i/H^{i+1} \subsetneq H'^{i+1}/H'^{i+1}$ for some $i \geq 1$. Since $H' \subseteq \mathrm{SL}_2(R)$, this implies that $\mathfrak{h}_i \neq \mathfrak{sl}_2(\mathbb{F})$ which contradicts Lemma 2.7. Therefore, $H = H'$. If $|\mathbb{F}| > 2$, we have $H = H' = \mathrm{SL}_2(R)$ by Lemma 2.3(iii). ☐

We claim that $G \supseteq \mathrm{SL}_2(R)$. If $|\mathbb{F}| > 2$, then Lemma 2.8 implies that $G \supseteq H = \mathrm{SL}_2(R)$. Now suppose that $|\mathbb{F}| = 2$. The group $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})]$ has cardinality 3 and has index 2 in $\mathrm{SL}_2(\mathbb{F})$. By Lemma 2.8, H is the index 2 subgroup of $\mathrm{SL}_2(R)$ consisting of matrices whose image modulo $\mathfrak{p}$ lies in $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})]$. By (e), there is an element $g \in G \cap \mathrm{SL}_2(R)$ whose image in $\mathrm{SL}_2(\mathbb{F})$ has order 2. Therefore, g represents the nonidentity coset of H in $\mathrm{SL}_2(R)$. Since $g \in G$ and $H \subseteq G$, we have $\mathrm{SL}_2(R) \subseteq G$. This completes the proof of the claim.

We thus have $G = \mathrm{GL}_2(R)$ since $G \supseteq \mathrm{SL}_2(R)$ and $\det(G) = R^\times$ by (a). The proposition follows from this and Lemma 2.8.

2.4. **Commutator subgroups of $\mathrm{GL}_2(R)$ and $\mathrm{SL}_2(R)$.** The following gives some information on commutator subgroups that will be useful later.

Proposition 2.9.

(i) *If $|\mathbb{F}| > 2$, then the commutator subgroup of $\mathrm{GL}_2(R)$ is $\mathrm{SL}_2(R)$.*

(ii) *If* $|\mathbb{F}| = 2$, *then the commutator subgroup of* $\mathrm{GL}_2(R)$ *is*

$$\{B \in \mathrm{SL}_2(R) : B \text{ modulo } \mathfrak{p} \text{ lies in } [\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})]\}.$$

In particular, $[\mathrm{SL}_2(R) : [\mathrm{GL}_2(R), \mathrm{GL}_2(R)]] = 2$.

Proof. Define $G := \mathrm{GL}_2(R)$. Note that G satisfies all the conditions of Proposition 2.1. Lemma 2.8 in the proof of Proposition 2.1 shows that $[G, G]$ is the group consisting of all $B \in \mathrm{SL}_2(R)$ for which B modulo $\mathfrak{p}$ lies in $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})]$. This proves (ii). Part (i) follows from Lemma 2.3(iii). □

Proposition 2.10. *Suppose* $|\mathbb{F}| > 3$,

(i) *The group* $\mathrm{SL}_2(R)$ *is equal to its own commutator subgroup.*
(ii) *The only closed normal subgroup of* $\mathrm{SL}_2(R)$ *with simple quotient is the group consisting of those matrices* $A \in \mathrm{SL}_2(R)$ *for which* $A \equiv \pm I \bmod \mathfrak{p}$.

Proof. Define the group $G = \mathrm{SL}_2(R)$ and let H be its commutator subgroup. With notation as in §2.2, we have $\overline{G} = \mathrm{SL}_2(\mathbb{F})$ and subgroups $\mathfrak{h}_i \subseteq \mathfrak{g}_i = \mathfrak{sl}_2(\mathbb{F})$ for all $i \geq 1$. The image of H modulo $\mathfrak{p}$ is $\overline{H} = [\overline{G}, \overline{G}] = [\mathrm{SL}_2(\mathbb{F}), \mathrm{SL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F})$, where the last equality uses Lemma 2.3(ii).

Take any $i \geq 1$. With $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \overline{G}$ and $x = \left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{g}_i$, the matrix $gxg^{-1} - x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ lies in $\mathfrak{h}_i$ by (2.1). In particular, $\mathfrak{h}_i \subseteq \mathfrak{sl}_2(\mathbb{F})$ contains a nonscalar matrix. The group $\mathfrak{h}_i$ is stable under conjugation by $\mathrm{GL}_2(\mathbb{F})$ since G is a normal subgroup of $\mathrm{GL}_2(R)$. Therefore, $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ by Lemma 2.4.

We have shown that H is a closed subgroup of $\mathrm{SL}_2(R)$ for which $\overline{H} = \mathrm{SL}_2(\mathbb{F})$ and $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F})$ for all $i \geq 1$. Therefore, $H = \mathrm{SL}_2(R)$. This proves (i).

Let N be a closed normal subgroup of $\mathrm{SL}_2(R)$ for which $S := \mathrm{SL}_2(R)/N$ is simple. The group S is finite since it is simple and profinite. Let $\varphi\colon \mathrm{SL}_2(R) \to S$ be the quotient map. The group S is nonabelian since $\mathrm{SL}_2(R)$ is equal to its own commutator subgroup. Let W be the closed normal subgroup of $\mathrm{SL}_2(R)$ consisting of all $A \in \mathrm{SL}_2(R)$ for which $A \equiv \pm I \pmod{\mathfrak{p}}$. The group W is pro-solvable and hence $\varphi(W)$ is a solvable normal subgroup of S. We have $\varphi(W) = 1$ since S is nonabelian and simple. Therefore, $W \subseteq N$. We have $\mathrm{SL}_2(R)/W \cong \mathrm{SL}_2(\mathbb{F})/\{\pm I\}$ which is simple by Lemma 2.3(i). Therefore, $W = N$ which proves (ii). □

3. Group theoretic criterion for large adelic image

Let G be a subgroup of $\mathrm{GL}_2(\widehat{A})$. The goal of this section is to give conditions that ensure that G and $\mathrm{GL}_2(\widehat{A})$ have the same commutator subgroup. For a nonzero ideal $\mathfrak{a}$ of A, we will denote by $G_{\mathfrak{a}}$ the image of G under the projection map $\mathrm{GL}_2(\widehat{A}) \to \mathrm{GL}_2(A_{\mathfrak{a}})$.

Let Λ be the set of nonzero prime ideals of A.

Theorem 3.1. *Let* G *be a closed subgroup of* $\mathrm{GL}_2(\widehat{A})$ *such that the following hold:*

(a) *For all* $\lambda \in \Lambda$, *we have* $G_\lambda \supseteq \mathrm{SL}_2(A_\lambda)$.
(b) *For all distinct* $\lambda_1, \lambda_2 \in \Lambda$ *with* $N(\lambda_1) = N(\lambda_2) > 3$, G *modulo* $\lambda_1\lambda_2$ *has a subgroup of cardinality* $N(\lambda_1)^2$.
(c) *For all distinct* $\lambda_1, \lambda_2 \in \Lambda$ *with* $N(\lambda_1) = N(\lambda_2) = 2$, *the group* $G_{\lambda_1\lambda_2} \cap \mathrm{SL}_2(A_{\lambda_1\lambda_2})$ *contains a subgroup that is conjugate in* $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ *to* $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in A_{\lambda_1\lambda_2}\}$.

(d) *Suppose* $q \in \{2,3\}$ *and let* $\mathfrak{a}$ *be the ideal that is the product of the prime ideals of* A *of norm* q. *Then* $\det(G_{\mathfrak{a}}) = A_{\mathfrak{a}}^{\times}$.

Then $[G,G] = [\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$. *In particular,* $[G,G] = \mathrm{SL}_2(\widehat{A})$ *when* $q > 2$.

3.1. **Proof of Theorem 3.1.** Define $H := [G,G]$; it is a closed subgroup of $\mathrm{SL}_2(\widehat{A})$.

Lemma 3.2. *For any distinct nonzero prime ideals* λ_1 *and* λ_2 *of* A *with norm at least* 4, *we have* $H_{\lambda_1\lambda_2} = \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$.

Proof. For each $1 \le i \le 2$, we have $G_{\lambda_i} \supseteq \mathrm{SL}_2(A_{\lambda_i})$ by (a). Since $\mathrm{SL}_2(A_{\lambda_i})$ is perfect by Proposition 2.10(i), we deduce that $H_{\lambda_i} = [G_{\lambda_i}, G_{\lambda_i}]$ equals $\mathrm{SL}_2(A_{\lambda_i})$. We thus have an inclusion of groups $H_{\lambda_1\lambda_2} \subseteq H_{\lambda_1} \times H_{\lambda_2} = \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ such that each projection $p_i\colon H_{\lambda_1\lambda_2} \to \mathrm{SL}_2(A_{\lambda_i})$ is surjective. Let N_1 and N_2 be the kernel of p_2 and p_1, respectively. We may identify N_i with a closed normal subgroup of $\mathrm{SL}_2(A_{\lambda_i})$ and hence have an inclusion $N_1 \times N_2 \subseteq H_{\lambda_1\lambda_2}$. By Goursat's lemma ([Rib76, Lemma 5.2.1]), the inclusion $H_{\lambda_1\lambda_2} \subseteq \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ induces a homomorphism

$$H_{\lambda_1\lambda_2}/(N_1 \times N_2) \hookrightarrow \mathrm{SL}_2(A_{\lambda_1})/N_1 \times \mathrm{SL}_2(A_{\lambda_2})/N_2$$

whose image is the graph of an isomorphism $\mathrm{SL}_2(A_{\lambda_1})/N_1 \xrightarrow{\sim} \mathrm{SL}_2(A_{\lambda_2})/N_2$.

Suppose the group $\mathrm{SL}_2(A_{\lambda_1})/N_1$ is trivial. We then have $N_i = \mathrm{SL}_2(A_{\lambda_i})$ for each $1 \le i \le 2$. Therefore, $\mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2}) = N_1 \times N_2 \subseteq H_{\lambda_1\lambda_2} \subseteq \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ and the lemma follows.

We may now assume that $\mathrm{SL}_2(A_{\lambda_1})/N_1$ is nontrivial and hence each N_i is a proper closed normal subgroup of $\mathrm{SL}_2(A_{\lambda_i})$. By Proposition 2.10(ii), we find that $N_i \subseteq \{B \in \mathrm{SL}_2(A_{\lambda_i}) : B \equiv \pm I \pmod{\lambda_i}\}$. Therefore, the homomorphism

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

obtained by composing reduction modulo $\lambda_1\lambda_2$ with the obvious quotient map has image equal to the graph of an isomorphism $\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{\pm I\} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$ of finite simple groups. By comparing cardinalities of these simple groups, we have $N(\lambda_1) = N(\lambda_2)$.

Now consider the homomorphism

$$\varphi\colon G_{\lambda_1\lambda_2} \to \mathrm{GL}_2(\mathbb{F}_{\lambda_1})/\{\pm I\} \times \mathrm{GL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$$

obtained by reducing modulo $\lambda_1\lambda_2$ and composing with the obvious quotient map. From (b), $\varphi(G_{\lambda_1\lambda_2})$ contains a group of order $N(\lambda_1)N(\lambda_2)$; it is a p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_{\lambda_1})/\{\pm I\} \times \mathrm{GL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$ where p is the prime dividing q. In particular, there is a $g \in G_{\lambda_1\lambda_2}$ such that $\varphi(g) = (I, g_2)$, where $g_2 \in \mathrm{GL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$ has order a positive power of p. We have already shown that $\varphi(H_{\lambda_1\lambda_2})$ is the graph of an isomorphism $\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{\pm I\} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$. So there is an $(h_1, h_2) \in \varphi(H_{\lambda_1\lambda_2})$ for which h_2 and g_2 do not commute (an element in $\mathrm{GL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$ that commutes with $\mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{\pm I\}$ will be represented by a scalar matrix and hence has order relatively prime to p). Since H is normal in G, we deduce that

$$(I, g_2)(h_1, h_2)(I, g_2)^{-1} = (h_1, g_2 h_2 g_2^{-1})$$

is also in $\varphi(H_{\lambda_1\lambda_2})$. Since $(h_1, g_2 h_2 g_2^{-1})$ and (h_1, h_2) are distinct elements of $\varphi(H_{\lambda_1\lambda_2})$, this contradicts that the group $\varphi(H_{\lambda_1\lambda_2})$ is the graph of a function. ☐

Lemma 3.3. *Let* $S_1, \ldots, S_r$ *be profinite groups that are all perfect with* $r > 1$. *Let* H *be a closed subgroup of* $S_1 \times \cdots \times S_r$ *such that the projection* $H \to S_i \times S_j$ *is surjective for all* $1 \le i < j \le r$. *Then* $H = S_1 \times \cdots \times S_r$.

Proof. When the S_i are finite, this is [Rib76, Lemma 5.2.2] and follows from Goursat's lemma. The general case follows directly from the finite group case since H is closed. □

Lemma 3.4. *Let Λ_1 be the set of nonzero prime ideals of A of norm at least 4. Then the projection $H \to \prod_{\lambda\in\Lambda_1} \mathrm{SL}_2(A_\lambda)$ is surjective.*

Proof. Let I be any finite nonempty subset of Λ_1 with cardinality at least 2. The group $\mathrm{SL}_2(A_\lambda)$ is perfect for all $\lambda \in \Lambda_1$ by Proposition 2.10(i). For any two distinct $\lambda_1, \lambda_2 \in I$, the projection $H \to \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ is surjective by Lemma 3.2. Therefore, the projection $H \to \prod_{\lambda\in I} \mathrm{SL}_2(A_\lambda)$ is surjective by Lemma 3.3. The lemma follows by increasing the set I and using that H is a closed subgroup of $\mathrm{SL}_2(\widehat{A}) = \prod_\lambda \mathrm{SL}_2(A_\lambda)$. □

Lemma 3.5. *Let Λ_2 be the set of nonzero prime ideals of A of norm at most 3. Then the projection $H \to \prod_{\lambda\in\Lambda_2}[\mathrm{GL}_2(A_\lambda), \mathrm{GL}_2(A_\lambda)]$ is surjective.*

Proof. We may assume that Λ_2 is nonempty and hence $q \in \{2, 3\}$. We claim that the projection

$$G \to \prod_{\lambda\in\Lambda_2} \mathrm{GL}_2(A_\lambda)$$

is surjective. The lemma follow immediately by taking commutator subgroups.

Suppose on the contrary that the claim fails. Then there is a minimal nonempty set $\Lambda_2' \subseteq \Lambda_2$ for which $G \to \prod_{\lambda\in\Lambda_2'} \mathrm{GL}_2(A_\lambda)$ is not surjective and we denote its image by B. For any $\lambda \in \Lambda_2'$, we have $G_\lambda = \mathrm{GL}_2(A_\lambda)$ by (a) and (d), and hence $|\Lambda_2'| \geq 2$.

Fix a place $\lambda_1 \in \Lambda_2'$ and define the groups $B_1 := \mathrm{GL}_2(A_{\lambda_1})$ and $B_2 := \prod_{\lambda\in\Lambda_2'-\{\lambda_1\}} \mathrm{GL}_2(A_\lambda)$. We can view B as a subgroup of $B_1 \times B_2$. The projections $p_i\colon B \to B_i$ are surjective by the minimality of Λ_2'. Let N_1 and N_2 be the kernels of p_2 and p_1, respectively. We can view N_i as a subgroup of B_i and hence $N_1 \times N_2 \subseteq B$. The image of the quotient map $G \to B_1/N_1 \times B_2/N_2$ is the graph of an isomorphism $B_1/N_1 \xrightarrow{\sim} B_2/N_2$ by Goursat's lemma ([Rib76, Lemma 5.2.1]).

If B_1/N_1 or B_2/N_2 is trivial, then $N_1 = B_1$ and $N_2 = B_2$ and hence $B \supseteq B_1 \times B_2 = \prod_{\lambda\in\Lambda_2'} \mathrm{GL}_2(A_\lambda)$ which contradicts our choice of Λ_2'.

So we may assume each N_i is a proper closed normal subgroup of B_i. There are thus proper closed normal subgroups M_i of B_i with $M_i \supseteq N_i$ such that the image of $G \to B_1/M_1 \times B_2/M_2$ is the graph of an isomorphism $B_1/M_1 \xrightarrow{\sim} B_2/M_2$ of finite simple groups. The group B_1 is prosolvable (this uses that $\mathrm{GL}_2(\mathbb{F}_2)$ and $\mathrm{GL}_2(\mathbb{F}_3)$ are solvable). Therefore, B_1/M_1 is a cyclic group of prime order.

Suppose that $q = 3$. Using that each B_i/M_i is abelian and Proposition 2.10(i), we find that $M_1 \supseteq \mathrm{SL}_2(A_{\lambda_1})$ and $M_2 \supseteq \prod_{\lambda\in\Lambda_2'-\{\lambda_1\}} \mathrm{SL}_2(A_\lambda)$. Since the homomorphism $G \to B_1/M_1 \times B_2/M_2$ is not surjective, we deduce that the projection $\det(G) \to \prod_{\lambda\in\Lambda_2'} A_\lambda^\times$ is not surjective. This contradicts (d).

Finally suppose that $q = 2$. We have $\Lambda_2 = \Lambda_2' = \{\lambda_1, \lambda_2\}$ for a unique λ_2. Since each B_i/M_i is abelian and $B_i = \mathrm{GL}_2(A_{\lambda_i})$, we have $M_i \supseteq [\mathrm{GL}_2(A_{\lambda_i}), \mathrm{GL}_2(A_{\lambda_i})]$. By (d), there is a $g \in G_{\lambda_1\lambda_2} \cap \mathrm{SL}_2(A_{\lambda_1\lambda_2})$ whose projection g_1 in $\mathrm{GL}_2(A_{\lambda_1})$ has order 2 modulo λ_1 and whose projection in $\mathrm{GL}_2(A_{\lambda_2})$ is the identity matrix. We have $g_1 \in N_1 \subseteq M_1$. Using Proposition 2.9(ii), the group $\mathrm{SL}_2(A_{\lambda_1})$ is generated by g_1 and $[\mathrm{GL}_2(A_{\lambda_1}), \mathrm{GL}_2(A_{\lambda_1})]$. Therefore, $M_1 \supseteq \mathrm{SL}_2(A_{\lambda_1})$. A similar argument shows that $M_2 \supseteq \mathrm{SL}_2(A_{\lambda_2})$. Since the homomorphism

$G \to B_1/M_1 \times B_2/M_2$ is not surjective, we deduce that the projection $\det(G) \to \prod_{\lambda\in\Lambda_2'} A_\lambda^\times$ is not surjective. This contradicts (d). $\square$

Define $B_1 := \prod_{\lambda\in\Lambda_1} \mathrm{SL}_2(A_\lambda)$ and $B_2 := \prod_{\lambda\in\Lambda_2}[\mathrm{GL}_2(A_\lambda), \mathrm{GL}_2(A_\lambda)]$. We have a natural inclusion

$$H \subseteq [\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})] = \prod_{\lambda\in\Lambda_1\cup\Lambda_2} [\mathrm{GL}_2(A_\lambda), \mathrm{GL}_2(A_\lambda)] = B_1 \times B_2,$$

where we have used Proposition 2.10(i). The projections $H \to B_1$ and $H \to B_2$ are surjective by Lemmas 3.4 and 3.5.

Suppose H is a proper subgroup of $B_1 \times B_2$. By Goursat's lemma ([Rib76, Lemma 5.2.1]), there are closed proper normal subgroups N_i of B_i for which we have an isomorphism $B_1/N_1 \cong B_2/N_2$. This implies that there is a finite simple group Q that shows up as a quotient of both B_1 and B_2. The group B_1 is perfect by Proposition 2.10(i) so Q is nonabelian. However, the group B_2 is prosolvable (since $GL_2(\mathbb{F}_2)$ and $\mathrm{GL}_2(\mathbb{F}_3)$ are solvable) and hence Q is cyclic. This gives a contradiction and thus $H = B_1\times B_2 = [\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$. Finally when $q > 2$, we have $[\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})] = \mathrm{SL}_2(\widehat{A})$ by Theorem 2.9(i).

4. Local fields and the image of inertia

Fix a nonzero prime ideal $\mathfrak{p}$ of A. Let K be a finite separable extension of $F_\mathfrak{p}$ which we consider as an A-field via the inclusions $A \subseteq F_\mathfrak{p} \subseteq K$. The integral closure of $A_\mathfrak{p}$ in K is a complete discrete valuation ring $\mathcal{O}$ whose maximal ideal we will denote by $\mathfrak{m}$. Define the residue field $\mathbb{F} := \mathcal{O}/\mathfrak{m}$.

Let $v\colon K^\times \to \mathbb{Z}$ be the discrete valuation corresponding to $\mathcal{O}$ normalized so that $v(K^\times) = \mathbb{Z}$ and we set $v(0) = +\infty$. We will also denoted by v the corresponding $\mathbb{Q}$-valued extension of v to a fixed separable closure K^{sep} of K. Let I_K be the inertia subgroup of $\mathrm{Gal}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and let K^{un} be the maximal unramified extension of K in K^{sep}.

Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld A-module of rank r. We shall say that ϕ is defined over $\mathcal{O}$ if $\phi_a \in \mathcal{O}\{\tau\}$ for all $a \in A$. The Drinfeld module ϕ has stable reduction (of rank r') if there exists a Drinfeld module $\phi'\colon A \to K\{\tau\}$ defined over $\mathcal{O}$ such that ϕ' and ϕ are isomorphic over K and the reduction of ϕ' modulo $\mathfrak{m}$ is a Drinfeld module $A \to \mathbb{F}\{\tau\}$ of rank $r' \geq 1$. Recall that ϕ has good reduction if it has stable reduction of rank r.

Suppose that ϕ has rank 2. The j-invariant of ϕ is $j_\phi := a_1^{q+1}/a_2 \in K$, where $\phi_t = t+a_1\tau+a_2\tau^2$. The Drinfeld module ϕ has potentially good reduction if and only if $v(j_\phi) \geq 0$, cf. [Ros03, Lemma 5.2].

4.1. **Image of inertia.** Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld A-module of rank 2. For a nonzero ideal $\mathfrak{a} \subseteq A$, the Galois action on the $\mathfrak{a}$-torsion of ϕ gives rise to a Galois representation $\bar\rho_{\phi,\mathfrak{a}}\colon \mathrm{Gal}_K \to \mathrm{GL}_2(A/\mathfrak{a})$. If ϕ has good reduction and $\mathfrak{p} \nmid \mathfrak{a}$, then $\bar\rho_{\phi,\mathfrak{a}}(I_K) = 1$. We now study the group $\bar\rho_{\phi,\mathfrak{p}}(I_K)$ when ϕ has good reduction.

Proposition 4.1. *Assume that $K/F_\mathfrak{p}$ is unramified. Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld module of rank 2 that has good reduction. Then one of the following hold:*

(a) *$\bar\rho_{\phi,\mathfrak{p}}(I_K)$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$ to a subgroup of $\left\{\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right) : a \in \mathbb{F}_\mathfrak{p}^\times, b \in \mathbb{F}_\mathfrak{p}\right\}$,*

(b) *$\bar\rho_{\phi,\mathfrak{p}}(I_K)$ is a cyclic subgroup of $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$ of order $q^{2\deg\mathfrak{p}} - 1$.*

Proof. We summarize material from §2 of [PR09b]. After replacing ϕ by an isomorphic Drinfeld module, we may assume that ϕ is defined over $\mathcal{O}$ and that reducing modulo $\mathfrak{m}$ gives a Drinfeld module of rank 2. Then $\phi[\mathfrak{p}]$ extends to a finite flat group scheme over $\mathcal{O}$. The connected and étale components of $\phi[\mathfrak{p}]$ give an exact sequence $0 \to \phi[\mathfrak{p}]^0 \to \phi[\mathfrak{p}] \to \phi[\mathfrak{p}]^{\text{ét}} \to 0$ of finite flat group schemes. Taking K^{sep}-points gives a short exact sequence

$$0 \to \phi[\mathfrak{p}]^0(K^{\text{sep}}) \to \phi[\mathfrak{p}](K^{\text{sep}}) \to \phi[\mathfrak{p}]^{\text{ét}}(K^{\text{sep}}) \to 0 \tag{4.1}$$

of $\mathbb{F}_\mathfrak{p}$-vector spaces that is Gal_K-equivariant. Let h be the height of the Drinfeld module ϕ modulo $\mathfrak{p}$. The $\mathbb{F}_\mathfrak{p}$-vector space $\phi[\mathfrak{p}]^\circ(K^{\text{sep}})$ has dimension h.

The action of I_K on $\phi[\mathfrak{p}]^{\text{ét}}(K^{\text{sep}})$ is trivial from the definition of an étale group scheme. So when $h = 1$, (a) follows from the exact sequence (4.1). We may now suppose that $h = 2$ and hence $\phi[\mathfrak{p}]^{\text{ét}}(K^{\text{sep}}) = 0$. Property (b) then follows from [PR09b, Proposition 2.7(ii)] which shows that I_K acts on $\phi[\mathfrak{p}]^0(K^{\text{sep}})$ via a fundamental character whose image is cyclic of order $q^{2\deg \mathfrak{p}} - 1$. □

The following proposition, which we prove in §4.2, gives constraints on $\bar{\rho}_{\phi,\mathfrak{a}}(I_K)$ when ϕ has stable and bad reduction.

Proposition 4.2. *Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld module of rank 2 that has stable reduction of rank 1. Consider an ideal $\mathfrak{a} = \mathfrak{p}^e\mathfrak{a}'$, where $e \geq 0$ is an integer and $\mathfrak{a}'$ is a nonzero ideal of A that is relatively prime to $\mathfrak{p}$.*

(i) *The group $\bar{\rho}_{\phi,\mathfrak{a}}(\text{Gal}_K)$ is conjugate in $\text{GL}_2(A/\mathfrak{a})$ to a subgroup of*

$$\left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) : a \in (A/\mathfrak{a})^\times \text{ with } a \equiv 1 \pmod{\mathfrak{a}'},\ b \in A/\mathfrak{a},\ c \in \mathbb{F}_q^\times \right\}. \tag{4.2}$$

(ii) *The cardinality of $\bar{\rho}_{\phi,\mathfrak{a}}(I_K)$ is divisible by the denominator of $\frac{v(j_\phi)}{N(\mathfrak{a})} \in \mathbb{Q}$ in lowest terms.*

(iii) *If $\gcd(v(j_\phi), q) = 1$ and $e \leq 1$, then $\bar{\rho}_{\phi,\mathfrak{a}}(I_K)$ contains a subgroup that is conjugate in $\text{GL}_2(A/\mathfrak{a})$ to $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in A/\mathfrak{a}\}$.*

4.2. **Proof of Proposition 4.2.** After possibly replacing ϕ with a K-isomorphic Drinfeld module, we may assume that ϕ is defined over $\mathcal{O}$ and that the reduction of ϕ modulo $\mathfrak{m}$ is a Drinfeld module of rank 1. We have $j_\phi \neq 0$ since ϕ has stable reduction of rank 1.

For a Drinfeld module $\psi\colon A \to K\{\tau\}$, a ψ-lattice is a finitely generated projective A-submodule Γ of ${}^\psi K^{\text{sep}}$ that is discrete and is stable under the action of Gal_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.

Associated to ϕ, we now recall the construction of its *Tate uniformization*; it is a pair (ψ, Γ) which consists of a Drinfeld module $\psi\colon A \to K\{\tau\}$ of rank 1 defined over $\mathcal{O}$ and a ψ-lattice Γ of rank 1. For details see Proposition 7.2 of [Dri74] and its proof; for further details see [Leh09, Chapter 4 §3]. There exists a unique Drinfeld module $\psi\colon A \to K\{\tau\}$ defined over $\mathcal{O}$ of rank 1 and a unique series $u = \tau^0 + \sum_{i=1}^\infty a_i\tau^i \in \mathcal{O}\{\{\tau\}\}$ with $a_i \in \mathfrak{m}$ and $a_i \to 0$ in K, such that

$$u\psi_a = \phi_a u \tag{4.3}$$

for all $a \in A$. We can identify u with the power series $u(x) = x + \sum_{i=1}^\infty a_i x^{q_i}$ and one can show that $u(z)$ converges for all $z \in K^{\text{sep}}$. By considering the analytic properties of u and

(4.3), one shows that the map

$$ {}^{\psi}K^{\mathrm{sep}} \to {}^{\phi}K^{\mathrm{sep}}, \quad z \mapsto u(z) \tag{4.4}$$

is a surjective homomorphism of A-modules whose kernel Γ is a ψ-lattice. Since ϕ has rank 2 and has stable reduction of rank 1, the A-module Γ has rank $2-1=1$.

Fix an $a \in A$ for which $\mathfrak{a} = (a)$. From the homomorphism (4.4) of A-modules, we obtain an isomorphism

$$\psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\sim} \phi[a] = \phi[\mathfrak{a}], \quad z+\Gamma \mapsto u(z) \tag{4.5}$$

of A-modules that is Gal_K-equivariant. We also have a Gal_K-equivariant short exact sequence of A-modules:

$$0 \to \psi[a] = \psi_a^{-1}(0) \to \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\psi_a} \Gamma/a\Gamma \to 0. \tag{4.6}$$

So by combining (4.5) and (4.6), we obtain a short exact sequence

$$0 \to \psi[\mathfrak{a}] \to \phi[\mathfrak{a}] \to \Gamma/\mathfrak{a}\Gamma \to 0 \tag{4.7}$$

of A-modules that is Gal_K-equivariant.

The $A/\mathfrak{a}$-module $\psi[\mathfrak{a}]$ is free of rank 1 since ψ has rank 1. Define the character $\chi_1 := \bar{\rho}_{\psi,\mathfrak{a}} \colon \mathrm{Gal}_K \to \mathrm{Aut}_A(\psi[\mathfrak{a}]) = (A/\mathfrak{a})^\times$. Since A is a PID, Γ is a free A-module of rank 1. The Galois action on Γ is thus given by a character $\chi_2 \colon \mathrm{Gal}_K \to \mathrm{Aut}_A(\Gamma) = A^\times = \mathbb{F}_q^\times$. The character χ_2 also describes the Galois action on the quotient $\Gamma/\mathfrak{a}\Gamma$. From (4.7) we may assume, after making an appropriate choice of basis of $\phi[\mathfrak{a}]$, that

$$\bar{\rho}_{\phi,\mathfrak{a}}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix}$$

holds for all $\sigma \in \mathrm{Gal}_K$.

To complete the proof of (i), it remains to show that $\chi_1(\sigma) \equiv 1 \pmod{\mathfrak{a}'}$ for all $\sigma \in I_K$. Equivalently, we need to show that the action of I_K on $\psi[\mathfrak{a}']$ is trivial. It thus suffices to prove that ψ has good reduction. We have $\psi_t \equiv \phi_t \pmod{\mathfrak{m}}$ by reducing (4.3) modulo $\mathfrak{m}$. This proves that ψ has good reduction since ϕ modulo $\mathfrak{m}$ is a Drinfeld module of rank 1 and ψ has rank 1.

We now prove (ii). Fix a generator γ of the A-module Γ and choose a $z \in K^{\mathrm{sep}}$ for which $\psi_a(z) = \gamma$.

Lemma 4.3. *We have* $v(z) = \frac{v(j_\phi)}{(q-1)N(\mathfrak{a})}$.

Proof. First suppose that $v(z) \geq 0$. Since ψ_a has coefficients in $\mathcal{O}$, we have $v(\gamma) = v(\psi_a(z)) \geq 0$. Since γ is nonzero and $0 = u(\gamma) = \gamma + \sum_{i=1}^{\infty} a_i \gamma^{q^i}$, we must have $v(\gamma) \geq v(a_i\gamma^{q^i})$ for some $i \geq 1$ with $a_i \neq 0$. So $v(\gamma) \geq v(a_i) + q^i v(\gamma) > q^i v(\gamma)$ which is impossible since $v(\gamma) \geq 0$. Therefore, $v(z) < 0$ and hence

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

By [Ros03, Lemma 5.3], we have $v(\gamma) = v(j_\phi)/(q-1)$ and the lemma follows. ☐

Let d be the denominator of $v(j_\phi)/N(\mathfrak{a}) \in \mathbb{Q}$. Let K^t be the maximal tamely ramified extension of K in K^{sep}. Let L be the minimal extension of K^t in K^{sep} for which $\mathrm{Gal}(K^{\mathrm{sep}}/L)$ fixes $z+\Gamma$. The Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K^t)$ acts trivially on Γ since the Galois action on Γ is given by χ_2. Therefore, $L = K^t(z)$. From the isomorphism (4.5), we find that $K^t(z) \subseteq K^t(\phi[\mathfrak{a}])$.

A rational number occurs as $v(\alpha)$ for some nonzero $\alpha \in K^t$ if and only if its denominator is relatively prime to q. By Lemma 4.3, we find that d is the minimal positive integer for which $dv(z) \in v(K^t - \{0\})$. Therefore, $[K^t(z) : K^t]$ is divisible by d. So d divides $[K^t(\phi[\mathfrak{a}]) : K^t]$ and hence also divides $|\bar{\rho}_{\phi,\mathfrak{a}}(I_K)|$. This completes the proof of (ii).

It remains to prove (iii), so assume $\gcd(v(j_\infty), q) = 1$ and $e \leq 1$. Let $G \subseteq \mathrm{GL}_2(A/\mathfrak{a})$ be the subgroup (4.2). Since $e \leq 1$, the group $B := \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in A/\mathfrak{a}\}$ is a p-Sylow subgroup of G, where p is the prime dividing q. We have $\bar{\rho}_{\phi,\mathfrak{a}}(I_\mathfrak{p}) \subseteq G$ from (i), so it suffices to show that $\bar{\rho}_{\phi,\mathfrak{a}}(I_\mathfrak{p})$ contains a subgroup of order $N(\mathfrak{a})$ (since this will be a p-Sylow subgroup of G and hence conjugate to B). The group $\bar{\rho}_{\phi,\mathfrak{a}}(I_\mathfrak{p})$ contains a subgroup of order $N(\mathfrak{a})$ by (i) and our assumption $\gcd(v(j_\infty), q) = 1$.

5. Frobenius polynomials

Consider a Drinfeld A-module $\phi\colon A \to F\{\tau\}$ of rank r. Take any nonzero prime ideal $\mathfrak{p}$ of A for which ϕ has good reduction. So after replacing ϕ by an isomorphic Drinfeld, we may assume that the coefficients of ϕ are integral at $\mathfrak{p}$ and that reducing modulo $\mathfrak{p}$ gives a Drinfeld module $\bar{\phi}\colon A \to \mathbb{F}_\mathfrak{p}\{\tau\}$ of rank r.

Let $P_{\phi,\mathfrak{p}}(x) \in A[x]$ be the characteristic polynomial of the Frobenius endomorphism $\pi_\mathfrak{p} := \tau^{\deg \mathfrak{p}} \in \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\bar{\phi})$; it is the degree r polynomial that is a power of the minimal polynomial of $\pi_\mathfrak{p}$ over F. The following is an easy consequence of [Gos96, Theorem 4.12.12].

Proposition 5.1. *Let $\mathfrak{p}$ be a nonzero prime ideal of A for which ϕ has good reduction. For any nonzero ideal $\mathfrak{a}$ of A that is relatively prime to $\mathfrak{p}$, $\bar{\rho}_{\phi,\mathfrak{a}}$ is unramified at $\mathfrak{p}$ and*

$$P_{\phi,\mathfrak{p}}(x) \equiv \det(xI - \bar{\rho}_{\phi,\mathfrak{a}}(\mathrm{Frob}_\mathfrak{p})) \pmod{\mathfrak{a}}.$$

We will need to explicitly know some Frobenius polynomials in order to prove Theorem 1.4.

Lemma 5.2. *With q fixed, let $\phi\colon A \to F\{\tau\}$ be the rank 2 Drinfeld module from Theorem 1.4.*

(i) *If $q \neq 2$, then*

$$P_{\phi,(t-c)}(x) = x^2 - x + (t - c)$$

for all nonzero $c \in \mathbb{F}_q$.

(ii) *If $q = 3$, then $P_{\phi,(t^2+t+2)}(x) = x^2 + 2x + t^2 + t + 2$.*

(iii) *If $q = 2$, then $P_{\phi,(t)}(x) = x^2 + t$ and $P_{\phi,(t+1)}(x) = x^2 + x + t + 1$.*

Proof. We first assume that $q \neq 2$ and prove (i). Define the prime ideal $\mathfrak{q} := (t - c)$ of A; note that ϕ has good reduction at $\mathfrak{q}$ since c is nonzero. The image of t in $\mathbb{F}_\mathfrak{q}$ is c, so the reduction of ϕ modulo $\mathfrak{q}$ is the Drinfeld A-module $\bar{\phi}\colon A \to \mathbb{F}_\mathfrak{q}\{\tau\} = \mathbb{F}_q\{\tau\}$ for which $t \mapsto c + \tau - c^{q-1}\tau^2 = c + \tau - \tau^2$. The j-invariant $j_{\bar{\phi}}$ of $\bar{\phi}$ is -1. By [Gek08, Proposition 2.11], the constant term of $P_{\phi,(t-c)}(x)$ is equal to $-(-1)^{-1}(t - c) = t - c$. We have $P_{\phi,(t-c)}(x) = x^2 - ax + (t - c)$ for a unique $a \in A$. By [Gek08, Proposition 2.14(ii)] (with $n = 1$), we have $a \in \mathbb{F}_q$ and $a = -1^{-1} j_{\bar{\phi}} = 1$. Therefore, $P_{\phi,(t-c)}(x) = x^2 - x + (t - c)$.

Parts (ii) and (iii) both were found using the algorithm outlined in [Gek08, §3.4] to compute $P_{\phi,\mathfrak{p}}$. ∎

6. Determinant of the image of Galois

Fix polynomials a_1 and a_2 in A with $a_2 \neq 0$, and let d be the degree of a_2. Let $\phi\colon A \to F\{\tau\}$ be the Drinfeld A-module of rank 2 for which $\phi_t = t + a_1\tau + a_2\tau^2$. The following result gives an explicit expression for the index of $\det(\rho_\phi(\mathrm{Gal}_F))$ in $\widehat{A}^\times$.

Theorem 6.1. *Let $\zeta \in \mathbb{F}_q^\times$ be the leading coefficient of $(-1)^{d+1}a_2$ in $A = \mathbb{F}_q[t]$ and let e be the order of ζ in $\mathbb{F}_q^\times$. Then*

$$[\widehat{A}^\times : \det(\rho_\phi(\mathrm{Gal}_F))] = \gcd(d-1, (q-1)/e).$$

We also give a condition that can be used to show that the image of $\bar{\rho}_{\phi,\mathfrak{a}}$ has maximal determinant.

Proposition 6.2. *Let $\mathfrak{a}$ be a nonzero ideal of A and define*

$$g := \gcd\big(\{d-1, q-1\} \cup \{v_\mathfrak{p}(a_2) : \mathfrak{p} \nmid \mathfrak{a} \text{ nonzero prime ideal of } A\}\big).$$

If $g = 1$, then $\det(\bar{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)) = (A/\mathfrak{a})^\times$.

We will prove Theorem 6.1 and Proposition 6.2 in §6.2.

6.1. Galois image for rank 1 Drinfeld modules.

Fix a nonzero $\Delta \in A$ and let $\psi\colon A \to F\{\tau\}$ be the Drinfeld A-module of rank 1 for which $\psi_t = t + \Delta\tau$. For each nonzero ideal $\mathfrak{a}$ of A, $\psi[\mathfrak{a}]$ is a free $A/\mathfrak{a}$-module of rank 1 with a Galois action that is described by a Galois representation

$$\bar{\rho}_{\psi,\mathfrak{a}}\colon \mathrm{Gal}_F \to \mathrm{Aut}_A(\psi[\mathfrak{a}]) = (A/\mathfrak{a})^\times.$$

Taking the inverse limit, we obtain an isomorphism $\rho_\psi\colon \mathrm{Gal}_F \to \widehat{A}^\times$. We now state a theorem of Gekeler that describes the index of the images of $\bar{\rho}_{\psi,\mathfrak{a}}$ and ρ_ψ.

Theorem 6.3. *Let d be the degree of Δ. Let $\zeta \in \mathbb{F}_q^\times$ be the leading coefficient of $(-1)^d\Delta$ and let e be its order in $\mathbb{F}_q^\times$.*

- (i) *Take any nonzero ideal $\mathfrak{a}$ of A. The integer $[(A/\mathfrak{a})^\times : \bar{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)]$ is the greatest common divisor of $d-1$, $(q-1)/e$, and the integers $v_\mathfrak{p}(\Delta)$ for nonzero prime ideals $\mathfrak{p} \nmid \mathfrak{a}$ of A.*
- (ii) *The group $\rho_\psi(\mathrm{Gal}_F)$ has finite index in $\widehat{A}^\times$ and*

$$[\widehat{A}^\times : \rho_\psi(\mathrm{Gal}_F)] = \gcd(d-1, (q-1)/e).$$

Proof. Before citing Gekeler's result (Theorem 3.13 of [Gek16]), we need to match his assumptions and notation. The representation $\bar{\rho}_{\psi,\mathfrak{a}}$ depends only on $\mathfrak{a}$ and the class of Δ in $F^\times/(F^\times)^{q-1}$; this can be deduced for example from [Gek16, Lemma 1.8]. So after dividing Δ by a suitable $(q-1)$-th power of a monic polynomial, we may assume that

$$\Delta = (-1)^d \zeta P_1^{k_1} \cdots P_s^{k_s}$$

where the $P_i \in A$ are distinct monic irreducible polynomials with $1 \leq k_i < q-1$. Note that this does not change the gcds in (i) and (ii).

We may order the irreducible polynomials so that $P_1, \ldots, P_r$ divide $\mathfrak{a}$ and $P_{r+1}, \ldots, P_s$ are relatively prime to $\mathfrak{a}$. Choose a generator c of the cyclic group $\mathbb{F}_q^\times$. We have $(-1)^d\zeta = c^{k_0}$ and $\zeta = c^{k_0^*}$ for unique $0 \leq k_0, k_0^* < q-1$. We have $k_0^* = k_0$ when $(-1)^d = 1$, i.e., when q is even or d is even. When q is odd and d is odd, we have $k_0^* \equiv (q-1)/2 + k_0 \pmod{q-1}$. Theorem 3.13 of [Gek16] now says that

$$[(A/\mathfrak{a})^\times : \bar{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)] = \gcd(d-1, q-1, k_0^*, k_{r+1}, \ldots, k_s).$$

Since $\zeta = c^{k_0^*}$ and c has order $q-1$ in $\mathbb{F}_q^\times$, we have $e = (q-1)/\gcd(q-1, k_0^*)$. So $\gcd(q-1, k_0^*) = (q-1)/e$ and hence

$$[(A/\mathfrak{a})^\times : \bar{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)] = \gcd(d-1, (q-1)/e, k_{r+1}, \ldots, k_s).$$

Part (i) now follows since the set $\{k_{r+1}, \ldots, k_s\}$ consists of those nonzero integers of the form $v_\mathfrak{p}(\Delta)$ for some nonzero prime ideal $\mathfrak{p} \nmid \mathfrak{a}$ of A.

When $\mathfrak{a}$ is divisible by all the irreducible polynomials $P_1, \ldots, P_s$, we have simply $[(A/\mathfrak{a})^\times : \bar{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)] = \gcd(d-1, (q-1)/e)$. Part (ii) is now immediate since $\rho_\psi(\mathrm{Gal}_F)$ is a closed subgroup of $\widehat{A}^\times$. ∎

6.2. **Proofs of Theorem 6.1 and Proposition 6.2.** Let $\psi\colon A \to F\{\tau\}$ be the rank 1 Drinfeld module for which $\psi_t = t - a_2\tau$. By Corollary 4.6 in [Ham93], we have

$$\det \rho_\phi = \rho_\psi. \tag{6.1}$$

Therefore, $[\widehat{A}^\times : \det(\rho_\phi(\mathrm{Gal}_F))] = [\widehat{A}^\times : \rho_\psi(\mathrm{Gal}_F)]$ and hence Theorem 6.1 follows from Theorem 6.3(ii) with $\Delta := -a_2$.

We now prove Proposition 6.2. We have $\det \bar{\rho}_{\phi,\mathfrak{a}} = \bar{\rho}_{\psi,\mathfrak{a}}$ by (6.1). With $\Delta := -a_2$, Theorem 6.3(i) implies that $[(A/\mathfrak{a})^\times : \det(\bar{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F))]$ divides g. In particular, $\det(\bar{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)) = (A/\mathfrak{a})^\times$ if $g = 1$.

7. Irreducibility

Let $\phi\colon A \to F\{\tau\}$ be a Drinfeld A-module of rank 2. Suppose that λ is a nonzero prime ideal of A for which

- $\bar{\rho}_{\phi,\lambda}\colon \mathrm{Gal}_F \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ is reducible,
- ϕ has stable reduction at λ.

After conjugating $\bar{\rho}_{\phi,\lambda}$, we may assume that

$$\bar{\rho}_{\phi,\lambda}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix} \tag{7.1}$$

for all $\sigma \in \mathrm{Gal}_F$, where $\chi_1, \chi_2\colon \mathrm{Gal}_F \to \mathbb{F}_\lambda^\times$ are characters. In this section, we will give a bound on the norm of λ.

Lemma 7.1. *Set $n := (q-1)^2(q+1)$.*

(i) *The characters χ_1^n and χ_2^n are both unramified at any nonzero prime ideal $\mathfrak{p} \neq \lambda$ of A.*
(ii) *One of the characters χ_1^n or χ_2^n is unramified at λ.*

Proof. Take any nonzero prime ideal $\mathfrak{p}$ of A. We shall view ϕ as being defined over $F_\mathfrak{p}$ and hence $\bar{\rho}_{\phi,\lambda}$, χ_1 and χ_2 are representations of $\mathrm{Gal}_{F_\mathfrak{p}}$. Let $I_\mathfrak{p}$ be an inertia subgroup of $\mathrm{Gal}_{F_\mathfrak{p}}$.

Suppose that $\mathfrak{p} = \lambda$ and ϕ has good reduction. The cardinality of the group $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ divides $q^{\deg\lambda}(q^{\deg\lambda}-1)^2$ by (7.1) and hence $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ cannot have a subgroup of cardinality $q^{2\deg\lambda}-1$. Therefore, property (a) of Proposition 4.1 holds and this implies that χ_1 or χ_2 is unramified at λ. Now suppose that $\mathfrak{p} = \lambda$ and ϕ does not have good reduction. By assumption on λ, the Drinfeld module ϕ has stable reduction of rank 1. Proposition 4.2(i) implies that one of χ_1^{q-1} or χ_2^{q-1} is unramified at λ. We have thus proved (ii) since $q-1$ divides n.

We may now assume that $\mathfrak{p} \neq \lambda$. We have $\phi_t = t + a_1\tau + a_2\tau^2$ with $a_1 \in F$ and $a_2 \in F^\times$. Define $m := \min\{v_\mathfrak{p}(a_i)/(q^i-1) : 1 \leq i \leq 2\}$ and take $1 \leq j \leq 2$ maximal such that $v_\mathfrak{p}(a_j)/(q^j-1) = m$.

Let K be the splitting field of $x^{q^j-1} = a_j$ over $F_\mathfrak{p}$ and fix a root $b \in K$. The extension $K/F_\mathfrak{p}$ is finite and Galois. The ramification index $e := e(K/F_\mathfrak{p})$ of the extension $K/F_\mathfrak{p}$ divides q^j-1. Let I_K be the inertia subgroup of $\mathrm{Gal}_K \subseteq \mathrm{Gal}_{F_\mathfrak{p}}$. For any $\sigma \in I_\mathfrak{p}$, we have $\sigma^e \in I_K$. It thus suffices to prove that $\chi_1^{n/e}(I_K) = 1$ and $\chi_2^{n/e}(I_K) = 1$.

Let $\mathcal{O}$ be the integral closure of $A_\mathfrak{p}$ in K. Let $\phi' \colon A \to K\{\tau\}$ be the Drinfeld module for which $\phi'_t = b\phi_t b^{-1}$. The Drinfeld module ϕ' is isomorphic to ϕ over K.

Suppose $j = 2$. Then ϕ' is defined over $\mathcal{O}$ and has good reduction. Since ϕ' has good reduction and $\mathfrak{p} \neq \lambda$, we have $\bar{\rho}_{\phi',\lambda}(I_K) = 1$. Therefore, $\chi_1(I_K) = 1$ and $\chi_2(I_K) = 1$. Since e divides q^2-1 and hence n, we have $\chi_1^{n/e}(I_K) = 1$ and $\chi_2^{n/e}(I_K) = 1$.

Suppose that $j = 1$. Then ϕ' is defined over $\mathcal{O}$ and has stable reduction of rank 1. By Proposition 4.2(i) and $\lambda \neq \mathfrak{p}$, we have $\chi_1^{q-1}(I_K) = 1$ and $\chi_2^{q-1}(I_K) = 1$. Since n/e is divisible by $n/(q-1) = (q-1)(q+1)$, we have $\chi_1^{n/e}(I_K) = 1$ and $\chi_2^{n/e}(I_K) = 1$. □

For a monic polynomial $P(x) \in A[x]$ and a positive integer $n \geq 1$, we let $P^{(n)}(x) \in A[x]$ be the monic polynomial whose roots (with multiplicity), in some algebraic closure, are precisely the roots of $P(x)$ raised to the n-th power.

Lemma 7.2. *Let n be a positive integer for which parts (i) and (ii) of Lemma 7.1 hold. Then there is a $\zeta \in \mathbb{F}_\lambda^\times$ such that $P_{\phi,\mathfrak{p}}^{(n)}(\zeta^{\deg \mathfrak{p}}) = 0$ in $\mathbb{F}_\lambda$ for all nonzero prime ideals $\mathfrak{p} \neq \lambda$ of A for which ϕ has good reduction.*

Proof. By assumption, there is an $i \in \{1,2\}$ such that χ_i^n is unramified at all nonzero prime ideals of A.

We claim that $\chi_i^n(\mathrm{Gal}(F^{\mathrm{sep}}/\overline{\mathbb{F}}_q(t)) = 1$. Let L be the minimal extension of $\overline{\mathbb{F}}_q(t)$ in F^{sep} for which $\chi_i^n(\mathrm{Gal}(F^{\mathrm{sep}}/L)) = 1$. The extension $L/\overline{\mathbb{F}}_q(t)$ corresponds to a morphism $\pi \colon C \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ of smooth projective and irreducible curves over $\overline{\mathbb{F}}_q$. From our assumptions on χ_i^n, π is unramified away from all points of $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$ except perhaps ∞. The morphism π has degree $N := [L : \overline{\mathbb{F}}_q(t)]$ which is relatively prime to q. Since $L/\overline{\mathbb{F}}_q(t)$ is tamely ramified, the Riemann–Hurwitz theorem implies that $2g-2 = N(2\cdot 0 - 2) + \sum_{i=1}^s (e_i - 1)$, where g is the genus of C and the $e_i \geq 1$ are the ramification indices at the s points of C lying over ∞. Since $\sum_{i=1}^s e_i = N$, we have $2g = 2 - N - s$. Since N and s are positive integers and $g \geq 0$, we must have $N = 1$. This proves the claim.

From the claim χ_i^n factors through a cyclic Galois group $\mathrm{Gal}(\mathbb{F}_{q^d}F/F)$ for some $d \geq 1$. So there is a $\zeta \in \mathbb{F}_\lambda^\times$ for which $\chi_i^n(\mathrm{Frob}_\mathfrak{p}) = \zeta^{\deg \mathfrak{p}}$ for all nonzero prime ideals $\mathfrak{p}$ of A. If $\mathfrak{p} \neq \lambda$ and ϕ has good reduction at $\mathfrak{p}$, then $\chi_i^n(\mathrm{Frob}_\mathfrak{p}) = \zeta^{\deg \mathfrak{p}}$ is a root of $\det(xI - \bar{\rho}_{\phi,\lambda}(\mathrm{Frob}_\mathfrak{p})^n) \equiv P_{\phi,\mathfrak{p}}^{(n)}(x) \pmod{\lambda}$. □

Proposition 7.3. *Let n be a positive integer for which parts (i) and (ii) of Lemma 7.1 hold. Let $d \geq 1$ be an integer for which ϕ has good reduction at multiple nonzero prime ideals of A with the same degree d. Then $\deg \lambda \leq 2nd$.*

Proof. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be distinct prime ideals of A with $\deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = d$ for which ϕ has good reduction. We may assume that $\lambda \notin \{\mathfrak{p}_1, \mathfrak{p}_2\}$ since otherwise $\deg \lambda = d$ and the proposition is immediate. For each $1 \le i \le 2$, set $Q_i(x) := P^{(n)}_{\phi,\mathfrak{p}_i}(x) \in A[x]$.

Let $r \in A$ be the resultant of the polynomials $Q_1(x)$ and $Q_2(x)$. By our choice of n and Lemma 7.2, the polynomials $Q_1(x)$ and $Q_2(x)$ have a common root modulo λ and hence $r \equiv 0 \pmod{\lambda}$.

Let L/F be the splitting field of $P_{\phi,\mathfrak{p}_1}(x)$ and $P_{\phi,\mathfrak{p}_2}(x)$. Let $|\cdot|_\infty$ be an absolute value on L that satisfies $|a|_\infty = q^{\deg a}$ for all nonzero $a \in A$. For any root $\pi \in L$ of $P_{\phi,\mathfrak{p}_i}(x)$, we have $|\pi|_\infty = N(\mathfrak{p}_i)^{1/2} = q^{(\deg \mathfrak{p}_i)/2} = q^{d/2}$, cf. [Gos96, Theorem 4.12.8(5)]. So for any root $\pi \in L$ of $Q_i(x)$, we have $|\pi|_\infty = q^{nd/2}$. Recall that the resultant r is the product of $\pi_1 - \pi_2$ as we vary over all roots π_1 and π_2 in L of $Q_1(x)$ and $Q_2(x)$, respectively. Therefore, $|r|_\infty \le (q^{nd/2})^4 = q^{2nd}$.

We claim that $Q_1(x)$ and $Q_2(x)$ do not have a common roots in L. To the contrary suppose that $\pi \in L$ is a root of $Q_1(x)$ and $Q_2(x)$. Take any $i \in \{1,2\}$. From [Gos96, Theorem 4.12.8(1)] applied to the reduction of ϕ modulo $\mathfrak{p}_i$, there is a unique place of $F(\pi)$ for which π has a zero and it lies over the place of $\mathfrak{p}_i$. We get a contradiction since $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and the claim follows.

From the claim, we have $r \neq 0$. Since r is a nonzero element of A with $|r|_\infty \le q^{2nd}$, we have $\deg r \le 2nd$. Since r is nonzero and $r \equiv 0 \pmod{\lambda}$, we have $\deg \lambda \le \deg r$. Therefore, $\deg \lambda \le \deg r \le 2nd$. □

8. Hilbert irreducibility

Fix an integer $r \ge 2$ and a nonzero ideal $\mathfrak{a}$ of A. For any $a = (a_1, \ldots, a_r) \in A^r$ with $a_r \neq 0$, we let $\phi(a)\colon A \mapsto F\{\tau\}$ be the Drinfeld A-module of rank r for which $\phi(a)_t = t + a_1\tau + \cdots + a_{r-1}\tau^{r-1} + a_r\tau^r$ and we let

$$\bar{\rho}_{\phi(a),\mathfrak{a}}\colon \operatorname{Gal}_F \to \operatorname{GL}_r(A/\mathfrak{a})$$

be the corresponding Galois representation. The goal of this section is to prove the following theorem which says that $\bar{\rho}_{\phi(a),\mathfrak{a}}$ is surjective for "most" a.

Theorem 8.1. *The set of $a \in A^r$ such that $a_r \neq 0$ and $\bar{\rho}_{\phi(a),\mathfrak{a}}(\operatorname{Gal}_F) = \operatorname{GL}_r(A/\mathfrak{a})$ has density 1.*

8.1. A version of Hilbert's irreducibility theorem.

Fix a positive integer r and a nonempty open subscheme U of $\mathbb{A}^r_F$. Consider a continuous and surjective representation

$$\rho\colon \pi_1(U) \to G,$$

where $\pi_1(U)$ is the étale fundamental group of U and G is a finite group. Here we are suppressing the base point of our fundamental group and hence the representation ρ is only determined up to conjugacy by an element in G.

Take any point $u \in U(F) \subseteq F^r$. Specialization by u gives rise to a continuous representation

$$\rho_u\colon \operatorname{Gal}_F \xrightarrow{u_*} \pi_1(U) \xrightarrow{\rho} G$$

that is uniquely determined up to conjugacy in G. In particular, the group $\rho_u(\operatorname{Gal}_F) \subseteq G$ is uniquely determined up to conjugacy in G. We will show that $\rho_u(\operatorname{Gal}_F) = G$ for all $u \in U(F) \cap A^r$ away from a set of density 0 after first proving an easy lemma.

Lemma 8.2. *Let I be a nonzero ideal of A and fix a subset $B \subseteq (A/I)^r$. Then the set of $a \in A^r$ whose image modulo I lies in B has density $|B|/N(I)^r$.*

Proof. Consider a positive integer d. Define the reduction map $\varphi_d\colon A^r(d) \to (A/I)^r$; it is a homomorphism of finite additive groups. By taking d sufficiently large, we may assume that φ_d is surjective. Therefore, the cardinality of $\varphi_d^{-1}(b)$ is the same for all $b \in (A/I)^r$. In particular, $|\varphi_d^{-1}(B)|/|A^r(d)| = |B|/|(A/I)^r|$ for all sufficiently large d. The lemma is now immediate. □

Theorem 8.3. *The set of $u \in U(F) \cap A^r$ for which $\rho_u(\mathrm{Gal}_F) = G$ has density 1.*

Proof. For a fixed algebraic closure $\overline{F}$ of F, we define the group $G_g := \rho(\pi_1(U_{\overline{F}}))$; it is a closed and normal subgroup of G. Let F'/F be the minimal extension in $\overline{F}$ for which $G_g = \rho(\pi_1(U_{F'}))$. The extension F'/F is Galois and we have a natural short exact sequence

$$1 \to G_g \to G \xrightarrow{\pi} \mathrm{Gal}(F'/F) \to 1.$$

Take any proper subgroup H of G and let S be the set of $u \in U(F) \cap A^r$ for which $\rho_u(\mathrm{Gal}_F)$ is conjugate in G to a subgroup of H. We will prove that S has density 0. This will prove the theorem since G has only finitely many proper subgroups. We have $\pi(\rho_u(\mathrm{Gal}_F)) = \mathrm{Gal}(F'/F)$ for all $u \in U(F)$, so we may assume that $\pi(H) = \mathrm{Gal}(F'/F)$ since otherwise S is empty. We thus have $H \cap G_g \subsetneq G_g$ since H is a proper subgroup of G. Define $C := \bigcup_{g \in G} gHg^{-1}$. Since G_g is a normal subgroup of G and $\pi(H) = \mathrm{Gal}(F'/F)$, we have

$$C \cap G_g = \bigcup_{g \in G} g(H \cap G_g)g^{-1} = \bigcup_{g \in G_g} g(H \cap G_g)g^{-1}.$$

Since $H \cap G_g$ is a proper subgroup of G_g, we have $C \cap G_g \subsetneq G_g$ by Jordan's lemma ([Ser03, Theorem 4']).

There is a ring $R := A[1/n] \subseteq F$ with a nonzero $n \in A$, an R-subscheme $\mathcal{U} \subseteq \mathbb{A}^r_R$, and a representation

$$\varrho\colon \pi_1(\mathcal{U}) \to G$$

so that $\mathcal{U}_F = U$ and base changing ϱ by F gives ρ. Take any nonzero prime ideal $\mathfrak{p}$ of A that does not divide n. We will also denote the prime ideal $\mathfrak{p}R$ of R by $\mathfrak{p}$; we have $R/\mathfrak{p} = A/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$. For each $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, specialization gives a homomorphism $u_*\colon \mathrm{Gal}_{\mathbb{F}_\mathfrak{p}} \to \pi_1(\mathcal{U})$ and we denote by Frob_u the image of the $N(\mathfrak{p})$-power Frobenius. Note that Frob_u in $\pi_1(\mathcal{U})$ is uniquely determined up to conjugacy. Define the set

$$\Omega_\mathfrak{p} := \{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) : \varrho(\mathrm{Frob}_u) \in G - C\}.$$

Now take any $u \in S$. We have $\rho_u(\mathrm{Gal}_F) \subseteq C$. If u modulo $\mathfrak{p}$ lies in $\mathcal{U}(\mathbb{F}_\mathfrak{p})$, then ρ_u is unramified at $\mathfrak{p}$ and $\rho_u(\mathrm{Frob}_\mathfrak{p})$ lies in the same conjugacy class of G as $\varrho(\mathrm{Frob}_u)$. So if u modulo $\mathfrak{p}$ lies in $\Omega_\mathfrak{p}$, then $\rho_u(\mathrm{Frob}_\mathfrak{p})$ lies in $G - C$ which contradicts that $\rho_u(\mathrm{Gal}_F) \subseteq C$. Therefore, the image of S modulo $\mathfrak{p}$ lies in $\mathbb{F}_\mathfrak{p}^r - \Omega_\mathfrak{p}$. By Lemma 8.2, we have

$$\bar{\delta}(S) \le \prod_{\mathfrak{p} \in \mathcal{P}} \frac{|\mathbb{F}_\mathfrak{p}^r - \Omega_\mathfrak{p}|}{|\mathbb{F}_\mathfrak{p}^r|} = \prod_{\mathfrak{p} \in \mathcal{P}} \Big(1 - \frac{|\Omega_\mathfrak{p}|}{N(\mathfrak{p})^r}\Big),$$

where $\mathcal{P}$ is any finite set of nonzero prime ideals of A that do not divide n. So to show that S has denisty 0 it suffices to prove that there is a positive constant $c < 1$ such that $1 - |\Omega_\mathfrak{p}|/N(\mathfrak{p})^r < c$ for infinitely many prime ideals $\mathfrak{p}$ of A.

Now take a nonzero prime ideal $\mathfrak{p}$ of A that splits completely in F' and does not divide n. Our assumption that $\mathfrak{p}$ splits completely in F' implies that $\varrho(\pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{p}})) \subseteq G_g$.

We claim that $\varrho(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$ for all but finitely many such $\mathfrak{p}$. Let R' be the integral closure of R in F'. We can base change ϱ to get a surjective representation $\varrho' \colon \pi_1(\mathcal{U}_{R'}) \to G_g$. To prove the claim, it suffices to show that $\varrho'(\pi_1((\mathcal{U}_{R'})_{\mathbb{F}_\mathfrak{P}})) = \varrho'(\pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{P}}))$ equals G_g for all but finitely many nonzero prime ideals $\mathfrak{P}$ of R'. The representation ϱ' corresponds to an étale cover $Y \to \mathcal{U}_{R'}$ of R'-schemes so that $Y_{F'}$ and $(\mathcal{U}_{R'})_{F'} = \mathcal{U}_{F'}$ are both geometrically irreducible. For nonzero prime ideals $\mathfrak{P}$ of R', we have an étale cover $Y_{\mathbb{F}_\mathfrak{P}} \to \mathcal{U}_{\mathbb{F}_\mathfrak{P}}$ of degree $|G_g|$. The claim follows from $Y_{\mathbb{F}_\mathfrak{P}}$ and $\mathcal{U}_{\mathbb{F}_\mathfrak{P}}$ being geometrically irreducible for all but finitely many $\mathfrak{P}$, cf. [Gro66, 9.7.8].

So by excluding a finite number of $\mathfrak{p}$, we may assume that $\varrho(\pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{p}})) = \varrho(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$. Then an explicit equidistribution result like [Ent21, Theorem 3] implies that

$$|\Omega_\mathfrak{p}| = |\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) : \varrho(\mathrm{Frob}_u) \in G_g - (C \cap G_g)\}| = \tfrac{|G_g - (C\cap G_g)|}{|G_g|} N(\mathfrak{p})^r + O(N(\mathfrak{p})^{r-1/2}),$$

where the implicit constant does not depend on $\mathfrak{p}$. To apply [Ent21, Theorem 3] we are using that the "complexity" of $Y_{\mathbb{F}_\mathfrak{P}} \to \mathcal{U}_{\mathbb{F}_\mathfrak{P}}$ can be bounded independent of the nonzero prime ideal $\mathfrak{P}$ of R' since they arise from a single morphism $Y \to \mathcal{U}_{R'}$.

Therefore, $1 - |\Omega_\mathfrak{p}|/N(\mathfrak{p})^r = |C \cap G_g|/|G_g| + O(N(\mathfrak{p})^{-1/2})$. Since $C \cap G_g \subsetneq G_g$, there is a constant $c < 1$ such that $1 - |\Omega_\mathfrak{p}|/N(\mathfrak{p})^r < c$ holds for all but finitely many prime ideals $\mathfrak{p}$ of A that split completely in F'. The result follows since there are infinitely many prime ideals $\mathfrak{p}$ of A that split completely in F'. ☐

8.2. **Proof of Theorem 8.1.** Define the F-algebra $R := F[b_1, \ldots, b_r, 1/b_r]$, where $b_1, \ldots, b_r$ are indeterminant variables over F. Let $\phi \colon A \to R\{\tau\}$, $\alpha \mapsto \phi_\alpha$ be the homomorphism of $\mathbb{F}_q$-algebras for which

$$\phi_t = t + b_1\tau + \cdots + b_{r-1}\tau^{r-1} + b_r\tau^r; \tag{8.1}$$

it is a Drinfeld A-module of rank r over the scheme $U := \operatorname{Spec} R$. Note that U is a nonempty open subscheme of $\mathbb{A}^r_F = \operatorname{Spec} F[b_1, \ldots, b_r]$. The $\mathfrak{a}$-torsion of ϕ gives rise to a representation

$$\bar\rho_{\phi,\mathfrak{a}} \colon \pi_1(U) \to \mathrm{GL}_r(A/\mathfrak{a})$$

like before.

Take any $a = (a_1, \ldots, a_r) \in U(F) \subseteq F^r$. We have $a_r \neq 0$, so (8.1) with b_i replaced by a_i gives a Drinfeld A-module $\phi(a) \colon A \to F\{\tau\}$ of rank r. Specializing $\bar\rho_{\phi,\mathfrak{a}}$ at a gives a representation $\mathrm{Gal}_F \to \mathrm{GL}_r(A/\mathfrak{a})$ that is isomorphic to $\bar\rho_{\phi(a),\mathfrak{a}}$. Theorem 8.1 will thus follow from Theorem 8.3 and the following lemma.

Lemma 8.4. *We have* $\bar\rho_{\phi,\mathfrak{a}}(\pi_1(U)) = \mathrm{GL}_r(A/\mathfrak{a})$.

Proof. Let V be the closed subvariety of U defined by the equation $b_r = 1$, i.e., corresponding to the prime ideal $\mathfrak{P} = (b_r - 1)$ of R. Specialization $\bar\rho_{\phi,\mathfrak{a}}$ at $\mathfrak{P}$ gives a representation

$$\varrho \colon \pi_1(V) \to \mathrm{GL}_r(A/\mathfrak{a}).$$

It suffices to prove that ϱ is surjective. The representation ϱ agrees with $\bar\rho_{\psi,\mathfrak{a}}$ where $\psi \colon A \to R'\{\tau\}$, $\alpha \mapsto \psi_\alpha$ is the Drinfeld A-module with $\psi_t = t + b_1\tau + \cdots + b_{r-1}\tau^{r-1} + \tau^r$ and $R' = F[b_1, \ldots, b_{r-1}]$.

Set $K := F(b_1, \ldots, b_{r-1})$. Viewing ψ as a Drinfeld A-module over K, it thus suffices to show that $\mathrm{Gal}(K(\psi[\mathfrak{a}])/K) \cong \mathrm{GL}_r(A/\mathfrak{a})$, where $\psi[\mathfrak{a}]$ is the $\mathfrak{a}$-torsion arising from ψ in a fixed separable closure of K. In [Bre16, Theorem 6], Breuer proves that $\operatorname{Gal}(K(\psi[\mathfrak{a}])/K) \cong \operatorname{GL}_r(A/\mathfrak{a})$ which had been earlier conjectured by Abhyankar. $\square$

9. Sieving

Let $\mathcal{B}$ be the set of $a = (a_1, a_2) \in A^2$ with $a_2 \neq 0$ for which the following hold:

- $\rho_{\phi(a),\lambda}(\operatorname{Gal}_F) = \operatorname{GL}_2(A_\lambda)$ for all nonzero prime ideals λ of A,
- the commutator subgroup of $\rho_{\phi(a)}(\operatorname{Gal}_F) \subseteq \operatorname{GL}_2(\widehat{A})$ is equal to $[\operatorname{GL}_2(\widehat{A}), \operatorname{GL}_2(\widehat{A})]$.

The main goal of this section is to prove the following theorem. We will use it in §9.2 to quickly prove Theorem 1.2 in the case $q \neq 2$.

Theorem 9.1. *The set $\mathcal{B}$ has density* 1*.*

9.1. Proof of Theorem 9.1.

Fix an integer $m \geq 2$.

- Let $\mathcal{R}$ be the set of $(a_1, a_2) \in A^2$ for which there are at least two distinct nonzero prime ideals $\mathfrak{p}$ of A that satisfy $\deg \mathfrak{p} > 1$, $v_\mathfrak{p}(a_1) = 0$ and $v_\mathfrak{p}(a_2) = 1$.
- Let $\mathcal{S}_m$ be the set of $(a_1, a_2) \in A^2$ for which $a_1 \not\equiv 0 \pmod{\mathfrak{p}}$ or $a_2 \not\equiv 0 \pmod{\mathfrak{p}}$ for all nonzero prime ideals $\mathfrak{p}$ of A with $\deg \mathfrak{p} > m$.
- Let $\mathcal{T}_m$ be the set of $(a_1, a_2) \in A^2$ for which there are two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of A of the same degree $d \leq m/(2(q-1)^2(q+1))$ for which $a_2 \not\equiv 0 \pmod{\mathfrak{p}_1}$ and $a_2 \not\equiv 0 \pmod{\mathfrak{p}_2}$.
- Let $\mathcal{U}_m$ be the set of $(a_1, a_2) \in A^2$ with $a_2 \neq 0$ for which $\bar{\rho}_{\phi(a),\lambda^2}(\operatorname{Gal}_F) = \operatorname{GL}_2(A/\lambda^2)$ for all nonzero prime ideals λ of A with $\deg \lambda \leq m$.

Lemma 9.2. *For any $a \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$ and nonzero prime ideal λ of A, we have $\rho_{\phi(a),\lambda}(\operatorname{Gal}_F) = \operatorname{GL}_2(A_\lambda)$.*

Proof. Take any $a = (a_1, a_2) \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$ and any nonzero prime ideal λ of A. We have $a_2 \neq 0$. Define $G := \rho_{\phi(a),\lambda}(\operatorname{Gal}_F)$; it is a closed subgroup of $\operatorname{GL}_2(A_\lambda)$. With $R := A_\lambda$, we will show that G satisfies the conditions of Proposition 2.1. Once we have verified that the conditions hold, Proposition 2.1 will imply that $G = \operatorname{GL}_2(A_\lambda)$.

Since $a \in \mathcal{R}$, there is a nonzero prime ideal $\mathfrak{p} \neq \lambda$ of A such that $v_\mathfrak{p}(a_1) = 0$ and $v_\mathfrak{p}(a_2) = 1$. In particular, $\phi(a)$ has stable reduction of rank 1 at $\mathfrak{p}$. Define the j-invariant $j_{\phi(a)} := a_1^{q+1}/a_2 \in F$. We have $v_\mathfrak{p}(j_{\phi(a)}) = -1$. Since $v_\mathfrak{p}(a_2) = 1$ and $\mathfrak{p} \neq \lambda$, $\det(G) = A_\lambda^\times$ by Proposition 6.2. This verifies condition (a) of Proposition 2.1.

Let $I_\mathfrak{p}$ be an inertia subgroup of Gal_F for the prime $\mathfrak{p}$. Take any $i \geq 1$. Since $\mathfrak{p} \neq \lambda$ and the denominator of $v_\mathfrak{p}(j_{\phi(a)})/N(\lambda^i) = -1/N(\lambda)^i$ is $N(\lambda)^i$, Proposition 4.2 implies that there is a subgroup of $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in A/\lambda^i\}$ of order $N(\lambda)^i$ that is conjugate in $\operatorname{GL}_2(A/\lambda^i)$ to a subgroup of $\bar{\rho}_{\phi(a),\lambda^i}(I_\mathfrak{p})$. So after choosing an appropriate basis for $\phi[\lambda^i]$ for all $i \geq 1$, we may assume that

$$\left\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in A/\lambda^i\right\} \subseteq \bar{\rho}_{\phi(a),\lambda^i}(\operatorname{Gal}_F). \tag{9.1}$$

We thus have $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G$ and hence condition (e) of Proposition 2.1 holds. With $i = 2$, (9.1) implies that condition (c) of Proposition 2.1 holds. If $N(\lambda) = 2$, then $\bar{\rho}_{\phi(a),\lambda^2}(\operatorname{Gal}_F) = \operatorname{GL}_2(A/\lambda^2)$ since $a \in \mathcal{U}_m$ and $m \geq 2$; this shows that condition (d) of Proposition 2.1 holds.

It remains to verify that condition (b) of Proposition 2.1 holds, i.e., show that $\bar{\rho}_{\phi(a),\lambda}(\operatorname{Gal}_F) = \operatorname{GL}_2(\mathbb{F}_\lambda)$. Since $a \in \mathcal{U}_m$, we may assume that $\deg \lambda > m$. Since $a \in \mathcal{S}_m$, we have $a_1 \not\equiv 0 \pmod{\lambda}$ or $a_2 \not\equiv 0 \pmod{\lambda}$. Therefore, $\phi(a)$ has stable reduction at λ. Since

$\bar{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)$ contains a subgroup of order $N(\lambda)$ by (9.1), Proposition 2.2 implies that $\bar{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) \supseteq \mathrm{SL}_2(\mathbb{F}_\lambda)$ or $\bar{\rho}_{\phi(a),\lambda}$ is reducible.

Suppose that $\bar{\rho}_{\phi(a),\lambda}$ is reducible. Since $a \in \mathcal{T}_m$, there are two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of A of the same degree $d \leq m/(2(q-1)^2(q+1))$ for which $\phi(a)$ has good reduction at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. By Lemmas 7.1 and 7.3 with $n := (q-1)^2(q+1)$, we have $\deg \lambda \leq 2(q-1)^2(q+1)d \leq m$. This is a contradiction since $\deg \lambda > m$.

Therefore, $\bar{\rho}_{\phi(a),\lambda}$ is irreducible and hence $\bar{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) \supseteq \mathrm{SL}_2(\mathbb{F}_\lambda)$. Since $\det(G) = A_\lambda^\times$, we deduce that $\det(\bar{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)) = \mathbb{F}_\lambda^\times$ and hence $\bar{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$. □

Lemma 9.3. *Take any $a \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$. Then the commutator subgroup of $\rho_\phi(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\widehat{A})$ is equal to $[\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$.*

Proof. Define $G := \rho_\phi(\mathrm{Gal}_F)$; it is a closed subgroup of $\mathrm{GL}_2(\widehat{A})$. We will now verify that G satisfies all the conditions of Theorem 3.1. For any nonzero prime ideal λ of A, we have $G_\lambda = \mathrm{GL}_2(A_\lambda)$ by Lemma 9.2. This verifies condition (a) of Theorem 3.1.

Now take any distinct nonzero prime ideals λ_1 and λ_2 of A. Since $a \in \mathcal{R}$, there is a nonzero prime ideal $\mathfrak{p}$ of A such that $v_\mathfrak{p}(a_1) = 0$, $v_\mathfrak{p}(a_2) = 1$, and $\deg \mathfrak{p} > 1$. In particular, $\phi(a)$ has stable reduction of rank 1 at $\mathfrak{p}$. We have $v_\mathfrak{p}(j_{\phi(a)}) = -1$.

Let $I_\mathfrak{p}$ be an inertia subgroup of Gal_F for the prime $\mathfrak{p}$. Take any $i \geq 1$. The denominator of $v_\mathfrak{p}(j_{\phi(a)})/N(\lambda_1\lambda_2) = -1/N(\lambda_1\lambda_2)$ is $N(\lambda_1)N(\lambda_2)$ and hence $\bar{\rho}_{\phi(a),\lambda_1\lambda_2}(I_\mathfrak{p})$ contains a subgroup of cardinality $N(\lambda_1)N(\lambda_2)$ by Proposition 4.2(ii). In particular, the image of G modulo $\lambda_1\lambda_2$ contains a subgroup of cardinality $N(\lambda_1)N(\lambda_2)$. This verifies that condition (b) of Theorem 3.1 holds.

Now suppose that $N(\lambda_1) = N(\lambda_2) = 2$. We have $\mathfrak{p} \notin \{\lambda_1, \lambda_2\}$ since $\deg \mathfrak{p} > 1$. Take any $i \geq 1$. Proposition 4.2 implies that $\bar{\rho}_{\phi(a),\lambda_1^i\lambda_2^i}(I_\mathfrak{p})$ is conjugate in $\mathrm{GL}_2(A/(\lambda_1^i\lambda_2^i))$ to a subgroup of $\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) : b \in A/(\lambda_1^i\lambda_2^i)\}$ and that $\bar{\rho}_{\phi(a),\lambda_1^i\lambda_2^i}(I_\mathfrak{p})$ has cardinality divisible by $N(\lambda_1^i\lambda_2^i)$. So after choosing appropriate bases for $\phi[\lambda_1^i\lambda_2^i]$ for all $i \geq 1$, we may assume that

$$\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) : b \in A_{\lambda_1\lambda_2}\} \subseteq \rho_{\phi(a),\lambda_1\lambda_2}(\mathrm{Gal}_F).$$

This verifies that condition (c) of Theorem 3.1 holds.

Now suppose that $q \in \{2, 3\}$ and let $\mathfrak{a}$ be the ideal that is the product of the prime ideals of A of degree 1. We have $\deg \mathfrak{p} > 1$. Since $v_\mathfrak{p}(a_2) = 1$ and $\mathfrak{p} \nmid \mathfrak{a}$, we have $\det(\bar{\rho}_{\phi,\mathfrak{a}^i}(\mathrm{Gal}_F)) = (A/\mathfrak{a}^i)^\times$ for all $i \geq 1$ by Proposition 6.2. Condition (d) of Theorem 3.1 is now immediate.

We have verified the conditions of Theorem 3.1 and hence G and $\mathrm{GL}_2(\widehat{A})$ have the same commutator subgroup. □

By Lemmas 9.2 and 9.3, we have an inclusion $\mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m \subseteq \mathcal{B}$ and hence

$$A^2 - \mathcal{B} \subseteq (A^2 - \mathcal{R}) \cup (A^2 - \mathcal{S}_m) \cup (A^2 - \mathcal{T}_m) \cup (A^2 - \mathcal{U}_m). \tag{9.2}$$

We now bounds the upper densities of the sets in the right-hand side of (9.2).

Lemma 9.4. *We have $\delta(A^2 - \mathcal{R}) = 0$.*

Proof. Recall that the reciprocal of the zeta function of $\mathbb{A}^1_{\mathbb{F}_q} = \operatorname{Spec} A$ is the power series $\prod_\mathfrak{p}(1 - T^{\deg \mathfrak{p}})$, where the product is over nonzero prime ideals of A, and it is equal to $1 - qT$. By considering $T = 1/q$, and hence $T^{\deg \mathfrak{p}} = 1/N(\mathfrak{p})$, we find that $\lim_{d\to+\infty} \prod_{\mathfrak{p},\, \deg \mathfrak{p} \leq d}(1 -$

$\frac{1}{N(\mathfrak{p})}) = 0$. We can choose two disjoint sets $\mathcal{P}_1$ and $\mathcal{P}_2$ of nonzero prime ideals of A with degree at least 2 such that

$$\lim_{d\to+\infty} \prod_{\mathfrak{p}\in\mathcal{P}_i,\, \deg\mathfrak{p}\le d} (1 - \tfrac{1}{N(\mathfrak{p})}) = 0 \tag{9.3}$$

for $1 \le i \le 2$.

Take any $1 \le i \le 2$ and let S_i be the set of $(a_1, a_2) \in A^2$ such that $(v_\mathfrak{p}(a_1), v_\mathfrak{p}(a_2)) \ne (0,1)$ for all $\mathfrak{p} \in \mathcal{P}_i$. Take any $\mathfrak{p} \in \mathcal{P}_i$ and let $\Omega_\mathfrak{p}$ be the set of $(b_1, b_2) \in (A/\mathfrak{p}^2)^2$ for which $b_1 \not\equiv 0 \pmod{\mathfrak{p}}$, $b_2 \equiv 0 \pmod{\mathfrak{p}}$ and $b_2 \not\equiv 0 \pmod{\mathfrak{p}^2}$. Define

$$\alpha_\mathfrak{p} := \tfrac{|(A/\mathfrak{p}^2)^2 - \Omega_\mathfrak{p}|}{|(A/\mathfrak{p}^2)^2|} = 1 - \tfrac{|\Omega_\mathfrak{p}|}{|(A/\mathfrak{p}^2)^2|} = 1 - (1 - \tfrac{1}{N(\mathfrak{p})})(\tfrac{1}{N(\mathfrak{p})} - \tfrac{1}{N(\mathfrak{p})^2}) \le (1 - \tfrac{1}{N(\mathfrak{p})})(1 + \tfrac{c}{N(\mathfrak{p})^2}),$$

where $c \ge 1$ is an absolute constant. Note that the image of S_i modulo $\mathfrak{p}^2$ lies in $(A/\mathfrak{p}^2)^2 - \Omega_\mathfrak{p}$. For any positive integer d, Lemma 8.2 implies that

$$\bar{\delta}(S_i) \le \prod_{\mathfrak{p}\in\mathcal{P}_i\ \deg\mathfrak{p}\le d} \alpha_\mathfrak{p} \le \prod_{\mathfrak{p}\in\mathcal{P}_i,\, \deg\mathfrak{p}\le d} (1 - \tfrac{1}{N(\mathfrak{p})})(1 + \tfrac{c}{N(\mathfrak{p})^2}).$$

Using the zeta function of $\mathbb{A}^1_{\mathbb{F}_q}$, we find that $\prod_{\mathfrak{p},\, \deg\mathfrak{p}\le d}(1+\frac{c}{N(\mathfrak{p})^2})$ can be bounded independent of d. So there is a positive constant C such that

$$\bar{\delta}(S_i) \le C \prod_{\mathfrak{p}\in\mathcal{P}_i,\, \deg\mathfrak{p}\le d} (1 - \tfrac{1}{N(\mathfrak{p})})$$

holds for any $d \ge 1$. By (9.3), we deduce that $\bar{\delta}(S_i) = 0$ and hence $\delta(S_i) = 0$.

We have $\mathcal{R} \supseteq A^2 - (S_1 \cup S_2)$ since the sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are disjoint. Since $\delta(S_1) = \delta(S_2) = 0$, we conclude that $\delta(\mathcal{R}) = 1$. □

Lemma 9.5. *For any $\varepsilon > 0$, we have $\bar{\delta}(A^2 - \mathcal{S}_m) < \varepsilon$ for all large enough $m \ge 1$.*

Proof. Define $\mathcal{C} := A^2 - \mathcal{S}_m$, i.e., the set of $(a_1, a_2) \in A^2$ for which $a_1 \equiv 0 \pmod{\mathfrak{p}}$ and $a_2 \equiv 0 \pmod{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of A with $\deg\mathfrak{p} > m$.

Fix an integer $d > m$. Let $\mathcal{P}(d)$ be the set of $(a_1, a_2) \in A^2$ with $\deg(a_1) \le d$ and $\deg(a_2) \le d$. Define $\mathcal{C}(d) := \mathcal{C} \cap \mathcal{P}(d)$.

Take any $(a_1, a_2) \in \mathcal{P}(d) - \{(0,0)\}$ with $a_1 \equiv 0 \pmod{\mathfrak{p}}$ and $a_2 \equiv 0 \pmod{\mathfrak{p}}$ for some nonzero prime ideal $\mathfrak{p}$ of A. Fix an $1 \le i \le 2$ for which $a_i \ne 0$. We have $a_i \equiv 0 \pmod{\mathfrak{p}}$ and hence $\deg\mathfrak{p} \le \deg a_i \le d$.

Therefore,

$$|\mathcal{C}(d)| \le \sum_{\mathfrak{p},\, m<\deg\mathfrak{p}\le d} \beta_\mathfrak{p}(d), \tag{9.4}$$

where $\beta_\mathfrak{p}(d)$ is the number of $(a_1, a_2) \in \mathcal{P}(d)$ such that $a_1 \equiv 0 \pmod{\mathfrak{p}}$ and $a_2 \equiv 0 \pmod{\mathfrak{p}}$. Take any nonzero prime ideal $\mathfrak{p}$ of A with $m < \deg(\mathfrak{p}) \le d$. The reduction modulo $\mathfrak{p}$ map $\mathcal{P}(d) \to \mathbb{F}_\mathfrak{p}^2$ is a surjective homomorphism of $\mathbb{F}_q$-vector spaces and hence the kernel has dimension $2(d+1) - 2\deg\mathfrak{p}$. Therefore, $\beta_\mathfrak{p}(d) = q^{2(d+1-\deg\mathfrak{p})}$. Using (9.4), we deduce that

$$\frac{|\mathcal{C}(d)|}{|\mathcal{P}(d)|} \le \sum_{\mathfrak{p},\, m<\deg\mathfrak{p}\le d} q^{-2\deg\mathfrak{p}} \le \sum_{\mathfrak{p},\, \deg\mathfrak{p}>m} q^{-2\deg\mathfrak{p}},$$

where we note that the series converges absolutely. So by taking $m \ge 1$ large enough, we will have $|\mathcal{C}(d)|/|\mathcal{P}(d)| < \varepsilon$ for all $d > m$. Therefore, $\bar{\delta}(A^2 - \mathcal{S}_m) = \bar{\delta}(\mathcal{C}) < \varepsilon$. □

Lemma 9.6. *For any $\varepsilon > 0$, we have $\bar{\delta}(A^2 - \mathcal{T}_m) < \varepsilon$ for all large enough $m \geq 1$.*

Proof. Let $d(m)$ be the largest integer for which $d(m) \leq m/(2(q-1)^2(q+1))$. By taking m large enough, we may assume that there are distinct nonzero prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of A with $\deg \mathfrak{p}_1 = \deg \mathfrak{p}_2 = d(m)$. Let Ω be the set of $b \in A/(\mathfrak{p}_1\mathfrak{p}_2)$ for which $b \equiv 0 \pmod{\mathfrak{p}_1}$ or $b \equiv 0 \pmod{\mathfrak{p}_2}$. The image of $A^2 - \mathcal{T}_m$ modulo $\mathfrak{p}_1\mathfrak{p}_2$ lies in Ω. By Lemma 8.2, we have $\bar{\delta}(A^2 - \mathcal{T}_m) = |\Omega|/|A/(\mathfrak{p}_1\mathfrak{p}_2)| \leq 1/N(\mathfrak{p}_1) + 1/N(\mathfrak{p}_2) = 2/q^{d(m)}$. Since $d(m) \to \infty$ as $m \to \infty$, we conclude that $\bar{\delta}(A^2 - \mathcal{T}_m) < \varepsilon$ for large enough m. □

Lemma 9.7. *We have have $\delta(A^2 - \mathcal{U}_m) = 0$.*

Proof. This follows from Theorem 8.1. □

From the inclusion (9.2), we have

$$\bar{\delta}(A^2 - \mathcal{B}) \leq \bar{\delta}(A^2 - \mathcal{R}) + \bar{\delta}(A^2 - \mathcal{S}_m) + \bar{\delta}(A^2 - \mathcal{T}_m) + \bar{\delta}(A^2 - \mathcal{U}_m).$$

Take any $\varepsilon > 0$. Using Lemmas 9.4, 9.5, 9.6 and 9.7, we deduce that $\bar{\delta}(A^2 - \mathcal{B}) < \varepsilon$ for all sufficiently large integers m. Since $\varepsilon > 0$ was arbitrary, we have $\bar{\delta}(A^2 - \mathcal{B}) = 0$ and hence $\delta(A^2 - \mathcal{B}) = 0$. Therefore, $\mathcal{B}$ has density 1.

9.2. **Proof of Theorem 1.2 when $q \neq 2$.** We assume throughout that $q \neq 2$.

Take any $a \in \mathcal{B}$. We have $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$ for all nonzero prime ideals λ of A by our definition of $\mathcal{B}$ and hence $a \in S_3$. We have $[\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})] = \mathrm{SL}_2(\widehat{A})$ by Proposition 2.9 and our assumption that $q \neq 2$. By our definition of $\mathcal{B}$, the commutator subgroup of $\rho_{\phi(a)}(\mathrm{Gal}_F)$ is $\mathrm{SL}_2(\widehat{A})$ and in particular we have $\rho_{\phi(a)}(\mathrm{Gal}_F) \supseteq \mathrm{SL}_2(\widehat{A})$. The index $[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)]$ thus agrees with $[\widehat{A}^\times : \det(\rho_{\phi(a)}(\mathrm{Gal}_F))]$ which divides $q-1$ by Theorem 6.3(ii). Therefore, $a \in S_2$. Since a was an arbitrary element of $\mathcal{B}$, we have $S_2 \supseteq \mathcal{B}$ and $S_3 \supseteq \mathcal{B}$. Theorem 9.1 implies that S_2 and S_3 have density 1.

Let $\mathcal{P}$ be the set of $(a_1, a_2) \in A^2$ with $a_2 \neq 0$ for which the leading coefficient of the polynomial $(-1)^{\deg a_2 + 1} a_2$ generates the cyclic group $\mathbb{F}_q^\times$. The set $\mathcal{P}$ has positive density; moreover, it has density $\varphi(q-1)/(q-1)$, where φ is Euler's totient function. For $a \in \mathcal{P}$, we have $[\widehat{A}^\times : \det(\rho_{\phi(a)}(\mathrm{Gal}_F))] = 1$ by Theorem 6.1.

We have $S_1 \supseteq \mathcal{P} \cap \mathcal{B}$ since $\rho_{\phi(a)}(\mathrm{Gal}_F) \supseteq \mathrm{SL}_2(\widehat{A})$ and $\det(\rho_{\phi(a)}(\mathrm{Gal}_F)) = \widehat{A}^\times$ for all $a \in \mathcal{P} \cap \mathcal{B}$. We have $\delta(\mathcal{P} \cap \mathcal{B}) = \delta(\mathcal{P}) > 0$ since $\mathcal{B}$ has density 1 by Theorem 9.1. Therefore, S_1 has a subset with positive density.

10. $q = 2$ and wild ramification at ∞

Throughout §10, we assume that $q = 2$. The goal of this section is to give a condition that ensures $\rho_\phi(\mathrm{Gal}_F)$ equals $\mathrm{GL}_2(\widehat{A})$ assuming it contains its commutator subgroup. Let $v_\infty \colon F^\times \twoheadrightarrow \mathbb{Z}$ be the valuation satisfying $v_\infty(a) = -\deg(a)$ for all nonzero $a \in A$.

Proposition 10.1. *Let $\phi\colon A \to F\{\tau\}$ be a Drinfeld A-module of rank 2 for which $v_\infty(j_\phi)$ is odd and $v_\infty(j_\phi) \leq -5$. Then the homomorphism*

$$\mathrm{Gal}_F \to \mathrm{GL}_2(\widehat{A})/[\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$$

obtained by composing ρ_ϕ with the obvious quotient map is surjective.

10.1. **Maximal abelian quotient.** For each $i \in \mathbb{F}_2$, define the prime ideal $\lambda_i = (t+i)$ of A. Define the homomorphism

$$\gamma_i \colon \operatorname{GL}_2(\widehat{A}) \to \operatorname{GL}_2(\mathbb{F}_{\lambda_i}) = \operatorname{GL}_2(\mathbb{F}_2) \to \operatorname{GL}_2(\mathbb{F}_2)/[\operatorname{GL}_2(\mathbb{F}_2), \operatorname{GL}_2(\mathbb{F}_2)] \cong \{\pm 1\},$$

where we are composing reduction modulo λ_i with the quotient map. We obtain a surjective continuous homomorphism

$$\beta \colon \operatorname{GL}_2(\widehat{A}) \to \widehat{A}^\times \times \{\pm 1\} \times \{\pm 1\}, \quad B \mapsto (\det(B), \gamma_0(B), \gamma_1(B)).$$

Lemma 10.2. *The kernel of β is $[\operatorname{GL}_2(\widehat{A}), \operatorname{GL}_2(\widehat{A})]$.*

Proof. We have $\operatorname{GL}_2(\widehat{A}) = \prod_\lambda \operatorname{GL}_2(A_\lambda)$, where the product is over the nonzero prime ideals of A. Therefore, the commutator subgroup of $\operatorname{GL}_2(\widehat{A})$ is equal to $\prod_\lambda [\operatorname{GL}_2(A_\lambda), \operatorname{GL}_2(A_\lambda)]$. Using Proposition 2.9, we obtain a description of $[\operatorname{GL}_2(\widehat{A}), \operatorname{GL}_2(\widehat{A})]$ that agrees with the kernel of β. □

10.2. **Cubic polynomials.** Consider a separable polynomial $f(x) = x^3 + bx + c \in K[x]$, where K is a field. Let r_1, r_2 and r_3 be the distinct roots of $f(x)$ in some separable closure of K and define the splitting field $K' := K(r_1, r_2, r_3)$. Using the numbering of the r_i, we have an injective homomorphism $\iota \colon \operatorname{Gal}(K'/K) \hookrightarrow \mathfrak{S}_3$ to the symmetric group on 3 letters. Let $\varepsilon \colon \operatorname{Gal}(K'/K) \to \{\pm 1\}$ be the homomorphism obtained by composing ι with the parity character.

Let L/K be the subfield of K' fixed by the kernel of ε. We want to explicitly describe the extension L/K. When K has odd characteristic, L is obtained by adjoining to K a square root of the discriminant of $f(x)$. This is not good enough for our application which concerns fields of characteristic 2. The following material comes from [Con] and is straightforward to prove.

Define the polynomial

$$R_2(x) := (x - (r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1))(x - (r_2^2 r_1 + r_1^2 r_3 + r_3^2 r_2)).$$

When expanded out, the coefficients of $R_2(x)$ are symmetric polynomials in r_1, r_2, r_3 and hence are polynomials in b and c. A direct computation shows that

$$R_2(x) = x^2 - 3cx + (b^3 + 9c^2).$$

One can then verify that the $f(x)$ and $R_2(x)$ have the same discriminant. In particular, $R_2(x)$ is separable since $f(x)$ is separable. Note that $r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1$ and $r_2^2 r_1 + r_1^2 r_3 + r_3^2 r_2$ are both fixed by any even permutation of the r_i but are swapped by any odd permutation of the r_i. Therefore, L is the splitting field of $R_2(x)$ in K'.

10.3. **Proof of Proposition 10.1.** By Lemma 10.2, it suffices to prove that $\beta \circ \rho_\phi \colon \operatorname{Gal}_F \to \widehat{A}^\times \times \{\pm 1\} \times \{\pm 1\}$ is surjective.

Take any $i \in \mathbb{F}_2$. With γ_i as in §10.1, we let L_i be the subfield of F^{sep} fixed by the kernel of the homomorphism $\gamma_i \circ \rho_\phi \colon \operatorname{Gal}_F \to \{\pm 1\}$.

Lemma 10.3. *We have $L_i = F(\alpha)$ with α a root of the polynomial*

$$x^2 - x + j_\phi/(t+i)^2 + 1 \in F[x].$$

Proof. We have $\phi_t = t + a_1\tau + a_2\tau^2$ for some $a_1 \in F$ and $a_2 \in F^\times$ and hence $\phi_{t+i} = (t+i) + a_1\tau + a_2\tau^2$. We have $\phi[\lambda_i] \cong \mathbb{F}_2^2$, so $\phi[\lambda_i] = \{0, r_1, r_2, r_3\}$ for distinct nonzero $r_1, r_2, r_3 \in F^{\mathrm{sep}}$. The values r_1, r_2, r_3 are the distinct roots in F^{sep} of the polynomial

$$f(x) := x^3 + (a_1/a_2)x + (t+i)/a_2 = a_2^{-1}x^{-1}((t+i)x + a_1x^2 + a_2x^4) \in F[x].$$

We have a character $\varepsilon\colon \mathrm{Gal}_F \to \{\pm 1\}$ corresponding to $f(x)$ as in §10.2.

With respect to a basis of $\phi[\lambda_i] \cong \mathbb{F}_2^2$, the action of the group $\mathrm{GL}_2(\mathbb{F}_2)$ on $\{r_1, r_2, r_3\}$ is faithful and transitive and induces an isomorphism $\mathrm{GL}_2(\mathbb{F}_2) \xrightarrow{\sim} \mathfrak{S}_3$. Using this, we find that ε agrees with $\gamma_i \circ \rho_\phi$. Therefore, L_i is the subfield of F^{sep} fixed by the kernel of ε. From §10.2, we find that $L_i \subseteq F^{\mathrm{sep}}$ is the splitting field over F of the polynomial

$$R_2(x) = x^2 - 3\big(\tfrac{t+i}{a_2}\big)x + \big(\tfrac{a_1}{a_2}\big)^3 + 9\big(\tfrac{t+i}{a_2}\big)^2 \in F[x].$$

Setting $y = a_2/(t+i)\,x$ and using that our field has characteristic 2, we find that L_i is the splitting field over F of the polynomial $y^2 - y + a_1^3/(a_2(t+i)^2) + 1 = y^2 - y + j_\phi/(t+i)^2 + 1$. ☐

Lemma 10.4. *The homomorphism*

$$\beta'\colon \mathrm{Gal}_F \to \{\pm 1\} \times \{\pm 1\}, \quad \sigma \mapsto (\gamma_0(\rho_\phi(\sigma)), \gamma_1(\rho_\phi(\sigma)))$$

is surjective and is totally ramified at the place ∞ of F.

Proof. Let L be the subfield of F^{sep} fixed by the kernel of β'. We have $L = L_0L_1$. For $i \in \mathbb{F}_2$, Lemma 10.3 implies that $L_i = F(\alpha_i)$ with α_i a root of the polynomial $f_i(x) := x^2 - x + j_\phi/(t+i)^2 + 1$.

We claim that each L_i/F is a quadratic extension that is totally ramified at the place ∞. Since we are in characteristic 2, the roots of $f_i(x)$ in L are α_i and $\alpha_i + 1$. In particular, $\alpha_i(\alpha_i + 1) = j_\phi/(t+i)^2 + 1$. We have $v_\infty(j_\phi/(t+i)^2) = v_\infty(j_\phi) + 2 < 0$, where we have used our assumption that $v_\infty(j_\phi) \le -5$. Therefore,

$$v_\infty(\alpha_i(\alpha_i+1)) = v_\infty(j_\phi/(t+i)^2 + 1) = v_\infty(j_\phi/(t+i)^2) = v_\infty(j_\phi) + 2.$$

Since $v_\infty(j_\phi)$ is odd by assumption, we find that $v_\infty(\alpha_i(\alpha_i+1))$ is a negative odd integer. After extending v_∞ to a $\mathbb{Q}$-valued valuation on F^{sep}, we find that one of the rational numbers $v_\infty(\alpha_i)$ or $v_\infty(\alpha_i+1)$ is negative and hence $v_\infty(\alpha_i) = v_\infty(\alpha_i+1) < 0$. Therefore, $2v_\infty(\alpha_i) = v_\infty(\alpha_i(\alpha_i+1))$ is an odd integer and hence $v_\infty(\alpha_i) \notin \mathbb{Z}$. We deduce that $L_i = F(\alpha_i)$ is a nontrivial extension of F that is ramified at ∞. The claim follows since $[L_i : F] \le 2$.

Define $\alpha := \alpha_0 + \alpha_1$; it is a root of the polynomial

$$x^2 - x + (j_\phi/t^2 + 1) + (j_\phi/(t+1)^2 + 1) = x^2 - x + j_\phi/(t(t+1))^2. \tag{10.1}$$

We claim that $F(\alpha)$ is a quadratic extension of F that totally ramified at the place ∞. The roots of (10.1) are α and $\alpha+1$, so $v_\infty(\alpha(\alpha+1)) = v_\infty(j_\phi/(t(t+1))^2) = v_\infty(j_\phi) + 4$ From our assumptions on $v_\infty(j_\phi)$, we deduce that $v_\infty(\alpha(\alpha+1))$ is a negative odd integer. Therefore, $v_\infty(\alpha) = v_\infty(\alpha+1)$ and $2v_\infty(\alpha)$ is an odd integer. We have $v_\infty(\alpha) \notin \mathbb{Z}$ and hence $F(\alpha)/F$ is a nontrivial extension ramified at ∞. The claim follows since $[F(\alpha) : F] \le 2$.

We now show that β' is surjective. It suffices to show that $[L : F] = 4$. Since $L = L_0L_1$ with $[L_i : F] = 2$, it suffices to show that $L_0 \ne L_1$. If $L_0 = L_1$, then for any $\sigma \in \mathrm{Gal}_F$, we have $\sigma(\alpha_i) = \alpha_i$ for both $i \in \mathbb{F}_2$ or $\sigma(\alpha_i) = \alpha_i + 1$ for both $i \in \mathbb{F}_2$. So if $L_0 = L_1$, then $\alpha = \alpha_0 + \alpha_1$ is fixed by Gal_F and hence $\alpha \in F$. Since $F(\alpha)/F$ is a nontrivial extension, we deduce that $L_0 \ne L_1$. This completes the proof that β' is surjective.

Suppose that L/F is not totally ramified at ∞. Since β' induces an isomorphism $\operatorname{Gal}(L/F) \cong \{\pm 1\} \times \{\pm 1\}$, one of the three quadratic extensions of F in L must be unramified at ∞. However, the three quadratic extensions of F in L are L_0, L_1 and $F(\alpha)$, and we have already shown that they are all ramified at ∞. Therefore, L/F is totally ramified at ∞. $\square$

Lemma 10.5. *The homomorphism* $\det \circ \rho_\phi \colon \operatorname{Gal}_F \to \widehat{A}^\times$ *is surjective and tamely ramified at the place* ∞ *of* F*.*

Proof. We have $\phi_t = t + a_1\tau + a_2\tau^2$ with $a_1 \in F$ and $a_2 \in F^\times$. Let $\psi \colon A \to F\{\tau\}$ be the rank 1 Drinfeld module for which $\psi_t = t - a_2\tau = t + a_2\tau$. By Corollary 4.6 in [Ham93], we have $\det \rho_\phi = \rho_\psi$.

So it suffices to show that $\rho_\psi \colon \operatorname{Gal}_F \to \widehat{A}^\times$ is surjective and tamely ramified at ∞. We have $a_2\psi_t a_2^{-1} = t+\tau$. So after replacing ψ by an isomorphic Drinfeld module, we may assume that ψ is the Carlitz module, i.e., $\psi_t = t + \tau$. For any nonzero ideal $\mathfrak{a}$ of A, the extension $F(\phi[\mathfrak{a}])/F$ is tamely ramified at ∞ and $\operatorname{Gal}(F(\phi[\mathfrak{a}])/F) \cong (A/\mathfrak{a})^\times$, cf. [Hay74, Theorems 2.3 and 3.1]. The lemma is now immediate. $\square$

We need to show that

$$\beta \circ \rho_\phi \colon \operatorname{Gal}_F \to \widehat{A}^\times \times \{\pm 1\} \times \{\pm 1\}$$

is surjective. Composing $\beta \circ \rho_\phi$ with the projection to $\widehat{A}^\times$ gives the homomorphism $\det \circ \rho_\phi$ which is surjective and tamely ramified at ∞ by Lemma 10.5. Composing $\beta \circ \rho_\phi$ with the projection to $\{\pm 1\} \times \{\pm 1\}$ gives a homomorphism β' which is surjective by Lemma 10.4.

Suppose $\beta \circ \rho_\phi$ is not surjective. Goursat's lemma ([Rib76, Lemma 5.2.1]) implies that there is a continuous and surjective homomorphism $\varphi \colon \operatorname{Gal}_F \to Q$, with $Q \neq 1$ a finite group, that factors through both $\det \circ \rho_\phi$ and β'. The homomorphism φ is tamely ramified at ∞ since it factors through $\det \circ \rho_\phi$. However, since φ factors through β', Lemma 10.4 implies that φ is wildly ramified at ∞. This gives a contradiction since $\varphi \neq 1$ and thus $\beta \circ \rho_\phi$ is surjective.

10.4. **Proof of Theorem 1.2 when** $q = 2$**.** We assume $q = 2$. Let $\mathcal{C}$ be the set of $(a_1, a_2) \in A^2$ with $a_1 a_2 \neq 0$ and $\deg(a_1) = \deg(a_2) - 1$. For any integer $d \geq 1$, we have

$$|\mathcal{C}(d)| = \sum_{i=1}^{d} (q-1)q^{i-1} \cdot (q-1)q^i = (q-1)^2 q(q^{2d}-1)/(q^2-1).$$

Therefore,

$$\delta(\mathcal{C}) = \lim_{d\to\infty} \frac{(q-1)^2 q(q^{2d}-1)/(q^2-1)}{q^{2(d+1)}} = \frac{(q-1)^2 q}{q^2(q^2-1)} = \frac{1}{6}.$$

Let $\mathcal{B}$ be the set from §9; it has density 1 by Theorem 9.1. We have $S_3 \supseteq \mathcal{B}$ and hence S_3 has density 1.

Take any $a \in \mathcal{B}$. Theorem 6.3(ii) and $q = 2$ implies that $\det(\rho_{\phi(a)}(\operatorname{Gal}_F)) = \widehat{A}^\times$. Since $\rho_{\phi(a)}(\operatorname{Gal}_F) \supseteq [\operatorname{GL}_2(\widehat{A}), \operatorname{GL}_2(\widehat{A})]$ and $\det(\rho_{\phi(a)}(\operatorname{Gal}_F)) = \widehat{A}^\times$, Lemma 10.2 implies that $[\operatorname{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\operatorname{Gal}_F)]$ divides 4. In particular, $a \in S_2$. We have shown that $S_2 \supseteq \mathcal{B}$ and hence S_2 has density 1.

Now take any $a \in \mathcal{C} \cap S_2$. We have $j_{\phi(a)} = a_1^{q+1}/a_2 = a_1^3/a_2$ and hence

$$v_\infty(j_{\phi(a)}) = -v_\infty(a_2) + 3v_\infty(a_1) = \deg(a_2) - 3\deg(a_1) = -2\deg(a_2) + 3,$$

where the last equality uses that $\deg(a_1) = \deg(a_2) - 1$. Therefore, $v_\infty(j_{\phi(a)})$ is an odd integer and $v_\infty(j_{\phi(a)}) \leq -5$ when $\deg(a_2) \geq 4$. So for any $a \in \mathcal{C} \cap \mathcal{S}_2$ with $\deg(a_2) \geq 4$, Proposition 10.1 and $\rho_{\phi(a)}(\mathrm{Gal}_F) \supseteq [\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$ implies that $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$. The set $\mathcal{C} \cap S_2$ has density $1/6$ and contains only finitely many a with $\deg(a_2) < 4$. Therefore, S_1 has a subset with positive density.

11. Proof of Theorem 1.4

11.1. **Proof of Theorem 1.4 when $q \neq 2$.** Fix a prime power $q > 2$ and let $\phi\colon A \to F\{\tau\}$ be the Drinfeld A-module for which

$$\phi_t = t + \tau - t^{q-1}\tau^2.$$

We will show that $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

Define the prime ideal $\mathfrak{p} := (t)$ of A and let $I_\mathfrak{p}$ be an inertia subgroup of Gal_F at $\mathfrak{p}$. Observe that $\mathfrak{p}$ is the only nonzero prime ideal of A for which ϕ has bad reduction. We have $j_\phi = -1/t^{q-1}$ and hence $v_\mathfrak{p}(j_\phi) = -(q-1)$. In particular, $\gcd(v_\mathfrak{p}(j_\phi), q) = 1$.

Lemma 11.1. *For any nonzero ideal $\mathfrak{a}$ of A, the character $\det \circ \bar{\rho}_{\phi,\mathfrak{a}}\colon \mathrm{Gal}_F \to (A/\mathfrak{a})^\times$ is surjective and is unramified at all nonzero prime ideals $\mathfrak{q} \nmid \mathfrak{a}$ of A.*

Proof. Let $\psi\colon A \to F\{\tau\}$ be the rank 1 Drinfeld module for which $\psi_t = t - (-t^{q-1})\tau = t + t^{q-1}\tau$. By Corollary 4.6 in [Ham93], we have $\det \rho_\phi = \rho_\psi$ and hence also $\det \bar{\rho}_{\phi,\mathfrak{a}} = \bar{\rho}_{\psi.\mathfrak{a}}$. We have $t\psi_t t^{-1} = t + \tau$ and hence ψ is isomorphic to the Carlitz module. The lemma is now an immediate consequence of [Hay74, Proposition 2.2 and Theorem 2.3]. ☐

Lemma 11.2. *For any nonzero prime ideal λ of A, $\bar{\rho}_{\phi,\lambda}$ is irreducible.*

Proof. We will prove the lemma by contradiction. Suppose that $\bar{\rho}_{\phi,\lambda}$ is reducible for some λ.

First suppose that $\lambda = \mathfrak{p} = (t)$. For each nonzero $c \in \mathbb{F}_q$, ϕ has good reduction at $(t-c)$. We have $P_{\phi,(t-c)}(x) = x^2 - x + t - c$ by Lemma 5.2(i). Therefore, $\bar{\rho}_{\phi,\mathfrak{p}}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$ contains an element whose characteristic polynomial is $x^2 - x - c \in \mathbb{F}_\mathfrak{p}[x] = \mathbb{F}_q[x]$. Since $\bar{\rho}_{\phi,\lambda}$ is reducible, we find that the polynomial $x^2 - x - c$ in $\mathbb{F}_q[x]$ is reducible for all $c \in \mathbb{F}_q$. When q is even, this is impossible since $\mathbb{F}_q$ has a quadratic extension which must be given by a polynomial of the form $x^2 - x - c \in \mathbb{F}_q[x]$. When q is odd, this is also impossible since otherwise $(-1)^2 - 4(-c) = 1 + 4c$ would be a square in $\mathbb{F}_q$ for all $c \in \mathbb{F}_q$. Therefore, $\lambda \neq \mathfrak{p}$.

After conjugating $\bar{\rho}_{\phi,\lambda}$, we may assume that (7.1) holds with characters $\chi_1, \chi_2\colon \mathrm{Gal}_F \to \mathbb{F}_\lambda^\times$. Since ϕ has good reduction away from $\mathfrak{p}$, χ_1 and χ_2 are unramified at all nonzero prime ideals of A except perhaps $\mathfrak{p}$ and λ. Proposition 4.2(i), with $\mathfrak{a} := \lambda$ and using $\lambda \neq \mathfrak{p}$, implies that one of the characters χ_1 or χ_2 is unramified at $\mathfrak{p}$. Since $\det \circ \bar{\rho}_{\phi,\lambda} = \chi_1\chi_2$ is unramified at $\mathfrak{p}$ by Lemma 11.1, we deduce that χ_1 and χ_2 are both unramified at $\mathfrak{p}$. Since $\bar{\rho}_{\phi,\lambda}$ is reducible and ϕ has good reduction at λ, Proposition 4.1 implies that χ_1 or χ_2 is unramified at λ.

We have verified that χ_1 and χ_2 satisfy (i) and (ii) of Lemma 7.1 with $n := 1$. By Lemma 7.2, there is a $\zeta \in \mathbb{F}_\lambda^\times$ such that $P_{\phi,\mathfrak{q}}(\zeta^{\deg \mathfrak{q}}) = 0$ holds in $\mathbb{F}_\lambda$ for all nonzero prime ideals $\mathfrak{q} \notin \{\mathfrak{p}, \lambda\}$ of A.

Assume that $q > 3$ or $\deg \lambda > 1$. Then there are distinct nonzero $c_1, c_2 \in \mathbb{F}_q$ with $\lambda \in \{(t - c_1), (t - c_2)\}$. Using Lemma 5.2(i), we have

$$c_2 - c_1 = P_{\phi,(t-c_1)}(\zeta) - P_{\phi,(t-c_2)}(\zeta) \equiv 0 + 0 \equiv 0 \pmod{\lambda}$$

which contradicts that c_1 and c_2 are distinct elements of $\mathbb{F}_q$.

It remains to consider the case where $q = 3$ and $\deg \lambda = 1$. In particular, $\lambda = (t - b)$ with $b \in \mathbb{F}_3^\times$ and $\mathbb{F}_\lambda = \mathbb{F}_3$. Define the prime ideal $\mathfrak{q} := (t^2 + t + 2)$ of A. We have $\zeta^{\deg \mathfrak{q}} = 1$ since $|\mathbb{F}_\lambda^\times| = 2 = \deg \mathfrak{q}$. Therefore, $P_{\phi,\mathfrak{q}}(1) \equiv 0 \pmod{\lambda}$. We have $P_{\phi,\mathfrak{q}}(x) = x^2 + 2x + t^2 + t + 2$ by Lemma 5.2(ii). Therefore,

$$0 \equiv P_{\phi,\mathfrak{q}}(1) \equiv 1^2 + 2 \cdot 1 + b^2 + b + 2 \equiv b^2 + b + 2 \pmod{\lambda}$$

and hence $b^2 + b + 2 = 0$ since $b \in \mathbb{F}_3$. However, this is a contradiction since $x^2 + x + 2$ is irreducible in $\mathbb{F}_3[x]$. □

Lemma 11.3. *For any nonzero prime ideal λ of A, we have $\rho_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$.*

Proof. Take any nonzero prime ideal λ of A. Set $G := \rho_{\phi,\lambda}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(A_\lambda)$. Using Lemma 11.1 with $\mathfrak{a} = \lambda^i$ and $i \geq 1$, we find that $\det(G) = A_\lambda^\times$.

Since $\gcd(v_\mathfrak{p}(j_\phi), q) = 1$, Proposition 4.2(iii) implies that $\bar{\rho}_{\phi,\lambda}(I_\mathfrak{p})$, and hence also $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$, contains a subgroup of cardinality $N(\lambda)$. The group $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ acts irreducibly on $\mathbb{F}_\lambda^2$ by Lemma 11.2. Proposition 2.2 implies that $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F) \supseteq \mathrm{SL}_2(\mathbb{F}_\lambda)$. Since $\det(G) = A_\lambda^\times$, we deduce that the image of G modulo λ is $\mathrm{GL}_2(\mathbb{F}_\lambda)$.

Fix a generator π of the ideal λ. Let P be a p-Sylow subgroup of $\bar{\rho}_{\phi,\lambda^2}(I_\mathfrak{p})$, where p is the prime dividing q. Proposition 4.2(ii) and $\gcd(v(j_\phi), q) = 1$ implies that the cardinality of P is divisible by $N(\lambda)^2$. Since a p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_\lambda)$ has cardinality $N(\lambda)$, we deduce that there is a $g \in P$ such that $g \equiv I + \pi B \pmod{\lambda^2}$ with $B \in M_2(A_\lambda)$ satisfying $B \not\equiv 0 \pmod{\lambda}$. After conjugating our representation $\bar{\rho}_{\phi,\lambda^2}$, we may assume by Proposition 4.2(ii) that

$$\bar{\rho}_{\phi,\lambda^2}(I_\mathfrak{p}) \subseteq \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) : a \in (A/\lambda^2)^\times, b \in A/\lambda^2, c \in \mathbb{F}_q^\times \right\}.$$

Therefore, $P \subseteq \{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in (A/\lambda^2)^\times \text{ with } a \equiv 1 \pmod{\lambda}, b \in A/\lambda^2 \}$ and hence B modulo λ is of the form $\left(\begin{smallmatrix} * & * \\ 0 & 0 \end{smallmatrix}\right)$. Since $B \not\equiv 0 \pmod{\lambda}$, we find that B modulo λ is not a scalar matrix.

We have now verified the conditions of Proposition 2.1 with $q > 2$ and hence $G = \mathrm{GL}_2(A_\lambda)$. □

Set $G := \rho_\phi(\mathrm{Gal}_F)$. We have $\det(G) = \widehat{A}^\times$ by Lemma 11.1, so it remains to prove that $\mathrm{SL}_2(\widehat{A})$ is a subgroup of G. For each nonzero prime ideal λ of A, $\mathrm{SL}_2(A_\lambda)$ is a subgroup of $G_\lambda = \rho_{\phi,\lambda}(\mathrm{Gal}_F)$ by Lemma 11.3. Take any two distinct nonzero prime ideals λ_1 and λ_2 of A. Proposition 4.2(iii) implies that $\bar{\rho}_{\phi,\lambda_1\lambda_2}(I_\mathfrak{p})$ has a subgroup of cardinality $N(\lambda_1)N(\lambda_2)$. In particular, G modulo $\lambda_1\lambda_2$ has a subgroup of cardinality $N(\lambda_1)N(\lambda_2)$. Using Theorem 3.1 and $q > 2$, we deduce that the commutator subgroup of G is $\mathrm{SL}_2(\widehat{A})$ and hence $G \supseteq \mathrm{SL}_2(\widehat{A})$ as desired.

11.2. **Proof of Theorem 1.4 when $q = 2$.** With $q = 2$, let $\phi\colon A \to F\{\tau\}$ be the Drinfeld A-module for which

$$\phi_t = t + t^3\tau + (t^2 + t + 1)\tau^2.$$

We will show that $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$. Since $q = 2$, we have $\det(\rho_\phi(\mathrm{Gal}_F)) = \widehat{A}^\times$ by Theorem 6.3(i).

Define the ideal $\mathfrak{p} := (t^2 + t + 1)$ of A. Observe that $\mathfrak{p}$ is the only nonzero prime ideal of A for which ϕ has bad reduction. Moreover, ϕ has stable reduction of rank 1 at $\mathfrak{p}$. We let $I_\mathfrak{p}$ be an inertia subgroup of Gal_F for the prime $\mathfrak{p}$. We have $j_\phi = (t^3)^{q+1}/(t^2+t+1) = t^9/(t^2+t+1)$ and hence $v_\mathfrak{p}(j_\phi) = -1$.

Lemma 11.4. *The homomorphism* $\mathrm{Gal}_F \to \mathrm{GL}_2(\widehat{A})/[\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$ *obtained by composing* ρ_ϕ *with the obvious quotient map is surjective.*

Proof. This follows from Proposition 10.1 since $v_\infty(j_\phi) = -7$. □

Lemma 11.5. *We have* $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$ *for all nonzero prime ideals* λ *of* A.

Proof. Assume that $\bar{\rho}_{\phi,\lambda}(\mathrm{Gal}_F) \neq \mathrm{GL}_2(\mathbb{F}_\lambda)$ for some λ. Proposition 4.2(iii) implies that $\bar{\rho}_{\phi,\lambda}(I_\mathfrak{p})$ contains a subgroup of order $N(\lambda)$. The representation $\bar{\rho}_{\phi,\lambda}$ is thus reducible by Proposition 2.2. After conjugating $\bar{\rho}_{\phi,\lambda}$, we may assume that

$$\bar{\rho}_{\phi,\lambda}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix}$$

for all $\sigma \in \mathrm{Gal}_F$, where $\chi_1, \chi_2 \colon \mathrm{Gal}_F \to \mathbb{F}_\lambda^\times$ are characters.

First assume that $\deg \lambda = 1$ and hence $\lambda = (t+i)$ for some $i \in \mathbb{F}_2$. The nonzero elements of $\phi[\lambda]$ are the roots of the separable polynomial

$$Q(x) := (t+i) + t^3 x + (t^2+t+1)x^3 \in A[x].$$

We have $\chi_1 = 1$ since $\mathbb{F}_\lambda = \mathbb{F}_2^\times$ and hence there is a nonzero element of $\phi[\lambda]$ lying in F. In particular, $Q(x)$ has a root in F. Therefore, the image of $Q(x)$ in $\mathbb{F}_\mathfrak{q}[x]$ has a root in $\mathbb{F}_\mathfrak{q}$ for all nonzero prime ideals $\mathfrak{q} \neq (t^2+t+1)$ of A. However, a computation shows that $Q(x)$ is irreducible modulo $\mathfrak{q}$ for some prime $\mathfrak{q} \in \{(t+1), (t^3+t+1)\}$.

Therefore, $\deg \lambda > 1$. Since ϕ has good reduction away from $\mathfrak{p}$, we find that χ_1 and χ_2 are unramified at all nonzero prime ideals of A except perhaps $\mathfrak{p}$ and λ. When $\lambda = \mathfrak{p}$, Proposition 4.2(i) and $\mathbb{F}_q^\times = \{1\}$ imply that χ_1 or χ_2 is unramified at $\mathfrak{p}$. When $\lambda \neq \mathfrak{p}$, Proposition 4.2(i) and $\mathbb{F}_q^\times = \{1\}$ imply that both χ_1 and χ_2 are unramified at $\mathfrak{p}$. When $\lambda \neq \mathfrak{p}$, ϕ has good reduction at λ and so Proposition 4.1, with the reducibility of $\bar{\rho}_{\phi,\lambda}$, implies that χ_1 or χ_2 is unramified at λ. In particular, we have verified that parts (i) and (ii) of Lemma 7.1 hold with $n := 1$.

By Lemma 7.2 with $n = 1$, there is a $\zeta \in \mathbb{F}_\lambda^\times$ such that $P_{\phi,\mathfrak{q}}(\zeta^{\deg \mathfrak{q}}) = 0$ in $\mathbb{F}_\lambda$ for all nonzero prime ideals $\mathfrak{q} \neq \lambda$ of A for which ϕ has good reduction. Since $\deg \lambda > 1$, we find that $P_{\phi,(t)}(x)$ and $P_{\phi,(t+1)}(x)$ have a common root modulo λ. Therefore, the resultant $r \in A$ of $P_{\phi,(t)}(x)$ and $P_{\phi,(t+1)}(x)$ is divisible by λ. The polynomials $P_{\phi,(t)}(x)$ and $P_{\phi,(t+1)}(x)$ where computed in Lemma 5.2(iii) and one finds that $r = t+1$. Therefore, $r = t+1 \equiv 0 \pmod{\lambda}$ which is a contradiction since $\deg \lambda > 1$. □

Lemma 11.6. *We have* $\rho_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$ *for all nonzero prime ideals* λ *of* A.

Proof. Set $G := \rho_{\phi,\lambda}(\mathrm{Gal}_F)$. We have $\det(G) = A_\lambda^\times$ since $\det(\rho_\phi(\mathrm{Gal}_F)) = \widehat{A}^\times$. The image of G modulo λ is equal to $\mathrm{GL}_2(\mathbb{F}_\lambda)$ by Lemma 11.5.

By Proposition 4.2(i) and (ii), $\bar{\rho}_{\phi,\lambda^2}(I_\mathfrak{p})$ has a subgroup of cardinality $N(\lambda)^2$ that is conjugate in $\mathrm{GL}_2(A/\lambda^2)$ to a subgroup of $\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in (A/\lambda^2)^\times, b \in A/\lambda^2\}$. So with a fixed uniformizer π of A_λ, we find that G contains a matrix of the form $I + \pi B$ with $B \in M_2(A_\lambda)$ and B modulo λ not a scalar matrix. When $\deg \lambda > 1$ and hence $|\mathbb{F}_\lambda| > 2$, Proposition 2.1 implies that $G = \mathrm{GL}_2(A_\lambda)$.

We now assume that $\deg \lambda = 1$ and hence $\mathbb{F}_\lambda = \mathbb{F}_2$. Since $\lambda \neq \mathfrak{p}$ and $\gcd(v(j_\phi), q) = 1$, Proposition 4.2(iii) implies that for any $i \geq 1$, $\bar{\rho}_{\phi,\lambda^i}(I_\mathfrak{p})$ contains a subgroup that is conjugate in $\mathrm{GL}_2(A/\lambda^i)$ to $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in A/\lambda^i\}$. Using that G is closed, we find that G has an element that is conjugate in $\mathrm{GL}_2(A_\lambda)$ to a matrix of the form $\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)$ with $b \not\equiv 0 \pmod{\lambda}$. In particular, G has an element with determinant 1 whose image modulo λ has order 2.

We will now show that $\overline{G} := \bar{\rho}_{\phi,\lambda^2}(\mathrm{Gal}_F)$ is equal to $\mathrm{GL}_2(A/\lambda^2)$. Let S be the subgroup of $\mathrm{SL}_2(A/\lambda^2)$ consisting of matrices whose image modulo λ is equal to $[\mathrm{GL}_2(\mathbb{F}_\lambda), \mathrm{GL}_2(\mathbb{F}_\lambda)]$. Since $\mathbb{F}_\lambda = \mathbb{F}_2$, we have $|S| = 2^3 \cdot 3$ and $[\mathrm{GL}_2(A/\lambda^2) : S] = 2^2$. The quotient $\mathrm{GL}_2(\mathbb{F}_\lambda)/S$ is abelian and hence the quotient map $\overline{G} \to \mathrm{GL}_2(\mathbb{F}_\lambda)/S$ is surjective by Proposition 10.1. In particular, $[\mathrm{GL}_2(A/\lambda^2) : \overline{G}] = [S : S \cap \overline{G}]$. We know that $\overline{G}$ contains a matrix g that is conjugate in $\mathrm{GL}_2(A/\lambda)$ to some $\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)$ with $b \not\equiv 0 \pmod{\lambda}$. Also g is not stable under conjugation by $\overline{G}$ since the image of $\overline{G}$ modulo λ is $\mathrm{GL}_2(\mathbb{F}_\lambda)$. Therefore, $|S \cap \overline{G}|$ is divisible by 4. The group $S \cap \overline{G}$ contains an element of order 3 since the image of $\overline{G}$ modulo λ is $\mathrm{GL}_2(\mathbb{F}_\lambda) = \mathrm{GL}_2(\mathbb{F}_2)$ and $[\mathrm{GL}_2(A/\lambda^2) : S] = 2^2$. Since $|S| = 2^3 \cdot 3$, we find that $[\mathrm{GL}_2(A/\lambda^2) : \overline{G}] = [S : S \cap \overline{G}]$ is equal to 1 or 2. If $[\mathrm{GL}_2(A/\lambda^2) : \overline{G}] = 2$, then $\overline{G}$ is a normal subgroup of $\mathrm{GL}_2(A/\lambda^2)$ with nontrivial abelian quotient; this would contradict Proposition 10.1. Therefore, we have index 1, i.e., $\overline{G} = \mathrm{GL}_2(A/\lambda^2)$.

We have now verified the conditions need to apply Proposition 2.1 with $|\mathbb{F}_\lambda| = 2$ to show that $G = \mathrm{GL}_2(A_\lambda)$. □

Lemma 11.7. *We have* $\rho_\phi(\mathrm{Gal}_F) \supseteq [\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$.

Proof. Define $G := \rho_\phi(\mathrm{Gal}_F)$; it is a closed subgroup of $\mathrm{GL}_2(\widehat{A})$. We have already observed that $\det(G) = \widehat{A}^\times$. The group $G_\lambda = \rho_{\phi,\lambda}(\mathrm{Gal}_F)$ is equal to $\mathrm{GL}_2(A_\lambda)$ for all nonzero prime ideals λ of A by Lemma 11.6.

Take any two distinct nonzero prime ideals λ_1 and λ_2 of A with $\deg \lambda_1 = \deg \lambda_2$. By Proposition 4.2(iii), $\bar{\rho}_{\phi,\lambda_1\lambda_2}(I_\mathfrak{p}) \subseteq \bar{\rho}_{\phi,\lambda_1\lambda_2}(\mathrm{Gal}_F)$ has a subgroup of cardinality $N(\lambda_1)N(\lambda_2) = N(\lambda_1)^2$.

Now suppose that $\deg \lambda_1 = \deg \lambda_2 = 1$ and hence $\mathfrak{p} \notin \{\lambda_1, \lambda_2\}$. For any integer $i \geq 1$, Proposition 4.2(iii) implies that $\bar{\rho}_{\phi,\lambda_1^i\lambda_2^i}(I_\mathfrak{p}) \subseteq \bar{\rho}_{\phi,\lambda_1^i\lambda_2^i}(\mathrm{Gal}_F)$ contains a subgroup conjugate in $\mathrm{GL}_2(A/(\lambda_1^i\lambda_2^i))$ to $\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) : b \in A/(\lambda_1^i\lambda_2^i)\}$. Therefore, the closed group $G_{\lambda_1\lambda_2} = \rho_{\phi,\lambda_1\lambda_2}(\mathrm{Gal}_F)$ contains a subgroup that is conjugate in $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ to $\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) : b \in A_{\lambda_1\lambda_2}\}$. We have $\det(\rho_{\phi,\lambda_1\lambda_2}(\mathrm{Gal}_F)) = A_{\lambda_1\lambda_2}^\times$ since $\det(\rho_\phi(\mathrm{Gal}_F)) = \widehat{A}^\times$.

We have verified the conditions of Theorem 3.1 for G and hence $G \supseteq [G, G] = [\mathrm{GL}_2(\widehat{A}), \mathrm{GL}_2(\widehat{A})]$. □

Lemmas 11.4 and 11.7 now imply that $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

References

[Bre16] Florian Breuer, *Explicit Drinfeld moduli schemes and Abhyankar's generalized iteration conjecture*, J. Number Theory **160** (2016), 432–450, DOI 10.1016/j.jnt.2015.08.021. MR3425215 ↑8.2

[Che24] Chien-Hua Chen, *Natural density of rank-2 Drinfeld modules with big Galois image* (2024), arXiv 2403.15109, primary class math.NT ↑1.6

[Che22a] ———, *Exceptional cases of adelic surjectivity for Drinfeld modules of rank 2*, Acta Arith. **202** (2022), no. 4, 361–377, DOI 10.4064/aa210405-23-11. MR4415990 ↑iii, 1.6

[Che22b] ———, *Surjectivity of the adelic Galois representation associated to a Drinfeld module of rank 3*, J. Number Theory **237** (2022), 99–123, DOI 10.1016/j.jnt.2020.06.004. MR4410021 ↑1.6

[Con] Keith Conrad, *Galois groups of cubics and quartics in all characteristics.* (unpublished expository article) https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquarticallchar.pdf. ↑10.2

[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

[Dri74] V. G. Drinfel′d, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656. ↑1.1, 4.2

[Ent21] Alexei Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, Int. Math. Res. Not. IMRN **14** (2021), 10409–10441, DOI 10.1093/imrn/rnz120. MR4285725 ↑8.1

[Gek16] Ernst-Ulrich Gekeler, *The Galois image of twisted Carlitz modules*, J. Number Theory **163** (2016), 316–330, DOI 10.1016/j.jnt.2015.11.021. MR3459573 ↑6.1

[Gek08] ———, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721. ↑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, 5, 7

[Gro66] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. **28** (1966), 255. MR217086 ↑8.1

[Ham93] Yoshinori Hamahata, *Tensor products of Drinfeld modules and v-adic representations*, Manuscripta Math. **79** (1993), no. 3-4, 307–327, DOI 10.1007/BF02568348. MR1223025 ↑6.2, 10.3, 11.1

[Hay74] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91. ↑10.3, 11.1

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570, DOI 10.1090/S0002-9947-09-04804-1. MR2563740 ↑1.6.1

[Leh09] Thomas Lehmkuhl, *Compactification of the Drinfeld modular surfaces*, Mem. Amer. Math. Soc. **197** (2009), no. 921, xii+94. ↑4.2

[PR09a] Richard Pink and Egon Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), no. 4, 882–907. ↑1.1, 2, 2.1, 2.3

[PR09b] ———, *Image of the group ring of the Galois representation associated to Drinfeld modules*, J. Number Theory **129** (2009), no. 4, 866–881. ↑4.1, 4.1

[Ray24a] Anwesh Ray, *The T-adic Galois representation is surjective for a positive density of Drinfeld modules*, Res. Number Theory **10** (2024), no. 3, Paper No. 56, 12, DOI 10.1007/s40993-024-00541-6. MR4755197 ↑1.6

[Ray24b] ———, *Galois representations are surjective for almost all Drinfeld modules* (2024), arXiv 2407.14264, primary class math.NT ↑1.6

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804, DOI 10.2307/2373815. MR457455 ↑3.1, 3.1, 3.1, 10.3

[Ros03] Michael Rosen, *Formal Drinfeld modules*, J. Number Theory **103** (2003), no. 2, 234–256. ↑4, 4.2

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1.1, 1.6.1

[Ser77] ———, *Linear representations of finite groups*, Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott. MR450380 ↑2

[Ser03] ———, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440 (electronic). ↑8.1

[Wil09] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009. MR2562037 ↑2.1

[Zyw11] David Zywina, *Drinfeld modules with maximal Galois action on their torsion points* (2011), arXiv 1110.4365, primary class math.NT ↑1.6, 1.6.1

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA

Email address: `zywina@math.cornell.edu`