Journal of Number Theory 129 (2009) 882–907

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Adelic openness for Drinfeld modules in generic characteristic

Richard Pink *, Egon Rütsche

Department of Mathematics, ETH Zürich, CH-8092 Zürich, Switzerland

ARTICLE INFO

Article history:
Received 29 February 2008
Revised 11 October 2008
Available online 19 January 2009
Communicated by G. Böckle

MSC:
11G09
11R58

Keywords:
Drinfeld modules
Torsion points
Galois representations

ABSTRACT

Let φ be a Drinfeld A-module of arbitrary rank and generic characteristic over a finitely generated field K. If the endomorphism ring of φ over an algebraic closure of K is equal to A, we prove that the image of the adelic Galois representation associated to φ is open.

0. Introduction

In [21] Serre proved that the image of the adelic representation associated to an elliptic curve over a number field without potential complex multiplication is open. The aim of this paper is to prove an analogue for Drinfeld modules of generic characteristic.

Let $\mathbb{F}_q$ be a finite field with q elements and of characteristic p. Let F be a finitely generated field of transcendence degree 1 over $\mathbb{F}_q$. Let A be the ring of elements of F which are regular outside a fixed place ∞ of F. Let K be a finitely generated field extension of F. Denote by K^{sep} the separable closure of K inside a fixed algebraic closure $\bar{K}$ and by $\mathrm{G}_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ the absolute Galois group of K. Let

$$\varphi : A \to K\{\tau\}, \quad a \mapsto \varphi_a$$

* Corresponding author.
E-mail addresses: pink@math.ethz.ch (R. Pink), egon.ruetsche@alumni.ethz.ch (E. Rütsche).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.12.002

be a Drinfeld A-module over K of rank r. Thus φ is of generic characteristic. (For the general theory of Drinfeld modules see for example Drinfeld [6], Deligne and Husemöller [5], Hayes [10] or Goss [9, Chapter 4].) For any non-zero ideal $\mathfrak{a}$ of A, the $\mathfrak{a}$-torsion

$$\varphi[\mathfrak{a}] := \bigcap_{a\in\mathfrak{a}} \operatorname{Ker}(\varphi_a : \mathbb{G}_{a,K} \to \mathbb{G}_{a,K})$$

is a finite étale subgroup scheme of $\mathbb{G}_{a,K}$. By Lang's theorem, its geometric points

$$\varphi[\mathfrak{a}]\bigl(K^{\mathrm{sep}}\bigr) = \bigl\{x \in K^{\mathrm{sep}} \bigm| \forall a \in \mathfrak{a}\colon\ \varphi_a(x) = 0\bigr\}$$

form a free $A/\mathfrak{a}$-module of rank r. For any non-zero prime $\mathfrak{p}$ of A, the $\mathfrak{p}$-adic Tate module

$$T_{\mathfrak{p}}(\varphi) := \varprojlim \varphi\bigl[\mathfrak{p}^n\bigr]\bigl(K^{\mathrm{sep}}\bigr)$$

of φ is a free $A_{\mathfrak{p}}$-module of rank r, where $A_{\mathfrak{p}}$ denotes the completion of A at $\mathfrak{p}$. It carries a continuous Galois representation

$$\rho_{\mathfrak{p}} : \mathrm{G}_K \to \mathrm{Aut}_{A_{\mathfrak{p}}}\bigl(T_{\mathfrak{p}}(\varphi)\bigr) \cong \mathrm{GL}_r(A_{\mathfrak{p}}).$$

Denote by $\mathbb{A}_F^f$ be the ring of finite adeles of F, and consider the adelic representation

$$\rho_{\mathrm{ad}} : \mathrm{G}_K \to \prod_{\mathfrak{p}\neq\infty} \mathrm{GL}_r(A_{\mathfrak{p}}) \subset \mathrm{GL}_r\bigl(\mathbb{A}_F^f\bigr).$$

Our main result is the following

Theorem 0.1 *(Adelic openness in generic characteristic). Let φ be a Drinfeld A-module of rank r over a finitely generated field K of generic characteristic. Assume that* $\mathrm{End}_{\bar{K}}(\varphi) = A$. *Then the image of the adelic representation*

$$\rho_{\mathrm{ad}} : \mathrm{G}_K \to \mathrm{GL}_r\bigl(\mathbb{A}_F^f\bigr)$$

is open.

When φ cannot be defined over a finite extension of F, this has already been proven in [4, Theorem 3] by different methods.

We also generalize the result to Drinfeld modules with arbitrary endomorphism ring $\mathrm{End}_{\bar{K}}(\varphi)$. To obtain a convenient result, we assume that all endomorphisms of φ are defined over K. Since the endomorphisms act on the Tate module and commute with the Galois representation, the image of G_K then lies in the centralizer $\mathrm{Cent}_{\mathrm{GL}_r(A_{\mathfrak{p}})}(\mathrm{End}_{\bar{K}}(\varphi))$. By exactly the same argument as in [13], Theorem 0.1 implies the following

Theorem 0.2. *Let φ be a Drinfeld A-module of rank r over a finitely generated field K of generic characteristic. Assume that* $\mathrm{End}_{\bar{K}}(\varphi) = \mathrm{End}_K(\varphi)$. *Then the image of the homomorphism*

$$\rho_{\mathrm{ad}} : \mathrm{G}_K \to \prod_{\mathfrak{p}} \mathrm{Cent}_{\mathrm{GL}_r(A_{\mathfrak{p}})}\bigl(\mathrm{End}_{\bar{K}}(\varphi)\bigr)$$

is open.

The methods used to establish these results are modeled to a great extent on the methods developed by Serre [19,21–23] to prove the corresponding results for elliptic curves and certain abelian varieties.

The article has five parts and an appendix. In Section 1 we list some known results on Drinfeld modules. Section 2 contains some preparatory results on matrix groups and fibers of algebraic morphisms. In Section 3 we prove that the residual representation is surjective for almost all primes $\mathfrak{p}$ of A in the case that $\mathrm{End}_{\bar{K}}(\varphi) = A$ and K is a finite extension of F. In Section 4 we prove Theorem 0.1 in the case that K is a finite extension of F. Section 5 contains a specialization result and uses it to prove the general case of Theorem 0.1. Appendix A contains two remarks on the article by Gardeyn [8]. We point out two gaps in that paper and show how to close them. The above notations and assumptions will remain in force throughout the article.

The material in this article was part of the doctoral thesis of the second author [18].

1. Known results on Drinfeld modules

The first stated result was proved independently by Taguchi [24,25] and Tamagawa [26].

Theorem 1.1 *(Tate conjecture for Drinfeld modules). Let φ_1 and φ_2 be two Drinfeld A-modules over K. Then for all primes $\mathfrak{p}$ of A the natural map*

$$\mathrm{Hom}_K(\varphi_1, \varphi_2) \otimes_A A_{\mathfrak{p}} \to \mathrm{Hom}_{A_{\mathfrak{p}}[\mathrm{G}_K]}\big(T_{\mathfrak{p}}(\varphi_1), T_{\mathfrak{p}}(\varphi_2)\big)$$

is an isomorphism.

The next result was proved by the first author [13].

Theorem 1.2. *Assume that* $\mathrm{End}_{\bar{K}}(\varphi) = A$. *Then for any finite set Λ of primes of A the image of the homomorphism*

$$\mathrm{G}_K \to \prod_{\mathfrak{p}\in\Lambda} \mathrm{GL}_r(A_{\mathfrak{p}})$$

is open.

Furthermore, the reduction modulo $\mathfrak{p}$ of $\rho_{\mathfrak{p}}$ is the continuous Galois representation on the module of $\mathfrak{p}$-torsion

$$\bar{\rho}_{\mathfrak{p}} : \mathrm{G}_K \to \mathrm{Aut}_{\kappa_{\mathfrak{p}}}\big(\varphi[\mathfrak{p}]\big(K^{\mathrm{sep}}\big)\big) \cong \mathrm{GL}_r(\kappa_{\mathfrak{p}})$$

over the residue field $\kappa_{\mathfrak{p}} := A/\mathfrak{p}$. We call it the residual representation at $\mathfrak{p}$. In [16] we proved

Theorem 1.3 *(Absolute irreducibility of the residual representation). Assume that* $\mathrm{End}_K(\varphi) = A$. *Then the residual representation*

$$\bar{\rho}_{\mathfrak{p}} : \mathrm{G}_K \to \mathrm{GL}_r(\kappa_{\mathfrak{p}})$$

is absolutely irreducible for almost all primes $\mathfrak{p}$ of A.

2. Preparatory results on algebraic groups

Proposition 2.1. *Let n be any natural number, let k be a field with at least* 4 *elements, and let H be an additive subgroup of the matrix ring* $\mathrm{M}_n(k)$*. Assume that H is invariant under conjugation by* $\mathrm{GL}_n(k)$*. Then either H is contained in the group of scalar matrices or H contains the group of matrices of trace* 0*.*

Proof. Let $T := \mathbb{G}_m^n$ denote the full diagonal torus. We identify its character group with $\mathbb{Z}^n$ by means of the standard basis $e_1, \ldots, e_n$. The torus T acts on $\mathrm{M}_n(k)$ by conjugation, and its weights are $e_i - e_j$ for all $i \neq j$ with multiplicity 1 and 0 with multiplicity n. The weight space W_0 of weight 0 is the group of diagonal matrices, and the weight space $W_{i,j}$ of weight $e_i - e_j$ is the group of matrices with all entries zero except, possibly, in the position (i, j). We thus can decompose $\mathrm{M}_n(k)$ as

$$\mathrm{M}_n(k) = W_0 \oplus \bigoplus_{i,j} W_{i,j}.$$

Since the multiplicative group k^* has at least 3 elements, any two distinct weights of the form $e_i - e_j$ remain distinct and different from 0 upon restriction to $T(k)$. Therefore H can be decomposed as

$$H = (H \cap W_0) \oplus \bigoplus_{i,j} (H \cap W_{i,j}).$$

Each $W_{i,j}$ is a k-vector space of dimension 1, and $T(k)$ acts on it through a surjective homomorphism $T(k) \twoheadrightarrow k^*$. Thus $H \cap W_{i,j}$ is either 0 or equal to $W_{i,j}$. The permutation matrices in $\mathrm{GL}_n(k)$ form a subgroup isomorphic to S_n which permutes the weights $e_i - e_j$ transitively. Since H is invariant under conjugation by $\mathrm{GL}_n(k)$, we find that either all $H \cap W_{i,j} = 0$ or all $H \cap W_{i,j} = W_{i,j}$. In other words, either H is contained in the group of diagonal matrices or H contains the sum of all $W_{i,j}$, which is the group of matrices with diagonal 0.

If H is contained in the group of diagonal matrices, take any element h of H and denote its diagonal entries by $h_1, \ldots, h_n$. Let $i \neq j$ and let $u \in \mathrm{GL}_n(k)$ be the matrix with entry 1 on the diagonal and in the position (i, j) and 0 elsewhere. Then uhu^{-1} has entry $h_i - h_j$ in the position (i, j). But this entry has to be 0 because $uhu^{-1} \in H$, and hence $h_i = h_j$. This can be done for any pair (i, j), which shows that H is contained in the group of scalar matrices.

If H contains the group of matrices with diagonal 0, we consider the trace form $\mathrm{M}_n(k) \times \mathrm{M}_n(k) \to k$, $(A, B) \mapsto \langle A, B\rangle := \mathrm{tr}(AB)$, which is a perfect pairing invariant under $\mathrm{GL}_n(k)$. The orthogonal complement $H^\perp$ of H is again a $\mathrm{GL}_n(k)$-invariant subgroup, and since the inclusion for orthogonal complements is reversed, it is contained in the group of diagonal matrices. The arguments in the other case show that $H^\perp$ is contained in the group of scalar matrices. Taking orthogonal complements again, we deduce that H contains the matrices of trace 0, as desired. □

Proposition 2.2. *Let n be any natural number, let k be a finite field, and let H be a normal subgroup of* $\mathrm{GL}_n(k)$ *containing a non-scalar matrix. Assume that* $(n, |k|)$ *is different from* $(2, 2)$ *and* $(2, 3)$*. Then we have*

$$\mathrm{SL}_n(k) \subset H.$$

Proof. For any non-scalar element $h \in \mathrm{GL}_n(k)$, there exists an element $g \in \mathrm{GL}_n(k)$ such that the commutator $ghg^{-1}h^{-1}$ is again non-scalar. Thus H contains a non-scalar element of $\mathrm{SL}_n(k)$. In particular, we have $n \geqslant 2$. Let Z denote the center of $\mathrm{SL}_n(k)$. Under the given assumptions $\mathrm{SL}_n(k)/Z$ is simple by [12], and $\mathrm{SL}_n(k)$ is perfect by [3, Corollary 4.3] or [17]. Since $H \cap \mathrm{SL}_n(k)$ is a normal subgroup of $\mathrm{SL}_n(k)$ that is not contained in Z, it follows that $H \cap \mathrm{SL}_n(k) = \mathrm{SL}_n(k)$. □

Proposition 2.3. *Let k be a finite field, let n be any natural number, and let H be a subgroup of $\mathrm{GL}_n(k)$ of index c. Assume that $(n, |k|)$ is different from $(2, 2)$ and $(2, 3)$ and that $c! < |\mathrm{PGL}_n(k)|$. Then we have*

$$\mathrm{SL}_n(k) \subset H.$$

Proof. Abbreviate $G := \mathrm{GL}_n(k)$. Then the action of G on the set of right cosets $\{gH \mid g \in G\}$ corresponds to a homomorphism from G to the symmetric group S_c on c elements. Thus its kernel N is a normal subgroup of G of index at most $c!$ and contained in H. The assumption implies that N has non-trivial image in $\mathrm{PGL}_n(k)$, and thus N contains a non-scalar element. By Proposition 2.2, we find that $\mathrm{SL}_n(k) \subset N \subset H$, as desired. □

Proposition 2.4. *Let X be an irreducible algebraic variety over a field L, let G be an irreducible algebraic group over L, and let $f : X \to G$ be a dominant morphism. Set $d := \dim(G)$ and $e := \dim(X)$. Then for all $n \geqslant d$ the fibers of the morphism*

$$f^n : X^n \to G, \quad (x_1, \ldots, x_n) \mapsto f(x_1) \cdot \cdots \cdot f(x_n)$$

have dimension at most $ne - d$.

Proof. Since f is dominant, there exists an open dense subset U of X such that all fibers of $f|_U$ have dimension $e - d$. We first consider the restriction of f^n to $X^{i-1} \times U \times X^{n-i}$ for any $1 \leqslant i \leqslant n$. We can write this restriction as the composite of morphisms

$$X^{i-1} \times U \times X^{n-i} \xrightarrow{\alpha} X^{i-1} \times G \times X^{n-i} \xrightarrow{\beta} X^{i-1} \times G \times X^{n-i} \xrightarrow{\gamma} G$$

where

$$\begin{aligned} \alpha(x_1, \ldots, x_n) &= \big(x_1, \ldots, x_{i-1}, f(x_i), x_{i+1}, \ldots, x_n\big), \\ \beta(x_1, \ldots, x_{i-1}, g, x_{i+1}, \ldots, x_n) &= \big(x_1, \ldots, x_{i-1}, f(x_1) \ldots f(x_{i-1}) g f(x_{i+1}) \ldots f(x_n), x_{i+1}, \ldots, x_n\big), \\ \gamma(x_1, \ldots, x_{i-1}, g, x_{i+1}, \ldots, x_n) &= g. \end{aligned}$$

Here α has fiber dimension $e - d$, the morphism β is an isomorphism, and γ has fiber dimension $(n-1)e$. Thus all fibers of $f^n|_{X^i \times U \times X^{n-i-1}}$ have dimension $\leqslant e - d + (n-1)e = ne - d$. Varying i, we find that all fibers of $f^n|_{X^n \setminus (X \setminus U)^n}$ have dimension $\leqslant ne - d$. On the other hand, all fibers of $f^n|_{(X \setminus U)^n}$ have dimension $\leqslant \dim((X \setminus U)^n) \leqslant n(e-1)$. Since $n \geqslant d$, this is also $\leqslant ne - d$, and the result follows. □

Proposition 2.5. *Let X and Y be schemes of finite type over $\operatorname{Spec} \mathbb{Z}$, and let $f : X \to Y$ be a morphism of finite type. Then there exists a constant c, depending only on X, Y and f, such that for any finite field k and any $y \in Y(k)$, we have*

$$\big|f^{-1}(y)(k)\big| \leqslant c|k|^{\dim(f^{-1}(y))}.$$

Proof. We use noetherian induction on Y, the case $Y = \emptyset$ being vacuous. Otherwise, since X and Y have only finitely many irreducible components, we can assume that both are irreducible. After replacing them by open charts we may also assume that they are affine. For points $y \notin f(X)$, there is nothing to prove; hence after replacing Y by the Zariski closure of $f(X)$ we can assume that f is dominant. Set $d := \dim(X)$ and $e := \dim(Y)$. Then after replacing X and Y by open subschemes we may assume that all fibers of f have dimension $d - e$.

Let η denote the generic point of Y. By Noether normalization, there exists a finite surjective morphism $f^{-1}(\eta) \to \mathbb{A}^{d-e} \times \eta$, say of degree n. This morphism extends to a morphism $f^{-1}(V) \to$

$\mathbb{A}^{d-e} \times V$ for an open neighborhood V of η in Y, which is still finite of degree n if V is sufficiently small. Then for all $y \in V(k)$, we find that

$$\left|f^{-1}(y)(k)\right| \leqslant n \cdot \left|\mathbb{A}^{d-e}(k)\right| = n|k|^{d-e},$$

and the proposition follows. □

3. Surjectivity of the residual representation

Throughout this section, we assume that K is a finite extension of F and that $\mathrm{End}_{\bar{K}}(\varphi) = A$. For any prime $\mathfrak{p}$ of A, we let $\Gamma_{\mathfrak{p}}$ denote the image of the residual representation

$$\bar{\rho}_{\mathfrak{p}} : \mathrm{G}_K \to \mathrm{GL}_r(\kappa_{\mathfrak{p}}).$$

We prove the following result.

Proposition 3.1. *In the above situation, we have $\Gamma_{\mathfrak{p}} = \mathrm{GL}_r(\kappa_{\mathfrak{p}})$ for almost all primes $\mathfrak{p}$ of A.*

Sketch of the proof. The main ingredients are the absolute irreducibility of the residual representation and the image of inertia at places above $\mathfrak{p}$. By standard methods we can identify the image of the tame inertia group with the multiplicative group of some finite extension k_n of $\kappa_{\mathfrak{p}}$. This image is the group of $\kappa_{\mathfrak{p}}$-valued points of a certain connected algebraic group, called the torus of inertia. The algebraic subgroup of $\mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$ that is generated by $\Gamma_{\mathfrak{p}}$ and the tori of inertia at all places above $\mathfrak{p}$ constitutes an algebraic group enveloping $\Gamma_{\mathfrak{p}}$ in a natural way. It plays a role analogous to that of the Zariski closure of the image of Galois in the whole $\mathfrak{p}$-adic representation over $F_{\mathfrak{p}}$ (compare [13]). The main intermediate step is to establish that this subgroup is equal to $\mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$. The rest is algebraic group theory.

Reduction steps. It is enough to prove Proposition 3.1 for any open subgroup of G_K. This allows us to replace K by any finite extension. In particular we may assume that

(a) φ has semistable reduction everywhere.

Next, recall that at any place ∞' of K above ∞, the Drinfeld module is uniformized by a lattice on which the decomposition group $\mathrm{D}_{\infty'}$ acts through a finite quotient. Similarly, for any place $\mathfrak{Q}$ of K where φ has bad reduction, the Tate uniformization involves a lattice on which the decomposition group $\mathrm{D}_{\mathfrak{Q}}$ acts through a finite quotient. Thus, after replacing K by a finite extension, we may assume that

(b) for any place ∞' above ∞, the decomposition group $\mathrm{D}_{\infty'}$ acts trivially on the associated lattice, and
(c) for any place $\mathfrak{Q}$ of bad reduction, the decomposition group $\mathrm{D}_{\mathfrak{Q}}$ acts trivially on the associated lattice.

We can also disregard any finite set of primes $\mathfrak{p}$. Thus by Theorem 1.3 we can restrict ourselves to primes $\mathfrak{p}$ for which

(d) the residual representation at $\mathfrak{p}$ is absolutely irreducible.

Furthermore, we can assume that

(e) all places $\mathfrak{P}$ of K above $\mathfrak{p}$ are unramified over $\mathfrak{p}$,
(f) φ has good reduction at all places above $\mathfrak{p}$, and
(g) $q_{\mathfrak{p}} := |\kappa_{\mathfrak{p}}| \geqslant 4$.

Torus of inertia. Consider any place $\mathfrak{P}$ of K above $\mathfrak{p}$ and a place $\bar{\mathfrak{P}}$ of $\bar{K}$ above $\mathfrak{P}$, with the respective residue fields $k_{\mathfrak{P}} \subset k_{\bar{\mathfrak{P}}}$. Then the inertia group $\mathrm{I}_{\mathfrak{P}}$ sits in an exact sequence

$$1 \to \mathrm{I}_{\mathfrak{P}}^p \to \mathrm{I}_{\mathfrak{P}} \to \mathrm{I}_{\mathfrak{P}}^t \to 1$$

where $\mathrm{I}_{\mathfrak{P}}^p$ and $\mathrm{I}_{\mathfrak{P}}^t$ denote the wild inertia group and tame inertia group, respectively. Fix a section $\mathrm{I}_{\mathfrak{P}}^t \to \mathrm{I}_{\mathfrak{P}}$. By (f) above, the Drinfeld module φ has good reduction at $\mathfrak{P}$. The connected-étale decomposition of the finite flat group scheme $\varphi[\mathfrak{p}]$ over the discrete valuation ring $\mathscr{O}_{K_{\mathfrak{P}}}$ yields an exact sequence

$$0 \to \varphi[\mathfrak{p}]^0\big(K^{\mathrm{sep}}\big) \to \varphi[\mathfrak{p}]\big(K^{\mathrm{sep}}\big) \to \varphi[\mathfrak{p}]^{et}\big(K^{\mathrm{sep}}\big) \to 0,$$

where $\mathrm{I}_{\mathfrak{P}}$ acts trivially on $\varphi[\mathfrak{p}]^{et}(K^{\mathrm{sep}})$. Denote by $h_{\mathfrak{P}}$ the height of the reduced Drinfeld module, and set $n := q_{\mathfrak{p}}^{h_{\mathfrak{P}}}$. Let k_n denote the subfield of $k_{\bar{\mathfrak{P}}}$ with n elements. By [16, Proposition 2.7] and (e) above we have up to conjugation

$$\bar{\rho}_{\mathfrak{p}}(\mathrm{I}_{\mathfrak{P}}) = \left(\begin{array}{c|c} k_n^* & \bar{\rho}_{\mathfrak{p}}(\mathrm{I}_{\mathfrak{P}}^p) \\ \hline 0 & 1 \end{array}\right) \subset \Gamma_{\mathfrak{p}} \tag{3.2}$$

and

$$\bar{\rho}_{\mathfrak{p}}\big(\mathrm{I}_{\mathfrak{P}}^t\big) = \left(\begin{array}{c|c} k_n^* & 0 \\ \hline 0 & 1 \end{array}\right) \subset \Gamma_{\mathfrak{p}}, \tag{3.3}$$

written in block matrices of size $h_{\mathfrak{P}}$, $r - h_{\mathfrak{P}}$. Since $k_n^* \neq \{1\}$, the centralizer of $\bar{\rho}_{\mathfrak{p}}(\mathrm{I}_{\mathfrak{P}}^t)$ in $\mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$ is

$$\left(\begin{array}{c|c} T_{\mathfrak{P}} & 0 \\ \hline 0 & \mathrm{GL}_{(r-h_{\mathfrak{P}}),\kappa_{\mathfrak{p}}} \end{array}\right)$$

for a torus $T_{\mathfrak{P}}$ over $\kappa_{\mathfrak{p}}$ with $T_{\mathfrak{P}}(\kappa_{\mathfrak{p}}) = k_n^*$. The torus $T_{\mathfrak{P}}$ is the Weil restriction $\mathrm{Res}_{\kappa_{\mathfrak{p}}}^{k_n} \mathbb{G}_{m,k_n}$ and thus of dimension $h_{\mathfrak{P}}$. Its $\Gamma_{\mathfrak{p}}$-conjugacy class in $\mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$ is independent of $\bar{\mathfrak{P}}$.

Algebraic group envelope of $\Gamma_{\mathfrak{p}}$. Let $H_{\mathfrak{p}}^{\circ}$ denote the connected algebraic subgroup of $\mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$ generated by all $\Gamma_{\mathfrak{p}}$-conjugates of $T_{\mathfrak{P}}$ for all $\mathfrak{P} \mid \mathfrak{p}$ (see [11, Proposition 7.5]). By construction it is normalized by the finite group $\Gamma_{\mathfrak{p}}$; hence $H_{\mathfrak{p}}^{\circ}$ and $\Gamma_{\mathfrak{p}}$ together generate an algebraic subgroup $H_{\mathfrak{p}}$ of $\mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$ with identity component $H_{\mathfrak{p}}^{\circ}$.

Eventually we want to show that $H_{\mathfrak{p}}^{\circ} = H_{\mathfrak{p}} = \mathrm{GL}_{r,\kappa_{\mathfrak{p}}}$. To begin with, we note that $H_{\mathfrak{p}}$ acts absolutely irreducibly on $\kappa_{\mathfrak{p}}^r$ because $\Gamma_{\mathfrak{p}}$ does so. Fix a place $\bar{\mathfrak{p}}$ of $\bar{F}$ above $\mathfrak{p}$ with residue field $\kappa_{\bar{\mathfrak{p}}}$. Then $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}$ acts irreducibly on $\kappa_{\bar{\mathfrak{p}}}^r$.

Lemma 3.4. *There exist a natural number $s_{\mathfrak{p}}$ and a decomposition*

$$\kappa_{\bar{\mathfrak{p}}}^r = W_1 \oplus \cdots \oplus W_{s_{\mathfrak{p}}}$$

into irreducible $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^{\circ}$-subrepresentations which are conjugate under $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}$.

Proof. Abbreviate $V := \kappa_{\bar{\mathfrak{p}}}^r$, and let W be a non-trivial $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$-invariant subspace of V of minimal dimension. Since $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$ is normalized by $\Gamma_\mathfrak{p}$, the subspace γW is also $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$-invariant for all $\gamma \in \Gamma_\mathfrak{p}$. The subspace $\sum_{\gamma\in\Gamma_\mathfrak{p}} \gamma W$ is $\Gamma_\mathfrak{p}$-invariant and therefore, by the irreducibility of V, equal to V. Since each γW is irreducible over $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$, a suitable subcollection will do. □

We fix a decomposition of $\kappa_{\bar{\mathfrak{p}}}^r$ as in Lemma 3.4. Then the algebraic subgroup of $\mathrm{GL}_{r,\kappa_{\bar{\mathfrak{p}}}}$ which normalizes each summand is isomorphic to $\mathrm{GL}_{t_\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^{s_\mathfrak{p}}$, where $t_\mathfrak{p}$ is the common dimension of the W_i. The algebraic subgroup of $\mathrm{GL}_{r,\kappa_{\bar{\mathfrak{p}}}}$ which maps each summand to some, possibly other, summand is isomorphic to $\mathrm{GL}_{t_\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^{s_\mathfrak{p}} \rtimes S_{s_\mathfrak{p}}$.

Lemma 3.5. *We have*

$$H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}} \subset \mathrm{GL}_{t_\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^{s_\mathfrak{p}} \rtimes S_{s_\mathfrak{p}}.$$

Proof. By Lemma 3.4 we have $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ \subset \mathrm{GL}_{t_\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^{s_\mathfrak{p}}$. Take any place $\mathfrak{P}$ above $\mathfrak{p}$. By the construction of $T_\mathfrak{P}$ there exists a basis of $\kappa_{\bar{\mathfrak{p}}}^r$ with respect to which

$$T_{\mathfrak{P},\kappa_{\bar{\mathfrak{p}}}} = \left(\begin{array}{ccc|ccc} * & & & & & \\ & \ddots & & & & \\ & & * & & & \\ \hline & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{array}\right) \cong \mathbb{G}_{m,\kappa_{\bar{\mathfrak{p}}}}^{h_\mathfrak{P}},$$

where the upper left block consists of diagonal $h_\mathfrak{P} \times h_\mathfrak{P}$-matrices. Consider the cocharacter

$$\mu_1 : \mathbb{G}_{m,\kappa_{\bar{\mathfrak{p}}}} \to T_{\mathfrak{P},\kappa_{\bar{\mathfrak{p}}}}, \quad t \mapsto \begin{pmatrix} t & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix},$$

which on $\kappa_{\bar{\mathfrak{p}}}^r$ has weight 1 with multiplicity 1 and weight 0 with multiplicity $r-1$. Without loss of generality we can assume that μ_1 has its non-trivial weight on W_1 and weight zero on all other W_i. Since $T_{\mathfrak{P},\kappa_{\bar{\mathfrak{p}}}} \subset H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$, it follows that, as an $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$-representation, the space W_1 is not isomorphic to W_i for any $i \neq 1$. By conjugation, we deduce that any two of the W_i are non-isomorphic $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$-representations. This shows that the decomposition in Lemma 3.4 is in fact the isotypical decomposition of $\kappa_{\bar{\mathfrak{p}}}^r$ under $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^\circ$. It is thus normalized by $H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}$, and the result follows. □

Using Lemma 3.5, we define $\alpha_\mathfrak{p}$ as the composite of the following homomorphisms

$$\mathrm{G}_K \to H_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}} \subset \mathrm{GL}_{t_\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}^{s_\mathfrak{p}} \rtimes S_{s_\mathfrak{p}} \twoheadrightarrow S_{s_\mathfrak{p}}.$$

Lemma 3.6. *The homomorphism $\alpha_\mathfrak{p}$ is unramified at all places of K lying above $\mathfrak{p}$.*

Proof. Consider any place $\mathfrak{P}$ of K above $\mathfrak{p}$. By (3.3) we have $\bar{\rho}_\mathfrak{p}(\mathrm{I}_\mathfrak{P}^t) = T_\mathfrak{P}(\kappa_\mathfrak{p}) \subset H_\mathfrak{p}^\circ(\kappa_\mathfrak{p})$; hence $\alpha_\mathfrak{p}(\mathrm{I}_\mathfrak{P}^t) = 1$. This implies that $\alpha_\mathfrak{p}(\mathrm{I}_\mathfrak{P})$ is a quotient of the group of coinvariants of $\bar{\rho}_\mathfrak{p}(\mathrm{I}_\mathfrak{P}^p)$ under $\bar{\rho}_\mathfrak{p}(\mathrm{I}_\mathfrak{P}^t)$. The description (3.2) shows that $\bar{\rho}_\mathfrak{p}(\mathrm{I}_\mathfrak{P}^p)$ is a k_n-vector space on which $\bar{\rho}_\mathfrak{p}(\mathrm{I}_\mathfrak{P}^t)$ acts through multiplication by k_n^*. Since $k_n^* \neq \{1\}$, that group of coinvariants is zero. This implies that $\alpha_\mathfrak{p}(\mathrm{I}_\mathfrak{P}) = 1$, and so $\alpha_\mathfrak{p}$ is unramified at $\mathfrak{P}$. □

Lemma 3.7. *For almost all primes $\mathfrak{p}$ of A the homomorphism $\alpha_\mathfrak{p}$ is unramified at all places of K where φ has bad reduction.*

Proof. Since there are only finitely many places $\mathfrak{Q}$ of K where φ has bad reduction, it suffices to prove the lemma for one of them. By (a) above, the Drinfeld module φ has semistable reduction at $\mathfrak{Q}$. Let $(\psi, \Lambda_\mathfrak{Q})$ be its Tate uniformization $\mathfrak{Q}$. Then ψ is a Drinfeld A-module over $K_\mathfrak{Q}$ of some rank $r' < r$ with good reduction at $\mathfrak{Q}$, and $\Lambda_\mathfrak{Q}$ is, via ψ, an A-lattice in $K_\mathfrak{Q}^{\mathrm{sep}}$ of rank $r - r'$. For any prime $\mathfrak{p}$ of A with $\mathfrak{p} \nmid \mathfrak{Q}$, we have an exact sequence

$$0 \to \psi[\mathfrak{p}]\big(K^{\mathrm{sep}}\big) \to \varphi[\mathfrak{p}]\big(K^{\mathrm{sep}}\big) \to \Lambda_\mathfrak{Q}/\mathfrak{p}\Lambda_\mathfrak{Q} \to 0$$

of representations of the decomposition group $\mathrm{D}_\mathfrak{Q}$. By good reduction the inertia group $\mathrm{I}_\mathfrak{Q}$ acts trivially on the first term, and by (c) it acts trivially on the third term. Therefore its image under $\bar{\rho}_\mathfrak{p}$ lies in a subgroup of the form

$$\left(\begin{array}{c|c} 1 & * \\ \hline 0 & 1 \end{array}\right) \cong \mathrm{Hom}\big(\Lambda_\mathfrak{Q}/\mathfrak{p}\Lambda_\mathfrak{Q}, \psi[\mathfrak{p}]\big(K^{\mathrm{sep}}\big)\big).$$

On the other hand, since $s_\mathfrak{p} \leqslant r$, every element of $S_{s_\mathfrak{p}}$ has order dividing $r!$. In particular, we have $\alpha_\mathfrak{p}(\mathrm{Frob}_\mathfrak{Q}^{r!}) = 1$. Therefore the restriction of $\alpha_\mathfrak{p}$ to $\mathrm{I}_\mathfrak{Q}$ factors through the group of coinvariants

$$\mathrm{Hom}\big(\Lambda_\mathfrak{Q}/\mathfrak{p}\Lambda_\mathfrak{Q}, \psi[\mathfrak{p}]\big(K^{\mathrm{sep}}\big)\big)_{\mathrm{Frob}_\mathfrak{Q}^{r!}}.$$

It suffices to prove that this group is zero for almost all $\mathfrak{p}$. Since $\mathrm{Frob}_\mathfrak{Q}^{r!}$ acts trivially on $\Lambda_\mathfrak{Q}/\mathfrak{p}\Lambda_\mathfrak{Q}$ by (c), it suffices to prove that the group of coinvariants $\psi[\mathfrak{p}](K^{\mathrm{sep}})_{\mathrm{Frob}_\mathfrak{Q}^{r!}}$ vanishes.

Denote by $f_\mathfrak{Q}$ the characteristic polynomial of $\mathrm{Frob}_\mathfrak{Q}^{r!}$ on the Tate module of ψ at $\mathfrak{p}$, which has coefficients in A and is independent of $\mathfrak{p}$. By purity, every eigenvalue of $\mathrm{Frob}_\mathfrak{Q}$ has valuation < 0 at ∞. Thus 1 is not an eigenvalue of $\mathrm{Frob}_\mathfrak{Q}^{r!}$, and so $f_\mathfrak{Q}(1)$ is a non-zero element of A. For all $\mathfrak{p} \nmid f_\mathfrak{Q}(1)$ no eigenvalue of $\mathrm{Frob}_\mathfrak{Q}^{r!}$ is congruent to 1 modulo a place lying above $\mathfrak{p}$; hence for these $\mathfrak{p}$ we have $\psi[\mathfrak{p}](K^{\mathrm{sep}})_{\mathrm{Frob}_\mathfrak{Q}^{r!}} = 0$, as desired. □

Lemma 3.8. *For almost all primes $\mathfrak{p}$ of A the homomorphism $\alpha_\mathfrak{p}$ is unramified everywhere and totally split at all places above ∞.*

Proof. For all places $\mathfrak{Q} \nmid \mathfrak{p}\infty$ where φ has good reduction, the inertia group at $\mathfrak{Q}$ acts trivially on $\varphi[\mathfrak{p}](K^{\mathrm{sep}})$. Therefore the homomorphism $\alpha_\mathfrak{p}$ is unramified at these places. By Lemma 3.6 it is unramified at all places $\mathfrak{Q} \mid \mathfrak{p}$. For places $\mathfrak{Q} \nmid \infty$ where φ has bad reduction, the assertion is Lemma 3.7. Finally, for places above ∞, the assertion follows from (b) above. □

Lemma 3.9. *For almost all primes $\mathfrak{p}$ of A we have $s_\mathfrak{p} = 1$.*

Proof. Let $\mathfrak{p}$ be any prime as in Lemma 3.8, and let $K^{(\mathfrak{p})}$ the field fixed by the kernel of $\alpha_\mathfrak{p}$. By Lemma 3.8 it is unramified over K. Moreover, its degree $[K^{(\mathfrak{p})}/K] \leqslant s_\mathfrak{p}! \leqslant r!$ is bounded independently of $\mathfrak{p}$. By Goss [9, Theorem 8.23.5], a function field analogue of the Hermite–Minkowski Theorem about unramified extensions, there are only finitely many possibilities for $K^{(\mathfrak{p})}$. Therefore their compositum K' is a finite extension of K such that $\alpha_\mathfrak{p}|_{\mathrm{G}_{K'}} : \mathrm{G}_{K'} \to S_{s_\mathfrak{p}}$ is trivial for almost all $\mathfrak{p}$. For these $\mathfrak{p}$ we find that

$$\bar{\rho}_\mathfrak{p}(\mathrm{G}_{K'}) \subset \mathrm{GL}_{t_\mathfrak{p}, \kappa_{\bar{\mathfrak{p}}}}^{s_\mathfrak{p}}.$$

If $s_\mathfrak{p} > 1$, this shows that $\varphi[\mathfrak{p}](K^{\mathrm{sep}})$ is not absolutely irreducible as a representation of $G_{K'}$. By Theorem 1.3, applied to φ considered as a Drinfeld A-module over K', this can only happen for finitely many $\mathfrak{p}$. Therefore $s_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$. □

Proposition 3.10. *For almost all primes $\mathfrak{p}$ of A we have*

$$H_\mathfrak{p}^\circ = H_\mathfrak{p} = \mathrm{GL}_{r,\kappa_\mathfrak{p}}.$$

Proof. Lemmas 3.4 and 3.9 imply that $H^\circ_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}}$ acts irreducibly on $\kappa_{\bar{\mathfrak{p}}}^r$ for almost all $\mathfrak{p}$. Moreover, as explained in the proof of Lemma 3.5, it possesses a cocharacter of weight 1 with multiplicity 1 and weight 0 with multiplicity $r-1$. By [13, Proposition A.3], these properties imply that $H^\circ_{\mathfrak{p},\kappa_{\bar{\mathfrak{p}}}} = \mathrm{GL}_{r,\kappa_{\bar{\mathfrak{p}}}}$. Therefore both inclusions $H^\circ_{\mathfrak{p},\kappa_\mathfrak{p}} \subset H_{\mathfrak{p},\kappa_\mathfrak{p}} \subset \mathrm{GL}_{r,\kappa_\mathfrak{p}}$ are equalities. □

Returning to the finite group $\Gamma_\mathfrak{p}$.

Lemma 3.11. *There exist a scheme Z of finite type over* $\mathrm{Spec}(\mathbb{Z})$ *and a closed subscheme $\mathscr{T} \subset \mathrm{GL}_r \times Z$ over Z, such that for almost all primes $\mathfrak{p}$ of A, any place $\mathfrak{P} \mid \mathfrak{p}$ of K, and any element $\gamma \in \Gamma_\mathfrak{p}$, there exists a point $z \in Z(\kappa_\mathfrak{p})$ such that $\mathscr{T}_z = \gamma T_\mathfrak{P} \gamma^{-1}$.*

Proof. Define

$$Z := \mathrm{GL}_r \times \left(\mathbb{A}^r\right)^{r-1}, \quad \text{and}$$

$$\mathscr{T} := \left\{(t, g, v_1, \ldots, v_{r-1}) \;\middle|\; tg = gt \text{ and } \forall i\colon\ tv_i = v_i\right\} \subset \mathrm{GL}_r \times Z.$$

Then Z is a scheme of finite type over $\mathrm{Spec}(\mathbb{Z})$, and $\mathscr{T}$ is a closed subscheme of $\mathrm{GL}_r \times Z$. Let $\mathfrak{p}$ satisfy (e), (f) and (g), and take any $\mathfrak{P} \mid \mathfrak{p}$ and $\gamma \in \Gamma_\mathfrak{p}$. Let t be a generator of $T_\mathfrak{P}(\kappa_\mathfrak{p}) = k_n^*$, and let $w_1, \ldots, w_{r-1} \in \kappa_\mathfrak{p}^r$ be generators of the space of invariants of $T_\mathfrak{P}$. Then

$$\mathrm{Cent}_{\mathrm{GL}_{r,\kappa_\mathfrak{p}}}(t) = \left(\begin{array}{c|c} T_\mathfrak{P} & 0 \\ \hline 0 & * \end{array}\right)$$

and

$$\mathrm{Stab}_{\mathrm{GL}_{r,\kappa_\mathfrak{p}}}(w_1) \cap \cdots \cap \mathrm{Stab}_{\mathrm{GL}_{r,\kappa_\mathfrak{p}}}(w_{r-1}) = \left(\begin{array}{c|c} T_\mathfrak{P} & 0 \\ \hline * & 1 \end{array}\right),$$

and their intersection is $T_\mathfrak{P}$. Conjugating by γ we deduce that the fiber $\mathscr{T}_z$ of $\mathscr{T}$ above $z = (\gamma t \gamma^{-1}, \gamma w_1, \ldots, \gamma w_{r-1})$ is $\gamma T_\mathfrak{P} \gamma^{-1}$. □

Lemma 3.12. *There exists a constant c depending only on r such that for almost all primes $\mathfrak{p}$ of A*

$$\left[\mathrm{GL}_r(\kappa_\mathfrak{p}) : \Gamma_\mathfrak{p}\right] \leqslant c.$$

Proof. Consider any prime $\mathfrak{p}$ as in Proposition 3.10. Then $\mathrm{GL}_{r,\kappa_\mathfrak{p}}$ is generated by the connected algebraic subgroups $\gamma T_\mathfrak{P} \gamma^{-1}$ for all $\mathfrak{P} \mid \mathfrak{p}$ and $\gamma \in \Gamma_\mathfrak{p}$. By [11, Proposition 7.5] it follows that the morphism

$$f_\mathfrak{p} : X_\mathfrak{p} := \bigtimes_{i=1}^{m} \gamma_i T_{\mathfrak{P}_i} \gamma_i^{-1} \to \mathrm{GL}_{r,\kappa_\mathfrak{p}}, \quad (t_1, \ldots, t_m) \mapsto t_1 \cdots t_m$$

is dominant for a suitable choice of m and $\mathfrak{P}_i \mid \mathfrak{p}$ and $\gamma_i \in \Gamma_\mathfrak{p}$. In fact, since $\dim(\mathrm{GL}_{r,\kappa_\mathfrak{p}}) = r^2$, we can achieve this with $m = r^2$; in particular, we can assume that m is independent of $\mathfrak{p}$. Next, by Proposition 2.4 the fibers of

$$X_\mathfrak{p}^{r^2} \to \mathrm{GL}_{r,\kappa_\mathfrak{p}}, \quad (x_1, \ldots, x_{r^2}) \mapsto f_\mathfrak{p}(x_1) \cdots f_\mathfrak{p}(x_{r^2})$$

have dimension at most $\dim(X_\mathfrak{p}^{r^2}) - \dim(\mathrm{GL}_{r,\kappa_\mathfrak{p}})$. We replace $X_\mathfrak{p}$ by $X_\mathfrak{p}^{r^2}$ and m by mr^2, which is still independent of $\mathfrak{p}$. Then with $e_\mathfrak{p} := \dim(X_\mathfrak{p})$ all fibers of $f_\mathfrak{p}$ have dimension at most $e_\mathfrak{p} - r^2$.

Let Z and $\mathscr{T} \subset \mathrm{GL}_r \times Z$ be as in Lemma 3.11. Then for every $1 \leqslant i \leqslant m$ we can choose a point $z_i \in Z(\kappa_\mathfrak{p})$ such that $\mathscr{T}_{z_i} = \gamma_i T_{\mathfrak{P}_i} \gamma_i^{-1}$. Denote the two projections by $\varepsilon : \mathscr{T} \to \mathrm{GL}_r$ and $\pi : \mathscr{T} \to Z$ and consider the morphism

$$f : \mathscr{T}^m \to \mathrm{GL}_r \times Z^m, \quad (t_1, \ldots, t_m) \mapsto \big(\varepsilon(t_1) \cdot \cdots \cdot \varepsilon(t_m), \pi(t_1), \ldots, \pi(t_m)\big).$$

By construction it induces the morphism $f_\mathfrak{p}$ in the fiber above the point $(z_1, \ldots, z_m) \in Z^m(\kappa_\mathfrak{p})$. Recall that $q_\mathfrak{p} = |\kappa_\mathfrak{p}|$. Since f is independent of $\mathfrak{p}$, Proposition 2.5 yields a constant c_1 independent of $\mathfrak{p}$ such that for all $g \in \mathrm{GL}_r(\kappa_\mathfrak{p})$ we have

$$\left|f_\mathfrak{p}^{-1}(g)(\kappa_\mathfrak{p})\right| \leqslant c_1 q_\mathfrak{p}^{\dim(f_\mathfrak{p}^{-1}(g))} \leqslant c_1 q_\mathfrak{p}^{e_\mathfrak{p} - r^2}.$$

On the other hand, we have $|T_{\mathfrak{P}_i}(\kappa_\mathfrak{p})| = q_\mathfrak{p}^{h_{\mathfrak{P}_i}} - 1$, and hence

$$\left|X_\mathfrak{p}(\kappa_\mathfrak{p})\right| = \prod_{i=1}^m \big(q_\mathfrak{p}^{h_{\mathfrak{P}_i}} - 1\big) \geqslant \prod_{i=1}^m \frac{1}{2} q_\mathfrak{p}^{h_{\mathfrak{P}_i}} = 2^{-m} q_\mathfrak{p}^{\sum h_{\mathfrak{P}_i}} = 2^{-m} q_\mathfrak{p}^{e_\mathfrak{p}}.$$

Since $f_\mathfrak{p}(X_\mathfrak{p}(\kappa_\mathfrak{p})) \subset \Gamma_\mathfrak{p}$, we deduce that

$$|\Gamma_\mathfrak{p}| \geqslant \left|f_\mathfrak{p}\big(X_\mathfrak{p}(\kappa_\mathfrak{p})\big)\right| \geqslant \frac{|X_\mathfrak{p}(\kappa_\mathfrak{p})|}{c_1 q_\mathfrak{p}^{e_\mathfrak{p} - r^2}} \geqslant \frac{2^{-m} q_\mathfrak{p}^{e_\mathfrak{p}}}{c_1 q_\mathfrak{p}^{e_\mathfrak{p} - r^2}} = \frac{q_\mathfrak{p}^{r^2}}{2^m c_1}.$$

Finally, it follows that

$$\big[\mathrm{GL}_r(\kappa_\mathfrak{p}) : \Gamma_\mathfrak{p}\big] = \frac{\prod_{i=0}^{r-1}(q_\mathfrak{p}^r - q_\mathfrak{p}^i)}{|\Gamma_\mathfrak{p}|} \leqslant 2^m c_1 \frac{\prod_{i=0}^{r-1}(q_\mathfrak{p}^r - q_\mathfrak{p}^i)}{q_\mathfrak{p}^{r^2}} \leqslant 2^m c_1.$$

Thus the lemma holds with $c := 2^m c_1$. □

Proof of Proposition 3.1. Let c be the constant in Lemma 3.12. Then we have $[\mathrm{GL}_r(\kappa_\mathfrak{p}) : \Gamma_\mathfrak{p}] \leqslant c$. As $|\kappa_\mathfrak{p}| > 3$ and $|\mathrm{PGL}_r(\kappa_\mathfrak{p})| > c!$ for almost all $\mathfrak{p}$, Proposition 2.3 implies that $\mathrm{SL}_r(\kappa_\mathfrak{p}) \subset \Gamma_\mathfrak{p}$ for almost all $\mathfrak{p}$. Since $T_\mathfrak{P}(\kappa_\mathfrak{p}) \subset \Gamma_\mathfrak{p}$ and $\det : T_\mathfrak{P}(\kappa_\mathfrak{p}) \cong k_n^* \to \kappa_\mathfrak{p}^*$ is the norm map, which is surjective, the determinant map $\det : \Gamma_\mathfrak{p} \to \kappa_\mathfrak{p}^*$ is surjective. Therefore $\Gamma_\mathfrak{p} = \mathrm{GL}_r(\kappa_\mathfrak{p})$ for almost all primes $\mathfrak{p}$ of A, as desired. □

4. Adelic openness in the case $[K/F] < \infty$

Throughout this section we assume that K is a finite extension of F and that $\mathrm{End}_{\bar{K}}(\varphi) = A$. For the most part we still consider the representation $\rho_\mathfrak{p}$ at a single prime $\mathfrak{p}$ of A. As before we abbreviate $q_\mathfrak{p} := |\kappa_\mathfrak{p}|$.

Congruence filtration. Let π be a uniformizer of A at $\mathfrak{p}$. The congruence filtration of $\mathrm{GL}_r(A_\mathfrak{p})$ is defined by

$$\begin{aligned} G^0_\mathfrak{p} &:= \mathrm{GL}_r(A_\mathfrak{p}), \quad \text{and} \\ G^i_\mathfrak{p} &:= 1 + \pi^i \mathrm{M}_r(A_\mathfrak{p}) \quad \text{for all } i \geqslant 1. \end{aligned}$$

Its successive subquotients possess natural isomorphisms

$$\begin{aligned} \nu_0 : G^{[0]}_\mathfrak{p} &:= G^0_\mathfrak{p}/G^1_\mathfrak{p} \xrightarrow{\sim} \mathrm{GL}_r(\kappa_\mathfrak{p}), \quad \text{and} \\ \nu_i : G^{[i]}_\mathfrak{p} &:= G^i_\mathfrak{p}/G^{i+1}_\mathfrak{p} \xrightarrow{\sim} \mathrm{M}_r(\kappa_\mathfrak{p}), \quad \big[1+\pi^i y\big] \mapsto [y] \quad \text{for } i \geqslant 1. \end{aligned}$$

For any subgroup H of $\mathrm{GL}_r(A_\mathfrak{p})$, we define $H^i := H \cap G^i_\mathfrak{p}$ and $H^{[i]} := H^i/H^{i+1}$. Via ν_i we identify the latter with a subgroup of $\mathrm{GL}_r(\kappa_\mathfrak{p})$ or $\mathrm{M}_r(\kappa_\mathfrak{p})$, respectively.

Proposition 4.1. *Let H be a closed subgroup of $\mathrm{GL}_r(A_\mathfrak{p})$. Assume that $q_\mathfrak{p} \geqslant 4$, that $\det(H) = \mathrm{GL}_1(A_\mathfrak{p})$, that $H^{[0]} = \mathrm{GL}_r(\kappa_\mathfrak{p})$, and that $H^{[1]}$ contains a non-scalar matrix. Then we have*

$$H = \mathrm{GL}_r(A_\mathfrak{p}).$$

Proof. First, consider the conjugation action

$$H^{[0]} \times H^{[1]} \to H^{[1]}, \quad \big([g],[h]\big) \mapsto \big[ghg^{-1}\big].$$

Under ν_0 and ν_1 it corresponds to the conjugation action

$$\mathrm{GL}_r(\kappa_\mathfrak{p}) \times \mathrm{M}_r(\kappa_\mathfrak{p}) \to \mathrm{M}_r(\kappa_\mathfrak{p}), \quad (g, X) \mapsto gXg^{-1}.$$

Since $H^{[0]} = \mathrm{GL}_r(\kappa_\mathfrak{p})$, it follows that $H^{[1]} \subset \mathrm{M}_r(\kappa_\mathfrak{p})$ is closed under conjugation by $\mathrm{GL}_r(\kappa_\mathfrak{p})$. Since it also contains a non-scalar matrix, by Proposition 2.1 it therefore contains the subgroup $\mathfrak{sl}_r(\kappa_\mathfrak{p})$ of all matrices of trace 0. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1/H^2 & \longrightarrow & H/H^2 & \longrightarrow & \mathrm{GL}_r(\kappa_\mathfrak{p}) & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle\det} & & \big\downarrow{\scriptstyle\det} & & \big\downarrow{\scriptstyle\det} & & \\ 0 & \longrightarrow & (1+\pi A_\mathfrak{p}/(\pi)^2)^* & \longrightarrow & (A_\mathfrak{p}/\mathfrak{p}^2)^* & \longrightarrow & \kappa^*_\mathfrak{p} & \longrightarrow & 0. \end{array}$$

The right vertical map is surjective with kernel $\mathrm{SL}_r(\kappa_\mathfrak{p})$. By assumption, the middle vertical map is surjective as well. By the snake lemma, we thus obtain a surjective homomorphism from $\mathrm{SL}_r(\kappa_\mathfrak{p})$ onto the cokernel of the left vertical map. This cokernel is an abelian p-group, but since $|\kappa_\mathfrak{p}| \geqslant 4$, the group $\mathrm{SL}_r(\kappa_\mathfrak{p})$ has no non-trivial abelian p-group as a quotient. Therefore the left vertical map is surjective. This means that the composite trace map $H^{[1]} \hookrightarrow \mathrm{M}_r(\kappa_\mathfrak{p}) \xrightarrow{\mathrm{tr}} \kappa_\mathfrak{p}$ is surjective. Together it follows that $H^{[1]} = \mathrm{M}_r(\kappa_\mathfrak{p})$.

Next consider the commutator subgroup H' of H. Since $\det(H) = \mathrm{GL}_1(A_\mathfrak{p})$, the proposition follows once we have shown that $H' = \mathrm{SL}_r(A_\mathfrak{p})$. This in turn is equivalent to $H'^{[i]} = \mathrm{SL}_r(A_\mathfrak{p})^{[i]}$ for all $i \geqslant 0$.

For $i = 0$ this results from $H'^{[0]} = (H^{[0]})' = \mathrm{GL}_r(\kappa_\mathfrak{p})' = \mathrm{SL}_r(\kappa_\mathfrak{p})$. For $i = 1$ consider the map

$$H^{[0]} \times H^{[1]} \to H'^{[1]}, \quad \big([g],[h]\big) \mapsto \big[ghg^{-1}h^{-1}\big]$$

induced by commutator map $H \times H \to H'$. Under ν_0 and ν_1, it corresponds to the map

$$\mathrm{GL}_r(\kappa_\mathfrak{p}) \times \mathrm{M}_r(\kappa_\mathfrak{p}) \to \mathfrak{sl}_r(\kappa_\mathfrak{p}), \quad (g, X) \mapsto gXg^{-1} - X.$$

It is an elementary fact that the image of this latter map generates $\mathfrak{sl}_r(\kappa_\mathfrak{p})$ as an additive group. Since $H^{[0]} = \mathrm{GL}_r(\kappa_\mathfrak{p})$ and $H^{[1]} = \mathrm{M}_r(\kappa_\mathfrak{p})$, it follows that $H'^{[1]} = \mathfrak{sl}_r(\kappa_\mathfrak{p})$. Assume now that $H'^{[i]} = \mathfrak{sl}_r(\kappa_\mathfrak{p})$ for some $i \geqslant 1$. In this case consider the map

$$H^{[1]} \times H'^{[i]} \to H'^{[i+1]}, \quad \big([g], [h]\big) \mapsto \big[ghg^{-1}h^{-1}\big]$$

induced by the commutator map $H \times H' \to H'$. Under ν_1, ν_i, and ν_{i+1} it corresponds to the Lie bracket

$$[\,,\,] : \mathrm{M}_r(\kappa_\mathfrak{p}) \times \mathfrak{sl}_r(\kappa_\mathfrak{p}) \to \mathfrak{sl}_r(\kappa_\mathfrak{p}), \quad (X, Y) \mapsto XY - YX.$$

By [15, Proposition 1.2] the image of this latter map generates $\mathfrak{sl}_r(\kappa_\mathfrak{p})$ as an additive group. Since $H^{[1]} = \mathrm{M}_r(\kappa_\mathfrak{p})$ and $H'^{[i]} = \mathfrak{sl}_r(\kappa_\mathfrak{p})$, it follows that $H'^{[i+1]} = \mathfrak{sl}_r(\kappa_\mathfrak{p})$, as desired. □

Wild ramification. Consider a prime $\mathfrak{p}$ of A and a place $\mathfrak{P}$ of K above $\mathfrak{p}$. Assume that $\mathfrak{P}$ is unramified over $\mathfrak{p}$ and that φ has good reduction at $\mathfrak{P}$ of height $h_\mathfrak{P}$. The image of the inertia group on the $\mathfrak{p}$-torsion $\varphi[\mathfrak{p}](K^{\mathrm{sep}})$ was described in (3.2). Similarly, the connected-étale decomposition of the finite flat group scheme $\varphi[\mathfrak{p}^2]$ over the discrete valuation ring $\mathcal{O}_{K_\mathfrak{P}}$ yields an exact sequence

$$0 \to \varphi\big[\mathfrak{p}^2\big]^0\big(K^{\mathrm{sep}}\big) \to \varphi\big[\mathfrak{p}^2\big]\big(K^{\mathrm{sep}}\big) \to \varphi\big[\mathfrak{p}^2\big]^{et}\big(K^{\mathrm{sep}}\big) \to 0,$$

where the inertia group $\mathrm{I}_\mathfrak{P}$ acts trivially on $\varphi[\mathfrak{p}^2]^{et}(K^{\mathrm{sep}})$. Thus up to conjugation the image of $\mathrm{I}_\mathfrak{P}$ in $\mathrm{GL}_r(A/\mathfrak{p}^2)$ lies in the subgroup

$$\left(\begin{array}{c|c} * & * \\ \hline 0 & 1 \end{array}\right) \subset \mathrm{GL}_r\big(A/\mathfrak{p}^2\big)$$

of block matrices of size $h_\mathfrak{P}$, $r - h_\mathfrak{P}$. Choose a lift $\kappa_\mathfrak{p} \hookrightarrow A/\mathfrak{p}^2$; it induces a lift $k_n^* \hookrightarrow \mathrm{GL}_{h_\mathfrak{P}}(A/\mathfrak{p}^2)$. Then (3.2) implies that up to conjugation the image of the tame inertia group $\mathrm{I}_\mathfrak{P}^t$ is the subgroup

$$J := \left(\begin{array}{c|c} k_n^* & 0 \\ \hline 0 & 1 \end{array}\right) \subset \mathrm{GL}_r\big(A/\mathfrak{p}^2\big).$$

Let $P \subset \mathrm{GL}_r(A/\mathfrak{p}^2)$ denote the image of the wild inertia group $\mathrm{I}_\mathfrak{P}^p$. In view of (3.2) it is contained in the subgroup

$$N := \left\{ \left(\begin{array}{c|c} a & b \\ \hline 0 & 1 \end{array}\right) \in \mathrm{GL}_r\big(A/\mathfrak{p}^2\big) \;\middle|\; a \equiv 1 \bmod \mathfrak{p} \right\}.$$

Consider the subgroups

$$L_1 := \left(\begin{array}{c|c} * & 0 \\ \hline 0 & 0 \end{array}\right), \qquad L_2 := \left(\begin{array}{c|c} 0 & * \\ \hline 0 & 0 \end{array}\right), \qquad L_1 \oplus L_2 \cong \left(\begin{array}{c|c} * & * \\ \hline 0 & 0 \end{array}\right) \subset \mathrm{M}_r(\kappa_\mathfrak{p}).$$

Then the image of P under the homomorphism

$$\pi : N \to L_1, \quad \left(\begin{array}{c|c} a & b \\ \hline 0 & 1 \end{array}\right) \mapsto \left(\begin{array}{c|c} (a-1)/\pi & 0 \\ \hline 0 & 0 \end{array}\right) \mod \mathfrak{p}$$

describes the action on $\varphi[\mathfrak{p}^2]^0(K^{\mathrm{sep}})$.

Lemma 4.2. *The group $\pi(P)$ has order at least $q_{\mathfrak{p}}^{h_{\mathfrak{P}}}$.*

Proof. (Compare Gardeyn [8, Proposition 4.5].) We will show this by determining the valuation at $\mathfrak{P}$ of torsion points in $\varphi[\mathfrak{p}^2]^0(K^{\mathrm{sep}})$. Let $a \in A$ be any function with a simple zero at $\mathfrak{p}$. Then $(a) = \mathfrak{p}\mathfrak{a}$ for an ideal $\mathfrak{a}$ of A which is prime to $\mathfrak{p}$. This implies that $\varphi[a] = \varphi[\mathfrak{p}] \oplus \varphi[\mathfrak{a}]$, where $\varphi[\mathfrak{a}]$ is étale, and therefore

$$\varphi[a]^0 = \varphi[\mathfrak{p}]^0$$

as group schemes over $\operatorname{Spec} \mathscr{O}_{K_{\mathfrak{P}}}$. Write $\varphi_a = \sum_i \varphi_{a,i}\tau^i$ with $\varphi_{a,i} \in \mathscr{O}_{K_{\mathfrak{P}}}$. Let $v_{\mathfrak{P}}$ denote the normalized valuation of $K_{\mathfrak{P}}$. Then

$$v_{\mathfrak{P}}(\varphi_{a,0}) = v_{\mathfrak{P}}\big(\iota(a)\big) = 1,$$

because $\operatorname{ord}_{\mathfrak{p}}(a) = 1$ and $\mathfrak{P}|\mathfrak{p}$ is unramified. Moreover, since φ has good reduction at $\mathfrak{P}$, there exists a unique integer $i_0 > 0$ such that

$$\begin{aligned} v_{\mathfrak{P}}(\varphi_{a,i}) &\geqslant 1 \quad \text{for } 0 < i < i_0, \\ v_{\mathfrak{P}}(\varphi_{a,i_0}) &= 0, \quad \text{and} \\ v_{\mathfrak{P}}(\varphi_{a,i}) &\geqslant 0 \quad \text{for } i > i_0. \end{aligned}$$

Thus

$$q^{i_0} = \big|\varphi[a]^\circ\big| = \big|\varphi[\mathfrak{p}]^\circ\big| = q_{\mathfrak{p}}^{h_{\mathfrak{P}}},$$

and so the Newton polygon of the polynomial $\varphi_a(x) = \sum \varphi_{a,i}x^{q^i}$ has the vertices $(1,1)$ and $(q_{\mathfrak{p}}^{h_{\mathfrak{P}}}, 0)$ and possibly $(u, 0)$ for some other (irrelevant) value $u \geqslant q_{\mathfrak{p}}^{h_{\mathfrak{P}}}$. It follows that every non-zero element $s \in \varphi[\mathfrak{p}]^0(K^{\mathrm{sep}})$ has the valuation

$$v_{\mathfrak{P}}(s) = \alpha := 1/\big(q_{\mathfrak{p}}^{h_{\mathfrak{P}}} - 1\big).$$

Fix any such s. Repeating the above arguments, we find that

$$\varphi\big[a^2\big]^\circ = \varphi\big[\mathfrak{p}^2\big]^\circ$$

and that the zeroes of valuation > 0 of the polynomial $\varphi_a(x) - s$ are precisely the elements $s' \in \varphi[\mathfrak{p}^2]^0(K^{\mathrm{sep}})$ with $as' = s$. The Newton polygon of this polynomial has the vertices $(0, \alpha)$ and $(q_{\mathfrak{p}}^{h_{\mathfrak{P}}}, 0)$ and $(u, 0)$; hence any such s' has the valuation

$$v_{\mathfrak{P}}(s') = \alpha / q_{\mathfrak{p}}^{h_{\mathfrak{P}}}.$$

We deduce that the wild ramification index of the field extension $K_{\mathfrak{P}}(s')/K_{\mathfrak{P}}$ is equal to $q_{\mathfrak{p}}^{h_{\mathfrak{P}}}$. As this index divides the order of $\pi(P)$, the lemma follows. □

Lemma 4.3. *If $q_{\mathfrak{p}} \geqslant 3$, then any additive subgroup $H \subset L_1 \oplus L_2$ that is normalized by J is the direct sum of its subgroups $H \cap L_1$ and $H \cap L_2$.*

Proof. It suffices to prove that L_1 and L_2 possess no non-trivial isomorphic subquotients as representations of J over $\mathbb{F}_p$. For this recall that $J \cong k_n^*$ for a field extension k_n of $\kappa_{\mathfrak{p}}$ of degree $h_{\mathfrak{P}}$. We let it act by multiplication on k_n and endow $k_n^\vee := \mathrm{Hom}_{\kappa_{\mathfrak{p}}}(k_n, \kappa_{\mathfrak{p}})$ with the contragredient representation. Then there are natural J-equivariant isomorphisms $L_1 \cong k_n \otimes_{\kappa_{\mathfrak{p}}} k_n^\vee$ and $L_2 \cong k_n^{r-h_{\mathfrak{P}}}$. Let $\bar{k}_n$ denote an algebraic closure of k_n. Then the representation $L_2 \otimes_{\mathbb{F}_p} \bar{k}_n$ over $\bar{k}_n$ consists of the irreducible characters

$$k_n^* \to \bar{k}_n^*, \quad u \mapsto u^{p^m}$$

for all integers $m \geqslant 0$. On the other hand we can identify $k_n \otimes_{\kappa_{\mathfrak{p}}} k_n^\vee$ with $k_n^{h_{\mathfrak{P}}}$ such that the action of $u \in k_n^*$ on the ith summand is given by multiplication by $u^{q_{\mathfrak{p}}^i - 1}$. Thus the representation $L_1 \otimes_{\mathbb{F}_p} \bar{k}_n$ over $\bar{k}_n$ consists of the irreducible characters

$$k_n^* \to \bar{k}_n^*, \quad u \mapsto u^{(q_{\mathfrak{p}}^i - 1)p^j}$$

for all integers $i, j \geqslant 0$. We must show that no two such characters of the respective kinds are equal. They are equal if and only if $u^{(q_{\mathfrak{p}}^i - 1)p^j} = u^{p^m}$ for all $u \in k_n^*$. Since k_n^* is cyclic of order $q_{\mathfrak{p}}^{h_{\mathfrak{P}}} - 1$, this is equivalent to

$$\left(q_{\mathfrak{p}}^i - 1\right)p^j \equiv p^m \mod \left(q_{\mathfrak{p}}^{h_{\mathfrak{P}}} - 1\right).$$

As $q_{\mathfrak{p}} - 1$ divides both $q_{\mathfrak{p}}^i - 1$ and $q_{\mathfrak{p}}^{h_{\mathfrak{P}}} - 1$, this congruence relation implies that $q_{\mathfrak{p}} - 1$ divides p^m. But $q_{\mathfrak{p}}$ is a power of p, and thus $q_{\mathfrak{p}} - 1$ is relatively prime to p^m; hence this is possible only if $q_{\mathfrak{p}} - 1 = 1$. But that was excluded by the assumption $q_{\mathfrak{p}} \geqslant 3$; hence the characters cannot be equal. □

Proposition 4.4. *In the above situation, if $q_{\mathfrak{p}} \geqslant 3$, the subgroup*

$$\{g \in P \mid g \equiv 1 \bmod \mathfrak{p}\}$$

has order at least $q_{\mathfrak{p}}^{h_{\mathfrak{P}}}$.

Proof. Consider the homomorphism

$$\pi' : N \to L_1 \oplus L_2, \quad \left(\begin{array}{c|c} a & b \\ \hline 0 & 1 \end{array}\right) \mapsto \left(\begin{array}{c|c} (a-1)/\pi & b \\ \hline 0 & 0 \end{array}\right) \mod \mathfrak{p},$$

which is clearly equivariant under J. Thus we can apply Lemma 4.3 to the subgroup $\pi'(P) \subset L_1 \oplus L_2$. Since the composite of π' with the projection $\mathrm{pr}_1 : L_1 \oplus L_2 \to L_1$ is the homomorphism π above, we deduce that

$$\pi(P) = \mathrm{pr}_1\left(\pi'(P)\right) \overset{4.3}{=} \mathrm{pr}_1\left(\pi'(P) \cap L_1\right) = \pi\left(P \cap \pi'^{-1}(L_1)\right) = \pi\left(\{g \in P \mid g \equiv 1 \bmod \mathfrak{p}\}\right).$$

Thus the lower bound from Lemma 4.2 implies the result. □

Subgroup generated by inertia.

Proposition 4.5. *In the above situation, for almost all primes* $\mathfrak{p}$ *of* A *and any (single) place* $\mathfrak{P}$ *of* K *above* $\mathfrak{p}$*, the images under* $\rho_\mathfrak{p}$ *of all* G_K*-conjugates of the inertia group* $\mathrm{I}_\mathfrak{P}$ *generate* $\mathrm{GL}_r(A_\mathfrak{p})$*.*

Proof. We may assume that $\mathfrak{P}$ is unramified over $\mathfrak{p}$, that φ has good reduction at $\mathfrak{P}$, and that $q_\mathfrak{p} \geqslant 4$. By Proposition 3.1 we may also assume that the residual representation $\bar{\rho}_\mathfrak{p} : G_K \to \mathrm{GL}_r(\kappa_\mathfrak{p})$ is surjective. Let $H \subset \mathrm{GL}_r(A_\mathfrak{p})$ denote the subgroup in question. We will show that the stated conditions imply that $H = \mathrm{GL}_r(A_\mathfrak{p})$.

We use the notations from the beginning of this section. The first condition in Proposition 4.1 holds by assumption. For the second recall that the determinant of $\rho_\mathfrak{p}$ coincides with the Galois representation on the Tate module of a Drinfeld module ψ of rank 1 over K (see Anderson [2]). As φ has good reduction at $\mathfrak{P}$, the Tate module of φ at any prime not below $\mathfrak{P}$ is unramified at $\mathfrak{P}$; hence the same holds for the Tate module of ψ. By the criterion of Néron–Ogg–Shafarevich (see Goss [9, Theorem 4.10.5]) it follows that ψ has good reduction at $\mathfrak{P}$. Since moreover $\mathfrak{P}$ is unramified over $\mathfrak{p}$, it follows that the representation $\mathrm{I}_\mathfrak{P} \to \mathrm{GL}_1(A_\mathfrak{p})$ associated to ψ is surjective (see Hayes [10, Proposition 9.1] or Gardeyn [8, Theorem 4.1]). Thus $\det(H) = \mathrm{GL}_1(A_\mathfrak{p})$, proving the second condition in Proposition 4.1. In particular this shows the desired assertion in the case $r = 1$. For the rest of the proof we therefore assume that $r \geqslant 2$.

For the third condition consider the subgroup $H^{[0]} \subset \mathrm{GL}_r(\kappa_\mathfrak{p})$. By (3.3) it contains the subgroup

$$\bar{\rho}_\mathfrak{p}\big(\mathrm{I}^t_\mathfrak{P}\big) = \left(\begin{array}{c|c} k_n^* & 0 \\ \hline 0 & 1 \end{array}\right)$$

written in block matrices of size $h_\mathfrak{P}$, $r - h_\mathfrak{P}$, where k_n is an extension of $\kappa_\mathfrak{p}$ of degree $h_\mathfrak{P}$. If $h_\mathfrak{P} > 1$, any generator of this subgroup is non-scalar. If $h_\mathfrak{P} = 1$, we have $|k_n^*| = |\kappa_\mathfrak{p}^*| \geqslant 4$; hence this subgroup contains a non-trivial element. Since $r \geqslant 2$, this element is again non-scalar. Thus in both cases it follows that $H^{[0]}$ contains a non-scalar element.

By construction H is a normal subgroup of $\rho_\mathfrak{p}(\mathrm{G}_K)$. As the residual representation is surjective by assumption, it follows that $H^{[0]}$ is a normal subgroup of $\mathrm{GL}_r(\kappa_\mathfrak{p})$. Since $q_\mathfrak{p} \geqslant 4$, Proposition 2.2 implies that $\mathrm{SL}_r(\kappa_\mathfrak{p}) \subset H^{[0]}$. Since the determinant induces on $\bar{\rho}_\mathfrak{p}(\mathrm{I}^t_\mathfrak{P})$ the norm map $k_n^* \to \kappa_\mathfrak{p}^*$, which is surjective, the determinant map $H^{[0]} \to \kappa_\mathfrak{p}^*$ is surjective. Together it follows that $H^{[0]} = \mathrm{GL}_r(\kappa_\mathfrak{p})$, proving the third condition in Proposition 4.1.

Next Proposition 4.4 implies that $H^{[1]}$ contains a subgroup of the group of block matrices of the form

$$\left(\begin{array}{c|c} * & * \\ \hline 0 & 0 \end{array}\right) \subset \mathrm{M}_r(\kappa_\mathfrak{p})$$

of order at least $q_\mathfrak{p}^{h_\mathfrak{P}}$. If $h_\mathfrak{P} > 1$, it thus contains a non-scalar element, and if $h_\mathfrak{P} < r$, every non-trivial element is non-scalar. Thus $H^{[1]}$ contains a non-scalar matrix, proving the fourth and last condition in Proposition 4.1. Altogether it now follows that $H = \mathrm{GL}_r(A_\mathfrak{p})$, as desired. □

Adelic representation. We can now prove the following special case of Theorem 0.1.

Theorem 4.6. *If* K *is a finite extension of* F *and* $\mathrm{End}_{\bar{K}}(\varphi) = A$*, the image of the adelic representation*

$$\rho_{\mathrm{ad}} : \mathrm{G}_K \to \prod_\mathfrak{p} \mathrm{GL}_r(A_\mathfrak{p})$$

is open.

Proof. Let Γ denote this image. Fix a finite set Λ of primes $\mathfrak{p}$ of A, such that Proposition 4.5 holds for all $\mathfrak{p} \notin \Lambda$ and that φ has good reduction at all places $\mathfrak{P}$ above $\mathfrak{p} \notin \Lambda$. For any such $\mathfrak{P}|\mathfrak{p}$, the inertia group $\mathrm{I}_{\mathfrak{P}}$ acts trivially on the Tate modules $T_{\mathfrak{p}'}(\varphi)$ for all $\mathfrak{p}' \neq \mathfrak{p}$. Thus its image under ρ_{ad} is contained in the subgroup

$$\mathrm{GL}_r(A_{\mathfrak{p}}) \times \prod_{\mathfrak{p}' \neq \mathfrak{p}} \{1\}.$$

The same follows for the subgroup $\Delta_{\mathfrak{P}}$ generated by all Γ-conjugates of $\rho_{\mathrm{ad}}(\mathrm{I}_{\mathfrak{P}})$. But Proposition 4.5 implies that the projection to the factor at $\mathfrak{p}$ induces a surjective homomorphism $\Delta_{\mathfrak{P}} \to \mathrm{GL}_r(A_{\mathfrak{p}})$. Therefore

$$\Delta_{\mathfrak{P}} = \mathrm{GL}_r(A_{\mathfrak{p}}) \times \prod_{\mathfrak{p}' \neq \mathfrak{p}} \{1\}.$$

By varying $\mathfrak{p}$ and $\mathfrak{P}$ we deduce that

$$\prod_{\mathfrak{p} \notin \Lambda} \mathrm{GL}_r(A_{\mathfrak{p}}) \subset \Gamma.$$

Therefore Γ is the inverse image of its image under the projection

$$\pi_\Lambda : \prod_{\mathfrak{p}} \mathrm{GL}_r(A_{\mathfrak{p}}) \to \prod_{\mathfrak{p} \in \Lambda} \mathrm{GL}_r(A_{\mathfrak{p}}).$$

But $\pi_\Lambda(\Gamma)$ is an open subgroup by Theorem 1.2; hence Γ is an open subgroup, as desired. □

5. The general case

Throughout this section, we assume that $\mathrm{End}_{\bar{K}}(\varphi) = A$, but now the transcendence degree of K is arbitrary. We prove the general case of Theorem 0.1 by reducing it to the case of a finite extension of F, using a specialization argument similar to [13]. We begin with some group theory.

Let $\mathfrak{p}$ be any prime of A, and let π be a uniformizer at $\mathfrak{p}$. For any $n \geqslant 1$ we define

$$G_{\mathfrak{p}}^n := 1 + \pi^n \mathrm{M}_r(A_{\mathfrak{p}}) \quad \text{and}$$
$$G_{\mathfrak{p}}^{n\prime} := G_{\mathfrak{p}}^n \cap \mathrm{SL}_r(A_{\mathfrak{p}}).$$

For any two integers $n \geqslant \ell \geqslant 1$ we have a natural group isomorphism

$$\log_{n,\ell} : G_{\mathfrak{p}}^n / G_{\mathfrak{p}}^{n+\ell} \xrightarrow{\sim} \mathrm{M}_r\big(\mathfrak{p}^n/\mathfrak{p}^{n+\ell}\big), \quad [1+X] \mapsto [X]. \tag{5.1}$$

As explained in [14], this can be considered as a logarithm map truncated after the first-order term. In the same way, the inverse isomorphism is an exponential map truncated after the first-order term. We denote it by $\exp_{n,\ell}$.

Lemma 5.2. *For any natural numbers $n, m \geqslant \ell \geqslant 1$, the following properties hold.*

(i) *The commutator $G_{\mathfrak{p}}^n \times G_{\mathfrak{p}}^n \to G_{\mathfrak{p}}^n$, $(g,h) \mapsto ghg^{-1}h^{-1}$ induces a bimultiplicative map*

$$\{\,,\}^- : G_{\mathfrak{p}}^n / G_{\mathfrak{p}}^{n+\ell} \times G_{\mathfrak{p}}^m / G_{\mathfrak{p}}^{m+\ell} \to G_{\mathfrak{p}}^{n+m} / G_{\mathfrak{p}}^{n+m+\ell},$$
$$\big([g],[h]\big) \mapsto \big[ghg^{-1}h^{-1}\big].$$

(ii) *The Lie bracket* $\mathrm{M}_r(\mathfrak{p}^n A_\mathfrak{p}) \times \mathrm{M}_r(\mathfrak{p}^n A_\mathfrak{p}) \to \mathrm{M}_r(\mathfrak{p}^n A_\mathfrak{p})$ *induces a bilinear map*

$$[\,,\,]^- : \mathrm{M}_r\big(\mathfrak{p}^n/\mathfrak{p}^{n+\ell}\big) \times \mathrm{M}_r\big(\mathfrak{p}^m/\mathfrak{p}^{m+\ell}\big) \to \mathrm{M}_r\big(\mathfrak{p}^{n+m}/\mathfrak{p}^{n+m+\ell}\big),$$
$$\big([X],[Y]\big) \mapsto [XY - YX].$$

(iii) *We have*

$$\log_{n+m,l}\big(\big\{[g],[h]\big\}^-\big) = \big[\log_{n,l}\big([g]\big), \log_{m,l}\big([h]\big)\big]^-.$$

Proof. Consider elements $g = 1 + X \in G_\mathfrak{p}^n$, and $h = 1 + Y \in G_\mathfrak{p}^m$. Their inverses are given by the geometric series

$$g^{-1} = 1 - X + X^2 - + \cdots \quad \text{and}$$
$$h^{-1} = 1 - Y + Y^2 - + \cdots.$$

Therefore

$$ghg^{-1} = gg^{-1} + gYg^{-1} = (1 + Y) + (XY - YX) + T(X,Y),$$

where T is a power series of degree $\geqslant 2$ in X and degree $\geqslant 1$ in Y. This implies that

$$\begin{aligned} ghg^{-1}h^{-1} &= (1+Y)(1+Y)^{-1} + (XY - YX)(1+Y)^{-1} + T(X,Y)(1+Y)^{-1} \\ &= 1 + (XY - YX) + T'(X,Y) + T(X,Y)(1+Y)^{-1}, \end{aligned}$$

where T' is a power series of degree $\geqslant 2$ in Y and degree at least $\geqslant 1$ in X. Since n, $m \geqslant \ell$, both $T'(X,Y)$ and $T(X,Y)$ vanish modulo $\mathfrak{p}^{n+m+\ell}$; hence

$$ghg^{-1}h^{-1} \equiv 1 + (XY - YX) \mod \mathfrak{p}^{n+m+\ell}.$$

Everything follows from this. □

Next consider a closed subgroup H of $\mathrm{GL}_r(A_\mathfrak{p})$, and set

$$H^n := H \cap G_\mathfrak{p}^n \quad \text{and}$$
$$H^{n'} := H \cap G_\mathfrak{p}^{n'}.$$

Lemma 5.3. *Consider any natural numbers* $n, m \geqslant \ell \geqslant 1$. *Assume that* $H^n/H^{n+\ell} = G_\mathfrak{p}^n/G_\mathfrak{p}^{n+\ell}$ *and that* $G_\mathfrak{p}^{m'}/G_\mathfrak{p}^{m+\ell'} \subset H^m/H^{m+\ell}$. *Then we have*

$$H^{n+m'}/H^{n+m+\ell'} = G_\mathfrak{p}^{n+m'}/G_\mathfrak{p}^{n+m+\ell'}.$$

Proof. By Lemma 5.2, we have the following commutative diagram

$$\begin{array}{ccc} G_\mathfrak{p}^n/G_\mathfrak{p}^{n+\ell} \times G_\mathfrak{p}^{m'}/G_\mathfrak{p}^{m+\ell'} & \xrightarrow{\{\,,\,\}^-} & G_\mathfrak{p}^{n+m'}/G_\mathfrak{p}^{n+m+\ell'} \\ \Big\downarrow{\scriptstyle \log_{n,\ell} \times \log_{m,\ell}} & & \Big\uparrow{\scriptstyle \exp_{n+m,\ell}} \\ \mathrm{M}_r(\mathfrak{p}^n/\mathfrak{p}^{n+\ell}) \times \mathrm{M}_r(\mathfrak{p}^m/\mathfrak{p}^{m+\ell}) & \xrightarrow{[\,,\,]^-} & \mathfrak{sl}_r(\mathfrak{p}^{n+m}/\mathfrak{p}^{n+m+\ell}). \end{array}$$

By (5.1) the vertical arrows are isomorphisms. By [15, Proposition 1.2], the set of commutators $[\mathrm{M}_r, \mathfrak{sl}_r]$ generates the group $\mathfrak{sl}_r$. Thus the subset

$$\exp_{n+m,\ell}\big(\big[\log_{n,\ell}\big(G_\mathfrak{p}^n/G_\mathfrak{p}^{n+\ell}\big), \log_{m,\ell}\big(G_\mathfrak{p}^{m\prime}/G_\mathfrak{p}^{m+\ell\prime}\big)\big]\big)$$

generates the group $G_\mathfrak{p}^{n+m\prime}/G_\mathfrak{p}^{n+m+\ell\prime}$. By assumption this subset is

$$\big\{H^n/H^{n+\ell}, H^m/H^{m+\ell}\big\}^-,$$

and therefore contained in $H^{n+m\prime}/H^{n+m+\ell\prime}$. The lemma follows. □

Proposition 5.4. *Assume that there exists a natural number $n \geqslant 1$ such that $H^n/H^{2n} = G_\mathfrak{p}^n/G_\mathfrak{p}^{2n}$. Then we have*

$$G_\mathfrak{p}^{n\prime} \subset H^n.$$

Proof. We must show that $G_\mathfrak{p}^{n\prime} = H^{n\prime}$. Since H is a closed subgroup of $\mathrm{GL}_r(A_\mathfrak{p})$, it is enough to show that $H^{in\prime}/H^{(i+1)n\prime} = G_\mathfrak{p}^{in\prime}/G_\mathfrak{p}^{(i+1)n\prime}$ for all $i \geqslant 1$. The assumption implies this already for $i = 1$. If it holds for some $i \geqslant 1$, the assumption and Lemma 5.3 show that it also holds for $i+1$. By induction the assertion follows for all i, as desired. □

Specialization with prescribed absolute endomorphism ring. Now we choose an integral scheme X of finite type over $\mathbb{F}_p$ with function field K such that φ extends to a family of Drinfeld A-modules of rank r over X. For any point $x \in X$, we get a Drinfeld A-module φ_x of rank r over the residue field k_x at x. Its characteristic is the image λ_x of x under the morphism $X \to \mathrm{Spec}(A)$. For any prime $\mathfrak{p} \neq \lambda_x$ of A, the specialization map induces an isomorphism

$$T_\mathfrak{p}(\varphi) \xrightarrow{\sim} T_\mathfrak{p}(\varphi_x). \tag{5.5}$$

Proposition 5.6. *In the above situation, if $\mathrm{End}_{\bar{K}}(\varphi) = A$, there exists a point $x \in X$ such that k_x is a finite extension of F and*

$$\mathrm{End}_{\bar{k}_x}(\varphi_x) = A.$$

Proof. Denote by $\widetilde{\Gamma}_\mathfrak{p}$ the image of G_K in the representation on $T_\mathfrak{p}(\varphi)$. By Theorem 1.2 it is an open subgroup of $\mathrm{GL}_r(A_\mathfrak{p})$; hence there exists an integer $n \geqslant 1$ such that $G_\mathfrak{p}^n \subset \widetilde{\Gamma}_\mathfrak{p}$. Let K' be the finite Galois extension of K such that $\mathrm{Gal}(K'/K) = \widetilde{\Gamma}_\mathfrak{p}/G_\mathfrak{p}^{2n}$, and let $\pi : X' \to X$ be the normalization of X in K'. By [13, Lemma 1.6], there exists a point $x \in X$ such that k_x is a finite extension of F and $\pi^{-1}(x) \subset X'$ is irreducible.

Denote by $\Delta_\mathfrak{p}$ the image of G_{k_x} in the representation on $T_\mathfrak{p}(\varphi_x)$. This is a closed subgroup of $\mathrm{GL}_r(A_\mathfrak{p})$. Since $\mathfrak{p} \neq \lambda_x$, the specialization isomorphism (5.5) turns $\Delta_\mathfrak{p}$ into a subgroup of $\widetilde{\Gamma}_\mathfrak{p}$. The irreducibility of $\pi^{-1}(x)$ means that $\mathrm{Gal}(k_{\pi^{-1}(x)}/k_x) \cong \mathrm{Gal}(K'/K)$. We find that $\Delta_\mathfrak{p} G_\mathfrak{p}^{2n} = \widetilde{\Gamma}_\mathfrak{p}$, and thus $\Delta_\mathfrak{p}^n G_\mathfrak{p}^{2n} = G_\mathfrak{p}^n$. In other words we have

$$\Delta_\mathfrak{p}^n/\Delta_\mathfrak{p}^{2n} = G_\mathfrak{p}^n/G_\mathfrak{p}^{2n}.$$

By Proposition 5.4 this implies that $G_\mathfrak{p}^{n\prime} \subset \Delta_\mathfrak{p}^{n\prime}$. In particular $\Delta_\mathfrak{p}$ contains an open subgroup of $\mathrm{SL}_r(A_\mathfrak{p})$. By Goss [9, Theorem 7.7.1], the image of $\Delta_\mathfrak{p}$ under the determinant is an open subgroup of $\mathrm{GL}_1(A_\mathfrak{p})$. Together this implies that $\Delta_\mathfrak{p}$ is an open subgroup of $\mathrm{GL}_r(A_\mathfrak{p})$.

Finally, all endomorphisms of φ_x are defined over some finite separable extension k'_x of k_x. This extension corresponds to an open subgroup of $\Delta_{\mathfrak{p}}$, which by the above is again open in $\mathrm{GL}_r(A_{\mathfrak{p}})$. By the easy direction of the Tate conjecture, it follows that $\mathrm{End}_{\bar{k}_x}(\varphi_x) = \mathrm{End}_{k'_x}(\varphi_x) = A$, as desired. □

Proof of Theorem 0.1. If K is a finite extension of F, the result is Theorem 4.6. In the general case choose x as in Proposition 5.6. Then Theorem 4.6 for the Drinfeld module φ_x shows that the image of the adelic representation associated to φ_x is open in $\mathrm{GL}_r(\mathbb{A}_F^f)$. By the specialization isomorphism (5.5) this image is a subgroup of the image of the adelic representation associated to φ. Thus the latter is open in $\mathrm{GL}_r(\mathbb{A}_F^f)$ as well. □

Appendix A. Two remarks on Gardeyn [8]

In [8] Gardeyn generalized Theorem 1.2 to simple τ-modules of dimension 1. In this appendix we show how to close two gaps in his proof.

Specialization. The first gap is in the proof of [8, Proposition 2.4] at the bottom of p. 318, where he addresses a specialization problem analogous to that in Proposition 5.6. He considers an integral scheme of finite type X with function field K and a family of τ-modules $\mathscr{M}$ over X whose generic fiber M has absolute endomorphism ring $\mathrm{End}_{\bar{K}}(M) = A$. He finds a point x of X whose residue field k_x is a finite extension of F, such that the commutant of the image of Galois associated to the reduction $\overline{\mathscr{M}}_x$ is the same as for M. He then deduces that the absolute endomorphism ring $\mathrm{End}_{\bar{k}_x}(\overline{\mathscr{M}}_x)$ is equal to A, although this follows only for the endomorphism ring $\mathrm{End}_{k_x}(\overline{\mathscr{M}}_x)$ over k_x. This gap can be closed by exactly the same group theoretical argument as in the proof of Proposition 5.6 above.

Action of inertia on torsion points. The second gap is in the proof of [8, Proposition 4.5]. There, Gardeyn studies the action of the inertia group $\mathrm{I}_{\mathfrak{P}}$ on the Tate module of a one-dimensional formal τ-module over K. A typical example for this is the submodule of the Tate module of a Drinfeld module $T_{\mathfrak{p}}(\varphi)$ on which the tame inertia group acts non-trivially. On p. 327, line 6, Gardeyn considers the field $\tilde{L}_i^\circ$. But this field exists only if $\mathrm{Gal}(L_\infty/\tilde{L}_i)$ is normalized by the group J. If it were normalized for all i, we could deduce that $\tilde{L}_i = L_i$ for all i, which is not true in general. Several other problems within the proof of that proposition arise. We therefore give a reasonably complete independent proof of the proposition. It will be instructive to work in a slightly more general setting that includes the case of Lubin–Tate formal groups in mixed characteristic (see Abrashkin [1] or Fontaine [7]).

Let E be a non-archimedean local field with discrete valuation ring $\mathscr{O}$ and maximal ideal $\mathfrak{p} = (\pi)$. Let $k = \mathscr{O}/\mathfrak{p}$ denote the residue field of, say, order q and characteristic p. Let L be a maximal unramified extension of E, and L^{sep} a maximal separable extension of L. Let ψ be a formal Lubin–Tate group of $\mathscr{O}$-modules of height s over the ring of integers $\mathscr{O}_L$. For every integer $n \geqslant 1$, the π^n-torsion points $\psi[\pi^n](L^{\mathrm{sep}})$ form a free module of rank s over $\mathscr{O}/\mathfrak{p}^n$. Thus the Tate module

$$T := \varprojlim_n \psi\big[\pi^n\big]\big(L^{\mathrm{sep}}\big)$$

is a free module of rank s over $\mathscr{O}$ together with a continuous representation

$$\rho : \mathrm{Gal}\big(L^{\mathrm{sep}}/L\big) \to \mathrm{Aut}_{\mathscr{O}}(T) \cong \mathrm{GL}_s(\mathscr{O}).$$

All this applies to the modules $\psi[\pi^n](L^{\mathrm{sep}}) := \varphi[\pi^n]^\circ(L^{\mathrm{sep}})$ over $\mathscr{O} = A_{\mathfrak{p}}$ for a Drinfeld A-module over $\mathscr{O}_L$ with good reduction of height s.

The aim is to characterize the image of ρ under the stated general conditions. One basic ingredient is the following fact. Let v denote the valuation on L^{sep} for which $v(\pi) = 1$.

Lemma A.1. *For any $n \geqslant 1$ and any primitive element $t \in \psi[\pi^n](L^{\mathrm{sep}})$ we have*

$$v(t) = \frac{1}{q^{s(n-1)}(q^s - 1)}.$$

Proof. In the case of a Drinfeld module this was proved in Lemma 4.2 for $n \leqslant 2$. The same argument works for all n and all formal Lubin–Tate groups. □

Choose primitive elements $t_n \in \psi[\pi^n](L^{\mathrm{sep}})$ such that $\psi(\pi)(t_{n+1}) = t_n$ for all $n \geqslant 1$. For every $n \geqslant 1$ let L_n denote the finite extension of L generated by $\psi[\pi^n](L^{\mathrm{sep}})$, and let $L'_n \subset L_n$ denote the subfield generated by t_n.

Recall (e.g. from Serre [20, Chapter IV §2–3]) that the Galois group G of any finite local field extension possesses a natural decreasing lower numbering filtration G_μ indexed by $\mu \geqslant 0$. Via the Herbrand function φ (see [20, p. 80]) this filtration is translated into the upper number filtration G^μ such that $G_\mu = G^{\varphi(\mu)}$. We will say that the extension of G has break α for the lower numbering filtration if $G_\mu \subsetneqq G_\alpha$ for all $\mu > \alpha$, and that it has break α for the upper numbering filtration if $G^\mu \subsetneqq G^\alpha$ for all $\mu > \alpha$. Since $\varphi(\mu) = \mu$ whenever μ is less than or equal to the smallest break for the lower numbering filtration, we find that the lowest breaks for the two numberings coincide. In particular G has the unique break α for the lower numbering filtration if and only if it has the unique break α for the upper numbering filtration.

Lemma A.2. *For every $n \geqslant 1$, the element t_n is a uniformizer of L'_n. Moreover,*

(a) *we have $L'_1 = L_1$ and it is Galois over L of degree $q^s - 1$, and*
(b) *for every $n \geqslant 1$, the extension L'_{n+1}/L'_n is Galois of degree q^s with unique break $q^{sn} - 1$ (for either filtration).*

Proof. We work out the argument in the case of equal characteristic p, where addition and subtraction in the formal group coincide with the usual ones. In the mixed characteristic case they still coincide in first order approximation, which suffices to adapt the argument.

For any non-zero element $t \in \psi[\pi](L^{\mathrm{sep}})$ and any element σ in the wild ramification group of L we have $v(\sigma(t) - t) > v(t)$. Since $\sigma(t) - t$ is again an element of $\psi[\pi](L^{\mathrm{sep}})$, Lemma A.1 shows that it must be zero. Thus the wild ramification group acts trivially on L_1. In particular the extension L'_1/L is tame and hence Galois. The number of distinct conjugates of t_1 in L'_1/L is therefore equal to the ramification degree, and so by Lemma A.1 it is $\geqslant q^s - 1$. All these conjugates are non-zero elements of the group $\psi[\pi](L^{\mathrm{sep}})$ of order q^s. It follows that the number of conjugates is equal to $q^s - 1$ and that they generate L_1. This proves (a). Since the ramification degree is $q^s - 1$, it also follows that t_1 is a uniformizer of L'_1.

Fix any $n \geqslant 1$ and assume that t_n is a uniformizer of L'_n. Then Lemma A.1 implies that L'_{n+1}/L'_n has ramification degree $\geqslant q^s$. For any $\sigma \in \mathrm{Gal}(L^{\mathrm{sep}}/L'_n)$ we calculate

$$\pi\big(\sigma(t_{n+1}) - t_{n+1}\big) = \sigma(\pi t_{n+1}) - \pi t_{n+1} = \sigma(t_n) - t_n = 0,$$

which shows that all conjugates of t_{n+1} over L'_n lie in $t_{n+1} + \psi[\pi](L^{\mathrm{sep}})$. It follows that the number of conjugates is equal to q^s and that L'_{n+1} is Galois of degree q^s over L'_n and has uniformizer t_{n+1}. Furthermore, to any non-trivial element σ of $\mathrm{Gal}(L'_{n+1}/L'_n)$ is associated the non-zero element $\sigma(t_{n+1}) - t_{n+1} \in \psi[\pi](L^{\mathrm{sep}})$, and by comparing its valuation with that of t_{n+1} using Lemma A.1 we find that $\sigma(t_{n+1}) - t_{n+1}$ is a unit times $t_{n+1}^{q^{sn}}$. Now the definition of the higher ramification groups implies that $\mathrm{Gal}(L'_{n+1}/L'_n)$ has the unique break $q^{sn} - 1$ for the lower numbering filtration. By induction on n the lemma follows. □

By Lemma A.2(a) the Galois group $\mathrm{Gal}(L_1/L)$ has order prime to p, while $H := \rho(\mathrm{Gal}(L^{\mathrm{sep}}/L_1))$ is a pro-p group. Thus we can write the image of ρ as a semidirect product

$$\rho\big(\mathrm{Gal}\big(L^{\mathrm{sep}}/L\big)\big) = J \ltimes H.$$

The tameness implies that the group J is cyclic of order $q^s - 1$. Under the embedding $J \hookrightarrow \mathrm{Aut}_k(T/\mathfrak{p}T) \cong \mathrm{GL}_s(k)$ it is therefore identified with the multiplicative group of a field extension $k_s \subset \mathrm{End}_k(T/\mathfrak{p}T)$ of k of degree s. It follows that $\mathscr{O}J \subset \mathrm{End}_{\mathscr{O}}(T)$ is an unramified extension of $\mathscr{O}$ of degree s, turning T into a free module of rank 1 over $\mathscr{O}J$. Using this one finds a natural decomposition of the matrix ring

$$M := \mathrm{End}_{\mathscr{O}}(T) = \bigoplus_{i \in \mathbb{Z}/s\mathbb{Z}} M(i), \tag{A.3}$$

where $M(i) \cong \mathscr{O}J$ with the action of J by the character $u \mapsto u^{q^i - 1}$.

Theorem A.4. *In the above situation, there exists a function $m : \mathbb{Z}/s\mathbb{Z} \to \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$ satisfying $m(0) = 1$ and $m(i) + m(i') \geqslant m(i + i')$ for all i, i', such that*

$$\rho\big(\mathrm{Gal}\big(L^{\mathrm{sep}}/L\big)\big) = J \ltimes \Big(1 + \bigoplus_{i \in \mathbb{Z}/s\mathbb{Z}} \mathfrak{p}^{m(i)} M(i)\Big),$$

where we use the convention $\mathfrak{p}^{\infty} := (0)$.

The rest of the appendix is devoted to proving Theorem A.4.

Lemma A.5. *For every $i \in \mathbb{Z}/s\mathbb{Z}$ we set $\overline{M}(i) := M(i)/\mathfrak{p}M(i)$, which is a k_s-vector space of dimension 1 on which $J \cong k_s^*$ acts through the character $u \mapsto u^{q^i - 1}$.*

(a) *If $i \not\equiv 0 \bmod (s)$, then $\overline{M}(i)$ is a simple $\mathbb{F}_p[J]$-module.*
(b) *If $i \not\equiv i' \bmod (s)$, then $\overline{M}(i) \ncong \overline{M}(i')$ as $\mathbb{F}_p[J]$-modules.*

Proof. (Compare Gardeyn [8] or Fontaine [7].) The kernel of the character is the multiplicative group of the fixed field of the automorphism $k_s \to k_s$, $u \mapsto u^{q^i}$. For $i \not\equiv 0 \bmod (s)$ this is a proper subfield of k_s; hence the kernel has order $\leqslant q^{s/2} - 1$. Thus the image of the character has order $\geqslant (q^s - 1)/(q^{s/2} - 1) = q^{s/2} + 1$, and so it does not lie in a proper subfield of k_s. This implies (a). It also shows that J acts non-trivially on $\overline{M}(i)$, and hence $\overline{M}(i) \ncong \overline{M}(0)$. By symmetry it remains to prove (b) in the case $s > i > i' > 0$. Then the modules are isomorphic if and only if there exists j such that

$$u^{(q^i - 1)p^j} = u^{q^{i'} - 1}$$

for all $u \in k_s^*$. As k_s^* is cyclic of order $q^s - 1$, this amounts to the congruence

$$\big(q^i - 1\big)p^j \equiv q^{i'} - 1 \mod \big(q^s - 1\big).$$

Since $(q^i - 1)p^j > q^{i'} - 1$, it follows that $(q^i - 1)p^j \geqslant q^s - 1$. Therefore $q^i p^j$ is a multiple of q^s. A direct calculation shows that the remainder of $(q^i - 1)p^j$ under division by $q^s - 1$ is

$$q^s - p^j + q^i p^j q^{-s} - 1.$$

Thus this number is equal to $q^{i'}-1$, and so

$$q^s+q^ip^jq^{-s}=q^{i'}+p^j.$$

From this it is straightforward to deduce a contradiction. □

For every $n\geqslant 1$ we can view the Galois group $\mathrm{Gal}(L_{n+1}/L_n)$ as a subgroup of

$$\mathrm{Ker}\big(\mathrm{Aut}_{\mathcal{O}}\big(T/\mathfrak{p}^{n+1}T\big)\to\mathrm{Aut}_{\mathcal{O}}\big(T/\mathfrak{p}^nT\big)\big)\cong 1+\pi^n(M/\mathfrak{p}M)$$

and thus of the additive group $M/\mathfrak{p}M$. As this identification is J-equivariant, we obtain in fact an $\mathbb{F}_p[J]$-submodule of $M/\mathfrak{p}M$. The decomposition (A.3) yields a decomposition

$$\overline{M}:=M/\mathfrak{p}M\cong\bigoplus_{i\in\mathbb{Z}/s\mathbb{Z}}\overline{M}(i)$$

and thus a J-invariant decreasing filtration of $M/\mathfrak{p}M$ with subquotients $\overline{M}(i)$ for $1\leqslant i\leqslant s$. From this we deduce a J-invariant filtration

$$L_n=L_{n,0}\subset L_{n,1}\subset\cdots\subset L_{n,s-1}\subset L_{n,s}=L_{n+1}$$

such that $\mathrm{Gal}(L_{n,i}/L_{n,i-1})$ embeds into $\overline{M}(i)$ for every $1\leqslant i\leqslant s$.

Lemma A.6. *For every $n\geqslant 1$ and every $1\leqslant i\leqslant s-1$ the extension $L_{n,i}/L_{n,i-1}$ is either trivial or Galois of degree q^s with a unique break that is $\not\equiv 0$ modulo (q^s-1).*

Proof. If the extension is non-trivial, Lemma A.5(a) implies that its Galois group is isomorphic to $\overline{M}(i)$ and that its ramification filtration has a unique break, say α. Let $\tilde{\pi}$ be a uniformizer of $L_{n,i}$. Then the definition of the higher ramification groups yields a natural and hence J-equivariant embedding

$$\overline{M}(i)\cong\mathrm{Gal}(L_{n,i}/L_{n,i-1})\hookrightarrow(\tilde{\pi})^\alpha/(\tilde{\pi})^{\alpha+1},\quad \sigma\mapsto\frac{\sigma(\tilde{\pi})}{\tilde{\pi}}-1\mod(\tilde{\pi})^{\alpha+1}.$$

The tame ramification group J acts through a faithful character on $(\tilde{\pi})/(\tilde{\pi})^2$; hence it acts on $(\tilde{\pi})^\alpha/(\tilde{\pi})^{\alpha+1}$ through the αth power of that character. Since it acts non-trivially on $\overline{M}(i)$, we find that α cannot be a multiple of $|J|=|k_n^*|=q^s-1$. This finishes the proof. □

Lemma A.7. *Let F be a non-archimedean local field. Let F_1 and F_2 be two finite Galois extensions of degree d over F with unique breaks $\alpha_1\neq\alpha_2$. Then the extensions are linearly disjoint, and F_1F_2/F_2 is Galois of degree d with a unique break $\equiv\alpha_1$ modulo $(d-1)$, and F_1F_2/F_1 is Galois of degree d with a unique break $\equiv\alpha_2$ modulo $(d-1)$.*

Proof. Since the breaks are different, the functoriality of the upper numbering filtration (see [20, Chapter IV §3 Proposition 14]) implies that the upper numbering of the composite extension F_1F_2/F has the breaks α_1 and α_2 with index d each. It follows that the extensions are linearly disjoint and that F_1F_2/F_2 and F_1F_2/F_1 are Galois of degree d. By symmetry, we may without loss of generality assume that $\alpha_1>\alpha_2$, so that F_2 is the fixed field of $\mathrm{Gal}(F_1F_2/F)^{\alpha_1}$. Using the yoga of the Herbrand function φ (see [20, §3]) one calculates that the lower numbering of the extension F_1F_2/F then has the breaks α_2 and $\alpha_1+(q^s-1)(\alpha_1-\alpha_2)$ with index d each. It follows that F_1F_2/F_2 has the unique break $\alpha_1+(q^s-1)(\alpha_1-\alpha_2)\equiv\alpha_1$ modulo $(d-1)$ and that F_1F_2/F_1 has the unique break α_2. □

Lemma A.8. *For all $n\geqslant 1$ we have $[L_{n,s}/L_{n,s-1}]=q^s$.*

Proof. Consider the following assertions:

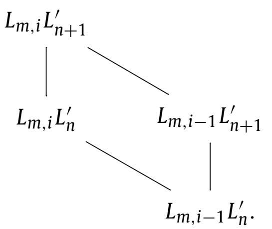
$A(n)$: $L_{n,s}=L_{n,s-1}L'_{n+1}$ and $[L_{n,s}/L_{n,s-1}]=q^s$.
$B(m,i,n)$: The extension $L_{m,i}L'_{n+1}/L_{m,i}L'_n$ is Galois of degree q^s with a unique break $\equiv 0$ modulo (q^s-1).
$C(m,i,n)$: The extension $L_{m,i}L'_n/L_{m,i-1}L'_n$ is either trivial or Galois of degree q^s with a unique break $\not\equiv 0$ modulo (q^s-1).

We will prove

$A(n)$ for all $n \geqslant 1$,
$B(m,i,n)$ for all $1 \leqslant m \leqslant n$ and $0 \leqslant i \leqslant s-1$, and
$C(m,i,n)$ for all $1 \leqslant m \leqslant n$ and $1 \leqslant i \leqslant s-1$.

Note first that $L'_n \subset L_{n,i-1} \subset L_{n,i}$; hence the assertion $C(n,i,n)$ is precisely Lemma A.6. In particular $C(m,i,n)$ holds whenever $n=1$. For all other assertions we use induction on n. We fix an integer $n \geqslant 1$ and assume $A(n')$ for all $n' < n$ and $C(m,i,n)$ for all m and i. We will then show $A(n)$ and $B(m,i,n)$ and $C(m,i,n+1)$ for all m and i. This proves the lemma, because the desired assertion is contained in $A(n)$.

Keeping n fixed we perform another induction over m and an innermost induction over i. We may thus fix $1 \leqslant m \leqslant n$ and $0 \leqslant i \leqslant s-1$ and assume $B(m',i',n)$ whenever $m' < m$ and $B(m,i',n)$ whenever $i' < i$. If $i=0$ and $m=1$, we note that $L_{1,0}=L_1=L'_1 \subset L'_n \subset L'_{n+1}$ by Lemma A.2(a); hence Lemma A.2(b) implies $B(1,0,n)$. If $i=0$ and $m>1$ we have $L_{m,0}=L_{m-1,s}=L_{m-1,s-1}L'_m$ by $A(m-1)$; since $L'_m \subset L'_n \subset L'_{n+1}$, the assertion $B(m-1,s-1,n)$ then implies $B(m,0,n)$. If $i>0$ we consider the field extensions



By $B(m,i-1,n)$ the right vertical extension is Galois of degree q^s with a unique break $\equiv 0$ modulo (q^s-1), and by $C(m,i,n)$ the lower oblique extension is either trivial or Galois of degree q^s with a unique break $\not\equiv 0$ modulo (q^s-1). If the lower extension is trivial, we can trivially deduce $B(m,i,n)$ and $C(m,i,n+1)$. Otherwise the two breaks are different; hence we can apply Lemma A.7 and again deduce $B(m,i,n)$ and $C(m,i,n+1)$.

By induction on m and i, we have thus proved $B(m,i,n)$ and $C(m,i,n+1)$ for all possible m and i except for $C(n+1,i,n+1)$. But that case was already covered at the beginning of the proof. Finally, consider the field extensions

$$L_{n,s-1} = L_{n,s-1}L'_n \subset L_{n,s-1}L'_{n+1} \subset L_{n+1} = L_{n,s}.$$

By construction the total extension has a subgroup of $\overline{M}(0)$ as Galois group; hence it has degree $\leqslant q^s$. But since the middle extension already has degree q^s by $B(n,s-1,n)$, it follows that the extension on the right is an equality and the total degree is q^s. This is just the assertion $A(n)$, finishing the proof. $\square$

Proof of Theorem A.4. Recall that for every $n \geqslant 1$ we have an $\mathbb{F}_p[J]$-equivariant embedding

$$\mathrm{Gal}(L_{n+1}/L_n) \hookrightarrow \overline{M} = \bigoplus_{i \in \mathbb{Z}/s\mathbb{Z}} \overline{M}(i).$$

Lemma A.5 implies that its image decomposes accordingly and that all its summands for $i \not\equiv 0 \bmod s$ are trivial or equal to $\overline{M}(i)$. Moreover, Lemma A.8 implies that the image contains the summand $\overline{M}(0)$. Together we deduce that

$$\mathrm{Gal}(L_{n+1}/L_n) \xrightarrow{\sim} \bigoplus_{i \in S(n)} \overline{M}(i)$$

for some subset $S(n) \subset \mathbb{Z}/s\mathbb{Z}$ with $0 \in S(n)$.

Next, the Lie bracket induces a map $\overline{M}(i) \times \overline{M}(i') \to \overline{M}(i+i')$ for all i and i', which is non-zero except for $i \equiv i' \equiv 0 \bmod s$. Using commutators as in Fontaine [7] or Gardeyn [8] or in Proposition 4.1 above, one finds that $i \in S(n)$ and $i' \in S(n')$ imply $i + i' \in S(n+n')$. Applying this with $n' = 1$ and $i' = 0 \in S(1)$ one deduces that $S(n) \subset S(n+1)$ for every $n \geqslant 1$. Thus with

$$m(i) := \inf\bigl\{n \geqslant 1\colon\ i \in S(n)\bigr\} \in \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$$

we have $m(0) = 1$ and $i \in S(n) \Leftrightarrow n \geqslant m(i)$. The above implication then implies that $m(i) + m(i') \geqslant m(i+i')$ for arbitrary i, i'. Thus the function m satisfies the first two conditions in Theorem A.4.

These conditions imply that

$$U := 1 + \bigoplus_{i \in \mathbb{Z}/s\mathbb{Z}} \mathfrak{p}^{m(i)} M(i)$$

is a J-invariant closed subgroup of $\mathrm{GL}_s(\mathcal{O})$ which possesses the same subquotients in the congruence filtration as H. It remains to show that $H = U$. For any $n \geqslant 1$ define

$$\begin{aligned}
G^n &:= 1 + \pi^n \mathrm{M}_s(\mathcal{O}),\\
G^{[n]} &:= G^n/G^{n+1} \cong \bigoplus_{i \in \mathbb{Z}/s\mathbb{Z}} \overline{M}(i),\\
H^{[n]} &:= \bigl(H \cap G^n\bigr)G^{n+1}/G^{n+1}, \quad \text{and}\\
U^{[n]} &:= \bigl(U \cap G^n\bigr)G^{n+1}/G^{n+1}.
\end{aligned}$$

By construction of the $m(i)$ the subgroup $H^{[n]}$ of $G^{[n]}$ consists of those summands $\overline{M}(i)$ with $m(i) \leqslant n$. Moreover, the subgroup HG^n/G^n of G^1/G^n is a successive extension of $n - m(i)$ copies of $\overline{M}(i)$ for all i with $m(i) < n$. In particular, Lemma A.5 implies that HG^n/G^n and $G^{[n]}/H^{[n]}$ possess no non-trivial isomorphic subquotient as $\mathbb{F}_p[J]$-module. It also implies that $H^{[n]} = U^{[n]}$. Suppose that $HG^n/G^n = UG^n/G^n$ as subgroups of G^1/G^n. Then we have an exact sequence

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G^{[n]}/H^{[n]} & \longrightarrow & HG^n/(H \cap G^n)G^{n+1} & \longrightarrow & HG^n/G^n & \longrightarrow & 1\\
 & & \| & & & & \| & & \\
 & & G^{[n]}/U^{[n]} & & & & UG^n/G^n & &
\end{array}$$

and each of H and U induces a J-equivariant splitting. As the extension is central, these splittings differ by a J-equivariant homomorphism $HG^n/G^n \to G^{[n]}/H^{[n]}$. But since these groups possess no non-trivial isomorphic subquotients, this homomorphism must be zero. This implies that

$HG^{n+1}/G^{n+1} = UG^{n+1}/G^{n+1}$ as subgroups of G^1/G^{n+1}. By induction we deduce that $H = U$, as desired. □

References

[1] V.G. Abrashkin, The image of the Galois group for some crystalline representations, Izv. Math. 63 (1) (1999) 1–36.
[2] G.W. Anderson, t-Motives, Duke Math. J. 53 (2) (1986) 457–502.
[3] H. Bass, J. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geqslant 3$) and Sp_{2n} ($n \geqslant 2$), Publ. Math. Inst. Hautes Études Sci. 33 (1967) 59–137.
[4] F. Breuer, R. Pink, Monodromy groups associated to non-isotrivial Drinfeld modules in generic characteristic, in: G. van der Geer, B. Moonen, R. Schoof (Eds.), Number Fields and Function Fields—Two Parallel Worlds, Birkhäuser, Boston, 2007.
[5] P. Deligne, D. Husemöller, Survey of Drinfeld Modules, in: Contemp. Math., vol. 67, 1987, pp. 25–91.
[6] V.G. Drinfeld, Elliptic modules, Mat. Sb. 94 (1974) 594–627 (in Russian); translated in Math. USSR Sb. 23 (1974) 561–592.
[7] J.M. Fontaine, Points d'ordre fini d'un groupe formel sur une extension non ramifiée de $\mathbb{Z}_p$, in: Journees Arithmetiques, Grenoble, 1973, Bull. Soc. Math. France Suppl. Mem. 37 (1974) 75–79.
[8] F. Gardeyn, Openness of the Galois image for τ-modules of dimension 1, J. Number Theory 102 (2003) 306–338.
[9] D. Goss, Basic Structures of Function Field Arithmetic, Springer-Verlag, Berlin, 1998.
[10] D.R. Hayes, Explicit class field theory in global function fields, in: Studies in Algebra and Number Theory, in: Adv. Math. Suppl. Stud., vol. 6, 1979, pp. 173–217.
[11] J.E. Humphreys, Linear Algebraic Groups, Springer-Verlag, New York, 1981.
[12] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.
[13] R. Pink, The Mumford–Tate conjecture for Drinfeld modules, Publ. Res. Inst. Math. Sci. 33 (3) (1997) 393–425.
[14] R. Pink, Compact subgroups of linear algebraic groups, J. Algebra 206 (2) (1998) 438–504.
[15] R. Pink, Strong approximation for Zariski dense subgroups over arbitrary global fields, Comment. Math. Helv. 75 (4) (2000) 608–643.
[16] R. Pink, E. Rütsche, Image of the group ring of the Galois representation associated to Drinfeld modules, J. Number Theory 129 (4) (2009) 866–881 (this issue).
[17] J.S. Rose, A Course on Group Theory, Dover, New York, 1994.
[18] E. Rütsche, Absolute irreducibility of the residual representation and Adelic openness in generic characteristic for Drinfeld modules, Diss. ETH Zurich, 2007.
[19] J.-P. Serre, Abelian ℓ-Adic Representations and Elliptic Curves, Benjamin, New York, 1968.
[20] J.-P. Serre, Corps Locaux, Hermann, Paris, 1968.
[21] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.
[22] J.-P. Serre, Lettre à Ken Ribet du 1/1/1981 et du 29/1/1981, in: Oeuvres, vol. IV, Springer-Verlag, Berlin, 2000, pp. 1–20.
[23] J.-P. Serre, Résumé des cours de 1985–1986, in: Annuaire du Collège de France (1986) 95–99 = Oeuvres, vol. IV, Springer-Verlag, Berlin, 2000, pp. 33–37.
[24] Y. Taguchi, The Tate conjecture for t-motives, Proc. Amer. Math. Soc. 123 (11) (1995) 3285–3287.
[25] Y. Taguchi, On ϕ-modules, J. Number Theory 60 (1996) 124–141.
[26] A. Tamagawa, The Tate conjecture for A-premotives, preprint, 1994.