The Galois Representations Associated to a Drinfeld Module in Special Characteristic, III: Image of the Group Ring

Richard Pink* Matthias Traulsen**

March 18, 2004

Abstract

Let K be a finitely generated field of transcendence degree 1 over a finite field, and set $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Let ϕ be a Drinfeld A-module over K in special characteristic. Set $E := \mathrm{End}_K(\phi)$ and let Z be its center. We show that for almost all primes $\mathfrak{p}$ of A, the image of the group ring $A_\mathfrak{p}[G_K]$ in $\mathrm{End}_A(T_\mathfrak{p}(\phi))$ is the commutant of E. Thus for almost all $\mathfrak{p}$ it is a full matrix ring over $Z \otimes_A A_\mathfrak{p}$. In the special case $E = A$ it follows that the representation of G_K on the $\mathfrak{p}$-torsion points $\phi[\mathfrak{p}]$ is absolutely irreducible for almost all $\mathfrak{p}$.

1 Introduction

For comparison let us briefly recall the situation for elliptic curves. Let E be an elliptic curve over a number field L without potential complex multiplication. For every rational prime ℓ let $E[\ell]$ denote its module of ℓ-torsion points and $T_\ell(E)$ its ℓ-adic Tate module. Both modules are free of rank 2 and carry natural Galois representations

$$\begin{aligned} \rho_\ell: \quad & G_L \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}\big(T_\ell(E)\big) \cong \mathrm{GL}_2(\mathbb{Z}_\ell), \\ \overline{\rho_\ell}: \quad & G_L \longrightarrow \mathrm{Aut}_{\mathbb{F}_\ell}\big(E[\ell]\big) \cong \mathrm{GL}_2(\mathbb{F}_\ell), \end{aligned}$$

where $G_L := \mathrm{Gal}(\bar{L}/L)$. Jean-Pierre Serre [13] proved that for almost all ℓ we have $\rho_\ell(G_L) = \mathrm{GL}_2(\mathbb{Z}_\ell)$. In particular, the residual representation $\overline{\rho_\ell}$ is absolutely irreducible for almost all ℓ.

With Drinfeld modules we are in a similar situation. Let ϕ be a Drinfeld A-module of rank r and characteristic $\mathfrak{p}_0$ over a finitely generated field K of transcendence degree 1. (Notations will be explained in Subsection 2.1.) Then for any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A with residue field $k_\mathfrak{p}$ we have natural Galois representations

$$\begin{aligned} \rho_\mathfrak{p}: \quad & G_K \longrightarrow \mathrm{Aut}_{A_\mathfrak{p}}\big(T_\mathfrak{p}(\phi)\big) \cong \mathrm{GL}_r(A_\mathfrak{p}), \\ \overline{\rho_\mathfrak{p}}: \quad & G_K \longrightarrow \mathrm{Aut}_{k_\mathfrak{p}}\big(\phi[\mathfrak{p}]\big) \cong \mathrm{GL}_r(k_\mathfrak{p}). \end{aligned}$$

If $\mathrm{End}_K(\phi) = A$, Yuichiro Taguchi [15], [16], [17] and Akio Tamagawa [19] proved that $\rho_\mathfrak{p}$ is absolutely irreducible over $\mathrm{Quot}(A_\mathfrak{p})$ for all $\mathfrak{p} \neq \mathfrak{p}_0$. Moreover, another result of Taguchi [15], [18] implies that $\overline{\rho_\mathfrak{p}}$ is irreducible for almost all $\mathfrak{p}$.

The purpose of this paper is to strengthen and generalize this result, assuming that ϕ has special characteristic. First we prove

*Dept. of Mathematics, ETH Zentrum, 8092 Zurich, Switzerland, pink@math.ethz.ch

**Dept. of Mathematics, ETH Zentrum, 8092 Zurich, Switzerland, traulsen@math.ethz.ch

Theorem A *Assume that* $\mathfrak{p}_0 \neq 0$ *and that* $\mathrm{End}_K(\phi) = A$. *Then for almost all primes* $\mathfrak{p}$ *of* A *the residual representation* $\overline{\rho_{\mathfrak{p}}}$ *is absolutely irreducible.*

We also generalize this to Drinfeld modules with arbitrary endomorphism ring. Of course, we can no longer expect that the residual representation is irreducible, let alone absolutely irreducible. We therefore read Theorem A as a statement on the image of the group ring. We will actually determine the image of the group ring on the full Tate module for almost all $\mathfrak{p}$. So let $B_{\mathfrak{p}}$ denote the image of the natural homomorphism

$$A_{\mathfrak{p}}[G_K] \longrightarrow \mathrm{End}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(\phi)\big).$$

Abbreviate $E := \mathrm{End}_K(\phi)$. For all $\mathfrak{p} \neq \mathfrak{p}_0$ the natural homomorphism

$$E_{\mathfrak{p}} := E \otimes_A A_{\mathfrak{p}} \longrightarrow \mathrm{End}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(\phi)\big)$$

is known to be injective (see Proposition 4.1), and by Taguchi [17] or Tamagawa [19] its image is the commutant of $B_{\mathfrak{p}}$. Let Z be the center of E, and write $c := [Z/A]$ and $e^2 = [E/Z]$. Then $d := r/ce$ is an integer. Set $Z_{\mathfrak{p}} := Z \otimes_A A_{\mathfrak{p}}$.

Theorem B *Assume that* $\mathfrak{p}_0 \neq 0$. *Then for almost all primes* $\mathfrak{p}$ *of* A *the rings* $E_{\mathfrak{p}}$ *and* $B_{\mathfrak{p}}$ *are commutants of each other in* $\mathrm{End}_{A_{\mathfrak{p}}}\big(T_{\mathfrak{p}}(\phi)\big)$. *More precisely, for almost all* $\mathfrak{p}$ *we have* $E_{\mathfrak{p}} \cong \mathrm{Mat}_{e\times e}(Z_{\mathfrak{p}})$ *and* $B_{\mathfrak{p}} \cong \mathrm{Mat}_{d\times d}(Z_{\mathfrak{p}})$.

Although the present proof applies only to Drinfeld modules in special characteristic, we expect that both theorems hold in generic characteristic as well. In fact, our proof of the implication Theorem A $\Longrightarrow$ Theorem B is valid in arbitrary characteristic. It actually simplifies in generic characteristic, because there the endomorphism ring is always commutative.

We also expect that both theorems extend to a finitely generated field K of arbitrary transcendence degree. In fact, our arguments do extend; the only missing ingredient is Taguchi's theorem on the isogeny conjecture, Theorem 2.2 below.

The article has three parts. Section 2 explains notations, lists various known ingredients, and translates Taguchi's theorem on the isogeny conjecture for Drinfeld modules into suitable statements for the Galois representations. In Section 3 we prove Theorem A under the stronger assumption $\mathrm{End}_{\overline{K}}(\phi) = A$. This is used in Section 4 to prove Theorem B. Finally, Theorem A in general follows directly from the special case $E = A$ of Theorem B. For an outline of the proofs see the introductions to Sections 3 and 4.

The material in this article was part of the doctoral thesis of the second author [20]. There it was applied to prove the isogeny conjecture for direct sums of Drinfeld modules in special characteristic. This application will be the subject of our article [12].

2 Some background

2.1 Notations

Throughout the article we use the following notation. Let p be a prime number and q a power of p. Let $\mathcal{C}$ and $\mathcal{X}$ be two smooth, irreducible, projective curves over the finite field $\mathbb{F}_q$ with q elements. By F and K we denote the respective function fields. We fix a closed point ∞ on $\mathcal{C}$ and let A be the ring of functions in F which are regular outside ∞.

Inside a fixed algebraic closure $\overline{K}$ of K we consider the following subextensions: the separable closure K^{sep}, the maximal abelian extension K^{ab}, the maximal unramified extension K^{nr} and the maximal unramified abelian extension $K^{\mathrm{ab,nr}}$. For every closed point $x \in \mathcal{X}$ we denote the completion of K at x by K_x and the valuation ring in K_x by $\mathcal{O}_x$. We let $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group of K.

Let k_0 be the field of constants of K. By $k_{0,d}$ we denote the field extension of k_0 of degree d. We set $G_K^{\mathrm{geom}} := \mathrm{Gal}(K^{\mathrm{sep}}/K\overline{k_0})$. The absolute Galois group $G_{k_0} = \mathrm{Gal}(\overline{k_0}/k_0)$ of k_0 is isomorphic to the Prüfer group $\widehat{\mathbb{Z}}$ and is topologically generated by the arithmetic Frobenius Frob_{k_0}. We have the short exact sequence

$$1 \to G_K^{\mathrm{geom}} \to G_K \to G_{k_0} \to 1.$$

By $K\{\tau\}$ we denote the twisted (noncommutative) polynomial ring in one variable, which satisfies the relation $\tau x = x^q \tau$ for all $x \in K$. Identifying τ with the endomorphism $x \mapsto x^q$, the ring $K\{\tau\}$ is isomorphic to the ring of $\mathbb{F}_q$-linear endomorphisms of the additive group scheme $\mathbb{G}_{a,K}$.

Throughout we will consider a Drinfeld A-module $\phi : A \to K\{\tau\}$, $a \mapsto \phi_a$ of rank r and characteristic $\mathfrak{p}_0$ over K. For the general theory of Drinfeld modules see Drinfeld [5] or Deligne-Husemöller [4]. For all nonzero ideals $\mathfrak{a}$ in A, we let

$$\phi[\mathfrak{a}] := \big\{x \in \overline{K} \;\big|\; \forall a \in \mathfrak{a}\colon \phi_a(x) = 0\big\}$$

denote the module of $\mathfrak{a}$-torsion of ϕ. If $\mathfrak{p}_0 \nmid \mathfrak{a}$, its points are defined over K^{sep} and form a free $A/\mathfrak{a}$-module of rank r. For any prime $\mathfrak{p}$ of A, we let $A_\mathfrak{p}$ denote the completion of A at $\mathfrak{p}$. For $\mathfrak{p} \neq \mathfrak{p}_0$ the $\mathfrak{p}$-adic Tate module $T_\mathfrak{p}(\phi) := \varprojlim \phi[\mathfrak{p}^n]$ of ϕ is a free $A_\mathfrak{p}$-module of rank r.

On all these modules there is a natural Galois action. In particular, for all $\mathfrak{p} \neq \mathfrak{p}_0$ we have continuous representations

$$\begin{aligned} \rho_\mathfrak{p} :\quad & G_K \longrightarrow \mathrm{Aut}_{A_\mathfrak{p}}\big(T_\mathfrak{p}(\phi)\big) \cong \mathrm{GL}_r(A_\mathfrak{p}), \\ \overline{\rho_\mathfrak{p}} :\quad & G_K \longrightarrow \mathrm{Aut}_{k_\mathfrak{p}}\big(\phi[\mathfrak{p}]\big) \cong \mathrm{GL}_r(k_\mathfrak{p}), \end{aligned}$$

where $k_\mathfrak{p} := A/\mathfrak{p}$ is the residue field at $\mathfrak{p}$. Clearly $\overline{\rho_\mathfrak{p}} \cong \rho_\mathfrak{p} \bmod \mathfrak{p}$. Both representations commute with the natural action of the endomorphism ring

$$E := \mathrm{End}_K(\phi) := \big\{u \in K\{\tau\} \;\big|\; \forall a \in A\colon \phi_a \circ u = u \circ \phi_a\big\}.$$

We will study these representations as $\mathfrak{p}$ varies, when ϕ has special characteristic.

2.2 Facts about Drinfeld modules

In the following, we recall selected results on the Galois representations associated to Drinfeld modules. We recover analogs of well-known results by Serre and Faltings for elliptic curves and abelian varieties. Let ϕ be as above.

Theorem 2.1 *(Pink [9] Prop. 2.6, [10] Theorem 1.1) Assume that* $\mathrm{End}_{\overline{K}}(\phi) = A$. *Then for all primes $\mathfrak{p} \neq \mathfrak{p}_0$ of A the image of $\rho_\mathfrak{p}$ is Zariski dense in* $\mathrm{GL}_{r,F_\mathfrak{p}}$.

In [9] Theorem 0.1 it is proved actually that the image is open in $\mathrm{GL}_r(F_\mathfrak{p})$, if moreover the characteristic $\mathfrak{p}_0$ is zero. A corresponding result in special characteristic is proved in Pink [11]. The next result concerns the isogeny conjecture for Drinfeld modules.

Theorem 2.2 *(Taguchi [15] Theorem 0.2, [18]) Up to K-isomorphism, there are only finitely many Drinfeld A-modules ϕ' for which there exists a K-isogeny $\phi \to \phi'$ of degree not divisible by $\mathfrak{p}_0$.*

This result can be translated into the following statements on Galois invariant submodules. Recall that every endomorphism of ϕ induces G_K-equivariant endomorphisms of $\phi[\mathfrak{p}^n]$ and of $T_\mathfrak{p}(\phi)$.

Proposition 2.3 *For almost all primes $\mathfrak{p}$ of A and all $n > 0$, every G_K-invariant $A/\mathfrak{p}^n$-submodule of $\phi[\mathfrak{p}^n]$ has the form $\alpha(\phi[\mathfrak{p}^n])$ for some $\alpha \in \mathrm{End}_K(\phi)$.*

Proof. Choose a finite set of representatives ϕ^i of the isomorphism classes of Drinfeld modules ϕ' in Theorem 2.2. For each i choose an isogeny $\varepsilon_i : \phi^i \to \phi$ of degree not divisible by $\mathfrak{p}_0$. Let S be the finite set of primes of A that divide the degree of one of these isogenies. We claim that the assertion holds for every $\mathfrak{p}$ outside $S \cup \{\mathfrak{p}_0\}$.

Fix such a prime $\mathfrak{p}$, a positive integer n, and a G_K-invariant $A/\mathfrak{p}^n$-submodule $H_\mathfrak{p} \subset \phi[\mathfrak{p}^n]$. Then there exists a Drinfeld A-module ϕ' over K and a separable K-isogeny $\eta : \phi \to \phi'$ with kernel $H_\mathfrak{p}$ (cf. Deligne-Husemöller [4] 4.1). By assumption, there is an isomorphism $\lambda : \phi' \stackrel{\sim}{\to} \phi^i$ for some i. The composite morphism $\beta := \varepsilon_i \circ \lambda \circ \eta$ is then a separable endomorphism of ϕ. Since by assumption $\mathfrak{p}$ does not divide the degree of ε_i, the isogeny ε_i induces an isomorphism $\phi^i[\mathfrak{p}^n] \stackrel{\sim}{\to} \phi[\mathfrak{p}^n]$; hence the $\mathfrak{p}$-primary part of $\ker \beta$ is equal to $H_\mathfrak{p}$.

In particular, the $\mathfrak{p}$-primary part of $\ker \beta$ is annihilated by $\mathfrak{p}^n$. Therefore we can find an element $a \in \mathfrak{p}^n \smallsetminus \mathfrak{p}^{n+1}$ that annihilates $\ker \beta$. Then by Deligne-Husemöller [4] 4.1 there exists an endomorphism α of ϕ such that $\beta \circ \alpha = \phi_a$ and $\ker \beta = \alpha(\phi[a])$. Taking $\mathfrak{p}$-primary parts, the last equality implies that $H_\mathfrak{p} = \alpha(\phi[\mathfrak{p}^n])$, as desired.

q.e.d.

The case $n = 1$ of Proposition 2.3 yields in particular

Corollary 2.4 *Assume that $\mathrm{End}_K(\phi) = A$. Then the representation $\overline{\rho_\mathfrak{p}}$ is irreducible for almost all primes $\mathfrak{p}$ of A.*

Proposition 2.5 *For almost all primes $\mathfrak{p}$ of A, every G_K-invariant $A_\mathfrak{p}$-submodule of $T_\mathfrak{p}(\phi)$ has the form $\alpha(T_\mathfrak{p}(\phi))$ for some $\alpha \in \mathrm{End}_K(\phi) \otimes_A A_\mathfrak{p}$.*

Proof. Let $\mathfrak{p}$ be as in Proposition 2.3, and consider any $A_\mathfrak{p}[G_K]$-submodule $H_\mathfrak{p} \subset T_\mathfrak{p}(\phi)$. For all $n \geq 0$ we have $T_\mathfrak{p}(\phi)/\mathfrak{p}^n T_\mathfrak{p}(\phi) \cong \phi[\mathfrak{p}^n]$; hence by Proposition 2.3 we have

$$H_\mathfrak{p} + \mathfrak{p}^n T_\mathfrak{p}(\phi) = \alpha_n(T_\mathfrak{p}(\phi)) + \mathfrak{p}^n T_\mathfrak{p}(\phi)$$

for some $\alpha_n \in E$. Since $E_\mathfrak{p}$ is compact, we can choose a subsequence α_{n_i} which converges to an element $\alpha \in E_\mathfrak{p}$. This convergence means that $\alpha_{n_i} \equiv \alpha \bmod \mathfrak{p}^{m_i} E_\mathfrak{p}$ with $m_i \to \infty$. Setting $\ell_i := \min\{n_i, m_i\}$, we deduce that

$$H_\mathfrak{p} + \mathfrak{p}^{\ell_i} T_\mathfrak{p}(\phi) = \alpha(T_\mathfrak{p}(\phi)) + \mathfrak{p}^{\ell_i} T_\mathfrak{p}(\phi)$$

for all i. Now as $\ell_i \to \infty$, the $\mathfrak{p}^{\ell_i} T_\mathfrak{p}(\phi)$ run through a fundamental system of neighborhoods of 0. Since $E_\mathfrak{p}$ is compact, and $H_\mathfrak{p}$ and $\alpha(T_\mathfrak{p}(\phi))$ are closed submodules of $T_\mathfrak{p}(\phi)$, we deduce that

$$H_\mathfrak{p} \;=\; \bigcap_i \big(H_\mathfrak{p} + \mathfrak{p}^{\ell_i} T_\mathfrak{p}(\phi)\big) \;=\; \bigcap_i \big(\alpha(T_\mathfrak{p}(\phi)) + \mathfrak{p}^{\ell_i} T_\mathfrak{p}(\phi)\big) \;=\; \alpha(T_\mathfrak{p}(\phi)),$$

as desired. **q.e.d.**

We also need information on the action of inertia and Frobenius. Let $\mathcal{U}$ be an open dense subscheme of $\mathcal{X}$ over which ϕ has good reduction.

Proposition 2.6 *(Cf. Goss [6] 4.12.12 (2)) Consider a point $x \in \mathcal{U}(k_{0,d})$. Then for every prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A not below x, the representation $\rho_\mathfrak{p}$ is unramified at x, and the characteristic polynomial of $\rho_\mathfrak{p}(\mathrm{Frob}_x)$ has coefficients in A and is independent of $\mathfrak{p}$.*

We denote this characteristic polynomial by f_x.

Proposition 2.7 *Assume that $\mathfrak{p}_0 \neq 0$. Then after replacing K by a suitable finite extension, for all primes $\mathfrak{p} \neq \mathfrak{p}_0$ of A and all closed points $x \in \mathcal{X}$, the restriction of $\rho_\mathfrak{p}$ to the inertia group at x is unipotent.*

Proof. For $x \in \mathcal{U}$ this follows from Proposition 2.6, even without extending K. Fix one of the remaining points $x \in \mathcal{X} \smallsetminus \mathcal{U}$ and consider the Tate uniformization (ψ, Λ) of ϕ, where ψ is a Drinfeld module of rank $r' \leq r$ over K_x which has potentially good reduction, and Λ is an A-lattice in K_x^{sep} via ψ of rank $r - r'$ which is invariant under G_{K_x} (cf. Drinfeld [5] §7). Then for every prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A there is a natural G_{K_x}-equivariant short exact sequence

$$0 \to T_\mathfrak{p}(\psi) \to T_\mathfrak{p}(\phi) \to \Lambda \otimes_A A_\mathfrak{p} \to 0.$$

Choose a finite extension L_x of K_x over which ψ acquires good reduction and which contains Λ. Since the reduction of ψ again has characteristic $\mathfrak{p}_0$, which is different from $\mathfrak{p}$, the inertia group of L_x acts trivially on $T_\mathfrak{p}(\psi)$. It also acts trivially on $\Lambda \otimes_A A_\mathfrak{p}$; hence it acts unipotently on $T_\mathfrak{p}(\phi)$.

Now as there are only finitely many points $x \in \mathcal{X} \smallsetminus \mathcal{U}$, there exists a normal finite extension K' of K whose local extension at each of these x contains L_x. Let $\mathcal{X}' \to \mathcal{X}$ be the corresponding finite covering. Then for every closed point $x' \in \mathcal{X}'$ above a point $x \in \mathcal{X}$ we either have $x \in \mathcal{U}$ or the local field $K'_{x'}$ contains L_x. In both cases the inertia group at x' acts unipotently, as desired. **q.e.d.**

2.3 Equidistribution of Frobenius elements

As a further ingredient we briefly recall Deligne's theorem on the equidistribution of Frobenius elements. As before let K be a function field of transcendence degree 1 over a finite field k_0. Let K'/K be a finite Galois extension with Galois group Γ. Let $\Gamma^\natural$ denote the set of conjugacy classes of Γ. Let $\mu^\natural$ be the direct image of the Haar measure on Γ of total volume 1, which satisfies $\mu^\natural(C) = |C|/|\Gamma|$ for every conjugacy class $C \in \Gamma^\natural$.

Let $\pi : \mathcal{X}' \to \mathcal{X}$ be the corresponding covering of smooth, projective, irreducible curves over k_0. Fix an open dense subscheme $\mathcal{U} \subset \mathcal{X}$ over which π is unramified. Then every closed point $x \in \mathcal{U}$ determines a Frobenius element $\mathrm{Frob}_x \in \Gamma$ which is unique up to conjugation, i.e., a unique element $[\mathrm{Frob}_x] \in \Gamma^\natural$. The Čebotarev density theorem says that every $C \in \Gamma^\natural$ occurs as Frobenius for a set of x of positive Dirichlet density $\mu^\natural(C)$.

We will need the following strengthening that takes the degrees of points into account. Recall that $k_{0,d}$ denotes the field extension of k_0 of degree d. Then there is also a Frobenius $\mathrm{Frob}_x \in \Gamma$ associated to every point $x \in \mathcal{U}(k_{0,d})$. Set

$$\mu_d^\natural := \frac{1}{|\mathcal{U}(k_{0,d})|} \cdot \sum_{x \in \mathcal{U}(k_{0,d})} \delta([\mathrm{Frob}_x]),$$

where $\delta(C)$ denotes the Dirac delta measure supported at C.

Theorem 2.8 *If the extension of constant fields in K'/K is trivial, the sequence of measures $\mu_d^\natural$ converges to $\mu^\natural$ as $d \to \infty$.*

Corollary 2.9 *If the extension of constant fields in K'/K is trivial, then for every $d \gg 0$, the Frobeniuses associated to $x \in \mathcal{U}_d$ meet all conjugacy classes in Γ.*

Theorem 2.8 is a special case of a general equidistribution theorem of Deligne [3] Théorème 3.5.3. A proof in the curve case can also be found in Katz [7] Chapter 3. Let us briefly explain how to deduce Theorem 2.8 from this general result.

Fix any rational prime $\ell \neq p$. Then $\mathcal{F} := (\pi_* \overline{\mathbb{Q}}_\ell)|\mathcal{U}$ is a lisse étale $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathcal{U}$ with finite monodromy group Γ, corresponding to the regular representation of Γ over $\overline{\mathbb{Q}}_\ell$. Since Γ is finite, all eigenvalues of its elements are roots of unity; hence $\mathcal{F}$ is pointwise pure of weight 0 in the sense of Deligne [3]. Moreover, since Γ is finite, all elements act semisimply. Furthermore, if the extension of constant fields in K'/K is trivial, the geometric étale fundamental group $\pi_1(\mathcal{U} \times \bar{k}_0)$ maps surjectively to Γ. Now Theorem 2.8 is a special case of Deligne's equidistribution theorem in the form of Katz [7] Theorem 3.6.

3 Absolute irreducibility of the residual representation

From now on and for the rest of this paper, we assume that $\mathfrak{p}_0 \neq 0$. In the present section we also assume that $\mathrm{End}_{\overline{K}}(\phi) = A$. Note that this is stronger than $\mathrm{End}_K(\phi) = A$. We will prove the following special case of Theorem A:

Theorem 3.1 *Assume that $\mathrm{End}_{\overline{K}}(\phi) = A$. Then for almost all primes $\mathfrak{p}$ of A the representation*

$$\overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow \mathrm{Aut}_{k_{\mathfrak{p}}}\big(\phi[\mathfrak{p}]\big)$$

is absolutely irreducible.

The idea of the proof is this: If $\overline{\rho_{\mathfrak{p}}}$ is irreducible, but not absolutely irreducible, we can consider it as a representation of some smaller dimension $s_{\mathfrak{p}}$ over an extension of $k_{\mathfrak{p}}$. The determinant of this representation is then an abelian character $\overline{\chi_{\mathfrak{p}}}$. Using information on the ramification in $\rho_{\mathfrak{p}}$ we show that $\overline{\chi_{\mathfrak{p}}}$ essentially comes from an abelian character of G_{k_0}. This means that for any finite extension $k_{0,d}$ of k_0, the value $\overline{\chi_{\mathfrak{p}}}(\mathrm{Frob}_x)$ for $x \in \mathcal{X}(k_{0,d})$ is independent of x. For the original representation this implies that some product of $s_{\mathfrak{p}}$ eigenvalues of $\rho_{\mathfrak{p}}(\mathrm{Frob}_x)$ modulo $\mathfrak{p}$ is independent of x.

Now the eigenvalues of $\rho_{\mathfrak{p}}(\mathrm{Frob}_x)$ are integral over A and independent of $\mathfrak{p}$, and there are only finitely many ways to choose less than r of them. Thus if the above happens for infinitely many $\mathfrak{p}$, there must exist an actual equality over A, i.e., a non-trivial algebraic relation between the eigenvalues of $\rho_{\mathfrak{p}}(\mathrm{Frob}_x)$ for any two points $x \in \mathcal{X}(k_{0,d})$. Using Deligne's equidistribution theorem, we finally show that this contradicts the fact that $\rho_{\mathfrak{p}}(G_K)$ is Zariski dense in GL_r.

In order to work in A rather than in a varying finite extension of A, we do not deal with the eigenvalues directly, but with the coefficients of the characteristic polynomial. The algebraic relation is then expressed as the vanishing of a certain resultant. To obtain the contradiction, it suffices to compare the image of a general element of G_K^{geom} with the image of the identity element.

3.1 The setup

By Corollary 2.4 the residual representation $\overline{\rho_{\mathfrak{p}}}$ is irreducible for almost all $\mathfrak{p}$. By Schur's lemma, for these primes the ring $\mathrm{End}_{k_{\mathfrak{p}}}(\overline{\rho_{\mathfrak{p}}})$ is a finite dimensional division algebra over the residue field $k_{\mathfrak{p}}$. Since $k_{\mathfrak{p}}$ is finite, every finite dimensional division algebra over $k_{\mathfrak{p}}$ is a commutative field. Therefore $\mathrm{End}_{k_{\mathfrak{p}}}(\overline{\rho_{\mathfrak{p}}})$ is a finite field extension of $k_{\mathfrak{p}}$ of some degree $s_{\mathfrak{p}}$. We denote this extension field by $k_{\mathfrak{p},s_{\mathfrak{p}}}$ and observe that $s_{\mathfrak{p}}$ must divide r. Setting $t_{\mathfrak{p}} := rs_{\mathfrak{p}}^{-1}$ we note that $\overline{\rho_{\mathfrak{p}}}$ factors through $\mathrm{GL}_{t_{\mathfrak{p}}}(k_{\mathfrak{p},s_{\mathfrak{p}}}) \subset \mathrm{GL}_r(k_{\mathfrak{p}})$.

To prove Theorem 3.1 we must show that $s_{\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$. In order to develop an indirect proof, we make the following

Assumption 3.2 *There exist $s > 1$ and t with $st = r$ and an infinite set S of primes of A such that for all $\mathfrak{p} \in S$ the representation $\overline{\rho_{\mathfrak{p}}}$ factors through $\mathrm{GL}_t(k_{\mathfrak{p},s})$.*

For $\mathfrak{p} \in S$ we can consider $\overline{\rho_{\mathfrak{p}}}$ as a homomorphism $G_K \to \mathrm{GL}_t(k_{\mathfrak{p},s})$. We write

$$\det_s : \mathrm{GL}_t\big(k_{\mathfrak{p},s}\big) \longrightarrow k_{\mathfrak{p},s}^*$$

for the determinant map and consider the composite homomorphism

$$\overline{\chi_{\mathfrak{p}}} := \det_s \circ \overline{\rho_{\mathfrak{p}}} : G_K \longrightarrow k_{\mathfrak{p},s}^*.$$

Lemma 3.3 *There is a finite field extension K'/K such that for every prime $\mathfrak{p} \in S$ the character $\overline{\chi_{\mathfrak{p}}}$ is trivial on $G_{K'}^{\mathrm{geom}}$.*

Proof. Proposition 2.7 implies that there is a finite extension K_1/K such that for all closed points $x \in \mathcal{X}$ the inertia subgroup of G_{K_1} at x has trivial image in $k_{\mathfrak{p},s}^*$, so the restriction of $\overline{\chi_{\mathfrak{p}}}$ to G_{K_1} is unramified everywhere. This means that $\overline{\chi_{\mathfrak{p}}}|_{G_{K_1}}$ factors through $\mathrm{Gal}(K_1^{\mathrm{nr}}/K_1)$. Moreover, it obviously factors through the maximal abelian quotient $\mathrm{Gal}(K_1^{\mathrm{ab,nr}}/K_1)$.

Further, the image of $G_{K_1}^{\mathrm{geom}}$ in $\mathrm{Gal}(K_1^{\mathrm{ab,nr}}/K_1)$ is finite by Katz-Lang [8] Theorem 2. Therefore $\overline{\chi_{\mathfrak{p}}}|_{G_{K_1}^{\mathrm{geom}}}$ has finite order, and so the restriction to some finite extension K' of K_1 is trivial, as desired. **q.e.d.**

It is sufficient to prove Theorem 3.1 for the restriction of $\overline{\rho_{\mathfrak{p}}}$ to an open subgroup of G_K, thus we can replace K by a finite field extension. We replace K by the extension field K' constructed in Lemma 3.3. Then for all $\mathfrak{p}$ in S the character $\overline{\chi_{\mathfrak{p}}}$ factors through a homomorphism $\overline{\overline{\chi_{\mathfrak{p}}}} : G_{k_0} \to k_{\mathfrak{p},s}^*$. The following commutative diagram with exact rows sums up the various mappings:

$$\begin{tikzcd}
1 \arrow[r] & G_K^{\mathrm{geom}} \arrow[r] \arrow[d] & G_K \arrow[r] \arrow[d, "\overline{\rho_{\mathfrak{p}}}"'] \arrow[dr, "\overline{\chi_{\mathfrak{p}}}"] & G_{k_0} \arrow[r] \arrow[d, "\overline{\overline{\chi_{\mathfrak{p}}}}"] & 1 \\
1 \arrow[r] & \mathrm{SL}_t\big(k_{\mathfrak{p},s}\big) \arrow[r] \arrow[d, hook] & \mathrm{GL}_t\big(k_{\mathfrak{p},s}\big) \arrow[r, "\det_s"'] \arrow[d, hook] & k_{\mathfrak{p},s}^* \arrow[r] \arrow[d, "\mathrm{Norm}"] & 1 \\
1 \arrow[r] & \mathrm{SL}_r\big(k_{\mathfrak{p}}\big) \arrow[r] & \mathrm{GL}_r\big(k_{\mathfrak{p}}\big) \arrow[r, "\det"] & k_{\mathfrak{p}}^* \arrow[r] & 1
\end{tikzcd}$$

3.2 Algebraic relations in GL_r

For any monic polynomial $f(T) = \prod_{i=1}^r (T - \alpha_i)$ of degree r and any integer $t > 0$ we set

$$f^{(t)}(T) := \prod_I \Big(T - \prod_{i \in I} \alpha_i\Big),$$

where the outer product ranges over all subsets $I \subset \{1, \ldots, r\}$ of cardinality t. Clearly the coefficients of $f^{(t)}$ are symmetric polynomials in the α_i, hence they are polynomials with coefficients in $\mathbb{Z}$ in the coefficients of f. The construction can therefore be applied to any monic polynomial with coefficients in any commutative ring. If f has coefficients in an algebraically closed field, then $f^{(t)}(\alpha) = 0$ if and only if f has t zeros with product α.

In the next lemma, we use Assumption 3.2 that S is infinite. Recall that f_x denotes the characteristic polynomial of $\rho_{\mathfrak{p}}(\mathrm{Frob}_x)$. Recall also that two polynomials have a common zero if and only if their resultant vanishes.

Lemma 3.4 *For all $d > 0$ and all $x, x' \in \mathcal{U}(k_{0,d})$ the resultant of the polynomials $f_x^{(t)}$ and $f_{x'}^{(t)}$ vanishes.*

Proof. Let $\mathfrak{p} \in S$. By Lemma 3.3, we know that

$$\overline{\chi_{\mathfrak{p}}}(\mathrm{Frob}_x) = \overline{\overline{\chi_{\mathfrak{p}}}}(\mathrm{Frob}_{k_0}^d) = \overline{\chi_{\mathfrak{p}}}(\mathrm{Frob}_{x'}),$$

so the determinants of $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_x)$ and $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_{x'})$ over $k_{\mathfrak{p},s}^*$ are equal. Thus, if we consider $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_x)$ and $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_{x'})$ as elements of $\mathrm{GL}_t(k_{\mathfrak{p},s})$, their characteristic polynomials g_x and $g_{x'}$ have the same constant term. This means that the product of the t zeros of g_x equals the product of the t zeros of $g_{x'}$.

Now the polynomials f_x and $f_{x'}$ are congruent modulo $\mathfrak{p}$ to the characteristic polynomials of $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_x)$ and $\overline{\rho_{\mathfrak{p}}}(\mathrm{Frob}_{x'})$ as elements of $\mathrm{GL}_r(k_{\mathfrak{p}})$, respectively. So g_x and $g_{x'}$ divide f_x and $f_{x'}$ modulo $\mathfrak{p}$, respectively, as polynomials over $\overline{k_{\mathfrak{p}}}$. Therefore $f_x^{(t)}$ and $f_{x'}^{(t)}$ must have a common zero modulo $\mathfrak{p}$; hence their resultant vanishes modulo $\mathfrak{p}$. Since this happens for the infinitely many $\mathfrak{p} \in S$, the assertion follows. **q.e.d.**

Next we use Lemma 3.4 to analyze the representation at any fixed prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A. For $n > 0$ we denote the images of the Galois groups G_K and G_K^{geom} under the representation $\rho_{\mathfrak{p}}$ modulo $\mathfrak{p}^n$ by $\Gamma_{\mathfrak{p},n}$ and $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$, respectively. We set $\Gamma''_{\mathfrak{p},n} := \Gamma_{\mathfrak{p},n}/\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$ and obtain the following diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G_K^{\mathrm{geom}} & \longrightarrow & G_K & \longrightarrow & G_{k_0} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Gamma_{\mathfrak{p},n}^{\mathrm{geom}} & \longrightarrow & \Gamma_{\mathfrak{p},n} & \longrightarrow & \Gamma''_{\mathfrak{p},n} & \longrightarrow & 1 \\
 & & \cap & & \cap & & & & \\
 & & \mathrm{SL}_r(A/\mathfrak{p}^n) & & \mathrm{GL}_r(A/\mathfrak{p}^n) & & & &
\end{array}$$

In order to apply Lemma 3.4, we need to approximate pairs of elements of $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$ by pairs of Frobenius elements of the same degree. This result is independent of Assumption 3.2.

Lemma 3.5 *For every $\mathfrak{p}$ and n there exists $d > 0$ such that every element of $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$ is the image of Frob_x for some $x \in \mathcal{U}(k_{0,d})$.*

Proof. Let $K_{\mathfrak{p},n}$ be the finite Galois extension of K with Galois group $\Gamma_{\mathfrak{p},n}$. Then its constant field is $k_{0,e}$ for $e := |\Gamma''_{\mathfrak{p},n}|$, and $K_{\mathfrak{p},n}/Kk_{0,e}$ is a finite Galois extension with Galois group $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$ whose extension of constant fields is trivial. By Proposition 2.6 it is unramified over $\mathcal{U}$. Applying Corollary 2.9 to $\mathcal{U} \times_{k_0} k_{0,e}$, we can find a multiple d of e such that the Frobeniuses associated to $x \in \mathcal{U}(k_{0,d})$ meet all conjugacy classes in $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$. **q.e.d.**

Now let

$$\Gamma_{\mathfrak{p}} \subset \mathrm{GL}_r(A_{\mathfrak{p}}) \quad \text{and} \quad \Gamma_{\mathfrak{p}}^{\mathrm{geom}} \subset \mathrm{SL}_r(A_{\mathfrak{p}})$$

be the projective limits of $\Gamma_{\mathfrak{p},n}$ and $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$ for $n \to \infty$.

Lemma 3.6 *Let $\gamma \in \Gamma_{\mathfrak{p}}^{\mathrm{geom}}$ and let f_γ be its characteristic polynomial. Then $f_\gamma^{(t)}(1)$ vanishes.*

Proof. For any $n > 0$ choose $d > 0$ as in Lemma 3.5. Then we can find x, $x' \in \mathcal{U}(k_{0,d})$ such that Frob_x maps to $\gamma \bmod \mathfrak{p}^n$ and $\mathrm{Frob}_{x'}$ to the identity element in $\Gamma_{\mathfrak{p},n}^{\mathrm{geom}}$. Setting $h(T) := (T-1)^r$, we get

$$f_x \equiv f_\gamma \pmod{\mathfrak{p}^n} \quad \text{and} \quad f_{x'} \equiv h \pmod{\mathfrak{p}^n}.$$

Thus

$$f_x^{(t)} \equiv f_\gamma^{(t)} \pmod{\mathfrak{p}^n}$$

and

$$f_{x'}^{(t)} \equiv h^{(t)} = (T-1)^{\binom{r}{t}} \pmod{\mathfrak{p}^n}.$$

By Lemma 3.4 the resultant of $f_x^{(t)}$ and $f_{x'}^{(t)}$ vanishes; hence the resultant of $f_\gamma^{(t)}$ and $(T-1)^{\binom{r}{t}}$ is congruent 0 modulo $\mathfrak{p}^n$. Since this is so for all n, the latter resultant must vanish. But this implies that $f_\gamma^{(t)}(1) = 0$. **q.e.d.**

3.3 Conclusion

Now we exploit the Zariski density statement from Theorem 2.1.

Lemma 3.7 *The commutator morphism*

$$\begin{aligned} [\,\cdot\,,\,\cdot\,] : \mathrm{GL}_r \times \mathrm{GL}_r &\longrightarrow \mathrm{SL}_r \\ (x,y) &\longmapsto [x,y] = yxy^{-1}x^{-1} \end{aligned}$$

is dominant.

Proof. It is known that the morphism $y \mapsto yxy^{-1}x^{-1}$ for fixed x has differential $1 - \mathrm{Ad}\,x$. In turn, $x \mapsto \mathrm{Ad}\,x(Y) - Y$ has differential $-\mathrm{ad}\,Y$, where $\mathrm{ad}\,Y(Z)$ is the Lie bracket on $\mathfrak{gl}_r$. (For both results see, e.g., Borel [1] I 3.16.)

Rather elementary computation shows that the Lie bracket is a surjective morphism $\mathfrak{gl}_r \oplus \mathfrak{gl}_r \to \mathfrak{sl}_r$. But the surjectivity of this differential implies that $[\,\cdot\,,\,\cdot\,]$ is dominant (Springer [14] Theorem 4.3.6). **q.e.d.**

Lemma 3.8 $\Gamma_{\mathfrak{p}}^{\mathrm{geom}}$ *is Zariski dense in* $\mathrm{SL}_{r,F_{\mathfrak{p}}}$.

Proof. All commutators of G_K are contained in G_K^{geom}, so the image of $\Gamma_{\mathfrak{p}} \times \Gamma_{\mathfrak{p}}$ under the commutator morphism

$$[\,\cdot\,,\,\cdot\,] : \mathrm{GL}_{r,F_{\mathfrak{p}}} \times \mathrm{GL}_{r,F_{\mathfrak{p}}} \to \mathrm{SL}_{r,F_{\mathfrak{p}}}$$

is contained in $\Gamma_{\mathfrak{p}}^{\mathrm{geom}}$. Furthermore $\Gamma_{\mathfrak{p}}$ is Zariski dense in $\mathrm{GL}_{r,F_{\mathfrak{p}}}$ by Theorem 2.1. We get

$$\big[\mathrm{GL}_{r,F_{\mathfrak{p}}}, \mathrm{GL}_{r,F_{\mathfrak{p}}}\big] = \big[\,\overline{\Gamma_{\mathfrak{p}}}, \overline{\Gamma_{\mathfrak{p}}}\,\big] \subset \overline{\big[\Gamma_{\mathfrak{p}}, \Gamma_{\mathfrak{p}}\big]} \subset \overline{\Gamma_{\mathfrak{p}}^{\mathrm{geom}}}.$$

Lemma 3.7 tells us that $[\,\cdot\,,\,\cdot\,]$ is dominant; hence

$$\mathrm{SL}_{r,F_{\mathfrak{p}}} = \overline{\big[\mathrm{GL}_{r,F_{\mathfrak{p}}}, \mathrm{GL}_{r,F_{\mathfrak{p}}}\big]} \subset \overline{\Gamma_{\mathfrak{p}}^{\mathrm{geom}}} \subset \mathrm{SL}_{r,F_{\mathfrak{p}}}.$$

We therefore have equality. **q.e.d.**

We are now ready to draw the desired conclusion:

Proof of Theorem 3.1. For $g \in \mathrm{GL}_{r,F_\mathfrak{p}}$ we denote the characteristic polynomial by f_g. Then

$$\psi : \mathrm{GL}_{r,F_\mathfrak{p}} \to \mathbb{A}^1_{F_\mathfrak{p}},\ g \mapsto f_g^{(t)}(1)$$

is a morphism of algebraic varieties. Its restriction to $\mathrm{SL}_{r,F_\mathfrak{p}}$ is non-constant, for instance because its value on the following kind of diagonal matrices is

$$\psi \begin{pmatrix} \alpha & & & \\ & \ddots & & \\ & & \alpha & \\ & & & \alpha^{-r+1} \end{pmatrix} = \bigl(1-\alpha^t\bigr)^{\binom{r-1}{t}} \cdot \bigl(1-\alpha^{t-r}\bigr)^{\binom{r-1}{t-1}}.$$

On the other hand, by Lemmata 3.6 and 3.8 we know that $\psi(\Gamma_\mathfrak{p}^{\mathrm{geom}}) = 0$ and that $\Gamma_\mathfrak{p}^{\mathrm{geom}}$ is Zariski dense in $\mathrm{SL}_{r,F_\mathfrak{p}}$. In view of this contradiction, Assumption 3.2 turns out to be false, and the theorem is proven. **q.e.d.**

4 The case of an arbitrary endomorphism ring

In this section we will prove Theorem B, where $E := \mathrm{End}_K(\phi)$ is arbitrary. Setting $E_\mathfrak{p} := E \otimes_A A_\mathfrak{p}$, we must show that $A_\mathfrak{p}[G_K]$ surjects to $\mathrm{End}_{E_\mathfrak{p}}(T_\mathfrak{p}(\phi))$ for almost all $\mathfrak{p}$. To explain the strategy, we assume that $E' := \mathrm{End}_{\overline{K}}(\phi)$ is commutative and separable over A. The additional arguments in the general case are of technical nature.

First we look at the residual representation. Let ϕ' denote the tautological extension of ϕ to a Drinfeld E'-module, which by construction is defined over a finite extension K' of K. Then for almost all $\mathfrak{p}$ we have $E'/\mathfrak{p}E' = \bigoplus_{\mathfrak{P}'|\mathfrak{p}} k_{\mathfrak{P}'}$, and hence $\phi[\mathfrak{p}] = \bigoplus_{\mathfrak{P}'|\mathfrak{p}} \phi'[\mathfrak{P}']$. By Taguchi's theorem in the form of Proposition 2.3, these direct summands are pairwise inequivalent irreducible $k_\mathfrak{p}[G_{K'}]$-modules for almost all $\mathfrak{p}$, and by Theorem 3.1 they are absolutely irreducible over $k_{\mathfrak{P}'}$. Thus $\phi[\mathfrak{p}]$ is a semisimple $k_\mathfrak{p}[G_{K'}]$-module such that $\mathrm{End}_{k_\mathfrak{p}[G_{K'}]}(\phi[\mathfrak{p}]) \cong E'/\mathfrak{p}E'$. Via Galois descent, we can deduce from this that $\phi[\mathfrak{p}]$ is a semisimple $k_\mathfrak{p}[G_K]$-module such that $\mathrm{End}_{k_\mathfrak{p}[G_K]}(\phi[\mathfrak{p}]) \cong E/\mathfrak{p}E$, for almost all $\mathfrak{p}$. By the theorem on bicommutants this means that $k_\mathfrak{p}[G_K]$ surjects to $\mathrm{End}_{E/\mathfrak{p}E}\bigl(\phi[\mathfrak{p}]\bigr)$ for almost all $\mathfrak{p}$.

To lift this result to the full Tate module, using Proposition 2.3 again we show that for almost all $\mathfrak{p}$, every $A_\mathfrak{p}[G_K]$-submodule of $T_\mathfrak{p}(\phi)$ has the form $\alpha(T_\mathfrak{p}(\phi))$ for some $\alpha \in E_\mathfrak{p}$. By successive approximation we can then prove that the image of $A_\mathfrak{p}[G_K]$ is equal to $\mathrm{End}_{E_\mathfrak{p}}(T_\mathfrak{p}(\phi))$, as desired.

4.1 The action of the endomorphism ring

Proposition 4.1 *(a) For every ideal $\mathfrak{a} \not\subset \mathfrak{p}_0$ of A the natural homomorphism*

$$E/\mathfrak{a}E \longrightarrow \mathrm{End}_{A/\mathfrak{a}}(\phi[\mathfrak{a}])$$

is injective.

(b) For every prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A the natural homomorphism

$$E_\mathfrak{p} \longrightarrow \mathrm{End}_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi))$$

is injective and its image is saturated.

Proof. To prove (a) we first assume that $\mathfrak{a}$ is principal, say $\mathfrak{a} = (a)$. Then $\phi[\mathfrak{a}] = \ker\bigl(\phi_a : \overline{K} \to \overline{K}\bigr)$. Since $a \notin \mathfrak{p}_0$, the polynomial ϕ_a is separable, and by the right division algorithm in $K\{\tau\}$ it generates the left ideal of all polynomials vanishing on $\phi[\mathfrak{a}]$. Consider any element α in the kernel of $E \to \mathrm{End}_{A/\mathfrak{a}}(\phi[\mathfrak{a}])$. Then $\alpha = \beta\phi_a$ for some element $\beta \in K\{\tau\}$. Both α and ϕ_a commute with ϕ_b for all $b \in A$; hence so does β. Thus $\beta \in E$, and so $\alpha \in Ea = \mathfrak{a}E$. This implies (a) whenever $\mathfrak{a}$ is principal.

For general $\mathfrak{a}$ choose any $a \in \mathfrak{a} \smallsetminus \mathfrak{p}_0$. Then $\phi[\mathfrak{a}] \subset \phi[(a)]$ are free modules of rank r over $A/\mathfrak{a}$ and $A/(a)$, respectively; hence

$$\mathrm{End}_{A/\mathfrak{a}}\big(\phi[\mathfrak{a}]\big) \;\cong\; \mathrm{Mat}_{r\times r}\big(A/\mathfrak{a}\big) \;\cong\; \mathrm{End}_{A/(a)}\big(\phi[(a)]\big) \otimes_A A/\mathfrak{a}.$$

By the principal ideal case we have

$$E/aE \;\hookrightarrow\; \mathrm{End}_{A/(a)}\big(\phi[(a)]\big) \;\cong\; \mathrm{Mat}_{r\times r}\big(A/(a)\big).$$

Since E is a torsion free A-module of finite type, it is locally free; hence E/aE is free over $A/(a)$. It is therefore a direct summand of the right hand side. This property is preserved under tensoring with $A/\mathfrak{a}$. It follows that

$$E/\mathfrak{a}E \;\hookrightarrow\; \mathrm{End}_{A/(a)}\big(\phi[(a)]\big) \otimes_A A/\mathfrak{a} \;\cong \mathrm{End}_{A/\mathfrak{a}}\big(\phi[\mathfrak{a}]\big)$$

is a direct summand, proving (a). Applying (a) to $\mathfrak{a} = \mathfrak{p}^n$ and taking the projective limit over n shows (b). **q.e.d.**

Let Z denote the center of E. Then E is an order in a finite dimensional central division algebra over the quotient field of Z. Write $c := [Z/A]$ and $e^2 = [E/Z]$. Then the rank of ϕ is $r = cde$ for an integer $d > 0$. For every prime $\mathfrak{p}$ of A we abbreviate $Z_\mathfrak{p} := Z \otimes_A A_\mathfrak{p}$. The completion and the residue field at a prime $\mathfrak{P}$ of Z will be denoted $Z_\mathfrak{P}$ and $k_\mathfrak{P}$, respectively. Standard properties of division algebras over global fields imply:

Lemma 4.2 *For almost all primes $\mathfrak{p}$ of A we have*

$$Z_\mathfrak{p} \;=\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} Z_\mathfrak{P}$$

$$E_\mathfrak{p} \;\cong\; \mathrm{Mat}_{e\times e}(Z_\mathfrak{p}) \;=\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Mat}_{e\times e}(Z_\mathfrak{P})$$

Moreover, if Z is separable over A, then for almost all $\mathfrak{p}$ we have

$$Z/\mathfrak{p}Z \;=\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} k_\mathfrak{P}$$

and

$$E/\mathfrak{p}E \;\cong\; \mathrm{Mat}_{e\times e}(Z/\mathfrak{p}Z) \;=\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Mat}_{e\times e}(k_\mathfrak{P}).$$

For $\mathfrak{P}|\mathfrak{p}$ as in Lemma 4.2 we let $E_\mathfrak{p} \cong \mathrm{Mat}_{e\times e}(Z_\mathfrak{p})$ act on $Z_\mathfrak{P}^{\oplus e}$ in the obvious way. Then $W_\mathfrak{P} := \mathrm{Hom}_{E_\mathfrak{p}}(Z_\mathfrak{P}^{\oplus e}, T_\mathfrak{p}(\phi))$ is a free $Z_\mathfrak{P}$-module of rank d, and its quotient $\overline{W_\mathfrak{P}} := W_\mathfrak{P}/\mathfrak{P}W_\mathfrak{P}$ is a $k_\mathfrak{P}$-vector space of dimension d. The decompositions in Lemma 4.2 and the well-known structure theory of modules over matrix rings imply:

Lemma 4.3 *For all primes $\mathfrak{p}$ as in Lemma 4.2 the natural homomorphism*

$$\bigoplus_{\mathfrak{P}|\mathfrak{p}} W_\mathfrak{P} \otimes_{Z_\mathfrak{P}} Z_\mathfrak{P}^{\oplus e} \longrightarrow T_\mathfrak{p}(\phi)$$

and, if Z is separable over A, the natural homomorphism

$$\bigoplus_{\mathfrak{P}|\mathfrak{p}} \overline{W_\mathfrak{P}} \otimes_{k_\mathfrak{P}} k_\mathfrak{P}^{\oplus e} \longrightarrow \phi[\mathfrak{p}]$$

are isomorphisms.

Letting G_K act trivially on $Z_{\mathfrak{P}}^{\oplus e}$ and $k_{\mathfrak{P}}^{\oplus e}$, by functoriality we obtain natural continuous representations of G_K on $W_{\mathfrak{P}}$ and on $\overline{W_{\mathfrak{P}}}$. By construction the above isomorphisms are $E_{\mathfrak{p}}[G_K]$-equivariant.

4.2 The residual representation

Throughout this subsection we assume that Z is separable over A and study the Galois representation on $\phi[\mathfrak{p}]$. From Taguchi's Theorem 2.2 we can deduce:

Lemma 4.4 *For almost all $\mathfrak{p}$ and all $\mathfrak{P}|\mathfrak{p}$ the $\overline{W_{\mathfrak{P}}}$ are irreducible $k_{\mathfrak{p}}[G_K]$-modules and pairwise inequivalent, and in particular, $\phi[\mathfrak{p}]$ is a semisimple $k_{\mathfrak{p}}[G_K]$-module.*

Proof. Let $\mathfrak{p}$ be a prime as in Lemma 4.3. Then by Proposition 2.3 any $k_{\mathfrak{p}}[G_K]$-submodule of $\phi[\mathfrak{p}]$ must have the form

$$\bigoplus_{\mathfrak{P}|\mathfrak{p}} \overline{W_{\mathfrak{P}}} \otimes_{k_{\mathfrak{P}}} U_{\mathfrak{P}}$$

with $k_{\mathfrak{P}}$-subspaces $U_{\mathfrak{P}} \subset k_{\mathfrak{P}}^{\oplus e}$. In particular, for any $k_{\mathfrak{P}}[G_K]$-submodule $\overline{V_{\mathfrak{P}}} \subset \overline{W_{\mathfrak{P}}}$ the submodule $\overline{V_{\mathfrak{P}}} \otimes_{k_{\mathfrak{P}}} k_{\mathfrak{P}}^{\oplus e}$ must have this form, which shows that $\overline{V_{\mathfrak{P}}} = 0$ or $\overline{W_{\mathfrak{P}}}$, proving that $\overline{W_{\mathfrak{P}}}$ is irreducible. A similar argument applied to the graph of a homomorphism shows that any two $\overline{W_{\mathfrak{P}}}$ are pairwise non-equivalent. **q.e.d.**

We want to show that the $\overline{W_{\mathfrak{P}}}$ are absolutely irreducible over $k_{\mathfrak{P}}$. In order to use Theorem 3.1 we must take into account all endomorphisms over $\overline{K}$. Set $E' := \mathrm{End}_{\overline{K}}(\phi)$ and let K'/K be a finite Galois extension over which all endomorphisms in E' are defined. Note that every $\phi[\mathfrak{p}]$ is an $E'[G_{K'}]$-module.

Lemma 4.5 *The center of E' is separable over A.*

Proof. Let Z' denote the center of E'. Then $E \cap Z'$ is contained in E and commutes with E; hence it is contained in Z. Since Z is separable over A, it follows that $E \cap Z'$ is separable over A. On the other hand there is a natural action of $\mathrm{Gal}(K'/K)$ on E', and thus on Z'. The set of invariants on E' is just E, and so the set of invariants on Z' is $E \cap Z'$. Therefore Z' is a finite Galois extension of $E \cap Z'$. In particular it is separable, and since separability is transitive, the lemma follows. **q.e.d.**

Lemma 4.6 *Let A' be a maximal commutative A-subalgebra of E' which is separable over A. Then for almost all $\mathfrak{p}$ the natural map*

$$A'/\mathfrak{p}A' \longrightarrow \mathrm{End}_{A'/\mathfrak{p}A'[G_{K'}]}(\phi[\mathfrak{p}])$$

is an isomorphism.

Proof. The tautological embedding $E' \hookrightarrow K'\{\tau\}$ restricts to a homomorphism $\phi' : A' \to K'\{\tau\}$ extending ϕ which is a Drinfeld A'-module of rank d. By definition its endomorphism ring is the commutant of A' in the endomorphism ring of ϕ. Since A' is maximal commutative in E', we deduce that $\mathrm{End}_{\overline{K}}(\phi') = A'$. By Theorem 3.1 we know that for almost all primes $\mathfrak{p}'$ of A' the $k_{\mathfrak{p}'}[G_{K'}]$-module $\phi[\mathfrak{p}']$ is absolutely irreducible over $k_{\mathfrak{p}'}$. Thus for those $\mathfrak{p}'$ we have

$$\mathrm{End}_{k_{\mathfrak{p}'}[G_{K'}]}(\phi'[\mathfrak{p}']) = k_{\mathfrak{p}'}.$$

Now since A' is separable over A, for almost all $\mathfrak{p}$ we have $A'/\mathfrak{p}A' = \bigoplus_{\mathfrak{p}'|\mathfrak{p}} k_{\mathfrak{p}'}$. Thus for those $\mathfrak{p}$ we get a decomposition

$$\phi[\mathfrak{p}] = \bigoplus_{\mathfrak{p}'|\mathfrak{p}} \phi'[\mathfrak{p}'].$$

Putting these facts together, we deduce that

$$\mathrm{End}_{A'/\mathfrak{p}A'[G_{K'}]}(\phi[\mathfrak{p}]) \;=\; \bigoplus_{\mathfrak{p}'|\mathfrak{p}} \mathrm{End}_{k_{\mathfrak{p}'}[G_{K'}]}(\phi'[\mathfrak{p}']) \;=\; \bigoplus_{\mathfrak{p}'|\mathfrak{p}} k_{\mathfrak{p}'} \;=\; A'/\mathfrak{p}A',$$

as desired. **q.e.d.**

Lemma 4.7 *For almost all* $\mathfrak{p}$ *the natural map*

$$E'/\mathfrak{p}E' \longrightarrow \mathrm{End}_{k_{\mathfrak{p}}[G_{K'}]}(\phi[\mathfrak{p}])$$

is an isomorphism.

Proof. After replacing K by K' we may assume that $E' = E$, which by Lemma 4.5 preserves the separability of Z over A. We will then use the isomorphism from Lemma 4.3. As the $\overline{W_{\mathfrak{P}}}$ are irreducible $k_{\mathfrak{p}}[G_K]$-modules by Lemma 4.4, Schur's lemma and Wedderburn's theorem force

$$\ell_{\mathfrak{P}} := \mathrm{End}_{k_{\mathfrak{p}}[G_K]}\big(\overline{W_{\mathfrak{P}}}\big)$$

to be a finite field extension of $k_{\mathfrak{P}}$. Further, the $\overline{W_{\mathfrak{P}}}$ are pairwise non-equivalent; hence

$$\begin{aligned}
\mathrm{End}_{k_{\mathfrak{p}}[G_K]}\big(\phi[\mathfrak{p}]\big) &\cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{End}_{k_{\mathfrak{p}}[G_K]}\big(\overline{W_{\mathfrak{P}}} \otimes_{k_{\mathfrak{P}}} k_{\mathfrak{P}}^{\oplus e}\big) \\
&= \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{End}_{k_{\mathfrak{p}}[G_K]}\big(\overline{W_{\mathfrak{P}}}\big) \otimes_{k_{\mathfrak{P}}} \mathrm{End}_{k_{\mathfrak{P}}}\big(k_{\mathfrak{P}}^{\oplus e}\big) \\
&= \bigoplus_{\mathfrak{P}|\mathfrak{p}} \ell_{\mathfrak{P}} \otimes_{k_{\mathfrak{P}}} \mathrm{Mat}_{e\times e}(k_{\mathfrak{P}}).
\end{aligned}$$

Since $E\otimes_A F$ is a simple F-algebra, by Bourbaki [2] §10, no 4, Proposition 4, it contains a maximal commutative subfield F' that is separable over the center $Z\otimes_A F$. Then $A' := E\cap F'$ is a maximal commutative subalgebra of E that is separable over Z. Because separability is transitive, it is also separable over A. Since E and hence A' act on $\phi[\mathfrak{p}]$ through the factors $\mathrm{Mat}_{e\times e}(k_{\mathfrak{P}})$, the above decomposition implies that

$$\mathrm{End}_{A'/\mathfrak{p}A'[G_K]}\big(\phi[\mathfrak{p}]\big) \;\supset\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \ell_{\mathfrak{P}} \otimes_{k_{\mathfrak{P}}} A'/\mathfrak{P}A'.$$

But here by Lemma 4.6 the left hand side is

$$A'/\mathfrak{p}A' \;=\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} A'/\mathfrak{P}A'$$

for almost all $\mathfrak{p}$. It follows that $\ell_{\mathfrak{P}} = k_{\mathfrak{P}}$ for almost all $\mathfrak{P}$. Thus for almost all $\mathfrak{p}$ we have

$$\mathrm{End}_{k_{\mathfrak{p}}[G_K]}\big(\phi[\mathfrak{p}]\big) \;\cong\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Mat}_{e\times e}(k_{\mathfrak{P}}) \;\cong\; E/\mathfrak{p}E,$$

as desired. **q.e.d.**

Lemma 4.8 *For almost all primes* $\mathfrak{p}$ *of* A *we have* $E/\mathfrak{p}E \cong (E'/\mathfrak{p}E')^{G_K}$.

Proof. The group G_K acts on E' through the finite quotient $G := \mathrm{Gal}(K'/K)$. We consider the homomorphism

$$\varepsilon : E' \to \bigoplus_{g\in G} E',\ \alpha \mapsto \big((g-1)\alpha\big)_{g\in G},$$

whose kernel clearly is $(E')^G = E$. It yields two short exact sequences

$$0 \to E \to E' \to \operatorname{im}\varepsilon \to 0$$

and

$$0 \to \operatorname{im}\varepsilon \to \bigoplus_{g\in G} E' \to \operatorname{coker}\varepsilon \to 0.$$

Now all these modules are of finite type over A, so they are locally free at almost all primes $\mathfrak{p}$. For those $\mathfrak{p}$ the modules $\mathrm{Tor}_1^A(\operatorname{im}\varepsilon, A/\mathfrak{p})$ and $\mathrm{Tor}_1^A(\operatorname{coker}\varepsilon, A/\mathfrak{p})$ vanish, so the sequences remain exact after tensoring with $A/\mathfrak{p}$. Therefore the sequence

$$0 \longrightarrow E/\mathfrak{p}E \longrightarrow E'/\mathfrak{p}E' \xrightarrow{\overline{\varepsilon}} \bigoplus_{g\in G} E'/\mathfrak{p}E'$$

with $\overline{\varepsilon} = \varepsilon \bmod \mathfrak{p}$ is exact. It follows that

$$E/\mathfrak{p}E = \ker\overline{\varepsilon} = (E'/\mathfrak{p}E')^G,$$

as desired. **q.e.d.**

Lemma 4.9 *For almost all $\mathfrak{p}$ the natural map*

$$E/\mathfrak{p}E \longrightarrow \mathrm{End}_{k_\mathfrak{p}[G_K]}(\phi[\mathfrak{p}])$$

is an isomorphism.

Proof. By Lemma 4.7 the natural map

$$E'/\mathfrak{p}E' \longrightarrow \mathrm{End}_{k_\mathfrak{p}[G_{K'}]}(\phi[\mathfrak{p}])$$

is an isomorphism for almost all $\mathfrak{p}$. On both sides we have an action of G_K. The invariants on the right hand side are $\mathrm{End}_{k_\mathfrak{p}[G_K]}(\phi[\mathfrak{p}])$, and for almost all $\mathfrak{p}$ the invariants on the left hand side are $E/\mathfrak{p}E$ by Lemma 4.8. The assertion follows. **q.e.d.**

Lemma 4.10 *For almost all $\mathfrak{p}$ we have a surjection*

$$k_\mathfrak{p}[G_K] \ \twoheadrightarrow\ \mathrm{End}_{E/\mathfrak{p}E}\big(\phi[\mathfrak{p}]\big) \ \cong\ \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{End}_{k_\mathfrak{P}}\big(\overline{W_\mathfrak{P}}\big) \ \cong\ \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Mat}_{d\times d}(k_\mathfrak{P}),$$

and in particular, the $\overline{W_\mathfrak{P}}$ are pairwise inequivalent $k_\mathfrak{p}[G_K]$-modules which are absolutely irreducible over $k_\mathfrak{P}$.

Proof. Lemma 4.4 says that $\phi[\mathfrak{p}]$ is a semisimple $k_\mathfrak{p}[G_K]$-module for almost all $\mathfrak{p}$. Therefore the image of $k_\mathfrak{p}[G_K]$ in $\mathrm{End}_{k_\mathfrak{p}}(\phi[\mathfrak{p}])$ is its own bicommutant. Since its commutant is $E/\mathfrak{p}E$ by Lemma 4.9, we deduce that $k_\mathfrak{p}[G_K]$ surjects to $\mathrm{End}_{E/\mathfrak{p}E}(\phi[\mathfrak{p}])$. The isomorphisms on the right hand side follow from Lemmata 4.2 and 4.3. **q.e.d.**

4.3 The representation on the Tate module

Now set $W_\mathfrak{p} := \bigoplus_{\mathfrak{P}|\mathfrak{p}} W_\mathfrak{P}$ and note that $T_\mathfrak{p}(\phi) \cong W_\mathfrak{p}^{\oplus e}$ by Lemma 4.3.

Lemma 4.11 *For almost all primes $\mathfrak{p}$ of A, every $A_\mathfrak{p}[G_K]$-submodule of $W_\mathfrak{p}$ has the form $\alpha(W_\mathfrak{p})$ for some $\alpha \in Z_\mathfrak{p}$.*

Proof. Consider any $A_\mathfrak{p}[G_K]$-submodule $H'_\mathfrak{p} \subset W_\mathfrak{p}$. Then we can apply Proposition 2.5 to the $A_\mathfrak{p}[G_K]$-submodule $(H'_\mathfrak{p})^{\oplus e} \subset (W_\mathfrak{p})^{\oplus e} \cong T_\mathfrak{p}(\phi)$, showing that $(H'_\mathfrak{p})^{\oplus e} = \alpha(T_\mathfrak{p}(\phi))$ for some $\alpha \in E_\mathfrak{p}$. Recall from Lemma 4.2 that $E_\mathfrak{p} \cong \mathrm{Mat}_{e\times e}(Z_\mathfrak{p})$, and let $\alpha_1, \ldots, \alpha_e \in Z_\mathfrak{p}$ denote the entries of any chosen row of α. Then $H'_\mathfrak{p} = \sum_{i=1}^{e} \alpha_i(W_\mathfrak{p})$. Now Lemma 4.2 also implies that for almost all $\mathfrak{p}$, every ideal in $Z_\mathfrak{p}$ is a principal ideal. Thus $H'_\mathfrak{p} = \alpha(W_\mathfrak{p})$ for some $\alpha \in Z_\mathfrak{p}$, as desired. **q.e.d.**

Lemma 4.12 *Let R be a commutative ring with identity, and let $M := R^{\oplus d}$ for some integer $d \geq 1$. Let $B \subset \mathrm{End}_R(M) = \mathrm{Mat}_{d\times d}(R)$ be a subring (not necessarily an R-subalgebra) satisfying the properties:*

(a) Every B-submodule of M has the form $\mathfrak{a}M$ for an ideal $\mathfrak{a} \subset R$.

(b) The quotients $M/\mathfrak{m}M$ for distinct maximal ideals $\mathfrak{m} \subset R$ are pairwise inequivalent B-modules.

Then the following statements are true:

(c) Consider integers r, $s \geq 0$ and a maximal ideal $\mathfrak{m} \subset R$, such that there exists a B-linear surjection $M^{\oplus r} \twoheadrightarrow (M/\mathfrak{m}M)^{\oplus s}$. Then $s \leq r$.

(d) Consider an integer $r \geq 0$ and a B-submodule $N \subset M^{\oplus r}$, such that for all maximal ideals $\mathfrak{m} \subset R$ the induced homomorphism $N \to (M/\mathfrak{m}M)^{\oplus r}$ is surjective. Then $N = M^{\oplus r}$.

(e) Assume moreover that for all maximal ideals $\mathfrak{m} \subset R$ the induced homomorphism $B \to \mathrm{Mat}_{d\times d}(R/\mathfrak{m})$ is surjective. Then $B = \mathrm{Mat}_{d\times d}(R)$.

Proof. First consider any maximal ideal $\mathfrak{m} \subset R$. Then $M/\mathfrak{m}M$ is a simple B-module, because by (a) there exist no other B-submodules between $\mathfrak{m}M$ and M.

Next consider any non-zero B-linear homomorphism $M \to M/\mathfrak{m}M$. By (a) its kernel has the form $\mathfrak{a}M$ for some ideal $\mathfrak{a} \subset R$. Since $M/\mathfrak{m}M$ is a simple B-module, the same follows for $M/\mathfrak{a}M$, which implies that $\mathfrak{a}$ is actually a maximal ideal of R. Now (b) shows that $\mathfrak{a} = \mathfrak{m}$. It follows that every B-linear homomorphism $M \to M/\mathfrak{m}M$ vanishes on $\mathfrak{m}M$.

We can now prove (c). Consider a B-linear surjection $f : M^{\oplus r} \twoheadrightarrow (M/\mathfrak{m}M)^{\oplus s}$. We can view it as an $s\times r$-matrix of B-linear homomorphisms $M \to M/\mathfrak{m}M$. By the preceding remarks any such homomorphism vanishes on $\mathfrak{m}M$. Therefore f comes from a B-linear surjection $(M/\mathfrak{m}M)^{\oplus r} \twoheadrightarrow (M/\mathfrak{m}M)^{\oplus s}$. Since $M/\mathfrak{m}M$ is a simple B-module, the Jordan-Hölder theorem now implies that $s \leq r$, as desired.

To prove (d) we use induction on r. The assertion is trivial for $r = 0$, so assume that $r > 0$. Let $M \xrightarrow{\iota} M^{\oplus r} \xrightarrow{\pi} M^{\oplus(r-1)}$ be the inclusion in the first factor and the projection to the remaining factors, respectively. The induction hypothesis implies that $\pi(N) = M^{\oplus(r-1)}$. On the other hand (a) implies that $\iota^{-1}(N) = \mathfrak{a}M$ for some ideal $\mathfrak{a} \subset R$. Thus we have an inclusion of short exact sequences of B-modules:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\iota} & M^{\oplus r} & \xrightarrow{\pi} & M^{\oplus(r-1)} & \longrightarrow & 0 \\
 & & \cup & & \cup & & \| & & \\
0 & \longrightarrow & \mathfrak{a}M & \longrightarrow & N & \longrightarrow & M^{\oplus(r-1)} & \longrightarrow & 0.
\end{array}$$

Suppose that $\mathfrak{a} \neq R$. Then we can choose a maximal ideal $\mathfrak{m} \subset R$ containing $\mathfrak{a}$. The image of $\mathfrak{a}M$ in $(M/\mathfrak{m}M)^{\oplus r}$ is then zero; hence the homomorphism $N \to (M/\mathfrak{m}M)^{\oplus r}$, which by assumption is surjective, factors through a B-linear surjection $M^{\oplus(r-1)} \twoheadrightarrow (M/\mathfrak{m}M)^{\oplus r}$. But by (c) this is impossible. Therefore $\mathfrak{a} = R$, and the five lemma implies that $N = M^{\oplus r}$, as desired. This proves (d).

Finally, (e) is the special case of (d) applied to the left B-submodule $B \subset \mathrm{Mat}_{d\times d}(R) \cong M^{\oplus d}$. **q.e.d.**

Proposition 4.13 *For almost all $\mathfrak{p}$ we have a surjection*

$$A_\mathfrak{p}[G_K] \longrightarrow\!\!\!\!\!\rightarrow \mathrm{End}_{E_\mathfrak{p}}\big(T_\mathfrak{p}(\phi)\big) \;\cong\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{End}_{Z_\mathfrak{P}}(W_\mathfrak{P}) \;\cong\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Mat}_{d\times d}(Z_\mathfrak{P}).$$

Proof. The isomorphisms on the right hand side follow from Lemmata 4.2 and 4.3, which also show that $Z_\mathfrak{p} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} Z_\mathfrak{P}$ and $W_\mathfrak{p} \cong Z_\mathfrak{p}^{\oplus d}$. Let $B_\mathfrak{p} \subset \mathrm{Mat}_{d\times d}(Z_\mathfrak{p})$ denote the image of the homomorphism in question. To prove equality we will show that $B := B_\mathfrak{p}$ satisfies the assumptions of Lemma 4.12 with $R := Z_\mathfrak{p}$ and $M := W_\mathfrak{p}$. First, assumption 4.12 (a) follows directly from Lemma 4.11.

For the other assumptions we want to use Lemma 4.10, which depends on the condition that Z is separable over A. So let $A \subset A' \subset Z$ be the largest subring that is totally inseparable over A. Then the primes $\mathfrak{p}$ of A are in bijection with the primes $\mathfrak{p}'$ of A', with equal residue fields. Now the tautological embedding $A' \subset Z \subset E \hookrightarrow K\{\tau\}$ is a Drinfeld A'-module ϕ' extending ϕ, such that $T_\mathfrak{p}(\phi) = T_{\mathfrak{p}'}(\phi')$ for almost all $\mathfrak{p}$. Since Z is separable over A', applying Lemma 4.10 to ϕ' shows that for almost all $\mathfrak{p}$ we have a surjection

$$k_{\mathfrak{p}'}[G_K] \longrightarrow\!\!\!\!\!\rightarrow \bigoplus_{\mathfrak{P}|\mathfrak{p}'} \mathrm{End}_{k_\mathfrak{P}}\big(\overline{W_\mathfrak{P}}\big) \;\cong\; \bigoplus_{\mathfrak{P}|\mathfrak{p}'} \mathrm{Mat}_{d\times d}(k_\mathfrak{P}).$$

But $k_{\mathfrak{p}'}[G_K] = k_\mathfrak{p}[G_K]$, which by construction has the same image as $B_\mathfrak{p}$. Thus for almost all $\mathfrak{p}$ we have a surjection

$$B_\mathfrak{p} \longrightarrow\!\!\!\!\!\rightarrow \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{End}_{k_\mathfrak{P}}\big(\overline{W_\mathfrak{P}}\big) \;\cong\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{Mat}_{d\times d}(k_\mathfrak{P}).$$

With $\mathfrak{m} := \mathfrak{P}$, $R/\mathfrak{m} = k_\mathfrak{P}$, and $M/\mathfrak{m}M = \overline{W_\mathfrak{P}}$ we deduce that the assumptions in 4.12 (b) and (e) are satisfied. Thus Lemma 4.12 implies that $B_\mathfrak{p} = \mathrm{Mat}_{d\times d}(Z_\mathfrak{p})$, as desired. **q.e.d.**

Finally, Proposition 4.13 and Lemmata 4.2 and 4.3 together imply Theorem B from the introduction. Theorem A follows from the special case $E = A$ of Theorem B.

References

[1] A. Borel, *Linear algebraic groups*, 2nd enlarged edition, Graduate Texts in Math. **126**, Springer-Verlag, 1991.

[2] N. Bourbaki, Algèbre, Chapitre 8: Modules et anneaux semi-simples, *Éléments de mathématique XXIII*, Hermann, 1958.

[3] P. Deligne, La conjecture de Weil II, *Publ. Math. IHES* **52** (1980), 138–252.

[4] P. Deligne and D. Husemöller, Survey of Drinfeld modules, *Contemp. Math.* **67** (1987), 25–91.

[5] V. G. Drinfeld, Elliptic modules (Russian), *Mat. Sbornik* **94** (1974), 594–627, transl. *Math. USSR Sbornik* **23** (1974), 561–592.

[6] D. Goss, *Basic structures of function field arithmetic*, Springer-Verlag, 1996.

[7] N. M. Katz, *Gauss sums, Kloosterman sums and monodromy groups*, Princeton University Press, 1988.

[8] N. M. Katz and S. Lang, Finiteness theorems in geometric classfield theory, *Enseign. Math.* (2) **27** (1981), 285–319.

[9] R. Pink, The Mumford-Tate conjecture for Drinfeld modules, *Publ. RIMS Kyoto University* **33** No. 3 (1997), 393–425.

[10] R. Pink, The Galois Representations Associated to a Drinfeld Module in Special Characteristic, I: Zariski Density, *Preprint* (August 2003), 20p.

[11] R. Pink, The Galois Representations Associated to a Drinfeld Module in Special Characteristic, II: Openness, *Preprint* (March 2004), 20p.

[12] R. Pink and M. Traulsen, The Isogeny Conjecture for t-Motives Associated to Direct Sums of Drinfeld Modules, *Preprint* (March 2004), 17p.

[13] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[14] T. A. Springer, *Linear algebraic groups*, 2nd edition, Birkhäuser, 1998.

[15] Y. Taguchi, Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "finite characteristics", *Duke Math. J.* **62** (1991), 593–599.

[16] Y. Taguchi, Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics", *J. Number Theory* **44** (1993), 292–314.

[17] Y. Taguchi, The Tate conjecture for t-motives, *Proc. Amer. Math. Soc.* **123** No. 11 (1995), 3285–3287.

[18] Y. Taguchi, Finiteness of an isogeny class of Drinfeld modules, *J. Number Theory* **74** (1999), 337–348.

[19] A. Tamagawa, The Tate conjecture for A-premotives, *Preprint*, 1994.

[20] M. Traulsen, *Galois representations associated to Drinfeld modules in special characteristic and the isogeny conjecture for t-motives*, Diss. ETH Zurich, 2003. Available via http://e-collection.ethbib.ethz.ch/show?type=diss&nr=15138.