The Galois representations associated to a Drinfeld module in special characteristic—III: Image of the group ring

Richard Pink*, Matthias Traulsen

Department of Mathematics, ETH Zentrum, 8092 Zurich, Switzerland

Received 16 April 2004; revised 7 October 2004
Available online 14 July 2005
Communicated by G. Böckle

Abstract

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

© 2005 Elsevier Inc. All rights reserved.

MSC: 11G09; 11R58

Keywords: Drinfeld modules; $t$-motives; Galois groups

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 $\ell$ let $E[\ell]$ denote its module of $\ell$-torsion points and $T_{\ell}(E)$ its $\ell$-adic...
Tate module. Both modules are free of rank 2 and carry natural Galois representations

\[
\rho_\ell : \ G_L \rightarrow \text{Aut}_{\mathbb{Z}_\ell} (T_\ell(E)) \cong \text{GL}_2(\mathbb{Z}_\ell),
\]
\[
\overline{\rho}_\ell : \ G_L \rightarrow \text{Aut}_{\mathbb{F}_\ell}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell),
\]

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

With Drinfeld modules we are in a similar situation. Let \( \phi \) be a Drinfeld \( A \)-module of rank \( r \) and characteristic \( p_0 \) over a finitely generated field \( K \) of transcendence degree 1. (Notations will be explained in Section 2.1.) Then for any prime \( p \neq p_0 \) of \( A \) with residue field \( k_p \) we have natural Galois representations

\[
\rho_p : \ G_K \rightarrow \text{Aut}_{A_p} (T_p(\phi)) \cong \text{GL}_r(A_p),
\]
\[
\overline{\rho}_p : \ G_K \rightarrow \text{Aut}_{k_p} (\phi[p]) \cong \text{GL}_r(k_p).
\]

If \( \text{End}_K(\phi) = A \), Taguchi [14–16] and Tamagawa [18] proved that \( \rho_p \) is absolutely irreducible over \( \text{Quot}(A_p) \) for all \( p \neq p_0 \). Moreover, another result of Taguchi [14,17] implies that \( \overline{\rho}_p \) is irreducible for almost all \( p \).

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

**Theorem A.** Assume that \( p_0 \neq 0 \) and that \( \text{End}_K(\phi) = A \). Then for almost all primes \( p \) of \( A \) the residual representation \( \overline{\rho}_p \) 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 \( p \). So let \( B_p \) denote the image of the natural homomorphism

\[
A_p[G_K] \rightarrow \text{End}_{A_p} (T_p(\phi)).
\]

Abbreviate \( E := \text{End}_K(\phi) \). For all \( p \neq p_0 \) the natural homomorphism

\[
E_p := E \otimes_A A_p \rightarrow \text{End}_{A_p} (T_p(\phi))
\]

is known to be injective (see Proposition 4.1), and by Taguchi [16] or Tamagawa [18] its image is the commutant of \( B_p \). 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 \( Z_p := Z \otimes_A A_p \) and note that both \( E_p \) and \( B_p \) are \( Z_p \)-algebras.
Theorem B. Assume that $p_0 \neq 0$. Then for almost all primes $p$ of $A$ the rings $E_p$ and $B_p$ are commutants of each other in $\text{End}_A(T_p(\phi))$. More precisely, for almost all $p$ we have $E_p \cong \text{Mat}_{e \times e}(Z_p)$ and $B_p \cong \text{Mat}_{d \times d}(Z_p)$ and an isomorphism of $B_p \otimes_{Z_p} E_p$-modules $T_p(\phi) \cong Z_p^{\otimes d} \otimes Z_p Z_p^{\otimes e}$.

The weaker statement obtained by tensoring with $F_p$ follows from the semisimplicity theorem and the Tate conjecture for endomorphisms proved by Taguchi [14,16] and Tamagawa [18], using the theorem on bicommutants. But the situation over $A_p$ is substantially subtler.

Although these results concern only 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 $\implies$ 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 $\text{End}_K(\phi) = A$. 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 [19]. 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 $\infty$ on $\mathcal{C}$ and let $A$ be the ring of functions in $F$ which are regular outside $\infty$.

Inside a fixed algebraic closure $\overline{K}$ of $K$ we consider the following subextensions: the separable closure $K^{\text{sep}}$, the maximal abelian extension $K^{\text{ab}}$, the maximal unramified extension $K^{\text{nr}}$ and the maximal unramified abelian extension $K^{\text{ab,nr}}$. 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 $O_x$. We let $G_K := \text{Gal}(K^{\text{sep}}/K)$ 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 $G_K^{\text{geom}} := \text{Gal}(K^{\text{sep}}/Kk_0)$. The absolute Galois group $G_{k_0} =
Gal(\overline{k_0}/k_0) of \(k_0\) is isomorphic to the Prüfer group \(\hat{\mathbb{Z}}\) and is topologically generated by the arithmetic Frobenius \(\text{Frob}_{k_0}\). We have the short exact sequence

\[1 \to G_{k_0}^{\text{geom}} \to G_K \to G_{k_0} \to 1.\]

By \(K\{\tau\}\) we denote the twisted (non-commutative) polynomial ring in one variable, which satisfies the relation \(\tau x = x^q\tau\) for all \(x \in K\). Identifying \(\tau\) 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 \(p_0\) over \(K\). For the general theory of Drinfeld modules, see Drinfeld [5] or Deligne–Husemöller [4]. For all non-zero ideals \(a\) in \(A\), let

\[\phi[a] := \{x \in \overline{K} \mid \forall a \in a : \phi_a(x) = 0\}\]

denote the module of \(a\)-torsion of \(\phi\). If \(p_0\) divides \(a\), its points are defined over \(K^{\text{sep}}\) and form a free \(A/a\)-module of rank \(r\). For any prime \(p\) of \(A\), we let \(A_p\) denote the completion of \(A\) at \(p\). For \(p \neq p_0\) the \(p\)-adic Tate module \(T_p(\phi) := \varprojlim \phi[p^n]\) of \(\phi\) is a free \(A_p\)-module of rank \(r\).

On all these modules there is a natural Galois action. In particular, for all \(p \neq p_0\) we have continuous representations

\[\rho_p : G_K \to \text{Aut}_{A_p}(T_p(\phi)) \cong \text{GL}_r(A_p),\]

\[\overline{\rho}_p : G_K \to \text{Aut}_{k_p}(\phi[p]) \cong \text{GL}_r(k_p),\]

where \(k_p := A/p\) is the residue field at \(p\). Clearly \(\overline{\rho}_p \cong \rho_p \mod p\). Both representations commute with the natural action of the endomorphism ring

\[E := \text{End}_K(\phi) := \{u \in K\{\tau\} \mid \forall a \in A : \phi_a \circ u = u \circ \phi_a\} .\]

We will study these representations as \(p\) varies, when \(\phi\) 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 \(\phi\) be as above.

**Theorem 2.1** (*Pink [9, Proposition 2.6] and [10, Theorem 1.1]*). Assume that \(\text{End}\overline{K}(\phi) = A\). Then for all primes \(p \neq p_0\) of \(A\) the image of \(\rho_p\) is Zariski dense in \(\text{GL}_r(F_p)\).
In [9] Theorem 0.1 it is proved actually that the image is open in $\text{GL}_r(F_p)$, if moreover the characteristic $p_0$ 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 [14] and [17, Theorem 0.2]). Up to $K$-isomorphism, there are only finitely many Drinfeld $A$-modules $\phi'$ for which there exists a $K$-isogeny $\phi \to \phi'$ of degree not divisible by $p_0$.

This result can be translated into the following statements on Galois invariant sub-modules. Recall that every endomorphism of $\phi$ induces $G_K$-equivariant endomorphisms of $\phi[p^n]$ and of $T_p(\phi)$.

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

**Proof.** Choose a finite set of representatives $\phi_i^j$ of the isomorphism classes of Drinfeld modules $\phi_i^j$ in Theorem 2.2. For each $i$ choose an isogeny $\varepsilon_i : \phi_i^j \to \phi$ of degree not divisible by $p_0$. 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 $p$ outside $S \cup \{p_0\}$.

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

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

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

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

**Proposition 2.5.** For almost all primes $p$ of $A$, every $G_K$-invariant $A_p$-submodule of $T_p(\phi)$ has the form $\gamma(T_p(\phi))$ for some $\gamma \in \text{End}_K(\phi) \otimes_A A_p$.

**Proof.** Let $p$ be as in Proposition 2.3, and consider any $A_p[G_K]$-submodule $H_p \subset T_p(\phi)$. For all $n \geq 0$ we have $T_p(\phi)/p^nT_p(\phi) \cong \phi[p^n]$; hence by Proposition 2.3 we have

$$H_p + p^nT_p(\phi) = \gamma_n(T_p(\phi)) + p^nT_p(\phi)$$
for some \( n \in E \). Since \( E_p \) is compact, we can choose a subsequence \( n_{i} \) which converges to an element \( n \in E_p \). This convergence means that \( n_{i} \equiv n \mod p^{m_i} E_p \) with \( m_i \rightarrow \infty \). Setting \( \ell_i := \min\{ n_i, m_i \} \), we deduce that

\[
H \cdot p + p^{\ell_i} T \cdot p(\phi) = \varepsilon(T_p(\phi)) + p^{\ell_i} T \cdot p(\phi)
\]

for all \( i \). Now as \( \ell_i \rightarrow \infty \), the \( p^{\ell_i} T \cdot p(\phi) \) run through a fundamental system of neighborhoods of 0. Since \( E_p \) is compact, and \( H \cdot p \) and \( \varepsilon(T_p(\phi)) \) are closed submodules of \( T \cdot p(\phi) \), we deduce that

\[
H = \bigcap_i \left( H \cdot p + p^{\ell_i} T \cdot p(\phi) \right) = \bigcap_i \left( \varepsilon(T_p(\phi)) + p^{\ell_i} T \cdot p(\phi) \right) = \varepsilon(T_p(\phi)),
\]

as desired. \( \square \)

We also need information on the action of inertia and Frobenius. Let \( \mathcal{U} \) be an open dense subscheme of \( \mathcal{X} \) over which \( \phi \) 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 \( p \neq p_0 \) of \( A \) not below \( x \), the representation \( \rho_p \) is unramified at \( x \), and the characteristic polynomial of \( \rho_p(\text{Frob}_x) \) has coefficients in \( A \) and is independent of \( p \).

We denote this characteristic polynomial by \( f_x \).

**Proposition 2.7.** Assume that \( p_0 \neq 0 \). Then after replacing \( K \) by a suitable finite extension, for all primes \( p \neq p_0 \) of \( A \) and all closed points \( x \in \mathcal{X} \), the restriction of \( \rho_p \) 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 \( x \in \mathcal{X} \setminus \mathcal{U} \) and consider the Tate uniformization \( (\psi, \Lambda) \) of \( \phi \), where \( \psi \) is a Drinfeld module of rank \( r' \leq r \) over \( K_x \) which has potentially good reduction, and \( \Lambda \) is an \( A \)-lattice in \( K_x^{\text{sep}} \) via \( \psi \) of rank \( r-r' \) which is invariant under \( G_{K_x} \) (cf. [5, §7]). Then for every prime \( p \neq p_0 \) of \( A \) there is a natural \( G_{K_x} \)-equivariant short exact sequence

\[
0 \rightarrow T_p(\psi) \rightarrow T_p(\phi) \rightarrow \Lambda \otimes_A A_p \rightarrow 0.
\]

Choose a finite extension \( L_x \) of \( K_x \) over which \( \psi \) acquires good reduction and which contains \( \Lambda \). Since the reduction of \( \psi \) again has characteristic \( p_0 \), which is different from \( p \), the inertia group of \( L_x \) acts trivially on \( T_p(\psi) \). It also acts trivially on \( \Lambda \otimes_A A_p \); hence it acts unipotently on \( T_p(\phi) \).

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

### 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 \( \Gamma \). Let \( \Gamma^a \) denote the set of conjugacy classes of \( \Gamma \). Let \( \mu^a \) be the direct image of the Haar measure on \( \Gamma \) of total volume 1, which satisfies \( \mu^a(C) = |C|/|\Gamma| \) for every conjugacy class \( C \in \Gamma^a \).

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

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 \( \text{Frob}_x \in \Gamma \) associated to every point \( x \in U(k_{0,d}) \). Set

\[
\mu^a_d := \frac{1}{|U(k_{0,d})|} \sum_{x \in U(k_{0,d})} \delta([\text{Frob}_x]),
\]

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 \( \mu^a_d \) converges to \( \mu^a \) 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 \( x \in U(k_{0,d}) \) meet all conjugacy classes in \( \Gamma \).

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 \( \mathcal{F} := (\pi_* \overline{\mathcal{O}}_{\ell})[\mathcal{U}] \) is a lisse étale \( \overline{\mathcal{O}}_{\ell} \)-sheaf on \( \mathcal{U} \) with finite monodromy group \( \Gamma \), corresponding to the regular representation of \( \Gamma \) over \( \overline{\mathcal{O}}_{\ell} \). Since \( \Gamma \) 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 \( \Gamma \) is finite, all elements act semisimply. Furthermore, if the extension of constant fields in \( K'/K \) is trivial, the geometric étale fundamental group \( \pi_1(\mathcal{U} \times \overline{k_0}) \) maps surjectively to \( \Gamma \). 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 \( p_0 \neq 0 \). In the present section we also assume that \( \text{End}_{\overline{K}}(\phi) = A \). Note that this is stronger than \( \text{End}_K(\phi) = A \). We will prove the following special case of Theorem A:

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

\[
\overline{\rho}_p : G_K \rightarrow \text{Aut}_{k_p} (\phi[p])
\]

is absolutely irreducible.

The idea of the proof is this: If \( \overline{\rho}_p \) is irreducible, but not absolutely irreducible, we can consider it as a representation of some smaller dimension \( s_p \) over an extension of \( k_p \). The determinant of this representation is then an abelian character \( \overline{\chi}_p \). Using information on the ramification in \( \rho_p \) we show that \( \overline{\chi}_p \) 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 \( \overline{\chi}_p(\text{Frob}_x) \) for \( x \in \mathcal{X}(k_{0,d}) \) is independent of \( x \). For the original representation this implies that some product of \( s_p \) eigenvalues of \( \rho_p(\text{Frob}_x) \) modulo \( p \) is independent of \( x \).

Now the eigenvalues of \( \rho_p(\text{Frob}_x) \) are integral over \( A \) and independent of \( p \), and there are only finitely many ways to choose less than \( r \) of them. Thus if the above happens for infinitely many \( p \), there must exist an actual equality over \( A \), i.e., a non-trivial algebraic relation between the eigenvalues of \( \rho_p(\text{Frob}_x) \) 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 \( \rho_p(G_K) \) is Zariski dense in \( \text{GL}_r \).

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 \( G_{\text{geom}}^K \) with the image of the identity element.

### 3.1. The setup

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

To prove Theorem 3.1 we must show that \( s_p = 1 \) for almost all \( p \). 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 $p \in S$ the representation $\overline{\rho}_p$ factors through $\text{GL}_t(k_{p,s})$.

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

$$\det_s : \text{GL}_t(k_{p,s}) \longrightarrow k^*_p,$$

for the determinant map and consider the composite homomorphism

$$\overline{\tau}_p := \det_s \circ \overline{\rho}_p : G_K \longrightarrow k^*_p.$$

Lemma 3.3. There is a finite field extension $K'/K$, such that for every prime $p \in S$ the character $\overline{\tau}_p$ is trivial on $G^\text{geom}_{K'}$.

Proof. Proposition 2.7 implies that there is a finite extension $K_1/K$, such that for all closed points $x \in X$ the inertia subgroup of $G_{K_1}$ at $x$ has trivial image in $k^*_p$, so the restriction of $\overline{\tau}_p$ to $G_{K_1}$ is unramified everywhere. This means that $\overline{\tau}_p|_{G_{K_1}}$ factors through $\text{Gal}(K_{1,\text{nr}}/K_1)$. Moreover, it obviously factors through the maximal abelian quotient $\text{Gal}(K^{\text{ab, nr}}_{1}/K_1)$.

Further, the image of $G^\text{geom}_{K_1}$ in $\text{Gal}(K^{\text{ab, nr}}_{1}/K_1)$ is finite by Katz–Lang [8, Theorem 2]. Therefore $\overline{\tau}_p|_{G^\text{geom}_{K_1}}$ has finite order, and so the restriction to some finite extension $K'$ of $K_1$ is trivial, as desired. □

It is sufficient to prove Theorem 3.1 for the restriction of $\overline{\rho}_p$ 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 $p$ in $S$ the character $\overline{\tau}_p$ factors through a homomorphism $\overline{\tau}_p : G_{k_0} \to k^*_p$. The following commutative diagram with exact rows sums up the various mappings:
3.2. Algebraic relations in \( \text{GL}_r \)

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

\[
f^{(t)}(T) := \prod_{I} \left( T - \prod_{i \in I} z_i \right),
\]

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 \( z_i \), 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 \( f^{(t)}(z) = 0 \) if and only if \( f \) has \( t \) zeros with product \( z \).

In the next lemma, we use Assumption 3.2 that \( S \) is infinite. Recall that \( f_x \) denotes the characteristic polynomial of \( \rho_p(\text{Frob}_x) \). 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 \( p \in S \). By Lemma 3.3, we know that

\[
\overline{\rho}_p(\text{Frob}_x) = \overline{\rho}_p(\text{Frob}_{x'}) = \overline{\rho}_p(\text{Frob}_{x'}),
\]

so the determinants of \( \overline{\rho}_p(\text{Frob}_x) \) and \( \overline{\rho}_p(\text{Frob}_{x'}) \) over \( k_{0,s}^p \) are equal. Thus, if we consider \( \overline{\rho}_p(\text{Frob}_x) \) and \( \overline{\rho}_p(\text{Frob}_{x'}) \) as elements of \( \text{GL}_r(k_{p,s}) \), 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 \( p \) to the characteristic polynomials of \( \overline{\rho}_p(\text{Frob}_x) \) and \( \overline{\rho}_p(\text{Frob}_{x'}) \) as elements of \( \text{GL}_r(k_p) \), respectively. So \( g_x \) and \( g_{x'} \) divide \( f_x \) and \( f_{x'} \) modulo \( p \), respectively, as polynomials over \( k_p \). Therefore \( f_x^{(t)} \) and \( f_{x'}^{(t)} \) must have a common zero modulo \( p \); hence their resultant vanishes modulo \( p \). Since this happens for the infinitely many \( p \in S \), the assertion follows. \( \square \)

Next we use Lemma 3.4 to analyze the representation at any fixed prime \( p \neq p_0 \) of \( A \). For \( n > 0 \) we denote the images of the Galois groups \( G_K \) and \( G_{K}^{\text{geom}} \) under the representation \( \rho_p \) modulo \( p^n \) by \( \Gamma_{p,n} \) and \( \Gamma_{p,n}^{\text{geom}} \), respectively. We set \( \Gamma_{p,n}^{(t)} := \)
Let $\Gamma_{p,n}/\Gamma_{p,n}^{\text{geom}}$ and obtain the following diagram with exact rows:

\[
\begin{array}{ccccccc}
1 & \rightarrow & G_K^{\text{geom}} & \rightarrow & G_K & \rightarrow & G_{k_0} & \rightarrow & 1 \\
1 & \rightarrow & \Gamma_{p,n}^{\text{geom}} & \rightarrow & \Gamma_{p,n} & \rightarrow & \Gamma_{p,n}'' & \rightarrow & 1 \\
\cap & & \cap & & \cap & & \cap & & \cap \\
\end{array}
\]

\[
\text{SL}_r(A/p^n) \quad \text{GL}_r(A/p^n)
\]

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

**Lemma 3.5.** For every $p$ and $n$ there exists $d > 0$, such that every element of $\Gamma_{p,n}^{\text{geom}}$ is the image of $\text{Frob}_x$ for some $x \in \mathcal{U}(k_0,d)$.

**Proof.** Let $K_{p,n}$ be the finite Galois extension of $K$ with Galois group $\Gamma_{p,n}$. Then its constant field is $k_{0,e}$ for $e := |\Gamma_{p,n}''|$, and $K_{p,n}/Kk_{0,e}$ is a finite Galois extension with Galois group $\Gamma_{p,n}^{\text{geom}}$ 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 $\Gamma_{p,n}^{\text{geom}}$. □

Now let

\[
\Gamma_p \subset \text{GL}_r(A_p) \quad \text{and} \quad \Gamma_p^{\text{geom}} \subset \text{SL}_r(A_p)
\]

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

**Lemma 3.6.** Let $\gamma \in \Gamma_p^{\text{geom}}$ and let $f_\gamma$ be its characteristic polynomial. Then $f_\gamma^{(1)}(1)$ 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 $\text{Frob}_x$ maps to $\gamma \mod p^n$ and $\text{Frob}_{x'}$ to the identity element in $\Gamma_{p,n}^{\text{geom}}$. Setting $h(T) := (T - 1)^r$, we get

\[
f_x \equiv f_\gamma \mod p^n \quad \text{and} \quad f_{x'} \equiv h \mod p^n.
\]
Thus

\[ f_x^{(t)}(t) \equiv f_{\gamma}^{(t)}(t) \pmod{p^n} \]

and

\[ f_x^{(t)}(t) \equiv h^{(t)} = (T - 1)^{(t)}(t) \pmod{p^n}. \]

By Lemma 3.4 the resultant of \( f_x^{(t)}(t) \) and \( f_x^{(t)}(t) \) vanishes; hence the resultant of \( f_{\gamma}^{(t)}(t) \) and \( (T - 1)^{(t)}(t) \) is congruent 0 modulo \( p^n \). Since this is so for all \( n \), the latter resultant must vanish. But this implies that \( f_{\gamma}^{(t)}(1) = 0. \)

3.3. Conclusion

Now we exploit the Zariski density statement from Theorem 2.1.

**Lemma 3.7.** For any field \( k \), the commutator subgroup \( \Gamma' \) of any Zariski dense subgroup \( \Gamma \subset \text{GL}_r(k) \) is a Zariski dense subgroup of \( \text{SL}_r(k) \).

**Proof.** Since all commutators of \( \text{GL}_r \) lie in \( \text{SL}_r \), we have \( \Gamma' \subset \text{SL}_r(k) \). The assertion is obvious for \( r \leq 1 \), so we assume \( r \geq 2 \). Then \( \Gamma \) contains a non-central element \( \gamma \). The morphism

\[ \text{GL}_r, k \to \text{SL}_r, k, \quad g \mapsto \gamma g^\gamma g^{-1} \]

then takes the value 1 at \( g = 1 \) and at least one other value. As \( \text{GL}_r, k \) is connected, it follows that the image of this morphism is not finite. By Zariski density we can therefore find \( \delta \in \Gamma \), such that \( \gamma \delta^\gamma g^\gamma g^{-1} \in \Gamma' \) is non-central. Thus the Zariski closure \( H \subset \text{SL}_r, k \) of \( \Gamma' \) is non-central. But by construction \( H \) is normalized by \( \Gamma \); hence it is also normalized by the Zariski closure of \( \Gamma \), which is \( \text{GL}_r, k \). Since \( \text{SL}_r, k \) possesses no non-central proper normal algebraic subgroups, it follows that \( H = \text{SL}_r, k \), as desired. \( \square \)

**Lemma 3.8.** \( \Gamma_p^{\text{geom}} \) is Zariski dense in \( \text{SL}_r, \mathbb{F}_p \).

**Proof.** Since \( \Gamma_p^{\text{geom}} \subset \text{SL}_r(\mathbb{F}_p) \), and the commutator subgroup of \( \Gamma_p \) is contained in \( \Gamma_p^{\text{geom}} \), this is a direct consequence of Lemma 3.7. \( \square \)

We are now ready to draw the desired conclusion:
Proof of Theorem 3.1. For \( g \in \GL_{r,F_p} \) we denote the characteristic polynomial by \( f_g \). Then

\[
\psi : \GL_{r,F_p} \to \mathbb{A}_F, \quad g \mapsto f_g(1)
\]
is a morphism of algebraic varieties. Its restriction to \( \SL_{r,F_p} \) is non-constant, for instance because its value on the following kind of diagonal matrices is

\[
\begin{pmatrix}
\alpha \\
\vdots \\
\alpha \\
\alpha^{r-1}+1
\end{pmatrix} = (1 - \alpha^1)^{(r-1)} \cdot (1 - \alpha^{r-1})^{(r-1)}.
\]

On the other hand, by Lemmata 3.6 and 3.8 we know that \( \psi(\Gamma_{p}^{\text{geom}}) = 0 \) and that \( \Gamma_{p}^{\text{geom}} \) is Zariski dense in \( \SL_{r,F_p} \). In view of this contradiction, Assumption 3.2 turns out to be false, and the theorem is proven.

\[\square\]

4. The case of an arbitrary endomorphism ring

In this section we will prove Theorem B, where \( E := \End_K(\phi) \) is arbitrary. Setting \( E_p := E \otimes A \rightarrow T_p(\phi) \) for almost all \( p \).

To explain the strategy, we assume that \( E' := \End_K(\phi) \) 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 \( \phi' \) denote the tautological extension of \( \phi \) to a Drinfeld \( E' \)-module, which by construction is defined over a finite extension \( K' \) of \( K \). Then for almost all \( p \) we have \( E'/pE' = \bigoplus_{\mathfrak{p} | p} k_{\mathfrak{p}} \), and hence \( \phi(p) = \bigoplus_{\mathfrak{p} | p} \phi'_{\mathfrak{p}} \). By Taguchi’s theorem in the form of Proposition 2.3, these direct summands are pairwise inequivalent irreducible \( k_{\mathfrak{p}} \)-modules for almost all \( p \), and by Theorem 3.1 they are absolutely irreducible over \( k_{\mathfrak{p}} \). Thus \( \phi(p) \) is a semisimple \( k_{\mathfrak{p}} \)-module, such that \( \End_{k_{\mathfrak{p}}}(\phi(p)) \cong E'/pE' \). Via Galois descent, we can deduce from this that \( \phi(p) \) is a semisimple \( k_{\mathfrak{p}} \)-module, such that \( \End_{k_{\mathfrak{p}}}(\phi(p)) \cong E/pE \), for almost all \( p \). By the theorem on bicommutants this means that \( k_{\mathfrak{p}}[\hat{G}_K] \) surjects to \( \End_{E/pE}(\phi(p)) \) for almost all \( p \).

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

4.1. The action of the endomorphism ring

Proposition 4.1. (a) For every ideal \( \alpha \notdivides p_0 \) of \( A \) the natural homomorphism

\[
E/\alpha E \to \End_{A/\alpha}(\phi[\alpha])
\]
is injective.
(b) For every prime $p \neq p_0$ of $A$ the natural homomorphism

$$E_p \rightarrow \text{End}_{A_p}(T_p(\phi))$$

is injective and its image is a direct summand.

**Proof.** To prove (a) we first assume that $a$ is principal, say $a = (a)$. Then $\phi[a] = \ker(\phi_a: K \rightarrow \overline{K})$. Since $a \not\in p_0$, the polynomial $\phi_a$ is separable, and by the right division algorithm in $K\{\tau\}$ it generates the left ideal of all polynomials vanishing on $\phi[a]$. Consider any element $\alpha$ in the kernel of $E \rightarrow \text{End}_{A/(a)}(\phi[a])$. Then $\alpha = \beta \phi_a$ for some element $\beta \in K\{\tau\}$. Both $\alpha$ and $\phi_a$ commute with $\phi_b$ for all $b \in A$; hence so does $\beta$. Thus $\beta \in E$, and so $\alpha \in Ea = aE$. This implies (a) whenever $a$ is principal.

For general $a$ choose any $a \in a \setminus p_0$. Then $\phi[a] \subset \phi[\langle a \rangle]$ are free modules of rank $r$ over $A/a$ and $A/(a)$, respectively; hence

$$\text{End}_{A/(a)}(\phi[a]) \cong \text{Mat}_{r \times r}(A/a) \cong \text{End}_{A/(a)}(\phi[\langle a \rangle]) \otimes_A A/a.$$  

By the principal ideal case we have

$$E/aE \hookrightarrow \text{End}_{A/(a)}(\phi[\langle a \rangle]) \cong \text{Mat}_{r \times r}(A/(a)).$$

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 $A/a$. It follows that

$$E/aE \hookrightarrow \text{End}_{A/(a)}(\phi[\langle a \rangle]) \otimes_A A/a \cong \text{End}_{A/a}(\phi[a])$$

is a direct summand, proving (a). Applying (a) to $a = p^n$ and taking the projective limit over $n$ shows (b). \qed

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 $\phi$ is $r = cde$ for an integer $d > 0$. For every prime $p$ of $A$ we abbreviate

$$Z_p := Z \otimes_A A_p.$$  

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

$$Z_p = \bigoplus_{\mathfrak{p} | \mathfrak{p}} Z_{\mathfrak{p}}$$
with complete discrete valuation rings $\mathbb{Z}_\mathfrak{p}$, and

$$E_p \cong \text{Mat}_{e \times e}(Z_p) = \bigoplus_{\mathfrak{q} \mid p} \text{Mat}_{e \times e}(Z_{\mathfrak{q}}).$$

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

$$Z/pZ = \bigoplus_{\mathfrak{q} \mid p} k_{\mathfrak{q}}$$

and

$$E/pE \cong \text{Mat}_{e \times e}(Z/pZ) = \bigoplus_{\mathfrak{q} \mid p} \text{Mat}_{e \times e}(k_{\mathfrak{q}}).$$

For $\mathfrak{q} | p$ as in Lemma 4.2 we let $E_p \cong \text{Mat}_{e \times e}(Z_p)$ act on $Z_{\mathfrak{q}}^{\oplus e}$ in the obvious way. We are interested in the $\mathbb{Z}_\mathfrak{p}$-module $W_{\mathfrak{q}} := \text{Hom}_{E_p}(Z_{\mathfrak{q}}^{\oplus e}, T_p(\phi))$ and the $k_{\mathfrak{q}}$-vector space $\overline{W_{\mathfrak{q}}} := W_{\mathfrak{q}}/\mathfrak{q}W_{\mathfrak{q}}$.

**Lemma 4.3.** For almost all primes $p$ of $A$ the evaluation homomorphism

$$\bigoplus_{\mathfrak{q} \mid p} W_{\mathfrak{q}} \otimes_{\mathbb{Z}_\mathfrak{p}} Z_{\mathfrak{q}}^{\oplus e} \longrightarrow T_p(\phi)$$

and, if $Z$ is separable over $A$, the induced homomorphism

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

are isomorphisms. Moreover $W_{\mathfrak{q}}$ is a free $\mathbb{Z}_\mathfrak{q}$-module of rank $d$, and $\overline{W_{\mathfrak{q}}}$ is a $k_{\mathfrak{q}}$-vector space of dimension $d$.

**Proof.** We begin with some preliminary remarks on modules over matrix rings. For any commutative ring with identity $R$ let $I_{ij} \in \text{Mat}_{e \times e}(R)$ denote the matrix with a single entry 1 in row $i$ and column $j$ and all other entries 0. Consider any $\text{Mat}_{e \times e}(R)$-module $M$. Then the orthogonal idempotents $I_{ii}$ induce a direct sum decomposition of $M$ into $R$-modules $M_i$, and the matrices $I_{ij}$ for $i \neq j$ induce isomorphisms between all $M_i$. From this one deduces easily that $M \cong M_{1}^{\oplus e}$ as a $\text{Mat}_{e \times e}(R)$-module. In addition, one obtains a natural isomorphism $M_1 \cong \text{Hom}_{\text{Mat}_{e \times e}(R)}(R^{\oplus e}, M)$, such that the evaluation map $M_1 \otimes_R R^{\oplus e} \rightarrow M$ is an isomorphism.
Returning to the lemma, note that the tautological embedding $Z \hookrightarrow E \hookrightarrow K\{\tau\}$ is a Drinfeld $Z$-module extending $\phi$. We call it $\psi$ and observe that its rank is $r/[Z/A] = de$. Then for any $p$ as in Lemma 4.2 we have a natural isomorphism

$$T_p(\phi) \cong \bigoplus_{\mathfrak{q}|p} T_{\mathfrak{q}}(\psi),$$

where $T_{\mathfrak{q}}(\psi)$ is a free $Z_p$-module of rank $de$. Next, the preliminary remarks applied to $R = Z_\mathfrak{q}$ and $M = T_{\mathfrak{q}}(\psi)$ yield an isomorphism

$$W_\mathfrak{q} \otimes_{Z_\mathfrak{q}} Z_\mathfrak{q}^{\otimes e} \sim T_{\mathfrak{q}}(\psi).$$

By construction $W_\mathfrak{q}$ is a submodule of a finitely generated free $Z_\mathfrak{q}$-module; hence it is itself finitely generated and free. The preceding isomorphism thus shows that the rank of $W_\mathfrak{q}$ is $d$. The lemma follows from this by combining everything and reducing modulo $p$. □

**Remark 4.4.** Letting $G_K$ act trivially on $Z_\mathfrak{q}^{\otimes e}$ and $k_\mathfrak{q}^{\otimes e}$, by functoriality we obtain natural continuous representations of $G_K$ on $W_\mathfrak{q}$ and on $W_\mathfrak{q}'$. By construction the isomorphisms in Lemma 4.3 are then equivariant under $A_p[G_K] \otimes_{A_p} E_p$, where $A_p[G_K]$ acts on the left-hand side through the first and $E_p$ through the second tensor factors.

### 4.2. The residual representation

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

**Lemma 4.5.** *For almost all $p$ and all $\mathfrak{q}|p$ the $\overline{W_\mathfrak{q}}$ are irreducible $k_p[G_K]$-modules and pairwise inequivalent, and in particular, $\phi[p]$ is a semisimple $k_p[G_K]$-module.*

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

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

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

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

**Lemma 4.6.** 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 $\text{Gal}(K'/K)$ 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. □

**Lemma 4.7.** Let $A'$ be a maximal commutative $A$-subalgebra of $E'$ which is separable over $A$. Then for almost all $p$ the natural map

$$A'/pA' \rightarrow \text{End}_{A'/pA'[G_{K'}]}(\phi[p])$$

is an isomorphism.

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

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

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

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

Putting these facts together, we deduce that

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

as desired. □

**Lemma 4.8.** For almost all $p$ the natural map

$$E'/pE' \rightarrow \text{End}_{k_{p}[G_{K'}]}(\phi[p])$$

is an isomorphism.
Proof. After replacing $K$ by $K'$ we may assume that $E' = E$, which by Lemma 4.6 preserves the separability of $Z$ over $A$. We will then use the isomorphism from Lemma 4.3. As the $\overline{W}_{\Psi}$ are irreducible $k_{\Psi}[G_{K}]$-modules by Lemma 4.5, Schur’s lemma and Wedderburn’s theorem force

$$\ell_{\Psi} := \text{End}_{k_{\Psi}[G_{K}]}(\overline{W}_{\Psi})$$

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

$$\text{End}_{k_{\Psi}[G_{K}]}(\phi[\mathfrak{p}]) \cong \bigoplus_{\Psi|\mathfrak{p}} \text{End}_{k_{\Psi}[G_{K}]}(\overline{W}_{\Psi} \otimes_{k_{\Psi}} k_{\Psi}^{\otimes e})$$

$$= \bigoplus_{\Psi|\mathfrak{p}} \text{End}_{k_{\Psi}[G_{K}]}(\overline{W}_{\Psi}) \otimes_{k_{\Psi}} \text{End}_{k_{\Psi}}(k_{\Psi}^{\otimes e})$$

$$= \bigoplus_{\Psi|\mathfrak{p}} \ell_{\Psi} \otimes_{k_{\Psi}} \text{Mat}_{e \times e}(k_{\Psi}).$$

Since $E \otimes_{A} F$ is a simple $F$-algebra, by Bourbaki [2, §10(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 $\text{Mat}_{e \times e}(k_{\Psi})$, the above decomposition implies that

$$\text{End}_{A'/pA'[G_{K}]}(\phi[\mathfrak{p}]) \supset \bigoplus_{\Psi|\mathfrak{p}} \ell_{\Psi} \otimes_{k_{\Psi}} A'/\Psi A'.$$

But here by Lemma 4.7 the left-hand side is

$$A'/pA' = \bigoplus_{\Psi|\mathfrak{p}} A'/\Psi A'$$

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

$$\text{End}_{k_{\Psi}[G_{K}]}(\phi[\mathfrak{p}]) \cong \bigoplus_{\Psi|\mathfrak{p}} \text{Mat}_{e \times e}(k_{\Psi}) \cong E/pE,$$

as desired. □

Lemma 4.9. For almost all primes $\mathfrak{p}$ of $A$ we have $E/pE \cong (E'/pE')^{G_{K}}$. 
Proof. The group $G_K$ acts on $E'$ through the finite quotient $G := \text{Gal}(K'/K)$. We consider the homomorphism

$$\varepsilon : E' \rightarrow \bigoplus_{g \in G} E', \quad x \mapsto \left( (g - 1)x \right)_{g \in G},$$

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

$$0 \rightarrow E \rightarrow E' \rightarrow \text{im } \varepsilon \rightarrow 0$$

and

$$0 \rightarrow \text{im } \varepsilon \rightarrow \bigoplus_{g \in G} E' \rightarrow \text{coker } \varepsilon \rightarrow 0.$$

Now all these modules are of finite type over $A$, so they are locally free at almost all primes $p$. For those $p$ the modules $\text{Tor}^A_1(\text{im } \varepsilon, A/p)$ and $\text{Tor}^A_1(\text{coker } \varepsilon, A/p)$ vanish, so the sequences remain exact after tensoring with $A/p$. Therefore the sequence

$$0 \rightarrow E/pE \rightarrow E'/pE' \xrightarrow{\bar{\varepsilon}} \bigoplus_{g \in G} E'/pE'$$

with $\bar{\varepsilon} = \varepsilon \mod p$ is exact. It follows that

$$E/pE = \ker \bar{\varepsilon} = (E'/pE')^G,$$

as desired. □

Lemma 4.10. For almost all $p$ the natural map

$$E/pE \rightarrow \text{End}_{k_p[G_K]}(\phi[p])$$

is an isomorphism.

Proof. By Lemma 4.8 the natural map

$$E'/pE' \rightarrow \text{End}_{k_p[G_{K'}]}(\phi[p])$$

is an isomorphism for almost all $p$. On both sides we have an action of $G_K$. The invariants on the right-hand side are $\text{End}_{k_p[G_K]}(\phi[p])$, and for almost all $p$ the invariants on the left-hand side are $E/pE$ by Lemma 4.9. The assertion follows. □
Lemma 4.11. For almost all \( p \) we have a surjection

\[
k_p[G_K] \longrightarrow \text{End}_{E/pE}(\phi[p]) \cong \bigoplus_{\Psi|p} \text{End}_{k_p}(W_{\Psi}) \cong \bigoplus_{\Psi|p} \text{Mat}_{d \times d}(k_{\Psi}),
\]

and in particular, the \( W_{\Psi} \) are pairwise inequivalent \( k_p[G_K] \)-modules which are absolutely irreducible over \( k_{\Psi} \).

Proof. Lemma 4.5 says that \( \phi[p] \) is a semisimple \( k_p[G_K] \)-module for almost all \( p \). Therefore the image of \( k_p[G_K] \) in \( \text{End}_{p}(\phi[p]) \) is its own bicommutant. Since its commutant is \( E/pE \) by Lemma 4.10, we deduce that \( k_p[G_K] \) surjects to \( \text{End}_{E/pE}(\phi[p]) \). The isomorphisms on the right-hand side follow from Lemmata 4.2 and 4.3. □

4.3. The representation on the Tate module

Now abbreviate \( W_p := \bigoplus_{\Psi|p} W_{\Psi} \) and note that \( T_p(\phi) \cong W_p^{\otimes e} \) as \( A_p[G_K] \)-modules by Lemma 4.3.

Lemma 4.12. For almost all primes \( p \) of \( A \), every \( A_p[G_K] \)-submodule of \( W_p \) has the form \( \alpha(W_p) \) for some \( \alpha \in Z_p \).

Proof. Consider any \( A_p[G_K] \)-submodule \( H'_p \subset W_p \). Then we can apply Proposition 2.5 to the \( A_p[G_K] \)-submodule \( (H'_p)^{\otimes e} \subset (W_p)^{\otimes e} \cong T_p(\phi) \), showing that \( (H'_p)^{\otimes e} = \alpha(T_p(\phi)) \) for some \( \alpha \in E_p \). Recall from Lemma 4.2 that \( E_p \cong \text{Mat}_{e \times e}(Z_p) \), and let \( \alpha_1, \ldots, \alpha_e \in Z_p \) denote the entries of any chosen row of \( \alpha \). Then \( H'_p = \sum_{i=1}^{e} \alpha_i(W_p) \). Now Lemma 4.2 also implies that for almost all \( p \), every ideal in \( Z_p \) is a principal ideal. Thus \( H'_p = \alpha(W_p) \) for some \( \alpha \in Z_p \), as desired. □

Lemma 4.13. Let \( R \) be a commutative ring with identity, and let \( M := R^{\otimes d} \) for some integer \( d \geq 1 \). Let \( B \subset \text{End}_R(M) = \text{Mat}_{d \times d}(R) \) be a subring (not necessarily an \( R \)-subalgebra) satisfying the properties:

(a) Every \( B \)-submodule of \( M \) has the form \( \alpha M \) for an ideal \( \alpha \subset R \).

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

Then the following statements are true:

(c) Consider integers \( r, s \geq 0 \) and a maximal ideal \( m \subset R \), such that there exists a \( B \)-linear surjection \( M^{\oplus r} \to (M/mM)^{\oplus s} \). 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 \( m \subset R \) the induced homomorphism \( N \to (M/mM)^{\oplus r} \) is surjective. Then \( N = M^{\oplus r} \).

(e) Assume moreover that for all maximal ideals \( m \subset R \) the induced homomorphism \( B \to \text{Mat}_{d \times d}(R/m) \) is surjective. Then \( B = \text{Mat}_{d \times d}(R) \).
Proof. First consider any maximal ideal \( m \subset R \). Then \( M/mM \) is a simple \( B \)-module, because by (a) there exist no other \( B \)-submodules between \( mM \) and \( M \).

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

We can now prove (c). Consider a \( B \text{-linear surjection} \ f : M^{\oplus r} \to (M/mM)^{\oplus s} \). We can view it as an \( s \times r \)-matrix of \( B \text{-linear homomorphisms} \ M \to M/mM \). By the preceding remarks any such homomorphism vanishes on \( mM \). Therefore \( f \) comes from a \( B \text{-linear surjection} \ (M/mM)^{\oplus r} \to (M/mM)^{\oplus s} \). Since \( M/mM \) 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 \( M \overset{l}{\to} M^{\oplus r} \overset{\pi}{\to} M^{\oplus (r-1)} \) 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 \( l^{-1}(N) = aM \) for some ideal \( a \subset R \). Thus, we have an inclusion of short exact sequences of \( B \)-modules:

\[
\begin{array}{cccc}
0 & \longrightarrow & M & \longrightarrow & M^{\oplus r} & \longrightarrow & M^{\oplus (r-1)} & \longrightarrow & 0 \\
& & \cup & & \cup & & \| & & \\
0 & \longrightarrow & aM & \longrightarrow & N & \longrightarrow & M^{\oplus (r-1)} & \longrightarrow & 0.
\end{array}
\]

Suppose that \( a \neq R \). Then we can choose a maximal ideal \( m \subset R \) containing \( a \). The image of \( aM \) in \( (M/mM)^{\oplus r} \) is then zero; hence the homomorphism \( N \to (M/mM)^{\oplus r} \), which by assumption is surjective, factors through a \( B \text{-linear surjection} \ M^{\oplus (r-1)} \to (M/mM)^{\oplus r} \). But by (c) this is impossible. Therefore \( a = R \), 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 \( B \subset \text{Mat}_{d \times d}(R) \cong M^{\oplus d} \). \( \square \)

Proposition 4.14. For almost all \( p \) we have a surjection

\[ A_p[G_K] \longrightarrow \text{End}_E_p(T_p(\phi)) \cong \bigoplus_{\Psi|p} \text{End}_{Z_p}(W_p) \cong \bigoplus_{\Psi|p} \text{Mat}_{d \times d}(Z_p). \]

Proof. The isomorphisms on the right-hand side follow from Lemmata 4.2 and 4.3, which also show that \( Z_p = \bigoplus_{\Psi|p} Z_p \) and \( W_p \cong Z_p^{\oplus d} \). Let \( B_p \subset \text{Mat}_{d \times d}(Z_p) \) denote the image of the homomorphism in question. To prove equality we will show that \( B := B_p \) satisfies the assumptions of Lemma 4.13 with \( R := Z_p \) and \( M := W_p \). First, assumption 4.13 (a) follows directly from Lemma 4.12.

For the other assumptions we want to use Lemma 4.11, 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 $p$ of $A$ are in bijection with the primes $p'$ of $A'$, with equal residue fields. Now the tautological embedding $A' \subset Z \subset E \hookrightarrow K[\tau]$ is a Drinfeld $A'$-module $\phi'$ extending $\phi$, such that $T_p(\phi) = T_p'(\phi')$ for almost all $p$. Since $Z$ is separable over $A'$, applying Lemma 4.11 to $\phi'$ shows that for almost all $p$ we have a surjection

$$k_{p'}[G_K] \longrightarrow \bigoplus_{\mathfrak{p}|p'} \text{End}_{k_{\mathfrak{p}}} \left(W_{\mathfrak{p}}\right) \cong \bigoplus_{\mathfrak{p}|p'} \text{Mat}_{d \times d}(k_{\mathfrak{p}}).$$

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

$$B_p \longrightarrow \bigoplus_{\mathfrak{p}|p} \text{End}_{k_{\mathfrak{p}}} \left(W_{\mathfrak{p}}\right) \cong \bigoplus_{\mathfrak{p}|p} \text{Mat}_{d \times d}(k_{\mathfrak{p}}).$$

With $m := \mathfrak{p}$, $R/m = k_{\mathfrak{p}}$, and $M/mM = \overline{W_{\mathfrak{p}}}$ we deduce that the assumptions in 4.13 (b) and (e) are satisfied. Thus Lemma 4.13 implies that $B_p = \text{Mat}_{d \times d}(Z_p)$, as desired.

Finally, Proposition 4.14 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


