COMPOSITIO MATHEMATICA

ℓ-independence for compatible systems of (mod ℓ) representations

Chun Yin Hui

Compositio Math. **151** (2015), 1215–1241.

doi:10.1112/S0010437X14007969

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY 150 YEARS

Compositio Math. 151 (2015) 1215–1241
doi:10.1112/S0010437X14007969

ℓ-independence for compatible systems of (mod ℓ) representations

Chun Yin Hui

Abstract

Let K be a number field. For any system of semisimple mod ℓ Galois representations $\{\phi_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_N(\mathbb{F}_\ell)\}_\ell$ arising from étale cohomology (Definition 1), there exists a finite normal extension L of K such that if we denote $\phi_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/K))$ and $\phi_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/L))$ by $\bar{\Gamma}_\ell$ and $\bar{\gamma}_\ell$, respectively, for all ℓ and let $\bar{\mathbf{S}}_\ell$ be the $\mathbb{F}_\ell$-semisimple subgroup of $\mathrm{GL}_{N,\mathbb{F}_\ell}$ associated to $\bar{\gamma}_\ell$ (or $\bar{\Gamma}_\ell$) by Nori's theory [*On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$, Invent. Math. **88** (1987), 257–275] for sufficiently large ℓ, then the following statements hold for all sufficiently large ℓ.

A(i) The formal character of $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ (Definition 1) is independent of ℓ and equal to the formal character of $(\mathbf{G}_\ell^\circ)^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$, where $(\mathbf{G}_\ell^\circ)^{\mathrm{der}}$ is the derived group of the identity component of $\mathbf{G}_\ell$, the monodromy group of the corresponding semi-simplified ℓ-adic Galois representation Φ_ℓ^{ss}.

A(ii) The non-cyclic composition factors of $\bar{\gamma}_\ell$ and $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ are identical. Therefore, the composition factors of $\bar{\gamma}_\ell$ are finite simple groups of Lie type of characteristic ℓ and are cyclic groups.

B(i) The total ℓ-rank $\mathrm{rk}_\ell\bar{\Gamma}_\ell$ of $\bar{\Gamma}_\ell$ (Definition 14) is equal to the rank of $\bar{\mathbf{S}}_\ell$ and is therefore independent of ℓ.

B(ii) The A_n-type ℓ-rank $\mathrm{rk}_\ell^{A_n}\bar{\Gamma}_\ell$ of $\bar{\Gamma}_\ell$ (Definition 14) for $n \in \mathbb{N}\backslash\{1,2,3,4,5,7,8\}$ and the parity of $(\mathrm{rk}_\ell^{A_4}\bar{\Gamma}_\ell)/4$ are independent of ℓ.

Contents

1. Introduction

Let K be a number field, $\mathscr{P} \subset \mathbb{N}$ the set of prime numbers, and X a complete non-singular variety defined over K. For $0 \leqslant i \leqslant 2\dim X$, the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ acts on the ith ℓ-adic étale cohomology group $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)$ for each prime number $\ell \in \mathscr{P}$. The dimension

Received 15 May 2013, accepted in final form 19 August 2014, published online 2 March 2015.
2010 Mathematics Subject Classification 11F80, 14F20, 20D05 (primary).
Keywords: Galois representations, ℓ-independence, big Galois image, étale cohomology.
Major revisions of the paper were done while the author was a postdoctoral fellow at The Hebrew University of Jerusalem, supported by Aner Shalev's ERC Advanced Grant no. 247034.

of $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)$ as a $\mathbb{Q}_\ell$-vector space is independent of ℓ and we denote it by N. We therefore obtain a system of continuous, ℓ-adic Galois representations indexed by $\mathscr{P}$,

$$\{\Phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{Q}_\ell)\}_{\ell \in \mathscr{P}},$$

which satisfies strict compatibility [Del74] in the sense of Serre [Ser98, ch. 1]. An ℓ-independence [Ser94] has been conjectured on the images of $\{\Phi_\ell\}$, which has been studied by many people. When X is an elliptic curve without complex multiplication, Serre proved that the Galois action on the ℓ-adic Tate module $T_\ell(X)$ is the whole $\mathrm{GL}(T_\ell(X))$ when ℓ is sufficiently large, by showing that the Galois action ϕ_ℓ on ℓ-torsion points $X[\ell] \cong T_\ell(X)/\ell T_\ell(X)$,

$$\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}(X[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell),$$

is surjective for $\ell \gg 1$ (see [Ser72]). This paper is motivated by the idea that the largeness of the ℓ-adic Galois image $\Gamma_\ell := \Phi_\ell(\mathrm{Gal}_K)$ can be studied by *taking* mod ℓ *reduction*. More precisely, given any continuous ℓ-adic representation $\Phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{Q}_\ell)$, one can find a Galois stable $\mathbb{Z}_\ell$-lattice of $\mathbb{Q}_\ell^N$ such that, up to some change of coordinates, we may assume that $\Phi_\ell(\mathrm{Gal}_K) \subset \mathrm{GL}_N(\mathbb{Z}_\ell)$ since Gal_K is compact. Then, by taking mod ℓ reduction $\mathrm{GL}_N(\mathbb{Z}_\ell) \to \mathrm{GL}_N(\mathbb{F}_\ell)$ and semi-simplification, we obtain a continuous semisimple mod ℓ Galois representation

$$\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)$$

which is independent of the choice of the $\mathbb{Z}_\ell$-lattice by Brauer–Nesbitt [CR88, Theorem 30.16]. We denote the mod ℓ Galois image $\phi_\ell(\mathrm{Gal}_K)$ by $\bar{\Gamma}_\ell$.

Definition 1. A system of mod ℓ Galois representations

$$\{\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)\}_{\ell \in \mathscr{P}}$$

is said to be *arising from étale cohomology* if it is the semi-simplification of a mod ℓ reduction of the ℓ-adic system or its dual system,

$$\{\Phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}(H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell))\}_{\ell \in \mathscr{P}},$$
$$\{\Phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}(H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)^\vee)\}_{\ell \in \mathscr{P}},$$

for a complete non-singular variety X defined over K and some i, where $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)^\vee := \mathrm{Hom}_{\mathbb{Q}_\ell}(H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell), \mathbb{Q}_\ell)$.

Let ρ^{ss} denote the semi-simplification for any finite-dimensional representation ρ over a perfect field (which is well-defined by Brauer–Nesbitt [CR88, Theorem 30.16]). Let $\{\Phi_\ell\}$ be a compatible system of ℓ-adic representations of Gal_K as in Definition 1; the algebraic monodromy group at ℓ of the semi-simplified system $\{\Phi_\ell^{\text{ss}}\}$, denoted by $\mathbf{G}_\ell$, is the Zariski closure of $\Phi_\ell^{\text{ss}}(\mathrm{Gal}_K)$ in $\mathrm{GL}_{N,\mathbb{Q}_\ell}$. Then $\mathbf{G}_\ell$ is reductive. Denote the sets of non-Archimedean valuations of K and $\bar{K}$ by Σ_K and $\Sigma_{\bar{K}}$, respectively. The strict compatibility of $\{\Phi_\ell\}$ implies that $\{\phi_\ell\}$ is strictly compatible in the following sense.

Definition 2. A system of mod ℓ Galois representations

$$\{\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)\}_{\ell \in \mathscr{P}}$$

is said to be *strictly compatible* if $\{\phi_\ell\}$ is continuous and semisimple and satisfies the following conditions.

(i) There is a finite subset $S \subset \Sigma_K$ such that ϕ_ℓ is *unramified* outside $S_\ell := S \cup \{v \in \Sigma_K : v \mid \ell\}$ for all ℓ.

(ii) For any $\ell_1, \ell_2 \in \mathscr{P}$ and any $\bar{v} \in \Sigma_{\bar{K}}$ extending some $v \in \Sigma_K \backslash (S_{\ell_1} \cup S_{\ell_2})$, the characteristic polynomials of $\phi_{\ell_1}(\mathrm{Frob}_{\bar{v}})$ and $\phi_{\ell_2}(\mathrm{Frob}_{\bar{v}})$ are the reductions mod ℓ_1 and mod ℓ_2 of some polynomial $P_v(x) \in \mathbb{Q}[x]$ that depends only on v.

Let $\rho : \mathbf{G} \to \mathrm{GL}_{N,F}$ be a faithful representation of a rank-r reductive algebraic group $\mathbf{G}$ defined over a field F. At the beginning of § 2 we define the *formal character* of ρ as an element of the quotient set $\mathrm{GL}_r(\mathbb{Z})\backslash\mathbb{Z}[\mathbb{Z}^r]$. Here $\mathbb{Z}[\mathbb{Z}^r]$ is the free abelian group generated by $\mathbb{Z}^r$, and $\mathrm{GL}_r(\mathbb{Z})$ acts naturally on $\mathbb{Z}[\mathbb{Z}^r]$. This allows us to define what is meant by two representations having *the same formal character* (see Definition 3′) and what it means for the formal character to be *bounded by a constant* $C > 0$ (see Definitions 4 and 4′). Let $\{\phi_\ell\}$ be a strictly compatible system of mod ℓ representations arising from étale cohomology (Definitions 1 and 2). This paper studies ℓ-independence of mod ℓ Galois images $\bar{\Gamma}_\ell$ for sufficiently large ℓ. Let $\mathfrak{g}$ be a Lie type. We define the *total ℓ-rank* $\mathrm{rk}_\ell\,\bar{\Gamma}$ and the *$\mathfrak{g}$-type ℓ-rank* $\mathrm{rk}_\ell^{\mathfrak{g}}\,\bar{\Gamma}$ of a finite group $\bar{\Gamma}$ in § 3.3, Definition 14. The main results are as follows.

THEOREM A (Main theorem). *Let K be a number field and $\{\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)\}_{\ell\in\mathscr{P}}$ a strictly compatible system of* mod ℓ *Galois representations arising from étale cohomology (Definitions 1 and 2). There exists a finite normal extension L of K such that if we denote $\phi_\ell(\mathrm{Gal}_K)$ and $\phi_\ell(\mathrm{Gal}_L)$ by $\bar{\Gamma}_\ell$ and $\bar{\gamma}_\ell$, respectively, for all ℓ and let $\bar{\mathbf{S}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ be the connected $\mathbb{F}_\ell$-semisimple subgroup associated to $\bar{\gamma}_\ell$ (or $\bar{\Gamma}_\ell$) by Nori's theory for $\ell \gg 1$, then the following hold for $\ell \gg 1$.*

(i) *The formal character of $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ is independent of ℓ (Definition 3′) and is equal to the formal character of $(\mathbf{G}_\ell^\circ)^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$, where $(\mathbf{G}_\ell^\circ)^{\mathrm{der}}$ is the derived group of the identity component of $\mathbf{G}_\ell$, the algebraic monodromy group of the semi-simplified representation Φ_ℓ^{ss}.*

(ii) *The composition factors of $\bar{\gamma}_\ell$ and $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ are identical modulo cyclic groups. Therefore, the composition factors of $\bar{\gamma}_\ell$ are finite simple groups of Lie type of characteristic ℓ and are cyclic groups.*

COROLLARY B. *Let $\bar{\mathbf{S}}_\ell$ be defined as above; then the following hold for $\ell \gg 1$.*

(i) *The total ℓ-rank $\mathrm{rk}_\ell\,\bar{\Gamma}_\ell$ of $\bar{\Gamma}_\ell$ (Definition 14) is equal to the rank of $\bar{\mathbf{S}}_\ell$ and is therefore independent of ℓ.*

(ii) *The A_n-type ℓ-rank $\mathrm{rk}_\ell^{A_n}\,\bar{\Gamma}_\ell$ of $\bar{\Gamma}_\ell$ (Definition 14) for $n \in \mathbb{N}\backslash\{1,2,3,4,5,7,8\}$ and the parity of $(\mathrm{rk}_\ell^{A_4}\,\bar{\Gamma}_\ell)/4$ are independent of ℓ.*

Remark 1.1. As an application of the main results, we prove in [HL14] that $\Phi_\ell(\mathrm{Gal}_K)$, the ℓ-adic Galois image arising from étale cohomology, has a certain maximality inside the algebraic monodromy group $\mathbf{G}_\ell$ if ℓ is sufficiently large and $\mathbf{G}_\ell$ is of type A. This generalizes Serre's open image theorem on non-CM elliptic curves [Ser72].

Remark 1.2. For any field F, define ι to be the involution of $\mathrm{GL}_{N,F}$ that sends A to $(A^t)^{-1}$. If Γ is a subgroup of $\mathrm{GL}_N(F)$, then Γ is semisimple on F^N if and only if $\iota(\Gamma)$ is semisimple on F^N. If ϕ_ℓ is the mod ℓ Galois representation arising from the dual representation $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)^\vee$ (Definition 1), then the mod ℓ representation arising from $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)$ is $\iota \circ \phi_\ell$ under a suitable basis, by Brauer–Nesbitt [CR88, Theorem 30.16]. Since ι is an automorphism of GL_N, it suffices to prove Theorem A by considering only the dual mod ℓ system $\{\phi_\ell\}$ and Galois images $\{\bar{\Gamma}_\ell\}$. Let $\phi_{\bar{v}}$ be the restriction of ϕ_ℓ to the inertia subgroup $I_{\bar{v}}$ such that $\bar{v} \in \Sigma_{\bar{K}}$ divides ℓ. The reason for choosing the dual system is that the characters of $\phi_{\bar{v}}^{\mathrm{ss}}$ have bounded exponents in the sense of Definition 8 for $\ell \gg 1$ by Serre's tame inertia conjecture, which was proved by Caruso [Car08] (see Theorem 2.3.1). Such boundedness makes our arguments simpler.

This paper can be considered as a 'mod ℓ' version of [Hui13], in which we studied ℓ-independence of monodromy groups of any compatible system of ℓ-adic representations by using the theory of abelian ℓ-adic representation [Ser98] and the representation theory of complex semisimple Lie algebras. The main difference between [Hui13] and this paper is that one gets nothing new by considering monodromy groups of mod ℓ Galois images, because they are just finite groups. The strategy in this paper is to first construct for each $\ell \gg 1$ a connected $\mathbb{F}_\ell$-reductive subgroup $\bar{\mathbf{G}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ with bounded formal characters (Definitions 4 and 4′) such that $[\bar{\Gamma}_\ell : \bar{\Gamma}_\ell \cap \bar{\mathbf{G}}_\ell(\mathbb{F}_\ell)]$ and $[\bar{\mathbf{G}}_\ell(\mathbb{F}_\ell) : \bar{\Gamma}_\ell \cap \bar{\mathbf{G}}_\ell(\mathbb{F}_\ell)]$ are both uniformly bounded (Theorem 2.0.5). The idea to construct such $\bar{\mathbf{G}}_\ell$ came from [Ser86], where Serre considered the Galois action on the ℓ-torsion points of abelian varieties A without complex multiplication. In Serre's case, the semisimple part $\bar{\mathbf{S}}_\ell$ of $\bar{\mathbf{G}}_\ell$ is constructed by Nori's theory [Nor87], and the center $\bar{\mathbf{C}}_\ell$ of $\bar{\mathbf{G}}_\ell$ is the mod ℓ reduction of some $\mathbb{Q}$-diagonalizable group $\mathbf{C}_\mathbb{Q}$, which is a subgroup of the centralizer of the monodromy $\mathbf{G}_\ell$ in $\mathrm{GL}_{N,\mathbb{Q}_\ell}$. Hence, $\{\bar{\mathbf{G}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}\}_\ell$ has bounded formal characters. The construction of $\mathbf{C}_\mathbb{Q}$ uses the abelian theory of ℓ-adic representations [Ser98] and the Tate conjecture for abelian varieties (proved by Faltings [Fal83]), which relates the endomorphism ring of A to the commutant of the Galois image Γ_ℓ in $\mathrm{End}_N(\mathbb{Q}_\ell)$. Although we do not in general have the luxury of the Tate conjecture for étale cohomology, it is still possible to construct reductive $\bar{\mathbf{G}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ satisfying the above conditions for $\ell \gg 1$ by using Nori's theory, tame inertia tori [Ser86] and Serre's tame inertia conjecture (proved by Caruso [Car08]). The constructions of these algebraic envelopes $\bar{\mathbf{G}}_\ell$ of $\bar{\Gamma}_\ell$ (see Definition 5) are accomplished in § 2. Once these nice envelopes are ready, we can use the techniques in [Hui13, § 3] to prove that the formal character (Definition 3) of the semisimple part $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ is independent of $\ell \gg 1$ (Theorem A). The number of A_n factors of $\bar{\mathbf{S}}_\ell$ for large n is then independent of ℓ for all $\ell \gg 1$ by [Hui13, Theorem 2.19]. Since the group of $\mathbb{F}_\ell$-rational points of $\bar{\mathbf{G}}_\ell$ is commensurate to the Galois image $\bar{\Gamma}_\ell$, one deduces ℓ-independence results for the number of Lie-type composition factors of $\bar{\Gamma}_\ell$ of characteristic ℓ for $\ell \gg 1$ (Corollary B). Section 3 is devoted to the proofs of Theorem A and Corollary B. The following table summarizes the symbols that are frequently used within this paper. Groups inside $\mathrm{GL}_{N,F}$ with $\mathrm{char}\, F > 0$ have their symbols overlined, and this should not be confused with base change to an algebraic closure.

Gal_F	The absolute Galois group of field F
K, L	Number fields
$\bar{v}$	A valuation of $\bar{K}$ that divides the prime ℓ
$I_{\bar{v}}$	The inertia subgroup of Gal_K at valuation $\bar{v}$
U_ℓ, V_ℓ, W_ℓ ($\bar{U}_\ell$, $\bar{V}_\ell$, $\bar{W}_\ell$), …	Vector spaces defined over $\mathbb{F}_\ell$ (over $\bar{\mathbb{F}}_\ell$)
$\bar{\Gamma}_\ell$, $\bar{\gamma}_\ell$, $\bar{\Omega}_\ell$, $\bar{\Omega}_{\bar{v}}$, …	Finite subgroups of $\mathrm{GL}_N(\mathbb{F}_\ell)$
$\mathbf{G}_\ell$, $\mathbf{T}_\ell$, …	Algebraic subgroups of $\mathrm{GL}_{N,\mathbb{Q}_\ell}$
$\bar{\mathbf{G}}_\ell$, $\bar{\mathbf{S}}_\ell$, $\bar{\mathbf{N}}_\ell$, $\bar{\mathbf{I}}_\ell$, $\bar{\mathbf{I}}_{\bar{v}}$, …	Algebraic subgroups of $\mathrm{GL}_{N,\mathbb{F}_\ell}$
Φ_ℓ, Ψ_ℓ, Θ_ℓ, …	Representations over $\mathbb{Q}_\ell$
ϕ_ℓ, ψ_ℓ, μ_ℓ, t_ℓ, $\rho_{\bar{v}}$, $f_{\bar{v}}$, $w_{\bar{v}}$, …	Representations over $\mathbb{F}_\ell$
ρ^{ss}	The semi-simplification of representation ρ
$\rho^\vee$	The dual representation of representation ρ

2. The algebraic envelope $\bar{\mathbf{G}}_\ell$

We define *formal character* and prove some related propositions before stating the main result (Theorem 2.0.5) of this section. Let $\rho : \mathbf{G} \to \mathrm{GL}_{N,F}$ be a faithful representation of a rank-r reductive algebraic group $\mathbf{G}$ defined over a field F. Choose a maximal torus $\mathbf{T}$ of $\mathbf{G}$ and denote the character group of $\mathbf{T}$ by $\mathbb{X}$. Let $\{w_1, w_2, \ldots, w_N\} \subset \mathbb{X}$ be the *multiset* of weights of $\rho|_{\mathbf{T}}$ over $\bar{F}$, and choose an isomorphism $\mathbb{X} \cong \mathbb{Z}^r$. Then the image of $w_1 + w_2 + \cdots + w_N \in \mathbb{Z}[\mathbb{X}] \cong \mathbb{Z}[\mathbb{Z}^r]$ in the quotient set $\mathrm{GL}(\mathbb{X})\backslash\mathbb{Z}[\mathbb{X}] \cong \mathrm{GL}_r(\mathbb{Z})\backslash\mathbb{Z}[\mathbb{Z}^r]$ is independent of the choices of maximal torus $\mathbf{T}$ and isomorphism $\mathbb{X} \cong \mathbb{Z}^r$.

DEFINITION 3. Let ρ be as above. The *formal character* of ρ is defined to be the image of $w_1 + w_2 + \cdots + w_N \in \mathbb{Z}[\mathbb{Z}^r]$ in $\mathrm{GL}_r(\mathbb{Z})\backslash\mathbb{Z}[\mathbb{Z}^r]$.

This definition of formal character is more general than the one in [Hui13, § 2.1]. It allows us to compare the formal characters of two N-dimensional faithful representations $\rho_1 : \mathbf{G}_1 \to \mathrm{GL}_{N,F_1}$ and $\rho_2 : \mathbf{G}_2 \to \mathrm{GL}_{N,F_2}$ over different fields whenever $\mathbf{G}_1$ and $\mathbf{G}_2$ have the same rank. Let $\mathbb{G}_m^N$ be the diagonal subgroup of GL_N. Every character χ of $\mathbb{G}_m^N$ can be expressed uniquely as $x_1^{m_1}x_2^{m_2}\cdots x_N^{m_N}$, a product of powers of *standard characters* $\{x_1, x_2, \ldots, x_N\}$, where x_i maps $(a_1, \ldots, a_N) \in \mathbb{G}_m^N$ to a_i for each i. The following proposition (definition) is particularly useful.

PROPOSITION 2.0.1 (Definition 3′). *Let ρ_1 and ρ_2 be as above. If $\mathbf{T}_1 \subset \mathbf{G}_1$ and $\mathbf{T}_2 \subset \mathbf{G}_2$ are maximal tori, the following statements are equivalent.*

(i) *The representations ρ_1 and ρ_2 have the same formal character.*

(ii) *The tori $\rho_1(\mathbf{T}_1)$ and $\rho_2(\mathbf{T}_2)$ are conjugate (in $\mathrm{GL}_{N,\bar{F}_1}$ and $\mathrm{GL}_{N,\bar{F}_2}$) to some subtori $\mathbf{D}_1$ and $\mathbf{D}_2$, respectively, of the diagonal subgroup $\mathbb{G}_m^N \subset \mathrm{GL}_N$ such that $\mathbf{D}_1$ and $\mathbf{D}_2$ are annihilated by the same set of characters of $\mathbb{G}_m^N$.*

Hence, formal characters of N-dimensional faithful representations are in bijective correspondence with subtori in $\mathbb{G}_m^N$ up to the natural action of the permutation group $\mathrm{Perm}(N)$ of N letters on $\mathbb{G}_m^N$.

Proof. From now on assume that $\mathbf{T}_j = \mathbb{G}^r_{m,\bar{F}_j}$ and $\rho_j(\mathbf{T}_j) \subset \mathbb{G}^N_{m,\bar{F}_j} \subset \mathrm{GL}_{N,\bar{F}_j}$ by base change to the algebraic closure of F_j and diagonalizations for $j = 1, 2$. Suppose that (i) holds; then, by taking an automorphism of the character group of $\mathbf{T}_1$ and a permutation of coordinates of $\mathbb{G}_m^N$, we obtain

$$x_i \circ \rho_1 = x_i \circ \rho_2$$

for all standard characters x_i of $\mathbb{G}_m^N$ if we identify the character groups of $\mathbb{G}^r_{m,\bar{F}_1}$ and $\mathbb{G}^r_{m,\bar{F}_2}$ in a natural way. This implies that the set of characters of $\mathbb{G}_m^N$ that annihilate $\mathbf{D}_j := \rho_j(\mathbf{T}_j)$ for $j = 1, 2$ are equal, which is statement (ii). Now suppose that (ii) holds; it suffices to consider the case where ρ_1 and ρ_2 are standard representations (inclusions), since $\rho : \mathbf{G} \to \mathrm{GL}_{N,F}$ and $\rho(\mathbf{G}) \subset \mathrm{GL}_{N,F}$ always have the same formal character. Statement (ii) implies that there exists an automorphism of $\mathbb{G}_m^N$ such that

$$\mathbf{D}_j = \{(a_1, \ldots, a_N) \in \mathbb{G}_m^N : a_1 = a_2 = \cdots = a_{N-r} = 1\}$$

for $j = 1, 2$, because $\mathbf{D}_1$ and $\mathbf{D}_2$ are connected. Then (i) follows easily.

Let $\rho : \mathbf{T} \to \mathrm{GL}_{N,\bar{F}}$ be a representation of a torus $\mathbf{T}$. Since the set of weights of ρ is obtained by diagonalizing $\rho(\mathbf{T})$ and is independent of diagonalizations, subtori of $\mathbb{G}_m^N$ that are conjugate to $\rho(\mathbf{T})$ differ only by a permutation of N coordinates. Therefore, the map from formal characters

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

of N-dimensional faithful representations to subtori of $\mathbb{G}_m^N$ modulo the action of $\mathrm{Perm}(N)$ is well-defined. Since the equivalence of (i) and (ii) implies injectivity and any subtorus of $\mathbb{G}_m^N$ is the formal character of the standard representation of the subtorus, the map is a bijective correspondence. □

Examples. Denote standard representation and faithful representation by Std and ρ, respectively. Listed below are some pairs of representations that have the same formal character:

(i) $(\mathrm{GL}_{2,\mathbb{Q}_\ell}, \mathrm{Std})$ and $(\mathrm{GL}_{2,\mathbb{F}_\ell}, \mathrm{Std})$;
(ii) $(\mathbf{G}, \rho)$ and $(\mathbf{H}, \rho|_{\mathbf{H}})$ if $\mathbf{H}$ is a reductive subgroup of $\mathbf{G}$ of the same rank;
(iii) $(\mathbf{G}, \rho)$ and $(\mathbf{G}, \rho^\vee)$;
(iv) $(\mathbf{G}, \rho)$ and $(\rho(\mathbf{G}), \mathrm{Std})$.

Definition 4. The formal character of ρ is said to be *bounded by a constant* $C > 0$ if there exists an isomorphism $\mathbb{X} \cong \mathbb{Z}^r$ such that the coefficients of the images of weights $w_1, w_2, \dots, w_N \in \mathbb{X}$ in $\mathbb{Z}^r$ have absolute values bounded by C.

Let N be a fixed integer and $\{\rho_i : \mathbf{G}_i \to \mathrm{GL}_{N_i,F_i}\}_{i\in I}$ a family of faithful representations of reductive groups such that $N_i \leqslant N$ for all $i \in I$. The family is said to have *bounded formal characters* if for all $i \in I$ the formal character of ρ_i is bounded by some constant $C > 0$.

Remark 2.0.2. Let $\{\rho_i\}_{i\in I}$ be a family of representations in Definition 4 having bounded formal characters. Then the number of distinct formal characters arising from the family is finite.

Let $\chi = x_1^{m_1} x_2^{m_2} \cdots x_N^{m_N}$ be a character of $\mathbb{G}_m^N$ expressed as a product of standard characters. We refer to the multiset $\{m_1, \dots, m_N\}$ as the *exponents* of χ and say that *the exponents are bounded by* $C > 0$ if $|m_i| < C$ for all $1 \leqslant i \leqslant N$. The following characterization of Definition 4 is very useful in this paper.

Proposition 2.0.3 (Definition 4′). *Let $\{\rho_i\}_{i\in I}$ be a family of faithful representations of reductive $\mathbf{G}_i$ such that ρ_i is N_i-dimensional and $N_i \leqslant N$ for all $i \in I$. Choose a maximal torus $\mathbf{T}_i$ of $\mathbf{G}_i$ for each $i \in I$. Then the following statements are equivalent.*

(i) *The family has bounded formal characters.*

(ii) *For any $i \in I$ and any subtorus $\mathbf{D}_i$ of the diagonal subgroup $\mathbb{G}_m^{N_i} \subset \mathrm{GL}_{N_i}$ that is conjugate (in $\mathrm{GL}_{N_i,\bar{F}_i}$) to $\rho_i(\mathbf{T}_i)$, one can choose a set R_i of characters of $\mathbb{G}_m^{N_i}$ such that the common kernel of R_i is $\mathbf{D}_i$ and the exponents of characters in R_i are bounded by a constant which is independent of $i \in I$.*

Proof. This follows easily from Definition 4, the bijective correspondence in Proposition 2.0.1, and Remark 2.0.2. □

Proposition 2.0.4. *Let $\{\rho_i\}_{i\in I}$ and $\{\phi_i\}_{i\in I}$ be two families of faithful representations of reductive $\mathbf{G}_i$ and $\mathbf{H}_i$ over field F_i with bounded formal characters such that the targets of ρ_i and ϕ_i are both equal to GL_{N_i,F_i} and $\rho_i(\mathbf{G}_i)$ commutes with $\phi_i(\mathbf{H}_i)$ for all $i \in I$. Then the family of standard representations*

$$\{\rho_i(\mathbf{G}_i) \cdot \phi_i(\mathbf{H}_i) \subset \mathrm{GL}_{N_i,F_i}\}_{i\in I}$$

also has bounded formal characters.

Proof. This follows easily from Remark 2.0.2, Proposition 2.0.3, and the fact (by the commutativity hypothesis) that any maximal torus of $\rho_i(\mathbf{G}_i) \cdot \phi_i(\mathbf{H}_i)$ is generated by some maximal torus of $\rho_i(\mathbf{G}_i)$ and some maximal torus of $\phi_i(\mathbf{H}_i)$. □

Let $\{\phi_\ell\}$ be the strictly compatible system of mod ℓ Galois representations arising from (Definitions 1 and 2) the dual system of ℓ-adic representations $\{\Phi_\ell\}$. Denote the image of ϕ_ℓ by $\bar{\Gamma}_\ell$ and the ambient space of the representation by $V_\ell \cong \mathbb{F}_\ell^N$ for each ℓ. Each $\bar{\Gamma}_\ell := \phi_\ell(\mathrm{Gal}_K)$ is a subgroup of $\mathrm{GL}_N(\mathbb{F}_\ell)$ for a fixed N. Suppose that K' is a finite normal extension of K. Since $[\phi_\ell(\mathrm{Gal}_K) : \phi_\ell(\mathrm{Gal}_{K'})] \leqslant [K' : K]$ for all ℓ and the restriction of $\{\phi_\ell\}$ to $\mathrm{Gal}_{K'}$ is semisimple [CR88, Theorem 49.2] and satisfies the compatibility conditions (Definition 2), we are free to replace K by K' in the course of proving the main theorem. The main result of this section states that for $\ell \gg 1$, $\bar{\Gamma}_\ell$ can be approximated by some connected reductive subgroup $\bar{\mathbf{G}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ with bounded formal characters (Definition $4'$).

THEOREM 2.0.5. *Let $\{\phi_\ell\}_{\ell\in\mathscr{P}}$ be a system of* mod ℓ *Galois representations as above. There exist a finite normal extension L of K and a connected $\mathbb{F}_\ell$-reductive subgroup $\bar{\mathbf{G}}_\ell$ of $\mathrm{GL}_{N,\mathbb{F}_\ell}$ for each $\ell \gg 1$ such that:*

(i) *$\bar{\gamma}_\ell := \phi_\ell(\mathrm{Gal}_L)$ is a subgroup of $\bar{\mathbf{G}}_\ell(\mathbb{F}_\ell)$ of uniformly bounded index;*
(ii) *the action of $\bar{\mathbf{G}}_\ell$ on $\bar{V}_\ell := V_\ell \otimes \bar{\mathbb{F}}_\ell$ is semisimple;*
(iii) *the representations $\{\bar{\mathbf{G}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell\gg 1}$ have bounded formal characters in the sense of Definition $4'$.*

DEFINITION 5. A system of connected reductive groups $\{\bar{\mathbf{G}}_\ell\}_{\ell\gg1}$ satisfying the conditions in the above theorem is called a *system of algebraic envelopes* of $\{\bar{\Gamma}_\ell\}_{\ell\gg1}$. We say that $\bar{\mathbf{G}}_\ell$ is the *algebraic envelope* of $\bar{\Gamma}_\ell$ when a system of algebraic envelopes is given.

We first establish in §§ 2.1–2.4 essential ingredients of the proof of Theorem 2.0.5. Then the proof is presented in § 2.5.

2.1 Nori's theory

The material in this subsection is due to Nori [Nor87]. Suppose $\ell > N-1$. Given a subgroup $\bar{\Gamma}$ of $\mathrm{GL}_N(\mathbb{F}_\ell)$, Nori's theory gives us a connected algebraic group $\bar{\mathbf{S}}_\ell$ that captures all the order-ℓ elements of $\bar{\Gamma}$ if ℓ is bigger than a constant that depends only on N.

Let $\bar{\Gamma}[\ell] = \{x \in \bar{\Gamma} : x^\ell = 1\}$. The normal subgroup of $\bar{\Gamma}$ generated by $\bar{\Gamma}[\ell]$ is denoted by $\bar{\Gamma}^+$. Define $\exp(x)$ and $\log(x)$ by

$$\exp(x) = \sum_{i=0}^{\ell-1} \frac{x^i}{i!} \quad \text{and} \quad \log(x) = -\sum_{i=1}^{\ell-1} \frac{(1-x)^i}{i}.$$

Denote by $\bar{\mathbf{S}}$ the (connected) algebraic subgroup of $\mathrm{GL}_{N,\mathbb{F}_\ell}$ defined over $\mathbb{F}_\ell$, generated by the one-parameter subgroups

$$t \mapsto x^t := \exp(t \cdot \log(x))$$

for all $x \in \bar{\Gamma}[\ell]$. Algebraic subgroups with the above property are said to be *exponentially generated*. The theorem we need is stated below.

THEOREM 2.1.1 [Nor87, Theorem B(1), 3.6(v)]. *There is a constant $c_0 = c_0(N)$ such that if $\ell > c_0$ and $\bar{\Gamma}$ is a subgroup of $\mathrm{GL}_N(\mathbb{F}_\ell)$, then:*

(i) *$\bar{\Gamma}^+ = \bar{\mathbf{S}}(\mathbb{F}_\ell)^+$;*
(ii) *$\bar{\mathbf{S}}(\mathbb{F}_\ell)/\bar{\mathbf{S}}(\mathbb{F}_\ell)^+$ is a commutative group of order no greater than 2^{N-1}.*

PROPOSITION 2.1.2. *Let $\bar{\mathbf{S}}_\ell$ be the algebraic group associated to $\bar{\Gamma}_\ell$ by Nori's theory for all $\ell > N-1$. There is a constant $c_1 = c_1(N) > c_0(N)$ which depends only on N such that if $\ell > c_1$, then the following hold:*

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

(i) $\bar{\mathbf{S}}_\ell$ *is a connected, exponentially generated, semisimple* $\mathbb{F}_\ell$*-subgroup of* $\mathrm{GL}_{N,\mathbb{F}_\ell}$;
(ii) $\bar{\mathbf{S}}_\ell$ *acts semi-simply on the ambient space* $\bar{V}_\ell \cong \bar{\mathbb{F}}_\ell^N$;
(iii) $[\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell) : \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell) \cap \bar{\Gamma}_\ell] \leqslant 2^{N-1}$.

Proof. Since $\bar{\Gamma}_\ell$ acts semi-simply on $\bar{V}_\ell$, so does $\bar{\Gamma}_\ell^+$; see [CR88, Theorem 49.2]. Property (ii) then follows from [EHK12, Theorem 24] for some sufficiently large constant $c_1(N)$ ($>c_0(N)$) depending only on N; see also [Ser86]. Since $\ell > c_0(N)$, $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)^+ = \bar{\Gamma}_\ell^+$ (Theorem 2.1.1) also acts semi-simply on $\bar{V}_\ell$. This implies that $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)^+$ cannot have normal ℓ-subgroups. If $\bar{\mathbf{S}}_\ell$ has a non-trivial unipotent radical $\bar{\mathbf{U}}_\ell$, then $\bar{\mathbf{U}}_\ell$ is defined over $\mathbb{F}_\ell$ (see [Spr08, Proposition 14.4.5(v)]) and $\bar{\mathbf{U}}_\ell(\mathbb{F}_\ell)$ is then a non-trivial normal ℓ-group of $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)^+$, which is a contradiction. Therefore $\bar{\mathbf{S}}_\ell$ is reductive; in fact, $\bar{\mathbf{S}}_\ell$ is semisimple since it is generated by unipotent elements $\bar{\Gamma}_\ell^+$. This proves (i). Since $\ell > c_0(N)$, (iii) is proved by Theorem 2.1.1. □

Definition 6. The *semisimple envelope* of $\bar{\Gamma}_\ell$ for all sufficiently large ℓ is defined to be the connected, semisimple $\mathbb{F}_\ell$-algebraic group $\bar{\mathbf{S}}_\ell$ in Proposition 2.1.2.

Remark 2.1.3. If K' is a finite extension of K, then the semisimple envelopes of $\phi_\ell(\mathrm{Gal}_{K'})$ and $\phi_\ell(\mathrm{Gal}_K)$ are identical for $\ell \gg 1$, because the order-ℓ elements of the two finite groups are the same when ℓ is large.

2.2 Characters of the tame inertia group

Let $\rho_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)$ be a continuous representation and $I_{\bar{v}}$ the inertia subgroup of Gal_K at $\bar{v} \in \Sigma_{\bar{K}}$ that divides ℓ. Let $I_{\bar{v}}^{\mathrm{w}}$ be the wild inertia (normal) subgroup of $I_{\bar{v}}$ and $\rho_{\bar{v}}^{\mathrm{ss}}$ the semi-simplification of the restriction of ρ_ℓ to $I_{\bar{v}}$. Since $\rho_\ell^{\mathrm{ss}}(I_{\bar{v}}^{\mathrm{w}})$ is an ℓ-group and is semisimple on $\mathbb{F}_\ell^N$, $\rho_{\bar{v}}^{\mathrm{ss}}(I_{\bar{v}}^{\mathrm{w}}) = \{1\}$ and $\rho_{\bar{v}}^{\mathrm{ss}}$ factors through a representation of the tame inertia group $I_{\bar{v}}^{\mathrm{t}} := I_{\bar{v}}/I_{\bar{v}}^{\mathrm{w}}$ (still denoted by $\rho_{\bar{v}}^{\mathrm{ss}}$):

$$\rho_{\bar{v}}^{\mathrm{ss}} : I_{\bar{v}}^{\mathrm{t}} \to \mathrm{GL}_N(\mathbb{F}_\ell).$$

The tame inertia group $I_{\bar{v}}^{\mathrm{t}}$ is a projective limit of cyclic groups of order prime to ℓ,

$$\theta_{\bar{v}} : I_{\bar{v}}^{\mathrm{t}} \xrightarrow{\cong} \varprojlim_k \mathbb{F}_{\ell^k}^*$$

(see [Ser72, Proposition 2]), where the projective system is given by norm maps of finite fields of characteristic ℓ. The isomorphism is unique up to action of $\mathrm{Gal}_{\mathbb{F}_\ell}$ on the target.

Definition 7. The *fundamental characters* of $I_{\bar{v}}^{\mathrm{t}}$ of level d (see [Ser72, § 1.7]) are defined to be

$$\theta_d^{\ell^j} \quad \text{for } j = 0, 1, \ldots, d-1,$$

where $\theta_d : I_{\bar{v}}^{\mathrm{t}} \xrightarrow{\theta_{\bar{v}}} \varprojlim_k \mathbb{F}_{\ell^k}^* \twoheadrightarrow \mathbb{F}_{\ell^d}^* \hookrightarrow \bar{\mathbb{F}}_\ell^*$.

Any continuous character $\chi : I_{\bar{v}}^{\mathrm{t}} \to \bar{\mathbb{F}}_\ell^*$ of $\rho_{\bar{v}}^{\mathrm{ss}}$ factors through a power of some θ_d. Character theory tells us that $\mathrm{Hom}(\mathbb{F}_{\ell^d}^*, \bar{\mathbb{F}}_\ell^*) \cong \mathrm{Hom}(\mathbb{F}_{\ell^d}^*, \mathbb{C}^*)$ is cyclic, generated by θ_d of order $\ell^d - 1$. Therefore, χ can always be expressed as a product of fundamental characters of level d:

$$\chi = (\theta_d)^{m_0} \cdot (\theta_d^\ell)^{m_1} \cdots (\theta_d^{\ell^{d-1}})^{m_{d-1}}.$$

Definition 8. Let $\chi : I_{\bar{v}}^{\mathrm{t}} \to \bar{\mathbb{F}}_\ell^*$ be a character of $\rho_{\bar{v}}^{\mathrm{ss}}$ and express χ as a product of fundamental characters of level d as above.

(i) The product is said to be *ℓ-restricted* if $0 \leqslant m_i \leqslant \ell - 1$ for all i, with not all m_i equal to $\ell - 1$. It is easy to see that the ℓ-restricted expression of χ is unique.

(ii) The *exponents* of χ are defined to be the multiset of powers $\{m_0, m_1, \ldots, m_{d-1}\}$ in the ℓ-restricted product. Note that the multiset is independent of the action of $\mathrm{Gal}_{\mathbb{F}_\ell}$ on the target.

LEMMA 2.2.1. *Let $V \cong \mathbb{F}_\ell^n$ be a continuous, irreducible subrepresentation of $\rho_{\bar{v}}$. Then the characters of the representation can be written as a product of fundamental characters of level n.*

Proof. For simplicity, assume that $\rho_{\bar{v}}$ is irreducible. The image of $I_{\bar{v}}^{\mathrm{t}}$ in $\mathrm{GL}(V)$ is a cyclic group of order prime to ℓ; therefore V is a $\mathbb{F}_\ell[x]/(f(x))$-module where x corresponds to a generator of the cyclic image and the minimal polynomial $f(x)$ is separable. Irreducibility of V implies that $f(x)$ is irreducible over $\mathbb{F}_\ell$. Thus $\rho_{\bar{v}}(I_{\bar{v}}^{\mathrm{t}})$ is contained in a maximal subfield F of $\mathrm{End}(V)$ and $\rho_{\bar{v}} : I_{\bar{v}}^{\mathrm{t}} \to F^* \subset \mathrm{GL}(V)$ can be written as a product of fundamental characters of level n as above. On the other hand, V has the structure of an F-vector space of dimension 1 such that the action of $\rho_{\bar{v}}(I_{\bar{v}}^{\mathrm{t}}) \subset F^*$ is through field multiplication. By tensoring F with F (on the right) over $\mathbb{F}_\ell$, we obtain an F-isomorphism

$$F \otimes F \to F \oplus F \oplus \cdots \oplus F,$$
$$x \otimes y \mapsto (xy, x^\ell y, \ldots, x^{\ell^{n-1}} y)$$

where $x, x^\ell, \ldots, x^{\ell^{n-1}}$ are just conjugates of x over $\mathbb{F}_\ell$. If $x \in \rho_{\bar{v}}(I_{\bar{v}}^{\mathrm{t}}) \subset F^*$, then we see that the action of $I_{\bar{v}}^{\mathrm{t}}$ on $V \otimes_{\mathbb{F}_\ell} F$ is a direct sum of products of fundamental characters of level n. $\square$

2.3 Exponents of characters arising from étale cohomology

Every character χ of $\rho_{\bar{v}}^{\mathrm{ss}} : I_{\bar{v}}^{\mathrm{t}} \to \mathrm{GL}_N(\mathbb{F}_\ell)$ can be written as

$$\chi = (\theta_n)^{m_0} \cdot (\theta_n^\ell)^{m_1} \cdots (\theta_n^{\ell^{n-1}})^{m_{n-1}},$$

a product of fundamental characters of level $n \leqslant N$, by Lemma 2.2.1. One would like to study the exponents $m_0, \ldots, m_{n-1}$ (Definition 8), and in the case of étale cohomology we have the following theorem proved by Caruso [Car08].

THEOREM 2.3.1 (Serre's tame inertia conjecture). *Let X be a proper and smooth variety over a local field K (a finite extension of $\mathbb{Q}_\ell$) with semi-stable reduction over $\mathscr{O}_K$, the ring of integers of K, and let i be an integer. The Galois group Gal_K acts on $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/\ell\mathbb{Z})^\vee$, the $\mathbb{F}_\ell$-dual of the ith cohomology group with $\mathbb{Z}/\ell\mathbb{Z}$ coefficients. If we restrict the representation to the inertia group of Gal_K, then the exponents of the characters of the tame inertia group on any Jordan–Hölder quotient of $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/\ell\mathbb{Z})^\vee$ lie between 0 and ei, where e is the ramification index of $K/\mathbb{Q}_\ell$.*

We now relate our mod ℓ Galois representation ϕ_ℓ to the representation $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/\ell\mathbb{Z})^\vee$ in Theorem 2.3.1. The cohomology group $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell)$ is a finitely generated, free $\mathbb{Z}_\ell$-module [Gab83] for $\ell \gg 1$:

$$H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell) \cong \mathbb{Z}_\ell \oplus \cdots \oplus \mathbb{Z}_\ell.$$

Reduction mod ℓ gives

$$H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell) \otimes \mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell\mathbb{Z},$$

and the semi-simplification of $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell) \otimes \mathbb{F}_\ell$ is then isomorphic to the semi-simplification of a mod ℓ reduction of the ℓ-adic representation $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)$ by Brauer–Nesbitt [CR88, Theorem 30.16]. Since the sequence

$$H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell) \xrightarrow{\ell} H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell) \to H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/\ell\mathbb{Z})$$

is exact [Mil13, Theorem 19.2], $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell) \otimes \mathbb{F}_\ell$ is isomorphic to $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/\ell\mathbb{Z})$. Recall that V_ℓ is the semi-simplification of a mod ℓ reduction of $H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_\ell)^\vee$. Thus, we conclude the following.

Proposition 2.3.2. *For all sufficiently large ℓ, $H^i_{\text{ét}}(X_{\bar{K}},\mathbb{Z}_\ell)\otimes\mathbb{F}_\ell$ is isomorphic to $H^i_{\text{ét}}(X_{\bar{K}},\mathbb{Z}/\ell\mathbb{Z})$ and the semi-simplification of $H^i_{\text{ét}}(X_{\bar{K}},\mathbb{Z}/\ell\mathbb{Z})$ is $V_\ell^\vee$.*

The following theorem is the main result of this subsection.

Theorem 2.3.3. *Let K be a number field. Let $\phi_\ell:\mathrm{Gal}_K\to\mathrm{GL}(V_\ell)\cong\mathrm{GL}_N(\mathbb{F}_\ell)$ be the* mod ℓ *Galois representation arising from the étale cohomology group $H^i_{\text{ét}}(X_{\bar{K}},\mathbb{Q}_\ell)^\vee$ for sufficiently large ℓ. If we restrict ϕ_ℓ to the inertia group $I_{\bar{v}}$ of a valuation $\bar{v}\,|\,\ell$ of $\bar{K}$ and semi-simplify the representation, then every character χ of the representation can be written as*

$$\chi=(\theta_{N!})^{m_0}\cdot(\theta_{N!}^{\ell})^{m_1}\cdots(\theta_{N!}^{\ell^{N!-1}})^{m_{N!-1}},$$

a product of fundamental characters of level $N!$ with exponents (Definition 8) $m_0,\dots,m_{N!-1}$ (depending on ℓ) that lie in $[0,ei]$, where e is the ramification index of $K_v/\mathbb{Q}_\ell$, with $v=\bar{v}|_K$ and K_v being the completion of K with respect to v.

Proof. Proposition 2.3.2 implies that if ℓ is sufficiently large, then the Galois representations $V_\ell=(V_\ell^\vee)^\vee$ and $(H^i_{\text{ét}}(X_{\bar{K}},\mathbb{Z}/\ell\mathbb{Z})^\vee)^{\mathrm{ss}}$ are isomorphic. Let χ be a character of $I^{\mathrm{t}}_{\bar{v}}$ given by the semi-simplification of the restriction of V_ℓ to the inertia subgroup $I_{\bar{v}}$. By Theorem 2.3.1, χ can be written as

$$\chi=(\theta_d)^{m_0}\cdot(\theta_d^{\ell})^{m_1}\cdots(\theta_d^{\ell^{d-1}})^{m_{d-1}},$$

a product of fundamental characters of level d ($\leqslant N$ by Lemma 2.2.1) with exponents $m_0,\dots,$ m_{d-1} belonging to $[0,ei]$, where e is the ramification index of $K_v/\mathbb{Q}_\ell$. Since d divides $N!$, $\theta_{N!}$ factors through χ. Consider the norm map $\mathrm{Nm}:\mathbb{F}^*_{\ell^{N!}}\to\mathbb{F}^*_{\ell^d}$ given by

$$x\mapsto x\cdot x^{\ell^d}\cdot x^{\ell^{2d}}\cdots x^{\ell^{(N!-d)}}.$$

Then we obtain a product of fundamental characters of level $N!$,

$$\begin{aligned}\chi&=(\mathrm{Nm}\circ\theta_{N!})^{m_0+m_1\ell+\cdots+m_{d-1}\ell^{d-1}}\\&=(\theta_{N!})^{s_0}\cdot(\theta_{N!}^{\ell})^{s_1}\cdots(\theta_{N!}^{\ell^{N!-1}})^{s_{N!-1}},\end{aligned}$$

with exponents $s_0,\dots,s_{N!-1}$ belonging to $[0,ei]$. □

2.4 Tame inertia tori and rigidity

Tame inertia tori were considered by Serre when he was studying Galois action on ℓ-torsion points of abelian varieties without complex multiplication [Ser86]. He observed that these tori have a certain rigidity, which will be explained in this subsection.

Assume $\ell>N-1$ as in § 2.1. Since every non-trivial element of every ℓ-Sylow subgroup of $\bar{\Gamma}_\ell$ is of order ℓ and $\bar{\Gamma}_\ell^+$ is contained in $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ by Theorem 2.1.1(i), the index $[\bar{\Gamma}_\ell:\bar{\Gamma}_\ell\cap\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)]$ is prime to ℓ. Let $\bar{\mathbf{N}}_\ell$ be the normalizer of $\bar{\mathbf{S}}_\ell$ in $\mathrm{GL}_{N,\mathbb{F}_\ell}$; clearly $\bar{\Gamma}_\ell\subset\bar{\mathbf{N}}_\ell$.

Theorem 2.4.1 [Ser86, § 1, Theorem]. *There are constants $c_2=c_2(N)$ and $c_3=c_3(N)$ such that if $\ell>c_2$, $\bar{\mathbf{S}}_\ell\subset\mathrm{GL}_{N,\mathbb{F}_\ell}$ is an exponentially generated semisimple algebraic group defined over $\mathbb{F}_\ell$, and the action on $\bar{V}_\ell\cong\bar{\mathbb{F}}_\ell^N$ is semisimple. If W_ℓ is the $\mathbb{F}_\ell$-subspace of*

$$U_\ell:=\bigoplus_{i=1}^{c_3}(\otimes^i V_\ell)$$

fixed by $\bar{\mathbf{S}}_\ell$, then $t_\ell:\bar{\mathbf{N}}_\ell/\bar{\mathbf{S}}_\ell\to\mathrm{GL}_{W_\ell}$ is an $\mathbb{F}_\ell$-embedding. Moreover, if $x\notin\bar{\mathbf{S}}_\ell$, then there is an element of $\bar{W}_\ell$ that is not fixed by x.

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

By Theorem 2.4.1, $\bar{\Gamma}_\ell/(\bar{\Gamma}_\ell \cap \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell))$ embeds in $\mathrm{GL}(W_\ell)$ with $\dim(W_\ell) \leqslant c_4 = c_4(N)$ uniformly for some integer c_4. Theorem 2.4.2 below is the main result of this subsection.

DEFINITION 9. For each ℓ, define $\mu_\ell : \mathrm{Gal}_K \to \mathrm{GL}(W_\ell)$ to be the composition $t_\ell \circ \phi_\ell$ and $\bar{\Omega}_\ell$ to be the image μ_ℓ, where t_ℓ is as in Theorem 2.4.1.

THEOREM 2.4.2. *Let $\bar{\mathbf{I}}_\ell$ be the algebraic group generated by a set of tame inertia tori $\bar{\mathbf{I}}_{\bar{v}}$ (Definition 10) for $\ell \gg 1$. There exist a constant $c_8 = c_8(N)$ and a finite normal field extension L/K such that if $\ell \gg 1$, then $\bar{\mathbf{I}}_\ell$ is a torus, called the inertia torus at ℓ, and $\mu_\ell(\mathrm{Gal}_L) \subset \bar{\Omega}_\ell$ is a subgroup of $\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell)$ such that:*

(i) $\{\bar{\mathbf{I}}_\ell \hookrightarrow \mathrm{GL}_{W_\ell}\}_{\ell \gg 1}$ *have bounded formal characters (Definition 4′);*
(ii) $[\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : \mu_\ell(\mathrm{Gal}_L)]$ *is bounded by c_8.*

THEOREM 2.4.3 [Jor78, Jordan's theorem on finite linear groups]. *For every n there exists a constant $J(n)$ such that any finite subgroup of GL_n over a field of characteristic zero possesses an abelian normal subgroup of index less than or equal to $J(n)$.*

The order of $\bar{\Omega}_\ell$ is prime to ℓ; thus $\bar{\Omega}_\ell$ can be lifted to a subgroup of $\mathrm{GL}_{N'}(\mathbb{C})$ such that N' depends only on N. Theorem 2.4.3 then tells us that $\bar{\Omega}_\ell$ has a abelian normal subgroup $\bar{J}_\ell$ of index less than a constant $c_5 = c_5(N) := J(N')$ depending on N'. Since N' depends on N, we have $[\bar{\Omega}_\ell : \bar{J}_\ell] \leqslant c_5$. If $\bar{v}$ divides ℓ, then the action of the inertia group $I_{\bar{v}}$ on W_ℓ is semisimple because $|\bar{\Omega}_\ell|$ is prime to ℓ. Since $\dim(W_\ell) \mid c_4!$, we obtain

$$\mu_\ell : I_{\bar{v}}^{\mathrm{t}} \overset{\theta_{c_4!}}{\twoheadrightarrow} \mathbb{F}_{\ell^{c_4!}}^* \to \mathrm{GL}(W_\ell).$$

By Theorem 2.3.3 and W_ℓ in Theorem 2.4.1, there exists $c_6 = c_6(N) \geqslant 0$ such that if χ is a character, then χ can be written as a product of fundamental characters of level $c_4!$,

$$\chi = (\theta_{c_4!})^{m_0} \cdot (\theta_{c_4!}^{\ell})^{m_1} \cdots (\theta_{c_4!}^{\ell^{c_4!-1}})^{m_{c_4!-1}},$$

with exponents $m_0, \ldots, m_{c_4!-1}$ belonging to $[0, c_6]$ for all $\ell \gg 1$. Therefore, we make the following definition.

DEFINITION 10. Denote the field $\mathbb{F}_{\ell^{c_4!}}$ by $\mathbb{E}_\ell$ for all ℓ. This gives a homomorphism

$$f_{\bar{v}} : \mathbb{E}_\ell^* \to \mathrm{GL}(W_\ell)$$

if $\ell > c_6(N) + 1$. Let $\bar{\mathbf{E}}_\ell$ denote $\mathrm{Res}_{\mathbb{E}_\ell/\mathbb{F}_\ell}(\mathbb{G}_m)$ (the Weil restriction of scalars) for all ℓ. We have $\bar{\mathbf{E}}_\ell(\mathbb{F}_\ell) = \mathbb{E}_\ell^*$. Then $f_{\bar{v}}$ extends uniquely [Hal11, § 3] to the following ℓ-restricted $\mathbb{F}_\ell$-morphism:

$$w_{\bar{v}} : \bar{\mathbf{E}}_\ell := \mathrm{Res}_{\mathbb{E}_\ell/\mathbb{F}_\ell}(\mathbb{G}_m) \to \mathrm{GL}_{W_\ell}.$$

Denote the image of $w_{\bar{v}}$ by $\bar{\mathbf{I}}_{\bar{v}}$ for $\bar{v} \mid \ell \gg 1$. It is called the *tame inertia torus at $\bar{v} \in \Sigma_{\bar{K}}$*.

LEMMA 2.4.4. *There exists a constant $c_7 = c_7(N)$ such that for any $\bar{v} \mid \ell > c_6(N) + 1$:*

(i) $\{\bar{\mathbf{I}}_{\bar{v}} \hookrightarrow \mathrm{GL}_{W_\ell}\}_{\bar{v}}$ *have bounded formal characters (Definition 4′);*
(ii) $[\bar{\mathbf{I}}_{\bar{v}}(\mathbb{F}_\ell) : f_{\bar{v}}(\mathbb{E}_\ell^*)] \leqslant c_7$.

Proof. Since $\dim(W_\ell)$ and $\dim(\bar{\mathbf{E}}_\ell)$ are bounded by a constant independent of ℓ and the exponents of the characters of $w_{\bar{v}}$ in terms of the fundamental characters [Hal11, § 3] belong to $[0, c_6]$, by Proposition 2.0.3 we find a set of characters $R_{\bar{v}}$ of uniformly bounded exponents of the diagonal subgroup of GL_{W_ℓ}, by diagonalizing $\bar{\mathbf{I}}_{\bar{v}}$; then assertion (i) follows. For assertion (ii), uniform boundedness of exponents of characters and the fact that $\dim(\bar{\mathbf{E}}_\ell) = c_4!$ (for all ℓ) imply that the number of connected components of $\mathrm{Ker}(w_{\bar{v}})$ is uniformly bounded by c_7. On the other hand, the number of $\mathbb{F}_\ell$-rational points of any $\mathbb{F}_\ell$-torus of dimension k lies between $(\ell-1)^k$ and $(\ell+1)^k$ by [Nor87, Lemma 3.5]. Therefore $\mu_\ell(I_{\bar{v}}^{\mathrm{t}}) = f_{\bar{v}}(\mathbb{E}_\ell^*)$ has at least

$$\frac{|\mathbb{E}_\ell^*|}{c_7(\ell+1)^{\dim(\mathrm{Ker}(w_{\bar{v}}))}} = \frac{\ell^{c_4!}-1}{c_7(\ell+1)^{\dim(\mathrm{Ker}(w_{\bar{v}}))}}$$

points, and $[\bar{\mathbf{I}}_{\bar{v}}(\mathbb{F}_\ell) : \mu_\ell(I_{\bar{v}}^{\mathrm{t}})]$ is bounded by

$$\frac{c_7(\ell+1)^{\dim(\mathrm{Ker}(w_{\bar{v}}))+\dim(\mathrm{Im}(w_{\bar{v}}))}}{\ell^{c_4!}-1} = \frac{c_7(\ell+1)^{c_4!}}{\ell^{c_4!}-1} \to c_7$$

when ℓ is large. This proves (ii). □

Lemma 2.4.5 (Rigidity; [Hal11, § 3], [Ser86, § 3]). *Let $s \in \mathrm{GL}(W_\ell)$ be a semisimple element and $f_{\bar{v}} : \mathbb{E}_\ell^* \to \mathrm{GL}(W_\ell)$ a representation such that the exponents of characters of $f_{\bar{v}}$ belong to $[0,c]$ for some $c > 0$. If $H \subset \mathbb{E}_\ell^*$ is a subgroup such that $f_{\bar{v}}(H)$ commutes with s in $\mathrm{GL}(W_\ell)$ and $c \cdot [\mathbb{E}_\ell^* : H] \leqslant \ell - 1$, then $\bar{\mathbf{I}}_{\bar{v}}$ commutes with s, and hence so does $f_{\bar{v}}(\mathbb{E}_\ell^*)$.*

Recall from Definition 2 that there is a finite subset $S \subset \Sigma_K$ such that ϕ_ℓ is unramified outside $S_\ell := S \cup \{v \in \Sigma_K : v \mid \ell\}$ for all ℓ.

Proof of Theorem 2.4.2. The following arguments are influenced by the arguments Serre gave for [Ser86, Theorem 1].

Denote the image of $\mu_\ell(I_{\bar{v}}^{\mathrm{t}})$ under the map $\bar{\Gamma}_\ell/(\bar{\Gamma}_\ell \cap \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)) \hookrightarrow \mathrm{GL}(W_\ell)$ by $\bar{\Omega}_{\bar{v}}$ whenever $\bar{v} \mid \ell$. Let $\bar{J}_\ell$ be a maximal abelian normal subgroup of $\bar{\Omega}_\ell := \mu_\ell(\mathrm{Gal}_K)$. We first prove that $\bar{\Omega}_{\bar{v}}$ commutes with $\bar{J}_\ell$ if ℓ is large. Since $\bar{\Omega}_{\bar{v}}$ and $\bar{J}_\ell$ are abelian and

$$[\bar{\Omega}_{\bar{v}} : \bar{\Omega}_{\bar{v}} \cap \bar{J}_\ell] \leqslant c_5$$

by Theorem 2.4.3 (Jordan), the tame inertia torus $\bar{\mathbf{I}}_{\bar{v}}$ at $\bar{v}$ (Definition 10) and hence $f_{\bar{v}}(\mathbb{E}_\ell^*) = \bar{\Omega}_{\bar{v}}$ commute with $\bar{J}_\ell$ if $\ell > c_5c_6 + 1$ by rigidity (Lemma 2.4.5). For any $\bar{v}_1, \bar{v}_2 \mid \ell$, since $\bar{\Omega}_{\bar{v}_1} \cap \bar{J}_\ell$ commutes with $\bar{\Omega}_{\bar{v}_2} \cap \bar{J}_\ell$ and these are of bounded index in $\bar{\Omega}_{\bar{v}_1}$ and $\bar{\Omega}_{\bar{v}_2}$, respectively, we obtain that $\bar{\mathbf{I}}_{\bar{v}_1}$ commutes with $\bar{\mathbf{I}}_{\bar{v}_2}$ if $\ell \gg 1$ by rigidity (Lemma 2.4.5). The subgroup $\bar{H}_\ell$ of $\bar{\Omega}_\ell$ generated by the inertia subgroups $\bar{\Omega}_{\bar{v}}$ for all $\bar{v} \mid \ell$ is abelian and normal for $\ell \gg 1$. As $\bar{J}_\ell$ is maximal normal abelian in $\bar{\Omega}_\ell$, we have that $\bar{H}_\ell \subset \bar{J}_\ell$ for all $\ell \gg 1$. Therefore each $\bar{\Omega}_\ell/\bar{J}_\ell$ corresponds to a field extension of K of degree bounded by c_5 that ramifies only in S (Definition 2) for $\ell \gg 1$. By Hermite's theorem [Lan94, p. 122], the composite of these fields is still a finite field extension K' of K. Therefore $\mu_\ell(\mathrm{Gal}_{K'}) \subset \bar{J}_\ell$ for $\ell \gg 1$.

Since the representations $\{\phi_\ell\}$ come from étale cohomology and $I_{\bar{v}} \cap \mathrm{Gal}_{K'}$ is the inertia subgroup of $\mathrm{Gal}_{K'}$ at $\bar{v}$ (see [Neu99, Proposition 9.5]), they are potentially semi-stable, which means that there exists a finite extension K'' of K' such that $\phi_\ell(I_{\bar{v}} \cap \mathrm{Gal}_{K''})$ is unipotent for any $\bar{v}$ not dividing ℓ (see [dJon96, § 1]). Therefore, for each $\ell \gg 1$, we have a finite abelian extension of K'' with Galois group $\mu_\ell(\mathrm{Gal}_{K''})$ contained in $\bar{J}_\ell$ that ramifies only at $v \in \Sigma_{K''}$ dividing ℓ. Since $\mu_\ell(\mathrm{Gal}_{K''})$ is an abelian Galois group over K'', each ramified prime $v \in \Sigma_{K''}$ dividing large ℓ corresponds to an inertia subgroup $\bar{I}_v'' \subset \mu_\ell(\mathrm{Gal}_{K''})$, and there are at most $[K'' : \mathbb{Q}]$ of them. For each inertia subgroup $\bar{I}_v''$, choose a tame inertia torus $\bar{\mathbf{I}}_{\bar{v}}$ such that $\bar{I}_v'' \subset \bar{\mathbf{I}}_{\bar{v}}(\mathbb{F}_\ell)$. Since these tame inertia tori commute with each other, the algebraic group $\bar{\mathbf{I}}_\ell$ generated by them is an $\mathbb{F}_\ell$-torus, called the *inertia torus at* ℓ. Since $\{\bar{\mathbf{I}}_{\bar{v}} \to \mathrm{GL}_{W_\ell}\}_{\bar{v}|\ell\gg1}$ have bounded formal characters (Lemma 2.4.4(i)) and each $\bar{\mathbf{I}}_\ell$ is generated by at most $[K'' : \mathbb{Q}]$ tame inertia tori, $\{\bar{\mathbf{I}}_\ell \hookrightarrow \mathrm{GL}_{W_\ell}\}_{\ell\gg1}$ have bounded formal characters by Proposition 2.0.4. This proves (i).

Let $\bar{I}''_\ell$ be the subgroup of $\mu_\ell(\mathrm{Gal}_{K''})$ generated by $\bar{I}''_v$ for all $v \,|\, \ell$. Then, for $\ell \gg 1$,

$$\mu_\ell(\mathrm{Gal}_{K''})/\bar{I}''_\ell$$

is the Galois group of a finite abelian extension of K'' that is unramified at every non-Archimedean valuation. By abelian class field theory, these fields generate a finite extension K''' of K''. Choose L normal over K such that $K''' \subset L$. Then we obtain

$$(*): \quad \mu_\ell(\mathrm{Gal}_L) \subset \bar{I}''_\ell \subset \bar{\mathbf{I}}_\ell(\mathbb{F}_\ell).$$

It remains to prove (ii). Suppose that $\bar{\mathbf{I}}_\ell$ is generated by tame inertia tori $\bar{\mathbf{I}}_{\bar{v}_i}$, $1 \leqslant i \leqslant k$, for some fixed $k \leqslant [K'' : \mathbb{Q}]$. We have

$$\begin{aligned}[\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : \mu_\ell(\mathrm{Gal}_L)] &= [\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : \bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) \cap \bar{\Omega}_\ell] \cdot [\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) \cap \bar{\Omega}_\ell : \mu_\ell(\mathrm{Gal}_L)] \\ &\leqslant [\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : f_{\bar{v}_1}(\mathbb{E}_\ell^*) \cdots f_{\bar{v}_k}(\mathbb{E}_\ell^*)] \cdot [L : K].\end{aligned}$$

It suffices to show that $[\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : f_{\bar{v}_1}(\mathbb{E}_\ell^*) \cdots f_{\bar{v}_k}(\mathbb{E}_\ell^*)]$ is bounded independently of ℓ. The proof is identical to that of Lemma 2.4.4(ii), since $f_{\bar{v}_1}(\mathbb{E}_\ell^*) \cdots f_{\bar{v}_k}(\mathbb{E}_\ell^*)$ is the image of

$$f_{\bar{v}_1} \times \cdots \times f_{\bar{v}_k} : (\mathbb{E}_\ell^*)^k \to \mathrm{GL}(W_\ell),$$

$\bar{\mathbf{I}}_\ell$ is the image of

$$w_{\bar{v}_1} \times \cdots \times w_{\bar{v}_k} : (\bar{\mathbf{E}}_\ell)^k \to \mathrm{GL}_{W_\ell},$$

k (depending on ℓ) is always less than $[K'' : \mathbb{Q}]$, and the exponents of characters (ℓ-restricted, Definition 10) of $w_{\bar{v}_1} \times \cdots \times w_{\bar{v}_k}$ are uniformly bounded. Hence, there exists $c_8 = c_8(N)$ such that $[\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : \mu_\ell(\mathrm{Gal}_L)] \leqslant c_8$ for $\ell \gg 1$. $\square$

2.5 Construction of $\bar{\mathbf{G}}_\ell$

An $\mathbb{F}_\ell$-torus $\bar{\mathbf{I}}_\ell \subset \mathrm{GL}_{W_\ell}$ was constructed in § 2.4 for $\ell \gg 1$, and we have the following map defined in Theorem 2.4.1:

$$t_\ell : \bar{\mathbf{N}}_\ell \twoheadrightarrow \bar{\mathbf{N}}_\ell/\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{W_\ell}.$$

One has to show that $\bar{\mathbf{I}}_\ell \subset t_\ell(\bar{\mathbf{N}}_\ell)$ so that $t_\ell^{-1}(\bar{\mathbf{I}}_\ell)$ is connected. It suffices to consider tame inertia tori $\bar{\mathbf{I}}_{\bar{v}}$. Recall the vector space U_ℓ from Theorem 2.4.1.

LEMMA 2.5.1. *Let $\bar{\mathbf{H}}_\ell$ be an algebraic subgroup of $\mathrm{GL}_{\bar{V}_\ell}$. Then $\bar{\mathbf{H}}_\ell$ acts on $\bar{U}_\ell$. If $\bar{\mathbf{H}}_\ell$ is invariant on the subspace*

$$\bar{W}_\ell \subset \bar{U}_\ell$$

fixed by $\bar{\mathbf{S}}_\ell$, then $\bar{\mathbf{H}}_\ell$ is contained in $\bar{\mathbf{N}}_\ell$.

Proof. Let $x \in \bar{\mathbf{H}}_\ell \backslash \bar{\mathbf{N}}_\ell$. Then there exists $s \in \bar{\mathbf{S}}_\ell$ such that $xsx^{-1} \notin \bar{\mathbf{S}}_\ell$. There exists $w \in \bar{W}_\ell$ such that

$$xsx^{-1}w \neq w$$

by the last statement of Theorem 2.4.1. Therefore,

$$sx^{-1}w \neq x^{-1}w$$

implies $x^{-1}w \notin \bar{W}_\ell$, which is a contradiction. Hence $\bar{\mathbf{H}}_\ell$ is contained in $\bar{\mathbf{N}}_\ell$. $\square$

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

Proposition 2.5.2. *The $\mathbb{F}_\ell$-torus $\bar{\mathbf{I}}_\ell$ in GL_{W_ℓ} is a subgroup of the image of*

$$t_\ell : \bar{\mathbf{N}}_\ell \twoheadrightarrow \bar{\mathbf{N}}_\ell/\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{W_\ell}$$

defined in Theorem 2.4.1.

Proof. Let $\bar{v} \mid \ell$ be a valuation of $\bar{K}$ and let $I_{\bar{v}}$ be the inertia subgroup of Gal_K at $\bar{v}$. The restriction $\phi_\ell : I_{\bar{v}} \to \mathrm{GL}(V_\ell)$ factors through a finite quotient $\pi_{\bar{v}} : I_{\bar{v}} \twoheadrightarrow J_{\bar{v}}$ such that $|J_{\bar{v}}| = \ell^k \cdot (\ell^{c_4!} - 1)$. Recall the vector spaces $W_\ell \subset U_\ell$ from Theorem 2.4.1 and $f_{\bar{v}} : \mathbb{E}_\ell^* \to \mathrm{GL}(W_\ell)$ from Definition 10. Consider the diagram below such that

$$r_\ell \circ \phi_\ell \circ i_{\bar{v}} = f'_{\bar{v}}$$

and the actions of $\mathbb{E}_\ell^*$ on W_ℓ via $f'_{\bar{v}}$ and $f_{\bar{v}}$ are the same.

$$\begin{tikzcd} J_{\bar{v}} \arrow[r, two heads, "\pi_{\bar{v}}"'] \arrow[d, "\phi_\ell"'] & \mathbb{E}_\ell^* \arrow[l, bend right, "i_{\bar{v}}"'] \arrow[d, "f'_{\bar{v}}"] \\ \mathrm{GL}_{V_\ell} \arrow[r, "r_\ell"] & \mathrm{GL}_{U_\ell} \end{tikzcd}$$

Here r_ℓ is the obvious map and $i_{\bar{v}}$ is a splitting of $\pi_{\bar{v}}$. This is possible because $\mathbb{E}_\ell^*$ defined in § 2.4 is cyclic of order $\ell^{c_4!} - 1$ prime to ℓ.

If ℓ is sufficiently large, then the exponents of the (ℓ-restricted) characters of representations $\phi_\ell \circ i_{\bar{v}}$ and $r_\ell \circ \phi_\ell \circ i_{\bar{v}}$ belong to $[0, i]$ and $[0, ic_3]$, respectively, by Theorem 2.3.3 and the construction of U_ℓ. Recall $\bar{\mathbf{E}}_\ell$ from Definition 10. By the Weil restriction of scalars, we obtain two $\mathbb{F}_\ell$-morphisms

$$\alpha_\ell : \bar{\mathbf{E}}_\ell \to \mathrm{GL}_{V_\ell},$$
$$\beta_\ell : \bar{\mathbf{E}}_\ell \to \mathrm{GL}_{U_\ell}.$$

Since $r_\ell \circ \alpha_\ell$ and β_ℓ are both ℓ-restricted [Hal11, § 3] and equal to $r_\ell \circ \phi_\ell \circ i_{\bar{v}}$ upon restricting to $\mathbb{E}_\ell^*$, by uniqueness [Hal11, § 3] we have that

$$r_\ell \circ \alpha_\ell = \beta_\ell.$$

The image $r_\ell \circ \phi_\ell \circ i_{\bar{v}}(\mathbb{E}_\ell^*) = f'_{\bar{v}}(\mathbb{E}_\ell^*)$ maps W_ℓ and hence $\bar{W}_\ell$ to itself, so $\beta_\ell(\bar{\mathbf{E}}_\ell)$ also maps $\bar{W}_\ell$ to itself. Since $r_\ell \circ \alpha_\ell(\bar{\mathbf{E}}_\ell) = \beta_\ell(\bar{\mathbf{E}}_\ell)$, we conclude that $\alpha_\ell(\bar{\mathbf{E}}_\ell) \subset \bar{\mathbf{N}}_\ell$ by Lemma 2.5.1. One also observes that the morphism

$$t_\ell : \bar{\mathbf{N}}_\ell \twoheadrightarrow \bar{\mathbf{N}}_\ell/\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{W_\ell}$$

maps $\alpha_\ell(\bar{\mathbf{E}}_\ell)$ to $\bar{\mathbf{I}}_{\bar{v}} := w_{\bar{v}}(\bar{\mathbf{E}}_\ell)$. Therefore, the tame inertia torus $\bar{\mathbf{I}}_{\bar{v}}$, and thus $\bar{\mathbf{I}}_\ell$, is a subgroup of $t_\ell(\bar{\mathbf{N}}_\ell)$. □

Definition 11. Let L be the normal extension of K in Theorem 2.4.2. Denote $\phi_\ell(\mathrm{Gal}_L)$ by $\bar{\gamma}_\ell$ for all ℓ. Then $[\bar{\Gamma}_\ell : \bar{\gamma}_\ell] \leqslant [L : K]$ for all ℓ.

Proof of Theorem 2.0.5 (i) and (ii). Since $\bar{\mathbf{S}}_\ell$ is a connected normal subgroup of $\bar{\mathbf{N}}_\ell$, $\bar{\mathbf{I}}_\ell$ is a torus and t_ℓ is an $\mathbb{F}_\ell$-morphism, Proposition 2.5.2 implies that $t_\ell^{-1}(\bar{\mathbf{I}}_\ell)$, the preimage of the $\mathbb{F}_\ell$-torus $\bar{\mathbf{I}}_\ell$, is a connected $\mathbb{F}_\ell$-reductive group $\bar{\mathbf{G}}_\ell$. Moreover, $\bar{\gamma}_\ell \subset \bar{\mathbf{G}}_\ell(\mathbb{F}_\ell)$ by construction of $\bar{\mathbf{G}}_\ell$ for $\ell \gg 1$. We obtain an exact sequence of $\mathbb{F}_\ell$ algebraic groups for $\ell \gg 1$,

$$1 \to \bar{\mathbf{S}}_\ell \to \bar{\mathbf{G}}_\ell \to \bar{\mathbf{I}}_\ell \to 1,$$

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

and hence

$$1 \to \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell) \to \bar{\mathbf{G}}_\ell(\mathbb{F}_\ell) \to \bar{\mathbf{I}}_\ell(\mathbb{F}_\ell).$$

Recall that $\mu_\ell(\mathrm{Gal}_L) = t_\ell(\bar{\gamma}_\ell)$ from Theorem 2.4.2. Since the semisimple envelopes (Definition 6) of $\bar{\Gamma}_\ell$ and $\bar{\gamma}_\ell$ are identical for $\ell \gg 1$ by Remark 2.1.3, the above exact sequence implies that

$$[\bar{\mathbf{G}}_\ell(\mathbb{F}_\ell) : \bar{\gamma}_\ell] \leqslant [\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell) : \bar{\gamma}_\ell \cap \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)][\bar{\mathbf{I}}_\ell(\mathbb{F}_\ell) : \mu_\ell(\mathrm{Gal}_L)] \leqslant 2^{N-1} c_8$$

by Proposition 2.1.2(iii) and Theorem 2.4.2 for $\ell \gg 1$. Since the derived group of $\bar{\mathbf{G}}_\ell$ is $\bar{\mathbf{S}}_\ell$, the action of $\bar{\mathbf{G}}_\ell$ on the ambient space is semisimple if $\ell \gg 1$ by Proposition 2.1.2(ii). Therefore, we have proved assertions (i) and (ii) of Theorem 2.0.5. $\square$

Proof of Theorem 2.0.5(iii). Let $\bar{\mathbf{S}}_\ell^{\mathrm{sc}} \to \bar{\mathbf{S}}_\ell$ be the simply connected cover of $\bar{\mathbf{S}}_\ell$. The representation $(\bar{\mathbf{S}}_\ell^{\mathrm{sc}} \to \bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}) \times \bar{\mathbb{F}}_\ell$ is semisimple and has a $\mathbb{Z}$-form which belongs to a finite set of $\mathbb{Z}$-representations of simply connected Chevalley schemes [EHK12, Theorem 24] if $\ell \gg 1$. Thus, $\{\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell \gg 1}$ have bounded formal characters (Definition 4′). Let $\bar{\mathbf{C}}_\ell$ be the center of $\bar{\mathbf{G}}_\ell$. Since $\bar{\mathbf{S}}_\ell$ acts semi-simply on $\bar{V}_\ell$ by Proposition 2.1.2(ii) for $\ell \gg 1$, we decompose the representation $\bar{\mathbf{S}}_\ell \to \mathrm{GL}(\bar{V}_\ell)$ into a sum of absolutely irreducible representations $\bar{M}_i$,

$$\bar{V}_\ell = \left(\bigoplus_1^{m_1} \bar{M}_1\right) \oplus \left(\bigoplus_1^{m_2} \bar{M}_2\right) \oplus \cdots \oplus \left(\bigoplus_1^{m_k} \bar{M}_k\right),$$

such that $\bar{M}_i \ncong \bar{M}_j$ if $i \neq j$. If $c \in \bar{\mathbf{C}}_\ell$, then $\bar{M}_i$ and $c(\bar{M}_i)$ are isomorphic representations of $\bar{\mathbf{S}}_\ell$ for all i. Hence, c is invariant on $\bigoplus_1^{m_i} \bar{M}_i$ and $\bigoplus_1^{m_i} \bar{M}_i$ is a subrepresentation of $\bar{\mathbf{G}}_\ell$ on $\bar{V}_\ell$ for all i. Let n_i be the dimension of $\bar{M}_i$. Denote the representation of $\bar{\mathbf{S}}_\ell$ on $\bar{M}_i$ under some coordinates by

$$u_i : \bar{\mathbf{S}}_\ell \to \mathrm{GL}_{n_i}(\bar{\mathbb{F}}_\ell).$$

Then, the representation of $\bar{\mathbf{G}}_\ell$ on $\bigoplus_1^{m_i} \bar{M}_i$ is given by

$$q_i : \bar{\mathbf{G}}_\ell \to \mathrm{GL}_{n_i m_i}(\bar{\mathbb{F}}_\ell),$$

so that upon restricting to $\bar{\mathbf{S}}_\ell$ the action is 'diagonal':

$$q_i : \bar{\mathbf{S}}_\ell \xrightarrow{u_i} \mathrm{GL}_{n_i}(\bar{\mathbb{F}}_\ell) \to \bigoplus_1^{m_i} \mathrm{GL}_{n_i}(\bar{\mathbb{F}}_\ell) \subset \mathrm{GL}_{n_i m_i}(\bar{\mathbb{F}}_\ell),$$
$$x \mapsto u_i(x) \mapsto (u_i(x), \ldots, u_i(x)).$$

Since u_i is a irreducible representation and $q_i(c)$ commutes with $q_i(\bar{\mathbf{S}}_\ell)$, $q_i(c)$ is contained in the subgroup

$$\bar{\mathbf{H}}_i = \begin{pmatrix} \bar{\mathbf{D}}_{11} & \bar{\mathbf{D}}_{12} & \ldots & \bar{\mathbf{D}}_{1m_i} \\ \bar{\mathbf{D}}_{21} & \bar{\mathbf{D}}_{22} & \ldots & \bar{\mathbf{D}}_{2m_i} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{\mathbf{D}}_{m_i 1} & \bar{\mathbf{D}}_{m_i 2} & \ldots & \bar{\mathbf{D}}_{m_i m_i} \end{pmatrix},$$

where $\bar{\mathbf{D}}_{jk}$ is the subgroup of scalars of $\mathrm{GL}_{n_i}(\bar{\mathbb{F}}_\ell)$ for $1 \leqslant j \leqslant m_i$ and $1 \leqslant k \leqslant m_i$. We see that $\bar{\mathbf{H}}_i$ is isomorphic to $\mathrm{GL}_{m_i}(\bar{\mathbb{F}}_\ell)$. Since $q_i(\bar{\mathbf{C}}_\ell)$ is a diagonalizable group which commutes with $q_i(\bar{\mathbf{S}}_\ell)$

and $q_i|_{\bar{\mathbf{S}}_\ell}$ is 'diagonal', we may assume that, after a change of coordinates by some element in $\bar{\mathbf{H}}_i \cong \mathrm{GL}_{m_i}(\bar{\mathbb{F}}_\ell)$, $q_i(\bar{\mathbf{C}}_\ell)$ is contained in the following torus $\bar{\mathbf{D}}_i$ for all i:

$$\bar{\mathbf{D}}_i = \begin{pmatrix} \bar{\mathbf{D}}_{11} & 0 & \dots & 0 \\ 0 & \bar{\mathbf{D}}_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \bar{\mathbf{D}}_{m_im_i} \end{pmatrix}.$$

Therefore, we may assume that $\bar{\mathbf{C}}_\ell$ is a subgroup of

$$\bar{\mathbf{B}}_\ell := \bar{\mathbf{D}}_1 \times \bar{\mathbf{D}}_2 \times \cdots \times \bar{\mathbf{D}}_k \subset \mathrm{GL}_N(\bar{\mathbb{F}}_\ell)$$

in suitable coordinates. That the torus $\bar{\mathbf{B}}_\ell$ centralizes $\bar{\mathbf{S}}_\ell$ implies $\bar{\mathbf{B}}_\ell \subset \bar{\mathbf{N}}_\ell$. Denote the restriction $t_\ell|_{\bar{\mathbf{B}}_\ell}$ by s_ℓ. Since $\bar{\mathbf{N}}_\ell$ acts on $\bar{W}_\ell$, we have

$$s_\ell : \bar{\mathbf{B}}_\ell \to \mathrm{GL}_{W_\ell}.$$

We obtain $(s_\ell^{-1}(\bar{\mathbf{I}}_\ell))^\circ = \bar{\mathbf{C}}_\ell^\circ$ because $\mathrm{Ker}(s_\ell)$ is discrete. Consider the construction of U_ℓ from Theorem 2.4.1. This implies that the exponents of characters of s_ℓ on $\bar{\mathbf{D}}_i \cong \prod_1^{m_i} \bar{\mathbb{F}}_\ell^*$ are between 0 and c_3 for all i. By Theorem 2.4.2(i) and the above, the system of diagonalizable groups $\{s_\ell^{-1}(\bar{\mathbf{I}}_\ell)\}_{\ell \gg 1}$ satisfies the bounded exponents condition in Definition 4′. Hence, $\{\bar{\mathbf{C}}_\ell^\circ = (s_\ell^{-1}(\bar{\mathbf{I}}_\ell))^\circ \hookrightarrow \bar{\mathbf{B}}_\ell \hookrightarrow \mathrm{GL}_{V_\ell}\}_{\ell \gg 1}$ have bounded formal characters. Since $\{\bar{\mathbf{C}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell \gg 1}$ and $\{\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell \gg 1}$ both have bounded formal characters and $\bar{\mathbf{C}}_\ell^\circ$ commutes with $\bar{\mathbf{S}}_\ell$ for $\ell \gg 1$, $\{\bar{\mathbf{G}}_\ell = \bar{\mathbf{C}}_\ell^\circ \cdot \bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell \gg 1}$ have bounded formal characters by Proposition 2.0.4. This proves Theorem 2.0.5(iii). □

3. ℓ-independence of $\bar{\Gamma}_\ell$

3.1 Formal character of $\bar{\mathbf{G}}_\ell \subset \mathbf{GL}_{N,\mathbb{F}_\ell}$

A system of algebraic envelopes $\{\bar{\mathbf{G}}_\ell\}_{\ell \gg 1}$ of $\{\bar{\Gamma}_\ell\}_{\ell \gg 1}$ (Definition 5) was constructed in § 2.5. Let $\mathbf{G}_\ell$ be the algebraic monodromy group of Φ_ℓ^{ss} for all ℓ. The compatibility (Definition 2) of the system $\{\phi_\ell\}$ implies that the formal characters of $\{\bar{\mathbf{G}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell \gg 1} \cup \{\mathbf{G}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}\}_{\ell \gg 1}$ are the same in the sense of Definition 3′.

Theorem 3.1.1. *Let $\{\bar{\mathbf{G}}_\ell\}_{\ell \gg 1}$ be a system of algebraic envelopes of $\{\bar{\Gamma}_\ell\}_{\ell \gg 1}$ (Definition 5).*

(i) *The formal characters of $\bar{\mathbf{G}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ and $\mathbf{G}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ are the same for $\ell \gg 1$.*

(ii) *The formal characters of $\{\bar{\mathbf{G}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}\}_{\ell \gg 1}$ are the same.*

Proof. The mod ℓ system $\{\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)\}$ comes from the ℓ-adic system $\{\Phi_\ell^{\mathrm{ss}} : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{Q}_\ell)\}$ (Definition 1). The algebraic monodromy group $\mathbf{G}_\ell$ is reductive for all ℓ. By taking a finite extension K^{conn} of K (see [Ser81]), we may assume that $\mathbf{G}_\ell$ is connected for all ℓ. This does not change the formal character of $\mathbf{G}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$. It is well known that these algebraic monodromy groups have same reductive rank r. Define

$$\mathrm{Char} : \mathrm{GL}_N \to \mathbb{G}_a^{N-1} \times \mathbb{G}_m,$$

which maps a matrix to the coefficients of its characteristic polynomial. We know that $\mathrm{Char}(\mathbf{G}_\ell)$ is a $\mathbb{Q}$-variety of dimension r that is independent of ℓ (by the compatibility conditions) and can be defined over $\mathbb{Z}[1/N']$ for some positive integer N' that is sufficiently divisible. Let $\mathbf{P}_{\mathbb{Z}[1/N']}$ be the Zariski closure of $\mathrm{Char}(\mathbf{G}_\ell)$ in the projective $\mathbb{P}^N_{\mathbb{Z}[1/N']}$. Since ϕ_ℓ is continuous, every element of $\bar{\Gamma}_\ell$ is the image of a Frobenius element. Therefore, $\mathrm{Char}(\bar{\Gamma}_\ell)$ is a subset of the $\mathbb{F}_\ell$-rational points of $\mathbf{P}_{\mathbb{F}_\ell} := \mathbf{P}_{\mathbb{Z}[1/N']} \times_{\mathbb{Z}} \mathbb{F}_\ell$ for $\ell \gg 1$.

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

Generic flatness [DG65, Theorem 6.9.1] implies that $\mathbf{P}_{\mathbb{Z}[1/N']}$ is flat over $\mathbb{Z}[1/N']$ for sufficiently divisible N', so the dimension of every irreducible component of $\mathbf{P}_{\mathbb{Z}[1/N']}$ is $r+1$ (see [Har77, ch. 3, Proposition 9.5]), and hence the dimension of every irreducible component of $\mathbf{P}_{\mathbb{F}_\ell}$ is r (see [Har77, ch. 3, Corollary 9.6]) for $\ell \gg 1$. Also, the Hilbert polynomial of $\mathbf{P}_{\mathbb{F}_\ell}$ and, in particular, the *degree* (call it d) of $\mathbf{P}_{\mathbb{F}_\ell} \subset \mathbb{P}^N_{\mathbb{F}_\ell}$ is independent of ℓ for $\ell \gg 1$ (see [Har77, ch. 3, Theorem 9.9]). Since d is a positive integer, we conclude that the number and the degrees of irreducible components of $\mathbf{P}_{\mathbb{F}_\ell}$ are bounded by d (see [Har77, ch. 1, Proposition 7.6(a) and (b)]). By [LW54, Theorem 1] and the above, we have that

$$|\mathbf{P}_{\mathbb{F}_\ell}(\mathbb{F}_\ell)| \leqslant 3d \cdot \ell^r$$

for $\ell \gg 1$. Let $\bar{\mathbf{T}}_\ell$ be a $\mathbb{F}_\ell$-maximal torus of $\bar{\mathbf{G}}_\ell$. Then [Nor87, Lemma 3.5] implies that $\bar{\mathbf{T}}_\ell$ has at least $(\ell-1)^{\dim(\bar{\mathbf{T}}_\ell)}$ $\mathbb{F}_\ell$-rational points. By Theorem 2.0.5(i), there is an integer $n>0$ such that the nth power of $\bar{\mathbf{T}}_\ell(\mathbb{F}_\ell)$ is contained in $\bar{\gamma}_\ell$ for $\ell \gg 1$. One sees, by diagonalizing $\bar{\mathbf{T}}_\ell$ in $\mathrm{GL}_{N,\bar{F}_\ell}$, that the order of the kernel of this nth-power homomorphism is less than or equal to n^N. Hence, we obtain that

$$|\bar{\mathbf{T}}_\ell(\mathbb{F}_\ell) \cap \bar{\gamma}_\ell| \geqslant \frac{(\ell-1)^{\dim(\bar{\mathbf{T}}_\ell)}}{n^N}.$$

Also, the morphism Char restricted to any maximal torus of GL_N is a finite morphism of degree $N!$. Thus, there is a constant $c>0$ such that

$$c \cdot \ell^{\dim(\bar{\mathbf{T}}_\ell)} \leqslant |\mathrm{Char}(\bar{\mathbf{T}}_\ell(\mathbb{F}_\ell) \cap \bar{\gamma}_\ell)| \leqslant |\mathrm{Char}(\bar{\gamma}_\ell)| \leqslant |\mathbf{P}_{\mathbb{F}_\ell}(\mathbb{F}_\ell)| \leqslant 3d \cdot \ell^r$$

for $\ell \gg 1$. This implies that $\dim(\bar{\mathbf{T}}_\ell) \leqslant r$ for $\ell \gg 1$.

On the other hand, for each $\ell \gg 1$ we can find a set R_ℓ of characters of $\mathbb{G}_m^N$ of exponents bounded by $C>0$ such that $\bar{\mathbf{T}}_\ell$ is conjugate in $\mathrm{GL}_{N,\bar{F}_\ell}$ to the kernel of R_ℓ by Theorem 2.0.5(iii) and Definition 4$'$. Let $\mathscr{L}$ be an infinite subset of prime numbers $\mathscr{P}$ such that for all $\ell, \ell' \in \mathscr{L}$ we have the equality $R_\ell = R_{\ell'}$. Denote this common set of characters by R, and define $\mathbf{Y}_{\mathbb{C}} = \{y \in \mathbb{G}^N_{m,\mathbb{C}} : \chi(y) = 1 \text{ for all } \chi \in R\}$ so that $\dim_{\mathbb{C}} \mathbf{Y}_{\mathbb{C}} = \dim_{\bar{\mathbb{F}}_\ell} \bar{\mathbf{T}}_\ell$ for all $\ell \in \mathscr{L}$. If $\bar{v}$ divides $v \in \Sigma_K \backslash S_\ell$ (the S_ℓ in Definition 2), then the characteristic polynomial of $\phi_\ell(\mathrm{Frob}_{\bar{v}})$ is just the mod ℓ reduction of the characteristic polynomial of $\Phi_\ell^{\mathrm{ss}}(\mathrm{Frob}_{\bar{v}}) = P_v(x) \in \mathbb{Q}[x]$, which depends only on v (Definition 2). Therefore, for each $v \notin S$ (Definition 2), we can put the roots of $P_v(x)$ in some order $\alpha_1, \alpha_2, \ldots, \alpha_N$ such that the following congruence equation holds:

$$\alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_N^{m_N} \equiv 1 \pmod{\ell'}$$

for any character $x_1^{m_1} x_2^{m_2} \cdots x_N^{m_N} \in R$ and

$$\ell' \in \mathscr{L}_v := \mathscr{L} \backslash \{\ell'' \in \mathscr{P} : \exists v' \in S_\ell \text{ such that } v' \mid \ell''\}$$

if $v \mid \ell$. Since $\alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_N^{m_N}$ is an algebraic number and $\mathscr{L}_v$ consists of infinitely many primes, we obtain the equality

$$\alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_N^{m_N} = 1$$

for any character $x_1^{m_1} x_2^{m_2} \cdots x_N^{m_N} \in R$. Therefore,

$$(\mathrm{Char}|_{\mathbb{G}_m^N})^{-1}(\{P_v(x) : v \in \Sigma_K \backslash S\}) \subset \bigcup_{g \in \mathrm{Perm}(N)} g(\mathbf{Y}_{\mathbb{C}}),$$

where $\mathrm{Perm}(N)$ is the group of permutations of N letters permuting the coordinates. Since $\{P_v(x) : v \in \Sigma_K \backslash S\}$ is Zariski dense in $\mathrm{Char}(\mathbf{G}_\ell)$ of dimension r and $\mathrm{Char}|_{\mathbb{G}_m^N}$ is a finite morphism of degree $N!$, the Zariski closure of $(\mathrm{Char}|_{\mathbb{G}_m^N})^{-1}(\{P_v(x) : v \in \Sigma_K\backslash S\})$ in $\mathbb{G}^N_{m,\mathbb{C}}$, denoted by $\mathbf{D}_\mathbb{C}$, is also of dimension r. Because we have obtained $\dim(\bar{\mathbf{T}}_\ell) \leqslant r$ at the end of the second paragraph and any maximal torus of the algebraic monodromy group $\mathbf{G}_\ell$ is conjugate in $\mathrm{GL}_{N,\mathbb{C}}$ to an irreducible component of $\mathbf{D}_\mathbb{C}$ (see [Ser81]), the inclusion

$$\mathbf{D}_\mathbb{C} \subset \bigcup_{g\in \mathrm{Perm}(N)} g(\mathbf{Y}_\mathbb{C})$$

implies that the formal characters of $\bar{\mathbf{G}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ and $\mathbf{G}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ are the same in the sense of Definition $3'$ for all $\ell \in \mathscr{L}$. There are only finitely many possibilities for R_ℓ by Remark 2.0.2 and Proposition 2.0.3. Upon excluding the primes ℓ such that R_ℓ appears finitely many times, we conclude that the formal characters of $\bar{\mathbf{G}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ and $\mathbf{G}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ are the same for $\ell \gg 1$. This proves (i) and hence (ii), since the formal character of $\mathbf{G}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ is independent of ℓ (see [Ser81]). □

3.2 Formal character of $\bar{\mathbf{S}}_\ell \subset \mathbf{GL}_{N,\mathbb{F}_\ell}$

We make the following assumptions for this subsection.

Assumptions. By taking a field extension of K, we may assume that:

(i) $\mathbf{G}_\ell$, the algebraic monodromy group of Φ_ℓ^{ss}, is connected for all ℓ (see [Ser81]);

(ii) for all ℓ, $\bar{\Omega}_\ell := \mu_\ell(\bar{\Gamma}_\ell)$ corresponds to an abelian extension of K that is unramified at all primes not dividing ℓ (see the first paragraph of the proof of Theorem 2.4.2).

Theorem 3.2.1 below is the main result of this subsection. Denote a finite extension of K by K'. Because $\bar{\mathbf{S}}_\ell$ is independent of K' over K for $\ell \gg 1$ by Remark 2.1.3, the assumptions above remain valid for K', and $\{\bar{\mathbf{G}}_\ell\}_{\ell\gg 1}$ constructed in § 2.5 are still algebraic envelopes of $\{\phi_\ell(\mathrm{Gal}_{K'})\}_{\ell\gg 1}$, we are free to replace K with K' in this subsection.

Theorem 3.2.1. *Let $\bar{\mathbf{S}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ be the semisimple envelope of $\bar{\Gamma}_\ell$ (Definition 6) for all $\ell \gg 1$.*

(i) *The formal character of $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ is equal to the formal character of $\mathbf{G}_\ell^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ for $\ell \gg 1$, where $\mathbf{G}_\ell^{\mathrm{der}}$ is the derived group of the algebraic monodromy group $\mathbf{G}_\ell$ of Φ_ℓ^{ss}.*

(ii) *The formal character of $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ is independent of ℓ if $\ell \gg 1$.*

In [Hui13, § 3], we used mainly abelian ℓ-adic representations to prove that the formal character of $\mathbf{G}_\ell^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ is independent of ℓ. To prove Theorem 3.2.1, we adopt this strategy in a mod ℓ fashion. The key point is to establish that the inertia characters of μ_ℓ (Definition 9) for $\ell \gg 1$ are in some sense the mod ℓ reductions of inertia characters of some Serre group $\mathbf{S}_\mathfrak{m}$ (see [Ser98, ch. 2] and Proposition 3.2.4).

Definition 12. For each prime $\ell \in \mathscr{P}$, choose a valuation $\bar{v}_\ell$ of $\bar{\mathbb{Q}}$ that extends the ℓ-adic valuation of $\mathbb{Q}$. This valuation on $\bar{\mathbb{Q}}$ is equal to the restriction of the unique non-Archimedean valuation on $\bar{\mathbb{Q}}_\ell$ (extending the ℓ-adic valuation on $\mathbb{Q}_\ell$) to $\bar{\mathbb{Q}}$ with respect to some embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$. Denote this valuation on $\bar{\mathbb{Q}}_\ell$ by $\bar{v}_\ell$ as well. We use the following notation:

- $\mathrm{Gal}_K^{\mathrm{ab}}$, the Galois group of the maximal abelian extension of K;
- I_K, the group of idéles of K;
- $(x_v)_{v\in\Sigma_K}$, a representation of a finite idéle;
- K_v, the completion of K with respect to $v \in \Sigma_K$;
- U_v, the unit group of K_v^*;

- k_v, the residue field of K_v;
- $\mathfrak{m}_0$, the modulus of empty support;
- $U_{\mathfrak{m}_0} := \prod_v U_v$;
- $K_\ell := \prod_{v|\ell} K_v = K \otimes \mathbb{Q}_\ell$;
- $\bar{\mathbb{Z}}_\ell$, the valuation ring of $\bar{v}_\ell$;
- $\mathfrak{p}_\ell$, the maximal ideal of $\bar{v}_\ell$;
- k_ℓ, the residue field of $\bar{v}_\ell$;
- $x_\ell := (x_v)_{v|\ell}$.

Let $\sigma : K \to \bar{\mathbb{Q}}$ be an embedding of K in $\bar{\mathbb{Q}}$. The composition of σ with $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ extends to a $\mathbb{Q}_\ell$-algebra homomorphism $\sigma_\ell : K_\ell \to \bar{\mathbb{Q}}_\ell$.

Remark 3.2.2. The field k_ℓ is an algebraic closure of $\mathbb{F}_\ell$ and the homomorphism σ_ℓ is trivial on the components K_v of K_ℓ when v is not equivalent to $\bar{v}_\ell \circ \sigma$.

Recall the representation $\mu_\ell : \mathrm{Gal}_K \to \mathrm{GL}(W_\ell)$ (abelian by assumption (ii)) from Definition 9. Thus, μ_ℓ induces the following ρ_ℓ for each ℓ by composing with $I_K \to \mathrm{Gal}_K^{\mathrm{ab}}$:

$$\rho_\ell : I_K \to \mathrm{GL}(W_\ell).$$

PROPOSITION 3.2.3. *If $\chi_\ell : I_K \to \bar{\mathbb{F}}_\ell^*$ is a character of ρ_ℓ for $\ell \gg 1$, then for any finite idéle $x \in U_{\mathfrak{m}_0}$ we have the congruence*

$$\chi_\ell(x) \equiv \prod_{\sigma \in \mathrm{Hom}(K,\bar{\mathbb{Q}})} \sigma_\ell(x_\ell^{-1})^{m(\sigma,\ell)} \ (\mathrm{mod}\ \mathfrak{p}_\ell)$$

such that $0 \leqslant m(\sigma,\ell) \leqslant c_6$.

Proof. Since $|\bar{\Omega}_\ell|$ is prime to ℓ, the homomorphism

$$U_v \hookrightarrow K_v^* \to I_K \xrightarrow{\rho_\ell} \mathrm{GL}(W_\ell)$$

factors through $\alpha_v : k_v^* \to \mathrm{GL}(W_\ell)$ for all $v \mid \ell$. On the other hand, let $\bar{v} \in \Sigma_{\bar{K}}$ divide ℓ. Since $\bar{\Omega}_\ell$ is abelian and of order prime to ℓ, the restriction of $\mu_\ell : \mathrm{Gal}_K \to \mathrm{GL}(W_\ell)$ to $I_{\bar{v}}$ factors through

$$I_{\bar{v}} \to I_{\bar{v}}^{\mathrm{t}} \xrightarrow{\cong} \varprojlim \mathbb{F}_{\ell^k}^* \to k_v^*$$

and induces $\beta_v : k_v^* \to \mathrm{GL}(W_\ell)$ that depends on $v = \bar{v}|_{\bar{K}}$. By [Ser72, Proposition 3], α_v and β_v are inverses of each other. Since $f_{\bar{v}}$ (Definition 10) factors through β_v and the exponents of any character of $f_{\bar{v}}$ when expressed as an ℓ-restricted (Definition 8) product of fundamental characters of level $c_4!$ are bounded by c_6 for $\ell \gg 1$ (§ 2.4), the exponents of χ_ℓ when expressed as an ℓ-restricted product of fundamental characters of level $[k_v : \mathbb{F}_\ell]$ are also bounded by c_6 for $\ell \gg 1$. Since ρ_ℓ is unramified at all v not dividing ℓ, ρ_ℓ is trivial on the subgroup $\prod_{v\nmid\ell} U_v$ of $U_{\mathfrak{m}_0} := \prod_v U_v$. Therefore we conclude the congruence for $\ell \gg 1$. □

DEFINITION 13. Let $\mathbf{S}_\mathfrak{m}$ be the Serre group of K with modulus $\mathfrak{m}$ (see [Ser98, ch. 2]), and let $\Theta : \mathbf{S}_\mathfrak{m} \to \mathbb{G}_{m,\bar{\mathbb{Q}}_\ell}$ be a character of $\mathbf{S}_\mathfrak{m}$ over $\bar{\mathbb{Q}}_\ell$. Since the image of the abelian representation Θ_ℓ attached to Θ,

$$\Theta_\ell : \mathrm{Gal}_K^{\mathrm{ab}} \to \mathbf{S}_\mathfrak{m}(\mathbb{Q}_\ell) \xrightarrow{\Theta} \bar{\mathbb{Q}}_\ell^*$$

(see [Ser98, ch. 2]), is contained in $\bar{\mathbb{Z}}_\ell^*$, define

$$\theta_\ell : I_K \to k_\ell^* \cong \bar{\mathbb{F}}_\ell^*$$

as the mod $\mathfrak{p}_\ell$ reduction of the composition of $I_K \to \mathrm{Gal}_K^{\mathrm{ab}}$ with Θ_ℓ.

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

Proposition 3.2.4. *Let χ_ℓ be a character of ρ_ℓ as above. If ℓ is sufficiently large, then there is a character Θ of $\mathbf{S}_{\mathfrak{m}_0}$ such that*

$$\chi_\ell(x) = \theta_\ell(x)$$

for all $x \in U_{\mathfrak{m}_0}$, where θ_ℓ is as in Definition 13.

Proof. Since $0 \leqslant m(\sigma, \ell) \leqslant c_6$ for all $\sigma \in \mathrm{Hom}(K, \bar{\mathbb{Q}})$ and $\ell \gg 1$ by Proposition 3.2.3, the proposition follows from the proof of [Ser72, Proposition 20]. □

Let $\Psi : \mathbf{S}_{\mathfrak{m}_0} \to \mathrm{GL}_{n,\mathbb{Q}}$ be a $\mathbb{Q}$-morphism of the Serre group $\mathbf{S}_{\mathfrak{m}_0}$ with finite kernel. Then Ψ induces a strictly compatible system $\{\Psi_\ell\}_{\ell\in\mathscr{P}}$ of abelian ℓ-adic representations of Gal_K (see [Ser98, ch. 2]) with $S = \emptyset$ (Definition 2),

$$\Psi_\ell : \mathrm{Gal}_K \to \mathrm{Gal}_K^{\mathrm{ab}} \to \mathrm{GL}_n(\mathbb{Q}_\ell).$$

We may assume that $\{\Psi_\ell\}$ is integral [Ser98, ch. 2, § 3.4] by twisting $\{\Psi_\ell\}$ with a suitable large power of the system of cyclotomic characters.

Proposition 3.2.5. *Let Ψ and $\{\Psi_\ell\}_{\ell\in\mathscr{P}}$ be as above.*

(i) *The subgroup generated by the characters of Ψ is of finite index in the character group of $\mathbf{S}_{\mathfrak{m}_0}$. Denote this index by k.*

(ii) *For any ℓ and character θ_ℓ of I_K induced from a character Θ of $\mathbf{S}_{\mathfrak{m}_0}$ as in Definition 13, we obtain the following congruence for all $x \in U_{\mathfrak{m}_0} \subset I_K$:*

$$\theta_\ell(x) \equiv \prod_{\sigma\in\mathrm{Hom}(K,\bar{\mathbb{Q}})} \sigma_\ell(x_\ell^{-1})^{m(\sigma)} \pmod{\mathfrak{p}_\ell},$$

such that $m(\sigma) \geqslant 0$ for all σ.

Proof. Statement (i) follows from the fact that Ψ is an isogeny from $\mathbf{S}_{\mathfrak{m}_0}$ onto $\Psi(\mathbf{S}_{\mathfrak{m}_0})$. Statement (ii) follows from the integrality of the system $\{\Psi_\ell\}$ and the theory of abelian ℓ-adic representations [Ser98, chs 2 and 3]. □

Denote the semi-simplification of some mod ℓ reduction of Ψ_ℓ by ψ_ℓ for all ℓ. Consider the following strictly compatible system of ℓ-adic representations:

$$\{\Phi_\ell \times \Psi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{Q}_\ell) \times \mathrm{GL}_n(\mathbb{Q}_\ell)\}_{\ell\in\mathscr{P}}.$$

The semi-simplification of some mod ℓ reduction of $\{\Phi_\ell \times \Psi_\ell\}_{\ell\in\mathscr{P}}$,

$$\{\phi_\ell \times \psi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell) \times \mathrm{GL}_n(\mathbb{F}_\ell)\}_{\ell\in\mathscr{P}},$$

is then a strictly compatible system of mod ℓ representations (Definition 2). Denote the image of $\phi_\ell \times \psi_\ell$ by $\bar{\Gamma}'_\ell$. Let $\bar{v} \in \Sigma_{\bar{K}}$ divide ℓ. When we restrict $\phi_\ell \times \psi_\ell$ to the inertia subgroup $I_{\bar{v}}$ of Gal_K and then semi-simplify, the exponents of characters of the tame inertia quotient $I_{\bar{v}}^{\mathrm{t}}$ for some level are bounded independently of ℓ by § 2.3, Proposition 3.2.5(ii) and [Ser72, Proposition 3]. Therefore, we can construct as in § 2 semisimple envelopes $\{\bar{\mathbf{S}}'_\ell\}_{\ell\gg1}$ (Definition 6), inertia tori $\{\bar{\mathbf{I}}'_\ell\}_{\ell\gg1}$ (Theorem 2.4.2) and algebraic envelopes $\{\bar{\mathbf{G}}'_\ell\}_{\ell\gg1}$ (Definition 5) of $\{\bar{\Gamma}'_\ell\}_{\ell\gg1}$.

Since ψ_ℓ is semisimple and abelian, we see that Nori's construction gives $\bar{\mathbf{S}}'_\ell = \bar{\mathbf{S}}_\ell \times \{1\} \subset \mathrm{GL}_{N,\mathbb{F}_\ell} \times \mathrm{GL}_{n,\mathbb{F}_\ell}$. The normalizer of $\bar{\mathbf{S}}_\ell \times \{1\}$ in $\mathrm{GL}_{N,\mathbb{F}_\ell} \times \mathrm{GL}_{n,\mathbb{F}_\ell}$ is $\bar{\mathbf{N}}_\ell \times \mathrm{GL}_{n,\mathbb{F}_\ell}$. We have

$$t_\ell \times \mathrm{id} : \bar{\mathbf{N}}_\ell \times \mathrm{GL}_{n,\mathbb{F}_\ell} \to \mathrm{GL}_{W_\ell} \times \mathrm{GL}_{n,\mathbb{F}_\ell}$$

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

with kernel $\bar{\mathbf{S}}_\ell \times \{1\}$. Therefore, we obtain a map

$$\mu_\ell \times \psi_\ell : \mathrm{Gal}_K^{\mathrm{ab}} \to \mathrm{GL}(W_\ell) \times \mathrm{GL}_n(\mathbb{F}_\ell)$$

with image denoted by $\bar{\Omega}'_\ell$. As $\bar{\Omega}'_\ell$ is abelian, denote the compositions of μ_ℓ and ψ_ℓ with $I_K \to \mathrm{Gal}_K^{\mathrm{ab}}$ by $\widetilde{\mu}_\ell$ and $\widetilde{\psi}_\ell$, respectively, for all ℓ. By $(*)$ in the proof of Theorem 2.4.2 and [Neu99, Proposition 9.5], we assume, by taking a finite extension of K, that

$$(**) : \quad (\widetilde{\mu}_\ell \times \widetilde{\psi}_\ell)\left(\prod_{v|\ell} U_v\right) = \bar{\Omega}'_\ell \quad \text{for all } \ell \gg 1.$$

PROPOSITION 3.2.6. *Let $p_2 : \mathrm{GL}_{W_\ell} \times \mathrm{GL}_{n,\mathbb{F}_\ell}$ be the projection to the second factor. Then p_2 is an isogeny from $\bar{\mathbf{I}}'_\ell$ onto $p_2(\bar{\mathbf{I}}'_\ell)$ for $\ell \gg 1$.*

Proof. Let $(x, 1) \in \mathrm{GL}_{W_\ell} \times \mathrm{GL}_{n,\mathbb{F}_\ell}$ be an element of $\bar{\Omega}'_\ell \cap \mathrm{Ker}(p_2)$, where $(x, 1) = (\widetilde{\mu}_\ell \times \widetilde{\psi}_\ell)(x_\ell)$ for some $x_\ell \in \prod_{v|\ell} U_v$ (Definition 12) by $(**)$ above. Since $\Psi : \mathbf{S}_{\mathfrak{m}_0} \to \mathrm{GL}_{n,\mathbb{Q}}$ has finite kernel and $\widetilde{\mu}_\ell \times \widetilde{\psi}_\ell$ is abelian and semisimple, we have $x^k = 1$ for $\ell \gg 1$ by the fact that $1 = \widetilde{\psi}_\ell(x_\ell)$ together with Propositions 3.2.4 and 3.2.5(i). Since $\bar{\Omega}'_\ell$ is abelian of order prime to ℓ, $x^k = 1$ implies that x has at most $k^{\dim(W_\ell)}$ possibilities (by diagonalizing the image of $\widetilde{\mu}_\ell$), which implies that

$$|\bar{\Omega}'_\ell \cap \mathrm{Ker}(p_2)| \leqslant k^{\dim(W_\ell)}.$$

Therefore, the $\mathbb{F}_\ell$-diagonalizable group $\mathrm{Ker}(p_2) \cap \bar{\mathbf{I}}'_\ell$ cannot have positive dimension for $\ell \gg 1$, because $[\bar{\mathbf{I}}'_\ell(\mathbb{F}_\ell) : \bar{\Omega}'_\ell \cap \bar{\mathbf{I}}'_\ell(\mathbb{F}_\ell)]$ is also uniformly bounded by Theorem 2.4.2(ii). Thus, p_2 is an isogeny from $\bar{\mathbf{I}}'_\ell$ onto $p_2(\bar{\mathbf{I}}'_\ell)$. □

Proof of Theorem 3.2.1. The mod ℓ system

$$\{\phi_\ell \times \psi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell) \times \mathrm{GL}_n(\mathbb{F}_\ell)\}$$

comes from the ℓ-adic system (i.e. the semi-simplification of a mod ℓ reduction)

$$\{\Phi_\ell^{\mathrm{ss}} \times \Psi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{Q}_\ell) \times \mathrm{GL}_n(\mathbb{Q}_\ell)\}.$$

Let $\mathbf{G}'_\ell$ be the algebraic monodromy group of the semisimple representation $\Phi_\ell^{\mathrm{ss}} \times \Psi_\ell$ for all ℓ. Thus $\mathbf{G}'_\ell$ is reductive and we may assume that $\mathbf{G}'_\ell$ is connected for all ℓ by taking a finite extension of K. Denote the projections to the first and second factors of $\mathrm{GL}_N \times \mathrm{GL}_n$ by p_1 and p_2, respectively. Consider the map

$$\mathrm{Char}_1 \times \mathrm{Char}_2 : \mathrm{GL}_N \times \mathrm{GL}_n \to (\mathbb{G}_a^{N-1} \times \mathbb{G}_m) \times (\mathbb{G}_a^{n-1} \times \mathbb{G}_m)$$

where $\mathrm{Char}_i = \mathrm{Char} \circ p_i$ for $i = 1, 2$. Note that the restriction of $\mathrm{Char}_1 \times \mathrm{Char}_2$ to $\mathbb{G}_m^N \times \mathbb{G}_m^n$ is a finite morphism. Let $\mathbf{T}'_\ell$ be a maximal torus of the monodromy group $\mathbf{G}'_\ell$ and $\bar{\mathbf{T}}'_\ell$ a maximal torus of $\bar{\mathbf{G}}'_\ell$, the algebraic envelope of the mod ℓ representation $\phi_\ell \times \psi_\ell$. Up to conjugation by $\mathrm{GL}_N \times \mathrm{GL}_n$ (over algebraically closed fields), we may assume that $\mathbf{T}'_\ell$ and $\bar{\mathbf{T}}'_\ell$ are diagonal (i.e. inside $\mathbb{G}_m^{N+n}$). We claim that, up to permutation of coordinates by $\mathrm{Perm}(N) \times \mathrm{Perm}(n)$, $\mathbf{T}'_\ell$ and $\bar{\mathbf{T}}'_\ell$ are annihilated by the same set of characters of $\mathbb{G}_m^{N+n}$ for all sufficiently large ℓ. The proof of the claim proceeds in exactly the same way as the proof of Theorem 3.1.1(i), with the following replacements:

- $\mathrm{GL}_N \longrightarrow \mathrm{GL}_N \times \mathrm{GL}_n$;
- morphism $\mathrm{Char} \longrightarrow$ morphism $\mathrm{Char}_1 \times \mathrm{Char}_2$;

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

- $\mathbb{Q}$-variety $\mathrm{Char}(\mathbf{G}_\ell) \longrightarrow \mathbb{Q}$-variety $\mathrm{Char}_1 \times \mathrm{Char}_2(\mathbf{G}'_\ell)$;
- $\mathrm{Perm}(N) \longrightarrow \mathrm{Perm}(N) \times \mathrm{Perm}(n)$.

Therefore, $\mathbf{T}''_\ell := \mathrm{Ker}(p_2 : \mathbf{T}'_\ell \to p_2(\mathbf{T}'_\ell))^\circ$ and $\bar{\mathbf{T}}''_\ell := \mathrm{Ker}(p_2 : \bar{\mathbf{T}}'_\ell \to p_2(\bar{\mathbf{T}}'_\ell))^\circ$ as subtori of $\mathbb{G}_m^N$ are annihilated by the same set of characters for $\ell \gg 1$. The torus $\mathbf{T}''_\ell$ is the formal character of $\mathbf{G}_\ell^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ (see [Hui13, proof of Theorem 3.19]). It suffices to show that $\bar{\mathbf{T}}''_\ell$ is a maximal torus of $\bar{\mathbf{S}}_\ell$ for $\ell \gg 1$. Since the dimension of the torus $\bar{\mathbf{I}}'_\ell$ is equal to the dimension of the center of the algebraic envelope $\bar{\mathbf{G}}'_\ell$ for $\ell \gg 1$ (see § 2.5) and p_2 is an isogeny from $\bar{\mathbf{I}}'_\ell$ onto $p_2(\bar{\mathbf{I}}'_\ell)$ by Proposition 3.2.6 for $\ell \gg 1$, the identity component of the kernel of

$$p_2 : \bar{\mathbf{G}}'_\ell \to p_2(\bar{\mathbf{G}}'_\ell) = p_2(\bar{\mathbf{I}}'_\ell)$$

is $\bar{\mathbf{S}}'_\ell$ (the semisimple part of $\bar{\mathbf{G}}'_\ell$) for $\ell \gg 1$. Since $p_2(\bar{\mathbf{T}}'_\ell) = p_2(\bar{\mathbf{G}}'_\ell) = p_2(\bar{\mathbf{I}}'_\ell)$ for $\ell \gg 1$, by construction $\bar{\mathbf{T}}''_\ell$ is a maximal torus of $\bar{\mathbf{S}}'_\ell = \bar{\mathbf{S}}_\ell \times \{1\}$ for $\ell \gg 1$. Hence, the formal characters of $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ and $\mathbf{G}_\ell^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ are the same for $\ell \gg 1$. This proves (i). Since the formal character of $\mathbf{G}_\ell^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$ is independent of ℓ (see [Hui13, Theorem 3.19]), we obtain (ii) from (i). ◻

3.3 Proofs of Theorem A and Corollary B

The following purely representation-theoretic result is crucial to the study of Galois images $\bar{\Gamma}_\ell$ for $\ell \gg 1$.

Theorem 3.3.1 [Hui13, Theorem 2.19]. *Let V be a finite-dimensional $\mathbb{C}$-vector space, and let $\rho_1 : \mathfrak{g} \to \mathrm{End}(V)$ and $\rho_2 : \mathfrak{h} \to \mathrm{End}(V)$ be two faithful representations of complex semisimple Lie algebras. If the formal characters of ρ_1 and ρ_2 are equal, then the number of A_n factors for $n \in \mathbb{N}\backslash\{1,2,3,4,5,7,8\}$ and the parity of A_4 factors of $\mathfrak{g}$ and $\mathfrak{h}$ are equal.*

Theorem 3.3.2. *The number of $A_n = \mathfrak{sl}_{n+1}$ factors for $n \in \mathbb{N}\backslash\{1,2,3,4,5,7,8\}$ and the parity of A_4 factors of $\bar{\mathbf{S}}_\ell \times_{\mathbb{F}_\ell} \bar{\mathbb{F}}_\ell$ are independent of ℓ if $\ell \gg 1$.*

Proof. Let $\bar{\mathbf{S}}_\ell^{\mathrm{sc}} \to \bar{\mathbf{S}}_\ell$ be the simply connected cover of the semisimple $\bar{\mathbf{S}}_\ell$ for $\ell \gg 1$. Then the representation $(\bar{\mathbf{S}}_\ell^{\mathrm{sc}} \to \bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}) \times \bar{\mathbb{F}}_\ell$ can be lifted to a representation of a simply connected Chevalley scheme $\mathbf{H}_{\ell,\mathbb{Z}}$ defined over $\mathbb{Z}$ for $\ell \gg 1$,

$$\pi_{\ell,\mathbb{Z}} : \mathbf{H}_{\ell,\mathbb{Z}} \to \mathrm{GL}_{N,\mathbb{Z}}$$

(see [EHK12, Theorem 24]), which is also a $\mathbb{Z}$-form of a representation of a simply connected $\mathbb{C}$-semisimple group $\mathbf{H}_{\ell,\mathbb{C}}$,

$$\pi_{\ell,\mathbb{C}} : \mathbf{H}_{\ell,\mathbb{C}} \to \mathrm{GL}_{N,\mathbb{C}}$$

(see [Ste68a]). Hence, $\bar{\mathbf{S}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ and $\pi_{\ell,\mathbb{C}}(\mathbf{H}_{\ell,\mathbb{C}}) \subset \mathrm{GL}_{N,\mathbb{C}}$ have the same formal character for $\ell \gg 1$. This and Theorem 3.2.1 imply that the formal character of $\pi_{\ell,\mathbb{C}}(\mathbf{H}_{\ell,\mathbb{C}}) \subset \mathrm{GL}_{N,\mathbb{C}}$ is independent of ℓ when ℓ is sufficiently large, which in turn implies that the formal character of $\mathrm{Lie}(\pi_{\ell,\mathbb{C}}(\mathbf{H}_{\ell,\mathbb{C}})) \hookrightarrow \mathrm{End}(\mathbb{C}^N)$ (see [Hui13, § 2.1]) is independent of ℓ when ℓ is sufficiently large. Therefore, the number of A_n factors for $n \in \mathbb{N}\backslash\{1,2,3,4,5,7,8\}$ and the parity of A_4 factors of $\pi_{\ell,\mathbb{C}}(\mathbf{H}_{\ell,\mathbb{C}})$ and hence $\mathbf{H}_{\ell,\mathbb{C}}$ (the homomorphism $\mathbf{H}_{\ell,\mathbb{C}} \to \pi_{\ell,\mathbb{C}}(\mathbf{H}_{\ell,\mathbb{C}})$ is an isogeny since $\bar{\mathbf{S}}_\ell^{\mathrm{sc}} \to \bar{\mathbf{S}}_\ell$ is an isogeny) are independent of ℓ for $\ell \gg 1$ by Theorem 3.3.1. Since the number of simple factors of $\bar{\mathbf{S}}_\ell^{\mathrm{sc}} \times \bar{\mathbb{F}}_\ell$ and $\mathbf{H}_{\ell,\mathbb{C}}$ of each type are equal, we are done. ◻

Let $\mathfrak{g}$ be a simple Lie type (e.g. $A_n, B_n, C_n, D_n, \ldots$) and $\bar{\Gamma}$ a finite group. Suppose $\ell \geqslant 5$. We measure the number of $\mathfrak{g}$-type simple factors of characteristic ℓ and the total number of Lie-type

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

simple factors of characteristic ℓ within the set of composition factors of $\bar{\Gamma}$ in the following sense. Let $\mathbb{F}_q$ be a finite field of characteristic ℓ, σ the Frobenius automorphism of $\bar{\mathbb{F}}_q/\mathbb{F}_q$ and $\bar{\mathbf{G}}$ a connected $\mathbb{F}_q$-group which is almost simple over $\bar{\mathbb{F}}_q$. The identification of $\bar{\mathbf{G}}_\sigma := \bar{\mathbf{G}}(\mathbb{F}_q)$ is related to $\mathfrak{g}$, the simple type of $\bar{\mathbf{G}} \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$, as shown in the following table [Ste68b, 11.6].

Type of $\bar{\mathbf{G}}$	Composition factors of $\bar{\mathbf{G}}(\mathbb{F}_q)$
A_1	$A_1(q) = \mathrm{PSL}_2(q)$ + cyclic groups
A_n $(n \geqslant 2)$	$A_n(q)$ or ${}^2A_n(q^2)$ + cyclic groups
B_n $(n \geqslant 2)$	$B_n(q)$ + cyclic groups
C_n $(n \geqslant 3)$	$C_n(q)$ + cyclic groups
D_4	$D_4(q)$ or ${}^2D_4(q^2)$ or ${}^3D_4(q^3)$ + cyclic groups
D_n $(n \geqslant 5)$	$D_n(q)$ or ${}^2D_n(q^2)$ + cyclic groups
E_6	$E_6(q)$ or ${}^2E_6(q^2)$ + cyclic groups
E_7	$E_7(q)$ + cyclic groups
E_8	$E_8(q)$ + cyclic groups
F_4	$F_4(q)$ + cyclic groups
G_2	$G_2(q)$ + cyclic groups

$\bar{\mathbf{G}}(\mathbb{F}_q)$ has only one non-cyclic composition factor, which is either a Chevalley group or a Steinberg group of type $\mathfrak{g}$. For example, the non-cyclic composition factor is $A_n(q)$ or ${}^2A_n(q^2)$ if $\mathfrak{g} = A_n$ and $n \geqslant 2$. For any semisimple algebraic group $\mathbf{H}/F$ and complex semisimple Lie algebra $\mathfrak{h}$, denote by $\mathrm{rk}\,\mathbf{H}$ and $\mathrm{rk}\,\mathfrak{h}$ the rank of $\mathbf{H}/\bar{F}$ and the rank of $\mathfrak{h}$, respectively.

DEFINITION 14. Suppose that $\ell \geqslant 5$ is a prime number and $q = \ell^f$. Let $\bar{\Gamma}$ be a finite simple group of Lie type (of characteristic ℓ) in the above table, and let $\mathfrak{g}$ be the simple Lie type of the corresponding $\bar{\mathbf{G}}$. We define the *$\mathfrak{g}$-type ℓ-rank* of $\bar{\Gamma}$ to be

$$\mathrm{rk}_\ell^{\mathfrak{g}}\,\bar{\Gamma} = \begin{cases} f \cdot \mathrm{rk}\,\mathfrak{g} & \text{if } \bar{\Gamma} \text{ is associated with } \mathfrak{g} \text{ in the above table,} \\ 0 & \text{otherwise.} \end{cases}$$

For a finite simple group $\bar{\Gamma}'$ not in the table, $\mathrm{rk}_\ell^{\mathfrak{g}}\bar{\Gamma}'$ is defined to be 0 for any $\mathfrak{g}$. We extend this definition to arbitrary finite groups by defining the $\mathfrak{g}$-type ℓ-rank of any finite group to be the sum of the $\mathfrak{g}$-type ℓ-ranks of its composition factors. The *total ℓ-rank* of a finite group $\bar{\Gamma}$ is defined to be

$$\mathrm{rk}_\ell\,\bar{\Gamma} := \sum_{\mathfrak{g}} \mathrm{rk}_\ell^{\mathfrak{g}}\,\bar{\Gamma}.$$

Remark 3.3.3. The definition of $\mathfrak{g}$-type ℓ-rank is equivalent to the following. For any finite simple group $\bar{\Gamma}$ of Lie type of characteristic ℓ, we have

$$\bar{\Gamma} = \bar{\mathbf{G}}(\mathbb{F}_{\ell^{f'}})^{\mathrm{der}}$$

for some adjoint simple group $\bar{\mathbf{G}}/\mathbb{F}_{\ell^{f'}}$ so that

$$\bar{\mathbf{G}} \times_{\mathbb{F}_{\ell^{f'}}} \bar{\mathbb{F}}_\ell = \prod^m \bar{\mathbf{H}},$$

where $\bar{\mathbf{H}}$ is an $\bar{\mathbb{F}}_\ell$-adjoint simple group of some Lie type $\mathfrak{h}$. We then set the $\mathfrak{g}$-type ℓ-rank of $\bar{\Gamma}$ to be

$$\mathrm{rk}_\ell^{\mathfrak{g}}\,\bar{\Gamma} := \begin{cases} f' \cdot \mathrm{rk}\,\bar{\mathbf{G}} & \text{if } \mathfrak{g} = \mathfrak{h}, \\ 0 & \text{otherwise.} \end{cases}$$

We extend this definition to arbitrary finite groups by defining the $\mathfrak{g}$-type ℓ-rank of any finite group to be the sum of the $\mathfrak{g}$-type ℓ-ranks of its composition factors.

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

Let $\bar{\mathbf{G}}$ be a connected semisimple algebraic group over $\mathbb{F}_q$ and $\pi : \bar{\mathbf{G}}^{\mathrm{sc}} \to \bar{\mathbf{G}}$ the simply connected cover of $\bar{\mathbf{G}}$. The simply connected $\bar{\mathbf{G}}^{\mathrm{sc}}$ and isogeny π are defined over $\mathbb{F}_q$ (see [Ste68b, 9.16]). The group $\bar{\mathbf{G}}^{\mathrm{sc}}$ is a direct product of $\mathbb{F}_q$-simple, simply connected semisimple groups $\bar{\mathbf{G}}_i^{\mathrm{sc}}$:

$$\bar{\mathbf{G}}_1^{\mathrm{sc}} \times \bar{\mathbf{G}}_2^{\mathrm{sc}} \times \cdots \times \bar{\mathbf{G}}_k^{\mathrm{sc}} \xrightarrow{\mathbb{F}_q \cong} \bar{\mathbf{G}}^{\mathrm{sc}}$$

(see [CF65, ch. 10, § 1.3]). For each $\bar{\mathbf{G}}_i^{\mathrm{sc}}$, there exist an integer m_i and an algebraic group $\bar{\mathbf{H}}_i^{\mathrm{sc}}$ defined over $\mathbb{F}_{q^{m_i}}$ such that $\bar{\mathbf{H}}_i^{\mathrm{sc}} \times_{\mathbb{F}_{q^{m_i}}} \bar{\mathbb{F}}_q$ is almost simple and

$$\bar{\mathbf{G}}_i^{\mathrm{sc}} \times_{\mathbb{F}_q} \mathbb{F}_{q^{m_i}} = \prod^{m_i} \bar{\mathbf{H}}_i^{\mathrm{sc}}.$$

We have that (see [CF65, ch. 10, § 1.3])

$$\bar{\mathbf{G}}_i^{\mathrm{sc}} = \mathrm{Res}_{\mathbb{F}_{q^{m_i}}/\mathbb{F}_q}(\bar{\mathbf{H}}_i^{\mathrm{sc}}),$$

so that

$$\bar{\mathbf{G}}_i^{\mathrm{sc}}(\mathbb{F}_q) = \bar{\mathbf{H}}_i^{\mathrm{sc}}(\mathbb{F}_{q^{m_i}}).$$

The following proposition relates $\mathrm{rk}_\ell^{\mathfrak{g}}\, \bar{\mathbf{G}}(\mathbb{F}_q)$ and $\mathrm{rk}_\ell\, \bar{\mathbf{G}}(\mathbb{F}_q)$ to $\bar{\mathbf{G}} \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$.

Proposition 3.3.4. *Let $\ell \geqslant 5$ be a prime and $\bar{\mathbf{G}}$ a connected semisimple algebraic group over $\mathbb{F}_q$, where $q = \ell^f$. The composition factors of $\bar{\mathbf{G}}(\mathbb{F}_q)$ are cyclic groups and finite simple groups of Lie type of characteristic ℓ. Moreover, if we let m be the number of almost simple factors of $\bar{\mathbf{G}} \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ of simple type $\mathfrak{g}$, then*

$$\mathrm{rk}_\ell^{\mathfrak{g}}\, \bar{\mathbf{G}}(\mathbb{F}_q) = mf \cdot \mathrm{rk}\,\mathfrak{g} \quad \text{and} \quad \mathrm{rk}_\ell\, \bar{\mathbf{G}}(\mathbb{F}_q) = f \cdot \mathrm{rk}\,\bar{\mathbf{G}}.$$

Proof. Since the kernel and cokernel of $\pi : \bar{\mathbf{G}}^{\mathrm{sc}}(\mathbb{F}_q) \to \bar{\mathbf{G}}(\mathbb{F}_q)$ are both abelian [Ste68b, 12.6], the composition factors of $\bar{\mathbf{G}}(\mathbb{F}_q)$ and $\prod_{i=1}^k \bar{\mathbf{H}}_i^{\mathrm{sc}}(\mathbb{F}_{q^{m_i}})$ defined above are identical modulo cyclic groups. Hence, the composition factors of $\bar{\mathbf{G}}(\mathbb{F}_q)$ are cyclic groups and finite simple groups of Lie type of characteristic ℓ by the table. Let

$$\{\bar{\mathbf{H}}_1^{\mathrm{sc}}, \bar{\mathbf{H}}_2^{\mathrm{sc}}, \ldots, \bar{\mathbf{H}}_j^{\mathrm{sc}}\}$$

be the subset of $\{\bar{\mathbf{H}}_1^{\mathrm{sc}}, \ldots, \bar{\mathbf{H}}_k^{\mathrm{sc}}\}$ of type $\mathfrak{g}$. The equation

$$m_1 + m_2 + \cdots + m_j = m$$

follows immediately from the fact that each $\bar{\mathbf{G}}_i^{\mathrm{sc}}$ is a direct product of m_i copies of $\bar{\mathbf{H}}_i^{\mathrm{sc}}$ over $\bar{\mathbb{F}}_q$. Since $\bar{\mathbf{H}}_i^{\mathrm{sc}}$ is almost simple over $\bar{\mathbb{F}}_q$, we obtain by Definition 14 that the $\mathfrak{g}$-type ℓ-rank satisfies

$$\mathrm{rk}_\ell^{\mathfrak{g}}\, \bar{\mathbf{G}}(\mathbb{F}_q) = \sum_{i=1}^k \mathrm{rk}_\ell^{\mathfrak{g}}\, \bar{\mathbf{H}}_i^{\mathrm{sc}}(\mathbb{F}_{q^{m_i}}) = \sum_{i=1}^j m_i f \cdot \mathrm{rk}\,\mathfrak{g} = mf \cdot \mathrm{rk}\,\mathfrak{g},$$

and therefore the total ℓ-rank satisfies

$$\mathrm{rk}_\ell\, \bar{\mathbf{G}}(\mathbb{F}_q) = f \cdot \mathrm{rk}\,\bar{\mathbf{G}}$$

as claimed. ∎

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

We can now prove our main results.

THEOREM A (Main theorem). *Let K be a number field and $\{\phi_\ell : \mathrm{Gal}_K \to \mathrm{GL}_N(\mathbb{F}_\ell)\}_{\ell\in\mathscr{P}}$ a strictly compatible system of* mod ℓ *Galois representations arising from étale cohomology (Definitions 1 and 2). There exists a finite normal extension L of K such that if we denote $\phi_\ell(\mathrm{Gal}_K)$ and $\phi_\ell(\mathrm{Gal}_L)$ by $\bar{\Gamma}_\ell$ and $\bar{\gamma}_\ell$, respectively, for all ℓ and let $\bar{\mathbf{S}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ be the connected $\mathbb{F}_\ell$-semisimple subgroup associated to $\bar{\gamma}_\ell$ (or $\bar{\Gamma}_\ell$) by Nori's theory for $\ell \gg 1$, then the following hold for $\ell \gg 1$.*

(i) *The formal character of $\bar{\mathbf{S}}_\ell \hookrightarrow \mathrm{GL}_{N,\mathbb{F}_\ell}$ is independent of ℓ (Definition $3'$) and is equal to the formal character of $(\mathbf{G}_\ell^\circ)^{\mathrm{der}} \hookrightarrow \mathrm{GL}_{N,\mathbb{Q}_\ell}$, where $(\mathbf{G}_\ell^\circ)^{\mathrm{der}}$ is the derived group of the identity component of $\mathbf{G}_\ell$, the algebraic monodromy group of the semi-simplified representation Φ_ℓ^{ss}.*

(ii) *The composition factors of $\bar{\gamma}_\ell$ and $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ are identical modulo cyclic groups. Therefore, the composition factors of $\bar{\gamma}_\ell$ are finite simple groups of Lie type of characteristic ℓ and are cyclic groups.*

Proof. By Proposition 2.1.2(i), $\bar{\mathbf{S}}_\ell \subset \mathrm{GL}_{N,\mathbb{F}_\ell}$ is a connected $\mathbb{F}_\ell$-semisimple subgroup for $\ell \gg 1$. Statement (i) is proved by Theorem 3.2.1. Since there is a finite normal extension L/K such that $\bar{\gamma}_\ell := \phi_\ell(\mathrm{Gal}_L)$ is a subgroup of $\bar{\mathbf{G}}_\ell(\mathbb{F}_\ell)$ of uniform bounded index (by Theorem 2.0.5) and $\bar{\mathbf{S}}_\ell$ is the derived group of $\bar{\mathbf{G}}_\ell$, the composition factors of $\bar{\gamma}_\ell$ and $\bar{\gamma}_\ell \cap \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ are identical modulo cyclic groups. Together with the $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)/\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)^+$ abelian and normal series

$$\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)^+ = \bar{\gamma}_\ell^+ \triangleleft \bar{\gamma}_\ell \cap \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell) \triangleleft \bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$$

for $\ell \gg 1$ by Theorem 2.1.1 and Remark 2.1.3, we conclude that the composition factors of $\bar{\gamma}_\ell$ and $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ are identical modulo cyclic groups. Since Proposition 3.3.4 implies that the non-cyclic composition factors of $\bar{\mathbf{S}}_\ell(\mathbb{F}_\ell)$ are finite simple groups of Lie type of characteristic ℓ, we obtain statement (ii). □

COROLLARY B. *Let $\bar{\mathbf{S}}_\ell$ be defined as above; then the following hold for $\ell \gg 1$.*

(i) *The total ℓ-rank $\mathrm{rk}_\ell\,\bar{\Gamma}_\ell$ of $\bar{\Gamma}_\ell$ (Definition 14) is equal to the rank of $\bar{\mathbf{S}}_\ell$ and is therefore independent of ℓ.*

(ii) *The A_n-type ℓ-rank $\mathrm{rk}_\ell^{A_n}\,\bar{\Gamma}_\ell$ of $\bar{\Gamma}_\ell$ (Definition 14) for $n \in \mathbb{N}\backslash\{1,2,3,4,5,7,8\}$ and the parity of $(\mathrm{rk}_\ell^{A_4}\,\bar{\Gamma}_\ell)/4$ are independent of ℓ.*

Proof. Since $\bar{\gamma}_\ell$ is a normal subgroup of $\bar{\Gamma}_\ell$ of index bounded by $[L:K]$, they have equal total ℓ-rank and $\mathfrak{g}$-type ℓ-rank for all sufficiently large ℓ. It suffices to prove (i) and (ii) for $\bar{\gamma}_\ell$. Assertion (i) is a direct consequence of Proposition 3.3.4 and Theorem A, and (ii) follows easily from Theorem 3.3.2, Proposition 3.3.4 and Theorem A; so we are done. □

ACKNOWLEDGEMENTS

It is my great pleasure to acknowledge my adviser, Michael Larsen, for useful conversations during the course of this work and for his helpful comments on an earlier preprint. I am also grateful to the anonymous referee for many helpful comments and suggestions, which have greatly improved the exposition of the paper.

References

Car08 X. Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), 629–699.

CF65 J. W. S. Cassels and A. Fröhlich (eds), *Algebraic number theory: Proceedings of an instructional conference organized by the London Mathematical Society (University of Sussex, Brighton, September 1–17)*, second edition (Academic Press, London, 1965).

CR88 C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley Classics Library, reprint of the 1962 original (John Wiley & Sons, New York, 1988).

dJon96 A. J. de Jong, *Smoothness, semi-stability and alterations*, Publ. Math. Inst. Hautes Études Sci. **83** (1996), 51–93.

Del74 P. Deligne, *La conjecture de Weil I*, Publ. Math. Inst. Hautes Études Sci. **43** (1974), 273–307.

DG65 J. Dieudonné and A. Grothendieck, *Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Seconde partie*, Publ. Math. Inst. Hautes Études Sci. **24** (1965), 5–231.

EHK12 J. Ellenberg, C. Hall and E. Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math. J. **161** (2012), 1233–1275.

Fal83 G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

Gab83 O. Gabber, *Sur la torsion dans la cohomologie l-adique d'une variété*, C. R. Acad. Sci. Paris **297** (1983), 179–182.

Hal11 C. Hall, *An open image theorem for a general class of abelian varieties*, Bull. Lond. Math. Soc. **43** (2011), 703–711.

Har77 R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52 (Springer, New York, 1977).

Hui13 C. Y. Hui, *Monodromy of Galois representations and equal-rank subalgebra equivalence*, Math. Res. Lett. **20** (2013), 705–728.

HL14 C. Y. Hui and M. Larsen, *Type A images of Galois representations and maximality*, Preprint (2014), arXiv:1305.1989.

Jor78 C. Jordan, *Mémoire sur les équations differentielles linéaires á intégrale algébrique*, J. Reine Angew. Math. **84** (1878), 89–215.

Lan94 S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, second edition (Springer, New York, 1994).

LW54 S. Lang and A. Wéil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

Mil13 J. S. Milne, *Lectures on étale cohomology* (online course notes), http://www.jmilne.org/math/CourseNotes/LEC.pdf.

Neu99 J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322 (Springer, Berlin, 1999).

Nor87 M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$, Invent. Math. **88** (1987), 257–275.

Ser72 J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

Ser81 J.-P. Serre, Letter to K. A. Ribet, Jan. 1, 1981, reproduced in *Oeuvres - Collected Papers IV*, no. 133 (Springer, 2000).

Ser86 J.-P. Serre, Lettre á Marie-France Vignéras du 10/2/1986, reproduced in *Oeuvres - Collected Papers IV*, no. 137 (Springer, 2000).

Ser94 J.-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, in *Motives (Seattle, WA, 1991)*, Proceedings of Symposia in Pure Mathematics, vol. 55, Part 1 (American Mathematical Society, Providence, RI, 1994), 377–400.

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press

Ser98 J.-P. Serre, *Abelian l-adic representation and elliptic curves*, Research Notes in Mathematics, vol. 7, second edition (A. K. Peters, Wellesley, MA, 1998).

Spr08 T. A. Springer, *Linear algebraic groups*, second edition (Birkhäuser, Boston, 2008).

Ste68a R. Steinberg, *Lectures on Chevalley groups* (Yale University Press, New Haven, CT, 1968).

Ste68b R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. **80** (1968).

Chun Yin Hui chunyin.hui@uni.lu, pslnfq@gmail.com
University of Luxembourg, Mathematics Research Unit,
6 rue Richard Coudenhove-Kalergi, L-1359, Luxembourg

https://doi.org/10.1112/S0010437X14007969 Published online by Cambridge University Press