COMPATIBLE SYSTEMS
OF SYMPLECTIC GALOIS REPRESENTATIONS
AND THE INVERSE GALOIS PROBLEM, II:
TRANSVECTIONS AND HUGE IMAGE

SARA ARIAS-DE-REYNA, LUIS DIEULEFAIT AND GABOR WIESE

COMPATIBLE SYSTEMS
OF SYMPLECTIC GALOIS REPRESENTATIONS
AND THE INVERSE GALOIS PROBLEM, II:
TRANSVECTIONS AND HUGE IMAGE

SARA ARIAS-DE-REYNA, LUIS DIEULEFAIT AND GABOR WIESE

This article is the second part of a series of three articles about compatible systems of symplectic Galois representations and applications to the inverse Galois problem.

This part is concerned with symplectic Galois representations having a huge residual image, by which we mean that a symplectic group of full dimension over the prime field is contained up to conjugation. A key ingredient is a classification of symplectic representations whose image contains a nontrivial transvection: these fall into three very simply describable classes, the reducible ones, the induced ones and those with huge image. Using the idea of an (n, p)-group of Khare, Larsen and Savin, we give simple conditions under which a symplectic Galois representation with coefficients in a finite field has a huge image. Finally, we combine this classification result with the main result of the first part to obtain a strengthened application to the inverse Galois problem.

1. Introduction

This article is the second of a series of three about compatible systems of symplectic Galois representations and applications to the inverse Galois problem.

This part is concerned with symplectic Galois representations having a *huge image*: for a prime ℓ, a finite subgroup $G \subseteq \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$ is called *huge* if it contains a conjugate (in $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$) of $\mathrm{Sp}_n(\mathbb{F}_\ell)$. By Corollary 1.3 below, this notion is the same as the one introduced in Part I [Arias-de-Reyna et al. 2013].

Whereas the classification of the finite subgroups of $\mathrm{Sp}_n(\overline{\mathbb{F}}_\ell)$ appears very complicated to us, it turns out that the finite subgroups containing a nontrivial transvection can be very cleanly classified into three classes, one of which is that of huge subgroups (see Theorem 1.1 below). Translating this group theoretic result into the language of symplectic representations whose image contains a nontrivial

transvection, these also fall into three very simply describable classes: the reducible ones, the induced ones and those with huge image (see Corollary 1.2).

Using the idea of an (n, p)-group of [Khare et al. 2008] (i.e., of a maximally induced place of order p, in the terminology of Part I), some number theory allows us to give very simple conditions under which a symplectic Galois representation with coefficients in $\overline{\mathbb{F}}_\ell$ has huge image (see Theorem 1.5 below).

This second part is independent of the first, except for Corollary 1.6, which combines the main results of Part I [Arias-de-Reyna et al. 2013] and the present Part II. In Part III [Arias-de-Reyna et al. 2015], written in collaboration with Sug Woo Shin, a compatible system satisfying the assumptions of Corollary 1.6 is constructed.

Statement of results. To fix terminology, we recall some standard definitions. Let K be a field. An n-dimensional K-vector space V equipped with a symplectic form (i.e., nonsingular and alternating), denoted by $\langle v, w \rangle = v \bullet w$ for $v, w \in V$, is called a *symplectic K-space*. A K-subspace $W \subseteq V$ is called a *symplectic K-subspace* if the restriction of $\langle \cdot, \cdot \rangle$ to $W \times W$ is nonsingular (hence, symplectic). The *general symplectic group* $\mathrm{GSp}(V, \langle \cdot, \cdot \rangle) =: \mathrm{GSp}(V)$ consists of those $A \in \mathrm{GL}(V)$ such that there is $\alpha \in K^\times$, the *multiplier* (or *similitude factor*) of A, such that we have $(Av) \bullet (Aw) = \alpha(v \bullet w)$ for all $v, w \in V$. The *symplectic group* $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle) =: \mathrm{Sp}(V)$ is the subgroup of $\mathrm{GSp}(V)$ of elements with multiplier 1. An element $\tau \in \mathrm{GL}(V)$ is a *transvection* if $\tau - \mathrm{id}_V$ has rank 1, i.e., if τ fixes a hyperplane pointwisely, and there is a line U such that $\tau(v) - v \in U$ for all $v \in V$. We will consider the identity as a "trivial transvection". Any transvection has determinant and multiplier 1. A *symplectic transvection* is a transvection in $\mathrm{Sp}(V)$. Any symplectic transvection has the form

$$T_v[\lambda] \in \mathrm{Sp}(V) : u \mapsto u + \lambda(u \bullet v)v$$

with *direction vector* $v \in V$ and *parameter* $\lambda \in K$; see, e.g., [Artin 1957, pp. 137–138].

The classification result on subgroups of general symplectic groups containing a nontrivial transvection which plays the key role in our approach is the following.

Theorem 1.1. *Let K be a finite field of characteristic at least 5 and V a symplectic K-vector space of dimension n. Then any subgroup G of $\mathrm{GSp}(V)$ which contains a nontrivial symplectic transvection satisfies one of the following assertions*:

(1) *There is a proper K-subspace $S \subset V$ such that $G(S) = S$.*

(2) *There are mutually orthogonal nonsingular symplectic K-subspaces $S_i \subset V$ with $i = 1, \ldots, h$ of dimension m for some $m < n$ such that $V = \bigoplus_{i=1}^h S_i$ and for all $g \in G$, there is a permutation $\sigma_g \in \mathrm{Sym}_h$ (the symmetric group on $\{1, \ldots, h\}$) with $g(S_i) = S_{\sigma_g(i)}$. Moreover, the action of G on the set $\{S_1, \ldots, S_h\}$ thus defined is transitive.*

(3) *There is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$.*

In Section 2 we show how this theorem can be deduced from results of Kantor [1979]. In a previous version of this article, we gave a self-contained proof, which is still available on arXiv. For our application to Galois representations, we provide the following representation theoretic reformulation of Theorem 1.1.

Corollary 1.2. *Let ℓ be a prime at least 5, let Γ be a compact topological group and*

$$\rho : \Gamma \to \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$$

a continuous representation (for the discrete topology on $\overline{\mathbb{F}}_\ell$). Assume that the image of ρ contains a nontrivial transvection. Then one of the following assertions holds:

(1) *ρ is reducible.*

(2) *There is a closed subgroup $\Gamma' \subsetneq \Gamma$ of finite index $h \mid n$ and a representation $\rho' : \Gamma' \to \mathrm{GSp}_{n/h}(\overline{\mathbb{F}}_\ell)$ such that $\rho \cong \mathrm{Ind}_{\Gamma'}^{\Gamma}(\rho')$.*

(3) *There is a finite field L of characteristic ℓ such that the subgroup generated by the symplectic transvections in the image of ρ is conjugated (in $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$) to $\mathrm{Sp}_n(L)$; in particular, the image is huge.*

The following corollary shows that the definition of a huge subgroup of $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$, which we give in Part I [Arias-de-Reyna et al. 2013], coincides with the simpler definition stated above.

Corollary 1.3. *Let K be a finite field of characteristic $\ell \geq 5$, V a symplectic K-vector space of dimension n, and G a subgroup of $\mathrm{GSp}(V)$ which contains a symplectic transvection. Then the following are equivalent:*

(i) *G is huge.*

(ii) *There is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$.*

Combining the group theoretic results above with (n, p)-groups, introduced by [Khare et al. 2008], some number theory allows us to prove the following theorem. Before stating it, let us collect some notation.

Set-up 1.4. Let n, N be positive integers with n even and $N = N_1 \cdot N_2$ with $\gcd(N_1, N_2) = 1$. Let L_0 be the compositum of all number fields of degree $\leq n/2$, which are ramified at most at the primes dividing N_2 (which is a number field). Let q be a prime which is completely split in L_0, and let p be a prime dividing $q^n - 1$ but not dividing $q^{n/2} - 1$, and $p \equiv 1 \pmod{n}$.

Theorem 1.5. *Assume Set-up 1.4. Let $k \in \mathbb{N}$, $\ell \neq p, q$ be a prime such that $\ell > kn! + 1$ and $\ell \nmid N$. Let $\chi_q : G_{\mathbb{Q}_{q^n}} \to \overline{\mathbb{Q}}_\ell^\times$ be a character satisfying the assumptions of Lemma 3.1, and $\bar{\chi}_q$ the composition of χ_q with the reduction map $\overline{\mathbb{Z}}_\ell \to \overline{\mathbb{F}}_\ell$. Let $\bar{\alpha} : G_{\mathbb{Q}_q} \to \overline{\mathbb{F}}_\ell^\times$ be an unramified character.*

Let

$$\rho : G_{\mathbb{Q}} \to \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$$

be a Galois representation, ramified only at the primes dividing $Nq\ell$, satisfying that a twist by some power of the cyclotomic character is regular in the sense of Definition 3.2 with tame inertia weights at most k, and such that

(1) $\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}}(\rho) = \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\bar{\chi}_q) \otimes \bar{\alpha}$,

(2) *the image of ρ contains a nontrivial transvection and*

(3) *for all primes ℓ_1 dividing N_1, the image under ρ of I_{ℓ_1}, the inertia group at ℓ_1, has order prime to $n!$.*

Then the image of ρ is a huge subgroup of $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$.

Combining Theorem 1.5 with the results of Part I [Arias-de-Reyna et al. 2013] of this series yields the following corollary.

Corollary 1.6. *Assume Set-up 1.4. Let $\rho_\bullet = (\rho_\lambda)_\lambda$ (where λ runs through the finite places of a number field L) be an n-dimensional a. e. absolutely irreducible a. e. symplectic compatible system, as defined in Part I [Arias-de-Reyna et al. 2013], for the base field $\mathbb{Q}$, which satisfies the following assumptions:*

- *For all places λ, the representation ρ_λ is unramified outside $Nq\ell$, where ℓ is the rational prime below λ.*

- *There are $a \in \mathbb{Z}$ and $k \in \mathbb{N}$ such that, for all but possibly finitely many places λ of L, the reduction mod λ of $\chi_\ell^a \otimes \rho_\lambda$ is regular in the sense of Definition 3.2, with tame inertia weights at most k.*

- *The multiplier of the system is a finite order character times a power of the cyclotomic character.*

- *For all primes ℓ not belonging to a density zero set of rational primes, and for each $\lambda \mid \ell$, the residual representation $\bar{\rho}_\lambda$ contains a nontrivial transvection in its image.*

- *For all places λ not above q, one has*

$$\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}}(\rho_\lambda) = \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\chi_q) \otimes \alpha,$$

  where $\alpha : G_{\mathbb{Q}_q} \to \overline{L}_\lambda^\times$ is some unramified character and $\chi_q : G_{\mathbb{Q}_{q^n}} \to \overline{\mathbb{Z}}^\times$ is a character such that its composite with the embedding $\overline{\mathbb{Z}}^\times \hookrightarrow \overline{\mathbb{Q}}_\ell^\times$ given by λ satisfies the assumptions of Lemma 3.1 for all primes $\ell \nmid pq$. In the terminology of Part I, q is called a maximally induced place of order p.

- *For all primes ℓ_1 dividing N_1 and for all but possibly finitely many places λ, the group $\bar{\rho}_\lambda(I_{\ell_1})$ has order prime to $n!$ (where I_{ℓ_1} denotes the inertia group at ℓ_1).*

Then we obtain:

(a) *For all primes ℓ not belonging to a density zero set of rational primes, and for each $\lambda \mid \ell$, the image of the residual representation $\bar{\rho}_\lambda$ is a huge subgroup of $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$.*

(b) *For any $d \mid \frac{p-1}{n}$ there exists a set $\mathcal{L}_d$ of rational primes ℓ of positive density such that for all $\ell \in \mathcal{L}_d$, there is a place λ of L above ℓ satisfying that the image of $\bar{\rho}_\lambda^{\mathrm{proj}}$ is $\mathrm{PGSp}_n(\mathbb{F}_{\ell^d})$ or $\mathrm{PSp}_n(\mathbb{F}_{\ell^d})$.*

The proofs of Theorem 1.5 and Corollary 1.6 are given in Section 3.

Remark 1.7. It is natural to ask which of the two alternatives in Corollary 1.6(b) actually holds. It is very hard to give a general answer. The same indeterminacy occurs in [Khare et al. 2008] (see its arXiv version arXiv:math/0610860v3).

In the very special case, when there is no residual inner twist at a prime λ, the multiplier determines which case one is in. More precisely, by definition there is no residual inner twist at λ if the residue fields modulo λ of $E_{\rho_\bullet}$ (the field of definition of $\rho_\bullet$) and $K_{\rho_\bullet}$ (the projective field of definition of $\rho_\bullet$) coincide (see [Arias-de-Reyna et al. 2013, Section 4]); call it $\mathbb{F}$. In that case, if the image of $\bar{\rho}_\lambda$ is huge, up to conjugation we have $\mathrm{Sp}_n(\mathbb{F}) \subseteq \bar{\rho}_\lambda(G_\mathbb{Q}) \subseteq \mathrm{GSp}_n(\mathbb{F})$ and thus $\mathrm{PSp}_n(\mathbb{F}) \subseteq \bar{\rho}_\lambda^{\mathrm{proj}}(G_\mathbb{Q}) \subseteq \mathrm{PGSp}_n(\mathbb{F})$. The first inclusion is an equality if and only if the multiplier of $\bar{\rho}_\lambda$ is a square in $\mathbb{F}$; otherwise the second inclusion is an equality.

When $n = 2$, in [Dieulefait and Wiese 2011] the difference between the field of definition and the projective one could be controlled due to special choices of modular forms; this allowed distinguishing between the two possibilities and, for every $d \geq 1$, realising the simple group $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$ as a Galois group over $\mathbb{Q}$ for a positive density set of primes ℓ.

If the two residue fields do not coincide, the multiplier is not enough to distinguish between the two cases.

2. Symplectic representations containing a transvection

This section is devoted to Theorem 1.1. This theorem can be deduced from more general results, like those of [Guralnick and Saxl 2003]. We prefer to deduce it from the results of Kantor [1979], together with some representation theory of groups. We hope that the detailed and quite elementary proof we give on page 6 will be of value to the number theory community.

Throughout the section, our setting will be the following: $\ell \geq 5$ denotes a prime number, n an even positive integer and V a symplectic n-dimensional vector space over a finite field K of characteristic ℓ.

Kantor's classification result. Kantor [1979] classifies subgroups of classical linear groups which are generated by a conjugacy class of elements of long root subgroups.

In this paper, we are only concerned with subgroups of the symplectic group $\mathrm{Sp}(V)$. This case is addressed in [Kantor 1979, §11].

We need some notation in order to state his result. First of all, recall that in the symplectic case, the elements of long root subgroups are precisely the symplectic transvections. Given a subgroup $H \subseteq \mathrm{Sp}(V)$, denote by $O_\ell(H)$ the maximal normal ℓ-subgroup contained in H, denote by $[H, H]$ the commutator subgroup of H, and by $Z_{\mathrm{Sp}(V)}(H)$ the centraliser of H in $\mathrm{Sp}(V)$. Below we state the result of Kantor in the symplectic case (leaving aside the cases of characteristic 2 and 3).

Theorem 2.1 (Kantor). *Assume that $\ell \geq 5$, and let $H \subseteq \mathrm{Sp}(V)$ be a subgroup satisfying the following conditions:*

(1) *There exists a set $\mathfrak{X} \subseteq H$ consisting of transvections, closed under conjugation in H, which generates H.*

(2) *$O_\ell(H) \leq [H, H] \cap Z_{\mathrm{Sp}(V)}(H)$.*

(3) *H does not preserve any nonsingular subspace of V.*

Then there is a subfield L of K such that H is conjugated (in $\mathrm{Sp}(V)$) to $\mathrm{Sp}_n(L)$.

We will apply this result in the case when H is an irreducible subgroup. In this case, conditions (2) and (3) are satisfied. We elaborate on condition (2). Let $W \subseteq V$ be the subspace of elements that are left invariant by all elements in $O_\ell(H)$. Since $O_\ell(H)$ is an ℓ-group acting on a finite ℓ-group V, the cardinality of W is divisible by ℓ (see Lemma 1 of Chapter IX of [Serre 1979]); hence $W \neq \{0\}$. Moreover, since $O_\ell(H)$ is a normal subgroup of H, it follows that H stabilises W. But H is an irreducible group; hence $W = V$ and $O_\ell(H) = \{\mathrm{Id}\}$. Furthermore, if we take into account that the conjugate of a transvection is again a transvection, we can reformulate condition (1) as follows: "the transvections contained in H generate H", or simply "H is generated by transvections". This discussion proves the following corollary.

Corollary 2.2. *Assume that $\ell \geq 5$, and let $H \subseteq \mathrm{Sp}(V)$ be an irreducible subgroup which is generated by transvections. Then there is a subfield L of K such that H is conjugated (in $\mathrm{Sp}(V)$) to $\mathrm{Sp}_n(L)$.*

Proof of the group theoretic results. We will make use of the following facts about transvections, the simple proofs of which are omitted.

Lemma 2.3. *Let $T_u[\lambda] \in \mathrm{Sp}(V)$ be a symplectic transvection. Then*

(a) *For any $A \in \mathrm{GSp}(V)$ with multiplier $\alpha \in K^\times$, we have $A T_u[\lambda] A^{-1} = T_{Au}\left[\frac{\lambda}{\alpha}\right]$.*

(b) *Suppose $W \subseteq V$ is a K-vector subspace stabilised by $T_u[\lambda]$ with $\lambda \in K^\times$. Then we have*

(1) *$u \in W$ or $u \in W^\perp$;*

(2) *$u \in W^\perp \Leftrightarrow T_u[\lambda]|_W = \mathrm{id}_W$.*

Proof of Theorem 1.1. Let $G \subseteq \mathrm{GSp}(V)$ be a subgroup which contains a nontrivial transvection. If the action of G on V is reducible, we are in case (1) of the theorem. Assume that the action of G on V is irreducible, and define the subgroup $H := \langle \tau \in G : \tau$ is a transvection$\rangle$. Note that H is nontrivial. If the action of H on V is irreducible, we can apply Corollary 2.2 to the group H and conclude that H is conjugate in $\mathrm{GSp}(V)$ to $\mathrm{Sp}_n(L)$ for some subfield $L \subseteq K$. This is case (3) of the theorem.

Assume then that the action of H on V is reducible. Let $W \subset V$ be a K-vector subspace on which H acts irreducibly. By Lemma 2.3(a), the group H is a normal subgroup of G. Thus we can apply Clifford's theorem (see [Curtis and Reiner 1981, (11.1)]), to obtain $g_1, \ldots, g_r \in G$ such that we have the equality of H-modules

$$(2\text{-}1) \qquad\qquad V = \bigoplus_{i=1}^r g_i W.$$

We first remark that W is not the trivial H-module, as otherwise H would act trivially on V and thus H would be the trivial group. Now consider $W' = \langle u \in W : \exists \lambda \in K^\times : T_u[\lambda] \in H \rangle$. As W is a nontrivial H-module, $W' \neq 0$. Let $T_v[\mu] \in H$ and $u \in W'$. By Lemma 2.3(b), $v \in W'$ or $v \in W^\perp$. In both cases, we have $T_v[\mu](u) = u + \mu(u \bullet v)v \in W'$, showing that H preserves W', so that the irreducibility of W implies $W' = W$.

Let $\widetilde{W} = gW$ be a conjugate of W for which we assume $\widetilde{W} \neq W$, so that $\widetilde{W} \cap W = 0$ since W is irreducible. We have just seen that there are $w_1, \ldots, w_m \in W$ spanning W and $\lambda_1, \ldots, \lambda_m \in K^\times$ such that $T_{w_1}[\lambda_1], \ldots, T_{w_m}[\lambda_m] \in H$. As H also preserves $\widetilde{W}$, Lemma 2.3(b) shows $w_i \in \widetilde{W}^\perp$ for $1 \leq i \leq m$. This proves two things. Firstly, $W \subseteq \widetilde{W}^\perp$ and this means that the decomposition (2-1) of V is into mutually orthogonal spaces. From this it follows these subspaces are also symplectic, i.e., that the pairing is nondegenerate on each subspace. Secondly, $T_{w_1}[\lambda_1]$ is the identity on $\widetilde{W}$, but it is nontrivial on W (e.g., by the nondegeneration of W, there is $u \in W$ such that $u \bullet w_1 \neq 0$, whence $T_{w_1}[\lambda_1](u) \neq u$). Hence, W and $\widetilde{W}$ are nonisomorphic as H-modules.

Considering the composite maps $gW \hookrightarrow V \xrightarrow{\text{projection}} g_i W$, in view of the irreducibility of the $g_i W$ and the fact that $g_i W \not\cong g_j W$ for $i \neq j$, it follows that gW is one of the $g_i W$. Thus, G acts on the set $\{g_1 W, \ldots, g_r W\}$. If this action were not transitive, then the sum of the spaces in one orbit would be a proper nontrivial G-submodule of V, contradicting the irreducibility of V. Thus, all statements of case (2) of the theorem are proved. $\square$

Proof of Corollary 1.2. Since Γ is compact and the topology on $\overline{\mathbb{F}}_\ell$ is discrete, the image of ρ is a subgroup of $\mathrm{GSp}_n(K)$ for a certain finite field K of characteristic ℓ. Therefore one of the three possibilities of Theorem 1.1 holds for $G := \mathrm{im}(\rho)$. If the first holds, then ρ is reducible, and if the third holds, then $\mathrm{im}(\rho)$ contains a group conjugate to $\mathrm{Sp}_n(L)$ for some subfield L of K.

Assume now that the second possibility holds. We use notation as in Theorem 1.1. Let Γ' be $\{g \in \Gamma \mid \sigma_g(1) = 1\}$, the stabiliser of the first subspace. This is a closed subgroup of Γ of finite index. Choose coset representatives and write $\Gamma = \bigsqcup_{i=1}^{h'} g_i \Gamma'$. The set $\{\gamma S_1 \mid \gamma \in \Gamma\}$ contains h' elements, namely precisely the $g_i S_1$ for $i = 1, \ldots, h'$. As the action of G on the decomposition is transitive, this set is precisely $\{S_1, \ldots, S_h\}$, whence $h = h'$. Define ρ' as the restriction of ρ to Γ' acting on S_1. Then as a Γ'-representation, we have the isomorphism

$$V \cong \bigoplus_{i=1}^{h} S_i \cong \bigoplus_{i=1}^{h} g_i S_1.$$

Proposition (10.5) of §10A of [Curtis and Reiner 1981] implies $\rho = \mathrm{Ind}_{\Gamma'}^{\Gamma}(\rho')$. $\square$

Proof of Corollary 1.3. Assume that G contains a subgroup conjugate (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(\mathbb{F}_\ell)$. In particular, G does not fix any proper subspace $S \subset V$, nor any decomposition $V = \bigoplus_{i=1}^{h} S_i$ into mutually orthogonal nonsingular symplectic subspaces. Hence by Theorem 1.1, there is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$. The other implication is clear. $\square$

3. Symplectic representations with huge image

In this section we establish Theorem 1.5.

(n, p)-groups. As a generalisation of dihedral groups, in [Khare et al. 2008], Khare, Larsen and Savin introduce so-called (n, p)-groups. We briefly recall some facts and some notation to be used. For the definition of (n, p)-groups, we refer to [loc. cit.]. Let q be a prime number, and let $\mathbb{Q}_{q^n}/\mathbb{Q}_q$ be the unique unramified extension of $\mathbb{Q}_q$ of degree n (inside a fixed algebraic closure $\overline{\mathbb{Q}}_q$). Assume p is a prime such that the order of q modulo p is n. Recall that $\mathbb{Q}_{q^n}^{\times} \simeq \mu_{q^n-1} \times U_1 \times q^{\mathbb{Z}}$, where μ_{q^n-1} is the group of (q^n-1)-th roots of unity and U_1 the group of 1-units. Let ℓ be a prime distinct from p and q. Assuming that $p, q > n$, in [loc. cit.], the authors construct a character $\chi_q : \mathbb{Q}_{q^n}^{\times} \to \overline{\mathbb{Q}}_\ell^{\times}$ that satisfies the three properties of the following lemma, which is proved in [loc. cit., Section 3.1].

Lemma 3.1. *Let $\chi_q : \mathbb{Q}_{q^n}^{\times} \to \overline{\mathbb{Q}}_\ell^{\times}$ be a character satisfying*:

- *χ_q has order $2p$.*
- *$\chi_q|_{\mu_{q^n-1} \times U_1}$ has order p.*
- *$\chi_q(q) = -1$.*

This character gives rise to a character (which by abuse of notation we call also χ_q) of $G_{\mathbb{Q}_{q^n}}$ by means of the reciprocity map of local class field theory.

Let

$$\rho_q = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\chi_q).$$

Then ρ_q is irreducible and symplectic, in the sense that it can be conjugated to take values in $\mathrm{Sp}_n(\overline{\mathbb{Q}}_\ell)$, and the image of the reduction $\bar\rho_q$ of ρ_q in $\mathrm{Sp}_n(\overline{\mathbb{F}}_\ell)$ is an (n, p)-group. Moreover, if $\bar\alpha : G_{\mathbb{Q}_q} \to \overline{\mathbb{F}}_\ell^\times$ is an unramified character, then $\bar\rho_q \otimes \bar\alpha$ is also irreducible.

Note that also the reduction of ρ_q is $\mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\bar\chi_q)$, which is an irreducible representation. Here $\bar\chi_q$ is the composite of χ_q and the projection $\overline{\mathbb{Z}}_\ell \twoheadrightarrow \overline{\mathbb{F}}_\ell$. To see why the last assertion is true, note that to see that

$$\bar\rho_q \otimes \bar\alpha = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\bar\chi_q \otimes (\bar\alpha|_{G_{\mathbb{Q}_{q^n}}}))$$

is irreducible, it suffices to prove that the n characters

$$\bar\chi_q \otimes (\bar\alpha|_{G_{\mathbb{Q}_{q^n}}}), (\bar\chi_q \otimes (\bar\alpha|_{G_{\mathbb{Q}_{q^n}}}))^q, \ldots, (\bar\chi_q \otimes (\bar\alpha|_{G_{\mathbb{Q}_{q^n}}}))^{q^{n-1}}$$

are different (see [Serre 1977, Proposition 23, Chapter 7]). But the order of the restriction of $\bar\chi_q \otimes (\bar\alpha|_{G_{\mathbb{Q}_{q^n}}})$ to the inertia group at q is p (since $\bar\alpha$ is unramified), and the order of q mod p is n.

Regular Galois representations. In our result we assume that our representation ρ is regular, which is a condition on the tame inertia weights of ρ.

Definition 3.2 (regularity). Let ℓ be a prime number, n a natural number, V an n-dimensional vector space over $\overline{\mathbb{F}}_\ell$ and $\rho : G_{\mathbb{Q}_\ell} \to \mathrm{GL}(V)$ a Galois representation, and denote by I_ℓ the inertia group at ℓ. We say that ρ is *regular* if there exists an integer s between 1 and n, and for each $i = 1, \ldots, s$, a set S_i of natural numbers in $\{0, 1, \ldots, \ell-1\}$, of cardinality r_i, with $r_1 + \cdots + r_s = n$, say $S_i = \{a_{i,1}, \ldots, a_{i,r_i}\}$, such that the cardinality of $S = S_1 \cup \cdots \cup S_s$ equals n (i.e., all the $a_{i,j}$ are distinct) and such that, if we denote by B_i the matrix

$$B_i \sim \begin{pmatrix} \psi_{r_i}^{b_i} & & & 0 \\ & \psi_{r_i}^{b_i \ell} & & \\ & & \ddots & \\ 0 & & & \psi_{r_i}^{b_i \ell^{r_i-1}} \end{pmatrix}$$

with ψ_{r_i} our fixed choice of fundamental character of niveau r_i and $b_i = a_{i,1} + a_{i,2}\ell + \cdots + a_{i,r_i}\ell^{r_i-1}$, then

$$\rho|_{I_\ell} \sim \begin{pmatrix} \boxed{B_1} & & * \\ & \ddots & \\ 0 & & \boxed{B_s} \end{pmatrix}.$$

The elements of S are called *tame inertia weights* of ρ. We will say that ρ has *tame inertia weights at most k* if $S \subseteq \{0, 1, \ldots, k\}$. We will say that a global representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ is *regular* if $\rho|_{G_{\mathbb{Q}_\ell}}$ is regular.

Lemma 3.3. *Let $\rho : G_{\mathbb{Q}_\ell} \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ be a Galois representation which is regular with tame inertia weights at most k. Assume that $\ell > k\, n! + 1$. Then all the $n!$-th powers of the characters on the diagonal of $\rho|_{I_\ell}$ are distinct.*

Proof. We use the notation of Definition 3.2. Assume we have that the $n!$-th powers of two characters of the diagonal coincide, say

$$(3\text{-}1) \qquad \psi_{r_i}^{n!(c_0+c_1\ell+\cdots+c_{r_i-1}\ell^{r_i-1})} = \psi_{r_j}^{n!(d_0+d_1\ell+\cdots+d_{r_j-1}\ell^{r_j-1})},$$

where $c_0, \ldots, c_{r_i-1}, d_0, \ldots, d_{r_j-1}$ are distinct elements of $S_1 \cup \cdots \cup S_s$.

Let $\psi_{r_i r_j}$ be a fundamental character of niveau $r_i r_j$ such that

$$\psi_{r_i r_j}^{\Phi_i^{(i,j)}} = \psi_{r_i} \quad \text{and} \quad \psi_{r_i r_j}^{\Phi_j^{(i,j)}} = \psi_{r_j},$$

where

$$\Phi_i^{(i,j)} = \frac{\ell^{r_i r_j} - 1}{\ell^{r_i} - 1} \quad \text{and} \quad \Phi_j^{(i,j)} = \frac{\ell^{r_i r_j} - 1}{\ell^{r_j} - 1}.$$

We can write (3-1) above as

$$\psi_{r_i r_j}^{\Phi_i^{(i,j)} n!(c_0+c_1\ell+\cdots+c_{r_i-1}\ell^{r_i-1})} = \psi_{r_i r_j}^{\Phi_j^{(i,j)} n!(d_0+d_1\ell+\cdots+d_{r_j-1}\ell^{r_j-1})}.$$

In other words, $\ell^{r_i r_j} - 1$ divides the quantity

$$C_0 = \left| \Phi_i^{(i,j)} n!(c_0+c_1\ell+\cdots+c_{r_i-1}\ell^{r_i-1}) - \Phi_j^{(i,j)} n!(d_0+d_1\ell+\cdots+d_{r_j-1}\ell^{r_j-1}) \right|.$$

Note that C_0 is nonzero because modulo ℓ it is congruent to $n!(c_0 - d_0)$, and by assumption all elements in $S_1 \cup \cdots \cup S_s$ are in different congruence classes modulo ℓ. But $|c_0 + c_1\ell + \cdots + c_{r_i-1}\ell^{r_i-1}| \le k(1 + \ell + \cdots + \ell^{r_i-1}) = k(\ell^{r_i} - 1)/(\ell - 1)$. Analogously $|d_0 + d_1\ell + \cdots + d_{r_j-1}\ell^{r_j-1}| < k(\ell^{r_j} - 1)/(\ell - 1)$. Thus C_0 is bounded above by

$$\max\left\{ \left| \Phi_i^{(i,j)} n!(c_0+c_1\ell+\cdots+c_{r_i-1}\ell^{r_i-1}) \right|, \left| \Phi_j^{(i,j)} n!(d_0+d_1\ell+\cdots+d_{r_j-1}\ell^{r_j-1}) \right| \right\}$$

$$\le n!k\left(\frac{\ell^{r_i r_j} - 1}{\ell - 1} \right) < n!k(\ell^{r_i r_j-1} + 2\ell^{r_i r_j-2}).$$

Since $\ell - 2 \ge n!k$, we have $\ell^2 - 1 > \ell^2 - 4 \ge n!k(\ell + 2)$ and thus

$$C_0 < n!k(\ell^{r_i r_j-1} + 2\ell^{r_i r_j-2}) = n!k(\ell + 2)\ell^{r_i r_j-2} < \ell^{r_i r_j} - 1.$$

Hence $\ell^{r_i r_j} - 1$ cannot divide C_0. $\qquad\qquad\square$

We will now use these lemmas to study the ramification at ℓ of an induced representation under the assumption of regularity (possibly after a twist by a power of the cyclotomic character) and boundedness of tame inertia weights.

Proposition 3.4. *Let $n, m, k \in \mathbb{N}$, $a \in \mathbb{Z}$ and let $\ell > k\,n! + 1$ be a prime, $K/\mathbb{Q}$ a finite extension such that $[K : \mathbb{Q}] \cdot m = n$, $\rho : G_K \to \mathrm{GL}_m(\overline{\mathbb{F}}_\ell)$ a Galois representation and let $\beta = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho$. If $\chi_\ell^a \otimes \beta$ is regular with tame inertia weights at most k, then $K/\mathbb{Q}$ does not ramify at ℓ.*

Proof. Assume that $K/\mathbb{Q}$ ramifies at ℓ; we will derive a contradiction. First of all, let us fix some notation: let $N/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$, and let us fix a prime λ of N above ℓ. Denote by $I_\ell \subset G_\mathbb{Q}$ the inertia group at ℓ, $I_{\ell,\mathrm{w}} \subset I_\ell$ the wild inertia group at ℓ and $I_N \subset G_N$ the inertia group at the prime λ. Let W be the $\overline{\mathbb{F}}_\ell$-vector space underlying ρ. For each $\gamma \in G_\mathbb{Q}$, let ${}^\gamma K = \gamma(K)$ and define ${}^\gamma \rho : G_{{}^\gamma K} \to \mathrm{GL}(W)$ by ${}^\gamma \rho(\sigma) = \rho(\gamma \sigma \gamma^{-1})$.

Let us now pick any $\gamma \in G_\mathbb{Q}$, $\sigma \in I_\ell$ and $\tau \in I_N$. Since $I_\ell/I_{\ell,\mathrm{w}}$ is cyclic, we have that the commutator $\sigma^{-1}\tau\sigma\tau^{-1}$ belongs to $I_{\ell,\mathrm{w}}$. Since $I_N \subset I_\ell$ is normal, $\sigma^{-1}\tau\sigma \in I_N \subset G_N \subset G_{{}^\gamma K}$, so we may apply ${}^\gamma \rho$ and conclude

$$
{}^\gamma\rho(\sigma^{-1}\tau\sigma){}^\gamma\rho(\tau^{-1}) = {}^\gamma\rho(\sigma^{-1}\tau\sigma\tau^{-1}) \in {}^\gamma\rho(I_{\ell,\mathrm{w}});
$$

hence ${}^\gamma\rho(\sigma^{-1}\tau\sigma)$ and ${}^\gamma\rho(\tau)$ have exactly the same eigenvalues.

Since $N/\mathbb{Q}$ ramifies in ℓ, we may pick $\sigma \in I_\ell \setminus G_N$, and since $N = \prod_{\gamma \in G_\mathbb{Q}} {}^\gamma K$, there exists some $\gamma \in G_\mathbb{Q}$ such that $\sigma \notin G_{{}^\gamma K}$. This implies that $\beta(\sigma\gamma)(W) \cap \beta(\gamma)(W) = 0$. Choose now a set of left-coset representatives $\{\gamma_1 G_K, \dots, \gamma_d G_K\}$ of G_K in $G_\mathbb{Q}$ with $\gamma_1 = \gamma$ and $\gamma_2 = \sigma\gamma$; Mackey's formula [Curtis and Reiner 1981, 10.13] implies that

$$
\mathrm{Res}_{G_N}^{G_\mathbb{Q}} \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho = \bigoplus_{i=1}^{d} \mathrm{Res}_{G_N}^{G_{\gamma_i K}} {}^{\gamma_i}\rho.
$$

Therefore $\beta(\tau)$ is a block-diagonal matrix, where one block is ${}^\gamma\rho(\tau)$ and another block is ${}^{\sigma\gamma}\rho(\tau) = {}^\gamma\rho(\sigma^{-1}\tau\sigma)$. But, by hypothesis, the tame inertia weights of $\chi_\ell^a \otimes \beta$ are bounded. By Lemma 3.3, we have that the $n!$-powers of the characters on the diagonal of $\chi_\ell^a \otimes \beta|_{I_\ell}$ are all different, which implies that the characters on the diagonal of $\beta|_{I_N}$ are all different. Thus ${}^\gamma\rho(\tau)$ and ${}^\gamma\rho(\sigma^{-1}\tau\sigma)$ cannot have the same eigenvalues for all $\tau \in I_N$. $\qquad\square$

Representations induced in two ways. We need a proposition concerning representations induced from different subgroups of a certain group G.

Proposition 3.5. *Let G be a finite group, $N \trianglelefteq G$, $H \leq G$. Assume $(G : N) = n$, and let $p > n$ be a prime. Let K be a field of characteristic coprime to $|G|$ containing all $|G|$-th roots of unity. Let S be a $K[H]$-module, $\chi : N \to K^\times$ a character, say $\chi = \chi_1 \otimes \chi_2$, where $\chi_1 : N \to K^\times$ (resp. $\chi_2 : N \to K^\times$) has order equal to a nontrivial power of p (resp. not divisible by p). Assume*

$$
\rho := \mathrm{Ind}_H^G(S) = \mathrm{Ind}_N^G(\chi),
$$

and furthermore the n characters $\{\chi_1^\sigma : \sigma \in G/N\}$ are different. Then $N \leq H$.

Following [Serre 1977, 7.2], if G is a finite group and we are given two G-modules V_1 and V_2, we will define $\langle V_1, V_2 \rangle_G := \dim \operatorname{Hom}_G(V_1, V_2)$. It is known (Lemma 2 of Chapter 7 of [loc. cit.]) that, if φ_1 and φ_2 are the characters of V_1 and V_2, then

$$\langle V_1, V_2 \rangle_G = \langle \varphi_1, \varphi_2 \rangle_G := \frac{1}{|G|} \sum_{g \in G} \varphi_1(g^{-1}) \varphi_2(g).$$

Before giving the proof, we will first prove a lemma.

Lemma 3.6. *Let G be a group, $N \trianglelefteq G$ and $H \leq G$ such that $(G : H) \leq n$. Let p be a prime such that $p > n$, let K be a field of characteristic coprime to $|G|$ containing all $|G|$-th roots of unity, and let $\chi : N \to K^\times$ be a character whose order is a nontrivial power of p. Then $\operatorname{Res}_{H \cap N}^N \chi$ is not trivial.*

Proof. Assume $\operatorname{Res}_{H \cap N}^N \chi$ is trivial. Then $H \cap N \leq \ker \chi$. But $\ker \chi \leq N$, and the index $(N : \ker \chi)$ is at least p. Therefore $(N : H \cap N) \geq p$. But on the other hand $p > n \geq (G : H) \geq (HN : H) = (N : N \cap H)$, a contradiction. □

Proof of Proposition 3.5. Observe that ρ is irreducible. Namely, there is a well-known criterion characterising when an induced representation is irreducible (see [Serre 1977, Proposition 23, Chapter 7]). In particular, since N is normal in G, we have that $\operatorname{Ind}_N^G \chi$ is irreducible if and only if χ is irreducible (which clearly holds) and, for all $g \in G/N$, $(\operatorname{Res}_N^G(\chi))^h$ is not isomorphic to $\operatorname{Res}_N^G(\chi)$. This last condition holds because the n characters $\{\chi_1^\sigma : \sigma \in G/N\}$ are different, and χ_2 has order prime to p.

Since ρ is irreducible, we have that

$$1 = \langle \rho, \rho \rangle_G = \langle \operatorname{Ind}_H^G(S), \operatorname{Ind}_N^G(\chi) \rangle_G = \langle S, \operatorname{Res}_H^G \operatorname{Ind}_N^G(\chi) \rangle_H = \cdots,$$

where in the last step we used Frobenius reciprocity. Now we apply Mackey's formula [Curtis and Reiner 1981, 10.13] on the right-hand side; note that, since N is normal, $H \backslash G / N \simeq G / (H \cdot N)$:

$$\cdots = \left\langle S, \bigoplus_{\gamma \in G/(H \cdot N)} \operatorname{Ind}_{H \cap N}^H \operatorname{Res}_{H \cap N}^N (\chi^\gamma) \right\rangle_H$$

$$= \sum_{\gamma \in G/(H \cdot N)} \left\langle S, \operatorname{Ind}_{H \cap N}^H \operatorname{Res}_{H \cap N}^N (\chi^\gamma) \right\rangle_H.$$

Hence there is a unique $\gamma \in G/(H \cdot N)$ such that

$$\langle S, \operatorname{Ind}_{H \cap N}^H \operatorname{Res}_{H \cap N}^N (\chi^\gamma) \rangle_H = 1.$$

If we prove that, for all γ, $\operatorname{Ind}_{H \cap N}^H \operatorname{Res}_{H \cap N}^N (\chi^\gamma)$ is irreducible, then we will have

$$S \simeq \operatorname{Ind}_{H \cap N}^H \operatorname{Res}_{H \cap N}^N (\chi^\gamma)$$

(for some γ); hence $\dim(S) = (H : H \cap N)$. But, on the other hand, since $\rho = \mathrm{Ind}_H^G(S) = \mathrm{Ind}_N^G(\chi)$, we have that $\dim(S) \cdot (G : H) = (G : N)$, so

$$\dim(S) = \frac{(G : HN)(HN : N)}{(G : HN)(HN : H)} = \frac{(H : N \cap H)}{(N : N \cap H)},$$

and therefore the conclusion is that $(N : N \cap H) = 1$; in other words, $N \leq H$.

Therefore to conclude, we only need to see that $\mathrm{Ind}_{H \cap N}^H \mathrm{Res}_{H \cap N}^N(\chi^\gamma)$ is irreducible. Since conjugation by γ plays no role here, let us just assume $\gamma = 1$. We apply again the criterion characterising when an induced representation is irreducible. In particular, since $H \cap N$ is normal in H, we have that $\mathrm{Ind}_{H \cap N}^H \mathrm{Res}_{H \cap N}^N(\chi)$ is irreducible if and only if $\mathrm{Res}_{H \cap N}^N(\chi)$ is irreducible (which clearly holds) and, for all $h \in H/N \cap H$, $(\mathrm{Res}_{H \cap N}^N(\chi))^h$ is not isomorphic to $\mathrm{Res}_{H \cap N}^N(\chi)$.

So pick $h \in H \setminus N$. We have

$$(\mathrm{Res}_{H \cap N}^N(\chi))^h = \mathrm{Res}_{H \cap N}^N(\chi^h).$$

Assume $\mathrm{Res}_{H \cap N}^N(\chi^h) = \mathrm{Res}_{H \cap N}^N(\chi)$. In particular, we obtain $\mathrm{Res}_{H \cap N}^N(\chi_1^h) = \mathrm{Res}_{H \cap N}^N(\chi_1)$. By Lemma 3.6, we have $\chi_1 = \chi_1^h$ as characters of N. But for all $\sigma \in G/N$, we know that $\chi_1^\sigma \neq \chi_1$. Now it suffices to note that $H/(H \cap N) \hookrightarrow G/N$. $\square$

Proofs. Finally we carry out the proof of Theorem 1.5.

Lemma 3.7. *Assume Set-up 1.4. Let $k \in \mathbb{N}$, $\ell \neq p, q$ be a prime such that $\ell > k\,n! + 1$ and $\ell \nmid N$. Let $\chi_q : G_{\mathbb{Q}_{q^n}} \to \overline{\mathbb{Q}}_\ell^\times$ be a character satisfying the assumptions of Lemma 3.1, and $\bar{\chi}_q$ the composition of χ_q with the reduction map $\overline{\mathbb{Z}}_\ell \to \overline{\mathbb{F}}_\ell$. Let $\bar{\alpha} : G_{\mathbb{Q}_q} \to \overline{\mathbb{F}}_\ell^\times$ be an unramified character.*

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$ be a Galois representation, ramified only at the primes dividing $Nq\ell$, such that a twist by some power of the cyclotomic character is regular in the sense of Definition 3.2 with tame inertia weights at most k, and satisfying (1) and (3) of Theorem 1.5. Then ρ is not induced from a representation of an open subgroup $H \subsetneq G_{\mathbb{Q}}$.

Proof. Let $H \subset G_{\mathbb{Q}}$ be an open subgroup, say of index h, and $\rho' : H \to \mathrm{GL}_{n/h}(\overline{\mathbb{F}}_\ell)$ a representation such that

$$\rho \cong \mathrm{Ind}_H^{G_{\mathbb{Q}}}(\rho').$$

Call S_1 and V, with $S_1 \subseteq V$, the spaces underlying ρ' and ρ, respectively, so that $\rho = \mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1)$. Recall that by assumption

$$\mathrm{Res}_{G_{\mathbb{Q}_q}}^{G_{\mathbb{Q}}}(\rho) = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\bar{\chi}_q) \otimes \bar{\alpha}.$$

We want to compute $\mathrm{Res}_{G_{\mathbb{Q}_q}}^{G_{\mathbb{Q}}} \mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1)$. Let us apply Mackey's formula [Curtis and Reiner 1981, 10.13]. By Lemma 3.1 we know that

$$\mathrm{Res}_{G_{\mathbb{Q}_q}}^{G_{\mathbb{Q}}} \mathrm{Ind}_H^{G_{\mathbb{Q}}}(S_1) = \mathrm{Ind}_{G_{\mathbb{Q}_{q^n}}}^{G_{\mathbb{Q}_q}}(\bar{\chi}_q) \otimes \bar{\alpha}$$

is irreducible, so there can only be one summand in the formula; hence

$$\operatorname{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}} \operatorname{Ind}^{G_{\mathbb{Q}}}_{H}(S_1) = \operatorname{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_q} \cap H} \operatorname{Res}^{H}_{G_{\mathbb{Q}_q} \cap H}(S_1),$$

and therefore

$$(3\text{-}2) \qquad \operatorname{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_q} \cap H} \operatorname{Res}^{H}_{G_{\mathbb{Q}_q} \cap H}(S_1) = \operatorname{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\bar{\chi}_q) \otimes \bar{\alpha}.$$

We now apply Proposition 3.5 to (3-2). Note that

$$\operatorname{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_q}} \rho = \operatorname{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\bar{\chi}_q) \otimes \bar{\alpha} = \operatorname{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^n}}}(\bar{\chi}_q \otimes (\bar{\alpha}|_{G_{\mathbb{Q}_{q^n}}})).$$

We can write $\bar{\chi}_q \otimes (\bar{\alpha}|_{G_{\mathbb{Q}_{q^n}}}) = \bar{\chi}_1 \otimes \bar{\chi}_2$, where $\bar{\chi}_1$ has order a power of p and $\bar{\chi}_2$ has order prime to p. Note that the restriction of $\bar{\chi}_q \otimes (\bar{\alpha}|_{G_{\mathbb{Q}_{q^n}}})$ to the inertia group I_q of $G_{\mathbb{Q}_q}$ coincides with the restriction of $\bar{\chi}_q$, which has order p. Thus $(\bar{\chi}_1 \otimes \bar{\chi}_2)|_{I_q} = \bar{\chi}_q|_{I_q} = \bar{\chi}_1|_{I_q}$. Since the order of q mod p is n, we know that the n characters $\bar{\chi}_1|_{I_q}, \bar{\chi}_1^q|_{I_q}, \ldots, \bar{\chi}_1^{q^n}|_{I_q}$ are distinct. We can take $G = \rho(G_{\mathbb{Q}_q})$ in the statement of Proposition 3.5, whose order is a divisor of $2np \cdot \operatorname{ord}(\bar{\alpha})$ and, hence, prime to ℓ. It thus follows that $G_{\mathbb{Q}_{q^n}} \leq (G_{\mathbb{Q}_q} \cap H)$.

Note that, on the one hand

$$n = \dim V = \dim(\operatorname{Ind}^{G_{\mathbb{Q}}}_{H} S_1) = (G_{\mathbb{Q}} : H) \dim(S_1).$$

On the other hand,

$$n = \dim(\operatorname{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_q} \cap H} \operatorname{Res}^{H}_{G_{\mathbb{Q}_q} \cap H}(S_1)) = (G_{\mathbb{Q}_q} : G_{\mathbb{Q}_q} \cap H) \dim(S_1);$$

hence $(G_{\mathbb{Q}} : H) = (G_{\mathbb{Q}_q} : G_{\mathbb{Q}_q} \cap H)$.

Let L be the number field such that $H = \operatorname{Gal}(\bar{\mathbb{Q}}/L)$. Now $\operatorname{Gal}(\bar{\mathbb{Q}}/L) \cap G_{\mathbb{Q}_q} = \operatorname{Gal}(\bar{\mathbb{Q}}_q/L_{\mathfrak{q}})$, where $\mathfrak{q}$ is a certain prime of L above q and $L_{\mathfrak{q}}$ denotes the completion of L at $\mathfrak{q}$. The inclusion $G_{\mathbb{Q}_{q^n}} \leq \operatorname{Gal}(\bar{\mathbb{Q}}_q/L_{\mathfrak{q}})$ means that we have the field inclusions

$$\mathbb{Q}_q \subseteq L_{\mathfrak{q}} \subseteq \mathbb{Q}_{q^n} \subseteq \bar{\mathbb{Q}}_q$$

and $[L_{\mathfrak{q}} : \mathbb{Q}_q] = (G_{\mathbb{Q}_q} : G_{\mathbb{Q}_q} \cap H) = (G_{\mathbb{Q}} : H) = [L : \mathbb{Q}]$; hence q is inert in $L/\mathbb{Q}$.

Let ℓ_1 be a prime dividing N_1, let $\widetilde{L}/\mathbb{Q}$ be a Galois closure of $L/\mathbb{Q}$, Λ_1 a prime of $\widetilde{L}$ above ℓ_1 and I_1 the inertia group of Λ_1 over $\mathbb{Q}$. Since $\gcd(|\rho(I_{\ell_1})|, n!) = 1$ and $\operatorname{Gal}(\widetilde{L}/\mathbb{Q})$ has order dividing $n!$, we get that the projection of $\rho(I_1) \subseteq \rho(I_{\ell_1})$ into $\rho(G_{\mathbb{Q}})/\rho(G_{\widetilde{L}})$ is trivial. Thus, $\rho(I_1) \subseteq \rho(G_{\widetilde{L}})$. Hence $\widetilde{L}/\mathbb{Q}$ is unramified at ℓ_1 and so is $L/\mathbb{Q}$.

To sum up, we know that L can only be ramified at the primes dividing $Nq\ell$. But L cannot ramify at q since $L_{\mathfrak{q}} \subseteq \mathbb{Q}_{q^n}$ (and $\mathbb{Q}_{q^n}$ is an unramified extension of $\mathbb{Q}_q$). We just saw that L cannot ramify at the primes dividing N_1. We also know that L cannot be ramified at ℓ (see Proposition 3.4). Hence L only ramifies at the primes dividing N_2. By the choice of q, it is completely split in L, and at the same time inert in L. This shows $L = \mathbb{Q}$ and $H = G_{\mathbb{Q}}$. □

Now we can easily prove the main group theoretic result.

Proof of Theorem 1.5. Let $G = \mathrm{Im}\rho$. Since G contains a transvection, one of the following three possibilities holds (cf. Corollary 1.2):

(1) ρ is reducible.

(2) There exists an open subgroup $H \subsetneq G_{\mathbb{Q}}$, say of index h with n/h even, and a representation $\rho' : H \to \mathrm{GSp}_{n/h}(\overline{\mathbb{F}}_\ell)$ such that $\rho \cong \mathrm{Ind}_H^{G_{\mathbb{Q}}} \rho'$.

(3) The group generated by the transvections in G is conjugated (in $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$) to $\mathrm{Sp}_n(\mathbb{F}_{\ell^r})$ for some exponent r.

By Lemma 3.1, G acts irreducibly on V; hence the first possibility cannot occur. By Lemma 3.7, the second possibility does not occur. Hence the third possibility holds, and this finishes the proof of the theorem. □

Proof of Corollary 1.6. This follows from the main theorem of Part I [Arias-de-Reyna et al. 2013] concerning the application to the inverse Galois problem. In order to be able to apply it, there are two things to check: Firstly, we note that $\rho_\bullet$ is maximally induced of order p at the prime q. Secondly, the existence of a transvection in the image of $\bar{\rho}_\lambda$ together with the special shape of the representation at q allow us to conclude from Theorem 1.5 that the image of $\bar{\rho}_\lambda$ is huge for all $\lambda \mid \ell$, where ℓ runs through the rational primes outside a density zero set. □

Acknowledgements

References

[Arias-de-Reyna et al. 2013] S. Arias-de-Reyna, L. V. Dieulefait, and G. Wiese, "Compatible systems of symplectic Galois representations and the inverse Galois problem, I: Images of projective representations", preprint, 2013. To appear in *Trans. Amer. Math. Soc.* arXiv 1203.6546

[Arias-de-Reyna et al. 2015] S. Arias-de-Reyna, L. V. Dieulefait, S. W. Shin, and G. Wiese, "Compatible systems of symplectic Galois representations and the inverse Galois problem, III: Automorphic construction of compatible systems with suitable local properties", *Math. Ann.* **361**:3-4 (2015), 909–925. MR 3319552 Zbl 06421505

[Artin 1957] E. Artin, *Geometric algebra*, Interscience, New York, 1957. MR 18,553e Zbl 0077.02101

[Curtis and Reiner 1981] C. W. Curtis and I. Reiner, *Methods of representation theory, I: With applications to finite groups and orders*, Wiley, New York, 1981. MR 82i:20001 Zbl 0469.20001

[Dieulefait and Wiese 2011] L. V. Dieulefait and G. Wiese, "On modular forms and the inverse Galois problem", *Trans. Amer. Math. Soc.* **363**:9 (2011), 4569–4584. MR 2012k:11069 Zbl 1264.11045

[Guralnick and Saxl 2003] R. M. Guralnick and J. Saxl, "Generation of finite almost simple groups by conjugates", *J. Algebra* **268**:2 (2003), 519–571. MR 2005f:20057 Zbl 1037.20016

[Kantor 1979] W. M. Kantor, "Subgroups of classical groups generated by long root elements", *Trans. Amer. Math. Soc.* **248**:2 (1979), 347–379. MR 80g:20057 Zbl 0406.20040

[Khare et al. 2008] C. Khare, M. Larsen, and G. Savin, "Functoriality and the inverse Galois problem", *Compos. Math.* **144**:3 (2008), 541–564. MR 2009m:11076 Zbl 1194.11062

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics **42**, Springer, New York, 1977. MR 56 #8675 Zbl 0355.20006

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. MR 82e:12016 Zbl 0423.12016

SARA ARIAS-DE-REYNA
FACULTÉ DES SCIENCES, DE LA TECHNOLOGIE ET DE LA COMMUNICATION
UNIVERSITY OF LUXEMBOURG
6, RUE RICHARD COUDENHOVE-KALERGI
L-1359 LUXEMBOURG
LUXEMBOURG

sara.ariasdereyna@uni.lu

LUIS DIEULEFAIT
DEPARTAMENT D'ÁLGEBRA I GEOMETRIA, FACULTAT DE MATEMATIQUES
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES, 585
08007 BARCELONA
SPAIN

ldieulefait@ub.edu

GABOR WIESE
FACULTÉ DES SCIENCES, DE LA TECHNOLOGIE ET DE LA COMMUNICATION
UNIVERSITY OF LUXEMBOURG
6, RUE RICHARD COUDENHOVE-KALERGI
L-1359 LUXEMBOURG
LUXEMBOURG

gabor.wiese@uni.lu

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

PACIFIC JOURNAL OF MATHEMATICS