Automorphic Galois representations and the inverse Galois problem

Sara Arias-de-Reyna*

Abstract

A strategy to address the inverse Galois problem over $\mathbb{Q}$ consists of exploiting the knowledge of Galois representations attached to certain automorphic forms. More precisely, if such forms are carefully chosen, they provide compatible systems of Galois representations satisfying some desired properties, e.g. properties that reflect on the image of the members of the system. In this article we survey some results obtained using this strategy.

MSC (2010): 11F80 (Galois representations); 12F12 (Inverse Galois theory).

1 Introduction

The motivation for the subject of this survey comes from Galois theory. Let L/K be a field extension which is normal and separable. To this extension one can attach a group, namely the group of field automorphisms of L fixing K, which is denoted as $\mathrm{Gal}(L/K)$. The main result of Galois theory, which is usually covered in the program of any Bachelor's degree in Mathematics, can be stated as follows:

Theorem 1.1 (Galois)**.** *Let L/K be a finite, normal, separable field extension. Then there is the following bijective correspondence between the sets:*

$$\left\{ \begin{array}{c} E \text{ field} \\ K \subseteq E \subseteq L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} H \subseteq \mathrm{Gal}(L/K) \\ \text{subgroup} \end{array} \right\},$$

$$\begin{array}{ccc} E & \longmapsto & \mathrm{Gal}(L/E) \\ L^H & \longleftarrow & L \end{array}$$

Usually the students are asked exercises of the following type: Given some finite field extension $L/\mathbb{Q}$ which is normal, compute the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ attached to it. But, one may also ask the inverse question (hence the name inverse Galois problem): Given a finite group G, find a finite, normal extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$. This is not a question one usually expects a student to solve! In fact, there are (many) groups G for which it is not even known if such a field extension exists.

Problem 1.2 (Inverse Galois Problem)**.** Let G be a finite group. Does there exist a Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$?

The first mathematician that addressed this problem was D. Hilbert. In his paper [13] he proves his famous Irreducibility Theorem, and applies it to show that, for all $n \in \mathbb{N}$, the symmetric group S_n and the alternating group A_n occur as Galois groups over the rationals. Since then, many mathematicians have thought about the inverse Galois problem, and in fact it is now solved (affirmatively) for many (families of) finite groups G. For instance, let us mention the result of Shafarevich that all solvable groups occur as Galois groups over the rationals (see [23] for a

*Université du Luxembourg, Faculté des Sciences, de la Technologie et de la Communication, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg, sara.ariasdereyna@uni.lu

detailed explanation of the proof). However, it is still not known if the answer is affirmative for every finite group G, and as far as I know, there is no general strategy that addresses all finite groups at once. An account of the different techniques used to address the problem can be found in [32].

Let K be a field, and let us fix a separable closure K_{sep}. There is a way to group together all the Galois groups of finite Galois extensions L/K contained in K_{sep}, namely the *absolute Galois group* of K. It is defined as the inverse limit

$$G_K := \text{Gal}(K_{\text{sep}}/K) = \varprojlim_{\substack{L/K \\ \text{finite Galois}}} \text{Gal}(L/K).$$

This group is a profinite group, and as such is endowed with a topology, called the *Krull topology*, which makes it a Hausdorff, compact and totally disconnected group. A very natural question to ask is what information on the field K is encoded in the topological group G_K. In this connection, a celebrated result of Neukirch, Iwasawa, Uchida and Ikeda establishes that, if K_1, K_2 are two finite extensions of $\mathbb{Q}$ contained in a fixed algebraic closure $\overline{\mathbb{Q}}$ such that $G_{K_1} \simeq G_{K_2}$, then K_1 and K_2 are conjugated by some element in $G_{\mathbb{Q}}$ (cf. [34], [16]). Let us note, however, that we cannot replace $\mathbb{Q}$ by any field. For example, the analogous statement does not hold when the base field is $\mathbb{Q}_p$, cf. [37] and [17]. Thus, we see that the absolute Galois group of $\mathbb{Q}$ encodes a wealth of information about the arithmetic of number fields. In this context, the inverse Galois problem can be formulated as the question of determining which finite groups occur as quotient groups of $G_{\mathbb{Q}}$.

A natural way to study $G_{\mathbb{Q}}$ is to consider its representations, that it, the continuous group morphisms $G_{\mathbb{Q}} \to \text{GL}_m(k)$, where k is a topological field and $m \in \mathbb{N}$. Such a representation will be called a *Galois representation*. Let us assume that k is a finite field, endowed with the discrete topology, and let

$$\rho : G_{\mathbb{Q}} \to \text{GL}_m(k)$$

be a Galois representation. Since the set $\{\text{Id}\}$ is open in $\text{GL}_m(k)$, we obtain that $\ker \rho \subset G_{\mathbb{Q}}$ is an open subgroup. In other words, there exists a finite Galois extension $K/\mathbb{Q}$ such that $\ker \rho = G_K$. Therefore

$$\text{Im}\rho \simeq G_{\mathbb{Q}}/\ker \rho \simeq G_{\mathbb{Q}}/G_K \simeq \text{Gal}(K/\mathbb{Q}).$$

This reasoning shows that, whenever we are given a Galois representation of $G_{\mathbb{Q}}$ over a finite field k, we obtain a realisation of $\text{Im}\rho \subset \text{GL}_m(k)$ as a Galois group over $\mathbb{Q}$. In this way, any source of Galois representations provides us with a strategy to address the inverse Galois problem for the subgroups of $\text{GL}_m(k)$ that occur as images thereof.

Geometry provides us with many objects endowed with an action of the absolute Galois group of the rationals, thus giving rise to such Galois representations. One classical example is the group of $\overline{\mathbb{Q}}$-defined ℓ-torsion points of an elliptic curve E defined over $\mathbb{Q}$. We will treat this example in Section 2. In this survey we will be interested in (compatible systems of) Galois representations arising from automorphic representations. In Section 4 we will describe Galois representations attached to an automorphic representation π which satisfies several technical conditions. The statements of the most recent results (to the best of my knowledge) on the inverse Galois problem obtained by means of compatible systems of Galois representations attached to automorphic representations can be found in Section 5, together with some ideas about their proofs.

A remarkable feature of this method is that, in addition, one obtains some control of the ramification of the Galois extension that is produced. Namely, it will only be ramified at the residual characteristic and at a finite set of auxiliary primes, that usually one is allowed to choose (inside some positive density set of primes). This will be highlighted in the statements below.

Acknowledgements: This article is an expanded version of the plenary lecture I delivered at the conference *Quintas Jornadas de Teoría de Números* (July 2013). I would like to thank the scientific committee for giving me the oportunity to participate in this conference, and the organising committee for their excellent work. I also want to thank Gabor Wiese for his remarks and suggestions on a previous version of this article.

2 Some classical cases

In this section we revisit some classical examples of Galois representations attached to geometric objects. We begin with the Galois representations attached to the torsion points of elliptic curves, and later we will see them as a particular case of Galois representations attached to modular forms.

2.1 Elliptic curves

An elliptic curve is a genus one curve, endowed with a distinguished base point. Every elliptic curve E can be described by means of a Weierstrass equations, that is, an affine equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the coefficients $a_1, \ldots, a_6$ lie in some field K. The most significant property of elliptic curves is that the set of points of E (defined over some field extension L/K) can be endowed with a commutative group structure, where the neutral element is the distinguished base point.

Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime number. We can consider the subgroup $E[\ell](\overline{\mathbb{Q}})$ of $E(\overline{\mathbb{Q}})$ consisting of ℓ-torsion points. This group is isomorphic to the product of two copies of $\mathbb{F}_\ell$. Moreover, since the elliptic curve is defined over $\mathbb{Q}$, the absolute Galois group $G_\mathbb{Q}$ acts naturally on the set of $\overline{\mathbb{Q}}$-defined points of E, and this action restricts to $E[\ell](\overline{\mathbb{Q}})$. We obtain thus a Galois representation

$$\overline{\rho}_{E,\ell} : G_\mathbb{Q} \to \mathrm{Aut}(E[\ell](\overline{\mathbb{Q}})) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

As explained in the introduction, the image of $\overline{\rho}_{E,\ell}$ can be realised as a Galois group over $\mathbb{Q}$. This brings forward the question of determining the image of such a Galois representation. In this context, there is a classical result by J. P. Serre from the seventies ([29], Théorème 2).

Theorem 2.1 (Serre)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication over $\overline{\mathbb{Q}}$. Then the representation $\overline{\rho}_{E,\ell}$ is surjective for all except finitely many primes ℓ.*

We can immediately conclude that $\mathrm{GL}_2(\mathbb{F}_\ell)$ can be realised as a Galois group over $\mathbb{Q}$ for all except finitely many primes ℓ. However, we can do even better by picking a particular elliptic curve and analysing the Galois representations attached to it.

Example 2.2. Let $E/\mathbb{Q}$ be the elliptic curve defined by the Weierstrass equation

$$y^2 + y = x^3 - x.$$

This curve is labelled 37A in [6], and it has the property that $\overline{\rho}_{E,\ell}$ is surjective *for all primes* ℓ (see [29], Example 5.5.6). Therefore we obtain that $\mathrm{GL}_2(\mathbb{F}_\ell)$ occurs as the Galois group of a finite Galois extension $K/\mathbb{Q}$. Moreover, we have additional information on the ramification of $K/\mathbb{Q}$; namely, it ramifies only at 37 (which is the conductor of E) and ℓ.

The next situation we want to analyse is that of Galois representations attached to modular forms. Let us recall that modular forms are holomorphic functions defined on the complex upper half plane, which satisfy certain symmetry relations. We will not recall here the details of the definition (see e.g. [9] for a complete treatment focusing on the relationship with arithmetic geometry). These objects, of complex-analytic nature, play a central role in number theory. At the core of this relationship is the fact that one can attach Galois representations of $G_\mathbb{Q}$ to them. More precisely, let f be a cuspidal modular form of weight $k \geq 2$, conductor N and character ψ (in short: $f \in S_k(N, \psi)$), which is a normalised Hecke eigenform. We may write the Fourier expansion of f as $f(z) = \sum_{n\geq 1} a_n q^n$, where $q = e^{2\pi iz}$. A first remark is that the *coefficient field* $\mathbb{Q}_f = \mathbb{Q}(\{a_n : \gcd(n, N) = 1\})$ is a number field. Denote by $\mathcal{O}_{\mathbb{Q}_f}$ its ring of integers. By a result of Deligne (cf. [7]), for each prime λ of $\mathcal{O}_{\mathbb{Q}_f}$ there exists a (continuous) Galois representation

$$\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_{\overline{\mathbb{Q}}_{f,\lambda}}),$$

related to f, where $\mathbb{Q}_{f,\lambda}$ denotes the completion of $\mathbb{Q}_f$ at the prime λ, $\overline{\mathbb{Q}}_{f,\lambda}$ an algebraic closure thereof and $\mathcal{O}_{\overline{\mathbb{Q}}_{f,\lambda}}$ is the valuation ring of $\overline{\mathbb{Q}}_{f,\lambda}$. Here the topology considered on $\mathrm{GL}_2(\mathcal{O}_{\overline{\mathbb{Q}}_{f,\lambda}})$ is the one induced by the ℓ-adic valuation.

The relationship between $\rho_{f,\lambda}$ and f is the following. First, $\rho_{f,\lambda}$ is unramified outside $N\ell$. Moreover, for each $p \nmid N\ell$, we can consider the image under $\rho_{f,\lambda}$ of a lift Frob_p of a Frobenius element at p (this is well defined because $\rho_{f,\lambda}$ is unramified at p). Then the characteristic polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ equals $T^2 - a_pT + \psi(p)p^{k-1}$.

We may compose each $\rho_{f,\lambda}$ with the reduction modulo the maximal ideal of $\mathcal{O}_{\overline{\mathbb{Q}}_{f,\lambda}}$, and we obtain a (residual) representation

$$\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\kappa(\overline{\mathbb{Q}}_{f,\lambda})) \simeq \mathrm{GL}_2(\overline{\mathbb{F}}_\ell),$$

where ℓ is the rational prime below λ. One of the main recent achievements in number theory has been the proof of Serre's Modularity Conjecture, which says that every Galois representation $\overline{\rho}_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ which is odd and irreducible is actually isomorphic to $\overline{\rho}_{f,\lambda}$ for some modular form f and some prime λ as above.

In this survey we are interested in the image of $\overline{\rho}_{f,\lambda}$. These images have been studied by K. Ribet (cf. [24], [25]). One first remark is that, when $\rho_{f,\lambda}$ is absolutely irreducible, then it can be conjugated (inside $\mathrm{GL}_2(\mathcal{O}_{\overline{\mathbb{Q}}_{f,\lambda}})$) so that its image is contained in $\mathrm{GL}_2(\mathcal{O}_{\mathbb{Q}_{f,\lambda}})$. Therefore, in this case we can assume that $\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\kappa(\mathbb{Q}_{f,\lambda}))$, where $\kappa(\mathbb{Q}_{f,\lambda})$ denotes the residue field of $\mathbb{Q}_{f,\lambda}$.

To state Ribet's result, we first introduce two more number fields related to f. The first one is the *twist invariant coefficient field of* f, which is the subfield of the coefficient field of f defined as $F_f := \mathbb{Q}(\{a_n^2/\psi(n) : \gcd(n, N) = 1\})$. The second field, which is a finite abelian extension of $\mathbb{Q}$, is the subfield K_f of $\overline{\mathbb{Q}}$ fixed by all inner twists of f (see [10] for details).

Theorem 2.3 (Ribet)**.** *Let $f = \sum_{n\geq 1} a_n q^n \in S_k(N, \psi)$ be a normalised cuspidal Hecke eigenform. Assume f does not have complex multiplication. Then for all except finitely many prime ideals λ of $\mathbb{Q}_f$,*

$$\overline{\rho}_{f,\lambda}(G_{K_f}) = \left\{ g \in \mathrm{GL}_2\left(\kappa\left(F_{f,\lambda'}\right)\right) : \det(g) \in (\mathbb{F}_\ell^\times)^{k-1} \right\},$$

where λ' is the ideal of $\mathcal{O}_{F_f}$ below λ and ℓ is the rational prime below λ.

This result suggests that we look at the representation $\overline{\rho}_{f,\lambda}^{\mathrm{proj}}$ obtained by composing $\overline{\rho}_{f,\lambda}$ with the projection map $\mathrm{GL}_2(\kappa(\mathbb{Q}_{f,\lambda})) \to \mathrm{PGL}_2(\kappa(\mathbb{Q}_{f,\lambda}))$.

More precisely, let k, r be integers greater than or equal to 1. Consider the set

$$\mathcal{A} := \{A \in \mathrm{GL}_2(\mathbb{F}_{\ell^r}) : \det A \in (\mathbb{F}_\ell^\times)^{k-1}\},$$

and let $\mathcal{A}^{\mathrm{proj}}$ be its projection under the map $\mathrm{GL}_2(\mathbb{F}_{\ell^r}) \to \mathrm{PGL}_2(\mathbb{F}_{\ell^r})$. Then if k is odd, we have $\mathcal{A}^{\mathrm{proj}} = \mathrm{PSL}_2(\mathbb{F}_{\ell^r})$, and if k is even, we have $\mathcal{A}^{\mathrm{proj}} = \mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ whenever r is odd and $\mathcal{A}^{\mathrm{proj}} = \mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ whenever r is even.

In any case it follows that, for f as above, the image of $\overline{\rho}_{f,\lambda}^{\mathrm{proj}}$ equals $\mathrm{PSL}_2\left(\kappa\left(F_{f,\lambda'}\right)\right)$ or $\mathrm{PGL}_2\left(\kappa\left(F_{f,\lambda'}\right)\right)$ for all except finitely many primes λ of $\mathcal{O}_{\mathbb{Q}_f}$.

A remarkable difference with the situation arising from elliptic curves is that we obtain realisations of linear groups over fields whose cardinality is not necessarily a prime number. In Example 2.2, we used an elliptic curve to obtain realisations of the members of the family $\{\mathrm{GL}_2(\mathbb{F}_\ell)\}_\ell$. However, now we have two parameters, namely the prime ℓ and the exponent r. If we pick a modular form as above, we will obtain realisations of members of one of the families $\{\mathrm{PSL}_2(\mathbb{F}_{\ell^r})\}_{\ell,r}$ or $\{\mathrm{PGL}_2(\mathbb{F}_{\ell^r})\}_{\ell,r}$, and the parameter r *depends on* f *and* ℓ.

Example 2.4 (Ribet, 1975)**.** Let $f \in S_{24}(1)$ be a normalised Hecke eigenform of level 1. The field of coefficients $\mathbb{Q}_f = \mathbb{Q}(\sqrt{144169})$ equals F_f; so we can expect to obtain realisations of $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ when ℓ is inert in $\mathbb{Q}_f$ and $\mathrm{PGL}_2(\mathbb{F}_\ell)$ when ℓ splits in $\mathbb{Q}_f$. Indeed, let ℓ be a prime different from 2, 3 and 47. Then f provides a realisation of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ if 144169 is a square modulo ℓ and a realisation of $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ if 144169 is not a square modulo ℓ. Moreover, the corresponding Galois extension $K/\mathbb{Q}$ with desired Galois group is unramified outside ℓ.

3 Compatible systems and the inverse Galois problem

The examples of the previous section suggest that, instead of considering isolated Galois representations $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ for a fixed prime ℓ, it is a good idea to look at a system of Galois representations $(\overline{\rho}_\ell)_\ell$, where ℓ runs through the prime numbers. The notion of *(strictly) compatible system of Galois representations* already appears in [28]. We recall the definition below.

Definition 3.1. Let $n \in \mathbb{N}$ and let F be a number field. A *compatible system* $\rho_\bullet = (\rho_\lambda)_\lambda$ *of* m*-dimensional representations of* G_F consists of the following data:

- A number field L.
- A finite set S of primes of F.
- For each prime $\mathfrak{p} \notin S$, a monic polynomial $P_\mathfrak{p}(X) \in \mathcal{O}_L[X]$ (with $\mathcal{O}_L$ the ring of integers of L).
- For each finite place λ of L (together with fixed embeddings $L \hookrightarrow L_\lambda \hookrightarrow \overline{L}_\lambda$) a continuous Galois representation
$$\rho_\lambda : G_F \to \mathrm{GL}_m(\overline{L}_\lambda)$$
such that ρ_λ is unramified outside $S \cup S_\ell$ (where ℓ is the rational prime below λ and S_ℓ is the set of primes of F above ℓ) and such that for all $\mathfrak{p} \notin S \cup S_\ell$ the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_\mathfrak{p})$ is equal to $P_\mathfrak{p}(X)$.

In our context, the main question to ask about a compatible system is the following: If we know that ρ_λ satisfies some property (A), does it follow that $\rho_{\lambda'}$ also satisfies (A) for another prime λ' of L? In other words, what properties "propagate" through a compatible system? The idea that the property of "being attached to a modular form" propagates through such a system lies at the core of the proof of the Taniyama-Shimura conjecture by A. Wiles and R. Taylor (which implies Fermat's Last Theorem), and also of the proof of Serre's Modularity Conjecture.

In this section we are interested in the relationship between the images of the members ρ_λ of a compatible system. An example of such a relationship is the following: if ρ_λ, $\rho_{\lambda'}$ are two semisimple representations belonging to a compatible system, then the image of ρ_λ is abelian if and only if the image of $\rho_{\lambda'}$ is abelian (see [28] and [12]).

The case of compatible systems of Galois representations attached to the Tate module of abelian varieties has received particular attention. Let A/F be an n-dimensional abelian variety, and assume that
$$(\rho_{A,\ell} : G_F \to \mathrm{GL}(V_{\mathbb{Q}_\ell}) \simeq \mathrm{GL}_{2n}(\mathbb{Q}_\ell))_\ell$$
is the compatible system of Galois representations attached to the ℓ-adic Tate module T_ℓ of A (where as usual $V_{\mathbb{Q}_\ell} = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell$)). To what extent does the image of ρ_ℓ depend on ℓ? There are several ways to phrase this question in a precise way. For example, define the *algebraic monodromy group* at ℓ, G_ℓ, as the Zarisky closure of $\rho_\ell(G_F)$ inside the algebraic group $\mathrm{GL}_{2n,\mathbb{Q}_\ell}$, and let G_ℓ^0 be the connected component of G_ℓ. In this connection, the Mumford-Tate conjecture predicts the existence of an algebraic group $G \subset \mathrm{GL}_{2n,\mathbb{Q}}$ such that, for all ℓ, $G_\ell^0 \simeq \mathbb{Q}_\ell \times_{\mathbb{Q}} G$ (see [27], Conjecture C.3.3 for a precise formulation). By work of J. P. Serre it is known that the (finite) group of connected components G_ℓ/G_ℓ^0 is independent of ℓ (see [31], 2.2.3).

There are many partial results in this direction. In particular cases, the conjecture is known to hold (for example, when $\dim A = 1$ cf. [28] and [29]. For higher dimension, when $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ and $n = 2$ or odd the conjecture holds with $G = \mathrm{GSp}_{2n,\mathbb{Q}}$; cf. [31], 2.2.8). In the general case, Serre has proved that the rank of G_ℓ is independent of ℓ [30]. More partial results can be found in [21], [14].

Another question is how close $\rho_\ell(G_F)$ is to its Zarisky closure G_ℓ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$. For results in this direction the reader is referred to [20] and [15].

A particular case, which is of interest to us (cf. Section 5), is proved by C. Hall in [11]. Let A/F be an n-dimensional abelian variety which is principally polarised and with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$.

Assume that there exists a prime $\mathfrak{p}$ of F such that the reduction of A at $\mathfrak{p}$ is semistable of toric dimension 1. Then there exists a constant M such that, for all primes $\ell \geq M$, the image of the mod ℓ Galois representation $\overline{\rho}_{A,\ell} : G_F \to \mathrm{GL}_{2n}(\mathbb{F}_\ell)$ coincides with $\mathrm{GSp}_{2n}(\mathbb{F}_\ell)$. As a consequence, it follows that A satisfies the Mumford-Tate conjecture; more precisely, the corresponding algebraic group is $\mathrm{GSp}_{2n,\mathbb{Q}}$. The proof of this result relies heavily on the fact that the existence of the prime $\mathfrak{p}$ implies that the image under $\overline{\rho}_{A,\ell}$ of the inertia group at $\mathfrak{p}$ contains a transvection.

For the applications to the inverse Galois problem, we will be interested in Galois representations taking values in linear groups over finite fields. For the rest of the section, we focus on symplectic groups GSp_{2n} for simplicity. Note that $\mathrm{GSp}_2 = \mathrm{GL}_2$ and $\mathrm{Sp}_2 = \mathrm{SL}_2$, so in the case of dimension 1 we are in the situation explained in Section 2. Consider the following setup:

Set-up 3.2. Let $\rho_\bullet = (\rho_\lambda)_\lambda$ be a $2n$-dimensional compatible system of Galois representations of $G_\mathbb{Q}$ as in Definition 3.1, such that for all λ, $\rho_\lambda : G_\mathbb{Q} \to \mathrm{GSp}_{2n}(\overline{L}_\lambda)$ for some number field L (we will say that such a system is *symplectic*).

Note that each of the ρ_λ is defined over a finite extension of L_λ inside $\overline{L}_\lambda$. Moreover, we can conjugate each ρ_λ to take values inside the ring of integers of this finite extension of L_λ, and further reduce it modulo λ, obtaining a residual representation $\overline{\rho}_\lambda$. When $\overline{\rho}_\lambda$ is absolutely irreducible, then ρ_λ can be defined over L_λ, and therefore $\overline{\rho}_\lambda$ takes values inside $\mathrm{GSp}_{2n}(\kappa(L_\lambda))$, where $\kappa(L_\lambda)$ denotes the residue field of L_λ. Recall the motivating example in Section 2 of compatible systems attached to modular forms. In this example, the field L can be taken to be the coefficient field $\mathbb{Q}_f$. Like in the case of compatible systems attached to modular forms, it will be convenient to consider the composition $\overline{\rho}_\lambda^{\mathrm{proj}}$ of $\overline{\rho}_\lambda$ with the natural projection $\mathrm{GSp}_{2n}(\kappa(L_\lambda)) \to \mathrm{PGSp}_{2n}(\kappa(L_\lambda))$. In what follows, we focus on obtaining realisations of groups in one of the families $\{\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})\}_{\ell,r}$ or $\{\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})\}_{\ell,r}$.

Assume that we are given a compatible system of Galois representations as in Set-up 3.2 such that all ρ_λ are residually absolutely irreducible. We obtain a system

$$(\overline{\rho}_\lambda : G_\mathbb{Q} \to \mathrm{GSp}_{2n}(\kappa(L_\lambda)))_\lambda.$$

For each prime λ of L, $\kappa(L_\lambda) \simeq \mathbb{F}_{\ell^{r(\lambda)}}$ for some integer $r(\lambda)$, which actually changes with λ! If we want to realise the family of groups $\{\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})\}_\ell$ for a fixed exponent r, it is clear that one compatible system will not suffice for our purposes (unless we are interested in $r = 1$ and we have $L = \mathbb{Q}$). This phenomenon already appeared in Section 2 in the case of compatible systems attached to modular forms.

The strategy to obtain Galois realisations will proceed as follows. We want to construct a compatible system of Galois representations $\rho_\bullet$ as in Set-up 3.2, such that the ρ_λ are absolutely irreducible, and such that the images of the corresponding representations $\overline{\rho}_\lambda$ are large in some sense which does not depend on λ. More precisely, we will say that the image of a representation $\overline{\rho}_\lambda : G_\mathbb{Q} \to \mathrm{GSp}_{2n}(\kappa(L_\lambda))$ is *huge* if it contains a conjugate (inside $\mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$) of $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$ (where ℓ is the prime below λ). A group theoretical reasoning shows that if $\overline{\rho}_\lambda$ has huge image, then the image of $\overline{\rho}_\lambda^{\mathrm{proj}}$ equals $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$ or $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ for some integer r (cf. Corollary 5.7 of [1]). Moreover, we will have to find some conditions to control the exponent r.

The presence of these two parameters, ℓ and r, gives rise to two different approaches to obtain results on the inverse Galois problem:

- **Vertical Direction:** Fix a prime number ℓ. Obtain realisations of $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ (resp. $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$) for all $r \in \mathbb{N}$.
- **Horizontal Direction:** Fix a natural number $r \geq 1$. Obtain realisations of $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ (resp. $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$) for all primes ℓ.

This nomenclature stems from the following representation: Place in a graphic the groups in the family $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ (resp. $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$) that are realised as Galois groups over $\mathbb{Q}$ by displaying in the x-axis the prime ℓ and in the y-axis the exponent r, and drawing a dot whenever the group

$\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ (resp. $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$) is realised as a Galois group over $\mathbb{Q}$ (see [10] for such a graphic when $n = 1$).

By exploiting the compatible systems of Galois representations attached to modular forms, the following results have been proved in the vertical direction (see Theorem 1.1 of [35]) and in the horizontal direction (see Theorem 1.1 of [10]).

Theorem 3.3 (Wiese)**.** *Let ℓ be a prime number. There exist infinitely many natural numbers r such that $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ occurs as the Galois group of a finite Galois extension $K/\mathbb{Q}$, which is unramified outside ℓ and an auxiliary prime q.*

Theorem 3.4 (Dieulefait, Wiese)**.** *Let $r \in \mathbb{N}$.*

1. *There exists a positive density set of primes ℓ such that $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ occurs as the Galois group of a finite Galois extension $K/\mathbb{Q}$, which is unramified outside ℓ and two (resp. three) auxiliary primes if n is even (resp. odd).*

2. *Assume that r is odd. There exists a positive density set of primes ℓ such that $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ occurs as the Galois group of a finite Galois extension $K/\mathbb{Q}$, which is unramified outside ℓ and two auxiliary primes.*

Let us look more closely at the approach in the horizontal direction. We fix a natural number r, and we want to realise $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ as Galois groups over $\mathbb{Q}$ for as many primes ℓ as we can. From the remarks above, it is clear that a single modular form will not suffice to realise $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ for *all* ℓ. However, nothing prevents us from looking at several modular forms. In fact, Serre's Modularity Conjecture, which is now a theorem, tells us that every irreducible, odd Galois representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ is attached to some modular form f. As a consequence, any realisation of $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ as the Galois group of a finite Galois extension $K/\mathbb{Q}$ with K imaginary can be obtained through this method (cf. Proposition 1.2 of [10]). By making use of Theorem 2.3, we know that for a normalised Hecke eigenform without complex multiplication, the image of $\overline{\rho}_{f,\lambda}$ is huge for all except finitely many prime ideals λ of $\mathbb{Q}_f$, and thus the image of $\overline{\rho}_{f,\lambda}^{\mathrm{proj}}$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$. The main obstacle here is to obtain some control on the exponent r. Under additional conditions, the field $\mathbb{F}_{\ell^r}$ coincides with $\kappa(\mathbb{Q}_{f,\lambda})$, reducing the problem to the analysis of $\mathbb{Q}_f$. But this is not a minor issue! Very little is known about these fields (although one can always compute them for any given modular form f). When the level of f is 1, there is a strong conjecture in this connection, namely Maeda's conjecture, stating that the degree $d_f = [\mathbb{Q}_f : \mathbb{Q}]$ should equal the dimension of $S_k(1)$ as a complex vector space (k being the *weight* of f) and the Galois group of the normal closure of $\mathbb{Q}_f/\mathbb{Q}$ is equal to the symmetric group S_{d_f}. Assuming this conjecture, one can improve Theorem 3.4 as follows (cf. Theorem 1.1 of [36]).

Theorem 3.5 (Wiese)**.** *Assume Maeda's Conjecture holds. Let $r \in \mathbb{N}$. Assume that r is even (resp. odd). There exists a density 1 set of primes ℓ such that $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ (resp. $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$) occurs as the Galois group of a finite Galois extension $K/\mathbb{Q}$, which is unramified outside ℓ.*

4 Galois representations attached to automorphic forms

In order to use the strategy outlined in the previous section to obtain results on the inverse Galois problem, we first need to find a source of compatible systems of Galois representations of $G_{\mathbb{Q}}$. As discussed in Section 2, elliptic curves defined over $\mathbb{Q}$ (and, analogously, abelian varieties of higher dimension which are defined over $\mathbb{Q}$) provide us with such systems, and, more generally, classical modular forms give rise to such systems. Both of these examples can be encompassed in the general framework provided by the Langlands conjectures. More precisely, given an automorphic representation π (which is *algebraic* in some precise sense) for an arbitrary connected reductive group G over $\mathbb{Q}$, one hopes that there exists a compatible system of Galois representations $(\rho_\bullet(\pi))$ attached to it, where $\rho_\lambda(\pi)$ takes values in the $\overline{\mathbb{Q}}_\ell$-points of a certain algebraic group attached to G (namely the Langlands dual of G). Conjecturally, then, we have many compatible systems of

Galois representations, which builds up the hope of eventually applying the strategy described in the previous section to realise many linear groups as Galois groups over the rationals.

There are several cases when these conjectures are known to hold. Recently, there has been a breakthrough in this connection due to P. Scholze [26] and M. Harris, K.-W. Lan, R. Taylor, J. Thorne. Namely, they attach compatible systems of Galois representations to regular, L-algebraic cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{A}_F)$, where F is a totally real or a CM number field.

However, in this section we will recall a less recent result, due to L. Clozel, R. Kottwitz, M. Harris, R. Taylor and several others, which is more restrictive, since it deals with RAESDC (regular, algebraic, essentially self-dual, cuspidal) automorphic representations. We will not recall here all definitions (the reader can look them up in [4]), but we will try to give some explanations.

Let $\mathbb{A}_{\mathbb{Q}}$ denote the ring of adeles of $\mathbb{Q}$. We consider so-called irreducible admissible representations π of $\mathrm{GL}_m(\mathbb{A}_{\mathbb{Q}})$. In fact, π is not literally a representation of the group $\mathrm{GL}_m(\mathbb{A}_{\mathbb{Q}})$ into some vector space. The interested reader can look at the details in [5]. In this survey, we will treat them as black boxes, focusing rather on the compatible systems of Galois representations that they give rise to.

A *RAESDC (regular, algebraic, essentially self-dual, cuspidal) automorphic representation of* $\mathrm{GL}_m(\mathbb{A}_{\mathbb{Q}})$ can be defined as a pair (π, μ) consisting of a cuspidal automorphic representation π of $\mathrm{GL}_m(\mathbb{A}_{\mathbb{Q}})$ and a continuous character $\mu : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to \mathbb{C}^{\times}$ such that:

1. (regular algebraic) π has *weight* $a = (a_i) \in \mathbb{Z}^n$.
2. (essentially self-dual) $\pi \cong \pi^{\vee} \otimes (\mu \circ \mathrm{Det})$.

Given a RAESDC automorphic representation π as above, there exist a number field $M \subset \mathbb{C}$, a finite set S of rational primes, and strictly compatible systems of semisimple Galois representations

$$\rho_\lambda(\pi) : G_{\mathbb{Q}} \to \mathrm{GL}_m(\overline{M}_\lambda),$$
$$\rho_\lambda(\mu) : G_{\mathbb{Q}} \to \overline{M}_\lambda^{\times},$$

where λ ranges over all finite places of M (together with fixed embeddings $M \hookrightarrow M_\lambda \hookrightarrow \overline{M}_\lambda$, where $\overline{M}_\lambda$ is an algebraic closure of the localisation M_λ of M at λ) such that the following properties are satisfied. Denote by ℓ the rational prime lying below λ.

1. $\rho_\lambda(\pi) \cong \rho_\lambda(\pi)^{\vee} \otimes \chi_\ell^{1-m} \rho_\lambda(\mu)$, where χ_ℓ denotes the ℓ-adic cyclotomic character.
2. The representations $\rho_\lambda(\pi)$ and $\rho_\lambda(\mu)$ are unramified outside $S \cup \{\ell\}$.
3. Locally at ℓ, the representations $\rho_\lambda(\pi)$ and $\rho_\lambda(\mu)$ are de Rham, and if $\ell \notin S$, they are crystalline.
4. $\rho_\lambda(\pi)$ is regular, with Hodge-Tate weights $\{a_1 + (m-1), a_2 + (m-2), \ldots, a_m\}$.
5. Fix any isomorphism $\iota : \overline{M}_\lambda \simeq \mathbb{C}$ compatible with the inclusion $M \subset \mathbb{C}$. Then
$$\iota\, \mathrm{WD}(\rho_\lambda(\pi)|_{G_{\mathbb{Q}_p}})^{\mathrm{F-ss}} \cong \mathrm{rec}(\pi_p \otimes |\mathrm{Det}|_p^{(1-m)/2}). \tag{4.1}$$
Here WD denotes the Weil-Deligne representation attached to a representation of $G_{\mathbb{Q}_p}$, $\mathrm{F-ss}$ means the Frobenius semisimplification, and rec is the notation for the (unitarily normalised) Local Langlands Correspondence.

The properties (1)–(5) above give us some information about the compatible system $(\rho_\bullet(\pi))$. If we want to realise groups in a given family of finite linear groups as Galois groups over $\mathbb{Q}$, we will need to find a suitable RAESDC automorphic representation such that the information provided by (1)–(5) allows us to ensure that the images of the corresponding residual representations $\overline{\rho}_\lambda(\pi)$ belong to this family. We can already make some remarks in this connection. For example, (1) implies that the image of $\rho_\lambda(\pi)$ lies in an orthogonal or symplectic group. (2) provides us with a

strong control on the ramification of the Galois realisation that we obtain. This is a characteristic feature of this strategy of addressing the inverse Galois problem. (3) and (4) are of a technical nature, and we will not mention them in the rest of the survey (except briefly in connection to the proof of Theorem 5.3). Instead, let us expand on the last property (5). Any π as above can be written as a certain restricted product of local components π_p, where p runs through the places of $\mathbb{Q}$. Equation (4.1), with is highly involved notation, is essentially telling us that this local component π_p determines the restriction of $\rho_\lambda(\pi)$ to a decomposition group $G_p \subset G_\mathbb{Q}$ at the prime p. As we will see in the next section, the possibility of prescribing the restriction of $\rho_\lambda(\pi)$ to G_p for a finite number of primes $p \neq \ell$ will be the essential ingredient for controlling the image of $\overline{\rho}_\lambda(\pi)$.

5 Main statements and ingredients of proof

In this section we state several results obtained through the strategy described in Section 3, that generalise Theorems 3.3 and 3.4 to $2n$-dimensional representations. The first result, due to C. Khare, M. Larsen and G. Savin (cf. [18]), can be encompassed in the vertical direction, as explained in Section 3.

Theorem 5.1 (Khare, Larsen, Savin)**.** *Fix $n, t \in \mathbb{N}$ and a prime ℓ. Then there exists a natural number r divisible by t such that either $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ or $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$ occurs as a Galois group over $\mathbb{Q}$.*

More precisely, there exists an irreducible Galois representation $\rho_\ell : G_\mathbb{Q} \to \mathrm{GSp}_{2n}(\overline{\mathbb{Q}}_\ell)$, unramified outside ℓ and an auxiliary prime q, such that the image of $\overline{\rho}_\ell^{\mathrm{proj}}$ is either $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ or $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$.

We also want to mention the following result, dealing with different families of linear groups (cf. [19]).

Theorem 5.2 (Khare, Larsen, Savin)**.** *Fix $t \in \mathbb{N}$ and a prime ℓ.*

1. *There exists an integer r divisible by t such that $G_2(\mathbb{F}_{\ell^r})$ can be realised as a Galois group over $\mathbb{Q}$.*
2. *Assume that ℓ is odd. There exists an integer r divisible by t such that either the group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^r})^{\mathrm{der}}$ or $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^r})$ can be realised as a Galois group over $\mathbb{Q}$.*
3. *Assume that $\ell \equiv 3, 5 \pmod 8$. There exists an integer r divisible by t such that the group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^r})^{\mathrm{der}}$ can be realised as a Galois group over $\mathbb{Q}$.*

In the horizontal direction there is the following result for symplectic groups, due to S. A., L. Dieulefait, S.-W. Shin and G. Wiese (cf. [3]).

Theorem 5.3 (A., Dieulefait, Shin, Wiese)**.** *Fix $n, r \in \mathbb{N}$. There exists a set of rational primes of positive density such that, for every prime ℓ in this set, the group $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ or $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$ can be realised as a Galois group over $\mathbb{Q}$.*

More precisely, there exists an irreducible Galois representation $\rho_\ell : G_\mathbb{Q} \to \mathrm{GSp}_{2n}(\overline{\mathbb{Q}}_\ell)$, unramified outside ℓ and two auxiliary primes, such that the image of $\overline{\rho}_\ell^{\mathrm{proj}}$ is either $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^r})$ or $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^r})$.

Note that, in [10], the authors can control whether the image is PSL or PGL because they choose their modular form in such a way that it does not have any nontrivial inner twist. Currently, this has not been generalised to $n > 1$.

In both results, there are essentially two different parts: on the one hand, one needs to find conditions on a compatible system of symplectic Galois representations to ensure that the images of the residual representations corresponding to the members of the system will be huge. On the other hand, one needs to show the existence of RAESDC automorphic representations whose

compatible systems satisfy the desired conditions. In [18], the existence of appropriate automorphic representations is shown by means of Poincaré series, which give automorphic representations on $\mathrm{SO}_{2n+1}(\mathbb{A}_{\mathbb{Q}})$. These are transferred to $\mathrm{GL}_{2n}(\mathbb{A}_{\mathbb{Q}})$ by means of Langlands functoriality. In [3], the existence of the desired automorphic representations is shown by exploiting results of S.-W. Shin on equidistribution of local components at a fixed prime in the unitary dual with respect to the Plancherel measure (cf. [33]).

In the rest of the section, we will expand on the first question, namely, on conditions on symplectic compatible systems that allow some control on the images of the residual representations corresponding to the members of the system. A first property of the image that we want to ensure is irreducibility. In both [18] and [3], this is achieved by means of a tamely ramified symplectic local parameter. More precisely, fix a prime ℓ, and let p, q be auxiliary primes such that the order of q modulo p is exactly $2n$. Let $\mathbb{Q}_{q^{2n}}$ be the unique unramified extension of $\mathbb{Q}_q$ of degree $2n$. Using class field theory, it can be proven that there exists a character $\chi_q : G_{\mathbb{Q}_{q^{2n}}} \to \overline{\mathbb{Q}}_\ell^\times$ of order $2p$ such that (1) the restriction of χ_q to the inertia group $I_{\mathbb{Q}_{q^{2n}}}$ has order exactly p; (2) $\chi_q(\mathrm{Frob}_{q^{2n}}) = -1$. Then it follows that the Galois representation $\rho_q := \mathrm{Ind}_{G_{\mathbb{Q}_{q^{2n}}}}^{G_{\mathbb{Q}_q}} \chi_q$ is irreducible and can be conjugated to take values inside $\mathrm{Sp}_{2n}(\overline{\mathbb{Q}}_\ell)$. As a consequence, we obtain the following result:

Lemma 5.4. *Let $(\rho_\bullet)$ be a $2n$-dimensional compatible system of Galois representations of $G_{\mathbb{Q}}$ as in Definition 3.1. Let p, q two primes such that the order of q modulo p is exactly $2n$. Let $G_q \subset G_{\mathbb{Q}}$ be a decomposition group at q, and assume that, for all primes λ of L which do not lie above p or q, we have*

$$\mathrm{Res}_{G_q}^{G_{\mathbb{Q}}} \rho_\lambda \simeq \mathrm{Ind}_{G_{\mathbb{Q}_{q^{2n}}}}^{G_{\mathbb{Q}_q}} \chi_q,$$

where ℓ is the rational prime below λ and $\chi_q : G_{\mathbb{Q}_{q^{2n}}} \to \overline{\mathbb{Q}}_\ell$ is a character as above. Then $\overline{\rho}_\lambda$ is irreducible.

More precisely, the image of $\overline{\rho}_\lambda$ contains a so-called $(2n, p)$-group (cf. [18] for the definition of this notion). Given a prime ℓ, if one chooses the auxiliary primes p and q in an appropiate way, it is possible to ensure that the image of $\overline{\rho}_\lambda$ is huge (i.e., it contains $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$). This idea appeared originally in the work of C. Khare and J.-P. Wintenberger on Serre's Modularity Conjecture for $n = 1$, and has been exploited in [35] and [18]. Let us briefly sketch how it works in the case when $n = 1$. Assume that we have a representation $\overline{\rho}_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, satisfying that the restriction of $\overline{\rho}_\lambda$ to a decomposition group at q is isomorphic to $\mathrm{Ind}_{G_{\mathbb{Q}_{q^{2n}}}}^{G_{\mathbb{Q}_q}} \overline{\chi}_q$. Consider the composition $\overline{\rho}_\lambda^{\mathrm{proj}}$ of $\overline{\rho}_\lambda$ with the projection $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. We certainly know that the image of $\overline{\rho}_\lambda^{\mathrm{proj}}$ is a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. L. E. Dickson has classified all finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ into four types of groups: a subgroup $H \subset \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ is either (1) equal to $\mathrm{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ for some r; or (2) a reducible subgroup; or (3) a dihedral subgroup D_s for some integer s coprime to ℓ; or (4) isomorphic to one of the alternating groups A_4, A_5 or the symmetric group S_4.

Since we know that the image of $\overline{\rho}_\lambda$ contains the subgroup $\overline{\rho}_\lambda(G_q)$, which is the dihedral group D_p, we can immediately exclude the possibilities (2) and (4) (provided p is large enough so that it does not divide the cardinality of A_5 and S_4). To conclude that the image of $\overline{\rho}_\lambda$ is huge, we have to exclude the case that it is a dihedral group. Assume then that this is the case. Then $\overline{\rho}_\lambda = \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \psi$ for some quadratic field extension $K/\mathbb{Q}$. In addition, we know that $\mathrm{Res}_{G_q}^{G_{\mathbb{Q}}} \overline{\rho}_\lambda \simeq \mathrm{Ind}_{G_{\mathbb{Q}_{q^{2n}}}}^{G_{\mathbb{Q}_q}} \overline{\chi}_q$. Is there a way to get a contradiction? The idea is that this can be achieved, provided we choose the auxiliary primes p and q carefully. If this is the case, these two conditions will be rendered incompatible because of the relationship between p, q and ℓ. The reader interested in the details is referred to [35]. In order for this strategy to work, we must start from a prime ℓ and choose p and q accordingly. Thus, this idea is particularly well suited to address the vertical direction.

In [18] this idea is generalised to the $2n$-dimensional setting. The first difficulty that arises is that the classification of finite subgroups of $\mathrm{GL}_{2n}(\overline{\mathbb{F}}_\ell)$ is much more intrincate when $n > 1$. The main group-theoretical tool that is used in [18] is a theorem from [22], which generalises a classic

theorem of Jordan from characteristic zero to arbitrary characteristic. More precisely, let $m \in \mathbb{N}$ be an integer. Then there exists a constant $J(m)$ such that, for any finite subgroup Γ of $\mathrm{GL}_m(\overline{\mathbb{F}}_\ell)$ there exist normal subgroups $\Gamma_3 \subset \Gamma_2 \subset \Gamma_1 \subset \Gamma$ such that the index $[\Gamma : \Gamma_1] \leq J(m)$, and such that Γ_3 is an ℓ-group, Γ_2/Γ_3 is an abelian group (whose order is not divisible by ℓ) and Γ_1/Γ_2 is a direct product of finite groups of Lie type in characteristic ℓ.

Going back to the setting of Galois representations, the main idea now is that, if $\Gamma \subset \mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$ is a finite subgroup such that there is a $(2n, p)$-group contained in all normal subgroups of Γ of index smaller than or equal to a constant $d(n)$ which depends only on n (this constant will be computed in terms of the quantity $J(2n)$ mentioned above), then it follows that Γ must contain $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$. Given a prime number ℓ, by choosing the auxiliary primes p and q in a suitable way, one can ensure that if $\mathrm{Res}^{G_{\mathbb{Q}}}_{G_q} \overline{\rho}_\lambda \simeq \mathrm{Ind}^{G_{\mathbb{Q}_q}}_{G_{\mathbb{Q}_{q^{2n}}}} \overline{\chi}_q$, then the group $\Gamma = \mathrm{im}\overline{\rho}_\lambda$ satisfies that $\overline{\rho}_\lambda(G_q)$ is a $(2n, p)$-group contained in all normal subgroups of Γ of index at most $d(n)$.

Now we focus our attention on the horizontal direction. Recall that, in this setting, we are given a compatible system $(\rho_\bullet)$, and we want that the image of the members $\overline{\rho}_\lambda$ are huge for as many primes λ of L as possible. In this context, the presence of a tamely ramified local parameter at an auxiliary prime q will not suffice to obtain huge image. Since the prime ℓ is now varying, we are not allowed to choose the auxiliary primes p and q in terms of ℓ. A new idea is required.

When $n = 1$, L. Dieulefait and G. Wiese construct Hecke eigenforms f such that the compatible system of Galois representations $(\rho_{f,\bullet})$ attached to f satisfies that, for all primes λ of $\mathbb{Q}_f$, the image of $\overline{\rho}_{f,\lambda}$ is huge (cf. [10]). The idea is to choose f in such a way that the corresponding compatible system has *two* tamely ramified parameters (at two different auxiliary primes), chosen in such a way that all possibilities for the image of $\overline{\rho}^{\mathrm{proj}}_{f,\lambda}$ given by Dickson's classification (see above) except huge image are ruled out.

For the $2n$-dimensional case, however, we need a new ingredient. The main result in [3] relies on a classification of finite subgroups of $\mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$ containing a transvection. More precisely, the main result in [2] shows that, if $\Gamma \subset \mathrm{GSp}_{2n}(\overline{\mathbb{F}}_\ell)$ is a finite subgroup which contains a (nontrivial) transvection, then either (1) Γ is a reducible subgroup; or (2) Γ is imprimitive; or (3) Γ is huge. The first possibility can be ruled out by introducing a tamely ramified parameter in the compatible system $(\rho_\bullet)$. The imprimitive case corresponds to the situation when ρ_λ is induced from some field extension $K/\mathbb{Q}$. To rule out this case, one needs to choose the auxiliary primes p and q in the tamely ramified parameter in a suitable way. If the compatible system is regular (in the sense that the tame inertia weights of $\overline{\rho}_\lambda$ are independent of λ and different, cf. [2] for a precise definition), then the second case in the classification can be ruled out, and the conclusion that the image of $\overline{\rho}_\lambda$ is huge can be drawn.

The question remains whether it is possible to enforce a compatible system $(\rho_\bullet)$ of Galois representations to satisfy, by means of a local condition, that the images of the residual representations $\overline{\rho}_\lambda$ contain a transvection. Recall that in Section 3, transvections already appeared in connection with the image of the Galois representation attached to the group of ℓ-torsion points of an abelian variety A defined over $\mathbb{Q}$. In this setting, to ensure that the image of $\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$ contains a transvection, C. Hall exploited the fact that, if A has a certain type of reduction at an auxiliary prime p_1, then the image of the inertia group at p_1 under $\overline{\rho}_{A,\ell}$ already contains a transvection. In the case of $2n$-dimensional compatible systems of Galois representations, the transvection can be obtained by imposing that the restriction of ρ_λ to a decomposition group at an auxiliary prime p_1 has a prescribed shape. Equivalently, this amounts to specifying the Weil-Deligne representation attached to the restriction of ρ_λ to G_{p_1}. If the compatible system $(\rho_\bullet(\pi))$ is attached to a RAESDC automorphic representation π, this condition can be expressed in terms of π. Here it is very important that the local component π_{p_1} of π determines, via the Local Langlands correspondence, not only the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_{p_1})$ for $\lambda \nmid p_1$, but the whole restriction $\rho_\lambda(\pi)|_{G_{p_1}}$. Moreover, one has to take care that the transvection in the image of $\rho_\lambda(\pi)$ does not become trivial under reduction modulo λ. In [3], the authors ensure that, for a density one set of rational primes ℓ and for every $\lambda|\ell$, the transvection is preserved after reduction modulo λ. The main tool they use is a level lowering result from [4], which they apply over infinitely many quadratic CM number fields.

Up to this point, we have sketched the main ideas in [35], [18] and [10], [3] to prove the existence of compatible systems of Galois representations $(\rho_\bullet)$ such that the images of the residual representations $\overline{\rho}_\lambda$ are huge, i.e., containing $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$. For the applications to the inverse Galois problem, we need a certain control of the largest exponent r such that $\mathrm{Sp}_{2n}(\mathbb{F}_{\ell^r})$ is contained in the image of $\overline{\rho}_\lambda$. We already remarked in Section 2 that, in the case of Galois representations attached to a Hecke eigenform f, this is linked to the knowledge of the coefficient field $\mathbb{Q}_f$, which proves to be a difficult task. However, even though it may be difficult to determine precisely what the coefficient field L of the compatible system is, it is possible to ensure that it contains a large subfield. In fact, the tamely ramified parameter at the prime q provides already a lower bound on the size of r. For the applications in the horizontal direction, one exploits that if $L/\mathbb{Q}$ contains a cyclic subextension $K/\mathbb{Q}$ of degree r, then there exists a positive density set of primes ℓ such that, at some prime λ of L above ℓ, the extension $L/\mathbb{Q}$ has the desired residue degree r.

References

[1] Sara Arias-de-Reyna, Luis Dieulefait and Gabor Wiese. *Compatible systems of symplectic Galois representations and the inverse Galois problem I. Images of projective representations.* Preprint arXiv:1203.6546 (2013).

[2] 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.* Preprint arXiv:1203.6552 (2013).

[3] Sara Arias-de-Reyna, Luis Dieulefait, Sug Woo Shin and Gabor Wiese. *Compatible systems of symplectic Galois representations and the inverse Galois problem III. Automorphic construction of compatible systems with suitable local properties.* Preprint arXiv: arXiv:1308.2192 (2013).

[4] Thomas Barnet-Lamb, Toby Gee, David Geraghty and Richard Taylor. *Potential automorphy and change of weight.* Annals of Mathematics, to appear (2013).

[5] Daniel Bump. *Automorphic forms and representations.* Cambridge Studies in Advanced Mathematics, **55**. Cambridge University Press, Cambridge, 1997.

[6] John E. Cremona. *Algorithms for modular elliptic curves.* Second edition. Cambridge University Press, Cambridge, 1997.

[7] Pierre Deligne. *Formes modulaires et représentations ℓ-adiques.* Séminaire Bourbaki vol. 1968/69 Exposé 355, Lecture Notes in Mathematics Volume **179**, 1971.

[8] Pierre Deligne and Jean-Pierre Serre. *Formes modulaires de poids 1.* Ann. Sci. École Norm. Sup. **7** (1974), pages 507–530.

[9] Fred Diamond and Jerry Shurman. *A first course in modular forms.* Graduate Texts in Mathematics, **228**. Springer-Verlag, New York, 2005.

[10] Luis Dieulefait and Gabor Wiese. *On modular forms and the inverse Galois problem.* Trans. Amer. Math. Soc. **363** (2011), no. 9, 4569–4584.

[11] Chris Hall. *An open-image theorem for a general class of abelian varieties.* With an appendix by Emmanuel Kowalski. Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711.

[12] Guy Henniart. *Représentations ℓ-adiques abéliennes.* Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981), pp. 107–126, Progr. Math., **22**, Birkhäuser Boston, Boston, MA, 1982.

[13] David Hilbert. *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.* J. Reine Angew. Math. , **110**, 104–129, 1892.

[14] Chun Yin Hui. *Monodromy of Galois representations and equal-rank subalgebra equivalence.* Preprint arXiv:1204.5271 (2013).

[15] Chun Yin Hui and Michael Larsen. *Type A Images of Galois Representations and Maximality.* Preprint arXiv:1305.1989 (2013).

[16] Masatoshi Ikeda. *Completeness of the absolute Galois group of the rational number field.* J. Reine Angew. Math. **291** (1977), 1–22.

[17] Moshe Jarden and Jürgen Ritter, *On the characterization of local fields by their absolute Galois groups.* J. Number Theory **11** (1979), no. 1, 113.

[18] Chandrashekhar Khare, Michael Larsen and Gordan Savin. *Functoriality and the inverse Galois problem.* Compos. Math. **144** (2008), no. 3, 541–564.

[19] Chandrashekhar Khare, Michael Larsen and Gordan Savin. *Functoriality and the inverse Galois problem. II. Groups of type B_n and G_2.* Ann. Fac. Sci. Toulouse Math. (6) **19** (2010), no. 1, 37–70.

[20] Michael J. Larsen. *Maximality of Galois actions for compatible systems.* Duke Math. J. **80** (1995), no. 3, 601–630.

[21] Michael J. Larsen and Richard Pink. *On ℓ-independence of algebraic monodromy groups in compatible systems of representations.* Invent. Math. **107** (1992), no. 3, 603–636.

[22] Michael J. Larsen and Richard Pink. *Finite subgroups of algebraic groups.* J. Amer. Math. Soc. **24** (2011), no. 4, 1105–1158.

[23] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg. *Cohomology of number fields.* Second edition. Grundlehren der Mathematischen Wissenschaften, **323**. Springer-Verlag, Berlin, 2008.

[24] Kenneth A. Ribet. *On ℓ-adic representations attached to modular forms.* Invent. Math. **28** (1975), 245–275.

[25] Kenneth A. Ribet. *On ℓ-adic representations attached to modular forms. II.* Glasgow Math. J. **27** (1985), 185–194.

[26] Peter Scholze. *On torsion in the cohomology of locally symmetric varieties.* Preprint arXiv:1306.2070 (2013).

[27] Jean-Pierre Serre. *Représentations ℓ-adiques.* Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), pp. 177–193. Japan Soc. Promotion Sci., Tokyo, 1977.

[28] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves.* McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute W. A. Benjamin, Inc., New York-Amsterdam 1968.

[29] Jean-Pierre Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15** (1972), no. 4, 259–331.

[30] Jean-Pierre Serre. *Lettre à Ken Ribet du 1/1/1981.* In *Oeuvres. Collected papers. IV. 19851998.* Springer-Verlag, Berlin, 2000.

[31] Jean-Pierre Serre. *Résumé des course 1984–1985.* In *Oeuvres. Collected papers. IV. 19851998.* Springer-Verlag, Berlin, 2000.

[32] Jean-Pierre Serre. *Topics in Galois theory.* Second edition. Research Notes in Mathematics, 1. A K Peters, Ltd., Wellesley, MA, 2008.

[33] Sug Woo Shin. *Automorphic Plancherel density theorem.* Israel J. Math. **192** (2012), no. 1, 83–120.

[34] Kôji Uchida. *Isomorphisms of Galois groups.* J. Math. Soc. Japan **28** (1976), no. 4, 617–620.

[35] Gabor Wiese. *On projective linear groups over finite fields as Galois groups over the rational numbers.* Modular forms on Schiermonnikoog, 343–350, Cambridge Univ. Press, Cambridge, 2008.

[36] Gabor Wiese. *An Application of Maeda's Conjecture to the Inverse Galois Problem.* Math. Res. Letters, to appear (2013).

[37] Shuji Yamagata. *A counterexample for the local analogy of a theorem by Iwasawa and Uchida.* Proc. Japan Acad. **52** (1976), no. 6, 276–278.