ANNALES
DE LA FACULTÉ
DES SCIENCES
DE
TOULOUSE
Mathématiques

Chandrashekhar Khare, Michael Larsen, Gordan Savin

Functoriality and the Inverse Galois problem II: groups of type B_n and G_2

Tome XIX, nº 1 (2010), p. 37-70.

<http://afst.cedram.org/item?id=AFST_2010_6_19_1_37_0>

Annales de la Faculté des Sciences de Toulouse Vol. XIX, n° 1, 2010
pp. 37–70

Functoriality and the Inverse Galois problem II: groups of type B_n and G_2

Chandrashekhar Khare[1], Michael Larsen[2], Gordan Savin[3]

Résumé. — Cet article donne une application du principe de fonctorialité de Langlands au problème classique suivant : quels groupes finis, en particulier quels groupes simples, apparaissent comme groupes de Galois sur $\mathbb{Q}$? Soit ℓ une nombre premier et t un entier positif. Nous montrons que les groupes finis simples de type de Lie $B_n(\ell^k) = 3DSO_{2n+1}(\mathbb{F}_{\ell^k})^{der}$ lorsque $\ell \equiv 3, 5 \pmod 8$ et $G_2(\ell^k)$ sont des groupes de Galois sur $\mathbb{Q}$ pour un entier k divisant t. En particulier, pour chacun de ces deux types de Lie et pour un entier ℓ fixé, nous construisons une infinité de groupes de Galois, mais nous n'avons pas de contrôle précis sur k.

Abstract. — This paper contains an application of Langlands' functoriality principle to the following classical problem: which finite groups, in particular which simple groups appear as Galois groups over $\mathbb{Q}$? Let ℓ be a prime and t a positive integer. We show that that the finite simple groups of Lie type $B_n(\ell^k) = 3DSO_{2n+1}(\mathbb{F}_{\ell^k})^{der}$ if $\ell \equiv 3, 5 \pmod 8$ and $G_2(\ell^k)$ appear as Galois groups over $\mathbb{Q}$, for some k divisible by t. In particular, for each of the two Lie types and fixed ℓ we construct infinitely many Galois groups but we do not have a precise control of k.

[*] Reçu le 11/07/08, accepté le 24/03/09

[1] Department of Mathematics, UCLA, Los Angeles CA 90095-1555, U.S.A.
shekhar@math.utah.edu

CK was partially supported by NSF grants DMS 0355528 and DMS 0653821, the Miller Institute for Basic Research in Science, University of California Berkeley, and a Guggenheim fellowship.

[2] Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.
larsen@math.indiana.edu

ML was partially supported by NSF grant DMS 0354772.

[3] Department of Mathematics, University of Utah, 155 South 1400 East, Room 233, Salt Lake City, UT 84112-0090, U.S.A.
savin@math.utah.edu

GS was partially supported by NSF grant DMS 0551846.

1. Introduction

1.1. Earlier work

Let ℓ be a prime. In our previous work [KLS], which generalised a result of Wiese [W], the Langlands functoriality principle was used to show that for every positive integer t there exists a positive integer k divisible by t such that either the finite simple group $\mathrm{C}_n(\ell^k) = \mathrm{PSp}_{2n}(\mathbb{F}_{\ell^k})$ or $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^k})$ (see also §13) is the Galois group of an extension of $\mathbb{Q}$ unramified outside $\{\ell, q, \infty\}$ where $q \neq 2$ is a prime that depends on t. The construction is based on the following three steps.

1. Starting with a cuspidal automorphic representation on the split group SO_{2n+1} constructed using the Poincaré series, we use the global lift of Cogdell, Kim, Piatetski-Shapiro and Shahidi [CKPS] and results of Jiang and Soudry [JS1] to obtain a self-dual cuspidal automorphic representation Π of $\mathrm{GL}_{2n}(\mathbb{A})$, with $\mathbb{A}$ the adeles of $\mathbb{Q}$, such that the following three conditions hold:
   - Π_∞ is cohomological.
   - Π_q is a supercuspidal representation of depth 0.
   - Π_v is unramified for all primes $v \neq \ell, q$.
2. The work of Kottwitz, Clozel, Harris-Taylor and Taylor-Yoshida yields the following theorem (see [Ty, Th. 3.6] or [Ha, Th. 1.1]). We use the conventions and notations of [Ha, §1].

   THEOREM 1.1. — *Let m be a positive integer, and let Π be a self-dual cuspidal automorphic representation Π of $\mathrm{GL}_m(\mathbb{A})$ such that Π_∞ is cohomological. Assume that for some finite place v_0 of $\mathbb{Q}$, Π_{v_0} is square integrable. Then attached to Π and a choice of an embedding $\iota : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$, there is an irreducible ℓ-adic representation $r'_\Pi : G_{\mathbb{Q}} \to \mathrm{GL}_m(\bar{\mathbb{Q}}_\ell)$ of the Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ such that for all primes v of $\mathbb{Q}$ of residue characteristic $\neq \ell$ we have:*

   $$WD_v(r'_\Pi)^{\mathrm{Frob-ss}} = \mathcal{L}(\Pi_v \otimes |\ |_v^{\frac{1-m}{2}}).$$

   Here $WD_v(r'_\Pi)$ is the Weil-Deligne parameter of $r'_\Pi|_{D_v}$ with D_v a decomposition group at v, $\mathcal{L}$ is the normalised local Langlands correspondence, and $Frob - ss$ denotes Frobenius semi-simplification.

   Remark. — Let χ_ℓ be the ℓ-adic cyclotomic character. If $m = 2n+1$ we consider a twist $r_\Pi = r'_\Pi \otimes \chi_\ell^n$ and note that we have

   $$WD_v(r_\Pi)^{\mathrm{Frob-ss}} = \mathcal{L}(\Pi_v).$$

3. The last step consists of reducing r'_Π modulo ℓ. The parameter of Π_q can be picked so that $r_\Pi(G_{\mathbb{Q}_q})$ is a metacyclic group deeply embedded in $r'_\Pi(G_\mathbb{Q})$ [KW]. That is, for some large positive integer d, $r'_\Pi(G_{\mathbb{Q}_q})$ is contained in every normal subgroup of $r'_\Pi(G_\mathbb{Q})$ of index less than or equal to d. This property is crucial to assure, using the main result of [LP], that the reduction modulo ℓ is a group either of type $\mathrm{PSp}_{2n}(\mathbb{F}_{\ell^k})$ or $\mathrm{PGSp}_{2n}(\mathbb{F}_{\ell^k})$.

1.2. Main theorem

The purpose of this work is to extend these results and to construct finite simple groups of type B_n and G_2 as Galois groups over $\mathbb{Q}$. In the case of G_2, our result depends on a recent technical improvement of Theorem 1.1 due to Shin [Sh] in the case that m is odd. He shows that we may drop the hypothesis of the existence of a place v_0 such that Π_{v_0} is square integrable. The resulting representation r'_Π is semi-simple although it is expected to be irreducible.

We can state our main theorem:

Theorem 1.2. — *Let t be a positive integer.*

1. *Let ℓ be a prime. Then there exists an integer k divisible by t such that the simple group $\mathrm{G}_2(\mathbb{F}_{\ell^k})$ appears as a Galois group over $\mathbb{Q}$.*
2. *Let ℓ be an odd prime. Then there exists an integer k divisible by t such that the finite simple group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ or the finite classical group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})$ appears as a Galois group over $\mathbb{Q}$.*
3. *If $\ell \equiv 3, 5 \pmod 8$, then there exists an integer k divisible by t such that the finite simple group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ appears as a Galois group over $\mathbb{Q}$.*

1.3. Sketch of proof

The construction of Galois groups in Theorem 1.2 is based on the functorial lift from Sp_{2n} to GL_{2n+1} [CKPS] plus the lift from G_2 to Sp_6 using the theta correspondence arising from the minimal representation of the exceptional group E_7 (see [Sa1] for a definition of the minimal representation). The main new technical difficulty in implementing the strategy of [KLS] in the present case, is that $\mathrm{GL}_{2n+1}(\mathbb{Q}_p)$ has self-dual supercuspidal representations only if $p = 2$. Thus, while we can still construct a self-dual cuspidal automorphic representation Π of GL_{2n+1} which should give rise to our desired Galois groups, the local component Π_q cannot be supercuspidal. For groups of type B_n we can remedy the situation by requiring that the local component Π_2 be supercuspidal (which we pick to be of positive depth). Existence of a global Π with such local component Π_2 is again obtained using the global lift from Sp_{2n} plus the recently announced backward lift from GL_{2n+1} to Sp_{2n} by Jiang and Soudry [JS2]. The local component Π_2 not only assures us of the existence of the ℓ-adic representation r_Π, without using new results of Shin, but it also gives us a certain control of the Galois group obtained by reducing r_Π modulo ℓ. More precisely, Π_2 can be picked so that the image of the local Langlands parameter at 2 is a finite group I in $\mathrm{GL}_{2n+1}(\mathbb{C})$ with the following properties:

- $I/[I,I] \cong \mathbb{Z}/(2n+1)\mathbb{Z}$.
- $[I,I] \cong (\mathbb{Z}/2\mathbb{Z})^{2n}$.

If $\ell \equiv 3,5 \pmod 8$ then the first property of I implies that the Galois group is $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ and not $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})$. If $n=3$ then the second property of I implies that Π_2 is not a lift from $\mathrm{G}_2(\mathbb{Q}_2)$ and the Galois group is not $\mathrm{G}_2(\mathbb{F}_{\ell^k})$.

Acknowledgments. — We would like to thank Dick Gross and Guy Henniart for helping us with irreducible supercuspidal parameters and Mark Reeder for his help with small representations of reductive groups. Thanks are also due to the referee for a careful reading of the paper and helpful suggestions.

2. Local discrete series parameters

Let k be a local field and G a connected reductive and split group over k. Conjecturally, representations of $G(k)$ correspond to (certain) homomorphisms

$$\phi : WD_k \to G^*(\mathbb{C})$$

of the Weil-Deligne group into the Langlands dual group $G^*(\mathbb{C})$. In this paper we shall be concerned with the following cases:

G	GL_n	Sp_{2n}	PGSp_6	G_2
G^*	GL_n	SO_{2n+1}	Spin_7	G_2

If $G = \mathrm{Sp}_{2n}$, it will be convenient to realize the dual group as $\mathrm{SO}(U)$ for some choice of a non-degenerate complex orthogonal space U of dimension

$2n+1$. Then a discrete series parameter for $\mathrm{Sp}_{2n}(k)$ is a homomorphism $\phi : WD_k \to \mathrm{SO}(U)$ such that, under the action of WD_k, the orthogonal space U decomposes into irreducible summands

$$U = U_1 \oplus \cdots \oplus U_s,$$

where each U_i is a non-degenerate orthogonal subspace of U. Moreover, if ϕ_i denotes the representation of WD_k on U_i, then $\phi_i \cong \phi_j$ if and only if $i = j$. In other words, we are requiring that the image of WD_k is not contained in a proper Levi factor in G^*.

Consider now the case $k = \mathbb{R}$. In this case the Weil-Deligne group is the same as the Weil group $W_{\mathbb{R}}$. For every non-zero integer a let η_a be a character of $W_{\mathbb{C}} \cong \mathbb{C}^\times$ defined by

$$\eta_a(z) = \left(\frac{z}{\bar{z}}\right)^a .$$

Let

$$\phi(a) = \mathrm{Ind}_{W_{\mathbb{C}}}^{W_{\mathbb{R}}} \eta_a .$$

This is an irreducible and orthogonal 2-dimensional representation of $W_{\mathbb{R}}$. Its determinant is the unique non-trivial quadratic character χ_∞ of $W_{\mathbb{R}}^{ab} \cong \mathbb{R}^\times$. Write $\phi(a_1, \dots, a_n))$ for a direct sum $\phi(a_1) \oplus \cdots \oplus \phi(a_n)$ where $a_1, \dots, a_n$ are non-zero integers. If $a_i \neq \pm a_j$ for $i \neq j$ then

$$\phi(a_1, \dots, a_n) \oplus \chi_\infty^n$$

is a discrete series parameter for the group $\mathrm{Sp}_{2n}(\mathbb{R})$. Note that the choice of exponent n in the last summand is made so that the image of the parameter is contained in $\mathrm{SO}_{2n+1}(\mathbb{C})$. Note also that the parameter is determined by, and determines, the a_i's up to permutation of indices and change of signs. If $n = 3$, then the image of the parameter is contained in $\mathrm{G}_2(\mathbb{C}) \subset \mathrm{SO}_7(\mathbb{C})$ if and only if

$$a_1 + a_2 + a_3 = 0$$

for some choices of signs of a_i's. Let σ_∞ be a generic discrete series representation of $\mathrm{Sp}_{2n}(\mathbb{R})$ (or of $\mathrm{G}_2(\mathbb{R})$) corresponding to this parameter.

Let Π_∞ be the lift of σ_∞ to $\mathrm{GL}_{2n+1}(\mathbb{R})$. The infinitesimal character of Π_∞ is represented by a $2n+1$-tuple

$$(a_1, \dots, a_n, -a_1, \dots, -a_n, 0).$$

In particular, Π_∞ is cohomological, as defined by Clozel [Cl].

3. Depth zero generic supercuspidal representations

Let q be an odd prime. Let $\Omega_{q'}$ denote the set of all complex roots of unity of order prime to q. The Frobenius acts on $\Omega_{q'}$ by

$$F(\tau) = \tau^q$$

for every τ in $\Omega_{q'}$. Note that all F-orbits are finite. These orbits play a key role in the description of tame parameters.

Lemma 3.1. — *Let τ be a root of 1 different from ± 1. Assume that the F-orbit of τ has m different elements:*

$$\tau, \tau^q, \ldots, \tau^{q^{m-1}}.$$

If τ^{-1} is on this list, that is, if $\tau^{-1} = \tau^{q^n}$ for some $n < m$ then $m = 2n$.

Proof. — First of all, note that $0 < n$ since $\tau \neq \pm 1$. Raising $\tau^{-1} = \tau^{q^n}$ to the q^n-th power gives $\tau = \tau^{q^{2n}}$. Since $\tau = \tau^{q^k}$ if and only if k is a multiple of m, and $0 < 2n < 2m$, it follows that $m = 2n$, as claimed. □

We are now ready to define irreducible tame self-dual parameters of $\mathrm{Sp}_{2n}(\mathbb{Q}_q)$. Let $\mathbb{Q}_{q^{2n}}$ be the unique unramified extension of $\mathbb{Q}_q$ of degree $2n$. Then

$$\mathbb{Q}_{q^{2n}}^\times = \langle q \rangle \times \mathbb{F}_{q^{2n}}^\times \times U_1$$

where U_1 is the maximal pro q-subgroup of $\mathbb{Q}_{q^{2n}}^\times$. A character of $\mathbb{Q}_{q^{2n}}^\times$ is called tame if it is trivial on U_1. Let ζ_{2n} be a primitive root in $\mathbb{F}_{q^{2n}}^\times$. Pick τ, a complex root of 1 such that the F-orbit $\tau, \tau^q, \ldots$ has precisely $2n$ distinct elements and $\tau^{q^n} = \tau^{-1}$. (For example, τ can be picked a primitive root of order $q^n + 1$.) Then τ defines a tame character η of $\mathbb{Q}_{q^{2n}}^\times$ by

$$\begin{cases} \eta(\zeta_{2n}) = \tau \\ \eta(q) = 1. \end{cases}$$

Let $W_{\mathbb{Q}_q}$ and $W_{\mathbb{Q}_{q^{2n}}}$ be the local Weil groups of $\mathbb{Q}_q$ and $\mathbb{Q}_{q^{2n}}$. Recall that

$$W_{\mathbb{Q}_q} / W_{\mathbb{Q}_{q^{2n}}} \cong \mathrm{Gal}(\mathbb{F}_{q^{2n}} / \mathbb{F}_q).$$

Via local class field theory we have an identification $W_{\mathbb{Q}_{q^{2n}}}^{ab} \cong \mathbb{Q}_{q^{2n}}^\times$. Note that $\eta \circ F^i \neq \eta$ for $1 < i \leqslant 2n$ and $\eta \circ F^n = \bar{\eta}$. In particular, the character η defines an irreducible, orthogonal $2n$-dimensional representation

$$\phi(\tau) = \mathrm{Ind}_{W_{\mathbb{Q}_{q^{2n}}}}^{W_{\mathbb{Q}_q}} (\eta).$$

of $W_{\mathbb{Q}_q}$. We note that the determinant of $\phi(\tau)$ is the unique unramified quadratic character χ_q of $W_{\mathbb{Q}_q}^{ab} \cong \mathbb{Q}_q^\times$.

Pick a sequence $\tau_1, \ldots, \tau_s$ of roots in $\Omega_{q'}$ belonging to different F-orbits of order $2n_1, \ldots, 2n_s$ such that $\tau^{q^{n_i}+1} = 1$ for every i and $2n_1 + \cdots + 2n_s = 2n$. Corresponding to this we have a tame regular discrete series parameter for the split group $\mathrm{Sp}_{2n}(\mathbb{Q}_q)$

$$\phi = \phi(\tau_1, \ldots, \tau_s) \oplus \chi_q^s$$

where, as in the case of real groups, the exponent s is picked to assure that the image of the parameter is contained in $\mathrm{SO}_{2n+1}(\mathbb{C})$. Note that the image $\phi(I_q)$ of the inertia subgroup $I_q \subseteq W_{\mathbb{Q}_q}$ is contained in a maximal torus of $\mathrm{SO}_{2n+1}(\mathbb{C})$ and $\phi(F)$ is an elliptic element of the Weyl group. If $s = 1$, for example, then the image of the inertia is a cyclic group generated by an element whose eigenvalues are

$$\tau, \tau^q, \ldots, \tau^{q^n}, \tau^{-1}, \ldots, \tau^{-q^n}, 1$$

and $\phi(F)$ correspond to the Coxeter element in the Weyl group.

Proposition 3.2. — *The image of a tame regular discrete series parameter $\phi = \phi(\tau_1, \ldots, \tau_s) \oplus \chi_q^s$ of $\mathrm{Sp}_6(\mathbb{Q}_q)$ is contained in $\mathrm{G}_2(\mathbb{C})$ if and only if one of the following two conditions holds:*

1. *$s = 3$ and $\tau_1\tau_2\tau_3 = 1$, for some choices of $\tau_i^{\pm}$ (F-orbit of τ_i consists of τ_i and τ_i^{-1}).*
2. *$s = 1$ and τ satisfies $\tau^{q^2-q+1} = 1$. (Recall that τ, a priori, satisfies a weaker condition $\tau^{q^3+1} = 1$.)*

Proof. — The weights of the 7-dimensional representation of $\mathrm{G}_2(\mathbb{C})$ are 0 and six short roots. Pick three short roots α_1, α_2 and α_3 such that $\alpha_1 + \alpha_2 + \alpha_3 = 0$. If t is a semi-simple element in $\mathrm{G}_2(\mathbb{C})$, put $\lambda_i^{\pm} = \pm\alpha_i(t)$. Then $\lambda_1^{\pm}, \lambda_2^{\pm}, \lambda_3^{\pm}$ and 1 are the eigenvalues of t in the 7-dimensional representation. Note that $\lambda_1\lambda_2\lambda_3 = 1$.

If the parameter ϕ is contained in $\mathrm{G}_2(\mathbb{C})$ then $\phi(F)$ corresponds to a Weyl group element in G_2 of even order. Since 2 and 6 are the only even orders of elements in the Weyl group of G_2, we see that $s = 1$ or 3. If $s = 3$ then $\phi(F)$ corresponds to -1 in the Weyl group and the condition $\lambda_1\lambda_2\lambda_3 = 1$ translates into $\tau_1\tau_2\tau_3 = 1$. If $s = 1$ then $\phi(F)$ corresponds to the Coxeter element. We can pick the Coxeter element (or alternatively the roots α_i) so that it cyclically permutes the roots

$$\alpha_1, -\alpha_2, \alpha_3, -\alpha_1, \alpha_2, -\alpha_3.$$

On the other hand, $\phi(I_q)$ is generated by a semi-simple element t with nontrvial eigenvalues $\tau, \tau^q, \tau^{q^2}, \tau^{-1}, \tau^{-q}, \tau^{-q^2}$ which $\phi(F)$ permutes cyclically in the given order. In particular, the condition $\lambda_1\lambda_2\lambda_3 = 1$ translates into $\tau^{1-q+q^2} = 1$, as desired. Conversely, if the parameter satisfies the conditions of (1) and (2) then we can factor ϕ through $\mathrm{G}_2(\mathbb{C})$ since -1 and the Coxeter element can be lifted from the Weyl group to $\mathrm{G}_2(\mathbb{C})$. □

Let σ_q be *a* generic supercuspidal representation of $\mathrm{Sp}_{2n}(\mathbb{Q}_q)$ (or of $\mathrm{G}_2(\mathbb{Q}_q)$) corresponding, via DeBacker-Reeder, to a tame parameter as above. Then the lift of σ_q to $\mathrm{GL}_{2n+1}(\mathbb{Q}_q)$ [Sa2] is

$$\Pi_1 \times \cdots \times \Pi_s \times \chi_q^s.$$

This is a tempered representation parabolically induced from supercuspidal representations $\Pi_1, \ldots, \Pi_s$ corresponding to irreducible tame paramters $\phi(\tau_1), \ldots, \phi(\tau_s)$ by the local Langlands correspondence [HT]. We note that the recipe of DeBacker-Reeder [DR] involves picking a hyperspecial compact subgroup of $\mathrm{Sp}_{2n}(\mathbb{Q}_p)$. Since there are two non-conjugate hyperspecial maximal compact subgroups here, there are two possible σ_q. They have the same lift to $\mathrm{GL}_{2n+1}(\mathbb{Q}_p)$ (by [Sa2]).

Of interest to us is the parameter of type $\phi(\tau) \oplus \chi_q$ where q and τ are picked using the following lemma (Lemma 3.4 in [KLS]):

Lemma 3.3. — *Given a positive integer $m = 2n$, a prime ℓ, a finite Galois extension K of $\mathbb{Q}$, and positive integers t and d, there exists odd primes p and q such that:*

1. *The primes ℓ, p and q are all distinct.*
2. *The prime p is greater than d.*
3. *If $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})$ contains an element of order p then $\mathbb{F}_{\ell^k}$ contains $\mathbb{F}_{\ell^t}$. In particular, t divides k.*
4. *The prime q splits completely in K.*
5. *The order of q in $\mathbb{F}_p^\times$ is exactly m.*

We shall now explain how to construct tame discrete series parameters using Lemma 3.3. Fix a positive integer $m = 2n$, a prime ℓ, and two positive integers t and d. Let K be the composite of all Galois extensions of $\mathbb{Q}$ of degree $\leqslant d$ and unramified outside $\{2, \ell, \infty\}$. This is a finite degree Galois extension of $\mathbb{Q}$ unramified outside $2, \ell, \infty$. Let p and q be the primes given by Lemma 3.3 applied to this field K. Let τ be a primitive p-th root of 1.

Since the order of q in $\mathbb{F}_p^\times$ is precisely $2n$, the Fr_q-orbit of τ gives rise to a tame parameter $\phi(\tau) \oplus \chi_q$. Moreover, if $n = 3$ then $\tau^{q^2-q+1} = 1$ since τ is of order p and p, by construction, divides $\Phi_6(q) = q^2 - q + 1$. In particular, this parameter is automatically a G_2-parameter. In any case, we note that the image of the inertia subgroup I_q is a cyclic group of order p. The image of the Weil group is a semi-direct product of the cyclic group $\mathbb{Z}/p\mathbb{Z}$ and the cyclic group $\mathbb{Z}/2n\mathbb{Z}$. This group is also called a *metacyclic* group and denoted by $\Gamma_{2n,p}$.

4. Irreducible supercuspidal parameters

As we have seen in the previous section, the image of a tame supercuspidal parameter $\varphi : W_k \to G^*$ is not irreducible when acting on the standard representation U of G^*. In particular, the lift to $\mathrm{GL}_n(k)$ ($n = \dim(U)$) of the corresponding supercuspidal representation is not supercuspidal. In order to remedy this, we need to introduce certain wildly ramified parameters. This will be done using (so-called) Jordan subgroups of the complex reductive group G^*. A Jordan subgroup J of G^* is an elementary abelian p-subgroup such that its normalizer N in G^* is a finite subgroup and J is a minimal normal subgroup of N (see [KT], page 505). The following is a partial list of Jordan subgroups.

G^*	J	N/J
SO_{2n+1}	$(\mathbb{F}_2)^{2n}$	S_{2n+1}
G_2	$(\mathbb{F}_2)^3$	$\mathrm{SL}_3(2)$

Here S_{2n+1} is the symmetric group of $2n + 1$ letters. We note that the conjugation action of N/J on J given by the standard representation of N/J on J. (In the first case we mean by this the restriction of the permutation representation of S_{2n+1} on $\mathbb{F}_2^{2n+1}$ to the hyperplane given by $\sum_{i=1}^{2n+1} x_i = 0$.) However the extension of N/J by J is not necessarily split.

We shall now construct a map $\varphi : W_{\mathbb{Q}_p} \to G^*$ such that the image of the wild inertia is J (in particular $p = 2$) and the image of $W_{\mathbb{Q}_p}$ is an intermediate subgroup $J \subseteq I \subseteq N$ acting irreducibly on the standard representation of G^*.

Let us consider the case $G^* = \mathrm{SO}_{2n+1}(\mathbb{C})$ first. Let us abbreviate $m = 2n + 1$, and let $\mathbb{Q}_{2^m}$ be the unramified extension of $\mathbb{Q}_2$ of degree m. Then

$$\mathbb{Q}_{2^m}^\times = \langle 2 \rangle \times \mathbb{F}_{2^m}^\times \times U$$

where U is a pro-2 group with a filtration $U \supset U_1 \supset U_2 \dots$ such that $U/U_1 \cong \mathbb{F}_{2^m}$. Let e be a primitive element in $\mathbb{F}_{2^m}$. Let $e_i = \mathrm{Fr}_2^{i-1}(e)$. Then

$e = e_1, e_2, \ldots, e_m$ give a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. In particular, we have fixed an isomorphism

$$U/U_1 \cong (\mathbb{F}_2)^m.$$

In this way any character of U/U_1 can be viewed as an m-tuple of signs. Let χ be the character corresponding to the m-tuple $(-,-,+,\ldots,+)$. We extend χ to $\mathbb{Q}_{2^m}^\times$ so that it is trivial on the first two factors. Since $W_{\mathbb{Q}_{2^m}}^{ab} \cong \mathbb{Q}_{2^m}^\times$ we can view χ as a character of $W_{\mathbb{Q}_{2^m}}$. Define

$$\phi_2 = \mathrm{Ind}_{W_{\mathbb{Q}_{2^m}}}^{W_{\mathbb{Q}_2}}(\chi).$$

Since the conjugates $\chi \circ \mathrm{Fr}_2^i$, for $i = 1, \ldots, m$, are mutually distinct this representation is irreducible by Mackey's criterion. Since χ is quadratic the representation ϕ_2 is also delf-dual and, since m is odd, it is orthogonal. Thus ϕ_2 defines a self-dual supercuspidal representation Π_2 of $\mathrm{GL}_{2n+1}(\mathbb{Q}_2)$ by the local Langlands correspondence.

For later purposes we need to describe the image of the representation ϕ_2. Note that the intersection of the kernels of $\chi \circ \mathrm{Fr}_2^i$ is equal to $\Delta\mathbb{F}_2$, the diagonal in $\mathbb{F}_2^m$.

Proposition 4.1. — *Recall that $m = 2n+1$. Let I be the image of $W_{\mathbb{Q}_2}$ under the representation ϕ_2. Then*

1. *$I/[I,I] \cong \mathbb{Z}/m\mathbb{Z}$.*
2. *$[I,I] \cong \mathbb{F}_2^m/\Delta(\mathbb{F}_2)$.*
3. *I is contained in a special orthogonal group.*
4. *If $m = 7$ then I is not contained in G_2.*

Proof. — Since $W_{\mathbb{Q}_2}/W_{\mathbb{Q}_{2^m}}$ is a cyclic group of order m, in order to prove the first two statements, it suffices to show that $[I,I]$ is given by the image of $W_{\mathbb{Q}_{2^m}}$. Note that the commutator of e_i and Fr_2 (for $1 \leqslant i \leqslant m$) in $W_{\mathbb{Q}_2}$ is equal to $e_i + e_{i+1}$ (where by convention we set $e_{m+1} = e_1$), considered as an element of $U/U_1 \cong \mathbb{F}_2^m$. Since m is odd, these elements generate $\mathbb{F}_2^m/\Delta(\mathbb{F}_2)$. The first two statements now follow. Since the determinant character is of order two and $I/[I,I]$ has odd order, it has to be trivial on I. This shows the third statement. Finally, if $m = 7$, then $\phi_2(e_i)$ has eigenvalues 1 (with multiplicity 5) and -1 (with multiplicity 2). Thus the eigenvalues cannot be written as $\lambda_1^{\pm 1}, \lambda_2^{\pm 1}, \lambda_3^{\pm 1}$ and 1, with $\lambda_1\lambda_2\lambda_3 = 1$. The proposition is proved. □

We now consider the Jordan subgroup in $\mathrm{G}_2(\mathbb{C})$. This is used only in §12, and thus the reader interested only in the proof of Theorem 1.2 may skip the rest of the section. Pick I, the intermediate group $J \subseteq I \subseteq N$, in advance so that I/J is the normalizer of an elliptic torus in $N/J \cong \mathrm{SL}_3(2)$. In particular, if we identify J with $\mathbb{F}_{2^3}$ then I/J can be identified as a semi-direct product of $\mathrm{Gal}(\mathbb{F}_{2^3}/\mathbb{F}_2)$ and $\mathbb{F}_{2^3}^\times$. Since the order of I/J is prime to J one easily checks that this extension splits. Note that I/J acts transitively on the set of non-trivial characters of J. Let ψ be a non-trivial additive character of $\mathbb{F}_2$. Then the composition of ψ with the trace map $\mathrm{Tr} : \mathbb{F}_{2^3} \to \mathbb{F}_2$ is an additive character of $\mathbb{F}_{2^3}$; its stabilizer in I/J is $\mathrm{Gal}(\mathbb{F}_{2^3}/\mathbb{F}_2)$. It follows, from Mackey's theory, that I has three irreducible faithful representations, all of dimension 7, corresponding to three characters of $\mathrm{Gal}(\mathbb{F}_{2^3}/\mathbb{F}_2)$. In particular, only one of these three representations is self-dual.

Proposition 4.2. — *Let $\varphi : W_{\mathbb{Q}_2} \to \mathrm{G}_2(\mathbb{C})$ be a parameter with the image I. Let $\phi_2 : W_{\mathbb{Q}_2} \to \mathrm{GL}_7(\mathbb{C})$ obtained by natural inclusion $\mathrm{G}_2(\mathbb{C}) \subseteq \mathrm{GL}_7(\mathbb{C})$. Then ϕ_2 is a self-dual, irreducible representation of $W_{\mathbb{Q}_2}$.*

Proof. — We know that any irreducible, complex representation of I either has J in the kernel or is faithful; in the latter case it is of dimension $2^3 - 1 = 7$. The group I, as seen above, has three faithful, irreducible, complex representations (only one of which is self-dual). Since the restriction of the standard 7-dimensional representation of $\mathrm{G}_2(\mathbb{C})$ to I is faithful and self-dual, it must be isomorphic to the unique irreducible, faithful, self-dual representation of I of dimension 7. □

It remains to show that the group I can be obtained as the image of the Weil group $W_{\mathbb{Q}_2}$. Let L be the Galois extension of $\mathbb{Q}_2$ given as the totally ramified extension of $\mathbb{Q}_{2^3}$ of degree 7. In other words, L is the splitting field of the polynomial

$$X^7 - 2 = 0.$$

Note that the Galois group of L is isomorphic to I/J. Let ϖ be a uniformizer in L, $U \subseteq L^\times$ the maximal pro-2 subgroup and $U \supseteq U_1 \supseteq \ldots$ the usual filtration. Then

$$L^\times = \langle \varpi \rangle \times \mathbb{F}_{2^3}^\times \times U.$$

Let χ be a character of $W_L^{ab} \cong L^\times$ which is trivial on the the first two factors of $L^\times$ and a non-trivial character of $U/U_1 \cong \mathbb{F}_{2^3}$. Consider the induced representation

$$\mathrm{Ind}_{W_L}^{W_{\mathbb{Q}_2}}(\chi).$$

This representation breaks up as a sum of three irreducible representations of dimension 7, one of which is self-dual. Let W_K be the kernel of this self dual representation. Then the Galois group of K over $\mathbb{Q}_2$ is isomorphic to I. In other words, we have constructed map $\varphi : W_{\mathbb{Q}_2} \to \mathrm{G}_2(\mathbb{C})$ with image I.

5. Local lift from G_2 to PGSp_6

The dual group of $\mathrm{PGSp}_6(\mathbb{Q}_p)$ is $\mathrm{Spin}_7(\mathbb{C})$. The group $\mathrm{Spin}_7(\mathbb{C})$ has a unique open orbit on the 8-dimensional spin representation. The stabilizer of a point in the open orbit is isomorphic to $\mathrm{G}_2(\mathbb{C})$. This gives an embedding

$$f : \mathrm{G}_2(\mathbb{C}) \to \mathrm{Spin}_7(\mathbb{C})$$

of dual groups, indicating that there should be a functorial, but non-endoscopic, lift of representations from $\mathrm{G}_2(\mathbb{Q}_p)$ to $\mathrm{PGSp}_6(\mathbb{Q}_p)$, once local Langlands parametrizations for the two groups are established. The Langlands parameterization is essentially known for depth zero representations. We shall now spell out some special cases of our interest.

In order to simplify notation let $G = \mathrm{G}_2(\mathbb{Q}_p)$ and $G' = \mathrm{PGSp}_6(\mathbb{Q}_p)$. Recall that a complex root of unity τ such that $\tau^{p^2-p+1} = 1$ defines a 7-dimensional orthogonal parameter $\phi(\tau) \oplus \chi_p$ which is contained in $\mathrm{G}_2(\mathbb{C})$. Therefore, it defines a generic supercuspidal representation $\sigma(\tau)$ of G and, by composing this parameter with the inclusion f, a generic supercuspidal representation $\sigma'(\tau)$ of G'. The representation $\sigma'(\tau)$, when restricted to $\mathrm{Sp}_6(\mathbb{Q}_p)$, breaks up as a sum of two representations in the L-packet for the parameter $\phi(\tau) \oplus \chi_p$.

We have the following:

- The functorial lift of the supercuspidal representation $\sigma(\tau)$ is the supercuspidal representation $\sigma'(\tau)$.
- The functorial lift of the Steinberg representation st_G is the Steinberg representation $\mathrm{st}_{G'}$.
- Let σ be an unramified representation of G corresponding to a semi-simple conjugacy class (Satake parameter) $s \in \mathrm{G}_2(\mathbb{C})$. Then the lift of σ is σ', an unramified representation of G' corresponding to the parameter $s' = f(s)$.

Although the local parameterizations for G and G' are not complete, a lift from G to G' is given by a correspondence arising from the minimal representation Σ of the split, adjoint $\mathrm{E}_7(\mathbb{Q}_p)$. More precisely, if σ is an irreducible representation of G, then we define $\Theta(\sigma)$ to be the set of isomorphism classes of all irreducible representations σ' of G' such that $\sigma \otimes \sigma'$ is a quotient of Σ.

Let $\psi : U \to \mathbb{C}^\times$ be a Whittaker character for G, where U is a maximal unipotent subgroup of G. Recall that a representation σ of G is ψ-generic (or simply generic) if $\sigma_{U,\psi}$, the space of ψ-twisted U-coinvariants, is nonzero. We have the same definition for representations of G' with respect to a Whittaker character $\psi' : U' \to \mathbb{C}^\times$, where U' is a maximal unipotent subgroup of G'. Let $\Theta_{\text{gen}}(\sigma)$ be the subset of $\Theta(\sigma)$ consisting of generic representations. This set is somewhat easier to determine.

Proposition 5.1. — *Let σ be an irreducible representation of $G = \mathrm{G}_2(\mathbb{Q}_p)$. Then $\Theta_{\text{gen}}(\sigma) \neq 0$ only if σ is generic. Moreover, $\Theta_{\text{gen}}(\sigma)$ contains at most one element.*

Proof. — Let σ' be in $\Theta_{gen}(\sigma)$. Then $\sigma \otimes \sigma'$ is a quotient of Σ. Since $\sigma'_{U',\psi'}$ is one dimensional, we see that σ is a quotient of $\Sigma_{U',\psi'}$. Since ([Ga, Th. 7.1])

$$\Sigma_{U',\psi'} = \mathrm{ind}_U^G(\psi),$$

as a G-module, it follows that σ is indeed generic. Moreover, since

$$\mathrm{Hom}_G(\mathrm{ind}_U^G(\psi), \sigma)$$

is one-dimensional for any generic representation σ (by uniqueness of the Whittaker functional), the second part follows immediately. The proposition is proved. □

Given a generic representation σ, the above proposition allows us to show that $\Theta_{\text{gen}}(\sigma) = \{\sigma'\}$ by simply showing that $\sigma \otimes \sigma'$ is a quotient of Σ.

Proposition 5.2. — *Assume that σ is an irreducible representation of $G = \mathrm{G}_2(\mathbb{Q}_p)$, belonging to either of the following two families:*

1. *Supercuspidal representations $\sigma(\tau)$.*
2. *Generic unramified representations.*

Then $\Theta_{\text{gen}}(\sigma) \neq \emptyset$ and the unique representation in $\Theta_{\text{gen}}(\sigma)$ is the functorial lift of σ, as described above.

Proof. — The supercuspidal representation $\sigma(\tau)$ is induced from a cuspidal representation ρ of the finite group $\mathrm{G}_2(\mathbb{F}_p)$, inflated to a hyperspecial maximal compact subgroup of G. Similarly, $\sigma'(\tau)$ is induced from a cuspidal representation ρ' of $\mathrm{PGSp}_6(\mathbb{F}_p)$. Gan shows in [Ga] that $\rho \otimes \rho'$ is a summand of the minimal representation of the adjoint group $\mathrm{E}_7(\mathbb{F}_p)$. By [Sa1] the minimal representation of $\mathrm{E}_7(\mathbb{F}_p)$ appears as the first non-trivial K-type of the minimal representation of $\mathrm{E}_7(\mathbb{Q}_p)$. (Here K is a hyperspecial maximal compact subgroup in $\mathrm{E}_7(\mathbb{Q}_p)$. In particular, $\mathrm{E}_7(\mathbb{F}_p)$ is a quotient of K by the first congruence subgroup, and the K-type is obtained by inflating the minimal representation of $\mathrm{E}_7(\mathbb{F}_p)$ to K.) It follows, by Frobenius reciprocity, that $\sigma(\tau)\otimes\sigma'(\tau)$ is a summand of Σ. This shows that $\Theta_{\mathrm{gen}}(\sigma(\tau))=\{\sigma'(\tau)\}$ as desired.

Finally, assume that σ is an unramified representation. Let $B=TU$ be a Borel subgroup of G. Then σ is a subquotient of $\mathrm{Ind}_B^G(\chi)$ for some unramified character χ of T. (The induction is normalized here.) Recall that any root α defines a co-root homomorphism $t\mapsto h_\alpha(t)$ from $\mathbb{Q}_p^\times$ into T. Let $\alpha_1,\alpha_2,\alpha_3$ be three short roots for G such that

$$\alpha_1+\alpha_2+\alpha_3=0.$$

This choice is unique up to the action of the Weyl group of G_2. We can now compose χ with the co-root homomophisms for α_i. In this way we get 3 characters χ_1,χ_2,χ_3 of $\mathbb{Q}_p^\times$ such that $\chi_1\chi_2\chi_3=1$. Now, if σ is generic then (and only then) the whole induced representation is irreducible. According to a result of Muić ([Mu, Prop. 3.1]) this happens if and only if

$$\chi_i\neq|\cdot|^{\pm1}\text{ and }\chi_i/\chi_j\neq|\cdot|^{\pm1}, 1\leqslant i<j\leqslant 3.$$

Next, consider the representation $\pi=\chi_1\times\chi_2\times\chi_3$ of $\mathrm{GL}_3(\mathbb{Q}_p)$ (here we use the notation of Bernstein and Zelevinski). Let $P=MN$ be a maximal parabolic of G' such that $M\cong\mathrm{GL}_3(\mathbb{Q}_p)$ (see [MaS]). Then the local lift of σ is the unique unramified quotient σ' of the representation of G' obtained by inducing π. By a result of Tadić ([Ta, Th. 7.1]) this induced representation is irreducible if and only if the same conditions as those of Muić are satisfied. In other words, an unramified representation σ is generic if and only if its local lift σ' is, and both are equal to a fully induced principal series representation. In particular, $\sigma'=\mathrm{Ind}_P^{G'}(\pi)$ (normalized induction). By Frobenius reciprocity, we have

$$\mathrm{Hom}_{G\times G'}(\Sigma,\sigma\otimes\sigma')=\mathrm{Hom}_{G\times M}(\Sigma_N,\sigma\otimes\pi)$$

where Σ_N is the (normalized) Jacquet functor. Next, we recall that the minimal representation of $\mathrm{E}_6(\mathbb{Q}_p)$ is a quotient of Σ_N [MaS] and that $\sigma\otimes\pi$ is a quotient of the minimal representation of $\mathrm{E}_6(\mathbb{Q}_p)$ [GaS2]. It follows that $\mathrm{Hom}_{G\times M}(\Sigma_N,\sigma\otimes\pi)\neq0$ and $\sigma\otimes\sigma'$ is a quotient of Σ, as desired. □

6. Global forms

In this section G will denote the split Sp_{2n} or G_2 over $\mathbb{Q}$. Fix a prime ℓ, and q an odd prime different from ℓ. By Theorem 4.5 [KLS] there exists a globally generic cuspidal automorphic representation σ of $G(\mathbb{A})$ such that

- σ_∞ is a generic integrable discrete series representation.
- σ_q is a tame supercuspidal generic representation; $\sigma_q = \sigma(\tau)$ if $G = \mathrm{G}_2$.
- σ_v is unramified for all $v \neq 2, q, \ell$.
- If $G = \mathrm{G}_2$ then σ_2 is unramified, and if $G = \mathrm{Sp}_{2n}$, σ_2 is the Jiang-Soudry descent of the self-dual supercuspidal representation of Π_2 introduced in Section 4.

The form σ lifts to an irreducible, self-dual, automorphic representation $\mathrm{GL}_{2n+1}(\mathbb{A})$ or $\mathrm{GL}_7(\mathbb{A})$, with *trivial* central character. This uses the lift of [CKPS] if G is Sp_{2n}. If G is G_2 we first use the exceptional theta lift [GRS] to obtain a non-zero generic automorphic form σ' on $\mathrm{PGSp}_6(\mathbb{A})$. The form σ' is cuspidal if the lift of σ to $\mathrm{PGL}_3(\mathbb{A})$ (via the minimal representation of E_6) is 0. This holds since σ_∞ is a discrete series representation and it cannot appear as a local component in the lift from $\mathrm{PGL}_3(\mathbb{A})$ [GaS1]. Thus, σ' is a generic cuspidal automorphic representation and its local p-adic components are determined by Proposition 5.2. The infinitesimal character of the real component σ'_∞ is integral and regular by the matching of infinitesimal characters in [HPS]. Next, we restrict σ' to $\mathrm{Sp}_6(\mathbb{A})$ and use the lift of [CKPS] to obtain an automorphic representation Π of $\mathrm{GL}_7(\mathbb{A})$.

Recall that χ_q is the unique non-trivial quadratic unramified character of the local Weil group. The local components of Π satisfy:

- Π_∞ has a regular and integral infinitesimal character.
- Π_q has the parameter $\phi(\tau) \oplus \chi_q$.
- Π_v is unramified for all $v \neq 2, q, \ell$.
- If $G = G_2$ then Π_2 is unramified, and if $G = \mathrm{Sp}_{2n}$ then Π_2 has the irreducible parameter ϕ_2.

Note that if Π_v is unramified then the eigenvalues of its Satake parameter are

$$\lambda_1^{\pm 1}, \ldots, \lambda_n^{\pm 1}, 1.$$

Moreover, if G is G_2 then we have one additional relation:

$$\lambda_1 \lambda_2 \lambda_3 = 1,$$

for some choice of sign, i.e., replacing λ_i by λ_i^{-1} if necessary for each $i \in \{1, 2, 3\}$. If Π_2 is the self-dual supercuspidal representation of $\mathrm{GL}_{2n+1}(\mathbb{Q}_2)$

with the parameter ϕ_2 then the lift Π is clearly cuspidal. If Π_2 is unramified then, since the parameter of Π_q is not irreducible, the global representation Π might not be cuspidal. We give a criterion which guarantees that it is cuspidal. Note that the conditions of the following proposition are automatically satisfied if q and the parameter $\phi(\tau) \oplus \chi_q$ are picked using Lemma 3.3.

Proposition 6.1. — *Assume that σ is a globally generic cuspidal automorphic representation of $\mathrm{Sp}_{2n}(\mathbb{A})$, such that σ_v is unramified at all (finite) primes $v \neq \ell, q$ and σ_q corresponds to the parameter $\phi(\tau) \oplus \chi_q$. If q splits in all quadratic extensions of $\mathbb{Q}$ unramified outside $\{\ell, \infty\}$, then Π, the global lift of σ to $\mathrm{GL}_{2n+1}(\mathbb{A})$, is cuspidal.*

Proof. — If Π is not cuspidal then by [CKPS], and the nature of the local parameter of Π_q, we have an isobaric sum

$$\Pi = \Sigma \boxplus \chi$$

where Σ is a cuspidal self-dual automorphic representation of $\mathrm{GL}_{2n}(\mathbb{A})$ and χ is a quadratic character of $\mathrm{GL}_1(\mathbb{A})$. The local component χ_v of χ is clearly unramified for all primes $v \neq \ell, q$. It is also unramified and non-trivial at q since it corresponds, via local class field theory, to the one-dimensional summand of the parameter of Π_q (denoted by the same symbol χ_q). By global class field theory χ corresponds to a quadratic extension of $\mathbb{Q}$ unramified outside $\{\ell, \infty\}$, such that q is inert in it. This is a contradiction. □

7. Minuscule and almost minuscule representations

Let G be a connected reductive group over an algebraically closed field of characteristic different from 2, and let T be a maximal torus in G. An irreducible algebraic representation V of G is called almost minuscule if $V^T \neq 0$ and the Weyl group acts transitively on the set of non-trivial weights of V. (Recall that an irreducible algebraic representation V of G is called minuscule if the Weyl group acts transitively on the set of weights of V.) These representations can be easily classified for an almost simple G. Assume first that the field characteristic is 0. Since $V^T \neq 0$ then, by Lie algebra action, V contains a root as a weight. All non-zero weights are now Weyl-group conjugates of that root. Therefore, if G is simply laced then V is the adjoint representation of G. If G is multiply laced then the weights are all short roots. We tabulate possible cases:

G	$\dim(V)$	$\dim(V^T)$
B_n	$2n+1$	1
C_n	$2n^2-n-1$	$n-1$
G_2	7	1
F_4	26	2

It is interesting to note that dimension of V^T is equal to the number of short simple roots. The Weyl group acts, naturally, on V^T. The action of long root reflections is trivial, while V^T is a reflection representation for the subgroup generated by simple short root reflections.

Proposition 7.1. — *Let G be an almost simple group over an algebraically closed field of characteristic $\ell > 2$. Then:*

1. *Any minuscule representation is isomorphic to a Frobenius twist of a representation with a minuscule weight as the highest weight.*
2. *Assume first that $\ell \neq 3$ if $G = \mathrm{G}_2$. Then any almost minuscule representation is a Frobenius twist of the almost minuscule representation with the highest weight equal to a short root. If $\ell = 3$ and $G = \mathrm{G}_2$ then there is one additional family of minuscule representations. It consists of Frobenius twists of the representation with the highest weight equal to a long root. In any case, the almost minuscule representations of G_2 are 7-dimensional.*

Proof. — Let $\alpha_1, \ldots, \alpha_r$ be the simple roots for G. We shall first characterize minuscule (and then almost minuscule) representations with the highest weight λ which is ℓ-restricted, i.e., $0 \leqslant \langle \lambda, \alpha_i^\vee \rangle \leqslant \ell - 1$ for all i. The general case will be later easily deduced from the Steinberg tensor product theorem.

For any root α, the group G contains a subgroup isomorphic to (a quotient of) SL_2. If $\langle \lambda, \alpha^\vee \rangle = n \leqslant \ell - 1$ then the action of SL_2 on the highest weight vector will give rise to the weights $\lambda, \lambda - \alpha, \ldots \lambda - n\alpha$. By examining the lengths of these weights we see that only the last one is in the Weyl group orbit of λ. This forces $n = 0$ or 1 if the representation is to be minuscule. In particular, if we write $n_i = \langle \lambda, \alpha_i^\vee \rangle$, then $n_i = 0$ or 1 for all i. Next, we claim that only one n_i could be 1. Otherwise, we can pick a path in the Dynkin diagram $\alpha_i, \alpha_{i+1}, \ldots, \alpha_j$ such that $n_i = n_j = 1$ and $n_k = 0$ for any α_k between α_i and α_j. Consider the root $\alpha = \alpha_i + \alpha_{i+1} + \cdots + \alpha_j$. Since $\langle \lambda, \alpha^\vee \rangle = 2$, this is a contradiction. (Note that we have just used the condition $\ell \neq 2$.) Finally, if the weight λ is fundamental but not minuscule then there exists a positive root α such that $\langle \lambda, \alpha^\vee \rangle = 2$. This is again a contradiction.

The proof of (2) is similar, except when $\langle \lambda, \alpha^\vee \rangle = 2$. Then $\lambda, \lambda - \alpha$ and $\lambda - 2\alpha$ are weights with $\lambda - \alpha$ the shortest length among the three weights. Since 0 is the only other orbit of weights, we must have $\lambda = \alpha$. If α is a long highest root, and the root system is of the type B_n, C_n or F_4 then there exists a short root β such that $\langle \alpha, \beta^\vee \rangle = 2$. This implies that the short root $\alpha - \beta$ is also a weight, and the representation cannot be almost minuscule. If $\ell = 3$ and $G = \mathrm{G}_2$ then this argument breaks down. The adjoint representation breaks up as $14 = 7 + 7'$ where 7 is the representation whose non-trivial weights are short roots, while $7'$ is a representation whose non-trivial weights are long roots.

It remains to deal with highest weights which are non necessarily ℓ-restricted. We need the following lemma.

Lemma 7.2. — *Let V_1 and V_2 be two non trivial and irreductible representations of G with such that V_1 is not isomorphic to the dual of V_2. Then the tensor product $V_1 \otimes V_2$ has two non-trivial Weyl group orbits of weights.*

Proof. — Let λ_1 and λ_2 be the highest weights of V_1 and V_2. Let λ_2^- be the lowest weight of V_2. Then $\lambda_1 + \lambda_2$ and $\lambda_1 + \lambda_2^-$ are weights of $V_1 \otimes V_2$ of different lengths. The latter of these two weights is non-zero since V_1 is not isomorphic to the dual of V_2, by our assumption. □

Any highest weight λ can be written as $\lambda = \lambda_0 + \ell\lambda_1 + \cdots + \ell^s\lambda_s$ for some ℓ-restricted highest weights $\lambda_1, \ldots, \lambda_s$. By the Steinberg tensor product theorem, the unique irreducible representation V with the highest weight λ is isomorphic to

$$V_0 \otimes V_1^{[1]} \otimes \cdots \otimes V_s^{[s]}$$

where V_i is the irreducible representation with the highest weight λ_i and $V_i^{[i]}$ is the i-th Frobenius twist of V_i. Lemma 7.2 implies that V can be (almost) minuscule only if V is a Frobenius twist of representation with an ℓ-restricted highest weight. The proposition is proved. □

It should be noted that the dimension of V^T is not necessarily the same as in the characteristic 0. For example, if $\ell = 3$ then any almost minuscule representation V of F_4 has dimension 25 and $\dim(V^T) = 1$. The main result of this section is the following:

Proposition 7.3. — *Let G be a connected reductive group over an algebraically closed field of characteristic ℓ different from 2. Let V be a faithful and irreducible algebraic representation of G of dimension $2n+1$, preserving a non-degenerate bilinear form. Assume that there exist $2n$ different weights in V permuted cyclically by a Weyl group element. Then $G = \mathrm{SO}_{2n+1}$ if $n \neq 3$, and is either SO_7 or G_2 if $n = 3$.*

Proof. — Let Z be the connected component of the center of G. The characters of Z form a lattice. In particular, the only self-dual character is the trivial character. This shows, since V is faithful and irreducible, that Z is trivial. Therefore G is semi-simple. Since weights of a self-dual representation come in pairs $\{\mu, -\mu\}$, and the Weyl group preserves the length of weights, the weight outside the cycle (of length $2n$ permuted by the Weyl group element of the statement of the proposition) must be trivial, so $\dim(V^T) = 1$. Next, let $G_1 \times \cdots \times G_k$ be a product of almost simple groups isogenous to G such that $V = V_1 \otimes \cdots \otimes V_k$ is a tensor product of irreducible, *non-trivial* representations of $G_1, \ldots, G_k$. Since $V^T \neq 0$, the zero weight must appear in each $V_1, \ldots, V_k$. But then V can be almost minuscule only if $k = 1$. Since the groups of type B_n and G_2, and no other groups, have a Weyl group element that permutes all short roots, V must be a Frobenius twist of the standard representation of SO_{2n+1} or it is a 7-dimensional representation of G_2. This completes the proof. □

8. Galois representations

Let Π be the self-dual cuspidal automorphic representation of $\mathrm{GL}_{2n+1}(\mathbb{A})$ constructed by lifting from $G(\mathbb{A}) = \mathrm{Sp}_{2n}(\mathbb{A})$, or from $G(\mathbb{A}) = \mathrm{G}_2(\mathbb{A})$ in Section 6. In particular,

- The infinitesimal character of Π_∞ is regular and integral.
- The local component Π_v is unramified for all $v \neq \ell, q$.
- The local parameter of Π_q is $\phi(\tau) \oplus \chi_q$ where q splits in any quadratic extension of $\mathbb{Q}$ ramified at ℓ only.
- If $G = G_2$ then Π_2 is unramified, and if $G = \mathrm{Sp}_{2n}$ then Π_2 is supercuspidal with parameter the irreducible representation ϕ_2 of §4.

By the generalization of Theorem 1.1 due to Shin [Sh], and the remark after Thorem 1.1, one can attach a semi-simple Galois representation to Π:

$$r_\Pi : G_{\mathbb{Q}} \to \mathrm{GL}_{2n+1}(\bar{\mathbb{Q}}_\ell)$$

such that for every prime $v \neq \ell$ the restriction of r_Π to the decomposition group D_v gives the Langlands parameter of Π_v, up to Frobenius semisimplification. Indeed, when the Weil-Deligne parameter $\mathcal{L}(\Pi_v)$ for all $v \neq \ell$ has monodromy $N = 0$, we can state Theorem 1.1 as

$$r_\Pi|_{D_v}^{\mathrm{Frob-ss}} = \mathcal{L}(\Pi_v)$$

where $\mathcal{L}(\Pi_v)$ may be regarded, using the embedding $\iota : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$, as a representation of the decomposition group D_v at v with values in $\mathrm{GL}_{2n+1}(\bar{\mathbb{Q}}_\ell)$.

Let us concentrate on the prime q. Here Π_q is the lift of a supercuspidal representation of $\mathrm{Sp}_{2n}(\mathbb{Q}_q)$ whose parameter, when restricted to the inertia group $I_{\mathbb{Q}_q}$, is a direct sum of $2n+1$ one dimensional characters. One is trivial and the other $2n$ are cyclically permuted by Fr_q. It follows that $r_\Pi(\mathrm{Fr}_q^{2n})$ commutes with $r_\Pi(I_q)$. This shows that $r_\Pi(\mathrm{Fr}_q^{2n})$ and $r_\Pi(\mathrm{Fr}_q)$ must be semi-simple. In other words, r gives exactly the parameter of Π_q. The same argument shows that the restriction of r_Π to D_2 gives the parameter of Π_2 if Π_2 is supercuspidal.

Proposition 8.1. — *If Π satisfies the above conditions at places ∞, 2 and q then the Galois representation r_Π is irreducible and orthogonal.*

Proof. — If Π_2 is supercuspidal, then the local parameter is irreducible and r_Π is irreducible. Thus assume that Π_2 is unramified. If r_Π is reducible then r_Π has two irreducible summands of dimensions $2n$ and 1. Since the eigenvalues of $r_\Pi(\mathrm{Fr}_v)$ are 1, $\lambda_i^{\pm}$, $(1 \leqslant i \leqslant n)$ the representation r_Π is self-dual. In particular, the one-dimensional summand is a quadratic character χ unramified outside $\{\ell, \infty\}$ and such that $\chi(\mathrm{Fr}_q) = -1$. This implies that there exists a quadratic extension unramified outside $\{\ell, \infty\}$ and such that q stays inert in it. This is a contradiction since q is picked so that it splits completely in every such quadratic extension. Therefore r_Π is irreducible. Since it is self-dual and of odd dimension, it is orthogonal as well. □

9. Zariski closure

Fix a prime ℓ, and positive integers d and t. (The integer t will not play any particular role in this section.) Let K be the composite of all Galois extensions of degree $\leqslant d$ that are unramified outside $\{2, \ell, \infty\}$. Let p and q be the odd primes attached to $m = 2n$, ℓ, d, t and K by Lemma 3.3. In particular, $p > d$ and q splits completely in K. Let Π be as in Section 6 where the parameter $\phi(\tau) \oplus \chi_q$ of the local component Π_q of Π is constructed by the recipe following Lemma 3.3. In particular, the representation r_Π is unramified at all primes different from 2, ℓ and q, and $r_\Pi(I_q)$ is of order p.

Lemma 9.1. — *Let $\Gamma = r_\Pi(G_\mathbb{Q})$ and let Γ^d be the intersection of all normal subgroups of Γ of index $\leqslant d$. Then $r_\Pi(D_q)$ is contained in Γ^d.*

Proof. — Let Γ' be a normal subgroup of Γ of index $\leqslant d$. We must show that the image of D_q lands in Γ'. Let L be the Galois extension of $\mathbb{Q}$ corresponding to Γ'. Obviously, L is unramified outside $\{2, \ell, q, \infty\}$. Moreover, since $r_\Pi(I_q)$ is of order p and $p > d$, it follows that L is unramified at q as well. Thus, L is contained in K (which by definition is the compositum of all Galois extensions unramified outside $\{2, \ell, \infty\}$ and of degree $\leqslant d$). This implies that q splits completely in L (as it does so in K) and $r_\Pi(D_q)$ is therefore contained in Γ', as desired. □

The above lemma shows that if Π_q is constructed by means of Lemma 3.3 then $\Gamma_{2n,p}$, the image of the decomposition group D_q, sits *deeply embedded* in $\Gamma = r_\Pi(G_{\mathbb{Q}})$. This property is crucial in controling the size of the image Γ of the Galois group.

Theorem 9.2. — *There exists a function $I : \mathbb{N} \to \mathbb{N}$ such that if Π is a self-dual cuspidal automorphic representation of $\mathrm{GL}_{2n+1}(\mathbb{A})$, as in Section 6, and such that the local parameter of Π_q is constructed by means of Lemma 3.3 with $d > I(n)$ then the Zariski closure of $r_\Pi(G_{\mathbb{Q}})$ is isomorphic to $\mathrm{SO}_{2n+1}(\bar{\mathbb{Q}}_\ell)$ if $n \neq 3$, and either $\mathrm{SO}_7(\bar{\mathbb{Q}}_\ell)$ or $\mathrm{G}_2(\bar{\mathbb{Q}}_\ell)$ if $n = 3$.*

Proof. — Let G be the Zariski closure of $r_\Pi(G_{\mathbb{Q}})$. Since r_Π is irreducible this is a reductive group. Let G° be its connected component. Recall that the image of the inertia subgroup I_q contains an element s in $\mathrm{GL}_{2n+1}(\bar{\mathbb{Q}}_\ell)$ of order p. We want to show that s is contained in G°. We need the following (Lem. 6.3 of [KLS]):

Lemma 9.3. — *There exists a function $J\colon \mathbb{N} \to \mathbb{N}$ such that for every integer $n > 0$ and every algebraic subgroup $H \subset \mathrm{GL}_n$ over a field of characteristic zero, there is normal subgroup $H_1 \subseteq H$ of index $\leqslant J(n)$ containing H°, the connected component, such that H_1/H° is abelian.*

We apply Lemma 9.3 to $G \subseteq \mathrm{GL}_{2n+1}(\bar{\mathbb{Q}}_\ell)$, the Zariski closure of $r_\Pi(G_{\mathbb{Q}})$. Let G_1 be the normal subgroup of G of index $\leqslant J(2n+1)$, containing G° and such that G_1/G° is abelian. If we pick $d > J(2n+1)$ then, by Lemma 9.1, the image of D_q must be contained in G_1. Since $\Gamma_{2n,p}$ is a semi-direct product of $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/2n\mathbb{Z} \subset \mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ one easily sees that the commutator subgroup of $r_\Pi(D_q)$ is $r_\Pi(I_q) \cong \mathbb{Z}/p\mathbb{Z}$. This shows that the projection of $r_\Pi(D_q)$ to the abelian quotient G_1/G° must contain s in the kernel. In other words, s is in G°.

Recall that the eigenvalues of s are

$$\tau, \tau^q, \ldots, \tau^{q^{n-1}}, \tau^{-1}, \tau^{-q}, \ldots, \tau^{-q^{n-1}}, 1.$$

where τ is a pth root of one. Moreover, these eigenvaules are *distinct*. It follows that the the centralizer of s in GL_{2n+1} is a torus. Thus, s is a regular semi-simple element in G° and the centralizer of s in G° is a maximal torus T. Next, note that the centralizer of s in G° is the same as the centralizer of $r_\Pi(\mathrm{Fr}_q) \cdot s \cdot r_\Pi(\mathrm{Fr}_q^{-1})$ (since it is so in GL_{2n+1}). It follows that $r_\Pi(\mathrm{Fr}_q)$ normalizes T. We need the following lemma.

Lemma 9.4. — *There exists a function* $J'\colon \mathbb{N} \to \mathbb{N}$ *such that for every integer* $n > 0$ *and every reductive group* H *of rank* n *over an algebraically closed field of characteristic zero, there is a normal subgroup* $H'_1 \subseteq H$ *of index* $\leqslant J'(n)$ *containing* H°*, the connected component, such that conjugation of* H° *by any element in* H'_1 *is inner.*

Proof. — The conjugation action of H on H° gives a homomorphism from a finite group H/H° to $\mathrm{Aut}\,(H^\circ)/\mathrm{Inn}\,(H^\circ)$. The latter group is contained in the group of automorphisms of a root datum $(X, \Delta, X^\vee, \Delta^\vee)$ of H°. It follows that H/H° maps into $\mathrm{GL}(X) \cong \mathrm{GL}_n(\mathbb{Z})$. Since there is a torsion-free congruence subgroup in $\mathrm{GL}_n(\mathbb{Z})$, the order of any finite subgroup in $\mathrm{GL}_n(\mathbb{Z})$ is bounded by the index of the torsion-free congruence subgroup. This proves the lemma. □

We apply Lemma 9.4 to $G \subseteq \mathrm{GL}_{2n+1}(\bar{\mathbb{Q}}_\ell)$, the Zariski closure of $r_\Pi(G_\mathbb{Q})$. Let G'_1 be a normal subgroup of G of index $\leqslant J'(2n+1)$, containing G° and such that G'_1 acts on G° as inner automorphisms. Now if we pick $d > J'(2n+1)$, in addition to $d > J(2n+1)$, then $r_\Pi(D_q)$ must be contained in G'_1, by Lemma 9.1. This shows that the conjugation by $r_\Pi(\mathrm{Fr}_q)$ is an inner automorphism. Hence the normalizer of the torus T in G° contains an element of order $2n$ which cyclically permutes the weights corresponding to the $2n$ eigenvalues of s different from 1. This shows that r_Π, under the action of G°, has at most two irreducible summands. If there are two summands, then they have dimensions $2n$ and 1. But, since G° is a normal subgroup and G acts irreducibly, G° cannot act with two summands of different dimensions. Hence G° acts irreducibly as well. Since r_Π is self-dual, it follows that G° satisfies conditions of Proposition 7.3, so it must be either SO_{2n+1} or G_2. It remains to show that $G = G^\circ$. First, r_Π is an irreducible $2n+1$-dimensional representation of G which restricts to the standard representation of G°. Second, since SO_{2n+1} and G_2 have no outer automorphisms, every connected component of G contains an element commuting with G°. Combining the two, it follows that any connected component of G contains a homothety by a scalar λ. On the other hand, since $r_\Pi(\mathrm{Fr}_v)$ has 1 as one of the eigenvalues for almost all primes v, by Čebotarev's density theorem the function $\det(1 - r_\Pi(g))$ must be 0 for all elements g in G. In particular, λ must be equal to 1 and this shows that $G = G^\circ$. The theorem is proved with $I(n) = \max(J(2n+1), J'(2n+1))$. □

According to Theorem 9.2 there are two possibilities for the Zariski closure if $n = 3$. The following two corollaries give us more precise statements in this case.

Corollary 9.5. — *Assume that* Π *comes from* $\mathrm{G}_2(\mathbb{A})$*, as in Section 6. Then the Zariski closure of* $r_\Pi(G_\mathbb{Q})$ *is* $\mathrm{G}_2(\bar{\mathbb{Q}}_\ell)$*.*

Proof. — Let G be the Zariski closure. We know that G is either SO_7 or G_2. It suffices to show that the rank of the maximal torus T is at most 2. To see this, recall that the eigenvalues of $r_\Pi(\mathrm{Fr}_v)$ are 1, $\lambda_i^\pm$ $(i = 1, 2, 3)$ for $v \neq q, \ell$. Therefore the characteristic polynomial of $r_\Pi(\mathrm{Fr}_v)$ is $f(x) = (x-1)g(x)$ with

$$g(x) = x^6 + ax^5 + bx^4 + cx^3 + bx^2 + ax + 1$$

a palindromic polynomial of degree 6. Moreover, the condition $\lambda_1\lambda_2\lambda_3 = 1$ gives one algebraic relation on the three coefficients a, b and c. By Čebotarev's density theorem, the same holds for the characteristic polynomial of all elements in the image of r and, therefore, for all elements in T. In particular, the dimension of T is less than or equal to 2. □

Corollary 9.6. — *Assume that Π_2, the local component of Π, is the irreducible self-dual cuspidal representation of $\mathrm{GL}_7(\mathbb{Q}_2)$ introduced in Section 4. Then the Zariski closure of r_Π is $\mathrm{SO}_7(\bar{\mathbb{Q}}_\ell)$.*

Proof. — This follows as the image of the inertia subgroup I_2 contains elements in $\mathrm{SO}_7(\bar{\mathbb{Q}}_\ell)$ which are not contained in G_2. □

Remark. — The method of proof of Theorem 9.2 can be used to give an alternate argument to prove the result of §6 of [KLS] that the Zariski closure of ρ_Π is GSp_{2n}. This would avoid the use of the crutch of reduction modulo ℓ that is used in [KLS].

10. A group-theoretic criterion

In this section we develop criteria which give us control over the image of ℓ-adic representations in the case of exceptional groups. As such, this section is somewhat more general then what is needed for the main results in this paper. However, the results of this section might have future applications. A possibility in this direction is presented in Section 12.

Let Γ be a profinite group and $d \geqslant 2$ an integer. We define Γ^d as the intersection of all open normal subgroups of Γ of index $\leqslant d$.

Lemma 10.1. — *If Γ is a profinite group, Δ a closed normal subgroup, and d a positive integer, then the image of Γ^d in Γ/Δ is $(\Gamma/\Delta)^d$.*

Proof. — The image in Γ/Δ of every open subgroup of Γ of index $\leqslant d$ is again open of index $\leqslant d$, and conversely, all open index $\leqslant d$ subgroups of Γ/Δ arise as images of open index $\leqslant d$ subgroups of Γ. □

Let $n \geqslant 2$ be an integer and p a prime congruent to 1 (mod n).

Definition 10.2. — *By a group of* type (n,p), *we mean any finite group* Γ *with a normal subgroup* Δ *isomorphic to* $\mathbb{Z}/p\mathbb{Z}$ *such that the image of* $\operatorname{Inn}\Gamma$ *in* $\operatorname{Aut}\Delta$ *is isomorphic to* $\mathbb{Z}/n\mathbb{Z}$.

As noted in the introduction, this is slightly different from the terminology in [KLS]. If $\ell \neq p$ is prime, a group of *type* (n,p,ℓ) will mean a (possibly finite) profinite group which is the extension of a group of type (n,p) by a pro-ℓ group.

Lemma 10.3. — *If* $0 \to \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to 0$ *is a short exact sequence of profinite groups,* $n \geqslant 2$, ℓ *and* p *are distinct primes, and* Γ_1 *is pro-*ℓ*, then* Γ_2 *contains a subgroup of type* (n,p,ℓ) *if and only if* Γ_3 *does.*

Proof. — Any extension of a group of type (n,p,ℓ) by a pro-ℓ group is again of type (n,p,ℓ), so one direction is trivial.

For the other, let Δ_2 be a closed subgroup of Γ_2 and Δ_2' an open normal pro-ℓ subgroup of Δ_2 such that $\Delta_2'' := \Delta_2/\Delta_2'$ is of type (n,p). Let $\Delta_1 := \Delta_2 \cap \Gamma_1$, $\Delta_1' := \Delta_2' \cap \Gamma_1$, and $\Delta_1'' := \Delta_1/\Delta_1'$. By the snake lemma, we have a right-exact sequence

$$\Delta_2'/\Delta_1' \to \Delta_2/\Delta_1 \to \operatorname{coker}(\Delta_1'' \to \Delta_2'') \to 0.$$

As Δ_2' is pro-ℓ, so is every quotient thereof, so Δ_2/Δ_1 is an extension of $\operatorname{coker}(\Delta_1'' \to \Delta_2'')$ by a pro-ℓ group.

Every quotient of a group $\Gamma_{n,p}$ of type (n,p) by an ℓ-group is again of type (n,p). Indeed, the quotient map preserves the normal subgroup of $\Gamma_{n,p}$ isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and therefore the image of $\operatorname{Inn}\Gamma_{n,p} \to (\mathbb{Z}/p\mathbb{Z})^\times$. □

We remark that for the non-trivial direction, the proof uses only the fact that Γ_1 is the inverse limit of finite groups of prime-to-p order.

Theorem 10.4. — *Let* ℓ *be a prime and* G *a connected reductive algebraic group over* $\bar{\mathbb{F}}_\ell$. *There exists a constant* B*, independent of* ℓ*, such that*

1. *If* $\operatorname{rk} G \leqslant 2$ *and* $p > B$ *is a prime distinct from* ℓ *and* $G(\bar{\mathbb{F}}_\ell)$ *contains a subgroup of type* $(6,p,\ell)$*, then* G *is of type* G_2.
2. *If* $\operatorname{rk} G \leqslant 4$ *and* $p_1, p_2 > B$ *are primes distinct from* ℓ *and* $G(\bar{\mathbb{F}}_\ell)$ *contains subgroups of type* $(8,p_1,\ell)$ *and* $(12,p_2,\ell)$*, then* G *is of type* F_4.
3. *If* $\operatorname{rk} G \leqslant 6$ *and* $p > B$ *is a prime distinct from* ℓ *and* $G(\bar{\mathbb{F}}_\ell)$ *contains a subgroup of type* $(9,p,\ell)$*, then* G *is of type* E_6.

4. *If* $\operatorname{rk} G \leqslant 7$ *and* $p_1, p_2 > B$ *are primes distinct from* ℓ *and* $G(\bar{\mathbb{F}}_\ell)$ *contains subgroups of type* $(18, p_1, \ell)$ *and* $(30, p_2, \ell)$*, then* G *is of type* E_7*.*

5. *If* $\operatorname{rk} G \leqslant 8$ *and* $p_1, p_2, p_3 > B$ *are primes distinct from* ℓ *and* $G(\bar{\mathbb{F}}_\ell)$ *contains subgroups of type* $(18, p_1, \ell)$*,* $(20, p_2, \ell)$*, and* $(30, p_3, \ell)$*, then* G *is of type* E_8*.*

Proof. — We claim that the root systems of type G_2, F_4, E_6, E_7, and E_8 respectively are the only root systems of rank less than or equal to 2, 4, 6, 7, and 8 respectively, which have Weyl group elements of order 6; 8 and 12; 9; 18 and 30; and 18, 20, and 30, respectively. To see that this is so, we compile a table of the orders of Weyl group elements for root systems of rank $\leqslant 8$. We write each root system as a sum of irreducible root systems, each coded as a single letter and a single digit, and arranged alphabetically. We order root systems first by rank and within rank, alphabetically. A root system is *exceptional* if it is simple of type G_2, F_4, E_6, E_7, or E_8. For brevity, we omit those root systems for which the set of possible Weyl element orders is a proper subset of that for some non-exceptional root system of equal or inferior rank. In case of equality, we print only the lexicographically smallest example. (For example, in our table, no root system of type C_n appears, since B_n is lexicographically inferior to it and has the same set of Weyl group orders. Likewise, $A_1 + A_4$ does not appear because its set of Weyl group orders is strictly dominated by that of B_5, which, though lexicographically superior, has the same rank.) Since the set of orders of elements of a finite group is determined by its subset of maximal elements with respect to divisibility, we exhibit only this subset.

Now, let $\Gamma_{n,p,\ell}$ be a subgroup of $G(\bar{\mathbb{F}}_\ell)$ of type (n, p, ℓ) for some $n \geqslant 2$ and some prime $p \neq \ell$. Let $\Delta_\ell \subset \Gamma_{n,p,\ell}$ denote a normal ℓ-subgroup such that the corresponding quotient group $\Gamma_{n,p}$ is of type (n, p). Now, $\Delta_\ell \subset G(\mathbb{F}_{\ell^k})$ for some k, and so it is contained in a Sylow ℓ-subgroup of $G(\mathbb{F}_{\ell^k})$. Such a subgroup is the group of $\mathbb{F}_{\ell^k}$-points of the unipotent radical of a Borel subgroup of G. By §30.3 of [Hu1], the normalizer of Δ_ℓ in G is contained in a parabolic subgroup P, proper if Δ_ℓ is non-trivial. If N denotes the unipotent radical of P, then $N(\bar{\mathbb{F}}_\ell) \cap \Gamma_{n,p,\ell}$ is an ℓ-group, so by Lemma 10.3, the image of $\Gamma_{n,p,\ell}$ in the Levi factor $M(\bar{\mathbb{F}}_\ell)$ is again of type (n, p, ℓ). The rank of M is equal to that of G, while the dimension is strictly less. Iterating this process we end up with a connected reductive group, which we again denote M, of the same rank as G such that $M(\bar{\mathbb{F}}_\ell)$ contains a subgroup $\Gamma_{n,p}$ of type (n, p). If M is an exceptional group, then $G = M$, since in each rank r, the exceptional group, if one exists, is the connected reductive group of maximal dimension in rank r.

Root System	Maximal Elements
A1	2
A2	$2, 3$
B2	4
G2	6
B3	$4, 6$
A2 + B2	12
A4	$4, 5, 6$
B4	$4, 6, 8$
F4	$8, 12$
B5	$8, 10, 12$
A2 + B4	24
A4 + B2	$12, 20$
A4 + G2	$12, 30$
A6	$7, 10, 12$
E6	$8, 9, 10, 12$
A1 + E6	$8, 10, 12, 18$
A2 + B5	$24, 30$
A4 + B3	$12, 20, 30$
A7	$7, 8, 10, 12, 15$
B7	$14, 20, 24$
E7	$8, 12, 14, 18, 30$
A2 + E6	$18, 24, 30$
A4 + F4	$24, 40, 60$
A6 + B2	$12, 20, 28$
A6 + G2	$12, 30, 42$
A8	$8, 9, 12, 14, 15, 20$
B2 + E6	$8, 20, 36$
B8	$14, 16, 20, 24, 30$
E8	$14, 18, 20, 24, 30$

Let $\Gamma_{n,p}$ be a subgroup of type (n, p) of $M(\bar{\mathbb{F}}_\ell)$ for some integer n, let x denote the image of a generator of the normal subgroup of $\Gamma_{n,p}$ isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and let $a \in \mathbb{Z}$ be such that its image in $\mathbb{Z}/p\mathbb{Z}$ is of order n in $(\mathbb{Z}/p\mathbb{Z})^\times$. As x and x^a are conjugate in $\Gamma_{n,p}$, x and x^a are conjugate in $M(\bar{\mathbb{F}}_\ell)$. Since $p \neq \ell$, they are semi-simple elements, and if $B < p$ is taken to be larger than the maximal number of components of the centralizer of any semi-simple element in any reductive connected group of rank $\leqslant 8$, it follows that x and x^a belong to a common maximal torus $T \subset M$. By a well-known theorem (cf. §3.1 of [Hu2]), there exists $w \in N_M(T)(\bar{\mathbb{F}}_\ell)$ such that $wxw^{-1} = x^a$. However, this implies that the order of the image of w in the Weyl group of M with respect to T is divisible by n. From our analysis of orders of elements in Weyl groups in rank $\leqslant 8$, it follows that M is exceptional and therefore that G is exceptional. □

Theorem 10.5. — *There exist constants A and B such that if*

1. *$d > A$ is an integer,*
2. *$p_1, p_2, p_3 > B$ and $\ell \notin \{p_1, p_2, p_3\}$ are primes,*
3. *K is an ℓ-adic field,*
4. *G is a connected reductive algebraic group over K such that*
   - *(a)* $\operatorname{rk} G \leqslant 2$,
   - *(b)* $\operatorname{rk} G \leqslant 4$,
   - *(c)* $\operatorname{rk} G \leqslant 6$,
   - *(d)* $\operatorname{rk} G \leqslant 7$, *or*
   - *(e)* $\operatorname{rk} G \leqslant 8$,
5. *$\Gamma \subset G(K)$ is a profinite subgroup such that (respectively)*
   - *(a)* Γ^d *has a subgroup of type* $(6, p_1, \ell)$,
   - *(b)* Γ^d *has a subgroup of type* $(8, p_1, \ell)$ *and* $(12, p_2, \ell)$,
   - *(c)* Γ^d *has a subgroup of type* $(9, p_1, \ell)$,
   - *(d)* Γ^d *has subgroups of type* $(18, p_1, \ell)$ *and* $(30, p_2, \ell)$, *or*
   - *(e)* Γ^d *has subgroups of type* $(18, p_1, \ell)$, $(20, p_2, \ell)$, *and* $(30, p_3, \ell)$,

then some finite quotient $\bar{\Gamma}$ of Γ satisfies

$$(H^{\mathrm{ad}}(\bar{\mathbb{F}}_\ell)^F)^{\mathrm{der}} \subset \bar{\Gamma} \subset H^{\mathrm{ad}}(\bar{\mathbb{F}}_\ell)^F, \tag{10.1}$$

where F is a Frobenius map and H^{ad} is a simple adjoint algebraic group of type G_2, F_4, E_6, E_7, *or* E_8 *respectively. In particular, in the first, second, and fifth case, $\bar{\Gamma}$ is simple.*

Proof. — Replacing K by a finite extension, we may assume first that G is split, and second that Γ fixes a hyperspecial vertex of the building of G over K (see, e.g., [La], and the remark below). Thus, there exists a smooth group scheme $\mathcal{G}$ over the ring of integers $\mathcal{O}$ of K whose generic fiber is G, whose special fiber is again reductive and connected, and such that $\Gamma \subset \mathcal{G}(\mathcal{O})$. The root datum of the special fiber of $\mathcal{G}$ is the same as that of G. Let $H := \mathcal{G}_{\bar{\mathbb{F}}_\ell}$ denote the geometric special fiber. Thus, Γ maps to $H(\bar{\mathbb{F}}_\ell)$ with finite image and pro-ℓ kernel. Replacing Γ by its image in $H(\bar{\mathbb{F}}_\ell)$, by Lemma 10.1 and Lemma 10.3, we still have that Γ^d has subgroups of the specified types. By Theorem 10.4, H is almost simple of type G_2, F_4, E_6, E_7, or E_8 according as we are in case (a), (b), (c), (d), or (e). Assuming $B > 3$, the image $\bar{\Gamma}$ of Γ in $H^{\mathrm{ad}}(\bar{\mathbb{F}}_\ell)$ again has the property that $\bar{\Gamma}^d$ has subgroups of the specified types. By Th. 0.5 of [LP], it follows that either $\bar{\Gamma}$ satisfies the condition (10.1) for some Frobenius map or that $\bar{\Gamma}$ is contained in a proper algebraic subgroup of $I \subset H^{\mathrm{ad}}$ with a component group I/I° whose order is bounded above by an absolute constant A. As $d > A$, it follows that $\bar{\Gamma}^d \subset I^\circ(\bar{\mathbb{F}}_\ell)$. If N denotes the unipotent radical of I°, the image of $\bar{\Gamma}^d$ in $(I/N)(\bar{\mathbb{F}}_\ell)$ contains a subgroup of type (n, p, ℓ). As I/N is reductive of rank less than or equal to the rank r of H^{ad} (which equals the rank of G) and as $\dim I/N \leqslant \dim I < \dim H^{\mathrm{ad}} = \dim G$, it follows that I/N cannot be exceptional of rank r, which contradicts Theorem 10.4. □

Remark. — If G is of type G_2, F_4 or E_8 then $G(K)$ is always split and simply connected. The profinite subgroup Γ is contained in a maximal parahoric subgroup of $G(K)$. The quotient of this maximal parahoric subgroup by its pro-ℓ radical is a simply connected semi-simple group H of rank r over the residual field of K. Let $\bar{\Gamma}$ be the projection of Γ into H. If Γ contains groups of type (n, p, ℓ) as specified in Theorem 10.5, then so does $\bar{\Gamma}$. By Theorem 10.4 H must be of the same type as G. This shows that the maximal parahoric subgroup containing Γ is hyperspecial.

11. Main Theorem

We are now ready to construct finite Galois groups over $\mathbb{Q}$. Let $r_\Pi : G_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_\ell)$ be the Galois representation attached to a self-dual cuspidal representation Π constructed in Section 6. Recall that Π is constructed so that the image of D_q in $\Gamma = r_\Pi(G_{\mathbb{Q}})$ is a group of type $(2n, p)$, denoted by $\Gamma_{2n,p}$, and contained in Γ^d. Let G be the Zariski closure of Γ. By Theorem 9.2 and its corollaries, if $d > I(n)$ then:

– $G = \mathrm{G}_2$ if Π is a lift from G_2

– $G = \mathrm{SO}_{2n+1}$ if Π is a lift from Sp_{2n} and the local component Π_2 is the supercuspidal representation defined in Section 4.

Note that by assumption $\ell > 2$ if $G = \mathrm{SO}_{2n+1}$. If $G = \mathrm{G}_2$ then by Theorem 10.5, Γ has a quotient isomorphic to $\mathrm{G}_2(\mathbb{F}_{\ell^k})$ (or a Ree group if $\ell = 3$) for some k provided that $d > \max(A, B)$ where A and B are in the statement of Theorem 10.5.

Assume now that $G = \mathrm{SO}_{2n+1}$, and hence $\ell > 2$, Π is a lift from Sp_{2n}, and the local component Π_2 is the supercuspidal representation defined in Section 4.

THEOREM 11.1. — *There exists a function $d : \mathbb{N} \to \mathbb{N}$ such that if Π_q is picked with $d > d(n)$ then $\Gamma = r_\Pi(G_\mathbb{Q})$ has a quotient $\bar{\Gamma}$ such that*

$$(\mathrm{SO}_{2n+1}(\bar{\mathbb{F}}_\ell)^F)^{\mathrm{der}} \subset \bar{\Gamma} \subset \mathrm{SO}_{2n+1}(\bar{\mathbb{F}}_\ell)^F, \tag{11.2}$$

where F is a Frobenius map.

Proof. — By enlarging the field K we can assume that G is split and that Γ is contained in a hyperspecial maximal parahoric subgroup. This means that G can be written as $G = \mathrm{SO}(V, Q)$ where V is a linear space over K and Q a split quadratic form, and there exists a lattice L stabilized by Γ such that Q takes integral values on L. Moreover, if $\bar{V}$ is the reduction modulo ℓ of L, then the quadratic form Q reduces modulo ℓ to a non-degenerate quadratic form $\bar{Q}$ on $\bar{V}$. In other words, the pair (L, Q) defines a smooth group scheme over the ring of integers of K whose generic fiber is G and such that $H := \mathrm{SO}(\bar{V}, \bar{Q})$ is the special fiber. Let $\bar{\Gamma}$ be the image of Γ in $H(\bar{\mathbb{F}}_\ell)$. By Th. 0.5 of [LP], it follows that either $\bar{\Gamma}$ satisfies the condition (11.2) for some Frobenius map or that $\bar{\Gamma}$ is contained in a proper algebraic subgroup of $I \subset H$ with a component group I/I° whose order is bounded above by an absolute constant $A(n)$. If we pick $d > A(n)$ then $\bar{\Gamma}^d \subset I^\circ(\bar{\mathbb{F}}_\ell)$. It follows that $\Gamma_{2n,p}$ is contained in I°. Under the action of $\Gamma_{2n,p}$, the orthogonal space $\bar{V}$ decomposes as a sum of two irreducible mutually orthogonal representations of dimensions $2n$ and 1. This implies that the nilpotent radical of I° is trivial. Indeed, if N is a non-trivial unipotent radical of I°,then there exists a non-trivial subspace $\bar{U}$ of $\bar{V}$ fixed by N. Since $\Gamma_{2n,p}$ normailizes N, $\bar{U}$ must be one of the two mutually orthogonal $\Gamma_{2n,p}$-summands. By orthogonality, N must preserve the other summand. Since that summand is also $\Gamma_{2n,p}$-irreducible, N must be trivial, a contradiction. Thus, I° is reductive. We claim that $\bar{V}$ is an irreducible I°-module. If not, then I° admits a $2n$-dimensional orthogonal representation such that there exists a Weyl group element in I° permuting transitively all weights. We need the following:

LEMMA 11.2. — *Let $\mathcal{G}$ be a connected reductive group over an algebraically closed field of characteristic $\neq 2$. Then $\mathcal{G}$ has no minuscule orthogonal representations of even dimension such that there exists a Weyl group element permuting transitively all weights.*

Proof. — We may assume that $\mathcal{G}$ is semi-simple and that $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_k$, a product of almost simple groups. If V is a minuscule, self-dual representation of $\mathcal{G}$ then $V = V_1 \otimes \cdots \otimes V_k$ where V_i are minuscule and self-dual representations of $\mathcal{G}_i$. If $\mathcal{G}$ has a Weyl group element $w = w_1 \times \cdots \times w_k$ permuting transitively all weights of V, then w_i must permute transitively all weights of V_i and dimensions of V_i must be pairwise relatively prime. If $\mathcal{G}$ is simple, an argument in §2 of [KLS] shows that the only minuscule, self-dual representations with such Weyl group element is the standard representation of Sp_{2n} and its Frobenius twists. (The list there includes also the standard representation of SO_{2n}, but this can be excluded by a direct inspection.) Since even numbers are never pairwise relatively prime, we conclude that $\mathcal{G}$ is simple and that the representation is the standard representation of Sp_{2n}. This representation is not orthogonal, however, and the lemma follows. $\square$

The lemma implies that $\bar{V}$ is an irreducible representation of I°. Therefore, the pair $(I^\circ, \bar{V})$ satisfies conditions of Proposition 7.3. It follows that $I^\circ = H$ or, if $n = 3$, $I^\circ = \mathrm{G}_2(\bar{\mathbb{F}}_\ell)$. Since G_2 has trivial center, no outer automorphisms, and it acts irreducibly on $\bar{V}$, any element of I/I° is represented by a scalar matrix. However, by Čebotarev's density theorem, any element in $\bar{\Gamma}$ has 1 as an eigenvalue. It follows that $I = I^\circ$ in all cases. Since the image of the local decomposition group D_2 contains elements of order 2 which are not contained in G_2 we see that I cannot be G_2. Thus we have $I^\circ = H$ in all cases. This is a contradiction. The theorem is proved with $d(n) = \max(A(n), I(n))$. $\square$

Summarizing, we have shown that mod ℓ reduction of the representations r_Π give rise to $\mathrm{G}_2(\mathbb{F}_{\ell^k})$ (or a Ree group if $\ell = 3$), $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ or $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})$ as Galois groups. In other words we have essentially proved the following theorem that we stated in the introduction:

Theorem 11.3. — *Let t be a positive integer.*

1. *Let ℓ be a prime. Then there exists an integer k divisible by t such that the simple group $\mathrm{G}_2(\mathbb{F}_{\ell^k})$ appears as a Galois group over $\mathbb{Q}$.*
2. *Let ℓ be an odd prime. Then there exists an integer k divisible by t such that the finite simple group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ or the finite classical group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})$ appears as a Galois group over $\mathbb{Q}$.*
3. *If $\ell \equiv 3, 5 \pmod 8$, then there exists an integer k divisible by t such that the finite simple group $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ appears as a Galois group over $\mathbb{Q}$.*

Proof. — Since $r_\Pi(I_q)$ has order p, the divisibility of k by t follows from part (3) of Lemma 3.3. If $n = 3$, $\ell = 3$, and we assume that t is even as we may, then no Ree group ${}^2\mathrm{G}_2(\mathbb{F}_{3^{2f+1}})$ contains an element of order p. Indeed,

$$ {}^2\mathrm{G}_2(\mathbb{F}_{3^{2f+1}}) < \mathrm{G}_2(\mathbb{F}_{3^{2f+1}}) < \mathrm{SO}_7(\mathbb{F}_{3^{2f+1}}), $$

and t does not divide $2f + 1$. This shows that the reduction of r_Π modulo ℓ cannot be a Ree group. It remains to deal with the third statement. Assume now that the Galois group given by part (2) is $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})$. Then the subgroup $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$ of index 2 defines a quadratic field L. This field is unramified outside $\{2, \ell, q, \infty\}$, since the same holds for the representation r_Π. Since the image of the inertia I_q is of order p, it lands in the subgroup $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$. Thus, L is unramified at q also. Moreover, by Proposition 4.1, the image of the decomposition group D_2 is a group such that the quotient by its commutator is odd. Such a group must be contained in the subgroup $\mathrm{SO}_{2n+1}(\mathbb{F}_{\ell^k})^{\mathrm{der}}$. This shows not only that that L is unramified at 2, but moreover 2 splits in L. We remind the reader that for an odd prime ℓ the unique quadratic field unramified outside $\{\ell, \infty\}$ is $\mathbb{Q}(\sqrt{\ell})$ if $\ell \equiv 1 \pmod 4$ and $\mathbb{Q}(\sqrt{-\ell})$ if $\ell \equiv 3 \pmod 4$. However, since 2 splits in this field if and only if $\ell \equiv 1, 7 \pmod 8$ we see that if $\ell \equiv 3, 5 \pmod 8$ the Galois group constructed in part (2) is in fact $\mathrm{SO}_{2n+1}(\mathbb{F}_\ell^k)^{\mathrm{der}}$. □

12. On future directions

One difficulty that we needed to address in this paper came from the fact that the group $\mathrm{GL}_{2n+1}(\mathbb{Q}_p)$ has no self-dual supercuspidal representation unless $p = 2$. In order to construct Galois groups of type B_n this problem was resolved by introducing the self-dual supercuspidal representation Π_2 of $\mathrm{GL}_{2n+1}(\mathbb{Q}_2)$ whose parameter contains a Jordan subgroup of $\mathrm{SO}_{2n+1}(\mathbb{C})$. For Galois groups of type G_2 the construction is based on a technical improvement of Theorem 1.1 due to Shin, which is based on the fundamental lemma for unitary groups. Another way, which avoids the use of the fundamental lemma, would be to pick Π_2 so that its parameter comes from the Jordan subgroup in G_2. More precisely the parameter of Π_2 should be the homomorphism $\phi_2 : W_{\mathbb{Q}_2} \to \mathrm{G}_2$ described in Proposition 4.2. In order to obtain a global lift from G_2 to GL_7 with this Π_2 as a local component one would need to complete the following (doable) program:

- Define, via induction from an open compact subgroup, a generic supercuspidal representation σ_2 of $\mathrm{G}_2(\mathbb{Q}_2)$ corresponding to the parameter ϕ_2.
- Compute the theta lift of σ_2 to $\mathrm{PGSp}_6(\mathbb{Q}_2)$.
- Show, using the method of [Sa2], that the further lift to $\mathrm{GL}_7(\mathbb{Q}_2)$ is Π_2.

A construction of supercuspidal representations attached to parameters arising from Jordan subgroups is a subject of the forthcoming paper by Gross and Reeder [GR]. The completion of the three step program would give Galois groups of type G_2 except in the residual characteristic 2 without using results of Shin [Sh]. There is yet another approach which removes the restriction $\ell \neq 2$, but introduces a different conjecture. Let G denote Sp_{2n} or G_2. Then using the trace formula it is possible to show that there exists a cuspidal automorphic representation σ of $G(\mathbb{A})$ unramified at all primes different from ℓ, q and such that

- σ_∞ is a discrete series representation with a large (unspecified) parameter (weight).
- σ_q is a specified supercuspidal representation.
- σ_ℓ is the Steinberg representation.

Assuming that σ is globally generic then Π, the lift of σ to $\mathrm{GL}_{2n+1}(\mathbb{A})$, is automatically cuspidal and has a discrete series representation at one local place, since Π_ℓ is the Steinberg representation of $\mathrm{GL}_{2n+1}(\mathbb{Q}_\ell)$. (We use here that the theta lift of the Steinberg representation of $\mathrm{G}_2(\mathbb{Q}_\ell)$ is the Steinberg representation of $\mathrm{PGSp}_6(\mathbb{Q}_\ell)$, see [GrS].) Since matrix coefficients of the Steinberg representation are in $L^{1+\epsilon}(G)$ and therefore not integrable, we note that the method of Poincaré series cannot be used to construct such σ.

In principle our method could be extended to other groups. The main limitation at the moment is the lack of ℓ-adic representations attached to automorphic representations. If we assume, for example, that one can attach a 26-dimensional ℓ-adic representation to an algebraic automorphic form of the exceptional group F_4 then we would be able to construct finite groups of type F_4 as Galois groups over $\mathbb{Q}$. Indeed, to this end one would pick a cuspidal automorphic representation σ of F_4 such that for two primes p_1 and p_2 the local components σ_{p_1} and σ_{p_2} are tame supercuspidal representations whose parameters have groups of type $(8, p_1)$ and $(12, p_2)$, respectively, as the image. Thus, if the two parameters at p_1 and p_2 are picked so that the images of the local decomposition groups are deeply embedded, then the results of Section 10 imply that the restriction modulo ℓ of the ℓ-adic representation attached to σ will give finite groups of type $\mathrm{F}_4(\mathbb{F}_{\ell^k})$ as Galois groups over $\mathbb{Q}$.

13. Errata to [KLS]

- With the definition of the group of type (n, p) in [KLS], to ensure that $\bar{\rho}(D_q)$ in §5.2 be of type (n, p) we should ask that the K of §3.3 also contain $\mathbb{Q}(\zeta_\ell)$, in addition to the other conditions there. Alternatively, and better, the definition of a group of type (n, p) in [KLS] could be modified (and made less restrictive) as in Definition

10.2 below. All relevant statements in [KLS] then go through with this altered definition, with obvious modifications in their proof.

- L. Dieulefait and G. Wiese pointed out a mistake in the arguments of [KLS] because of which the main theorem of loc. cit. has to be weakened as follows:

  Theorem 13.1. — *If we fix a prime ℓ and integers $n, t \geqslant 1$ with $n = 2m$ even, the finite simple group* $\mathrm{PSp}_n(\mathbb{F}_{\ell^k})$ *or* $\mathrm{PGSp}_n(\mathbb{F}_{\ell^k})$ *occurs as a Galois group over $\mathbb{Q}$ for some integer k divisible by t.*

  The mistakes in the arguments are:

  – The last sentence of Corollary 2.6 is wrong, as also is the last sentence of its proof. Both should be disregarded.

  – The last paragraph of §5.2 is wrong and should be disregarded.

  – Remark (iii) on page 561 should be disregarded.

Bibliography

[Ca] Carter (R.). — Finite Groups of Lie Type, Wiley Classics Library, New York, 1993.

[Cl] Clozel (L.). — Représentations galoisiennes associées aux représentations automorphes autoduales de GL(n). Inst. Hautes Études Sci. Publ. Math. No. 73, p. 97-145 (1991).

[CKPS] Cogdell (J.), Kim (H.), Piatetski-Shapiro (I.) and Shahidi (F.). — Functoriality for the classical groups. Publ. Math. Inst. Hautes Études Sci. No. 99, p. 163-233 (2004).

[DR] DeBacker (S.) and Reeder (M.). — Depth zero supercuspidal L-packets and their stability. Annals of Math. 169, No. 3, p. 795-901 (2009).

[Ga] Gan (W. T.). — Exceptional Howe correspondences over finite fields. Compositio Math. 118, p. 323-344 (1999).

[GaS1] Gan (W. T.) and Savin (G.). — Real and global lifts from PGL_3 to G_2. Inter. Math. Res. Not. 50, p. 2699-2724 (2003).

[GaS2] Gan (W. T.) and Savin (G.). — Endoscopic lifts from PGL_3 to G_2. Compositio Math. 140, p. 793-808 (2004).

[GRS] Ginzburg (D.), Rallis (S.) and Soudry (D.). — A tower of theta correspondences for G_2. Duke Math. J. 88, p. 537-624 (1997).

[GR] Gross (B. H.) and Reeder (M.). — Arithmetic invariants of discrete Langlands parameters. In preparation.

[GrS] Gross (B. H.) and Savin (G.). — Motives with Galois group of type G_2: an exceptional theta correspondence. Compositio Math. 114, p. 153-217 (1998).

[HT] Harris (M.), Taylor (R.). — The geometry and cohomology of some simple Shimura varieties. Annals of Mathematics Studies, 151. Princeton University Press, Princeton, NJ, 2001. viii+276 pp.

[Ha] HARRIS (M.). — Potential automorphy of odd-dimensional symmetric powers of elliptic curves, and applications. to appear in Algebra, Arithmetic, and Geometry: Manin Festschrift (Birkhuser, in press).

[HPS] HUANG (J. S.), PANDŽIĆ (P.) and SAVIN (G.). — New dual pair correspondences. Duke Math. J. 82, p. 447-471 (1996).

[Hu1] HUMPHREYS (J. E.). — Linear Algebraic Groups. Graduate Texts in Mathematics, 21. Springer-Verlag, New York, 1975.

[Hu2] HUMPHREYS (J. E.). — Conjugacy classes in semi-simple algebraic groups. Mathematical Surveys and Monographs, 43. American Mathematical Society, Providence, RI, 1995.

[JS1] JIANG (D.), SOUDRY (D.). — The local converse theorem for $\mathrm{SO}(2n+1)$ and applications. Ann. of Math. (2) 157 (2003), no. 3, 743-806.

[JS2] JIANG (D.), SOUDRY (D.). — Lecture at the workshop on Automorphic Forms, Geometry and Arithmetic. Oberwolfach, February 2008. Announcement available at `http://www.mfo.de/`

[KLS] KHARE (C.), LARSEN (M.) and SAVIN (G.). — Functoriality and the inverse Galois problem. Compositio Math. 144 (2008), 541–564.

[KT] KOSTRIKIN (A. I.) and TIEP (P. H.). — Orthogonal Decompositions and Integral Lattices, De Gruyter Expositions in Mathematics 15, Walter de Gruyter, Berlin - New York, 1994.

[KW] KHARE (C.) and WINTENBERGER (J-P.). — Serre's modularity conjecture (I), Invent Math. 178, p. 485-504 (2009).

[La] LARSEN (M.). — Maximality of Galois actions for compatible systems. Duke Math. J. 80, no. 3, p. 601-630 (1995).

[LP] LARSEN (M.) and PINK (R.). — Finite subgroups of algebraic groups. preprint available at `http://www.math.ethz.ch/~pink/publications.html`

[MaS] MAGAARD (K.) and SAVIN (G.). — Exceptional theta correspondences. Compositio Math. 107, p. 89-123 (1997).

[Moy] MOY (A.). — The irreducible orthogonal and symplectic Galois representations of a p-adic field (the tame case). Journal of Number Theory 10, p. 341-344 (1984).

[Mu] MUIĆ (G.). — The unitary dual of p-adic G_2. Duke Math. J. 90, p. 465-493 (1997).

[Sa1] SAVIN (G.). — K-types of minimal representations (p-adic case). Glasnik Mat. Vol. 31(51), p. 93-99.

[Sa2] SAVIN (G.). — Lifting of generic depth zero representations of classical groups. J. of Algebra 319, p. 3244-3258 (2008).

[Sh] SUG WOO SHIN. — Galois representations arising from some compact Shimura varieties. Preprint, IAS, (2008).

[Ta] TADIĆ (M.). — Representations of p-adic symplectic groups. Compositio Math. 90, p. 123-181 (1994).

[Ty] TAYLOR (R.). — Galois representations. Ann. Fac. Sci. Toulouse Math. 13, p. 73-119 (2004).

[W] WIESE (G.). — On projective linear groups over finite fields as Galois groups over the rational numbers. Modular Forms on Schiermonnikoog edited by Bas Edixhoven, Gerard van der Geer and Ben Moonen. Cambridge University Press, p. 343-350 (2008).