Adjoint Swan conductors I: The essentially tame case

Mark Reeder*
reederma@bc.edu

September 17, 2016

Abstract

Let $\mathcal{W}$ be the Weil group of a p-adic field and let $\mathfrak{g}$ be a simple complex Lie algebra. We prove lower bounds for Swan conductors of representations of $\mathcal{W}$ by automorphisms of $\mathfrak{g}$ and give necessary and sufficient conditions for equality. We also relate these bounds to the Local Langlands Correspondence and to the representation theory of p-adic groups.

1 Introduction

Let G be a complex semisimple (or reductive) Lie group and let $g \in G$ have centralizer $C_G(g)$. From the fact that g is contained in at least one Borel subgroup of G, it follows that

$$\dim C_G(g) \geq \operatorname{rank} G. \tag{1}$$

Those $g \in G$ for which $\dim C_G(g) = \operatorname{rank} G$ are called *regular*; their study was inititated by Kostant [13] and Steinberg [21]. Regular elements are precisely those which are contained in only finitely many Borel subgroups of G. Later in [24] Steinberg extended this result to arbitrary $g \in G$ by showing that the singularity of g is measured by

$$\dim C_G(g) - \operatorname{rank} G = 2 \dim \mathcal{B}_G^g, \tag{2}$$

where $\mathcal{B}_G^g$ is the variety of all Borel subgroups of G containing g.

A *Langlands parameter* may be thought of as an "element" in G (or a group close to G), enhanced by arithmetic data arising from a Galois extension of p-adic fields. From this viewpoint, both (1) and (2) become statements about tamely ramified Langlands parameters. Our goal in this multi-part paper is to prove analogues of (1) and (2) for wildly ramified Langlands parameters, in which $\dim \mathcal{B}_G^g$ is replaced by and combined with (a variant of) the Swan conductor of the adjoint representation of G.

*Supported by NSF grant DMS-1303418

This interaction between two apparently distinct areas of mathematics - local Galois theory and complex Lie theory - is predicted by the Local Langlands Conjectures (LLC). Our results verify unconditionally some consequences of the LLC which arise from the formal degree conjecture of [10] and the construction of epipelagic representations of p-adic groups [18]. The latter are minimized in this paper, in order to highlight the Galois vs Lie interaction. However our results also imply a new existence result for epipelagic representations.

Let k be a field which is complete and locally compact with respect to a discrete valuation, of residue characteristic $p > 0$. Fix a separable closure $\bar{k}$ and let $\mathcal{W} \subset \mathrm{Gal}(\bar{k}/k)$ be the Weil group of k. Let K and K^t be the maximal unramified and tamely ramified extensions, respectively, of k contained in $\bar{k}$. We have corresponding normal subgroups

$$\mathcal{P} < \mathcal{I} < \mathcal{W},$$

where $\mathcal{I} = \mathrm{Gal}(\bar{k}/K)$ and $\mathcal{P} = \mathrm{Gal}(\bar{k}/K^t)$.

Let

$$\varphi : \mathcal{W} \longrightarrow \mathrm{GL}(V)$$

be a continuous finite-dimensional complex representation. The image $I := \varphi(\mathcal{I})$ is finite, and $P := \varphi(\mathcal{P})$ is the unique Sylow p-subgroup of I. We have $I = S \cdot P$, where S is a cyclic subgroup of I, of order prime to p; this *tame inertial factor* S is unique up to P-conjugacy. If $P = 1$ we say φ is *tamely ramified*. Otherwise φ is *wildly ramified*. If I fixes no nonzero vector in V we say φ is *totally ramified*.

The valuation on k and its extension fields gives rise to a finite filtration $P = P_1 \geq P_2 \geq \cdots$ by *ramification subgroups* of P, and the wild ramification of φ is measured by the *Swan conductor*:

$$\mathsf{sw}(\varphi, V) = \sum_{j \geq 1} \frac{\dim(V/V^{P_j})}{[I : P_j]}. \tag{3}$$

Here V^{P_j} is the subspace of vectors fixed by the ramification group P_j and the sum is actually finite.

Suppose now that $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$ is a continuous representation of $\mathcal{W}$ by automorphisms of a simple complex Lie algebra $\mathfrak{g}$. In this situation we consider a variant of the Swan conductor, namely

$$\mathsf{swr}(\varphi, \mathfrak{g}) := \mathsf{sw}(\varphi, \mathfrak{g}) + \mathrm{rank}\, \mathfrak{g}^I,$$

where we have added the rank of the (reductive) Lie subalgebra $\mathfrak{g}^I$ of I-fixed vectors in $\mathfrak{g}$. So we have $\mathsf{swr}(\varphi, \mathfrak{g}) = \mathsf{sw}(\varphi, \mathfrak{g})$ exactly when φ is totally ramified.

By analogy with (1) and (2), our results will consist of lower bounds for $\mathsf{swr}(\varphi, \mathfrak{g})$ along with analysis of those φ for which equality occurs.

As a simple example, suppose I is contained in a torus. Then $\mathrm{rank}\, \mathfrak{g}^I = \mathrm{rank}\, \mathfrak{g}$, so we have

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq \mathrm{rank}\, \mathfrak{g},$$

with equality if and only if φ is tamely ramified.

In this first paper we consider the next level of complexity: We say φ is *essentially tame* if P is contained in a torus. This generalizes the definition for GL_n given in [5]. If we assume at the outset that p does not divide the order of the Weyl group of $\mathfrak{g}$ then all representations $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$ are essentially tame, as follows from an old result of Borel and Serre [2].

To simplify the exposition, we will also assume in this introduction that I lies in the neutral component $G = \mathrm{Aut}(\mathfrak{g})^\circ$. (This corresponds to the LLC for p-adic groups splitting over K.) More general parameters are treated in the body of the paper.

The cyclic group S normalizes a Cartan-Borel pair $\mathfrak{t} \subset \mathfrak{b}$ inside the reductive Lie algebra $\mathfrak{g}^P$. Let $\mathfrak{t}^S$ be the subspace of S-invariants in $\mathfrak{t}$ and let $L = C_G(\mathfrak{t}^S)$ be the centralizer of $\mathfrak{t}^S$ in G. Then L is a Levi subgroup of G containing S. We have $L = G$ precisely when φ is totally ramified.

The essentially tame condition means that $\mathfrak{t}$ is actually a Cartan subalgebra of $\mathfrak{g}$. Let W be the Weyl group of $\mathfrak{t}$ in $\mathfrak{g}$ and let R be the set of roots of $\mathfrak{t}$ in $\mathfrak{g}$. The action of S on $\mathfrak{t}$ gives a map $S \to \mathrm{Aut}(R)$ into the automorphism group of the root system R. The assumption that $I \subset G$ implies that the image of S actually lies in W.

We can now state our main result.

Theorem 1.1. *Assume $\varphi : \mathcal{W} \to G$ is wildly ramified and essentially tame. Then we have*

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq \dim C_L(S) \tag{4}$$

with equality if and only if the following conditions hold:

(i) $L = G$ (so φ is totally ramified);

(ii) The second ramification group P_2 is trivial;

(iii) The image of S in W is elliptic and regular.

Here the image of S is *elliptic in W* if S fixes no nonzero vector in the root lattice $\mathbb{Z}R$, and the image of S is *regular in W* if S acts freely on R. (Note that regularity in G and in W are distinct notions. For historical reasons we cannot avoid this unfortunate conflict of terminology.)

Applying (2) to L, the inequality (4) may be written as

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq 2\dim \mathcal{B}_L^S + \mathrm{rank}\, G,$$

where $\mathcal{B}_L^S$ is the variety of Borel subgroups of L containing S. Now if S has elliptic regular image in W, then S is also regular in G if and only if the image of S in W is a Coxeter element. Since $\dim \mathcal{B}_G^S = 0$ exactly when S is regular in G, we obtain:

Corollary 1.2. *Assume $\varphi : \mathcal{W} \to G$ is wildly ramified and essentially tame. Then we have*

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq \mathrm{rank}\, G, \tag{5}$$

with equality if and only if the following hold:

(i) $L = G$ (so φ is totally ramified);

(ii) The second ramification group P_2 is trivial;

(iii) The image of S in W is generated by a Coxeter element.

The inequality (5) was proved in [9] assuming *a priori* that $L = G$ (and that $I \subset G$). The significance of (5) will be discussed later in this introduction. The full version of Thm. 1.1 is given in Thm. 4.1 below.

We also prove a converse to Thm. 1.1, which amounts to an existence result:

Theorem 1.3. *Assume that p does not divide the order of W. Given an elliptic regular cyclic subgroup $S \subset \mathrm{Aut}(R)$, there exists a totally ramified representation $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$ whose tame inertial factor is S and for which $\mathsf{swr}(\varphi, \mathfrak{g}) = \dim C_G(S)$.*

The full version of 1.3 is given in section 5. The proofs of Thms. 1.1 and 1.3 are mostly uniform arguments, along with some case-by-case analysis of exceptional root systems.

So far, our analogies to (1) and (2) only apply to semisimple (in fact torsion) elements in G. The unipotent part arises as follows. A *discrete parameter* is a homomorphism

$$\psi : \mathcal{W} \times \mathrm{SL}_2(\mathbb{C}) \longrightarrow G$$

which is continuous on $\mathcal{W}$ and algebraic on $\mathrm{SL}_2(\mathbb{C})$, and whose image has finite centralizer in G. Via the Jordan decomposition, a discrete parameter may again be regarded as a "element" of G: the restriction $\varphi = \psi|_{\mathcal{W}}$ is the "semisimple" part, and $\psi|_{\mathrm{SL}_2}$ is the "unipotent" part, via the Jacobson-Morozov theorem.

Let I, S, P be defined as above for $\varphi := \psi|_{\mathcal{W}}$. Then $\psi(\mathrm{SL}_2)$ is contained in the connected centralizer $H = C_G(I)^\circ$. Let $u \in H$ be the image under ψ of a nontrivial unipotent element of SL_2 and let $\mathcal{B}_H^u$ be the variety of Borel subgroups of H containing u. Applying (2) to H and u, we have that

$$\dim C_H(u) - \mathrm{rank}\, H = 2 \dim \mathcal{B}_H^u.$$

Now take the average of this geometric difference and the arithmetic difference from Cor.1.2 and define

$$\mathsf{v}(\psi) := \tfrac{1}{2}[\dim C_H(u) - \mathrm{rank}\, H] + \tfrac{1}{2}[\mathsf{swr}(\varphi, \mathfrak{g}) - \mathrm{rank}\, G]. \qquad (6)$$

From [9] it is known that $\mathsf{v}(\psi)$ is an integer.

As a simple example, if φ is tamely ramified then $I = S = \langle s \rangle$, say, so we have $\mathcal{B}_H^u = \mathcal{B}_G^g$, where $g = su$. In this case we just have $\mathsf{v}(\psi) = \dim \mathcal{B}_G^g = \frac{1}{2}[\dim C_G(g) - \mathrm{rank}\, G]$, as in (2).

Cor. 1.2 implies the following generalization of (1) and extends the notion of regular element to discrete parameters.

Corollary 1.4. *Assume that p does not divide the order of W. For every discrete parameter ψ we have $\mathsf{v}(\psi) \geq 0$, and $\mathsf{v}(\psi) = 0$ if and only if one of the following holds.*

1. *$\psi|_{\mathcal{W}}$ is tamely ramified and su is a regular element in G, or*
2. *$\psi|_{\mathcal{W}}$ is totally and wildly ramified and $g = s$ is a regular torsion element of minimal order.*

The elements in case 2 are Kostant's *principal elements*, cf. [13]; they are representatives in G of Coxeter elements in W.

We now explain the role of p-adic groups in the above results. Assume the residue field of k has finite cardinality q, and let $\mathcal{G}$ be a simply connected group over k whose absolute root datum is dual to that of G. The LLC predicts the existence of a finite-to-one surjective mapping $\pi \mapsto \psi_\pi$ from the set of (equivalence classes of) discrete series representations of $\mathcal{G}(k)$ to the set of (G-conjugacy classes of) discrete parameters $\psi : \mathcal{W} \times \mathrm{SL}_2(\mathbb{C}) \to G$. For example if $\pi = St$ is the Steinberg representation then ψ_{St} is trivial on $\mathcal{W}$ and u is a regular unipotent element in G.

Each discrete series representation π has a numerical invariant $\deg(\pi)$, the *formal degree*, whose value depends on a choice of Haar measure on $\mathcal{G}(k)$. We choose the measure making $\deg(St) = 1$. Based on examples and heuristic arguments, one expects the formal degree of any discrete series representation π to have the form

$$\deg(\pi) = q^{d(\pi)} \cdot \Gamma(q),$$

where $d(\pi)$ is a *nonnegative* integer and $\Gamma(x) \in \mathbb{Q}(x)$ is a rational function such that $\Gamma(0) \neq 0$. Here, q is the cardinality of the residue field of k; see [9, 7.2] for a more precise statement.

A conjectural formula for $\deg(\pi)$ in terms of an adjoint gamma value of ψ_π was given in [10]. As shown in [9], this prediction implies that

$$d(\pi) = \mathsf{v}(\psi_\pi), \tag{7}$$

where $\mathsf{v}(\psi_\pi)$ is the integer defined in (6). Thus, $d(\pi)$ plays a role for representations of general groups $\mathcal{G}(k)$ that is similar to the role played by the exponents of Godement-Jacquet local epsilon factors attached to representations of $\mathrm{GL}_n(k)$, whose direct analogues have not been defined for general $\mathcal{G}$. Equation (7) and its heuristics lead to the expectation (but not a proof) that $\mathsf{v}(\psi) \geq 0$ for any discrete parameter ψ; this expectation is confirmed by Cor. 1.4 in the case $p \nmid |W|$.

All of our results described so far are unconditional. However, if we *assume* the LLC and its expected properties, including (7), then Cor. 1.4 classifies those discrete series representations of $\mathcal{G}(k)$ having formal degree prime to p, as follows.

Corollary 1.5. *Assume that p does not divide the order of W and that the LLC with property* (7) *holds. Then for every irreducible discrete series representation π of $\mathcal{G}(k)$ we have $d(\pi) \geq 0$, and $d(\pi) = 0$ if and only if one of the following holds:*

1. *π is a depth-zero lift from the Steinberg representation on an endoscopic group for $\mathcal{G}$, or*
2. *π is a simple supercuspidal representation.*

The representations in case 1 interpolate between the Steinberg representation St (where u is regular in G) and the depth zero supercuspidal representations in [7] (where $u = 1$ and s is regular). The intermediate representations in case 1 were found by the author in 2001, but are not yet written up for publication. The representations in case 2 are constructed in [9].

As a by-product, Thm 1.3 sharpens the existence criteria for epipelagic representations constructed in [18], where the residue field of k was assumed to be sufficiently large. Thm. 1.3 implies that this existence criterion holds assuming only that p does not divide $|W|$. It is likely that even this last assumption is not necessary (cf. [8]).

In this first paper we have assumed φ is essentially tame. Without this assumption the structure of φ changes drastically. For example, S no longer gives rise to a subgroup of the Weyl group.

However, the inequality of Cor. 1.2 is still expected to hold, even though the conditions for equality will be completely different. This will be the topic of [16].

I thank the referees for valuable comments, including corrections to some errors in the tables of section 4.6.

Basic notation for groups: If g is a permutation of a set X then $X^g := \{x \in X : \ gx = x\}$. If J is a group acting on X then $X^J = \cap_{g \in J} X^g$. If $g, h, \ldots$ are elements or subsets of J then $\langle g, h, \ldots \rangle$ is the subgroup of J generated by $g, h, \ldots$. If $g \in J$ has finite order then $|g|$ is the order of $\langle g \rangle$. The centralizer of an element $g \in J$ or a subgroup $H < J$ is denoted by $C_J(g)$ or $C_J(H)$.

2 Ramification groups and Swan conductors

Throughout this paper, k is a field which is complete and locally compact with respect to a discrete valuation and which has residue characteristic $p > 0$. The Weil group of k, and its inertia and wild inertia subgroups are usually denoted $\mathcal{W} > \mathcal{I} > \mathcal{P}$, respectively. Sometimes for clarity we write $\mathcal{W}_k = \mathcal{W}$, etc. For more details in this section see [19].

By a "representation" $\varphi : \mathcal{W} \to \mathrm{GL}(V)$ we mean that φ is a continuous representation of $\mathcal{W}$ on a finite dimensional complex vector space V, where $\mathrm{GL}(V)$ has the discrete topology. Thus, continuity is equivalent to $\ker \varphi$ being an open subgroup of $\mathcal{W}$. This implies that the inertial image $\varphi(\mathcal{I})$ is finite.

Given a representation $\varphi : \mathcal{W} \to \mathrm{GL}(V)$, let $I = \varphi(\mathcal{I})$ and $P = \varphi(\mathcal{P})$ be the images of the inertia and wild inertia subgroups and let

$$P = P_1 \geq P_2 \geq \cdots \geq P_c > P_{c+1} = 1$$

be the ramification filtration in the lower numbering. Each P_j is normal in $\varphi(\mathcal{W})$, and $I = S \cdot P$, where S is cyclic of order prime to p. The Swan conductor of φ may be defined by the explicit formula

$$\mathsf{sw}(\varphi, V) = \sum_{j \geq 1} \frac{\dim(V/V^{P_j})}{[I : P_j]}. \tag{8}$$

A more illuminating definition of $\mathsf{sw}(\varphi, V)$ is the following. Let $\{P^u : \ u \geq 0\}$ be the upper numbering of the ramification subgroups. This is now a filtration by real numbers in which $P^0 = I$ and for $u > 0$ we have $P^u = P_j$ for some $j = j(u) \geq 1$. The *depth* of φ is the following (well-defined) real number:

$$\mathrm{depth}(\varphi) := \max\{u : \ P^u \neq 1\}.$$

The Swan conductor $\mathsf{sw}(\varphi, V)$ is then characterized by the following two properties:

1. $\mathsf{sw}(\varphi_1 \oplus \varphi_2, V_1 \oplus V_2) = \mathsf{sw}(\varphi_1, V_1) + \mathsf{sw}(\varphi_2, V_2)$.
2. $\mathsf{sw}(\varphi, V) = \dim(V) \cdot \mathrm{depth}(\varphi)$ if V is irreducible.

It is clear that $\mathsf{sw}(\varphi, V)$ depends only on the inertial image I together with its filtration, and that $\mathsf{sw}(\varphi, V) = 0$ if and only if $P = 1$. Less obviously, $\mathsf{sw}(\varphi, V)$ is actually an *integer*.

The Swan conductor has an inductivity formula [19, VI.2] which we will need only in a simple case: Suppose (φ, V) is induced from a representation $\rho : \mathcal{W}_L \to \mathrm{GL}(U)$, where L/k is a totally and tamely ramified finite extension. Then we have

$$\mathsf{sw}(\varphi, V) = \mathsf{sw}(\rho, U). \tag{9}$$

3 Representations on Lie algebras

Throughout this paper $\mathfrak{g}$ is a simple complex Lie algebra, $\mathrm{Aut}(\mathfrak{g})$ is the algebraic group of automorphisms of $\mathfrak{g}$, and $G = \mathrm{Aut}(\mathfrak{g})^\circ$ is the neutral component of $\mathrm{Aut}(\mathfrak{g})$. We will study representations $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$ of $\mathcal{W}$ by Lie algebra automorphisms. Two such representations are considered equivalent if they are conjugate by G.

Given a representation $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$, let $I = \varphi(\mathcal{I})$, $P = \varphi(\mathcal{P})$, with $I = S \cdot P$ and ramification groups P_j be as in section 2. Since I is finite, it consists of semisimple automorphisms of the complex Lie algebra $\mathfrak{g}$. Hence each fixed-point subspace $\mathfrak{g}^I$, $\mathfrak{g}^{P_j}$ is a reductive Lie-subalgebra of $\mathfrak{g}$ [23, 2.19]. We set

$$\mathfrak{g}_0 = \mathfrak{g}^I \qquad \text{and} \qquad \mathfrak{g}_1 = \mathfrak{g}^P.$$

We define the *Swan-rank* $\mathsf{swr}(\varphi, \mathfrak{g})$ of φ by the formula

$$\mathsf{swr}(\varphi, \mathfrak{g}) = \mathsf{sw}(\varphi, \mathfrak{g}) + \mathrm{rank}\, \mathfrak{g}_0. \tag{10}$$

Since equivalence is defined via conjugation by Lie algebra automorphisms, it is clear that if φ_1 and φ_2 are equivalent representations of $\mathcal{W}$ by automorphisms of $\mathfrak{g}$ then $\mathsf{swr}(\varphi_1, \mathfrak{g}) = \mathsf{swr}(\varphi_2, \mathfrak{g})$.

Each subalgebra $\mathfrak{g}^{P_j}$ is preserved by I. In particular we have a canonical S-stable decomposition

$$\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{m}, \tag{11}$$

where $\mathfrak{m}$ is spanned by the nontrivial P-isotypic components in $\mathfrak{g}$. Since P acts trivially on $\mathfrak{g}_1$ we have

$$\mathsf{sw}(\varphi, \mathfrak{g}) = \mathsf{sw}(\varphi, \mathfrak{m}).$$

3.1 A Levi subalgebra

Recall our notation: $\mathfrak{g}_1 = \mathfrak{g}^P$ and $\mathfrak{g}_0 = \mathfrak{g}^I$. The cyclic group S normalizes $\mathfrak{g}_1$, so we have $\mathfrak{g}_0 = \mathfrak{g}_1^S$. We choose, as we may [22, Thm.7.5], S-stable Cartan and Borel subalgebras $\mathfrak{t}_1 \subset \mathfrak{b}_1$ of $\mathfrak{g}_1$.

The fixed-point subalgebra

$$\mathfrak{t}_0 := \mathfrak{t}_1^S$$

is a Cartan subalgebra of $\mathfrak{g}_0$ and contains regular elements of $\mathfrak{g}_1$. Let

$$\mathfrak{l} = \{x \in \mathfrak{g} : \ [x, \mathfrak{t}_0] = 0\}$$

be the centralizer of $\mathfrak{t}_0$ in $\mathfrak{g}$. We have

$$\dim \mathfrak{t}_0 = \operatorname{rank} \mathfrak{g}_0 \quad \text{and} \quad \mathfrak{l} \cap \mathfrak{g}_1 = \mathfrak{t}_1. \tag{12}$$

The centralizer $L = C_G(\mathfrak{t}_0)$ is the Levi subgroup of G with Lie algebra $\mathfrak{l}$. We have $S < L$ and $\mathfrak{l}^S$ is the centralizer of $\mathfrak{t}_0$ in $\mathfrak{g}^S$. Hence $\mathfrak{l}^S$ is a Levi subalgebra of $\mathfrak{g}^S$, so we have

$$\operatorname{rank} \mathfrak{g}^S \leq \dim \mathfrak{l}^S. \tag{13}$$

The next result relates this inequality to the decomposition $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{m}$ from (11).

Lemma 3.1. *Suppose we have*

$$\dim \mathfrak{m}^S \leq \mathsf{sw}(\varphi, \mathfrak{m}). \tag{14}$$

Then $\dim \mathfrak{l}^S \leq \mathsf{swr}(\varphi, \mathfrak{g})$ *with equality if and only if the following hold:*

(a) $\dim \mathfrak{m}^S = \mathsf{sw}(\varphi, \mathfrak{m})$*;*

(b) $[\mathfrak{t}_0, \mathfrak{m}^S] = 0$.

Proof. We note that $[\mathfrak{g}_1, \mathfrak{m}] \subset \mathfrak{m}$. Since $\mathfrak{t}_0 \subset \mathfrak{g}_1$ and $\mathfrak{t}_1 = \mathfrak{l} \cap \mathfrak{g}_1$, we have

$$\mathfrak{l} = (\mathfrak{l} \cap \mathfrak{g}_1) \oplus (\mathfrak{l} \cap \mathfrak{m}) = \mathfrak{t}_1 \oplus (\mathfrak{l} \cap \mathfrak{m}). \tag{15}$$

Taking S-fixed points on both sides of (15), we obtain

$$\mathfrak{l}^S = \mathfrak{t}_0 \oplus (\mathfrak{l}^S \cap \mathfrak{m}),$$

so that, by (12) we have

$$\dim \mathfrak{l}^S = \operatorname{rank} \mathfrak{g}_0 + \dim(\mathfrak{l}^S \cap \mathfrak{m}). \tag{16}$$

It is clear that $\mathfrak{l}^S \cap \mathfrak{m} \subset \mathfrak{m}^S$ and that we have $\mathfrak{l}^S \cap \mathfrak{m} = \mathfrak{m}^S$ if and only if $[\mathfrak{t}_0, \mathfrak{m}^S] = 0$. Thus we obtain the chain of inequalities:

$$\dim \mathfrak{l}^S \underset{(16)}{=} \operatorname{rank} \mathfrak{g}_0 + \dim(\mathfrak{l}^S \cap \mathfrak{m}) \leq \operatorname{rank} \mathfrak{g}_0 + \dim \mathfrak{m}^S \leq \operatorname{rank} \mathfrak{g}_0 + \mathsf{sw}(\varphi, \mathfrak{m}) = \mathsf{swr}(\varphi, \mathfrak{g}). \tag{17}$$

The lemma follows. □

Remark: The choice of $(\mathfrak{t}_1, \mathfrak{b}_1)$ is canonical, in the following sense. If $(\mathfrak{t}_1', \mathfrak{b}_1')$ is a different choice then there is an element $g \in C_G(P)^\circ$ such that $\operatorname{Ad}(g)\mathfrak{t}_1 = \mathfrak{t}_1'$ and $\operatorname{Ad}(g)\mathfrak{b}_1 = \mathfrak{b}_1'$. One checks that S and gSg^{-1} give the same group of automorphisms of $\mathfrak{t}_1'$.

4 Essentially tame representations

We retain the notation of section 3.

From now on we assume that our representation $\varphi : \mathcal{W} \to \operatorname{Aut}(\mathfrak{g})$ is essentially tame. Recall this means that the wild inertial image P is contained in a torus. This is equivalent to the condition

$$\operatorname{rank} \mathfrak{g}_1 = \operatorname{rank} \mathfrak{g}. \tag{18}$$

In the following situations φ is essentially tame:

- p does not divide the order of the Weyl group of G [2];
- p is not a torsion prime for G and P is abelian [23, 2.25(a)];
- p does not divide the order of the fundamental group of G and P is of type (p, p) [1, 3.12];
- P is cyclic and is contained in G.

As in section 3.1 we choose S-stable Cartan and Borel subalgebras $\mathfrak{t}_1 \subset \mathfrak{b}_1$ of $\mathfrak{g}_1$. Condition (18) means that $\mathfrak{t}_1$ is also a Cartan subalgebra of $\mathfrak{g}$, and that P is contained in the maximal torus $T_1 = C_G(\mathfrak{t}_1)$. We have

$$I \subset \mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1) := \{s \in \mathrm{Aut}(\mathfrak{g}) : \ s(\mathfrak{t}_1) = \mathfrak{t}_1\}.$$

Let R be the set of roots of T_1 in $\mathfrak{g}$. For each $\alpha \in R$ let $\mathfrak{g}_\alpha = \{y \in \mathfrak{g} : [x, y] = \langle \alpha, x\rangle y \ \forall x \in \mathfrak{t}_1\}$ be the corresponding root space. The two summands in (11) are stable under $\mathrm{ad}(\mathfrak{t}_1)$, giving a partition

$$R = R_1 \sqcup R^1, \tag{19}$$

where

$$\begin{aligned} R_1 &= \{\alpha \in R : \ \mathfrak{g}_\alpha \subset \mathfrak{g}_1\} = \{\alpha \in R : \ \alpha(P) = 1\}, \\ R^1 &= \{\alpha \in R : \ \mathfrak{g}_\alpha \subset \mathfrak{m}\} \ \ = \{\alpha \in R : \ \alpha(P) \neq 1\}. \end{aligned}$$

Since $\mathfrak{t}_1 = \mathfrak{l} \cap \mathfrak{g}_1$, no root in R_1 can vanish on all of $\mathfrak{t}_0$. Hence if $\mathfrak{g}_\alpha \subset \mathfrak{l}$, we must have $\alpha \in R^1$.

The group $\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1)$ naturally surjects onto the automorphism group $\mathrm{Aut}(R)$ of the root system R; the group P acts trivially on R and the image of S is a cyclic subgroup $S_R < \mathrm{Aut}(R)$, of order prime to p.

Let $\mathfrak{b}$ be a Borel subalgebra of $\mathfrak{g}$ such that $\mathfrak{b}_1 = \mathfrak{b} \cap \mathfrak{g}_1$, and let $\Delta \subset R$ be the set of simple roots of $\mathfrak{t}_1$ in $\mathfrak{b}$. This gives a splitting

$$\mathrm{Aut}(R) = W \rtimes \mathrm{Aut}(R, \Delta)$$

where $W = W(R)$ is the Weyl group of R and $\mathrm{Aut}(R, \Delta) = \{\vartheta \in \mathrm{Aut}(R) : \ \vartheta(\Delta) = \Delta\}$.

4.1 Automorphisms of root systems

We pause to review some general facts about automorphisms of root systems. See [17] for more details.

We say that a subgroup $C < \mathrm{Aut}(R)$ is *elliptic* if C fixes no nonzero vector in the root lattice $\mathbb{Z}R$, and that C is *$\mathbb{Z}$-regular* if C acts freely on R. We also say that an element $\sigma \in \mathrm{Aut}(R)$ is elliptic and/or $\mathbb{Z}$-regular if $\langle\sigma\rangle$ is so.

Fix a coset $W\vartheta$ of W in $\mathrm{Aut}(R)$ and let $(W\vartheta)_{\mathsf{ellreg}}$ be the set of elliptic $\mathbb{Z}$-regular elements of $W\vartheta$. It is known that $(W\vartheta)_{\mathsf{ellreg}}$ is nonempty. For each integer $m \geq 1$ let

$$(W\vartheta)^m_{\mathsf{ellreg}} = \{\sigma \in (W\vartheta)_{\mathsf{ellreg}} : \ |\sigma| = m\}.$$

If it is nonempty then $(W\vartheta)^m_{\mathsf{ellreg}}$ consists of a single W-orbit, under conjugation. The maximum such order is the *twisted Coxeter number* of $W\vartheta$:

$$h_\vartheta := \max\{m : (W\vartheta)^m_{\mathsf{ellreg}} \neq \varnothing\},$$

(cf. [20, sec. 6], [15, sec. 5]).

Let $\mathfrak{t}_1, T_1, R$ be as in the previous section. The action of $\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1)$ on R gives a surjective mapping $f : \mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1) \to \mathrm{Aut}(R)$. If $\sigma \in \mathrm{Aut}(R)$ is elliptic then the fiber $f^{-1}(\sigma)$ is a single T-conjugacy class in $\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1)$. If, in addition, σ is $\mathbb{Z}$-regular then the elements of $f^{-1}(\sigma)$ have the same order as σ [17, Prop. 8]. If $W\vartheta$ is a coset of W in $\mathrm{Aut}(R)$ and $\sigma \in (W\vartheta)^m_{\mathsf{ellreg}}$ then $m = h_\vartheta$ if and only if the fixed-point subalgebra $\mathfrak{g}^s$ is abelian, for any $s \in f^{-1}(\sigma)$.

4.2 Statement of the main result

Our representation $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$ has given rise to a cyclic subgroup $S_R < \mathrm{Aut}(R)$, depending on a choice of S-stable pair $(\mathfrak{t}_1, \mathfrak{b}_1)$ in $\mathfrak{g}_1$. From the remark at the end of section 3.1, it follows that the properties of S_R being elliptic and/or $\mathbb{Z}$-regular are independent of this choice.

Let $\mathfrak{l}$ be the Levi subalgebra defined in section 3.1. We note that

$$\mathfrak{l} = \mathfrak{g} \quad \Leftrightarrow \quad \mathfrak{g}_0 = 0 \quad \Leftrightarrow \quad \mathfrak{t}_0 = 0 \quad \Leftrightarrow \quad S_R \text{ is elliptic in } \mathrm{Aut}(R). \tag{20}$$

We can now state our main theorem in full generality.

Theorem 4.1. *Suppose $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g})$ is an essentially tame and wildly ramified representation. Then we have*

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq \dim \mathfrak{l}^S. \tag{21}$$

Equality holds if and only if the following conditions hold:

1. $\mathfrak{l} = \mathfrak{g}$;
2. $P_2 = 1$;
3. S_R *is both elliptic and $\mathbb{Z}$-regular.*

Remark/Example: When (21) is an equality we necessarily have $\mathfrak{l} = \mathfrak{g}$, by (20). However, we cannot replace $\mathfrak{l}$ by $\mathfrak{g}$ in the statement of Thm. 4.1 without the additional assumption that $\mathfrak{g}_0 = 0$ (the "totally ramified" condition). This is shown by the following example.

In the group G of type G_2 consider the copy of the symmetric group S_3 generated by s, t where $\mathfrak{g}^t \simeq \mathfrak{sl}_3$ and s is an involution such that $stst = 1$. Note that s normalizes $\mathfrak{g}^t$, acting there as the unique outer involution of $\mathfrak{sl}_3$ (up to SL_3-conjugacy), so that $\mathfrak{g}^{\langle s,t\rangle} \simeq \mathfrak{so}_3$. For any s-stable Cartan-Borel pair $\mathfrak{t}_1 \subset \mathfrak{b}_1$, the fixed-point space $\mathfrak{t}_1^s$ is a line, and $\mathfrak{t}_1^s$ is a Cartan subalgebra of $\mathfrak{g}^{\langle s,t\rangle}$.

Assume that $p = 3$. For each totally ramified Galois extension E/k with $\mathrm{Gal}(E/k) \simeq S_3$ we get a representation $\varphi : \mathcal{W} \to G$ whose image $\varphi(\mathcal{W}) = \langle s, t\rangle$ has ramification filtration

$$\varphi(\mathcal{W}) = I > P_1 = \cdots = P_c > 1$$

for some odd integer c, where $S = \langle s \rangle$ and $P_1 = \langle t \rangle$. Note that φ is essentially tame, since P_1 is cyclic. From the above discussion we have

$$\mathfrak{g}_1 = \mathfrak{g}^t = \mathfrak{sl}_3, \qquad \mathfrak{g}_0 = \mathfrak{g}^{\langle s,t \rangle} = \mathfrak{so}_3, \qquad \mathfrak{l} \simeq \mathfrak{gl}_2, \qquad \dim \mathfrak{l}^S = 2.$$

It follows that

$$\mathsf{swr}(\varphi, \mathfrak{g}) = 3c + \operatorname{rank} \mathfrak{so}_3 = 3c + 1 \in \{4,\ 10, 16,\ \dots\}.$$

Hence $\mathsf{swr}(\varphi, \mathfrak{g}) \gneq \dim \mathfrak{l}^S$, as promised by Thm. 4.1. Indeed, the automorphism $\sigma \in \operatorname{Aut}(R)$ induced by s acting on $\mathfrak{t}_1$ is a reflection, hence is not elliptic. In fact the difference $4 - 2$ is minimal, since it must be even, a priori.

For $k = \mathbb{Q}_3$ we find in [11] that there are two totally ramified S_3-extensions E/k with $c = 1$, generated by the roots of $x^6 + 3x^2 + 3$ and $x^6 + 6x^2 + 6$. Since $\mathfrak{g}^s = \mathfrak{so}_4$, we have $\mathsf{swr}(\varphi, \mathfrak{g}) = 4 < 6 = \dim \mathfrak{g}^s$. This shows that we cannot replace $\mathfrak{l}$ by $\mathfrak{g}$ in the inequality (21).

Corollary 4.2. *Suppose $\varphi : \mathcal{W} \to \operatorname{Aut}(\mathfrak{g})$ is essentially tame and wildly ramified. Then*

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq \operatorname{rank} \mathfrak{g}^S,$$

with equality if and only if S_R is generated by a twisted Coxeter automorphism and $P_2 = 1$.

We note that $\operatorname{rank} \mathfrak{g}^S$ depends only on the projection of S_R to $\operatorname{Aut}(R)/W(R)$: This projection is isomorphic to a cyclic subgroup $\langle \vartheta \rangle < \operatorname{Aut}(R, \Delta)$ and $\operatorname{rank} \mathfrak{g}^S$ is the number of $\langle \vartheta \rangle$-orbits in Δ.

Proof. Since $\mathfrak{l}^S$ is a Levi subalgebra of $\mathfrak{g}^S$ we have, using (21), that

$$\mathsf{swr}(\varphi, \mathfrak{g}) \geq \dim \mathfrak{l}^S \geq \operatorname{rank} \mathfrak{l}^S = \operatorname{rank} \mathfrak{g}^S. \tag{22}$$

Hence the inequality of Cor. 4.2 holds.

Assume that $\mathsf{swr}(\varphi, \mathfrak{g}) = \operatorname{rank} \mathfrak{g}^S$. Then we also have equality in (21), so $\mathfrak{l} = \mathfrak{g}$, $P_2 = 1$, and S_R is elliptic and $\mathbb{Z}$-regular. But also $\dim \mathfrak{g}^S = \operatorname{rank} \mathfrak{g}^S$ from (22), so $\mathfrak{g}^S$ is abelian. Hence S_R is a twisted Coxeter element (see section 4.1).

Conversely, if $P_2 = 1$ and S_R is a twisted Coxeter element then $\mathfrak{g}^S$ is abelian and also $\mathfrak{l} = \mathfrak{g}$ by (20). Hence by Thm. 4.1 we have $\mathsf{swr}(\varphi, \mathfrak{g}) = \dim \mathfrak{g}^S = \operatorname{rank} \mathfrak{g}^S$. □

4.3 Proof of the inequality (21)

By Lemma 3.1 it is enough to prove the simpler inequality

$$\dim \mathfrak{m}^S \leq \mathsf{sw}(\varphi, \mathfrak{m}). \tag{23}$$

For each $\alpha \in R$, the root space $\mathfrak{g}_\alpha$ is one-dimensional and from (19) we have

$$\mathfrak{m} = \sum_{\alpha \in R^1} \mathfrak{g}_\alpha,$$

where $R^1 = \{\alpha \in R : \ \alpha(P) \neq 1\}$. Note that S_R preserves R^1, since P is normal in I. Let R^1/S be the set of S_R-orbits on R^1 and for each orbit $\mathcal{O} \in R^1/S$ set

$$\mathfrak{g}_{\mathcal{O}} := \sum_{\alpha \in \mathcal{O}} \mathfrak{g}_\alpha$$

so that

$$\mathfrak{m} = \bigoplus_{\mathcal{O} \in R^1/S} \mathfrak{g}_{\mathcal{O}}$$

as I-modules.

Since P is nontrivial on $\mathfrak{g}_{\mathcal{O}}$, we have $\mathsf{sw}(\varphi, \mathfrak{g}_{\mathcal{O}}) \geq 1$ for each $\mathcal{O} \in R^1/S$. And since each $\dim \mathfrak{g}_\alpha = 1$ we have

$$\dim \mathfrak{g}_{\mathcal{O}}^S \leq 1. \tag{24}$$

Thus we have

$$\dim \mathfrak{g}_{\mathcal{O}}^S \leq 1 \leq \mathsf{sw}(\varphi, \mathfrak{g}_{\mathcal{O}}). \tag{25}$$

It follows that

$$\dim \mathfrak{m}^S = \sum_{\mathcal{O} \in R^1/S} \dim \mathfrak{g}_{\mathcal{O}}^S \leq \sum_{\mathcal{O} \in R^1/S} 1 \leq \sum_{\mathcal{O} \in R^1/S} \mathsf{sw}(\varphi, \mathfrak{g}_{\mathcal{O}}) = \mathsf{sw}(\varphi, \mathfrak{m}), \tag{26}$$

so the inequality in Thm. 4.1 is proved. We consider the case of equality in the next section.

4.4 Analysis of equality

It is easy to show that if S_R is elliptic and $\mathbb{Z}$-regular and $P_2 = 1$ then $\mathsf{swr}(\varphi, \mathfrak{g}) = \dim \mathfrak{l}^S$. Indeed, from the equivalences (20) we have that $\mathfrak{l}^S = \mathfrak{g}^S$ and $\mathfrak{g}_0 = 0$. It follows that $\mathfrak{g}_1 = \mathfrak{t}_1$, so that $R^1 = R$,

$$\mathfrak{m} = \sum_{\alpha \in R} \mathfrak{g}_\alpha = \sum_{\mathcal{O} \in R/S} \mathfrak{g}_{\mathcal{O}}$$

and $\mathfrak{g}^S = \mathfrak{m}^S$. Since $|S| = |S_R|$ we have $\dim \mathfrak{g}_{\mathcal{O}}^S = 1$ for each $\mathcal{O} \in R/S$, hence

$$\dim \mathfrak{m}^S = |R/S|.$$

The equality $|S| = |S_R|$ also implies that P is the full stabilizer in I of any root $\alpha \in R$, so that $\mathfrak{g}_{\mathcal{O}} = \mathrm{Ind}_P^I \mathfrak{g}_\alpha$, as I-modules, for any $\alpha \in \mathcal{O}$. Since $P_2 = 1$ we have $\mathsf{sw}(\varphi, \mathfrak{g}_{\mathcal{O}}) = 1$, using (9). It follows that $\mathsf{sw}(\varphi, \mathfrak{g}) = |R/S|$, so that $\mathsf{swr}(\varphi, \mathfrak{g}) = \mathsf{sw}(\varphi, \mathfrak{g}) = \dim \mathfrak{m}^S = \dim \mathfrak{g}^S = \dim \mathfrak{l}^S$, as claimed.

For the nontrivial direction, assume that $\mathsf{swr}(\varphi, \mathfrak{g}) = \dim \mathfrak{l}^S$. Since we have already verified the simpler inequality (14), we may invoke parts (a) and (b) of Lemma 3.1.

From part (a) of 3.1 we have $\dim \mathfrak{m}^S = \mathsf{sw}(\varphi, \mathfrak{m})$. Using (26), this implies that

$$\dim \mathfrak{g}_{\mathcal{O}}^S = 1 = \mathsf{sw}(\varphi, \mathfrak{g}_{\mathcal{O}})$$

for all $\mathcal{O} \in R^1/S$.

Now $I = \mathrm{Gal}(E/K)$ where E is a finite (and totally ramified) Galois extension of the maximal unramified extension K of k. Let $E_\alpha = E^{I_\alpha}$, where I_α is the stabilizer in I of a root $\alpha \in \mathcal{O}$. Since $I_\alpha \supset P$, the extension E_α/K is tamely ramified, so the induction formula (9) gives

$$1 = \mathsf{sw}(\varphi, \mathfrak{g}_{\mathcal{O}}) = \mathsf{sw}(\varphi_\alpha, \mathfrak{g}_\alpha), \tag{27}$$

where φ_α is the restriction of φ to $\mathcal{W}_{E_\alpha}$. It now follows from local class-field theory that $\alpha(P)^p = 1$. Since this holds for all $\alpha \in R$ we have

$$P \subset T_1[p], \tag{28}$$

where $T_1[p] = \{t \in T_1 : \ t^p = 1\}$.

Next, from part (b) of Lemma 3.1 we have $[\mathfrak{t}_0, \mathfrak{m}^S] = 0$. I claim that in fact $[\mathfrak{t}_0, \mathfrak{m}] = 0$. Recall that $R^1 = \{\alpha \in R : \ \mathfrak{g}_\alpha \subset \mathfrak{m}\}$. If $x \in \mathfrak{t}_0$ and $\mathcal{O} \in R^1/S$ then x acts on $\mathfrak{g}_{\mathcal{O}}$ by the scalar $\langle \alpha, x\rangle$ for any $\alpha \in \mathcal{O}$, since x is S-invariant. Hence x acts by $\langle \alpha, x\rangle$ on the one-dimensional space $\mathfrak{g}_{\mathcal{O}}^S$. But $[\mathfrak{t}_0, \mathfrak{g}_{\mathcal{O}}^S] \subset [\mathfrak{t}_0, \mathfrak{m}^S] = 0$, so $\langle \alpha, x\rangle = 0$, and we have $[x, \mathfrak{g}_{\mathcal{O}}] = 0$. Hence $[\mathfrak{t}_0, \mathfrak{m}] = 0$, as claimed.

Since $\mathfrak{l}$ is the centralizer of $\mathfrak{t}_0$ in $\mathfrak{g}$, this means that $\mathfrak{m} \subset \mathfrak{l}$. From (15) it follows that

$$\mathfrak{l} = \mathfrak{t}_1 \oplus \mathfrak{m}. \tag{29}$$

In terms of roots, this means that

$$R_1 = \{\alpha \in R : \ \langle \alpha, \mathfrak{t}_0\rangle \neq 0\} \quad \text{and} \quad R^1 = \{\alpha \in R : \ \langle \alpha, \mathfrak{t}_0\rangle = 0\}. \tag{30}$$

Recall that

$$\mathfrak{m} = \sum_{\alpha \in R^1} \mathfrak{g}_\alpha,$$

and set

$$\mathfrak{n} = \sum_{\alpha \in R_1} \mathfrak{g}_\alpha.$$

Equations (30) imply that $[\mathfrak{m}, \mathfrak{n}] \subset \mathfrak{n} \subset \mathfrak{g}_1$. But from the original definitions of R_1 and R^1 after (19) we have

$$R_1 = \{\alpha \in R : \ \alpha(P) = 1\} \quad \text{and} \quad R^1 = \{\alpha \in R : \ \alpha(P) \neq 1\} \tag{31}$$

and equations (31) imply that $[\mathfrak{m}, \mathfrak{n}] \subset \mathfrak{m}$. Since $\mathfrak{g}_1 \cap \mathfrak{m} = 0$, this shows that

$$[\mathfrak{m}, \mathfrak{n}] = 0.$$

The derived subalgebra $\mathfrak{h} = [\mathfrak{l}, \mathfrak{l}]$ is generated by the nontrivial root spaces in $\mathfrak{l}$, which is to say, by $\mathfrak{m}$ (see (29)). It follows that $\mathfrak{h}$ is an ideal in the simple Lie algebra $\mathfrak{g}$. If $\mathfrak{h} = 0$ then $\mathfrak{l} = \mathfrak{t}_1$, so $\mathfrak{m} = 0$. This means $P = 1$, contrary to our assumption that φ is wildly ramified. Therefore $\mathfrak{h} = \mathfrak{g}$, so $\mathfrak{l} = \mathfrak{g}$ and $\mathfrak{t}_0 = 0$, so $\mathfrak{g}_0 = 0$.

We have now proved Assertion 1 of Thm. 4.1. Note also that the vanishing of $\mathfrak{g}_0$ implies that $\mathfrak{g}_1$ is abelian, so in fact $\mathfrak{g}_1 = \mathfrak{t}_1$ is a Cartan subalgebra of $\mathfrak{g}$. We have $R_1 = \varnothing$, $R^1 = R$ and S_R is elliptic.

We turn now to the ramification filtration $P = P_1 \geq P_2 \geq \cdots$. Define integers a and c_α (for $\alpha \in R$) as follows:

$$a = \max\{j \in \mathbb{Z}_{\geq 1} : P = P_j\}, \qquad c_\alpha = \max\{j \in \mathbb{Z}_{\geq 1} : \ \alpha(P_j) \neq 1\}.$$

The equation $\mathsf{sw}(\varphi_\alpha, \mathfrak{g}_\alpha) = 1$ (see (27)) can be written as

$$[I_\alpha : P] = \sum_{j=1}^{c_\alpha} \frac{1}{[P : P_j]}. \tag{32}$$

Since clearly $P_{c_\alpha} \neq P_{1+c_\alpha}$, we have $c_\alpha \geq a$, so

$$[I_\alpha : P] = \sum_{j=1}^{c_\alpha} \frac{1}{[P : P_j]} \geq \sum_{j=1}^{a} \frac{1}{[P : P_j]} = a \geq 1. \tag{33}$$

Lemma 4.3. *The cyclic group S_R is $\mathbb{Z}$-regular if and only if $P_2 = 1$.*

Proof. If $P_2 = 1$ then for all α we have $c_\alpha = 1$, hence $I_\alpha = P \subset T_1$, so S_R is $\mathbb{Z}$-regular. Conversely, if S_R is $\mathbb{Z}$-regular, then $|S| = |S_R|$. This implies that $[I_\alpha : P] = 1$ for all α. Hence $c_\alpha = 1$, so $\alpha(P_2) = 1$ for all α, so $P_2 = 1$. $\square$

It remains only to prove that S_R is $\mathbb{Z}$-regular. Let

$$R^\circ = \{\alpha \in R : \ |S_R \cdot \alpha| = |S_R|\} \tag{34}$$

be the set of roots in R whose stabilizer in S_R is trivial, and let

$$Z = \{t \in T_1 : \ \alpha(t) = 1 \ \forall \alpha \in R^\circ\}. \tag{35}$$

It is easy to check that if $I_\alpha = P$ then $\alpha \in R^\circ$. (The converse need not be true, if S_R is not $\mathbb{Z}$-regular.)

Let $\mathbb{Z}R^\circ$ be the subgroup of the root lattice $\mathbb{Z}R$ generated by R°. Say that S_R is *almost regular* if $[\mathbb{Z}R : \mathbb{Z}R^\circ]$ is finite and every prime dividing $[\mathbb{Z}R : \mathbb{Z}R^\circ]$ also divides $|S_R|$. This excludes the residue characteristic p from dividing $[\mathbb{Z}R : \mathbb{Z}R^\circ]$. Since $\mathbb{Z}R/\mathbb{Z}R^\circ$ surjects onto $\mathrm{Hom}(Z, \mathbb{C}^\times)$, it follows that Z has no elements of order p when S_R is almost regular.

Lemma 4.4. *If S_R is almost regular then S_R is $\mathbb{Z}$-regular (so in fact $R^\circ = R$).*

Proof. The proof will rely on equation (32), which has been established for every root $\alpha \in R$.

We first show that $|S| = |S_R|$. Set

$$\ell = |S|, \qquad m = |S_R|.$$

A lift of S_R to a Tits subgroup of $\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1)$ (corresponding to a choice of pinning in $\mathfrak{g}$, see [25]) has order equal to m or to $2m$. Since S_R is elliptic, all of its lifts to $\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}_1)$ have the same order and are in fact T_1-conjugate. Since S is one such lift, we have that $\ell \in \{m, 2m\}$.

We assume that $\ell = 2m$ and find a contradiction as follows. Let $S_R = \langle \sigma \rangle$ and let $s \in S$ be a lift of σ. We have $s^m = t$, where t is the unique element of order two in S and $S \cap T_1 = \langle t \rangle$, since $|\sigma| = m$. Clearly $t \in I_\alpha$ for every $\alpha \in R$, and the group $\langle t \rangle \cdot P_1 \subset T_1$ is abelian.

Let K be an algebraic closure of the residue field of k, and let $\mu_\ell(\mathsf{K}) = \{z \in \mathsf{K}^\times : \ z^\ell = 1\}$. There is a canonical embedding $I/P \hookrightarrow \mathsf{K}^\times$ [19, IV.2 Prop. 9] whose image is $\mu_\ell(\mathsf{K})$, giving an isomorphism

$$\theta : S \xrightarrow{\sim} \mu_\ell(\mathsf{K}). \tag{36}$$

Set $\zeta = \theta(s)$. For each $j \geq 1$ we also have embeddings $\theta_j : P_j/P_{j+1} \hookrightarrow \mathsf{K}^+$, such that

$$\theta_j(sxs^{-1}) = \zeta^j \theta_j(x), \qquad \text{for all } x \in P_j. \tag{37}$$

Under the embedding (36), we have $\theta(t) = -1$. The assumption $\ell = 2m$ forces $p \neq 2$, so $-1 \neq 1$ in K. Since t centralizes P_1, it follows from (37) that all jumps in the lower filtration numbering are even. In particular we have $P_1 = P_2$. From (32) we have, for all $\alpha \in R$,

$$[I_\alpha : P] = \sum_{j=1}^{c_\alpha} \frac{1}{[P : P_j]} \begin{cases} = 1 & \text{if} \quad c_\alpha = 1 \\ = 2 & \text{if} \quad c_\alpha = 2 \\ > 2 & \text{if} \quad c_\alpha > 2. \end{cases}$$

Take any $\alpha \in R^\circ$ and let s^k generate the stabilizer of α in S. Then $\sigma^k = 1$, since $\alpha \in R^\circ$. It follows that $s^k \in S \cap T_1$, so $s^k = 1$ or t. In either case we have $[I_\alpha : P] \leq 2$, so $c_\alpha \leq 2$. This shows that $\alpha(P_3) = 1$ for all $\alpha \in R^\circ$, so $P_3 \subset Z$. But S_R is almost regular, so p does not divide $|Z|$. Hence $P_3 = 1$. This means $c_\beta \leq 2$ for *any* root $\beta \in R$, so that $[I_\beta : P] \leq 2$.

Now $\mathbb{Z}$-regular elliptic elements of $\mathrm{Aut}(R)$ lift to elements of the same order, so σ cannot be $\mathbb{Z}$-regular, by our assumption that $\ell = 2m$. Hence there exists a root β fixed by some power $\sigma^i \neq 1$. But since $[I_\beta : P] \leq 2$, it follows that s^i is an involution in S, so we must have $s^i = t$, forcing $\sigma^i = 1$; this is the desired contradiction.

Therefore $|S| = |S_R|$. This implies that the stabilizers of a root β in S and S_R are isomorphic. Hence for every $\alpha \in R^\circ$ we have $[I_\alpha : P] = 1$, so that $c_\alpha = 1$, meaning that $P_2 \subset \ker \alpha$. Since this holds for all $\alpha \in R^\circ$, we have $P_2 \subset Z$. Again using the assumption that S_R is almost regular, we must have $P_2 = 1$. From Lemma 4.3 it follows that S_R is $\mathbb{Z}$-regular. □

To complete the analysis of equality in Thm. 4.1 it now suffices to show that S_R is almost regular.

We regard $T_1[p]$ as a vector space over $\mathbb{F}_p$, on which S_R acts by semisimple linear transformations, preserving the subspace $P \subset T_1[p]$ (see (28)). Let $\mathrm{spec}(\sigma) \subset \overline{\mathbb{F}}_p^\times$ be the set of eigenvalues of σ in $T_1[p]$. If P_i/P_{i+1} is nonzero for some i, then $\zeta^i \in \mathrm{spec}(\sigma)$.

We define integers m_1 and b as follows.

$$\begin{aligned} m_1 &= \max\{\text{order of an element in } \mathrm{spec}(\sigma)\}, \\ b &= \min\{i \in \mathbb{Z}_{\geq 1} : \ \zeta^i \in \mathrm{spec}(\sigma)\}. \end{aligned} \tag{38}$$

Recall that a is the largest integer j such that $P_j = P$. Since σ acts via ζ^a on P_a/P_{a+1} and this quotient is nontrivial by the choice of a, we have that $b \leq a$.

Lemma 4.5. *Assume that* (32) *holds for some* $\alpha \in R$ *and let* $\mathcal{O}$ *be the* S_R*-orbit of* α*. Then* $|\mathcal{O}| \leq m_1$ *and equality implies* $c_\alpha = a$*.*

Proof. The characteristic polynomial of σ on $T_1[p]$ is the reduction modulo p of the characteristic polynomial $\det(t - \sigma)$ of σ on the co-weight lattice $\check{X}$ of T_1. the latter is a product of cyclotomic polynomials:

$$\det(t - \sigma) = \Phi_{m_1}(t) \cdots \Phi_{m_r}(t),$$

where $m_1 \geq m_2 \geq \cdots \geq m_r$ are the orders of the eigenvalues in $\overline{\mathbb{Q}}$ of σ on $\check{X}$. Reducing these polynomials modulo p gives the characteristic polynomial of σ on $T_1[p]$, where the eigenvalues of σ, now in $\overline{\mathbb{F}}_p$, have the same orders m_i. We also note that if $\eta \in \operatorname{spec}(\sigma)$ and d is an integer relatively prime to $|\eta|$ then $\eta^d \in \operatorname{spec}(\sigma)$.

I claim that in fact $b = m/m_1$, where we recall that $m = |\sigma|$. Since $m_i \mid m$ for every i, and each power ζ^{m/m_i} is a root of Φ_{m_i}, we have that $\zeta^{m/m_i} \in \operatorname{spec}(\sigma)$. From the definition of b we have $b \leq m/m_1$.

On the other hand,

$$|\zeta^b| = \frac{m}{(b, m)}.$$

Let d, e be integers such that $(b, m) = bd + me$. Then $(d, |\zeta^b|) = 1$ so $\zeta^{bd} \in \operatorname{spec}(\sigma)$. But $\zeta^{bd} = \zeta^{(b,m)}$, so $(b, m) = b$, by minimality of b. Hence $b \mid m$ and $m/b = |\zeta^b| \leq m_1$, so $m/m_1 \leq b$. Hence $b = m/m_1$, as claimed.

Assume now that (32) holds for $\alpha \in R$ with S_R-orbit $\mathcal{O}$. The stabilizer of α in I has the form $I_\alpha = \langle s_\alpha \rangle \ltimes P$, for some $s_\alpha \in S$. From (33) we have

$$|s_\alpha| = [I_\alpha : P] = \sum_{j=1}^{c_\alpha} \frac{1}{[P : P_j]} \geq a \geq b.$$

It follows that

$$|\mathcal{O}| = \frac{m}{|s_\alpha|} \leq \frac{m}{b} = m_1,$$

and equality implies $c_\alpha = a$. ∎

The rest of the proof of 4.1 takes place purely in the setting of root systems. We treat the classical and exceptional root systems separately.

4.5 Classical Root Systems

In this section R is one of the classical irreducible root systems $A_{n-1},\ B_n,\ C_n, D_n$. We assume $\sigma \in \operatorname{Aut}(R)$ is elliptic and that (32) holds for every $\alpha \in R$, and we will show that σ is almost regular. By Lemma 4.4 this will complete the proof of Thm. 4.1 for classical Lie algebras.

Let ϑ be the projection of σ to $\operatorname{Aut}(R, \Delta)$, where Δ is a base of R.

We can ignore the case $R = A_{n-1}$ with $\vartheta = 1$, since all elliptic elements in $W(A_{n-1})$ are Coxeter elements, which are $\mathbb{Z}$-regular. Likewise when $R = D_4$ there is only one elliptic nonregular automorphism, namely $\sigma = -\vartheta$ where $\vartheta \in \mathrm{Aut}(R,\Delta)$ has order three. In this case it is easy to check that $\mathbb{Z}R^\circ = \mathbb{Z}R$.

In all other classical cases the elliptic automorphisms of R may be described uniformly: via the evident containments of root systems $A_{n-1} \subset D_n \subset B_n$, each automorphism $\sigma \in \mathrm{Aut}(R)$ (with the above exclusions) is the restriction of an automorphism of B_n.

Let $[1,n] = \{1,2,\dots,n\}$, and let $\{e_j : j \in [1,n]\}$ be the standard basis of $\mathbb{R}^n$. For each subset $J \subset [1,n]$, let W_J be the group of permutations and sign changes of $\{\pm e_j : j \in J\}$. Then W_J is a Weyl group of type $B_{|J|}$. In particular, $W_{[1,n]} \simeq W(B_n)$.

If $\sigma \in \mathrm{Aut}(R)$ is elliptic (with the above exclusions), there is a set partition $[1,n] = J_1 \sqcup \cdots \sqcup J_r$ such that

$$\sigma = \sigma_1 \cdots \sigma_r,$$

and each σ_p is a Coxeter element in $W(B_{n_p})$, where $n_p = |J_p|$. (For A_{n-1} with $|\vartheta| = 2$ all n_p are odd and each σ_p is an n_p-cycle multiplied by -1.) Then

$$|\sigma| = 2\,\mathrm{lcm}(n_1,\dots,n_r).$$

We order the J_p's so that $n_1 \geq n_2 \geq \cdots \geq n_r$ and consider the $\langle\sigma\rangle$-orbit of a root $\alpha = e_i \pm e_j$, where $i \in J_1$ and $j \in J_q$, with $2 \leq q \leq r$. Since each σ_p is $\mathbb{Z}$-regular in W_{J_p}, a power $\sigma^k = \sigma_1^k \cdots \sigma_r^k$ fixes α iff $\sigma_1^k = \sigma_q^k = 1$, iff both $2n_1, 2n_q$ divide k. So the stabilizer in $\langle\sigma\rangle$ of α is generated by

$$\sigma_\alpha := \sigma^{2\,\mathrm{lcm}(n_1,n_q)}$$

and the orbit $\mathcal{O} = \langle\sigma\rangle \cdot \alpha$ has cardinality

$$|\mathcal{O}| = 2\,\mathrm{lcm}(n_1,n_q) = \frac{2n_1 n_q}{(n_1,n_q)}.$$

The characteristic polynomial $\det(t-\sigma)$ of σ on $\check{X}$ is given by

$$\det(t-\sigma) = \prod_{p=1}^{r}(t^{n_p}+1)$$

(or this divided by $(t+1)$ in case $A_{n-1},\ \vartheta \neq 1$), so the largest order of a σ-eigenvalue is $2n_1$. By Lemma 4.5 we have

$$\frac{2n_1 n_q}{(n_1,n_q)} \leq 2n_1$$

which means $n_q \mid n_1$. This implies $|\mathcal{O}| = 2n_1$, and since this holds for all $2 \leq q \leq r$ we also have $|\sigma| = 2n_1$. Hence $\sigma_\alpha = 1$.

We have shown that R° contains all roots of the form $\alpha = e_i \pm e_j$ with $i \in J_1$ and $j \in J_q$, where $2 \leq q \leq r$. One checks that the span of these roots has index a power of two in $\mathbb{Z}R$. Since $|\sigma|$ is even, this means σ is almost regular, as claimed. □

Example: The proof above uses Lemma 4.5, which in turn uses equation (32). This is necessary: Let $G = \mathrm{SO}_{21}$, and let σ have partition $(n_1,n_2,n_3) = (5,3,2)$, so σ is elliptic of order $m = 60$. In this case, the set R° is empty, so σ is far from being almost regular.

4.6 Exceptional Root Systems

Let R be a simple (reduced) root system of exceptional type. In contrast to the classical cases, it turns out that every elliptic $\sigma \in \mathrm{Aut}(R)$ is almost regular. In fact, we always have $\mathbb{Z}R^\circ = \mathbb{Z}R$, for any elliptic $\sigma \in \mathrm{Aut}(R)$.

This is a case-by-case calculation; the results are presented in the tables below.

The first column gives the elliptic conjugacy classes of $\sigma \in \mathrm{Aut}(R)$ which are not $\mathbb{Z}$-regular. When a class is given two names, for example $E_8(a_4) = -A_8$, the left-hand name is that of [6], and the right-hand name is something more explicit: in this case -1 times a Coxeter element of type A_8.

The next columns contain the order $|\sigma|$ and the characteristic polynomial $\det(t - \sigma)$ on $\check{X}$, written as a product of cyclotomic polynomials. Next is a representative of the class written as a product of reflections (and possibly -1) according to the labelling of the extended diagram. The rightmost column gives a set of roots in R° which span $\mathbb{Z}R$.

Each segment of rows bounded by horizontal lines consists of powers of the elements in the top row of the segment. For our purposes, we need only consider the element in this top row.

Elliptic non-$\mathbb{Z}$-regular conjugacy classes in $W(F_4)$

$0 — 1 — 2 \Rightarrow 3 — 4$

Class of σ	m	$\det(t-\sigma)$	σ	$\alpha \in R^\circ$ spanning $\mathbb{Z}R$
D_4	6	$\Phi_2^2\Phi_6$	$r_0r_1r_2r_3r_2r_3$	$\Delta - \{\alpha_3\},\ \alpha_3+\alpha_4$
A_1C_3	6	$\Phi_2^2\Phi_6$	$r_0r_2r_3r_4$	Δ
A_3A_1	4	$\Phi_2^2\Phi_4$	$r_0r_1r_2r_4$	$\Delta - \{\alpha_4\},\ \alpha_3+\alpha_4$

Elliptic non-$\mathbb{Z}$-regular conjugacy classes in $\mathrm{Aut}(E_6)$

1 2 3 4 5
6
0

Class of σ	m	$\det(t-\sigma)$	σ	$\alpha \in R^\circ$ spanning $\mathbb{Z}R$
A_1A_5	6	$\Phi_6\Phi_3\Phi_2^2$	$r_0r_1r_2r_3r_4r_5$	Δ
$-A_4$	10	$\Phi_{10}\Phi_2^2$	$-r_1r_2r_3r_4$	Δ
$-E_6(a_2) = -(E_6^2)$	6	$\Phi_6\Phi_3^2$	$-(r_1r_2r_3r_4r_5r_6)^2$	$\Delta - \{\alpha_6\},\ \alpha_3+\alpha_6$
$-(2A_2)$	6	$\Phi_6^2\Phi_2^2$	$-r_1r_2r_4r_5$	$\Delta - \{\alpha_6\},\ \alpha_3+\alpha_6$
$-A_2$	6	$\Phi_6\Phi_2^4$	$-r_3r_6$	$\Delta - \{\alpha_1,\alpha_5\},\ \alpha_1+\alpha_2,\ \alpha_4+\alpha_5$

Elliptic non-$\mathbb{Z}$-regular conjugacy classes in $\mathrm{Aut}(E_7)$

0 1 2 3 4 5 6
7

Class of σ	m	$\det(t-\sigma)$	σ	$\alpha \in R^\circ$ spanning $\mathbb{Z}R$
$E_7(a_3) = -A_2A_4$	30	$\Phi_{10}\Phi_6\Phi_2$	$-r_0r_1r_2r_3r_5r_6$	$\alpha_4,\ \alpha_3+\alpha_4,\ \alpha_4+\alpha_5$
$A_1D_6 = (-A_2A_4)^3$	10	$\Phi_{10}\Phi_2^3$		$\alpha_3+\alpha_4+\alpha_7,\ \alpha_4+\alpha_5+\alpha_6$
$3A_1D_4 = (-A_2A_4)^5$	6	$\Phi_6\Phi_2^5$		$\alpha_2+\alpha_3+\alpha_4,\ \alpha_1+\alpha_2+\alpha_3+\alpha_4$
$E_7(a_2) = -E_6$	12	$\Phi_{12}\Phi_6\Phi_2$	$-r_1r_2r_3r_4r_5r_7$	Δ
$2A_3\ A_1 = (-E_6)^3$	4	$\Phi_4^2\Phi_2^3$		
A_7	8	$\Phi_8\Phi_4\Phi_2$	$r_0r_1r_2r_3r_4r_5r_6$	Δ
A_5A_2	6	$\Phi_6\Phi_3^2\Phi_2$	$r_0r_1r_2r_3r_7r_5r_6$	$\Delta - \{\alpha_5,\alpha_6\},\ \alpha_4+\alpha_5,\ \alpha_4+\alpha_5+\alpha_6$
$A_1D_6(a_2) = -2A_2$	6	$\Phi_6^2\Phi_2^3$	$-r_1r_2r_5r_6$	$\Delta - \{\alpha_7\},\ \alpha_3+\alpha_7$

Elliptic non-$\mathbb{Z}$-regular conjugacy classes in $\mathrm{Aut}(E_8)$

0 1 2 3 4 5 6 7
8

Class of σ	m	$\det(t-\sigma)$	σ	$\alpha \in R^\circ$ spanning $\mathbb{Z}R$
D_8	14	$\Phi_{14}\Phi_2^2$	$r_0r_1r_2r_3r_4r_5r_6r_8$	Δ
$D_8(a_1)$	12	$\Phi_{12}\Phi_4^2$	$r_0r_1r_2r_3r_4r_5r_4r_6r_5r_8$	Δ
$2D_4 = D_8(a_1)^2$	6	$\Phi_6^2\Phi_2^4$		
$D_8(a_2) = -A_4A_2$	30	$\Phi_{10}\Phi_6\Phi_2^2$	$-r_1r_2r_3r_4r_6r_7$	$\alpha_5,\ \alpha_5+\alpha_6,\ \alpha_4+\alpha_5,\ \alpha_5+\alpha_8$
$2A_1D_6 = D_8(a_2)^3$	10	$\Phi_{10}\Phi_2^4$		$\alpha_3+\alpha_4+\alpha_5,\ \alpha_5+\alpha_6+\alpha_7$
$4A_1D_4 = D_8(a_2)^5$	6	$\Phi_6\Phi_2^6$		$\alpha_2+\alpha_3+\alpha_4+\alpha_5,\ \alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5$
$E_8(a_4) = -A_8$	18	$\Phi_{18}\Phi_6$	$-r_0r_1r_2r_3r_4r_5r_6r_7$	Δ
$A_8 = (-A_8)^2$	9	$\Phi_9\Phi_3$		
A_1E_7	18	$\Phi_{18}\Phi_2^2$	$r_0r_2r_3r_4r_5r_6r_7r_8$	Δ
$A_1E_7(a_4) = (A_1E_7)^3$	6	$\Phi_6^3\Phi_2^2$		
$A_1E_7(a_2) = -E_6$	12	$\Phi_{12}\Phi_6\Phi_2^2$	$-r_3r_4r_5r_6r_7r_8$	$\Delta - \{\alpha_1\},\ \alpha_1+\alpha_2$
$2A_3\ 2A_1 = (-E_6)^3$	4	$\Phi_4^2\Phi_2^4$		
A_2E_6	12	$\Phi_{12}\Phi_3^2$	$r_0r_1r_3r_4r_5r_6r_7r_8$	$\Delta - \{\alpha_1\},\ \alpha_1+\alpha_2$
$A_2E_6(a_2) = (A_2E_6)^2$	6	$\Phi_6^2\Phi_3^2$		
$E_8(a_7) = -A_2E_6$	12	$\Phi_{12}\Phi_6^2$	$-r_0r_1r_3r_4r_5r_6r_7r_8$	$\Delta - \{\alpha_1\},\ \alpha_1+\alpha_2$
$A_3D_5(a_1)$	12	$\Phi_6\Phi_4^2\Phi_2^2$	$r_0r_1r_2r_6r_5r_4r_6r_5r_7r_8$	$\alpha_3,\ \alpha_4,\ \alpha_5,\ \alpha_6,\ \alpha_8,$
				$\alpha_2+\alpha_3,\ \alpha_1+\alpha_2+\alpha_3,\ \alpha_6+\alpha_7$
A_7A_1	8	$\Phi_8\Phi_4\Phi_2^2$	$r_0r_1r_2r_3r_4r_5r_8r_7$	$\Delta - \{\alpha_7\},\ \alpha_6+\alpha_7$
$A_5A_2A_1$	6	$\Phi_6\Phi_3^2\Phi_2^2$	$r_0r_1r_2r_3r_4r_6r_7r_8$	$\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4,\ \alpha_5,$
				$\alpha_5+\alpha_6,\ \alpha_5+\alpha_6+\alpha_7,\ \alpha_5+\alpha_8$

5 Existence of parameters satisfying equality

As always, $\mathfrak{g}$ is a simple complex Lie algebra. Choose any Cartan subalgebra $\mathfrak{t} \subset \mathfrak{g}$ and let $\mathrm{Aut}(\mathfrak{g},\mathfrak{t}) = \{g \in \mathrm{Aut}(\mathfrak{g}) :\ g\cdot\mathfrak{t} = \mathfrak{t}\}$, and let R be the set of roots of $\mathfrak{t}$ in $\mathfrak{g}$. Let $\check{X} = \mathrm{Hom}(\mathbb{Z}R,\mathbb{Z})$ be the $\mathbb{Z}$-module of one-parameter algebraic subgroups of the maximal torus $T = C_G(\mathfrak{t})$.

We assume that the residue characteristic p does not divide the order of the Weyl group of R. This implies that in fact p does not divide $|\mathrm{Aut}(R)|$.

Let $\sigma \in \mathrm{Aut}(R)$ be elliptic and $\mathbb{Z}$-regular, and let $|\sigma| = m$. The aim of this section is to show there exists an essentially tame representation $\varphi : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g},\mathfrak{t})$ with inertial image $I = SP$ as in section 3, such that $S_R = \langle\sigma\rangle$, and for which equality holds in Thm. 4.1, meaning that $P_2 = 1$ and

$$\mathsf{swr}(\varphi, \mathfrak{g}) = \mathsf{sw}(\varphi, \mathfrak{g}) = \dim \mathfrak{g}^S.$$

Let k be the residue field of k, say $|\mathsf{k}| = q$, a power of the prime p. Let K be an algebraic closure of k. Then k is the fixed-field of the Frobenius automorphism $\mathrm{F} : x \mapsto x^q$ on K.

Lemma 5.1. *If $\sigma \in \mathrm{Aut}(R)$ is elliptic and $\mathbb{Z}$-regular then σ is conjugate to σ^q in $\mathrm{Aut}(R)$.*

Proof. Recall from section 4.1 that in each coset of $W(R)$ in $\mathrm{Aut}(R)$ there is at most one elliptic $\mathbb{Z}$-regular $W(R)$-orbit (under conjugation) whose elements have the given order $m = |\sigma|$. Hence σ^q is conjugate to σ under $W(R)$ exactly when σ and σ^q have the same image in $\mathrm{Aut}(R)/W(R)$. This last condition fails to hold in just one case: R has type D_4, σ has order three in $\mathrm{Aut}(R)/W(R)$, and $q \equiv 2 \mod 3$. But here $\mathrm{Aut}(R)/W(R)$ is the symmetric group S_3, in which the two elements of order three are conjugate. It follows that σ is conjugate to σ^q in $\mathrm{Aut}(R)$, as claimed. □

Let $\tau \in \mathrm{Aut}(R)$ be any element such that $\tau\sigma\tau^{-1} = \sigma^q$.

Each root $\alpha \in R$ extends a linear functional on the K-vector space

$$\mathsf{V} := \mathsf{K} \otimes_{\mathbb{Z}} \check{X}.$$

Likewise the action of $\mathrm{Aut}(R)$ on $\check{X}$ extends K-linearly to V. Thus we have a decomposition

$$\mathsf{V} = \bigoplus_{\zeta \in \mu_m(\mathsf{K})} \mathsf{V}(\sigma, \zeta),$$

into eigenspaces $\mathsf{V}(\sigma, \zeta) := \{v \in \mathsf{V} :\ \sigma \cdot v = \zeta v\}$, for eigenvalues $\zeta \in \mu_m(\mathsf{K}) = \{z \in \mathsf{K}^\times :\ z^m = 1\}$.

The twisted Frobenius operator $\mathrm{F}_\tau := \mathrm{F} \otimes \tau$ on $\mathsf{K} \otimes \check{X} = \mathsf{V}$ preserves each eigenspace $\mathsf{V}(\sigma, \zeta)$. To check this, we first note that $\tau^{-1}\sigma\tau = \sigma^r$, where $rq \equiv 1 \mod m$, so that

$$\sigma \circ \mathrm{F}_\tau = \mathrm{F}_\tau \circ \sigma^r.$$

Next, for all $v \in \mathsf{V}$ we have $\mathrm{F}_\tau(\zeta v) = \zeta^q\, \mathrm{F}_\tau(v)$. It now follows that for $v \in \mathsf{V}(\sigma, \zeta)$ we have

$$\sigma\, \mathrm{F}_\tau(v) = \mathrm{F}_\tau(\sigma^r v) = \mathrm{F}_\tau(\zeta^r v) = \zeta^{rq}\, \mathrm{F}_\tau(v) = \zeta\, \mathrm{F}_\tau(v),$$

so $\mathrm{F}_\tau(v) \in \mathsf{V}(\sigma, \zeta)$ as claimed.

We define

$$\mathsf{V}(\sigma, \zeta)_{\mathsf{reg}} = \{v \in \mathsf{V}(\sigma, \zeta) :\ \langle \alpha, v\rangle \neq 0\ \ \forall \alpha \in R\}.$$

From [17, Prop.1] there exists and we choose $\zeta \in \mu_m(\mathsf{K})$ of order m such that $\mathsf{V}(\sigma, \zeta)_{\mathsf{reg}}$ is nonempty. Since F_τ permutes R (via τ), the space $\mathsf{V}(\sigma, \zeta)_{\mathsf{reg}}$ is preserved by F_τ. Define

$$\mathsf{V}(\sigma, \zeta)_{\mathsf{reg}}^{\mathrm{F}_\tau} = \{v \in \mathsf{V}(\sigma, \zeta)_{\mathsf{reg}} :\ \mathrm{F}_\tau(v) = v\}.$$

In [18, section 7] it is shown how each $v \in \mathsf{V}(\sigma, \zeta)_{\mathsf{reg}}^{\mathrm{F}_\tau}$ gives rise to a totally ramified representation $\varphi_v : \mathcal{W} \to \mathrm{Aut}(\mathfrak{g}, \mathfrak{t})$ with $S_R = \langle\sigma\rangle$ and such that

$$\mathsf{sw}(\varphi_v, \mathfrak{g}) = \dim \mathfrak{g}^S$$

as in Thm. 4.1. The existence of such parameters φ_v is thus a consequence of the following.

Proposition 5.2. *There exists* ζ *as above for which the space* $\mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau}_{\mathsf{reg}}$ *is nonempty.*

Proof. Let h be the order of q in $(\mathbb{Z}/m)^\times$. The sum

$$\widetilde{\mathsf{V}} := \mathsf{V}(\sigma,\zeta) + \mathsf{V}(\sigma,\zeta^q) + \mathsf{V}(\sigma,\zeta^{q^2}) + \cdots + \mathsf{V}(\sigma,\zeta^{q^{h-1}})$$

is stable under the commuting actions of F and τ. The action of τ therefore commutes with F_τ and induces isomorphisms

$$\mathsf{V}(\sigma,\zeta^{q^i}) \xrightarrow{\sim} \mathsf{V}(\sigma,\zeta^{q^{i-1}}), \qquad \mathsf{V}(\sigma,\zeta^{q^i})^{\mathrm{F}_\tau} \xrightarrow{\sim} \mathsf{V}(\sigma,\zeta^{q^{i-1}})^{\mathrm{F}_\tau},$$

for $i = 0, 1, \ldots, h-1$.

By Hilbert's Theorem 90 there exists $g \in \mathrm{GL}(\widetilde{\mathsf{V}})$ such that $\tau = g^{-1}\,\mathrm{F}(g)$. The action of g on $\widetilde{\mathsf{V}}$ intertwines F and F_τ, and therefore restricts to a k-isomorphism $\widetilde{\mathsf{V}}^{\mathrm{F}} \xrightarrow{\sim} \widetilde{\mathsf{V}}^{\mathrm{F}_\tau}$. Thus we have

$$h \cdot \dim_{\mathsf{K}} \mathsf{V}(\sigma,\zeta) = \dim_{\mathsf{K}} \widetilde{\mathsf{V}} = \dim_{\mathsf{k}} \widetilde{\mathsf{V}}^{\mathrm{F}} = \dim_{\mathsf{k}} \widetilde{\mathsf{V}}^{\mathrm{F}_\tau} = h \cdot \dim_{\mathsf{k}} \mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau},$$

so that

$$\dim_{\mathsf{k}} \mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau} = \dim_{\mathsf{K}} \mathsf{V}(\sigma,\zeta). \tag{39}$$

If $\dim_{\mathsf{K}} \mathsf{V}(\sigma,\zeta) = 1$ then, since $\mathsf{V}(\sigma,\zeta)_{\mathsf{reg}} \neq \varnothing$, we have $\mathsf{V}(\sigma,\zeta) \cap \ker\alpha = \{0\}$ for each $\alpha \in R$. It follows that

$$\mathsf{V}(\sigma,\zeta)_{\mathsf{reg}} = \mathsf{V}(\sigma,\zeta) - \{0\},$$

so that

$$\mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau}_{\mathsf{reg}} = \mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau} - \{0\}.$$

Hence from (39) we have

$$|\mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau}_{\mathsf{reg}}| = q - 1, \tag{40}$$

so the proposition holds in the case $\dim_{\mathsf{K}} \mathsf{V}(\sigma,\zeta) = 1$.

Next we note that if the proposition holds for some $\sigma,\ \tau,\ \zeta$, and if $d \mid m$, then the proposition also holds for $\sigma^d,\ \tau,\ \zeta^d$, because

$$\mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau}_{\mathsf{reg}} \subset \mathsf{V}(\sigma^d,\zeta^d)^{\mathrm{F}_\tau}_{\mathsf{reg}}. \tag{41}$$

In types B_n, C_n, G_2, F_4, E_n, every elliptic $\mathbb{Z}$-regular automorphism in $\mathrm{Aut}(R)$ is of the form σ^d [17, section 7], where σ is also elliptic $\mathbb{Z}$-regular and $\dim_{\mathsf{K}} V(\sigma,\eta) = 1$ for any $\eta \in \mathsf{K}^\times$ whose order is that of σ. Hence the proposition is proved in these cases.

For R of type D_{n+1} ($n \geq 2$), there are additional such σ of the following form. First note that $\mathrm{Aut}(D_{n+1}) = W(B_{n+1})$ acts on $\mathsf{V} = \mathsf{K}^{n+1}$ by permutations and sign changes of the basis $\{v_1,\ldots,v_{n+1}\}$. The subgroup $W(B_n)\times W(B_1)$ preserves the partition $\{\pm v_1,\ldots,\pm v_n\}\sqcup\{\pm v_{n+1}\}$. We have $\sigma = y^\ell \times z$, where $y \in W(B_n)$ and $z \in W(B_1)$ are Coxeter elements, and ℓ is an odd divisor of n. Note that y^ℓ also has order m. Choose any $\tau \in W(B_n)$ such that $\tau y \tau^{-1} = y^q$ and let $\zeta \in \mathsf{K}^\times$ have order m. Arguing as for (41), there exists $v \in \mathsf{K}^n \cap \mathsf{V}(y^\ell,\zeta)^{\mathrm{F}_\tau}$ such that $\langle\alpha, v\rangle \neq 0$ for all $\alpha \in B_n$. Writing $v = c_1v_1 + \cdots + c_nv_n$ with $c_i \in \mathsf{K}$, we have $c_i \pm c_j \neq 0$ for all $i \neq j$ and $c_i \neq 0$ for all i. It follows that $\langle\alpha, v\rangle \neq 0$ for all $\alpha \in R$, so that $v \in \mathsf{V}(\sigma,\zeta)^{\mathrm{F}_\tau}_{\mathsf{reg}}$.

For R of type A_n ($n \geq 2$) the situation is similar: besides the Coxeter elements in $W(A_n)$, the additional $\mathbb{Z}$-regular elliptic automorphisms $\sigma \in \mathrm{Aut}(R)$ are of the form $\sigma = y^\ell \times z$, where y is a Coxeter element in $W(B_n)$; in this case we must have n/ℓ odd. Now V is the quotient of K^{n+1} by the diagonal embedding of K. Take $v \in \mathsf{V}(y^\ell, \zeta)^{\mathrm{F}_\tau}$ regular for B_n, as above. The image of v in V belongs to $\mathsf{V}(\sigma, \zeta)^{\mathrm{F}_\tau}_{\mathsf{reg}}$. □

6 Representations of p-adic groups

Prop. 5.2 also has an application to the representation theory of semisimple p-adic groups. We sketch the background; for more details in this section see [18].

Recall that K denotes the maximal unramified extension of k in $\bar{k}$, and the residue field K of K is an algebraic closure of the residue field k of k.

Let $\mathcal{G}$ be a connected and simply connected almost simple algebraic group defined over k. We further assume $\mathcal{G}$ is quasi-split over k and split over a tamely ramified extension of k. For the moment we make no restrictions on the residue characteristic p of k. Let $\mathcal{S}$ be a maximal k-split torus of $\mathcal{G}$. The centralizer $\mathcal{T} := C_{\mathcal{G}}(\mathcal{S})$ is a maximal torus of $\mathcal{G}$ and $\mathcal{T}$ is defined over k. Let $\check{R}$ be the root system of $\mathcal{G}$ with respect to $\mathcal{T}$, and let R be the dual root system. Let W denote the Weyl group of R.

The given action of $\mathrm{Gal}(\bar{k}/k)$ on $\mathcal{T}$ transfers to an action on R. The resulting homomorphism

$$\varepsilon : \mathcal{W}_k \to \mathrm{Aut}(R)$$

determines the k-isomorphism class of the simply connected group $\mathcal{G}$. Since $\mathcal{G}$ is quasi-split, there is a base Δ of R such that $\varepsilon(\mathcal{W}_k) \subset \mathrm{Aut}(R, \Delta)$. The tamely ramified condition means that ε is trivial on the wild inertia subgroup of $\mathcal{W}_k$, and that the image of the inertia subgroup $\mathcal{I}_k$ is cyclic, say $\varepsilon(\mathcal{I}_k) = \langle \vartheta \rangle$, for some $\vartheta \in \mathrm{Aut}(R, \Delta)$ of order prime to p. The full image $\varepsilon(\mathcal{W}_k)$ is generated by ϑ and the image $\phi = \varepsilon(\mathrm{F})$ of a Frobenius element $\mathrm{F} \in \mathcal{W}_k$; these satisfy the relation $\phi\vartheta\phi^{-1} = \vartheta^q$.

The complete root datum of $\mathcal{G}$ is $(\check{X}, \check{R}, X, R)$, where

$$X = \mathrm{Hom}(\mathrm{GL}_1, \mathcal{T}) = \mathbb{Z}R, \qquad \check{X} = \mathrm{Hom}(\mathcal{T}, \mathrm{GL}_1) = \mathrm{Hom}(\mathbb{Z}R, \mathbb{Z}).$$

We let $\check{\rho} \in \check{X}$ be the unique element such that $\langle \alpha, \check{\rho} \rangle = 1$ for all $\alpha \in \Delta$, where here $\langle\ ,\ \rangle$ denotes the canonical pairing between X and $\check{X}$. Note that $\check{\rho}$ is fixed by $\mathrm{Aut}(R, \Delta)$, hence by $\varepsilon(\mathcal{W}_k)$.

Let $\mathcal{A} = \mathbb{R} \otimes X$, regarded as an affine space with basepoint 0. Via ε, the Weil group $\mathcal{W}_k$ also acts on $\mathcal{A}$ (fixing the basepoint) and we let

$$\mathcal{A}(k) = \mathcal{A}^{\varepsilon(\mathcal{W}_k)}, \qquad \mathcal{A}(K) = \mathcal{A}^{\varepsilon(\mathcal{I}_k)} = \mathcal{A}^\vartheta$$

denote the respective fixed-point subspaces of $\mathcal{W}_k$ and $\mathcal{I}_k$. The line $0 + \mathbb{R}\check{\rho}$ is contained in $\mathcal{A}(k)$. Associated to the pair (R, ϑ) is an affine root system Ψ_K consisting of affine functions on $\mathcal{A}^\vartheta$, whose Weyl group $W_{\mathsf{aff}}(R, \vartheta)$ is a discrete group of affine automorphisms of $\mathcal{A}^\vartheta$, generated by the reflections about the hyperplanes $\psi^{-1}(0)$, for $\psi \in \Psi_K$; see [18, (3.2)].

According to Bruhat-Tits [4], each point $x \in \mathcal{A}(k)$ determines a bounded open (parahoric) subgroup $\mathcal{G}_x(K) < \mathcal{G}(K)$. Moy-Prasad [14] defined a countable filtration of $\mathcal{G}_x(K)$ by normal subgroups, whose distinct terms we write here as

$$\mathcal{G}_x(K) > \mathcal{G}_{x,1}(K) > \mathcal{G}_{x,2}(K) > \cdots .$$

(For simplicity of exposition, our notation differs slightly from that of [14].) Taking fixed-points under $\mathrm{Gal}(K/k)$ gives a corresponding filtration

$$\mathcal{G}_x(k) > \mathcal{G}_{x,1}(k) > \mathcal{G}_{x,2}(k) > \cdots .$$

The top two quotients

$$\mathsf{H}_x = \mathcal{G}_x(K)/\mathcal{G}_{x,1}(K), \qquad \mathsf{V}_x = \mathcal{G}_{x,1}(K)/\mathcal{G}_{x,2}(K)$$

are, respectively, a reductive algebraic group and a K-vector space, both defined over k; the action of H_x on V_x, induced by the conjugation action of $\mathcal{G}_x(K)$ on $\mathcal{G}_{x,1}(K)$, gives an algebraic representation of H_x on V_x.

A linear functional λ in the dual space $\check{\mathsf{V}}_x$ of V_x is *stable* if its orbit under H_x is Zariski-closed with finite stabilizer $\mathsf{H}_{x,\lambda}$. Given a k-rational stable functional $\lambda \in \check{\mathsf{V}}_x(\mathsf{k})$ and an irreducible representation ρ of $\mathsf{H}_{x,\lambda}(\mathsf{k})$, the epipelagic construction in [18] produces an irreducible supercuspidal representation $\pi_{\lambda,\rho}$ of $\mathcal{G}(k)$. We have $\pi_{\lambda,\rho} = \pi_{\lambda',\rho'}$ if and only if (λ, ρ) and (λ', ρ') are conjugate under $\mathsf{H}_x(\mathsf{k})$. Let $\Pi_x(k)$ be the set of these representations $\pi_{\lambda,\rho}$ as (λ, ρ) varies over a set of representatives of the $\mathsf{H}_x(\mathsf{k})$-orbits of pairs (λ, ρ) as above.

We now resume our assumption that $p \nmid |W|$. In [18, Cor. 5.1], it was shown that $\check{\mathsf{V}}_x$ contains stable functionals over K if and only if x is conjugate under $W_{\mathsf{aff}}(R, \vartheta)$ to a point in $\mathcal{A}$ of the form $0 + \frac{1}{m}\check{\rho}$, where m is the order of an elliptic $\mathbb{Z}$-regular element of the coset $W\vartheta$. This amounts to a criterion for $\Pi_x(k')$ to be non-empty, for a sufficiently large finite unramified extension k'/k. (In [8] this criterion is shown to be valid without any assumptions on p, but still assuming k' is sufficiently large.)

In the case $p \nmid |W|$, we can now replace k' by k, as follows. Let $x = 0 + \frac{1}{m}\check{\rho}$, where m is the order of an elliptic $\mathbb{Z}$-regular element of the coset $W\vartheta$. Let $\zeta \in \mathsf{K}^\times$ have order m. By the Lang-Steinberg theorem for H_x, there exists a Cartan subspace (see [26] for the definition) $\mathfrak{c} \subset \check{\mathsf{V}}_x$ such that $\mathrm{F}(\mathfrak{c}) = \mathfrak{c}$ [18, section 6]. From [18, 7.3] there exist $\sigma \in W\vartheta$, $\tau \in W\phi$ such that $\tau\sigma\tau^{-1} = \sigma^q$, and there is an isomorphism

$$\mathfrak{c} \xrightarrow{\sim} \mathsf{V}(\sigma, \zeta) \tag{42}$$

intertwining the action of F on $\mathfrak{c}$ with F_τ on $V(\sigma, \zeta)$. From [17, Lemma 13] it follows that the stable functionals in $\mathfrak{c}$ correspond to points in $\mathsf{V}(\sigma, \zeta)_{\mathsf{reg}}$, under the map (42). It follows that V_x has stable functionals rational over k if and only if $\mathsf{V}(\sigma, \zeta)_{\mathsf{reg}}^{\mathrm{F}_\tau}$ is nonempty.

Thus, from Prop. 5.2 we conclude:

Corollary 6.1. *Assume that p does not divide $|W|$. Then $\Pi_x(k)$ is nonempty if and only if x is conjugate under $W_{\mathsf{aff}}(R, \vartheta)$ to a point in $\mathcal{A}(k)$ of the form $0 + \frac{1}{m}\check{\rho}$, where m is the order of an elliptic $\mathbb{Z}$-regular element of $W\vartheta$.*

Remark: It seems likely that Cor. 6.1 holds without any assumption on p.

References

[1] A. Borel, *Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tohoku Math. J., **13** (1961), pp. 216-240.

[2] A. Borel, J.P. Serre, *Sur certains sous-groupes des groupes de Lie compacts*, Comment. Math. Helv., **27** (1953), pp. 128-139.

[3] N. Bourbaki, *Lie groups and Lie algebras*, Chap. 4-6, Springer-Verlag, Berlin, 2002.

[4] F. Bruhat, J. Tits, *Groupes réductifs sur un corps local I*, Publ. Math. Inst. Hautes Études Sci. No. 48, (1972), pp. 5–251.

[5] C. Bushnell, G. Henniart, *The essentially tame local Langlands correspondence, I*, J. of the Amer. Math. Soc., **18** (2005), no. 3, pp. 685–710.

[6] R. Carter, *Conjugacy classes in the Weyl group*, Compositio Math., **25**, (1972), pp. 1–59.

[7] S. DeBacker and M. Reeder, *Depth-Zero Supercuspidal L-packets and their Stability*, Annals of Math., **169**, No.3, (2009), pp. 795–901.

[8] J. Fintzen, B. Romano, *Stable vectors in Moy-Prasad filtrations*, preprint, August 2015.

[9] B. Gross, M. Reeder, *Arithmetic invariants of discrete Langlands parameters*, Duke Math. Jour., **154** (2010), pp. 431–508.

[10] K. Hiraga, A. Ichino, T. Ikeda, *Formal degrees and adjoint gamma factors*, J. Amer. Math. Soc., **21** (2008), no. 1, pp. 283–304.

[11] J.W. Jones, D.P. Roberts, *Database of Local Fields*, http://math.asu.edu/~jj/localfields.

[12] T. Kaletha, *Epipelagic L-packets and rectifying characters*, Invent. Math., **202** (2015), pp. 1-89.

[13] B. Kostant, *The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group*, Amer. J. Math., **81** (1959), pp. 973–1032.

[14] A. Moy, G. Prasad, *Unrefined minimal K-types for p-adic groups*, Inv. Math. , **116** (1994), pp. 393–408.

[15] M. Reeder, *Torsion automorphisms of simple Lie algebras*, L'Enseignement Math., **56** (2) (2010), pp. 3–47.

[16] ______, *Adjoint Swan conductors II: Dyadic exercises in exceptional groups*, in preparation.

[17] M. Reeder, P. Levy, J.-K. Yu, B. Gross, *Gradings of positive rank on simple Lie algebras*, Transformation Groups, **17**, No 4, (2012), pp. 1123–1190.

[18] M. Reeder, J.-K. Yu, *Epipelagic representations and invariant theory*, J. of the Amer. Math. Soc., **27** (2014), no. 3, pp. 437–477.

[19] J.-P. Serre, *Local fields*, Springer-Verlag, 1979.

[20] T.A. Springer, *Regular elements in finite reflection groups*, Inv. Math., **25** (1974), pp. 159–198.

[21] R. Steinberg, *Regular elements of semi-simple algebraic groups*, Publ. Math. Inst. Hautes Études Sci. No. 25, (1965), pp. 49–80.

[22] ______, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc., **80** (1968).

[23] ______, *Torsion in reductive groups*, Advances in Math. **15** (1975), pp. 63–92.

[24] ______, *On the desingularization of the unipotent variety*, Invent. Math., **36** (1976), pp. 209–224.

[25] J. Tits, *Normalisateurs de tores I. Groups de Coxeter étendus*, Jour. Alg., **4**, (1966), pp. 96–116.

[26] E. B. Vinberg, *The Weyl group of a graded Lie algebra*, Izv. Akad. Nauk SSSR Ser. Mat., **40** no. 3 (1976), pp. 488-526. English translation: Math. USSR-Izv. **10** (1977), pp. 463–495.