Elliptic centralizers in Weyl groups and their coinvariant representations

Mark Reeder
Department of Mathematics, Boston College
Chestnut Hill, MA 02467
reederma@bc.edu

June 9, 2009

Abstract

The centralizer $C(w)$ of an elliptic element w in a Weyl group has a natural symplectic representation on the group of w-coinvariants in the root lattice. We give the basic properties of this representation, along with applications to p-adic groups - classifying maximal tori and computing inducing data in L-packets - as well as to elucidating the structure of the centralizer $C(w)$ itself. We give the structure of each elliptic centralizer in $W(E_8)$ in terms of its coinvariant representation, and we refine Springer's theory for elliptic regular elements to give explicit complex reflections generating $C(w)$. The case where w has order three is examined in detail, with connections to mathematics of the 19th century. A variation of the methods recovers the subgroup $W(H_4) \subset W(E_8)$.

1 Introduction

Let $W = W(R)$ be the Weyl group of an irreducible root system R with root lattice $X = \mathbb{Z}R$. For each $w \in W$, the coinvariants $X_w := X/(1-w)X$ form a finitely generated abelian group with an action of the centralizer $C(w)$ of w in W. We say that w is *elliptic* if X_w is finite. In this case X_w is a finite abelian group of order equal to the determinant of $1-w$ on X. Using the minimal polynomial of w, one can define a canonical alternating bilinear form $\langle\cdot,\cdot\rangle_w$ on X_w, whose isometry group we denote by $Sp(X_w)$. This form is preserved by the action of $C(w)$, so we have a homomorphism

$$\varrho_w : C(w) \longrightarrow Sp(X_w), \tag{1}$$

called the *coinvariant representation* of $C(w)$. More generally, the normalizer $N(w)$ of the cyclic group generated by w acts on X_w, now by similitudes of $\langle\cdot,\cdot\rangle_w$, and ϱ_w is the restriction of a representation

$$\tilde{\varrho}_w : N(w) \longrightarrow GSp(X_w). \tag{2}$$

These and other basic facts about coinvariant representations are proved in section 1 below.

This study of coinvariant representations was motivated by various problems in the structure and representation theory of reductive groups over p-adic fields, arising in recent work on the local Langlands correspondence ([13], [17], [20], [27]; see [16] for an introduction). These problems are of two related types: conjugacy of maximal tori and the structure of certain supercuspidal L-packets. Preliminary to this is the basic question of the structure of $C(w)$ itself, for which we have no general theory. We now give a brief description of these problems and how coinvariant representations help to solve them.

Conjugacy of maximal tori: In a connected reductive group G over an algebraically closed field, all maximal tori are conjugate. If G is defined over a general field k, then the maximal tori in G which are defined over k are in general not conjugate to one another by the group $G(k)$ of k-rational points in G. Assume that k is perfect with absolute Galois group Γ and that G is quasi-split over k with maximal torus T contained in a k-rational Borel subgroup of G. Let W be the absolute Weyl group of T. The classification of rational conjugacy classes of maximal tori in G (and in inner forms of G) can be approached in two steps, analogously to the theory of L-packets. First, one partitions the tori into "stable" classes $\mathcal{T}_\xi$, indexed by cohomology classes of Galois cocycles $\xi : \Gamma \to W$. Second, the rational classes in $\mathcal{T}_\xi$ are in bijection with the orbits in the cohomology $H^1(k, T_\xi)$ of the twisted torus T_ξ under the canonical affine action of the group $W_\xi(k)$ of k-rational points in the twist of W by ξ. This follows from standard Galois cohomology arguments and a result of Raghunathan; see Prop. 6.5 below. Thus, the classification of maximal tori in G is determined by the affine action of $W_\xi(k)$ on $H^1(k, T_\xi)$, for each class of cocycles $\xi : \Gamma \to W$.

We can make this more explicit when k is p-adic. For simplicity we also assume G is split over k and simply-connected, so that $X = X_*(T)$ and a Galois cocycle is just a homomorphism $\xi : \Gamma \to W$. If ξ is unramified, it is determined by an element $w \in W$, the image of Frobenius, which is elliptic precisely when T_ξ is anisotropic. Then Tate-Nakayama duality gives an isomorphism $H^1(k, T_\xi) \simeq X_w$. We have $W_\xi(k) = C(w)$ and the affine action of $W_\xi(k)$ on $H^1(k, T_\xi)$ coincides with the linear action of $C(w)$ on X_w via the coinvariant representation ϱ_w (see Lemma 6.11 below). Hence, the $G(k)$-classes of unramified maximal tori in the stable class $\mathcal{T}_\xi$ are in bijection with the orbits of $C(w)$ on X_w, via ϱ_w. This was previously shown in [13], but the proof here is simpler and appears in the broader context presented above; see section 6.11. Table 1 below gives the orbits of $C(w)$ on X_w for each conjugacy class of elliptic elements w in the Weyl group of E_8.

Suppose next that ξ is tamely ramified with inertial image generated by an elliptic element $w \in W$. The image u of Frobenius lies in the normalizer $N(w)$. (Cocycles ξ of this type arise from the simple wild Langlands parameters of [17].) Now $W_\xi(k) = C(w)^u$ is the centralizer of u in $C(w)$ and $H^1(k, T_\xi) = (X_w)_u = X_w/(1 - \tilde{\varrho}_w(u))X_w$ is the coinvariants of u in X_w under the coinvariant representation of $N(w)$. The rational classes in $\mathcal{T}_\xi$ are in bijection with the orbits of $C(w)^u$ on $(X_w)_u$ under the action induced by ϱ_w, but now twisted by a certain cocycle $\delta : C(w)^u \to (X_w)_u$. We show that in many cases δ is a coboundary; in this case, the classification of rational classes in $\mathcal{T}_\xi$ is again governed by the coinvariant representation ϱ_w. In general, the classification is reduced to the calculation of δ. We also note that the *in*variants $(X_w)^u$ appear in the structure of the lft Neron model of T_ξ (cf. [21, 7.6] and [25]).

Supercuspidal L-packets: Given p-adic group G as above, with elliptic $w \in W$, unramified twist T_w and a sufficiently nice character $\chi : T_w(k) \to \mathbb{C}^\times$, one can construct (cf. [13] [20] and [27]) a finite set $\Pi_w(\chi)$ of supercuspidal representations of $G(k)$, each induced from a certain maximal compact subgroup of $G(k)$. Since $G(k)$ has several conjugacy-classes of maximal compact subgroups, we wish to determine which ones arise for each representation in $\Pi_w(\chi)$.

The set $\Pi_w(\chi)$ constitutes an L-packet in accordance with the local Langlands conjecture. Among other things, this means we have a bijection $X_w \to \Pi_w(\chi)$, denoted $\rho \mapsto \pi_w(\chi, \rho)$, with the property that $\pi_w(\chi, \rho)$ and $\pi_w(\chi, \rho')$ are induced from the same maximal compact subgroup if ρ and ρ' belong to the same orbit of $C(w)$ in X_w. Moreover, the point stabilizers of $C(w)$ in X_w determine the maximal compact subgroups appearing in $\Pi_w(\chi)$. Thus, the coinvariant representation can be used to determine the inducing data of the representations in $\Pi_w(\chi)$. For G of type E_8, one can read off the inducing maximal compact subgroups in the L-packets $\Pi_w(\chi)$ from Table 1.

Centralizers in Weyl groups: In the study of root systems, it is a basic question to ask for the structure of the centralizers of elements in a Weyl group W. The conjugacy classes in W were determined by Carter [6] using the root system. He also found the orders of the centralizers, but not their group structure.

If W is of classical type, it is straightforward to describe all centralizers using the presentation of W as permutations and sign changes. Among exceptional Weyl groups, the most interesting is $W = W(E_8)$, our main focus from now on.

The coinvariant representation can be useful for describing the structure of $C(w)$, as in the following well-known example (cf. [3], [26]): Let $W = W(E_8)$ with $w = -1$. Then $C(w) = W$ and $X_w = X/2X$, on which W preserves the quadratic form $q(x) = \frac{1}{2}\langle x, x\rangle \mod 2$, where $\langle\ ,\ \rangle$ is the symmetric W-invariant pairing on X. The image of ϱ_w turns out to be the full orthogonal group of q, so W is presented as a covering

$$1 \longrightarrow \langle -1\rangle \longrightarrow W \longrightarrow O_8^+(2) \longrightarrow 1. \tag{3}$$

For any elliptic $w \in W(E_8)$, the form $\langle\ ,\ \rangle_w$ is nondegenerate and satisfies $\langle x, x\rangle_w = 0$ for all $x \in X_w$. The coinvariant representation often gives a similar description of $C(w)$ as a covering of a classical group. To illustrate, using Carter's notation for conjugacy classes: for $w = A_2^4$ we have the exact sequence

$$1 \longrightarrow \langle w\rangle \longrightarrow C(w) \xrightarrow{\varrho_w} Sp_4(3) \longrightarrow 1, \tag{4}$$

and for $w = A_1^4 D_4$, we have the exact sequence

$$1 \longrightarrow \langle w\rangle \longrightarrow C(w) \xrightarrow{\varrho_w} O_6^-(2) \longrightarrow 1. \tag{5}$$

Often ϱ_w is surjective (as in (4)) or has a relatively large image (as in (5)). Table 1 in section 2.2 gives the description of all elliptic centralizers $C(w)$ in $W(E_8)$ in terms of their coinvariant representations ϱ_w.

Regular elements, complex reflection groups, graded Lie algebras and cyclotomic structures: Following Springer, an element $w \in W$ is called *regular* if some eigenvector v of w in $\mathbb{C} \otimes X$ has trivial stabilizer in W. Springer showed that when w is regular, the centralizer $C(w)$ acts faithfully as a complex reflection group on the w-eigenspace containing v, and that the degrees of the complex reflection group $C(w)$ are those degrees of W which are divisible by the order of w. Knowing the degrees, one can usually locate $C(w)$ in the Shephard-Todd classification of complex reflection groups. However, Springer uses invariant theory to characterize reflection groups, a method which does not produce the actual reflections in $C(w)$ in an obvious way. Therefore it remains to complete Springer's theory of regular elements by finding the complex reflections which generate $C(w)$, for regular w. In section 3 we do this for those w with irreducible minimal polynomial on X; we call such elements *cyclotomic*.

When w is cyclotomic we find the reflections generating $C(w)$ by viewing $V := \mathbb{Q} \otimes X$ as a vector space over a the cyclotomic field $K = \mathbb{Q}(w) \subset \mathrm{End}(V)$. The reflections arise from an equivalence relation on the set of roots, via the action of K.

It is a remarkable fact that in the Weyl groups of types G_2, F_4 and E_8, the cyclotomic elements are precisely those which are both elliptic and regular. Hence the centralizer of an elliptic regular element $w \in W(E_8)$ of order d is the automorphism group of a cyclotomic $\mathbb{Z}[\zeta_d]$-structure on the E_8-root lattice $X(E_8)$, where ζ_d is a complex root of unity of order d. Some of these cyclotomic structures, e.g., for $d = 3, 4$, were found by *ad hoc* methods in the 19th century [8]. Recent literature on lattice theory [2] mentions the $\mathbb{Z}[\zeta_{15}]$-structure on $X(E_8)$. These, indeed all of the cyclotomic structures on $X(E_8)$ are unified by viewing them as arising from elliptic regular elements in $W(E_8)$.

Cyclotomic elements also appear in Vinberg's theory of graded Lie algebras [35]. If $\mathfrak{g}$ is a simple complex Lie algebra and G_σ is the identity component of the centralizer of an automorphism $\sigma \in \mathrm{Aut}(\mathfrak{g})$ of order d, then the representation of G_σ on the ζ_d-eigenspace $\mathfrak{g}_\sigma$ of σ shares many properties with the adjoint representation of G on $\mathfrak{g}$. In particular, the closed orbits of G_σ in $\mathfrak{g}_\sigma$ are controlled by a finite group W_σ analogous to W. Vinberg [35, Prop. 19] shows that if σ is an inner automorphism normalizing a Cartan subalgebra and acting there via a cyclotomic element $w \in W$, then $W_\sigma \simeq C(w)$ and W_σ is in particular a complex reflection group. Thus, our results give the reflections generating W_σ in this case.

When w is cyclotomic, the coinvariant group X_w is zero unless the order d of w is a power of a prime p, in which case X_w is the reduction modulo $\mathfrak{P}$ of the $\mathbb{Z}[\zeta_d]$-module X, where $\mathfrak{P} = (1-\zeta_d)\mathbb{Z}[\zeta_d]$ is the unique prime ideal of $\mathbb{Z}[\zeta_d]$ ramified over $\mathbb{Z}$.

This interplay between complex and modular representations, while useful in both directions, is especially striking when w is elliptic of order three. Here it is worthwhile to consider all root systems where this occurs, as each has unique features which are related to geometric structures investigated by Maschke and his contemporaries, and later by Coxeter. These are discussed in Appendix A.

Finally, in Appendix B, we use a variant of our method for producing reflections out of cyclotomic structures to explain the (known, cf. [23]) embedding of the non-crystallographic Coxeter group $W(H_4)$ in $W(E_8)$ as the centralizer of a $\mathbb{Z}[\tau]$-structure on the E_8 root lattice, where τ is the golden ratio.

I thank D. Vogan for his comments on an earlier version of this paper, S. DeBacker for pointing me to Raghunathan's article [24], and B. Gross for filling the margins with meticulous criticism.

Contents

2 The coinvariant representation

2.1 Quadratic lattices

Let X be a $\mathbb{Z}$-lattice in a $\mathbb{Q}$-vector space V of dimension n, and suppose we have a positive definite quadratic form $\langle\ ,\ \rangle$ on V taking integer values on X. Let $A = A(X)$ be the (finite) subgroup of the orthogonal group $O(V)$ preserving X. We assume that $w \in A$ is **elliptic**, that is, w has no nonzero fixed vectors in V. Equivalently, the group of coinvariants

$$X_w := X/(1-w)X$$

is finite, of order $|X_w| = \det(1-w) = F(1)$, where $F(t) = \det(t-w)$ is the characteristic polynomial of w in $\mathrm{End}(X)$. Since w is of finite order and preserves X, its characteristic polynomial factors as a product of cyclotomic polynomials

$$F(t) = \Phi_{d_1}(t)^{e_1} \cdot \Phi_{d_2}(t)^{e_2} \cdots \Phi_{d_k}(t)^{e_k},$$

where $d_1 < d_2 < \cdots < d_k$ and the e_i are positive integers. Here $\Phi_d(t)$ is the minimal polynomial of the complex roots of unity of order d. Since w is elliptic we have $d_1 \geq 2$, and

$$F(1) = \prod_{i \in I} \ell_i^{e_i},$$

where I is the set of indices $i \in \{1, 2, \ldots, k\}$ for which d_i is a power of a prime ℓ_i. The minimal polynomial of w in $\mathrm{End}(X)$ is

$$M(t) = \Phi_{d_1}(t) \cdot \Phi_{d_2}(t) \cdots \Phi_{d_k}(t),$$

and the integer

$$m := M(1) = \prod_{i \in I} \ell_i$$

divides $F(1)$. The polynomial

$$\dot{M}(t) = \frac{M(t) - M(1)}{t-1}$$

also has integer coefficients, and satisfies

$$(1-t)\dot{M}(t) + M(t) = m.$$

Let $\mathbb{Z}[w]$ be the $\mathbb{Z}$-subalgebra of $\mathrm{End}(X)$ generated by w. In the ring $\mathbb{Z}[w]$, we have the equation

$$(1-w)\dot{M}(w) = m. \tag{6}$$

It follows that $mX \subset (1-w)X$, so that $mX_w = 0$ and X_w is a $\mathbb{Z}/m\mathbb{Z}$-module. This also implies that we have a well-defined pairing

$$\langle\ ,\ \rangle_w : X_w \times X_w \to \mathbb{Z}/m\mathbb{Z}$$

given by

$$\langle x, y\rangle_w = \langle \lambda_x, \dot{M}(w)\lambda_y\rangle \mod m,$$

where $x, y \in X_w$ have lifts $\lambda_x, \lambda_y \in X$.

Lemma 2.1 *The pairing $\langle\ ,\ \rangle_w$ is skew-symmetric : $\langle x, y\rangle_w = -\langle y, x\rangle_w$ for all $x, y \in X_w$. If the quadratic lattice X is even, then $\langle x, x\rangle_w = 0$ for all $x \in X_w$*

Proof: Since w preserves the form $\langle\ ,\ \rangle$, we have

$$\langle \mu, \dot{M}(w)\lambda\rangle = \langle \lambda, \dot{M}(w^{-1})\mu\rangle$$

for all $\lambda, \mu \in X$. But $M(t)$ is also the minimal polynomial of w^{-1}, so

$$(1-w^{-1})\dot{M}(w^{-1}) = m = (1-w)\dot{M}(w),$$

or

$$-w^{-1}(1-w)\dot{M}(w^{-1}) = (1-w)\dot{M}(w).$$

Since $1-w$ is a unit in $\mathrm{End}(V)$, this implies that

$$\dot{M}(w^{-1}) = -w\dot{M}(w) = (1-w)\dot{M}(w) - \dot{M}(w) = m - \dot{M}(w). \tag{7}$$

This implies the first assertion. Since w preserves the symmetric form $\langle\ ,\ \rangle$, we have, for all $\lambda \in X$,

$$\langle \lambda, \dot{M}(w)\lambda\rangle = \langle \lambda, \dot{M}(w^{-1})\lambda\rangle,$$

so (7) also implies that

$$\langle \lambda, \dot{M}(w)\lambda\rangle = \langle \lambda, m - \dot{M}(w)\lambda\rangle,$$

or

$$\langle \lambda, \dot{M}(w)\lambda\rangle = m \cdot \frac{\langle \lambda, \lambda\rangle}{2} \in m\mathbb{Z}$$

if $\langle \lambda, \lambda \rangle \in 2\mathbb{Z}$. This proves the last assertion ■

We say the form $\langle\ ,\ \rangle_w$ is *nondegenerate* if the radical

$$X_w^0 := \{u \in X_w :\ \langle u, X_w \rangle_w = 0\ \}$$

is zero. We can determine X_w^0 using the dual lattice

$$\hat{X} := \{\lambda \in V :\ \langle \lambda, X \rangle \subset \mathbb{Z}\}.$$

Note that $X \subseteq \hat{X}$ because we have assumed that $\langle\ ,\ \rangle$ is integer-valued on X.

Lemma 2.2 *We have*

$$X_w^0 = \frac{X \cap (1-w)\hat{X}}{(1-w)X} = \ker[X_w \to \hat{X}_w],$$

where the latter map is induced by the inclusion $X \hookrightarrow \hat{X}$. If $X = \hat{X}$ is self-dual, then the form $\langle\ ,\ \rangle_w$ is nondegenerate for every elliptic $w \in A(X)$.

Proof: Let $\lambda \in X$ have image $x \in X_w$. By (6) we have

$$\begin{aligned}\langle x, X_w \rangle_w = 0 &\Leftrightarrow \langle \dot{M}(w)\lambda, X \rangle \subset m\mathbb{Z} \\ &\Leftrightarrow \dot{M}(w)\lambda \in m\hat{X} \\ &\Leftrightarrow \dot{M}(w)\lambda \in \dot{M}(w)(1-w)\hat{X} \\ &\Leftrightarrow \lambda \in (1-w)\hat{X},\end{aligned} \tag{8}$$

Since $\dot{M}(w)$ is invertible on V. The lemma follows. ■

Let $C_A(w)$ be the centralizer of w in $A(X)$. This group acts naturally on X_w, giving a canonical homomorphism

$$\varrho_w : C_A(w) \to Sp(X_w),$$

where $Sp(X_w)$ is the group of automorphisms of the group X_w preserving the form $\langle\ ,\ \rangle_w$. We call ϱ_w the *coinvariant representation* of $C_A(w)$. Clearly ϱ_w contains w in its kernel. Often, $\ker \varrho_w$ is generated by w, but this is not always the case, and the following Lemma can be used to determine $\ker \varrho_w$ in particular cases.

Lemma 2.3 *An element $v \in C_A(w)$ belongs to $\ker \varrho_w$ exactly when the matrix of $(I-v)\cdot(I-w)^{-1}$ with respect to a basis of X is integral.*

Proof: This is immediate from the observation that $\varrho_w(v) = 1$ iff $(1-v)X \subset (1-w)X$. ■

The representation ϱ_w extends to a representation $\tilde{\varrho}_w : N_A(w) \to \mathrm{Aut}(X_w)$ of the subgroup $N_A(w) \subset A(X)$ normalizing the group $\langle w \rangle$ generated by w. If $u \in N_A(w)$ then $uwu^{-1} = w^{s(u)}$, where $s(u)$ is an integer prime to the order d of w. Since m divides d, we obtain a homomorphism $\sigma : N_A(w) \to (\mathbb{Z}/m\mathbb{Z})^\times$, defined by $\sigma(u) = s(u) + m\mathbb{Z}$.

Proposition 2.4 *For every $u \in N_A(w)$ and $x, y \in X_w$, we have*

$$\langle \tilde{\varrho}_w(u)x, \tilde{\varrho}_w(u)y\rangle_w = \sigma(u)\langle x, y\rangle_w.$$

In particular, $\tilde{\varrho}_w$ sends $N_A(w)$ to the similitude group $GSp(X_w)$.

Proof: We must show that

$$\langle u\lambda, \dot{M}(w)u\mu\rangle \equiv \sigma(u)\langle \lambda, \dot{M}(w)\mu\rangle \mod m,$$

or equivalently,

$$\langle \lambda, \dot{M}(w)\mu\rangle \equiv \sigma(u)\langle u^{-1}\lambda, \dot{M}(w)u^{-1}\mu\rangle \mod m,$$

for all $\lambda, \mu \in X$. Since u preserves the form $\langle\ ,\ \rangle$ on X and $u\dot{M}(w)u^{-1} = \dot{M}(w^{s(u)})$, it suffices to show that

$$\dot{M}(w) \equiv s\dot{M}(w^s) \mod m\mathbb{Z}[w],$$

for every positive integer s prime to m. For this, we may assume $s = p$ is a prime not dividing m. Viewing our problem in $\mathbb{Z}[t]$, we must show that $\dot{M}(t) - p\dot{M}(t^p)$ belongs to the ideal generated by m and $M(t)$ in $\mathbb{Z}[t]$.

Since $M(t) = \Phi_{d_1}(t) \cdot \Phi_{d_2}(t) \cdots \Phi_{d_k}(t)$ and p does not divide any d_i, we have $M(t^p) = M(t) \cdot N(t)$, where

$$N(t) = \Phi_{pd_1}(t) \cdot \Phi_{pd_2}(t) \cdots \Phi_{pd_k}(t)$$

and $N(1) = 1$. Hence

$$\begin{aligned} \Phi_p(t) \cdot [\dot{M}(t) - p\dot{M}(t^p)] &= \Phi_p(t) \cdot \frac{M(t) - m}{t-1} - p\Phi_p(t) \cdot \frac{M(t)N(t) - m}{t^p - 1} \\ &= \Phi_p(t) \cdot \frac{M(t) - m}{t-1} - p \cdot \frac{M(t)N(t) - m}{t-1} \\ &= \left[\frac{\Phi_p(t) - pN(t)}{t-1}\right] \cdot M(t) + \left[\frac{p - \Phi_p(t)}{t-1}\right] \cdot m. \end{aligned} \tag{9}$$

Since $\Phi_p(1) = p$ and $N(1) = 1$, the terms in square brackets in the last line of (9) belong to $\mathbb{Z}[t]$. It now suffices to show that $\Phi_p(t)$ is a unit in the ring $\mathbb{Z}[t]/(m, M(t))$. By the Chinese remainder theorem, we may assume m is a power of a prime $\ell \neq p$. An argument like that of Hensel's Lemma reduces us to the case $m = \ell$. But $\Phi_p(t)$ is a unit in $\mathbb{F}_\ell[t]/(M(t))$ since the roots of Φ_p and $M(t)$ in $\bar{\mathbb{F}}_\ell$ have relatively prime orders. This concludes the proof of Prop. 2.4. ■

2.2 Table of elliptic centralizers and coinvariants in E_8

Let X be the lattice generated by the root system R of type E_8, with quadratic form $\langle\ ,\ \rangle$ normalized so that $\langle \alpha, \alpha\rangle = 2$ for all $\alpha \in R$, so that $\hat{X} = X$. The automorphism group $A(X) = W$ is the Weyl group of R and we write $C(w) = C_A(w)$ for the centralizer in W of an element $w \in W$. For any elliptic element $w \in W$, the form $\langle\ ,\ \rangle_w$ is nondegenerate on X_w, by Lemma 2.2 . Hence X_w and its character group are isomorphic as modules for $C(w)$. We can view X and W as the algebraic character group and Weyl group of a maximal torus $\hat{T}$ in a complex Lie group $\hat{G}$ of type E_8. The fixed-point subgroup $\hat{T}^w$ is canonically the character group of X_w, so the form $\langle\ ,\ \rangle_w$ identifies $X_w = \hat{T}^w$ as $C(w)$-modules. Since $\hat{G}$ is simply-connected, the centralizer $\hat{G}_t$ is connected for every $t \in \hat{T}^w$ and the stabilizer W_t of t in W is the Weyl group of $\hat{T}$ in $\hat{G}_t$. Since $w \in W_t$ is elliptic, it follows that $\hat{G}_t$ is semisimple, and t belongs to one of nine conjugacy-classes in $\hat{G}$, where the Dynkin diagram of $\hat{G}_t$ is obtained by removing a node from the extended Dynkin diagram of $\hat{G}$. In particular, the order of t is at most six, for any elliptic $w \in W$.

In Table 1 we tabulate the conjugacy classes of elliptic elements $w \in W(E_8)$ in the notation of [6], along with their orders and characteristic polynomials. Classes which are negatives of each other have the same centralizer (but different coinvariants) and are grouped together. Next, we give the group structure of X_w, the order of $C(w)$ (obtained from [6]) and the kernel and image in the extension

$$1 \longrightarrow \ker \varrho_w \longrightarrow C(w) \longrightarrow \operatorname{im} \varrho_w \longrightarrow 1.$$

Finally we give the orbit decomposition of $X_w - \{0\} = \hat{T}^w - \{1\}$ under $C(w)$, where the *orbit type* of the orbit through $t \in \hat{T}^w$ is type of the Dynkin diagram of the centralizer $\hat{G}_t$. The details behind these results, and further information about each centralizer are given in later sections, indicated in the rightmost column in 1.

Class of w	$\lvert w\rvert$	$\det(t-w)$	X_w	$\lvert C(w)\rvert$	$\ker \varrho_w \bullet \mathrm{im}\, \varrho_w$	nonzero orbit types	details
E_8	30	Φ_{30}	0	$2\cdot 3\cdot 5$	$\langle w\rangle \bullet 1$	-	-
$E_8(a_1)$	24	Φ_{24}	0	$2^3\cdot 3$	$\langle w\rangle \bullet 1$	-	-
$E_8(a_2)$	20	Φ_{20}	0	$2^2\cdot 5$	$\langle w\rangle \bullet 1$	-	-
$E_8(a_5)$	15	Φ_{15}	0	$2\cdot 3\cdot 5$	$\langle E_8\rangle \bullet 1$	-	-
$E_8(a_3)$	12	Φ_{12}^2	0	$2^5\cdot 3^2$	$[\langle w^4\rangle \times U_2(3)] \bullet 1$	-	3.4.5 4.2.4
$E_8(a_6)$	10	Φ_{10}^2	0	$2^3\cdot 3\cdot 5^2$	$[\langle -w\rangle \times SL_2(5)] \bullet 1$	-	3.4.3
A_4^2	5	Φ_5^2	5^2	$2^3\cdot 3\cdot 5^2$	$\langle w\rangle \bullet SL_2(5)$	$24[A_4^2]$	4.2.1
$D_8(a_3)$	8	Φ_8^2	2^2	$2^6\cdot 3$	$[\langle w\rangle \cdot Q_8] \bullet SL_2(2)$	$3[D_8]$	3.4.4 4.2.2
$E_8(a_8)$	6	Φ_6^4	0	$2^7\cdot 3^5\cdot 5$	$[\langle -w\rangle \times Sp_4(3)] \bullet 1$	-	3.4.2
A_2^4	3	Φ_3^4	3^4	$2^7\cdot 3^5\cdot 5$	$\langle w\rangle \bullet Sp_4(3)$	$80[A_2E_6]$	4.1,A.3
$D_4(a_1)^2$	4	Φ_4^4	2^4	$2^{10}\cdot 3^2\cdot 5$	$[\langle w\rangle \cdot (2^3{\cdot}2^2)] \bullet Sp_4(2)$	$15[D_8]$	3.4.1 4.2.3
A_1^8	2	Φ_2^8	2^8	$2^{14}{\cdot}3^5{\cdot}5^2{\cdot}7$	$\langle w\rangle \bullet O_8^+(2)$	$120[A_1E_7]{+}135[D_8]$	1
$E_8(a_4)$	18	$\Phi_{18}\Phi_6$	0	$2\cdot 3^3$	$[\langle w\rangle \times 3] \bullet 1$	-	-
A_8	9	$\Phi_9\Phi_3$	3^2	$2\cdot 3^3$	$\langle w\rangle \bullet 6$	$6[A_8]+2[A_2E_6]$	5.1
$E_8(a_7)$	12	$\Phi_{12}\Phi_6^2$	0	$2^5\cdot 3^2$	$[\langle w\rangle \times SL_2(3)] \bullet 1$	-	
A_2E_6	12	$\Phi_{12}\Phi_3^2$	3^2	$2^5\cdot 3^2$	$\langle w\rangle \bullet SL_2(3)$	$8[E_6A_2]$	5.2
$A_1^2A_3^2$	4	$\Phi_4^2\Phi_2^4$	$4^2{\cdot}2^2$	$2^{11}\cdot 3^2$	$\langle w\rangle \bullet Sp(X_w)$	$48[A_3D_5]{+}12[A_1E_7]$ $+3[D_8]$	5.10
$A_5A_2A_1$	6	$\Phi_6\Phi_3^2\Phi_2^2$	$3^2{\cdot}2^2$	$2^5\cdot 3^3$	$\langle w\rangle \bullet [SL_2(3){\times}SL_2(2)]$	$24[A_5A_2A_1]$ $+8[A_2E_6]+3[A_1E_7]$	5.2
D_8	14	$\Phi_{14}\Phi_2^2$	2^2	$2^2\cdot 7$	$\langle w\rangle \bullet 2$	$1[A_1E_7]+2[D_8]$	5.1
$D_8(a_2)$	30	$\Phi_{10}\Phi_6\Phi_2^2$	2^2	$2^2\cdot 3\cdot 5$	$\langle w\rangle \bullet 2$	$1[A_1E_7]+2[D_8]$	5.1
$D_8(a_1)$	12	$\Phi_{12}\Phi_4^2$	2^2	$2^3\cdot 3^2$	$\langle w\rangle \bullet SL_2(2)$	$3[D_8]$	2.3
A_7A_1	8	$\Phi_8\Phi_4\Phi_2^2$	$8{\cdot}2$	2^7	$\langle w\rangle \bullet \mathrm{Aut}(C_8{\times}C_2)$	$8[A_7A_1]+4[A_3D_5]$ $+2[A_1E_7]+1[D_8]$	5.2
$A_1^2D_6$	10	$\Phi_{10}\Phi_2^4$	2^4	$2^4\cdot 3\cdot 5^2$	$\langle w\rangle \bullet S_5$	$10[A_1E_7]+5[D_8]$	5.6
D_4^2	6	$\Phi_6^2\Phi_2^4$	2^4	$2^5\cdot 3^4$	$[\langle w\rangle{\times}S_3] \bullet [(S_3^2){\cdot}2]$	$6[A_1E_7]+9[D_8]$	5.7
$A_1^4D_4$	6	$\Phi_6\Phi_2^6$	2^6	$2^8\cdot 3^5\cdot 5$	$\langle w\rangle \bullet O_6^-(2)$	$36[A_1E_7]+27[D_8]$	5.8
$A_3D_5(a_1)$	12	$\Phi_6\Phi_4^2\Phi_2^2$	4^2	$2^6\cdot 3^2$	$\langle w\rangle \bullet SL_2(\mathbb{Z}/4)$	$12[A_3D_5]+3[D_8]$	5.9
$A_2E_6(a_2)$	6	$\Phi_6^2\Phi_3$	3^2	$2^6\cdot 3^3$	$[\langle w^2\rangle{\times}SL_2(3)] \bullet SL_2(3)$	$8[A_2E_6]$	5.5
A_1E_7	18	$\Phi_{18}\Phi_2^2$	2^2	$2^2\cdot 3^3$	$\langle w\rangle \bullet SL_2(2)$	$3[A_1E_7]$	5.2
$A_1E_7(a_2)$	12	$\Phi_{12}\Phi_6\Phi_2^2$	2^2	$2^4\cdot 3^2$	$[2{\times}\langle w\rangle] \bullet SL_2(2)$	$3[A_1E_7]$	5.3
$A_1E_7(a_4)$	6	$\Phi_6^3\Phi_2^2$	2^2	$2^5\cdot 3^5$	$[\pm C_{E_6}(w)] \bullet SL_2(2)$	$3[A_1E_7]$	5.4

Table 1: Elliptic Centralizers in $W(E_8)$ and their coinvariant representations

3 Cyclotomic automorphisms of root systems

In Table1 above, we have listed first those classes in W with irreducible minimal polynomials. The centralizers of such classes can be understood in a uniform way that is analogous to the description of centralizers in classical groups over fields (see e.g. [32]).

Let W be Weyl group of an irreducible root system R, acting on the root lattice $X = \mathbb{Z}R$. Set $V = \mathbb{Q} \otimes V$ and $\bar{V} = \bar{\mathbb{Q}} \otimes V$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We say $w \in W$ is *cyclotomic* if its minimal polynomial $M(t)$ on V is irreducible over $\mathbb{Q}$. This means that $M(t)$ is the cyclotomic polynomial $\Phi_d(t)$, where d is the order of w. Extending the W-invariant pairing $\langle\ ,\ \rangle$ to $\bar{V}$, we say $w \in W$ is *regular* (cf. [31]) if w has an eigenvector in $\bar{V}$ not orthogonal to any root in R.

Lemma 3.1 *Every non-identity cyclotomic element $w \in W$ is elliptic and regular. For R of type G_2, F_4, E_8 every elliptic regular element in W is cyclotomic.*

Proof: If $w \in W$ is cyclotomic the Galois group $\Gamma = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is transitive on the eigenvalues of w. This Galois action extends to $\bar{V}$, acting trivially on V, so as to commute with the W-action. Thus, Γ permutes the eigenspaces of w transitively.

Each root $\alpha \in R$ may be viewed as a linear functional on $\bar{V}$, via the pairing $\langle\ ,\ \rangle$. In this guise, the map $\alpha : \bar{V} \to \bar{\mathbb{Q}}$ commutes with the Γ-action on $\bar{V}$ and $\bar{\mathbb{Q}}$. Hence if α vanishes on one eigenspace of w, it must vanish on all eigenspaces, so that $\alpha = 0$, a contradiction. Therefore every root $\alpha \in R$ restricts to a nonzero functional on every w-eigenspace in $\bar{V}$. Since R is finite, it follows that every w-eigenspace in $\bar{V}$ contains a regular vector. In particular, w is regular. It is clear that w is elliptic if $w \neq 1$.

If R has type G_2, F_4 or E_8, Springer's list of regular elements [31, 5.4] shows that all elliptic regular elements are cyclotomic. ■

In this chapter, we will sharpen Springer's results by finding the reflections in $C(w)$ for cyclotomic elements w and then we work out the details for cyclotomic centralizers in type E_8.

3.1 Cyclotomic elements and exponents

The cyclotomic classes in W can be classified in terms of the exponents of W.

If $v \in W$ has irreducible *characteristic* polynomial $\Phi_e(t)$, then for each divisor $d \mid e$, the element $w = v^{e/d}$ is cyclotomic, with minimal polynomial $\Phi_d(t)$. In fact, a case-by-case check shows that all cyclotomic elements $w \neq \pm 1$ can be found in this way:

Lemma 3.2 *If $w \in W$ is cyclotomic of order $d > 2$ then $w = v^{e/d}$ where $v \in W$ has irreducible characteristic polynomial $\Phi_e(t)$ and d divides e.*

In turn, the elements with irreducible characteristic polynomial can be classified as follows.

Lemma 3.3 *Let $e \geq 2$ be an integer. Then the following are equivalent:*

1. *There exists $v \in W$ with characteristic polynomial $\Phi_e(t)$.*

2. *The exponents* $\{m_1, \dots, m_n\}$ *of* W *represent the cosets in* $(\mathbb{Z}/e\mathbb{Z})^\times$.

If these conditions hold, then v *is regular, unique up to conjugacy, and the centralizer* $C(v) = \langle v' \rangle$ *is cyclic of order equal to the unique degree* $d_i = m_i + 1$ *of* W *which is divisible by* e. *Conditions 1,2 also hold with* (e, v) *replaced* (d_i, v').

Proof: Assuming condition 1, regularity was proved by Springer in [31, 4.11] and also follows from the proof of Lemma 3.8 above. Uniqueness now follows from [31, 4.2], which also shows that the eigenvalues of v are η^{m_i}, $i = 1, \dots, n$, where $\eta \in \bar{\mathbb{Q}}^\times$ has order e. But these eigenvalues are the roots of $\Phi_e(t)$, so $\{m_1, \dots, m_n\}$ is a system of representatives for $(\mathbb{Z}/e\mathbb{Z})^\times$.

Now assume condition 2 holds. We may assume $n \geq 2$. Then $n = \phi(e)$ is even. Moreover, for any prime $p \mid e$, we have the constraints

$$p \leq n + 1, \qquad p \nmid m_i, \quad 1 \leq i \leq n. \tag{10}$$

For $R = A_n$, with exponents $\{1, 2, \dots, n\}$, the second constraint implies that $p \geq n + 1$. Hence $n = p - 1$ for some prime p, and v is a Coxeter element, with characteristic polynomial $\Phi_p(t)$.

For B_n, C_n, constraints (10) imply that n is a power of 2 and v is a Coxeter element in W, with characteristic polynomial $t^n + 1 = \Phi_{2n}(t)$.

Consider $R = D_n$. We have seen that n is even. But then $n-1$ appears twice as an exponent; conditions 1,2 never hold.

For G_2, F_4, E_6, E_8, there are few primes satisfying the constraints (10) and few possibilities for e such that $\phi(e) = n$. With the exception of $e = 4$ for G_2 and $e = 16$ for E_8, there is an element $v \in W$ of order e. These are tabulated below, in the notation of [6], for conjugacy-classes in W.

R	exponents	e	v
G_2	$1, 5$	3,6	$A_2,\ G_2$
F_2	$1, 5, 7, 11$	$8, 12$	$B_4,\ F_4$
E_6	$1, 4, 5, 7, 8, 11$	9	$E_6(a_1)$
E_8	$1, 7, 11, 13, 17, 19, 23, 29$	$15, 20, 24, 30$	$E_8(a_5),\ E_8(a_2),\ E_8(a_1),\ E_8$

For the cases in this table, we have $C(v) = \langle v \rangle$, except for class A_2 in G_2 and $E_8(a_5)$, which are each the square of a Coxeter element v', and $C(v) = \langle v' \rangle$. ■

Proposition 3.4 *If* $w \in W$ *is cyclotomic then* $C(w)$ *is irreducible on every eigenspace of* w *in* $\bar{V}$.

Proof: We may assume $w \neq \pm 1$. Let $w = v^{e/d}$ as in Lemma 3.2. We will actually show that $C(w) \cap N(v)$ is irreducible on every eigenspace of w, where $N(v)$ denotes the normalizer in W of the subgroup $\langle v \rangle$ generated by v. There is a homomorphism

$$\sigma : N(v) \longrightarrow (\mathbb{Z}/e\mathbb{Z})^\times$$

defined by $n^{-1}vn = v^{\sigma(n)}$, for $n \in N(v)$. It follows from [31, 4.7] that σ is surjective, so we have an exact sequence

$$1 \longrightarrow C(v) \longrightarrow N(v) \xrightarrow{\sigma} (\mathbb{Z}/e\mathbb{Z})^\times \longrightarrow 1, \tag{11}$$

by which the group $(\mathbb{Z}/e\mathbb{Z})^\times$ permutes the eigenspaces of v in $\bar{V}$. The following fact is used implicitly in [31].

Lemma 3.5 *If $v \in W$ is regular, then $(\mathbb{Z}/e\mathbb{Z})^\times$ freely permutes the regular eigenspaces of v.*

Proof: Let $E \subset \bar{V}$ be an eigenspace for v containing a regular vector, and suppose $n \in N(v)$ preserves E. Since v is a scalar on E, the commutator $[n, v]$ fixes E pointwise. Therefore $[n, v]$ fixes a regular vector, so $[n, v] = 1$. ∎

Returning to the proof of Prop. 3.4, we have $w \in W$ of order d with eigenvalue ζ and $w = v^{e/d}$ where $v \in W$ has characteristic polynomial $\Phi_e(t)$ and $d \mid e$. We also have $\zeta = \eta^{e/d}$, where η is an eigenvalue of v. Let Δ be the kernel of the natural map $(\mathbb{Z}/e\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/d\mathbb{Z})^\times$. The sequence (11) restricts to another exact sequence

$$1 \longrightarrow C(v) \longrightarrow N(v) \cap C(w) \xrightarrow{\sigma} \Delta \longrightarrow 1. \qquad (12)$$

Since v is regular with eigenvalues of multiplicity one, Lemma 3.5 implies that the group Δ freely permutes the eigenlines of v in $\bar{V}$. On the other hand, the eigenvalues of v in $\bar{V}(w, \zeta)$ are η^i, where $i \in \Delta$. Hence $\dim \bar{V}(w, \zeta) = |\Delta|$, so Δ is transitive on the v-eigenlines in $\bar{V}(w, \zeta)$. This shows that $N(v) \cap C(w)$ is irreducible on $\bar{V}(w, \zeta)$. ∎

3.2 An equivalence relation

Fix a cyclotomic element $w \in W$. The $\mathbb{Q}$-algebra $K = \mathbb{Q}(w) \subset \mathrm{End}(V)$ is a field. Let V_K be the abelian group V viewed as a vector space over K. Every $\alpha \in R$ spans a K-line $K\alpha = \{f(w)\alpha : f \in \mathbb{Q}[t]\}$ in V_K. We say that two roots $\alpha, \beta \in R$ are *K-equivalent* if $K\alpha = K\beta$. This is an equivalence relation on R. For each K-equivalence class $S \subset R$, the rational span $\mathbb{Q}S$ is contained in $K\alpha$ for any $\alpha \in S$. Conversely, since $w\alpha$ is K-equivalent to α for any $\alpha \in S$, we have $KS \subset K\alpha$. This shows that $\mathbb{Q}S = K\alpha$ for any root $\alpha \in S$. We also note that

$$S = R \cap \mathbb{Q}S. \qquad (13)$$

Equation (13) implies that S is a root subsystem in R, of rank equal to the degree of K over $\mathbb{Q}$. Let $A(S)$ and $W(S)$ denote the automorphism and Weyl groups of S, respectively. Then $W(S)$, being generated by reflections from S, is a subgroup of $W = W(R)$. However, the group $A(S)$ need not be contained in $A(R)$. For each K-equivalence class $S \subset R$, the subgroup

$$C_S(w) := W(S) \cap C(w)$$

consists of the K-linear elements of $W(S)$. If $r \in C_S(w)$ and $\alpha \in S$ then $r \cdot \alpha = \eta_S(r)\alpha$ for some scalar $\eta_S(\alpha) \in K^\times$ which is independent of α. This defines an injective homomorphism

$$\eta_S : C_S(w) \longrightarrow K^\times. \qquad (14)$$

It follows that the group $C_S(w)$ is cyclic, of order dividing the number of roots of unity in $K^\times$.

The orthogonal form $\langle\ ,\ \rangle$ on V gives rise to a hermitian form $h(x,y)$ on V_K characterized by the identity

$$\langle ax, y\rangle = \mathrm{tr}(ah(x,y)), \qquad \text{for all } a \in K,$$

where $\mathrm{tr} : K \to \mathbb{Q}$ is the trace. If L is a K-line in V then the orthogonal complements of L with respect to $\langle\ ,\ \rangle$ and h coincide as $\mathbb{Q}$-subspaces of V. Let $U(V_K,h)$ be the unitary group of the form h on V_K. The centralizer $C(w)$ consists of the elements in W which act K-linearly on V_K and we have

$$C(w) = W \cap U(V_K, h).$$

A K-*reflection* on V_K is an element $g \in U(V_K,h)$ of finite order whose fixed-point set is a K-hyperplane. A K-reflection has exactly one K-eigenvalue $\eta \neq 1$ and $\eta = \det(w|V_K)$ is a root of unity in $K^\times$.

Lemma 3.6 *Any nontrivial element $r \in C_S(w)$ is a K-reflection with nontrivial K-eigenvalue $\eta = \eta_S(r)$, pointwise-fixing K-hyperplane orthogonal to S with respect to h, having the formula*

$$r(x) = x - (1-\eta)\frac{h(x,\alpha)}{h(\alpha,\alpha)}\alpha, \tag{15}$$

for any $\alpha \in S$.

Proof: Since $r \in W(S)$, it pointwise-fixes the $\langle\ ,\ \rangle$-orthogonal complement of $\mathbb{Q}S$ which coincides with the h-orthogonal complement of the K-line $KS = \mathbb{Q}S$. Since $r \in U(V_K,h)$, it follows that r is a K-reflection. We have seen that η is a non-trivial eigenvalue of r occurring in the K-line KS. Since the right side of (15) also pointwise fixes the orthogonal complement of KS and acts by the scalar η on KS, it must agree with $r(x)$. ∎

Lemma 3.7 *Every K-reflection $r \in C(w)$ is contained in $C_S(w)$ for a unique K-equivalence class $S \subset R$.*

Proof: Let L be the nontrivial K-eigenline of r. Then the fixed-point set of r in V_K is the orthogonal complement L' of L with respect to h. As $\mathbb{Q}$-vector spaces, L' is also the $\langle\ ,\ \rangle$-orthogonal complement L. The subgroup W' of W fixing L' pointwise is generated by reflections about the roots orthogonal to L' [3, V.3 Prop.2]. The set S of these roots is non-empty, since $1 \neq r \in W'$. Since $S \subset L$, it follows that S is a K-equivalence class and $r \in C_S(w)$. Uniqueness follows from equation (13). ∎

Proposition 3.8 *If $w \in W$ is cyclotomic then $C(w)$ is generated by the cyclic subgroups $C_S(w)$, with S ranging over the K-equivalence classes in R.*

Proof: The centralizer $C(w)$ preserves each eigenspace of w in $\bar{V}$. Hence for every eigenvalue ζ of w we have a representation

$$\pi_\zeta : C(w) \longrightarrow GL(\bar{V}(w,\zeta))$$

on the ζ-eigenspace $\bar{V}(w,\zeta)$ of w in $\bar{V}$. Since $\bar{V}(w,\zeta)$ contains a regular vector, the map π_ζ is injective. By Springer's results [31, 4.2,6.4], the image of π_ζ is generated by reflections.

The eigenspace $\bar{V}(w,\zeta)$ is defined over K, hence every reflection in the image of π_ζ has its nontrivial eigenvalue in K. Embedding $K \subset \bar{\mathbb{Q}}$ via $w \to \zeta$, we have a $C(w)$-equivariant isomorphism

$$\bar{\mathbb{Q}} \otimes_K V_K \xrightarrow{\sim} \bar{V}(w,\zeta)$$

sending $v \in V_K$ to $\sum_{k=1}^{d} \zeta^{-k} w^k v$. Hence π_ζ maps the K-reflections in $C(w)$ bijectively onto the reflections in $\pi_\zeta\,(C(w))$. The result follows. ∎

S_1	w_1	e	ℓ
A_1	A_1	2	1
A_{p-1}	$A_{p-1},\ -A_{p-1}$	$p,\ 2p$	$1,\ 2$
B_{2^r}, C_{2^r}	B_{2^r}	2^{r+1}	1
$D_{2^r},\ r \geq 2$	B_{2^r}	2^{r+1}	2
D_4	F_4	12	3
E_6	$E_6(a_1),\ -E_6(a_1)$	$9,\ 18$	$1,\ 2$
E_8	$E_8,\ E_8(a_1),\ E_8(a_2),\ E_8(a_5)$	$30,\ 24,\ 20,\ 15$	1
F_4	$F_4,\ B_4$	$12,\ 8$	1
G_2	$G_2,\ A_2$	$6,\ 3$	1

Table 2: Possible root systems S_1 and automorphisms $w_1 \in A(S_1)$

3.3 The possible equivalence classes

We next tabulate the possibilities for a K-equivalence class in $S \subset R$, where $K \subset \mathrm{End}(V)$ is the field generated over $\mathbb{Q}$ by a nontrivial cyclotomic element $w \in W$. This will allow us to verify that $C_S(w)$ is nontrivial. Let $d > 1$ be the order of w.

By the definition of K-equivalence, we have $wS = S$. Thus, w acts on the root system S via an automorphism $w_S \in A(S)$ having characteristic polynomial $\Phi_d(t)$ on $\mathbb{Q}S$. This implies that the group generated by w_S acts transitively on the irreducible components $S_1, \cdots, S_c$ of S, that $c \mid d$, and that $w_S^c = (w_1, \cdots, w_c)$, for certain elements $w_i \in A(S_i)$.

The possibilities for S_1 are given in Table 2, using the notation of [6] for conjugacy-classes in Weyl groups, extended to $A(R)$ in the obvious way. We set $e := d/c$; this is the order of w_1 in $A(S_1)$. In the last column we give the order ℓ of w_1 in the quotient group $A(S_1)/W(S_1)$. In the second row p is a prime ≥ 3.

To arrive at Table 2 we first observe that on the $\mathbb{Q}$ vector space $\mathbb{Q}S$, the element w_S^c has characteristic polynomial

$$\det(tI - w_S^c) = \Phi_e(t)^{\phi(d)/\phi(e)} = \prod_{i=1}^{c} \det(tI - w_i), \tag{16}$$

where $\det(tI - w_i)$ is the characteristic polynomial of w_i on $\mathbb{Q}S_i$. By the transitivity of w_S on the S_i, there is an integer $m \geq 1$ such that

$$\det(tI - w_i) = \Phi_e(t)^m$$

for all i. Comparing degrees in (16), we find that

$$\phi(ce) = \phi(d) = m \cdot c \cdot \phi(e). \tag{17}$$

But equation (17) can only hold if $m = 1$ and every prime dividing d also divides e. It follows that S_1 is an irreducible root system of rank $\phi(e)$ admitting an automorphism w_1 with characteristic polynomial $\det(tI - w_1) = \Phi_e(t)$, such that $\phi(e) \mid \phi(d)$. These constraints lead to Table 2.

Corollary 3.9 *For each K-equivalence class $S \subset R$, the group $C_S(w)$ is nontrivial.*

Proof: Recall that $w_S \in A(S)$ is the automorphism of S induced by w. If $w_S^\nu \in W(S)$ for some $\nu \geq 1$ then w_S^ν acts trivially on the orthogonal complement of $\mathbb{Q}S$ and acts on $\mathbb{Q}S$ as w^ν. Hence w_S^ν commutes with w on V, so that $w_S^\nu \in C_S(w)$.

Therefore it suffices to show that $w_S^{c\ell} \neq 1$. If $w_S^{c\ell} = 1$, then $w_1^\ell = 1$, which implies $e \mid \ell$. But according to Table 2, this does not happen. ■

Corollary 3.10 *The subgroup of $C(w)$ generated by the subgroups $C_S(w)$ as S ranges over the K-equivalence classes containing a short root of R acts irreducibly on V_K.*

Proof: From the transitivity of W on roots of a given length [3, VI.1 Prop 11], it follows that for any two short roots $\alpha, \beta \in R$, there is a sequence

$$\alpha = \alpha_0,\ \alpha_1,\ \ldots\ ,\ \alpha_k = \beta \tag{18}$$

of short roots in R such that $\langle \alpha_i, \alpha_{i+1} \rangle \neq 0$ for $0 \leq i < k$.

The hermitian form $h(x, y)$ satisfies $T\left(h(x, y)\right) = \langle x, y \rangle$. It follows the sequence (18) also satisfies $h(\alpha_i, \alpha_{i+1}) \neq 0$ for $0 \leq i < k$.

Now suppose $U \subset V_K$ is a nonzero K-subspace preserved all the groups $C_S(w)$ where S contains a short root. Take a nonzero element $x \in U$. Since the short roots span V, there is $\alpha \in R$ such that $\langle x, \alpha \rangle \neq 0$. Let S be the K-equivalence class containing α. By Cor. 3.9, there is a nontrivial K-reflection $r_S \in C_S(w)$, given by the formula

$$r_S(x) = x - (1 - \eta)\frac{h(x, \alpha)}{h(\alpha, \alpha)}\alpha,$$

where $1 \neq \eta \in \bar{\mathbb{Q}}^\times$. Since $T\left(h(x, \alpha)\right) = \langle x, \alpha \rangle \neq 0$, this shows that $\alpha \in U$. Let $\beta \in R$ be an arbitrary short root, and choose a sequence as in (18). Repeating the previous argument with x, α replaced by α, α_1 shows that $\alpha_1 \in U$. In this way, we see that $\beta \in U$. Hence all short roots are contained in U, so $U = V$. ■

One more consequence of Table 2 will be useful for our study of cyclotomic classes in E_8.

Corollary 3.11 *Suppose $w \in A(R)$ is cyclotomic of even square-free order d. Then one of the following holds.*

1. $w = -1$;
2. $R = G_2$ *or* E_8 *and* w *is a Coxeter element;*
3. $d = 2p$, *where* $p \in \{3, 5\}$. *Each K-equivalence class S has type A_{p-1}, $C_S(w)$ is generated by a Coxeter element in $W(S)$ and there are $|R|p^{-1}$ reflections in $C(w)$, each of order p.*

Proof: Since d is square-free and e contains every prime divisor of d, we must have $e = d$, so $c = 1$ and each $S = S_1$ is irreducible. The third column of Table 2 gives the asserted possibilities for S. ■

3.4 Cyclotomic structures on the E_8 root lattice

In this section $W = W(E_8)$ is the Weyl group of the root system R of type E_8 and $X = \mathbb{Z}R$ is the E_8 root lattice. Cyclotomic $\mathbb{Z}[\zeta_d]$-structures on X for $d = 3$ and 4 were known in the 19th century [8]. Recent literature on lattice theory [2] mentions the $\mathbb{Z}[\zeta_{15}]$-structure on X. All of these, and other cyclotomic structures on X arise from cyclotomic elements in W. In fact there is exactly one cyclotomic class in W of every order

$$d \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30\}.$$

In this section we determine the K-equivalence classes S and the orders of the subgroups $C_S(w)$ for each class of cyclotomic elements $w \in W$. We thereby find the number N of reflections in $C(w)$, along with its Shephard-Todd classification. Since $N = \sum(d_i - 1)$, where the d_i are the degrees of $C(w)$, we can compare our results with those of Springer [31]. We ignore the classes of odd order d, since their negatives have the same centralizer. If $d = 2$ then $w = -1$, so $C(w) = W$. If $d \in \{20, 24, 30\}$, we have $[K : \mathbb{Q}] = \phi(d) = 8$ so $S = R$ and $C(w) = \langle w \rangle$. The nontrivial cases are as follows.

3.4.1 $d = 4$

Here w belongs to the class $D_4(a_1)^2$ and $w^2 = -1$. This implies that $\langle \alpha, w\alpha \rangle = 0$ for all $\alpha \in R$. Hence all K-equivalence classes have type A_1^2 and $C_S(w) = \langle w_S^2 \rangle$ has order two. There are $240/4 = 60$ K-equivalence classes, each contributing a single K-reflection to $C(w)$, so $N = 60$. We note that $60 = 7 + 11 + 19 + 23$, in accordance with [31].

3.4.2 $d = 6$

Here w belongs to the class $E_8(a_8)$. By Lemma 3.11, there are 40 K-equivalence classes S, each of type A_2, and each $C_S(w)$ is cyclic of order three, giving a total of $N = 80$ K-reflections in W_K. The roots in S are the vertices of a planar hexagon and form a single orbit under $\langle w \rangle$ (cf. section A.3 below). We note that $80 = 11 + 17 + 23 + 29$, in accordance with [31]. [1]

3.4.3 $d = 10$

Here w belongs to the class $E_8(a_6)$. By Lemma 3.11, there are 12 K-equivalence classes S, each of type A_4, consisting of two w-orbits. Each $C_S(w)$ is cyclic of order five, generated by a Coxeter element in $W(S)$, giving a total of $N = 48$ K-reflections in $C(w)$. We note that $48 = 19 + 29$, in accordance with [31].

3.4.4 $d = 8$

Here w belongs to the class $D_8(a_3)$ and $w^4 = -1$. We have $c\phi(e) = \phi(8) = 4$. Table 2 implies that S has type A_1^4 or D_4. To analyze this dichotomy, we first make some preliminary remarks on subsystems of type

[1] In [31, 5.4], the degree $d_4 = 30$ is omitted by mistake in the row for $d = 6$ but it appears in the row for $d = 3$, which has the same centralizer.

A_1^4 in R, which we call *tetrads*. We say that a tetrad $T = \pm\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$ is *even* if $\alpha_0+\alpha_1+\alpha_2+\alpha_3 \in 2X$, and T is *odd* otherwise. In [6, Lemma 11], Carter proves:

Lemma 3.12 *Let R be a root system of type E_8 with Weyl group W. The even and odd tetrads in R each form a single orbit under W. The even tetrads are precisely those which are contained in a subsystem of type D_4.*

Return now to our cyclotomic element $w \in W$ of order $d = 8$. Every K-equivalence class S contains a unique w-stable tetrad. This is clear if $S \simeq A_1^4$ is itself a tetrad. If $S \simeq D_4$, then w, having order eight, must act on S as a Coxeter element $w_S \in W(B_4)$. It follows that are three w-orbits on S. It is easy to check that these orbits are classified by the value of $\langle\alpha, w\alpha\rangle \in \{-1, 0, +1\}$. The orbit $\{\alpha \in S : \langle\alpha, w\alpha\rangle = 0\}$ is the unique w-stable tetrad in S. Let us define

$$\varsigma := 1 + w + w^{-1} \in \mathrm{End}(V).$$

If $\beta \in S$ satisfies $\langle\beta, w\beta\rangle = -1$, then $\langle\varsigma\beta, w\varsigma\beta\rangle = +1$. Hence the w-orbits in S are represented by $\{\alpha, \beta, \varsigma\beta\}$ for any choice of roots α, β in S such that $\langle\alpha, w\alpha\rangle = 0$, $\langle\beta, w\beta\rangle = -1$.

To count the K-equivalence classes of each type, we must look at the roots in a more explicit way. As in [3], the roots of R are the vectors

$$e_i \pm e_j, \qquad \tfrac{1}{2}\sum c_i e_i,$$

in $\mathbb{R}^8$, where $1 \le i \ne j \le 8$ and $c_i \in \{\pm 1\}$ with $\prod c_i = +1$. The pairing $\langle\ ,\ \rangle$ is then the usual dot product on $\mathbb{R}^8$. For visual clarity, we use an abbreviated notation for roots of the form $\frac{1}{2}\sum c_i e_i$, as in the following example:

$$\tfrac{1}{2}(1,-1,-1,1,1,-1,1,-1) = [+--+\mid +-+-].$$

The roots of the form $e_i \pm e_j$ comprise a root subsystem R' of R of type D_8. We choose $w \in W(R')$ such that

$$w : e_1 \mapsto e_2 \mapsto e_3 \mapsto e_4 \mapsto -e_1, \quad e_5 \mapsto e_6 \mapsto e_7 \mapsto e_8 \mapsto -e_5.$$

Using the criteria in 3.12, we find there are 18 w-stable tetrads in R; twelve of these tetrads are odd and six of them are even. The twelve K-equivalence classes $S \simeq A_1^4$ are the w-orbits through the following twelve roots α:

$$\begin{array}{cc} e_1 \pm e_6, & e_1 \pm e_8, \\ [++++\mid \pm\mp\pm\mp], & [\pm\mp\pm\mp \mid ++++], \\ [++++\mid \pm\mp\mp\pm], & [\pm\mp\mp\pm \mid ++++]. \end{array} \tag{19}$$

The six K-equivalence classes $S \simeq D_4$ are each the union of three w-orbits, through $\alpha, \beta, \varsigma\beta$, with $\langle\alpha, w\alpha\rangle = 0$, $\langle\beta, w\beta\rangle = -1$, as shown:

α	β	$\varsigma\beta$
$e_1 - e_3$:	$e_1 - e_2$	$-e_3 - e_4$
$e_5 - e_7$:	$e_5 - e_6$	$-e_7 - e_8$
$e_1 \pm e_5$:	$[+-+-\mid \pm\mp\pm\mp]$	$[++--\mid \pm\pm\mp\mp]$
$e_1 \pm e_7$:	$[+-+-\mid \mp\pm\pm\mp]$	$[++--\mid \pm\pm\pm\pm]$

If $S = 4A_1$ is a tetrad, then $C_S(w) = \{\pm 1\}$ has order two. If $S = D_4$, then $C_S(w) = \langle w_S^2 \rangle$ has order four. Thus, there are $N = 12 \cdot 1 + 6 \cdot 3 = 30$ reflections in $C(w)$. We note that $30 = 7 + 23$, in accordance with [31].

The determinant $\det : U(V_K, h) \to K^\times$ maps $C(w)$ onto $\langle w^2 \rangle$, with kernel $C(w)_1 = C(w) \cap SU(V_K, h) = \tilde{O}$, the binary octahedral group, which contains the binary tetrahedral group $\tilde{T} = Q_8 \cdot 3$ with index two. Thus, $C(w) = \langle w \rangle \cdot \tilde{O}$. The six reflections of type A_1^4 are the elements $w^2 \cdot \{\pm i, \pm j, \pm k\} \subset w^2 \cdot Q_8$. The twelve reflections of order four are the elements $\pm w \cdot x$ where $x \in \tilde{O} - \tilde{T}$ has an eigenvalue equal to $\pm w^{-1}$ on V_K.

3.4.5 $d = 12$

Here w belongs to the class $E_8(a_3)$. We have $c\phi(e) = \phi(12) = 4$. Using Table 2 we find two possibilities for a K-equivalence class: $S = A_2^2$ or $S = D_4$. This time, the orbit-invariant

$$\langle \alpha, w\alpha \rangle \in \{-1, 0, +1\}$$

determines the isomorphism type of S. Indeed, for any $\alpha \in R$, the relation $w^4 - w^2 + 1 = 0$ implies that

$$\langle \alpha, w^2\alpha \rangle = 2 + \langle \alpha, w^4\alpha \rangle.$$

Since $w^2\alpha \neq \alpha \neq -w^4\alpha$ we must have $\langle \alpha, w^2\alpha \rangle = 1$. Writing the relation as $w^3 - w + w^{-1} = 0$ shows that

$$\langle \alpha, w^3\alpha \rangle = \langle \alpha, w\alpha \rangle - \langle \alpha, w^{-1}\alpha \rangle = 0.$$

If $\langle \alpha, w\alpha \rangle = 0$ then S contains, hence coincides with A_2^2 and has root basis

$$\{\alpha, -w^2\alpha\} \cup \{w\alpha, -w^3\alpha\}$$

for the two A_2 components. Hence $|S| = 12$ and consists of a single w-orbit. We have $c = 2$ and w^2 acts as the graph automorphism on each component of S. The group $C_S(w) = \langle w_S^4 \rangle$ has order three.

If $\langle \alpha, w\alpha \rangle = 1$ then $S = D_4$ with root basis

$$\{w\alpha - \alpha, \quad w^2\alpha - w\alpha, \quad w\alpha - w^3\alpha, \quad \alpha - w^2\alpha + w^3\alpha\},$$

where $w^2\alpha - w\alpha$ corresponds to the branch node. Now $|S| = 24$ so S consists of two w-orbits. The orbit not containing α satisfies $\langle \beta, w\beta \rangle = -1$. Here w_S is a Coxeter element in $W(F_4) = A(D_4)$, whose image in $A(D_4)/W(D_4)$ is a triality. The group $C_S(w) = \langle w_S^3 \rangle$ has order four.

We can count the number of K-equivalence classes of each type, by invoking Springer's results instead of verifying them. Let a and b be the number of K-equivalence classes of type $2A_2$ and D_4, respectively. Counting w-orbits in each type, we have one equation. $a + 2b = 240/12 = 20$. On the other hand, The degrees of E_8 are $2, 8, 12, 14, 18, 20, 24, 30$, so by [31] the degrees of $C(w)$ are $12, 24$, and there are $N = 11 + 23 = 34$ reflections in $C(w)$. Counting the number of reflections in each group $C_S(w)$, we get a second equation$2a + 3b = 34$. It follows that $a = 8$ and $b = 6$.

Table 3 summarizes the cases where $W \neq C(w) \neq \langle w \rangle$. Row "number of S" gives the number of K-equivalence classes S of each type. Row "N" gives the number of reflections in $C(w)$ of each order. For example, when $d = 8$ there are 18 reflections of order two and 12 reflections of order four. The last row gives the label for $C(w)$ according to the Shephard-Todd classification [29].

d :	4	3, 6	8	5, 10	12
class	$D_4(a_1)^2$	$A_2^4,\ E_8(a_8)$	$D_8(a_3)$	$A_4^2,\ E_8(a_6)$	$E_8(a_3)$
$\|C(w)\|$:	$8{\cdot}12{\cdot}20{\cdot}24$	$12{\cdot}18{\cdot}24{\cdot}30$	$8 \cdot 24$	$20 \cdot 30$	$12 \cdot 24$
$\dim V_K$	4	4	2	2	2
type of S	$2A_1$	A_2	A_1^4, D_4	A_4	A_2^2, D_4
$\|C_S(w)\|$	2	3	2, 4	5	3, 4
number of S	60	80	12, 6	12	8, 6
N	2^{60}	3^{80}	$2^{18}4^{12}$	5^{48}	$2^6 3^{16} 4^{12}$
ST number	31	32	9	16	10

Table 3: Reflection groups $C(w)$ for cyclotomic $w \in W(E_8)$

4 Coinvariants of cyclotomic lattices

Return to a general irreducible root system R with Weyl group W and root lattice $X = \mathbb{Z}R$. For any elliptic $w \in W$, with coinvariants $X_w = X/(1-w)X$, we have $|X_w| = \det(1-w)$, but this does not determine the abelian group X_w completely. However, if w is cyclotomic, the group X_w has a simple description:

Lemma 4.1 *Suppose $w \in W$ is cyclotomic of order d. If d is not a prime power, then $X_w = 0$. If d is a power of a prime p, then X_w is a vector space over $\mathbb{F}_p$ of dimension $n/\phi(d)$, where $n = \dim V$.*

Proof: This follows from the elementary fact that $\Phi_d(1) = 1$ unless d is a power of a prime p, in which case $\Phi_d(1) = p$. Since $m = \Phi_d(1)$ kills X_w, this proves the Lemma. ■

More suggestively, suppose that w is cyclotomic of order d a power of a prime p. Then $\mathfrak{O} = \mathbb{Z}[w]$ is the ring of integers in the cyclotomic field $K = \mathbb{Q}(w) \subset \mathrm{End}(V)$. The ideal $\mathfrak{P} = (1-w)\mathfrak{O}$ is the unique prime ideal in $\mathfrak{O}$ ramified over $\mathbb{Z}$ and we have $p\mathfrak{O} = \mathfrak{P}^{\phi(d)}$ and $\mathfrak{O}/\mathfrak{P} \simeq \mathbb{F}_p$. Let $X_{\mathfrak{O}}$ be the abelian group X, viewed as an $\mathfrak{O}$-module. Then we have $X_w = X_{\mathfrak{O}}/\mathfrak{P}X_{\mathfrak{O}}$, showing that X_w is the reduction modulo p of the $\mathfrak{O}$-lattice $X_{\mathfrak{O}}$. The hermitian form $h(x,y)$ on V_K is $\mathfrak{O}$-valued on $X_{\mathfrak{O}}$, and we have $h(x,y) \equiv \langle x, y\rangle_w \mod \mathfrak{P}$.

4.1 Elliptic trialities

It is convenient to give the name *triality* to any group element of order three. This is the smallest order of an interesting elliptic element $w \in W$.

One can classify elliptic trialities as follows. An elliptic triality $w \in W$ is necessarily cyclotomic: its minimal polynomial is $M(t) = t^2 + t + 1$ and its characteristic polynomial is $\det(tI - w) = (t^2 + t + 1)^k$, where $2k$, the rank of R, must be even. Since w is cyclotomic, it is regular, so there is at most one W-conjugacy class of elliptic trialities in W, by [31, 4.2]. The connection index $f = [P(R) : Q(R)]$ divides $\det(1-w)$, hence must be a power of 3. It follows that R has one of the types A_2, G_2, F_4, E_6, E_8. Elliptic trialities exist in each of these cases: the prime 3 divides the Coxeter number and does not divide any exponent, so for any Coxeter element $v \in W$, the element $w = v^{h/3}$ is an elliptic triality (cf. Lemma 3.2).

R	$\|C_A(w)\|$	$Sp(X_w)$	$\|Sp(X_w)\|$
A_2	$2 \cdot 3$	$\mathbb{F}_3^\times$	$3-1$
G_2	6	$\mathbb{F}_3^\times$	$3-1$
F_4	$6 \cdot 12$	$SL_2(3)$	$3(3^2-1)$
E_6	$2 \cdot 6 \cdot 9 \cdot 12$	$\left[\mathbb{F}_3^\times \times SL_2(3)\right] \ltimes \mathbb{F}_3^2$	$2 \cdot 3^3(3^2-1)$
E_8	$12 \cdot 18 \cdot 24 \cdot 30$	$Sp_4(3)$	$3^4(3^4-1)(3^2-1)$

Table 4: The coinvariant representation for elliptic trialities

By Lemma 4.1, the coinvariant group X_w is a vector space over $\mathbb{F}_3$ of dimension equal to half the rank of R. Since $3 = (1-w)(2+w)$, we have $\dot{M}(t) = 2 + t$ and the corresponding symplectic form on X_w is given by

$$\langle \rho_\lambda, \rho_\mu \rangle_w = \langle \lambda, (2+w)\mu \rangle \mod 3,$$

in the notation of section 2.1.

The order of $C(w)$ is the product of the degrees of W which are divisible by 3. Multiplying by $[A : W]$ gives the order of the centralizer $C_A(w)$ of w in the automorphism group A of R. These are given in Table 4, along with a concrete description of the group $Sp(X_w)$ and its order.

In each case, we have

$$|C_A(w)| = 3|Sp(X_w)|. \tag{20}$$

This suggests the following result.

Proposition 4.2 *If w is an elliptic triality then the coinvariant representation $\varrho_w : C_A(w) \to Sp(X_w)$ is a surjective three-fold covering with kernel generated by w.*

Proof: In view of (20), it suffices to prove that the kernel of ϱ_w is generated by w. We require two lemmas.

Lemma 4.3 *Suppose $w \in W$ is an elliptic triality, let $\lambda \in X$ and set $\delta = (1-w)\lambda$. Then*

$$2\langle w\lambda, \lambda \rangle = -\langle \lambda, \lambda \rangle \qquad \textit{and} \qquad \langle \delta, \delta \rangle = 3\langle \lambda, \lambda \rangle \in 3\mathbb{Z}.$$

Proof: Since $w + w^{-1} = -1$, we have

$$2\langle w\lambda, \lambda \rangle = \langle w\lambda, \lambda \rangle + \langle \lambda, w^{-1}\lambda \rangle = \langle w\lambda, \lambda \rangle + \langle w^{-1}\lambda, \lambda \rangle = -\langle \lambda, \lambda \rangle.$$

It follows that

$$\langle \delta, \delta \rangle = \langle (1-w)\lambda, (1-w)\lambda \rangle = 2\langle \lambda, \lambda \rangle - 2\langle w\lambda, \lambda \rangle = 3\langle \lambda, \lambda \rangle \in 3\mathbb{Z},$$

as claimed. ∎

Lemma 4.4 *Suppose $\alpha, \beta \in R$ are short roots. Let $w \in W$ be an elliptic triality, and suppose α, β have the same class in X_w. Then $\beta = w^i\alpha$ for some $i = 0, 1, 2$.*

Proof: Our normalization (**??**) implies that $\langle\alpha,\alpha\rangle = \langle\beta,\beta\rangle = 2$. We are assuming the element $\delta = \alpha - \beta$ vanishes in X_w, so there is $\lambda \in X$ such that

$$\delta = (1-w)\lambda, \tag{21}$$

and we can apply Lemma 4.3:

$$\langle\delta,\delta\rangle = 3\langle\lambda,\lambda\rangle, \qquad 2\langle w\lambda,\lambda\rangle = -\langle\lambda,\lambda\rangle.$$

On the other hand, since $\delta = \alpha - \beta$, we have

$$\langle\delta,\delta\rangle = 4 - 2\langle\alpha,\beta\rangle \in 3\mathbb{Z}. \tag{22}$$

Since $\langle\alpha,\beta\rangle \in \mathbb{Z}$, [3, VI.1.3] implies

$$\langle\alpha,\beta\rangle \in \{0,\pm1,\pm2\}.$$

However, equation (22) limits the possibilities to

$$\langle\alpha,\beta\rangle \in \{-1,2\}.$$

If $\langle\alpha,\beta\rangle = 2$ then $\alpha = \beta$. Hence from now on we assume $\langle\alpha,\beta\rangle = -1$, which means

$$\langle\delta,\delta\rangle = 6, \qquad \text{and} \qquad \langle\lambda,\lambda\rangle = 2.$$

But a vector in X of norm equal to that of a short root is itself a root [Kac [19, Prop. 5.10 a)]. Thus, λ is also a short root and we have

$$\langle w\lambda,\lambda\rangle = -\tfrac{1}{2}\langle\lambda,\lambda\rangle = -1.$$

This implies that

$$\langle\lambda,\alpha\rangle - \langle\lambda,\beta\rangle = \langle\lambda,\delta\rangle = \langle\lambda,(1-w)\lambda\rangle = \langle\lambda,\lambda\rangle - \langle\lambda,w\lambda\rangle = 3.$$

But λ,α,β are roots of the same length, so as above, we have

$$\langle\lambda,\alpha\rangle,\ \langle\lambda,\beta\rangle \in \{0,\pm1,\pm2\}.$$

Since $\langle\lambda,\alpha\rangle - \langle\lambda,\beta\rangle = 3$, there are two possibilities:

$$\langle\lambda,\alpha\rangle = 2 \quad \text{and} \quad \langle\lambda,\beta\rangle = -1, \tag{23}$$

or

$$\langle\lambda,\alpha\rangle = 1 \quad \text{and} \quad \langle\lambda,\beta\rangle = -2. \tag{24}$$

The first possiblity (23) implies that $\lambda = \alpha$, so (21) reads as

$$\alpha = \beta + (1-w)\alpha,$$

that is,

$$\beta = w\alpha.$$

Likewise, the second possibility implies that $\alpha = w\beta$. The lemma is proved. ■

Now we can prove Prop. 4.2. Suppose that $u \in C_A(w)$ acts trivially on X_w. Then for every short root $\alpha \in R$, the roots α and $u\alpha$ have the same image in X_w. Lemma 4.4 implies that α and $u\alpha$ are in the same w-orbit. Hence u preserves each K-equivalence class S containing a short root in R, where K is the subfield of $\mathrm{End}(V)$ generated by w. This means that u preserves the K-line in V_K through S. It follows that u commutes with $C_S(w)$. The short roots span V, so u has all of its eigenvalues in K. But the subgroup of $C(w)$ generated by the $C_S(w)$ for S containing a short root is irreducible on V_K, by Cor. 3.10. Hence u acts on V_K by a scalar in K. The roots of unity in K are generated by $-w$. Since -1 acts nontrivially on X_w, we see that $u \in \langle w\rangle$, as claimed. ■

We have shown that for any elliptic triality, the coinvariant representation ϱ_w gives an exact sequence

$$1 \longrightarrow \langle w\rangle \longrightarrow C_A(w) \longrightarrow Sp(X_w) \longrightarrow 1. \tag{25}$$

If $R \neq E_6$, the dimension of V_K is not divisible by 3, so the subgroup $C_A(w)'$ of $C_A(w)$ of determinant one on V_K is a complement to $\langle w\rangle$ and we have

$$C_A(w) = \langle w\rangle \times Sp(X_w).$$

All elliptic trialities may be seen in E_8: for $R = G_2, F_4, E_6, E_8$, let us write $C_R(w) = C_{A(R)}(w)$. If $w \in W(E_8)$ is an elliptic triality, then we can write $w = xyz$, where

$$x \in W(G_2), \quad xy \in W(F_4) \subset W(E_6)$$

are elliptic trialities in the respective groups and

$$C_{G_2}(x) = C_{G_2}(w), \quad C_{F_4}(xy) = C_{F_4}(w), \quad C_{E_6}(xy) = C_{E_6}(w).$$

Since $w \notin C_{E_6}(w)$, the projection of $C_{E_8}(w)$ into $Sp(X_w) = Sp_4(3)$ is injective on the groups $C_R(w)$, for $R = G_2, F_4, E_6$. Their images give the following chain of algebraic subgroups of $Sp_4(3)$ (with respect to a basis of X_w making the matrix of the form $\langle\ ,\ \rangle_w$ antidiagonal):

$$\begin{array}{ccccccc}
C_{G_2}(w) & \subset & C_{F_4}(w) & \subset & C_{E_6}(w) & \subset & C_{E_8}(w) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \subset & \begin{bmatrix} 1 & 0 & 0 & * \\ 0 & * & * & 0 \\ 0 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \subset & \begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & * \end{bmatrix} & \subset & Sp_4(3).
\end{array}$$

Here $*$ represents arbitrary independent elements of $\mathbb{F}_3$ such that the indicated matrix preserves the form $\langle\ ,\ \rangle_w$. Hence, for $R = E_6$, the sequence (25) does not split. We will revisit elliptic trialities in section A.

4.2 Cyclotomic centralizers and coinvariants for E_8

In this section we analyze the coinvariant representations for the remaining cyclotomic classes in type E_8. Recall that there is exactly one W-conjugacy class of cyclotomic elements in W for each order $d \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30\}$. To be elliptic, we of course need $d \geq 2$. The case $d = 2$ is well-known (cf. the introduction) and $d = 3$ was covered in the previous section. Henceforth we only consider $d \geq 4$. We ignore $d = 6, 10$ since $X_w = 0$ and $-w$ has the same centralizer with $X_{-w} \neq 0$. We also ignore those d where $C(w) = \langle w \rangle$, since there is nothing to say in these cases. For $d = 12$ we have $|C(w)| = 288$ but $X_w = 0$. See, however 4.2.4 for a modular interpretation of this centralizer.

What remain are $d = 4, 5, 8$. In these cases the group $Sp(X_w)$ is the isometry group of a nondegenerate symplectic form over a finite field. The following result has been proved for $d = 3$.

Proposition 4.5 *If W has type E_8 and $w \in W$ is cyclotomic of order $d \geq 3$ a prime power, then the coinvariant representation $\varrho_w : C(w) \to Sp(X_w)$ is surjective.*

We prove this by examining $d = 4, 5, 8$ separately.

4.2.1 Coinvariants for $d = 5$

This section contains the proof of Prop. 4.5 for $d = 5$. We will see that a sharper result holds:

$$C(w) = \langle w \rangle \times SL_2(5).$$

The field $K = \mathbb{Q}(w)$ is generated by fifth roots of unity and $\mathfrak{P} = (1-w)\mathfrak{O}$ is the ramified prime in the ring of integers $\mathfrak{O} = \mathbb{Z}[w]$. Let h be the invariant hermitian form on $X_{\mathfrak{O}}$, as in section 4. For any K-equivalence class $S \subset R$, the K-reflection r_S acts on $X_w = X_{\mathfrak{O}}/\mathfrak{P}X_{\mathfrak{O}} \simeq \mathbb{F}_5^2$ by

$$r_S(x) = x - h(x, \alpha)\rho_\alpha = x - \langle x, \alpha \rangle_w \rho_\alpha, \tag{26}$$

where $\alpha \in S$ and ρ_α denotes the image of α in X_w. Since the pairing $\langle \ , \ \rangle_w$ is nondegenerate on X_w, there are two roots α, β such that $\langle \rho_\alpha, \rho_\beta \rangle_w \neq 0 \mod 5$ and $\{\rho_\alpha, \rho_\beta\}$ is a basis of X_w. Letting S, T be the K-equivalence classes of α, β, the coinvariant representation is given in terms of this basis by

$$\varrho_w(r_S) = \begin{bmatrix} 1 & \langle \rho_\beta, \rho_\alpha \rangle_w \\ 0 & 1 \end{bmatrix}, \qquad \varrho_w(r_T) = \begin{bmatrix} 1 & 0 \\ \langle \rho_\alpha, \rho_\beta \rangle_w & 1 \end{bmatrix}. \tag{27}$$

Hence $\varrho_w(r_S)$ and $\varrho_w(r_T)$ generate $SL_2(5)$, proving surjectivity of ϱ_w for $d = 5$. Since $|C(w)| = 600 = 5 \cdot |SL_2(5)|$, this proves Prop. 4.5 for $d = 5$. Since w has nontrivial determinant on V_K we have $C(w) = \langle w \rangle \times Sp(X_w) = \langle w \rangle \times SL_2(5)$, as claimed.

4.2.2 Coinvariants for $d = 8$

This section contains the proof of Prop. 4.5 for the case $d = 8$, where w belongs to the cyclotomic class $D_8(a_3)$, with minimal polynomial $M(t) = t^4 + 1$. The field $K = \mathbb{Q}(w)$ is generated by the eighth roots of unity. Recall that each K-equivalence class S contains a root $\alpha \in S$ such that $\langle \alpha, w\alpha \rangle = 0$ and that

$\{\alpha, w\alpha, w^2\alpha, w^3\alpha\}$ is a tetrad. Now $\dot{M}(w) = 1 + w + w^2 + w^3$ and $S \simeq A_1^4$ or $S \simeq D_4$. By Lemma 3.12, the latter holds iff $\dot{M}(w)\alpha \in 2X$. Since $2 = (1 - w)\dot{M}(w)$, we have $S \simeq D_4$ precisely when $\alpha \in (1 - w)X$, meaning that $\rho_\alpha = 0$. So the roots in an even tetrad vanish in X_w and the roots in an odd tetrad do not vanish. The three nonzero vectors in X_w are the images of $e_1 + e_6$, $[+ + ++ \mid + - +-]$ and $[+ + ++ \mid + - -+]$. We have $h(\alpha, \alpha) = 2$ so formula (26) holds in this case as well, and the same argument shows that $\operatorname{im} \varrho_w = Sp(X_w) = SL_2(2) = S_3$.

In section 3.4.4 we saw that ϱ_w is surjective on the hyperoctahedral group $\tilde{O}$. Since Q_8 is the unique normal subgroup of $\tilde{O}$ with quotient S_3, it follows that $\ker \varrho_w$ is a central product $\langle w \rangle \cdot Q_8$ of order 32.

4.2.3 Coinvariants for $d = 4$

This section contains the proof of Prop. 4.5 for the case $d = 4$. Let $\bar{X} = X/2X$, and let $O(\bar{X})$ be the orthogonal group of the quadratic form $q = \frac{1}{2}\langle x, x\rangle \mod 2$ on $\bar{X}$. The map $W \to O(\bar{X})$ sends w to an involution $\bar{w} \in O(\bar{X})$ and the projection $X \to \bar{X}$ induces an isomorphism $\bar{X}_w \simeq X_w$ on coinvariants. Let $\bar{X}^w$ denote the invariants of w in $\bar{X}$. Since $\dim \bar{X}^w = \dim \bar{X}_w = 4$ it follows that $\bar{X}^w = (1 - w)\bar{X}$, which implies that $\bar{X}^w$ is a maximal q-isotropic subspace of $\bar{X}$. The subgroup $U \subset O(\bar{X})$ acting trivially on $\bar{X}^w$ also acts trivially on $\bar{X}_w$ and is the unipotent radical of the parabolic subgroup in $O(\bar{X})$ with Levi $GL_4(2)$. It follows that $\ker \varrho_w = \tilde{U} \cap C(w)$, where $\tilde{U}$ is the pre-image of U in W.

The centralizer $C_{O(\bar{X})}(\bar{w})$ surjects onto $Sp(\bar{X}_w)$ with kernel U, and the pre-image of $C_{O(\bar{X})}(\bar{w})$ in W is the normalizer $N(w) = \{v \in W : \ w^v = w^{\pm 1}\}$, since $w^2 = -1$. One can check that $N(w)$ preserves the form $\langle\ ,\ \rangle_w$. Hence the coinvariant representation ϱ_w extends to a surjection $N(w) \to Sp(X_w)$ with kernel $\tilde{U}$. To see that ϱ_w is surjective on $C(w)$, it remains only to show that $\tilde{U}$ is not contained in $C(w)$. This can be done by a direct computation: The element w, viewed in $W(D_8)$, is a product of four commuting B_2-Coxeter elements of the form $(ij)t_j$, where (ij) is a transposition and t_j is a sign change. One easily finds a permutation z inverting w, such that $\rho_w(z) \neq 1$, using Lemma 2.3. Thus, we have shown that ϱ_w is surjective.

It follows that $\ker \varrho_w$ has order 64. To find its structure, let x_i be the square of each B_2-Coxeter element in w, for $i = 1, 2, 3, 4$. Each x_i belongs to $C(w)$. Using Lemma 2.3, one checks that $x_i \in \ker \varrho_w$ for each i. Along with w, these elements x_i generate a subgroup $A \simeq (C_4 \times C_2^4)/\Delta C_2$ of index 2^2 in $\ker \varrho_w$. Additional computation in W_{D_8} shows that $\ker \varrho_w \simeq A \rtimes K_4$, where the Klein four-group K_4 acts on A by permuting the coordinates.

4.2.4 Coinvariants for $d = 12$

Here $X_w = 0$, so the coinvariant representation gives no information about $C(w)$. However, w^4 is an elliptic triality, so we have

$$C(w) \subset C(w^4) = \langle w^4 \rangle \times Sp_4(3),$$

via the coinvariant representation of $C(w^4)$. Note that w is linear over the field $K = \mathbb{Q}(w^4)$, with $\det(t - w|V_K) = \Phi_{12}(t)$, which reduces to Φ_4^2 on X_{w^4}. Hence the centralizer of w in $Sp_4(3)$ is $U_2(3)$. This shows that

$$C(w) = \langle w^4 \rangle \times C_{Sp_4(3)}(w^4) \simeq C_3 \times U_2(3).$$

5 Non-cyclotomic classes in E_8

5.1 The abelian group X_w and orbit types

The group X_w has cardinality $|X_w| = \det(1-w)$, but in the non-cyclotomic cases, the group structure of X_w is not immediately evident. It is helpful to also consider the subgroup $\hat{T}^w$ of fixed-points of w in the torus $\hat{T} = X \otimes \mathbb{C}^\times$, which may be viewed as a maximal torus in the complex Lie group $\hat{G}$ of type E_8. Since E_8 is simply-laced and the lattice X is self-dual, we have $X_w \simeq \hat{T}^w$ as $C(w)$-modules. If $t \in \hat{T}^w$ then w belongs to the stabilizer W_t, which is a reflection subgroup of W, since $\hat{G}$ is simply-connected. As w is elliptic, W_t has rank eight. It follows that t belongs to one of the nine conjugacy-classes of elements in $\hat{G}$ with semisimple centralizer. These correspond to the nodes of the affine Dynkin diagram; the order of t is equal to the corresponding coefficient of the highest root. This is tabulated for $t \neq 1$ as follows:

type of W_t	D_8	A_1A_7	$A_1A_2A_5$	A_4^2	D_5A_3	E_6A_2	A_1E_7	A_8
order of t	2	4	6	5	4	3	2	3

The $C(w)$-orbit of t has cardinality equal to the index $[C(w) : C_t(w)]$, where $C_t(w) = C(w) \cap W_t$. We define the *type* of the orbit $C(w) \cdot t$ to be the type of W_t, as in the table just above. It turns out that each orbit type appears at most once in X_w. We indicated this in Table 1 as (size of orbit)[type of orbit]. To find all the orbit types, one need only check which W_t contain a conjugate of w.

For example, suppose w belongs to the class $A_3D_5(a_1)$, where $|X_w| = 16$. A conjugate of w appears in two subgroups W_t, of types A_3D_5, and D_8, with indices $[C(w) : C_t(w)] = 12$ and 3, respectively, giving the size of each orbit. In Table 1 we indicate this orbit decomposition of $X_w - \{0\}$ as

$$12[A_3D_5] + 3[D_8].$$

Since X_w has 12 elements of order four and 3 elements of order two, we find that $X_w \simeq (\mathbb{Z}/4\mathbb{Z})^2$.

The orbit types are also important for the structure of L-packets, see section (—) below.

5.2 Injectivity results for the coinvariant representation

The following observations enable us to show in several cases at once that $\ker \varrho_w = \langle w \rangle$, and are useful in the more difficult cases below.

Lemma 5.1 *Let W' be a reflection subgroup of $W = W(E_8)$ generated by reflections corresponding to a maximal subdiagram of the affine diagram of W. Suppose $w \in W'$ is elliptic and generates its own centralizer in W' Then* $\ker \varrho_w = \langle w \rangle$.

Proof: View W as the Weyl group of a maximal torus $\hat{T}$ in a complex Lie group $\hat{G}$ of type E_8. Since $\hat{G}$ is simply-laced, simply-connected and adjoint, we have that W' is the centralizer in W of some element $t \in \hat{T}^w$ and $\hat{T}^w \simeq X_w$ as $C(w)$-modules. Since $\ker \varrho_w$ acts trivially on X_w, it fixes t. It follows that $\ker \varrho_w \subset W' \cap C(w) = \langle w \rangle$. Since the reverse containment is clear, the Lemma is proved. ■

Lemma 5.2 *Let $W' = W_1' \times W_2'$ be a reflection subgroup of $W = W(E_8)$ generated by reflections corresponding to a maximal subdiagram of the affine diagram of W which is the union of two orthogonal subdiagams whose reflections generate W_1' and W_2', respectively. Suppose $w = w_1 w_2 \in W'$ is elliptic, where $w_i \in W_i'$ generates its own centralizer in W_i' for $i = 1, 2$. Assume that the order of $\varrho_w(w_1)$ divides the order of w_2. Then* $\ker \varrho_w = \langle w \rangle$.

Proof: We have $C(w) \cap W' = \langle w_1 \rangle \times \langle w_2 \rangle$. Let d be the order of $\varrho_w(w_1)$, so that $\langle w_1 \rangle \cap \ker \varrho_w = \langle w_1^d \rangle$. Then $\ker \varrho_w \subset \langle w \rangle \cdot \langle w_1^d \rangle$. But if d divides the order of w_2 then $w_1^d = w^d$. Therefore $\ker \varrho_w = \langle w \rangle$. ■

Lemma 5.3 *Let $\{\beta_1, \ldots, \beta_k\}$ be a non-empty set of orthogonal roots contained in an even tetrad T and let $w = uv$, where $u = r_{\beta_1} \cdots r_{\beta_k}$ and $v\beta_i = \beta_i$ for $1 \leq i \leq k$. Then u acts nontrivially on X_w.*

Since W is transitive on even tetrads, we may assume that $T = \{\alpha_2, \alpha_4, \alpha_8, \alpha_2 + \alpha_4 + \alpha_8 + 2\alpha_3\}$. The normalizer of T in the subgroup $\langle r_2, r_3, r_4, r_8 \rangle \simeq W(D_4)$ is transitive on T. Hence we may assume that $\alpha_2 \in T$. We have

$$u\alpha_1 = \alpha_1 + \mu,$$

where $\mu = \sum_{i \in I} \beta_i$ and the set $I = \{i : \langle \alpha_1, \beta_i \rangle \neq 0\}$ has cardinality one or two. It suffices to prove that $\mu \notin (1 - w)X$.

Suppose $\mu = (1 - w)\lambda$, with $\lambda \in X$. Since $w\mu = -\mu$, we have $\dot{M}(w)\mu = \dot{M}(-1)\mu$, where $M(t)$ is the minimal polynomial of w and $\dot{M}(t) = (M(t) - M(1))/t - 1$, as before. Since -1 is an eigenvalue of w, we have $M(-1) = 0$, so $\dot{M}(-1) = \frac{1}{2}M(1)$ and

$$\tfrac{1}{2}M(1)\mu = \dot{M}(w)\mu = \dot{M}(w)(1 - w)\lambda = M(1)\lambda,$$

so that $\mu = 2\lambda$. But then we have

$$|I| = \tfrac{1}{2}\langle \mu, \mu \rangle = 2\langle \lambda, \lambda \rangle,$$

implying that 4 divides $|I|$, contradicting $|I| \in \{1, 2\}$. ■

5.3 $A_1E_7(a_2)$

We now turn to the individual cases not covered by the previous results. Here w lives in the subgroup $W_t \simeq W(A_1E_7)$ stabilizing an involution $t \in \hat{T}$. More precisely, w is a commuting product $w = uv$, where u is a reflection and $v \in W(E_7)$ has order 12 and centralizer of order 24. The minimal polynomial of w is $M(t) = \Phi_{12}(t)\Phi_6(t)\Phi_2(t)$ so $M(1) = 2$ and $X_w \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Since $|C_{W_t}(w)| = 2 \cdot 24$, so $[C(w) : C_{W_t}(w)] = 6 = |SL_2(2)|$, it follows that $\ker \varrho_w = C_{W_t}(w)$ and ϱ_w is surjective. Moreover, since $\Phi_2(t)$ divides $\det(t - v)$, it follows that the long element w_7 of $W(E_7)$ is not in $\langle v \rangle$. Hence $\ker \varrho_w = \langle u \rangle \times \langle w_7 \rangle \times \langle v \rangle$ is abelian of type $(2, 2, 12)$.

5.4 $A_1E_7(a_4)$

Here $w = -v$, where $v \in W(E_6)$ is in the class A_2^3. Hence $C(w)$ contains a reflection subgroup isomorphic to $W(A_2) \times C_{E_6}(v)$. We have $w^3 = -1$, so $X/2X \simeq \mathbb{F}_2^8$ surjects onto $X_w \simeq \mathbb{F}_2^2$, with kernel equal to the image of $(1-v)X$ in $X/2X$. Since $X = Q(A_2) + Q(E_6)$ modulo two, it follows that $(1-v)X = Q(E_6)$ modulo two. Since $W(E_6)$ acts trivially on $X/Q(E_6)$, it follows that $\langle -1 \rangle \times C_{E_6}(v) \subset \ker \varrho_w$. We have seen that $\langle -1 \rangle \times C_{E_6}(v)$ is the Heisenberg parabolic subgroup of $Sp_4(3)$, and has order 6^4. On the other hand, direct computation shows that ϱ_w is injective on $W(A_2)$. Since $|C(w)| = 6^5$, it follows that $C(w) = \langle -1 \rangle \times C_{E_6}(w) \times W(A_2)$ and that ϱ_w is projection onto the factor $W(A_2) \simeq SL_2(2)$.

5.5 $A_2E_6(a_2)$

Here w^2 has type A_2^4, and $x := \varrho_{w^2}(w)$ is an involution on $X_{w^2} \simeq \mathbb{F}_3^4$ with eigenvalues $1, 1, -1, -1$. The natural map $X_{w^2} \to X_w$ is projection onto the $+1$-eigenspace of w. It follows that

$$C(w) = \langle w^2 \rangle \times C_{Sp_4(3)}(x) = \langle w^2 \rangle \times SL_2(3) \times SL_2(3),$$

That ρ_w is projection onto one of the $SL_2(3)$-factors.

5.6 $A_1^2D_6$

Let $t \in \hat{T}$ be an involution of type A_1E_7. In $W(E_7)$, let s be an involution of type A_1D_6. The centralizer $W_{s,t}$ has type $2A_1D_6$ and w is a Coxeter element in $W_{s,t}$. The orders are given by

$$|C_{s,t}(w)| = 2^3 \cdot 5, \quad |C(w)| = 2^4 \cdot 3 \cdot 5^2, \quad |Sp_4(2)| = 2^4 \cdot 3^2 \cdot 5 = 720.$$

Since $\ker \varrho_w$ contains an element of order five and $C_{s,t}(w)$ has no elements of order three, the index $k = [C_{s,t}(w) : \ker \varrho_w]$ divides 2^3 and $|\operatorname{im} \varrho_w| = 30k$. But $k \neq 8$ since $Sp_4(2) = S_6$ has no subgroup of index three. Hence $k \in \{1, 2, 4\}$. Lemma 5.3 implies that $k = 4$.

Therefore $|\operatorname{im} \varrho_w| = 120$ and $\operatorname{im} \varrho_w$ is one of the two outer-conjugate subgroups H, H' in $Sp_4(2)$ isomorphic to S_5. These are distinguished by H containing transvections while H' does not. Let r, r' denote the reflections generating $W(2A_1)$ in $C(w)$. Then $\varrho_w(r), \varrho(r')$ are transvections on X_w, so $\operatorname{im} \varrho_w = H$.

This H comes from a point-stabilizer in S_6 under the isomorphism $S_6 \to Sp_4(2)$, which can be seen as follows. Let $\tilde{E}$ be the set of even subsets of $S = \{1, \dots, 6\}$, with addition given by symmetric difference, and bilinear form $\langle u, v \rangle = |u \cap v| \mod 2$. The radical is the line $\{\varnothing, S\}$, so $E := \tilde{E}/\{\varnothing, S\}$ is a nondegenerate symplectic 4-space over $\mathbb{F}_2$. Every nonzero vector in E can be uniquely represented by one of the 15 pairs $[ij]$. A transposition $(ij) \in S_6$ becomes the transvection $t_{ij}(v) = v + \langle v, [ij] \rangle [ij]$ on E and $H = \langle t_{12}, t_{23}, t_{34}, t_{45} \rangle$. The nonzero orbits of H on E are

$$\{[ij] : \ 1 \leq i < j \leq 5\}, \qquad \{[i6] : \ 1 \leq i \leq 5\}. \tag{28}$$

The stabilizers in W of involutions in $\hat{T}$ are of type $W(A_1E_7)$ and $W(D_8)$ and w is contained in groups of both types, where it has centralizers of orders $2^3 \cdot 3 \cdot 5$ and $2^4 \cdot 3 \cdot 5$. The orbits in (28) correspond to ten orbits of type A_1E_7 and five orbits of type D_8.

5.7 D_4^2

Since this class is also $A_1^2 D_6(a_2)$, this is similar to the previous case 5.6, whose notation we keep. We again have $X_w \simeq E$, with

$$|C_{s,t}(w)| = 2^4 \cdot 3^2, \quad |C(w)| = 2^5 \cdot 3^4, \quad |Sp_4(2)| = |S_6| = 2^4 \cdot 3^2 \cdot 5,$$

the index $\ell = [C_{s,t}(w) : \ker \varrho_w]$ divides 2^3. We cannot have $\ell = 2^3$, lest S_6 have a subgroup of index five. Lemma 5.3 then implies that $\ell = 2^2$. The image of ϱ_w is the subgroup $K = S_3^2 \cdot 2 \subset S_6$ of index ten stabilizing a bisection $(abc)(def)$ of S. The nonzero orbits of K on E are

$$\{[ij] : \ 1 \leq i,j \leq 3 \ \text{ or } \ 4 \leq i,j \leq 6\}, \quad \{[ij] : \ 1 \leq i \leq 3 \ \text{ and } \ 4 \leq j \leq 6\}.$$

These are six involutions of type $A_1 E_7$ and six involutions of type D_8, respectively. Computing in $W(D_8)$, we find that the elements

$$x = w^2 r_2 r_3 r_2 r_8, \quad z = r_9 (r_4 r_3 r_2 r_3 r_4)(r_5 r_4 r_3 r_4 r_5)(r_6 r_5 r_4 r_5 r_6)$$

generate an $S_3 \subset \ker \varrho_w$, where r_9 is the reflection about the highest root in E_7. It follows that

$$\ker \varrho_w = \langle w \rangle \times \langle x, z \rangle \simeq C_6 \times S_3.$$

5.8 $A_1^4 D_4$

The minimal polynomial of w is $\Phi_6 \Phi_2^6$, so $X_w \simeq \mathbb{F}_2^6$. Since $X_w \simeq \hat{T}^w$, we can view X_w as a $C(w)$-stable subspace of the eight dimensional $\mathbb{F}_2$-space $X_2 = \hat{T}[2]$, with W-invariant form $q(x) = \frac{1}{2}\langle x, x \rangle$ split over $\mathbb{F}_2$.

On X_2, w has eigenvalues $1^6, \zeta, 1+\zeta$, where $\zeta \in \mathbb{F}_4$ is a cube root of unity. It follows that the centralizer of w in $O(X_2, q)$ is isomorphic to $O_6^-(2) \times O_2^-(2)$, a product of nonsplit orthogonal groups. Since $X_w = (X_2)^w$, we see that ϱ_w is the projection of onto $O_6^-(2)$. Since $O_2^-(2) \simeq C_3$, the kernel of ϱ_w has order six, hence is generated by w. Since $|C(w)| = 2^8 \cdot 3^5 \cdot 5$, we have

$$|\operatorname{im} \varrho_w| = 2^7 \cdot 3^4 \cdot 5 = |O_6^-(2)|.$$

Thus, $\operatorname{im} \varrho_w \simeq O_6^-(2) \subset Sp_6(2)$, which has two orbits on non-zero vectors in X_w, determined by the values of the invariant quadratic form $q|X_w$. We can also think of $O_6^-(2) = W(E_6)$, via reduction modulo two of the E_6 root lattice. Hence the $C(w)$-orbits in X_w correspond to $W(E_6)$-orbits of involutions in the torus of the adjoint group of type E_6. In this view there are 36 vectors in X_w with $W(E_6)$-stabilizers of type $A_1 A_5$ (for $q = 1$) and 27 vectors with $W(E_6)$-stabilizer of type D_5 (for $q = 0$). In $W(E_8)$ this gives the orbit structure $36[A_1 E_7] + 27[D_8]$.

5.9 $A_3D_5(a_1)$

Let $t \in \hat{T}$ have centralizer $W_t = W(A_3D_5)$. Then $|C_t(w)| = 2^4 \cdot 3$ and $t \in \hat{T}^w$ has $C(w)$-orbit of size $[C(w) : C_t(w)] = 12$. Since $4X_w = 0$ and X_w has at least 12 elements of order 4, it follows that $X_w \simeq R \oplus R$, where $R = \mathbb{Z}/4\mathbb{Z}$. Hence there are exactly 12 vectors of order four in X_w, forming a single orbit of type A_3D_5. The three vectors of order two form an orbit of type D_8.

Since $\langle\ ,\ \rangle_w$ is nondegenerate, there exists a basis u, v of X_w such that $\langle u, v\rangle_w = 1$. By skew symmetry, we have $\langle u, u\rangle_w, \langle v, v\rangle_w \in \{0, 2\}$. Subtracting one basis vector from the other if necessary, we can arrange that $\langle u, u\rangle_w = \langle v, v\rangle_w$. If this value is 2, one counts eight vectors $u' \in X_w$ with $\langle u', u'\rangle_w = 2$, which is incompatible with $C(w)$ having an orbit of size 12. Hence $\langle u, u\rangle = \langle v, v\rangle = 0$, so $Sp(X_w) = SL_2(R)$ and $|Sp(X_w)| = 2^4 \cdot 3$. Since $C(w)$ is transitive on the 12 vectors of order four in X_w, we have $Sp(X_w) = \operatorname{im} \varrho_w \cdot U$, where $U \simeq C_4$ is the stabilizer of t. But $\rho_w(C_t(w)) \subset U$, and a direct computation using Lemma 2.3 shows that ϱ_w maps the A_3-factor in w to an element of order four, so in fact $\rho_w(C_t(w)) = U$, implying that ϱ_w is surjective, with kernel $\langle w\rangle$.

5.10 $A_3^2A_1^2$

Here w can also be viewed as $A_1^4D_4(a_1)$. We have $|C(w)| = 2^{11} \cdot 3^2$ and w is contained in reflection subgroups

$$W_1 \simeq W(A_3D_5), \quad W_2 \simeq W(A_1E_7), \quad W_3 \simeq W(D_8)$$

with indices

$$[C(w) : C_1(w)] = 48, \quad [C(w) : C_2(w)] = 12, \quad [C(w) : C_3(w)] = 3.$$

Since $|X_w| = 64$ and $4X_w = 0$ and there are 48 elements in X_w of order four, X_w must have type $(4, 4, 2, 2)$, with automorphism group of order

$$|\operatorname{Aut}(X_w)| = 2^{14} \cdot 3^2.$$

It follows from the above count that $\operatorname{im} \varrho_w$ is transitive on the $\operatorname{Aut}(X)$-orbits in X_w.

We can write $W_1 = W(D_3) \times W(D_5)$ and correspondingly $\hat{T} = \hat{T}_3 \times_Z \hat{T}_5$, where $\hat{T}_n$ is a maximal torus in $Spin_n$ and $Z \simeq \mu_4$ is the diagonally embedded center of each factor. Let $s \in \hat{T}_5$ have Kac coordinates equal to 1 on a branch node, zero on all other nodes. We can take w to be a Coxeter element in the centralizer $C_{W_1}(s) \simeq W(D_3) \times [W(D_3) \times W(D_2)]$. Write $w = abc$ accordingly. Then

$$\ker \varrho_w \subset C_{W_1}(s, w) = \langle a\rangle \times \langle b\rangle \times \langle c\rangle.$$

Applying Lemma 2.3 to elements in $C_{W_1}(s, w)$ shows that $\ker \varrho_w = \langle w\rangle$, so that $|\operatorname{im} \varrho_w| = 2^9 \cdot 3^2$.

We show that ϱ_w is surjective by computing the order of the group $Sp(X_w)$ of automorphisms of $X_w \simeq (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^2$ preserving the alternating form $\langle\ ,\ \rangle_w$. Since the class of w is determined by $\det(t-w)$, we can check that $w = v^3$, where v belongs to the class $A_3D_5(a_1)$. The v-invariants in $X_w \simeq \hat{T}^w$ are a submodule $U \simeq \hat{T}^v \simeq (\mathbb{Z}/4\mathbb{Z})^2$. Choose an element $y \in X_w$ of order two such that $\langle y, U\rangle_w = 0$. Since v has order three on X_w, we have $y + vy + v^2y = 0$ and $\{0, y, vy, v^2y\}$ is a subspace $Y \simeq (\mathbb{Z}/2\mathbb{Z})^2$ giving an orthogonal decomposition

$$X_w = U \oplus Y.$$

Applying the argument of 5.9 to U, we can choose bases $\{u_1, u_2\},\ \{y_1, y_2\}$ of U and Y such that

$$\langle u_1, u_2\rangle = \langle y_1, y_2\rangle = 1, \quad \langle u_1, u_1\rangle = \langle y_1, y_1\rangle = 0.$$

We compute the stabilizer of u_1 in $Sp(X_w)$: Suppose

$$g = \begin{bmatrix} 1 & a & x & z \\ 0 & b & y & t \\ 0 & c & p & r \\ 0 & d & q & s \end{bmatrix} \in Sp(X_w).$$

Here, $a, b \in \mathbb{Z}/4\mathbb{Z}$, $c, d, p, q, r, s \in \mathbb{Z}/2\mathbb{Z}$, and $x, y, z, t \in 2\mathbb{Z}/4\mathbb{Z}$. We have

$$\begin{aligned}
0 &= \langle u_1, v_1\rangle_w = \langle u_1, gv_1\rangle_w = y, \\
0 &= \langle u_1, v_2\rangle_w = \langle u_1, gv_2\rangle_w = t, \\
1 &= \langle u_1, u_2\rangle_w = \langle u_1, gu_2\rangle_w = b, \\
0 &= \langle u_2, v_1\rangle_w \ \Rightarrow\ x = cq + dp, \\
0 &= \langle u_2, v_2\rangle_w \ \Rightarrow\ z = cs + dr, \\
1 &= \langle v_1, v_2\rangle_w = ps + qr.
\end{aligned}$$

Therefore,

$$g = \begin{bmatrix} 1 & a & x & z \\ 0 & 1 & 0 & 0 \\ 0 & c & p & r \\ 0 & d & q & s \end{bmatrix},$$

where $x = cq + dp$ and $z = cs + dr$. We find exactly $2^5 \cdot 3$ choices for g. Since $C(w)$ is already transitive on elements of order four in X_w, so is $Sp(X_w)$, and we have

$$|Sp(X_w)| = 48 \cdot 2^5 \cdot 3 = 2^9 \cdot 3^2 = |\operatorname{im} \varrho_w|.$$

Hence ϱ_w is surjective, as claimed.

6 Maximal tori in quasi-split groups

This section and the next contain applications of our study of coinvariant representations to the classification of maximal tori in p-adic groups and associated supercuspidal L-packets. We begin in greater generality, with the rough classification of maximal tori in quasi-split groups over any perfect field k. In the spirit of the Langlands correspondence, the rational classes of maximal tori will be partitioned into "stable classes", in which the rational classes correspond to orbits of a certain rational Weyl group on a Galois cohomology group. When we specialize k to be a p-adic field, this becomes a coinvariant representation, or subquotient thereof.

For basic results in Galois cohomology we follow [28] Let k be a perfect field and let $\Gamma = \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of k. For any algebraic k-group L, let $H^1(k, L) = H^1(\bar{k}/k, L)$ denote the first Galois cohomology set of L. If M is a subgroup of L defined over k, let $\ker^1(M, L)$ denote the kernel of the map $H^1(k, M) \to H^1(k, L)$ induced by the inclusion $M \hookrightarrow L$.

Let G be a connected semisimple quasi-split algebraic group defined over k. By *maximal torus in G* we mean a subgroup of G which is a maximal torus and is defined over k. We consider two notions of conjugacy: Two maximal tori S, S' in G are *rationally congugate* if they are conjugate by an element of $G(k)$, and they are *stably conjugate* if their groups $S(k)$ and $S'(k)$ of rational points are conjugate by an element of $G = G(\bar{k})$. Each stable class is partitioned into rational classes.

Let A be a maximal k-split torus in G and let $T = C_G(A)$ be the centralizer of A. Then T is a maximal torus in G, since G is quasi-split. The Weyl group W is the quotient N/T, where N is the normalizer of T. Let $\pi : H^1(k, N) \to H^1(k, W)$ be the map induced by the projection $N \to W$ and let $\pi_1 : \ker^1(N, G) \to H^1(k, W)$ be the restriction of π to $\ker^1(N, G)$.

Proposition 6.1 *The stable classes of maximal tori in G are in bijection with $H^1(k, W)$. The set of rational classes of maximal tori in the stable class corresponding to a class $x \in H^1(k, W)$ is in bijection with the fiber $\pi_1^{-1}(x) \subset \ker^1(N, G)$.*

When k is finite, we have $H^1(k, G) = 1$ and $\pi_1 = \pi$ is actually a bijection, as follows from the Lang-Steinberg theorem. Each stable class consists of a single rational class and these classes are in bijection with $H^1(k, W)$, as is well-known (cf. [5]). When k is p-adic, a version of Prop. 6.1 was proved for unramified tori by DeBacker [12].

From now on, we assume that k is infinite and we identify algebraic k-groups with their groups of k-rational points. The proof of Prop. 6.1, along with a more precise description of the fibers of π, will occupy the rest of this section.

Lemma 6.2 *The set of rational conjugacy classes of maximal tori in G is in bijection with* $\ker^1(N, G)$.

Proof: This is a special case of a basic principal in Galois cohomology. Indeed, if S is a maximal torus in G then $S = gTg^{-1}$ for some g in G, and since S is defined over k we have $g^{-1}\gamma(g) \in N$ for all $\gamma \in \Gamma$. Sending the rational class of S to the class of the cocycle $\gamma \mapsto g^{-1}\gamma(g)$ gives the asserted bijection. ■

Next, by a result of Raghunathan, we know that each fiber of π_1 is non-empty.

Lemma 6.3 *The map $\pi_1 : \ker^1(N, G) \to H^1(k, W)$ is surjective.*

Proof: See [24], which requires G to be quasi-split, as we have assumed. ■

The proof of Prop. 6.1 is completed by the next result:

Lemma 6.4 *Let S, S' be maximal tori in G whose rational classes correspond to $c, c' \in \ker^1(N, G)$ as in Lemma 6.2. Then S and S' are stably conjugate if and only if $\pi_1(c) = \pi_1(c')$.*

Proof: Write $S = {}^hT$, $S' = {}^\ell T$, so that

$$\xi_\gamma = h^{-1}\gamma(h) \in c \qquad \text{and} \qquad \eta_\gamma = \ell^{-1}\gamma(\ell) \in c'. \tag{29}$$

Suppose that $\mathrm{Ad}(g)[S(k)] = S'(k)$ for some $g \in G$. Since k is infinite, $S(k)$ is Zariski-dense in S and likewise for S'. In particular It follows that ${}^{gh}T = {}^\ell T$, so we get an element

$$n := \ell^{-1}gh \in N.$$

I claim that $n\xi_\gamma\gamma(n)^{-1}$ and η_γ have the same image in W.

Choose an element $s \in S'(k)$ whose centralizer is S'. We have $s^g \in S(k)$, so for each $\gamma \in \Gamma$ the element $g\gamma(g)^{-1}$ centralizes s, hence belongs to S'. Now,

$$n\xi_\gamma\gamma(n)^{-1} = nh^{-1}\gamma(hn^{-1}) = \ell^{-1}g\gamma(g^{-1}\ell),$$

so it must be shown that

$$\ell^{-1}g\gamma(g^{-1}\ell) \in \ell^{-1}\gamma(\ell)T \qquad \text{for all} \qquad \gamma \in \Gamma.$$

But this holds because

$$\gamma(\ell)^{-1}g\gamma(g^{-1}\ell) = \eta_\gamma^{-1}\ell^{-1}g\gamma(g)^{-1}\ell\eta_\gamma \in \mathrm{Ad}(\eta_\gamma^{-1})\,\mathrm{Ad}(\ell^{-1})S' = \mathrm{Ad}(\eta_\gamma^{-1})T = T.$$

For the converse, suppose ξ_γ and η_γ are as in (29) and that $t_\gamma\xi_\gamma = \eta_\gamma$ for some cocycle $t_\gamma \in T$. Let $g = \ell h^{-1}$. Then

$$\gamma(g) = \ell t_\gamma h^{-1}.$$

For any $s \in S(k)$ we have $\mathrm{Ad}(h^{-1})s \in T$, so

$$\gamma(gsg^{-1}) = \mathrm{Ad}(\ell t_\gamma h^{-1})s = \mathrm{Ad}(\ell h^{-1})s = gsg^{-1}.$$

This shows that $\mathrm{Ad}(g)$ maps $S(k)$ to $S'(k)$, and completes the proof of Prop. 6.1. ■

6.1 The fibers of π_1

To determine the rational classes in a stable class of maximal tori, we study the fibers of π_1. This requires the notion of twisting in Galois cohomology. If L is an algebraic k-group and $\xi : \Gamma \to \mathrm{Aut}(L)$ is a Galois cocycle, then L_ξ denotes the k-group twisted by ξ: we have $L_\xi = L$ as sets, with new Γ-action given by $\gamma_\xi(\ell) = \xi_\gamma \cdot \gamma(\ell)$, where $\gamma(\ell)$ is the original action of Γ on L and $\xi_\gamma\cdot$ is the action of $\mathrm{Aut}(L)$ on L. If ξ takes values in L instead of $\mathrm{Aut}(L)$, the twisting is understood with respect to the cocycle $\mathrm{Ad}(\xi) : \Gamma \to \mathrm{Aut}(L)$ given by $\mathrm{Ad}(\xi)_\gamma(\ell) = \xi_\gamma\ell\xi_\gamma^{-1}$.

Fix a cocycle $\xi : \Gamma \to W$ and let T_ξ be the twist of T via the natural map $W \to \mathrm{Aut}(T)$. By Lemma 6.3 there exists $g \in G$ such that the cocycle $\dot\xi_\gamma := g^{-1}\gamma(g)$ takes values in N and whose projection to W lies in the class of ξ. One checks that the conjugation map $\mathrm{Ad}(g) : T_\xi \to gTg^{-1}$ is k-rational. Thus, the twisted torus T_ξ embeds as a maximal torus in G for any cocycle $\xi : \Gamma \to W$.

We also have the twisted groups $N_{\dot\xi}$ and $G_{\dot\xi}$. The latter is k-isomorphic to G via the map $\mathrm{Ad}(g) : G_{\dot\xi} \to G$ and we have a commutative square, whose horizontal maps are induced by inclusion and whose vertical maps are bijections:

$$\begin{array}{ccc} H^1(k, N_{\dot\xi}) & \longrightarrow & H^1(k, G_{\dot\xi}) \\ {\scriptstyle \tau_{\dot\xi}}\downarrow & & \downarrow{\scriptstyle \mathrm{Ad}(g)} \\ H^1(k, N) & \longrightarrow & H^1(k, G). \end{array} \tag{30}$$

Here $\tau_{\dot\xi}$ is the twisting bijection $\tau_{\dot\xi}[\zeta] = [\zeta\dot\xi]$ [28, 5.3]. Note that $\tau_{\dot\xi}$ sends $\ker^1(N_{\dot\xi}, G_{\dot\xi})$ to $\ker^1(N, G)$.

The exact sequence of k-groups

$$1 \longrightarrow T_\xi \longrightarrow N_{\dot\xi} \longrightarrow W_\xi \longrightarrow 1$$

gives an exact sequence of pointed sets [28, 5.1(2)] in the top row of the following diagram.

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & W_\xi(k)^\circ & \longrightarrow & W_\xi(k) & \xrightarrow{\delta_\xi} & \ker^1(T_\xi, G_{\dot\xi}) & \xrightarrow{\iota_\xi} & \ker^1(N_{\dot\xi}, G_{\dot\xi}) & \xrightarrow{\pi_\xi} & H^1(k, W_\xi) \\ & & & & & & & & {\scriptstyle \tau_{\dot\xi}}\downarrow & & \downarrow{\scriptstyle \tau_\xi} \\ & & & & & & & & \ker^1(N, G) & \xrightarrow{\pi_1} & H^1(k, W). \end{array} \tag{31}$$

Here $W_\xi(k) = \{w \in W : \xi_\gamma\gamma(w)\xi_\gamma^{-1} = w\}$ is the group of k-rational points in the twisted group W_ξ and $W_\xi(k)^\circ = N_{\dot\xi}(k)/T_\xi(k)$ consists of the elements in $W_\xi(k)$ having a k-rational representative in $N_{\dot\xi}$. The maps $\iota_\xi, \pi_\xi, \pi_1$ are induced by the maps on underlying groups and δ_ξ is the coboundary map. For $w \in W_\xi(k)$, $\delta_\xi(w)$ is the class of cocycles of the form

$$\gamma \mapsto \dot w\gamma_{\dot\xi}(\dot w)^{-1} = \dot w\dot\xi_\gamma\gamma(\dot w)^{-1}\dot\xi_\gamma^{-1},$$

where $\dot w \in N$ is a lift of w. The map τ_ξ is the projection of the previous $\tau_{\dot\xi}$, and is given by $\tau_\xi[\eta] = [\eta\xi]$.

The group $W_\xi(k)$ acts on $H^1(k, T_\xi)$ via the rule

$$(w * \zeta)_\gamma = \dot w\zeta_\gamma\gamma_\xi(\dot w)^{-1},$$

where $\dot w$ is a lift of w in N and ζ is a cocycle in T_ξ. This is an *affine* action of $W_\xi(k)$ on the abelian group $H^1(k, T_\xi)$. Indeed, the coboundary $\delta_\xi : W_\xi(k) \to H^1(k, T_\xi)$ is a cocycle on $W_\xi(k)$ and we have

$$w * \zeta = (w \cdot \zeta)\delta_\xi(w),$$

where $w \cdot \zeta$ is the *linear* action of $W_\xi(k)$ on $H^1(k, T_\xi)$, which is the restriction of the natural action of W on T (cf. [28, I.5.6]). The affine and linear actions coincide on the subgroup $W_\xi(k)^\circ = \ker \delta_\xi$.

Suppose the class of ζ belongs to $\ker^1(T_\xi, G_{\dot\xi})$, so that $\zeta_\gamma = h^{-1}\gamma_{\dot\xi}(h)$ for some $h \in G$. Then $(w*\zeta)_\gamma = \dot w h^{-1}\gamma_{\dot\xi}(h\dot w^{-1})$. Hence the affine action of $W_\xi(k)$ on $H^1(k, T_\xi)$ preserves $\ker^1(T_\xi, G_{\dot\xi})$.

By Prop. 6.1, the class $x \in H^1(k, W)$ of ξ determines a stable class $\mathcal{T}_x$ of maximal tori in G and the rational classes in $\mathcal{T}_x$ are in bijection with the fiber $\pi_1^{-1}(x)$. The next result makes this more precise.

Proposition 6.5 *The rational classes in $\mathcal{T}_x$ are in bijection with the orbits of $W_\xi(k)$ on $\ker^1(T_\xi, G_{\dot\xi})$ under the affine action.*

Proof: Under the twisting bijection $\tau_{\dot\xi}$, we have

$$\pi_1^{-1}(x) = \tau_{\dot\xi}(\ker \pi_\xi) = \tau_{\dot\xi}(\operatorname{im} \iota_\xi).$$

It follows that the set of rational classes in $\mathcal{T}_x$ are in bijection with the set of fibers of ι_ξ. From the definition of $H^1(k, N_{\dot\xi})$, the fibers of ι_ξ are the orbits of $W_\xi(k)$ in $H^1(k, T_\xi)$ under the affine action. ■

6.2 Weyl groups

A maximal torus S in G has several Weyl groups: The *absolute Weyl group* of S is the quotient $W_S = N_S/S$, where N_S is the normalizer of S in G. The *big rational Weyl group* of S is the group $W_S(k) = W_S^\Gamma$ of k-rational points in W_S. Finally, the *small rational Weyl group* is the subgroup $W_S(k)^\circ \subset W_S(k)$ consisting of elements in $W_S(k)$ which have a representative in $N_S(k) = N_S^\Gamma$.

Suppose S corresponds to the class of the cocycle $\dot\xi$ in N, and let ξ be the projection of $\dot\xi$ to W. If $\dot\xi_\gamma = g^{-1}\gamma(g)$, the map $\operatorname{Ad}(g)$ gives an isomorphism $W_\xi \to W_S$ which is defined over k. Hence $\operatorname{Ad}(g)$ restricts to an isomorphism

$$W_\xi(k) \xrightarrow{\sim} W_S(k). \tag{32}$$

In particular, the the isomorphism type of $W_S(k)$ depends only on the stable class of S corresponding to the class of ξ in $H^1(k, W)$.

We have seen that the rational classes of maximal tori in the stable class of S are in bijection, via the twisting bijection $\tau_{\dot\xi}$, with the image of the map

$$\iota_\xi : \ker^1(T_\xi, G_{\dot\xi}) \to \ker^1(N_{\dot\xi}, G_{\dot\xi})$$

induced by the inclusion $T \hookrightarrow N$. Explicitly, a cocycle $\zeta : \Gamma \to T_\xi$ corresponds to the maximal torus $S_\zeta := hTh^{-1}$, where $h^{-1}\gamma(h) = \zeta_\gamma\dot\xi_\gamma$. Let $W_\xi(k, \zeta)$ denote the stabilizer in $W_\xi(k)$, under the affine action, of the class of ζ in $\ker^1(T_\xi, G_{\dot\xi})$.

Lemma 6.6 *The map $\operatorname{Ad}(h)$ restricts to an isomorphism $W_\xi(k, \zeta) \xrightarrow{\sim} W_{S_\zeta}(k)^\circ$. Thus, the small rational Weyl group of S is isomorphic to a point-stabilizer in $W_\xi(k)$ on the orbit in $\ker^1(T_\xi, G_{\dot\xi})$ corresponding to S as in Prop. 6.5.*

Proof: It is straightforward to check that any $w \in W_\xi(k, \zeta)$ has a lift $\dot w \in N$ fixing the cocycle ζ itself, that is, we may choose $\dot w$ so that $\dot w\zeta_\gamma\gamma_{\dot\xi}(\dot w)^{-1} = \zeta_\gamma$ for all $\gamma \in \Gamma$. It then follows that $\gamma(h\dot wh^{-1}) = h\dot wh^{-1}$ for all $\gamma \in \Gamma$. Therefore $h\dot wh^{-1} \in N_{S_\zeta}(k)$ as desired. The argument is reversible. ■

6.3 Nontriviality of the cocycle: SL_2

We have seen that the affine action of $W_\xi(k)$ on $H^1(k, T_\xi)$ is the twist of the linear action by the cocycle $\delta_\xi : W_\xi(k) \to H^1(k, T_\xi)$. If δ_ξ is a coboundary, then the affine and linear orbits are in bijection. In this section we compute δ_ξ for the non-split tori in SL_2, and find that δ_ξ is not always a coboundary.

Let W be the Weyl group of the diagonal torus in $T \subset SL_2$. A nontrivial cocycle $\xi : \Gamma \to W$ is a homomorphism factoring through an isomorphism $\mathrm{Gal}(E/k) \to W$, where E/k is a quadratic extension, with absolute Galois group $\Gamma_E = \ker \xi$. The twisted torus T_ξ is the one-dimensional unitary group U_1 of E/k and $W_\xi(k) = W$. By Hilbert's Thm. 90, any cocycle $c : \Gamma \to T_\xi$ may be adjusted by a coboundary so as to take just two values:

$$c_\gamma = \begin{cases} 1 & \text{if} \quad \gamma \in \Gamma_E \\ x & \text{if} \quad \gamma \in \Gamma - \Gamma_E \end{cases}$$

for some $x \in T(k) = k^\times$. This leads to an isomorphism

$$H^1(k, T_\xi) \simeq k^\times / NE^\times,$$

where $NE^\times$ is the norm group of E. Since $x^{-1} \equiv x \mod NE^\times$, it follows that the linear action of W on $H^1(k, T_\xi)$ is trivial. Hence the coboundary map $\delta_\xi : W_\xi(k) \to H^1(k, T_\xi)$ may be viewed as a group homomorphism

$$\delta_\xi : W \to k^\times / NE^\times$$

which is determined by the image $\delta_\xi(w)$ of the nontrivial element of W.

Proposition 6.7 *$\delta_\xi(w)$ is the class of -1 in $k^\times/NE^\times$.*

Proof: If $\mathrm{char}\, k = 2$ then the projection $N \to W$ splits, which implies that δ_ξ is trivial, just as -1 is trivial in $k^\times/NE^\times$. Assume that $\mathrm{char}\, k \neq 2$ and write $E = k(\epsilon)$, where $\epsilon = \sqrt{e}$ and e is a non-square in $k^\times$.

There is a torus S in the stable class $\mathcal{T}_\xi$ with rational points

$$S(k) = \left\{ \begin{bmatrix} a & eb \\ b & a \end{bmatrix} : \ a, b \in k^\times, \ a^2 - eb^2 = 1 \right\}.$$

We have $S = gTg^{-1}$, where

$$g = \begin{bmatrix} 1 & -\epsilon/2 \\ 1/\epsilon & 1/2 \end{bmatrix}$$

and S determines the lifted cocycle given (for $\gamma \in \Gamma - \Gamma_E$) by

$$\dot{\xi}_\gamma = g^{-1}\gamma(g) = \begin{bmatrix} 0 & -2/\epsilon \\ \epsilon/2 & 0 \end{bmatrix} \in N.$$

Choosing $\dot{w} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, we have

$$\delta_{\dot{\xi}}(\dot{w})_\gamma = \dot{w}\dot{\xi}_\gamma \dot{w}^{-1} \dot{\xi}_\gamma^{-1} = \begin{bmatrix} e/4 & 0 \\ 0 & 4/e \end{bmatrix}.$$

Since $e/4$ and -1 have the same class in $k^\times/NE^\times$, the proposition is proved.

An alternative proof runs as follows: Viewing E as a two-dimensional k-vector space, the normalizer of S in $GL_2(k)$ is $E^\times \rtimes \langle\sigma\rangle$, where σ generates $\mathrm{Gal}(E/k)$. Since $\det\sigma = -1$, there is an element of $N_S(k)$ outside $S(k)$ exactly when there is an element of $E^\times$ of norm equal to -1. Since $|W| = 2$, the claim now follows from Lemma 6.6. ■

6.4 p-adic groups

From now on, k is a finite extension of $\mathbb{Q}_p$ for some prime p. Let G be a connected, quasi-split, semisimple algebraic group over k. In this situation we can make the classification of tori more explicit.

First, it is suggestive to reformulate the classification of maximal tori in analogy with local Langlands conjecture for representations of $G(k)$. Let $R \subset X^*(T)$ be the set of roots of T in G. There is a base $B \subset R$ preserved by Γ, since G is quasi-split, and the k-structure on G is given (up to isomorphism) by a continuous homomorphism

$$\psi_G : \Gamma \longrightarrow \mathrm{Aut}(R, B)$$

from Γ into the group of automorphisms of R preserving B. The semidirect product

$$^LW := W \rtimes \mathrm{Aut}(R, B)$$

is the full automorphism group of the root system R. We define a *Langlands parameter* for W to be a continuous homomorphism

$$\varphi : \Gamma \to {}^LW$$

whose projection onto $\mathrm{Aut}(R, B)$ is the map ψ_G. We consider two parameters to be equivalent if they are conjugate by the action of W. Let $C_W(\varphi)$ be the centralizer in W of the image $\varphi(\Gamma)$ and let $[X_\varphi]_{\mathrm{tor}}$ be the torsion subgroup of the coinvariants of $\varphi(\Gamma)$ in the co-character group $X = X_*(T)$. Set $\delta_\varphi = \delta_\xi$, where ξ is the projection of φ to W. The action of W on X induces the linear action of $C_W(\varphi)$ on $[X_\varphi]_{\mathrm{tor}}$. The affine action of $C_W(\varphi)$ on $[X_\varphi]_{\mathrm{tor}}$ is the twist of the linear action by the cocycle $\delta_\varphi : C_W(\varphi) \to [X_\varphi]_{\mathrm{tor}}$.

Proposition 6.8 *The equivalence classes of Langlands parameters $\varphi : \Gamma \to {}^LW$ are in bijection with the stable classes of maximal tori in G. Denoting this correspondence by $\varphi \mapsto \mathcal{T}_\varphi$, we have*

1. *$W_S(k) \simeq C_W(\varphi)$ and $H^1(k, S) \simeq [X_\varphi]_{\mathrm{tor}}$, for any $S \in \mathcal{T}_\varphi$.*
2. *The rational classes in $\mathcal{T}_\varphi$ are in bijection with the orbits of $C_W(\varphi)$ in $[X_\varphi]_{\mathrm{tor}}$ under the affine action.*

Proof: The projection of φ onto W of a Langlands parameter φ is a cocycle $\xi : \Gamma \to W$. Conversely, every cocycle $\xi : \Gamma \to W$ gives a parameter $\varphi(\gamma) = \xi_\gamma \rtimes \psi_G(\gamma) \in {}^LW$. Equivalent parameters φ, φ' correspond to cohomologous cocycles ξ, ξ' and from the definition of twisting we have $C_W(\varphi) = W_\xi(k)$. The result now follows from (32) and Prop. 6.1. ■

Thus, a stable class of maximal tori is analogous to a stable L-packet of representations of $G(k)$. In fact, this is more than an analogy: One can regard the L-packets of supercuspidal representations constructed in [13], [20] [27] as "induced" from the L-packets of tori described here, see section 6.8 below.

6.5 Triviality of the cocycle: Odd coinvariants

From Prop. 6.8, to find the rational classes in a stable class $\mathcal{T}_\varphi$ is equivalent to finding the affine orbits of $C_W(\varphi)$ in $[X_\varphi]_{\text{tor}}$. Both of these groups depend only on the image of φ in W. However, this affine action depends on the cocycle δ_φ, which as we have seen in section 6.3, may involve the arithmetic of k. In this section we point out situations where δ_φ is a coboundary, which implies that the set of affine orbits of $C_W(\varphi)$ on $[X_\varphi]_{\text{tor}}$ is in bijection with the set of linear orbits.

Assume that G is split over k. Following Tits, there is an extension

$$1 \longrightarrow T[2] \longrightarrow \dot{W} \longrightarrow W \longrightarrow 1,$$

where $T[2] = \{t \in T : \ t^2 = 1\}$ and $\dot{W}$ is a subgroup of $N(k)$. Recall that the normalizer of an element h in a group H is the normalizer in H of the cyclic group generated by h.

Lemma 6.9 *Assume that $w \in W$ is such that $\det(1-w)$ is odd. Then for any lift $\dot{w} \in \dot{W}$ of w, the projection $\dot{W} \to W$ induces an isomorphism*

$$N_{\dot{W}}(\dot{w}) \stackrel{\simeq}{\longrightarrow} N_W(w)$$

between the normalizer of $\dot{w}$ in $\dot{W}$ and the normalizer of w in W, which restricts to an isomorphism on centralizers.

Proof: If $u \in N_W(w)$ then $uwu^{-1} = w^q$ for some q relatively prime to the order of w. Choose an arbitrary lift $\dot{u} \in \dot{W}$, so that

$$\dot{u}\dot{w}\dot{u}^{-1} = \dot{w}^q t,$$

for some $t \in T[2]$. Since w is conjugate to w^q, we have that $\det(1-w^q) = \det(1-w)$ is odd, so the map

$$1 - w^q : T[2] \longrightarrow T[2]$$

is an isomorphism. If we choose $s \in T[2]$ so that $s^{1-w^q} = t$ then $(s\dot{u})\dot{w}(s\dot{u})^{-1} = \dot{w}^q$. This proves that $N_{\dot{W}}(\dot{w}) \to N_W(w)$, as well as the restriction to centralizers, is surjective. To see injectivity, suppose $t \in T[2] \cap N_{\dot{W}}(\dot{w})$. Then for some integer q we have $t\dot{w}t^{-1} = \dot{w}^q$. But $t\dot{w}t^{-1} = \dot{w}t^{w-1}$, so t^{w-1} is a power of $\dot{w}$ and hence belongs to $T[2]^w$. Since $T[2]^w$ is trivial it follows that $t = 1$. ∎

Now suppose we have a Langlands parameter $\varphi : \Gamma \to W$ which is trivial on the wild inertia subgroup of Γ. Then φ is generated by two elements w, u, where w generates the image of the inertia subgroup and $u = \varphi(\mathrm{F})$ is the image of a Frobenius element $\mathrm{F} \in \Gamma$, with the relation $uwu^{-1} = u^q$, where q is the cardinality of the residue field of k. Since u belongs to the normalizer of w, it acts on X_w and normalizes $C(w)$; let $(X_w)_u$ and $C(w)^u$ denote the co-invariants and invariants, respectively. The following is now immediate from our remarks in this section.

Proposition 6.10 *Assume G is split over k and that the Langlands parameter $\varphi : \Gamma \to W$ is tame, with inertial image generated by an element $w \in W$ having $\det(1-w)$ odd, and let $u = \varphi(\mathrm{F}) \in W$ be the image of a Frobenius element $\mathrm{F} \in \Gamma$. Then*

1. *$H^1(k, T_\varphi) \simeq (X_w)_u$, where T_φ is the twist of T by φ.*

2. *The rational classes of maximal tori in the stable class of φ are in bijection with the orbits of $C(w)^u$ on $(X_w)_u$.*

Remarks:

1. Recall from Prop. 2.4 that u acts on X_w as a similitude of the alternating form $\langle\ ,\ \rangle_w$, with multiplier q.

2. For W of type E_8, we have $\det(1-w)$ odd exactly when w or $-w$ belongs to one of the conjugacy classes E_8, $A_2E_6(a_2)$ and $E_8(a_i)$ for $1 \le i \le 8$ (see Table 1).

6.6 Triviality of the cocycle: G_2

If the extension $N(k) \to W$ splits, then the cocycle δ_φ is automatically a coboundary. Let G be the split k-group of type G_2, with Weyl group W dihedral of order 12. In this case, we can show that $N(k) \to W$ splits, as follows. The maximal proper Levi subgroups in G are isomorphic to GL_2, so both of the simple reflections $r_1, r_2 \in W$ lift to involutions $\dot{r}_i \in N(k)$. Their product $\dot{c} = \dot{r}_1\dot{r}_2$ projects to a Coxeter element $c \in W$, hence $\dot{c}^6 \in T$ and is fixed by c. But G is both simply-connected and adjoint, so T^c is trivial and $\dot{c}$ has order six. It follows that the subgroup of $N(k)$ generated by $\dot{r}_1$ and $\dot{r}_2$ projects isomorphically onto W.

Fix a subgroup $U \subset W$ and a Galois extension E/k with $\mathrm{Gal}(E/k) \simeq U$. Let $\mathrm{Aut}_W(U)$ be the image of the natural map from the normalizer $N_W(U)$ to $\mathrm{Aut}(U)$. Then the W-conjugacy classes of homomorphisms $\varphi : \Gamma \to W$ which factor through an isomorphism $\mathrm{Gal}(E/k) \simeq U$ are in bijection with the cosets of $\mathrm{Aut}_W(U)$ in $\mathrm{Aut}(U)$. In G_2 we actually have $\mathrm{Aut}_W(U) = \mathrm{Aut}(U)$ except when U is generated by a pair of orthogonal reflections, in which case $\mathrm{Aut}_W(U) = 1$ and $\mathrm{Aut}(U) \simeq S_3$. Thus the extension E/k gives a unique stable class of maximal tori in G, except when E/k is biquadratic, when we get six stable classes.

Since the extension $N(k) \to W$ splits, we have $W_\varphi(k) = C_W(U)$ and the set of rational classes of maximal tori in the stable class corresponding to φ is again in bijection with the linear orbits of $C_W(U)$ in the coinvariant group $[X_U]_{\mathrm{tor}}$. The following table gives the number of rational classes in each stable class of non-split tori in G_2. The relevant Galois extensions E/k have Galois groups isomorphic to the dihedral group D_n of order $2n$ or to the cyclic group C_n of order n, for some $n \in \{2, 3, 6\}$. The subgroups A_2 (resp. $\tilde{A}_2$) are generated by reflections about long (resp. short) root hyperplanes.

$U = \operatorname{im}\varphi$	$C_W(\varphi)$	$[X_\varphi]_{\rm tor}$	orbits
$G_2 \simeq D_6$	$\langle -1\rangle$	0	1
$A_2 \simeq D_3$	$\langle -1\rangle$	3	$1+2$
$\tilde{A}_2 \simeq D_3$	$\langle -1\rangle$	0	1
$2A_1 \simeq D_2$	$2A_1$	2	$1+1$
$\langle c\rangle \simeq C_6$	$\langle c\rangle$	1	1
$\langle c^2\rangle \simeq C_3$	$\langle c\rangle$	3	$1+2$
$\langle c^3\rangle = \langle -1\rangle$	W	2^2	$1+3$
$\langle r_1\rangle \simeq C_2$	$2A_1$	0	1
$\langle r_2\rangle \simeq C_2$	$2A_1$	0	1

The column "orbits" gives the partition of $[X_\varphi]_{\rm tor}$ into $C_W(\varphi)$-orbits. For example, if $\operatorname{im}\varphi = C_3$, so that $C_W(\varphi)$ is cyclic generated by a Coxeter element, then there are two orbits in $X_\varphi = [X_\varphi]_{\rm tor}$ of size 1 and 3, whose corresponding tori have small rational Weyl groups cyclic of orders 6 and $6/3 = 2$, respectively.

6.7 Triviality of the cocycle: Unramified tori

Let the residue field $\mathfrak{f}$ of our p-adic field k have cardinality q and let $\bar{\mathfrak{f}}$ be an algebraic closure of $\mathfrak{f}$. The kernel of the natural action of Γ on $\bar{\mathfrak{f}}$ is the inertia subgroup $\Gamma_0 \lhd \Gamma$, whose fixed field in $\bar{k}$ is a maximal unramified extension K/k, and

$$\Gamma/\Gamma_0 \simeq \operatorname{Gal}(K/k) \simeq \operatorname{Gal}(\bar{\mathfrak{f}}/\mathfrak{f}).$$

We fix an element $\mathrm{F} \in \Gamma$ whose inverse projects to the q-power map in $\operatorname{Gal}(\bar{\mathfrak{f}}/\mathfrak{f})$. A cocycle or homomorphism from Γ into another group is called *unramified* if it is trivial on Γ_0. Such a map is completely determined by its value on F. A k-torus S is called unramified if the Γ_0 acts trivially on $X_*(S)$.

Assume that G splits over K. Equivalently, our maximally split torus T is unramified. This means that ψ_G is unramified, and is determined by an element $\vartheta := \psi_G(\mathrm{F}) \in \operatorname{Aut}(R, B)$. A twisted torus T_ξ is unramified precisely when the cocycle $\xi : \Gamma \to W$ is unramified, in which case ξ is determined by an element $w := \xi(\mathrm{F}) \in W$. If $\varphi : \Gamma \to {}^L W$ is the Langlands parameter associated to φ as in section **??** we have $\varphi(\mathrm{F}) = w\vartheta$.

Lemma 6.11 *If T_ξ is unramified then the linear and affine actions of $W_\xi(k)$ on $H^1(k, T_\xi)$ coincide.*

Proof: Since G is K-split and k-quasi-split, there is a F-stable hyperspecial vertex o in the apartment $\mathcal{A}(K)$ of $T(K)$ in the Bruhat-Tits building of $G(K)$. The group $N(K)$ acts on $\mathcal{A}(K)$ and we let $N(K)_o$ denote the stabilizer of o in $N(K)$. The subgroup $T(K)_o = T \cap N(K)_o$ is a pro-algebraic $\mathfrak{f}$-group acting trivially on $\mathcal{A}(K)$.

Since ϑ preserves B, there is an extension

$$1 \longrightarrow T[2] \longrightarrow \dot{W} \longrightarrow W \longrightarrow 1$$

where $T[2] = \{t \in T : \ t^2 = 1\}$ and $\dot{W}$ is an F-stable finite subgroup of $N(K)_o$ [34, Prop.3].

Let $w = \xi(\mathrm{F})$. Any lift $\dot{w} \in \dot{W}$ of w gives a lift of ξ to a cocycle $\dot{\xi}$ in $\dot{W}$ whose homomorphism $\tilde{\dot{\xi}}$ is unramified and such that $\dot{\xi}(\mathrm{F}) = \dot{w}$.

Let $x \in W_\xi(k)$ and choose any lift $\dot{x} \in N(K)$ of x and let $d = \delta_\xi(\dot{x}) = \dot{x}\dot{w}\,\mathrm{F}(\dot{x})^{-1}\dot{w}^{-1}$. Applying the Lang-Steinberg theorem to the pro-algebraic $\mathfrak{f}$-group $T(K)_o$ twisted by w, we get an element $t \in T(K)_o$ such that $\dot{t}\,\mathrm{F}_w(\dot{t})^{-1} = d$. Replacing $\dot{x}$ by $\dot{x}t^{-1}$ gives a new lift of $\dot{x}$ in N for which $\delta_\xi = 1$. Hence δ_ξ is trivial, so the linear and affine actions coincide, as claimed. ■

We recover a result proved in [13, 2.11]. Let $\xi : \Gamma \to W$ be an unramified cocycle with $\xi(\mathrm{F}) = w$ and let $X_{w\vartheta} = [X/(1 - w\vartheta)X]_{\mathrm{tor}} \simeq H^1(k, T_\xi)$. The stable class $\mathcal{T}_w$ corresponding to ξ consists of unramified maximal tori in G.

Corollary 6.12 *The rational classes of maximal tori in $\mathcal{T}_w$ are in bijection with the orbits of the centralizer $C_W(w\vartheta)$ on $X_{w\vartheta}$ under the linear action. If $T_\lambda \in \mathcal{T}_w$ is a maximal torus in the rational class corresponding to $\lambda \in X_{w\vartheta}$, then the stabilizer $C_W(w\vartheta, \lambda)$ is isomorphic to the small rational Weyl group of T_λ.*

6.8 Supercuspidal L-packets

In this section we briefly indicate how coinvariant representations appear in the local Langlands correspondence. For more background on the local Langlands correspondence from this point of view, see [16], for example.

To simplify the discussion, we assume our p-adic group G is simply-connected, semisimple and split over k. The dual group of G the complex semisimple Lie group $\hat{G}$ of adjoint type whose root datum is dual to that of G. A *supercuspidal parameter* for G is a continuous homomorphism $\varphi : \Gamma \to \hat{G}$ whose image has finite centralizer $A_\varphi = C_{\hat{G}}(\varphi)$. Two parameters are regarded as equivalent if they are conjugate by $\hat{G}$.

In this setting, the local Langlands conjecture predicts that each equivalence class of supercuspidal parameters φ should correspond to a finite set Π_φ of irreducible supercuspidal representations of $G(k)$ and that there should be a bijection between Π_φ and the set of irreducible representations of the finite group A_φ.

Fix a supercuspidal parameter $\varphi : \Gamma \to \hat{G}$. The image $D = \varphi(\Gamma)$ is the Galois group of a finite extension E/k, with lower ramification filtration by normal subgroups of D:

$$D \geq D_0 \geq D_1 \geq \cdots \geq D_m > 1,$$

where D_0 is the inertia subgroup of D and D_1, the wild ramification group, is the p-Sylow subgroup of D_0.

Suppose that for some $j \geq 0$ the group D_j is contained in a maximal torus $\hat{T}$ of $\hat{G}$ and moreover that D_j is in "general position" in $\hat{T}$, meaning that $\hat{T} = C_{\hat{G}}(D_j)$ is the full centralizer of D_j in $\hat{G}$. Then D is contained in the normalizer $\hat{N}$ of $\hat{T}$ and we have a cocycle

$$\bar{\varphi} : \Gamma \xrightarrow{\varphi} \hat{N} \longrightarrow W$$

with coinvariant representation

$$X_{\bar{\varphi}} \simeq \mathrm{Irr}(A_\varphi) \simeq H^1(k, T_{\bar{\varphi}}).$$

Thus, our L-packet Π_φ should have the form

$$\Pi_\varphi = \{\pi_\lambda : \ \lambda \in X_{\bar\varphi}\}$$

and it is natural to expect the tori in the rational class containing λ to be involved in the construction of the representation π_λ.

Such L-packets have been constructed in [13], [20], [27] and [17]. We confine ourselves here to the settings of [13] and [20], where φ is unramified. This means $j = 0$ and the image of D in W is generated by an elliptic element $w \in W$ arising from the image $\varphi(\mathrm{F})$ of a Frobenius element in Γ.

Thus, $X_{\bar\varphi} = X_w$ is a coinvariant representation of $W_{\bar\varphi}(k) = C(w)$ as considered in the first part of the paper and the torus $T_{\bar\varphi} = T_w$ is unramified, so that the affine and linear actions of $C(w)$ on X_w coincide, by Lemma 6.11.

The L-packet Π_φ is constructed as follows. For each $\lambda \in X_w$ we have an embedding $\mathrm{Ad}(g) : T_w \hookrightarrow T_\lambda \subset G$, where $g \in G(\bar k)$ splits the class of λ in G, and the image T_λ is an anisotropic maximal torus of G contained in a unique maximal compact subgroup K_λ. The parameter φ determines a character $\chi : T_w(k) \to \mathbb{C}^\times$ by the local Langlands correspondence for T_w. Transporting χ to $T_\lambda(k)$ and using Deligne-Lusztig induction, we get a representation κ_λ of K_λ, whence by compact induction an irreducible supercuspidal representation

$$\pi(\chi, \lambda) = \mathrm{ind}_{K_\lambda}^{G(k)} \kappa_\lambda.$$

These representations comprise the L-packet

$$\Pi_\varphi = \{\pi(\chi, \lambda) : \ \lambda \in X_w\}.$$

To make this more explicit, we should give the conjugacy class of K_λ in terms of λ. Since T_λ determines K_λ, the latter depends only on the rational class of T_λ, which in turn depends only on the $C(w)$-orbit of λ. Thus, the $C(w)$-orbits in X_w correspond to the maximal compact subgroups appearing as inducing data for the representations in Π_φ. More precisely, for $y \in C(w)$ we have the equivariance property [27]

$$\pi(\chi^y, \lambda) \simeq \pi(\chi, \varrho_w(y)\lambda), \tag{33}$$

where $C(w)$ acts on characters of $T_w(k)$ via its isomorphism with the big rational Weyl group of T_w from section 6.2, and ϱ_w is the coinvariant representation of $C(w)$ on X_w.

The maximal compact subgroup K_λ is the stabilizer in $G(k)$ of a vertex x_λ in the Bruhat-Tits building $\mathcal{B}$ of $G(k)$. By conjugating, we can arrange that x_λ belongs to the apartment $\mathcal{A}$ of T in $\mathcal{B}$. The precise definition of x_λ requires a choice of hyperspecial vertex $o \in \mathcal{A}$, by which we identify $\mathcal{A}$ with the vector space $\mathbb{R} \otimes X$. Modulo translations by X (which do not change the $G(k)$-conjugacy class of K_λ), x_λ is the image of λ under the isomorphism

$$(1-w)^{-1} : X_w \xrightarrow{\sim} (1-w)^{-1}X/X \subset \mathcal{A}/X.$$

The image of this map is the subgroup $\tilde T^w$ of elements fixed by w in a maximal torus $\tilde T$ of the complex simply-connected group $\tilde G$ of the same type as G. The type of the vertex x_λ (or K_λ) coincides with the type of the centralizer of the image of x_λ in $\tilde T^w$. Therefore, the conjugacy class of K_λ is the orbit type of λ, as discussed in section 2.2 for E_8. For E_8 we can read off the classes of maximal compact subgroups from Table 1. For example, if w (the image of Frobenius under φ) belongs to the class $A_1^2A_3^3$ in W, then Π_φ contains 64 representations induced from K_λ's of type E_8 ($\times 1$), D_8 ($\times 3$), A_1E_7 ($\times 12$) and A_3D_5 ($\times 48$).

A Appendix: Further remarks on Elliptic trialities

A.1 Elliptic trialities in F_4

Each case of elliptic trialities has special features, relating to other areas of mathematics. We explore these next, starting with the simplest nontrivial case.

The F_4 root lattice $X = Q(F_4)$ is the subgroup of $\mathbb{R}^4$ consisting of vectors whose coordinates are all integers or all half-integers. Identifying the standard basis of $\mathbb{R}^4$ with $1, i, j, k$, the Hamilton quaternion relations impart a ring structure to X. This ring $\mathcal{H}$, with underlying additive group X, is isomorphic to the endomorphism ring $\mathrm{End}(E)$ of the unique supersingular elliptic curve E in characteristic two, with affine equation $y^2 + y = x^3$. We refer to [30] for the basic facts about elliptic curves. The automorphism group of any elliptic curve has order dividing 24 [30, Thm. 10.1] and the curve E attains this maximum: we have $\mathrm{Aut}(E) = \mathcal{H}^\times \simeq SL_2(3)$. This isomorphism is given by the action of $\mathrm{Aut}(E)$ on the group $E[3] = \{P \in E : \ 3P = 0\}$ of 3-torsion points, on which the Weil pairing is a symplectic form invariant under $\mathrm{Aut}(E)$.

A ring isomorphism

$$\theta : \mathcal{H} \xrightarrow{\sim} \mathrm{End}(E)$$

intertwines the quadratic form $\langle x, x\rangle$ on X with the form on $\mathrm{End}(E)$ given by the degree of an endomorphism. Hence θ sends the short roots in X to the units $\mathrm{Aut}(E)$. The Frobenius endomorphism F of E has degree two, so θ sends the long roots in X to the twisted Frobenii $\sigma\,\mathrm{F}$ with $\sigma \in \mathrm{Aut}(E)$.

Fix an elliptic triality $w \in W(F_4)$. Prop. 4.2 shows that

$$C_{W(D_4)}(w) \simeq SL_2(3).$$

The element $\omega := \theta(w \cdot 1) \in \mathrm{Aut}(E)$ satisfies

$$\theta(w\lambda) = \theta(\lambda)\omega, \qquad \text{for all } \lambda \in \mathcal{H}. \tag{34}$$

Since ω has order three, it fixes a unique line in the two-dimensional $\mathbb{F}_3$-vector space $E[3] = \{P \in E : 3P = 0\}$. Let P be a non-identity point in this line. Then the map

$$\mathcal{H} \longrightarrow E[3], \qquad A \mapsto \theta(A) \cdot P$$

induces an an $SL_2(3)$-equivariant isomorphism

$$X_w = \mathcal{H}/(1 - w)\mathcal{H} \xrightarrow{\sim} E[3].$$

We conclude this example with a remark on the 24-cell; this is the unique regular convex self-dual polytope in four dimensions (see [11, chap.8]). It is comprised of 24 octahedra, centered at 24 roots of a fixed length in X. The symmetry group of the 24-cell is $W(F_4)$ and the fixed-point-free triality symmetries of the 24-cell are exactly the elliptic trialities $w \in W(F_4)$ and $C_{W(D_4)}(w) = SL_2(3)$ acts simply-transitively on the 24 octahedra.

We can write w as a product $w = uv$ of commuting trialities u, v, where $u \in W(D_4)$. The element $-u$ has order six and generates a Borel subgroup B of $SL_2(3)$. The B-orbit of an octahedral cell is a solid polyhedral torus, consisting of six octahedra meeting in a sequence of pairwise-common faces. The whole 24-cell, a polyhedral decomposition of the three-sphere, is the union of four such octahedral tori, which are mutually linked.

The subgroup B is also the stabilizer of a vertex under the action of $SL_2(3)$ on the tetrahedron via the map $SL_2(3) \to SL_2(3)/\pm 1 = Alt(4)$. The quotient map $SL_2(3) \to SL_2(3)/B$ thus gives a map from the 24-cell to the tetrahedron, which is a polyhedral analogue of the Hopf fibration $S^3 \to S^2$, in which the fibers have been fattened into linked polyhedral tori made out of octohedra glued at their faces.

A.2 Elliptic trialities in E_6

Let us change coordinates slightly, and view the elliptic curve E above as defined in $\mathbb{P}^2$ by the cubic polynomial $f = X^2Z + Y^3 + XZ^2$. The 3-torsion points on any elliptic curve are also the inflection points, hence are independent of the choice of origin defining the group structure. For our curve E, the 3-torsion points coincide with the $\mathbb{F}_4$-rational points:

$$E[3] = E(\mathbb{F}_4).$$

The polynomial f may be viewed as a hermitian form on $\mathbb{F}_4^3$, and $E(\mathbb{F}_4)$ is the set of f-isotropic lines in $\mathbb{F}_4^3$. The projective unitary group $PU_3(2)$ of f, of order $9 \cdot 24$, acts transitively on the curve E with group structure ignored. The stabilizer of a point in $E(\mathbb{F}_4)$ is a Borel subgroup in $PU_3(2)$ and is isomorphic to $SL_2(3)$. Thus we may identify the points in $E(\mathbb{F}_4)$ with the Borel subgroups of $PU_3(2)$. Given a Borel subgroup B, and letting E_B be the elliptic curve (over $\mathbb{F}_4$) defined by f with identity element B, we have $\mathrm{Aut}(E_B) = B$. To see this explicitly, let B be the stabilizer of $O = [1, 0, 0] \in E$. Then ([30, p.327]) $B = \mathrm{Aut}(E)$ is given in X, Y, Z coordinates by the projective matrices

$$\begin{bmatrix} 1 & us & t \\ 0 & u & s^2 \\ 0 & 0 & 1 \end{bmatrix}, \qquad u \in \mathbb{F}_4^\times, \quad [s, t, 1] \in E(\mathbb{F}_4). \tag{35}$$

The subgroup with $u = 1$ is the quaternion group Q_8; these eight automorphisms happen to be parametrized by the points in $E(\mathbb{F}_4)$ distinct from O. This is explained by the Bruhat decomposition: since $PU_3(2)$ has rank one, the 2-Sylow subgroup of any Borel subgroup acts simply-transitively, by conjugation, on the remaining Borel subgroups.

The group (E, O) acts on itself by translations, and this action turns out to be linear on $E(\mathbb{F}_4)$. To see this, it suffices, by the transitivity of Q_8, to note that translation by the point $P = [0, 0, 1]$ is given by the linear map $[X, Y, Z] \mapsto [Z, Y, X + Z]$. Thus, $E(\mathbb{F}_4)$ embeds in $PU_3(4)$ as a normal subgroup, and we have

$$PU_3(2) = E(\mathbb{F}_4) \rtimes SL_2(3). \tag{36}$$

An elliptic triality $w \in W(F_4)$ is also an elliptic triality in $W(E_6)$. Let $\zeta \in \bar{\mathbb{Q}}^\times$ have order three, and let V_K be the K-vector space $V = \mathbb{Q} \otimes Q(E_6)$ where ζ acts on V via w. The group $C_{W(E_6)}(w)$ preserves the hermitian form h on V_K (see section 3.2). Let X_K be the abelian group $X = Q(E_6)$, viewed as a

$\mathbb{Z}[\zeta]$-module. Since 2 remains prime in $\mathbb{Z}[\zeta]$, the form h induces a hermitian form on the vector space $X_K/2X_K \simeq \mathbb{F}_4^3$. This gives an isomorphism

$$C_{W(E_6)}(w) \simeq U_3(2),$$

in which w maps to a scalar matrix in $U_3(2)$, so that

$$C_{W(E_6)}(w)/\langle w\rangle \simeq PU_3(2).$$

Since all hermitian forms in three variables are equivalent, we see that $C_{E_6}(w)/\langle w\rangle$ is the automorphism group of the curve E with group structure ignored.

There is a connection with Weil representations. In section 4.1, we have seen that $C_{A(E_6)}(w)$ is a maximal parabolic subgroup in $Sp_4(3)$ with Heisenberg group H for unipotent radical. The Levi subgroup of $C_{A(E_6)}(w)$ is $\mathbb{F}_3^\times \times SL_2(3)$, where the first factor is generated by the graph automorphism of E_6. It follows that

$$C_{W(E_6)}(w) = SL_2(3) \ltimes H.$$

The center of H is generated by w. From section 3.1, the eigenspaces $\bar{V}(w,\zeta)$ and $\bar{V}(w,\zeta^2)$ are three dimensional irreducible representations of $C_{W(E_6)}(w)$, affording the central characters $w \mapsto \zeta$, $w \mapsto \zeta^2$ of H. It follows that $\bar{V}(w,\zeta)$ and $\bar{V}(w,\zeta^2)$ are the Weil representations of $C_{W(E_6)}(w) = SL_2(3) \ltimes H$ [15, 2.4].

The action of $C_{W(E_6)}(w)$ on X_K and X_w may also be seen in the Hessian configuration, much studied in the 19th century, for which a complete account in the classical style can be found in [4, 7.3]. The projective curve C_λ with equation $x^3+y^3+z^3-\lambda xyz=0$ is singular precisely for $\lambda=\infty,1,\zeta,\zeta^2$, where C_λ becomes a triangle. The resulting twelve lines in $\mathbb{P}^2$ form the Hessian configuration, whose group of collineations is $PU_3(2)$. This is proved in [4] by a judicious labelling of coordinates, which identifies the Hessian configuration with the configuration of all lines in the affine plane over $\mathbb{F}_3$, whose symmetry group is $PU_3(2)$, as we have seen in (36).

This can be seen more naturally using the coinvariants X_w and the twelve K-equivalence classes of roots in E_6 as follows. Each K-equivalence class S determines a line KS in V_K, whence a hyperplane in the complexified dual space $\mathbb{V}=[V_K\otimes_K\mathbb{C}]^*$. These hyperplanes give the Hessian configuration in $\mathbb{P}(\mathbb{V})$. On the other hand, by Lemma 4.4, S determines a nonsingular line in $X_w \simeq \mathbb{F}_3^3$, whence a hyperplane in the dual space X_w^*. All hyperplanes in X_w^* arise except the one annihilated by the singular line in X_w, which is the radical of the form $\langle\ ,\ \rangle_w$. We denote this singular hyperplane by H_0. Thus, the twelve K-equivalence classes S are in bijection with the lines in the affine space $\mathbb{P}(X_w^*)-\{H_0\}$. Since each of these modular lines comes from reduction modulo $P=(1-\zeta)\mathbb{Z}[\zeta]$ of a complex line in $\mathbb{P}(\mathbb{V})$, this shows that the complex and modular Hessian configurations coincide.

A.3 Elliptic trialities in E_8

Let w be an elliptic triality in $W(E_8)$, let $X=Q(E_8)$, $V=\mathbb{Q}\otimes X$, and let $K=\mathbb{Q}(\zeta)$ be generated by an element of order three in $\bar{\mathbb{Q}}^\times$. Each K-equivalence class of roots is an orbit of $-w$, and is the vertex set of one of Coxeter's 40 planar hexagons (cf. [10, p.480]). The centralizer $C_{E_8}(w)$of w in $W(E_8)$ has order

$$|C_{E_8}(w)| = 12 \cdot 18 \cdot 24 \cdot 30 = 155520.$$

Here $12, 18, 24, 30$ are the degrees of $W(E_8)$ which are divisible by 3. We have

$$C_{E_8}(w) = \langle w \rangle \times \bar{C}_{E_8}(w),$$

where $\bar{C}_{E_8}(w)$ is the subgroup of $C_{E_8}(w)$ having determinant one on V_K and has order

$$|\bar{C}_{E_8}(w)| = 51840.$$

From Prop. 4.2, the representation of $C_{E_8}(w)$ on X_w gives an isomorphism

$$\bar{C}_{E_8}(w) \simeq Sp_4(3). \tag{37}$$

Just as for E_6, there is also a mod 2 picture. Again the hermitian form h on V_K becomes a cubic polynomial h_2 on $X_K/2X_K$. This time we get a two-fold covering

$$1 \longrightarrow \{\pm 1\} \longrightarrow C_{E_8}(w) \longrightarrow U_4(2) \longrightarrow 1, \tag{38}$$

under which w maps to a generator of the center of $U_4(2)$. This last group has order

$$|U_4(2)| = 2^6(2^4-1)(2^3+1)(2^2-1)(2+1) = 2^6 \cdot 3^5 \cdot 5$$

and preserves the nonsingular cubic surface $S \subset \mathbb{P}^3$ defined by h_2.

A line on $S(\mathbb{F}_4)$ is an h-isotropic plane in $\mathbb{F}_4^4$. The group $U_4(2)$ acts transitively on isotropic planes and the stabilizer of one such is a semidirect product $GL_2(4) \ltimes \mathbb{F}_2^4$, of order $2^6(2^4-1)(2^2-1)$. Since

$$\frac{2^6(2^4-1)(2^3+1)(2^2-1)(2+1)}{2^6(2^4-1)(2^2-1)} = 27,$$

This shows that $U_4(2)$ acts transitively on the lines in S and that every such line is rational over $\mathbb{F}_4$. Not all lines are rational over $\mathbb{F}_2$, so the action of $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$ on the set of lines is nontrivial.

The symmetry group of the configuration of 27 lines in S is $W(E_6)$, whose order $|W(E_6)| = 2^7 \cdot 3^4 \cdot 5$ is twice that of $PU_4(2)$. Since $W(E_6)$ has a unique character of order two, namely the sign character ϵ, the action of $U_4(2)$ on the configuration of lines in S gives an isomorphism of simple groups

$$PU_4(2) \xrightarrow{\sim} W(E_6)_+ = \ker \epsilon.$$

The nonidentity coset of $PU_4(2)$ in $W(E_6)$ contains the nontrivial element of $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$ acting on the lines in S. Lifting back to the two-fold cover $C_{E_8}(w)$ of $U_4(2)$ via (38), we find that

$$C_{E_8}(w) \simeq \langle w \rangle \times \widetilde{W(E_6)}_+,$$

where $\widetilde{W(E_6)}_+$ is a two-fold cover of $W(E_6)_+$. Comparing with (37), we recover the isomorphism (cf. [7])

$$Sp_4(3) \simeq \widetilde{W(E_6)}_+.$$

Since $Sp_4(3)$ equals its own derived group, the covering

$$\begin{array}{ccc} Sp_4(3) & \hookrightarrow & SU_4 \\ \downarrow & & \downarrow \\ W(E_6)_+ & \hookrightarrow & SO_6 \end{array}$$

is non-split, in complete analogy with the binary tetrahedral covering

$$\begin{array}{ccc} Sp_2(3) & \hookrightarrow & SU_2 \\ \downarrow & & \downarrow \\ W(A_3)_+ & \hookrightarrow & SO_3. \end{array}$$

In summary, we have three avatars of the group $\bar{C}_{E_8}(w)$ of order 51840:

$$\begin{aligned} \bar{C}_{E_8}(w) &\simeq Sp_4(3) && \text{from the coinvariant representation on } X_w, \\ &\simeq PU_4(2) && \text{from the hermitian form } h_2 \text{ on } X_K/2X_K, \\ &\simeq \widetilde{W(E_6)}_+ && \text{from the 27 lines on the cubic surface } S:(h_2=0). \end{aligned}$$

The eigenspaces $\bar{V}(w,\zeta)$ and $\bar{V}(w,\zeta^2)$ are in duality via the pairing $\langle\ ,\ \rangle$ on $\bar{V}$ and afford the two distinct four dimensional representations of $Sp_4(3)$ over $\bar{\mathbb{Q}}$ [7]. The exterior squares of these representations are irreducible and isomorphic to one another; let

$$\Lambda := \Lambda^2\bar{V}(w,\zeta) \simeq \Lambda^2\bar{V}(w,\zeta^2).$$

As a representation of $Sp_4(3)$, Λ is the unique cuspidal unipotent representation, denoted by θ_{10} in [33]. As a representation of $U_4(2)$, Λ is the unipotent representation corresponding to the partition $4 = 2+1+1$. As shown in [18], the representation $\Lambda \otimes \bar{\mathbb{Q}}_\ell$ can be realized on the quotient of the ℓ-adic cohomology group $H^2(S)$ by the one-dimensional subspace spanned by a hyperplane section. We note that, for the elliptic trialities in F_4 and E_8, the middle exterior powers of $\bar{V}(w,\zeta)$ are realized in the cohomology groups $H^1(E)$ and $H^2(S)$, respectively.

A.4 Maschke's view

The representation of $\bar{C}_{E_8}(w)$ on V_K gives a subgroup $G \subset GL_4(K)$ of order 51840 which was discovered by Witting and whose invariant theory was determined by Maschke [22] in 1888, before the theory of root systems was developed. Maschke first shows that G is a nonsplit two-fold cover of its image in $G/\{\pm1\} \subset PGL_4(K)$. This is the covering (38) above. Next, Maschke computes the stabilizer H in G of a coordinate hyperplane $V_0 \subset V_K$ and shows that the image H' of H in $PGL(V_0)$ is the Hessian group of order 216, concluding from this that $|H| = 6 \cdot 216$. In our context, H is the image of $C_{E_7}(w) = \{\pm1\} \times C_{E_6}(w)$ in

$\bar{C}_{E_8}(w)$ and the projection $C_{E_6}(w) \to H'$ is the Hessian covering from section A.2 (note that the present w contains an elliptic triality in $W(E_6)$ as a factor).

Maschke goes on to show that the H- and G-invariant polynomials on V_0 and V_K are generated by explicit polynomials whose degrees ($6, 12, 18$ and $12, 18, 24, 30$, respectively) are as we would find today from Springer's theory.

B Appendix: A variation on the notion of K-equivalence: $W(H_4) \hookrightarrow W(E_8)$

Let $w \in W(E_8)$ be cyclotomic of order 10. The operator $\tau = w + w^{-1} \in \mathrm{End}(V)$ satisfies the equation $\tau^2 = \tau + 1$ of the golden ratio. The field $k = \mathbb{Q}(\sqrt{5}) \simeq \mathbb{Q}(\tau)$ embeds in $\mathrm{End}(V)$, via $\frac{1}{2}(1 + \sqrt{5}) \mapsto \tau$, and we let V_k be the k-vector space with underlying abelian group V. We will show that the subgroup $C(\tau)$ of elements in $W(E_8)$ commuting with τ in $\mathrm{End}(V)$ is a reflection group on V_k, isomorphic to the non-crystallographic Coxeter group $W(H_4)$. From the equation

$$w^2 - w + 1 - w^{-1} + w^{-2} = 0,$$

it follows that

$$\langle \alpha, w\alpha \rangle = \langle \alpha, w^2\alpha \rangle + 1 \tag{39}$$

for every $\alpha \in R$, which implies that $\langle \alpha, w\alpha \rangle \in \{0, 1\}$. For $i \in \{0, 1\}$, let $R_i = \{\alpha \in R : \langle \alpha, w\alpha \rangle = i\}$.

Lemma B.1 *The operator τ maps R_0 bijectively onto R_1, and has the following properties:*

1. $\langle \alpha, \tau\alpha \rangle = 0$*;*
2. $s_\alpha s_{\tau\alpha} \in C(\tau)$ *for all* $\alpha \in R_0$*;*
3. *The w-orbits of α and $\tau\alpha$ comprise a root subsystem of type A_4.*

Proof: If $\langle \alpha, w\alpha \rangle = 0$, then $\langle \alpha, w^2\alpha \rangle = -1$ by (39), so that $\alpha + w^2\alpha \in R$. Hence $\tau\alpha = w^{-1}(\alpha + w^2\alpha) \in R$. It is straightforward to check that

$$\langle \tau\alpha, \tau w\alpha \rangle = 1, \qquad \text{and} \quad \langle \alpha, \tau\alpha \rangle = 0.$$

The first of these equations shows that $\tau\alpha \in R_1$. Using $\tau^2 = \tau + 1$ a straightforward calculation shows that τ commutes with $s_\alpha s_{\tau\alpha}$, proving 2. For the bijectivity, note that $\tau - 1$ sends $R_1 \to R_0$ and $\tau(\tau - 1) = 1$. For 3, one checks that $\{w\alpha,\ w^3\alpha,\ \alpha,\ w^2\alpha\}$ forms a base of an A_4. ■

From Lemma B.1, it follows that the k-equivalence classes are the subsystems of R of the form

$$S = \{\pm\alpha, \pm\tau\alpha\} \simeq 2A_1, \qquad \text{for} \quad \alpha \in R_0.$$

These give 60 k-reflections $s_\alpha s_{\tau\alpha}$ generating a reflection subgroup $C(\tau)^\circ \subset C(\tau)$. From the classification of real reflection groups, we see that $C(\tau)^\circ$ is the Coxeter group of type H_4. We no longer know *a priori* that $C(\tau)$ is a reflection group.

To see the Coxeter generators of $C(\tau)^\circ$, number the simple roots of E_8 as shown:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & 8 & & \end{matrix} \tag{40}$$

and let s_i be the corresponding simple reflections. Choose a "bipartite" Coxeter element

$$v = s_2 s_4 s_6 s_8 s_1 s_3 s_5 s_7$$

(writing s_i for s_{α_i}). The element $w = v^3$ is cyclotomic of order ten. One checks that

$$\alpha_1, \alpha_2, \alpha_3, \alpha_8 \in R_0, \qquad \alpha_4, \alpha_5, \alpha_6, \alpha_7 \in R_1$$

and that

$$\tau : \alpha_1 \mapsto \alpha_7, \quad \alpha_2 \mapsto \alpha_6, \quad \alpha_3 \mapsto \alpha_5, \quad \alpha_8 \mapsto \alpha_4.$$

Thus we recover the "inflation map" of [23] (defined there in terms of icosians). As in [ibid.] the Coxeter relations in $W(E_8)$ immediately imply that the k-reflections

$$r_1 = s_1 s_7, \quad r_2 = s_2 s_6, \quad r_3 = s_3 s_5, \quad r_4 = s_4 s_8$$

satisfy the Coxeter relations of $W(H_4)$, according to the diagram 1—2—3$\overset{5}{—}$4.

We now show that $C(\tau)^\circ = C(\tau)$. Since its minimal polynomial is irreducible mod 2, τ gives an $\mathbb{F}_4$-structure to the abelian group $X/2X$. The quotient $C(\tau)/\pm 1$ is the subgroup of $O_8^+(2)$ acting $\mathbb{F}_4$-linearly on $X/2X$. Hence $C(\tau)/\pm 1$ is an orthogonal group in four variables over $\mathbb{F}_4$. There are two such groups: $O_4^\epsilon(4)$, where $\epsilon = \pm$. Since $|O_4^\epsilon(4)| = 2 \cdot 4^2(4^2 - \epsilon 1)(4^2 - 1)$ and $C(\tau)$ contains the subgroup $C(\tau)^\circ = W(H_4)$ of order 120^2, it follows that $\epsilon = +$ and that $C(\tau)^\circ = C(\tau)$ as claimed.

References

[1] J. D. Adler, *Refined anisotropic K-types and supercuspidal representations*, Pacific J. Math., **185** (1998), pp. 1–32.

[2] E. Bayer-Fluckiger and I. Suarez, *Ideal lattices over totally real number fields and Euclidean minima*, Arch. Math. (Basel), **86** (2006), pp. 217-225.

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

[4] E. Brieskorn and H. Knörrer, *Plane Algebraic Curves*, Birkhäuser, 1981.

[5] R. Carter, *Finite Groups of Lie Type*, Wiley, 1985.

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

[7] J.H. Conway, et al. *ATLAS of finite groups*, Clarendon Press, Oxford, 1985.

[8] J.H. Conway and N.J.A. Sloan *Sphere Packings, Lattices and Groups*, Springer, 1999.

[9] J.H. Conway and D.A. Smith *On quaternions and octonions*, A.K.Peters, 2003.

[10] H.S.M. Coxeter, *The polytope* 2_{21}, *whose twenty-seven vertices correspond to the lines on the general cubic surface*, Am. J. Math., **61** (1940), pp. 457-486.

[11] ———, *Regular polytopes*, Dover, 1973.

[12] S. DeBacker, *Parametrizing conjugacy classes of maximal unramified tori*, Mich. Math. J., **54** (2006), pp. 157–178.

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

[14] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math., **103** (1976), pp. 103–161.

[15] P. Gerardin, *Weil representations associated to finite fields*, Jour. of Alg., **46** (1977), pp. 54–101.

[16] B. H. Gross and M. Reeder, *From Laplace to Langlands via representations of orthogonal groups*, Bull. Am. Math. Soc., **43** (2006), pp. 163–205.

[17] ———, *Arithmetic invariants of discrete Langlands parameters*, preprint, 2009.

[18] R. Hotta and K. Matsui *On a Lemma of Tate-Thompson*, Hiroshima Math. J., **8** (1978), pp. 255–268.

[19] V. Kac *Infinite dimensional Lie algebras*, 3rd ed., Cambridge, 1995.

[20] D. Kazhdan and Y. Varshavsky, *Endoscopic decomposition of characters of certain cuspidal representations*, Electron. Res. Announc. Amer. Math. Soc., **10** (2004), pp. 11-20.

[21] R. Kottwitz *Isocrystals with additional structure. II*, Compositio Math., **109** (1997), pp. 255–339.

[22] H. Maschke, *Aufstellung des vollen Formensystems einer quaternären Gruppe von 51840 linearen Substitutionen*, Math. Ann., **33** (1888), pp. 317–344.

[23] R. Moody and J. Patera, *Quasicrystals and icosians*, J. Phys. A: Math. Gen., **26** (1993), pp. 2829-2853.

[24] M.S. Raghunathan, *Tori in quasi-split groups*, J. Ramanujan Math. Soc., **19** (2004), no. 4, pp. 281-287.

[25] M. Rapaport *A guide to the reduction modulo* p *of Shimura varieties*, Astérisque, **298** (2005), pp. 271–318.

[26] M. Reeder, *Level-two structure of simply-laced Coxeter groups*, J. Alg, **285** (2005), pp. 29-57.

[27] ______, *Supercuspidal L-packets of positive depth and twisted Coxeter elements*, J. reine angew. Math., **620**, (2008), pp. 1-33.

[28] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, 2002.

[29] G.C. Shephard, J.A. Todd *Finite unitary reflection groups*, Canadian J. Math., **6** (1954), pp. 274–304.

[30] J. Silverman *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

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

[32] T. A. Springer and R. Steinberg, *Conjugacy Classes*, Seminar in algebraic groups and related finite groups, Lecture Notes in Math., **131** (1970), pp. 167–266.

[33] B. Srinivasan, *Characters of the finite symplectic group $Sp(4,q)$*, Trans. Amer. Math. Soc., **131** (1968), pp. 488–525.

[34] J. Tits, *Sur les constantes de structure et le théorèm d'existence des algèbres de Lie semi-simples*, Inst. Hautes Études Sci. Publ. Math., No. 31 (1966), pp. 21-58.

[35] E.B. Vinberg, *The Weyl group of a graded Lie algebra*, Math. USSR Isvestiya, **10** (1976), No. 3, pp. 463–495.