Cyclotomic structures on root lattices

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

July 28, 2006

1 Introduction

The centralizer $C(w)$ of an element w in a Weyl group W plays an important role in the structure and representation theory of split reductive groups G over finite and p-adic fields k, where W is the absolute Weyl group of G.

If k is finite, this is well-known: the element w determines a maximal k-torus $T_w \subset G$ and $C(w)$ may be identified with the k-rational points in the Weyl group $W(T_w, G)$ of T_w in G. For every character χ of $T_w(k)$, the Deligne-Lusztig construction [12] gives a virtual representation $R^G_{T_w}(\chi)$ of $G(k)$ whose self-intertwining number is the order of the stabilizer of χ in $C(w)$.

If k is p-adic then w determines an unramified maximal k-torus T_w, which now can be embedded as a maximal torus in G in several ways. Assume G is simply-connected. Each class in the Galois cohomology group $H^1(k, T_w)$ determines an embedding $T_w \hookrightarrow G$ and two classes in $H^1(k, T_w)$ give $G(k)$-conjugate embeddings iff they are conjugate under the natural action of $C(w)$ on $H^1(k, T_w)$. Let $C(w, \rho)$ be the stabilizer of the class $\rho \in H^1(k, T_w)$. If $T_w \xrightarrow{\sim} T^\rho_w \subset G$ is an embedding belonging to the class $\rho \in H^1(T_w, G)$, then $C(w)$ is isomorphic to the big Weyl group of k-rational elements in $W(T^\rho_w, G)$ and $C(w, \rho)$ is isomorphic to the small Weyl group of elements in $W(T^\rho_w, G)$ which have representatives in $G(k)$.

On the representation theory side, suppose w is elliptic (i.e. T_w is anisotropic) and χ is a sufficiently regular character of $T_w(k)$. Then, in accordance with the

local Langlands conjecture, one can construct (cf. [11], [19]) a finite set of representations $\Pi_w(\chi) = \{\pi(\chi, \rho) : \ \rho \in H^1(k, T_w)\}$, with the equivariance property:

$$\pi(\chi^y, \rho) \simeq \pi(\chi, y \cdot \rho) \qquad \text{for} \quad y \in C(w),$$

which implies that $\pi(\chi, \rho)$ and $\pi(\chi, y \cdot \rho)$ are induced from the same maximal compact subgroup of $G(k)$ and that their characters agree near the identity, at least in certain cases [11, 12.4.3]. Similar results hold for nonsplit unramified groups G, where w is now an element of the group A of automorphisms of the absolute root system of G, such that the coset of w in A/W corresponds to the splitting data of G over k.

Thus we are led to study the action of $C(w)$ on $H^1(k, T_w)$, for $w \in A$. This is a problem in basic Lie theory which arises in diverse contexts. It can be stated in elementary terms: if $X = \mathrm{Hom}(GL_1, T_w)$ denotes the cocharacter group of T_w then Tate-Nakayama duality gives a natural isomorphism

$$H^1(k, T_w) \simeq X_w,$$

where $X_w := X/(1-w)X$ is the group of coinvariants of w in X. The group X_w is finite because w is elliptic. Equivalently, the number $m := M(1)$ is nonzero, where $M(t)$ is the minimal polynomial of w on X. It is easy to show (see section 4.1 below) that $mX_w = 0$ and that there is a natural $\mathbb{Z}/m\mathbb{Z}$-valued skew-symmetric pairing $\langle\ ,\ \rangle_w$ on X_w, preserved by the natural action of $C(w)$ on X_w. Thus, we have a natural homomorphism

$$\varrho_w : C(w) \longrightarrow Sp(X_w),$$

where $Sp(X_w)$ is the group of automorphisms of X_w preserving $\langle\ ,\ \rangle_w$, and our problem reduces to studying the image of ϱ_w.

For classical groups, this is straightforward (cf. [14, chap.14]). Exceptional groups, especially E_8, encourage the search for uniform, Lie theoretic methods for determining the image of ϱ_w.

Two cases appear already in Bourbaki [2]. If w is a Coxeter element, then $C(w)$ is generated by w, X_w is isomorphic to the fundamental group of the dual group of G, the form $\langle\ ,\ \rangle_w$ is identically zero, and ϱ_w is trivial. (This case is not without interest for p-adic groups, see [19].) The other case is where W has type E_n and $w = -1$. Here $C(w) = W$ and $X_w = X/2X$. The form $\langle\ ,\ \rangle_w$ arises from a quadratic form q on $X/2X$. Using methods that apply only to this case ([2] or [18]), one can show that the image of ϱ_w is the orthogonal group of q.

We will see that for $w \neq -1$ we often have $\langle\ ,\ \rangle_w$ nondegenerate and $\operatorname{im} \varrho_w = Sp(X_w)$. The implication for the corresponding L-packets $\Pi_w(\chi)$ is that all the nongeneric representations in the packet are induced from the same maximal compact subgroup and, in certain cases, behave the same near the identity of $G(k)$.

A general approach to ϱ_w must begin with a Lie-theoretic description of $C(w)$, on which it seems that the only general results are due to Springer [22]. These apply when w is regular (no eigenvector of w lies on a root hyperplane), so we confine ourselves to regular w. Then, by Springer, we know that $C(w)$ acts faithfully on a regular eigenspace of w as a (complex) reflection group whose degrees are those degrees of W which are divisible by the order of w. This tells us the order of $C(w)$ and the number of reflections in $C(w)$. However, this is not enough to determine the image of ϱ_w, for Springer arrives at his results via invariant theory, which does not actually produce any reflections in $C(w)$, or give the order of the reflections, or say if $C(w)$ is an irreducible reflection group. The degrees alone do not answer these questions and they do not determine the isomorphism type of the reflection group $C(w)$.

We can sharpen Springer's results for certain regular elements. We say that w is **cyclotomic** if its minimal polynomial $M(t)$ is irreducible over $\mathbb{Q}$. For G_2, F_4 and E_8 this is not an additional restriction: in these cases the elliptic regular elements in W are precisely the nonidentity cyclotomic elements.

Let $V = \mathbb{Q} \otimes X$ be the rational reflection representation of W. The $\mathbb{Q}$-subalgebra in $\operatorname{End}(V)$ generated by a cyclotomic element w of order d is a cyclotomic field $K = \mathbb{Q}(\zeta_d)$, and $C(w)$ is the subgroup of W acting K-linearly on V. Cyclotomic structures on the E_8-root lattice for $K = \mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4)$ were known in the 19th century [6]. Recent literature on lattice theory [1] mentions the $\mathbb{Q}(\zeta_9)$-structure on E_6 and the $\mathbb{Q}(\zeta_{15})$-structure on E_8. All of these cyclotomic structures arise from cyclotomic elements in W. In the first part of this paper we use the field K to find the reflections in the centralizer of a cyclotomic element.

More general fields K are also of interest. For example, in $W(E_8)$ there is a cyclotomic element w of order ten, such that $w + w^{-1}$ generates a field $K \simeq \mathbb{Q}(\sqrt{5})$ whose centralizer in $W(E_8)$ is the exceptional Coxeter group $W(H_4)$ (see section 3.4.2). This subgroup has been previously understood via auxilliary structures such as icosians (cf. [17]).

So we take an arbitrary field $K \subset \operatorname{End}(V)$ which is closed under the adjoint involution on $\operatorname{End}(V)$ arising from the W-invariant inner product on V. Let V_K be the group V regarded as a K-vector space and consider the subgroup W_K of elements in W commuting with K. Say that two roots α and β are K-equivalent if $K\alpha = K\beta$. Each equivalence class S is a subroot system of R and gives rise

to a cyclic subgroup $W_K(S) \subset W_K$ whose nonidentity elements are reflections on V_K. We show that all reflections in W_K are obtained in this way, and we give an explicit formula for the canonical W_K-invariant hermitian form on V_K, thereby giving a formula for each reflection. Different types of root systems S can occur as K-equivalence classes, leading to reflections of different orders in W_K. These are worked out in the various cases for E_8, in sections 3.3 and 3.4.

In general, W_K is not generated by reflections. Indeed, for E_8 there is a copy of $\mathbb{Q}(\sqrt{2})$ in $\mathrm{End}(V)$ for which W_K is the extension of $W(F_4)$ by its graph automorphism. (This subgroup of $W(E_8)$ is not related to the standard $W(F_4)$ contained in $W(E_6)$; it seems to have gone unnoticed till now.) However, for $K = \mathbb{Q}(\sqrt{5})$ as above, and for $K = \mathbb{Q}(w)$ by Springer's theory, we know that W_K is generated by the subgroups $W_K(S)$. We can show moreover that W_K is irreducible on V_K. This implies that $C(w)$ is actually an irreducible reflection group on every w-eigenspace in $\mathbb{C} \otimes V$, when w is cyclotomic.

These results on reflections allow us to analyze the action of $C(w)$ on the coinvariants X_w for w cyclotomic. It is easy to see that $X_w = 0$ unless the order of w is a power of a prime p, in which case $m = p$, so X_w is a vector space over $\mathbb{F}_p$. In fact, we have $p \in \{2, 3, 5\}$. The image of ϱ_w is computed using the reflections found above and reduction modulo p. For $R = E_8$ we find that ϱ_w is surjective for $w \neq -1$.

We then focus on the case where $w \in W$ is elliptic of order three; such elements are cyclotomic. Then R has one of the types $A_2,\ G_2,\ D_4,\ F_4,\ E_6,\ E_8$ and w is unique up to W-conjugacy in each case. If we enlarge $C(w)$ to the centralizer of w in the full automorphism group of R, then ϱ_w is surjective. This is proved in a uniform way, but the individual cases have various connections to: elliptic curves and the 24 cell (for F_4), hermitian curves and Weil representations (for E_6), and the 27 lines on a cubic surface and unipotent representations (for E_8). A relation between E_8 and the 27 lines was found by Coxeter in the last two sections of [8]; our remarks here amount to little more than a different approach to Coxeter's observations.

Finally, in the last chapter, we apply our results on cyclotomic elements to L-packets of supercuspidal representations of p-adic groups.

Contents

2 Reflections

2.1 Hermitian forms

Let V be a $\mathbb{Q}$-vector space of dimension n and fix a nondegenerate symmetric $\mathbb{Q}$-bilinear form $\langle\ ,\ \rangle$ on V. We denote the corresponding adjoint involution on $\mathrm{End}(V)$ by $f \mapsto f^*$; it is defined by the equation $\langle fx, y\rangle = \langle x, f^*y\rangle$ for $f \in \mathrm{End}(V)$ and $x, y \in V$.

Next, let K be a number field with an automorphism $\sigma \in \mathrm{Aut}(K)$ such that $\sigma^2 = 1$. Fix a nonzero $\mathbb{Q}$-linear map $T : K \to \mathbb{Q}$. Every $\mathbb{Q}$-linear functional $K \to \mathbb{Q}$ is of the form $x \mapsto T(ax)$ for a unique $a \in K$.

If T is the trace, then $T(x^\sigma) = T(x)$, but it will be more convenient to make other choices of T which are not necessarily σ-invariant. In general, there is a unique element $b \in K$ such that $T(x^\sigma) = T(xb)$ for all $x \in K$. From the calculation

$$T(x) = T(x^\sigma b) = T\left((xb^\sigma)^\sigma\right) = T(xb^\sigma b),$$

we see that $b^\sigma b = 1$. By Hilbert's Theorem 90, there is $c \in K^\times$ such that

$$b = c^\sigma c^{-1}. \tag{1}$$

We then have $T(xc) = T((xc)^\sigma)$ for all $x \in K$.

Assume we are given an embedding of $\mathbb{Q}$-algebras

$$j : K \hookrightarrow \mathrm{End}(V)$$

such that $j(a^\sigma) = j(a)^*$ for all $a \in K$. We write V_K to denote the abelian group V considered as a K-vector space, via the embedding j. The symmetric form $\langle\ ,\ \rangle$ on V gives rise to a hermitian form H on V_K, as follows (cf. [23, IV.2]).

For every pair of elements $x, y \in V_K$, there is $h(x, y) \in K$ such that

$$\langle j(a)x, y\rangle = T\left(a\, h(x, y)\right), \qquad \text{for all} \quad a \in K.$$

This defines a nondegenerate K-valued pairing h on V_K which is hermitian up to scalar. More precisely, if $c \in K^\times$ is an element satisfying (1) then the scaled form

$$H(x, y) := c\, h(x, y),$$

characterized by the identity

$$T\left(a\ H(x,y)\right) = \langle j(ac)x, y\rangle, \tag{2}$$

is σ-hermitian on V_K: we have $H(y,x) = H(x,y)^\sigma$ for all $x, y \in V_K$. The equation $T\left(H(x,y)\right) = \langle j(c)x, y\rangle$ shows that H is nondegenerate and that any K-subspace $U \subset V_K$ has the same orthogonal complement, whether taken with respect to $\langle\ ,\ \rangle$ or H.

2.2 An explicit formula for H

Let $\zeta \in K$ be a primitive element, so that $K = \mathbb{Q}(\zeta)$, and let

$$M(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n$$

be the minimal polynomial of ζ over $\mathbb{Q}$. Then $\{1, \zeta, \ldots, \zeta^{n-1}\}$ is a $\mathbb{Q}$-basis of K. For our $\mathbb{Q}$-linear map $T : K \to \mathbb{Q}$, let us take

$$T(c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1}) = c_0 \qquad (c_i \in \mathbb{Q}).$$

With these choices, we can give a more explicit formula for H, as follows. We work with the unscaled form $h = c^{-1}H$, writing it as

$$h = \sum_{i=0}^{n-1} h_i \zeta^i,$$

where each h_i is a $\mathbb{Q}$-bilinear form on V. From the relation

$$h(j(\zeta)x, y) = \zeta h(x, y)$$

we get

$$\begin{aligned}
\sum_{i=0}^{n-1} h_i(j(\zeta)x, y)\zeta^i &= \sum_{i=1}^{n} h_{i-1}(x,y)\zeta^i \\
&= \sum_{i=1}^{n-1} h_{i-1}(x,y)\zeta^i - h_{n-1}(x,y)[a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}] \\
&= -a_0 h_{n-1}(x,y) + \sum_{i=1}^{n-1} \left[h_{i-1}(x,y) - a_i h_{n-1}(x,y)\right]\zeta^i.
\end{aligned}$$

Comparing coefficients of ζ, we find by induction that

$$h_i(x,y) = h_0\left(x, f_i(z)y\right),$$

where $f_i(t) = a_0^{-1}(a_i + a_{i-1}t + \cdots + a_1 t^{i-1} + a_0 t^i)$ and $z = j(1/\zeta^\sigma)$. But also

$$h_0(x,y) = T\left(h(x,y)\right) = \langle x, y\rangle,$$

so we get the formula

$$h(x,y) = \sum_{i=0}^{n-1} \langle x, f_i(z)y\rangle \zeta^i. \tag{3}$$

2.3 Root systems and an equivalence relation

Retain the set-up of section 2.1: we have a number field K with involution σ, an orthogonal space V over $\mathbb{Q}$, an embedding $j : K \hookrightarrow \mathrm{End}(V)$ which intertwines σ with the adjoint involution on V, and V_K denotes the abelian group V, regarded as a K-vector space, via j.

Assume now that the orthogonal space V is definite and that R is a finite root system in V whose Weyl group $W = W(R)$ preserves the form $\langle\ ,\ \rangle$. Let $A = A(R)$ be the group of orthogonal automorphisms of V which preserve R. In this section we study the subgroup

$$W_K := W \cap GL(V_K)$$

consisting of the elements in W which centralize the image $j(K)$ of K in $\mathrm{End}(V)$.

Each root $\alpha \in R$ may be regarded as a vector in the K-vector space V_K. We say that two roots $\alpha, \beta \in R$ are ***K*-equivalent** if $K\alpha = K\beta$.

For each K-equivalence class $S \subset R$, let $V(S)$ be the $\mathbb{Q}$-subspace of V generated by S. Then $V(S) = K\alpha$ for any $\alpha \in S$. We have

$$S = R \cap V(S). \tag{4}$$

To see this, let $\alpha \in R \cap V(S)$ and write $\alpha = c_1\alpha_1 + \cdots + c_s\alpha_s$ with $c_i \in \mathbb{Q}$ and $\alpha_i \in S$. By the definition of K-equivalence, there are $f_i \in j(K)$ such that $\alpha_i = f_i\alpha_1$, so

$$\alpha = (c_1 + c_2 f_2 + \cdots + c_s f_s)\alpha_1 \in K\alpha_1,$$

hence $\alpha \in S$. The other containment in (4) is clear.

Equation (4) 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 $W(R)$. However, the group $A(S)$ need not be contained in $A(R)$.

Consider the group

$$W_K(S) := W_K \cap W(S),$$

consisting of the K-linear elements of $W(S)$. If we fix $\alpha \in S$, we have a homomorphism

$$\eta_S : W_K(S) \longrightarrow K^\times, \qquad \text{such that} \quad w\alpha = \eta_S(w)\alpha \tag{5}$$

for all $w \in W_K(S)$. One checks that η_S is independent of the choice of $\alpha \in S$ and that η_S is injective. It follows that the group $W_K(S)$ is cyclic, of order dividing the number of roots of unity in $K^\times$.

A ***K*-reflection** on V_K is an element $g \in GL(V_K)$ of finite order whose fixed-point set is a K-hyperplane. A K-reflection has exactly one eigenvalue $\eta \neq 1$ and $\eta = \det(w)$ is a root of unity in $K^\times$. Any nonidentity element $r \in W_K(S)$ is a K-reflection with nontrivial eigenvalue $\eta = \eta_S(r)$, fixing the K-hyperplane orthogonal to $V(S)$ (with respect to H or $\langle\ ,\ \rangle$, recall it is the same). We have the formula

$$r(x) = x - (1-\eta)\frac{h(x,\alpha)}{h(\alpha,\alpha)}\alpha \tag{6}$$

for any $\alpha \in S$.

For example, if $K = \mathbb{Q}$ then each equivalence class is a pair $S = \{\pm\alpha\}$, forming a root system of type A_1, and K-reflections are the usual reflections in W. At the other extreme, if $[K : \mathbb{Q}] = \dim V$, then R itself is the unique K-equivalence class, and W_K is cyclic.

Lemma 2.1 *Every K-reflection $r \in W_K$ is contained in $W_K(S)$ 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. The subgroup W' of W fixing L' pointwise is generated by reflections about the roots orthogonal to L' [2, V.3 Prop.2]. The set S of these roots is nonempty, since $1 \neq r \in W'$. Hence S is a K-equivalence class and $r \in W_K(S)$. Uniqueness follows from equation (4). ■

3 The cyclotomic case

There are many fields $K \subset \mathrm{End}(V)$; "usually" one has $W_K \subseteq \{\pm 1\}$. In this section we will show that if $j(K)$ is generated by an automorphism of the irreducible root system R then W_K is irreducible on V_K, the groups $W_K(S)$ are all non-trivial, and they generate W_K. Along the way, we give a classification of possible root systems S which arise, which facilitates our later calculations.

3.1 Reflections in the cyclotomic case

We say that an element $w \in A(R)$ is **cyclotomic** if the minimal polynomial $M(t)$ of w on V is irreducible over $\mathbb{Q}$. Let d be the order of w. Then $M(t) = \Phi_d(t)$ is the cyclotomic polynomial, whose roots are the elements of order d in $\bar{\mathbb{Q}}^\times$. Fix a root ζ of $\Phi_d(t)$ and let $K = \mathbb{Q}(\zeta)$, with involution $\zeta^\sigma = \zeta^{-1}$. Then we have an embedding $j : K \to \mathrm{End}(V)$ given by $j(\zeta) = w$, such that $j(\zeta^\sigma) = w^{-1} = w^*$. The image $j(K)$, hence the group W_K, is independent of the choice of ζ. Indeed, W_K is just the centralizer $C(w)$ of w in W.

Proposition 3.1 *In the situation just described, the group W_K is generated by the cyclic subgroups $W_K(S)$, with S ranging over the K-equivalence classes in R.*

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

Each root $\alpha \in R$ may be viewed as a 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. This means that every w-eigenspace in $\bar{V}$ contains a regular vector. The stabilizer in W of a regular vector is trivial.

The group $W_K = C(w)$ preserves each eigenspace of w in $\bar{V}$. Hence 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 [22, 4.2,6.4] we have that 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. 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 W_K bijectively onto the reflections in $\pi_\zeta(W_K)$. The result follows. ■

We now examine the groups $W_K(S)$ in more detail. Let S be a K-equivalence class in R. Then w acts on S via an automorphism $w_S \in A(S)$ having characteristic polynomial $\Phi_d(t)$ on $V(S)$. 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 $w_S^c = (w_1, \cdots, w_c)$, where each $w_i \in A(S_i)$ has order $e := d/c$.

On $V(S)$, viewed as a $\mathbb{Q}$-vector space, the element w_S^c has characteristic polynomial

$$\det(tI_{V(S)} - w_S^c) = \Phi_e(t)^{\phi(d)/\phi(e)} = \prod_{i=1}^{c} \det(tI_{V(S_i)} - w_i). \tag{7}$$

By the transitivity of w_S on the S_i, each polynomial $\det(tI_{V(S_i)} - w_i)$ has the same degree. Hence there is an integer $m \geq 1$ such that

$$\det(tI_{V(S_i)} - w_i) = \Phi_e(t)^m$$

for all i. Comparing degrees in (7), we find that

$$\phi(d) = m \cdot c \cdot \phi(e). \tag{8}$$

The following lemma is an elementary consequence of (8); its proof is left to the reader.

Lemma 3.2 *We have $m = 1$ and that every prime dividing d must divide e. In particular, we have $e > 1$.*

Hence $S = cS_1$, where S_1 is an irreducible root system of rank $\phi(e)$ admitting an automorphism w_1 with characteristic polynomial

$$\det(tI_{V(S_1)} - w_1) = \Phi_e(t).$$

We have the numerical constraints

$$\phi(d) = c \cdot \phi(e) \quad \text{and} \quad d \text{ divides both } |S| \text{ and } |A(S)|. \tag{9}$$

The first item has been shown above and the last two are forced by all w-orbits having d elements and $A(S)$ containing the element w_S of order d, respectively.

The possibilities for S_1 are given in the table below, using the notation of [4] for conjugacy-classes in Weyl groups, extended to $A(R)$ in the obvious way. Recall that e 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.

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

Lemma 3.3 *For each K-equivalence class $S \subset R$, the group $W_K(S)$ 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 KS and acts on S as w^ν. Hence w_S^ν commutes with w on V, so that $w_S^\nu \in W_K(S)$.

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 $e \mid \ell$. The table above shows this does not happen. ■

Lemma 3.4 *Assume R is irreducible. Then W_K acts irreducibly on V_K.*

Proof: We use the following basic fact: Given any two roots $\alpha, \beta \in R$, there is a sequence

$$\alpha = \alpha_0,\ \alpha_1,\ \ldots\ ,\ \alpha_k = \beta \tag{10}$$

of roots in R such that $\langle \alpha_i, \alpha_{i+1} \rangle \neq 0$ for $0 \leq i < k$. This can be seen as follows. By viewing β as part of a basis of simple roots, we see that there is $\gamma \in R$ of the same length as α, such that $\langle \beta, \gamma \rangle \neq 0$. Hence we may suppose $\langle \alpha, \alpha \rangle = \langle \beta, \beta \rangle$. The claim follows from transitivity of W on roots of a given length [2, VI.1 Prop 11].

The form $h(x,y)$ from section 2.1 satisfies $T\left(h(x,y)\right) = \langle x, y\rangle$. It follows the sequence (10) 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 $W_K(S)$. Take a nonzero element $x \in U$. Choose $\alpha \in R$ such that $\langle x, \alpha\rangle \neq 0$, and let S be the K-equivalence class containing α. By Lemma 3.3, there is a K-reflection $r_S \in W_K(S)$ of order $m > 1$, having the formula

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

where $\eta \in \bar{\mathbb{Q}}^\times$ has order m. Since $T\left(h(x,\alpha)\right) = \langle x, \alpha\rangle \neq 0$, this shows that $\alpha \in U$. Let $\beta \in R$ be arbitrary, and choose a sequence as in (10). 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 $R \subset U$, so $U = V$. ■

Corollary 3.5 *Suppose $w \in A(R)$ is cyclotomic with 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}, $W_K(S)$ is generated by a Coxeter element in $W(S)$ and there are $|R|p^{-1}$ reflections in W_K, 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 the table above gives the asserted possibilities for S. ■

3.2 Cyclotomic elements and exponents

One can characterize the cyclotomic elements in a Weyl group $W = W(R)$, in terms of the exponents $\{m_1, \ldots, m_n\}$ of W. With one exception, these are all obtained as powers of elements $v \in W$ with irreducible characteristic polynomial. The latter are characterized as follows.

Lemma 3.6 *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 $\{m_1, \ldots, m_n\}$ 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 [22, 4.11] and also follows from the proof of Lemma 3.1 above. Uniqueness now follows from [22, 4.2], which also shows that the eigenvalues of v are η^{m_i}, $i = 1, \ldots, n$, where $\eta \in \bar{\mathbb{Q}}^\times$ has order e. But these eigenvalues are the roots of $\Phi_e(t)$, so $\{m_1, \ldots, m_n\}$ 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

$$p \leq n + 1, \qquad p \nmid m_i, \quad 1 \leq i \leq n. \tag{11}$$

For $R = A_n$, with exponents $\{1, 2, \ldots, n\}$, 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 (11) 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 (11) 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 [4], 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 $C(v) = \langle v' \rangle$. ■

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

Lemma 3.7 *Suppose $w \in W$ has irreducible minimal polynomial on V. Then one of the following holds:*

1. *There is $v \in W$ with irreducible characteristic polynomial $\Phi_e(t)$ such that $w = v^{e/d}$ for some divisor $d \mid e$.*

2. *$R = E_7$ and $w = -1$.*

In Lemma 3.4 above we proved that if w has irreducible minimal polynomial on V then each eigenspace $\bar{V}(w, \zeta)$ is irreducible for $C(w)$. In fact, we can use Lemma 3.7 to prove irreducibility on a much smaller subgroup of $C(w)$, excluding the case of $w = -1 \in W(E_7)$.

First, a remark on normalizers of regular elements in W. Let $v \in W$ have order e, let $C(v)$ be the centralizer of v in W and let $N(v)$ be 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

$$n^{-1}vn = v^{\sigma(n)}, \qquad n \in N(v).$$

It follows from [22, 4.7] that σ is surjective, so we have an exact sequence

$$1 \longrightarrow C(v) \longrightarrow N(v) \xrightarrow{\sigma} (\mathbb{Z}/e\mathbb{Z})^\times \longrightarrow 1, \tag{12}$$

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 [22].

Lemma 3.8 *If v is regular, then $(\mathbb{Z}/e\mathbb{Z})^\times$ freely permutes the regular eigenspaces of v.*

Proof: Suppose $\bar{V}(v, \zeta')$ is an eigenspace for v containing a regular vector, and $n \in N(v)$ preserves $\bar{V}(v, \zeta')$. Since v is a scalar on $\bar{V}(v, \zeta')$, the commutator $[n, v]$ fixes $\bar{V}(v, \zeta')$ pointwise. Therefore $[n, v]$ fixes a regular vector, so $[n, v] = 1$. ■

We now return to our cyclotomic element $w \in W$ of order d and eigenvalue ζ. Write $w = v^{e/d}$ where $v \in W$ has characteristic polynomial $\Phi_e(t)$ and $d \mid e$. Then $\zeta = \eta^{e/d}$, 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 (12) restricts to another exact sequence

$$1 \longrightarrow C(v) \longrightarrow N(v) \cap C(w) \xrightarrow{\sigma} \Delta \longrightarrow 1. \tag{13}$$

Since v is regular with eigenvalues of multiplicity one, Lemma 3.8 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 already irreducible on $\bar{V}(w,\zeta)$.

3.3 Cyclotomic structures on E_8

We determine the K-equivalence classes S and the orders of the subgroups $W_K(S)$ for each of the fields K arising from cyclotomic elements $w \in W = W(E_8)$. We thereby find the number of reflections of each order, along with the Shephard-Todd classification of the complex reflection group $C(w) = W_K$.

There is exactly one cyclotomic class in $W(E_8)$ of every order

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

The field K is generated by the d^{th} roots of unity. We omit the classes of odd order d since their negatives have the same centralizer. If $d = 2$ then $w = -1$, so $W_K = W$. If $d \in \{20, 24, 30\}$, we have $[K : \mathbb{Q}] = \phi(d) = 8$ so $S = R$ and $W_K = \langle w \rangle$. The nontrivial cases are as follows.

3.3.1 $d = 4$

Here w belongs to the class $2D_4(a_1)$ 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 $2A_1$ and $W_K(S) = \langle w_S^2 \rangle$ has order two. There are $240/4 = 60$ K-equivalence classes, each contributing a single K-reflection to W_K.

3.3.2 $d = 6$

Here w belongs to the class $E_8(a_8)$. By 3.5, there are 40 K-equivalence classes S, each of type A_2, and each $W_K(S)$ is cyclic of order three, giving a total of 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 6.6 below).

3.3.3 $d = 10$

Here w belongs to the class $E_8(a_6)$. By 3.5, there are 12 K-equivalence classes S, each of type A_4, consisting of two w-orbits. Each $W_K(S)$ is cyclic of order

five, generated by a Coxeter element in $W(S)$, giving a total of 48 K-reflections in W_K.

3.3.4 $d = 8$

Here w belongs to the class $D_8(a_3)$ and $w^4 = -1$. We have $c\phi(e) = \phi(8) = 4$. The table in section 3.1 and the constraints (9) show that S has type $4A_1$ or D_4. To analyze this dichotomy, we first make some preliminary remarks on subsystems of type $4A_1$ in E_8, which we call **tetrads**. Recall that $X = Q(E_8)$ is the E_8-root lattice. 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.

Lemma 3.9 *Let R be a root system of type E_8. The even and odd tetrads in R each form a single orbit under $W(R)$. The even tetrads are precisely those which are contained in a subsystem of type D_4.*

Proof: Set $R_0 := R$ and choose a root $\alpha_0 \in R_0$. Let $R_1 \simeq E_7$ be the set of roots in R_0 orthogonal to α_0. Choose $\alpha_1 \in R_1$ and let $R_2 \simeq D_6$ be the set of roots in R_1 orthogonal to α_1. Choose $\alpha_2 \in R_2$ and let $R_3 \simeq D_4 \times A_1$ be the roots in R_2 orthogonal to α_2. Choose $\alpha_3' \in D_4$, $\alpha_3'' \in A_1$.

For $i = 0, 1, 2$ the groups $W(R_i)$ are transitive on R_i, but $W(R_3)$ has two orbits in R_3. It follows that

$$T' := \pm\{\alpha_0, \alpha_1, \alpha_2, \alpha_3'\}, \qquad T'' := \pm\{\alpha_0, \alpha_1, \alpha_2, \alpha_3''\}$$

represent the two $W(R)$-orbits of tetrads in R. One can check that T' is odd and T'' is even.

If the general tetrad $T = \pm\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$ is contained in $S \simeq D_4$, then there is a base $\{\beta, \alpha_1, \alpha_2, \alpha_3\}$ of S with $\langle \beta, \alpha_i \rangle \neq 0$ for $i = 1, 2, 3$. (That is, β corresponds to the branch node.) The highest root for this base is $\alpha_0 = 2\beta + \alpha_1 + \alpha_2 + \alpha_3$. It follows that $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \in 2X$. Conversely, if $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = 2\lambda \in 2X$, one checks that $\langle \lambda, \lambda \rangle = 2$, so in fact λ is a root. Moreover, $\langle \lambda, \alpha_i \rangle = 1$ for each i. It follows that $\beta = \lambda - \alpha_1 - \alpha_2 - \alpha_3$ is a root, and $\{\beta, \alpha_1, \alpha_2, \alpha_3\}$ is the base of a D_4 with highest root α_0. ■

Return now to our cyclotomic element $w \in W(E_8)$ of order $d = 8$. Every K-equivalence class S contains a unique w-stable tetrad. This is clear if $S \simeq 4A_1$ 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 set of $\alpha \in S$ for which $\langle \alpha, w\alpha \rangle = 0$ form 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 $\langle \varsigma\beta, w\varsigma\beta \rangle = +1$ so 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 [2], the roots of $R = E_8$ 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 D_8 subsystem of E_8. We choose $w \in W(D_8)$ 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 3.9, 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 $S \simeq 4A_1$ are the w-orbits through the following twelve roots α:

$$\begin{array}{ll} e_1 \pm e_6, & e_1 \pm e_8, \\ [+ + ++ \mid \pm \mp \pm\mp], & [\pm \mp \pm\mp \mid + + ++], \\ [+ + ++ \mid \mp \pm \mp\pm], & [\mp \pm \mp\pm \mid + + ++]. \end{array} \tag{14}$$

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 itself a tetrad, then $W_K(S) = \{\pm 1\}$ has order two. If $S = D_4$, then $W_K(S) = \langle w_S^2 \rangle$ has order four. It follows that there are $12 \cdot 1 + 6 \cdot 3 = 30$ reflections in W_K. This is consistent with Springer's theory: the degrees of $C(w)$ are the degrees of E_8 which are divisible by 8, namely $8, 24$, and $7 + 23 = 30$.

3.3.5 $d = 12$

Here w belongs to the class $E_8(a_3)$. We have $c\phi(e) = \phi(12) = 4$. Using the table in section 3.1 and the constraints (9) we find two possibilities for a K-equivalence class: $S = 2A_2$ 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 $2A_2$ 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 $W_K(S) = \langle w_S^4 \rangle$ 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 $W_K(S) = \langle w_S^3 \rangle$ has order four.

We can count the number of K-equivalence classes of each type, as follows. 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 $a + 2b = 240/12 = 20$. The degrees of E_8 are $2, 8, 12, 14, 18, 20, 24, 30$. By Springer's theory, the degrees of W_K are $12, 24$, so there are $11 + 23 = 34$ reflections in W_K. Counting the number of reflections in each group $W_K(S)$, we get $2a + 3b = 34$. It follows that $a = 8$ and $b = 6$. (In the earlier case $d = 8$ this method led to only one equation, so we had to examine the roots.)

The table below summarizes the cases where $W \neq C(w) \neq \langle w \rangle$. Row "number of S" gives the number of 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 notation for $C(w)$ according to the Shephard-Todd classification.

d :	4	3, 6	8	5, 10	12
class	$2D_4(a_1)$	$4A_2,\ E_8(a_8)$	$D_8(a_3)$	$2A_4,\ E_8(a_6)$	$E_8(a_3)$
$\lvert C(w)\rvert$:	$8{\cdot}12{\cdot}20{\cdot}24$	$12{\cdot}18{\cdot}24{\cdot}30$	$8 \cdot 24$	$20 \cdot 30$	$12 \cdot 24$
$\dim V_K$	4	4	2	2	2
type of S	$2A_1$	A_2	$4A_1, D_4$	A_4	$2A_2, D_4$
$\lvert W_K(S)\rvert$	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

3.4 Some subfields of cyclotomic fields

Continuing with $R = E_8$, we consider two examples where the image of a field $k \hookrightarrow \mathrm{End}(V)$ is not generated by an element of $A(R)$.

3.4.1 $\mathbb{Q}(\sqrt{2})$

We use the notation of section 3.3.4. The embedding $K = \mathbb{Q}(\zeta_8) \hookrightarrow \mathrm{End}(V)$ sends $1 + \zeta_8 + \zeta_8^{-1}$ to the operator $\varsigma = 1 + w + w^{-1} \in \mathrm{End}(V)$, satisfying

$$\varsigma^2 = 2\varsigma + 1, \qquad \varsigma^* = \varsigma.$$

This gives an embedding of the subfield $k = \mathbb{Q}(\sqrt{2}) \subset K$ in $\mathrm{End}(V)$.

Let $a, b \in \mathbb{Q}$, and suppose $\eta = a\alpha + bw\alpha + bw^{-1}\alpha \in R$. Then we must have

$$\begin{aligned} \langle \alpha, \eta \rangle &= 2(a + b\langle \alpha, w\alpha \rangle) \in \{0, \pm 1, \pm 2\}, \\ \tfrac{1}{2}\langle \eta, \eta \rangle &= a^2 + 2b^2 + 2ab\langle \alpha, w\alpha \rangle = 1. \end{aligned} \tag{15}$$

If $\langle \alpha, w\alpha \rangle = 0$, the two equations (15) have only the solutions $\eta = \pm\alpha$. In this case, we have $W(S) = \langle s_\alpha \rangle$ and $W_k(S) = 1$, since ς does not have rational eigenvalues.

If $\langle \alpha, w\alpha \rangle = -1$, we find the solutions $\eta = \pm\alpha,\ \pm\varsigma\alpha$. By a straightforward calculation, one proves the following:

Lemma 3.10 *Suppose $\sigma \in \mathrm{End}(X)$ satisfies an equation of the form $\sigma^2 = c\sigma + 1$ for some $c \in \mathbb{Z}$, and $\alpha \in R$ satisfies $\langle \alpha, \sigma\alpha \rangle = 0$. Then $\sigma\alpha \in R$, and σ commutes with $s_\alpha s_{\sigma\alpha}$.*

It follows that $W_k(S) = \langle s_\alpha s_{\varsigma\alpha} \rangle$ has order two. Thus, we find that each K-equivalence class of type D_4 contributes four k-reflections of order two, giving a total of $6 \cdot 4 = 24$ k-reflections in W_k. Since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, these 24 reflections generate a rank four Coxeter group, which must be of type F_4, by the classification. We can see this explicitly, as follows.

Let $u = 1 + \sqrt{2}$. Using the linear map $T : k \to \mathbb{Q}$ given by $T(a + bu) = a$, the form $h(x, y)$ from section 2.1 is

$$h(x, y) = \langle x, y \rangle + \langle x, \varsigma y \rangle u.$$

We have $h(x, y) = h(y, x)$, since ς is symmetric.

If $\langle \alpha, w\alpha \rangle = -1$, then $h(\alpha, \alpha) = 2$, so the reflection $r_\alpha := s_\alpha s_{\varsigma\alpha}$ is given by

$$r_\alpha(x) = x - h(x, \alpha)\alpha.$$

If also $\langle \beta, w\beta \rangle = -1$, where β lies in another k-equivalence class, then on the two dimensional space $k\alpha + k\beta$, the product $r_\alpha r_\beta$ has matrix

$$r_\alpha r_\beta = \begin{bmatrix} h(\alpha, \beta)^2 - 1 & h(\alpha, \beta) \\ -h(\alpha, \beta) & -1 \end{bmatrix}, \tag{16}$$

in terms of the k-basis $\{\alpha, \beta\}$. Since

$$h(\alpha, \beta) = \langle \alpha, \beta \rangle + \langle \alpha, \varsigma\beta \rangle u,$$

there are three possibilities for the order of $r_\alpha r_\beta$ as follows:

1. $\langle\alpha,\beta\rangle = \langle\alpha,\varsigma\beta\rangle = 0 \quad \Rightarrow \quad |r_\alpha r_\beta| = 2;$

2. $\langle\alpha,\beta\rangle = 0 \neq \langle\alpha,\varsigma\beta\rangle \quad \Rightarrow \quad |r_\alpha r_\beta| = 3;$

3. $\langle\alpha,\beta\rangle\langle\alpha,\varsigma\beta\rangle = -1 \quad \Rightarrow \quad |r_\alpha r_\beta| = 4.$

For example, the four k-reflections coming from a single K-equivalence class of type D_4 generate a $W(B_2)$.

Let

$$\begin{aligned} \alpha_1 &= e_1 - e_2, \quad \alpha_2 = [+-+- \mid -++-], \\ \alpha_4 &= e_8 - e_7, \quad \alpha_3 = [++-+ \mid +-++] = w\alpha_2. \end{aligned} \tag{17}$$

One checks that $\langle\alpha_i, w\alpha_i\rangle = -1$ for $i = 1,2,3,4$ and that the k-reflections

$$r_i := s_{\alpha_i} s_{\varsigma\alpha_i}$$

satisfy the Coxeter relations for F_4, according to the diagram 1—$2\overset{4}{—}3$—4.

Let $W_k' \simeq W(F_4)$ denote the subgroup of W_k generated by the k-reflections. Since the latter are even elements in $W(E_8)$, this subgroup W_k' is not conjugate to the standard $W(F_4) \subset W(E_6) \subset W(E_8)$.

We also have $W_k' \neq W_k$. In other words, W_k is not generated by k-reflections. Indeed, we can write $w = v^3$, where $v \in W(E_8)$ has order 24. Then $v \in W_k$, but $W(F_4)$ contains no element of order 24. Since k is real and H is definite, the group W_k is a finite subgroup of the compact orthogonal group $O_4(\mathbb{R})$. From the classification (cf. [7, p.47]), we find that W_k is the extension of $W_k' = W(F_4)$ by its graph automorphism, which arises from an isometry over $\mathbb{Q}(\sqrt{2})$.

3.4.2 $\mathbb{Q}(\sqrt{5})$

Again take $R = E_8$ and 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. We have an embedding $k = \mathbb{Q}(\sqrt{5}) \hookrightarrow \mathrm{End}(V)$, sending $\frac{1}{2}(1+\sqrt{5}) \mapsto \tau$. From the equation

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

it follows that

$$\langle\alpha, w\alpha\rangle = \langle\alpha, w^2\alpha\rangle + 1 \tag{18}$$

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 3.11 *The operator τ maps R_0 bijectively onto R_1, and has the following properties:*

1. $\langle \alpha, \tau\alpha \rangle = 0$*;*
2. $s_\alpha s_{\tau\alpha} \in W_k$ *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 (18), 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 $\tau\alpha \in R_1$, and the second, combined with Lemma 3.10, 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 3.11, 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 $s_\alpha s_{\tau\alpha}$ in the reflection subgroup $W_k' \subset W_k$. From the classification of real reflection groups, we see that W_k' is the Coxeter group of type H_4.

To see the Coxeter generators, number the simple roots of E_8 as shown:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & 8 & & \end{array} \tag{19}$$

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 [17] (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$.

In contrast to the previous section, this time we have $W_k' = W_k$. This can be seen as follows. Let X_k be the lattice X, viewed as a module over the ring of integers $\mathfrak{o} = \mathbb{Z}[\tau]$ in k. Since 2 remains prime in $\mathfrak{o}$, the quotient $X_k/2X_k$ is a four dimensional vector space over $\mathfrak{o}/2\mathfrak{o} \simeq \mathbb{F}_4$. The form $H(x,y)$ is symmetric and the formula (3) reads as

$$H(x,y) = -\langle x,y\rangle - \langle x, y + wy + w^{-1}y\rangle\tau.$$

Since $\langle x,x\rangle \in 2\mathbb{Z}$ for all $x \in X$, we have $H(x,x) \in 2\mathfrak{o}$, so that W_k preserves the $\mathbb{F}_4$-valued quadratic form $q(x) \equiv \frac{1}{2}H(x,x) \mod 2\mathfrak{o}$ on $X_k/2X_k$. It is well-known that kernel of the action of W on $X/2X$ is $\{\pm 1\}$, so we have an injection

$$W_k/\{\pm 1\} \hookrightarrow O_4^\epsilon(4), \tag{20}$$

where $\epsilon = \pm$ is $+$ if the form q is split and $\epsilon = -$ otherwise. Since $|O_4^\epsilon(4)| = 2\cdot 4^2(4^2-\epsilon)(4^2-1)$ and W_k contains the subgroup $W_k' = W(H_4)$ of order 120^2, it follows that $\epsilon = +$, that $W_k' = W_k$ and that (20) is an isomorphism.

4 Coinvariants

4.1 Lattices and skew-symmetric forms

Let V be a finite dimensional $\mathbb{Q}$-vector space of dimension n, and let $X \subset V$ be a free $\mathbb{Z}$-module of rank n. Let w be an automorphism of V of finite order, preserving X. We assume that w 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

$$|X_w| = \det(1-w),$$

For $\lambda \in X$, we let

$$\rho_\lambda := \lambda + (1-w)X \in X_w$$

be the coset containing λ.

Let $M(t)$ be the monic minimal polynomial of w on V and set

$$m := M(1).$$

There is a unique polynomial $J(t) \in \mathbb{Z}[t]$, with $\deg J < \deg M$, such that

$$(1-t)J(t) + M(t) = m.$$

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

$$(1-w)J(w) = m. \tag{21}$$

It follows that $mX \subset (1-w)X$, so that

$$mX_w = 0, \tag{22}$$

and X_w is a $\mathbb{Z}/m\mathbb{Z}$-module. Explicit formulas for $J(t)$ in certain cases are given in section 4.3 below.

Note that $M(t)$ is also the minimal polynomial of w^{-1}, so that

$$(1-w^{-1})J(w^{-1}) = m = (1-w)J(w),$$

or

$$-w^{-1}(1-w)J(w^{-1}) = (1-w)J(w).$$

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

$$J(w^{-1}) = -wJ(w) = (1-w)J(w) - J(w) = m - J(w). \tag{23}$$

Let $\hat{V}$ be the dual space of V and let $\hat{X} = \mathrm{Hom}(X, \mathbb{Z})$ be the dual lattice, with the natural pairing $\langle \cdot, \cdot \rangle : X \times \hat{X} \to \mathbb{Z}$. For $\lambda \in X$, we have

$$\begin{aligned} \langle J(w)\lambda, \hat{X} \rangle \subset m\mathbb{Z} &\Leftrightarrow J(w)\lambda \in mX \\ &\Leftrightarrow J(w)\lambda \in J(w)(1-w)X \\ &\Leftrightarrow \lambda \in (1-w)X, \end{aligned} \tag{24}$$

by (21). From (23), we have

$$\langle J(w)\lambda, \hat{\mu} \rangle \equiv -\langle \lambda, J(w)\hat{\mu} \rangle \mod m,$$

for $\lambda \in X,\ \hat{\mu} \in \hat{X}$. It follows that we have a duality

$$X_w \times \hat{X}_w \longrightarrow \mathbb{Z}/m\mathbb{Z}, \qquad (\rho_\lambda, \rho_{\hat{\mu}}) \mapsto \langle J(w)\lambda, \hat{\mu} \rangle \mod m, \tag{25}$$

where $\lambda \in X$, $\hat{\mu} \in \hat{X}$ are lifts of ρ_λ, $\rho_{\hat{\mu}}$, respectively.

4.2 Quadratic lattices

Now suppose $\langle \cdot, \cdot \rangle$ is a symmetric positive definite $\mathbb{Q}$-bilinear form on V, taking integer values on X. We can then identify $V = \hat{V}$ and regard the dual lattice $\hat{X}$ as

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

Note that $X \subseteq \hat{X}$.

Assume w preserves the form $\langle\ ,\ \rangle$. Then the pairing (25) restricts to an $\mathbb{Z}/m\mathbb{Z}$-bilinear form on X_w, given by

$$\langle \rho_\lambda, \rho_\mu \rangle_w := \langle J(w)\lambda, \mu \rangle \mod m, \qquad \text{for} \quad \lambda,\ \mu \in X, \tag{26}$$

which is skew-symmetric, by (23). More precisely the form $\langle\ ,\ \rangle_w$ is symplectic (that is, $\langle \rho, \rho \rangle_w = 0$ for all $\rho \in X_w$) if $m > 2$, or if $m = 2$ and $\langle \lambda, \lambda \rangle \in 2\mathbb{Z}$ for all $\lambda \in X$. The form $\langle\ ,\ \rangle_w$ is orthogonal if $m = 2$ and $\langle \lambda, \lambda \rangle \notin 2\mathbb{Z}$ for some $\lambda \in X$. A calculation similar to (24) shows that the form $\langle\ ,\ \rangle_w$ has radical

$$X_w^0 = [X \cap (1-w)\hat{X}]/(1-w)X = \ker[X_w \longrightarrow \hat{X}_w], \tag{27}$$

where the latter map is induced by the inclusion $X \hookrightarrow \hat{X}$.

In particular, if $X = \hat{X}$, then $\langle\ ,\ \rangle_w$ is nondegenerate on X_w. At the other extreme, the form $\langle\ ,\ \rangle_w$ can be identically zero on X_w, as we shall see in section 4.4.

4.3 Cyclotomic lattices and reduction modulo p

Retain the set-up of the previous two sections. As before, we say that w is cyclotomic if its minimal polynomial $M(t)$ is irreducible over $\mathbb{Q}$.

Lemma 4.1 *Suppose w is cyclotomic of order $d > 1$. If d is not a prime power, then $X_w = 0$. If d is a power of a prime p, then*

$$X_w \simeq \mathbb{F}_p^{a(d)},$$

where $a(d) = n \cdot \phi(d)^{-1}$.

Proof: Since $m = \Phi_d(1)$ kills X_w, this follows from (22) and the elementary fact that $\Phi_d(1) = 1$ unless d is a power of a prime p, in which case $\Phi_d(1) = p$. ■

Suppose that w is cyclotomic of order d a power of a prime p and let $\zeta \in \bar{\mathbb{Q}}^\times$ have order d. As before, the field $K = \mathbb{Q}(\zeta)$ embeds in $\mathrm{End}(V)$ via $\zeta \mapsto w$

and $\mathbb{Z}[w]$ is the image of the ring of integers of K. The element $1-w \in \mathbb{Z}[w]$ generates the unique ramified prime ideal $P \subset \mathbb{Z}[w]$; we have $p\mathbb{Z}[w] = P^{\phi(d)}$ and $\mathbb{Z}[w]/P \simeq \mathbb{F}_p$.

Let X_K be the abelian group X, viewed as an $\mathbb{Z}[w]$ module. Then we have

$$X_w = X_K/PX_K,$$

so that X_w is the reduction modulo p of the $\mathbb{Z}[w]$-lattice X_K.

The relation between the hermitian form h and the pairing $\langle\ ,\ \rangle_w$ is as follows. For $x, y \in X_K$, we have (see (3))

$$h(x,y) = \sum_{i=0}^{\phi(d)-1} \langle x, f_i(w)y\rangle \zeta^i \equiv \sum_{i=0}^{\phi(d)-1} \langle x, f_i(w)y\rangle \mod P,$$

where $f_i(t) = a_i + a_{i-1}t + \cdots + a_1 t^{i-1} + t^i$, and $\Phi_d(t) = \sum_{i=0}^{\phi(d)-1} a_i t^i$. Using the relation $a_i = a_{\phi(d)-i}$ and the fact that $\Phi_d(1) = p$, one can check that

$$(1-t)\sum_{i=0}^{\phi(d)-1} f_i(t) + \Phi_d(t) = p.$$

It follows that the polynomial $J(t)$ of section 4.1 is given by

$$J(t) = \sum_{i=0}^{\phi(d)-1} f_i(t),$$

so that we have

$$h(x,y) \equiv -\langle x, y\rangle_w \mod P.$$

4.4 Root lattices

Let V be a quadratic space as in section 4.2 and let R be an irreducible reduced root system in V. For each $\alpha \in R$, we set

$$\check{\alpha} = \frac{2\alpha}{\langle \alpha, \alpha\rangle}, \qquad \check{R} = \{\check{\alpha} :\ \alpha \in R\}.$$

We assume R is compatible with the quadratic structure on V, that is,

$$\langle \alpha, \check{\beta}\rangle \in \mathbb{Z} \qquad \text{for all } \alpha, \beta \in R$$

and the reflection $s_\alpha(x) = x - \langle x, \check{\alpha}\rangle\alpha$ on V preserves R. The inner product $\langle\ ,\ \rangle$ is normalized so that

$$1 \in \langle R, R\rangle \subset \mathbb{Z}. \tag{28}$$

In most cases, the normalization (28) makes $\langle\alpha,\alpha\rangle = 2$ for each short root $\alpha \in R$. The exceptions are $R = B_n$ and C_2, where $\langle\alpha,\alpha\rangle = 1$ for each short root.

Let $Q(R)$ and $Q(\check{R})$ be the $\mathbb{Z}$-lattices in V generated by R and $\check{R}$, and let

$$P(R) = \widehat{Q(\check{R})} = \{\lambda \in V :\ \langle\lambda, \check{R}\rangle \subset \mathbb{Z}\},$$

$$P(\check{R}) = \widehat{Q(R)} = \{\lambda \in V :\ \langle\lambda, R\rangle \subset \mathbb{Z}\}.$$

We have $Q(R) \subset P(R)$ and $Q(\check{R}) \subset P(\check{R})$, along with a duality

$$P(R)/Q(R) \times P(\check{R})/Q(\check{R}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

induced by our pairing $\langle x, y\rangle$. Let

$$f = [P(R) : Q(R)] = [P(\check{R}) : Q(\check{R})].$$

For any $\alpha \in R$ and $\lambda \in P(R)$ we have $(1 - s_\alpha)\lambda = \langle\lambda, \check{\alpha}\rangle\alpha \in \mathbb{Z}\alpha$. It follows easily that $(1 - w)P(R) \subset Q(R)$, which implies that

$$f \mid \det(1 - w). \tag{29}$$

We apply section 4.1 to the lattice $X = Q(R)$, with $\hat{X} = P(\check{R})$. Thus we have a skew-symmetric form $\langle\ ,\ \rangle_w$ on X_w with radical

$$X_w^0 = \left[Q(R) \cap (1 - w)P(\check{R})\right]/(1 - w)Q(R) = \ker[X_w \longrightarrow \hat{X}_w].$$

The normalization (28) makes the forms $\langle\ ,\ \rangle_w$ symplectic in all cases except $R = B_n, C_2$, where the forms $\langle\ ,\ \rangle_w$ are orthogonal.

If $R = \check{R}$, then since $(1 - w)P(R) \subset Q(R)$, the map $1 - w$ induces an isomorphism

$$P(R)/Q(R) \xrightarrow{\sim} X_w^0. \tag{30}$$

For $R = E_8$ in particular, the form $\langle\ ,\ \rangle_w$ is a nondegenerate symplectic form on X_w for all elliptic $w \in W(E_8)$.

If $R \neq \check{R}$, then the radical X_w^0 depends on w. The various cases work out as follows. If $R = B_n$, we have $X = Q(R) = \mathbb{Z}^n$ with the usual inner product $\langle e_i, e_j\rangle = \delta_{ij}$. The elliptic classes in $W(B_n)$ are in bijection with partitions of

n: to the partition $n = n_1 + \cdots + n_r$ corresponds the class of $w \in W(B_n)$ with characteristic polynomial

$$\det(tI_V - w) = \prod_{i=1}^{r} 1 + x^{n_i}.$$

We have $X_w \simeq (\mathbb{Z}/2\mathbb{Z})^r$. Since $X = \hat{X}$, the pairing $\langle\ ,\ \rangle_w$ is a nondegenerate orthogonal form on $(\mathbb{Z}/2\mathbb{Z})^r$.

For $R = C_n$ with $n \geq 3$, the elliptic classes are those of $W(B_n)$. We have $X = Q(R) = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \sum x_i \in 2\mathbb{Z}\}$ and $X_w \simeq (\mathbb{Z}/2\mathbb{Z})^r$ as above. The form $\langle\ ,\ \rangle_w$ is symplectic with radical

$$X_w^0 \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{for} \quad r \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{for} \quad r \text{ even.} \end{cases} \tag{31}$$

For G_2 and F_4 we list in the following tables the elliptic classes, their characteristic polynomials and the corresponding groups X_w, X_w^0. The forms $\langle\ ,\ \rangle_w$ are symplectic.

Class of $w \in W(G_2)$	$\det(tI_V - w)$	X_w	X_w^0
G_2	Φ_6	0	0
A_2	Φ_3	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$
$A_1 + \tilde{A}_1$	Φ_2^2	$(\mathbb{Z}/2\mathbb{Z})^2$	0

Class of $w \in W(F_4)$	$\det(tI_V - w)$	X_w	X_w^0
F_4	Φ_{12}	0	0
$F_4(a_1)$	Φ_6^2	0	0
D_4	$\Phi_2^2\Phi_6$	$(\mathbb{Z}/2\mathbb{Z})^2$	0
$D_4(a_1)$	Φ_4^2	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$
B_4	Φ_8	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$A_2 + \tilde{A}_2$	Φ_3^2	$(\mathbb{Z}/3\mathbb{Z})^2$	0
$A_3 + \tilde{A}_1$	$\Phi_2^2\Phi_4$	$(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$	$(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$A_1 + C_3$	$\Phi_2^2\Phi_6$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$
$4A_1$	Φ_2^4	$(\mathbb{Z}/2\mathbb{Z})^4$	$(\mathbb{Z}/2\mathbb{Z})^2$

5 Elliptic regular coinvariants for E_8

Let $w \in W = W(E_8)$ be elliptic and regular. Recall that for E_8 this is equivalent to w being cyclotomic and $\neq 1$. By Lemma 4.1, the space of coinvariants X_w is nonzero iff the order of w is a power of the prime p. Recall that the symplectic form $\langle\ ,\ \rangle_w$ is nondegenerate on X_w. Hence we have a natural homomorphism $\varrho_w : C(w) \longrightarrow Sp(X_w)$ from the centralizer $C(w)$ of w in W to the group of automorphisms of the nondegenerate symplectic space X_w over $\mathbb{F}_p$.

If $w = -1$ then $X_w = X/2X$ and $C(w) = W$ preserves the quadratic form $q(x) = \frac{1}{2}\langle x, x\rangle \mod 2$ on $X/2X$. It is well known that image of ϱ_w is the orthogonal group $O(X/2X, q)$, which is properly contained in $Sp(X/2X)$.

In this section and the next we prove

Proposition 5.1 *If $w \in W = W(E_8)$ is elliptic and regular and not equal to -1 then the natural map $\varrho_w : C(w) \longrightarrow Sp(X_w)$ is surjective.*

Proof: The class of w is determined by its order $d \in \{3, 4, 5, 8\}$. The case $d = 3$ is the most complicated and is covered in the next section.

Consider the case $d = 5$, and let $K \subset \bar{\mathbb{Q}}^\times$ be the field generated by a fifth root of unity $\zeta \in \bar{\mathbb{Q}}^\times$. Since $\Phi_5(t) = 1 + t + t^2 + t^3 + t^4$, the form $h(x, y)$ on V_K is given by

$$h(x,y) = \langle x,y\rangle + \langle x, y+wy\rangle\zeta + \langle x, y+wy+w^2y\rangle\zeta^2 + \langle x, y+wy+w^2y+w^3y\rangle\zeta^3$$

and

$$h(x, y) \equiv -\langle x, y\rangle_w \mod P,$$

where $P = (1 - \zeta)\mathbb{Z}[\zeta]$ is the ramified prime in $\mathbb{Z}[\zeta]$.

From section 3.3.3 we have for $\alpha \in R$ either

$$\langle \alpha, w\alpha\rangle = 0 \quad \text{and} \quad \langle \alpha, w^2\alpha\rangle = -1$$

or

$$\langle \alpha, w\alpha\rangle = -1 \quad \text{and} \quad \langle \alpha, w^2\alpha\rangle = 0,$$

which leads to

$$h(\alpha, \alpha) = 2 + 2\zeta + \zeta^2 = (1 - \zeta)(1 + 2\zeta + 2\zeta^2 + \zeta^3),$$

or

$$h(\alpha, \alpha) = 2 + \zeta + \zeta^2 + \zeta^3 = (1 - \zeta)(1 + \zeta + \zeta^2 + \zeta^3),$$

respectively. Hence $h(\alpha,\alpha)(1-\zeta)^{-1} \equiv 1 \mod P$. It follows that the action of the K-reflection r_S on $X_w = X_K/PX_K \simeq \mathbb{F}_5^2$ is given by

$$r_S(x) = x - h(x,\alpha)\bar{\alpha} = x + \langle x,\alpha\rangle_w \bar{\alpha}, \tag{32}$$

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

$$r_S = \begin{bmatrix} 1 & \langle\beta,\alpha\rangle_w \\ 0 & 1 \end{bmatrix}, \qquad r_T = \begin{bmatrix} 1 & 0 \\ \langle\alpha,\beta\rangle_w & 1 \end{bmatrix}. \tag{33}$$

Hence r_S and r_T generate $SL_2(5)$, proving surjectivity for $d = 5$.

Consider the case $d = 8$ and let K be the field generated by the eighth roots of unity. Recall that each K-equivalence class S contains a root $\alpha \in S$ such that $\langle\alpha, w\alpha\rangle = 0$. We have $S \simeq 4A_1$ or $S \simeq D_4$. By Lemma 3.9, the latter holds iff $J(w)\alpha \in 2X$. Since $2 = (1-w)J(w)$, we have

$$S \simeq D_4 \quad \Leftrightarrow \quad \alpha \in (1-w)X \quad \Leftrightarrow \quad \rho_\alpha = 0.$$

For $S \simeq 4A_1$, we have $h(\alpha,\alpha) = 2$ so formula (32) holds in this case as well, and the rest of the proof is identical to the previous case.

For the case $d = 4$, we take a different tack. Let $\bar{X} = X/2X$, and let $O(\bar{X})$ be the orthogonal group of the quadratic form q defined above. The map $W \to O(\bar{X})$ sends w to an involution in $O(\bar{X})$ and the projection $X \to \bar{X}$ induces an isomorphism $\bar{X}_w \simeq X_w$ on coinvariants. Letting $\bar{X}^w$ denote the invariants of w in $\bar{X}$, we have an exact sequence

$$0 \longrightarrow \bar{X}^w \longrightarrow \bar{X} \xrightarrow{1-w} \bar{X} \longrightarrow \bar{X}_w \longrightarrow 0.$$

Hence the subgroup $U \subset O(\bar{X})$ acting trivially on $\bar{X}^w$ and $\bar{X}_w$ is the unipotent radical of the parabolic subgroup in $O(\bar{X})$ with Levi $GL_4(2)$. Let $\tilde{U}$ be the pre-image of U in W. We have

$$|U| = 2^6, \qquad |\tilde{U}| = 2^7.$$

The normalizer $N(w) = \{v \in W :\ w^v = w^{\pm 1}\}$ preserves the form $\langle\ ,\ \rangle_w$ on $\bar{X}_w$, and $\tilde{U}$ is the kernel of the induced map $N(w) \longrightarrow Sp(\bar{X}_w) = Sp_4(2)$.

Counting orders, we find the latter map is surjective. I claim there exists $v \in \tilde{U}$ such that $w^v = w^{-1}$. This will imply that we have an exact sequence

$$1 \longrightarrow \tilde{U} \cap C(w) \longrightarrow C(w) \longrightarrow Sp(\bar{X}_w) \longrightarrow 1,$$

completing the proof in this case.

To verify the claim, we use the notation of section 3.3.4 for roots of E_8. For $0 \leq i \leq 6$, let

$$\alpha_i = e_{i+1} - e_{i+2}, \quad \alpha_7 = e_7 + e_8, \quad \alpha_8 = \tfrac{1}{2}(-1,-1,-1,-1,-1,-1,-1,-1).$$

These roots correspond to the nodes in the extended Dynkin diagram, labelled as follows:

$$\begin{array}{cccccccc} 8 & 7 & 5 & 4 & 3 & 2 & 1 & 0 \\ & & 6 & & & & & \end{array}$$

We may take $w \in W(D_8)$, writing (ij) and t_i for a transposition and sign change, respectively:

$$w = (12)t_2 \cdot (34)t_3 \cdot (56)t_6 \cdot (78)t_8.$$

The element

$$v = (12) \cdot (34) \cdot (56) \cdot (78) = s_0 s_2 s_4 s_6$$

conjugates w to w^{-1} and fixes each $\rho_{\alpha_i} \in \bar{X}_w$. This last is clear except for $i = 1, 3$, but here we have $v\alpha_1 = -w\alpha_1$, $v\alpha_3 = w\alpha_3$. This completes the proof in this case. ■

6 Elliptic trialities

Let R be an irreducible root system, with $X = Q(R)$, $A = A(R)$, $W = W(R)$ as before. A **triality** is a group element of order three. An elliptic triality in A is cyclotomic with minimal polynomial $M(t) = t^2 + t + 1$ and characteristic polynomial $\det(t \cdot I_V - w) = (t^2+t+1)^k$, where $2k$, the rank of R, must be even. By regularity, there is at most one W-conjugacy class of elliptic trialities in A. If $w \in W$ then (29) implies that the index $[P(R) : Q(R)]$ is a power of 3. It follows that R has one of the types

$$A_2, \qquad G_2, \qquad F_4, \qquad E_6, \qquad E_8. \tag{34}$$

Elliptic trialities exist for each case in (34): 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.

If $w \notin W$ then $R = D_4$ and w is an elliptic triality in $W(F_4) = A(D_4)$. In this case, the inclusion $Q(D_4) \hookrightarrow P(D_4) = Q(F_4)$ induces an isomorphism on w-coinvariants. Hence the case $R = D_4$ is subsumed by the case $R = F_4$.

6.1 Coinvariants for trialities

By Lemma 4.1, we have

$$X_w \simeq \mathbb{F}_3^k. \tag{35}$$

Since $3 = (1-w)(2+w)$, we have $J(t) = 2+t$ and the corresponding symplectic form on X_w is given by

$$\langle x, y\rangle_w = \langle (2+w)x, y\rangle \mod 3.$$

Lemma 6.1 *Suppose $w \in A$ 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 6.2 *Suppose $\alpha, \beta \in R$ are short roots. Let 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 (28) implies that $\langle \alpha, \alpha\rangle = \langle \beta, \beta\rangle = 2$ for the cases in (34). We are assuming the element $\delta = \alpha - \beta$ vanishes in X_w, so there is $\lambda \in X$ such that

$$\delta = (1-w)\lambda, \tag{36}$$

and we can apply Lemma 6.1:

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

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

$$\langle \delta, \delta\rangle = 4 - 2\langle \alpha, \beta\rangle \in 3\mathbb{Z}. \tag{37}$$

Since $\langle \alpha, \beta \rangle \in \mathbb{Z}$, [2, VI.1.3] implies

$$\langle \alpha, \beta \rangle \in \{0, \pm 1, \pm 2\}.$$

However, equation (37) 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 [16, 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

$$\langle \lambda, \alpha \rangle,\ \langle \lambda, \beta \rangle \in \{0, \pm 1, \pm 2\}.$$

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

$$\langle \lambda, \alpha \rangle = 2 \quad \text{and} \quad \langle \lambda, \beta \rangle = -1, \tag{38}$$

or

$$\langle \lambda, \alpha \rangle = 1 \quad \text{and} \quad \langle \lambda, \beta \rangle = -2. \tag{39}$$

The first possiblity (38) implies that $\lambda = \alpha$, so (36) 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 the main result of this section. The automorphism group $A = A(R)$ of R contains W as a normal subgroup; we have $A = W$ for $R = G_2, F_4, E_8$ and $[A : W] = 2$ for $R = A_2, E_6$. Recall that the case $R = D_4$ is contained in the case $R = F_4$. If $w \in W$ is an elliptic triality, the centralizer $C_A(w)$ of w in A acts on the $\mathbb{F}_3$- vector space X_w, preserving the symplectic form $\langle\ ,\ \rangle_w$.

Proposition 6.3 *Let $w \in W$ be an elliptic triality. The natural action of $C_A(w)$ on X_w gives an exact sequence*

$$1 \longrightarrow \langle w \rangle \longrightarrow C_A(w) \longrightarrow Sp(X_w) \longrightarrow 1,$$

where $Sp(X_w)$ is the isometry group of the symplectic form $\langle\ ,\ \rangle_w$ on X_w. This sequence splits in all cases except $R = E_6$.

Proof: If $x \in A$, then xwx^{-1} is another elliptic triality, hence is W-conjugate to w. This shows that

$$|C_A(w)| = [A : W] \cdot |C_W(w)|,$$

hence this order is the given by degrees. These are tabulated below, along with a concrete description of the group $Sp(X_w)$ and its order.

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

In each case, we have

$$|C_A(w)| = 3|Sp(X_w)|.$$

Hence it suffices to prove that the kernel of the map $C_A(w) \to Sp(X_w)$ is generated by w.

Suppose that $u \in C_A(w)$ acts trivially on X_w. Then for every short root $\alpha \in R$, the roots $\alpha, u\alpha$ have the same image in X_w. Lemma 6.2 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. The short roots span V, so u has all of its eigenvalues in K.

Let $\mathcal{S}$ be the set of K-equivalence classes in R containing a short root. Since u preserves KS for $S \in \mathcal{S}$, it follows that u commutes with the group $W_K(S)$. The proof of Lemma 3.4 shows that the subgroup of W_K generated the groups $W_K(S)$ for $S \in \mathcal{S}$ is irreducible on V_K. This implies that u acts on V_K by a scalar in K. The roots of unity in $K^\times$ are generated by $-w$. Since -1 is acts nontrivially on the $\mathbb{F}_3$-vector space X_w, it follows that $u \in \langle w \rangle$, as claimed. ■

6.2 Subgroups of $Sp_4(3)$

All centralizers of elliptic trialities are algebraic subgroups of $Sp_4(3)$. We ignore A_2 since the automorphism group of this root system is $W(G_2)$. For this discussion it is convenient to number the simple roots of E_8 as follows:

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

and let

$$\begin{aligned} \alpha_9 &= \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 + 2\alpha_6, \\ \alpha_0 &= 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 5\alpha_4 + 4\alpha_5 + 3\alpha_6 + 3\alpha_7 + 2\alpha_8 \end{aligned}$$

be the highest roots in the E_6 Coxeter subsystem and E_8, respectively. Let $s_i \in W(E_8)$ be the reflection for α_i.

As our elliptic triality in $W(E_8)$, we take $w = w_0w_1w_2w_3$, where

$$w_0 = s_0s_8, \quad w_1 = s_1s_2, \quad w_2 = s_5s_4, \quad w_3 = s_6s_9.$$

Then

$$w_1 \in W(G_2), \quad w_1w_2w_3 \in W(F_4) \subset W(E_6)$$

are elliptic trialities in the respective groups. Let us write $C_R(x) = C_{A(R)}(x)$ for $R = G_2,\ F_4,\ E_6$ and $x \in W(E_8)$. We have

$$C_{G_2}(w_1) = C_{G_2}(w) \quad \text{and} \quad C_R(w_1w_2w_3) = C_R(w) \quad \text{for} \quad R = F_4, E_6.$$

Let ρ_i be the image of α_i in X_w. The quadruple $(\rho_0, \rho_6, \rho_3, \rho_7)$ is an ordered basis of $X_w = \mathbb{F}_3^4$ on which the form $\langle\ ,\ \rangle_w$ has matrix

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \tag{41}$$

From Proposition 6.3, we have

$$C_{E_8}(w) = \langle w \rangle \times Sp_4(3),$$

where $Sp_4(3)$ is identified with the elements of $C_{E_8}(w)$ of determinant one on V_K. 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 $Sp_4(3)$:

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

Here $*$ represents arbitrary independent elements of $\mathbb{F}_3$ such that the indicated matrix preserves the form (41).

6.3 A remark on transitivity

Let us call a vector $v \in X_w$ **nonsingular** if v lies outside the radical of $\langle\ ,\ \rangle_w$ when $R = E_6$, and if v is nonzero in the remaining cases. One can check that each root gives a nonsingular vector in X_w.

The idea for Lemma 6.2 came from the observation that the number of nonsingular vectors in X_w is one third the number of short roots, as follows.

$$\begin{array}{ll} A_2: & 3-1 \ = 6/3 \\ G_2: & 3-1 \ = 6/3 \\ F_4: & 3^2-1 = 24/3 \\ E_6: & 3^3-3 = 72/3 \\ E_8: & 3^4-1 = 240/3. \end{array} \tag{42}$$

Moreover, since $Sp(X_w)$ is transitive on nonsingular vectors in X_w. It follows from Proposition 6.3 that $C_A(w)$ is transitive on the set of short roots in R. In fact, since the highest short root is fixed by diagram symmetries, the smaller group $C_W(w)$ transitive on short roots. In the cases $R = G_2, F_4$ where there are multiple root lengths, there is an involution on E interchanging long and short roots and inverting w. It follows that $C_W(w)$ is also transitive on long roots in R.

6.4 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 [21] for the basic facts about elliptic curves. The automorphism group of any elliptic curve has order dividing 24 [21, 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 $w \in W(F_4)$. Proposition 6.3 shows that

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

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

$$\theta(w\lambda) = \theta(\lambda)\omega, \qquad \text{for all } \lambda \in \mathcal{H}. \tag{43}$$

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

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

Thus, the elliptic curve E gives an interpretation of the abstract isomorphism (35). In the next section, we'll see that E is also relevant to the elliptic triality in $W(E_6)$.

Before getting to that, we conclude the F_4 example with a remark on the 24-cell; this is the unique regular convex self-dual polytope in four dimensions (see [9, 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 $w \in W(F_4)$. From the last paragraph in section 6.3 we conclude that $C_{W(D_4)}(w) = SL_2(3)$ 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 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 tori.

6.5 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 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 ([21, p.327]) $B = \mathrm{Aut}(E)$ is given in

X, Y, Z coordinates by the projective matrices

$$\begin{bmatrix} 1 & us & t \\ 0 & u & s^2 \\ 0 & 0 & 1 \end{bmatrix}, \qquad u \in \mathbb{F}_4^\times, \quad [s,t,1] \in E(\mathbb{F}_4). \tag{44}$$

The subgroup with $u = 1$ is the quaternion group Q; 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, 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

$$PU_3(4) = E(\mathbb{F}_4) \rtimes SL_2(3).$$

Now, an elliptic triality $w \in W(F_4)$ is also an elliptic triality in $W = W(E_6)$. 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 $C_W(w) = W_K$ preserves the hermitian form h on V_K (see section 2.1). 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

$$W_K \simeq U_3(2),$$

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

$$W_K/\langle w \rangle \simeq PU_3(2).$$

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

Let $A = A(E_6)$ be the full automorphism group of the E_6 root system. In section 6.2, we have seen that $C_A(w)$ is a maximal parabolic subgroup in $Sp_4(3)$ with Heisenberg group H for unipotent radical. The Levi subgroup of $C_A(w)$ 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 3.2, the eigenspaces $\bar{V}(w,\zeta)$ and $\bar{V}(w,\zeta^2)$ are three dimensional irreducible representations of $C_W(w)$, 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 $C_W(w) = SL_2(3) \ltimes H$ [13, 2.4].

6.6 Elliptic trialities in E_8

For an elliptic triality $w \in W = W(E_8)$, the analogue of the elliptic curve E with its 3-torsion points is a cubic surface S with its 27 lines. 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. [8, p.480]).

Just as for E_6, the hermitian form h on V_K becomes a cubic polynomial on $X_K/2X_K$, which this time gives a two-fold covering

$$1 \longrightarrow \{\pm 1\} \longrightarrow C_{W(E_8)}(w) \longrightarrow U_4(2) \longrightarrow 1, \tag{45}$$

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.

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 $\mathbb{F}_4$. Using the Bruhat decomposition, one can check that 19 of the lines on S are rational over $\mathbb{F}_2$. Hence 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 $C_{W(E_8)}(w)$ of $U_4(2)$ via (45), we find that

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

where $\widetilde{W(E_6)}^+$ is a two-fold cover of $W(E_6)^+$.

On the other hand our split exact sequence in Proposition 6.3 realizes $Sp_4(3)$ as the subgroup of $C_{W(E_8)}(w) = W_K$ with determinant one on V_K. Thus we recover the isomorphism (cf. [5])

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

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

$$Sp_4(3) \to W(E_6)^+ \subset SO_6(\mathbb{R})$$

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

$$Sp_2(3) \to W(A_3)^+ \subset SO_3(\mathbb{R}).$$

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 $\bar{\mathbb{Q}}$ [5]. 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 [24]. As a representation of $U_4(2)$, Λ is the unipotent representation corresponding to the partition $4 = 2 + 1 + 1$. As shown in [15], 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. Thus, 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.

7 p-adic groups

Let k be a field of characteristic zero, complete with respect to a discrete valuation. This means that k is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, for some

integer prime p. Let K be a maximal unramified extension of k and let Frob be a topological generator of $\mathrm{Gal}(K/k)$. Fix an element $\varpi \in k$ of valuation $= 1$.

All connected reductive k-groups H that we consider will be split over K; we identify H with its group of K-rational points. The group of k-rational points is $H(k) = H^F$, where F is the endomorphism of H arising from the k-structure on H.

As mentioned in the introduction, the study of cyclotomic structures in this paper arose from the construction of L-packets in [11], [19]. For more background, see [14]. We recall this construction in the simplest case of a simply-connected k-group G which actually splits over k. Let F be the Frobenius endomorphism of G. Fix a maximal k-split torus in $T \subset G$. The root system R will be the system of co-roots of T in G. Since G is simply connected, the abelian group $X = \mathbb{Z}R = \mathrm{Hom}(GL_1, T)$ is the group of co-characters of T. Let N and $W = N/T$ be the normalizer and Weyl groups of T in G, respectively. The group N acts by affine transformations on the apartment $\mathcal{A} = \mathbb{R} \otimes X$ in the Bruhat-Tits building $\mathcal{B}$ of G. Given $n \in N$, there are unique elements $\lambda \in X$ and $w \in W$ such that n acts on $\mathcal{A}$ by the affine transformation $t_\lambda w : x \mapsto \lambda + wx$, and this gives a surjective homomorphism from N to the affine Weyl group $W_{\mathsf{aff}} = X \rtimes W$.

7.1 Tori and their characters

For any $w \in W$, we have a twisted k-torus T_w, where $T_w = T$ as sets, and the Frobenius endomorphism of T_w is wF, so that $T_w(k) = T^{wF}$. The torus T_w is anisotropic over k, equivalently $T_w(k)$ is compact, precisely if w is elliptic. The Galois cohomology group $H^1(K/k, T_w)$ is isomorphic to the torsion subgroup of X_w: If $\lambda \in X$ represents a torsion class $\rho_\lambda \in X_w$, then ρ_λ corresponds to the class $[c_\lambda] \in H^1(K/k, T_w)$ of the cocycle c_λ ending Frob to $\lambda(\varpi) \in T$.

We henceforth fix an elliptic element $w \in W$. Then X_w is finite, so we have an isomorphism

$$X_w \simeq H^1(K/k, T_w). \tag{46}$$

Each class $\rho \in H^1(K/k, T_w)$ determines an embedding $T_w \hookrightarrow G$, as follows. View ρ as a coset in X, via (46) and let $\lambda \in \rho$. The transformation $t_\lambda w$ has a unique fixed point $x_\lambda \in \mathcal{A}$, given by

$$x_\lambda = (1 - w)^{-1}\lambda = \frac{1}{m} J(w)\lambda.$$

The stabilizer G_{x_λ} of of x_λ in G is preserved by F and $K_\lambda := G^F_{x_\lambda}$ is a maximal compact subgroup of G^F. By the Lang-Steinberg theorem, there is an element

$p_\lambda \in G_{x_\lambda}$ such that $p_\lambda^{-1} F(p_\lambda) \in N \cap G_{x_\lambda}$ is a lift of $t_\lambda w$ in N. Conjugation by p_λ gives a map $\mathrm{Ad}(p_\lambda)$ on G which restricts to an embedding

$$\mathrm{Ad}(p_\lambda) : T \xrightarrow{\sim} T_\lambda \subset G \tag{47}$$

of T onto an F-stable torus T_λ in G, such that $\mathrm{Ad}(p_\lambda) \circ wF = F \circ \mathrm{Ad}(p_\lambda)$. We have $T_\lambda^F \subset K_\lambda$; in fact, K_λ is the unique maximal compact subgroup of G^F containing T_λ^F. Note that the embedding (47) depends on w, which has been fixed at the outset and suppressed from the notation.

Two such tori T_λ and T_μ (for $\lambda, \mu \in X$) are G^F-conjugate iff ρ_λ and ρ_μ are conjugate under the action of the centralizer $C(w) = C_W(w)$ on X_w. The map $\mathrm{Ad}(p_\lambda)$ sends the centralizer $C(w)$ to the group $W(T_\lambda, G)^F$ of F-rational points in the Weyl group of T_λ in G, and sends the stabilizer $C(w, \rho_\lambda)$ of ρ_λ to the subgroup $W(T_\lambda, G^F)$ of elements in $W(T_\lambda, G)^F$ having representatives in G^F.

Thus, the map $\lambda \mapsto T_\lambda$ induces a bijection from the $C(w)$-orbits in X_w to the G^F-orbits in the set $\mathcal{T}_w$ of F-stable maximal tori $S \subset G$ such that S^F is G-conjugate to T^{wF}. This map lifts to X_w as follows. Fix a character $\chi : T^{wF} \to \mathbb{C}^\times$ which is regular, in the sense of [14]. Given $\lambda \in X$, let $\chi_\lambda = \chi \circ \mathrm{Ad}(p_\lambda)$ be the corresponding character of T_λ^F. Thus we have an element $(T_\lambda, \chi_\lambda)$ in the set $\hat{\mathcal{T}}_{w,\chi}$ of pairs (S, θ), where S is an F-stable torus in G, θ is a character of S^F, and there is $g \in G$ such that $(S^F, \theta) = ({}^g(T^{wF}), {}^g\chi)$.

The group G^F acts by conjugation on $\mathcal{T}_w$ and $\hat{\mathcal{T}}_{w,\chi}$, with finitely many orbits, and the maps above give a commutative diagram [11, Lemma 9.6.1]

$$\begin{array}{ccc} X_w & \xrightarrow{\sim} & \hat{\mathcal{T}}_{w,\chi}/G^F \\ \downarrow & & \downarrow \\ X_w/C(w) & \xrightarrow{\sim} & \mathcal{T}_w/G^F \end{array} \tag{48}$$

where the horizontal maps are bijections, the left vertical map is the natural quotient and the right vertical map is induced by the projection onto the first factor.

For example, suppose G has type E_8 and w is cyclotomic. Recall that if $w = -1$, then $C(w)$ surjects onto the orthogonal group of $q(x) = \frac{1}{2}\langle x, x\rangle$ on $X_w = X/2X$, so there are three orbits: $\{0\},\ q = 0,\ q = 1$.

If $w \neq -1$, then Proposition 5.1 shows that there are two G^F-classes of tori in $\mathcal{T}_w$. One of them, represented by T_0, has $W(T_0, G)^F = W(T_0, G^F) \simeq C(w)$. The other, represented by T_λ for $\lambda \in R$, has $W(T_\lambda, G^F)$ being the two-fold cover of the stabilizer of a nonzero vector in $Sp(X_w)$.

7.2 Supercuspidal representations

The embeddings of anisotropic unramified tori in G are mirrored in the representation theory of G^F. Given $(S,\theta) \in \hat{\mathcal{T}}_{w,\chi}$, the compact maximal torus S^F fixes a unique point x in the building $\mathcal{B}$ of G, whose stabilizer $K_x = G^F_x$ is the unique maximal compact subgroup of G^F containing S^F. From the pair (S,θ), constructions due to Adler and Deligne-Lusztig give us a finite dimensional irreducible representation $\kappa(S,\theta)$ of K_x, which induces to an irreducible supercuspidal representation

$$\pi(S,\theta) := \mathrm{Ind}_{K_x}^{G^F} \kappa(S,\theta)$$

of G^F. We have $\pi(S,\theta) \simeq \pi(S',\theta')$ iff the pairs (S,θ) and (S',θ') are G^F-conjugate. Hence, for $\rho \in X_w$, we can define

$$\pi(\chi,\rho) := \pi(\chi_\lambda, T_\lambda)$$

for any $\lambda \in \rho$.

Thus, for each regular character χ of T^{wF}, we have a finite set ("L-packet")

$$\Pi_w(\chi) := \{\pi(\chi,\rho) : \ \rho \in X_w\}$$

of isomorphism classes of representations of G^F, parameterized by X_w.

The centralizer $C(w)$ enters this picture via the equivariance property [19]

$$\pi(\chi^y,\rho) = \pi(\chi, y\cdot\rho), \qquad y \in C(w). \tag{49}$$

Note that (49) is compatible with the isomorphism $C(w,\rho_\lambda) \simeq W(T_\lambda, G^F)$. It also shows that two classes $\pi(\chi,\rho)$ and $\pi(\chi, y\cdot\rho)$ contain representatives which are induced from the same maximal compact subgroup K_λ, the only difference being a twist of the character on T_λ by an element of G which normalizes T^F_λ. This simplifies the determination of the groups K_λ from which we induce to get the representations in $\Pi_w(\chi)$.

Since G is simply-connected, the G^F-conjugacy classes of maximal compact subgroups K are in bijection with maximal proper subdiagrams of the affine Dynkin diagram of G, which gives the type of the maximal reductive quotient of K. If $\rho_\lambda = 0$ then K_λ is hyperspecial and corresponds to the ordinary Dynkin diagram of G. If $\rho_\lambda \neq 0$, one can find the type of K_λ by first computing the point $x_\lambda = (1-w)^{-1}\lambda$ and then determining the root system consisting of all $\check{\alpha} \in \check{R}$ which take integer values on x_λ. In practice, it is more efficient to determine the stabilizer W_{x_λ} of x_λ in the affine Weyl group W_{aff}. The tangent space of $\mathcal{A}$ at x_λ is

the reflection representation of W_{x_λ}, so the latter contains the element $t_\lambda w \in W_{x_\lambda}$ having the same characteristic polynomal as w.

If G has type E_8 and w is cyclotomic then this method turns out to be sharp: Recall that if $X_w \neq 0$ then w is determined by its order $d \in \{2, 3, 4, 5, 8\}$. We list the prime-power orders of cyclotomic elements in the maximal finite subgroups of W_{aff}, other than W, as follows:

D_8	A_1A_7	$A_2A_1A_5$	$2A_4$	D_5A_3	E_6A_2	E_7A_1	A_8
$2, 4, 8$	none	none	5	none	3	2	none

The types of the inducing subgroups K_λ, for $\rho_\lambda \neq 0$, are then determined as follows: For $d = 2$ there are two orbits of $C(w)$ on $X_w - \{0\}$ and we find D_8 and E_7A_1 as the two types of maximal compact subgroups, other than K_0, appearing as inducing data in $\Pi_w(\chi)$. For $d \in \{3, 4, 8\}$ there is just one orbit of $C(w)$ on $X_w - \{0\}$, and indeed we find a unique type for each d in the table above.

References

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

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

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

[4] ———, *Conjugacy classes in the Weyl group*, Seminar in Algebraic Groups and related finite groups, Lecture Notes in Math. **131**, Springer-Verlag (1970), pp. 297–318.

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

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

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

[8] 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.

[9] _____, *Regular polytopes*, Dover, 1973.

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

[11] S. DeBacker and M. Reeder, *Depth-zero supercuspidal L-packets and their stability*, preprint, (2004), www2.bc.edu/~reederma/papers.html.

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

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

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

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

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

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

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

[19] _____, *Some supercuspidal L-packets of positive depth*, preprint, (2005), www2.bc.edu/~reederma/papers.html.

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

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

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

[23] 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.

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