ON SIMPLY LACED LIE ALGEBRAS AND THEIR MINUSCULE REPRESENTATIONS

JACOB LURIE

1. Introduction

The Lie algebra E_6 may be defined as the algebra of endomorphisms of a 27-dimensional complex vector space $M_{\mathbf{C}}$ which annihilate a particular cubic polynomial. This raises a natural question: what is this polynomial? If we choose a basis for $M_{\mathbf{C}}$ consisting of weight vectors $\{X_w\}$ (for some Cartan subalgebra of E_6), then any invariant cubic polynomial must be a linear combination of monomials $X_w X_{w'} X_{w''}$ where $w + w' + w'' = 0$. The problem is then to determine the coefficients of these monomials.

Of course, the problem is not yet well-posed, since we still have a great deal of freedom to scale the basis vectors X_w. If we work over the integers instead of the complex numbers, then much of this freedom disappears. The $\mathbf{Z}$-module M then decomposes as a direct sum of 27 weight spaces which are free $\mathbf{Z}$-modules of rank 1. The generators of these weight spaces are well-defined up to a sign. Using a basis for M consisting of such generators, a little bit of thought shows that the invariant cubic polynomial may be written as a sum

$$\sum_{w+w'+w''=0} \epsilon_{w,w',w''} X_w X_{w'} X_{w''}$$

where $\epsilon_{w,w',w''} = \pm 1$. The problem is now reduced to the determination of the signs $\epsilon_{w,w',w''}$. However, this problem is again ill-posed, since the X_w are only well-defined up to a sign.

This problem is resolved by examining more carefully what we mean by working "over $\mathbf{Z}$". First, let us consider the problem of constructing the (split) Lie algebra of E_6 over $\mathbf{Z}$. We know that this algebra should be a direct sum of the corresponding cocharacter lattice of rank 6 and 72 "root spaces" which are free $\mathbf{Z}$-modules of rank 1. Since there is no canonical choice of generator for these root spaces, one again encounters sign ambiguities which makes it difficult to give a direct definition of the Lie bracket. The set Γ of roots has a two-fold cover $\widetilde{\Gamma}$ consisting of all possible generators for root spaces. Moreover, this covering has a natural partially defined "multiplication" which arises from the Lie bracket. It turns out that this two-fold covering and its "multiplication" have a particularly transparent structure which is best understood by considering a two-fold covering $\widetilde{\Lambda}$ of the entire root lattice Λ. This leads to a construction of E_6, and every other simply-laced Lie algebra, over the integers.

The same ideas likewise may be applied to give a construction of all minuscule representations of simply laced algebras (again over $\mathbf{Z}$). We will describe this construction, together with a formalism which allows one to characterize multilinear maps between such representations. In particular, our formalism will apply to the cubic form on the representation M of E_6, and enable us to determine the signs $\epsilon_{w,w',w''}$.

Let us now summarize the contents of this paper. In §2 we will summarize the background material on which we draw. Much of this material (root systems, quadratic forms over $\mathbf{F}_2$, del Pezzo surfaces) is standard, while some (such as the connection between unitary structures and $\langle \pm \mathbf{1} \rangle$-extensions) is more obscure.

In §3 our work begins. First we show how to construct a Lie algebra, given the data of a double cover of its root lattice. We then develop a formalism which enables us to build its minuscule representations in an analogous way. Using this formalism, we will also be able to construct a number of natural multilinear maps between minuscule representations.

In §4, we apply our formalism to study an extension $\widetilde{W}$ of the Weyl group W of a (simply-laced) semisimple Lie algebra. Using this group, we will then show that the invariant multilinear maps constructed in §4 are the only ones which exist.

Finally, in §5 and §6, we specialize to the cases of E_6 and E_7. In these cases our formalism leads to explicit descriptions of the minuscule representations of these algebras, and of the invariant forms they carry.

1.1. **Acknowledgments.** I would like to thank Dick Gross, Joe Harris, and Brian Conrad for many helpful discussions.

1.2. **Notation and Terminology.** If M is a free module over a commutative ring R (for example a vector space over a field), we denote the dual module by $M^\vee$. If $x_1, \ldots, x_n$ is a basis for M, then we let $x_1^*, \ldots, x_n^*$ denote the dual basis for $M^\vee$. We will denote the symmetric and exterior powers of M by $\mathbb{S}^n(M)$ and $\wedge^n M$, respectively. These we regard as *quotients* of the n-fold tensor power of M. If S is an R-algebra, we let M_S denote $M \otimes_R S$ (we will use this convention only in the case $R = \mathbf{Z}$, so S can be an arbitrary ring).

A bilinear form $f(x, y)$ defined on a group M is said to be *alternating* if $f(x, x) = 0$ for all x. Note that this implies $f(x, y) = -f(y, x)$, but the converse fails in general when 2 is not invertible.

The symmetric group S_n acts on $M^{\otimes n}$. Correspondingly we get a *norm* (or *symmetrization*) map $M^{\otimes n} \to M^{\otimes n}$, given by the formula

$$m_1 \otimes \ldots \otimes m_n \mapsto \sum_{\sigma \in S_n} m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(n)}$$

This map induces a map from coinvariants to invariants; that is, a map $\phi : \mathbb{S}^n(M) \to (M^{\otimes n})^{S_n}$. The image of an element of $\mathbb{S}^n(M)$ under this map is called its *polarization*; it is a symmetric tensor. One also has a natural map $\psi : (M^{\otimes n})^{S_n} \to \mathbb{S}^n(M)$ in the other direction, given by restricting the projection. The composites $\phi \circ \psi$ and $\psi \circ \phi$ are both simply multiplication by $n! = |S_n|$. If $n!$ is invertible in R, then ϕ and ψ are both isomorphisms, which permits us to identify $\mathbb{S}^n(M)$ with the collection of symmetric tensors. Working over the integers (as we shall throughout this paper), one must be careful at the primes dividing $n!$.

We let $\langle \pm \mathbf{1} \rangle$ denote the two-element group of units of the ring $\mathbf{Z}$. In what follows we will frequently be concerned with extensions of groups (or sets) by $\langle \pm \mathbf{1} \rangle$. We follow the following general convention: if G is some object (such as a group), then $\widetilde{G}$ will generally denote a $\langle \pm \mathbf{1} \rangle$-extension of G. The extension will be specified in context. Elements of $\widetilde{G}$ will be denoted by $\widetilde{g}$, and the image of $\widetilde{g}$ in G will be denoted g.

If q is a prime power, we denote by $\mathbf{F}_q$ a finite field with q elements. If $K \subseteq L$ is a finite extension of fields and $x \in L$, we let $\mathrm{Tr}(x) \in K$ denote the trace of x. If S is a finite set, we let $|S|$ denote the cardinality of S.

If L is a Lie algebra acting on a module M, we write $M^L = \{m \in M : Lm = 0\}$. Elements of M^L are said to be *invariants* under L.

In what follows, we will discuss the Lie algebras of simply-laced, simply connected, semisimple groups which are split over $\mathbf{Z}$. The restriction to simply-laced groups is essential to what follows. However, our discussion could easily be modified so as to apply to groups over an arbitrary ground scheme which are not necessarily simply connected; their Lie algebras contain the Lie algebras of the simply-connected analogues with finite index. To simplify our exposition, we will leave these modifications to the reader.

2. Background

2.1. **Quadratic Forms.** In this section we briefly review some basic facts on quadratic forms. For details, we refer the reader to [2], Chapter 6.3. Let R be a commutative ring. A *quadratic space* over R is a projective R-module M of (finite) constant rank, equipped with a function $q : M \to R$ which possesses the following properties:

- $q(\lambda m) = \lambda^2 q(m)$.
- The function $\langle x, y \rangle = q(x+y) - q(x) - q(y)$ is R-linear in each variable. It is called the *bilinear form associated to* q.

Such a function q is said to be a *quadratic form* on M.

By definition, $\langle x, x \rangle = q(2x) - 2q(x) = 2q(x)$. If 2 is not a zero-divisor in R, then q is determined by $\langle x, x \rangle$: there is a one-to-one correspondence between quadratic forms q on M and symmetric bilinear forms $\langle , \rangle$ having the property that $\langle x, x \rangle$ is always divisible by 2. (For this reason, a quadratic space over $\mathbf{Z}$ is

also called an *even lattice*.) Thus, if 2 is invertible in R, quadratic forms and symmetric bilinear forms are essentially the same thing. At the other extreme, note that $\langle x, x\rangle = 0$ if $2 = 0$ in R, so $\langle , \rangle$ is an alternating bilinear form.

If $\langle , \rangle$ induces an isomorphism of M into its dual, we say q is *nondegenerate*. If 2 is not invertible in R, this is impossible unless M has even rank (as one sees by base change to a field of characteristic 2).

If M has even rank and q is nondegenerate on M, then we may associate to (M, q) a cohomology class in $H^1_{\text{ét}}(\operatorname{Spec} R, \mathbf{Z}/2\mathbf{Z})$, called the *discriminant* of q. This cohomology class classifies the center of the even part of the Clifford algebra associated to (M, q), which is a finite étale R-algebra of rank 2. The discriminant is additive (relative to the obvious notion of "direct sum" for quadratic spaces).

Example 2.1.1. Suppose (M, q) is a quadratic space, with M a free R-module of rank $2n$. If $x_1, \ldots, x_{2n}$ is a basis for M, then

$$A = (\langle x_i, x_j\rangle)$$

is an R-valued matrix; its determinant D is called the *determinant of* (M, q) and is well-defined up to the square of a unit in R. Note that D is invertible in R if and only if q is nondegenerate.

Assume now that R is local, (M, q) is nondegenerate, and 2 is a unit in R. An easy argument shows that we may choose $x_1, \ldots, x_{2n}$ so that the matrix A is diagonal. On the other hand, consider the product $X = x_1 x_2 \ldots x_{2n}$ in the Clifford algebra of (M, q). A simple argument shows that the center of the even part of the Clifford algebra is the free R-module generated by 1 and X. It follows by an easy computation that

$$X^2 = (-1)^n q(x_1) q(x_2) \ldots q(x_{2n}) = (-1)^n \frac{D}{2^{2n}}$$

Thus, under the canonical identification

$$H^1_{\text{ét}}(\operatorname{Spec} R, \mathbf{Z}/2\mathbf{Z}) \simeq R^\times / R^{\times 2}$$

obtained from Kummer theory, we see that the discriminant of (M, q) is represented by $(-1)^n D$.

In the special case $R = \mathbf{F}_2$ (which is really the only case of interest to us), the cohomology group $H^1_{\text{ét}}(\operatorname{Spec} R, \mathbf{Z}/2\mathbf{Z})$ is isomorphic to $\mathbf{Z}/2\mathbf{Z}$; in this case the discriminant is also called the *Arf invariant* of q. Quadratic forms of rank $2n$ with Arf invariant 0 are distinguished by the fact that they have $2^{2n-1} + 2^{n-1}$ isotropic vectors, while the forms with Arf invariant 1 have only $2^{2n-1} - 2^{n-1}$ isotropic vectors (a vector $v \in V$ is *isotropic* if $q(v) = 0$). Alternatively, quadratic spaces over $\mathbf{F}_2$ with Arf invariant 0 may be characterized by the existence of an n-dimensional subspace on which q vanishes identically. For proofs of these facts, we refer the reader to [2].

Note that if (M, q) is a quadratic space over R and $R \to R'$ is any ring homomorphism, we get a natural induced quadratic space $(M_{R'}, q_{R'})$ over R'. We will generally be interested in quadratic spaces over $\mathbf{F}_2$ which arise from even lattices via "reduction modulo 2". The result of such an operation is described in the following result:

Theorem 2.1.2. *Let Λ be an even lattice (that is, a quadratic space over $\mathbf{Z}$), (V, q) the associated quadratic space over $\mathbf{F}_2$. Assume Λ is nondegenerate over $\mathbf{Q}$. Via the form $\langle , \rangle$ we may identify Λ with a subgroup of $\Lambda^\vee$ having finite index d. Then (V, q) is nondegenerate if and only if d is odd. Its Arf invariant is equal to*

$$\begin{cases} 0 & \text{if } d \equiv \pm 1 \pmod 8 \\ 1 & \text{if } d \equiv \pm 3 \pmod 8 \end{cases}$$

Proof. Note that d is the absolute value of the determinant of Λ; hence the reduction of d modulo 2 is equal to the determinant of (V, q). This proves the first claim. For the second, let $R = \mathbf{Z}_{(2)}$ denote the localization of $\mathbf{Z}$ at the prime 2. Since d is odd, Λ_R is a nondegenerate quadratic space over R; let x denote its discriminant. Over $\mathbf{Q}$, the discriminant classifies the finite extension $\mathbf{Q}[\sqrt{\pm d}]$ (or $\mathbf{Q} \times \mathbf{Q}$, in the case $d = \pm 1$). Here the sign is chosen so that $\pm d \equiv 1 \pmod 4$, so 2 does not ramify in the corresponding quadratic extension of $\mathbf{Q}$. It follows that x classifies the étale R-algebra which is the integral closure R' of R in $\mathbf{Q}[\sqrt{\pm d}]$. Then the Arf invariant of (V, q) is 0 or 1 depending on whether or not the prime 2 splits or remains prime in $\mathbf{Q}[\sqrt{\pm d}]$. Our hypotheses imply that 2 cannot ramify in this extension, so we may write $\pm d = 4k + 1$. Then

$R' = R[\frac{1+\sqrt{4k+1}}{2}]$ is obtained by adjoining to R a root of the polynomial $x^2 - x - k$. Modulo 2, this equation has a solution if and only if k is even; that is, if $d \equiv \pm 1 \pmod 8$. ■

If (M, q) is a quadratic space, we denote by $O(M, q)$ the group of all R-automorphisms of M compatible with the form q. For any $x \in M$ with $q(x)$ invertible in R, the map

$$r_x : m \mapsto m - q(x)^{-1}\langle m, x\rangle x$$

is a 2-torsion element of $O(M, q)$, loosely understood as "reflection in the hyperplane corresponding to x". If R is a field and q is nondegenerate, then these reflections generate $O(M, q)$ unless $R = \mathbf{F}_2$, M has dimension 4, and the Arf invariant of (M, q) is trivial (for a proof, see the first chapter of [4]).

Finally, we recall for later use the statement of Witt's extension theorem (see also [4]):

Theorem 2.1.3. *Assume that R is a field and that q is nondegenerate. If U and U' are subspaces of M and $\alpha : U \to U'$ is an isomorphism such that $q(u) = q(\alpha(u))$, then α admits an extension to an element of $O(M, q)$.*

2.2. **Root Lattices.** In this section we will review the facts that will be needed concerning simply laced-root systems. For details, proofs, or a discussion of non-simply laced root systems, we refer the reader to [3].

Let us fix a bit of terminology. A *lattice* is a free $\mathbf{Z}$-module of finite rank equipped with a symmetric bilinear form $\langle , \rangle$. We will generally be interested in lattices Λ satisfying the following additional conditions:

- Λ is *even*: for any $\lambda \in \Lambda$, $\langle \lambda, \lambda \rangle$ is an even integer. Equivalently, $q(\lambda) = \frac{1}{2}\langle \lambda, \lambda \rangle$ is a quadratic form on Λ.
- Λ is *positive definite*: $\langle \lambda, \lambda \rangle > 0$ for any $\lambda \neq 0$.
- The set $\Gamma = \{\alpha \in \Lambda : q(\alpha) = 1\}$ generates Λ as a $\mathbf{Z}$-module.

These three properties characterize those lattices which arise as root lattices of simply laced, semisimple algebraic groups. For the remainder of this subsection we will assume Λ is such a lattice, corresponding to such an algebraic group G. We shall refer to Γ as its set of *roots*; this is a finite set. Note that if α and β are roots, then $\alpha + \beta$ is a root if and only if $\langle \alpha, \beta \rangle = -1$.

If α is a root, then

$$r_\alpha(\gamma) = \gamma - \langle \alpha, \gamma \rangle \alpha$$

is an automorphism of Λ. The set of all such reflections generates a group W called the *Weyl group*. Since Γ is finite, W-stable, and generates Λ, W is a finite group.

Via the bilinear form $\langle , \rangle$, we may identify Λ with a subset of the dual lattice $\Lambda^\vee$. The pairing $\langle , \rangle$ then extends to a $\mathbf{Q}$-valued bilinear form on $\Lambda^\vee$. The quotient $\Lambda^\vee / \Lambda$ is a finite group which is naturally dual to the center of the simply connected group G.

Since Λ is positive definite, each coset C of Λ in $\Lambda^\vee$ contains finitely many elements which have minimal norm $\langle v, v \rangle$. The collection of such elements of C will be denoted by C_0; they are called *minuscule weights*. We let t_C denote the value of $\langle v, v \rangle$ on C_0. Note that according to our convention, 0 *is* a minuscule weight.

Example 2.2.1. Consider the free $\mathbf{Z}$-module M spanned by generators $e_1, \ldots, e_n$, where $\langle e_i, e_j \rangle = \delta_{ij}$. Let $s = e_1 + \ldots + e_n$, and set $A_{n-1} = \{\lambda \in M : \langle \lambda, s \rangle = 0\}$.

It is clear that A_{n-1} is even and positive-definite. Moreover, the set

$$\{\lambda \in A_{n-1} : \langle \lambda, \lambda \rangle = 2\} = \{e_i - e_j : i \neq j\}$$

generates A_{n-1}, so that A_{n-1} has the three properties listed above; it is the root lattice of the group $G = \mathrm{SL}_n$. The group W may be identified with the symmetric group S_n, which acts by permuting the e_i.

Since M is nondegenerate, we may identify the dual $A_{n-1}^\vee$ of A_{n-1} with $M/\mathbf{Z}s$. Thus the group $A_{n-1}^\vee / A_{n-1}$ may be identified with $M/(\mathbf{Z}s + A_{n-1}) \simeq \mathbf{Z}/n\mathbf{Z}$, the isomorphism induced by the map $\lambda \mapsto \langle \lambda, s \rangle \pmod n$, defined for $\lambda \in M$. If C denotes the coset of A_{n-1} in $A_{n-1}^\vee$ corresponding to $0 \leq k < n$ via this isomorphism, then the minuscule weights of C are precisely the images of the elements of the set

$$\{e_{i_1} + e_{i_2} + \ldots + e_{i_k}\}_{1 \leq i_1 < i_2 < \cdots < i_k \leq n}$$

in $M/\mathbf{Z}s$. The norm $\langle v, v \rangle$ of such a weight is $\frac{k(n-k)}{n}$.

Example 2.2.2. Let M denote the free $\mathbf{Z}$-module spanned by generators $e_1, \ldots, e_n$ satifying $\langle e_i, e_j \rangle = \delta_{ij}$, $s = e_1 + \ldots + e_n$, and set $D_n = \{\lambda \in M : \langle \lambda, s \rangle \equiv 0 \pmod 2\}$.

Once again it is easy to see that D_n is positive definite and even, and the set

$$\{\lambda \in D_n : \langle \lambda, \lambda \rangle = 2\} = \{\pm e_i \pm e_j : i \neq j\}$$

generates D_n if $n > 1$, so D_n has the three properties enumerated above. In fact, D_n is the root lattice of the group $G = \mathrm{Spin}(2n)$. The group W may be identified with a semidirect product of the symmetric group S_n and its natural representation on $D_n/2M$; it acts by permuting the e_i and changing an even number of signs.

The lattice $D_n^\vee$ may be identified with $M + \frac{1}{2}s \subseteq \frac{1}{2}M$, so the quotient $D_n^\vee/D_n$ is isomorphic to $\mathbf{Z}/4\mathbf{Z}$ (if n is odd, so $s \notin D_n$) or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (if n is even, so $s \in D_n$).

The sets of minuscule weights corresponding to the four cosets of D_n in $D_n^\vee$ are $\{0\}$, $\{\pm e_i\}$ and the Weyl group orbits of $\frac{1}{2}s$ and $\frac{1}{2}(s - e_1)$. The norms of these four classes of weights are 0, 1, $\frac{n}{4}$, and $\frac{n}{4}$, respectively.

Note that if $n = 2$, D_n actually decomposes as a direct sum $A_1 \oplus A_1$. If $n = 3$, D_n is isomorphic to A_n.

Example 2.2.3. Once again, let M denote the free $\mathbf{Z}$-module spanned by generators $e_0, \ldots, e_n$, and set

$$\langle e_i, e_j \rangle = \begin{cases} -1 & \text{if } i = j = 0 \\ 1 & \text{if } i = j > 0 \\ 0 & \text{otherwise} \end{cases}$$

Let $s = 3e_0 - (e_1 + \ldots + e_n)$, and let $E_n = \{\lambda \in M : \langle \lambda, s \rangle = 0\}$. E_n is an even lattice of rank n. M has signature $(n, 1)$, so E_n is positive-definite if and only if $\langle s, s \rangle = n - 9$ is negative; that is, if $n \leq 8$. Finally, one may check that E_n is generated by $\Gamma = \{\lambda \in E_n : \langle \lambda, \lambda \rangle = 2\}$ if and only if $n \geq 3$.

Again, M is nondegenerate, so we may identify $E_n^\vee$ with the quotient $M/\mathbf{Z}s$. Thus $E_n^\vee/E_n$ is isomorphic to $M/\mathbf{Z}s + E_n \simeq \mathbf{Z}/\langle s, s \rangle \mathbf{Z}$; this cyclic group is generated by the image of e_1. In the next subsection we will give a geometric interpretation of the minuscule weights of the coset corresponding to this generator.

E_3 is isomorphic to the direct sum of A_1 and A_2, E_4 is isomorphic to A_4, and E_5 is isomorphic to D_5. However, the lattices E_6, E_7, and E_8 are new; they correspond to the exceptional groups with the same names.

If Λ and Λ' are two lattices possessing the three properties listed at the beginning of this section, then the orthogonal direct sum $\Lambda \oplus \Lambda'$ shares those properties. A basic result in the theory of root systems asserts that every such lattice may be obtained as an orthogonal direct sum of lattices of the form A_n, D_n ($n \geq 4$), E_6, E_7, and E_8 in a unique manner. On the other hand, the lattices just mentioned are *irreducible*, in the sense that they cannot be further decomposed in the same way. The situation for irreducible root lattices is summarized in the following:

Λ	$\Lambda^\vee/\Lambda$	$\lvert C_0 \rvert$	t_C
A_{n-1}	$\mathbf{Z}/n\mathbf{Z}$	$\binom{n}{k}$	$\frac{k(n-k)}{n}$
D_{2n}	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$1, 2^{2n-1}, 4n, 2^{2n-1}$	$0, \frac{n}{2}, 1, \frac{n}{2}$
D_{2n+1}	$\mathbf{Z}/4\mathbf{Z}$	$1, 2^{2n}, 4n+2, 2^{2n}$	$0, \frac{2n+1}{4}, 1, \frac{2n+1}{4}$
E_6	$\mathbf{Z}/3\mathbf{Z}$	$1, 27, 27$	$0, \frac{4}{3}, \frac{4}{3}$
E_7	$\mathbf{Z}/2\mathbf{Z}$	$1, 56$	$0, \frac{3}{2}$
E_8	$\{0\}$	1	0

We will need one more concept from the theory of root systems: that of a *root basis*, or *system of simple roots*. A root basis is a subset $\Delta \subseteq \Gamma$ which freely generates Λ, such that in the expression for any element $\alpha \in \Gamma$ as a linear combination of elements of Δ, the coefficients which appear are either all positive or all negative. The basic fact we shall need is that root bases exist, and the Weyl group W acts transitively on them (in fact, it acts simply transitively).

We conclude with a generalization of a well-known fact concerning the action of the Weyl group on the minuscule weights.

Theorem 2.2.4. *Let $C, C', C'' \in \Lambda^\vee/\Lambda$ be such that $C + C' + C'' = 0$. Then*

$$\{(c, c', c'') \in C_0 \times C_0' \times C_0'' : c + c' + c'' = 0\}$$

consists of a single Weyl group orbit.

Proof. Clearly it suffices to treat the case when Λ is irreducible. For this, we apply the classification and verify the result directly in each case. We give details for A_n, the most interesting case. There we may identify $\Lambda^\vee/\Lambda$ with the group $\mathbf{Z}/(n+1)\mathbf{Z}$. If $0 \leq i \leq n$ and C is the corresponding coset, we may identify the minimal elements of C with i-element subsets of $\{0, \ldots, n\}$. Given three cosets which sum to 0, there is a corresponding triple $0 \leq i, j, k \leq n$ with $i + j + k \equiv 0 \pmod{n+1}$. If $i = j = k = 0$ the result is obvious, while if $i+j+k > n+1$ we may replace each coset with its negative and reduce to the case $i+j+k \leq n+1$. Finally, if $i + j + k = n + 1$, then the assertion is equivalent to the evident fact that the symmetric group S_{n+1} acts transitively on the set of triples (X, Y, Z) of disjoint subsets of $\{0, \ldots n\}$ having respective sizes i, j, and k. ∎

Corollary 2.2.5. *Let $C \in \Lambda^\vee/\Lambda$. Then W acts transitively on C_0.*

Proof. Apply the last theorem to the cosets $C, -C$, and Λ. ∎

2.3. **del Pezzo Surfaces.** In this section, we review the connection between del Pezzo surfaces and exceptional root lattices. For more details, see [12].

We will invoke this discussion only sparingly in the rest of this paper, so the present section may be safely omitted by a reader who is unfamiliar with classical algebraic geometry.

For simplicity, we work over the complex numbers. Let S denote the surface obtained by blowing up $\mathbf{P}^2$ at n distinct points $p_1, \ldots, p_n$. Then $\mathrm{H}^2(S, \mathbf{Z})$ is the free lattice on generators H, $E_1, \ldots E_n$, where H is the pullback of the hyperplane class on $\mathbf{P}^2$ and the E_i are the classes of the exceptional divisors. The *negative* of the intersection pairing endows $\mathrm{H}^2(S, \mathbf{Z})$ with the structure of a lattice, isomorphic to the lattice M we used in the construction of the exceptional lattices.

We let K_S denote the canonical bundle (the top exterior power of the holomorphic cotangent bundle) of S. Let $s = -c_1(K_S) \in \mathrm{H}^2(S, \mathbf{Z})$. Then $s = 3H - (E_1 + \ldots + E_n)$. If $n \leq 8$ and the points $p_1, \ldots, p_n$ are in general position, then $-K_S$ is ample (surfaces with this property are called *del Pezzo* surfaces). We will henceforth assume this to be the case. Then the lattice

$$E_n = \{x \in \mathrm{H}^2(S, \mathbf{Z}) : x \cup s = 0\}$$

may be identified with the primitive cohomology of S (relative to an embedding of S in projective space via some power of the anticanonical bundle $-K_S$).

Of particular interest to us are the "lines" on S; that is, effective divisors E on S with $E.(-K_S) = 1$ (such divisors map to lines if we map S to projective space via its "anti-canonical series"). The Hodge index theorem implies that $E.E \leq 0$. Since the arithmetic genus of E is

$$\frac{1}{2}(E.E + E.K_S)$$

we see that E is a smooth rational curve with self-intersection -1. Conversely, suppose E is any divisor with $E.E = E.K_S = -1$. Then $K_S - E$ cannot be effective (it has negative intersection with the ample class $-K_S$), so $h^2(S, E) = h^0(S, K_S - E) = 0$, and the Riemann-Roch theorem implies

$$h^0(S, E) \geq 1 + \frac{1}{2}(E.E - K_S.E) = 1$$

so that E is an effective class.

We can give the "lines" on S a lattice-theoretic interpretation, as follows. Note that if $e \in \mathrm{H}^2(S, \mathbf{Z})$ is the class of a line E, then $\langle e, s \rangle = -e.s = 1$, so that the image of e is a generator of $E_n^\vee/E_n$. Let e' denote the image of e in $E_n^\vee$. One easily calculates that $\langle e', e' \rangle = \frac{10-n}{9-n}$. If $e'' \in E_n^\vee$ is any other lattice element representing the same coset of E_n, then $e'' = e' + \lambda$ for $\lambda \in E_n$, so that $\langle e'', e'' \rangle \equiv \langle e', e' \rangle \pmod 2$. If $n < 8$, then

$$\frac{10-n}{9-n} < 2$$

which implies that $\langle e', e' \rangle \leq \langle e'', e'' \rangle$. If equality holds, one easily checks that e'' is the image of the class of a unique "line" on S. Thus, for $n < 8$, the "lines" on S correspond bijectively to the elements in $E_n^\vee$ of minimal length among those representing a fixed generator of $E_n^\vee / E_n$. For $n = 8$, this argument breaks down. The 240 lines on S correspond to the 240 roots of the E_8 lattice.

Example 2.3.1. If $n \leq 6$ and the points $p_1, \ldots, p_n$ are chosen in general position, then $-K_S$ is actually very ample and gives rise to an embedding of S in $\mathbf{P}^{9-n}$ as a surface of degree $9 - n$. For $n = 0$, the image surface contains no lines. If $n = 1$, S contains a single line: the exceptional divisor of the blow up. If $n = 2$, S contains three lines: the two exceptional divisors and the proper transform of the line joining the two chosen points in $\mathbf{P}^2$. For $n = 3$ or 4, the same reasoning shows that we get 6 and 10 lines, respectively.

If $n = 5$, $-K_S$ embeds S in $\mathbf{P}^4$ as an intersection of two quadric hypersurfaces. In this case S contains 16 lines. In addition to the 5 exceptional divisors and the proper transforms of the 10 lines joining the 5 chosen points, we have the proper transform of the conic passing through the 5 points.

If $n = 6$, $-K_S$ embeds S in $\mathbf{P}^3$ as a smooth cubic surface. In this case S contains 27 lines (6 exceptional divisors, 15 proper transforms of lines, and 6 proper transforms of conics). This situation is much-studied in classical geometry; we will return to it in our discussion of E_6.

If $n = 7$, $-K_S$ is not very ample, but still has no base locus. It induces a map to $\mathbf{P}^2$, which realizes S as a double cover of the plane branched over a smooth quartic curve Δ. In this case S contains 56 "lines" (7 exceptional divisors, 21 proper transforms of lines, 21 proper transforms of conics, and the proper transforms of the 7 cubics which pass through all 7 points and are double at one of the points), which project two-to-one onto the 28 bitangents to Δ.

If $n = 8$, $-K_S$ corresponds to a pencil of plane cubics passing through the points $p_1, \ldots, p_8$. This linear series has a nonempty base locus: the ninth point of intersection of the pencil. There are 240 "lines" on S, but their geometric interpretation is less clear.

2.4. **$\langle \pm \mathbf{1} \rangle$-Extensions.** Let A be an abelian group. In this section we will be concerned with groups $\widetilde{A}$ which are *extensions of* A by $\langle \pm \mathbf{1} \rangle$. In other words, we want to study exact sequences of the form

$$0 \to \langle \pm \mathbf{1} \rangle \to \widetilde{A} \to A \to 0$$

Note that since the group $\langle \pm \mathbf{1} \rangle$ has no nontrivial automorphisms, such an extension is necessarily central.

Two $\langle \pm \mathbf{1} \rangle$-extensions of A are *isomorphic* (as extensions of A) if there is an isomorphism between them (as groups) compatible with the maps to A. Isomorphism classes of $\langle \pm \mathbf{1} \rangle$-extensions are classified by the cohomology group $\mathrm{H}^2(A, \langle \pm \mathbf{1} \rangle)$.

Since A is abelian, the group law $A \times A \to A$ is a group homomorphism. Consequently we get a sequence of natural maps

$$\begin{array}{rcl} \mathrm{H}^2(A, \langle \pm \mathbf{1} \rangle) & \to & \mathrm{H}^2(A \times A, \langle \pm \mathbf{1} \rangle) \\ & \to & \mathrm{Hom}(\mathrm{H}_2(A \times A, \mathbf{Z}), \langle \pm \mathbf{1} \rangle) \\ & \to & \mathrm{Hom}(\mathrm{H}_1(A, \mathbf{Z}) \otimes \mathrm{H}_1(A, \mathbf{Z}), \langle \pm \mathbf{1} \rangle) \\ & \simeq & \mathrm{Hom}(A \otimes A, \langle \pm \mathbf{1} \rangle) \end{array}$$

More concretely, we can associate to any $\langle \pm \mathbf{1} \rangle$-extension $\widetilde{A}$ of A a bilinear $\mathbf{Z}/2\mathbf{Z}$-valued form $\langle , \rangle : A \times A \to \mathbf{Z}/2\mathbf{Z}$ by the equation

$$(-1)^{\langle x, y \rangle} = \widetilde{x}\widetilde{y}\widetilde{x}^{-1}\widetilde{y}^{-1}$$

One can easily show that $\langle , \rangle$ is well-defined, bilinear, and strictly alternating (that is, $\langle a, a \rangle = 0$ for any $a \in A$). Thus the above construction actually yields a natural transformation

$$\phi : \mathrm{H}^2(A, \langle \pm \mathbf{1} \rangle) \to \mathrm{Hom}(\wedge^2 A, \mathbf{Z}/2\mathbf{Z})$$

Suppose now that A is annihilated by 2. Then we can define a finer invariant of $\widetilde{A}$ as follows. For $v \in A$, define $q(v) \in \mathbf{Z}/2\mathbf{Z}$ by the equation

$$(-1)^{q(v)} = \widetilde{v}^2 \in \langle \pm \mathbf{1} \rangle$$

It is easy to verify that q is a quadratic form on the $\mathbf{F}_2$-vector space A. In fact, $q(v+u)-q(v)-q(u) = \langle v, u \rangle$ is the alternating form defined above. In other words, we get a natural transformation

$$\phi' : \mathrm{H}^2(A, \langle \pm \mathbf{1} \rangle) \to \mathbb{S}^2(A)^\vee$$

In simple cases, these invariants completely characterize the extensions:

Theorem 2.4.1. *If A is a finitely generated, free $\mathbf{Z}$-module then ϕ is an isomorphism. If A is a finite-dimensional $\mathbf{F}_2$-vector space, then ϕ' is an isomorphism.*

Proof. Using the Künneth formula, one sees that it suffices to prove these assertions in the cases where $A = \mathbf{Z}$ and $A = \mathbf{F}_2$, respectively. In these cases, it is easy to check the result directly. ∎

Let us now return to the general case. If $\widetilde{A}$ is any $\langle \pm \mathbf{1} \rangle$-extension of an abelian group A, we will write $\mathrm{Aut}(\widetilde{A})$ to denote its group of automorphisms *as an extension of* A; that is, the collection of all automorphisms leaving $\langle \pm \mathbf{1} \rangle \subseteq \widetilde{A}$ stable (this is frequently, but not always, the full automorphism group of $\widetilde{A}$). This group acts naturally on the quotient $A \simeq \widetilde{A}/\langle \pm \mathbf{1} \rangle$, so we get a natural homomorphism $\mathrm{Aut}(\widetilde{A}) \to \mathrm{Aut}(A)$. The kernel of this homomorpism consists of those $\psi : \widetilde{A} \to \widetilde{A}$ which have the form $\psi(\widetilde{a}) = \epsilon(a)\widetilde{a}$, where $\epsilon(a) \in \langle \pm \mathbf{1} \rangle \subseteq \widetilde{A}$. One can easily check that such a map is a homomorphism if and only if $\epsilon : A \to \langle \pm \mathbf{1} \rangle$ is a homomorphism. In other words, we have an exact sequence

$$0 \to \mathrm{Hom}(A, \langle \pm \mathbf{1} \rangle) \to \mathrm{Aut}(\widetilde{A}) \to \mathrm{Aut}(A)$$

This sequence is generally not exact on the right. Indeed, any $\psi \in \mathrm{Aut}(\widetilde{A})$ induces an automorphism of A which must preserve any structure invariantly associated to the extension $\widetilde{A}$. Thus, if $A = V$ is a finite-dimensional $\mathbf{F}_2$-vector space, we get a factorization

$$\mathrm{Aut}(\widetilde{V}) \to O(V, q) \subseteq \mathrm{Aut}(V)$$

The map on the left is surjective; this follows from the fact that the extension $\widetilde{A}$ is classified up to isomorphism by q. Thus we actually get a short exact sequence

$$0 \to V^\vee \to \mathrm{Aut}(\widetilde{V}) \to O(V, q) \to 0$$

Similar reasoning may be applied in case A is a finitely-generated free $\mathbf{Z}$-module. In this case the sequence takes the form

$$0 \to \mathrm{Hom}(A, \langle \pm \mathbf{1} \rangle) \to \mathrm{Aut}(\widetilde{A}) \to \mathrm{Aut}(A, \langle , \rangle) \to 0$$

where $\mathrm{Aut}(A, \langle , \rangle)$ denotes the "symplectic group" of all automorphisms of A compatible with the alternating form $\langle , \rangle$.

2.5. **Unitary Structures and $\langle \pm \mathbf{1} \rangle$-extensions.** If V is an $\mathbf{F}_2$-vector space, extensions of V by $\langle \pm \mathbf{1} \rangle$ correspond bijectively to quadratic forms on V. For any quadratic form q, there is an extension $\widetilde{V}$, unique up to isomorphism, such that $\widetilde{v}^2 = (-1)^{q(v)}$. However, there is no functorial manner in which $\widetilde{V}$ may be associated to the pair (V, q). Indeed, the natural surjection $\mathrm{Aut}(\widetilde{V}) \to O(V, q)$ does not split in general. However, this surjection may well split over some large subgroup of $O(V, q)$. Correspondingly, one might hope to define $\widetilde{V}$ functorially in terms of (V, q) *and* some additional data. We will now show that this is possible when given a Hermitian structure on V.

In what follows, we fix a generator ω for the multiplicative group of $\mathbf{F}_4$. Let V be an $\mathbf{F}_4$-vector space equipped with a Hermitian form h. That is, $h : V \times V \to \mathbf{F}_4$ is map which is linear in the first variable and satisfies the law $h(x, y) = \overline{h(y, x)}$, where $\overline{x} = x^2$ denotes the nontrivial automorphism of $\mathbf{F}_4$ over $\mathbf{F}_2$. Then $q(v) = h(v, v) \in \mathbf{F}_2$ defines a quadratic form on the underlying $\mathbf{F}_2$-vector space; the associated symplectic form is given by $\langle u, v \rangle = \mathrm{Tr}(h(u, v))$.

We define a group $\overline{V}$ as follows. The elements of $\overline{V}$ are formal symbols $\pm\overline{v}$, where $v \in V$. We define multiplication so that

$$\overline{v}\overline{u} = (-1)^{\mathrm{Tr}\,(\omega h(v,u))}\overline{v+u}$$

$$(-x)y = x(-y) = -(xy)$$

It is easy to see that $\overline{V}$ is a group. The element $\overline{0}$ is the identity of $\overline{V}$, and $-\overline{0}$ is a central involution. The quotient of $\overline{V}$ by the subgroup generated by $-\overline{0}$ is canonically isomorphic to V again; thus $\overline{V}$ is a $\langle\pm\mathbf{1}\rangle$-extension of V. Furthermore, for $v \in V$, $\overline{v}$ is a lift of v and $\overline{v}^2 = (-1)^{\mathrm{Tr}\,(\omega q(v))}\overline{0} = (-1)^{q(v)}\overline{0}$, as desired.

Let G denote the group of all semilinear automorphisms of V compatible with the form q. That is, an element $g \in G$ is an $\mathbf{F}_2$-linear orthogonal transformation of (V, q) with the property that $g(tv) = \sigma_g(t)g(v)$, where σ_g is an automorphism of $\mathbf{F}_4$ over $\mathbf{F}_2$. The assignment $g \to \sigma_g$ is a homomorphism from G to $\mathrm{Gal}(\mathbf{F}_4 : \mathbf{F}_2)$ whose kernel is the unitary group $U(V, h)$. We define an action of G on $\overline{V}$ as follows:

$$g(\pm\overline{v}) = \begin{cases} \pm\overline{g(v)} & \text{if } \sigma_g \text{ is the identity} \\ \pm(-1)^{q(v)}\overline{g(v)} & \text{otherwise} \end{cases}$$

In particular, the map $V \to V$ given by multiplication by $\omega \in \mathbf{F}_4^\times$ lies in the unitary group, giving a canonical automorphism of $\overline{V}$ of order 3, which we will denote by $\overline{\omega}$.

Theorem 2.5.1. *Let $\widetilde{V}$ be some $\langle\pm\mathbf{1}\rangle$ extension of an $\mathbf{F}_2$-vector space V' such that the associated quadratic space (V, q) is $2n$-dimensional and nondegenerate. The definition of $\overline{\omega}$ gives a one-to-one correspondence between the following types of data:*

- *$\mathbf{F}_4$-structures on V, together with Hermitian forms h inducing the quadratic form q and isomorphisms $\widetilde{V} \simeq \overline{V}$ over V.*
- *Elements $g \in \mathrm{Aut}(\widetilde{V})$ of order 3 such that that g fixes only the center of $\widetilde{V}$.*

Such data exist if and only if the Arf invariant of (V, q) is equal to n.

Proof. One direction is clear: given an $\mathbf{F}_4$-structure on V together with a Hermitian form h and an isomorphism $\widetilde{V} \simeq \overline{V}$, the automorphism $\overline{\omega}$ pulls back to an automorphism of $\widetilde{V}$ with the appropriate properties. We must now show that if $g \in \mathrm{Aut}(\widetilde{V})$ has order 3 and fixes only the center of $\widetilde{V}$, then from g we may reconstruct the rest of the data on V.

Since g must fix the center, we have an induced action of g on V. Since g has order 3,

$$0 = g^3 - 1 = (g-1)(1+g+g^2)$$

annihilates V. On the other hand, since g has no fixed points on V, $g - 1$ is invertible so $1 + g + g^2 = 0$. Thus we may define an action of $\mathbf{F}_4$ on V by setting $\omega v = g(v)$.

We define h as follows. Let $\langle , \rangle$ denote the alternating form associated to q. Since $v + \omega v + \omega^2 v$ vanishes, we have $\langle v, u\rangle + \langle \omega v, u\rangle + \langle \omega^2 v, u\rangle = 0$ for any u. Thus either all three of these terms vanish, in which case we set $h(v, u) = 0$, or $\langle \omega^i v, u\rangle = \langle \omega^j v, u\rangle = 1$ and $\langle \omega^k v, u\rangle = 0$, in which case we set $h(v, u) = \omega^{-k}$. One easily checks that h is a Hermitian form on V. For any $v \in V$ we have $\langle v, v\rangle = 0$, and so $h(v, v) = \langle \omega v, v\rangle = \langle \omega^2 v, v\rangle$. On the other hand,

$$q(v) = q(\omega^2 v) = q(v + \omega v) = q(v) + q(\omega v) + \langle v, \omega v\rangle = \langle v, \omega v\rangle$$

so that h induces the given form q on V.

For $\widetilde{v} \in \widetilde{V}$, set $\epsilon_{\widetilde{v}} = \widetilde{v}g(\widetilde{v})g^2(\widetilde{v})$. We define a map $\phi : \widetilde{V} \to \overline{V}$ by the rule $\phi(\widetilde{v}) = \epsilon_{\widetilde{v}}\overline{v}$. For $\widetilde{v}, \widetilde{u} \in \widetilde{V}$, we have

$$\epsilon_{\widetilde{v}\widetilde{u}} = \widetilde{v}\widetilde{u}g(\widetilde{v}\widetilde{u})g^2(\widetilde{v}\widetilde{u}) = \epsilon_{\widetilde{v}}\epsilon_{\widetilde{u}}(-1)^{\langle u, g(v)\rangle + \langle u, g^2(v)\rangle + \langle g(u), g^2(v)\rangle}$$

Since $\langle g(u), g^2(v)\rangle = \langle u, g(v)\rangle$, the exponent is equal to

$$\langle u, g^2(v)\rangle = \langle u, \omega^2 v\rangle = \mathrm{Tr}\, h(u, \omega^2 v) = \mathrm{Tr}\,(\omega h(u, v))$$

From this it follows that $\phi(\widetilde{v}\widetilde{u}) = \phi(\widetilde{v})\phi(\widetilde{u})$, so ϕ is a group homomorphism. Using the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \longrightarrow & \widetilde{V} & \longrightarrow & V & \longrightarrow 0 \\ & & \downarrow & & \downarrow \phi & & \downarrow & \\ 0 & \longrightarrow & \mathbf{Z}/2\mathbf{Z} & \longrightarrow & \overline{V} & \longrightarrow & V & \longrightarrow 0 \end{array}$$

we see that ϕ is an isomorphism. The automorphism $\overline{\omega}$ carries $\pm\overline{v}$ to $\pm\overline{\omega v}$; to see that this goes over to the automorphism $g \in \mathrm{Aut}(\widetilde{V})$, we need to check that $\epsilon_{\widetilde{v}} = \epsilon_{g(\widetilde{v})}$. That is, we need to know that

$$\widetilde{v} g(\widetilde{v}) g^2(\widetilde{v}) = g(\widetilde{v}) g^2(\widetilde{v}) g^3(\widetilde{v})$$

In other words, we must show that $\widetilde{v}$ commutes with $g(\widetilde{v})g^2(\widetilde{v})$. The commutator is given by

$$\langle v, g(v) + g^2(v) \rangle = \langle v, \omega v + \omega^2 v \rangle = \langle v, v \rangle = 0$$

as required. This completes the reconstruction of our original data from the automorphism g. It is easy to see that the recipe we just gave is the only one possible, which completes the proof of the main claim.

For the last point, note that all nondegenerate Hermitian spaces (V, h) over $\mathbf{F}_4$ split as direct sums of one-dimensional nondegenerate Hermitian spaces over $\mathbf{F}_4$. In such a space, q is nonzero on all three nonzero vectors, so (V, q) has Arf invariant 1. Inductively we see that a nondegenerate quadratic space admitting a compatible Hermitian structure must have Arf invariant n. On the other hand, nondegenerate quadratic spaces of even dimension are classified up to isomorphism by their Arf invariant, so if (V, q) has Arf-invariant n then it admits a compatible Hermitian structure. Since $\langle \pm \mathbf{1} \rangle$ extensions of $\mathbf{F}_2$-vector spaces are classified up to isomorphism by the associated quadratic form, it follows that that an isomorphism $\widetilde{V} \simeq \overline{V}$ always exists. ∎

By Theorem 2.1.2, we see that Theorem 2.5.1 applies in particular in case $V = \Lambda/2\Lambda$ where Λ is a root lattice of type E_6, E_8, or A_n ($n \equiv 0, 2 \pmod 8$). We will make use of this in our discussion of E_6.

3. Constructions

We assume now, and throughout the rest of this paper, that Λ is a positive definite even lattice generated by $\Gamma = \{\alpha \in \Lambda : \langle \alpha, \alpha \rangle = 2\}$. We let V denote the $\mathbf{F}_2$-vector space $\Lambda/2\Lambda$. The form

$$q : \Lambda \to \mathbf{Z}$$
$$q(\lambda) = \frac{\langle \lambda, \lambda \rangle}{2}$$

descends to an $\mathbf{F}_2$-valued quadratic form on V which we also denote by q.

The $\mathbf{Z}$-valued bilinear form $\langle , \rangle$ induces a $\mathbf{Z}/2\mathbf{Z}$-valued bilinear form which we will also denote by $\langle , \rangle$. Since Λ is even, $\langle , \rangle$ is alternating (interpreted as a $\mathbf{Z}/2\mathbf{Z}$-valued form), and therefore classifies some $\langle \pm \mathbf{1} \rangle$-extension $\widetilde{\Lambda}$ of Λ. Similarly, the form q classifies a $\langle \pm \mathbf{1} \rangle$-extension $\widetilde{V}$ of V. Either of these may be recovered from the other. Indeed, if we start with $\widetilde{V}$, we can set

$$\widetilde{\Lambda} = \Lambda \times_V \widetilde{V} = \{(\lambda, \widetilde{v}) \in \Lambda \times \widetilde{V} : \lambda \equiv v \pmod 2\}$$

Suppose instead that we begin with the extension $\widetilde{\Lambda}$. One can easily check that the map

$$\phi : \widetilde{\Lambda} \to \widetilde{\Lambda}$$
$$\widetilde{\lambda} \mapsto (-1)^{q(\lambda)} \widetilde{\lambda}^2$$

is a group homomorphism. The image of ϕ is a normal subgroup of $\widetilde{\Lambda}$. It is not hard to see that the cokernel of ϕ is a $\langle \pm \mathbf{1} \rangle$-extension of V corresponding to the quadratic form q.

The extension $\widetilde{\Lambda}$ will play a crucial role in resolving sign ambiguities when Λ is the root lattice of a simply-laced semisimple group G. Over the integers, the corresponding Lie algebra is almost completely determined by the lattice Λ. The lattice Λ itself may be identified with the tangent space to a maximal torus. The remainder of the Lie algebra is a direct sum of root spaces, each of which is a free $\mathbf{Z}$-module of rank 1. However, there is no canonical choice of generator for these root spaces, and this makes it difficult to describe the Lie bracket. To resolve this problem, we will actually introduce *two* generators for each root

space, corresponding to the two preimages of a root in $\widetilde{\Lambda}$. These generators will be indexed by the set $\widetilde{\Gamma}$, the preimage of Γ in $\widetilde{\Lambda}$.

3.1. **The Lie Algebra L.** Let L' denote the free abelian group generated by symbols $X_{\widetilde{\gamma}}$ where $\widetilde{\gamma} \in \widetilde{\Gamma}$, modulo the relations $X_{-\widetilde{\gamma}} = -X_{\widetilde{\gamma}}$. For $x \in \langle \pm \mathbf{1} \rangle$, we let ϵ_x denote the corresponding element of $\mathbf{Z}$. Now set $L = \Lambda \oplus L'$. We endow L with a bilinear bracket operation $[,]$ as follows:

- $[\lambda, \lambda'] = 0$ for $\lambda, \lambda' \in \Lambda$.
- $[\lambda, X_{\widetilde{\gamma}}] = -[X_{\widetilde{\gamma}}, \lambda] = \langle \lambda, \gamma \rangle X_{\widetilde{\gamma}}$ for $\lambda \in \Lambda$.
- $[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = X_{\widetilde{\gamma}\widetilde{\gamma}'}$ if $\gamma + \gamma' \in \Gamma$.
- $[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = \epsilon_{\widetilde{\gamma}\widetilde{\gamma}'\gamma}$ if $\gamma + \gamma' = 0$.
- $[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = 0$ otherwise.

Theorem 3.1.1. *L is a Lie algebra over $\mathbf{Z}$.*

Proof. One easily sees that the above definition is compatible with the relation $X_{-h} = -X_h$. To complete the proof, we must show that the bracket is alternating ($[X, X] = 0$) and that the Jacobi identity holds ($[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0$). The skew-symmetry is obvious from the definitions; we must check the Jacobi identity. By symmetry it suffices to consider four cases:

- $x, y, z \in \Lambda$. Then all brackets vanish and we are done.
- $x, y \in \Lambda$, $z = X_{\widetilde{\gamma}}$. Then $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = \langle x, \gamma \rangle \langle y, \gamma \rangle X_{\widetilde{\gamma}} - \langle y, \gamma \rangle \langle x, \gamma \rangle X_{\widetilde{\gamma}} + 0 = 0$.
- $x \in \Lambda$, $y = X_{\widetilde{\gamma}}$, $z = X_{\widetilde{\gamma}'}$. If $\gamma + \gamma' = 0$, then

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0 - \langle x, \gamma' \rangle \epsilon_{\widetilde{\gamma}\widetilde{\gamma}'\gamma} + \langle x, \gamma \rangle \epsilon_{\widetilde{\gamma}\widetilde{\gamma}'}\gamma' = 0$$

  If $\gamma + \gamma' \in \Gamma$, then

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = \langle x, \gamma + \gamma' \rangle X_{\widetilde{\gamma}\widetilde{\gamma}'} - \langle x, \gamma' \rangle X_{\widetilde{\gamma}\widetilde{\gamma}'} + \langle x, \gamma \rangle X_{\widetilde{\gamma}'\widetilde{\gamma}}$$

  Since $\gamma + \gamma'$ is a root, $\langle \gamma, \gamma' \rangle = -1$, so $\widetilde{\gamma}\widetilde{\gamma}' = -\widetilde{\gamma}'\widetilde{\gamma}$; then $X_{\widetilde{\gamma}'\widetilde{\gamma}} = -X_{\widetilde{\gamma}\widetilde{\gamma}'}$ and the result follows.

  If $\gamma + \gamma' \neq 0$ is not in Γ, then all three terms vanish.
- $x = X_{\widetilde{\alpha}}$, $y = X_{\widetilde{\beta}}$, $z = X_{\widetilde{\gamma}}$. There are two cases to consider. First suppose $\alpha + \beta + \gamma = 0$. Then $\beta + \gamma = -\alpha \in \Gamma$, so that $[x,[y,z]] = [X_{\widetilde{\alpha}}, X_{\widetilde{\beta}\widetilde{\gamma}}] = \epsilon_{\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}}\alpha$. Similarly $[y,[z,x]] = \epsilon_{\widetilde{\beta}\widetilde{\gamma}\widetilde{\alpha}}\beta$ and $[z,[x,y]] = \epsilon_{\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta}}\gamma$. Since $\alpha + \beta$ is a root, we must have $\langle \alpha, \beta \rangle = -1$ so $\widetilde{\alpha}\widetilde{\beta} = -\widetilde{\beta}\widetilde{\alpha}$; similarly $\widetilde{\alpha}\widetilde{\gamma} = -\widetilde{\gamma}\widetilde{\alpha}$ and $\widetilde{\beta}\widetilde{\gamma} = -\widetilde{\gamma}\widetilde{\beta}$. Thus $\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma} = \widetilde{\beta}\widetilde{\gamma}\widetilde{\alpha} = \widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta} = \pm 1$, so

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = \pm(\alpha + \beta + \gamma) = 0$$

  Now suppose $\alpha + \beta + \gamma \neq 0$. If $[x,[y,z]] + [y,[z,x]] + [z,[x,y]]$ is to be nonzero, at least one term, say $[x,[y,z]]$ must be nonzero. Without loss of generality $\beta + \gamma$ and $\alpha + \beta + \gamma$ are both roots; in other words $\langle \beta, \gamma \rangle = -1$ and $\langle \alpha, \beta + \gamma \rangle = -1$. Since the asymmetry of the bracket is known, we may further assume (possibly switching y and z) that $\langle \alpha, \beta \rangle \leq -1$ and $\langle \alpha, \gamma \rangle \geq 0$. If $\langle \alpha, \beta \rangle = -1$, then $[y,[z,x]] = 0$, $[x,[y,z]] = X_{\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}}$ and $[z,[x,y]] = X_{\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta}}$. But these cancel since $\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta} = \widetilde{\alpha}\widetilde{\gamma}\widetilde{\beta} = -\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}$.

  Finally, suppose that $\langle \alpha, \beta \rangle = -2$, so that $\alpha = -\beta$. Then $[x,[y,z]] = X_{\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}} = \epsilon_{\widetilde{\alpha}\widetilde{\beta}} X_{\widetilde{\gamma}}$, $[y,[z,x]] = 0$, and $[z,[x,y]] = [z,(\widetilde{\alpha}\widetilde{\beta})\alpha] = -\langle \gamma, \alpha \rangle \epsilon_{\widetilde{\alpha}\widetilde{\beta}} z$, and the sum vanishes once again.

■

Theorem 3.1.2. *$L_{\mathbf{C}}$ is a simply-laced, semisimple Lie algebra over $\mathbf{C}$, with root lattice Λ.*

Proof. Recall ([11], Chapter VI) that semisimplicity of a complex Lie algebra is equivalent to the nondegeneracy of the *Killing form*

$$(X, Y)_k = \mathrm{Tr}\{Z \mapsto [X,[Y,Z]]\}$$

An easy computation shows that

$$L_{\mathbf{C}} = \Lambda_{\mathbf{C}} \oplus \bigoplus_{\pm\alpha \in \Gamma} (\mathbf{C} X_{\pm\widetilde{\alpha}} \oplus \mathbf{C} X_{\pm\widetilde{-\alpha}})$$

is an orthogonal decomposition of $L_{\mathbf{C}}$ into nondegenerate subspaces. Thus $L_{\mathbf{C}}$ is semisimple. $\Lambda_{\mathbf{C}}$ is obviously a Cartan subalgebra, identified with its dual via the Killing form. The root spaces for this Cartan subalgebra are spanned by the $X_{\widetilde{\alpha}}$. Identifying $\Lambda_{\mathbf{C}}$ with its dual via $\langle , \rangle$, we see that the roots span exactly the lattice $\Lambda \subseteq \Lambda_{\mathbf{C}}$. ■

Over $\mathbf{Z}$, the Killing form is far from nondegenerate. We can define a "better" symmetric bilinear form $(,)$ on L as follows:

$$(\lambda, \lambda') = \langle \lambda, \lambda' \rangle$$
$$(\lambda, X_{\widetilde{\alpha}}) = (X_{\widetilde{\alpha}}, \lambda) = 0$$
$$(X_{\widetilde{\alpha}}, X_{\widetilde{\beta}}) = \begin{cases} \epsilon_{\widetilde{\alpha}\widetilde{\beta}} & \text{if } \alpha + \beta = 0 \\ 0 & \text{otherwise} \end{cases}$$

An easy computation shows that $(,)$ is an L-invariant pairing of $L \otimes L \to \mathbf{Z}$. Furthermore, the restriction of $(,)$ to the orthogonal complement of Λ is irreducible. It follows that the absolute value of the determinant of $(,)$ is equal to $|\Lambda^{\vee}/\Lambda|$. If Λ is irreducible, then the irreducibility of the adjoint representation of $L_{\mathbf{C}}$ implies that $(,)_k = c(,)$ for some constant c. We can determine c by evaluating both sides on a root α. We obtain

$$2c = (\alpha, \alpha)_k = \sum_{\beta} \langle \beta, \alpha \rangle^2 = 2 \sum_{\langle \beta, \alpha \rangle \geq 0} \langle \beta, \alpha \rangle^2$$

Thus $c = 4 + |\{\beta : \langle \beta, \alpha \rangle = 1\}|$.

The values of c are given in the following table:

Λ	c
A_{n-1}	$2n$
D_n	$4n-4$
E_6	24
E_7	36
E_8	60

See Chapter I.4 of [13] for a calculation of this constant for more general Lie algebras and a discussion of its relationship to the "bad primes" of a Lie algebra.

Remark 3.1.3. If, in the definition of $(,)_k$, we compute traces with respect to representations other than the standard representation, we can do a little better. Using the standard representations of A_n and D_n, we get $c = 1$ and $c = 2$, respectively. The nontrivial minuscule representations of E_6 and E_7 give $c = 6$ and $c = 12$.

3.2. **Cosets $C \in \Lambda^{\vee}/\Lambda$.** Recall that a representation of a semisimple Lie algebra (over $\mathbf{C}$) is said to be *minuscule* if the Weyl group acts transitively on its nonzero weights. There is one minuscule representation corresponding to each $\Lambda^{\vee}/\Lambda$ (we will later show how to construct this representation); it is characterized by the property that its highest weight vector has minimal length (within that coset). We will take this as our starting point.

Let C be a coset of Λ in $\Lambda^{\vee}$. Recall that t_C denotes the minimal value attained by $\langle , \rangle$ on C. We write $C_0 = \{x \in C : \langle x, x \rangle = t_C\}$; by 2.2.5, this consists of a single orbit under the Weyl group.

Before we begin, we will need a few combinatorial facts about the set C_0. Since all elements of C_0 have the same length, no three of them can lie on a line. For some lines, we can be even more specific:

Lemma 3.2.1. *Let $v \in C_0$ and let α be a root. Then $v + t\alpha \in C_0$ if and only if $t = 0$ or $t = -\langle \alpha, v \rangle$.*

Proof. $v - \langle \alpha, v \rangle \alpha$ is the image of v under the reflection through the hyperplane orthogonal to α; since C_0 is invariant under W we must have $v - \langle \alpha, v \rangle \alpha \in C_0$.

For the "only if" direction, note that $v, v - \langle \alpha, v \rangle \alpha$, and $v + t\alpha$ all lie on a line. It follows that these three points are not distinct; either $t = 0$, $t = -\langle \alpha, v \rangle$, or $\langle \alpha, v \rangle = 0 \neq t$. In the last case, Weyl invariance gives $v - t\alpha \in C_0$, and we get a contradiction since $\{v - t\alpha, v, v + t\alpha\}$ is a set of distinct collinear points of C_0. ■

Lemma 3.2.2. *If $v \in C_0$, $\alpha \in \Gamma$, then $|\langle v, \alpha\rangle| \leq 1$.*

Proof. Replacing α by $-\alpha$ if necessary we may assume $\langle v, \alpha\rangle \geq 0$. By minimality we must have

$$\langle v - \alpha, v - \alpha\rangle \geq \langle v, v\rangle$$

Using $\langle \alpha, \alpha\rangle = 2$, this gives $\langle v, \alpha\rangle \leq 1$ as desired. ■

Lemma 3.2.3. *Let $v \in C_0$, and let α, β be roots with $\alpha + \beta \neq 0$. Assume $v + \alpha \in C_0$ and $v + \alpha + \beta \in C_0$. Then $\langle \alpha, \beta\rangle = 0$ if $v + \beta \in C_0$ and -1 otherwise.*

Conversely, if $\langle \alpha, \beta\rangle = -1$ and $v + \alpha + \beta \in C_0$, then either $v + \alpha \in C_0$ or $v + \beta \in C_0$.

Proof. Since $v + \alpha \in C_0$, we have $\langle v, \alpha\rangle = -1$; similarly $\langle v + \alpha, \beta\rangle = \langle v, \beta\rangle + \langle \alpha, \beta\rangle = -1$. If $v + \beta \in C_0$, we get $\langle v, \beta\rangle = -1$ and thus $\langle \alpha, \beta\rangle = 0$.

Now suppose $v + \beta \notin C_0$. Then $v + \beta$ is not the image of v under the reflection r_β corresponding to β, so $\langle v, \beta\rangle \neq 1$. Then $\langle v, \beta\rangle \geq 0$ so we must have $\langle \alpha, \beta\rangle \leq -1$. Since $\alpha \neq -\beta$; we also have $\langle \alpha, \beta\rangle \geq -1$, proving the assertion.

For the converse, note that $\alpha+\beta$ is a root. Thus $v+\alpha+\beta \in C_0$ just means $-1 = \langle v, \alpha+\beta\rangle = \langle v, \alpha\rangle + \langle v, \beta\rangle$. Without loss of generality we have $\langle v, \alpha\rangle = -1$, $\langle v, \beta\rangle = 0$, which proves $v + \alpha \in C_0$. ■

3.3. **The Category $\mathcal{C}$.** In order to construct the minuscule representation corresponding to a coset of Λ in $\Lambda^\vee$, we will need some sort of data analogous to the two-fold cover $\widetilde{\Lambda}$ of Λ. The most straightforward approach is to attempt to embed $\widetilde{\Lambda}$ in some $\langle \pm \mathbf{1}\rangle$-extension $\widetilde{\Lambda^\vee}$ of $\Lambda^\vee$. Unfortunately, this is not always possible (though this idea has its merits, which will be spelled out in §3.5 and §3.9). In general, the best we can hope for is to cover the cosets of Λ "one at a time".

We let $\mathcal{C}$ denote the category whose objects are maps $\pi : \widetilde{C} \to \Lambda^\vee$, where $\widetilde{C}$ is a $\widetilde{\Lambda}$-torsor (that is, a set on which the group $\widetilde{\Lambda}$ acts on the left, freely and transitively) and π is $\widetilde{\Lambda}$-equivariant. Here $\widetilde{\Lambda}$ acts on $\Lambda^\vee$ by translations by elements of its quotient group Λ.

If $\pi : \widetilde{C} \to \Lambda^\vee$ and $\pi' : \widetilde{C'} \to \Lambda^\vee$ are objects of $\mathcal{C}$, a *morphism* from π to π' is a $\widetilde{\Lambda}$-equivariant map $\phi : \widetilde{C} \to \widetilde{C'}$ such that $\pi' \circ \phi = \pi$. Such a morphism is necessarily invertible, so $\mathcal{C}$ is a groupoid.

We now show that $\mathcal{C}$ has the structure of a (nonadditive) tensor category. To begin, let us define the tensor product of two objects of $\mathcal{C}$.

Let $\pi : \widetilde{C} \to \Lambda^\vee$ be an object in $\mathcal{C}$. There is also a natural right action of $\widetilde{\Lambda}$ on $\widetilde{C}$, by the formula

$$x\widetilde{\gamma} = (-1)^{\langle \pi(x), \gamma\rangle}\widetilde{\gamma}x$$

One easily checks that the left and right actions of $\widetilde{\Lambda}$ commute with one another.

Now suppose $\pi : \widetilde{C} \to \Lambda^\vee$ and $\pi' : \widetilde{C'} \to \Lambda^\vee$ both lie in $\mathcal{C}$. Define $\pi \otimes \pi' : \widetilde{C} \times_{\widetilde{\Lambda}} \widetilde{C'} \to \Lambda^\vee$ by the formula $(\pi \otimes \pi')(\widetilde{c} \times \widetilde{c'}) = \pi(\widetilde{c}) + \pi'(\widetilde{c'})$. One readily checks that $\pi \otimes \pi'$ is an object of $\widetilde{C}$; further there are natural isomorphisms

$$(\pi \otimes \pi') \otimes \pi'' \simeq \pi \otimes (\pi' \otimes \pi'')$$

which constitute an associativity constraint for $\mathcal{C}$.

The natural map $\pi_0 : \widetilde{\Lambda} \to \Lambda \to \Lambda^\vee$ gives rise to a canonical "identity" object of $\mathcal{C}$. Furthermore one can define $\widetilde{C}^{-1} = \{\widetilde{c}^{-1} : \widetilde{c} \in \widetilde{C}\}$; this has a left $\widetilde{\Lambda}$ action given by $\widetilde{\gamma}\widetilde{c}^{-1} = (\widetilde{c}\widetilde{\gamma}^{-1})^{-1}$ and a map to $\Lambda^\vee$ given by $(\pi^{-1})(\widetilde{c}^{-1}) = -\pi(c)$.

One has canonical isomorphisms $\pi_0 \otimes \pi \simeq \pi$, $\pi \otimes \pi_0 \simeq \pi$, and $\pi \otimes \pi^{-1} \simeq \pi_0 \simeq \pi^{-1} \otimes \pi$ (the last defined so that $\widetilde{c} \times \widetilde{c}^{-1} \to 1 \in \widetilde{\Lambda}$). Thus we have a tensor structure (with duality) on the category $\mathcal{C}$.

3.4. **Minuscule Representations.** We are now ready to construct the minuscule representations of L. Fix an object π of $\mathcal{C}$. Let $\widetilde{C}_0$ denote $\pi^{-1}(C_0)$. Let M_π denote the free abelian group generated by symbols $\{Y_{\widetilde{c}}\}_{\widetilde{c} \in \widetilde{C_0}}$, modulo the relations $Y_{-\widetilde{c}} = -Y_{\widetilde{c}}$. Thus, the rank of M is equal to the cardinality of C_0.

We define a bilinear map $[,] : L \otimes M_\pi \to M_\pi$ as follows:

$$[x, Y_{\widetilde{c}}] = \begin{cases} \langle x, c\rangle Y_{\widetilde{c}} & \text{if } x \in \Lambda \\ Y_{\widetilde{\gamma}\widetilde{x}} & \text{if } x = X_{\widetilde{\gamma}} \text{ and } \gamma + c \in C_0 \\ 0 & \text{if } x = X_{\widetilde{\gamma}} \text{ and } \gamma + c \notin C_0 \end{cases}$$

Theorem 3.4.1. *The map described above defines an action of L on M_π.*

Proof. We must show that the relation $[[x,y],u] = [x,[y,u]] - [y,[x,u]]$ is satisfied. Since this relation is bilinear we may assume $u = Y_{\widetilde{c}}$. If $x, y \in \Lambda$ the result is obvious. If $x \in \Lambda$, $y = X_{\widetilde{\gamma}}$, then

$$[[x,y],u] = \langle x, \gamma \rangle [X_{\widetilde{\gamma}}, Y_{\widetilde{c}}] = \langle x, \gamma \rangle Y_{\widetilde{\gamma c}}$$

(with the understanding that $Y_{\widetilde{\gamma c}} = 0$ if $\gamma + c \notin C_0$.) Meanwhile the left side is

$$[x, Y_{\widetilde{\gamma c}}] - \langle x, c \rangle Y_{\widetilde{\gamma c}} = (\langle \gamma + c, x \rangle - \langle c, x \rangle) Y_{\widetilde{\gamma c}}$$

as desired. The case where $x = X_{\widetilde{\gamma}}$, $y \in \Lambda$ is handled by the same reasoning.

Thus we are reduced to considering the case where $x = X_{\widetilde{\gamma}}$, $y = X_{\widetilde{\gamma}'}$. There are several cases, depending on the value of $n = \langle \gamma, \gamma' \rangle$. Suppose first that $n = -2$. Then

$$[[x,y],z] = (\widetilde{\gamma}\widetilde{\gamma}'\langle \gamma \rangle, c \rangle Y_{\widetilde{c}}$$

$[x,[y,z]]$ vanishes unless $\langle \gamma, c \rangle = 1$, in which case $[x,[y,z]] = Y_{\widetilde{\gamma}\widetilde{\gamma}'\widetilde{c}}$. Similarly $[y,[x,z]] = Y_{\widetilde{\gamma}'\widetilde{\gamma c}}$ if $\langle \alpha, c \rangle = -1$ and vanishes otherwise. Since $\widetilde{\gamma}$ and $\widetilde{\gamma}'$ commute and $-2 < \langle \alpha, \gamma \rangle < 2$, we get

$$[x,[y,z]] - [y,[x,z]] = \langle \alpha, \gamma \rangle Y_{\widetilde{\gamma}\widetilde{\gamma}'\widetilde{c}} = \epsilon_{\widetilde{\gamma}\widetilde{\gamma}'} \langle \gamma, c \rangle Y_{\widetilde{c}}$$

as desired.

If $n = -1$, then $[x,y] = X_{\widetilde{\gamma}\widetilde{\gamma}'}$. If $\gamma + \gamma' + c \notin C_0$ there is nothing to prove. Otherwise, $[[x,y],z] = Y_{\widetilde{\gamma}\widetilde{\gamma}'\widetilde{c}}$. By Lemma 3.2.3 we have without loss of generality $\gamma' + c \notin C_0$ and $\gamma + c \in C_0$, so $[x,[y,z]] = 0$ and

$$-[y,[x,z]] = -[X_{\widetilde{\gamma}'}, Y_{\widetilde{\gamma c}}] = -Y_{\widetilde{\gamma}'\widetilde{\gamma c}} = Y_{\widetilde{\gamma}\widetilde{\gamma}'\widetilde{c}}$$

as needed.

If $n = 0$, then $[x,y] = 0$, so we just need to show $[x,[y,z]] = [y,[x,z]]$. If $\langle \gamma, \gamma' \rangle = 0$, then $\widetilde{\gamma}\widetilde{\gamma}' = \widetilde{\gamma}'\widetilde{\gamma}$. Without loss of generality we may assume $[x,[y,z]] \neq 0$; then $\gamma + \gamma' + c, \gamma' + c \in C_0$. It suffices to show that both sides are equal to $Y_{\widetilde{\gamma}\widetilde{\gamma}'\widetilde{c}} = Y_{\widetilde{\gamma}'\widetilde{\gamma c}}$, which in turn follows from the fact that $\gamma + c \in C_0$, again by Lemma 3.2.3.

If $n > 0$, we have again $[x,y] = 0$ so the left side vanishes. Lemma 3.2.3 shows that $c, c+\gamma'$, and $c+\gamma'+\gamma$ cannot all lie in C_0, so $[x,[y,z]]$ vanishes. Similarly $[y,[x,z]]$ vanishes and we are done. ∎

Consequently we get a functor $\pi \rightsquigarrow M_\pi$ from the groupoid $\mathcal{C}$ to the category of representations of L. The automorphism group of any object $\pi \in \mathcal{C}$ is $\langle \pm \mathbf{1} \rangle$; this group acts on M_π, multiplying by $\langle \pm \mathbf{1} \rangle$. We will later show that this is the full automorphism group of M_π (as a representation of L).

Clearly M_π decomposes into weight spaces corresponding to the elements of C_0. Thus over $\mathbf{C}$, M_π is a minuscule representation corresponding to the coset C; in particular it is irreducible. In fact, a much stronger irreducibility result holds:

Theorem 3.4.2. *Let R be a commutative ring, and let $M \subseteq M_\pi \otimes_{\mathbf{Z}} R$ be a submodule invariant under the action of L_R. Then $M = \mathfrak{a}(M_\pi \otimes_{\mathbf{Z}} R)$ for some ideal $\mathfrak{a} \subseteq R$.*

Note that this result does *not* hold for the adjoint representation of L (for example, $M = 2\mathfrak{pgl}_2$ is an invariant subspace of $\mathfrak{sl}_2$ over $\mathbf{Z}$ which has index 4, and hence is not of the above form).

Proof. Each element of M can be written as a sum

$$\sum_{c \in C_0} k_{\widetilde{c}} Y_{\widetilde{c}}$$

where $k_{-\widetilde{c}} = -k_{\widetilde{c}}$. Let K be the set of all coefficients $k_{\widetilde{c}}$ which occur in such decompositions, and let $\mathfrak{a}$ be the ideal generated by K. Clearly $M \subseteq \mathfrak{a}(M_\pi \otimes_{\mathbf{Z}} R)$, so it suffices to verify the reverse inclusion. For this, it suffices to show that for any $k \in K$ and any $\widetilde{c}$, we have $kY_{\widetilde{c}} \in M$.

We now apply the fact that W operates transitively on C_0. Since W is generated by the reflections r_α and

$$[X_{\widetilde{\alpha}}, Y_{\widetilde{c}}] = Y_{\widetilde{c}'}, c' = r_\alpha(c)$$

when $\langle \alpha, c \rangle = -1$, it suffices to verify that for each nonzero $k \in K$, there is *some* $\widetilde{c}$ with $kY_{\widetilde{c}} \in M$.

Consider all sums

$$s = \sum_{c \in C_0} k_{\widetilde{c}} Y_{\widetilde{c}} \in M$$

such that $k_{\widetilde{c}} = k$ for some $\widetilde{c}$. We know that at least one such sum exists. Therefore we may consider the one with the minimal number of nonzero terms. If s has only one nonzero term, then $kY_{\widetilde{c}} = s \in M$ and we are done. Otherwise, we may assume that $k = k_{\widetilde{c}}$ and that $k_{\widetilde{d}} \neq 0$ for $c \neq d$. The transitivity of W implies that the sets $\{\alpha \in \Gamma : \langle \alpha, c\rangle = -1\}$ and $\{\alpha \in \Gamma : \langle \alpha, d\rangle = -1\}$ have the same size. Since $c \neq d$, these sets are not identical; therefore there is a root α with $\langle \alpha, c\rangle = -1 < \langle \alpha, d\rangle$. Then $[X_{\widetilde{\alpha}}, s]$ lies in M, contains k as a coefficient, and has fewer nonzero terms, a contradiction. ■

3.5. **Cosets of Odd Order.** The isomorphism class of an object $\pi \in \mathcal{C}$ is determined by the image of π in $\Lambda^\vee$. This makes the category $\mathcal{C}$ almost superfluous; it is necessary only because every object has non-trivial automorphisms (in fact, the automorphism group of any object in $\mathcal{C}$ is $\langle \pm \mathbf{1}\rangle$ assuming $\langle , \rangle$ is nondegenerate on Λ). However, it is possible to canonically associate an object of $\mathcal{C}$ to every coset of odd order, thus simplifying our formalism in this case.

Let Λ_o denote the union of all cosets of Λ in $\Lambda^\vee$ having odd order. Then there is a canonical isomorphism $\Lambda_o/2\Lambda_o \simeq \Lambda/2\Lambda = V$. Let $\widetilde{\Lambda}_o$ denote the fiber product $\Lambda_o \times_V \widetilde{V}$. This is a $\langle \pm \mathbf{1}\rangle$-extension of Λ_o containing $\widetilde{\Lambda}$. For any coset C of Λ in Λ_o, its preimage $\widetilde{C}$ in $\widetilde{\Lambda}_o$ is a $\widetilde{\Lambda}$-torsor. Moreover, the composite

$$\pi_C : \widetilde{C} \to \widetilde{\Lambda}_o \to \Lambda_o \subseteq \Lambda^\vee$$

is an object of $\mathcal{C}$, naturally associated to the coset C. Furthermore, there are canonical isomorphisms $\pi_\Lambda \simeq \pi_0$, $\pi_{-C} \simeq \pi_C^{-1}$, $\pi_C \otimes \pi_{C'} \simeq \pi_{C+C'}$, determined by the group structure on $\widetilde{\Lambda}_0$.

3.6. **Multiplication.** We now show how the tensor structure on the category $\mathcal{C}$ manifests itself in the world of Lie algebra representations. Let π and π' be objects in $\mathcal{C}$. We define a map $\phi_{\pi,\pi'} : M_\pi \otimes M_{\pi'} \to M_{\pi\otimes\pi'}$. Set

$$\phi_{\pi,\pi'}(Y_{\widetilde{c}}, Y_{\widetilde{c}'}) = \begin{cases} Y_{\widetilde{c}\,\widetilde{c}'} & \text{if } c + c' \in (C + C')_0 \\ 0 & \text{otherwise} \end{cases}$$

Theorem 3.6.1. *The map $\phi_{\pi,\pi'}$ is L-invariant.*

Proof. For ease of notation, let us just write ϕ for $\phi_{\pi,\pi'}$. The Λ-invariance of ϕ is clear, so it suffices to show that for any $\widetilde{\alpha} \in \widetilde{\Gamma}$, $\widetilde{c} \in \widetilde{C}$, $\widetilde{c}' \in \widetilde{C'}$, we have $[X_{\widetilde{\alpha}}, \phi(Y_{\widetilde{c}}, Y_{\widetilde{c}'})] = \phi([X_{\widetilde{\alpha}}, Y_{\widetilde{c}}], Y_{\widetilde{c}'}) + \phi(Y_{\widetilde{c}}, [X_{\widetilde{\alpha}}, Y_{\widetilde{c}'}])$. Both sides are integral multiples of $Y_{\widetilde{\alpha}\widetilde{c}\widetilde{c}'}$ which vanishes unless $\langle \alpha, \alpha + c + c'\rangle \leq 1$, or in other words $\langle \alpha, c + c'\rangle \leq -1$. Thus we may assume without loss of generality that $\langle \alpha, c\rangle = -1$ and $\langle \alpha, c'\rangle \leq 0$.

First suppose $\langle \alpha, c'\rangle = 0$. Then the last term vanishes, so we just need to prove that $[X_{\widetilde{\alpha}}, \phi(Y_{\widetilde{c}}, Y_{\widetilde{c}'})] = \phi(Y_{\widetilde{\alpha}\widetilde{c}}, Y_{\widetilde{c}'})$. If $c + c' \notin (-C - C')_0$, the left side vanishes, but so does the right side since $\alpha + c + c'$ is the result of applying the simple reflection r_α to $c + c'$ and therefore does not lie in $(-C - C')_0$. On the other hand, if $c + c' \in (-C - C')_0$, then $\alpha + c + c' \in (-C - C')_0$ by the same reasoning and both sides are equal to $Y_{\widetilde{\alpha}\widetilde{c}\widetilde{c}'}$.

Now assume $\langle \alpha, c'\rangle = -1$. Then $\langle \alpha, c + c'\rangle = -2$, so we have $c + c' \notin (-C - C')_0$ and $\phi(Y_{\widetilde{c}}, Y_{\widetilde{c}'}) = 0$. Thus we are reduced to showing $\phi(Y_{\widetilde{\alpha}\widetilde{c}}, Y_{\widetilde{c}'}) + \phi(Y_{\widetilde{c}}, Y_{\widetilde{\alpha}\widetilde{c}'}) = 0$. If $\alpha + c + c' \notin (-C - C')_0$, both terms vanish and we are done. Otherwise, the sum is equal to $Y_{\widetilde{\alpha}\widetilde{c}\,\widetilde{c}'} + Y_{\widetilde{c}\widetilde{\alpha}\widetilde{c}'}$, which vanishes since $\widetilde{c}\widetilde{\alpha} = -\widetilde{\alpha}\widetilde{c}$. ■

Example 3.6.2. Let $\pi_0 : \widetilde{\Lambda} \to \Lambda^\vee$ denote the identity of $\mathcal{C}$. We have $\Lambda_0 = \{0\}$, so M_{π_0} is a rank 1 $\mathbf{Z}$-module. It has a canonical generator corresponding to the identity element of $\widetilde{\Lambda}$. Correspondingly there are canonical isomorphisms $M_\pi \otimes M_{\pi_0} \xrightarrow{\sim} M_\pi$, $M_{\pi_0} \otimes M_\pi \xrightarrow{\sim} M_\pi$. These isomorphisms are given by the maps ϕ_{π,π_0} and $\phi_{\pi_0,\pi}$, together with the identity constrints $\pi \xrightarrow{\sim} \pi \otimes \pi_0$ and $\pi \xrightarrow{\sim} \pi_0 \otimes \pi$. Thus our construction above is compatible with the identity constraints on $\mathcal{C}$.

Example 3.6.3. There is a natural isomorphism $\pi \otimes \pi^{-1} \simeq \pi_0$; composing with $\phi_{\pi,\pi^{-1}}$, we get an L-invariant pairing

$$M_\pi \otimes M_{\pi^{-1}} \to \mathbf{Z}$$

One may easily check that this is a perfect pairing of M_π with $M_{\pi^{-1}}$.

3.7. **Commutativity.** If π and π' are objects of $\mathcal{C}$, then $\pi \otimes \pi'$ and $\pi' \otimes \pi$ have the same image in $\Lambda^\vee$, so they are isomorphic. We now show how to single out a particularly nice choice of isomorphism between them.

Given any element $v \in C$, note that that $\langle v, v \rangle \equiv t_C \pmod{2\mathbf{Z}}$. This is because $v = v_0 + \lambda$, where $\lambda \in \Lambda$ and v_0 has minimal length, so

$$\langle v, v \rangle = \langle v_0, v_0 \rangle + 2\langle \lambda, v_0 \rangle + \langle \lambda, \lambda \rangle \equiv t_C \pmod{2\mathbf{Z}}$$

Thus, for any $v \in C$, $v' \in C'$, we have $t_{C+C'} \equiv \langle v + v', v + v' \rangle \equiv t_C + t_{C'} + 2\langle v, v' \rangle \pmod{2\mathbf{Z}}$. Thus, if we set

$$t_{C,C'} = \frac{t_{C+C'} - t_C - t_{C'}}{2}$$

then $\langle v, v' \rangle - t_{C,C'}$ is always an integer.

Now let $\pi : \widetilde{C} \to \Lambda^\vee$ and $\pi' : \widetilde{C}' \to \Lambda^\vee$ be objects in $\mathcal{C}$. We define a map $\eta_{\pi,\pi'} : \widetilde{C} \otimes \widetilde{C}' \to \widetilde{C}' \otimes \widetilde{C}$ by the rule

$$\eta_{\pi,\pi'}(\widetilde{v} \otimes \widetilde{v}') = (-1)^{\langle v, v' \rangle - t_{C,C'}} \widetilde{v}' \otimes \widetilde{v}$$

One easily checks that $\eta_{\pi,\pi'}$ is a well-defined isomorphism in the category $\mathcal{C}$.

Remark 3.7.1. Although η is functorial and the compositions $\eta_{\pi,\pi'} \circ \eta_{\pi',\pi}$ naturally give the identity, the isomorphisms $\eta_{\widetilde{C},\widetilde{C'}}$ do *not* define a commutativity constraint on the category $\mathcal{C}$. This is because

$$(\eta_{\pi,\pi'} \otimes id_{\pi''})(id_\pi \otimes \eta_{\pi',\pi''}) \neq \eta_{\pi \otimes \pi',\pi''}$$

in general. Indeed, these isomorphisms are off by a sign $(-1)^{\{C,C',C''\}}$, where

$$2\{C, C', C''\} = t_{C+C'+C''} - t_{C+C'} - t_{C+C''} - t_{C'+C''} + t_C + t_{C'} + t_{C''}$$

Remark 3.7.2. Suppose C and C' are cosets of odd order. Then the composite

$$\pi_C \otimes \pi_{C'} \simeq \pi_{C+C'} \simeq \pi_{C'} \otimes \pi_C$$

differs from the isomorphism $\eta_{\pi_C,\pi_{C'}}$ by the sign $(-1)^{t_{C,C'}}$ (where the latter is well-defined since $\langle C, C' \rangle$ has odd denominator).

Remark 3.7.3. If C is n-torsion, then $\langle nC, C \rangle = \langle \Lambda, C \rangle = 0 \in \mathbf{Q}/\mathbf{Z}$. Thus $t_C \in \langle C, C \rangle \subseteq \frac{1}{n}\langle nC, C \rangle$ lies in $\frac{1}{n}\mathbf{Z}$.

Suppose C is a 2-torsion element of $\Lambda^\vee/\Lambda$, and let $v \in C$ have minimal length. If $\pi : \widetilde{C} \to \Lambda^\vee$ is an object of $\mathcal{C}$ covering the coset C and $\widetilde{v}$ is a preimage of v, then

$$\eta_{\pi,\pi}\widetilde{v} \otimes \widetilde{v} = (-1)^{\langle v, v \rangle - t_{C,C}} \widetilde{v} \otimes \widetilde{v}$$

Using the fact that $C + C = \Lambda$, we see that $t_{C,C} = -t_C$, so $\eta_{\pi,\pi} = (-1)^{2t_C}$.

We will call a 2-torsion coset C *orthogonal* if t_C is an integer, and *symplectic* otherwise. In a moment we will justify this terminology by showing that it reflects the nature of the invariant bilinear forms on the corresponding (self-dual) minuscule representation.

Let us now consider the commutativity properties of the maps $\phi_{\pi,\pi'}$.

Theorem 3.7.4. *The diagram*

$$\begin{array}{ccc} M_\pi \otimes M_{\pi'} & \simeq & M_{\pi'} \otimes M_\pi \\ \downarrow & & \downarrow \\ M_{\pi \otimes \pi'} & \overset{\eta_{\pi,\pi'}}{\simeq} & M_{\pi' \otimes \pi} \end{array}$$

commutes.

Proof. The commutativity translates directly into the condition that $\eta_{\pi,\pi'}(\widetilde{v}\widetilde{v}') = \widetilde{v}'\widetilde{v}$ when $v \in C_0$, $v' \in C'_0$, and $v + v' \in (C + C')_0$. But then

$$t_{C+C'} = \langle v + v', v + v' \rangle = \langle v, v \rangle + \langle v', v' \rangle + 2\langle v, v' \rangle = t_C + t_{C'} + 2\langle v, v' \rangle$$

so that $\langle v, v' \rangle = t_{C,C'}$ and the result follows from the definition. ∎

Now let $\pi : \widetilde{C} \to \Lambda^\vee$ be any object of $\mathcal{C}$. We have a natural multiplication

$$\phi_{\pi,\pi} : M_\pi \otimes M_\pi \to M_{\pi\otimes\pi}$$

A special case of the commutativity above shows that $\phi_{\pi,\pi}(x,y) = M_{\eta_{\pi,\pi}}\phi_{\pi,\pi}(y,x)$. Here $\eta_{\pi,\pi}$ is an automorphism of $\pi\otimes\pi$. Thus $\phi_{\pi,\pi}$ is symmetric or antisymmetric depending as $\eta_{\pi,\pi}$ is trivial or nontrivial. The triviality of $\eta_{\pi,\pi}$ can be checked on an element $\widetilde{v}\otimes\widetilde{v}$, where $v \in C_0$. We see that $\eta_{\pi\otimes\pi}(\widetilde{v}\otimes\widetilde{v}) = (-1)^{t_C - t_{C,C}}\widetilde{v}\otimes\widetilde{v}$, so the relevant sign is

$$(-1)^{2t_C - \frac{t_{2C}}{2}}$$

Example 3.7.5. If C is 2-torsion, then $\phi_{\pi,\pi}$ defines a bilinear form on M_π. Since $t_{2C} = 0$, the above calculation shows that this form is symmetric or alternating, depending on the sign $(-1)^{2t_C}$. In other words, M_π is an orthogonal representation if C is orthogonal, and a symplectic representation if C is symplectic.

3.8. **Examples.** Let us now discuss the results of these constructions in various cases. First, let us briefly outline what happens in the reducible case. If Λ is an orthogonal direct sum of smaller lattices Λ_i, we may take $\widetilde{\Lambda}$ to be a central product of the groups $\widetilde{\Lambda}_i$. The Lie algebra L may be identified with the product of the corresponding algebras L_i. There is a natural multifunctor

$$P : \prod_i \mathcal{C}_i \rightsquigarrow \mathcal{C}$$

which allows us to make a functorial identification

$$M_{P\{\pi_i\}} \simeq \bigotimes_i M_{\pi_i}$$

The multifunctor P is "linear" with respect to the tensor category structures. With respect to the product decomposition above, the maps ϕ may be computed componentwise. In other words, we can reduce everything to the case when Λ is irreducible. We now consider this case.

Example 3.8.1. Suppose $\Lambda = A_{n-1}$. Then L is $\mathfrak{sl}_n(\mathbf{Z})$, the Lie algebra of endomorphisms of $\mathbf{Z}^n$ having trace 0. There is an isomorphism of $\Lambda^\vee/\Lambda$ with $\mathbf{Z}/n\mathbf{Z}$. Fix $\pi_1 \in \mathcal{C}$ having image corresponding to $1 \in \mathbf{Z}/n\mathbf{Z}$; we may identify M_{π_1} with $\mathbf{Z}^n$, the standard representation of L. If we set $\pi_k = \pi_1^{\otimes k}$ for $0 \le k \le n$, then M_{π_k} is naturally isomorphic to $\wedge^k(M_{\pi_1})$, If $k + k' \le n$, then the natural map $M_{\pi_k} \otimes M_{\pi_{k'}} \to M_{\pi_{k+k'}}$ is just exterior multiplication. Note π_0 and π_n are isomorphic, but not canonically: the choice of isomorphism corresponds to the specification of an orientation on $\mathbf{Z}^n$. The remaining bilinear maps (corresponding to $k + k' > n$) have a similar interpretation as exterior multiplication between exterior powers of the dual of the standard representation.

Note from this example that the two natural maps $\phi_{\pi\otimes\pi',\pi''} \circ (\phi_{\pi,\pi'} \otimes 1)$ and $\phi_{\pi,\pi'\otimes\pi''} \circ (1 \otimes \phi_{\pi',\pi''})$ from $M_\pi \otimes M_{\pi'} \otimes M_{\pi''}$ to $M_{\pi\otimes\pi'\otimes\pi''}$ need not coincide. For example, take $n = 2$ and fix an isomorphism $\pi_0 \to \pi_2$ corresponding to a symplectic form $[,]$ on $M = M_{\pi_1}$; then we get two maps $M \otimes M \otimes M \to M$ which are given respectively by

$$(v \otimes u \otimes w) \mapsto [v,u]w$$

and

$$(v \otimes u \otimes w) \mapsto [u,w]v$$

Thus our maps $\phi_{\pi,\pi'}$ are not compatible with the associativity constraints on $\mathcal{C}$.

Example 3.8.2. Let $\Lambda = D_n$. Then L is the Lie algebra of $\mathrm{Spin}(2n)$. There are four cosets of Λ in $\Lambda^\vee$. The corresponding representations of L are the trivial representation, the standard representation on $\mathbf{Z}^{2n}$, and the two half-spin representations $\Delta^\pm$. The only really interesting multiplicative structures we obtain are maps

$$\mathbf{Z}^{2n} \otimes \Delta^\pm \to \Delta^\mp$$

(and "transposes" thereof). These have a natural interpretation in terms of the action of the corresponding Clifford algebra (which contains $\mathbf{Z}^{2n}$) acting on its spin representation (isomorphic to $\Delta^+ \oplus \Delta^-$).

If $\Lambda = E_8$, then L is a form of the Lie algebra E_8 over $\mathbf{Z}$. $\Lambda^\vee/\Lambda$ is trivial, so there are no nontrivial minuscule representations. The other two exceptional cases, E_6 and E_7, are more interesting and we will discuss them in §5 and §6.

3.9. **The Category $\mathcal{S}$.** For cosets of odd order, we were able to simplify things by considering objects of $\mathcal{C}$ of the form π_C. We now develop an analogous formalism to handle cosets of order 2. We define a new category $\mathcal{S}$ as follows. An object of $\mathcal{S}$ is a pair (π, e) where π is an object of $\mathcal{C}$ and $e : \pi \otimes \pi \to \pi_0$ is an isomorphism. A morphism $(\pi, e) \to (\pi', e')$ in $\mathcal{S}$ is a morphism $\phi : \pi \to \pi'$ of underlying $\mathcal{C}$-objects satisfying the compatibility condition $e = e' \circ (\phi \otimes \phi)$

Remark 3.9.1. Roughly speaking, objects of $\mathcal{S}$ parametrize *self-dual* minuscule representations of L, where we keep track of the isomorphism of the representation with its dual via the isomorphism e.

There is a natural product operation on $\mathcal{S}$:

$$(\pi, e) \otimes (\pi', e') = (\pi \otimes \pi', (e \otimes e') \circ (1 \otimes \eta_{\pi,\pi'} \otimes 1))$$

This product is functorial. It is also associative: the natural isomorphism $(\pi \otimes \pi') \otimes \pi'' \simeq \pi \otimes (\pi' \otimes \pi'')$ is compatible with any e, e', e''. To see this, note that both of the corresponding maps

$$(\pi \otimes \pi' \otimes \pi'') \otimes (\pi \otimes \pi' \otimes \pi'') \to \pi_0$$

differ from the symmetrically defined isomorphism

$$(e \otimes e' \otimes e'') \circ (1 \otimes \eta_{\pi',\pi} \circ \eta_{\pi'',\pi'} \circ 1) \circ (1 \otimes 1 \otimes \eta_{\pi'',\pi} \otimes 1 \otimes 1)$$

by the same sign $(-1)^{\{C,C',C''\}}$. Consequently the isomorphism classes of objects of $\mathcal{S}$ form a group which surjects naturally onto the group of 2-torsion elements of $\Lambda^\vee/\Lambda$. The kernel of this surjection is canonically isomorphic to $\langle \pm \mathbf{1} \rangle$.

If (π, e) is any object of $\mathcal{S}$, the map e defines a morphism of $\mathcal{C}$ objects $\pi \otimes \pi \simeq \pi_0$. This prolongs to an isomorphism of $\mathcal{S}$-objects $(\pi, e) \otimes (\pi, e) \simeq (\pi_0, e')$, where $e' : \pi_0 \otimes \pi_0 \to \pi_0$ is determined by the compatibility $e' \circ (e \otimes e) = e_0 \circ (e \otimes e) \circ (id_\pi \otimes \eta_{\pi,\pi} \otimes id_\pi)$, where $e_0 : \pi_0 \otimes \pi_0 \simeq \pi_0$ is the standard map. e' and e_0 differ by the sign of $\eta_{\pi,\pi}$. This determines the group structure on the isomorphism classes of elements of $\mathcal{S}$.

The group $\widetilde{\Lambda}_o$ provides particularly nice representatives (in $\mathcal{C}$) for cosets of odd order. Let us now attempt to handle cosets of order 2 in the same way. For any object $E = (\pi : \widetilde{C} \to \Lambda^\vee, e)$ of $\mathcal{S}$, we let $\widetilde{\Lambda}_E$ be the disjoint union $\widetilde{\Lambda}_E = \widetilde{\Lambda} \cup \widetilde{C}$. $\widetilde{\Lambda}$ is a group which operates on $\widetilde{C}$ on the right and on the left. Together with the map $e : \widetilde{C} \times \widetilde{C} \to \widetilde{\Lambda}$, we get a multiplication operation on $\widetilde{\Lambda}_E$. Clearly the identity of $\widetilde{\Lambda}$ serves as an identity element for $\widetilde{\Lambda_e}$ and multiplicative inverses exist. The associative law is more subtle. For $\widetilde{v} \in \widetilde{\Lambda}_E$, let us write

$$\deg(\widetilde{v}) = \begin{cases} 0 & \text{if } \widetilde{v} \in \widetilde{\Lambda} \\ 1 & \text{otherwise} \end{cases}$$

Theorem 3.9.2. *For $\widetilde{x}, \widetilde{y}, \widetilde{z} \in \widetilde{\Lambda}_E$, $\widetilde{x}(\widetilde{y}\widetilde{z}) = (-1)^{2t_C \deg(\widetilde{x}) \deg(\widetilde{y}) \deg(\widetilde{z})}(\widetilde{x}\widetilde{y})\widetilde{z}$*

Proof. If any of $\widetilde{x}$, $\widetilde{y}$, and $\widetilde{z}$ has degree 0 then $\widetilde{x}(\widetilde{y}\widetilde{z}) = (\widetilde{x}\widetilde{y})\widetilde{z}$, so the result is clear. The functions $\widetilde{x} \otimes \widetilde{y} \otimes \widetilde{z} \to \widetilde{x}(\widetilde{y}\widetilde{z}), (\widetilde{x}\widetilde{y})\widetilde{z}$ give two isomorphisms $\widetilde{C} \otimes \widetilde{C} \otimes \widetilde{C} \to \widetilde{C}$ which differ by a sign $\epsilon = \pm 1$. Take $\widetilde{x} = \widetilde{y} = \widetilde{z}$, where $x \in C_0$. Then $\widetilde{x}e(\widetilde{x}, \widetilde{x}) = \epsilon e(\widetilde{x}, \widetilde{x})\widetilde{x}$, so that $\epsilon = (-1)^{\langle x, 2x \rangle} = (-1)^{2t_C}$ as desired. ∎

Consequently $\widetilde{\Lambda}_E$ is a group if and only if C is orthogonal. If C is symplectic, as is the case for the nontrivial coset of the root lattice of E_7, then $\widetilde{\Lambda}_E$ satisfies a more complicated "graded-associative law".

4. The Group $\widetilde{W}$

The Weyl group of a semisimple group G is usually defined as a quotient $N(T)/T$, where T is a maximal torus of G and $N(T)$ its normalizer. For many purposes it is important to consider representatives of elements of the Weyl group inside of G. However, since the sequence

$$0 \to T \to N(T) \to W \to 0$$

does not split in general, one must first pass to some extension of W. Tits ([14]) observed that one can get by with a finite extension by working with algebraic groups over $\mathbf{Z}$ and restricting the above sequence to $\mathbf{Z}$-valued points (on which it is still exact). $T(\mathbf{Z})$ is a finite 2-torsion abelian group, so the $\mathbf{Z}$-points of $N(T)$ constitute a finite extension $\widetilde{W}$ of W which actually lies in G. In this section, we will give a combinatorial construction of this group and analyze its structure, for the case of simply-laced groups.

Remark 4.0.3. Our notation $\widetilde{W}$ violated our convention in that $\widetilde{W}$ is not a central extension of W by $\langle \pm \mathbf{1} \rangle$. We trust that no confusion will result.

4.1. **Construction of $\widetilde{W}$.** Fix a basis $\Delta \subseteq \Gamma$ of simple roots. Recall ([10], Chapter 1.9) that W may be presented by generators $\{r_\alpha\}_{\alpha \in \Delta}$ subject to the relations:

$$\begin{gathered} r_\alpha^2 = 1 \\ \langle \alpha, \beta \rangle = 0 \Longrightarrow r_\alpha r_\beta = r_\beta r_\alpha \\ \langle \alpha, \beta \rangle = -1 \Longrightarrow r_\alpha r_\beta r_\alpha = r_\beta r_\alpha r_\beta \end{gathered} \tag{4.1}$$

We will construct an extension of $\widetilde{W}$ by giving a slightly more complicated set of generators and relations. To begin with, $\widetilde{W}$ should contain the $\mathbf{Z}$-points of a torus in the associated group. For simplicity, we work with the simply-connected form; then $T(\mathbf{Z})$ is may be naturally identified with $V = \Lambda/2\Lambda$. For v in V or Λ, we will write e_v to denote the corresponding element of $\widetilde{W}$. Let $\widetilde{\Delta}$ denote the preimage of Δ in $\widetilde{\Lambda}$. We now define $\widetilde{W}$ to be the free group generated over V by formal symbols $\{n_{\widetilde{\alpha}}\}_{\widetilde{\alpha} \in \widetilde{\Delta}}$ subject to the following relations:

$$\begin{gathered} n_{-\widetilde{\alpha}} = n_{\widetilde{\alpha}}^{-1} \\ n_{\widetilde{\alpha}}^2 = e_\alpha \\ n_{\widetilde{\alpha}} e_v = e_{r_\alpha(v)} n_{\widetilde{\alpha}} \\ \langle \alpha, \beta \rangle = 0 \Longrightarrow n_{\widetilde{\alpha}} n_{\widetilde{\beta}} = n_{\widetilde{\beta}} n_{\widetilde{\alpha}} \\ \langle \alpha, \beta \rangle = -1 \Longrightarrow n_{\widetilde{\alpha}} n_{\widetilde{\beta}} n_{\widetilde{\alpha}} = n_{\widetilde{\beta}} n_{\widetilde{\alpha}} n_{\widetilde{\beta}} \end{gathered} \tag{4.2}$$

An equivalent presentation is given in [14].

Example 4.1.1. For the lattice A_1, $\widetilde{W}$ is isomorphic to $\mathbf{Z}/4\mathbf{Z}$, generated by any symbol n_α.

If we set each e_v equal to the identity, the relations (4.2) for the $n_{\widetilde{\alpha}}$ reduce to the relations (4.1) for the r_α. Hence we have an exact sequence

$$V \to \widetilde{W} \to W \to 0$$

We will soon show that this sequence may be extended by 0 on the left.

4.2. **Representations of $\widetilde{W}$.** We will now investigate the structure of the group $\widetilde{W}$. The group $\widetilde{V}$ acts on itself by conjugation; the kernel of this action contains -1 so we get an induced action of V on $\widetilde{V}$. For $\widetilde{v} \in \widetilde{V}$, $\widetilde{\alpha} \in \widetilde{\Gamma}$, set

$$n_{\widetilde{\alpha}}(\widetilde{v}) = \begin{cases} \widetilde{v} & \text{if } \langle \alpha, v \rangle = 0 \\ \widetilde{\alpha}\widetilde{v} & \text{otherwise} \end{cases}$$

One readily verifies that the relations above are satisfied, so we get an action of $\widetilde{W}$ on $\widetilde{V}$ compatible with the action of $\widetilde{W}$ on $\widetilde{V}$. There is also a natural action of $\widetilde{W}$ on Λ (via W). Moreover these two actions induce the same action on $\Lambda/2\Lambda$. Thus we obtain a natural action of $\widetilde{W}$ on

$$\widetilde{\Lambda} \simeq \Lambda \times_V \widetilde{V} = \{\lambda, \widetilde{v}) \in \Lambda \times \widetilde{V} : \lambda \equiv v \pmod 2\}$$

Representations of L also give rise to representations of $\widetilde{W}$. Let M be any representation of L on which the action of each generator $X_{\widetilde{\gamma}}$ is nilpotent. Then each $\exp(X_{\widetilde{\gamma}})$ is an automorphism of $M_{\mathbf{Q}} = M \otimes_{\mathbf{Z}} \mathbf{Q}$. Thus we may define an automorphism $n_{\widetilde{\gamma}} = \exp(X_{\widetilde{\gamma}}) \exp(-X_{\widetilde{\gamma}^{-1}}) \exp(X_{\widetilde{\gamma}})$. If M decomposes into ($\Lambda^\vee$-valued) weight spaces under the action of L, then V acts on M by the rule

$$v(x) = (-1)^{\langle v, \lambda \rangle} x$$

whenever x lies in the weight space corresponding to λ. A slightly tedious calculation shows that this induces an action of $\widetilde{W}$ on $M_{\mathbf{Q}}$.

In the special case $M = M_\pi$ of the representations constructed in the last section, the square of the action of any $X_{\widetilde{\gamma}}$ is zero; thus $\exp(X_{\widetilde{\gamma}}) = 1 + X_{\widetilde{\gamma}}$, and the automorphism $n_{\widetilde{\gamma}}$ is actually defined on M_π itself (before making a base change to $\mathbf{Q}$). This property also holds for representations of L that are obtained by taking tensor products of representations of the form M_π.

Let us compute the action of $n_{\widetilde{\alpha}}$ on M_π. If $\langle \alpha, c \rangle = 0$, then $Y_{\widetilde{c}}$ is invariant under $\exp(X_{\widetilde{\alpha}})$ and $\exp(-X_{\widetilde{\alpha}^{-1}})$. If $\langle \alpha, c \rangle = -1$, then $\exp(X_{\widetilde{\alpha}}) \exp(-X_{\widetilde{\alpha}^{-1}}) \exp(X_{\widetilde{\alpha}}) Y_{\widetilde{c}} = Y_{\widetilde{\alpha c}}$. Similarly if $\langle \alpha, c \rangle = 1$ we get $n_{\widetilde{\alpha}} Y_{\widetilde{c}} = -Y_{\widetilde{\alpha}^{-1}\widetilde{c}}$.

In particular, $n_{\widetilde{\alpha}}^2 Y_{\widetilde{c}} = (-1)^{\langle \alpha, c \rangle} Y_{\widetilde{c}}$. If we define an action of V on M_π by $e_\lambda(Y_{\widetilde{c}}) = (-1)^{\langle \lambda, c \rangle} Y_{\widetilde{c}}$, then the above calculation shows that $n_{\widetilde{\alpha}}^2 = e_\alpha$. It is clear that $n_{\widetilde{\alpha}}$ and $n_{\widetilde{\beta}}$ commute when $\langle \alpha, \beta \rangle = 0$. Moreover if $\langle \alpha, \beta \rangle = -1$, then a quick calculation shows that $n_{\widetilde{\alpha}} n_{\widetilde{\beta}} n_{\widetilde{\alpha}} = n_{\widetilde{\beta}} n_{\widetilde{\alpha}} n_{\widetilde{\beta}}$. Consequently we get an action of $\widetilde{W}$ on M_π. Note that this action permutes the generators $Y_{\widetilde{c}}$. Thus $\widetilde{W}$ acts on the set $\widetilde{C}_0$ (in a manner compatible with the action of W on C_0).

Our analysis provides the setting for the following theorem:

Theorem 4.2.1. *The group $\widetilde{W}$ acts in a natural way on the groups $\widetilde{\Lambda}$, $\widetilde{\Gamma}$, and each representation M_π. If $g, h \in \widetilde{W}$ are such that g and h induce the same automorphism of $\widetilde{\Lambda}$ and of M_π for every $\pi \in \mathcal{C}$, then $g = h$.*

Proof. Let $z = gh^{-1}$. Since W acts faithfully on Λ, the image of z in W is the identity; thus we may assume $z = e_\lambda$ for some $\lambda \in \Lambda$. We also know that z acts trivially on $\widetilde{V}$, which implies that $\langle \lambda, v \rangle$ is even for every $v \in \Lambda$. If $\lambda \notin 2\Lambda$, then there is some $v \in \Lambda^\vee$ with $\langle \lambda, v \rangle$ odd. Let C be the coset of v; then $\langle \lambda, c \rangle$ is odd for all $c \in C$. Choose $\pi : \widetilde{C} \to \Lambda^\vee$ in $\mathcal{C}$ to have image C. Then z acts on M_π by multiplication by -1, contrary to the hypothesis. ∎

The above proof also shows the following:

Corollary 4.2.2. *The natural map $V \to \widetilde{W}$ is injective.*

We now show that the group $\widetilde{W}$ is independent of the choice of simple roots Δ. Before doing this, we need to make some preliminary remarks. First, we will study the action of $\widetilde{W}$ on $\widetilde{\Lambda}$ more closely.

Lemma 4.2.3. *Let $\widetilde{\beta}$, $\widetilde{\alpha} \in \widetilde{\Gamma} \subseteq \widetilde{\Lambda}$, and let $g = n_{\widetilde{\beta}} \in \widetilde{W}$.*

$$g(\widetilde{\alpha}) = \begin{cases} -\widetilde{\beta}^2 & \text{if } \langle \alpha, \beta \rangle = -2 \\ \widetilde{\beta}\widetilde{\alpha} & \text{if } \langle \alpha, \beta \rangle = -1 \\ \widetilde{\alpha} & \text{if } \langle \alpha, \beta \rangle = 0 \\ -\widetilde{\beta}^{-1}\widetilde{\alpha} & \text{if } \langle \alpha, \beta \rangle = 1 \\ -\widetilde{\beta}^{-2}\widetilde{\alpha} & \text{if } \langle \alpha, \beta \rangle = 2 \end{cases}$$

Proof. We assume $\langle \alpha, \beta \rangle \leq 0$, the other cases being analogous. It suffices to show that both sides are have the same images in both Λ and $\widetilde{V}$. For Λ this is obvious. In $\widetilde{V}$, we have $g(\widetilde{\alpha}) = \widetilde{\alpha}$ if $\langle \alpha, \beta \rangle$ is even and

$g(\widetilde{\alpha}) = \widetilde{\beta}\widetilde{\alpha}$ otherwise. This proves the result in case $\langle \alpha, \beta \rangle$ is 0 or -1. If $\langle \alpha, \beta \rangle = -2$, then $g(\widetilde{\alpha}) = \widetilde{\alpha}$ in $\widetilde{V}$. On the other hand, $\widetilde{\alpha}$ and $-\widetilde{\beta}^2\widetilde{\alpha}$ differ by $-\widetilde{\beta}^2$ which lies in the kernel of the projection $\widetilde{\Lambda} \to \widetilde{V}$. ■

Note that $\widetilde{W}$ is generated by the symbols $n_{\widetilde{\alpha}}$, $\widetilde{\alpha} \in \widetilde{\Delta}$. Consequently every $g \in \widetilde{W}$ has some minimal expression as a product of these generators; the minimal number of generators required we will call the *length of* g.

We now investigate the action of $\widetilde{W}$ on sets of the form $\widetilde{C}_0$.

Lemma 4.2.4. *Let $\pi : \widetilde{C} \to \Lambda^\vee$ be an object of $\mathcal{C}$, $\widetilde{v} \in \widetilde{C}_0$, $\widetilde{\alpha} \in \widetilde{\Gamma}$, $g \in \widetilde{W}$. If $\langle \alpha, v \rangle = -1$ then $g(\widetilde{\alpha}\widetilde{v}) = g(\widetilde{\alpha})g(\widetilde{v})$.*

Proof. Both expressions make sense because $\langle \alpha, v \rangle = -1$ implies that $\widetilde{\alpha}\widetilde{v} \in \widetilde{C_0}$, and also the fact that W preserves lengths shows that $\langle g(\alpha), g(v) \rangle = -1$ so that also $g(\widetilde{\alpha})g(\widetilde{v}) \in \widetilde{C}_0$. Using induction on the length of g, we can easily reduce to the case where g has length 1; say $g = n_{\widetilde{\beta}}$. We will assume $\langle \beta, v \rangle \leq 0$, the other cases being analogous.

First suppose $\langle \beta, v \rangle = 0$, so $g(\widetilde{v}) = \widetilde{v}$. Since $\alpha + v \in C_0$, we see that $-1 \leq \langle \beta, \alpha \rangle \leq 1$. If $\langle \beta, \alpha \rangle = -1$, then $g(\widetilde{\alpha}\widetilde{v}) = \widetilde{\beta}\widetilde{\alpha}\widetilde{v} = g(\widetilde{\alpha})g(\widetilde{v})$ as desired. If $\langle \beta, \alpha \rangle = 0$, then $g(\widetilde{\alpha}\widetilde{v}) = \widetilde{\alpha}\widetilde{v} = g(\widetilde{\alpha})g(\widetilde{v})$. If $\langle \beta, \alpha \rangle = 1$, then $g(\widetilde{\alpha}\widetilde{v}) = -\widetilde{\beta}^{-1}\widetilde{\alpha}\widetilde{v} = g(\widetilde{\alpha})g(\widetilde{v})$.

Now suppose $\langle \beta, v \rangle = -1$. Then $g(\widetilde{v}) = \widetilde{\beta}\widetilde{v}$. We have $0 \leq \langle \beta, \alpha \rangle \leq 2$. If $\langle \beta, \alpha \rangle = 0$, then

$$g(\widetilde{\alpha}\widetilde{v}) = \widetilde{\beta}\widetilde{\alpha}\widetilde{v} = \widetilde{\alpha}\widetilde{\beta}\widetilde{v} = g(\widetilde{\alpha})g(\widetilde{v})$$

If $\langle \beta, \alpha \rangle = 1$, then

$$g(\widetilde{\alpha}\widetilde{v}) = \widetilde{\alpha}\widetilde{v} = \widetilde{\alpha}\widetilde{\beta}^{-1}\widetilde{\beta}\widetilde{v} = (-\widetilde{\beta}^{-1}\widetilde{\alpha})(\widetilde{\beta}\widetilde{v}) = g(\widetilde{\alpha})g(\widetilde{v})$$

Finally, if $\langle \beta, \alpha \rangle = 2$, then

$$g(\widetilde{\alpha}\widetilde{v}) = -\widetilde{\beta}^{-1}\widetilde{\alpha}\widetilde{v} = -\widetilde{\beta}^{-2}\widetilde{\beta}\widetilde{\alpha}\widetilde{v} = (-\widetilde{\beta}^{-2}\widetilde{\alpha})(\widetilde{\beta}\widetilde{v}) = g(\widetilde{\alpha})g(\widetilde{\beta})$$

and the proof is complete. ■

To show that the group $\widetilde{W}$ does not depend on the choice of root basis Δ, we first define elements $n_{\widetilde{\alpha}} \in \widetilde{W}$ in general. Pick any $\widetilde{\alpha} \in \widetilde{\Gamma}$, and set

$$n_{\widetilde{\alpha}} = \widetilde{w} n_{\widetilde{\beta}} \widetilde{w}^{-1}$$

where $\widetilde{w}$ is chosen so that $\widetilde{\alpha} = \widetilde{w}(\widetilde{\beta})$ and $\widetilde{\beta} \in \widetilde{\Delta}$

Lemma 4.2.5. *The above definition is independent of the choice of $\widetilde{w}$.*

Proof. It suffices to show that the equation defining $n_{\widetilde{\alpha}}$ actually holds when $\widetilde{\alpha} \in \widetilde{\Delta}$. To verify this, we need to show that both sides induce the same transformations of Λ, $\widetilde{V}$, and each M_π. In the first two cases this is easy, so we concentrate on the third.

Let $\pi : \widetilde{C} \to \Lambda^\vee$ be an object of $\mathcal{C}$, and let $\widetilde{c} \in \widetilde{C}_0$. We must show that

$$n_{\widetilde{\alpha}} \widetilde{w} Y_{\widetilde{c}} = \widetilde{w} n_{\widetilde{\beta}} Y_{\widetilde{c}}$$

If $\langle \beta, c \rangle = 0$, both sides are equal to $\widetilde{w} Y_{\widetilde{c}}$ and there is nothing to prove. We will assume that $\langle \beta, c \rangle = -1$, the other case being analogous. We must show that

$$\widetilde{w} Y_{\widetilde{c}} = Y_{\widetilde{c}'} \Rightarrow \widetilde{w} Y_{\widetilde{\beta}\widetilde{c}} = Y_{\widetilde{w}(\widetilde{\beta})\widetilde{c}'}$$

which is just a special case of Lemma 4.2.4. ■

Now if we replace Δ with any other system Δ' of simple roots, we get an alternative system of generators $n_{\widetilde{\delta}'}$ for $\widetilde{W}$; these generate $\widetilde{W}$ and are subject to the same relations since they differ from the old generators by conjugation. Moreover one easily checks that this new description of $\widetilde{W}$ is compatible with the actions of $\widetilde{W}$ on $\widetilde{\Lambda}$ and M_π described above.

Note that $n_{\widetilde{\alpha}} = n_{-\widetilde{\alpha}^{-1}}$. To see this, it suffices to check that both elements of $\widetilde{W}$ induce the same transformation on Λ, $\widetilde{V}$, and each M_π. On Λ, both induce the simple reflection corresponding to $\pm\alpha$. For $\widetilde{V}$, this follows from the fact that $\widetilde{\alpha}$ and $-\widetilde{\alpha}^{-1}$ have the same image in $\widetilde{V}$. For the M_π, this follows from our earlier calculations.

Theorem 4.2.6. *Let $\pi : \widetilde{C} \to \Lambda^\vee$ be an object of $\mathcal{C}$. There is a unique action of $\widetilde{W}$ on $\widetilde{C}$ which extends the action of $\widetilde{W}$ on $\widetilde{C}_0$ and such that the left action $\widetilde{\Lambda} \times \widetilde{C} \to \widetilde{C}$ is $\widetilde{W}$-equivariant.*

Proof. Uniqueness is obvious. Pick $\widetilde{v} \in \widetilde{C}_0$, and let $g(\widetilde{v}) = \widetilde{\gamma}_g \widetilde{v}$ for $g \in \widetilde{W}$. We define an action of $\widetilde{W}$ on the whole of $\widetilde{C}$ by the formula $g(\widetilde{\lambda}\widetilde{v}) = g(\widetilde{\lambda})\widetilde{\gamma}_g \widetilde{v}$. Clearly this definition does not change if we replace $\widetilde{v}$ by $-\widetilde{v}$. We know that W acts transitively on C_0. Thus, in order for this definition to be independent of the choice of $\widetilde{v}$, it is necessary and sufficient that $\widetilde{\gamma}_{gh} = \widetilde{\gamma}_g g(\widetilde{\gamma}_h)$. This cocycle condition is also equivalent to the fact that we have defined an action; that is, that $(gh)\widetilde{v} = g(h\widetilde{v})$.

We prove the cocycle condition is satisfied by induction on the length of h. If the length of h is zero, there is nothing to prove. If the length of h is > 1, then we may write h as a product $h'h''$ where h' and h'' have smaller length. Then, using the inductive hypothesis we get

$$\widetilde{\gamma}_{gh} = \widetilde{\gamma}_{gh'h''} = \widetilde{\gamma}_{gh'} gh'(\widetilde{\gamma}_{g''}) = \widetilde{\gamma}_g g(\widetilde{\gamma}_{h'}) gh'(\widetilde{\gamma}_{h''}) = \widetilde{\gamma}_g g(\widetilde{\gamma}_{h'} h'(\widetilde{\gamma}_{h''})) = \widetilde{\gamma}_g g(\widetilde{\gamma}_h)$$

as required.

We are thus reduced to proving the result in the case h has length 1; that is, $h = n_{\widetilde{\alpha}}$. Replacing $\widetilde{\alpha}$ with $-\widetilde{\alpha}^{-1}$ if necessary, we may assume that $\langle \alpha, v \rangle \leq 0$. If $\langle \alpha, v \rangle = 0$, then $h(\widetilde{v}) = \widetilde{v}$, so $\widetilde{\gamma}_h$ is the identity, and $\widetilde{\gamma}_{gh} = \widetilde{\gamma}_g$ as desired. Otherwise $\langle \alpha, v \rangle = -1$; then $h(\widetilde{v}) = \widetilde{\alpha}\widetilde{v}$, and we must show that $g(\widetilde{\alpha}\widetilde{v}) = g(\widetilde{\alpha})g(\widetilde{v})$. This is precisely the statement of 4.2.4. ∎

Remark 4.2.7. Let $\pi : \widetilde{C} \to \Lambda^\vee$ and $\pi' : \widetilde{C}' \to \Lambda^\vee$ be objects in $\mathcal{C}$. The group $\widetilde{W}$ acts on $\widetilde{C}$ and $\widetilde{C}'$, compatibly with its action on $\widetilde{\Lambda}$; thus we get an induced action of $\widetilde{W}$ on $\widetilde{C} \times_{\widetilde{\Lambda}} \widetilde{C}'$. In fact, this agrees with the action defined above (for the object $\pi \otimes \pi'$). This follows from the uniqueness statement and the fact that $\phi_{\pi,\pi'}$, being a map of L-modules, is $\widetilde{W}$-equivariant.

Remark 4.2.8. The group $\widetilde{W}$ acts on $\widetilde{V}$ and Λ_o in a compatible manner; thus it acts on $\widetilde{\Lambda}_o$. This action leaves $\widetilde{C}$ stable for any coset C of odd order. We claim this agrees with the action defined above on $\widetilde{C}$. In view of the uniqueness statement of the last theorem, it suffices to check the agreement on $\widetilde{C}_0$, and for generators of $\widetilde{W}$. This follows easily from our earlier calculations.

4.3. **The Structure of $\widetilde{W}$.** The Weyl group W acts orthogonally on V via some homomorphism $\psi : W \to O(V, q)$. This homomorphism is covered by the action of $\widetilde{W}$ on $\widetilde{V}$ we have defined, which gives a homomorphism $\widetilde{\psi} : \widetilde{W} \to \mathrm{Aut}\, \widetilde{V}$. Restricting $\widetilde{\psi}$ to $V \subseteq \widetilde{W}$, one gets automorphisms of $\widetilde{V}$ that are trivial on V. Recall that this group is canonically isomorphic to $V^\vee$. Thus we have a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \longrightarrow & \widetilde{W} & \longrightarrow & W & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \widetilde{\psi} & & \downarrow \psi & & \\ 0 & \longrightarrow & V^\vee & \longrightarrow & \mathrm{Aut}(\widetilde{V}) & \longrightarrow & O(V,q) & \longrightarrow & 0 \end{array} \tag{4.3}$$

Here the map $V \to V^\vee$ simply corresponds to the pairing $\langle , \rangle \pmod 2$.

Lemma 4.3.1. *If Γ is irreducible, then the kernel of ψ is either trivial or ± 1, depending on whether or not $-1 \in W$.*

Proof. Suppose $w \in W$ induces the identity on V. Then for any root α, $w(\alpha)$ is another root which is congruent to α modulo 2Λ. Since Γ is simply laced, one easily sees that $w(\alpha) = \epsilon_\alpha \alpha$ where $\epsilon_\alpha = \pm 1$. If $\langle \alpha, \beta \rangle = -1$, then $-1 = \langle w(\alpha), w(\beta) \rangle = \epsilon_\alpha \epsilon_\beta \langle \alpha, \beta \rangle = -\epsilon_\alpha \epsilon_\beta$, so $\epsilon_\alpha = \epsilon_\beta$. This implies that the function ϵ is constant on each component of the Dynkin diagram corresponding to a choice of simple roots. Since Γ is irreducible and the simple roots generate Λ, we see that $w = \pm 1$, as desired. ∎

Remark 4.3.2. We could do the same construction for lattices other than the root lattice. In particular, if we did the same construction starting with $\Lambda^\vee/2\Lambda^\vee$, we would get an extension $\widetilde{W}'$ of W by $V^\vee$, which could be identified with the **Z**-points in the normalizer of a torus in a split adjoint semisimple group over **Z**. One has a diagram analogous to 4.3 as above, but the left column is replaced by the identity isomorphism

$$V^\vee \simeq V^\vee$$

Consequently we may identify $\widetilde{W}'$ with the fiber product $\mathrm{Aut}(\widetilde{V}) \times_{O(V,q)} W$, the set of all pairs $(\alpha, w) \in \mathrm{Aut}(\widetilde{V}) \times W$ which induce the same automorphism of V.

Remark 4.3.3. Under the map ψ, the reflection r_α goes to the "reflection"

$$v \to v - \langle v, \alpha\rangle \alpha$$

The image of ψ is the subgroup of $O(V,q)$ generated by such reflections.

Remark 4.3.4. In the case of E_6, $\Lambda^\vee/\Lambda$ has order 3. Hence the natural map $V \to V^\vee$ is an isomorphism. The element -1 is not in the Weyl group so that ψ is injective. The quadratic form q is nondegenerate on V. Since the 36 pairs of roots all go over to nonisotropic vectors in V, we see that (V,q) has nontrivial Arf invariant and every non-isotropic element is the image of a root. Hence the image of ψ is group generated by all reflections: that is, all of $O(V,q)$. Thus ψ is an isomorphism. Our diagram now shows that $\widetilde{\psi}$ is an isomorphism.

For other groups, such as E_7, the situation is more complicated. Let us now investigate the diagram 4.3 more closely. There is an induced "snake homomorphism" δ from the kernel of the representation of W on V to the group $\Lambda^\vee/(\Lambda + 2\Lambda^\vee)$.

Theorem 4.3.5. *The map δ vanishes.*

Proof. Clearly it suffices to prove this in the case Γ is irreducible. If ψ is injective there is nothing to prove. Otherwise, we may assume that -1 lies in the Weyl group. Let $\widetilde{w} \in \widetilde{W}$ be a lifting of $-1 \in W$. Then $\widetilde{w}$ acts on $\widetilde{\Lambda}$ covering the map $\Lambda \stackrel{-1}{\to} \Lambda$; hence we get $\widetilde{w}(\widetilde{v}) = (-1)^{q'(v)}\widetilde{v}^{-1}$, where $q' : \Lambda \to \mathbf{Z}/2\mathbf{Z}$ is some function. Since $\widetilde{W}$ acts by automorphisms, q' is forced to satisfy the equation $q'(v+u) = q'(v) + q'(u) + \langle v, u\rangle$. Thus q' differs from q by a linear functional, so we may write $q'(v) = q(v) + \langle \lambda, v\rangle$ for some well-defined $\lambda \in V^\vee$. Since the automorphism

$$\widetilde{v} \to (-1)^{q(v)}\widetilde{v}^{-1}$$

is trivial on $\widetilde{V}$, the desired result is equivalent to the assertion that λ lies in the image of V.

Dually, this is equivalent to the assertion that the form on V defined by pairing with λ vanishes on the kernel of the natural map $V \to V^\vee$. Any element of this kernel may be represented in the form 2μ, where $\mu \in \Lambda^\vee$. Let $\pi : \widetilde{C} \to \Lambda^\vee$ be such that $\pi(\widetilde{\mu}) = \mu$. Since $2\mu \in \Lambda$, there is an isomorphism $e : \pi \otimes \pi \simeq \pi_0$. Let $E = (\pi, e)$. Working in $\widetilde{\Lambda}_E$, we have by definition

$$(\widetilde{\mu}\widetilde{\mu})(\widetilde{\mu}\widetilde{\mu})^{\widetilde{w}} = (-1)^{q'(2\mu)}$$

We have seen that the group $\widetilde{W}$ acts naturally on each torsor $\widetilde{C}$, compatible with all morphisms in $\widetilde{C}$. Hence $\widetilde{W}$ acts naturally on $\widetilde{\Lambda}_E$ compatibly with its multiplication. Thus

$$(-1)^{q'(2\mu)} = (\widetilde{\mu}\widetilde{\mu})(\widetilde{\mu}^{\widetilde{w}}\widetilde{\mu}^{\widetilde{w}}) = \widetilde{\mu}(\widetilde{\mu}(\widetilde{\mu}^{\widetilde{w}}\widetilde{\mu}^{\widetilde{w}}) = \pm\widetilde{\mu}((\widetilde{\mu}\widetilde{\mu}^{\widetilde{w}})\widetilde{\mu}^{\widetilde{w}}) = \pm(\widetilde{\mu}\widetilde{\mu}^{\widetilde{w}})^2 = \pm 1$$

where the sign depends on whether C is orthogonal or symplectic. On the other hand, $q(2\mu) = \frac{\langle 2\mu, 2\mu\rangle}{2} = 2\langle \mu, \mu\rangle$ is even or odd depending on whether or not C is orthogonal or symplectic. It follows that

$$q(2\mu) \equiv q'(2\mu) \pmod 2$$

and so $\lambda(2\mu) = 0$ as desired. ∎

Consequently we get a short exact sequence of finite abelian groups:

$$0 \to (\Lambda \cap 2\Lambda^\vee)/2\Lambda \to \ker\widetilde{\psi} \to \ker\psi \to 0$$

.

Remark 4.3.6. We may describe this extension more explicitly. Let us assume once again that $-1 \in W$, and consider a lifting of -1 to some $\widetilde{w} \in \ker \widetilde{\psi}$. Then $\widetilde{w}^2$ is the image of some class $\lambda \in V$. To determine λ, consider a finite-dimensional representation V of $L_{\mathbf{C}}$ having highest weight $\mu \in \Lambda^\vee$. Recall that $\widetilde{W}$, may be identified with a group of $\mathbf{C}$-points of the associated simply connected group, so it acts on V in a manner compatible with its action on $\Lambda^\vee$. Let Y be a weight vector for μ, so that $Y^{\widetilde{w}}$ is a weight vector for $\mu^{\widetilde{v}} = -\mu$. Since $-1 \in W$, V is self-dual via some L-invariant pairing $(,)$. Then $\langle , \rangle$ is also Weyl-invariant, so we get $(Y, Y^{\widetilde{w}}) = (Y^{\widetilde{w}}, Y^{\widetilde{w}^2}) = (Y^{\widetilde{w}}, (-1)^{\langle \lambda, \mu \rangle} Y)$. Thus $\langle \lambda, \mu \rangle = \pm 1$ depending on whether the representation V is orthogonal or symplectic.

Remark 4.3.7. Let S denote the finite abelian group of isomorphism classes of objects in $\mathcal{S}$. Our results suggest a kind of "duality" between the exact sequences

$$0 \to (\Lambda \cap 2\Lambda^\vee)/2\Lambda \to \ker \widetilde{\psi} \to \ker \psi \to 0$$

and

$$0 \to \langle \pm \mathbf{1} \rangle \to S \to (\Lambda^\vee \cap \frac{1}{2}\Lambda)/\Lambda \to 0$$

4.4. **Invariant Tensors.** Let $\pi^i : \widetilde{C^i} \to \Lambda^\vee$ be objects of $\mathcal{C}$ for $1 \leq i \leq k$, and write M_i for M_{π^i}. An element of $M = M_1 \otimes \cdots \otimes M_k$ has the form

$$x = \sum_{c_i \in (C_i)_0} m_{\widetilde{c_1}, \ldots, \widetilde{c_k}} Y_{\widetilde{c_1}} \otimes \cdots \otimes Y_{\widetilde{c_k}}$$

where the coefficients satisfy the relation

$$m_{\widetilde{c_1}, \ldots, \widetilde{c_{i-1}}, -\widetilde{c_i}, \widetilde{c_{i+1}}, \ldots, \widetilde{c_k}} = -m_{\widetilde{c_1}, \ldots, \widetilde{c_{i-1}}, \widetilde{c_i}, \widetilde{c_{i+1}}, \ldots, \widetilde{c_k}}$$

so each term in the sum is independent of the representatives $\{\widetilde{c_i}\}$ chosen to represent the $\{c_i\}$. We have the same description of elements of M_R for any commutative ring R: one only needs to allow the coefficients to take values in R.

If x is invariant under the action of the whole of L, then it is invariant under the action of $\widetilde{W}$. This in turn is equivalent to $m_{\widetilde{c_1}, \ldots, \widetilde{c_k}} = m_{\widetilde{w}\widetilde{c_1}, \ldots, \widetilde{w}\widetilde{c_k}}$ for all $\widetilde{w} \in W$.

If $k = 3$, more information is available:

Lemma 4.4.1. *Suppose that $k = 3$ and that $x \in M_R$ is L_R-invariant. The coefficient $m_{\widetilde{c}_1, \widetilde{c}_2, \widetilde{c}_3}$ vanishes unless $c_1 + c_2 + c_3 = 0$.*

Proof. Over $\mathbf{Z}$, this follows from the Λ-invariance of x. However, we want to give a proof that is valid over an arbitrary commutative ring.

To show that $c_1 + c_2 + c_3 = 0$, it suffices to show that $\langle \alpha, c_1 + c_2 + c_3 \rangle = 0$ for every $\alpha \in \Gamma$. Replacing α by $-\alpha$ if necessary, we may assume $k = \langle \alpha, c_1 + c_2 + c_3 \rangle \leq 0$. If $k = 0$ we are done. If $k = -1$, then $\alpha \in \Lambda$ does not annihilate x, a contradiction.

Suppose $k < -1$. Then $\langle \alpha, c_i \rangle \leq 0$ for each i. Without loss of generality, $\langle \alpha, c_1 \rangle = -1$. Then the coefficient of $Y_{\widetilde{\alpha}\widetilde{c_1}} \otimes Y_{\widetilde{c}_2} \otimes Y_{\widetilde{c}_3}$ in $X_{\widetilde{\alpha}} x$ is $m_{\widetilde{c}_1, \widetilde{c}_2, \widetilde{c}_3}$. The L-invariance of x then implies that this coefficient vanishes. ∎

Using this, we can easily prove the following:

Theorem 4.4.2. *Let $k = 3$. Then $(M_R)^{L_R}$ is a free R-module of rank 1 if $C_1 + C_2 + C_3 = 0 \in \Lambda^\vee/\Lambda$, and vanishes otherwise.*

Proof. The vanishing follows from the lemma we just proved. For the second claim, fix a triple $\widetilde{c}_1, \widetilde{c}_2, \widetilde{c}_3$ such that $c_1 + c_2 + c_3 = 0$. This induces a map

$$\psi : (M_R)^{L_R} \to R$$
$$x \mapsto m_{\widetilde{c}_1, \widetilde{c}_2, \widetilde{c}_3}$$

Since W acts transitively on the collection of triples $\{(a_1, a_2, a_3) \in C_0^1 \times C_0^2 \times C_0^3 : a_1 + a_2 + a_3 = 0\}$, the $\widetilde{W}$-invariance of $x \in (M_R)^{L_R}$ shows that all nonzero coefficients of x are determined by $m_{\widetilde{c}_1, \widetilde{c}_2, \widetilde{c}_3}$. This

proves that ψ is injective. For the surjectivity, we choose an isomorphism $\pi^1 \otimes \pi^2 \simeq (\pi^3)^{-1}$. The "transpose" of the multiplication map ϕ_{π^1,π^2} gives rise to an element x of $(M_R)^{L_R}$ with $\psi(x) = \pm 1$. ■

Corollary 4.4.3. *Let π be an object of $\mathcal{C}$, $M = M_\pi$. Then all L_R-endomorphisms of M_R are given by scalar multiplication by elements of R.*

Proof. Apply Theorem 4.4.2 to π, π^{-1}, and π_0. ■

Using this, we can finally prove our claim concerning the automorphism group of the representations M_π.

Corollary 4.4.4. *Let π be an object of $\mathcal{C}$, $M = M_\pi$. Every L_R-automorphism of M_R is given by scalar multiplication by a unit in R. In particular, every automorphism of M is given by multiplication by ± 1.*

Remark 4.4.5. These results do not generalize in a simple way to invariant tensors of degree $k > 3$. We will see this when we examine E_7 in the case $k = 4$.

5. The Lie Algebra E_6

Let C be a 3-torsion element of $\Lambda^\vee/\Lambda$, and let $\pi : \widetilde{C} \to \Lambda^\vee$ have image C. Let η be a generator for the rank 1 $\mathbf{Z}$-module $(M_\pi \otimes M_\pi \otimes M_\pi)^L$. We can choose an isomorphism $\pi \otimes \pi \simeq \pi^{-1}$ so that η corresponds to the map $\phi_{\pi,\pi}$. This map is symmetric or skew-symmetric depending on the sign $(-1)^{2t_C - \frac{t_{2C}}{2}}$; since $t_{2C} = t_{-C} = t_C$, we see that η is symmetric in the first two factors if $3t_C \equiv 0 \pmod 4$ and antisymmetric otherwise. Exactly the same reasoning applies to symmetry when other factors are exchanged. Thus η is either completely symmetric or completely antisymmetric.

This applies in particular if C is a generator of $\Lambda^\vee/\Lambda$ when $\Lambda = E_6$, which we will assume for the remainder of this section. We have seen that $t_C = \frac{4}{3}$, so that η is completely symmetric. Thus we see that the minuscule representation M_π is a rank 27 $\mathbf{Z}$-module equipped with with a symmetric trilinear form η. This section is devoted to the study of η.

Remark 5.0.6. To avoid cumbersome notation, we will actually study the invariant cubic *polynomial* on M_π, rather than the invariant form. The polynomial lives in $\mathbb{S}^3 M_\pi$, while the invariant form lives in $\mathbb{S}^3(M_\pi{}^\vee)$. Up to replacing π by π^{-1}, there is no difference.

5.1. **The Weyl Group of E_6.** Before diving in to the study of E_6, we collect here a few facts concerning its Weyl group. The computations necessary to justify the numerical assertions which follow are elementary, so we leave them to the reader.

We saw earlier that the Weyl group W of E_6 is isomorphic to the orthogonal group of the nondegenerate 6-dimensional $\mathbf{F}_2$ quadratic space, which has Arf invariant 1. This group has order $2^7 3^4 5$. Theorem 2.5.1 shows that V admits an Hermitian structure which induces its quadratic form. The automorphisms of V which preserve this Hermitian structure form a subgroup of W isomorphic to the unitary group $U_3(2)$, which has order $2^3 3^4$. Its center has order 3, and it is isomorphic to the centralizer of its center in W (a fact which underlies what follows).

Another subgroup of W will be relevant in what follows. Since V has Arf invariant 1, a maximal isotropic subspace $U \subseteq V$ is 2-dimensional. The stabilizer of such a subspace is a maximal parabolic subgroup P of W, and has index 45 in W. In P there is a unique nontrivial transformation which is the identity when restricted to $U^\perp$; this is a central involution $\sigma \in P$, and P is the centralizer of σ in W. By Witt's extension theorem, W acts transitively on the isotropic planes contained in V. Thus there are precisely 45 such planes.

For more details we refer the reader to [5].

5.2. **The Invariant Cubic.** Since Λ has index 3 in $\Lambda^\vee$, we have $\Lambda_o = \Lambda^\vee$. Note that if $v_0, v_1, v_2 \in C_0$ are such that $v_0 + v_1 + v_2 = 0$, then $\langle v_i + v_j, v_i + v_j \rangle = \langle v_k, v_k \rangle = t_C$, so we cannot have $v_i = v_j$. It follows that as σ ranges over the symmetric group S_3, all 6 terms $\pm Y_{\widetilde{v_{\sigma(0)}}} \otimes Y_{\widetilde{v_{\sigma(1)}}} \otimes Y_{\widetilde{v_{\sigma(2)}}}$ are distinct. Consequently, the symmetric tensor η is the polarization of an integral cubic polynomial $\Theta(z) \in \mathbb{S}^3 M_\pi$. More explicitly, we may write this cubic as a sum

$$\Theta(z) = \sum_{\{w,w',w''\} \subseteq C_0, w+w'+w''=0} (\widetilde{w}\widetilde{w}'\widetilde{w}'') Y_{\widetilde{w}} Y_{\widetilde{w}'} Y_{\widetilde{w}''}$$

Remark 5.2.1. Returning for the moment to the situation of general Λ, suppose C is a coset of odd order in $\Lambda^\vee/\Lambda$. If $v, v' \in C_0$ have the same reduction modulo $2\Lambda_o$ (recall that Λ_o is the union of all cosets $\in \Lambda^\vee/\Lambda$ having odd order), then $v - v' \in \Lambda \cap 2\Lambda_o = 2\Lambda$. Then $\frac{v+v'}{2} \in C$, contradicting the minimality of $\langle v, v\rangle = \langle v', v'\rangle$. Thus the reduction map $C_0 \to \Lambda_o/2\Lambda_o \simeq \Lambda/2\Lambda$ is *injective*.

This remark applies in particular to the case of E_6: the triples $\{w, w', w''\}$ appearing in the above sum are determined by their reductions $\{\overline{w}, \overline{w}', \overline{w}''\}$ in V. Any such triple consists of the nonzero elements in some plane of V. Since $t_C = \frac{4}{3}$ is divisible by 4, q vanishes identically on such a plane. Moreover, the Weyl group acts on the set of triples $\{w, w', w''\}$ which sum to zero compatible with its action on the isotropic 2-planes of V. Since $W \to O(V, q)$ is surjective in this case, Witt's extension theorem implies that W acts transitively on the isotropic planes. Thus there are precisely 45 terms in the expression for the Θ, which correspond bijectively to the 45 isotropic planes in V.

In order to get a more explicit formula for Θ, we need to choose a set of generators for its weight spaces. In order to do this, we need to introduce some additional data. Note that V is a 6-dimensional quadratic space over $\mathbf{F}_2$ with Arf invariant 1, so it admits a compatible Hermitian structure by Theorem 2.5.1. Fix an element $\overline{\omega} \in \mathrm{Aut}(\widetilde{V})$ of order 3 with only central fixed points. This determines a Hermitian form h on V characterized by the property that $\mathrm{Tr}(h(v, v')) = \langle v, v'\rangle$. Using the identification of $\widetilde{V}$ with the group $\overline{V}$ provided by Theorem 2.5.1, we get canonical liftings $\overline{v}_{\overline{\omega}} \in \widetilde{V}$ for each $v \in V$. If $\overline{\omega}$ is clear from context we will simply write $\overline{v}$ instead of $\overline{v}_{\overline{\omega}}$.

Now we have a canonical basis for M_π, given by $\{Y_{\overline{v}}\}_{v \in C_0}$. Given a triple $\{v, v', v''\}$ of nonzero elements in an isotropic plane, we can ask: in the invariant cubic, what is the sign on the term $Y_{\overline{v}} Y_{\overline{v}'} Y_{\overline{v}''}$? This is easily computed: we know the sign to be given by

$$\overline{v}\,\overline{v}'\overline{v}'' = (-1)^{\mathrm{Tr}(\omega h(v,v') + \omega h(v,v'') + \omega h(v',v''))}$$

Using the fact that $v'' = v + v'$ and that $h(v, v) = q(v) = 0$, we see that the sign is given by $(-1)^{\mathrm{Tr}(\omega h(v',v''))}$.

Since $v' + v'' = v$ is isotropic, we have $0 = \langle v', v''\rangle = \mathrm{Tr}(h(v', v''))$ so that $h(v', v'') \in \mathbf{F}_2$. If $h(v', v'') = 0$, then since $h(v', v') = q(v') = 0 = q(v'') = h(v'', v'')$, h must vanish on the entire $\mathbf{F}_4$-vector space generated by v' and v''. Since V is nondegenerate, this vector space can be at most 1-dimensional and we see that v' and v'' are linearly dependent. Conversely, if v' and v'' are linearly dependent, than $h(v', v'')$ is a multiple of $h(v', v') = q(v') = 0$. Therefore the sign $\overline{v}\,\overline{v}'\overline{v}''$ is 1 if $\{w, w', w''\}$ span an $\mathbf{F}_4$-line in V, and -1 otherwise.

There are 27 nonzero isotropic vectors in V and the multiplicative group $\mathbf{F}_4^\times$ acts freely on them. The 9 orbits correspond bijectively to 9 terms in the invariant cubic with coefficient 1, while the other 36 terms have coefficient -1 (assuming the form to be written in terms of the canonical basis obtained from $\overline{\omega}$). Note that although the basis $Y_{\overline{v}}$ depends on the choice of $\overline{\omega}$, the signs in the cubic form depend only on the induced $\mathbf{F}_4$-structure on V. They are even unchanged if the $\mathbf{F}_4$-structure is altered by an automorphism of $\mathbf{F}_4$. (For example, we could replace $\overline{\omega}$ with $\overline{\omega}^2$; this has the effect of replacing $\overline{v}$ with $(-1)^{q(v)}\overline{v}$, and in particular leaves every generator $Y_{\overline{v}}$ for M_π unchanged.) Thus, we have proven the following:

Theorem 5.2.2.

$$\Theta(z) = \sum_{p = \{0, v, v', v''\} \subseteq V} Y_{\overline{v}} Y_{\overline{v}'} Y_{\overline{v}''} - \sum_{q = \{0, v, v', v''\} \subseteq V} Y_{\overline{v}} Y_{\overline{v}'} Y_{\overline{v}''}$$

where p ranges over the 9 isotropic planes in V which are $\mathbf{F}_4$-invariant and q ranges over the remaining 36 isotropic planes which are not.

5.3. **Combinatorics of the Signs.** The goal of this section is to prove that our explicit description of the cubic invariant under E_6, as given in the last section, is "optimal" in some sense. We continue to assume Γ is the root system of E_6, and $C \in \Lambda^\vee/\Lambda$ is nontrivial. We will frequently identify C_0 with its image in V.

Let us introduce some terminology. Let X denote the set of all isotropic 2-dimensional subspaces of V. If $x, y \in X$, we call x and y *adjacent* if $x \cap y$ is nontrivial. Note that for $x \in X$, any isotropic vector orthogonal to all of x must lie in x, since otherwise the 3-dimensional subspace spanned by that vector and x would be totally isotropic, contradicting the fact that $\Lambda/2\Lambda$ has Arf invariant 1. Consequently, if $x, y \in X$ are not adjacent then the restriction of $\langle , \rangle$ to $x \times y$ is nondegenerate, so $(x \oplus y, q|(x \oplus y))$ is a nondegenerate

quadratic space of Arf invariant 0. q cuts out a split quadric surface in $\mathbf{P}(x \oplus y)$, which has two rulings by lines. $\mathbf{P}(x)$ and $\mathbf{P}(y)$ are lines of the quadric which do not meet, hence they belong to the same ruling, together with some other line $\mathbf{P}(z)$. In this situation we will say that x, y and z are *collinear*. The quadric surface has another ruling by lines, corresponding to another collinear triple x', y', z', which we will refer to as the *conjugate triple* to $\{x, y, z\}$. The following easy fact will be needed in the next section:

Theorem 5.3.1. *W acts transitively on the collinear (noncollinear) triples of nonadjacent elements of X.*

Proof. In both cases this is a consequence of Witt's extension theorem. ■

A *basis* is a choice $\overline{v} \in \widetilde{C_0}$ of preimage for each $v \in \widetilde{C_0}$. Every basis B determines a map $s_B : X \to \{\pm 1\}$, given by $\{v, v', v''\} \to \overline{v}\,\overline{v}'\overline{v}''$. A *signing* is an element of $\{\pm 1\}^X$ which arises in this way. If s is a signing, we let $X_s = \{x \in X : s(x) = 1\}$, and $|s| = |X_s|$.

A *marking* is an element $g \in \mathrm{Aut}(\widetilde{V})$ of order 3 with only central fixed points. We saw in the last section that every marking determines a basis B with $|s_B| = 9$. If g is a marking then g^2 is also a marking, which we will refer to as the *conjugate marking*; we have seen that conjugate markings determine the same basis.

Every basis B (in this combinatorial sense) gives a $\mathbf{Z}$-basis for M_C, with respect to which we may write the invariant cubic as

$$\sum_{x=\{0,v,v',v''\}\in X} s_B(x) Y_{\overline{v}} Y_{\overline{v}'} Y_{\overline{v}''}$$

Thus, $|s|$ is the number of terms in the corresponding expression for Θ in which the coefficient 1 appears.

There are 2^{27} possible choices of basis, and some will be better than others. One might ask if it is possible to choose a basis B such that s_B is constant; that is, all the signs in the invariant cubic are the same. This is in fact impossible: there does not exist a basis B such that $|s_B| = 0$. This naturally leads us to ask: what is the minimal value of $|s_B|$, and for what "optimal bases" is this value achieved? This question is answered by the following result:

Theorem 5.3.2. *For any basis B, we have $|s_B| \geq 9$, and equality holds if and only if B is the basis associated to some marking.*

The proof of this result will occupy the rest of this section. Our first objective is to determine the basic relationships between the various objects we are considering.

Note that the group $V^\vee$ acts freely on the collection of all basis: if B is a basis, then set $\lambda B = \{(-1)^{\lambda(v)}\overline{v} : \overline{v} \in B\}$. $V^\vee$ also acts freely on the collection of markings via right multiplication inside $\mathrm{Aut}(\widetilde{V})$. If g is a marking with associated basis B, then the basis associated to $g\lambda$ is the set

$$B_{g\lambda} = \{\widetilde{v} \in \widetilde{C_0} : \widetilde{v}^{(g\lambda)}\widetilde{v}^{(g\lambda)^2}\widetilde{v} = 0 \in \widetilde{V}\}$$

But

$$\widetilde{v}^{(g\lambda)}\widetilde{v}^{(g\lambda)^2}\widetilde{v} = (-1)^{\lambda(v)+\lambda(v)+\lambda(g(v))}\widetilde{v}^{g}\widetilde{v}^{g^2}\widetilde{v}$$

Thus $B_{g\lambda} = g(\lambda)B_g$.

Theorem 5.3.3.
- *There are* 5120 *markings.*
- *Two markings determine the same basis if and only if they are conjugate.*
- *There are 2^{27} bases. Two bases determine the same signing if and only if they differ by the action of $V^\vee$. Thus there are 2^{21} signings.*

Proof. We begin with the third claim. For any pair of bases $B = \{\overline{v}\}$ and $B' = \{\hat{v}\}$, we can define a function $\lambda : C_0 \to \pm 1$ by the rule $\lambda(v) = \overline{v}\hat{v}$. Our goal is to show that λ extends to a linear functional on V if and only if $s_B = s_{B'}$. One direction is obvious; for the other, note that $s_B = s_{B'}$ translates into the statement that $\lambda(v + v') = \lambda(v) + \lambda(v')$ whenever $\langle v, v'\rangle = 0$.

Let $x \in V$. If $x = 0$, set $f(x) = 0$; if $x \neq 0$ but $q(x) = 0$ set $f(x) = \lambda(x)$. Finally, if $q(x) = 1$, then choose y such that $\langle y, x\rangle = 1$ and $q(y) = 0$ (there are 12 such choices for y), and set $f(x) = \lambda(y) + \lambda(x + y)$. We first show that f is well-defined. For this, we must show that if $q(x) = 1$ and y, y' are chosen with $\langle y, x\rangle = \langle y', x\rangle = 1$, $q(y) = q(y') = 0$, then $\lambda(y) + \lambda(x + y) = \lambda(y') + \lambda(x + y')$. If $y = y' + x$ this is

obvious. Replacing y' by $x+y'$ if necessary, we may assume $\langle y, y' \rangle = 1$. We may rewrite the desired equality as $\lambda(y) + \lambda(x+y') = \lambda(y') + \lambda(x+y)$, which follows since both sides are equal to $\lambda(x+y+y')$ by our assumption on λ.

Now we must show that f is linear. Note that the relation $f(x+y) = f(x)+f(y)$ is symmetric in x, y, and $z = f(x+y)$. If any of x, y, and z is zero, the result is obvious, so assume otherwise. If $q(x) = q(y) = q(z) = 0$ the result follows from our assumption on λ. If $q(x) = q(y) = 0$, $q(z) = 1$, the result follows from the definition of $f(z)$. So now assume $q(x) = q(y) = 1$. We can choose w with $\langle x, w \rangle = \langle y, w \rangle = 1$, $q(w) = 0$ (there are 4 such choices for w). Then

$$f(x) + f(y) = \lambda(w) + \lambda(x+w) + \lambda(w) + \lambda(y+w) = f(x+w) + f(y+w) = f(z)$$

by the case just handled.

Now we verify the second statement. Suppose two markings g and g' determine the same basis. Then they determine the same signing s. Pick $v \in C_0$; the results of the last section show that for $v \in x$, $s(x) = 1$ if and only if $x = \{v, g(v), g^2(v)\}$. The same is true of g' so we get $g'(v) \in \{g(v), g^2(v)\}$. Replacing g' by its conjugate if necessary, we may assume $g(v) = g'(v)$. Now we claim that g and g' induce the same $\mathbf{F}_4$-structure on V. Note that $K = \{w : \langle v, w \rangle = 1, q(w) = 0\}$, together with v, spans V, so it suffices to check equality for $w \in K$. The above argument shows that either $g(w) = g'(w)$ or $g^2(w) = g'(w)$. But $\langle v, w \rangle = 1$ implies $\langle g(v), g(w) \rangle = 1$, which is impossible in the latter case.

Thus g and g' induce the same action on V, so $g' = g\lambda$ for some $\lambda \in V^\vee$. Our earlier analysis now applies to show that $B_g = B_{g'} = g(\lambda) B_g$, which gives $\lambda = 0$ and $g = g'$.

For the first statement, note that $V^\vee$ acts freely on the set of markings, and its orbits correspond to all possible $\mathbf{F}_4$-structures on V compatible with q. The number of such orbits is equal to the index of $U(V,h)$ in $O(V,q)$, which is $\frac{2^7 3^4 5}{2^3 3^4} = 80$. ∎

If g is a marking, let us write s_g for s_{B_g}. We will call such signings *special*. The proposition above shows that there are 40 special signings. Note that if s is special, corresponding to some $\mathbf{F}_4$-structure on V, then X_s consists of all isotropic $\mathbf{F}_4$-lines in V. No two distinct $\mathbf{F}_4$-lines meet nontrivially, so the elements of X_s are pairwise nonadjacent. Consequently, for $x, y \in X_s$, there is a unique $z \in X$ such that x, y, and z are collinear. In fact, this z also lies in X_s. The situation is summarized by the following proposition.

Theorem 5.3.4. *If s is special, $x, y \in X_s$, then there is a unique $z \in X_s$ with collinear to x and y. This notion of "collinear" endows X_s with the structure of a two-dimensional affine space over $\mathbf{F}_3$. There are 12 collinear triples $\{x, y, z\}$ in X_s, and $X - X_s$ is a disjoint union of the 12 conjugate triples $\{x', y', z'\}$.*

Proof. We will postpone a proof of the assertions regarding the structure of X_s until the next section. Granting these for the moment, let us prove the last claim. Since we know $X - X_s$ has 36 elements, it suffices to show that given distinct collinear $\{x_0, y_0, z_0\}, \{x_1, y_1, z_1\} \subseteq X_s$, the conjugate triples $\{x_0', y_0', z_0'\}$ and $\{x_1', y_1', z_1'\}$ are disjoint. If not, then without loss of generality $x_0' = x_1'$, and x_0' meets x_0, y_0, z_0, x_1, y_1, and z_1 nontrivially. Since $p, q \in X_s$ meet nontrivially if and only if they coincide and $x_0' - \{0\}$ has 3 elements, the set $\{x_0, y_0, z_0, x_1, y_1, z_1\}$ can contain at most 3 elements, thus $\{x_0, y_0, z_0\} = \{x_1, y_1, z_1\}$, contrary to our assumption. ∎

Lemma 5.3.5. *Let s be a special signing, s' any signing. Suppose $X_s \cap X_{s'} = \emptyset$ ($X_s \cap X_{s'} = \{x\}$)). Then $X_{s'}$ has at least 12 elements ($X_{s'}$ contains at least 8 elements not adjacent to x).*

Proof. Consider V to be endowed with the $\mathbf{F}_4$-structure corresponding to s. We can choose bases B and B' so that $s = s_B$, $s' = s_{B'}$; then there is some function $\epsilon : C_0 \to \pm 1$ such that $\widetilde{v} \in B$ if and only if $\epsilon(v)\widetilde{v} \in B'$.

For each $y \in X_s$ ($X_s - \{x\}$), $y \notin X_{s'}$. Thus the set of $\{v \in y - \{0\} : \epsilon(v) = -1\}$ is odd. Note that $\mathbf{F}_4^\times$ acts freely on the 36 elements of $X - X_s$. Let $\{z, \omega z, \omega^2 z\}$ denote an orbit. Then $z \cup \omega z \cup \omega^2 z$ consists of 0 together with three isotropic F_4-lines. Each of these isotropic lines contains an odd number of v with $\epsilon(v) = -1$ (if z is not adjacent to x). So $z \cup \omega z \cup \omega^2 z$ contains an odd number of nonzero v with $\epsilon(v) = -1$. Consequently, we see that one of $\{z, \omega z, \omega^2 z\}$ contains an odd number of nonzero v with $\epsilon(v) = -1$. Say z does, then $s'(z) = -s(z) = 1$.

We have shown that every $\mathbf{F}_4^\times$-orbit on $X - X_s$ (whose members are adjacent to x) meets $X_{s'}$. An easy count shows that there are 12 (8) such orbits, and the proposition follows. ■

We may now prove a weak version of our main result.

Lemma 5.3.6. *Suppose s is a signing with $|s| \leq 9$. Then $|s| = 9$.*

Proof. There are 40 special signings s', each of which assumes the value 1 on $\frac{1}{5}$ of the elements of X. By homogeneity, for each $x \in X$, there are 8 special signings that are positive on x. Thus there are at most 72 pairs (x, s') where $s(x) = s'(x) = 1$ and s' is special. By the Pigeonhole Principle, there is a special signing s' for which $X_{s'} \cap X_s$ has size at most 1. If $X_s \cap X_{s'}$ is empty, then $|s| \geq 12$, a contradiction. Otherwise, there is some $x \in X_s \cap X_{s'}$ and X_s contains at least 8 other elements not adjacent to x. Thus $|s| \geq 9$ and we are done. ■

We must now show that if $|s| = 9$, s is special. Our basic strategy is to find special signings s' which approximate s, in the sense that $X_s \cap X_{s'}$ may be made large. So we need to obtain some tools for measuring the size of $X_s \cap X_{s'}$.

Lemma 5.3.7. *Let s be an arbitrary signing and s' special. Then*

$$|s| \equiv |X_s \cap X_{s'}| + k \pmod 2$$

where k is the number of lines in the affine space $X_{s'}$ meeting X_s is an odd number of points.

Proof. Each element of X_s either lies in $X_{s'}$ or lies in a triple $\{x', y', z'\}$ conjugate to a line $\{x, y, z\}$ of $X_{s'}$. Since there are an even number of lines, it suffices to show that for every such triple $\{x, y, z\}$,

$$|X_s \cap \{x, y, z\}| + 1 \equiv |X_s \cap \{x', y', z'\}| \pmod 2$$

or in other words, $s(x)s(y)s(z) = -s(x')s(y')s(z')$. Let $s = s_B$, $s' = s_{B'}$, and let $\epsilon : C_0 \to \pm 1$ be such that $\widetilde{v} \in B$ if and only if $\epsilon(v)\widetilde{v} \in B'$. Then

$$s(w) = s'(w) \prod_{v \in w - \{0\}} \epsilon(v)$$

Since the nonzero elements of $x \cup y \cup z$ and the nonzero elements of $x \cup y \cup z$, it suffices to verify that $s'(x)s'(y)s'(z) = -s'(x')s'(y')s'(z')$, which is obvious. ■

Corollary 5.3.8. *Let s be a signing with $|s| = 9$, and let s' be a special signing. Then $|X_s \cap X_{s'}|$ cannot be equal to 2 or 4. If $|X_s \cap X_{s'}| = 3$ then $|X_s \cap X_{s'}|$ is a line of $X_{s'}$.*

Proof. Let $K = X_s \cap X_{s'}$. Then the lemma implies that $9 \equiv |K| + k \pmod 2$, where k is the number of lines in $X_{s'}$ meeting K in an odd number of points. But k is readily computed directly: if $|K| = 2$, then $k = 6$. If $|K| = 4$ then $k = 8$ if K contains a line of $X_{s'}$ and $k = 6$ otherwise. If $|K| = 3$ and K is not a line, then $k = 3$. In each case we get a contradiction. ■

Lemma 5.3.9. *Let s be a signing, s' a special signing. Then $|s| \geq |X_s \cap X_{s'}| + k$, where k is the number of of lines in $X_{s'}$ meeting X_s exactly twice.*

Proof. It suffices to show that for each line $\{x, y, z\} \subseteq X_{s'}$ meeting X_s exactly twice, the conjugate line $\{x', y', z'\}$ meets $X_{s'}$. Assume $x, y \in X_s$. Write $s = s_B$, $s' = s_{B'}$, and let $\epsilon : C_0 \to \pm 1$ be such that $\widetilde{v} \in B$ if and only if $\epsilon(v)\widetilde{v} \in B'$. Then on $x - \{0\}$ and $y - \{0\}$, ϵ assumes the value -1 an even number of times, while on $z - \{0\}$ it assumes the value -1 an odd number of times. Consequently ϵ assumes the value -1 an odd number of times on $(x \cup y \cup z) - \{0\} = (x' \cup y' \cup z') - \{0\}$. Without loss of generality, ϵ assumes the value -1 an odd number of times on $x' - \{0\}$. Then $s(x') = -s'(x') = 1$, so $x' \in X_s$ as desired. ■

Corollary 5.3.10. *Let s be a signing with $|s| = 9$, and let s' be a special signing. Then $|X_s \cap X_{s'}|$ cannot be $5, 6, 7,$ or 8.*

Proof. Let $K = X_s \cap X_{s'}$. The lemma shows that $9 \geq |K| + k$, where k is the number of lines of $X_{s'}$ meeting K exactly twice.

If $|K| = 8$, then any of the four lines through the unique element of $X_{s'} - K$ meets K exatly twice. Thus $9 \geq 8 + 4$, a contradiction.

If $|K| = 7$, any line meeting $X_{s'} - K$ meets K exactly twice except for the line joining the two points of $X_{s'} - K$. Thus $9 \geq 7 + 6$, a contradiction.

Suppose $|K| = 6$. If $X_{s'} - K$ is a line, then $k = 8$ is the number of lines not parallel to this line, so $9 \geq 6 + 8$. If $X_{s'} - K$ is not a line, then a line meets K exactly twice if and only if it meets $X_{s'} - K$ exactly once, so $k = 6$ and $9 \geq 6 + 6$.

Finally, suppose $|K| = 5$. If $X_{s'} - K$ contains a line, then $k = 7$ and $9 \geq 5 + 7$. If $X_{s'} - K$ does not contain a line, we need to work a little harder. Let K be the union of the lines $\{x, y, z\}$ and $\{x, y', z'\}$. The last lemma shows that X_s meets the lines conjugate to $\overline{yy'}$, $\overline{yz'}$, $\overline{zy'}$ and $\overline{zz'}$. Consequently, we see that each of $\{y, z, y', z'\}$ is adjacent to two other points of X_s, and each point of $X_s - X_{s'}$ is adjacent to two points in $\{y, z, y', z'\}$. Thus x is the only point in X_s which is not adjacent to another point of X_s. Consequently, for any special s'' such that $|X_s \cap X_{s''}| = 1$, we get $X_s \cap X_{s''} = \{x\}$. Suppose there are n such special signings s''. For any other special signing, $|X_s \cap X_{s''}| \geq 3$. Counting the number of pairs $\{(w, s'') : w \in X_{s''}\}$ in two different ways, we get $72 \geq n + 3(40 - n)$, so that $n \geq 24$. On the other hand, there are exactly 8 special signings s'' with $x \in X_{s''}$, so that $n \leq 8$, a contradiction. ∎

Lemma 5.3.11. *Let s be a signing, s' a special signing, and suppose $|X_s \cap X_{s'}|$ is a line in $X_{s'}$. Then there is another special signing s'' with $|X_s \cap X_{s''}| > 3$.*

Proof. Let $\{x, y, z\} \subseteq X_{s'}$ be a line parallel to $X_s \cap X_{s'}$. Write $s = s_B$, $s' = s_{B'}$, and let $\widetilde{v} \in B$ if and only if $\epsilon(v)\widetilde{v} \in B'$. Then since $\{x, y, z\}$ does not meet X_s, ϵ assumes the value -1 an odd number of times on $x - \{0\}$, $y - \{0\}$, and $z - \{0\}$, hence on $(x \cup y \cup z) - \{0\}$. If $\{x', y', z'\}$ is the conjugate line, then without loss of generality, ϵ assumes the value -1 an odd number of times on x', so that $s(x') = -s'(x') = 1$. It suffices to show that we can choose s'' special so that $X_s \cap X_{s'} \subseteq X_{s''}$ and $x' \in X_{s''}$.

Consider V to be endowed with an $\mathbf{F}_4$-structure corresponding to s'. The line $X_{s'} \cap X_s$ corresponds to an $\mathbf{F}_4$-subspace $M \subseteq V$ on which q is nondegenerate. Correspondingly we may decompose $V = M \oplus M^\perp$ as $\mathbf{F}_4$-Hermitian spaces. We may define a new $\mathbf{F}_4$-structure on V which is the same on M, but conjugated by the nontrivial automorphism of $\mathbf{F}_4$ on $M^\perp$. This gives rise to new special signing s''. Since the $\mathbf{F}_4$-structures agree on M, we get $X_s \cap X_{s'} \subseteq X_{s''}$. To complete the proof, we show that $x' \in X_{s''}$.

By construction, x' is not adjacent to any element of $X_s \cap X_{s'}$. Thus x' meets M trivially, so it projects isomorphically to $M^\perp$. Thus we may identify x' with $\{m + g(m) : m \in M^\perp\}$, where $g : M^\perp \to M$ is some $\mathbf{F}_2$-linear map. q is isotropic on x'; thus

$$0 = q(m + g(m)) = q(m) + q(g(m)) + \langle m, g(m) \rangle = q(m) + q(g(m))$$

so that g is an isometry. Thus $g(M^\perp)$ is a 2-dimensional subspace of M on which g has Arf invariant 1. There are precisely two such subspaces, and these are permuted by $\mathbf{F}_4^\times$; since this group has odd order, it permutes them trivially, so $g(M^\perp)$ is an $\mathbf{F}_4$-line in M.

Given $\mathbf{F}_4$-structures on M and $M^\perp$, the condition that x' be an $\mathbf{F}_4$-subspace of V is that g be $\mathbf{F}_4$-linear. An $\mathbf{F}_2$-isomorphism of two one-dimensional $\mathbf{F}_4$-vector spaces is either linear or antilinear. Since we know $x' \notin X_{s'}$, g is not linear with respect to the original $\mathbf{F}_4$-structure on $M^\perp$. Thus it is linear with respect to the twisted structure and we get $x' \in X_{s''}$ as desired. ∎

We can now give the proof of Theorem 5.3.2:

Proof. We have seen that $|s| = 9$. Choose s' special so that $n = |X_s \cap X_{s'}|$ is as large as possible. If $n \leq 1$, then $X_s \cap X_{s'} \leq 1$ always, so that

$$72 = \{(x, s') : x \in X_s \cap X_{s'}\} = \sum_{s'} |X_s \cap X_{s'}| \leq 40$$

Thus $n > 1$. On the other hand, Corollary 5.3.8, Lemma 5.3.10 and Corollary 5.3.11 imply that $n \neq 2, 3, 4, 5, 6, 7, 8$. Thus $n = 9$, and $X_s = X_{s'}$, so $s = s'$ is special. ∎

Remark 5.3.12. There are other ways to understand our optimal expression for the cubic form. For example, one may identify the group E_6 with the set of automorphisms of

$$\mathrm{Hom}(V_0, V_1) \oplus \mathrm{Hom}(V_1, V_2) \oplus \mathrm{Hom}(V_2, V_0)$$

preserving the cubic form

$$(\phi, \phi', \phi'') \to \det(\phi) + \det(\phi') + \det(\phi'') + \mathrm{Tr}(\phi'' \circ \phi' \circ \phi)$$

Here the V_i are taken to be free modules of rank 3 equipped with specified generators of the $\wedge^3(V_i)$ (so that the determinants are well defined). See [1] for details. One sees immediately that with respect to a choice of basis of the V_i, the cubic form is expressed as a sum of 45 monomials with 36 plus signs and 9 minus signs. Thus, (the negative of) this expression of the cubic is associated to some marking $g \in \widetilde{W} \subseteq E_6$. Choose bases $\{v_i, v_i', v_i''\}$ for the V_i so that the associated volume form on each V_i is given by $v_i \wedge v_i' \wedge v_i''$, and consider the maps g_i defined by the condition that $g_i(v_i) = v_i'$, $g_i(v_i') = v_i''$, $g_i(v_i'') = v_i$. Together these maps induce a transformation of

$$\mathrm{Hom}(V_0, V_1) \oplus \mathrm{Hom}(V_1, V_2) \oplus \mathrm{Hom}(V_2, V_0)$$

which is the required marking.

It is not difficult to check that the centralizer of a marking $g \in E_6$ is a subgroup of the form $H = (\mathrm{SL}_3 \times \mathrm{SL}_3 \times \mathrm{SL}_3)/\mu_3$, where μ_3 is a central subgroup embedded diagonally. Under the action of the group H, a nontrivial minuscule representation of E_6 decomposes as above:

$$V \simeq \mathrm{Hom}(V_0, V_1) \oplus \mathrm{Hom}(V_1, V_2) \oplus \mathrm{Hom}(V_2, V_0)$$

Of course, g is not a marking with respect to a maximal torus of H, since g is central in H.

5.4. **Cubic Surfaces.** Let S be a smooth cubic surface (over the complex numbers). For general background on such surfaces, we refer the reader to [8].

Recall that we may identify Λ with the primitive cohomology of S (that is, the collection of all classes $x \in \mathrm{H}^2(S, \mathbf{Z})$ having zero intersection with $-K_X$) and $\Lambda^\vee$ with the quotient of $\mathrm{H}^2(S, \mathbf{Z})/\mathbf{Z}c_1(K_S)$. Via this identification, the elements of C_0 are precisely the images of the funademental classes of the 27 lines on S.

Three vectors sum to zero in $\Lambda^\vee$ if and only if their sum in $\mathrm{H}^2(S, \mathbf{Z})$ is a multiple of the hyperplane class. Since a line has degree 1, we see that three weights of M_π sum to zero if and only if the three corresponding lines constitute a hyperplane section of S. In other words, we may identify X (the collection of isotropic planes in V) with the collection of tritangent planes to S. Note that two such planes correspond to adjacent elements of X if and only if their line of intersection is contained in X.

The following fact will be needed later:

Lemma 5.4.1. *Let Q denote the abelian group generated by symbols $\{g_L\}$, where L ranges over the lines on Z, subject to the relations:*

$$g_L + g_{L'} + g_{L''} = 0 \text{ if } L \cup L' \cup L'' \text{ is a hyperplane section of } Z$$

The natural map $\phi : Q \to \Lambda^\vee$ is an isomorphism.

Proof. It is easy to see that ϕ is surjective. Realize S as $\mathbf{P}^2$ blown up at 6 points $\{p_i\}$. For each index i, the exceptional divisor E_i over p_i is a line on Z, as is the proper transform C_i of a conic passing through the remaining 5 points. The other lines on Z are the proper transforms L_{ij} of lines joining p_i and p_j. Let Q_0 denote the subgroup of Q generated by the g_{E_i}. Then $\Lambda^\vee/\phi(Q_0)$ is isomorphic to $\mathbf{Z}/3\mathbf{Z}$. Thus $\phi(Q_0)$ has rank 6; and $\phi|Q_0$ is an isomorphism onto its image. Thus, to prove ϕ is injective, it suffices to show that Q/Q_0 has size ≤ 3. Let g_L' denote the image of g_L in Q/Q_0.

Since E_i, L_{ij}, and C_j are coplanar, we see that $g'_{L_{ij}} + g'_{C_j} = 0$. Applying this twice, we see that $g'_{L_{ij}} = g'_{L_{kj}}$ for any i, j, k. Applying this twice, we see that $g'_{L_{ij}}$ does not depend on i or j; let us denote this element of G/G_0 by g_L'. From $g'_{L_{ij}} + g'_{C_j} = 0$, we see that $g'_{C_j} = -g'_L$, so g'_L generates G/G_0. If a, b, c, d, e, f are all distinct, then L_{ab}, L_{cd}, and L_{ef} are coplanar. It follows that $0 = g'_{L_{ab}} + g'_{L_{cd}} + g'_{L_{ef}} = 3g'_L$, so that Q/Q_0 has size at most 3 as required. ∎

For nonzero isotropic $x \in V$, we let l_x denote the corresponding line of S. Then l_x meets l_y if and only if $\langle x, y \rangle = 0$, in which case x and y generate an element of X corresponding to the tritangent hyperplane spanned by l_x and l_y. Hence each line of S meets precisely 10 of the other 26 lines. Moreover, since V has no totally isotropic 3-dimensional subspaces, given any $p \in X$ and any nonzero isotropic x not contained in p, $x \notin p^{\perp}$ so that the form $y \to \langle x, x \rangle$ vanishes on precisely one nonzero element of p. Thus given a tritangent plane to S meeting S in $l \cup l' \cup l''$, each of the other 24 lines meets exactly one of l, l', and l''.

Of particular interest to us are *Eckardt planes*: tritangent planes meeting S in three concurrent lines. The point of concurrency of these lines is called an *Eckardt point* of S. Suppose p and p' are Eckardt points of S. The corresponding elements of X are adjacent exactly when the line $\overline{pp'}$ is contained in S. In this case we shall say that p and p' are *adjacent*.

Lemma 5.4.2. *Suppose p and p' are non-adjacent Eckardt points of S, corresponding to $x, x' \in X$. Then $\overline{pp'}$ meets S in a third point p'' which is also an Eckardt point of S. If $x'' \in X$ is the corresponding element, then x, x', x'' are collinear (in our combinatorial sense).*

Proof. One easily shows that p'' is distinct from p and p'. Let P and P' be the tangent planes to S at p and p'. Then P meets S in three lines l_0, l_1, and l_2, P' in lines l'_0, l'_1, and l'_2. Rearranging the indices if necessary, we may assume l_i and l'_i meet for all i. Then l_i and l'_i span a tritangent hyperplane Q_i, containing a third line l''_i of S. Since Q_i contains both p and p', it contains the line $\overline{pp'}$ and hence also p''. If p'' was a point of l_i, then $l_i \subseteq S$ would be forced to coincide with $\overline{pp''} = \overline{pp'}$, contrary to the assumption that p and p' are non-adjacent. Similarly p'' is not a point of l'_i, so p'' must belong to l''_i. It follows that l''_0, l''_1, l''_2 all meet at p'', so that p'' is a third Eckardt point of S. Furthermore, the lines $\{l_0, l_1, l_2, l'_0, l'_1, l'_2, l''_0, l''_1, l''_2\}$ may be identified with the 9 points on a quadric surface over $\mathbf{F}_2$ (the zero locus of q on the projectivization of the four-dimensional $\mathbf{F}_2$-space spanned by x and x'), which is ruled by lines corresponding to p, p', and p'' so that x, x', and x'' are collinear. ∎

We would now like to obtain an explicit formula for the invariant cubic form in terms of the combinatorics of the 27 lines on a cubic surface. However, this is impossible without specifying some additional data, since the signs are not uniquely determined until we choose a basis for M_π. What we need is some geometric analogue of our notion of a marking. This should take the form of additional data on S, which permit us to distinguish 9 of the tritangent hyperplanes from the other 36. Recall that a marking determines an element of the Weyl group W of order 3 which does not fix any element of $\Lambda^{\vee}$. In view of this, the following is a natural definition:

Definition 5.4.3. A *signing* of a smooth cubic surface S is an action of the group $G = \mu_3$ of $3rd$ roots of unity on S, such all G-invariant elements of $\mathrm{H}^2(S, \mathbf{Z})$ are multiples of the hyperplane class $c_1(K_S^{\vee})$.

A general cubic surface does not carry a signing (in a moment we shall obtain a characterization of exactly which cubic surfaces do admit signings). However, we shall soon see that signed cubics exist, which is all that we shall need.

Note that a marking of S determines an $\mathbf{F}_4$-structure on V. This admits a lifting to a marking $g \in \mathrm{Aut}(\widetilde{V})$, which determines a special signing s_g. Moreover s_g depends only on the marking of S and not on the further choice of g. Thus, we are motivated to study signed cubic surfaces.

Let S be a signed cubic surface, and let $V = \mathrm{H}^0(S, K_S^{\vee})$. There exists a representation of G on the canonical bundle K_S so that $S \hookrightarrow \mathbf{P}(V^{\vee})$ is G-equivariant (for example, the representation induced by the action of G on V). Let χ denote the identity character of $G = \mu_3$. We have a decomposition $V = V_0 \oplus V_1 \oplus V_2$ into isotypics for the characters χ^0, χ^1, and χ^2. Let d_i denote the dimension of V_i. Twisting the representation of G on K_S by a character and applying an automorphism of G if necessary, we may assume without loss of generality that $d_0 \geq d_1 \geq d_2$.

Theorem 5.4.4. *$d_0 = 3$, $d_1 = 1$, and $d_2 = 0$, and the cubic defining S is contained in the χ^0-isotypic of $\mathbb{S}^3(V)$.*

Proof. Let $x \in \mathrm{H}^2(S, \mathbf{Z})$ be the class of a line contained in S, $g \in G$ a generator of G. Then $x + x^g + x^{g^2}$ is G-invariant, hence a multiple of the hyperplane class. From this we see that every G-orbit of lines on S

is a plane section of S. Since such a plane section is spanned by the three lines in which it meets S, it is necessarily stable under G. Thus the 9 orbits of G on the 27 lines give us 9 planes in $\mathbf{P}^3$ stable under G, corresponding to 9 distinct G-stable 1-dimensional subspaces of V. Such a subspace must be contained in an isotypic V_i. If $d_i \leq 2$, the linear functions in V_i vanish on a line $l_i \subseteq \mathbf{P}(V^\vee)$, hence any such tritangent must contain the three points of intersection of l_i with S. Since any point of S is contained in at most three lines of S, V_i can contain the linear forms cutting out at most 3 tritangent planes. If $d_j \leq 1$, then V_j contains only one line. Hence $d_0 = d_1 = 2$, $d_2 = 0$ and $d_0 = 2$, $d_1 = d_2 = 1$ are ruled out by numerical considerations. If $d_0 = 4$, then G acts trivially on S and we do not have a signing. This proves the first claim.

For the second, note that the other isotypics of V are of the form $V_1 \otimes \mathbb{S}^2(V_0)$ and $V_1 \otimes V_1 \otimes V_0$; hence any cubic in these spaces is reducible. Since S is smooth, its defining equation must lie in $\mathbb{S}^3(V)_0$. ■

We have the decomposition $\mathbb{S}^3(V)_0 = \mathbb{S}^3(V_0) \oplus \mathbb{S}^3(V_1)$, so the defining equation of S has the form

$$f(x, y, z) + w^3 = 0$$

In other words, S is a cyclic 3-fold cover of the plane branched over the cubic curve Δ cut out by f, and G is the Galois group for the covering.

Let us proceed under the assumption that S is a such a cover of $\mathbf{P}^2$, branched over a *smooth* cubic curve Δ. In this case, it is easy enough to identify the 27 lines on S. If l is a flex line of Δ, then $S_l = S \times_{\mathbf{P}^2} l$ is a cyclic three-fold cover of l totally branched over a point; in other words, S_l (a hyperplane section of S) consists of three lines meeting in a point. Thus, the 27 lines break into 9 orbits under the action of G, and each orbit is may be considered as a 3-fold cover of one of the 9 flex lines to C. We see that for any $x \in \mathrm{H}^2(S, \mathbf{Z})$ which is the class of a line, $x + g(x) + g^2(x)$ is the hyperplane class. (Here g is a generator of the Galois group G of S over $\mathbf{P}^2$.) It follows that $1 + g + g^2$ annihilates the primitive cohomology of S, so that the action of G on S is a signing of S. In other words, we have establishes that the signed cubics are none other than the cyclic cubics: cubic surfaces that may be expressed as cyclic 3-fold covers of the plane branched over a smooth plane cubic. For our purposes the important consequence is that *signed cubic surfaces exist.*

Now, if S is a cyclic cubic, we may identify $\Delta \subseteq \mathbf{P}^2$ with a particular hyperplane section of S. The above analysis shows that each of the 9 flex points of Δ is an Eckardt point of S. If s is the signing determined by the signing of S, then X_s consists of those $x \in X$ for which the corresponding plane meets S in a G-orbit of lines; these are precisely the tritangent planes lying over the 9 flex lines to Δ. In other words, we may identify X_s with the 9 flex points of the plane cubic Δ. Since we have established that "geometric" and "combinatorial" collinearity have the same meaning, this proves that our combinatorial notion of collinearity provides X_s with the structure of a two-dimensional affine space over $\mathbf{F}_3$. This proves Theorem 5.3.4, as promised.

We can now give a formula for the invariant cubic in terms of the geometry of S as follows:

Theorem 5.4.5. *Let S be a cyclic 3-fold cover of $\mathbf{P}^2$ branched over a smooth cubic curve Δ. Introduce a variable Y_l for each of the 27 lines of S, and for each tritangent plane P let*

$$Y_P = \prod_{l \subseteq P} Y_l$$

Then the cubic invariant under E_6 may be written in the form

$$\Theta = \sum_p Y_{P_p} - \sum_P Y_P$$

where the first sum is taken over all flex points $p \in C$ (with P_p the corresponding Eckardt plane) and the second sum over the remaining 36 tritangent planes.

We will close this section with a few amusing remarks related to signed cubic surfaces; these remarks will not be needed later, so they may be safely omitted if the reader desires. Let us examine the automorphism group of a signed cubic S. Automorphisms of S commuting with the action of G will act on $\mathbf{P}^2 = S/G$, necessarily preserving the branch locus C. Conversely, any automorphism of $\mathbf{P}^2$ preserving C can be extended

to an automorphism of S in three different ways. The automorphism group H of the general plane cubic has order 18; it is a semi-direct product of $\mathbf{Z}/2\mathbf{Z}$ acting by inversion on the group H_0 of 3-torsion points of the associated elliptic curve. Thus we see that any cyclic cubic has carries an action of a group $\widetilde{H}$, where $\widetilde{H}$ is a central extension of H by G.

For any flex point $p \in C$, there is a unique element of H of order two which stabilizes p. Let σ_p denote a preimage of this element in H. Then σ_p permutes the three lines of S which meet at p; since σ_p commutes with the action of G, it must permute the three lines in an alternating fashion. Altering the choice of σ_p by an element of G, we may arrange that σ_p fixes the three lines. Then σ_p^2 is the identity on a plane and stabilizes three lines not contained in that plane, so it must act trivially on $\mathbf{P}^3$ and hence on S.

Consequently, $\widetilde{H}$ is a semidirect product of $\mathbf{Z}/2\mathbf{Z}$ with $\widetilde{H}_0$, the preimage of H_0 in $\widetilde{H}$. This last group is a Heisenberg extension corresponding to the Weil pairing on H_0. From this description, we see that the projection $\widetilde{H} \to H$ admits a section over a subgroup $H' \subseteq H$ if and only if $H_0 \not\subseteq H'$. In particular, if p, p', and p'' are distinct flex points of C, then the subgroup of $\widetilde{H}$ generated by σ_p, $\sigma_{p'}$ and $\sigma_{p''}$ is isomorphic to S^3 (its image in H) if p, p', and p'' are collinear, and all of $\widetilde{H}$ otherwise.

In fact, the existence of the involution σ_p does not require that S be a cyclic cubic, but only the existence of an Eckardt point p on S. Let us return to the situation of a general cubic surface S, defined by a homogeneous cubic $f(w, x, y, z) = 0$ and having an Eckardt point $p = (1 : 0 : 0 : 0)$. Let us assume the corresponding Eckardt plane is given by $x = 0$. Then $f(w, 0, y, z)$ is a product of three linear factors, each of which vanishes where $y = z = 0$. Thus f has the form

$$cx^3 + l(w, y, z)x^2 + q(w, y, z)x + g(y, z)$$

Since S is nonsingular at $(1 : 0 : 0 : 0)$, we must have $q(1, 0, 0) \neq 0$. Replacing w by an appropriate linear combination of w, y, and z, we may assume that $q(w, y, z) = w^2 + q'(y, z)$ for some q'. Finally, by adding a multiple of x to w, we may arrange that

$$f(x, y, z, w) = c'x^3 + l'(y, z)x^2 + (w^2 + q'(y, z))x + g(y, z)$$

Note that this equation is invariant under the involution σ_p of $\mathbf{P}^3$ carrying (w, x, y, z) to $(-w, x, y, z)$. This involution fixes p and the plane defined by $w = 0$, which meets S in a smooth cubic C since a singular point of C would also be a singular point of S.

Note that any line or plane containing p is fixed setwise, but not pointwise, by σ_p. In particular, σ_p stabilizes the three lines which meet at p, and every tritangent plane that contains one of these lines. Note that any line stable under σ_p has two fixed points under σ_p; thus it is either contained in the plane $w = 0$ or meets p. Since the plane section of S cut out by $w = 0$ is smooth, *any line of S stable under σ_p passes through p.* On the other hand, a line l of S not passing through p lies in a unique tritangent plane meeting S in $l \cup l' \cup l''$, where l'' meets p. Then we must have $\sigma_p(l) = l'$, $\sigma_p(l') = l$. In particular, the action of σ_p on the 27 lines is *determined by incidence relations among the lines.* We leave it to the reader to verify that this involution σ_p agrees with the involution defined above in the case S is cyclic.

Now we would like to study the relationships between the involutions σ_p as p varies over the Eckardt points of S. The following fact is basic to what follows:

Lemma 5.4.6. *An automorphism σ of a smooth cubic S which fixes all 27 lines setwise must be the identity.*

Proof. Since S is anticanonically embedded in $\mathbf{P}^3$, σ extends to an automorphism of $\mathbf{P}^3$. σ must fix all points of intersection of lines of S which meet. But among such pairwise intersections there are 5 points, no four of which are coplanar. Thus σ is trivial on $\mathbf{P}^3$, hence on S. ■

Now suppose p, p', p'' are collinear, non-adjacent Eckardt points. Since σ_p stabilizes the line joining p, p', and p'', and has only two fixed points on this line, we see that σ_p must permute $\{p', p''\}$ nontrivially. The same reasoning applies to the involutions $\sigma_{p'}$, $\sigma_{p''}$. Thus we get a surjective homomorphism ϕ from the subgroup of $\mathrm{Aut}(S)$ generated by the involutions σ_p, $\sigma_{p'}$, $\sigma_{p''}$ to the symmetric group S_3.

Theorem 5.4.7. *ϕ is an isomorphism.*

Proof. Since automorphisms of S are determined by their action on the 27 lines, the behavior of the involutions σ_p, $\sigma_{p'}$, and $\sigma_{p''}$ are determined by incidence relations among the 27 lines, and the Weyl group W acts transitively on collinear triples of elements of X, it suffices to verify this in the case where S is a cyclic cover of P^2 branched over a smooth conic C, and p, p', p'' are collinear flex points of C. But this follows from our analysis of the group $\widetilde{H}$ given earlier. ■

Now suppose that p, q, and r are Eckardt points which are nonadjacent but not collinear. The argument above (this time using the fact that W acts transitively on noncollinear, pairwise nonadjacent triples of elements of X) applies again to show that the group generated by σ_p, σ_q, and σ_r does not depend on the cubic S. If S is a cyclic cover of $\mathbf{P}^2$ branched over C and p, q, and r are nonadjacent flex points of C, then this group is the group $\widetilde{H}$ defined above. In particular, this group has a central subgroup G whose action gives a signing of S. Thus we have proven:

Theorem 5.4.8. *Suppose S is a smooth cubic surface with three nonadjacent, noncollinear Eckardt points p, q, and r. Then the plane spanned by p, q and r meets S in a smooth cubic curve C, and S is isomorphic to a cyclic 3-fold cover of that plane branched over C.*

In other words, the classes of signed cubics, cyclic cubics, and cubics with three noncollinear pairwise nonadjacent Eckardt points coincide. (One could be more precise. For example, a signing of a cubic is equivalent to an identification of that cubic with a three-fold cover of $\mathbf{P}^2$ and of μ_3 with its Galois group.)

5.5. **Defining E_6.** Over the complex numbers, one can define the Lie algebra E_6 as the collection of endomorphisms of a 27-dimensional complex vector space which leave annihilate a cubic polynomial on that vector space. We now show that this description of E_6 is valid over an arbitray commutative ring. Aside from its intrinsic interest, this proof will serve as a nice "warm-up" for the next section, where we will investigate the more difficult problem of defining E_7.

In the following, we let $M = M_\pi$ be a nontrivial minuscule representation of L, and we write $M_R = (M_\pi)_R = (M_\pi) \otimes_{\mathbf{Z}} R$ for any commutative ring R. Let Θ be the invariant cubic polynomial on M constructed earlier.

Theorem 5.5.1. *Let R be a commutative ring. Then L_R is the Lie algebra of all endomorphisms of M_R which annihilate Θ.*

Proof. Let L' be the Lie algebra of all endomorphisms of M_R which annihilate Θ. Note that M_R has a natural $\Lambda^\vee$ grading; it decomposes into weight spaces $M_\lambda = RY_{\widetilde{\lambda}}$. This induces a $\Lambda^\vee$ grading of $\mathrm{End}_R(M_R)$. Since Θ is homogeneous of degree 0, L' is a graded submodule of $\mathrm{End}_R(M_R)$. Thus L' decomposes into weight spaces L'_α ($\alpha \in \Lambda^\vee$). By construction we have

$$L'_\alpha M_\lambda \subseteq M_{\lambda+\alpha}$$

We need only show that each weight space L'_α is contained in L_R. Choose $x \in L'_\alpha$. If $x = 0$ there is nothing to prove. Otherwise, we may assume that x induces a nontrivial map $M_\lambda \to M_{\alpha+\lambda}$ for some $\lambda \in C_0$. Note that this implies $\alpha \in \Lambda$. There are several cases to consider, depending on the value of $\langle \lambda, \alpha + \lambda \rangle \equiv \frac{4}{3} \pmod{\mathbf{Z}}$:

- $\langle \lambda, \alpha+\lambda \rangle = \frac{4}{3}$. Then $\lambda = \alpha+\lambda$, so $\alpha = 0$. Thus x leaves each weight space M_μ stable. Suppose x acts on M_μ by the scalar $f(\mu)$. From the invariance of Θ, we see that $f(\alpha) + f(\beta) + f(\gamma) = 0$ whenever $\alpha, \beta, \gamma \in C_0$ are weights which sum to zero. By Lemma 5.4.1, f is induced by a homomorphism $\Lambda^\vee \to R$, or equivalently an element of Λ_R, which proves $x \in \Lambda_R \subseteq L_R$.
- $\langle \lambda, \alpha + \lambda \rangle = \frac{1}{3}$. Then $\langle \alpha, \alpha \rangle = \langle \alpha + \lambda, \alpha + \lambda \rangle - 2\langle \alpha, \lambda \rangle - \langle \lambda, \lambda \rangle = 2$, so $\alpha \in \Gamma$. Choose $\widetilde{\alpha} \in \widetilde{\Gamma}$ over α, $\widetilde{\lambda} \in \widetilde{C_0}$ over λ. It is clear that x annihilates $Y_{\widetilde{\mu}}$ unless $\mu + \alpha \in C_0$ (that is, unless $\langle \alpha, \mu \rangle = -1$). If $\mu + \alpha \in C_0$, we have $xY_{\widetilde{\mu}} = c_\mu Y_{\widetilde{\alpha}\widetilde{\mu}}$ for some scalars $c_\mu \in C_0$. If $\langle \mu, \lambda \rangle = \frac{-2}{3}$, then there is some $\nu \in C_0$ with $\mu + \nu + \lambda = 0$; this implies $\langle \alpha, \nu \rangle = 2$ which is impossible. Thus for $\mu \neq \lambda$, we must have $\langle \mu, \lambda \rangle = \frac{1}{3}$, so that $\gamma = -\mu + -\lambda - \alpha$ lies in C_0. Examining the coefficient of $Y_{\widetilde{\alpha}\widetilde{\mu}} Y_{\widetilde{\alpha}\widetilde{\lambda}} Y_{\widetilde{\gamma}}$ in $x(\Theta)$, we deduce that $c_\mu = c_\lambda$. Thus $x = c_\lambda X_{\widetilde{\alpha}} \in L_R$ and we are done.

- $\langle \lambda, \alpha + \lambda \rangle = \frac{-2}{3}$. Then $\langle \alpha, \alpha \rangle = 4$, $\langle \lambda, \alpha \rangle = -2$. Then $\lambda = -\frac{\alpha}{2} + \lambda'$, where $\langle \lambda', \alpha \rangle = 0$. If $\mu \in C_0$ is also such that $\mu + \alpha \in C_0$, then we may apply the same reasoning to write $\mu = -\frac{\alpha}{2} + \mu'$. Then $\langle \lambda, \mu \rangle = \langle -\frac{\alpha}{2}, -\frac{\alpha}{2} \rangle + \langle \lambda', \mu' \rangle$. Since $\langle \lambda', \lambda' \rangle = \langle \mu', \mu' \rangle = \frac{1}{3}$, we must have $\langle \lambda', \mu' \rangle \geq -\frac{1}{3}$. Thus $\langle \lambda, \mu \rangle \geq \frac{2}{3}$. Since $\langle \lambda, \mu \rangle \equiv \frac{4}{3} \pmod{\mathbf{Z}}$, we get $\langle \lambda, \mu \rangle = \frac{4}{3}$, and so $\lambda = \mu$.

  Now choose $\mu, \nu \in C_0 - \{\lambda\}$ such that $\lambda + \mu + \nu = 0$. The coefficient of $Y_{\widetilde{\alpha}\widetilde{\lambda}} Y_{\widetilde{\mu}} Y_{\widetilde{\nu}}$ in $x(\Theta)$ is $\pm c$, where $x(Y_{\widetilde{\lambda}}) = c Y_{\widetilde{\alpha}\widetilde{\lambda}}$. The invariance of Θ shows that $c = 0$, which contradicts the choice of λ.

■

6. The Lie Algebra E_7

In this section, we will discuss the case in which Λ is the root lattice of E_7. Then Λ has index 2 in $\Lambda^\vee$, so it has one nontrivial coset C. Fix $E = (\pi, e) \in \mathcal{S}$ with $\pi : \widetilde{C} \to \Lambda^\vee$ having image C. We have $t_C = 3/2$, so that the corresponding representation M_π is self-dual and symplectic.

It is well-known that the representation M_π of dimension 56 has an invariant quartic form. We would like to write this form down in some nice way, analogous to what we have already done for E_6. This is more difficult for a number of reasons:

- The map $\widetilde{\psi} : \widetilde{W} \to \mathrm{Aut}(\widetilde{V})$ is no longer an isomorphism. Indeed, ψ is a surjection with kernel $-1 \in W$, and $\widetilde{\psi}|V$ has kernel and cokernel isomorphic to $\mathbf{Z}/2\mathbf{Z}$. The snake sequence breaks into short exact pieces $0 \to \mathbf{Z}/2\mathbf{Z} \to \ker \widetilde{\psi} \to \mathbf{Z}/2\mathbf{Z} \to 0$ and $0 \to \mathbf{Z}/2\mathbf{Z} \to \mathrm{coker}\, \widetilde{\psi} \to 0$. Since V_π is symplectic, our earlier calculations show that the first of these sequences is not split. Since the image of $\widetilde{\psi}$ has index 2 in $\mathrm{Aut}(\widetilde{V})$, it is a normal subgroup. On the other hand, this group has a unique subgroup $\mathrm{Aut}_0(\widetilde{V})$ of index 2, consisting of automorphisms which act trivially on the center of $\widetilde{V}$. Thus we get a short exact sequence $0 \to \mathbf{Z}/4\mathbf{Z} \to \widetilde{W} \to \mathrm{Aut}_0(\widetilde{V}) \to 0$, a rather more complicated situation.
- Our formalism for constructing trilinear forms on minuscule representations can no longer be applied, and there seems to be no simple analogue for tensor products of four or more representations.
- Since the coset C has even order, we no longer have a nice representative π_C in $\mathcal{C}$ or the group $\widetilde{\Lambda}_o$ at our disposal. We instead work with an arbitrary π covering C together with an isomorphism $e : \pi \otimes \pi \simeq \pi_0$, and the corresponding covering $\widetilde{\Lambda}_E$ of $\Lambda^\vee$ defined in §3.9.
- For E_6, the Weyl group W acts transitively not only on the weights of the fundamental representation, but on 45 triples of weights that sum to zero. The analogous statement for E_7 is false: W has three distinct orbits on quadruples of weights which sum to zero: those quadruples of the form $\{x, x, -x, -x\}$ (of which there are 28), those of form $\{x, y, -x, -y\}$ (for $x \neq y$, there are 378 of these), and the remaining 630 "general" quadruples $\{w, x, y, z\}$ for which no pairwise sums vanish.
- In order to get our most explicit description of the cubic form invariant under E_6, we chose a clever basis for the fundamental representation which was invariant under a large subgroup of $\widetilde{W}$. This subgroup (the centralizer of an element of order 3 having no nontrivial fixed points in Λ) acts transitively on the weights and has only two orbits (of size 9 and 36) on triples of weights that summed to zero, corresponding to two different signs. The same approach could be applied to E_7, but the results are not nearly so spectacular. For example, it is impossible to find a subgroup $G \subseteq \widetilde{W}$ which acts transitively on the set C_0 *and* stabilizes a basis $B \subseteq \widetilde{C_0}$. For suppose such a pair (G, B) did exist. Since $\mathrm{Aut}_0(V)$ is a perfect group, $\ker \widetilde{\psi} \simeq \mathbf{Z}/4\mathbf{Z}$ is central in $\widetilde{W}$. Choose a generator $\widetilde{w}$ for $\ker \widetilde{\psi}$. Since $\widetilde{w}$ centralizes G, G must also stabilize the basis $B^{\widetilde{w}}$. Since G acts transitively on C_0, it follows that either $B^{\widetilde{w}} = B$ or $B^{\widetilde{w}} = -B$. In either case, we have $-B = B^{\widetilde{w}^2} = B$, a contradiction.

Despite these obstacles, we can still salvage a bit of our old analysis. In particular, we will find that the object $\widetilde{\Lambda}_E$ serves as a satisfactory "stand-in" for $\widetilde{\Lambda}_o$, even though the former is not associative.

6.1. **The Invariant Quartic.** To begin, let K denote the collection of all ordered 4-tuples $(w, x, y, z) \in C_0^4$ with $w + x + y + z = 0$. We let K_0 denote the subset consisting of all 4-tuples of the form $(x, x, -x, -x)$ or some permutation thereof, K_1 the subset of 4-tuples which are some permutation of $(x, y, -x, -y)$ $(x \neq y)$,

and $K_2 = K - (K_0 \cup K_1)$ the collection of "general" elements of K. We let $\widetilde{K}$, $\widetilde{K}_0$, $\widetilde{K}_1$, and $\widetilde{K}_2$ denote the preimages of these sets in $\widetilde{C}_0^4$.

Lemma 6.1.1. *Let $(\widetilde{w},\widetilde{x},\widetilde{y},\widetilde{z}) \in \widetilde{K}_2$ Then the expression $(\widetilde{w}\widetilde{x})(\widetilde{y}\widetilde{z}) \in \widetilde{\Lambda}_E$ is symmetric in $\widetilde{w}$, $\widetilde{x}$, $\widetilde{y}$, and $\widetilde{z}$.*

Proof. The equation $w+x+y+z=0$ implies that $-\frac{3}{2} = -\langle w,w\rangle = \langle w,x\rangle + \langle w,y\rangle + \langle w,z\rangle$. Since w and x have the same length and $w \neq -x$, $\langle w,x\rangle > -\frac{3}{2}$. On the other hand, $\langle w,x\rangle \equiv t_C$ modulo $\mathbf{Z}$, so $\langle w,x\rangle \geq -\frac{1}{2}$. Summing the same inequalities over y and z, we see that equality must hold, so $\langle w,x\rangle = \langle w,y\rangle = \langle w,z\rangle = -\frac{1}{2}$. Then $wx = (-1)^{\langle w,x\rangle - t_C} xw = xw$, and similarly for other pairwise products. This shows that the expression above is unchanged by exchanging w with x or y with z. To complete the proof, it suffices to show invariance under interchange of x and y. This follows from the associativity properties of the product:

$$(\widetilde{w}\widetilde{x})(\widetilde{y}\widetilde{z}) = \widetilde{w}(\widetilde{x}(\widetilde{y}\widetilde{z})) = -\widetilde{w}((\widetilde{x}\widetilde{y})\widetilde{z}) = -\widetilde{w}((\widetilde{y}\widetilde{x})\widetilde{z}) = \widetilde{w}(\widetilde{y}(\widetilde{x}\widetilde{z})) = (\widetilde{w}\widetilde{y})(\widetilde{x}\widetilde{z})$$

■

If $w+x+y+z=0$ because of some pairwise cancellations, say $w+x=0=y+z$, then the above result no longer holds, because $\widetilde{w}\widetilde{x} \neq \widetilde{x}\widetilde{w}$. In this case, one must be more careful in how one chooses to form the product. Given such a triple $\widetilde{w},\widetilde{x},\widetilde{y},\widetilde{z}$, one can assume (switching $\widetilde{y}$ and $\widetilde{z}$ if necessary) that $2\langle x,y\rangle \equiv 3 \pmod 2$. Then $2\langle w,z\rangle = 2\langle -x,-y\rangle = 2\langle x,y\rangle \equiv 3 \pmod 4$ as well. Then one has $\widetilde{w}\widetilde{z} = \widetilde{z}\widetilde{w}$, $\widetilde{x}\widetilde{y} = \widetilde{y}\widetilde{x}$. Moreover, $x+y=-(w+z)$, so $\widetilde{w}\widetilde{z}$ commutes with $\widetilde{x}\widetilde{y}$. Thus the four-fold product $(\widetilde{w}\widetilde{z})(\widetilde{x}\widetilde{y})$ is independent of the order in which the factors are chosen, *provided* that the pairs $(\widetilde{x},\widetilde{y})$ and $(\widetilde{w},\widetilde{z})$ are multiplied *first*. Moreover, this pairing is entirely intrinsic to the quadruple $(\widetilde{w},\widetilde{x},\widetilde{y},\widetilde{z})$.

Thus, whenever we have an ordered quadruple $\widetilde{Q} = (\widetilde{w},\widetilde{x},\widetilde{y},\widetilde{z}) \in \widetilde{K}$, we may associate a well-defined sign $\epsilon_{\widetilde{Q}}$ by the formula

$$\epsilon\widetilde{Q} = (\widetilde{w}\widetilde{x})(\widetilde{y}\widetilde{z})$$

where we assume the tuple has been reordered so $2\langle w,x\rangle \equiv 2\langle y,z\rangle \equiv 4 \pmod 2$. The discussion above guarantees that $\epsilon_{\widetilde{Q}}$ is well-defined and is unchanged if we apply a permutation to $\widetilde{Q}$.

Note that $\epsilon_{\widetilde{Q}}$ changes sign whenever any of its arguments changes sign. (Since calculating $\epsilon_{\widetilde{Q}}$ involves an even number of applications of e, it is even independent of the choice of e). For such a quadruple, we let $Y_{\widetilde{Q}}$ denote the product

$$Y_{\widetilde{w}} \otimes Y_{\widetilde{x}} \otimes Y_{\widetilde{y}} \otimes Y_{\widetilde{z}}$$

in $M_\pi^{\otimes 4}$; then $\epsilon_{\widetilde{Q}} Y_{\widetilde{Q}}$ is a well-defined element of $M_\pi^{\otimes 4}$ depending only on the underlying 4-tuple $Q = (w,x,y,z) \in K$; we denote this element by Y_Q.

We are now in a position to describe the form invariant under E_7:

Theorem 6.1.2. *The tensor*

$$\Theta = 2\sum_{Q\in K_0} Y_Q - \sum_{Q\in K_1} Y_Q - 2\sum_{Q\in K_2} Y_Q \in M_\pi^{\otimes 4}$$

in $M_\pi^{\otimes 4}$ is L-invariant.

Proof. By construction, Θ is Λ-invariant and $\widetilde{W}$-invariant. Let $\widetilde{\alpha} \in \widetilde{\Gamma}$; we must show that $[\widetilde{\alpha},\Theta] = 0$. The quantity $[\widetilde{\alpha},\Theta]$ is a weight vector for α; we must show that the coefficent c of the monomial $Y_{\widetilde{w}}Y_{\widetilde{x}}Y_{\widetilde{y}}Y_{\widetilde{z}}$ vanishes whenever $w+x+y+z=\alpha$. Without loss of generality,

$$-1 \leq \langle w,\alpha\rangle \leq \langle x,\alpha\rangle \leq \langle y,\alpha\rangle \leq \langle z,\alpha\rangle \leq 1$$

and the middle quantities sum to $\langle \alpha,\alpha\rangle = 2$. If $\langle w,\alpha\rangle = \langle x,\alpha\rangle = 0$ and $\langle y,\alpha\rangle = \langle z,\alpha\rangle = 1$, the proof that $c=0$ proceeds just as in the trilinear case (one needs only $\widetilde{W}$-invariance).

Otherwise, we have $\langle w,\alpha\rangle = -1$, $\langle x,\alpha\rangle = \langle y,\alpha\rangle = \langle z,\alpha\rangle = 1$. The relevant contributions come from terms of the form $[X_{\widetilde{\alpha}}, Y_{(w,x-\alpha,y,z)}]$ (and similarly with y or z in place of x) and the coefficient contributed by such a term is $C_k\epsilon_{\widetilde{Q}}$ where $\widetilde{Q} = \{\widetilde{w},\widetilde{\alpha}^{-1}\widetilde{x},\widetilde{y},\widetilde{z}\} \in \widetilde{K}_k$. Here $C_k = 2,-1,-2$ accordingly as $k=0,1,2$. We must show the sum of these contributions is 0.

Note that

$$-1 = \langle \alpha, w \rangle = \langle w + x + y + z, w \rangle = \frac{3}{2} + \langle x, w \rangle + \langle y, w \rangle + \langle z, w \rangle$$

Thus it is impossible to have $\langle x, w \rangle, \langle y, w \rangle$, and $\langle z, w \rangle$ all smaller than than $-\frac{1}{2}$, so at least one of x, y, or z is equal to $-w$. If $x = y = z = -w$, then $\alpha = w + x + y + z = w - w - w - w = -2w$, so $2 = \langle \alpha, \alpha \rangle = \langle -2w, -2w \rangle = 6$, a contradiction. Suppose $x = y = -w$, $z \neq -w$. Then $z - \alpha = -w$. Now $\widetilde{Q} = (\widetilde{w}, \widetilde{x}, \widetilde{y}, \widetilde{\alpha}^{-1}\widetilde{z}) \in \widetilde{K}_0$, while $\widetilde{Q}' = (\widetilde{w}, \widetilde{\alpha}^{-1}\widetilde{x}, \widetilde{y}, \widetilde{z}), \widetilde{Q}'' = (\widetilde{w}, \widetilde{x}, \widetilde{\alpha}^{-1}\widetilde{y}, \widetilde{z}) \in \widetilde{K}_1$. Thus it suffices to show that $\epsilon_{Q'} = \epsilon_Q = \epsilon_{Q''}$. By symmetry, it suffices to show the equality on the left side. For this we just invoke the definition: note that $\langle w, x - \alpha \rangle = \langle w, x \rangle - \langle w, \alpha \rangle = -\frac{1}{2}$ and $\langle x, y \rangle = \langle w, w \rangle = 3/2$, so

$$\begin{aligned}
\epsilon_{\widetilde{Q}'} &= (\widetilde{y}\widetilde{z})((\widetilde{\alpha}^{-1}\widetilde{x})\widetilde{w}) \\
&= (\widetilde{y}(\widetilde{z}\widetilde{\alpha}^{-1}))(\widetilde{x}\widetilde{w}) \\
&= -(\widetilde{y}(\widetilde{\alpha}^{-1}\widetilde{z}))(\widetilde{x}\widetilde{w}) \\
&= ((\widetilde{\alpha}^{-1}\widetilde{z})\widetilde{y})(\widetilde{x}\widetilde{w}) \\
&= (\widetilde{\alpha}^{-1}\widetilde{z})(\widetilde{y}(\widetilde{x}\widetilde{w})) \\
&= -(\widetilde{\alpha}^{-1}\widetilde{z})((\widetilde{y}\widetilde{x})\widetilde{w}) \\
&= (\widetilde{\alpha}^{-1}\widetilde{z})(\widetilde{w}(\widetilde{y}\widetilde{x})) \\
&= ((\widetilde{\alpha}^{-1}\widetilde{z})\widetilde{w})(\widetilde{y}\widetilde{x}) \\
&= \epsilon_{\widetilde{Q}}
\end{aligned}$$

Now let us suppose $z = -w$, but $x, y \neq -w$. Then $x + y = \alpha$, so $x \neq y$ and $\widetilde{Q} = (\widetilde{w}, \widetilde{x}, \widetilde{y}, \widetilde{\alpha}^{-1}\widetilde{z}) \in \widetilde{K}_2$, while

$$\widetilde{Q}' = (\widetilde{w}, \widetilde{\alpha}^{-1}\widetilde{x}, \widetilde{y}, \widetilde{z}) \neq (\widetilde{w}, \widetilde{x}, \widetilde{\alpha}^{-1}\widetilde{y}, \widetilde{z}) = \widetilde{Q}''$$

both lie in $\widetilde{K}_1$. Reasoning as above, it suffices to show that

$$\epsilon_{\widetilde{Q}} = -\epsilon_{\widetilde{Q}'} = -\epsilon_{\widetilde{Q}''}$$

By symmetry it suffices to show the first equality. Since $y - \alpha = -x \neq w$, we have $\langle y - \alpha, w \rangle < \frac{3}{2}$ so $\langle y, w \rangle < \frac{1}{2}$. Since $y \neq -w$, $\langle y, w \rangle > \frac{-3}{2}$, so $\langle y, w \rangle = \frac{-1}{2}$, and

$$\epsilon_{\widetilde{Q}'} = (\widetilde{y}\widetilde{w})((\widetilde{\alpha}^{-1}\widetilde{x})\widetilde{z}) = -(\widetilde{y}\widetilde{w})(\widetilde{x}(\widetilde{\alpha}^{-1}\widetilde{z})) = -\epsilon_{\widetilde{Q}}$$

as required. ∎

6.2. **Defining E_7.** Over the complex numbers, E_7 can be defined as the algebra of automorphisms of its 56-dimensional representation which leave invariant a symplectic form and an invariant quartic polynomial. However, this description is not valid over a field of characteristic 2. First, the object we want to consider is not the invariant quartic, but its polarization, a symmetric tensor in $M_\pi^{\otimes 4}$. Even if the quartic polynomial is written (over $\mathbf{Z}$) in "lowest terms", its polarization is divisble by 2. Hence we consider instead the polarization divided by 2; this is the tensor

$$\Theta = 2 \sum_{Q \in K_0} Y_Q - \sum_{Q \in K_1} Y_Q - 2 \sum_{Q \in K_2} Y_Q$$

which we constructed in the last section. The problem now is that the "interesting part" of this tensor is the third term, which still vanishes in characteristic 2. Consequently, we must be more careful if we are to give a description of E_7 which is valid in all characteristics.

In order to do this, we need to consider *all* invariant tensors of degree 4. Before proceeding, note that the symplectic form on M gives rise to an L-invariant isomorphism of M with its dual. Thus the distinction between covariant and contravariant tensors disappears, and we can (and shall) identify Θ with a multilinear form on M.

Over the complex numbers, we have the decomposition $M_{\mathbf{C}} \otimes M_{\mathbf{C}} \simeq \wedge^2 M_{\mathbf{C}} \oplus \mathbb{S}^2(M_{\mathbf{C}})$. Neither of these summands is irreducible: M has an invariant symplectic form, so $\wedge^2 M_{\mathbf{C}}$ contains a copy of the trivial representation and $\mathbb{S}^2(M_{\mathbf{C}})$ contains a copy of the adjoint representation. However, one can easily check that the residual representations are irreducible, so $M_{\mathbf{C}} \otimes M_{\mathbf{C}}$ is a direct sum of four nonisomorphic irreducible

representations. Since $-1 \in W$, all of these representations are self-dual. Thus $(M_{\mathbf{C}} \otimes M_{\mathbf{C}} \otimes M_{\mathbf{C}} \otimes M_{\mathbf{C}})^{L_{\mathbf{C}}}$ is four dimensional.

It is not hard to see where all these invariant tensors come from. Let $[,]$ denote the invariant symplectic form on M (say, corresponding to the isomorphism $e : \pi \otimes \pi \simeq \pi_0$). Via this form we may identify M with its dual. Thus we get 3 invariant tensors corresponding to the forms

$$\Phi_1 : (w, x, y, z) \mapsto [w, x][y, z]$$
$$\Phi_2 : (w, x, y, z) \mapsto [w, y][x, z]$$
$$\Phi_3 : (w, x, y, z) \mapsto [w, z][x, y]$$

Together with the form Θ, these generate the space of invariant 4-tensors over $\mathbf{C}$. Over $\mathbf{Z}$, the picture is rather similar: $(M \otimes M \otimes M \otimes M)^L$ is a free $\mathbf{Z}$-module of rank 4. Moreover, the tensors Θ, Φ_1, Φ_2, and Φ_3 are well-defined elements of this module. However, they do not generate the full module, only a submodule of index 2. The full module of L-invariants is generated by Φ_1, Φ_2, Φ_3 and

$$\Psi = \frac{\Theta + \Phi_1 + \Phi_2 + \Phi_3}{2}$$

(the integrality of which follows readily from our formula for Θ).

Our goal now is to prove that E_7 may be identified with the collection of endomorphisms of M leaving invariant $\Psi \in M_\pi^{\otimes 4}$ and the symplectic structure on M. For this we will need some preliminary results.

Lemma 6.2.1. *Let G_7 be the free abelian group generated by symbols $\{g_c\}_{c \in C_0}$, subject to the relations*

$$g_{-c} = -g_c$$
$$a + b + c + d = 0 \Rightarrow g_a + g_b + g_c + g_d = 0$$

Then the natural homomorphism $G_7 \to \Lambda^\vee$ is an isomorphism.

Proof. Since every element of Γ is a sum of two elements of C_0 and Γ generates Λ, Λ is contained in the image of ϕ. Together with C_0, Λ generates $\Lambda^\vee$, so ϕ is surjective.

Pick $c \in C_0$, and let $J = \{g_{c'} \in C_0 : \langle c, c' \rangle = \frac{-1}{2}\}$. Let G' be the quotient of G by the subgroup generated by g_c. Then G' is generated by the images $g'_{c'}$ of the elements of J which satisfy the relations

$$x + y + z = -c \Rightarrow g'_x + g'_y + g'_z$$

By 5.4.1, G' is a quotient of the weight lattice of E_6, and is therefore free of rank 6. Since G surjects onto a $\mathbf{Z}$-module of rank 7, G must be free of rank 7, and ϕ must be an isomorphism. ∎

Lemma 6.2.2. *Let $\alpha \in \Gamma$, $\mu, \nu \in \{v \in C_0 : \langle v, \alpha \rangle = -1\}$. Then either $\mu + \nu = -\alpha$ or $\langle \mu, \nu \rangle = \frac{1}{2}$.*

Proof. If $\langle \mu, \nu \rangle = \frac{-1}{2}$, then $\langle \mu + \nu, \mu + \nu \rangle = 2$, so $\mu + \nu$ is a root β. Then

$$\langle \alpha, \beta \rangle = \langle \alpha, \mu \rangle + \langle \alpha, \nu \rangle = -2$$

so $\beta = -\alpha$, as desired. ∎

Theorem 6.2.3. *Let R be a commutative ring. Then L_R is the Lie algebra of all endomorphisms of M_R leaving $[,]$ and Ψ invariant.*

Proof. Our proof follows that of Theorem 5.5.1. We let L' denote the Lie algebra of all endomorphisms of M_R leaving $[,]$ and Ψ invariant. Note that M_R has a natural $\Lambda^\vee$-grading into weight spaces $M_\lambda = RY_{\tilde{\lambda}}$. This induces a grading of $\mathrm{End}_R(M_R)$. Since $[,]$ and Ψ are homogeneous of degree zero, L' is a graded R-submodule of $\mathrm{End}_R(M_R)$. Thus, we get a decomposition of L' into weight spaces L'_α having the property that

$$L'_\alpha M_\lambda \subseteq M_{\lambda+\alpha}$$

We need only show that each root space L'_α is contained in L_R. Let $x \in L'_\alpha$. If $x = 0$ there is nothing to prove. Otherwise there is some $\lambda \in C_0$ such that x induces a nontrivial map $M_\lambda \to M_{\lambda+\alpha}$. Then $\alpha \in \Lambda$. There are several cases to consider:

- $\langle \lambda, \alpha + \lambda \rangle = \frac{3}{2}$. Then $\lambda = \alpha + \lambda$, so $\alpha = 0$. Then x stabilizes each weight space M_μ, so it acts by some scalar $f(\mu)$ on that space.

  From the invariance of $[,]$, we see that $f(-\lambda) = -f(\lambda)$. The invariance of Ψ then that if $a, b, c, d \in C_0$ with $a + b + c + d = 0$, then $f(a) + f(b) + f(c) + f(d) = 0$. Thus f induced a well-defined homomorphism $G_7 \to R$. By Lemma 6.2.1, f is induced by a homomorphism $\Lambda^\vee \to R$, or equivalently an element of Λ_R, which proves $x \in \Lambda_R \subseteq L_R$.
- $\langle \lambda, \alpha + \lambda \rangle < \frac{1}{2}$. Let $x Y_{\widetilde{\lambda}} = k Y_{\widetilde{c}}$. Choose $\gamma, \mu, \nu \in C_0$ such that $(\lambda + \alpha, \gamma, \mu, \nu) \in K_2$ and $\gamma, \mu, \nu \neq \lambda$. One easily checks that $\gamma + \alpha, \mu + \alpha, \nu + \alpha \notin C_0$. The invariance of Ψ implies that

  $$\Psi(xY_{\widetilde{\lambda}}, Y_{\widetilde{\gamma}}, Y_{\widetilde{\mu}}, Y_{\widetilde{\nu}}) + \Psi(Y_{\widetilde{\lambda}}, xY_{\widetilde{\gamma}}, Y_{\widetilde{\mu}}, Y_{\widetilde{\nu}}) + \Psi(Y_{\widetilde{\lambda}}, Y_{\widetilde{\gamma}}, xY_{\widetilde{\mu}}, Y_{\widetilde{\nu}}) + \Psi(Y_{\widetilde{\lambda}}, Y_{\widetilde{\gamma}}, Y_{\widetilde{\mu}}, xY_{\widetilde{\nu}}) = 0$$

  Examining the left side, we see that the only nonvanishing term is $\Psi(kY_{\widetilde{c}}, Y_{\widetilde{\gamma}}, Y_{\widetilde{\mu}}, Y_{\widetilde{\nu}}) = \pm k$. This forces $k = 0$ and we are done.
- $\langle \lambda, \lambda + \alpha \rangle = \frac{1}{2}$. Then α is actually a root in Γ.

  Pick $\widetilde{\alpha} \in \widetilde{\Gamma}$ lying over α. Then

  $$x Y_{\widetilde{\mu}} = \begin{cases} k_\mu Y_{\widetilde{\alpha}\widetilde{\mu}} & \text{if } \langle \alpha, \mu \rangle = -1 \\ 0 & \text{otherwise} \end{cases}$$

  To show that x is a multiple of $X_{\widetilde{\alpha}} \in L_R$, it suffices to show that the scalars k_μ are all the same. Let μ and ν be such that $\langle \alpha, \mu \rangle = \langle \alpha, \nu \rangle = -1$. If $\mu + \nu = -\alpha$, then the invariance of $[,]$ implies

  $$0 = [xY_{\widetilde{\mu}}, Y_{\widetilde{\nu}}] + [Y_{\widetilde{\mu}}, xY_{\widetilde{\nu}}] = \pm(k_\mu - k_\nu)$$

  so $k_\mu = k_\nu$. Otherwise, $\langle \mu, \alpha + \nu \rangle = \frac{-1}{2}$ by Lemma 6.2.2, so we can find $\gamma, \delta \in C_0$ with $(\mu, (\alpha + \nu), \gamma, \delta) \in K_2$. Since there are 5 choices for the pair (γ, δ), we may assume that $\gamma, \delta \neq -\alpha - \mu$, $\gamma, \delta \neq -\alpha - \nu$. Applying Lemma 6.2.2 again, we see that $\langle \gamma, \alpha \rangle = \langle \delta, \alpha \rangle = 0$. Applying the invariance of Ψ and using the fact that x annihilates $Y_{\widetilde{\gamma}}$ and $Y_{\widetilde{\delta}}$, we get

  $$0 = \Psi(xY_{\widetilde{\mu}}, Y_{\widetilde{\nu}}, Y_{\widetilde{\gamma}}, Y_{\widetilde{\delta}}) + \Psi(Y_{\widetilde{\mu}}, xY_{\widetilde{\nu}}, Y_{\widetilde{\gamma}}, Y_{\widetilde{\delta}}) = \pm(k_\mu - k_\nu)$$

  Thus $k_\mu = k_\nu$ and we are done.

■

Remark 6.2.4. If 2 is invertible in R, then the above result holds with Ψ replaced by the symmetric tensor Θ (since the invariance of the Φ_i follows from the invariance of the symplectic form on M). Thus, away from the prime 2, we recover the classical description of E_7.

References

[1] Adams, J. *Lectures on Exceptional Lie Groups*. University of Chicago Press, 1996.
[2] Adkins, W. and J. Weintraub. *Algebra: an Approach via Module Theory*. Springer-Verlag, 1992.
[3] Bourbaki, N. *Groupes et Algébres de Lie*, Chapitre VI. Masson, 1981.
[4] Chevalley, C. *The Algebraic Theory of Spinors*. In Claude Chevalley's Collected Works, Volume 2, Springer-Verlag 1997.
[5] Conway, J.H. et al. *Altas of Finite Groups*. Clarendon Press, 1975.
[6] Frenkel, I., Lepowsky, J. and A. Meurman. *Vertex Operator Algebras and the Monster*. Academic Press, 1988.
[7] Fulton, W. and J. Harris. *Representation Theory: A First Course*. Springer-Verlag, 1991.
[8] Griffiths, P. and J. Harris. *Principles of Algebraic Geometry*. Wiley, 1978.
[9] Hartshorne, R. *Algebraic Geometry*. Springer-Verlag, 1977.
[10] Humphreys, J.E. *Reflection Groups and Coxeter Groups*. Cambridge University Press, 1990.
[11] Serre, J.P. *Lie Algebras and Lie Groups*. Springer-Verlag, 1992.
[12] Shafarevich, I.R., ed. *Algebraic Geometry II*. Encyclopaedia of Mathematical Sciences, Volume 35, Springer Verlag, 1996.
[13] Springer, T.A. and R. Steinberg *Conjugacy Classes*. In Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Mathematics Volume 131, Springer-Verlag, 1970.
[14] Tits, J. *Normalisateurs de tores. I. Groupes de Coxeter étendus* in Journal of Algebra **4**, 1966, 96-116.

E-mail address: lurie@math.harvard.edu