Component Groups of Centralizers Corresponding to Unramified L-packets

by

Brent Fraser

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Science

in

M.Sc. Mathematics, Pure Mathematics

Carleton University

Ottawa, Ontario

©2014

Brent Fraser
Abstract

A theorem of Keys states that the cardinality of an unramified L-packet is equal to the order of a component group of a centralizer of a semi-simple element. We compute the component groups of centralizers in connected, quasi-simple, linear algebraic groups. We also compute the component groups for certain similitude groups.
Introduction

There is a connection between number theory and the representation theory of algebraic groups which was discovered by Langlands. Part of this discovery is that in some cases, one may associate an irreducible representation of an algebraic group $G(F)$ over a $p$-adic field $F$ with a factor of an L-function ([14]). However, this association outlined by Langlands remains mostly conjectural.

One case in which this association is known is that of irreducible unramified representations of split, connected, reductive groups over $p$-adic fields. In this case, we can associate a single factor of an L-function to a finite set of irreducible representations. These finite sets are called L-packets. Our goal is to compute the cardinality of these L-packets in the special case that $G$ is quasi-simple. For example, we look at the special linear group $G(F) = SL_n(F)$ in great detail.

In order to achieve our goal of computing the cardinality of an L-packet, we use a theorem of Keys ([11]). This theorem expresses the cardinality as the order of the component group of the centralizer of a semi-simple element in some complex algebraic group. Our first task is to provide sufficient background in order to define the objects introduced above and to state the required theorem. Although this work is not original and takes up almost half of this thesis, it is included for completeness.

The main contribution of this thesis is the computation of the component groups
of centralizers of semi-simple elements in $G(\mathbb{C})$. This work is original and has some independent value in terms of the structure theory of algebraic groups.

The reader is expected to be comfortable with undergraduate mathematics and basic theory of Lie algebras. All other required concepts will be explained as they are introduced.

Section 1 is where we explain $p$-adic fields and their Galois theory. This section is independent of Section 2 and Section 4. The ultimate goal here is to define the Weil group which is a modified Galois group. We begin by defining $p$-adic numbers and outlining some basic results. We then extend these results on $p$-adic numbers to finite field extensions of $F$. We are particularly interested in unramified field extensions. We characterize all unramified extensions in terms of roots of unity and show that they correspond precisely to the finite extensions of the finite field $\mathbb{F}_q$, where $q$ is a power of $p$.

The Weil group $W_F$ is a dense subgroup of the absolute Galois group of $F$. It is generated by the preimage of a Frobenius automorphism $Fr_q$ in the absolute Galois group of $\mathbb{F}_q$. We review some basic results of Galois theory and cover Galois theory over $p$-adic fields in greater detail.

In Section 2, we focus on the structure theory of linear algebraic groups. These groups are affine varieties which can be viewed as subgroups of $GL_n$. They are en-
dowed with the Zariski topology. Here, we describe the Zariski topology on an affine space and we define an affine variety. Then we define a linear algebraic group, reductive groups, semi-simple groups and quasi-simple groups. We will mostly restrict our attention to quasi-simple groups later.

Attached to each linear algebraic group is a quadruple, called a root datum. A root datum partially characterizes a linear algebraic group. The notion of a root datum involves the idea of a maximal torus and a system of roots, which we will define. For a given system of roots, there are finitely many corresponding connected, semi-simple linear algebraic groups. For a group $G$, a simple operation involving a natural pairing on its root datum gives another root datum. This new root datum corresponds to a group $\hat{G}$, which is called the dual group of $G$. In our discussion, we take $\hat{G}$ to be defined over $\mathbb{C}$ instead of the algebraic closure of $F$. We describe these concepts in detail for $GL_n$ and some other simple examples.

By this point, we have introduced enough theory to define an admissible homomorphism $\phi: W_F \to \hat{G}$ which is a map from the Weil group to the complex dual group of $G$. This homomorphism $\phi$ is what determines an L-packet. Similarly, $\phi$ also determines a semi-simple element $s \in \hat{G}$ for which we compute the centralizer $Z_{\hat{G}}(s)$ and its component group $Z_{\hat{G}}(s)/Z_{\hat{G}}(s)^0$.

Towards the end of Section 2, there is some remaining structure theory that is
necessary for the computations of the component groups. We define the Weyl group of $G$ which acts on the roots. We also define Borel subgroups which correspond bijectively to bases of root systems.

Section 3 is where we state the theorems which motivate this thesis. Namely, that the cardinality of an unramified L-packet equals the order of the corresponding component group. We define unramified, admissible homomorphisms $\phi$, unramified characters, and L-packets. Denoting the L-packet by $\Pi_\phi$, we have the following picture.

$$\phi: W_F \to \hat{G} \rightarrow s = \phi(Fr_q^{-1}) \downarrow$$

$$\Pi_\phi \quad Z_{\hat{G}}(s)/Z_{\hat{G}}(s)^0 \downarrow$$

We conclude Section 3 by giving a sketch of the reasoning behind the fact that $|\Pi_\phi| = |Z_{\hat{G}}(s)/Z_{\hat{G}}(s)^0|$.

Section 4 is the heart of this thesis. We give a detailed outline of the method which we use to compute the component group of the centralizer of a semi-simple element of an adjoint, quasi-simple, complex group $G$. We will explain how, for a given element $s$, the component group $Z_G(s)/Z_G(s)^0$ may be identified with a subgroup of an extension of the Weyl group. This extension of the Weyl group is called the affine Weyl group and acts on the real vector space $E$ generated by the
roots of $G$. If $x$ is a vector in $E$ then there is a map which sends $x$ to a maximal tours in $G$. This map is denoted by $\exp$. We use a theorem of Reeder in [17] which relates the stabilizer $\tilde{W}_x$ of an element $x \in E$ with the component group of the centralizer of $s = \exp(x)$.

We obtain a partial characterization of $\tilde{W}_x$ from [17]. From another perspective, elements of $\tilde{W}_x$ may be viewed as automorphisms of the augmented Dynkin diagram of $G$. The elements of this automorphism group are known and may be computed explicitly. Using these facts, we compute $\tilde{W}_x$ and $Z_G(s)/Z_G(s)^0$.

All quasi-simple groups are isomorphic to a quotient $G/H$ for some algebraic group $G$ with $H \subseteq Z$ where $Z$ is the centre of $G$. With this general approach in place, we compute $s = \exp(x)$ and the component groups for $G/Z$ equal to $PGL_n(\mathbb{C})$, $SO_{2n+1}(\mathbb{C})$, $PSp_{2n}(\mathbb{C})$, $PSO_{2n}(\mathbb{C})$, $E_6$, and $E_7$. The remaining quasi-simple groups of the form $G/Z$ have connected centralizers.

We require some more theory to deal with the cases where $G/H$ has nontrivial centre. It turns out that the only cases of interest are $G = SL_n(\mathbb{C})$ and $G = Spin_{2n}(\mathbb{C})$. We look at lifts of $s \in G/Z$ to intermediate subgroups $G/H$. We then compute all possible component groups of centralizers for a given lift. Thus, we obtain all possible component groups of centralizers in these intermediate cases.

Lastly, we consider component groups of centralizers in similitude groups. Ex-
amples of such groups are $GL_n(C)$ and $GSO_{2n}(C)$. We show that they are always connected.

Section 5 is where we compare our results to [10] where Keys computes the cardinality of L-packets in terms of analytically defined groups. More precisely, the groups are subgroups of the Weyl group $W_G$ which we shall denote by $R_\chi$. We show in Section 3 that we have the following picture

\[
\phi \quad \longrightarrow \quad s \\
\downarrow \quad \quad \quad \quad \quad \quad \downarrow \\
\Pi_\phi \quad \longrightarrow \quad R_\chi \quad \longrightarrow \quad \cong \quad Z_G(s)/Z_G(s)^0
\]

The isomorphism here is the isomorphism defined in [11]. We point out that in each adjoint case, our component groups are isomorphic to the corresponding group computed by Keys. We conclude with possibilities for future research.

1 $p$-Adic Fields

We wish to develop an understanding of $p$-adic fields. Here, we follow two books [4] and [6]. We begin with the notion of the $p$-adic valuation $v_p$ and $p$-adic absolute value $|\cdot|_p$ on $Q$ for some positive prime $p \in Z$. We will construct the field of $p$-adic numbers $Q_p$ as the completion of $Q$ with respect to $|\cdot|_p$. We then describe some topological properties of $Q_p$, introduce the ring of integers $Z_p$, the notion of a uniformizer, and
the residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

We will extend these ideas to general $p$-adic fields which are finite extensions $F$ of $\mathbb{Q}_p$. The $p$-adic absolute value on $\mathbb{Q}_p$ extends to $F$ and $F$ retains the same topological properties. While introducing the general notion of the ring of integers $\mathcal{O}_F$, a uniformizer $\varpi$ and the residue field $K$, we show that $K$ is a finite extension of $\mathbb{F}_p$. In fact we will determine explicitly the degree of the extension $K/\mathbb{F}_p$ and show how it relates to the degree of $F/\mathbb{Q}_p$.

We define unramified $p$-adic field extensions since these are the field extensions that will be of primary interest later. The main result here is that unramified extensions of $\mathbb{Q}_p$ correspond bijectively to extensions of the residue field $\mathbb{F}_p$. We state this as a lemma and then show that there is a unique unramified, degree $f$ extension of $\mathbb{Q}_p$ for every $f \geq 1$. All such extensions are given by adjoining roots of unity to a $p$-adic field $F$. We finish the section by describing the maximal unramified extension $F_u$ of $F$.

After this point, we will have almost built up enough of a foundation to begin defining the Weil group which is our ultimate goal in this preliminary section. Before this is done, we spend our time characterizing the Galois groups over $p$-adic fields. Specifically, we show that the bijection between unramified extensions of $\mathbb{Q}_p$ and finite extensions $\mathbb{F}_p$ passes to an isomorphism of the corresponding Galois groups. We
finish the section by defining and outlining the important properties of the topology on the absolute Galois group \( \text{Gal}(\overline{F}/F) \).

Finally, we will be able to define the Weil group which is tailored to suit unramified extensions of \( p \)-adic fields. For this, we follow [15]. First we show that for \( q = p^n \), \( \text{Gal}(\overline{F}_q/F_q) \) contains a dense cyclic subgroup. The Weil group over the finite field \( F_q \) is defined to be this subgroup. There is a homomorphism from \( \text{Gal}(\overline{F}/F) \) to \( \text{Gal}(\overline{F}_q/F_q) \) which allows us to construct a short exact sequence

\[
1 \to \text{Gal}(\overline{F}/F_u) \to \text{Gal}(\overline{F}/F) \to \text{Gal}(\overline{F}_q/F_q) \to 1.
\]

From this short exact sequence, we define the absolute Weil group \( W(\overline{F}/F) \) to be the subgroup of the absolute Galois group \( \text{Gal}(\overline{F}/F) \) given by the inverse image of the Weil group over \( F_q \). The absolute Weil group is a dense subgroup of \( \text{Gal}(\overline{F}/F) \) ([20], Theorem 1.4.1). We wish to define the Weil group because it retains some properties of the absolute Galois group while being easier to work with.

1.1 Understanding \( \mathbb{Q}_p \)

As previously noted, we begin with exploring \( \mathbb{Q}_p \). We follow ([6], Chapter 3, sections 2, 3, Chapter 5, sections 1-6) and ([4], Chapter 7, sections 1-5, 7, 8). Let \( p \in \mathbb{Z} \) be a positive prime and notice that for all \( x \in \mathbb{Q}^\times \), we may write \( x = p^{\alpha} m^n \), \( \alpha, m, n \in \mathbb{Z} \) and \( p \nmid m, n \).
Definition 1.1.1. A valuation on a field $F$ is a map $v : F^\times \to \mathbb{Q}$ which, for all $x, y \in F$, satisfies

1. $v(xy) = v(x) + v(y)$, and
2. $v(x + y) \leq \min\{v(x), v(y)\}$.

Definition 1.1.2. We define the $p$-adic valuation $v_p$ on $\mathbb{Q}$ by $v_p(x) = \alpha$ for all nonzero $x = p^{\alpha \frac{m}{n}} \in \mathbb{Q}$, and by convention, we define $v_p(0) = \infty$.

It is not difficult to show that $v_p$ is a valuation on $\mathbb{Q}_p$.

Definition 1.1.3. For a field $F$, an absolute value $|\cdot| : F \to \mathbb{R}_+$ is defined by

i) $|x| = 0$ if and only if $x = 0$,

ii) $|xy| = |x||y|$ for all $x, y \in F$,

iii) $|x + y| \leq |x| + |y|$ for all $x, y \in F$,

and we say $|\cdot|$ is non-archimedean if

iv) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in F$.

Note that property iv) implies property iii).

Definition 1.1.4. We define the $p$-adic absolute value $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ by $|x|_p = p^{-v_p(x)}$. 

13
Let us give a sketch of why $|\cdot|_p$ truly is a non-archimedean absolute value on $\mathbb{Q}$. The convention $v_p(0) = \infty$ gives property i). Property 1) in Definition 1.1.1 gives property ii) and property 2) in Definition 1.1.1 gives property iv).

**Definition 1.1.5.** We define $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Specifically, $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$ where $\mathcal{C}$ is the set of Cauchy sequences of $\mathbb{Q}$ with respect to $|\cdot|$ and $\mathcal{N}$ is the set of null sequences of $\mathbb{Q}$. A copy of $\mathbb{Q}$ sits inside of $\mathbb{Q}_p$ via mapping $x \in \mathbb{Q}$ to the constant sequence $(x) + \mathcal{N}$. In addition $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ using this general construction.

It is fairly straightforward to show that for all $(x_n), (y_n) \in \mathcal{C}$, $(x_n) + (y_n) = (x_n + y_n) \in \mathcal{C}$ and $(x_n)(y_n) = (x_n y_n) \in \mathcal{C}$. Then $\mathbb{Q}_p$ is a ring with addition is defined by

\[ ((x_n) + \mathcal{N}) + ((y_n) + \mathcal{N}) = (x_n + y_n) + \mathcal{N} \]

and multiplication is defined by

\[ ((x_n) + \mathcal{N})((y_n) + \mathcal{N}) = (x_n y_n) + \mathcal{N} \]

for all $(x_n) + \mathcal{N}, (y_n) + \mathcal{N} \in \mathbb{Q}_p$. Since $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$ ([6], Lemma 3.2.8), $\mathbb{Q}_p$ is a field.

Let’s show how $\mathbb{Q}_p$ inherits the $p$-adic absolute value from $\mathbb{Q}$. 

---

14
Definition 1.1.6. For \( \lambda = (x_n) + N \in \mathbb{Q}_p \) we define the \( p \)-adic absolute value by
\[
|\lambda|_p = \lim_{n \to \infty} |x_n|_p.
\]

Firstly, notice that \( |\cdot|_p \) is well defined on \( \mathbb{Q}_p \) since as \( n \) increases, \( |x_n|_p \) for a null sequence \( (x_n) \) tends to 0. As \( (x_n) \) is Cauchy, the inequality \( ||x_n|_p - |m|_p| \leq |x_n - m|_p \) implies that \( (|x_n|_p) \) is a Cauchy sequence in \( \mathbb{R} \). Therefore the limit of \( |x_n|_p \) as \( n \) tends to \( \infty \) exists since \( \mathbb{R} \) is complete.

Lemma 1.1.7. The absolute value \( |\cdot|_p \) on \( \mathbb{Q} \) extends to a non-archimedean absolute value on \( \mathbb{Q}_p \).

Proof. Let \( \lambda = (x_n) + N, \gamma = (y_n) + N \in \mathbb{Q}_p \). The fact that \( |\cdot|_p \) satisfies property i) of Definition 1.1.3 on \( \mathbb{Q}_p \) follows from the fact that \( |\lambda|_p = \lim_{n \to \infty} |x_n|_p \) exists and is 0 if and only if \( (x_n) \in N \). Property ii) of Definition 1.1.3 follows from \( \lim_{n \to \infty} |x_n y_n|_p = \lim_{n \to \infty} |x_n|_p \lim_{n \to \infty} |y_n|_p \).

Now for all \( n > 0, |x_n + y_n| \leq \max\{|x_n|_p, |y_n|_p\} \). Suppose \( |\lambda|_p \geq |\gamma|_p \). Then we know that there exists some \( N > 0 \) such that \( |x_n|_p \geq |y_n|_p \) for all \( n > N \). Therefore \( |x_n + y_n|_p \leq |x_n|_p \) for all \( n > N \) which implies \( |\lambda + \gamma|_p \leq |\lambda|_p \). Hence
\[
|\lambda + \gamma|_p \leq \max\{|\lambda|_p, |\gamma|_p\}
\]
so \( |\cdot|_p \) satisfies iv) of Definition 1.1.3. \( \square \)

The following lemma gives us a better understanding how sequences in \( \mathbb{Q} \) behave with respect to \( |\cdot|_p \). Namely, it states that the absolute value of a convergent sequence stabilizes.
Lemma 1.1.8. For all \((x_n) \in C\) such that \((x_n) \notin N\), there exists \(N > 0\) such that \(n, m > N\) implies \(|x_n|_p = |x_m|_p\).

Proof. First we will show that all triangles with respect to \(|\cdot|_p\) are isosceles. Let \(x \neq y \in Q_p\) and without loss of generality, assume \(|x|_p > |y|_p\). Then \(|x + y|_p \leq |x|_p\) and \(|x|_p \leq \max\{|x + y|_p, |y|_p\}\) since \(x = (x + y) - y\). As \(|x|_p > |y|_p\), we have \(|x|_p \leq |x + y|_p\) which implies \(|x|_p = |x + y|_p\).

Now, let \((x_n) \in C \setminus N\). Since \((x_n)\) is Cauchy, there exists an \(M, N_1 > 0\) such that \(|x_n|_p > M\) for all \(n > N_1\). Moreover, there exists \(N_2 > 0\) such that \(|x_n - x_m|_p < M\) for all \(n, m > N_2\). Take \(N = \max\{N_1, N_2\}\) so for all \(n, m > N\), \(|x_n - x_m|_p < |x_n|_p\) and \(|x_n - x_m|_p < |x_m|_p\). Hence, \(|x_n - x_m|_p < \max\{|x_n|_p, |x_m|_p\}\). Considering the triangle with sides \(|x_n|_p\), \(|-x_m|_p\) and \(|x_n + (-x_m)|_p\) gives \(|x_n|_p = |x_m|_p\).

Since every \(|x_n|_p\) stabilizes, we know that for any \(\lambda \in Q_p\), \(|\lambda|_p = p^{-\alpha}\) for some \(\alpha \in \mathbb{Z}\). Then we can see that the image of \(|\cdot|_p\) on \(Q_p\) is equal to the image of \(|\cdot|_p\) on \(Q\). It then follows that \(v_p\) extends to a \(p\)-adic valuation on \(Q_p\).

Definition 1.1.9. With the previous notation, the \(p\)-adic valuation on \(Q_p\) is defined by \(v_p(x) = \alpha\). Then we have \(|\lambda|_p = p^{-v_p(\lambda)}\).

We wish to determine some basic topological properties of \(Q_p\). We can conclude that \(Q_p\) is a metric space when equipped with the metric topology given by \(d(x, y) = |x - y|_p\) for all \(x, y \in Q_p\). By construction, \(Q_p\) is a complete topological field.
With respect to the metric $d(\cdot, \cdot)$, the open ball of radius $r$ centred at $a \in \mathbb{Q}_p$ is $B(a, r) = \{ x \in \mathbb{Q}_p \mid |a - x|_p < r \}.$

Let us define the ring of integers of $\mathbb{Q}_p$.

**Definition 1.1.10.** The ring of integers of $\mathbb{Q}_p$ is $\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \}$.

It is not difficult to show that $\mathbb{Z}_p$ is a ring using Definition 1.1.3, iv). We will show a few important results about the ring of integers.

**Lemma 1.1.11.**

i) The units in $\mathbb{Z}_p$ are $\mathbb{Z}_p^\times = \{ x \in \mathbb{Q}_p \mid |x|_p = 1 \}.$

ii) $p\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \mid |x|_p < 1 \}$ is a maximal ideal of $\mathbb{Z}_p$.

iii) For any $n \geq 1$, $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Namely, $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

iv) For all $x \in \mathbb{Q}_p$, $x = up^{v_p(x)}$ for some $u \in \mathbb{Z}_p^\times$ and $Q_p = \mathbb{Z}_p[\frac{1}{p}]$.

**Proof.** i) Suppose $x \in \mathbb{Z}_p$ is a unit of $\mathbb{Z}_p$. Since $|x|_p \leq 1$, we have $|x^{-1}|_p = |x|_p^{-1} \geq 1$.

This implies $|x^{-1}|_p = 1$ as $x^{-1} \in \mathbb{Z}_p$. Hence $\mathbb{Z}_p^\times \subseteq \{ x \in \mathbb{Q}_p \mid |x|_p = 1 \}$. Conversely, if $x \in \mathbb{Z}_p$ and $|x|_p = 1$ then $x^{-1} \in Q_p$ such that $|x^{-1}|_p = 1$. Therefore $x^{-1} \in \mathbb{Z}_p$ so $x \in \mathbb{Z}_p^\times$. Hence $\mathbb{Z}_p^\times \supseteq \{ x \in \mathbb{Q}_p \mid |x|_p = 1 \}$ which gives $\mathbb{Z}_p^\times = \{ x \in \mathbb{Q}_p \mid |x|_p = 1 \}$.
ii) Suppose \(x \in \mathbb{Q}_p\) such that \(|x|_p < 1\). Then \(|x|_p \leq \frac{1}{p}\) which implies \(|\frac{1}{p}x|_p \leq 1\).

Hence \(\frac{1}{p}x \in \mathbb{Z}_p\) or equivalently \(x \in p\mathbb{Z}_p\). Now suppose \(I\) is an ideal of \(\mathbb{Z}_p\) such that \(p\mathbb{Z}_p \subseteq I \subseteq \mathbb{Z}_p\). If \(I \neq p\mathbb{Z}_p\) then \(I \cap \mathbb{Z}_p^\times \neq \emptyset\) by 1). Then we must have \(I = \mathbb{Z}_p\).

Therefore \(p\mathbb{Z}_p\) is maximal since \(p\mathbb{Z}_p \neq \mathbb{Z}_p\).

iii) Suppose \(x \in \mathbb{Z}_p\) and let \(n \geq 1\). Since \(\mathbb{Q}\) is dense in \(\mathbb{Q}_p\), there exists integers \(a, b\) such that \(|x - \frac{a}{b}|_p \leq p^{-n}\). Without loss of generality, we assume \(\gcd(a, b) = 1\).

We have
\[
\left| \frac{a}{b} \right|_p = \left| \frac{a}{b} - x + x \right|_p \leq \max \left\{ |x|_p, \left| x - \frac{a}{b} \right|_p \right\} \leq 1
\]
since \(x \in \mathbb{Z}_p\). This implies \(\frac{a}{b} \in \mathbb{Z}_p\) and \(p \nmid b\). Hence \(b\) is a unit in \(\mathbb{Z}/p^n\mathbb{Z}\) so there exists \(b' \in \mathbb{Z}\) such that \(bb' \equiv 1 \mod p^n\). Thus \(bb' = kp^n + 1\) for some \(k \in \mathbb{Z}\) and
\[
\left| \frac{a}{b} - ab' \right|_p = \left| \frac{a}{b} (1 - bb') \right|_p = \left| \frac{a}{b} \right|_p |1 - (kp^n + 1)|_p \leq p^{-n}
\]
since \(\frac{a}{b} \in \mathbb{Z}_p\). Now \(ab' \equiv \alpha_n \mod p^n\) for some \(0 \leq \alpha_n \leq p^n - 1\). Then \(\alpha_n = ab' - tp^n\) for some \(t \in \mathbb{Z}\) and
\[
|x - \alpha_n|_p = \left| (x - \frac{a}{b}) + (\frac{a}{b} - ab') + tp^n \right|_p
\]
\[
\leq \max \left\{ \left| x - \frac{a}{b} \right|_p, \left| \frac{a}{b} - ab' \right|_p, |tp^n|_p \right\}
\]
\[
\leq p^{-n}.
\]

Therefore the sequence of integers \((\alpha_n)\) converges to \(x\) in \(\mathbb{Z}_p\).
Let \( \bar{x} \) denote the image of \( x \in \mathbb{Z}_p \) in \( \mathbb{Z}_p/p^n\mathbb{Z}_p \) and consider the map \( \psi : \mathbb{Z}_p/p^n\mathbb{Z}_p \rightarrow \mathbb{Z}/p^n\mathbb{Z} \) defined by \( \psi(\bar{x}) = \bar{\alpha}_n \). By the construction of \( (\alpha_n) \), each \( \alpha_n \) is unique so \( \psi \) is well-defined. Since \( \mathbb{Z} \subseteq \mathbb{Z}_p \), \( \psi \) is surjective. We also have

\[
\ker \psi = \{ \bar{x} \mid \alpha_n \in p^n\mathbb{Z} \} = \{ \bar{0} \}
\]

so \( \psi \) is injective. For \( y \in \mathbb{Z}_p \) and \( (\gamma_n) \) defined for \( y \) in the same way as \( (\alpha_n) \) for \( x \), \( (\alpha_n - \gamma_n) \) converges to \( x - y \). Then

\[
\psi(\bar{x} - \bar{y}) = \psi(\bar{x} - \bar{y}) = \bar{\alpha}_n - \bar{\gamma}_n = \bar{\alpha}_n - \bar{\gamma}_n = \psi(\bar{x}) - \psi(\bar{y}).
\]

Hence \( \psi \) is an isomorphism of groups. Taking \( n = 1 \) gives \( \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p \).

iv) Let \( x \in \mathbb{Q}_p \) such that \( x \neq 0 \). Then

\[
|x^{p^{-v_p(x)}}|_p = |x|_p|p|^{v_p(x)} = p^{-v_p(x)}p^{v_p(x)} = 1
\]

which implies \( x^{p^{-v_p(x)}} = u \) for some \( u \in \mathbb{Z}_p^\times \). Then \( x \in p^{v_p(x)}\mathbb{Z}_p \) which implies \( \mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}] \).

\[
\text{Definition 1.1.12. We say that an element } \varpi \in p\mathbb{Z}_p \text{ with } |\varpi| = \frac{1}{p} \text{ is a uniformizer of } \mathbb{Q}_p.
\]

We can see that \( p \in p\mathbb{Z}_p \) is a uniformizer of \( \mathbb{Q}_p \).

\[
\text{Definition 1.1.13. We say that } \mathbb{Z}_p/p\mathbb{Z}_p \text{ is the residue field of } \mathbb{Q}_p.
\]

We will return to these concepts for arbitrary \( p \)-adic fields.
1.2 Finite Extensions of $\mathbb{Q}_p$

With our understanding of $\mathbb{Q}_p$, we can generalize many results to an arbitrary $p$-adic field $F$.

**Definition 1.2.1.** A $p$-adic field is a complete field which has characteristic 0, has a discrete non-archimedean absolute value and a finite residue field.

A field $F$ is a $p$-adic field if and only if $F$ is a finite extension of $\mathbb{Q}_p$ ([4], chapter 8, Lemma 1.1). This means that if we wish to understand $p$-adic fields, we need only look at finite extensions of $\mathbb{Q}_p$.

We begin by formally defining some concepts that were only mentioned in the previous sections. Then we can match up the results for $F$ with what we know about $\mathbb{Q}_p$. We will show that $|\cdot|_p$ extends from $\mathbb{Q}_p$ to $F$. We also show that $F$ has a residue field $K$ and a uniformizer $\wp$ where $K/F_p$ is finite and $F = \mathcal{O}_F[\frac{1}{\wp}]$. Suppose $F$ is a $p$-adic field with $[F: \mathbb{Q}_p] = n$.

Recall that we may view $F$ as a vector space over $\mathbb{Q}_p$. It is clear that $F$ acts on itself by left multiplication which is a linear transformation. Given a basis of $F$ over $\mathbb{Q}_p$ and an element $x \in F^\times$, we have a matrix $A_x$ of the linear transformation of $x$ acting on $F$. The norm $N_{F/\mathbb{Q}_p}$ of $F$ over $\mathbb{Q}_p$ is defined by $N_{F/\mathbb{Q}_p}(x) = \det(A_x)$ for all $x \in F^\times$.

**Definition 1.2.2.** For all $x \in F^\times$, the $p$-adic absolute value on $F$ is given by
Now, one may easily verify that $|\cdot|$ truly is an absolute value on $F$. In fact, $|\cdot|$ is the unique extension of $|\cdot|_p$ to a non-archimedean absolute value on $F$ ([6], Theorem 5.3.5). We also have that extending the $p$-adic absolute value is compatible under field extensions.

**Lemma 1.2.3.** Suppose $Q_p \subseteq L \subseteq F$ where $[L: Q_p] = m$, $[F: Q_p] = n$ then for all $x \in L$, $\sqrt[n]{|N_{L/Q_p}(x)|_p} = \sqrt[m]{|N_{F/Q_p}(x)|_p}$.

**Proof.** Let $x \in L$. By basic facts of finite degree field extensions,

$$N_{F/Q_p}(x) = N_{L/Q_p}(N_{F/L}(x)) = N_{L/Q_p}(x^{[F:L]}) = N_{L/Q_p}(x^{[F:Q_p]/[L:Q_p]}) = N_{L/Q_p}(x)^{\frac{m}{n}}$$

which gives

$$\sqrt[n]{|N_{F/Q_p}(x)|_p} = (|N_{L/Q_p}(x)|_p^{\frac{m}{n}})^\frac{1}{n} = \sqrt[m]{|N_{L/Q_p}(x)|_p}$$

Since the $p$-adic absolute value extends to $F$, the $p$-adic valuation extends to $F$ as well.

21
**Definition 1.2.4.** For \( x \in F^\times \), \(|x| = p^{-v_p(x)}\) where \( v_p(x) = \frac{1}{n} v_p(N_{F/Q_p}(x)) \) is the \( p \)-adic valuation on \( F \) and we say \( v_p(0) = \infty \).

It follows that \( v_p(x) \in \frac{1}{n} \mathbb{Z} \). In fact \( v_p: F^\times \rightarrow \mathbb{Q} \) is a homomorphism and the image is contained in \( \frac{1}{e} \mathbb{Z} \) for some greatest positive integer \( e \in \mathbb{Z} \) which divides \( n \).

**Definition 1.2.5.** We say \( e = e(F/Q_p) \) is the ramification index. We say \( F/Q_p \) is unramified if \( e = 1 \). We also define \( f(F/Q_p) = \frac{n}{e} \).

When there is no ambiguity, we will write \( f = f(F/Q_p) \).

**Definition 1.2.6.** We say \( \varpi \in F \) is a uniformizer of \( F \) if \( v_p(\varpi) = \frac{1}{e} \).

Note that “the” uniformizer of \( Q_p \) is \( p \) and \( v_p(p) = 1 \). This matches our definition since \( v_p(Q_p^\times) = \mathbb{Z} \). Clearly any uniformizer \( \varpi \) of \( F \) satisfies \(|\varpi| = p^{-\frac{1}{e}} \). Note that a uniformizer is not unique.

**Definition 1.2.7.** The ring of integers of \( F \) is defined as \( \mathcal{O}_F = \{ x \in F \mid |x| \leq 1 \} \).

This definition matches with the notion of the ring of integers \( \mathbb{Z}_p \) in an obvious way. In the general case, we set \( \mathcal{P}_F = \{ x \in F \mid |x| < 1 \} \) which is a maximal ideal of \( \mathcal{O}_F \), analogous to \( p\mathbb{Z}_p \).

**Definition 1.2.8.** We define the residue field of \( F \) by \( K = \mathcal{O}_F/\mathcal{P}_F \).

We have results for \( \mathcal{O}_F \) that parallel Lemma 1.1.11 for \( \mathbb{Z}_p \).
Lemma 1.2.9.

i) The $p$-adic units are $\mathcal{O}_F^\times = \{ x \in F \mid |x| = 1 \}$.

ii) $\mathcal{P}_F = \{ x \in F \mid |x| < 1 \}$ is a maximal ideal of $\mathcal{O}_F$ which is generated by $\varpi$.

iii) $K$ if a finite extension of $\mathbb{F}_p$.

iv) For all $x \in F$, $x = u\varpi^{ev_p(x)}$ for some $u \in \mathcal{O}_F^\times$ and $F = \mathcal{O}_F[\frac{1}{\varpi}]$.

Proof. The proof of (1), (2) and (4) are almost identical the the proof of Lemma 1.1.11, i), ii) and iv) except we use $\varpi$ instead of $p$. We only show a proof for iii).

We have that for all $x \in \mathbb{Z}_p$, $x \in \mathcal{P}_F$ if and only if $x \in p\mathbb{Z}_p$. Then the injection $\mathbb{Z}_p \hookrightarrow \mathcal{O}_F$ induces an injection $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow K$ as the previous argument shows that we have a homomorphism with trivial kernel.

Now suppose $[F : \mathbb{Q}_p] = n$. Let $x_1, \ldots, x_{n+1} \in \mathcal{O}_F$. Then there exists $c_1, \ldots, c_{n+1} \in \mathbb{Q}_p$ such that $\sum_{i=1}^{n+1} c_i x_i = 0$ and not all $c_i$ are 0. Since we may multiply through by any factor we wish, we may assume without loss of generality that $\max_{1 \leq i \leq n+1} \{|c_i|\} = 1$. Then, passing to the residue field, we get $\sum_{i=1}^{n+1} \bar{c}_i \bar{x}_i = 0$ where not all $\bar{c}_i$ are 0. Hence $[K : \mathbb{Z}_p] \leq n$.

If fact, one can determine the degree of $[K : \mathbb{F}_p]$ exactly.

Lemma 1.2.10. For the residue field $K$ of $F$, we have $[K : \mathbb{F}_p] = f$ and $K \cong \mathbb{F}_{p^f}$. 

23
Proof. The proof is relatively long. See ([6], Proposition 5.4.6). A sketch of the proof is as follows. Suppose $[K:F_p] = m$. Then choose representatives $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_F$ such that $\bar{\alpha}_1, \ldots, \bar{\alpha}_m$ form a basis of $K$ over $F_p$. The idea is to show $\{\varpi^j \alpha_i \mid 0 \leq j \leq e-1, 1 \leq i \leq m\}$ is a basis of $F$ over $Q_p$. This then gives $em = [F:Q_p]$ which implies $m = f$.

Finally, we can describe the topology on $F$ given by the metric, $d(x, y) = |x - y|$ for all $x, y \in F$, in the same way we described the topology on $Q_p$.

1.3 Unramified $p$-adic Extensions

We defined unramified extensions previously to be a $p$-adic field $F$ such that $[F:Q_p] = n$ is finite and $v_p(F^\times) = \mathbb{Z}$. In this case (Lemma 1.2.10) $K = F_{p^n}$. An immediate consequence here is that the uniformizers of $Q_p$ are uniformizers of $F$; i.e. we may take $\varpi = p$. Our goal here is to characterize the unramified extensions of $Q_p$ in terms of $m$th roots of unity where $p \nmid m$ and in terms of the finite field extension $K/F_p$. We will show that there is a bijection between the unramified field extensions $F$ of $Q_p$ and the finite field extensions $F_{p^f}$ of $F_p$ (up to isomorphism). This bijection will arise from the fact that every unramified extension is given by $Q_p(\alpha)$ for $\alpha$ a primitive $(p^f - 1)$-st root of unity. Then $F$ is the splitting field of $X^{p^f} - X$ over $Q_p$ and its residue field $K$ is the splitting field of $X^{p^f} - X$ over $F_p$. Firstly, we determine
the possible degrees of unramified extensions of \( \mathbb{Q}_p \).

**Lemma 1.3.1.** For each \( f \geq 1 \), there exists an unramified field extension \( F \) of \( \mathbb{Q}_p \) such that \( [F : \mathbb{Q}_p] = f \). Each such extension corresponds to a degree \( f \) extension of \( \mathbb{F}_p \).

**Proof.** Recall that for every \( f \geq 1 \), \( \mathbb{F}_p^\times \) is a cyclic group of order \( p^f - 1 \). Then \( \mathbb{F}_p^f = \mathbb{F}_p(\alpha) \) where \( \alpha \) is a generator of \( \mathbb{F}_p^\times \). Moreover, \( \mathbb{F}_p^f \cong \mathbb{F}_p[x]/m_\alpha(x) \) where \( m_\alpha(x) \) is the minimal polynomial of \( \alpha \) and \( m_\alpha(x) \) has degree \( f \). Hence there exists an irreducible polynomial of degree \( f \) over \( \mathbb{F}_p \) for all \( f \geq 1 \). We can choose any lift of any such polynomial to \( \mathbb{Z}_p \). We then get an irreducible polynomial of degree \( f \) over \( \mathbb{Q}_p \) ([6], Corollary 5.3.8). Adjoining a root of this polynomial to \( \mathbb{Q}_p \) therefore gives an extension \( F \) of \( \mathbb{Q}_p \) with degree \( f \). Moreover, since \( [\mathbb{F}_p^f : \mathbb{F}_p] = f \) and \( [F : \mathbb{Q}_p] = fe \) we have \( fe = f \). Hence \( e = 1 \) and \( F/\mathbb{Q}_p \) is unramified.

In fact, we can say exactly what the unramified extensions of \( \mathbb{Q}_p \) are. We use Hensel’s Lemma to pass from roots a polynomial in \( \mathbb{K} \) to roots of a polynomial in \( F \).

**Lemma 1.3.2** (Hensel’s Lemma). Let \( F/\mathbb{Q}_p \) be a finite extension with uniformizer \( \varpi \). Let \( g(X) \in \mathcal{O}_F[X] \). Suppose there exists \( \alpha \in \mathcal{O}_F \) such that \( g(\alpha) \equiv 0 \mod \varpi \) and \( g'(\alpha) \not\equiv 0 \mod \varpi \) where \( g'(X) \) is the formal derivative of \( g(X) \). Then there exists \( \beta \in \mathcal{O}_F \) such that \( \beta \equiv \alpha \mod \varpi \) and \( g(\beta) = 0 \).
For the proof of Hensel’s Lemma, see ([6], Theorem 5.4.8).

**Lemma 1.3.3.** Suppose $F/\mathbb{Q}_p$ is an unramified extension of degree $f$. Then $F$ contains a primitive $(p^f - 1)$-st root of unity which is the lift of a primitive $(p^f - 1)$-st root of unity in the residue field $K$ of $F$. Moreover, the image in $K$ of a primitive $(p^f - 1)$-st root of unity of $F$ is itself a primitive $(p^f - 1)$-st root of unity.

**Proof.** Let $F/\mathbb{Q}_p$ be an unramified extension of degree $f$, let $\varpi$ be a uniformizer of $F$ and let $K$ be the residue field of $F$. Then $K$ contains the cyclic group of $(p^f - 1)$-st roots of unity by Lemma 1.2.10. Moreover, by basic properties of cyclic groups, $K$ contains the distinct $m$-th roots of unity for all $m | p^f - 1$. Let $\alpha \in K$ be a primitive $(p^f - 1)$-st root of unity. We choose a lift of $\alpha$ to $\mathcal{O}_F^\times$ and apply Lemma 1.3.2 with $g(x) = X^{p^f - 1} - 1$. Therefore, there exists $\beta \in \mathcal{O}_F^\times$ such that $\beta$ is a $p^f - 1$-st root of unity and $\beta \equiv \alpha \mod \varpi$. Take $k \geq 1$ minimal such that $\beta^k = 1$. Then $\bar{1} \equiv \beta^k \mod \varpi$ which implies $\alpha^k \equiv 1 \mod \varpi$. Since $\alpha$ is a primitive root of unity and $k$ is minimal, we have $k = p^f - 1$. Hence $\beta$ is a primitive $(p^f - 1)$-st root of unity in $F$.

For the final assertion, let $\zeta$ be a primitive $(p^f - 1)$-st root of unity in $F$ and denote its image in $K$ by $\bar{\zeta}$. Choose a minimal $k \in \mathbb{N}$ such that $\bar{\zeta}^k = \bar{1}$. This implies $\zeta^k = 1 + \gamma$ for some $\gamma \in \mathcal{P}_F$. Equivalently, $\zeta^k \equiv 1 \mod \varpi$. Now

$$\left(\zeta^k\right)^{p^r} = \sum_{t=0}^{p^r} \binom{p^r}{t} \gamma^t \equiv 1 \mod \varpi^{r+1}$$
for all \( r \geq 0 \) since \( p^r \in \mathcal{P}_F \). Thus
\[
\zeta^k \equiv (\zeta^k)^{p^r} \equiv 1 \mod \varpi^{r+1}
\]
for all \( r \geq 0 \). It follows that \( \zeta^k - 1 \in \mathcal{P}_F^{p+1} \) for all \( r \geq 0 \). This implies
\[
|\zeta^k - 1| \leq |\varpi^{r+1}| = p^{-(r+1)}
\]
for all \( r \geq 0 \). Therefore \( |\zeta^k - 1| = 0 \) which gives \( \zeta^k - 1 = 0 \); i.e. \( \zeta^k = 1 \). We conclude that \( k = p^f - 1 \) as \( k \) was chosen to be minimal. Hence \( \tilde{\zeta} \) is a \((p^f - 1)\)-st root of unity. \( \square \)

To summarize, primitive \((p^f - 1)\)-st roots of unity in \( F \) correspond bijectively with primitive \((p^f - 1)\)-st roots of unity in \( K \).

**Lemma 1.3.4.** Each unramified extension of \( \mathbb{Q}_p \) of degree \( f \) can be obtained by adjoining a primitive \((p^f - 1)\)-st root of unity to \( \mathbb{Q}_p \).

**Proof.** Let \( F \) be an unramified extension of \( \mathbb{Q}_p \) with degree \( f \) and let \( \alpha \) be a primitive \((p^f - 1)\)-st root of unity in \( F \). Lemma 1.3.3 guarantees that such an \( \alpha \) exists. Then we have \( \mathbb{Q}_p \subseteq \mathbb{Q}_p(\alpha) \subseteq F \). Let \( k \) be the residue field of \( \mathbb{Q}_p(\alpha) \) over \( \mathbb{Q}_p \). Let \( \bar{\alpha} \) be the image of \( \alpha \) in \( k \). Then, by Lemma 1.3.3, \( \bar{\alpha} \) is a primitive \((p^f - 1)\)-st root of unity in \( k \). Therefore \( \mathbb{F}_{p^f} \subseteq k \subseteq K \) which implies \([k : \mathbb{F}_p] \geq f\). But \([K : \mathbb{F}_p] = f \) since \([F : \mathbb{Q}_p] = f\) so \([k : \mathbb{F}_p] = f\). Therefore \([\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geq f\) so \([\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = f\) and \( F = \mathbb{Q}_p(\alpha) \). \( \square \)

27
Corollary 1.3.5. Let $\alpha \in \overline{\mathbb{Q}_p}$ be an $m^{th}$ root of unity such that $p \nmid m$. Then $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is an unramified extension. Moreover, for any unramified extension $F/\mathbb{Q}_p$, $F(\alpha)/\mathbb{Q}_p$ is also an unramified extension.

Proof. If $p \nmid m$ there exists $f$ such that $m \mid p^f - 1$ since $p$ is a unit in $\mathbb{Z}/m\mathbb{Z}$. By Lemma 1.3.1 and Lemma 1.3.4, there exists a primitive $(p^f - 1)$-st root of unity $\zeta$ such that $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is an unramified extension of degree $f$. We have $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\zeta)$. Therefore $v_p(\mathbb{Q}_p(\alpha)) \subseteq v_p(\mathbb{Q}_p(\zeta)) \subseteq \mathbb{Z}$ which implies $e(\mathbb{Q}_p(\alpha)/\mathbb{Q}_p) = 1$. Hence $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is unramified.

Now, by Lemma 1.3.4, $F = \mathbb{Q}_p(\gamma)$ for some $k^{th}$ root of unity $\gamma$ such that $p \nmid k$. Then $F(\alpha) = \mathbb{Q}_p(\alpha, \gamma)$. Since $v_p(\mathbb{Q}_p(\alpha)) \subseteq \mathbb{Z}$ and $v_p(\mathbb{Q}_p(\gamma)) \subseteq \mathbb{Z}$, we have $v_p(F) \subseteq \mathbb{Z}$. Hence $e(F/\mathbb{Q}_p) = 1$ and $F/\mathbb{Q}_p$ is unramified. \hfill \square

Corollary 1.3.6. For each $f \geq 1$ there is, up to isomorphism, exactly one unramified extension $F$ of $\mathbb{Q}_p$ with degree $f$ and the unramified extensions of $\mathbb{Q}_p$ are in bijection with the finite extensions of $\mathbb{F}_p$.

Proof. Existence follows from Lemma 1.3.1 and uniqueness follows from Lemma 1.3.4.

In the proof of Lemma 1.3.4, we showed that

$$[k : \mathbb{F}_p] = f = [K : \mathbb{F}_p]$$

28
where \( k \) is the residue field of \( \mathbb{Q}_p(\alpha) \), \( \alpha \) a primitive \( p^f - 1 \)-st root of unity. Then \( K \) and \( k \) are both the splitting field of \( X^{p^f} - X \) over \( F_p \) so \( K = k \). Hence each unramified extension \( F/\mathbb{Q}_p \) of degree \( f \) corresponds to exactly one extension of \( F_p \); namely \( F_{p^f} \).

However, this holds for all \( f \) so we have a bijection between the unramified extensions and the finite extensions of \( F_p \). \( \square \)

**Corollary 1.3.7.** A \( p \)-adic field \( F \) is the splitting field of \( X^{p^f} - X \) over \( \mathbb{Q}_p \) if and only if \( F/\mathbb{Q}_p \) is an unramified extension of degree \( f \).

*Proof.* Suppose \( F/\mathbb{Q}_p \) is unramified of degree \( f \). Let \( g(X) = X^{p^f} - X \in F[X] \) and let \( \bar{g}(X) = g(X) \mod \mathcal{P}_F \in K[X] \). Then taking the formal derivative of \( \bar{g}(X) \) gives \( \bar{g}'(X) = -1 \) so for all \( \bar{\alpha} \in K \), we apply Lemma 1.3.2 to get \( \alpha \in \mathcal{O}_F \) such that \( g(\alpha) = 0 \) and \( \alpha \equiv \bar{\alpha} \mod \mathcal{O}_F \). However Lemma 1.2.10 says \( K = F_{p^f} \) so we take \( \alpha \) to be a primitive \( (p^f - 1) \)-st root of unity. Then, by Lemma 1.3.3, \( \alpha \) lifts to a primitive \( (p^f - 1) \)-st root of unity. Hence \( g(X) \) splits in \( F \). Therefore \( F \) contains the splitting field of \( g(X) \) over \( \mathbb{Q}_p \). By Corollary 1.3.6, we must have that \( F \) is the splitting field of \( g(X) \).

Conversely, if \( F \) is the splitting field of \( X^{p^f} - X \) over \( \mathbb{Q}_p \) then every root of \( X^{p^f-1} - 1 \) is an element of \( F \). Hence \( F \) contains all the \( (p^f - 1) \)-st roots of unity. Therefore \( F = \mathbb{Q}_p(\alpha) \) where \( \alpha \) is a primitive \( (p^f - 1) \)-st root of unity. So, by Lemma 1.3.4, \( F/\mathbb{Q}_p \) is unramified with degree \( f \). \( \square \)
To summarize these results, we have the following diagram:

\[
\begin{array}{c}
F/Q_p \text{ unramified of degree } f & \hookleftarrow \text{ degree } f \text{ extensions of } F_p \\
\downarrow \quad \downarrow & \quad \uparrow \quad \uparrow \\
\text{Splitting field of } X^{p^f} - X \text{ over } Q_p & \hookleftarrow \text{Splitting field of } X^{p^f} - X \text{ over } F_p
\end{array}
\]

Now we define a maximal unramified extension of \( Q_p \) and denote this extension by \((Q_p)_u\). We define \((Q_p)_u\) to be \( Q_p \) adjoin all \((p^f - 1)\)-st roots of unity for all \( f \geq 1 \). This construction is maximal in the following sense. If \( L/Q_p \) is unramified then, by Lemma 1.3.4, \( L \) is \( F \) adjoin some \((p^f - 1)\)-st roots of unity where \( f \geq 1 \) so \( L \subseteq (Q_p)_u \). Although we defined unramified extensions to be finite extensions, we still say \((Q_p)_u/Q_p\) is unramified in the following sense. By Corollary 1.3.5, \( \nu_p \) restricted to \((Q_p)_u\) has image \( \mathbb{Z} \) and \((Q_p)_u\) has residue field \( \overline{\mathbb{F}_p} \) since \( X^{p^f} - X \) splits in the residue field for all \( f \geq 1 \). It is also worth noting that since extending \( |\cdot|_p \) is compatible with finite field extensions (Lemma 1.2.10), we can define \( |\cdot| \) on \((Q_p)_u\) in the obvious way; for all \( x \in L \subseteq (Q_p)_u \) with \( [L : Q_p] = n \) we define \( |x| = \sqrt[n]{|\text{N}_{L/Q_p}(x)|_p} \) for some \( L/Q_p \).

One may generalize the notion of a maximal unramified extension for an arbitrary \( p \)-adic field \( F \). In the discussion above, simply replace \( Q_p \) by \( F \), \((Q_p)_u\) by \( F_u \), \( p^f \) by \( q^f \) where \( q \) is a power of \( p \), and \( F_p \) by \( \mathbb{F}_q \) which is the residue field of \( F \).
1.4 Galois Groups over $p$-adic Fields

Consider a $p$-adic field $F$ with residue field $\mathbb{F}_q$, $q = p^n$. Recall that for a field $K$, the absolute Galois group $\text{Gal}(\overline{K}/K)$ is the group of automorphisms of the algebraic closure of $K$ which fix $K$. Our goal is to understand the Galois groups of extensions of finite fields, the Galois groups of unramified $p$-adic field extensions, $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ and $\text{Gal}(\overline{F}/F)$. We begin with a general reminder of Galois theory. By Corollary 1.3.6, there is a bijection between unramified extensions $F$ of $\mathbb{Q}_p$ and finite extensions $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$. We will show that this bijection passes to an isomorphism of the corresponding Galois groups $\text{Gal}(F/\mathbb{Q}_p)$ and $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

For all $n \geq 1$, $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. In fact, $\mathbb{F}_p$ is equal to the set of roots of $X^{p^n} - X$ so $|\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. Recall that the Frobenius automorphism $Fr_p$ is defined by $Fr_p: \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}, Fr_p(x) = x^p$ for all $x \in \mathbb{F}_{p^n}$ with $|Fr_p| = n$. Thus $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic with generator $Fr_p$; i.e. $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}) = \langle Fr_p \rangle$. This is shown in Example 7, [5] on page 566. By similar arguments, one can show $Fr_p \in \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ so $\langle Fr_p \rangle$ is a subgroup of $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

**Proposition 1.4.1.** Suppose $F/\mathbb{Q}_p$ is an unramified extension of degree $n$. There is a (non-canonical) $\sigma \in \text{Gal}(F/\mathbb{Q}_p)$ such that $\text{Gal}(F/\mathbb{Q}_p) = \langle \sigma \rangle$. Moreover, we may define an action of $\sigma$ on $\mathbb{F}_{p^n}$ which corresponds to $Fr_p$. In particular $\text{Gal}(F/\mathbb{Q}_p) \cong \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ and $F/\mathbb{Q}_p$ is abelian.
Proof. By Corollary 1.3.7, $F$ is the splitting field of $X^{p^n} - X$ over $\mathbb{Q}_p$ so $F/\mathbb{Q}_p$ is Galois with $|\text{Gal}(F/\mathbb{Q}_p)| = [F : \mathbb{Q}_p] = n$. Let $\sigma \in \text{Gal}(F/\mathbb{Q}_p)$. Since $F/\mathbb{Q}_p$ is Galois, Definition 1.2.2 gives that for all $x \in F$ we have

$$|\sigma(x)| = \sqrt[p^n]{|N_{F/\mathbb{Q}_p}(\sigma(x))|} = \sqrt[p^n]{\prod_{\eta \in \text{Gal}(F/\mathbb{Q}_p)} \eta(\sigma(x))} = \sqrt[p^n]{\prod_{\eta \in \text{Gal}(F/\mathbb{Q}_p)} \eta(x)} = |x|.$$ 

Thus $\sigma(\mathcal{O}_F) = \mathcal{O}_F$, $\sigma(\mathcal{P}_F) = \mathcal{P}_F$ and $\sigma$ has a well-defined action on $K = \mathcal{O}_F/\mathcal{P}_F$. Similarly, $\sigma$ has a well-defined action on $\mathbb{Z}_p/p\mathbb{Z}_p$. Since $\sigma \in \text{Gal}(F/\mathbb{Q}_p)$, this action of $\sigma$ is an automorphism $\bar{\sigma}$ of $K$ which fixes $\mathbb{Z}_p/p\mathbb{Z}_p$. Using $K \cong \mathbb{F}_{p^n}$ and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ we see that $\bar{\sigma} \in \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. The map $\sigma \mapsto \bar{\sigma}$ is a homomorphism. Now $F = \mathbb{Q}_p(\zeta)$ where $\zeta$ is a primitive $(p^n - 1)$-st root of unity. By Lemma 1.3.3, we also have that $\bar{\zeta}$ the image of $\zeta$ in $\mathbb{F}_{p^n}$ is also a primitive $(p^n - 1)$-st root of unity. $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$ so $\mathbb{F}_{p^n} = \bar{\mathbb{F}_p}(\bar{\zeta})$. Therefore $\sigma$ is completely determined by $\sigma(\zeta)$ and $\bar{\sigma}$ is completely determined by $\bar{\sigma}(\bar{\zeta})$. Now suppose $\bar{\sigma}(\bar{\zeta}) = \bar{\zeta}$. This implies $\sigma(\zeta) \in \zeta + \mathcal{P}_F$; i.e. $\zeta^k = \zeta + x$ for some $x \in \mathcal{P}_F$, $k \geq 1$. But $|\zeta^{-1}| = 1$ and $x\zeta^{-1} \in \mathcal{P}_F$. 

32
Thus $\zeta^{k-1} = 1 + x\zeta^{-1}$ and it follows that $\zeta^{k-1} \in 1 + \mathcal{P}_F$. We apply the same argument as in Lemma 1.3.3 to get $\zeta^{k-1} = 1$. We must have $\zeta^k = \zeta$, $x = 0$ and $p^n \mid k$. Hence $\sigma$ is the identity automorphism. Therefore the map $\sigma \mapsto \overline{\sigma}$ is a injection. However $|\text{Gal}(F/Q_p)| = |\text{Gal}(F_{p^n}/F_p)|$ so the map is a bijection. Therefore we can choose $\sigma \in \text{Gal}(F/Q_p)$ such that $\sigma$ acts as $Fr_p$ on $K$. Moreover, this $\sigma$ has order $n$ so $\text{Gal}(F/Q_p)$ is cyclic with generator $\sigma$.

We define $F^{ab}$ to be the maximal abelian extension of $F$. To prove $F^{ab}$ exists, note that applying ([5], Proposition 21 (2), §14.4) shows that the compositum of abelian extensions is itself abelian. We may then apply Zorn’s Lemma to the set of abelian extensions of $F$.

**Corollary 1.4.2.** For $F$ a $p$-adic field, $F_u \subseteq F^{ab}$.

*Proof.* Let $F/Q_p$ be unramified. For any $m^{\text{th}}$ root of unity $\zeta$ where $p \nmid m$, $F(\zeta)/Q_p$ is unramified by Corollary 1.3.5. Then, by Proposition 1.4.1, $\text{Gal}(F(\zeta)/Q_p)$ is abelian. We construct the maximal unramified abelian extension of $F$ by adding all $(p^f - 1)$-st roots of unity to $F$ for $f \geq 1$. Then by using the same reasoning that $F^{ab}$ exists, we have that this maximal unramified abelian extension is $F$ adjoin all $m^{\text{th}}$ root of unity where $p \nmid m$. Hence the maximal unramified abelian extension is $F_u$. Therefore $F_u \subseteq F^{ab}$. □
We will now look at the absolute Galois group $\text{Gal}(\overline{F}/F)$. This group can be made into a topological group for which the Fundamental Theorem of Galois Theory applies. The topology on $\text{Gal}(\overline{F}/F)$ is called the Krull topology and is defined by the open sets being $\emptyset$, $\text{Gal}(\overline{F}/F)$ and \{\(\sigma\text{Gal}(\overline{F}/K) \mid K/F \text{ finite Galois}, \sigma \in \text{Gal}(\overline{F}/F)\}\. As a topological group, $\text{Gal}(\overline{F}/F)$ is compact, Hausdorff and totally disconnected ([16], Theorem 17.6). It is not difficult to see from this definition that multiplication and inversion are homeomorphisms.

**Lemma 1.4.3.** Suppose $F$ is a $p$-adic field with residue field $\mathbb{F}_q$. Then $\text{Gal}(F_u/F) \cong \text{Gal}(\overline{F}_q/\mathbb{F}_q)$.

**Proof.** We will show the following diagram outlines the desired group isomorphism.

\[
\begin{array}{c}
\text{Gal}(F_u/F) \rightarrow \prod_{K/F \text{ unramified}} \text{Gal}(K/F) \rightarrow \prod_{n \geq 1} \text{Gal}(\mathbb{F}_q^n/\mathbb{F}_q) \\
\longrightarrow \text{Gal}(\overline{F}_q/\mathbb{F}_q)
\end{array}
\]

Recall from the discussion at the end of Section 1.3 that $\overline{F}_q$ is the residue field of $F_u$. For all $\sigma \in \text{Gal}(F_u/F)$ and for all finite unramified extensions $K/F$, $\sigma|_K \in \text{Gal}(K/F)$. By the proof of Proposition 1.4.1, we may identify $\sigma|_K$ with $\overline{\sigma}|_{\mathbb{F}_q^n} \in \text{Gal}(\mathbb{F}_q^n/\mathbb{F}_q)$ where $[K:F] = n$. Every $\sigma \in \text{Gal}(F_u/F)$ is completely determined by its actions on the roots of unity. Since primitive roots of unity in $F_u$ correspond to primitive roots of unity in $\overline{F}_q$, the map $\sigma \mapsto (\overline{\sigma}|_{\mathbb{F}_q^n})_{n \geq 1}$ is an injective homomorphism.
of groups. On the other hand, for all \( \eta \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \), \( \eta|_{\mathbb{F}_{q^n}} \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \) and each \( \eta \) is completely determined by its restriction to the finite extensions of \( \mathbb{F}_q \). Therefore \( \eta \mapsto (\eta|_{\mathbb{F}_{q^n}})_{n \geq 1} \) is an injective homomorphism of groups.

Thus, we have injective homomorphisms \( \text{Gal}(F_u/F) \rightarrow \prod_{n \geq 1} \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \) and \( \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \rightarrow \prod_{n \geq 1} \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \). The images of both injections are subgroups of the group \( \prod_{n \geq 1} \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \). Moreover, each map has the same image. For a similar argument, see [16], Theorem 17.6. Therefore we get the desired isomorphism and \( \text{Gal}(F_u/F) \cong \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \).

### 1.5 The Weil Group

We now know enough about the Galois group over a \( p \)-adic field \( F \) with residue field \( \mathbb{F}_q \), \( q = p^n \), that we can define the Weil group \( W(\overline{F}, F) \) in \( \text{Gal}(\overline{F}/F) \). To achieve this, the first step is to determine how \( \text{Gal}(\overline{F}/F) \) is related to \( \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \). Lemma 1.4.3 allows us to identify \( \text{Gal}(F_u/F) \) with \( \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \) so we may construct a short exact sequence with \( \text{Gal}(\overline{F}/F_u) \), \( \text{Gal}(\overline{F}/F) \) and \( \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \). Next, we look at the subgroup of \( \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \) generated by \( F_{r_q} \). This is the Weil group over the finite field \( \mathbb{F}_q \). We will show that this is a dense cyclic subgroup so it retains many topological properties of the Galois group while being much simpler to work with.

We then define the absolute Weil group in terms of the inverse image of \( <F_{r_q}> \).
Gal($\overline{F}/F$) with respect to the constructed short exact sequence. This gives a dense subgroup of $\text{Gal}(\overline{F}/F)$ which is much simpler to work with while being topologically similar to $\text{Gal}(\overline{F}/F)$ ([20], Theorem 1.4.1). We will not show that the absolute Weil group is dense in $\text{Gal}(\overline{F}/F)$.

We first consider finite fields since we wish to consider unramified extensions of $\mathbb{Q}_p$. We look at the group generated by the Frobenius automorphism in $\text{Gal}(\overline{F}_q/F_q)$.

**Lemma 1.5.1.** The subgroup $< Fr_q >$ of $\text{Gal}(\overline{F}_q/F_q)$ is a proper dense subgroup.

**Proof.** We know that $Fr_q \in \text{Gal}(\overline{F}_q/F_q)$ since the $Fr_q$ fixes $F_q$ and is an automorphism of every finite extension of $F_q$. Therefore $< Fr_q >$ is a subgroup of $\text{Gal}(\overline{F}_q/F_q)$ which implies $\text{Gal}(\overline{F}_q/\text{Fix}< Fr_q >) = < Fr_q >$. Then, [16], Theorem 17.8, gives $\text{Fix}< Fr_q > = \text{Fix}< Fr_q >$ and $< Fr_q > = \text{Gal}(\overline{F}_q/\text{Fix}< Fr_q >)$. Since $\text{Fix}< Fr_q > = F_q$, it follows that $< Fr_q > = \text{Gal}(\overline{F}_q/F_q)$. Hence $< Fr_q >$ is dense in $\text{Gal}(\overline{F}_q/F_q)$.

The discussion in [5] at end end of page 652 gives that $\text{Gal}(\overline{F}_q/F_q)$ is uncountable. Since $< Fr_q >$ is countable, it follows that $< Fr_q >$ is a proper subgroup of $\text{Gal}(\overline{F}_q/F_q)$. \(\square\)

Now we define the Weil group of $\overline{F}_q/F_q$.

**Definition 1.5.2.** The Weil group $W(\overline{F}_q,F_q)$ is the cyclic topological group $< Fr_q >$ with the discrete topology.
We will now determine how \( \text{Gal}(\overline{F}/F) \) is related to \( \text{Gal}(\overline{F}_q/F_q) \). By Lemma 1.4.3, we have

\[
\text{Gal}(\overline{F}/F) \xrightarrow{\eta \mapsto \eta|_{F_u}} \text{Gal}(F_u/F) \cong \text{Gal}(\overline{F}_q/F_q).
\]

The map \( \eta \mapsto \eta|_{F_u} \) is surjective since it follows from [5], Theorem 13.4.27 that every \( \sigma \in \text{Gal}(F_u/F) \) can be extended to an automorphism of \( \overline{F} \). Moreover, this map has kernel \( \text{Gal}(\overline{F}/F_u) \). Putting this all together gives the short exact sequence

\[
1 \to \text{Gal}(\overline{F}/F_u) \to \text{Gal}(\overline{F}/F) \to \text{Gal}(\overline{F}_q/F_q) \to 1.
\]

We call \( \text{Gal}(\overline{F}/F_u) \) the inertia group of \( \overline{F} \) and denote it by \( I \).

**Definition 1.5.3.** The (absolute) Weil group \( W(\overline{F}, F) \) is the inverse image of \( W(\overline{F}_q, F_q) \) in \( \text{Gal}(\overline{F}/F) \) with respect to the previous short exact sequence.

Now, we have the short exact sequence

\[
1 \to I \to W(\overline{F}, F) \to W(\overline{F}_q, F_q) \to 1.
\]

We endow \( W(\overline{F}, F) \) with the topology such that this is a short exact sequence of topological groups. Abusively denoting \( \sigma \) from Proposition 1.4.1 by \( Fr_q \), we have \( W(\overline{F}, F) = < Fr_q > I \) which is given the discrete topology on \( < Fr_q > \) and relative topology on \( I \subseteq \text{Gal}(\overline{F}/F) \).

We may write

\[
W(\overline{F}, F) = \bigcup_{m \in \mathbb{Z}} (Fr_q)^m \text{Gal}(\overline{F}/F_u) = \bigcup_{m \in \mathbb{Z}} (Fr_q)^m I
\]
which is a subgroup of $\text{Gal}(\overline{F}/F)$.

2 Linear Algebraic Groups, Dual Groups and Root Datum

This section is devoted to defining and characterizing reductive linear algebraic groups. We follow [19] and [8]. We begin with defining the Zariski topology. The Zariski topology is defined in terms of closed sets and the closed sets are given by common zeros of sets of polynomials. Hence the closed sets correspond to ideals in a polynomial algebra. We will also show that the notion of connectedness corresponds to prime ideals in a polynomial algebra.

We will define a linear algebraic group over an algebraically closed field $K$. Essentially, a linear algebraic group $G$ is a set of points over a field $K$ with the structure of a topological group. We define two important types of linear algebraic group. The first is a semi-simple group and the second is a reductive group. We will focus on groups that satisfy one of these conditions. The subsection is concluded with a series of examples. These examples will also reoccur throughout the other subsections.

With the notion of a linear algebraic group in place, we then wish to define its root datum which is a quadruple that encodes much of the structure of the group.
A root system is a set of vectors which encodes the structure of the Lie algebra of a given group. A root datum is an augmentation of a root system. We state an important theorem which gives a bijective correspondence between root data and connected reductive linear algebraic groups. The number of such groups which have a root datum with a fixed root system is determined by a finite quotient group which depends only on the root datum. This group is called the fundamental group.

Many results here will not be proven. Instead, we will illustrate the ideas by way of example. Most examples will focus on $GL_n$ since it is fairly simple and we are only concerned with its subgroups. This is due to the fact that every linear algebraic group is isomorphic to a closed subgroup of $GL_n$ ([19], Theorem 2.3.7). First we define a character on $G$ which is a homomorphism from $G$ to $K^\times$. There is also the notion of a dual character which is a homomorphism from $K^\times$ to $G$. We define a maximal torus $T$ of $G$ which is often taken to be a diagonal subgroup of $G$.

Lastly, we introduce the Weyl group which is the normalizer of a torus modulo its centralizer. Borel subgroups will be introduced as well. Borel subgroups correspond bijectively with the bases of the roots. This allows us to recover information about a group from its root datum or recover information about the root datum from the group.

We wish to define a linear algebraic group over a $p$-adic field. The results for
an algebraically closed field extend to an arbitrary subfield $F$ when multiplication
and inversion are defined over $F$ and taking a certain tensor product with $K$ over
$F$ recovers the original group $G$. In this case, the group defined over $F$ is called an
$F$-group or an $F$-form of $G$. Then we define a split $F$-torus, which is $F$-isomorphic
to a group of diagonal matrices. We then focus on reductive linear algebraic groups
with a maximal split $F$-torus. We make use of examples here as well. We conclude
with a theorem which states that for any given root datum, a reductive $F$-split $F$
group exists.

2.1 The Zariski Topology on an Affine Space

For a vector space $V$ defined over an algebraically closed field $K$, we will define an
(affine) algebraic set $X$. It is basically the set of zeros in $V$ of sets of $K$-valued
polynomials. We define The Zariski topology on $V$ where the closed sets are the
algebraic sets. This makes $V$ a compact space where points are closed. The topology
on an algebraic set $X$ is given by the subspace topology. We then define the notion
of irreducibility which is stronger than connectedness. Irreducibility is preserved
by continuous maps and there is an algebraic formulation of the criterion as well.
Namely, $X$ is irreducible if and only if the ideal of functions vanishing on $X$ is prime.

We introduce the notion of an affine space which we endow with the Zarski
topology and define regular functions on open sets of an affine space $X$. A regular function on an open set is a rational functions defined at every point in the set. The set of regular functions on a given open set forms a $K$-algebra so we get a map from open sets to $K$-algebras, denoted $\mathcal{O}_X$. We say $\mathcal{O}_X$ is a sheaf. An affine variety is the pair $(X, \mathcal{O}_X)$ in which $X$ is an affine set.

Let $K$ be an algebraically closed field, $V = K^m$ and consider the polynomial algebra $K[T_1, \ldots, T_m]$. For a subset $X \subseteq V$, define the ideal $\mathcal{I}(X) = \{ f \in K[T_1, \ldots, T_m] \mid f(x) = 0 \text{ for all } x \in X \}$ and we define the set $\mathcal{V}(I) = \{ x \in V \mid f(x) = 0 \text{ for all } f \in I \}$ for an ideal $I$ of $K[T_1, \ldots, T_m]$. Hilbert’s Nullstellensatz ([8], Theorem (Hilbert’s Nullstellensatz)) gives $\mathcal{V}(I) \neq \emptyset$ for any proper ideal $I$ and $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ where $\sqrt{I} = \{ f \in K[T_1, \ldots, T_m] \mid f^n \in I \text{ for some } n \geq 1 \}$ is the radical of $I$. This gives a bijection between affine sets in $V$ and radical ideals of $K[T_1, \ldots, T_m]$.

**Lemma 2.1.1.** The map $I \mapsto \mathcal{V}(I)$ satisfies the following properties.

1. $\mathcal{V}(\{0\}) = V$ and $\mathcal{V}(K[T_1, \ldots, T_m]) = \emptyset$.
2. $I \subseteq J$ implies $\mathcal{V}(J) \subseteq \mathcal{V}(I)$.
3. $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$.
4. For a collection of ideals $\{I_\alpha \mid \alpha \in A\}$, if $I = \sum_{\alpha \in A} I_\alpha$ then $\mathcal{V}(I) = \bigcap_{\alpha \in A} \mathcal{V}(I_\alpha)$.

**Proof.** Property i) and ii) are simple to prove.
For iii), note that \( \mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J) \). However, \( IJ \subseteq I \cap J \) so by ii) we have \( \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J) \). Hence \( \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J) \).

Lastly, to prove iv), we have \( \bigcap_{\alpha \in A} \mathcal{V}(I_\alpha) \subseteq \mathcal{V}(I) \). Now, for any \( \gamma \in A \), we have \( I_\gamma \subseteq I \). If \( \bigcap_{\alpha \in A} \mathcal{V}(I_\alpha) \not\subseteq \mathcal{V}(I) \) then there exists \( x \in \mathcal{V}(I) \) such that \( x \notin I_\gamma \) for some \( \gamma \). This implies \( x \notin \mathcal{V}(I) \) since \( I_\gamma \subseteq I \) which is a contradiction. Hence \( \bigcap_{\alpha \in A} \mathcal{V}(I_\alpha) = \mathcal{V}(I) \).

Properties i), iii) and iv) define a topology on \( V \) by defining the closed sets.

**Definition 2.1.2.** The Zariski topology on \( V \) is given by defining the closed sets to be \( \mathcal{V}(I) \) where \( I \) is an ideal of \( K[T_1, \ldots, T_m] \).

The Zariski topology on a closed set \( X \subseteq V \) is given by defining the closed sets to be \( \mathcal{V}(I) \) where \( I \) is an ideal of \( K[T_1, \ldots, T_m] \) with \( I(X) \subseteq I \). This is simply the subspace topology on \( X \).

We define a notion related to connectedness in the Zariski topology.

**Definition 2.1.3.** We say \( X \subseteq V \) is reducible if \( X \) is the union of two proper, nonempty, closed subsets. If \( X \) is not reducible, we say \( X \) is irreducible.

**Lemma 2.1.4.** For a closed subset \( X \subseteq V \), we have

1. if \( X \) is irreducible and we have a continuous map \( f : X \to Y \) then \( f(X) \) is irreducible, and
2. *X* is irreducible if and only if \( \mathcal{I}(X) \) is a prime ideal.

**Proof.**

1. Let \( X \) be irreducible let \( f : X \rightarrow Y \) be continuous. Suppose \( f(X) = Y_1 \cup Y_2 \) for closed subsets \( Y_1, Y_2 \subseteq f(X) \). Then \( X = f^{-1}(Y_1) \cup f^{-1}(Y_2) \). Since \( f \) is continuous, \( f^{-1}(Y_1), f^{-1}(Y_2) \) are closed in \( X \) so we have a contradiction. Hence \( f(X) \) is irreducible.

2. Suppose \( X \) is irreducible and let \( f, g \in K[T_1, \ldots, T_m] \) such that \( fg \in \mathcal{I}(X) \). Then for all \( x \in X, f(x) = 0 \) or \( g(x) = 0 \) so \( X = (X \cap \mathcal{V}(I_f)) \cup (X \cap \mathcal{V}(I_g)) \) where \( I_f = (f) \) and \( I_g = (g) \). Since \( X \) is irreducible, \( X \subseteq \mathcal{V}(I_f) \) or \( X \subseteq \mathcal{V}(I_g) \) which implies \( f \in \mathcal{I}(X) \) or \( g \in \mathcal{I}(X) \). Hence \( \mathcal{I}(X) \) is prime.

Conversely, suppose \( \mathcal{I}(X) \) is a prime ideal and assume \( X = \mathcal{V}(I_1) \cup \mathcal{V}(I_2) \) for some ideals \( I_1, I_2 \). Suppose \( X \neq \mathcal{V}(I_1) \). By Lemma 2.1.1 iii), \( X = \mathcal{V}(I_1 \cap I_2) \) so there exists \( f \in I_1 \) such that \( f \notin \mathcal{I}(X) \). Now, for all \( g \in I_2, fg \in \mathcal{I}(X) \). Hence \( I_2 \subseteq \mathcal{I}(X) \) since \( \mathcal{I}(X) \) is prime. Therefore \( X = \mathcal{V}(I_2) \) so \( X \) is irreducible. \( \Box \)

Note that if \( X \) is disconnected then \( X = U_1 \cup U_2 \) for disjoint, nonempty open sets \( U_1, U_2 \) so \( X = \overline{U_1} \cup \overline{U_2} \). Now \( U_1 = \overline{U_1} \) which is closed so \( U_1 = \overline{U_1} \). Since \( U_1 \) and \( U_2 \) are disjoint, nonempty open sets, \( \overline{U_1} \neq X \). Similarly, \( \overline{U_2} \neq X \). Thus \( \overline{U_1} \) and \( \overline{U_2} \) are proper subsets of \( X \). Hence \( X \) is reducible. Therefore, if \( X \) is irreducible, \( X \) is connected.

**Definition 2.1.5.** For an (affine) algebraic set \( X \subseteq V \), the affine algebra of \( X \) is
the quotient algebra $K[X] = K[T_1, \ldots, T_m]/I(X)$.

Note that the affine algebra of an algebraic set $X$ is finitely generated and 0 is the only nilpotent element.

Let $I$ be an ideal of $K[X]$ and $Y \subseteq X$. Define $V_X(I) = \{x \in X \mid f(x) = 0 \text{ for all } f \in I\}$ and $J_X(Y) = \{f \in K[X] \mid f(y) = 0 \text{ for all } y \in Y\}$. There is an abuse of notation here. For $f \in K[X]$, $f(x) = 0$ means we choose a representative of $f + I(X)$ then evaluate at $x$. This is well defined since for all $g \in J(X)$, $g(x) = 0$ for all $x \in X$.

**Definition 2.1.6.** The principal open sets of $X$ are the open sets $D(f) = \{x \in X \mid f(x) \neq 0\}$ where $f \in K[X]$.

Note that every closed set in $X$ is the intersection of sets of the form $V((f))$. By taking complements, we see that the principal open sets form a basis for the topology on $X$.

**Definition 2.1.7.** Let $x \in X$ and $f$ be a $K$-valued function such that $f$ is defined on a neighbourhood $U$ of $x$. We say $f$ is regular at $x$ if there exists $g, h \in K[X]$ and some open subset $U'$ of $U \cap D(f)$ such that $f(y) = g(y)h(y)^{-1}$ for all $y \in U'$.

If $f$ is defined on an open set $U \subseteq X$, we say $f$ is regular at every $x \in U$. We denote the set of regular functions on $U$ by $O_X(U)$. 44
In this case, $\mathcal{O}_X$ acts as a function from open sets in $X$ to $K$-algebras.

**Definition 2.1.8.** We say $\mathcal{O}_X$ is a sheaf of $K$-valued functions if $\mathcal{O}_X$ satisfies the following properties.

1. For nonempty open sets $U \subseteq U'$, $f \in \mathcal{O}_X(U')$ implies $f|_U \in \mathcal{O}_X(U)$.

2. Let $U$ be open and $\{U_i\}_{i \in I}$ be an open covering of $U$. If $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ for functions $f_i \in \mathcal{O}_X(U_i)$, $f_j \in \mathcal{O}_X(U_j)$ and all $i,j \in I$ then there exists $f \in \mathcal{O}_X(U)$ such that $f|_{U_i} = f_i$ for all $i \in I$.

In this case, we say $(X, \mathcal{O}_X)$ is a ringed space.

It is not difficult to check that $\mathcal{O}_X$ is a sheaf for an affine set $X$.

**Definition 2.1.9.** For any subset $Y \subseteq X$, we endow $Y$ with the subspace topology. Then we define an induced ringed space $(Y, \mathcal{O}_Y)$ in the following way. Suppose $U$ is open in $Y$. Then $f : U \to \mathbb{C}$ belongs to $\mathcal{O}_Y(U)$ if there exists an open covering $\{U_i\}_{i \in I}$ of $U$ in $X$ and, for each $i \in I$, there exists $f_i \in \mathcal{O}_X(U_i)$ such that $f_i|_{U_i \cap U} = f|_{U_i \cap U}$.

It is also not difficult to check that $\mathcal{O}_Y$ is a sheaf.

**Definition 2.1.10.** The pair $(X, \mathcal{O}_X)$ is called an affine algebraic variety over $K$. 

45
Let $X$ be an affine algebraic set. We will describe the sheaf $\mathcal{O}_X$. For any $f \in K[X]$, we have $\mathcal{O}_X(D(f)) = \{gf^n \mid g \in K[X], n \in \mathbb{N}\}$ ([5], Section, 15.5, Proposition 57). Let $f, g \in K[X]$. Then

\begin{align*}
\mathcal{O}_X(D(f) \cup D(g)) \\
= \{kh^{-1} \mid h, k \in K[X], h(x) \neq 0 \text{ for all } x \in D(f) \cup D(g)\} \\
= \{kh^{-1} \mid h, k \in K[X], h(x) \neq 0 \text{ for all } x \in D(f) \text{ and for all } x \in D(g)\} \\
= \mathcal{O}_X(D(f)) \cap \mathcal{O}_X(D(g)).
\end{align*}

We also have

\begin{align*}
D(f) \cap D(g) &= \{x \in X \mid f(x) \neq 0 \text{ and } g(x) \neq 0\} \\
&= \{x \in X \mid f(x)g(x) \neq 0\} \\
&= D(fg)
\end{align*}

which gives

\begin{align*}
\mathcal{O}_X(D(f) \cap D(g)) &= \{kh^{-1} \mid h, k \in K[X], h(x) \neq 0 \text{ for all } x \in D(f) \cap D(g)\} \\
&= \{kh^{-1} \mid h, k \in K[X], h(x) \neq 0 \text{ for all } x \in D(fg)\} \\
&= \mathcal{O}_X(D(fg)).
\end{align*}

Since the principal open sets form a basis for the Zariski topology on $X$, we have completely determined $\mathcal{O}_X$. 

46
Now
\[ D(1) = \{ x \in X \mid 1 \neq 0 \} = X \]
so
\[ \mathcal{O}_X(X) = \mathcal{O}_X(D(1)) = \{ g \mid g \in K[X] \} = K[X]. \]

**Definition 2.1.11.** Let \( \phi: X \to Y \) be a continuous map of affine varieties and for \( V \) open in \( Y \) define \( \phi_V^*: \mathcal{O}_Y(V) \to \mathcal{O}_X(\phi^{-1}(V)) \) by \( \phi_V^*(f) = f \circ \phi|_{\phi^{-1}(V)}. \) Then \( \phi \) is a morphism of affine algebraic varieties if for all \( V \) open in \( Y \), \( \phi_V^*(\mathcal{O}_Y(V)) \hookrightarrow \mathcal{O}_X(\phi^{-1}(V)) \).

In general, a morphism \( \phi: X \to Y \) where \( X \subseteq K^m \), \( Y \subseteq K^l \) is of the form \( \phi(x) = (\psi_1(x), \ldots, \psi_l(x)), \psi_i \in K[X] \) for all \( 1 \leq i \leq l \) ([8], Section 1.5, page 10).

### 2.2 Linear Algebraic Groups

Once again, let \( K \) be an algebraically closed field and \( V = K^m \). Our goal for this section is to define a linear algebraic group. A linear algebraic group is essentially an affine variety with a group structure where multiplication and inversion are polynomial maps. We will focus on two types of linear algebraic group; reductive groups and semi-simple groups. The section is concluded with several examples.

**Definition 2.2.1.** Suppose \( G \) is an affine algebraic variety with a group structure
given by the morphisms $\mu: G \times G \rightarrow G$, $\mu(x, y) = xy$ and $i: G \rightarrow G$, $i(x) = x^{-1}$.

Then we say $G$ is a linear algebraic group.

From this point onwards, $G$ is a linear algebraic group. Note that the topology on $G$ is the Zariski topology.

We will look at some simple examples of a linear algebraic groups. In general, we will consider subgroups of $GL_n$ over an arbitrary subfield of an algebraically closed field.

**Example 2.2.2.** Consider $G = K$ as an additive group. We have already shown that $G$ is an affine variety. Then $G$ is certainly a linear algebraic group with $\mu(x, y) = x + y$ and $i(x) = -x$ for all $x, y \in K$ since $\mu$ and $i$ are both morphisms.

In fact, the following theorem shows that we need only be concerned with subgroups of $GL_n$ where $\mu$ is the usual matrix multiplication and $i$ is the usual matrix inversion.

**Theorem 2.2.3.** Let $G$ be a linear algebraic group over $K$. Then $G$ is isomorphic to a closed subgroup of $GL_n$ for some $n \geq 1$.

For a proof of Theorem 2.2.3, see ([19], Theorem 2.3.7 (i)).

We assume that $G$ is a closed subgroup of $GL_n$ for some $n \geq 1$ from this point onwards.
Now, we say an element $g \in G$ is unipotent if $g - I$ is nilpotent; i.e. if $(g - I)^t = 0$ for some positive integer $t$. We say $g$ is semi-simple if $g$ is diagonalizable. We may decompose $g$ with the Jordan decomposition ([19], Theorem 2.4.8 (i), (iii)). The Jordan decomposition is the unique decomposition $g = g_s g_u = g_u g_s$ where $g_s$ is semi-simple and $g_u$ is unipotent. We say a subgroup of $G$ is unipotent if all of its elements are unipotent.

**Definition 2.2.4.** The unipotent radical of a group $G$ is the maximal, closed, connected, normal, unipotent subgroup and is denoted $R_u(G)$. A linear algebraic group $G$ is reductive if $R_u(G)$ is trivial.

**Definition 2.2.5.** The radical of $G$ is the maximal, closed, connected, normal, solvable subgroup and is denoted $R(G)$. A linear algebraic group $G$ is semi-simple if $R(G)$ is trivial.

**Definition 2.2.6.** If $G$ has no proper, connected, closed, normal subgroup then we say $G$ is quasi-simple.

Note that by ([19], Corollary 2.4.13), semi-simple groups are reductive. We begin by looking at semi-simple matrix groups over $K$. However, we will consider reductive groups and quasi-simple groups at a later point.

**Example 2.2.7.** Let $M_n$ be the set of an $n \times n$ matrices over $K$. Then $K[M_n] =$
Let \( T \) denote the determinant of \( A \in M_n \). Then \( \det \) is a polynomial function so it is certainly regular on \( M_n \). Let \( G \) be the general linear group over \( K \), \( GL_n = \{ A \in M_n \mid \det(A) \neq 0 \} \) with the usual matrix multiplication. Now, \( G \) is the principal open set given by \( \det \neq 0 \) in \( M_n \). We have

\[
K[G] \cong K[T_{ij}, U_{1 \leq i,j \leq n}] / (U \det - 1) \cong K[T_{ij}, \det^{-1}]_{1 \leq i,j \leq n}.
\]

In the discussion at the end of Section 2.1, we described the sheaf on \( M_n = K^{n^2} \). We also showed that the functions that are regular on \( D(f) \cap D(g) \) are the functions which are regular on \( D(fg) \) for any \( f, g \in K[T_{ij}]_{1 \leq i,j \leq n} \). Therefore, the functions which are regular on \( D(f) \cap G \) are \( \{ \frac{g}{f^{t\det}} \mid g \in K[T_{ij}]_{1 \leq i,j \leq n}, t \in \mathbb{N} \} \).

Thus, after identifying \( K[G] \) with \( K[T_{ij}, \det^{-1}]_{1 \leq i,j \leq n} \), we have that for any \( f \in K[G] \),

\( \mathcal{O}_G(D(f)) = \{ \frac{g}{f^t} \mid g \in K[G], t \in \mathbb{N} \} \).

Since matrix multiplication and inversion are polynomial maps in \( T_{ij} \) and \( \det \), they are morphisms. Then \( G \) is an affine algebraic variety so \( G \) is a linear algebraic group.

Now \( K[T_{ij}, U]_{1 \leq i,j \leq n} \) is a unique factorization domain and \( U \det - 1 \) is irreducible so \( (U \det - 1) \) is a prime ideal. Hence \( G \) is irreducible by Lemma 2.1.4, 2. By taking conjugates of diagonal matrices, it is not difficult to show that the only normal subgroups of \( G \) are the groups of the scalar matrices. However, the only unipotent scalar matrix is the identity matrix \( I \). Hence \( R_u(G) = \{ I \} \) and \( G \) is reductive.
However, $G$ is not semi-simple since the group of scalar matrices is isomorphic to $GL_1$ and forms a closed, connected, normal, solvable subgroup of $G$.

As a special case, consider $G = GL_1 = K^\times$ with the usual multiplication. Then

$$K[G] = K[T,U]/(UT - 1) \cong K[T,T^{-1}].$$

Then $G$ is denoted by $G_m$. The results for $GL_n$ certainly hold for $G$ so $G$ is an irreducible reductive group.

Now, let $G$ be a closed subgroup of $GL_n$ over $K$. Consider the inclusion $G \hookrightarrow GL_n$. The restriction of multiplication and inversion from $GL_n$ to $G$ are morphisms since they are polynomial maps. Since $G$ is closed in $GL_n$, we have $G = \bigcap_{\alpha \in A} \mathcal{V}(f_\alpha)$ for some set $\{f_\alpha \in K[GL_n] \mid \alpha \in A\}$. Then $I(GL_n) \subseteq I(G)$ which implies $K[G]$ is a quotient of $K[GL_n]$. We define an induced ringed space $(G, \mathcal{O}_G) = (G, \mathcal{O}_{GL_n}|_G)$ of $(GL_n, \mathcal{O}_{GL_n})$ so $G$ is an affine algebraic variety. Hence $G$ is a linear algebraic group.

The sheaf on $G$ is characterized in the same way as was done for $M_n$ and $GL_n$. We can write $\mathcal{O}_G(D(f))$ for any $f \in K[G]$ and determine $\mathcal{O}_G(U)$ for an open set $U$ but writing $U$ as a union and intersection of principal open sets.

**Example 2.2.8.** Let $G$ be the special linear group $SL_n = \{A \in GL_n \mid \det(A) = 1\}$. We have $K[G] = K[T_{ij}]_{1 \leq i,j \leq n}/(\det - 1)$. Now $G$ is a subgroup of $GL_n$ and $G$ is closed since $G = \mathcal{V}(\det - 1)$ in $GL_n$. Thus, by the previous discussion, $G$ is a linear algebraic group.
Now \((\det - 1)\) is a prime ideal so \(G\) is irreducible by Lemma 2.1.4, 2. As with \(GL_n\), it is not difficult to show that the only normal subgroups are the subgroups of scalar matrices. These are all finite groups in \(SL_n\) so they are not connected. Hence \(R(G) = \{I\}\) so \(G\) is semi-simple.

**Example 2.2.9.** Let \(G\) be the non-singular diagonal matrices \(D_n = \{A \in GL_n \mid A_{ij} = 0 \text{ for all } i \neq j\}\). We have

\[
K[G] = K[T_{ij}, U]_{1 \leq i,j \leq n}/(T_{ij}, U \det - 1)_{1 \leq i \neq j \leq n} \cong K[T_{ii}, T^{-1}_{ii}]_{1 \leq i \leq n}.
\]

Now \(G\) is a subgroup of \(GL_n\) and \(G\) is closed since \(G = \mathcal{V}(T_{ij} \mid i \neq j) \cap \mathcal{V}(U \det - 1)\) in \(GL_n\). Hence \(G\) is a linear algebraic group. Moreover, \(K[G]\) is a unique factorization domain and \((T_{ij}, U \det - 1 \mid 1 \leq i \neq j \leq n)\) is irreducible so \((T_{ij}, U \det - 1 \mid 1 \leq i \neq j \leq n)\) is prime. Therefore \(G\) is irreducible. We also have that \(R_u(G) = \{I\}\) since \(I\) is the only unipotent matrix so \(G\) is reductive. Since \(D_n \cong G_m^n\) is abelian, it is solvable. Thus, \(D_n\) is not semi-simple.

### 2.3 Root Data

Let \(G\) be a linear algebraic group over an algebraically closed field \(K\). We will outline the theory required to define a root datum of \(G\) without any proof. We will then show the computations explicitly for \(GL_n\). In general, we decompose \(G\) using a maximal torus which is a subgroup of \(G\). Tori are isomorphic to diagonal matrix
groups. This theory is analogous to the theory of Lie groups and Lie algebras ([8], Chapter 9-10, [19], Chapter 4). We then state the correspondence between root data and connected, reductive linear algebraic groups. Namely, the number of groups corresponding to a given root datum with a fixed root system is determined by a finite quotient of groups which comes from the root datum. We call this group the fundamental group. We will also show that each root datum naturally corresponds to a dual root datum. Thus, connected, reductive, linear algebraic groups correspond to a dual group which arises from the dual root datum.

**Definition 2.3.1.** Let $\chi: G \rightarrow G_m$ be a homomorphism of algebraic groups. We say $\chi$ is a rational character of $G$ and we denote the set of rational characters by $X^*(G)$.

Let $\lambda: G_m \rightarrow G$ be a homomorphism of algebraic groups. We say $\lambda$ is a cocharacter of $G$ and we denote the set of cocharacters by $X_*(G)$.

Now $X^*(G)$ is an abelian group since $\chi \in X^*(G)$ is a homomorphism and $G_m$ is abelian. By contrast, $X_*(G)$ is only an abelian group if $G$ is an abelian group.

**Example 2.3.2.** Let $G = G_m$ and consider $\chi: G \rightarrow G_m$ defined by $\chi(a) = a$ for all $a \in G$. Now $\chi$ is a morphism from $G$ to $G_m$. Moreover, $\chi$ is a homomorphism of linear algebraic groups so $\chi$ is certainly a rational character of $G$. The integers act on the rational characters by $t \cdot \chi(a) = \chi(a)^t = a^t$ for all $t \in \mathbb{Z}$. For any $t$, 53
\( t \cdot \chi \in X^*(G) \) and we write \( t \cdot \chi = \chi^t \). Let \( \eta \in X^*(G) \). Then \( \eta \) is a morphism so, as shown in Example 2.2.7, \( \eta \in K[T, T^{-1}] \). Thus \( \eta = \sum_{i=0}^{s} a_i T^{t_i} \) for some \( s \geq 0 \), \( t_i \in \mathbb{Z} \). This implies that \( \eta = \sum_{i=0}^{s} a_i \chi^{t_i} \). By the linear independence of characters ([5], Theorem 7, Chapter 14), \( \eta = \chi^j \) for some \( j \). Therefore \( X^*(G) = \{ \chi^t \mid t \in \mathbb{Z} \} \).

Since \( G = G_m \), we also have \( X_*(G) = X^*(G) \).

**Example 2.3.3.** Let \( G = D_n \) be a diagonal group. Then define \( \chi_i : G \to G_m \) by \( \chi_i(A) = x_i \) for all \( A = \text{diag}(a_1, \ldots, a_n) \in G \). It is not difficult to see that \( \chi_i \) is a character of \( G \) and

\[
X^*(G) = \langle \chi_i \mid 1 \leq i \leq n \rangle = \left\{ \prod_{i=1}^{n} \chi_i^{t_i} \mid t_i \in \mathbb{Z} \right\}.
\]

Define \( \lambda_i : G_m \to G \) by \( \lambda_i(a) = \text{diag}(1, \ldots, 1, a, 1, \ldots, 1) \) where \( a \) is in the \( i^{th} \) entry.

It is not difficult to see that \( \lambda_i \) is a cocharacter and

\[
X_*(G) = \langle \lambda_i \mid 1 \leq i \leq n \rangle = \left\{ \prod_{i=1}^{n} \lambda_i^{t_i} \mid t_i \in \mathbb{Z} \right\}.
\]

It is also a simple exercise to show that mapping \( \prod_{i=1}^{n} \chi_i^{t_i} \) to \((t_1, \ldots, t_n) \in \mathbb{Z}^n \) is an isomorphism of groups so \( X^*(G) \cong \mathbb{Z}^n \). Similarly \( X_*(G) \cong \mathbb{Z}^n \).

**Definition 2.3.4.** We say that a linear algebraic group \( G \) is diagonalizable if \( G \) is isomorphic to a closed subgroup of \( D_n \) for some \( n \). We say \( G \) is an algebraic torus if \( G \cong D_n \) for some \( n \).
As with the theory of Lie groups and Lie algebras, we can decompose $G$ using a maximal torus $T$. The analogy extends further since the decomposition depends on how $G$ acts on a given vector space (its Lie algebra) under the adjoint representation $Ad$ ([8], page 66). The decomposition corresponds to roots.

We can now define the root datum of $G$. A root datum encodes the structure of $G$ via the roots and rational characters of $G$ with respect to a maximal torus $T$. In fact, we will see that isomorphism classes of root data are in bijection with isomorphism classes of connected, reductive linear algebraic groups.

**Definition 2.3.5.** A root datum is a quadruple $\Psi = (X, R, X^\vee, R^\vee)$ that satisfies the following. Both $X$ and $X^\vee$ are free abelian groups of finite rank with a perfect pairing $<,>: X \times X^\vee \rightarrow \mathbb{Z}$. More specifically, there is a bijection from $X$ to $X^\vee$ denoted by $\alpha \mapsto \alpha^\vee$ for all $\alpha \in X$ and $<,>$ is a nondegenerate bilinear form. Furthermore, we have finite subsets $R$ and $R^\vee$ of $X$ and $X^\vee$ respectively such that the map $\alpha \mapsto \alpha^\vee$ for all $\alpha \in R$ is a bijection from $R$ to $R^\vee$.

For all $\alpha \in R$, we define endomorphisms $s_\alpha$ and $s_\alpha^\vee$ of $X$ and $X^\vee$ respectively by $s_\alpha(x) = x - <x, \alpha^\vee> \alpha$ and $s_\alpha^\vee(y) = y - <\alpha, y> \alpha^\vee$ for all $x \in X$, $y \in X^\vee$. Then we impose the following condition. If $\alpha \in R$ then $<\alpha, \alpha^\vee> = 2$ and $s_\alpha(R) = R$, $s_\alpha^\vee(R^\vee) = R^\vee$.

With the notation above, we define a root system.
Definition 2.3.6. Let $E$ be a real vector space. Then we say $R$ is a root system of $E$ if the following conditions are satisfied.

1) $R$ is finite, $0 \notin R$ and $E = \text{span}\{R\}$.

2) For all $\alpha \in R$, there exists $\alpha^\vee \in R^\vee$ such that $<\alpha, \alpha^\vee> = 2$.

3) There exists a reflection $s_\alpha$ of $\alpha$ that leaves $R$ stable.

4) For all $\alpha \in R$, $\alpha^\vee(R) \subseteq \mathbb{Z}$.

In this case, the elements of $R$ are called roots.

Let $\Psi = (X, R, X^\vee, R^\vee)$ be a root datum. Let $Q = \text{span}_{\mathbb{Z}}\{R\}$ in $X$ and let $E = R \otimes_{\mathbb{Z}} Q$. By construction, $R$ is a root system of $E$. For each root $\alpha \in R$, we call $\alpha^\vee$ a coroot.

We can see that $s_\alpha$ is a reflection in $E$ which sends $\alpha$ to $-\alpha$. Then it is clear that $s_\alpha^\vee$ is a reflection in $R \otimes_{\mathbb{Z}} Q^\vee$ which sends $\alpha^\vee$ to $-\alpha^\vee$.

Recall the notions of a semi-simple group and a quasi-simple group from Definition 2.2.5 and Definition 2.2.6 respectively. Most of our work later in this thesis is restricted to semi-simple, quasi-simple groups. We can classify semi-simple, quasi-simple groups in terms of their root systems. A semi-simple group is quasi-simple if and only if its root system is not a nontrivial direct sum ([8], Theorem 27.5c).
Example 2.3.7. Let $G = GL_n(K)$. We will define a root datum $\Psi(G,T)$ of $G$ with respect to a maximal torus $T$. Our first step is to determine a maximal torus of $G$. Let $T = \{ \text{diag}(x_1, \ldots, x_n) \mid x_i \in K^\times \}$. The map $T \to D_n$ given by $\text{diag}(x_1, \ldots, x_n) \mapsto \text{diag}(x_1, \ldots, x_n)$ is certainly a group isomorphism and a morphism of varieties. Thus $T \cong D_n$ and $T$ is a torus. Suppose $T \leq S$ for some torus $S$. Then $S \cong D_m$ for some $m \geq n$ and $S$ is abelian. Therefore $S \subseteq Z_G(T)$. We will show $Z_G(T) = T$. Let $A \in Z_G(T)$. We have $AD = DA$ for all $D = \text{diag}(x_1, \ldots, x_n) \in T$. This implies $A_{ij}x_j = A_{ij}x_i$ for all $1 \leq i, j \leq n$. Choosing $x_i \neq x_j$ gives $A_{ij} = 0$ so $A$ is a diagonal matrix. Thus $A \in T$ so $Z_G(T) \subseteq T$. However, $T \subseteq Z_G(T)$. Hence $Z_G(T) = T$ and we must have $S = T$. Therefore $T$ is maximal.

Now let $X = X^*(T)$ and $X^\vee = X_*(T)$ which were determined in Example 2.3.3. For all $\lambda \in X^\vee$, $\chi \in X$, we have $\chi \circ \lambda \in X^*(G_m)$. Then for all $t, l \in \mathbb{Z}$ and $1 \leq i \neq j \leq n$, $\chi^t_i \circ \lambda^l_j(a) = 1$ and $\chi^t_i \circ \lambda^l_i(a) = a^{tl}$ for all $a \in G_m$. Thus we define a perfect pairing $\langle, \rangle : X \times X^\vee \to \mathbb{Z}$ by $\langle \chi, \lambda \rangle = k$ where $\chi \circ \lambda(a) = a^k$ for all $a \in G_m$.

Our goal is to decompose $G$ with respect to an action of the maximal abelian subgroup $T$. Since $G$ is contained in $\mathfrak{g} = M_n$, we consider the action of conjugation on $\mathfrak{g}$ by elements of $G$. This is the adjoint representation, denoted by $\text{Ad}$. Let $E_{ij}$ be the $n \times n$ matrix with 1 in the $ij^{th}$ entry and 0 everywhere else. Then $\mathfrak{g} = ...$
span\(_K\{E_{ij} \mid 1 \leq i, j \leq n\}\). We can decompose \(\mathfrak{g}\) into a direct sum of subspaces \(\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid \text{Ad}(h)(x) = \alpha(h)x \text{ for all } h \in T\}\) where \(\alpha\) is a linear map from \(T\) to \(K\). We say \(\mathfrak{g}_\alpha\) is a root space and \(\alpha\) is a root when \(\mathfrak{g}_\alpha \neq \{0\}\) and \(\alpha \neq 0\). Moreover, \(\mathfrak{g}_0 = t\) where \(t = \langle E_{ii} \mid 1 \leq i \leq n\rangle\). Thus \(\mathfrak{g} = t \oplus (\oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha)\) where \(\Phi\) is the set of roots. Then we take \(R = \Phi\).

Carrying out the computations outlined above gives the following. Let the diagonal matrix \(h = \text{diag}(x_1, \ldots, x_n)\) be an arbitrary element of \(T\). Then for \(i \neq j\), we have \(\text{Ad}(h)(E_{ij}) = x_ix_j^{-1}\) which implies \(\alpha_{ij}\) defined by \(\alpha_{ij}(h) = x_ix_j^{-1}\) is a root and \(\mathfrak{g}_{\alpha_{ij}} = \langle E_{ij}\rangle\). Therefore, the set of roots is \(R = \{\alpha_{ij} \mid 1 \leq i \neq j \leq n\}\). Note that \(\alpha_{ij} = \chi_i\chi_j^{-1}\) so \(R = \{\chi_i\chi_j^{-1} \mid 1 \leq i \neq j \leq n\}\) which is certainly a finite subset of \(X\).

Now, we make use of the condition \(\langle \alpha, \alpha^\vee \rangle = 2\) for all \(\alpha \in R\) to determine \(R^\vee\). Recall that, \(\langle \prod_{i=1}^n \chi_i^{t_i}, \prod_{i=1}^n \lambda_i^{l_i} \rangle = \sum_{i=1}^n t_il_i\) for any \(t_i, l_i \in \mathbb{Z}\). Then

\[
2 = \langle \alpha_{ij}, \alpha_{ij}^\vee \rangle = \langle \chi_i\chi_j^{-1}, \prod_{k=1}^n \lambda_k^{l_k} \rangle = l_i - l_j
\]

for some \(l_k \in \mathbb{Z}\). Taking \(l_i = 1, l_j = -1\) and \(l_k = 0\) for \(k \neq i, j\) satisfies the equation so we set \(\alpha_{ij}^\vee = \lambda_i\lambda_j^{-1}\). Hence \(R^\vee = \{\lambda_i\lambda_j^{-1} \mid 1 \leq i \neq j \leq n\}\). Notice that \(R\) is a root system of \(\mathbb{R} \otimes \mathbb{Z} \text{span}_\mathbb{Z}\{R\}\) and \(R^\vee\) is a root system \(\mathbb{R} \otimes \mathbb{Z} \text{span}_\mathbb{Z}\{R^\vee\}\).

There is a general approach to determining the root datum \(\Psi(G,T)\) of \(G\) with respect to \(T\) where \(G\) is not necessarily \(GL_n\). As in Example 2.3.7, \(X = X^*(T)\) and \(X^\vee = X_*(T)\). Since \(\chi \circ \lambda \in X^*(G_m)\) for all \(\lambda \in X^\vee, \chi \in X\), we define a perfect
pairing $\langle \cdot, \cdot \rangle : X \times X^\vee \to \mathbb{Z}$ by $\langle \chi, \lambda \rangle = k$ where $\chi \circ \lambda (a) = a^k$ for all $a \in G_m$.

To determine $R$ and $R^\vee$ we proceed as follows. We make use of the notion of a Lie algebra of a group. This is essentially the linearization of a Lie group. Let $\mathfrak{g}$ be the Lie algebra of $G$ and let $\mathfrak{t}$ be the Lie algebra of $T$. We decompose $\mathfrak{g}$ with respect to the adjoint action of $T$ on $\mathfrak{g}$. Alternatively, this action corresponds to an action of $\mathfrak{t}$ on $\mathfrak{g}$ given by $h \cdot x = [h, x]$ where $[h, x] = hx - xh$ is called the Lie bracket on $\mathfrak{g}$. As in Example 2.3.7, we can obtain a root space decomposition of $\mathfrak{g}$ and $R$ corresponds to the set of linear maps $\{ \alpha \mid \alpha \neq 0 \text{ and } \mathfrak{g}_\alpha \neq \{0\} \}$ from $\mathfrak{t}$ to $K$. The correspondence is given by identifying each root $\alpha$ with a rational character. Lastly, $R^\vee$ is given by imposing $2 = \langle \alpha, \alpha^\vee \rangle$ and solving the resulting equations.

**Example 2.3.8.** Let $G = SL_2$ defined over $K$. Then $T = \{ \text{diag}(a, a^{-1}) \mid a \in K^\times \}$ is a maximal torus of $G$. Let $\Psi = (X, R, X^\vee, R^\vee)$ be the root datum of $G$ obtained as above. Thus $X = \{ \chi^t \mid t \in \mathbb{Z} \}$ where $\chi(\text{diag}(a, a^{-1})) = a$ and $X^\vee = \{ \lambda^t \mid t \in \mathbb{Z} \}$ where $\lambda(a) = \text{diag}(a, a^{-1})$. The Lie algebras of $G$ and $T$ are $\mathfrak{g} = \{ A \in \mathfrak{gl}_2 \mid \text{Tr}(A) = 0 \}$ and $\mathfrak{t} = \{ \text{diag}(a, -a) \mid a \in K \}$. It is simple to show that $R = \{ \pm \alpha \}$ where $\alpha(\text{diag}(a, -a)) = 2a$. Then, as a subset of $X$, $R = \{ \chi^{\pm 2} \}$. Solving $\langle \chi^2, \lambda^t \rangle = 2$ gives $t = 1$ so $R^\vee = \{ \lambda^{\pm 1} \}$.

**Example 2.3.9.** Let $G$ be the projective general linear group $PGL_2$ defined over $K$. Let $Z = \{ xI \mid x \in K^\times \}$ be the centre of $GL_2$ and let $T = \{ \text{diag}(a, b) \mid a, b \in K^\times \}$. 59
Then $T$ is a maximal torus of $GL_2$. Now $Z$ is a subgroup of $T$ so $T' = T/Z = \{ \text{diag}(a,1)Z \mid a \in K^\times \}$ is a maximal torus of $G$. We have the short exact sequence

$$1 \rightarrow Z \rightarrow T \rightarrow T' \rightarrow 1$$

so, by Corollary 8.3 in [1], we get another short exact sequence

$$1 \rightarrow X^*(T') \rightarrow X^*(T) \xrightarrow{\chi \mapsto \chi|_Z} X^*(Z) \rightarrow 1.$$

After identifying $X^*(T')$ with its image in $X^*(T)$, we have $X^*(T)/X^*(T') \cong X^*(Z)$ and $\chi$ is trivial on $Z$ for all $\chi \in X^*(T')$. Hence $X^*(T') = \{ \chi_1^t \chi_2^{-t} \mid t \in \mathbb{Z} \}$ where $\chi_1, \chi_2$ are from Example 2.3.7. Since $Z = \{ xI \mid x \in K^\times \}$, it is not difficult to see that $X^*(Z) \cong \mathbb{Z}$ where $X^*(Z) = \text{Hom}(Z, G_m)$. Using notation from Example 2.3.7 again, we see $\lambda_1 = \lambda_2^{-1}$ modulo $Z$ so

$$X_*(T') = \langle \lambda_1, \lambda_2 \rangle / \langle \lambda_1 \lambda_2 \rangle \cong \{ \lambda_1^t \mid t \in \mathbb{Z} \} \cong X_*(T).$$

Note that there is a conflict of notation with $\langle, \rangle$. In this case, we use it to denote the group generated by $\lambda_1$ and $\lambda_2$. It will be clear when $\langle, \rangle$ denotes the pairing from Definition 2.3.5.

Now, Let $\Psi = (X, R, X^\vee, R^\vee)$ be the root datum of $G$. Then $X = X^*(T')$ and $X^\vee = X_*(T')$. The Lie algebra $\mathfrak{g}$ of $G$ is equal to the Lie algebra of $GL_2$ modulo the scalar matrices. This is isomorphic to the Lie algebra of $SL_2$. From Example 2.3.7, $R = \{(\chi_1 \chi_2^{-1})^{\pm 1}\}$. Imposing the condition on $\langle, \rangle$ gives $R^\vee = \{ \lambda_1^{\pm 2} \lambda_1 \lambda_2 \}$.  

60
We will show that there is a bijective correspondence between isomorphism classes of connected, reductive, linear algebraic groups and isomorphism classes of root data. This result requires the notion of isomorphic root data.

**Definition 2.3.10.** Let \( \Psi = (X, R, X^\vee, R^\vee) \) and \( \Psi_1 = (X_1, R_1, X_1^\vee, R_1^\vee) \) be root data. Suppose there is an isomorphism from \( X_1 \) to \( X \) which sends \( R_1 \) to \( R \) and a dual isomorphism from \( \mathbb{Q} \otimes_{\mathbb{Z}} X^\vee \) to \( \mathbb{Q} \otimes_{\mathbb{Z}} X_1^\vee \) which sends \( R^\vee \) to \( R_1^\vee \). Then we say \( \Psi \) is isomorphic to \( \Psi_1 \) and write \( \Psi \cong \Psi_1 \).

We now discuss how isomorphisms of root data are given by isomorphisms of connected, reductive, linear algebraic groups that preserve the maximal tori.

**Definition 2.3.11.** Suppose \( \phi: G \to G_1 \) is a surjective homomorphism of connected, reductive, linear algebraic groups over \( K \). We say \( \phi \) is an isogeny if \( \ker \phi \) is finite.

Let \( \Psi(G, T) = (X, R, X^\vee, R^\vee) \) and \( \Psi(G_1, T_1) = (X_1, R_1, X_1^\vee, R_1^\vee) \) be root data of \( G \) and \( G_1 \) respectively. Suppose \( \phi: G \to G_1 \) is an isogeny which satisfies \( \phi(T) = T_1 \). Define \( f: X_1 \to X \) by \( f(\chi_1) = \chi_1 \circ \phi \) and \( f^\vee: X^\vee \to X_1^\vee \) by \( f^\vee(\lambda) = \phi \circ \lambda \) for all \( \chi_1 \in X_1 \) and for all \( \lambda \in X^\vee \). Since \( \phi \) is a homomorphism, \( f \) and \( f^\vee \) are
homomorphisms. Moreover, for all $\chi_1 \in X_1$, $\lambda \in X^\vee$, we have

$$a^{<f(\chi_1),\lambda>} = a^{<\chi_1 \circ \phi,\lambda>}$$

$$= (\chi_1 \circ \phi) \circ \lambda(a)$$

$$= \chi_1 \circ (\phi \circ \lambda)(a)$$

$$= a^{<\chi_1,\phi \circ \lambda>}$$

$$= a^{<\chi_1,f^\vee(\lambda)>}$$

for every $a \in K^\times$. This implies $<f(\chi_1),\lambda> = <\chi_1,f^\vee(\lambda)>$ for all $\chi_1 \in X_1$, $\lambda \in X^\vee$.

Now if $\phi$ is an isomorphism then $T \cong T_1$ and $f, f^\vee$ are isomorphisms. Then $\phi$ and $\phi^{-1}$ send subgroups corresponding to the roots of one group to the subgroups corresponding to the roots of the other group ([19], Section 9.6.1) so $\phi$ induces a bijection of $R_1$ onto $R$ and $R^\vee$ onto $R_1^\vee$. The induced bijections are $f$ and $f^\vee$. Hence $f$ and $f^\vee$ preserve the roots of $\Psi(G,T)$ and $\Psi(G_1,T_1)$. Therefore $f$ and $f^\vee$ are the desired isomorphisms so $\Psi(G,T) \cong \Psi(G_1,T_1)$. We can also obtain an isomorphism of connected, reductive, linear algebraic groups that preserve the maximal tori from an isomorphism of root data.

**Theorem 2.3.12.** Suppose $f : \Psi(G_1,T_1) \rightarrow \Psi(G,T)$ is an isomorphism of root data. Then there exists an isomorphism $\phi : G \rightarrow G_1$ of connected, reductive, linear
algebraic groups such that $\phi(T) = T_1$. Moreover, $f$ is the isomorphism of root data induced by $\phi$ and $\phi$ is unique up to conjugation by $T$.

For a proof of Theorem 2.3.12, see ([19], Theorem 9.6.2).

**Theorem 2.3.13.** Let $\Psi$ be a root datum. Then there exists a unique, connected, reductive, linear algebraic group $G$ over $K$ with maximal torus $T$ such that $\Psi$ is isomorphic to the root datum of $G$ with respect to $T$.

For a proof of Theorem 2.3.13, see ([19], Theorem 10.1.1).

This concludes the discussion showing that there is a bijective correspondence between isomorphism classes of connected, reductive, linear algebraic groups over $K$ and isomorphism classes of root data.

We will now introduce the concept of a dual group. For every root datum $\Psi = (X, R, X^\vee, R^\vee)$, there is a dual root datum $\Psi^\vee = (X^\vee, R^\vee, X, R)$. It is not difficult to check that $\Psi^\vee$ is a root datum. Hence, for a root datum $\Psi$ of $G$, the dual root datum $\Psi^\vee$ corresponds to a unique, connected, reductive, linear algebraic group.

**Definition 2.3.14.** Let $G$ be a connected, reductive, linear algebraic group with root datum $\Psi$. The dual group of $G$ is the unique, connected, reductive, linear algebraic group which corresponds to the dual root datum $\Psi^\vee$. The dual group of $G$ is denoted
Example 2.3.15. Let $G = GL_n$ defined over $K$ with maximal torus $T$ being the set of invertible diagonal matrices. We will show that the dual group of $G$ is $\hat{G} = G$. We determined the root datum $\Psi(X, R, X^\vee, R^\vee)$ of $G$ in Example 2.3.7. The root datum of $\hat{G}$ is $\Psi^\vee = (X^\vee, R^\vee, X, R)$. Using notation from Example 2.3.7, define $f : X^\vee \to X$ by $f(\lambda_i) = \chi_i$ for all $1 \leq i \leq n$. It is not difficult to see that $f$ is an isomorphism of groups that sends $R^\vee$ to $R$. Since $(X^\vee)^\vee = X$ and $(R^\vee)^\vee = R$, we take $f^\vee = f$ to be the dual isomorphism. Hence $\Psi \cong \Psi^\vee$. By Theorem 2.3.13, there is a unique, connected, reductive, linear algebraic group $\hat{G}$ with root datum $\Psi^\vee$. However, Theorem 2.3.12 gives that $\hat{G} \cong G$. Hence $G$ is its own dual group.

Example 2.3.16. Let $G = SL_2$ defined over $K$. We will show that the dual group of $G$ is $\hat{G} = PGL_2$. In Example 2.3.8, we determined the root datum $\Psi = (X, R, X^\vee, R^\vee)$ of $G$. We can express $\Psi$ in terms of the root datum of $GL_n$ which we determined in Example 2.3.7. Using the notation of Example 2.3.7 and Example 2.3.8, we identify $\chi$ with $\chi_1$ and $\chi^{-1}$ with $\chi_2$. Hence $X = \langle \chi_1, \chi_2 \rangle / \langle \chi_1 \chi_2 \rangle$. This gives $R = \{ (\chi_1 \chi_2^{-1})^{\pm 1} \langle \chi_1 \chi_2 \rangle \}$. Similarly, we identify $\lambda$ with $\lambda_1 \lambda_2^{-1}$. Thus $X^\vee = \langle \lambda_1 \lambda_2^{-1} \rangle$ and $R^\vee = \{(\lambda_1 \lambda_2^{-1})^{\pm 1}\}$.

We know that the root datum of $\hat{G}$ is given by $\Psi^\vee = (X^\vee, R^\vee, X, R)$. We also know the root datum $\Psi_1 = (X_1, R_1, X_1^\vee, R_1^\vee)$ of $PGL_2$ from Example 2.3.9. We will show
that $\Psi_1 \cong \Psi^\vee$. The isomorphism from Example 2.3.15 induces a homomorphism $f : X^\vee \longrightarrow X_1$ defined by $f(\lambda_1\lambda_2^{-1}) = \chi_1\chi_2^{-1}$. It is not difficult to see that $f$ is well-defined isomorphism of groups. It is also clear that $f$ sends $R^\vee$ to $R_1$. The dual isomorphism from Example 2.3.15 induces a homomorphism $f^\vee : X_1^\vee \longrightarrow X$ defined by $f^\vee(\lambda_i < \lambda_1\lambda_2 >) = \chi_i < \chi_1\chi_2 >$ for $i = 1, 2$. Hence $f^\vee$ is a well-defined isomorphism of groups that sends $R_1^\vee$ to $R$. Hence $\Psi^\vee \cong \Psi_1$. By Theorem 2.3.13, there is a unique, connected, reductive, linear algebraic group $\hat{G}$ with root datum $\Psi^\vee$. However, Theorem 2.3.12 gives that $\hat{G} \cong PGL_2$.

Theorem 2.3.13 describes the bijective correspondence between root data and connected, reductive, linear algebraic groups. The correspondence between root systems and connected, reductive, linear algebraic groups is not bijective. However, for certain root systems, there are only finitely many possibilities of corresponding connected, semi-simple, linear algebraic groups.

**Definition 2.3.17.** Let $\Psi = (X, R, X^\vee, R^\vee)$ be a root datum of $G$. We say $Q = \text{span}_\mathbb{Z}\{R\}$ is the root lattice of $R$ and $P = \{x \in \mathbb{R} \otimes_\mathbb{Z} Q \mid <x, R^\vee > \subseteq \mathbb{Z}\}$ is the weight lattice of $R$.

Note that $Q$ is a subgroup of $P$. Observe that

$$Q \subseteq X \subseteq P$$
and $P/Q$ depends only on $R$. The root systems that correspond to finitely many possibilities of corresponding connected, semi-simple linear algebraic groups are the root systems that satisfy $P/Q$ finite. The quotient group $P/Q$ is finite if an only if $G$ is semi-simple ([19], Proposition 8.1.8, (ii)).

**Definition 2.3.18.** The quotient group $P/Q$ is the fundamental group of $G$. If $G$ is semi-simple and $X = Q$ the we say $X$ is adjoint. If $G$ is semi-simple and $X = P$ we say $X$ is simply connected.

Fix a root datum $\Psi(G,T) = (X,R,X^\vee,R^\vee)$ of a semi-simple group $G$. In general, $Q \subseteq X \subseteq P$ so the finite number of intermediate lattices in $X$ are parametrized by subgroups of the fundamental group $P/Q$. Hence there are a finite number of semi-simple groups, whose root datum $\Psi$ is determined by $P/Q$.

**Example 2.3.19.** Let $G = SL_2$ defined over $K$ and recall that $G$ is semi-simple.

We determined the root datum $\Psi = (X,R,X^\vee,R^\vee)$ of $G$ in Example 2.3.8. Now

$$Q = \text{span}_\mathbb{Z}\{R\} = \langle \chi^2 \rangle \cong 2\mathbb{Z} \subseteq \mathbb{Z} \cong X$$
and

\[ P = \{ x \in \mathbb{R} \otimes_{\mathbb{Z}} Q \mid < x, \lambda^t > \in \mathbb{Z} \text{ for all } \lambda^t \in R^\vee \} \]
\[ = \{ \chi^k \mid < \chi^k, \lambda^t > \in \mathbb{Z}, t = \pm 1 \} \]
\[ = \{ \chi^k \mid \pm k \in \mathbb{Z} \} \]
\[ = < \chi > \]
\[ = X \]
\[ \cong \mathbb{Z}. \]

Hence \( G \) is simply connected and the fundamental group is \( P/Q \cong \mathbb{Z}/2\mathbb{Z} \).

**Example 2.3.20.** Let \( G = PGL_2 \) defined over \( K \). Similarly to \( SL_2 \), \( G \) is semi-simple. We determined the root datum \( \Psi = (X, R, X^\vee, R^\vee) \) of \( G \) in Example 2.3.9.

Hence

\[ Q = < \chi_1 \chi_2^{-1} > \cong \mathbb{Z} \cong X \]

and

\[ P = \{ x \in \mathbb{R} \otimes_{\mathbb{Z}} Q \mid < x, \lambda > \in \mathbb{Z} \text{ for all } \lambda \in R^\vee \} \]
\[ = \{ \chi_1^k \chi_2^{-k} \mid < \chi_1^k \chi_2^{-k}, \lambda^t > \in \mathbb{Z}, t = \pm 2 \} \]
\[ = \{ \chi_1^k \chi_2^{-k} \mid \pm k \in \frac{1}{2} \mathbb{Z} \} \]
\[ \cong \mathbb{Z}/2\mathbb{Z}. \]
We can see that the fundamental group $P/Q \cong \mathbb{Z}/2\mathbb{Z}$ is the same as the fundamental group of $SL_2$ and $G$ is adjoint. We expect the fundamental groups of $PGL_2$ and $SL_2$ to be the same since the root system of $PGL_2$ is isomorphic to the root system $SL_2$.

Examples 2.3.19 and 2.3.20 together with Example 2.3.16 showed a specific case where a group $G$ is simply connected and its dual group $\hat{G}$ is adjoint. This is true for all semi-simple groups $G$. Fix a root datum $(X, R, X^\vee, R^\vee)$ and recall that the pairing $<,>$ is a perfect pairing. Then we have $P \cong \text{Hom}(Q^\vee, \mathbb{Z})$ via the map $\chi \mapsto \langle \chi, \cdot \rangle$ for all $\chi \in P$. Similarly, $X \cong \text{Hom}(X^\vee, \mathbb{Z})$ via the map $\chi \mapsto \langle \chi, \cdot \rangle$ for all $\chi \in X$. Suppose $X = P$. This is true if and only if

$$X^\vee = \{ \lambda \in R \otimes_{\mathbb{Z}} Q^\vee \mid \langle X, \lambda \rangle \subseteq \mathbb{Z} \}$$

$$= \{ \lambda \in R \otimes_{\mathbb{Z}} Q^\vee \mid \langle P, \lambda \rangle \subseteq \mathbb{Z} \}$$

$$= Q^\vee.$$

Similarly, $X^\vee = P^\vee$ if and only if $X = Q$. Therefore $G$ is simply connected if and only if $\hat{G}$ is adjoint.

By definition, a maximal torus $T$ is isomorphic to $D_n \cong (K^\times)^n$. However, if $T$ is a maximal torus of an adjoint group, there is an isomorphism of $T$ to $(K^\times)^n$ which corresponds to the image of $T$ under a base of $R$. We will only require this result for
complex groups so we prove the following proposition only for complex groups.

**Proposition 2.3.21.** Let $G$ be adjoint group defined over $\mathbb{C}$. For every maximal torus $T$ of $G$, we have $T \cong (\mathbb{C}^\times)^m$ for some integer $m \geq 1$. Moreover, given a base $\Delta = \{\alpha_1, \ldots, \alpha_m\}$ of the roots $R$ and $t \in T$, an isomorphism is given by $t \mapsto (\alpha_1(t), \ldots, \alpha_m(t))$. Hence $\alpha_j$ picks out the $j^{\text{th}}$ coordinate of the image of $t$ in $(\mathbb{C}^\times)^m$.

**Proof.** Let $G$ be a semi-simple, adjoint, group with maximal torus $T$ and root datum $\Psi(G,T) = (X,R,X^\vee,R^\vee)$. Then $X = Q$ and $X^\vee = P^\vee$. First we show that $X^\vee \otimes_\mathbb{Z} \mathbb{C}^\times$ is isomorphic to $T$. Let $\Delta = \{\alpha_1, \ldots, \alpha_m\}$ be a base for $R$. Then $X = \text{span}_\mathbb{Z}\{\alpha_1, \ldots, \alpha_m\}$, there exists a set of coweights $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\} \subseteq P^\vee$ which satisfies $\langle \alpha_i, \bar{\omega}_j \rangle = \delta_{i,j}$ for all $1 \leq i, j \leq m$, and $X^\vee = \text{span}_\mathbb{Z}\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ ([2], Chapter VI, Section 1.10). Define $\phi: X^\vee \otimes_\mathbb{Z} \mathbb{C}^\times \to T$ by

$$\phi \left( \sum_{i=1}^{m} \bar{\omega}_i \otimes z_i \right) = \prod_{i=1}^{m} \bar{\omega}_i(z_i).$$

It is clear that $\phi$ is a well defined homomorphism.

Suppose $\sum_{i=1}^{m} \bar{\omega}_i \otimes z_i \in \ker \phi$; i.e.

$$\phi \left( \sum_{i=1}^{m} \bar{\omega}_i \otimes z_i \right) = \prod_{i=1}^{m} \bar{\omega}_i(z_i) = 1.$$

Then

$$\alpha_k \left( \prod_{i=1}^{m} \bar{\omega}_i(z_i) \right) = 1.$$
for all $\alpha_k \in \Delta$. This implies

$$1 = \alpha_k \left( \prod_{i=1}^{m} \bar{\omega}_i(z_i) \right) = \prod_{i=1}^{m} \alpha_k(\bar{\omega}_i(z_i)) = \prod_{i=1}^{m} z_i^{<\alpha_k,\bar{\omega}_i>} = z_k$$

for all $1 \leq k \leq m$. Thus

$$\ker \phi = \text{span}_\mathbb{Z}\{\bar{\omega} \otimes 1 \mid \bar{\omega} \in P^\vee\}$$

$$= \text{span}_\mathbb{Z}\{\bar{\omega} \otimes 1^0 \mid \bar{\omega} \in P^\vee\}$$

$$= \text{span}_\mathbb{Z}\{0 \cdot \bar{\omega} \otimes 1 \mid \bar{\omega} \in P^\vee\}$$

$$= \{0\}$$

so $\phi$ is injective.

Now suppose $t \in T$ and let $z_k = \alpha_k(t)$ for all $1 \leq k \leq m$. Then

$$\alpha_k \left( \phi \left( \sum_{i=1}^{m} \bar{\omega}_i \otimes z_i \right) t^{-1} \right) = \alpha_k \left( \prod_{i=1}^{m} \bar{\omega}_i(z_i) t^{-1} \right)$$

$$= \alpha_k \left( \prod_{i=1}^{m} \bar{\omega}_i(\alpha_i(t)) t^{-1} \right)$$

$$= \alpha_k(t) \alpha_k(t^{-1})$$

$$= 1$$

for all $1 \leq k \leq m$. 

70
As in Example 2.3.7, the root spaces \( g_\alpha \) generate \( g \) so we know \( \phi (\sum_{i=1}^{m} \bar{\omega}_i \otimes z_i) t^{-1} \) must commute with every element in \( g \). Equivalently, \( \phi (\sum_{i=1}^{m} \bar{\omega}_i \otimes z_i) t^{-1} \) is a central element of \( G \). This follows from the discussion after Example 2.4.10. Since \( G \) is adjoint, the centre of \( G \) is trivial. Hence \( \phi (\sum_{i=1}^{m} \bar{\omega}_i \otimes z_i) t^{-1} = 1 \) so we conclude that \( \phi \) is surjective since for all \( t \in T \), since there exists \( \sum_{i=1}^{m} \bar{\omega}_i \otimes z_i \in X^\vee \otimes_\mathbb{Z} C^\times \) such that \( \phi (\sum_{i=1}^{m} \bar{\omega}_i \otimes z_i) = t \). We have shown \( X^\vee \otimes_\mathbb{Z} C^\times \cong T \).

Consider the map \((z_1, \ldots, z_m) \mapsto (\sum_{i=1}^{m} \bar{\omega}_i \otimes z_i)\). It is not difficult to show that this is an isomorphism from \((C^\times)^m\) to \( X^\vee \otimes_\mathbb{Z} C^\times \). Composing this isomorphism with the previous isomorphism gives \( T \cong (C^\times)^m \) as desired.

\[ \Box \]

2.4 Algebraic Group Structure

We will be introducing two groups which contain information about the structure of \( G \) and its root datum. The first is the Weyl group which is a group of reflections which acts on the root datum. The Weyl group is isomorphic to the normalizer of a maximal torus in \( G \) modulo the centralizer of the torus. The second are Borel subgroups. These are subgroups of \( G \) which correspond bijectively to the bases of the root datum.

**Definition 2.4.1.** The Weyl group \( W(\Psi) \) of the root datum \( \Psi \) is defined by \( W(\Psi) = \langle s_\alpha \mid \alpha \in R \rangle \) where the \( s_\alpha \) are the reflections defined in Definition 2.3.5.
Example 2.4.2. We will determine the Weyl group of $G = GL_n(K)$. Recall $s_{\alpha}(x) = x - \langle x, \alpha^\vee \rangle \alpha$ for all $x \in X$. In Example 2.3.7, we determined the roots of $\Psi(G,T)$ where $T$ is the set of diagonal matrices. Then

$$s_{\alpha_{ij}}(\alpha_{lk}) = \begin{cases} -\alpha_{lk} & \text{if } l = i, k = j \text{ or } l = j, k = i \\ \alpha_{lk} & \text{if } l \neq i, k \neq j \\ \alpha_{lk} - \alpha_{ij} & \text{if } l \neq i, k = j \text{ or } l = i, k \neq j \\ \alpha_{lk} + \alpha_{ij} & \text{if } l \neq j, k = i \text{ or } l = j, k \neq i \end{cases}$$

If we define $\alpha_{ij} = \epsilon_i - \epsilon_j$ where $\epsilon_k(h) = x_k$ for all $1 \leq k \leq n$ then we can see that $s_\alpha$ is completely determined by its action of each $\epsilon_k$. We can also see that $s_{\alpha_{ij}}$ sends $\epsilon_i - \epsilon_j$ to $\epsilon_j - \epsilon_i$. This simplifies to $s_{\alpha_{ij}}$ sending $\epsilon_i$ to $\epsilon_j$ and $\epsilon_j$ to $\epsilon_i$. Thus we identify $s_{\alpha_{ij}}$ with the transposition $(ij)$ in $S_n$. Hence $\{s_{\alpha_{ij}} \mid 1 \leq i \neq j \leq n\} \cong \{(ij) \mid 1 \leq i \neq j \leq n\}$ which gives $W(\Psi) \cong S_n$.

There is an algebraic notion of the Weyl group of $G$, given by $W(G,T) = N_G(T)/Z_G(T)$, which is isomorphic to $W(\Psi)$ ([19], Section 7.1.4).

Definition 2.4.3. Suppose there exists $\lambda \in X^\vee$ such that $\langle \alpha, \lambda \rangle \neq 0$ for all $\alpha \in R$. Then we say $R^+ = \{\alpha \in R \mid \langle \alpha, \lambda \rangle > 0\}$ is a system of positive roots and $R^- = \{\alpha \in R \mid \langle \alpha, \lambda \rangle < 0\}$ is a system of negative roots.
A base $\Delta = \{\alpha_1, \ldots, \alpha_l\} \subset R$ of a root system $R$ is a basis of the vector space $R \otimes \mathbb{Z} \operatorname{span}_\mathbb{Z}\{R\}$ such that for all $\alpha \in R$, $\alpha = \sum_{i=1}^l c_i \alpha_i$ where each $c_i$ has the same sign. We say the roots of $\Delta$ are simple roots.

For a root system $R$, we see that $R = R^+ \cup R^-$. We also have that the Weyl group permutes the bases of $R$ transitively ([7], Section 10.1, page 49).

**Example 2.4.4.** Let $G = GL_2(K)$. Then the set roots with respect to the diagonal subgroup $T$ is $R = \{\alpha_12, \alpha_21\} = \{\alpha, -\alpha\}$. Now $\langle \alpha, \alpha^\vee \rangle > 0$ and $\langle -\alpha, \alpha^\vee \rangle < 0$ so $R^+ = \{\alpha\}$ is a system of positive roots and $R^- = \{-\alpha\}$ is a system of negative roots. There are two possible bases, $\Delta^+ = \{\alpha\}$ or $\Delta^- = \{-\alpha\}$.

From Example 2.4.2, we see that $W(\Psi) = \{s_\alpha, I\} \cong S_2$ since $s_\alpha = s_{-\alpha}$. As $s_\alpha$ permutes $\alpha$ and $-\alpha$, we have that $s_\alpha$ permutes $\Delta^+$ and $\Delta^-$. The same is true of $I$.

Hence, the action of the Weyl group on the roots permutes the bases.

**Example 2.4.5.** Let $G = GL_3(K)$ and let $T$ be the set of invertible diagonal matrices in $G$. Then $T$ is a maximal torus of $G$ and, as shown in Example 2.3.7, the roots with respect to $T$ are

$$R = \{\alpha_{12}, \alpha_{13}, \alpha_{21}, \alpha_{23}, \alpha_{31}, \alpha_{32}\} = \{\pm \alpha_{12}, \pm \alpha_{13}, \pm \alpha_{23}\}$$

since $\alpha_{ij} = -\alpha_{ji}$. Now $\alpha_{13} = \alpha_{12} + \alpha_{23}$ so let $\alpha_1 = \alpha_{12}$ and $\alpha_2 = \alpha_{23}$ which gives $R = \{\pm \alpha_1, \pm \alpha_2, \pm (\alpha_1 + \alpha_2)\}$. There are several possible bases for $R$. For
example, we can take $\Delta = \{\alpha_1, \alpha_2\}$ or $\Delta = \{\alpha_1, -\alpha_1 - \alpha_2\}$. There are also several possible positive root systems. Since $\langle \alpha, \alpha_1 \rangle + \langle \alpha_2 \rangle \neq 0$ for all $\alpha \in R$, we may take $R^+ = \{\alpha_1, \alpha_2, \alpha_1 + \alpha_2\}$. Another possibility is given by $\langle \alpha, \alpha_1 \rangle - 2\alpha_2 \neq 0$ for all $\alpha \in R$. This gives $R^+ = \{\alpha_1, -\alpha_2, -\alpha_1 - \alpha_2\}$. In either case, $R^- = R - R^+$.

In Example 2.4.2, we showed that $W(\Psi) \cong S_3$. We will compute the Weyl group explicitly and show its action on the set of bases. Let $\Delta = \{\alpha_1, \alpha_2\}$ be an ordered basis for $R \otimes \mathbb{Z} \text{span}_\mathbb{Z}\{R\}$. Using the computations in Example 2.4.2, we see that, as matrices acting on coordinate vectors, we have

$$s_{\alpha_1} = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \quad s_{\alpha_2} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}, \quad s_{\alpha_1 + \alpha_2} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

and $s_{-\alpha} = s_\alpha$ for all $\alpha \in R$. Thus

$$W(\Psi) = \langle s_{\alpha_1}, s_{\alpha_2}, s_{\alpha_1 + \alpha_2} \rangle$$

$$= \left\langle \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \right\rangle$$

$$= \{I, s_{\alpha_1}, s_{\alpha_2}, s_{\alpha_1 + \alpha_2}, s_{\alpha_1}s_{\alpha_2}, s_{\alpha_2}s_{\alpha_1}\}$$

and we can see that $W(\Psi) \cong S_3$. Now we can determine $W(\Psi) \cdot \Delta$. We have

$$I \cdot \Delta = \Delta, \quad s_{\alpha_1} \cdot \Delta = \{-\alpha_1, \alpha_1 + \alpha_2\}, \quad s_{\alpha_2} \cdot \Delta = \{\alpha_1 + \alpha_2, -\alpha_2\},$$

74
\[ s_{\alpha_1 + \alpha_2} \cdot \Delta = \{-\alpha_2, -\alpha_1\}, \quad s_{\alpha_1} s_{\alpha_2} \cdot \Delta = \{\alpha_1, -\alpha_1 - \alpha_2\}, \]
\[ s_{\alpha_2} s_{\alpha_1} \cdot \Delta = \{-\alpha_1 - \alpha_2, \alpha_2\}. \]

It is not difficult to see that every set of roots listed above is a base. Moreover, there are no other bases of \( R \) since we must satisfy the following condition from Definition 2.4.2. For \( \Delta = \{\gamma_1, \gamma_2\} \), we have that for all \( \alpha \in R \), \( \alpha = c_1 \gamma_1 + c_2 \gamma \) where each \( c_i \) has the same sign. Hence the action of the Weyl group on the set of bases is transitive and permutes the bases.

**Definition 2.4.6.** A Borel subgroup of \( G \) is a maximal, closed, connected, solvable subgroup.

**Example 2.4.7.** Let \( B \) be the group of invertible \( n \times n \) upper triangular matrices over \( K \). Then \( B \) is a subgroup of \( GL_n(K) \). The affine algebra of \( B \) is \( K[B] = K[T_{ij}, U_{1 \leq i, j \leq n}] / (T_{ij}, U \det -1)_{1 \leq j < i \leq n} \). We can see that \( (T_{ij}, U \det -1)_{1 \leq j < i \leq n} \) is a prime ideal so, by Lemma 2.1.4, 2, \( B \) is irreducible. This implies \( B \) is connected. Since \( B = \bigcap_{1 \leq j < i \leq n} \mathcal{V}(T_{ij}) \cap \mathcal{V}(U \det -1) \), \( B \) is closed. We will give a sketch of why \( B \) is solvable. It is not difficult to show that \( B^{(1)} = [B, B] \) is the set of upper triangular matrices with 1 on the diagonal. It is also fairly straightforward to show that \( B^{(2)} = [B^{(1)}, B^{(1)}] \) is the subgroup of \( B^{(1)} \) with 0 immediately above the diagonal. Continuing in this way, we can see that \( B^{(i)} \) is the set of upper triangular matrices with 1 on the diagonal and more zeros above the diagonal. Thus, there exists a \( j \geq 1 \)
such that $B^{(j)}$ is the set of matrices with 1 on the diagonal and the only other entry which is nonzero is the top right entry. This is an abelian group so $B^{(j)}$ is trivial. Therefore $B$ is solvable. One can show that $B$ is maximal since other entries being nonzero would give a group which is not solvable. Hence $B$ is a Borel subgroup of $GL_n(K)$.

**Proposition 2.4.8.** Let $B$ be a Borel subgroup of $G$. Maximal tori of $B$ are maximal tori of $G$ and the roots of $B$ with respect to a maximal torus $T$ in $G$ is a system of positive roots in $R$.

For a proof of Proposition 2.4.8, see ([8], Corollary 21.3 A, [19], Proposition 7.4.6).

A fixed Borel subgroup determines a set of positive roots of $R$, and a set of positive roots determine a base for $R$. Hence, Proposition 2.4.8 tells us that a Borel subgroup completely determines a base of $R$. This holds in the reverse direction as well.

**Example 2.4.9.** Let $G = GL_2(\mathbb{C})$ and let $B$ be the group of invertible upper triangular matrices in $G$. We know $B$ is a Borel subgroup of $G$ from Example 2.4.4. Let $T$ be the group of diagonal matrices in $G$. Then $T$ is certainly a maximal torus of $G$ and $B$. The Lie algebra of $B$ is the set of upper triangular matrices in $M_2$ so there is only one root of $B$ with respect to $T$, $\alpha_{12} = \alpha$ from Example 2.4.4. Now $\{\alpha\}$ is
certainly a positive root system for $R$ and we may take $\Delta = \{\alpha\}$ to be a base.

**Example 2.4.10.** Let $G = GL_3(\mathbb{C})$ and let $B$ be the group of invertible upper triangular matrices in $G$. We know $B$ is a Borel subgroup of $G$ from Example 2.4.4. Let $T$ be the group of diagonal matrices in $G$. Then $T$ is certainly a maximal torus of $G$ and $B$. The Lie algebra of $B$ is the set of upper triangular matrices in $M_3$ so the roots of $B$ with respect to $T$ are $\alpha_{12} = \alpha_1$, $\alpha_{23} = \alpha_2$ and $\alpha_{13} = \alpha_1 + \alpha_2$ from Example 2.4.5. We also showed in Example 2.4.5 that $\{\alpha_1, \alpha_2, \alpha_1 + \alpha_2\}$ is a positive root system for $R$. The corresponding base is $\Delta = \{\alpha_1, \alpha_2\}$.

Given a base for a root system, there is a method to determine the corresponding Borel subgroup. By ([19], Theorem 7.2.4), every root corresponds to a copy of $SL_2$ in $G$. This subgroup is $G_\alpha = Z_G((\ker \alpha)^0)$ for a root $\alpha$ ([19], Section 7.1) and the subgroups $G_\alpha$ generate $G$ ([19], Lemma 7.1.3). Denote the additive group $(K, +)$ by $G_\alpha$. There exists an injection $u_\alpha: G_\alpha \longrightarrow G$ such that the image of $u_\alpha$, denoted by $U_\alpha$ is a closed subgroup of $G$ contained in $G_\alpha$. This map is defined by the property

$$tu_\alpha(x)t^{-1} = u_\alpha(\text{Ad}(t)x) = u_\alpha(\alpha(t)x)$$

for all $t \in T$, $x \in K$. In addition, $T$ together with the subgroups $U_\alpha$, $\alpha \in R$ generate $G$ ([19], Proposition 8.1.1). For $K = \mathbb{C}$, we may simply take $U_\alpha = \exp(g_\alpha)$ where $\exp$ is the exponential map on $g$. The following proposition gives how a Borel subgroup is generated.
Proposition 2.4.11. Let $\Delta$ be a base for a root system $R(G,T)$. Then, for any positive root system $R^+$, $B = \langle T, U_\alpha \mid \alpha \in R^+ \rangle$ is a Borel subgroup of $G$.

For a proof of Proposition 2.4.11, see ([19], Proposition 8.2.4, (ii)).

Thus, taking both Proposition 2.4.8 and Proposition 2.4.11 into consideration, we see that there is a bijection between Borel subgroups of $G$ containing $T$ and bases of $R$.

Example 2.4.12. Let $G = GL_n(\mathbb{C})$. From Example 2.3.3, we have $R = \{\alpha_{ij} \mid 1 \leq i \neq j \leq n\}$. However, $\alpha_{ij} = -\alpha_{ji}$ so the roots are $\pm \alpha_{ij}$, $1 \leq i < j \leq n$. We also have that each root is a linear combination of $\alpha_{i(i+1)}$, $1 \leq i < n$. We relabel the roots $\alpha_{i(i+1)} = \alpha_i$. Then $\Delta = \{\alpha_i \mid 1 \leq i < n\}$ is a base.

In this case, we may take $U_\alpha = \exp(g_\alpha)$. Now $g_\alpha = \langle E_{i(i+1)} \rangle$ so

$$\exp(g_\alpha) = \exp(E_{i(i+1)}) = \langle I + E_{i(i+1)} \rangle.$$

Hence $B = \langle \text{diag}(x_1, \ldots, x_n), I + E_{i(i+1)} \mid x_j \in K, 1 \leq i < n \rangle$ is a Borel subgroup of $G$.

2.5 F-Groups

We previously defined linear algebraic groups over an algebraically closed field $K$. The notion of a linear algebraic group generalizes to an arbitrary field $F$. Our goal
is to be able to work over a $p$-adic field. For this section, we consider an arbitrary field $F \subseteq K$ where $K$ is algebraically closed. We return to the definition of a variety. The concepts discussed in Section 2.1 can be extended to define affine varieties over $F$. We will define the notion of a split $F$-group which is a reductive linear algebraic group that is defined over $F$ and has a maximal torus defined over $F$. In this case, we say that the maximal torus is $F$-split. We will outline this concept with a simple example. Let $V = K^m$ and let $X$ be a closed subset of $V$.

Definition 2.5.1. We say that $F$ is a field of definition of an algebraic set $X \subseteq V$ if $I(X)$ is generated by polynomials with coefficients in $F$. In this case, the affine $F$-algebra is given by $F[X] = F[T_1, \ldots, T_m]/(I[X] \cap F[T_1, \ldots, T_m])$.

Example 2.5.2. Consider $G_m$ over $C$. Recall that, in Example 2.2.7 we showed $C[G_m] = C[T_1, T_2]/(T_1T_2 - 1)$. Then $R$ is a field of definition of $G_m$ since $T_1T_2 - 1$ is defined over $R$. Let $G = R^\times = G_m(R)$. Hence $R[G] = R[T_1, T_2]/(T_1T_2 - 1)$.

Definition 2.5.3. An $F$-structure on $X$ is an $F$-subalgebra $F[X]$ of $K[X]$ which is finitely generated over $F$ and satisfies $K \otimes_F F[X] \cong K[X]$.

The rational points of $F[X]$ is the set of homomorphisms $F[X] \rightarrow F$ over $F$.

Note that the Zariski topology is defined on $F$-structures in the same way as previously defined in Section 2.1. We say a set is $F$-open if it is an affine open set in the Zariski topology defined over $F$-structures.
Example 2.5.4. Let $G = G_m$. Define $\phi \colon C \otimes_R R[G] \to C[G]$ by $\phi(\alpha \otimes T_1) = \alpha T_1$ and $\phi(\alpha \otimes T_2) = \alpha T_2$. It is not difficult to see that $\phi$ is a surjective morphism defined over $R$. It is a simple exercise to show that $C \otimes_R (T_1 T_2 - 1) \subseteq \ker \phi$. However, if $\sum_{i \in I} \alpha_i \otimes f_i(T_1, T_2) \in \ker \phi$ then $\sum_{i \in I} \alpha_i f_i(T_1, T_2) \in (T_1 T_2 - 1)$. This implies that $\sum_{i \in I} \alpha_i f_i(T_1, T_2) = (T_1 T_2 - 1) \sum_{j \in J} \gamma_j g_j(T_1, T_2)$ which gives

$$\sum_{i \in I} \alpha_i \otimes f_i(T_1, T_2) = \sum_{j \in J} \gamma_j \otimes g_j(T_1, T_2)(T_1 T_2 - 1) \in C \otimes_R (T_1 T_2 - 1).$$

Hence $\ker \phi$ is trivial so $\phi$ is an isomorphism. Thus $R[G]$ is an $R$-structure of $C[G]$.

The $R$-rational points of $R[G]$ are the homomorphisms from $R[T_1, T_2]/(T_1 T_2 - 1)$ to $R$. Suppose such a homomorphism sends $T_1$ to $x$ and $T_2$ to $y$. We have $T_1 T_2 - 1 \mapsto 0$ so $y = x^{-1}$. Thus, the $R$-rational points of $R[G]$ are given by the real solutions of $T_1 T_2 - 1 = 0$. All solutions are of the form $(x, x^{-1}), x \in \mathbb{R}^\times$ so we may identify the set of $R$-rational points with $\mathbb{R}^\times$.

Example 2.5.5. Now consider $S = S^1$. We have

$$S = \{ a \in G_m(C) \mid aa^* = 1 \} = \{ a \in C^\times \mid a \bar{a} = 1 \} = \{ x + iy \mid x^2 + y^2 = 1 \}.$$

Then $R[S] = R[X, Y]/(X^2 + Y^2 - 1)$. Note that $R[S]$ is a subalgebra of $C[G_m]$.

Define $\psi : C[T_1, T_2]/(T_1 T_2 - 1) \to C \otimes_R R[X, Y]/(X^2 + Y^2 - 1) \psi(T_1) = X + iY$ and $\psi(T_2) = X - iY$. Then $(T_1 T_2 - 1) \subseteq \ker \psi$ and $\text{Im}(T_1 T_2 - 1) = (X^2 + Y^2 - 1)$. However, $f \in \ker \psi$ implies $(X + iY)(X - iY) - 1 \mid f(X + iY, X - iY)$. This gives
\[ T_1T_2 - 1 \mid f(T_1, T_2) \] which shows that \( \ker \psi \) is trivial. Hence \( \psi \) is injective so \( \psi \) is an isomorphism. Hence \( \mathbb{R}[S] \) is an \( \mathbb{R} \)-structure of \( \mathbb{C}[G_m] \).

Similar to the previous example, the \( \mathbb{R} \)-rational points are the real solutions of \( X^2 + Y^2 - 1 = 0 \). Thus, the set of \( \mathbb{R} \)-rational points is \( \{(\cos \theta, \sin \theta) \mid \theta \in \mathbb{R}\} \) which we may identify with \( S^1 \).

**Definition 2.5.6.** Let \( (X, \mathcal{O}_X) \) be an affine variety. If \( F[X] \) is an \( F \)-structure on \( X \) and if for every \( F \)-open subset \( U \subseteq X \) we have an \( F \)-subalgebra \( \mathcal{O}_X(U)(F) \) of \( \mathcal{O}_X \) such that \( K \otimes_F \mathcal{O}_X(U)(F) \cong \mathcal{O}_X(U) \) then we say \( (X, \mathcal{O}_X(F)) \) is an affine \( F \)-variety.

**Definition 2.5.7.** For \( F \)-varieties \( X \) and \( Y \), a morphism \( \phi: X \to Y \) is defined over \( F \) if \( \phi \) is continuous with respect to the \( F \)-open sets and for any \( U \) open in \( Y \), the induced morphism \( \phi^{-1}(U) \to U' \) is defined over \( F \). In this case we say \( \phi \) is an \( F \)-morphism.

Now we define a linear algebraic group over \( F \).

**Definition 2.5.8.** A linear algebraic group \( G \) is a (linear) \( F \)-group if it is an affine \( F \)-variety, multiplication morphism \( \mu \) and inversion morphism \( i \) are defined over \( F \) and the identity element \( e \) is an \( F \)-rational point.

**Definition 2.5.9.** An \( F \)-torus \( T \) is an \( F \)-group which is a torus. We say \( T \) is \( F \)-split if \( T \) is \( F \)-isomorphic to \( D_n \) for some \( n > 0 \). If \( T \) is a maximal tours of an \( F \)-group \( G \) and \( T \) is \( F \)-split, we say \( G \) is \( F \)-split.
Note that an equivalent definition for $T$ to be $F$-split is if the every character is defined over $F$.

**Example 2.5.10.** Let $G = G_m$ over $\mathbb{C}$. Let $T = \mathbb{R}^\times$ and $S = S^1$. We can see that multiplication and inversion are defined over $\mathbb{R}$ in $T$ and $1$ is a rational point of $T$. Therefore $T$ is a split $\mathbb{R}$-form of $G$.

We also have that multiplication and inversion in $S$ is certainly defined over $\mathbb{R}$. Thus $S$ is an $\mathbb{R}$-form of $G$. Notice that $\psi$ from Example 2.5.5 is not defined over $\mathbb{R}$ so $S$ is not split.

It is worth mentioning that there is no map defined over $\mathbb{R}$ that sends $T_1T_2 - 1$ to $X^2 + Y^2 - 1$ so $S^1 \not\cong \mathbb{R}^\times$. We would expect this since $\mathbb{R}^\times$ is a split $\mathbb{R}$-form while $S^1$ is not.

We can see that, in general, there is more than one $F$-group for a given root datum.

**Theorem 2.5.11.** Let $\Psi = (X,R,X^\vee, R^\vee)$ be a root datum with base $\Delta$. There exists a connected, reductive, $F$-split $F$-group $G$ with root datum $\Psi$. Moreover, $G$ contains an maximal $F$-torus and a Borel subgroup defined over $F$ such that $T \subseteq B$.

For a proof of Theorem 2.5.11, see ([19], Theorem 16.3.3).
3 Unramified Admissible Homomorphisms and L-Packets

Let \( F \) be a \( p \)-adic field with uniformizer \( \varpi \) and let \( G \) be a connected, reductive, linear algebraic \( F \)-group with maximal tours \( T \) which is split over \( F \). We will take the dual group \( \hat{G} \) of \( G \) to be defined over \( \mathbb{C} \). Theorem 2.5.11 guarantees that this is possible. Recall from the end of Section 1.5 that the Weil group over \( F \) is given by 
\[
W(F/F) = \bigcup_{m \in \mathbb{Z}} (Fr_q)^m I
\]
where \( I = \text{Gal}(\overline{F}/F_u) \) is the inertia group. In this section, we follow [13] to describe the Langlands correspondence.

**Definition 3.1.1.** Suppose \( \phi: W(F/F) \to \hat{G} \) is a homomorphism. If \( \phi(I) \) is trivial and \( \phi(Fr_q) \) is semi-simple then we say \( \phi \) is an unramified admissible homomorphism.

It is clear that unramified admissible homomorphisms are determined by the cyclic portion \( < Fr_q > \) of the Weil group.

**Definition 3.1.2.** An admissible homomorphism \( \phi \) is tempered if \( \phi(W(F/F)) \) is bounded in \( \hat{G} \subseteq GL_n(\mathbb{C}) \) (under any norm).

For the remainder of this section, let \( \phi \) be an unramified tempered admissible homomorphism. This implies \( \phi(< Fr_q >) \) is bounded. Let \( s = \phi(Fr_q^{-1}) \in \hat{T} \). Since tori are diagonalizable, \( \hat{T} \cong (\mathbb{C}^\times)^k \) for some \( k \geq 1 \) so, fixing an isomorphism, \( s \) may
be identified with some \((s_1, \ldots, s_k) \in (\mathbb{C}^\times)^k\). Note that \(\phi\) being tempered identifies \(s\) with an element of \((S^1)^k\) where \(S^1\) is the circle group in \(\mathbb{C}^\times\).

Our goal is to compute the component group \(Z_{\hat{G}}(s)/Z_{\hat{G}}(s)^0\) of the centralizer \(Z_{\hat{G}}(s)\) for \(s = \phi(Fr^{-1}_q)\). We will only be concerned with \(\phi\) up to \(\hat{G}\)-conjugacy. This implies that we are only concerned with \(s\) up to \(N_{\hat{G}}(\hat{T})/Z_{\hat{G}}(\hat{T}) \cong W_{\hat{G}}\) conjugacy classes.

There is another important object attached to \(\phi\) called an L-packet. The goal of this thesis is to compute the cardinality of these L-packets. In order to define an L-packet, we shall define a character \(\chi\) of \(T(F)\) via \(s = \phi(Fr^{-1}_q)\). Then we will induce \(\chi\) to a representation of \(G(F)\). The L-packet attached to \(\phi\) is the set of irreducible subrepresentations of the induced representation on \(G(F)\). We will see that this L-packet is equal in size to \(Z_{\hat{G}}(s)/Z_{\hat{G}}(s)^0\).

Recall that, by Lemma 1.2.9 iv), \(F^\times \cong \mathcal{O}_F^\times \times <\varpi>\).

**Definition 3.1.3.** An unramified character of \(F^\times\) is a character \(\chi: F^\times \to \mathbb{C}^\times\) such that the restriction of \(\chi\) to \(\mathcal{O}_F^\times\) is trivial.

Given \(\phi\), we want to define unramified characters which will give us a representation of \(T(F)\). We define unramified characters \(\chi_1, \ldots, \chi_k\) by \(\chi_j(\varpi) = s_j\) for all \(1 \leq j \leq k\). Then \(\chi = (\chi_1, \ldots, \chi_k)\) is a character of \((F^\times)^k\). Now \(T(F) \cong (F^\times)^k\) since \(T\) is split. There is a canonical isomorphism to transfer \(\chi\) to a character of
$T(F)$ ([13], 2.1.3). We abuse notation and write $\chi$ for the corresponding character of $T(F)$.

Let $B$ be a Borel subgroup of $G$ defined over $F$ which contains $T$. By Proposition 2.4.11, $B = TU$ where $U$ is the group generated by the root groups corresponding to the positive roots (see the discussion following Example 2.4.10). Similarly, let $\bar{U}$ denote the group generated by the root groups corresponding to the negative roots. The induced representation $\text{ind}^G_B \chi$ of $G(F)$ is defined to be left translation on the space of locally constant functions $f: G(F) \to \mathbb{C}$ which satisfy

$$f(gtu) = |\text{Ad}_U(t)|^{-\frac{1}{2}} \chi^{-1}(t)f(g) \text{ for all } g \in G(F), t \in T(F), u \in U(F)$$

where

$$|\text{Ad}_U(t)| = \prod_{\alpha \in R^+(G,T)} |\alpha(t)| \text{ for all } t \in T(F).$$

We are interested in the irreducible subrepresentations of $\text{ind}^G_B \chi$. There are finitely many of these subrepresentations and they are independent of the choice of $B$ up to equivalence ([3], Corollary 3.6.9).

**Definition 3.1.4.** The L-packet $\Pi_\phi$ of $\phi$ is the set of irreducible subrepresentations of $\text{ind}^G_B \chi$ up to equivalence.

Thus, each unramified tempered admissible homomorphism $\phi$ has an associated L-packet $\Pi_\phi$ and component group $Z_G(s)/Z_G(s)^0$. We have the following picture...
We follow Section 1 and 2 of [10] to describe a set of intertwining operators of ind$_B^G\chi$ characterized by a subgroup $R_\chi$ of $W_G$.

Let $W_\chi = \{ w \in W_G \mid w \cdot \chi = \chi \}$. For any $w \in W_\chi$, the integral $A(w, \chi)f(g) = \int_{U \cap w^{-1}Uw}f(g\bar{w})d\bar{u}$ on $f$ in the space of ind$_B^G\chi$ defines an intertwining operator.

There is a theorem of Harish-Chandra which states that $\{A(w, \chi) \mid w \in W_\chi\}$ spans Hom$_G$(ind$_B^G\chi$). Let $\Phi$ be a root system and let $\Delta' = \{ \alpha \in \Phi \mid A(w, \lambda) is scalar \}$. Define $R = \{ w \in W_\chi \mid \alpha \in \Delta' and \alpha > 0 implies w \cdot \alpha > 0 \}$. There exists a subgroup $R_\chi$ of $W_\chi$ and a normalization $A(w, \chi) = c_wA(w, \chi)$ for some scalar $c_w \in \mathbb{C}^\times$ such that $R_\chi \cong \{A(w, \chi) \mid w \in R\}$ which spans Hom$_G$(ind$_B^G\chi$) and $|R_\chi| = \dim(\text{Hom}_G(\text{ind}_B^G\chi))$ (Theorem in [10], Section 2).

It turns out that $R_\chi \cong Z_G(s)/Z_G(s)^0$ ([11], Proposition 2.6) and that $Z_G(s)/Z_G(s)^0$ is abelian (we will show this later). Suppose $\text{ind}_B^G\chi = \oplus_{j=1}^n \pi_j$ where each $\pi_j$ is irreducible. Schur’s Lemma gives that $\text{Hom}(\pi_i, \pi_j) \cong \mathbb{C}$ when $\pi_i$ and $\pi_j$ are equivalent. Otherwise, $\text{Hom}(\pi_i, \pi_j) \cong 0$. It also follows from Schur’s Lemma that if $\pi_i$ and $\pi_j$ are
equivalent for some $i \neq j$, we can find intertwining operators of $\text{ind}^G_B \chi$ which do not commute. This would contradict the fact that $R_\chi$ is abelian. Hence the irreducible subrepresentations of $\text{ind}^G_B \chi$ occur with multiplicity one and

$$|\Pi_\phi| = \dim(\text{Hom}_G(\text{ind}^G_B \chi)) = |R_\chi| = |Z_G(s)/Z_G(s)^0|.$$  (0)

The completed picture is

$$\begin{array}{ccc}
\phi & \rightarrow & s \\
\downarrow & & \downarrow \\
\Pi_\phi & \sim & Z_G(s)/Z_G(s)^0 \\
\end{array}$$

Incidentally, the factor of an $L$-function corresponding to $\Pi_\phi$ can be found in [13] and is given by

$$L(z, \phi) = \frac{1}{\det(I - |\varpi|^z \phi(F_{q^{-1}}))}$$

where $z \in \mathbb{C}$.

**Example 3.1.5.** Let $G(F) = \text{PGL}_2(F)$ and let $Z$ be set of scalar matrices in $\text{GL}_2(F)$. Then $T(F) = \{\text{diag}(a, 1)Z \mid a \in F^\times\} \cong F^\times$ is a maximal torus of $G(F)$ and $\hat{G} = \text{SL}_2(\mathbb{C})$. Define $\phi(F_{q^{-1}}) = \text{diag}(|\varpi|^\nu, |\varpi|^{-\nu}) \in \hat{G}$ for some $\nu \in i\mathbb{R}$. This produces an unramified character. Define the unramified character $\chi_1$ by

$$\chi_1(\text{diag}(a, 1)Z) = |a|^{2\nu}.$$  

Then $\chi_1(\text{diag}(\varpi, 1)Z) = \alpha_1(\phi(F_{q^{-1}}))$ where $\alpha_1$ is the positive root of $\hat{G}$. Define $\chi = \chi_1$ which is a character on $F^\times$.

Now, $\hat{G}$ is embedded in $\text{GL}_n(\mathbb{C})$ via the identity map so we have

$$\det(I - |\varpi|^z \phi(F_{q^{-1}})) = \begin{vmatrix} 1 - |\varpi|^{z+\nu} \\ 1 - |\varpi|^{z-\nu} \end{vmatrix} = 1 - |\varpi|^{z+\nu} - |\varpi|^{z-\nu} + |\varpi|^{2z}$$

87
so the factor of an L-function corresponding to $\Pi_\phi$ is

$$L(z, \phi) = \frac{1}{1 - |\varpi|^{z+\nu} - |\varpi|^{z-\nu} + |\varpi|^{2z}} = \frac{1}{1 - |\varpi|^z(|\varpi|^\nu + |\varpi|^{-\nu} - |\varpi|^{2z})}.$$  

We know that $\hat{G} = SL_2(\mathbb{C})$ is simply connected so $Z_{\hat{G}}(\phi(Fr^{-1})) = Z_{\hat{G}}(\phi(Fr^{-1}))^0$. Thus $|\Pi_\phi| = |Z_{\hat{G}}(\phi(Fr^{-1}))/Z_{\hat{G}}(\phi(Fr^{-1}))^0| = 1$ so $\text{ind}_{B, X}^G$ is irreducible.

The work of this thesis is completely motivated by (0). We introduced $p$-adic fields and related Galois theory in order to define the objects in (0). We learn from (0) that we can determine the number of irreducible subrepresentations in a relatively elementary manner. We focus on computing component groups of centralizers of semi-simple elements in connected, quasi-simple linear algebraic groups. In Section 5, we will compare our work on $Z_G(s)/Z_G(s)^0$ with the work of Keys on $R_X$.

4 Component Groups

Let $G$ be a connected, semi-simple linear algebraic group over $\mathbb{C}$ with maximal torus $T$. In this section, $G$ will play the role of the dual group from Section 3. We do this to simplify notation. Let $s \in T$ be a semi-simple element such that $<s>$ is bounded. By Definition 2.3.4, $s \in T \cong (\mathbb{C}^\times)^k$ for some $k \geq 1$. We can identify $s$ as an element of $(S^1)^k$ where $S^1$ is the unit circle in $\mathbb{C}$. Now [9], Theorem 2.2, gives the following. The centralizer $Z_G(s)$ of $s$ is a reductive group which, in certain cases,
is not connected. Moreover, $Z_G(s)$ is generated by the root groups where each root is trivial on $s$ together with the Weyl group representatives which commute with $s$. Since $Z_G(s)$ is reductive, so is $Z_G(s)^0$ and $Z_G(s)^0$ is generated only by the root groups.

We wish to compute the component group $Z_G(s)/Z_G(s)^0$. This is a finite group which encodes some of the structure of these centralizers. Consider the case where $Z_G(s)/Z_G(s)^0$ is cyclic with generator $g$. The map $Z_G(s)^0 \rtimes \langle g \rangle \to Z_G(s)$ defined by $(a, g) \mapsto ag$ is an epimorphism. It is not difficult to show that the kernel is $\langle (g^{-m}, g^m) \rangle$ where $m$ is the order of $Z_G(s)/Z_G(s)^0$. The first isomorphism theorem gives $Z_G(s) \cong Z_G(s)^0 \rtimes \langle g \rangle / \langle (g^{-m}, g^m) \rangle$. This type of argument can be generalized to arbitrary finite abelian groups. We will see later that $Z_G(s)/Z_G(s)^0$ is in fact a finite abelian group so we can always recover $Z_G(s)$ when given $Z_G(s)^0$ and the generators of $Z_G(s)/Z_G(s)^0$.

We will compute these component groups for every quasi-simple $G$. When $G$ is simply connected, the component group is trivial ([9], Theorem 2.11). The simplest nontrivial case to compute is when $G$ is adjoint. For simply connected, semi-simple $G$, we have surjective homomorphisms

$$G \to G/H \to G/Z$$

where $Z$ is the finite centre of $G$ and $H$ is a subgroup of $Z$. From [18], Lemma 2.8,
we have the following classification of quasi-simple groups. Every connected, quasi-

simple, algebraic group is isomorphic to $G/H$ for some simply connected group $G$

and some central subgroup $H$. Moreover, a connected, quasi-simple, group is adjoint 

if and only if it is isomorphic to $G/Z$ for some simply connected group $G$ with centre $Z$.

Our method is to compute the component groups $Z_{G/Z}(s)/Z_{G/Z}(s)^0$ for $s \in 

G/Z$ then to look at lifts $s'$ of $s$ to the intermediate subgroups $G/H$ to determine

$Z_{G/H}(s')/Z_{G/H}(s')^0$. This method gives the component group of centralizers for $s$ in 

any quasi-simple algebraic group.

We shall round off the discussion by showing that for simply connected, quasi-

simple $G$ and $c \in Z$ with $|c| = 2$, the component groups for the similitude group

$G_m \times G/\{(1,1),(-1,c)\}$ are trivial. This extends the connectedness of centralizers 

of semi-simple elements in simply connected groups, stated in [9] Theorem 2.11, to 

these similitude groups.

4.1 General Approach for the Adjoint Quasi-simple Case

Let $G$ be quasi-simple and adjoint with maximal torus $T$. Let $R$ be the roots of $G$

with respect to $T$. Let $\Delta = \{\alpha_1, \ldots, \alpha_m\}$ be a base of $R$ and let $W = < s_\alpha \mid \alpha \in R >$

be the Weyl group of $G$. Recall from Definition 2.3.17 that $Q$ is the root lattice and
$P$ is the weight lattice of $G$. The dual root and weight lattices are denoted by $Q^\vee$ and $P^\vee$ respectively. It is typical to write the characters and co-characters of $G$ additively. We will do this from this point onward.

We will consider $s = \exp(x) \in T$ with $x \in \mathbb{R} \otimes_{\mathbb{Z}} Q^\vee$. Note that Proposition 2.3.21 implies that $\alpha(\exp(x)) = e^{2\pi i <\alpha,x>}$ for all $\alpha \in R$ completely defines the function $\exp : \mathbb{R} \otimes_{\mathbb{Z}} Q^\vee \to T$. There are three main group actions involved in determining the component group $Z_G(s)/Z_G(s)^0$. A sketch of these ideas is as follows. First, we will show that a subgroup of $P^\vee \rtimes W$ is isomorphic to $P^\vee/Q^\vee$ and acts on $\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee$. Second, we show that this action induces the action of a subgroup of $W$ on the image of a certain subset of $\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee$ under $\exp$. Lastly we show that the aforementioned subgroup of $P^\vee \rtimes W$ acts on an extension of the Dynkin diagram. This action is compatible with with the action on $\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee$. The following is an explanation of these ideas in more detail.

Firstly, we will show that $P^\vee \rtimes W$ is a group which acts on certain simplicial subsets of $\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee$ called alcoves. Each base $\Delta$ of $R$ corresponds to an alcove $C$ with vertices corresponding to the fundamental weights. After fixing a base, we will be interested in the subgroup $\tilde{W}_C$ of $P^\vee \rtimes W$ which is the stabilizer of the fixed alcove $C$. The action of $\tilde{W}_C$ on $C$ is determined by how it permutes the vertices of $C$. The subgroup $\tilde{W}_C$ is isomorphic to $P^\vee/Q^\vee$ whose structure is known. We will
see that \( s \) is given by \( s = \exp(x) \) for some \( x \in \tilde{C} \). It turns out that the component group \( Z_G(s)/Z_G(s)^0 \) is isomorphic to the subgroup of \( \tilde{W}_C \) which fixes \( x \).

The second idea is that the action of \( \tilde{W}_C \) on \( C \) extends to the image \( \exp(\tilde{C}) \). Given an element \((\omega^\vee, \sigma) \in \tilde{W}_C\), we will see that this second action is determined completely by \( \sigma \) which lies in the Weyl group \( W \). Moreover, a representative of \( \sigma \) such that \((\omega^\vee, \sigma) \) fixes \( s \) is a representative of \( Z_G(s)/Z_G(s)^0 \) and all representatives are of this form.

The final idea is that the action of \( \tilde{W}_C \) on the vertices of \( C \) induces a new action on an extension \( \tilde{D} \) of the Dynkin diagram. The graph \( \tilde{D} \) is constructed by adding a vertex to the Dynkin diagram corresponding to the highest root \( \tilde{\alpha}_0 \) with edges defined in the same way as the usual Dynkin diagram. We will show that this new action is a graph automorphism of \( \tilde{D} \). This entails showing that the edges are preserved since it will be clear that \( \tilde{W}_C \) permutes the vertices \( \Delta \cup \{\tilde{\alpha}_0\} \) of \( \tilde{D} \). If we are given the action \((\omega^\vee, \sigma) \in \tilde{W}_C \) on \( \tilde{D} \) and we are given \( \omega^\vee \), the permutation action of \( \sigma \) on \( R \) can be readily deduced.

The procedure for determining all possible \( s \) with nontrivial \( Z_G(s)/Z_G(s)^0 \) is as follows. We know the structure of \( \tilde{W}_C \) since we know the structure of \( P^\vee/Q^\vee \). Thus we know how many generators we must determine and what their orders in \( \tilde{W}_C \) must be. Let \((\omega^\vee, \sigma) \) be a generator of \( \tilde{W}_C \). Due to a theorem in [17], we can determine
ω and we can determine the action of \((ω, σ)\) on \(\tilde{D}\). From this, we deduce \(σ\) as mentioned above.

Once the generators of \(\tilde{W}_C\) are determined, we look at its nontrivial subgroups. Each nontrivial subgroup fixes \(x\) for some \(x \in \tilde{C}\). We compute all possible \(x\) for each nontrivial subgroup which gives all possible \(s = \exp(x) \in T\). All maximal tori are conjugate to each other and conjugation is a continuous group automorphism. Thus, we compute every \(s \in T\) and the corresponding \(Z_G(s)/Z_G(s)\) up to conjugation.

As previously discussed, we begin by defining and examining the action of \(P^\vee \rtimes W\) on the alcoves in \(\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee\). The following discussion follows [2], Chapters V and VI. We can identify the generators of \(W\) with reflections on the roots \(R^\vee\) of \(\hat{G}\). This gives rise to an action of \(W\) on \(\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee\). Then \(Q^\vee \rtimes W\) acts on \(\mathbb{R} \otimes_{\mathbb{Z}} Q^\vee\) by reflections in \(W\) followed by translations by elements in \(Q^\vee\). It is simple to show that this action is generated by orthogonal reflections in the hyperplanes

\[
L_{α, t} = \{x \in \mathbb{R} \otimes_{\mathbb{Z}} Q^\vee \mid <α, x> = t\},
\]

for all \(α \in R, t \in \mathbb{Z}\). These reflections are given by

\[
s_{α, t}^\vee(x) = x - (⟨α, x⟩ - t)α^\vee = s_α^\vee(x) + tα^\vee
\]

where \(x \in \mathbb{R} \otimes_{\mathbb{Z}} Q^\vee\). The group \(P^\vee \rtimes W\) acts in the same manner except with translation by elements in \(P^\vee\).
**Definition 4.1.1.** The affine Weyl group is the group $\tilde{W}^a = Q^\vee \rtimes W$. The extended affine Weyl group is the group $\tilde{W} = P^\vee \rtimes W$.

We can see that $\tilde{W}^a$ is a group with multiplication given by

$$(\beta, \sigma)(\gamma, \eta) = (\sigma \cdot \gamma + \beta, \sigma \eta).$$

It is clear that $\tilde{W}^a$ is a subgroup of $\tilde{W}$.

Define an alcove $C$ to be a connected component of $R \otimes_{\mathbb{Z}} Q^\vee \setminus \{L_{\alpha, t} \mid \alpha \in R, t \in \mathbb{Z}\}$. The base $\Delta$ of $R$ determines an alcove in the following way. Let $\tilde{\alpha}_0 = \sum_{i=1}^{m} a_i \alpha_i$ be the highest root of $R$. That is, $\sum_{i=1}^{m} a_i$ is maximal where all $a_i$ are positive integers. Let $a_0 = 1$ and let $\alpha_0$ be the affine map $\alpha_0 = 1 - \tilde{\alpha}_0$ defined by $<\alpha_0, x> = 1 - <\tilde{\alpha}_0, x>$ for all $x \in R \otimes_{\mathbb{Z}} Q^\vee$. The alcove corresponding to $\Delta$ is

$$C = \{ x \in R \otimes_{\mathbb{Z}} Q^\vee \mid <\alpha_i, x > > 0 \text{ for all } 0 \leq i \leq m \}$$

([2], Chapter VI, Section 2, Proposition 5). The closure of $C$ is the closed linear hull of $\{\omega^\vee_0, \ldots, \omega^\vee_m\}$ given by

$$\bar{C} = \left\{ \sum_{i=0}^{m} x_i \omega^\vee_i \mid x_i \geq 0, \sum_{i=0}^{m} a_i x_i = 1 \right\}$$

where $\{\omega^\vee_1, \ldots, \omega^\vee_m\}$ is the subset of coweights in $P^\vee$ satisfying $<\alpha_i, \omega^\vee_i> = 1$ and $<\alpha_i, \omega^\vee_j> = 0$ for all $1 \leq i \neq j \leq m$ and $\omega^\vee_0 = 0$ for convenience of notation. The $\omega^\vee_i$, $1 \leq i \leq m$, are called the fundamental weights of $R^\vee$. Note that $x_0 = 1 - \sum_{i=1}^{m} a_i x_i$
is non-negative so we may write
\[ \bar{C} = \left\{ \sum_{i=0}^{m} x_i \omega_i^\vee \mid x_i \geq 0, 0 \leq \sum_{i=1}^{m} a_i x_i \leq 1 \right\}. \]

Finally, the \( m + 1 \) vertices of \( \bar{C} \) are given by \( v_i = a_i^{-1} \omega_i^\vee, 1 \leq i \leq m \) and \( v_0 = 0 = \omega_0^\vee \).

Form this point onward, we write \( X^*(T) \) additively.

**Example 4.1.2.** Consider \( G = PSO_8 \). As we will see in Section 4.5, we have
\[ R = \{ \pm \epsilon_i \pm \epsilon_j \mid 1 \leq i \neq j \leq 4 \}. \]

Take
\[ \Delta = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4 \} = \{ \epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \epsilon_3 - \epsilon_4, \epsilon_3 + \epsilon_4 \} \]
and \( \bar{\alpha}_0 = \alpha_1 + 2\alpha_2 + \alpha_3 + \alpha_4 \). The fundamental weights are
\[ \omega_0^\vee = 0, \]
\[ \omega_1^\vee = \epsilon_1 = \alpha_1^\vee + \alpha_2^\vee + \frac{1}{2}(\alpha_3^\vee + \alpha_4^\vee), \]
\[ \omega_2^\vee = \epsilon_1 + \epsilon_2 = \alpha_1^\vee + 2\alpha_2^\vee + \alpha_3^\vee + \alpha_4^\vee, \]
\[ \omega_3^\vee = \frac{1}{2}(\epsilon_1 + \epsilon_2 + \epsilon_3 - \epsilon_4) = \frac{1}{2}(\alpha_1^\vee + 2\alpha_2^\vee + 2\alpha_3^\vee + \alpha_4^\vee), \]
\[ \omega_4^\vee = \frac{1}{2}(\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4) = \frac{1}{2}(\alpha_1^\vee + 2\alpha_2^\vee + \alpha_3^\vee + 2\alpha_4^\vee). \]

Now \( a_i = 1 \) for \( i \neq 2 \) and \( a_2 = 2 \) so the closure of the alcove corresponding to \( \Delta \) is
\[ \bar{C} = \left\{ \sum_{i=0}^{4} x_i \omega_i^\vee \mid x_i \geq 0, x_0 + x_1 + 2x_2 + x_3 + x_4 = 1 \right\} \]
with vertices \( v_i = \omega_i^\vee \) for \( i \neq 2 \) and \( v_2 = \frac{1}{2} \omega_2^\vee \).

Now, \( \tilde{W}^a \) permutes the alcoves simply transitively ([2], Chapter V, Section 3.2). Hence \( \tilde{W} \) permutes the alcoves transitively. Denote the stabilizer of the action of \( \tilde{W} \) on the alcove \( C \) by \( \tilde{W}_C = \{ \rho \in \tilde{W} \mid \rho \cdot C = C \} \). From [2], Chapter VI, Section 2.3, we obtain that \( \tilde{W}^a \) is a normal subgroup of \( \tilde{W} \) and

\[
\tilde{W} = \tilde{W}_C \ltimes \tilde{W}^a. \tag{1}
\]

These two facts give

\[
P^\vee / Q^\vee \cong (P^\vee \rtimes W) / (Q^\vee \rtimes W) = \tilde{W} / \tilde{W}^a = \tilde{W}_C \ltimes \tilde{W}^a / \tilde{W}^a \cong \tilde{W}_C.
\]

The component groups we wish to compute can be realized as subgroups of \( \tilde{W}_C \cong P^\vee / Q^\vee \). Note that \( P^\vee / Q^\vee \) is finite abelian. The structure of all possible fundamental groups is given by the Plates in [2].

We can determine more explicitly the stabilizer \( \tilde{W}_C \) of the alcove \( C \). For all \( i, 1 \leq i \leq m \), such that \( a_i = 1 \), there exists a unique \( \rho_i \in \tilde{W}_C \) such that \( \rho_i \cdot v_0 = v_i \) and we have

\[
\tilde{W}_C = \{ \rho_i \mid a_i = 1 \} \tag{2}
\]

([2], Chapter VI, Section 2.3, Proposition 6). Writing \( \tilde{W}_C \) in this way is a crucial step. We will use (2) often.
Since $v_0 = 0$, it follows that $(\omega^\vee, \sigma) \cdot v_0 = \omega^\vee$ for any $(\omega^\vee, \sigma) \in \tilde{W}$. Thus, for all $a_i = 1$, we conclude

$$\rho_i = (\omega_i^\vee, \sigma_i)$$

for some $\sigma_i \in W$. Via $\tilde{W}_C \cong P^\vee/Q^\vee$, we obtain that $\{\omega_i^\vee | a_i = 1\}$ is a complete system of representatives of $P^\vee/Q^\vee$.

Define $\tilde{W}_x = \{\rho \in \tilde{W}_C | \rho \cdot x = x\}$ for $x \in \tilde{C}$. By definition, $\tilde{W}_x$ is a subgroup of $\tilde{W}_C$.

**Theorem 4.1.3.** Let $x \in \tilde{C}$ and let $s = \exp(x)$. Then $\tilde{W}_x \cong \mathbb{Z}_G(s)/\mathbb{Z}_G(s)^0$.

**Proof.** We give only a sketch of the proof. The details are in [17], Proposition 2.1. Let $\tilde{W}'_x$ be the stabilizer of $x$ in $\tilde{W} = P^\vee \rtimes W$ and let $W_s$ be the stabilizer of $s$ in $W$. We may write $\tilde{W}'_x = \tilde{W}_x \ltimes (\tilde{W}'_x)^0$ where $(\tilde{W}'_x)^0$ is the normal subgroup of $\tilde{W}'_x$ generated by reflection about the hyperplanes through $x$. Note that $(\tilde{W}'_x)^0$ is nontrivial only when $x$ is on a wall of $C$. The projection map $\pi: \tilde{W} \to W$ restricted to $\tilde{W}'_x$ has image $W_s$. We will see later in Corollary 4.1.5 that $\pi|_{\tilde{W}'_x}$ is a bijection so $\tilde{W}'_x \cong W_s$. Define the group $\tilde{W}_s^0 = \pi((\tilde{W}'_x)^0)$. Then, by the first isomorphism theorem,

$$\tilde{W}_x \cong \tilde{W}_s^0/(\tilde{W}'_x)^0 \cong W_s/W_s^0$$

and $W_s^0$ is generated by reflections for the roots $\{\alpha \in \mathcal{R} | \alpha(s) = 1\}$.
Now let $N_s = N_G(T) \cap Z_G(s)$ and $N_s^0 = N_G(T) \cap Z_G(s)^0$. Then the quotient map $N_s \to Z_G(s)/Z_G(s)^0$ has kernel $N_s^0$. It follows from [9], Theorem 2.2 that $N_s/N_s^0 \cong Z_G(s)/Z_G(s)^0$. To complete the proof, we require $W_s/W_s^0 \cong N_s/N_s^0$. We know $W_s = N_s/T$ and $Z_G(s)^0$ is reductive with Weyl group $W_s^0 = N_s^0/T$. Therefore

$$\tilde{W}_x \cong W_s/W_s^0 \cong N_s/N_s^0 \cong Z_G(s)/Z_G(s)^0.$$ 

\[ \square \]

We now arrive at the second group action. For $\rho \in \tilde{W}_C$, define $\rho \cdot \exp(x) = \exp(\rho \cdot x)$. This defines an action of $\tilde{W}_C$ on $\exp(\tilde{C})$. We can describe this action more precisely.

**Proposition 4.1.4.** Let $\rho = (\omega^\vee, \sigma) \in \tilde{W}$ and let $s = \exp(x)$ for some $x \in \tilde{C}$. The action of $\rho$ on $s$ is given by $\rho \cdot s = \sigma \cdot s$.

**Proof.** Let $\alpha \in \tilde{R}$. Then

$$\alpha(\rho \cdot s) = \alpha(\exp(\rho \cdot x))$$

$$= e^{2\pi i \langle \alpha, \rho \cdot x \rangle}$$

$$= e^{2\pi i \langle \alpha, \sigma \cdot x + \omega^\vee \rangle}$$

$$= e^{2\pi i \langle \alpha, \sigma \cdot x \rangle} e^{2\pi i \langle \alpha, \omega^\vee \rangle}$$

98
Now \( \alpha = \sum_{l=1}^{m} q_l \alpha_l \) where \( q_l \in \mathbb{Z} \) for all \( 0 \leq l \leq m \). Since \( \omega^\vee \) is a fundamental weight of \( R^\vee \), \( \langle \alpha, \omega_j^\vee \rangle = q_j \). Thus \( e^{2\pi i \langle \alpha, \omega_j^\vee \rangle} = 1 \) so

\[
\alpha(\rho \cdot s) = e^{2\pi i \langle \alpha, \sigma \cdot x \rangle} = \alpha(\exp(\sigma \cdot x)) = \alpha(\sigma \cdot s).
\]

This equation is true if and only if \( \alpha((\rho \cdot s)^{-1}(\sigma \cdot s)) = 1 \). Since \( \alpha \) was arbitrary, \( \alpha((\rho \cdot s)^{-1}(\sigma \cdot s)) = 1 \) for all \( \alpha \in R \). Similar to the proof of Proposition 2.3.21, we have \( (\rho \cdot s)^{-1}(\sigma \cdot s) \in Z_\mathcal{G} \). However, \( \mathcal{G} \) is adjoint so \( Z_\mathcal{G} \) is trivial. Thus \( (\rho \cdot s)^{-1}(\sigma \cdot s) = 1 \) which implies \( \rho \cdot s = \sigma \cdot s \).

**Corollary 4.1.5.** Suppose \( x \in \bar{C} \) and \( s = \exp(x) \). For any \( \rho = (\omega^\vee, \sigma) \in \tilde{W}_x \), we have \( \sigma \cdot s = s \) where \( s = \exp(x) \). Conversely, if \( \sigma \cdot s = s \) for \( \sigma \in W \) then \( (\omega^\vee, \sigma) \cdot x = x \) for some \( \omega^\vee \in P^\vee \).

**Proof.** Suppose \( \sigma \cdot s = s \). For any \( \alpha \in R \), \( \alpha(\exp(\sigma \cdot x)) = e^{2\pi i \langle \alpha, \sigma \cdot x \rangle} \). We obtain \( e^{2\pi i \langle \alpha, \sigma \cdot x \rangle} = e^{2\pi i \langle \alpha, x \rangle} \) which gives \( \langle \alpha, x - \sigma \cdot x \rangle \in \mathbb{Z} \). Now, for \( y \in R \otimes_\mathbb{Z} Q^\vee \), \( \langle \alpha, y \rangle \in \mathbb{Z} \) for all \( \alpha \in R \) if and only if \( y \in P^\vee \). Therefore \( x - \sigma \cdot x \in P^\vee \). Hence \( \sigma \cdot x + \omega^\vee = x \) for some \( \omega^\vee \in P^\vee \) which is equivalent to \( (\omega^\vee, \sigma) \cdot x = x \).

The converse follows directly from Proposition 4.1.4. \( \square \)

**Proposition 4.1.6.** Every \( \sigma \in W \) is completely determined by its action on \( \exp(\bar{C}) \).
Proof. Suppose $\sigma(t) = t$ for all $t \in \exp(\bar{C})$. It follows from Proposition 2.3.21 that this is equivalent to $\alpha(\sigma(t)) = \alpha(t)$ for all $t \in \exp(\bar{C})$ and all $\alpha \in \Delta$. This is true if and only if $(\sigma \cdot \alpha - \alpha)(t) = 0$ for all $t \in \exp(\bar{C})$ and all $\alpha \in \Delta$.

Now suppose $f \in \text{Hom}(T, G_m) = X^*(T)$. Without loss of generality, we may assume $T = (C^\times)^k$ for some $k \geq 1$. As in Example 2.3.3, $f(t_1, \ldots, t_k) = t_1^{l_1} \cdots t_k^{l_k}$ for some $l_1, \ldots, l_k \in \mathbb{Z}$. Thus, if $f|_{\exp(\bar{C})}$ is trivial then $e^{il_1\theta_1} \cdots e^{il_k\theta_k} = 1$ for all $\theta_1, \ldots, \theta_k \in \mathbb{R}$. Therefore $l_1, \ldots, l_k = 0$ which gives $f$ is trivial.

Thus $(\sigma \cdot \alpha - \alpha)(t) = 0$ for all $t \in \exp(\bar{C})$ and for all $\alpha \in \Delta$ is equivalent to $(\sigma \cdot \alpha - \alpha) = 0$ for all $\alpha \in \Delta$; i.e. $\sigma$ is the identity in $W$.

This shows that if two Weyl group elements are identical on $\exp(\bar{C})$ then they are the same Weyl group elements. \hfill \Box

We will now describe the third group action. We can realize the based root system as a graph. We will show that the group $\tilde{W}_C$ can be thought of as a subgroup of the automorphisms of a graph $\tilde{D}$ determined by the root system and the highest root. This will be useful in determining explicitly the elements of $\tilde{W}_C$.

For $x \in \bar{C}$ and $s = \exp(x)$, we will show

$$Z_G(s)/Z_G(s)^0 \cong \tilde{W}_x \hookrightarrow \tilde{W}_C \cong P^\vee/Q^\vee \hookrightarrow \text{Aut}(\tilde{D}).$$

We have described the first three maps in this section. It remains to show the last
injection. We follow ([2], Chapter VI, Sections 2.3 and 4.3).

**Definition 4.1.7.** The Dynkin diagram of $G$ is a graph with vertices given by the roots in $\Delta$. For $\alpha, \beta \in \Delta$, the corresponding vertices are joined by $<\alpha, \beta^\vee> <\beta, \alpha^\vee>$ edges. For an edge which connects two vertices that correspond to roots of different lengths, put $>$ or $<$ on the edge such that the arrow points to the shorter root.

The augmented Dynkin diagram of $G$ is the Dynkin diagram of $G$ with an added vertex corresponding to the highest root $\tilde{\alpha}_0$. This added vertex is connected to a vertex $\alpha \in \Delta$ by $<\tilde{\alpha}_0, \alpha^\vee> <\alpha, \tilde{\alpha}_0^\vee>$ edges.

By [7], Section 9.4, any two vertices are joined by zero, one, two or three edges. In fact, since we are only dealing with quasi-simple groups, any two vertices must be joined by at least one path.

Recall that from (2), we have $\tilde{W}_C = \{\rho_i \mid a_i = 1\}$ where $\rho_i$ is the unique element in $\tilde{W}$ which sends $v_0$ to $v_i$. We also determined that $\rho_i = (\omega_i^\vee, \sigma_i)$ for some $\sigma_i \in W$. We will define an action of these $\rho_i$ on $\bar{C}$ preserves the set of vertices $\{v_i \mid 0 \leq i \leq m\}$ of $\bar{C}$. Through the bijection between the vertices and the fundamental weights together with $\omega_i^\vee$, $\tilde{W}_C$ permutes the set $\{\omega_i^\vee \mid 0 \leq i \leq m\}$. We define the action of $\tilde{W}_C$ on $\Delta \cup \{\tilde{\alpha}_0\}$ by

$$\rho_i \cdot \alpha_j = \alpha_k$$

if and only if

$$\rho_i \cdot \omega_j^\vee = \omega_k^\vee,$$

$$\rho_i \cdot \alpha_j = \tilde{\alpha}_0$$

if and only if

$$\rho_i \cdot \omega_j^\vee = \omega_0^\vee.$$
\[ \rho_i \cdot \tilde{\alpha}_0 = \alpha_k \text{ if and only if } \rho_i \cdot \omega_0^\vee = \omega_k^\vee \]

for all \(1 \leq j, k \leq m\). This action certainly permutes \(\Delta \cup \{\tilde{\alpha}_0\}\). The following theorem is due to [2] Chapter VI, Section 4.3.

**Theorem 4.1.8.** The fundamental group \(P^\vee / Q^\vee\) of \(\hat{G}\) is isomorphic to a subgroup of \(\text{Aut}(\hat{D})\).

**Proof.** We have shown in the discussion above that each element of \(\tilde{W}_C \cong P^\vee / Q^\vee\) corresponds to a unique permutation of the roots in \(\Delta \cup \{\tilde{\alpha}_0\}\). It remains to be shown that this action preserves the edges of \(\hat{D}\); i.e. we must show

\[ < \rho \cdot \alpha, \rho \cdot \beta^\vee > < \rho \cdot \beta, \rho \cdot \alpha^\vee > = < \alpha, \beta^\vee > < \beta, \alpha^\vee > \]

for all \(\alpha \neq \beta \in \Delta \cup \{\tilde{\alpha}_0\}\).

Let \(\langle \cdot, \cdot \rangle\) be a \(W\)-invariant inner product on \(\mathbb{R} \otimes_{\mathbb{Z}} Q\). Let \(H\) and \(H'\) be hyperplanes of \(\hat{G}\) with unit normals \(\frac{\alpha}{||\alpha||}\) and \(\frac{\alpha'}{||\alpha'||}\) respectively. Let \(r_H\) and \(r_{H'}\) be the reflections about the hyperplanes \(H\) and \(H'\). Suppose \(|r_Hr_{H'}| = m\). Then \(\left(\frac{\alpha}{||\alpha||}, \frac{\alpha'}{||\alpha'||}\right) = -\cos\left(\frac{\pi}{m}\right)\) ([19], Lemma 7.5.1). One can show that \(r_{\rho \cdot H} = \rho r_H \rho^{-1}\) for any affine map \(\rho\). Since \(\tilde{W}\) is a set of affine maps, it follows for all \(\rho \in \tilde{W}\). Therefore

\[ |r_{\rho \cdot H}r_{\rho \cdot H'}| = |\rho r_Hr_{H'}\rho^{-1}| = |r_Hr_{H'}| = m \]

which implies

\[ \left( \frac{\rho \cdot \alpha}{||\rho \cdot \alpha||}, \frac{\rho \cdot \alpha'}{||\rho \cdot \alpha'||} \right) = -\cos\left(\frac{\pi}{m}\right) = \left( \frac{\alpha}{||\alpha||}, \frac{\alpha'}{||\alpha'||} \right). \]
By [8], page 229,

$$\langle \alpha, (\alpha')^\vee \rangle = \frac{2(\alpha, \alpha')}{(\alpha', \alpha')} = \frac{2}{||\alpha'||^2} (\alpha, \alpha')$$

we conclude

$$\langle \rho \cdot \alpha, \rho \cdot \beta^\vee \rangle < \rho \cdot \beta, \rho \cdot \alpha^\vee > = \frac{2}{||\rho \cdot \beta||^2} (\rho \cdot \alpha, \rho \cdot \beta) \frac{2}{||\rho \cdot \alpha||^2} (\rho \cdot \beta, \rho \cdot \alpha)$$

$$= 2 \left( \frac{\rho \cdot \alpha}{||\rho \cdot \alpha||}, \frac{\rho \cdot \beta}{||\rho \cdot \beta||} \right) 2 \left( \frac{\rho \cdot \beta}{||\rho \cdot \beta||}, \frac{\rho \cdot \alpha}{||\rho \cdot \alpha||} \right)$$

$$= 2 \left( \frac{\alpha}{||\alpha||}, \frac{\beta}{||\beta||} \right) 2 \left( \frac{\beta}{||\beta||}, \frac{\alpha}{||\alpha||} \right)$$

$$= \frac{2}{||\beta||^2} (\alpha, \beta) \frac{2}{||\alpha||^2} (\beta, \alpha)$$

$$= \langle \alpha, \beta^\vee \rangle < \beta, \alpha^\vee >$$

as desired. \qed

Now we can properly outline the strategy for computing $Z_G(s)/Z_G(s)^0$. For any $\rho_i \in \tilde{W}_C$, we know $\rho_i = (\omega_i^\vee, \sigma_i)$ for some $\sigma_i \in W$. We also know that $\rho_i \cdot v_0 = v_i$ which implies $\rho_i \cdot \tilde{\alpha}_0 = \alpha_i$. Since $\rho_i$ corresponds to an element in $\text{Aut}(\tilde{D})$, we can use its action on $\tilde{\alpha}_0$ to deduce its action on $\Delta \cup \{\tilde{\alpha}_0\}$. This gives the action of $\rho_i$ on the vertices of $\tilde{C}$ from which we obtain several equations of the form $\rho_i \cdot v_j = v_k$. Solving these equations gives $\sigma_i$. Since we know the structure of $P^\vee/Q^\vee$, it is sufficient to compute the generators of $\tilde{W}_C$.

To determine $Z_G(s)/Z_G(s)^0$ for a given $s$, we look at all possible (nontrivial) subgroups of $\tilde{W}_C$. Each subgroup is $\tilde{W}_x$ for some $x \in \tilde{C}$ and $\tilde{W}_x \cong Z_G(s)/Z_G(s)^0$ where
\[ s = \exp(x) \]. The generators for each \( \tilde{W}_x \) having been determined, we can compute the corresponding \( x \). We compute \( s = \exp(x) \) by computing \( \alpha(s) = e^{2\pi i \langle \alpha, x \rangle} \) for sufficiently many \( \alpha \in R \). With enough equations of this form, we are able to compute the entries of \( s \). In this way, we determine all possible \( s \) in \( T \).

Let \( T' \) is another maximal torus of \( G \) and let \( s' \in T' \) be semi-simple such that \( <s'> \) is bounded. Since all maximal tori are conjugate to each other, there exists some \( g \in G \) such that \( gTg^{-1} = T' \). Thus \( s' = gsg^{-1} \) for some semi-simple \( s \in T \) such that \( <s> \) is bounded. We have

\[ Z_G(s')/Z_G(s')^0 = Z_G(gsg^{-1})/Z_G(gsg^{-1})^0 \cong Z_G(s)/Z_G(s)^0 \]

so we find all possible \( s \) and all possible \( Z_G(s)/Z_G(s)^0 \) up to conjugation.

Some adjoint, quasi-simple groups have trivial \( Z_G(s)/Z_G(s)^0 \) for all \( s \). We will restrict our analysis to the groups over \( \mathbb{C} \) such that there is some \( s \in G \) where \( Z_G(s)/Z_G(s)^0 \) is nontrivial. These groups (up to isomorphism) are \( PGL_n(\mathbb{C}) \) for \( n \geq 2 \), \( SO_{2n+1}(\mathbb{C}) \) for \( n \geq 2 \), \( PSp_{2n}(\mathbb{C}) \) for \( n \geq 2 \), \( SO_{2n}(\mathbb{C}) \) for \( n \geq 4 \), groups of type \( E_6 \) and groups of type \( E_7 \) ([2], Chapter VI, Section 4.5 - Section 4.13).

### 4.2 \( PGL_n(\mathbb{C}) \)

We will look at the adjoint case for a quasi-simple group of type \( A_n \) for \( n \geq 2 \). That is, we consider \( G = PGL_n(\mathbb{C}) = GL_n(\mathbb{C})/Z \) where \( Z \) is the set of scalar matrices.
We state several facts here without proof. The details can be found in [2], Chapter VI, Section 4.7. We will skip several cumbersome computations for the general case. However, the computations for $PGL_4(\mathbb{C})$ will be done in detail. Let $T$ be the set of diagonal matrices in $G$. The root datum of $G$ is determined in a similar manner to Example 2.3.9 where this was computed for the case $n = 2$. We have

$$R = \{ \epsilon_i - \epsilon_j \mid 1 \leq i \neq j \leq n \}$$

and we may take $\Delta = \{ \alpha_1, \ldots, \alpha_{n-1} \}$ where $\alpha_i = \epsilon_i - \epsilon_{i+1}$. The highest root is $\tilde{\alpha}_0 = \sum_{i=1}^{n-1} \alpha_i$ which implies

$$a_i = 1 \text{ and } v_i = \omega_i^\vee \text{ for all } 1 \leq i \leq n - 1. \quad (\ast)$$

The fundamental weights are given by

$$\omega_i^\vee = \frac{1}{n} \left( (n - i) \sum_{j=1}^{i-1} j \alpha_j^\vee + i \sum_{j=i}^{n-1} (n - j) \alpha_j^\vee \right)$$

for all $1 \leq i \leq n - 1$. We will use an abuse of notation for simplicity. Identify $X_*(T)$ with $X^*(T)$ through the pairing $<,>$ by writing $\epsilon_i \in X_*(T)$ to represent the cocharacter which $< \epsilon_i, \cdot >$ sends to 1. Then we may (abusively) write

$$\omega_i^\vee = \sum_{j=1}^{i} \epsilon_j - \frac{i}{n} \sum_{j=1}^{n} \epsilon_j. \quad (I)$$

The extended Dynkin diagram $\tilde{D}$ is
Let \( S_n \) denote the permutation group of on \( n \) elements. Now \( W \cong S_n \) where \( s_{\alpha_i - \alpha_j} \) interchanges \( \alpha_i \) and \( \alpha_j \) for all \( 1 \leq i \neq j \leq n \) ([7], Section 12.2, Table 1). So \( \tilde{W} \cong P^\vee \rtimes S_n \).

Since \( a_i = 1 \) for all \( 1 \leq i \leq n - 1 \) and \( \omega_0^\vee = 0 \), the closure of the alcove corresponding \( \Delta \) is

\[
\bar{C} = \left\{ \sum_{i=0}^{n-1} x_i \omega_i^\vee \mid x_i \geq 0, \sum_{i=0}^{n-1} x_i = 1 \right\} = \left\{ \sum_{i=1}^{n-1} x_i \omega_i^\vee \mid x_i \geq 0, 0 \leq \sum_{i=1}^{n-1} x_i \leq 1 \right\}.
\]

All \( a_i = 1 \) also gives \( \tilde{W}_C = \{ \rho_i \mid 0 \leq i \leq n - 1 \} \) by (2). Now \( \text{Aut}(\tilde{D}) \cong \{1, -1\} \ltimes \mathbb{Z}/n\mathbb{Z} \) where \( \mathbb{Z}/n\mathbb{Z} \) acts by rotations of the graph and \( -1 \) interchanges \( \alpha_i \) and \( \alpha_{n-i} \) for all \( 1 \leq i \leq n - 1 \).

By (3), we have \( \rho_i = (\omega_i^\vee, \sigma_i) \) for some \( \sigma_i \in W \). We know that \( P^\vee/Q^\vee \cong \mathbb{Z}/n\mathbb{Z} \) so \( \tilde{W}_C \) is a cyclic group of order \( n \). We will determine \( \sigma_1 \) and show that \( \rho_1 \) generates \( \tilde{W}_C \).

We know \( \rho_1 \) sends \( v_0 \) to \( v_1 \) so \( \rho_1 \) must send \( \tilde{\alpha}_0 \) to \( \alpha_1 \). We will show \( \rho_1 \) corresponds to a rotation of \( \tilde{D} \) by way of contradiction.

Assume \( \rho_1 \) corresponds to some \((-1, r) \in \text{Aut}(\tilde{D})\). Since \( \rho_1 \cdot \tilde{\alpha}_0 = \alpha_1 \), \( r \) must be
the rotation which sends \( \tilde{\alpha}_0 \) to \( \alpha_{n-1} \); i.e. \( r = n - 1 \). Now

\[
(-1, n - 1)^2 = (1, 1 + n - 1) = (1, 0)
\]

which implies \( \rho_1^2 = \rho_0 \). Hence, \( \rho_1^2 \) must be trivial. Thus

\[
0 = v_0 = \rho_1^2(v_0) = \rho_1^2(\omega_0^\vee) = \rho_1(\omega_1^\vee) = \sigma_1 \cdot \omega_1^\vee + \omega_1^\vee.
\]

The action of \( \sigma_1 \) permutes the \( \epsilon_j \), \( 1 \leq j \leq n \). Thus, in the notation of (I), this gives that \( \sigma_1 \cdot \epsilon_1 = -\epsilon_1 + \frac{2}{n} \sum_{j=1}^n \epsilon_j \) and we arrive at a contradiction.

Therefore \( \rho_1 \) corresponds to the rotation of \( \tilde{\mathcal{D}} \) which sends \( \tilde{\alpha}_0 \) to \( \alpha_1 \). It sends \( \alpha_i \) to \( \alpha_{i+1} \) for all \( 0 \leq i \leq n - 2 \) and \( \alpha_{n-1} \) to \( \tilde{\alpha}_0 \). Therefore, \( \rho_1 \cdot v_i = v_{i+1} \) for all \( 0 \leq i \leq n - 2 \), and \( \rho_1 \cdot v_{n-1} = v_0 \). By (I) and (\( \star \)), we have the system of linear equations

\[
\begin{align*}
\rho_1 \cdot \left( \sum_{j=1}^i \epsilon_j - \frac{i}{n} \sum_{j=1}^n \epsilon_j \right) &= \sum_{j=1}^{i+1} \epsilon_j - \frac{i+1}{n} \sum_{j=1}^n \epsilon_j, \quad 0 \leq i \leq n - 2 \\
\rho_1 \cdot \left( \sum_{j=1}^{n-1} \epsilon_j - \frac{n-1}{n} \sum_{j=1}^n \epsilon_j \right) &= \omega_0^\vee = 0.
\end{align*}
\]

Solving for \( \sigma_1 \cdot \omega_i^\vee \) where \( \sigma_1 \) permutes the \( \epsilon_j \), \( 1 \leq j \leq n \), gives

\[
\sigma_1 \cdot \left( \sum_{j=1}^i \epsilon_j - \frac{i}{n} \sum_{j=1}^n \epsilon_j \right) = \sum_{j=1}^{i+1} \epsilon_j - \frac{i+1}{n} \sum_{j=1}^n \epsilon_j - \left( \epsilon_1 - \frac{1}{n} \sum_{j=1}^n \epsilon_j \right) = \sum_{j=2}^{i+1} \epsilon_j - \frac{i}{n} \sum_{i=1}^n \epsilon_j
\]
for all $1 \leq i \leq n - 2$ and

$$\sigma_1 \cdot \left( \sum_{j=1}^{n-1} \epsilon_j - \frac{n-1}{n} \sum_{j=1}^{n} \epsilon_j \right) = \sigma_1 \cdot \left( -\epsilon_n + \frac{1}{n} \sum_{j=1}^{n} \epsilon_j \right)$$

$$= -\epsilon_1 + \frac{1}{n} \sum_{j=1}^{n} \epsilon_j.$$  

We can deduce that $\sigma_1$ sends $\epsilon_i$ to $\epsilon_{i+1}$ for all $1 \leq i \leq n - 1$ and sends $\epsilon_n$ to $\epsilon_1$ so $\sigma_1 = s_{\epsilon_1-\epsilon_2} s_{\epsilon_2-\epsilon_3} \cdots s_{\epsilon_{n-2}-\epsilon_{n-1}}$ which corresponds to the permutation of the indices $(1\ 2\ 3\ \ldots\ n) \in S_n$. Thus $\rho_1 = (\omega_1^\vee, \sigma_1)$ has order $n$ since $\sigma_1$ has order $n$, and we get $\tilde{W}_C = <\rho_1>.$

**Example 4.2.1.** Consider $n = 4$. We have $\Delta = \{\alpha_1, \alpha_2, \alpha_3\}$ and $\tilde{\alpha}_0 = \sum_{i=1}^{3} \alpha_i$.

The fundamental weights are

$$\omega_0^\vee = 0,$$

$$\omega_1^\vee = \epsilon_1 - \frac{1}{4} (\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4) = \frac{3}{4} \epsilon_1 - \frac{1}{4} (\epsilon_2 + \epsilon_3 + \epsilon_4),$$

$$\omega_2^\vee = \epsilon_1 + \epsilon_2 - \frac{1}{2} (\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4) = \frac{1}{2} (\epsilon_1 + \epsilon_2 - \epsilon_3 - \epsilon_4),$$

$$\omega_3^\vee = \epsilon_1 + \epsilon_2 + \epsilon_3 - \frac{3}{4} (\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4) = \frac{1}{4} (\epsilon_1 + \epsilon_2 + \epsilon_3) - \frac{3}{4} \epsilon_4.$$

The closure of the alcove corresponding to $\Delta$ is

$$\tilde{C} = \left\{ \sum_{i=0}^{3} x_i \omega_i^\vee \mid x_i \geq 0, \sum_{i=0}^{3} x_i = 1 \right\} = \left\{ \sum_{i=1}^{3} x_i \omega_i^\vee \mid x_i \geq 0, 0 \leq \sum_{i=1}^{3} x_i \leq 1 \right\}.$$
As in the general case, take \(\rho_1 = (\omega_1^\vee, \sigma_1)\) where \(\rho_1 \cdot \omega_i^\vee = \omega_{i+1}^\vee\) for \(0 \leq i \leq 2\) and \(\rho_1 \cdot \omega_3^\vee = \omega_0^\vee\). This gives

\[
\begin{cases}
\sigma_1 \cdot \omega_i^\vee = \omega_{i+1}^\vee - \omega_1^\vee \text{ for all } 1 \leq i \leq 2 \\
\sigma_1 \cdot \omega_3^\vee = -\omega_1^\vee
\end{cases}
\]

which may be written as

\[
\begin{cases}
\sigma_1 \cdot \left(\frac{3}{4} \epsilon_1 - \frac{1}{4} (\epsilon_2 + \epsilon_3 + \epsilon_4)\right) = \frac{3}{4} \epsilon_2 - \frac{1}{4} (\epsilon_1 + \epsilon_3 + \epsilon_4) \\
\sigma_1 \cdot \left(\frac{1}{2} (\epsilon_1 + \epsilon_2 - \epsilon_3 - \epsilon_4)\right) = \frac{1}{2} (-\epsilon_1 + \epsilon_2 + \epsilon_3 - \epsilon_4) \\
\sigma_1 \cdot \left(\frac{1}{4} (\epsilon_1 + \epsilon_2 + \epsilon_3) - \frac{3}{4} \epsilon_4\right) = -\frac{3}{4} \epsilon_1 + \frac{1}{4} (\epsilon_2 + \epsilon_3 + \epsilon_4).
\end{cases}
\]

We can see that \(\sigma_1\) corresponds to \((1 2 3 4) \in S_4\). The group \(\tilde{W}_C = <\rho_1>\) is isomorphic to \(\mathbb{Z}/4\mathbb{Z}\). The two nontrivial cases for \(\tilde{W}_x\) are \(\tilde{W}_x = \tilde{W}_C\) and \(\tilde{W}_x = <\rho_1^2>\).

Now that we have determined \(\rho_1\), which generates \(\tilde{W}_C\), we can determine arbitrary elements of \(\tilde{W}_C\) explicitly. Induction on \(t \geq 1\) shows

\[
\rho_1^t = (\rho_1^{t-1} \cdot \omega_1^\vee, \sigma^t) = (\omega_{t \mod n}^\vee, \sigma_1^t).
\]
Let \( x = \sum_{i=0}^{n-1} x_i \omega_i^\vee \in \mathcal{C} \). Then

\[
\rho_1^t \cdot x = x_0 \omega_1^\vee + x_1 \omega_2^\vee + \ldots + x_{n-t-1} \omega_{n-1}^\vee + x_{n-t} \omega_0^\vee + x_{n-t+1} \omega_1^\vee + \ldots + x_{n-1} \omega_{t-1}^\vee \\
= \sum_{i=0}^{n-1} x_i \omega_{i+1}^\vee \mod n \\
= \sum_{i=0}^{n-1} x_i \omega_{(i+t)}^\vee \mod n.
\]

Now we consider each possibility for \( \tilde{W}_x \). We have \( \tilde{W}_x = \langle \rho_1^t \rangle \) for some \( t \) dividing \( n \). Therefore we solve

\[
\rho_1^t \cdot x = x. \tag{4}
\]

This gives a system of equations, the number of which is given by the number of disjoint cycles in \( \sigma_1^t \). If \( t = 1 \) then from (4) we have

\[
x_0 = x_1 = x_2 = \ldots = x_{n-1}.
\]

Thus, by (\( \ast \)), we obtain

\[
x_0 = 1 - \sum_{i=1}^{n-1} a_i x_i = 1 - (n - 1)x_1
\]

which gives

\[
x_1 = x_2 = \ldots = x_{n-1} = \frac{1}{n}.
\]

We call this element the *barycentre* of \( \mathcal{C} \).
Suppose $1 < t < n$. Then $\sigma_1^t$ is a product of $t$ disjoint cycles of length $\frac{n}{t}$. The resulting $t$ equations from (4) are:

$$
\begin{align*}
  x_0 &= x_t = x_{2t} = \ldots = x_{n-t} \\
  x_1 &= x_{t+1} = x_{2t+1} = \ldots = x_{n-t+1} \\
  &\vdots \\
  x_{t-1} &= x_{2t-1} = \ldots = x_{n-1}
\end{align*}
$$

but since $x_0 = 1 - \sum_{i=1}^{n-1} x_i$, the first equation gives

$$
x_t = \ldots = x_{n-t} = 1 - \sum_{i=1}^{n-1} x_i.
$$

We rearrange terms to obtain

$$
x_t = \ldots = x_{n-t} = 1 - \sum_{i=1}^{t-1} (x_i + x_{t+i} + \ldots + x_{n-t+i}) - (x_t + x_{2t} + \ldots + x_{n-t})
$$

$$
= 1 - \sum_{i=1}^{t-1} \frac{n}{t} x_i - \left( \frac{n}{t} - 1 \right) x_t.
$$

This equation reduces to

$$
x_t = \ldots = x_{n-t} = \frac{t}{n} - \sum_{i=1}^{t-1} x_i.
$$

As mentioned at the end of Section 4.1, we have equations of the form $\alpha(\exp(x)) = e^{2\pi i \langle \alpha, x \rangle}$ for all $\alpha \in R$. It is relatively straightforward to solve the resulting system
of equations. Thus, for $s = \exp(x)$, we have

$$s = \text{diag}(s_1, s_2, \ldots, s_n)Z$$

with component group $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/\mathbb{Z}$ where

$$s_k = \zeta^{\frac{n}{t} - k} \begin{bmatrix}
eq 2\pi i \sum_{j=1}^{j-1} x_j & 0 & \ldots & 0 & 0 \\ 0 & \neq 2\pi i \sum_{j=2}^{j-1} x_j & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \neq 2\pi i x_{t-1} & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}$$

and $\zeta = e^{2\pi i \frac{t}{n}}$ is a primitive $\frac{n}{t}$th root of unity. Note that for the case where $t$ does not divide $n$, $s = \text{diag}(\gamma^{n-1}, \gamma^{n-2}, \ldots, \gamma, 1)Z$ where $\gamma = e^{2\pi i \frac{n-1}{n}}$ is a primitive $n$th root of unity.

**Example 4.2.2.** Consider once again to the case of $n = 4$. For a given $x = \sum_{i=0}^{3} x_i \omega_i^j \in \bar{C}$,

$$(\epsilon_1 - \epsilon_j)(\exp(x)) = \left(\sum_{k=1}^{j-1} \alpha_k\right) (\exp(x)) = e^{2\pi i \sum_{k=1}^{j-1} \alpha_k x} = e^{2\pi i \sum_{k=1}^{j-1} x_k}$$

for $2 \leq j \leq 4$. Recall that each $\epsilon_j$ picks out the $jj$th entry of $s$. Without loss of generality, we may take $\epsilon_4(s) = 1$. Then $\epsilon_1(s) = e^{2\pi i \sum_{k=1}^{j} x_k}.$

Now, for $2 \leq j \leq 4$,

$$e^{2\pi i \sum_{k=1}^{j-1} x_k} = (\epsilon_1 - \epsilon_j)(s) = \epsilon_1(s)\epsilon_j(s)^{-1} = e^{2\pi i \sum_{j=1}^{3} x_j \epsilon_j(s)^{-1}}$$

112
which implies

\[ \varepsilon_j(s) = e^{2\pi i \sum_{k=1}^3 x_k} e^{-2\pi i \sum_{k=1}^{j-1} x_k} = e^{2\pi i \sum_{k=j}^3 x_k} \]

for all \( 2 \leq j \leq 4 \). Thus

\[ s = \begin{bmatrix}
    e^{2\pi i (x_1 + x_2 + x_3)} & 0 & 0 & 0 \\
    0 & e^{2\pi i (x_2 + x_3)} & 0 & 0 \\
    0 & 0 & e^{2\pi i x_3} & 0 \\
    0 & 0 & 0 & 1
\end{bmatrix} \in \mathbb{Z}. \]

We begin with \( \tilde{W}_x = \tilde{W}_C \). We solve \( \rho_1 \cdot x = x \) for \( x = \sum_{i=0}^{3} x_i \omega_i^\vee \in \tilde{C} \). We have

\[ \rho_1 \cdot x = x_0 \omega_1^\vee + x_1 \omega_2^\vee + x_2 \omega_3^\vee + x_3 \omega_0^\vee \]

so \( \rho_1 \cdot x = x \) implies

\[ x_0 = x_1 = x_2 = x_3. \]

Since \( x_0 = 1 - (x_1 + x_2 + x_3) \), we obtain \( x_1 = x_2 = x_3 = 1 - (x_1 + x_2 + x_3) \) which

implies

\[ x_1 = x_2 = x_3 = \frac{1}{4}. \]

Thus \( s \) is the barycentre of \( \tilde{C} \) and

\[ s_1 = e^{3\pi i}, s_2 = -1, s_3 = e^{\frac{1}{2} \pi i}, s_4 = 1. \]
Therefore \( s = \exp(x) \) is given by
\[
s = \begin{bmatrix}
e^{\frac{2\pi i}{2}} & 0 & 0 & 0 \\
0 & -1 & 0 & 0 \\
0 & 0 & e^{\frac{\pi i}{2}} & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]
and \( Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/4\mathbb{Z} \).

Next, consider \( \bar{W}_x = \langle \rho_1^2 \rangle \). We solve \( \rho_1^2 \cdot x = x \). Now
\[
\rho_1^2 \cdot x = x_0\omega_2^\gamma + x_1\omega_3^\gamma + x_2\omega_0^\gamma + x_3\omega_1^\gamma = x_0\omega_2^\gamma + x_1\omega_3^\gamma + x_3\omega_1^\gamma
\]
so \( \rho_1^2 \cdot x = x \) gives
\[
\begin{cases}
x_0 = x_2 \\
x_1 = x_3
\end{cases}
\]
Since \( x_0 = 1 - (x_1 + x_2 + x_3) \), we obtain \( x_2 = 1 - (x_1 + x_2 + x_3) \). This implies
\[
x_2 = \frac{1}{2}(1 - (x_1 + x_3)) = \frac{1}{2} - x_1.
\]

Finally,
\[
s_1 = e^{\pi i} \begin{bmatrix} e^{2\pi i x_1} & 0 \\ 0 & 1 \end{bmatrix}, \quad s_2 = \begin{bmatrix} e^{2\pi i x_1} & 0 \\ 0 & 1 \end{bmatrix}
\]
so $s = \exp(x)$ is given by

$$s = \begin{bmatrix}
-\epsilon^{2\pi ix_1} & 0 & 0 & 0 \\
0 & -1 & 0 & 0 \\
0 & 0 & e^{2\pi ix_1} & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}$$

and $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z}$.

### 4.3 $SO_{2n+1}(\mathbb{C})$

We will look at $G = SO_{2n+1}(\mathbb{C})$, $n \geq 2$, which is the adjoint, quasi-simple group of type $B_n$. We state several facts here without proof. The details can be found in [2], Chapter VI, Section 4.5. Consider the $2 \times 2$ matrix

$$s_\theta = \begin{bmatrix}
\cosh \theta & i \sinh \theta \\
-i \sinh \theta & \cosh \theta
\end{bmatrix}$$

where $\theta \in \mathbb{C}$ and let $T$ be the set of block diagonal matrices

$$T = \{ \text{diag}(s_{\theta_1}, \ldots, s_{\theta_n}, 1) \mid \theta_j \in \mathbb{C}, 1 \leq j \leq n \}$$

which is a maximal torus of $G$ ([12], page 252). It is not difficult to show that

$$X^*(T) = \langle \epsilon_j \mid 1 \leq j \leq n \rangle$$

and

$$R = \{ \pm \epsilon_i \pm \epsilon_j \mid 1 \leq i \neq j \leq n \} \cup \{ \pm \epsilon_j \mid 1 \leq j \leq n \}$$
where $\epsilon_j(diag(s_{\theta_1}, \ldots, s_{\theta_n}, 1)) = \epsilon^\theta$. We may take $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ where $\alpha_j = \epsilon_j - \epsilon_{j+1}$ for all $1 \leq j \leq n - 1$ and $\alpha_n = \epsilon_n$. The highest root is $\tilde{\alpha}_0 = \alpha_1 + \sum_{i=2}^n 2\alpha_i$ which implies

\[ a_1 = 1 \text{ and } a_i = 2 \text{ for all } 2 \leq i \leq n. \]  

(*)

Thus $v_1 = \omega^\vee_1$ and $v_i = \frac{1}{2}\omega^\vee_i$ for all $2 \leq i \leq n$. The fundamental weights are given by

\[ \omega^\vee_i = \sum_{j=1}^{i-1} j\alpha^\vee_j + i \left( \sum_{j=i}^{n-1} \alpha^\vee_j + \frac{1}{2}\alpha^\vee_n \right) \]

for all $1 \leq i \leq n$. As in Section 4.2, we may (abusively) write

\[ \omega^\vee_i = \sum_{j=1}^i \epsilon_j. \]  

(II)

The extended Dynkin diagram $\tilde{D}$ for $n \geq 3$ is

![Dynkin Diagram](image)

and the extended Dynkin diagram $\tilde{D}$ for $n = 2$ is

![Dynkin Diagram](image)

Now $W \cong (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$ where $s_{\epsilon_i-\epsilon_j}$ interchanges $\epsilon_i$ and $\epsilon_j$ while $s_{\epsilon_i}$ interchanges $\epsilon_i$ and $-\epsilon_i$ for all $1 \leq i \neq j \leq n$ ([7], Section 12.2, Table 1). Note that
the conjugation action $s_{\epsilon_i-s_j}s_{\epsilon_j}s_{\epsilon_i-s_j} = s_{\epsilon_i}$ makes $W$ a semidirect product. Then $	ilde{W} \cong P^{\gamma} \rtimes ((\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n)$.

The closure of the alcove corresponding to $\Delta$ is

$$\bar{C} = \left\{ \sum_{i=0}^{n} x_i \omega_i^\gamma \mid x_i \geq 0, \sum_{i=0}^{n} a_i x_i = 1 \right\}$$

$$= \left\{ \sum_{i=0}^{n} x_i \omega_i^\gamma \mid x_i \geq 0, x_0 + x_1 + \sum_{i=2}^{n} 2x_i = 1 \right\}$$

$$= \left\{ \sum_{i=1}^{n} x_i \omega_i^\gamma \mid x_i \geq 0, 0 \leq x_1 + 2 \sum_{i=2}^{n} x_i \leq 1 \right\}.$$

Since $a_i = 1$ only for $i = 0, 1$ we have $\tilde{W}_C = \{ \rho_0, \rho_1 \}$ by (2), where $\rho_0$ is the identity element. We can see that Aut($\tilde{D}$) $\cong \mathbb{Z}/2\mathbb{Z}$, where the nontrivial element interchanges $\tilde{\alpha}_0$ and $\alpha_1$ in addition to fixing $\alpha_i$ for all $2 \leq i \leq n$. We have $\tilde{W}_C \cong$ Aut($\tilde{D}$).

From (3), we know $\rho_1 = (\omega^{\gamma}, \sigma_1)$ for some $\sigma_1 \in W$ which acts as signed permutations on the $\epsilon_j$, $1 \leq j \leq n$. We also know that $\rho_1$ must interchange $\tilde{\alpha}_0$ and $\alpha_1$ in addition to fixing $\alpha_i$ for all $2 \leq i \leq n$. Therefore, $\rho_1 \cdot v_i = v_i$ for all $2 \leq i \leq n$, $\rho_1 \cdot v_0 = v_1$ and $\rho_1 \cdot v_1 = v_0$. By (II), solving for $\sigma_1 \cdot v_i$ gives the system of linear equations

$$\begin{cases} 
\sigma_1 \cdot \epsilon_1 = -\epsilon_1 \\
\sigma_1 \cdot \left( \frac{1}{2} \sum_{j=1}^{i} \epsilon_j \right) = \frac{1}{2} \left( -\epsilon_1 + \sum_{j=2}^{i} \epsilon_j \right) \text{ for all } 2 \leq i \leq n
\end{cases}$$

We can deduce that $\sigma_1$ fixes $\epsilon_i$ for all $2 \leq i \leq n$ so $\sigma_1 = s_{\epsilon_1}$. 117
Let $x = \sum_{i=0}^{n} x_i \omega_i^\vee \in \bar{C}$. There are no nontrivial subgroups of $\bar{W}_C$ so the only case to consider is $\bar{W}_x = \bar{W}_C = \langle \rho_1 \rangle$. Therefore, we solve $\rho_1 \cdot x = x$ which gives

$$x_0\omega_1^\vee + x_1\omega_0^\vee + \sum_{i=2}^{n} x_i \omega_i^\vee = \sum_{i=0}^{n} x_i \omega_i^\vee.$$ 

This, together with $(*$), reduces to

$$x_1 = x_0 = 1 - \sum_{i=1}^{n} a_i x_i = 1 - x_1 - 2 \sum_{i=2}^{n} x_i.$$ 

Solving for $x_1$ gives

$$x_1 = \frac{1}{2} - \sum_{i=2}^{n} x_i.$$ 

As mentioned at the end of Section 4.1 and similar to the computations in Example 4.2.2, we have equations of the form $\alpha(\exp(x)) = e^{2\pi i \langle \alpha, x \rangle}$ for all $\alpha \in R$. It is relatively straightforward to solve the resulting system of equations. Thus, for $s = \exp(x)$, we have

$$s = \begin{bmatrix} s_{\theta_1} \\ \vdots \\ s_{\theta_n} \\ 1 \end{bmatrix}$$ 

with component group $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z}$ where

$$\theta_k = 2\pi i \sum_{j=k}^{n} x_j$$
for all $1 \leq k \leq n$. Note that

$$
\theta_1 = 2\pi i \sum_{j=1}^{n} x_j = 2\pi i \left( x_1 + \sum_{j=2}^{n} x_j \right) = 2\pi i \left( \frac{1}{2} - \sum_{j=2}^{n} x_j + \sum_{j=2}^{n} x_j \right) = \pi i
$$

so $s_{\theta_1} = -I$.

### 4.4 $PSp_{2n}(\mathbb{C})$

We will look at $G = PSp_{2n}(\mathbb{C}) = Sp_{2n}(\mathbb{C})/Z$ where $Z = \{ \pm I \}$ and $n \geq 2$. This is the adjoint, quasi-simple group of type $C_n$. We state several facts here without proof. The details can be found in [2], Chapter VI, Section 4.6. Let $T$ be the set of diagonal matrices in $G$. Then

$$
T = \{ \text{diag}(A, A^{-1})Z \mid A = \text{diag}(s_1, \ldots, s_n), s_j \in \mathbb{C}^\times, 1 \leq j \leq n \}
$$

which is a maximal torus of $G$ ([12], page 253). It is also not difficult to show that

$$
X^*(T) = \langle \pm \epsilon_j \pm \epsilon_i, \pm 2\epsilon_j \mid 1 \leq j \neq i \leq n \rangle
$$

and

$$
R = \{ \pm \epsilon_i \pm \epsilon_j \mid 1 \leq i \neq j \leq n \} \cup \{ \pm 2\epsilon_j \mid 1 \leq j \leq n \}
$$

where $\epsilon_j(\text{diag}(A, A^{-1})) = s_j$. We may take $\Delta = \{ \alpha_1, \ldots, \alpha_n \}$ where $\alpha_j = \epsilon_j - \epsilon_{j+1}$ for all $1 \leq j \leq n - 1$ and $\alpha_n = 2\epsilon_n$. The highest root is $\tilde{\alpha}_0 = \sum_{i=1}^{n-1} 2\alpha_i + \alpha_n$ which implies

$$
a_i = 2 \text{ for all } 1 \leq i \leq n - 1 \text{ and } a_n = 1. \tag{*}
$$
Thus \( v_i = \frac{1}{2} \omega_i^\vee \) for all \( 1 \leq i \leq n-1 \) and \( v_n = \omega_n^\vee \). The fundamental weights are given by

\[
\omega_i^\vee = \sum_{j=1}^{i-1} j \alpha_j^\vee + i \left( \sum_{j=i}^{n} \alpha_j^\vee \right)
\]

for all \( 1 \leq i \leq n-1 \) and

\[
\omega_n^\vee = \frac{1}{2} \left( \sum_{j=1}^{n} j \alpha_j^\vee \right).
\]

As in Section 4.2, we may (abusively) write

\[
\omega_i^\vee = \sum_{j=1}^{i} \epsilon_j \quad \text{(III)}
\]

for all \( 1 \leq i \leq n-1 \) and

\[
\omega_n^\vee = \frac{1}{2} \sum_{j=1}^{n} \epsilon_j. \quad \text{(IV)}
\]

The extended Dynkin diagram \( \tilde{D} \) is

\[
\tilde{\alpha}_0 \rightarrow \alpha_1 \rightarrow \alpha_2 \cdots \rightarrow \alpha_{n-2} \rightarrow \alpha_{n-1} \rightarrow \alpha_n
\]

Now, \( W \cong (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n \), where \( s_{\epsilon_i - \epsilon_j} \) interchanges \( \epsilon_i \) and \( \epsilon_j \) while \( s_{2\epsilon_i} \) interchanges \( \epsilon_i \) and \( -\epsilon_i \) for all \( 1 \leq i \neq j \leq n \) ([7], Section 12.2, Table 1). Note that the conjugation action \( s_{\epsilon_i - \epsilon_j} s_{2\epsilon_j} s_{\epsilon_i - \epsilon_j} = s_{2\epsilon_i} \) makes \( W \) a semidirect product. Then \( \tilde{W} \cong P^\vee \rtimes ((\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n) \).
The closure of the alcove corresponding to $\Delta$ is

$$
\bar{C} = \left\{ \sum_{i=0}^{n} x_i \omega_i^\lor | x_i \geq 0, \sum_{i=0}^{n} a_i x_i = 1 \right\}
= \left\{ \sum_{i=0}^{n} x_i \omega_i^\lor | x_i \geq 0, x_0 + x_n + \sum_{i=1}^{n-1} 2x_i = 1 \right\}
= \left\{ \sum_{i=1}^{n} x_i \omega_i^\lor | x_i \geq 0, 0 \leq x_n + 2 \sum_{i=1}^{n-1} x_i \leq 1 \right\}.
$$

Since $a_i = 1$ only for $i = 0, n$ we have $\tilde{W}_C = \{\rho_0, \rho_n\}$ by (2), where $\rho_0$ is the identity element. We can see that Aut($\tilde{D}$) $\cong \mathbb{Z}/2\mathbb{Z}$ where the nontrivial element interchanges $\alpha_i$ and $\alpha_{n-i}$ for all $1 \leq i \leq n - 1$ in addition to interchanging $\tilde{\alpha}_0$ and $\alpha_n$. We have $\tilde{W}_C \cong$ Aut($\tilde{D}$).

From (3), we know $\rho_n = (\omega_n^\lor, \sigma_n)$ for some $\sigma_n \in W$ which acts as signed permutations on the $\epsilon_j$, $1 \leq j \leq n$. We also know that $\rho_n$ must interchange $\alpha_i$ and $\alpha_{n-i}$ for all $1 \leq i \leq n - 1$ in addition to interchanging $\tilde{\alpha}_0$ and $\alpha_n$. Therefore, $\rho_n \cdot v_i = v_{n-i}$ for all $0 \leq i \leq n$. By (III) and (IV), solving for $\sigma_n \cdot v_i$ gives the system of linear equations

$$
\begin{cases}
\sigma_n \cdot \left( \frac{1}{2} \sum_{j=1}^{i} \epsilon_j \right) = -\frac{1}{2} \sum_{j=n-i+1}^{n} \epsilon_j & \text{for all } 1 \leq i \leq n - 1 \\
\sigma_n \cdot \left( \frac{1}{2} \sum_{j=1}^{n} \epsilon_j \right) = -\frac{1}{2} \sum_{j=1}^{n} \epsilon_j.
\end{cases}
$$

We can deduce that $\sigma_n \cdot \epsilon_i = -\epsilon_{n-i+1}$ for all $1 \leq i \leq n$. It follows that we have

$$
\sigma_n = \prod_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} s_{\epsilon_i} s_{\epsilon_{n-i+1}} s_{\epsilon_i - \epsilon_{n-i+1}}.
$$
Let \( x = \sum_{i=0}^{n} x_i \omega_i^\vee \in \bar{C} \). The only case to consider is \( \bar{W}_x = \bar{W}_C = \langle \rho_n \rangle \).

Therefore, we solve \( \rho_n \cdot x = x \) which gives

\[
\sum_{i=0}^{n} x_{n-i} \omega_i^\vee = \sum_{i=0}^{n} x_i \omega_i^\vee.
\]

This reduces to \( x_i = x_{n-i} \) for all \( 0 \leq i \leq n \). By (\(*\)), we have

\[
x_n = x_0 = 1 - \sum_{i=1}^{n} a_i x_i = 1 - 2 \sum_{i=1}^{n-1} x_i - x_n.
\]

Solving for \( x_n \) gives

\[
x_n = \frac{1}{2} - \sum_{i=1}^{n-1} x_i.
\]

As mentioned at the end of Section 4.1 and similar to the computations in Example 4.2.2, we have equations of the form \( \alpha(\exp(x)) = e^{2\pi i \langle \alpha, x \rangle} \) for all \( \alpha \in R \). It is relatively straightforward to solve the resulting system of equations. Thus, for \( s = \exp(x) \), we have

\[
s = \begin{bmatrix} A & 0 \\ 0 & A^{-1} \end{bmatrix} Z
\]

with component group \( Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z} \) where

\[
A = \begin{bmatrix} i \\ i e^{-\pi i x_1} \\ \ddots \\ i e^{-\pi i \sum_{j=1}^{n-1} x_j} \end{bmatrix}.
\]
4.5 \textit{PSO}_{2n}(C)

We will look at $G = \text{PSO}_{2n}(C) = \text{SO}_{2n}(C)/\mathbb{Z}$ where $\mathbb{Z} = \{\pm I\}$ and $n \geq 4$. This is the adjoint, quasi-simple group of type $D_n$. We state several facts here without proof. The details can be found in [2], Chapter VI, Section 4.8. Recall the $2 \times 2$ matrices $s_\theta$ from Section 4.3. Then

$$T = \{\text{diag}(s_{\theta_1}, \ldots, s_{\theta_n}) \mathbb{Z} \mid \theta_j \in \mathbb{C}, 1 \leq j \leq n\}$$

is a maximal torus of $G$ ([12], page 253). Also, similarly to Section 4.3, we have

$$X^*(T) = < \pm \epsilon_j \pm \epsilon_i \mid 1 \leq j \neq i \leq n >$$

and

$$R = \{\pm \epsilon_i \pm \epsilon_j \mid 1 \leq i \neq j \leq n\}$$

where $\epsilon_j(\text{diag}(s_{\theta_1}, \ldots, s_{\theta_n})) = e^{\theta_j}$. We may take $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ where $\alpha_j = \epsilon_j - \epsilon_{j+1}$ for all $1 \leq j \leq n - 1$ and $\epsilon_n = \epsilon_{n-1} + \epsilon_n$. The highest root is $\tilde{\alpha}_0 = \alpha_1 + \sum_{i=2}^{n-2} 2\alpha_i + \alpha_{n-1} + \alpha_n$ which implies

$$a_1 = a_{n-1} = a_n = 1 \text{ and } a_i = 2 \text{ for all } 2 \leq i \leq n - 2. \tag{*}$$

Thus $v_j = \omega_i$ for $i = 1, n-1, n$ and $v_i = \frac{1}{2}\omega_i$ for all $2 \leq i \leq n - 2$. The fundamental weights are given by

$$\omega_i = \sum_{j=1}^{i-1} j\alpha_j + i \left( \sum_{j=1}^{n-2} \alpha_j \right) + \frac{1}{2} i(\alpha_{n-1} + \alpha_n)$$
for all $1 \leq i \leq n-2$, 

$$
\omega^\vee_{n-1} = \frac{1}{2} \left( \sum_{j=1}^{n-2} j\alpha^\vee_j + n\alpha^\vee_{n-1} + (n-2)\alpha^\vee_n \right)
$$

and

$$
\omega^\vee_{n-1} = \frac{1}{2} \left( \sum_{j=1}^{n-2} j\alpha^\vee_j + (n-2)\alpha^\vee_{n-1} + n\alpha^\vee_n \right).
$$

As in Section 4.2, we may (abusively) write

$$
\omega^\vee_i = \sum_{j=1}^{i} \epsilon_j
$$

(V)

for all $1 \leq i \leq n-2$,

$$
\omega^\vee_{n-1} = \frac{1}{2} \left( \sum_{j=1}^{n-1} \epsilon_j - \epsilon_n \right)
$$

(VI)

and

$$
\omega^\vee_n = \frac{1}{2} \left( \sum_{j=1}^{n} \epsilon_j \right).
$$

(VII)

The extended Dynkin diagram $\tilde{D}$ is

Now $W \cong (\mathbb{Z}/2\mathbb{Z})^{n-1} \times S_n$, where $s_{\epsilon_i - \epsilon_j}$ interchanges $\epsilon_i$ and $\epsilon_j$ while $s_{\epsilon_i + \epsilon_j}$ sends $\epsilon_i$ to $-\epsilon_j$ and $\epsilon_j$ to $-\epsilon_i$ for all $1 \leq i \neq j \leq n$ ([7], Section 12.2, Table 1). Note that
the conjugation action $s_{\epsilon_i-\epsilon_j}s_{\epsilon_j}s_{\epsilon_i-\epsilon_j} = s_{\epsilon_i}$ makes $W$ a semidirect product. Then $W \cong P^\vee \rtimes ((\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes S_n)$.

The closure of the alcove corresponding to $\Delta$ is

$$\bar{C} = \left\{ \sum_{i=0}^{n} x_i \omega_i^\vee \mid x_i \geq 0, \sum_{i=0}^{n} a_i x_i = 1 \right\}$$

$$= \left\{ \sum_{i=0}^{n} x_i \omega_i^\vee \mid x_i \geq 0, x_0 + x_1 + x_{n-1} + x_n + \sum_{i=2}^{n} 2x_i = 1 \right\}$$

$$= \left\{ \sum_{i=1}^{n} x_i \omega_i^\vee \mid x_i \geq 0, 0 \leq x_1 + x_{n-1} + x_n + 2 \sum_{i=2}^{n} x_i \leq 1 \right\}.$$ 

Since $a_i = 1$ only for $i = 0, 1, n - 1, n$ we have $W_C = \{\rho_0, \rho_1, \rho_{n-1}, \rho_n\}$ by (2) where $\rho_0$ is the identity element. If $n = 4$ then $\text{Aut}(\bar{\tilde{D}}) \cong S_4$ which acts by permutations on the vertices that fix $\alpha_2$. If $n \neq 4$ then $\text{Aut}(\bar{\tilde{D}}) = \langle \eta_1, \eta_2, \eta_3 \rangle$ where $\eta_1$ interchanges $\tilde{\alpha}_0$ and $\alpha_1$; $\eta_2$ interchanges $\alpha_i$ and $\alpha_{n-i}$ for all $1 \leq i \leq n - 1$ in addition to interchanging $\tilde{\alpha}_0$ and $\alpha_n$; and $\eta_3$ interchanges $\alpha_{n-1}$ and $\alpha_n$.

From (3), we know $\rho_1 = (\omega_1^\vee, \sigma_1), \rho_{n-1} = (\omega_{n-1}^\vee, \sigma_{n-1})$ and $\rho_n = (\omega_n^\vee, \sigma_n)$ for some $\sigma_1, \sigma_{n-1}, \sigma_n \in W$ which act as signed permutations on the $\epsilon_j$, $1 \leq j \leq n$. We have two cases to consider; $n$ even and $n$ odd.

Suppose $n$ is even. Then $P^\vee/Q^\vee \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ([2], Chapter VI, Section 4.8). We know $\rho_{n-1}$ must send $\tilde{\alpha}_0$ to $\alpha_{n-1}$ and is of order 2. Thus $\rho_{n-1}$ must interchange $\tilde{\alpha}_0$ and $\alpha_{n-1}$. Looking at $\bar{\tilde{D}}$, this implies $\rho_{n-1}$ must also interchange $\alpha_i$ and $\alpha_{n-i}$. 125
for all $2 \leq i \leq n - 2$. Moreover $\rho_{n-1}$ must interchange $\alpha_n$ and $\alpha_1$. Therefore $\rho_{n-1}$ interchanges $v_0$ and $v_{n-1}$; $v_1$ and $v_n$; and $v_i$ and $v_{n-i}$ for all $2 \leq i \leq n - 2$. By (V), (VI) and (VII), solving for $\sigma_{n-1} \cdot v_i$ gives the system of linear equations

$$\begin{align*}
\sigma_{n-1} \cdot \epsilon_1 &= \epsilon_n \\
\sigma_{n-1} \cdot \left( \frac{1}{2} \sum_{j=1}^{i} \epsilon_j \right) &= \frac{1}{2} \left( - \sum_{j=n-i+1}^{n-1} \epsilon_j + \epsilon_n \right) \quad \text{for all } 2 \leq i \leq n - 2 \\
\sigma_{n-1} \cdot \left( \frac{1}{2} \left( \sum_{j=1}^{n-1} \epsilon_j - \epsilon_n \right) \right) &= \frac{1}{2} \left( - \sum_{j=1}^{n-1} \epsilon_j + \epsilon_n \right) \\
\sigma_{n-1} \cdot \left( \frac{1}{2} \sum_{j=1}^{n} \epsilon_j \right) &= \frac{1}{2} \left( \epsilon_1 - \sum_{j=2}^{n-1} \epsilon_j + \epsilon_n \right)
\end{align*}$$

We can deduce that $\sigma_{n-1} \cdot \epsilon_i = -\epsilon_{n-i+1}$ for all $2 \leq i \leq n - 2$ and $\sigma_{n-1} \cdot \epsilon_i = \epsilon_{n-i+1}$ for $i = 1, n$ so

$$\sigma_{n-1} = s_{\epsilon_1-\epsilon_n} \prod_{i=2}^{n} s_{\epsilon_i+\epsilon_{n-i+1}}.$$  

Similarly, $\rho_n$ interchanges $\tilde{\alpha}_0$ and $\alpha_n$. Thus $\rho_n$ interchanges $\alpha_i$ and $\alpha_{n-i}$ for all $1 \leq i \leq n - 1$. Therefore $\rho_n$ interchanges $v_i$ and $v_{n-i}$ for all $0 \leq i \leq n$. By (V), (VI) and (VII), solving for $\sigma_n \cdot v_i$ gives the system of linear equations

$$\begin{align*}
\sigma_n \cdot \epsilon_1 &= -\epsilon_n \\
\sigma_n \cdot \left( \frac{1}{2} \sum_{j=1}^{i} \epsilon_j \right) &= -\frac{1}{2} \sum_{j=n-i+1}^{n} \epsilon_j \quad \text{for all } 2 \leq i \leq n - 2 \\
\sigma_n \cdot \left( \frac{1}{2} \left( \sum_{j=1}^{n-1} \epsilon_j - \epsilon_n \right) \right) &= \frac{1}{2} \left( \epsilon_1 - \sum_{j=2}^{n-1} \epsilon_j \right) \\
\sigma_n \cdot \left( \frac{1}{2} \sum_{j=1}^{n} \epsilon_j \right) &= -\frac{1}{2} \sum_{j=1}^{n} \epsilon_j
\end{align*}$$

We can deduce that $\sigma_n \cdot \epsilon_i = -\epsilon_{n-i+1}$ for all $1 \leq i \leq n$ so

$$\sigma_n = \prod_{i=1}^{n} s_{\epsilon_i+\epsilon_{n-i+1}}.$$  

Note that $\tilde{W}_C = \langle \rho_{n-1}, \rho_n \rangle$ and $\rho_1 = \rho_{n-1} \rho_n$. Let $x = \sum_{i=0}^{n} x_i \omega_i^\vee \in \tilde{C}$. We have four cases to consider: $\tilde{W}_x = \langle \rho_{n-1} \rangle$, $\tilde{W}_x = \langle \rho_n \rangle$, $\tilde{W}_x = \langle \rho_{n-1} \rho_n \rangle$ and

126
\( \tilde{W}_x = \tilde{W}_C. \)

Consider \( \tilde{W}_x = < \rho_{n-1} > \). We solve \( \rho_{n-1} \cdot x = x \) which gives

\[
x_0 \omega_{n-1}^\vee + x_1 \omega_n^\vee + \sum_{i=2}^{n-2} x_i \omega_{n-i}^\vee + x_{n-1} \omega_0^\vee + x_n \omega_1^\vee = \sum_{i=0}^{n} x_i \omega_i^\vee.
\] (5)

This reduces to

\[
x_{n-1} = x_0, \quad x_1 = x_n, \quad x_i = x_{n-i} \text{ for all } 2 \leq i \leq n - 2.
\] (6)

By (⋆),

\[
x_{n-1} = x_0 = 1 - \sum_{i=1}^{n} a_i x_i = 1 - x_1 - 2 \sum_{i=2}^{n-2} x_i - x_{n-1} - x_n.
\]

Solving for \( x_{n-1} \) gives

\[
x_{n-1} = \frac{1}{2} - \sum_{i=1}^{n-2} x_i = \frac{1}{2} - x_1 - 2 \sum_{i=2}^{n-1} x_i - x_n^\frac{n}{2}.
\]

As mentioned at the end of Section 4.1 and similar to the computations in Example 4.2.2, we have equations of the form \( \alpha(\exp(x)) = e^{2\pi i < \alpha, x >} \) for all \( \alpha \in \mathbb{R} \). It is relatively straightforward to solve the resulting system of equations. Thus, for \( s = \exp(x) \), we have

\[
s = \begin{bmatrix} s_{\theta_1} \\ \vdots \\ s_{\theta_n} \end{bmatrix} Z
\]
with component group $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z}$ where

$$
\theta_k = \begin{cases} 
\pi i \left( 2 \sum_{j=k}^{n-2} x_j + x_{n-1} + x_n \right), & 1 \leq k \leq n-1 \\
\pi i (-x_{n-1} + x_n), & k = n
\end{cases}
$$

which reduces to

$$
\theta_k = \begin{cases} 
\pi i \left( \frac{1}{2} + x_1 + \sum_{j=1}^{n-2} x_j \right), & k = 1 \\
\pi i \left( \frac{1}{2} - \sum_{j=2}^{k-1} x_j + \sum_{j=k}^{n-2} x_j \right), & 1 < k \leq n-1 \\
\pi i \left( \frac{1}{2} + x_1 + \sum_{j=1}^{n-2} x_j \right), & k = n.
\end{cases}
$$

Consider $\tilde{W}_x = \langle \rho_n \rangle$. We solve $\rho_n \cdot x = x$ which gives

$$
x_0 \omega_n^\vee + x_1 \omega_{n-1}^\vee + \sum_{i=2}^{n-2} x_i \omega_{n-i}^\vee + x_{n-1} \omega_1^\vee + x_n \omega_0^\vee = \sum_{i=0}^{n} x_i \omega_i^\vee.
$$

This reduces to

$$
x_n = x_0, \ x_1 = x_{n-1}, \ x_i = x_{n-i} \text{ for all } 2 \leq i \leq n-2.
$$

By $(\star)$,

$$
x_n = x_0 = 1 - x_1 - 2 \sum_{i=2}^{n-2} x_i - x_{n-1} - x_n.
$$
Solving for $x_n$ gives

$$x_n = \frac{1}{2} - \sum_{i=1}^{n-2} x_i = \frac{1}{2} - x_1 - 2 \sum_{i=2}^{n-1} x_i - x_n.$$ 

We solve the system of equations $\alpha(\exp(x)) = e^{2\pi i <\alpha, x>}$ for all $\alpha \in R$. Thus, for $s = \exp(x)$, we have

$$s = \begin{bmatrix}
  s_{\theta_1} \\
  \vdots \\
  s_{\theta_n}
\end{bmatrix} Z$$

with component group $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z}$ where

$$\theta_k = \begin{cases}
  \pi i \left( 2 \sum_{j=k}^{n-2} x_j + x_{n-1} + x_n \right), & 1 \leq k \leq n-1 \\
  \pi i (-x_{n-1} + x_n), & k = n.
\end{cases}$$

Similarly to the previous case, this reduces to

$$\theta_k = \begin{cases}
  \pi i \left( \frac{1}{2} + 2 \sum_{j=1}^{k-1} x_j + x_{\frac{n}{2}} \right), & k = 1 \\
  \pi i \left( \frac{1}{2} + \sum_{j=k}^{n-k} x_j \right), & 1 < k \leq \frac{n}{2} \\
  \pi i \left( \frac{1}{2} - \sum_{j=n-k+1}^{n-1} x_j \right), & \frac{n}{2} < k \leq n-1 \\
  \pi i \left( \frac{1}{2} - 2 \sum_{j=1}^{\frac{n}{2}-1} x_j - x_{\frac{n}{2}} \right), & k = n.
\end{cases}$$

Consider $\bar{W}_x = <\rho_{n-1}\rho_n>$. We solve $\rho_{n-1}\rho_n \cdot x = x$ which gives

$$x_0\omega_1 + x_1\omega_0 + \sum_{i=2}^{n-2} x_i\omega_i + x_{n-1}\omega_n + x_n\omega_{n-1} = \sum_{i=0}^{n} x_i\omega_i.$$
This reduces to

\[ x_1 = x_0, \ x_{n-1} = x_n \]

By (⋆),

\[ x_1 = x_0 = 1 - x_1 - 2 \sum_{i=2}^{n-2} x_i - x_{n-1} - x_n. \]

Solving for \( x_1 \) gives

\[ x_1 = \frac{1}{2} - \sum_{i=2}^{n-1} x_i. \]

We solve the system of equations \( \alpha(\exp(x)) = e^{2\pi i <\alpha,x>} \) for all \( \alpha \in \mathbb{R} \). Thus, for \( s = \exp(x) \), we have

\[
s = \begin{bmatrix} s_{\theta_1} & \ddots & \cr \vdots & \ddots & \cr s_{\theta_n} & \end{bmatrix} Z
\]

with component group \( Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z} \) where

\[
\theta_k = \begin{cases} 
\pi i \left( 2 \sum_{j=k}^{n-2} x_j + x_{n-1} + x_n \right), & 1 \leq k \leq n - 1 \\
\pi i (-x_{n-1} + x_n), & k = n
\end{cases}
\]

which reduces to

\[
\theta_k = \begin{cases}
\pi i, & k = 1 \\
2\pi i \sum_{j=k}^{n-1} x_j, & 1 < k \leq n - 1 \\
0, & k = n.
\end{cases}
\]
Lastly, consider $\tilde{W}_x = \tilde{W}_C$. We solve $\rho_{n-1} \cdot x = x$ and $\rho_n \cdot x = x$ simultaneously. This gives (5) and (7) which reduce to (6) and (8). Therefore, we have

$$x_1 = x_{n-1} = x_n = x_0, x_i = x_{n-i} \text{ for all } 2 \leq i \leq n - 2.$$ 

By (⋆),

$$x_1 = x_{n-1} = x_n = x_0 = 1 - x_1 - 2 \sum_{i=2}^{n-2} x_i - x_{n-1} - x_n.$$ 

Solving for $x_1$ gives

$$x_1 = x_{n-1} = x_n = \frac{1}{4} - \frac{1}{2} \sum_{i=2}^{n-2} x_i = \frac{1}{4} - \sum_{i=2}^{n-1} x_i = \frac{1}{2} x_n.$$ 

We solve the system of equations $\alpha(\exp(x)) = e^{2\pi i \langle \alpha, x \rangle}$ for all $\alpha \in R$. Thus, for $s = \exp(x)$, we have

$$s = \begin{bmatrix} s_{\theta_1} \\ \vdots \\ s_{\theta_n} \end{bmatrix} Z$$

with component group $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where

$$\theta_k = \begin{cases} 
\pi i \left( 2 \sum_{j=k}^{n-2} x_j + x_{n-1} + x_n \right), & 1 \leq k \leq n - 1 \\
\pi i (-x_{n-1} + x_n), & k = n 
\end{cases}$$
which reduces to

\[
\theta_k = \begin{cases} 
\pi i, & k = 1 \\
\pi i \left( \frac{1}{2} + \sum_{j=k}^{n-k} x_j \right), & 1 < k \leq \frac{n}{2} \\
\pi i \left( \frac{1}{2} - \sum_{j=n-k+1}^{k-1} x_j \right), & \frac{n}{2} < k \leq n - 1 \\
0, & k = n.
\end{cases}
\]

Now suppose \( n \) is odd. Then \( P'/Q' \cong \mathbb{Z}/4\mathbb{Z} \) ([2], Chapter VI, Section 4.8). We know \( \rho_1 \) must send \( \tilde{\alpha}_0 \) to \( \alpha_1 \). This implies \( \rho_1 \) interchanges \( \tilde{\alpha}_0 \) and \( \alpha_1 \) in addition to interchanging \( \alpha_{n-1} \) and \( \alpha_n \). Hence \( \rho_1 \) has order 2. There is only one element of \( \tilde{W}_C \) with order 2 so \( \rho_n \) must have order 4. We know \( \rho_1 \) must send \( \tilde{\alpha}_0 \) to \( \alpha_n \). Therefore \( \rho_1 \) must send \( \alpha_{n-1} \) to \( \tilde{\alpha}_0 \), \( \alpha_n \) to \( \alpha_1 \), and \( \alpha_i \) to \( \alpha_{n-i} \) for all \( 0 \leq i \leq n-2 \). Therefore sends \( v_{n-1} \) to \( v_0 \), \( v_n \) to \( v_1 \), and \( v_i \) to \( v_{n-i} \) for all \( 0 \leq i \leq n-2 \). By (V), (VI) and (VII), solving for \( \sigma_n \cdot v_i \) gives the system of linear equations

\[
\begin{cases} 
\sigma_n \cdot \epsilon_1 = -\epsilon_n \\
\sigma_n \cdot \left( \frac{1}{2} \sum_{j=1}^{i} \epsilon_j \right) = -\frac{1}{2} \sum_{j=n-i+1}^{n} \epsilon_j \text{ for all } 2 \leq i \leq n-2 \\
\sigma_n \cdot \left( \frac{1}{2} \left( \sum_{j=1}^{n-1} \epsilon_j - \epsilon_n \right) \right) = -\frac{1}{2} \sum_{j=1}^{n} \epsilon_j \\
\sigma_n \cdot \left( \frac{1}{2} \sum_{j=1}^{n} \epsilon_j \right) = \frac{1}{2} \left( \epsilon_1 - \sum_{j=2}^{n} \epsilon_j \right)
\end{cases}
\]

We can deduce that \( \sigma_n \cdot \epsilon_1 = -\epsilon_n \), \( \sigma_n \cdot \epsilon_i = -\epsilon_{n-i+1} \) for all \( 2 \leq i \leq n-1 \), and \( \sigma_n \cdot \epsilon_n = \epsilon_1 \) so \( \sigma_n = s_{\epsilon_1 + \epsilon_n} s_{\epsilon_{\frac{n}{2}+1} - \epsilon_n} s_{\epsilon_{\frac{n}{2}+1} + \epsilon_n} \prod_{i=2}^{\frac{n}{2}} s_{\epsilon_i + \epsilon_{n-i+1}} \).

Since \( \tilde{W}_C = < \rho_n > \) is of order 4, we have two cases to consider: \( \tilde{W}_x = \tilde{W}_C \) and

132
Consider \( \tilde{W}_x = \tilde{W}_C \). We solve \( \rho_n \cdot x = x \) which gives

\[
x_0\omega_n^\vee + x_1\omega_{n-1}^\vee + \sum_{i=2}^{n-2} x_i\omega_{n-i}^\vee + x_{n-1}\omega_0^\vee + x_n\omega_1^\vee = \sum_{i=0}^n x_i\omega_i^\vee.
\]

This reduces to

\[
x_1 = x_{n-1} = x_n = 0, \quad x_i = x_{n-i} \text{ for all } 2 \leq i \leq n - 2.
\]

By \( (\ast) \),

\[
x_1 = x_{n-1} = x_n = 1 - x_1 - 2\sum_{i=2}^{n-2} x_i - x_{n-1} - x_n.
\]

Solving for \( x_1 \) gives

\[
x_1 = x_{n-1} = x_n = \frac{1}{4} - \frac{1}{2}\sum_{i=2}^{n-2} x_i = \frac{1}{4} - \frac{\lfloor \frac{n}{2} \rfloor}{2}\sum_{i=2}^{n} x_i.
\]

We solve the system of equations \( \alpha(\exp(x)) = e^{2\pi i \langle \alpha, x \rangle} \) for all \( \alpha \in R \). Thus, for \( s = \exp(x) \), we have

\[
s = \begin{bmatrix}
  s_{\theta_1} \\
  \vdots \\
  s_{\theta_n}
\end{bmatrix} Z
\]

with component group \( Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/4\mathbb{Z} \) where

\[
\theta_k = \begin{cases} 
  \pi i \left( 2 \sum_{j=k}^{n-2} x_j + x_{n-1} + x_n \right), & 1 \leq k \leq n - 1 \\
  \pi i (-x_{n-1} + x_n), & k = n.
\end{cases}
\]

133
Similarly to the last case for $n$ even, this reduces to

$$\theta_k = \begin{cases} 
\pi i, & k = 1 \\
\pi i \left( \frac{1}{2} + \sum_{j=k}^{n-k} x_j \right), & 2 \leq k \leq \left\lfloor \frac{n}{2} \right\rfloor \\
\frac{\pi i}{2}, & k = \left\lfloor \frac{n}{2} \right\rfloor + 1 \\
\pi i \left( \frac{1}{2} - \sum_{j=n-k+1}^{k-1} x_j \right), & \left\lfloor \frac{n}{2} \right\rfloor + 1 < k \leq n - 1 \\
0, & k = n.
\end{cases}$$

Consider $\tilde{W}_x = <\rho_n^2>$. We solve $\rho_n^2 \cdot x = x$ which gives

$$x_0\omega_1^\vee + x_1\omega_0^\vee + \sum_{i=2}^{n-2} x_i\omega_i^\vee + x_{n-1}\omega_n^\vee + x_n\omega_{n-1}^\vee = \sum_{i=0}^{n} x_i\omega_i^\vee.$$ 

This reduces to

$$x_1 = x_0, \quad x_{n-1} = x_n.$$

By (⋆),

$$x_1 = 1 - x_1 - 2 \sum_{i=2}^{n-2} x_i - x_{n-1} - x_n.$$

Solving for $x_1$ gives

$$x_1 = \frac{1}{2} - \sum_{i=2}^{n-1} x_i.$$

We solve the system of equations $\alpha(\exp(x)) = e^{2\pi i <\alpha,x>}$ for all $\alpha \in R$. Thus, for
\[ s = \exp(x), \text{ we have} \]

\[
\begin{bmatrix}
  s_{\theta_1} \\
  \ddots \\
  \vdots \\
  s_{\theta_n}
\end{bmatrix}
\]

with component group \( Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z} \) where

\[
\theta_k = \begin{cases} 
\pi i \left( 2 \sum_{j=k}^{n-2} x_j + x_{n-1} + x_n \right), & 1 \leq k \leq n - 1 \\
\pi i (-x_{n-1} + x_n), & k = n
\end{cases}
\]

which reduces to

\[
\theta_k = \begin{cases} 
\pi i, & k = 1 \\
2\pi i \sum_{j=k}^{n-1} x_j, & 1 < k \leq n - 1 \\
0, & k = n.
\end{cases}
\]

4.6 \( E_6 \)

We will look at the case of a quasi-simple, adjoint group of type \( E_6 \). We state several facts here without proof. Unlike Sections 4.2-4.5, we do not offer any matrix representation for this group. The smallest matrix group in which \( E_6 \) can be described is \( GL_{27}(\mathbb{C}) \). Doing the necessary computations with such matrices is far to cumbersome and offers no benefit here. The details can be found in [2], Chapter VI, Section 4.12.
The roots are given by

\[ R = \{ \pm \epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq 5 \} \]

\[ \cup \left\{ \pm \frac{1}{2} \left( \epsilon_8 - \epsilon_7 - \epsilon_6 + \sum_{i=1}^5 (-1)^{\nu(i)} \epsilon_i \right) \mid \sum_{i=1}^5 \nu(i) \equiv 0 \mod 2 \right\}. \]

We may take

\[ \Delta = \{ \alpha_1, \ldots, \alpha_6 \} \]

\[ = \left\{ \frac{1}{2} \left( \epsilon_1 + \epsilon_8 - \sum_{i=2}^7 \epsilon_i \right), \epsilon_1 + \epsilon_2, \epsilon_2 - \epsilon_1, \epsilon_3 - \epsilon_2, \epsilon_4 - \epsilon_3, \epsilon_5 - \epsilon_4 \right\} \]

and the highest root is given by \( \tilde{\alpha}_0 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6 \). Thus

\[ a_1 = a_6 = 1, \; a_2 = a_3 = a_5 = 2, \; a_4 = 3, \]

and

\[ v_1 = \omega_1^\vee, \; v_2 = \frac{1}{2} \omega_2^\vee, \; v_3 = \frac{1}{2} \omega_3^\vee, \; v_4 = \frac{1}{3} \omega_4^\vee, \; v_5 = \frac{1}{2} \omega_5^\vee, \; v_6 = \omega_6^\vee. \]

The fundamental weights are given by

\[ \omega_1^\vee = \frac{1}{4} (4\alpha_1^\vee + 3\alpha_2^\vee + 5\alpha_3^\vee + 5\alpha_4^\vee + 4\alpha_5^\vee + 2\alpha_6^\vee), \]

\[ \omega_2^\vee = \alpha_1^\vee + 2\alpha_2^\vee + 2\alpha_3^\vee + 3\alpha_4^\vee + 2\alpha_5^\vee + \alpha_6^\vee, \]

\[ \omega_3^\vee = \frac{1}{3} (5\alpha_1^\vee + 6\alpha_2^\vee + 10\alpha_3^\vee + 12\alpha_4^\vee + 8\alpha_5^\vee + 4\alpha_6^\vee), \]

136
\[\omega_4^\vee = 2\alpha_1^\vee + 3\alpha_2^\vee + 4\alpha_3^\vee + 6\alpha_4^\vee + 4\alpha_5^\vee + 2\alpha_6^\vee,\]

\[\omega_5^\vee = \frac{1}{3}(4\alpha_1^\vee + 6\alpha_2^\vee + 8\alpha_3^\vee + 12\alpha_4^\vee + 10\alpha_5^\vee + 5\alpha_6^\vee),\]

\[\omega_6^\vee = \frac{1}{3}(2\alpha_1^\vee + 3\alpha_2^\vee + 4\alpha_3^\vee + 6\alpha_4^\vee + 5\alpha_5^\vee + 4\alpha_6^\vee).\]

As in Section 4.2, we may (abusively) write

\[\omega_1^\vee = \frac{2}{3}(\epsilon_8 - \epsilon_7 - \epsilon_6),\]

\[\omega_2^\vee = \frac{1}{2}(\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5 - \epsilon_6 - \epsilon_7 + \epsilon_8),\]

\[\omega_3^\vee = \frac{5}{6}(\epsilon_8 - \epsilon_7 - \epsilon_6) + \frac{1}{2}(-\epsilon_2 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5),\]

\[\omega_4^\vee = \epsilon_3 + \epsilon_4 + \epsilon_5 - \epsilon_6 - \epsilon_7 + \epsilon_8,\]

\[\omega_5^\vee = \frac{2}{3}(\epsilon_8 - \epsilon_7 - \epsilon_6) + \epsilon_4 + \epsilon_5,\]

\[\omega_6^\vee = \frac{1}{3}(\epsilon_8 - \epsilon_7 - \epsilon_6) + \epsilon_5.\]

The extended Dynkin diagram \(\tilde{D}\) is

![Dynkin Diagram](image)
Now, the closure of the alcove corresponding to $\Delta$ is

$$\bar{C} = \left\{ \sum_{i=0}^{n} x_i \omega_i^\vee | x_i \geq 0, \sum_{i=0}^{n} a_i x_i = 1 \right\}$$

$$= \left\{ \sum_{i=0}^{n} x_i \omega_i^\vee | x_i \geq 0, x_0 + x_1 + 2x_2 + 2x_3 + 3x_4 + 2x_5 + x_6 = 1 \right\}$$

$$= \left\{ \sum_{i=1}^{n} x_i \omega_i^\vee | x_i \geq 0, 0 \leq x_1 + 2x_2 + 2x_3 + 3x_4 + 2x_5 + x_6 \leq 1 \right\}.$$ 

Since $a_i = 1$ only for $i = 0, 1, 6$, we have $\bar{W}_C = \{ \rho_0, \rho_1, \rho_6 \}$ by (2), where $\rho_0$ is the identity element. We can see that $\text{Aut}(\tilde{D}) \cong \mathbb{Z}/3\mathbb{Z} \times \{1, -1\}$ where $\mathbb{Z}/3\mathbb{Z}$ acts by rotations and $\{1, -1\}$ acts by a reflection. Since $\tilde{W}_C$ has order 3, we must have $\tilde{W}_C \cong \mathbb{Z}/3\mathbb{Z}$ which acts on $\tilde{D}$ by rotations. By (3), $\rho_1 = (\omega_1^\vee, \sigma_1)$ for some $\sigma_1 \in W$.

We also know that $\rho_1$ sends $\tilde{\alpha}_0$ to $\alpha_1$ since $\rho_1 \cdot v_0 = v_1$. Therefore $\rho_1$ acts as the clockwise rotation on $\tilde{D}$; i.e.

$$\rho_1 \cdot \alpha_1 = \alpha_6, \rho_1 \cdot \alpha_6 = \tilde{\alpha}_0, \rho_1 \cdot \alpha_2 = \alpha_3, \rho_1 \cdot \alpha_3 = \alpha_5, \rho_1 \cdot \alpha_5 = \alpha_2, \rho_1 \cdot \alpha_4 = \alpha_4,$$

$$\rho_1 \cdot v_1 = v_6, \rho_1 \cdot v_6 = v_0, \rho_1 \cdot v_2 = v_3, \rho_1 \cdot v_3 = v_5, \rho_1 \cdot v_5 = v_2, \rho_1 \cdot v_4 = v_4.$$ 

This is sufficient for determining the action of $\rho_1$ on a given $x \in \tilde{C}$. Note that $\rho_1$ has order 3 so $\bar{W}_C = \langle \rho_1 \rangle$.

Let $x = \sum_{i=0}^{n} x_i \omega_i^\vee \in \tilde{C}$. There are no nontrivial subgroups of $\bar{W}_C$ so the only
case to consider is $\tilde{W}_x = \tilde{W}_C = <\rho_1>$. Therefore, we solve $\rho_1 \cdot x = x$ which gives

$$x_1 = x_6 = x_0, \; x_2 = x_3 = x_5.$$

We also have

$$x_0 = 1 - x_1 - 2x_2 - 2x_3 - 3x_4 - 2x_5 - x_6$$

so

$$x_1 = x_6 = \frac{1}{3} - \frac{2}{3}(x_2 + x_3 + x_5) - x_4 = \frac{1}{3} - 2x_2 - x_4.$$ 

In this case, $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/3\mathbb{Z}$ for $s = \exp(x)$.

4.7 $E_7$

We look the case of a quasi-simple, adjoint group of type $E_7$. We state several facts here without proof. Similar to Section 4.6, we do not offer any matrix representation for this group. The smallest matrix group in which $E_7$ can be described is $GL_{56}(\mathbb{C})$. Doing the necessary computations with such matrices is far to cumbersome and offers no benefit here. The details can be found in [2], Chapter VI, Section 4.11. The roots are given by

$$R = \{\pm \epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq 6\} \cup \{\epsilon_7 - \epsilon_8\} \cup \left\{\pm \frac{1}{2} \left(\epsilon_7 - \epsilon_8 + \sum_{i=1}^{6} (-1)^{\nu(i)} \epsilon_i\right) \mid \sum_{i=1}^{8} \nu(i) \equiv 1 \mod 2\right\}.$$
We may take

$$\Delta = \{ \alpha_1, \ldots, \alpha_7 \} = \left\{ \frac{1}{2} \left( \epsilon_1 + \epsilon_8 - \sum_{i=2}^{7} \epsilon_i \right), \epsilon_1 + \epsilon_2, \epsilon_2 - \epsilon_1, \epsilon_3 - \epsilon_2, \epsilon_4 - \epsilon_3, \epsilon_5 - \epsilon_4, \epsilon_6 - \epsilon_5 \right\}$$

and the highest root is given by $\tilde{\alpha}_0 = 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7$. Thus,

$$a_1 = a_2 = a_6 = 2, \quad a_3 = a_5 = 3, \quad a_4 = 4, \quad a_7 = 1,$$

and

$$v_1 = \frac{1}{2} \omega_1^\vee, \quad v_2 = \frac{1}{2} \omega_2^\vee, \quad v_3 = \frac{1}{3} \omega_3^\vee, \quad v_4 = \frac{1}{4} \omega_4^\vee, \quad v_5 = \frac{1}{3} \omega_5^\vee, \quad v_6 = \frac{1}{2} \omega_6^\vee, \quad v_7 = \omega_7^\vee.$$

The fundamental weights are given by

$$\omega_1^\vee = 2\alpha_1^\vee + 2\alpha_2^\vee + 3\alpha_3^\vee + 4\alpha_4^\vee + 3\alpha_5^\vee + 2\alpha_6^\vee + \alpha_7^\vee,$$

$$\omega_2^\vee = \frac{1}{2} (4\alpha_1^\vee + 7\alpha_2^\vee + 8\alpha_3^\vee + 12\alpha_4^\vee + 9\alpha_5^\vee + 8\alpha_6^\vee + 3\alpha_7^\vee),$$

$$\omega_3^\vee = 3\alpha_1^\vee + 4\alpha_2^\vee + 6\alpha_3^\vee + 8\alpha_4^\vee + 6\alpha_5^\vee + 4\alpha_6^\vee + 2\alpha_7^\vee,$$

$$\omega_4^\vee = 4\alpha_1^\vee + 6\alpha_2^\vee + 8\alpha_3^\vee + 12\alpha_4^\vee + 9\alpha_5^\vee + 6\alpha_6^\vee + \alpha_7^\vee,$$

$$\omega_5^\vee = \frac{1}{2} (6\alpha_1^\vee + 9\alpha_2^\vee + 12\alpha_3^\vee + 18\alpha_4^\vee + 15\alpha_5^\vee + 10\alpha_6^\vee + 5\alpha_7^\vee),$$

$$\omega_6^\vee = 2\alpha_1^\vee + 3\alpha_2^\vee + 4\alpha_3^\vee + 6\alpha_4^\vee + 5\alpha_5^\vee + 4\alpha_6^\vee + 3\alpha_7^\vee,$$

140
\[ \omega_7 = \frac{1}{2} (2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7). \]

As in Section 4.2, we may (abusively) write

\[ \omega_1^\vee = \epsilon_8 - \epsilon_7, \]

\[ \omega_2^\vee = \frac{1}{2} (\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 - 2\epsilon_7 + 2\epsilon_8), \]

\[ \omega_3^\vee = \frac{1}{2} (-\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 - 3\epsilon_7 + 3\epsilon_8), \]

\[ \omega_4^\vee = \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 - 2\epsilon_7 + 2\epsilon_8, \]

\[ \omega_5^\vee = \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 - \frac{3}{2}\epsilon_7 + \frac{3}{2}\epsilon_8, \]

\[ \omega_6^\vee = \epsilon_5 + \epsilon_6 - \epsilon_7 + \epsilon_8, \]

\[ \omega_7^\vee = \epsilon_6 - \frac{1}{2}\epsilon_7 + \frac{1}{2}\epsilon_8. \]

The extended Dynkin diagram \( \tilde{D} \) is

![Extended Dynkin Diagram](image-url)
Now, the closure of the alcove corresponding to $\Delta$ is

$$\tilde{C} = \left\{ \sum_{i=0}^{n} x_i \omega_i^\vee \mid x_i \geq 0, \sum_{i=0}^{n} a_i x_i = 1 \right\}$$

$$= \left\{ \sum_{i=0}^{n} x_i \omega_i^\vee \mid x_i \geq 0, x_0 + 2x_1 + 2x_2 + 3x_3 + 4x_4 + 3x_5 + 2x_6 + x_7 = 1 \right\}$$

$$= \left\{ \sum_{i=1}^{n} x_i \omega_i^\vee \mid x_i \geq 0, 0 \leq 2x_1 + 2x_2 + 3x_3 + 4x_4 + 3x_5 + 2x_6 + x_7 \leq 1 \right\}.$$

Since $a_i = 1$ only for $i = 0, 7$, we have $\tilde{W}_C = \{\rho_0, \rho_7\}$ by (2). Note that $\rho_0$ is the identity element. We can see that $\text{Aut}(\tilde{D}) \cong \mathbb{Z}/2\mathbb{Z}$ which acts on $\tilde{D}$ by a reflection. Since $\tilde{W}_C$ has order 2, we must have $\tilde{W}_C \cong \mathbb{Z}/2\mathbb{Z}$. By (3), $\rho_7 = (\omega_i^\vee, \sigma_7)$ for some $\sigma_7 \in W$. We know that $\rho_7$ sends $\tilde{\alpha}_0$ to $\alpha_7$ since $\rho_7 \cdot v_0 = v_7$. Therefore $\rho_7$ interchanges $\tilde{\alpha}_0$ and $\alpha_7$; $\alpha_1$ and $\alpha_6$; $\alpha_3$ and $\alpha_5$; and fixing $\alpha_2$ and $\alpha_4$. Thus, $\rho_7$ interchanges $v_0$ and $v_7$; $v_1$ and $v_6$; $v_3$ and $v_5$; and fixes $v_2$ and $v_4$. This is sufficient for determining the action of $\rho_7$ on a given $x \in \tilde{C}$. Note that $\rho_7$ has order 2 so $\tilde{W}_C = \langle \rho_7 \rangle$.

Let $x = \sum_{i=0}^{n} x_i \omega_i^\vee \in \tilde{C}$. There are no nontrivial subgroups of $\tilde{W}_C$ so the only case to consider is $\tilde{W}_x = \tilde{W}_C = \langle \rho_7 \rangle$. Therefore, we solve $\rho_1 \cdot x = x$ which gives

$$x_7 = x_0, x_1 = x_6, x_3 = x_5.$$

We also have

$$x_0 = 1 - 2x_1 - 2x_2 - 3x_3 - 4x_4 - 3x_5 - 2x_6 - x_7$$

142
so
\[ x_7 = \frac{1}{2} - x_1 - x_2 - 2x_4 - x_6 - \frac{3}{2}(x_3 + x_5) = \frac{1}{2} - 2x_1 - x_2 - 2x_4 - 3x_3. \]

In this case, \( Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/2\mathbb{Z} \) for \( s = \exp(x) \).

### 4.8 Intermediate Case of Type \( A_n \)

Recall from the beginning of Section 4 that every connected, quasi-simple, algebraic group is isomorphic to \( G/H \) for some simply connected group \( G \) and some central subgroup \( H \) and we have surjective homomorphisms

\[ G \to G/H \to G/Z \]

where \( Z \) is the finite centre of \( G \). We will look at lifts \( s' \in G/H \) of \( s \in G/Z \) to the intermediate subgroups \( G/H \) to determine \( Z_{G/H}(s')/Z_{G/H}(s')^0 \). This method only applies to groups of type \( A_n \) and \( D_n \) since the simply connected groups of the other cases have a centre of prime order.

We will to show that \( Z_{G/H}(s')/Z_{G/H}(s')^0 \) is isomorphic to a subgroup of the component group \( Z_{G/Z}(s)/Z_{G/Z}(s)^0 \). Consider the map \( \iota_H : G/H \to G/Z \) defined by \( \iota_H(gH) = gZ \) for all \( g \in G \). Now, suppose \( s' \in G/H \) is a lift of \( s \in G/Z \); i.e. \( s = s'Z \). It is not difficult to see that \( \iota_H \) induces a homomorphism \( Z_{G/H}(s') \to Z_{G/Z}(s) \).

Quotient maps are continuous so the induced homomorphism preserves connected
components. That is, $\iota_H$ induces the homomorphism

$$\iota_{s'}: \frac{Z_{G/H}(s')}{Z_{G/H}(s')^0} \to \frac{Z_{G/Z}(s)}{Z_{G/Z}(s)^0}.$$ 

Denote the stabilizer of $s$ in $W_{G/Z}$ by $W_{G/Z}(s)$ and recall that from the proof of Theorem 4.1.3, the map $W_{G/Z}(s)/W_{G/Z}(s)^0 \to Z_{G/Z}(s)/Z_{G/Z}(s)^0$ is an isomorphism. Similarly, $W_{G/H}(s')$ denotes the stabilizer of $s'$ in $W_{G/H}$ and $W_{G/H}(s')/W_{G/H}(s')^0 \cong Z_{G/H}(s')/Z_{G/H}(s')^0$. This gives

$$W_{G/H}(s')/W_{G/H}(s')^0 \cong Z_{G/H}(s')/Z_{G/H}(s')^0 \quad (9)$$

Note that we abandon the notation of Theorem 4.1.3 to eliminate ambiguity.

**Proposition 4.8.1.** Let $G$ be a simply connected group with centre $Z$ and let $H \subseteq Z$ be a central subgroup. Let $s \in G/Z$ and let $s' \in G/H$ be a lift of $s$. The map $\iota_{s'}: \frac{Z_{G/H}(s')}{Z_{G/H}(s')^0} \to \frac{Z_{G/Z}(s)}{Z_{G/Z}(s)^0}$ is injective.

**Proof.** The top isomorphism of (9) gives for each element of the component group $Z_{G/H}(s')/Z_{G/H}(s')^0$, a representative $\bar{w} \in Z_{G/H}(s')$ which satisfies $w = \bar{w}T/H \in W_{G/H}(s')$. Suppose $\bar{w}Z_{G/H}(s')^0 \in \ker \iota_{s'}$. Then, following the maps in (9), we have $\bar{w}Z \in Z_{G/Z}(s)^0$ so $\bar{w}T/Z \in W_{G/Z}(s)^0$. Thus $\bar{w}T/Z$ is a product of reflections $s_\alpha$ where $\alpha \in R(G/Z, T/Z)$ such that $\alpha(s) = 1$ ([9], Theorem 2.2). Equivalently,
\( \bar{W}/Z = \prod_{j=1}^{k} \bar{s}_j T/Z \) for some \( k \geq 1 \) and \( \beta_j \in R(G/H, T/H) \) such that \( \beta_j(s') = 1 \) for all \( 1 \leq j \leq k \). Therefore, \( w = \bar{w}T/H \) also belongs to \( W_{G/H}(s')^0 \) and this element corresponds to the identity element in \( Z_{G/H}(s')/Z_{G/H}(s')^0 \).

\[ \square \]

Note that since we have determined all possible \( Z_{G/Z}(s)/Z_{G/Z}(s) \) up to conjugation, our method gives all possible \( Z_{G/H}(s')/Z_{G/H}(s') \) up to conjugation.

Let \( G = SL_n(C) \), \( n \geq 2 \), which is the simply connected group of type \( A_n \). Then the centre of \( G \), is \( Z = \{ \mu^n I \mid 1 \leq q \leq n \} \) where \( \mu \) is a primitive \( n^{th} \) root of unity. Let \( s = \exp(x) \in G/Z \) be as in Section 4.2 with \( \tilde{W}_x = < \rho_1^n > \) for some \( m \) which divides \( n \). Hence \( Z_{G/Z}(s)/Z_{G/Z}(s)^0 \cong \mathbb{Z}/m\mathbb{Z} \).

Let \( H \) be a central subgroup of \( G \). Then

\[
H = \{ \mu^{nq} I \mid 1 \leq q \leq k \} = < \mu^n I >
\]

and \( |H| = k \) for some \( k \) which divides \( n \). Let \( d = \gcd(k, m) \). We will show

\[
Z_{G/H}(s')/Z_{G/H}(s')^0 \cong \mathbb{Z}/d\mathbb{Z}.
\]

Proposition 4.8.1 gives that \( Z_{G/H}(s')/Z_{G/H}(s')^0 \) is isomorphic to a subgroup of \( \mathbb{Z}/m\mathbb{Z} \) so we may conclude \( Z_{G/H}(s')/Z_{G/H}(s')^0 \) is cyclic. We show that an element of order \( d \) exists in \( Z_{G/H}(s')/Z_{G/H}(s')^0 \). Then we show that the order of every element of \( Z_{G/H}(s')/Z_{G/H}(s')^0 \) divides \( k \) and \( |Z_{G/H}(s')/Z_{G/H}(s')^0| \) divides \( m \).
Recall

\[ s = \text{diag} (s_1, s_2, \ldots, s_m) Z \]

where

\[
\begin{bmatrix}
  e^{2\pi i \sum_{j=1}^{m-1} x_j} \\
  e^{2\pi i \sum_{j=2}^{m-1} x_j} \\
  \ddots \\
  e^{2\pi i \frac{x_m}{m-1}} \\
  1
\end{bmatrix}
\]

and \( \zeta = e^{2\pi i \frac{1}{m}} \) is a primitive \( m \)th root of unity. For convenience, write \( s_l = \zeta^{m-l} A \) for all \( 1 \leq l \leq m \).

Now let \( s_G = \text{diag} (s_1, s_2, \ldots, s_m) \in G \) and let \( \alpha = \zeta^{\frac{m}{d}} \) which is a primitive \( d \)th root of unity. Then \( \alpha \alpha^* = \alpha^* \alpha \) implies

\[
\alpha s_l = \zeta^{\frac{m}{d}} s_l = \zeta^{m-(l - \frac{m}{d})} A = \begin{cases} 
  s_{l-\frac{m}{d}}, & \frac{m}{d} < l \leq m \\
  s_{m+l-\frac{m}{d}}, & 1 \leq l \leq \frac{m}{d}
\end{cases}
\]

so \( \alpha \) permutes the blocks \( s_l \) of \( s_G \) as follows

\[
\alpha s_G = \text{diag} (s_1, s_2, \ldots, s_m)
= \text{diag} (s_{m+1-\frac{m}{d}}, s_{m+2-\frac{m}{d}}, \ldots, s_m, s_1, \ldots, s_{m-\frac{m}{d}}).
\]

We can see that that \( \alpha s_l \neq s_l \) for every \( 1 \leq l \leq m \). Therefore, the minimal \( q \) such that \( \alpha^q s_G = s_G \) is \( q = d \).
Recall that $W_G \cong S_n$ permutes the entries of $T$. Let $w$ be the element in $W_G$ which corresponds to the action of $\alpha$ on $s_G$. Then

$$w \cdot s = w \cdot s_G Z = s_G Z = s.$$ 

Hence $w$ corresponds to an element in $W_{G/Z}(s)$. However, since $d$ divides $k$, $\alpha$ is also a $k^{th}$ root of unity so $\alpha \in H$. Thus

$$w \cdot s = w \cdot s_G H = s_G H = s$$

and $w$ also corresponds to an element in $W_{G/H}(s')$.

After identifying $w$ with its image in $Z_{G/Z}(s)$ and $Z_{G/H}(s')$ from (9), injectivity from Proposition 4.8.1 gives

$$|wZ_{G/Z}(s)^0| = |wZ_{G/H}(s')^0| = d.$$ 

Hence $Z_{G/H}(s')/Z_{G/H}(s')^0$ contains an element of order $d$ so it follows that $d$ must divide $|Z_{G/H}(s')/Z_{G/H}(s')^0|$.

Now, let $y \in W_{G/H}(s')$. Then $y \cdot s' = s'$ implies $y \cdot s_G = \mu^t s_G$ for some $1 \leq t \leq k$. Thus, for any $q \geq 2$,

$$y^q \cdot s_G = y^{q-1}(y \cdot s_G) = y^{q-1} \cdot (\mu^t s_G) = \mu^{qt} y^{q-1} \cdot s_G = \mu^{qt} y^t s_G$$

which gives $y^k \cdot s_G = s_G$. Therefore $y^k$ can be identified with an element of $W_G(s_G)$, or equivalently, an element of $Z_G(s_G)$. However, $G$ is simply connected so $Z_G(s_G) = 147$
Thus, after identification, $y^k Z_G(s_G)^0$ is trivial. Then Proposition 4.8.1 gives that $y^k Z_{G/H}(s')^0$ is trivial. Therefore $|y Z_{G/H}(s')^0|$ must divide $k$.

As previously stated, $Z_{G/H}(s')/Z_{G/H}(s')^0$ is isomorphic to a subgroup of the component group $Z_G(s)/Z_G(s)^0 \cong \mathbb{Z}/m\mathbb{Z}$. It follows that $|Z_{G/H}(s')/Z_{G/H}(s')^0|$ divides $m$. Therefore $Z_{G/H}(s')/Z_{G/H}(s')^0$ is isomorphic to a cyclic group of order dividing $m$. However, all elements of $Z_{G/H}(s')/Z_{G/H}(s')^0$ have order dividing $k$, and there exists an element of order $d = \gcd(k, m)$. Thus $Z_{G/H}(s')/Z_{G/H}(s')^0 \cong \mathbb{Z}/d\mathbb{Z}$.

### 4.9 Intermediate Case of Type $D_n$

The simply connected, complex group of type $D_n$ is $Spin_{2n}(\mathbb{C})$ which is a double cover of $SO_{2n}(\mathbb{C})$. Thus $SO_{2n}(\mathbb{C})$ is the only intermediate group of type $D_n$ so let $G = SO_{2n}(\mathbb{C})$, $n \geq 2$. Then the centre of $G$ is $Z = \{ \pm I \}$. Let $s = \exp(x) \in G/Z$ be as in Section 4.5. Recall that

$$s = \begin{bmatrix}
  s_{\theta_1} \\
  \vdots \\
  s_{\theta_n}
\end{bmatrix} Z$$

where

$$s_{\theta_j} = \begin{bmatrix}
  \cosh \theta_j & i \sinh \theta_j \\
  -i \sinh \theta_j & \cosh \theta_j
\end{bmatrix}$$

for all $1 \leq j \leq n$. Note that $s_{\theta_j}^{-1} = s_{-\theta_j}$.
Let $s'$ be a lift of $s$ to $G$. Proposition 4.8.1 implies that $Z_G(s')/Z_G(s')^0$ may be identified with a subgroup of $Z_G/Z(s)/Z_G(s)^0$. Then for any $\rho_i \in \tilde{W}_x$,

$$\rho_i \cdot s'Z = \rho_i \cdot s = s = s'Z$$

if and only if $\rho_i \cdot s' = s'$ or $\rho_i \cdot s' = -s'$. Since $\tilde{W}_x$ is at most of order 4, we will determine which elements of $\tilde{W}_x$ fix $s'$. Since $Z_G(s')/Z_G(s')^0$ is isomorphic to a subgroup of $\tilde{W}_x$, this will completely determine $Z_G(s')/Z_G(s')^0$. We have two cases to consider: $n$ is even and $n$ is odd.

Suppose $n$ is even. Then $Z_G/Z(s)/Z_G(s)^0$ is a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Recall that $\rho_{n-1}$ and $\rho_n$ are elements of the extended affine Weyl group that fix the alcove corresponding to $s$. They are defined in (2) and described in Section 4.5. We will show that if $\rho_{n-1}$ or $\rho_n$ fix $s$ then they must send $s'$ to $-s'$. However, if $\rho_{n-1}\rho_n$ fixes $s$, it also fixes $s'$.

Suppose $s$ is fixed by $\rho_{n-1}$ or $\rho_n$. For $2 \leq k \leq \frac{n}{2}$, we have

$$\theta_k + \theta_{n-k+1} = \pi i \left( \frac{1}{2} + \sum_{j=k}^{n-k} x_j + \frac{1}{2} - \sum_{j=n-(n-k+1)+1}^{(n-k+1)-1} x_j \right)$$

$$= \pi i \left( 1 + \sum_{j=k}^{n-k} x_j - \sum_{j=k}^{n-k} x_j \right)$$

$$= \pi i$$

so $e^{\theta_k} = -e^{-\theta_{n-k+1}}$. Thus,

$$s_{\theta_k} = -s_{-\theta_{n-k+1}} = -s_{\theta_{n-k+1}}^{-1}$$

149
for all $2 \leq k \leq n - 1$.

Let $s$ be fixed by $\rho_{n-1}$. We have $s_{\theta_k} = -s_{-\theta_{n-k+1}}$ for all $2 \leq k \leq n - 1$. We also have $\theta_1 = \theta_n + \pi i$ so $s_{\theta_1} = -s_{\theta_n}$. By Proposition 4.1.4, $\rho_{n-1}$ acts on $s$ by $\sigma_{n-1} = s_{\epsilon_1 - \epsilon_n} \prod_{i=2}^{n} s_{\epsilon_i + \epsilon_{n-i+1}}$. So $\rho_{n-1}$ interchanges $s_{\theta_1}$ and $s_{\theta_n}$ in addition to sending $s_{\theta_k}$ to $s_{\theta_{n-k+1}}^{-1}$ for all $2 \leq k \leq n - 1$. However, $s_{\theta_{n-k+1}}^{-1} = -s_{\theta_k}$ for all $2 \leq k \leq n - 1$. Thus $\rho_{n-1} \cdot s' = -s'$. Therefore, for $\tilde{W}_x = \langle \rho_{n-1} \rangle$, $Z_G(s')/Z_G(s')^0$ is trivial.

Let $s$ be fixed by $\rho_n$. We have $s_{\theta_k} = -s_{-\theta_{n-k+1}}$ for all $2 \leq k \leq n - 1$. In this case, we have $\theta_1 = -\theta_n + \pi i$ which implies $s_{\theta_1} = -s_{-\theta_n}$. It follows that $s_{\theta_{n-k+1}}^{-1} = -s_{\theta_k}$ for all $1 \leq k \leq n$. Proposition 4.1.4 gives that $\rho_n$ acts on $s$ by $\sigma_n = \prod_{i=1}^{n} s_{\epsilon_i + \epsilon_{n-i+1}}$. Hence $\rho_n$ sends $s_{\theta_k}$ to $s_{\theta_{n-k+1}}^{-1}$ for all $1 \leq k \leq n$. Thus $\rho_n \cdot s' = -s'$. Therefore, for $\tilde{W}_x = \langle \rho_n \rangle$, $Z_G(s')/Z_G(s')^0$ is trivial.

Let $s$ be fixed by $\rho_{n-1}\rho_n$. We have $\theta_1 = \pi i$ and $\theta_n = 0$ so $s_{\theta_1} = s_{\theta_1}$ and $s_{\theta_n}^{-1} = s_{\theta_n}$. Now
\[
\sigma_{n-1} \sigma_n = \left( s_{\epsilon_1 - \epsilon_n} \prod_{i=2}^{n} s_{\epsilon_i + \epsilon_{n-i+1}} \right) \left( \prod_{i=1}^{n} s_{\epsilon_i + \epsilon_{n-i+1}} \right) = s_{\epsilon_1 - \epsilon_n} s_{\epsilon_1 + \epsilon_n}
\]
so $\rho_{n-1}\rho_n$ sends $s_{\theta_k}$ to $s_{\theta_k}^{-1} = s_{\theta_k}$ for $k = 1, n$ and fixes $s_{\theta_k}$ for all $2 \leq k \leq n - 1$. Thus $\rho_{n-1}\rho_n \cdot s' = s'$. Therefore, for $\tilde{W}_x = \langle \rho_{n-1}\rho_n \rangle$, $Z_G(s')/Z_G(s')^0 \cong \mathbb{Z}/2\mathbb{Z}$.

We have already shown that $\rho_{n-1}$ and $\rho_n$ do not fix $s'$ but $\rho_{n-1}\rho_n$ fixes $s'$. Thus, for $\tilde{W}_x = \tilde{W}_G = \langle \rho_{n-1}, \rho_n \rangle$, $Z_G(s')/Z_G(s')^0 \cong \mathbb{Z}/2\mathbb{Z}$.

Now suppose $n$ is odd. Then $Z_G/\mathbb{Z}(s)/Z_G(s)^0$ is a subgroup of $\mathbb{Z}/4\mathbb{Z}$. We will
show that if $\rho_n$ fixes $s$ then it sends $s'$ to $-s'$. However, if $\rho_n^2$ fixes $s$, it also fixes $s'$.

Identical to the case of $n$ even and $\rho_{n-1}$ fixing $s$, we have $\theta_k + \theta_{n-k+1} = \pi i$ for all $2 \leq k \leq n - 1$. This implies $s_{\theta_k} = -s_{-\theta_{n-k+1}}$ for all $2 \leq k \leq n - 1$. We also have $\theta_1 = \pi i$ and $\theta_n = 0$ so $s_{\theta_1}^{-1} = s_{\theta_n}$, $s_{\theta_n}^{-1} = s_{\theta_n}$ and $s_{\theta_1} = -s_{\theta_n}$. Proposition 4.1.4 gives that $\rho_n$ acts on $s$ by

$$
\sigma_n = s_{\epsilon_1+\epsilon_n}s_{\epsilon_{\lfloor \frac{n}{2} \rfloor+1}-\epsilon_n}s_{\epsilon_{\lfloor \frac{n}{2} \rfloor+1}+\epsilon_n}\prod_{i=2}^{\lfloor \frac{n}{2} \rfloor}s_{\epsilon_i+\epsilon_{n-i}+1}.
$$

Hence $\rho_n$ sends $s_{\theta_k}$ to $s_{\theta_n-k+1}^{-1} = -s_{\theta_k}$ for all $1 \leq k \leq n - 1$. We also have $\rho_n$ sends $s_{\theta_1}$ to $s_{\theta_n}^{-1} = -s_{\theta_1}$ and $s_{\theta_n}$ to $s_{\theta_1}^{-1} = -s_{\theta_n}$. Thus $\rho_n \cdot s' = -s'$.

Now

$$
\sigma_n^2 = \left(s_{\epsilon_1+\epsilon_n}s_{\epsilon_{\lfloor \frac{n}{2} \rfloor+1}-\epsilon_n}s_{\epsilon_{\lfloor \frac{n}{2} \rfloor+1}+\epsilon_n}\prod_{i=2}^{\lfloor \frac{n}{2} \rfloor}s_{\epsilon_i+\epsilon_{n-i}+1}\right)^2
$$

$$
= (s_{\epsilon_1+\epsilon_n}s_{\epsilon_{\lfloor \frac{n}{2} \rfloor+1}-\epsilon_n}s_{\epsilon_{\lfloor \frac{n}{2} \rfloor+1}+\epsilon_n})^2
$$

$$
= s_{\epsilon_1-\epsilon_n}s_{\epsilon_1+\epsilon_n}
$$

so $\rho_n^2$ sends $s_{\theta_k}$ to $s_{\theta_k}^{-1} = s_{\theta_k}$ for $k = 1, n$ and fixes $s_{\theta_k}$ for all $2 \leq k \leq n - 1$. Thus $\rho_n^2 \cdot s' = s'$. Therefore, in both cases, $Z_G(s')/Z_G(s')^0 \cong \mathbb{Z}/2\mathbb{Z}$.

Proposition 4.8.1 implies that the orders of the component groups for intermediate groups divide the orders of the component groups for the adjoint groups. Our computations for intermediate groups of type $A_n$ and $D_n$ allow us to generalize this result.

As mentioned in Section 4.8, intermediate groups of type $A_n$ are of the form
$SL_n(\mathbb{C})/ <\beta I>$ for some primitive $k^{th}$ root of unity $\beta$ where $k$ divides $n$. Then, for $Z_{PGL_n(\mathbb{C})}(s)/Z_{PGL_n(\mathbb{C})}(s)^0$ of order $m$, the order of $Z_{SL_n(\mathbb{C})/\langle \beta I \rangle}(s')/Z_{SL_n(\mathbb{C})/\langle \beta I \rangle}(s')^0$ is $\gcd(k,m)$.

We can see that the order of $Z_{SO_{2n}(\mathbb{C})}(s')/Z_{SO_{2n}(\mathbb{C})}(s')^0$ is either trivial or of order 2. Now, the simply connected groups of type $D_n$ is $Spin_{2n}(\mathbb{C})$ which is a double cover of $SO_{2n}(\mathbb{C})$. Thus the centre of $Spin_{2n}(\mathbb{C})$ has order 4 and $SO_{2n}(\mathbb{C}) \cong Spin_{2n}(\mathbb{C})/H$ for some central subgroup of order 2. Hence, for $Z_{PSO_{2n}(\mathbb{C})}(s)/Z_{PSO_{2n}(\mathbb{C})}(s)^0$ of order $m$, the order of $Z_{SO_{2n}(\mathbb{C})}(s')/Z_{SO_{2n}(\mathbb{C})}(s')^0$ is $\gcd(|H|,m)$ or 1.

Using the notation of 4.8, we have proven the following proposition.

**Proposition 4.9.1.** Let $G$ be a simply connected group with centre $Z$. Let $H \subseteq Z$ be a central subgroup and let $s' \in G/H$ be a lift of $s \in G/Z$. Suppose $Z_{G/Z}(s)/Z_{G/Z}(s)^0$ has order $m$. Then $|Z_{G/H}(s')/Z_{G/H}(s')^0| = \gcd(|H|,m)$ or $Z_{G/H}(s')/Z_{G/H}(s')^0$ is trivial.

### 4.10 Similitude Groups

Let $G$ be a complex, connected, quasi-simple, simply connected, algebraic group with maximal tours $T$, and suppose $c \in Z_G$ such that $|c| = 2$. Recall from Example 2.2.7 that $G_m = \mathbb{C}^\times$. Consider the subgroup $H = < -1, c >$ of $G_m \times G$.

**Definition 4.10.1.** The group $\bar{G} = (G_m \times G)/H$ is called a similitude group of $G$. 

152
There is a more general definition of a similitude group but we are only interested in the type of group defined above.

Now, $\bar{G}$ is an algebraic group ([19], Proposition 5.5.10). It follows that $\bar{G}$ is reductive and connected since $G_m$ and $G$ are reductive and connected. However, $\bar{G}$ is not quasi-simple since $(G_m \times \{I\})/H$ is a proper, connected, closed, normal subgroup.

**Example 4.10.2.** Let $G = SL_2(\mathbb{C})$ and let $H = \langle -1, -I \rangle$. Thus $\bar{G} = (\mathbb{C}^\times \times SL_2(\mathbb{C}))/H$ and we will show $\bar{G} \cong GL_2(\mathbb{C})$.

Define the map $\eta: \mathbb{C}^\times \times SL_2(\mathbb{C}) \to GL_2(\mathbb{C})$ by $\eta(a, A) = aA$ for all $a \in \mathbb{C}^\times$ and $A \in SL_2(\mathbb{C})$. For all $X \in GL_2(\mathbb{C})$, $X = xx^{-1}X$ where $x = \det(X)^{\frac{1}{2}}$. It is easy to see that $x^{-1}X \in SL_2(\mathbb{C})$ so $\eta(x, x^{-1}X) = X$. Hence $\eta$ is surjective. Suppose $(a, A) \in \ker \eta$. Then $aA = I$ which implies $A = \frac{1}{a}I$ and $a^2 = 1$. Therefore, $\ker \eta = \{(1, I), (-1, -I)\} = H$. It follows that $\bar{\eta}: \bar{G} \to GL_2(\mathbb{C})$ defined by $\bar{\eta}((a, A)H) = aA$ is a bijection.

The multiplication map is a morphism so $\eta$ is continuous. Proposition 6.13 in [1] gives that $\bar{\eta}$ is continuous. Then Proposition 5.5.10 in [19] gives that $\bar{\eta}$ is a homeomorphism so we have $\bar{G} \cong GL_2(\mathbb{C})$.

Note that for $n$ odd, $GL_n(\mathbb{C}) \cong \mathbb{C}^\times \times SL_n(\mathbb{C})$. Computing component groups for this case is simple so it is not of interest to us.
The following theorem extends the connectedness theorem for component groups of centralizers of semi-simple elements in quasi-simple groups. We had mentioned previously that quasi-simple, simply connected groups have connected centralizers. We make a similar claim for similitude groups which we know are not quasi-simple.

**Theorem 4.10.3.** Let \( s \in (\mathbb{G}_m \times T)/H \leq \bar{G} \) be semi-simple such that \( < s > \) is bounded in \( \bar{G} \). Then \( Z_{\bar{G}}(s)/Z_{\bar{G}}(s)^0 \) is trivial.

**Proof.** Let \( s' = (s_1, s_2) \in \mathbb{G}_m \times T \) which is a maximal torus of \( \mathbb{G}_m \times G \). First we will show that there is a continuous surjection from \( Z_{\mathbb{G}_m \times G}(s') \) to \( Z_{\bar{G}}(s) \).

Consider the map \( \phi: Z_{\mathbb{G}_m \times G}(s') \to Z_{\bar{G}}(s) \) defined by \( \phi(z') = z'H \). Note that \( \phi(s') = s \).

Suppose \( z'H = (a, x)H \in Z_{\bar{G}}(s) \). Then

\[
z's'z'^{-1}H = (a, x)(s_1, s_2)(a^{-1}, x^{-1})H = (as_1a^{-1}, xs_2x^{-1})H = (s_1, xs_2x^{-1})H
\]

so \( z's'z'^{-1}H = (s_1, s_2)H \) if and only if \( (s_1, xs_2x^{-1}) = (s_1, s_2) \) or \( (s_1, xs_2x^{-1}) = (-s_1, s_2) \). Since \( s_1 \neq -s_1 \), we have \( z's'z'^{-1}H = (s_1, s_2)H \) if and only if \( xs_2x^{-1} = s_2 \); i.e. \( x \in Z_G(s_2) \). Note that \( x \in Z_G(s_2) \) implies \( z' \in Z_{\mathbb{G}_m \times G}(s') \). In particular, \( \phi \) is
surjective. Moreover $\phi$ is continuous so it preserves connected components. Namely,

$$\phi(Z_{G_m \times T}(s')) = Z_G(s) \text{ and } \phi(Z_{G_m \times T}(s')^0) = Z_{\bar{G}}(s)^0. \quad (10)$$

The next step is to show that $Z_{G_m \times G}(s')$ is connected. Let $(a, x) \in Z_{G_m \times G}(s')$. This is true if and only if $a \in Z_{G_m}(s_1)$ and $x \in Z_G(s_1)$. Note that $Z_{G_m}(s_1) = G_m$ since $G_m$ is abelian. Therefore $Z_{G_m \times G}(s') = G_m \times Z_G(s_2)$.

We showed that $G_m$ is connected in Example 2.2.7. As mentioned at the beginning of Section 4, $Z_G(s_2)$ is connected since $G$ is simply connected. Therefore $G_m \times Z_G(s_2)$ is connected in the Zariski topology. Thus $Z_{G_m \times G}(s')^0 = G_m \times Z_G(s_2)$. Hence, we have

$$Z_{G_m \times G}(s')^0 = G_m \times Z_G(s_2) = Z_{G_m \times G}(s'). \quad (11)$$

Putting (10) and (11) together gives

$$Z_G(s) = \phi(Z_{G_m \times G}(s')) = \phi(Z_{G_m \times G}(s')^0) = Z_{\bar{G}}(s)^0$$

so $Z_{\bar{G}}(s)/Z_{\bar{G}}(s)^0$ is trivial. $\square$

5 Conclusions and Future Research

We have computed centralizers for all bounded semi-simple elements of connected, quasi-simple, complex linear algebraic groups. As mentioned in Section 3, (0), the
group \( R_\chi \), with \( s = \phi(Fr_q^{-1}) \), is isomorphic to \( Z_\hat{G}(s)/Z_\hat{G}(s)^0 \). We compare our results on the component groups in the adjoint case with the work of Keys in [10] where \( R_\chi \) was computed by using analytic techniques. It is worth noting that computing \( R_\chi \) requires some deep results in representation theory and harmonic analysis whereas computing \( Z_\hat{G}(s)/Z_\hat{G}(s)^0 \) requires only basic algebra and some topology.

Keys shows that, for \( G \) of type \( A_n \), \( R_\chi \cong \mathbb{Z}/m\mathbb{Z} \) for some \( m \) dividing \( n \). For \( G \) of type \( B_n \), \( C_n \) or \( E_7 \), \( R_\chi \cong \mathbb{Z}/2\mathbb{Z} \). For \( G \) of type \( E_6 \), \( R_\chi \cong \mathbb{Z}/3\mathbb{Z} \). For \( G \) of type \( D_n \), \( R_\chi \cong \mathbb{Z}/2\mathbb{Z} \), \( R_\chi \cong \mathbb{Z}/4\mathbb{Z} \) or \( R_\chi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). The latter two cases for \( D_n \) occur only when \( n \) is odd or \( n \) is even respectively. This coincides precisely with our algebraic computations of \( Z_\hat{G}(s)/Z_\hat{G}(s)^0 \) in Sections 4.2-4.7.

It seems likely that our methods for computing \( Z_\hat{G}(s)/Z_\hat{G}(s)^0 \) will extend to more general algebraic groups. We only considered quasi-simple groups in this thesis. One could weaken this condition to considering semi-simple groups. For example, one could look at \( G_1 \times G_2/ <g_1, g_2> \) for \( G_1, G_2 \) connected, quasi-simple linear algebraic groups and \( g_1 \in G_1, g_2 \in G_2 \) central elements of order 2. Perhaps an argument similar to that of Section 4.10 would be sufficient in determining component groups of centralizers in this case.
References


