Finite Groups of Lie Type

Ayush Jain
The Shri Ram School Aravali, India
ayushj2007@gmail.com

July, 2023

Abstract

This paper provides an overview of three finite groups of Lie type: *General Linear Groups*, *Symplectic Groups*, and *Unitary Groups*. These groups are also classified as classical groups. We prove the simplicity property of their projective subgroups using Iwasawa's Lemma. We also discuss important subgroups of these groups such as *Borel Subgroup* and *Weyl Group*.

1 Introduction

A *group* in mathematics is a non-empty set with a binary operation on its elements that satisfies three axioms: the operation is associative, the set has an identity element, and each element of the set has an inverse element.

Definition 1.1 (Group)**.** Let G be a non-empty set and let $*$ be a binary operation on G, $* : G \times G \mapsto G$. Then $(G; *)$ is a group if the following axioms are satisfied.

G1 **associativity**: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

G2 **identify element**: there exist an identify element e such that $a * e = e * a = a$ for all $a \in G$.

G3 **inverses:** for all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

Some examples of groups include, the set of integers $(\mathbb{Z}; +)$ with addition as binary operation and 0 as identity element; the set of complex numbers $(\mathbb{C}; +)$ under addition operation; a vector space under addition operation; and the trivial group

that consists of only an identity element. The set of all invertible matrices is also a group under matrix multiplication operation and is called the *general linear group*.

We can create relations between various groups using maps. For example, the groups $\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ can be related by a map that maps every element of $\mathbb{Z}$ to an element in $\mathbb{Z}/3\mathbb{Z}$ by applying *mod 3*. The map that preserves the group operation is called *homomorphism*. When a homomorphism is both surjective and injective, it is called *isomorphism*. An isomorphism from a group to itself called *automorphism*. An example of an automorphism is the map $h : \mathbb{Z} \mapsto \mathbb{Z}$ where $h(u) = -u$.

A *finite group* is a group with a finite number of elements. The *order* of a group, denoted by $|G|$ gives the number of elements in the finite group G.

A subgroup is a subset of another group that also qualifies as a group itself. A subgroup is called *normal subgroup* if it is invariant under conjugation by any element of the parent group. That is a subgroup N of a group G is called a normal subgroup if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. A group is called *simple* if its only normal subgroups are the trivial group and the group itself.

The *classification theorem* classifies[1] all finite simple groups into one of the following groups [1].

- a *cyclic group* C_p of order p where p is a prime
- An *alternating group* of order ≥ 5
- A finite group of *Lie Type*
- One of the 27 sporadic groups (27th is sometimes referred to as the *Tits group*)

This paper focuses on the finite groups of Lie Type, which are general linear groups with elements from finite fields. These groups can be considered as the finite analogous of *Lie Groups*. They can be subdivided further into smaller families, one of which is the classical groups [2]. Not all classical groups are of Lie type, but some of their subgroups such as the Projective Special Linear group can be categorized as Lie Type.

[1]The significant effort to classify all simple groups took 20 years and occupies 5000 pages in the literature

The classical groups we will discuss in this paper are Special Linear, Symplectic, and Unitary groups [9]. They are linear groups and their special automorphism groups of bilinear (Symplectic) and sesquilinear forms (Unitary).

The paper is organized as follows: Section 2 offers an introductory overview of *finite fields* and *vector spaces*, along with some important definitions of group theory. Section 3 discusses General Linear Groups. Section 4 discusses bilinear form and Symplectic groups. Section 5 describes sequilinear form and Unitary Groups. We prove the simplicity property of projective subgroup of each of these groups and also discuss important sub-groups of these groups.

2 Vector Spaces and Finite Fields

First we provide a basic definition and overview of *Fields* and *Vector Spaces*, which is the space we will be using.

Definition 2.1. A *field* is a set F with two binary operations (namely addition and multiplication), and the following axioms:

- Associativity of addition and multiplication
- Commutativity of addition and multiplication
- Existence of Multiplicative and Additive identity, denoted by 1 and 0 respectively
- $\forall a \in F$ existence of an additive inverse denoted by $-a$
- $\forall b \in F$, $b \neq 0$ existence of a multiplicative inverse denoted by b^{-1}
- Satisfies Distributive Law, given by $x(y+z) = xy + xz$

Definition 2.2. The characteristic of a *finite field* is the smallest natural number m such that m times the identity element yields 0. For example, in $\mathbb{Z}/p\mathbb{Z}$, the identity element is 1, and the characteristic is p, since $p * 1 = 0$

A finite field is a Field F with a finite number of elements. We can show that the field generated by the element 1 in F (call it F_0) is isomorphic to the integers

modulo a prime p. The field F_0 is defined as the prime subfield of F (see [5]).

Since vector space axioms follow from field axioms, the field F_0 is a vector space. And since F is finite, F_0 is also finite. Any finite dimensional vector space has a basis of n vectors, say $v_1, v_2, \ldots, v_n$, and every vector has a unique representation in the form $\sum_{i=1}^{n} a_i v_i$ with $a_i \in F_0$, so we can say that the field has p^n elements.

One of the most important properties of Finite Fields is that the multiplicative group of non zero elements is cyclic in nature. For the following theorems, let q be the order of the of the field.

Theorem 2.3. *There exists a multiplicative group G of a finite field F such that all elements of G can be generated by some exponent of $g \in G$.*

Proof. Let G be the multiplicative group of the field. Let d be any positive divisor of q, and $f(d)$ be the number of elements with order d. Suppose that there exists an element $a \in G$ such that a has order d. Let H be the group generated by a. Since d is the order of a, for all $x \in H$, $x^d = 1$.

Hence H has $\phi(d)$ elements, which means $f(d) = \phi(d)$. Using the identity $\sum_{d|q} \phi(d) = \sum_{d|q} f(q) = q$, we have $f(q) = \phi(q)$ and for any natural number q the totient function is non zero. This implies that there exists at least one such element which generates the field. □

Theorem 2.4. *For any natural m, the number of solutions to the equation $x^m = 1$ is given by $(m, q-1)$, where (a, b) denotes the greatest common divisor of a and b.*

Proof. let u be a generator of the finite field F_q of order q. The multiplicative subgroup is given by $F_q - \{0\}$ is a cycle of length $q-1$, which means that $x^n = 1$ only when $x^{(n,q-1)} = 1$. Let $(n, q-1) = t$. We know that $F_q - \{0\} = \{u^k : k = 1, 2, 3, \ldots, q-2\}$. We want to find elements u^k such that $(u^k)^t = u^{kt} = 1$. This happens if and only if $q-1$ divides kt since u is a generator. You can further observe that $q-1$ divides kt only if k is a multiple of $\frac{q-1}{t}$ since t divides $q-1$. Therefore it follows that the number of solutions is $(n, q-1)$ □

Theorem 2.5. *For any rational prime p and natural number d, there exists a finite field of order p^d and is unique up to isomorphism.*

Proof. This is proven in [9, Section 3.2] □

Definition 2.6. *A vector space* (also called a linear space) is a set whose elements, vectors, can be added together and multiplied by numbers called scalars. Scalars are often real numbers, but can be complex numbers or, more generally, elements of any field. The operations of vector addition and scalar multiplication must satisfy vector axioms.

Next we look at some definitions and properties related to groups which we will use in this paper.

Definition 2.7. The *order* of an element a in a group S is the smallest natural number m such that $a^m = 1$

Definition 2.8. The *order* of a group, not to be confused with the order of an element, is the number of elements in that group. For a group G, this is denoted by $|G|$

Definition 2.9. The *kernel* of a group homomorphism $\phi : G \to H$ is defined as

$$\ker \phi = \{g \in G : \phi(g) = e_H\}$$

Where e_H is the identity of the group H (see [8])

Definition 2.10. A matrix A is said to be *invertible* if $\exists A^{-1}$ such that $A \cdot A^{-1} = A^{-1} \cdot A = I$

Definition 2.11. Let a group G act on a set X. The action is said to be *transitive* if $\forall x, y \in X$, $\exists g \in G$ such that $g \cdot x = y$ [4] .

Definition 2.12. The group action $G \times \Omega \to \Omega$ may preserve a special kind of partition of Ω known as blocks. A *block* is a subset δ of Ω such that for any group element g, one of the following is true

- $g \cdot \delta = \delta$
- $g\delta \cap \delta = \phi$

Definition 2.13. A *primitive group action* is the action that is transitive and has no non trivial group blocks.

3 The General Linear Group

Definition 3.1. Let V be a vector space with its element taken from the finite field $\mathbb{F}_q$ of order q. Then the *general linear group* is the set of all the linear maps from V to itself which are invertible.

Another way to define this group would be the set of all $n \times n$ invertible square matrices with entries from $\mathbb{F}_q$. The general linear group is denoted by $GL_n(q)$.

Let the center of this group be Z. Z is a normal subgroup of all scalar matrices in the form λI_n, where $\lambda \in \mathbb{F}_q$ and $\lambda \neq 0$. We can show that Z is a cyclic group of order $q-1$. If we quotient Z with $GL_n(q)$, we get a group called Projective General Linear group, abbreviated as $PGL_n(q)$.

We can create a homomorphism from the general linear group to the multiplicative group of the field using determinants. This is due to the multiplicative property of the determinants.

If we investigate the kernel of action of the homomorphism, we get the *special linear group* $SL_n(q)$. This consists of all matrices with determinant 1. Similar to the general linear group, we can quotient it with its subgroup of scalars to obtain the Projective Special Linear group $PSL_n(q)$.

3.1 Orders of the Linear Groups

An interesting result for the classical groups is that one can represent the orders of its elements using formulas. For example, we can say that

$$|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

We know that for a matrix to be invertible, all the rows must have at least one entry that is non zero, and all the rows and columns must be distinct that is every vector defining the space must be linearly independent.

Since there are q total elements in the field $\mathbb{F}_q$, there are q^n possible options for the elements of the first row. However, there is one case where all n elements are 0, so we subtract that one case. Similarly, there are q^n options for the second row. If we want to keep all the rows distinct, we have $q^n - q$ options to fill out the third

row, and so on. This gives us the final formula

$$|Gl_n(q)| = q^{\frac{n(n-1)}{2}} \prod_{i=0}^{n} (q^i - 1)$$

Similarly, we can use derive the equations of the orders of some of the subgroups of the general linear group. For the group $SL_n(q)$ we can use the order of the general linear group itself. For any matrix with determinant m, since we take entries in a field, we have $m^{-1} \in \mathbb{F}_q$. If we multiply the first row with the scalar m^{-1} we get matrices with determinant 1. Conversely, for any determinant with determinant 1, we multiply the first row with m we get matrices with determinant m. So this means there's a bijection between the matrices with determinant 1 and matrices with any other determinant in $\mathbb{F}_q$. This implies:

$$|SL_n(q)| = \frac{1}{q-1}|Gl_n(q)|$$
$$|SL_n(q)| = \frac{1}{q-1} \cdot q^{\frac{n(n-1)}{2}} \prod_{i=0}^{n} (q^i - 1)$$

To get the order of $PSL_n(q)$ we need to find out the scalar λI_n for which matrices have a determinant 1. If we use the fact that the determinant is multiplicative, we have that $\det(\lambda I_n) = \lambda^n$, so we need to find the solutions to the equation $\lambda^n = 1$. We know from our knowledge of finite fields that this is equal to $(n, q-1)$, which means that the order of $PSL_n(q)$ can be given as

$$|PSL_n(q)| = \frac{1}{(n, q-1)}|GL_n(q)|$$
$$|PSL_n(q)| = \frac{1}{(n, q-1)} \cdot q^{\frac{n(n-1)}{2}} \prod_{i=0}^{n} (q^i - 1)$$

3.2 Simplicity of $PSL_n(q)$

An important result of linear groups is that $PSL_n(q)$ is simple for $n > 2$ and $q > 3$. The proof of the simplicity of $PSL_n(q)$ requires Iwasawa's Lemma (Theorem 3.6), which gives a method of classification of simple groups [3].

Definition 3.2. A group action $\phi : G \times X \to X$ is called *faithful* if there are no group elements g such that $gx = g$ for all $x \in X$.

Definition 3.3. *Stabilizer of a point* is that permutation in the group which does not change the given point.

Definition 3.4. For any group G, if we take two elements $a, b \in G$, the *commutator* of the two elements if defined as $a^{-1}b^{-1}ab$ and is denoted by $[a, b]$. The commutator subgroup is the set of all possible commutators of a group.

Definition 3.5. A group is said to be *perfect*, if it is equal to its own commutator subgroup.

Theorem 3.6 (Iwasawa)**.** *If G is a finite perfect group, acting faithfully and primitively on a set Ω, such that the point stabiliser H has a normal abelian subgroup A, whose conjugates generate G, then G is simple.*

We want to show that the group $PSL_n(q)$ is perfect in order for it to satisfy the condition of Iwasawa's Lemma. We can do this by showing that $SL_n(q)$ is equal to its own commutator subgroup. For any two elements a and b, such that $a, b \in SL_n(q)$, the group generated by the operation $a^{-1}b^{-1}ab$ is equal to $SL_n(q)$.

Definition 3.7. A *transvection* is an elementary matrix that represents the addition of a multiple of a row/column added onto another row/column. It is typically generated by taking a identity matrix and replacing one of the zero elements with a non-zero element λ

First, we show that $SL_n(q)$ can be generated by transvections. And then we show that every transvection is a commutator of the group. This implies that $SL_n(q)$ would be perfect and therefore, $PSL_n(q)$ is perfect.

Lemma 3.8. $SL_n(q)$ is generated by transvections

Proof. Using the definition of transvections, we can say that the above claim is equivalent to saying that the elements of $SL_n(q)$ can be reduced to the identity matrix using the row operation $r_i \to r_i + \lambda r_j$.

An elementary result of matrices, *Gauss - Jordan Elimination*, says that all matrices that are invertible can be reduced to the identity matrix using elementary row operations as defined above. Since all matrices, by definition, in the group $SL_n(q)$ are invertible, we can say that it can be reduced to the identity matrix using the row operation $r_i \to r_i + \lambda r_j$. □

Next we show that $SL_n(q)$ is perfect, except for a few special cases.

Lemma 3.9. $PSL_n(q)$ is perfect for all n, q except for $SL_2(2)$ and $SL_2(3)$.

Proof. First, we show that every transvection is a commutator of the elements in the group. An easy calculation shows that

$$\left[\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&0&0\\0&1&0\\0&x&1\end{pmatrix}\right]=\begin{pmatrix}1&0&0\\0&1&0\\-x&0&1\end{pmatrix}$$

so with a suitable choice of a basis, we can say that if $n > 2$, then every commutator is a transvection in $SL_n(q)$. Hence, the result follows from the lemma 3.8. □

We now define abelian subgroup A, with the following property: if $n = 2$ and $q > 3$, then $\mathbb{F}_q$ contains at least one non zero element satisfying $x^2 \neq 1$. In such cases the commutator

$$\left[\begin{pmatrix}1&0\\y&1\end{pmatrix},\begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}\right]=\begin{pmatrix}1&0\\y(x^2-1)&1\end{pmatrix}$$

will be an arbitrary element of the abelian group A.

Now, we apply Iwasawa's lemma. If we take $n \geq 2$ and let $SL_n(q)$ act on a set Ω of the 1-dimensional subspaces of $\mathbb{F}_q^n$ so that the kernel of action is a set of scalar matrices, and thus we obtain an action of $PSL_n(q)$ on Ω. This action is primitive and faithful as $PSL_n(q)$ is perfect.

To study the stabiliser of a point we take 1 space $\langle\langle 1, 0, \ldots, 0\rangle\rangle$. The stabiliser then consists of matrices with first row $(\lambda, 0, \ldots, 0)$ for some $\lambda \neq 0$.

We can show that the subgroup of matrices with the shape $\begin{pmatrix}1&0_{n-1}\\v_{n-1}&I_{n-1}\end{pmatrix}$ where v_{n-1} is a arbitrary column vector with length $n-1$, is a part of the normal abelian subgroup A. Moreover, all non trivial elements are transvections. With a suitable basis, we can show that every transvection is contained as some conjugate of A.

Therefore, $PSL_n(q)$ satisfies all the conditions for Iwasawa's Lemma when $n > 2$ and $q > 3$. Hence the group $PSL_n(q)$ is simple if $n > 2$ and $q > 3$.

3.3 Subgroups of the General Linear Groups

Some of the important subgroups of the general linear group include B, N, T subgroups, and the *Weyl Group* [6].

This notation is also used in discussing general Lie Groups. Lie Groups have a $B - N$ pair, which is derived from these subgroups.

The subgroup B, also known as the *Borel Subgroup*, is the set of all lower triangular matrices (note: they are invertible so a part of $GL_n(q)$). N is a set of all monomial matrices (matrices consisting of only one non zero entry in every row and column).

The set $T = B \cap N$, called the *maximal split torus*, consists of all the diagonal matrices which forms a normal subgroup of N.

The quotient group $W = N/T$ is called the *Weyl Group*. This group is isomorphic to the symmetric group S_n consisting of all permutations of $n-$tuples of coordinates.

The Subgroup U of all lower uni-triangular matrices (lower trianglular matrices with diagonal entries 0), has an order of $q^{\frac{n(n-1)}{2}}$. Moreover, B is a semi-direct product of U and T so B has order $q^{\frac{n(n-1)}{2}} \cdot (q-1)^n$.

The *Borel Subgroup* can be defined as the stabiliser of a chain of subspaces.

$$0 = V_0 < V_1 < V_2 < V_3 < \cdots < V_N = V$$

.

These subspaces are defined by $V_i = \{(x_1, x_2, \ldots, x_i, 0, \ldots, 0)\}$ such that $\dim(V_i) = i$. Such a chain of subspaces is known as a flag and if the chain has a subspace with each possible dimension then it is known as the *maximal flag*. Thus B is the stabiliser of a maximal flag.

The *parabolic subgroups* are the stabilisers of flags, and the maximal parabolic subgroup is the stabiliser of the subspaces W such that $0 < W < V$. If W has a dimension k, then we can choose a basis for W such as $\{e_1, e_2, \ldots, e_k\}$ and extend it in the form $\{e_1, e_2, e_3, \ldots, e_n\}$ to make a basis for V. The elements which form the stabiliser of the subspace W then have the shape $\begin{pmatrix} A & 0 \\ C & D \end{pmatrix}$. Where A and D are invertible $k \times k$ and $(n-k) \times (n-k)$ matrices respectively, and C is an arbitrary matrix with dimensions $k \times (n-k)$.

4 The Bilinear Form and Symplectic Groups

4.1 Bilinear Forms

The symplectic groups are defined using a bilinear form which is defined below.

Definition 4.1. A *bilinear form* is map $V \times V \to F$ where V is a vector space and F is a field. The function $B : V \times V \to F$ is linear in each argument separately. It has the following properties

- $B(u + v, w) = B(u, w) + B(v, w)$
- $B(u, v + w) = B(u, v) + B(u, w)$
- $B(\lambda u, v) = B(u, \lambda v) = \lambda B(u, v)$

An example of such a map is the vector dot product in $\mathbb{R}^n$

Bilinear forms can be classified into 3 different categories: *symmetric, skew-symmetric, alternating.*

- If $B(u, v) = B(v, u)$ the map is symmetric
- If $B(u, v) = -B(v, u)$ the map is skew-symmetric
- If $B(u, u) = 0$ the map is alternating

We can show that any alternating form is also skew-symmetic.

Lemma 4.2. An alternating bilinear form is skew-symmetric

Proof. We have for all w, $B(w, w) = 0$. So let $w = u + v$ for some u and v. We can say such u and v exist since we are in a field, so we can just take $u = w$ and $v = 0$. Accordingly, we have

$$\begin{aligned} 0 &= B(u + v, u + v) \\ &= B(u, u) + B(u, v) + B(v, u) + B(v, v) \\ &= B(u, v) + B(v, u) \end{aligned}$$

This means that, $B(u, v) = -B(v, u)$. □

We can represent the bilinear forms using matrices. Given any vector space V, with the basis $\{e_1, e_2, e_3, \ldots, e_n\}$, the associated $n \times n$ matrix A of a bilinear form with basis V is given by $A_{ij} = B(e_i, e_j)$. The associated matrix is symmetric or skew-symmetric if the bilinear form is symmetric or skew-symmetric, respectively.

Definition 4.3. A bilinear form is called *singular* if the associated matrix is not invertible. Conversely, it is non-singular if the matrix is invertible.

We now look at the properties of vector spaces that characterize the properties of the bilinear form f.

Definition 4.4. We say $a \perp b$ if $f(a,b) = 0$ i.e. a and b are *perpendicular* or *orthogonal*. Furthermore, for any set S, we say $S^{\perp} = \{a \in V : a \perp s, \forall s \in S\}$. $S^{\perp}$ is termed as the *orthogonal complement* of S

A non zero vector perpendicular to itself is called isotropic. Also, we can say that $f(v,v)$ is the norm of v. The radical of f denoted by rad f is the set $V^{\perp}$, and f is considered non singular if the radical is non zero, and singular otherwise.

Definition 4.5. If f is a form on a vector space V , an *isometry* of f is a linear map $g : V \to V$ which preserves the form, in the sense that $f(u^g, v^g) = f(u,v)$ for all $u, v \in V$. The *isometry group* is the group of all such maps.

We obtain different classical groups from the isometries of forms that are non linear. We classify the forms in order to classify the groups. This is done by varying the basis in a such a way that the corresponding matrix of that form takes a specific shape. Accordingly, given any bilinear form f, we want to take a basis such that f is not too complicated. If there are any two vectors a and b, with $f(a,b) = \lambda$ where $\lambda \neq 0$, then chose the first two basis vectors as $e_1 = a$ and $f_1 = \lambda^{-1}b$. This means that

$$f(e_1, f_1) = -f(f_1, e_1) = 1$$
$$f(e_1, e_1) = f(f_1, f_1) = 0$$

Now, if we restrict the form to $\{e_1, f_1\}^{\perp}$ and continue, we will find that we get the basis vectors $e_1, e_2, e_3, \ldots, e_m$ and $f_1, f_2, f_3, \ldots, f_m$. This basis is known as a *symplectic basis*, and the form f will be termed as a *symplectic form*. A property of this bilinear form is that for all basis vectors e_i and f_j where $i \neq j$, we have $f(e_i, f_j) = 0$. Otherwise, we have $f(e_i, f_i) = -f(f_i, e_i) = 1$

4.2 Symplectic Groups

A Symplectic Group is classical groups that is defined as follows

Definition 4.6. The *symplectic group* $Sp_{2m}(q)$ is the isometry group of a non-singular alternating bilinear form f on $V \cong \mathbb{F}_{2q}^n$

In other words, it is the subgroup of $GL_{2m}(q)$ consisting of all elements g such that $f(u^g, v^g) = f(u, g)$ for all $u, v \in V$. From our knowledge of bilinear forms, we can say that $Sp_2m(q)$ has a symplectic basis $\{e_1, e_2, e_3, \ldots, f_1, f_2, f_3, \ldots, f_m\}$ such that all vectors are *perpendicular* to each other except those in the form e_i, f_i.

We know that $f(\lambda u, \lambda v) = \lambda^2 f(u, v)$ which equals to $f(u, v)$ if and only if $\lambda^2 = 1$ or $\lambda = \pm 1$. So the only scalars of $Sp_{2m}(q)$ are ± 1. If we quotient these out we get $PSp_{2m}(q)$. This group is also simple in most cases and the proof will be given later.

4.3 Order of the Symplectic Group

Similar to the special linear groups, the symplectic groups also have an equation that encompasses their orders depending on the finite field that is being used. To calculate the order, we need to count the number of ways to find a symplectic basis.

We know that e_1 can be any non zero vector. Since there are $2m$ entries, and only 1 vector can be classified as a zero vector, there are $q^{2m}-1$ ways to choose it. Therefore, we can say that $e_1^{\perp}$ has dimension $2m-1$, which means it has q^{2m-1} vectors. This implies that there are $q^{2m} - q^{2m-1}$ different vectors v such that $f(u, v) \neq 0$. These come in sets of $q-1$ scalar multiples, one for each possible value for f_1, implying that there are q^{2m-1} different choices of vectors. Doing this for all e_i and f_i, we get

$$\begin{aligned} |Sp_{2m}(q)| &= \prod_{i=1}^{m} (q^{2i} - 1) \cdot q^{2i-1} \\ &= q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1) \end{aligned}$$

4.4 Simplicity of $PSp_{2m}(q)$

Similar to the special linear group, the projective symplectic group is also simple for all cases where $m > 2$ and $q > 3$. We use a similar strategy as before where we use Iwasawa's Lemma to prove the simplicity of the group. We make use of transvections again, but this time we will be looking over *Symplectic Transvection*.

Definition 4.7. A *symplectic transvection* is a linear map in the form

$$T_v(\lambda) : x \mapsto x + \lambda f(x, v)v$$

Where f is a fixed non singular bilinear form (symplectic form) on the vector space V where $v \neq 0$ and $\lambda \neq 0$.

As provided in [9, Section 3.5.2], the sketch of the proof involve that we show that the group generated by symplectic transvections S is congruent to the group $SP_{2m}(q)$. We also want to show that S acts transitively on the set of ordered symplectic bases. After investigating the stabiliser, it follows that $S = SP_{2m}(q)$. Then we use Iwasawa's Lemma to prove that $PSp_{2m}(q)$ is simple.

Lemma 4.8. The set S generated by symplectic transvections acts transitively on the set of ordered symplectic bases.

Proof. Let v, w be two distinct non-zero vectors. If $f(v, w) = \lambda \neq 0$, then the transvection maps v to w such that $T_{v-w}(\lambda^{-1}) : v \mapsto w$. Otherwise, we pick another vector x such that $f(v, x) \neq 0$ and $f(w, x) \neq 0$. We can say that such an x exists because f is non singular, which means that $\exists y, z$ with $f(v, y) = f(w, z)$ and $f(v, z) \neq 0$ and $f(w, y) \neq 0$. Hence a suitable, linear combination of y and z has the required properties. Next, we can map v to x and x to w, and deduce that S acts transitively on non zero vectors, which includes the set of symplectic bases.

Suppose we take a fixed vector u, and $f(u, w) = f(v, w) = \lambda \neq 0$. Then, $T_{v-w}(\lambda^{-1})v \mapsto w$ fixes u. Otherwise, let $x = u + v$, so that $f(u, x) = 1$ and $f(v, x) = f(w, x) = -1$, so we can map v to x and x to w while fixing u. We can then use induction to show that S is transitive on symplectic bases, which means $Sp_{2m}(q)$ is generated by symplectic transvections. □

We have shown that the hypothesis of Iwasawa's Lemma is true. The above lemma shows that it is generated by symplectic transvections. When $Sp_{2m}(q)$ acts on one dimensional spaces, we proved that the stabiliser of a point is transitive to the q^{2m-1} points to which it is not orthogonal. It is also transitive to the $\frac{q^{2m-1}-1}{q-1} - 1$ points which are orthogonal but not equal to it. If we take vectors v and w both orthogonal to u, then either $f(v, w) = \lambda \neq 0$ in which case $T_{v-w}(\lambda^{-1}) : v \mapsto w$, otherwise, there exists a vector x with $f(v, x) = 0 = f(w, x)$ and we can map v via x to w while fixing u. So the action is primitive.

Moreover, we can show that symplectic transvections $T_v(\lambda)$ for a fixed vector v forms a normal abelian subgroup of stabiliser of the point $\langle v \rangle$.

Lemma 4.9. $Sp_2(q) \cong SL_2(q)$

Proof. As discussed in [7], if we write the elements of $V = k^2$ as row vectors, we can define

$$f : V \times V \to k, (x, y) \mapsto \det \begin{pmatrix} x \\ y \end{pmatrix}$$

It is clear that f is a symplectic form. Now if $X \in GL_2(q)$, then we have

$$f(xX, yX) = \det \begin{pmatrix} xX \\ yX \end{pmatrix} = \det \begin{pmatrix} x \\ y \end{pmatrix} \cdot \det(X)$$

Thus $f(xX, yX) = f(x, y)$ if and only if $\det(X) = 1$, which is true for all $X \in SL_2(q)$. □

Now we need to verify that the symplectic transvections are commutators, which would imply that the group is perfect, meeting the last condition of Iwasawa. This can be inferred for all $q > 3$ since $Sp_2(q) \cong SL_2(q)$, which means that $PSp_{2m}(q)$ is simple for all $q > 3$.

4.5 Subgroups of the Symplectic Groups

We can construct the subgroups of the symplectic groups similar to that of the general linear group. We take the *Borel Subgroup* B to be the stabiliser for the maximal flag of the subspaces

$$0 < W_1 < W_2 < \cdots < W_m = (W_m)^\perp < (W_{m-1})^\perp < \cdots < (W_1)^\perp < V$$

We define the subspace W_k as $\{e_1, e_2, e_3, \ldots, e_k\}$ where e_i is a basis vector of V. Note: we order the basis of V as $\{e_1, e_2, \ldots, e_m, f_m, f_{m-1}, \ldots, f_1\}$ to emphasize the structure.

We define maps on these basis vectors to fix all the vectors e_k and f_k except

$$\begin{aligned} x_{ij}(\lambda) : f_i &\mapsto f_i + \lambda f_j \\ e_j &\mapsto e_j - \lambda e_i \\ y_{ij}(\lambda) : f_i &\mapsto f_i + \lambda e_j \\ f_j &\mapsto f_j + \lambda e_i \end{aligned}$$

We can show that the group of unitriangular matrices U is generated by these maps in conjunction with the symplectic transvections $T_{e_i}(-\lambda) : f_i \mapsto f_i - \lambda e_i$.

The torus T is defined by the diagonal maps $f_i \mapsto \lambda f_i$ and $e_i \mapsto \lambda^{-1} e_i$. This means it is the semi-direct product of cyclic groups of order $q - 1$ and similar to the general linear groups, $B = UT$.

5 Sesquilinear Forms and Unitary Group

5.1 Sesquilinear Forms

A sesquilinear form is a generalization of a bilinear form, and forms the basis of Unitary Groups.

Definition 5.1. An *automorphism* is an isomorphism from a field onto itself. The order of the automorphisms is the number of possible isomorphisms which map the field to itself.

We will use fields with automorphism of order 2 to describe sesquilinear form. This field will have order q^2 where q is a prime power (see section 2). We define $\bar{x} = x^q$ for all $x \in \mathbb{F}_{q^2}$. A *conjugate symmetric sesquilinear form* is defined over a vector space V as a map $f : V \times V \to F$ satisfying the following properties.

- $f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$
- $f(w, v) = \bar{f(v, w)}$

From the above properties it follows:

$$f(u, \lambda v + w) = \bar{\lambda} f(u, v) + f(u, w)$$

We want to find a basis for sesquilinear forms that is as convenient as possible. For a sesquilinear form f, if we choose a vector a such that $f(a, a) \neq 0$, then $f(a, a) = \bar{f(a, a)}$. Moreover, the multiplicative group of the field $\mathbb{F}_{q^2}$ has order $q^2 - 1$. This means $\exists \lambda \in \mathbb{F}_{q^2}$ such that $\lambda\bar{\lambda} = \lambda^{q+1} = f(a, a)$. Accordingly, we have vector $e_1 = \lambda^{-1} \cdot a$ satisfying $f(e_1, e_1) = 1$.

Now we restrict the form f just to $e_1^{\perp}$, which means all vectors b in this restricted space have $f(b, b) = 0$. Then, $\forall u, v$ we have

$$\begin{aligned} 0 &= f(u + \lambda v, u + \lambda v) \\ &= f(u, u) + \bar{\lambda} f(u, v) + \lambda f(v, u) + \lambda\bar{\lambda} f(v, v) \\ &= \bar{\lambda} f(u, v) + \lambda f(v, u) \end{aligned}$$

Therefore, we can choose 2 values of λ forming a basis from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$. For the sake of simplicity, we choose $\lambda_1 = 1$ and $\lambda_2 \neq \bar{\lambda_2}$. If we solve the equations for the values of $f(u, v)$ and $f(v, u)$, we get that both of them are 0. This means that if the form is non singular, then we have found a basis where every vector (all of norm 1), is perpendicular to all other vectors. Such basis is termed as an *orthonormal basis*.

5.2 The Unitary Group

Definition 5.2. A *unitary group* is an isometry groups of a non singular sesquilinear form over a vector space V. This means it is a subgroup of $GL_n(q^2)$ containing all elements g such that $\forall u, v \in V \ f(u^g, v^g) = f(u, v)$.

In simpler terms, the unitary group $GU_n(q)$ has the property that $g\bar{g}^T = I_n$ $\forall g \in GU_n(q)$ that is the inverse of all elements g is the transpose of the conjugate of g. This means that if $\det(g) = \lambda$, and by definition $\lambda\bar{\lambda} = \lambda^{q+1}$, we have that $\lambda^{q+1} = 1$. Now since λ is in a cyclic group of order $q^2 - 1 = (q+1)(q-1)$, this statement is equivalent to saying λ is in a unique subgroup of order $q+1$. This subgroup is called the Special Unitary Group and it consists of all $g \in GU_n(q)$ such that $\det(g) = 1$.

There are $q+1$ such λ in $\mathbb{F}_{q^2}$. We can say that the center of this group Z has order $q+1$ and consists of all scalar matrices λI_n. The quotient $GU_n(q)/Z$, denoted by $PGU_n(q)$ is known as the projective general unitary group. Similarly, by finding the quotient of the Special Unitary group with its center gives us the projective special unitary group, denoted by $PSU_n(q)$

5.3 Order of the Unitary Group

To find the order of the group we need to find the number of vectors with norm 1. We defined z_n to be the norm 0 vectors, and y_n to be the norm 1 vectors, where n is the dimension of the vector space. The total number of vectors is given by q^{2n} which can also be written as $1 + z_n + y_n(q-1)$. We can recursively solve for z_n to get the relation $z_{n+1} = z_n + y_n(q^2-1)$. Solving the characteristic polynomial of this relation, we get $z_n = (q^n - (-1)^n)(q^n + (-1)^n)$. Solving for y_n we get $y_n = q^{n-1}(q^n - (-1)^n)$. We can inductively iterate through n to get the order. Since we want an orthonormal basis, by choosing one vector at a time, we have

$$\begin{aligned} |GU_n(q)| &= \prod_{i=1}^{n} q^{i-1}(q^i - (-1)^i) \\ &= q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - (-1)^i) \end{aligned}$$

5.4 Simplicity of PSU_n

The proof of simplicity of $PSU_n$is similar to that for symplectic groups, therefore we will only write the sketch of the proof. Since $PSU_2(q) \cong PSL_2(q)$, we need to consider $n > 2$. The Iwasawa's Lemma in this case is applied to the permutations of the isotropic spaces with unitary transvections as the generators.

Definition 5.3. A *unitary transvection* T_v is defined as

$$T_v(\lambda) : x \mapsto x + \lambda f(x, v)v$$

Where $\lambda \neq 0$ and $v \neq 0$.

We can show that the unitary transvection $T_v(\lambda)$ is isometric if and only if $\lambda = 0$ or $\lambda^{q-1} = -1$. Since $\lambda \neq 0$, we will define the unitary transvections with $\lambda^{q-1} = -1$.

The sketch of the proof involves the following steps. Step 1: prove that the unitary transvections for any fixed v will form an abelian subgroup with stabiliser $\langle v \rangle$. Step 2: show that the group acts primitively on the set of 1-isotropic spaces. Step 3: show that the unitary transvections generate $SU_n(q)$ in all cases except $SU_3(2)$. Step 4: show that all unitary transvections are commutators of $SU_n(q)$ for $n > 3$. Using Iwasawa's lemma, it follows that $PSU_n(q)$ is simple for all cases where $n > 3$.

6 Acknowledgements

This study was done during Summer 2023 as a part of the "Independent Research and Paper Writing" course at Euler's Circle. It was completed under the guidance of Professor Simon Rubinstein-Salzedo of Euler Circle and Lisa Liu of Stanford University. I thank them for their support and guidance in writing this paper.

References

[1] Alejandro Adem and R. James Milgram. *Finite Groups of Lie Type*, pages 213–243. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[2] Marjorie Lee Browne. A note on the classical groups. *The American Mathematical Monthly*, 62(6):424–427, 1955.

[3] Keith Conrad. Simplicity of $\mathrm{PSL}_n(q)$.

[4] Gustavo de Paula and Andre Nies. Primitive group actions and their descriptions. *University of Auckland Journal*, 2009.

[5] David Forney. *Principles of Digital Communication*, chapter 7. Finite Fields. 2019.

[6] Hiss Gerhard. Finite groups of lie type and their representation. *Lehrstuhl D f¨ur Mathematik*, 2006.

[7] Nick Gill and Pablo Spiga. Binary permutation groups: alternating and classical groups. *Am. J. Math.*, 142(1):1–43, 2020.

[8] Brian C. Hall. *Elementary Introduction to Groups and Their Representations.* Springer, 2000.

[9] Robert A. Wilson. *The finite simple groups.*, volume 251 of *Grad. Texts Math.* London: Springer, 2009.