Finite Groups of Lie Type

Vishwasri Srinivasan

July 2024

1 Introduction

The study of finite groups of Lie type occupies a central position in modern algebra and group theory. These groups, first systematically explored by Évariste Galois in the early 19th century and later formalized by Sophus Lie, serve as a link between algebraic structures and geometric intuitions. They are used in diverse areas of mathematics, such as representation theory, combinatorics, and number theory. This paper aims to provide an exposition on finite groups of Lie type, with a focus on understanding their construction, orders, and the conditions under which they are simple. We begin by discussing the foundational concepts of algebraic groups and fields before providing an introduction of finite groups of Lie type. We then examine several key families of these groups, including the general linear group $GL_n(\mathbb{F}_q)$, the special linear group $SL_n(\mathbb{F}_q)$, and the orthogonal group, highlighting their construction fundamental properties, and simplicity conditions.

1.1 Groups

A **group** $(G, \cdot)$ is a set G equipped with a binary operation $\cdot$ that satisfies the following four axioms:

1. **Closure:** For all $a, b \in G$, the result of the operation $a \cdot b$ is also in G.
2. **Associativity:** For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. **Identity Element:** There exists an element $e \in G$ such that for every element $a \in G$, the equation $e \cdot a = a \cdot e = a$ holds.
4. **Inverse Element:** For each element $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$, where e is the identity element.

One example is $G = \mathbb{Z}$, the set of integers and consider the binary operation of addition, denoted by $+$. We will show that $(\mathbb{Z}, +)$ forms a group.

1. Closure: For any two integers $a, b \in \mathbb{Z}$, the sum $a + b$ is also an integer, thus closure holds.

2. Associativity: Addition of integers is associative, i.e., for all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.

3. Identity Element: The identity element for addition in $\mathbb{Z}$ is 0, as $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$.

4. Inverse Element: For each integer $a \in \mathbb{Z}$, its inverse with respect to addition is $-a$, since $a + (-a) = (-a) + a = 0$.

Therefore, $(\mathbb{Z}, +)$ satisfies all the axioms and is a group.

The **order of a group** G, denoted $|G|$, is the number of elements in the set G. If $|G|$ is finite, G is called a **finite group**.

The **order of an element** g in a group G is the smallest positive integer n such that $g^n = e$, where e is the identity element of G.

A **subgroup** H of a group G is a subset of G that forms a group under the operation of G.

An important theorem relating to this definition is the Two-Step Subgroup Test.

1.1.1 Two-Step Subgroup Test

Let G be a group and H a non-empty subset of G. Then H is a subgroup of G if and only if the following two conditions hold:

1. For all $a, b \in H$, the product $ab \in H$. (Closure under operation)
2. For all $a \in H$, the inverse $a^{-1} \in H$. (Closure under inverses)

Proof: To prove the Two-Step Subgroup Test, we will show the following:

- If H is a subgroup of G, then conditions (1) and (2) hold.
- If conditions (1) and (2) hold, then H is a subgroup of G.

For the first part of the proof, assume H is a subgroup of G. By definition, H satisfies the group axioms under the operation inherited from G. In particular:

1. Closure under operation: Since H is a group, for any $a, b \in H$, the product $ab \in H$.
2. Closure under taking inverses: Since H is a group, for any $a \in H$, the inverse $a^{-1} \in H$.

Therefore, if H is a subgroup of G, conditions (1) and (2) hold.

For the second part of the proof, assume the two conditions hold. Now, we need to verify the subgroup axioms for H:

1. **Identity Element:** Since H is non-empty, let e be the identity element of G. Let $a \in H$. Since $a \in H$ and H is closed under inverses, $a^{-1} \in H$. Since H is closed under multiplication, $aa^{-1} = e \in H$.

2. **Associativity:** The operation on H is inherited from G, which is associative. Therefore, the operation is associative on H.

3. **Closure under multiplication:** This is given by condition (1).

4. **Inverse Element:** This is given by condition (2).

Therefore, H satisfies the subgroup axioms and is a subgroup of G.

A **normal subgroup** N of a group G is a subgroup that is invariant under conjugation by any element of G. That is, $N \triangleleft G$ if for every $n \in N$ and $g \in G$, the element $gng^{-1} \in N$.

Consider the group $G = (\mathbb{Z}, +)$, where $\mathbb{Z}$ is the set of integers under addition. Let $H = 2\mathbb{Z}$ be the subgroup of even integers in G. H is a normal subgroup of G since for any $n \in \mathbb{Z}$ and $h \in H$, we have $n + h + (-n) \in H$.

1.1.2 Relations between Groups

A **homomorphism** between two groups G and H is a function $\phi : G \to H$ that preserves the group operation. More formally, a homomorphism satisfies the condition that for all $a, b \in G$, $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, where $\cdot$ denotes the group operation in G and H.

Let G and H be algebraic structures of the same type. An **isomorphism** $\phi : G \to H$ is a bijective homomorphism that preserves the operations of the structures.

Homomorphisms generalize the concept of isomorphisms by allowing for non-bijective mappings that preserve the group structure.

Let $\phi : G \to H$ be a homomorphism between groups G and H. The **kernel** of ϕ, denoted by $\ker(\phi)$, is defined as $\ker(\phi) = \{g \in G : \phi(g) = e_H\}$, where e_H is the identity element of H. The **image** of a homomorphism is defined as $\mathrm{Im}(\phi) = \{\phi(g) : g \in G\}$, which is a subgroup of H.

A **simple group** has no nontrivial normal subgroups. Examples include the alternating group A_n for $n \geq 5$. Now, we will discuss a way to classify a certain kind of simple group.

1.1.3 Classification Theorem

The **Classification Theorem for Finite Simple Groups** states that every finite simple group belongs to one of the following categories:

1. Cyclic groups of prime order.
2. Alternating groups of degree at least 5.
3. Simple groups of Lie type.
4. 26 sporadic groups.

We will focus on **finite groups of Lie type**, groups that can be seen as the group of rational points over a finite field of a connected type Lie group. Before introducing our first finite group of Lie type, we must discuss the a few more definitions.

1.1.4 Group Actions

A **group action** of a group G on a set X is a function $\cdot : G \times X \to X$ that satisfies certain properties, such as the identity element acting as the identity function on X.

Some examples of group actions are rotation of a cube, permutation of a set, symmetries of a polygon.

A group action is said to be **faithful** if different group elements induce different permutations of the set X.

A group action of a group G on a set X is said to be **transitive** if, for any $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$.

A group G acts **primitively** on a set Ω if the only blocks of Ω preserved by G are the trivial ones: $\emptyset$ and Ω.

Also, in the context of group actions, a **block** is a non-empty subset B of the set X such that for all $g \in G$, either $g \cdot B = B$ or $g \cdot B \cap B = \emptyset$.

The **stabilizer** of an element x in a group action is the subgroup that fixes x, while the **orbit** of x is the set of all elements in X that x can be mapped to under the group action.

A **permutation groups** is a group whose elements are permutations of a set, forming a group under composition.

The **commutator subgroup** is the group generated by all the commutators $aba^{-1}b^{-1}$ for a, b in the group.

A group G is called **perfect** if G is equal to its commutator subgroup G'.

1.2 Fields

A **field** is a set equipped with two operations, addition and multiplication, satisfying certain properties like closure, associativity, distributivity, and the existence of inverses.

A **subfield** of a field is a subset that is itself a field under the same operations.

The **order of a field** is the number of elements in the field, and a finite field is a field with a finite number of elements.

1.3 Some Basic Linear Algebra

A **vector space** is a set of vectors equipped with two operations, vector addition and scalar multiplication, satisfying certain properties.

Examples include the set of all real-valued functions defined on a closed interval, with operations defined pointwise.

Also, a square matrix A is said to be **invertible** if there exists another square matrix B such that $AB = BA = I$, where I is the identity matrix.

2 General Linear Group

The **general linear group** $GL_n(\mathbb{F})$ is the group of all invertible $n \times n$ matrices with entries from a field $\mathbb{F}$, under the operation of matrix multiplication. Formally,

$$GL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid \det(A) \neq 0\},$$

where $M_n(\mathbb{F})$ denotes the set of all $n \times n$ matrices over $\mathbb{F}$, and $\det(A)$ is the determinant of A.

For $n \geq 2$, the group $GL_n(\mathbb{F})$ is not simple because it has a non-trivial normal subgroup, the **center** $Z(GL_n(\mathbb{F}))$, consisting of scalar matrices:

$$Z(GL_n(\mathbb{F})) = \{\lambda I_n \mid \lambda \in \mathbb{F}^*\},$$

where $\mathbb{F}^*$ is the multiplicative group of the field $\mathbb{F}$.

2.0.1 Center of $GL(n, F)$ is a Normal Subgroup

Note that the proof is clear for $n = 1$, so we consider the case where $n \geq 2$ here. Suppose i, j are distinct elements of $\{1, 2, 3, \ldots, n\}$ and $\lambda \in F$. Define $e_{ij}(\lambda)$ to be the matrix with λ in the $(ij)^{\text{th}}$ entry and zeroes elsewhere. $e_{ij}(1)$ is termed the $(ij)^{\text{th}}$ matrix unit. Define $E_{ij}(\lambda)$ as the sum of the identity matrix and $e_{ij}(\lambda)$:

$$E_{ij}(\lambda) = I + e_{ij}(\lambda).$$

Since, $E_{ij}(\lambda)$ and $E_{ij}(-\lambda)$ are two-sided multiplicative inverses for any $\lambda \in F$, $E_{ij}(\lambda) \in GL(n, F)$. Any matrix that commutes with $E_{ij}(1)$ must also commute with $e_{ij}(1)$, because of distributivity and the fact that the matrix commutes with the identity. Thus, any matrix in the center of $GL(n, F)$ commutes with $e_{ij}(1)$ for $i \neq j$. Suppose A is a matrix with $a_{ji} \neq 0$ for some $i \neq j$. Consider the matrix $B = e_{ij}(1)$. Then, the $(jj)^{\text{th}}$ entry of AB is nonzero, while the $(jj)^{\text{th}}$ entry of BA is zero. Thus, any matrix that commutes with all the off-diagonal matrix units $e_{ij}(1)$ cannot have any off-diagonal entries. Suppose A is a diagonal matrix with $a_{ii} \neq a_{jj}$. Then A does not commute with the permutation matrix corresponding to the transposition of i and j, because conjugation by that matrix switches a_{ii} with a_{jj}.

Combining the first two steps yields that any matrix in the center of $GL(n, F)$ must be diagonal, and the third step then yields that it must be scalar. Looking at when two scalar matrices commute, we see that the matrix must in fact be a scalar matrix with the scalar value itself a nonzero element of F.

To show that $Z(GL(n, F))$ is a normal subgroup, we need to show that for any $g \in GL(n, F)$ and any $z \in Z(GL(n, F))$, the element gzg^{-1} is also in $Z(GL(n, F))$. Since z is a scalar matrix, say $z = \lambda I$ for some $\lambda \in F$, we have:

$$gzg^{-1} = g(\lambda I)g^{-1} = \lambda(gIg^{-1}) = \lambda I = z.$$

Therefore, $gzg^{-1} = z \in Z(GL(n, F))$, proving that the center $Z(GL(n, F))$ is a normal subgroup of $GL(n, F)$.

2.1 Projective General Linear Group

The **projective general linear group** $PGL_n(\mathbb{F})$ is defined as the quotient group:

$$PGL_n(\mathbb{F}) = GL_n(\mathbb{F})/Z(GL_n(\mathbb{F})).$$

For $n \geq 2$ and $\mathbb{F}$ a finite field, $PGL_n(\mathbb{F})$ is simple.

2.1.1 Simplicity of $PGL_n(\mathbb{F})$

We will prove that $PGL_n(\mathbb{F})$ is simple for $n \geq 2$ and $\mathbb{F}$ a finite field. Let N be a non-trivial normal subgroup of $PGL_n(\mathbb{F})$. We need to show that $N = PGL_n(\mathbb{F})$. Consider the action of $PGL_n(\mathbb{F})$ on the projective space $\mathbb{P}^{n-1}(\mathbb{F})$. The group $PGL_n(\mathbb{F})$ acts transitively on $\mathbb{P}^{n-1}(\mathbb{F})$. This means that for any two points in $\mathbb{P}^{n-1}(\mathbb{F})$, there exists an element in $PGL_n(\mathbb{F})$ that maps one point to the other. Consider the stabilizer subgroup of a point in $\mathbb{P}^{n-1}(\mathbb{F})$. This stabilizer is isomorphic to $PGL_{n-1}(\mathbb{F})$. Since $PGL_{n-1}(\mathbb{F})$ is simple for $n-1 \geq 2$, any normal subgroup of $PGL_n(\mathbb{F})$ must either act trivially on $\mathbb{P}^{n-1}(\mathbb{F})$ or be the whole group. Since N is non-trivial, it must act non-trivially on $\mathbb{P}^{n-1}(\mathbb{F})$. Therefore, N must be the whole group $PGL_n(\mathbb{F})$.

We have shown that any non-trivial normal subgroup of $PGL_n(\mathbb{F})$ must be the whole group. Therefore, $PGL_n(\mathbb{F})$ is simple for $n \geq 2$ and $\mathbb{F}$ a finite field.

3 Special Linear Group

The **special linear group** $SL_n(\mathbb{F})$ is the group of all $n \times n$ matrices with determinant 1, under the operation of matrix multiplication. Formally,

$$SL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid \det(A) = 1\}.$$

Note that this group can also be defined as the kernel of the homomorphism

$$\det : GL(n, F) \to F^\times = \{x \in F \mid x \neq 0\}$$

where F is a field.

3.0.1 $SL_n(\mathbb{F})$ is a normal subgroup of $GL_n(\mathbb{F})$

Because the determinants of the elements of $SL_n(\mathbb{F})$ are not 0, they are nonsingular. So $SL_n(\mathbb{F})$ is a subset of $GL_n(\mathbb{F})$. With this, we need only to show that $SL_n(\mathbb{F})$ is a subgroup of $GL_n(\mathbb{F})$. Let $\mathbf{A}$ and $\mathbf{B}$ be elements of $SL_n(\mathbb{F})$. Since $\mathbf{A}$ is nonsingular we have that it has an inverse $\mathbf{A}^{-1} \in \mathrm{GL}(n, K)$. As

$$\det\left(\mathbf{A}^{-1}\right) = \frac{1}{\det(\mathbf{A})}$$

, we can say

$$\det\left(\mathbf{A}^{-1}\right) = 1$$

So $\mathbf{A}^{-1} \in \mathrm{SL}(n, K)$. Also,

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B}) = 1$$

Using the Two-Step Subgroup Test, we can now say that $SL_n(\mathbb{F})$ is a subgroup of $GL_n(\mathbb{F})$. To prove that it is a normal subgroup of the latter, suppose $A \in SL_n(F)$ and $B \in GL_n(F)$. Now

$$\det\left(BAB^{-1}\right) = \det(B) \det(A) \det(B)^{-1} = \det(A) = 1,$$

since multiplication in F is commutative. Since, $BAB^{-1} \in SL_n(F)$, $SL_n(F)$ is normal in $GL_n(F)$.

3.0.2 $SL_n(\mathbb{F})$ is the commutator subgroup of $GL_n(\mathbb{F})$

Let N be the commutator subgroup of the general linear group $\mathrm{GL}(2, F)$, defined as:

$$N = \left\langle ABA^{-1}B^{-1} \mid A, B \in \mathrm{GL}(2, F) \right\rangle.$$

First, it is clear that N is contained in the special linear group $\mathrm{SL}(2, F)$, since $\det(ABA^{-1}B^{-1}) = 1$ for any $A, B \in \mathrm{GL}(2, F)$. Next, we claim that N contains all matrices

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

where $b \in F$.

This follows from noting that

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & b \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}.$$

By taking transposes, it also follows that N contains all matrices

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix},$$

where $c \in F$.

Further, N contains all matrices

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

where $a \in F^{\times}$, since

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}.$$

Now let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, F).$$

Then $ad - bc = 1$. Using the above results,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix} \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

if $a \neq 0$, and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -d/b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ab & 1 \end{pmatrix} \begin{pmatrix} 1/b & 0 \\ 0 & b \end{pmatrix},$$

if $b \neq 0$, and similarly for other cases.

Thus, $\mathrm{SL}(2, F) \subseteq N$, implying $N = \mathrm{SL}(2, F)$ for finite fields F. This completes the proof.

3.1 Orders of $SL_n(\mathbb{F}_q)$ and $GL_n(\mathbb{F}_q)$

The finite groups $GL(n, q), SL(n, q)$ have orders:

$$|GL(n, q)| = q^{\frac{n(n-1)}{2}} (q^n - 1) \left(q^{n-1} - 1\right) \cdots (q - 1)$$
$$|SL(n, q)| = q^{\frac{n(n-1)}{2}} (q^n - 1) \left(q^{n-1} - 1\right) \cdots \left(q^2 - 1\right)$$

Proof: Let V be an n-dimensional vector space over $F = GF(q)$. Then V has q^n elements. Choose a basis $(v_1, v_2, \cdots, v_n)$ for V. Then an automorphism f of V is given by its value on the basis. There are $q^n - 1$ choices for $f(v_1)$. Given $f(v_1)$, there are $q^n - q^1$ choices for $f(v_2)$ since it can be any vector not in the span of $f(v_1)$. There are $q^n - q^2$ choices for $f(v_3)$ and so on. Thus

$|GL(V)| = (q^n - 1)(q^n - q) \cdots \left(q^n - q^{n-1}\right) = q^{1+2+\cdots+(n-1)}(q^n - 1) \cdots (q-1)$

And $|SL(n,q)| = |GL(V)| / |F^\times| = |GL(n,q)|/(q-1)$.

3.2 Projective Special Linear Group

The **projective special linear group** $PSL_n(\mathbb{F})$ is defined as the quotient group:

$$PSL_n(\mathbb{F}) = SL_n(\mathbb{F})/Z(SL_n(\mathbb{F})),$$

where $Z(SL_n(\mathbb{F}))$ is the center of $SL_n(\mathbb{F})$, consisting of scalar matrices with determinant 1.

3.2.1 Properties of $PSL_n(\mathbb{F})$

1. **Quotient Group:** $PSL_n(\mathbb{F})$ is formed by identifying matrices in $SL_n(\mathbb{F})$ that differ by a scalar matrix.
2. **Simplicity:** For $n \geq 2$ and $\mathbb{F}$ a finite field, $PSL_n(\mathbb{F})$ is simple.

3.2.2 Examples of $PSL_n(\mathbb{F})$

Let's look at the case $n = 2$ and $q = 5$, i.e. 2 by 2 matrices whose entries are integers mod 5. This is the smallest example of $\mathrm{PSL}(n,q)$ which is a simple group. We denote these matrices by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and the requirement of having determinant 1 means $ad - bc = 1$. A rough estimate of the number of matrices in $\mathrm{SL}(2,5)$ would be 125 since we have three degrees of freedom (four variables minus constraining equation) and each degree of freedom can take on five possible values. However, as you cannot always fix three variables and solve for the fourth, the exact number of elements turns out to be 120. To transition from $\mathrm{SL}(2,5)$ to $\mathrm{PSL}(2,5)$ we must look at the center of $\mathrm{SL}(2,5)$. These are the diagonal matrices in $\mathrm{SL}(2,5)$ with constant entries along the diagonal. This implies $a = d$ and $b = c = 0$. Since the determinant is 1, we have $a^2 = 1$, so $a = 1$ or $a = 4$. More intuitively we could say $a = 1$ or $a = -1$ since 4 and -1 are the same mod 5. We consider a matrix and its negative to be the same matrix. Since $\mathrm{SL}(2,5)$ had 120 elements and we've identified elements in pairs, $\mathrm{PSL}(2,5)$ has 60 elements.

Now, let us look at PSL$(3,5)$. This is the set of 3 by 3 matrices with elements from the integers mod 5 and determinant 1. The center of SL$(3,5)$ is the set of multiples of the identity matrix with determinant 1. If the diagonal elements are a, then the determinant condition says $a^3 = 1$. If we cube the numbers $0, 1, 2, 3, 4$ and take the remainders by 5, we see that 1 is the only cube root of 1 mod 5. This means that the center is just the identity matrix, and modding out by the group identity does nothing. Now we have that PSL$(3,5) =$ SL$(3,5)$.

3.3 Order of $PSL_n(\mathbb{F}_q)$

For a finite field $\mathbb{F}_q$ with q elements, the order of $PSL_n(\mathbb{F}_q)$ is given by:

$$|PSL_n(\mathbb{F}_q)| = \frac{|SL_n(\mathbb{F}_q)|}{|Z(SL_n(\mathbb{F}_q))|}.$$

3.4 Simplicity of $PSL_n(\mathbb{F}_q)$

To find and prove the simplicity conditions of $PSL_n(\mathbb{F}_q)$, we will use Iwasawa's Lemma.

3.4.1 Iwasawa's Lemma

This lemma assumes that G is a primitive permutation group on Ω. Suppose that some point stabilizer G_α contains an abelian normal subgroup A (that is, $A \lhd G_\alpha$) whose conjugates in G generate all of G. Then any nontrivial normal subgroup N of G contains G', the commutator subgroup of G. In particular, if G is perfect, then G is simple.

Proof: Suppose N is a normal subgroup of G different from $\{1\}$. Our first claim is that there exists an $\alpha \in \Omega$ for which $N \not\subset G_\alpha$. Assume to the contrary that N is contained in every stabilizer. But, since G acts faithfully on Ω, no nontrivial element of N can induce the identity permutation on Ω, a contradiction. So, let $\alpha \in \Omega$ be such that $N \not\subset G_\alpha$. Since the action of G on Ω is primitive, the stabilizers G_β are maximal subgroups of G. It follows that the subgroup NG_α must be all of G. Let $A \lhd G_\alpha$ be as in the statement of Iwasawa's Lemma. Let $g \in G = NG_\alpha$, and write $g = nh$, where $n \in N$ and $h \in G_\alpha$. Then

$$gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1} \subset NAN = NA,$$

where the last equality follows by normality of N. But, since the conjugates of A in G generate G, we see that $G = NA$. By the Second Isomorphism Theorem, we have that

$$G/N \cong NA/N \cong A/(A \cap N).$$

The rightmost factor is obviously abelian, which implies $G' \subseteq N$. This completes the proof.

3.4.2 Application of Iwasawa's Lemma to $PSL_n(\mathbb{F}_q)$

Now, we will apply the lemma to prove the simplicity of $PSL_n(\mathbb{F}_q)$ for $n \geq 2$ and $\mathbb{F}_q$ a finite field. Consider the action of $PSL_n(\mathbb{F}_q)$ on the projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$. This action is primitive because the stabilizers of points in $\mathbb{P}^{n-1}(\mathbb{F}_q)$ are maximal subgroups. The point stabilizer in $PSL_n(\mathbb{F}_q)$ is isomorphic to $PGL_{n-1}(\mathbb{F}_q)$, which contains an abelian normal subgroup A (the center of $PGL_{n-1}(\mathbb{F}_q)$). The conjugates of A in $PSL_n(\mathbb{F}_q)$ generate the entire group $PSL_n(\mathbb{F}_q)$. By Iwasawa's Lemma, any nontrivial normal subgroup N of $PSL_n(\mathbb{F}_q)$ contains the commutator subgroup $PSL_n(\mathbb{F}_q)'$. Since $PSL_n(\mathbb{F}_q)$ is perfect, $PSL_n(\mathbb{F}_q) = PSL_n(\mathbb{F}_q)'$, and thus $N = PSL_n(\mathbb{F}_q)$. Therefore, $PSL_n(\mathbb{F}_q)$ is simple.

4 Orthogonal Groups

The **orthogonal group**, $O(n)$, is the subset of orthogonal matrices, those invertible real matrices whose inverse is equal to its transpose. In other words,

$$O(n) = \left\{Q \in \mathrm{GL}_n(\mathbb{R}) \mid Q^\top = Q^{-1}\right\}$$

First, we will prove that $O(n) \leq \mathrm{GL}_n(\mathbb{R})$. Let $\phi \in O(n)$. By definition,

$$O(n) = \{\phi \in \mathrm{GL}_n(\mathbb{R}) \mid \forall x, y \in \mathbb{R}^n : \langle \phi x, \phi y\rangle = \langle x, y\rangle\}$$

Then, in particular, $\phi \in \mathrm{GL}_n(\mathbb{R})$ and ϕ^{-1} exists. For all $x, y \in \mathbb{R}^n$, we have

$$\left\langle \phi^{-1}x, \phi^{-1}y\right\rangle = \left\langle \phi\phi^{-1}x, \phi\phi^{-1}y\right\rangle = \langle x, y\rangle$$

This implies $\phi^{-1} \in O(n)$. Additionally, if $\psi \in O(n)$, then for all $x, y \in \mathbb{R}^n$,

$$\langle \psi\phi x, \psi\phi y\rangle = \langle \phi x, \phi y\rangle = \langle x, y\rangle$$

Thus, we conclude $\psi \cdot \phi \in O(n)$. Trivially, the identity transformation is in $O(n)$. Therefore, $O(n)$ is a non-empty subset of the group $\mathrm{GL}_n(\mathbb{R})$ and is closed under composition and taking inverses. Hence, we conclude that $O(n)$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Also, a square matrix U is orthogonal if and only if its column vectors form an orthonormal set. Let U be an $n \times n$ orthogonal matrix and let $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n$ be the column vectors of U. Then

$$U^\top U = (u_{ij})^\top (u_{ij}) = \left(\boldsymbol{u}_i^\top \boldsymbol{u}_j\right) = (\boldsymbol{u}_i \cdot \boldsymbol{u}_j)$$

Therefore, $U^\top U = I_n$ if and only if $\boldsymbol{u}_i \cdot \boldsymbol{u}_j = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$ if and only if the columns of U are an orthonormal set.

Since $U^\top = U^{-1}$ and $UU^\top = UU^{-1} = I$, it also follows that the row vectors of an orthogonal matrix U must also form an orthonormal set. The orthogonal group $O(n)$ consists of all rotation and reflection matrices of $\mathbb{R}^n$, when interpreted geometrically.

This time, we will discuss another way to define orthogonal groups rather than describing their orders and simplicity conditions.

4.0.1 Another Definition for Orthogonal Groups

We will again start with a few preliminary definitions.

If V is a vector space over a field K, a function $f : V \times V \to K$ is called a **bilinear form** if, for each $v \in V$, the functions $f(v, u)$ and $f(u, v)$ are linear functionals on V.

A bilinear form f is called **symmetric** if $f(v, u) = f(u, v)$ for all $u, v \in V$, and it is called alternating if $f(v, v) = 0$ for all v
$\in V$.

An inner product space (V, f) is **nondegenerate** (or nonsingular) if one (and hence any) of the inner product matrices of f is nonsingular.

If $f : V \times V \to K$ is either symmetric, alternating, or hermitian (which will not be defined in this paper), then we call the ordered pair (V, f) an **inner product space**.

Let (V, f) be an inner product space. If $\{v_1, \ldots, v_n\}$ is an ordered basis of V, then the inner product matrix of f relative to this basis is

$$A = [f(v_i, v_j)]$$

It is clear that f is completely determined by an inner product matrix, for if $u = \sum \alpha_i v_i$ and $w = \sum \beta_i v_i$, then

$$(u, w) = \sum_{i,j} \alpha_i \beta_j f(v_i, v_j)$$

Now we can define orthogonal groups again. The **orthogonal group** $O_n(\mathbb{F})$ is the group of $n \times n$ matrices A over $\mathbb{F}$ that preserve a non-degenerate symmetric bilinear form, i.e., $A^T A = I_n$. Formally,

$$O_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid A^T A = I_n\}.$$

5 References

1. D. Gorenstein, *Finite Simple Groups: An Introduction to Their Classification*, Plenum Press, 1982.

2. M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 2000.

3. W. Feit, *The Representation Theory of Finite Groups*, North-Holland, 1982.