# Finite Groups of Lie Type

Vishwasri Srinivasan

July 2024

# Introduction

- Initially explored by Évariste Galois in the 19th century and formalized by Sophus Lie.
- Finite groups of Lie type:
  - Arise from Lie algebras and algebraic groups over finite fields.
  - Are used in various areas of mathematics (representation theory, combinatorics, number theory).
- Aim of this talk:
  - Provide an exposition on finite groups of Lie type.
  - Focus on their construction, properties, order, and simplicity conditions.

# Definitions

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

- **Closure:** For all $a, b \in G$, the result of the operation $a \cdot b$ is also in $G$.
- **Associativity:** For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **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.
- **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.

# Order and Subgroups

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**.

A **subgroup** $H$ of a group $G$ is a subset of $G$ that forms a group under the operation 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 $gng^{-1} \in N$.

**Example:** 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 $n + h + (-n) \in H$.

# Homomorphisms and Isomorphisms

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 following condition:

- **Preservation of Operation:** For all $a, b \in G$, $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, where $\cdot$ denotes the group operation in $G$ and $H$.

An **isomorphism** $\phi : G \to H$ is a bijective homomorphism that preserves the operations of the structures.

# Kernels, Images, Simple Groups

Let $\phi : G \to H$ be a homomorphism between groups $G$ and $H$.

The **kernel** of $\phi$, 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 group $G$ is called **simple** if it has no nontrivial proper normal subgroups, i.e., the only normal subgroups of $G$ are the trivial group $\{e\}$ and $G$ itself.

# Classification Theorem for Finite Simple Groups

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. Some examples include the general linear group, special linear groups, and orthogonal groups.

# 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 matrix multiplication. Formally,

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

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

**Example:** Consider $GL_2(\mathbb{R})$, the group of invertible $2 \times 2$ matrices with real entries. For instance,

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in GL_2(\mathbb{R}),$$

since $\det(A) = 1 \cdot 4 - 2 \cdot 3 = -2 \neq 0$.

# General Linear Group over Finite Fields

When $\mathbb{F} = \mathbb{F}_q$ (the finite field with $q$ elements), $GL_n(\mathbb{F}_q)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_q$. The order of $GL_n(\mathbb{F}_q)$ is given by:

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

# Deriving the Order of $GL_n(F_q)$

- We need to determine the number of non-singular $n \times n$ matrices over the finite field $F_q$.
- The first row $u_1$ can be any non-zero vector, giving $q^n - 1$ possibilities.
- For any choice of $u_1$, the second row $u_2$ can be any vector not a multiple of $u_1$, giving $q^n - q$ possibilities.
- For any choice of $u_1$ and $u_2$, the third row $u_3$ can be any vector not a linear combination of $u_1$ and $u_2$, giving $q^n - q^2$ possibilities.
- Continuing in this manner, the $k$-th row can be any vector not a linear combination of the previous $k-1$ rows, giving $q^n - q^{k-1}$ possibilities.
- Therefore, the number of non-singular matrices is:

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

# Special Linear Group

The **special linear group** $SL_n(\mathbb{F})$ is the subgroup of $GL_n(\mathbb{F})$ consisting of matrices with determinant 1. Formally,

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

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

# Special Linear Group over Finite Fields

When $\mathbb{F} = \mathbb{F}_q$, $SL_n(\mathbb{F}_q)$ is the group of all $n \times n$ matrices over $\mathbb{F}_q$ with determinant 1. The order of $SL_n(\mathbb{F}_q)$ is given by:

$$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{q-1} = \frac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})}{q-1}.$$

# Deriving the Order of $SL_n(F_q)$

- Consider the set of all $n \times n$ matrices over the finite field $F_q$ with $q$ elements.
- The special linear group $SL_n(F_q)$ consists of all matrices with determinant 1.
- We know the order of the general linear group $GL_n(F_q)$:

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

- To find the order of $SL_n(F_q)$, note that multiplying the first row of a matrix with determinant 1 by any non-zero field element $a$ results in a matrix with determinant $a$.
- Each non-zero determinant can be achieved this way, creating a bijection between matrices with different determinants.
- Hence, the total number of matrices is divided among the $q - 1$ possible non-zero determinants.
- Therefore:

$$|SL_n(F_q)| = \frac{1}{q-1} |GL_n(F_q)|$$

# Projective Special Linear Group

The **projective special linear group** $PSL_n(\mathbb{F})$ is defined as the quotient group of the special linear group $SL_n(\mathbb{F})$ by its center $Z(SL_n(\mathbb{F}))$. The center $Z(SL_n(\mathbb{F}))$ consists of scalar matrices $\lambda I_n$ where $\lambda^n = 1$. Formally,

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

**Order:** The order of $PSL_n(\mathbb{F}_q)$ is:

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

$PSL_n(\mathbb{F}_q)$ is simple for $n \geq 2$ and $q$ sufficiently large.

# Definitions for Proof - 1

A **group action** of a group $G$ on a set $\Omega$ is a mapping $\cdot : G \times \Omega \to \Omega$ such that:

$$\begin{cases} g_1 \cdot (g_2 \cdot \omega) = (g_1 g_2) \cdot \omega, & \text{for all } g_1, g_2 \in G \text{ and } \omega \in \Omega, \\ e \cdot \omega = \omega, & \text{for all } \omega \in \Omega, \end{cases}$$

where $e$ is the identity element of $G$.

**Example:** Consider the group $G = \mathbb{Z}/4\mathbb{Z}$ (integers modulo 4) acting on the set $\Omega = \{1, 2, 3, 4\}$ by rotation. Each element $g \in G$ represents a rotation of $\Omega$ by $g$ positions. For instance, $1 \cdot 2 = 3$ and $3 \cdot 4 = 3$.

# Definitions For Proof - 2

**Primitive Group Action:** A group action of $G$ on $\Omega$ is called **primitive** if the only $G$-invariant partitions of $\Omega$ are trivial (singletons or the whole set $\Omega$).

**Stabilizers:** The **stabilizer** of a point $\omega \in \Omega$ under the action of $G$, denoted $G_\omega$ or $G(\omega)$, is the subgroup of $G$ that fixes $\omega$, i.e.,

$$G_\omega = \{g \in G \mid g \cdot \omega = \omega\}.$$

# Iwasawa's Lemma

**Iwasawa's Lemma:** Let $G$ be a primitive permutation group on $\Omega$. Suppose that some point stabilizer $G_\alpha$ contains an abelian normal subgroup $A$ (i.e., $A \lhd G_\alpha$) whose conjugates in $G$ generate all of $G$. Then any nontrivial normal subgroup $N$ of $G$ contains $G'$, the commutator subgroup of $G$. If $G$ is perfect, then $G$ is simple.

It states that any non-trivial normal subgroup of a group containing an abelian normal subgroup must also contain the commutator subgroup.

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

1. Consider $PSL_n(\mathbb{F}_q)$ acting on $\mathbb{P}^{n-1}(\mathbb{F}_q)$, where the action is primitive.
2. The stabilizer of a point in $\mathbb{P}^{n-1}(\mathbb{F}_q)$ is isomorphic to $PGL_{n-1}(\mathbb{F}_q)$.
3. $PGL_{n-1}(\mathbb{F}_q)$ contains an abelian normal subgroup (its center), whose conjugates generate $PSL_n(\mathbb{F}_q)$.
4. Apply Iwasawa's Lemma to show any non-trivial normal subgroup of $PSL_n(\mathbb{F}_q)$ contains the commutator subgroup $PSL_n(\mathbb{F}_q)'$, which equals $PSL_n(\mathbb{F}_q)$ as $PSL_n(\mathbb{F}_q)$ is perfect.
5. Conclude that $PSL_n(\mathbb{F}_q)$ is simple for $n \geq 2$ and $q > 3$ .

# Orthogonal Groups

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,

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

**Example:**
Consider $O_2(\mathbb{R})$, the group of all $2 \times 2$ orthogonal matrices with real entries. For instance,

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in O_2(\mathbb{R}),$$

since $A^T A = I_2$.

# Thank You

Thank you for your attention!