Simple Finite Groups of Lie Type

Rayhaan Patel

Euler Circle

July 11, 2025

Introduction

Definition 1

A *group* G is a set paired with a binary operation on its elements, $\cdot$ that satisfies the following axioms:

1. Closure: for all $a, b \in G$, $a \cdot b \in G$.
2. Associativity: for all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. Existence of Identity: There exists some $1 \in G$ such that for all $a \in G$, $1 \cdot a = a \cdot 1 = a$.
4. Existence of Inverses: For all $a \in G$, there exists some $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 2

If G has a subset, S, which is also a group under the same operation as G, we call S a *subgroup*, $S \leq G$.

Definition 3

We call a subgroup N of a group G *normal* if for all $g \in G$ and all $n \in N$, $gng^{-1} \in N$.

Definition 4

We call a group G *simple* if the whole group G and the trivial subgroup $\{1\}$ are the only normal subgroups of G.

The *Hölder Program* is a program to classify all finite groups, which involves classifying all simple finite groups (completed in the Enormous Theorem), then finding all ways of "putting simple groups together."

Theorem 5 (The Enormous Theorem)

Every simple finite group G can be classified as

1. *A cyclic group of prime order.*
2. *An alternating group of order greater than 5.*
3. *A group of Lie type. These are further broken down into 16 infinite families.*
4. *One of 26 Sporadic groups.*

Whenever we have a subset S of a group G, where all elements of G are a product of elements of S and their inverses, this is called a set of *generators* of G.

Theorem 6

All simple finite groups are generated by 2 of their elements.

Definition 7

A *field* is a set $\mathbb{F}$ with two binary operations, addition and multiplication defined on all elements satisfying the following axioms:

1. $\mathbb{F}$ is an abelian group under addition with identity 0.
2. $\mathbb{F}\backslash\{0\}$ also written as $\mathbb{F}^\times$ is an abelian group under multiplication with identity 1.
3. Multiplication distributes over addition: for all $a, b, c \in \mathbb{F}$, $a(b + c) = ab + ac$. This also implies that $0a = 0$ for all $a \in \mathbb{F}$.

We say $\mathbb{F}_q$ is the unique field with q elements.

Linear Groups

Lie groups are groups that are also manifolds, and the group operation and taking inverses correspond to smooth maps of the manifold.

Example

$GL_n(\mathbb{R})$ is a submanifold of $\mathbb{R}^{n^2}$, and also a group.

The classical groups are finite groups of lie type related to subgroups of $GL_n(q)$ when $\mathbb{F}$ is a finite field.

Theorem 8

$|GL_n(q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$.

Proof.

For a matrix to be in $GL_n(q)$ it must have nonzero determinant, so its columns must be linearly independent. There are q^n possible values for the first column, and we subtract 1 to avoid the case where all entries are 0. The second column cannot be one of the q multiples of the first so there are $q^n - q$ possibilities and so on. ∎

Definition 9

Given a group G, its center, $Z(G)$ is the subgroup such that for all $a \in Z(G)$ and $b \in G$, $a \cdot b = b \cdot a$.

The center of $GL_n(q)$ is the set of *scalar matrices* λI_n such that $\lambda \in \mathbb{F}_q$ We can quotient $GL_n(q)$ by its center to get $PGL_n(q)$. Since there are $q-1$ possibilities for λ, $|Z(GL_n(q)) = q-1|$ and $|PGL_n(q)| = \frac{1}{q-1}|GL_n(q)|$.

Definition 10

We define the *special linear group*, $SL_n(q) \leq GL_n(q)$ to be the subgroup of matrices with determinant 1.

Its center also consists of scalar matrices, and since $\det(\lambda I_n) = \lambda^n$, $\lambda^n = 1$. We can take the quotient of $SL_n(q)$ by its center to get $PSL_n(q)$, which is one of the 16 infinite families of Lie groups in the classification theorem.

Simplicity of $PSL_n(q)$

Definition 11

A *transvection* in a vector space, V is a linear transformation that fixes a hyperplane H and has determinant 1.

Transvections are shear transformations of vector spaces. Given a transvection, T, then we can choose a basis such that T has a matrix of the following from:

$$\begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots & 0 \\ \vdots & \vdots & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Lemma 12

$SL_n(q)$ is generated by transvections.

Lemma 13

If N is a normal subgroup of $SL_n(q)$, and $A \in N$ but $A \notin Z(SL_n(q))$, then there exists some transvection $T \in N$.

Theorem 14

The groups $PSL_n(q)$ when $n \geq 3$ are simple.

Proof.

We show that $PSL_n(q)$ is simple by showing that if a normal subgroup N of $SL_n(q)$ contains some $A \notin Z(SL_n(q))$ then $N = SL_n(q)$ If N contains a transvection T, then for all transvections $t \in SL_n(q)$ there exists $g \in SL_n(q)$ such that $gTg^{-1} = t$ since all transvections are similar. Thus, $t \in N$, and since $SL_n(q)$ is generated by transvections, and N contains all transvections, $SL_n(q) = N$. Therefore $PSL_n(q)$ is simple. ■