Finite Groups of Lie Type

Ayush Jain

ayushj2007@gmail.com

Euler Circle

July 2023

A Brief Introduction

Definition

A simple group is a group with only two normal subgroups, the trivial subgroup containing the identity, and the subgroup consisting of the entire group itself

Pertaining to these simple groups, there is a theorem known as the classification theorem, which says that every **finite** simple group can be classified as one of the following

1. a cyclic groups of prime order
2. an alternating group of order ≥ 5
3. a group of lie type
4. one of the 27 sporadic groups

Groups of Lie Type

Definition

A group of Lie type refers to the group of rational points on a reductive linear algebraic group with values in a finite field.

One of the first ways these groups were investigated was looking over the classical groups. These can be defined as a special linear, orthogonal, unitary, or symplectic groups. There are many variations of these which can be found by taking quotients making the projective linear groups

Finite Fields

A field F can be defined with the following axioms. There exists two binary operations (addition and multiplication) with the following properties

1. Associativity of addition and multiplication
2. Commutativity of addition and multiplication
3. Existence of Multiplicative and Additive identity, denoted by 1 and 0 respectively
4. Existence of an additive inverse $\forall a \in F$ denoted by $-a$
5. Existence of a multiplicative inverse $\forall b \in F$, $b \neq 0$ denoted by b^{-1}
6. Satisfies Distributive Law

Finite Fields

When we look at finite fields, they have many different properties. Let us take a finite field F. Say q is the order of the multiplicative group of the field.

Proposition

A field has no zero divisors

Proposition

The number of elements in F is always in the form p^d where $p \in \mathbb{Z}$ is a prime, and $d \in \mathbb{N}$

Finite Fields

Proposition

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

Proposition

For any natural m, the number of solutions to the equation $x^m = 1$ is given by $(m, q-1)$

The General Linear Groups

Definition

The General Linear Group is the set of all $n \times n$ invertible matrices. We can take the entries over the finite field $\mathbb{F}_q$ with order q, denoted by $GL_n(q)$

There are many interesting subgroups of the general linear group. The center of the group is the set of scalar matrices λI_n, where $\lambda \in \mathbb{F}_q$. Call this set Z. Noticeably, Z is a cyclic subgroup of order $q - 1$. Moreover, if we quotient this group with G, the group G/Z is the projective general linear group denoted by $PGL_n(q)$.

The General Linear Group

Also since $\det(AB) = \det(A) \cdot \det(B)$, this determinant map is a group homomorphism from $GL_n(q)$ onto the multiplicative group of the field, and its kernel is a normal subgroup of index $q - 1$.

This kernel is called the special linear group $SL_n(q)$, and consists of all the matrices of determinant 1. Similarly, we can quotient $SL_n(q)$ by the subgroup of scalars it contains, to obtain the projective special linear group $PSL_n(q)$, sometimes abbreviated to $L_n(q)$.

Equations of the Orders of the Groups

A fun property is that you can represent the orders of these groups using polynomials. For example, we have

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

We know that there are q total elements in the field $\mathbb{F}_q$, which means 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, but in interest to keep all the rows distinct there's $q^n - q$ options, we have $q^n - q^2$ options to fill out the third row, and so on.

Equations of the Orders of the Groups

For any matrix with determinant m, since we take entries in a field, we know that $m^{-1} \in \mathbb{F}_q$. If we multiply the first row with the scalar m^{-1} we get all matrices with determinant 1. Conversely, for any matrix with determinant 1, we multiply the first row with m and get one with determinant m. So this means there's a bijection with the matrices with determinant 1 and matrices with any other determinant in $\mathbb{F}_q$.

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

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

Equations of the Orders of the Groups

To get the order of $PSL_n(q)$ we need to find out for which scalars λI_n have a determinant of 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 $(n, q-1)$

$$|PSL_n(q)| = \frac{1}{(n, q-1)}|GL_n(q)|$$

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

Simplicity of $PSL_n(q)$

One of the interesting results from studying these linear groups is that the Projective Special Linear group is actually simple for any $n > 2$ and $q > 3$. A large part of proving this relies on Iwasawa's Lemma which classifies which groups are simple. We first look over some preliminary results

Theorem (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.

Definition

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

Simplicity of $PSL_n(q)$

Lemma

$SL_n(q)$ is generated by transvections

Proof.

By our definition of transvections, we can say that the above claim is equivalent to saying that the elements of $PSL_n(q)$ can be reduced to the identity matrix using the row operation $r_i \to r_i + \lambda r_j$. An elementary result of matrices shows that this is possible for any matrix with determinant 1. $\square$

Simplicity of $PSL_n(q)$

Definition

A group is said to be perfect if it is equal to it's own commutator subgroup

Lemma

$PSL_n(q)$ is perfect except for the cases $PSL_2(2)$ and $PSL_2(3)$.

Proof. We can show that every transvection is in fact a commutator of the $PSL_n(q)$. Accordingly, we have

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

Simplicity of $PSL_n(q)$

with a suitable choice of a basis, we can show that every transvection is a commutator in $PSL_n(q)$. If $n = 2$ and $q > 3$, then $\mathbb{F}_q$ contains a non zero element x with $x^2 \neq 1$, then the commutator

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

Which will be an arbitrary element of our abelian group A.

Application of Iwasawa's Lemma

In order to apply this, we take $n \geq 2$ we let $PSL_n(q)$ 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 we obtain an action of $PSL_n(q)$ on Ω. This action is primitive.

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 $\lambda \neq 0$.

Application of Iwasawa's Lemma

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 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.

Using our preliminary results, we can use Iwasawa's Lemma and show that for $n > 2$ and $q > 3$, the group $PSL_n(q)$ is simple