Classification of Finite Simple Groups

Let G be a finite group. We say that G is *simple* if it has no normal subgroups other that G or 1_G. A major accomplishment of the 20th century was the classification of finite simple groups. The classification can be broadly viewed as:

(1) Cyclic groups of prime order

(2) Alternating groups A_n, for $n \geq 5$.

(3) Finite Simple Groups of Lie Type

(4) The 26 Sporadic Simple Groups

Our interest will be in finite simple groups of Lie type. First, we'll say a few words about the sporadic simple groups. (pg. 254 - Aschbacher)

- **Monster Group:**
  (a) Uniqueness was proven by the existence of a 196,883 dimensional faithful representation.
    - (Norton - 1985) Never published
    - (Griess, Meierfrankenfeld, & Seger - 1989)

  (b) Conway & Norton conjectured: There is a graded G-module

$$V = \bigoplus_{m \geq -1} V_m$$

  with $\dim V_m = c(m)$, where

$$j(q) = \sum_{m \geq -1} c(m) q^m$$

  is the unique normalized main modular function.
    - (Borchereds - 1992)

- **Mathieu Groups**
  - Realized as multiply transitive permuation groups.
  - First sporadic groups discovered
  - M_{12} introduced in 1861
  - Witt in 1938 constructed these as automorphism groups of Steiner systems.

$\mathrm{PSL}_2(\mathbb{F}_q), q \geq 4$ is Simple. We now look at finite groups of Lie type, which will be our interest for the rest of the talk. We will focus on two examples:

(1) $\mathrm{PSL}_2(\mathbb{F}_q)$, where $q = p^e$ for some prime p. These groups are simple except $\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3$ and $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$.

(2) Suzuki groups ${}^2B_2(q^2)$.

Remark 1. Each group of Lie type corresponds to a Dynkin diagram and the action from which they are obtained.

We define the projective linear groups as follows:

$$\mathrm{PGL}_n(\mathbb{F}) = \mathrm{GL}_n(\mathbb{F})/Z(\mathrm{GL}_n(\mathbb{F}))$$

and

$$\mathrm{PSL}_n(\mathbb{F}) = \mathrm{SL}_n(\mathbb{F})/Z(\mathrm{SL}_n(\mathbb{F}))$$

where $Z(\mathrm{GL}_n(\mathbb{F}) = Z(\mathrm{SL}_n(\mathbb{F}) = \langle \lambda\, \mathrm{I}_n \rangle$ for $\lambda \in \mathbb{F}^*$.

Remark 2.

(1) These groups all have a well-defined action on projective space.

(2) The group $\mathrm{PGL}_n(\mathbb{F})$ is of Lie type and corresponds to the Dynkin diagram A_{n-1}.

Our goal is to prove that:

Theorem 1. *If $\mathbb{F}$ is a finite field with order 4 or larger, then $\mathrm{PSL}_2(\mathbb{F})$ is simple.*

To do this, we will first work through some results for $\mathrm{SL}_2(\mathbb{F})$.

Definition 1. Let $\mathbb{F}$ be any field and $G = \mathrm{GL}_2(\mathbb{F})$ or $G = \mathrm{SL}_2(\mathbb{F})$. Then the *standard Borel subgroup B* of G is the group of upper triangular matrices in G. For $G = \mathrm{SL}_2(\mathbb{F})$,

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}^* \text{ and } b \in \mathbb{F} \right\}.$$

Proposition 1 (Bruhat Decomposition)**.** *Let* $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *and* $G = \mathrm{SL}_2(\mathbb{F})$*. Then there is a decomposition of* G *into disjoint subsets*

$$G = B \sqcup BwB.$$

Moreover, B *is a maximal subgroup of* G*.*

Proof. Let $g \in G$ and write $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $c = 0$, then $g \in B$. If $c \neq 0$, then

$$\begin{aligned} \begin{pmatrix} b - adc^{-1} & a \\ 0 & -c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & dc^{-1} \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a & b - adc^{-1} \\ c & 0 \end{pmatrix} \begin{pmatrix} 1 & dc^{-1} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= g \in BwB. \end{aligned}$$

<u>Disjoint:</u> We make the observation that

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} * & * \\ -d_1 a_2 & * \end{pmatrix} \notin B$$

because $a_1 d_1 = 1$, $a_2 d_2 = 1$, and $-d_1 a_2 \neq 0$.

We are left to show that $\langle B, g \rangle = G$ for $g \in G \setminus B$. That is, the standard Borel subgroup is maximal in G. Let $g \neq B$ so $g \in BwB$. Then there exist $b_1, b_2 \in B$ such that we can write $g = b_1 w b_2$. Well

(1) $w \in \langle B, g \rangle$

(2) $BwB \subseteq \langle B, g \rangle$

and therefore $G = B \sqcup BwB \subseteq \langle B, g \rangle$. We conclude that $G = \langle B, g \rangle$. □

We now define

$$U := \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F} \right\}$$

and

$$\overline{U} := \left\{ \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \mid \beta \in \mathbb{F} \right\}$$

Facts:

(1) $U \leq B$ and in fact $U \lhd B$

(2) U is abelian and isomorphic to $\langle \mathbb{F}, + \rangle$.

(3) One can show that $\overline{U} = wUw^{-1}$.

Proposition 2.

(1) *For any finite field* $\mathbb{F}$, $\mathrm{SL}_2(\mathbb{F}) = \langle U, \overline{U} \rangle$.

(2) *Let* $\mathbb{F}$ *be a field,* $\#\mathbb{F} \geq 4$*, then* $\mathrm{SL}_2(\mathbb{F})$ *is perfect. That is,* $[\mathrm{SL}_2(\mathbb{F}), \mathrm{SL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F})$.

Lemma 1. *Let* $G = \mathrm{SL}_2(\mathbb{F})$. *Then*

$$\bigcap_{g \in G} gBg^{-1} = Z(G).$$

We now prove the theorem:

Proof. Let $G = \mathrm{SL}_2(\mathbb{F}_q), q \geq 4$. Take $N \lhd G$ and invoke the 4th isomorphism theorem. It is enough to show that $N \leq Z(G)$ or $N = G$.

Since the standard Borel subgroup B is maximal in G, either $NB = B$ or $NB = G$.

(1) $N \leq B \Rightarrow N < gBg^{-1}$ for all $g \in G$ and therefore

$$N \leq \bigcap_{g \in G} gBg^{-1} = Z(G).$$

Remark 3. All Borel subgroups are conjugate to the standard Borel subgroup.

(2) Suppose that $NB = G$. Then there exists $x \in N$ and $b \in B$ with $w = xb$. So,

$$\begin{aligned} \overline{U} = wUw^{-1} &= xbU(xb)^{-1} \\ &= xbUb^{-1}x^{-1} \\ &= xUx^{-1} \\ &\leq NU \end{aligned}$$

but $G = \langle U, \overline{U} \rangle = NU$. Applying the second isomorphism theorem, one sees that

$$G/N = NU/N \cong \frac{U}{U \cap N}$$

which is abelian. Hence $N \supset G' = G$ and therefore $N = G$.

$\square$