Brad Bentz
MATH 251

Let $G = \mathrm{SL}_2(F)$ where F is a field of at least 4 elements. Define the following subgroups:

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in G \right\} \qquad B^T = \left\{ \begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix} \in G \right\} \qquad U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G \right\} \qquad U^T = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \in G \right\}$$

and define the matrix $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. We will begin by relating the structure of G to these subgroups.

Theorem 1 *G is generated by U and U^T.*

Proof: First, by direct calculation, we see that for any $a \neq 0$

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

and also that

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

so therefore any nonzero diagonal matrix is in $\langle U, U^T \rangle$.

Now, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an arbitrary element of G with $a \neq 0$. Note that because the determinant is 1 we have $d = (bc+1)/a$. Then,

$$\begin{pmatrix} 1 & a^{-1}c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ab & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & \frac{bc+1}{a} \end{pmatrix}.$$

Therefore, this matrix is in $\langle U, U^T \rangle$. Now, suppose $a = 0$ and the matrix is of the form $\begin{pmatrix} 0 & -b \\ b^{-1} & d \end{pmatrix}$. Then,

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

Therefore, matrices of this form are also in $\langle U, U^T \rangle$. But all matrices in G have one of these two forms because either $a = 0$ or $a \neq 0$. Therefore, $G = \langle U, U^T \rangle$.

$\square$

Next, we will decompose G into a disjoint union of subsets.

Theorem 2 *G is equal to the disjoint union $B \sqcup BwB$.*

Proof: Let $a, c \neq 0$. A general element of BwB has the form

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} -bc & ac^{-1} - bd \\ -ca^{-1} & -da^{-1} \end{pmatrix}$$

and so necessarily the value in the bottom left of the matrix is nonzero. This component is zero for matrices in B and so the sets are necessarily disjoint.

Let $r, p \neq 0$. Consider an arbitrary matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Then,

$$\begin{pmatrix} pr^{-1} & 1 \\ 0 & rp^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -p & -psr^{-1} \\ 0 & -p^{-1} \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

This shows that any element of G with first column nonzero is in BwB. Now, suppose $p = 0$ (and therefore we have $q = -r^{-1}$). Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -r & -s \\ 0 & -r^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -r^{-1} \\ r & s \end{pmatrix}$$

This shows that any element of G with first column having a zero and then a nonzero element is in BwB. But this means that any element of G with the bottom left element nonzero is in BwB.

Finally, any element of G with the element in the first column, second row zero is necessarily of the form $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ which is in B. Therefore, the proof is complete.

□

Theorem 3 *B is a maximal subgroup of S. Equivalently, any subgroup containing B is either B or G.*

Proof: Using theorem 2, this is equivalent to the statement (for any $c \neq 0$)

$$\langle B, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rangle = G.$$

First, without loss of generality, $d \neq 0$. Otherwise, the product bc is necessarily nonzero (for the matrix to have determinant 1) so we can replace $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$ with $\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & 0 \end{pmatrix}\right)^2 = \begin{pmatrix} (a+c)^2 + bc & b(a+c) \\ c(a+c) & bc \end{pmatrix}$. For simplicity, let $H = \langle B, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rangle$.

I will first show that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$ then $\begin{pmatrix} 1 & 0 \\ d^{-1}c & 1 \end{pmatrix} \in H$. This follows because

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} 1 & -bd^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ d^{-1}c & 1 \end{pmatrix}.$$

Now, let p solve the equation $(d^{-1}cp + 1)^{-1} d^{-1} c = x$ (for arbitrary x.) We have $p = (cx^{-1}d^{-1} - 1)dc^{-1}$. Then,

$$\begin{pmatrix} 1 & 0 \\ d^{-1}c & 1 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p \\ \frac{c}{d} & cpd^{-1} + 1 \end{pmatrix} \implies \begin{pmatrix} 1 & 0 \\ (d^{-1}cp + 1)^{-1} d^{-1} c & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in H.$$

But, because all matrices of the form $U \subset B$ and U^T are in H we must have $H = G$ by theorem 1. □

Here we will use the fact that the field has four or more elements.

Lemma 1 *A field F with four or more elements contains a nonzero element that does not square to one.*

Proof: In any field, the only elements that can square to 1 are ± 1. If F has four or more elements, only three of them can be 0 or ± 1. This means that at least one element is nonzero and does not square to one. □

Now, let $'$ denote commutator subgroup.

Theorem 4

$$G = G'.$$

Proof: Choose an a such that $a \neq 0$ and $a^2 \neq 1$. Such an a exists by the lemma. Then,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b(a^2 - 1) \\ 0 & 1 \end{pmatrix} \in U.$$

Because $a^2 \neq 1$ and b is a free parameter, all elements of U can be expressed in this form. But also notice that these elements are in B' so $U \subset B'$ and necessarily $U \subset G'$. Because conjugator subgroups are normal, $wUw^{-1} \subset G'$ but, the general form of a matrix in wUw^{-1} is

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

Therefore, we can see that $wUw^{-1} = U^T$ so this implies $U, U^T \subset G'$ or $G' = G$. □

Theorem 5

$$\bigcap_{g \in G} gBg^{-1} = Z(G) = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof: A matrix of the form wBw^{-1} has the form

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

This means that $wBw^{-1} = B^T$ and that $B \cap (wBw^{-1})$ is all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Now, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ be an element where all entries are nonzero. Then we have

$$gBg^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -ayc - \frac{bc}{x} + adx & ya^2 - bxa + \frac{ba}{x} \\ -yc^2 + dxc - \frac{dc}{x} & \frac{ad}{x} - bcx + acy \end{pmatrix}.$$

In order for the top right element to be zero, we require that $y = bx/a - b/(xa)$. After substituting this in, the matrix is equal to $\begin{pmatrix} x & 0 \\ \frac{c(x^2-1)}{ax} & \frac{1}{x} \end{pmatrix}$ so in order for the element on the bottom left to be zero we require that $x^2 = 1$. Here, we can either choose $x = \pm 1$ and these choices correspond to the matrices $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This proves that to be in the center the matrix must have the form $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. □

Theorem 6 *If $H \lhd G$ then $H \subset Z(G)$ or $H = G$.*

Proof: First, note that $B \subset HB$ so either $HB = B$ or $HB = G$ by theorem 3. In the first case, $H \subset B$ and, by normality, $H \subset \bigcap_{g \in G} gBg^{-1}$ or $H \subset Z(G)$ by theorem 5.

If $HB = G$ write $w = hb$ where $h \in H$ and $b \in B$. Then note that

$$wUw^{-1} = U^T = hbUb^{-1}h^{-1} = hUh^{-1} \subset HU.$$

This means that $U, U^T \subset HU$ so $HU = G$ by theorem 1. Finally,

$$G/H = HU/H \cong U/(U \cap H)$$

and U is abelian so G/H is abelian which implies $G' \subset H$. By theorem 4, $G = G'$ so $G \subset H$. But also $H \subset G$ so we have $G = H$.

□

Finally, we have all of the theorems we need to make the desired conclusion.

Theorem 7 $\mathrm{PSL}_2(\mathrm{F}) = G/Z(G)$ *is a simple group.*

Proof: Let $K \lhd G/Z(G)$. Then we can pull K back to a normal subgroup of G. By theorem 6, this normal subgroup is either a subgroup of the center or equal to G. Therefore, we can conclude that $K = \{e\}$ or $K = G/Z(G)$ so $G/Z(G)$ is simple. □