Normal subgroups of SL_2

In this note matrices and vectors have coordinates in a given field F. The special linear group $SL_2(F)$ is denoted by SL_2 and the space F^2 of column vectors by V. Our object is to prove

Theorem. *Let F be a field, with $|F| > 5$. The only proper normal subgroup of SL_2 is the group $\{\pm I\}$. Hence the quotient group $PSL_2 = SL_2/\{\pm I\}$ is a simple group.*

It is not hard to analyze the cases that F has order ≤ 5 which are not covered by the theorem. The conclusion of the theorem is false when F has order 2 or 3. It is true if F has order 4 or 5, though the proof we are giving doesn't handle those cases.

If F is a finite field and has order q, the order of SL_2 is $q^3 - q$. So the order of PSL_2 is $\frac{1}{2}(q^3 - q)$ unless $-I = I$, which happens when q is a power of 2. If $-I = I$, then $PSL_2 = SL_2$, and the order of PSL_2 is $q^3 - q$. For example, $PSL_2(\mathbb{F}_4)$ and $PSL_2(\mathbb{F}_5)$ both have order 60. In fact, these two groups are isomorphic, and they are also isomorphic to the alternating group A_5.

The orders of the smallest nonabelian simple groups are

$$60,\ 168,\ 360,\ 504,\ 660,\ 1092,\ 2448.$$

A simple group with one of these orders is isomorphic to $PSL_2(F)$ for some field F. The order of F can be 4 or 5 for the simple group of order 60, and it is 7, 9, 8, 11, 13 and 17, respectively in the remaining cases. The next smallest simple group is the alternating group A_7, which has order 2520.

There is a general reason that helps to explain why a group may have few normal subgroups: If a normal subgroup N contains an element A, then it contains the entire conjugacy class $\{BAB^{-1}\}$ of A. It is also closed under products and inverses. So if the conjugacy class is large, then N will be a large subgroup. The commutator $ABA^{-1}B^{-1}$ is an example of an element that can be obtained from A by these operations, and it is important to note that while A is in the subgroup, B can be arbitrary.

To prove the theorem, we must show that if a normal subgroup N of SL_2 contains an element $A \neq \pm I$, then it is the whole group. Starting with A, we must be able to construct an arbitrary element $P \in SL_2$ by a sequence of operations, each of which is conjugation, multiplication, or inversion.

We do this in two steps: The first step (Lemmas 1 and 4) constructs a matrix $P \in N$ which has an eigenvalue λ that is in the field F, and is not ± 1. Then because N is normal, it contains the conjugacy class of P. The second step (Lemma 5) shows that this conjugacy class generates SL_2.

We'll use the notation

$$E = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\ ,\ E' = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \tag{1}$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\ ,\ \Lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}.$$

The hypothesis on the order of F appears in the first lemma.

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

Proof. Let $r \in F$. If $r^2 = 0$ then $r = 0$. If $r^2 = 1$, then $r = \pm 1$. Finally, if $r^2 = -1$, then r is a root of the polynomial $x^2 + 1$, and this polynomial has at most two roots in F. Altogether, there are at most five elements which we must avoid when choosing r. □

Lemma 2. *Let (v_1, v_2) be a basis of V, let $[\mathbf{B}]$ denote the matrix whose columns are v_1 and v_2 and let λ be a nonzero element of F. There is a unique matrix $B \in SL_2$, namely $B = [\mathbf{B}]\Lambda[\mathbf{B}]^{-1}$, such that $Bv_1 = \lambda v_1$ and $Bv_2 = \lambda^{-1}v_2$.* □

Lemma 3. *The only matrices $A \in SL_2$ for which* **all** *nonzero vectors are eigenvectors are I and $-I$.*

Proof. If e_1 and e_2 are eigenvectors of a matrix A, say $Ae_i = \lambda_i e_i$, then A is the diagonal matrix with diagonal entries λ_i. The only case in which $v = e_1 + e_2$ is also an eigenvector is that $\lambda_1 = \lambda_2$, and then $A = \lambda_1 I$. In that case $\lambda_1 = \pm 1$ because $det(A) = 1$. □

Lemma 4. *Let A be a matrix in SL_2 which is not $\pm I$, and let r be an element of F. There is a matrix $B \in SL_2$ such that the commutator $C = ABA^{-1}B^{-1}$ has eigenvalues $\lambda = r^2$ and $\lambda^{-1} = r^{-2}$.*

Proof. We choose a vector v_1 in V which is *not* an eigenvector of A, and we set $v_2 = Av_1$. Then v_1 and v_2 are independent, so they form a basis of V. Let B denote the matrix such that $Bv_1 = rv_1$ and $Bv_2 = r^{-1}v_2$. Then

$$Cv_2 = ABA^{-1}B^{-1}v_2 = ABA^{-1}rv_2 = ABrv_1 = Ar^2v_1 = r^2v_2.$$

This shows that $\lambda = r^2$ is an eigenvalue of C. Because $C \in SL_2$, the other eigenvalue is λ^{-1}. □

Lemma 5. *Let λ be an element of F which is not ± 1 or 0. The matrices having eigenvalues λ and λ^{-1} generate SL_2 and they form a single conjugacy class in SL_2.*

Proof. The matrices with eigenvalues λ and λ^{-1} are in SL_2. Let H denote the subgroup of SL_2 they generate. For any $x \in F$, the terms on the left side of the equation

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

are in H, and so the right side E is in H too. Similar reasoning shows that the matrices of the form E' are in H. Lemma 6 (which was a homework problem) shows that $H = SL_2$.

It remains to show that the matrices in question form a single conjugacy class. Suppose that B has eigenvalues λ and λ^{-1}. The assumption that $\lambda \neq \lambda^{-1}$ enters here. It implies that $\lambda \neq \pm 1$. So a pair of eigenvectors v_1 and v_2 with these eigenvalues forms a basis $\mathbf{B}$, and $B = [\mathbf{B}]\Lambda[\mathbf{B}]^{-1}$. We can adjust v_1 by a scalar factor to make $\det[\mathbf{B}] = 1$. Then $[\mathbf{B}]$ and Λ are in SL_2. This shows that B is in the conjugacy class of Λ. □

Lemma 6. *The matrices of the types (1), with x in F, generate SL_2.*

Proof. (This was a homework problem.) These matrices are in SL_2. Let H be the subgroup they generate. To prove that $H = SL_2$, we show that every matrix $A \in SL_2$ can be reduced to the identity using the row operations defined by these matrices, which are to add a multiple of one row to another. This will show that there are elementary matrices $E_1, ..., E_k$ of type (1) such that $E_k \cdots E_2E_1A = I$. Then $A = E_1^{-1} \cdots E_k^{-1}$.

The first step is to make sure that the entry c of A isn't zero. If $c = 0$, then $a \neq 0$, and we add (*row* 1) to (*row* 2). Next, having a matrix where $c \neq 0$, we can change a to 1 by adding the appropriate multiple of (*row* 2) to (*row* 1). Having done this, our third step clears out the c entry by adding a multiple of (*row* 1) to (*row* 2). The result is a matrix of the form

$$A' = \begin{pmatrix} 1 & b' \\ 0 & d' \end{pmatrix}.$$

Since A is in SL_2, so is A'. Therefore $d' = 1$, and one more row operation reduces A' to the identity. □