A FAMILY OF FINITE SIMPLE GROUPS

D. Katz

The purpose of this note is to exhibit for my algebra class an important family of finite simple groups. The family comes from matrix theory over finite fields. We begin by fixing some notation and recalling some definitions. Throughout we let F denote a field containing at least 5 elements and we always assume that the characteristic of F is either zero or greater than two. This simply means that in the field F, $2 \neq 0$. Recall that $\mathrm{SL_n}(F)$ denotes the set of $n \times n$ matrices over F with determinant one. $\mathrm{SL_n}(F)$ is a group under matrix multiplication called the *special linear group*. Let K denote the center of $\mathrm{SL_n}(F)$. Then K is a normal subgroup of $\mathrm{SL_n}(F)$. Note that, on the one hand, any matrix in the center of $\mathrm{SL_n}(F)$ must be a scalar matrix, while on the other hand, its determinant must equal one. Thus, K consists of the $n \times n$ scalar matrices over F with an nth root of unity from F down the diagonal. The factor group $\mathrm{SL_n}(F)/K$ is called the *projective linear group* and is denoted $\mathrm{PSL_n}(F)$. We are going to show that $\mathrm{PSL_2}(F)$ is a simple group. When F is a finite field, $\mathrm{PSL_2}(F)$ is a finite group, so we will then have a class of finite simple groups. The proof that $\mathrm{PSL_2}(F)$ is simple will involve a number of steps. But the basic strategy is the following. By the correspondence theorem from class, we must show that there are no normal subgroups of $\mathrm{SL_2}(F)$ properly containing K. For this we will show that if N is a normal subgroup of $\mathrm{SL_2}(F)$ properly containing K, then by conjugating the elements of N, we get all of $\mathrm{SL_2}(F)$.

Theorem. $\mathrm{PSL_2}(F)$ *is a simple group.*

Proof. As mentioned above, it suffices to prove the following statement. If N is a normal subgroup of $\mathrm{SL_2}(F)$ containing K, then $N = \mathrm{SL_2}(F)$. We note that since 1, -1 are the only square roots of unity, in this case K consists of the two matrices $I, -I$, where I is the 2×2 identity matrix. The proof of this statement requires a number of steps.

Step 1 : N contains a triangular matrix A not in K. To see this, start with $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belonging to N, but not K. If $c = 0$, then A is the required matrix.

If $c \neq 0$, then taking $\lambda := -a/c$, we get

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & * \\ c & d+a \end{pmatrix} \in N,$$

since $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix}$. Call this new matrix A and write it : $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$. Since $\det(A) = 1$, $bc = -1$. Let $0 \neq u \in F$ and set $P := \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix}$. Then $P^{-1}A^{-1}PA \in N$ and $P^{-1}A^{-1}PA = \begin{pmatrix} u^2 & (1-u^2)bd \\ 0 & u^{-2} \end{pmatrix}$. We need to select u so that this new matrix isn't in K. If it were in K, then u^2 is 1 or -1, so $u^4 = 1$. Thus u is a root of the polynomial $X^4 - 1$. Since this polyomial has at most four roots in F, we can find a non-zero $u \in F$ such that $u^4 \neq 1$ – unless $F = \mathbb{Z}_5$. Using such an element u yields the desired triangular matrix in N, but not in K.

If F is the field $\mathbb{Z}_5$ and $d \neq 0$, then $P^{-1}A^{-1}PA$ still has the required form, by choosing $u = 3$ (in $\mathbb{Z}_5$), say. Suppose $d = 0$. Then returning to the case that $A = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$, $bc = -1 \equiv 4$ in $\mathbb{Z}_5$, so the pair (b, c) is one of the pairs $(1,4), (2,2), (3,3), (4,1)$. Choose $t, w \in \mathbb{Z}_5$ such that $t^2c - w^2b = 0$ and u, v such that $ut - vw = 1$. Then

$$\begin{pmatrix} u & v \\ w & t \end{pmatrix} \cdot \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \cdot \begin{pmatrix} t & -v \\ -w & u \end{pmatrix} = \begin{pmatrix} vct - wub & -v^2c + u^2b \\ t^2c - w^2b & -vtc + uwb \end{pmatrix}$$

is triangular, belongs to N and doesn't belong to K, since the (1,1) entry of this matrix equals -1 times the (2,2) entry. This completes the proof of Step 1.

Step 2 : N contains a matrix of the form $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, with $u \neq 0$. To see this, by the previous step, N contains a matrix of the form $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ not in K. Let $b' := b + d - a$ and set $A' := \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$. Note that $A' := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot A \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, so A' belongs to N. Suppose $d \neq a$. Since $\det(A) = 1$, $ad = 1$. Therefore $(A')^{-1} = \begin{pmatrix} d & -b' \\ 0 & a \end{pmatrix}$, so $(A')^{-1} \cdot A = \begin{pmatrix} 1 & ad - d^2 \\ 0 & 1 \end{pmatrix}$ belongs to N, and has the required form. If $a = d$, then since $\det(A) = 1$, a is 1 or -1 and $b \neq 0$. Thus either $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, which is what we want or $A = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$ and $A^2 = \begin{pmatrix} 1 & -2b \\ 0 & 1 \end{pmatrix}$ is the matrix we seek, since $-2b \neq 0$. This completes the proof of Step 2.

Step 3 : The conjugacy class in $\mathrm{SL}_2(F)$ of the matrix $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ contains the matrices $\begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & a^2u \\ 0 & 1 \end{pmatrix}$, for all $0 \neq a$ in F. To see this we just note that

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & a^2u \\ 0 & 1 \end{pmatrix}.$$

Step 4 : The additive group $(F, +)$ is generated by the squares of the elements of F. To see this, we show that $x \in F$ can be written $x = a^2 - b^2 = (a+b)(a-b)$, for elements $a, b \in F$. Indeed, we take $a := (x+1)/2$ and $b := (1-x)/2$. Note, these elements exist in F, since we are assuming $2 \neq 0$, so we can divide by 2. It follows that $a + b = 1$ and $a - b = x$, so $(a+b)(a-b) = x$, as required.

Step 5 : The group $\mathrm{SL}_2(F)$ can be generated by the matrices $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$, as u varies over F. To see this, we first note that the basic elementary row operation of adding a multiple of one row to another is obtained by multiplying by a matrix of one of the two types in question. Indeed, if we want to add u times the first row of the matrix A to the second row of A, then we multiply A on the left by the matrix $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$. Now start with an arbitrary matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(F)$ and row reduce it to the identity as follows. If needed, by adding the first row to the second, we may assume $c \neq 0$. Then we add a multiple of the second row to the first, changing a to 1. Then, add $-c$ times the (new) first row to the second, changing c to 0. Now the matrix has the form $\begin{pmatrix} 1 & b' \\ 0 & d' \end{pmatrix}$. Since the determinant of this matrix is 1, $d' = 1$. Now we take $-b'$ times the second row and add it to the first row to obtain the identity matrix I. Thus we have a product $U_4 \cdot U_3 \cdot U_2 \cdot U_1 \cdot A = I$, where each U_i is a matrix of one of the two required types. Thus, $A = U_1^{-1} \cdot U_2^{-1} \cdot U_3^{-1} \cdot U_4^{-1}$. But the inverse of each U_i is also a matrix of the required type, since, for example, the inverse of $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ is just $\begin{pmatrix} 1 & -u \\ 0 & 1 \end{pmatrix}$. Thus, each matrix in $\mathrm{SL}_2(F)$ is a product of matrices of the required type. This completes the proof of Step 5.

We are now almost finished with the proof. By Step 2, N contains at least one matrix of the form $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, with $u \neq 0$. By Step 3, N contains $\begin{pmatrix} 1 & a^2u \\ 0 & 1 \end{pmatrix}$

and $\begin{pmatrix} 1 & b^2u \\ 0 & 1 \end{pmatrix}$, for all non-zero elements a and b in F. Thus N contains each $\begin{pmatrix} 1 & -b^2u \\ 0 & 1 \end{pmatrix}$, the inverse of $\begin{pmatrix} 1 & b^2u \\ 0 & 1 \end{pmatrix}$. Therefore,

$$\begin{pmatrix} 1 & a^2u \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -b^2u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a^2-b^2)u \\ 0 & 1 \end{pmatrix}$$

belongs to N for all a, b. By Step 4, if we vary a and b over F, we obtain all of the elements of F. Since $u \neq 0$, the product $(a^2 - b^2)u$ also realizes the elements of F. Thus, $\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$ belongs to N for all $v \in F$. Step 3 then gives that the matrices $\begin{pmatrix} 1 & 0 \\ -v & 1 \end{pmatrix}$ also belong to N as v varies over F. But then so do all of the matrices $\begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}$. Therefore, by Step 5, $N = \mathrm{SL}_2(F)$. $\square$

Remark. The orders of the smallest non-abelian simple groups are 60, 168, 360, 504, 660, 1092 and 2,448. For each of these seven integers n, there is, up to isomorphism, just one simple group of order n and each of these groups arise as $\mathrm{PSL}_2(F)$ for an appropriate choice of F.

For example, take $F := \mathbb{Z}_5$. We show that $|\mathrm{PSL}_2(\mathbb{Z}_5)| = 60$. To do this, we first calculate $|\mathrm{SL}_2(\mathbb{Z}_5)|$. For matrices in $\mathrm{SL}_2(\mathbb{Z}_5)$ of the form $\begin{pmatrix} a & 0 \\ * & * \end{pmatrix}$, there are 4 non-zero choices for a. Thus, such a matrix has the form $\begin{pmatrix} a & 0 \\ * & a^{-1} \end{pmatrix}$ and for a fixed a, we have 5 choices for *. This gives 20 matrices of the form $\begin{pmatrix} a & 0 \\ * & a^{-1} \end{pmatrix}$. Similarly, there are 20 matrices of the form $\begin{pmatrix} 0 & b \\ b^{-1} & * \end{pmatrix}$. For matrices of the form $\begin{pmatrix} a & b \\ * & * \end{pmatrix}$, with both a and b non-zero, there are $4 \cdot 4 = 16$ choices for the first row. Moroever, such a matrix is $\begin{pmatrix} a & b \\ u & v \end{pmatrix}$, with $av - bu = 1$. Any choice of v then determines u and we can make 5 choices for v, once a and b have been chosen. Thus, there are $5 \cdot 16 = 80$ matrices with both a and b non-zero. It follows that $|\mathrm{SL}_2(\mathbb{Z}_5)| = 20 + 20 + 80 = 120$. Thus, $|\mathrm{PSL}_2(\mathbb{Z}_5)| = 120/2 = 60$. Therefore, by the theorem above, $|\mathrm{PSL}_2(\mathbb{Z}_5)|$ is a simple group of order 60. A similar counting argument shows that $|\mathrm{PSL}_2(\mathbb{Z}_7)| = 168$.

Finally, we point out that what we have now shown is that $\mathrm{PSL}_2(\mathbb{Z}_5)$ is a simple group of order 60, and thus by the theorem from class, this group must be isomorphic to A_5. As we saw in class, A_n is simple for all $n \geq 5$. Likewise, it can be shown that for any $n \geq 2$, $\mathrm{PSL_n}(F)$ is a simple group. Thus, two of the families of finite simple groups are $\{A_n\}_{n\geq 5}$ and $\{\mathrm{PSL_n}(F)\}_{n\geq 2}$, with F a finite field having at least 5 elements.

Department of Mathematics, University of Kansas