

Today I want to explain part of the proof of Theorem 34.6. In these notes I will write the entire proof. However, in the lecture, I will explain the outline of the proof and just a few of the details. I also want to explain what is projective space so we can see where the name *projective unimodular* comes from (unimodular means determinant 1).

First, let's answer the question: What is  $Z_0 = Z \cap SL(2, q)$ ?

The elements are diagonal matrices:

$$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

with determinant 1. So:  $x^2 = 1$ , or  $x = \pm 1$ . (The polynomial  $x^2 - 1$  has at most 2 roots by Corollary 33.9 so these are the only solutions.) When the characteristic of the field is 2 then  $1 = -1$ . So  $Z \cap SL(2, q)$  is trivial in that case.

**Theorem 34.7.** *If  $q$  is odd then  $Z \cap SL(2, q)$  has two elements. If  $q$  is even then  $Z \cap SL(2, q)$  has only one element.*

**Corollary 34.8.** *The order of  $PSL(2, q)$  is given by*

- (1)  $|PSL(2, q)| = q(q^2 - 1)$  if  $q$  is even
- (2)  $|PSL(2, q)| = \frac{1}{2}q(q^2 - 1)$  if  $q$  is odd.

For example, we have:

$$\begin{aligned} q = 2 & : |PSL(2, 2)| = 2(4 - 1) = 6 \\ q = 3 & : |PSL(2, 3)| = \frac{1}{2}3(9 - 1) = 12 \\ q = 4 & : |PSL(2, 4)| = 4(16 - 1) = 60 \\ q = 5 & : |PSL(2, 5)| = \frac{1}{2}(25 - 1) = 60 \end{aligned}$$

Before going into the proof that  $PSL(2, q)$  is simple for  $q \geq 4$ , I want to explain the name. This group is the symmetry group of projective space.

**34.4. projective space.** Let's do  $PSL(2, \mathbb{R})$  since that is the most familiar version of projective space.

**Definition 34.9.** *Real  $n$ -dimensional projective space is defined to be the space of all lines through the origin in  $\mathbb{R}^{n+1}$ . It is denoted  $\mathbb{R}P^n$ .*

For example, 1-dimensional projective space, also called the **projective line**  $\mathbb{R}P^1$  is the set of all (straight) lines through the origin in the plane  $\mathbb{R}^2$ . Multiplication by any  $2 \times 2$  matrix maps lines to lines. So  $GL(2, \mathbb{R})$  acts on  $\mathbb{R}P^1$ . The central matrices

$$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

sends every line through the origin to itself. So,  $Z = Z(GL(2, \mathbb{R}))$  is in the kernel of this action. So the quotient group

$$PGL(2, \mathbb{R}) = \frac{GL(2, \mathbb{R})}{Z}$$

acts on  $\mathbb{R}P^1$  by linear symmetries including reflections. The subgroup

$$PSL(2, \mathbb{R}) = \frac{SL(2, \mathbb{R})}{Z \cap SL(2, \mathbb{R})}$$

gives only orientation preserving linear maps, i.e. no reflections.

If we replace  $\mathbb{R}$  with the finite field  $F = GF(q)$  then we get a finite plane  $F^2$  which has only  $q^2$  points and we get the *finite projective line*  $FP^1$  consisting of the lines through the origin. Each line has  $q$  points and two lines meet only at the origin. So,

$$|FP^1| = \frac{q^2 - 1}{q - 1} = q + 1.$$

This leads to the following theorem.

**Theorem 34.10.**  *$PSL(2, q)$  is isomorphic to a subgroup of the symmetric group on  $q + 1$  letters.*

**Corollary 34.11.**  *$PSL(2, 2) \cong S_3$  and  $PSL(2, 3) \cong A_4$ .*

**34.5. proof of simplicity of  $PSL(2, q)$ : outline.** The proof of the simplicity of  $PSL(2, q)$  for  $q \geq 4$  goes as follows.

The outline of the proof is the following.

- (1) To avoid cosets, we first reformulate the proof in terms of matrices. We want to show that any nontrivial normal subgroup of  $PSL(2, q)$  must be all of  $PSL(2, q)$ . This desired statement is equivalent to saying that every normal subgroup  $N \trianglelefteq SL(2, q)$  which properly contains the center  $Z \cap SL(2, q)$  must be all of  $SL(2, q)$ .
- (2) Suppose that  $N$  is as described in (1). Then  $N$  contains at least  $q(q - 1)$  elements.
- (3) If  $q \geq 4$  then

$$|N| \geq (q - 1)q \geq 3q = 2q + q > 2q + 2$$

- (4)  $|N| > 2q + 2$  implies that  $N$  contains an element of the form

$$B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

which is not in  $Z$ .

- (5) If  $N$  contains an element  $B$  as above, then  $N$  contains an elementary matrix  $E_{12}(a)$  or  $E_{21}(b)$ .

- (6) If  $N$  contains one elementary matrix then  $N$  contains all elementary matrices.
- (7) Every element of  $SL(2, q)$  is a product of elementary matrices. Therefore,  $N = SL(2, q)$ .

This proof is based on the proof given in Rotman's "An introduction to the theory of groups" with one step changed because either Rotman made a mistake or I am really dense and I couldn't understand it. (If  $M$  has trace 0 then  $M^2 \in Z$  making the rest of the argument invalid.)

**34.6. details of the proof.** I will start with the last two steps.

**Lemma 34.12.** *In a cyclic group of odd order, every element has a unique square root. (I.e., for all  $g \in G$  there is a unique  $x \in G$  so that  $x^2 = g$ .) In a cyclic group of even order exactly half of the elements have a square root.*

*Proof.* In  $\mathbb{Z}_{2k}$  half the elements are even. In  $\mathbb{Z}_{2k+1}$  all the elements are even since odd numbers are negative even numbers.  $\square$

**Lemma 34.13** (Step 6). *If a normal subgroup  $N$  of  $SL(2, q)$  contains one elementary matrix then it contains all elementary matrices.*

*Proof.* I will prove this first in the case when  $q$  is even. Suppose that  $N \trianglelefteq SL(2, q)$  and  $E_{12}(a) \in N$ . Take any other elementary matrices:  $E_{12}(b)$  or  $E_{21}(b)$ . Since  $F^\times$  has an odd number ( $q - 1$ ) of elements, there is an  $x \in F^\times$  so that  $x^2 = ba^{-1}$  or  $b = x^2a = -x^2a$ . But then

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & x^2a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in gNg^{-1} = N$$

where  $g = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ . So  $N$  contains all elementary matrices of the form  $E_{12}(b)$ . Also,

$$\begin{pmatrix} 0 & -x^{-1} \\ x & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & x^{-1} \\ -x & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -x^2a & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

So  $N$  contains all elementary matrices of the form  $E_{21}(b)$ .

In the case when  $q$  is odd,  $q - 1$  is even. Since  $F^\times$  is cyclic, exactly half of the nonzero elements  $b \in F$  can be written in the form  $b = x^2a$ . So,  $N$  contains  $E_{12}(b)$  for  $\frac{1}{2}(q - 1)$  choices of the element  $b$ . But  $N$  also contains the identity which is  $I_2 = E_{12}(0)$ . So,  $N$  contains  $E_{12}(b)$  for  $\frac{1}{2}(q + 1)$  choices of  $b$ . This is more than half the elements of  $F$ . But the mapping  $\phi(b) = E_{12}(b)$  is a homomorphism:

$$\phi(a)\phi(b) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + b \\ 0 & 1 \end{pmatrix} = \phi(a + b)$$

So, the set of all  $b$  so that  $E_{12}(b) \in N$  is an additive subgroup of  $F$ . As such the number of such  $b$  divides  $q$  by Lagrange's Theorem. Since this number is greater than  $q/2$  it must be equal to  $q$ . So  $N$  contains all  $E_{12}(b)$ . Conjugating by  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  we see that  $N$  also contains all  $E_{21}(b)$ . This proves the lemma in all cases.  $\square$

**Lemma 34.14** (Step 7). *Every element of  $SL(n, F)$  is a product of elementary matrices for any field  $F$*

*Proof.* I will prove this only in the case that we need: when  $n = 2$ . Take any matrix with determinant 1:

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

Suppose that  $a \neq 0$ . Then  $ad - bc = 1$ . So

$$d = a^{-1}(1 + bc)$$

Take the following three elementary matrices:

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

$$E_{12}(-a)E_{21}(a^{-1})E_{12}(-a) = \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix}$$

If  $a = -1$  this is:

$$E_{12}(1)E_{21}(-1)E_{12}(1) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

So, we get a product of 6 elementary matrices:

$$\begin{aligned} & E_{12}(-a)E_{21}(a^{-1})E_{12}(-a)E_{12}(1)E_{21}(-1)E_{12}(1) \\ &= \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \end{aligned}$$

Now multiply on the left by  $E_{21}(ca^{-1})$  and on the right by  $E_{12}(ba^{-1})$  to get

$$\begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b/a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & a^{-1}(1 + bc) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

So, our matrix is a product of 8 elementary matrices.

If we started with a  $2 \times 2$  matrix  $A$  where  $a = 0$  then  $AE_{21}(1)$  has upper left entry not zero. So  $AE_{21}(1)$  is a product of 8 elementary matrices, making  $A$  a product of 9 elementary matrices.  $\square$

**Lemma 34.15** (Steps 4,5). *Suppose that  $N$  is a normal subgroup of  $SL(2, q)$  which contains more than  $2q + 2$  elements. Then  $N$  contains at least one elementary matrix.*

*Proof. Step 4.* First we find the matrix  $B$ .

The group  $N$  acts on the projective line  $FP^1$  which has  $q+1$  elements. The orbit-stabilizer formula says:

$$|N_x| = \frac{|N|}{|Nx|}$$

If  $|N| > 2q + 2 = 2|FP^1| \geq 2|Nx|$  then the stabilizer  $N_x$  has at least 3 elements. The center  $Z \cap SL(2, q)$  has at most 2 elements. So  $N_x$  has a noncentral element for every line  $x$ . Let  $x$  be the  $x$ -axis. Then  $N$  contains a noncentral element  $B$  so that  $B$  sends the  $x$ -axis to the  $x$ -axis. This is the same as saying that

$$B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \notin Z$$

This completes Step 4.

**Step 5.** Now we want to show that  $N$  contains an elementary matrix given that it contains  $B$ .

Note that  $c = a^{-1}$  since  $ac = \det B = 1$ . If  $a = 1$  then  $B$  is an elementary matrix and we are done. So, we may assume that  $a \neq 1$ . When  $q$  is even this also implies  $a \neq -1$  since  $1 = -1$ . If  $q$  is odd then we might have  $a = -1$ . In that case,  $c = -1$  and  $b \neq 0$  (otherwise  $B = -I_2 \in Z$ ). So,

$$B^2 = \begin{pmatrix} 1 & -2b \\ 0 & 1 \end{pmatrix} = E_{12}(-2b)$$

is an elementary matrix. ( $-2b \neq 0$  since  $q$  is odd.)

So, we may assume that  $a \neq \pm 1$ . Since  $g = E_{12}(1) \in SL(2, F)$  and  $E_{12}(1)^{-1} = E_{12}(-1)$  then  $gBg^{-1} \in gNg^{-1} = N$  and  $B^{-1} \in N$ . So  $N$  also contains their product:

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_g \underbrace{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}}_B \underbrace{\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}}_{g^{-1}} \underbrace{\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}}_{B^{-1}} = \underbrace{\begin{pmatrix} 1 & 1 - a^2 \\ 0 & 1 \end{pmatrix}}_{E_{12}(1-a^2)}$$

Since  $a \neq \pm 1$ ,  $1 - a^2 \neq 0$ . So this is an elementary matrix contained in  $N$ . □

Since steps 1 and 3 don't require proof, we just need to prove step 2.

**Lemma 34.16** (Step 2). *If  $N$  is a nontrivial normal subgroup of  $SL(2, q)$  which properly contains the center  $Z \cap SL(2, q)$  then  $N$  has at least  $q(q-1)$  elements.*

*Proof.* Take any element  $A \in N$  which is not in the center  $Z$ . Then

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

where we can assume that  $c \neq 0$  (otherwise  $A$  is the matrix  $B$  that we are looking for showing that  $N = SL(2, q)$  with  $q(q^2 - 1)$  elements).

Since  $c \neq 0$ , The following matrices are all different elements of  $N$ :

$$\underbrace{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}}_g \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_A \underbrace{\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}}_{g^{-1}} = \begin{pmatrix} a + cx & * \\ c & d - cx \end{pmatrix} \in gNg^{-1} = N$$

where I didn't care what was  $*$ . This gives  $q$  elements of  $N$  with the same  $c$ . If we take  $x = dc^{-1}$  we would get a zero in the lower right corner. Then the upper right corner must be  $-c^{-1}$ :

$$C = \begin{pmatrix} a + d & -c^{-1} \\ c & 0 \end{pmatrix} \in N$$

The inverse is

$$C^{-1} = \begin{pmatrix} 0 & c^{-1} \\ -c & a + d \end{pmatrix} \in N$$

Taking commutator with  $h = E_{12}(y)$  we get

$$\underbrace{\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}}_h \underbrace{\begin{pmatrix} a + d & -c^{-1} \\ c & 0 \end{pmatrix}}_C \underbrace{\begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix}}_{h^{-1}} \underbrace{\begin{pmatrix} 0 & c^{-1} \\ -c & a + d \end{pmatrix}}_{C^{-1}} =$$

$$\begin{pmatrix} a + d + cy & * \\ c & -cy \end{pmatrix} \begin{pmatrix} 0 & c^{-1} \\ -c & a + d \end{pmatrix} = \begin{pmatrix} * & * \\ c^2y & * \end{pmatrix}$$

As  $y$  runs over all nonzero elements of  $F$ ,  $c^2y$  runs over all  $q-1$  elements of  $F^\times$ . For each of these we can let  $x$  run over the  $q$  elements of  $F$  and we get a total of  $q(q-1)$  elements of  $N$  and we are done.  $\square$

**34.7. step 1 and the 3rd isomorphism theorem.** The first step in this proof uses the third isomorphism theorem. Given a homomorphism of groups

$$\phi : G \rightarrow H$$

the first isomorphism theorem says that the kernel of  $\phi$  is a normal subgroup of  $G$  and the image of  $\phi$  is a subgroup of  $H$ . The second isomorphism theorem says that

$$G/\ker \phi \cong \text{im } \phi$$

and the third isomorphism theorem says:

**Theorem 34.17.** *There is a 1-1 correspondence between subgroups  $K$  of the image of  $\phi$  and subgroups of  $G$  which contain  $\ker \phi$ . This correspondence is given by  $K \leftrightarrow \phi^{-1}K$ . Furthermore,  $K \trianglelefteq \text{im } \phi$  if and only if  $\phi^{-1}K \trianglelefteq G$ .*

**Corollary 34.18.** *Suppose that  $\phi : G \rightarrow H$  is a surjective homomorphism of groups. Then  $H$  is a simple group if and only if the only normal subgroups of  $G$  which contain the kernel of  $\phi$  are  $G$  and  $\ker \phi$ .*

In the present situation, the homomorphism in question is the surjective mapping

$$\phi : SL(2, q) \rightarrow PSL(2, q)$$

To show that  $PSL(2, q)$  is simple we need to show that the only normal subgroup of  $SL(2, q)$  which contains  $\ker \phi = Z_0 = Z \cap SL(2, q)$  are  $Z_0$  and  $SL(2, q)$ . That proves Step 1.