Title: Simple Groups Of Type PSL(2,q)

Author: Nicolás Kupfer Subi

Advisor: José Burillo

Department: Applied Mathematics IV

Academic year: 2012 - 2013
Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Bachelor’s Degree Thesis

Simple Groups Of Type $PSL_2(q)$

Nicolás Kupfer Subi

Advisor: José Burillo

Departament de Matemàtica Aplicada IV
to my science teachers at highschool, that so strongly tried to discourage me from studying mathematics.
Abstract

Key words: Simple Group Theory

MSC2000: Codes from the Mathematic Subject Classification

This paper is an introduction to the theory of simple and finite groups. The proof of the simplicity of the Projective Special Linear Group (PSL) and some homomorphisms between them will be covered. In addition, a few things of the simple non-cyclic groups of order less than 1000 will also be said.
Index

1 Introduction 2
   1.1 Preliminaries 2
   1.2 What is a simple group? 2
   1.3 What will we do with them? 3
   1.4 What is $PSL_2$? 4
   1.5 What type of groups do they yield? 4
   1.6 Which groups are they? 5
   1.7 Order of $PSL_2(q)$ 5

2 Simplicity of $PSL_2(q)$ 6
   Proof of the simplicity of the groups of $PSL_2(q)$ type
      2.1 Preliminaires 6
      2.2 Setup 6
      2.3 Final steps 10

3 Group Isomorphisms 13
   Study of the five groups and their isomorphisms
      3.1 Isomorphism $PSL_2(5) \cong A_5$ 13
         3.1.1 Facts 13
         3.1.2 Isomorphism 14
      3.2 Isomorphism $PSL_2(4) \cong A_5$ 17
         3.2.1 The field $F_4$ 17
         3.2.2 Facts 17
         3.2.3 Isomorphism 18
      3.3 $PSL_2(7)$ 20
         3.3.1 Facts 20
         3.3.2 Isomorphisms 20
      3.4 $PSL_2(8)$ 21
         3.4.1 The field $F_8$ 21
         3.4.2 Facts 21
      3.5 Isomorphism $PSL_2(9) \cong A_6$ 22
         3.5.1 The field $F_9$ 22
         3.5.2 Facts 22
         3.5.3 Isomorphism 22
      3.6 $PSL_2(11)$ 24
         3.6.1 Facts 24
Chapter 1

Introduction

1.1 Preliminaries

This work has the goal of showing the groups of type $\text{PSL}_2(q)$, prove their simplicity, present the five simple non-abelian groups of order less than 1000 and study them at some detail. The project, originally more ambitious that the one here presented, proposed to study and analize those groups, but has suffered a transformation resulting in what is shown: we have given much more importance to the proofs of simplicity, isomorphisms between groups and the need to have a self-contained project.

1.2 What is a simple group?

Stepping through the definitions quickly:

1) A group is a set $G$ (in our case, finite) along with an operator (denoted $\cdot$), altogether denoted $(G, \cdot)$, satisfying

   a) if $a, b \in G$ then $a \cdot b = ab \in G$ (i.e. $G$ is closed under ‘$\cdot$’).
   
   b) there exists a unique identity element $e$ such that $ae = ea = a$, $\forall a \in G$
   
   c) for each $a \in G$ there exists a unique $b \in G$ such that $ab = e$
   
   d) the operation is associative: $(ab)c = a(bc)$

2) A subgroup of $G$ is a subset $H \subseteq G$ such that $H$ has a group structure with the induced operation in $G$. The notation for subgroup is $H < G$.

3) Suppose now $g \in G$. A subgroup $N < G$ is said to be normal (and denoted $N \triangleleft G$) if for each $g \in G$, $gNg^{-1} = N$, that is, if $g$ conjugates any element of $N$ into $N$, but not necessarily into itself.

   An equivalent definition is that, for any $g \in G$ and for any $n \in N$, there exists $n' \in N$ such that $gng^{-1} = n'$.

4) Finally, getting to the matter of the subject, a simple group is a group whose only normal subgroups are the group itself and the identity (called trivial group); that is to say, a group that contains no non-trivial normal subgroups. Simple groups can be considered as the basic building blocks of the whole
group theory, much as the prime numbers are considered the basic blocks of arithmetic.

First introduced by Galois in 1832, who gave a formal definition of normal subgroup and found the simple groups $A_n$ for $n \geq 5$ and $PSL_2(F_q)$ for $p \geq 5$, the latter studied in this article, simple groups have been a field of intense mathematical research over the last century; the classification of simple groups theorem (whose complete proofs spans an estimate 5,000 pages) was completed in 2008, so it is still a very recent field.

Given a subgroup $H < G$, $d = |H|$, then $d| |G|$ (this is known as Lagrange’s Theorem). But, given a finite group $G$ and a divisor $d$ such that $d| |G|$, then not always exists a subgroup $H < G$ with $|H| = d$. This is true, however, when $d = p$ is a prime dividing $|G|$ (i.e., when $p| |G|$) leading to a $p$-subgroup and, finally getting to the point, it is true when $d = p^r$, being $p^r$ the maximum power of $p$ in the prime factorization of $|G|$: then $p^r = |H|$ and $H$ is called a Sylow $p$-subgroup of $G$.

If $G$ is a simple group, for each subgroup $H \subseteq G$ there must exist at least another subgroup $H' \neq H$, $|H'| = |H'|$, satisfying $gHg^{-1} = H'$ for some $g \in G$ (and we say $H$ and $H'$ are conjugate, and each subgroup may have more than one conjugate). This is so because if such $H'$ did not exist, then we would have $gHg^{-1} = H$ for every $g \in G$ (i.e., $H \triangleleft G$).

Getting to the point: we will need to know how many Sylow $p$-subgroups of each kind are in a given group $G$ (for instance, to study the group isomorphisms later presented in chapter 3), and a powerful tool for this study is a set of three theorems, called Sylow Theorems, presented below:

**Theorem 1.2.1** (1st Sylow Theorem). Let $p$ be a prime number, and $G$ a group of order $n$, with $n = p^r m$ and gcd$(p, m) = 1$. Then $G$ has a subgroup of order $p^r$.

**Theorem 1.2.2** (2nd Sylow Theorem). Let $H$ be a $p$-subgroup of $G$, and $S$ be a Sylow $p$-subgroup of $G$. Then, there exists $g \in G$ such that $H \subseteq gSg^{-1}$. In particular, any Sylow $p$-subgroups are conjugate.

**Theorem 1.2.3** (3rd Sylow Theorem). The number of Sylow $p$-subgroups $n_p$ of a group $G$ with $|G| = p^r m$ divides $m$ and is congruent with 1 modulo $p$. That is, $n_p \equiv 1 \pmod p$ and $n_p|m$.

### 1.3 What will we do with them?

The purpose of this work is to study the matrix groups that will be defined just below, $PSL$.

This family of groups have the property of being ‘all’ simple (we will discuss it eventually), and present the appropriate information, as well as isomorphisms between different kinds of groups.
1.4 What is $\text{PSL}$?

Consider the set of invertible $n \times n$ matrices over a field (in our case, finite) $F$, denoted by $\text{GL}_n(F)$, called the General Linear Group, evidently because it yields a group (for instance, when $n = 2$ we obtain the Lie Group): the product of two invertible matrices is also invertible, and given any invertible matrix, its inverse will be in $\text{GL}$ too, since it is also invertible.

When we are in finite fields of order $q$ like ours, we denote it by $\text{GL}_n(F_q)$ or just $\text{GL}_n(q)$. And this has a famous subgroup (which, by the way, is normal in it, though this is not of our concern) called $\text{SL}$, the Special Linear Group (and formally denoted $\text{SL}_n(q)$) that consists in the matrices with unit determinant.

What we are doing here, though, differs notoriously from it.

The same way we define a projective line $\mathbb{P}^1$ over $\mathbb{R}$ (the Real numbers), or the complex plane $\mathbb{P}^2$ over $\mathbb{R}^2$, etc., we define the Projective Special Linear Group $\text{PSL}_n(q)$ the same way, that is, we obtain $\text{PSL}$ using the same equivalence relation: given two matrices $a, b$ in $\text{SL}$ they will be the same in $\text{PSL}$ if, and only if, there exists an element $\lambda \in F_q$ such that $\lambda a = b$.

Formally, considering the equivalence relation $\sim$ satisfying

\[ a \sim b \iff \exists \lambda \in F_q \text{ such that } \lambda a = b \]

then $\text{PSL}$ comes along by saying

\[ \text{PSL} = \text{SL} / \sim \]

so two matrices are the same in $\text{PSL}$ if one is a scalar multiple of the other.

1.5 What type of groups do they yield?

The interesting part comes when studying the $\text{PSL}_n(q)$ groups, for we discover that they produce simple groups (except for two cases: $\text{PSL}_2(2)$ and $\text{PSL}_2(3)$).

This is in fact a theorem, and the complete proof (for the case $n = 2$) will be covered in the next section. The proof of simplicity for $n > 2$ will not be covered, since the five simple groups studied here are from the family $\text{PSL}_2(q)$.

Moreover, there are only 5 simple non-abelian groups of order less than 1000. And each of those groups is isomorphic to one of type $\text{PSL}_2(q)$ (that is to say, each of those 5 groups is a group of $\text{PSL}$ type). In addition, even though $\text{PSL}_n(q)$ generates different groups as $n$ and $q$ vary, we find some coincidences among them: $\text{PSL}_2(4)$ and $\text{PSL}_2(5)$ are isomorphic (this will be proven in section 3.2, page 17), and $\text{PSL}_2(7)$ and $\text{PSL}_3(2)$ are also isomorphic (see 3.3.2 on page 20).
1.6 Which groups are they?

The list of the five groups here treated are:

<table>
<thead>
<tr>
<th>Order</th>
<th>Factorization</th>
<th>Group</th>
<th>Isomorphic To</th>
<th>Field $F_q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>$2^2 \cdot 3 \cdot 5$</td>
<td>$PSL_2(4)$</td>
<td>$A_5$</td>
<td>$\mathbb{Z}_2[x] \left/ (x^2 = x + 1) \right.$</td>
</tr>
<tr>
<td>60</td>
<td>$2^2 \cdot 3 \cdot 5$</td>
<td>$PSL_2(5)$</td>
<td>$A_5$</td>
<td>$\mathbb{Z}/5\mathbb{Z}$</td>
</tr>
<tr>
<td>168</td>
<td>$2^3 \cdot 3 \cdot 7$</td>
<td>$PSL_2(7)$</td>
<td>$PSL_3(2)$</td>
<td>$\mathbb{Z}/7\mathbb{Z}$</td>
</tr>
<tr>
<td>360</td>
<td>$2^3 \cdot 3^2 \cdot 5$</td>
<td>$PSL_2(9)$</td>
<td>$A_6$</td>
<td>$\mathbb{Z}_3[x] \left/ (x^2 = x + 1) \right.$</td>
</tr>
<tr>
<td>504</td>
<td>$2^3 \cdot 3^2 \cdot 7$</td>
<td>$PSL_2(8)$</td>
<td>$-$</td>
<td>$\mathbb{Z}_2[x] \left/ (x^3 = x + 1) \right.$</td>
</tr>
<tr>
<td>660</td>
<td>$2^3 \cdot 3 \cdot 5 \cdot 11$</td>
<td>$PSL_2(11)$</td>
<td>$-$</td>
<td>$\mathbb{Z}/11\mathbb{Z}$</td>
</tr>
</tbody>
</table>

1.7 Order of $PSL_2(q)$

We want to compute the order of the Projective Special Linear Group over the field of $q$ elements, $F_q$, generated by $2 \times 2$ matrices. For this, we will start by computing the order of $PGL_2(q)$, the Projective General Linear Group, formed by invertible matrices of any determinant.

For the first column, any nonzero vector will be valid, thus $q^2 - 1$ possibilities. For the second column, any not null vector will be valid, as long as it is not a scalar multiple of the first; thus $q^2 - 1 - (q - 1) = q^2 - q$ possibilities for the second one.

Now this generates, of course, a matrix with non-zero determinant (i.e., from $GL_2(q)$), hence we need to restrict it to the set of matrices with determinant 1 (i.e., from $PGL_2(q)$), and we achieve this dividing by the number of non-zero elements in $F_q$:

$$
\frac{(q^2 - 1)(q^2 - q)}{q - 1} = q^3 - q
$$

and this is the order of $PGL_2(q)$.

Now, and as said before on section 1.4 (page 4), we must divide by the center of $PGL_2(q)$ (called $SZ_2(q)$ in this case, is naturally associated with the scalar matrices whose elements are the square roots of 1) to obtain $PSL_2(q)$, which has order 2 if $q$ is odd and order 1 if $q$ is even. This is so because when $q$ is even the polynomial $x^2 + 1 = 0$ is in fact $(x + 1)^2 = 0$, so the only square root of 1 is 1. This is very easy to see in practice; for example the only element $a \in F_4$ such that $a^2 = 1$ is 1; in $F_5$ there are two, 1, $-1$; in $F_7$ two again, 1, $-1$, etc.

With that, we can compute a general form that contemplates this:

$$
|PSL_2(q)| = \frac{1}{\gcd(2, q - 1)} \cdot (q^3 - q)
$$

This formula will be extensively used along the study of the 5 groups that will be presented here.
Chapter 2

Simplicity of $\text{PSL}_2(q)$

2.1 Preliminaires

In this section we will prove the simplicity of the set of groups $\text{PSL}_2(q)$ for $q \geq 4$, that is, over the field $F_q$ with $|F_q| \geq 4$.

Starting with a bit of setup, we will present and prove all necessary facts to simplify the proof at its most.

**Definition 2.1.1** (transvection). Let $V$ be a vector space. A transvection is a linear mapping $v \in V \mapsto v + f(v)a$ for some $f \in V^*$ and some $a \in V$. In terms of coordinates, we can define a (coordinate) transvection as a matrix $A$ such that $\text{rk}(A - I) = 1$ and $(A - I)^2 = 0$. If we denote by $\text{Fixed}(A)$ the subspace of $V$ that is fixed by an element $A \in \text{SL}_n(V)$, then we can also define a transvection as such element if it satisfies $\dim(\text{Fixed}(A)) = n - 1$ and $\det(A) = 1$.

This was a general definition of a transvection, generalized for any vector space, finite or not. The definition that suits us better is the following:

**Definition 2.1.2** (transvection). A transvection matrix is a matrix consisting of ones on the diagonal and a single non-zero element out of it. In addition, such matrices $A$ hold the properties $\text{rk}(A - I) = 1$ and $(A - I)^2 = 0$.

2.2 Setup

Let us start with the required preliminaries for the theorem:

**Proposition 2.2.1.** $\text{SL}_n(F)$, the Special Linear Group, is generated by transvections.

**Proof.** All we need to do is choose a generic element and decompose it as a product of transvections. Let

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

be such generic element, with $ad - bc = 1$
Let us start with the easiest case, where \( b = 0 \). This implies \( ad = 1 \), since it must have determinant one.

- Case \( c = 0 \)
  
  Here, the matrix we are considering is diagonal, and its decomposition as a product of such transvections is:

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

- Case \( c \neq 0 \)

\[
\begin{pmatrix}
a & 0 \\
c & a^{-1}
\end{pmatrix}
= \begin{pmatrix} 1 & (a - 1)c^{-1} \\ 0 & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 \\ b^{-1}(a - 1) & 1 \end{pmatrix}
\]

- If \( b \neq 0 \) we require a most exhaustive case-based decomposition:

- Case \( d = 0 \)

  For the same reason as before, now \( b \) and \( c \) must be nonzero and satisfying \(-c = b^{-1}\)

\[
\begin{pmatrix}
a & b \\
-b^{-1} & 0
\end{pmatrix}
= \begin{pmatrix} 1 & 0 \\ -b^{-1} & 1 \end{pmatrix}
\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 \\ b^{-1}(a - 1) & 1 \end{pmatrix}
\]

- Case \( d \neq 0 \)

  \* if \( a = 0 \)

\[
\begin{pmatrix}
0 & b \\
-b^{-1} & d
\end{pmatrix}
= \begin{pmatrix} 1 & 0 \\ (d - 1)b^{-1} & 1 \end{pmatrix}
\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 \\ -b^{-1} & 1 \end{pmatrix}
\]

  \* and finally, the general case:

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
= \begin{pmatrix} 1 & 0 \\ b^{-1}d & 1 \end{pmatrix}
\begin{pmatrix} 1 & (1 - a)b \\ 0 & 1 \end{pmatrix}
\begin{pmatrix} 1 & 0 \\ 1 & b \\ -b^{-1} & 1 \end{pmatrix}
\begin{pmatrix} 0 & 1 \end{pmatrix}
\]

♠
We have now seen that any element in $SL_2(q)$ can be decomposed as a product of transvections. (Note that, in the general case, we might think $c$ plays no role; that is only half true, since once we fix $a, b$ and $d$ (and all $\neq 0$), $c$ is determined by the relation $c = (ad - 1)b^{-1}$.)

Next step is to find a generating set of the group, which we will need for the following proposition.

**Note 2.2.2.** Suppose we have a transvection

$$\sigma_{\lambda} := \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

and we want to obtain $\sigma_{\mu}$ through $SL_2(q)$-conjugacy. Thus, for this purpose, if we compute its conjugate through $\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}$ we obtain:

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1^{-1} & 0 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} 1 & a_1^2 \lambda \\ 0 & 1 \end{pmatrix}$$

but with another conjugacy element, $\begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix}$ we obtain a similar but different element, $\begin{pmatrix} 1 & a_2^2 \lambda \\ 0 & 1 \end{pmatrix}$

Since both elements are in $SL_2(F)$, its product will also be, and is

$$\begin{pmatrix} 1 & (a_1^2 + a_2^2) \lambda \\ 0 & 1 \end{pmatrix}$$

Then, choosing $a_1, a_2$ such that $a_1^2 + a_2^2 = \mu \lambda^{-1}$, we can obtain the desired conjugated transvection.

We will now prove that such two elements exist. We want to see that any element of a finite field is expressable as a sum of two squares. For this, we need two lemmas that will help us get through the proof of the following proposition.

**Lemma 2.2.3.** Every subgroup of the multiplicative group of a finite field is cyclic.

**Proof.** By induction on the order of the subgroup, suppose $G$ to be a multiplicative subgroup of a field $F$, with $|G| = n$ and $G$ being non-cyclic.

If $n = p^k$ with $p$ prime, not all $p^k$ elements of $G$ will have order $n$; and, since they generate subgroups of $G$ their order must divide $n$, so any element in $G$ will have order $p^r$ for each $i = 1, \ldots, p^k$. But then each $p^r$ divides $p^{k-1}$, so the equation $x^{p^{k-1}} = 1$ holds for each element in $G$, which is impossible since a polynomial of degree $d$ can have at most $d$ roots.

Now, if $n = ab$, with $\gcd(a, b) = 1$, then $(\cdot)^a : G \to G$ has a kernel $A$ of size at most $a$ (since, again, the kernel is the set of elements $x \in G$ such that $x^a = 1$) and a range $B$ of size at most $b$ (for the same reasoning), so $|A| = a$ and $|B| = b$ by the first isomorphism theorem. Finally, applying induction to $a$ and $b$, a product $xy$ of cyclic generators $x, y$, for $A, B$ respectively, generates $G$.  

$\blacksquare$
Note 2.2.4. In particular, given a finite field $F$, since it is a subgroup of itself, its multiplicative subgroup is also cyclic.

Lemma 2.2.5. Let $G$ be a finite group. If $A \subseteq G$ and $B \subseteq G$, with $|A| + |B| > G$, then $G = AB$. (Note: It could happen that $A = B$)

Proof. Let $g \in G$ be an arbitrary element.
We know that the set $gB^{-1} := \{gb^{-1} | b \in B\}$ is a subset of the same cardinality as $G$, therefore $|gB^{-1}| + |A| > G$, which means that exists $a \in A$ such that $a = gb^{-1}$ for some $b \in B$. And this is what we wanted, since now $g = ab$. ♠

Proposition 2.2.6. Let $F$ be a finite field of $q$ elements, and let $x \in F$. Then there exist $a_1, a_2 \in F$ such that $x = a_1^2 + a_2^2$.

Proof. Case of characteristic 2 The square mapping is surjective and every element is a square, because the multiplicative group is of odd order.

Case of odd characteristic We know the multiplicative group of $F$, $F^*$, has $q - 1$ elements. By the first lemma, $F^*$ is cyclic of order $q - 1$ (even), and exactly half of the $q - 1$ elements (the even powers of the generator) are squares. But since 0 is also a square, we get in total $(q+1)/2$.
Now, if $G$ denotes the additive group of $F$, considering the groups $A = B$ consisting of this $(q+1)/2$ elements, by the second lemma they generate $G$ and hence $F$, so every element in $F$ is a sum of [at most] two squares. ♠

To make notation easier, we will define

$$\tau_\gamma := \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$$

Note that any transvection in $SL_2(F)$ is rather $\sigma_x$ or $\tau_x$ for some $x \in F$, $x \neq 0$.
If we choose any $\gamma \in F$ and conjugate $\sigma_\lambda$ as before in such a way that we obtain $\sigma_{-\gamma}$ then, through a conjugacy with the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ we obtain $\tau_\gamma$.

Proposition 2.2.7. Given two transvections in $SL_2(F)$, we can always obtain one from the other by conjugacy, or as a product of conjugated elements.

Proof. This is just a union of all the things we have just seen. Let $u$ and $v$ be such transvections (the notation is slightly different to avoid messing notation), and we define

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

since we will use it often.

i) If $u = \sigma_x$ and $v = \sigma_y$.
Remember that any element in $F$ can be expressed as a sum of two squares (see note 2.2.2, page 8). Now, given $\sigma_x$ we can obtain $\sigma_y$ as a product of conjugated elements (as in the mentioned note, and using that $x, y \neq 0$ and $y = (a_1^2 + a_2^2)x$.)
ii) If $u = \tau_x$ and $v = \sigma_y$ (or vice versa) for some $x, y \in F_q$ then, by the previous point we can obtain $\sigma_{-x}$ through conjugacy of $v$ (or $u$ in the other case) and then, through the conjugacy of $s$, obtain $\tau_x$.

iii) Finally, if both $u = \tau_x$ and $v = \tau_y$, by the previous point (using the inverse conjugate, $s^{-1}$) we can transform $v$ into $\sigma_y$, then transform it into $\sigma_{-x}$ and apply the same reasoning again.

♣

Note 2.2.8. If $x = y$ (case i) and iii) $u = v$, and it is a trivial case. If $x = -y$ (case ii) we obtain one from the other easily: $\tau_y = s\sigma_{-y}s^{-1}$.

Note 2.2.9. Since $PSL_2(q)$ is a subgroup of $SL_2(q)$ and the latter is generated by transvections, then $PSL_2(q)$ is generated by transvections.

2.3 Final steps

As we could see in proposition 2.2.1, $SL_n(F)$ is generated by transvections, which meant any element could be written as a product of those. But now we want to do the opposite. We want to obtain a transvection given an element. And we want to do so in such a way both elements belong to the same normal group. Rephrasing:

Lemma 2.3.1. Given any non-identity element in $PSL_2(q)$, $q \neq 2, 3, 5$, we can obtain a transvection from it by conjugacy and commutation.

Proof. Let

$$A = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in PSL_2(q)$$

be any matrix. Consisting of four cases, the proof is basically constructive. We may assume $A$ is not a transvection, since that is what we want to obtain, for if $A$ were a transvection, we would be done.

1) Case $z = 0$.

Let $A$ given and of the form

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

Since $A$ is not a transvection, $x \neq x^{-1}$, so $x^2 \neq 1$; now $y$ can be any element, even zero, and we may choose $B$ conveniently

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

to obtain

$$ABA^{-1}B^{-1} = \begin{pmatrix} 1 & 1 - x^2 \\ 0 & 1 \end{pmatrix}$$
which is a transvection.

For the following steps the matrix $B$ will be given directly.

2) $z \neq 0$.

$$A = \begin{pmatrix} x & 0 \\ z & x^{-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad BAB^{-1} = \begin{pmatrix} x & -z \\ 0 & x \end{pmatrix}$$

and we are in case 1).

3) $y, z \neq 0, t = 0$.

$$A = \begin{pmatrix} x & y \\ -y^{-1} & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix},$$

$$BAB^{-1}A^{-1} = \begin{pmatrix} \alpha^2 & xy(\alpha^2 - 1) \\ 0 & \alpha^{-2} \end{pmatrix}$$

and we would, again, be in the first case but only if the condition $\alpha^4 \neq 1$ holds, since we need $a_{11}^2 = (\alpha^2)^2 \neq 1$, because in the first case we obtain

$$\begin{pmatrix} 1 & 1 - a_{11}^2 \\ 0 & 1 \end{pmatrix}$$

But in $F_q$, if $q = 2, 3, 5$, these elements do not exist, so we must consider that case separately; that is the main reason why the proof excludes them.

4) General case, $y, z, t \neq 0, x = t^{-1}(1 + yz)$.

$$A = \begin{pmatrix} x & y \\ z & t \end{pmatrix}, \quad B = \begin{pmatrix} 1 & xz^{-1} \\ 0 & 1 \end{pmatrix}, \quad B^{-1}A^{-1}B = \begin{pmatrix} x + t & z^{-1} \\ -z & 0 \end{pmatrix}$$

which is exactly case 3).

We have been through all the necessary steps of the preliminaries in order to proof the main theorem straightforward. In this last lemma we have seen the reasoning does not apply to the 2, 3 and 5 element fields, $F_2 \cong \mathbb{Z}_2$, $F_3 \cong \mathbb{Z}_3$ and $F_5 \cong \mathbb{Z}_5$, since any element $a$ in these satisfies $a^4 = 1$.

Makes sense, given that $PSL_2(2) \cong S_3$ and $PSL_2(3) \cong A_4$ are not simple. And for $F_5$, we will see in the next section (theorem 3.1.1 page 13) that $PSL_2(5) \cong A_5$ is simple; for this reason, then, we will include in in the following theorem.

Getting it now straightforward:

**Theorem 2.3.2.** $PSL_2(q)$ is simple if $q \geq 4$. 


Proof. Suppose it is not. Then there exists $H \triangleleft G = PSL_2(q)$, where $H \neq \{id\}$. Let $\rho \in H$, $\rho \neq id$. Since $H \triangleleft G$, we can conjugate $\rho$ (as in the previous lemma) and obtain a transvection (which will be in $H$), hence $H$ contains all transvections.

We know they generate $SL_2(F)$, therefore also generate $G < SL_2(F)$. So, if $H$ has any non-identity element, $H = G = PSL_2(q)$ contains no non-trivial normal subgroups, and is simple. ♠
Chapter 3

Group Isomorphisms

3.1 Isomorphism $\text{PSL}_2(5) \cong A_5$

$\text{PSL}_2(5)$ is the only simple group from the family $\text{PSL}_2(q)$ seen in the previous theorem that is not covered by the proof. For that reason, we will construct an isomorphism between it and $A_5$.

In addition, in the next section an isomorphism between $\text{PSL}_2(4)$ (which the proof assures its simplicity) and $A_5$ will be presented, leading to an isomorphism between these three groups here mentioned.

3.1.1 Facts

We know, from the order counting formula, the order of the group is 60. Hence $|\text{PSL}_2(5)| = 60$.

Since $60 = 2^2 \cdot 3 \cdot 5$, 3 and 5 being primes leading to cyclic groups.

The Sylow theorems state there can only be 1 or 6 Sylow 5-subgroups, since it must be a number $n_5$ such that $n_5 | 60$ and also $n_5 \equiv 1 \pmod{5}$. Since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

generate two different Sylow 5-subgroups, there must be 6.

The same reasoning can be applied to find the number of Sylow 3-subgroups $n_3$. Again using Sylow’s third theorem, $n_3 | 60$ and $n_3 \equiv 1 \pmod{3}$: the only possibilities are 1, 4 or 10. Again,

$$\begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 4 & 4 \end{pmatrix}$$

are 5 different Sylow 3-subgroups, so $n_3$ must be 10.

Finally, counting elements we find that $4n_5 + 2n_3 + 1 = 45$, so the set of Sylow 2-subgroups contain 15 non-identity elements. In addition, since the candidates

\footnote{See \[1\] (page 90, Corollary 10) for a detailed proof.}
for $n_2$ are 1, 3, 5, 15 and the intersection of such subgroups must be 1 or 2, the only possible number is 5, hence there are exactly 5 Sylow 2-subgroups, presented below:

$$s_1 = \begin{cases} 
(1,0), & (2,0), & (0,2), & (0,1) \\
(0,1), & (0,3), & (3,0), & (1,0) 
\end{cases}$$

$$s_2 = \begin{cases} 
(1,0), & (2,1), & (3,4), & (1,0) \\
(0,1), & (0,3), & (3,2), & (1,4) 
\end{cases}$$

$$s_3 = \begin{cases} 
(1,0), & (2,2), & (1,0), & (2,2) \\
(0,1), & (0,3), & (3,4), & (1,3) 
\end{cases}$$

$$s_4 = \begin{cases} 
(1,0), & (2,3), & (4,0), & (3,2) \\
(0,1), & (0,3), & (3,1), & (1,2) 
\end{cases}$$

$$s_5 = \begin{cases} 
(1,0), & (2,4), & (2,4), & (4,0) \\
(0,1), & (0,3), & (3,3), & (1,1) 
\end{cases}$$

where each Sylow (holding a Klein group structure $V_4$) has been obtained by conjugation of the previous one through the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ of order 5.

We can conclude saying that $PSL_2(5)$ has 5 Sylow 2-subgroups, 10 Sylow 3-subgroups and 6 Sylow 5-subgroups.

We can now associate each of this Sylow 2-subgroups, $\{s_1, s_2, s_3, s_4, s_5\}$ to $\{1, 2, 3, 4, 5\}$ by the natural correspondance $s_i \mapsto i$, thus getting a homomorphism from $G$ to $S_5$ from the conjugation action in $G$ onto the set of Sylow 2-subgroups, namely $X$.

This is so because Sylow’s second theorem asserts all the Sylow 2-subgroups belong to the same conjugacy class by $G$ (which allows us to obtain a subgroup by conjugation of another one) and, for any $g \in G$, the action by conjugation induces a permutation $s_i \mapsto s_{g(i)}$. Our point here is to see that this $\sigma$ is precisely a permutation in $A_5$, since that would imply the existence of such isomorphism, from $G$ to $A_5$, as stated before.

### 3.1.2 Isomorphism

We will present the isomorphism in the form of a theorem, since it is widely known this way.

**Theorem 3.1.1.** $PSL_2(5)$ is isomorphic to $A_5$, which is simple. Therefore, $PSL_2(5)$ is simple.

**Proof.** Using the set-up presented just before, we have defined a homomorphism naturally.

Next, we must see that the image of the homomorphism lives in $A_5$, so we must rule out the possibility of having permutations of odd order. Those are (1) the transpositions, (2) the cicles of order 4 and (3) the products of a 3-cycle and a transposition, the latter disjoints.
(1) Suppose an element \( g \in G \) such that its image is a single transposition in \( S_5 \). That means \( g^2 = id \), and without any loss of generality we can assume \( gxg^{-1} = (s_1s_2)(s_3)(s_4)(s_5) \). On the other hand, we know the intersection of any pair of Sylow 2-subgroups is trivial, so there is no order-two element belonging to two of them. In fact, \( g \) belongs to a Sylow 2-subgroup (because Sylow’s second theorem asserts all Sylow 2-subgroups belong to the same conjugacy class), so \( g \) must be one of the 15 distinct elements from the set of Sylow 2-subgroups; but, analyzing the action by conjugation of \( g \) onto \( X \) we obtain a product of transpositions (which belongs to \( A_5 \)). This happens because \( g \) leaves fixed the Sylow 2-subgroup to which it pertains, and transposes two-two the other four subgroups (for example, the element \( \left( \frac{2}{0} \frac{0}{2} \right) \in s_1 \) induces the permutation \( (s_2 s_3)(s_4 s_5) \) in \( S_5 \)). In other words, assuming that \( g \) acts as a single transposition leads to a contradiction.

(2) By the simple fact of supposing that \( g \) induces a 4-cycle, we deduce \( g \in G \) is a matrix of order 4, leading to a cyclic group of order four. This is of course impossible, since all five Sylow 2-subgroups are isomorphic to the Klein group, and any matrix of order 4 would generate a subgroup of \( G \) of order four, hence be isomorphic to the other Sylow 2-subgroups.

(3) For this last case we need to check is that \( g \) cannot induce a permutation of order six, namely the product of a transposition and a cycle, both disjoint. Since \( g \) is a matrix, it must be a matrix of order 6. To see it, we know (from point (1)) that any matrix of order 2 is one of the 15 non-identity elements of the Sylow 2-subgroups, so if we compute the cube of a generic matrix, \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right)^3 \in G \), and we see that no values of \( a, b, c, d \in F_5 \) (subjected to the convenient restrictions that \( PSL \) imposes) allow us to obtain any matrix from any of the Sylow 2-subgroups (for we have seen any matrix of order 2 is one of those), we can conclude no matrix of order 6 exists.

Now for the last part, we have a homomorphism from \( G = PSL_2(5) \) to \( A_5 \), and both groups have the same order. It remains to see that it is one-to-one, hence an isomorphism.

First we need to introduce the concept of all the normalizer of a subgroup \( S \), which is \( N_G(S) = \{ n \in G \ | \ \exists g \in G, s \in S \text{ such that } gsg^{-1} = n \} \)
and satisfies \( S \triangleleft N_G(S) \) for all subgroups \( S \) of \( G \).
Following the path, the order of the normalizer of the Sylow 2-subgroups can be computed using the formula counting orbit. Since we know that all Sylow 2-subgroups belong to the same orbit, we have
\[ 5 = |T_S| = [G : N_G(S)] \]
where \( T_S \) denotes the orbit and \( S \) is any of the Sylow 2-subgroups, and therefore the normalizer has order 12.

We need to see that the intersection of the normalizers \( M \) of the Sylow 2-subgroups is trivial. This must be so since we want to prove \( G \) to be simple, and because \( M \) is normal: if \( m \in M \), any Sylow 2-subgroup is fixed by it, but also any conjugate of \( m \) of the form \( gmg^{-1} \) for any \( g \in G \).
Two Sylow 2-subgroups intersect only in $id$, and since the normalizers have order 12 that leaves us at most 9 elements for $M$. But $|M|\mid 60$, which reduces the options to $|M| = 1, 2, 3, 4, 6$.

- **2** can be discarded, because then $M = \{id, m\}$, $M \triangleleft G$ and, for all $g \in G$ we would have $gmg^{-1} = m$, so $gm = mg$, and $m$ will be in the center of $G$, $Z(G)$. But the center of $PSL_n(q)$ is trivial, due to the center being the scalar multiples of the identity matrix, giving us $m = id$.

- **3** can be discarded too, because $M \triangleleft G$ would imply $M$ being the unique 3-Sylow, which we know it is not true (there are 10).

- **4** is not a valid order. As we have said in point (1) just above, all the subgroups of order 4 belong to one of the Sylow 2-subgroups. And if a Sylow 2-subgroup were $M$ it would be normal, again leading to a contradiction.

- Suppose now $M$ has order **6**. Since $M \triangleleft G$, $G/M \twoheadrightarrow A_5$ is a bijection (because the elements in $M$ are precisely the preimages of the identity in $A_5$, $id$), thanks to the first isomorphism theorem. And that would mean the image $Im$ has order 10, being $Im < A_5$. But $A_5$ has no subgroup of that order, a contradiction: a subgroup of order 10 cannot be a cycle, therefore it must be the product of a subgroup of order 2 and one of order 5 (which would not be disjoint), giving us an element of order 2 or 3 !

With all this in mind, we can proceed to the final step of the proof, consisting in showing the injectiveness of the homomorphism.

Suppose $gXg^{-1} = hXh^{-1}$, $g, h \in G$, induce the same permutation. Hence, $(h^{-1}g)X(h^{-1}g)^{-1} = X$, associated the identity permutation. So

$$gs_i g^{-1} = hs_i h^{-1} \quad \forall i = 1, 2, 3, 4, 5$$

$$h^{-1}g s_i (h^{-1}g)^{-1} = s_i \quad \forall i = 1, 2, 3, 4, 5$$

Hence $h^{-1}g$ belongs to $M$, the intersection of all the normalizers, but since $M = \{id\}$, $h^{-1}g = id$, so $g = h$ as desired.

We have proved that the homomorphism is in fact a isomorphism, so

$$PSL_2(5) \cong A_5$$

and, in particular, is **simple**.

♠
3.2 Isomorphism $\text{PSL}_2(4) \cong A_5$

3.2.1 The field $F_4$

$F_4$, also called Galois Field of 4 elements, $GF(2^2)$ or simply $GF(4)$ is a field of order 4 generated by the quotient

$$\mathbb{Z}_2[x] \bigg/ \langle x^2 = x + 1 \rangle$$

We construct $F_4$ as a quadratic extension of $\mathbb{Z}/2\mathbb{Z}$ by the roots of the polynomial $x^2 = x + 1$. If $\alpha$ denotes one root, then $\alpha + 1$ is the other one. Then, from the logic $1+1 = 0$ and $\alpha^2 = \alpha + 1$ we obtain that its four elements are $\{0, 1, \alpha, \alpha+1\}$.

The multiplication table has a very simple structure, so it will be presented below:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>$\alpha$</th>
<th>$\alpha+1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$\alpha+1$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>0</td>
<td>$\alpha$</td>
<td>$\alpha+1$</td>
<td>1</td>
</tr>
<tr>
<td>$\alpha+1$</td>
<td>0</td>
<td>$\alpha+1$</td>
<td>1</td>
<td>$\alpha$</td>
</tr>
</tbody>
</table>

With this information in hand, we can proceed to study the group structure of $\text{PSL}_2(4)$.

3.2.2 Facts

$G = \text{PSL}_2(4)$, a well known group, has been shown to be simple in the previous theorem that covered the simplicity of all this family of groups. Let us start by finding out its Sylow subgroups or, more precisely, how many are of each kind.

Using the formula for the order of $\text{PSL}_2(q)$ given in section 1.7, we have $|\text{PSL}_2(4)| = 60 = 2^2 \cdot 3 \cdot 5$; now, as in the case of $\text{PSL}_2(5)$, we want to obtain the Sylow $p$-subgroups.

With the same notation as before, $n_5$ can only be 1 or 6, but since $G$ is simple the only possible value is 6.

Now, for the Sylow 3-subgroups, $n_3$ can be 4 or 10 (and again 1 is excluded because $G$ is simple). Since

$$\left\langle \begin{pmatrix} \alpha & 1 \\ 0 & \alpha + 1 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} \alpha & \alpha \\ 0 & \alpha + 1 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} 0 & \alpha \\ \alpha & 1 \end{pmatrix} \right\rangle$$

are 5 Sylow 3-subgroups, we must conclude $n_3 = 10$.

Finally, using a counting method we find we are left with 15 non-identity elements, all belonging to some Sylow 2-subgroup. Pointing out the potential
candidates for the number of Sylow 2-subgroups, \( n_2 = 3, 5, 15 \), we find \( n_2 = 3 \) does not give us enough elements, and \( n_2 = 15 \) gives us at least 31 non-identity distinct elements, far too many. Therefore, \( n_2 = 5 \), and the intersection of Sylow 2-subgroups is trivial.

The 5 Sylow 2-subgroups are

\[
\begin{align*}
  s_1 & = \left\{ \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & \alpha + 1 \\ 0 & 1 \end{smallmatrix} \right) \right\} \\
  s_2 & = \left\{ \left( \begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} \alpha + 1 & \alpha \\ \alpha & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 0 & 1 \\ \alpha & 1 \end{smallmatrix} \right) \right\} \\
  s_3 & = \left\{ \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 0 \\ \alpha + 1 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 0 \\ \alpha & 1 \end{smallmatrix} \right) \right\} \\
  s_4 & = \left\{ \left( \begin{smallmatrix} 0 & 1 \\ \alpha & 0 \end{smallmatrix} \right), \left( \begin{smallmatrix} \alpha + 1 & 1 \\ \alpha + 1 & \alpha \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 1 \\ \alpha & \alpha + 1 \end{smallmatrix} \right) \right\} \\
  s_5 & = \left\{ \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 0 \\ \alpha & \alpha + 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 0 & \alpha \\ 1 & \alpha \end{smallmatrix} \right), \left( \begin{smallmatrix} 0 & \alpha \\ \alpha + 1 & 1 \end{smallmatrix} \right) \right\}
\end{align*}
\]

and it is very simple to verify that in fact they hold the group structure \( \{id, a, b, ab\} \), satisfying that each of those elements is of order 2, that is, each Sylow 2-subgroup is a Klein group \( V_4 \).

In conclusion, \( PSL_2(4) \) consists of 5 Sylow 2-subgroups, 10 Sylow 3-subgroups and 6 Sylow 5-subgroups.

We see it has the same order as \( A_5 \) and as \( PSL_2(5) \), and we intuit they might be isomorphic (in fact, the unique simple group of order 60 is, up to isomorphism, \( A_5 \); however, this fact will not be used: on the contrary, what we will do here is to explicitly construct an isomorphism to prove it).\(^2\)

\[\text{Note 3.2.1. For the homomorphism } PSL_2(4) \cong A_5 \text{ we have an advantage with respect to the isomorphism recently proved in section 3.1: we know beforehand } PSL_2(4) \text{ is simple, so only two things can happen: its kernel is the whole group or it is trivial.}\]

\[\text{3.2.3 Isomorphism}\]

**Proposition 3.2.2.** \( PSL_2(4) \) is isomorphic to \( A_5 \) and, in particular, to \( PSL_2(5) \).

**Proof.** \( G = PSL_2(4) \) has 5 Sylow 2-subgroups and acts on them by conjugation.

So we can define a homomorphism naturally

\[
\phi : PSL_2(4) \rightarrow S_5 \\
g \mapsto gXg^{-1}
\]

We want to study the action of conjugation of \( G \) on its set \( X \) of 5 Sylow 2-subgroups \( s_i \). Since all Sylow 2-subgroups belong to the same conjugacy class, we know that the conjugate of \( s_i \) via \( g \in G \) will be \( gs_ig^{-1} = s_j \) for some \( j \).

On the other hand, an element in a Sylow 2-subgroup can be associated with a (disjoint) product of transpositions in \( A_5 \), since if \( k \in s_i \) then \( kXk^{-1} \) does exactly that to \( X \): leaves fixed the other elements of the Sylow 2-subgroup

\[\text{See } [1] \text{ (page 147, Proposition 23) for the proof of uniqueness.}\]

\[\text{2See } [1] \text{ (page 147, Proposition 23) for the proof of uniqueness.}\]
to which it pertains and transposes two-two the other 4 Sylow 2-subgroups. For example, taking the element \( u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in s_1 \), it induces the permutation \((s_2 \ s_3)(s_4 \ s_5)\), leaving \( s_1 \) fixed.

More generally, given a Sylow 2-subgroup we know that the action of conjugation of \( G \) into \( X \) gives us again a Sylow 2-subgroup (the same one or a different one), and its elements are associated with the product of two disjoint transpositions.

So if we denote them by \( t_{ij}, i = 1, 2, 3, 4, 5, j = 1, 2, 3 \), then \( t_{ij} \) fixes \( i \), so

\[
\begin{align*}
    t_{11} &= (23)(45) \\
    t_{12} &= (24)(35) \\
    t_{13} &= (25)(34) \\
    t_{21} &= (13)(45) \\
    t_{22} &= (14)(35) \\
    t_{23} &= (15)(34)
\end{align*}
\]

and so on: this is a more formal explanation of the example. With this notation, then, the elements in the Sylow 2-subgroup \( s_i \) are

\[
s_i = \{id, t_{i1}, t_{i2}, t_{i3}\}
\]

Hence, element by element, the action of conjugation is associated with the even permutations in \( A_5 \), and their conjugates too, since they again are elements of some Sylow 2-subgroup. This means the image lives in \( A_5 \).

Finally, consider now a matrix of order 5

\[
h = \begin{pmatrix} \alpha & \alpha + 1 \\ \alpha & 0 \end{pmatrix}
\]

We see that

\[
\phi(h) = hXh^{-1}
\]

permutes all 5 Sylow 2-subgroups in a cycle of length five, that is to say there is an element in \( G \) whose image by \( \phi \) is not the identity. Hence, the first isomorphism theorem states that

\[
G/\ker(\phi) \rightarrow A_5
\]

is an isomorphism. Now \( G = PSL_2(4) \) is simple and \( \ker(\phi) \triangleleft G \), but also \( \ker(\phi) \neq G \) because \( \phi(h) \neq \text{id} \), so \( \ker(\phi) \) must be trivial, leading to an isomorphism \( PSL_2(4) \cong A_5 \); in addition, using the previous section, \( PSL_2(4) \cong PSL_2(5) \). 

\[\Box\]
3.3 PSL$_2(7)$

3.3.1 Facts

In this section we will study $PSL_2(7)$, the Projective Special Linear Group of $2 \times 2$ matrices over the field of seven elements, $\mathbb{Z}/7\mathbb{Z}$. This group has important applications in number theory, algebra and geometry, and holds a direct relationship with Fermat’s Last Theorem for $n = 7$, as well as with Fermat’s Curve of degree 7, $X^7 + Y^7 = Z^7$.

Using the counting formula seen in the section about the order of $PSL_2(q)$,

$$|PSL_2(7)| = \frac{1}{2}(7^3 - 7) = 168 = 2^3 \cdot 3 \cdot 7,$$

consisting of 7 Sylow 2-subgroups, 28 Sylow 3-subgroups and 8 Sylow 7-subgroups, where the intersection of the Sylow 2-subgroups is a subgroup of order 2.

Moreover, the Sylow 3-subgroups and Sylow 7-subgroups are cyclic (since they are of prime order), while the Sylow 2-subgroups are all isomorphic to the dihedral group $D_8$.

3.3.2 Isomorphisms

One of the particular characteristics of this group is that is isomorphic to $GL_3(2) \cong PSL_3(2)$, the set of $3 \times 3$ matrices over the field of two elements $\mathbb{Z}/2\mathbb{Z}$.

We know that, in order for a isomorphism to exists, $GL_3(2)$ must be simple, and as a matter of fact it is. The general theorem states:

**Theorem 3.3.1.** $PSL_n(q)$ is simple for any $n, q$, except for $PSL_2(2)$ and $PSL_2(3)$.

---

3See [3] for a detailed explanation.

4From $PSL_2(7)$ and over, this fact will not be explained in detail here, since the required calculations span several pages. In addition, the purpose of this work is neither to study this groups nor their Sylow $p$-subgroups exhaustively.

5We will not cover this proof, nor the proof of the group isomorphism (because of its length, and because it does not suit to the thread of this work), but we have dedicated it a couple of lines. The complete proof, not assuming simplicity of $GL_3(2)$ can be found in [2].
3.4 $\text{PSL}_2(8)$

3.4.1 The field $F_8$

The field of 8 elements (also called Galois Field $GF(8)$ or $GF(2^3)$) can be obtained by quotienting polynomials over the ring $\mathbb{Z}_2[x]$ by the ideal $(x^3 = x+1)$, so we have

$$F_8 = GF(2^3) = \mathbb{Z}_2[x]/(x^3 = x+1)$$

and the elements are

$$0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1$$

The group structure of $F_8$ will be presented in the following multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>$\alpha$</th>
<th>$\alpha + 1$</th>
<th>$\alpha^2$</th>
<th>$\alpha^2 + 1$</th>
<th>$\alpha^2 + \alpha$</th>
<th>$\alpha^2 + \alpha + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
<td>$\alpha^2 + \alpha$</td>
<td>$\alpha + 1$</td>
<td>$1$</td>
<td>$\alpha^2 + \alpha + 1$</td>
<td>$\alpha^2 + 1$</td>
</tr>
<tr>
<td>$\alpha + 1$</td>
<td>$\alpha^2 + \alpha$</td>
<td>$\alpha^2 + 1$</td>
<td>$\alpha^2 + \alpha + 1$</td>
<td>$\alpha^2$</td>
<td>$1$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>$\alpha + 1$</td>
<td>$\alpha^2 + \alpha + 1$</td>
<td>$\alpha^2 + \alpha$</td>
<td>$\alpha$</td>
<td>$\alpha^2 + 1$</td>
<td>$1$</td>
</tr>
<tr>
<td>$\alpha^2 + 1$</td>
<td>$1$</td>
<td>$\alpha^2$</td>
<td>$\alpha$</td>
<td>$\alpha^2 + \alpha + 1$</td>
<td>$\alpha + 1$</td>
<td>$\alpha^2 + \alpha$</td>
</tr>
<tr>
<td>$\alpha^2 + \alpha$</td>
<td>$\alpha^2 + \alpha + 1$</td>
<td>$1$</td>
<td>$\alpha^2 + 1$</td>
<td>$\alpha + 1$</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
</tr>
<tr>
<td>$\alpha^2 + \alpha + 1$</td>
<td>$\alpha^2 + 1$</td>
<td>$\alpha$</td>
<td>$1$</td>
<td>$\alpha^2 + \alpha$</td>
<td>$\alpha^2$</td>
<td>$\alpha + 1$</td>
</tr>
</tbody>
</table>

3.4.2 Facts

The turn for $\text{PSL}_2(8)$ has come; our calculations now will have to be done over the field of 8 elements $F_8$. This group, of order greater than $\text{PSL}_2(9)$ (we will explain why when studying the latter) has order

$$|\text{PSL}_2(8)| = \frac{1}{1}(8^3 - 8) = 504 = 2^3 \cdot 3^2 \cdot 7$$

consisting of 9 Sylow 2-subgroups, 28 Sylow 3-subgroups and 36 Sylow 7-subgroups. As always, since 3 and 7 are prime their correspondent Sylow subgroups will be cyclic, whence the Sylow 2-subgroups present a dihedral 2-group $D_8$ structure.

We know no matrix of order 8 exists, since that would mean the Sylow 2-subgroups form a cyclic group (they are all isomorphic, so all must be $D_8$); however, since there are 9, there must exist an element that cycles through each and every one of them (and, in fact, there is more than one). Choosing one of them,

$$\begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix}$$

we see it conjugates through every Sylow 2-subgroup (and we will call it $h$). That means, if $S$ is a Sylow 2-subgroup, then

$$\{S, \ hSh^{-1}, \ h^2Sh^{-2}, \ldots, \ h^8Sh^{-8}\}$$

are the 9 Sylow 2-subgroups.
3.5 Isomorphism $\text{PSL}_2(9) \cong A_6$

3.5.1 The field $F_9$

$F_9$, also called Galois Field of 9 elements, $GF(3^2)$ or simply $GF(9)$ is a field of order 9 generated by the quotient

$$
\mathbb{Z}_3[x] \bigg/ \langle x^2 = x + 1 \rangle
$$

Using the same method as in $F_4$, we construct $F_9$ as a quadratic extension of $\mathbb{Z}/3\mathbb{Z}$ by the roots of the polynomial $x^2 = x + 1$. Again, if $\alpha$ denotes one root, then $\alpha + 1$ is the other one. But now, $1 + 1 + 1 = 0$ and $\alpha^2 = \alpha + 1$ we obtain that its nine elements are $\{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$.

Presenting a multiplication table for $F_9$ would be pointless, since we will not study $\text{PSL}_2(9)$; for that reason, we jump to the sections that matter us most.

3.5.2 Facts

It comes the turn of studying (though not in depth) the group $\text{PSL}_2(9)$. Surprisingly, its order is 360, much less than $\text{PSL}_2(8)$, which is 504. This is a consequence of the formula for the order of $\text{PSL}_2(q)$, because $\text{PSL} = \text{SL}/\text{SZ}$, and the only square root of 1 in $F_8$ is 1, whence in $F_9 = F_3[x]/(x^2 + 1)$ we have 2, namely 1 and 2. (Note: $\text{SZ}$ is the center of $\text{SL}$, as explained in section 1.7.) Therefore the center $\text{SZ}$ of $F_9$ is only $\{(1, 0), (1, 1)\}$, while the center $\text{SZ}$ of $F_9$ has two elements, $\{(1, 0), (2, 0)\}$; this is the direct cause of this fact. We have seen before $\text{PSL}_2(4)$ and $\text{PSL}_2(5)$ have the same order, and that holds just for this same reason.

Finally, $|\text{PSL}_2(9)| = 360 = 2^3 \cdot 3^2 \cdot 5$, consisting of 36 Sylow 2-subgroups, 10 Sylow 3-subgroups and 45 Sylow 5-subgroups.

3.5.3 Isomorphism

**Proposition 3.5.1.** $\text{PSL}_2(9)$ is isomorphic to $A_6$

*Idea of the proof.* We want to construct an isomorphism

$$G = \text{PSL}_2(9) \rightarrow A_6$$

and to do that we consider a subgroup $H_1$ of index 6 (and order 60) and the action by $G$ on the six cosets in $H_1$, namely $g_1H_1, g_2H_1, \ldots, g_6H_1$. These 6 groups (which we will call $H_i$, and $\mathcal{H} = \{H_1, \ldots, H_6\}$) exist and each of them is isomorphic to $\text{PSL}_2(5) \cong \text{PSL}_2(4) \cong A_5$ (this can be seen by computing the subgroups of $G$ and observing that in fact they have the structure of alternating group. Another way is to notice that its order is 60 and use that $A_5$ is the unique simple group of order 60.\(^6\))

Now we have a homomorphism by the action on the left cosets

$$
\phi : G \rightarrow S_6
$$

$$g \mapsto gH
$$

---

\(^6\)See [1] (page 147, Proposition 23) for the proof of uniqueness.
and it can be seen that the image of \( \phi \) is inside \( A_5 \). Moreover, the permutation induced by \( g \) is not constant for, given an element \( h \in p_i \), \( \phi(h) \neq \text{id} \). That is to say, if \( h \) induces a permutation on \( \mathcal{H} \) of the form

\[
\phi(h) : (H_1 H_2 H_3 H_4 H_5 H_6) \mapsto (H_{\sigma(1)} H_{\sigma(2)} H_{\sigma(3)} H_{\sigma(4)} H_{\sigma(5)} H_{\sigma(6)})
\]

all we are saying is that \( \sigma \neq \text{id} \) when \( h \in H_i \) for some \( i \).

By the same reasoning as in the case of \( \text{PSL}_2(4) \) the first isomorphism theorem states that

\[
G/\ker(\phi) \cong A_6
\]

and, since \( \ker(\phi) \triangleleft G \) and \( \ker(\phi) \neq G \) it must happen that \( \ker(\phi) = \text{id} \), meaning that \( \phi \) is a isomorphism. 

\[\blackdiamondsuit\]
3.6 \textbf{PSL}_2(11)

3.6.1 Facts

Our latter group to study, the greatest simple non-abelian group of order less than 1000, also the greater studied here, is $PSL_2(11)$, the Projective Special Linear Group of $2 \times 2$ matrices over the field of eleven elements, $\mathbb{Z}/11\mathbb{Z}$.

Using the counting formula (now for the last time) we find that:

$$|PSL_2(11)| = \frac{1}{2}(11^3 - 11) = 660 = 2^2 \cdot 3 \cdot 5 \cdot 11$$

consisting of 55 Sylow 2-subgroups, 55 Sylow 3-subgroups, 66 Sylow 5-subgroups and 12 Sylow 11-subgroups.

The Sylow 3-subgroups, Sylow 5-subgroups and Sylow 11-subgroups are cyclic (since they are of prime order), while the Sylow 2-subgroups are all isomorphic to the Klein group $V_4$. 
Bibliography


[2] Why is PSL(2,7) isomorphic to GL(3,2)?, by Ed Scheinerman
   http://www.math.vt.edu/people/brown/doc/PSL(2,7)_GL(3,2).pdf

   http://library.msri.org/books/Book35/files/elkies.pdf