Generating Sequences of the Two Dimensional Special Projective Linear Group over Fields of Prime Order, PSL(2, p)

Benjamin Philip Nachman

Advisor: Keith Dennis

May 16, 2012

Abstract

As an infinite family of simple groups, the two dimensional special projective linear groups $\mathrm{PSL}(2, \mathrm{p})$ are interesting algebraic objects. While the groups are well known in the sense that their subgroup lattice structure is completely determined, properties of their generating sequences are still not entirely understood. With recent developments in this direction, one can begin to completely answer questions associated with the properties of generating sequences of $\mathrm{PSL}(2, \mathrm{p})$. The culmination of this discussion is in a conjecture for the size of irredundant generating sequences of the maximal length. A related notion to generating sequences is that of the replacement property - an attribute of groups that is analogous to the Steinitz Exchange Property for vector spaces. It will be shown that $\mathrm{PSL}(2, \mathrm{p})$ sometimes has this property, but does not have it in general.

Acknowledgements

First and foremost, I must thank my advisor Professor Keith Dennis for the countless discussions we have had in his office, in the library and over email. He has been my supporter and advocate since I took his linear algebra class my sophomore year. That class changed my perception of mathematics and got me hooked on learning more abstract algebra.

The success that I have been blessed with in the math department would not have been possible without several others who have been supporters outside of the classroom. I would like to thank Professor Ravi Ramakrishna for being a source of advice in the mathematics department beyond the classroom. After taking his class I was so excited about Galois Theory that I wrote up a ~ 100 page document containing the construction of the complex numbers and proof of their algebraic closure. He read through this document and offered feedback, much of which is incorporated in my writing of this document. Also, I am thankful for the support of my academic advisor, Professor Strichartz, who was been my longest advocate in the department. Finally, I would like to thank Professor Camil Muscalu. He has taught me to use all my senses in understanding the art which is mathematics.

I would also like to thank my other research advisors, Professors Jim Alexander and Itai Cohen, who have supported my work in mathematics even though at times it has taken me away from physics.

My parents and brothers have always supported me in all my endeavors. No finite amount of text could describe how much I am indebted to them. This thesis is a discussion about finite objects and so my infinite gratitude for my family must wait until I see them in person!

Contents

0.1 Introduction 1

1 Subgroup Structure of PSL(2, p) **2**
1.1 The 2D Projective Linear Group over the field of p elements: PSL(2, p) 3
1.1.1 Constructing PSL(2, p) in GAP 4
1.1.2 General Properties 5
1.1.3 Subgroups: Dickson's Theorem 6
1.1.4 Application: Computing the Maximal Subgroups 24

2 Irredundant Generating Sequences **25**
2.1 Generating Sequences 26
2.1.1 Categorizing Groups Based on Generating Sequences 27
2.2 Irredundant Generating Sequences of PSL(2, p) 28

3 The Replacement Property **32**
3.1 The Replacement Property 33

A GAP Scripts **39**
A.1 Applying Dickson's Theorem 40
A.2 Computing m(PSL(2, p)) 42
A.3 Converting Matrix Representations over $\mathbb{F}_p$ 44

B Data **45**
B.1 Replacement Property Computations 46

Bibliography **47**

0.1 Introduction

This document is organized into three chapters. The first chapter discusses the construction and structure of PSL(2, p). This includes a complete description of the lattice of subgroups via Dickson's Theorem. All the results in this first chapter are already well-known. Careful proofs are given of the relevant properties in order to build the necessary machinery for later discussions. The second chapter focuses on irredundant generating sequences for PSL(2, p). Specifically, the discussion is focused on the invariant m which is the maximal length of such sequences. For many primes, this length is already known but its value in general for all p is an open question. Finally, in the third chapter the replacement property is considered in the context of PSL(2, p). In some sense, the generating sequences of this group are not well behaved in general because it does not satisfy the replacement property for all primes. A proof of this statement is given in addition to showing that PSL(2, p) does not always fail the replacement property. These results are also new.

The background necessary for this thesis is an introduction to group theory. For example, the first part of *Abstract Algebra* by Dummit and Foote [6] would suffice.

In the process of researching, many computations have been made for specific cases. The sizes of the relevant groups are so large that the computations are unwieldy to do by hand. Therefore, it is useful to employ the algebraic computation language `GAP` [7]. Original source code will be shown in places. Familiarity with `GAP` is not necessary to understand the theorems in the thesis, but programming knowledge and with `GAP` in particular will help parse these scripts. These scripts are presented with many comments for those who are not fluent in this language.

Chapter 1

Subgroup Structure of $\mathrm{PSL}(2, \mathrm{p})$

1.1 The 2D Projective Linear Group over the field of p elements: $\mathrm{PSL}(2,\mathrm{p})$

There are at least two equivalent ways of constructing PSL(2, p). The first is more straightforward, but less geometric. Let V be a 2 dimensional vector space over the field of p elements. The General Linear Group, GL(V) = GL(2, p), is the set of invertible 2×2 matrices over p. This group is also the automorphism group of V. One then constructs the Special Linear Group SL(V) = SL(2, p) $\leq$ GL(2, p) as the set of elements in GL(2, p) which have determinant equal to 1. The Projective Linear Group is then defined as the quotient SL(V)/Z(SL(V)), where Z(·) is the center of the group. For example, let $p = 2$. Then, V has precisely four vectors:

$$V = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \tag{1.1}$$

Furthermore, there are 16 total 2×2 matrices. However, not all of these matrices are invertible. For a generic matrix of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, invertibility requires the following:

$$\mathrm{Det}\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = ad - bc \neq 0 \tag{1.2}$$

The ones which are not invertible have $ad = bc$. There are two possibilities for ad. In the first case, $ad = 1$ and then one needs $a = d = 1$ and also $b = c = 1$. In the second case, $ad = 0$. Then, there are nine possibilities: either a or d or both are zero and either c or d or both are zero. Therefore, GL(2, 2) has six elements:

$$\mathrm{GL(V)} = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \tag{1.3}$$

and since 1 is the only nonzero element, each of these matrices has determinant one and so GL(V) = SL(V). The next step is to compute Z(GL(V)). For example consider the following commutator:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.4}$$

but

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.5}$$

and so GL(V) is a non-commutative group of order six. Up to isomorphism, there is only one such group: S_3, the symmetric group on three letters. Since $\mathrm{Z}(\mathrm{S}_3)$ is trivial, it must be that $\mathrm{S}_3 \cong \mathrm{GL(V)} \cong \mathrm{PSL}(2, 2)$.

While the above discussion is an algebraic construction of PSL(2, p), there exists a more geometric description of this group in terms of the Projective Space of V [9]. The Projective Space P(V) is the set of one dimensional subspaces of V, i.e. the set of lines through the origin. Any such line can be parameterized by the equation $f(x) = mx$ with $m \in \mathbb{F}_p$ and is uniquely determined by m. Since there are p elements in $\mathbb{F}_p$, there are p lines determined this way. There is then one additional line which has infinite slope and is governed by the equation $x = 0$. Therefore, P(V) has $p + 1$ elements. Then, just as SL(V) acts naturally on V, PSL(V) acts naturally on P(V). Pick any $v \in V$. Let $[v]$ denote the set of $v \in V$ that are on the same line. In other words, define the equivalence relation $\sim$ by $v \sim w$ if $v = mw$ for $0 \neq m \in \mathbb{F}_p$. Then, $[v]$ is simply the equivalence class of v under $\sim$. For a linear transformation $T \in \mathrm{SL(V)}$, define $[T] \in \mathrm{PSL(V)}$ by $[T][v] = [Tv]$. The claim is that PSL(V) is the set of such (special) projective transformations, with the group operation of composition. In order to prove this, one will need a proposition:

Proposition 1. *For any $[T_1], [T_2]$ in the set of projective transformations, $[T_1] = [T_2]$ if and only if $T_1 = mT_2$ for some $0 \neq m \in \mathbb{F}_p$.*

Proof. First, suppose that $[T_1] = [T_2]$. Then, $[T_1][v] = [T_2][v]$ for all $v \in V$. By construction, this means that $[T_1 v] = [T_2 v]$ for all $v \in V$. Furthermore, note that $T_1 v = m(T_2 v)$ for all $v \in V$. Then, $(T_1 - mT_2)(v) = 0$. Since this is true for all $v \in V$, it must be that $T_1 - mT_2 = 0$, the zero transformation. Thus, $T_1 = mT_2$.

Conversely, suppose that $T_1 = mT_2$. Then, for all $[v] \in \mathrm{P(V)}$,

$$[T_1][v] = [mT_2][v] = [mT_2 v] = [T_2(mv)] = [T_2][mv] = [T_2][v] \tag{1.6}$$

and since this is true for all $[v] \in \mathrm{P(V)}$, it must be that $[T_1] = [T_2]$.

□

If π is the canonical map from SL(V) to PSL(V), define the map

$$\phi : \mathrm{PSL}(2, \mathrm{p}) \to \{\text{Projective Transformations}\}$$

as $g \mapsto [\pi^{-1} g]$. The symbol $\pi^{-1}(g)$ means the following: take any representative of the inverse image of g under the projection. With the above definition, the claim is that ϕ is an isomorphism. First, one needs to ensure that ϕ is well-defined. Take any $g \in \mathrm{PSL}(2, \mathrm{p})$ and consider two elements in the inverse image $\pi^{-1} g$. Such elements will be related by a central element of SL(V). The center of SL(V) is given by the below proposition:

Proposition 2. *The center of* GL(V) *is isomorphic to* $\mathbb{F}_p^*$ *and is precisely given by the set of scalar matrices,* mI *for some* $m \in \mathbb{F}_p^*$ *and* I *the* 2×2 *identity matrix.*

Then, two elements in $\pi^{-1} g$ are related by $T_1 = mT_2$ for some $m \in \mathbb{F}_p$. Two such elements give rise to the same projective transformation and so ϕ is well defined. It is not hard to show that ϕ is a homomorphism and is both injective and surjective.

Now, before going in to the general properties of $\mathrm{PSL}(2, \mathrm{p})$, another explicit construction for a particular p is given using this second definition of $\mathrm{PSL}(2, \mathrm{p})$. Let $p = 3$. This is slightly less trivial than $p = 2$ because now there are non-identity scalars to deal with. In this case, $|V| = 9$. There are five elements of P(V):

$$\mathrm{P(V)} = \left\{ \left[\begin{pmatrix} 0 \\ 0 \end{pmatrix} \right], \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \right], \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right], \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right], \left[\begin{pmatrix} 1 \\ 2 \end{pmatrix} \right] \right\} \tag{1.7}$$

For the field of three elements in dimension two, GL(V) acts transitively on V and since there are 4 nonzero elements of P(V), the set of all projective maps will be isomorphic to S_4, the symmetric group on 4 letters. There are 24 such transformations. All of these must have determinant 1 or 2 (i.e. nonzero) since they are invertible. By symmetry, half will have determinant 1 and so PSL(V) will have 12 elements. There is only one 12 element subgroup of S_4, namely A_4. Thus, $\mathrm{PSL}(2, 3) \cong \mathrm{A}_4$. Note that A_4 is also the quotient of S_4 by its center, in accordance with the first definition of $\mathrm{PSL}(2, \mathrm{p})$.

1.1.1 Constructing $\mathrm{PSL}(2, \mathrm{p})$ in GAP

In proving theorems, it is often necessary to make algebraic computations that are too complicated to do by hand. GAP is a computer language that is available for making such computations with a computer. Many common groups, such as $\mathrm{PSL}(2, \mathrm{p})$ are constructed from built-in libraries within GAP. However, groups constructed in this manner are represented as subgroups of the symmetric group S_n for a large enough n. For the purpose of the work presented in this thesis, it is useful to consider elements as matrices in $\mathrm{SL}(2, \mathrm{p})$ (of course this is not unique because of the quotient by the center). The second description of $\mathrm{PSL}(2, \mathrm{p})$ in the previous section allows one to make this connection. The first step is to construct the two dimensional special linear group. GAP stores this group as a set of matrices.

```
SLp:=SL(2,p);
```

Next, let $\mathrm{SL}(2, \mathrm{p})$ act on the set of vectors of the two dimensional vector space over $\mathbb{F}_p$. To do this, one first needs to generate the set of vectors. Beginning with a nonzero vector in this space, all the other

vectors are generated via the action of GL(2, p). GAP represents elements of $\mathbb{F}_p^*$ as Z(p)^n where Z(p) is the smallest generator of $\mathbb{F}_p$ that generates the cyclic multiplicative group. For example, Z(7) is 3 and Z(5) is 2. One can check this in GAP with the command PrimitiveRootMod(p). The nonzero vector is constructed by

```
v:=[1,0]*Z(p)^0;
```

Next, let GL(2, p) act on this vector to get the set of all other vectors. This is possible because this action is transitive. Since the projective space is defined as an action on lines and not on the set of all vectors, one can use the action 'OnLines' which actually will return the set of normalized vectors (and the initial vector is normalized).

```
V:=Orbit(GL(2,p),v,OnLines);
```

Now, one realizes PSL(2, p) as the action of SL(2, p) on V.

```
act:=ActionHomomorphism(SLp,orb,OnLines);
```

In other words, given an element of SL(2, p), act will map this element to the relevant permutation of the set of lines which is called V. Now, one needs a way of going between this representation of PSL(2, p)and the one that is constructed naturally in GAP. To do this, first take the image of act:

```
myPSL:=Image(act);
```

and then construct an isomorphism from it to the PSL(2, p) that is constructed in GAP:

```
iso:=IsomorphicSubgroups(myPSL,PSL(2,p));
```

Then, if one has an element x of PSL(2, p) in the permutation representation, the following command will return a matrix:

```
PreImagesRepresentative(act,ImagesRepresentative(iso[1],x));
```

The only further complication is that this matrix will have elements in $\mathbb{F}_p^* \cup \{0\}$ which is usually less useful than having elements in $\mathbb{F}_p$. The script in the Appendix A.3 converts between these two representations. For example:

```
decodeMat([[Z(3)^1,0*Z(3)],[Z(3)^2,Z(3)^9]],3);
```

returns the matrix $[[2, 0], [1, 2]]$.

1.1.2 General Properties

The special projective linear groups have many nice properties, most of which are not discussed here or even needed. For example, for $p > 3$, PSL(2, p) is a simple group. For all p, PSL(2, p) is a centerless group. This is not immediate, since the center of a the factor group by the center need not be centerless. The only general property that is discussed here is the order of PSL(2, p), which is needed later in describing its subgroups.

Proposition 3. *If $p > 2$, then* $|\mathrm{PSL}(2, \mathrm{p})| = (p + 1)p(p - 1)/2$

Proof. A standard fact from linear algebra is that a $n \times n$ matrix over a field F is invertible if and only if its rows form a basis of F^n. For a finite field F, $F \cong \mathbb{F}_p$. The proposition is then reduced to counting the number of possible bases over $\mathbb{F}_p^2$. Each vector is a 2-tuple of elements of the field. The first vector can be any nonzero element of the vector space. For a generic vector, there are p possibilities for the first component of the vector and p possibilities for the second. Thus, there are p^2 total vectors in the space. There are $p^2 - 1$ nonzero vectors. Now, one needs to figure out how many choices there are for the second vector in the basis. The only requirement for it to be linearly independent from the first (and thus to form a basis with the first pick) is for it not to be a multiple of the first. There are $p^2 - 1$ total vectors and there are $p - 1$ nonzero scalars to multiply the first vector by. Thus, there are $p^2 - 1 - (p - 1)$ possible vectors for the second choice in the basis. This means that

$$|\mathrm{GL}(2,\mathrm{p})| = (p^2-1)((p^2-1)-(p-1)) = (p-1)^2(p+1)(p+1-1) = (p-1)^2(p+1)p \tag{1.8}$$

The next step is to determine the size of $\mathrm{SL}(2,\mathrm{p})$. To do this, one needs to divide by $p-1$, which is the number of possible determinants of a matrix in $\mathrm{GL}(2,\mathrm{p})$, in order to isolate matrices with the same determinant $(+1)$. This means that

$$|\mathrm{SL}(2,\mathrm{p})| = (p-1)p(p+1) \tag{1.9}$$

If $p > 2$, then the number of scalar determinant one matrices is equal to 2 (if $p = 2$, the center is trivial). Therefore,

$$|\mathrm{PSL}(2,\mathrm{p})| = (p-1)p(p+1)/2 \tag{1.10}$$

□

1.1.3 Subgroups: Dickson's Theorem

The subgroup structure of $\mathrm{PSL}(2,\mathrm{p})$ is very well known. Most importantly for the purposes of this thesis is the collection of maximal subgroups. This was completely determined by American mathematician Leonard Dickson about a century ago [5]. First, his theorem is stated[1], then there is a brief discussion of the strategy for the proof.

Theorem 1 (Dickson)**.** *For $p > 5$, the maximal subgroups of $\mathrm{PSL}(2,\mathrm{p})$ are isomorphic to one of the following groups:*

1. $\mathbb{Z}_p \rtimes \mathbb{Z}_{(p-1)/2}$*, The non-abelian solvable group of order $p(p-1)/2$*
2. D_{p-1}*, the Dihedral Group of size $p-1$*
3. D_{p+1}
4. $\mathrm{A}_4, \mathrm{S}_4$ *or* A_5

Moreover, while subgroups of types $(1), (2)$ *and* (3) *always exist, a maximal subgroup isomorphic to S_4 exists if and only if $p \equiv \pm 1 \mod 8$, subgroups isomorphic to A_5 exist if and only if $p \equiv \pm 1 \mod 10$ and subgroups isomorphic to A_4 are maximal if and only if $p \equiv 3, 13, 27, 37 \mod 40$.*

To outline the proof, fix a prime p. Let F be an algebraically closed field of characteristic p. To begin, one finds the subgroups of a different group, $\mathrm{SL(V)}$ where V is a vector space of two dimensional matrices over the field F. Then, $\mathrm{SL}(2,\mathrm{p})$ is embedded in $\mathrm{SL(V)}$ to find the subgroups of $\mathrm{SL}(2,\mathrm{p})$. Next, subgroups of $\mathrm{PSL}(2,\mathrm{p})$ are constructed via the fourth isomorphism law. Finally, these results are put together to form the final version of Dickson's theorem.

To begin, here are some useful definitions. Let

$$d_\omega = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \qquad t_\lambda = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \qquad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{1.11}$$

for any $\omega \in F^*, \lambda \in F$. Soon, it will be shown that every element $x \in \mathrm{SL(V)}$ is conjugate to either d_ω or $\pm t_\lambda$. First, a few preliminary results are needed about d_ω, t_λ and w.

Lemma 1. *These special elements have the folloing multiplication rules:*

$$d_\omega d_{\omega'} = d_{\omega\omega'} \qquad\qquad t_\lambda t_\mu = t_{\lambda+\mu}$$

[1] We will follow the proof in Suzuki's book [13]. However, Suzuki presents the proof in a slightly different way than the approach given here. Furthermore, he leaves out many details, which are filled in throughout this thesis.

Proof. This is follows immediately from matrix multiplication. For example, take t_λ, t_μ. Then,

$$t_\lambda t_\mu = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \lambda + \mu & 1 \end{pmatrix} = t_{\lambda+\mu} \tag{1.12}$$

□

Lemma 2. *The center of* SL(V) *is* $\mathrm{Z}(\mathrm{SL(V)}) \cong \mathbb{Z}_2$.

Proof. The only matrices which commute with every other matrix are the scalar matrices. This reduces to finding which scalar matrices are in SL(V). Let $x \in \mathrm{Z}(\mathrm{SL(V)})$. Then

$$x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \tag{1.13}$$

but, by the construction of SL(V), the determinant of x must be 1 and so $\alpha^2 = 1$. Therefore, $\alpha = \pm 1$ and so the center has order 2. □

In fact, this is the unique element of order 2. To see this, let $x \in \mathrm{SL(V)}$ of order 2. Note that if

$$x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{1.14}$$

then

$$x^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \tag{1.15}$$

so if x has order two, these are equal. This means that $\gamma = \beta = 0$ and since the determinant is 1, $\alpha = \delta = \pm 1$. Now, the machinery is sufficient to return to looking at the conjugacy classes of SL(V).

Proposition 4. *Any element* $x \in \mathrm{SL(V)}$ *is conjugate to either* d_ω *or* $\pm t_\lambda$.

Proof. Let f be the characteristic equation of x. Since F is algebraically closed, f has at least one root in F. Let ω be such a root (and thus an eigenvalue). Let u_1 be the corresponding eigenvector so that $xu_1 = \omega u_1$. Let v be any vector that is linearly independent from u_1 (many such vectors exist - only one is required which is not a multiple of u_1). Then, in the basis $\{v, u_1\}$

$$x = \begin{pmatrix} xv & xu_1 \end{pmatrix} = \begin{pmatrix} \delta & 0 \\ \gamma & \omega \end{pmatrix} \tag{1.16}$$

It is not clear that such a change of basis can be accomplished with an element of SL(V). Let $u_2 = qv$ for some $q \in F^*$. Then, u_1, u_2 will still be a basis. In this new basis,

$$x = \begin{pmatrix} qxv & xu_1 \end{pmatrix} = \begin{pmatrix} q\delta & 0 \\ q\gamma & \omega \end{pmatrix} \tag{1.17}$$

which has determinant $q(\delta\omega - \gamma)$. Since this determinant is nonzero, there exists $q \in F^*$ such that this determinant is one. Thus, the change of basis can indeed be accomplished within SL(V) conjugation. Now, absorb q into δ, γ so that $q = 1$. Since the determinant of x must be 1, $\omega = \delta^{-1}$. Now, there are two cases. First case: $\omega = \delta$. Then, $\omega^2 = 1$ and so $\omega = \pm 1$. Such an x is therefore clearly conjugate to $\pm t_\lambda$. Second case: $\omega \neq \delta$. From linear algebra one can concluded that the eigenvector corresponding to the eigenvalue δ must be linearly independent from u_1. Let it be u_2. Thus, $\{u_2, u_1\}$ from a basis and in that basis, x has the form

$$x = \begin{pmatrix} xu_2 & xu_1 \end{pmatrix} = \begin{pmatrix} \delta & 0 \\ 0 & \omega \end{pmatrix} \tag{1.18}$$

And by the above discussion, changing bases to arrive at this form can be done within SL(V) conjugation. Thus, x is conjugate to d_ω.

□

Now, since all the conjugacy classes of all the elements of SL(V) have been determined, one can classify the centralizers of all the elements $x \in \mathrm{SL(V)}$. This is because if $x = yd_\omega y^{-1}$, then $\mathrm{C}_{\mathrm{SL(V)}}(x) = y\mathrm{C}_{\mathrm{SL(V)}}y^{-1}$ (and likewise if x is conjugate to $\pm t_\lambda$). First, a few more definitions are needed.

$$T \equiv \langle\{t_\lambda\}\rangle \qquad D \equiv \langle\{d_\omega\}\rangle \qquad Z \equiv \mathrm{Z(SL(V))} \tag{1.19}$$

Then,

Proposition 5. *The centralizers of all elements of* SL(V) *can be classified as one of the following:*

$$\mathrm{C}_{\mathrm{SL(V)}}(t_\lambda) = T \times Z \cong T \times \mathbb{Z}_2 \qquad \mathrm{C}_{\mathrm{SL(V)}}(d_\omega) = D \tag{1.20}$$

for $\omega \neq \pm 1$ *and* $\lambda \neq 0$.

Proof. Take any element in $y \in \mathrm{C}_{\mathrm{SL(V)}}(\mathrm{t}_\lambda)$. Generically write

$$y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1.21}$$

Then,

$$\begin{pmatrix} a & b \\ \lambda a + c & \lambda b + d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} \lambda b + a & b \\ \lambda d + c & d \end{pmatrix} \tag{1.22}$$

Therefore, for $\lambda \neq 0$, $b = 0$ and $a = d$, so

$$y = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \tag{1.23}$$

but, since $y \in \mathrm{SL(V)}$, it must be that $a^2 = 1$ and so $a = \pm 1$. If $a = 1$, then $y \in T$. If $a = -1$, then y is a product of the nontrivial element of order 2 and an element of T. Therefore, $\mathrm{C}_{\mathrm{SL(V)}}(t_\lambda) \subseteq TZ = T \times Z$. Since elements of Z commute with any element of SL(V), it remains to show that elements of T commute with each other. This is clear from our preliminary results on these matrices. Therefore, $T \times Z \subseteq \mathrm{C}_{\mathrm{SL(V)}}(t_\lambda)$ and so they are equal. Now, one can make a similar computation for $d_\omega \neq \pm 1$. Take any element $y \in \mathrm{C}_{\mathrm{SL(V)}}(d_\omega)$ and write it with the generic form as before. Then,

$$\begin{pmatrix} a\omega & b\omega^{-1} \\ c\omega & d\omega^{-1} \end{pmatrix} = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} = \begin{pmatrix} a\omega & b\omega \\ c\omega^{-1} & d\omega^{-1} \end{pmatrix} \tag{1.24}$$

Therefore, since $x \neq x^{-1}$, it must be that $c = 0$ and $b = 0$. Therefore, $y \in D$ and so $\mathrm{C}_{\mathrm{SL(V)}}(d_\omega) \subseteq D$. Now, all that is left to show is that two elements in D commute with each other. But, this is clear because multiplying elements in D is the same as multiplying the upper left and lower right components separately.

□

This gives the following:

Corollary 1. *The centralizer of an element* $x \in \mathrm{SL(V)}$ *is abelian unless* $x \in Z$.

Proof. The previous proposition shows that the centrealizer of x is either $T \times Z$ or D if x is not in the center. In addition, it is clear that elements of T commute with each other and elements of D commute with each other. Therefore, $T \times Z$ and D, and thus the centralizers of all non-central elements, are abelian. □

Now, one can begin looking at the subgroups of SL(V). Pick any $G \leq \mathrm{SL(V)}$. First, suppose that $Z \not\subseteq G$. Since the intersection of these two groups must then be trivial,

$$|GZ| = |G||Z|/|G \cap Z| = |G||Z| = 2|G| \tag{1.25}$$

Therefore, since the index of G in GZ is 2, $G \trianglelefteq GZ$. Since $Z \trianglelefteq \mathrm{SL(V)}$, $GZ \cong G \times Z$. Thus, the structure of G is uniquely determined by GZ in the sense that one can look only at subgroups which contain Z and then project to the quotient to recover all subgroups. Therefore, without loss of generality, in the following discussion, only subgroups which contain Z are considered. Here are a few preliminary results:

Proposition 6. *Let $G \leq \mathrm{SL(V)}$ with $Z \subseteq G$. Let M be the set of all maximal abelian subgroups of G. Then, if $x \in G - Z$, $\mathrm{C}_G(x) \in M$.*

Proof. From the above Corollary 1, $x \notin Z$ implies that $\mathrm{C}_{\mathrm{SL(V)}}(x)$ is abelian. Therefore, $\mathrm{C}_G(x) = G \cap \mathrm{C}_{\mathrm{SL(V)}}(x)$ is abelian as well. Suppose that a maximal abelian subgroup H of G contained $\mathrm{C}_{\mathrm{SL(V)}}(x)$. Then, all the elements of H commute with x as well so $H = \mathrm{C}_{\mathrm{SL(V)}}(x)$. □

Corollary 2. *For any two distinct $A, B \in M$, $A \cap B = Z$*

Proof. Take $x \in A \cap B$. Then, $\mathrm{C}_G(x)$ contains both A and B, since they are abelian and so commute with everything inside themselves, namely x. But, A and B are maximal abelian subgroups of G, so $\mathrm{C}_G(x)$ cannot be abelian. But, the contrapositive of the previous proposition implies that $x \in Z$ and so $A \cap B \subseteq Z$. It is also clear that any $H \in M$ must contain Z, otherwise, one could form a larger abelian subgroup out of Z and H. Therefore, $A \cap B = Z$. □

Before diving into the next proposition, one needs the following lemma:

Lemma 3. *Let $x \in \mathrm{SL(V)}$ of finite order n. Then x is conjugate to $\pm t_\lambda$ ($\lambda \neq 0$) if and only if $p|n$ (in which case the order of x is either p or $2p$).*

Proof. Take any $t_\lambda \in T$. Then, $t_\lambda^p = t_{p\lambda} = t_0 = 1$, since elements in the matrices are in a field with characteristic p. If one takes $-t_\lambda$, then $-t_\lambda^p = -t_{p\lambda} = -1$ and so $(-t_\lambda)^{2p} = 1$. Since the order of $\pm t_\lambda$ must divide p or $2p$, it must be that these are in fact the orders. Therefore, since conjugation preserves order, if x is conjugate to $\pm t_\lambda$, it will have order p or $2p$ and p divides both of these.

Now for the converse. By Proposition 4, x is conjugate to d_ω or $\pm t_\lambda$. Suppose that x is conjugate to d_ω. Then, $(d_\omega)^n = d_{\omega^n} = 1$. This means that $\omega^n = 1$ and since n is the order, $\omega^m \neq 1$ for $m < n$ (i.e. ω is a primitive n^{th} root of unity). Suppose that $p|n$. Then, $n = mp^q$ for some m relatively prime to p. Since ω is a primitive n^{th} root of unity, ω is a solution to the equation

$$X^n - 1 = 0 \tag{1.26}$$

However, this can be rewritten as

$$0 = X^{mp^q} - 1 = (X^m - 1)^{p^q} \tag{1.27}$$

since p is zero in the field (and the binomial expansion formula has been used). Therefore, ω is also a solution to $X^m - 1 = 0$. But, ω was primitive, a contradiction. Therefore, x cannot be conjugate to d_ω and therefore must be conjugate to $\pm t_\lambda$.

□

Next is a proposition which describes the set M of maximal abelian subgroups of $G \leq \mathrm{SL(V)}$ in more detail.

Proposition 7. *Let P be a Sylow p-subgroup of G. Then, any $A \in M$ is either cyclic with order relatively prime to p or is of the form $P \times Z$.*

Proof. Take any element $x \in G$. Then, $\langle Z, x \rangle$ is abelian and properly contains x. Therefore, if $Z \neq G$, then any member $A \in M$ must contain an element $x \notin Z$ - otherwise, a larger abelian subgroup of G can be formed by adding in a non-central element. One can always pick such an element so that $A = \mathrm{C}_G(x)$. This is because $\mathrm{C}_G(x) \in M$ and $\mathrm{C}_G(x) \cap A = Z$ (if they are different), but they both contain $x \notin Z$, a contradiction. By Proposition 4, x is conjugate to d_ω for $\omega \neq \pm 1$ or $\pm t_\lambda$ for $\lambda \neq 0$.

If the former is true, then $\mathrm{C}_{\mathrm{SL(V)}}(x)$ is conjugate to D. But, $D \cong F^*$, so $\mathrm{C}_G(x) = A$ is isomorphic to a finite subgroup H of F^*. But, all such groups are cyclic. In addition, H must have subgroups of all orders dividing $|H|$. Suppose p divided the order of H. Then, there will be nontrivial elements in

A which are conjugate to $\pm t_\lambda$ by the lemma. However, no such elements exist in D, a contradiction. Therefore, $|H|$ is relatively prime to p.

Now, suppose that x is conjugate to $\pm t_\lambda$. Then, $\mathrm{C}_G(x)$ is isomorphic to $T \times Z$. It is easy to see that T is isomorphic to the additive group F^+. Therefore, T contains at least one nontrivial finite subgroup. But any such subgroup must have order a power of p since the characteristic of F is p. Therefore, $A = Q \times Z$ with Q an elementary abelian p group. In fact, Q is a Sylow p subgroup of G. First of all, Q is contained in some Sylow p-subgroup of G, call it P. The claim is that the center of P is not trivial. To see this, consider the class equation:

$$|P| = |\mathrm{Z}(P)| + \sum |P : C_P(g_i)| \tag{1.28}$$

for g_i the representatives of the distinct conjugacy classes of elements in P. If P is not abelian the sum is nonzero. All of the indices in the sum must be powers of p and p divides the order of P and so p divides the order of $\mathrm{Z}(P)$ as well. Let $z \in \mathrm{Z}(P)$ be nontrivial. Then, z commutes with everything in P, so P is contained in the centralizer of z in G, i.e.

$$A \cong Q \times Z \subseteq P \times Z \subseteq C_G(z) \tag{1.29}$$

but, clearly, $z \notin Z$ (since it has order p), so $\mathrm{C}_{\mathrm{SL(V)}}(z)$ is abelian and therefore $\mathrm{C}_G(z)$ is also abelian. Thus, $\mathrm{C}_G(z) \in M$. It is maximal because if it were properly contained in an abelian subgroup of G, there would be more elements which commuted with z. This implies that $A = \mathrm{C}_G(z)$ and so $Q \times Z = P \times Z$ as desired. □

The description of M is continued in what follows:

Proposition 8. *For $A \in M$ and $|A|$ relatively prime to p, then $|\mathrm{N}_G(A) : A| \leq 2$.*

Proof. By the previous proposition, Prop 7, A is cyclic and a generator of A is conjugate to d_ω ($\omega \neq \pm 1$). Since $|\mathrm{N}_G(A) : A|$ is invariant under conjugation of A, one can consider d_ω to be a generator of A. Take any element in the normalizer of A in SL(V) and conjugate d_ω:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad\omega - bc\omega^{-1} & ab(\omega^{-1} - \omega) \\ cd(\omega - \omega^{-1}) & da\omega^{-1} - cb\omega \end{pmatrix} \tag{1.30}$$

For this to be in the normalizer, it is required that either $a = 0$ or $b = 0$ and either $c = 0$ or $d = 0$ since A is a subgroup of D. It cannot be that $a = 0$ and $c = 0$ or $b = 0$ and $d = 0$, because then the matrix would not be invertible. Therefore, either $a = 0$ and $d = 0$ or $b = 0$ and $c = 0$. If $b = 0$ and $c = 0$, then, the matrix would be an element of D. If $a = 0$ and $d = 0$, then it is required that $-bc = 1$, or that $b = \pm 1$ and $c = \mp 1$, so the matrix is $\pm w$. Therefore, $N_{SL(V)}(A) \subseteq \langle D, w \rangle$ and inclusion the other way is clear.

Now, consider the former case in which $b = c = 0$. One needs to know what elements in G have this form. Suppose that there is an element in G with this structure which is not in A, call it d_Ω. Then, $\langle A, d_\Omega \rangle$ will be abelian because d_Ω and d_ω commute. This cannot be since A is a maximal abelian subgroup of G. Thus, $\mathrm{N}_G(A) \subseteq \langle A, w \rangle$.

Therefore, there are only two possibilities. If $w \in A$, then the order of the normalizer is twice the size of A. Otherwise, it is the same size as A. In the case that $w \in A$, note that

$$w^{-1} d_\omega w = d_\omega^{-1} \tag{1.31}$$

□

Next is a counting argument. As before, take G such that $Z \leq G$. Define g such that $|G| = 2g$. Let Q be a Sylow p-subgroup of G and let $|Q| = q$ and $|\mathrm{N}_G(Q) : Q| = 2k$. Note that one can write this because for $p > 2$, Q does not contain Z as $|Q|$ is relatively prime to 2 but clearly, $Z \subseteq \mathrm{N}_G(Q)$ as $Z \leq G$ and Z normalizes Q. Let M be the set of maximal abelian subgroups of G. The work above shows that M

has two kinds of elements: subgroups conjugate to $Q \times Z$ (conjugate because all Sylow p subgroups are conjugate) or a cyclic subgroup which has order relatively prime to p. Furthermore, for the second type of subgroup,

$$|\mathrm{N}_G(A) : A| \leq 2 \tag{1.32}$$

Let $\{C_i\}$ be the set of conjugacy classes of elements of M of order relatively prime to p. Order them so that for a representative A_i of C_i, $\mathrm{N}_G(A_i) = A_i$ for $i \leq s$ and $|\mathrm{N}_G(A_j) : A_j| = 2$ for $s < j \leq s + t$. Finally, it is clear that $Z \in A_i$, so let $|A_i| = 2g_i$ for $i = 1, ..., s + t$. First of all, note that every element $x \in G$ is contained in $C_G(x)$, which is an element of M, so every element of x is contained in some element of M. The only elements in common between two distinct subgroups of M are in the center. Consider some fixed A_i. This group has $2g_i - 2$ non-central elements. There are $|G : \mathrm{N}_G(A_i)|$ conjugates of A_i, which is $2g/(2g_i\epsilon)$ where $\epsilon = 1$ for $i \leq s$ and 2 otherwise. Therefore, the number of non-central elements that a conjugacy class C_i contains is

$$(2g_i - 2) \times \frac{2g}{2g_i\epsilon} = \frac{2g}{g_i\epsilon}(g_i - 1) \tag{1.33}$$

Next, consider the conjugacy class of $Q \times Z$. Any conjugate will have $2q - 2$ non-central elements. There are $2g/(2qk) = g/qk$ such conjugates. Since there are $2g-2$ total non-central elements in G, the following equation holds:

$$2(g - 1) = \frac{2g}{qk}(q - 1) + 2g \sum_{i=1}^{t} \frac{g_i - 1}{g_i\epsilon} \tag{1.34}$$

this can be rewritten as

$$1 = \frac{1}{g} + \frac{q - 1}{qk} + \sum_{i=1}^{s} \frac{g_i - 1}{g_i} + \sum_{i=s+1}^{s+t} \frac{g_i - 1}{2g_i} \tag{1.35}$$

Since each g_i is an integer greater than 1,

$$\frac{g_i - 1}{g_i} \geq \frac{1}{2} \tag{1.36}$$

Furthermore, since q is either 1 or a power of p the equation implies that

$$1 > \frac{s}{2} + \frac{t}{4} \tag{1.37}$$

Therefore, there are 6 possible cases for G:

Case	s	t
1	1	0
2	1	1
3	0	0
4	0	1
5	0	2
6	0	3

This will allow for the classification of the subgroups of SL(V), considering one case at a time[2].

Proposition 9 (Case 1)**.** *$Q \neq G$ and G is an elementary abelian normal subgroup of G (and thus is unique). The factor group G/Q is a cyclic group whose order is relatively prime to p.*

[2]Let this be a disclaimer that in the subsequent discussion, it is assumed, but perhaps not always stated, that $p > 2$. Furthermore, some of the subsequent work only holds if p is not one of the small primes 3 or 5. Since this thesis is concerned with the behavior of PSL(2, p) for all primes, these cases are not isolated and considered separately.

Proof. Eq. 1.35 becomes

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{g_1} \tag{1.38}$$

which is

$$\frac{1}{g} + \frac{1}{k} = \frac{1}{qk} + \frac{1}{g_1} \tag{1.39}$$

By construction $q > 1$. The claim is that this implies $k > 1$. To see this suppose that instead $k = 1$. Then,

$$\frac{1}{q} = \frac{1}{g} - \frac{1}{g_1} + 1 \tag{1.40}$$

It cannot be that $g = g_1$ since then $q = 1$. Therefore, $\frac{1}{g} - \frac{1}{g_1} < 0$. Note that

$$\left|\frac{1}{g} - \frac{1}{g_1}\right| < \frac{1}{g_1} - \frac{1}{g_1 + 1} = \frac{1}{g_1(g_1+1)} \leq \frac{1}{2} \tag{1.41}$$

and so the right side of Eq. 1.40 is strictly bigger than $1/2$. Therefore, q cannot be an integer if $q > 1$. This contradiction leads to the conclusion that $k > 1$. More work is now required to see why this is important.

In the proof of Prop. 7, it was shown that the maximal abelian groups of G which have order not relativity prime to p are isomorphic to $R \times Z$, where R is a subgroup of T and is also a Sylow-P subgroup. Therefore, all Sylow-P subgroups are conjugate to subgroups of T. Since conjugation will preserve the lattice structure of subgroups, without loss of generality assume that Q is a subgroup of T. The centralizer of t_λ has already been computed in SL(V), but now consider the normalizer. Take any element in $y \in \mathrm{N}_{\mathrm{SL(V)}}(t_\lambda)$. Generically write

$$y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1.42}$$

Then,

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad - ba\lambda - bc & -\lambda b^2 \\ \lambda a^2 & -bc + ba\lambda + ad \end{pmatrix} \tag{1.43}$$

for y to be in the normalizer, one needs $b = 0$ and $ad = 1$. Therefore,

$$y = \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} = t_c d_a \tag{1.44}$$

Thus, $\mathrm{N}_{\mathrm{SL(V)}}(t_\lambda) \subseteq TD$. The reverse inclusion is clear and so $\mathrm{N}_{\mathrm{SL(V)}}(t_\lambda) = TD$. Therefore, $\mathrm{N}_G(Q) \subseteq TD$. In fact, it is clear from the form of T, D that all such elements normalizes Q and so $\mathrm{N}_G(Q) = TD \cap G$. Furthermore, in the proof of Prop. 7, it was shown that the maximal abelian subgroups which contains Q are of the form $Q \times Z$ and so all elements $t \in G \cap T$ must be in Q. Thus, $T \cap \mathrm{N}_G(Q) = Q$. By the second isomorphism theorem, $N(Q)/Q$ is isomorphic to a (finite) subgroup of $TD/T \cong D \cong F^*$. This means that $N(Q)/Q$ is cyclic. Additionally, the order must be relatively prime to p since F^* is composed of all the invertible elements in F. Let x be a generator of this cyclic quotient (and so the order of x is relatively prime to p) such that K is a subgroup generated by a lift of x to $\mathrm{N}_G(Q)$ with $\mathrm{N}_G(Q) = QK$ and $Q \cap K$ trivial.

Now, the claim is that $K \in M$, i.e. is a maximal abelian subgroup of G. To begin, note that $|K| = 2k > 2$. Let $K \leq A \in M$. This is possible since K is cyclic (and thus abelian) and so is contained in a maximal

abelian subgroup. Since K is cyclic of order relatively prime to p, by Prop. 7, A will also be cyclic and have order relatively prime to p. Now, some geometry is needed to complete the proof.

Let P(V) be the projective line of V. One needs to characterize the fixed points of P(V) under the action of SL(V). Take any $x \in \mathrm{SL(V)}$. Suppose that x has two fixed points $P, Q \in \mathrm{SL(V)}$. Let $u, v \in V$ correspond to P, Q, i.e. $[u] = P, [v] = Q$ under the equivalence relation defined in the earlier discussion of projective geometry. Since x fixes $[u]$, it must be that $xu = mu$ for some $m \in F^*$. Likewise, $xv = nv$ for some $n \in F^*$. Since n, m are eigenvalues of x and x has determinant 1, it must be that $nm = 1$ and so it is possible to write $n = m^{-1}$. It is thus clear that x could not have any more fixed points, since then there would be three distinct eigenvalues of x, which is not possible. Furthermore, d_ω will have exactly two fixed points because it has two distinct eigenvalues so long as $\omega \neq \pm 1$.

Next, consider the fixed points of T. In a given fixed basis (say u, v) one knows that the elements of T fix v since $x_{12} = 0$ and $x_{22} = 1$. Thus, there is a point $Y \in \mathrm{P(V)}$ which is fixed by all of T. It is also clear that in the diagonal form, elements of D also fix Y. Therefore, TD is contained in the stabilizer of P. Now, take any element x in the stabilizer of $[v]$. Such an element sends v to ωv for some $\omega \neq 0$. Therefore, one can write (in the u, v basis)

$$x = \begin{pmatrix} x_{11} & 0 \\ x_{21} & \omega \end{pmatrix} \tag{1.45}$$

but since $x \in \mathrm{SL(V)}$, $x_{11} = \omega^{-1}$. Therefore,

$$x = \begin{pmatrix} \omega^{-1} & 0 \\ x_{21} & \omega \end{pmatrix} = d_{\omega^{-1}} t_{x_{21}} \tag{1.46}$$

and so $x \in TD$ so the stabilizer of $[v]$ is TD.

Now, back to Case 1. A generator of A is conjugate to d_ω for $\omega \neq \pm 1$. Therefore, such a generator fixes two points P_1, P_2 in P(V). By the same reason, a generator x of K also has two fixed points - in fact they must be the same two fixed points. Every element of T has a common fixed point, call it P. The stabilizer of P is TD. Since $K \subseteq TD$, K must fix P. Thus, one of P_1, P_2 is P. Therefore, since a generator of A fixes P_1, P_2, it fixes P and so is in the stabilizer of P. This gives

$$A \subseteq \mathrm{Stab}(P) \cap G = TD \cap G = \mathrm{N}_G(Q) = QK \tag{1.47}$$

This means

$$A = QK \cap A = (Q \cap A)K = K \tag{1.48}$$

and so K belongs to M. There is only one element in M for Case 1, so $k = g_1$. Therefore, the equation the proof started with gives $g = qk$ and so $G = \mathrm{N}_G(Q)$.

□

Proposition 10 (Case 2)**.** *The order of $|G|$ is relatively prime to p and G is either the group of order $4n$ defined by the presentation*

$$\langle x, y | x^n = y^2, y^{-1}xy = x^{-1} \rangle \tag{1.49}$$

where n is odd, or $G \cong \mathrm{SL}(2, 3)$.

Proof. Eq. 1.35 becomes

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{g_1} + \frac{g_2 - 1}{2g_2} \tag{1.50}$$

which is

$$\frac{1}{g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2} \tag{1.51}$$

Suppose that $q > 1$ (i.e. there is a nontrivial Sylow-p subgroup). Then, $(q-1)/qk \geq 1/qk \geq 1/2k$. Therefore,

$$\frac{1}{2g_2} - \frac{q-1}{qk} = \frac{1}{g} + \frac{1}{2} - \frac{1}{g_1} \tag{1.52}$$

becomes

$$\frac{1}{2g_2} - \frac{1}{2k} \geq \frac{1}{2g_2} - \frac{q-1}{qk} = \frac{1}{g} + \frac{1}{2} - \frac{1}{g_1} > \frac{1}{2} - \frac{1}{g_1} \geq 0 \tag{1.53}$$

where the last inequality is because A_1 contains the center and cannot be the center and so $g_1 > 1$. It cannot be the center because then it would not be maximal abelian (since one could always add one more element and it would still be abelian). Therefore, $k > g_2$. Most notably, this means that $k > 1$ and so by the same logic in Case 1, k must be equal to g_i for some i. Since $k \neq g_2$, it must be that $k = g_1$. However, this means that the above inequality is

$$\frac{1}{2g_2} + \frac{1}{2g_1} > \frac{1}{2} \tag{1.54}$$

but, $g_1, g_2 > 1$ (they cannot be the center) and so this is a contradiction. Therefore, $q = 1$. Thus, the order of G is relatively prime to p (otherwise, it would have a nontrivial Sylow-p subgroup). Furthermore, Eq. 1.50 becomes

$$1 = \frac{1}{g} + \frac{g_1 - 1}{g_1} + \frac{g_2 - 1}{2g_2} \tag{1.55}$$

which means that

$$\frac{1}{g_1} + \frac{1}{2g_2} = \frac{1}{2} + \frac{1}{g} \tag{1.56}$$

or

$$\frac{1}{g_1} + \frac{1}{2g_2} > \frac{1}{2} \implies \frac{1}{g_1} > \frac{1}{4} \tag{1.57}$$

This means that $g_1 = 2$ or $g_1 = 3$. Consider each of these cases separately. First, suppose that $g_1 = 2$. Then, Eq. 1.50 becomes

$$g = 2g_2 \tag{1.58}$$

Since $|\mathrm{N}_G(A_2) : A_2| = 2$, it must be that $G = \mathrm{N}_G(A_2)$. The A_i are cyclic, so let x be a generator of A_2 and y a generator of A_1. By construction, $\mathrm{N}_G(A_1) = A_1$. The claim is that this means A_1 is a Sylow-2 subgroup of G. The size $|A_1| = 4$, so it is a 2 group. There is a standard corollary[3] to Sylow's Theorems which says that if P is a p-subgroup of G and if P is a Sylow-p subgroup of $\mathrm{N}_G(P)$, then P is a Sylow-p subgroup of G. Since $\mathrm{N}_G(A_1) = A_1$, so A_1 is a Sylow-2 subgroup of $\mathrm{N}_G(A_1)$ and so is a Sylow-2 subgroup of G. Therefore, since the intersection of A_1 and A_2 is Z, it must be that A_2/Z is odd, otherwise A_2 would contain a Sylow-2 subgroup, conjugate to A_1. Therefore, if $|A_2| = 2n$, then n is odd.

[3] For example, see p. 98 in [13].

Recall from the proof of Prop. 8 that $|\mathrm{N}_G(A_2) : A_2| = 2$ means that A_2 is conjugate to a subgroup of $\langle D, w\rangle$. Without loss of generality, suppose that $G = \langle A_2, w\rangle$. Then, there is a subgroup of G which is $\langle w\rangle$ and having order 4 must be conjugate to A_1 (as it is a Sylow-2 subgroup). Therefore, one can let $y = w$. In this case, the observation at the end of the proof of Prop. 8 says that $y^{-1}xy = x^{-1}$. Furthermore, $x^{2n} = y^4 = e$, the identity since w has order 4 and x is a generator of a cyclic group of order $2n$. In fact, $x^n = y^2$, since both of these elements have order 2 and are not the identity and thus are in Z, which has only one such element of this kind. It is routine to show that these two relations uniquely define a finite group of order $4n$ [13].

Now, suppose that $g_1 = 3$. Then, Eq. 1.50 becomes

$$g_2 = \frac{3g}{6+g} = 3 - \frac{18}{6+x} \tag{1.59}$$

for g_2 to be an integer, one needs 18 to be a multiple of $6+g$. Since $g > 1$, there is only one such solution, which is $g = 12$. This then gives $g_2 = 2$. There are only 15 groups of order 24 and it is possible to uniquely determine which one is G. First of all, G has a cyclic self normalizing subgroup of order six and a cyclic subgroup of order four, which is normalized by a subgroup of order eight. By the same reason as in the previous case, from the proof of Prop. 8, $|\mathrm{N}_G(A_2) : A_2| = 2$ means that $N_G(A_2)$ is conjugate to $\langle A_2, w\rangle$. Since w conjugates elements of A_2 to their inverse, for x a generator of A_2, there exists an element y in the normalizer of A_2 such that $yxy^{-1} = x^{-1}$. Therefore, $N_G(A_2)$ is a group of order 8 with elements x and y such that $yxy^{-1} = x^{-1}$. In addition, $x^2 = y^2$, since both of these elements have order 2 and so are in Z, which has only one such element. Therefore, $\mathrm{N}_G(A_2)$ is isomorphic to Q_8, the quaternion group [7]. It is straightforward to show that $G \cong \mathrm{SL}(2,3)$ [13]. Note that this means that $G/Z \cong A_4$. □

Proposition 11 (Case 3)**.** *$G = Q \times Z$.*

Proof. If $s = t = 0$, then the only maximal abelian subgroups of G are the ones conjugate to $Q \times Z$. Take any element $g \in G$ such that the order of G is relatively prime to p. Consider $\mathrm{C}_G(g)$. This is a maximal abelian subgroup. Since the only maximal abelian subgroups are conjugate to $Q \times Z$, it must be that $g \in Z$. Therefore, all non-central elements in G are a power of the prime p and thus are contained in a Sylow p subgroup of G. Therefore, $G = Q \times Z$. □

Proposition 12 (Case 4)**.** *This can only happen if $p = 2$ or 3. If $p = 3$, $G \cong \mathrm{SL}(2,3)$.*

Proof. Eq. 1.35 becomes

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1} \tag{1.60}$$

or

$$\frac{1}{2} = \frac{1}{g} + \frac{q-1}{qk} - \frac{1}{2g_1} \tag{1.61}$$

Also, $g \geq 2g_1$ since $A_1 \leq \mathrm{N}_G(A_1) \leq G$ and $|\mathrm{N}_G(A_1) : A_1| = 2$. Therefore,

$$\frac{q-1}{qk} = \frac{1}{2} - \frac{1}{g} + \frac{1}{2g_1} \geq \frac{1}{2} \tag{1.62}$$

This means $q > 1$. Since $(q-1)/q < 1$, it cannot be that $k \geq 2$ and so $k = 1$. Then, Eq. 1.35 becomes

$$\frac{1}{2} + \frac{1}{g} = \frac{1}{q} + \frac{1}{2g_1} \tag{1.63}$$

i.e.

$$\frac{1}{q} + \frac{1}{2g_1} > \frac{1}{2} \tag{1.64}$$

As in Case 2, this means $q = 2$ or $q = 3$. In the former case, $p = 2$, which is already excluded. In the later case, $p = 3$. Since $\mathrm{PSL}(2, 3) \cong \mathrm{A}_4$, no further details are necesary.

□

Proposition 13 (Case 5)**.** *If $|Q| = 3$, then $G \cong \mathrm{S}_5$. Otherwise, $g = q(q^2 - 1)/d$ (d=1 or d=2).*

Proof. Eq. 1.35 becomes

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1} + \frac{g_2 - 1}{2g_2} \tag{1.65}$$

or

$$\frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk} \tag{1.66}$$

If $q = 1$, then (suppose without loss of generality that $g_1 \geq g_2$)

$$\frac{1}{g_1} \leq \frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} \tag{1.67}$$

which means $g = g_1$, but $\mathrm{N}_G(A_1) = 2|A_1|$, i.e. G has a subgroup which is larger than $|G|$, a contradiction. Thus, $q > 1$. This means $(q - 1)/q \geq 1/2$. Then, Eq. 1.35 says the following:

$$\frac{1}{2} \geq \frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk} \geq \frac{1}{g} + \frac{1}{k} \geq \frac{1}{k} \tag{1.68}$$

Which means $k \geq 2$. As was shown earlier, since $k > 1$, it must be that k is equal to one of the g_i. Without loss of generality, let $k = g_1$. Then, Eq. 1.35 gives the relation

$$\frac{1}{2g_2} = \frac{1}{g} - \frac{1}{qg_1} + \frac{1}{2g_1} \tag{1.69}$$

Since $|A_i|$ is relatively prime to p, it must be that $g \geq g_1 q$. In fact, since the normalizer of A_i is twice as large (and thus also has order relatively prime to p), this is strict equality, or $\frac{1}{g} - \frac{1}{g_1 q} < 0$. Therefore, the above says

$$\frac{1}{2g_2} < \frac{1}{2g_1} \implies g_1 < g_2 \tag{1.70}$$

Now, the claim is $q \equiv 1 \mod g_1$. First of all, take any non-identity element $x \in Q$. Then, from earlier note that $\mathrm{C}_G(x)$ is $Q \times Z$. Therefore, the number of elements in $\mathrm{N}_G(Q)$ conjugate to x is

$$|\mathrm{N}_G(Q) : \mathrm{C}_{\mathrm{N}_G(Q)}(x)| = |\mathrm{N}_G(Q) : Q \times Z| = k \tag{1.71}$$

By construction, if one conjugates elements of Q by elements of $\mathrm{N}_G(Q)$, the result is elements of Q. Therefore, if an element $x \in Q - \{e\}$ has k conjugates in $\mathrm{N}_G(Q)$, it really has k conjugates inside $Q - \{e\}$. Since the number of conjugacy classes of elements in Q without the identity must be an integer, it must be that $(q - 1)/k$ is an integer. Thus, $q \equiv 1 \mod k$, as claimed.

Let $ag = 2g_1 g_2 q$ (it is not clear here that $a \in \mathbb{Z}$). Then,

$$\frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qg_1} \tag{1.72}$$

becomes

$$g_1 q = a + (q - 2)g_2 \tag{1.73}$$

This makes it clear that a is an integer. By construction it must be positive (since $g_i, q, g > 0$). Thus, $g_1 > (q - 2)g_2/q$. In addition,

$$g_2 \mod g_1 = \frac{g_1 q - a}{q - 2} \mod g_1 = \frac{a}{2 - q} \mod g_1 = a \mod g_1 \tag{1.74}$$

where the fact that $q \mod g_1 = 1 \mod g_1$ form earlier has been used. Eq. 1.74 says that $g_2 = a + lg_1$ for some integer l. Now, consider two cases: $q \geq 4$ and $q < 4$. First, suppose that $q \geq 4$. From Eq. 1.73, $g_1 > 2g_2/q > 2g_2/4$. Thus,

$$2g_1 > g_2 > g_1 \tag{1.75}$$

Therefore,

$$2 > a/g_1 + l > 1 \implies 1 > \frac{a}{2g_1} + \frac{l}{2} > \frac{1}{2} \tag{1.76}$$

Now, note that since $g \geq 2qg_2$, it must be that $a/2g_1 = g_2q/g \leq 1/2$. This tells says l cannot be negative, otherwise $a/2g_1 + l/2$ would be less than $1/2$. It also cannot be that $l > 1$, otherwise this same quantity would be larger than 1. Therefore, $l = 0$ or $l = 1$. First, suppose that $l = 0$. Then, $g_2 = a$. This means $g = 2g_1q$. However, $g \geq 2g_2q > 2g_1q$ since the order of $\mathrm{N}_G(A_2)$ is relatively prime to p and so the order of G (2g) is greater than the product of the order of the normalizer of A_2 ($4g_1$) and the order of a Sylow-p subgroup (q). Thus, $l = 1$. This means

$$g_2 = g_1 + a \tag{1.77}$$

Then, Eq. 1.73 says

$$g_1q = a + (q-2)g_2 = g_1q = a + (q-2)(g_1 + a) \implies 2g_1 = a(1-q) \tag{1.78}$$

Rearranging gives $2g_2 = a(q+1)$ and $2g = a(q^2-1)q$ and

$$\frac{2}{a} = \frac{q-1}{g_1} \tag{1.79}$$

Since q is $1 \mod g_1$ the right hand side is an integer and so $d \equiv 2/a$ is an integer. This completes this case. Now, suppose $q < 4$. This means either $p = 2$ or $p = 3$. Ignore the case $p = 2$ and consider $q = p = 3$. Since q is $1 \mod g_1$, there is an integer l so that $3 = 1 + lg_1$. This means $2 = lg_1$ and so it must be that $l = 1$ and $g_1 = 2$. Next, since $g_1 > (q-2)g_2/q$, $g_1 > g_2/3$, i.e. $g_2 < 6$. Also, $g_2 > g_1$ so $2 < g_2 < 6$. Furthermore, g_2 is relatively prime to $p = 3$ so $g_2 = 4$ or $g_2 = 5$. In the first case ($g_2 = 4$), $a = 2$ and the second case ($g_2 = 5$) $a = 1$. Therefore, $g = 60$ or $g = 2 * 2 * 4 * 3/2 = 3(3-1)(3+1)/2$, which is a subgroup of the type in the first case of the proposition. Since this thesis cares about generic p, the proof that for this $g = 60$ group, $G \cong \mathrm{SL}(2,5)$ is omitted.

□

Proposition 14 (Case 6)**.** *G is isomorphic to either*

$$\langle x, y | x^n = y^2, y^{-1}xy = x^{-1} \rangle \tag{1.80}$$

for n even, or $G \cong \mathrm{S}_5 \cong \mathrm{SL}(2,5)$ or $G/Z \cong \mathrm{S}_4$.

Proof. Eq. 1.35 becomes

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1-1}{2g_1} + \frac{g_2-1}{2g_2} + \frac{g_3-1}{2g_3} \tag{1.81}$$

or

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{2} + \frac{1}{g} + \frac{q-1}{qk} \tag{1.82}$$

Suppose that $q > 1$. Then, $(q-1)/q \geq 1/2$ and so $(q-1)/(qk) \geq 1/(2k)$. From the proof of Case 1, one knows that k is one of the g_i. Without loss of generality, suppose that $k = g_1$. Then,

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} \geq \frac{1}{2} + \frac{1}{g} + \frac{1}{2g_1} \tag{1.83}$$

since $g_i > 1$,

$$\frac{1}{2} \geq \frac{1}{2g_2} + \frac{1}{2g_3} \geq \frac{1}{2} + \frac{1}{g} \tag{1.84}$$

which is a contradiction. Therefore, $q = 1$. This implies that

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{2} + \frac{1}{g} > \frac{1}{2} \tag{1.85}$$

without loss of generality, let $1 < g_1 \leq g_2 \leq g_3$. If $g_1 = 3$, then,

$$\frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{3} + \frac{1}{g} \tag{1.86}$$

but, the left hand side is at most $1/3$ and so this is not possible. Therefore, $g_1 = 2$. Then,

$$\frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{4} + \frac{1}{g} \tag{1.87}$$

If $g_2 = 2$, then $g = 2g_3$. If $g_2 = 3$,

$$\frac{1}{2g_3} = \frac{1}{12} + \frac{1}{g} \tag{1.88}$$

which means that $g_3 \leq 5$. If $g_2 = 4$,

$$\frac{1}{2g_3} = \frac{1}{8} + \frac{1}{g} \tag{1.89}$$

which would mean that $g_3 < 4$, a contradiction. Thus, there are only two possibilities. The first case is when $g_1 = 2, g_2 = 2$ and $g = 2g_3$. Thus, $G = \mathrm{N}_G(A_3)$ since the index between these is two by construction. Let x be a generator of A_3. Then, as in Case 2, there is an element y of G which conjugates x to its inverse, where y is conjugate to w. If x has order $2n$, then this means that G is a subgroup of

$$\langle x, y | x^n = y^2, y^{-1}xy = x^{-1} \rangle \tag{1.90}$$

and since $|A_2| = 4$ and $\mathrm{N}_G(A_2) = 8$, it must be that the size of a Sylow-2 subgroup is at least 8. This means that n must be even because A_3 must contain a Sylow-p subgroup of order at least 4 (and so n must be divisible by half of that). It has not been shown that G is defined by this presentation, but this is a routine exercise.

The second case is $g_1 = 2, g_2 = 3$ and $3 \leq g_3 \leq 5$. If $g_3 = 3$ then Eq. 1.88 says that $g = 12$. Therefore, subgroups of G of order 3 are Sylow-3 subgroups and are thus all conjugate. This means that A_2 and A_3 are conjugate. However, A_i are chosen to be not conjugate by construction and so there is a contradiction. Thus, $g_3 = 4$ (and so $g = 24$ by Eq. 1.88) or $g_3 = 5$ (and so $g = 60$).

First, suppose that $g = 24$ (so that $|G| = 48$). Then, $|\mathrm{N}_G(A_2)| = 12$ and so $|G : \mathrm{N}_G(A_2)| = 4$. Let G act on the set of cosets of $\mathrm{N}_G(A_2)$ by conjugation. This gives a non-trivial homomorphism from G to S_4, the symmetric group on four letters. It is not hard to show that Z is the kernel. Thus, the image is S_4, which one can deduce by counting the sizes of groups. This means that $G/Z = \mathrm{S}_4$. The group G is uniquely defined as a central extension of S_4, but in the end for $\mathrm{PSL}(2, \mathrm{p})$, one only cares about the factor group by the center.

Next, suppose that $g = 60$ and so $|G| = 120$. One plays the same game as in the previous case. A Sylow-2 subgroup must have order at least 8. Since 16 does not divide 120 (and neither does any higher power of 2) it must be that the Sylow-2 subgroup is precisely of order 8 and thus conjugate to A_1. By the same logic as in the proof of Case 2, this Sylow-2 subgroup is isomorphic to Q_8. It is an elementary fact that Q_8 has three subgroups of order 4 (which are normal in Q_8). Each of these (as well as A_1) are isomorphic to $\mathbb{Z}_4$. Since these are abelian, they must be contained in some maximal abelian subgroup

of G. The only ones with an order which has 4 as a divisor is A_1. Thus, these subgroups of Q_8 must be conjugate to A_1. There are $|G : \mathrm{N}_G(A_1)| = 15$ subgroups conjugate to A_1. Therefore, there must be 5 Sylow-2 subgroups in G. Let G act on the set of Sylow-2 subgroups. This gives a homomorphism from G to S_5, the symmetric group on 5 letters. Since all the Sylow-2 subgroups are conjugate, it must be that the non-central elements of G act nontrivially on this set. Therefore, G/Z is isomorphic to the image of the homomorphism which is a subgroup of S_5. Since the order of the image is 60, it must be normal in S_4 and thus is isomorphic to A_4. Thus, $G \cong \mathrm{S}_4 \cong \mathrm{SL}(2,5)$. □

Now, all of these cases can be collected in one place:

Theorem 2. *A subgroup of* $\mathrm{PSL}(2,\mathrm{p})$ *is isomorphic to one of the following groups:*

1. *The dihedral group of order* $p \pm 1$ *and their subgroups*
2. *A group* H *of order* $p(p-1)/2$ *and its subgroups. A Sylow p-subgroup* Q *of* H *is elementary abelian,* $Q \trianglelefteq H$ *and the factor group* H/Q *is cyclic of order* $(p-1)/2$.
3. $\mathrm{A}_4, \mathrm{S}_4$ *or* A_5

Proof. From all the work with the various cases above, one knows what the subgroups of SL(V) that contain the center look like. Since $\mathrm{PSL}(2,\mathrm{p})$ is contained in $\mathrm{SL(V)}/Z$, the correspondence theorem (a.k.a. fourth isomorphism theorem) states that the subgroups of $\mathrm{PSL}(2,\mathrm{p})$ must be of the form G/Z where G is a subgroup of SL(V) which contains Z. Consider each of the six cases. Before proceeding, note that since $|\mathrm{SL}(2,\mathrm{p})| = (p-1)p(p+1)$, it must be that a Sylow-p subgroup has order p, since p cannot divide $p \pm 1$. Let G be a subgroup of $\mathrm{PSL}(2,\mathrm{p})$. First, consider Case 2. Here, G is isomorphic to $\mathrm{SL}(2,3)/Z \cong \mathrm{A}_4$ or H/Z where

$$H = \langle x, y | x^n = y^2, y^{-1}xy = x^{-1} \rangle \tag{1.91}$$

From the proof of this case, y is conjugate to w in SL(V). Squaring w gives the negative identity which is in Z and so $y^2 = 1$ in H/Z. Therefore,

$$H/Z = \langle x, y | x^n = y^2 = 1, y^{-1}xy = x^{-1} \rangle \tag{1.92}$$

It is not hard to show that this is precisely D_{2n}, the dihedral group of order n [6]. In Case 3, one gets the cyclic Sylow-p subgroup of $\mathrm{PSL}(2,\mathrm{p})$. Case 4 only happens if $p = 3$ in which case $G \cong \mathrm{SL}(2,3)/Z \cong \mathrm{A}_4$. In Case 5, one either has that $G \cong \mathrm{S}_5/Z \cong \mathrm{A}_5$ or $|G| = 2p(p^2-1)/d$ where $d = 1$ or 2. If $d = 2$, then going mod the center will give a group with precisely the same size as $\mathrm{PSL}(2,\mathrm{p})$. Thus, if G is a subgroup it must be the entire group. If $d = 2$, then $|G|$ is larger than the size of $\mathrm{PSL}(2,\mathrm{p})$ and so this possibility can be ignored. In Case 6, one either havs $G \cong \mathrm{A}_5$ or S_4 or G is isomorphic to H/Z where

$$H = \langle x, y | x^n = y^2, y^{-1}xy = x^{-1} \rangle \tag{1.93}$$

once again, this is a dihedral group. Now, return to Case 1. This will correspond to groups of the second type in the theorem. In this case, G contains the cyclic Sylow-p subgroup. Furthermore, it was proved in that case that the quotient of G by the normal Sylow-p subgroup is cyclic of order relatively prime to p. All that remains is to describe the order of G in this case. For this, one needs to know the number of Sylow-p subgroups. This must be congruent to 1 mod p and must divide $p(p+1)(p-1)$. This last bit is because it is clear that for $p \neq 2$, the number of Sylow-p subgroups of $\mathrm{PSL}(2,\mathrm{p})$ is the same as the number in $\mathrm{SL}(2,\mathrm{p})$. The number of subgroups thus must divide $p+1$ and or $p-1$. However, in order to be congruent to 1 mod p, it must be that the number of Sylow p subgroups is precisely $p+1$. Therefore, the index of the normalizer of Q in $\mathrm{PSL}(2,\mathrm{p})$ is $(p+1)$ and so the order of the normalizer is $p(p-1)/2$. The subgroup G normalizes Q and so is contained in the normalizer and thus has order at most $p(p-1)/2$.

□

With the above theorem, one can begin to find how often and how many of these subgroups occur.

Theorem 3. *Let* $G = \mathrm{PSL}(2,\mathrm{p})$. *Then,*

1. *G always contains subgroups isomorphic to the dihedral groups in Part (1) and the groups of Part (2) of the previous theorem.*
2. *G contains* A_5 *if and only if* $p \equiv \pm 1 \mod 5$.
3. *G contains* A_4 *if and only if* $p \neq 2$.
4. *G contains* S_4 *if and only if* $p \equiv \pm 1 \mod 8$.

Each part of this theorem will be proved one at a time as Dickson's Theorem is completed.

Proposition 15. *G always contains subgroups isomorphic to the dihedral groups in Part (1) and the groups of Part (2) of the previous theorem.*

Proof. From Case 5, $\mathrm{PSL}(2,\mathrm{p})$ has cyclic subgroups of order $p \pm 1$. Furthermore, the normalizer is twice as big. In addition, these normalizers cannot be abelian because the cyclic subgroups of order $p \pm 1$ are maximal abelian. Therefore, the normalizers are precisely the dihedral groups of order $2(p \pm 1)$.

The group of order $p(p-1)/2$ also must exist because it is the normalizer of the Sylow-p subgroup, whose existence Sylow's theorem guarantees. □

Proposition 16. A_5 *is a subgroup of* $\mathrm{PSL}(2,\mathrm{p})$ *if and only if* $2 \neq p \equiv \pm 1 \mod 5$.

Proof. Since A_5 is simple, its center is trivial and so under the isomorphism theorems, one only needs to show that A_5 is a subgroup of $\mathrm{SL}(2,\mathrm{p})$ if and only if $2 \neq p \equiv \pm 1 \mod 5$. First of all, if $\mathrm{A}_5 \subset \mathrm{SL}(2,\mathrm{p})$, then 5 divides $|\mathrm{SL}(2,\mathrm{p})| = (p-1)p(p+1)$. Since $\mathrm{A}_5 \cong \mathrm{SL}(2,5)$ it is trivial if $5|p$ (so ignore that case). Therefore, either $5|(p+1)$ or $5|(p-1)$. Thus, $p \equiv \pm 1 \mod 5$.

Now, for the converse. Suppose that $p \equiv \pm 1 \mod 5$. The argument is similar in both cases, but for the sake of brevity consider only the case where $p \equiv +1 \mod 5$. Since $\mathbb{F}_p^*$ has $p-1$ elements, this multiplicative group has order divisible by 5. Therefore, by Cauchy's theorem, $\mathbb{F}_p^*$ has an element of order 5, call it z. Consider two matrices in $\mathrm{SL}(2,\mathrm{p})$:

$$x = \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \qquad y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1.94}$$

with the two equations $a + d = -1$ and $az + dz^{-1} = 0$. The solutions to these equations are

$$a = \frac{1}{z^2 - 1} \qquad d = -\frac{z^2}{z^2 - 1} \tag{1.95}$$

since z has order 5, these are well defined. The claim is that with these restrictions on y give $y^3 = (xy)^4 = 1$. This is a straightforward matrix computation. Below is a part of the one which shows that $y^3 = 1$.

$$y^3 = \begin{pmatrix} a^3 + 2abc + bcd & a^2b + b^2c + abd + bd^2 \\ a^2c + acd + bc^2 + cd^2 & abc + 2bcd + d^3 \end{pmatrix} \tag{1.96}$$

It is not hard to see that the first entry is 1. Similar computations work for the other components. Note that $ad - bc = 1$ and $a + d = -1$. Then,

$$b = \frac{ad - 1}{c} = \frac{a(-1-a) - 1}{c} = -\frac{a^2 + a + 1}{c} \tag{1.97}$$

Therefore,

$$\begin{aligned} a^3 + 2abc + bcd &= a^3 - 2a(a^2 + a + 1) - d(a^2 + a + 1) \\ &= a^3 - 2a(a^2 + a + 1) + (a+1)(a^2 + a + 1) \\ &= a^3 - 2a^3 - 2a^2 - 2a + a^3 + a^2 + a + a^2 + a + 1 \\ &= 1 \end{aligned} \tag{1.98}$$

One can also show that[4] $\mathrm{A}_5 = \langle a, b | a^3 = (ab)^4 = 1 \rangle$. Therefore, there exists a homomorphism $\phi : \mathrm{A}_5 \twoheadrightarrow \langle x, y \rangle \leq \mathrm{SL}(2, \mathrm{p})$. Since A_5 is simple, $\langle x, y \rangle$ is isomorphic to A_5 or is trivial. Since x is not trivial, $\langle x, y \rangle \cong \mathrm{A}_5$.

□

Proposition 17. *G contains A_4 if and only if $p \neq 2$.*

Proof. If $p = 3$ then $\mathrm{SL}(2,3)/Z \cong \mathrm{A}_4$. If $p > 3$, then either p is 1 or -1 mod 3 and so $p^2 \equiv 1 \mod 3$. Then, just as in the proof of the previous proposition, there are elements $x, y \in \mathrm{SL}(2, \mathrm{p})$ such that $x^3 = y^3 = 1$ and $xy \notin Z$ but $(xy)^2 \in Z$. It is not hard to show that $\langle x, y \rangle \cong \mathrm{SL}(2,3)$ and so the image in $\mathrm{PSL}(2, \mathrm{p})$is A_4. □

Proposition 18. *G contains S_4 if and only if $p \equiv \pm 1 \mod 8$.*

Proof. First suppose that G contains a subgroup H isomorphic to S_4. Then, since the Sylow-2 subgroup of S_4 is isomorphic to the quaternion group, it must be that the Sylow-2 subgroup of G has order at least 8. Therefore, 8 must divide $p - 1$ or $p + 1$ (since it does not divide p) and so p is ± 1 mod 8.

Conversely, suppose that $p \equiv \pm 1 \mod 8$. Then, since 8 divides $p + 1$ or $p - 1$, it must be that the Sylow-2 subgroup has order at least 8. By the previous proposition, G contains a subgroup A isomorphic to A_4. Let Q be the unique elementary abelian Sylow-2 subgroup of A. From Sylow, it must be that Q is contained in some Sylow-2 subgroup of G. Since such subgroup has order at least 8 and Q has order 4, it must be that this is proper containment. Thus, A is not the normalizer of Q in G. Looking through the possible subgroups which could be the normalizer, one can see that it must be S_4. □

Now that the elements of $\mathrm{PSL}(2, \mathrm{p})$ are understood, it is possible to identify the order of elements merely by the trace of a lift to $\mathrm{SL}(2, \mathrm{p})$ [13][11].

Lemma 4. *Let I be the 2×2 identity matrix and take $\pm I \neq x \in \mathrm{SL}(2, \mathrm{F})$. Then,*

1. *$x^2 \neq I$ if and only if $p = 2$ and $\mathrm{tr}(x) = 0$.*
2. *$x^2 = -I$ if and only if $\mathrm{tr}(x) = 0$.*
3. *$x^3 = \pm I$ if and only if $\mathrm{tr}(x) = \mp 1$.*
4. *$x^4 = -I$ if and only if $\mathrm{tr}(x) = \pm\sqrt{2}$.*

Proof. The element x is conjugate to $\pm t_\lambda$ or d_ω. Furthermore, it has been shown that if the former is true, then $x^p \in Z$, so if $x^2 \in Z$ then $p = 2$. Furthermore, since traces are preserved under conjugation, $\mathrm{tr}(x) = \pm 2$ which is zero in a field of characteristic 2. Next, suppose that x is conjugate to d_ω. Then, $\mathrm{tr}(x) = \omega + \omega^{-1}$. If $x \notin Z$ but $x^2 \in Z$ then $\omega^2 = -1$, so $\omega^{-1} = -\omega$ and thus $\mathrm{tr}(x) = \omega + \omega^{-1} = 0$ as desired.

Next, suppose that $x^3 = I$. Note that this means that

$$0 = (x^3 - I) = (x^2 + x + I)(x - I) \tag{1.99}$$

Since $x \neq \pm I$, it must be that $x^2 + x + I = 0$ so $x^2 + x = -I$ or $x + x^{-1} = -I$, since $x^{-1} = x^2$. Now, suppose that $x^3 = -I$. Note that this implies that

$$0 = (x^3 + I) = (x^2 - x + I)(x + I) \tag{1.100}$$

Since $x \neq \pm I$, it must be that $x^2 - x + I = 0$ so $x^2 - x = -I$ and thus $x^{-1} + x = I$ since $-x^2 = x^{-1}$. Therefore, if $x \in \mathrm{SL}(2, \mathrm{p})$ then x has order 3 if $\mathrm{tr}(x) = -1$ and order 6 if $\mathrm{tr}(x) = +1$.

Now, suppose $x^4 = -I$. There exists an ω such that x is conjugate to d_ω. Then, $\omega^4 = -1$. This means that $\omega^2 = -\omega^{-2}$. Then,

[4] See for example, page 176 in [13].

$$(\omega + \omega^{-1})^2 = \omega^2 + 2\omega\omega^{-1} + \omega^{-2} \tag{1.101}$$
$$= 2$$

Therefore, $\mathrm{tr}(x)^2 = 2$.

□

One can use trace identities to write down conditions for other orders as well [8]. For example, for $A \in \mathrm{SL}(2,\mathrm{p})$, $A \neq \pm I$ and $\pm\mathrm{tr}(A)^3 + \mathrm{tr}(A)^2 \mp 2\mathrm{tr}(A) - 1 = 0$ then A has order 7. Similarly, if $\mathrm{tr}(A)^2 \pm \mathrm{tr}(A) - 1 = 0$ then A has order 5. In fact, the traces of elements even carry information about subgroups. For example, there is a theorem by McCullough [11] which relates traces of elements to the subgroup that they generate. One result from this theorem will be needed later and so it is proved here. That paper considers a slightly different case than the present one, but the proof goes through without much modification. Let $p \equiv 1 \mod 8$ (so that $\sqrt{2} \in \mathbb{F}_p$ - see for example [12]). The following is true:

Theorem 4. *Let $A, B \in \mathrm{SL}(2,\mathrm{p})$ with no more than one of $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)$ equal to zero. Then, $\pi(\langle A, B\rangle) = \mathrm{S}_4$ if $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB) \in \{0, \pm 1, \pm\sqrt{2}\}$ (and at least one is $\pm\sqrt{2}$) and $\mathrm{tr}([A,B]) = 1$.*

Before proving this, preliminary lemmas need to be established to build some trace technology in $\mathrm{SL}(2,\mathrm{p})$.

Lemma 5. *Let $a, b \in \mathrm{SL}(2,\mathrm{p})$. Let $\pi : \mathrm{SL}(2,\mathrm{p}) \to \mathrm{PSL}(2,\mathrm{p})$ be the standard projection. Then, $\pi(\langle a, b\rangle)$ is the same as each of the following groups:*

$$\pi(\langle a^{-1}, b\rangle),\ \pi(\langle b, a\rangle),\ \pi(\langle a^{-1}, ab\rangle),\ \pi(\langle -a, b\rangle),\ \pi(\langle -a, -b\rangle)$$

Proof. This is clear since $\pi(a) = \pi(-a)$. □

Now, the goal is to see how these actions on the set of generators change the traces of the generators. Then, one can simply look at traces of elements instead of the elements themselves. To attack this, it is necessary to establish a few trace identities in $\mathrm{SL}(2,\mathrm{p})$.

Lemma 6. *For $a, b \in \mathrm{SL}(2,\mathrm{p})$, $\mathrm{tr}(a^{-1}b) + \mathrm{tr}(ab) = \mathrm{tr}(a)\mathrm{tr}(b)$*

Proof. Take

$$a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad b = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \tag{1.102}$$

Then,

$$a^{-1}b = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{22}b_{11} - a_{12}b_{21} & a_{22}b_{12} - a_{12}b_{22} \\ -a_{21}b_{11} + a_{11}b_{21} & -a_{21}b_{12} + a_{11}b_{22} \end{pmatrix} \tag{1.103}$$

$$ab = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} \tag{1.104}$$

therefore,

$$\begin{aligned} \mathrm{tr}(a^{-1}b) + \mathrm{tr}(ab) &= a_{11}b_{11} + a_{12}b_{21} + a_{21}b_{12} + a_{22}b_{22} - a_{22}b_{11} + a_{12}b_{21} + a_{21}b_{12} - a_{11}b_{22} \\ &= a_{22}b_{11} + a_{11}b_{22} + a_{11}b_{11} + a_{22}b_{22} \\ &= (a_{11} + a_{22})(b_{11} + b_{22}) \\ &= \mathrm{tr}(a)\mathrm{tr}(b) \end{aligned} \tag{1.105}$$

□

Lemma 7 (Fricke)**.** *For $a, b \in SL(2,p)$, $\mathrm{tr}([a,b]) = \mathrm{tr}(a)^2 + \mathrm{tr}(b)^2 + \mathrm{tr}(ab) - \mathrm{tr}(a)\mathrm{tr}(b)\mathrm{tr}(ab) - 2$*

Proof. All that is required is the repeated use of the previous lemma and its immediate consequences such as $\mathrm{tr}(a^2) = \mathrm{tr}(a)^2 - 2$. The first computation is

$$\begin{aligned} \mathrm{tr}(a)\mathrm{tr}(b)\mathrm{tr}(ab) &= \mathrm{tr}(a)\left[\mathrm{tr}(b^{-1}ab) + \mathrm{tr}(ab^2)\right] \\ &= \mathrm{tr}(a)^2 + \mathrm{tr}(a)\mathrm{tr}(ab^2) \\ &= \mathrm{tr}(a)^2 + \mathrm{tr}(b^2) + \mathrm{tr}(a^2b^2) \\ &= \mathrm{tr}(a)^2 + \mathrm{tr}(b)^2 - 2 + \mathrm{tr}(a^2b^2) \end{aligned} \tag{1.106}$$

which means that the righthand side of the lemma is $\mathrm{tr}(ab)^2 - \mathrm{tr}(a^2b^2)$. The next computation is the lefthand side:

$$\begin{aligned} \mathrm{tr}(aba^{-1}b^{-1}) = \mathrm{tr}(a^{-1}b^{-1}ab) = \mathrm{tr}((ba)^{-1}(ab)) &= \mathrm{tr}((ba)^{-1})\mathrm{tr}(ab) - \mathrm{tr}(baab) \\ &= \mathrm{tr}(ab)^2 - \mathrm{tr}(a^2b^2) \end{aligned} \tag{1.107}$$

and so the Fricke trace identity is proved.

□

Now, it is possible to return to considering the consequences of Lemma 5. Let $T(a,b) = (\mathrm{tr}(a), \mathrm{tr}(b), \mathrm{tr}(ab))$. For each of the equivalent generating sets in Lemma 5, the goal is to write down the sets of equivalent traces.

Lemma 8. *Let $a, b \in \mathrm{SL}(2,\mathrm{p})$. Let $\pi : \mathrm{SL}(2,\mathrm{p}) \to \mathrm{PSL}(2,\mathrm{p})$ be the standard projection. Then, one can always pick a different generating set a', b' of $\pi(\langle a, b\rangle)$ so that if $T(a,b) = (\alpha,\beta,\gamma)$ then $T(a',b')$ can be chosen to be one of the following:*

$$(\alpha,\beta,\alpha\beta-\gamma),\ (\beta,\alpha,\gamma),\ (\alpha,\gamma,\beta),\ (-\alpha,\beta,-\gamma),\ (-\alpha,-\beta,\gamma)$$

Proof. First, note that one can choose (a^{-1}, b) as a generating set. Since $\mathrm{tr}(a^{-1}) = \alpha$, all that needs to be computed is

$$\mathrm{tr}(a^{-1}b) = \mathrm{tr}(a)\mathrm{tr}(b) - \mathrm{tr}(ab) = \alpha\beta - \gamma \tag{1.108}$$

Next, note that (b, a) can be used as a generating set. Trivially, this leaves the trace of the product unchanged and simply swaps α and β. Now, consider (a^{-1}, ab) as a generating set. This switches β and γ, leaving α unchanged. The multiplication by the negative signs is trivial; clearly if $(-a, b)$ is used as a generating set, the traces will be $(-\alpha,\beta,-\gamma)$ and if both a and b are negated, there is no change to the trace of the product. □

Now, Theorem 4 can be proved.

Proof of Theorem 4. First of all, by the lemma, if B has trace $\sqrt{2}$, then A and B can be switched and generate the same group. Similarly, if AB has trace $\sqrt{2}$, then one can switch A and AB and generate the same group. Therefore, without loss of generality, suppose that $\mathrm{tr}(A) = \sqrt{2}$. Since no two of $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)$ are zero, by the same logic one can take $\mathrm{tr}(B)$ to be nonzero. Let $\mathrm{tr}(A) = \alpha$, $\mathrm{tr}(B) = \beta$ and $\mathrm{tr}(AB) = \gamma$. First, consider the case where $(\alpha,\beta) = (\sqrt{2},\sqrt{2})$. By the Fricke trace identity

$$\mathrm{tr}([A,B]) = \mathrm{tr}(A)^2 + \mathrm{tr}(B)^2 + \mathrm{tr}(AB) - \mathrm{tr}(A)\mathrm{tr}(B)\mathrm{tr}(AB) - 2 \tag{1.109}$$

for $\gamma \in \{-\sqrt{2}, -1, 0, 1, \sqrt{2}\}$, the possible values of $\mathrm{tr}([A,B])$ are respectively $(4+2\sqrt{2}, 5, 2, 1, 4-2\sqrt{2})$. Quick arithmetic computations show that the only possibility is for $\gamma = 1$. By the lemma, one can always pick new generators A', B' so that $(\alpha,\beta,\gamma) \mapsto (\alpha,\gamma,\beta) \mapsto (\alpha,\gamma,\alpha\gamma-\beta)$. In the case at hand, this means the traces are $(\sqrt{2},\sqrt{2},1) \mapsto (\sqrt{2},1,\sqrt{2}) \mapsto (\sqrt{2},1,0)$. This means that $\pi(A')$ has order 4, $\pi(B')$ has order 3 and $\pi(A'B')$ has order 2. This is precisely a presentation[5] of S_4 and so $\mathrm{S}_4 \cong \pi(\langle A', B'\rangle) = \pi(\langle A, B\rangle)$.

[5] This is a solution to exercise 6 in Section 6.3 of [6].

Now, consider the case where $\beta = 1$ (this also covers the case where $\beta = -1$ by the lemmas). Then, the Fricke trace identity gives

$$\mathrm{tr}([A, B]) = 1 + \gamma^2 - \gamma\sqrt{2} \tag{1.110}$$

Setting this equal to 1 results in $\gamma(\gamma - \sqrt{2}) = 0$. The two solutions of this are $\gamma = \sqrt{2}$ and $\gamma = 0$. The first case was covered above. In the second case, $(\alpha, \beta, \gamma) = (\sqrt{2}, 1, 0)$, which as above means that $\pi(\langle A, B\rangle) \cong \mathrm{S}_4$. □

1.1.4 Application: Computing the Maximal Subgroups

For further computations, it will be necessary to generate the list of maximal subgroups for $\mathrm{PSL}(2, \mathrm{p})$ for large p. The algebra programming language `GAP` has a built-in algorithm for computing the set of maximal subgroups. However, it is generic. By using Dickson's Theorem, one can do much better (in terms of efficiency and space). The idea is to take the subgroups spelled out in Dickson's Theorem and to inject them into $\mathrm{PSL}(2, \mathrm{p})$, which `GAP` can create efficiently. The `GAP` script is reproduced in Appendix A.1.

Chapter 2

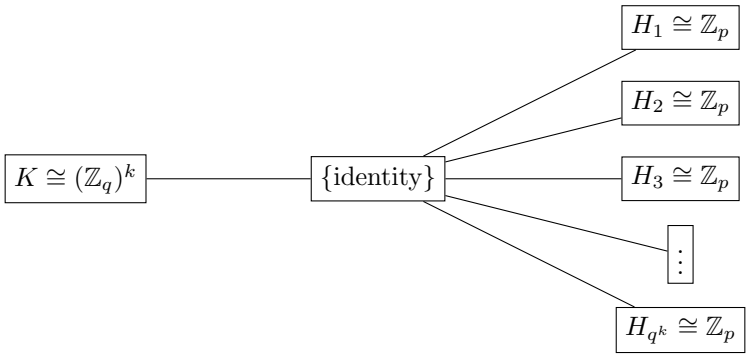
Irredundant Generating Sequences

2.1 Generating Sequences

The main purpose of this thesis is to study a specific subset of generating sequences of finite groups. Before getting too far, it is necessary to pause to explain precisely what is meant by generating sequence.

Definition 1. *Let G be a group. A sequence $g_1, ..., g_n$ for $g_i \in G$ is called a Generating Sequence if $\langle g_1, ..., g_n \rangle = G$.*

For example, consider the group $G = (\mathbb{Z}_q)^k \rtimes \mathbb{Z}_p$ where the subgroup K isomorphic to $(\mathbb{Z}_q)^k$ is minimal normal in G. It is easy to see what the subgroup lattice of this group looks like. There are q^k subgroups $H_i \cong \mathbb{Z}_p$, all of which are conjugate as Sylow-p subgroups. Furthermore since H_i has p elements, all q^k of these groups intersect trivially. One can depict this subgroup structure pictorially in the following diagram:



With such a simple lattice structure, one can easily compute properties of generating sequences. For example, consider the number of length two generating sequences. Every nontrivial pair of elements $(x, y) \in G \times G$ will have order structure (Order(x),Order(y)) of the form $(p, q), (q, p), (p, p)$ or (q, q). Clearly, if one has two elements of order q, then they can generate at most $K \neq G$ and so a length two generating sequence must have one of the first three order structures listed in the previous sentence. Furthermore, any sequence of the first two types, $(p, q), (q, p)$, will be a generating sequence. This is clear because an element of order p will generate one of the H_i, which is maximal in G and so adding any element no in H_i, namely any element of order q, will generate all of G. The next computation is to determine how many sequences are of this form. There are $q^k - 1$ non-identity elements in K, q^k possible H_i to chose from and $p - 1$ non-identity elements in each H_i. The two types (p, q) and (q, p) will give the same number of sequences and so the number of sequences of both types will be

$$2(q^k - 1)q^k(p - 1)$$

Now, one needs to determine how many length two generating sequences exist with elements of orders (p, p). All that is required is that the two elements come from different H_i. Then, the same logic as before applies, namely, each H_i is maximal and so adding any other element of G not in H_i will generate the entire group. There are q^k H_i to choose from, each with $p - 1$ elements. Then, one has $q^k - 1$ other H_j to choose from such that $i \neq j$. There are $p - 1$ choices for an element in each H_j. Adding this to the term from before, one has that the total number of length two generating sequences of G is given by the following expression:

$$(q^k - 1)q^k(p^2 - 1)$$

For a more concrete example, consider $k = 1, q = 3, p = 2$ so that $G \cong S_3$, the symmetric group on 3 letters and the smallest non-Abelian group. According to the formula, there should be 18 generating sequences of length 2. If $e, \tau_1 = (1, 2), \tau_2 = (2, 3), \tau_3 = (1, 3), \sigma = (1, 2, 3), \sigma^2 = (1, 3, 2)$ are the elements of S_3 then the generating sequences are listed below (up to switching elements).

Sequence	Orders
(τ_1, σ)	2,3
(τ_2, σ)	2,3
(τ_3, σ)	2,3

Sequence	Orders
(τ_1, σ^2)	2,3
(τ_2, σ^2)	2,3
(τ_3, σ^2)	2,3

Sequence	Orders
(τ_1, τ_2)	2,2
(τ_1, τ_3)	2,2
(τ_2, τ_3)	2,2

As another example, let $G = V$, a finite-dimensional vector space. Then, any basis will form a generating sequence of G. In fact, any set of vectors which contains a basis as a subset will be a generating sequence.

Any sequence which does not contain a basis as a subset will not generate G and thus will not be a generating sequence. However, one can see that there are arbitrarily large (constrained only by the size of the group) generating sets. Therefore, a restriction is made to the following class of generating sequences:

Definition 2. *A generating sequence $g_1, ..., g_n$ is called irredundant if it is no longer a generating sequence after removing any one element.*

With this definition, for a vector space the set of irredundant generating sequences is precisely the set of bases of V. Furthermore, if V is finite dimensional (say dimension n), then the size of any irredundant generating sequence has length n. This is due to the elementary Linear Algebra result which says that all bases have the same number of elements. The following is a study of the properties of the set of irredundant generating sequences of the finite group $\mathrm{PSL}(2, \mathrm{p})$.

2.1.1 Categorizing Groups Based on Generating Sequences

There are two obvious invariants of a group that one can construct based on irredundant generating sequences: the minimum and maximum length of possible sequences. After discussing the properties of these and other functions of the set of irredundant generating sequences, the attention will be focused on $\mathrm{PSL}(2, \mathrm{p})$.

Minimal Length

Definition 3. *Denote by $r(G)$ the minimum length of an (irredundant) generating sequence.*

A trivial example is the cyclic groups, for which $r(G) = 1$. This is the defining property of a cyclic group. For another example consider $G = \mathrm{A}_4$. The maximal subgroups are isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_2^2$. Therefore, taking a generator of the cyclic group of order 3 and adding any element of order 2 will irredundantly generate the group. Since A_4 is not cyclic, one needs at least two elements and so $r(G) = 2$. For any non-abelian finite simple group $r(G)$ has been completely determined by Robert Guralnick, a professor at the University of Southern California [10]. The theorem, which invokes the classification of finite simple groups is as follows:

Theorem 5 (3/2 Generation)**.** *Given any $x \in G$, there exists a $y \in G$ so that $G = \langle x, y \rangle$. In particular, $r(G) = 2$ for any G a non-abelian finite simple group.*

Since for $p > 3$, $G = \mathrm{PSL}(2, \mathrm{p})$ is simple and this powerful theorem says that $r(G) = 2$. However, the 3/2 Generation theorem is much more general and powerful than is needed to determine $r(\mathrm{PSL}(2, \mathrm{p}))$. It is actually a trivial consequence of elementary linear algebra that $\mathrm{PSL}(2, \mathrm{p})$ can be generated by two elements. The argument simply involves a careful manipulation of elementary matrices.

Maximal Lengths

Definition 4. *Denote by $m(G)$ the maximum length of an irredundant generating sequence.*

For example for $\mathrm{PSL}(2, \mathrm{p})$, it is easy to see that $m(G) \geq 3$. From the earlier order computation of $\mathrm{PSL}(2, \mathrm{p})$ it is clear that $|\mathrm{PSL}(2, \mathrm{p})|$ must be even because $p + 1$ and $p - 1$ are both even. Therefore, there exist nontrivial elements of order 2. Let H be the subgroup generated by all the elements of order 2. This subgroup must be normal and since it is nontrivial it must be all of G because $\mathrm{PSL}(2, \mathrm{p})$ is simple. Furthermore, two elements of order 2 generate a dihedral group, which is a proper subgroup (dihedral groups are not simple). Therefore, there must exist an irredundant generating sequence of length at least 3 (with elements all of order 2).

The function $m(G)$ is known for several types of groups. As a trivial example, for a vector space V, $r(V) = m(V) = \dim(V)$ since all bases have the same size. A less trivial example is the symmetric groups S_n of order $n!$. These groups along with a few others are discussed in Julius Whiston's Thesis [15]. For the symmetric groups, the answer is (which uses the classification of finite simple groups) as follows [14]:

Theorem 6. *For $G = \mathrm{S}_n$ the symmetric group on n letters, $m(G) = n - 1$.*

In the course of the proof, a limit is placed on the value of m for subgroups of S_n and so the author concludes that $m(\mathrm{A}_n) \leq n-2$. Since $(123), (124), ..., (12n)$ generate A_n, $m(\mathrm{A}_n) = n-2$ [4]. In addition to these specific examples, $m(G)$ has some nice general properties. For examples, $m(G \times H) = m(G) + m(H)$ [3]. One can use this to compute $m(G)$ for any finite abelian group G via the cyclic decomposition in the structure theorem for finite abelian groups.

2.2 Irredundant Generating Sequences of $\mathrm{PSL}(2, \mathrm{p})$

While the complete classification of generating sequences of $\mathrm{PSL}(2, \mathrm{p})$ is not known, there has been a lot of progress in that direction. The strongest theorem to date is by Julius Whiston and Jan Saxl of the University of Cambridge in 2002 [16]:

Theorem 7 (Whiston and Saxl)**.** *Let $G = \mathrm{PSL}(2, \mathrm{p})$, p prime. Then, $m(G) = 3$ or 4. If $p \neq \pm 1 \mod 10$ or $p \neq \pm 1 \mod 8$, then $m(G) = 3$.*

The exceptional cases are the ones in which S_4 or A_5 are subgroups of $\mathrm{PSL}(2, \mathrm{p})$. If $m(G) = 4$, let $\{x_1, x_2, x_3, x_4\}$ be an irredundant generating set. Let H_1 be a maximal subgroup containing $\langle x_2, x_3, x_4 \rangle$ and analogously define H_2, H_3, H_4. In the course of their proof, Whiston and Saxl show that in the case $m(G) = 4$, it must be that at least one of the H_i is isomorphic to either S_4 or A_5. In fact, one can learn even more in general about the x_i and the H_i. Another proposition in Whiston and Saxl's paper says the following:

Proposition 19. *No more than three H_i can be of the form $\mathrm{D}_{p\pm 1}$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_{(p-1)/2}$. If three of the H_i are of this form, then $m(G) = 3$.*

This means that when $m(G) = 4$ at least *two* of the H_i must be isomorphic to A_5 or S_4. To proceed, it is important to understand the generating sequences of S_4 and A_5. First of all, from Whiston's thesis, $m(\mathrm{S}_n) = n-1$ which is 3 for S_4 and since $\mathrm{A}_5 \cong \mathrm{PSL}(2, 5)$, $m(\mathrm{A}_5) = 3$. Next, note that

Lemma 9. *Every irredundant sequence of length 3 in $G \cong \mathrm{S}_4$ or $G \cong \mathrm{A}_5$ must generate.*

Proof. This follows from a careful consideration of the lattice of subgroups. The union of the sets of possible subgroups for these two groups have isomorphism classes $\{\mathrm{A}_4, \mathrm{D}_{10}, \mathrm{D}_8, \mathrm{S}_3, \mathbb{Z}_5, \mathbb{Z}_2^2, \mathbb{Z}_4, \mathbb{Z}_2, \{e\}\}$. All of these groups have $m(H) \leq 2$. If one has an irredundant sequence of length 3, it generates a subgroup of G. However, it cannot generate a proper subgroup because the maximal length of such a sequence for all the proper subgroups is less than 3, i.e. $m(H) \leq 2$ for all proper subgroups $H < G$. □

This property of S_4 and A_4 is more general and is given the following name in [16]:

Definition 5. *A finite group G is said to be flat if $m(H) \leq m(G)$ for $H \leq G$ and is called strongly flat if $m(H) < m(G)$ for any proper subgroup $H < G$.*

So in this language, both S_4 and A_5 are strongly flat. In fact, all symmetric groups are strongly flat [16].

Since the orders of S_4 and A_5 are relatively small, one can easily compute the possible orders of elements in irredundant generating sequences of length 3. To save space, below is the script for a 'brute force' `GAP` computation:

```
findorders:=function()
    local G,Ele,s,a,b,c,abc;
    G:=SymmetricGroup(4); #or G:=AlternatingGroup(5);
    Ele:=Elements(G);
    s:=Size(Ele);
    for a in [1..s] do;
        for b in [a+1..s] do
            for c in [b+1..s] do
                abc:=Subgroup(G,[Ele[a],Ele[b],Ele[c]]);
                #Check that the sequence {a,b,c} generates
                if (not(Size(abc)=Size(G))) then
                    continue;
                fi;
```

```
                #Now, check that it is irredundant
                if (Size(Subgroup(G,[Ele[a],Ele[b]]))=Size(G)) then
                    continue;
                fi;
                if (Size(Subgroup(G,[Ele[a],Ele[c]]))=Size(G)) then
                    continue;
                fi;
                if (Size(Subgroup(G,[Ele[b],Ele[c]]))=Size(G)) then
                    continue;
                fi;
                Print(Order(Ele[a])," , ", Order(Ele[b]), " , ", Order(Ele[c]), "\n");
                od;
            od;
    od;
end;
```

The program proves the following:

Lemma 10. *Length three irredundant sequences* (x, y, z) *in* S_4 *and* A_5 *have order structure* $(\mathrm{Order(x)}, \mathrm{Order(y)}, \mathrm{Order(z)})$ *equal to one of the triples below. Furthermore, all of these appear except* $(3, 3, 3)$*, which appears for* A_5 *but not* S_4*. Since both of these groups are strongly flat and* $m(G) = 3$*, it must be that all of these sequences are in fact generating sequences as well.*

$$(2, 2, 2), (2, 2, 3), (2, 3, 2), (2, 3, 3), (3, 3, 3), (3, 2, 2), (3, 2, 3), (3, 3, 2)$$

By Proposition 19, at least two of the H_i are contained in an isomorphic copy of S_4 or A_5. Without loss of generality, suppose that H_1 and H_2 are contained in isomorphic copies of S_4 or A_5. Then, x_2, x_3, x_4 is an irredundant sequence of length 3 sitting inside an isomorphic copy of S_4 or A_5. However, by Lemma 5, these length three irredundant sequences must generate the S_4 or A_5 they sit inside. Thus, x_2, x_3, x_4 have orders 2 or 3 by Lemma 6. Repeating this same argument for x_1, x_3, x_4 reveals that x_1 also must have order 2 or 3. Therefore,

Proposition 20. *If* $m(G) = 4$*, the possible orders of elements in an irredundant generating sequence of length* 4 *in* $\mathrm{PSL}(2, \mathrm{p})$ *are* 2 *and* 3*.*

Now, one can make an efficient computation in GAP to determine if $m(G) = 4$. Every length 4 irredundant generating sequence must originate from a length 3 irredundant generating sequence of $H = \mathrm{S}_4$ or $H = \mathrm{A}_5$. Therefore, the computation begins by determining all such irredundant generating sequences for an isolated copy of S_4 or A_5 in GAP. To limit the number of computations that need to be made, one can consider all sequences up to the action of the H on the sequences by element-by-element conjugation. This is because the goal is to prove the existence of a length four generating sequence. It is sufficient to look at all sequences up to conjugacy in G, since conjugating a length four irredundant generating sequence will produce another (possibly identical) length four irredundant generating sequence. Furthermore, conjugation in H can be extended to conjugation in G by using the lift of the conjugating element in H to G. To reduce the number of computations even further, one would like to simply look at the sequences up to the action of the entire automorphism group, not simply the inner automorphisms. However, it is a standard result that $\mathrm{Aut}(\mathrm{S_n}) \cong \mathrm{S}_n$ for $n \neq 6$ and so for these groups one does not gain anything from this [6]. In addition, even though A_5 is not isomorphic to its automorphism group, $\mathrm{Aut}(\mathrm{A}_5) \cong \mathrm{S}_5$ is not contained ($p \neq 5$) in the automorphism group of $\mathrm{PSL}(2, \mathrm{p})$, $\mathrm{PGL}(2, \mathrm{p})$ and so automorphisms on A_5 cannot be extended in general to automorphisms on G [1]. Thus one cannot guarantee that all sequences have been represented if only the automorphism classes of length 3 irredundant generating sequences in H have been considered. Below is the computation to generate the sequences in H:

```
FindSeq:=function(G)
    #G is eithe A5 or S4
    local gens,g,A,H,C,c,test,D,rep,mylist;
    gens:=[];
    A:=Elements(G);
    #Look at all the generating sets of G
    C:=Combinations([1..Size(G)],3);
```

```
    mylist:=[];
    for c in C do
        test:=Set([A[c[1]],A[c[2]],A[c[3]]]);
        #We do not need to consider two sequences if they are conjugate to each other.
        D:=Set(Orbit(G,test,OnSets));
        rep:=Elements(D);
        rep:=rep[1];
        mylist:=Union(mylist,[rep]);
    od;
    mylist:=Filtered(mylist,x->Size(Subgroup(G,Elements(x)))=Size(G));
    for c in mylist do #Make sure this is an irredundant generating sequence
        if (Size(Subgroup(G,[c[1],c[2]]))=Size(G)) then
            continue;
        fi;
        if (Size(Subgroup(G,[c[1],c[3]]))=Size(G)) then
            continue;
        fi;
        if (Size(Subgroup(G,[c[2],c[3]]))=Size(G)) then
            continue;
        fi;
        Append(gens,[c]);
    od;

    return gens;
end;
```

The algorithm to determine if $m(G) = 4$ operates as follows. First, construct A_5 and S_4. Embed these abstract groups into $\mathrm{PSL}(2, \mathrm{p})$ and get a list $H_1, H_2, ..., H_n$ of conjugacy classes of subgroups isomorphic to one of these maximal subgroups. Then, using the embedding maps, lift length three irredundant generating sequences computed with the above program from S_4 or A_5 to the H_i. Finally, systematically add all elements of order two and three to see if an irredundant length four sequence can be constructed. If the end of the list of such elements is reached and no length 4 irredundant generating sequence has been found, then such a sequence does not exist and so $m(G) = 3$. This computation has been carried (See the appendix for the script) for all primes up to 300. The surprising result is that $m(G) = 3$ unless $p = 7, 11, 19$ or 31. This leads to the following conjecture:

Conjecture 1. $m(\mathrm{PSL}(2, \mathrm{p})) = 3$ *unless* $p = 7, 11, 19$ *or* 31. *In these cases,* $m = 4$.

There was not sufficient time before the deadline of this thesis to complete the proof (or provide a counter example) of this conjecture. However, this work is ongoing and tools have been recently developed which will hopefully allow for the proof or disproof of this statement.

Examples of length four irredundant generating sequences (lifted to $\mathrm{SL}(2, \mathrm{p})$ so one can see the matrices) are below for (respectively) $p = 7, 11, 19, 31$:

$$\left\{\begin{pmatrix}4 & 6\\ 3 & 3\end{pmatrix}, \begin{pmatrix}5 & 4\\ 4 & 2\end{pmatrix}, \begin{pmatrix}0 & 4\\ 5 & 0\end{pmatrix}, \begin{pmatrix}0 & 6\\ 1 & 0\end{pmatrix}\right\}, \left\{\begin{pmatrix}0 & 5\\ 2 & 1\end{pmatrix}, \begin{pmatrix}8 & 1\\ 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 8\\ 8 & 10\end{pmatrix}, \begin{pmatrix}4 & 8\\ 2 & 7\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}4 & 7\\ 3 & 15\end{pmatrix}, \begin{pmatrix}1 & 18\\ 2 & 18\end{pmatrix}, \begin{pmatrix}18 & 14\\ 8 & 1\end{pmatrix}, \begin{pmatrix}2 & 8\\ 16 & 17\end{pmatrix}\right\}, \left\{\begin{pmatrix}3 & 30\\ 10 & 28\end{pmatrix}, \begin{pmatrix}25 & 27\\ 17 & 6\end{pmatrix}, \begin{pmatrix}17 & 1\\ 20 & 14\end{pmatrix}, \begin{pmatrix}1 & 8\\ 23 & 30\end{pmatrix}\right\}$$

Note that all of these elements have zero trace and so each have order 2.

Using `GAP`, one can learn more about the length 4 irredundant generating sequences of $\mathrm{PSL}(2, \mathrm{p})$ for $p = 7, 11, 19, 31$. Of primary interest are the total number of sequences and the number of orbits under conjugation and by the action of the automorphism group, $\mathrm{PGL}(2, \mathrm{p})$. The computation, outlined below, involves an extension of a program highlighted earlier. The `FindSeq` functions are used, with the modification that all lifts of generating sequences that extend to length four irredundant generating sequences are computed, not just (the first) one. The result is then conjugated by all the elements of $G = \mathrm{PSL}(2, \mathrm{p})$. By construction, after removing duplicates, this list will comprise all such sequences.

```
#p is one of 7,11,19,31
A:=FindSeq2(p); #These functions are outlined elsewhere but have been modified
                #to find all lifts of generating sequences that extend to length 4
                #irredundant generating sequences, not just one.
A2:=FindSeq(p);
Append(A,A2);
G:=PSL(2,p);
B:=[];
for g in G do
    for a in A do
        Append(B,[[g*a[1]*g^-1,g*a[2]*g^-1,g*a[3]*g^-1,g*a[4]*g^-1]]);
    od;
od;
Size(B);
C:=[];
for b in B do
    Append(C,[Elements(b)]);
od;
C:=Set(C); #This removes duplicates
Size(C); #This is the total number of length 4 irredundant generating sequences.
D1:=OrbitsDomain(G,C,OnSets);
Size(D1); #This is the total number up to conjugation
D2:=OrbitsDomain(AutomorphismGroup(G),C,OnSets);
Size(D2); #This is the total number up to Automorphism
```

First, consider $p = 7$. Since $p \equiv -1 \mod 8$, all irredundant generating sequences of length four must contain two copies of S_4 as maximal subgroups in the corresponding family of maximal subgroups in general position. Under the algorithm for computing such sequences, the program produces eight sequences of the maximal length. The elements are then conjugated by every element of G and duplicate sequences are removed. This procedure should produce a list of all possible irredundant length four generating sequences. There are 1344 sequences before removing duplicates, which results in the final result of 252 possible sequences. Every one of these sequences has all elements of order two. In fact, up to the action of G on the sequences by element-wise conjugation, there are only two conjugacy classes of sequences. Furthermore, this is the same number of orbits of these sequences under the action of the automorphism group of G, $\mathrm{PGL}(2,7)$.

Next, let $p = 11$. In this case, $p \equiv +1 \mod 10$ and so all irredundant generating sequences of the maximal length must contain two copies of A_5 in the corresponding list of maximal subgroups in general position. The raw number of sequences from the algorithm is 74. Before removing duplicates, there are 48840 sequences. The net number of irredundant generating sequences of length four after removing duplicates is 11935. Unlike for $p = 7$, not all the elements in these sequences have order two. However in line with what was shown earlier, they do all have order two or three. Up to the action of G on the sequences by conjugation, there are 22 conjugacy classes and under the action of the automorphism group, there are 14 orbits.

The computation was also carried out for $p = 19$ and $p = 31$. All of these results are summarized in the table below.

	7	11	19	31
Length 4 irredundant generating sets:	252	11935	7695	14880
Conjugacy classes of sets	2	22	4	1
Automorphism classes of sets	2	14	3	1

The fact that for $p = 31$ there is only one automorphism class of length 4 irredundant generating sequences was already known to Philippe Cara of The Vrije Universiteit Brussel [2].

Chapter 3

The Replacement Property

3.1 The Replacement Property

Before stating the definition of the replacement property, there will be some motivation with arguably the nicest type of (abelian) group: a finite dimensional vector space. Let V be an n dimensional vector space over the field F and let $\mathcal{B} = \{v_1, ..., v_n\}$ be a basis. Now, take any set $\mathcal{A} = \{w_1, ..., w_m\}$ of linearly independent vectors in V. Then, a standard linear algebra result says that up to reordering of the v_i, $\{w_1, ..., w_m, v_1, v_2, ..., v_{n-m}\}$ is a basis of V. In Dummit and Foote, Theorem 3, Section 11.1 [7], this is called *A Replacement Theorem* and is related to the classical *The Steinitz Exchange Property.* The idea is to generalize this notion of replacing an element of a basis to arbitrary groups. Instead of looking at bases, the generalization is generating sets. Also, instead of replacing many elements of the generating set, the focus will be on replacing a single element. This leads to the following definition:

Definition 6 (Replacement Property)**.** *A group G satisfies the replacement property for the generating sequence $s = (g_1, ..., g_k)$ if for any g in G, g not the identity, there exists an i so that $s' = (g_1, ..., g_{i-1}, g, g_{i+1}..., g_k)$ generates G.*

A group G is said to satisfy the replacement property for n if it satisfies the replacement property for all sequences of length $n = m(G)$. A variation on an argument of Tarski shows that if the replacement property holds for the integer n, then we must have $N = m(G)$ [3]. Why is the replacement property useful? It turns out that the replacement property provides an excellent handle for studying generating sequences of finite groups. For example, knowing if a group satisfies the replacement property can give information about the generating sequence structure of the direct product of groups [3].

With the definition above, it is clear that vector spaces satisfy the replacement property because one can take any basis and any nonzero vector to give a new basis with one of the basis elements replaced with the chosen nonzero vector. As another example, consider S_3. As was observed earlier, one can use one transposition and one 3-cycle to generate the group. Given any other transposition, the initial one can be replaced with the new one to produce a new generating sequence. Likewise, any 3-cycle can replace the chosen one and still generate the group. A similar argument works for the sequences which have two transpositions. In fact, we have the following theorem due to Dan Collins [3]:

Theorem 8. *For all n, S_n satisfies the replacement property.*

However, not all groups satisfy the replacement property. For example, consider $G \cong Q_8$, the Quaternion Group. If we think of G as the elements $\{\pm 1, \pm i, \pm j \pm k\}$, then it is clear that i, j is a generating sequence of G. However, we cannot replace either of i or j in this sequence with -1 because $i^2 = j^2 = -1$ and so $\{-1, i\}$ is a proper subgroup of G. More generally if the Frattini subgroup of a group is nontrivial, then the nontrivial non-generating elements will cause G to fail the replacement property. For Q_8, $\{\pm 1\}$ is the Frattini subgroup and so it fails the replacement property. One could modify the definition of the replacement property to exclude such cases. Either way, there are examples of groups which are Frattini free and still fail the replacement property. For $p \equiv +1 \mod 8$, PSL(2, p) is such a group. Before showing this, the definition of replacement property must be reworked slightly. This property has been phrased in terms of generating sequences, but it can be restated in terms of certain sets of maximal subgroups. To begin, the notion of a sequence of subgroups being in *General Position* is defined:

Definition 7 (General Position)**.** *Let $I = \{1, ..., n\}$. A sequence $(H_1, ..., H_n)$ of proper subgroups of a finite group G are said to be in General Position if $\cap_{i \in J} H_i \subsetneq \cap_{i \in K} H_i$ for all $J, K \subset I$ and $K \subsetneq J$.*

For example, if one has a sequence (H_1, H_2, H_3) of proper subgroups, then they are in general position if

$$H_1 \cap H_2 \subsetneq H_1, H_2$$
$$H_1 \cap H_3 \subsetneq H_1, H_3$$
$$H_2 \cap H_3 \subsetneq H_2, H_3$$
$$H_1 \cap H_2 \cap H_3 \subsetneq H_1 \cap H_2, H_1 \cap H_3, H_2 \cap H_3$$

It is not yet clear how this is related to the replacement property. Before making this connection, the idea of subgroups in general position needs to be related to sequences. Let $(M_1, ..., M_n)$ be a sequence of maximal subgroups of a finite group G and let $(g_1, .., g_n)$ be a sequence of elements of G. These two sequences are said to correspond to each other if $g_i \notin M_i$ for any $i \in \{1, ..., n\}$ but $g_j \in M_i$ whenever $j \neq i$. With this connection, there is a relationship between maximal subgroups in general position and irredundant generating sequences [3]:

Proposition 21. *If $(g_1, ..., g_n)$ is an irredundant generating sequence, then it corresponds to a sequence of maximal subgroups $(M_1, ..., M_n)$ in general position.*

Proof. Let $H_i = \langle g_1, ..., g_{i-1}, g_{i+1}, ..., g_n \rangle$. Since $(g_1, ..., g_n)$ is an irredundant generating sequence, H_i is a proper subgroup of G. Therefore, there exists a maximal subgroup $H_i \leq M_i$. Note that $g_i \notin M_i$, since M_i is also a proper subgroup, but $g_j \in M_i$ for all $j \neq i$ by construction. Therefore, $(M_1, ..., M_n)$ corresponds to $(g_1, ..., g_n)$. Now, one needs to show that the maximal subgroups are in general position. By construction, for $J \subset I = \{1, .., n\}$ then $g_j \in \cap_{i \in J} M_i$ if and only if $j \notin J$. Therefore, the subgroups $\cap_{i \in J} M_i$ are all distinct as no two of them intersect $\{g_1, ..., g_n\}$ in the same way. □

Now that a relationship exists between irredundant generating sequences and maximal subgroups in general position, one can construct a criteria on maximal subgroups for establishing the replacement property. Using the same ideas as in the previous proposition, one can prove the following [3]

Proposition 22. *Suppose $s = (g_1, ..., g_n)$ is an irredundant generating sequence of a finite group G and $g \in G$ is an element for which s fails the replacement property. Then, there exists a sequence of maximal subgroups of G corresponding to s such that g is in every M_i.*

Proof. If s fails the replacement property for g, then for each i, the sequence $(g_1, ..., g_{i-1}, g, g_{i+1}, ..., g_n)$ generates a proper subgroup H_i of G. Pick a maximal subgroup $H_i \leq M_i$. Then, $(M_1, ..., M_n)$ corresponds to s by definition and furthermore, $g \in \cap M_i$ by construction. □

An equivalent (contraposition) statement that is more useful in practice is the following [3]:

Corollary 3. *Suppose that $s = (g_1, ..., g_n)$ is an irredundant generating sequence of the finite group G. If every sequence of maximal subgroups $(M_1, ..., M_n)$ corresponding to g intersects trivially, then s satisfies the replacement property.*

Now, the necessary tools have been established to prove that for certain p, $\mathrm{PSL}(2, \mathrm{p})$ satisfies the replacement property. This simple proof is due to Professor Keith Dennis. The statement looks very general, but with the conjecture in the previous chapter, it seems like it only applies to four groups: $\mathrm{PSL}(2, 7)$, $\mathrm{PSL}(2, 11)$, $\mathrm{PSL}(2, 19)$ and $\mathrm{PSL}(2, 31)$.

Proposition 23. *Let $G = \mathrm{PSL}(2, \mathrm{p})$ and suppose that $m(G) = 4$. Then, G satisfies the replacement property.*

Proof. Let $s = (g_1, g_2, g_3, g_4)$ be an irredundant generating sequence of length 4 and let (M_1, M_2, M_3, M_4) be a corresponding sequence of maximal subgroups in general position. From Whiston and Saxl if $m = 4$, then at least two of the M_i must be isomorphic to S_4 or A_5.

Let $\lambda(H)$ be the number of primes in the prime decomposition of $|H|$ (with multiplicities). For subgroups H_i in general position, $|H_i \cap H_j| < |H_i|$ for $i \neq j$ and so it must be that $\lambda(H_i \cap H_j) < \lambda(H_i)$. Since $|\mathrm{A}_5| = 60 = 2^2 \times 3 \times 5$, $\lambda(\mathrm{A}_5) = 4$. Similarly, $|\mathrm{S}_4| = 24 = 2^3 \times 3$ and so $\lambda(S_4) = 4$ as well. If M_4 is isomorphic to S_4 or A_5, then $\lambda(M_1 \cap M_4) \leq 3$, $\lambda(M_1 \cap M_2 \cap M_4) \leq 2$ and $\lambda(M_1 \cap M_2 \cap M_3 \cap M_4) \leq 1$. The aim is to show that this intersection is trivial, which is true if and only if $\lambda(\cap M_i) = 0$. Therefore, to find a contradiction, suppose that $\lambda(\cap M_i) = 1$. Then, $\lambda(M_1 \cap M_4) = 3$ and $\lambda(M_1 \cap M_2 \cap M_4) = 2$.

To begin, suppose that one of the $M_i \cong \mathrm{S}_4$. Without loss of generality, suppose that $M_4 \cong \mathrm{S}_4$. Then, consider the sequence $(M_1 \cap M_4, M_2 \cap M_4, M_3 \cap M_4)$ of subgroups in M_4. The subgroups of S_4 are isomorphic to $\mathrm{A}_4, \mathrm{D}_8, \mathrm{S}_3, \mathbb{Z}_2^2, \mathbb{Z}_4, \mathbb{Z}_3, \mathbb{Z}_2, \{e\}$. The only ones with $\lambda = 3$ are A_4 and D_8. The intersection of any two of these will be a subgroup of A_4 or D_8 with $\lambda = 2$, of which there are only two: $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$.

Before proceeding, a quick fact is needed about $\mathbb{Z}_2^2 \leq S_4$. Let $V \leq \mathrm{D}_8 \leq \mathrm{S}_4$ be isomorphic to a subgroup $\mathbb{Z}_2^2$. It is a standard exercise to show that for $G = S_4$, the derived subgroup $[G, G] = A_4$ and the second derived subgroup $[[G, G], [G, G]]$ isomorphic to V. The derived series are all normal subgroups (in G) and so V is normal in G. Since V sits inside a Sylow-2 subgroup (D_8) and all the Sylow-2 subgroups conjugate to each other, it must be that V sits inside each of the D_8. The intersection of distinct D_8 must therefore be V since 4 is the largest proper divisor of 8. Therefore, the intersection between any two $M_i \cap M_4$ must be this V. Intersecting the two will again result in V and so the groups are not in general position. Therefore, all possible maximal subgroups intersect trivially and thus G satisfies the replacement property.

Next, suppose that one of the $M_i \cong A_5$. Without loss of generality, suppose that $M_4 \cong \mathrm{A}_5$. Then, consider the sequence $(M_1 \cap M_4, M_2 \cap M_4, M_3 \cap M_4)$ of subgroups in M_4. The subgroups of A_5 are isomorphic to $\mathrm{A}_4, \mathrm{D}_{10}, \mathbb{Z}_5, \mathrm{S}_3, \mathbb{Z}_2^2, \mathbb{Z}_2, \{e\}$. The only one with $\lambda = 3$ is A_4. The intersection of any two of these will be a subgroup of A_4 with $\lambda = 2$, of which there is only one: $\mathbb{Z}_2^2$.

However, the claim is that two copies of A_4 in A_5 must intersect in a cyclic subgroup (including the trivial group). Suppose instead that there are two subgroups $H_1, H_2 \cong \mathrm{A}_4$ that contain the same copy of V. It was already discussed that V is normal in H_1, H_2 (and as the Sylow-2 subgroup, is unique). Note that $H_1, H_2 \leq \mathrm{N}_{\mathrm{A}_5}(V)$. But, V cannot be normal in A_5, because this is a simple group. On the other hand, A_4 is maximal. Therefore, $H_1 = H_2 = \mathrm{N}_{\mathrm{A}_5}(V) \cong \mathrm{A}_4$. Thus, two distinct H_i cannot intersect in V and so G satisfies the replacement property.

□

It turns out that $\mathrm{PSL}(2, \mathrm{p})$ does not satisfy the replacement property in general. The data in Appendix B.1 leads to the following conjectured theorem:

Theorem 9. *Let p be a prime with $p \equiv +1 \mod 8$. Let $G = \mathrm{PSL}(2, \mathrm{p})$. If $m(G) = 3$, then G fails the replacement property.*

Proof. In order to show that G fails the replacement property, this proof produces an explicit example of an element $w \in G$ and a length three generating set $\{g_1, g_2, g_3\}$ such that replacing any g_i by w will result in a set which no longer generates G. The discussion will be grounded in the properties of elements in the examples of Appendix B.1. The task is to extend these attributes to elements for any $p \equiv 1 \mod 8$. Since it is easier to work with matrices than with elements in $\mathrm{PSL}(2, \mathrm{p})$, often, elements in $\mathrm{SL}(2, \mathrm{p})$ will be used instead of their projections into G. For the sake of clarity, capital letters will denote elements in $\mathrm{SL}(2, \mathrm{p})$ and lower case letters will denote their projections in $G = \mathrm{PSL}(2, \mathrm{p})$.

Consider four elements in G, denoted a, b, c, w. If $\pi : \mathrm{SL}(2, \mathrm{p}) \to G$, is the canonical projection, then let A, B, C, W be such that $\pi(A) = a, \pi(B) = b, \pi(C) = c$ and $\pi(W) = w$. Using the form of A, B, C, W as in Appendix B.1 it will be shown that a, b, c, w have the required properties and that they exist for all relevant primes. In particular, the claim is that $\{wa, wb, wc\}$ is a length 3 irredundant generating set of G, but the element w will be such that it cannot replace any of these elements to recover a generating sequence. For $r, s, t, u \in \mathbb{F}_p$ let

$$A = \begin{pmatrix} r & s \\ s & -r \end{pmatrix} \quad B = \begin{pmatrix} t & u \\ u & -t \end{pmatrix} \quad W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{3.1}$$

Notice that W also came up in proving Dickson's Theorem. Since A and B have determinant 1, $r^2 + s^2 = t^2 + u^2 = -1$. Note that A, B and W are traceless. By Lemma 4, it must be that A, B and W have order 4 and a, b and w have order 2. Furthermore, notice that

$$WA = \begin{pmatrix} -s & r \\ r & s \end{pmatrix} \quad WB = \begin{pmatrix} -u & t \\ t & u \end{pmatrix} \quad AW = \begin{pmatrix} s & -r \\ -r & -s \end{pmatrix} \quad BW = \begin{pmatrix} u & -t \\ -t & -u \end{pmatrix} \tag{3.2}$$

and so $AW = -WA$ and similarly, $BW = -WB$. Since AW, AB are still traceless, aw and bw also have order 2. Therefore, $\langle a, w \rangle = \{a, w, aw, \mathrm{id}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and likewise, $\langle b, w \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Now, generically write

$$C = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{3.3}$$

where $\alpha\delta - \beta\gamma = 1$. The examples in the data show that c has order 2, so $\alpha + \delta = 0$. Furthermore, $\mathrm{Tr}(WC) = +1$ which by Lemma 4 means that the order of wc is 3. The product WC has the form

$$WC = \begin{pmatrix} -\gamma & -\delta \\ \alpha & \beta \end{pmatrix} \tag{3.4}$$

and so the condition that $\mathrm{Tr}(WC) = +1$ becomes $\beta - \gamma = +1$. In the data, it appears that one can make the choice $\beta = 0$ so that $\gamma = -1$. Furthermore since $\alpha\delta - \beta\gamma = 1$, $\beta = 0$ implies that $\alpha = \delta^{-1}$ and since

the trace of C is zero, $\alpha = -\delta$. Thus, $\alpha^{-1} = -\alpha$, or α has order 4 in $\mathbb{F}_p$. Does such an element exist? Since $p \equiv 1 \mod 8$, $8|(p-1)$, which is the order of the cyclic group $\mathbb{F}_p^*$. Therefore, $\mathbb{F}_p^*$ has an element of order 8 and so also has an element of order 4. Fix such an element and call it i. Then,

$$C = \begin{pmatrix} -i & 0 \\ -1 & i \end{pmatrix} \tag{3.5}$$

Note that

$$w(cw)w^{-1} = wcww = wc \tag{3.6}$$

However, since $(cw)(wc) = 1$,

$$w(cw)w^{-1} = (cw)^{-1} \tag{3.7}$$

Therefore, $\langle c, w\rangle = \langle w, wc\rangle = \langle x, y | x^2 = y^3 = 1, xyx^{-1} = y^{-1}\rangle \cong \mathrm{S}_3$. The last isomorphism in the preceding sentence is due to a standard presentation of S_3, for example given in Section 1.2 of [6]. The next step is to show that $\langle aw, cw\rangle \cong \mathrm{S}_4$. The idea is to use the trace technology laid out in Theorem 4. In order to apply the theorem, some nonzero traces are required. The trace of WA is 0 and the trace of $WC = +1$. Therefore, the Theorem 4 only applies if $WCWA$ has a particular trace. Multiplying these elements gives rise to the following matrix:

$$WCWA = \begin{pmatrix} -s - ir & r - is \\ is & -ir \end{pmatrix} \tag{3.8}$$

so that $\mathrm{tr}(WCWA) = -s - 2ir$. The required constraint from the Theorem is that $(s + 2ir)^2 = 2$. If this holds, then Theorem 4 says that $\langle aw, cw\rangle \cong \mathrm{S}_4$ if $\mathrm{tr}\left([WA, WC]\right) = +1$. Simple arithmetic using the forms of A, C and W yields the following computation:

$$\begin{aligned} \mathrm{tr}\left([WA, WC]\right) &= \mathrm{tr}\left[(WA)(WC)(WA)^{-1}(WC)^{-1}\right] \\ &= \mathrm{tr}\left[WAWCAWCW\right] \\ &= -\mathrm{tr}\left[(AWC)^2\right] \\ &= -2i^2s^2 + 4isr - r^2 + 2i^2r^2 \\ &= 2s^2 + 4isr - 3r^2 \end{aligned} \tag{3.9}$$

Setting this expression equal to 1 and using the constraint that $s^2 + r^2 = -1$ (from the determinant), one finds that

$$3s^2 + 4isr - 2r^2 = 0 \tag{3.10}$$

which has solution

$$r = \left(i \pm \frac{\sqrt{2}}{2}\right) s \tag{3.11}$$

and then inserting this back into $s^2 + r^2 = -1$, one arrives at

$$s^2 = -\frac{2}{9} \pm \frac{4}{9} i\sqrt{2} = \left[\frac{1}{3}\left(2i \pm \sqrt{2}\right)\right]^2 \tag{3.12}$$

and so the question has simply boiled down to the existence of an element $\zeta \in \mathbb{F}_p$ such that $\zeta^2 = 2$ (and $p \neq 3$, so 3^{-1} makes sense). It is a standard result in elementary number theory (c.f. [12]) that 2 has

a square root if $p \equiv \pm 1 \mod 8$ (fix one and call it $\sqrt{2}$). Therefore, all that is left to show in order to apply Theorem 4 is for $\mathrm{tr}(WCWA) = -s - 2ir$ to have the correct form. Using the expressions for r and s above, a quick computation shows that $-s - 2ir = \sqrt{2}$, as required by the theorem. Therefore, $\langle wa, wc\rangle \cong \mathrm{S}_4$. An analogous discussion shows that if one fixes s as one solution to Eq. 3.12, then picking the other solution for u and constructing t as was done for r will give $\langle wb, wc\rangle \cong \mathrm{S}_4$ as well.

The strategy to demonstrate that w cannot replace wa, wb or wc will be to show that w is in the subgroups generated by (maximal subgroups containing) $\langle wa, wc\rangle$, $\langle wb, wc\rangle$ and $\langle wa, wb\rangle$. The first step in this process is to prove that $\langle wa, wc\rangle = \langle a, c, w\rangle$. Note that

$$WAWC = -AWWC = AC \tag{3.13}$$

and since $(ac)(ca) = 1$, $ac, ca \in \langle wa, wc\rangle$. Furthermore, since $(wc)(cw) = (aw)(wa) = 1$, $cw, wc, aw, wa \in \langle wa, wc\rangle$. Now, take any element $x \in \langle a, c, w\rangle$. By construction, such an element can be written as a string in the alphabet $a, c, w, a^{-1} = a, c^{-1} = c, w^{-1} = w$ (no need to worry about uniqueness). Suppose that x can be written with an even number of letters in the string. Then, this element is in $\langle wa, wc\rangle$ because every possible pairing of letters from the above alphabet is in $\langle wa, wc\rangle$. For example, consider the word

$$x = awcwaccwawcw \tag{3.14}$$

One can group these letters into pairs:

$$x = (aw)(cw)(ac)(cw)(aw)(cw) \tag{3.15}$$

and then it is clear that every element in parenthesis is in $\langle wa, wc\rangle$. Instead of an even number of letters, suppose that x can be written as a string with an odd number of letters from the alphabet. Then, one can form x from a string in $\langle wa, wc\rangle$ by adding one of a, b, w. This is clear because if there are n letters that make up x, then $n - 1$ will be an even number and so the substring of the first $n - 1$ letters will be in $\langle wa, wc\rangle$ by the preceding argument. Thus, every element in $\langle a, c, w\rangle$ can be formed from an element in $\langle wa, wc\rangle$ by adding one of a, c, w or id. This means that

$$|\langle a, c, w\rangle| \leq 4|\langle wa, wc\rangle| \tag{3.16}$$

However, from above, $\langle wa, wc\rangle \cong \mathrm{S}_4$ so $|\langle a, c, w\rangle| \leq 96$. Furthermore, by Dickson's Theorem, S_4 is maximal in G and so no proper subgroup can contain $\langle wa, wc\rangle$. Therefore, either $\langle a, c, w\rangle = \langle wa, wc\rangle$ or $\langle a, c, w\rangle = G$. Since $p \equiv 1 \mod 8$, $p \geq 17$ so by Proposition 3, $|G| \geq 2448 > 96$ and thus $\langle a, c, w\rangle = \langle wa, wc\rangle$. By an analogous argument, $\langle b, c, w\rangle = \langle wb, wc\rangle$. The last consideration is to study $\langle wa, wb\rangle$. This group is generated by two elements of order 2 and so must be dihedral. To see how large it is, one needs to know the order of $wawb = awwb = ab$. This amounts to computing the trace of AB, which is

$$\mathrm{tr}(AB) = 2(rt + su) = -8i/3 \tag{3.17}$$

This is certainly not zero and a quick arithmetic computation shows that it is also not ± 1 or $\pm\sqrt{2}$. Therefore, by Lemma 4 , the order of ab is more than 4 and so $ab \notin \mathrm{S}_4$. It is also clear that $\langle wa, wb\rangle \neq G$ because G is not dihedral. The final step before concluding is to show that $\langle a, b, w\rangle$ is a proper subgroup of G. This procedure is similar to the one above by considering the index of $\langle wa, wb\rangle$ in $\langle a, b, w\rangle$. Since $wawb = ab \in \langle wa, wb\rangle$, as before, every possible pair of letters in $\langle a, b, w\rangle$ is in $\langle wa, wb\rangle$ and therefore, one arrives at the same bound as earlier:

$$|\langle a, b, w\rangle| \leq 4|\langle wa, wb\rangle| \tag{3.18}$$

Recall that $\langle wa, wb\rangle$ is dihedral. From Dickson's Theorem, the largest dihedral subgroup of G has order $p + 1$. Therefore

$$|\langle a, b, w\rangle| \leq 4|\langle wa, wb\rangle| \leq 4(p+1) < \frac{p(p+1)(p-1)}{2} \tag{3.19}$$

Since for $p \geq 17$, $p(p-1)/2 = 136$. Let M be a maximal subgroup of G which contains $\langle wa, wb\rangle$. Since $\langle a, b, w\rangle$ is proper and contains $\langle wa, wb\rangle$, $w \in M$.

Now, all the machinery is in place to conclude. The set $\{wa, wb, wc\}$ will generate G because $wb \notin \langle wa, wc\rangle$ and $\langle wa, wc\rangle$ is maximal, so the subgroup generated by all three elements, which contains a maximal subgroup, must be all of G. Furthermore, it is clear that w cannot replace any of wa, wb, wc because w is in the maximal subgroup containing each pair. Explicitly, the set $\{w, wb, wc\}$ cannot generate G because $w \in \langle wb, wc\rangle \cong \mathrm{S}_4$. The same holds for replacing wb. Finally, w cannot replace wc because the maximal subgroup which contains $\langle wa, wb\rangle$ also contains w and so $\langle w, wa, wb\rangle \leq M < G$. Therefore G fails the replacement property if $m(G) = 3$. □

Appendix A

GAP Scripts

A.1 Applying Dickson's Theorem

```
PSLMax:=function(p)
    #This program returns all of the maximal subgroups of PSL(2,p) via Dickson's Theorem.
    local G,D,H,h,A,Q,out,q;
    G:=PSL(2,p);
    out:=[];
    #Note that each element of out is of the form [Group,"StructureDescription"]

    #First, get the max subgroups iso to D_{p-1}
    if (p>12) then
      D:=DihedralGroup(p-1);
      H:=IsomorphicSubgroups(G,D);
      for h in H do
        A:=Image(h);
        Q:=RightCosets(G,A); #This is a subroutine which generates \\
         #the right cosets of A in G.
        for q in Q do
          Append(out,[[A^Representative(q),"D_{p-1}"]]);
        od;
      od;
    fi;

    #Second, get the max subgroups iso to D_{p+1}
    if (not (p=7 or p=9)) then
      D:=DihedralGroup(p+1);
      H:=IsomorphicSubgroups(G,D);
      for h in H do
        A:=Image(h);
        Q:=RightCosets(G,A);
        for q in Q do
          Append(out,[[A^Representative(q),"D_{p+1}"]]);
        od;
      od;
    fi;

    #Third, get the max subgroups iso to Z_p semi Z_{(p-1)/2}
    D:=Representative(ConjugacyClassesMaximalSubgroups\\
     (AutomorphismGroup(DihedralGroup(2*p)))[1]);
    H:=IsomorphicSubgroups(G,D);
    for h in H do
      A:=Image(h);
      Q:=RightCosets(G,A);
      for q in Q do
          Append(out,[[A^Representative(q),"Z_p semi Z_{(p-1)/2}"]]);
      od;
    od;

    #Fourth, get the max subgroups iso to A5
    if (p mod 10 = 1 or p mod 10 = 9) then
      D:=AlternatingGroup(5);
      H:=IsomorphicSubgroups(G,D);
      for h in H do
        A:=Image(h);
        Q:=RightCosets(G,A);
        for q in Q do
          Append(out,[[A^Representative(q),"A5"]]);
        od;
```

```
      od;
    fi;

    #Fifth, get the max subgroups iso to A4
    if ((p mod 8 = 3 or p mod 8 = 5) and not(p mod 10 = 1 or p mod 10 = 9)) then
      D:=AlternatingGroup(4);
      H:=IsomorphicSubgroups(G,D);
      for h in H do
        A:=Image(h);
        Q:=RightCosets(G,A);
        for q in Q do
          Append(out,[[A^Representative(q),"A4"]]);
        od;
      od;
    fi;

    #Finally, get the max subgroups iso to S4
    if (p mod 8 = 1 or p mod 8 = 7) then
      D:=SymmetricGroup(4);
      H:=IsomorphicSubgroups(G,D);
      for h in H do
        A:=Image(h);
        Q:=RightCosets(G,A);
        for q in Q do
          Append(out,[[A^Representative(q),"S4"]]);
        od;
      od;
    fi;

    return out;

end;


ConjugateSG:=function(H,g,G)
    #Given a subgroup H of a group G and an element g\in G, this returns \\
     #the conjugate subgroup of H in G by the conjugation of g.
    local h,new;
    new:=[];
    for h in Elements(H) do
        Append(new,[g^(-1)*h*g]);
    od;
    return Subgroup(G,new);
end;
```

A.2 Computing $m(\mathrm{PSL}(2,\mathrm{p}))$

```
FindSeq:=function(p)
    #This program finds all sequences of length 4 which contain an A5 as one\\
     #of the associated maximal subgroups in General Position.
    local G,gens,g,igens,ig,A5,H,elm,A,s,found,temp,c1,c2,n1,n2,temp2,h,a;
    G:=PSL(2,p);
    s:=Size(G);
    A:=ConjugacyClasses(G);
    A:=Elements(A);
    A:=Filtered(A,x->((Order(Representative(x))=2) or (Order(Representative(x))=3)));

    gens:=[];
    igens:=[];
    A5:=AlternatingGroup(5);
    H:=IsomorphicSubgroups(G,A5);

    #There are only 25 irredundant generating sets of A5 of length 3
    #up to action of A5 by conjugation on itself. We then list them \\
    #here and insert them one by one in PSL(2,p) and try to extend them. \\

    gens:=Set([ [ (3,4,5), (2,3)(4,5), (1,2)(4,5) ], [ (3,4,5), (2,3)(4,5), (1,2)(3,4) ],
  [ (3,4,5), (2,3)(4,5), (1,2)(3,5) ], [ (3,4,5), (2,3)(4,5), (1,3)(4,5) ],
  [ (3,4,5), (2,3)(4,5), (1,4,5) ], [ (3,4,5), (2,3)(4,5), (1,4)(3,5) ],
  [ (3,4,5), (2,3)(4,5), (1,5,4) ], [ (3,4,5), (2,3)(4,5), (1,5)(3,4) ],
  [ (3,4,5), (2,3,4), (1,3,4) ], [ (3,4,5), (2,3,4), (1,4,3) ],
  [ (3,4,5), (2,3,4), (1,5)(3,4) ], [ (3,4,5), (2,3,5), (1,2)(3,5) ],
  [ (3,4,5), (1,2)(4,5), (1,3)(4,5) ], [ (3,4,5), (1,2)(4,5), (1,4)(3,5) ],
  [ (3,4,5), (1,2)(4,5), (1,5)(3,4) ], [ (2,3)(4,5), (2,4)(3,5), (1,2)(4,5) ],
  [ (2,3)(4,5), (2,4)(3,5), (1,2)(3,4) ], [ (2,3)(4,5), (2,4)(3,5), (1,2)(3,5) ],
  [ (2,3)(4,5), (1,2)(4,5), (1,2)(3,4) ], [ (2,3)(4,5), (1,2)(4,5), (1,2)(3,5) ],
  [ (2,3)(4,5), (1,2)(4,5), (1,3)(2,4) ], [ (2,3)(4,5), (1,2)(4,5), (1,4)(3,5) ],
  [ (2,3)(4,5), (1,2)(4,5), (1,5)(3,4) ], [ (2,3)(4,5), (1,2)(3,4), (1,4)(2,5) ],
  [ (2,3)(4,5), (1,2)(3,5), (1,5)(2,4) ] ]);

    found:=[];
    for a in A do

        Print("Checking Order: ",Order(Representative(a)),"\n");

        for h in H do
            c1:=1;
            c2:=1;
            n1:=Size(gens);
            n2:=Size(a);

            #Find the image of the generating set
            for g in gens do
                Print(c1/n1,"\n");
                c1:=c1+1;
                igens:=[];
                for elm in g do
                    ig:=ImagesRepresentative(h,elm);
                    Append(igens,[ig]);
                od;

                #Now, let's systematically try adding in one of the elements of order 2
                #for elm in a do #there will be more than one for order 3 considered
```

```
                #as well.

                    temp2:=ShallowCopy(igens);
                    Append(temp2,[elm]);
                    if (Size(Subgroup(G,temp2))=s) then
                        temp:=([temp2[1],temp2[2],temp2[3]]);;
                        if (Size(Subgroup(G,temp))=s) then
                            continue;
                        fi;
                        temp:=([temp2[1],temp2[2],temp2[4]]);;
                        if (Size(Subgroup(G,temp))=s) then
                            continue;
                        fi;
                        temp:=([temp2[1],temp2[3],temp2[4]]);;
                        if (Size(Subgroup(G,temp))=s) then
                            continue;
                        fi;
                        temp:=([temp2[2],temp2[3],temp2[4]]);;
                        if (Size(Subgroup(G,temp))=s) then
                            continue;
                        fi;
                        Append(found,temp2);
                        break;
                    fi;
                od;
                if (Size(found)>0) then
                    break;
                fi;
            od;
            if (Size(found)>0) then
                break;
            fi;
        od;
        if (Size(found)>0) then
            break;
        fi;
    od;
    return found;
end;
```

The same script for S_4 is very similar. The only replacement is for the generating sequences to lift. These are replaced with the following:

```
   #There are only 9 irredundant generating sets of S4 of length 3 up to \\
   #action by Aut(S4)
    gens:=Set([ [ (3,4), (2,3), (1,2) ], [ (3,4), (2,3), (1,2)(3,4) ],
     [ (3,4), (2,3), (1,3) ], [ (3,4), (2,3), (1,3)(2,4) ],
     [ (3,4), (2,3,4), (1,2)(3,4) ], [ (3,4),(2,3,4), (1,3,4) ],
     [ (3,4), (2,3,4), (1,3)(2,4) ],  [ (3,4), (2,3,4), (1,4,3) ],
     [ (3,4), (2,3,4), (1,4)(2,3) ] ]);
```

A.3 Converting Matrix Representations over $\mathbb{F}_p$

```
decode:=function(n,p)
    #Given GAPs representation of elements of F_p converts such a \\
    #representation to one that is used to in Z_p
    local i,m,gen;

    gen:=PrimitiveRootMod(p);

    if (n=0*Z(p)) then
        return 0;
    fi;

    for i in [0..p] do
        if ((Z(p)^i-n=0*Z(p))) then
            m:=i;
            #Print(i,"\n");
            break;
        fi;
    od;
    return gen^m mod p;
end;

decodeMat:=function(M,p)
    #This function decodes a matrix
    local Mout;
    Mout:=[[0,0],[0,0]];
    Mout[1][1]:=decode(M[1][1],p);
    Mout[2][1]:=decode(M[2][1],p);
    Mout[1][2]:=decode(M[1][2],p);
    Mout[2][2]:=decode(M[2][2],p);
    return Mout;
end;
```

Appendix B

Data

B.1 Replacement Property Computations

```
p=17

<a,b,c,w> PSL(2,17)
<a,b,w> D16
<a,c,w> S4
<b,c,w> S4
Intersection(<a,b,w>,<a,c,w>,<b,c,w>)=Z2
<a,w> C2 x C2
<b,w> C2 x C2
<c,w> S3
a [ [ 5, 12 ], [ 12, 12 ] ]
b [ [ 10, 1 ], [ 1, 7 ] ]
c [ [ 4, 0 ], [ 16, 13 ] ]
w [ [ 0, 16 ], [ 1, 0 ] ]
<a,b> D16
<a,c> D8
<b,c> D8
<wa,wb> D16
<wa,wc> S4
<wb,wc> S4
```

```
p=41

<a,b,c,w> PSL(2,41)
<a,b,w> D40
<a,c,w> S4
<b,c,w> S4
Intersection(<a,b,w>,<a,c,w>,<b,c,w>)=Z2
<a,w> C2 x C2
<b,w> C2 x C2
<c,w> S3
a [ [ 34, 14 ], [ 14, 7 ] ]
b [ [ 35, 39 ], [ 39, 6 ] ]
c [ [ 9, 0 ], [ 40, 32 ] ]
w [ [ 0, 40 ], [ 1, 0 ] ]
<a,b> D40
<a,c> D8
<b,c> D8
<wa,wb> D40
<wa,wc> S4
<wb,wc> S4
```

```
p=89

<a,b,c,w> PSL(2,89)
<a,b,w> D88
<a,c,w> S4
<b,c,w> S4
Intersection(<a,b,w>,<a,c,w>,<b,c,w>)=Z2
<a,w> C2 x C2
<b,w> C2 x C2
<c,w> S3
a [ [ 27, 31 ], [ 31, 62 ] ]
b [ [ 56, 45 ], [ 45, 33 ] ]
c [ [ 34, 0 ], [ 88, 55 ] ]
w [ [ 0, 88 ], [ 1, 0 ] ]
<a,b> D88
<a,c> D8
<b,c> D8
<wa,wb> D88
<wa,wc> S4
<wb,wc> S4
```

```
p=97

<a,b,c,w> PSL(2,97)
<a,b,w> D96
<a,c,w> S4
<b,c,w> S4
Intersection(<a,b,w>,<a,c,w>,<b,c,w>)=Z2
<a,w> C2 x C2
<b,w> C2 x C2
<c,w> S3
a [ [ 11, 84 ], [ 84, 86 ] ]
b [ [ 44, 87 ], [ 87, 53 ] ]
c [ [ 75, 0 ], [ 96, 22 ] ]
w [ [ 0, 96 ], [ 1, 0 ] ]
<a,b> D48
<a,c> D8
<b,c> D8
<wa,wb> D48
<wa,wc> S4
<wb,wc> S4
```

Bibliography

[1] Arnaud Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[2] Philippe Cara. On the unique independent set of four elements in PSL(2,31). Combinatorics '04 Conference, 2004.

[3] Dan Collins. *Generating Sequences of Finite Groups.* Unpublished, 2012.

[4] Daniel Collins. *Generating Sequences of Finite Groups.* Senior Thesis. Cornell University Mathematics Department, 2010.

[5] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory.* with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[6] David S. Dummit and Richard M. Foote. *Abstract algebra.* John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[7] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[8] Monique Gradolato and Bruno Zimmermann. Extending finite group actions on surfaces to hyperbolic 3-manifolds. *Math. Proc. Cambridge Philos. Soc.*, 117(1):137–151, 1995.

[9] Pierre Antoine Grillet. *Abstract algebra*, volume 242 of *Graduate Texts in Mathematics.* Springer, New York, second edition, 2007.

[10] Robert M. Guralnick. Generation of simple groups. *J. Algebra*, 103(1):381–401, 1986.

[11] Darryl McCullough. *Exceptional subgroups of SL(2,F).* Unpublished.

[12] J.H. Silverman. *A friendly introduction to number theory.* Pearson Prentice Hall, 2006.

[13] M. Suzuki. *Group theory.* Number v. 1 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1982.

[14] Julius Whiston. Maximal independent generating sets of the symmetric group. *J. Algebra*, 232(1):255–268, 2000.

[15] Julius Whiston. *The Minimal Generating Sets of Maximal Size of Selected Groups.* Ph.D. Thesis. Cambridge University, 2001.

[16] Julius Whiston and Jan Saxl. On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$. *J. Algebra*, 258(2):651–657, 2002.