Dickson's Classification of Finite Subgroups of the Two-dimensional Special Linear Group over an Algebraically Closed Field

Christopher Butler

December 18, 2019

Popular Science Summary

In order to explain what this paper is about, it is necessary to first define a few of the mathematical concepts which it concerns. A *group* is a set of objects, called *elements*, together with a rule, called an *operation*, which tells us how two elements combine with each other to make a third. Furthermore, to be considered a group it must also satisfy 4 conditions, called *axioms*. One of which is that the group must be *closed* under it's operation. This means that whenever any two elements in the group are combined, the resulting element is also part of the group. The remaining axioms require that the group must also be *associative*, have an *identity* element and each element must have an *inverse*. The way in which the elements in a group act with each other is called the group's *structure*. If 2 groups have the same number of elements and share the same structure, then they are regarded as being *isomorphic* to each other, which essentially means that they equivalent. Many everyday things can be regarded as groups, such as the symmetries of geometrical objects, or the number systems we use.

The set of 2 x 2 matrices whose *determinant* is equal to 1, together with the operation of ordinary matrix multiplication, forms a group called the *special linear group*. This is a group because the product of 2 matrices has a determinant equal to the product of the determinants of the 2 matrices, so since 1 x 1 = 1, this new element also belongs to the group, hence the axiom of being closed is satisfied. Furthermore, it is crucial that the entries in the matrices are taken from a specified *ring* or *field*. Rings and fields are, like groups, abstract mathematical objects, albeit they satisy even more axioms than groups do. Crucially, rings and fields have both an additive and a multiplicative identity.

This paper focuses on $SL(2, F)$, which is the two-dimensional special linear group whose entries are taken from an *algebraically closed* field. Algebraically closed fields are infinite in size, which means that the resulting special linear group is also infinite. A *subgroup* of a group is simply a group with the added requirement that each of it's elements must also belong to the original group. Thus a finite subgroup of $SL(2, F)$ is any finite set of elements belonging to this infinite group $SL(2, F)$, which satisfy the 4 axioms of being a group.

This paper classifies all the possible structures which a finite subgroup of $SL(2, F)$ could have. The result has implications within the study of finite *simple* groups. This classification was first done by American mathematician Leonard Eugene Dickson in 1901. The purpose of this reformulation is to make it accessible to a wider audience by providing a more detailed explanation at the various stages of the proof.

Abstract

This paper is a reformulation of Leonard Dickson's complete classification of the finite subgroups of the two-dimensional special linear group over an arbitrary algebraically closed field, $SL(2, F)$. The approach is to construct a class equation of the conjugacy classes of maximal abelian subgroups of an arbitrary finite subgroup of $SL(2, F)$. In turn, this leads to only 10 possible classes of structures of this subgroup up to isomorphism.

Acknowledgements

I would like to take this opportunity to thank my advisor Arne Meurman. This paper would not have been possible without the guidance and insight he gave during our weekly discussions.

Contents

Introduction

The general linear group of degree n is the group formed by the set of n x n invertible matrices, together with the operation of ordinary matrix multiplication, with the entries of each matrix coming from a specific ring or field. The special linear group is a subgroup of the general linear group, namely those matrices with a deteminant equal to 1. In this work, we focus on the two-dimensional case, with entries coming from an algebraically closed field, F. This is denoted by $GL(2, F)$ for the general linear group and $SL(2, F)$ for the special linear group. Recall that an algebraically closed field is a field which contains the roots to any non-constant polynomial in $F[x]$, with coefficients in F. They are infinite in size and two such examples are the field of complex numbers and the field of algebraic numbers.

In 1901, Leonard Eugene Dickson published his book *Linear Groups, with an Exposition of the Galois Field Theory* [3]. In this work, he obtains a complete classification of the finite subgroups of $SL(2, F)$. This paper is a reformulation of Dickson's classification theorem and loosely follows Chapter 3, §6 in Michio Suzuki's book *Group Theory I* [9]. This classification theorem is of particular interest in the study of finite simple groups and Suzuki himself describes it as *one of the indispensable tools in studying the basic properties of linear groups which underlie the concept of p-stability* [9, p.392].

The paper begins with a brief overview of some preliminary requirements which are necessary to the understanding of the proof. They are standard group theory results which may or may not have been covered in a first course given on group theory, the majority of which are cited without proof. A more advanced reader may choose to skip over this chapter.

The main body of work begins in Chapter 1 and focuses on the infinite group $SL(2, F)$. We make some important observations about the conjugacy of the elements in this group and the centre of the group. Some important elements and subgroups of $SL(2, F)$ are defined and their centralisers and normalisers determined. We show that the action of $SL(2, F)$ on the projective line is triply transitive, which is a vital tool used several times throughout the paper in determining group structure.

In Chapter 2 we consider an arbitrary finite subgroup G of $SL(2, F)$. The notion of a *maximal abelian subgroup* is introduced and utilised to construct a class equation, whereby G is partitioned into the conjugacy classes of it's maximal abelian subgroups. This plays a crucial role in determining the possible structures of G. We find that the number and type of these conjugacy classes are restricted to just 6 different cases.

The final chapter examines these 6 cases individually. In each case we determine the possible structures that G could have. The 10 possible structures of G are finally consolidated into the classification theorem.

Chapter 0

Preliminaries

This section briefly outlines some standard group theory results which perhaps may not have been covered in a first course in Group Theory. Since they are not the main focus of this paper, most of the proofs have been omitted. A more advanced reader may choose to skip this first chapter, using it only for reference purposes as and when the results are subsequently cited.

0.1 Some Elementary Theorems

The following theorems are all well-known fundamental results in group theory. If the reader is interested in the proofs, they can be found in Hungerford [6].

Lagrange's Theorem. *Let G be a finite group. Then the order of any subgroup of G divides the order of G.*

First Isomorphism Theorem. *Let $\phi : G \to G'$ be a homomorphism of groups. Then,*

$$G/Ker\ \phi \cong Im\ \phi.$$

Hence, in particular, if ϕ is surjective then,

$$G/Ker\ \phi \cong G'.$$

Second Isomorphism Theorem. *Let H and N be subgroups of G, and $N \lhd G$. Then,*

$$H/H \cap N \cong HN/N.$$

Third Isomorphism Theorem. *Let H and K be normal subgroups of G and $K \subset H$. Then H/K is a normal subgroup of G/K and,*

$$(G/K)/(H/K) \cong G/H.$$

Cauchy's Theorem. *If the order of a finite group G is divisible by a prime number p, then G has an element of order p.*

0.2 Sylow Theory

In 1872, Norweigian mathematician Peter Ludwig Sylow published his theorems regarding the number of subgroups of a fixed order that a given finite group contains. Today these are collectively known as the Sylow Theorems and play a vital role in determining the structure of finite groups. I will use the results of these theorems several times throughout this paper and I state them here without proof. If the reader would like to read further, the proofs can be found in most introductory texts on group theory, such as Bhattacharya [2], except Corollary 0.2 which can be found in Alperin and Bell [1, p.64] .

Definition. Let G be a finite group and p a prime, a **Sylow *p*-subgroup** of G is a subgroup of order p^r, where p^{r+1} does not divide the order of G.

Let p be a prime. A group G is called a ***p*-group** if the order of each of it's elements is a power of p. Similarly, a subgroup H of G is called a ***p*-subgroup** if the order of each of it's elements is a power of p.

In each of the following results, G is a finite group of order $p^r m$, where p is a prime which does not divide m.

First Sylow Theorem. *If p^k divides $|G|$, then G has a subgroup of order p^k.*

Second Sylow Theorem. *All Sylow p-subgroups of G are conjugate.*

Third Sylow Theorem. *The number of Sylow p-subgroups n_p divides m and satisfies $n_p \equiv 1(mod\ p)$.*

Corollary 0.1. *A Sylow p-subgroup of G is unique if and only if it is normal.*

Corollary 0.2. *Any p-subgroup of G is contained in a Sylow p-subgroup.*

0.3 Group Action

Definition. Let G be a group and X be a set. Then G is said to **act** on X if there is a map $\phi : G \times X \to X$, with $\phi(a, x)$ denoted by a^*x, such that for $a, b \in G$ and $x \in X$, the following 2 properties hold:

$$\begin{aligned} &(i) \quad a^*(b^*x) = (ab)^*x, \\ &(ii) \quad {I_G}^*x = x. \end{aligned}$$

The map ϕ is called the **group action** of G on X.

Definition. Let G be a group acting on a set X and let $x \in X$. Then the set,

$$Stab(x) = \{g \in G : gx = x\},$$

is called the **stabiliser** of x in G. Each g in $S_G(x)$ is said to **fix** x, whilst x is said to be a **fixed point** of each g in $S_G(x)$. Also, the set,

$$\text{Orb}(x) = \{gx : g \in G\},$$

is called the **orbit** of x in G.

The orbit and the stabiliser of an element are closely related. The following theorem is a consequence of this relationship and it will be useful throughout this paper.

Orbit-Stabiliser Theorem. *Let G be a finite group acting on a set X. Then for each $x \in X$,*

$$|G| = |\text{Orb}(x)||\text{Stab}(x)|.$$

The following standard theorem will all play a vital roll later on.

Theorem 0.3. *Let G be a group and H a subgroup of G of finite index n. Then there is a homomorphism $\phi : G \longrightarrow S_n$ such that,*

$$ker(\phi) = \bigcap_{x \in G} xHx^{-1}.$$

Proof. See [2, p.110] for proof. □

0.4 Conjugation

Definition. Let G be a group and a an element of G. An element $b \in G$ is said to be **conjugate** to a if $b = xax^{-1}$ for some $x \in G$.

Let H_1 be a proper subgroup of G and fix $x \in G \setminus H_1$. The set $H_2 = \{g \in G : g = xh_1x^{-1}, \forall h_1 \in H_1\}$ is said to be a **conjugate subgroup** of H_1. We write $H_2 = xH_1x^{-1}$. It is trivial to show that H_2 is a subgroup of G.

Conjugation plays an important roll thoughout the paper, in particularly the following properties about conjugate elements and subgroups.

Proposition 0.4. *Let a, b be conjugate elements of a group G and A, B be conjugate subgroups of G. Then the following properites hold:*

(i) If either a or b has finite order, then both a and b have the same order.

(ii) $A \cong B$.

Proof. (i) Since a and b are conjugate elements in G, $b = xax^{-1}$ for some $x \in G$. Suppose that b has finite order and $b^k = I_G$ for some $k \in \mathbb{Z}^+$,

$$I_G = b^k = (xax^{-1})^k = xa^kx^{-1} \Rightarrow a^k = I_G.$$

Alternatively suppose that a has finite order and $a^k = I_G$ for some $k \in \mathbb{Z}^+$,

$$a^k = I_G \Rightarrow I_G = xa^kx^{-1} = (xax^{-1})^k = b^k.$$

Thus $a^k = I_G \iff b^k = I_G$. Thus a and b have the same order.

(ii) Since A and B are conjugate, there exists some $x \in G$ such that $B = xAx^{-1}$. Define the map ϕ by,

$$\begin{aligned} \phi : A &\longrightarrow xAx^{-1}, \\ a_1 &\longmapsto xa_1x^{-1}. \end{aligned} \qquad (\forall\, a_1 \in A)$$

We show that ϕ is a homomorphism between A and $B = xAx^{-1}$.

$$\phi(a_1a_2) = xa_1a_2x^{-1} = (xa_1x^{-1})(xa_2x^{-1}) = \phi(a_1)\phi(a_2).$$

Now consider an arbitrary $k \in ker(\phi)$.

$$k \in ker(\phi) \iff \phi(k) = I_G \iff xkx^{-1} = I_G \iff k = I_G.$$

So $ker(\phi) = \{I_G\}$ which means ϕ is injective. Now let $b_1 \in B = xAx^{-1}$. Thus $b_1 = xa_1x^{-1}$ for some $a_1 \in A$. Since $a_1 \in A$, $\phi(a_1) = xa_1x^{-1} = b_1$ and so ϕ is surjective. Thus ϕ is an isomorphism and A and B are isomorphic.

□

The final part of this proposition is an important result which shows that since conjugate subgroups are isomorphic, conjugation preserves group structure and properties. In particular, conjugate subgroups have the same cardinality and if one is abelian or cyclic, then so is the other.

0.5 Automorphism

Definition. An **automorphism** of a group G is a isomorphism from G onto itself. The set of all automorphisms of G forms a group under composition and is denoted by $Aut(G)$.

An **inner automorphism** is an automorphism whereby G acts on itself by conjugation. That is, each $g \in G$ induces a map, $i_g : G \to G$, where $i_g(x) = gxg^{-1}$ for each $x \in G$. The set of all inner automorphisms is denoted by $Inn(G)$ and is a normal subgroup of $Aut(G)$ (For proof of this see [2, p.104].

0.6 Direct Product

Definition. If $G_1, G_2, ..., G_n$ are groups, we define a coordinate operation on the Cartesian product $G_1 \times G_2 \times ... \times G_n$ as follows:

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n),$$

where $a_i, b_i \in G_i$. It is easy to verify that $G_1 \times G_2 \times ... \times G_n$ is a group under this operation. This group is called the **direct product** of $G_1, G_2, ..., G_n$.

Lemma 0.5. *Let A and B be normal subgroups of G with $A \cap B = \{I_G\}$. Then $AB \cong A \times B$.*

Proof. First note that the elements of A commute with the elements of B, since $\forall\, a \in A$ and $b \in B$,

$$\begin{aligned} aba^{-1}b^{-1} &= a(ba^{-1}b^{-1}) \in A, && \text{(since } A \lhd G) \\ aba^{-1}b^{-1} &= (aba^{-1})b^{-1} \in B. && \text{(since } B \lhd G) \end{aligned}$$

Therefore $aba^{-1}b^{-1} \in A \cap B = \{I_G\}$, and $ab = ba$.

Define the operation $*$ on $A \times B$ by $(a_1, b_1) * (a_2, b_2) = (a_1a_2, b_1b_2)$. Now define the map ϕ by,

$$\begin{aligned} \phi : A \times B &\longrightarrow AB, \\ (a, b) &\longmapsto ab. && (\forall\, a \in A,\ b \in B) \end{aligned}$$

We show that ϕ is a homomorphism between $A \times B$ and AB.

$$\begin{aligned} \phi((a_1, b_1) * (a_2, b_2)) &= \phi(a_1a_2, b_1b_2) \\ &= a_1a_2b_1b_2 \\ &= a_1b_1a_2b_2 \\ &= \phi(a_1, b_1)\phi(a_2, b_2). \end{aligned}$$

Thus ϕ is a homomorphism and clearly surjective. It remains to show that it is injective.

$$\begin{aligned} \phi(a_1, b_1) &= \phi(a_2, b_2), \\ a_1b_1 &= a_2b_2, \\ a_1b_1b_2^{-1} &= a_2, \\ b_1b_2^{-1} &= a_1^{-1}a_2 \in A \cap B. \end{aligned}$$

Since $A \cap B = \{I_G\}$, we have $b_1b_2^{-1} = I_G = a_1^{-1}a_2$ and so $b_1 = b_2$, $a_1 = a_2$ and ϕ is injective. So ϕ is an isomorphism and $AB \cong A \times B$.

□

Corollary 0.6. *Let A and B be subgroups of G. If $A \cap B = \{I_G\}$ and $ab = ba$ $\forall a \in A$, $b \in B$. Then $AB \cong A \times B$.*

Proof. Since A and B commute, the argument outlined in Lemma 0.5 also holds here. □

Chapter 1

Properties of $SL(2, F)$ over an Algebraically Closed Field

1.1 General Notation

Throughout this paper, F will denote an arbitrary algebraically closed field. For convenince we let L denote the infinite group $SL(2, F)$. The letter p will be used to denote the characteristic of F. Recall that the characteristic of a field is the smallest number of times which the multilplicative identity of the field, say 1, needs to be summed to reach the additive identity of the field, say 0. If there is no such number, then we regard p as being zero, otherwise it is always a prime.

Unless otherwise stated, the letters $\alpha, \beta, \gamma, \delta, \lambda, \mu,$ and σ will denote elements of F and ω and ρ elements of F^*, where F^* are the non-zero elements of F.

1.2 Subsets of L

In this chapter we make some useful observations about specific elements and subgroups of L. We define the following elements of L as follows.

$$d_\omega = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix}, \qquad t_\lambda = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}, \qquad w = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \quad (\omega \in F^* \text{ and } \lambda \in F)$$

We also define the following subsets of L.

$$D = \{d_\omega\}, \qquad T = \{t_\lambda\}, \qquad H = DT.$$

Observe that H is the set of all lower triangular matrices in L whilst Dw is the set of all anti-diagonal matrices.

$$H = DT = \{d_\omega t_\lambda\} = \left\{ \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \right\} = \left\{ \begin{bmatrix} \omega & 0 \\ \lambda\omega^{-1} & \omega^{-1} \end{bmatrix} \right\}. \qquad (1.1)$$

$$Dw = \{d_\omega w\} = \left\{ \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} = \left\{ \begin{bmatrix} 0 & \omega \\ -\omega^{-1} & 0 \end{bmatrix} \right\}. \qquad (1.2)$$

These elements and subgroups are fundamental to this paper and this notation will be used throughout.

Lemma 1.1. *For any $\omega, \rho \in F^*$ and $\lambda, \mu \in F$ we have:*

$$d_\omega d_\rho = d_{\omega\rho}, \quad t_\lambda t_\mu = t_{\lambda+\mu}, \quad d_\omega t_\lambda d_\omega^{-1} = t_\sigma \ \ (\sigma = \lambda\omega^{-2}), \quad w d_\omega w^{-1} = d_\omega^{-1}.$$

Proof. These identities are all easily shown by matrix multiplication:

$$d_\omega d_\rho = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix} = \begin{bmatrix} \omega\rho & 0 \\ 0 & \omega^{-1}\rho^{-1} \end{bmatrix} = d_{\omega\rho}.$$

$$t_\lambda t_\mu = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \lambda+\mu & 1 \end{bmatrix} = t_{\lambda+\mu}.$$

$$d_\omega t_\lambda d_\omega^{-1} = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix} = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} \omega^{-1} & 0 \\ \lambda\omega^{-1} & \omega \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \lambda\omega^{-2} & 1 \end{bmatrix} = t_\sigma.$$

$$w d_\omega w^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -\omega \\ \omega^{-1} & 0 \end{bmatrix} = \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix} = d_\omega^{-1}.$$

□

Lemma 1.2. *(i) The sets D and T are subgroups of L and*

$$D \cong F^*, \qquad T \cong F.$$

(ii) T is a normal subgroup of H and $H/T \cong D$.

Proof. (i) The function $\psi : F^* \to D$ defined by $\psi(\omega) = d_\omega$ is a homomorphism between the group F^* under normal multiplication and D under normal matrix multiplication:

$$\psi(\omega\rho) = d_{\omega\rho} = d_\omega d_\rho = \psi(\omega)\psi(\rho). \qquad \text{(by Lemma 1.1)}$$

Observe that ψ is trivially injective and surjective and thus an isomorphism. So $D \cong F^*$ and D is a subgroup of L.

The function $\phi : F \to T$ defined by $\phi(\lambda) = t_\lambda$ is a homomorphism between the group F under addition and T under normal matrix multiplication:

$$\phi(\lambda + \mu) = t_{\lambda+\mu} = t_\lambda t_\mu = \phi(\lambda)\phi(\mu). \qquad \text{(by Lemma 1.1)}$$

It's clear that ϕ is injective and surjective and thus an isomorphism. So $T \cong F$ and T is a subgroup of L.

(ii) Let t_μ and $d_\omega t_\lambda$ be arbitrary elements of T and H respectively. Conjugating t_μ by $d_\omega t_\lambda$ gives,

$$\begin{aligned}(d_\omega t_\lambda)t_\mu(d_\omega t_\lambda)^{-1} &= (d_\omega t_\lambda)t_\mu(t_\lambda^{-1}d_\omega^{-1}) \\ &= d_\omega(t_\lambda t_\mu t_{-\lambda})d_\omega^{-1} && \text{(since } t_\lambda^{-1} = t_{-\lambda}) \\ &= d_\omega t_\mu d_\omega^{-1} && \text{(by Lemma 1.1)} \\ &= t_\sigma \in T. && \text{(where } \sigma = \mu\omega^{-2} \text{ by Lemma 1.1)}\end{aligned}$$

Since t_μ was chosen arbitrarily from T we have $(d_\omega t_\lambda)T(d_\omega t_\lambda)^{-1} = T$ and since $d_\omega t_\lambda$ was chosen arbitrarily from H, we have that $T \lhd H$.

The function $\pi : H \to D$ defined by $\pi(d_\omega t_\lambda) = d_\omega$ is a homomorphism between H under normal matrix multiplication and D under normal matrix multiplication:

$$\begin{aligned}\pi(d_\omega t_\lambda d_\rho t_\mu) &= \pi(d_\omega d_\rho t_\sigma t_\mu) && \text{(where } \sigma = \lambda\rho^2 \text{ by Lemma 1.1)} \\ &= d_\omega d_\rho \\ &= \pi(d_\omega t_\lambda)\pi(d_\rho t_\mu).\end{aligned}$$

We see that π is trivially surjective and has kernel

$$ker(\pi) = \{d_\omega t_\lambda \in H : \pi(d_\omega t_\lambda) = I_L\} = T.$$

Thus by the First Isomorphism Theorem,

$$\begin{aligned}H/ker(\pi) &\cong \mathrm{Im}(\pi), \\ H/T &\cong D.\end{aligned}$$

□

1.3 The Centre of L

Definition. The **centre** $Z(G)$ of a group G is the set of elements of G that commute with every element of G.

$$Z(G) = \{z \in G : \forall g \in G, \;\; gz = zg\}.$$

It is an immediate observation that $Z(G)$ is a normal subgroup of G, since for each $z \in Z$, $gzg^{-1} = gg^{-1}z = z$, $\forall g \in G$. It's also clear that a group is abelian if and only if $Z(G) = G$.

For ease of notation, $Z(L)$ will be denoted simply by Z throughout the rest of this paper.

Lemma 1.3. $Z = \langle -I_L \rangle$.

Proof. Take an arbitrary element $x = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in L$ and an arbitrary element $z = \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} \in Z$ and consider their product:

$$zx = \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} = xz,$$

$$\begin{bmatrix} z_1\alpha + z_2\gamma & z_1\beta + z_2\delta \\ z_3\alpha + z_4\gamma & z_3\beta + z_4\delta \end{bmatrix} = \begin{bmatrix} z_1\alpha + z_3\beta & z_2\alpha + z_4\beta \\ z_1\gamma + z_3\delta & z_2\gamma + z_4\delta \end{bmatrix}. \tag{1.3}$$

Equating either the top left or bottom right entries, we see that $z_2\gamma = z_3\beta$. Since β and γ can take any values in F, for equality to always hold we must have $z_2 = 0 = z_3$. Hence equation (1.3) simplifies to

$$\begin{bmatrix} z_1\alpha & z_1\beta \\ z_4\gamma & z_4\delta \end{bmatrix} = \begin{bmatrix} z_1\alpha & z_4\beta \\ z_1\gamma & z_4\delta \end{bmatrix}.$$

Thus

$$z_1 = z_4 \qquad \text{and} \qquad z = \begin{bmatrix} z_1 & 0 \\ 0 & z_1 \end{bmatrix}.$$

Since we are working in the special linear group, $\det(z) = 1$, thus $z_1 = \pm 1$ and $Z = \langle -I_L \rangle$ as required. Observe that this is a cyclic group of order 2 except in the case of $p = 2$ where $-I_L = I_L$.

□

Lemma 1.4. *If $p \neq 2$, then L contains a unique element of order 2.*

Proof. Consider an arbitrary element $x \in L$ with order 2. That is $x^2 = I_L$, $x \neq I_L$ and thus $x = x^{-1}$.

$$x = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^{-1} = \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}.$$

Thus $\alpha = \delta$, $\beta = -\beta \Rightarrow 2\beta = 0$ and $\gamma = -\gamma \Rightarrow 2\gamma = 0$. In the case of $p \neq 2$ this gives $\beta = 0 = \gamma$. So

$$x = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}.$$

Also $\alpha^2 = 1$ since $x \in SL(2, F)$, so $\alpha = \pm 1$. For x to have order 2, we must have $\alpha = -1$. Hence there is a unique element of order 2, namely $-I_L$.

□

1.4 Conjugacy of the Elements of L

Proposition 1.5. *Each element of L is conjugate to either d_ω for some $\omega \in F^*$, or to $\pm t_\lambda$ for some $\lambda \in F$.*

Proof. Since F is algebraically closed, any element $x \in L$ can be regarded as a linear transformation in the 2 dimensional vector space over F, with the eigenvalues π_1 and π_2.

• If π_1 and π_2 are distinct, then x is thus diagonalisable. That is, there exists an invertible matrix $a \in GL(2, F)$ such that $y = axa^{-1}$ is a diagonal matrix. Furthermore, we can multiply a by a suitable scalar to find an element in L which conjugates x and y:

$$\text{Set } b = \frac{a}{\sqrt{\det(a)}}, \quad \text{thus } bxb^{-1} = \frac{a}{\sqrt{\det(a)}}\, x\, (\sqrt{\det(a)}\,)\, a^{-1} = axa^{-1} = y.$$

Observe that $\det(b) = 1$, hence x and y are conjugate in L. Furthermore, since y is a diagonal matrix it must belong to the set D, showing that x is conjugate to d_ω for some $\omega \in F^*$.

• If $\pi_1 = \pi_2$ then x has just one repeated eigenvalue. Suppose that x is diagonalisable. Then there exists an element $c \in GL(2, F)$ and a diagonal matrix $\pi_1 I_G$ such that $x = c(\pi_1 I_G)c^{-1} = \pi_1 I_G$. Thus $x = \pm I_G$, which trivially belongs to both D and $T \times Z$.

Now assume that x is not diagonalisable. Chapter 7 of [5] shows that there exists an element $d \in GL(2, F)$, such that $x = djd^{-1}$, where,

$$j = \begin{bmatrix} \pi_1 & 1 \\ 0 & \pi_1 \end{bmatrix}$$

is the Jordan Normal Form of x. By the method described above, we can multiply d by a suitable scalar to show that x is conjugate to j in L. Now we conjugate j by an element of L whose top left entry is 0.

$$\begin{bmatrix} 0 & -\gamma^{-1} \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \pi_1 & 1 \\ 0 & \pi_1 \end{bmatrix} \begin{bmatrix} \delta & \gamma^{-1} \\ -\gamma & 0 \end{bmatrix} = \begin{bmatrix} 0 & -\gamma^{-1} \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \pi_1\delta - \gamma & \pi_1\gamma^{-1} \\ -\pi_1\gamma & 0 \end{bmatrix} = \begin{bmatrix} \pi_1 & 0 \\ -\gamma^2 & \pi_1 \end{bmatrix}$$

Now clearly the determinant of x is equal to the determinant of j, namely 1, which means that $\pi_1 = \pm 1$. This shows that j is conjugate in L to some element in $T \times Z$ as well as x. Furthermore, since conjugation is transitive, x is conjugate to $\pm t_\lambda$ for some $\lambda \in F$.

□

1.5 Centralisers & Normalisers

Definition. The **centraliser** $C_G(H)$ of a subset H of a group G is the set of elements of G which commute with each element of H.

$$C_G(H) = \{g \in G : gh = hg, \quad \forall h \in H\}.$$

Definition. The **normaliser** $N_G(H)$ of a subset H of a group G is the set of elements of G which stabilise H under conjugation.

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Both the centraliser and normaliser of a subset H are subgroups of G. Note also that the centraliser is a stronger condition than the normaliser and any element in the centraliser of H is also in its normaliser. If H is a singleton then it's clear that its centraliser and normaliser are equal.

Proposition 1.6. *(i) $N_L(T_1) \subset H$, where T_1 is any subgroup of T with order greater than 1.*

(ii) $C_L(\pm t_\lambda) = T \times Z$ where $\lambda \neq 0$.

Proof. (i) Let t_λ be an arbitary element of T_1 with $\lambda \neq 0$. To determine the normaliser of T_1 in L we consider which $x \in L$ satisfy $xt_\lambda x^{-1} \in T_1$.

$$\begin{aligned} xt_\lambda x^{-1} &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \delta & -\beta \\ \delta\lambda - \gamma & \alpha - \beta\lambda \end{bmatrix} \\ &= \begin{bmatrix} \alpha\delta - \beta\gamma + \beta\delta\lambda & -\beta^2\lambda \\ \delta^2\lambda & \alpha\delta - \beta\gamma - \beta\delta\lambda \end{bmatrix}. \end{aligned}$$

Since $xt_\lambda x^{-1} \in T_1$ we have $-\beta^2\lambda = 0$ and since $\lambda \neq 0$, we have $\beta = 0$. Since t_λ was chosen arbitrarily, any element which normalises T_1 is a lower diagonal matrix and is therefore in H by (1.1). Thus $N_L(T_1) \subset H$ as required.

(ii) To determine the centraliser of t_λ in L, we consider which $y \in L$ satisfy $yt_\lambda = t_\lambda y$ for an arbitrarily chosen t_λ, with $\lambda \neq 0$.

$$yt_\lambda = t_\lambda y,$$

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix},$$

$$\begin{bmatrix} \alpha + \beta\lambda & \beta \\ \gamma + \delta\lambda & \delta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma + \alpha\lambda & \delta + \beta\lambda \end{bmatrix}. \tag{1.4}$$

Equating the top left entries of (1.4) gives $\alpha + \beta\lambda = \alpha$ which means $\beta = 0$ since $\lambda \neq 0$ by assumption. Equating the bottom left entries gives that $\alpha = \delta$. Finally, since $\det(y) = 1$, we have $\alpha\delta = 1$ so $\alpha = \pm 1$. Thus a $y \in C_L(t_\lambda)$ is

$$y = \begin{bmatrix} \alpha & 0 \\ \gamma & \alpha \end{bmatrix}. \qquad \text{(where } \alpha = \pm 1\text{)}$$

So $y = \pm t_\sigma$ for some $\sigma \in F$, and $TZ = \{\pm t_\sigma\} \subset C_L(t_\lambda)$. Now take an arbitrary $t_\mu z \in TZ$.

$$\begin{aligned} (t_\mu z)t_\lambda &= t_\lambda(t_\mu z), \\ t_\mu t_\lambda z &= t_\lambda t_\mu z, && \text{(since } z \in Z) \\ t_{\mu+\lambda} &= t_{\mu+\lambda}. \end{aligned}$$

Thus $t_\mu z$ and indeed the whole of TZ is contained in $C_L(t_\lambda)$, so $C_L(t_\lambda) = TZ$.

Since T commutes elementwise with Z and $T \cap Z = \{I_G\}$, we can apply Corollary 0.6 and assert that $C_L(t_\lambda) = TZ \cong T \times Z$ as required. The centraliser of $-t_\lambda$ is also $T \times Z$, since an element x commutes with $-t_\lambda$ if and only if it commutes with t_λ:

$$xt_\lambda = t_\lambda x \iff -(xt_\lambda) = -(t_\lambda x) \iff x(-t_\lambda) = (-t_\lambda)x.$$

Note that in case of $\lambda = 0$, $\pm t_\lambda \in Z$ and thus it's centraliser is the whole of L.

□

Proposition 1.7. *(i) $N_L(D_1) = \langle D, w\rangle$, where D_1 is any subgroup of D with order greater than 2.*

(ii) $C_L(d_\omega) = D$ where $\omega \neq \pm 1$.

Proof. (i) Since $|D_1| > 3$, we can choose a $d_\omega \in D_1 \backslash Z$, that is where $\omega \neq 1$. To determine the normaliser of D_1 in L we consider which $x \in L$ satisfy $xd_\omega x^{-1} \in D_1$.

$$\begin{aligned} xd_\omega x^{-1} &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \delta\omega & -\beta\omega \\ -\gamma\omega^{-1} & \alpha\omega^{-1} \end{bmatrix} \\ &= \begin{bmatrix} \alpha\delta\omega - \beta\gamma\omega^{-1} & \alpha\beta(\omega^{-1} - \omega) \\ \gamma\delta(\omega - \omega^{-1}) & \alpha\delta\omega^{-1} - \beta\gamma\omega \end{bmatrix} \in D_1. \end{aligned} \tag{1.5}$$

Since (1.5) is in D_1, the top right and bottom left entries must be 0. Since $\omega \neq \pm 1$, we have $\omega \neq \omega^{-1}$ and so $\alpha\beta = 0 = \gamma\delta$.

• If $\alpha = 0$, then β and γ are non-zero since $\det(x) = 1$, thus $\delta = 0$. So $\det(x) = -\gamma\beta = 1$ and $-\gamma = \beta^{-1}$. (1.5) becomes

$$\begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix} = d_\omega^{-1}.$$

Since D_1 is a group, it contains the inverse of each of it's elements, so $d_\omega^{-1} \in D_1$ as required. In this case we have $x \in wD$.

• If $\alpha \neq 0$, then similarly $\beta = 0$, $\delta = \alpha^{-1}$ and $\gamma = 0$. (1.5) now becomes

$$\begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} = d_\omega \in D_1.$$

This time we have $x \in D$. So $x \in D \cup wD = \langle D, w \rangle$ and any element which normalises D_1 is in $\langle D, w \rangle$, thus $N_L(D_1) \subset \langle D, w \rangle$.

Now take an arbitrary $y \in \langle D, w \rangle = D \cup wD$. If $y \in D$ then $y = d_{\rho 1}$, for some $\rho 1 \in F^*$.

$$d_{\rho 1} d_\omega d_{\rho 1}^{-1} = d_\omega \in D_1. \qquad \text{(by Lemma 1.1)}$$

If $y \in wD$ then $y = wd_{\rho 2}$, for some $d_{\rho 2} \in F^*$.

$$\begin{aligned} (wd_{\rho 2}) d_\omega (wd_{\rho 2})^{-1} &= wd_{\rho 2} d_\omega d_{\rho 2}^{-1} w^{-1} \\ &= wd_\omega w^{-1} \\ &= d_\omega^{-1} \in D_1. \qquad \text{(by Lemma 1.1)} \end{aligned}$$

Thus y indeed who whole of $\langle D, w \rangle$ is contained in $N_L(D_1)$. This inclusion gives the desired result, $N_L(D_1) = \langle D, w \rangle$.

(ii) Now we consider which $y \in L$ satisfy $yd_\omega = d_\omega y$ for an arbitrarily chosen d_ω, with $\omega \neq \pm 1$.

$$\begin{aligned} yd_\omega &= d_\lambda y, \\ \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} &= \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \\ \begin{bmatrix} \alpha\omega & \beta\omega^{-1} \\ \gamma\omega & \delta\omega^{-1} \end{bmatrix} &= \begin{bmatrix} \alpha\omega & \beta\omega \\ \gamma\omega^{-1} & \delta\omega^{-1} \end{bmatrix}. \end{aligned} \tag{1.6}$$

Equating the top right and bottom left entries of (1.6) gives that $\beta = 0 = \gamma$ since Since $\omega \neq \omega^{-1}$. Thus $\delta = \alpha^{-1}$ and

$$x = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} \in D.$$

Thus x and indeed the whole of $C_L(d_\omega)$ is contained in D. Now take an arbitrary $d_\rho \in D$.

$$d_\rho d_\omega = d_{\rho\omega} = d_\omega d_\rho.$$

So clearly $D \subset C_L(d_\omega)$ and thus $C_L(d_\omega) = D$ as required. □

Proposition 1.8. *Let a and b be conjugate elements in a group G. Then $\exists\, x \in G$ such that $xC_G(a)x^{-1} = C_G(b)$.*

Proof. This proposition essentially claims that conjugate elements have conjugate centralisers. Since a and b are conjugate there exists an $x \in G$ such that $b = xax^{-1}$. Let g be an arbitrary element of $C_G(a)$. Then,

$$\begin{aligned}(xgx^{-1})(xax^{-1}) &= xgax^{-1} \\ &= xagx^{-1} && \text{(since } g \in C_G(a)\text{)} \\ &= (xax^{-1})(xgx^{-1}).\end{aligned}$$

Thus $xgx^{-1} \in C_G(xax^{-1})$. Since g was chosen arbitrarily,

$$xC_G(a)x^{-1} \subset C_G(xax^{-1}) = C_G(b).$$

Conversely, let h be an arbitary element of $C_G(xax^{-1})$. Then,

$$\begin{aligned}(x^{-1}hx)a &= x^{-1}h(xax^{-1})x \\ &= x^{-1}(xax^{-1})hx && \text{(since } h \in C_G(xax^{-1})\text{)} \\ &= a(x^{-1}hx).\end{aligned}$$

So $x^{-1}hx \in C_G(a)$ and since h was arbitrarily chosen from $C_G(xax^{-1})$, $x^{-1}C_G(xax^{-1})x \subset C_G(a)$. Multiplication on the left by x and on the right by x^{-1} gives $C_G(b) = C_G(xax^{-1}) \subset xC_G(a)x^{-1}$. Since we have shown that each set contains the other, $xC_G(a)x^{-1} = C_G(b)$ as required.

□

Corollary 1.9. *The centraliser of an element x in L is abelian unless x belongs to the centre of L.*

Proof. This is almost an immediate consequence of the preceding results. Propositions 1.6 and 1.7 show that an element of the form $\pm t_\lambda$ which does not lie in the centre of L has centraliser $T \times Z$, whilst a non-central element of the form d_ω has centraliser D. Both T and D are abelian since they are isomoprhic to F and F^* respectively. Let $t_\lambda z_1$ and $t_\mu z_2$ be arbitrary elements of $T \times Z$.

$$\begin{aligned}(t_\lambda z_1)(t_\mu z_2) &= t_\lambda t_\mu z_2 z_1 && \text{(since } z_1 \in Z\text{)} \\ &= t_\mu t_\lambda z_2 z_1 && \text{(since } T \text{ is abelian)} \\ &= (t_\mu z_2)(t_\lambda z_1). && \text{(since } z_2 \in Z\text{)}\end{aligned}$$

Thus $T \times Z$ is also abelian. Since every element of L is conjugate to d_ω or $\pm t_\lambda$ by Proposition 1.5 and conjugate elements have conjugate centralisers by Proposition 1.8, the centraliser of each $x \in L \setminus Z$ is conjugate to either $T \times Z$ or D. Proposition 0.4(iii) shows that conjugate subgroups are isomorphic and therefore have the same structure, thus since both $T \times Z$ and D are abelian, $C_L(x)$ is also abelian. Note that in general this does hold for $x \in Z$, since its centraliser is the whole of L which is not abelian unless $L = Z$.

□

1.6 The Projective Line & Triple Transitivity

It is convenient to sometimes take a geometric viewpoint and regard the elements of L as pairs of vectors in the 2-dimensional vector space over F, which we will denote V. An element of L is thus a linear transformation of V.

Definition. Let $\mathscr{L}$ be the set of all 1-dimensional subspaces of V. A subset $\mathscr{S}$ of $\mathscr{L}$ is called a **subspace** of $\mathscr{L}$ if there is a subspace U of V such that $\mathscr{S}$ is the set of all 1-dimensional spaces of U. We have dim $U =$ dim $\mathscr{S} + 1$. The set $\mathscr{L}$ on which this concept of subspaces is defined is called the **projective line** on V and an element of $\mathscr{L}$ is a 0-dimensional subspace of $\mathscr{L}$ and consequently called a **point**. The projective line can be considered as a straight line in the field, plus a point at infinity.

Any 1-dimensional subspace of V is a set of vectors of the form ηu, where u is a non-zero vector of V and $\eta \in F^*$. Thus the points of $\mathscr{L}$ are equivalence classes with the following relation defined on the set of vectors of V.

$$u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \sim \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = v \iff u = \eta v, \qquad (\text{for } \eta \in F^*).$$

Notice that u and v are equivalent if and only if $u_1 v_2 = v_1 u_2$. Importantly each point P_i of $\mathscr{L}$ can be represented by a corresponding equivalence class of vectors of V, that is, P corresponds to u if $P = u_1/u_2$. In the case when $u_2 = 0$, this corresponds to the point at infinity.

Definition. Let S be a permutation group which acts on a set X and $\{x_1, x_2, x_3\}$ and $\{x'_1, x'_2, x'_3\}$ be two subsets of distinct elements of X. Then S is said be **triply transitive** on X if there is an element $\pi \in S$ such that,

$$x_i^\pi = x'_i, \qquad (i = 1,2 \text{ or } 3).$$

Theorem 1.10. *Let $\mathscr{L}$ be the projective line over the field F. Then L is triply transitive on the set of the points of $\mathscr{L}$.*

Proof. Let P_1, P_2 and P_3 be distinct points of $\mathscr{L}$ and p_i be a vector in V corresponding to P_i. Since each P_i is distinct, p_1, p_2 and p_3 are thus pairwise linearly independent. Thus p_1 and p_2 form a basis for V and it's clear that there exist $\alpha, \beta \in F^*$ such that,

$$p_3 = \alpha p_1 + \beta p_2.$$

Now, let Q_1, Q_2 and Q_3 be three more distinct points of $\mathscr{L}$ and q_i be a vector in V corresponding to Q_i. Similarly, by the above argument, there exist $\gamma, \delta \in F^*$ such that,

$$q_3 = \gamma q_1 + \delta q_2.$$

Let $\pi \in GL(2,F)$ be the linear transformation which sends αp_1 to γq_1 and βp_2 to δq_2. Thus,

$$\pi(p_3) = \pi(\alpha p_1 + \beta p_2) = \pi(\alpha p_1) + \pi(\beta p_2) = \gamma q_1 + \delta q_2 = q_3$$

Hence we get $P_1^\pi = Q_1$, $P_2^\pi = Q_2$ and $P_3^\pi = Q_3$ and $GL(2,F)$ is triply transitive. Now set,

$$\eta = \sqrt{\frac{1}{\det\,\pi}}.$$

Consider the mapping θ which sends αp_1 to $\eta\gamma q_1$ and βp_2 to $\eta\delta q_2$. Observe that,

$$\det\,\theta = \eta^2 \det\,\pi = 1$$

So $\theta \in SL(2,F) = L$ and since $P_1^\theta = Q_1$, $P_2^\theta = Q_2$ and $P_3^\theta = Q_3$, we have that L is also triply transitive.

□

The following proposition looks at what happens when the group L acts on the projective line $\mathscr{L}$.

Proposition 1.11. *(i) Each element of the form d_ω (with $\omega \neq \pm 1$), fixes the same two points on the projective line $\mathscr{L}$ and fixes no other point.*

(ii) Each element of the form $\pm t_\lambda$ (with $\lambda \neq 0$), fixes the same point P on $\mathscr{L}$ and fixes no other point. Furthermore, $\mathrm{Stab}(P) = H$.

(iii) All conjugate elements have the same number of fixed points on $\mathscr{L}$.

(iv) Any noncentral element of L has at most 2 fixed points on $\mathscr{L}$.

Proof. (i) Let P be a fixed a point of an arbitrary $d_\omega \in D$, with $\omega \neq \pm 1$ and let u belong to the corresponding equivalence class of vectors of V to P.

$$d_\omega u = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1\omega \\ u_2\omega^{-1} \end{bmatrix} \sim \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

$$u_1 u_2 \omega = u_1 u_2 \omega^{-1}.$$

Since $\omega \neq \pm 1$, ω does not equal ω^{-1}, and so either $u_1 = 0$ or $u_2 = 0$. Thus u is equivalent to either the vector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and these correspond to 2 distinct points of $\mathscr{L}$ which are fixed by d_ω.

(ii) Let P be a fixed a point of an arbitrary t_λ, with $\lambda \neq 0$, and let u be the corresponding element of V to P.

$$t_\lambda u = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1 \\ u_1\lambda + u_2 \end{bmatrix} \sim \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

$$u_1 u_2 = {u_1}^2 \lambda + u_1 u_2.$$

This gives ${u_1}^2\lambda = 0$ and since $\lambda \neq 0$ we have $u_1 = 0$. Thus t_λ has just one fixed point, P which corresponds to the equivalence class of $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ in V. We show also that P is also the only fixed point of $-t_\lambda$, with $\lambda \neq 0$.

$$-t_\lambda u = \begin{bmatrix} -1 & 0 \\ \lambda & -1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} -u_1 \\ u_1\lambda - u_2 \end{bmatrix} \sim \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

$$-u_1u_2 = {u_1}^2\lambda - u_1u_2.$$

So again $u_1 = 0$ and $-t_\lambda$ fixes P and no other point. We now calculate the stabiliser of P in L, by considering which $x \in L$ fix P.

$$xu = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \beta \\ \delta \end{bmatrix} \sim \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Thus $\beta = 0$ and $x \in H$. Since x was chosen arbitrarily from Stab(P), we have Stab$(P) \subset H$. Now let an arbitrarily chosen $y \in H$ act on P.

$$yu = \begin{bmatrix} \alpha & 0 \\ \gamma & \alpha^{-1} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha^{-1} \end{bmatrix} \sim \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Thus y and indeed H is contained in Stab(P), so Stab$(P) = H$ as desired.

(iii) Let P_i $(i = 1, 2, ...)$ be the fixed points of $x \in L$ and let y be conjugate to x in L. That is, there exists a $g \in L$ such that $x = gyg^{-1}$.

$$\begin{aligned} xP_i &= P_i, \\ gyg^{-1}P_i &= P_i, \\ y(g^{-1}P_i) &= (g^{-1}P_i). \end{aligned}$$

This shows that P_i is a fixed point of x if and only if $g^{-1}P_i$ is a fixed point of y. Thus conjugate elements have the same number of fixed points.

(iv) By Proposition 1.5(i), every element of L is conjugate to either d_ω or $\pm t_\lambda$, so since conjugate elements have the same number of fixed points, every element of $L\backslash Z$ has either the same number of fixed points as d_ω (with $\omega \neq \pm 1$), namely 2, or the same number as $\pm t_\lambda$, (with $\lambda \neq 0$), namely 1.

□

Chapter 2

The Maximal Abelian Subgroup Class Equation

2.1 A Finite Subgroup of L

We now return to the realm of finite groups and consider G to be an arbitrary finite subgroup of L. We will still continue to use Z to denote the centre of L, and will use $Z(G)$ whenever we refer to the centre of G.

Observe that if Z is not contained in G, then Z must contain a non-identity element, thus $|Z| = 2$ and $p \neq 2$ by Lemma 1.3. Recall that L has a unique element of order 2 by Lemma 1.4, $-I_L$, which is not in G, therefore G has no element of order 2.

By Cauchy's Theorem, which says that if a prime p divides the order of a finite group, then the group contains an element of order p, we deduce that 2 does not divide the order of G.

This means that $|G|$ and $|Z|$ are relatively prime, so $G \cap Z = \{I_L\}$ and we can use Corollary 0.6 to show that $GZ \cong G \times Z$. This shows that regardless of whether G contains Z or not, its structure is uniquely determined by GZ, so it suffices to only consider the case when $Z \subset G$.

2.2 Maximal Abelian Subgroups

Definition. Let H and J be subgroups of a group G where H is abelian. H is called **maximal abelian** if J is not abelian whenever $H \subsetneq J$.

A group G is said to be **elementary abelian** if it is abelian and every non-trivial element has order p, where p is prime.

Notation. Let $\mathfrak{M}$ denote the set of all maximal abelian subgroups of G.

Maximal abelian subgroups play an important role in determining the structure of G. In particular, every element in G must be contained in some maximal abelian subgroup, since every element commutes at least with itself and Z. This will allow us to decompose G into the conjugacy classes of these maximal abelian subgroups. Note also that unless $G = Z$, Z is not a maximal abelian subgroup, because for each $x \in G \backslash Z$, $\langle Z, x\rangle$ is clearly a larger abelian subgroup than Z.

We will shortly prove an important theorem regarding the maximal abelian subgroups of G, but in order to do so we require the following two lemmas.

Lemma 2.1. *If G is a finite group of order p^m where p is prime and $m > 0$, then p divides $|Z(G)|$.*

Proof. Let $C(x)$ be the set of elements of G which are conjugate in G to x, we call this the conjugacy class of x. Bhattacharya shows that the set of all conjugacy classes form a partition of G [2, p.112]. Now consider the following rearranged class equation of G, where S is a subset of G containing exactly one element from each conjugacy class not contained in $Z(G)$.

$$|G| - \sum_{x \in S} [G : N_G(x)] = |Z(G)|. \tag{2.1}$$

Since $|G| = p^m$, each subgroup of G is of order p^k for some $k \leq m$. In particular each $N_G(x)$ has order p^k and is strictly contained in G since $x \notin Z(G)$ by assumption. Thus each $[G : N_G(x)] > 1$, and are therefore divisible by p. Since p divides the left hand side of (2.1), it must also divide the right, thus p divides $|Z(G)|$.

□

Lemma 2.2. *Every finite subgroup of a multiplicative group of a field is cyclic.*

Proof. See [9, p.41]. □

Theorem 2.3. *Let G be an arbitrary finite subgroup of L containing Z.*

(i) If $x \in G \backslash Z$ then we have $C_G(x) \in \mathfrak{M}$.

(ii) For any two distinct subgroups A and B of $\mathfrak{M}$, we have

$$A \cap B = Z.$$

(iii) An element A of $\mathfrak{M}$ is either a cyclic group whose order is relatively prime to p, or of the form $Q \times Z$ where Q is an elementary abelian Sylow p-subgroup of G.

(iv) If $A \in \mathfrak{M}$ and $|A|$ is relatively prime to p, then we have $[N_G(A) : A] \leq 2$. Furthermore, if $[N_G(A) : A] = 2$, then there is an element y of $N_G(A) \backslash A$ such that,

$$yxy^{-1} = x^{-1} \qquad \forall x \in A.$$

(v) Let Q be a Sylow p-subgroup of G. If $Q \neq \{I_G\}$, then there is a cyclic subgroup K of G such that $N_G(Q) = QK$. If $|K| > |Z|$, then $K \in \mathfrak{M}$.

Proof. (i) Let x be chosen arbitrarily from $G \backslash Z$. Then by Corollary 1.9, $C_L(x)$ is abelian. By definition, $C_G(x) = C_L(x) \cap G$, and using the elementary fact that the intersection of 2 groups is itself a group, we have $C_G(x) < C_L(x)$. Now since every subgroup of an abelian group is abelian, $C_G(x)$ is also abelian.

Now let J be a maximal abelian subgroup of G containing $C_G(x)$. Since J is abelian and $x \in C_G(x) \subset J$, we have $jx = xj$, $\forall j \in J$, thus $J \subset C_G(x)$. Therefore $J = C_G(x)$ and $C_G(x) \in \mathfrak{M}$.

(ii) Consider $x \in A \cap B$. Since both A and B are abelian, x commutes with each $a \in A$ and $b \in B$ and thus $C_G(x)$ contains both A and B. If $x \in G \setminus Z$, then $C_G(x) \in \mathfrak{M}$ by (i) and because A and B are distinct we have $A \subsetneq A \cup B \subset C_G(x)$. This contradicts the fact that A is maximum abelian and thus $x \in Z$. Finally, note that Z is contained in every maximal abelian subgroup, since otherwise we would have the contradiction that $\langle A, Z \rangle$ would generate a larger abelian subgroup than A. Hence $A \cap B = Z$.

(iii) First consider the trivial case of $G = Z$. Here G is the only element of $\mathfrak{M}$. If $p \neq 2$ then $|G| = 2$ and G is a cyclic group whose order is relatively prime to p. If $p = 2$ then $G = I_G$ which is trivially a S_p-subgroup.

Now assume $G \neq Z$. Since $Z \notin \mathfrak{M}$, each $A \in \mathfrak{M}$ contains at least one $x \notin Z$. By Proposition 1.5 this x is conjugate to either d_ω or $\pm t_\lambda$ in L. It suffices to only consider these cases:

• ***x* conjugate to $\boldsymbol{d_\omega}$ in *L***. There is a $y \in L$ such that $x = y d_\omega y^{-1}$. Since $x \notin Z$, we have $d_\omega \notin Z$, because otherwise we get the contradiction,

$$x = y d_\omega y^{-1} = d_\omega \in Z.$$

Thus $\omega \neq \pm 1$. Let $A = C_G(x)$, since $C_G(x) \in \mathfrak{M}$ by part (i). Observe that

$$\begin{aligned} C_G(d_\omega) &< C_L(d_\omega) && \text{(see proof of (i))} \\ &= D && \text{(by Lemma 1.7)} \\ &\cong F^*. && \text{(by Lemma 1.2)} \end{aligned}$$

Since A is conjugate to $C_G(d_\omega)$ by Proposition 1.8, we have that A is isomorphic to a finite subgroup of F^* and by Lemma 2.2, A is cyclic. By Lagrange's Theorem any finite subgroup of F^* has an order which divides $p^m - 1$ for some $m \in \mathbb{Z}^+$, and since $p \nmid (p^m - 1)$, $|A|$ is relatively prime to p.

• ***x* conjugate to $\boldsymbol{\pm t_\lambda}$ in *L***. Again let $A = C_G(x) \in \mathfrak{M}$. A is conjugate to

$C_G(\pm t_\lambda)$ in L by Proposition 1.8. Since $x \notin Z$, we have $\lambda \neq 0$. Observe that

$$\begin{aligned} C_G(\pm t_\lambda) &< C_L(\pm t_\lambda) \\ &= T \times Z && \text{(by Lemma 1.6)} \\ &\cong F \times Z. && \text{(by Lemma 1.2)} \end{aligned}$$

So A is isomorphic to a finite subgroup of $F \times Z$, call it $Q \times Z$. Now $A = Q \times Z \cong QZ$ by Corollary 0.6, which means that an arbitrary element of A is of the form $q_1 z_1$, where $q_1 \in Q$, $z_1 \in Z$.

$$\begin{aligned} q_1 z_1 q_2 z_2 &= q_2 z_2 q_1 z_1, && (A \in \mathfrak{M}) \\ q_1 q_2 z_1 z_2 &= q_2 q_1 z_1 z_2, && (z_1,\, z_2 \in Z) \\ q_1 q_2 z_1 z_2 (z_1 z_2)^{-1} &= q_2 q_1 z_1 z_2 (z_1 z_2)^{-1}, \\ q_1 q_2 &= q_2 q_1. \end{aligned}$$

Thus Q is also abelian. Recall from the proof of Proposition 1.5(ii) that all non-trivial elements of T have order p, so each non-trivial element of Q has order p which means that Q is elementary abelian. Thus Q has order p^m, for some $m \in \mathbb{Z}^+$.

Now let S be a Sylow p-subgroup containing Q. We apply Lemma 2.1 to determine that p divides $|Z(S)|$, moreover $|Z(S)| \geq p$.

If $p = 2$, then $Z = I_L$ by Lemma 1.3. So $|Z| = 1$ and hence $|Z(S)| \geq 2 > |Z|$. If $p > 2$, then $Z = \langle -I_L \rangle$ also by Lemma 1.3. So $|Z| = 2$ and again we get $|Z(S)| > 2 = |Z|$.

So $Z(S)$ must contain at least one element which is not in Z, let y be one such element. Let $s_1 z_1$ be an arbitrary element of $S \times Z$.

$$\begin{aligned} (s_1 z_1) y (s_1 z_1)^{-1} &= (s_1 z_1) y (z_1^{-1} s_1^{-1}) \\ &= s_1 y (z_1 z_1^{-1}) s_1^{-1} && \text{(since } y \in L,\ z_1 \in Z) \\ &= y (s_1 s_1^{-1}) && \text{(since } s_1 \in S,\ y \in Z(S)) \\ &= y \end{aligned}$$

Thus $s_1 z_1 \in C_G(y)$ and since it was chosen arbitrarily, $S \times Z \subset C_G(y)$. Also since $y \in G \backslash Z$ we have $C_G(y) \in \mathfrak{M}$ by part (i).

$$A = Q \times Z \subset S \times Z \subset C_G(y).$$

Since A and $C_G(y)$ are both in $\mathfrak{M}$ it must be that $A = C_G(y)$. This means $Q = S$ and Q is a Sylow p-subgroup of G.

(iv) If $|A| \leq 2$ then $A = Z = G$. So A is trivially normal in G and $[N_G(A) : A] = 1$.

Now assume that $|A| > 2$. Since $|A|$ is relatively prime to p, we have that A is a cyclic group conjugate to a finite subgroup of D in L by the proof of part (iii), call this subgroup $\widetilde{A}$. Thus both $\widetilde{A}$ and D have orders greater than 2. Applying Proposition 1.7 we observe that

$$N_L(\widetilde{A}) = \langle D, w\rangle = N_L(D). \tag{2.2}$$

Since A and $\widetilde{A}$ are conjugate in L, there exists an element $z \in L$ such that $zAz^{-1} = \widetilde{A}$. This z determines an inner automorphism of L defined by

$$i_z : L \longrightarrow L, \qquad \text{where} \quad i_z(t) = ztz^{-1} \quad \forall\, t \in L.$$

Let $i_z(G) = \widetilde{G}$ denote the image of G under i_z. Since A is a maximal abelain subgroup of G it's a simple task to show that $\widetilde{A}$ is a maximal abelian subgroup of $\widetilde{G}$ and I will leave this to the reader to verify. We now show that $i_z(N_G(A)) = N_{\widetilde{G}}(\widetilde{A})$. Take an arbitrary $g \in N_G(A)$.

$$\begin{aligned}
(zgz^{-1})\widetilde{A}(zgz^{-1})^{-1} &= zg(z^{-1}\widetilde{A}z)g^{-1}z^{-1} \\
&= z(gAg^{-1})z^{-1} && (\text{since } zAz^{-1} = \widetilde{A}) \\
&= zAz^{-1} && (\text{since } g \in N_G(A)) \\
&= \widetilde{A}.
\end{aligned}$$

So $zgz^{-1} = i_z(g) \in N_{\widetilde{G}}(\widetilde{A})$ and since it was chosen arbitrarily, $i_z(N_G(A)) \subset N_{\widetilde{G}}(\widetilde{A})$. Now take an arbitrary $zhz^{-1} \in N_{\widetilde{G}}(\widetilde{A})$.

$$\begin{aligned}
\widetilde{A} &= (zhz^{-1})\widetilde{A}(zhz^{-1})^{-1} \\
&= zh(z^{-1}\widetilde{A}z)h^{-1}z^{-1} \\
&= zhAh^{-1}z^{-1}. && (\text{since } A = z^{-1}\widetilde{A}z)
\end{aligned}$$

Now multiplication on the left by z^{-1} and right by z gives:

$$A = z^{-1}\widetilde{A}z = hAh^{-1},$$

so $h \in N_G(A)$. Furthermore, zhz^{-1} and indeed the whole of $N_{\widetilde{G}}(\widetilde{A})$ is contained in $i_z(N_G(A))$. Thus $i_z(N_G(A)) = N_{\widetilde{G}}(\widetilde{A})$. In particular, we have,

$$[N_G(A) : A] = [N_{\widetilde{G}}(\widetilde{A}) : \widetilde{A}]. \tag{2.3}$$

Since $\widetilde{G} < L$, the normaliser of $\widetilde{A}$ in $\widetilde{G}$ is simply the normaliser of $\widetilde{A}$ in L restricted to $\widetilde{G}$, thus $N_{\widetilde{G}}(\widetilde{A}) < N_L(\widetilde{A}) = N_L(D)$ by (2.2). Now since $D \lhd N_L(D)$, the Second Isomorphism Theorem shows that,

$$N_{\widetilde{G}}(\widetilde{A})/(N_{\widetilde{G}}(\widetilde{A}) \cap D) \;\cong\; DN_{\widetilde{G}}(\widetilde{A})/D. \tag{2.4}$$

Clearly $\widetilde{A} \subset \widetilde{G} \cap D$. We show that this inclusion is infact an equality. Assume that there exists some $d_\omega \in \widetilde{G} \cap D$ which is not in $\widetilde{A}$. The group $\langle d_\omega, \widetilde{A}\rangle$ is thus an abelian subgroup of $\widetilde{G}$, strictly larger than $\widetilde{A}$ and contradicting the fact that $\widetilde{A}$ is maximal abelian in $\widetilde{G}$. Thus $\widetilde{A} = \widetilde{G} \cap D$. It is trivial to see that $\widetilde{A} \subset N_{\widetilde{G}}(\widetilde{A}) \cap D$. Also $N_{\widetilde{G}}(\widetilde{A}) \cap D \subset \widetilde{G} \cap D = \widetilde{A}$. So,

$$\widetilde{A} = N_{\widetilde{G}}(\widetilde{A}) \cap D. \tag{2.5}$$

Observe also that,

$$DN_{\widetilde{G}}(\widetilde{A}) = \{D, \langle D, w\rangle\} \subset \langle D, w\rangle = N_L(D). \tag{2.6}$$

Now we piece the preceding results together to give the desired result.

$$\begin{aligned} N_{\widetilde{G}}(\widetilde{A})/\widetilde{A} &\cong N_{\widetilde{G}}(\widetilde{A})/(N_{\widetilde{G}}(\widetilde{A}) \cap D) && \text{(by (2.5))} \\ &\cong DN_{\widetilde{G}}(\widetilde{A})/D && \text{(by (2.4))} \\ &\subset N_L(D)/D && \text{(by (2.6))} \\ &= \langle D, w\rangle/D \cong \mathbb{Z}_2. \end{aligned}$$

We have shown that $N_{\widetilde{G}}(\widetilde{A})/\widetilde{A}$ is isomorphic to a subset of $\mathbb{Z}_2$. Thus by (2.3) we have established that,

$$[N_G(A) : A] = [N_{\widetilde{G}}(\widetilde{A}) : \widetilde{A}] \leq 2.$$

For the second part, if $[N_G(A) : A] = 2$, then the above argument shows that $N_{\widetilde{G}}(\widetilde{A})/\widetilde{A} \cong \mathbb{Z}_2$. Thus $DN_{\widetilde{G}}(\widetilde{A}) = N_L(D) = \langle D, w\rangle$. This means that $N_{\widetilde{G}}(\widetilde{A})$ contains some element wd_ω. In fact, since $wd_\omega \notin D$, we have $wd_\omega \in N_{\widetilde{G}}(\widetilde{A})\backslash\widetilde{A}$. Take any element $x \in A$. Since $\widetilde{A} = zAz^{-1}$, $zxz^{-1} \in \widetilde{A}$, call it d_σ. Let $y = z^{-1}wd_\omega z$. Since $wd_\omega \in N_{\widetilde{G}}(\widetilde{A})\backslash\widetilde{A}$ it follows that $y \in N_G(A)\backslash A$. We show that this y inverts x:

$$\begin{aligned} yxy^{-1} &= (z^{-1}wd_\omega z)(z^{-1}d_\sigma z)(z^{-1}d_\omega^{-1}w^{-1}z) \\ &= z^{-1}wd_\omega d_\sigma d_\omega^{-1}w^{-1}z \\ &= z^{-1}wd_\sigma w^{-1}z \\ &= z^{-1}d_\sigma^{-1}z && \text{(by Lemma 1.1)} \\ &= x^{-1}. \end{aligned}$$

(v) By part (iii), Q is conjugate to a finite subgroup of T in L. In fact, without loss of generality we can assume that $Q \subset T$, moreoever $Q \subset T \cap G$. We show that this is in fact an equality by showing that the reverse inclusion also holds. Let t_λ be an arbitrary element of $T \cap G$. Then $\langle t_\lambda, Q\rangle$ is a p-group of G which must be equal to Q since it is a Sylow p-subgroup of G. Thus $t_\lambda \in Q$ and

$$Q = T \cap G. \tag{2.7}$$

Since $|Q| > 1$, Proposition 1.6 gives that $N_G(Q) \subset N_L(Q) \subset H$. So $N_G(Q) \subset H \cap G$. Now take an arbitrarily chosen $d_\omega t_\lambda \in H \cap G$ and $t_\mu \in Q$.

$$\begin{aligned}
(d_\omega t_\lambda)t_\mu(d_\omega t_\lambda)^{-1} &= d_\omega(t_\lambda t_\mu t_{-\lambda})d_\omega^{-1} \\
&= d_\omega t_\mu d_\omega^{-1} && \text{(by Lemma 1.1)} \\
&= t_\sigma. && \text{(where } \sigma = \mu\omega^{-2}\text{, by Lemma 1.1)}
\end{aligned}$$

Since it is a product of elements of G, $t_\sigma \in T \cap G = Q$ by (2.7). Thus $d_\omega t_\lambda \in N_G(Q)$ and indeed the whole of $H \cap G$ is contained in $N_G(Q)$ and

$$N_G(Q) = H \cap G. \tag{2.8}$$

We now define a map ϕ by,

$$\phi : N_G(Q) \longrightarrow D, \qquad \text{where} \quad \phi(d_\omega t_\lambda) = d_\omega \quad \forall\ d_\omega t_\lambda \in N_G(Q).$$

Next we determine the kernel of ϕ.

$$\begin{aligned}
ker(\phi) &= \{d_\omega t_\lambda \in N_G(Q) : \phi(d_\omega t_\lambda) = I_G\} \\
&= N_G(Q) \cap T \\
&= H \cap G \cap T && \text{(by (2.8))} \\
&= T \cap G = Q. && \text{(by (2.7))}
\end{aligned}$$

We show that ϕ is a group homomorphism. Take $d_\omega t_\lambda$, $d_\rho t_\mu$ from $N_G(Q)$.

$$\begin{aligned}
\phi(d_\omega t_\lambda d_\rho t_\mu) &= \phi(d_\omega d_\rho t_\sigma t_\mu) && \text{(where } \sigma = \lambda\rho^2\text{, by Lemma 1.1)} \\
&= d_\omega d_\rho \\
&= \phi(d_\omega t_\lambda)\phi(d_\rho t_\mu).
\end{aligned}$$

Thus by the First Isomorphism Theorem,

$$N_G(Q)/Q \cong \phi(N_G(Q)), \tag{2.9}$$

Since $N_G(Q)$ is a finite group, it's image under ϕ is thus a finite subgroup of D. Furthermore, since $D \cong F^*$ (by Lemma 1.2), $\phi(N_G(Q))$ is a cyclic group whose order divides $p^m - 1$ and is therefore relatively prime to p, and by (2.9), so too is $N_G(Q)/Q$.

Let r be the order of $N_G(Q)/Q$. Since it is cyclic, $N_G(Q)/Q$ is generated by a single element, namely a coset of Q in $N_G(Q)$, call it kQ. So $|kQ| = r$. Observe that,

$$\begin{aligned}
(kQ)^r &= Q, \\
k^r Q &= Q, \\
k^r &\in Q.
\end{aligned}$$

Since Q is elementary abelian, each of it's non-trivial elements has order p, so k has order r or rp. In either case, since $\gcd(r,p) = 1$, the order of k^p is r. Let $K = \langle k^p \rangle$. Now $|K| = r$ and

$$\begin{aligned} |N_G(Q)| &= r|Q| \\ &= |K||Q| \\ &= |QK|. && \text{(since } Q \cap K = I_G\text{)} \end{aligned}$$

Thus,

$$N_G(Q) = QK. \tag{2.10}$$

Now assume $|K| > |Z|$. Since K is abelian, it must be contained in some maximal abelian group $A \in \mathfrak{M}$. By part (iii), A must also be a cyclic group whose order is relatively prime to p.

Since A is conjugate in L to a subgroup of D, each non-central element of A has exactly 2 fixed points on the projective line $\mathscr{L}$ by Proposition 1.11. Let $A = \langle x \rangle$ and let P_1 and P_2 be the points fixed by x. We show by induction on n that x^n also fixes P_1 and P_2, for all $n \in \mathbb{Z}^+$. We do this by assuming first that x^{n-1} fixes P_i.

$$x^n P_i = x(x^{n-1}P_i) = x(P_i) = P_i.$$

The importance of this is that since each element of A can be expressed as some power of x, they must have the same two fixed points, namely P_1 and P_2. In other words,

$$A \subset S_L(P_i), \qquad (i = 1 \text{ or } 2) \tag{2.11}$$

By Proposition 1.11(ii), each element of T has a common fixed point P and $\mathrm{Stab}(P) = H$. Since $K \subset H$, each element in K fixes P. Also, since $K \subset A$, this P must be equal to either P_1 or P_2. Therefore by (2.11), $A \subset \mathrm{Stab}(P) = H$. We arrive at the following result:

$$\begin{aligned} A &\subset H \cap G \\ &= N_G(Q) && \text{(by (2.8))} \\ &= QK. && \text{(by (2.10))} \end{aligned}$$

Furthermore, we get,

$$\begin{aligned} A &= QK \cap A \\ &= QK \cap AK && (K \subset A \text{ so } A = AK) \\ &= (Q \cap A)K \\ &= K && (Q \cap A = I_G) \end{aligned}$$

Thus $K \in \mathfrak{M}$.

□

For the duration of this paper, unless otherwise stated, Q will denote a Sylow p-subgroup of G and K will be as described above.

2.3 Conjugacy of Maximal Abelian Subgroups

Definition. The set $\mathcal{C}_i = \{xA_ix^{-1} : x \in G\}$ is called the **conjugacy class** of $A_i \in \mathfrak{M}$.

Notation. Let A_i^* be the non-central part of $A_i \in \mathfrak{M}$, let $\mathfrak{M}^*$ be the set of all A_i^* and let $\mathcal{C}_i^*$ be the conjugacy class of A_i^*.

For some $A_i \in \mathfrak{M}$ and $A_i^* \in \mathfrak{M}^*$ let,

$$C_i = \bigcup_{x \in G} xA_ix^{-1}, \quad \text{and} \quad C_i^* = \bigcup_{x \in G} xA_i^*x^{-1}.$$

In other words, C_i denotes the set of elements of G which belong to some element of $\mathcal{C}_i$. It's evident that $C_i^* = C_i \setminus Z$ and that there is a C_i corresponding to each $\mathcal{C}_i$. Clearly we have the relation,

$$|C_i^*| = |A_i^*||\mathcal{C}_i^*|. \tag{2.12}$$

Theorem 2.4. *Let G be a finite subgroup of L and S be a subset of $\mathfrak{M}^*$ containing exactly one element from each of its conjugacy classes.*

(i) The set of C_i^* form a partition of $G \backslash Z$. That is,

$$G\backslash Z = \bigcup_{A_i^* \in S} C_i^*, \qquad \text{and} \qquad C_i^* \cap C_j^* = \varnothing, \qquad \forall\, i \neq j.$$

(ii) $|\mathcal{C}_i^*| = |\mathcal{C}_i|$.

(iii) $|\mathcal{C}_i| = [G : N_G(A_i)]$.

(iv)

$$|G\backslash Z| = \sum_{A_i^* \in S} |A_i^*|[G : N_G(A_i)].$$

Proof. (i) Define a relation $\sim$ on $\mathfrak{M}^*$ as follows:

$$A_i^* \sim A_j^* \quad \text{if} \quad A_i^* = xA_j^*x^{-1} \quad \text{for some} \quad x \in G.$$

• If we choose $x \in A_i^*$, then clearly $A_i^* = A_i^*xx^{-1} = xA_i^*x^{-1}$, thus $A_i^* \sim A_i^*$ and $\sim$ is reflexive.

• If $A_i^* \sim A_j^*$, then $\exists\, x \in G$ such that,

$$A_i^* = xA_j^*x^{-1} \iff x^{-1}A_i^*x = A_j^* \iff A_j^* = yA_i^*y^{-1} \quad \text{for } y = x^{-1} \in G.$$

Thus $A_j^* \sim A_i^*$ and $\sim$ is symmetric.

• If $A_i^* \sim A_j^*$ and $A_j^* \sim A_k^*$, then $\exists\, x, y \in G$ such that,

$$A_i^* = xA_j^*x^{-1} \text{ and } A_j^* = yA_k^*y^{-1} \Rightarrow A_i^* = xyA_k^*y^{-1}x^{-1} = (xy)A_k^*(xy)^{-1}.$$

Thus $A_i^* \sim A_k^*$ (since $xy \in G$), which shows that $\sim$ is transitive and moreover an equivalence relation on $\mathfrak{M}^*$.

The equivalence class of A_i^* in $\mathfrak{M}^*$ therefore coincides with the set $\mathcal{C}_i^* = \{xA_i^*x^{-1} : x \in G\}$. Furthermore, this tells us that each A_i^* belongs to exactly one conjugacy class. Thus the conjugacy classes $\mathcal{C}_i^*$ form a partition of $\mathfrak{M}^*$,

$$\mathfrak{M}^* = \bigcup_{A_i^* \in S} \mathcal{C}_i^*, \qquad \text{and} \qquad \mathcal{C}_i^* \cap \mathcal{C}_j^* = \varnothing, \qquad \forall\, i \neq j.$$

Since the set of $\mathcal{C}_i^*$ are pairwise disjoint, it follows that the set of C_i^* are also pairwise disjoint and we get the desired result,

$$G \backslash Z = \bigcup_{A_i^* \in S} C_i^*, \qquad \text{and} \qquad C_i^* \cap C_j^* = \varnothing, \qquad \forall\, i \neq j.$$

(ii) Let $xA_ix^{-1} \in \mathcal{C}_i$ and $xA_i^*x^{-1} \in \mathcal{C}_i^*$. Since $xA_ix^{-1} \backslash Z = xA_i^*x^{-1}$, it is quite clear that,

$$xA_ix^{-1} \in \mathcal{C}_i \iff xA_i^*x^{-1} \in \mathcal{C}_i^*.$$

Thus $|\mathcal{C}_i^*| = |\mathcal{C}_i|$ as desired.

(iii) Now we define a map ϕ by:

$$\begin{aligned} \phi : \mathcal{C}_i &\longrightarrow G/N_G(A_i), \\ \phi(xA_ix^{-1}) &= xN_G(A_i). \end{aligned} \qquad (\forall\, x \in G,\ A_i \in \mathfrak{M})$$

Clearly ϕ is trivially surjective. We now show that it is both well-defined and injective.

$$\begin{aligned} xN_G(A_i) = yN_G(A_i) &\iff y^{-1}xN_G(A_i) = N_G(A_i) \\ &\iff y^{-1}x \in N_G(A_i) \\ &\iff (y^{-1}x)A_i(y^{-1}x)^{-1} = A_i \\ &\iff y^{-1}xA_ix^{-1}y = A_i \\ &\iff xA_ix^{-1} = yA_iy^{-1}. \end{aligned}$$

Hence ϕ is well-defined and injective. This shows that ϕ is a bijection proving that $|\mathcal{C}_i| = [G : N_G(A_i)]$. This is a crucial result which shows that the number of maximal abelian subgroups conjugate to A_i is equal to the index of the normaliser of A_i in G.

(iv) This follows directly from parts (i), (ii) and (iii) and (2.12).

$$G\backslash Z = \bigcup_{A_i^* \in S} C_i^*, \qquad \text{and} \qquad C_i^* \cap C_j^* = \varnothing, \qquad \forall\, i \neq j,$$

$$\begin{aligned} |G\backslash Z| &= \sum_{A_i^* \in S} |C_i^*| = \sum_{A_i^* \in S} |A_i^*||\mathcal{C}_i^*| = \sum_{A_i^* \in S} |A_i^*||\mathcal{C}_i| \\ &= \sum_{A_i^* \in S} |A_i^*|[G : N_G(A_i)]. \end{aligned}$$

□

This theorem proves that the non-central parts of the maximal abelian subgroups form a partition of the non-central part of G. This will serve as a powerful tool in decomposing G and counting its elements.

2.4 Constructing The Class Equation

It is necessary to prove the following 2 short lemmas before we proceed further.

Lemma 2.5. *$N_G(A) = N_G(A^*)$.*

Proof. (iii) Let $x \in N_G(A^*)$. Take an arbitary $a \in A = A^* \cup Z$. If $a \in A^*$, then since $x \in N_G(A^*)$, we have $xax^{-1} \in A^* \subset A$. If $a \in Z$, then $xzx^{-1} = zxx^{-1} = z \in A$. Therefore x is in the normaliser of A and $N_G(A^*) \subset N_G(A)$.

Conversely, take $y \in N_G(A)$ and $a \in A^*$. $yay^{-1} \in A = A^* \cup Z$. If $yay^{-1} \in Z$, then

$$\begin{aligned} yay^{-1} &= z, && \text{(some } z \in Z) \\ a &= y^{-1}zy = y^{-1}yz = z \notin A^*. \end{aligned}$$

This contradicts the fact that $a \in A^*$. Therefore $yay^{-1} \in A^*$ and $y \in N_G(A^*)$. Since y was chosen arbitrarily we get $N_G(A) \subset N_G(A^*)$ and hence $N_G(A) = N_G(A^*)$.

□

Lemma 2.6. *$N_G(Q \times Z) = N_G(Q)$.*

Proof. If $p = 2$ then $Z = I_G$ and the result is trivial. Now assume $p \neq 2$. Thus $|Z| = 2$. Let x and q_1 be arbitrarily chosen elements of $N_G(Q)$ and Q respectively.

$$\begin{aligned} xq_1x^{-1} &= q_2, && \text{(for some } q_2 \in Q) \\ xq_1x^{-1}z_1 &= q_2z_1, \\ xq_1z_1x^{-1} &= q_2z_1 \in Q \times Z. \end{aligned}$$

Thus any element x which is in $N_G(Q)$ is also in $N_G(Q \times Z)$ so we have $N_G(Q) \subset N_G(Q \times Z)$.

Let q_1z_1 be an arbitrarily chosen element of $Q \times Z$ such that $q_1 \in Q$ and $z_1 \in Z$. Now let y be an arbitrarily chosen element of $N_G(Q \times Z)$.

$$yq_1z_1y^{-1} = q_2z_2 \in Q \times Z. \qquad \text{(where } q_2 \in Q \text{ and } z_2 \in Z\text{)}$$

Consider now the order of q_1z_1 in G. Since $p \neq 2$, $Q \cap Z = I_G$ and $|q_1z_1| = |q_1||z_1|$. Note that q_1z_1 and q_2z_2 are conjugate in G, and thus their orders are equal. This means that $|z_1| = |z_2|$, because otherwise 2 would divide one of them and not the other. Thus $z_1 = z_2$ and,

$$\begin{aligned} yq_1z_1y^{-1} &= q_2z_2 = q_2z_1 \\ yq_1y^{-1}z_1 &= q_2z_1, \\ yq_1y^{-1} &= q_2 \in Q \end{aligned}$$

Hence $y \in N_G(Q)$. Furthermore, since y was chosen arbitrarily, any element which is in $N_G(Q \times Z)$ is also in $N_G(Q)$, so $N_G(Q \times Z) = N_G(Q)$ as desired.

□

We now start to count the elements of the seperate components of G and use the preceeding 2 theorems to construct what will be an invaluable formula in determining the structure of G, something we will call the **Maximal Abelian Subgroup Class Equation** of G.

First we spilt $\mathfrak{M}$ into the conjugacy classes of it's elements. Theorem 2.3(iii) tells us that every maximal abelian subgroup is either a cyclic subgroup whose order is relatively prime to p or of the form $Q \times Z$ where Q is a Sylow p-subgroup. Let $\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_s, \mathcal{C}_{s+1}, ..., \mathcal{C}_{s+t}$ (where $s, t \in \mathbb{Z}^+$) denote the conjugacy classes of the cyclic subgroups whose order is relatively prime to p. Recall that part (iv) of Theorem 2.3 tells us that $[N_G(A) : A] = 1$ or 2. Let A_i be a representative from each $\mathcal{C}_i$ such that,

$$[N_G(A_i) : A_i] = 1, \qquad \text{(for } i \leq s\text{)}$$

$$[N_G(A_i) : A_i] = 2., \qquad \text{(for } s < i \leq s+t\text{)}$$

Now let Q_1 and Q_2 be any two Sylow p-subgroups of G. By the Second Sylow Theorem, Q_1 and Q_2 are conjugate to each other in G. That is, there exists a $g \in G$ such that $gQ_1g^{-1} = Q_2$.

$$\begin{aligned} gQ_1g^{-1} = Q_2 &\iff gQ_1g^{-1}Z = Q_2Z \\ &\iff gQ_1Zg^{-1} = Q_2Z \\ &\iff g(Q_1 \times Z)g^{-1} = (Q_2 \times Z). \qquad \text{(by Corollary 0.6)} \end{aligned}$$

So $Q_1 \times Z$ and $Q_2 \times Z$ belong to the same conjugacy class, furthermore there is thus only 1 conjugacy class of elements of this form in $\mathfrak{M}$. Let $\mathcal{C}_{Q \times Z}$ denote this conjugacy class and let $Q \times Z$ be a representative from it. The following diagram provides a visual representation of G divided into it's maximal abelian subgroups.

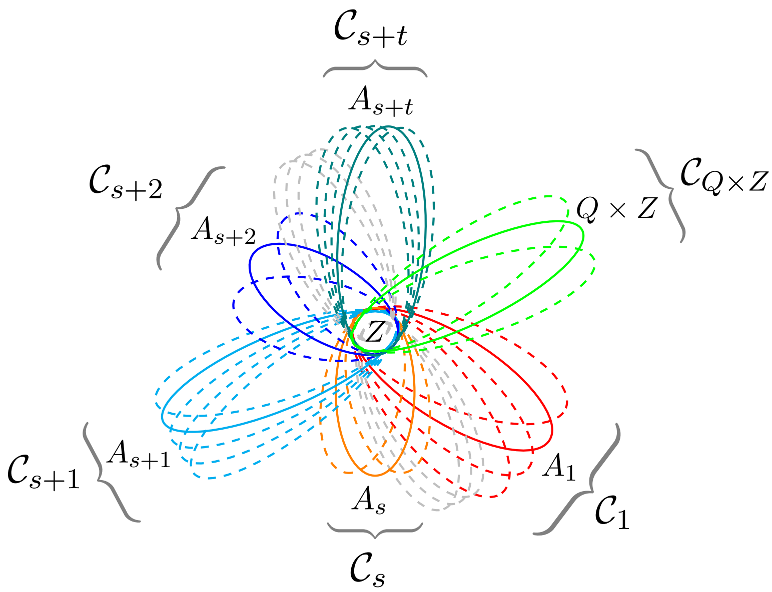

Fig 1: G arranged into it's maximal abelian subgroups

We can reformulate the counting formula in Theorem 2.4(iv) using the notation we have introduced to show that it agrees with the intuitive approach that Fig 1 suggests.

$$|G \backslash Z| = \sum_{A_i^* \in S} |A_i^*|[G : N_G(A_i)] = \sum_{A_i^* \in S} |C_i^*| = |C_{Q\times Z}^*| + \sum_{i=1}^{s+t} |C_i^*|.$$

We are now able to begin to evaluate G. Firstly, let $|Z| = e$ and $|G| = eg$. We know well by now that $e = 1$ or 2 depending on whether p equals 2 or not, and by Lagrange's Theorem, the order of a subgroup divides the order of the group, so e divides $|G|$ since $Z < G$.

We consider the cyclic case first. Again, by Lagrange's Theorem, since Z is a subgroup of each A_i, e divides $|A_i|$. So set $|A_i| = eg_i$. Since $Z \notin \mathfrak{M}$, each A_i is therefore strictly larger than Z and so each g_i is an integer greater than or equal to 2.

To determine the order of each C_i, we return to the set $\mathfrak{M}^*$. The size of one representative of each class is,

$$|A_i^*| = |A_i \backslash Z| = eg_i - e = e(g_i - 1).$$

The number of A_i^* in each conjugacy class $\mathcal{C}_i$ for $i \leq s$ is thus,

$$|\mathcal{C}_i^*| = |\mathcal{C}_i| = [G : N_G(A_i)] = \frac{|G|}{|A_i|} = \frac{eg}{eg_i} = \frac{g}{g_i}.$$

Therefore the total number of elements of G in the noncentral part of C_i for $i \leq s$ is,

$$\sum_{i=1}^{s} |C_i^*| = \sum_{i=1}^{s} |A_i^*||\mathcal{C}_i^*| = \sum_{i=1}^{s} \frac{eg(g_i - 1)}{g_i}. \tag{2.13}$$

The number of A_i^* in each conjugacy class $\mathcal{C}_i$ for $s < i \leq s + t$ is thus,

$$|\mathcal{C}_i^*| = |\mathcal{C}_i| = [G : N_G(A_i)] = \frac{|G|}{2|A_i|} = \frac{eg}{2eg_i} = \frac{g}{2g_i}.$$

Therefore the total number of elements of G in the noncentral part of C_i for $s < i \leq s + t$ is,

$$\sum_{i=s+1}^{s+t} |C_i^*| = \sum_{i=s+1}^{s+t} |A_i^*||\mathcal{C}_i^*| = \sum_{i=s+1}^{s+t} \frac{eg(g_i - 1)}{2g_i}. \tag{2.14}$$

We next determine the order of $C_{Q\times Z}$. Let $|Q| = q$. If $p \nmid |G|$ then $q = 1$ and if $p = 0$, then we consider a Sylow p-subgroup to simply be I_G. So q is always at least 1. Since $Z < K$, we can let $|K| = ek$. Observe that if $K \in \mathfrak{M}$, then by Theorem 2.3(v), $K = A_i$ for some $0 < i \leq t$ and $k = g_i$. Recall that $N_G(Q) = QK$ and so,

$$\begin{aligned}
|N_G(Q \times Z)^*| &= |N_G(Q \times Z)| && \text{(by Lemma 2.5)}\\
&= |N_G(Q)| && \text{(by Lemma 2.6)}\\
&= |QK| = eqk.
\end{aligned}$$

Again we count the size and number of these maximal abelian groups.

$$|(Q \times Z)^*| = |QZ| - |Z| = e(q - 1).$$

Since there is only one conjugacy class of $Q \times Z$, the number of $(Q \times Z)^*$ in $\mathfrak{M}^*$ is thus,

$$|\mathcal{C}_{Q\times Z}^*| = |\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{|G|}{|N_G(Q \times Z)^*|} = \frac{eg}{eqk} = \frac{g}{qk}.$$

Therefore the total number of elements of G in the noncentral parts of each $Q \times Z$ is,

$$|C_{Q\times Z}^*| = |(Q \times Z)^*||\mathcal{C}_{Q\times Z}^*| = \frac{eg(q - 1)}{qk}. \tag{2.15}$$

We now sum together (2.13), (2.14) and (2.15) to create the **Maximal Abelian Subgroup Class Equation** of G.

$$
\begin{aligned}
|G\backslash Z| &= |C^*_{Q\times Z}| + \sum_{i=1}^{s+t} |C^*_i|, \\
|G\backslash Z| &= |(Q\times Z)^*||\mathcal{C}^*_{Q\times Z}| + \sum_{i=1}^{s} |A^*_i||\mathcal{C}^*_i| + \sum_{i=s+1}^{s+t} |A^*_i||\mathcal{C}^*_i|, \\
eg - e &= \frac{eg(q-1)}{qk} + \sum_{i=1}^{s} \frac{eg(g_i-1)}{g_i} + \sum_{i=s+1}^{s+t} \frac{eg(g_i-1)}{2g_i}, \\
1 &= \frac{1}{g} + \frac{q-1}{qk} + \sum_{i=1}^{s} \frac{g_i-1}{g_i} + \sum_{i=s+1}^{s+t} \frac{g_i-1}{2g_i}. \qquad (2.16)
\end{aligned}
$$

Since $g, k, q \in \mathbb{Z}^+$ this implies that,

$$\frac{1}{g} > 0 \quad \text{and} \quad \frac{q-1}{qk} \geq 0.$$

Also, since $g_i \geq 2$ for $1 \leq i \leq s+t$, we have,

$$\frac{g_i-1}{g_i} \geq \frac{1}{2}, \quad \sum_{i=1}^{s} \frac{g_i-1}{g_i} \geq \frac{s}{2} \quad \text{and} \quad \sum_{i=s+1}^{s+t} \frac{g_i-1}{2g_i} \geq \frac{t}{4}.$$

Thus we can find a lower bound for (2.16) which limits the possible number of conjugacy classes somewhat,

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

There are only 6 possible different pairs of values which s and t can take:

Case	I	II	III	IV	V	VI
s	1	1	0	0	0	0
t	0	1	0	1	2	3

Each case will be examined individually in the next chapter.

Chapter 3

Dickson's Classification Theorem

3.1 Five Lemmas

Before we detemine the structure of G in each of the 6 cases, it is necessary to prove a number of lemmas which will be used.

Lemma 3.1. *Let H be a proper subgroup of a p-group G. Then $H \subsetneq N_G(H)$.*

Proof. Let S denote the set of left cosets of H in G. That is,

$$S = \{xH : x \in G\}, \quad \text{and} \quad |S| = [G : H] = p^k. \quad \text{(for some } k \geq 1)$$

Consider the action of H on S by left multiplication. We calculate the stabiliser of $xH \in S$ in H.

$$\begin{aligned} \mathrm{Stab}(xH) &= \{y \in H : yxH = xH\} \\ &= \{y \in H : x^{-1}yx \in H\}. \end{aligned}$$

If $x \in H$ then $x^{-1}yx \in H$ for all $y \in H$. Thus the $\mathrm{Stab}(xH) = H$ and by the Orbit-Stabiliser Theorem,

$$|\mathrm{Orb}(xH)| = [H : \mathrm{Stab}(xH)] = 1.$$

Observe that,

$$S = \bigcup_{xH \in S} \mathrm{Orb}(xH),$$

where the orbits are pairwise disjoint. Now since p divides $|S|$, p divides the sum of all the orbit sizes. Furthermore, since each orbit size is 1 or a multiple of p, there must be at least p elements of S which have an orbit of 1. In particular, there exists an $x_1H \in S$ which has an orbit of 1 and $x_1 \notin H$. That is,

$$\begin{aligned} yx_1H &= x_1H, & (\forall y \in H) \\ x_1^{-1}yx_1 &\in H, \\ x_1^{-1}Hx_1 &\subset H, \\ x_1 &\in N_G(H) \backslash H. \end{aligned}$$

□

Lemma 3.2. *Let Q be a Sylow p-subgroup and K a maximal abelian subgroup of G such that $N_G(Q) = QK$ and $Q \cap K = \{I_G\}$. If $[N_G(K) : K] = 2$, then Q is not a normal subgroup of G.*

Proof. The approach here is proof by contradiction, so we begin by assuming that $Q \lhd G$. Thus $N_G(Q) = G$ and $N_G(K) \subset N_G(Q)$. Consider the natural homomorphism of $N_G(Q)$ onto $N_G(Q)/Q$,

$$\begin{aligned} \phi : N_G(Q) &\longrightarrow N_G(Q)/Q, \\ \phi(x) &= xQ, \\ ker(\phi) &= \{x \in N_G(Q) : \phi(x) = I_G Q\} = Q. \end{aligned}$$

Let ϕ' be the restiction of ϕ to $N_G(K)$:

$$\phi' = \phi|_{N_G(K)} : N_G(K) \longrightarrow N_G(Q)/Q.$$

Thus $ker(\phi') = ker(\phi) \cap N_G(K) = Q \cap N_G(K)$. By the 1st Isomorphism Theorem,

$$\begin{aligned} \mathrm{Im}(\phi') &\cong N_G(K)/ker(\phi'), \\ N_G(Q)/Q &\cong N_G(K)/(Q \cap N_G(K)), \\ K &\cong N_G(K)/(Q \cap N_G(K)), && (N_G(Q) = QK) \\ |Q \cap N_G(K)| &= [N_G(K) : K] = 2. && \text{(by assumption)} \end{aligned}$$

So 2 divides $|Q|$, which implies that $2 \nmid |K|$ since $Q \cap K = \{I_G\}$. Moreover, $|Q \cap N_G(K)|$ and $|K|$ are relatively prime.

Take $a \in ker(\phi') = Q \cap N_G(K)$ and $b \in N_G(K)$.

$$\begin{aligned} \phi'(bab^{-1}) &= \phi'(b)\phi'(a)\phi'(b^{-1}) \\ &= \phi'(b)(I_G Q)\phi'(b^{-1}) \\ &= \phi'(b)\phi'(b^{-1})(I_G Q) = I_G Q. \end{aligned}$$

Thus $bab^{-1} \in ker(\phi') = Q \cap N_G(K)$ and so $Q \cap N_G(K) \lhd N_G(K)$.

Now let $x \in Q \cap N_G(K)$ and $y \in K$. Notice that both x and y are elements of $N_G(K)$,

$$\begin{aligned} xyx^{-1}y^{-1} &= (xyx^{-1})y^{-1} \in K, && \text{(since } K \lhd N_G(K)) \\ xyx^{-1}y^{-1} &= x(yx^{-1}y^{-1}) \in Q \cap N_G(K), && \text{(since } Q \cap N_G(K) \lhd N_G(K)) \\ xyx^{-1}y^{-1} &\in K \cap (Q \cap N_G(K)) \\ &= I_G, && \text{(since } \gcd(|Q \cap N_G(K)|, |K|) = 1) \\ xy &= yx. \end{aligned}$$

Therefore $(Q \cap N_G(K)) \times K$ is an abelian subgroup of which K is a proper subgroup. This contradicts the fact that K is a maximal abelian subgroup, thus Q is not a normal subgroup of G.

□

Lemma 3.3. *Let p be the prime characteristic of F and let $q = p^k$ for some $k > 0$. Set,*

$$R = \{\lambda \in F : \lambda^q - \lambda = 0\}. \tag{3.1}$$

Then R is a subfield of F.

Proof. Since R is a subset of F it suffices to show that the following 3 criteria are met:

(i) $0, 1 \in R$.
(ii) If $\lambda_1, \lambda_2 \in R$, then $\lambda_1 - \lambda_2 \in R$.
(iii) If $\lambda_1, \lambda_2 \in R$ and $\lambda_1 \neq 0 \neq \lambda_2$, then $\lambda_1 \lambda_2^{-1} \in R$.

We see immediately that (i) is satified. Since p is the characteristic of F, any coeffiecients which are a multiple of p vanish. We get,

$$(\lambda_1 - \lambda_2)^q = (\lambda_1^p - \lambda_2^p)^{p^{k-1}} = ... = \lambda_1^q - \lambda_2^q = \lambda_1 - \lambda_2.$$

Thus $\lambda_1 - \lambda_2 \in R$ and (ii) is also satisifed. Finally observe that if λ_2 is a non-zero element of R, then $\lambda_2^{-1} = \lambda_2^{-q}$ and,

$$(\lambda_1 \lambda_2^{-1})^q = \lambda_1^q \lambda_2^{-q} = \lambda_1 \lambda_2^{-1}.$$

So $\lambda_1 \lambda_2^{-1} \in R$ and R is a subfield of F.

□

Each finite field is uniquely determined up to isomorphism by the number of elements it contains [8, p.227]. Since the R defined in (3.1) has q elements, from now on when we use the notation $\mathbb{F}_q$ to denote a field of q elements, we shall actually mean,

$$\mathbb{F}_q = R \subset F. \tag{3.2}$$

Lemma 3.4. *Let $\mathbb{F}_q$ be the field of q elements, where q is the power of a prime. The order of $GL(2, \mathbb{F}_q)$ is $(q^2 - 1)(q^2 - q)$ and the order of $SL(2, \mathbb{F}_q)$ is $q(q^2 - 1)$.*

Proof. In order to prove this, we again take a geometric viewpoint. Recall that $GL(2, \mathbb{F}_q)$ is the group of 2 x 2 invertible matrices over $\mathbb{F}_q$ under ordinary matrix multiplication. The order of $GL(2, \mathbb{F}_q)$ is thus equal to the number of ordered pairs $\{u, v\}$ of linearly independent vectors in a 2-dimensional vector space over $\mathbb{F}_q$.

There are clearly q^2 different vectors in the 2-dimensional vector space over $\mathbb{F}_q$. The only restriction on the first vector u, is that it must be non-zero, so there are $(q^2 - 1)$ choices for u. To ensure the second vector v is linearly independent of u, it must not be of the form αu, where $\alpha \in \mathbb{F}_q$. Since there are q choices for α, there are $(q^2 - q)$ choices for v.

Thus the order of $GL(2, \mathbb{F}_q)$ is the product of the number of choices of u and the number of choices of v, that is, $(q^2-1)(q^2-q)$ as required. Now consider the map ϕ defined as,

$$\phi : GL(2, \mathbb{F}_q) \longrightarrow \mathbb{F}_q^*, \qquad \text{where } \phi(x) = \det(x), \quad \forall\, x \in GL(2, \mathbb{F}_q).$$

Next we determine the kernel of ϕ.

$$ker(\phi) = \{GL(2, \mathbb{F}_q) : \det(x) = 1\} = SL(2, \mathbb{F}_q).$$

We show that ϕ is a group homomorphism. Take $x, y \in GL(2, \mathbb{F}_q)$,

$$\phi(xy) = \det(xy) = \det(x)\det(y) = \phi(x)\phi(y).$$

Clearly ϕ is surjective, since $\alpha \in \mathbb{F}_q^*$ is the determinant of $\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{F}_q)$. Therefore by the First Isomorphism Theorem,

$$GL(2, \mathbb{F}_q)/SL(2, \mathbb{F}_q) \cong \mathbb{F}_q^*.$$

Thus,

$$|SL(2, \mathbb{F}_q)| = \frac{|GL(2, \mathbb{F}_q)|}{|\mathbb{F}_q^*|} = \frac{(q^2-1)(q^2-q)}{q-1} = q(q^2-1).$$

□

Lemma 3.5. *Let N be a normal subgroup of a group G and let H be a subgroup of G which contains N.Then,*

$$H/N \lhd G/N \iff H \lhd G$$

Proof. If $H \lhd G$, then it follows from the Third Isomorphism Theorem that $H/N \lhd G/N$. Conversely, assume that H/N is normal in G/N. Let x be an arbitrary element of G and h be an arbitrary element of H. Since H/N is normal in G/N we have,

$$xhx^{-1}N = (xN)(hN)(x^{-1}N) = (xN)(hN)(xN)^{-1} \in H/N.$$

Thus $xhx^{-1} \in H$. Since x and h were chosen arbitrarily, we have that $H \lhd G$. □

3.2 The Six Cases

We now address individually the 6 possible combinations of s and t in (2.16) and determine the structure of G in each case.

Case I:

Claim: *In this case, the Sylow p-subgroup Q is different from G and is an elementary abelian normal subgroup of G. The factor group G/Q is a cyclic group whose order is relatively prime to p.*

Proof. Here, $s = 1$ and $t = 0$. Equation (2.16) simplifies to:

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{g_1},$$
$$1 = \frac{1}{g} + \frac{1}{k} - \frac{1}{qk} + 1 - \frac{1}{g_1},$$
$$\frac{1}{qk} + \frac{1}{g_1} = \frac{1}{g} + \frac{1}{k}. \tag{3.3}$$

• **Case Ia: $q = 1$**. Here we have $Q = I_G$ and is trivially an elementary abelian normal subgroup of G. Equation (3.3) gives $g = g_1$, thus $G/Q = G = A_1$, which indeed is a cyclic group whose order is relatively prime to p.

• **Case Ib: $q > 1$**. If $k = 1$ then (3.3) gives,

$$\frac{1}{q} + \frac{1}{g_1} = \frac{1}{g} + 1 \ > \ 1.$$

But since both $1/q$ and $1/g_i$ are at most $1/2$ each, this is a contradiction. Thus $k > 1$. This means that $|K| = ek > e = |Z|$, so $k = g_1$ by Theorem 2.3(v). Equation (3.3) now gives $qk = g$.

$$|G| = eg = eqk = |N_G(Q)|.$$

Thus $G = N_G(Q)$ and so $Q \lhd G$. Therefore $Q \neq G$ and is an elementary abelian normal subgroup of G. Also,

$$G/Q = N_G(Q)/Q \cong K = A_1.$$

Thus G/Q is a cyclic group whose order is relatively prime to p.

□

Case II:

Claim: *The order of G is relatively prime to p and either $G \cong SL(2,3)$ or G is the group of order $4n$, where n is odd, defined by the presentation:*

$$\langle\, x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1} \,\rangle.$$

Proof. Here, $s = 1 = t$. Equation (2.16) simplifies to:

$$1 = \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{g_1} + \frac{g_2 - 1}{2g_2},$$
$$1 = \frac{1}{g} + \frac{q-1}{qk} + 1 - \frac{1}{g_1} + \frac{1}{2} - \frac{1}{2g_2},$$
$$\frac{1}{g_1} + \frac{1}{2g_2} = \frac{1}{2} + \frac{1}{g} + \frac{q-1}{qk}. \tag{3.4}$$

First assume that $q > 1$. This means $(q-1)/qk \geq 1/2k$ and consequently we bound (3.4) from below:

$$\frac{1}{2g_2} = \frac{1}{2} - \frac{1}{g_1} + \frac{1}{g} + \frac{q-1}{qk} \ > \ \frac{1}{2k}.$$

Thus $k > g_2 \geq 2$. So $K \in \mathfrak{M}$ and $k = g_i$ for some i. Since it is strictly greater than g_2, we have $k = g_1$. Equation (3.4) now becomes

$$\begin{aligned}
\frac{1}{g_1} + \frac{1}{2g_2} \ &= \ \frac{1}{2} + \frac{1}{g} + \frac{q-1}{qg_1}, \\
\frac{1}{g_1} + \frac{1}{2g_2} \ &> \ \frac{1}{2} + \frac{1}{2g_1}, \\
\frac{1}{4} + \frac{1}{4} \ \geq \ \frac{1}{2g_1} + \frac{1}{2g_2} \ &> \ \frac{1}{2}.
\end{aligned}$$

This contradiction disproves the assumption that $q > 1$, so we have that $q = 1$. This means that Q, a Sylow p-subgroup of G, is simply the identity element and so $|G|$ is relatively prime to p. Also, Equation (3.4) now reduces to:

$$\frac{1}{g_1} + \frac{1}{2g_2} = \frac{1}{2} + \frac{1}{g}. \tag{3.5}$$

If $g_1 \geq 4$ we get

$$\frac{1}{2g_2} = \frac{1}{2} + \frac{1}{g} - \frac{1}{g_1} \ > \ \frac{1}{4}.$$

Since $g_2 > 1$ this gives a contradiction and thus $g_1 < 4$. We now have two seperate cases to consider.

- **Case IIa: $g_1 = 2$.** Equation (3.5) becomes

$$\frac{1}{2g_2} = \frac{1}{g}, \ \implies \ g = 2g_2.$$

If $e = 1$, then $p = 2$. Also since $q = 1$, 2 does not divide $|G|$, but $|G| = eg = e2g_2$ which is a contradiction. So $e = 2$ and $p \neq 2$. We now have:

$$\begin{aligned}
|N_G(A_2)| &= 2|A_2| = 2eg_2 = eg = |G|, && \text{(since } s+t=2\text{)} \\
|N_G(A_1)| &= |A_1| = eg_1 = 4. && \text{(since } s=1\text{)}
\end{aligned}$$

Thus $G = N_G(A_2)$, that is $A_2 \lhd G$.

By Corollary 0.2, A_1 is contained in a Sylow 2-subgroup of G, call it S. If S is strictly larger than A_1, then by Lemma 3.1, $A_1 \subsetneq N_S(A_1) \subset N_G(A_1)$. Since $A_1 = N_G(A_1)$ we conclude that A_1 is a Sylow 2-subgroup of G. This means that 8 does not divide $|G| = 4g_2$ and so $g_2 = n$, where n is odd.

Since A_2 is cyclic it is generated by a single element, so let $A_2 = \langle x \rangle$ and thus

$x^{2n} = I_G$. Recall that because $[N_G(A_2) : A_2] = 2$, Theorem 2.3(iv) tells us that there exists a $y \in N_G(A_2)\backslash A_2$ such that $yxy^{-1} = x^{-1}$.

Recall from Chapter 2 that the number of A_i in each conjugacy class $\mathcal{C}_i$ is equal to $[G : N_G(A_i)]$ so,

$$|\mathcal{C}_2| = [G : N_G(A_2)] = 1.$$

Due to the fact that y belongs to some maximal abelian subgroup of G, and since $y \notin A_2$ and $|\mathcal{C}_2| = 1$, it must be that y belongs to A_1 or one of its conjugate subgroups. Thus y has an order which divides $|A_1| = 4$ and since the only elements of order 1 and 2 lie in Z, the order of y is 4. Furthermore, both x^n and y^2 have order 2. Recalling that G has at most 1 element of order 2, this gives the relation $x^n = y^2$.

Let H be the group generated by x and y and the above relations:

$$H = \langle\, x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1}\rangle.$$

Notice that the second relation gives that $yx^ny^{-1} = x^{-n}$, so

$$x^{-n} = yx^ny^{-1} = yy^2y^{-1} = y^2 = x^n.$$

This shows that $y^4 = x^{2n} = I_G$ and that H is finite. Moreoever,

$$H = \{x^k, x^ky : 0 < k \leq 2n\}.$$

Thus $|H| = 4n = |G|$ and $H = G$.

- **Case IIb: $g_1 = 3$**. Equation (3.5) becomes

$$\frac{1}{2g_2} = \frac{1}{6} + \frac{1}{g} \;>\; \frac{1}{6}.$$

Therefore $g_2 = 2$ and $g = 12$. Again, since $q = 1$ and 2 divides $|G|$, we have $p \neq 2$ and so $e = 2$. Thus we have,

$$|G| = eg = 24, \qquad |A_1| = eg_1 = 6, \qquad |A_2| = eg_2 = 4.$$

Again we determine the number of maximal abelian subgroups in each conjugacy class.

$$|\mathcal{C}_1| = [G : N_G(A_1)] = \frac{|G|}{|A_1|} = \frac{24}{6} = 4,$$

$$|\mathcal{C}_2| = [G : N_G(A_2)] = \frac{|G|}{2|A_2|} = \frac{24}{8} = 3.$$

The figure below shows G divided into it's maximal abelian subgroups:

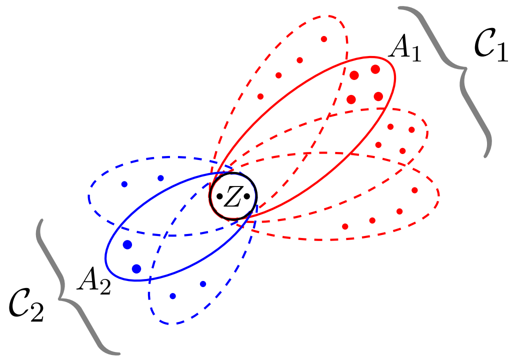

Fig 2: The elements of G arranged into maximal abelian subgroups.

Let $A_2 = \langle x \rangle$. By Theorem 2.3(iv), there is an element $y \in N_G(A_2) \backslash A_2$ such that $yxy^{-1} = x^{-1}$. Since $N_G(A_2)$ has order 8, the order of y must divide 8. The order of y cannot be 8 since $N_G(A_2)$ is not cyclic and the only elements with order 1 or 2 are found in Z, thus y has order 4. By the uniqueness of the element of order 2, we have $x^2 = y^2$. So

$$N_G(A_2) = \langle x, y \mid x^2 = y^2, yxy^{-1} = x^{-1} \rangle.$$

For simplicity let $N = N_G(A_2)$. Since $|A_1| = 6$, the only elements in C_1 with order 2^k are those in Z, so every element of G with order 2^k must belong to C_2. Since C_2 has order 8 it is equal to N because each element of N has order 2^k. Furthermore, N is thus a unique Sylow 2-subgroup of G and by Corollary 0.1, we have $N \lhd G$.

Now consider the quotient group G/N, that is the set of left (or right) cosets of N in G.

$$G/N = \{N, rN, r^2N\} \cong \langle r \rangle \cong \mathbb{Z}_3,$$

where r is some element of $G \backslash N$ with order 3. Without loss of generality we may regard r to be a generator of H, where H is the cyclic subgroup of A_1 of order 3.

Let H act on N by conjugation. Since $|H| = 3$ the orbit of $x \in N$ has size 1 or 3.

$$\mathrm{Orb}(x) = \{r^k x r^{-k} : r^k \in H\}.$$

Since H is not contained in the centraliser of x we conclude that the orbit of x has size 3. Let A_2, A_2' and A_2'' be the 3 elements of $\mathcal{C}_2$. Without loss of generality we may assume $y \in A_2'$ and consequently $xy \in A_2''$. Using the two relations between x and y we observe that,

$$(xy)^{-1} = y^{-1}x^{-1} = y^{-1}(yxy^{-1}) = xy^{-1} = x^{-1}x^2y^{-1} = x^{-1}y = yx$$

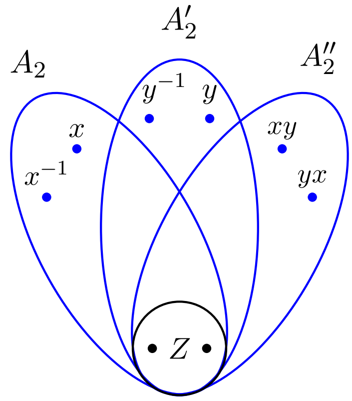

Fig 3: The elements of N arranged into maximal abelian subgroups.

The elements of Z are fixed points under this group action and the remaining 6 elements of N form 2 orbit cycles of order 3, with each cycle containing exactly one element from the noncentral parts of A_2, A_2' and A_2'' in some order. If y inverts x, then y inverts all powers of x including x^{-1}. Also, if y inverts x, then y^{-1} inverts x^{-1} and thus inverts x also. So the 2 relations we have established between x and y actually hold for any pair of elements of $N \setminus Z$ which belong to different elements of $\mathfrak{M}$. Therefore without loss of generality, we may assume that x and y are in the same orbit cycle and that $rxr^{-1} = y$. Fig 3 shows that there are only 2 elements which could complete this cycle, xy and yx. If $ryr^{-1} = xy$, then we have the following 3 relations on G.

$$rxr^{-1} = y, \qquad ryr^{-1} = xy, \qquad rxyx^{-1} = x. \tag{3.6}$$

Otherwise $ryr^{-1} = yx$. In this case, consider the orbit of x under conjugation by r^2 instead. This gives the same orbit cycle but in the opposite direction:

$$r^2xr^{-2} = yx, \qquad r^2yxr^{-2} = y, \qquad r^2yr^{-2} = x.$$

Observe that $x(yx) = x(x^{-1}y) = y$. Thus without loss of generality we can rename r^2 as r, yx as y and y as xy. Notice that this now gives the same relations as in (3.6). Since x and y generate a group of order 8 and r has order 3, the group given by the following presentation has order at most 24 and is thus a presentation of G.

$$\langle x, y, r \,|\, x^2 = y^2,\, yxy^{-1} = x^{-1},\, r^3 = I,\, rxr^{-1} = y,\, ryr^{-1} = xy,\, rxyr^{-1} = x\rangle,$$

By Lemma 3.4, we observe that the order of $SL(2, 3)$ is $3(3^2 - 1) = 24$. Now consider the following the elements of $SL(2, 3)$:

$$a = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \qquad c = \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}.$$

One can verify easily that each of the following relations hold:

$$\begin{aligned} a^2 &= b^2, & bab^{-1} &= a^{-1}, & c^3 &= I, \\ cac^{-1} &= b, & cbc^{-1} &= ab, & cabc^{-1} &= a. \end{aligned}$$

Since G and $SL(2,3)$ have the same order and since their respective generators satisfy the corresponding relations, there is an isomorphism mapping $x \mapsto a$, $y \mapsto b$ and $r \mapsto c$. Thus,

$$G = \langle x, y, r\rangle \cong \langle a, b, c\rangle = SL(2,3).$$

□

Case III:

Claim: *We have* $G = Q \times Z$.

Proof. Here, $s = 0 = t$. Equation (2.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk}, \\ 1 &= \frac{1}{g} + \frac{1}{k} - \frac{1}{qk}, \\ 1 + \frac{1}{qk} &= \frac{1}{g} + \frac{1}{k}. \end{aligned} \tag{3.7}$$

Since $s = 0 = t$, there are no cyclic maximal abelian subgroups whose order is relatively prime to p, so $K \notin \mathfrak{M}$. Then by Theorem 2.3(v) we have,

$$ek = |K| \leq |Z| = e.$$

Thus $k = 1$ and equation (3.7) reduces to $1/q = 1/g$, that is $g = q$.

$$\begin{aligned} |G| = eg = eq &= |Q \times Z|, \\ G &= Q \times Z. \end{aligned}$$

□

Case IV:

Claim: *Either* $p = 2$ *and* G *is isomorphic to the dihedral group of order* $2n$*, where* n *is odd, or* $p = 3$ *and* $G \cong SL(2,3)$.

Proof. Here, $s = 0$ and $t = 1$. Equation (2.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1}, \\ 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2} - \frac{1}{2g_1}, \\ \frac{1}{2} + \frac{1}{2g_1} &= \frac{1}{g} + \frac{q-1}{qk}. \end{aligned} \tag{3.8}$$

Recall that $|A_1| = eg_1$ and $[N_G(A_1) : A_1] = 2$ and so,

$$eg = |G| \geq |N_G(A_1)| = 2eg_1.$$

So $g \geq 2g_1$ and $1/2g_1 \geq 1/g$ and hence we can bound Equation (3.8):

$$\frac{1}{2} \leq \frac{1}{2} + \frac{1}{2g_1} - \frac{1}{g} = \frac{q-1}{qk}.$$

Clearly this forces $k = 1$ and also $q > 1$. We can now simplify and bound Equation (3.8) as follows:

$$\frac{1}{q} + \frac{1}{4} \geq \frac{1}{q} + \frac{1}{2g_1} = \frac{1}{g} + \frac{1}{2} > \frac{1}{2}.$$

This gives $1/q > 1/4$ and so q is equal to either 2 or 3. We examine each case individually.

- **Case IVa: $q = 2$.** Equation (3.8) becomes

$$\frac{1}{2g_1} = \frac{1}{g}, \implies g = 2g_1,$$

and we show that A_1 is a normal subgroup of G:

$$|G| = eg = e2g_1 = 2|A_1| = |N_G(A_1)|.$$

In this case, a Sylow p-subgroup has order 2 so we have $p = 2$ and also $e = 1$. By it's definition, the order of A_1 is relatively prime to $p = 2$, so we have that $|A_1| = g_1 = n$, where n is odd, and consequently G has order $2n$.

We now know enough about the structure of G to establish some relations on it. Let $A_1 = \langle x \rangle$, so $x^n = I_G$. By Theorem 2.3(iv) there exists a $y \in N_G(A_1) \backslash A_1$ such that $yxy^{-1} = x^{-1}$.

$$|\mathcal{C}_1| = [G : N_G(A_1)] = 1.$$

$$|\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{|G|}{eqk} = \frac{2n}{2} = n.$$

The only maximal abelian subgroups of G are thus A_1 and the n conjugate subgroups of $\mathcal{C}_{Q\times Z}$.

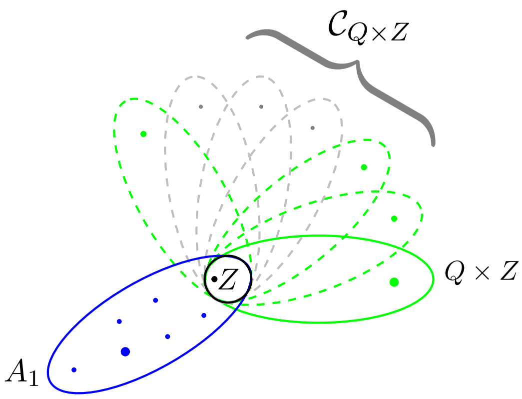

Fig 4: The elements of G arranged into maximal abelian subgroups.

Since y belongs to some maximal abelian subgroup and $y \notin A_1$, y must belong to some element of $\mathcal{C}_{Q\times Z}$. Since $|Q \times Z| = 2$, the order of y is 2 and $y^2 = I_G$. We have established the following presentation of G.

$$G = \langle x, y \mid x^n = I_G = y^2,\ yxy^{-1} = x^{-1} \rangle.$$

Let D_n denote the dihedral group of order $2n$, that is the group of symmetries of a regular polygon wih n vertices. Let r denote a clockwise rotation by $2\theta/n$ radians and s denote a reflection. For n odd, it can easily be verified that D_n has the following presentation.

$$D_n = \langle r, s \mid r^n = I = s^2,\ srs^{-1} = r^{-1} \rangle.$$

Since G and D_n have the same order and since their respective generators satisfy the corresponding relations, there is an isomorphism mapping $x \mapsto r$ and $y \mapsto s$. Thus,

$$G = \langle x, y \rangle \cong \langle r, s \rangle = D_n.$$

- **Case IVb: $q = 3$**. Now equation (3.8) becomes

$$\frac{1}{2g_1} = \frac{1}{g} + \frac{1}{6} > \frac{1}{6}.$$

This means that $g_1 = 2$ and $g = 12$. Since $q = 3$ we have $p = 3$ and $e = 2$. Furthermore we have,

$$|G| = 24, \quad |A_1| = 4, \quad |N_G(A_1)| = 8, \quad |Q \times Z| = 6 \quad |N_G(Q \times Z)| = 6$$

$$|\mathcal{C}_1| = [G : N_G(A_1)] = \frac{24}{8} = 3$$
$$|\mathcal{C}_{Q\times Z}| = [G : N_G(Q \times Z)] = \frac{24}{6} = 4$$

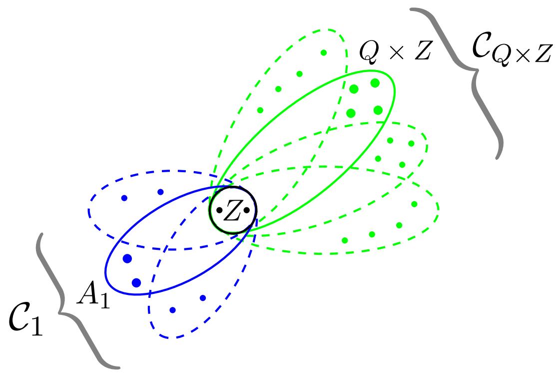

Fig 5: The elements of G arranged into maximal abelian subgroups.

Notice that Fig 5 is almost identical to Fig 2 in the study of Case IIb. This is a strong indication that these 2 cases are isomorphic to each other and hence also to $SL(2,3)$, albeit not a proof. However, an argument analogous to the one outlined in the proof of Case IIb can be directly applied here with a simple renaming of the conjugacy classes and representatives. It would be tedious to repeat this argument again and I will leave it to the reader to verify.

□

Case V:

Claim: *We have one of the following three cases:*

(i) $G \cong SL(2, \mathbb{F}_q)$.

(ii) $G \cong \langle SL(2, \mathbb{F}_q), d_\pi \rangle$, *where* $\pi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\pi^2 \in \mathbb{F}_q$ *and* $SL(2, \mathbb{F}_q) \lhd G$.

(iii) $G \cong SL(2,5)$ *and* $p = 3 = q$.

Proof. Here, $s = 0$ and $t = 2$. Equation (2.16) simplifies to:

$$\begin{aligned} 1 &= \frac{1}{g} + \frac{q-1}{qk} + \frac{g_1 - 1}{2g_1} + \frac{g_2 - 1}{2g_2}, \\ \frac{1}{2g_1} + \frac{1}{2g_2} &= \frac{1}{g} + \frac{q-1}{qk}. \end{aligned} \tag{3.9}$$

Recall that,

$$eg = |G| \geq |N_G(A_i)| \geq 2eg_i, \qquad \text{thus } \frac{1}{g} \leq \frac{1}{2g_i}.$$

Equation (3.9) is therefore bounded from below:

$$\frac{2}{g} \leq \frac{1}{2g_1} + \frac{1}{2g_2} = \frac{1}{g} + \frac{q-1}{qk}.$$

Therefore $q > 1$, since if $q = 1$ we arrive at the contradiction $2/g \leq 1/g$. With this in mind we have $(q-1)/q \geq 1/2$ and since $g_i \geq 2$ this allows us to bound (3.9) on either side.

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

This gives $k > 1$ and so by Theorem 2.3(v), k must equal g_1 or g_2 since the inequality $ek = |K| > |Z| = e$ holds. Without loss of generality we let $k = g_1$ and (3.9) becomes,

$$\begin{aligned} \frac{1}{2g_1} + \frac{1}{2g_2} &= \frac{1}{g} + \frac{q-1}{qg_1} = \frac{1}{g} + \frac{1}{g_1} - \frac{1}{qg_1}, \\ \frac{1}{2g_2} &= \frac{1}{g} + \frac{1}{2g_1} - \frac{1}{qg_1}. \end{aligned} \tag{3.10}$$

Let $N_G(Q)$ act on $Q\backslash I_G$ by conjugation and consider the stabiliser in $N_G(Q)$ of an arbitrarily chosen $x \in Q\backslash I_G$.

$$\begin{aligned}
\mathrm{Stab}(x) &= \{g \in N_G(Q) : gxg^{-1} = x\} \\
&= C_G(x) \cap N_G(Q) \\
&= (Q \times Z) \cap N_G(Q) && \text{(by Theorem 2.3(iii))} \\
&= Q \times Z. && \text{(since } Q \times Z \subset N_G(Q))
\end{aligned}$$

Thus by the Orbit-Stabiliser Theorem,

$$|\mathrm{Orb}(x)| = [N_G(Q) : Q \times Z] = \frac{eqk}{eq} = k$$

Since x was chosen arbitrarily from $Q\backslash I_G$, each element of $Q\backslash I_G$ has an orbit in $N_G(Q)$ of size k. Considering also the fact that $Q\backslash I_G$ is equal to the union of the pairwise disjoint orbits of its elements, we conclude that $k = g_1$ divides $|Q\backslash I_G|$. Thus there exists some $d \in \mathbb{Z}^+$ such that,

$$q - 1 = dg_1. \tag{3.11}$$

Now set,

$$i = \frac{2g_1g_2q}{g} > 0, \tag{3.12}$$

and multiply (3.10) by ig to give,

$$g_1q = i + (q-2)g_2. \tag{3.13}$$

Thus i is an integer and since it is greater than zero by definition, (3.13) gives,

$$g_1 > \frac{(q-2)g_2}{q}. \tag{3.14}$$

Also, using (3.11) and (3.13) we get,

$$\begin{aligned}
g_1q &= i + (q-1)g_2 - g_2 \\
&= i + dg_1g_2 - g_2, \\
g_2 &= i + (dg_2 - q)g_1. \qquad (3.15)
\end{aligned}$$

Applying Lemma 3.2 we observe that Q is not normal in G, and so

$$eg = |G| > |N_G(Q)| = eqk = eqg_1,$$

$$\frac{1}{qg_1} > \frac{1}{g}.$$

And (3.10) gives us,

$$\frac{1}{2g_2} = \frac{1}{g} - \frac{1}{qg_1} + \frac{1}{2g_1} < \frac{1}{2g_1},$$

$$g_1 < g_2. \tag{3.16}$$

Consider now,

$$[G : N_G(Q)] = \frac{eg}{eqk} = \frac{g}{qg_1} = \frac{2g_2}{i} \in \mathbb{Z}. \qquad \text{(by (3.12))}$$

Thus i divides $2g_2$. Recall that the order of A_2 is relatively prime to p by Theorem 2.3(iii), so g_2 is also relatively prime to p. Therefore if $p \neq 2$, i is relatively prime to p and if $p = 2$ then p divides i but p^2 does not. Now since Q is a Sylow p-subgroup of G, this means that greatest common denominator of i and q is either 1 or 2. Now consider,

$$[G : N_G(A_2)] = \frac{eg}{2eg_2} = \frac{g_1 q}{i} \in \mathbb{Z}. \qquad \text{(by (3.12))}$$

Thus i divides $g_1 q$ and since $\gcd(i, q) = 1$ or 2, i must divide $2g_1$. So there exists some $m \in \mathbb{Z}^+$ such that,

$$i = \frac{2g_1}{m}. \tag{3.17}$$

We consider now the separate cases which arise for different values of q.

• **Cases Va and Vb: $q \geq 4$.** This condition gives us a lower bound for the inequality in (3.14),

$$g_1 > \frac{(q-2)g_2}{q} > \frac{g_2}{2}.$$

Combining this with (3.16) we have,

$$g_1 < g_2 < 2g_1. \tag{3.18}$$

Substituting (3.17) into (3.15) gives,

$$g_2 = \left(\frac{2}{m} + dg_2 - q\right) g_1$$

Thus (3.18) gives that,

$$1 < \frac{2}{m} + dg_2 - q < 2.$$

This means that $2/m$ is some fraction between 0 and 1 and $dg_2 - q = 1$. So (3.15) becomes,

$$g_2 = g_1 + i. \tag{3.19}$$

Substituting this into (3.10) we find that,

$$\begin{aligned} g_1 q &= i + (q-2)(g_1 + i), \\ 2g_1 &= i(q-1) = idg_1, && \text{(by (3.11))} \\ 2 &= id. \end{aligned}$$

We remark that since both i and d are positive integers, i (and indeed d) must equal 1 or 2. Thus by (3.19) and (3.12),

$$g_1 = \frac{i(q-1)}{2}, \qquad g_2 = \frac{i(q+1)}{2}, \qquad g = \frac{2g_1g_2q}{i} = \frac{iq(q^2-1)}{2}.$$

Thus we have the following expressions for the orders of K and G:

$$|K| = \frac{ei(q-1)}{2}, \qquad |G| = \frac{eiq(q^2-1)}{2}. \tag{3.20}$$

By Proposition 1.11, each noncentral element of Q has a unique common fixed point on the projective line $\mathscr{L}$, call it P_1. Furthermore, we saw in the proof of Theorem 2.3(v) that each noncentral element of K also fixes P_1 as well as one other point, call it P_2. Let u be a noncentral element of Q and set $P_3 = P_2^u$. Clearly P_3 is different from P_1 and P_2 because otherwise a contradiction is reached. By Theorem 1.10, $PSL(\mathscr{L})$ is triply transitive, so there exists a $v \in L$ such that,

$$P_1^v = R_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \qquad P_2^v = R_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad P_3^v = R_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Observe that,

$$\begin{aligned} vQv^{-1}R_1 &= vQP_1 = vP_1 = R_1, \\ vKv^{-1}R_i &= vKP_i = vP_i = R_i. \qquad (i = 1, 2) \end{aligned}$$

Thus vQv^{-1} fixes R_1 whilst vKv^{-1} fixes both R_1 and R_2. The only elements of L that fix R_1 are the lower triangular matrices, thus $vQv^{-1} \subset H$, whilst the only elements that fix R_2 are the upper triangular matrices, thus $vKv^{-1} \subset D$. Furthermore, each noncentral element of vQv^{-1} has order p. The only elements of H with order p are those in T, thus $vQv^{-1} \subset T$. Since $u \in Q \setminus I_G$, we have that $vuv^{-1} = t_\gamma$ for some $\gamma \in F$.

$$vuv^{-1}R_2 = vuP_2 = vP_3 = R_3,$$

$$\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ \gamma \end{bmatrix} \sim \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \Longrightarrow \gamma = 1.$$

So $vuv^{-1} = t_1$. If we now consider $\widetilde{G} = vGv^{-1}$ instead of G, we can assume without loss of generality that,

$$Q \subset T, \qquad K \subset D, \qquad u = t_1.$$

Let x be a generator of K. By Theorem 2.3(iv) there exists a $y \in N_{\widetilde{G}}(K) \setminus K$ such that $yx = x^{-1}y$. Since R_1 is fixed by both x and x^{-1} we have,

$$x^{-1}yR_1 = yxR_1 = yR_1.$$

Thus x^{-1} fixes yR_1, that is $yR_1 \in \{R_1, R_2\}$. Similarly, $yR_2 \in \{R_1, R_2\}$. Assume $yR_1 = R_1$. Since R_1 and R_2 are distinct points in $\mathscr{L}$ this implies that $yR_2 = R_2$.

$$yR_1 = \begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\beta\\ \delta\end{bmatrix} \sim \begin{bmatrix}0\\1\end{bmatrix} \Longrightarrow \beta = 0.$$

$$yR_2 = \begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}\alpha\\ \gamma\end{bmatrix} \sim \begin{bmatrix}1\\0\end{bmatrix} \Longrightarrow \gamma = 0.$$

Thus $y \in D$, which is a contradiction since elements in D do not invert $x \in D$, hence,

$$yR_1 = R_2, \qquad \text{and} \quad yR_2 = R_1. \tag{3.21}$$

This allows us to determine more about y,

$$yR_1 = \begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\beta\\ \delta\end{bmatrix} \sim \begin{bmatrix}1\\0\end{bmatrix} \Longrightarrow \delta = 0.$$

$$yR_2 = \begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}\alpha\\ \gamma\end{bmatrix} \sim \begin{bmatrix}0\\1\end{bmatrix} \Longrightarrow \alpha = 0.$$

Thus y is an anti-diagonal matrix. Recalling (1.2), for some $\rho \in F^*$ we have,

$$y = d_\rho w = \begin{bmatrix}0 & \rho\\ -\rho^{-1} & 0\end{bmatrix}.$$

Consider now the set of right cosets of $N_{\widetilde{G}}(Q)$ of the form $N_{\widetilde{G}}(Q)yq$, (where $q \in Q$) in $N_{\widetilde{G}}(Q)yQ$. For $q_1, q_2 \in Q$ we have,

$$\begin{aligned} N_{\widetilde{G}}(Q)yq_1 = N_{\widetilde{G}}(Q)yq_2 &\iff yq_2{q_1}^{-1}y^{-1} \in N_{\widetilde{G}}(Q)\\ &\iff q_2{q_1}^{-1} \in y^{-1}N_{\widetilde{G}}(Q)y\\ &\iff (Q \cap y^{-1}N_{\widetilde{G}}(Q)y)q_2 = (Q \cap y^{-1}N_{\widetilde{G}}(Q)y)q_1. \end{aligned}$$

So the number of right cosets of $N_{\widetilde{G}}(Q)$ in $N_{\widetilde{G}}(Q)yQ$ is equal to the number of right cosets of $Q \cap y^{-1}N_{\widetilde{G}}(Q)y$ in Q. That is,

$$[N_{\widetilde{G}}(Q)yQ : N_{\widetilde{G}}(Q)] = [Q : Q \cap y^{-1}N_{\widetilde{G}}(Q)y]. \tag{3.22}$$

Let g be an arbitrary element of $N_{\widetilde{G}}(Q)$. By Theorems 1.6(i) and 1.11(ii) we have $N_{\widetilde{G}}(Q) \subset H = \mathrm{Stab}(R_1)$, thus g fixes R_1. Using (3.21) we see that,

$$y^{-1}gyR_2 = y^{-1}gR_1 = y^{-1}R_1 = R_2.$$

Hence R_2 is a fixed point of $y^{-1}gy$. Since g was chosen arbitrarily, we assert that each element of $y^{-1}N_{\widetilde{G}}(Q)y$ fixes R_2. On the contrary, the only element of Q which fixes R_2 is $I_{\widetilde{G}}$, thus $Q \cap yN_{\widetilde{G}}(Q)y^{-1} = I_{\widetilde{G}}$.

$$[N_{\widetilde{G}}(Q)yQ : N_{\widetilde{G}}(Q)] = [Q : Q \cap y^{-1}N_{\widetilde{G}}(Q)y] = q,$$
$$|N_{\widetilde{G}}(Q)yQ| = q|N_{\widetilde{G}}(Q)|. \tag{3.23}$$

We show next that $N_{\widetilde{G}}(Q)yQ \cap N_{\widetilde{G}}(Q) = \varnothing$. Let $t_\lambda d_\omega$ and t_μ be arbitrarily chosen from $N_{\widetilde{G}}(Q)$ and Q respectively so that $t_\lambda d_\omega y t_\mu$ is an arbitrary element of $N_{\widetilde{G}}(Q)yQ$.

$$\begin{aligned} t_\lambda d_\omega y t_\mu &= \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix} \\ &= \begin{bmatrix} \omega & 0 \\ \omega\lambda & \omega^{-1} \end{bmatrix} \begin{bmatrix} \rho\mu & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \\ &= \begin{bmatrix} \omega\rho\mu & \omega\rho \\ \omega\lambda\rho\mu - \omega^{-1}\rho^{-1} & \omega\rho\lambda \end{bmatrix}. \end{aligned} \tag{3.24}$$

Since ω, $\rho \in F^*$, the top right entry of (3.24) is non-zero. Recall also that $N_{\widetilde{G}}(Q) \subset H$ by Theorem 1.6(i) and that H is the set of all lower triangular matrices of L. Since $t_\lambda d_\omega d_\rho w t_\mu$ was chosen arbitraily, no element of $N_{\widetilde{G}}(Q)yQ$ is in H whilst the whole of $N_{\widetilde{G}}(Q)$ is contained in H, thus they are disjoint. Using (3.23) and (3.20) we also observe that,

$$|N_{\widetilde{G}}(Q)yQ| + |N_{\widetilde{G}}(Q)| = (q+1)|N_{\widetilde{G}}(Q)| = (q+1)eqg_1 = \frac{eiq(q^2-1)}{2} = |\widetilde{G}|.$$

Since $N_{\widetilde{G}}(Q)yQ$ and $N_{\widetilde{G}}(Q)$ are disjoint and the sum of their orders is equal to the order of $\widetilde{G}$, they partition $\widetilde{G}$ into the set of elements that belong to H and the set that don't.

$$\widetilde{G} = N_{\widetilde{G}}(Q)yQ \cup N_{\widetilde{G}}(Q). \tag{3.25}$$

Let $\mathbb{N} = \{\lambda : t_\lambda \in Q\}$. We will show that $\mathbb{N} = \mathbb{F}_q$. For each $t_\lambda \in Q \setminus Z$, the element $yt_\lambda y^{-1} \notin H$, so by (3.25), $yt_\lambda y^{-1} \in N_{\widetilde{G}}(Q)yQ$. Thus there exists $t_\mu, t_\upsilon \in Q$ and $d_\omega \in K$ such that,

$$yt_\lambda y^{-1} = t_\mu d_\omega y t_\upsilon,$$

$$\begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} 0 & -\rho \\ \rho^{-1} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \upsilon & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & \rho \\ -\rho^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & -\rho \\ \rho^{-1} & -\rho\lambda \end{bmatrix} = \begin{bmatrix} \omega & 0 \\ \omega\mu & \omega^{-1} \end{bmatrix} \begin{bmatrix} \rho\upsilon & \rho \\ -\rho^{-1} & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & -\rho^2\lambda \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \omega\rho\upsilon & \omega\rho \\ \omega\rho\mu\upsilon - \omega^{-1}\rho^{-1} & \omega\rho\mu \end{bmatrix}.$$

Equating the top right entries gives,

$$\omega = -\rho\lambda. \tag{3.26}$$

Since $t_1 \in Q$, so is it's inverse, thus $-1 \in \mathbb{N}$. Letting $\lambda = -1$ in (3.26) gives $\omega = \rho$, which means that $d_\rho \in K$. Consequently, this shows that $w = d_\rho^{-1} y \in \widetilde{G}$ and we may replace y by w in (3.25) without it affecting the partition of $\widetilde{G}$. This is equivalent to letting $\rho = 1$, and (3.26) simplifies to,

$$\omega = -\lambda. \tag{3.27}$$

Let $\mathbb{M} = \{\omega : d_\omega \in K\}$. Recall from (3.20) that $|K| = i(q-1)$. We consider the different cases which arise depending on the values of i and e.

Let **Case Va** be the case when $e = 1$ or $i = 1$. Observe that i and e cannot both equal 1, since this would imply that 2 divides $q-1$ (by (3.20)), but if $e = 1$ it follows that $q-1$ is even. Hence $ei = 2$ and K has order $q-1$. Furthermore, the order of each element of K divides $q-1$, so for each $\omega \in \mathbb{M}$,

$$\omega^{q-1} = 1. \tag{3.28}$$

Also, the following polynomial has at most $q-1$ roots in F.

$$x^{q-1} = 1. \tag{3.29}$$

By (3.2), $\mathbb{F}_q \subset F$ and each element of $\mathbb{F}_q^*$ is a root of (3.29). Thus each ω of $\mathbb{M}$ is in $\mathbb{F}_q^*$ and since they have the same cardinality, $\mathbb{M} = \mathbb{F}_q^*$. By (3.27), λ also ranges over $\mathbb{F}_q^*$ and considering also that λ can be 0, we have $\mathbb{N} = \mathbb{F}_q$.

Observe that each element of $\widetilde{G}$ is either of the form $t_\lambda d_\omega$ or $t_\lambda d_\omega w t_\mu$ (where $\lambda, \mu \in \mathbb{F}_q$, $\omega \in \mathbb{F}_q^*$), so $\widetilde{G} \subset SL(2, \mathbb{F}_q)$. Also, Propostion 3.4 gives that, $|SL(2, \mathbb{F}_q)| = q(q^2-1) = |\widetilde{G}|$, so $\widetilde{G} = SL(2, \mathbb{F}_q)$. Since $\widetilde{G}$ is conjugate in L to G, we have $G \cong SL(2, \mathbb{F}_q)$ as desired.

Let **Case Vb** be the case when $i = 2 = e$. This time the order of each element of K divides $2(q-1)$, so for each $\omega \in \mathbb{M}$,

$$\omega^{2(q-1)} = 1. \tag{3.30}$$

As in the case of $i = 1$, each element of $\mathbb{F}_q^*$ is a root of the polynomial in (3.29), as are each ω^2. Thus ω^2 ranges over $\mathbb{F}_q^*$ and by (3.2), $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Simple matrix multiplication shows that,

$$d_\omega^{-1} t_\lambda d_\omega = t_{\omega^2 \lambda}.$$

Hence since $t_0, t_1 \in Q$, it follows that $t_{\omega^2} \in Q$ for each $\omega^2 \in \mathbb{F}_q^*$, thus $\mathbb{N} = \mathbb{F}_q$. Since K is a cyclic group of order $2(q-1)$, so too is $\mathbb{M}$. Let π be a generator of $\mathbb{M}$. It follows that π^2 has order $q-1$ and is therefore a generator of $\mathbb{F}_q^*$. Since $K = \langle d_\pi \rangle$, we have:

$$\widetilde{G} = \langle t_\lambda, d_\pi, w : \lambda \in \mathbb{F}_q \rangle = \langle SL(2, \mathbb{F}_q), d_\pi \rangle.$$

Again, since $\widetilde{G}$ is conjugate in L to G, we have $G \cong \langle SL(2,\mathbb{F}_q), d_\pi\rangle$ as desired. Now we take an arbitrary x from $SL(2,\mathbb{F}_q)$ and conjugate it by d_π.

$$\begin{aligned} d_\pi x d_\pi^{-1} &= \begin{bmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \pi^{-1} & 0 \\ 0 & \pi \end{bmatrix} \\ &= \begin{bmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{bmatrix} \begin{bmatrix} \alpha\pi^{-1} & \beta\pi \\ \gamma\pi^{-1} & \delta\pi \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta\pi^{-2} \\ \gamma\pi^2 & \delta \end{bmatrix}. \end{aligned}$$

Since $\pi^2 \in \mathbb{F}_q$, we have that $d_\pi x d_\pi^{-1} \in SL(2,\mathbb{F}_q)$ and since x was chosen arbitrarily, d_π belongs to the normaliser of $SL(2,\mathbb{F}_q)$ in $\langle SL(2,\mathbb{F}_q), d_\pi\rangle$. This shows that $SL(2,\mathbb{F}_q) \lhd \langle SL(2,\mathbb{F}_q), d_\pi\rangle$ as desired.

• **Cases Vc and Vd: $\boldsymbol{q \le 3}$**. Since $q-1 = dg_1 \ge 2$ by (3.11), q cannot equal 2. So $q = 3 = p$, $e = 2$ and thus $g_1 = 2$. The inequalities in (3.16) and (3.14) give,

$$2 < g_2 < 6.$$

Also, since g_2 is relatively prime to $p = 3$, we have $g_2 = 4$ or 5. Let **Case Vc** be the case when $g_2 = 4$. (3.10) becomes,

$$\frac{1}{8} = \frac{1}{g} + \frac{1}{4} - \frac{1}{6},$$

which gives $g = 24$. Observe that,

$$|K| = 4 = i(q-1), \qquad |G| = 48 = iq(q^2-1),$$

where $i = 2$, thus we have the situation as described in Case Vb. That is, $G \cong \langle SL(2,\mathbb{F}_q), d_\pi\rangle$ with $q = 3$.

Alternatively, **Case Vd** occurs when $g_2 = 5$. (3.10) becomes,

$$\frac{1}{10} = \frac{1}{g} + \frac{1}{4} - \frac{1}{6}.$$

Thus $g = 60$ and $|G| = 120$. We verify, using Proposition 3.4, that $SL(2,5)$ has the same order as G, that is $|SL(2,5)| = 5(5^2-1) = 120$. Observe that,

$$\begin{aligned} |\mathcal{C}_1| &= [G : N_G(A_1)] = \frac{eg}{2eg_1} = 15, \\ |\mathcal{C}_2| &= [G : N_G(A_2)] = \frac{eg}{2eg_2} = 6, \\ |\mathcal{C}_{Q\times Z}| &= [G : N_G(Q\times Z)] = \frac{eg}{ekq} = 10. \end{aligned}$$

Now consider the quotient group G/Z of order 60. It's trivial that for all $A_i, A_j \in \mathfrak{M}$, A_i/Z belongs to the same conjugacy class as A_j/Z if and only A_i and A_j belong to the same conjugacy class. So the number of subgroups conjugate to A_i/Z is $|\mathcal{C}_i|$. Similarly, the number of subgroups conjugate to $(Q\times Z)/Z$ is $|\mathcal{C}_{Q\times Z}|$.

We now calculate the order of each maximal abelian subgroup of G when we quotient out Z.

$$|A_1/Z| = 2, \qquad |A_2/Z| = 5, \qquad |(Q \times Z)/Z| = 3.$$

We now know enough about G/Z to determine the order of each of it's elements:

• The identity has order 1.
• The non-central element of A_1/Z has order 2, as does the non-central element in each of the $|\mathcal{C}_1| = 15$ subgroups conjugate to A_1/Z. So there are 15 elements of order 2.
• The 4 non-central elements of A_2/Z have order 5, as do the non-central elements in each of the $|\mathcal{C}_2| = 6$ subgroups conjugate to A_2/Z. Thus there are 24 elements of order 5.
• The 2 non-central elements of $(Q \times Z)/Z$ have order 3, as do the non-central elements in each of the $|\mathcal{C}_{Q\times Z}| = 10$ subgroups conjugate to $(Q \times Z)/Z$. Thus there are 20 elements of order 3.

Since $1 + 15 + 24 + 20 = 60$, all elements of G/Z are accounted for.

Let N be a normal subgroup of G/Z. Observe that each non-central element of A_2/Z is a generator of it, so if N contains one non-central element of A_2/Z, then it contains the whole of it, due to the closure of the group under multiplication and the fact that each element of A_2/Z is a power of any non-central element. Also, it can easily be seen that normal subgroups are composed of whole conjugacy classes, so since N is normal in G, if it contains A_2/Z, it must contain all subgroups conjugate to A_2/Z. The consequence of this is that if N has an element of order 5, then it contains all 24 elements of G/Z of order 5. Similarly, if it contains an element of order 2, it contains all 15 of them and if it contains an element of order 3, it contains all 20 of them. This means that $|N|$ is partitioned by some or all of the elements in $\{1, 15, 20, 24\}$. Bearing in mind that the order of N divides 60 and that N contains the identity element, this means that N is equal to either the identity element or it is the whole of G/Z, since it's easy to see that no other partition of those numbers divides 60. Thus G/Z has no non-trivial normal subgroups and is simple.

By [4, p.145], the only simple groups of order 60 are those isomorphic to the alternating group A_5 (not to be confused with an element of $\mathfrak{M}$), thus $G/Z \cong A_5$. Since $Z \cong \mathbb{Z}_2$, we have that G is isomorphic to a central extension of A_5 which, according to Schur [7], is unique and isomorphic to $SL(2, 5)$ as desired. The proofs of these 2 claims are beyond the scope of this thesis. $\square$

Case VI:

Claim: *We have one of the following three cases:*

(i) $G = \langle\, x, y \,|\, x^n = y^2,\ yxy^{-1} = x^{-1} \,\rangle$, *where* n *is even.*

(ii) $G = \widehat{S}_4$.

(iii) $G \cong SL(2,5)$ *and* p *does not divide* $|G|$.

Where $\widehat{S}_4$ *is one of the representation groups of the symmetric group* S_4 *in which the transpositions correspond to the elements of order 4.*

Proof. Here, $s = 0$ and $t = 3$. Equation (2.16) simplifies to:

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

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2}. \tag{3.31}$$

First assume that $q > 1$ and $k = 1$. (3.31) is thus bounded as follows,

$$\frac{3}{4} > \frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{q-1}{qk} + \frac{1}{2} > 1,$$

which is a contradiction. Now assume that $q > 1$ and $k > 1$. This means that $k = g_i$ for some i. Without loss of generality we can assume that $k = g_1$. Now (3.31) becomes,

$$\frac{1}{2} \geq \frac{1}{2g_2} + \frac{1}{2g_3} \geq \frac{1}{g} + \frac{1}{2} > \frac{1}{2},$$

which again is a contradiction, thus we conclude that $q = 1$. (3.31) simplifies and we can now determine the possible values of each g_i.

$$\frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{1}{2}. \tag{3.32}$$

Without loss of generality we may assume that $2 \leq g_1 \leq g_2 \leq g_3$. If $g_1 \neq 2$ we arrive at the following contradiction

$$\frac{1}{6} + \frac{1}{6} + \frac{1}{6} \geq \frac{1}{2g_1} + \frac{1}{2g_2} + \frac{1}{2g_3} = \frac{1}{g} + \frac{1}{2}.$$

Thus $g_1 = 2$ and we have,

$$\frac{1}{2g_2} + \frac{1}{2g_3} > \frac{1}{4}. \tag{3.33}$$

Clearly g_2 must equal either 2 or 3. If $g_2 = 2$ it is easily shown that $g = 2g_3$. If $g_2 = 3$ we see that $g_3 \in \{3, 4, 5\}$. Assume that g_2 and $g_3 = 3$. Notice that since $g_1 = 2$, 2 must divide the order of G. Recall also that a Sylow p-subgroup of G has order 1, so we assert that $p \neq 2$ and $e = 2$. We see from (3.32) that $|G| = 24$ and thus a Sylow 3-subgroup has order 3. The maximal abelian subgroups conjugate to A_2 or A_3 have order 6 and therefore each contains a Sylow 3-subgroup of G. Let B_2 and B_3 be the Sylow 3-subgroups contained in A_2 and A_3 respectively. Observe that for $i = 2$ or 3,

$$A_i \cong \mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong B_i \times Z \cong B_i Z. \tag{3.34}$$

Let $b_2 \in B_2$, $b_3 \in B_3$ and $z \in Z$. Recall that B_2 and B_3 are conjugate in G by Sylow's Second Theorem, so there exists an $x \in G$ such that,

$$\begin{aligned} xb_2x^{-1} &= b_3, \\ xb_2x^{-1}z &= b_3z, \\ xb_2zx^{-1} &= b_3z. \end{aligned}$$

Since b_2, b_3 and z were chosen arbitrarily, we observe that B_2Z is conjuagate to B_3Z and thus by (3.34), $A_2 \cong A_3$. This contradicts the fact that A_2 and A_3 are representatives of different conjugacy classes of maximal abelian subgroups of G, which means that g_2 and g_3 cannot both equal 3. Thus we are left with the following three cases:

$$\begin{array}{lll} g_1 = 2, & g_2 = 2, & g = 2g_3. \\ g_1 = 2, & g_2 = 3, & g_3 = 4. \\ g_1 = 2, & g_2 = 3, & g_3 = 5. \end{array}$$

- **Case VIa: $\boldsymbol{g_1 = 2, g_2 = 2, g = 2g_3}$.** First observe that,

$$[G : N_G(A_1)] = \frac{eg}{2eg_1} = \frac{g_3}{2}.$$

Thus $g_3/2$ is an integer which means that g_3 must be even, call it n. Now let $A_3 = \langle x \rangle$. Since $|A_3| = eg_3$, the order of x is $2n$ and x^n has order 2. By Theorem (2.3)(iv) there exists a $y \in N_G(A_3) \backslash A_3$ such that $yxy^{-1} = x^{-1}$. Also,

$$|\mathcal{C}_3| = [G : N_G(A_3)] = 1.$$

Since $y \notin A_3$ and A_3 has no conjugate subgroups (aside from itself), y must lie in a maximal abelian subgroup conjugate to either A_1 or A_2. This means that since $|A_1| = 4 = |A_2|$ and $y \notin Z$, the order of y must be 4. By the uniqueness of the element of order 2, we have the relation $x^n = y^2$ and G is given by the presentation,

$$G = \langle\, x, y \,|\, x^n = y^2,\ yxy^{-1} = x^{-1} \,\rangle. \qquad \text{(where } n \text{ is even)}$$

• **Case VIb: $g_1 = 2, g_2 = 3, g_3 = 4$**. In this case (3.32) becomes,

$$\frac{1}{4} + \frac{1}{6} + \frac{1}{8} = \frac{1}{g} + \frac{1}{2}.$$

Thus $g = 24$ and $|G| = 48$. Consider the quotient group G/Z of order 24 and the quotient group $N_G(A_2)/Z$ which, for convenience, we will call H.

$$|H| = \frac{2eg_2}{e} = 6.$$

Let x be an element of order 6 from A_2. By Theorem 2.3(iv) there exists a $y \in N_G(A_2) \backslash A_2$ such that $yx = x^{-1}y$. Thus for $xZ, yZ, x^{-1}Z \in H$ we have,

$$yZxZ = yxZ = x^{-1}yZ = x^{-1}ZyZ.$$

If H is abelian, then $xZ = x^{-1}Z$ and thus $x^2 \in Z$. Also, since x has order 6, x^2 has order 3. This is contradiction since there is no element of order 3 in Z. Thus H is non-abelian and is therefore isomorphic to the symmetric group S_3.

Now we determine the normal subgroups of H. The identity and H itself are trivially normal. Furthermore, the elementary result that any subgroup of index 2 is normal implies that A_2/Z, the subgroup of H of order 3, is normal. It remains to check the subgroups of order 2. Let r be a generator of one of the subgroups of order 2 and let x be an arbitrary element of H. If $\langle r \rangle$ is normal in H, then $xrx^{-1} \in \{I, r\}$. Since $r \neq I$ it follows that $xrx^{-1} \neq I$. Alternatively if $xrx^{-1} = r$, then $r \in Z(H)$. By the elementary result that $Z(S_n) = \{I\}$ for $n > 2$, we have that $Z(H) = \{I\}$ and the contradiction $r = I$. Thus $xrx^{-1} \notin \langle r \rangle$ and H has no normal subgroup of order 2. We conclude that the only normal subgroups of H are those of order 1, 3 or 6.

Note that the index of H in G/Z is 4. Let G/Z act by left multiplication on the set of left cosets of H. By Theorem 0.3, this action induces a homomorphism $\phi : G/Z \longrightarrow S_4$ with kernel,

$$ker(\phi) = \bigcap_{x \in G/Z} xHx^{-1} \subset H.$$

Recall the elementary result that the kernel of a homomorphism is a normal subgroup of it's domain. Thus the kernel of ϕ is normal in G/Z and consequently in H as well, that is $ker(\phi) \in \{I, A_2/Z, H\}$.

If $ker(\phi) = A_2/Z$, then $A_2/Z \lhd G/Z$ and by Lemma 3.5 $A_2 \lhd G$. This is a contradiction since the normaliser in G of A_2 is a proper subgroup of G, thus $ker(\phi) \neq A_2/Z$.

If $ker(\phi) = H$, then $H \lhd G/Z$. Take an arbitrary $x \in G/Z$. Since A_2/Z is a subgroup of H we get,

$$x(A_2/Z)x^{-1} \subset H.$$

Furthermore, since A_2/Z has order 3, any subgroup conjugate to it has order 3. Since the only subgroup of H of order 3 is A_2/Z, and since x was chosen arbitrarily, $A_2/Z \lhd G/Z$. We have already shown that this leads to a contradiction, thus $ker(\phi) \neq H$.

We conclude that $ker(\phi) = \{I\}$ and so ϕ is injective. Since G/Z has 24 elements, it's image under ϕ is the whole of S_4, that is $G/Z \cong S_4$. Thus G is a *representation group* of S_4, denoted by $\widehat{S}_4$ (for a full defintion of this, see [9]). Suzuki proves that S_4 has 2 distinct representation groups up to isomorphism [9, p.301], which are distinguished by the property that the elements corresponding to transpositions have either order 2 or order 4. Since G has a unique element of order 2, it must be isomorphic to the representation group of S_4 in which the transpositions correspond to the elements of order 4, as desired.

- **Case VIc: $\boldsymbol{g_1 = 2, g_2 = 3, g_3 = 5}$.** In this case (3.32) becomes,

$$\frac{1}{4} + \frac{1}{6} + \frac{1}{10} = \frac{1}{g} + \frac{1}{2}.$$

Thus $|g| = 60$ and $|G| = 120$. Observe that a simple relabelling of the maximal abelian subgroups gives the same situation as described in **Case Vd:**. Thus $G \cong SL(2,5)$, however in this case p does not divide $|G|$.

$\square$

3.3 Dickson's Classification Theorem

We now state the main result of this paper, Dickson's classification of finite subgroups of $SL(2,F)$. Observe that it is not the focus of this paper to determine whether the following groups actually exist, rather that this theorem can be regarded as an *upper bound*, so to speak, of the only possible subgroups of $SL(2,F)$.

Theorem 3.6. *Let F be an arbitary algebraically closed field of characteristic p. Any finite subgroup G of $SL(2,F)$ is isomorphic to one of the following groups.*

***Class I**: When $p = 0$ or $|G|$ is relatively prime to p:*

(i) A cyclic group.

(ii) The group defined by the presentation:

$$\langle\, x, y \,|\, x^n = y^2,\, yxy^{-1} = x^{-1} \,\rangle.$$

(iii) The Special Linear Group $SL(2,3)$.

(iv) The Special Linear Group $SL(2,5)$.

(v) $\widehat{S}_4$, the representation group of S_4 in which the transpositions correspond to the elements of order 4.

Class II: *When $|G|$ is divisible by p:*

(vi) Q is elementary abelian, $Q \lhd G$ and G/Q is a cyclic group whose order is relatively prime to p.

(vii) $p = 2$ and G is a dihedral group of order $2n$, where n is odd.

(viii) The Special Linear Group $SL(2, 5)$, where $p = 3 = q$.

(ix) The Special Linear Group $SL(2, \mathbb{F}_q)$.

(x) The group $\langle SL(2, \mathbb{F}_q), d_\pi \rangle$, where $SL(2, \mathbb{F}_q) \lhd \langle SL(2, \mathbb{F}_q), d_\pi \rangle$.

Here, Q is a Sylow p-subgroup of G of order q, $\mathbb{F}_q$ is a field of q elements, $\mathbb{F}_{q^2}$ is a field of q^2 elements, $\pi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\pi^2 \in \mathbb{F}_q$.

Proof. If $Z \not\subset G$, then G has no element of order 2 and $|G|$ is therefore odd. Observe that in Cases II, IV, V and VI, $|G|$ is always even, thus we have either Case I or III. These correspond to Class I (i) or Class II (vi).

If $Z \subset G$, then G has the same structure as one of the 6 cases previously discussed. We match the separate cases to the above classes.

Case Ia: This leads to Class I (i).
Case Ib: This leads to Class II (vi).
Case IIa: This leads to Class I (ii) where n is odd.
Case IIb: This leads to Class I (iii).
Case III: If $G = Z$ this leads to Class I (i), otherwise to Class II (vi).
Case IVa: This leads to Class II (vii).
Case IVb: This leads to Class II (ix) with $q = 3$.
Case Va: This leads to Class II (ix).
Case Vb: This leads to Class II (x).
Case Vc: This leads to Class II (x) with $q = 3$.
Case Vd: This leads to Class II (viii).
Case VIa: This leads to Class I (ii) where n is even.
Case VIb: This leads to Class I (v).
Case VIc: This leads to Class I (iv).

$\square$

Bibliography

[1] Alperin, J.L., Bell, R.B. *Groups and Representations.* Springer, (1995).

[2] Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R. *Basic Abstract Algebra, Second Edition.* Cambridge University Press, (1994).

[3] Dickson, L.E. *Linear Groups, with an Exposition of the Galois Field Theory.* B.G.Teubner, Leipzig, (1901).

[4] Dummit, D.S., Foote, R.M. *Abstract Algebra.* Wiley, (2004).

[5] Holst, A., Ufnarovski, V. *Matrix Theory.* Studentlitteratur, (2014).

[6] Hungerford, T.W. *Abstract Algebra: An Introduction, Third Edition.* Brooks/Cole, Cengage Learning, (2014).

[7] Schur, I. *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen.* Journal für die reine und angewandte Mathematik (Crelles Journal) (139), p.155-250. De Gruyter, (1911).

[8] Stewart, I. *Galois Theory, Third Edition.* Chapman & Hall/CRC, (2003).

[9] Suzuki, M. *Group Theory I.* Spinger-Verlag, Berlin, Heidelberg, New York, (1982).