Methods For Identifying Finite Groups

Sarah Astill - 321130

April 2005

I warrant that the content of this dissertation is the direct result of my own work and that any use in it of published or unpublished material is fully and correctly referenced.

Signed ....

Date ....

CONTENTS

1. *Introduction* 1

2. *Further Group Theory* 7

   2.1 Some Elementary Results 7

   2.2 Group Actions and Automorphism Groups 11

   2.3 Some Further Results 15

3. *Some Representation Theory* 18

   3.1 Representations and Modules 18

   3.2 An Application 24

4. *Identifying Groups by Constructing Amalgams and the Coset Graph* 27

   4.1 Amalgams and Completions 27

   4.2 The Coset Graph 30

   4.3 An Example of a Coset Graph 33

   4.4 Periodic Groups with Dihedral Centraliser of an Involution 39

   4.5 Identifying the Group 46

   4.6 The Theorem 52

5. *Identifying Groups by Counting Involutions* 53

   5.1 The Hypothesis and Preliminary Results 53

   5.2 Case 1: $\rho = 2$ 61

   5.3 $\mathrm{PGL}_2(\mu)$ 64

   5.4 Case 2: $\rho > 2$ 70

   5.5 $\mathrm{PSL}_2(2^\epsilon)$ 75

   5.6 The Theorem 76

6. Conclusion 78

1. INTRODUCTION

Any finite simple group is isomorphic to one of the following

- C_p - The cyclic groups of prime p order,
- Alt_n - The alternating groups of degree $n \geq 5$,
- Finite simple groups of *Lie* type,
- 26 *sporadic* finite simple groups.

This is the classification of the finite simple groups which was completed in 1981 and the proof of which consists of over 10,000 journal pages. Methods for recognising the isomorphism type of a finite group are of course necessary throughout.
A fundamental result in the classification is Feit and Thompson's odd order theorem of 1963.

Odd Order Theorem (Feit-Thompson)**.** *Finite groups of odd order are soluble.*
[1, p259]

The only simple, soluble groups are the groups of prime orders (see [12, p153, (7.55)]) so the odd order theorem tells us that if G is a simple group and non-abelian then G cannot have odd order otherwise G would be soluble and hence cyclic of prime order and so abelian. So any non-abelian, finite simple group has even order. Cauchy's theorem tells us that any finite group of even order has an element of order two. Thus a great deal of group theory in the 1960's and 70's was concerned with involutions (elements of order two). Indeed, the Brauer-Fowler Theorem (1965) suggested that considering the centraliser of an involution would be a good approach to the classification problem and this was used in much of the mathematics that contributed to the eventual classification.

Brauer-Fowler Theorem. *Let H be a finite group. Then there exists at most a finite number of finite simple groups G with an involution whose centraliser in G is isomorphic to H.*
[1, p243, (45.5)]

For example the Thompson Order Formula gives a formula for finding the order of a group G with more than one conjugacy class of involutions by considering the centralisers of involutions.

Thompson Order Formula. *Let G be a group with $k \geq 2$ conjugacy classes of involutions, ${x_1}^G, {x_2}^G, \ldots, {x_k}^G$ say, and let n_i be the number of ordered pairs (u, v) with $u \in x_1^G$, $v \in x_2^G$ and $x_i \in \langle uv \rangle$. Then*

$$|G| = |C_G(x_1)||C_G(x_2)| \left(\sum_{i=1}^{k} \frac{n_i}{|C_G(x_i)|} \right).$$

[1, p244,(45.6)]

In Chapter 4 we will consider the centraliser of an involution however we are faced with a group with just one class of involutions and so a different approach is needed here. In Chapter 5, which is almost entirely based on the 2001 paper *Counting Involutions* by Aschbacher, Meierfrankenfeld and Stellmacher [2], we consider a group which may or may not have more than one class of involutions and so we rely upon a technique of Bender [3]. This technique considers the distribution of involutions within the cosets of a given subgroup. Bender proves that if the index of the given subgroup is sufficiently small compared to the number of involutions then few involutions will lie in a coset in which they are a unique involution. This idea that involutions are in a sense *well distributed* between cosets is used in *Counting Involutions* as it appears to work no matter how many classes of involutions.

The main theorem of Chapter 5 is

Theorem. *Let G be a finite group and $M \leq G$. Let M be such that its conjugates in G are either equal to M or intersect trivially with M. Suppose then that $M^* := N_G(M) = MC_{M^*}(z)$ for some involution z from M^* and assume also that $C_G(x)$ has odd order for each non-trivial*

$x \in M$. Suppose further that M is not normal in G and that the number of involutions in G is greater than the index of M in G. Then one of the following are true.

- *$G \cong \mathrm{PGL}_2(\mu)$ or $\mathrm{PSL}_2(\mu)$ where $\mu = |M|$ is a power of some prime p and M is an elementary abelian p-group,*
- *$G \cong \mathrm{PSL}_2(2^\epsilon)$ for some integer $\epsilon \geq 2$ and M has order $2^\epsilon + 1$,*
- *$G = RM^*$ for some elementary abelian group of order $2^{2\delta}$ and M^* is dihedral of order $2(2^\delta + 1)$ for some positive integer δ.*

[2, p1]

Two of these cases identify the group as a *linear* group. For a natural number n and a prime power q, $\mathrm{GL}_n(q)$ is known as the *general linear* group. This is the group of all $n \times n$ invertible matrices with entries from the finite field $\mathrm{GF}(q)$ (note that $\mathrm{GF}(q)$ is known as the *Galois field of order* q which is the unique field of this size). Alternatively it can be viewed as the group of all invertible linear transforms from a vector space of dimension n over $\mathrm{GF}(q)$. $\mathrm{GL}_n(q)$ has a subgroup $\mathrm{SL}_n(q)$, the *special linear* group. This group has index $q-1$ (possibly equal to 1) in $\mathrm{GL}_n(q)$ and is the subgroup of all matrices with determinant 1. The theorem identifies factor groups of these two linear groups. The first is the *projective linear* group, $\mathrm{PGL}_n(q)$ which is $\mathrm{GL}_n(q)$ factored by its center (which turns out to be the diagonal matrices). The second is the *projective special linear* group, $\mathrm{PSL}_n(q)$, which is $\mathrm{SL}_n(q)$ factored by its center (which again turns out to be diagonal matrices). The group turns out to be isomorphic to $\mathrm{PSL}_2(q)$ under certain conditions and $\mathrm{PGL}_2(q)$ under certain other conditions. Both groups can be embedded into symmetric groups by considering the action on sets of 1-dimensional vector spaces. To say a group H can be embedded in a group G means there is an injective homomorphism from H into G, so the image of H is a subgroup of G. Proving that the injective images of these linear groups inside of a symmetric group is unique (up to conjugation by elements of the symmetric group) proves that an abstract group which can be embedded in the same way into the same symmetric group must be isomorphic to the given linear group. The subtlety here in recognising the groups as isomorphic is understanding that an actual isomorphism between groups is not necessary and this is made clear by the proof given.

The main theorem in Chapter 4 is

Theorem. *Let G be a periodic group with exactly one conjugacy class of involutions such that the centraliser in G of an involution $t \in G$ is $C_G(t) \cong \mathrm{Dih}(8)$. Then $G \cong \mathrm{PSL}_3(2)$ or $G \cong \mathrm{Alt}(6)$.* [11, p12]

In the first case we recognise that $\mathrm{PSL}_3(2)$ can be embedded in $\mathrm{Sym}(7)$. Consider the set of seven vectors

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

$\mathrm{PSL}_3(2)$ is a group of cosets of $\mathrm{Z}(\mathrm{SL}_3(2))$. However $\mathrm{Z}(\mathrm{SL}_3(2))$ turns out to be trivial and $\mathrm{SL}_3(2)$ turns out to be the whole of $\mathrm{GL}_3(2)$. So $\mathrm{PSL}_3(2)$ is isomorphic to the group of all invertible matrices with 0 and 1 entries. It is hence easy to see that this group acts on the set of vectors. Moreover this action is faithful and we will see that this allows us to define an embedding in $\mathrm{Sym}(7)$. Having recognised that $\mathrm{PSL}_3(2)$ is isomorphic to a subgroup of $\mathrm{Sym}(7)$ we can prove our arbitrary group is isomorphic to $\mathrm{PSL}_3(2)$ by embedding it in $\mathrm{Sym}(7)$ in such a way that we get the same subgroup.

In the second case we prove our group is isomorphic to $\mathrm{Alt}(6)$. The alternating groups are the subgroups of the symmetric groups containing even permutations only. An important fact is that the alternating groups of degree five or more are simple groups (see [12, p65, 3.60]). The alternating group $\mathrm{Alt}(n)$ has index two inside of the corresponding symmetric group $\mathrm{Sym}(n)$ and a consequence of the simplicity is that it is the unique subgroup with index two. To prove an arbitrary group G is isomorphic to $\mathrm{Alt}(6)$ we hence have to prove it can also be embedded at this index. To do this we find a subgroup K isomorphic to $\mathrm{Alt}(5)$ and let G act on the six cosets. The kernel of this action is

$$\mathrm{Core}_G(K) = \bigcap_{g \in G} K^g.$$

This is a normal subgroup of K which is a simple group and so we have to prove it cannot be equal to K and so must be trivial. This gives the embedding in Sym(6) as required.

In order to understand enough about our abstract group to find this group K we need to introduce some new tools. We hence investigate in detail the so-called *coset graph.* This provides a useful tool as we can consider how G acts on this graph. Knowing how a group acts on a set immediately gives information about a group. However seeing how the group acts on the coset graph gives more information. It turns out that vertex stabilisers are G-conjugate as are the edge stabilisers. How these subgroups intersect inside the group is mirrored by how the vertices join up. The coset graph is almost like a planar graph representation of the geometric structure of the group, i.e. how the subgroups fit inside the group.

Consider the following graph Γ^* which turns out to be analogous to the graph that will be considered in Chapter 4. Let Ω be the set of six points $\{1, 2, 3, 4, 5, 6\}$ and let V be the set of permutations

$$V := \{(a, b)(c, d)(e, f) \mid a, b, c, d, e, f \in \Omega\} \cup \{(i, j) \mid i, j \in \Omega\}.$$

Consider the relation

$$(i, j) \sim (a, b)(c, d)(e, f) \text{ if and only if } \{i, j\} \in \{\{a, b\}, \{c, d\}, \{e, f\}\}.$$

From this we can form a graph with vertex set V and edges between vertices which are related by $\sim$.

This graph is connected and bi-partite which means that the vertices form two disjoint sets such that edges exist only between vertices from opposite sets. It is easy to see the vertex set has size 30 and each vertex has valency three.

With a little thought we can see that no cycle can have length four or six. Just consider without loss of generality the vertex $(1, 2)$ which is adjacent to $(1, 2)(3, 4)(5, 6)$. This is then adjacent to $(3, 4)$ and $(5, 6)$ but no vertex of the form $(a, b)(c, d)(e, f)$ can form a four cycle. Similar reasoning shows there can be no cycles of length six. Of course we could also just write out the whole graph to verify this.

Alt(6) is the group of even permutations on six letters so consider an action of Alt(6) on the vertices of the graph simply as an action on the six letters. It is clear that this action maintains the graph and from here we can think about which elements of Alt(6) fix points and which elements fix edges (or two adjacent points). It turns out that the stabiliser of a vertex is isomorphic to Sym(4) and the stabiliser of an edge is isomorphic to Dih(8) (see Section 4.3). The coset graph we will later consider turns out to be exactly the same graph.

To summarise, the aim of this report is to introduce some techniques for recognising finite groups. It is necessary in the classification of the finite simple groups to be able to recognise groups and to also recognise when one simple group can be classified in more than one way (when a simple group can be classified in more than one way it is known as an *exceptional isomorphism*). We begin by introducing some necessary group theory in Chapter 2 and some representation theory in Chapter 3. This is needed for Chapters 4 and 5. The former introduces the concept of an amalgam and investigates the coset graph in preparation for recognising the periodic group as described. The latter expands upon the paper *Counting Involutions* eventually proving the possible isomorphism type of the finite group.

2. FURTHER GROUP THEORY

It is necessary to begin by introducing some group theory. We begin with some elementary group theory and go on to consider some further results related to group actions and group automorphisms. Included also, without proof, are some advanced results which will be relied upon in later chapters. Unless otherwise stated groups are assumed to be finite. Knowledge of group actions and Sylow's theorem is assumed.

2.1 Some Elementary Results

In Chapters 4 and 5 we will need to become familiar with some new types of groups. These are *elementary abelian groups*, *dihedral groups*, *automorphism groups*, *p-radical subgroups* for a given prime p and *commutator subgroups*.

Definition 2.1. *A group A is called elementary abelian if it is abelian and there exists some prime p such that $a^p = 1$ for every $a \in A$.*

The reader is referred at this point to the *structure theorem for finitely generated abelian groups* 8.24 in [12]. This states that every finite abelian group is the direct product of cyclic subgroups. This can be used to show that any elementary abelian group of size p^n say, is a direct product of n cyclic groups of order p and gives the following result.

Lemma 2.2. *An elementary abelian group A of order p^n for some prime p and integer n is isomorphic to a direct product of n cyclic groups of order p and so is unique up to isomorphism.*

Definition 2.3. *A group D is called dihedral if it is generated by two elements, say $D = \langle x, i\rangle$ where i is an involution and $x^i = x^{-1}$.*

This definition implies uniqueness of dihedral groups up to isomorphism. If D and E are dihedral groups of size $2n$ say (each contains an involution so the order is always even), then each is generated by an involution and an element inverted by the involution. Hence mapping both such elements in D to the corresponding element in E gives an isomorphism. Any non-abelian group which can be generated by two involutions is also dihedral. To see this let $D = \langle s, t\rangle$ where s, t are involutions, then $D = \langle s, st\rangle$ and the element st is inverted by s so D is dihedral.

Lemma 2.4. *If $A \leq G$ is a finite cyclic group and $t \in G - A$ is an involution inverting A then $D := \langle A, t\rangle$ is dihedral and A has index two in D.*

(To say t *inverts* A is to say that $a^t = a^{-1}$ for every $a \in A$.)

Proof. $D = \langle A, t\rangle = \langle a, t\rangle$ (where $\langle a\rangle = A$) is dihedral by definition since t is an involution and inverts A so in particular $a^t = a^{-1}$.
Since the set $\{a, t\}$ generates D and $A \trianglelefteq D$ then the set $\{Aa, At\}$ generates the group D/A. This is because for any $Ad \in D/A$, ($d \in D$), the element d is generated by elements from $\{a, t\}$ and so the corresponding choice of elements from $\{Aa = A, At\}$ will give Ad (because $AxAy = Axy$ since A is a normal subgroup). Thus $D/A = \langle A, At\rangle = \langle At\rangle$ since At is an element of order two. It follows that $|D/A| = 2$ and so A has index two in D. Moreover $D = A \cup At = A\langle t\rangle$.

□

Since any finite dihedral group contains an involution then it must have even order. In Chapter 5 we will also consider finite groups with odd order. Such a group contains no involutions but can be generated in a different way.

Lemma 2.5. *Suppose G is a group of odd order then $G = \langle g^2 \mid g \in G\rangle$.*

Proof. Any element in G has odd order. So pick $x \in G^{\#}$ ($^{\#}$ means the group without its identity) with order $2k + 1$ say. Let $h = x^k$. Then $1 = xx^{2k} = xh^2$. So $x = (h^{-1})^2 \in \langle g^2 \mid g \in G\rangle$.

□

Definition 2.6. *An automorphism of a finite group G is an isomorphism $\alpha : G \to G$. The set, $\mathrm{Aut}(G)$, of all automorphisms forms a group with respect to composition of maps.*

Example 2.7. Consider the automorphism group of $C_2 \times C_2$. $C_2 \times C_2 = \{(1,1),(x,1),(1,x),(x,x)\}$ is generated by $(1,x)$ and $(x,1)$. Since $(1,1)$ is the identity this is always fixed and so any automorphism is determined by the images of these generators. This gives six automorphisms

$$\begin{array}{ccccccccccc}
\phi_1 & : & (x,1) & \longmapsto & (x,1)) & \phi_4 & : & (x,1) & \longmapsto & (1,x) \\
 & & (1,x) & \longmapsto & (1,x) & & & (1,x) & \longmapsto & (x,x) \\
\phi_2 & : & (x,1) & \longmapsto & (x,1) & \phi_5 & : & (x,1) & \longmapsto & (x,x) \\
 & & (1,x) & \longmapsto & (x,x) & & & (1,x) & \longmapsto & (x,1) \\
\phi_3 & : & (x,1) & \longmapsto & (1,x) & \phi_6 & : & (x,1) & \longmapsto & (x,x) \\
 & & (1,x) & \longmapsto & (x,1) & & & (1,x) & \longmapsto & (1,x).
\end{array}$$

It is clear that these six automorphism are acting faithfully on the set $\{(1,x),(x,1),(x,x)\}$ and it follows that $\mathrm{Aut}(C_2 \times C_2) \cong \mathrm{Sym}(3)$.

For each $g \in G$ an automorphism of G can be defined which we will call C_g where $C_g : x \mapsto x^g$. This automorphism is called the *inner automorphism of G induced by g*. The set of all inner automorphisms of G, $\mathrm{Inn}(G)$, is a subgroup of $\mathrm{Aut}(G)$. Given a non-empty set of automorphisms A, of G and some $H \leq G$ then H is A-invariant if $h\alpha \in H$ for every $h \in H$ and every $\alpha \in A$. In particular if H is $\mathrm{Aut}(G)$-invariant then H is said to be *characteristic* in G (or H char G). Notice that this is a stronger condition on H than normality which is equivalent to being $\mathrm{Inn}(G)$-invariant.

Lemma 2.8. *If $H \trianglelefteq G$ and K is a characteristic subgroup of H then $K \trianglelefteq G$.*

Proof. $H \trianglelefteq G$ so for each $g \in G$, $H^g = H$ and so the inner automorphism C_g, on restriction to H, is an automorphism of H. Since K char H then K is C_g invariant so $kC_g = k^g \in K$ for all $k \in K$. This holds for each $g \in G$ and so $K \trianglelefteq G$.

□

Definition 2.9. *Let G be a finite group and p a prime. Then G has a unique largest normal p-subgroup $O_p(G)$. This is called the p-radical of G.*

In fact $O_p(G)$ is the intersection of all the Sylow p-subgroups in G.

Lemma 2.10. *Let G be a finite group and p a prime. Then $O_p(G)$ is a characteristic subgroup of G.*

Proof. Let $\alpha \in \mathrm{Aut}(G)$, then α is a bijection so for $S \in \mathrm{Syl}_p(G)$, $S\alpha \in \mathrm{Syl}_p(G)$ and so

$$O_p(G)\alpha = (\bigcap_{S\in\mathrm{Syl}_p(G)} S)\alpha = \bigcap_{S\in\mathrm{Syl}_p(G)} (S\alpha) = \bigcap_{S\in\mathrm{Syl}_p(G)} S = O_p(G).$$

□

Definition 2.11. *The commutator of two elements x, y of a group G is*

$$[x, y] = x^{-1}y^{-1}xy.$$

Given $H, K \leq G$ the commutator subgroup is

$$[H, K] = \langle [h, k] \mid h \in H, k \in K\rangle.$$

Similarly, given $H \leq G$ and some $x \in G$ the commutator subgroup is

$$[H, x] = \langle [h, x] \mid h \in H\rangle.$$

Notice that $[x^g, y^g] = [x, y]^g$ and the result holds in the commutator subgroups also.

The *derived subgroup* of a group G is

$$G' := [G, G].$$

G' is a normal subgroup of G since for an element $[g, h] \in G'$ it is easy to see that for any $x \in G$ $[g, h]^x = [g^x, h^x] \in G'$.

Lemma 2.12. *The derived subgroup G' of a group G is the unique smallest normal subgroup K of G such that G/K is abelian.*

Proof. Let $K \trianglelefteq G$. G/K is abelian if and only if $Kxy = KxKy = KyKx = Kyx$ for all $x, y \in G$ if and only if $Kxyx^{-1}y^{-1} = K$ if and only if $[x, y] \in K$ for all $x, y \in G$. So G/K is abelian if and only if $G' \leq K$. Since $G' \trianglelefteq G$ then G/G' is abelian. Moreover if K is another normal subgroup with the same order as G' and with G/K abelian then $G' \leq K$ but then they must be equal which gives uniqueness.

□

Example 2.13. Consider the derived subgroup of $G := \mathrm{Dih}(8)$. This group has three normal subgroups at index two and one normal subgroup at index four namely its center. Suppose G' had index two in G then G/G' would clearly be abelian. However G has two other subgroups at this index which must both have abelian factor groups contradicting the uniqueness. By the previous result though the derived subgroup is contained in these index two subgroups and so cannot be G itself. Also G is non-abelian and so its derived subgroup is non-trivial. Hence $G' = Z(G)$.

Now consider $S := \mathrm{Sym}(n)$ for some $n \geq 5$. Clearly $S/\mathrm{Alt}(n) \cong C_2$ is abelian and so $S' \leq \mathrm{Alt}(n)$. However $S' \trianglelefteq \mathrm{Alt}(n)$ which is a simple group and S is not abelian so S' is non-trivial hence $S' = \mathrm{Alt}(n)$.

Finally a result which is often useful is Dedekind's Modular Law.

Lemma 2.14 (Dedekind's Rule)**.** *Suppose $A, B, C \leq G$ with $B \leq A$. Then*

$$A \cap (BC) = B(A \cap C).$$

Proof. Let bx any element from $B(A \cap C)$ where $b \in B$, $x \in C \cap A$. Since $B \leq A$ then $b \in A$ and so $bx \in A$ and $bx \in BC$. Hence $B(A \cap C) \subseteq A \cap (BC)$.

Let $a \in A \cap (BC)$ then $a = bc$ for some $b \in B$ and $c \in C$. Thus $b^{-1}a = c \in A \cap C$ as $B \leq A$. It follows that $a \in B(A \cap C)$ and so $A \cap (BC) = B(A \cap C)$.

□

2.2 Group Actions and Automorphism Groups

The way a finite group acts on a set of points gives many clues about the structure of that group. A particular example the reader may be familiar with is the action of a group on the set of cosets of a subgroup gives a homomorphism into a symmetric group. In this project we aim to manipulate groups in this way by creating sets and groups on which an abstract group can act so as to gain some insight into the structure of the group. For this purpose we need to understand more about group actions.

Definition 2.15. *A group G acts faithfully on a set Ω if only the identity fixes every point. G acts regularly if it acts transitively and each $\omega \in \Omega$ has trivial stabiliser, $G_\omega = 1$. The action is said to be semi-regular if each point stabiliser is trivial.*

Notice that a regular or semi-regular action is also a faithful action. Notice also that a group G can only act regularly on a set Ω if $|G| = |\Omega|$. Regular and semi-regular actions will prove particularly interesting to us in the next chapter where it will be shown how to manipulate regular and semi-regular groups.

Definition 2.16. *Let G be a group acting on a set Ω. A non-empty set $\Delta \subseteq \Omega$ is a block of imprimitivity on the action of G on Ω if for every $g \in G$ either*

$$\Delta \cdot g = \Delta \text{ or } \Delta \cdot g \cap \Delta = \emptyset$$

where $\Delta \cdot g = \{\delta \cdot g \mid \delta \in \Delta\}$.

Trivial examples are when $\Delta = \Omega$ or when Δ is a singleton subset. In Chapter 4 we will see a non-trivial example. Blocks of imprimitivity provide a partition of the set since if Δ is a block then so is each Δ^g.

Lemma 2.17. *Let $S = \mathrm{Sym}(\Omega)$. Suppose $G \leq S$ is abelian and transitive on Ω. Then G is regular and $C_S(G) = G$.*

Proof. The kernel of the action is trivial since $G \leq S$ and only the identity permutation fixes everything in Ω. For $\omega \in \Omega$ let $g \in G - G_\omega$ and $h \in G_\omega$. Then $\omega^g = \omega^{hg} = (\omega^g)^h$ as G is abelian.

Since G is transitive on Ω then h fixes every $\omega \in \Omega$ so h is in the kernel of the action and so must be the identity. It follows that $G_\omega = 1$ for every $\omega \in \Omega$ and so the action is regular.

Since G is abelian, $G \leq C_S(G) =: C$. Let $c \in C$. Since G is transitive, $\omega \cdot c = \omega \cdot g$ for some $g \in G$. But then $gc^{-1} \in C_\omega$. Let $\theta \in \Omega$. Then $\theta = \omega \cdot h$ for some $h \in G$ as G is transitive. This gives us that

$$\theta \cdot (gc^{-1}) = \omega \cdot (hgc^{-1}) = \omega \cdot (gc^{-1}h) = \omega \cdot h = \theta$$

(since gc^{-1} commutes with G). However θ was arbitrary so gc^{-1} fixes every point in Ω and so $c = g \in G$ and $C_S(G) = G$.

□

Note that unless the meaning is unclear then we will often write ωg instead of $\omega \cdot g$ for an element g acting on some point ω.

Lemma 2.18. *Let $G \leq S$ (where $S = \mathrm{Sym}(\Omega)$ as before). Then $N_S(G)/C_S(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.*

Proof. Define

$$\begin{array}{rcccl} \phi & : & N_S(G) & \longrightarrow & \mathrm{Aut}(G) \\ & & x & \longmapsto & C_x \end{array}$$

where C_x defines conjugation by x. ($C_x : g \mapsto g^x$, $g \in G$).

This defines a homomorphism as C_{xy} is equal to $C_x C_y$. The kernel of this homomorphism is $C_S(G)$. The result follows by an isomorphism theorem.

□

Suppose a group G acts on a set Ω. Define

$$\mathrm{Fix}_\Omega(G) = \{\omega \in \Omega \mid \omega^g = \omega \ \forall g \in G\}.$$

Lemma 2.19. *Let p be a prime and G be a p-group acting on a finite set Ω. Then*

$$|\mathrm{Fix}_\Omega(G)| \equiv |\Omega| \bmod p.$$

Proof. Let $\Omega_1, \ldots, \Omega_n$ be the orbits of the action of G on Ω. Each orbit must have length a power of p. The size of $\mathrm{Fix}_\Omega(G)$ is the number of orbits of length one. Suppose m orbits have length one then $|\Omega| = \sum_{i=1}^{n} |\Omega_i| \equiv m \bmod p$ which gives the result.

□

Lemma 2.20. *Let G be a finite group acting transitively on a set Ω, let $H = G_\omega$ for some $\omega \in \Omega$ and $K \leq H$ with the property that $K^G \cap H = K^H$. Then $N_G(K)$ is transitive on $\mathrm{Fix}_\Omega(K)$.*

(Note that $K^H = \{K^h \mid h \in H\}$ is a set of conjugates of K.)

Proof. Let $\mu \in \mathrm{Fix}(K)$. Since G is transitive, $\mu = \omega^g$ for some $g \in G$. For any $k \in K$, $\omega^g = \mu = \mu^k = \omega^{gk}$, so $k^{g^{-1}} \in H$. It follows that $K^{g^{-1}} \in K^G \cap H = K^H$ and so $K^{g^{-1}} = K^h$ for some $h \in H$ and then $g^{-1}h^{-1} \in N_G(K)$. Given that $\mu = \omega^g$ we get that $\mu^{g^{-1}h^{-1}} = \omega^{h^{-1}} = \omega$. So $N_G(K)$ is transitive on $\mathrm{Fix}(K)$.

□

Lemma 2.21 (Frattini Argument)**.** *Let K be a finite normal subgroup of a group G and P a Sylow p-subgroup of K (for some prime p) then $G = N_G(P)K$.*

Proof. For $g \in G$, since $K \trianglelefteq G$, $P^g \leq K^g = K$ and so $P^g \in \mathrm{Syl}_p(K)$. Since the Sylow p-subgroups of K are conjugate in K then there exists $k \in K$ such that $P^g = P^k$ and then $P^{gk^{-1}} = P$. Hence $gk^{-1} \in N_G(P)$ and so $g \in N_G(P)K$. Thus $G = N_G(P)K$.

□

An action of a transitive group G on a set Ω is said to be 2-transitive if for any two pairs of distinct elements $\alpha \neq \beta \in \Omega$ and $\gamma \neq \delta \in \Omega$ there exists $g \in G$ such that

$$(\alpha, \beta) \cdot g := (\alpha \cdot g, \beta \cdot g) = (\gamma, \delta).$$

Lemma 2.22. *A group G is 2-transitive on a set Ω if and only if for $\omega \in \Omega$, G_ω is transitive on $\Omega - \{\omega\}$.*

Proof. Let $\gamma, \delta \in \Omega - \{\alpha\}$. Suppose that G is 2-transitive on Ω. Then there exists $g \in G$ such that $(\gamma \cdot g, \omega \cdot g) = (\gamma, \omega) \cdot g = (\delta, \omega)$. Clearly $g \in G_\omega$.

Conversely let $\alpha \neq \beta \in \Omega$ and $\gamma \neq \delta \in \Omega$. Since G is transitive there exists $g \in G$ such that $\alpha \cdot g = \gamma$. Set $\epsilon = \beta \cdot g$. Since $\beta \neq \alpha$ then $\epsilon \neq \alpha \cdot g = \gamma$. Assuming G_γ is transitive on $\Omega - \{\gamma\}$ then there exists $h \in G_\gamma$ such that $\epsilon \cdot h = \delta$. Hence

$$(\alpha, \beta) \cdot gh = (\alpha \cdot gh, \beta \cdot gh) = (\gamma \cdot h, \epsilon \cdot h) = (\gamma, \delta)$$

and so G is 2-transitive.

□

Lemma 2.23. *Suppose $H \lneq G$ where G is a p-group for some prime p. Then $H \lneq N_G(H)$.*

Proof. Let Ω be the set of right cosets of H in G. Since G acts on this group by right multiplication then so does H. Each orbit has length a power of p. The number of orbits of this action of length one must also be a multiple of p as Ω is a union of its orbits. There is at least one orbit of length one namely the trivial coset H. Clearly there must be another and so there exists $g \in G - H$ with $Hg \cdot h = Hg$ for each $h \in H$. However then $H^g = H$ and $g \in N_G(H) \neq H$.

□

An automorphism of a group G is said to be fixed-point free if it leaves only the identity of G fixed.

Lemma 2.24. *Let ϕ be a fixed-point free automorphism of order two of a finite group G. Then ϕ inverts every element of G and G is abelian.*

Proof. Define

$$\begin{array}{rcccc} \theta & : & G & \longrightarrow & G \\ & & g & \longmapsto & g^{-1}(g\phi). \end{array}$$

Then θ is injective since $x^{-1}x\phi = y^{-1}y\phi$ if and only if $yx^{-1} = y\phi(x\phi)^{-1} = (yx^{-1})\phi$ if and only if $yx^{-1} = 1$ (as the automorphism is fixed-point free) if and only if $x = y$. Also θ is onto since G is finite. So for each $g \in G$ there is some $h \in G$ such that $g = h^{-1}(h\phi)$ therefore $g\phi = (h^{-1})\phi h = g^{-1}$ (as ϕ has order two). So ϕ inverts every element of G. Now let $x, y \in G$ then

$$x^{-1}y^{-1} = (x\phi)(y\phi) = (xy)\phi = (xy)^{-1} = y^{-1}x^{-1}$$

and so $xy = yx$ and G is abelian.

□

2.3 Some Further Results

The following lemma by Bender considers the distribution of involutions in cosets and will provide an essential tool in Chapter 5. It is necessary to introduce some simple notation first.

Let $\mathcal{J}$ be the set of involutions in a finite group G and for any $S \subseteq G$, let $n(S) = |\mathcal{J} \cap S|$ be the number of involutions in S.

Now given $M \leq G$ define

$$f = f(G, M) = \frac{n(G)}{|G : M|} - 1.$$

Notice that $f > 0$ if and only if $n(G) > |G : M|$.

For a subgroup M of G and an integer m define b_m to be the number of non-trivial cosets from G/M with exactly m involutions

$$b_m = b_m(G, M) = |\{C \in G/M - \{M\} \mid n(C) = m\}|.$$

Lemma 2.25. *[3] **(Bender)** For $M \leq G$ with $n(G) > |G : M|$, then*

$$b_1 = \frac{1}{f}(n(M) + \sum_{i>1}(i-1)b_i - 1 - b_0) - 1 - b_0 - \sum_{i>1} b_i.$$

Proof. It is clear that

- (1) $|G : M| = 1 + \sum_{i \geq 0} b_i$,
- (2) $|\mathcal{J}| = |\mathcal{J} \cap M| + \sum_{i \geq 1} i b_i$.

Rearranging (1) gives

$$b_1 = |G : M| - 1 - b_0 - \sum_{i \geq 2} b_i.$$

Rearranging the expression for f gives

$$|G : M| = \frac{1}{f}(|\mathcal{J}| - |G : M|).$$

Substituting this into the expression for b_1 gives

$$b_1 = \frac{1}{f}(|\mathcal{J}| - |G : M|) - 1 - b_0 - \sum_{i \geq 2} b_i.$$

Finally, including the expressions (1) and (2) gives

$$\begin{aligned} b_1 &= \tfrac{1}{f}(|\mathcal{J} \cap M| + \textstyle\sum_{i \geq 1} i b_i - 1 + \sum_{i \geq 0} b_i) - 1 - b_0 - \sum_{i \geq 2} b_i \\ &= \tfrac{1}{f}(n(M) - 1 - b_0 + b_2 + 2b_3 + 3b_4 + \ldots) - 1 - b_0 - \textstyle\sum_{i \geq 2} b_i. \end{aligned}$$

□

We state, without proof, the Baer-Suzuki Theorem (see Theorem 8.2 in [9]).

Theorem 1 (Baer-Suzuki). *Suppose $x \in G$ is an element of prime power order for some prime p. If $\langle x, x^g \rangle$ is a p-group for every $g \in G$ then $x \in O_p(G)$.*

We require also some knowledge of *Frobenius* and *Zassenhaus* groups.

Definition 2.26. *Let G be a group acting transitively on a set X such that no element of $G^{\#}$ fixes more than one point of X and at least one element of $G^{\#}$ fixes one point of X. Then G is a Frobenius group.*

A Frobenius group G has Frobenius complement $H = G_x$ for some $x \in X$ and Frobenius kernel $K = G \backslash \bigcup_{g \in G} \{H^g \backslash \{1\}\}$ as described in [1, p190-1] .

Definition 2.27. *Let G be a group acting 2-transitively on a set X such that only the identity fixes three elements of X but the subgroup fixing two points is non-trivial. Then G is a Zassenhaus group.*

For $x \in X$, since G is 2-transitive and only the identity fixes three points then $N := G_x$ is transitive on $X \backslash \{x\}$ (by Lemma 2.22) and only the identity fixes two points. Also the subgroup fixing two points is non-trivial and so at least one element of $N^{\#}$ fixes a point. Therefore N is a Frobenius group. Let H and K be the Frobenius complement and kernel respectively then G is said to be of type (H, K) and degree n where n is the size of the set X.

Finally we also state without proof, Theorem 3.5 from [9] which we will require in Chapter 5.

Theorem 2 (Zassenhaus). *Let G be a Zassenhaus group of type (H,K) and degree $m+1$ where m is odd. Suppose H is cyclic, inverted by an involution of G and $|H| = \frac{m-1}{2}$. Then $G \cong \mathrm{PSL}_2(m)$.*

3. SOME REPRESENTATION THEORY

Representation theory gives us a way of formalising group actions and understanding how group actions can give an embedding of a group into a more familiar linear or symmetric group. In particular we will see how the theory can be used when a group is seen to act on an elementary abelian group or on the cosets of a particular subgroup.

3.1 Representations and Modules

Definition 3.1. *A linear representation of a group G on a vector space V over a field F is a homomorphism*

$$\varphi : G \to \mathrm{GL}(V).$$

The degree of φ is the dimension of V over F.
A permutation representation of G on a set Ω is a homomorphism

$$\varphi : G \to \mathrm{Sym}(\Omega).$$

The degree of φ is $|\Omega|$.

The kernel of a representation is $\mathrm{Ker}(\varphi) = \{g \in G \mid g\varphi = 1\}$ where depending on the representation 1 may be the identity matrix or the identity permutation. A representation is faithful if its kernel is trivial.
Recall that a group action defines a permutation representation of the group and if this group action is faithful then the permutation representation is injective.

Example 3.2. Let G be a finite group and $H \leq G$ with $|G : H| = n$. Then G acts on the right cosets of H in G by right multiplication. The kernel of this action is called the *core of H in G*.

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} H^g.$$

If this kernel is trivial then the action is faithful and the permutation representation gives an embedding of G into $\mathrm{Sym}(n)$.

Two permutation representations $\phi, \psi : G \to \mathrm{Sym}(\Omega)$ are said to be *equivalent* if for each $g \in G$ there exists $\sigma \in \mathrm{Sym}(\Omega)$ such that

$$(g\phi)^{\sigma} = g\psi.$$

Similarly two linear representations $\phi, \psi : G \to \mathrm{GL}(V)$ are equivalent if for each $g \in G$ there exists some $A \in GL(V)$ such that

$$(g\phi)^{A} = g\psi.$$

Definition 3.3. *A vector space V over a field F is an FG-module if there is a group G and a multiplication $v \cdot g$ defined by G on V satisfying*

- $v \cdot g \in V$;
- $v \cdot (gh) = (v \cdot g) \cdot h$;
- $v \cdot 1 = v$;
- $(\lambda v) \cdot g = \lambda(v \cdot g)$;
- $(u + v) \cdot g = u \cdot g + v \cdot g$;

for all $u, v \in V,\ g, h \in G,\ \lambda \in F$.

Notice that the product of the zero vector with any element of the groups must be the zero vector since $0 \cdot g = (0 + 0) \cdot g = 0 \cdot g + 0 \cdot g$.

An FG-module is faithful if $vg = v$ for all $v \in V$ if and only if g is the identity of G.

Notice that if $\varphi : G \to \mathrm{GL}(V)$ is a representation, then the vector space V becomes an FG-module when we define

$$v \cdot g := v(g\varphi).$$

Notice also that if V is an FG-module and we define

$$\begin{array}{rcccl} \phi_g & : & V & \longrightarrow & V \\ & & v & \longmapsto & v \cdot g \end{array}$$

then ϕ_g is a linear transform of V. Moreover

$$\begin{array}{rcccl} \phi & : & G & \longrightarrow & \mathrm{GL}(V) \\ & & g & \longmapsto & \phi_g \end{array}$$

is a representation. We see that these two ideas are interchangeable.

An important application is when a group acts on an elementary abelian group. This is because an elementary abelian group, A say, can be regarded as a vector space over the field $\mathrm{GF}(p)$. We see this by defining a vector space V to be the elements of A with vector addition defined to be the group multiplication

$$u + v := uv \quad \forall\ u, v \in V$$

and scaler multiplication defined as

$$\lambda v := v^{\lambda} \quad \forall\ \lambda \in \mathrm{GF}(p),\ \forall\ v \in V.$$

This definition is well defined in the finite field $\mathrm{GF}(p)$ since each non-identity element of A has order p so $v^n = v^{n+zp}$ for any integer z. With these definitions it is easy to check that V is a vector space. Also any automorphism of A acts linearly on the vectors and similarly any linear transform gives an automorphism of A and so Aut(M) $\cong$ GL(V). Recall Example 2.7 where $M = C_2 \times C_2$ is elementary abelian and so can be viewed as a vector space of dimension two over a field of characteristic two. This demonstrates that $\mathrm{Sym}(3) \cong \mathrm{Aut}(C_2 \times C_2) \cong \mathrm{GL}_2(2) \cong \mathrm{SL}_2(2)$. Notice that with this definition subgroups of A are exactly vector subspaces and vice versa.

From now on unless it seems ambiguous we will write ωg for $\omega \cdot g$.

Definition 3.4. *If V is an FG-module and W a subspace of V then W is an FG-submodule if and only if $wg \in W$ for each $w \in W$ and $g \in G$.*
An FG-module V is irreducible if it is non-zero and has no FG-submodules except $\{0\}$ and V.

Definition 3.5. *Given FG-modules V and W then $\phi : V \to W$ is an FG-homomorphism if ϕ is a linear transform and*

$$(vg)\phi = (v\phi)g \quad \forall\ v \in V \ \mathit{and}\ \forall\ g \in G.$$

(We say ϕ commutes with G.)

The set of all FG-homomorphisms from V to W is the set $\mathrm{Hom}_{FG}(V, W)$*.*

Lemma 3.6 (Schur's Lemma)**.** *If V is an irreducible FG-module then* $\mathrm{Hom}_{FG}(V, V)$ *is a division ring.*

Proof. Let $0 \neq \phi \in \mathrm{Hom}_{FG}(V, V)$. Set $W = V\phi$. Since ϕ is non-zero, so is W. Hence for all $v \in V$ and $g \in G$

$$(v\phi)g = (vg)\phi \in W$$

and so W is an FG-submodule. Since V is irreducible and $W \neq \{0\}$ then $V = W$. So ϕ is onto and by the rank-nullity result ϕ is a non-singular linear transform on V and thus invertible. Clearly ϕ^{-1} is a linear transform and $vg = (v\phi^{-1})\phi g = (v\phi^{-1})g\phi$ ($v\phi^{-1} \in V$ as ϕ^{-1} is bijective) and so $(v\phi^{-1})g = (vg)\phi^{-1}$ and $\phi^{-1} \in \mathrm{Hom}_{FG}(V, V)$. A quick check verifies $\mathrm{Hom}_{FG}(V, V)$ is a ring with usual addition and composition of functions and so it is a division ring.

□

It is a fact from ring theory that a finite division ring is a field (see [5, p101, 8.6]). So if F is a finite field and V finite dimensional then $\mathrm{Hom}_{FG}(V, V)$ is finite and hence a field. It is also a well known fact that the multiplicative group of a finite field (and hence any subgroup also) is cyclic (see [12, p18 2.21]).

Lemma 3.7. *If V is a faithful FG-module where G is an abelian group and F is a finite field, then G is cyclic.*

Proof. Define

$$\begin{array}{rcccl} \phi & : & G & \longrightarrow & \mathrm{Hom}_{FG}(V, V)^{\times} \\ & & g & \longmapsto & \phi_g \end{array}$$

($^{\times}$ indicates the multiplicative group.)

where $v\phi_g = vg$ for each $v \in V$. Each ϕ_g is a linear transform from V to V since $(v + \lambda w)\phi_g = (v + \lambda w)g = vg + \lambda wg = (v\phi_g) + \lambda(w\phi_g)$ and ϕ_g is an FG-homomorphism since G is abelian so for any h in G, $(vh)\phi_g = vhg = vgh = (v\phi_g)h$. Since V is faithful, ϕ is an injective mapping into $\mathrm{Hom}_{FG}(V, V)$.

Also ϕ is a homomorphism since

$$v\phi_g\phi_h = (vg)\phi_h = vgh = v\phi_{gh}$$

so

$$(gh)\phi = \phi_{gh} = \phi_h\phi_h = (g\phi)(h\phi)$$

and so G is isomorphic to a subgroup of the multiplicative group $\mathrm{Hom}_{FG}(V,V)^\times$ which is necessarily cyclic.

□

A representation $\phi : G \longrightarrow \mathrm{Sym}(\Omega)$ is said to be semi-regular if for each $\omega \in \Omega$, $\omega g\phi = \omega$ if and only if $g = 1$. It is said to be regular if we have further that $G\phi$ transitive on Ω. Notice that a semi-regular representation is faithful.

Lemma 3.8. *Suppose*

$$\begin{array}{rcccl} \phi & : & G & \longrightarrow & \mathrm{Sym}(\Omega) \\ \psi & : & G & \longrightarrow & \mathrm{Sym}(\Omega) \end{array}$$

are regular permutation representations of G. Then ϕ and ψ are equivalent representations.

Proof. G is transitive so for a fixed $\omega \in \Omega$ we can write

$$\Omega = \{\omega \cdot (g\phi) \mid g \in G\} = \{\omega \cdot (g\psi) \mid g \in G\}.$$

Define

$$\begin{array}{rcccl} \sigma & : & \Omega & \longrightarrow & \Omega \\ & & \omega \cdot g\phi & \longmapsto & \omega \cdot g\psi. \end{array}$$

Then for $g_1, g_2 \in G$

$$\begin{array}{rrcl} & \omega \cdot g_1\phi\sigma & = & \omega \cdot g_2\phi\sigma \\ \Rightarrow & \omega \cdot g_1\psi & = & \omega \cdot g_2\psi \end{array}$$

and so,

$$\omega = \omega \cdot (g_1\psi)(g_2\psi)^{-1} = \omega \cdot (g_1{g_2}^{-1}\psi).$$

Since ψ is a regular action then $g_1 = g_2$.

So σ is one-to-one and since Ω is finite, it is onto also. So $\sigma \in \mathrm{Sym}(\Omega)$.

Let $\mu \in \Omega$ and $h \in G$. Then $\mu = \omega \cdot g\psi$ for some $g \in G$.

$$\begin{aligned}
\mu \cdot (g_1\phi)^\sigma &= \omega \cdot (g\psi)\sigma^{-1}(g_1\phi)\sigma \\
&= \omega \cdot (g\phi)(g_1\phi)\sigma \\
&= \omega \cdot (gg_1)\phi\sigma \\
&= \omega \cdot (gg_1)\psi \\
&= \omega \cdot (g\psi)(g_1\psi) \\
&= \mu \cdot g_1\psi.
\end{aligned}$$

So $(g_1\phi)^\sigma = g_1\psi$ for all $g_1 \in G$ and the representations are equivalent.

□

Corollary 3.9. *If G and H are isomorphic groups and*

$$\begin{aligned}
\phi_1 &: G \longrightarrow \mathrm{Sym}(\Omega) \\
\phi_2 &: H \longrightarrow \mathrm{Sym}(\Omega)
\end{aligned}$$

are regular permutation representations then the representations of G and H are conjugate in $\mathrm{Sym}(\Omega)$.

Proof. Let θ be an isomorphism between G and H. Then ϕ_1 and $\theta\phi_2$ are representations of G and so for some $\sigma \in \mathrm{Sym}(\Omega)$, $(G\phi_1)^\sigma = (G\theta)\phi_2 = H\phi_2$.

□

Corollary 3.10. *If $G \leq \mathrm{Sym}(\Omega)$ is regular on Ω then* $\mathrm{Aut}(G) \cong N_{\mathrm{Sym}(\Omega)}(G)/C_{\mathrm{Sym}(\Omega)}(G)$.

Proof. By Lemma 2.18 since $G \leq \mathrm{Sym}(\Omega)$, $N_{\mathrm{Sym}(\Omega)}(G)/C_{\mathrm{Sym}(\Omega)}(G)$ is isomorphic to a subgroup of the full automorphism group of G. Let $\alpha \in \mathrm{Aut}(G)$. Then there eixsts $\sigma \in \mathrm{Sym}(\Omega)$ such that for any $g \in G$ we get that $g^\sigma = g\alpha \in G$. So σ normalises G. Now α is an automorphism of G so the automorphism α is equivalent to conjugating by an element of the normaliser of G in $\mathrm{Sym}(\Omega)$. The result follows.

□

3.2 An Application

Suppose that V is an n-dimensional vector space over a finite field $F = \mathrm{GF}(p)$ (p a prime) and an irreducible and faithful FG-module where G is an abelian group.

Notice that F can be considered as a set of linear transformations of V by defining

$$\theta_\lambda : v \mapsto \lambda v$$

for each $\lambda \in F$. Moreover this is a set of FG-homomorphisms since from the definition of an FG-module

$$(v\theta_\lambda)g = (\lambda v)g = \lambda(vg) = (vg)\theta_\lambda$$

for each $v \in V$, $g \in G$ and $\lambda \in F$. Define a mapping

$$\begin{array}{cccc} \phi_F & : & F & \longrightarrow & \mathrm{Hom}_{FG}(V,V) \\ & & \lambda & \longmapsto & \theta_\lambda \end{array}$$

We have seen already that G can also be considered as a set of linear transforms and since G is abelian then G can be considered as a set of FG-homomorphisms by defining

$$\begin{array}{cccc} \phi_G & : & G & \longrightarrow & \mathrm{Hom}_{FG}(V,V) \\ & & g & \longmapsto & \varphi_g \end{array}$$

($\varphi_g : v \mapsto vg$).

So consider $C := \langle F\phi_F, G\phi_G \rangle$ the subring of $\mathrm{Hom}_{FG}(V,V)$ generated by the images of F and G. Since V is irreducible and finite dimensional over a finite field then by Schur's Lemma $\mathrm{Hom}_{FG}(V,V)$ is a finite field. Notice $\varphi_{g^{-1}} = (\varphi_g)^{-1} \in C$ and $\theta_{\lambda^{-1}} = (\theta_\lambda)^{-1} \in C$. So C is closed under taking inverses and hence must be a subfield.

Define, for a fixed non-zero vector v,

$$\begin{array}{cccc} \phi & : & C & \longrightarrow & V \\ & & c & \longmapsto & vc. \end{array}$$

The representations of G and F as linear transformations gives us a way of multiplying elements of G and F. Since $C = \langle F\phi_F, G\phi_G \rangle$ is generated by such products then C can be considered as an FG-module by defining multiplication in this way. Hence ϕ is an FG-homomorphism from C to V.

The kernel of this FG-homomorphism is $\ker\phi = \{c \in C \mid vc = 0\}$. This is an ideal of the field C. (It is non-empty since the zero in C is in $\ker\phi$, and C is a field and so commutative therefore for any $k \in \ker\phi$ and any $c \in C$, $vck = vkc = 0c = 0$ so $ck, kc \in \ker\phi$.) It is a fact from basic field theory that any field has only two ideals (see [7, p335, 6.2.6]), $\{0\}$ and the field itself. However the kernel cannot be the whole of C since C contains a 'one' (namely the identity transformation) and $v1_C = v \neq 0$ and so the kernel must be trivial.

This forces $C \cong V$ so $|C| = |V| = p^n$. We have that C is a finite field so $C \cong \mathrm{GF}(p^n)$ by the uniqueness of fields of prime power order (see [8, p75]). Notice that for a non-zero $v \in V$, vC is a non-zero FG-submodule of V and so $V = vC$.

Suppose H is another abelian group and V is an irreducible, faithful FH-module. Let $D = \langle F\phi_F, H\phi_H\rangle$ as before ($\phi_H : H \to \mathrm{Hom}_{FH}(V, V)$ as expected). Then $D \cong \mathrm{GF}(p^n) \cong C$. Let θ be a ring isomorphism between C and D. Notice $F\phi_F \subseteq C \cap D$. So we assume that θ acts as the identity on this intersection. Define

$$\begin{array}{rccl} \hat{\theta} & : & V = vC & \longrightarrow & V = vD \\ & & vc & \longmapsto & v(c\theta). \end{array}$$

For $vc_1, vc_2 \in vC$, $vc_1 + vc_2 = v(c_1 + c_2)$ and so

$$(v(c_1 + c_2))\hat{\theta} = v((c_1 + c_2)\theta) = v(c_1\theta + c_2\theta) = (vc_1)\hat{\theta} + (vc_2)\hat{\theta}.$$

Similarly for $vc \in vC$ and $\lambda \in F$, $\lambda vc = v(\theta_\lambda c)$ where $\theta_\lambda c \in C$. Thus

$$(\lambda vc)\hat{\theta} = (v\theta_\lambda c)\hat{\theta} = v(\theta_\lambda\theta)(c\theta) = v\theta_\lambda(c\theta) = \lambda v(c\theta) = \lambda(vc)\hat{\theta}.$$

Hence $\hat{\theta}$ is linear.

Suppose $(vc)\hat{\theta} = v(c\theta) = 0$. Since $vD = v(C)\theta = V$ then $v(c\theta) = 0$ only when $c\theta = 0$. However θ is an isomorphism so $c\theta = 0$ only when $c = 0$. So $\hat{\theta}$ is injective and thus surjective by the rank-nullity result. Hence $\hat{\theta}$ is an invertible linear transform of V and thus $\hat{\theta} \in \mathrm{GL}(V)$.

Moreover we see that $\hat{\theta}$ conjugates C to D. For any $d \in D$, $d = c\theta$ for some $c \in C$. Let w be any element of V then $w = vc_1$ for some $c_1 \in C$ and so

$$w(\hat{\theta}d\hat{\theta}^{-1}) = vc_1(\hat{\theta}(c\theta)\hat{\theta}^{-1}) = v(c_1\theta)(c\theta)\hat{\theta}^{-1} = v(c_1c)\theta\hat{\theta}^{-1} = vc_1c = wc.$$

So for each $d \in D$, $c^{\hat{\theta}} = d = c\theta$.

So if G and H act regularly on $V\backslash\{0\}$ then $|G| = |H| = |V| - 1 = p^s - 1$ so $G = C^\times$ and $H = D^\times$ and so $H = G^{\hat{\theta}}$. This gives the following result.

Lemma 3.11. *Suppose G and H are abelian groups and V is a finite dimensional vector space over a finite field F of prime power order. Suppose further that V is an irreducible and faithful FG and FH-module and that via this multiplication both G and H are seen to act regularly on the non-zero vectors of V then the representations of G and H are conjugate in* $\mathrm{GL}(V)$*.*

Proof. Since G and H act regularly on $V - \{0\}$ then $|G| = |H| = |V| - 1 = p^s - 1$. Since ϕ_G and ϕ_H as described are injective (V is a faithful module) then it must be that $G\phi_G = C^\times$ and $H\phi_H = D^\times$. It follows that $H\phi_H = (G\phi_G)^{\hat{\theta}}$ for $\hat{\theta} \in \mathrm{GL}(V)$ and so the representations are conjugate.

□

We actually have a stronger result than this. G and H are more than just conjugate, they are equivalent. Two groups acting on a set Ω are said to be equivalent if there is an isomorphisms which maps elements of one group to the other in such a way that element-wise they act in the same way on the set. More formally, if the groups are G_1 and G_2 say, then $\alpha : G_1 \to G_2$ is an isomorphism such that for every $\omega \in \Omega$ and every $g_1 \in G_1$,

$$\omega \cdot g_1 = \omega \cdot (g_1\alpha).$$

So, returning to our groups from the lemma, for each $g \in G$ there is some unique element $h \in H$ such that $(g\phi_G)^{\hat{\theta}} = h\phi_H$. In Chapter 5 we will require this result but only in its weaker stated form. Although understanding that there is equivalence is not necessary it helps to see this equivalence in Chapter 5 when we prove two groups which are acting in the same way are isomorphic.

4. IDENTIFYING GROUPS BY CONSTRUCTING AMALGAMS AND THE COSET GRAPH

4.1 Amalgams and Completions

This chapter introduces the concept of an amalgam and of completions of amalgams. From this we look at the construction of a coset graph and see how a group acts on a coset graph. We use this to identify a periodic group with certain properties.

An amalgam $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ is a quintuple consisting of three groups A, B and C and two injective (but not usually surjective) homomorphisms $\phi_1 : C \to A$ and $\phi_2 : C \to B$.
A completion (G, ψ_1, ψ_2) of an amalgam $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ is a group G such that $\psi_1 : A \to G$ and $\psi_2 : B \to G$ are homomorphisms with $G = \langle A\psi_1, B\psi_2\rangle$ and such that

$$\phi_1\psi_1 = \phi_2\psi_2.$$

That is that the following diagram commutes:

$$\begin{tikzcd}
 & A \arrow[dr, "\psi_1"] & \\
C \arrow[ur, "\phi_1"] \arrow[dr, "\phi_2"'] & & G \\
 & B \arrow[ur, "\psi_2"'] &
\end{tikzcd}$$

A completion is faithful if ψ_1 and ψ_2 are injective.

It is clear that a trivial completion can always be constructed where ψ_1 and ψ_2 map A and B simply to the identity, however the existence of a faithful completion is not so obvious. In the proof of the following theorem we find a *transversal* of a subgroup inside a group. This is a set of coset representatives. When either the index of the subgroup is not finite (so the transversal will have infinite size) or when the size of the subgroup is not finite (so there is an infinite number of choices of coset representatives) it is not clear that finding a transversal makes sense. It turns out that in both cases is does make sense to find a transversal as in a similar proof of the Normal-Form theorem by Serre in [13, p3, Thm 1].

Lemma 4.1. *Given an amalgam $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ there exists a faithful completion. In particular if A and B are finite then there exists a finite faithful completion.*

Proof. Let $\mathcal{S}$ be a left transversal of $C\phi_1$ in A and $\mathcal{T}$ a left transversal of $C\phi_2$ in B. Any $a \in A$ can be written uniquely as $sc\phi_1$ for some $s \in \mathcal{S}$ and some $c \in C$, and similarly any $b \in B$ as $tc\phi_2$ for some $t \in \mathcal{T}$ and $c \in C$. Define

$$\Omega := A \times \mathcal{T} = \{(a,t) \mid a \in A, t \in \mathcal{T}\}$$

and

$$\Omega' := \mathcal{S} \times B = \{(s,b) \mid s \in \mathcal{S}, b \in B\}.$$

Then A acts on Ω via

$$(a,t) \bullet a_1 := (aa_1, t)$$

and B acts on Ω' via

$$(s,b) \circ b_1 := (s, bb_1).$$

(Where $\bullet$ and $\circ$ are intended to represent *different* group actions.)
Define $\Theta : \Omega \to \Omega'$ by $(sc\phi_1, t)\Theta = (s, tc\phi_2)$. Indeed, let (s,b) be any element of Ω'. Then there exists $t \in \mathcal{T}$ and $c \in C$ such that $b = tc\phi_2$ and so $(s,b) = (s, tc\phi_2)$. Now, $sc\phi_1 \in A$, so $(sc\phi_1, t) \in \Omega$ and so $\Theta : (sc\phi_1, t) \mapsto (s, tc\phi_2) = (s,b)$. Hence Θ is onto.

So suppose $(a,t)\Theta = (a',t')\Theta$. Then there exist $c, c' \in C$ and $s, s' \in \mathcal{S}$ such that

$$(a,t) = (sc\phi_1, t)$$

and

$$(a',t') = (s'c'\phi_1, t').$$

Now,

$$(sc\phi_1, t)\Theta = (s'c'\phi_1, t')\Theta \iff (s, tc\phi_2) = (s', t'c'\phi_2) \iff s = s' \text{ and } tc\phi_2 = t'c'\phi_2.$$

And since any $b \in B$ is written uniquely as $tc\phi_2$ then we must have $t = t'$ and $c\phi_2 = c'\phi_2$ and so $c = c'$ as ϕ_2 is injective and then we have $c\phi_1 = c'\phi_1$. Hence

$$(a, t) = (sc\phi_1, t) = (s'c'\phi_1, t') = (a', t')$$

and so Θ is injective and hence a bijection.

With this bijection we can define an action of B on Ω:

$$(a, t) * b = (((a, t)\Theta) \circ b)\Theta^{-1}.$$

Notice that given any $d \in C$, $d\phi_1$, as an element of A acts on Ω by

$$(sc\phi_1, t) \bullet d\phi_1 = (sc\phi_1 d\phi_1, t) = (s(cd)\phi_1, t)$$

and $d\phi_2$, as an element of B, acts on Ω by

$$\begin{aligned}(sc\phi_1, t) * d\phi_2 &= (((sc\phi_1, t)\Theta) \circ d\phi_2)\Theta^{-1} \\ &= ((s, tc\phi_2) \circ d\phi_2)\Theta^{-1} \\ &= (s, tc\phi_2 d\phi_2)\Theta^{-1} \\ &= (s, t(cd)\phi_2)\Theta^{-1} \\ &= (s(cd)\phi_1, t).\end{aligned}$$

So $c\phi_1$ acts as $c\phi_2$ on Ω. Notice also that both these actions on Ω are faithful and so there exist monomorphisms

$$\Psi_1 : A \to \mathrm{Sym}(\Omega)$$

$$\Psi_2 : B \to \mathrm{Sym}(\Omega).$$

So $G := \langle \Psi_1(A), \Psi_2(B) \rangle$ is a faithful completion of $\mathcal{A}$. Moreover if A and B are finite then it is clear that G is a finite faithful completion.

□

Example 4.2. The amalgam that will be considered later in this chapter is a $(\mathrm{Sym}(4), \mathrm{Sym}(4), \mathrm{Dih}(8))$ amalgam. The lemma proves that there is a finite faithful completion of this amalgam inside of $\mathrm{Sym}(24 \times 3)$

4.2 The Coset Graph

We begin with a detailed examination of the coset graph.

Given subgroups P_1 and P_2 of G with $C \leq P_1 \cap P_2$, define the (right) coset graph of P_1 and P_2 in G to be $\Gamma = \Gamma(G, P_1, P_2, C)$ which has vertex set

$$V(\Gamma) = \{P_i g \mid g \in G, i = 1, 2\}$$

and edges between vertices which represent cosets that share a coset of C in G.

$$E(\Gamma) = \{Ck \mid k \in G\}.$$

Two vertices $P_1 g$ and $P_2 h$ are joined by the edge Ck if and only if $Ck \subseteq P_1 g \cap P_2 h$. In particular Γ is a bi-partite graph which is to say that the vertices can be written as two disjoint sets $\{P_1 g \mid g \in G\}$ and $\{P_2 g \mid g \in G\}$, with edges only between vertices from differing sets.

It is sensible at this point to make the assumption that the index of C in $P_1 \cap P_2$ is finite.

For $\alpha, \beta \in V(\Gamma)$ define $d(\alpha, \beta)$ to be the distance between α and β which is the length of the shortest path between them. If α and β are not connected by a path then $d(\alpha, \beta) = \infty$. A connected component is said to have diameter n if the distance between any two vertices is at most n.

It is important to recognise that with this definition of a coset graph it is possible that there will be multiple edges between vertices. If the index of C in $P_1 \cap P_2$ is n (assuming the index is finite) then there are exactly n cosets of C in $P_1 \cap P_2$ (say $Cx_1, Cx_2, ..., Cx_n$ where $\{x_1, ..., x_n\} \subseteq P_1 \cap P_2 - C^{\#}$ is a transversal of C in $P_1 \cap P_2$) and so for any edge $\{P_i g, P_j h\} \in E(\Gamma)$ there exists some $k \in G$ with $Ck \subseteq P_i g \cap P_j h$. Notice that $Ck \subseteq P_i g \cap P_j h$ if and only if $P_i g = P_i k$ and $P_j h = P_j k$ and so there are at least n cosets of C contained in $P_i k \cap P_j k$ (namely $Cx_1 k, Cx_2 k, ..., Cx_n k$) hence there must be at least n edges between $P_i g$ and $P_j h$. There can be no more since if $Cx \subseteq P_i g \cap P_j h = P_i k \cap P_j k = (P_i \cap P_j)k$ then $Cxk^{-1} \subseteq P_i \cap P_j$ and so $Cx = Cx_i k$ for some i.

Notice that in the case $C = P_1 \cap P_2$ there will be no multiple edges and it will make sense to talk about edges as cosets or as vertex pairs $\{P_1 g, P_2 h\}$.

The group G acts on this graph Γ by acting on the cosets by right multiplication. So for a vertex $\delta := P_ig$ let $\delta \cdot x := P_igx$ for any $x \in G$. This action of G on Γ preserves Γ as a graph since if $Ck \in E(\Gamma)$ with, say, $Ck \subseteq P_ig \cap P_jh$ (so that Ck is an edge between the vertices P_ig and P_jh) and x is any element of G then clearly $Ckx \subseteq P_igx \cap P_jhx$ so Ckx is an edge between the images of the two vertices.

G is transitive on the set of cosets of each P_i in G and so G has two orbits on $V(\Gamma)$ and G is transitive on the cosets of C and so G is transitive on edges.

Lemma 4.3. *The stabiliser in G of any vertex P_ig is conjugate to P_i. The stabiliser in G of any edge is conjugate to C.*

Proof. For any vertex $\delta = P_ig$ and $x \in G$ acting on this vertex, $\delta \cdot x = P_igx = P_ig$ if and only if $x \in g^{-1}P_ig = P_i^g$, so $\text{Stab}_G(\delta) = G_\delta = P_i^g$.
Let Ck be any edge. Then the stabiliser of this edge is the set $\{g \in G \mid Ckg = Ck\}$ and this is clearly equal to C^k.

□

For any vertex δ let $\Gamma(\delta)$ be the set of all vertices that share an edge with δ and in the case of multiple edges let $E(\gamma, \delta) := \{Ck \mid Ck \subseteq \gamma \cap \delta\}$ be the set of all edges between the vertices γ and δ.

Lemma 4.4. *For any vertex δ, G_δ is transitive on $\Gamma(\delta)$ and the sets $E(\delta, \gamma)$ form blocks of imprimitivity.*

Proof. Given vertices δ, γ that share a set of edges, then as before $\delta = P_1k$, $\gamma = P_2k$ (without loss of generality by the choice of P_1 and P_2) and $Cx_1k, \ldots, Cx_nk \subseteq \delta \cap \gamma$ and these n cosets account for the n edges between δ and γ. Now $G_\delta = P_1^k$ by Lemma 4.3 and each of $x_1, \ldots, x_n \in P_1$ so given two cosets Cx_ik, Cx_jk then $x := k^{-1}x_i^{-1}x_jk \in G_\delta$ and sends Cx_ik to Cx_jk. In fact $x \in G_{\delta\gamma} = (P_1 \cap P_2)^k$. So $G_{\delta\gamma}$ act transitively on $E(\gamma, \delta)$.

Now suppose γ, β are distinct elements of $\Gamma(\delta)$. Suppose $Ck_1 \subseteq \delta \cap \gamma$ and $Ck_2 \subseteq \delta \cap \beta$. Then $\gamma = P_2k_1$, $\beta = P_2k_2$ and $\delta = P_1k_1 = P_1k_2$. Now $P_1k_1 = P_1k_2$ so $k_2k_1^{-1} \in P_1$ therefore $x := k_1^{-1}k_2 = k_1^{-1}k_2k_1^{-1}k_1 \in P_1^k = G_\delta$ and x sends Ck_1 to Ck_2. Also the other cosets of C shared by δ and γ are of the form Cx_ik_1 with $x_i \in (P_1 \cap P_2) - C^{\#}$ and $Cx_ik_1 \cdot x = Cx_ik_2$ which is a coset of C shared by δ and β. Hence x takes γ to β.

Thus G_δ is transitive on $\Gamma(\delta)$ and transitive on each $E(\delta, \gamma)$. If for any two vertices δ, γ with $E(\delta, \gamma) \neq \emptyset$ then if $Cx_ik, Cx_jk \in E(\delta, \gamma)$ then $G_\delta = P_1^k$ so any element of G_δ has form $k^{-1}pk$ for some $p \in P_1$ and so $Cx_ik \cdot k^{-1}pk = Cx_ipk$, $Cx_jk \cdot k^{-1}pk = Cx_jpk \in E(\delta, \beta)$ for some $\beta \in \Gamma(\delta)$ and this holds for each $1 \leq i, j \leq n$ thus $E(\delta, \gamma)$ are blocks of imprimitivity.

□

Corollary 4.5. *If P_1 and P_2 are finite groups and $\delta = P_ig$ for some $g \in G$ and $i = 1$ or 2 then $|\Gamma(\delta)| = |P_i : C|$.*

Proof. For any $\gamma \in \Gamma(\delta)$ if some $g \in G_\delta$ fixes γ then $g \in G_{\delta\gamma}$ and vice versa so $G_{\delta\gamma} = \mathrm{Stab}_{G_\delta}\{\gamma\}$ which is conjugate to C. So by the orbit-stabiliser theorem $|\Gamma(\delta)| = |G_\delta : G_{\delta\gamma}| = |P_i : C|$.

□

Lemma 4.6. *$\Gamma(G, P_1, P_2, C)$ is a connected graph if and only if $G = \langle P_1, P_2 \rangle$.*

Proof. Suppose first that $G = \langle P_1, P_2 \rangle$. Let $\delta = P_1$ and $\gamma = P_2$, then $C \leq \gamma \cap \delta$ so C is an edge between them. Let Φ be the connected component of Γ containing this edge. Then each element of $G = \langle P_1, P_2 \rangle = \langle G_\delta, G_\gamma \rangle$ stabilises at least one of δ or γ. So for any vertex α that is connected via a path to δ and γ then αg must be connected to δ nd γ. Thus the whole component Φ is invariant under G. Every vertex β in Γ is of the form P_ig and so $Cg \subseteq P_ig \cap P_jg$ is an edge in Φ connecting β. Thus Γ is connected.

Suppose now that Γ is connected and that $G > H = \langle P_1, P_2 \rangle$. Let $\delta = P_1$ and choose some $\gamma = P_ig$ such that $P_ig \nsubseteq H$ and $n = d(\delta, \gamma)$ is as small as possible. Since Γ is connected then there is a path $(\delta = \delta_0, \delta_1, \delta_2, \ldots, \delta_n = \gamma)$ from δ to γ. Since n is minimal $\delta_{n-1} = P_ih$ and $\delta_{n-2} = P_jk$ for some $h, k \in H$. By Lemma 4.4 P_i^h is transitive on $\Gamma(\delta_{n-1})$ so there exists $x \in P_i^h \leq H$ such that $P_jg = P_jkx \subseteq H$. This is a contradiction and so $G = H = \langle P_1, P_2 \rangle$.

□

Lemma 4.7. *The kernel of the action of G on Γ is the largest normal subgroup of G which is contained in C.*

Proof. Let N be the largest normal subgroup of G contained in C. If K is the kernel of the action of G on Γ then every element of K fixes every vertex and edge of Γ. So in particular fixes the edge C and so $K \leq C$ and then $K \leq N$.

Conversely, N is normal in G so for every $n \in N$, $g \in G$ we have $n^{g^{-1}} \in N \leq C \leq P_1, P_2$ so $P_i gn = P_i g$ for $i = 1, 2$ and for every $P_i g \in V(\Gamma)$ and so N fixes every vertex of Γ. Moreover $Cgn = Cg$ for every edge Cg and so N fixes Γ therefore $N \leq K$ which gives equality.

□

Definition 4.8. *An amalgam $\mathcal{A} = (P_1, P_2, C, \phi_1, \phi_2)$ is simple if for every $1 \neq K \leq C$ either $K\phi_1$ is not normal in P_1 or $K\phi_2$ is not normal in P_2 or both are true.*

Notice that if $\mathcal{A}$ is not simple and G is a faithful completion of $\mathcal{A}$ then $G = \langle P_1\psi_1, P_2\psi_2 \rangle$ is not simple and if G is a faithful completion and a simple group then $\mathcal{A}$ is a simple amalgam.
Notice also that if G is a faithful completion of a non-simple amalgam then G does not act faithfully on the associated coset graph since there exists some $K \leq C$ with $K\phi_1 \trianglelefteq P_1$ and $K\phi_2 \trianglelefteq P_2$ so $K\phi_1\psi_1 = K\phi_2\psi_2 \trianglelefteq G$ and then by Lemma 4.7 G does not act faithfully on Γ.

From now on we consider coset graphs with $C = P_1 \cap P_2$. Notice then that edges can be defined in a more natural way as vertex pairs.

$$E(\Gamma) = \{\{P_1 g, P_2 h\} \mid P_1 g \cap P_2 h \neq 1.\}$$

This definition is of course equivalent to the earlier definition whenever $C = P_1 \cap P_2$ since there can be no multiple edges. We now consider an example of this.

4.3 An Example of a Coset Graph

Consider $G = \mathrm{Alt}(6)$. Recall the graph Γ^* in Chapter 1. Then let

$$A := \mathrm{Stab}_G(\{1,2\}) = \langle (12)(34), (12)(45), (12)(56) \rangle \cong \mathrm{Sym}(4).$$

Clearly $\langle (12)(34), (12)(45), (12)(56) \rangle \leq \mathrm{Stab}_G(\{1,2\})$. So consider which elements of Sym(6) fix $\{1,2\}$. Clearly any permutation from $\mathrm{Sym}(\{3,4,5,6\})$ will do as will any permutation from $\mathrm{Sym}(\{1,2\})$. This gives 48 permutations. Let $H = \mathrm{Stab}_{\mathrm{Sym}(6)}(\{1,2\})$ be this group of order 48. Since $(12) \in H$ then $H \nleq G$. So using an isomorphism theorem

$$H/(H \cap G) \cong HG/G \cong \mathrm{Sym}(6)/G \cong C_2.$$

So $\mathrm{Stab}_G(\{1,2\}) = H \cap G$ has order 24.

Now consider $\langle (12)(34), (12)(45), (12)(56) \rangle$ acting on the set $\{3,4,5,6\}$. The action is clearly faithful since the only non-identity permutation of $\{1,2,3,4,5,6\}$ that can fix $3,4,5$ and 6 is $(12) \notin \mathrm{Alt}(6)$. This faithful action gives an embedding in Sym(4). We can verify the group has size 24 by finding an element of order three and a subgroup of size eight in $\langle (12)(34), (12)(45), (12)(56) \rangle$ giving an isomorphism as required.

Let

$$B := \mathrm{Stab}_G(\{1,2\},\{3,4\},\{5,6\}) = \langle (12)(34), (13)(24), (35)(46) \rangle \cong \mathrm{Sym}(4).$$

Consider which permutations in Sym(6) stabilise $\{1,2\}$, $\{3,4\}$ and $\{5,6\}$. The transpositions (12), (34), (56) which swap the pairs account for eight elements. However we can also swap pairs with pairs, for example (13)(24) swaps the pairs $\{1,2\}$ and $\{3,4\}$, and the subgroup of elements doing this is isomorphic to Sym(3). The product of these elements gives a stabiliser, H say, in Sym(6) of size $6 \times 8 = 48$. Since $(12) \in H$ then $H \nleq G$. So using an isomorphism theorem as before,

$$H/(H \cap G) \cong HG/G \cong \mathrm{Sym}(6)/G \cong C_2.$$

So $\mathrm{Stab}_G(\{1,2\},\{3,4\},\{5,6\}) = H \cap G$ has order 24.

Now $\langle (12)(34), (13)(24), (35)(46) \rangle$ is a group of size 24 (we see this as before by finding an element of order three and a subgroup of size eight). To recognise it is isomorphic to Sym(4) it is necessary to find a subgroup of index four and show a faithful action by the group on the cosets of this subgroup.

$$K := \langle (164)(253), (35)(46) \rangle$$

is one such subgroup. The kernel of this action is the intersection of the conjugates of K. Conjugating K by (12)(34) and then again by (163)(425) gives three distinct conjugates of K

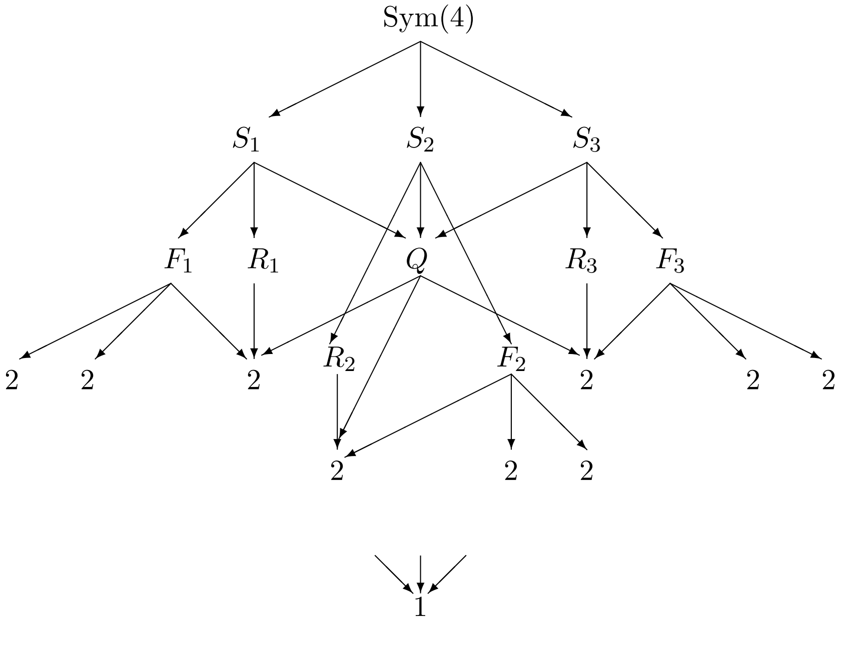
which intersect trivially. Hence the action is faithful. This gives $\langle (12)(34), (13)(24), (35)(46)\rangle$ isomorphic to Sym(4).

The groups A and B have an intersection of size eight

$$C := \langle (12)(34), (12)(3546)\rangle.$$

C is generated by an involution and an element inverted by that involution and so is dihedral by definition. Hence $A \cap B = C \cong \mathrm{Dih}(8)$.
Consider the amalgam $\mathcal{A} := (A, B, C, 1, 1)$ where 1 is the identity embedding. Then $(G, 1, 1)$ is a faithful completion. With this amalgam and completion we can form the coset graph $\Gamma = \Gamma(G, A, B, C)$. Each vertex in the coset graph has valency three since $|\mathrm{Sym}(4) : \mathrm{Dih}(8)| = 3$ and G is a faithful completion since it is generated by A and B so the graph is connected.

We first look in detail at the subgroup structure of Dih(8) and the 2-subgroups of Sym(4).



The 2-subgroups of Sym(4) consist of three Sylow 2-subgroups of size eight which are dihedral-$S_1, S_2, S_3 \cong \mathrm{Dih}(8)$. Each of these has three subgroups of size four. The first type is the cyclic four groups-$R_1, R_2, R_3 \cong C_4$, the second is the so-called *fours groups*-$F_1, F_2, F_3 \cong V_4 =$

$\langle(12)(34),(13)(24)\rangle$. Finally each of the three dihedral groups intersect at a special fours group $Q = O_2(\mathrm{Sym}(4)) \cong V_4$. The subgroups labelled 2 are simply subgroups isomorphic to C_2. Sym(4) also has a subgroup of size twelve (the alternating group) and four Sylow 3-subgroups of size three, each of which has a distinct normaliser which gives four subgroups of size six. The only normal subgroups in Sym(4) are Alt(4) and Q. It is a fact that Sym(4) can be generated by two of its non-radical fours groups.

The following diagram shows the complete subgroup structure of Dih(8).

$$\begin{tikzcd}
 & & \mathrm{Dih}(8) \arrow[dl] \arrow[d] \arrow[dr] & & \\
 & F_1 \arrow[dl] \arrow[d] \arrow[dr] & C_4 \arrow[d] & F_2 \arrow[dl] \arrow[d] \arrow[dr] & \\
2 \arrow[drr] & 2 \arrow[dr] & Z(\mathrm{Dih}(8)) \arrow[d] & 2 \arrow[dl] & 2 \arrow[dll] \\
 & & 1 & &
\end{tikzcd}$$

With this knowledge of Sym(4) and Dih(8) it is clear that the amalgam $\mathcal{A}$ is simple. Suppose not then some non-trivial subgroup of C is normal in both A and B. However both A and B have only one normal 2-subgroup which is the 2-radical subgroup. The 2-radical of A is $Q(A) := \langle(34)(56),(35)(46)\rangle$ and the 2-radical of B is $Q(B) := \langle(12)(34),(34)(56)\rangle$. Hence $\mathcal{A}$ is a simple amalgam.

Claim 1. Γ *has no four-cycle.*

Suppose $\alpha, \beta, \gamma, \delta$ is a four-cycle in Γ. Each point stabiliser is isomorphic to Sym(4) and each edge (or two point path) stabiliser is isomorphic to Dih(8). Consider the stabiliser of a path of length three. This must be the intersection of the two edge stabilisers each isomorphic to Dih(8). Consider the diagram on the next page of subgroups inside of Alt(6) and imagine that

G_δ and G_γ also intersect at $G_{\delta\gamma}$. Copies of Dih(8) inside Sym(4) intersect at the 2-radical group $O_2(\mathrm{Sym}(4))$. Notice that inside a particular Sym(4) point stabiliser there is a unique 2-radical group which is a three point stabiliser.

$\mathcal{A}$ is a simple amalgam and so each pair of point stabilisers which intersect at an edge stabiliser are conjugate to A and B. If they share the same 2-radical normal subgroup then A and B must share a normal subgroup which is not the case. Now inside of each Sym(4) are two other three point stabilisers These are non-radical fours groups inside this Sym(4) but must be 2-radicals inside of an adjacent copy of Sym(4).

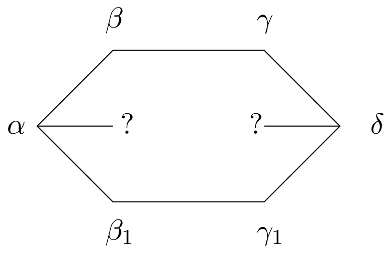
$$\begin{tikzcd}
& G_\delta \arrow[dl] \arrow[dr] & & G_\alpha \arrow[dl] \arrow[dr] & & G_\beta \arrow[dl] \arrow[dr] & & G_\gamma \arrow[dl] \arrow[dr] & \\
 & & G_{\alpha\delta} \arrow[dl] \arrow[dr] & & G_{\alpha\beta} \arrow[dl] \arrow[dr] & & G_{\beta\gamma} \arrow[dl] \arrow[dr] & & \\
& \begin{array}{c} G_{\alpha\delta\gamma} \\ = O_2(G_\delta) \end{array} & & \begin{array}{c} G_{\alpha\beta\delta} \\ = O_2(G_\alpha) \end{array} & & \begin{array}{c} G_{\alpha\beta\gamma} \\ = O_2(G_\beta) \end{array} & & &
\end{tikzcd}$$

$G_\alpha \cong \mathrm{Sym}(4)$ is generated by two of its non-radical fours groups so $G_\alpha = \langle G_{\alpha\beta\gamma}, G_{\alpha\delta\gamma}\rangle$. However repeating this argument with γ and α swapped would give $G_\gamma = \langle G_{\alpha\beta\gamma}, G_{\alpha\delta\gamma}\rangle$. So $G_\alpha = G_\gamma$.

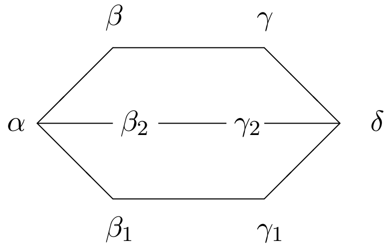
This means that $G_\alpha \supseteq G_{\gamma\beta} \in \mathrm{Syl}_2(G_\gamma)$ and we also clearly have $G_{\alpha\beta} \subseteq G_\alpha$. Then $G_\beta = \langle G_{\alpha\beta}, G_{\beta\gamma}\rangle \subseteq G_\alpha$ and so $O_2(G_\alpha) = O_2(G_\beta) \trianglelefteq G_\beta = G_\alpha$. This gives a contradiction since G is transitive on edges so without loss of generality $G_\alpha = A$ and $G_\beta = B$ but then $O_2(G_\alpha) \trianglelefteq A \cap B \cong \mathrm{Dih}(8)$ which contradicts $\mathcal{A}$ being a simple amalgam.

Claim 2. Γ *has no six-cycle.*

Suppose $\alpha, \beta, \gamma, \delta, \gamma_1, \beta_1$ is a six-cycle.



Consider the stabiliser of a path of length four. $G_{\alpha\beta\gamma\delta} = Z(G_{\beta\gamma})$ and $G_{\alpha\beta_1\gamma_1\delta} = Z(G_{\beta_1\gamma_1})$, these are four path stabilisers only and so these groups of order two must be transitive on $\Gamma(\delta) - \{\gamma\}$ and on $\Gamma(\alpha) - \{\beta\}$. This means that a non-trivial element must swap the other vertices of α and δ but it must also maintain the six cycle and so there must be another six cycle.



Rotating this diagram and arguing again with different vertices in the place of α and δ would give a graph with only fourteen vertices. So there must be either fourteen vertices else there can be no six cycle in this graph.

From this we must conclude that given any vertex α there must be three vertices at distance one, six at distance two and twelve at distance three. This leaves eight at distance four and there can be no vertices at distance five. Thus we have bounded the diameter of this graph. This is an important example since we will later be considering a coset graph which turns out to be exactly this graph and so it is necessary to keep this in mind.

4.4 Periodic Groups with Dihedral Centraliser of an Involution

In the remainder of this chapter we let G be a periodic group with exactly one conjugacy class of involutions such that the centraliser in G of an involution $u \in G$ is $C_G(u) \cong \mathrm{Dih}(8)$. A periodic group is one in which every element has finite order, however a periodic group is not necessarily finite itself, for example, the additive group $\mathbb{Q}^+/\mathbb{Z}^+$ is periodic but not finite.

Lemma 4.9. *Let t be an involution in G and $S = C_G(t)$.*

1. $S \cong \mathrm{Dih}(8)$
2. *The two distinct fours groups F_1, F_2 contained in S each have normaliser $N_G(F_1) \cong N_G(F_2) \cong \mathrm{Sym}(4)$.*
3. *For $i \in \{1, 2\}$, $P_i = N_G(F_i)$ is self-normalising and if $S \leq P_i \cap P_i{}^g$ then $P_i = P_i{}^g$.*
4. *If S is a subgroup of any finite $H \leq G$ then $S \in \mathrm{Syl}_2(H)$.*

Proof. There is some involution u with $C_G(u) \cong \mathrm{Dih}(8)$. Since all involutions are conjugate, there exists some $g \in G$ with $t = u^g$ and then $S = C_G(t) = C_G(u^g) = C_G(u)^g \cong \mathrm{Dih}(8)$ proving (1).

Let F_1, F_2 be the two fours groups in S. If F' is another fours groups containing t then F' would centralise t and thus be contained in S, so no other fours groups contains t. Each $F_i = \{1, t, t', t''\}$ and so

$$C_G(F_i) = C_G(t) \cap C_G(t') = C_{C_G(t)}(t') = C_S(t') = F_i.$$

F_i is index two in S and thus is normal in S so $S \leq N_G(F_i)$. Elements of $S - F_i$ act by conjugation on F_i inducing the permutation (t', t''). Repeating the argument with t' in place of t gives $C_G(t')$ also normalising F_i which will also be a fours group in $C_G(t')$ and so elements of

$C_G(t') - F_i$ induce the permutation (t, t'') on F_i. Now $\mathrm{Aut}(F_i) \cong \mathrm{Sym}(3)$ by Example 2.7 since a fours group is isomorphic to $C_2 \times C_2$. By Lemma 2.18 $N_G(F_i)/C_G(F_i) \leq \mathrm{Aut}(F_i)$ and we have that F_i is its own centraliser and $C_G(t) \cup C_G(t') \subseteq N_G(F_i)$ has size at least 12. Thus it must have size equal to 12 and $N_G(F_i)/C_G(F_i) \cong \mathrm{Aut}(F_i)$.

Let $M := N_G(F_i)$ a group of order 24. Consider the number of Sylow 3-subgroups of M. By Sylow's theorem there must be one or four. Suppose there is just one, call it T, then T must be normal in M. However then $[F_i, T] \leq F_i \cap T = 1$ (since each commutator element looks like $f^{-1}t^{-1}ft$ and $f^{-1}t^{-1}f \in T$ by normality of T and $t^{-1}ft \in F$ by normality of F, and $F_i \cap T = 1$ since every non-identity element of T has order three and no element of F_i can have order three). This implies that $T \leq C_G(F_i) = F_i$ which is impossible. Hence M has four Sylow 3-subgroups which must intersect trivially and given $T \in \mathrm{Syl}_3(M)$, then $N := N_M(T)$ is a subgroup of index four in M. The action of M on the cosets of N gives a homomorphism from N to Sym(4)

$$\phi \quad : \quad M \quad \longrightarrow \quad \mathrm{Sym}(4).$$

This has kernel $\mathrm{Ker}(\phi) = \bigcap_{m \in M} N_M(T)^m = \bigcap_{m \in M} N_M(T^m)$. This kernel is normal in both M and N. Since M has four Sylow 3-subgroups then the kernel is the intersection of the normalisers of these four subgroups. Each normaliser is a group of size six containing its corresponding Sylow subgroup. The Sylow 3-subgroups intersect trivially and so the normalisers can at most intersect at an element of order two. However if the kernel has size two then an involution in N is centralised by M by the normality of the kernel. This is a contradiction since the centraliser of any involution in G has size eight. Hence this homomorphism is injective and so bijective and we see that $M = N_G(F_i) \cong \mathrm{Sym}(4)$ proving (2).

Any element normalising S must centralise t so S must be self normalising. Suppose H is a finite subgroup of G containing S then $S \in \mathrm{Syl}_2(H)$ since if there is a power of two greater than three dividing $|H|$ then S is contained in a Sylow 2-subgroup of H. But then by Lemma 2.23 S is strictly contained in its normaliser which is a contradiction. This proves (4).

Let $P_i = N_G(F_i) \cong \mathrm{Sym}(4)$. Since $P_i \trianglelefteq N_G(P_i)$ and $S \in \mathrm{Syl}_2(P_1)$ then by a Frattini argument (Lemma 2.21) $N_G(P_i) = N_G(S)P_i$. However S is self normalising in G and so $N_G(P_i) = SP_i = P_i$ and so P_i is self normalising also.

Suppose $S \subseteq P_i \cap P_i^g$ for some $g \in G$. Then S is a Sylow 2-subgroup of P_i and of P_i^g. So S and S^g are both Sylow 2-subgroups of P_i^g. There must then exist some $h \in P_i^g$ with $S^{gh} = S$. However S is self normalising so it must be that $gh \in S$. This gives a contradiction because then $P_i = P_i^{gh} = P_i^g$ and so each conjugate of S is contained in just one conjugate of P_1 and one conjugate of P_2 proving (3). In particular since $P_1 \neq P_2$ (because $O_2(P_1) = F_1 \neq F_2 = O_2(P_2)$) and $S \subseteq P_1 \cap P_2$ (because S normalises both F_1 and F_2) then P_1 and P_2 cannot be conjugate in G.

□

Since F_1 and F_2 were chosen to be distinct fours groups then $P_1 = N_G(F_1)$ and $P_2 = N_G(F_2)$ must be distinct copies of Sym(4) else we would have a group isomorphic to Sym(4) with two normal fours groups which is not possible. Since $S \leq P_1 \cap P_2$ has size eight and $P_1 \neq P_2$ then it must be that $S = P_1 \cap P_2$.

$$\begin{tikzcd}
 & G \arrow[dl] \arrow[dr] & \\
P_1 \arrow[dr] & & P_2 \arrow[dl] \\
 & S = P_1 \cap P_2 \arrow[dl] \arrow[dr] & \\
F_1 & & F_2
\end{tikzcd}$$

Thus $(P_1, P_2, S, 1, 1)$ is a simple amalgam of the form $(\mathrm{Sym}(4), \mathrm{Sym}(4), \mathrm{Dih}(8))$. We can hence investigate the coset graph $\Gamma = \Gamma(G, P_1, P_2, S)$. Each vertex has degree three since $|P_i : S| = 3$ but G may not equal $\langle P_1, P_2 \rangle$ and so the graph may not be connected. Using what we know from Lemma 4.3 then from the previous lemma we have the following corollary.

Corollary 4.10. *Let $\alpha, \beta \in V(\Gamma)$ then $G_\alpha \cong \mathrm{Sym}(4)$, $G_{\alpha\beta} \cong \mathrm{Dih}(8)$ and if $G\alpha\beta \leq G_\alpha \cap G_\alpha^g$ for some $g \in G$ then $G_\alpha = G_\alpha^g$ and then $g \in G_\alpha$.*

Notice that since all involutions are conjugate there is a one-to-one correspondence between edges of Γ and involutions in G such that $i \in G \cap \mathcal{J}$ is related to an edge $\{\alpha, \beta\}$ if and only if $i \in Z(G_{\alpha\beta})$ if and only if $G_{\alpha\beta} = C_G(i)$. Define the map

$$\begin{array}{rcccc} \phi & : & G \cap \mathcal{J} & \longrightarrow & E(\Gamma) \\ & & i & \longmapsto & \{\alpha, \beta\} \end{array}$$

such that $i \mapsto \{\alpha, \beta\}$ if $i \in Z(G_{\alpha\beta})$. This map makes sense since $i = t^g$ for some $g \in G$ and so $C_G(i) = C_G(t^g) = S^g$ and this conjugate of S must fix the edge $\{P_1 g, P_2 g\}$ and so $i \in Z(S^g) = Z(G_{P_1 g P_2 g})$. Moreover $i \in Z(G_{\alpha\beta}) \cap Z(G_{\gamma\delta})$ forces $Z(G_{\alpha\beta}) = Z(G_{\gamma\delta})$ but then $G_{\alpha\beta} = C_G(i) = G_{\gamma\delta}$. The next lemma proves that this cannot happen for $\{\alpha, \beta\} \neq \{\gamma, \delta\}$ and so this map is well defined. The map is clearly injective since each $Z(G_{\alpha\beta})$ contains just one involution and is surjective since each edge stabiliser is a conjugate of S, say $G_{\alpha\beta} = S^g = C_G(t)^g = C_G(t^g)$, so $t^g \in Z(G_{\alpha\beta})$.

Lemma 4.11. *Let $\alpha, \beta, \gamma, \delta \in V(\Gamma)$ and $\{\alpha, \beta\}, \{\gamma, \delta\} \in E(\Gamma)$. If $G_\alpha = G_\delta$ then $\alpha = \delta$ and if $G_{\alpha\beta} = G_{\gamma\delta}$ then $\{\alpha, \beta\} = \{\gamma, \delta\}$.*

Proof. Suppose first that $G_\alpha = G_\delta$. Since G is transitive on edges, there exists $g \in G$ such that $\{\alpha, \beta\}g = \{\gamma, \delta\}$. Suppose that $\alpha g = \delta$ then by considering conjugates of point stabilisers we see that $G_\alpha^g = G_\delta = G_\alpha$. So by Corollary 4.10 $g \in G_\alpha$ and then $\alpha = \alpha g = \delta$. So suppose then that $\alpha g = \gamma$. In this case though we have that $G_\gamma^{g^{-1}} = G_\alpha = G_\delta \leq G_{\gamma\delta}$. However then $G_{\gamma\delta} \leq G_\gamma \cap G_\gamma^{g^{-1}}$ so Corollary 4.10 forces $G_\gamma = G_\gamma^{g^{-1}} = G_\delta$ which is a contradiction.

Now suppose that $G_{\alpha\beta} = G_{\gamma\delta}$. Again there exists some g satisfying $\{\alpha, \beta\}g = \{\gamma, \delta\}$ and then $G_{\alpha\beta}^g = G_{\gamma\delta} = G_{\alpha\beta} \leq G_\alpha, G_\beta$. Then $G_{\alpha\beta}^g \leq G_\alpha^g \cap G_\alpha$ and so $G_\alpha^g = G_\alpha$ and $g \in G_\alpha$ so $\{\alpha, \beta\}g = \{\alpha, \beta g\}$. However the same argument gives $g \in G_\beta$ so $\{\gamma, \delta\} = \{\alpha, \beta\}g = \{\alpha, \beta\}$.

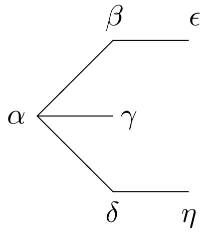
□

The amalgam $(\mathrm{Sym}(4), \mathrm{Sym}(4), \mathrm{Dih}(8))$ is simple. This forces the action of G on the graph to be faithful since the kernel of the action is the largest normal subgroup of G contained in $\mathrm{Dih}(8)$ which must be trivial.

Each point stabiliser is isomorphic to $\mathrm{Sym}(4)$ and each edge (or two point path) stabiliser is the intersection of two point stabilisers and is isomorphic to $\mathrm{Dih}(8)$ so in particular is a Sylow

2-subgroup of the point stabiliser. This forces some structure to our abstract group.

Consider the following vertices.



$G_{\alpha\beta}$ is the intersection of G_α and G_β and similarly $G_{\alpha\delta}$ is the intersection of G_α and G_δ. $G_{\alpha\beta\delta}$ is the intersection of these two Sylow 2-subgroups of Sym(4). However if α, β, γ are all fixed then δ must also be fixed. So $G_{\alpha\beta\gamma}$ must be the intersection of each of the three Sylow 2-subgroups and so must be $O_2(\mathrm{Sym}(4))$. A four point path stabiliser $G_{\delta\alpha\beta\epsilon}$ must be the intersection of the two fours-groups $G_{\delta\alpha\beta}$ and $G_{\alpha\beta\epsilon}$ from $G_{\alpha\beta} \cong \mathrm{Dih}(8)$. The fours-groups in Dih(8) intersect at the center of the group so $G_{\alpha\beta\delta\epsilon} = Z(G_{\alpha\beta})$. It follows that the stabiliser of any five point path is trivial. There can be no four cycles since as in the earlier example (Section 4.3) this would contradict the simplicity of the amalgam.

Lemma 4.12. *Assume $\eta, \delta, \alpha, \beta, \epsilon$ is a path of length four. Then*

- $G_{\delta\alpha\beta} = O_2(G_\alpha)$,
- $G_{\delta\alpha\beta\epsilon} = Z(G_{\alpha\beta})$,
- $G_{\eta\delta\alpha\beta\epsilon} = 1$.

Lemma 4.13. *Suppose for $\alpha, \beta \in V(\Gamma)$, $d(\alpha, \beta) \geq 4$ then $G_{\alpha\beta}$ has odd order.*

Proof. Suppose not then $G_{\alpha\beta}$ has even order and so by Cauchy's Theorem has an element z of order two. Since z is an involution in $G_\alpha \cong \mathrm{Sym}(4)$ then z is contained in a Sylow 2-subgroup and so $z \in G_{\alpha\gamma}$ for some $\gamma \in \Gamma(\alpha)$. Each involution in Dih(8) is contained in one of the two fours-groups each of which stabilise a path of length three and each involution in the fours group is contained in a subgroup of order two which is the center of an edge stabiliser,

$z \in Z(G_{\gamma\delta})$ (for some vertex δ with $d(\alpha,\delta) \leq 1$), moreover this edge shares a vertex with $\Gamma(\alpha)$. The same argument gives that $z \in Z(G_{\gamma_1\delta_1})$ where one of γ_1 or δ_1 is in $\Gamma(\beta)$. Since $E(\Gamma)$ is in one-to-one correspondence with $G \cap \mathcal{J}$ then $Z(G_{\gamma\delta}) = Z(G_{\gamma_1\delta_1})$ and $G_{\gamma\delta} = G_{\gamma_1\delta_1}$ which forces $\{\gamma,\delta\} = \{\gamma_1,\delta_1\}$ by Lemma 4.11 and then $d(\alpha,\beta) \leq 3$ which is a contradiction.

□

Lemma 4.14. *Suppose $\alpha,\beta \in V(\Gamma)$ are both cosets of the same group P_i ($i \in \{1,2\}$) with $d(\alpha,\beta) \geq 4$. Then $|G_\alpha \cap G_\beta| = 3$.*

Note that $d(\alpha,\beta) \geq 4$ allows for the possibility that there is no path between these vertices because then $d(\alpha,\beta) = \infty \geq 4$.

Proof. Let $\alpha_1,\alpha_2,\alpha_3$ be the three vertices in $\Gamma(\alpha)$ and let x_1,x_2,x_3 be the involutions corresponding to the edges $\{\alpha,\alpha_1\},\{\alpha,\alpha_2\},\{\alpha,\alpha_3\}$ respectively. Let $\{\beta,\beta_1\}$ be an edge and y the corresponding involution. For each $j \in \{1,2,3\}$ the edges corresponding to y and x_j have distance at least three. Suppose x_jy has even order $2k$ say. Then $z' := (x_jy)^k$ is an involution and so corresponds to some edge $\{\gamma,\delta\}$ where $z' \in Z(G_{\gamma\delta})$. Both x_j and y commute with this involution and so both are contained in its centraliser $C_G(z')$ which is the stabiliser of the edge $\{\gamma,\delta\}$. This forces both $C_G(x_j)$ and $C_G(y)$ to intersect with $C_G(z')$ at a fours group which forces both to share an edge with one of δ or γ but then $d(x_j,y) = 2$. Hence x_jy must have odd order (G is periodic so every element has finite order).

Let this order be $2k+1$. Then let $z_j = x_j(yx_j)^k$. This element is an involution (since both x_j and y are involutions) and it conjugates x_j to y and since it has order two then also y to x_j. So z_j swaps the edges $\{\alpha,\alpha_j\}$ and $\{\beta,\beta_1\}$. Since α and β are different cosets of the same group then it must be that $\alpha \cdot z_j = \beta$ and $\beta_1 \cdot z_j = \alpha_j$.

Define $h_j = z_1z_j$. Then h_j conjugates x_1 to x_j and any element which swaps these two edges must fix α and so h_j normalises G_α. Also $h_j = z_1z_j$ conjugates x_1 to y and then y to x_j and so h_j fixes the edge $\{\beta,\beta_1\}$ and thus fixes β and so normalises G_β. However G_α and G_β are self normalising so $h_1 = 1, h_2, h_3 \in G_\alpha \cap G_\beta$ which has odd order dividing 24. Thus $|G_\alpha \cap G_\beta| = 3$.

□

In this proof it appears that we are acting on the edges of the graph by conjugation rather than by right multiplication on the vertices. This action makes sense since we showed a one-to-one correspondence between edges of Γ and involutions in G.

Lemma 4.15. *The diameter of each connected component is at most four.*

Proof. Let Γ_0 be a connected component of Γ. Choose $\alpha, \beta \in V(\Gamma_0)$ so that $d(\alpha, \beta) = 4$. If this is not possible then clearly the result holds. So α and β are cosets of the same group. By the previous result $|G_\alpha \cap G_\beta| = 3$. Let x be a non-trivial element of this group then x has order three and fixes α and β. Let $\{\alpha_1, \alpha_2, \alpha_3\} = \Gamma(\alpha)$. If x fixes any of these then x is in an edge stabiliser, but this is impossible as edge stabilisers have size eight. So x must cycle the neighbours of α. This forces each of $\alpha_1, \alpha_2, \alpha_3$ to begin a path from α to β, i.e. $d(\beta, \alpha_i) = 3$ for each a_1. Thus no vertex of Γ_0 has distance five from β.

□

In particular note that this forces each connected component to be finite.

Lemma 4.16. Γ *is connected.*

Proof. Suppose Γ is not connected and let Γ_1, Γ_2 be distinct connected components of Γ. Let $\{\alpha_i, \beta_i\}$ be an edge from Γ_i $(i = 1, 2)$. Define $G_i := \langle G_{\alpha_i}, G_{\beta_i} \rangle$. G_{α_i} and G_{β_i} both fix a vertex and so G_i preserves Γ_i. Thus the coset graph (G_i, α_i, β_i) is simply Γ_i .

G_i acts faithfully on Γ_i (else a non-trivial normal subgroup of G_i would be contained in $G_{\alpha_i\beta_i}$ which is impossible as the amalgam is simple). So by Lemma 4.15 G_i must be finite.

Let $\{\gamma_i, \delta_i\}$ be any other edge in Γ_i then G_i is transitive on edges and so there exists g in G_i with $\{\alpha_i, \beta_i\} \cdot g = \{\gamma_i, \delta_i\}$. So the stabilisers of these edges must be conjugate in G_i and hence the involutions in G corresponding to each edge in Γ_i must be conjugate in G_i. So by the same reasoning as given for G the involutions in G_i are in one-to-one correspondence with the edges in Γ_i.

So if there exists an involution in $G_1 \cap G_2$ then this would correspond to an edge in both Γ_1 and Γ_2 which is impossible. Hence $G_1 \cap G_2$ has odd order.

Without loss of generality let α_1 and α_2 be cosets of P_1 in G and let $\gamma_1 \in \Gamma(\beta_1) - \{\alpha_1\}$. Then by Lemma 4.14

$$|G_{\alpha_1} \cap G_{\alpha_2}| = 3 = |G_{\gamma_1} \cap G_{\alpha_2}|.$$

Now $G_{\alpha_1} \cap G_{\gamma_1} = G_{\alpha_1\beta_1\gamma_1}$ (since there can be no four cycles) which has size four. If $G_{\alpha_1} \cap G_{\alpha_2} = G_{\gamma_1} \cap G_{\alpha_2}$ then $G_{\alpha_1} \cap G_{\alpha_2} \leq G_{\alpha_1} \cap G_{\gamma_1}$ which is impossible given their sizes. This forces $G_{\alpha_1} \cap G_{\alpha_2}$ and $G_{\gamma_1} \cap G_{\alpha_2}$ to intersect trivially. Within Sym(4), two elements of order three generate Alt(4) (consider any two elements of order three then the group they generate is clearly transitive on the four points so has order a multiple of four and clearly order a multiple of three but cannot generate the whole of Sym(4)) and so

$$\mathrm{Alt}(4) \cong \langle G_{\alpha_1} \cap G_{\alpha_2}, G_{\gamma_1} \cap G_{\alpha_2} \rangle \leq G_1 \cap G_2$$

which is a contradiction as $G_1 \cap G_2$ has odd order.

□

Fundamentally this forces G to be finite.

4.5 Identifying the Group

In the following result which will provide the possible orders of G we consider the vertices at a particular distance from some vertex. For a vertex α define

$$\Delta_j(\alpha) = \{\beta \in \Gamma \mid d(\alpha, \beta) = j\}.$$

Theorem 3. *Let G be a periodic group with one class of involutions such that for an involution t, $C_G(t) \cong \mathrm{Dih}(8)$. Then either*

- $|G| = 168$ *and* $|V(\Gamma)| = 14$, *or*
- $|G| = 360$ *and* $|V(\Gamma)| = 30$.

Proof. Since G is finite then $|G : P_1| = |G : P_2| = m < \infty$. So $|G| = 24m$ and $|V(\Gamma)| = 2m$ since there are m cosets of each P_i. Now consider a vertex α and $\Delta_j(\alpha) = \Delta_j$ for $j = 0, 1, 2, 3, 4$. Then

$$|\Delta_0| + |\Delta_2| + |\Delta_4| = m = |\Delta_1| + |\Delta_3|.$$

Clearly $|\Delta_0| = 2$ and $|\Delta_1| = 3$. Since there can be no four cycles then $|\Delta_2| = 6$. This gives that $m = |\Delta_4| + 7 = |\Delta_3| + 3$.

Suppose first that Γ has diameter at most three then $|\Delta_4| = 0$ so $m = 7$ and this satisfies the first case.

So suppose not, then Γ has diameter four. Consider G_α acting on Δ_4. By Lemma 4.14 the stabiliser of each vertex in Δ_4 has size three and so each orbit has length eight. In particular $|\Delta_4| \geq 8$. However since there are six vertices at distance two from α there can be at most twelve at distance three. This gives the inequalities:

$$m = |\Delta_4| + 7 \geq 8 + 7 = 15$$

$$m = |\Delta_3| + 3 \leq 12 + 3 = 15.$$

Hence $m = 15$, $|\Delta_3| = 12$, $|\Delta_4| = 8$ and so $|G| = 360$ and $|V(\Gamma)| = 30$.

□

Theorem 4. *Let G be a group of size 168 with exactly one conjugacy class of involutions such that the centraliser in G of an involution $t \in G$ is $C_G(t) \cong \mathrm{Dih}(8)$. Then $G \cong \mathrm{PSL}_3(2)$.*

Proof. Since G acts faithfully on the graph Γ then G acts faithfully on the set $\{G/P_1\}$ of size seven. This is because there can be no four cycles so if G fixes every vertex which is a coset of P_1 then it must fix all vertices and then it must be the identity. Since G acts faithfully on a set of size seven then there is an embedding of G into Sym(7)

$$\phi \ : \ G \ \longrightarrow \ \mathrm{Sym}(7).$$

Since G is an arbitrary group we take the liberty of calling this image under ϕ simply G. Recall Example 2.13, the derived group of Dih(8) is its center. Hence the central involution inside any Dih(8) can be written as a commutator of elements of Dih(8). Since G is now embedded in Sym(7) and since each involution is centralised by a group isomorphic to Dih(8) then each involution z satisfies

$$z \in C_G(z)' \leq \mathrm{Sym}(7)' = \mathrm{Alt}(7).$$

So every involution in G embeds into Alt(7). Now $S \cong \mathrm{Dih}(8)$ is generated by involutions from G and so also embeds into Alt(7). Moreover S is a Sylow 2-subgroup of Alt(7). Since Sylow subgroups are conjugate then every Sylow 2-subgroup of Alt(7) is dihedral and conjugate to S so without loss of generality

$$S := \langle (24)(56), (13)(45) \rangle.$$

The two fours groups are then

$$F_1 := \langle (26)(45), (13)(45) \rangle$$

and

$$F_2 := \langle (26)(45), (24)(56) \rangle.$$

Consider $\mathrm{PSL}_3(2)$ acting on the set of vectors described in Chapter 1 by left multiplication. This action is faithful and so $\mathrm{PSL}_3(2)$ can also be embedded in $\mathrm{Sym}(7)$

$$\psi \ : \ \mathrm{PSL}_3(2) \ \longrightarrow \ \mathrm{Sym}(7).$$

Let $X = \mathrm{PSL}_3(2)\psi$.

Consider the group

$$\left\langle \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

This group is dihedral of order eight (as it is generated by two non-commuting involutions). Considering how it acts on the set of size seven (by labelling vectors with numbers) then we can see that these matrices of order two correspond to even permutations in $\mathrm{Sym}(7)$. Let Y be the image of this group under ψ then Y is a Sylow 2-subgroup of $\mathrm{Alt}(7)$ and so is conjugate to S in $\mathrm{Alt}(7)$. Thus by conjugating where necessary G and X share a subgroup isomorphic to $\mathrm{Dih}(8)$. Let P_1 and P_2 be the normalisers of F_1 and F_2 in G respectively. We have $P_1 \cong \mathrm{Sym}(4)$ and so contains a cyclic subgroup C of order three. Since F_1 is normal in P_1 then P_1 and hence C acts on the non-identity elements of F_1 by conjugation. Since F_1 is self centralising in G then C must act regularly. F_1 is elementary abelian and so can be viewed as a vector space and moreover as a faithful and irreducible $\mathrm{GF}(2)C$-module. Hence by Lemma 3.11 C is determined up to conjugation in $\mathrm{Aut}(F_1) \cong N_{\mathrm{Sym}(4)}(F_1)/C_{\mathrm{Sym}(4)}(F_1)$. Now S is a subgroup of X also and the normaliser in X will also contain an element of order three and hence a cyclic subgroup of order three. Thus there exists an element of P_1 such that its image under conjugation by such an element is C. Now F_1 and C generate P_1 so G and the conjugate of X (which we'll continue to call X) intersect at a group isomorphic to $\mathrm{Sym}(4)$.

$$\begin{tikzcd}
 & & \mathrm{Sym}(7) \arrow[dl] \arrow[dr] & \\
 & G \arrow[dl] \arrow[dr] & & X \arrow[dl] \\
P_2 \arrow[dr] & & P_1 \arrow[dl] \arrow[dr] & \\
 & F_2 & & F_1
\end{tikzcd}$$

Now it turns out that $N_{\mathrm{Alt}(7)}(F_1) = \langle S, (124)(365)\rangle$ which has size 24 and so this equals P_1. Since $\langle (124)(365)\rangle \leq G$ is a Sylow 3-subgroup then each element in G of order three has this cycle shape. Consider $P_2 = N_G(F_2)$, clearly $\mathrm{Sym}(\{0,1,3\} \leq N_{\mathrm{Sym}(7)}(F_2)$. P_2 contains an element of order three with cycle shape $3^2.1$. Let the fixed point be 6 (or else re-label the points). The four possible elements are then (013)(245), (013)(254) and their squares. The elements (13),(45) interchange these choices whilst normalising S and P_1 (so not changing the intersection we have formed between G and X). Hence

$$G \geq \langle (24)(56), (13)(45), (124)(365), (013)(254)\rangle = \langle P_1, P_2\rangle = G.$$

Consider the element

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

in $\mathrm{PSL}_3(2)$. This element has order three. Considering the action of this element on the set of seven vectors we can write down a permutation for x. From this we can see that as a permutation it has cycle shape $3^2.1$. Since elements of order three generate Sylow 3-subgroups in X which are all conjugate in X then the elements in X of order three all have this cycle shape.

So up to conjugation by elements normalising P_1 then an element in Sym(7), of cycle type $3^2.1$, normalising the fours groups F_2 (which is contained in both G and X) is unique. Hence G and X are conjugate groups inside Sym(7). Since the representations of $\mathrm{PSL}_3(2)$ and G are injective then this gives $G \cong \mathrm{PSL}_3(2)$.

□

Theorem 5. *Let G be a group of size 360 with exactly one conjugacy class of involutions such that the centraliser in G of an involution $t \in G$ is $C_G(t) \cong \mathrm{Dih}(8)$. Then $G \cong \mathrm{Alt}(6)$.*

Proof. Notice that there can be no six cycles in the coset graph $\Gamma = \Gamma(G, P_1, P_2)$ by the same reasoning as in the earlier example. Define $\mathrm{opp}(\alpha) = \{\beta \in \Gamma \mid d(\alpha, \beta) = 4\}$. Then this set of vertices of the same coset type as α has size eight. By Lemma 4.14 for each $\beta \in \mathrm{opp}(\alpha)$ $G_\alpha \cap G_\beta$ is a group of size three which is necessarily cyclic. Since the order of a point stabiliser of the action of G_α on $\mathrm{opp}(\alpha)$ has size three then by the orbit-stabiliser theorem G_α is transitive on the set. Fix a β in $\mathrm{opp}(\alpha)$. Let X be the set of vertices in Γ which are cosets of the same type as α (then $|X| = 15$). Consider the set, which contains at least two elements α and β,

$$\mathrm{Fix}_X(G_\alpha \cap G_\beta) = \{\gamma \in X \mid \gamma \cdot g = \gamma \ \forall g \in G_\alpha \cap G_\beta\}.$$

Since $G_\alpha \cap G_\beta$ is a group of size three then $|\mathrm{Fix}_X(G_\alpha \cap G_\beta)| \equiv |X| \bmod 3 \equiv 0 \bmod 3$ by Lemma 2.19. So $|\mathrm{Fix}_X(G_\alpha \cap G_\beta)| \geq 3$ so there exists some λ also fixed by $G_\alpha \cap G_\beta$.

Suppose λ is at distance two from α. Then since there can be no four cycles then every element fixing α and λ fixes a path of length two. However then by Lemma 4.12 $G_\alpha \cap G_\beta$ is a subgroup of a group of size eight which is a contradiction. Hence $d(\alpha, \lambda) = 4$ and by the same argument $d(\beta, \lambda) = 4$. So $\lambda \in \mathrm{opp}(\alpha) \cap \mathrm{opp}(\beta)$. Suppose $|\mathrm{Fix}_X(G_\alpha \cap G_\beta)| > 3$ then since each element is either α or in $\mathrm{opp}(\alpha)$ then the set must have size six or nine. If it has size six then there are two elements in $\mathrm{opp}(\alpha)$ which are not fixed and so must be in the same orbit, but an orbit of size two is not possible. If it has size nine then $\mathrm{opp}(\alpha) \cup \{\alpha\} = \mathrm{opp}(\beta) \cup \{\beta\}$ and the group $H := \langle G_\alpha, G_\beta \rangle$ is transitive on this set of size nine with point stabiliser $H_\alpha = H \cap G_\alpha = G_\alpha$ and so $|H| = 9 \times 24 = 216$ but this does not divide $|G| = 360$, a contradiction. Hence $\mathrm{Fix}_X(G_\alpha \cap G_\beta) = \{\alpha, \beta, \lambda\}$.

The derived subgroup of $\mathrm{Sym}(4)$ is $\mathrm{Alt}(4)$ and so $G'_\alpha \cong \mathrm{Alt}(4)$. Moreover $G'_\alpha \cap G'_\beta = G_\alpha \cap G_\beta \leq G'_\alpha$ and so both β and λ have orbits of length four under the action of G'_α on $\mathrm{opp}(\alpha)$. Let these orbits be $O_1 = \{\beta, \beta_1, \beta_2, \beta_3\}$ and $O_2 = \{\lambda, \lambda_1, \lambda_2, \lambda_3\}$ (β and λ cannot be in the same orbit since $G_\alpha \cap G_\beta$ acts on this orbit and so $|\mathrm{Fix}_{O_1}(G_\alpha \cap G_\beta)| \equiv |O_1| \bmod 3 \equiv 1 \bmod 3$, so $G_\alpha \cap G_\beta$ would have to fix each of the four elements of the orbit but we have shown already this does not happen). Consider now the orbits of $G_\alpha \cap G_\beta$. Since this group has size three then the orbit lengths must be one or three. So they must be

$$\{\beta\},\ \{\lambda\},\ \{\beta_1, \beta_2\beta_3\},\ \{\lambda_1, \lambda_2, \lambda_3\}.$$

So $G_\alpha \cap G_\beta$ is transitive on $O_1 - \{\beta\}$ so by Lemma 2.22 G_α is 2-transitive on O_1. Now suppose $d(\beta, \beta_1) = 2$ then by 2-transitivity it must be that

$$d(\beta, \beta_2) = d(\beta_1, \beta_2) = d(\beta, \beta_3) = d(\beta_1, \beta_3) = d(\beta_2, \beta_3) = 2.$$

However then there must be a six cycle which is not possible. So $\beta_1, \beta_2, \beta_3 \in \mathrm{opp}(\alpha) \cap \mathrm{opp}(\beta)$. Now considering the orbits of the action of G'_β on $\mathrm{opp}(\beta)$ in the same way then there must be an orbit of size four containing $\beta_1, \beta_2, \beta_3$ and one of either α or λ.

Suppose first that an orbit of G'_β on $\mathrm{opp}(\beta)$ is $\{\beta_1, \beta_2, \beta_3, \lambda\}$. Then by the same arguments we must have

$$\{\beta_1, \beta_2, \beta_3\} \in \mathrm{opp}(\alpha) \cap \mathrm{opp}(\beta) \cap \mathrm{opp}(\lambda).$$

Now, G_α is transitive on $\mathrm{opp}(\alpha)$ so there exists an element $g \in G_\alpha$ swapping the vertices β and λ and so also swapping $\{\beta_1, \beta_2, \beta_3\}$ and $\{\lambda_1, \lambda_2, \lambda_3\}$. Moreover it must be that $G_\alpha \cap G_\lambda = G_\alpha \cap G_\beta$ and so $g \in N_{G_\alpha}(G_\alpha \cap G_\beta) \cong N_{\mathrm{Sym}(4)}(C_3) \cong \mathrm{Sym}(3)$. So this shows that

$$\{\lambda_1, \lambda_2, \lambda_3\} \in \mathrm{opp}(\alpha) \cap \mathrm{opp}(\beta) \cap \mathrm{opp}(\lambda).$$

This gives that $\mathrm{opp}(\alpha) \cap \mathrm{opp}(\beta) \cap \mathrm{opp}(\lambda)$ has size six and so the set

$$\Omega := \mathrm{opp}(\alpha) \cup \{\alpha\} = \mathrm{opp}(\beta) \cup \{\beta\} = \mathrm{opp}(\alpha) \cap \mathrm{opp}(\beta) \cap \mathrm{opp}(\lambda)$$

has size nine. The group $H = \langle G_\alpha, G_\beta \rangle$ then acts transitively on this set and so as before $|H| = 216$ which is impossible.

Thus $\{\beta_1, \beta_2, \beta_3, \alpha\}$ must be an orbit of G'_β on $\mathrm{opp}(\beta)$.

Consider now the orbits of $\langle G'_\alpha, G'_\beta \rangle$ on Ω. The orbit containing α must contain $\beta_1, \beta_2, \beta_3$ and the orbit containing β_1 must contain β and so the orbit must be

$$X_1 := \{\beta, \beta_1, \beta_2, \beta_3, \alpha\}.$$

$G_\alpha \cap G_\beta$ is cyclic of order three and fixes α and β and cycles the remaining three. So the pointwise set stabiliser $\mathrm{Stab}_G(X_1) = 1$. Thus G'_α acts faithfully on X_1 fixing α and similarly G'_β acts faithfully fixing β. Since $G'_\alpha \cong \mathrm{Alt}(4)$ and $G'_\beta \cong \mathrm{Alt}(4)$ both act faithfully on five points then there is an injective representation mapping $\langle G'_\alpha, G'_\beta\rangle$ into Sym(5). Moreover the index of this representation is two since $|\langle G'_\alpha, G'_\beta\rangle| = 5|G'_\alpha| = 60$ since the action on X_1 is transitive and $\mathrm{Stab}_{\langle G'_\alpha, G'_\beta\rangle}(\alpha) = G'_\alpha$. Hence $\langle G'_\alpha, G'_\beta\rangle \cong \mathrm{Alt}(5)$.

Recall we found an element $g \in G_\alpha$ which swaps β with λ and $\{\beta_1, \beta_2, \beta_3\}$ with $\{\lambda_1, \lambda_2, \lambda_3\}$. So in exactly the same way

$$X_2 := \{\alpha, \lambda, \lambda_1, \lambda_2, \lambda_3\}$$

is an orbit of $\langle G'_\alpha, G'_\lambda\rangle$ on Ω and it follows that $\langle G'_\alpha, G'_\lambda\rangle \cong \mathrm{Alt}(5)$.

Let $K := \langle G'_\alpha, G'_\beta\rangle$ then $\langle G'_\alpha, G'_\lambda\rangle = K^g$. Suppose $K = K^g$. Then K (K^g) is transitive on the elements of X_1 (X_2) so $X_1 = \alpha^K = \alpha^{K^g} = X_2$. However $X_1 \neq X_2$ so $K^g \neq K$. G acts on the cosets of K in G giving a homomorphism

$$\psi \ : \ G \ \longrightarrow \ \mathrm{Sym}(6)$$

and the kernel of this homomorphism is $\bigcap_{x \in G} K^x$ which is normal in K and so isomorphic to a normal subgroup of Alt(5), however Alt(5) is simple and since $K^g \neq K$ then this kernel must be trivial. Thus $G \cong \mathrm{Alt}(6)$.

□

4.6 The Theorem

Theorems 4 and 5 provide the main theorem of this chapter.

Theorem 6. *Let G be a periodic group with exactly one conjugacy class of involutions such that the centraliser in G of an involution $t \in G$ is $C_G(t) \cong \mathrm{Dih}(8)$. Then $G \cong \mathrm{PSL}_3(2)$ or $G \cong \mathrm{Alt}(6)$.*

5. IDENTIFYING GROUPS BY COUNTING INVOLUTIONS

In this chapter we will identify a finite group from minimal knowledge about a particular subgroup. Techniques from previous chapters will be used to explain how the group acts on cosets of a subgroup. We will also be considering representations of the group as it acts on a certain elementary abelian subgroup. This chapter and the resulting theorem is based entirely on the 2001 paper *Counting Involutions* by Aschbacher, Meierfrankenfeld and Stellmacher.

5.1 The Hypothesis and Preliminary Results

We begin with an elementary definition which we need to state the hypothesis which we will assume throughout this chapter.

Definition 5.1. *A subgroup M of a group G is a TI-subgroup if $M \cap M^g = \{1\}$ for any $g \in G - N_G(M)$.*

Our hypothesis is thus:

- G is a finite group with $M \leq G$,
- M is a TI-subgroup,
- $M^* := N_G(M) = MC_{M^*}(z)$ for some involution z from M^*,
- $C_G(x)$ has odd order for each $x \in M^\#$.

Several familiar groups satisfy this hypothesis. Consider $G = \mathrm{Sym}(4)$. Let M be any Sylow 3-subgroup, perhaps $M = \langle(123)\rangle$. Since M has prime order it is clearly TI. Also the centraliser of (123) (and (132)) is the group M and hence has odd order. The normaliser of M in G is a group isomorphic to Sym(3), $M^* = \langle(123),(23)\rangle$. Clearly $M^* = M\langle(23)\rangle$ and $\langle(23)\rangle$ is the centraliser in M^* of the element $z = (23)$. Hence Sym(4) satisfies the hypothesis.

The groups $\mathrm{PGL}_2(q)$, $\mathrm{PSL}_2(q)$ (q a prime power) will also be seen to satisfy the hypothesis by considering a subgroup of cosets each with a representative which is upper triangular. There are however fundamental differences between these groups and so several different cases will be considered. For example Sym(4) has two conjugacy classes of involutions, involutions of cycle type (ab) and involutions of cycle type $(ab)(cd)$. Whereas $\mathrm{PSL}_2(q)$ where q is a power of two turns out to have just one class of involutions.

Recall the statement of Bender's Lemma from Chapter 2. Recall also the notation used where $\mathcal{J}$ is the set of involutions in G; for any $S \subseteq G$, $n(S) = |\mathcal{J} \cap S|$ is the number of involutions in S; and $b_m = b_m(G, M)$ is the number of non-trivial cosets from G/M with exactly m involutions.

Notice from the assumption that $C_G(x)$ has odd order for each non-trivial element of M that M must have odd order and hence contains no involutions. Let $\mu = |M|$. Notice also that the normaliser of M in G, $M^* = MC_{M^*}(z)$, contains an involution so cannot be M itself. It is also assumed that M is not trivial else $M^\#$ would be meaningless.

For a group G, $m_2(G)$ is the 2-rank of G. This is the power of the largest elementary abelian 2-subgroup in G.

It is necessary to point out that the involution z which satisfies $M^* = MC_{M^*}(z)$ is fixed.

Lemma 5.2. *1. M is abelian of odd order and is inverted by z.*

2. $\mathcal{J} \cap M^* = z^M$.

3. $m_2(M^*) = 1$.

4. $C_{M^*}(z)$ is complement to M in M^* and $[z, M^*] = M$.

5. $n(Mz) = \mu$ and $Mz = z^M$ is the unique coset of M in G containing more than one involution.

Proof. (1) Let $W := C_G(M)$ then $C_G(M) \leq N_G(M) = M^*$ so $W = C_{M^*}(M)$. For any involution $i \in M^*$, $C_M(i) = 1$ since $C_G(y)$ has odd order for all $y \in M^\#$. So W has odd order and hence has no elements of order two. The inner automorphism of M corresponding to i, C_i, is thus fixed-point free on M. So by Lemma 2.24 M is abelian and inverted by each such i. In particular since M is abelian then $M \leq W$.

(2) Let i be any involution inverting any element of M. Since M is TI, i must be in M^*. Hence i must invert every non-trivial element of M. Since z inverts M, $zi \in W$. As W has odd order, Lemma 2.5 implies that $zi = w^2$ for some $w \in W$. So

$$i = zw^2 = zwzzw = w^{-1}zw \in z^W.$$

(z inverts w since w has odd order $2k+1$ say so $w = (w^{2k})^{-1} = (zi \dots zi)^{-1} = iz \dots iz$ which is inverted by z)

Apply Dedekind's rule (Lemma 2.14) with $M = B \leq W = A$, and $C_{M^*}(z) = C$. Then since $W \leq M^*$

$$W = W \cap M^* = W \cap MC_{M^*}(z) = M(W \cap C_{M^*}(z)) = MC_W(z).$$

Hence for each involution $i \in z^W$ there exists $m \in M, x \in C_W(z)$ with $mx \in W$ and $i = z^{mx}$. But x commutes with M and with z so $i = z^{mx} = z^{xm} = z^m \in z^M$. If i is any involution in M^*, then $i \in z^M$ and clearly any element in z^M is an involution in M^*.

(3) Suppose there is an elementary abelian 2-subgroup in M^* of order greater than two. Then there are distinct involutions z^n, z^m $(n, m \in M)$ whose product has order two also. So since z inverts M

$$1 = (z^n z^m)^2 = n^{-1}(nm^{-1})^z mn^{-1}(nm^{-1})^z m = n^{-1}(mn^{-1})mn^{-1}(mn^{-1})m = (n^{-1}m)^4.$$

But $n^{-1}m \in M$ so must have odd order, and so $n = m$. Therefore the greatest order of an elementary abelian 2-subgroup is two.

(4) $M \cap C_{M^*}(z) = C_M(z) = 1$ (otherwise z would be in $C_G(m)$ for each $m \in M$ which would then have even order) and by hypothesis $M^* = MC_{M^*}(z)$ hence $C_{M^*}(z)$ is complement to M in M^*.

$M^* = MC_{M^*}(z)$, so since z commutes with elements of $C_{M^*}(z)$ and inverts elements of M then

$$\begin{aligned}[z, M^*] &= \{zx^{-1}m^{-1}zmx \mid m \in M, x \in C_{M^*}(z)\} \\ &= \{x^{-1}zm^{-1}zmx \mid m \in M, x \in C_{M^*}(z)\} \\ &= \{(m^2)^x \mid m \in M, x \in C_{M^*}(z)\}.\end{aligned}$$

So $[z, M^*] = M^{C_{M^*}(z)}$ by Lemma 2.5 and this is simply M.

(5) Let $m \in M$. Then m has odd order, $2k+1$ say. Let $n = m^k$ then $n^2 m = 1$. Since z inverts M,

$$m = n^{-1}n^{-1} = n^{-1}n^z$$

and so

$$mz = z^n \in z^M.$$

Hence $Mz \leq z^M$.

Also for any $z^m \in z^M$,

$$z^m z = m^{-1}m^z = m^{-1}m^{-1} \in M.$$

Hence $z^m \in Mz$ and so $z^M = Mz$.

Now suppose i, j are distinct involutions in some coset C of M in G. Then $ij \in M^\#$ and both i and j invert this element ij. However, by (2), any such involution must be in $M^* \cap \mathcal{J} = z^M = Mz$. So $C = Mz$. Clearly $n(Mz) = \mu = |M|$.

□

Corollary 5.3. *Mz is the only coset of M in M^* containing an involution.*

Proof. By part (5) $z^M = Mz$ is the set of involutions in M^*. So it is clear that every involution lies in this coset.

□

We now extend our original hypothesis. Assume further that

- $M \ntrianglelefteq G$ (so $M^* \neq G$),
- $n(G) > |G : M|$.

The second point may seem an unusual thing to hypothesis however it is necessary to assume this in order to apply Bender's result (Lemma 2.25). Returning to our example where $G = \mathrm{Sym}(4)$ and M had order three. Notice that Sym(4) has nine elements of order two (six involutions of cycle type 2.1^3 and three of type $2^2.1$) and the index of M in G is of course eight. This example hence satisfies the extended hypothesis.

Recall that b_m is the number of non-trivial coset of M in G with exactly m involutions. We know already that $b_\mu = 1$, $b_i = 0$ for any $i \neq 0, 1, \mu$ and from the corollary $b_0 \geq |M^* : M| - 2$. So by Lemma 2.25

$$b_1 = \frac{1}{f}(\mu - (b_0 + 2)) - (b_0 + 2).$$

Where $f = \frac{n(G)}{|G:M|} - 1 > 0$. This value is non-negative so rearranging gives

$$\mu - b_0 - 2 \geq f(b_0 + 2)$$

and then

$$\mu \geq (f + 1)(b_0 + 2) > b_0 + 2.$$

Hence $b_0 < \mu - 2$. Bender's Lemma is a powerful tool here, it allows us to see how involutions are distributed between the cosets.

From now on let

- $|M^* : M| = \alpha$.
- $|C_G(z)|/\alpha = \rho$.
- $N = |G : M^*|$.

Our group now looks like this.

$$\begin{tikzcd}
 & & G \arrow[d, "N"] & \\
C_G(z) \arrow[dr, "\rho"] & & M^* \arrow[dl, "\mu"'] \arrow[dr, "\alpha"] & \\
 & C_{M^*}(z) \arrow[dr, "\alpha"'] & & M \arrow[dl, "\mu"] \\
 & & 1 &
\end{tikzcd}$$

Notice that since M and $C_{M^*}(z)$ intersect trivially, $|C_{M^*}(z)| = \alpha$ and α divides $|C_G(z)|$. Also $\alpha - 2 \leq b_0 < \mu - 2$ so $\alpha < \mu$.

A group action we will consider throughout this chapter is the action of G (and hence any subset of G) on the set of cosets of M^* in G by right multiplication.

$$M^*x \cdot g := M^*xg, \quad M^*x \in G/M^*, \ g \in G.$$

An element x fixes a coset M^*g if and only if $x \in M^{*g}$. So M^{*g} is the stabiliser of this particular coset in G. Of course if we consider just the subgroup M^* acting on the cosets then the stabiliser would be $M^* \cap M^{*g}$. We must therefore investigate such subgroups.

We now use the information we gathered from Bender's result to show that involutions are nicely distributed between certain cosets of M.

Lemma 5.4. *Let $g \in G - M^*$. Then $n(Mg) = 1$ and $n(M^*g) = \alpha$.*

Proof. Suppose $n(Mg) \neq 1$ then from part 5 of the Lemma 5.2, $n(Mg) = 0$. Suppose for some $m \in M$, $n(Mgm) \neq 0$ then some $ngm \in Mgm$ has order two. Hence, $1 = (ngm)^2$ and so $(mng)^{-1} = mng \in Mg$. This is impossible since Mg contains no involutions and if $mng = 1$ then $g^{-1} = mn \in M$ which is also impossible. Consider the action of M on the cosets of M in G and in particular the orbit containing Mg, $\{Mgm \mid m \in M\}$. This orbit has length μ and each coset in this orbit contains no involutions. So $b_0 \geq \mu$. This contradicts the deduction above that $b_0 < \mu - 2$. Hence $n(Mg) = 1$ for any $g \in G - M^*$.

M^* is a union of α cosets of M, $(Mx_1 \cup \ldots \cup Mx_\alpha)$, and so M^*g is a union of α cosets, $(Mx_1g \cup \ldots \cup Mx_\alpha g)$, each containing one involution and so $n(M^*g) = \alpha$.

□

We consider now subgroups of the form $M^* \cap M^{*g}$ in order to understand two-point stabilisers and to later help us recognise the important subgroup $C_{M^*}(z)$.

Lemma 5.5. *Set $C = M^* \cap M^{*c}$ for some $c \in G - M^*$. Then C is complement to M in M^*, C is inverted by the unique involution from Mc and itself contains a unique involution i such that $C = C_{M^*}(i)$.*

Proof. Let $U = \{u \in M^*c \mid u^2 = 1\}$ be the set of involutions in M^*c. By Lemma 5.4 this set has size α and is a set of coset representatives for the cosets of M in M^*c. Notice each involution $u \in U$ normalises C since $u = mc$ $(m \in M)$ so $M^{*u} = M^{*c}$ and $M^{*cu} = M^{*uu} = M^*$.
Pick $j \in U$ and set V to be the set of elements of C inverted by j. The set $\{uj \mid u \in U\}$ of size α is contained in V (each $uj \in C$ since $u = xc = c^{-1}x^{-1}, j = yc = c^{-1}y^{-1} \in M^*c$ so $uj = xy^{-1} = (x^{-1}y)^c \in M^* \cap M^{*c}$).

Now, M^*c is a union of its M-cosets: $M^*c = \bigcup_{u \in U} Mu$. But $M^*c = M^*j$, so $M^* = M^*cj$ which gives

$$M^* = \bigcup_{u \in U} Muj \leq MV \leq MC.$$

So we must have that $M^* = MC$ and in particular C must have even order and thus contain an involution.
Let i be an involution in C. Now, $i \in M^*$ so i inverts M, and so,

$$[M \cap C, i] = \{m^{-1}imi \mid m \in M \cap C\} = \{m^{-1}m^{-1} \mid m \in M \cap C\} = M \cap C$$

by Lemma 2.5 since $M \cap C$ has odd order. Hence

$$\begin{array}{rcll} M \cap C & = & [M \cap C, i] \leq [M^{*c}, i] & \text{(since } M \cap C \leq M^{*c}) \\ & & = [M^{*c}, z^{mc}] & (i = z^{mc} \text{ for some } m \in M) \\ & & = [M^{*mc}, z^{mc}] & \\ & & = [M^*, z]^{mc} & \text{(see Definition 2.11)} \\ & & = M^c & \text{(by Lemma 5.2 part (4)).} \end{array}$$

Thus $M \cap C \leq M \cap M^c = 1$. Hence M and C intersect trivially. So C is a complement to M in M^*. Hence $|C| = \alpha$ so $C = V = \{uj \mid u \in U\}$ and C is inverted by j. By Lemma 2.24 C is abelian and so $C \leq C_{M^*}(i)$. However $|C_{M^*}(i)| = |(C_{M^*}(z))^{mc}| = \alpha = |C|$. So $C = C_{M^*}(i)$. From part (3) of Lemma 5.2 $m_2(M^*) = 1$ so since C is abelian i must be the unique involution in C.

□

We can now improve upon our knowledge of the size of G.

Lemma 5.6.

- *$N = \mu(\rho - 1) + 1$,*
- *$|G| = N\mu\alpha = (\mu(\rho - 1) + 1)\mu\alpha$ and*
- *$b_1 = \alpha\mu(\rho - 1)$.*

Proof. For each $g \in G - M^*$, $M^* \cap M^{*g}$ contains a unique involution. So there is a unique involution $i = z^n$ (some $n \in M$) in $M^* \cap \mathcal{J} = z^M$ fixing M^*g. So $M^*g \in \text{Fix}_{G/M^*}(i) - \{M^*\}$. Since i is unique then M^*g can be in no other such set. So $G/M^* - \{M^*\}$ is a disjoint union of sets

$$\bigcup_{n \in M} \{\text{Fix}_{G/M^*}(z^n) - \{M^*\}\}.$$

Let $\Gamma = \text{Fix}_{G/M^*}(z)$ be the set of fixed points of G/M^* by z. Notice this is the same as $\text{Fix}(\langle z \rangle)$ where $\langle z \rangle \leq M^* = G_{M^*}$. Notice also that $z^G \cap M^* \leq z^{M^*}$ since any $z^g \in z^G \cap M^*$ has order two in M^* so is in $z^M \leq z^{M^*}$. Hence $z^G \cap M^* = z^{M^*}$ and so by Lemma 2.20, $N_G(\langle z \rangle) = C_G(z)$ is transitive on Γ. So since $C_{M^*}(z)$ stabilises M^*. The orbit-stabiliser theorem gives

$$|\Gamma| = |C_G(z) : C_{M^*}(z)| = |C_G(z)|/\alpha = \rho.$$

Notice, for all $n \in M$, $|\text{Fix}_{G/M^*}(z^n)| = |\Gamma| = \rho$, since

$$\begin{array}{rcl} \text{Fix}_{G/M^*}(z) & \longrightarrow & \text{Fix}_{G/M^*}(z^n) \\ M^*g & \longmapsto & M^*gn \end{array}$$

is a bijection. So each $\text{Fix}_{G/M^*}(z^n) - \{M^*\}$ has size $\rho - 1$ and so $N = |G/M^*| = \mu(\rho - 1) + 1$.

The other results follow from this.

□

Lemma 5.7. *Every element of $C_G(z) - \{M^*\}$ is an involution inverting $C_{M^*}(z)$ and if $\rho > 2$ then $C_G(z)$ is an elementary abelian 2-group E_{2^ϵ}; $\alpha = 2$ and $\rho = 2^{\epsilon-1}$ ($\epsilon \geq 2$).*

Proof. If $C_G(z) \leq M^*$ then $C_G(z) = C_{M^*}(z)$. So

$$\rho = \left|\frac{C_G(z)}{\alpha}\right| = \left|\frac{C_G(z)}{C_{M^*}(z)}\right| = 1.$$

Then by Lemma 5.6, $N = 1$ and this contradicts the assumption that $M^* \neq G$. So there exists some $g \in C_G(z) - M^*$.

Let $A = M^* \cap M^{*g}$. Then $z = z^g \in M^* \cap M^{*g}$ so by Lemma 5.5 $A = C_{M^*}(z)$ and is inverted by the involution $t \in M^*g$. So $A = M^* \cap M^{*t}$.

Since t inverts A and $z \in A$, t centralises z as does g, so $gt \in C_G(z)$, and since $t \in Mg$ then $gt \in M \cap C_G(z) = C_M(z) = 1$ by hypothesis. So each such $g \in C_G(z) - M^*$ is an involution inverting A.

Now suppose $\rho > 2$. Then $|C_G(z) : A| = |C_G(z)|/\alpha = \rho \geq 3$ so there are at least two non-trivial cosets of A in $C_G(z)$. One such coset is At and so there exists some $x \in C_G(z) - \{A, At\}$ with $At \neq Ax$ so $xt \notin A$. So each of x, t and xt invert A therefore xt must invert and centralise A and so each element of A must have order two ($a^{-1} = a^{xt} = (a^{-1})^t = a$) and A must be elementary abelian. So by part 3 of Lemma 5.2, A must have order two and then $\rho = |C_G(z)|/|A|$ is a power of two and every element of $C_G(z)$ has order two and so it is an elementary abelian 2-group.

□

5.2 Case 1: $\rho = 2$

We consider first the case when the index of the centraliser in M^* of z in the centraliser in G is just two. By Lemma 5.6 and since $|\mathcal{J}| = b_1 + \mu$ we have

- $|G| = \mu(\mu + 1)\alpha$.
- $|G : C_G(z)| = \mu(\mu + 1)/2$.
- $|G : M^*| = \mu + 1$.
- $|\mathcal{J}| = \mu(\alpha + 1)$.

Lemma 5.8. *G acts 2-transitively on G/M^* and M acts regularly on $G/M^* - \{M^*\}$. $A = C_{M^*}(z)$ is semi-regular on M and $|A| = \alpha = \mu - 1$ or $(\mu - 1)/2$.*

Proof. Let M act on G/M^*. Since M fixes the trivial coset then we can also let M act on just the set of non-trivial cosets. If any element m in M fixes some M^*g then $m \in M \cap M^{*g} = M \cap (M^* \cap M^{*g}) = 1$ by Lemma 5.5. Hence M is semi-regular on $G/M^* - \{M^*\}$. However, since $|M| = |G/M^* - \{M^*\}|$ then the action must be transitive which gives regularity.

M is transitive on $G/M^* - \{M^*\}$ and so M^* is also transitive. Thus G is 2-transitive on G/M^* by Lemma 2.22.

Suppose $1 \neq X \leq A$ with $1 \neq C_M(X)$. $C_M(z) = 1$ so $z \notin X$. Since A is abelian and $m_2(M^*) = 1$ then A can have only one element of order two, namely z, and so $|X|$ is odd.
Let $\text{Fix}(X) = \{M^*g \in G/M^* \mid M^*gx = M^*g \ \forall x \in X\}$. Then $C_M(X)$ acts regularly on $\text{Fix}(X) - \{M^*\}$ as M is regular on $G/M^* - \{M^*\}$. By Lemma 5.7 there is an involution $t \in C_G(z) - \{M^*\}$ inverting X. The action of $C_M(X)$ on $\text{Fix}(X) - \{M^*\}$ is equivalent to the action of $C_{M^t}(X)$ on $\text{Fix}(X) - \{M^*t\}$ and so $C_{M^t}(X)$ is regular also. Hence the full stabiliser of M^* in $Y = \langle C_M(X), C_{M^t}(X)\rangle$ is $C_M(X)$ which is transitive and so by Lemma 2.22, Y is 2-transitive on $\text{Fix}(X)$. Also $Y \leq C_G(X)$ so there is some $g \in C_G(X)$ sending M^* to M^*t. However $A\langle t\rangle = M^* \cap M^{*t}\langle t\rangle$ is the global stabiliser of $\{M^*m, M^*t\}$. Also each element of At inverts X and since $1 \neq X$ has odd order then no element can be inverted and centralised so $g \notin C_G(X)$. It follows that $C_M(a) = 1$ for each $1 \neq a \in A$ and so A is semi-regular on M.

We have that $|\mathcal{J}| = \mu(\alpha + 1)$ and $|z^G| = |G : C_G(z)| = \mu(\mu + 1)/2$ so since $z^G \subseteq \mathcal{J}$ then $\mu(\mu+1)/2 \leq \mu(\alpha+1)$ so $\alpha \geq (\mu-1)/2$. Also A is semi-regular on M so $M^{\#}$ is a union of orbits of A and so α divides $\mu - 1$. This gives that $\alpha = \mu - 1$ or $(\mu - 1)/2$.

□

Lemma 5.9. *M has no A-invariant subgroups and is elementary abelian. A is cyclic.*

Proof. If $|A| = \mu - 1$ then A is regular on $M^{\#}$. Suppose $1 \neq N \lneqq M$ is A-invariant. Then for any $n \in N^{\#}$ and $x \in M - N$ there exists an $a \in A$ with $n^a = m \notin N$ so this is impossible.

If $|A| = (\mu - 1)/2$ and N is an A-invariant subgroup strictly contained in M then $|N| \leq \mu/3$ (μ is odd). Let $n \in N^{\#}$. Since A is semi-regular on M then $C_A(n) = 1$, so provided $\mu > 3$ then

$$|\{n^A\}| = |A| = \alpha = (\mu - 1)/2 > \mu/3 \geq |N|$$

which is a contradiction. So suppose $\mu \leq 3$. Then $\mu \neq 1, 2$ so $\mu = 3$ but then $|A| = 1$ which is impossible as $z \in A$.

Let p be a prime factor of $|M|$. Let $\Pi = \{x \in M \mid x^p = 1\}$. Since M is abelian, Π is a subgroup of M. Π is A-invariant since any $x^a \in \Pi^A$ has order p or 1. Since M has no A-invariant subgroups, $\Pi = M$ and so M is elementary abelian.

Now A acts semi-regularly, and hence faithfully, on M. We have now that M is an elementary abelian group and can thus be regarded as a vector space. Thus by Lemma 3.7 A is cyclic.

□

Corollary 5.10. *$|G| = \mu(\mu + 1)(\mu - 1)$ or $\mu(\mu + 1)(\mu - 1)/2$ where μ is a prime power.*

Lemma 5.11. *$A = M^* \cap M^{*t}$ acts semi-regularly on $G/M^* - \{M^*, M^*t\}$. In particular if $|A| = \mu - 1$ then A acts regularly.*

Proof. Notice that $A = \mathrm{Stab}_{M^*}(M^*t)$. Let $\Sigma = G/M^* - \{M^*, M^*t\}$. For $M^*g \in \Sigma$, $M^*g = M^*tm$ for some $m \in M^{\#}$ since M is regular. This gives

$$M^*ga = M^*tma = M^*taa^{-1}ma = M^*tm^a.$$

Suppose for $M^*g \in \Sigma$, $M^*ga = M^*g$. Then for some $m \in M$, $M^*tm^a = M^*t$. So that $m^a \in M^{*t} \cap M = 1$. But then $m = 1$ and $M^*g = M^*t \notin \Sigma$.

Of course if $|A| = \mu - 1 = |\Sigma|$ then A is regular on Σ.

□

We now investigate the two possibilities

- $\alpha = \mu - 1$,
- $\alpha = (\mu - 1)/2$.

Case 1(a): $\alpha = \mu - 1$

Lemma 5.12. *A is contained at index two in a unique dihedral group D such that the action of D on G/M^* does not fix M^*.*

Proof. By Lemma 5.7 every $t \in C_G(z) - A$ is an involution inverting A. Let $D_t = \langle A, t\rangle$. Then $D_t = \langle a, t \mid t^2 = 1, a^t = a^{-1}\rangle$ (where a generates A) is dihedral and by Lemma 2.4 $D_t = A\langle t\rangle$ with A having index two in D_t. Notice that $t \in D_t$ and t swaps the cosets M^* and M^*t so D_t does not fix M^*.

Now let j be any other element of $C_G(z) - A$. Since $2 = r = |C_G(z) : A|$ then $At = Aj$ and so $D_t = A\langle t\rangle = A\langle j\rangle = D_j$. Let D be this dihedral group. Then the action of D on G/M^* does not fix M^*.

Suppose D' is another dihedral group with A at index two and not fixing M^*. For D' to be twice as big as A, $D' = \langle A, i\rangle$ for some involution i with i normalising A, moreover i must not fix M^*.

We will see later that G can be embedded in $\mathrm{Sym}(\mu + 1) \cong \mathrm{Sym}(G/M^*)$ (by considering a representation of the action of G on G/M^*). Consider how A embeds into this symmetric group as a group of permutations. Since A is a two point stabiliser then A fixes two points. Moreover since A is cyclic and transitive on the remaining points then the representation of A as permutations must be generated by a cycle of length $(\mu + 1) - 2 = \alpha$. Hence, any element normalising A but not fixing M^* must swap M^* and M^*t. This holds in $\mathrm{Sym}(\mu+1)$ and so also in G.

So i must swap M^* and M^*t and then $M^*t = M^*i$. It follows that $it = ttit \in M^* \cap M^{*t} = A$ and then $i \in At = C_G(z) - A$ and $D' = D$. So A is of index two in a unique dihedral group D with D not fixing M^*.

□

5.3 $\mathrm{PGL}_2(\mu)$

We consider the group $\mathrm{PGL}_2(\mu) = \mathrm{GL}_2(\mu)/S$ where $S = Z(\mathrm{GL}_2(\mu)) = \{\mathrm{diag}(\lambda, \lambda) \mid \lambda \in \mathrm{GF}(\mu)\}$ is the subgroup of all scalar matrices. Let $\overline{X} = \mathrm{PGL}_2(\mu)$. Then X has size $\mu(\mu + 1)(\mu - 1)$.

$\overline{X}$ has the subgroups:

$$\overline{Y} = \left\{ S\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid x \in \mathrm{GF}(\mu) \right\}$$

of order μ. Notice that since

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

then every element has order dividing p where μ is a power of p. Also $\overline{Y}$ is clearly abelian and so it is elementary abelian. $\overline{X}$ also has the subgroups

$$\overline{Z} = \left\{ S\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathrm{GF}(\mu), b \in \mathrm{GF}(\mu) - \{0\} \right\}$$

of order $\mu(\mu-1)$, and

$$\overline{W} = \left\{ S\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathrm{GF}(\mu) - \{0\} \right\}$$

Notice that $\overline{W}$ is isomorphic to $\mathrm{GF}(\mu)^{\times}$ and is therefore cyclic and that every element of $\overline{Z}$ is a product of an element from $\overline{Y}$ and an element from $\overline{W}$ so $\overline{Z} = \overline{YW}$.

$\overline{X}$ acts faithfully on a set of 1-spaces. Consider the set

$$\Omega = \{\langle(1,a)\rangle \mid a \in \mathrm{GF}(\mu)\} \cup \{\langle(0,1)\rangle\}.$$

$\overline{X}$ acts on this set since for any

$$S\begin{pmatrix} 1 & a \\ b & c \end{pmatrix} \in \overline{X}$$

and any 1-space $\langle(1,d)\rangle$ then

$$\left\langle\begin{pmatrix} 1 & d \end{pmatrix}\right\rangle \cdot S\begin{pmatrix} 1 & a \\ b & c \end{pmatrix} := \left\langle\begin{pmatrix} 1 & d \end{pmatrix}\begin{pmatrix} 1 & a \\ b & c \end{pmatrix}\right\rangle = \left\langle\begin{pmatrix} 1+bd & a+cd \end{pmatrix}\right\rangle.$$

It is easy to see that this action is well defined. Clearly this is only the same 1-space if $a = b = 0$ and $c = 1$ and so the action is faithful.

Moreover $\overline{Z}$ is the stabiliser of $\langle(0,1)\rangle$ since

$$\left\langle\begin{pmatrix} 0 & 1 \end{pmatrix}\right\rangle \cdot S\begin{pmatrix} 1 & a \\ b & c \end{pmatrix} = \left\langle\begin{pmatrix} b & c \end{pmatrix}\right\rangle$$

and this is $\langle(0,1)\rangle$ if and only if $b=0$. $\overline{W}$ is a two point stabiliser. It fixes the same space as $\overline{Z}$ and also the space $\langle(1,0)\rangle$.

$\overline{Y}$ is regular on the set $\Omega - \{\langle(0,1)\rangle\}$ since their sizes are equal and $\overline{Y}$ is transitive. For any 1-spaces $\langle(1,a)\rangle$ and $\langle(1,b)\rangle$ there is an element of $\overline{Y}$ taking one to the other.

$$\left\langle\begin{pmatrix} 1 & a \end{pmatrix}\right\rangle \cdot S\begin{pmatrix} 1 & b-a \\ 0 & 1 \end{pmatrix} = \left\langle\begin{pmatrix} 1 & b \end{pmatrix}\right\rangle.$$

$\overline{W}$ is regular on $\Omega - \{\langle(1,0)\rangle, \langle(0,1)\rangle\}$ in the same way.

Observe also that $\overline{W}$ acts regularly on $\overline{Y}^{\#}$ via

$$S\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \bullet S\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} := S\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} = S\begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix}.$$

Proposition 5.13. *Suppose q is a power of some prime p and $X \leq \mathrm{Sym}(q+1)$ of size $q(q+1)(q-1)$ with $Z \leq X$ a point stabiliser of size $q(q-1)$ and an elementary abelian $Y \leq Z$ is regular on the remaining points. Suppose further that $W \leq Z$ is cyclic and a two point stabiliser and that it is regular on the remaining points and on the non-trivial elements of Y. Finally suppose that $Z = YW$. Then Z is determined up to conjugation in $\mathrm{Sym}(q+1)$.*

Proof. Y is regular on q points and so has size q. We have that q is a prime power and is the size of Y which is elementary abelian. So by Lemma 2.2 Y is unique up to isomorphism. By Corollary 3.9 then Y is determined up to conjugation in $\mathrm{Sym}(q)$. So suppose another group X' satisfies the hypothesis.

$$\begin{tikzcd}
 & & & \mathrm{Sym}(q+1) \arrow[dll] \arrow[drr] & & & \\
 & X' \arrow[d] & & & & X \arrow[d] & \\
 & Y'W' \arrow[dl] \arrow[dr] & & & & YW \arrow[dl] \arrow[dr] & \\
W' & & Y' & & Y & & W
\end{tikzcd}$$

Then a conjugate of this group X'^g exists which satisfies the hypothesis and for which the elementary abelian regular group Y'^g is equal to Y.

$$\begin{tikzcd}
 & & \mathrm{Sym}(q+1) \arrow[dl] \arrow[dr] & & \\
 & X'^g \arrow[d] & & X \arrow[d] & \\
 & YW'^g \arrow[dl] \arrow[dr] & & YW \arrow[dl] \arrow[dr] & \\
W'^g & & Y & & W
\end{tikzcd}$$

W is abelian and acts regularly on $Y^{\#}$. Y is an elementary abelian group and so can be viewed as a vector space. Moreover Y is a faithful and irreducible (by Lemma 5.9) $\mathrm{GF}(p)W$-module by defining a multiplication to be this action. Thus by Lemma 3.11 a linear representation of W is determined up to conjugation in $\mathrm{GL}(Y)$ so W is determined up to conjugation in $\mathrm{Aut}(Y)$. However Y is regular on the points it doesn't fix so by Corollary 3.10 and Lemma 2.17 $\mathrm{Aut}(Y) \cong N_{\mathrm{Sym}(q)}(Y)/C_{\mathrm{Sym}(q)}(Y)$ so each automorphism is an inner automorphism and so is the same as conjugating by an element from $N_{\mathrm{Sym}(q)}(Y) \leq \mathrm{Sym}(q) \leq \mathrm{Sym}(q+1)$. So again suppose another group X'^g satisfies the hypothesis then it contains the subgroup Y and there exists some $h \in N_{\mathrm{Sym}(q)}(Y)$ conjugating the cyclic W'^{g} to W and leaving $Y = Y^{h}$ invariant. So X'^{gh} contains the subgroups Y and W and thus YW.

$$\begin{tikzcd}
 & \mathrm{Sym}(q+1) \arrow[dl] \arrow[dr] & \\
X'^{gh} \arrow[dr] & & X \arrow[dl] \\
 & YW \arrow[dl] \arrow[dr] & \\
W & & Y
\end{tikzcd}$$

Thus $Z = YW$ is determined up to conjugation in $\mathrm{Sym}(q+1)$.

□

This argument is fundamental to recognising the isomorphism type of our abstract group. It is an argument we will see again in this chapter. We can now prove the main theorem for this case and recognise G as a projective linear group.

Theorem 7. *G is isomorphic to* $\mathrm{PGL}_2(\mu)$.

Proof. Both G and $\mathrm{PGL}_2(\mu)$ act faithfully on a set of size $\mu+1$. Permutation representations can hence be defined.

$$\begin{array}{rcrcl} \Phi & : & G & \longrightarrow & \mathrm{Sym}(\mu+1) \\ \Psi & : & \mathrm{PGL}_2(\mu) & \longrightarrow & \mathrm{Sym}(\mu+1). \end{array}$$

Since G is an arbitrary group and Φ a monomorphism of G, $G\Phi$ satisfies the original hypothesis. So we call this image in $\mathrm{Sym}(\mu+1)$ simply G.

Let $q = \mu$, $X = \mathrm{Im}(\Psi)$, $Y = \mathrm{Im}(\Psi|_{\overline{Y}})$, $Z = \mathrm{Im}(\Psi|_{\overline{Z}})$ and $W = \mathrm{Im}(\Psi|_{\overline{W}})$. Then by Proposition 5.13 Z is determined up to conjugation in $\mathrm{Sym}(\mu+1)$. Clearly G also satisfies Proposition 5.13 so there exists $g \in \mathrm{Sym}(\mu+1)$ such that $M^{*g} = Z$. Again since G is arbitrary then we call the conjugate of G by g simply G.

A is a cyclic subgroup of $\mathrm{Sym}(\mu+1) \cong \mathrm{Sym}(G/M^*)$ and a two point stabiliser which is transitive on $G/M^* - \{M^*, M^*t\}$ by Lemma 5.11. So a generator of A is an $|A|$-cycle of $G/M^* - \{M^*, M^*t\}$ (where t is such that $A = M^* \cap M^{*t}$) and so it is clear that the centraliser in S of A is $C_S(A) = A \times \langle \tau \rangle$ where τ is the transposition swapping M^* and M^*t. Now, A is regular on a set of size $\mu - 1$ so by Lemmas 2.17 and 3.10 $C_{\mathrm{Sym}(\mu-1)}(A) = A$ and $\mathrm{Aut}(A) = N_{\mathrm{Sym}(\mu-1)}(A)/A$. So we see that $B := N_{\mathrm{Sym}(\mu+1)}(A)_{M^*} = N_{\mathrm{Sym}(\mu-1)}(A) = \mathrm{Aut}(A) \ltimes A$ and then $N_{\mathrm{Sym}(\mu+1)}(A) = \langle \tau \rangle B$. By Lemma 5.12 A is contained at index two in a unique dihedral group $D \leq G$ such that D does not fix M^*. Hence within $\mathrm{Sym}(\mu+1)$ A is contained uniquely at index two in D such that $D \not\leq B$ and D is dihedral. Moreover, since M^* is transitive on $G/M^* - \{M^*\}$ then $G = \langle M^*, t \rangle = \langle M^*, D \rangle$. This D is unique and so since we let $M^* = Z$ then D uniquely contains Z also and so

$$G = \langle D, M^* \rangle = \langle D, Z \rangle \subseteq X.$$

We conclude that $G = X$ and so via the appropriate conjugations and representations G is isomorphic to $\mathrm{PGL}_2(\mu)$.

□

Recall the example $G = \mathrm{Sym}(4)$ with $M = \langle (123) \rangle$. Then $\mu = 3$ and $\alpha = 2$. So we must have that $\mathrm{Sym}(4) \cong \mathrm{PGL}_2(3)$.

Case 1(b): $\alpha = (\mu - 1)/2$

Theorem 8. *G has one conjugacy class of involutions and is isomorphic to* $\mathrm{PSL}_2(\mu)$.

We have $|\mathcal{J}| = \frac{\mu(\mu+1)}{2} = |z^G|$ so G has one class of involutions.

By Lemma 5.8 G is 2-transitive on G/M^* and by Lemma 5.11 A is semi-regular on $\Sigma = G/M^* - \{M^*, M^*t\}$ so for $M^*g \in \Sigma$, $\mathrm{Stab}_A(M^*g) = 1$. It follows that any three-point stabiliser is trivial. Thus G is a Zassenhaus group and M^* is a point stabiliser and so a Frobenius group with complement A and some kernel which we will call K. Hence G is a Zassenhaus group of type (A, K) and degree $\mu + 1$. By Theorem 2 (Zassenhaus) $G \cong \mathrm{PSL}_2(\mu)$.

5.4 Case 2: $\rho > 2$

We return now to the case when the index of the centraliser of z in M^* in the whole centraliser is greater than two. We have that $C_G(z) \cong E_{2^\epsilon}$, $\alpha = 2$ and $\rho = 2^{\epsilon-1}$ for some integer $\epsilon > 2$ and so by Lemma 5.6

- $|G| = 2\mu(\mu(2^{\epsilon-1} - 1) + 1)$.
- $|z^G| = |G : C_G(z)| = \mu(\mu(2^{\epsilon-1} - 1) + 1)/2^{\epsilon-1}$.
- $|\mathcal{J}| = \mu(2^\epsilon - 1)$.

Let $\delta = \epsilon - 1$.

$$\mu(\mu(2^\delta - 1) + 1)/2^\delta = |z^G| \leq |\mathcal{J}| = \mu(2^\delta)$$

and so

$$\mu(2^\delta - 1) \leq 2^\delta(2^{\delta+1} - 1) - 1 = (2^\delta - 1)(2^{\delta+1} + 1)$$

and then

$$\mu \leq 2^{\delta+1} + 1 = 2^\epsilon + 1. \tag{5.1}$$

Case 2(a) *: G has more than one conjugacy class of involutions*

In this case the inequality (5.1) is strict.

Lemma 5.14. $\mu = 2^\delta + 1$.

Proof. We have $|G : C_G(z)| = \mu(\mu(2^\delta - 1) + 1)/2^\delta$, therefore

$$\mu(2^\delta - 1) + 1 = \frac{2^\delta |G : C_G(z)|}{\mu}.$$

Also $\frac{|G:C_G(z)|}{\mu} \in \mathbb{Z}$ since μ is odd, and so

$$0 \equiv \mu(2^\delta - 1) + 1 \equiv \mu - 1 \bmod 2^\delta.$$

This gives that $\mu - 1$ is strictly less than $2^{\delta+1}$ and a multiple of 2^{δ} so it must be that $\mu = 2^{\delta}+1$.

□

Note that for $i \in \mathcal{J} - z^G$, i is an involution not from M^* so i inverts no element of M as M is TI (see Lemma 5.2).

Lemma 5.15. *Each element of G of odd order is in a conjugate of M and each $i \in \mathcal{J} - z^G$ inverts no element of G odd order.*

Proof. Let $x \in G^{\#}$ have odd order. Pick $y \in \langle x \rangle$ such that y has prime order p. Set $\Omega = G/M$. Then $|\Omega| = 2^{2d+1}$. Now $\langle y \rangle$ is a subgroup of G of prime order which acts on Ω. Also $|\Omega|$ and p are co-prime so $|\Omega| \not\equiv 0 \bmod p$. Each orbit of $\langle y \rangle$ on Ω has length 1 or p. Suppose there are m orbits of length 1. Then $|\Omega| \equiv m \bmod p$ (by Lemma 2.19). Thus $m \not\equiv 0 \bmod p$ and in particular $m \neq 0$. So there is at least one orbit of length 1. Hence there exists some $g \in G$, $Mg \in G/M$ such that $Mgy = Mg$ and then $y \in M^g$, y is a power of x so commutes with x therefore

$$y = y^{x^{-1}} \in M^{gx} \cap M^g \neq 1.$$

Since M is TI, $M^{gx} = M^g$ therefore $x \in N_G(M^g) = N_G(M)^g$. So $M^g x \in N_G(M)^g/M^g$ which is a two group. But $M^g x$ has odd order so $M^g x = M^g$ and so $x \in M^g$.

Suppose i inverts some non-trivial element of a conjugate of M, M^g say. Then for some $m \in M$,

$$(m^g)^i = (m^g)^{-1} = (m^{-1})^g \;\therefore\; m^{gig^{-1}} = m^{-1}.$$

So $i^{g^{-1}}$ is an involution inverting an element of M so $i^{g^{-1}} \in z^M$ and then $i^{g^{-1}} = z^n$ for some $n \in M$. However this means that $i = z^{ng} \in z^G$. Thus i can invert no element of any conjugate of M and so no element of odd order.

□

We thus come to the main theorem for this case. The theorem fails to assign an isomorphism type to the group but does however provide some useful information about the group.

Theorem 9. *Let $R = O_2(G)$. Then M is semi-regular on R, $R \cong E_{2^{2\delta}}$, $G = RM^*$, M is cyclic and M^* is dihedral.*

Proof. R is a normal subgroup of G so M certainly acts by conjugation on R. By the original hypothesis $C_G(x)$ is of odd order for each $x \in M^{\#}$ so must intersect trivially with R. This implies that $C_R(x) = 1$ and so M is semi-regular on R.

Let $i \in \mathcal{J} - z^G$ and define $x := ii^g$. Then i inverts x so x must have even order which will be a power of two (since $|G| = |M|2^{2\delta+1}$). Hence $\langle i, i^g \rangle$ is a 2-group for every $g \in G$. By Theorem 1 (Baer-Suzuki) $i \in O_2(G) = R$. Therefore, $\mathcal{J} - z^G \subseteq R$.

Suppose V is an M-invariant, non-trivial subgroup of R. Since no element of $V^{\#}$ is fixed by any element of M (as M acts semi-regularly on R) then each orbit has length $2^\delta + 1$ and so

$$|V^{\#}| \equiv 0 \bmod 2^\delta + 1.$$

In particular $|V| \geq 2^\delta + 2$. Also, R is a 2-group so $|R| \leq 2^{2\delta+1}$ and V must also be a 2-group so $|V| = 2^{\delta+\eta}$ for some $\eta \in \mathbb{Z}$ and $|V^{\#}| = 2^{\delta+\eta} - 1$ must be a multiple of $2^\delta + 1$. Therefore

$$\frac{2^{\delta+\eta} - 1}{2^\delta + 1} = \frac{(2^\delta + 1)(2^\eta - 2^{\eta-\delta})}{2^\delta + 1} = (2^\eta - 2^{\eta-\delta}) \in \mathbb{Z}.$$

This gives $\eta \geq \delta$ and so $2^{2\delta} \leq |V| \leq |R| \leq 2^{2\delta+1}$.

Recall that $|M^*| = 2|M| = 2(2^\delta + 1)$ so the only elements of M^* of order a power of two have order exactly two. Suppose $x \in R \cap M^*$, then x must have order two and so $x = z^g \in z^G$ for some $g \in G$. Since $R \trianglelefteq G$ then $z^G \subseteq R$ and so $\mathcal{J} \subseteq R$. This is a contradiction though since

$$|\mathcal{J} \cup \{1\}| = (2^\delta + 1)(2^{\delta+1} - 1) + 1 > 2^{2\delta+1} = |R|.$$

We conclude that $M^* \cap R = 1$ and so R is complement to M^* in G and hence $|R| = |V| = 2^{2\delta}$. By Lemma 5.2 (3) R must be elementary abelian and so can be viewed as a vector space over GF(2). We have seen that as such it is an irreducible GF(2)M-module and so by Lemma 3.7 M is cyclic.

Since $M = \langle m \rangle$ is cyclic and $M^* = MA = M \cup Mz$ then $M^* = \langle m, z \rangle$ where z is an involution inverting m. So by definition M^* is dihedral.

□

***Case 2(b)**: G has one conjugacy class of involutions*

The inequality (5.1) in this case is an equality and $\mu = 2^\epsilon+1$, $|G| = 2^\epsilon(2^{2\epsilon}-1)$. Also $C_G(z) \cong E_{2^\epsilon}$ so for every $i \in \mathcal{J} = z^M$, $i = z^m$ for some $m \in M$ and then $C_G(i) = C_G(z^m) = C_G(z)^m \cong E_{2\epsilon} \in \mathrm{Syl}_2(G)$.

The methods used in this section to identify G parallel case (1a) but with different groups playing the roles of point stabiliser and two point stabiliser and so most of the methods used are essentially the same and it is suggested the reader refer back to this section for more information.

Lemma 5.16. *Let $S = C_G(z)$. Consider G acting on the set $\Omega = G/N_G(S)$. Then $N_G(S)$ is a maximal subgroup and a point stabiliser, S is regular on 2^ϵ points, and a two point stabiliser, B, is regular on $2^\epsilon - 1$ points and cyclic. Finally $N_G(S) = SB$.*

Proof. Let $S^* := N_G(S)$. If i is an involution normalising S then $\langle S, i\rangle$ is a 2-group strictly containing S. So since S is a Sylow 2-subgroup then it must be that $S^* \cap \mathcal{J} = S$. Now $S = C_G(z)$ and is elementary abelian so it is clear that each $x \in S^\#$ is an involution and that $S = C_G(x)$ also. Now each involution is conjugate to z so the centraliser of each involution is conjugate to S so the conjugates of S must be equal or else intersect trivially. Now $|\mathcal{J}| = (2^\epsilon + 1)(2^\epsilon - 1)$ and each conjugate of S contains $2^\epsilon - 1$ involutions so there must be $2^\epsilon + 1$ distinct conjugates and so $|G : S^*| = 2^\epsilon + 1$ and $|S^*| = 2^\epsilon(2^\epsilon - 1)$.

We get that S acts regularly on $\Omega - \{S^*\}$ since for $g \notin S^*$ then $S^*g \cdot s = S^*g$ for $s \in S$ if and only if $s \in S^{*g} \cap S = N_G(S^g) \cap S = 1$. So S acts semi-regularly on the set and transitively since $|S| = 2^\epsilon = |\Omega - \{S^*\}|$.

Let $u \in \mathcal{J} - S$ then $u \notin S^*$ so $S^*u \neq S^*$. Let $B = S^* \cap S^{*u} = N_G(S) \cap N_G(S^u)$ a two point stabiliser. Since any involution normalising S must be in S and since S and S^u share no involutions, B must have odd order which must divide $2^\epsilon - 1$.

Consider the $2^\epsilon + 1$ cosets of S^* in G and the set of involutions $\mathcal{J}$ of size $(2^\epsilon + 1)(2^\epsilon - 1)$. We have that $2^\epsilon - 1$ of these are in S^* and by the pigeon hole principle at least one other coset contains at least $2^\epsilon - 1$ involutions. Without loss of generality let this coset be S^*u (else change choice of u). Let $U = S^*u \cap \mathcal{J}$ and let $V = \{uv \mid v \in U\}$. Each element of V is an element of B (exactly as in the proof of Lemma 5.5). It follows that $|B| = 2^\epsilon - 1$ and as before, by Lemma 2.24 B is inverted by u and is abelian.

B acts semi-regularly on $S^\#$ since for $s \in S^\#$ then $s^n = s$ if and only if $n \in C_G(s) \cap N = S \cap N = 1$

so since $|B| = |S^{\#}|$ then B is regular. Thus by Lemma 3.7 B is cyclic.

S is regular on $\Omega - \{S^*\}$ so for $S^*g \in \Omega - \{S^*, S^*u\}$ we can find $s \in S$ such that $S^*us = S^*g$. Then for any $b \in B$, $S^*g \cdot b = S^*us \cdot b = S^*u(bb^{-1}sb) = S^*u(s^b)$ (b fixes the coset S^*u) and so $S^*g \cdot b = S^*g$ if and only if $s^b s \in N_G(S^{*u}) \cap S = 1$ which is impossible as B is regular unless $b = 1$. So B is semi-regular on $\Omega - \{S^*, S^*u\}$ and thus regular. (Notice this forces any three point stabiliser to be trivial.)

Now $|SB| = 2^\epsilon(2^\epsilon - 1) = |S^*|$ and so S^* is equal to this product, it also clearly fixes the point $S^* \in \Omega$. If g is any element not in S^* then $\langle S^*, g\rangle = G$ since $S \leq S^*$ is transitive on the non-trivial cosets and so $\langle S^*, g\rangle = \{S^*, S^*g \cdot s \mid s \in S\} = G$. Hence S^* is maximal.

□

Lemma 5.17. *There is a unique dihedral group D containing B at index two. This dihedral group does not fix S^*.*

Proof. For every involution $i \in G - S$, $C_B(i) \leq C_G(i)$ and so $C_B(i)$ is a 2-group. However $C_B(i) \leq B$ which has odd order and so $C_B(i)$ has odd order and so it must be that $C_B(i) = 1$. So any involution normalising B must give a fixed-point free automorphism and so by Lemma 2.24 the involution must invert B.

Let $D_u = \langle B, u\rangle = B\langle u\rangle$ (as before). We have that u inverts B and so D_u is dihedral with B at index two. Since $B = S^* \cap S^{*u}$ then any involution normalising B must either fix or swap the two conjugates. S^* (and so its conjugates also) is self-normalising since it is maximal and for $g \notin S^*$, $S^g \neq S$ so $S^{*g} = N_G(S^g) \neq N_G(S) = S^*$. So any involution fixing S^* and S^{*u} must be in B which is impossible. Any involution i swapping the conjugates must in fact be contained in S^*u. We showed before that $B = \{uv \mid v \in S^*u \cap \mathcal{J}\}$ and so $ui \in B$ and so $D_u = B\langle u\rangle = B\langle i\rangle = D_i$. Let D be this unique subgroup and we are done.

□

G acts faithfully on the set Ω and so there exists an injective permutation representation

$$\phi \ : \ G \ \longrightarrow \ \mathrm{Sym}(2^\epsilon + 1).$$

Since G is an abstract group and ϕ a monomorphism then the permutation representation of G in $\mathrm{Sym}(2^\epsilon + 1)$ satisfies any hypotheses about G and so we call the image of G simply G.

5.5 $\mathrm{PSL}_2(2^\epsilon)$

$\mathrm{PSL}_2(2^\epsilon) = \mathrm{SL}_2(2^\epsilon)/Z(\mathrm{SL}_2(2^\epsilon)) \cong \mathrm{SL}_2(2^\epsilon)$ ($Z(\mathrm{SL}_2(2^\epsilon)) = 1$ since this is a group of diagonal matrices $\mathrm{diag}(\lambda, \lambda)$ where $\lambda \in \mathrm{GF}(2^\epsilon)^\times$ has order dividing two, which is impossible unless $\lambda = 1$.) We will consider the action of $\mathrm{SL}_2(2^\epsilon)$ rather than $\mathrm{PSL}_2(2^\epsilon)$ to make the notation more simple. Of course the actions are equivalent.

In a very similar way to Section 5.3 $\overline{X} = SL_2(2^\epsilon)$ acts faithfully on the set $\Pi = \{\langle(1, a)\rangle \mid a \in \mathrm{GF}(2^\epsilon)\} \cup \langle(0, 1)\rangle$ via

$$\left\langle\begin{pmatrix} a_1 & b_1 \end{pmatrix}\right\rangle \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \left\langle\begin{pmatrix} a_1a + b_1c & a_1b + b_1d \end{pmatrix}\right\rangle.$$

Define the following subgroups

$$\overline{Y} := \left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathrm{GF}(2^\epsilon)\right\}.$$

$$\overline{Z} := \left\{\begin{pmatrix} b & a \\ 0 & b^{-1} \end{pmatrix} \mid a \in \mathrm{GF}(2^\epsilon), b \in \mathrm{GF}(2^\epsilon) - \{0\}\right\}.$$

$$\overline{W} := \left\{\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \mid b \in \mathrm{GF}(2^\epsilon) - \{0\}\right\}.$$

Consider the element

$$i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This element inverts every element of $\overline{W}$ and so $\langle\overline{W}, i\rangle$ is a dihedral group containing $\overline{W}$ at index two.

In the same way as we have seen already $\overline{Z}$ has size $2^\epsilon(2^\epsilon - 1)$ and stabilises the space $\langle(0, 1)\rangle$. A subgroup $\overline{Y}$ has size 2^ϵ and is regular on the remaining points and is elementary abelian. $\overline{W}$ has size $2^\epsilon - 1$, stabilises the two spaces $\langle(0, 1)\rangle$ and $\langle(1, 0)\rangle$ and is isomorphic to the cyclic group $\mathrm{GF}(2^\epsilon)^\times$ and is hence cyclic. Finally $\overline{W}$ acts on $\overline{Y}$ by conjugation and this action is regular and clearly $\overline{Z} = \overline{XW}$.

Since $\mathrm{SL}_2(2^\epsilon)$ (and hence $\mathrm{PSL}_2(2^\epsilon)$) acts faithfully on $2^\epsilon + 1$ points then there is an injective permutation representation

$$\psi \quad : \quad \mathrm{SL}_2(2^\epsilon) \quad \longrightarrow \quad \mathrm{Sym}(2^\epsilon + 1).$$

Let $X = \overline{X}\psi$, $Y = \overline{Y}\psi$, $Z = \overline{Z}\psi$ and $W = \overline{W}\psi$ then by Proposition 5.13 Z is determined inside $\mathrm{Sym}(2^\epsilon + 1)$ up to conjugation.

Conjugating $G \leq \mathrm{Sym}(2^\epsilon + 1)$ appropriately and retaining its name as before we get that G and X share the same subgroup $S^* = Z$

Theorem 10. $G \cong \mathrm{PSL}_2(2^\epsilon)$

Arguing exactly as in Theorem 7, $B = W$ and $N_{\mathrm{Sym}(2^\epsilon+1)}(B) = N_{\mathrm{Sym}(2^\epsilon-1)}(B)\langle\sigma\rangle$ where σ is a transposition which swaps S^* and S^*u. Any dihedral group in $\mathrm{Sym}(2^\epsilon + 1)$ with B at index two which isn't a subgroup of $N_{\mathrm{Sym}(2^\epsilon-1)}(B)$ must swap S^* and S^*u and so must be contained in G. Hence D is unique within $\mathrm{Sym}(2^\epsilon + 1)$. However $\overline{W}$ and hence its representation is contained in such a dihedral group and so these groups must be the same. Hence

$$G = \langle S^*, D\rangle = \langle Z, D\rangle = X$$

(since both S and Z are maximal subgroups). Thus by appropriate representations and conjugations $G \cong \mathrm{PSL}_2(2^\epsilon)$.

5.6 The Theorem

Theorems 7, 8, 9 and 10 provide the main theorem of this chapter. This theorem is taken from the 2001 paper *Counting Involutions* by Aschbacher, Meierfrankenfeld and Stellmacher.

Theorem 11. *Let G be a finite group with $M \leq G$ a TI-subgroup, $M^* := N_G(M) = MC_{M^*}(z)$ for some involution z from M^* and assume also that $C_G(x)$ has odd order for each $x \in M^{\#}$. Suppose further that M is not normal in G and that the number of involutions in G is greater than the index of M in G. Suppose further that M is not normal in G and that the number of involutions in G is greater than the index of M in G. Then one of the following are true.*

- *$G \cong \mathrm{PGL}_2(\mu)$ or $\mathrm{PSL}_2(\mu)$ where $\mu = |M|$ is a power of some prime p and M is an elementary abelian p-group,*

- *$G \cong \mathrm{PSL}_2(2^\epsilon)$ for some integer $\epsilon \geq 2$ and M has order $2^\epsilon + 1$,*

- *$G = RM^*$ for some elementary abelian group of order $2^{2\delta}$ and M^* is dihedral of order $2(2^\delta + 1)$ for some positive integer δ.*

6. CONCLUSION

This project has introduced and applied methods for identifying the isomorphism type of a finite group. We have used results from group theory and studied group actions in order to understand how we can manipulate a group by finding a set for it to act on. We have introduced the concept of a representation of a group so as to further understand how groups can be embedded into symmetric and linear groups. We have seen the relationship between linear representations and actions of a group on an elementary abelian vector space. In particular we have proved Schur's Lemma and used it to prove a result in which two groups acting on an elementary abelian subgroup can, in some circumstances, be proved to be conjugate inside a particular group.

Using these results we set about understanding the coset graph. With particular reference to the graph first introduced in Chapter 1 we studied how groups act on their coset graphs. This theory was used to recognise a periodic group with one conjugacy class of involutions and each involution centralised by a group isomorphic to Dih(8) in two possible ways. In the first case the group turned out to be isomorphic to $\mathrm{PGL}_3(2)$ and we saw this by embedding both groups inside Sym(7). In the second case we proved the group to be isomorphic to Alt(6) and saw that this was so by using the graph to find a subgroup of index six to act faithfully on.

We moved on to study the methods used in *Counting Involutions.* We saw that several cases were possible and considered them separately. In the first case we identified the group to be $\mathrm{PGL}_2(q)$ for some prime power q. This was done by embedding $\mathrm{PGL}_2(q)$ inside of a symmetric group and proving a certain subgroup was uniquely determined up to conjugation. We then proved there was a unique dihedral group which together with the subgroup would generate $\mathrm{PGL}_2(q)$. This proved that inside of the symmetric group any group satisfying the hypothesis was conjugate to $\mathrm{PGL}_2(q)$. This gave us the necessary isomorphism. This technique was used again in slightly different circumstances to prove our arbitrary group was isomorphic to $\mathrm{PSL}_2(2^n)$.

The main theorem of Chapter 4 can be used to prove some exceptional isomorphisms. The groups $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(9)$, $\mathrm{Sp}_4(2)'$ and M_{10}' can be shown to satisfy the hypothesis and so inspection of the group orders confirms

$$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2) \quad \text{and} \quad \mathrm{PSL}_2(9) \cong \mathrm{Sp}_4(2)' \cong M_{10}' \cong \mathrm{Alt}(6).$$

The study of amalgams and the coset graph can also be extended. Further study could include investigating the universal completion which is, in a sense, the largest possible completion of an amalgam. This can be used to prove the theorem of Tutte and Sims.

Theorem (Tutte, Sims)**.** *Let* (G_1, G_2, G_{12}) *be a simple amalgam and* G *a faithful completion. Assume* $|G_1 : G_{12}| = 3$ *and* $|G_2 : G_{12}| = 2$*. Then* $|G_1|$ *divides* $2^4.3$*.*

The main theorem of Chapter 5 is used in *Counting Involutions* to prove the theorem

Theorem. *Let* G *be a finite group containing an involution* z *such that* $T = C_G(z)$ *is dihedral of order eight. Then one of the following hold*

- $G = TO(G)$,
- $G \cong \mathrm{Sym}(4) \cong \mathrm{PGL}_2(3)$,
- $G \cong \mathrm{Sym}(5) \cong \mathrm{PGL}_2(5)$,
- $G \cong \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$,
- $G \cong \mathrm{Alt}(6) \cong \mathrm{PSL}_2(9)$.

Of course the final two possibilities here are the same exceptional isomorphisms that can be proven using the coset graph method and so we have identified two different ways of proving these isomorphisms.

Further study could include Chapter 13 of [9], *Zassenhaus Groups.* Zassenhaus groups are 2-transitive groups in which only the identity fixes three points. The proof of Theorem 8 relies on a theorem of Zassenhaus and a great deal of preparatory theory.

Another interesting area for further study could include a generalisation of an argument that was used in this report. The argument was used to recognise that $\mathrm{PGL}_2(q)$ could be determined up to conjugation in $\mathrm{Sym}(q+1)$ and that $\mathrm{PSL}_2(2^n)$ could be determined up to conjugation in $\mathrm{Sym}(2^n+1)$. Similar arguments were also used to recognise $\mathrm{PSL}_3(2)$ in Chapter 4. The methods used were very similar and a more general result seems plausible. It would also be interesting to generalise the main theorem of Chapter 5 by considering the case when the number of involutions in the group is less than or equal to the index of the particular subgroup.

BIBLIOGRAPHY

[1] Ashbacher, M. *Finite Group Theory.*
Cambridge University Press, 1986.

[2] Aschbacher, M. Meierfrankenfeld, U. Stellmacher, B. Counting Involutions, *Illinois Journal of Mathematics,* **45, 3** (2001), 1051-1060.

[3] Bender, H. Finite Groups with Large Subgroups, *Illinois Journal of Mathematics,* **18** (1974), 223-228.

[4] Cohen, D. *Combinatorial Group Theory: A Topolological Approach.*
Cambridge University Press, 1989.

[5] Cohn, P.M. *Algebra - 2nd Edition - Volume 2.*
John Wiley and Sons, 1989.

[6] Dicks, W. & Dunwoody, M.J. *Groups Acting on Graphs.*
Cambridge University Press, 1989.

[7] Fraleigh, J.B. *A First Course in Abstract Algebra - 6th Edition.*
Addison Wesley Longman, 2000.

[8] Gall, L. *Classical Galois Theory.*
Markham Publishing Company, 1971.

[9] Gorenstein, D. *Finite Groups, 2nd Edition.*
Chelsea Publishing Company, 1980.

[10] Kosniowski, C. *A First Course in Algebraic Topology.*
Cambridge University Press, 1980.

[11] Parker, C. *Rank 2 Amalgams.* Unpublished Udine notes, 2004.

[12] Rose, J.S. *A Course on Group Theory.*

Dover, 1978.

[13] Serre, J.P. *Trees.*

Springer-Verlag, 1980. (Translated by J. Stillwell.)

[14] Solomon, R. A Brief History of the Classification of the Finite Simple Groups, *Bulletin (New Series) of the American Mathematical Society,* **38, 3** (2001), 315-352.

[15] http://www.ams.org/mathscinet