Honors Project: Some Minimal Group Embeddings

by

Acamaro Cutcher

An undergraduate honors project submitted
in partial fulfillment of the requirements for the

Fariborz Maseeh Department of Mathematics and Statistics
Honors Track

Under the supervision of
Prof. Liubomir Chiriac

Portland State University

June 21, 2024

Abstract

This project delves into the concept of minimal embeddings of finite groups, drawing motivation from Cayley's Theorem, which posits that every group of order n can be embedded into S_n, the symmetric group on n symbols. We begin by providing a complete classification of groups with orders up to 15. For each such group G, we identify the smallest m such that S_m contains a subgroup isomorphic to G. Notably, we uncover instances where the value of m is given by the sum of the prime powers present in the prime factorization of $|G|$. It should be emphasized that in general, for an arbitrary finite group, this is very much an open problem. Our investigation is inspired by a paper of Heffernan, MacHale and McCann.

1 Introduction

Classically, a group G can be thought as a collection of permutations: Every element in the group G, can be associated with a permutation of a set. This approach allows us to relate abstract algebraic structures to tangible geometrical objects or combinatorial properties. This is essentially the statement of Cayley's Theorem, a fundamental result in group theory. It asserts that if $|G| = n$, then G is isomorphic to a subgroup of the Symmetric Group S_n.

Heffernan, MacHale and McCann considered in [1] some refinements to Cayley's Theorem, with a particular emphasis on minimal group embeddings. The family of groups considered in the aforementioned paper restricts to those of order 15 or less. The purpose of this project is to explore some of the questions raised there. Our first result gives a classification of such groups.

Theorem 1. *The following table is the complete list of all finite groups of order 15 or less.*

n	*Groups of order n*	n	*Groups of order n*
1	$\mathbb{Z}_1$	*9*	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$
2	$\mathbb{Z}_2$	*10*	$\mathbb{Z}_{10}, D_5$
3	$\mathbb{Z}_3$	*11*	$\mathbb{Z}_{11}$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	*12*	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, D_6, Q_3, A_4$
5	$\mathbb{Z}_5$	*13*	$\mathbb{Z}_{13}$
6	$\mathbb{Z}_6, D_3$	*14*	$\mathbb{Z}_{14}, D_7$
7	$\mathbb{Z}_7$	*15*	$\mathbb{Z}_{15}$
8	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q_2$		

Notation: Cyclic groups are represented by $\mathbb{Z}_n$, where n represents the order of the group. The dihedral group of order $2n$ is denoted by D_n and Q_n is the di-cyclic group of order $4n$. Specifically Q_2 is the Quaternion group and A_4 is the alternating group of S_4.

Once our finite group classification is complete, a natural question that arises is to determine the minimum Symmetric group that contains a given group. More precisely for all G from Theorem 1, find the smallest n, such that G can be embedded in S_n.

Theorem 2. *The following table lists each group of order 15 or less with its smallest Symmetric group in which it can be embedded in.*

Group	Smallest Symmetric Group	Group	Smallest Symmetric Group
$\mathbb{Z}_1$	$\langle e\rangle \leq S_1$	$\mathbb{Z}_{15}$	$\langle(12345)(678)\rangle \leq S_8$
$\mathbb{Z}_2$	$\langle(12)\rangle \leq S_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle(12),(34)\rangle \leq S_4$
$\mathbb{Z}_3$	$\langle(123)\rangle \leq S_3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle(12),(34),(56)\rangle \leq S_6$
$\mathbb{Z}_4$	$\langle(1234)\rangle \leq S_4$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle(12),(3456)\rangle \leq S_6$
$\mathbb{Z}_5$	$\langle(12345)\rangle \leq S_5$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\langle(123),(456)\rangle \leq S_6$
$\mathbb{Z}_6$	$\langle(123)(45)\rangle \leq S_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	$\langle(12),(34),(567)\rangle \leq S_7$
$\mathbb{Z}_7$	$\langle(123\ldots67)\rangle \leq S_7$	D_3	$\langle(123),(12)\rangle \leq S_3$
$\mathbb{Z}_8$	$\langle(123\ldots78)\rangle \leq S_8$	D_4	$\langle(1234),(12)(34)\rangle \leq S_4$
$\mathbb{Z}_9$	$\langle(123\ldots89)\rangle \leq S_9$	D_5	$\langle(12345),(14)(32)\rangle \leq S_5$
$\mathbb{Z}_{10}$	$\langle(12345)(67)\rangle \leq S_7$	D_6	$\langle(123),(12),(45)\rangle \leq S_5$
$\mathbb{Z}_{11}$	$\langle(123\ldots10\,11)\rangle \leq S_{11}$	D_7	$\langle(1234567),(27)(36)(45)\rangle \leq S_7$
$\mathbb{Z}_{12}$	$\langle(1234)(567)\rangle \leq S_7$	A_4	$\langle(123),(12)(34)\rangle \leq S_4$
$\mathbb{Z}_{13}$	$\langle(123\ldots12\,13)\rangle \leq S_{13}$	Q_2	$\langle(1234)(5678),(1638)(2547)\rangle \leq S_8$
$\mathbb{Z}_{14}$	$\langle(1234567)(89)\rangle \leq S_9$	Q_3	$\langle(123),(12)(4567)\rangle \leq S_7$

This seemly mundane question of minimal group embeddings has led us to interesting results. The most intriguing one is that Q_2, the quaternion group has as its minimal embedding S_8, where as the larger di-cyclic group of 12 elements, Q_3, has as its minimal embedding S_7.

We have not ventured beyond groups of order 15 given the extended complexity to classify all groups of order 16 which contain 14 non-isomorphic groups. Furthermore, the number of groups of order 2^k grow with increasing magnitude as stated in [1], which is shown below:

n	Number of groups	n	Number of groups
16	14	256	56,092
32	51	512	10,494,213
64	267	1,024	49,487,365,422
128	2,328		

The classification of finite groups of order n, was stated by Cayley as the "general problem" in Group Theory. His thoughts led him to classify all groups of order 12 or less in 1889 [1]. An effort that has led to the "Jordan-Hölder Program" which sought to classify all finite simple groups which form the "building blocks" for any finite group. Moreover, Cayley's initial ideas have grown to inspire modern programming languages in computational discrete algebra specifically for computational group theory know as "Groups, Algorithms, Programming" (GAP), as well as modern repository known as the Small Groups Library in GAP.

Even with the enormous computational power we have in our present day and powerful computer algebra systems, finding groups of a given order n is still out of reach. Even when n is relatively small if it has many non coprime factors the problem remains difficult.

2 Background

We prove two basic facts in Group Theory. The first is a general method to compute the size of the set HK, where H and K are subgroups of a finite group. In the second part we prove that a group is isomorphic to the direct product of two of its subgroups given certain constraints. These facts together with the Sylow Theorems and the Fundamental Theorem of Finite Groups will aid us in proving Theorem 1.

Proposition 1. *If H and K are subgroups of a finite group G, then*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof. Recall that the set $HK = \{\ hk \mid h \in H,\ k \in K\ \}$ is usually not a subgroup of G.

Define an action of the group $H \times K$ on the set HK as follows:

$$(h, k) \cdot y = hyk^{-1}$$

for all $(h, k) \in H \times K$ and $y \in HK$.

We now verify that this is certainly a group action.

First, it is clear that

$$(e, e) \cdot y = eye^{-1} = y$$

Moreover,

$$\begin{aligned}(h_1, k_1) \cdot ((h_2, k_2) \cdot y) &= (h_1, k_1) \cdot (h_2 y k_2^{-1}) \\ &= h_1(h_2 y k_2^{-1})k_1^{-1} \\ &= (h_1 h_2) y (k_1 k_2)^{-1} \\ &= (h_1 h_2, k_1 k_2) \cdot y\end{aligned}$$

Thus, this is a valid group action.

The group action is in fact transitive. See that the identity element is part of the set HK, since $e = e \cdot e \in HK$, then any element $hk \in HK$ can be reached by the group action $(h, k^{-1}) \cdot e = hk$. Now by the Orbit-Stabilizer Theorem we obtain the following result:

$$|HK| = \frac{|H \times K|}{|\mathrm{Stab}(e)|} = \frac{|H| \cdot |K|}{|\mathrm{Stab}(e)|}$$

It remains to show that $|\mathrm{Stab}(e)| = |H \cap K|, tothatendconsider$:

$$\begin{aligned}\mathrm{Stab}(e) &= \{(h, k) \in H \times K \mid (h, k) \cdot e = e\} \\ &= \{(h, k) \in H \times K \mid hk^{-1} = e\} \\ &= \{(h, k) \in H \times K \mid h = k\},\end{aligned}$$

This leads us to conclude that:

$$\mathrm{Stab}(e) = \{(h, h) \in H \times K \mid h \in H \cap K\}.$$

So we obtain that $|\mathrm{Stab}(e)| = |H \cap K|$. Therefore, $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$. □

Proposition 2. *Suppose A and B are subgroups of G such that*

(i) $A \triangleleft G$ *and* $B \triangleleft G$;

(ii) $AB = G$;

(iii) $A \cap B = \{e\}$.

Then $G \cong A \times B$.

Proof. We first observe that (i), (ii), (iii) imply two more properties:

(iv) If $ab = a_1b_1$ with $a, a_1 \in A$ and $b, b_1 \in B$, then $a = a_1$ and $b = b_1$.

(v) If $a \in A$ and $b \in B$, then $ab = ba$.

To prove (iv), note that $ab = a_1b_1$ implies $a_1^{-1}a = b_1b^{-1}$. Since $a_1^{-1}a \in A \cap B$, $b_1b^{-1} \in A \cap B$, and $A \cap B = \{e\}$, it follows that $a_1^{-1}a = b_1b^{-1} = e$, so $a = a_1$ and $b = b_1$.

To prove (v), we will show that $bab^{-1}a^{-1} \in A \cap B$.

Since $a \in A$ and $A \triangleleft G$:

$$bab^{-1}a^{-1} = (bab^{-1})a^{-1} \in A.$$

Similarly, since $b^{-1} \in B$ and $B \triangleleft G$:

$$bab^{-1}a^{-1} = b(ab^{-1}a^{-1}) \in B.$$

This shows that $bab^{-1}a^{-1} \in A \cap B = \{e\}$. Hence $bab^{-1}a^{-1} = e$, and so $ab = ba$.

We will use these two properties to prove Proposition 2.

Now define $f : A \times B \to G$ by $f((a, b)) = ab$. Then f is onto (surjective) by (ii). Furthermore, f is injective because if $f((a, b)) = f((a_1, b_1))$, then $ab = a_1b_1$ so by (iv) $a = a_1$ and $b = b_1$.

Finally, f is an homomorphism since:

$$\begin{aligned} f((a_1, b_1)(a_2, b_2)) = f((a_1a_2, b_1b_2)) &= a_1a_2b_1b_2 \\ &= a_1b_1a_2b_2, \text{ by (v)} \\ &= f((a_1, b_1))f((a_2, b_2)). \end{aligned}$$

In conclusion, f is a isomorphism, i.e., $G \cong A \times B$.

□

We state, without proof, the following well known theorems is Group Theory which will be utilized in subsequent proofs.

Theorem 3 (Fundamental Theorem of Finite Abelian Groups)**.**
Let G *be a finite abelian group such that* $|G| = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots p_r^{e_r}$. *Then*

$$G \cong \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}$$

where each p_i *is a prime number not necessarily distinct and* e_i *is an integer.*

Theorem 4 (Sylow I)**.** *Given* G *such that*

$$|G| = n = p^r \cdot m$$

where p^r *is the largest power of* p, *i.e.* $\gcd(p^r, m) = 1$, *then there exists a subgroup* $H \leq G$ *such that*

$$|H| = p^r$$

Definition 1 (Sylow $p-$subgroup)**.** *Let G be a group whose $|G| = n = p^r m$ where $\gcd(p^r, m) = 1$. Then a subgroup $H \leq G$, whose $|H| = p^r$ is called a Sylow $p-$subgroup.*

Theorem 5 (Sylow II)**.**
a) *Given $H \leq G$, if H is a Sylow p-subgroup, then any other Sylow p-subgroup $H' \leq G$ is conjugate to H, i.e., there exists $g \in G$ such that*

$$gHg^{-1} = H'.$$

Remark 3. *As a consequence of Theorem 5, if there exist a unique Sylow $p-$subgroup, call it H, then it is normal, i.e., for all $g \in G$,*

$$gHg^{-1} = H.$$

Theorem 6 (Sylow III)**.** *Let G be a group such that $|G| = p^r \cdot m$. Then the number of Sylow $p-$subgroups of G divides m and is congruent to 1 modulo p.*

3 Proof of Theorem 1, Part I

We give a partial proof of Theorem 1. More precisely, we classify all groups of order 15 or less, except groups of order 8 and 12. We address these two cases in the following sections.

To begin it is clear that the classification of abelian groups of any given order is a straight forward task while applying the Fundamental Theorem of Finite Abelian Groups. Our challenge begins by proving that groups of certain order disallow non-abelian groups, then we can easily apply the aforementioned theorem to classify all possible groups of that order. The orders which do have non-abelian groups can then be classified using the properties of normal subgroups or the Sylow Theorems.

Remark 4. *It is well known that all groups of prime order are isomorphic to a cyclic group.*

Proposition 5. *Groups of order p^2, with p-prime, are abelian.*

Proof.

Let G be a group of order p^2, where p is a prime number and let $Z(G)$ be the center of G. Recall that the center of G is the set of elements in G that commute with every element of G. It can be verified that $Z(G)$ is a normal subgroup of G.

By Lagrange's Theorem the order $Z(G)$ divides the order of G, which implies that $|Z(G)| = 1$, p or p^2. We will use without proof the well known fact that the center of a prime power ordered group is non-trivial. This leaves us with two option, either the order of $|Z(G)| = p$ or p^2.

If the later case is true then we are done. This owes to the fact that the $|Z(G)| = |G|$, which would imply that $Z(G) = G$ and therefore proving that G is abelian.

On the other hand, suppose that $|Z(G)| = p$, then it's corresponding quotient group $G/Z(G)$ is cyclic group of order p. Then by definition:

$$\exists \tau \in G/Z(G) \quad : \quad G/Z(G) = \langle \tau \rangle$$

Since τ is a coset by $Z(G)$:

$$\exists t \in G \quad : \quad \tau = tZ(G)$$

Thus each coset of $Z(G)$ in G is equal to $(tZ(G))^i = t^i Z(G)$ for some positive integer i.

Fix a $x, y \in G$, then for some positive integer m, n

$$x \in t^m Z(G), \quad y \in t^n Z(G)$$

Then $x = t^m z_1, y = t^n z_2$ for some $z_1, z_2 \in Z(G)$.

Now we can show that x and y do in fact commute. This owes to the fact that the elements in the center commute with all elements in the group and that the exponents with the same base commute.

$$\begin{aligned} xy = (t^m z_1)(t^n z_2) = t^m(z_1 t^n)z_2 = t^m(t^n z_1)z_2 = (t^m t^n)(z_1 z_2) = (t^{m+n})(z_2 z_1) = (t^{n+m})(z_2 z_1) \\ = (t^n t^m)(z_2 z_1) = t^n(t^m z_2)z_1 = t^n(z_2 t^m)z_1 = (t^n z_2)(t^m z_1) = yx \end{aligned}$$

This applies for all $x, y \in G$, thereby proving that G is abelian. Moreover, this fact contradicts our assumption that $|Z(G)| = p$, therefore we have that $Z(G) = G$.

□

Proposition 6. *Assume $|G| = pq$ where p and q are primes, $p < q$, and $p \nmid (q-1)$. Then G is a cyclic group, i.e., $G \cong \mathbb{Z}_{pq}$.*

Proof.

By Cauchy's Theorem know that there are elements in G, called them x and y such that $|x| = p$ and $|y| = q$. If we consider the order of the element xy, it will be the least common multiple of p and q, given that they are both prime, then $|xy| = pq$. Therefore G is a cyclic group isomorphic to $\mathbb{Z}_{pq}$.

□

Proposition 7. *Let G be a group of order $2p$, where $p \geq 3$ is an odd prime. Then G is either cyclic or dihedral.*

Proof.

Let G be a group of order $2p$, where p is a prime number. Then the order of an element $x \in G$ must divide $|G| = 2p$. For that reason the order of x can only be $1, 2, p$ or $2p$. We know by Cauchy's Theorem that there exist an element, α and $\beta \in G$, such that the order of α and β is 2 and p respectively.

Now let $A = \langle \alpha \rangle$ and $B = \langle \beta \rangle$.

Furthermore, owing to the fact that the index of B is 2, we have that $B \triangleleft G$, hence $\forall \gamma \in G$ $\gamma B \gamma^{-1} = B$. With this in mind, consider conjugation by $\alpha \in A$ on $\beta \in B$:

$$\alpha\beta\alpha^{-1} \in \{e, \beta, \beta^2, \ldots, \beta^{p-1}\}$$

It is clear that $\alpha\beta\alpha^{-1} \neq e$ as otherwise this would lead to the conclusion that $\beta = e$, for that reason we are left with the following options, namely that $\alpha\beta\alpha^{-1} = \beta^k$, where $k \in \{1, 2, \ldots, p-1\}$.

With this in mind, now consider consider conjugation by α on β^k.

$$\alpha\beta^k\alpha^{-1} = \beta^{k^2}$$

See that this is the same as double conjugation by α on β.

$$\alpha^2\beta\alpha^{-2} = \alpha\beta^k\alpha^{-1} = \beta^{k^2}$$

given that the order of α is 2, we can conclude that $\beta = \beta^{k^2}$, which in turn implies that $\beta^{k^2-1} = e$.

Now, given that the order of β is p, we require that:

$$p | k^2 - 1$$

Henceforth it can be shown that k can only be 1 or $p-1$.

In the first case see that if $k=1$, we can conclude that $\alpha\beta = \beta\alpha$. So the order of $\alpha\beta$ is the least common multiple of 2 and p which is $2p$. Therefore, there does exist a element in G which has order 2p, allowing us to conclude that $G \cong \mathbb{Z}_{2p}$.

In the second case, assume that $k = p-1$.

With that in mind, consider the group formed by multiplying A with B, where multiplication between elements in A and B are define by the relation $\alpha\beta = \beta^{p-1}\alpha$.

The order of AB is given by the identity in Proposition 2, namely:

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Owing to the fact that A and B are cyclic groups of different order, they have trivial intersection. Therefore $|AB| = 2p$. For that reason we are left to conclude that $G \cong AB$, i.e.

$$G \cong \langle \alpha, \beta \mid \alpha^2 = e, \beta^p = e, \alpha\beta\alpha^{-1} = \beta^{-1} \rangle.$$

Given that this is the exact group definition of a dihedral group, we can conclude that $G \cong D_p$. By this method of exhaustion, we have shown that G is either isomorphic to a cyclic group or a dihedral group.

□

Remark 8.

1. *Groups of order 6 are isomorphic to $\mathbb{Z}_6$ or D_3 by Proposition 7.*
2. *Groups of order 10 are isomorphic to $\mathbb{Z}_{10}$ or D_5 by Proposition 7.*
3. *Groups of order 14 are isomorphic to $\mathbb{Z}_{14}$ or D_7 by Proposition 7.*

Remark 9.

We classify all abelian groups of order p, p^2 or pq, where p and q are prime numbers, using the Fundamental Theorem of Finite Abelian Groups. Moreover, by Remark 4 and Proposition 5 and 6 we are guaranteed that groups of order p, p^2 and pq have no non-abelian groups.

1. *Groups of order 2 are $\mathbb{Z}_2$.*
2. *Groups of order 3 are $\mathbb{Z}_3$.*
3. *Groups of order 4 are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.*
4. *Groups of order 5 are $\mathbb{Z}_5$.*
5. *Groups of order 7 are $\mathbb{Z}_7$.*
6. *Groups of order 9 are $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.*
7. *Groups of order 11 are $\mathbb{Z}_{11}$.*
8. *Groups of order 13 are $\mathbb{Z}_{13}$.*
9. *Groups of order 15 are $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$.*

4 Proof of Theorem 1, Part II

We continue the proof of Theorem 1 by proving the groups of order 8.

Proposition 10. *There are five non-isomorphic groups of order 8. The abelians ones are* $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. *The non-abelian groups are the Dihedral group* D_4 *and the Quaternion group* Q_2.

Proof.

If G is an abelian group of order 8, the fundamental theorem of Finite Abelian Groups (Theorem 3) implies that G isomorphic to either $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore we may assume for the rest of the proof that G is a non-abelian group of order 8.

First, we claim that G has an element of order 4. Indeed, the order of every element in G divides 8, so it either 1, 2, 4, 8. Given that G is a non-abelian group, it contains no elements of order 8. Moreover if every non-identity element had order 2, then for every $a, b \in G$ we'd have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, so G would be abelian. It follows that there exists a non-identity element of order different from 2, and the only such possible is 4.

Let x be an element of order 4 in G, and H be the cyclic group generated by x. Since H has index 2 in G, then it's a normal subgroup of G.

Let $y \in G \setminus H$. Considering that H is normal, we have

$$yHy^{-1} = H$$

and, in particular, $yxy^{-1} \in H$.

We now distinguish the following four cases.

(1) Assume $yxy^{-1} = e$. This forces $yx = y$, and so $x = e$, which is a contradiction. Hence $yxy^{-1} \neq e$.

(2) Assume $yxy^{-1} = x$. Then $yx = xy$.

This implies that any power of x and y commute, i.e. $x^m y^n = y^n x^m$.

Recall that the index of H is 2, so the group G can be expressed as the following union $G = H \cup yH$. Then every element in G can be express in the form $y^n x^m$ for some $n \in \mathbb{Z}_2$ and $m \in \mathbb{Z}_4$.

Let $a, b \in G$, then $a = y^{n_1}x^{m_1}$ and $b = y^{n_2}x^{m_2}$. Then multiplication of ab results in:

$$ab = y^{n_1}x^{m_1}y^{n_2}x^{m_2} = y^{n_1}(y^{n_2}x^{m_1})x^{m_2} = (y^{n_2}y^{n_1})(x^{m_2}x^{m_1}) = (y^{n_2}x^{m_2})(y^{n_1}x^{m_1}) = ba$$

So we see that our assumption leads us to conclude that G is an abelian group which is a contradiction. Therefore $yxy^{-1} \neq x$.

(3) Assume $yxy^{-1} = x^2$. Given that the order of an element does not change under conjugation we get that the order of $yxy^{-1}$is equal to the order of x, i.e., $|yxy^{-1}| = |x| = 4$. However $|x^2| = 2$, which proves that $yxy^{-1} \neq x^2$.

(4) Assume $yxy^{-1} = x^3 = x^{-1}$.

Then conjugation by y on x, results in

$$yxy^{-1} = x^{-1}.$$

(a) Consider the case where $|y| = 2$. We wish to show that G is isomorphic to D_4, where:

$$D_4 = \langle r, s \mid r^4 = f^2 = e, fr = r^{-1}f \rangle.$$

We are going to define the mapping $\phi : G \to D_4$ as follows:

$$\phi(e) = e,\ \phi(x) = r,\ \phi(x^2) = r^2,\ \phi(x^3) = r^3$$
$$\phi(y) = f,\ \phi(yx) = fr,\ \phi(yx^2) = fr^2,\ \phi(yx^3) = fr^3$$

Given that G and D_4 have the same order, ϕ is a bijection. As well, given any elements in G, say $a = y^{n_1}x^{m_1}$ and $b = y^{n_2}x^{m_2}$, it is clear that:

$$\begin{aligned}
\phi(ab) &= \phi(y^{n_1}x^{m_1}y^{n_2}x^{m_2}) \\
&= \phi(y^{n_1}y^{n_2}x^{-m_1}x^{m_2}) \\
&= \phi(y^{n_1+n_2}x^{-m_1+m_2}) \\
&= f^{n_1+n_2}r^{-m_1+m_2} \\
&= f^{n_1}f^{n_2}r^{-m_1}r^{m_2} \\
&= f^{n_1}r^{m_1}f^{n_2}r^{m_2} \\
&= \phi(y^{n_1}x^{m_1})\phi(y^{n_2}x^{m_2}) \\
&= \phi(a)\phi(b)
\end{aligned}$$

This shows that ϕ is isomorphism. Therefore $G \cong D_4$.

(b) Consider the case where $|y| = 4$.

We recall that the Quaternion group, denoted by Q_2, consist of the elements $\{\pm 1, \pm i, \pm j, \pm k\}$ subject to the relation $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, see that in particular the Quaternion group can be expressed more abstractly as:

$$Q_2 = \langle i, j \mid i^4 = 1,\ i^2 = j^2 = -1,\ jij^{-1} = i^{-1} \rangle$$

Given the relation $i^2 = j^2$, we wish to prove that $y^2 = x^2$. To this end consider that $G = H \cup yH$, then $y^2 \in H \cup yH$. Since $yH \neq H$, then $y^2H \neq yH$, so our only option is for $y^2H = H$, which implies that $y^2 \in H$. See that the order of y^2 is two, then our only option is for $y^2 = x^2$. Now define the mapping $\gamma : G \to Q_2$ as follows:

$$\gamma(e) = 1,\ \ \gamma(x) = i,\ \ \gamma(x^2) = -1,\ \ \gamma(x^3) = -i$$
$$\gamma(y) = j,\ \ \gamma(y\ x) = j\ i = -k,\ \ \gamma(y\ x^2) = j\ i^2 = -j,\ \ \gamma(y\ x^3) = j\ i^3 = k$$

Similarly as before given that G and Q_2 have the same order, and it is clear γ is a bijection. Moreover, in the same manner as discussed above for all a and b in G we can show that $\gamma(ab) = \gamma(a)\gamma(b)$. We have that γ is an isomorphism, therefore $G \cong Q_2$.

In conclusion, the only non abelian groups of order 8 are D_4 and Q_2

□

5 Proof of Theorem 1, Part III

In this section we wish to demonstrate that there are only 5 possible group structures of order 12, namely the abelian groups $\mathbb{Z}_4 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ and non-abelian groups D_6, A_4, Q_3.

Lemma 11. *Any Group of order 12 has at least one normal subgroup.*

Proof.

Let G be a group of order 12. The third Sylow theorem indicates that the possible number of Sylow 3-subgroups is 1 and 4 and the possible number of Sylow 2-subgroups is 1 and 3. In such a case where we have a unique Sylow p-subgroup be it 2 or 3, then it is guaranteed to be a normal subgroup.

Moreover, if we assume that there can exist 3 Sylow 2-subgroups and 4 Sylow 3-subgroup, then the size of the group must have 18 elements given difference in group structure, all these subgroups would only intersect at the identity element. Hence there must at least exist one unique Sylow p-subgroup which will a normal subgroup to G.

□

Note that this fact can also be seen when taking into account Figure 1 and Figure 2.

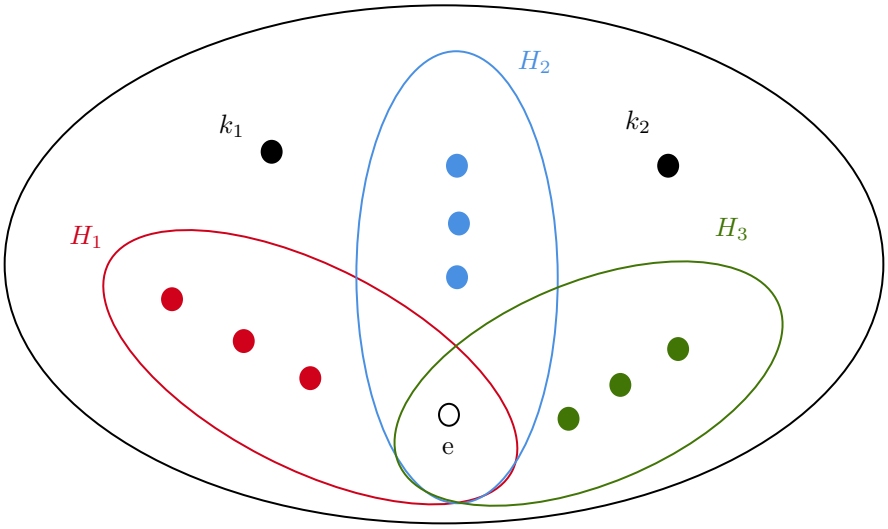

Figure 1: Consider the group of order 12 with $n_2 = 3$, which are the groups H_1, H_2, H_3 of order 4. We are left with two elements which means that we can only build a unique Sylow 3-subgroup comprising the element $\{e, k_1, k_2\}$.

Theorem 7. *There are two abelian groups of order 12 namely $\mathbb{Z}_4 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.*

Proof.

Let G be a group of order 12, such that $n_3 = 1$ and $n_2 = 1$, where n_p represent the number of Sylow p-subgroups. Then we have a unique Sylow 3-subgroup call it K and a unique Sylow 2-subgroup label it as H. Then K and H are normal subgroups of G.

Since the group structures of K and H are different it can only be the case that $H \cap K = \{e\}$.

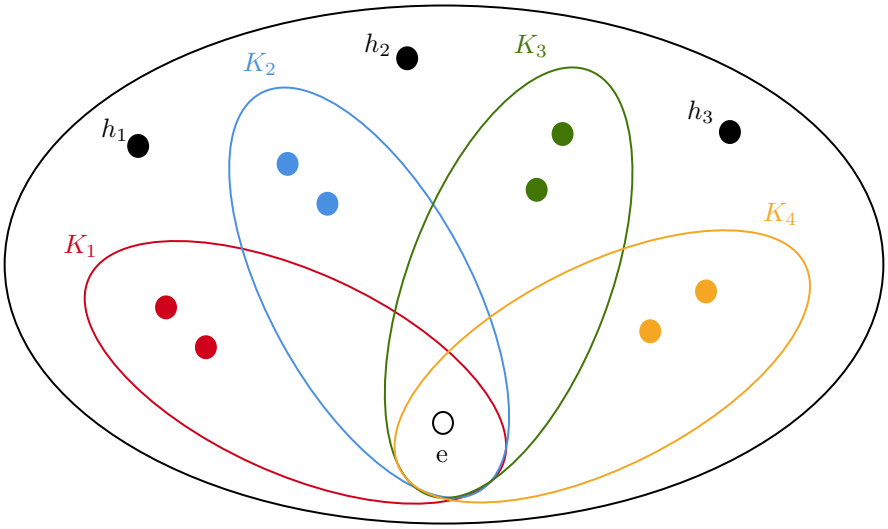

Figure 2: Consider the Group of order 12 with $n_3 = 4$, which are the the groups K_1, K_2, K_3, K_4, then we are left with the elements h_1, h_2, h_3 from which we can only build a unique Sylow-2 group comprising the element $\{e, h_1, h_2, h_3\}$

Moreover, consider the group HK and pick two element in this group, h_1k_1 and h_2k_2, then if $h_1k_1 = h_2k_2$, we get that $h_2^{-1}h_1 = k_2k_1^{-1}$, since $H \cap K = \{e\}$. We have that $h_1 = h_2$ and $k_1 = k_2$. So, every $hk \in HK$ is distinct so the order of HK is 12. Owing to the fact that $|G| = 12$, we have that $G = HK$. Hence, we can conclude by Proposition 2 that $G \cong H \times K$, i.e., $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

□

Theorem 8. *If G is a non abelian group of order 12 and has a unique Sylow 2-subgroup, then G is isomorphic to A_4.*

Proof.

Let H be the unique Sylow 2-subgroup of G. Since H has order 4 then $H \cong \mathbb{Z}_4$ or $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. As discussed above H is a normal subgroup of G.

Moreover, owing to the fact that G is non abelian and has a unique Sylow 2-subgroup by the Sylow Theorems this would imply that there exist 3 Sylow 3-subgroups. Owing to the fact that G is a non-abelian group, there can not exists another Sylow 3-subgroup otherwise it would force G to be abelian.

With that in mind, let $x \in G \setminus H$, then x is a generator of a Sylow 3-subgroup which we denote as K. Consider the group HK, by (Theorem 1) the order of this group is:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{4 \cdot 3}{1} = 12$$

Therefore $G \cong HK$. So we are left to show exactly to what group is H isomorphic to. To this end, recall that H is a unique Sylow 2-subgroup, so $H \triangleleft G$. Thus, conjugation by x on the subgroup H gives us:

$$xHx^{-1} = H$$

This implies that for some $y, y_1 \in H$ we have that $xyx^{-1} = y_1$.

First assume that $H \cong \mathbb{Z}_4$, therefore H is generated by some element called it y. We have that $H = \langle y \rangle = \{e, y, y^2, y^3\}$. We'll show that this leads to a contradiction

(1) Assume that $y_1 = e$, then:

$$xyx^{-1} = e$$
$$y = x^{-1}x = e$$

which is a contradiction, since y is the generator of the subgroup H.

(2) Assume that $y_1 = y$, then:

$$xyx^{-1} = y$$
$$xy = yx$$

This result contradicts our assumption that G is non-abelian. To see this consider any two elements say h_1k_1 and h_2k_2 in HK.

It is clear that for some $n_1, n_2 \in \{0, 1, 2, 3\}$ and $m_1, m_2 \in \{0, 1, 2\}$ we can express:

$$h_1k_1 = y^{n_1}x^{m_1}$$
$$h_2k_2 = y^{n_2}x^{m_2}$$

Then we have:

$$\begin{aligned} h_1k_1h_2k_2 &= y^{n_1}x^{m_1}y^{n_2}x^{m_2} \\ &= y^{n_1}(y^{n_2}x^{m_1})x^{m_2} \\ &= (y^{n_2}y^{n_1})(x^{m_2}x^{m_1}) \\ &= (y^{n_2}x^{m_2})(y^{n_1}x^{m_1}) \\ &= h_2k_2h_1k_1 \end{aligned}$$

(3) Assume that $y_1 = y^2$, then:

$$xyx^{-1} = y^2$$

This equality is a contradiction. The order of the element xyx^{-1} is 4 nonetheless the order of y^2 is only 2. So this relation can not hold true.

(4) Assume that $y_1 = y^3$.

$$xyx^{-1} = y^3$$
$$xy = y^3x$$

Now we check if this relation generates any contradictions, first consider $(xy)^2$.

$$(xy)^2 = (xy)(xy) = (y^3x)(xy) = y^3x^2y$$

and

$$(xy)^2 = (xy)(xy) = (xy)(y^3x) = x^2$$

Lastly we check $(xy)^3$:

$$(xy)^3 = (xy)(xy)^2 = (xy)(y^3x^2y) = y$$

However it is also the case that:

$$(xy)^3 = (xy)(xy)^2 = (xy)(x^2) = (y^3x)(x^2) = y^3$$

Therefore from our initial assumption $xy = y^3x$, we can conclude that $y = y^3$, which is a contradiction.

Given that we have exhausted all possible elements for which y_1 can be, our assumption that $H \cong \mathbb{Z}_4$ is not true.

By exclusion $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $H = \{e, a, b, ab\}$, where $a^2 = b^2 = (ab)^2 = e$. We are left to find what conjugation by x is valid:

(1) Assume that conjugation by x fixes all element in H. Then

$$\begin{aligned} xax^{-1} &= a \\ xbx^{-1} &= b \\ x(ab)x^{-1} &= ab \end{aligned}$$

We have that

$$xa = ax,\ xb = bx,\ x(ab) = (ab)x$$

Note that the following is also true

$$x^2a = ax^2,\ x^2b = bx^2,\ x^2(ab) = (ab)x^2$$

Therefore every element of the group H commutes with every element in the group K.

Moreover if we consider the elements $h_1k_1, h_2, k_2 \in HK = G$ then $h_1, h_2 \in \{e, a, b, ab\}$ and $k_1, k_2 \in \{e, x, x^2\}$.

Owing to the fact that every element in H commutes with ever element in K:

$$(h_1k_1)(h_2k_2) = h_1(h_2k_1)k_2 = (h_2h_1)(k_2k_1) = h_2(k_2h_1)k_1 = (h_2k_2)(h_1k_1)$$

This implies that the group G is abelian which is a contradiction, since we assumed that G is non abelian. Therefore our assumption that composition by x fixes every element is erroneous.

(2) Assume that composition by x fixes only one element in H. With out lost of generality assume that:

$$xax^{-1} = b,\ xbx^{-1} = a,\ x(ab)x^{-1} = ab$$

Consider double conjugation by on the element b, this gives us:

$$x^2bx^{-2} = x(xbx^{-1})x^{-1} = xax^{-1} = b$$

Given that $x^2 = x^{-1}$ and $x^{-2} = x$ we can write:

$$x^2bx^{-2} \ = \ x^{-1}bx \ = \ b$$

which in turn gives us:

$$xbx^{-1} \ = \ b$$

This is however a contradiction since we assumed that $xbx^{-1} = a$. The same reasoning follows if we decide to fix different element in H other than ab.

Therefore our assumption that composition by x fixes one element is false.

(3) Last we are left to consider that composition by x permutes every element a, b, ab in H.

$$xax^{-1} = b,\ xbx^{-1} = ab \tag{1}$$

To this end consider the Alternating Group of four elements.

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (134), (143), (124), (142), (234), (243)\}$$

We define a mapping $f : G \to A_4$ as follows:

$$\begin{aligned} f(a) &= (1\,2)(3\,4) \\ f(b) &= (1\,4)(2\,3) \\ f(x) &= (1\,2\,3) \end{aligned}$$

We claim that this is a isomorphism from G to A_4.

The following elements $\{e, (12)(34), (13)(24), (14)(23)\}$ from A_4 form the klein-four group, the which is easily seen from the table below. This subgroup we will denote as $\bar{H}$.

	e	$(12)(34)$	$(13)(24)$	$(14)(23)$
e	e	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	e	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	e	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	e

Similarly the multiplication table of the subgroup H of G is:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

It is clear that f defines a isomorphism between the group $\bar{H}$ and H.

Moreover, if we let $\bar{K} = \langle(123)\rangle$, then clearly by it's multiplication table below, it constitutes a subgroup of A_4.

	e	(123)	(132)
e	e	(123)	(132)
(123)	(123)	(132)	e
(132)	(132)	e	(123)

If we compare this multiplication table of K:

	e	x	x^2
e	e	x	x^2
x	x	x^2	e
x^2	x^2	e	x

It is clear that f is an isomorphism between $\bar{K}$ and K.

Now, if we consider the group $\bar{H}\bar{K}$, owing to the fact that each element in $\bar{H}$ has order 2 and $\bar{K}$ has order 3, except for the identity, their intersection can only be the identity. Therefore the size this group is

$$|\bar{H}\bar{K}| = \frac{|\bar{H}|\,|\bar{K}|}{|\bar{H} \cap \bar{K}|} = \frac{4 \cdot 3}{1} = 12$$

This directly implies that $\bar{H}\bar{K} = A_4$.

Since it is the case that $H \cong \bar{H}$ and $K \cong \bar{K}$, to be able to state that the function f is an isomorphism between HK and $\bar{H}\bar{K}$ we need our function to have the following conditions:

$$f(x)f(a)f(x^{-1}) = f(b),\ f(x)f(b)f(x^{-2}) = f(ab)$$

By simple calculation we get

$$f(x)f(a)f(x^{-1}) = (123)(12)(34)(132) = (14)(23) = f(b)$$

$$f(x)f(b)f(x^{-1}) = (123)(14)(23)(132) = (13)(24) = (12)(34)(14)(23) = f(ab)$$

Therefore if we consider the multiplication table for HK and $\bar{H}\bar{K}$, the function f is an isomorphism.

Therefore, If G is a non abelian group of order 12 and has a unique Sylow 2-subgroup. Then G is isomorphic to A_4.

□

Theorem 9. *If G is a non-abelian group of order 12 and has a unique Sylow 3-subgroup. Then G is isomorphic to either D_6 or Q_3.*

Proof.

Let K be the unique Sylow 3-subgroup of G. Then $K = \langle x\rangle$ and is normal subgroup of G. As stated before if there is a unique Sylow 3-subgroup then there exists 3 Sylow 2-subgroups of G, as shown in Figure 1.

By the Second Sylow Theorem, Theorem 5, we know that all Sylow 2-subgroups are conjugate to each other. Therefore, all 3 subgroups must have the same group structure. Given that these Sylow 2-subgroups contain only four elements, these 3 Sylow 2-subgroups are either isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Case I. Consider the case where all Sylow 2-subgroups are isomorphic to $\mathbb{Z}_4$. Let H be a Sylow 2-subgroup, then it is generated by some element call it $y \in G$.

Now if we consider the group KH, given that H and K have different group structure then these two groups only intersect at the identity. So the order of the group HK is:

$$|KH| = \frac{|K|\ |H|}{|K \cap H|} = \frac{3 \cdot 4}{1} = 12.$$

Thus $G = KH$. Lastly we are left to understand the underlying group operation between elements of H and K. To such an end, note that K is a normal group of G, hence conjugation $y \in H$ does not alter the group, i.e.,

$$yKy^{-1} = K$$

So, $yxy^{-1} \in K$ where $K = \langle x \rangle$. We are left to check to what element in K does yxy^{-1} yield a valid relationship.

To such an end:

1. Consider the case were $yxy^{-1} = e$. Then $x = y^{-1}y = e$, which is a contradiction. Therefore an invalid relation.

2. Consider the case were $yxy^{-1} = x$. Then $xy = yx$, or more generally for any power $x^n y^m = y^m x^n$. Then given any two element in KH of the form $y^{n_1}x^{m_1}$ and $y^{n_2}x^{m_2}$ where $n_1, n_2 \in \mathbb{Z}_4$ and $m_1, m_2 \in \mathbb{Z}_3$. Then we can show that these two elements commute as show below:

   $$y^{n_1}x^{m_1}y^{n_2}x^{m_2} = y^{n_1}(y^{n_2}x^{m_1})x^{m_2} = (y^{n_2}y^{n_1})(x^{m_2}x^{m_1}) = y^{n_2}x^{m_2}y^{n_1}x^{m_1}.$$

   Therefore, this relation would imply that G is in fact abelian. This however contradicts our initial assumption that G is non-abelian.

3. Consider the case were $yxy^{-1} = x^2$.

   To this end note the Dicylic group of order 12, Q_3:

   $$Q_3 = \{a, b \mid a^6 = 1, a^3 = b^2, bab^{-1}a = e\}$$

   and the elements in the group KH:

   $$KH = \{e, x, x^2, y, y^2, y^3, xy, xy^2, xy^3, x^2y, x^2y^2, x^2y^3\}$$

   Given the relation $yxy^{-1} = x^2$ of which can be also written as $yx = x^2y$, we wish show that Q_3 is isomorphic to KH. First we can calculate the order of elements in KH, for example the element xy^2.

   To start consider $(xy^2)^2$:

   $$\begin{aligned}(xy^2)(xy^2) = (xy)(yx)(y^2) = (xy)(x^2y)(y^2) = x(yx)(xy^3) \\ = x(x^2y)(xy^3) = x^3(yx)(y^3) = x^3(x^2y)y^3 = x^2\end{aligned} \tag{2}$$

Given that the order of x^2 is 3, we can conclude that then the order xy^2 is 6.
Moreover, it's clear that the order of y^2 is 2. As well y^2 is the same as $(xy^2)^3$, as shown below:

$$(xy^2)^3 = (xy^2)^2(xy^2) = x^2(xy^2) = y^2$$

Now define the function f to be the mapping from KH to Q_3 as:

$$\begin{aligned} f(xy^2) &= a \\ f(y) &= b \end{aligned}$$

It's clear that every element from KH is mapped to Q_3, and given that

$$bab^{-1}a = e$$

and

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

we know that the group operation in KH is the same as the group operation in Q_3. Given that f maps generators and preserves the group structure, we can conclude that KH is isomorphic to Q_3. More explicitly, we can stated that $G \cong Q_3$ when G has a unique Sylow 3-subgroup and every Sylow 2-subgroups are cyclic.

Case II. For the last case we wish to show that if all Sylow 2-subgroups are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ then G will be isomorphic to D_6. Let H be a Sylow 2-subgroup, then every element except for the identity has order 2. We write:

$$H = \{e, a, b, ab\}$$

Note that $G = KH$, given that $|KH| = 12$. Given that K is a normal subgroup of G, consider conjugation by some element in H. As follows we have that:

$$\begin{aligned} axa^{-1} &= x^u \\ bxb^{-1} &= x^v \\ (ab)x(ab)^{-1} &= x^{u \cdot v} \end{aligned}$$

such that $u, v \in \{0, 1, -1\}$.

At first it is clear that if u or v or both are equal to 0. Then we are lead to conclude that $x = e$, which is a contradiction as x is the generator for K.

Moreover, if we consider the case where u, v equal 1. Then we are lead to conclude that every element commutes:

$$\begin{aligned} ax &= xa \\ bx &= xb \\ abx &= xab \end{aligned}$$

which as shown before this leads us to conclude that our group is abelian, which we assumed it was not. Hence u and v can not equal 1 given that it leads to a contradiction.

Lastly, we can choose u, v to be either 1 and -1 or -1 and 1 respectively. Note that both choices are equivalent to letting u, v be equal to -1 and -1. So with out lost of generality we will choose u to equal to 1 and v to equal -1. This result in:

$$\begin{aligned} axa &= x \\ bxb &= x^{-1} \\ (ab)x(ab) &= x^{-1} \end{aligned}$$

Now we wish to show that there exist an isomorphism between G and the D_6. To this end, consider the order of the element (ax):

$$(ax)(ax) = (axa)x = x \cdot x = x^2.$$

Given that the order of x^2 is 3, we can conclude that the order of ax is 6.

Moreover note that $|b| = 2$. Hence if we consider the function f to map from KH to D_6:

$$f((ax)^n b^m) = r^n f^m, \text{ where } n, \ m \text{ are integers.}$$

See that all elements from KH are mapped to D_6, therefore the map is a bijection.

Finally, if we consider group structure of the dihedral group of order 6, then we require the relationship between r and f to hold:

$$D_6 = \langle \ r, f \mid r^6 = f^2 = e, rf = r^{-1}f \ \rangle$$

To this end consider that:

$$(ax^2)b = a(x^{-1}b) = a(bx) = b(ax)$$

Hence:

$$f((ax^2)b) = f(ax^2) \cdot f(b) = r \cdot f = f \cdot r^{-1} = f(b) \cdot f(ax) = f(bax)$$

Since $(ax)^{-1} = (ax^2)$, it is evident that the group operation KH is the same as the group operation in D_6. Furthermore we can show that f is a homomorphism which allowing us to conclude that f is an isomorphism. Therefore, $G \cong D_6$.

□

This concludes our classification of all groups up to order 15.

6 Proof of Theorem 2, Part I

In the previous section we sought to classify all groups of order 15 or less. For some of these groups we find the Symmetric Group of least order in which it can be embedded; we shall refer to this as the minimal embedding.

6.1 Cyclic Groups

Lemma 12. *Let p be a prime number and $r \geq 1$ an integer. The minimal embedding of a cyclic group $G \cong \mathbb{Z}_{p^r}$ is S_{p^r}.*

Proof.

In any symmetric group S_n, the order of an element $\pi \in S_n$ is given by the least common multiple of the length of the cycles in its cycle decomposition. In other words, if we decompose π into disjoint cycles:

$$\pi = \sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdot \sigma_4 \cdots \sigma_k$$

then the order $ord(\pi)$ in S_n is the $\text{lcm}(l_1, l_2, \ldots, l_k)$, where l_i is the length of σ_i for $1 \leq i \leq k$.

Moreover, given that all possible cycle types of S_n are given by partitions of n. It is clear that

$$l_1 + l_2 + l_3 + \cdots + l_k \leq n \tag{3}$$

Now suppose that one could embed $G \cong \mathbb{Z}_{p^r}$ into a symmetric group S_n with $n < p^r$. Then S_n would necessarily contain an element, π, of order p^r. By the above discussion:

$$p^r = \text{lcm}(l_1, l_2, \ldots, l_k)$$

for some positive integer $l_1, l_2, \ldots, l_k$.

In particular, each l_i must divide p^r. Given that p is a prime, each l_i is restricted to be a power of p no greater than p^r. So we may re-write the equation above to:

$$\text{lcm}(l_1, l_2, l_3, \ldots, l_k) = \text{lcm}(p^{\gamma_1}, p^{\gamma_2}, p^{\gamma_3}, \ldots, p^{\gamma_r}) = p^{\text{Max}\{\gamma_1, \gamma_2, \ldots, \gamma_k\}} = p^r$$

where γ_i is some integer less than or equal to r for $1 \leq i \leq k$.

Hence, there exists some index i such that $\gamma_i = r$ for $1 \leq i \leq k$. Therefore, the cycle length, l_i, for that same index i, would be p^r.

However, as we noted in Equation 3 we have that:

$$l_1 + l_2 + \cdots + l_r \leq n < p^r$$

which contradicts our previous argument that there exists some cycle whose length is p^r. It follows that if $G \cong \mathbb{Z}_{p^r}$ is embedded in some S_n then $n \geq p^r$.

Finally, we note that such an embedding is possible for $n = p^r$.

Consider, the permutation $(1\ 2\ 3 \ldots\ p^r)$ of p^r elements generates a cyclic subgroup of S_{p^r} whose order is p^r. Given that two cyclic groups of the same order are isomorphic, then $G \cong \langle (1\ 2\ 3 \ldots\ p^r) \rangle \leq S_{p^r}$. So we conclude that S_{p^r} is the minimal embedding of G.

□

As a consequence we obtain the following table:

Group	Minimal Embedding	Group	Minimal Embedding
$\mathbb{Z}_2$	S_2	$\mathbb{Z}_8$	S_8
$\mathbb{Z}_3$	S_3	$\mathbb{Z}_9$	S_9
$\mathbb{Z}_4$	S_4	$\mathbb{Z}_{11}$	S_{11}
$\mathbb{Z}_5$	S_5	$\mathbb{Z}_{13}$	S_{13}
$\mathbb{Z}_7$	S_7		

Next we wish to prove the minimal group embedding for $\mathbb{Z}_6$ and $\mathbb{Z}_{10}$. To achieve this goal we will use again the idea from the previous lemma combined with the fact that possible cycle types of S_n are given by partitions of n.

Lemma 13.

1. *The minimal embedding of* $\mathbb{Z}_6$ *is* S_5.
2. *The minimal embedding of* $\mathbb{Z}_{10}$ *is* S_7.
3. *The minimal embedding of* $\mathbb{Z}_{12}$ *is* S_7.
4. *The minimal embedding of* $\mathbb{Z}_{14}$ *is* S_9.
5. *The minimal embedding of* $\mathbb{Z}_{15}$ *is* S_8.

Proof.

To start we wish to prove that S_5 is the minimal Symmetric Group in which $\mathbb{Z}_6$ can be embedded in. See that $\mathbb{Z}_6$ can be expressed in cyclic notation as $\mathbb{Z}_6 \cong \langle (123)(45) \rangle \leq S_5$.

Furthermore, assume by way of contradiction that $\mathbb{Z}_6 \hookrightarrow S_4$, then this would imply that there exist a permutation in S_4 in which the least common multiple of the cycle lengths is 6. This entails that there exists a cycle in the permutation which is a multiple of 3. See that there is only a multiple of 3 less than 4, namely 3 it's self. So we will have an permutation with a cycle type that involves a 3-cycle.

As stated before all possible cycle types of S_n are given by partitions of n. In particular the only partition of 4 that involves a 3 is $3+1 = 4$. However, in this case the least common multiple of the cycle lengths is just $\text{lcm}(3, 1) = 3$. Hence there can not exist a permutation in S_4 of order 6, so we have reach a contradiction. Therefore the minimal embedding of $\mathbb{Z}_6$ is S_5.

The exact same proof method applies to $\mathbb{Z}_{10}$ and $\mathbb{Z}_{14}$.

Similarly, we can conclude that the minimal Symmetric Group in which $\mathbb{Z}_{12}$ can be embedded in is S_7. Notice that $\mathbb{Z}_{12}$ can be expressed in cyclic notation as $\mathbb{Z}_{12} \cong \langle (1234)(567) \rangle \leq S_7$.

If we assume by way of contradiction that $\mathbb{Z}_{12} \hookrightarrow S_6$, then there exist a permutation in which the least common multiple of the cycles lengths is 12. This would imply by the same reasoning as before that there exist a cycle in the permutation which is a multiple of 4. There is only a multiple of 4 less than 6, exactly 4 it's self. So we are forced to have a cycle type that contains a 4-cycle.

Moreover, there are only two partition of 6 that contains a 4 which are $4+1+1 = 6$ and $4+2 = 6$. However, the least common multiple of these cycle lengths is just $\text{lcm}(4, 1, 1) = \text{lcm}(4, 2) = 4$. Hence there can not exist a permutation in S_6 which is of order 12, therefore S_7 is the minimal Symmetric Group in which $\mathbb{Z}_{12}$ can be embedded in.

The same proof technique applies to $\mathbb{Z}_{15}$.

□

6.2 Dihedral Groups

Furthermore, consider the minimal group embedding of any dihedral group D_n of order $2n$, where n is some positive integer greater than 2. Given that we are considering groups of order at most 15 we restrict ourself to the following lemma:

Lemma 14.

1. *The minimal embedding of D_3 is S_3.*
2. *The minimal embedding of D_4 is S_4.*
3. *The minimal embedding of D_5 is S_5.*
4. *The minimal embedding of D_7 is S_7.*

Proof. It is well known that D_3 is isomorphic to S_3. Hence S_3 is it's minimal embedding.

On the other hand, see that the group representation of $D_4 = \langle r, f \mid r^4 = e, f^2 = e, rf = fr^{-1} \rangle$. We wish to prove that $D_4 \hookrightarrow S_4$ by proving that $D_4 \cong \langle (1234), (12)(34) \rangle$. To start see that $\langle r \rangle \cong \langle (1234) \rangle$ given that both are cyclic groups of the same order, furthermore, if we establish the mapping $\gamma : D_4 \to \langle (1234), (12)(34) \rangle$ to be:

$$\gamma(r^m) = (1234)^m \qquad \gamma(f) = (12)(34) \qquad \gamma(rf) = (1234)(12)(34)$$

where m is an integer, we obtain the following relations

$$\gamma(r)\gamma(f) = (1234)(12)(34) = \gamma(rf)$$

and

$$\gamma(r)\gamma(f) = (1234)(12)(34) = (12)(34)(1432) = (12)(34)(1234)^{-1} = \gamma(f)\gamma(r^{-1})$$

See that every element in D_4 is mapped to a unique element in $\langle (1234), (12)(34) \rangle$. Therefore γ is a bijective homomorphism. So we can conclude that $D_4 \hookrightarrow S_4$ given that

$$D_4 \cong \langle (1234), (12)(34) \rangle \leq S_4.$$

Lastly, $D_4 \not\hookrightarrow S_3$ given that the order of $|D_4| = 8$ does not divide the order of $|S_3| = 6$. Thus, S_4 is the minimal embedding of D_4. The same reasoning can be applied to prove the minimal embedding of D_5 and D_7 with the exception that $\gamma(f) = (25)(34)$ and $\gamma(f) = (27)(36)(45)$ respectively. It should be noted that if p is prime and $n < p$ then S_n has no elements of order p. □

Lemma 15. *The minimal embedding of D_6 is S_5.*

Proof.

Consider the group representation of $D_6 = \langle r, f \mid r^6 = e, f^2 = e, rf = fr^{-1} \rangle$. Notice that $\langle r \rangle \cong \langle (123)(45) \rangle$ given that both are cyclic groups which share the same order. Now consider the mapping $\gamma : D_6 \to \langle (123)(45), (12) \rangle$ to be:

$$\gamma(r^m) = (123)^m(45)^m \quad \gamma(f) = (12) \quad \gamma(rf) = (123)(45)(12) = (13)(45)$$

where m is any integer. We have the following relations:

$$\gamma(r)\gamma(f) = (123)(45)(12) = (13)(45) = \gamma(rf)$$

and

$$\gamma(r)\gamma(f) = (123)(45)(12) = (13)(45) = (12)(132)(45) = \gamma(f)\gamma(r^{-1})$$

Given that every element in D_6 is mapped to a unique element in $\langle (123)(45), (12) \rangle$. We can conclude that γ is a bijective homomorphism. So we can conclude that $D_6 \hookrightarrow S_5$ given that

$$D_6 \cong \langle (123), (12), (45) \rangle \leq S_5$$

Lastly see, that D_6 can not be embedded in S_4. This owes to the fact that D_6 has a cyclic subgroup of order 6, where as S_4 has no elements of order 6.

□

6.3 Non Cyclic Abelian Groups

Next consider the following non-cycic abelian groups

$$\mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

Lemma 16.

1. *The minimal embedding of* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *is* S_4.
2. *The minimal embedding of* $\mathbb{Z}_2 \times \mathbb{Z}_4$ *is* S_6.
3. *The minimal embedding of* $\mathbb{Z}_3 \times \mathbb{Z}_3$ *is* S_6.

Proof. To begin consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. See that $\mathbb{Z}_2 \times \mathbb{Z}_2$ can not be embedded in S_3 given that the order of $\mathbb{Z}_2 \times \mathbb{Z}_2$ does not divide the order of S_3. So it's minimal embedding is S_4 by Cayley's theorem.

Now consider the following abelian groups, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. We wish to show that their minimal embedding is S_6. First, see that both groups can be embedded in S_6, owing to the fact that they are isomorphic to the cyclic representations shown below:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \langle (1\ 2)\ ,\ (3\ 4)\ ,\ (5\ 6) \rangle \leq S_6 \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \cong \langle (1\ 2)\ ,\ (3\ 4\ 5\ 6) \rangle \leq S_6$$

Nonetheless, see that these two groups can not be embedded in S_4 nor in S_5, owing to the fact that if such an embedding were possible they both would be Sylow 2-subgroups conjugate to D_4, by the Sylow Theorems. This owes to the fact that D_4 being of order 8 is a Sylow 2-subgroup of S_4 and S_5. Therefore we obtain a contradiction because D_4 is a non-abelian group. Therefore, S_6 is the minimal embedding for $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Continuing with minimal embeddings, consider the group $\mathbb{Z}_3 \times \mathbb{Z}_3$, which has as it's minimum embedding S_6. This owes to fact $\mathbb{Z}_3 \times \mathbb{Z}_3$ is isomorphic to the cyclic representation:

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \cong \langle (1\ 2\ 3)\ ,\ (4\ 5\ 6) \rangle \leq S_6$$

and that the order of $\mathbb{Z}_3 \times \mathbb{Z}_3$ being 9, does not divide the order of S_4 or S_5 which is 24 and 120 respectively.

□

Remark 17. *By similar methods used in Lemma 16 it can be proven that* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *has as it's minimal embedding* S_7 *as stated in [1].*

7 The Alternating Group and Dicyclic groups

Finally we consider the Alternating group and the Di-cyclic groups.

Lemma 18. *The minimal embedding of A_4 is S_4.*

Proof. See that $A_4 \leq S_4$ and $|A_4| \not| |S_3|$. Therefore A_4 has as it minimal embedding S_4.

□

Now we wish to prove that the minimal embedding of Q_2 is S_8. To this end consider the group G acting on a set S. Then

$$g \in G,\ x \in S\ :\ g \cdot x \in S$$

For a fixed $g \in G$, define

$$\begin{aligned} \lambda \cdot g : S &\rightarrow S \\ x &\mapsto g \cdot x \end{aligned}$$

Then $\lambda \cdot g$ is a permutation of S.

Now define a map:

$$\begin{aligned} F : G &\rightarrow Perm(S) \\ g &\rightarrow \lambda \cdot g \end{aligned}$$

It's known that F is a group homomorphism.

Moreover $Ker(F) = \{g \in G : gx = x, \forall x \in S\} = \bigcap_{x \in S} Stab(x)$.

Now consider the following Lemma.

Lemma 19. *The Quaternion Group Q_2 does not embed in S_n with $n < 8$.*

Proof.

Suppose otherwise, then there exists an injective group homomorphism $F : Q_2 \rightarrow Perm(S)$, with $|S| < 8$. Injective means trivial kernel, so $\bigcap_{x \in S} Stab(x) = \{e\}$.

Now, by the Orbit-Stabilizer theorem:

$$|Orbit(x)| = [Q_2 : Stab(x)]$$

Thus

$$\frac{|Q_2|}{|Stab(x)|} = |Orbit(x)| \leq |s| < 8 = |Q_2|,$$

which contradicts that $|Stab(x)| > 1$, i.e., the Stabilizer subgroup is non-trivial for every $x \in S$.

One specific feature of Q_2 is that every non-trivial subgroup contains the subgroup $\{\pm 1\}$. In other words, the intersection of the stabilizer contains at least 2 elements. This contradicts our assumption that we have a trivial kernel.

□

Lemma 20. *The minimal embedding of Q_2 is S_8.*

Proof. Lastly we are left to show that $Q_2 \hookrightarrow S_8$. Consider the group representation of Q_2, which is

$$Q_2 = \langle i, j | i^4 = 1; i^2 = j^2; j^{-1}ij = i^{-1} \rangle$$

Let γ be the function that maps Q_2 to a subgroup of S_8 given by:

$$\gamma(i^m) = (1234)^m(5678)^m, \gamma(j^n) = (1638)^n(2547)^n$$
$$\gamma(ij) = (1234)(5678)(1638)(2547) = (1735)(2648)$$

where m and n are any integer. Observe that γ is a bijection, as shown below every element from Q_2 is mapped to a distinct permutation in S_8.

$$\gamma(i) = (1234)(5678)$$
$$\gamma(i)^2 = (1234)^2(5678)^2 = (13)(24)(57)(68) = \gamma(-1)$$
$$\gamma(i)^3 = (1234)^3(5678)^3 = (1432)(5876) = \gamma(-i)$$
$$\gamma(i)^4 = (1234)^4(5678)^4 = e = \gamma(1)$$

$$\gamma(j) = (1638)(2547)$$
$$\gamma(j)^2 = (1638)^2(2547)^2 = (13)(24)(57)(68) = \gamma(-1)$$
$$\gamma(j)^3 = (1638)^3(2547)^3 = (1836)(2745) = \gamma(-j)$$
$$\gamma(j)^4 = (1638)^4(2547)^4 = e = \gamma(1)$$

$$\gamma(ij) = (1735)(2648) = \gamma(k)$$
$$\gamma(ij)^2 = (1735)^2(2648)^2 = (13)(24)(57)(68) = \gamma(-1)$$
$$\gamma(ij)^3 = (1735)^3(2648)^3 = (1537)(2846) = \gamma(-k)$$
$$\gamma(ij)^4 = (1735)^4(2648)^4 = e = \gamma(1)$$

Moreover, see that the first two group relations hold, namely, $\gamma(i)^4 = e$ and $\gamma(j)^2 = \gamma(i)^2$.

We have that γ is homomorphism given that:

$$\gamma(ij) = (1234)(5678)(1638)(2547) = \gamma(i)\gamma(j)$$

Lastly we have that:

$$\gamma(j)\gamma(i)^{-1} = \gamma(j)\gamma(i)^3 = (1638)(2547)(1432)(5876) = (1735)(2648) = \gamma(i)\gamma(j)$$

So, we obtain:

$$\gamma(j)^{-1}\gamma(i)\gamma(j) = \gamma(i)^{-1}$$

Given that γ is a bijective homomorphism, we can conclude that:

$$Q_2 \cong \langle (1234)(5678), (1638)(2547) \rangle \leq S_8$$

Therefore Q_2 has as it's minimal embedding S_8.

□

Lemma 21. *The minimal embedding of Q_3 is S_7.*

Proof. Consider the group representation for Q_3:

$$Q_3 = \langle\ x, y \mid x^4 = y^3 = e,\ xyx^{-1} = y^{-1}\ \rangle$$

We have an element of order 4, and another element of order 3. Now, every element of order 3 in S_6 is either a 3-cycle or the product of two distinct 3-cycles. In othe words if τ has order 3 in S_6, then τ is of the form (123) or (123)(456).

Case 1. $\tau = (123)$
A well known fact from Group Theory states that if σ is any element of S_6 then:

$$(\sigma)(\tau)(\sigma)^{-1} = (\sigma(1)\sigma(2)\sigma(3))$$

Given that we want to have the same group structure we require that xyx^{-1} holds true. Thus,

$$(\sigma)(\tau)(\sigma)^{-1} = \tau^{-1} = (132)$$

However, this implies that either $\sigma(1) = 1$, or $\sigma(2) = 2$, or $\sigma(3) = 3$. Without lost of generality, assume that $\sigma(1) = 1$. Then $\sigma(2) = 3$ and $\sigma(3) = 2$, i.e., σ swaps 2 and 3. However, this makes it impossible for σ to contain a 4-cycle, therefore σ cannot have order 4.

Case 2. $\tau = (123)(456)$
This case follows the same proof pattern as Case 1, the only difference is that: $(\sigma)(\tau)(\sigma)^{-1} = (\sigma(1)\sigma(2)\sigma(3))(\sigma(4)\sigma(5)\sigma(6))$.

So we can conclude that Q_3 can not be embedded in S_6.

Finally, by the same methods used to find an isomorphism from Q_2 to a subgroup in S_8, we can prove that there exist subgroup in S_7 isomorphic to Q_3 as stated in [1]. Specifically, it can shown that:

$$Q_3 \cong \langle (123), (12)(4567) \rangle \leq S_7.$$

Therefore, Q_3 has as it's minimal embedding S_7.

□

References

[1] Robert Heffernan, Des MacHale, and Brendan McCann. Cayley's theorem revisited: Embeddings of small finite groups. *Mathematics Magazine*, 91(2):103–111, 2018.