Summer 2016

When There Is A Unique Group Of A Given Order And Related Results

Haya Ibrahim Binjedaen

WHEN THERE IS A UNIQUE GROUP OF A GIVEN ORDER AND RELATED RESULTS

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

Haya Binjedaen

July 2016

WHEN THERE IS A UNIQUE GROUP OF A GIVEN ORDER AND RELATED RESULTS

Mathematics

Missouri State University, July 2016

Master of Science

Haya Binjedaen

ABSTRACT

It is well-known that any group whose order is a prime number must be cyclic, that is there is only one group of that order up to isomorphism. This is also the case for some non-prime orders, for example there is only one group of order 15 up to isomorphism. This thesis provides the necessary background material to completely characterize those n for which there is a unique group of order n, namely when $\gcd(n, \varphi(n)) = 1$ with φ being the Euler totient function. We also determine for which n there are exactly two groups of order n up to isomorphism.

KEYWORDS: group, isomorphic, non-isomorphic, abelian groups, direct product, semidirect product, order.

This abstract is approved as to form and content

Dr. Les Reid, Dr. Richard Belshoff
Co-Chairpersons, Advisory Committee
Missouri State University

WHEN THERE IS A UNIQUE GROUP OF A GIVEN ORDER AND RELATED RESULTS

By

Haya Binjedaen

A Masters Thesis
Submitted to The Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Mathematics

July 2016

Approved:

Dr. Les Reid, Co-Chairperson

Dr. Richard Belshoff, Co-Chairperson

Dr. Kishor Shah, Member

Dr. Julie J. Masterson, Graduate College Dean

ACKNOWLEDGEMENTS

In the beginning, I wish to thank, first and foremost, Dr. Les Reid and Dr. Richard Belshoff for agreeing to be my thesis advisor. I am gratefully indebted to them for their very valuable comments on this thesis. Also, I would like to thank them for their advice and for their generosity. Without it, I would not have finished this thesis and approach my dream. Particularly, I am thankful to them for encouraging me to use correct grammar and consistent notation in my writings and for carefully reading and commenting on this thesis. Their patience and support helped me overcome many crisis situations and finish this dissertation. I hope that one day I would become as good an advisor to my students as Dr. Les Reid and Dr. Richard Belshoff have been to me. Besides my advisors, I would like to thank the other member of my thesis committee Dr. Kishor Shah.

I would like to thank my program advisor Dr. Matthew Wright. The door to Dr. Wright office was always open whenever I had a question about my academic program. I owe my deepest gratitude to the department head Dr. William Bray. He was always available at any time I needed him and was always ready to help. I would also like to thank all my English language teachers in the English Language Institute for helping me understand and speak English, which helped my on my academic journeys.

I thank Missouri State University for accepting me, and for giving me the chance to prove myself. Also, I cannot find words to express my gratitude to Saudi Arabia's Government for providing me with the opportunity to study in the United States to make my dream come true. I would love to thank Saudi Arabia's Government for supporting me financially from when I first came to the United States until I finished my thesis. I owe my deepest gratitude to my advisor Sawsan Aiad in the Saudi Arabian Cultural Mission for her help any time I needed her.

Finally, I owe my deepest gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. I especially thank my mom for her love and patience without which none of this would have been possible. I would like to think my dad for believing in me. Also, I would like to thank my brother Mohammed for aiding and encouraging me throughout this endeavor. I cannot find words to express my gratitude to my sisters Dalal and Reema for pushing me towards achieving my goal. Last but not the least, I would like to warmly appreciate the generosity and understanding of my friends for their support.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

In this thesis we will discuss and prove results and theorems from group theory. One of the main problems in group theory is to categorize groups up to isomorphism. For instance, how many groups of order n are there up to isomorphism? For which integer n is there a unique group of order n? For which integer n are there two groups of order n?

In Chapter 2, we summaries the basic definitions and properties of finite groups. We provide examples of groups both abelian and non-abelian. Then we outline some important definitions, examples, and theorems about subgroups. Two important theorems are Lagrange's Theorem and Cauchy's Theorem. After that we discuss some important theorems and definitions about conjugates, normal subgroups, and the centers of groups, which we will need in this paper.

In Chapter 3, we outline some basic definitions and theorems about homomorphisms, isomorphisms, and automorphisms. Then we give the definition, properties, and some examples of the Euler φ-function. Finally in this chapter we will go over two important theorems about automorphism groups.

We begin Chapter 4 by discussing Sylow's Theorem which plays a major role in this thesis. Then we move to some important definitions and theorems about direct products, semi-direct products, finitely-generated groups, and the fundamental theorem of finitely-generated abelian groups. At the end of this chapter, we investigate direct products and semi-direct products.

In chapter 5, we completely characterize these integers n for which there is a unique group of order n up to isomorphism.

In chapter 6, we determine for which integers n there are exactly two groups of order n up to isomorphism.

2. BACKGROUND

Before starting the main part of this thesis, a review is necessary. In this section, we will provide some basic definitions, theorems, and examples of groups.

The definitions below are given by Hungerford [2, p.172].

DEFINITION 2.1: A **group** is a nonempty set G equipped with a binary operation $*$ that satisfies the following axioms:

1. Closure: If $a \in G$ and $b \in G$, then $a * b \in G$.
2. Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
3. There is an element $e \in G$ (identity) such that $a * e = e * a = a$ for every $a \in G$.
4. For each $a \in G$ there is an element $a^{-1} \in G$ (inverse) such that $a * a^{-1} = a^{-1} * a = e$.

A group is said to be **abelian** if it satisfies this axiom:

5. Commutativity: $a * b = b * a$ for all $a, b \in G$.

DEFINITION 2.2: For $n \in \mathbb{Z}^+$, two integers a and b are said to be **congruent modulo** n, written $a \equiv b \pmod{n} \iff n \mid a - b$.

The set of all congruence classes of the integers for a modulus n is called the set of **integers modulo** n, denoted by $\mathbb{Z}_n$ and defined as follows:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

An important subset of $\mathbb{Z}_n$ consists of all collection of residue classes which have a multiplicative inverse in $\mathbb{Z}_n$ denoted by $(\mathbb{Z}_n)^\times$: $(\mathbb{Z}_n)^\times = \{\bar{a} \in \mathbb{Z}_n |$ there exists $\bar{b} \in \mathbb{Z}_n$ with $\bar{a}\bar{b} = \bar{1}\}$.

PROPOSITION 2.3: $(\mathbb{Z}_n)^\times = \{\bar{a} |\ \gcd(a,n) = 1\}$.

EXAMPLE 2.4: $(\mathbb{Z}_9)^\times = \{1, 2, 4, 5, 7, 8\}$.

Here are some examples of abelian and nonabelian groups:

EXAMPLE 2.5: 1. $\mathbb{Z}_n$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are abelian groups under addition.

2. $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$ and $\mathbb{Z}_n^\times$ are abelian groups under multiplication.

EXAMPLE 2.6: Let $G = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{R}, \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0\}$. This is a nonabelian group because, for example

$$\begin{bmatrix} 1 & 2 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 7 & 5 \\ 18 & 14 \end{bmatrix} \neq \begin{bmatrix} 5 & 12 \\ 6 & 16 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 6 \end{bmatrix}.$$

DEFINITION 2.7: The **order** of an element a in a group G is the smallest positive integer n such that $a^n = 1$, denoted by $|a| = n$. If there is no such n, then $|a| = \infty$.

Following this definition, are two examples of the order of a group element.

EXAMPLE 2.8: 1. In the additive group $\mathbb{Z}_{12}$,$|2| = 6$ since 2+2+2+2+2+2 = 0 and $2 \cdot n \neq 0$ for any $0 < n < 6$.

2. In the multiplicative group $\mathbb{Z}_7$,$|2| = 3$ since $2 \cdot 2 \cdot 2 = 1$ and $2^n \neq 1$ for any $0 < n < 3$.

DEFINITION 2.9: Let G be a group. A subset H of G is a **subgroup** of G if H is nonempty and for all $a, b \in H$ then $ab \in H$ and $a^{-1} \in H$. If H is a subgroup of G, we denote this by $H \leq G$.

Here is an example of subgroup.

EXAMPLE 2.10: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ under addition.

NOTATION: If $S \subseteq G$ then $\langle S \rangle$ is the smallest subgroup of G containing S. If $S = \{a\}$ we will denote $\langle S \rangle$ by $\langle a \rangle$.

THEOREM 2.11: If G is a group and $a \in G$, then $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

DEFINITION 2.12: The group $\langle a \rangle$ is the **cyclic subgroup generated by** a and if the subgroup $\langle a \rangle$ is the entire group G, then G is called a **cyclic group**.

EXAMPLE 2.13: $\mathbb{Z}_n$ is a cyclic group for all positive integers n.

NOTATION: We will denote a "generic" cyclic group of order n under multiplication by C_n.

It is necessary to note the following remark.

REMARK 2.14: Every cyclic group is an abelian group.

DEFINITION 2.15: The order of group G is the number of elements in G, denoted $|G|$.

PROPOSITION 2.16: If $H = \langle a \rangle$, then $|H| = |a|$.

THEOREM 2.17: Every subgroup of a cyclic group is cyclic.

One of the basic important theorems about finite groups is Lagrange's Theorem.

THEOREM 2.18: (Lagrange's Theorem) If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Following is a brief example of Lagrange's Theorem.

EXAMPLE 2.19: If $|G| = 15$ then the only possible orders for a subgroup are $1, 3, 5$, and 15.

COROLLARY 2.20: If $|G| = n < \infty$ and $x \in G$ then $|x|$ divides $|G|$.

LEMMA 2.21: Let G be a group with identity element e. If $a \in G$ and if $a^n = e$, then the order of a divides n.

Proof. Assume $|a| = t$ for some t. This is means t is the smallest positive integer such that $a^t = e$. Divide n by t using the Division Algorithm: $n = tq + r$ for some integers q and r, where $0 \leq r < t$. Now $e = a^n = a^{tq+r} = a^{tq}a^r = (a^t)^q a^r = a^r$. We have $a^r = e$ and $0 \leq r < t$. Because t is the smallest positive integer such that

$a^t = 1$, then we must have $r = 0$. Therefore $n = tq$. Thus the order of a divides n. □

THEOREM 2.22: If G is a group with prime order p, then G is cyclic.

Proof. Let G be a group and $|G| = p$. Choose any $a \in G$ that is a nonidentity element of G. Then $|\langle a\rangle|$ divides $|G|$, thus $|\langle a\rangle| = 1$ or p since p is prime. But since $|\langle a\rangle| > 1$, $|\langle a\rangle| = p$. Hence $\langle a\rangle$ is all of G, so G is a cyclic group of order p. □

Another major theorem that is related to Lagrange's Theorem is Cauchy's Theorem. Cauchy's Theorem is a partial converse of Lagrange's Theorem.

THEOREM 2.23: (Cauchy's Theorem) If G is a finite group and $p \mid |G|$ where p is prime, then G has an element of order p.

Here is a brief application of Cauchy's Theorem.

EXAMPLE 2.24: Let $G = \mathbb{Z}_9$, so $|\mathbb{Z}_9| = 9$ and $3|9$. There exists at least one element of $\mathbb{Z}_9$ which has order 3. In this case, 3 and 6 both work.

The next proposition will be used consistently throughout this paper.

PROPOSITION 2.25: If H and K are subgroups of group G, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$.

The proof for this proposition is excluded from this paper but can be found in Dummit and Foote [1, p 93]

DEFINITION 2.26: Let G be a group and N a subgroup of G. The element gng^{-1} is called the **conjugate** of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} | n \in N\}$ is called the **conjugate** of N by g. The element g is said to **normalize** N if $gNg^{-1} = N$. A subgroup N of a group G is called **normal** if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

COROLLARY 2.27: If H and K are subgroups of G and $H \leq N_G(K)$, then:

1. HK is a subgroup of G and
2. If $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

DEFINITION 2.28: Define $Z(G) = \{g \in G | gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. this subset of G is called the **center** of G.

THEOREM 2.29: If $|G| = p^n$ with p prime then $|Z(G)| \neq 1$.

Proof. the proof for this theorem is excluded from this paper but can be found in Dummit and Foote [1, p.125]. □

THEOREM 2.30: If $G/Z(G)$ is cyclic then G is abelian.

Proof. Assume $G/Z(G)$ is cyclic with generator $xZ(G)$. choose any $g \in G$. So $gZ(G) = (xZ(G))^k = x^kZ(G)$ for some $k \in \mathbb{Z}$. Hence $x^{-k}g = z \in Z(G)$. Then $g = x^kz$. Given $g_1, g_2 \in G$, where $g_1 = x^{k_1}z_1$ and $g_2 = x^{k_2}z_2$. Therefore, $g_1g_2 = x^{k_1}z_1x^{k_2}z_2 = x^{k_1}x^{k_2}z_1z_2 = x^{k_1+k_2}z_1z_2 = x^{k_2+k_1}z_1z_2 = x^{k_2}x^{k_1}z_1z_2 = x^{k_2}z_2x^{k_1}z_1 = g_2g_1$. □

Now that elementary facts about groups have been examined, we will explore homomorphisms, isomorphisms, and automorphisms in the next chapter.

3. HOMOMORPHISMS, ISOMORPHISMS, AND AUTOMORPHISMS

Roughly, a correspondence between two mathematical structures that are algebraically identical is called an isomorphism. A weaker notation than isomorphism is that of homomorphism. An isomorphism between a group and itself is called an automorphism.

Below is the definition of homomorphism given by Hungerford [2, p.172].

DEFINITION 3.1: Let G and H be groups with operations $\star$ and $\circ$ respectively. A map $\Psi : G \longrightarrow H$ such that $\Psi(a \star b) = \Psi(a) \circ \Psi(b)$ for all $a, b \in G$ is called a **homomorphism**.

LEMMA 3.2: If $\Psi : G \longrightarrow H$ is a homomorphism and $\gcd(|H|, |G|) = 1$, then $\Psi(x) = 1_H$ for all $x \in G$.

Proof. Let $x \in G$ then $|x|$ divides $|G|$ by Corollary 2.20. Let $|x| = n$, so $x^n = 1$ hence $\Psi(x)^n = \Psi(1) = 1$ by lemma 2.21. So that $|\Psi(x)|$ divides n, hence $|\Psi(x)|$ divides $|G|$.

On the other hand, $\Psi(x) \in H$, so $|\Psi(x)|$ divides $|H|$ by Corollary 2.20. Therefore $|\Psi(x)|$ divides $|H|$ and $|G|$. Since $\gcd(|H|, |G|) = 1$, then $|\Psi(x)| = 1$. Hence $\Psi(x) = 1_H$ because the only element of order 1 is the identity. □

DEFINITION 3.3: The function $\Psi : G \longrightarrow H$ is called an **isomorphism**, and G is said to be isomorphic to H (written $G \cong H$), if

1. Ψ is a bijection
2. Ψ is a homomorphism.

With these definitions, it can be proved that the following facts are true.

REMARK 3.4: If $\Psi : G \longrightarrow H$ is an isomorphism, then

- G is abelian if and only if H is abelian
- $|G| = |H|$
- $|a| = |\Psi(a)|$ for all $a \in G$.

THEOREM 3.5: All cyclic groups of order n are isomorphic.

DEFINITION 3.6: Let G be a group. An isomorphism from G to itself is called an **automorphism** of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

DEFINITION 3.7: The **Euler φ-function** $\varphi(n)$ for a positive integer n is defined to be the number of positive integers less than or equal to n that are relatively prime to n.

Here are some relationships between n and $\varphi(n)$

1. $\varphi(1) = 1$
2. $\varphi(p) = p - 1$ where p is prime
3. $\varphi(p^a) = p^{a-1}(p-1)$ where p is prime
4. $\varphi(ab) = \varphi(a)\varphi(b)$ if $\gcd(a, b) = 1$
5. $\varphi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}) = (p_1 - 1)(p_2 - 1)\ldots\ldots(p_k - 1)p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots\ldots p_k^{\alpha_k - 1}$.

Now we apply the Euler φ-function to some examples.

EXAMPLE 3.8:
1. $\varphi(7) = 6$
2. $\varphi(9) = \varphi(3^2) = 6$
3. $\varphi(14) = \varphi(2)\varphi(7) = 6$

The lemma below is given by Rose [3, p.82].

LEMMA 3.9: If G is a group then $\mathrm{Aut}(G)$ is also a group.

Now we look at a proposition examining what an automorphism group can be isomorphic to.

PROPOSITION 3.10: We have Aut $(C_n) \cong (\mathbb{Z}_n)^\times$ and this is an abelian group of order $\varphi(n)$.

Proof. Let $C_n = \langle x \rangle$ and let $\sigma : C_n \longrightarrow C_n$ be a homomorphism defined by $\sigma(x) = x^a$ for some $a \in \mathbb{Z}$. We know $\sigma(x)$ determines all the values of σ. Denote this homomorphism by σ_a. We must have $\gcd(a, n) = 1$, because x and x^a have the same order n if and only if σ is an automorphism. Define $\psi : \mathrm{Aut}(C_n) \longrightarrow (\mathbb{Z}_n)^\times$ by $\psi(\sigma_a) = a \pmod{n}$.

Injective: Suppose $\psi(\sigma_a) = \psi(\sigma_b)$. Then $a \pmod{n} = b \pmod{n}$ and therefore $a = b + kn$ for some integer k. Now $x^a = x^{b+kn} = x^b(x^n)^k = x^b$. Hence $\sigma_a = \sigma_b$, and this proves ψ is injective.

Surjective: ψ is clearly surjective from the definition.

Homomorphism: We must show $\psi(\sigma_a \circ \sigma_b) = \psi(\sigma_a)\psi(\sigma_b)$. Note that for all σ_a, σ_b in $\mathrm{Aut}(C_n)$. $(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x)$. Therefore, $\psi(\sigma_a \circ \sigma_b) = \psi(\sigma_{ab}) = ab \pmod{n} = \psi(\sigma_a)\psi(\sigma_b)$. So the map ψ is homomorphism. Hence $\mathrm{Aut}(C_n) \cong (\mathbb{Z}_n)^\times$. □

The next proposition will be heavily used throughout the rest of this paper. It is important to keep the corollary in mind.

PROPOSITION 3.11: $\mathrm{Aut}(C_p) \cong C_{p-1}$ where p is prime.

Proof. The proof of this proposition can be found in Dummit and Foote, Corollary.19,[1, p.314]. □

Table 1 on the next page show the automorphism groups for some given groups.

Table 1: Automorphism Groups

Group G	$\mathrm{Aut}(G)$
C_1	C_1
C_2	C_1
C_3	C_2
C_4	C_2
C_5	C_4
C_6	C_2
C_7	C_6
C_8	$C_2 \times C_2$
C_9	C_6
C_{10}	C_4
C_{11}	C_{10}
C_{12}	$C_2 \times C_2$
C_{13}	C_{12}
C_{14}	C_6
C_{15}	$C_4 \times C_2$

4. DIRECT AND SEMIDIRECT PRODUCTS

THEOREM 4.1: (Sylow's Theorem) Let G be a finite group of order $p^\alpha k$, where p is prime and $p \nmid k$ then:

1. G has a subgroup of order p^α
2. If H and K are Sylow p-subgroups of G, then there exists $a \in G$ such that $H = a^{-1}Ka$.
3. The number of Sylow p-subgroups of a finite group G, denoted n_p divides $|G|$ and is of the form $1 + pk$ for some integer $k \geq 0$.

EXAMPLE 4.2: Let $|G| = 45 = 3^2 \cdot 5$. In G, a Sylow 3-subgroup has size 9 and Sylow 5-subgroup has size 5. By Sylow's theorem $n_3|5$ and $n_3 \equiv 1 \pmod 3$, hence $n_3 = 1$ and $n_5|9$ and $n_5 \equiv 1 \pmod 5$, so we have $n_5 = 1$. Therefore G has a normal Sylow 3-subgroup and Sylow 5-subgroup.

DEFINITION 4.3: The **direct product** $G_1 \times G_2 \times ..... \times G_n$ of the groups $G_1, G_2, ..., G_n$ with operations $\star_1, \star_2, ..., \star_n$ respectively, is the set of n-tuples $(g_1, g_2, ..., g_n)$ where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, ..., g_n) \star (h_1, h_2, ..., h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, ..., g_n \star_n h_n).$$

NOTE: If $G_1, G_2, ..., G_n$ are groups, then $G_1 \times G_2 \times ..... \times G_n$ has order $|G_1||G_2|.....|G_n|$.

DEFINITION 4.4: A group G is **finitely generated** if there is a finite subset S of G such that $G = \langle S \rangle$.

THEOREM 4.5: (**Fundamental Theorem of Finitely-Generated Abelian**

Groups) If G is a finitely-generated abelian group, then

$$G \cong \mathbb{Z}^r \times C_{n_1} \times C_{n_2} \times ..... \times C_{n_s}$$

for some $r, n_1, n_2, ..., n_s \in \mathbb{Z}$, where $r \geq 0$, $n_j \geq 2$ for all j, and $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.

LEMMA 4.6: $C_m \times C_n \cong C_{mn}$ if and only if $(m, n) = 1$ for $m, n \in \mathbb{Z}^+$

Proof. The proof for this lemma is excluded from this paper but can be found in Dummit and Foote [1, p.163]. □

Here is an example of the lemma.

EXAMPLE 4.7: $C_6 \cong C_2 \times C_3$.

The next theorem holds great importance in this paper.

THEOREM 4.8: Suppose H and K are subgroups of group G such that

1. $H \trianglelefteq G$ and $K \trianglelefteq G$ and
2. $H \cap K = 1$

Then $HK \cong H \times K$.

Proof. The proof for this lemma is excluded from this paper but can be found in Dummit and Foote [1, p.171]. □

PROPOSITION 4.9: Let G be a group of order pq, where p and q are prime such that $p < q$. If $p \nmid (q-1)$, then $G \cong C_{pq}$.

Proof. G has Sylow subgroups C_p and C_q. Also, $n_p | q$ and $n_p = 1 + pk$ for some integer $k \geq 0$. So either $n_p = 1$ or $n_p = q$. If $n_p = q$, then $q = 1 + pk$ for some integer $k \geq 0$ and so $p|(q-1)$ which contradicts our hypothesis $p \nmid (q-1)$. Therefore $n_p = 1$ and $C_p \trianglelefteq G$. By Corollary 2.27 C_pC_q is a subgroup of G. By Proposition

2.25, $|C_pC_q| = \frac{|C_p||C_q|}{|C_p \cap C_q|} = \frac{p \cdot q}{1} = |G|$. Hence $G = C_pC_q$. We have $n_q = 1$ or p (since $n_q|p$) and $n_q = 1 + kq$ for some integer $k \geq 0$. If $n_q = p$, then $q = 1 + kp > p$ for all $k > 0$, a contradiction to $q > p$. Therefore $n_q = 1$ and C_q is normal in G. Now $G = C_pC_q \cong C_p \times C_q$ by Theorem 4.9 and $G \cong C_{pq}$ by Lemma 4.6. □

DEFINITION 4.10: Let H and K be groups and let $\psi : K \longrightarrow \text{Aut } (H)$ be a group homomorphism. Let $G = \{(h, k)|h \in H \text{ and } k \in K\}$. Define multiplication on G by $(h_1, k_1)(h_2, k_2) = (h_1\psi(k_1)(h_2), k_1k_2)$. This multiplication makes G a group of order $|G| = |K||H|$, where the identity of G is $(1, 1)$, and $(h, k)^{-1} = (\psi(k^{-1})(h^{-1}), k^{-1})$ which is the inverse of (h, k). The group G is called **the semi-direct product** of H and K with respect to ψ (denoted by $H \rtimes_\psi K$).

Here are examples of semi-direct products.

EXAMPLE 4.11: 1. $C_3 \rtimes C_4 = \langle x, y|x^4 = y^3 = 1, x^{-1}yx = y^{-1}\rangle$

2. $(C_3 \times C_3) \rtimes C_2 = \langle x^2 = y^3 = z^3 = 1|yz = zy, x^{-1}yx = y^{-1}, x^{-1}zy = z^{-1}\rangle$.

The following theorem is also used constantly throughout the remaining pages of this thesis.

THEOREM 4.12: Suppose H and K are subgroups of group G such that

1. $H \trianglelefteq G$, and
2. $H \cap K = 1$
3. $|G| = |HK|$.

Then $G \cong H \rtimes_\psi K$ for some ψ.

Proof. Let $\psi : K \longrightarrow \text{Aut}(H)$ be given by $\psi(k)(h) = khk^{-1}$. Then one can check that $G \cong H \rtimes_\psi K$. □

REMARK 4.13: If H and K are groups and $\psi : K \longrightarrow \mathrm{Aut}(H)$ is the trivial homomorphism, i.e. $\psi(k_1) = \mathrm{id}$, for all $k_1 \in K$. Therefore $(h_1, k_1)(h_2, k_2) = (h_1\psi(k_1)(h_2), k_1k_2) = (h_1h_2, k_1k_2)$. Hence $H \rtimes_\psi K \cong H \times K$.

LEMMA 4.14: Let $|G| = pq$ where p and q are primes with $p < q$, where $p|q-1$. Then there is a nonabelian group of order pq.

Proof. By Cauchy's Theorem, G has elements of orders p and q, and therefore cyclic subgroups $C_q = \langle x \rangle$ and $C_p = \langle y \rangle$. We have $\mathrm{Aut}(C_q) \cong (\mathbb{Z}_q)^\times$ which has order $q-1$, and since $p|q-1$, there is an element $d \in (\mathbb{Z}_q)^\times$ of order p by Cauchy's Theorem. There is a non-trivial homomorphism $\phi : C_p \longrightarrow \mathrm{Aut}(C_q)$ defined by $\phi(y)(x) = x^d$. The group $C_q \rtimes_\phi C_p$ has order pq and since ϕ is not the trivial homomorphism, it is nonabelian. □

LEMMA 4.15: If there are g non-isomorphic groups of order d and $d|n$ then there are (at least) g non-isomorphic groups of order n.

Proof. If C_i are non-isomorphic groups of order d where $i = \{1, 2, ..., g\}$. Then $C_i \times C_{n/d}$ for $i = \{1, 2, ..., g\}$ are non-isomorphic groups of order n by The Krull-Schmidt Theorem. □

THEOREM 4.16: The center of a direct product is the direct product of the centers $Z(G_1 \times G_2 \times \times .... \times G_n) = Z(G_1) \times Z(G_2) \times ..... \times Z(G_n)$.

LEMMA 4.17: $Z(C_q \rtimes C_p) = 1$.

Proof. We have $Z(C_q \rtimes C_p) = 1, p, q$, or pq.

1. If $Z(C_q \rtimes C_p) = pq$ then it abelian group which is contradiction.
2. If $Z(C_q \rtimes C_p) = p$ then $|(C_q \rtimes C_p)/Z(C_q \rtimes C_p)| = \frac{pq}{p} = q$. Hence $(C_q \rtimes C_p)/Z(C_q \rtimes C_p)$ is cyclic. So it is abelian, which is contradiction.

3. If $Z(C_q \rtimes C_p) = q$ then $|(C_q \rtimes C_p)/Z(C_q \rtimes C_p)| = \frac{pq}{q} = p$. Hence $(C_q \rtimes C_p)/Z(C_q \rtimes C_p)$ is cyclic. So it is abelian, which is contradiction.

   Therefore $Z(C_q \rtimes C_p) = 1$. □

LEMMA 4.18: If $\gcd(|K|, |\mathrm{Aut}|H|) = 1$, Then $H \rtimes K \cong H \times K$.

Proof. By Lemma 3.2 and Remark 4.13 we have $H \rtimes K \cong H \times K$. □

On the next two pages Table 2 and Table 3 show groups of small order (up to isomorphism) and comments about these groups.

Table 2: Groups of small order (up to isomorphism)

Order n		No.of Groups	Abelian Groups	Non-abelian Groups
1	-	1	C_1	-
2	2^1	1	C_2	-
3	3^1	1	C_3	-
4	2^2	2	C_4, $C_2 \times C_2$	-
5	5^1	1	C_5	-
6	$2^1.3^1$	2	C_6	S_3
7	7^1	1	C_7	-
8	2^3	5	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	D_8,Q_8
9	3^2	2	C_9, $C_3 \times C_3$	-
10	$2^1.5^1$	2	C_{10}	D_{10}
11	11^1	1	C_{11}	-
12	$2^2.3^1$	5	C_{12}, $C_6 \times C_2$	A_4,D_{12},$C_3 \rtimes C_4$
13	13^1	1	C_{13}	-
14	$2^1.7^1$	2	C_{14}	D_{14}
15	$3^1.5^1$	1	C_{15}	-

Table 3: Comments on groups of small order

Abelian Groups	Non-abelian Groups	Comment
C_1	-	-
C_2	-	Order p
C_3	-	Order p
C_4, $C_2 \times C_2$	-	Order p^2
C_5	-	Order p
C_6	S_3	Order pq and $p \mid q-1$
C_7	-	Order p
C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	D_8,Q_8	Order p^3
C_9, $C_3 \times C_3$	-	Order p^2
C_{10}	D_{10}	Order pq and $p \mid q-1$
C_{11}	-	Order p
C_{12}, $C_6 \times C_2$	A_4,D_{12},$C_3 \rtimes C_4$	-
C_{13}	-	Order p
C_{14}	D_{14}	Order pq and $p \mid q-1$
C_{15}	-	Order pq and $p \nmid q-1$

5. UNIQUE GROUP OF A GIVEN ORDER

For p prime, up to isomorphism, there is a unique group of order p, namely C_p by Theorem 2.22 and Theorem 3.5. Also there are other cases that do not have prime order, but there is a unique group of that order. For example the only group of order 15 is C_{15}. In this section we completely determine when there is a unique group of a given order n.

DEFINITION 5.1: A **square-free** integer is an integer that cannot be divided by any perfect square number other then 1.

Here are a few examples of square-free integers.

EXAMPLE 5.2: 1. any prime p is square-free integer.

2. **15** is square-free integer.

3. **12** is not square-free integer since $2^2 \mid 12$.

LEMMA 5.3: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ where the p_i are distinct primes for $i = 1, ..., k$ and let φ denote the Euler φ-function. Then $\gcd(n, \varphi(n)) = 1$ if and only if $\alpha_i = 1$ for $1 \leqslant i \leqslant k$ (i.e n is square-free) and $p_i \nmid (p_j - 1)$ for $i \neq j$, $(1 \leqslant i, j \leqslant k)$.

Proof. ($\Leftarrow$) If $\alpha_i = 1$ and $p_i \nmid (p_j - 1)$, so $n = p_1 p_2 \ldots\ldots\ldots p_k$ and $\varphi(n) = (p_1 - 1)(p_2 - 1)....(p_k - 1)$. Hence $\gcd(n, \varphi(n)) = 1$ since $p_i \nmid (p_j - 1)$.

($\Rightarrow$) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p^{\alpha_k}$. Assume $\gcd(n, \varphi(n)) = 1$,then $\varphi(n) = (p_1 - 1)(p_2 - 1)\ldots\ldots\ldots(p_k - 1) p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots\ldots\ldots p_k^{\alpha_k - 1}$. We must have $\alpha_i - 1 = 0$ for all $i = 1, 2, ..., k$, otherwise p_i divides $\gcd(n, \varphi(n)) = 1$. Therefore $\alpha_i = 1$ for all i. Also, if $p_i \mid p_j - 1$ for some j, then p_i is a common divisor of n and $\varphi(n)$, a contradiction. Therefore $p_i \nmid p_j - 1$ for all $i \neq j$, $1 \leq i, j \leq k$. □

Before proceeding we need to know the definition of a solvable group and the statement of the Feit-Thompson Theorem.

DEFINITION 5.4: A group G is **solvable** if and only if $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq .... \trianglelefteq N_t \trianglelefteq N_{t+1} = G$ such that $|N_{i+1}/N_i| = p_i$ where p_i is prime number.

THEOREM 5.5: (Feit-Thompson Theorem) Every group of odd order is solvable.

Now we come to one of the main result of the thesis.

THEOREM 5.6: Let $|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_k^{\alpha_k}$ where $n \in \mathbb{Z}^+$. Then there is a unique group of order n (up to isomorphism) if and only if $\gcd(n, \varphi(n)) = 1$, where φ denotes the Euler φ-function.

Proof. ($\Rightarrow$) We want to show if there is a unique group of order n, then $\gcd(n, \varphi(n)) = 1$. So, we will show if $\gcd(n, \varphi(n)) \neq 1$, then there is more than one group of order n. Assume $\gcd(n, \varphi(n)) \neq 1$. There are two cases by Lemma 5.3.

Case 1: Some $\alpha_i > 1$, then $\gcd(n, \varphi(n)) \geq p_i$. So there exist two non-isomorphic abelian groups: $C_{p_i} \times C_{p_i} \times C_{n/p_i^2}$, and $C_{p_i{}^2} \times C_{n/p_i^2}$. Therefore there is more than one group of order n.

Case 2: All $\alpha_i = 1$ and there are p_i, p_j such that $p_i | p_j - 1$ for some $i, j \in \{1, 2, ..., k\}$ where $i \neq j$. Without loss of generality let $i = 1$ and $j = 2$. By Lemma 4.14 , there is a non-ableian group H of order $p_1 p_2$. Then $H \times C_{n/(p_1 p_2)}$ and C_n are a non-isomorphic groups of order n.

($\Leftarrow$) Assume $\gcd(n, \varphi(n)) = 1$, so $n = p_1 p_2 .....p_k$ and $p_i \nmid (p_j - 1)$ for all i, j, where $p_1, p_2..., p_k$ are distinct prime numbers.

We will prove by induction on k that $C_{p_1 p_2 .... p_k}$ is the only group of order $p_1 p_2 .... p_k$.

(1) If $k = 1$, then $n = p_1$, where p_1 is prime and we know that any group of prime order is isomorphic to C_{p_1}. Therefore, the result holds for $k = 1$.

(2) Assume by induction that the result holds for $k = r$, that is the only group of order $p_1 p_2 .... p_r$ (up to isomorphism) is $C_{p_1 p_2 .... p_r}$.

(3) Now want to prove the result for $k = r + 1$, where $r + 1 > 1$.

CLAIM: $|G|$ is odd.

PROOF THE CLAIM: Let us suppose $|G|$ is even. Then $|G| = 2p_2.....p_{r+1}$. Since $r+1 > 1$ there exists $p_2 > p_1 = 2$, so p_2 is an odd prime. Therefore $2|p_2 - 1$. So by Lemma 4.14 and Lemma 4.15 there are two non-isomorphic groups of order n. Therefore $|G|$ must be odd.

By the Feit-Thompson Theorem G is solvable. In particular $N_r \trianglelefteq G$. With out loss of generality let $|G/N_r| = p_1$, then $|N_r| = p_2....p_{r+1}$ and hence by induction we get $N_r \cong C_{p_2...p_{r+1}}$. By Cauchy's theorem, there exists an $x \in G$ such that $|x| = p_1$. Let $H = \langle x \rangle$ then $|HN_r| = \frac{|H||N_r|}{|H \cap N_r|} = \frac{p_1 p_2....p_{r+1}}{1} = |G|$. So since $H \cap N_r = 1$, $N_r \trianglelefteq G$ and $|HN_r| = |G|$, we have a semidirect product $G \cong N_r \rtimes_\psi H$ where $\psi : H \longrightarrow \mathrm{Aut}(N_r)$ is a homomorphism, and $\mathrm{Aut}(N_r) \cong (\mathbb{Z}_{p_2....p_{r+1}})^\times$, where $|(\mathbb{Z}_{p_2....p_{r+1}})^\times| = \varphi(p_2....p_{r+1}) = (p_2 - 1)(p_3 - 1).....(p_{r+1} - 1)$. Since $\gcd(|H|, |\mathrm{Aut}(N_r)|) = 1$, then by Lemma 3.2, $\psi(x) =$id. Hence $G \cong N_r \rtimes H \cong N_r \times H$ by Remark 4.13. Therefore, $G \cong N_r \times H \cong C_{p_2....p_{r+1}} \times C_{p_1} \cong C_{p_1.....p_{r+1}}$. Hence $C_{p_1 p_2....p_{r+1}}$ is the only group of order $p_1 p_2....p_{r+1}$. □

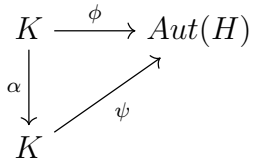
Here is an example of a unique group of given order.

EXAMPLE 5.7: Let $|G| = 255 = 3 \cdot 5 \cdot 17$. Then the only group of order 255 (up to isomorphism) is $C_{255} \cong C_3 \times C_5 \times C_{17}$ since $3 \nmid (5-1)$, $3 \nmid (17-1)$ and $5 \nmid (17-1)$.

6. TWO GROUPS OF A GIVEN ORDER

In this section we prove when there are exactly two groups of a given order up to isomorphism.

LEMMA 6.1: If there are $\phi, \psi : K \longrightarrow \text{Aut } (H)$ homomorphisms and there exists an automorphism $\alpha : K \longrightarrow K$ such that $\psi = \phi \circ \alpha$. Then $H \rtimes_\psi K \cong H \rtimes_\phi K$.



Proof. Consider $\Omega : H \rtimes_\psi K \longrightarrow H \rtimes_\phi K$ given by $\Omega(h, k) = (h, \alpha(k))$.

To show $H \rtimes_\psi K \cong H \rtimes_\phi K$ we need to check that Ω is a bijecttion homomorhism.

First we need to show that Ω is bijection. Since α is bijection, Ω is a bijection.

Now we need to check that Ω is a homomorhism.

$$\Omega((h_1, k_1) \cdot (h_2, k_2)) = \Omega(h_1\psi(k_1)(h_2), k_1k_2) = (h_1\psi(k_1)(h_2), \alpha(k_1k_2))$$

On the other hand,

$$\begin{aligned} \Omega(h_1, k_1) \cdot \Omega(h_2, k_2) &= (h_1\alpha(k_1)) \cdot (h_2\alpha(k_2)) \\ &= (h_1\phi(\alpha((k_1))(h_2), \alpha(k_1)\alpha(k_2)) \\ &= (h_1\psi(k_1)(h_2), \alpha(k_1k_2)) \end{aligned}$$

Hence $\Omega((h_1, k_1).(h_2, k_2)) = \Omega(h_1, k_1).\Omega(h_2, k_2)$. Thus Ω is homomorphism. We conclude that $H \rtimes_\psi K \cong H \rtimes_\phi K$. □

THEOREM 6.2: If $|G| = pq$ where $p < q$ are primes, then

1. If $p \nmid q-1$, then $G \cong C_p \times C_q$. Thus, there is only one group of order n up to isomorphism.

2. If $p \mid q-1$, then either $G \cong C_p \times C_q$, or $G \cong C_p \rtimes_\phi C_q$. Thus, there are exactly two groups of order n up to isomorphism.

Proof. When $p \nmid (q-1)$, this is Proposition 4.9. By the proof of Lemma 4.14, $G \cong C_q \rtimes_\phi C_p$ for some homomorphism ϕ, where $\phi : C_p \longrightarrow \text{Aut } (C_q) \cong (\mathbb{Z}_q)^\times$. There are p homomorphisms $\phi_i : C_p \longrightarrow (\mathbb{Z}_q)^\times$ given by $\phi_i(x) = r^i$, $0 \leq i \leq (p-1)$. Since ϕ_0 is trivial homomorphism, $C_q \rtimes_{\phi_0} C_p \cong C_q \times C_p$ and G is cyclic of order pq. Each ϕ_i for $i \neq 0$ gives a non-abelian group $C_q \rtimes_{\phi_i} C_p$. We now show that these are all isomorphic. The map $\alpha : C_p \longrightarrow C_p$ defined by $\alpha(x) = x^i$ is an isomorphism for $1 \leq i \leq (p-1)$ because $\gcd(i,p) = 1$, and $\phi_1 \circ \alpha = \phi_i$. By Lemma 6.2, $C_q \rtimes_{\phi_1} C_p \cong C_q \rtimes_{\varphi_i} C_p$ for $1 \leq i \leq (p-1)$. □

We now give an is an example of theorem 6.2.

EXAMPLE 6.3: Let $|G| = 21 = 7 \cdot 3$ where $3 < 7$ and both primes. We have $3|7-1$ hence there are two groups of order 21 which are $G \cong C_{21} \cong C_3 \times C_7$ and $G \cong C_7 \rtimes C_3$.

SPECIAL CASE: If $|G| = 2p$ where p is prime, then the groups of this order (up to isomorphism) are C_{2p} and D_{2p}.

THEOREM 6.4: If $|G| = p^2$ with p is prime, then there are exactly two groups of this order (up to isomorphism) namely C_{p^2} and $C_p \times C_p$.

Proof. Since $|G| = p^2$ with p is prime, then the center $|Z(G)| \neq 1$ by Theorem 2.29. In particular, by Lagrange's Theorem $|Z(G)| = p$ or p^2.

1. If $|Z(G)| = p^2$, then $G = Z(G)$, hence G is an abelian group.

2. If $|Z(G)| = p$ then $|G/Z(G)| = p^2/p = p$, thus $G/Z(G)$ is a cyclic by Theorem 2.22. Since $G/Z(G)$ is cyclic G is an abelian group by Theorem 2.30.

By the Fundamental Theorem of Finitely-Generated Abelian Groups, we may conclude, $G \cong C_{p^2}$ or $G \cong C_p \times C_p$. □

THEOREM 6.5: If $|G| = p^2q$ where p and q are distinct primes, such that $p \nmid q-1$ and $q \nmid p^2-1$ then there are exactly two groups of this order (up to isomorphism) namely C_{p^2q} and $C_p \times C_p \times C_q$.

Proof. Let $p \nmid q-1$ and $q \nmid p^2-1$ By Sylow's Theorem $n_p \equiv 1 \pmod{p}$ and $n_p|q$, so the divisors of q are 1 or q, but it cannot be q because by assumption $p \nmid q-1$. Therefore there is a unique Sylow p-subgroup denoted by H and $H \trianglelefteq G$. Similarly, by Sylow's Theorem $n_q \equiv 1 \pmod{q}$ and $n_q|p^2$, so $n_q = 1$, p, or p^2. Also since $q \nmid p^2-1$, then $n_q \neq p^2$. If $n_q = p$ then $q|p-1$ so $q|(p-1)(p+1)$ hence $q|p^2-1$ which is contradiction. Therefore $n_q = 1$. So there is a unique Sylow q-subgroup call it K and $K \trianglelefteq G$. By Lagrange's Theorem since the only divisor of $|H|$ and $|K|$ is $\{1\}$, $H \cap G = \{1\}$. Hence, $|HK| = \frac{|H||K|}{|H \cap K|} = |G|$. So $G = HK$. Since $H \trianglelefteq G$, $K \trianglelefteq G$, $HK = G$ and $H \cap K = 1$, then by Theorem 4.9, $G = H \times K$ and since $K \cong C_q$ and $H \cong C_{p^2}$ or $C_p \times C_p$ then $G \cong H \times K \cong C_{p^2} \times C_q$ or $G \cong H \times K \cong C_q \times C_p \times C_p$. □

Here is an example of Theorem 6.5

EXAMPLE 6.6: Let $|G| = 45 = 3^2 \cdot 5$ where 3 and 5 both primes. We have $3 \nmid 5-1$ and $5 \nmid 9-1$. Hence there are exactly two groups (up to isomorphism) of order 45 which are $G \cong C_{45} \cong C_9 \times C_5$ and $G \cong C_3 \times C_3 \times C_5 \cong C_{15} \times C_3$.

THEOREM 6.7: Let $|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$. Then there are exactly two groups (up to isomorphism) of order n if and only if:

I. All $\alpha_i = 1$, and $p_r|p_s - 1$ for exactly one pair (r, s) or

II. There is exactly one $\alpha_t = 2$, and all the rest are equal to 1 with $p_i \nmid p_t + 1$ and $p_i \nmid p_j - 1$ for any (i, j).

In case I, either $G \cong C_n$ or $G \cong (C_{p_s} \rtimes C_{p_r}) \times C_{n/p_r p_s}$, where $C_{p_s} \rtimes C_{p_r}$ is the unique nonabelian group of order $p_s p_r$ up to isomorphism from Theorem 6.2.
In case II, $G \cong C_n$ or $G \cong C_{p_t} \times C_{p_t} \times C_{n/p_t^2}$.

Proof. ($\Rightarrow$) We will prove this by contraposition for three cases:
Case A: If $\alpha_i = 1$ for all i, then we have two cases:

(a) Assume there are two pairs (r, s) and (r', s') such that $p_r | p_s - 1$ and $p_{r'} | p_{s'} - 1$. So we have $G \cong (C_{p_s} \rtimes C_{p_r}) \times C_{n/p_r p_s} = G_1$, $G \cong (C_{p'_s} \rtimes C_{p'_r}) \times C_{n/p'_r p'_s} = G_2$ or $G \cong C_n$. By Theorem 4.17 we have $Z(C_{p_s} \rtimes C_{p_r}) = \{1\}$ and $Z(C_{p'_s} \rtimes C_{p'_r}) = \{1\}$. By Theorem 4.16 $Z(G_1) \cong C_{n/p_r p_s}$ and $Z(G_2) \cong C_{n/p'_r p'_s}$. If $G_1 \cong G_2$, then $p_s p_r = p_{s'} p_{r'}$ hence we have two cases:

1. $p_r = p_{r'}$ and $p_s = p_{s'}$. This contradict the fact that $(p_r, p_s) \neq (p_{r'}, p_{s'})$.

2. $p_r = p_{s'}$ and $p_s = p_{r'}$. Now $p_{s'} = p_r < p_s = p_{r'} < p_{s'}$ implies $p_{s'} < p_{s'}$ which is contradiction.

(b) If there is no pair such that $p_r | p_s - 1$ then by Theorem 5.4 there is a unique group of order n.
Case B: If $\alpha_t = 2$ and $\alpha_i = 1$ for all $i \neq t$, then we have two cases:

(a) $p_i | p_j - 1$ for some i, j, so there are two abelian groups which are $C_{p_t} \times C_{p_t} \times C_{n/p^2}$ and $C_{p_{t^2}} \times C_{n/p^2}$ and a non-abelian group of order $p_i p_j$ winch is $C_{p_i} \rtimes C_{p_i} \times C_{n/p_i p_j}$.

(b) Assume $p_i | p_t + 1$. This implies p_i divides $|\mathrm{Aut}(C_{p_t} \times C_{p_t})| = |\mathrm{GL}_2(\mathbb{Z}_{p_t})| = (p_t^2 - 1)(p_t^2 - p_t)$ by Dummit and Foote [1, p.136]. By Cauchy's Theorem there is an $\alpha \in$ Aut $(C_{p_t} \times C_{p_t})$ of order p_i. Define $\phi : C_{p_i} \longrightarrow$ Aut $(C_{p_t} \times C_{p_t})$ by $\phi(x) = \alpha$. This is non trivial, so $(C_{p_t} \times C_{p_t}) \rtimes C_{p_i}$ is non-abelian. Hence we have $((C_{p_t} \times C_{p_t}) \rtimes C_{p_i}) \times C_{n/p_{t^2} p_i}$ is a third group of order n.

Case C: If $\alpha_r \geq 3$ or $\alpha_s, \alpha_r \geq 2$ for some r, s.

(a) Assume $\alpha_r \geq 3$, then we have three non-isomorphic abelian groups which are:

1. $C_{p_r} \times C_{p_r} \times C_{p_r} \times C_{n/p_r^3}$
2. $C_{p_{r^2}} \times C_{p_r} \times C_{n/p_r^3}$
3. $C_{p_{r^3}} \times C_{n/p_r^3}$.

(b) Assume $\alpha_s, \alpha_r \geq 2$, then we have four non-isomorphic abelian groups which are:

1. $C_{p_r} \times C_{p_r} \times C_{p_s} \times C_{p_s} \times C_{n/p_r^2 p_s^2}$
2. $C_{p_r^2} \times C_{p_s} \times C_{p_s} \times C_{n/p_r^2 p_s^2}$
3. $C_{p_r} \times C_{p_r} \times C_{p_s^2} \times C_{n/p_r^2 p_s^2}$
4. $C_{p_r^2} \times C_{p_s^2} \times C_{n/p_r^2 p_s^2}$.

($\Leftarrow$) We show that if either

1. All $\alpha_i = 1$, and $p_r | p_s - 1$ for exactly one pair (r, s) or
2. There is exactly one $\alpha_t = 2$, and all the rest are equal to 1 with $p_i \nmid p_t + 1$ and $p_i \nmid p_j - 1$ for any (i, j).

Then there are only two groups (up to isomorphism) of order n.

First we assume that all $\alpha_i = 1$, i.e $|G| = n = p_1 p_2 ... p_k$, and $p_r | (p_s - 1)$ for exactly one pair $(r.s)$. Note that $k \neq 1$ because if $k = 1$ then $|G| = p$ and there is only one group of order p. We will prove our claim by induction on k.

Base Case If $k = 2$ then we have $n = p_1 p_2$ and without loss of generality $p_1 | p_2 - 1$. The result follows by Theorem 6.2, part 2

Induction Hypothesis Assume the result holds for $m > 2$.

Inductive Step We want to prove it holds for $k = m + 1$. We have two cases:

(a) If n is even, so $n = 2pq....$ thus we have $2|p-1$ and $2|q-1$ which contradicts the uniqueness of (r, s).

(b) If n is odd, by the Feit-Thompson Theorem G is solvable and thus there is an $N \trianglelefteq G$ such that $|G/N| = p_i$, where $|N| = n/p_i = p_1p_2...p_{i-1}p_{i+1}....p_{m+1}$. By the usual argument, $G \cong N \rtimes_\psi C_{p_i}$ for some ψ.

(i) Suppose $p_i = p_r$. Since $|N| = p_1p_2....p_{r-1}p_{r+1}....p_{m+1}$ and $p_\alpha \nmid p_\beta - 1$ for any $p_\beta||N|$ and $p_\alpha||N|$, hence by Theorem 5.6 $N \cong C_{n/p_r}$.

Let $\psi : C_{p_r} \longrightarrow \mathrm{Aut}(C_{n/p_r}) \cong (\mathbb{Z}_{n/p_r})^\times = (\mathbb{Z}_{p_1})^\times \times (\mathbb{Z}_{p_2})^\times \times ..... \times (\mathbb{Z}_{p_{r-1}})^\times \times (\mathbb{Z}_{p_{r+1}})^\times \times .... \times (\mathbb{Z}_{p_k})^\times$ be a homomorphism, where $|(\mathbb{Z}_{n/p_r})^\times| = (p_1 - 1)(p_2 - 1)....(p_{r-1} - 1)(p_{r+1} - 1).....(p_{k+1} - 1).....(p_k - 1)$. Now $p_r|p_s - 1$ and $p_r \nmid p_j - 1$ for $j \neq s$, Therefore the action of C_{p_r} on C_{p_j} is trivial except possibly when $j = s$. Thus $C_{n/p_r} \rtimes_\psi C_{p_r} \cong C_n$ if ψ is trivial. $C_{n/p_r} \rtimes_\psi C_{p_r} \cong (C_{p_s} \rtimes C_{p_r}) \times C_{n/p_rp_s}$ if ψ is non-trivial

(ii) Suppose $p_i = p_s$, so we have $p_\alpha \nmid p_\beta - 1$ in N for any $p_\beta||N|$ and $p_\alpha||N|$, Theorem 5.6 implies $N \cong C_{n/p_s}$. Therefore $G \cong C_{n/p_s} \rtimes_\psi C_{p_s}$ where $\psi : C_{p_s} \longrightarrow \mathrm{Aut}(C_{n/p_s})$ is a homomorphism, $\mathrm{Aut}(C_{n/p_s}) = (\mathbb{Z}_{p_1p_2...p_{s-1}p_{s+1}...p_k})^\times$, and $|(\mathbb{Z}_{p_1p_2...p_{s-1}p_{s+1}...p_k})^\times| = (p_1 - 1)(p_2 - 1)...(p_{s-1} - 1)(p_{s+1} - 1)....(p_k - 1)$.

Since $\gcd(\mathrm{Aut}|N|, |K|) = 1$ then by Lemma 4.18 $G \cong C_{n/p_s} \rtimes C_{p_s} \cong C_{n/p_s} \times C_{p_s} \cong C_n$. Therefore, $G \cong C_{n/p_s} \times C_{p_s} \cong C_{p_1...p_{m+1}}$. Hence C_n is the only group of order $n = p_1p_2....p_k$ when $p_i = p_s$.

(iii) Suppose $p_i \neq p_r$ and $p_i \neq p_s$. We have $p_s||N|$ and $p_r||N|$. Since $|N|$ has m prime factors, by induction we have $N \cong C_{n/p_i} = N_1$ or $N \cong (C_{p_r} \rtimes C_{p_s}) \times C_{n/p_rp_sp_i} = N_2$. As usual $G \cong N \rtimes C_{p_i}$ for either choice of N.

Case 1: $N \cong N_1$. Since $\gcd(|C_{p_i}|, |\ \mathrm{Aut}(N_1)|) = 1$, by Lemma 4.18 $G \cong C_{n/p_i} \times C_{p_i} \cong C_n$.

Case 2: $N \cong N_2$. Now $\mathrm{Aut}((C_{p_s} \rtimes C_{p_r}) \times C_{n/p_rp_sp_i}) \cong \mathrm{Aut}(C_{p_s} \rtimes C_{p_r}) \times \mathrm{Aut}(C_{n/p_rp_sp_i})$. We have $|\mathrm{Aut}(C_{p_s} \rtimes C_{p_r})| = (p_r - 1)p_r$ (Walls, p 459-462). Hence

$|\mathrm{Aut}((C_{p_s} \rtimes C_{p_r}) \times C_{n/p_r p_s p_i})| = p_r(p_r-1)(p_1-1)(p_2-1).....(p_r-1)...(p_s-1)...(p_k-1)$. By the hypothesis p_i does not divide any of these factors. So by Lemma 4.18, $G \cong ((C_{p_s} \rtimes C_{p_r}) \times C_{n/p_r p_s p_i}) \times C_{p_i} \cong (C_{p_s} \rtimes C_{p_r}) \times C_{n/p_r p_s}$.

Now we will prove the second part (II) of the theorem. Assume there is exactly one $\alpha_t = 2$, and all the rest are equal to 1 with $p_i \nmid p_t + 1$ and $p_i \nmid p_j - 1$ for any (i, j):

We prove this part by induction on k.

Base Case: If $k = 1$, then $|G| = p^2$ and hence G is abelian, then $G \cong C_p \times C_p$ or $G \cong C_{p^2}$ by Fundamental Theorem of Finitely-Generated Abelian Groups.

Note: If $k > 1$, the hypotheses imply n is odd.

Induction Step: Let $k > 1$, so n is odd , hence G is solvable, so $N \trianglelefteq G$. Since $|N| = n/p_i = p_i p_2 ... p_{i-1} p_{i+1} ... p_k$, we have two cases

(i) If $p_i = p_t$, then $|N| = n/p_t = p_i p_2 ... p_t ... p_k$, where $[G : N] = p_t$. Choose $x \in G \setminus N$, then $x^{p_t} \in N$. We have $N \cong C_{n/p_t} = \{y\}$. Then $xyx^{-1} = y^a$, therefore $y = x^{p_t} y s^{-p_t} = y^{a^{p_t}}$. Hence $a^{p_t} = 1 \mod p_i p_2 .... p_t ... p_k$. Therefore the $|a| = 1$ or p_t. Since the order of a in $|(\mathbb{Z}_{p_1 p_2 ... p_k})^\times| = (p_1 - 1)(p_2 - 1).....(p_k - 1)$. So $|a| = 1$ Therefore $xy = yx$.

(ii) If $p_i \neq p_t$ then by induction $N \cong C_{n/p_i} \cong C_{p_t^2} \times C_{n/p_t^2 p_i}$ or $N \cong C_{p_t} \times C_{p_t} \times C_{n/p_t^2 p_i}$. By Cauchy's Theorem there exists a subgroup isomorphic to C_{p_i}. Assume we have $G \cong N \rtimes_\psi C_{p_i}$,where $\psi : C_{p_i} \longrightarrow \mathrm{Aut}(N)$.

If $N \cong C_{n/p_i}$, $|\mathrm{Aut}(C_{n/p_i})| = |\mathrm{Aut}(C_{p_1})| \cdot |\mathrm{Aut}(C_{p_2})| \cdot .... \cdot |\mathrm{Aut}(C_{p_t^2})| \cdot ..... \cdot |\mathrm{Aut}(C_{p_k})|$. So $|\mathrm{Aut}(C_{n/p_i})| = (p_1-1)(p_2-1)...\widehat{(p_i-1)}....p_t(p_t-1)....(p_k-1)$. Since p_i does not divide any of these factors, by Lemma 4.18, $C_{n/p_i} \times C_{p_i} \cong C_n$.

If $N \cong C_{p_t} \times C_{p_t} \times C_{n/p_t^2 p_i}$, $|\mathrm{Aut}(C_{p_t} \times C_{p_t}) \times (C_{n/p_t^2 p_i})| = |GL_2(\mathbb{Z}_{p_t})| \cdot |(\mathbb{Z}_{n/p_t^2 p_i})^\times| = (p_t^2-1)(p_t^2-p_t)(p_1-1)(p_2-1).....\widehat{(p_i-1)}....(p_k-1) = p_t(p_t-1)^2(p_t+1)(p_1-1)(p_2-1).....\widehat{(p_i-1)}....(p_k-1)$. Since p_i does not divide any of these factors, by Lemma 4.18, $G \cong C_{p_t} \times C_{p_t} \times C_{n/p_t^2 p_i} \times C_{p_i}$. □

Below are examples of theorem 6.7

EXAMPLE 6.8:

1. Let $|G| = 165 = 3 \cdot 5 \cdot 11$. Then there are two groups of order 165 (up to isomorphism) which are $C_{165} \cong C_3 \times C_5 \times C_{11}$ and $(C_{11} \rtimes C_5) \times C_3$ since $5|(11-1)$, but $3 \nmid (5-1)$ and $3 \nmid (11-1)$

2. Let $|G| = 2275 = 5^2 \cdot 7 \cdot 13$. Then there are two groups of order 2275 up to isomorphism namely $C_{2275} \cong C_{25} \times C_7 \times C_{13}$ and $C_5 \times C_5 \times C_7 \times C_{13}$ since $7 \nmid (5+1)$, $13 \nmid (5+1)$, $7 \nmid (13-1)$, $5 \nmid (3-1)$ and $5 \nmid (7-1)$.

7. CONCLUSION

Let $f(m)$ be the number of groups of order m up to isomorphism. For example $f(15) = 1$ and $f(21) = 2$. In this thesis we have characterized these m for which $f(m) = 1$ (Theorem 5.6) and for which $f(m) = 2$ (Theorem 6.7).

One future research topic would be determine when $f(m) = 3$ or $f(m) = 4$, i.e. there are exactly three groups and exactly four groups of order m up to isomorphism.

One may ask if for every n is there an m such that $f(m) = n$?. For instance, can we find m such that $f(m) = 5$? Yes, $f(8)$ is the number of non isomorphism groups of order 8 is 5 namely C_8, $C_3 \times C_4$, $C_2 \times C_2 \times C_2$, D_8, and Q_8. Experimental evidence indicates the answer is yes for all n, but this is another topic for future research.

REFERENCES

[1] D. Dummit, and F. Foote, Abstract Algebra (3rd ed), John Wiley, 2004.

[2] T.W. Hungerford, Abstract Algebra: An Introduction (3rd ed), Brooks Cole, 2013

[3] H. E. Rose, A Course on Finite Groups, Springer, 2010

[4] G.L. Walls, Automorphism Groups, American Mathematical Monthly, v.93. 459-462.