Al-TAHADI UNIVERSITY
FACULTY OF SCIENCE
Department of Mathematics

Presentation of finite groups of small order

A dissertation submitted to the department of mathematics in partial fulfillment of the requirements for the degree of Master of Science in mathematics

By

Mohmad K.M.Said

Revised and supervised by

Dr. Shaban A. Traina

Spring 2006

الجماهيرية العربية الليبية الشعبية الاشتراكية العظمى
جامعة التحدي
سرت

إن الدراسة ليست غاية في حد ذاتها
و إنما الغاية هي خلق الإنسان النموذجي الجديد

التاريخ : ....
الموافق : ..10..1..2007.. ف
الرقم الاشاري : ك ع / 13 / 1 /

Faculty of Science

Department of Mathematics

Title of Thesis

((Presentation of Finite Groups of Small Order))

By

Mohmad K. M. Said

Approved by:

Dr. Shaban A. Traina ....
(Supervisor)

Dr. Ibrahim A. Tentush ....
(External examiner)

Dr. . Ameer Abdul M. Jaseem ....
(Internal examiner)

Countersigned by:

Dr. Mohamed Ali Salem

(Dean of Faculty of Science)

w.altahadi.edu.ly

altahadi.edu.ly 674 ✉ 054 / 60361 - 62151 ☏ 054 / 60363 - 65704 ☎

بسم الله الرحمن الرحيم

يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات

والله بما تعملون خبير

صدق الله العظيم

سورة المجادلة

Acknowledgment

I am grateful to my teacher

Dr. Shaban A. Traina

Who teach; supervise and guide me during training period.

A large debt of gratitude is owed to him for revising most efficiently and patiently for this work.

I am also indebted to all specialist teachers who have helped me when I was working in their units.

M.Sc
Mohmad K.M.Said

Dedication

To my beloved Palestinians and the precious Libya.

To Palestinians, Iraqis and Lebanese martyrs.

To every one who is eligible to friendship.

Mohmad K.M.Said

Contents

INTRODUCTION

The term group was used by Galois around 1830 to describe sets of one-to-one function on finite sets that could be grouped to form a closed set. As is the case with most fundamental concepts in mathematics, the modern definition of a group that follows is the result of a long evolutionary process.

In word, a group is a set together with an associative operation such that there is an identity, every element has an inverse, and any pair of elements can be combined without going outside the set.

In this project, we derive several important arithmetic relationships between a group and certain of its subgroups. Recall that the converse of Lagrange's theorem is false on the other hand, Sylow'theorems give a necessary condition for the existence of subgroup. Numerical examples discussed in this project makes the Sylow theorems is an important result in finite group theory. Other important concepts are the direct and semi-direct product of groups which show how to piece together groups to make larger groups. Our project is to start with one large group and decompose it into a product of smaller groups. These methods are useful to give us a simple way to construct all finite groups.

We also present a convenient way to define a group with certain prescribed properties. We simply begin with a set of elements that generate the group and a set of equations called relations that specify the condition that these generators are to satisfy. This way determines the group up to isomorphism.

CHAPTER 1

PRELIMINARIES

In this chapter, a basic algebraic structure called group is introduced and some important definitions, lemmas, theorems and examples are given.
The references of the following material are [2],[3],[4],[5],[7],[11],[12].

Definition 1.1:

A group is a nonempty set G on which there is defined a binary operation $(a, b) \to ab$ satisfying the following properties.

- *Closure*: If a and b belong to G, then ab is also in G;
- *Associativity*: $(ab)c = a(bc)$ for all $a,b,c \in G$;
- *Identity*: There is an element $e \in G$ such that $ae = ea = a$ for all $a \in G$.
- *Inverse*: If $a \in G$, then there is an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

A group G is called *abelian* if the binary operation is commutative, i.e., $ab = ba$ for all $a,b \in G$.

Lemma 1.1:

If G is a group then:

1. Its identity is unique.
2. Every $a \in G$ has a unique inverse $a^{-1} \in G$.
3. If $a \in G$, then $(a^{-1})^{-1} = a$.

4. For $a,b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

By the associative law, products of any finite number of elements of a group G in a certain order are meaningful. Thus one may define the powers of an element a of G as follows:

For any positive integer n,

$$a^n = \underbrace{aa\ldots a}_{n}, a^0 = 1, a^{-n} = \left(a^{-1}\right)^n.$$

Obviously we have

$$a^m a^n = a^{m+n} \text{ and } \left(a^m\right)^n = a^{mn} \text{ for any integers } m,n.$$

Definition 1.2:

The group G is called *finite* if $|G|$ is a positive integer; otherwise G is called *infinite*.

Definition 1.3:

The order of an element a of a group G is the least positive integer n such that $a^n = e$, where e is the identity element in G and it is denoted by $o(a)$ or $|a|$.

Theorem 1.1:

If every non-identity element of a group G has order 2, then G is abelian.

Proof:

Let $a,b \in G$ such that $a \neq e \neq b$ where $a^2 = e = b^2$.

$\therefore \quad (ab)^2 = e$ and $\quad a^2b^2 = ee = e$.

$(ab)(ab) = a^2b^2$.

$abab = aabb$.

$(a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1})$.

$\therefore\ ba = ab \quad \forall \quad a,b \in G$.

Definition 1.4:

Let $(G_1,\circ)$ and $(G_2,*)$ be two groups, then a function $f:(G_1,\circ) \to (G_2,*)$ is called a group homomorphism if $f(x \circ y) = f(x) * f(y) \quad \forall \quad x,y \in G_1$.

Definition 1.5:

Two groups $(G_1,\circ)$ and $(G_2,*)$ are isomorphic if there exist a function $f:(G_1,\circ) \to (G_2,*)$ such that:

1. f is one –to –one, and onto.
2. $f(x \circ y) = f(x) * f(y)\ \forall\ x,y \in G_1$

This is denoted by $G_1 \cong G_2$.

Definition 1.6:

Let G be a group and H a subset of G, then H is called a subgroup of G if H is a group.

Definition 1.7:

If G is a group, then $\{e\}$ and G are improper (or trivial) subgroups of G. All other subgroups are proper (or non-trivial) subgroups.

Proposition 1.1:

Let G be a group and H a nonempty subset of G. Then the following statements are equivalent:

i. $H \leq G$;

ii. $ab \in H$ *and* $a^{-1} \in H$ *for any* $a,b \in H$;

iii. $ab^{-1} \in H$ (*or* $a^{-1}b \in H$) *for any* $a,b \in H$.

iv. $H^2 \subseteq H$ (if G is finite).

The intersection of a collection of subgroups of a group G is also a subgroup of G, but the union of several subgroups is not necessarily a subgroup.

Definition 1.8:

Let G be a group and $M \subseteq G$. The intersection of all subgroups of G containing M is called the *subgroup generated by* M, denoted by $\langle M \rangle$, i.e.

$$\langle M \rangle = \bigcap_{i \in I} \{H_i : H_i \leq G, M \subseteq H_i\}.$$

Remark 1.1:

In checking that the inverse of an element of $\langle A \rangle$ also belongs to $\langle A \rangle$, we use the fact that

$$(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}.$$

Definition 1.9:

For any $N \leq G$ and any $g \in G$ let $gN = \{gn : n \in N\}$ and $Ng = \{ng : n \in N\}$

called respectively a *left coset* and a *right coset* of N in G. Any element of a *coset* is called a *representative* for the coset.

Remark 1.2:

If H is a subgroup of an abelian group G and $a \in G$, then $aH = Ha$.
Observe that $eH = H = He$ and that $a = ae \in aH$ and $a = ea \in Ha$.

In general

$$aH \neq Ha.$$

Theorem 1.2:

Let H be a subgroup of a group G and $a, b \in G$. Then

1. $aH = bH$ if and only if $b^{-1}a \in H$.
2. $Ha = Hb$ if and only if $ab^{-1} \in H$.

Definition 1.10:

If H is a subgroup of a group G, then G is equal to the union of all right (or left) cosets of H in G.

i.e. $G = a_1H \bigcup a_2H \bigcup \ldots \bigcup a_nH$, where $a_1, a_2, \ldots, a_n \in G$.

Theorem 1.3:

If $H \leq G$, then $Ha = aH = H$, $\forall \quad a \in H$.

Note that :

$$Ha = H \quad \textit{iff} \quad a \in H.$$

Definition 1.11:

Two sets A and B are disjoint if $A \bigcap B = \phi$.

Definition 1.12:

If $H \leq G$,then the number of left (right) cosets of H in G is finite .
The number of disjoint left (right) cosets of H in G is called the index of H in G, denoted by $[G:H]$.

The following theorem is a basic property of subgroups of a finite group.

Theorem 1.4 : (Lagrange's theorem)

If G is a finite group and H is a subgroup of G , then the order of H divides the order of G $(|G|/|H|)$ and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.

Theorem 1.5:

If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular $x^{|G|} = e$ for all x in G.

Definition 1.13:

A subgroup N of a group G is said to be a *normal* subgroup of G if $xnx^{-1} \in N \ \forall \ n \in N$ and $x \in G$, this denoted by $N \triangleleft G$.

Remark 1.3:

Every subgroup of an abelian group is a normal. And any group G has at least two normal subgroups, that is G and $\{e\}$, called *the trivial* normal subgroups.

Lemma 1.2:

Let $N \leq G$, then N is a normal subgroup of G iff

1. $xNx^{-1} = N \quad \forall \quad x \in G$.

Definition 1.14:

Let n be a fixed positive integer .Define a relation ~ on Z by $a \sim b$ *iff* $a \equiv b(\bmod n)$ Clearly ~ is an equivalence relation. We shall denote the equivalence class of a by $[a]$ this is called the congruence class of residue class of a modulo n and consists of all integers which congruent to a modulo n, *i.e.* $[a] = \{b \in Z \mid a \equiv b(\bmod n)\}$.

$$= \{a, a \pm n, a \pm 2n, \ldots\}.$$

The set of equivalence classes under this equivalence relation will be denoted by Z_n and called the set of integers modulo n .

Note that :

$$Z_n = \{[0],[1],[2],\ldots,[n-1]\}$$

Definition 1.15:

Let G be a group and $H \lhd G$, then the quotient group is defined by

$G/H = \{aH : a \in G\}$, all left cosets of H in G with a binary operation defined on G/H as follows:

$$aHbH = abH \quad \forall \quad aH, bH \in G/H.$$

Theorem 1.6:

A quotient group of an abelian group is abelian .

Definition 1.16:

Let $G_1, G_2, \ldots, G_n$ be groups, then the Cartesian product

$X_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$.

Can be made into a group under the following operation:

$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$.

Where $(x_1, x_2, \ldots, x_n)$, $(y_1, y_2, \ldots, y_n) \in X_{i=1}^{n} G_i$ and $X_{i=1}^{n} G_i$ is called the external direct product of $G_1, G_2, \ldots, G_n$.

Remark 1.4:

1. $\left| X_{i=1}^{n} G_i \right| = X_{i=1}^{n} |G_i|$.
2. $X_{i=1}^{n} G_i$ is abelian if G_i is abelian for each $i = 1, 2, \ldots, n$.

Definition 1.17:

Let G be a group and $H, K \leq G$. Define

$$HK = \{hk : h \in H, k \in K\}.$$

Theorem 1.7:

Let G be a group, and let H and K be two subgroups of G. Then

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

Definition 1.18:

Let $H, K \lhd G$, then G is called the internal direct product of H and K written $G = H \otimes K$, if $G = HK$ and $H \cap K = \{e\}$.

Theorem 1.8:

Let H and K be normal subgroups of the finite group G with $|G| = |H|.|K|$.
If either $G = HK$ or $H \bigcap K = \{e\}$, then $G = H \otimes K$.

Theorem 1.9:

Let G be a group with normal subgroups H and K such that $G = H \otimes K$.
Then $G \cong H \times K$.

Definition 1.19:

A group G is said to be a *semidirect product* of the subgroups N and K written $N \rtimes K$ if

- N is normal in G ;
- $N \bigcap K = \{e\}$; and
- $NK = G$.

Note that:

K is not necessarily a normal subgroup of G.

Definition 1.20:

Let p be a prime number. An element a of a group G is called a p-*element* if its order $o(a)$ is a power of p.

Lemma 1.3:

Let G be a finite group and $H \leq G$, then :

1. if $[G:H] = 2$, then $H \lhd G$.
2. if $[G:H] = p$ and p is the smallest prime dividing $|G|$, then $H \lhd G$.

3. if $|G|=2r$, $r=$ odd, then G has a normal subgroup of index 2.

4. if H is a Sylow p-subgroup and $n_p=1$, then $H \lhd G$.

Lemma 1.4:

Any group of order $2p$, where p is a prime number has a normal subgroup of order p.

Definition 1.21:

Let G be a group and a be an element of G. Then the *centralizer* or *normalizer* of a in G, denoted by $C(a)$, is the set of all elements of G which commute with a,

i.e. $$C(a)=\{b \in G : ba=ab\}.$$

Note that:

- The center of G is abelian.
- G is abelian iff *cent* $G=G$.
- *cent* $G \lhd G$.

Theorem 1.10:

If G is a finite p-group with more than one element, then *cent* $G \neq \{e\}$.

Definition 1.22:

Let G be a group and let p be a prime.

- A group of order p^{α} for some $\alpha \geq 1$ is called a *p-group*. Subgroups of G which is a p-group are called *p-subgroups*.

- If G is a group of order $p^{\alpha}m$, where p is a prime not dividing m, then a subgroup of order p^{α} is called a *Sylow p-subgroup* of G.
- The set of Sylow *p*-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow *p*-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from the context).

Theorem 1.11: (sylow's theorems)

Let G be a group of order $p^{\alpha}m$, where p is a prime not dividing m.

1. Sylow *p*-subgroup of G exist, i.e., $Syl_p(G) \neq \phi$.
2. If P is Sylow *p*-subgroup of G and Q is any *p*-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow *p*-subgroups of G are conjugate in G.
3. The number of Sylow *p*-subgroups of G is of the form $1 + kp$,

   i.e. $$n_p \equiv 1 (\mathrm{mod}\ p).$$

Further, n_p is the index in G of the normelizer $N_G(P)$ for any Sylow *p*-subgroup P, hence n_p divides m.

CHAPTER TWO

FINITE GROUPS

Before discussing cyclic groups further we prove that the various properties of finite cyclic groups.

The references of the following material be [1],[6],[8],[9],[10],[11].

Section 2.1 some Important Finite Groups

2.1.1 Cyclic Groups

Definition 2.1.1:

If $a \in C$, then the subgroup $\langle a \rangle = \{ a^n : n \in Z \}$ is called the *cyclic subgroup* of C generated by a, If $\langle a \rangle = C$, then we say that C is a *cyclic group* and that a is a *generator* of C.

Remark 2.1.1:

A finite cyclic group C_n of order n is presented by

$C_n = \langle a \rangle = \{ a : a^n = e \}$.

The element of C_n are of the from $C_n = \{ e, a, a^2, \ldots, a^{n-1} \}$.

And $o(a^r) = \frac{n}{(n,r)}$.

Note that : There may exist more than one generator of a cyclic group.

Lemma 2.1.1:

1. if a is a generator of a cyclic group G then a^{-1} is also a generator of G.
2. the order of a cyclic group is equal to the order of any generator of the group.

Lemma 2.1.2:

Any two cyclic groups of the same order are isomorphic.

Lemma 2.1.3:

Let G be a cyclic group, generated by a. Then G is abelian.

Theorem 2.1.1:

Every subgroup of a cyclic group is cyclic.

Proof:

Suppose that $G = \langle G \rangle = \{g^k : k \in Z\}$ is a cyclic group and let H be a subgroup of G. If $H = \{e\}$, then H is cyclic, so we assume that $H \neq \{e\}$, and let $g^k \in H$ with $g^k \neq e$. Then, since H is a subgroup, $g^{-k} = (g^k)^{-1} \in H$. Therefore, since k or $-k$ is positive, H contains a positive power of g, not equal to e. So let m be the smallest positive integer such that $g^m \in H$. Then, certainly all powers of g^m are also in H, so we have $\langle g^m \rangle \subseteq H$. We claim that this inclusion is equality.

To see this, let g^k be any element of H (recall that all elements of G, and hence H, are powers of g since G is cyclic). By the division algorithm, we may write $k = qm + r$ where $0 \leq r < m$. But

$$g^k = g^{qm+r} = g^{qm} g^r = (g^m)^q g^r \quad \text{so that} \quad g^r = (g^m)^{-q} g^k \in H.$$

Since m is the smallest positive integer with $g^m \in H$ and $0 \leq r < m$, it follows that we must have $r = 0$. Then $g^k = (g^m)^q \in \langle g^m \rangle$. Hence we have shown that $H \subseteq \langle g^m \rangle$ and hence $H = \langle g^m \rangle$. That is H is cyclic with generator g^m where m is the smallest positive integer for which $g^m \in H$.

Theorem 2.1.2:

Every quotient group of a cyclic group is cyclic.

Theorem 2.1.3:

If $\gcd(m,n)=1$, then $C_m \times C_n \cong C_{mn}$.

Lemma 2.1.4:

If numbers m_i for $i = 1,2,\ldots,n$ are such that the *gcd* of any two of them is equal to 1, then $X_{i=1}^{n} C_{m_i}$ is cyclic and isomorphic to $C_{m_1 m_2 \ldots m_n}$.

Remark 2.1.2:

The preceding lemma shows that if G is a finite group of order n which is written as a product of powers of distinct prime numbers, as in $n=(p_1)^{r_1}(p_2)^{r_2}\ldots(p_r)^{r_r}$,

then C_n is isomorphic to

$$C_{(p_1)^{r_1}} \times C_{(p_2)^{r_2}} \times \ldots \times C_{(p_r)^{r_r}}.$$

Lemma 2.1.5:

A finite abelian group G of order n is isomorphic to a direct product $C_{m_1} \times C_{m_2} \times \ldots \times C_{m_r}$ where m_{i+1} divides m_i and $m_1 m_2 \ldots m_r = n$.

General Dihedral Group

Definition 2.1.2:

The general dihedral group D_n is presented by two generators as follows:

$D_n = \langle a,b \ : a^n = b^2 = e \ , \ ba = a^{n-1}b \rangle$, $n = 2,3,4,\ldots$ $|D_n| = 2n$.

D_n is a non abelian group for $n \geq 3$.

Remark 2.1.3:

D_n can be written as a semidirect product of $C_n = \langle a \rangle$ by $C_2 = \langle b \rangle$, i.e.

$D_n = \langle a \rangle \rtimes \langle b \rangle = C_n \rtimes C_2$.

$\therefore \; D_n \cong C_n \rtimes C_2$.

Theorem 2.1.4:

$D_{2n} \cong D_n \times C_2$ for n is odd.

Proof:

$G = D_{2n} = \langle a, b : a^{2n} = b^2 = e, ba = a^{-1}b \rangle$. Take $H = \langle a^2, b \rangle$.

$(a^2)^n = e$, $b^2 = e$, $ba^2 = a^{-2}b = (a^2)^{-1} b$.

$\therefore \; H \cong D_n$.

Let $K = \langle a^n \rangle$.

$\because K \lhd G$, since $ba^n b^{-1} = a^n \in K$ and $a^2 a^n a^{-2} = a^n \in K$.

$\because H \bigcap K = \{e\}$.

$\therefore |H||K| = 2n \times 2 = 4n = |D_{2n}|$.

$\therefore \; D_{2n} \cong D_n \times C_2$.

General Quaternion Group

For $n \geq 3$, $Q_n = \{ a, b \mid a^{2^{n-1}} = e, \; b^2 = a^{2^{n-2}}, \; ba = a^{-1}b \}$, $|Q_n| = 2^n$.

Q_n is a non-abelian group for all n.

Note that :

$$Q_3 \not\cong D_4 , \; Q_4 \not\cong D_8 \text{ and } Q_5 \not\cong D_{16}.$$

Symmetric Groups S_n

Definition 2.1.3:

A *permutation* of a set A is a one-to-one and onto function $f : A \to A$.

Note that :

The set of all permutation of A is denoted by S_A. S_A is a group with respect to the composition of functions.

Definition 2.1.4:

Let $A = \{1, 2, \ldots, n\}$. The group S_n of all permutations of the set $\{1, 2, \ldots, n\}$ is called the *symmetric group*.

Note that :

a) $|S_n| = n!$

b) S_n is non-abelian for $n \geq 3$.

c) Elements of S_n are written in the form :

$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$, where $i_1, i_2, i_3, \ldots, i_n \in \{1, 2, \ldots, n\}$ and $i_1, i_2, i_3, \ldots, i_n$ are distinct.

Definition 2.1.5:

Let S be a set, and let $a_1, a_2, \ldots, a_n$ be distinct elements of S. A permutation of S that sends a_i to a_{i+1} for $i = 1, 2, \ldots, n-1$, and sends a_n to a_1 is called a *cycle* of order n, or n*-cycle* and is denoted by $(a_1, a_2, \ldots, a_n)$, where

$$(a_1, a_2, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}.$$

Note that:

$$S_3 \cong D_3 \text{ and } S_4 \ncong D_{12}.$$

Theorem 2.1.5: (Cayley theorem)

Any group is isomorphic to a group of permutation.

i.e. Any group is isomorphic to a subgroup of a symmetric group.

Alternating Group A_n

Definition 2.1.6:

The permutation is called even if it's the product of an even number of transposition. Otherwise is called *odd*.

Remark 2.1.4:

The product of two even permutations is an even permutation; also the inverse of an even permutation is even.

Definition 2.1.7:

For each integer n satisfying $n > 1$, the alternating group A_n is the subgroup of the symmetric group S_n consisting of all even permutation of the set $\{1, 2, \ldots, n\}$.

i.e. $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$.

Note that :

1. $|A_n| = n!/2$.
2. $A_n \lhd S_n$.
3. A_n is non-abelian for $n \geq 4$.
4. $A_3 \cong C_3$, $A_4 \ncong Q_6$ and $A_4 \ncong D_6$.

Section 2.2 Some Finite Groups of Special Orders

Groups of order p

Theorem 2.2.1:

Any group of order p, where p is a prime number, is cyclic and isomorphic to C_p.

Proof:

Let G be a finite group of order p. *i.e.* $|G| = p$.

Let $a \in G$ such that $a \neq e$.

$\because\ |a| \setminus |G|$.

$\therefore\ |a| \setminus p$.

$\therefore\ |a| = 1$ or $|a| = p$.

But $|a| \neq 1$ since $a \neq e$.

$\therefore\ |a| = p$.

Therefore $G = \langle a \rangle$

$\therefore\ G$ is a cyclic group.

And we know that any two cyclic groups of the same order are isomorphic.

$\therefore\ G \cong C_p$.

Groups of order p^2

Theorem 2.2.2:

Any group of order p^2, where p is a prime number, is abelian.

Proof:

Let G be a group with $|G| = p^2$.

Since *cent* $G \neq \{e\}$ (by theorem 1.10), then $|centG| \neq 1$ and $|centG| \setminus |G|$.

$\therefore\ |centG| = p$ or $|centG| = p^2$.

If $|centG| = p$ so $centG \lhd G$, then $|G/centG| = p$, whence $G/centG$ is cyclic.

Let $G/centG$ be generated by the coset a $cent\ G$.

Then a typical element of $G/centG$ has the form $a^n centG$ for some integer n.

Let $x, y \in G \Rightarrow x = a^n c,\ y = a^m c'$, where $m, n \in Z$ and $c,\ c' \in\ cent\ G$.

$xy = a^n c a^m c' = a^{n+m} cc' = a^{m+n} c'c = a^m c' a^n c = yx$.

$\therefore\ xy = yx \quad \forall \quad x, y \in G.$

Therefore G is commutative which implies that $G = cent\ G$ and so

$cent\ G$ has order p^2 , a contradiction.

This leaves only the possible that $|centG| = p^2$ which implies that G is commutative.

Note that :

If $|G| = p^2$, then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.

Groups of order p^3

Lemma 2.2.1:

Any abelian group of order p^3, where p is a prime number is isomorphic to C_{p^3}, $C_{p^2} \times C_p$ or $C_p \times C_p \times C_p$.

Lemma 2.2.2:

Any non-abelian group of order p^3, where p is an odd prime number is isomorphic to the group with a presentation either.

i. $\{a, b, c \mid a^p = b^p = c^p = e\ ,\ ab = cac^{-1},\ ba = ab,\ bc = cb\}$, or

ii. $\{a, b \mid a^{p^2} = e,\ b^p = e,\ ba = a^{p+1} b\}$.

Note that :

The previous lemma is not applicable for any non-abelian group of order $2^3 = 8$, where $p = 2$, this case will be discussed in the following chapter.

Groups of order pq

Theorem 2.2.3:

Let p and q be prime numbers, where $p < q$ and $q \not\equiv 1 (\bmod\ p)$. Then any group of order pq is cyclic.

Proof:

Let G be a group of order pq. *i.e.* $|G| = pq$.

Then G contains Sylow subgroups N_p and N_q of orders p and q respectively.

Let n_p be the number of N_p, then $n_p \mid pq$ and $n_p \equiv 1 (\bmod\ p)$.

Clearly $p \nmid n_p$, and therefore either $n_p = 1$ or $n_p = q$. But $q \not\equiv 1 (\bmod\ p)$. Then $n_p = 1$ which implies that $N_p \lhd G$.

A similar argument shows that $N_p \lhd G$, since $p < q$ and therefore $p \not\equiv 1\ (\bmod\ q)$.

Now $N_p \cap N_q \leq N_p$ and $N_p \cap N_q \leq N_q$.

$\therefore\ |N_p \cap N_q| \mid p$ and $|N_p \cap N_q| \mid q$ (by Lagrange's theorem)

Therefore $|N_p \cap N_q| = 1$ and $N_p \cap N_q = \{e\}$ $\rightarrow (1)$

$$|N_p N_q| = \frac{|N_p||N_q|}{|N_p \cap N_q|} = |N_p||N_q| = pq = |G| \qquad \rightarrow (2)$$

Also since any group whose order is prime number must be cyclic, then the groups N_p and N_q are cyclic.

$\therefore\ N_p \cong C_p$ and $N_q \cong C_q$ $\rightarrow (3)$

From (1), (2) & (3) we get:

$G \cong C_p \times C_q \cong C_{pq}$ (by theorem 2.1.6)

$\therefore\ G \cong C_{pq}$.

Note that :

If $p|q-1$, where $p < q$, then the previous theorem is not applicable. Group of this type will be discussed in the following chapter.

<u>**Groups of order**</u> $2p$

<u>**Theorem 2.2.4:**</u>

Any group of order $2p$, where p is a prime number, is isomorphic to either C_{2p} or D_p.

Proof:

Let G be a group of with $|G| = 2p$.

If p is an even prime, then $|G| = 2(2) = 2^2 = 4$.

$\therefore\ G \cong C_2 \times C_2 \cong D_2$ or $G \cong C_4$.

If p is a prime number greater than 2, then the group G contains elements x and y whose orders are 2 and p respectively (by First Sylow theorem)

$\therefore\ \exists\ N \le G$ where $N = \langle y \rangle$ which is a *Sylow* p*-subgroup* of G.

Let n_p be the number of *Sylow* p*-subgroup* of G such that $n_p|2p$ and $n_p \equiv 1 (\text{mod } p)$.

$\therefore\ n_p = 1$ ($\because$ 2, p and $2p$ are not congruent to 1 modulo p).

$\therefore\ N \lhd G$.

Now consider the element $xyx^{-1} \in G$.

$\therefore\ xyx^{-1} \in N \quad (\because N \lhd G)$.

Therefore $xyx^{-1} = y^k$ for some integer k.

Moreover $p \nmid k$ ($\because$ xyx^{-1} is not identity element of G).

$\therefore\ y^{k^2} = \left(y^k\right)^k = (xyx^{-1})^k = xy^k x^{-1} = x(xyx^{-1})x^{-1} = x^2 y x^{-2}$.

But $x^2 = x^{-2} = e$, since x is an element of order 2.

$\therefore\ y^{k^2}=y \ \Rightarrow\ y^{k^2-1}=e$.

But $p|\, k^2-1$, since y is an element of order p.

Moreover $k^2-1=(k-1)(k+1)$, then either $p|\,(k-1)$, in which case $xyx^{-1}=y$,

or else $p|\,(k+1)$, in which case $xyx^{-1}=y^{-1}$.

In the case when $xyx^{-1}=y$ we see that $xy=yx$ which implies that G is abelian but $|xy|=2p$, then G is cyclic and isomorphism to C_p.

In the case when $xyx^{-1}=y^{-1}$ we see that $xy=y^{-1}x$ therefore the group G is isomorphic to the dihedral group D_p of order $2p$.

CHAPTER THREE

APPLICATIONS OF SYLOW THEOREMS AND MORE

In this chapter we will try to classify all groups of order 8, 12, 16, 18, 20, 21, 24, 27, 28, and 30 up to isomorphism.

Groups of order 8:

We know from lemma (2.1.5) that every abelian group of order 8 is isomorphic to $C_8, C_4 \times C_2$ or $C_2 \times C_2 \times C_2$.

Suppose that G be a non-abelian group of order 8.
If G had an element of order 8 , then G would be cyclic, and hence abelian which contradicts our assumption that G is not abelian.

Therefore G has no element of order 8, so every element except the identity is of order either 2 or 4.
If each element of G except the identity had order 2, then from theorem (1.1) G would be abelian which contradicts our assumption that G is not abelian.
$\therefore G$ must contain at least one element of order 4.
Let $a \in G$ with $|a| = 4$, and let $N = \langle a \rangle$ be a subgroup of G of order 4.
$\because N \lhd G$ and there are precisely 2 cosets, given by N and bN, for any element $b \notin N$.
$\therefore G = N \bigcup bN$.
$\because N \lhd G$, then $bN \in G/N$ and $|G/N| = 2$.
$\therefore |bN| = 2 \Rightarrow b^2 \in N$.
$\therefore$ we have four possibilities for b^2:

1. $b^2 = e$ 2. $b^2 = a$ 3. $b^2 = a^2$ 4. $b^2 = a^3$.

If $b^2 = a$ or $b^2 = a^3$, then b would be of order 8 which a contradicts.

$\therefore b^2 = e$ or $b^2 = a^2$.

$\because N \lhd G$, then $bab^{-1} \in N$.

$\therefore |bab^{-1}| = 2$ or 4.

If $(bab^{-1})^2 = e$, so $a^2 = e$, a contradiction to the choice of a.

If $(bab^{-1})^4 = e$, then $a^4 = e$

$\therefore |bab^{-1}| = 4$.

So , either $bab^{-1} = a$ or $bab^{-1} = a^3$.

If $bab^{-1} = a$, then $ba = ab$ and so G would be abelian which contradicts our assumption.

$\therefore bab^{-1} = a^3$ so $ba = a^3 b$.

We have show that G contains elements a,b such that $a^4 = e$, $ba = a^3 b$, and $b^2 = e$ or $b^2 = a^2$.

If $a^4 = e$, $b^2 = e$, and $ba = a^3 b$, then G is isomorphic to the dihedral group D_4.

If $a^4 = e . b^2 = a^2$, and $ba = a^3 b$, then G is isomorphic to the quaternion group Q.

<u>Groups of order 12:</u>

Let G be a group of order 12. i.e. $|G| = 12 = 2^2.3$.

$\therefore G$ has Sylow 2-subgroup of order 4 say H, and Sylow 3-subgroup of order 3 say K .

Let n be the number of Sylow 2-subgroup, and m be the number of Sylow 3-subgroup.

$\because$ $n \equiv 1 (\text{mod } 2)$, $n | 3$ and $m \equiv 1 (\text{mod } 3)$, $m | 4$.

$\therefore n=1$ or $n=3$ and $m=1$ or $m=4$.

Therefore we have four possibilities:

1. $n=1$ and $m=1$.
2. $n=1$ and $m=4$.
3. $n=3$ and $m=1$.
4. $n=3$ and $m=4$.

Now we verify each possible case of them:

1. $n=1$ and $m=1$.

$\therefore H \lhd G$ and $K \lhd G$.

Moreover, $|HK| = \dfrac{|H||K|}{|H \cap K|} = |H||K| = 4.3 = 12 = |G|$.

$\therefore G \cong H \times K$.

We have two possibilities of H:

$H \cong C_4$ or $H \cong C_2 \times C_2$.

$\therefore G \cong C_2 \times C_2 \times C_3 \cong C_2 \times C_6$ or $G \cong C_4 \times C_3 \cong C_{12}$.

2. $n=1$ and $m=4$.

i. $H = \langle a : a^4 = e \rangle$ and $K = \langle b : b^3 = e \rangle$.

$\because H \lhd G$, and we have $H \cap K = \{e\}$ and $|HK| = |G|$.

$\therefore G = HK$, and have $G = H \rtimes K$.

$\therefore G \cong C_4 \rtimes C_3$.

$\because H \lhd G \quad \Rightarrow \quad bab^{-1} \in H$.

$\because |bab^{-1}| = 4 \quad \Rightarrow \quad bab^{-1} = a$ or a^3.

If $bab^{-1} = a$, then $ba = ab$ and so G is abelian.

$\therefore bab^{-1} = a^3 \quad \Rightarrow \quad ba = a^3 b$.

We have to show that the group G under this assumption is cyclic.

$\therefore (ab)^2 = abab = aa^3bb = b^2$.

$(ab)^3 = a, \ldots, (ab)^{12} = e$.

$\therefore G$ is cyclic and hence abelian.

$\therefore\ G \cong C_4 \rtimes C_3 \cong C_{12}$.

Therefore there is no non-abelian group of order 12 with $n=1$ and $m=4$ and $H \cong C_4$.

ii. Let $H=\{e,x,y,z\}$ be a group of order 4 which is not cyclic, thus $H \cong C_2 \times C_2$ and $K=\langle c : c^3 = e\rangle$.

$\because G=H \rtimes K \quad \Rightarrow G \cong (C_2 \times C_2) \rtimes C_3$.

$\because H \lhd G$, then $chc^{-1} \in H \quad \forall \quad h \in H$.

Assume G is non-abelian group.

$\because chc^{-1} \neq h$ for at least one element $h \in H$.

Suppose that $cxc^{-1} \neq x$. We may assume that $cxc^{-1}=y$.

Put $x=a$, $y=b$, and $z=ab$. Then $cac^{-1}=b$.

$\therefore ca=bc$, which implies $a=c^{-1}bc$.

Now we consider $cbc^{-1} \in H$.

If $cbc^{-1}=a$, then $cbc^{-1}=c^{-1}bc \Rightarrow b=c^{-2}bc^2$.

Then as $c^2=c^{-1}$, $(c^2)^{-1}=c$.

$\therefore b=cbc^{-1}$, and hence $a=b$ this is a contradiction.

If $cbc^{-1}=b$, then $b=c^{-1}bc=a \Rightarrow b=a$ which is a contradiction.

If $cbc^{-1}=e$, then $b=c^{-1}c=e$ which is a contradiction.

$\therefore cbc^{-1}=ab \Rightarrow cb=abc$.

Consequently G is defined by:

$a^2=b^2=e,\ c^3=e,\ ab=ba,\ ca=bc,\ cb=abc$.

Therefore the elements of G are:

$e,c,c^2,a,b,ab,ac,bc,abc,ac^2,bc^2,abc^2$, and has 3 elements of order 2 and 8 elements of order 3.

$\therefore G \cong A_4$.

3. $n = 3$ and $m = 1$.

   i. $H = \langle a : a^4 = e \rangle$ and $K = \langle c : c^3 = e \rangle$.

$\because G = K \rtimes H \Rightarrow G \cong C_3 \rtimes C_4$.

$\because K \lhd G$ so $aca^{-1} \in K$.

$\therefore aca^{-1} = e, c$ or c^2.

If $aca^{-1} = e$, then $c = e$ which is a contradiction.

If $aca^{-1} = c$, then $ac = ca$ which means that G is abelian.

$\therefore G \cong C_{12}$.

If $aca^{-1} = c^2 \quad \Rightarrow \quad ac = c^2 a$.

Consequently G is defined by:

$$a^4 = e, c^3 = e, ac = c^2 a, ac^2 = ca.$$

The distinct elements of G are:

$e, a, a^2, a^3, c, c^2, ac, a^2c, a^3c, ac^2, a^2c^2, a^3c^2$, and has 1 element of order 2, 2 elements of order 3, 6 elements of order 4 and 2 elements of order 6.

$\therefore G \cong \langle a, c : a^4 = c^3 = e, ac = c^2 a, ac^2 = ca \rangle$.

   ii. $H = \{e, x, y, z\} \cong C_2 \times C_2$, $K = \langle c : c^3 = e \rangle$.

c

$\because G = K \rtimes H \quad \Rightarrow \quad G = C_3 \rtimes (C_2 \times C_2)$.

$\because K \lhd G$, we have $hch^{-1} \in K \quad \forall \quad h \in G$.

By assumption for at least one element $h \in$ H such that $hch^{-1} \neq c$

Let $x \in H$ such that $xcx^{-1} = c^2$.

Again put $x = a$, $y = b$ and $z = ab$.

$\therefore ac = c^2 a$.

We claim that $S = \{e, a, c, c^2, ac, ac^2\}$ is a subgroup of G.

$\therefore S$ is a group of order 6 and S is a non-abelian group.

Also S has 2 elements of order 3 and 3 element of order 2.

$\therefore S \cong D_3$.

Now $S \lhd G \quad \Rightarrow \quad bcb^{-1} \in S$ where $b \notin S$.

$\therefore |bcb^{-1}| = 3$.

Therefore either $bcb^{-1} = c$ or c^2.

We shall now choose an element $h \in H, h \notin S$ Such that $hch^{-1} = c$.

If $bcb^{-1} = c$ then $h = b$.

If $bcb^{-1} = c^2$ and we have $aca^{-1} = c^2$ then

$(ab)c(ab)^{-1} = a(bcb^{-1})a^{-1} = ac^2a^{-1} = (aca^{-1})^2 = aca^{-1}\ aca^{-1} = c^2c^2 = c.$

$\therefore h = ab.$

$\therefore$ there exists an element $h \notin S$ in H such that $hch^{-1} = c.$

Consider $M = \langle h \rangle$, $|M| = 2$

Clearly $S \bigcap M = \{e\}$, $|S||M| = |G|$ and so $G \cong S \times M$.

But $S \cong D_3$, $M \cong C_2$.

$\therefore G \cong D_3 \times C_2 \cong D_6$.

$\therefore G \cong D_6$.

4. $n = 3$ and $m = 4$.

If $m = 4$, then G has 4 Sylow 3-subgroups.

Hence G has 8 distinct elements of order 3.

If $n = 3$, then G has 3 Sylow 2-subgroups of order 4.

Hence G has at least 5 distinct elements of order 2.

But $|G| = 12$.

Hence there is no group of type $n = 3$ and $m = 4$.

<u>Groups of order 16:</u>

We know from lemma (2.1.5) that every abelian group of order 16 is isomorphic to $C_{16}, C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times C_2 \times C_2$ or $C_2 \times C_2 \times C_2 \times C_2$.

Suppose that G be anon-abelian group of order 16.

If G had an element of order 16, then G would be cyclic, and hence abelian which is contradicts our assumption that G is not abelian.

$\therefore G$ has no elements of order 16. So every element except the identity is of order either 2, 4 or 8.

If each element of G except identity had order 2, then from theorem (1.1) G would be abelian which a coutradicts our assumption.

If G contain at least one element of order 8.

Let $a \in G$ with $|a| = 8$.

<u>Case (1)</u>

Let $N = \langle a \rangle$ be a subgroup of G of order 8.

$\therefore N \triangleleft G$ and there are precisely 2 cosets, given by N and bN, for any element $b \notin N$.

$\because N \triangleleft G$ then $bN \in G/N$ and $|G/N| = 2$.

$\therefore |bN| = 1$ or 2 $\Rightarrow$ $b^2 \in N$.

We have eight possibilities for b^2

1. $b^2 = e$ 2. $b^2 = a$ 3. $b^2 = a^2$ 4. $b^2 = a^3$ 5. $b^2 = a^4$
6. $b^2 = a^5$ 7. $b^2 = a^6$ 8. $b^2 = a^7$.

If $b^2 = a, a^3, a^5$ or a^7, then b would be of order 16.

$\therefore b^2 = e$ or $b^2 = a^2$ or $b^2 = a^4$ or $b^2 = a^6$.

$\because N \triangleleft G$, then $bab^{-1} \in N$

$\therefore |bab^{-1}| = 8$.

So, either $bab^{-1} = a, a^3, a^5$ or a^7.

If $bab^{-1} = a \Rightarrow ba = ab$ and so G would be abelian.

If $bab^{-1}=a^3 \Rightarrow ba=a^3b$.

If $b^2=e$.

$a=a, a^2=a^2, \ldots, a^7b=a^7b$. and the presentation $\left(a,b: a^8=b^2=e, ab=ba^3\right)$ is anon-abelian group of order 16, and the presentation $\left(a,b: a^8=b^2=e, ab=ba^3\right)$ which is called the quasihedral (or semihedral) group which has 3 elements of order 2, 6 elements of order 4 and 4 elements of order 8.

If $b^2=a^2 \Rightarrow b=a, b^2=a^2, b^3=a^3, b^4=a^4, b^5=a^5, b^6=a^6, b^7=a^7$ and $b^8=a^8$.

$\therefore$ G is abelian group which is a contradaction our assumption.

If $b^2=a^4 \Rightarrow b=a^2, b^2=a^4, b^3=a^6, b^4=e$.

$\therefore G=\{e,a,a^2,a^3,a^4,a^5,a^6,a^7\}$.

If $b^2=a^6 \Rightarrow b=a^3, b^2=a^6, b^3=a, b^4=a^4, b^5=a^7, b^6=a^2$, $b^7=a^5$ and $b^8=e$.

$\because b=a^3$ and $a^4=b^4 \Rightarrow a=a^3$ and $a^2=a^6$ this is a contradiction.

If $bab^{-1}=a^5 \Rightarrow ba=a^5b$.

If $b^2=e$.

$\therefore a=a, a^2=a^2, \ldots, a^7b=a^7b$.

and we have presentation $\left(a,b: a^8=b^2=e, ab=ba^5\right)$ is anon-abelian group of order 16 which has 8 elements of order 8, 4 elements of order 4 and 3 elements of order 2 which is called the modular group.

If $b^2=a^2 \Rightarrow b=a, b^2=a^2, b^3=a^3, b^4=a^4, b^5=a^5, b^6=a^6, b^7=a^7$ and $b^8=a^8$.

$\therefore$ G is abelian group which is a contradiction our assumption.

If $b^2=a^4 \Rightarrow b=a^2, b^2=a^4, b^3=a^6$ and $b^4=e$.

$\therefore G \not\cong \left(a,b: a^8=e, b^2=a^4, ab=ba^5\right)$.

If $b^2=a^6 \Rightarrow b=a^3, b^2=a^6, b^3=a, b^4=a^4, b^5=a^5, b^6=a^2, b^7=a^5$ and $b^8=e$.

$\because b=a^3$ and $b^4=a^4 \Rightarrow \left(b^2\right)^2=\left(a^2\right)^2 \Rightarrow b^2=a^2 \Rightarrow b=a \Rightarrow a=a^3$

and $a^2=a^6$ this is contradiction.

If $bab^{-1} = a^7 \Rightarrow ba = a^7 b$.

If $b^2 = e$.

$\therefore a = a, a^2 = a^2, \ldots a^7 b = a^7 b$.

And we have presentation $(a, b : a^8 = b^2 = e, ba = a^7 b)$ is anon-abelian group of order 16 which has 9 elements of order 2, 2 elements of order 4 and 4 elements of order 8.

$\therefore G \cong D_8$.

If $b^2 = a^2$, then G is a group of order $8 < |G| = 16$.

$\therefore G \not\cong (a, b : a^8 = e, b^2 = a^2, ba = a^7 b)$.

If $b^2 = a^4$

$\therefore a = a, a^2 = a^2, \ldots, a^7 b = a^7 b$.

And we have presentation $(a, b : a^8 = e, a^4 = b^2, ba = a^7 b)$ is anon-abelian group of order 16 which has 4 elements of order 8, 10 elements of order 4 and 1 element of order 2.

$\therefore G \cong Q_4$.

If $b^2 = a^6$.

$\because b = a^3$ and $b^4 = a^4 \Rightarrow b = a$.

$\therefore a = a^3, a^2 = a^6$ this is a contradiction.

<u>**Case (2):**</u>

If N is not cyclic, then $N \cong C_4 \times C_2$ or $N \cong C_2 \times C_2 \times C_2$.

1. $N \cong C_4 \times C_2 = \{a, b : a^4 = b^2 = e, ba = ab\}$.

$\because N \lhd G$, then G/N is of order 2 and thus isomorphic to C_2.

If $c \in G$ and $c \notin N$, we must then have $c^2 \in N$.

$\because$ every element of N has order 1, 2 or 4 then $|c^2| = 1, 2$ or 4.

$\because N \lhd G$, then $cnc^{-1} \in N \ \forall \ n \in N$.

$\therefore\ cac^{-1} \in N$ and $cbc^{-1} \in N$

$\therefore\ |cac^{-1}|$=2 or 4 and $|cbc^{-1}|$=2.

$\therefore\ cac^{-1} = a, a^2$ or a^3 and $cbc^{-1} = b$.

If $|c^2|$=2, then $|c|$=4.

But "any group of order p^2,where p is aprime number, is abelian"

$\therefore\ |c^2|$=4, then $|c|$=8 but any group generated by $a^4 = b^2 = e$, $c^8 = e$ with $cac^{-1} = a$,a^2 or a^3 and $cbc^{-1} = b$ must be of order less than 16.

$\therefore\ c^2 = e.$

If $cac^{-1} = a$ and $cac^{-1} = b$ then $ca = bc$ then G is abelian which a contradicts our assumption that G is not abelian.

If $cac^{-1} = a^2$ and $cbc^{-1} = b$

$\therefore ca = a^2c$ and $cb = bc$

$ca^2 = (ca)a = (a^2c)a = a^2(a^2c) = c$

$\therefore a = a, a^2 = a^2 \ldots, a^7b = a^7b$.

And we have:

$a = b^2a = b(ba) = bab$ and $a = c^2a = c(ca) = cac$.

$\therefore G \cong (a,b,c : a^4 = b^2 = c^2 = e, cbca^2b = e, bab = a, cac = a)$.

If $cac^{-1} = a^3$ and $cbc^{-1} = b$.

$\therefore ca = a^3c$ and $cb = bc$.

$\therefore a = a, a^2 = a^2, \ldots, a^3bc = a^3bc$.

And we have G is a non-abelian group which has 11 elements of order 2 and 4 elements of order 4.

$\therefore G \cong D_4 \times C_2$.

2. let $N \cong C_2 \times C_2 \times C_2 = \{a,b,d : a^2 = b^2 = d^2 = e, ab = ba, ad = da, bd = db\}$.

$\because N \lhd G$, then G/N is of order 2 and thus isomorphic to C_2.

$\because c \in G$ and $c \notin N$, we must then have $c^2 \in N$.

$\because$ every element of N has order 1 or 2 then $|c^2| = 1$ or 2.

$\because N \lhd G$, then $cnc^{-1} \in N \quad \forall \quad n \in N$.

$\therefore |cac^{-1}| = 2$ and $|cbc^{-1}| = 2$ and $|cdc^{-1}| = 2$.

$\therefore cac^{-1} = a$ and $cbc^{-1} = b$ and $cdc^{-1} = d$.

$\therefore ca = ac$ and $cb = bc$ and $cd = dc$.

$\therefore G = \{e, a, b, d, c, ab, ad, ac, bd, bc, dc, abc, abd, adc, bdc, abdc\}$ is abelian group which a contradict of our assumption.

If each element of G except the identity had order 4.

Let $a \in G$ with $|a| = 4$.

1. let $N = \langle a \rangle$ be a subgroup of G of order 4.

$\because N \lhd G$ and there are precisely 2 cosets given by N and bN, for any element $b \notin N$.

$\therefore G = N \bigcup bN$.

$\because N \lhd G$, then $bN \in G/N$ and $|G/N| = 4$.

$\therefore |bN| = 1, 2$ or 4.

But $bN \neq N$ then $|bN| \neq 1$.

$\therefore |bN| = 2$ or 4.

If $|bN| = 2 \quad \Rightarrow b^2 \in N$.

If $|bN| = 4 \quad \Rightarrow b^4 \in N$.

- If $b^2 \in N$.

We have four possibilities for b^2:

1. $b^2 = e$ 2. $b^2 = a$ 3. $b^2 = a^2$ 4. $b^2 = a^3$.

$\because N \lhd G$, then $bab^{-1} \in N$.

$\therefore \left|bab^{-1}\right| = 4$.

So, either $bab^{-1} = a$ or a^3.

If $bab^{-1} = a$, then $ba = ab$ and so G would be abelian.

$\therefore bab^{-1} = a^3 \Rightarrow ba = a^3b$.

If $b^2 = e \Rightarrow G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

$\therefore G \not\equiv \left(a, b : a^4 = b^2 = e, ba = a^3b\right)$.

If $b^2 = a$.

$\therefore G = \{e, a, a^2, a^3, b, b^3, b^5, b^7, ab\}$.

$\therefore G \not\equiv \left(a, b : a^4 = e, b^2 = a, ba = a^3b\right)$.

If $b^2 = a^2$.

$G = \{e, a, a^2, a^3, b, b^2, b^3, ab, a^2b, a^3b, ab^2, a^2b^2, a^3b^2, ab^3, a^2b^3, a^3b^3\}$ which is a non-abelian group of order 16 which has 7 elements of order 2 and 8 elements of order 4.

$\therefore G \equiv \left(a, b : a^4 = b^4 = e, abab = e, ba^3 = ab^3\right)$.

If $b^2 = a^3$

$G = \{e, a, a^2, a^3, b, b^3, b^5, b^7, ab\}$.

$\therefore G \not\equiv \left(a, b : a^4 = e, b^2 = a^3, ba = a^3b\right)$.

- If $b^4 \in N$.

We have four possibilities for b^4:

1. $b^4 = e$ 2. $b^4 = a$ 3. $b^4 = a^2$ 4. $b^4 = a^3$.

If $b^4 = a$ or $b^4 = a^3$, then b would be of order 16.

$\therefore b^4 = e$ or $b^4 = a^2$.

$\because N \lhd G$, then $bab^{-1} \in N$.

$\therefore \left|bab^{-1}\right| = 4$.

So, either $bab^{-1} = a$ or a^3.

If $bab^{-1} = a$, then $ba = ab$ and so G would be abelian.

$\therefore bab^{-1} = a^3 \Rightarrow ba = a^3b$.

If $b^4 = e$.

Then we have a presentation $(a.b : a^4 = b^4 = e, ab = ba^3)$is a non-abelian group of order 16 which has 12 elements of order 4 and 3 elements of order 2.

$\therefore G \cong (a, b : a^4 = b^4 = e, ab = ba^3)$.

If $b^4 = a^2$.

$G = \{e, a, a^2, a^3, b, b^3, b^5, b^7, ab\}$.

$\therefore G \not\cong (a, b : a^4 = e, b^4 = a^2, ba = a^3b)$.

2. if N is not cyclic, then $N \cong C_2 \times C_2$.

$\because N \lhd G$, then G/N is of order 4 and thus isomorphic to C_4.

If $c \in G$ and $c \notin N$, we must then have $c^4 \in N$.

$\because$ every element of N has order 1 or 2, then $|c^4| = 1$ or 2.

$\because N \lhd G$, then $cnc^{-1} \in N \quad \forall \quad n \in N$.

$\therefore |cac^{-1}| = 1$ or 2 and $|cbc^{-1}| = 1$ or 2.

$\therefore cac^{-1} = a$ and $cbc^{-1} = b \Rightarrow ca = ac$ and $cb = bc$.

If $|c^4| = 2$, then $|c| = 8$.

<u>**Groups of order 18:**</u>

We know that from lemma (2.1.5) that every abelian group of order 18 is isomorphic to C_{18} or $C_6 \times C_3$.

Suppose that G is a non-abelian group of order 18.:

By Sylow theory, G contains a normal subgroup H of order 9, and then $H \cong C_9$ or $H \cong C_3 \times C_3$.

Case (1)

If H is cyclic ,then let a be a generator of H. i.e. $H=\langle a:a^9=e\rangle$.

$\because H \lhd G$, then G/H is of order 2 and thus isomorphic to C_2.

If $b\in G$ and $b\notin H$, we must then have $b^2\in H$, since every element of H except the identity element has order 3 or 9 , then $|b^2|$=1,3 or 9.

If $|b^2|$=9, then $|b|$=18 and thus G is cyclic and hence abelian.

$\because H \lhd G$, then $bab^{-1}\in H$

$\therefore |bab^{-1}|=9$

$\therefore bab^{-1}=a,a^2,a^4,a^5,a^7$ or a^8.

If $|b^2|$=3, then $|b|$=6 but any group generated by $a^9=b^6=e$ with $bab^{-1}=a,a^2,a^4,a^5,a^7$ or a^8 must be of order less then 18.

$\therefore b^2=e$.

If $bab^{-1}=a \Rightarrow ba=ab$, which would make G abelian.

If $bab^{-1}=a^2 \Rightarrow ba=a^2b$ but not all elements of any group which generated by a,b such that $a^9=b^2=e, ba=a^2b$ are distinct.

$\therefore \langle a,b:a^9=b^2=e,ba=a^2b\rangle=\{e,a,a^2,b,ab,a^2b\}$.

$\therefore G\not\cong\langle a,b:a^9=b^2=e,ba=a^2b\rangle$.

A similar study of $a=(bb)a=b(ba)$.

For

$\langle a,b:a^9=e.b^2=e.ba=a^4b\rangle$,

$\langle a,b:a^9=e,b^2=e,ba=a^5b\rangle$, and

$\langle a,b:a^9=e,b^2=e,ba=a^7b\rangle$,

Shows that $a^3=e$ in each group, so this yields to group of order 6.

This leaves just $\langle a,b : a^9 = e, b^2 = e, ba = a^8 b\rangle$, and all elements of this group are distinct because $\langle a,b : a^9 = e, b^2 = e, ba = a^8 b\rangle \cong D_9$.

Case (2)

If H is not cyclic, then $H \cong C_3 \times C_3$ which is abelian.

$\because H \lhd G$, then G/H is of order 2 and thus isomorphic to C_2.

If $c \in G$ and $c \notin H$, we must then have $c^2 \in H$.

$\because$ every element of H has order 1 or 3, then $|c^2| = 1$ or 3.

$\because H \lhd G$, then $chc^{-1} \in H \quad \forall \quad h \in H$.

$\therefore \; cac^{-1} \in H$ and $cbc^{-1} \in H$

$\therefore |cac^{-1}| = 3$ and $|cbc^{-1}| = 3$.

$\therefore \; cac^{-1} = a$ or a^2 and $cbc^{-1} = b$ or b^2.

If $|c^2| = 3$, then $|c| = 6$ but any group generated by $a^3 = b^3 = e$, $c^6 = e$ with $cac^{-1} = a$ or a^2 and $cbc^{-1} = b$ or b^2 must be of order less than 18.

$\therefore \; c^2 = e$.

If $ca = ac$ and $cb = bc$ then G is abelian.

If $cac^{-1} = a^2$ and $cbc^{-1} = b$, then all elements of the group G_1 with presentation $\langle a,b,c : a^3 = b^3 = c^2 = e, ba = ab, ca = a^2 c, cb = bc\rangle$ are distinct.

This group has 6 elements order 6, 8 elements of order 3 and 3 elements of order 2.

Similarly, if $cac^{-1} = a$ and $cbc^{-1} = b^2$, then all elements of the group G_2 with presentation $\langle a,b,c : a^3 = b^3 = c^2 = e, ba = ab, ca = ac, cb = b^2 c\rangle$ are distinct and this group has 6 elements order 6, 8 elements order 3 and 3 elements of order 2.

$\therefore G_1 \cong G_2$.

But $S_3 \times C_3 = \langle a,b : a^3 = e, b^2 = e, ab = ba^2\rangle \times \langle c : c^3 = e\rangle$. .

$\because S_3 \times C_3$ has 6 elements of order6, 8 elements of order 3 and 3 elements of order 2.

$\therefore G \cong S_3 \times C_3$.

If $cac^{-1} = a^2$ and $cbc^{-1} = b^2$, then $ca = a^2c$.

$\therefore$ The group with presentation $\langle a,b,c : a^3 = b^3 = c^2 = e, ca = a^2c, cb = b^2c, bc = ab \rangle$ is isomorphic to $(C_3 \times C_3) \times C_2$.

$\therefore G \cong \langle a,b,c : a^3 = b^3 = c^2 = e, ca = a^2c, cb = b^2c, bc = ab \rangle$.

Groups of order 20:

Let G be a group order 20. i.e $|G| = 20 = 5.2^2$

$\therefore G$ has Sylow 2-subgroup of order 4 say H, and Sylow 5-subgroup of order 5 say K.

Let n be the number of Sylow 2-subgroup,and let m be the number of Sylow-subgroub.

$\because n = 1$ or 5 and $m = 1$.

Therefore we have two possibilities:

1. $n = 1$ and $m = 1$.
2. $n = 5$ and $m = 1$.

Now we verify each possible of them:

1. $n = 1$ and $m = 1$

$\therefore G \cong C_2 \times C_{10}$ or $G \cong C_{20}$.

Now assume that G is not abelian.

2. If $n = 5$ and $m = 1$.

i. $H = \langle a : a^4 = e \rangle \cong C_4$ and $K = \langle b : b^5 = e \rangle$.

$\because G = K \rtimes H$ therefore $G \cong C_5 \rtimes C_4$.

$\because K \lhd G$, and $|aba^{-1}| = 5$.

$\therefore aba^{-1}=b,b^2,b^3$ or b^4.

If $aba^{-1}=b \Rightarrow ab=ba$ then G is abelian.

If $aba^{-1}=b^2 \Rightarrow ab=b^2a$, and $a=a,a^2=a^2,\ldots,a^3b^4=a^3b^4$.

The group with presentation $(a,b:a^4=b^5=e,ab=b^2a)$ is a non-abelian group of order 20 which has 4 element of order 5,10 element of order 4 and 5 element of order 2.

If $aba^{-1}=b^3 \Rightarrow ab=b^3a$, and $a=a,a^2=a^2,\ldots,a^3b^4=a^3b^4$.

The group with presentation $(a,b:a^4=b^5=e,ab=b^3a)$ is a non abelian group of order 20 which has 4 elements of order 5,10 elements of order 4 and 5 element of order 2.

$\therefore G\cong(a,b:a^4=b^5=e,ba=ab^2)$

If $aba^{-1}=b^4 \Rightarrow ab=b^4a$,and $a=a,b=b,\ldots,a^3b^4=a^3b^4$.

The group with presentation $(a,b:a^4=b^5=e,bab=a)$ is anon –abelian group of order 20 which has 4 elements of order 10, 4 elements of order 5 and 10 elements of order 4 and 1 elements of order 2.

$\therefore G\cong(a,b:a^4=b^5=e,bab=a)$.

ii. Let $H=\{e,x,y,z\}\cong C_2\times C_2$, and $K=\langle c:c^5=e\rangle$.

$\therefore G=K\rtimes H$.

$\therefore G\cong C_5\rtimes(C_2\times C_2)$.

$\because K\triangleleft G$, we have $hch^{-1}\in H \quad \forall \quad h\in H$.

By assumption for at least one element $h\in H$ such that $hch^{-1}\neq c$

Let $x\in H$ such that $xcx^{-1}=c^2,c^3$ or c^4.

Again put $x=a$, $y=b$ and $z=ab$.

$\therefore ac=c^2a$ or $ac=c^3a$ or $ac=c^4a$

If $ac=c^2a \Rightarrow c=c^4$ and $c^2=c^3$ this is a contradiction.

If $ac = c^3a \Rightarrow c = c^4$ and $c^2 = c^3$ this is a contradiction.

If $ac = c^4a \Rightarrow a = a, c = c, c^2 = c^2, \ldots, ac^4 = ac^4$.

$\therefore\ ac = c^4a$.

We clain that $S = \{e, a, c, c^2, c^3, c^4, ac, ac^2, ac^3, ac^4\}$ is subgroup of G.

Such that S is a group of order 6 and S is anon-ablian group.

Also that S has 5 elements of order 2 and 4 elements of order 5.

$\therefore S \cong D_5$

$\because S \lhd G \Rightarrow bcb^{-1} \in S$ where $b \notin S$

$\therefore \left|bcb^{-1}\right| = 5$.

$\therefore bcb^{-1} = c, c^2, c^3$ or c^4 .

If $bcb^{-1} = c$ then $h = b$.

If $bcb^{-1} = c^2$ then

$(ab)c(ab)^{-1} = c^4 \Rightarrow$ a contradiction.

If $bcb^{-1} = c^4$ and we have $aca^{-1} = c^4$ then $(ab)c(ab)^{-1} = c$.

$\therefore h = ab$

$\therefore$ There exist an element $h \notin S$ in H such that $hch^{-1} = c$.

Consider $M = \langle h \rangle$, $|M|$=2.

Clearly $S \cap M = \{e\}$, $|S|\ |M|\ = |G|$, and so $G \cong S \times M$

But $S \cong D_5$, $M \cong C_2$.

$\therefore G \cong D_5 \times C_2 \cong D_{10}$

Groups of order 21:

We know that from lemma (2.1.5) that every abelain group of order 21 is isomorphic to C_{21}.

Suppose that G is anon –abelian group of order 21.

By sylow theory, G contains a normal subgroup H of order 7, and H must by cyclic.

Let a be generator of H. i.e. $H=\langle a : a^7 = e\rangle$.

$\because H \triangleleft G$, then G/H is of order 3 and thus isomorphic to C_3.

If $b \in G$ and $b \notin H$, we must then have $b^3 \in H$.

$\because$ every element of H has order 1 or 7.

$\therefore |b^3| = 7$, then $|b| = 21$ and thus G is cyclic and hence abelian.

$\therefore b^3 = e$.

$\because H \triangleleft G \quad \Rightarrow \quad bab^{-1} \in H$.

$\therefore |bab^{-1}| = 7 \quad \Rightarrow \quad bab^{-1} = a,\ a^2,\ a^3,\ a^4,\ a^5$ or a^6.

If $(a,b:\ a^7 = e,\ b^3 = e,\ ba = ab\ )$, then G is abelian.

If $(a,b:\ a^7 = e,\ b^3 = e,\ ba = a^2 b)$, then all elements of the group with this presentation are distinct.

$\therefore G \cong (a,b:\ a^7 = e,\ b^3 = e,\ ba = a^2 b)$.

This group has 6 elements of order 7 and 14 elements of order 3.

If $(a,b:\ a^7 = e,\ b^3 = e,\ ba = a^3 b)$, then not all elements of this group are distinct and we will prove that by using the associative law as follow:

$$a = a^2 = a^3 = a^4 = a^5 = a^6 = a^7 = e.$$

$\therefore$ every element in the group with presentation $(a,b:\ a^7 = e,\ b^3 = e,\ ba = a^3 b)$ is equal to e, b or b^2, that is, this group is isomorphic to C_3.

A similar study of $(bb)a = b(ba)$

For $(a,b:\ a^7 = e,\ b^3 = e, ba = a^5 b)$, and $(a,b:\ a^7 = e,\ b^3 = e, ba = a^6 b)$.

Shows that $a^6 = a$ again, so this yield a gain these two groups are isomorphic to C_3.

If $(a,b:\ a^7=e,\ b^3=e,\ ba=a^4b)$, then all elements of the group with this presentation are distinct.

$\therefore G\cong(a,b:\ a^7=e,\ b^3=e,\ ba=a^4b)$.

$\therefore$ this group has 6 elements of order 7 and 14 elements of order 3.

$\therefore(a,b:\ a^7=e,\ b^3=e,\ ba=a^4b)\cong(a,b:\ a^7=e,\ b^3=e,\ ba=a^2b)$.

Group of order 28:

Let G be a group order 28. i.e. $|G|=7.2^2$.

$\therefore$ G has Sylow 2-subgroup of order 4 Say H, and Sylow 7-subgroup of order 7 Say K.

Let n be the number of Sylow 2-subgroup, and let m be the number of Sylow 7-subgroub.

$n=1\pmod 2$, $n\backslash 7$ and $m=1\pmod 7$, $m|4$.

$\therefore n=1$ or 7 and $m=1$.

Therefore we have two possibilities :

1. $n=1$ and $m=1$.
2. $n=7$ and $m=1$.

Now we verify each possible of them:

1. $n=1$ and $m=1$.

$\because H\lhd G$ and $K\lhd G$.

$\therefore H\cap K=\{e\}\Rightarrow|H\cap K|=1$ and $|HK|=|G|$.

$\therefore G\cong H\times K$.

We have two possibilities of H:

i. $H\cong C_4$ $\Rightarrow$ $G\cong C_4\times C_7\cong C_{28}$

ii. $H\cong C_2\times C_2$ $\Rightarrow$ $G\cong C_2\times C_2\times C_7\cong C_2\times C_{14}$.

2. $n=7$ and $m=1$.

a. $H=\langle a:a^4=e\rangle$ and $K=\langle c:c^7=e\rangle$.

$\therefore G = K \rtimes H \Rightarrow G \cong C_7 \rtimes C_4$.

$\because K \lhd G$ so $aca^{-1} \in k$.

$\therefore |aca^{-1}| = 7$.

$\therefore aca^{-1} = c, c^2, c^3, c^4, c^5$ or c^6.

If $aca^{-1} = c \Rightarrow ac = ca \Rightarrow$ a contradicts.

If $aca^{-1} = c^2 \Rightarrow ac = c^2 a$ and $ca = c^2 a$.

$\therefore ac = ca \Rightarrow G$ is abelian group.

If $aca^{-1} = c^3 \Rightarrow ac = c^3 a$ but not all elements of any group which generated by a, c such that $a^4 = c^7 = e$, $ac = c^3 a$ are distinct.

$\therefore G = \{e, a, a^2, a^3, c, c^3, ac, ac^3, a^2c, a^2c^3, a^3c, a^3c^3\}$.

A similar study of $c = a^4(c) = a^3(ac)$. For

$\langle a, c : a^4 = c^7 = e, ac = c^4 a \rangle$.

$\langle a, c : a^4 = c^7 = e, ac = c^5 a \rangle$.

So this yields to group of order 12.

If $aca^{-1} = c^6 \Rightarrow ac = c^6 a$.

$a = a, a^2 = a^2, a^3 = a^3, \ldots, a^3c^6 = a^3c^6$.

$\therefore$ This leave just $\langle a, c : a^4 = c^7 = e, ca = ac^6 \rangle$, and all elements of this group are distinct and this group is order 28.

b. Let $H = \{e, x, y, z\} \cong C_2 \times C_2$ and $K = \langle c : c^7 = e \rangle$.

$\because G = K \rtimes H \Rightarrow G \cong C_7 \rtimes (C_2 \times C_2)$.

$\because K \lhd G$, we have $hch^{-1} \in H \quad \forall \quad h \in H$.

By assumption for at least one element $h \in H$ such that $hch^{-1} \neq c$

Let $x \in H$ such that $xcx^{-1} = c^6$.

Again put $x = a$, $y = b$ and $z = ab$.

$\therefore ac = c^6 a$.

We again that $S=\{e,a,c,c^2,c^3,c^4,c^5,c^6,ac,ac^2,ac^3,ac^4,ac^5,ac^6\}$ is a subgroup of G.

$\therefore$ S is a group of order 14 and S is anon-ablian group.

Also that S has 7 elements of order 2 and 6 element of order 7.

$\therefore S\cong D_7$.

$\because$ $S\lhd G \quad\Rightarrow\quad bcb^{-1}\in S$ where $b\notin S$.

$\therefore |bcb^{-1}|=7$.

$\therefore bcb^{-1}=c,c^2,c^3,c^4,c^5$ or c^6 we shall now choose an element $h\in H, h\notin S$ such that $hch^{-1}=c$.

If $bcb^{-1}=c$ then $h=b$.

If $bcb^{-1}=c^2$ and we have $c^6=aca^{-1}$ then $(ab)c(ab)^{-1}=c^5$.

$\therefore h\neq ab$

If $bcb^{-1}=c^3 \Rightarrow (ab)c(ab)^{-1}=c^4 \quad\Rightarrow\quad h\neq ab$.

If $bcb^{-1}=c^4 \Rightarrow (ab)c(ab)^{-1}=c^3 \quad\Rightarrow\quad h\neq ab$.

If $bcb^{-1}=c^5 \Rightarrow (ab)c(ab)^{-1}=c^2 \quad\Rightarrow\quad h\neq ab$.

If $bcb^{-1}=c^6$ and we have $c^6=aca^{-1}$ then $(ab)c(ab)^{-1}=c$.

$\therefore h=ab$

$\therefore$ There exist an element $h\notin S$ in H such that $hch^{-1}=c$.

Consider $M=\langle h\rangle$, $|M|=2$.

Clearly $S\cap M=\{e\}$, $|S|.|M|=|G|$, and so $G\cong S\times M$

But $S\cong D_7$, $M\cong C_2$.

$\because$ $G\cong C_7\times C_2\cong D_{14}$.

Groups of order 30:

We know from lemma (2.1.5) that every abelian group of order 30 is isomorphic to C_{30}.

Suppose that G be anon-abelian group of order 30.

If G had an element of order 30 ,then G would be cyclic , and hence abelian.

$\therefore$ every element except the identity is of order either 2,3,5,6,10 or15.

If each element of G except identity had order 2, then G would be abelian.

If each element of G except the identity had order 3 or 5, then G would be abelian.

If each element of G except the identity had order 6 or 10, then $G \cong C_6$ or D_3 or $G \cong C_{10}$ or D_5.

Thus G must contain at least one element of order 15.

Let $a \in G$ with $|a| = 15$, and let $N = \langle a \rangle$ be a subgroup of G of order 15

$\because N \lhd G$ and there are precisely 2 cosets, given by N and bN, for any element $b \notin N$.

$\because N \lhd G$, then $bN \in G/N$ and $|G/N| = 2$.

$\therefore |bN| = 2 \quad \Rightarrow \quad b^2 \in N$.

$\therefore$ we have fifteen possibilities for b^2:

1. $b^2 = e$ 2. $b^2 = a$ 3. $b^2 = a^2$ 4. $b^2 = a^3$ 5. $b^2 = a^4$

6. $b^2 = a^5$ 7. $b^2 = a^6$ 8. $b^2 = a^7$ 9. $b^2 = a^8$ 10. $b^2 = a^9$

11. $b^2 = a^{10}$ 12. $b^2 = a^{11}$ 13. $b^2 = a^{12}$ 14. $b^2 = a^{13}$ 15. $b^2 = a^{14}$.

If $b^2 = a, a^2, a^4, a^7, a^8, a^{11}, a^{11}, a^{13}$ or a^{14} then b would be of order 30.

If $b^2 = a^3, a^6, a^9, a^{12}$ then $G \cong C_{10}$ or D_5.

If $b^2 = a^5, a^{10}$ then $G \cong C_6$ or D_3.

$\therefore b^2 = e$

$\because N \lhd G$, then $bab^{-1} \in N$

$\therefore \left|bab^{-1}\right| = 15.$

So, either $bab^{-1} = a, a^2, a^4, a^7, a^8, a^{11}, a^{11}, a^{13}$ or a^{14}.

If $bcb^{-1}=a \Rightarrow ba = ab$ and so G would be abelian.

If $bcb^{-1}=a^2 \Rightarrow ba = a^2b$. Then

$a = a^4, a^2 = a^8 = a^{13} = a^7, a^3 = a^{12} = a^5, a^6 = a^9, a^{10} = a^{10}, a^{11} = a^{14}$.

If $bcb^{-1}=a^4 \Rightarrow ba = a^4b$.

$\therefore a = a, a^2 = a^2, \ldots a^{14}b = a^{14}b$, and we have non-abelian group of order 30 such that this group which has 8 elements of order 15, 10 elements of order 6, 4 elements of order 5, 2 elements of order 3 and 5 elements of order 2.

$\therefore G \cong D_5 \times C_3$.

If $bcb^{-1}=a^7 \Rightarrow ba = a^7b$. Then

$a = a^{12}, a^2 = a^8$ which is a contradiction.

If $bcb^{-1}=a^8 \Rightarrow ba = a^8b$. Then

$a = a^4, a^2 = a^8, a^3 = a^9, a^4 = a^{10}$ which is a contradiction.

If $bcb^{-1}=a^{11} \Rightarrow ba = a^{11}b$. Then

$a = a, a^2 = a^2, \ldots, a^{14}b = a^{14}b$, and we have non-abelian group of order 30 such that this group which has 8 elements of order 15, 12 elements of order 10, 4 elements of order 5, 2 elements of order 3 and 3 elements of order 2.

$\therefore G \cong D_3 \times C_5$.

If $bcb^{-1}=a^{13} \Rightarrow ba = a^{13}b$. Then

$a = a^{13}, a^2 = a^8$ which is a contradiction.

If $bcb^{-1}=a^{14} \Rightarrow ba = a^{14}b$ and $a^{15} = e$, $b^2 = e$ then G is isomorphic to the dihedral group D_{15}.

CHAPTER FOUR

CONCLUSION

In this chapter, we classify all groups of order less than or equal 30.

Groups of order 1 and all prime orders (1 group:1 abelian, 0 non abelian)

Any group of order 1 or of prime order p is cyclic and isomorphic to C_p.

Groups of order 4 (2 groups:2 abelian, 0 non-abelian)

Any group of order 4 is abelian and isomorphic to either

$$\left.\begin{matrix} C_4 \\ C_2 \times C_2 \end{matrix}\right\} \textit{abelian.}$$

Groups of order 6 (2 groups: 1 abelian, 1 non-abelian)

Any group of order 6 is isomorphic to either

$$C_6 \quad \} \textit{ abelian.}$$

$$S_3 \quad \} \textit{ non-abelian.}$$

Groups of order 8 (5 groups: 3 abelian, 2 non-abelian)

Any group of order 8 is isomorphic to

$$\left.\begin{matrix} C_8 \\ C_4 \times C_2 \\ C_2 \times C_2 \times C_2 \end{matrix}\right\} \textit{abelian.}$$

$$\left.\begin{matrix} D_4 \\ Q_3 \end{matrix}\right\} \textit{non-abelian.}$$

<u>Groups of order 9</u> (2 groups: 2 abelian, 0 non-abelian)

Any group of order 8 is abelian and isomorphic to

C_9
$C_3 \times C_3$ } *abelian*

<u>Groups of order 10</u> (2 groups: 1 abelian, 1 non-abelian)

Any group of order 10 is isomorphic to

C_{10} } *abelian.*

D_5 } *non-abelian.*

<u>Groups of order 12</u> (5 groups: 2 abelian, 3 non-abelian)

Any group of order 12 is isomorphic to

C_{12}
$C_6 \times C_2$ } *abelian.*

A_4
D_6
$C_3 \rtimes C_4$ } *non-abelian.*

<u>Groups of order 14</u> (2 groups: 1 abelian, 1 non-abelian)

Any group of order 14 is isomorphic to

C_{14} } *abelian.*

D_7 } *non-abelian.*

<u>Groups of order 15</u> (1 groups: 1 abelian, 0 non-abelian)

Any group of order 4 is abelian and isomorphic to either

C_{15} } *abelian.*

<u>Groups of order 16</u> (14 groups: 5 abelian, 9 non-abelian)

Any group of order 16 is isomorphic to

$$\left.\begin{array}{l} C_{16} \\ C_8 \times C_2 \\ C_4 \times C_4 \\ C_4 \times C_2 \times C_2 \\ C_2 \times C_2 \times C_2 \times C_2 \end{array}\right\} \textit{abelian.}$$

$$\left.\begin{array}{l} D_8 \\ D_4 \times C_2 \\ Q_3 \times C_2 \\ (a,b : a^8 = b^2 = e, ab = ba^5) \\ (a,b : a^4 = b^4 = e, ab = ba^3) \\ (a,b : a^8 = b^2 = e, ab = ba^3) \\ (a,b : a^8 = e, b^2 = a^4, aba = b) \\ (a,b : a^4 = b^4 = e, abab = e, ba^3 = ab^3) \\ (a,b,c : a^4 = b^2 = c^2 = e, cbca^2b = e, bab = a, cac = a) \end{array}\right\} \textit{non-abelian.}$$

<u>Groups of order 18</u> (5 groups: 2 abelian, 3 non-abelian)

Any group of order 18 is isomorphic to

$$\left.\begin{array}{l} C_{18} \\ C_6 \times C_3 \end{array}\right\} \textit{abelian.}$$

$$\left.\begin{array}{l} D_9 \\ S_3 \times C_3 \\ (C_3 \times C_3) \times C_2 \end{array}\right\} \textit{non-abelian.}$$

<u>Groups of order 20</u> (5 groups: 2 abelian, 3 non-abelian)

Any group of order 20 is isomorphic to

$$\left.\begin{array}{l} C_{20} \\ C_{10}\times C_2 \end{array}\right\} \textit{abelian.}$$

$$\left.\begin{array}{l} D_{10} \\ \left(a,b:a^4=b^5=e,bab=a\right) \\ \left(a,b:a^4=b^5=e,ba=ab^2\right) \end{array}\right\} \textit{non-abelian.}$$

<u>Groups of order 21</u> (2 groups: 1 abelian, 1 non-abelian)

Any group of order 21 is isomorphic to

$$C_{21} \quad \} \textit{ abelian.}$$

$$\left(a,b:a^7=b^3=e,ba=a^2b\right) \quad \} \textit{ non-abelian.}$$

<u>Groups of order 22</u> (2 groups: 1 abelian, 1 non-abelian)

Any group of order 22 is isomorphic to

$$C_{22} \quad \} \textit{ abelian.}$$

$$D_{11} \quad \} \textit{ non-abelian.}$$

<u>Groups of order 24</u> (15 groups: 3 abelian, 12 non-abelian)

Any group of order 24 is isomorphic to

$$\left.\begin{array}{l} C_{24} \\ C_{12}\times C_2 \\ C_6\times C_2\times C_2 \end{array}\right\} \textit{abelian.}$$

S_4
D_{12}
Q_{12}
$A_4 \times C_2$
$D_6 \times C_2$
$D_4 \times C_3$
$Q_4 \times C_3$
$D_3 \times C_4$
$Q_6 \times C_2$
$\langle 2,3,3 \rangle$
$\langle 4,6 \mid 2,2 \rangle$
$\langle -2,2,3 \rangle$
} *non-abelian.*

<u>Groups of order 25</u> (2 groups: 2 abelian, 0 non-abelian)

Any group of order 25 is abelian and isomorphic to either

C_{25}
$C_5 \times C_5$
} *abelian.*

<u>Groups of order 26</u> (2 groups: 1 abelian, 1 non-abelian)

Any group of order 26 is isomorphic to either

C_{26} } *abelian.*

D_{13} } *non-abelian.*

<u>Groups of order 27</u> (5 groups: 3 abelian, 2 non-abelian)

Any group of order 27 is isomorphic to either

C_{27}
$C_9 \times C_3$
$C_3 \times C_3 \times C_3$
} *abelian.*

$$\left.\begin{array}{l}\langle a,b : a^9 = b^3 = e, ba = a^4 b\rangle \\ \langle a,b,c : a^3 = b^3 = c^3 = e, ab = cac^2, ba = ab, bc = cb\rangle\end{array}\right\} \textit{non-abelian.}$$

<u>Groups of order 28</u> (4 groups: 2 abelian, 2 non-abelian)

Any group of order 28 is isomorphic to either

$$\left.\begin{array}{l}C_{28} \\ C_{14} \times C_2\end{array}\right\} \textit{abelian.}$$

$$\left.\begin{array}{l}D_{14} \\ \langle a,b : a^4 = b^7 = e, a^{-1}ba = b^{-1}\rangle\end{array}\right\} \textit{non-abelian.}$$

<u>Groups of order 30</u> (4 groups: 1 abelian, 3 non-abelian)

Any group of order 30 is isomorphic to either

$$C_{30} \quad \} \textit{ abelian.}$$

$$\left.\begin{array}{l}D_{15} \\ D_5 \times C_3 \\ D_3 \times C_5\end{array}\right\} \textit{non-abelian.}$$

Reference

[1] Curtis, Wilson " the atlas of finite groups " , Cambridge Press (1998).

[2] D.R. Wilkins, "Topics in group theory", Part II, Course 311: Michaela's term , (2001).

[3] D.S. Dummit and R.M. foote , "Abstract algebra ", John Wiley and Sons , Inc, University of Vermont, Third edition, (2004).

[4] D.S. Malik, John M. Mordeson, M.K.Sen "fundamental of abstract algebra", McGraw-Hill companies, International series in pure and applied mathematics, (1997).

[5] I.N. Herstein " Abstract algebra ", Third edition, university of Chicago, John Wiley and Sons, Inc (1999).

[6] J.A. Beachy "Abstract Algebra ", Northern Illinois, Second Edition, (2000).

[7] J. B. Fraleigh " A first course in abstract Algebra", Boston San Fracisco New York, London Toronto Sydney Tokyo Singapore Madrid and Mexico City Paris Cape town Hong Kong Montreal, Addison- Wesley (2003).

[8] J.H. Kwak and M.Y. Xu, "Finite group theory for combinatorists", Com^2MaC-KOSEF, Korea, Pohang, Volume one, (2005).

[9] J.S. Milne "Group theory", www.jmilne.org/math/, Third edition, (2003).

[10] J. Sullivan, "Classification of finite abelian groups", Notes based on an article by Navarro in the Amer. Math. Monthly, February (2003).

[11] M. Hall, " The theory of groups ", Chelsea Publishing Company New York, N.Y, Marshall Hall, Jr, Second edition, (1976).

[12] R. B. Ash, "Abstract algebra: the basic graduate year", John Willy and Sons Inc., University of Illinois, (2000).

ملخص باللغة العربية

تصنيف المجموعات المنتهية ذات الرتب الصغيرة

تبحث هذه الأطروحة في مسألة تصنيف المجموعات ذات الرتب الآتية $2p, p^3, p^2, pq, p$

حيث q, p أعداد أولية . تعطى التوصيفات (مولدات و علاقات) لهذه الزمر.

الطريقة المستخدمة هي الضرب المباشر و الشبه المباشر للزمر ، و هذه الطريقة مناسبة لإستنتاج التوصيفات لمثل هذه الزمر .

تحتوي الأطروحة على أربعة فصول يقدم الفصل الأول مبادئ ضرورية لنظرية الزمر و يشرح الفصل الثاني الزمر المنتهية وبعض الخواص لهذه المجموعات ويبين الفصل الثالث كيفية إثبات هذه التصنيفات عن طريق الضرب المباشر والغير مباشر ونظريات سيلو . كما يحتوي الفصل الرابع على توصيفات الزمر ذات الرتب أقل من أو يساوي 31 .

حيث انهينا وبحمد الله هذا البحث بقائمة المصادر المستخدمة لعرض هذه الأطروحة بعد الفصل الرابع.

الجماهيرية العربية الليبية الشعبية الاشتراكية العظمى

ان الدراسة ليست غاية في حد ذاتها
و إنما الغاية هي خلق الإنسان النموذجي الجديد

جامعة التحدي
سرت

التاريخ : ....
الموافق : ..15-1-2007ف
الرقم الاشاري : ك ع /13/1/2007ف

كليـــة العلـــــوم
قســـم الرياضيات

عنـــوان البحـــث

((عرض الزمر المنتهية ذو رتب صغيرة))

مقدمـــة مــــن الطـــالب

محمد كمال محمد سعيد

* * لجنــة المناقشـــة :

الدكتور / شعبان علي اطرينه ....
(مشــرف الرســـالـــة)

الدكتور / أمير عبدالمجيد خواجه ....
(ممتحـن داخلـــي)

الدكتور / إبراهيم عبدالله تنتوش ....
(ممتحـن خارجـي)

يعتمـد :-
د. محمد علي سالم الفرجاني
أمين اللجنة الشعبية لكلية العلوم

www.altahadi.edu.ly

info@altahadi.edu.ly 674 ✉ 054 / 60361 - 62151 ☏ 054/ 60363 - 65704 ☎

جامعة التحدي – سرت

كلية العلوم – قسم الرياضيات

بحث بعنوان:

عرض الزمر المنتهية ذو رتب صغيرة

استكمالاً لمتطلبات الإجازة العالية الماجستير في علوم الرياضيات

مقدمة من الطالب:

محمد كمال محمد سعيد

تحت إشراف الأستاذ:

د. شعبان علي طريبة

العام الجامعي 2006ف