Abstract Algebra 1

References:

- Introduction to Modern Abstract Algebra, by David M. Burton.
- Contemporary abstract algebra, by Gallian and Joseph.
- Groups and Numbers, by R. M. Luther.
- A First Course in Abstract Algebra, by J. B. Fraleigh.
- Group Theory, by M. Suzuki.
- Abstract Algebra Theory and Applications, by Thomas W. Judson.
- Abstract Algebra, by I. N. Herstein.
- Basic Abstract Algebra, by P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul.

1. Definition and Examples of Groups.

Definition(1-1):

A set G is a group if it is satisfying the following four axioms

i. $\exists$ a binary operation $G \times G \longmapsto G$ (**closure**) $(a, b) \longmapsto ab$
ii. $a(bc) = (ab)c \; \forall a, b, c \in G$ (**associativity**),
iii. $\exists 1 \in G$ s.t. $a1 = a = 1a \; \forall a \in G$
iv. $\forall a \in G, \exists a^{-1} \in G$ s.t. $aa^{-1} = 1 = a^{-1}a$ (**inverse**)

Examples(1-2):

1. $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot)$ is a group.

Solution: $\forall a, b, c \in \mathbb{R}^*$, we have

$i. ab \in \mathbb{R}^*$, ii. $a(bc) = (ab)c$, iii. $\exists 1 \in \mathbb{R}^* \ni a1 = a = 1a$, iv. $\forall a \in \mathbb{R}^*, \exists a^{-1} = \frac{1}{a} \in \mathbb{R}^* \ni aa^{-1} = 1 = a^{-1}a$

2. $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\},\cdot)$ is a group.

3. $(\mathbb{C}^* = \mathbb{C} \setminus \{0\},\cdot)$ is a group.

Solution: i, ii are clear,

iii. $\exists 1 \in \mathbb{C}^* \ni (a+ib)1 = a+ib = 1(a+ib)$,

iv. $(a+ib)^{-1} = \frac{a-ib}{a^2+b^2}$

4. $(GL(2,\mathbb{R}),\cdot)$ is a group.

Solution: i, ii are clear, iii. $\exists \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R}) \ni \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, iv. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$

5. $(S_3,\circ)$ is a group.

Solution: $S_3 = \{i,(12),(13),(23),(123),(132)\}$

$\circ$	i	(12)	(13)	(23)	(123)	(132)
i	i	(12)	(13)	(23)	(123)	(132)
(12)	(12)	i	(132)	(123)	(23)	(13)
(13)	?	?	?	?	?	?
(23)	?	?	?	?	?	?
(123)	?	?	?	?	?	?
(132)	?	?	?	?	?	?

We note that axioms i, ii and iii from above table are satisfy axiom iv.

a	i	(12)	(13)	(23)	(123)	(123)

a^{-1}	?	?	?	?	?	?

6. $(G = \{0, -1, 1, 2\}, +)$ is not a group.

Solution: since $1 + 2 = 3 \notin G$

7. $(G = \{-1, 1\}, \cdot)$ is a group.

Solution:

$\cdot$	-1	1
-1	?	?
1	?	?

8. Let $G = \{a, b, c, d\}$ be a set. Define a binary operation $*$ on G by the following table

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Show that $(G, *)$ is a group.

Solution: axioms i,ii are satisfy from above table, iii. The identity element is a, axiom iv.

x	a	b	c	d
x^{-1}	?	?	?	?

9. $(G = \{1, -1, i, -i\}, \cdot)$ is a group.

Solution:

$\cdot$	1	-1	i	$-i$
1	?	?	?	?
-1	?	?	?	?
i	?	?	?	?
$-i$	?	?	?	?

10. Let $G = \mathbb{Z}, a * b = a + b + 2$, show that $(G,*)$ is a group.

Solution: $\forall a, b, c \in \mathbb{Z}$, we have i. $a * b = a + b + 2 \in \mathbb{Z}$,

ii. $a * (b * c) = a * (b + c + 2) = a + b + c + 4, (a * b) * c = (a + b + 2) * c = a + b + c + 4$,

iii. $a * u = a + u + 2 = a, u = -2$,

iv. $a * z = -2 \Rightarrow a + z + 2 = -2 \Rightarrow z = -a - 4$

11. Let $G = \{f_1, f_2, f_3, f_4\}$ with f_i s.t. $i = 1,2,3,4$ are mappings on $\mathbb{R} \setminus \{0\}$ s.t. $f_1(x) = x, f_2(x) = -x, f_3(x) = \frac{1}{x}, f_4(x) = -\frac{1}{x}$. Show that $(G,\circ)$ is a group.

Solution:

$\circ$	f_1	f_2	f_3	f_4
f_1	?	?	?	?
f_2	?	?	?	?
f_3	?	?	?	?
f_4	?	?	?	?

12. Let $G = \mathbb{R} \times \mathbb{R} = \{(a, b): a, b \in \mathbb{R}, a \neq 0\}$ and $*$ be defined by $(a, b) * (c, d) = (ac, bc + d)$. Show that $(G,*)$ is a group.

Solution: i. $(a,b)*(c,d)=(ac,bc+d)\in G$

ii. $(a,b)*[(c,d)*(e,f)]=(a,b)*(ce,de+f)=(ace,bce+de+f),[(a,b)*(c,d)]*(e,f)=(ac,bc+d)*(e,f)=(ace,bce+de+f)$.

iii. $(a,b)*(x,y)=(a,b)\Rightarrow(ax,bx+y)=(a,b)\Rightarrow x=1,bx+y=b\Rightarrow b+y=b\Rightarrow y=0$,

iv. $(a,b)*(w,z)=(1,0)\Rightarrow(aw,bw+z)=(1,0)\Rightarrow w=\frac{1}{a},ba^{-1}+z=0\Rightarrow z=\frac{-b}{a}$

13. Let $(G,*)$ be an arbitrary group, the set of the functions from G into G with the composition $(F_G,\circ)$ is forms a group, where $F_G=\{f_a: a\in G\}, f_a: G\mapsto G$ s.t. $f_a(x)=a*x, x\in G$.

Solution: i. Let $f_a, f_b\in F_G, a,b\in G$

$(f_a\circ f_b)(x)=f_a\left(f_b(x)\right)=f_a(b*x)=a*(b*x)=(a*b)*x=f_{a*b}(x)\in F_G$

ii. $(f_a\circ f_b)\circ f_c=f_{a*b}\circ f_c=f_{(a*b)*c}=f_{a*(b*c)}=f_a\circ f_{b*c}=f_a\circ(f_b\circ f_c)$

iii. f_e is an identity of F_G, since $f_a\circ f_e=f_{a*e}=f_{e*a}=f_e\circ f_a=f_a$

iv. the inverse of f_a in F_G is $f_{a^{-1}}$, since $f_a\circ f_{a^{-1}}=f_{a*a^{-1}}=f_{a^{-1}*a}=f_{a^{-1}}\circ f_a=f_e$

14. Let n be a positive integer and take $w=\cos(\frac{2\pi}{n})+i\sin(\frac{2\pi}{n})\in\mathbb{C}$, then $(C_n=\{1,w,w^2,\dots,w^{n-1}\},\cdot)$ is an abelian group.

Definition(1-3): A group $(G,*)$ is an abelian if $a*b=b*a\ \forall a,b\in G$.

Example(1-4): Determine whether the previous examples are abelian .

Exercises:

1. Determine whether $(G,*)$ an abelian group.
   - $G = \mathbb{Z}, a * b = a + b + 3$
   - $G = \mathbb{R} \times \mathbb{R} = \{(a,b): a,b \in \mathbb{R}\}$ s.t. $(a,b) * (c,d) = (a+b, b+d+2bd)$
   - $(G = \{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ)$ where $f_1(x) = x, f_2(x) = \frac{1}{x}, f_3(x) = 1 - x, f_4(x) = \frac{x-1}{x}, f_5(x) = \frac{x}{x-1}, f_6(x) = \frac{1}{1-x}$
   - $G = \{(a,b): a,b \in \mathbb{R}, a \neq 0, b \neq 0\}$ s.t. $(a,b) * (c,d) = (ab, bd)$
   - $(G = \{an: n \in \mathbb{Z}\}, +)$
   - $G = \mathbb{Q}^*, a * b = \frac{ab}{2}$
2. Show that, $\left(G = \left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\}, \cdot\right)$ is a group.
3. Show that, $(C_8, \cdot)$ is an abelian group.

2. Some Properties of Groups

Theorem(2-1): If $(G,*)$ a group, then the left and right cancellation laws hold in G, that is:

1. $a * b = a * c \Rightarrow b = c$
2. $b * a = c * a \Rightarrow b = c, \forall a, b, c \in G$.

Proof: 1. Suppose $a * b = a * c$, then $\exists a^{-1} \in G$

$\ni a^{-1} * (a * b) = a^{-1} * (a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$.

(2) **(Homework).**

Theorem(2-2): In a group $(G,*)$, there is exactly one element e in G such that $e * a = a * e = a \forall a \in G$.

Proof: Assume that G has two identity elements e and e^*, this means for all $a \in G$, we have $a * e = e * a = a$ and $a * e^* = e^* * a = a$

$e * e^* = e^* * e = e$ and $e^* * e = e * e^* = e^* \Rightarrow e = e^*$.

Theorem(2-3): In a group $(G,*)$, the inverse element of each element of G is a unique.

Proof: Let $a \in G$ and a has two inverses x and x^*, such that

$a * x = x * a = e$ and $a * x^* = x^* * a = e$

$\Rightarrow x = x * e = x * (a * x^*) = (x * a) * x^* = e * x^* = x^*$.

Theorem(2-4): If $(G,*)$ is a group, then

1. $e^{-1} = e$
2. $(a^{-1})^{-1} = a \ \forall a \in G$
3. $(a * b)^{-1} = b^{-1} * a^{-1} \ \forall a, b \in G$

Proof: 1. Let $e^{-1} = x$

$x * e = e * x = x \dots 1$

$e * x = x * e = e \dots 2$

From 1 and 2, $x = e \Rightarrow e^{-1} = e$.

(2) $(a^{-1})^{-1} = (a^{-1})^{-1} * e = (a^{-1})^{-1} * (a^{-1} * a)$

$$= ((a^{-1})^{-1} * a^{-1}) * a = e * a = a.$$

(3) since $(a * b) \in G \Rightarrow (a * b)^{-1} \in G$

$(a * b) * (a * b)^{-1} = (a * b)^{-1} * (a * b) = e$

$(a * b) * (a * b)^{-1} = e$

$a^{-1} * (a * b) * (a * b)^{-1} = a^{-1} * e$

$(a^{-1} * a) * b * (a * b)^{-1} = a^{-1}$

$e * b * (a * b)^{-1} = a^{-1}$

$b^{-1} * b * (a * b)^{-1} = b^{-1} * a^{-1}$

$e * (a * b)^{-1} = b^{-1} * a^{-1}$

$(a * b)^{-1} = b^{-1} * a^{-1}$.

<u>**Theorem(2-5):**</u> Let $(G,*)$ be a group, then

i. $(a * b)^{-1} = a^{-1} * b^{-1}$ iff G is an abelian group.

ii. If $a = a^{-1}$, then G is an abelian group.

Proof: i. ($\Longrightarrow$) let $(G,*)$ be a group and $(a*b)^{-1} = a^{-1} * b^{-1}$

To prove $(G,*)$ is an abelian group.

Let $a, b \in G$, to prove $a * b = b * a \ \ \forall a, b \in G$

$a * b = ((a*b)^{-1})^{-1}$

$\qquad = (b^{-1} * a^{-1})^{-1}$

$\qquad = (b^{-1})^{-1} * (a^{-1})^{-1}$

$\qquad = b * a$

($\Longleftarrow$) let $(G,*)$ be an abelian group, to prove $(a*b)^{-1} = a^{-1} * b^{-1}$

$(a*b)^{-1} = b^{-1} * a^{-1} = a^{-1} * b^{-1}$.

(ii) let $a = a^{-1}$,

to prove $a * b = b * a \ \ \forall a, b \in G$

$a * b = (a*b)^{-1} = b^{-1} * a^{-1} = b * a$.

Remark(2-6): The converse of above part is not true, for example let $(G = \{1, -1, i, -i\}, \cdot)$ be an abelian group with $a = i \Rightarrow a^{-1} = -i \Rightarrow a \neq a^{-1}$.

Theorem(2-7): In a group $(G,*)$, the equations $a * x = b$ and $y * a = b$ have a unique solutions.

Proof: $a * x = b$

$\Rightarrow a^{-1} * (a * x) = a^{-1} * b$

$\Rightarrow (a^{-1} * a) * x = a^{-1} * b$

$\Rightarrow e * x = a^{-1} * b$

$\Rightarrow x = a^{-1} * b$

To show the solution is a unique

Let $x^* \in G \ni a * x^* = b$

$\Rightarrow a * x^* = a * x$

$\Rightarrow x^* = x.$

The proof of $y * a = b$ (**Homework).**

3. Certain Elementary Theorems on Groups.

Definition(3-1): Let $(G,*)$ be a group, the integer powers of a, $a \in G$ is defined by:

1. $a^n = a * a * \dots * a$ (n-times)
2. $a^0 = e$
3. $a^{-n} = (a^{-1})^n, n \in \mathbb{Z}^+$
4. $a^{n+1} = a^n * a, n \in \mathbb{Z}^+$

Example(3-2): In $(\mathbb{R}, +)$, we have

$3^0 = 0,$

$3^2 = 3 + 3 = 6,$

$3^{-3} = (3^{-1})^3 = (-3) + (-3) + (-3) = -9$

Example(3-3): In $(\mathbb{R}, \cdot)$, we have

$2^0 = 1,$

$2^3 = 2 \cdot 2 \cdot 2 = 8,$

$2^{-4} = (2^{-1})^4 = (\frac{1}{2})^4 = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{16}$

Example(3-4): In $(G = \{1, -1, i, -i\}, \cdot)$, we have

$i^0 = 1,$

$i^2 = i \cdot i = -1,$

$i^{-2} = (i^{-1})^2 = (-i)^2 = -i \cdot -i = -1$

Theorem(3-5): Let $(G,*)$ be a group and $a \in G, m, n \in \mathbb{Z}$, then:

1. $a^n * a^m = a^{n+m} \ \forall n, m \in \mathbb{Z}$ **(Homework)**
2. $(a^n)^m = a^{nm} \ \ \forall n, m \in \mathbb{Z}^+$
3. $a^{-n} = (a^n)^{-1} \ \forall n \in \mathbb{Z}^+$
4. $(a * b)^n = a^n * b^n \ \forall n \in \mathbb{Z} \Leftrightarrow G$ is an abelian group.

Proof: (2) let $P(m): (a^n)^m = a^{nm}$

if $m = 1 \Rightarrow P(1): (a^n)^1 = a^n = a^{n \cdot 1}$

$\Rightarrow P(1)$ is a true.

Suppose that $P(k)$ is a true with $k \in \mathbb{Z}^+, \ k \leq m$

$\Rightarrow (a^n)^k = a^{nk}$

We have to prove that $P(k+1)$ is a true

$P(k+1): (a^n)^{k+1} = a^{n(k+1)}$

$$
\begin{aligned}
(a^n)^{k+1} &= (a^n)^k * (a^n)^1 \\
&= a^{nk} * a^n \\
&= a^{nk+n} \\
&= a^{n(k+1)}
\end{aligned}
$$

$\Rightarrow P(k+1)$ is a true

By the principle of mathematical indication

$\Rightarrow P(m)$ is a true $\forall m \in \mathbb{Z}^+$.

(3) if $n = 1 \Rightarrow P(1): (a^{-1})^1 = a^{-1} = (a^1)^{-1}$

Suppose that if $n = k$ is a true

$\Rightarrow P(k): (a^{-1})^k = (a^k)^{-1}$

We must prove $P(k+1)$ is a true

$P(k+1): (a^{-1})^{k+1} = (a^{k+1})^{-1}$

$(a^{-1})^{k+1} = (a^{-1})^k * (a^{-1})^1$

$= (a^k)^{-1} * (a^1)^{-1}$

$= (a^{k+1})^{-1}$

$\Rightarrow P(k+1)$ is a true

By the principle of mathematical indication

$\Rightarrow P(n)$ is a true $\forall\, n \in \mathbb{Z}^+$.

(4) $(\Rightarrow)$ if $n = 2 \Rightarrow (a * b)^2 = a^2 * b^2$

$(a * b) * (a * b) = a * a * b * b$

$a * (b * a) * b = a * (a * b) * b$

$(b * a) * b = (a * b) * b$

$b * a = a * b$

$\Rightarrow G$ is an abelian group

$(\Leftarrow)$ let G be an abelian group and $P(n): (a * b)^n = a^n * b^n$

If $n = 1 \Rightarrow (a * b)^1 = a^1 * b^1$ is a true

Suppose that $P(k)$ is a true with $k \in \mathbb{Z}^+,\ k \leq m$

$\ni P(k): (a * b)^k = a^k * b^k$

We must prove $P(k+1)$ is a true

$$P(k+1): (a * b)^{k+1} = (a * b)^k * (a * b)^1$$

$$= a^k * b^k * a^1 * b^1$$

$$= (a^k * b^k) * (b * a)$$

$$= a^k * (b^k * b) * a$$

$$= a^k * a * b^{k+1}$$

$$= a^{k+1} * b^{k+1}$$

$\Longrightarrow P(k+1)$ is a true $\forall\, n \in \mathbb{Z}^+$.

Definition(3-6): (The order of a Group)

The number of elements of a group G is called the order of G and it is denoted by $|G|$ or $O(G)$. The group G is called a finite if $|G| < \infty$ and an infinite group otherwise.

Definition(3-7): (The order of an element)

The order of an element a, $a \in G$ is the least positive integer n such that $a^n = e$ where e is the identity element of G. We denoted to order a by $|a|$ or $O(a)$. This means $|a| = n$ if $a^n = e,\ n \in \mathbb{Z}^+$.

Example(3-8): $(\mathbb{Z}, +)$ is an infinite group.

Example(3-9): The trivial group $G = \{0\}$, $|G| = 1$, G is the only group of order one.

Example(3-10): Find the order of G and the order of their elements, where$G = \{1, -1, i, -i\}$.

Solution: $|G| = 4$ and $|1| = 1$, $|-1| = 2$

$|i| = 4$ and $|-i| = 4$.

Exercises:

- Find the order of $(G = \{1, -1\}, \cdot)$ and the order of their elements.
- Find the order of $(C_6, \cdot)$ and the order of their elements.
- Find the order of $(S_3, \circ)$ and the order of their elements.
- Let $G = \{a, b, c, d\}$ be a set. Define a binary operation $*$ on G by the following table

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Find the order of G and their elements

4. Two Important Groups

Definition(4-1): Let $a, b, n \in \mathbb{Z},\ n > 0$. Then a is congruent to b modulo n if $a - b = nk, k \in \mathbb{Z}$ and denoted by $a \equiv b$ or $a \equiv b \pmod{n}$.

Examples(4-2):

1. $17 \equiv 5 \pmod{6}$, since $17 - 5 = 12 = (6)(2)$.
2. $8 \equiv 4 \pmod{2}$, since $8 - 4 = 4 = (2)(2)$.
3. $-12 \equiv 3 \pmod{3}$, since $-12 - 3 = -15 = (3)(-5)$.
4. $5 \not\equiv 2 \pmod{2}$, since $5 - 2 = 3 \neq (2)(k), \forall\, k \in \mathbb{Z}$.

Theorem(4-3): The congruence modulo n is an equivalence relation on the set of integers.

Proof: let $a, b, c, n \in \mathbb{Z},\ n > 0$

$a - a = 0 = (n)(0) \Rightarrow a \equiv a \pmod{n}$

$\Rightarrow$ the reflexive is a true.

If $a \equiv b \pmod{n}$, to prove $b \equiv a \pmod{n}$

$a \equiv b \pmod{n} \Rightarrow a - b = nk,\ k \in \mathbb{Z}$, so

$b - a = -nk = n(-k), -k \in \mathbb{Z} \Rightarrow b \equiv a \pmod{n}$

$\Rightarrow$ the symmetric is a true.

If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, to prove $a \equiv c \pmod{n}$

Since $a \equiv b \pmod{n}$, then $a - b = nk$ and

$b \equiv c \pmod{n}$, then $b - c = nk^*$

By adding these two equations

$\Rightarrow a - c = n(k + k^*), k + k^* \in \mathbb{Z}$

$\Rightarrow a \equiv c \pmod{n}$

$\Rightarrow$ the transitive is a true.

$\Rightarrow$ the congruence modulo n is an equivalent relation.

Definition(4-4): let $a \in \mathbb{Z}, n > 0$. The congruence class of a modulo n, denoted by $[a]$ is the set of all integers that are congruent to a modulo n.

This means, $[a] = \{z \in \mathbb{Z}: z \equiv a \pmod{n}\}$

$$= \{z \in \mathbb{Z}: z = a + kn, k \in \mathbb{Z}\}$$

Example(4-5): if $n = 2$, find [0] and [1].

Solution: $[0] = \{z \in \mathbb{Z}: z = 0 + 2k, k \in \mathbb{Z}\}$

$$= \{0, \pm 2, \pm 4, \dots\}$$

$[1] = \{z \in \mathbb{Z}: z \equiv 1 \pmod{2}\}$

$= \{z \in \mathbb{Z}: z = 1 + 2k, k \in \mathbb{Z}\}$

$= \{\pm 1, \pm 3, \pm 5, \dots\}$.

Example(4-6): if $n = 3$, find [1] and [7].

Solution: $[1] = \{z \in \mathbb{Z}: z \equiv 1 \pmod{3}\}$

$$= \{z \in \mathbb{Z}: z = 1 + 3k, k \in \mathbb{Z}\}$$

$$= \{1, -2, 4, 7, -5, \dots\}$$

[7] (**Homework**)

Definition(4-7): The set of all congruence classes modulo n is denoted by Z_n (which is read Z mod n). Thus,

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

Or $Z_n = \{0,1,2, \dots, n-1\}$

Z_n has n elements.

Example(4-8): $Z_1 = \{0\}, Z_2 = \{0,1\}, Z_3 = \{0,1,3\}$.

Now, we define the addition on Z_n (write $+_n$) by the following: for any $[a], [b] \in Z_n$, $[a] +_n [b] = [a +_n b]$.

Similarly, we define the multiplication on Z_n (write $\cdot_n$) by the following: for any $[a], [b] \in Z_n$, $[a] \cdot_n [b] = [a \cdot_n b], \forall [a], [b] \in Z_n$.

It is easy to note that $(Z_n, +_n)$ is an abelian group with identity $[0]$ and for every $[a] \in Z_n, [a]^{-1} = [n-a]$. This group is called the additive group of integers modulo n.

Example(4-9): $(Z_4, +_4)$, $Z_4 = \{0,1,2,3\}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

i. The closure is a true.

ii. The associative is a true.

iii. 0 is an identity element.

iv. The inverse: $1^{-1} = 4 - 1 = 3, 2^{-1} = 4 - 2 = 2, 3^{-1} = 4 - 3 = 1$.

v. An abelian: $1 +_4 2 = 3 = 2 +_4 1, 1 +_4 3 = 0 = 3 +_4 1$.

Example(4-10): $(Z_4, \cdot_4)$,

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

It is clear that we cannot have a group, since the number 1 is an identity, but the numbers 0 and 2 have no inverses. Thus $(Z_4, \cdot_4)$ isnot group.

The Permutations:

Definition(4-11): A permutation or symmetric of a set A is a function from A into A that is both one to one and onto. $f: A \longmapsto A$ (one to one and onto) and $\text{Symm}(A) = \{f: f: A \longmapsto A, f \text{ one to one and onto}\}$ the set of all permutation on A. If A is the finite set $\{1,2,\dots,n\}$, then the set of all permutation of A is denoted by S_n where $O(S_n) = n!$, where $n! = n(n-1)\dots(3)(2)(1)$.

Example(4-12): let $A = \{1,2\}$. Write all permutation on A.

Solution: $f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

$S_2 = \text{Symm}(A) = \{ f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},\ f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$.

Example(4-13): let $A = \{1,2,3\}$. Write all permutation on A.

Solution: $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$,

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$S_3 = \text{Symm}(A) = \{ f_1, f_2, f_3, f_4, f_5, f_6\}$, $O(S_3) = (3)(2) = 6$.

<u>Theorem(4-14):</u> If $A \neq \emptyset$, then the set of all permutation on A forms a group with composition of mapping. This means, let $A \neq \emptyset$, then $(\text{Symm}(A), \circ)$ is a group.

Proof: $\text{Symm}(A) = \{f : f : A \longmapsto A \text{ is a mapping}\}$

Since there is $i_A : A \longmapsto A$ a permutation on A

$i_A \in \text{Symm}(A) \Longrightarrow \text{Symm}(A) \neq \emptyset$

(i) Closure: let $f, g \in \text{Symm}(A)$

$f : A \longmapsto A, g : A \longmapsto A \Longrightarrow f \circ g : A \longmapsto A \Longrightarrow f \circ g \in \text{Symm}(A)$

(ii) The associative is a true, since the composition of the mappings is an associative.

(iii) The identity: since $i_A \in \text{Symm}(A)$ and $i_A \circ f = f \circ i_A = f$, for all f in $\text{Symm}(A) \Longrightarrow i_A$ is an identity element.

(iv) The inverse: $\forall f : A \longmapsto A, \exists f^{-1} : A \longmapsto A \Longrightarrow f^{-1} \in \text{Symm}(A)$ and $f \circ f^{-1} = f^{-1} \circ f = i_A \Longrightarrow (\text{Symm}(A), \circ)$ is a group.

<u>Example(4-15):</u> let $A = \{1,2,3\}$, then $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ and $(S_3, \circ)$ is a group. This group is called a symmetric group.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_5	f_6	f_4
f_3	f_3	f_1	f_2	f_6	f_4	f_5
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

$(S_3, \circ)$ is not an abelian group.

<u>Definition(4-16):</u> (The dihedral group D_n of order $2n$)

The n-th dihedral group is the group of symmetries of the regular n-gon, $O(D_n) = 2n$.

D_3: is the third dihedral group. $O(D_3) = (2)(3) = 6$.

Example(4-17): the group of symmetries of square D_4 or $G_S, O(D_4) = 8$, $G_S = D_4 = \{r_1, r_2, r_3, r_4, v, h, D_1, D_2\}$, where r_i is a clockwise rotation.

(i) Write all elements of G_S as a permutation. (**Homework**)

(ii) Is $(G_S, \circ)$ an abelian? Use table (**Homework**).

Definition(4-18): A permutation f of a set A is a cycle of length n if there exist $a_1, a_2, \dots, a_n \in A$ such that $f(a_1) = a_2, f(a_2) = a_3, \dots, f(a_{n-1}) = a_n, f(a_n) = a_1$ and $f(x) = x$ for $x \in A$ but $x \notin \{a_1, a_2, \dots, a_n\}$. we write $f = (a_1, a_2, \dots, a_n)$.

Example(4-19): If $A = \{1,2,3,4,5\}$, then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1,3,5,4) \circ (2) = (1,3,5,4)$$

Observe that,

$$(1,3,5,4) = (3,5,4,1) = (5,4,1,3) = (4,1,3,5).$$

Example(4-20): Let $A = \{1,2,3,4,5,6\}$ be a set of a group S_6. Then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (1,4,2) \circ (3) \circ (5,6) = (1,4,2) \circ (5,6)$$

And

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} = (1,6) \circ (2,4,5) \circ (3) = (1,6) \circ (2,4,5)$$

These permutations above are not cycles.

Theorem(4-21): Every permutation f of a finite set A is a product of disjoint cycles.

Definition(4-22): A cycle of length two is a transposition.

Example(4-23): The permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24)$ is a transposition.

Property(4-24): Any permutation can be expressed as the product of transpositions. This means $(a_1, a_2, \dots, a_n) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_n)$. Therefore any cycle is a product of transposition.

Example(4-25): We note that $(16)(253) = (16)(25)(23)$.

Definition(4-26): A permutation is even or odd according as it can be written as the product of an even or odd number of transpositions.

Example(4-27): Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$. Is f even or odd permutation.

Solution: $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) = (13)(12)$

f has two transpositions, thus f is an even permutation.

Example(4-28): Determine an even and odd permutation of D_4. (**Homework**)

Definition(4-29): (Alternating group)

The Alternating group on n letters denoted by A_n is the group consisting of all even permutations in the symmetric group S_n.

$O(A_n) = \frac{n!}{2}, A_n \subset S_n$

Example(4-30): Let $S_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6\}$, then $A_3 = \{i, f_2, f_3\}$ is a subgroup of S_3. $O(A_3) = \frac{6}{2} = 3$

Example(4-31): Find A_4 from S_4. (**Homework**)

5. Subgroups and Their Properties

Definition(5-1): Let $(G,*)$ be a group and $H \subset G$, H a non-empty subset of G. Then $(H,*)$ is a subgroup of $(G,*)$, if $(H,*)$ is itself a group.

Definition(5-2): Let $(G,*)$ be a group and $H \subset G$, then $(H,*)$ is a subgroup of $(G,*)$ if,

1. $\forall\, a, b \in H \Rightarrow a * b \in H$;
2. The identity element of G is an element of H, $(e \in G \Rightarrow e \in H)$;
3. $\forall\, a \in H \Rightarrow a^{-1} \in H$.

Remark(5-3): Each group $(G,*)$ has at least two subgroups $(\{e\},*)$ and $(G,*)$, these subgroups are known trivial subgroups and improper, any subgroup different from these subgroups known proper subgroup.

Example(5-4): $(\mathbb{Z},+)$ is a proper subgroup of $(\mathbb{R},+)$.

Example(5-5): $(H = \{-1,1\},\cdot)$ is a proper subgroup of $(G = \{-1,1,-i,1\},\cdot)$.

Example(5-6): $(H = \{0,2\},+_4)$ is a proper subgroup of $(Z_4,+_4)$, but $(H = \{0,3\},+_4)$ not subgroup of $(Z_4,+_4)$.

Example(5-7): $(\mathbb{Q} \setminus \{0\},\cdot)$ is a subgroup of $(\mathbb{R} \setminus \{0\},\cdot)$.

Theorem(5-8): Let $(G,*)$ be a group and $H \subset G$, then $(H,*)$ is a subgroup of $(G,*)$ iff $a * b^{-1} \in H,\ \forall\, a, b \in H$.

Proof: $(\Rightarrow)$ let $(H,*)$ be a subgroup of $(G,*)$ and $a, b \in H$, then $a, b^{-1} \in H \Rightarrow a * b^{-1} \in H$

$(\Leftarrow)$ let $a * b^{-1} \in H$, to prove $(H,*)$ be a subgroup of $(G,*)$

1. Since $H \neq \emptyset \Rightarrow \exists\, b \in H \ni b * b^{-1} \in H \Rightarrow e \in H$;
2. Since $b \in H$ and $e \in H \Rightarrow e * b^{-1} \in H \Rightarrow b^{-1} \in H$;

3. Let $a \in H$ and $b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H \Rightarrow (H,*)$ is a subgroup of $(G,*)$.

Example(5-9): Let $(\mathbb{Z},+)$ be a group and $H = \{5a : a \in \mathbb{Z}\}$. Show that $(H,+)$ is a subgroup of $(\mathbb{Z},+)$.

Solution: let $x, y \in H$, to prove $x + y^{-1} \in H$

$x \in H \Rightarrow x = 5a, a \in \mathbb{Z}$

$y \in H \Rightarrow y = 5b, b \in \mathbb{Z}$

$x + y^{-1} = 5a + (5b)^{-1} = 5a + 5(-b) = 5(a - b) \in H$

$\Rightarrow (H,+)$ is a subgroup of $(\mathbb{Z},+)$.

Theorem(5-10): If $(H_i,*)$ is the collection of subgroup of $(G,*)$, then $(\cap H_i,*)$ is also subgroup of $(G,*)$.

Proof: 1. Since $\exists e \in H_i, \forall i \Rightarrow e \in \cap H_i \Rightarrow \cap H_i \neq \emptyset$;

2. let $x, y \in \cap H_i$, to prove $x * y^{-1} \in \cap H_i$

Since $x, y \in \cap H_i \Rightarrow x, y \in H_i, \forall i \Rightarrow x * y^{-1} \in H_i, \forall i$

$\Rightarrow x * y^{-1} \in \cap H_i \Rightarrow (\cap H_i,*)$ is a subgroup of $(G,*)$.

Theorem(5-11): Let $(H_i,*)$ be the collection of subgroups of $(G,*)$ and let H_k and $H_j \in \{H_i\}$ such that there is $H_e \in \{H_i\}$, $H_k \subseteq H_\ell$ and $H_j \subseteq H_\ell$, then $(\cup H_i,*)$ is also subgroup of $(G,*)$.

Proof: 1. Since $\exists e \in H_i$ for some $i \Rightarrow e \in \cup H_i \Rightarrow \cup H_i \neq \emptyset$;

2. let $x, y \in \cup H_i$, then $x, y \in H_k$ or $x, y \in H_j$, so $x, y \in H_\ell$

$\Rightarrow x * y^{-1} \in H_\ell \Rightarrow x * y^{-1} \in \cup H_i$

$\Rightarrow (\cup H_i,*)$ is a subgroup of $(G,*)$.

Theorem(5-12): Let$(H_1,*)$ and $(H_2,*)$ are two subgroups of $(G,*)$, then $(H_1 \cup H_2,*)$ is a subgroup of $(G,*)$ iff $H_1 \subset H_2$ or $H_2 \subset H_1$.

Proof: $(\Longrightarrow)$ let $(H_1 \cup H_2,*)$ is a subgroup of $(G,*)$,

to prove $H_1 \subset H_2$ or $H_2 \subset H_1$

suppose that $H_1 \not\subset H_2$ and $H_2 \not\subset H_1$

$\Longrightarrow \exists a \in H_1, a \notin H_2$ and $\exists b \in H_2, b \notin H_1$

$\Longrightarrow a, b \in H_1 \cup H_2 \Longrightarrow a * b^{-1} \in H_1 \cup H_2$

$\Longrightarrow a * b^{-1} \in H_1$ or $a * b^{-1} \in H_2$

$\Longrightarrow a, b \in H_1$ or $a, b \in H_2$, but this is contradiction

$\Longrightarrow H_1 \subset H_2$ or $H_2 \subset H_1$

$(\Longleftarrow)$ let $H_1 \subset H_2$ or $H_2 \subset H_1$

To prove $(H_1 \cup H_2,*)$ is a subgroup of $(G,*)$

If $H_1 \subset H_2 \Longrightarrow H_1 \cup H_2 = H_2$ is a subgroup of $(G,*)$

If $H_2 \subset H_1 \Longrightarrow H_1 \cup H_2 = H_1$ is a subgroup of $(G,*)$

$\Longrightarrow (H_1 \cup H_2,*)$ is a subgroup of $(G,*)$.

Remark(5-13): $(H_1 \cup H_2,*)$ need not be a subgroup of $(G,*)$, for example:

$H_1 = \{r_1, r_3\}$ is a subgroup of G_S

$H_2 = \{r_1, v\}$ is a subgroup of G_S

$H_1 \cup H_2 = \{r_1, r_3, v\}$ is not a subgroup of G_S, since $r_3 \circ v = h \notin H_1 \cup H_2$.

Definition(5-14): Let $(G,*)$ be a group and $(H,*)$, $(K,*)$ are two subgroups of $(G,*)$, then the product of H and K is the set:

$H * K = \{h * k : h \in H, k \in K\}$

Notes(5-15):

1. $H * H$ is write H^2;
2. If $H = \{a\}$, then $H * K = a * K$. If $K = \{b\}$, then $H * K = H * b$;
3. $H \cup K \subseteq H * K$.

Theorem(5-16): Let $(G,*)$ be a group and $(H,*), (K,*)$ are two subgroups of $(G,*)$, then

1. $H * K \neq \emptyset$ and $H * K \subseteq G$.
2. $H \subseteq H * K$ and $K \subseteq H * K$.
3. $(H * K,*)$ is a subgroup of $(G,*)$ iff $H * K = K * H$.
4. If $(G,*)$ is an abelian group, then $(H * K,*)$ is a subgroup of $(G,*)$.

Proof:

1. $e \in H$ and $e \in K \Rightarrow e * e = e \in H * K \Rightarrow H * K \neq \emptyset$, and let $x \in H * K \Rightarrow x = a * b \ni a \in H \subseteq G$, and $b \in K \subseteq G \Rightarrow a \in G$, and $b \in G \Rightarrow a * b = x \in G \Rightarrow H * K \subset G$.
2. Let $x \in H \Rightarrow x = x * e \in H * K \Rightarrow x \in H * K \Rightarrow H \subseteq H * K$, similarly, $K \subseteq H * K$.
3. $(\Rightarrow)$ suppose $(H * K,*)$ is a subgroup of $(G,*)$, to prove $H * K = K * H$, this means $H * K \subseteq K * H$ and $K * H \subseteq H * K$, let $x \in H * K \Rightarrow x = a * b \ni a \in H$ and $b \in K$, since $H * K$ is a subgroup of $G \Rightarrow x^{-1} \in H * K$, let $x^{-1} = c * d \ni c \in H$ and $d \in K$, $x = (x^{-1})^{-1} = (c * d)^{-1} = d^{-1} * c^{-1} \ni d^{-1} \in K$ and $c^{-1} \in H \Rightarrow x = d^{-1} * c^{-1} \in K * H \Rightarrow H * K \subseteq K * H$, to prove $K * H \subseteq H * K$ (**Homework**).

$(\Leftarrow)$ let$H * K = K * H$, to prove $(H * K,*)$ is a subgroup of $(G,*)$

$H * K \neq \emptyset$ and $H * K \subseteq G$ (by 1)

Let $x, y \in H * K$, to prove $x * y^{-1} \in H * K$

$x \in H * K \Longrightarrow x = a * b \ni a \in H$ and $b \in H$

$y \in H * K \Longrightarrow y = c * d \ni c \in H$ and $d \in H$

$x * y^{-1} = (a * b) * (c * d)^{-1}$

$= (a * b) * (d^{-1} * c^{-1})$

$= a * (b * d^{-1}) * c^{-1}$

$\Longrightarrow (b * d^{-1}) * c^{-1} \in K * H = H * K$

$\Longrightarrow (b * d^{-1}) * c^{-1} \in H * K$

$\Longrightarrow \exists p \in H, q \in K \ni (b * d^{-1}) * c^{-1} = p * q$

$\Longrightarrow a * (b * d^{-1}) * c^{-1} = a + p + q \in H * K$

$\Longrightarrow x * y^{-1} \in H * K$

$\Longrightarrow (H * K, *)$ is a subgroup of $(G, *)$.

4. $H * K \neq \emptyset$, let $x, y \in H * K$

To prove $x * y^{-1} \in H * K$

$x \in H * K \Longrightarrow x = a * b \ni a \in H$ and $b \in K$

$y \in H * K \Longrightarrow y = c * d \ni c \in H$ and $d \in K$

$x * y^{-1} = (a * b) * (c * d)^{-1}$

$= (a * b) * (d^{-1} * c^{-1})$

$= (a * b) * (c^{-1} * d^{-1})$

$= a * (b * c^{-1}) * d^{-1}$

$= (a * c^{-1}) * (b * d^{-1})$

$\Rightarrow x * y^{-1} \in H * K$

$\Rightarrow (H * K,*)$ is a subgroup of $(G,*)$.

Example(5-17): In $(Z_8, +_8)$, let $H = \{0,4\}$ and $K = \{0,2,4,6\}$. Find $H +_8 K$.

Solution: $H +_8 K = \{0,2,4,6\}$.

Note(5-18): Let $(H,*)$ and $(K,*)$ are two subgroups of $(G,*)$, then:

1. $H * K \neq K * H$;
2. $(H * K,*)$ need not be a subgroup of $(G,*)$, give example (**Homework).**

Example(5-18): Is $H = \{0,6\}$ is a subgroup of $(Z_8, +_8)$? (**Homework).**

Example(5-19): Is $H = \{0,12\}$ is a subgroup of $(Z_4, +_4)$? (**Homework).**

Definition(5-20): The center of a group $(G,*)$ denoted by Cent(G) or $C(G)$ is the set $C(G) = \{c \in G: c * x = x * c, \forall\, x \in G\}$.

Note(5-21): $C(G) \neq \emptyset$, since $\exists e \in G \ni e * x = x * e\ \forall x \in G \Rightarrow e \in C(G)$.

Example(5-22): The group $(\mathbb{R} \setminus \{0\},\cdot)$, $C(\mathbb{R}) = \mathbb{R}$, since $(\mathbb{R} \setminus \{0\},\cdot)$ is an abelian group.

Example(5-23): The group $(S_3,\circ)$, $C(S_3) = \{f_1\}$, since

$C(S_3) = \{f \in S_3: f \circ g = g \circ f\ \ \forall g \in S_3\} = \{f_1\}$.

Theorem(5-24): Let $(G,*)$ be a group. Then$(C(G),*)$ is a subgroup of $(G,*)$.

Proof: $C(G) \neq \emptyset$, $C(G) = \{a \in G: x * a = a * x, \forall\, x \in G\} \subseteq G$

let $a, b \in C(G)$, to prove $a * b^{-1} \in C(G)$

$a \in C(G) \Rightarrow a * x = x * a\ \forall\, x \in G$

$b \in C(G) \Rightarrow b * x = x * b\ \forall\, x \in G$

To prove $(a * b^{-1}) * x = x * (a * b^{-1})\ \forall x \in G$

$$(a * b^{-1}) * x = a * (b^{-1} * x)$$

$$= a * (x^{-1} * b)^{-1}$$

$$= a * (b * x^{-1})^{-1}$$

$$= a * (x * b^{-1})$$

$$= (a * x) * b^{-1}$$

$$= (x * a) * b^{-1}$$

$$= x * (a * b^{-1})$$

$\Rightarrow (a * b^{-1}) \in C(G)$

$\Rightarrow (C(G),*)$ is a subgroup of $(G,*)$.

<u>Theorem(5-25):</u> Let $(G,*)$ be a group, then $C(G) = G$ iff G is an abelian group.

Proof: $(\Longrightarrow)\ \forall\, a \in G \Longrightarrow a \in C(G)$

$\Longrightarrow a * x = x * a\ \forall\, x \in G$

$\Longrightarrow a * x = x * a\ \forall\, x, a \in G$

$\Longrightarrow G$ is an abelian group.

$(\Longleftarrow)$ suppose that G is an abelian group, to prove $C(G) = G$

This means $C(G) \subseteq G$ and $G \subseteq C(G)$

By definition of $C(G)$, $C(G) \subseteq G$

To prove $G \subseteq C(G)$

Let $x \in G, G$ is an abelian group

$\Rightarrow x * a = a * x \;\; \forall a \in G$

$\Rightarrow x \in C(G)$

$\Rightarrow G \subseteq C(G)$

$\Rightarrow C(G) = G.$

6. More Results of Subgroups

Cyclic Group:

Definition(6-1) Let $(G,*)$ be a group and $a \in G$, the cyclic subgroup of G generated by a is denoted by $\langle a \rangle$ and defined as

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{\dots, a^{-1}, a^0, a^1, \dots\}$$

If $G = \langle a \rangle$, then G is called a cyclic group.

Definition(6-2): A group $(G,*)$ is called cyclic group generated by a iff $\exists a \in G \ni G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

Example(6-3): In $(Z_9, +_9)$, find the cyclic subgroup generated by 2,3,1.

Solution: $\langle 2 \rangle = \{2^k, k \in \mathbb{Z}\} = \{\dots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, \dots\}$

$= \{\dots, 3,5,7,0,2,4,6, \dots\} = \{0,1,2, \dots, 8\} = Z_9$

$\Rightarrow Z_9$ is a cyclic group generated by 2.

$\langle 3 \rangle = \{\dots, 3^{-3}, 3^{-2}, 3^{-1}, 3^0, 3^1, 3^2, 3^3, \dots\}$

$= \{\dots, 3,6,0,3,6, \dots\}$

$= \{0,3,6\}$ is a cyclic subgroup of Z_9.

$\langle 1 \rangle = \{\dots, 1^{-3}, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, 1^3, \dots\}$

$= \{\dots, 6,7,8,0,1,2,3, \dots\}$

$= Z_9$ is generated by 1.

Example(6-4): In $(\mathbb{Z}, +)$, find a cyclic group generated by $1, 2, -1$.

Solution: $\langle 1 \rangle = \{1^k, k \in \mathbb{Z}\} = \{\dots, 1^{-3}, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, 1^3, \dots\}$

$= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{Z}$

$\langle 2\rangle = \{2^k, k \in \mathbb{Z}\} = \{\dots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, \dots\}$

$= \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} \neq Z_9$

$\langle -1\rangle = \{(-1)^k, k \in \mathbb{Z}\}$

$= \{\dots, (-1)^{-3}, (-1)^{-2}, (-1)^{-1}, (-1)^0, (-1)^1, (-1)^2, (-1)^3, \dots\}$

$= \{\dots, 2, 1, o, -1, -2, \dots\} = \mathbb{Z}$

$\Rightarrow (\mathbb{Z}, +)$ is a cyclic group generated by 1 and -1.

Example(6-5): Is$(S_3, \circ)$ a cyclic group?

Solution: $\langle f_1\rangle = \{{f_1}^k, k \in \mathbb{Z}\} = \{\dots, {f_1}^{-3}, {f_1}^{-2}, {f_1}^{-1}, {f_1}^0, {f_1}^1, {f_1}^2, {f_1}^3, \dots\}$

$= \{f_1\} \neq S_3$

$\langle f_2\rangle = \{{f_2}^k, k \in \mathbb{Z}\} = \{\dots, {f_2}^{-2}, {f_2}^{-1}, {f_2}^0, {f_2}^1, {f_2}^2, \dots\}$

$= \{\dots, f_2, f_3, f_1, f_2, f_3, \dots\}$

$= \{f_1, f_2, f_3\} \neq S_3$

$\langle f_3\rangle = \{f_1, f_2, f_3\} \neq S_3$

$\langle f_4\rangle = \{f_1, f_4\} \neq S_3$

$\langle f_5\rangle = \{f_1, f_5\} \neq S_3$

$\langle f_6\rangle = \{f_1, f_6\} \neq S_3$

$\Rightarrow (S_3, \circ)$ is not a cyclic group.

Example(6-6): In $(Z_6, +_6)$, find a cyclic subgroup generated by 1,2,5. (**Homework**)

Theorem(6-7): Every cyclic group is an abelian.

Proof: let $(G, *)$ be a cyclic group, $\Rightarrow \exists a \in G \ni G = \langle a\rangle = \{a^k, k \in \mathbb{Z}\}$

To prove G is an abelian group

Let $x, y \in G$, to prove $x * y = y * x \; \forall \, x, y \in G$

$x \in G = \langle a \rangle \Rightarrow x = a^m \ni m \in \mathbb{Z}$

$y \in G = \langle a \rangle \Rightarrow y = a^n \ni n \in \mathbb{Z}$

$x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$

$\Rightarrow G$ is an abelian group.

Note(6-8): The converse of above theorem is not true in general, for example.

$(G = \{e, a, b, c\}, *) \ni a^2 = b^2 = c^2 = e$

$a^2 = e \Rightarrow a * a = e \Rightarrow a^{-1} = a$

$b^2 = e \Rightarrow b * b = e \Rightarrow b^{-1} = b$

$c^2 = e \Rightarrow c * c = e \Rightarrow c^{-1} = c$

$e^{-1} = e \Rightarrow x^{-1} = x \;\; \forall \, x \in G$

$\Rightarrow (G,*)$ is an abelian group, but $(G,*)$ is not a cyclic group, since

$\langle e \rangle = \{e\} \neq G$

$\langle a \rangle = \{a^k, k \in \mathbb{Z}\} = \{e, a\} \neq G$

$\langle b \rangle = \{b^k, k \in \mathbb{Z}\} = \{e, b\} \neq G$

$\langle c \rangle = \{c^k, k \in \mathbb{Z}\} = \{e, c\} \neq G$

$\Rightarrow (G,*)$ is not a cyclic.

Theorem(6-9): $\langle a \rangle = \langle a^{-1} \rangle \; \forall \, a \in G$.

Proof: $\langle a \rangle = \{a^k, k \in \mathbb{Z}\} = \{(a^{-1})^{-k}, -k \in \mathbb{Z}\}$

$= \{(a^{-1})^m, m = -k \in \mathbb{Z}\} = \langle a^{-1} \rangle$.

Theorem(6-10): If $(G,*)$ is a finite group of order n generated by a, then $G =: \langle a \rangle = \{a^k, k \in \mathbb{Z}\} = \{a^1, a^2, \ldots, a^n = e\}$, such that n is the least positive integer $\ni a^n = e$, this means $O(a) = n = O(G)$.

Example(6-11): Show that $(Z_n, +_n)$ is a cyclic group.

Solution: $Z_n = \{0,1, \ldots, \mathrm{n}-1\}$

$O(Z_n) = n$, to prove $Z_n = \langle 1 \rangle$

$\langle 1 \rangle = \{1^k, k \in \mathbb{Z}\} = \{1, 1^2, 1^3, \ldots, 1^n = 0\}$

$= \{1,2,3, \ldots, n = 0\} = Z_n$

$\Rightarrow Z_n = \langle 1 \rangle$ and $O(Z_n) = O(1) = n$.

Definition(6-12): (Division Algorithm for $\mathbb{Z}$)

If a, b are integers, with $b > 0$. Then there is a unique pair of integers$q, r \ni a = bq + r, 0 \leq r < b$.

The number q is called the quotient and r is called the remainder when a is divided by b.

Example(6-13): Find the quotient q and remainder r, when 38 is divided by 7 according to the division algorithm.

Solution: $38 = 7(5) + 3, 0 \leq 3 < 7$

$\Rightarrow q = 5,\ r = 3$.

Example(6-14): $a = 23, b = 7$.

Solution: $23 = 7(3) + 2, 0 \leq 2 < 7$

$\Rightarrow q = 3,\ r = 2$.

Example(6-15): $a = 15, b = 2$.

Solution: $15 = 2(7) + 1, 0 \leq 1 < 2$

$\Rightarrow q = 7,\ r = 1.$

Theorem(6-16): A subgroup of a cyclic group is a cyclic.

Proof: let G be a cyclic group generated by a and let H be a subgroup of G

If $H = \{e\}$, then $H = \langle e \rangle$ is a cyclic

If $H \neq \{e\}$ and $H \neq G$ (H is a proper subgroup), then

$x \in H \Rightarrow x = a^m, m \in \mathbb{Z}$

$x^{-1} \in H \Rightarrow x^{-1} = a^{-m}, -m \in \mathbb{Z}$

Let m be a least positive integer such that $a^m \in H$

to prove $H = \langle a^m \rangle = \{(a^m)^g : g \in \mathbb{Z}\}$

to prove $H \subseteq \langle a^m \rangle, \langle a^m \rangle \subseteq \langle a^m \rangle$

let $y \in H \Rightarrow y = a^s, s \in \mathbb{Z}$

by division algorithm of s and m

$s = mg + r \Rightarrow r = s - mg$

$a^r = a^{s-mg} = a^s * (a^{-m})^g, 0 \leq r < m$

$a^r \in H$ but $0 \leq r < m \Rightarrow r = 0 \Rightarrow s = mg$

$a^s = (a^m)^g \in \langle a^m \rangle$

$y = a^s \in \langle a^m \rangle \Rightarrow H \subseteq \langle a^m \rangle$

To prove $\langle a^m \rangle \subseteq H$

Let $x \in \langle a^m \rangle \Rightarrow x = (a^m)^g, g \in \mathbb{Z}$

$a^m \in H \Rightarrow (a^m)^g \in H \Rightarrow x \in H \Rightarrow \langle a^m \rangle \subseteq H$

$\Rightarrow (H,*)$ is a cyclic subgroup.

Corollary(6-17): If $(G,*)$ is a finite cyclic group of order n generated by a, then every subgroup of G is a cyclic generated by $a^m \ni \frac{n}{m}$.

Proof: suppose $(G,*)$ is a finite, $O(G) = n$

$G = \langle a \rangle = \{a, a^2, \dots, a^n = e\}$

Let $(H,*)$ be a subgroup of $(G,*)$, then$(H,*)$ is a cyclic

such that $H = \langle a^m \rangle$, to prove $\frac{n}{m}$ $(n = mg, g \in \mathbb{Z})$

$e \in H \Rightarrow a^n \in H$, by division algorithm of n, m

$\Rightarrow n = mg + r, 0 \leq r < m$

$r = n - mg \Rightarrow a^r = a^n * (a^m)^{-g}$

$a^r \in H$, but $0 \leq r < m$

If $r = 0 \Rightarrow n = mg \Rightarrow \frac{n}{m}$.

Example(6-18): Find all subgroups of $(Z_{15}, +_{15})$.

Solution: $O(Z_{15}) = 15$, $H = \langle 1^m \rangle$, $\frac{15}{m}$

If $m = 1 \Rightarrow H_1 = Z_{15}$

If $m = 3 \Rightarrow H_2 = \{3,6,9,12\}$

If $m = 5 \Rightarrow H_3 = \{5,10,0\}$

If $m = 15 \Rightarrow H_4 = \{0\}$.

Corollary(6-19): If $(G,*)$ is a finite cyclic group of prime order, then G has no a proper subgroup.

Proof: let $(G,*)$ be a finite group such that

$O(G) = p$ (p is a prime number)

$G = \langle a \rangle = \{a, a^2, \dots, a^p = e\}$

Let $(H,*)$ be a cyclic subgroup

$H = \langle a^m \rangle \ni \frac{p}{m} \Rightarrow m = 1$ or $m = p$

If $m = 1 \Rightarrow H = \langle a \rangle = G$ (not a proper subgroup)

If $m = p \Rightarrow H = \langle a^p = e \rangle = \{e\}$ (not a proper subgroup)

$\Rightarrow G$ has no a proper subgroup.

<u>Example(6-20):</u> Find all subgroup of $(Z_7, +_7)$.

Solution: $O(Z_7) = 7$

Let $H = \langle 1^m \rangle$, $\frac{7}{m} \Rightarrow m = 1$ or $m = 7$

If $m = 1 \Rightarrow H_1 = \langle 1 \rangle = Z_7$

If $m = 7 \Rightarrow H_2 = \langle 1^7 \rangle = \{0\}$.

<u>Definition(6-21):</u> A positive integer c is said to be a greatest common divisor of two non-zero numbers x, y iff

1. $\frac{x}{c}, \frac{y}{c}$
2. If $\frac{x}{a}, \frac{y}{a} \Rightarrow \frac{c}{a}$.

<u>Example(6-22):</u> Find g. c. d. (12,18).

Solution: g. c. d. $(12,18) = 6$, since

1. $\frac{12}{6}, \frac{18}{6}$

2. $\frac{12}{3}, \frac{18}{3} \Rightarrow \frac{6}{3}$

$\frac{12}{1}, \frac{18}{1} \Rightarrow \frac{6}{1}$

$\frac{12}{2}, \frac{18}{2} \Rightarrow \frac{6}{2}$.

Remark(6-23): If $(G,*)$ is a finite cyclic group of order n generated by a, then the generator of G is $a^k \ni \text{g.c.d.}(k,n) = 1$.

Example(6-24): Find all generators of $(Z_6, +_6)$.

Solution: $O(Z_6) = 6,\ Z_6 = \langle 1 \rangle$

$Z_6 = \langle 1^k \rangle \ni \text{g.c.d.}(k,6) = 1, \text{k} = 1,2,3,4,5$

$\text{k} = 1 \Rightarrow \text{g.c.d.}(1,6) = 1 \Rightarrow Z_6 = \langle 1 \rangle$

$\text{k} = 2 \Rightarrow \text{g.c.d.}(2,6) \neq 1 \Rightarrow Z_6 \neq \langle 1^2 \rangle = \langle 2 \rangle$

$\text{k} = 3 \Rightarrow \text{g.c.d.}(3,6) \neq 1 \Rightarrow Z_6 \neq \langle 1^3 \rangle = \langle 3 \rangle$

$\text{k} = 4 \Rightarrow \text{g.c.d.}(4,6) \neq 1 \Rightarrow Z_6 \neq \langle 1^4 \rangle = \langle 4 \rangle$

$\text{k} = 5 \Rightarrow \text{g.c.d.}(5,6) = 1 \Rightarrow Z_6 = \langle 1^5 \rangle = \langle 5 \rangle$

therefore, the generators of $Z_6$are 1,5.

Theorem(6-25): If $(G,*)$ is an infinite cyclic group generated by a, then:

1. The numbers a, a^{-1} are only generators of G;
2. Every subgroup of G except $\{e\}$ is an infinite subgroup.

Proof: (1) suppose $G = \langle a \rangle$, to prove $G = \langle a^{-1} \rangle$

Let $a \in G \ni G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$

Let $b \in G \ni G = \langle b \rangle = \{\dots, b^{-2}, b^{-1}, b^0, b^1, b^2, \dots\}$

$a \in G = \langle a \rangle \Rightarrow a = b^r, r \in \mathbb{Z} \dots 1$

$b \in G = \langle a \rangle \Rightarrow b = a^s, s \in \mathbb{Z} \dots 2$

Substitute 1 in 2, we get $b = (b^r)^s \Rightarrow b^1 = b^{rs}$

$1 = rs \Rightarrow r = s = 1$ or $r = s = -1$

If $r = s = 1 \Rightarrow a = b \Rightarrow G = \langle a \rangle$

If $r = s = -1 \Rightarrow b = a^{-1} \Rightarrow G = \langle a^{-1} \rangle$.

(2) let $(H,*)$ be a subgroup of $(G,*) \ni H \neq \{e\}$

To prove $(H,*)$ is an infinite

Suppose that $(H,*)$ is a finite such that $O(H) = k$

$(H,*)$ is a cyclic subgroup

$H = \langle a^m \rangle = \{(a^m)^1, (a^m)^2, \dots (a^m)^k = e\}$

$a^{mk} = e \Rightarrow O(a) = mk \Rightarrow O(a) = O(G)$, but this is contradiction

$(G = \langle a \rangle, G$ is a finite$)$

Thus, $(H,*)$ is an infinite.

Definition(6-26): Let $(H,*)$ be a subgroup of a group $(G,*)$. The set $a * H = \{a * h : h \in H\}$ of G is the left coset of H containing a, while the subset $H * a = \{h * a : h \in H\}$ is the right coset of H containing a.

Example(6-27): If $(Z_6, +_6), a = 1, H = \{0,2,4\}$, then

$1 +_6 H = \{1,3,5\}$, $H +_6 1 = \{1,3,5\}$

$3 +_6 H = \{3,5,1\}$, $H +_6 3 = \{3,5,1\}$

Notes(6-28):

1. $a * H$ is not subgroup (in general), give an example (**Homework**);
2. $a * H \neq H * a$ (in general), for example

$(S_3,\circ)$, $H = \{f_1, f_4\}$, $a = f_2$

$f_2 \circ H = \{f_2, f_5\}$, $H \circ f_2 = \{f_2, f_6\}$

$\Rightarrow f_2 \circ H \neq H \circ f_2$.

Theorem(6-29): Let $(H,*)$ be a subgroup of $(G,*)$ and $a \in G$, then

1. H is itself left coset of H in G.

Proof: $e \in G, e * H = \{e * h : h \in H\} = H$.

2. If $(G,*)$ is an abelian group, then $a * H = H * a$.

Proof: $a * H = \{a * h : h \in H\} = \{h * a : h \in H\} = H * a$.

The converse of above theorem is not true in general, for example

$(S_3,\circ)$, $H = \{f_1, f_2, f_3\}$, $a = f_4$

$f_4 \circ H = \{f_4, f_5, f_6\}$, $H \circ f_4 = \{f_4, f_6, f_5\}$

$\Rightarrow f_2 \circ H = H \circ f_2$, but $(S_3,\circ)$ is not an abelian.

3. $a \in a * H$

Proof: $a = a * e \in a * H$.

4. $a * H = H$ iff $a \in H$

Proof: $(\Longrightarrow)$ suppose that $a * H = H$, then by 3 $\Longrightarrow a \in H$.

$(\Longleftarrow)$ suppose that $a \in H$, to prove $a * H = H$

This means $a * H \subseteq H$ and $H \subseteq a * H$

Let $x \in a * H \Rightarrow x = a * h \in H \Rightarrow a * H \subseteq H$

To prove $H \subseteq a * H$

Let $b \in H \Rightarrow b = e * b = (a * a^{-1}) * b = a * (a^{-1} * b) \Rightarrow b \in a * H$

$\Rightarrow H \subseteq a * H \Rightarrow H = a * H.$

5. $a * H = b * H$ iff $a^{-1} * b \in H$

Proof: $(\Rightarrow)$ $a * H = b * H$

$a^{-1} * (a * H) = a^{-1} * (b * H)$

$(a^{-1} * a) * H = (a^{-1} * b) * H)$

$H = (a^{-1} * a) * H$, by 4 $\Rightarrow a^{-1} * b \in H$

$(\Leftarrow)$ suppose that $a^{-1} * b \in H$

by 4 $\Rightarrow (a^{-1} * b) * H = H \Rightarrow b * H = a * H.$

6. $a * H = b * H$ or $(a * H) \cap (b * H) = \emptyset$

Proof: suppose that $(a * H) \cap (b * H) \neq \emptyset$

To prove $a * H = b * H$

$\exists\, x \ni x \in a * H$ and $x \in b * H$

$x = a * h_1$ and $x = b * h_2 \ni h_1, h_2 \in H$

$a * h_1 = b * h_2 \Rightarrow h_1 = a^{-1} * b * h_2$

$\Rightarrow h_1 * {h_2}^{-1} = a^{-1} * b \in H$

by 5 $\Rightarrow a * H = b * H$

or suppose $a * H \neq b * H$

to prove $(a * H) \cap (b * H) = \emptyset$

suppose $(a * H) \cap (b * H) \neq \emptyset$

$\exists x \in a * H$ and $x \in b * H$

$x = a * h_1$ and $x = b * h_2$

$a^{-1} * b = h_1 * {h_2}^{-1} \Rightarrow a^{-1} * b \in H$

$\Rightarrow a * H = b * H$, but this is contradiction

$\Rightarrow \ (a * H) \cap (b * H) = \emptyset.$

7. The set of all distinct left coset of H in G form a partition on G.

Proof: to prove $G = \bigcup_{a \in G} a * H$ and $a_i * H \cap a_j * H = \emptyset$

$a_i * H, a_j * H$ are distinct $\Rightarrow a_i * H \cap a_j * H = \emptyset$

To prove $G = \bigcup_{a \in G} a * H$

$a * H \subseteq G \ \forall a \in G$ (by definition of a coset)

$$\Rightarrow \bigcup_{a \in G} a * H \subseteq G \ldots 1$$

$$\forall a \in G \Rightarrow a \in a * H \Rightarrow a \in \bigcup_{a \in G} a * H$$

$$\Rightarrow G \subseteq \bigcup_{a \in G} a * H \ldots 2$$

From 1,2, we have $G = \bigcup_{a \in G} a * H$.

Note(6-30): Every coset (left or right) of a subgroup H of a group $(G,*)$ has the same number of elements as H.

Example(6-31): The group $(Z_6, +_6)$ is an abelian. Find the partition of Z_6 into coset of the subgroup $H = \{0,3\}$.

Solution: $0 + H = \{0,3\} = H$

$1 + H = \{1,4\}$

$2 + H = \{2,5\}$

$3 + H = \{3,0\}$

$4 + H = \{4,1\}$

$5 + H = \{5,2\}$

All the cosets of H are $\{0,3\}, \{1,4\}, \{2,5\}$ and since $(Z_6, +_6)$ is an abelian group, then the left coset is an equal to the right coset.

Example(6-32): In $(S_3,\circ)$, let $H = \{f_1, f_4\}$. Find the partition of S_3 into left coset of H and the partition into right coset of H. (**Homework**)

Definition(6-33): Let $(H,*)$ be a subgroup of a group $(G,*)$. The number of left cosets or right cosets of H in G is called the index of H in G and denoted by $[G: H]$.

Note(6-34): If $(G,*)$ is a finite group, then $[G: H] = \frac{O(G)}{O(H)}$.

Example(6-35): $(S_3,\circ), H = \{f_1, f_2, f_3\}$

$$\Rightarrow [S_3: H] = \frac{O(S_3)}{O(H)} = \frac{6}{3} = 2$$

Example(6-36): $(Z_6, +_6), H = \{0,3\}$

$$\Rightarrow [Z_6: H] = \frac{O(Z_6)}{O(H)} = \frac{6}{2} = 3$$

Theorem(6-37): (Lagrange Theorem)

Let H be a subgroup of a finite group $(G,*)$. Then the order of H is a divisor of the order of G.

Proof: let G be a finite group $\ni O(G) = n$ and H be a subgroup of $G \ni O(H) = m$

To prove $\frac{O(G)}{O(H)}$ (to prove $\frac{n}{m}$, $n = mk$)

Since G is a finite $\Longrightarrow [G:H] = k$

Let $a_1 * H, a_2 * H, \dots, a_k * H$ are left cosets of H

$a_1 * H \cup a_2 * H \cup \dots \cup a_k * H = G$ and $a_i * H \cap a_j * H = \emptyset$

$O(a_1 * H) + O(a_2 * H) + \cdots + O(a_k * H) = O(G)$

$m + m + \cdots + m$ (k-times) $= n$

$$mk = n \Longrightarrow \frac{n}{m} \Longrightarrow \frac{O(G)}{O(H)}$$

Corollary(6-38): If $(G,*)$ is a finite group, then the order of any element of G divides the order of G.

Proof: suppose that $(G,*)$ is a finite such that $O(G) = n$

Let $a \in G \Longrightarrow a$ has a finite order such that $O(a) = m$

To prove such that $\frac{O(G)}{O(a)}$

Since $a \in G \Longrightarrow H = \langle a \rangle$ is a cyclic group

$H = \{a, a^2, \dots, a^m = e\}, O(a) = m \Longrightarrow \frac{O(G)}{O(H)}$ (by Lagrange Theorem)

$$\Longrightarrow \frac{O(G)}{O(a)}$$

Corollary(6-39): If $(G,*)$ is a finite group, then $a^{O(G)} = e \ \forall a \in G$.

Proof: suppose that $O(G) = n$

Let $a \in G \ni O(a) = m$ (by Corollary of Lagrange)

$\Rightarrow \frac{O(G)}{O(a)} \Rightarrow \frac{n}{m} \Rightarrow n = mk$

$a^{O(G)} = a^n = (a^m)^k = e^k = e$

$\Rightarrow a^{O(G)} = e \ \forall a \in G.$

Corollary(6-40): Every group of prime order is a cyclic.

Proof: let $(G,*)$ be a finite $\ni O(G) = p \Rightarrow \frac{p}{O(a)} \ \forall a \in G$

$O(a) = 1$ or p

If $O(a) = 1 \Rightarrow a = e$

If $O(a) = p \Rightarrow O(a) = O(G) \Rightarrow G = \langle a \rangle$

$\Rightarrow G$ is a cyclic group.

Corollary(6-41): Every group of order less than 6 is an abelian.

Proof: let $(G,*)$ be a finite group $\ni O(G) < 6$

$O(G) = 1$ or 2 or 3 or 4 or 5

If $O(G) = 1 \Rightarrow G = \{e\} \Rightarrow G$ is an abelian

If $O(G) = 2$ or 3 or $5 \Rightarrow G$ is a cyclic $\Rightarrow G$ is an abelian

If $O(G) = 4 \Rightarrow \frac{4}{O(a)} \Rightarrow O(a) = 1$ or 2 or 4

If $O(a) = 1 \Rightarrow a = e$

If $O(a) = 2 \ \forall a \in G \Rightarrow a^2 = e \Rightarrow a = a^{-1} \ \forall a \in G$

$\Rightarrow G$ is an abelian

If $O(a) = 4 \Rightarrow O(a) = O(G) \Rightarrow G = \langle a \rangle$

$\Rightarrow G$ is a cyclic $\Rightarrow G$ is an abelian.

7. Normal Subgroups and Quotient Groups

Definition(7-1): Let $(G,*)$ be a group and $a, b \in G$, then a is a conjugate to b and denoted by $a \sim b$ iff $\exists x \in G \ni b = x * a * x^{-1}$ and $b \sim a$ iff $\exists x \in G \ni a = x * b * x^{-1}$.

$$a \nsim b \text{ iff } b \neq x * a * x^{-1} \quad \forall x \in G$$

Example(7-2): In $(S_3, \circ)$, is $f_3 \sim f_2$?

Solution: $x = f_1 \Rightarrow f_1 \circ f_3 \circ f_1^{-1} = f_3 \neq f_2$

$x = f_2 \Rightarrow f_2 \circ f_3 \circ f_2^{-1} = f_1 \circ f_2^{-1} = f_3 \neq f_2$

$x = f_3 \Rightarrow f_3 \circ f_3 \circ f_3^{-1} = f_2 \circ f_2 = f_3 \neq f_2$

$x = f_4 \Rightarrow f_4 \circ f_3 \circ f_4^{-1} = f_5 \circ f_4 = f_2$

$x = f_5 \Rightarrow f_5 \circ f_3 \circ f_5^{-1} = f_6 \circ f_5 = f_2$

$x = f_6 \Rightarrow f_6 \circ f_3 \circ f_6^{-1} = f_4 \circ f_6 = f_2$

$\Rightarrow \exists x \in S_3 \ni x \circ f_3 \circ x^{-1} = f_2$

$\Rightarrow f_3 \sim f_2$

Is $f_1 \sim f_2$ and $f_1 \sim f_1$? **(Homework)**

Example(7-3): In $(Z_4, +_4)$, is $1 \sim 2$?

Solution: $x = 1 \Rightarrow 1 +_4 1 +_4 1^{-1} = 2 +_4 3 = 5 = 1 \neq 2$

$x = 2 \Rightarrow 2 +_4 1 +_4 2^{-1} = 3 +_4 2 = 5 = 1 \neq 2$

$x = 3 \Rightarrow 3 +_4 1 +_4 3^{-1} = 3 +_4 1 = 4 = 0 \neq 2$

$x = 0 \Rightarrow 0 +_4 1 +_4 0^{-1} = 1 \neq 2$

$\Rightarrow 1 \nsim 2$

Remark(7-4): If $(G,*)$ is an abelian group and $a, b \in G$, then $a \sim b \Leftrightarrow a = b$.

Proof: suppose that $a \sim b \Leftrightarrow \exists x \in G \ni b = x * a * x^{-1}$

$\Leftrightarrow b = x * x^{-1} * a \Leftrightarrow b = a$

Theorem(7-5): The relation (conjugate) is an equivalent relation.

Proof: (1) reflexive

let $a \in G$, to prove $a \sim a$

$\exists e \in G \ni a = e * a * e^{-1} \Rightarrow a \sim a$

(2) symmetric

Let $a, b \in G$ and $a \sim b$, to prove $b \sim a$

$a \sim b \Rightarrow \exists x \in G \ni b = x * a * x^{-1}$

$\Rightarrow x^{-1} * b = a * x^{-1}$

$\Rightarrow x^{-1} * b * x = a \Rightarrow b \sim a$

(3) transitive

Let $a, b, c \in G \ni a \sim b$ and $b \sim c$, to prove $a \sim c$

$a \sim b \Rightarrow \exists x \in G \ni b = x * a * x^{-1}$ ... 1

$b \sim c \Rightarrow \exists y \in G \ni c = y * b * y^{-1}$ ... 2

Substitute 1 in 2, we get

$c = y * (x * a * x^{-1}) * y^{-1}$

$c = (y * x) * a * (y * x)^{-1}$

$c = z * a * z^{-1}$(where $z = y * x \in G$)

$\Rightarrow a \sim c$.

Definition(7-6): Let $(G,*)$ be a group and $a \in G$, then the conjugate of a is denoted by $c(a)$ and defined as

$c(a) = \{b \in G: a \sim b\}$

or $c(a) = \{b \in G: a = x * a * b^{-1}\}$

or $c(a) = \{x * a * b^{-1}, \forall x \in G\}$

The set of all elements conjugate to a is called the conjugate class of a.

Examples(7-7): Find the conjugate class of each element in the following groups:

1. $(S_3,\circ)$ **(Homework)**
2. $(G_S,\circ)$ **(Homework)**
3. $(G = \{1,-1,i,-i\},\cdot) \ni i^2 = -1$.

Solution: $c(i) = \{x \cdot i \cdot x^{-1}, \forall x \in G\}$

$= \{1 \cdot i \cdot 1^{-1}, -1 \cdot i \cdot (-1)^{-1}, i \cdot i \cdot i^{-1}, -i \cdot i \cdot (-i)^{-1}\}$

$= \{i,i,i,i\} = \{i\}$

$c(1) = \{1\}, c(-1) = \{-1\}, c(-i) = \{-i\}$.

Example(7-8): Find $c(3)$ in $(Z_4, +_4)$.

Solution: $c(3) = \{0 +_4 3 +_4 0^{-1}, 1 +_4 3 +_4 1^{-1}, 2 +_4 3 +_4 2^{-1}, 3 +_4 3 +_4 3^{-1}\}$

$= \{3\}$ (by Remark if G is an abelian group and $a \sim b$, then $a = b$)

Note(7-9): Let $(G,*)$ be a group and $a \in G$, then $c(a)$ need not be a subgroup of $(G,*)$, for example in $(S_3,\circ)$, $c(f_3) = \{f_2, f_3\}$ is not a subgroup of S_3.

Theorem(7-10): Let $(G,*)$ be a group and $a, b \in G$, then

1. $a \in c(a)\ \forall a \in G$.

Proof: since $a \sim a\ \forall a \in G$ ($\sim$ is a reflexive)

$a \in c(a) \Rightarrow c(a) \neq \emptyset$

2. $c(a) = c(b) \Leftrightarrow a \sim b\ \forall a, b \in G$.

Proof: ($\Rightarrow$) suppose that $c(a) = c(b)$, to prove $a \sim b$

By 1, $a \in c(a) = c(b) \Rightarrow a \in c(b) \Rightarrow a \sim b$

($\Leftarrow$) suppose that $a \sim b$, to prove $c(a) = c(b)$

This means $c(a) \subseteq c(b)$ and $c(b) \subseteq c(a)$

Let $x \in c(b) \Rightarrow x \sim a$ and $a \sim b \Rightarrow x \sim b$

$\Rightarrow x \in c(b) \Rightarrow c(a) \subseteq c(b) \ldots 1$

Let $x \in c(b) \Rightarrow x \sim b$ and $a \sim b \Rightarrow x \sim a$

$\Rightarrow x \in c(a) \Rightarrow c(b) \subseteq c(a) \ldots 2$

From 1, 2, we get $c(a) = c(b)$

3. $c(a) \cap c(b) = \emptyset$ iff $a \nsim b$ (**Homework**)
4. $c(a) \cap c(b) = \emptyset$ or $c(a) = c(b)$ (**Homework**)
5. $b \in c(a) \Leftrightarrow c(a) = c(b)$

Proof: ($\Rightarrow$) let $b \in c(a) \Rightarrow b \sim a \Rightarrow c(a) = c(b)$ (by Theorem)

($\Leftarrow$) $c(a) = c(b) \Rightarrow a \sim b \Rightarrow b \sim a \Rightarrow b \in c(a)$.

6. $c(a) = \{a\}\ \forall a \in G \Leftrightarrow G$ is an abelian group.

Proof: $c(a) = \{a\}\ \forall a \in G \Leftrightarrow x * a * x^{-1} = a\ \forall a \in G$

$\Leftrightarrow x * a = a * x \Leftrightarrow G$ is an abelian group.

7. $c(a) = \{a\} \Leftrightarrow a \in C(G)$ (**Homework**)
8. $c(e) = \{e\}$ (**Homework**)

Definition(7-11): Let $(G,*)$ be a group and $a \in G$, then the normalizer of a is denoted by $N(a)$ and defined as $N(a) = \{x \in G: x * a = a * x\}$.

Example(7-12): In $(Z_8, +_8)$. Find $N(3)$.

Solution: $N(3) = \{x \in Z_8: x+_8 3 = 3+_8 x\}$

$= \{0,1,2,3,4,5,6,7\} = Z_8$

Theorem(7-13): Let $(G,*)$ be a group and $a \in G$, then

1. $(N(a),*)$ is a subgroup of $(G,*)$.

Proof: $N(a) = \{x \in G: x * a = a * x\} \subseteq G$

Since $e * a = a * e \Rightarrow e \in N(a) \Rightarrow N(a) \neq \emptyset$

Closure: let $x, y \in N(a)$, to prove $x * y \in N(a)$

$x \in N(a) \Rightarrow x * a = a * x$

$y \in N(a) \Rightarrow y * a = a * y$

$(x * y) * a = x * (y * a) = x * (a * y) = (x * a) * y = (a * x) * y$

$= a * (x * y) \Rightarrow x * y \in N(a)$

Let $x \in N(a)$, to prove $x^{-1} \in N(a)$

Since $x \in N(a) \Rightarrow x * a = a * x \Rightarrow x * a * x^{-1} = a$

$\Rightarrow a * x^{-1} = x^{-1} * a \Rightarrow x^{-1} \in N(a) \Rightarrow (N(a),*)$ is a subgroup.

2. $C(G) = \cap N(a) \ \forall \ a \in G$ (**Homework**)
3. $N(a) = G \ \forall a \in G \Leftrightarrow (G,*)$ is an abelian.

Proof: $(\Rightarrow)$ suppose that $N(a) = G \ \forall a \in G$, to prove G is an abelian

$\forall x \in G = N(a) \Rightarrow x \in N(a) \ \ \forall a \in G$

$\Rightarrow x \in N(a)\ \forall x, a \in G \Rightarrow x * a = a * x\ \forall x, a \in G$

$\Rightarrow (G,*)$ is an abelian

$(\Leftarrow)$ suppose that $(G,*)$ is an abelian, to prove $N(a) = G$

This means $N(a) \subseteq G$ and $G \subseteq N(a)$

$N(a) \subseteq G$ (by definition of $N(a)$)

To prove $G \subseteq N(a)$

Let $x \in G$ and G is an abelian

$\Rightarrow x * a = a * x\ \forall x, a \in G$

$\Rightarrow x \in N(a)\ \forall a \in G \Rightarrow G \subseteq N(a) \Rightarrow G = N(a)\ \forall a \in G$

4. $N(a) = G \Leftrightarrow a \in G$ (**Homework**)
5. $c(a) = [G: N(a)]$

Proof: $c(a) = \{x * a * x^{-1}: \forall x \in G\}$

$[G: N(a)] = \{x * N(a), \forall x \in G\}$

Define $f: [G: N(a)] \longrightarrow c(a) \ni f\big(x * N(a)\big) = x * a * x^{-1}\ \forall x \in G$

To prove f is a map, f is an one to one, f is an onto (**Homework**)

6. If $(G,*)$ is a finite group, then $\frac{O(G)}{O(c(a))}$

Proof: by 1 $\Rightarrow (N(a),*)$ is a subgroup of $(G,*)$

By Lagrange Theorem $\Rightarrow \frac{O(G)}{O(N(a))}$

$O(G = O\big(N(a)\big) \cdot [G: N(a)] = O\big(N(a)\big) \cdot O(c(a))$

$\Rightarrow \dfrac{O(G)}{O(c(a))}$

Definition(7-14): Let $(H,*), (K,*)$ are two subgroups of $(G,*)$, then H is a conjugate subgroup of K iff $\exists x \in G \ni K = x * H * x^{-1}$ and denoted by $H \sim K$.

$$H \nsim K \Leftrightarrow K \neq x * H * x^{-1} \forall x \in G$$

Example(7-15): In $(S_3, \circ), H = \{f_1, f_6\},\ K = \{f_1, f_5\}$. Is $H \sim K$?

Solution: this means, $\exists x \in S_3 \ni x \circ H \circ x^{-1} = K$?

$x = f_1 \Rightarrow f_1 \circ \{f_1, f_6\} \circ f_1^{-1} = \{f_1 \circ f_1 \circ f_1^{-1}, f_1 \circ f_6 \circ f_1^{-1}\}$

$= \{f_1, f_6\} \neq K$

$x = f_2 \Rightarrow f_2 \circ \{f_1, f_6\} \circ f_2^{-1} = \{f_2 \circ f_1 \circ f_2^{-1}, f_2 \circ f_6 \circ f_2^{-1}\}$

$= \{f_1, f_5\} = K$

$\Rightarrow \exists x = f_2 \ni H \sim K$.

Example(7-16): In $(Z_{12}, +_{12}), H = \{0,4,8\}, K = \{0,3,6,9\}$. Is $H \sim K$?

Solution: this means, $\exists x \in Z_{12} \ni x +_{12} H +_{12} x^{-1} = K$

$x = 1 \Rightarrow 1 +_{12} \{0,4,8\} +_{12} 1^{-1} = H \neq K$

Since $x +_{12} H +_{12} x^{-1} = x +_{12} x^{-1} +_{12} H = H \neq K$

$\Rightarrow H \nsim K$.

Example(7-17): In $(G_S, \circ)$, let $H = \{r_1, r_4\}, K = \{r_1, r_2\}$. Is $H \sim K$?

(**Homework**)

Theorem(7-18): Let $(H,*), (K,*)$ are two subgroups of $(G,*)$ and $H \sim K$, then $O(H) = O(K)$.

Proof: since $H \sim K \Rightarrow \exists x \in G \ni K = x * H * x^{-1}$

To prove $O(H) = O(K) = O(x * H * x^{-1})$

Define$f:(H,*) \longrightarrow (x*H*x^{-1},*) \ni f(h) = x*h*x^{-1} \forall h \in H$

To prove f is a map ?

Let $h_1 = h_2$, to prove $f(h_1) = f(h_2)$

Since $h_1 = h_2 \Rightarrow x*h_1*x^{-1} = x*h_2*x^{-1} \Rightarrow f(h_1) = f(h_2)$

$\Rightarrow f$ is a map.

Is f an one to one ? let $f(h_1) = f(h_2)$

$\Rightarrow x*h_1*x^{-1} = x*h_2*x^{-1}$

$\Rightarrow h_1 = h_2 \Rightarrow f$ is an one to one.

Is f an onto? $R_f = \{f(h): \forall h \in H\} = \{x*h*x^{-1}: \forall h \in H\}$

$= x*H*x^{-1} \Rightarrow f$ is an onto.

$\Rightarrow O(H) = O(x*H*x^{-1}) = O(K)$.

Theorem(7-19): Let $(H,*)$ be a subgroup of $(G,*)$ and $x \in G$, then $(x*H*x^{-1},*)$ is a subgroup of $(G,*)$.

Proof: $e \in G$ and $e*H*e^{-1} = H \neq \emptyset \Rightarrow x*H*x^{-1} \neq \emptyset$

$x*H*x^{-1} = \{x*h*x^{-1}: \forall h \in H\}$

Let $a, b \in x*H*x^{-1}$, to prove $a*b^{-1} \in x*H*x^{-1}$

Let $a \in x*H*x^{-1} \Rightarrow a = x*h_1*x^{-1} \ni h_1 \in H$

Let $b \in x*H*x^{-1} \Rightarrow b = x*h_2*x^{-1} \ni h_2 \in H$

$a*b^{-1} = (x*h_1*x^{-1})*(x*h_2*x^{-1})^{-1}$

$= (x*h_1*x^{-1})*(x*{h_2}^{-1}*x^{-1})$

$= (x*h_1)*(x^{-1}*x)*({h_2}^{-1}*x^{-1})$

$x * (h_1 * h_2{}^{-1}) * x^{-1} \in x * H * x^{-1}$

$\Rightarrow (x * H * x^{-1}, *)$ is a subgroup of $(G, *)$.

Note(7-20): The relation of conjugate is equivalent relation on the set of all subgroups of G. (**Homework**)

Definition(7-21): Let $(H,*)$ be a subgroup of $(G,*)$, then the conjugate class of H is denoted by $C(H)$ and define as

$$C(H) = \{x * H * x^{-1} : \forall x \in G\}$$

Example(7-22) $(S_3, \circ), H = \{f_1, f_4\}$:, find $C(H)$.

Solution: $C(H) = \{x * H * x^{-1} : \forall x \in S_3\}$

$= \{f_1 \circ \{f_1, f_4\} \circ f_1{}^{-1}, f_2 \circ \{f_1, f_4\} \circ f_2{}^{-1}, \dots, f_6 \circ \{f_1, f_4\} \circ f_6{}^{-1}\}$

$= \{\{f_1, f_4\}, \{f_1, f_6\}, \dots, \{f_1, f_5\}\}$

Example(7-23): $(G = \{e, a, b, c, d\}, *), a^2 = b^2 = c^2 = e$, is the four-Klien group. G is an abelian, $H = \{e, a\} \subseteq G$, find $C(H)$.

Solution: $C(H) = \{x * H * x^{-1} : \forall x \in G\}$

$= \{x * x^{-1} * H : \forall x \in G\} = H$.

Deffinition(7-24): Let $(H,*)$ be a subgroup of $(G,*)$, then the normalizer of H is denoted by $N(H)$ and defined as

$$N(H) = \{x \in G : x * H = H * x\}$$

Example(7-25): The group $(G_S, \circ), H = \{r_2, r_3\}$, find $N(H)$.

Solution: $N(H) = \{x \in G_S : x \circ H = H \circ x\}$

$x = r_1 \Rightarrow r_1 \circ H = H \circ r_1$

$x = r_2 \Rightarrow r_2 \circ H = H \circ r_2$

$N(H) = \{r_1, r_2, r_3, r_4, h, v, D_1, D_2\} = G_S$

Examples(7-26): Find $C(H), N(H)$ to each of the following:

1. The group $(S_3, \circ), H_1 = \{f_1, f_5\}, H_2 = \{f_1, f_4\}$. (**Homework**)
2. The group $(G_S, \circ), H_1 = \{r_3, r_1, v, h\}, H_2 = \{r_1, D_1\}$. (**Homework**)
3. The group $(Z_{12}, +_{12}), H = \{0,4,8\}$. (**Homework**)

Theorem(7-27): Let $(H,*)$ be a subgroup of $(G,*)$, then

1. $(N(H),*)$ is a subgroup of $(G,*)$ containing H.

Proof: since $e * H = H * e \Rightarrow e \in N(H) \neq \emptyset$

$N(H) = \{x \in G \ni x * H = H * x\} \subseteq G$

Let $a, b \in N(H)$, to prove $a * b^{-1} \in N(H)$

This means $(a * b^{-1}) * H = H * (a * b^{-1})$

Since $a \in N(H) \Rightarrow a * H = H * a$

$b \in N(H) \Rightarrow b * H = H * b$

$b * H * b^{-1} = H \Rightarrow H * b^{-1} = b^{-1} * H \Rightarrow b^{-1} \in N(H)$

$(a * b^{-1}) * H = a * (b^{-1} * H) = a * (H * b^{-1}) \ (b^{-1} \in N(H))$

$= (a * H) * b^{-1} = (H * a) * b^{-1} = H * (a * b^{-1})$

$\Rightarrow a * b^{-1} \in N(H) \Rightarrow (N(H),*)$ is a subgroup of $(G,*)$

To prove $H \subseteq N(H)$

Let $a \in H \Rightarrow a * H = H,\ H * a = H \Rightarrow a * H = H * a$

$\Rightarrow a \in N(H) \Rightarrow H \subseteq N(H)$

2. If $(G,*)$ is an abelian group, then $N(H) = G$.

Proof: suppose that G is an abelian group, to prove $N(H) = G$

This means $N(H) \subseteq G,\ G \subseteq N(H)$

By definition of $N(H) \Longrightarrow N(H) \subseteq G$

Let $x \in G \Longrightarrow x * H = H * x \Longrightarrow x \in N(H) \Longrightarrow G \subseteq N(H)$

$\Longrightarrow G = N(H)$

3. $O\big(C(H)\big) = O([G\colon N(H)])$ (**Homework**)
4. If $(G,*)$ is a finite group, then $\frac{O(G)}{O(C(H))}$

Note(7-28): If $N(H) = G$, then $(G,*)$ is an abelian group. (**Homework**)

Definition(7-29): A subgroup $(H,*)$ is called a self-conjugate iff $C(H) = H$, this means $x * H * x^{-1} = H\ \forall x \in G$.

Example(7-30): In $(S_3,\circ), H_1 = \{f_1, f_2, f_3\}, H_2 = \{f_1, f_5\}$

$C(H_1) = H_1 \Longrightarrow H_1$ is a self-conjugate

$C(H_2) \neq H_2 \Longrightarrow H_2$ is not a self-conjugate.

Definition(7-31): A subgroup $(H,*)$ is called a normal subgroup of $(G,*)$ denoted by $H \Delta G \Leftrightarrow H$ is a self-conjugate

Or $H \rhd G \Leftrightarrow x * H * x^{-1} = H\ \forall x \in G$

$H \ntriangleright G \Leftrightarrow \exists x \in G \ni x * H * x^{-1} \neq H$

Example(7-32): The group $(G_S,\circ), H = \{r_3, r_1, v, h\}$

$C(H) = H \Longrightarrow H \rhd G_S$

Example(7-33): The group $(S_3,\circ), H = \{f_1, f_5\}$

$C(H) \neq H \Longrightarrow H \ntriangleright S_3$

Example(7-34): The group $(Z_4, +_4), H = \{0,4\}$

$C(H) = H \Rightarrow H \rhd Z_4$

Theorem(7-35): Let $(H,*)$ be a subgroup of $(G,*)$, then

1. $H \rhd G \Leftrightarrow x * H = H * x \ \forall x \in G.$

Proof: $H \rhd G \Leftrightarrow x * H * x^{-1} = H \ \forall x \in G$

$\Leftrightarrow x * H = H * x \ \forall x \in G$

2. $H \rhd G \Leftrightarrow N(H) = G$

Proof: $(\Rightarrow)$ suppose that $H \rhd G$, to prove $N(H) = G$

This means $N(H) \subseteq G, G \subseteq N(H)$

$N(H) \subseteq G$ (by definition of $N(H)$)

To prove $G \subseteq N(H)$

Let $x \in G \Rightarrow x * H = H * x \Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$

$\Rightarrow G = N(H)$

$(\Leftarrow)$ suppose that $G = N(H)$, to prove $H \rhd G$

$\forall x \in G \Rightarrow x \in N(H) \Rightarrow x * H = H * x \Rightarrow H \rhd G$ (by 1)

3. $H \rhd G \Leftrightarrow c(a) \subseteq H \ \forall a \in H$

Proof: : $(\Rightarrow)$ suppose that $H \rhd G$, to prove $c(a) \subseteq H \ \forall a \in H$

Since $H \rhd G$ by definition $x * H * x^{-1} = H \Rightarrow x * H * x^{-1} \subseteq H$

$c(a) = \{x * a * x : \forall a \in H\} \subseteq H$

$(\Leftarrow)$ suppose that $c(a) \subseteq H \ \forall a \in H$

To prove $H \rhd G$, this means $x * H * x^{-1} = H$

Which is $x * H * x^{-1} \subseteq H,\ H \subseteq x * H * x^{-1}$

$c(a) \subseteq H \Rightarrow x * H * x^{-1} \subseteq H \ldots 1$

To prove $H \subseteq x * H * x^{-1}$

Let $b \in H \Rightarrow b = e * b * e$

$b = (x * x^{-1}) * b * (x * x^{-1}) = x * (x^{-1} * b * x) * x^{-1}$

$b = x * h * x^{-1} \in x * H * x^{-1}$

$\Rightarrow H \subseteq x * H * x^{-1} \ldots 2$

From 1,2, we get $H = x * H * x^{-1} \forall a \in G \Rightarrow H \rhd G$

4. $H \rhd G \Leftrightarrow (x * H) * (y * H) = (x * y) * H\ \forall x, y \in G$

Proof: ($\Rightarrow$) suppose that $H \rhd G \Rightarrow H * x = x * H$

$(x * H) * (y * H) = (x * H * y) * H = x * (H * y) * H$

$= x * (y * H) * H = (x * y) * (H * H) = (x * y) * H$

($\Leftarrow$) suppose that $H \ntriangleright G \Rightarrow \exists x \in G \ni x * H * x^{-1} \neq H$

$(x * H) * (x^{-1} * H) \neq H * H \Rightarrow (x * x^{-1}) * H \neq H$

$\Rightarrow e * H \neq H$, but this is contradiction $\Rightarrow H \rhd G$

<u>**Theorem(7-36):**</u> Let $(G,*)$ be a group, then

1. $\{e\} \rhd G$ (**Homework**)
2. $G \rhd G$ (**Homework**)
3. $C(G) \rhd G$ (**Homework**)

<u>**Theorem(7-37):**</u> Every subgroup of an abelian group is a normal subgroup.

Proof: let $(G,*)$ be an abelian group and $(H,*)$ be a subgroup of $(G,*)$, to prove $x * H * x^{-1} = H \ \forall x \in G$

$x * H * x^{-1} = (x * x^{-1}) * H = e * H = H \Longrightarrow H \rhd G.$

Note(7-38): The converse of above theorem is not true, for example

$(G = \{\pm 1, \pm i, \pm j, \pm k\}, \cdot) \ni i^2 = j^2 = k^2 = -1$

$ij = k$

$ji = -k \Longrightarrow ij \neq ji \Longrightarrow G$ is not an abelian.

The subgroups of G are $\{1\}, G, \{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}$

Theorem(7-39): Let $(H,*)$ be a subgroup of $(G,*) \ni [G{:}H] = 2$, then $H \rhd G$.

Proof: since $[G{:}H] = 2$, then there are two distinct left (right) cosets of H in G. $H, a * H \ni a \in G - H$ (left cosets of H in G)

$H, H * H \ni a \in G - H$ (right cosets of H in G)

$H \cup a * H = G, H \cap a * H = \emptyset \ldots 1$

$H \cup H * a = G, H \cap H * a = \emptyset \ldots 2$

If $a \in H \Longrightarrow a * H = H = H * a \Longrightarrow a * H = H * a \ \forall \ a \in H$

If $a \in G - H \Longrightarrow a * H = G - H = H * a \Longrightarrow a * H = H * a \ \forall \ a \in H$

$\Longrightarrow a * H = H * a \ \forall \ a \in G \Longrightarrow H \rhd G.$

Note(7-40): The converse of above theorem is not true, for example

$(G_S, \circ), H = \{r_1, r_4\}, H \rhd G_S$, but $[G_S{:}H] = 4 \neq 2$.

Note(7-41): If $H \rhd G$, then $H \cap G \not\rhd G, (H * K) \not\rhd G$, where H, K are two subgroups of the group $(G,*)$.

Consider $(S_3, \circ), H = \{f_1\} \rhd S_3$ and $K = \{f_1, f_4\} \not\trianglerighteq S_3$

$H * K = \{f_1, f_4\} \ntrianglerighteq S_3$, since $C(H * K) \neq H * K$.

$(G_S, \circ), H = \{r_1, r_3, h, v\}, K = \{r_1, v\}$

$H \cap K = \{r_1, v\} \ntrianglerighteq G_S$, since $C(H * K) \neq H * K$

$H \rhd G_S, K \ntrianglerighteq G_S$.

Definition(7-42): A group $(G, *)$ is called a simple group iff G has no proper normal subgroup.

Examples(7-43):

1. The group $(S_3, \circ)$ is not a simple, since $H = \{f_1, f_2, f_3\} \rhd S_3$.
2. The group $(G_S, \circ)$ is not a simple, since $H = \{r_1, r_3, h, v\} \rhd G_S$.
3. The group $(Z_6, +_6)$ is not a simple, since $H = \{0,3\} \rhd Z_6$.
4. The group $(Z_3, +_3)$ is a simple group, since Z_3 has no proper subgroup.

Definition(7-44): Let $H \rhd G$ and $\frac{G}{H} = \{x * H : x \in G\}$. Define $\otimes$ on $\frac{G}{H}$ as follows: $(x * H) \otimes (y * H) = (x * y) * H \ \forall x, y \in G$, $(\frac{G}{H}, \otimes)$ is called a quotient group of G by H.

Theorem(7-45): Let $H \rhd G$, then $(\frac{G}{H}, \otimes)$ is a group.

Proof: $\frac{G}{H} = \{x * H : x \in G\}$, since $e * H = H \in \frac{G}{H} \neq \emptyset$

Closure: let $a * H, b * H \in \frac{G}{H}$, $(a * H) \otimes (b * H) = (a * b) * H \in \frac{G}{H}$

Associative: let $a * H, b * H, c * H \in \frac{G}{H}$

$[(a * H) \otimes (b * H)] \otimes (c * H) = [(a * b) * H] \otimes (c * H)$

$= ((a * b) * c) * H = (a * (b * c)) * H = (a * H) \otimes [(b * c) * H]$

$= (a * H) \otimes [(b * H) \otimes (c * H)]$

Identity: $e * H = H \in \frac{G}{H}$

$(a*H)\otimes(e*H)=(a*e)*H=a*H \ \forall a*H\in\frac{G}{H}$

$(e*H)\otimes(a*H)=(e*a)*H=a*H$

$\Rightarrow e*H$ is an identity element of $\frac{G}{H}$

Inverse: let $a*H\in\frac{G}{H}$, to prove $(a*H)^{-1}=a^{-1}*H$

$(a*H)\otimes(a^{-1}*H)=(a*a^{-1})*H=e*H=H$

$(a^{-1}*H)\otimes(a*H)=(a^{-1}*a)*H=e*H=H$

$\Rightarrow \forall a*H\in\frac{G}{H}\ \exists a^{-1}*H\in\frac{G}{H}\Rightarrow(\frac{G}{H},\otimes)$ is a group.

<u>**Example(7-46):**</u> In the group $(Z_6,+_6), H=\{0,3\}$, find $\frac{Z_6}{H}$ (if exist).

Solution: $H\rhd Z_6\Rightarrow\frac{Z_6}{H}$ exist

$o+_6H=H$

$1+_6H=\{1,4\}$

$2+_6H=\{2,5\}$

$3+_6H=\{3,0\}=H$

$4+_6H=\{4,1\}=1+_6H$

$5+_6H=\{5,2\}=2+_6H$

$\Rightarrow\frac{Z_6}{H}=\{H,1+_6H,2+_6H\}$

$o\left(\frac{Z_6}{H}\right)=3$

$\otimes$	H	$1+_6H$	$2+_6H$

H	H	$1+_6H$	$2+_6H$
$1+_6H$	$1+_6H$	$2+_6H$	H
$2+_6H$	$2+_6H$	H	$1+_6H$

$\Rightarrow (\frac{Z_6}{H}, \otimes)$ is a quotient group, H is an identity.

$(1+_6H)^{-1} = 1^{-1}+_6H = 5+_6H = 2+_6H$

$(2+_6H)^{-1} = 2^{-1}+_6H = 4+_6H = 1+_6H$

<u>Example(7-47):</u> In the group $(Z_{20}, +_{20}), H = \langle 5 \rangle$, find $\frac{Z_{20}}{H}$ (if exist).(**Homework**)

<u>Example(7-48):</u> In the group $(S_3,\circ), H = \{f_1, f_2, f_3\}$, find $\frac{S_3}{H}$ (if exist).

Solution: since $H \rhd S_3 \Rightarrow \frac{S_3}{H}$ exist

$f_1 \circ H = H$

$f_2 \circ H = \{f_2, f_3, f_1\} = H$

$f_3 \circ H = \{f_3, f_1, f_2\} = H$

$f_4 \circ H = \{f_4, f_6, f_5\}$

$f_5 \circ H = \{f_5, f_4, f_6\} = f_4 \circ H$

$f_6 \circ H = \{f_6, f_5, f_4\} = f_4 \circ H$

$\Rightarrow \frac{S_3}{H} = \{H, f_4 \circ H\}$

But if $H = \{f_1, f_4\}, H \ntriangleright S_3 \Rightarrow \frac{S_3}{H}$ is not exist.

<u>Theorem(7-49):</u> The quotient group of an abelian is an abelian.

Proof: suppose that $(G,*)$ is an abelian group and $(H,*)$ is a subgroup of $(G,*) \ni$ $H \rhd G \Rightarrow \frac{G}{H}$ is a group

Let $a * H, b * H \in \frac{G}{H} \Longrightarrow (a * H) \otimes (b * H) = (a * b) * H$

$= (b * a) * H = (b * H) \otimes (a * H) \Longrightarrow (\frac{G}{H}, \otimes)$ is an abelian group.

Theorem(7-50): If $(G,*)$ is a cyclic group, then $(\frac{G}{H}, \otimes)$ is a cyclic group.

Proof: suppose that $(G,*)$ is a cyclic group, H is a subgroup of G.

$\Longrightarrow \exists a \in G \ni G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, since G is a cyclic$\Longrightarrow$ G is an abelian

$\Longrightarrow H \rhd G \Longrightarrow \frac{G}{H}$ is a group. To prove $\frac{G}{H}$ is a cyclic group, this means there is $a * H \in \frac{G}{H} \ni \frac{G}{H} = \langle a * H \rangle = \{(a * H)^k : k \in \mathbb{Z}\}$, to prove

$\frac{G}{H} \subseteq \langle a * H \rangle, \langle a * H \rangle \subseteq \frac{G}{H}$, let $x * H \in \frac{G}{H} \Longrightarrow x \in G = \langle a \rangle \Longrightarrow x = a^r, r \in \mathbb{Z}$

$x * H = a^r * H = (a * a * \dots * a) * H (r\text{-times})$

$= a * H \otimes \dots \otimes a * H (r\text{-times})$

$(a * H)^r \in \langle a * H \rangle \Longrightarrow x \in \langle a * H \rangle \Longrightarrow \frac{G}{H} \subseteq \langle a * H \rangle$

To prove $\langle a * H \rangle \subseteq \frac{G}{H}$, let $y * H \in \langle a * H \rangle$

$y * H = (a * H)^s \ni s \in \mathbb{Z}$

$y * H = a^s * H \in \frac{G}{H} \Longrightarrow y * H \in \frac{G}{H} \Longrightarrow \langle a * H \rangle \subseteq \frac{G}{H} \Longrightarrow \langle a * H \rangle = \frac{G}{H}$

Therefore, $(\frac{G}{H}, \otimes)$ is a cyclic group.

Note(7-51): The converse of above theorem is not true, for example:

$(S_3, \circ), H = \{f_1, f_2, f_3\} \rhd S_3 \Longrightarrow \frac{S_3}{H}$ is a group, $\frac{S_3}{H} = \{H, f_4 \circ H\}$

$O\left(\frac{S_3}{H}\right) = 2$ (prime order), $\frac{S_3}{H}$ is a cyclic group, but $(S_3, \circ)$ is not a cyclic

$\frac{S_3}{H} = \langle f_4 \circ H \rangle = \{f_4 \circ H, (f_4 \circ H)^2\} = \{f_4 \circ H, f_1 \circ H = H\}$

Theorem(7-52): Let $(G,*)$ be a group and $(\frac{G}{C(G)}, \otimes)$ is a cyclic group, then $(G,*)$ is an abelian group.

Note(7-53): The converse of this theorem is not true, for example:

$(G = \{e, a, b, c, d\},*), a^2 = b^2 = c^2 = e$, G is an abelian (not a cyclic)

$C(G) = G \Rightarrow \frac{G}{C(G)} = \frac{G}{G} = \{e, a, b, c, d\} \Rightarrow \frac{G}{C(G)}$ is not a cyclic.

Definition(7-54): Let $(G,*)$ be a group. If $a, b \in G$, then the commutator of a, b is $[a, b] = a * b * a^{-1} * b^{-1}$.

The commutator $[a, b] = e \Leftrightarrow a * b = b * a$, this means a, b are commute, the identity element $e = [e, e]$ is a commutator.

Example(7-55): In the group$(Z_4, +_4)$.

$[3,2] = 3 +_4 2 +_4 3^{-1} +_4 2^{-1} = 3 +_4 2 +_4 1 +_4 2 = 0$

Example(7-56): In the group$(\mathbb{Z}, +)$.

$[5,4] = 5 + 4 + 5^{-1} + 4^{-1} = 5 + 4 - 5 - 4 = 0$

Note(7-57): The commutator is an identity iff $(G,*)$ is an abelian group.

Definition(7-58): Let $(G,*)$ be a group, then the commutator subgroup of $(G,*)$ denoted by $[G, G]$ is the collection of all the finite products of commutators in G.

$[G, G] = \left\{\prod [a_i, b_i] : a_i, b_i \in G\right\} = \{[a_1, b_1] * [a_2, b_2] * \dots * [a_k, b_k]\}$

Theorem(7-59): The group $([G, G],*)$ is a normal subgroup.

Proof: to prove $[G, G]$ is a subgroup of G.

$[G,G] \neq \emptyset$, since $[e,e] \in [G,G], e \in G$

Let $x, y \in [G,G]$, to prove $x * y^{-1} \in [G,G]$

$x = [a_1, b_1] * \dots * [a_n, b_n]$

$y = [c_1, d_1] * \dots * [c_n, d_n]$

$x * y^{-1} = [a_1, b_1] * \dots * [a_n, b_n] * ([c_1, d_1] * \dots * [c_n, d_n])^{-1}$

$= [a_1, b_1] * \dots * [a_n, b_n] * [c_1, d_1] * \dots * [c_n, d_n] \in [G,G]$

Thus, $x * y^{-1} \in [G,G] \Rightarrow [G,G]$ is a subgroup of G.

To prove $[G,G]$ is a normal subgroup, let $x \in [G,G]$

To prove $x * [G,G] * x^{-1} \subseteq [G,G]$, let $a \in x * [G,G] * x^{-1}$

$a = x * c * x^{-1}, c \in [G,G] = x * c * x^{-1} * e = x * c * x^{-1} * c^{-1} * c$

$= x * c * (x^{-1} * c^{-1}) * c = [x, c] * c$

Therefore, $a \in [G,G] \Rightarrow [G,G]$ is a normal subgroup of G.

Theorem(7-60): Let $(H,*)$ be a normal subgroup of G, then $(\frac{G}{H}, \otimes)$ is an abelian iff $[G,G] \subseteq H$.

Proof: suppose that $a * H, b * H \in \frac{G}{H}$ and $\frac{G}{H}$ is an abelian

$\Leftrightarrow (a * b) * H = (b * a) * H \Leftrightarrow H * (a * b) = H * (b * a)$

$\Leftrightarrow a * b * (b * a)^{-1} \in H \Leftrightarrow [a, b] \in H$

$\Leftrightarrow [G,G] \subseteq H \; \forall [a,b] \in [G,G], a, b \in G$.

Corollary(7-61): Prove that $(\frac{G}{[G,G]}, \otimes)$ is an abelian group. (**Homework**)

8. Homomorphism, Examples and Basic Concepts

Definition(8-1): Let $(G,*),(G',\circ)$ be two groups and $f:(G,*) \longrightarrow (G',\circ)$ be a mapping, then f is called a homomorphism iff $f(a*b)=f(a)\circ f(b) \forall a,b \in G$.

Example(8-2): Let $f:(\mathbb{R},+) \longrightarrow (\mathbb{R}^+,\cdot), \ni f(a)=2^a \ \forall a \in \mathbb{R}$. Is f a homo. ?

Solution: let $a,b \in \mathbb{R} \Rightarrow f(a+b)=2^{a+b}=2^a \cdot 2^b = f(a)\cdot f(b)$

thus, f is a homo.

Example(8-3): Let $f:(\mathbb{Z},+) \longrightarrow (\mathbb{Z},+), \ni f(x)=3x+2 \ \forall x \in \mathbb{Z}$. Is f a homo. ?

Solution: let $x,y \in \mathbb{Z} \Rightarrow f(x+y)=3(x+y)+2$

$= 3x+3y+2 \ldots 1$

$f(x)+f(y)=(3x+2)+(3y+2)=3x+3y+4 \ldots 2$

We have $1 \neq 2 \Rightarrow f(x+y) \neq f(x)+f(y)$

Therefore, f is not a homo.

Example(8-4): Let $f:(S_3,\circ) \longrightarrow (S_3,\circ), \ni f(x)=x \ \forall x \in S_3$. Is f a homo. ? **(Homework)**

Example(8-5): Let $f:(Z_6,+_6) \longrightarrow (Z_6,+_6), \ni f(x)=x \ \forall x \in Z_6$. Is f a homo. ? **(Homework)**

Example(8-6): Let $f:(\mathbb{R},+) \longrightarrow (\mathbb{Z},+), \ni f(a)=2a-1 \ \forall a \in \mathbb{R}$. Is f a homo. ?

Solution: $f(a+b)=2(a+b)-1=2a+2b-1 \ldots 1$

$f(a)+f(b)=(2a-1)+(2b-1)=2a+2b-2 \ldots 2$

We have $1 \neq 2 \Rightarrow f(a+b) \neq f(a)+f(b)$

Therefore, f is not a homo.

Example(8-7): Let $f: (\mathbb{Z}, +) \longrightarrow (\{1, -1\}, \cdot)$,

$\ni f(a) = \begin{cases} 1 & a \ even \\ -1 & a \ odd \end{cases} \forall a \in \mathbb{Z}$. Is f a homo. ?

Solution: let $a, b \in \mathbb{Z}$

1. $a, b \in E$

$f(a + b) = 1, \quad (a + b \in E), f(a) \cdot f(b) = 1 \cdot 1 = 1$

2. $a, b \in O \Rightarrow a + b \in E$

$f(a + b) = 1, \quad (a + b \in E), f(a) \cdot f(b) = -1 \cdot -1 = 1$

3. If $a \in E,\ b \in O \Rightarrow a + b \in O$

$$f(a + b) = -1, \quad (a + b \in O), f(a) \cdot f(b) = 1 \cdot -1 = -1$$

Therefore, $f(a + b) = f(a) \cdot f(b)\ \forall a, b \in \mathbb{Z} \Longrightarrow f$ is a homo.

Example(8-8): Let $f: (G, *) \longrightarrow (G, *) \ni f(a) = x * a * x^{-1}\ \forall a \in G$. Is f a homo. ?

Solution: let $a, b \in G \ni f(a * b) = x * (a * b) * x^{-1}$ ... 1

$f(a) * f(b) = (x * a * x^{-1}) * (x * b * x^{-1})$

$= x * (a * b) * x^{-1}$ ... 2

We have $1 = 2 \Longrightarrow$ therefore, f is a homo.

Example(8-9): Let $f: (G, *) \longrightarrow (G', \cdot) \ni f(a) = e'\ \forall a \in G$. Is f a homo. ?

Solution: let $a, b \in G \ni f(a * b) = e' = e' \cdot e' = f(a) \cdot f(b)$

$\Longrightarrow$ Therefore, f is a trivial homo.

Example(8-10): Let $H \rhd G$ and $f: (G, *) \longrightarrow \left(\frac{G}{H}, \otimes\right) \ni f(a) = a * H\ \forall a \in G$. Is f a homo. ?

Solution: let $a, b \in G \ni f(a * b) = (a * b) * H \ldots 1$

$f(a) \otimes f(b) = (a * H) \otimes (b * H) = (a * b) * H \ldots 2$

We have $1 = 2 \Longrightarrow$ Therefore, f is a natural homo.

Definition(8-11): Let $f: (G,*) \longrightarrow (G',\circ)$ be a mapping, then

1. f is called a monomorphism (mono.) iff f is a homo. and one to one.
2. f is called an epimorphism (epi.) iff f is a homo. and onto.
3. f is called an isomorphism (iso.) iff f is a homo., one to one and onto.

Definition(8-12): Any two groups $(G,*), (G',\circ)$ are isomorphic iff there is an isomorphism map between them and denoted by $G \cong G'$.

This means, $G \cong G' \Leftrightarrow \exists f: (G,*) \longrightarrow (G',\circ)$ and f is an isomorphism.

Example(8-13): Let $(G = \{2^n : n \in \mathbb{Z}\}, \cdot)$, show that $(\mathbb{Z}, +) \cong (G, \cdot)$.

Solution: define $f: (\mathbb{Z}, +) \longrightarrow (G, \cdot) \ni f(n) = 2^n \ \forall n \in \mathbb{Z}$

Homo.? let $n_1, n_2 \in \mathbb{Z} \Longrightarrow f(n_1 + n_2)$

$= 2^{n_1+n_2} = 2^{n_1} \cdot 2^{n_2} = f(n_1) \cdot f(n_2) \Longrightarrow f$ is a homo.

One to one? let $f(n_1) = f(n_2)$, to prove $n_1 = n_2$

$2^{n_1} = 2^{n_2} \Longrightarrow n_1 = n_2 \Longrightarrow f$ is a one to one

Onto? $R_f = \{f(n) : n \in \mathbb{Z}\} = \{2^n : n \in \mathbb{Z}\} = G \Longrightarrow f$ is an onto

$\Longrightarrow f$ is an isomorphism $\Longrightarrow (\mathbb{Z}, +) \cong (G, \cdot)$

Theorem(8-14): Let $f: (G,*) \longrightarrow (G',\cdot)$ be an isomorphism, then

1. $f(e) = e'$ such that e the identity of G.

Proof: let $a \in G \Longrightarrow a * e = a \Longrightarrow f(a * e) = f(a)$

$f(a) \cdot f(e) = f(a)$

Let $f(a) \in G' \Rightarrow f(a) \cdot e' = f(a) \Rightarrow f(a) \cdot f(e) = f(a) \cdot e'$

$\Rightarrow f(e) = e'$.

2. $f(a^{-1}) = (f(a))^{-1} \forall a \in G$

Proof: let $a \in G \Rightarrow a * a^{-1} = e \Rightarrow f(a * a^{-1}) = f(e) = e'$

$f(a) \cdot f(a^{-1}) = f(e) = e'$

let $f(a) \in G' \Rightarrow f(a) \cdot \left(f(a)\right)^{-1} = e'$

$f(a) \cdot f(a^{-1}) = f(a) \cdot \left(f(a)\right)^{-1} \Rightarrow (a^{-1}) = (f(a))^{-1}$.

3. If $(H,*)$ is a subgroup of a group $(G,*)$, then $(f(H),\cdot)$ is a subgroup of $(G',\cdot)$.

Proof: $f(H) = \{f(x): x \in H\} \subseteq G'$

$e \in H \Rightarrow f(e) \in f(H) \Rightarrow e' \in f(H) \neq \emptyset$

Let $a, b \in f(H)$, to prove $a \cdot b^{-1} \in f(H)$

$a \in f(H) \Rightarrow a = f(x) \ni x \in H$

$b \in f(H) \Rightarrow b = f(y) \ni y \in H$

$\Rightarrow x * y^{-1} \in H \Rightarrow a \cdot b^{-1} = f(x) \cdot \left(f(y)\right)^{-1} = f(x) \cdot f(y^{-1})$

$= f(x * y^{-1}) \Rightarrow a \cdot b^{-1} = f(x * y^{-1}) \in f(H)$

4. If $(K,\cdot)$ is a subgroup of $(G',\cdot)$, then $(f^{-1}(K),*)$ is a subgroup of $(G,*)$.

Proof: $f^{-1}(K) = \{x \in G: f(x) \in K\} \subseteq G$

$f(e) = e' \Rightarrow e \in f^{-1}(K) \Rightarrow f^{-1}(K) \neq \emptyset$

Let $x, y \in f^{-1}(K)$, to prove $x * y^{-1} \in f^{-1}(K)$

$x \in f^{-1}(K) \Rightarrow f(x) \in K$

$y \in f^{-1}(K) \Rightarrow f(y) \in K$

$f(x) \cdot (f(y))^{-1} \in K \Rightarrow f(x) \cdot f(y^{-1}) \in K \Rightarrow f(x * y^{-1}) \in K$

$\Rightarrow x * y^{-1} \in f^{-1}(K) \Rightarrow (f^{-1}(K), *)$ is a subgroup of $(G, *)$.

5. If $H \rhd G$ and f an onto, then $f(H) \rhd G'$.

Proof: let $y \in G', a \in f(H)$, to prove $y \cdot a \cdot y^{-1} \in f(H)$

$y \in G'$ and f is an onto $\Rightarrow \exists x \in G \ni f(x) = y$

$a \in f(H) \Rightarrow a = f(h) \ni h \in H$

$x \in G, h \in H$ and $H \rhd G \Rightarrow x * h * x^{-1} \in H$

$\Rightarrow f(x * h * x^{-1}) \in f(H) \Rightarrow f(x) \cdot f(h) \cdot f(x^{-1}) \in f(H)$

$\Rightarrow y \cdot a \cdot y^{-1} \in f(H) \Rightarrow f(H) \rhd G'$.

6. If $K \rhd G'$, then $f^{-1}(K) \rhd G$.

Proof: $(f^{-1}(K), *)$ is a subgroup of $(G, *)$, to prove $f^{-1}(K) \rhd G$

Let $x \in G \Rightarrow f(x) = y \in G'$

$a \in f^{-1}(K) \Rightarrow f(a) \in K$

$f(x) \in G'$, $f(a) \in K$ and $K \rhd G'$

$f(x) \cdot f(a) \cdot (f(x))^{-1} \in K \Rightarrow f(x) \cdot f(a) \cdot f(x^{-1}) \in K$

$\Rightarrow f(x * a * x^{-1}) \in K \Rightarrow x * a * x^{-1} \in f^{-1}(K) \Rightarrow f^{-1}(K) \rhd G$.

<u>Theorem(8-15):</u> The relation of isomorphic is an equivalent.

Proof: Reflexive: to prove $(G,*) \cong (G,*), \exists\, i: (G,*) \longrightarrow (G,*) \ni i(x) = x\ \forall x \in G$ and i is a homomorphism, one to one and onto, thus i is an isomorphism $\Longrightarrow (G,*) \cong (G,*)$.

Symmetric: let $(G,*) \cong (G',\cdot)$, to prove $(G',\cdot) \cong (G,*)$, $\exists\, f: (G,*) \longrightarrow (G',\cdot) \ni f$ is an isomorphism, f is a bijective

$\Longrightarrow \exists f^{-1}: (G',\cdot) \longrightarrow (G,*) \Longrightarrow f^{-1}$ is an one to one and onto, to prove f^{-1} is a homomorphism, let $a, b \in G', f$ is an onto$\Longrightarrow \exists x, y \in G \ni f(x) = a, f(y) = b, f^{-1}(a \cdot b) = f^{-1}\big(f(x) \cdot f(y)\big) = f^{-1}\big(f(x * y)\big) = x * y = f^{-1}(a) * f^{-1}(b)$

Thus, f^{-1} is a homomorphism, f^{-1} is an isomorphism,

$\Longrightarrow (G',\cdot) \cong (G,*)$.

Transitive: let $(G,*) \cong (G',\cdot)$ and $(G',\cdot) \cong (G'',\odot)$, to prove

$(G,*) \cong (G'',\odot), \exists\, f: (G,*) \longrightarrow (G',\cdot) \ni f$ is an isomorphism, $\exists\, g: (G',\cdot) \longrightarrow (G'',\odot) \ni g$ is an isomorphism. $\exists g \circ f: (G,*) \longrightarrow (G'',\odot) \ni g \circ f$ is a bijective. Let $a, b \in G, (g \circ f)(a * b) = g\big(f(a * b)\big) = g\big(f(a) \cdot f(b)\big) = g\big(f(a)\big) \odot g\big(f(b)\big) = (g \circ f)(a) \odot (g \circ f)(b)$

Hence, $g \circ f$ is a homomorphism$\Longrightarrow g \circ f$ is an isomorphism

$\Longrightarrow (G,*) \cong (G'',\odot) \Longrightarrow \cong$ is an equivalent relation.

Theorem(8-16): Prove that

1. Every two finite cyclic group of the same order are isomorphic.

Proof: let $(G,*), (G',\cdot)$ are two finite cyclic groups, $\ni O(G) = O(G') = n$

G is a cyclic $\Longrightarrow \exists a \in G \ni G = \langle a \rangle = \{a^k, k \in \mathbb{Z}\} = \{a^1, a^2, \dots, a^k = e\}$

G' is a cyclic $\Longrightarrow \exists b \in G' \ni G' = \langle b \rangle = \{b^n, n \in \mathbb{Z}\} = \{b, b^2, \dots, b^n = e\}$

Define $f:(G,*) \longrightarrow (G',\cdot) \ni f(a^k) = b^k \forall k \in \mathbb{Z}$, let $a^r = a^s \Rightarrow r \equiv s (\mathrm{mod}\, n) \Rightarrow r - s = ng \ni g \in \mathbb{Z} \Rightarrow r = ng + s \Rightarrow b^r = b^{ng+s} = (b^n)^g \cdot b^s \Rightarrow b^r = b^s$, thus f is a map.

Let $f(a^r) = f(a^s) \Rightarrow b^r = b^s \Rightarrow r \equiv s(\mathrm{mod}\, n) \Rightarrow r - s = ng \Rightarrow r = ng + s \Rightarrow a^r = (a^n)^g \cdot a^s \Rightarrow a^r = a^s \Rightarrow f$ is a one to one.

$R_f = \{f(a^k): \forall k \in \mathbb{Z}\} = \{b^k: \forall k \in \mathbb{Z}\} = G' \Rightarrow f$ is an onto.

$f(a^r * a^s) = f(a^{r+s}) = b^{r+s} = b^r \cdot b^s = f(a^r) \cdot f(a^s) \Rightarrow f$ is a homomorphism$\Rightarrow f$ is an isomorphism$\Rightarrow G \cong G'$.

2. Every finite cyclic group is an isomorphism to$(Z_n, +_n)$.

Proof: let $(G,*)$ be a finite cyclic group $\ni O(G) = m$

$G = \langle a \rangle = \{a^1, a^2, \dots, a^m = e\}$

(1) if $m < n \Rightarrow O(G) < O(Z_n) \Rightarrow f$ is not an onto$\Rightarrow G \ncong Z_n$

(2) if $m = n \Rightarrow G \cong Z_n$

define $f:(G,*) \longrightarrow (Z_n, +_n) \ni f(a^k) = k \ \forall k \in \mathbb{Z}^+$, let $a^r = a^s \Rightarrow r \equiv s(\mathrm{mod}\, n) \Rightarrow r = s \Rightarrow f(a^r) = f(a^s) \Rightarrow f$ is a map.

Let $f(a^r) = f(a^s) \Rightarrow r \equiv s(\mathrm{mod}\, n) \Rightarrow r = ng + s \Rightarrow a^r = a^s \Rightarrow f$ is an one to one.

$f(a^r * a^s) = f(a^{r+s}) = r + s = r +_n s = f(a^r) +_n f(a^s) \Rightarrow f$ is a homomorphism.

$R_f = \{f(a^k): \forall k \in \mathbb{Z}^+\} = \{k: \forall k \in \mathbb{Z}^+\} = Z_n \Rightarrow f$ is an onto$\Rightarrow f$ is an isomorphism$\Rightarrow (G,*) \cong (Z_n, +_n)$.

3. Every two infinite cyclic group are isomorphic.

Proof: let $(G,*), (G',\cdot)$ are infinite cyclic groups.

$G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$

$G' = \langle b \rangle = \{\dots, b^{-2}, b^{-1}, b^0, b^1, b^2, \dots\}$

Define $f: (G,*) \longrightarrow (G',\cdot) \ni f(a^k) = b^k \forall k \in \mathbb{Z}$

- f is a map **(Homework)**
- f is an one to one **(Homework)**
- f is an onto **(Homework)**
- f is a homomorphism **(Homework)**

4. Every infinite cyclic group is an isomorphic to $(\mathbb{Z}, +)$.

Proof: since G is a cyclic $\Longrightarrow G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$

$G \longrightarrow \cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots$

$\mathbb{Z} \longrightarrow \cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots$

Define $f: (G,*) \longrightarrow (\mathbb{Z}, +) \ni f(a^k) = k \forall k \in \mathbb{Z}$ **(check)**

<u>Definition(8-17):</u> Let $(G,*)$ be a group, define

(1) $\text{Hom}(G) = \{f : f: (G,*) \longrightarrow (G,*) \ni f \text{ is a homomorphism}\}$

(2) $\text{Aut}(G) = \{f : f: (G,*) \longrightarrow (G,*) \ni f \text{ is an isomorphism}\}$

<u>Theorem(8-18):</u> Let $(G,*)$ be a group, then

(1) $(\text{Aut}(G), \circ)$ is a group.

Proof: 1,2 and 3 **(check)**

Inverse: let $f: (G,*) \longrightarrow (G,*)$, f is an isomorphism, since f is a bijective $\Longrightarrow$ $\exists f^{-1}: (G,*) \longrightarrow (G,*)$ and since f is an isomorphism $\Longrightarrow f^{-1}$ is an isomorphism $\Longrightarrow$ $f^{-1} \in \text{Aut}(G)$ and $f \circ f^{-1} = f^{-1} \circ f = i \Longrightarrow (\text{Aut}(G), \circ)$ is a group.

(2) $(\text{Aut}(G), \circ)$ is a subgroup of $(\text{Symm}(G), \circ)$.

Proof: $\text{Aut}(G) = \{f : f: (G,*) \longrightarrow (G,*) \ni f \text{ is an isomorphism}\}$

$\text{Symm}(G) = \{f: f: (G,*) \longrightarrow (G,*) \ni f \text{ is a bijective}\}$

$\text{Aut}(G) \neq \emptyset$, since $\exists i: (G,*) \longrightarrow (G,*) \ni i$ is an isomorphism

$\text{Aut}(G) \subseteq \text{Symm}(G)$ and $(\text{Aut}(G),\circ)$ is a group

$\Rightarrow (\text{Aut}(G),\circ)$ is a subgroup of $(\text{Symm}(G),\circ)$.

Definition(8-19): Let $(G,*)$ be a group and $x \in G$. Define $f_x: (G,*) \longrightarrow (G,*) \ni f_x(a) = x * a * x^{-1}, \forall a \in G$, then f_x is called an inner automorphism of G and $\text{Inn}(G) = \{f_x: \forall x \in G\}$ or $\text{I}(G) = \{f_x: \forall x \in G\}$.

Theorem(8-20): Let $(G,*)$ be a group and $x \in G$, then:

(1) f_x is an isomorphism map.

Proof: $f_x(a) * f_x(b) = (x * a * x^{-1}) * (x * b * x^{-1})$

$= x * a * (x^{-1} * x) * b * x^{-1} = x * a * b * x^{-1} = f_x(a * b)$

Thus, f_x is a homomorphism.

Let $f_x(a) = f_x(b) \Rightarrow x * a * x^{-1} = x * b * x^{-1} \Rightarrow a = b \Rightarrow f_x$ is an one to one.

$R_{f_x} = \{f_x(a): \forall a \in G\} = G \Rightarrow f_x$ is an isomorphism map.

(2) $(\text{I}(G),\circ)$ is a subgroup of $(\text{Aut}(G),\circ)$.

Proof: $\text{I}(G) = \{f_x: f_x: (G,*) \longrightarrow (G,*) \ni f_x \text{ is an isomorphism}\}$

$\text{Aut}(G) = \{f: f: (G,*) \longrightarrow (G,*) \ni f \text{ is an isomorphism}\}$

$a \in G \Rightarrow f_e \in \text{I}(G) \neq \emptyset$

$f_e(a) = e * a * e^{-1} = a \Rightarrow \text{I}(G) \subseteq \text{Aut}(G)$

Closure: let $f_x, f_y \in \text{I}(G)$, $(f_x \circ f_y)(a) = f_x(f_y(a)) = f_x(y * a * y^{-1}) = x * (y * a * y^{-1}) * x^{-1} = (x * y) * a * (x * y)^{-1} = f_{x*y}(a)$

Inverse: let $f_x \in \mathrm{I}(G), x^{-1} \in G \Rightarrow f_{x^{-1}} \in \mathrm{I}(G)$, $f_x \circ f_{x^{-1}} = f_{x*x^{-1}} = f_e \Rightarrow f_{x^{-1}} \circ f_x = f_{x^{-1}*x} = f_e \Rightarrow (f_x)^{-1} = f_{x^{-1}} \Rightarrow (\mathrm{I}(G),\circ)$ is a subgroup of $(\mathrm{Aut}(G),\circ)$.

(3) $\mathrm{I}(G) \rhd \mathrm{Aut}(G)$

Proof: $\mathrm{I}(G) = \{f_x : f_x : (G,*) \longrightarrow (G,*) \ni f_x$ is an isomorphism$\}$

$\mathrm{Aut}(G) = \{f : f : (G,*) \longrightarrow (G,*) \ni f$ is an isomorphism$\}$

Let $g \in \mathrm{Aut}(G), f_x \in \mathrm{I}(G), (g \circ f_x \circ g^{-1})(a) = g \circ f_x(g^{-1}(a)) = g(f_x(g^{-1}(a)) = g(x * g^{-1}(a) * x^{-1}) = g(x) * a * g(x^{-1}) = g(x) * a * (g(x))^{-1} = f_{g(x)}(a) \in \mathrm{I}(G) \Rightarrow \mathrm{I}(G) \rhd \mathrm{Aut}(G)$.

Definition(8-21): Let $f : (G,*) \longrightarrow (G',\cdot)$ be a group homomorphism, then the kernel of f denoted by $\ker f$ and defined by $\ker f = \{x \in G : f(x) = e'\}$

Example(8-22): let $f : (\mathbb{R},+) \longrightarrow (\mathbb{R}^+,\cdot) \ni f(x) = 3^x$, find $\ker f$ $\forall x \in \mathbb{R}$.

Solution: f is a homomorphism (**check**) $\Rightarrow \ker f$ an exist,

$\ker f = \{x \in \mathbb{R} : f(x) = 1\} = \{x \in \mathbb{R} : 3^x = 1\} = \{x = 0\}$

Example(8-23): Let $f : (G,*) \longrightarrow (G',\cdot) \ni f$ is a trivial homomorphism, find $\ker f$ $\forall x \in G$.

Solution: $f(x) = e'$ $\forall x \in G, f$ is a homomorphism $\Rightarrow \ker f$ is an exist.

$\ker f = \{x \in G : f(x) = e'\} = G$.

Example(8-24): let $f : (\mathbb{Z},+) \longrightarrow (Z_3,+_3) \ni f(x) = [x]\ \forall x \in \mathbb{Z}$, find $\ker f$ $\forall x \in \mathbb{Z}$.

Solution: f is a homomorphism (**check**)

$\mathrm{Ker} f = \{x \in \mathbb{Z} : f(x) = [0]\} = \{x \in \mathbb{Z} : [x] = [0]\} = \{x \in \mathbb{Z} : x \equiv 0 (\mathrm{mod}\ 3)\} = \{x \in \mathbb{Z} : x = 3k\ \forall k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\} \subseteq \mathbb{Z}$.

Theorem(8-25): Let $f : (G,*) \longrightarrow (G',\cdot)$ be a group homomorphism, then:

(1) $(\text{Ker}f,*)$ is a subgroup of $(G,*)$.

Proof: $\ker f=\{x\in G: f(x)=e'\}\subseteq G, f(e)=e' \Rightarrow e\in \ker f\neq \emptyset$.

Let $a,b\in\ker f$, $f(a*b^{-1})=f(a)\cdot f(b^{-1})=f(a)\cdot f(b))^{-1}=e'\cdot(e')^{-1}=e'\Rightarrow$ $f(a*b^{-1})=e'\Rightarrow a*b^{-1}\in\ker f \Rightarrow$ $(\text{Ker}f,*)$ is a subgroup of $(G,*)$.

(2) $\text{Ker}f \rhd G$

Proof: $(\text{Ker}f,*)$ is a subgroup of $(G,*)$.

Let $x\in G, a\in \text{Ker}f, f(x*a*x^{-1})=f(x)\cdot f(a)\cdot f(x^{-1})=f(x)\cdot e'\cdot (f(x))^{-1}=e'\Rightarrow x*a*x^{-1}\in\text{Ker}f\Rightarrow \text{Ker}f\rhd G$.

(3) $\text{Ker}f=\{e\}$ iff f is an one to one.

Proof: $(\Rightarrow)$ suppose that $\text{Ker}f=\{e\}$

Let $f(a)=f(b)\Rightarrow f(a)\cdot (f(b))^{-1}$

$=f(b)\cdot (f(b))^{-1}\Rightarrow f(a)\cdot f(b^{-1})=e'$

$\Rightarrow f(a*b^{-1})=e'\Rightarrow a*b^{-1}\in\text{Ker}f\Rightarrow a*b^{-1}=e \Rightarrow a=b$

$(\Leftarrow)$ let $a\in\text{Ker}f$

$f(a)=f(e)\Rightarrow a=e\Rightarrow \text{Ker}f=\{e\}$.

9. Fundamental Theorems of Homomorphism

The First Fundamental Theorem of Isomorphism:

Theorem(9-1): Let $f:(G,*) \longrightarrow (G',\cdot)$ be an onto, homomorphism, then

$(\frac{G}{\ker f},\otimes) \cong (G',\cdot)$.

Proof: f is an onto $\Rightarrow R_f = \{f(a): a \in G\} = G'$

$\ker f \rhd G \Rightarrow \frac{G}{\ker f}$ is a group.

Define $\left(\frac{G}{\ker f},\otimes\right) \longrightarrow (G',\circ) \ni g(a * \ker f) = f(a)\ \forall a \in G$

Let $a * \ker f = b * \ker f \Rightarrow a^{-1} * b \in \ker f \Rightarrow f(a^{-1} * b) = e'$

$\Rightarrow f(a^{-1}) \cdot f(b) = e' \Rightarrow \left(f(a)\right)^{-1} \cdot f(b) = e' \Rightarrow f(b) = f(a)$

$\Rightarrow g(a * \ker f) = g(b * \ker f) \Rightarrow g$ is a map.

Let $g(a * \ker f) = g(b * \ker f) \Rightarrow f(a) = f(b)$

$\Rightarrow e' = \left(f(a)\right)^{-1} \cdot f(b) = f(a^{-1}) \cdot f(b) \Rightarrow e' = f(a^{-1} * b)$

$\Rightarrow a^{-1} * b \in \ker f \Rightarrow a * \ker f = b * \ker f \Rightarrow g$ is an one to one.

$R_g = \{g(a * \ker f): a \in G = \{f(a): a \in G\} = G' \Rightarrow g$ is onto.

$g[(a * \ker f)\otimes(b * \ker f)] = g((a * b) * \ker f)$

$= f(a * b) = f(a) \cdot f(b) = g(a * \ker f) \cdot g(a * \ker f)$

$\Rightarrow g$ is a homomorphism, hence g is an isomorphism

$\Rightarrow (\frac{G}{\ker f},\otimes) \cong (G',\cdot)$

Example(9-2): Let $f: (\mathbb{Z}, +) \longrightarrow (\{1, -1\}, \cdot) \ni f(a) = \begin{cases} 1 & a \in E \\ -1 & a \in O \end{cases}$

$\forall a \in \mathbb{Z}$, show that $(Z_2, +_2) \cong (\{1, -1\}, \cdot)$ by two ways.

(1) Since $O(Z_2) = O(\{1, -1\}) = 2$ and $(Z_2, +_2), (\{1, -1\}, \cdot)$ are cyclic groups $\Rightarrow (Z_2, +_2) \cong (\{1, -1\}, \cdot)$

(2) By use the first theorem of isomorphism if is clear that f is a homomorphism. $R_g = \{f(a): a \in \mathbb{Z}\} = \{1, -1\} = \text{Cod } f$

$\Rightarrow f$ is an onto $\Rightarrow (\frac{\mathbb{Z}}{\ker f}, \otimes) \cong (\{1, -1\}, \cdot)$

$\ker f = \{a \in \mathbb{Z}: f(a) = 1\} = E \Rightarrow (\frac{\mathbb{Z}}{E}, \otimes) \cong (\{1, -1\}, \cdot)$

$(\mathbb{Z}, +)$ is a cyclic group $\Rightarrow (\frac{\mathbb{Z}}{E}, \otimes)$ is a cyclic

$O\left(\frac{\mathbb{Z}}{E}\right) = 2 \Rightarrow (Z_2, +_2) \cong (\frac{\mathbb{Z}}{E}, \otimes) \Rightarrow (Z_2, +_2) \cong (\{1, -1\}, \cdot)$

Corollary(9-3): Let $(G, *)$ be a group, then $(\frac{G}{Z(G)}, \otimes) \cong (I(G), \circ)$, where $Z(G)$ is a center of G.

Proof: define $g: (G, *) \longrightarrow (I(G), \circ) \ni g(x) = f_x \forall x \in G$

$I(G) = \{f_x: x \in G\}$

Let $x = y \Rightarrow x + a = y + a \Rightarrow x * a * x^{-1} = y * a * y^{-1}$

$\Rightarrow f_x(a) = f_y(a) \Rightarrow g(x) = g(y) \Rightarrow g$ is a map.

$g(x * y) = f_{x*y} = f_x \circ f_y = g(x) \circ g(y) \Rightarrow g$ is a homomorphism.

$R_g = \{g(x): x \in G\} = \{f_x: \forall x \in G\} = I(G) \Rightarrow g$ is an onto.

By the first theorem of isomorphism $\Rightarrow (\frac{G}{kerf}, \otimes) \cong (I(G), \circ)$

$ker f = \{x \in G: g(x) = e'\} = \{x \in G: f_x(a) = f_e(a)$

$= \{x \in G: x * a * x^{-1} = a\ \forall a \in G\} = \{x \in G: x * a = a * x\ \forall a \in G\}$

$= Z(G) \Rightarrow (\frac{G}{Z(G)}, \otimes) \cong (I(G), \circ)$

The Second Theorem of Isomorphism:

Theorem(9-4): Let $(H,*), (K,*)$ be two subgroups of $(G,*) \ni K \rhd H$, then

(1) $(H * K,*)$ is a subgroup of $(G,*)$

(2) $K \rhd H * K$

(3) $(H \cap K) \rhd H$

(4) $(\frac{H*K}{K}, \otimes) \cong (\frac{H}{H \cap K}, \otimes)$

Proof: since $K \rhd H * K \Rightarrow (\frac{H*K}{K}, \otimes)$ is a group.

And since $(H \cap K) \rhd H \Rightarrow (\frac{H}{H \cap K}, \otimes)$ is a group.

Define $f: (H * K,*) \longrightarrow \left(\frac{H}{H \cap K}, \otimes\right) \ni f(a * b) = a * (H \cap K) \forall a \in H$

$a * b = c * d \Rightarrow c^{-1} * a = d * b^{-1} \Rightarrow c^{-1} * a \in H, c^{-1} * a \in K$

$\Rightarrow c^{-1} * a \in H \cap K \Rightarrow c * (H \cap K) = a * (H \cap K)$

$\Rightarrow f(c * d) = f(a * b) \Rightarrow f$ is a map.

$R_f = \{f(a * b): \forall a \in H\} = \{a * (H \cap K): a \in H\} = \dfrac{H}{H \cap K}$

Thus, f is an onto.

$f[(a * b) * (c * d)] = f[(a * c * c^{-1} * b) * (c * d)]$

$= f[(a * c) * (c^{-1} * b * c) * d]$

Since $c \in G, b \in K, K \rhd G \Rightarrow c * b * c^{-1} \in K$

Let $c * b * c^{-1} = r \in K$

$f[(a * b) * (c * d)] = f[(a * c) * (r * d)] = (a * c) * (H \cap K)$

$= [a * (H \cap K)] \otimes [c * (H \cap K)] = f(a * b) \otimes f(c * d) \Rightarrow f$ is a homo.

By the first theorem of isomorphism $\Rightarrow \frac{H*K}{kerf} \cong \frac{H}{H \cap K}$

$kerf = \{a * b \in H * K \ni f(a * b) = e'\}$

$= \{a * b \in H * K \ni a * (H \cap K) = H \cap K\}$

$= \{a * b \in H * K \ni a \in H \cap K\}$

$= \{a * b \in H * K \ni a \in H, a \in K\}$

$= \{a * b \in H * K \ni a \in K, b \in K\} = K$

Therefore, $\frac{H*K}{K} \cong \frac{H}{H \cap K}$

The Third Fundamental Theorem of Isomorphism:

Theorem(9-5): Let $(H,*), (K,*)$ be two normal subgroups of $(G,*) \ni H \subseteq K$, then:

(1) $H \rhd K$

(2) $(\frac{K}{H}, \otimes) \rhd (\frac{G}{H}, \otimes)$

(3) $(\frac{\frac{G}{H}}{\frac{K}{H}}, \otimes) \cong (\frac{G}{K}, \otimes)$

Proof: 1. Since $(H,*), (K,*)$ are subgroups and $H \subseteq K$

$\Rightarrow (H,*)$ is a subgroup of $(K,*)$

Let $x \in K, a \in H, x \in K \subseteq G \Rightarrow x \in G, a \in H, H \rhd G \Rightarrow x * a * x^{-1} \in H$

Thus, $H \rhd K$.

Proof: 2. since $H \rhd K \Rightarrow (\frac{K}{H}, \otimes)$ is a group

Since $H \rhd G \Rightarrow (\frac{G}{H}, \otimes)$ is a group

$$\frac{K}{H} = \{a * H : a \in K\} \subseteq \{a * H : a \in G\} = \frac{G}{H}$$

$\frac{K}{H} \subseteq \frac{G}{H} \Rightarrow (\frac{K}{H}, \otimes)$ is a subgroup of $(\frac{G}{H}, \otimes)$

Let $x * H \in \frac{G}{H}, a * H \in \frac{K}{H}$

$(x * H) \otimes (a * H) \otimes (x * H)^{-1}$

$= \big((x * a) * H\big) \otimes (x^{-1} * H) = (x * a * x^{-1}) * H$

$\Rightarrow (x * a * x^{-1}) * H \in \dfrac{K}{H} \Rightarrow (\dfrac{K}{H}, \otimes) \rhd (\dfrac{G}{H}, \otimes)$

Proof: 3. $\frac{K}{H} \rhd \frac{G}{H} \Rightarrow (\frac{\frac{G}{H}}{\frac{K}{H}}, \otimes)$ is a group.

$K \rhd G \Rightarrow (\frac{G}{H}, \otimes)$ is a group.

Define $f: \left(\frac{G}{H}, \otimes\right) \longrightarrow \left(\frac{G}{K}, \otimes\right) \ni f(a * H) = a * K \ \forall a \in G$

$a * H = b * H \Rightarrow a^{-1} * b \in H \subseteq K \Rightarrow a^{-1} * b \in K \Rightarrow a * K = b * K$

$\Rightarrow f(a * H) = f(b * H) \Rightarrow f$ is a map.

$R_f = \{f(a * H) : a \in G\} = \{a * K : a \in G\} = \frac{G}{K} \Rightarrow f$ is an onto.

$f[(a * H) \otimes (b * H)] = f[(a * b) * H = (a * b) * K = (a * K) \otimes (b * K)$

$= f(a * H) \otimes f(b * H) \Rightarrow f$ is a homomorphism.

By the first theorem of isomorphism $\Rightarrow (\frac{\frac{G}{H}}{kerf}, \otimes) \cong \left(\frac{G}{K}, \otimes\right)$

$\ker f = \{a * H : f(a * H) = e' = \{a * H : a * K = K\}$

$= a * H \in \frac{G}{H} : a \in K\} = \frac{K}{H}$

Therefore, $(\frac{\frac{G}{H}}{\frac{K}{H}}, \otimes) \cong (\frac{G}{K}, \otimes)$.

10. The Jordan-Holder Theorem and Related Concepts.

Definition(10-1):

By a *chain* for a group $(G,*)$ is meant any finite sequence of subsets of

$G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ descending from G to $\{e\}$ with the property that all the pairs $(H_i,*)$ are subgroups of $(G,*)$.

Remark(10-2):

The integer n is called the length of the chain. When $n = 1$, then the chain in definition (1-1) will called the trivial.

Example(10-3):

Find all chains in a group $(Z_4, +_4)$.

Solution: The subgroups of a group $(Z_4, +_4)$ are :

- $H_1 = (Z_4, +_4)$
- $H_2 = (\{0\}, +_4)$
- $H_3 = (\langle 2 \rangle, +_4) = (\{0,2\}, +_4)$

The chains of a group $(Z_4, +_4)$ are

$Z_4 \supset \{0\}$ is a chain of length one

$Z_4 \supset \langle 2 \rangle \supset \{0\}$ is a chain of length two.

Example(10-4):

In the group $(Z_{12}, +_{12})$ of integers modulo 12, the following chains are normal chains:

$$Z_{12} \supset \langle 6 \rangle \supset \{0\},$$

$$Z_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\},$$

$$Z_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \{0\},$$

$$Z_{12} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \{0\}.$$

All subgroups are normal, since $(Z_{12}, +_{12})$ is a commutative group.

Definition(10-5): (***Normal Chain***)

If $(H_i,*)$ is a normal subgroup of a group $(G,*)$ for all $i = 1, \dots, n$, then the chain $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is called a *normal chain*.

Example(10-6):

Find all chains in the following groups and determine their length and type.

- $(Z_6, +_6)$;
- $(Z_8, +_8)$;
- $(Z_{18}, +_{18})$ (**Homework**);
- $(Z_{21}, +_{21})$ (**Homework).**

Solution: The subgroups of a group $(Z_6, +_6)$ are :

$H_1 = (Z_6, +_6)$

$H_2 = (\{0\}, +_6)$

$H_3 = (\langle 2 \rangle, +_6) = (\{0,2,4\}, +_6)$

$H_4 = (\langle 3 \rangle, +_6) = (\{0,3\}, +_6)$

Then the chains in $(Z_6, +_6)$ are:

$Z_6 \supset \{0\}$ is a trivial chain of length one

$Z_6 \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two

$Z_6 \supset \langle 3 \rangle \supset \{0\}$ is a normal chain of length two.

The subgroups of a group $(Z_8, +_8)$ are :

$H_1 = (Z_8, +_8)$

$H_2 = (\{0\}, +_8)$

$H_3 = (\langle 2 \rangle, +_8) = (\{0,2,4,6\}, +_8)$

$H_4 = (\langle 4 \rangle, +_6) = (\{0,4\}, +_8)$

Then the chains in $(Z_8, +_8)$ are:

$Z_8 \supset \{0\}$ is a trivial chain of length one

$Z_8 \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two

$Z_8 \supset \langle 4 \rangle \supset \{0\}$ is a normal chain of length two

$Z_8 \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$ is a normal chain of length three.

Definition(10-7): (***Composition Chain***)

In the group $(G,*)$, the descending sequence of sets

$$G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$$

forms a *composition chain* for $(G,*)$ provided

1. $(H_i,*)$ is a subgroup of $(G,*)$,
2. $(H_i,*)$ is a normal subgroup of $(H_{i-1},*)$,
3. The inclusion $H_{i-1} \supseteq K \supseteq H_i$, where $(K,*)$ is a normal subgroup of $(H_{i-1},*)$, implies either $K = H_{i-1}$ or $K = H_i$.

Remark(10-8):

Every composition chain is a normal, but the converse is not true in general, the following example shows that.

Example(10-9):

In the group $(Z_{24}, +_{24})$, the normal chain

$$Z_{24} \supset \langle 2 \rangle \supset \langle 12 \rangle \supset \{0\}$$

is not a composition chain, since it may be further refined by inserting of the set $\langle 4 \rangle$ or $\langle 6 \rangle$. On other hand,

$$Z_{24} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \langle 8 \rangle \supset \{0\}$$

and

$$Z_{24} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}$$

are both composition chains for $(Z_{24}, +_{24})$.

Example(10-10):

Find all chains in the following groups and determine their length and type.

- $(Z_8, +_8)$;
- $(Z_{12}, +_{12})$;
- $(Z_{18}, +_{18})$ (**Homework**).

Solution: The subgroups of a group $(Z_8, +_8)$ are :

$H_1 = (Z_8, +_8)$

$H_2 = (\{0\}, +_8)$

$H_3 = (\langle 2 \rangle, +_8) = (\{0,2,4,6\}, +_8)$

$H_4 = (\langle 4 \rangle, +_8) = (\{0,4\}, +_8)$

Then the chains in $(Z_8, +_8)$ are:

$Z_8 \supset \{0\}$ is a trivial chain of length one.

$Z_8 \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two, but it is not composition chain, since there is a normal subgroup $\langle 4 \rangle$ in Z_8, such that $\langle 2 \rangle \supset \langle 4 \rangle$.

$Z_8 \supset \langle 4 \rangle \supset \{0\}$ is a normal chain of length two, but it is not composition chain, since there is a normal subgroup $\langle 2 \rangle$ in Z_8, such that $\langle 2 \rangle \supset \langle 4 \rangle$.

$Z_8 \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$ is a composition chain of length three.

The subgroups of a group $(Z_{12}, +_{12})$ are :

$H_1 = (Z_{12}, +_{12})$

$H_2 = (\{0\}, +_{12})$

$H_3 = (\langle 2 \rangle, +_{12}) = (\{0,2,4,6,8,10\}, +_{12})$

$H_4 = (\langle 3 \rangle, +_{12}) = (\{0,3,6,9\}, +_{12})$

$H_5 = (\langle 4 \rangle, +_{12}) = (\{0,4,8\}, +_{12})$

$H_6 = (\langle 6 \rangle, +_{12}) = (\{0,6\}, +_{12})$

Then the chains in $(Z_{12}, +_{12})$ are:

$Z_{12} \supset \{0\}$ is a trivial chain of length one.

$Z_{12} \supset \langle 2 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 3 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 4 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 6 \rangle \supset \{0\}$ is a normal chain of length two.

$Z_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$ is a composition chain of length three.

$Z_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \{0\}$ is a composition chain of length three.

<u>**Example(10-11):**</u>

Let $(G,*)$ be the group of symmetries of the square.

A normal chain for $(G,*)$ which fails to be a composition chain is

$$G \supset \{R_{180}, R_{360}\} \supset \{R_{360}\}.$$

Example(10-12): (Homework)

Determine the following chain whether normal, composition:

$$G \supset \{R_{90}, R_{180}, R_{270}, R_{360}\} \supset \{R_{180}, R_{360}\} \supset \{R_{360}\}.$$

Example(10-13):

The group $(Z, +)$ has no a composition chain, since the normal subgroups of $(Z, +)$ are the cyclic subgroups $(\langle n \rangle), +)$, n a nonnegative integer, Since the inclusion $\langle kn \rangle \subseteq \langle n \rangle$ holds for all $k \in Z_+$, there always exists a proper subgroup of any given group.

Definition(10-14):

A normal subgroup $(H,*)$ is called a *maximal normal subgroup* of the group $(G,*)$ if $H \neq G$ and there exists no normal subgroup $(K,*)$ of $(G,*)$ such that $H \subset K \subset G$.

Example(10-15):

In the group $(Z_{24}, +_{24})$, the cyclic subgroups $(\langle 2 \rangle, +_{24})$ and $(\langle 3 \rangle, +_{24})$ are both maximal normal with orders 12 and 8, respectively.

Example(10-16):

Determine the maximal normal subgroups in the group $(Z_{12}, +_{12})$.

Solution: The normal subgroups of $(Z_{12}, +_{12})$ are:

$H_1 = (\langle 2 \rangle, +_{12}) = (\{0,2,4,6,8,10\}, +_{12})$

$H_2 = (\langle 3 \rangle, +_{12}) = (\{0,3,6,9\}, +_{12})$

$H_3 = (\langle 4 \rangle, +_{12}) = (\{0,4,8\}, +_{12})$

$H_4 = (\langle 6 \rangle, +_{12}) = (\{0,6\}, +_{12})$

The maximal normal subgroups of $(Z_{12}, +_{12})$ are H_1 and H_2, since there is no normal subgroup in Z_{12} containing H_1 and H_2.

Remark(10-17):

A chain $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is a composition of a group $(G,*)$, if each normal subgroup $(H_i,*)$ is a maximal normal subgroup of $(H_{i-1},*)$, for all $i = 1, \dots, n$.

Example(10-18):

In the group $(Z_{12}, +_{12})$ the chains $Z_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$ is a composition of Z_{12}, since

$\langle 2 \rangle$ is a maximal normal subgroup of Z_{12},

$\langle 4 \rangle$ is a maximal normal subgroup of $\langle 2 \rangle$,

$\{0\}$ is a maximal normal subgroup of $\langle 4 \rangle$, and

$Z_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \{0\}$ is a composition of Z_{12}, since

$\langle 3 \rangle$ is a maximal normal subgroup of Z_{12},

$\langle 6 \rangle$ is a maximal normal subgroup of $\langle 3 \rangle$,

$\{0\}$ is a maximal normal subgroup of $\langle 6 \rangle$.

Theorem(10-19):

A normal subgroup $(H,*)$ of the group $(G,*)$ is a maximal if and only if the quotient $({}^{G}/_{H}, \otimes)$ is a simple.

Proof:

$\Rightarrow$) Let $H \trianglerighteq K \Rightarrow \frac{K}{H} \trianglerighteq \frac{G}{H} \Rightarrow H = K$ or $K = G$

Since H is a maximal, $\Rightarrow \frac{K}{H} = H$ or $\frac{K}{H} = \frac{G}{H}$ $\Rightarrow \frac{G}{H}$ is a simple

$\Leftarrow$) let ${}^{G}/_{H}$ be a simple

$\Rightarrow {}^{G}/_{H}$ has two normal subgroups which are $e * H$ and ${}^{G}/_{H}$, but $e * H = H$

Therefore H is a maximal ■

Corollary(10-20):

The group $({}^{G}/_{H}, \otimes)$ is a simple, if $|{}^{G}/_{H}|$ is a prime number.

Examples(10-21):

1. Show that $(\langle 2 \rangle, +_{12})$ is a maximal normal subgroup of $(\mathrm{Z}_{12}, +_{12})$.
2. Show that $(\langle 3 \rangle, +_{15})$ is a maximal normal subgroup of $(\mathrm{Z}_{15}, +_{15})$. (**Homework**)

Solution(1): $(\langle 2 \rangle, +_{12}) = (\{0,2,4,6,8,10\}, +_{12})$

$|{}^{G}/_{H}| = \frac{|G|}{|H|} = \frac{|\mathrm{Z}_{12}|}{|\langle 2 \rangle|} = \frac{12}{6} = 2$ is a prime $\Rightarrow \frac{\mathrm{Z}_{12}}{\langle 2 \rangle}$ is a simple (by Corollary (10-20)).

From Theorem (10-19), we get that $\langle 2 \rangle$ is a maximal normal subgroup of Z_{12}.

Corollary(10-22):

A normal chain $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is a composition of a group $(G,*)$, if $({}^{H_i}/_{H_{i-1}}, \otimes)$ is a simple group for all $i = 1, \dots, n$.

Example(10-23):

Show that $\mathrm{Z}_{60} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\}$ is a composition chain of a group $(\mathrm{Z}_{60}, +_{60})$.

Solution: $\frac{|\mathrm{Z}_{60}|}{|\langle 3 \rangle|} = \frac{60}{20} = 3$ is a prime $\Rightarrow \frac{\mathrm{Z}_{60}}{\langle 3 \rangle}$ is a simple.

So, we get that $\langle 3 \rangle$ is a maximal normal subgroup of Z_{60}.

$\frac{|\langle 3\rangle|}{|\langle 6\rangle|} = \frac{20}{10} = 2$ is a prime $\Rightarrow \frac{\langle 3\rangle}{\langle 6\rangle}$ is a simple.

So, we get that $\langle 6\rangle$ is a maximal normal subgroup of $\langle 3\rangle$.

$\frac{|\langle 6\rangle|}{|\langle 12\rangle|} = \frac{10}{5} = 2$ is a prime $\Rightarrow \frac{\langle 6\rangle}{\langle 12\rangle}$ is a simple.

So, we get that $\langle 12\rangle$ is a maximal normal subgroup of $\langle 6\rangle$.

$\frac{|\langle 12\rangle|}{|\{0\}|} = \frac{5}{1} = 5$ is a prime $\Rightarrow \frac{\langle 12\rangle}{\{0\}}$ is a simple.

So, we get that $\{0\}$ is a maximal normal subgroup of $\langle 12\rangle$.

By corollaries (10-19) and (1-21), we have that $Z_{60} \supset \langle 3\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}$ is a composition chain of a group $(Z_{60}, +_{60})$.

Theorem(10-24):

Every finite group $(G,*)$ with more than one element has a composition chain.

Theorem(10-25): (Jordan-Holder)

In a finite group $(G,*)$ with more than one element, any two composition chains are equivalent.

Example(10-26):

In a group $(Z_{60}, +_{60})$, show that the two chains

$$Z_{60} \supset \langle 3\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}$$

$$Z_{60} \supset \langle 2\rangle \supset \langle 6\rangle \supset \langle 30\rangle \supset \{0\},$$

are compositions and equivalent.

Solution:

$({}^{Z_{60}}/_{\langle 3\rangle}, \otimes) \cong ({}^{\langle 2\rangle}/_{\langle 6\rangle}, \otimes)$, since $\left|{}^{Z_{60}}/_{\langle 3\rangle}\right| = \frac{60}{20} = 3 = \left|{}^{\langle 2\rangle}/_{\langle 6\rangle}\right| = \frac{30}{10}$,

$\left({}^{\langle 3\rangle}/_{\langle 6\rangle},\otimes\right) \cong \left({}^{Z_{60}}/_{\langle 2\rangle},\otimes\right)$, since $\left|{}^{\langle 3\rangle}/_{\langle 6\rangle}\right| = \frac{20}{10} = 2 = \left|{}^{Z_{60}}/_{\langle 2\rangle}\right| = \frac{60}{30}$,

$\left({}^{\langle 6\rangle}/_{\langle 12\rangle},\otimes\right) \cong \left({}^{\langle 30\rangle}/_{\{0\}},\otimes\right)$, since $\left|{}^{\langle 6\rangle}/_{\langle 12\rangle}\right| = \frac{10}{5} = 2 = \left|{}^{\langle 30\rangle}/_{\{0\}}\right| = \frac{2}{1}$,

$\left({}^{\langle 12\rangle}/_{\{0\}},\otimes\right) \cong \left({}^{\langle 6\rangle}/_{\langle 30\rangle},\otimes\right)$, since $\left|{}^{\langle 12\rangle}/_{\{0\}}\right| = \frac{5}{1} = 5 = \left|{}^{\langle 6\rangle}/_{\langle 30\rangle}\right| = \frac{10}{2}$.

Therefore, by Jordan-Holder theorem the two chains

$$Z_{60} \supset \langle 3\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}$$

$$Z_{60} \supset \langle 2\rangle \supset \langle 6\rangle \supset \langle 30\rangle \supset \{0\},$$

are compositions and equivalent.

Exercises(10-27):

- Check that the following chains represent composition chains for the indicated group.

a. For $(Z_{36}, +_{36})$, the group of integers modulo 36:

$$Z_{36} \supset \langle 3\rangle \supset \langle 9\rangle \supset \langle 18\rangle \supset \{0\}.$$

b. For $(G_s,*)$, the group of symmetries of the square:

$$G \supset \{R_{180}, R_{360}, D_1, D_2\} \supset \{R_{360}, D_1\} \supset \{R_{360}\}.$$

c. For $(\langle a\rangle,*)$, a cyclic group of order 30:

$$\langle a\rangle \supset \langle a^5\rangle \supset \langle a^{10}\rangle \supset \{e\}.$$

d. For $(S_3,\circ)$, the symmetric group on 3 symbols:

$$S_3 \supset \{i, (123), (132)\} \supset \{i\}.$$

- Find a composition chain for the symmetric group $(S_4,\circ)$.
- Prove that the cyclic subgroup $(\langle n\rangle, +)$ is a maximal normal subgroup of $(Z, +)$ if and only if n is a prime number.

- Establish that the following two composition chains for $(Z_{36}, +_{36})$ are equivalent:

$$Z_{24} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\},$$

$$Z_{24} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \langle 12 \rangle \supset \{0\}.$$

- Find all composition chains for $(Z_{36}, +_{36})$.
- Find all composition chains for $(G_5, *)$.

11. P- Groups and Related Concepts.

Definition(11-1): **(p- Group)**

A finite group $(G,*)$ is said to be p- *group* if and only if the order of each element of G is a power of fixed prime p.

Definition(11-2): **(p- Group)**

A finite group $(G,*)$ is said to be p- *group* if and only if $|G| = p^k, k \in Z$, where p is a prime number.

Example(11-3):

Show that $(Z_4, +_4)$ is a p- group.

Solution: $Z_4 = \{0,1,2,3\}$ and $|\ Z_4| = 4 = 2^2$

$\Rightarrow$ Z_4 is a 2- group, with

$o(0) = 1 = 2^0$,

$o(1) = 4 = 2^2$,

$o(2) = 2 = 2^1$,

$o(3) = 4 = 2^2$.

Example(11-4):

Determine whether $(Z_6, +_6)$ is a p- group.

Solution: $Z_6 = \{0,1,2,3,4,5\}$ and $|\ Z_6| = 6 \neq P^k$

$\Rightarrow$ Z_6 is not p- group.

Example(11-5): (Homework)

Determine whether $(G_s, \circ)$ is a p- group.

Examples(11-6):

- $(Z_8, +_8)$ is a 2- group, since $|Z_8| = 8 = 2^3$,
- $(Z_9, +_9)$ is a 3- group, since $|Z_9| = 9 = 3^2$,
- $(Z_{25}, +_{25})$ is a 5- group, since $|Z_{25}| = 25 = 5^2$.

Theorem(11-7):

Let $H \Delta G$, then G is a p- group if and only if H and $G/_H$ are p- groups.

Proof: $(\Longrightarrow)$ Assume that G is a p- group, to prove that H and $G/_H$ are p- groups.

Since G is a p- group $\Longrightarrow$ $o(a) = p^x$, for some $x \in Z^+, \forall a \in G$.

Since $H \subseteq G \Longrightarrow \forall a \in H$ group $\Longrightarrow o(a) = p^x$, for some $x \in Z^+$.

So, H is a p- group.

To prove $G/_H$ is a p- group.

Let $a * H \in G/_H$, to prove $o(a * H)$ is a power of p.

$(a * H)^{p^x} = a^{p^x} * H = e * H = H$, ($a^{p^x} = e$ since G is a p- group

$\Longrightarrow o(a * H) = p^x$

($\Longleftarrow$) Suppose that H and ${}^{G}/_{H}$ are p- groups, to prove G is a p- group.

Let $a \in G$, to prove $o(a)$ is a power of p.

$(a * H)^{p^x} = H \ldots (1)$ (${}^{G}/_{H}$ is a p- group)

$(a * H)^{p^x} = a^{p^x} * H \ldots (2)$

From (1) and (2), we have $a^{p^x} * H = H \Rightarrow a^{p^x} \in H$ and H is a p- group,

$\Rightarrow o(a^{p^x}) = p^r, r \in Z^+$

$\Rightarrow (a^{p^x})^{p^r} = e \Rightarrow a^{p^{x+r}} = e,\ x + r \in Z^+,$

$\Rightarrow o(a) = p^{x+r}$

Therefore, G is a p- group ■

Examples(11-8):

Apply theorem(2-7) on $(Z_{32}, +_{32})$.

Solution:

$|Z_{32}| = 32 = 2^5$ is a 2- group.

By theorem (2-7), H and ${}^{G}/_{H}$ are 2- groups.

${}^{o(G)}/_{o(H)} \Rightarrow o(H) = 2^x, 0 \leq x \leq 5.$

$o(H) = 2^0$ or 2^1 or 2^2 or 2^3 or 2^4 or 2^5,

$o(H) = 2^0$ is a 2- group $\Rightarrow o({}^{G}/_{H}) = {}^{o(G)}/_{o(H)} = \frac{2^5}{2^0} = 2^5$ is a 2- group.

$o(H) = 2^1$ is a 2- group $\Rightarrow {}^{o(G)}/_{o(H)} = 2^4$

$o(H) = 2^2$ is a 2- group $\Rightarrow {}^{o(G)}/_{o(H)} = 2^3$

$o(H) = 2^3$ is a 2- group $\Rightarrow {}^{o(G)}/_{o(H)} = 2^2$

$o(H) = 2^4$ is a 2- group $\Rightarrow {}^{o(G)}/_{o(H)} = 2$

$o(H) = 2^5$ is a 2- group $\Rightarrow {}^{o(G)}/_{o(H)} = 1.$

Remark(11-9):

If G is a non-trivial p- group, then $\text{Cent}(G) \neq e$.

Theorem(11-10):

Every group of order p^2 is an abelian.

Proof: Let G be a group of order p^2, to prove G is an abelian.

Let Cent(G) is a subgroup of G.

By Lagrange Theorem ${}^{o(G)}/_{o(\text{Cent}(G))}$,

$\Rightarrow {}^{p^2}/_{o(\text{Cent}(G))}$

$\Rightarrow o(\text{Cent}(G)) = p^0$ or p^1 or p^2

If $o(\text{Cent}(G)) = p^0 \Rightarrow \text{Cent}(G) = \{e\}$, but this is contradiction with remark(2-9), so $o(\text{Cent}(G)) \neq p^0$.

If $o(\text{Cent}(G)) = p^2 = o(G) \Rightarrow \text{Cent}(G) = G$

$\Rightarrow G$ is an abelian.

If $o(\text{Cent}(G)) = p^1 \Rightarrow o\left({}^{G}/_{\text{Cent}(G)}\right) = \frac{p^2}{p^1} = p$

$G/_{\text{Cent(G)}}$ is a cyclic.

Therefore, G is an abelian ■

Remark(11-11):

The converse of theorem(2-10) is not true in general, for example $(Z_8, +_8)$ is an abelian, but $o((Z_8) = 2^3 \neq p^2$.

Exercises(11-12):

- Let P and Q be two normal p-subgroups of a finite group G. Show that PQ is a normal p-subgroup of G.
- Determine whether $(Z_{125}, +_{125})$ is a p-group.
- Determine whether $(Z_{121}, +_{121})$ is a p-group.
- Determine whether $(Z_{41}, +_{41})$ is a p-group.
- Determine whether $(Z_{16}, +_{16})$ is a p-group.
- Determine whether $(Z_{625}, +_{625})$ is a p-group.
- Determine whether $(Z_{185}, +_{185})$ is a p-group.
- Determine whether $(Z_{128}, +_{128})$ is a p-group.
- Determine whether $(Z_{256}, +_{256})$ is a p-group.
- Determine whether $(Z_{100}, +_{100})$ is a p-group.
- Show that $G_\ell = \{\pm 1, \pm i, \pm j, \pm k\}, \cdot)$ is a p-group.

12. Sylow Theorems

Definition(12-1): (***Sylow p- Subgroup***)

Let $(G,*)$ be a finite group and p is a prime number, a subgroup $(H,*)$ of a group G is called *sylow p- subgroup* if

1. $(H,*)$ is a p- group,
2. $(H,*)$ is not contained in any other p- subgroup of G for the same prime number p.

Example(12-2):

Find sylow 2- subgroups and sylow 3- subgroup of the group $(Z_{24}, +_{24})$.

Solution: The proper subgroups of the group $(Z_{24}, +_{24})$ are

1. $(\langle 2\rangle, +_{24}) \Rightarrow o(\langle 2\rangle) = 12 \neq P^k \Rightarrow \langle 2\rangle$ is not p- subgroup.
2. $(\langle 3\rangle, +_{24}) \Rightarrow o(\langle 3\rangle) = 8 = 2^3 \Rightarrow \langle 3\rangle$ is a 2- subgroup.
3. $(\langle 4\rangle, +_{24}) \Rightarrow o(\langle 4\rangle) = 6 \neq P^k \Rightarrow \langle 4\rangle$ is not p- subgroup.
4. $(\langle 6\rangle, +_{24}) \Rightarrow o(\langle 6\rangle) = 4 = 2^2 \Rightarrow \langle 6\rangle$ is a 2- subgroup.
5. $(\langle 8\rangle, +_{24}) \Rightarrow o(\langle 8\rangle) = 3 = 3^1 \Rightarrow \langle 8\rangle$ is a 3- subgroup.
6. $(\langle 12\rangle, +_{24}) \Rightarrow o(\langle 12\rangle) = 2 = 2^1 \Rightarrow \langle 12\rangle$ is a 2- subgroup.

Theorem(12-3): (First Sylow Theorem)

Let $(G,*)$ be a finite group of order $\mathrm{p}^k q$, where p is a prime number is not dividing q, then G has sylow p- subgroup of order p^k.

Example(12-4):

Find sylow 2- subgroup of the group $(Z_{12}, +_{12})$.

Solution: $o(Z_{12}) = 12 = (4)(3) = (2^2)(3)$, and $2 \nmid 3$

$\Rightarrow$ by first sylow theorem, the group $(Z_{12}, +_{12})$ has sylow 2- subgroup of order 2^2.

$\Rightarrow (\langle 3\rangle, +_{12})$ is a sylow 2- subgroup.

Example(12-5):

Find sylow 7- subgroup of the group $(Z_{42}, +_{42})$.

Solution: $o(Z_{42}) = 42 = (7)(6)$, and $7 \nmid 6$

$\Rightarrow$ by first sylow theorem, the group $(Z_{42}, +_{42})$ has sylow 7- subgroup of order 7^1.

$\Rightarrow (\langle 6\rangle, +_{42})$ is a sylow 7- subgroup.

Example(12-6):

Find sylow 3- subgroup of the group $(Z_{24}, +_{24})$.

Solution: $o(Z_{24}) = 24 = (3)(8) = (3^1)(8)$, and $3 \nmid 8$

$\Rightarrow$ by first sylow theorem, the group $(Z_{24}, +_{24})$ has sylow 3- subgroup of order 3^1.

$\Rightarrow (\langle 8 \rangle, +_{24})$ is a sylow 3- Subgroup.

Theorem(12-7):

Let p a prime number and G be a finite group such that $p^x \backslash o(G), x \geq 1$, then G has a subgroup of order p^x which is called sylow p- subgroup of G.

Example(12-8):

Are the following groups $(S_3,\circ)$ and $(G_s,\circ)$ have sylow p- subgroups.

Solution:

$(S_3,\circ)$, $O(S_3) = 6 = (2)(3)$,

$2 \backslash 6 \Rightarrow \exists$ a subgroup H such that $o(H) = 2$ which is called sylow 2- subgroup.

Also, $3 \backslash 6 \Rightarrow \exists$ a subgroup K such that $o(K) = 3$ which is called sylow 3- subgroup.

$(G_s,\circ)$, $o(G_s) = 2^3$ is 2- subgroup.

Every subgroup of G_s is 2- subgroup, $o(H) = 2^0$ or 2^1 or 2^2 or 2^3 .

Theorem(12-9): (Second Sylow Theorem)

The number of distinct sylow p-subgroups is $k = 1 + tp, t = 0,1, \ldots$ which is divide the order of G.

Example(12-10):

Find the distinct sylow p-subgroups of $(S_3,\circ)$.

Solution:

$o(S_3) = 6 = (2)(3)$,

$2 \setminus 6 \Longrightarrow \exists$ a subgroup H such that $o(H) = 2$.

The number of sylow 2-subgroups is $k_1 = 1 + 2t, t = 0,1, \dots$ and $k_1 \setminus 6$

if $t = 0 \Rightarrow k_1 = 1$ and $1 \setminus 6$

if $t = 1 \Rightarrow k_1 = 3$ and $3 \setminus 6$

if $t = 2 \Rightarrow k_1 = 5$ and $5 \nmid 6$

if $t = 3 \Rightarrow k_1 = 7$ and $7 \nmid 6$

so, there are two sylow 2-subgroups.

$3 \setminus 6 \Longrightarrow \exists$ a subgroup K such that $o(K) = 3$.

The number of sylow 3-subgroups is $k_2 = 1 + 3t, t = 0,1, \dots$ and $k_2 \setminus 6$

if $t = 0 \Rightarrow k_2 = 1$ and $1 \setminus 6$

if $t = 1 \Rightarrow k_2 = 4$ and $4 \nmid 6$

if $t = 2 \Rightarrow k_2 = 7$ and $7 \nmid 6$

So, there is one sylow 3-subgroup.

Example(12-11):

Find the number of sylow p-subgroups of G such that $o(G) = 12$.

Solution: $o(G) = 12 = (3)(2^2)$

$3 \setminus 12 \Longrightarrow \exists$ a subgroup H such that $o(H) = 3$.

The number of sylow 3-subgroups is $k_1 = 1 + 3t, t = 0,1, \dots$ and $k_1 \setminus 12$

if $t = 0 \Rightarrow k_1 = 1$ and $1 \setminus 12$

if $t = 1 \Rightarrow k_1 = 4$ and $4 \setminus 12$

if $t = 2 \Rightarrow k_1 = 7$ and $7 \nmid 12$

if $t = 3 \Rightarrow k_1 = 10$ and $10 \nmid 12$

So, there are two sylow 3-subgroups of G.

The number of sylow 2-subgroups is $k_2 = 1 + 2t, t = 0,1, \dots$ and $k_2 \setminus 12$

if $t = 0 \Rightarrow k_2 = 1$ and $1 \setminus 12$

if $t = 1 \Rightarrow k_2 = 3$ and $3 \setminus 12$

if $t = 2 \Rightarrow k_2 = 5$ and $5 \nmid 12$

if $t = 3 \Rightarrow k_2 = 7$ and $7 \nmid 12$

So, there are two sylow 2-subgroups of G.

Remark(12-12):

The group G has exactly one sylow p-subgroup H if and only if $H\Delta G$.

Example(12-13):

$(S_3,\circ), H = \{f_1 = i, f_2 = (123), f_3 = (132)\}$

$H\Delta G \Rightarrow$ H is a sylow 3-subgroup of S_3,

So, there is one sylow 3-subgroup of S_3.

Exercises(12-14);

- Show that there is no simple group of order 200.
- Show that there is no simple group of order 56.
- Show that there is no simple group of order 20.
- Show that whether $(G_\ell,\cdot)$ is a sylow.

13. Solvable Groups and Their Applications

Definition(13-1):

A group $(G,*)$ is called a solvable group if and only if, there is a finite collection of subgroups of $(G,*)$, $H_0, H_1, \ldots, H_n$ such that

1. $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$,
2. $H_{i+1} \Delta H_i \quad \forall i = 0, \ldots, n-1$,
3. $H_i/_{H_{i+1}}$ is a commutative group $\forall i = 0, \ldots, n-1$.

Theorem(13-2):

Every commutative group is a solvable group.

Proof:

Suppose that $(G,*)$ is a commutative, to show that $(G,*)$ is a solvable.

Let $G = H_0$ and $H_1 = \{e\}$

1. $G = H_0 \supset H_1 = \{e\}$
2. $H_1 \Delta H_0$ satisfies, since $\{e\}\Delta G$, or (every subgroup of commutative group is a normal)
3. $G/_{\{e\}} \cong G$ is a commutative group, or (the quotient of commutative group is a commutative)

So, $(G,*)$ is a solvable group,

Example(13-3):

Show that $(S_3, \circ)$ is a solvable group.

Solution: let $H_0 = S_3, H_1 = \{f_1 = i, f_2 = (123), f_3 = (132)\}, H_2 = \{f_1\}$

1. $S_3 = H_0 \supset H_1 \supset H_2 = \{e\}$
2. $H_2 \Delta H_1$ satisfies, since $\{ f_1\}\Delta\{f_1, f_2, f_3\}$, $H_1 \Delta H_0$ is true,

3. To prove H_i/H_{i+1} is a commutative group $\forall i = 0,1$

$o\left(H_1/H_2\right) = \frac{o(H_1)}{o(H_2)} = \frac{3}{1} = 3 < 6 \Rightarrow H_1/H_2$ is a commutative group

$o\left(H_0/H_1\right) = \frac{o(H_0)}{o(H_1)} = \frac{6}{3} = 2 < 6 \Rightarrow H_0/H_1$ is a commutative group

Therefore, $(S_3,\circ)$ is a solvable group.

Example(13-4): **(Homework)**

Show that $(G_s,\circ)$ is a solvable group.

Theorem(13-5):

Every subgroup of a solvable group is a solvable.

Proof: let $(H,*)$ be a subgroup of $(G,*)$ and $(G,*)$ is a solvable group.

To prove $(H,*)$ is a solvable.

Since G is a solvable $\Longrightarrow$

there is a finite collection of subgroups of $(G,*)$, $G_0, G_1, \dots, G_n$ such that

1. $G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{e\}$,
2. $G_{i+1} \Delta G_i \quad \forall i = 0, \dots, n-1$,
3. G_i/G_{i+1} is a commutative group $\forall i = 0, \dots, n-1$.

Let $H_i = H \cap G_i, \ \ i = 0, \dots, n$

$H_0 = H \cap G_0, H_1 = H \cap G_1, \dots, H_n = H \cap G_n = \{e\}$

Each H_i is a subgroup of $(G,*)$.

1. $H = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$ is hold

2. $H_{i+1} \Delta H_i \quad \forall i = 0, \dots, n-1, \qquad H_i = H \cap G_i,\ H_{i+1} = H \cap G_{i+1},$ since $G_{i+1} \Delta G_i \Rightarrow H_{i+1} \Delta H_i$

3. To prove $H_i/_{H_{i+1}}$ is a commutative group $\forall i = 0, \dots, n-1$.

Let $f_i: H_i \longrightarrow G_i/_{G_{i+1}}, i = 0, \dots, n-1$ such that $f_i(x) = x * G_{i+1} \forall x \in H_i \subseteq G_i$.

To prove f_i is a homomorphism,

$f_i(x * y) = f_i(x) \otimes f_i(y)$?

$f_i(x * y) = x * y * G_{i+1} = (x * G_{i+1}) \otimes (y * G_{i+1}) = f_i(x) \otimes f_i(y)$

So, f_i is a homomorphism

f_i is onto ?

$R_{f_i} = \{f_i(x): x \in H_i\} = \{x * G_{i+1}: x \in H_i\} = f_i(H_i) \neq G_i/_{G_{i+1}}$

$f_i(H_i) \subseteq G_i/_{G_{i+1}} \Rightarrow f_i$ is not onto

$H_i/_{\ker f_i} \cong f_i(H_i)$ (by theorem of homomorphism)

$\ker f_i = \{x \in H_i: f_i(x) = e'\} = \{x \in H_i: x * G_{i+1} = G_{i+1}\} = \{x \in H_i: x \in G_{i+1}\}$
$= \{x \in H_i: x \in H \cap G_{i+1}\} = H_{i+1}$

so, $\left(H_i/_{H_{i+1}}, \otimes\right) \cong (f_i(H_i), \otimes)$

$f_i(H_i) \subseteq G_i/_{G_{i+1}}$ and $G_i/_{G_{i+1}}$ is a commutative

Hence, $f_i(H_i)$ is a commutative

Therefore, $H_i/_{H_{i+1}}$ is a commutative

So, $(H, *)$ is a solvable ■

Theorem(13-6):

Let $H\Delta G$ and G is a solvable, then $G/_H$ is a solvable.

Theorem(13-7):

Let $H\Delta G$ and both H, $G/_H$ are solvable, then $(G,*)$ is a solvable.

Proof: since $(H,*)$ is a solvable $\Rightarrow$

there is a finite collection of subgroups of $(G,*)$, $H_0, H_1, \dots, H_n$ such that

1. $G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$,
2. $H_{i+1}\Delta H_i \quad \forall i = 0, \dots, n-1$,
3. $H_i/_{H_{i+1}}$ is a commutative group $\forall i = 0, \dots, n-1$.

Since $(G/_H, \otimes)$ is a solvable $\Rightarrow$

there is a finite collection of subgroups of $(G,*)$, $\frac{G_0}{H}, \frac{G_1}{H}, \dots, \frac{G_r}{H}$ such that

1. $\frac{G}{H} = \frac{G_0}{H} \supset \frac{G_1}{H} \supset \cdots \supset \frac{G_r}{H} = \{e\} = H$,
2. $\frac{G_{i+1}}{H}\Delta\frac{G_i}{H} \quad \forall i = 0, \dots, r-1$,
3. $\frac{G_i}{H}\Big/\frac{G_{i+1}}{H}$ is a commutative group $\forall i = 0, \dots, r-1$.

To prove $(G,*)$ is a solvable group.

$$\frac{G}{H} = \frac{G_0}{H} \Rightarrow G = G_0$$

$\frac{G_r}{H} = H \Rightarrow G_r = \{e\}$ or $G_r = H$

$H\Delta G_r \Rightarrow H \subseteq G_r \Rightarrow G_r = H$

So, there is a finite collection $G_0, G_1, \dots, G_r = H_0, H_1, \dots, H_n$ such that

1. $G = G_0 \supset G_1 \supset \cdots \supset G_r = H = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\}$.
2. To prove $G_{i+1} \Delta G_i \quad \forall i = 0, \dots, r-1$

Let $x \in G_i$ and $a \in G_{i+1}$ to prove $x * a * x^{-1} \in G_{i+1}$

$$x \in G_i \Rightarrow x * H \in \frac{G_i}{H}$$

$$a \in G_{i+1} \Rightarrow a * H \in \frac{G_{i+1}}{H}$$

$$\frac{G_{i+1}}{H} \Delta \frac{G_i}{H} \Rightarrow (x * H) \otimes (a * H) \otimes (x * H)^{-1} \in \frac{G_{i+1}}{H}$$

$$\Rightarrow (x * a * x^{-1}) * H \in \frac{G_{i+1}}{H} \Rightarrow x * a * x^{-1} \in G_{i+1} \Rightarrow G_{i+1} \Delta G_i$$

3. To prove $\frac{G_i}{G_{i+1}}$ is a commutative group $\forall i = 0, \dots, r-1$

$\frac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}}$ is a commutative group and $\frac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}} \cong \frac{G_i}{G_{i+1}}$ $\left(\frac{\frac{G}{H}}{\frac{K}{H}} \cong \frac{G}{K}\right)$

$\Rightarrow \frac{G_i}{G_{i+1}}$ is a commutative group

Therefore, $(G,*)$ is a solvable group ■

Exercises(13-8):

- Show that every p-group is a solvable group.
- Show that $(S_4, \circ)$ is a solvable group.
- Show that $(Z_4, +_4)$ is a solvable group.
- Show that $(Z_8, +_8)$ is a solvable group.
- Show that $(Z_5, +_5)$ is a solvable group.
- Show that $(Z_6, +_6)$ is a solvable group.
- Show that $(Z_{12}, +_{12})$ is a solvable group.

- Show that $(Z_{24}, +_{24})$ is a solvable group.

14. Applications of Group Theory

14-1 Cayley Theorem

Theorem(14-1-1): (Cayley Theorem)

Every group is an isomorphic to a group of permutations.

This means if $(G,*)$ is any group, then $(G,*) \cong (F_G,\circ)$, where $F_G = \{f_a : a \in G\}, f_a: G \longrightarrow G \ni f_a(x) = a * x, \forall x \in G$.

Proof: define $g: G \longrightarrow F_G$ by $g(a) = f_a, \forall a \in G$

To prove g is a homomorphism, one to one and onto.

1. g is a homomorphism, let $a, b \in G$

$g(a * b) = f_{a*b} = f_a \circ f_b = g(a) \circ g(b) \Longrightarrow g$ is a homomorphism.

2. g is a one to one, let $g(a) = g(b), \ \forall a, b \in G$

$\Longrightarrow f_a = f_b \Longrightarrow f_a(x) = f_b(x) \Longrightarrow a * x = b * x \Longrightarrow a = b$

$\Longrightarrow g$ is a one to one.

3. g is a onto, $g(G) = \{g(a): a \in G\} = \{f_a: a \in G\} = F_G$

Therefore, $G \cong F_G$ ■

Corollary(14-1-2):

Every finite group $(G,*)$ of order n is an isomorphic to $(S_n,\circ)$.

Example(14-1-3):

Consider the following Cayley table of a group $(G = \{e, a, b, c\},*)$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Show that $(G,*)$ is an isomorphic to a subgroup of $(S_4,\circ)$.

Solution:

$f_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}$, $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4) = (1)$

$f_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$

$f_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$

$f_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$

Hence, $(G,*)$ is an isomorphic to the subgroup of $(S_4,\circ)$:

$\{(1),(12)(34),(13)(24),(14)(23)\}$.

Example(14-1-4): (Homework)

Let $(G = \{1,-1,i,-i\},\cdot)$ be a group, apply Cayley Theorem on G.

Example(14-1-5): (Homework)

Show that $(Z_3,+_3)$ is an isomorphic to a subgroup of $(S_3,\circ)$.

Exercises(14-1-6):

- Apply Cayley Theorem on $(Z_4,+_4)$.
- Apply Cayley Theorem on $(G = \{\pm 1, \pm i, \pm j, \pm k\},\cdot)$.

- Apply Cayley Theorem on $(G=\{1,-1\},\cdot)$.
- Apply Cayley Theorem on $(G=\{A=\begin{pmatrix}1&0\\0&1\end{pmatrix}, B=\begin{pmatrix}1&0\\0&-1\end{pmatrix}, C=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}, D=,\begin{pmatrix}-1&0\\0&1\end{pmatrix},\cdot)$.

14-2 Direct Product

Definition(14-2-1):

Let $(H,*)$ and $(K,*)$ be two normal subgroups of $(G,*)$, then $(G,*)$ is called an internal direct product of H and K (G is a decomposition by H and K) if and only if $G=H*K$ and $H\cap K=\{e\}$.

Example(14-2-2):

Consider the following Cayley table of a group $(G=\{e,a,b,c\},*)$, $a^2=b^2=c^2=e$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Let $H=\{e,a\}$ and $K=\{e,b\}$, show that $G=H\otimes K$ is a decomposition by H and K.

Solution: $H,K\Delta G$ since G is a commutative group

$H * K = \{e, a, b, c\}$ and $H \cap K = \{e\}$

Hence, $G = H \otimes K$ is decomposition by H and K.

Example(14-2-3):

Let $(G,*)$ be any group with $H = G$ and $K = \{e\}$, show that

$G = H \otimes K$ is a decomposition by H and K.

Solution: $H, K \Delta G$

$H * K = G * \{e\} = G$

$H \cap K = G \cap \{e\} = \{e\}$

Therefore, $G = H \otimes K$ is a decomposition by H and K.

Example(14-2-4):

Let $(Z_4, +_4)$ be a group. Is Z_4 has a proper decomposition.

Solution: the subgroups of Z_4 are $Z_4, \{0,2\}, \{0\}$

Let $H = Z_4$ and $K = \{0,2\}$

$H \otimes_4 K = Z_4 \otimes_4 \{0,2\} = Z_4$

$H \cap K = Z_4 \cap \{0,2\} = \{0,2\}$

So, $Z_4 \neq Z_4 \otimes \{0,2\}$

Let $H = \{0\}$ and $K = \{0,2\}$

$H \otimes_4 K = K \neq Z_4$

Therefore, Z_4 has no proper decomposition.

Theorem(14-2-5):

Let H and K be two subgroups of G and $G = H \otimes K$, then ${}^{G}/_{H} \cong K$ and ${}^{G}/_{K} \cong H$.

Proof:

Since $G = H \otimes K \Longrightarrow H * K = G$ and $H \cap K = \{e\}$

${}^{G}/_{H} = {}^{H * K}/_{H}$ and ${}^{H * K}/_{H} \cong {}^{K}/_{H \cap K}$ (by second theorem of isomorphic)

${}^{G}/_{H} \cong {}^{K}/_{\{e\}} \Longrightarrow {}^{G}/_{H} \cong K$ and

${}^{G}/_{K} = {}^{H * K}/_{K}$ and ${}^{H * K}/_{K} \cong {}^{H}/_{H \cap K}$

${}^{G}/_{K} \cong {}^{H}/_{\{e\}} \Longrightarrow {}^{G}/_{K} \cong H$ ■

Definition(14-2-6):

Let $(G_1,*)$ and $(G_2,\circ)$ be two groups, define $G_1 \times G_2 = \{(a,b): a \in G_1, b \in G_2\}$ such that $(a,b)\odot(c,d) = (a * c, b \circ d) \ni a,c \in G_1, b,d \in G_2$. Then $(G_1 \times G_2, \odot)$ is a group which is called an external direct product of G_1 and G_2.

Example(14-2-7): (Homework)

Show that $(G_1 \times G_2, \odot)$ is a group.

Example(14-2-8):

Let $G_1 = (Z_3, +_3)$ and $G_2 = (Z_2, +_2)$. Find $G_1 \times G_2$.

Solution:

$G_1 \times G_2 = Z_3 \times Z_2 = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$

$(1,1)\odot(2,1) = (0,0)$

$o(Z_3 \times Z_2) = o(Z_3).o(Z_2) = 6.$

Theorem(14-2-9):

Let $(G_1,*)$ and $(G_2,\circ)$ be two groups, then

1. $(G_1 \times G_2, \odot)$ is an abelian if and only if both G_1 and G_2 are abelian.
2. $G_1 \times \{e_2\} \triangle G_1 \times G_2$.
3. $\{e_1\} \times G_2 \triangle G_1 \times G_2$.
4. $G_1 \cong G_1 \times \{e_1\}$.
5. $G_2 \cong \{e_2\} \times G_2$.

Proof:

1. $(\Longrightarrow)$ suppose that $G_1 \times G_2$ is an abelian, to prove $G_1$and G_2 are abelian.

Let $(a, e_2), (b, e_2) \in G_1 \times G_2 \ni a, b \in G_1, e_2 \in G_2$

Since $G_1 \times G_2$ is an abelian, then

$(a, e_2)\odot(b, e_2) = (b, e_2)\odot(a, e_2)$

$(a * b, e_2) = (b * a, e_2) \Longrightarrow a * b = b * a$

Hence, $(G_1,*)$ is an abelian.

Similarly that $(G_2,*)$ is an abelian.

$(\Longleftarrow)$ suppose that $(G_1,*)$ and $(G_2,\circ)$ are abelian, to prove $G_1 \times G_2$ is an abelian.

Let $(a, b), (c, d) \in G_1 \times G_2$, to prove $(a, b)\odot(c, d) = (c, d)\odot(a, b)$

$(a, b)\odot(c, d) = (a * c, b \circ d)$

$(c, d)\odot(a, b) = (c * a, d \circ b)$

$a * c = c * a$ ($G_1$is an abelian)

$b \circ d = d \circ b$ ($G_2$is an abelian)

$\Longrightarrow (a, b)\odot(c, d) = (c, d)\odot(a, b)$

Therefore, $G_1 \times G_2$ is an abelian.

2. To prove $G_1 \times \{e_2\} \triangle G_1 \times G_2$

$G_1 \times \{e_2\} = \{(a, e_2): a \in G_1\} \neq \emptyset$

To prove $(G_1 \times \{e_2\}, \odot)$ is a subgroup of $G_1 \times G_2$

Let $(a, e_2), (b, e_2) \in G_1 \times \{e_2\}$

$(a, e_2)\odot(b, e_2)^{-1} = (a, e_2)\odot(b^{-1}, e_2{}^{-1}) = (a * b^{-1}, e_2)$

So, $(G_1 \times \{e_2\}, \odot)$ is a subgroup of $G_1 \times G_2$.

To prove $G_1 \times \{e_2\} \triangle G_1 \times G_2$

Let $(x, y) \in G_1 \times G_2$ and $(a, e_2) \in G_1 \times \{e_2\}$

To prove $(x, y)\odot(a, e_2)\odot(x, y)^{-1} \in G_1 \times \{e_2\}$

$(x * a * x^{-1}, y * e_2 * y^{-1}) = (x * a * x^{-1}, e_2) \in G_1 \times \{e_2\}$

Hence, $G_1 \times \{e_2\} \triangle G_1 \times G_2$.

3. **(Homework).**
4. To prove $G_1 \cong G_1 \times \{e_2\}$.

Proof:

Define $f: (G_1,*) \longrightarrow (G_1 \times \{e_2\}, \odot) \ni f(a) = (a, e_2)$

f is a map ? let $a_1, a_2 \in G_1$ and $a_1 = a_2 \Longrightarrow (a_1, e_2) = (a_2, e_2) \Longrightarrow f(a_1) = f(a_2)$, so f is a map

f is an one to one ? let $f(a_1) = f(a_2) \Longrightarrow (a_1, e_2) = (a_2, e_2) \Longrightarrow a_1 = a_2$, so f is a one to one.

f is a homomorphism ? $f(a * b) = (a * b, e_2) = (a, e_2)\odot(b, e_2) = f(a)\odot f(b)$, so f is a homomorphism

f is an onto ? $R_f = \{f(a): a \in G_1\} = \{(a, e_2): a \in G_1\} = G_1 \times \{e_2\}$ so f is an onto.

Therefore, $(G_1,*) \cong (G_1 \times \{e_2\}, \odot)$ ■

5. (**Homework**)

Theorem(14-2-10):

Let $(G_1,*)$ and $(G_2,\circ)$ be two p-groups, then $(G_1 \times G_2, \odot)$ is a p-group.

Proof:

Since G_1 is p-group $\Rightarrow o(G_1) = p^{k_1}, k_1 \in Z^+$

Since G_2 is p-group $\Rightarrow o(G_2) = p^{k_2}, k_2 \in Z^+$

$o(G_1 \times G_2) = o(G_2) \times o(G_1) = p^{k_1} \times p^{k_2} = p^{k_1+k_2}, k_1 + k_2 \in Z^+$

Therefore, $G_1 \times G_2$ is a p-group ■

Exercises(14-2-11):

- Let $H = \{0,2,4\}$ and $K = \{0,3\}$ are subgroups of $(Z_6, +_6)$, show that $Z_6 = H \otimes K$ is a decomposition.
- Let $H = \{0\}$, show that $Z_7 = H \otimes Z_7$ is a decomposition.
- Find $Z_3 \times Z_7$.
- Is $S_3 \times Z_2$ an abelian?
- Is $G_s \times Z_2$ an abelian?
- Is $S_3 \times G_S$ an abelian?
- Is $\{\pm 1, \pm i\} \times Z_2$ an abelian?
- Is $Z_4 \times Z_8$ a p-group?
- Is $Z_5 \times Z_{25}$ a p-group?
- Is $Z_{11} \times Z_{121}$ a p-group?
- Is $Z_7 \times Z_{49}$ a p-group?
- Is $Z_{27} \times Z_3$ a p-group?
- Is $Z_5 \times Z_{125}$ a p-group?

- Is $Z_2 \times Z_{64}$ a p-group?
- Is $Z_4 \times Z_{128}$ a p-group?
- Is $Z_9 \times Z_{81}$ a p-group?
- Is $Z_{27} \times Z_{81}$ a p-group?
- Is $Z_{128} \times Z_8$ a p-group?
- Is $Z_2 \times Z_{256}$ a p-group?