Chapter one

Group theory

1. Basics

$\mathbb{N} = \{0,1,2, 3,4. . . \}$. The set of natural numbers.

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ The set of all integers.

$\mathbb{Z}^{\#}$ $-$ The set of nonnegative integers

$\mathbb{Q} = \{\frac{x}{y},\ y \neq 0:\ x,\ y \in \mathbb{Z}\}$. The set of rational numbers

$\mathbb{Q}^{+}$ $-$ The set of positive rational numbers

$\mathbb{Q}^{*}$ $-$ The set of nonzero rational numbers.

$Irr = \{\exists\, x, s.t. x > 0\ and\ x \notin\ \mathbb{Q}\}$. Some positive real numbers are irrational.

$\mathbb{R}$ $-$ The set of real numbers

$\mathbb{R}^{+}$ $-$ The set of positive real numbers

$\mathbb{R}^{*} = \{\, x \in \mathbb{R}, x \neq 0\}$. The set of nonzero real numbers

$\mathbb{C} = \{\, x + yi : x, y\ \in \mathbb{R}\}$. The set of complex numbers

$\mathbb{C}^{*}$ $-$ The set of nonzero complex numbers

The order or cardinality of a set A will be denoted by $|A|$. If A is a finite set the order of A is simply the number of elements of A.

Definition 1.1. The Cartesian product of two sets A and B is collection

$$A \times B = \{(a, b) \mid a \in A, b \in B\},$$

Definition 1.2. For any set X, the power set of X, written $P(X)$, is defined to be the set

$$P(X) = \{A \mid A\ is\ a\ subset\ of\ X\}.$$

Example. Let $X = \{1,2,3\}$. Then

$$P(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

Here $P(X)$ has 2^3 elements.

Definition 1.3. Principle of Well-Ordering: Every nonempty subset of $\mathbb{Z}^\#$ has a smallest (least) element, i.e., if $\emptyset \neq S \subseteq \mathbb{Z}^\#$, then there exists $x \in S$ such that $x \leq y$ for all $y \in S$.

Theorem 1.4. (Division Algorithm) Let $x, y \in Z$ with $y \neq 0$. Then there exist unique integers q and r such that $= qy + r,\ 0 \leq r < |y|$.

Definition 1.5

(i) An integer $p > 1$ is called prime if the only divisors of p are ± 1 and $\pm p$.

(ii) Two integers x and y are called relatively prime if $gcd(x,y) = 1$.

We shall use the following notation for some common sets of numbers.

2. Groups

Definition 2.1. Let S be a nonempty set. Any function $*$ from Cartesian product $S \times S$ to S called ***binary operation*** on S. Then for all $x,\ y \in S$ we shall write $*(x,y) as\ x * y$.

Examples.

1- Ordinary addition and multiplication is a binary operation.

2- Ordinary subtraction is a binary operation on the set of integers but not binary operation on the set of $\mathbb{Z}^+$.

3- The set of odd integers is binary operation under multiplication (.) but not binary operation under addition (+).

4- - Let A be a nonempty set and $P(A)$ be the set of all subsets of A(power set of A). Then $\cap$ and $\cup$ are binary operations on $P(A)$.

Definition 2.2. A ***mathematical system*** is a nonempty set of elements together with one or more binary operations defined on this set.

Examples.

1- $(Z,+)$, $(Z,.)$, $(P(A), \cap)$ are Mathematical system.

2- $(nZ_e,+,.)$ is Mathematical system but $(Z_o,+,.)$ is not Mathematical system.

3- Let $S = \{1,-1,i,-i\}$, $with\ i^2 = -1$ and $(\cdot)$ is a multiplication operation defined on S. Then $(S,.)$ is a mathematical system.

Definition 2.3. A group G consists of a set G together with a binary operation $*$ for which the following properties are satisfied:

(I) $(x * y) * z = x * (y * z)$ for all elements x, y and z of G (the Associative Law);

(II) there exists an element e of G (known as the identity element of G) such that

$e * x = x = x * e$, for all elements x of G;

(III) for each element x of G there exists an element x' of G (known as the inverse of x) such that $x * x' = e = x' * x$ (where e is the identity element of G).

The order $|G|$ of a finite group G is the number of elements of G.

Examples. 1- $(Z,+), (R,+), (R-\{0\},.)\ and\ (M_{n\times n}(R),+)$ are groups.

2- $(P(A),\Delta)$ is a group, but $(P(A),\cap)$ and $(P(A),\cup)$ are not groups.

Example. Let $S = \{a,b,c\}$. Let $\bullet$ be the binary operation on S with the following composition table:

$\bullet$	a	b	c
a	b	c	a
b	a	c	a
c	b	b	c

Then it is not associative; for example $(a \bullet b) \bullet\ c = c \bullet\ c =\ c, a \bullet\ (b \bullet\ c) = a \bullet\ a = b$.

Definition 2.4. A group G is called an abelian group (or commutative) if the binary operation of G is commutative $(x * y = y * x\ for\ all\ x, y \in G)$.

Then $\bullet$ is not commutative; for example above as $a\ \bullet b = c, b \bullet\ a =\ a$.

Examples.

1- Let a be any nonzero real number and consider the set G of integral multiples of a $G = \{na |\ n \in Z\}$. Then $(G, +)$ is a commutative group .

2- Let * be a binary operation defined of the set Q^{+} as follows:

$a * b = \frac{a.b}{3}, for\ all\ a, b \in Q^{+}$. Show that $(Q^{+},*)$ is a commutative group.

3- Let $S =\ \mathbb{R} - \{-1\}$ and * defined of S as follows:

$a * b = a + b + ab, for\ all\ a, b \in S$. Show that $(S,*)$ is a group.

4- Let $Q_8 = \{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$ with

$$i^2 = j^2 = k^2 = -1$$

$$i.j = k, \quad j.k = i, \quad k.i = j$$

$$j.i = -k, \quad k.j = -1, \quad i.k = -j$$

Then $(Q_8, .)$is not a commutative group and is said a **quaternion group**.

Definition 2.5. A *Semigroup* is a pair $(S, *)$ consisting of a nonempty set S together with an associative binary operation $*$ defined on S.

Example. $(P(A),\cap)$ and $(P(A),\cup)$ are semigroups for any set A.

SOLVED PROBLEMS:

Q1/Determine if the following sets G with the operation indicated form a group. If not, point out which of the group axioms fail.

(a) G = set of all integers, $a * b = a - b$.

(b) G = set of all integers, $a*b = a + b + ab$.

(c) G = set of nonnegative integers, $a * b = a + b$.

(e) $G = Z^+, a * b = max\{a, b\}$,

(f) $G = Z \times Z, (a, b) * (e, d) = (a + e, b + d)$,

(g) $G = R^\# \times R^\#, (a, b) * (e, d) = (ae + bd, ad +. bd)$.

Q2/ Let S be the set of all real numbers $\neq -1$, Define * on S by $a * b = a + b + ab$.

(a) Show that * gives a binary operation on S.

(b) Show that (S, *) is a group.

(c) Find the solution of the equation 2*x*3=7 in S.

3- Elementary Properties of Groups.

Lemma 3.1.

1- A group G has exactly one identity element e satisfying $e * x = x = x * e$ for all $x \in G$.

2- An element x of a group G has exactly one inverse x^{-1} .

3- $(x^{-1})^{-1} = x, for\ all\ x \in G$.

4- If $x, y \in G$, then $(x * y)^{-1} = y^{-1} * x^{-1}$.

5- The cancellation laws holds in that if $x * y = x * z$ or y$* x = z * x$ implies y$= z$.

Proof. (1) Suppose that $(G,*)$ has two identity elements e_1 and e_2.

Since $e_1 {*} a = a {*} e_1 = a\ \ and\ e_2 {*} a = a {*} e_2 = a,\ \ for\ all\ a\ in\ G.$

In particular if e_1 is identity element, then $e_1 * e_2 = e_2$. But e_2 is also identity element, so we have $e_1 * e_2 = e_1$. Thus we obtain $e_1 = e_1 * e_2 = e_2$ and consequently $e_1 = e_2$. That is if the group has an identity element, then there is a unique. ■

(5) Since $a \in G$, then there is $a^{-1} \in G$.

Multiplying the equation $a * b = a * c$ on the left side by a^{-1}, we obtain

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

The by **(II),** this becomes

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

Hence $e * b = e * c$, therefore $b = c$. ■

Theorem 3.2. The group $(G, *)$ is abelian if and only if

$(a * b)^{-1} = a^{-1} * b^{-1}, for\ all\ a, b \in G.$

Proof. Suppose that G is Abelain group. Hence by Theorem 3.1 part (4) we have

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

Conversely, suppose that $(a * b)^{-1} = a^{-1} * b^{-1}$. Hence

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

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

That is we get $(a * b)^{-1} * (b * a) = e$, therefore $a * b = b * a$. ■

Corollary 3.3. The only solution of the group equation $x * x = x\ is\ x = e$.

Definition 3.4. In any group $(G, *)$, the ***integral powers*** of an element $x \in G$ are defined by

$$x^n = x * x * ... * x \quad \text{(n-factors)}$$

$$x^0 = e,$$

$$x^{-n} = \underbrace{x^{-1} * x^{-1} * ... * x^{-1}}_{n-times} = (x^{-1})^n, \qquad \text{where } n \in \mathbb{Z}^+.$$

Theorem 3.5. Let $(G, *)$ be a group, $x \in G$ and $n, m \in \mathbb{Z}$. Then

1- $x^n * x^m = x^{n+m} = x^m * x^n$.

2- $(x^n)^m = x^{nm} = (x^m)^n$.

3- $x^{-n} = (x^n)^{-1}$,

4- $e^n = e$.

Remark. If additive notation is employed for an Abelain group then the notation 'x^n ' is replaced by 'nx' for all integers n and elements x of the group. Then the theorem 3.5 states that $(m + n)x = mx + nx$ and $(mn)x = m(n(x))$ for all integers m and n.

Solve the following problems

Q1/ If G is an abelian group, prove that $(a * b)^n = a^n * b^n$ for all integers n.

Q2/ Let $(G,.)$ be a group such that $(a * b)^2 = a^2 * b^2$ for every $a, b \in G$. Prove that the group is commutative.

Q3/ If G is a group in which $a^2 = e$ for all $a \in G$, show that G is abelian.

Q4/ Let G be a group, and suppose that a and b are any elements of G. Show that $(aba^{-1})^n = ab^na^{-1}$, for any positive integer n.

4. Integers Modulo n

Definition 4.1. Let n be a fixed positive integer. Two integers a *and* b are said to be ***congruent modulo n***, written $a \equiv b(mod\ n)$ if and only if $a - b = kn$ for some integer k or $(a - b)$ is divisible by n.

Examples 1- $26 \equiv 2(mod\ 3)$. 2- $15 \equiv 7(mod\ 2)$

1- $3 \not\equiv 2(mod\ 4)$ 4- $-2 \equiv 6(mod\ 8)$

Theorem 4.2. Let n be a fixed positive integer and a, b are arbitrary integers. Then $a \equiv b(mod\ n)$ if and only if a *and* b have the same remainder when divided by n.

Proof. Let $a \equiv b(mod\ n) \Rightarrow a - b = kn \text{ or } a = b + kn$ for some integer k,

and let $b = qn + r$ when divided by n and r is remainder, $0 \leq r < n$.

Now $a = b + kn = qn + r + kn = (q + k)n + r$,

then a has the same remainder of b when divided by n.

Conversely, let $a = q_1n + r \text{ and } b = q_2n + r,\ q_1, q_2 \in z, (0 \leq r < n)$.

Now $a - b = (q_1n + r) - (q_2n + r) = (q_1 - q_2)n$

Therefore $a \equiv b(mod\ n)$.

Theorem 4.3. Let n be a fixed positive integer and a, b, c and d are arbitrary integers. Then:

1- $a \equiv a(mod\ n)$.

2- If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$.

3- If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$.

4- If $a \equiv b(mod\ n)\ and\ c \equiv d(mod\ n)$, then $a + c \equiv b + d(mod\ n)$ and $a.c \equiv b.d(mod\ n)$.

5- If $a \equiv b(mod\ n)$, then $a.c \equiv b.c(mod\ n)$.

6- If $a \equiv b(mod\ n)$, then $a^k \equiv b^k(mod\ n)$ for every positive integer k.

Proof. H.W.

Remark. The converse of part (5) is not true, for example $5.2 \equiv 1.2(mod\ 8)$ but $5 \equiv 1(mod\ 8)$.

Theorem 4.4. If $ca = ab(mod\ n)$ and c is relatively prime to n, then $a \equiv b(mod\ n)$.

Proof. If $ca = cb(mod\ n)$, then $c(a - b) = kn$ for some integer k.

Since c is relatively prime to n, then n is not divide c. Thus n must divide $a - b$, that is $a \equiv b(mod\ n)$.

Definition 4.5. For an arbitrary integer a, let $[a]$ denote the set of all integer numbers congruent to a modulo n:

$$[a] = \{\ x \in Z\ /\ x \equiv a(mod\ n)\ \} = \{\ x \in Z\ /\ x \equiv a + kn\ for\ some\ integer\ k\ \}.$$

We call $[a]$ the congruence class modulo n determined by a, and a is a representative of this class.

Examples.

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

2- If $n = 3$, then $[0] = \{ x \in Z \,/\, x \equiv 0 (mod\ 3)\}$

$$= \{ x \in Z \,/\, x = 3k, for\ some\ k \in Z \}$$

$$= \{\ldots, -6, -3, 0, 3, 6, \ldots\} = [3] = [6] = [-3]$$

$$[1] = \{ x \in Z \,/\, x \equiv 1 (mod\ 3)\}$$

$$= \{ x \in Z \,/\, x = 1 + 3k, for\ some\ k \in Z \}$$

$$= \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$$

We see that every integer lies in one of these classes. Integers in the same congruence class are congruent modulo 3, while integers in different classes are incongruent modulo 3.

Remark. We select the smallest nonnegative integer for each congruence class to represent it.

Theorem 4.6. Let n be a positive integer and Z_n be as defined above. Then:

1- For each $[a] \in Z_n$, $[a] \neq \emptyset$.

2- If $[a] \in Z_n$ and $b \in [a]$, then $[a] = [b]$.

3- For any $[a], [b] \in Z_n$ such that $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$..

4- $\cup \{[a], a \in Z\} = Z$.

Proof.

Theorem 4.7. For each positive integer n, the mathematical system $(Z_n, +_n)$ forms a commutative group. Known as the group of integers modulo n.

Proof. **(1)** A binary operation $+_n$ may be defined on Z_n as follows:

For each $[a], [b] \in Z_n$, let $[a] +_n [b] = [a + b]$.

To prove that $+_n$ is well defined

Let $[a] = [b]$ and $[c] = [d]$.

Now $a \in [a] = [b]$ and $c \in [c] = [d]$

$\Rightarrow a \equiv b (mod\ n) and\ c \equiv d (mod\ n) \Rightarrow (a+c) = (b+d)(mod\ n) \Rightarrow a + c \in [b+d]$

$\Rightarrow [a+c] = [b+d]\ or\ [a]+_n[c] = [b]+_n[d]$

Thus the operation $+_n$ is well defined.

(2) If $[a],[b],[c] \in Z_n$, then

$[a]+_n([b]+_n[c]) = [a]+_n[b+c] = [a+(b+c)]$

$$= [(a+b)+c] = [a+b]+_n[c] = ([a]+_n[b])+_n[c].$$

(3) By definition of $+_n$, its clear that $[0]$ is the identity element.

(4) If $[a] \in Z_n$, then $[n-a] \in Z_n$, and $[a]+_n[n-a] = [a+(n-a)] = [n] = [0]$, so that $[a]^{-1} = [n-a]$.

(5) For any $[a],[b] \in Z_n$, $[a]+_n[b] = [a+b] = [b+a] = [b]+_n[a]$.

Therefore $(Z_n, +_n)$ is a commutative group.

Example. $Z_9 = \{[0],[1],[2],[3],[4],[5],[6],[7],[8]\}$

$$[1]^{-1} = [8], [5]^{-1} = [4], [6]^{-1} = [3].$$

Remark. For simplicity, we often write $Z_n = \{0, 1, 2, \dots, n-1\}$.

Definition 4.8. Let n be a fixed positive integer. Consider Z_n Let $\cdot_n$ be define on Z_n by for all $[a],[b] \in Z_n$

$$[a] \cdot_n [b] = [ab].$$

$(Z_n, \cdot_n)$ is a mathematical system.

$Z_n^{\times}$ ={ the set of all multiplicative inverse elements}.

Example. Find $Z_9^{\times} = \{1,2,4,5,7,8\}$, since $1 \cdot_9 1 = 1$, $2 \cdot_9 5 = 1, 4 \cdot_9 7 = 1, 8 \cdot_9 8 = 1$.

Solve the following problems

Q1/ Prove that if $a \equiv b\ (mod\ n)$, then $ca \equiv cb\ (mod\ cn)$.

Q2/ Find all solutions x, where $0 \leq x < 15$, of the equation $3x \equiv 6 \ (mod\ 15)$.

Q3/ Prove that $6^n \equiv 6 \ (mod\ 10) for\ any\ n \in Z^+$.

Q4/ For any integer n, prove that either $n^2 \equiv 0 \ (mod\ 4)\ or\ n^2 \equiv 1 \ (mod\ 4)$.

Q5/ Suppose $a^2 \equiv b^2 \ (mod\ n), where$ n is aprime number . Prove that either

$a \equiv b \ (mod\ n),$ or $a \equiv -b \ (mod\ n)$.

Q6/ Find the multiplicative inverse of each nonzero element of Z_9.

Q7/ In Z_{18} find all units (list the multiplicative inverse) .

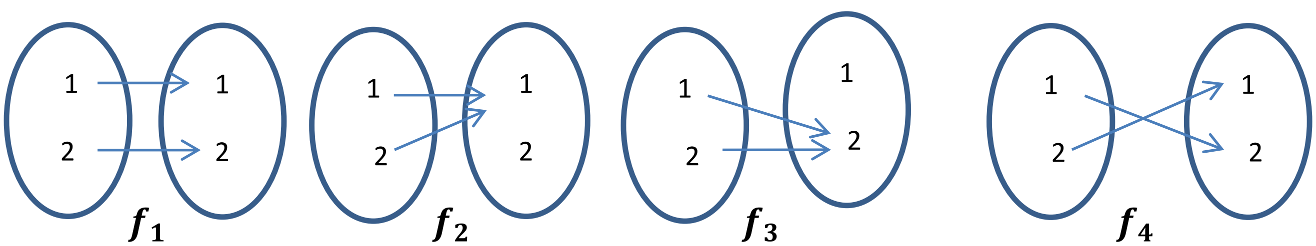
Q8/ Write out multiplication tables for the set $Z_{15}^{\times}$.

5. Permutation groups.

Definition 5.1. A ***permutation*** of a set A is a function from A into A that is both one-to-one and onto itself.

Example. The function $f(x) = x + 1$ is a permutation of the set $\mathbb{Z}$.

Let $A = \{1,2\}$, the there are four functions from A to A, which are



Thus $Map(A) = \{\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3}, \boldsymbol{f_4}\}$. Is $Map(A)$ a group with respect to composition of functions?

f_1 and f_4 are onto and one to one function(bijections) but the f_2 and f_3 are neither Injective (onto) nor surjective (one to one).

Remark. The set of all permutations of the set A will be denoted by the symbol S_A

For any positive integer n, the symmetric group on the set $\{1, 2, 3,. . ., n\}$ is called the *symmetric group on n elements*, and is denoted by S_n

Suppose that $A = \{1, 2, \dots, n\}$

For any $f \in S_n$, $f = \{(1, f(1)), (2, f(2)), \dots, (n, f(n))\}$. Also we can represent f in

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

For example if $A = \{1, 2, 3, 4, 5\}$ and

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$, then

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$$

Theorem 5.2. Let A be a nonempty set. Then $(Sym(A), o)$ is a group (called ***symmetric group of the set A***).

Proof. Clearly if $f, g \in Sym(A)$, then $f \circ g \in Sym(A)$. hence $Sym(A)$ is closed under o.

For $f, g, h \in Sym(A)$, we show that $(f \text{o} g)\text{o}h = f\text{o}(g\text{o}h)$.

$$(f\text{o}g)\text{o}h(x) = (f\text{o}g)(h(x)) = f\left(g(h(x))\right) = f(g\text{o}h(x)) = f\text{o}(\text{g}\text{o}h)(x).$$

I. Hence (***I***) is satisfied.

The identity map I_A is a permutation of the set A and is identity element such that $f \circ I_A = I_A \circ f = f$. Therefore (***II***) is satisfied.

For proving S_A has an inverse, suppose that $f \in Sym(A)$, that is f is one to one and onto function. Therefore f^{-1} is also one to one and onto function, hence $f^{-1} \in Sym(A)$ such that $f^{-1} \circ f = f \circ f^{-1} = I_{A.}$ Thus (***III***) is satisfied. Hence $(Sym(A), \circ)$. ■

Remark. The set of all permutations of the set N=$\{1, 2, 3, \dots, n\}$ will be denoted by the symbol S_n and S_n contains $n!$ distinct elements.

Example. Let $A = \{1, 2, 3\}$. Then there are $3! = 6$ permutations in S_3, namely

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

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

O	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_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Note that $f_2 \circ f_4 = f_6, \quad and\ f_4 \circ f_2 = f_3$ as the table above, we get $(S_3, \circ)$ forms a group as the symmetric group on n symbols, which is non commutative for $n \geq 3$.. .

Definition 5.3. A permutation f of a set A is a ***cycle of length k*** if there exist $n_1, n_2, \dots\ , n_k \in A$ such that

$$f(n_i) = n_{n+1,}\ for\ all\ 1 \leq i \leq k - 1,$$

$$f(n_k) = n_1\ and$$

$$f(m) = m, for\ all\ m \in A\ but\ m \notin \{n_1, n_2, \dots\ , n_k\}.$$

We write $f = (n_1, n_2, \dots\ , n_k)$.

Example . In $(S_6, \circ)$, if we have

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix} = (1\ \ 3\ \ 4\ \ 2\ \ 5\ \ 6\ )$ and the inverse of f is

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

Theorem 5.4. Every permutation can be written as a product of disjoint cycles.

Two cycles $(a_1, a_2, \dots, a_n)$ and $(b_1, \dots, b_m)$ are said to be disjoint if $a_i \neq b_j$ for all i , j.

Example. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 4 & 8 & 2 & 6 & 3 \end{pmatrix}$$

$1 \to 5 \to 8 \to 3 \to 1$. Therefore σ contains the cycle (1 5 8 3).
$2 \to 7 \to 6 \to 2$. Therefore σ contains the cycle (2 7 6),
Note that the cycles (1 5 8 3) and (2 7 6) are disjoint, and σ contains the product (or composition) (1 5 8 3)(2 7 6).
.

Definition 5.5. A cycle of length two is called ***transposition***.

In the example above $(S_3, \circ)$, f_4, f_5 *and* f_6 are transpositions.

Lemma 5.6. Every permutation can be written a product of transpositions.

That is mean $f = (n_1, n_2, \dots , n_k) = (f = (n_1, n_k)(n_1, n_{k-1}) \dots (n_1, n_2)$

Example. In $(S_3, \circ)$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ \ 2\ \ 3) = (1\ \ 3)(1\ \ 2)$

Note that these transpositions are not disjoint and so they don't have to commute. Since

$$(1\ \ 2)(1\ \ 3) \neq (1\ \ 3)(1\ \ 2)$$

Definition 5.7. A permutation of a finite set is ***even*** if it can be written as a product of even number of transpositions, and is ***odd*** if it can be written as a product of odd number of transpositions.

For example $S_3 = \{ i, (1\ \ 2\ \ 3),\ (1\ \ 3\ \ 2), (2\ \ 3), (1\ \ 3), (1\ \ 2)\}$, then

$i, (1\ \ 2\ \ 3)\ and\ (1\ \ 3\ \ 2)$ are even transpositions however $(2\ \ 3), (1\ \ 2)\ and\ (1\ \ 3)$ are odd transpositions.

Theorem 5.8. Every permutation in S_n can be written as a product of either an even number of transpositions, or an odd number of transpositions but **not both**.

Definition 5.9. All even permutations is called ***alternating group*** and denoted by A_n. i.e $A_n = \{\sigma \in S_n : \sigma\ is\ even\}$.

Theorem 5.10. If $n \geq 2$, the collection of all even permutations of $\{1, 2, \ \dots, n\}$forms a subgroup of order $\frac{n!}{2}$ of the symmetric group S_n.

For example $|S_3| = 3! = 6$, then $|A_3| = \frac{3!}{2} = \frac{6}{2} = 3$.

Solve the following problems:

Q1/ Determine whether the given function is a permutation of R.

1- $f: R \longrightarrow R$ defined by $f(x) = x + l$.
2- $f: R \longrightarrow R$ defined by $f(x) = x^2$.
3- $f: R \longrightarrow R$ defined by $f(x) = -x^3$.

Q2/ Find the number of elements in the set $\{\delta \in S_4\ | \delta(3) = 3\}$.

Q3/ Express the permutation of {1, 2, 3, 4, 5, 6, 7, 8} as a product of disjoint cycles, and then as a product of transpositions. 1f

$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 4 & 7 & 8 & 3 & 1 \end{pmatrix}$, $\quad \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 7 & 3 & 8 & 6 & 5 & 4 \end{pmatrix}$.

Q4/ What is the order of the cycle (1 2 8 5 7)?

Q5/ Consider the three permutation in S_6

$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 6 & 1 \end{pmatrix}$, $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$, $\lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 1 & 5 \end{pmatrix}$

Compute

(a) $\gamma\delta$ (b) $\gamma\delta^2$ (c) $\gamma^2\lambda$ (d) λ^{100} (e) $(\gamma\lambda)^{-1}$

Q6/ Compute the order of $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 2 & 10 & 4 & 6 & 8 & 9 & 11 & 1 & 3 & 7 \end{pmatrix}$. For $\sigma = (2\ \ 10\ \ 7)$, compute the order of $\sigma\tau\sigma^{-1}$. Is τ an even permutation or an odd permutation?

6. Cyclic group.

Definition 6.1. Let $(G, *)$ be a group. Then G is said to be ***cyclic group*** if there exists an element $a \in G$ such that every element of G is of the form a^n for some integer n. Such an element a is called a generator of the group and written as

$$G =< a >= \{a^n \mid n \in Z\}.$$

Examples.

1- $(Z, +)$ is cyclic group generated by 1 and -1. Then $Z =< 1 >=< -1 >$
2- $(Q, +)$ is not cyclic group.
3- If $G = \{1, -1, i, -i\}$, where $i^2 = -1$, then $(G, .)$ is a cyclic group generated by i and $-i$ and $G =< i >=< -i >$.
4- $(Z_5,\ +_5)$ is a cyclic group and $Z_5 =< 1 >=< 2 >=< 3 >=< 4 >$.

Remark. In $(Z_n,\ +_n)$, if n is prime, then every elements is generator except 0.

Definition 6.2. If $(G, *)$ is a finite group, then the ***order of*** $(\boldsymbol{G}, \boldsymbol{*})$ is the number of elements in G and denoted by $|G|$ or $o(G)$ and if G is infinite, then we say G has an infinite order.

Definition 6.3. Let $(G, *)$ be a group. Then the ***order of an element a*** in G is the least positive integer n such that $a^n = e$, where e is the identity element of G, and denoted by $o(a) = n$.

Example. $(Z_8, +_8)$, Then $o(Z_8)=8$ and $o(2) = 4$ where $2 \in Z_8$.

Lemma 6.4. Let $(G,*)$ be a group and $a, b \in G$ has a finite order. Then

1- $o(a) = o(a^{-1})$

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

Proof. 1- if $o(a) = n$, then by Theorem 3.5 we have

$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$

Suppose that m be a least positive integer satisfyies $(a^{-1})^m = e$, then

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

Which is contradiction for $o(a) = n$, for a lest positive integer n such that $(a^{-1})^n = e$, hence $o(a^{-1}) = n$.

2-H.W.

Example.

2- In a group $(Q_8, .)$, we find $(-1)^2 = 1$ *and* $o(-1) = 2$ *but* $(-1) \neq 1$.

3- In $(Z, +)$, $O(1)$is infinite since 1≠0, 1+1 ≠0, 1+1+1≠0, …

i.e $1 + 1 + 1 = 1^3$.

Theorem 6.5. Every cyclic group is abelian.

Proof. Let $(G,*)$ be a cyclic group generated by an element a. That is

$G =< a >= \{a^n : n \in Z\}$.

Let x, y be any two elements of G, then there exist integers n *and* m such that

$x = a^n$ *and* $y = a^m$. Then

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

Therefore $(G,*)$ is abelian group.

Definition 6.6. Let $(G,*)$ *and* $(H,\bullet)$be two groups,

$$G \times H = \{(g, h): g \in G \text{ and } h \in H\}$$

For all $(g_1, h_1),\ (g_2,\ h_2) \in G \times H$, then

$(g_1, h_1).(g_2,\ h_2) = (g_1 * g_2,\ h_1 \bullet h_2) \in G \times H.$

H.w. Prove that $(G \times H, .)$ is a group.

Example. describe the direct product of $(Z_{2,} +_2)$ and $(Z_{3,} +_3)$.

Solve the following problems

Q1/ If (G, *) be a group and let x be an element of G of order 20. Find $o(x^4)$, $o(x^7)$, $o(x^{11})$.

Q2/ Find the order of the elements

a- $(2,2) in\ Z_{12} \times Z_4$

b- $\big([1],\ (1\ \ 2)\big) in\ Z_2 \times S_4$.

Q3/ Give an example of a group with the property described, or explain why no example exists.

a. A finite group that is not cyclic

b. An infinite group that is not cyclic

c. A cyclic group having only one generator

d. An infinite cyclic group having two generators

e. A finite cyclic group having four generators .

f. A nonabelian cyclic group.

Q4/ List the generators of Z_{12}.

Q5/ Show that Q^+ is not a cyclic group.

Q6/ Let $G = \{a, b, c, d\}$ be a group. Complete the following Cayley table for this group.

*	a	b	c	d
a				
b				
c			b	
d		b		

7. Subgroups.

Definition 7.1. Let $(G, *)$ e a group and H be a nonempty subset of G. The pair $(H, *)$ is said to be a subgroup of $(G, *)$ if $(H, *)$ is itself a group.

Example.

(1) $(Z_e, +)$ and $(nZ, +)$ are a subgroup of $(Z, +)$.

(2) $(Q - \{0\}, .)$ is a subgroup of $(R - \{0\}, .)$.

(3) Let $G = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$ and $a.b = b.a = c, a.c = c.a = b$ $and\ \ b.c = c.b = a$. The pair (G, .) is a group, known as Klein's four-group.

Remarks.

1- The binary operation on the subgroup H must be the same binary operation on the group G.

2- Any group has at least two subgroups, $(\{e\}, *)$ the identity element e of the group, and the group itself are called trivial subgroups. The other subgroups called proper subgroups.

Example. R^* is a subset of R and both are groups. But $R^*$is **not** a subgroup of R, since the operation that makes R^* a group is multiplication and the operation that makes R a group is addition.

Theorem 7.2. Let $(G, *)$ be a group and $\emptyset \neq H \subseteq G$. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if $a, b \in H$ implies $a * b^{-1} \in H$.

Proof. If $(H, *)$ is a subgroup of $(G, *)$ and $a, b \in H$, then $b^{-1} \in H$ and so by the closure condition $a * b^{-1} \in H$

Conversely, suppose $a * b^{-1} \in H$ for all $a, b \in H$ and H is a nonempty subset of G, then H contains at least one element let b,

1- We take $a = b$ to see $a * a^{-1} \in H$ that is $e \in H$.

2- Since $b \in H\ and\ by$ (1) $e \in H$ implies that $b^{-1} = e * b^{-1} \in H$.

3- If $a, b \in H$, then by (2) we have $b^{-1} \in H$, so that $a * b = a * (b^{-1})^{-1} \in H$,hence H is closed with respect to the operation $*$.

4- Since $*$ is an associative operation in G and $a, b, c \in H \subseteq G$, therefore H satisfied the associative law as a subset of G.

Then $(H, *)$ is a subgroup of $(G, *)$.

Example.

1- Let $(G, .) = (Z \times Z, .)$ be a group and $H = \{(a, \ a): \ a \in Z\}$. Show that $(H, .)$ be a subgroup of $(G, .)$.

2- Let$(Gl_2(R), \ .)$ be a group and $H = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl_2(R): ad - bc = 1\} \subseteq Gl_2(R)$.

Show that $(H, .)$ be a subgroup of $(Gl_2(R), .)$.

Definition 6.3. The center of a group $(G, *)$, denoted by $cent(G)$ or $Z(G)$ is the set $cent(G) = \{c \in G : \ (c * x = x * c \ for \ all \ x \in G\}$.

Remark. The group $(G, *)$ is commutative if and only if $cent(G) = G$.

Examples.(1) In the group $(Q_8, .), cent(Q_8) = \{1, -1\}$.

(1) Klien's four-group

(2) $(S_3 . \bullet)$

(3) $(Gl_2(R), \ .)$

Theorem 7.4. Let $(G, *)$ be a group. Then $(cent(G), *)$ is a subgroup of the group $(G, *)$.

Proof. Since $e \in cent(G)$, then $cent(G) \neq \emptyset$.

Consider any two elements $a, b \in cent(G)$, we must prove that $a * b^{-1} \in cent(G)$.

We know for all $x \in G$, we have

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

which implies $a * b^{-1} \in cent(G)$. Then by Theorem 7.2 we get $(cent(G), *)$ is a subgroup of $(G, *)$.

Theorem 7.5. If $(H_1, *)$ and $(H_2, *)$ are two subgroups of the group $(G, *)$, then $(H_1 \cap H_2, *)$ is also a subgroup of $(G, *)$.

Proof. Since the sets H_1 and H_2 contains the identity element of $(G, *)$, the intersection $H_1 \cap H_2 \neq \emptyset$.

Now suppose that $a \; and \; b$ are any two elements of $H_1 \cap H_2$, then $a, b \in H_1$ and $a, b \in H_2$. Since $(H_1, *)$and $(H_2,*)$ are subgroups, it follows that $a*b^{-1} \in H_1 \; and \; a*b^{-1} \in H_2$, then $a*b^{-1} \in H_1 \cap H_2$, which implies $(H_1 \cap H_2, *)$ is a subgroup of $(G, *)$.

Remark.(1) If $(H_i, *)$ is an arbitrary indexed collection of subgroups of the group $(G, *)$, then $(\cap H_i, *)$ is also a subgroup of $(G, *)$.

(2) The union of two subgroups $(H_1, *)$ and($H_2,*)$ of the group $(G, *)$ need not be subgroup of $(G, *)$.

For example. $(\{0, 6\}, +_{12})$ and $(\{0, 4, 8\}, +_{12})$ are two subgroups of the group $(Z_{12}, +_{12})$, then the union is $(\{0, 4, 6, 8\}, +_{12})$ is not subgroup of $(Z_{12}, +_{12})$.

Theorem 7.6. Let $(H_1, *)$ and($H_2,*)$ be two subgroups of the group $(G, *)$. Then $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$ iff $H_1 \subseteq H_2 \; or \; H_2 \subseteq H_1$.

Proof. Suppose that $H_1 \subseteq H_2 \; or \; H_2 \subseteq H_1$, then $H_1 \cup H_2 = H_2 \; or \; H_1 \cup H_2 = H_1$.

Since H_1 and H_2 are subgroups, then $H_1 \cup H_2$ is a subgroup of G.

Conversely, suppose that $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$ such that

$H_1 \not\subset H_2 \; and \; H_2 \not\subset H_1$, then there exists an elements $a \; and \; b$ such that

$a \in H_1 - H_2$ and $b \in H_2 - H_1$.

Since $H_1 \cup H_2$ is a subgroup of G, then $a*b^{-1} \in H_1 \cup H_2$

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

Suppose $*b^{-1} \in H_2 \Rightarrow a = a*b^{-1} * b \in H_2$, which is contradiction, and if $a*b^{-1} \in H_1$

$\Rightarrow b^{-1} = a^{-1} * a*b^{-1} \in H_1 \Rightarrow$ b ∈ H, which is contradiction**.** Then either $H_1 \subseteq H_2$ *or* $H_2 \subseteq H_1$.

Remark. Let $(H_i, *)$ be an indexed collection of subgroups of the group $(G, *)$. Suppose the family of subsets $\{H_i\}$ has the property that for any two of its members H_i and H_j there exists a set H_k (depending on i *and* j) in $\{H_i\}$ such that $H_i \subseteq H_k$ *and* $H_j \subseteq H_k$. Then $(\cup H_i, *)$ is also a subgroup of $(G, *)$.

Definition 7.7. If $(G,*)$ is an arbitrary group and $\emptyset \neq S \subseteq G$, then the symbol (S) will represent the set

$$(S) = \cap \{H \mid S \subseteq H; (H,*) \text{ is a subgroup of } (G,*)\}.$$

Theorem 7.8 . The pair $((S),*)$ is a subgroup of $(G,*)$, known the subgroup generated by the set S.

Definition 7.9 Let $(G,*)$ be a group and a be an element in G. Then a cyclic subgroup $((a),*)$ is called a subgroup generated by an element a.

Example. In $(Z_4, +_4)$ a subgroup generated by 2 is ([2]) = { [0], [2]}

Theorem 7.10. Every subgroup of cyclic group is cyclic.

Proof. Let $(G, *)$ be a cyclic group generated by the element a and let $(H, *)$ be a subgroup of $(G, *)$.

If $H = \{e\}$, then $H = < e >$ is cyclic.

If $H \neq \{e\}$, then there exist $x \in H$ such that $x = a^m$ for some $m \in Z$.

If $a^m \in H$, where $m \neq 0$, then $a^{-m} \in H$, hence H must contains positive powers of a. Let n be the smallest positive integer such that $a^n \in H$.

we must to show that $H = (a^n)$.

Let $a^k \in H \Rightarrow (a^k)^n \in H, for\ all\ k \in Z$, therefore $(a^n) \subseteq H$.

By the Division Algorithm there exist integers $q\ and\ r$ for which

$k = nq + r,\ 0 \leq r < n.$

Since both $a^n,\ a^k \in H$, and $r = k - nq, therefore\ x^r = x^{k-nq} \in H$

If r>0, we have contradiction to the assumption that a^n is a minimal positive power of $a\ in\ H$. Accordingly $r = 0\ and\ k = nq \Rightarrow a^k = (a^n)^q \in (a^n)$.

$H \subseteq (a^n)$. Consequently $H = (a^n)$.

Examples Let $(Z_n,\ +_n)$ is cyclic group generated by $< 1 >$. Then every subgroups are cyclic.

Definition 7.11. Let $(G,*)$ be a group and H, K be nonempty subsets of G. The product of $H\ and\ K$ is the set $H * K = \{h * k: h \in H, k \in K\}$.

Example.

1- Let $(Z_8,\ +_8)$, $H = \{1,5\}$ and $K = \{2, 4, 6\}$. Then

$$H{+_8}K = \{1{+_8}2, 1{+_8}4, 1{+_8}6, 5{+_8}2, 5{+_8}4, 5{+_8}6\} = \{3, 5, 7, 1\}.$$

Hence $(H{+_8}K, +_8)$ is not a subgroup of $(Z_8,\ +_8)$.

2- Let $(S_3,\bullet)$, $H = \{i, (1\ \ 2)\}\ and\ K = \{i, (1\ \ 3)\}$. Then

$$H \bullet K = \{i \bullet i, i \bullet (1\ \ 3), (1\ \ 2) \bullet i, (1\ \ 2) \bullet (1\ \ 3)\} = \{i, (1\ \ 3), (1\ \ 2), (1\ \ 3\ \ 2)\}$$

Hence $(H \bullet K,\ \bullet)$ is not a subgroup of $(S_3,\bullet)$.

Theorem 7.12. If $(H,*)$ and $(K,*)$ are subgroups of the group $(G,*)$ such that $H * K = K * H$, then $(H * K,*)$ is a subgroup of $(G,*)$.

Proof. Note that $H * K = K * H$ is not mean $h * k = k * h, for\ all\ h \in H\ and\ k \in K$, but it means $for\ all\ h \in H\ and\ k \in K,$ there exist $h_1 \in H\ and\ k_1 \in K$ such that $h * k = k_1 * h_1$.

Since $e \in H\ and\ e \in K$, then $e = e * e \in H * K$, hence $H * K \neq \emptyset$. Let $x, y \in H * K$.

We must to show that $x * y^{-1} \in H * K$.

Now let $x = h_1 * k_1$ and $y = h_2 * k_2$, where $h_1, h_2 \in H\ and\ k_1,\ k_2 \in K$. Hence

$$x * y^{-1} = (h_1 * k_1) * (h_2 * k_2)^{-1} = (h_1 * k_1) * (k_2^{-1} * h_2^{-1}) = h_1 * (k_1 * k_2^{-1}) * h_2^{-1})$$

Since $(K,*)$ is a subgroup of $(G,*)$, then $k_1^{-1} * k_2^{-1} \in K$ and therefore

$$k_1 * k_2^{-1} * h_2^{-1} \in K * H \text{ and } K * H = H * K,$$

then there exist elements $h \in H\ and\ k \in K$ such that $k_1 * k_2^{-1} * h_2^{-1} = h * k$, we conclude that $x * y^{-1} = h_1 * (h * k) = (h_1 * h) * k \in H * K$.

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

Corollary 7.13. If $(H,*)\ and\ (K,*)$ are subgroups of the commutative group $(G,*)$, then $(H * K,*)$ is a subgroup of $(G,*)$.

Solve the following

Q1/ Find all cyclic subgroups of Z_{15}.

Q2/ Find all cyclic subgroups of $Z_{20}^{\times}$.

Q3/ Let G be an abelian group, and let n be a fixed positive integer. Show that

$N = \{ g \in G | g = a^n\ for\ some\ a \in G\}$ is a subgroup of G.

Q4/ If G is an abelian group and if $H = \{a \in G \mid a^2 = e\}$, show that H is a subgroup of G. Give an example of a nonabelian group for which the H is *not* a subgroup.

Q5/ In the group of symmetries of the equilateral triangle, find:

a) all subgroups.

b) The center of the group .

Q6/ list the elements of the subgroup generated by the given subset.

1. The subset {2, 4} of Z_{12}
2. The subset {2, 6} of Z_{12}
3. The subset {6, 12} of Z_{18}
4. The subset {15, 30} of Z_{36}.

Q7/ Let (H, *) be a subgroup of f the group (G, *) and the set N(H) be defined by $N(H) = \{a \in G: a * H * a^{-1} = H\}$. Prove that the pair (N(H), *) is a subgroup of (G, *), called the normalize of H in G.

Q8/ Let G be a group, with subgroup H. Show that $K = \{(x, x) \in G \times G | x \in H\}$ is a subgroup of $G \times G$.

Q9/ In Z_{20}, find the order of the subgroup <16>; find the order of <14>.

Q10/ Let $(M(\mathbb{R}), \oplus)$ be a group of all real continuous functions over R and let $F = \{f \in M(\mathbb{R}): f$ is differentiable} and $h = \{f \in M(\mathbb{R}): f(1) = 0\}$. Show that $(H, \oplus)$ is subgroup of the group $(M(\mathbb{R}), \oplus)$.

8. Cosets and Lagrange's Theorem

Definition 8.1. Let $(H,*)$ be a subgroup of the group $(G,*)$ and let $a \in G$. The set $a * H = \{a * h: h \in H\}$ is called left coset of H in G. The element a is representative of $a * H$ and $H * a = \{h * a: h \in H\}$ is called a right coset of H in G.

Remark. If e is the identity element of $(G, *)$, then

$e * H = \{ e * h: h \in H\} = \{h: h \in H\} = H$. That is H itself is a left coset of H.

Example . Let $(Z_{10}, +_{10})$ be a group and $H = \{0, 5\}$ be a subgroup of $(Z_{10}, +_{10})$.

$1 +_{10} H = \{1, 6\}$, $2 +_{10} H = \{2, 7\}$, $3 +_{10} H = \{3, 8\}$, $4 +_{10} H = \{4, 9\}$, $5 +_{10} H = \{5, 0\}$

$6 +_{10} H = \{1, 6\}$, $7 +_{10} H = \{2, 7\}$, $8 +_{10} H = \{3, 8\}$, $9 +_{10} H = \{4, 9\}$.

There are only five distinct cosets.

Theorem 8.2. If $(H,*)$ is a subgroup of the group $(G,*)$, then $a * H = H$ if and only if $a \in H$.

Proof. Suppose that $a * H = H$. Since $e \in H$, then $a = a * e \in a * H = H \Longrightarrow a \in H$. Conversely, suppose that $a \in H$. Since H is closed under * operation, hence for all $h \in H$, then $a * h \in H$, therefore $a * H \subseteq H$. The opposite inclusion by $h \in H$, hence

$h = e * h = (a * a^{-1}) * h = a * (a^{-1} * h) \in a * H$ and consequently $H \subseteq a * H$.

Therefore $H = a * H$.

Theorem 8.3. If $(H,*)$ is a subgroup of the group $(G,*)$, then $a * H = b * H$ if and only if $a^{-1} * b \in H$.

Proof. Suppose that $a * H = b * H$. Then $for\ all\ h \in H$, there exist $h_1 \in H$ such that $b * h_1 = a * h$. From this we get

$$a^{-1} * b = h * h_1^{-1}.$$

Since $(H,*)$ is a subgroup, then $a^{-1} * b = h * h_1^{-1} \in H$

Conversely, let $a^{-1} * b \in H$. Then by Theorem 8.2 $(a^{-1} * b) * H = H$. This implies that for any $h \in H$, there exist an element $h' \in H$ such that

$$h = (a^{-1} * b) * h' \Leftrightarrow a * h = b * h' \Leftrightarrow a * H \subseteq b * H.$$

At the same way we get $b * H \subseteq a * H$, consequently $a * H = b * H$.

Example. Let $(G,*) = (Z_{12}, +_{12})$ and $H = \{0, 4, 8\}$. Then all left cosets are

$$0 +_{12} H = \{0, 4, 8\} = 4 +_{12} H = 8 +_{12} H$$

$$1 +_{12} H = \{1, 5, 9\} = 5 +_{12} H = 9 +_{12} H$$

$$2 +_{12} H = \{2, 6, 10\} = 6 +_{12} H = 10 +_{12} H$$

$$3 +_{12} H = \{3, 7, 11\} = 7 +_{12} H = 11 +_{12} H$$

and the distinct left cosets are $\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6, 10\}, \{3, 7, 11\}$.

Note that the number of distinct left cosets equal $\frac{O(G)}{O(H)}$ is called the index of $H \ in \ G$ and the number of elements in each cosets are equal .

Theorem 8.4. If $(H,*)$ is a subgroup of the group $(G,*)$, then either the coset $a * H \ and \ b * H$ are disjoint or else $a * H = b * H$

Proof. Suppose that $(a * H) \cap (b * H) \neq \emptyset$, then there exist $c \in a * H \cap b * H$
$\Rightarrow c \in a * H \ and \ c \in b * H$. Since $c \in a * H$, there exist an element $h_1, \ h_2 \in H$ such that $c = a * h_1$ and $c = b * h_2$. It follows that $a * h_1 = b * h_2 \Rightarrow a^{-1} * b = h_1 * \ h_2^{-1}$.
Since $(H,*)$ is a subgroup, then $h_1 * \ h_2^{-1} \in H$,that is $a^{-1} * b \in H$. By Theorem 7.3 we get $a * H = b * H$.

Theorem 8.5. If $(H,*)$ is a subgroup of the group $(G,*)$, then the left(right) cosets of $H \ in \ G$ forms a partition of the set G.

Proof. If each $a \in G$, then $a \in a * H$. Sine each element can belong to one and only one left coset of $H \ in \ G$. Thus

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

Hence the set G is a partitioned by H into disjoint sets, each of which has exactly as many elements as H.

Theorem 8.6.(Lagrange theorem) Let $(H,*)$ be a subgroups of a finite group $(G,*)$. Then the order of $H$and the index of $H \ in \ G$ are divides the order of G.

Proof. Since G is a finite group, then $G = \{a_1, a_2, \ \dots, a_n\}$, $(H,*)$ is a subgroup of $(G,*)$ of order k and the index of $H \ in \ G$ is r.
Hence there exist r distinct left cosets of $H \ in \ G$ say $a_1 * H, a_2 * H, \dots, a_n * H$.
Thus by Theorem 8.5, we get

$G = (a_1 * H) \cup (a_2 * H) \cup \ \dots \cup (a_r * H)$ and $|a_i * H| = |H| = k, for\ i = 1, 2, \dots, r.$

$$|G| = |a_1 * H| + |a_2 * H| + \ \dots + |a_r * H| = \underbrace{k + k + \cdots + k}_{r-times} = r.k$$

$$= (index\ of\ H\ in\ G)(order\ of\ H)$$

Consequently order of H is divide the order of G.

.

Corollary 8.7. If $(G,*)$ is a group of order n, then the order of any element $e \neq a \in G$ is a factor of n, and $a^n = e$.

Proof. Let the element a in the group $(G,*)$ have order k. Then the cyclic subgroup generated by a is of order k.

Let $=< a > \Rightarrow |H| = k$. By **Theorem 8.6** k is divisor of n, that is $n = rk$ for some $r \in Z^+$. Hence

$$a^n = a^{rk} = (a^k)^r = e^r = e.$$

Theorem 8.8. Every group $(G,*)$ of prime order is cyclic.

Proof. Let $(G,*)$ be a group such that $|G| = p,\ p$ is prime, and let H be a cyclic subgroup of G generated by $e\ \neq a \in G$; i.e $H = (a)$. By **Theorem 8.6** $|H|$ divides $|G|$, then either $|H| = 1$or $|H| = p$. Since $|H| \neq 1$, then must be $|H| = p = |G|$. Therefore $G = (a)$.

Remark. The converse of Lagrange theorem is not true in general, for example the group $(A_4,\ o)$ is of order 12, then the factors of 12 are 1, 2, 3, 4, 6, 12. Then A_4 has no subgroup of order 6.

Solve the following Problems

Q1/ List the left cosets of the subgroup

(a) H = {i; (13)} of S_3.

(b) $(Z_e, +)\ of\ (Z, +)$,
(c) $(Z, +)\ of\ (Q, +)$,
(d) $(< 4 >, +_{12})\ of\ (Z_{12}, +_{12})$.
(f) ((1 3), 0) of $S_3 \times Z_2$
(f) Find all left cosets of the subgroup $\{R_{360}, D_1\}$ of the group D_4 given by Table.

Q2/ Give an example of a group $(G,*)$ and a subgroup $(H,*)$ of $(G,*)$ such that $aH = bH$, but $Ha \neq Hb$ for some $a, b \in G$.

Q3/ Let G be a group generated by a, b such that $O(b) = 2$, $O(a) = 6$, and $(ab)^2 = e$. Show that
(a) $aba = b$,
(b) $(a^2b)^2 = e$,
(c) $ba^2b = a^4$,

Q3/ Let $G = \{a, b, c, d\}$ be a group. Complete the following Cayley table for this group.

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

Q4/ find the index $[G: H]$, if $G = Z_6 \times Z_4$ and $H = \{0\} \times Z_4$
Q5/ Let G be a finite group and $A\ and\ B$ be subgroups of G such that $A \subseteq B \subseteq G$. Prove that $[G : A] = [G : B][B : A]$.

Q6/ Can an element of an *infinite* group have *finite* order? Explain.

Q7/ Suppose H is a subgroup of a group G, and $[G : H] = 2$. Suppose also that a and b are in G, but not in H. Show that $ab \in H$.

Q8/ Prove that every proper subgroup of a group of order p^2 (p aprime) is cyclic.

9. Normal subgroups and quotient groups.

Definition 9.1. A subgroup $(H,*)$ of the group $(G,*)$ is said to be normal(or invariant) in $(G,*)$ if and only if every left coset of H in G is also a right coset of H in G(i.e. $a * H = H * a$ for every $a \in G$).

Example. Let $V = \{e, a, b, c\}$ with $ab = ba = c, bc = cb = a, ac = ca = b \; and$ $a^2 = b^2 = c^2 = e$. If $H = \{e, a\}$, then $eH = H = He$

$$bH = \{b, c\} = Hb$$

$$cH = \{c, b\} = Hc$$

$$aH = \{a, e\} = Ha$$

Therefore H is normal subgroup of V.

Theorem 9.2. Let $(H,*)$ be a subgroup of the group $(G,*)$. Then $(H,*)$ is a normal subgroup of $(G,*)$ if and only if $a * H * a^{-1} \subseteq H \; for \; each \; a \in G$.

Proof. Suppose that $a * H * a^{-1} \subseteq H$ for each $a \in G$. We must prove that $a * H = H * a$

Let $a * h \in a * H$.

Now $a * h = (a * h) * e = \big((a * h) * (a^{-1} * a)\big) = \big((a * h * a^{-1}) * a\big)$.

Since $a * h * a^{-1} \in a * H * a^{-1} \subseteq H$, then there exist $h_1 \in H$ such that

$a * h = (a * h * a^{-1}) * a = h_1 * a \; and \; h_1 * a \in H * a$, so we conclude $a * H \subseteq H * a$.

We obtain the opposite inclusion, $H * a \subseteq a * H$, by similar way upon observing that our hypothesis also implies

$a^{-1} * H * a = a^{-1} * H * (a^{-1})^{-1} \subseteq H$.

Then $H * a = a * H$ for all $a \in G$. Therefore H is normal subgroup of G.

Conversely, Suppose $a * H = H * a$ for each $a \in G$.

Let $a * h_1 * a^{-1} \in a * H * a^{-1}, h_1 \in H$.

Since $a * H = H * a$, then there exist $h_2 \in H$ such that $a * h_1 = h_2 * a$.

Consequently

$a * h_1 * a^{-1} = (h_2 * a) * a^{-1} = h_2 * (a * a^{-1}) = h_2$, which implies $a * H * a^{-1} \subseteq H$.

Example. Let (S_3, o). Then $H = \{e, (1\ \ 2\ \ 3),\ (\ 1\ \ 3\ \ 2)\}$ is normal subgroup but $\{e,\ (1\ \ 2)\},\ \{e,\ (1\ \ 3)\}\ and\ \{e,\ (2\ \ 3)\}$ are not normal subgroups of (S_3, o).

Theorem 9.3. Let $(G,*)$ be a group. Then $(cent\ G,*)$ is normal subgroup of $(G,*)$.

Proof. By Theorem 6.4 $(cent\ G,*)$ is a subgroup of $(G,*)$. Then we have only to show that $a * centG * a^{-1} \subseteq cent\ G$ for all $a \in G$.

Let $a * c * a^{-1} \in a * cent\ G * a^{-1}$, for $c \in cent\ G$.

Since $c \in cent\ G$, then $c * a = a * c$, for all $a \in G$.

Now $a * c * a^{-1} = c * a * a^{-1} = c * e = c \in cent\ G$.

Therefore $a * cent\ G * a^{-1} \subseteq cent\ G$, hence by Theorem 8.2 $(cent\ G,\ *)$ is normal subgroup of $(G,*)$.

Theorem 9.4. If $(H,*)$ is a subgroup of the group with $[G\colon H] = 2$, then $(H,*)$ is a normal subgroup of the group $(G,*)$.

Proof. Since $[G\colon H] = 2$, then there exist exactly two cosets H and $G - H$.

Let $a \in G$. Then either $a \in H\ or\ a \in G - H$.

If $a \in H$, then $a * H = H = H * a$, hence H is a normal subgroup.

If $a \in G - H$, then $H \cap a * H = \emptyset \Rightarrow G = H \cup (a * H)$ and $H \cap H * a = \emptyset \Rightarrow G = H \cup (H * a)$. Therefore $a * H = H * a\ for\ all\ a \in G$. hence H is a normal subgroup of G.

Definition 9.5. If $(H,*)$ is normal subgroup of the group $(G,*)$, then the collection of distinct cosets of H in G is denoted by G/H and defined as follows:

$$G/H\ =\ \{a * H\ :\ a \in G\}.$$

A binary operation $\otimes$ is defined on G/H by

$$(a * H)\otimes(b * H) = (a * b) * H \; for \; all \; a * H, b * H \in G/H.$$

We must prove that $\otimes$ is well defined.

Let $a * H = b * H$ and $c * H = d * H$. We must prove that $(a * c) * H = (b * d) * H$

Now since $a * H = b * H \Rightarrow a^{-1} * b \in H$ and $c * H = d * H \Rightarrow c^{-1} * d \in H$.

Now

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

Since $a^{-1} * b \in$ H $\Rightarrow d^{-1} * (a^{-1} * b) * d \in d^{-1} * H * (d^{-1})^{-1} \subseteq H$

and Since H is closed, we get $c^{-1} * d \in H$, hence

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

$\Rightarrow (a * H)\otimes(c * H) = (b * H)\otimes(d * H)$. Therefore $\otimes$ is well defined.

Theorem 9.6. If $(H,*)$ is a normal subgroup of the group $(G,*)$, then $(G/H, \otimes)$ forms a group, known as the quotient group of G by H.

Proof. By definition we observe that G/H is closed under operation $\otimes$.

1- associativity of $\otimes$ on G/H,

$$\begin{aligned}[(a * H)\otimes(b * H)]\otimes(c * H) &= \big((a * b) * H\big)\otimes(c * H) \\ &= \big(a * (b * c)\big) * H \\ &= (a * H)\otimes\big((b * c) * H\big) \\ &= (a * H)\otimes[(b * H)\otimes(c * H)].\end{aligned}$$

Hence $\otimes$ is associative.

2- $H = e * H$ is the identity element of G/H, where e is the identity element of G.

$$(a * H)\otimes(e * H) = (a * e) * H = a * H = (e * a) * H = (e * H)\otimes(a * H).$$

3- The inverse of $a * H$ is $a^{-1} * H$, where a^{-1} is the inverse of a in G.

Now

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

Hence $(G/H, \otimes)$ is a group.

Remark. We have $\left|\frac{G}{N}\right| = [G : N]$. In particular, if G is a finite group, then $|G/N| = |G|/|N|$.

Solve the following Problems

Q1/ Let H be a normal subgroup of a group G. Prove that if G is commutative, then so is the quotient group G/H.

Q2/ Suppose $(H,*)$ and $(K,*)$ are normal subgroups of the group $(G,*)$ with $H \cap K = [e\}$. Show that $h * k = k * h \; for \; all \; h \in H \; and \; k \in K$.

Q3/ Prove that if the quotient group $(G/cen(G), \otimes)$ is cyclic , then $(G,*)$ is a commutative group.

Q4/ Let $(H,*)$ be a proper subgroup of $(G,*)$ such that $for \; all \; x, y \in G/H, xy \in H$. Prove that $(H,*)$ is a normal subgroup of $(G,*)$.

Q5/ Show that every subgroup of an abelian group is normal.

Q6/ Show that every group of prime order is simple.
Q7/ Prove that the quotient group of an abelian group is abelian.

Q8/ (a) Give an example of an abelian group G/H such that G is not abelian.Explain.
(b) Give an example of a cyclic group G/H such that G is not cyclic. Explain.

Q9/ Let H, K be normal subgroups of a group G. If $G/H = G/K$ then show that

$$H = K.$$

Q10/ Let H be a normal subgroup of a group G. If $xyx^{-1}y^{-1} \in H$, for all $x , y \in G$, then show that G/H is abelian.

Q11/ If H is a subgroup of a group G and N a normal subgroup of G then show that $H \cap N$ is a normal subgroup of H.

10. Homomorphisms.

Definition 9.1. If $(G,*)$ and $(H,\ o)$ are groups, then a function $f : G \longrightarrow H$ is a homomorphism if $f(x * y) = f(x)\ o\ f(y)\ for\ all\ x, y \in G$.

Examples.

1- Let $(G,*)$ and $(G',\ o)$ be two groups. Then the function $f : G \longrightarrow G'$ such that $f(x) = e'\ for\ any\ x \in G$ is a homomorphism and called a trivial homomorphism. In fact,

$$f(x * y) = e' = e'\ o\ e' = f(x)\ o\ f(y)$$

2- Let $(G,*)$ be any group and $f: G \to G$ defined by $f(x) = x\ for\ all\ x \in G$ is a is a homomorphism and is called an identity homomorphism. In fact,

$$f(x * y) = x * y = f(x) * f(y), for\ all\ x, y \in G.$$

Definition 9.2. A homomorphism f from the group $(G,*)$ into group (G', o) is called an isomorphism if f is one-to-one and onto function. Two groups G and G' are called isomorphic, denoted by $G \cong G'$, if there exists an isomorphism between them.

Example. Let $(R, +)$ and $(R^+,\ .)$ be two groups, where R is the set of real numbers, and $f: R \to R^+$ defined by $f(x) = e^x\ for\ all\ x \in R$. Show that f is an isomorphism.

$for\ all\ x, y \in R$, we have

$f(x + y) = e^{x+y} = e^x\ .\ e^y = f(x).\ f(y)$.

Hence f is a homomorphism.

Suppose that $f(x) = f(y) \Rightarrow e^x = e^y \Rightarrow x = y$. Hence f is one-to-one.

Since $f(x) = e^x$ is defined $for\ all\ x \in R$ and its inverse $g(x) = ln\ x$ is also defined $all\ x \in R^+$, that is $f(\ln x) = e^{\ln x} = x$. Hence f is onto.

Therefore f is an isomorphism and $(R, +) \cong (R^+,\ .)$.

Definition 9.3. An isomorphism f from $(G,*)$ into itself is called an automorphisms. The set of all automorphisms of G is denoted by $Aut(G)$

Example. A function $f:(Z,+) \longrightarrow (Z,+)$ defined by $f(n) = -n, for\ all\ n \in Z$. Hence f is an automorphisms.

Theorem 9.4. Let $f:(G,*) \longrightarrow (G',\ o)$ is a group homomorphism. Then

1- $f(e) = e'$, where e and e' are identity elements of G and G' respectively.

2- $f(x^{-1}) = (f(x))^{-1}, for\ all\ x \in G$.

3- $f(x^n) = (f(x))^n, for\ all\ x \in G\ and\ n \in Z$.

4- If $O(x) = n$, then $O(f(x))$ is divides n.

Proof.

1- For all $x \in G$, we have

$$e * x = x = x * e \Longrightarrow f(x) o\, e' = f(x) = f(e * x) = f(x) o f(e).$$

Hence by cancellation law we get $e' = f(e)$.

2- H.w

3- By using induction, if $n = 0$, then $f(x^0) = f(e) = e'$, that is the statement is true.

If $n = 1$, then $f(x^1) = f(x)$, that is the statement is true too.

Suppose the statement is true for n such that n is a positive integer, that is

$$f(x^n) = (f(x))^n.$$

Now $f(x^{n+1}) = f(x^n * x) = f(x^n) o f(x) = \left(f(x)\right)^n o f(x) = (f(x))^{n+1}$.

Finally, if $n < 0$, put $n = -m$, such that m is positive integer. Hence

$f(x^n) = (f(x^{-m}) = (f(x^m))^{-1} = (f(x)^m)^{-1} = (f(x))^{-m} = (f(x))^n$.

4- H.w.

Theorem 9.5. Every finite cyclic group of order n is isomorphic to the group $(Z_n, +_n)$.

Proof. Let $(G,*)$ be a cyclic group of order n generated by a. Hence by Theorem 6.11

$$G = (a) = \{e, a, a^2, \quad \dots \ , a^{n-1}\}.$$

Let $f: G \longrightarrow Z_n$ be a function defined by $f(a^k) = [k], for\ all\ 0 \leq k < n$.

To prove that f is one-to-one , suppose that

$$f(a^i) = f(a^j) \Longrightarrow [i] = [j] \Longrightarrow i \equiv j (mod\ n)$$

Hence there exist an integer l such that $i - j = ln \Longrightarrow i = j + ln$, therefore,

$a^i = a^{j+ln} = a^j$, that is f is one-to-one.

It is clear that is f is onto.

Now $for\ all\ a^i, a^j \in G, f(a^i * a^j) = f(a^{i+j}) = [i + j] = [i]+_n[j] = f(a^i)+_n f(a^j)$.

Hence f is an isomorphism and $(G,*) \cong (Z_n, \ +_n)$.

Theorem 9.6. Every infinite cyclic group is isomorphic with the group $(Z, +)$.

Proof. Let $(G,*)$ be an infinite cyclic group generated by a. Hence

$$G = (a) = \{a^n : n \in Z\}.$$

Such that $a^i \neq a^j, for\ all\ i \neq j$

Let $f: G \longrightarrow Z$ be a function defined by $f(a^k) = k, \ k \in Z$.

To prove that f is one-to-one , suppose that

$$f(a^i) = f(a^j) \Longrightarrow i = j \Longrightarrow a^i = a^j.$$

Hence f is one-to-one.

It is clear that is f is onto.

Now $for\ all\ a^i, a^j \in G, f(a^i * a^j) = f(a^{i+j}) = i + j == f(a^i) + f(a^j)$.

Hence f is an isomorphism, therefore, $(G,*) \cong (Z, +)$

Corollary. Any two cyclic groups of the same order are isomorphic.

Example. Show that the two groups $(Q, +)$ and($Q^+, \ .)$ are not isomorphic.

Suppose that there exists an isomorphism $f:(Q,+)\longrightarrow(Q^{+},\ .)$.

Let $3\in Q^{+}$. Since f is onto, then there an element $x\in Q$ such that $f(x)=3$.

$$f(x)=f\left(\frac{x}{2}+\frac{x}{2}\right)=f\left(\frac{x}{2}\right).f\left(\frac{x}{2}\right)=\left(f\left(\frac{x}{2}\right)\right)^{2}=3.$$

But it is contradicting, the fact $f\left(\frac{x}{2}\right)$ is a rational number and there is no exists a rational number equal to 3.

Theorem 9.7. Let f be a homomorphism from the group $(G,*)$ into the group (G',o). Then

1- If $(H,*)$ is a subgroup of $(G,*)$, then $(f(H),\ o)$ is a subgroup of $(G',\ o)$.

2- If (K,o) is a subgroup of (G',o), then $(f^{-1}(K),\ *)$ is a subgroup of $(G,*)$.

Proof. (1) $f(H)=\{\,f(x):\ x\in H\}$

Since $e\in H$, then $f(e)\in f(H)\Longrightarrow f(H)\neq\emptyset$.

Let $f(x),\ f(y)\in f(H), for\ x,y\in H$.

Now $f(x)o\,f(y)^{-1}=f(x)o\,f(y^{-1})=f(x*y^{-1})\in f(H)$, Since $x*y^{-1}\in H$.

Therefore by Theorem 6.2, we get $f(H)$ is a subgroup of G'.

(2) H.W.

Theorem 9.8. Let f be a homomorphism from the group $(G,*)$ into the group (G',o). Then

1- If (K,o) is a normal subgroup of (G',o), then $(f^{-1}(K),\ *)$ is a normal subgroup of $(G,*)$.

2- If $f(G)=G'$ and $(H,*)$ is a normal subgroup of $(G,*)$, then $(f(H),\ o)$ is a normal subgroup of $(G',\ o)$.

Proof. (1) By theorem 8.7 $(f^{-1}(K),\ *)$ is a subgroup of $(G,*)$.

Now to show that $(f^{-1}(K), *)$ is a normal subgroup of $(G,*)$, suppose $x \in f^{-1}(K)$ and $g \in G$. Since f is a homomorphism, then we have

$f(g * x * g^{-1}) = f(g) o f(x) o\, f(g)^{-1} = f(g) o f(x) o f(g^{-1})$, Since $f(x) \in K, f(g) \in G'$ and $(K,*)$ is a normal subgroup of (G', o).

Therefore $f(g) o f(x) o f(g^{-1}) \in K \Longrightarrow g * x * g^{-1} \in f^{-1}(K)$. Hence $(f^{-1}(K),*)$ is a normal subgroup of $(G,*)$.

Definition 9.9. Let f be a homomorphism from the group $(G,*)$ into the group (G', o) and Let e' be the idenitiy element of (G', o). Then **kerenel of f,** denoted by $ker\, f$, is the set $\ker f = \{a \in G : f(a) = e'\}$.

Theorem 9.10. If f is a homomorphism from the group $(G,*)$ into the group (G', o), Then $(ker\, f,*)$ is a normal subgroup of $(G,*)$.

Proof. Since $(\{e'\}, o)$ is a normal subgroup of (G', o) and $\ker f = f^{-1}(\{e'\})$, then by Theorem 9.8 $(\ker f,*)$ is a normal subgroup of the group $(G, *)$.

Theorem 9.11. Let f be a homomorphism from the group $(G,*)$ into the group (G', o). Then f is one-to-one if and only if $\ker f = \{e\}$.

Proof. Suppose the function f is one-to-one. Let $x \in \ker f \Longrightarrow f(x) = e' = f(e)$.

Since f is one-to-one, we get $x = e \Longrightarrow \ker f = \{e\}$.

Conversely, suppose that $\ker f = \{e\}$. Let $x, y \in G$ and $f(x) = f(y)$.

To prove f is one-to-one, we must show that $x = y$. But if

$$f(x) = f(y) \Longrightarrow f(x) o f^{-1}(y) = e'$$

$$\Longrightarrow f(x) o f(y^{-1}) = e' (f\ is\ homorphism)$$

$$\Longrightarrow f(x * y^{-1}) = e'.$$

Which implies $x * y^{-1} \in \ker f$. But $\ker f = \{e\}$. Therefore $x * y^{-1} = e \Longrightarrow x = y$.

Theorem 9.12. (Cayley's Theorem)If $(G,*)$ is an arbitrary group, then

$$(G,*) \cong (F_G, o).$$

Proof. $F_G = \{f_a : a \in G\}$, we define the function $f_a: G \longrightarrow G\ by\ f_a(x) = a * x, x \in G$.

(f_a is called the left multiplication function).

Now define the function $f: G \longrightarrow F_G$ by $g(a) = f_a,\ for\ each\ a \in G$.

It is clear that the function is onto. If

$f(a) = f(b) \Longrightarrow f_a = f_b \Longrightarrow f_a(x) = f_b(x), for\ all\ x \in G \Longrightarrow a * x = b * x \Longrightarrow a = b$.

Which show that f is one-to-one.

We proof that f is a homomorphism:

$$f(a * b) = f_{a*b} = f_a o f_b = f(a) o f(b).$$

Hence f is an isomorphism and $(G,*) \cong (F_G,\ o)$.

Example. Consider $(G,*) = (R^{\#}, +)$, for $a \in R^{\#}$ is the left-multiplication function f_a, defined by $f_a(x) = a + x,\quad x \in\ R^{\#}$.

11.The Fundamental of Isomorphisms Theorems.

Theorem 10.1. (First Isomorphism Theorem)

If f is a homomorphism from the group $(G,*)$ onto the group (G', o). Then

$$\left({}^{G}\!/_{\ker f},\ \ \otimes\right) \cong (G', o).$$

Proof. Put $ker\ f\ =\ K$. We define a function φ: ${}^{G}\!/_{K} \longrightarrow G'$ by

$\varphi(x + K) = f(x),\ \ for\ x \in G$.

We must show that φ is well defined, suppose $x + K = y + K \Longrightarrow x * y^{-1} \in K = \ker f$.

Therefore $f(x * y^{-1}) = e'$. But f is homomorphism, then

$f(x) o f(y^{-1}) = e' \Longrightarrow f(x) o (f(y))^{-1} = e'$

$\Longrightarrow f(x) = f(y) \Longrightarrow\ \varphi(x + K) = \varphi(y + K)$.

Hence φ is well defined.

Now to show that φ is a homomorphism, suppose that

$$\varphi\big((x*K)\otimes(y*K)\big)=\varphi\big((x*y)*K\big)$$
$$=f(x*y)$$
$$=f(x)of(y)$$
$$=\varphi(x*K)o\varphi(y*K).$$

Hence φ is a homomorphism.

Let $\varphi(x*K)=\varphi(y*K)\Longrightarrow f(x)=f(y)\Longrightarrow f(x)o(f(y))^{-1}=e'$.

Since f is a homomorphism, therefore

$f(x)of(y^{-1})=e'\Longrightarrow f(x*y^{-1})=e'\Longrightarrow x*y^{-1}\in K\Longrightarrow x*K=y*K.$

Hence φ is one-to-one.

Finally, for all $z\in G'$ there exists $y\in G$ such that $z=f(y)=\varphi(y+K)$.

Hence φ is onto. Therefore φ is an isomorphism and $\left({}^{G}/_{K},\ \otimes\right)\cong(G',o)$.

Lemma 10.2. If $(H,*)$ is a subgroup of the group $(G,*)$ and $(K,*)$ is a normal subgroup of $(G,*)$, then $(H\cap K,*)$ is a normal subgroup og the group $(H,*)$.

Proof. Let $h\in H\ and\ l\in H\cap K\Longrightarrow l\in H\ and\ l\in K.$

Since $(H,*)$ is a subgroup of the group $(G,*)$, then $h*l*h^{-1}\in H$ and

Since $(K,*)$ is a normal subgroup of the group $(G,*)$, then $h*l*h^{-1}\in K$.

Hence $h*l*h^{-1}\in H\cap K, for\ al\ \ h\in H\ and\ l\in H\cap K$, therefore $(H\cap K,*)$ is a normal subgroup og the group $(H,*)$.

Theorem 10.3. (Second Isomorphism Theorem)

If $(H,*)$ is a subgroup of the group $(G,*)$ and $(K,*)$ is a normal subgroup of $(G,*)$, then

$$H*K/K\cong H/H\cap K.$$

Proof. First we must to show that $(K,*)$ is a normal subgroup of $(H*K,*)$ and by lemma 9.2 we have $(H\cap K,*)$ is a normal subgroup of $(H,*)$.

We prove the theorem by using Theorem 9.1, then so we define a function

$\varphi: H*K\longrightarrow H/H\cap K$ by $\varphi(h*k)=h*(H\cap K), for\ all\ h\in H\ and\ k\in K.$

We show that φ is well defind

Let $h * k = h_1 * k_1, for\ h_1, h \in H\ and\ k_1, k \in K$.

$\Longrightarrow h_1^{-1} * h = k_1 * k^{-1} \Longrightarrow h_1^{-1} * h \in H \cap K$.

By Theorem 6.18 we get $h_1 *(H \cap K) = h * (H \cap K) \Longrightarrow \varphi(h_1 * k) = \varphi(h * k)$.

To show that φ is onto. Suppose $h * k, h_1 * k_1 \in H * K, for\ h, h_1 \in H\ and\ k, k_1 \in K$.

Since $(K,*)$ is a normal subgroup of $(G,*)$, then

$h_1^{-1} * k * h_1 \in K$. put $k_2 = h_1^{-1} * k * h_1 \Longrightarrow h_1 * k_2 = k * h_1$.

$$\varphi\big((h * k) * (h_1 * k_1)\big) = \varphi(h * h_1 * k * k_1)$$

$$= (h * h_1) * (H \cap K)$$

$$= \big(h * (H \cap K)\big) \otimes \big(h_1 * (H \cap K)\big)$$

$$= \varphi(h * h_1) \otimes \varphi(k * k_1)$$

Hence φ is a homorphism.

For all $h * (H \cap K) \in H/H \cap K$, for $h \in H$, then $\varphi(h * e) = h * (H \cap K)$.

Hence φ is onto.

By Theorem 10.1, we get $H * K/\ker\varphi \cong H/H \cap K$.

Now

$$\ker\varphi = \{h * k : h \in H,\ \ k \in K;\ \varphi(h * k) = H \cap K\}$$

$$= \{h * k : h \in H,\ \ k \in K; h * (H \cap K) = H \cap K\}$$

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

Therefore $H * K/K \cong H/H \cap K$.

Theorem 10.4. (Third Isomorphism Theorem)

If $(H,*)$ and $(K,*)$ are normal subgroups of the group $(G,*)$ and $(H,*)$ is a subgroup of $(K,*)$, then

1- $(K/H,\otimes)$ is a normal subgroup of the group $(G/H,\otimes)$ and

2- $\frac{G/H}{K/H} \cong G/K$.

Proof. 1- H.W.

2- We prove the theorem by using Theorem 9.1, then so we define a function $\varphi: G/H \longrightarrow G/K$ by $\varphi(x * H) = x * K, for\ all\ x * H \in G/H$.

We show that φ is well defined. Suppose that $x * h, y * H \in G/H,\ for\ \ x, y \in G$ and $x * h = \ y * H \Longrightarrow x^{-1} * y \in H \subseteq K \Longrightarrow x^{-1} * y \in K \Longrightarrow x * K = y * K$.

Hence $\varphi(x * H) = \varphi(y * H)$, that is φ is well defined.

Let $x * h, y * H \in G/H,\ for\ \ x, y \in G$. Then

$$\varphi\big((x * H) \otimes (y * H)\big) = \varphi((x * y) * H)$$
$$= (x * y * K)$$
$$= (x * K) \otimes (y * K)$$
$$= \varphi(x * H) \otimes \varphi(y * H)$$

Hence φ is a homomorphism.

It is clear by definition φ is onto.

By Theorem 10.1, we get $G/H\ /\ ker\,\varphi \cong G/K$.

Now

$$\ker\varphi = \left\{x * H \in \tfrac{G}{H} : \varphi(x * H) = K\right\}$$
$$= \left\{x * H \in \frac{G}{H} : (x * K) = K\right\} = \left\{x * H \in \frac{G}{H} : x \in K\right\} = \frac{K}{H}$$

Therefore $\frac{G/H}{K/H} \cong G/K$.

Solve the following Problems

Q1/ Determine whether the indicated function f is a homomorphism from the first group into the second group. If f is a homomorphism, determine its kernel.

a) $f: (\mathbb{R}^*, .) \longrightarrow (\mathbb{R}^*, .)$ defined by $f(a) = a^3, \; for\ all\ a \in \mathbb{R}^*$.
b) $f: (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ defined by $f(a) = 3a, \; for\ all\ a \in \mathbb{R}$.
c) $f: (Z_8, +_8) \longrightarrow (Z_8, +_8)$ defined by $f([a]) = [5a]$,
d) Let $G = \{a, a^2, a^3, a^4, a^5 = e\}$ be the cyclic group generated by a.
$f: (Z_5, +_5) \longrightarrow G$ defined by $f(n) = a^n, \; for\ all\ n \in Z_5$.

Let $G = \{a, a^2, a^3, \ldots, a^{12} = e\}$ be a cyclic group generated by a. Show that $f : G \to G$ defined by $f(x) = x^4$, for all $x \in G$, is a group homomorphism. Find $Ker(f)$.

Q2/ Let G be an abelian group. Show that $f : G \to G$ defined by $f(x) = x^{-1}$, for all $x \in G$, is an automorphism.

Q3/ Let $G = \{1, -1\}$ be a group under multiplication. Show that $f: (Z, +) \to G$ defined by

$$f(n) = \begin{cases} 1 & if\ n\ is\ even \\ -1 & if\ n\ is\ odd \end{cases}$$

is onto group homomorphism. Find $Ker(f)$.

Q4/ Let $(G,*)$ be a finite commutative group. Let $n \in Z$ be such that n and |G| are relatively prime. Show that the function $f : G \longrightarrow G$ defined by $f(a) = a^n$ $for\ all\ a \in G$ is an isomorphism of $(G,*)$ onto $(G,*)$.

.

Q5/ Let G be a group and $A\ and\ B$ be normal subgroups of G such that $A \cong B$. Show by an example that $G/A \ncong G/B$.

Q6/ Consider two groups $(Z,+)$ and $(G,.)$ $with$ $G = \{-1, 1, -i, i\}$ where $i^2 = -1$. Show that the mapping defined by $f(n) = (-i)^n, for\ n \in Z$ is a homomrphism from $(Z,+)$ onto $(G,*)$ and determine $ker\ f$.

Q7/ Prove that every proper subgroup of a group of order p^2 (p aprime) is cyclic.

Q8/ Show that (a) $(Z_{20}/< 5 >,\ \otimes) \cong (Z_5,\ +_5)$.

(b) $(3Z/9Z,\ \otimes) \cong (Z_3,\ +_3)$.

Q9/ Let $(G,*) \cong (G',\circ)$.

(a) If G is abelain group then so is G'.

(b) If G is cyclic group then so is G'.

.