ABSTRACT ALGEBRA

Pure Mathematics 7

كلية التربية بالغردقة

1-Sets:

Def. A collection of well-defined objects is called a *set*.
We used capital letters A,B,C,…to denote a set and small letters a,b,c,… to denote the elements of a set. The symbol $a \in A$ means "a is an element of the set A" and $a \notin A$ means "a is not an element of the set A".

- **Set Formulation:**

(1) The Tabulation Method:

We indicate a set by listing all its elements and enclosing them within braces. For example,

$$A = \{1,2,3,4,5\}.$$

$$B = \{a,b,c,d\}.$$

$$Z = \{0,\pm 1,\pm 2,....\}.$$

(2) The Rule Method:

We state the characteristic property by which we can determine whether or not a given object is an element of the set. We write $A = \{x : x \text{ has } p\}$ to say that "A is the set of all elements x for which a certain property p holds ". For example,

$$A = \{x : x \text{ is a solution of } x^2 - 5x + 6 = 0\}.$$

$$B = \{x : x \text{ is an integer}, x^2 \le 100\}.$$

$$X = \{x : x \text{ is prime number}, 1 < x < 10\}.$$

A set A is called a *subset* of a set B if every element of A is an element of B.
Symbolically we write $A \subseteq B$ to say that A is a subset of B.

A is called *proper subset* of B and is denoted by $A \subset B$ if there exists in B at least an element which is not an element of A.
A subset which is not proper is said to be *improper subset*.

Examples:

1- If B be the set of all English alphabets , and A the set of all vowels , then $A \subset B$.

2- If $Z = \{0,\pm 1,\pm 2,...,\pm n,...\}$ and $N = \{1,2,3,..., n,...\}$, then $N \subset Z$.

Two sets A and B are said to be *equal* iff every element of A is an element of B and vice versa, i.e., $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$.

Remark: The signs " : , $\wedge$, $\vee$, $\Leftrightarrow$ " are used to denote " such that , and , or , iff " .

Examples:

1- If $A=\{1,2,3,4,5\}$ and $B=\{2,4,3,1,5\}$, then $A=B$.

2- If $A=\{1,2,3,4,5,6,7,8,9,10\}$ and $B=\{I,II,III,IV,V,VI,VII,VIII,IX,X\}$, then $A=B$.

3- If A is the set of letters in the word " calculate " and $B=\{c,a,l,u,t,e\}$, then $A=B$.

A set consisting of only one element is said to be *singleton set* .

A set which contains no elements is called an *empty* (or *null* or *void*) *set*. It is generally denoted by ϕ.

A set which contains all element is said to be *universal set* ,It is generally denoted by U .

Given a set B and a subset A of B , we call the set of all elements of B which are not elements of A the *complement* of A in B and denoted by A' (or A^C or $B-A$), i.e. $A'=\{x : x\in B, x\notin A\}$.

Given two sets A and B, we define their *intersection* $A\cap B$ as the set of all elements which are common to both A and B. We say that A and B are *disjoint* if $A\cap B=\phi$. We also define the *union* of A and B ,denote $A\cup B$ as the set of all elements which belong to at least one of the two sets A and B. The union of two disjoint sets A and B is denoted by $A+B$ and is called the sum of A and B.

Sometimes, a diagrammatical representation of sets helps in understanding relationships between different sets. This is done by what is known as *Venn's diagram*. It is a diagram in which members of a set are represented by the points of a plane enclosed by a curve drawn in the plane.

Examples:

1- If $A=\{0,\pm2,\pm4,...\}$ and $B=\{0,\pm1,\pm3,...\}$, then $A\cap B=\{0\}$ is a singleton set.

2- If $A=\{x : x^2=4, x \text{ is odd}\}$, then $A=\phi$.

3- If $N=\{1,2,3,...\}$, $A=\{1,3,5,...,2n+1,...\}$, and $B=\{2,4,6,...,2n,...\}$, then $A\cap B=\phi$ and $A\cup B=A+B=N$.

4- The set consisting of all students of a university forms a universal set, whereas students of different faculties form subsets of this universal set.

5- If B is the set of all natural numbers $1,2,3,...$ and A is the set of all even natural numbers, then A' is the set of all odd natural numbers.

The following properties of $\cap$ and $\cup$ for arbitrary sets A,B,C are satisfied:

(1) $A\cap B=B\cap A$, $A\cup B=B\cup A$ (commutative law).

(2) $(A\cap B)\cap C=A\cap(B\cap C)$, $(A\cup B)\cup C=A\cup(B\cup C)$ (associative law).

(3) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$, $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ (distributive law).

(4) $A\cap A=A$, $A\cup A=A$ (idempotent law).

(5) $A\cap U=A$, $A\cup\phi=A$ (identity law).

(6) $(A\cap B)'=A'\cup B'$, $(A\cup B)'=A'\cap B'$ (De Morgan's law).

(7) $(A')'=A$ (involution law).

Given X a set , then the set $P(X)$ of all subsets of X is called a *power set* of X .

The collection of all mutually disjoint subsets of a set X whose union is the whole set X is called a *partition* of a set X .

The number of elements in a set X is called the *order of the set* X , and denoted by $O(X)$.

Given two sets A and B we define the *Cartesian product* $A\times B$ of A and B to be the set of all *ordered pairs* (a,b) of elements $a\in A$ and $b\in B$, i.e. $A\times B=\{(a,b):a\in A\wedge b\in B\}$.

By definition, two ordered pairs (a,b) and (c,d) are equal iff $a=c$ and $b=d$. When $A=B=R$ the set of all real numbers, then $A\times B=R\times R=R^2$ represent the real plane.

Examples:

1- If $X=\{1,2,3\}$ then $P(X)=\{\phi,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},X\}$.

2- If $A=\{1,2,3\}$, $B=\{a,b\}$ then:

$A\times B=\{(1,a),(2,a),(3,a),(1,b),(2,b),(3,b)\}$.

3- A set $\{\{1,2\},\{3,4\},\{5,6\},...\}$ form a partition of a set of all natural numbers N , also a set $\{\{1,4,7,...\},\{2,5,8,...\},\{3,6,9,...\}\}$, but a set $\{\{1,2\},\{2,3\},\{3,4\},...\}$ is not a partition of N (verify that?).

Exercises:

1- Give some examples of collections which is not considered Set (by its mathematical Meaning)?.

2- Give an example for:

(1) A set contains two elements.
(2) A set contains only one element.
(3) An empty set.
(4) An infinite set.

3- By using the Tabulation Method. Represent each of the following sets:

(1) $X=\{ x: x \text{ is a factor of } 6 \}$.
(2) $Y=\{ y: y \text{ is a solution of } y^2=0 \}$.
(3) $A=\{ a: a\in Z^+, a \text{ is odd number}, 1<a<10\}$.
(4) $B=\{ b: b \text{ prime number}, 1<b<12\}$.
(5) $S = \{ x : x \text{ is a multiple of } 3 \}$.

4- By using the Rule Method. Represent each of the following sets:

(1) $S=\{ a, e, i, o, u \}$.
(2) $S=\{10, 100, 1000, 10000, ...\}$.
(3) $S=\{ 1, 1/2, 1/3, 1/4, ...\}$.

5- By using the Algebraic Symbols. Rewrite the following expression:

There exist only eight subsets of a set $A=\{3,5,8,9\}$ contains the element 8 .

6- Let A={a,b,c}.Show that whether of the following is true, and whether is false (Give reasons for your assertion):

(1) $\{a\}\in A$ (2) $\{a,b\}\subset P(A)$ (3) $\{\phi\}\subset P(A)$
(4) $A\in P(A)$ (5) $\{a,b\}\subset A$ (6) $\{a\}\subset P(A)$
(7) $\{d\}\subset P(A)$ (8) $\{\{b\}\}\subset P(A)$

7- For an arbitrary sets A,B,C. Verify that:

(1) $A\cap(A^c\cup B) = A\cap B$
(2) $A\cup(B-A) = A\cup B$
(3) $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$
(4) $A\times(B-C) = (A\times B)-(A\times C)$
(5) $(A\times A)\cap(B\times C) = (A\cap B)\times(A\cap C)$

2-Binary Relations:

Def.1 A subset $\Re \subseteq A \times B$ is called a *binary relation* between a two sets A, B. And if $(a,b) \in \Re$ we say that the element $a \in A$ associates with the element $b \in B$ by a relation $\Re$ and denoted $a \Re b$.

Remark: When $\Re \subseteq A \times A$ we say that $\Re$ is a relation on a set A.

Def.2: For a relation $\Re \subseteq A \times B$ we define two sets:

$D_{\Re} = \{a \in A : a \Re b\} \subset A$, $G_{\Re} = \{b \in B : a \Re b\} \subset B$, the set $D_{\Re}$ is called the *domain* of $\Re$, and the set $G_{\Re}$ is called the *range* of $\Re$.

Def.3: If $\Re_1 \subseteq A \times B$ and $\Re_2 \subseteq B \times C$ we define a *composite relation*

$\Re_2 \circ \Re_1 = \{(a,c) : \exists b \in B ; (a,b) \in \Re_1 \wedge (b,c) \in \Re_2\}$.

Examples:

1- If $\Re$ is a relation on a set $X = \{2,3,4,6\}$ defined by:

$(a,b) \in \Re \Leftrightarrow a \setminus b \ \ \forall a,b \in X$. ($a \setminus b$ means a divide b)

$\therefore \Re = \{(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(6,6)\}$,

$D_{\Re} = \{2,3,4,6\} = G_{\Re} = X$.

2- If $\Re$ is a relation on a set $X = \{1,2,3,4\}$ defined by:

$(a,b) \in R \Leftrightarrow a > b \ \ \forall a,b \in X$.

$\therefore \Re = \{(2,1),(3,1),(3,2),(4,1),(4,2),(4,3)\}$, $D_{\Re} = \{2,3,4\}$, $G_{\Re} = \{1,2,3\}$.

3- If $\Re_1, \Re_2$ are two relations on a set $X = \{1,2,3\}$;

$\Re_1 = \{(1,1),(1,3),(2,1),(2,2),(3,1),(3,3)\}, \Re_2 = \{(1,1),(1,2),(2,2),(3,1)\}$.

$\therefore \Re_2 \circ \Re_1 = \{(1,1),(1,2),(2,2),(3,1),(3,2),(2,1)\}$,

$\Re_1 \circ \Re_2 = \{(1,1),(1,3),(1,2),(2,2),(2,1),(3,1),(3,3)\}$.

Def.4: A binary relation $\Re$ on a set X is called an *equivalence relation* if it satisfies the following conditions:

(E1) $\forall a \in X \Rightarrow (a,a) \in \Re$ (Reflexivity)

(E2) $\forall (a,b) \in \Re \Rightarrow (b,a) \in \Re$ (Symmetry)

(E3) $\forall (a,b),(b,c) \in \Re \Rightarrow (a,c) \in \Re$ (Transitivity)

Examples:

1- If $\Re$ is a relation on a set of all natural numbers $N = \{1,2,3,...\}$ defined by $(a,b) \in \Re \Leftrightarrow a = b \ \ \forall a,b \in N$

Then: (E1) $\forall a \in N ; a = a \Rightarrow (a,a) \in \Re$

(E2) $\forall (a,b) \in \Re \Rightarrow a = b \Rightarrow b = a \Rightarrow (b,a) \in \Re$

(E3) $\forall (a,b),(b,c) \in \Re \Rightarrow a = b,\ b = c \Rightarrow a = c \Rightarrow (a,c) \in \Re$

So, $\Re$ is an equivalence relation.

2- If $\Re$ is a relation on a set of all integers $Z=\{0,\pm1,\pm2,...\}$ defined by:

$$(a,b)\in\Re \Leftrightarrow \frac{a-b}{n}\in Z \quad \forall a,b\in Z, n\in N, n\geq 2$$

Then: (E1) $\forall a\in Z; \frac{a-a}{n}=0\in Z \Rightarrow (a,a)\in\Re$

(E2) $\forall (a,b)\in\Re \Rightarrow \frac{a-b}{n}\in Z \Rightarrow \frac{b-a}{n}\in Z \Rightarrow (b,a)\in\Re$

(E3) $\forall (a,b),(b,c)\in\Re \Rightarrow \frac{a-b}{n}, \frac{b-c}{n}\in Z$

$$\Rightarrow \frac{a-b}{n}+\frac{b-c}{n}=\frac{a-c}{n}\in Z \Rightarrow (a,c)\in\Re$$

So, $\Re$ is an equivalence relation. This relation is called the *congruent modulo* n and denoted by $a\equiv b(\text{mod } n)$.

Def.5: If $\Re$ is an equivalence relation on a set X we define the *equivalence class* of an element $a\in X$ to be a set $C(a)=\{b\in X:(a,b)\in\Re\}$, the equivalence class of an element $a\in X$ may denoted by $[a]$ or $\bar{a}$.

The set of all equivalence classes of the relation $a\equiv b(\text{mod } n)$ is called the set of residue classes, and is denoted by $Z/n=\{\bar{0},\bar{1},\bar{2},...,\overline{n-1}\}$ (or by $Z_n=\{0,1,2,...,n-1\}$).

The set of residue classes of the equivalence relation on a set X form a partition of a set X.

Example: The equivalence classes of the relation $a\equiv b(\text{mod } 6)$ is:

$C(0)=\{...,-12,-6,0,6,12,...\}$, $C(1)=\{...,-11,-5,1,7,13,...\}$,

$C(2)=\{...,-10,-4,2,8,14,...\}$, $C(3)=\{...,-9,-3,3,9,15,...\}$,

$C(4)=\{...,-8,-2,4,10,16,...\}$, $C(5)=\{...,-7,-1,5,11,17,...\}$.

Proposition: The defining conditions (E1),(E2),(E3) of an equivalence relation $\Re$ are logically equivalent to the following two conditions:
(i) $a\Re a$. (ii) $a\Re b\wedge b\Re c\Rightarrow c\Re a$.

Proof: We prove (E1),(E2),(E3) $\Leftrightarrow$ (i),(ii):
Let (E1),(E2),(E3) hold. Then (E1) is the same (i), and
$a\Re b\wedge b\Re c\Rightarrow a\Re c\Rightarrow c\Re a$ i.e. (ii) hold. (from (E3),(E2))
Conversely, let (i),(ii) hold. Then (i) $\Rightarrow$ (E1), $a\Re b\Rightarrow a\Re b\wedge b\Re b\Rightarrow b\Re a$ i.e. (E2) hold. (from (i),(ii)) ,and
$a\Re b\wedge b\Re c\Rightarrow c\Re a\Rightarrow a\Re c$ i.e. (E3) hold. (from (ii),(E2)).

Exercises:

1- Let $X=\{0,1,2,3,4,5\}$. Define on X a relation $\Re$ by:

$(a,b)\in\Re \Leftrightarrow \frac{a-b}{3}\in Z \ \forall a,b\in X..$

Write $\Re$ as a set of ordered pairs ,Verify that $\Re$ is an equivalence relation, and characterize the equivalence classes.

2- Let $X=\{1,2,3\}$. Define on $P(X)$ a relation $\Re$ by:

$(A,B)\in\Re \Leftrightarrow O(A)=O(B) \ \forall A,B\in P(X)$.

Prove that $\Re$ is an equivalence relation, and characterize the equivalence classes.

3- Let $X=\{(a,b): a,b\in Z, b\neq 0\}$. Define on X a relation $\Re$ by:

$(a_1,b_1)\Re(a_2,b_2) \Leftrightarrow a_1b_2=b_1a_2 \ \forall (a_1,b_1),(a_2,b_2)\in X$.

Prove that $\Re$ is an equivalence relation, and characterize the equivalence classes.

Solved Problem: Let $\Re$ be an equivalence relation on a set S.

Show that for all $a,b\in S$:

(i) $b\in C(a)\Leftrightarrow a\in C(b)$

(ii) *either* $C(a)\cap C(b)=\phi$ *or* $C(a)=C(b)$

Proof:

(i) $b\in C(a)\Leftrightarrow b\in\{x\in S:(a,x)\in\Re\}$

$\Leftrightarrow (a,b)\in\Re$

$\Leftrightarrow (b,a)\in\Re$

$\Leftrightarrow a\in\{x\in S:(b,x)\in\Re\}$

$\Leftrightarrow a\in C(b).$

(ii) Suppose $C(a)\cap C(b)\neq\phi$,

let $x\in C(a)\cap C(b)\Leftrightarrow x\in C(a)\wedge x\in C(b)$

$\Leftrightarrow (a,x)\in\Re\wedge(b,x)\in\Re$

$\Leftrightarrow (a,x)\in\Re\wedge(x,b)\in\Re$

$\Leftrightarrow (a,b)\in\Re.$

let $y\in C(a)\Leftrightarrow (a,y)\in\Re,\ (a,b)\in\Re$

$\Leftrightarrow (b,a)\in\Re\wedge(a,y)\in\Re$

$\Leftrightarrow (b,y)\in\Re$

$\Leftrightarrow y\in C(b).$

$\therefore C(a)=C(b)$ *QED.*

(i.e. Two equivalence classes are either disjoint or identical).

3-Mappings:

Def.1: Given two non-empty sets A, B. A relation (or rule) f which associates with each element $a \in A$, a well-defined (or unique) element $b \in B$ is called a *mapping* (or function) from A into B.
It is denoted by $f : A \to B$ (or $A \xrightarrow{f} B$),the set A is called the *domain* of f, the set B is called the *co-domain* of f, and the set $f(A)$ is called the *range* of f.

- **Types of mappings:**

Def.2: A mapping $f : A \to B$ is called *onto* (or surjective) if each element of the co-domain B associates with element of the domain A (i.e., $f(A) = B$).
Def.3: A mapping $f : A \to B$ is called *1-1* (or injective) if $\forall a_1, a_2 \in A$, $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.
Def.4: A mapping $f : A \to B$ is called *1-1 corresponding* (or bijective) if it is both onto and 1-1.
Def.5: A mapping $f : A \to B$ is called *invertible* (or has inverse map $f^{-1} : B \to A$) if it is 1-1 corresponding.

- **Composition of mappings:**

Def.6: Given two mappings $f : A \to B$, $g : D \to C$; $f(A) \subseteq D$.
The *composite mapping* $g \circ f : A \to C$ is defined by:
$(g \circ f)(a) = g(f(a)) \ \forall a \in A$.
If $f : A \to B$, $g : B \to C$ the composite mapping $g \circ f : A \to C$ is always defined , and $f \circ g$ is defined only when $g(B) \subseteq A$, so it is not necessary $f \circ g = g \circ f$.

Examples:

1- If $f : R \to R$; $f(x) = x^2 \ \forall x \in R$ (R is the set of all real numbers), then the domain of f is R, also the co-domain of f is R, and the range of f is R^+ (is the set of all non-negative real numbers).
2- If $f : Z \to Z$; $f(x) = 2x - 1 \ \forall x \in Z$, then the domain of f is Z, also the co-domain of f is Z ,and the range of f is the set of all odd numbers, and we determine the type of f as follow:

(1) $y \in Z, y = f(x) \Rightarrow y = 2x-1 \Rightarrow x = \frac{y+1}{2} \notin Z$

$\therefore f$ is not onto.

(2) $\forall x_1, x_2 \in Z,\ f(x_1) = f(x_2) \Rightarrow 2x_1 - 1 = 2x_2 - 1 \Rightarrow x_1 = x_2$

$\therefore f$ is 1-1.

3- If $f : R \to R;\ f(x) = 2x+3\ \forall x \in R$, then

(1) $\forall y \in R, y = f(x) \Rightarrow y = 2x+3 \Rightarrow x = \frac{y-3}{2} \in R$

$\therefore f$ is onto.

(2) $\forall x_1, x_2 \in R,\ f(x_1) = f(x_2) \Rightarrow 2x_1 + 3 = 2x_2 + 3 \Rightarrow x_1 = x_2$

$\therefore f$ is 1-1.

From (1),(2) f is 1-1 corresponding, so f is invertible, and the inverse mapping is $f^{-1} : R \to R;\ f^{-1}(x) = \frac{x-3}{2}\ \forall x \in R$.

4- If $f, g : R \to R;\ f(x) = 2x-3, g(x) = x^2+3x+1\ \forall x \in R$, then:

$(f \circ g)(x) = f(g(x)) = f(x^2+3x+1) = 2(x^2+3x+1) - 3 = 2x^2 + 6x - 1,$

$(g \circ f)(x) = g(f(x)) = g(2x-3) = (2x-3)^2 + 3(2x-3) + 1 = 4x^2 - 6x + 1.$

Exercises:

1- Given the following relations $\Re_1, \Re_2, \Re_3, \Re_4$ on a set $A = \{1,2,3,4\}$. Explain in each case why the relation is or not a mapping, (determine the type of a mapping):

$\Re_1 = \{(1,3),(2,4),(1,1),(4,3),(4,4),(3,1)\},$

$\Re_2 = \{(2,4),(1,1),(3,1),(4,3)\},$

$\Re_3 = \{(2,3),(1,2),(3,4),(4,1)\},$

$\Re_4 = \{(1,4),(2,2),(3,2)\}.$

2- If $f : N \to N;\ f(n) = n+1\ \forall n \in N$.

(i) determine the domain, the co-domain, and the range of f.

(ii) Is f onto (1-1)?

3- Determine the type of each of the following mappings:

(i) $f : Z \to Z;\ f(x) = 2x+1\ \forall x \in Z$

(ii) $f : R \to R^+;\ f(x) = x + \sqrt{x^2+1}\ \forall x \in R$

(iii) $f : R \to R;\ f(x) = \begin{cases} \frac{x^2-1}{x} & \text{if } x \neq 0, \\ 0 & \text{otherwise.} \end{cases} \quad \forall x \in R.$

4- Determine each of the following mappings is invertible (define the inverse mapping for the invertible mappings):

(i) $f : N \to Z^+ \; ; \; f(n) = n - 1 \;\; \forall n \in N$

(ii) $f : R \to R \; ; \; f(x) = 2x - 3 \;\; \forall x \in R$

(iii) $f : Z \to Z \; ; \; f(x) = 2x \quad \forall x \in Z.$

5- If $f : R \to R \;\; , \; g : R \to R \; ; \; f(x) = 1 - x \; , \; g(x) = x^2 \;\; \forall x \in R$ compute $(f \circ g)(-1), (g \circ f)(4)$

Solved Problem: Let $f : A \to B \;\; , \; g : B \to C$ two mappings prove that:

(i) $g \circ f$ is onto if each of f and g is onto.

(ii) $g \circ f$ is 1-1 if each of f and g is 1-1.

Proof: (i) because each of f and g is onto, then

$$f(A) = B, g(B) = C,$$

$$\therefore (g \circ f)(A) = g(f(A)) = g(B) = C.$$

i.e. $g \circ f$ is onto.

(ii) because each of f and g is 1-1, then

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \;\; \forall a_1, a_2 \in A,$$

$$g(b_1) = g(b_2) \Rightarrow b_1 = b_2 \;\; \forall b_1, b_2 \in B.$$

$$\therefore (g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow g(f(a_1)) = g(f(a_2))$$

$$\Rightarrow f(a_1) = f(a_2)$$

$$\Rightarrow a_1 = a_2 \quad \forall \; a_1, a_2 \in A.$$

i.e. $g \circ f$ is 1-1.

4-Binary Operations:

Def.1: A mapping $b: A\times A\to A$; $b(x,y)=z\in A\ \forall (x,y)\in A\times A$ is called a *binary operation* on a set A.
We use symbols such as $*,\circ,\#,\oplus,\otimes,...etc$ for a binary operations.

Def.2: A binary operation $*$ on a set A is called *associative* if: $(x*y)*z=x*(y*z)\ \forall x,y,z\in A$, and it is called *commutative* if: $x*y=y*x\ \forall x,y\in A$.

Def.3: If $*$ is a binary operation on a set A, the element $e\in A$ is called the *identity element* w.r.t. $*$ if: $x*e=e*x=x\ \forall x\in A$,
and the element $y\in A$ is called the *inverse* of the element $x\in A$ w.r.t. $*$ if: $x*y=y*x=e$.

Examples:

1- If $*,\otimes$ defined on a set of all nature numbers N by:
$a*b=a^b, a\otimes b=a+b-2a^2b^2\ \forall a,b\in N$.
Then $*$ is a binary operation on N, because $a*b=a^b\in N\ \forall a,b\in N$, but $\otimes$ is not binary operation on N because,
$a\otimes b=a+b-2a^2b^2\notin N\ \forall a,b\in N$ (for example put $a=1,b=2$).

2- If $*$ defined on a set of integers Z by:
$x*y=x+y-3\ \forall x,y\in Z$.
(i) Is $*$ binary operation on Z?
(ii) Is $*$ commutative? Is it associative?
(iii) Does $*$ have an identity? Is exist an inverse w.r.t. $*$?
(Give reasons for your answer).

The Answer:
(i) $*$ is binary operation on Z because,
$x*y=x+y-3\in Z\ \forall x,y\in Z$
(ii) $x*y=x+y-3=y+x-3=y*x\ \forall x,y\in Z$, i.e. $*$ commutative,
$(x*y)*z=(x+y-3)*z=(x+y-3)+z-3=x+y+z-6,$
$x*(y*z)=x*(y+z-3)=x+(y+z-3)-3=x+y+z-6.$
$\therefore (x*y)*z=x*(y*z)\ \forall x,y,z\in Z$, i.e. $*$ associative.
(iii) Let $x*e=e*x=x\ \forall x\in Z$
$\therefore x+e-3=e+x-3=x\Rightarrow e=3\in Z$
i.e. $*$ have an identity $e=3$,
let $x*y=y*x=e\ \forall x,y\in Z$
$\therefore x+y-3=y+x-3=3\Rightarrow y=6-x\in Z$
i.e. $\exists$ an inverse of $x\in Z$ is $6-x\in Z$ w.r.t. $*$

3- If $\otimes$ defined on a set $X = R - \{1\}$; R is the set of real numbers by:

$x \otimes y = x + y - xy \ \forall x, y \in X$.

(i) Is $\otimes$ binary operation on X ?

(ii) Is $\otimes$ commutative? Is it associative?

(iii) Does $\otimes$ have an identity? Is exist an inverse w.r.t. $\otimes$?

(Give reasons for your answer).

- **Representation by tables:**

If $X = \{-1,0,1\}$ we can represent the ordinary operations "$+$" and "$\times$" on X by the following tables:

$+$	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

$\times$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

As it can be seen from the tables above:

If all elements in a table belongs to a set X , the operation is a binary operation on a set X , and if all elements in a table are symmetric around the diameter of the table , a binary operation is commutative. Otherwise it is not.

So, "$\times$" is a commutative binary operation on X , but "$+$" is not binary operation on X .

Remark: Only an operation defined on a finite set can be represented by table.

Exercise: If $*$ defined on a set $X = \{0,1,2,3,4\}$ by:

$$x * y = \begin{cases} x + y & if\ x + y < 5, \\ (x + y) - 5 & if\ x + y \geq 5 \end{cases} \quad \forall x, y \in X..$$

(i) Represent $*$ by table.

(ii) Is $*$ binary operation on X ?

(iii) Is $*$ commutative? Is it associative?

(iv) Does $*$ have an identity? Is exist an inverse w.r.t. $*$?

(Give reasons for your answer).

w.r.t. means: with respect to

- **Addition & Multiplication mod n:**

We define addition and multiplication on $Z_n = \{0,1,2,...,n-1\}$
(Z_n is a set of all equivalence classes of the equivalence relation $a \equiv b(\text{mod } n)$) as follows:

$a \oplus_n b$ is the remainder of $\frac{a+b}{n}$ $\quad \forall a,b \in Z_n$,

$a \otimes_n b$ is the remainder of $\frac{a \times b}{n}$ $\quad \forall a,b \in Z_n$.

Example: we represent the two operations $\oplus_4$ and $\otimes_4$ on $Z_4 = \{0,1,2,3\}$ by the following tables:

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exercises:

1- In each of the following $*$ is the specified binary operation on the set Z of integers.
Determine in each case whether the operation is commutative, whether is associative , whether there is an identity for the operation , and whether there is an inverse w.r.t. the operation?

(i) $a * b = b$
(ii) $a * b = a + b + ab$
(iii) $a * b = 2a + 2b$
(iv) $a * b = a + b - 1$
(v) $a * b = a + ab$

2- Let $P(X)$ be the power set of a set $X = \{1,2\}$.

(i) Is the binary operation $\cap$ on $P(X)$ commutative?
Is it associative? Does it have an identity?.
(ii) Answer the same questions for the binary operation $\cup$ on $P(X)$.
(iii) Answer the same questions for the binary operation Δ on $P(X)$ (where $A \Delta B = (A \cup B) - (A \cap B)$ $\forall A, B \in P(X)$).

5-Groups:

Def.1: Let G be non-empty set, and $*$ binary operation on G.
The couple $<G,*>$ is said to be a *group* if the following conditions are satisfied:

(G1) $a*b \in G \ \forall a,b \in G$ (closure).

(G2) $(a*b)*c = a*(b*c) \ \forall a,b,c \in G$ (associative).

(G3) $\exists e \in G;\ a*e = e*a = a \ \forall a \in G$ (existence of identity).

(G4) $\forall a \in G \ \exists a^{-1} \in G;\ a*a^{-1} = a^{-1}*a = e$ (existence of inverse).

If only the condition (G1) is satisfied, $<G,*>$ is said to be *groupoid* , if only the two conditions (G1),(G2) are satisfied, $<G,*>$ is said to be *semi-group*, and if only the three conditions (G1),(G2),(G3) are satisfied, $<G,*>$ is said to be *monoid*.

Def.2: A group $<G,*>$ is said to be *commutative* (or *abelian*) if it satisfies the commutative law: $a*b = b*a \ \forall a,b \in G$.

Def.3: By the order of a group $<G,*>$ we mean the number of its distinct elements, and denoted $O(G)$ (or $|G|$).

A group $<G,*>$ is said to be finite if its order is finite, and is said to be infinite if its order is infinite.

Remark: We write G instead of $<G,*>$ when a binary operation $*$ is the usual multiplication.

Examples:

1- Each of the following sets with the usual definition of addition of numbers is a group:

Z the set of all integers.

Q the set of all rational numbers.

R the set of all real numbers.

C the set of all complex numbers.

2- Each of the following sets with the usual definition of multiplication of numbers is a group:

Q^+ the set of all positive rational numbers.

R^+ the set of all positive real numbers.

$Q^* = Q - \{0\}$.

$R^* = R - \{0\}$.

$C^* = C - \{0\}$.

3- $< Z_n, \oplus_n >$ is abelian group ; $Z_n = \{0,1,2,...,n-1\}$ is the set of residue classes, and $\oplus_n$ the addition of residue classes.

The identity of this group is the residue class 0 and the inverse of any class a; $0 < a < n-1$ is the class $n-a$.

If $n = 4$ **we prove that** $< Z_4, \oplus_4 >$ **is abelian group as follows:**

We represent $< Z_4, \oplus_4 >$ by the following table:

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(G1) $\oplus_4$ is a binary operation on Z_4 as it can be seen from the table above.

(G2) Associative law holds in general for the two operations $\oplus_n, \otimes_n$ on Z_n. So $\oplus_4$ is associative on Z_4 .

(G3) 0 is the identity as it can be seen from the table above.

(G4)

The element	0	1	2	3
The inverse	0	3	2	1

$\oplus_4$ is commutative as it can be seen from the table above.

$\therefore < Z_4, \oplus_4 >$ is abelian group.

4- $< A, \times >$ is abelian group ; $A = \{a : a = 3^n, n \in Z\}$, and $\times$ the usual multiplication of numbers.

The identity of this group is $3^0 = 1$, and the inverse of any element 3^n is 3^{-n}.

5- $< M(A), \circ >$ is a group ; $M(A)$ is the set of all 1-1 corresponding mappings from A to A, and $\circ$ the composition of mappings.

The identity of this group is the identity mapping $I : A \to A; I(a) = a$ $\forall a \in A$, and the inverse of any mapping $f \in M(A)$ is the mapping $f^{-1} \in M(A); f \circ f^{-1} = f^{-1} \circ f = I$.

This group is not commutative, because in general $f \circ g \neq g \circ f$.

Properties: Let $< G,* >$ be a group. The following properties are satisfied:

(1) The identity element e is unique. For, if e_1, e_2 are two identities in $< G,* >$, then $e_1 * e_2 = e_1 = e_2$.

(2) The inverse element a^{-1} is unique. For, if b, c are two inverses of a, then $b*a = e, a*c = e,\ b = b*e = b*(a*c) = (b*a)*c = e*c = c$.

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

(4) $a * x = a * y \Rightarrow x = y,\ \ x * a = y * a \Rightarrow x = y$ (cancellation laws).

Proof: For $a * x = a * y \Rightarrow x = y$.

$$a * x = a * y \Rightarrow a^{-1} * (a * x) = a^{-1} * (a * y)$$
$$\Rightarrow (a^{-1} * a) * x = (a^{-1} * a) * y$$
$$\Rightarrow e * x = e * y$$
$$\Rightarrow x = y.$$

Similarly, for $x * a = y * a \Rightarrow x = y$.

(5) The equations $a * x = b$ and $y * a = b$ have unique solutions $x = a^{-1} * b$ and $y = b * a^{-1}$ in $< G,* >$.

Proof: For the equation $a * x = b$.

$L.H.S. = a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b = R.H.S.$,

let x_1, x_2 are two solutions of the equation $a * x = b$, then

$a * x_1 = b,\ a * x_2 = b,\ \therefore a * x_1 = a * x_2 \Rightarrow x_1 = x_2$

i.e. the solution is unique. Similarly, for the equation $y * a = b$.

Examples: The solution of the equation $2x = 3$ in a group $< Z_4, \oplus_4 >$ is $2 \oplus_4 x = 3 \Rightarrow x = 2^{-1} \oplus_4 3 = 2 \oplus_4 3 = 1$,

and the solution of the equation $5x = -2$ in a group $< Z,* >$;

Z the set of integers, $a * b = a + b - 3\ \ \forall a, b \in Z$

is $5 * x = -2 \Rightarrow x = 5^{-1} * (-2) = (6-5) * (-2) = 1 * (-2) = 1 + (-2) - 3 = -4$

(Verify that?).

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

Proof:

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

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

Similarly, we can prove that $(b^{-1} * a^{-1}) * (a * b) = e$,

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

(7) $a^n = a * a * ... * a \ \ (n \ times)$, $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} \ \ (n \ times)$,

$a^n * a^m = a^{n+m}$, $(a^n)^m = a^{nm}$.

Remark: In the additive group $< G,+ >$,

$na = a + a + ... + a \ \ (n \ times)$, $-na = (-a) + (-a) + ... + (-a) \ \ (n \ times)$,

$(n+m)a = na + ma$, $n(ma) = (nm)a$.

Exercises:

1- Which of the following is group? Give reasons for your assertion.

(i) $< Z,\times >$; Z the set of integers.

(ii) $< Z,- >$; Z the set of integers.

(iii) $< Z_E,+ >$; Z_E the set of all even integers.

(iv) $< Z,* >$; Z the set of integers, $a * b = a + b + 1$.

(v) $< R,* >$; R the set of all real numbers, $a * b = a + b - 5$.

(vi) $< A,\times > ; A = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} : i^2 = -1\}$.

(vii) $< A,\times > ; A = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\}$.

(viii) $< A,\times > ; A = \{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in R, xy = 1\}$.

(ix) $< A,\times > ; A = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in R, x^2 + y^2 \neq 0\}$.

2- Let $X = R - \{1\}$, $a * b = a + b - ab \ \ \forall a,b \in X$ .Verify that $< X,* >$ is abelian group, and determine the solution of the equation $3x = 5$ in this group.

3- In a group $< G,* >$ what is the element $(a * b^{-1} * c^{-1})^{-1}$ equal to?

4- Show that a group $< G,* >$ is commutative if $x^2 = e \ \ \forall x \in G$.

5- Show that a group $< G,* >$ is commutative if:

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

6- Show that a group $< G,* >$ of order 3 is abelian? .

7- Show that a group G is abelian iff $(ab)^2 = a^2 b^2 \ \ \forall a,b \in G$.

8- If G is an abelian group, Prove that: $(ab)^n = a^n b^n \ \forall a,b \in G, n \in Z^+$ (Hint: use the mathematical induction).

6-Special types of groups:

1- Group of Permutations:

Def.1: A 1-1 mapping of a finite set $S=\{1,2,3,...,n\}$ onto itself is said to be *permutation* of degree n.

If α is a permutation of a set $S=\{1,2,3,...,n\}$, we write:

$$\alpha=\begin{pmatrix}1 & 2 & 3 & ..... & n\\ \alpha(1) & \alpha(2) & \alpha(3) & ..... & \alpha(n)\end{pmatrix}=\begin{pmatrix}i\\ \alpha(i)\end{pmatrix};1\le i\le n.$$

Example: If α,β,γ are permutations of a set $S=\{1,2,3,4\}$,

$$\alpha=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\beta=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\gamma=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}.$$

α,β,γ can represented by:

$$\alpha=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}=\begin{pmatrix}2&3&4&1\\2&1&4&3\end{pmatrix}=\begin{pmatrix}3&4&1&2\\1&4&3&2\end{pmatrix}=\begin{pmatrix}4&1&2&3\\4&3&2&1\end{pmatrix}$$

$$=(1\ 3)(2)(4)=(1\ 3),$$

$$\beta=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1\ 4\ 3\ 2),\quad \gamma=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4).$$

Each of a representations $(1\ 3),(1\ 4\ 3\ 2),(1\ 3)(2\ 4)$ is said to be a *cycle representation* of a permutation.

The *composition of the two permutations* α,β is defined as follow:

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

and the inverse of a permutation β is defined as follow:

$$\beta^{-1}=\begin{pmatrix}4&1&2&3\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1\ 2\ 3\ 4).,$$

and the permutation $I=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ is the identity.

We say that there is an inversion in a permutation

$\alpha=\begin{pmatrix}1 & 2 & 3 & ..... & n\\ \alpha(1) & \alpha(2) & \alpha(3) & ..... & \alpha(n)\end{pmatrix}$, if for $i<j$ we have:

$\dfrac{\alpha(i)-\alpha(j)}{i-j}<0$ or, in other words, when a bigger number precedes a smaller number in α, and the total number of inversions in α is denoted by V_α.

Def.2: A permutation is called *even (odd) permutation* if the number of its inversions is even (odd).

Examples:

1- The number of inversions in a permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ is $V_\alpha = 2+1+0+0 = 3$ (odd), so it is odd,

the number of inversions in a permutation $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ is $V_\beta = 3+0+0+0 = 3$(odd), so it is also odd, and the number of inversions in a permutation $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ is $V_\gamma = 2+2+0+0 = 4$ (even), so it is even.

2- A permutation:

$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$ is odd;

$V_\rho = 3+3+1+4+1+1+0+0 = 13$ (odd).

Def.3: A set of all permutations of a finite set $S = \{1,2,3,...,n\}$ with the operation of a composition form a group of order $n!$, it is called a *group of permutations* (or substitution) of degree n, and it is denoted by P_n (or S_n).

Example: A set S_3 of all permutations of a finite set $S = \{1,2,3\}$ with the operation of a composition form a group of order 6,

$S_3 = \{I, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$

(Verify that? Hint: represent $< S_3, \circ >$ by table).

Remarks:

(1) The identity permutation I is an even permutation.

(2) The composition of two even permutations is even permutation, also the composition of two odd permutations is even permutation, and the composition of two permutations one of them even and the other odd is odd permutation,

(3) There are an equal number of even and odd permutations in a group S_n.

Exercises:

1- Given a permutations:

$$\alpha=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix},\beta=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix},\gamma=\begin{pmatrix}1&2&3&4&5&6\\5&2&4&3&1&6\end{pmatrix}.$$

(i) Write each of α,β,γ by a cycle representation.

(ii) Compute $\alpha\circ\beta,\ \alpha^2\circ\beta,\ \alpha\circ\gamma\circ\alpha^{-1}$

2- Determine which of the following is even (odd) permutation:

(i) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&6&9&7&2&5&8&1&3\end{pmatrix}$.

(ii) $(1\ 2\ 3)\circ(2\ 4\ 6)\circ(5\ 4\ 3\ 2)$.

3- Verify that $<S_3^+,\circ>;S_3^+$ is the set of all even permutations of degree 3 is an abelian group, but $<S_3^-,\circ>;S_3^-$ is the set of all odd permutations of degree 3 is not a group?.

4- Verify that $<X,\circ>;$

$X=\{I,(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2)\}\subset S_4$

is an abelian group?.

2- Cyclic Groups:

Def.1: We say that G is a *cyclic group* if it is generated by at least one of its elements , say $a\in G$, i.e. $\forall x\in G\exists n\in Z;\ x=a^n$

(or $\forall x\in G\exists n\in Z;\ x=na$ when G is an additive group), and we denote $G=<a>$.

Examples:

1- $<Z,+>$ is cyclic group generated by $1,-1$ .For,

(G1) $a+b\in Z\ \ \forall a,b\in Z$.

(G2) $(a+b)+c=a+(b+c)\ \ \forall a,b,c\in Z$.

(G3) $\exists 0\in Z;0+a=a+0=a\ \ \forall a\in Z$.

(G4) $\forall a\in Z\ \exists -a\in Z;(-a)+a=a+(-a)=0$.

$\therefore <Z,+>$ is a group,

$0(1)=0,1(1)=1,(-1)(1)=-1,2(1)=2,(-2)(1)=-2,...$ and so on,

$0(-1)=0,1(-1)=-1,(-1)(-1)=1,2(-1)=-2,(-2)(-1)=2,...$ and so on.

$\therefore <Z,+>$ is cyclic group generated by $1,-1$.

2- $< G,\times >; G=\{1,-1,i,-i\}, i=\sqrt{-1}$ is cyclic group generated by $i,-i$
For, the table of $< G,\times >$ is:

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

(G1) $\times$ is a binary operation on G as it can be seen from the table above.
(G2) Associative law holds in general for $\times$.
(G3) 1 is the identity.
(G4)

The element	1	-1	i	-i
The inverse	1	-1	-i	i

$\therefore G$ is a group,
$i^1=i, i^2=-1, i^3=-i, i^4=1 \ \therefore G=< i >$
$(-i)^1=-i, (-i)^2=-1, (-i)^3=i, (-i)^4=1 \ \therefore G=< -i >$

3- $< Z_3, \oplus_3 >$ is cyclic group generated by $1, 2$ (verify that?).

4- $< Z_7-\{0\}, \otimes_7 >$ is cyclic group generated by $3,5$ (verify that?).

5- $< X, \circ >; X=\{I, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} \subset S_4$
is cyclic group generated by $(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)$ (verify that?).

Remarks:

(1) The generator of a cyclic group is not unique. For example, the additive group $< Z,+ >$ is cyclic group generated by $1,-1$.

(2) Every cyclic group is abelian.
Proof: Let $G=< a >$ and let $g_1, g_2 \in G; g_1=a^r, g_2=a^s, r,s \in Z$
$\therefore g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1.$

(3) When $G=< a >$ is of finite order, say n, then the distinct elements of G are: $e=a^0, a, a^2, a^3, ..., a^{n-1}, a^n=e$. For, in this case, all powers of a can not be different, so we must have:
$a^h=a^k; h,k \in Z, h \neq k$. If $h>k$ then $a^{h-k}=e$.

(4) When $G=< a >$ is of infinite order, then the elements of G are:
$e=a^0, a^{\pm 1}, a^{\pm 2}, ..., a^{\pm n}, ...$.

Def.2: By the order (or period) of an element a of a group G, we mean the least positive integer m such that $a^m = e$.
The order of all elements in a group $< \{1,-1,i,-i\}, \times >$ is:

The element	1	-1	i	-i
The order	1	2	4	4

Theorem: Given $G =< a >$ a cyclic group of order n. An element a^m for $1 \le m < n$ is a generator of G iff $(m,n) = 1$.

Proof:

Let $G =< a^m >$. Then $a = (a^m)^\alpha ; \alpha \in Z$,

i.e. $a^1 = a^{\alpha m} \Rightarrow a^{1-\alpha m} = a^0 = e = e^\beta = (a^n)^\beta = a^{\beta n} ; \beta \in Z$

$\therefore 1 - \alpha m = \beta n \Rightarrow \alpha m + \beta n = 1$

i.e. $(m,n) = 1$.

Conversely, let $(m,n) = 1$. Then $\exists \alpha, \beta \in Z ; \alpha m + \beta n = 1$,

$\therefore a = a^1 = a^{\alpha m + \beta n} = a^{\alpha m} a^{\beta n} = (a^m)^\alpha (a^n)^\beta = (a^m)^\alpha (e)^\beta = (a^m)^\alpha e = (a^m)^\alpha$

i.e. $G =< a^m >$.

Example: A group $< G, \times >; G = \{1 = \omega^8, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$ of order 8 is cyclic group; $G =< \omega >$, the other generators of this group are $\omega^3, \omega^5, \omega^7$ such that $(3,8) = 1, (5,8) = 1, (7,8) = 1$.

Exercises:

1- Give an example to prove or disprove the following statements:
(i) Every abelian group is cyclic.
(ii) If $G =< a >$ cyclic group. Then $G =< a^{-1} >$.
(iii) Every element of a cyclic group generates the group.

2- Determine the order of all elements in a group $< S_3, \circ >$.
Is $< S_3, \circ >$ cyclic group?.

3- Find the generators of the cyclic group $G =< a >$ of orders $7, 10$ and 21.

7-Subgroups:

Def.1: A non-empty subset H of a group G is said to be a *subgroup* of G, if H itself is a group w.r.t. the same binary operation in G.
The fact that H is a subgroup of G will be denoted by $H \leq G$.
Every group G has two *improper subgroups*, namely, G itself and $\{e\}$, and any subgroup other than G and $\{e\}$ is called *proper sub- group*.

Examples:

1- The set Z_E of all even integers forms a subgroup w.r.t. addition in the additive group Z of all integers.

2- The set Q of all rational numbers is a group w.r.t. addition, and the set Q^+ of all positive rational numbers is a group w.r.t. multiplication.
Although Q^+ is a subset of Q; we can not consider Q^+ as a subgroup of Q, since the binary operations in Q and Q^+ are different.

3- If $< G,\times >; G = \{1,-1,i,-i\}, < H_1,\times >; H_1 = \{1,-1\}, < H_2,\times >; H_2 = \{i,-i\}$
Then $H_1 \leq G$, but H_2 is not subgroup of a group G, since $< H_2,\times >$ is not a group.

Theorem1: A non-empty subset H of a group G is a subgroup of G iff the following two conditions are satisfied:

(i) $\forall a,b \in H \Rightarrow ab \in H.$

(ii) $\forall a \in H \Rightarrow a^{-1} \in H.$

Proof: Suppose the conditions (i) and (ii) hold in H. Then
by (i) H closed w.r.t. multiplication in G i.e. (G1).
The associative law holds in H, since it holds in G i.e. (G2).
Since $H \neq \phi$, let $a \in H$, then by (ii) $a^{-1} \in H$ i.e. (G4).
And by (i) we get $aa^{-1} = a^{-1}a = e \in H$ i.e. (G3).
Thus H is a group w.r.t. multiplication in G, i.e. $H \leq G$.
The conditions are therefore sufficient.
Conversely, let H is a subgroup of G, the conditions (i),(ii) then follow from the group conditions in H. Hence the conditions are necessary.

Theorem2: A non-empty subset H of a group G is a subgroup of G iff $\forall a,b \in H \Rightarrow ab^{-1} \in H$.

Proof: Let H is a subgroup of G. Then:

$\forall a,b \in H \Rightarrow a^{-1}, b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Conversely, let $\forall a,b \in H \Rightarrow ab^{-1} \in H$. Since $H \neq \phi$, let $a \in H$, then

$\forall a \in H \Rightarrow aa^{-1} = e \in H$ i.e.(G3), $\forall e,a \in H \Rightarrow ea^{-1} = a^{-1} \in H$ i.e.(G4),

$\forall a,b \in H \Rightarrow a,b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$ i.e.(G1),

and the associative law holds in H, since it holds in G i.e.(G2).

Thus H is a group w.r.t. multiplication in G, i.e. $H \leq G$.

Theorem3: Let $H_1 \leq G$, $H_2 \leq G$. Then $H_1 \cap H_2 \leq G$, but is not necessary to be $H_1 \cup H_2 \leq G$.

Proof:

$$\begin{aligned} \forall a,b \in H_1 \cap H_2 &\Rightarrow a,b \in H_1 \wedge a,b \in H_2 \\ &\Rightarrow ab^{-1} \in H_1 \wedge ab^{-1} \in H_2 \\ &\Rightarrow ab^{-1} \in H_1 \cap H_2 \\ &\Rightarrow H_1 \cap H_2 \leq G. \end{aligned}$$ (From Theorem2)

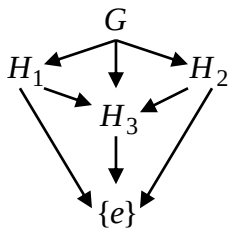
For, is not necessary to be $H_1 \cup H_2 \leq G$ we give an example:

$H_1 = \{I,(1\ 2)\}$, $H_2 = \{I,(1\ 3)\}$ are two subgroups of a group of permutations S_3, but $H_1 \cup H_2 = \{I,(1\ 2),(1\ 3)\}$ is not group (verify that?).

- **Lattice diagram of a sub-groups:**

Let H_1, H_2, H_3 are proper subgroups of a group G, and H_3 is proper subgroup of a group H_1 and of a group H_2.

Then we can represent the set of all subgroups H_1, H_2, H_3 and the two improper subgroups $G, \{e\}$ by the following lattice diagram:

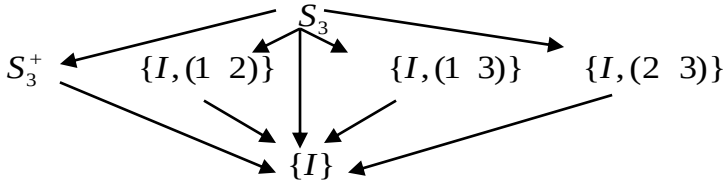


Solved Problem: List all the subgroups of a group S_3 and represent it by lattice diagram.

The Answer: The proper subgroups of S_3 are:

$S_3^+, \{I,(1\ 2)\}, \{I,(1\ 3)\}, \{I,(2\ 3)\}$, and the two improper subgroups of S_3 are: $S_3, \{I\}$. Thus the set of all subgroups of a group S_3 is:

$\{S_3^+, \{I,(1\ 2)\}, \{I,(1\ 3)\}, \{I,(2\ 3)\}, S_3, \{I\}\}$ and it represented by the following lattice diagram:



- **Decomposition of a group:**

Def.1: Let H be a subgroup of a group G and $a \in G$.

The set $aH = \{ah : h \in H\}$ is called a *left coset* of H in G generated by a.

Similarly, the set $Ha = \{ha : h \in H\}$ is called a *right coset* of H in G generated by a.

Examples:

1- The left coset and the right coset of a subgroup $H = \{1,-1\}$ in a group $G = <\{1,-1,i,-i\},\times>$ generated by $i \in G$ are:

$$iH = \{i\times 1, i\times(-1)\} = \{i,-i\},$$

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

2- The left coset of a subgroup S_3^+ in a group $< S_3, \circ >$ generated by $(1\ 2) \in S_3$ is:

$$(1\ 2)S_3^+ = \{(1\ 2)\circ I, (1\ 2)\circ(1\ 2\ 3), (1\ 2)\circ(1\ 3\ 2)\}$$
$$= \{(1\ 2), (2\ 3), (1\ 3)\}.$$

and the right coset of a subgroup S_3^+ in a group $< S_3, \circ >$ generated by $(1\ 2\ 3) \in S_3$ is:

$$S_3^+(1\ 2\ 3) = \{I\circ(1\ 2\ 3), (1\ 2\ 3)\circ(1\ 2\ 3), (1\ 3\ 2)\circ(1\ 2\ 3)\}$$
$$= \{(1\ 2\ 3), (1\ 3\ 2), I\}.$$

Proposition1: Every subgroup of an abelian group is abelian, but the converse is not true in general

(e.g. $S_3^+ \le S_3$, S_3^+ is abelian but S_3 is not abelian).

Proposition2: If $H \le G$ then the identity element in H is the same identity element in G , and the inverse of an element in H is the same inverse in G .

Proposition3: Two left cosets of a subgroup H in a group G are either disjoint or identical.

Proof: Suppose $aH \cap bH \neq \phi$ and let

$c \in aH \cap bH \Rightarrow c = ah_i = bh_j \ ; h_i, h_j \in H$,

$a = c(h_i)^{-1} = (bh_j)(h_i)^{-1} = bh_k \ ; (h_j)(h_i)^{-1} = h_k \in H$,

$\therefore aH = (bh_k)H = b(h_k H) = bH.$

Lagrange's Theorem: Let H be a subgroup of a finite group G . Then the order of H is a factor of the order of G .

Proof: Let G be a finite group of order n and H be a subgroup of G of order m . Suppose $eH, a_1H, a_2H, ..., a_{l-1}H$ be the left cosets of a subgroup H in a group G . Then $ah_1, ah_2, ..., ah_m$ are the distinct elements of aH ,

$$\therefore O(G) = O(eH) + O(a_1H) + ... + O(a_{l-1}H)$$
$$= O(H) + O(H) + ... + O(H). \quad (l - times)$$

$\therefore n = lm.$

Remark: The reverse of Lagrange's Theorem is not true in general. For example $O(S_4^+) = 12$ (S_4^+ is the group of all even permutations of degree 4), but there is no subgroup of S_4^+ of order 6 .

Def.2: The number of left (or right) cosets of H in G is called the index of H in G . It is denoted by $(G:H)$ (i.e. $(G:H) = \frac{O(G)}{O(H)}$).

Corollary.1: A finite group of prime order has no proper subgroup.

Corollary.2: The order of an element of a finite group is a factor of the order of the group.

Corollary.3: Every finite group of prime order is cyclic.

Corollary.4: The number of all subgroups of a finite cyclic group G is equal to the number of a positive factors of the order of G .

Example: $< Z_{12}, \oplus_{12} >$ is a cyclic group (verify that?), $O(Z_{12}) = 12$, and the positive factors of 12 are 1,2,3,4,6,12 Thus the number of all subgroups of $< Z_{12}, \oplus_{12} >$ is 6

(It is $<1>, <2>, <3>, <4>, <6>, <0>$)

Exercises:

1- Verify that $aH = Ha = H$, $bH \neq Hb$, for $H = \{I, (1\ 2)\}$, $a = (1\ 2), b = (1\ 3) \in S_3$

2- Determine all subgroups of a group $< G = Z_9 - \{0,3,6\}, \otimes_9 >$, and represent it by lattice diagram.

- **Normal subgroups, Simple groups, and Factor groups:**

Def.1: A subgroup H of a group G is called a *normal subgroup* (or invariant subgroup or self-conjugate subgroup) of G if:

$aH = Ha \ \ \forall a \in G$.

i.e. if the left and right decompositions of G w.r.t. H are identical.

The fact that H is a normal subgroup of a group G will be denoted by $H \Delta G$

Def.2: An element aHa^{-1} where $a \in G$ and $h \in H$ is called a *conjugate* of h in G.

The defining condition of a normal subgroup can be replaced by a weaker condition:

$aHa^{-1} \subseteq H \ \ \forall a \in G$.

Def.3: A group which has no proper normal subgroup is said to be *simple group*.

Examples:

1- A subgroup $\{I, (1\ 2)\}$ is simple , but it is not normal subgroup of a group S_3 (verify that?).

2- A subgroup $H = \{1, -1\}$ is simple , and it is normal subgroup of a group $G = \{1, -1, i, -i\}$ w.r.t. $\times$ (verify that?).

3- A subgroup S_3^+ is a normal subgroup of a group S_3 (verify that?) Is it simple?.

4- $< Z_4, \oplus_4 >$ is not simple group, also $< Z, + >$ is not simple group (verify that?).

Given a group G and $H \Delta G$. Let Γ be the set of all cosets of H in G. We define in Γ a multiplication operation as follows:
$(Ha)(Hb) = H(ab) \ \forall Ha, Hb \in \Gamma$.
The associativity in Γ is assured by the associativity in G.
The coset $He = H$ is the identity in Γ.
Every coset Ha in Γ has Ha^{-1} as its inverse.
So, the set Γ of all cosets of H in G forms a group w.r.t. the above definition of multiplication of cosets. It is called the *factor group* (or the *quotient group*), and it is denoted by G/H.

Example: Let $G =< a >$ be a cyclic group of order 10.
To determine the factor groups of G by Lagrange's theorem, if G has any subgroups, then it would be of order $1,2,5,10$.
Being cyclic, G is abelian and so every subgroup of it is normal.
The two improper subgroups are:
$G = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$, $E = \{e\}$.
The two proper subgroups are:
$H = \{e, a^5\}$ of order 2 and $K = \{e, a^2, a^4, a^6, a^8\}$ of order 5
Therefore,
$G/G = \{[G]\}$, $G/E = \{[e], [a], [a^2], [a^3], [a^4], [a^5], [a^6], [a^7], [a^8], [a^9]\}$
are factor groups of order 1 and 10 respectively. Also,
$G/H = \{H, aH, a^2H, a^3H, a^4H\} = \{[e, a^5], [a, a^6], [a^2, a^7], [a^3, a^8], [a^4, a^9]\}$
and $G/K = \{K, aK\} = \{[e, a^2, a^4, a^6, a^8], [a, a^3, a^5, a^7, a^9]\}$.

8-Homomorphism and Isomorphism between groups:

Def.1: A mapping $f: G_1 \to G_2$ where $< G_1, * >, < G_2, \# >$ two groups is said to be a *homomorphism* if: $f(a*b) = f(a) \# f(b) \ \forall a,b \in G_1$.
If $G_1 = G_2$ f is called an *endomorphism*, a 1-1 homomorphism is called *monomorphism*, and an onto homomorphism is called an *epiomorphism* .

Examples:

1- A mapping $f :< R, + > \to < X, \times >$; R the set of all real numbers, $X = R - \{0\}$, $f(n) = 3^n$ is a homomorphism. For:
$f(m+n) = 3^{m+n} = 3^m \times 3^n = f(m) \times f(n) \ \forall m,n \in R$.

2- A mapping $f :< Z, + > \to < Z, + >$; Z the set of integers , $f(n) = n+1$ is not homomorphism. For: $f(m+n) \neq f(m) + f(n) \ \forall m,n \in Z$ (verify that?).

3- A mapping $f :< Z, + > \to < A, \times >$; $A = \{1, -1, i, -i\}$,
$f(n) = \begin{cases} 1 & \text{if } n \text{ even}, \\ -1 & \text{if } n \text{ odd}. \end{cases}$ is a homomorphism. For:
let $m,n \in Z$, we have the following three cases:

(1) If each of m,n even number, then $m+n$ is even,
$\therefore f(m) = f(n) = 1$, $f(m+n) = 1 = 1 \times 1 = f(m) \times f(n)$.

(2) If each of m,n odd number, then $m+n$ is even,
$f(m) = f(n) = -1$, $f(m+n) = 1 = (-1) \times (-1) = f(m) \times f(n)$.

(3) If one of m,n even and the other odd, then $m+n$ is odd,
$\therefore f(m) = 1, f(n) = -1 \vee f(m) = -1, f(n) = 1$,
$f(m+n) = -1 = 1 \times (-1) = f(m) \times f(n)$,
$f(m+n) = -1 = (-1) \times 1 = f(m) \times f(n)$.

i.e. $f(m+n) = f(m) \times f(n) \ \forall m,n \in Z$. So, f is a homomorphism.

4- A mapping $g :< Z, + > \to < A, \times >$; Z the set of integers , $A = \{1, -1, i, -i\}$, $g(n) = \begin{cases} -1 & \text{if } n \text{ even}, \\ 1 & \text{if } n \text{ odd}. \end{cases}$ is not homomorphism. For:
$2,4 \in Z$, we have $g(2) = g(4) = -1$, $g(2+4) = g(6) = -1$,
$g(2) \times g(4) = (-1) \times (-1) = 1 \ \therefore g(2+4) \neq g(2) \times g(4)$.

5- A mapping $f :< S_3, \circ > \to < Z_4, \oplus_4 >$; $f(a) = \begin{cases} 0 & \text{if } a \text{ even}, \\ 2 & \text{if } a \text{ odd}. \end{cases} \forall a \in S_3$
is a homomorphism (verify that?).

Theorem1: Let $f :< G_1,* >\to< G_2,\# >$ be a homomorphism, and let e_1, e_2 are the identities in G_1, G_2 respectively. Then:

$(i)\ f(e_1) = e_2$.

$(ii)\ f(x^{-1}) = [f(x)]^{-1}\ \ \forall x \in G_1$.

Proof:

(i) *let* $x \in G_1$, $f(x) \in G_2$.

$\therefore f(x) = f(x * e_1) \Rightarrow f(x)\# e_2 = f(x)\# f(e_1) \Rightarrow e_2 = f(e_1)$.

$(ii) \because f(e_1) = e_2$

$\therefore f(x * x^{-1}) = e_2 \Rightarrow f(x)\# f(x^{-1}) = e_2$

$\Rightarrow [f(x)]^{-1}\#[f(x)\# f(x^{-1})] = [f(x)]^{-1}\# e_2$

$\Rightarrow [[f(x)]^{-1}\# f(x)]\# f(x^{-1}) = [f(x)]^{-1}$

$\Rightarrow e_2\# f(x^{-1}) = [f(x)]^{-1}$

$\Rightarrow f(x^{-1}) = [f(x)]^{-1}$.

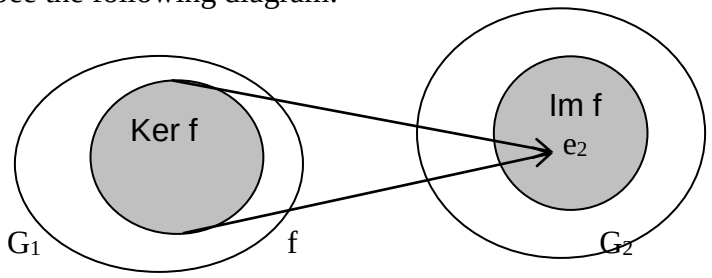
- **The Kernel and Image of a Homomorphism:**

Def.2: Let $f : G_1 \to G_2$ be a homomorphism.

The set: $\ker f = \{x : x \in G_1, f(x) = e_2\} \subset G_1$ is called the *kernel* of the homomorphism f. And the set:

$\text{Im } f = \{y : y \in G_2, \exists x \in G_1; f(x) = y\} \subset G_2$ is called the *image* of the homomorphism f.

See the following diagram:



Examples:

1- The kernel, and the image of a homomorphism $f :< Z,+ >\to< A,\times >$;

$A=\{1,-1,i,-i\}$, $f(n)=\begin{cases}1 & \text{if } n \text{ even},\\ -1 & \text{if } n \text{ odd}.\end{cases}$ are:

$\ker f=\{n : n\in Z,\ n \text{ even}\}=\{0,\pm 2,\pm 4,...\}\subset Z,$

$\text{Im } f=\{1,-1\}\subset A.$

2- The kernel, and the image of a homomorphism

$f :< S_3,\circ >\to< Z_4,\oplus_4 >;\ f(a)=\begin{cases}0 & \text{if } a \text{ even},\\ 2 & \text{if } a \text{ odd}.\end{cases}$ are:

$\ker f=\{I,(1\ 2\ 3),(1\ 3\ 2)\}\subset S_3,$

$\text{Im } f=\{0,2\}\subset Z_4.$

3- Let $A=\{a,b\}$ .Then $< P(A),\Delta >$ is an abelian group , and let $B=\{1,-1,i,-i\}$ .Then $< B,\times >$ is also an abelian group (verify that?).

A mapping $f : P(A)\to B;\ f(X)=1\ \forall X\in P(A)$ is a homomorphism, and $\ker f=P(A)$, $\text{Im } f=\{1\}$.

Theorem2: Let $f :< G_1,* >\to< G_2,\# >$ be a homomorphism, and let e_1,e_2 are the identities in G_1,G_2 respectively. Then:

(i) $\ker f$ is a subgroup of a group G_1 .

(ii) $\text{Im } f$ is a subgroup of a group G_2 .

Proof: We use the fact that a subset H of a group G is a subgroup of G iff $\forall a,b\in H\Rightarrow ab^{-1}\in H.$

(i) *let* $x_1,x_2\in \ker f\Rightarrow f(x_1)=f(x_2)=e_2$,

$\because f(x_2^{-1})=[f(x_2)]^{-1}=[e_2]^{-1}=e_2$,

$\therefore f(x_1*x_2^{-1})=f(x_1)\#f(x_2^{-1})=e_2\#e_2=e_2\Rightarrow x_1*x_2^{-1}\in \ker f.$

$\therefore \ker f\le G_1.$

(ii) *let* $y_1,y_2\in \text{Im } f\Rightarrow \exists\ x_1,x_2\in G_1\ ;\ f(x_1)=y_1\ ,\ f(x_2)=y_2$,

$\therefore y_1\#y_2^{-1}=f(x_1)\#[f(x_2)]^{-1}=f(x_1)\#f(x_2^{-1})=f(x_1*x_2^{-1})\in \text{Im } f.$

$\therefore \text{Im } f\le G_2.$

Theorem3: Let $f :< G_1,* >\to< G_2,\# >$ be a homomorphism, and let e_1, e_2 are the identities in G_1, G_2 respectively. Then f is 1-1 iff $\ker f = \{e_1\}$.

Proof: Let f is 1-1 we prove that $\ker f = \{e_1\}$ as follows:

$$x \in \ker f \Rightarrow f(x) = e_2 \ , \ f(e_1) = e_2$$
$$\Rightarrow f(x) = f(e_1)$$
$$\Rightarrow x = e_1.$$

i.e. $\ker f = \{e_1\}$.

Conversely, let $\ker f = \{e_1\}$ we prove that f is 1-1 as follows:

$$x_1, x_2 \in G_1 \ , \ f(x_1) = f(x_2) \Rightarrow f(x_1)\#[f(x_2)]^{-1} = f(x_2)\#[f(x_2)]^{-1}$$
$$\Rightarrow f(x_1)\# f(x_2^{-1}) = e_2$$
$$\Rightarrow f(x_1 * x_2^{-1}) = e_2$$
$$\Rightarrow x_1 * x_2^{-1} \in \ker f = \{e_1\}$$
$$\Rightarrow x_1 * x_2^{-1} = e_1$$
$$\Rightarrow x_1 = x_2.$$

i.e. f is 1-1 .

Def.3: A homomorphism $f : G_1 \to G_2$ is called an *isomorphism* if it is 1-1 corresponding (i.e. f is 1-1 and f is onto), in this case we say that the two groups G_1, G_2 are isomorphic, and denote $G_1 \cong G_2$

Def.4: An isomorphism of a group onto itself is called an *auto- morphism* of the group.

- In order to show $G_1 \cong G_2$ we proceed as follows:

(Step1): Define a mapping f i.e. describe the element $f(x)$ in G_2 for every $x \in G_1$.

(Step2): Show that f is 1-1.

(Step3): Show that f is onto.

(Step4): Show that f is a homomorphism.

Examples:

1- To show that $< Z,+ > \cong < Z_E,+ >$ where Z the set of integers, and Z_E the set of all even integers:

(Step1): Define a mapping $f : Z \to Z_E$ by $f(x) = 2x \ \forall x \in Z$.

(Step2): $x_1, x_2 \in Z$, $f(x_1) = f(x_2) \Rightarrow 2x_1 = 2x_2 \Rightarrow x_1 = x_2$ So f is 1-1.

(Step3): $y \in Z_E$, $y = f(x) \Rightarrow y = 2x \Rightarrow x = \frac{y}{2} \in Z$ So f is onto.

(Step4): $x_1, x_2 \in Z$, $f(x_1 + x_2) = 2(x_1 + x_2) = 2x_1 + 2x_2 = f(x_1) + f(x_2)$

So f is a homomorphism.

Consequently, $< Z,+ > \cong < Z_E,+ >$.

2- Similarly, $< R,+ > \cong < R^+,\times >$ where R the set of real numbers, and R^+ the set of positive real numbers.

(Hint: Define a mapping $f : R \to R^+$ by $f(x) = e^x \ \forall x \in R$).

3- Similarly, $< Z,+ > \cong < A,\times >$ where Z the set of integers,

and $A = \{a : a = 3^n, n \in Z\}$.

(Hint: Define a mapping $f : Z \to A$ by $f(n) = 3^n \ \forall n \in Z$).

4- Let G be a multiplicative group. The mapping $f : G \to G$ defined by $f(x) = x^{-1} \ \forall x \in G$ is not an isomorphism. For,

although f is 1-1 and onto, it does not homomorphism ;

$f(xy) = (xy)^{-1} = y^{-1}x^{-1} \neq x^{-1}y^{-1} \neq f(x)f(y)$.

However, if G be a multiplicative abelian group, f is an auto-morphism of G.

Theorem4: Every cyclic group of infinite order is isomorphic to the additive group $< Z,+ >$.

Proof: Let $G = < a > = \{a^n : n \in Z\}$,

(Step1): Define a mapping $f : G \to Z$ by $f(a^n) = n \ \forall a^n \in G$.

(Step2): $a^n, a^m \in G$, $f(a^n) = f(a^m) \Rightarrow n = m \Rightarrow a^n = a^m$ So f is 1-1.

(Step3): $\forall n \in Z \ \exists \ a^n \in G$; $f(a^n) = n$ So f is onto.

(Step4): $a^n, a^m \in G$, $f(a^n a^m) = f(a^{n+m}) = n + m = f(a^n) + f(a^m)$

So f is a homomorphism.

Consequently, $< G,\times > \cong < Z,+ >$.

Theorem5: Every cyclic group of finite order n is isomorphic to the additive group $< Z_n, \oplus_n >$.

Proof: Let $G = \{e = a^0, a, a^2, ..., a^{n-1}\}$ and $Z_n = \{0,1,2,..., n-1\}$,

(Step1): Define a mapping $f : G \to Z_n$ by $f(a^r) = r \ \forall a^r \in G$.

(Step2): $a^r, a^s \in G$, $f(a^r) = f(a^s) \Rightarrow r = s \pmod n$ i.e. $r = nq + s$

So $a^r = a^{nq+s} = a^{nq} a^s = e a^s = a^s$ i.e. f is 1-1.

(Step3): $\forall r \in Z_n \ \exists \ a^r \in G$; $f(a^r) = r$ So f is onto.

(Step4): $a^r, a^s \in G$, $f(a^r a^s) = f(a^{r+s}) = r + s = f(a^r) + f(a^s)$

So f is a homomorphism.

Consequently, $< G, \times > \cong < Z_n, \oplus_n >$.

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

Solved Problem(1): Verify that the two cyclic groups $< S_3^+, \circ >$ and $< Z_3, \oplus_3 >$ are isomorphic.

The Answer: We can represent $< S_3^+, \circ >$ and $< Z_3, \oplus_3 >$ by the following table:

$\circ$ / $\oplus_3$	I / 0	(1 2 3) / 1	(1 3 2) / 2
I / 0	I / 0	(1 2 3) / 1	(1 3 2) / 2
(1 2 3) / 1	(1 2 3) / 1	(1 3 2) / 2	I / 0
(1 3 2) / 2	(1 3 2) / 2	I / 0	(1 2 3) / 1

As it can be seen from the table above: the similar elements in the two groups are neighboring in the table. So, $S_3^+ \cong Z_3$.

Solved Problem(2): Show that there exists no isomorphism between $< R,+ >$ and $< R,\times >$, where R the set of real numbers.

The Answer: Suppose that f is an isomorphism from $< R,+ >$ to $< R,\times >$. Then $f(x+0) = f(x) \Rightarrow f(x) \times f(0) = f(x) \Rightarrow f(0) = 1$,

$$f(x+(-x)) = f(0) \Rightarrow f(x) \times f(-x) = 1 \Rightarrow f(-x) = \frac{1}{f(x)},$$

because f is an isomorphism it is onto,

i.e. $\forall\, y \in < R,\times > \exists\, x \in < R,+ > ; y = f(x)$,

then for $0 \in < R,\times > \exists\, x \in < R,+ > ; 0 = f(x)$,

but $f(-x) = \frac{1}{f(x)} \Rightarrow f(-x) = \frac{1}{0} \notin R$ which gives contradiction.

So, there exists no isomorphism between $< R,+ >$ and $< R,\times >$.

Exercises:

1- Which of the following is a homomorphism?
(Give reasons for your answer)
and determine $\ker f$, $\mathrm{Im}\, f$ for a homomorphism.

(i) $f :< Z,+ > \to < Z,+ > ; f(n) = n^2$, Z the set of integers.

(ii) $f :< Z,+ > \to < Z,+ > ; f(n) = 2n$

(iii) $f :< Z,+ > \to < Z,+ > ; f(n) = n+1$

(iv) $f :< R,\times > \to < R,\times > ; f(n) = n^2$, R the set of real numbers.

(v) $f :< P\{a,b\},\Delta > \to < Z,+ > ; f(X) = O(X)\ \ \forall\, X \in P\{a,b\}$.

2- Let $f :< C,\times > \to < R,\times >$ be a mapping ,where C the set of complex numbers, and R the set of real numbers, defined by:

$f(a+ib) = |a+ib| = \sqrt{a^2+b^2}$. Verify that f is a homomorphism.

Is f an isomorphism?.

3- Let $f :< X,\oplus > \to < Y,\otimes >$ be a mapping defined by $f(x) = -x$ where:

$$\begin{aligned} a \oplus b &= a+b+ab \ \ \forall\, a,b \in X = R-\{-1\}, \\ a \otimes b &= a+b-ab \ \ \forall\, a,b \in Y = R-\{1\}. \end{aligned} \quad ; R \text{ the set of real numbers.}$$

Verify that $X \cong Y$.

4- Verify that the two cyclic groups $< Z_5 - \{0\},\otimes_5 >$ and $< G = \{1,i,-i,-1\},\times >$ are isomorphic.

==========