CHAPTER - 1

GROUPS AND SUBGROUPS

One of the amazing features of twentieth century mathematics has been its recognition of the power of the ***abstract*** approach. This has given rise to a large body of new results and problems and has, infact, led us to open up whole new areas of mathematics whose very existence had not even been suspected. The ***algebra*** which has evolved as an outgrowth of all this is not only a subject with an independent life and vigor - it is one of the important current research areas in mathematics - but it also serves as the unifying thread which interlaces almost all of mathematics - geometry, number theory, analysis, topology and even applied mathematics.

In this chapter we shall embark on the study of the algebraic object known as a ***group*** which seves as one of the fundamental building blocks for the subject today called ***abstract algebra***. The concept of a group is central to abstract algebra : other well-known algebraic structures such as rings, fields and vector spaces can all be seen as groups endowed with additional operations and axioms.

The concept of a group arose from the study of polynomial equations, starting with *Évariste Galois* in the 1830s. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870.

§ 1. BINARY OPERATIONS

The definition of a group, by a set of axioms, involves the concept of a set with binary operation. In this section we shall define a set with binary operation and study some general properties of sets with binary operations. Intuitively, a set with binary operation is a set in which an abstract product is defined such that the product of any two elements of the set is again an element of the set. The precise definition for a binary operation on a set is as follows:

Definition. *Let S be a nonempty set. A* ***binary operation*** *or a* ***binary composition*** $*$ *on a set S is a mapping which associates to each*

ordered pair (a, b) *of elements in* S, *a uniquely defined eleme*
denoted by $a*b$, *of* S.

Thus a binary operation $*$ on a set S is just a function $*: S\times S$
where the image of (a, b) in $S\times S$ under $*$ is denoted by $a*b$.

i. e., $\qquad *((a, b)) = a*b.$

We can use any symbol to denote different binary operations on a
We can use the symbols $*$, $*'$, $+$, $\times$, $\oplus$, $\otimes$ etc.

Sometimes a binary operation on S provides a binary operation o
subset H of S also. We make a formal definition as below :

Definition. *Let* $*$ *be a binary operation on a nonempty set* S *a*
let H *be a subset of* S. *The subset* H *is* ***closed under*** $*$ *if for*
$a, b\in H$, *we also have* $a*b\in H$. *In this case, the binary operation*
H *given by restricting* $*$ *to* H *is the* ***induced operation*** *of* $*$ *on* H.

Remark 1. By our very definition of a binary operation $*$ on S, th
set S is closed under $*$, but a proper subset may not be as the example
given below show.

Remark 2. Remember that in an attempt to define a binary operation
$*$ on a set S we must be sure of the following conditions :

(i) Exactly one element is assigned to each possible ordered pair o
elements of S.

(ii) For each ordered pair of elements of S, the element assigned to i
is again in S.

The condition 1 ensures that $*$ *is well defined on* S and the condition
2 ensures that S *is closed under the operation* $*$.

Illustrative Examples

1. Let $\mathbb{Z}^+$ be the set of all positive integers (natural numbers). Since
sum of any two positive integers is a positive integer, '+' is well defined on
$\mathbb{Z}^+$ and $\mathbb{Z}^+$ is closed under addition and so '+' is a binary composition on
$\mathbb{Z}^+$. Multiplication is also a binary composition on $\mathbb{Z}^+$.

Since $\mathbb{Z}^+$ is not closed under subtraction, ($4\in\mathbb{Z}^+$, $7\in\mathbb{Z}^+$ but
$4-7=-3\notin\mathbb{Z}^+$), subtraction is not a binary operation on $\mathbb{Z}^+$. Similarly
division is not a binary operation on $\mathbb{Z}^+$.

On $\mathbb{Z}^+$, we define a binary operation $*$ by $a*b$ equals the smaller of a

and b, or the common value if $a = b$.

Then $2 * 11 = 2$, $15 * 9 = 9$ and $6 * 6 = 6$.

On $\mathbb{Z}^+$, we define another binary operation $\oplus$ by

$$a \oplus b = a + b + 2.$$

Then $2 \oplus 3 = 7$, $5 \oplus 2 = 9$ and $9 \oplus 11 = 22$.

2. The set $\mathbb{Q}$ of all rational numbers is closed under addition, multiplication and subtraction and these operations are well defined on $\mathbb{Q}$. Hence addition, multiplication and subtraction are binary operations on $\mathbb{Q}$. Since division by zero is not defined and zero is an element of $\mathbb{Q}$, division is not a binary operation on $\mathbb{Q}$.

3. The set $\mathbb{R}$ of all real numbers is closed under addition, multiplication and subtraction and these operations are well defined on $\mathbb{R}$. Hence addition, multiplication and subtraction are binary operations on $\mathbb{R}$. Since division by zero is not defined and zero is an element of $\mathbb{R}$, division is not a binary operation on $\mathbb{R}$.

4. Our usual addition + on the set $\mathbb{R}$ of all real numbers doesnot induce a binary operation on the set $\mathbb{R}^*$ of nonzero real numbers because $2 \in \mathbb{R}^*$ and $-2 \in \mathbb{R}^*$, but $2 + (-2) = 0$ and $0 \notin \mathbb{R}^*$. Thus $\mathbb{R}^*$ is not closed under +. Obviously, multiplication and division are binary operations on $\mathbb{R}^*$.

5. Let S be a set and $P(S)$ be the power set of S i.e., the set of all subsets of S. Then, since the union and intersection of any two subsets of S is again a subset of S, both union $\cup$ and intersection $\cap$ are binary operations on S.

6. Let V be the set of all vectors in space. Then the operation of vector addition, vector subtraction and vector multiplication are binary operations as for any $\mathbf{a}, \mathbf{b} \in V$, $\mathbf{a} + \mathbf{b}$, $\mathbf{a} - \mathbf{b}$ and $\mathbf{a} \times \mathbf{b}$ are all vectors and as such belong to the set V. However, dot product is not a binary operation, since the dot product of any two vectors is a scalar quantity.

If we restrict the set of vectors to only coplanar vectors, then the vector multiplication will not be a binary composition because $\mathbf{a} \times \mathbf{b}$ is a vector perpendicular to the plane containing $\mathbf{a}$ and $\mathbf{b}$ and as such it will not belong to the set of coplanar vectors to which $\mathbf{a}$ and $\mathbf{b}$ belong.

7. Let $M(\mathbb{R})$ be the set of all matrices with real entries. The u matrix addition + is not a binary operation on this set since $A + B$ is defined for an ordered pair (A, B) of matrices having different numbe rows or of columns. Similar is the case with matrix multiplication.

If M denote the set of all $m \times n$ matrices, then the operations addition and subtraction of matrices are binary operations since for $A, B \in M$, both $A + B$ and $A - B$ are defined and $A + B \in M$ and $A - B \in$

Similarly in the set of all $n \times n$ square matrices, the multiplicatio matrices is a binary operation.

8. Let F be the set of all real valued functions having as domain the $\mathbb{R}$ of real numbers. We are familiar from calculus with the bin operations $+, -, \cdot$, and $\circ$ on F. Namely, for each ordered pair (f, g) functions in F, we define for each $x \in \mathbb{R}$

$f + g$ by $(f + g)(x) = f(x) + g(x)$ addition,

$f - g$ by $(f - g)(x) = f(x) - g(x)$ subtraction,

$f \cdot g$ by $(f \cdot g)(x) = f(x)g(x)$ multiplication,

and $f \circ g$ by $(f \circ g)(x) = f\big(g(x)\big)$ composition.

All four of these functions are again real valued with domain $\mathbb{R}$ and so F is closed under all four operations $+, -, \cdot$, and $\circ$.

Let us define another operation '$*$' to give the usual quotient of f by g, that is, $f * g = h$, where $h(x) = f(x) / g(x)$. Since functions in F were to be defined for all real numbers, $h \notin F$ for some $f, g \in F$. For example, if $f(x) = \cos x$ and $g(x) = x^2$, then $h(0)$ is undefined and so $h \notin F$.

9. Let S be a set consisting of 20 people, no two of whom are of the same height. Define $*$ by $a * b = c$, where c is the tallest person among the 20 in S. Then $*$ is well defined on S and S is closed under the operation $*$. Hence $*$ is a binary operation on S.

10. Let S be a set consisting of 20 people, no two of whom are of the same height. Define $*$ by $a * b = c$, where c is the shortest person in S who is taller than both a and b. This $*$ is not everywhere defined, since if either a or b is the tallest person in the set, $a * b$ is not determined.

11. If a and b are any two integers ***addition modulo n*** of a and b, denoted by $a +_n b$, is the least non-negative integer, obtained as remainder

when their ordinay sum $a + b$ is divided by n. For any $n \in \mathbb{Z}^+$, let

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Then the operation '$+_n$' known as *addition modulo n* is a binary operation on $\mathbb{Z}_n$.

10. For a finite set, a binary operation on the set can be defined by means of a table in which the elements of the set are listed across the top as heads of columns and at the left side as heads of rows. We always require that the elements of the set be listed as heads across the top in the same order as heads down the left side. Consider the finite set $S = \{a, b, c\}$ and the table given below :

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

The above table defines the binary operation '$*$' on $S = \{a, b, c\}$ by the following rule :

(i th entry on the left) $*$ (j th entry on the top)

= entry in the i th row and j th column of the table body.

Hence according to the above table

$a * a = b$ $\quad$ $a * b = c$ $\quad$ $a * c = b$

$b * a = a$ $\quad$ $b * b = c$ $\quad$ $b * c = b$

$c * a = c$ $\quad$ $c * b = b$ $\quad$ $c * c = a$.

Problem 1. *Let + and · be the usual binary operations of addition and multiplication on the set* $\mathbb{Z}$ *and let* $H = \{n^2 : n \in \mathbb{Z}^+\}$. *Determine whether H is closed under* (a) *addition and* (b) *multiplication.*

Solution. (a) Since $1^2 = 1$ and $2^2 = 4$, $1, 4 \in H$. But $1 + 4 = 5 \notin H$. Hence H is not closed under addition.

(b) Choose any $r, s \in H$. Then by definition of H, $r = n^2$ and $s = m^2$, for some $n, m \in \mathbb{Z}^+$.

Then $\quad rs = n^2m^2 = (nm)^2$.

Since $\mathbb{Z}^+$ is closed under multiplication, $nm \in \mathbb{Z}^+$ and so, by the defini-

tion of H, $rs = (nm)^2 \in H$. Hence H is closed under multiplication.

Problem 2. *Draw the composition table for the binary operation* '$+_6$' *addition modulo* 6, *on the set* $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

Solution. For any $a, b \in \mathbb{Z}_6$, $a +_6 b$ is equal to the least non-negative integer, obtained as remainder when their ordinay sum $a + b$ is divided by 6. Therefore $0 +_6 0 = 0, 0 +_6 1 = 1, 0 +_6 2 = 2, 0 +_6 3 = 3, 0 +_6 4 = 4, 0 +_6 5 = 5, 1 +_6 0 = 1, 1 +_6 1 = 2, 1 +_6 2 = 3, 1 +_6 3 = 4, 1 +_6 4 = 5, 1 +_6 5 = 0, \ldots., 5 +_6 0 = 5, 5 +_6 1 = 0, 5 +_6 2 = 1, 5 +_6 3 = 2, 5 +_6 4 = 3, 5 +_6 5 = 4$. The table representing this operation is as given below :

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4