Dr. O. P. Raman
Dept of Mathematics

For T. D. C. Part II

Paper - 3

Abstract (Modern) Algebra

1.2 Definition : Group/Abelian group

(a) Group : Let G be non-empty set and o be a binary operation on G. Then the set G together with the operation o, denoted by (G, o) is called a group iff (i.e., if and only if) the following axioms (conditions) are satisfied :

G_1 : If $a, b \in G$, then $a \, o \, b \in G$ *(closure)*

G_2 : If $a, b, c \in G$, then $(a \, o \, b) \, o \, c = a \, o (b \, o \, c)$ *(associative law)*

G_3 : There exists an element e of G such that $a \, o \, e = e \, o \, a = a$ for all elements $a \in G$. *(existence of identity)*

The element e is called an identity of the group G.

G_4 : For each element $a \in G$ there exists an element a' of G such that $a \, o \, a' = a' \, o \, a = e$. *(existence of inverse)*

The element a' is called an inverse of a in G.

The most common notation for the inverse of $a \in G$ is a^{-1}.

Thus if the set G be given and a binary operation o be defined on G such that all the four conditions are satisfied, then we say that G is a group under the operation o or G is a group w.r.t. the operation o.

It follows, therefore, that if any one of the conditions out of the four is not satisfied, then that set does not form a group.

✓ ▸ **Ex.6.** *Prove that the set of rational numbers is an Abelian group under addition.*

Soln. Let Q be the set of rational numbers, that is, numbers of the form $\frac{p}{q}$ where p, q are integers and $q \neq 0$. If the set Q is an Abelian group under addition, then it must satisfy the five conditions, when the operation is +. We shall presently see that it does satisfy all five conditions.

(i) If $\frac{a}{b}$ and $\frac{c}{d} \in Q$, then $\frac{a}{b}+\frac{c}{d}$ which is $=\frac{ad+bc}{bd}$ (a rational number) also $\in Q$

Thus condition (i) is satisfied.

(ii) If $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q$, then $\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{adf+bcf+bde}{bdf}$

Also, $\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{cf+de}{df}=\frac{adf+bcf+bde}{bdf}$

$$\therefore \quad \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right).$$

Thus condition (ii) is satisfied.

(iii) The identity is zero, for $\frac{a}{b}+0=\frac{a}{b}$.

(iv) The inverse of $\frac{a}{b}$ is $\left(-\frac{a}{b}\right)$ for $\frac{a}{b}+\left(-\frac{a}{b}\right)=0$.

(v) $\frac{a}{b}+\frac{c}{d}=\frac{c}{d}+\frac{a}{b}$.

Thus we see that the set Q satisfies all the five conditions of a group under addition and hence it is an Abelian group w.r.t., addition.

✓ ▸ **Ex.7.** *Prove that the set of non-zero rational numbers forms an Abelian group under multiplication.*

Soln. Let Q^* be the set of non-zero rational numbers. It can be shown as in the previous example that

(i) The product of two rational numbers is a rational number.
Hence if $a, b \in Q^*$, then $a \cdot b = Q^*$.

(ii) The multiplication of rational numbers is associative.
Hence if $a, b, c \in Q^*$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) The identity of Q^* is $1 \in Q^*$, for $a \cdot 1 = 1 \cdot a = a$, for every $a \in Q^*$.

(iv) The inverse of $a \in Q^*$ is $\frac{1}{a} \in Q^*$, for $a \cdot \left(\frac{1}{a}\right)=\left(\frac{1}{a}\right) \cdot a = 1$.

Thus all the group postulates are satisfied and hence Q^* is a group.

Moreover Q^* is an Abelian group since the multiplication in Q^* is commutative.

$\times$	$+1$	-1	$+i$	$-i$
$+1$	1	-1	i	$-i$
-1	-1	1	$-i$	i
$+i$	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Clearly every entry in the table is $+1, -1, +i$ or $-i$.

Hence M is closed.

(ii) Associativity follows from the fact that the real numbers and complex numbers are associative.

(iii) The identity is + 1 and this is obvious from the first row of the table.

(iv) The inverses of $1, -1, +i, -i$ are respectively $1, -1, -i$ and i. Hence M is a group.

Also M is an Abelian group since the table is symmetrical about the main diagonal which begins from the left hand corner.

The identity of S is e ... $\frac{2r\pi i}{}$ ... $\frac{2(n-r)\pi i}{}$ ... their product = $e^{\frac{2n\pi i}{n}} =$

▸ **Ex.18.** *Prove that the four fourth roots of unity i.e., the set* $(1, -1, i, -i)$ *is an Abelian grou w.r.t., multiplication.*

Soln. Let $M = \{1, -1, i, -i\}$.

(ii) We verify Axiom 1 for M :

$$1 \cdot 1 = 1$$
$$1 \cdot (-1) = -1$$
$$1 \cdot i = i$$
$$1 \cdot (-i) = -i$$
$$i \cdot 1 = i$$
$$i \cdot (-1) = -i$$
$$i \cdot i = -1$$
$$i \cdot (-i) = 1$$

$$(-1) \cdot 1 = -1$$
$$(-1) \cdot (-1) = 1$$
$$(-1) \cdot i = -i$$
$$(-1) \cdot (-i) = i$$
$$(-i) \cdot 1 = -i$$
$$(-i) \cdot (-1) = i$$
$$(-i) \cdot i = 1$$
$$(-i) \cdot (-i) = -1.$$

It is to be noted that in a finite group i.e., in a group in which the number is finite we ca exhibit all possible multiplications. It is convenient to arrange them in a table (called multiplication table) as given below :

• Note : If $a \in G$ and b is the inverse of a, then a is the inverse of b.

Theorem II. To prove that $(ab)^{-1} = b^{-1}a^{-1}$ where $a, b \in G$.

Or, The inverse of the product of two elements of a group is the product of the inverses taken in reverse order.

Proof : Let $a, b \in G$ and let their inverses be a^{-1} and b^{-1} respectively.

Now, $(b^{-1}a^{-1})(ab) = b^{-1}\{a^{-1}(ab)\}$ (Associative law)

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

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

Similarly, $(ab)(b^{-1}a^{-1}) = a\{b(b^{-1}a^{-1})\}$

$$= a\{(bb^{-1})a^{-1}\}$$

$$= a\{(ea^{-1})\} = aa^{-1} = e.$$

Hence $b^{-1}a^{-1}$ is the inverse of ab.

The rule given in the above theorem is known as the **reversal law.** The reversal law can be generalised as follows :

$$(abc\,mn)^{-1} = n^{-1}m^{-1}\ldots c^{-1}b^{-1}a^{-1};\text{ where } a, b, c, \ldots m, n \in G.$$

By the use of this theorem, we prove the following important result about groups.

1.16 | Theorem

✓ ***If a and b are elements of a group G, the equations (i) $ax=b$ and (ii) $ya=b$ unique solutions in G.***

Proof : (i) Consider the equation $ax=b$

We are going to show that $a^{-1}b$ is the solution of the given equation.

It has to be observed that $a^{-1}b \in G$, for a^{-1} and $b \in G$ and therefore $a^{-1}b \in G$.

If $a^{-1}b$ is the solution of the equation, then $x=a^{-1}b$ must satisfy the given equa

Now putting $x=a^{-1}b$ in (1), we get the

L.H.S. $=a(a^{-1}b)=(aa^{-1})b=eb=b$.

Therefore the equation has a solution $x=a^{-1}b$.

Now we are going to show that $x=a^{-1}b$ is the unique solution.

If not, suppose $x=c$ is another solution in G.

Putting $x=c$ in (1), we have $ac=b$.

Multiplying both sides by a^{-1} on the left, we get $a^{-1}(ac)=a^{-1}b$

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

$$\therefore \quad c=a^{-1}b$$

which means that whatever solution we assume for the given equation, it will come to be $a^{-1}b$.

Hence the solution $x=a^{-1}b$ is unique. The proof of (ii) is similar.

This theorem empowers us to define a group in an alternative way. Hence the follow theorem.

1.12 Cancellation Laws in a Group

Theorem : If $a, b, c \in G$, then

(i) $ab = ac \Rightarrow b = c$ (left cancellation law)

(ii) $ba = ca \Rightarrow b = c$ (right cancellation law).

Proof : (i) Given that $ab = ac$ ... (1)

Let a^{-1} be the inverse of a in G. Multiplying (i.e., applying the group operation)both sides of (1) by a^{-1} on the left, we get $a^{-1}(ab) = a^{-1}(ac)$

which by associative law becomes $(a^{-1}a)b = (a^{-1}a)c$.

Since by postulates (G_4), $a^{-1}a = e$, the identity in G, we have $eb = ec$.

Now by postulate (G_3), we have $eb = b$ and $ec = c$.

Therefore we get $b = c$ and the first part of the theorem is proved.

(ii) Given that $ba = ca$ ... (2)

Let a^{-1} be the inverse of a in G.Multiplying both sides of (2) by a^{-1} on the right, we get

$$(ba)a^{-1} = (ca)a^{-1}$$

$\Rightarrow$ $$b(aa^{-1}) = c(aa^{-1}) \quad \text{[by postulate } G_2\text{]}$$

$\Rightarrow$ $$be = ce \quad \text{[by postulate } G_4\text{]}$$

$\therefore$ $$b = c \quad \text{[by postulate } G_3\text{]}$$

1.13 Theorem

✓ **The identity element in a group is unique.**

Proof : Let G be a group and let e be an identity element. We have to prove that e is unique.

If not, suppose e' be another identity element in a group G.

Since e is the identity element of G, therefore $ae = ea = a$

Similarly since e' is the identity element of G, therefore $ae' = e'a = a$ ... (1)
for every $a \in G$. ... (2)

Since the equation (1) is true for every $a \in G$ and since $e' \in G$, therefore putting $a = e'$ in (1) we get

$$e'e = ee' = e'$$

Similarly putting $a = e$ in (2), we get $ee' = e'e = e$ ... (3)

Hence from (3) and (4), it follows that $e = e'$ which means that the identity in a group is unique. ... (4)

Second method : From (1) and (2), we have $ae = ae'$.

Therefore from the cancellation law $e = e'$.

Hence the identity in a group is unique.

(b) Abelian Group : In addition to the above four conditions if the set G satisfies more condition viz.

G_5 :For every pair of elements a and b in G,

$$a \circ b = b \circ a \qquad \text{(commutative la}$$

then G is said to be an *Abelian group or a commutative group.*

Also, when $a \circ b = b \circ a$, we say that the elements a and b commu

Ex.1. *Prove that the set of integers is an Abelian group under addition.*

Soln. Let I be the set of integers, that is $I = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

In order to show that I is a group we need to show that all the four postulates of a gro are satisfied. We take up all the group postulates one by one.

(i) The sum of two integers is an integer. Hence if $a, b \in I$, then $a + b \in I$.

(ii) Addition of integers is associative.

Hence if $a, b, c \in I$, then $a + (b + c) = (a + b) + c$.

(iii) The identity of I is $0 \in R$ for $a + 0 = 0 + a = a$ for all $a \in I$.

(iv) The inverse of $a \in I$ is $-a \in I$, for $a + (-a) = (-a) + a = 0$.

Thus all the group postulates are satisfied and hence I is a group. Moreover I is Abelian group, since addition in I is commutative.