5

Groups, Rings and Fields

Structure

Objectives

After studying this Chapter, you should be able to understand :

- *Binary composition, various types of composition, composition tables.*
- *Groups, rings and fields.*

5 0. INTRODUCTION

These are some special types of mathematical systems. The purpose of these is to help in performing certain mathmatical operations on a set. In the first three chapters we studied the algebra of certain binary operations and in the fourth chapter we acquainted ourselves with the real number system. Now, we take up some mathematical composition with certain number systems and the binary operations defined on them. The two together form a mathematical system. Before coming to certain special algebraic structures like groups and fields we shall like to discuss binary compositions.

5·1 BINARY COMPOSITIONS

A binary composition is a composition set of order pairs of numbers which are associated under a binary system, observing the rules of operations of such a system. The operations may be symbolised by say * (asterisk). What is of importance is the observance of the rules of operations dealt in earlier chapters. Here these rules are integrated into binary composition system.

Def *Let S be a non-emnty set. A mapping $* : S \times S \Rightarrow S$ is said to be a binary composition on the set S.*

Illustrations 1. Let R be the set of real numbers. Then addition $+$ is a binary composition in R, since to every ordered pair (a, b) of real numbers, we get $a+b$ which is also a real number.

Multiplication '.' and subtraction '—' are also binary compositions in R, since $a \cdot b$ and $a-b$ are also real numbers. But division is not a binary composition in R, since $a \div 0$ is meaningless.

2. Union $\cup$ and intersection $\cap$ are binary compositions in the power set of a given set since the union and intersection of two subsets of a given set are again subsets of the set. Thus

$$A \in P(S) \text{ and } B \in P(S) \Rightarrow A \cup B \in P(S)$$

$$A \in P(S) \text{ and } B \in P(S) \Rightarrow A \cap B \in P(S)$$

3. Conjunction ($\wedge$) and disjunction ($\vee$) are binary compositions in the set of all sentences.

4. Let Q be the set of rational numbers. Then the mapping $* : Q \times Q \Rightarrow Q$ defined by $a * b = a+b$, where as $a, b \in Q$ is an addition composition on the set Q of rational numbers.

Also, the mapping $* : Q \times Q \Rightarrow Q$ defind by $a * b = ab$ where $a, b \in Q$, is a multiplication composition on the set Q of rational numbers.

5·2. VARIOUS TYPES OF COMPOSITIONS

I. Commutative Composition. The binary composition $*$ on a set S is called *commutative* (or Abelian), if for every $a, b \in S$.

$$a*b = b*a$$

Illustrations 1. Both addition and multiplication compositions on set N of natural numbers are commutative, because $a+b=b+a$ and $a \cdot b = b \cdot a$ for every $a, b \in N$.

2. The addition and multiplication compositions on set Q, of rational numbers, on set R of real numbers and on set C, of complex numbers are also commutative.

3. The substraction composition on the set of integers, I, is not commutative, because $a-b \neq b-a$ for every $a, b \in I$.

4. The intersection and union compositions in the set of all subsets of a set are both commutative.

II. Associative composition. The binary composition $*$ on a set S is called *associative* if for every $a, b, c \in S$,

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

Illustrations 1. The addition and multiplication compositions on set of natural numbers, on set of rational numbers, on set of real numbers and on set of complex numbers are associative.

2. Both intersection and union compositions on set P or subsets of a set are associative, because

$$(A \cup B) \cup C = A \cup (B \cup C)$$

and $(A \cap B) \cap C = A \cap (B \cap C)$, where $A, B, C \in P$.

3. The subtraction operation on set of integers I is not associative because

$$a-(b-c) \neq (a-b)-c, \text{ for every } a, b, c \in I$$

4. In set Q, the composition defined as

$$a*b = a+b+ab$$

is associative because

$$\begin{aligned}(a*b)*c &= (a+b+ab)*c \\ &= (a+b+ab)+c+(a+b+ab)c \\ &= a+b+c+ab+bc+ac+abc\end{aligned}$$

Also
$$\begin{aligned}a*(b*c) &= a*(b+c+bc) \\ &= a+(b+c+bc)+a(b+c+bc) \\ &= a+b+c+ab+bc+ac+abc \\ &= (a*b*)*c\end{aligned}$$

5. In set R of real numbers, the composition defined by

$$a*b = a \cdot b^2$$

is not associative because

$$\begin{aligned}(a*b)*c &= (ab^2)*c \\ &= (ab^2)c^2 = ab^2c^2\end{aligned}$$

and
$$\begin{aligned}a*(b*c) &= a*(bc^2) \\ &= a(bc^2)^2 = ab^2c^4 \neq (a*b)*c\end{aligned}$$

III. Identity element for a composition. An element, donoted by e, of a set S is called an *identity element* for the composition*, on S if

$$a*e = e*a = a \; \forall \; a \in S$$

Illustrations 1. Let + be the composition of addition on set R of real number where 0 is the identity element for the composition because for every real number $a \in R$, $0+a=a+0=a$.

2. Let '.' be the composition of multiplication on set R of real numbers then 1 is the identity element for the composition because for every real number $a \in R$, $1 . a = a = a . 1$.

3. 0 is the identity for the addition composition on the sets of natural numbers, rational numbers and complex numbers. 1 is the identity for the multiplication composition on the sets of natural numbers, rational numbers and complex numbers.

4. For the union composition on a set S_1, out of the subsets of the set S, the null set $\phi \in S_1$, is the identity.

IV. Invertible element for a binary composition having an identity element. If a set S contains an identity element e, for the composition* and if $a*b = e = b*a$ for every $a, b \in S$, then a is called the *inverse* of b and b is called the *inverse* of a.

Illustrations 1. In the addition composition on set of real numbers, every real number 'a' has an additive inverse $(-a)$, because

$$a+(-a)=0=(-a)+a$$

where 0 is the identity element

In multiplication composition on the set of real numbers, a has a multiplicative inverse $\frac{1}{a}$, because

$$a.\frac{1}{a}=1=\frac{1}{a}.a,$$ where 1 is the identity element.

2. In the multiplication composition on the sets of rational numbers and complex numbers, every element except 0 is invertible.

5·3 COMPOSITION TABLES

If S is a finite set consisting of n elements then a composition* in S can be described by a table consisting of n rows and n columns in which the entry at the intersection of the row headed by an element $a\in S$ and the column headed by an element $b\in S$ is $a*b$. Such tables are called composition tables.

Illustrations 1. Let $S=\{a, b, c\}$. The table below gives a composition * in S.

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

From the table we find that

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

2. Let $S=\{1, \omega, \omega^2\}$ where ω is cube root of unity so that $w^3=1$

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

V. Distributive Laws for the compositions. If * and Δ be two compositions on set S and

(*i*) if $a\Delta(b * c)=(a\Delta b) * (a\Delta c)$, where $a, b, c \in S$, then * and Δ are said to satisfy the *left-distributive law.*

(*ii*) If $(b * c)\Delta a=(b\Delta a) * (c\Delta a)$, where $a, b, c \in S$, then * and Δ are said to satisfy the *right-distributive law.* The two laws together are called *distributive laws.*

Illustration. The compositions of addition and multiplication on the set of integers obey both the distributive laws.

We now take up certain special algebraic structures under the headings of groups, rings and fields.

5·4. GROUPS $(G, \oplus, \odot)$

Basically, a group is a special type of set with some relationships amongst its elements. In previous chapters we have quoted many sets in which the elements had no clear relationship with each other. We now consider sets which have special properties to allow us to add, multiply and combine the elements in some specified manner. We shall now describe, sets which possesses certain properties and form into groups.

Definition. A group is an algebric or a mathematical system consisting of a set G of elements $a, b, c, \ldots$and a single binary composition. This binary composition gives a rule of combination of the elements, and should be well defined. The symbol * is used to denote this composition or operation.

A non-empty set G of elements $a, b, c, \ldots$on which a binary operation* is defined, is said to form a group $(G, *)$ if the following properties are satisfied.

$\mathbf{G_1}$. *Closure.* There exists unique element $a * b \in G$ for every $a, b \in G$ such that

$$a * b \in G \ \forall \ a, b \in G$$

This also shows that it is an internal composition

$\mathbf{G_2}$. *Associative* :

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

for all $a, b, c \in G$.

$\mathbf{G_3}$. *Identity* : There exists an identity element say $e \in G$ such that

$$a * e = a = e * a$$

On the right of a it is right-identity and on the left of a it is the left-identity.

$\mathbf{G_4}$. *Inverse* : For every element $a \in G$, there corresponds an element $b \in G$ such that

$$a * b = e = b * a$$

The element b is called the inverse of a, it can also be denoted by a^{-1} but that will be confused with a negative index. The symbol (*) can be substituted by $\oplus$ for binary addition and $\odot$ for binary multiplication as the case may be.

It should be further noted that even though a large number of groups satisfy the commutative property, this is not a necessary requirement for a group.

A group consisting of finite number of elements is called a finite group. A group which does not restrict itself to a finite number of elements is called an *infinite group*. The order of a finite group refers to the number of elements in the non-empty finite set.

5·5. AN ABELIAN GROUP

A group $(G, *)$ *is said to be commutaitve or Abelian* group if $a * b = b * a$ for every $a, b \in G$.

Illustrations 1. A set of integers $I = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ forms a group with respect to addition because there is an identity element 0 and the inverse say $(-a)$ for $a \in I$. The group $(I, +)$ is an Abelian group as it is commutative under addition. But the set of integers is not a multiplicative group since there is absence of multiplicative inverses as in the case of 0 and 2.

2. The set of all positive rational numbers Q^+ is an Abelian group under multiplication. For

(*i*) If $a, b \in Q^+$, then a . b also exists in the set.

(*ii*) There exists an identity element 1.

(*iii*) The composition under multiplication is associative.

(*iv*) There exists an inverse $\frac{1}{a}$ for every $a \in Q^+$.

(*v*) The operation is also commutative and therefore forms an Abelian group.

3. The set of real numbers with the ordinary addition composition is an Abelian group.

4. The set of all non-zero rational numbers with the ordinary multiplication composition is an Abelian group.

5. *Prove that set of all integers with the ordinary addition as composition is a group.*

Proof. Let Z be the set of all integers and $+$ be the given binary composition.

(*i*) Let a, b be any two elements of Z.

Now $a + b \in Z$, since the sum of any two integers is also an integer.

Therefore $+$ satisfies the closure law.

(*ii*) Let a, b, c be any three elements of Z.

Then $(a+b)+c=a+(b+c)$ is true, since this is valid for all integers a, b, c.

Therefore $+$ satisfies the associative law.

(iii) Since $a+0=a=0+a$, $\forall a\in Z$, therefore the identity element 0 exists. It is the integer 0.

(iv) Since $a+(-a)=0=(-a)+a$, $\forall a\in Z$, therefore every element possesses an inverse.

Since Z satisfies all the properties of a group, $(Z,+)$ is a group.

6. *Show that the set $G=\{1, \omega, \omega^2\}$, where 1, ω, ω^2 are cube roots of unity, forms an Abelian group with respect to multiplicatton composition.*

Proof. *(i) Closure Property* :

$$1\odot\omega=\omega\in G\ ;\ \omega\odot\omega^2=\omega^3=1\in G\ ;\ \omega^2\odot 1=\omega^2\in G$$

(ii) Associativity :

$$(1\odot\omega)\odot\omega^2=1\odot(\omega\odot\omega^2)$$

(iii) Identity element is 1, since

$$1\odot\omega=\omega,\qquad 1\odot\omega^2=\omega^2,\qquad 1\odot 1=1$$

(iv) Inverse of each element exists :

$$1\odot 1=1 \text{ for } 1\in G$$

$$\omega\odot\omega^2=\omega^3=1,\ \omega^2\odot\omega=\omega^3=1$$

So, 1, ω^2, ω are respectively the inverses for 1, ω, ω^2.

(v) Commutativity :

$$1\odot\omega=\omega=\omega\odot 1,\ \omega\odot\omega^2=\omega^3=1=\omega^2\odot\omega$$

and $\omega^2\odot 1=\omega^2=1\odot\omega^2$

$(G, \odot)$ satisfies all the properties for Abelian group.

7. The set I of integers with the binary composition $*$ defined as $a * b=a-b$; $a, b\in I$ is not a group

because $a * (b * c)=a-(b-c)=a-b+c$

and $(a * b) * c=(a-b)-c=a-b-c$

Therefore $a * (b * c)\neq(a * b) * c$ and thus the property G_2 is not satisfied.

5·6. PROPERTIES OF A GROUP

I. Uniqueness of Identity. *Identity element of a group is unique.*

Proof. Let e and e' be the two identity elements of the group $(G, *)$.

$\therefore$ $a * e=a=e * a,\ \forall a\in G$ ...(1)

and $a * e'=a=e' * a$ ...(2)

Subsistituting $a=e'$ in (1). we have

$e' * e=e'=e * e'$ ...(3)

and putting $a=e$ in (2), we have

$$e * e'=e=e' * e \qquad \ldots(4)$$

From (3) and (4), we have $e'=e$

There cannot be two identity elements for $(G, *)$. Hence identity element of group is unique.

II. Uniqueness of inverse. *In a group every element possesses a unique inverse.*

Proof. Let a^{-1} and a' be two inverses of a in G.

$$\therefore \quad a * a'=e=a' * a \qquad \ldots(1)$$

and
$$a^{-1} * a=e=a * a^{-1} \qquad \ldots(2)$$

Now
$$a^{-1}=a^{-1} * e \qquad [\text{From } (G_2)]$$
$$=a^{-1} * (a * a') \quad [\text{Associative Law}]$$
$$=(a^{-1} * a) * a'$$
$$=e * a' \qquad [\text{From } (G_4)]$$
$$=a'$$

Hence the inverse of a is unique.

III. Cancellation Property. *For any group* $(G, *)$

(*i*) $a * b=a * c \quad \Rightarrow \quad b=c$

(*ii*) $b * a=c * a \quad \Rightarrow \quad b=c$, where $a, b, c \in G$

Proof. (*i*) Consider

$$a * b=a * c$$

The operation with inverse a^{-1} will give

$$a^{-1}*(a*b)=a^{-1}*(a*c)$$
$$\Rightarrow \quad (a^{-1}*a)b=(a^{-1}*a)*c \qquad \text{(By associative law)}$$
$$\Rightarrow \quad e*b=e*c$$
$$\Rightarrow \quad b=c$$

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

IV. *For every* $a, b \in G$, *each of the equations* $a*x=b$, $y*a=b$ **have** *unique solutions.*

Prof. Consider the equations

$$a*x=b \qquad y*a=b$$

Pre-multiplying and post-multiplying by a^{-1}, we get

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

This shows the existence of solutions of the above two equestions. To show uniqueness, let there be another x_1, y_1 such that

$$a*x_1=b \qquad y_1*a=b$$

then $\quad a*x=a*x_1, \qquad y*a=y_1*a.$

By Cancellation law, $x=x_1$, $y=y_1$, uniqueness follows.

V. *In a Group* $(G,*)$. $(a^{-1})^{-1}=a, \forall\ a\in G$. In other words, for every $a\in G$, the inverse of an inverse of a is 'a' only, *i.e., the inverse of an inverse of the element of a group is the element itself.*

Proof. We know that

$$b^{-1}*b=e$$

Replacing b by a^{-1}, we get

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

Operating on the right by a, we get

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

$$\Rightarrow \quad (a^{-1})^{-1}*(a^{-1}*a)=a \qquad \text{[Associative property]}$$

$$\Rightarrow \quad (a^{-1})^{-1}*e=a$$

$$\Rightarrow \quad (a^{-1})^{-1}=a \qquad \text{[Using Identity law]}$$

VI. *In a group* $(G, *)$,

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

In other words *the inverse of the product of two elements of a group is the product of their inverses taken in the reverse order.*

Proof. Let e be the identity element of the group G.

Now

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

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

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

$$=a*a^{-1}=e$$

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

$\Rightarrow$ By def of the inverse element of a group, $b^{-1}*a^{-1}$ is an inverse of $a*b$.

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

Example 1. *Prove that the numbers 1, i, -1, $-i$, where $i=\sqrt{-1}$ with ordinary multiplication as the composition is an Abelian group.*

Solution, Let us form the composition table for multiplication.

$\odot$	1	$-$	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(*i*) From the above table it is clear that multiplication is a binary operation as all the elements inside the above table are elements of G.

(*ii*) Also

$1\odot(i\odot -i)=(1\odot i)\odot -i$; since

$1\odot(i\odot -i)=(1\odot 1)=1$ and $(1\odot i)\odot -i=(i\odot -i)=1$

Associative property is satisfied.

(*iii*) 1 is the identity element, since

$1\odot 1=1,\ 1\odot(-1)=-1,\ 1\odot -i=-i$

(*iv*) We can verify that inverses of every element exit. Suppose we want to find inverse of i.

Look to the row in which leading element is i, *i.e.*, the third row. See the identity element 1 in that row then the number at the head of this column, *i.e*, $-i$ will be the inverse of i. Thus $(i)^{-1}=-i$.

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

(*v*) Again $1\odot i=i\odot 1,\ -i\odot i=i\odot -i$, etc., *i.e.*, the composition is commutative.

Hence the above set is an abelian group for multiplication.

Example 2. *Prove that the set Q^+ of all positive rational numbers forms an Abelian group for the composition $*$ defind as*

$$a*b=\frac{ab}{2}$$

Solution. (*i*) *Closure property.* Let a, b be the two elements of the above set.

$$\therefore \qquad a*b=\frac{a.b}{2}\in Q^+$$

(*ii*) *Associative property.* Let $a, b, c \in Q^+$ then

$$(a*b)*c=\left(\frac{a.b}{2}\right)*c$$

$$=\frac{1}{2}\left[\left(\frac{a.b}{2}\right).c\right]$$

$$=\tfrac{1}{4}[(a.b).c]$$

$$=\tfrac{1}{4}[a(b.c)]$$

$$=\frac{1}{2}\left[a.\left(\frac{b.c}{2}\right)\right]$$

$$= \tfrac{1}{2}[a \cdot (b * c)]$$
$$= a*(b*c)$$

Hence $\quad i*b)*c = a*(b*c)$

(*iii*) *Identity.* $2 \in Q^+$ serves as an identity because

$$a*2 = \frac{a \cdot 2}{2} = a, \ \forall \ a \in Q^+$$

$\therefore$ Identity element exists and belongs to the set.

(*iv*) *Inverse.* For $a \in Q^+, \frac{4}{a} \in Q^+$ is the inverse as

$$a * \frac{4}{a} = \frac{a \cdot \frac{4}{a}}{2} = \frac{4}{2} = 2$$

$\therefore$ Inverse element exists and belongs to the set.

(*v*) *Commutative property.*

$$a*b = \frac{ab}{2} = \frac{ba}{2} = b*a$$

Hence Q^+ is an Abelian group.

Example. 3. *Prove that the set Q of all rational numbers other than 1 with the operation defined by*

$$a*b = a+b-ab$$

constitutes an Abelian group.

Solution. (*i*) *Closure property.* Let $a, b \in Q$ so that both a and b are rational numbers other than unity.

$a*b = a+b-ab$ is also a rational number.

(*ii*) *Associative property.* For all $a, b, c \in Q$

$$(a*b)*c = (a+b-ab)*c$$
$$= (a+b-ab)+c-(a+b-ab)c$$
$$= a+b+c-ab-ac-bc+abc$$

Also $\quad a*(b*c) = a*(b+c-bc)$
$$= a+(b+c-bc)-a(b+c-bc)$$
$$= a+b+c-ab-ac-bc+abc$$

$\therefore \quad (a*b)*c = a*(b*c)$

(*iii*) *Identity.* If e be the identity then

$$a*e = a \quad \Rightarrow \quad a+e-ae = a$$
$$\Rightarrow \quad e(1-a) = 0$$
$$\Rightarrow \quad e = 0, \text{ as } a \neq 1$$

$\therefore \quad 0 \in Q$ is the identity element.

(*iv*) *Inverse.* If b is the inverse of a, then

$$a*b=e$$

$$\Rightarrow \quad a+b-ab=0$$

$$\Rightarrow \quad b=\frac{a}{a-1}$$

$\frac{a}{a-1} \in Q$ is the inverse element.

(*v*) *Commutative property.* For all $a, b \in Q$

$$a*b=a+b-ab$$

$$b*a=b+a-ab$$

$$=a+b-ab=a*b$$

Hence the set Q with the above composition forms an Abelian group.

Example 4. *Let an ordered pair of real numbers be called a complex number, and let addition $\oplus$ of complex numbers be defind by*

$$(a, b)\oplus(c, d)=(a+c, b+d)$$

Show that the set of complex numbers together with binary operation $\oplus$ forms a group.

Solution. Let C be the set of complex number, *i.e.*,

$$C=\{(a, b) \mid a, b \in R\}$$

where R is the set of real numbers.

(*i*) *Closure property.* Let $(a, b), (c, d) \in C$, as the sum of the complex numbers is a complex number. Therefore

$$(a, b)\oplus(c, d)=(a+c, b+d) \in C$$

(*ii*) *Associative law.* $\forall (a, b), (c+d), (e+f) \in C$

$$(a, b)\oplus\{(c, d)\oplus(e, f)\}=(a, b)\oplus\{(c+e), (d+f)\}$$

$$=\{(a+c+e), (b+d+f)\} \quad \ldots(1)$$

and $\{(a, b)\oplus(c, d)\}\oplus(e, f)=\{(a+c), (b+d)\}\oplus(e, f)$

$$=\{(a+c+e), (b+d+f)\} \quad \ldots(2)$$

$\therefore \quad (1)=(2)$

(*iii*) *Identity element.* The element $(0, 0) \in C$ is the identity element as

$$(a, b)\oplus(0, 0)=(a, b)=(0, 0)\oplus(a, b)$$

(*iv*) *Existence of inverse.* $(-a, -b) \in C$ is an inverse of (a, b) as

$(a, b)\oplus(-a, -b)=(0, 0)=(-a, -b)\oplus(a, b) \forall$ all $(a, b) \in C$

(*v*) *Commutative law.* For all $(a, b), (c, d) \in C$

$$(a, b)\oplus(c, d)=(a+c, b+d)=(c+a, d+b)=(c, d)\oplus(a, b)$$

Hence $(C, \oplus)$ is an abelian group.

Example 5. *Show that the set*

$$G=(x+\sqrt{2}y : x, y\in Q)$$

is an abelian group with respect to addition, Q being the set of rationals.

(C.A. Entrance December 1983)

Solution. Since $x, y\in Q$, set of rational numbers, therefore, $x+\sqrt{2}y$ is a set of irrational numbers, G.

Let us see whether the set G satisfies the requisites of an abelian group.

1. **Closure property.** The addition of any two irrational numbers is also a irrational number of the same form, *e.g.*, let x_1, y_1 and $x_2, y_2\in Q$, then

$$(x_1+\sqrt{2}y_1)+(x_2+\sqrt{2}y_2)=(x_1+x_2)+\sqrt{2}(y_1+y_2)$$

and
$$(x_2+\sqrt{2}y_2)+(x_1+\sqrt{2}y_1)=(x_2+x_1)+\sqrt{2}(y_2+y_1)$$

The set G is closed.

2. **Associative law.** The addition of irrational numbers is associative, therefore, the set G satisfies the associative law.

3. **Identity element.** 'O' is the identity element of the given set.

4. **Inverse element.** $-x-2\sqrt{y}$ is the inverse of the element $x+\sqrt{2}y$ because

$$(x+\sqrt{2}y)+(-x-\sqrt{2}y)=(-x-\sqrt{2}y)+(x+\sqrt{2}y)=0$$

5. **Commutative law.** The addition of any two irrational numbers is commutative, the set G satisfies the commutative law.

Hence $G=\{x+\sqrt{2}y : x, y\in Q\}$

forms an abelian group.

Example 6. *G is a group in which every element is its own inverse, so that, for example,* $x^2=y^2=(xy)^2=e$. *Show that* $xy=yx$.

(C.A. Intermediate May, 1981)

Solution. We have

$$x^2=e\Rightarrow xx=e, \text{ i.e., } x=x^{-1} \quad ...(1)$$

$$y^2=e\Rightarrow yy=e, \text{ i.e., } y=y^{-1} \quad ...(2)$$

$$(xy)^2=e\Rightarrow (xy)\,(xy)=e$$

i.e.,
$$(xy)=(xy)^{-1}$$
$$=y^{-1}.x^{-1}$$
$$=yx \text{ [From (1) and (2)]}$$

$\therefore$
$$xy=yx$$

5·7. MODULO

We are familiar with the operations on sets which are concerned with union, intersection or complementation. We now take up some new type of operations on sets. Let us take a set $G=\{0, 1, 2, 3, 4, 5\}$. We have to define the operation which we want to have on this set. The formal instruction is like this :

"Select any element of the set, say 4 and then select another element of the set, say 5 ; with this ordered pair of elements the operation

associates exactly one number according to the rule ; determine the sum of 4 and 5 ; divide the sum by 5 and find the number."

Let this remainder be the number that the operation associates with 4 and 5. This is indicated by $4 \oplus_5 5 = 4$. We can say that the remainder 4 associates 4 and 5 through a certain operation. Similarly other associations can be expressed as $2 \oplus_5 3 = 0$, $3 \oplus_5 4 = 2$, etc. The results of the operation $\oplus_5$ on a set of element {0, 1, 2, 3, 4, 5} has been shown in the tabular form :

$\oplus_5$	0	1	2	3	4	5
0	0	1	2	3	4	0
1	1	2	3	4	0	1
2	2	3	4	0	1	2
3	3	4	0	1	2	3
4	4	0	1	2	3	4
5	0	1	2	3	4	0

The above table shows a binary composition with the addition operation on a set of numbers {0, 1, 2, 3, 4, 5} and the composition is called addition modulo 5.

Definition of Addition modulo m. Let a and b be any two integers and m be a positive integer. Then the addition modulo m denoted by $a \oplus_m b$ is defined as

$$a \oplus_m b = r,$$

where r is the least non-negative remainder obtained by dividing the ordinary sum of a and b, *viz.*, $a+b$ by m. In other words, *for finding* $a \oplus_m b$, *we add a and b in the ordinary way and then from the sum we remove the integral multiples of m in such a manner that the remainder r left out is either zero or a positive integer less than m, e.g.*,

1. $9 \oplus_5 6 = 0$, since $9+6=5(3)$
2. $12 \oplus_7 8 = 6$, since $12+8=7(2)+6$
3. $-10 \oplus_4 4 = 2$, since $-10+4=(-2)4+2$

Multiplication modulo p. The multiplication modulo p of any two integers a and b is denoted by $a \odot_p b$ and is defined as

$$a \oplus_p b = r,$$

where r is the least non-negative remainder obtained by dividing the ordinary product of ab by p. In other words, *we find ordinary product of two numbers a and b, viz., ab and from this product we remove the multiples of p in such a way that remainder r left out is a positive integer less than p, e.g.*,

1. $4 \odot_6 7 = 4$, since $4 \times 7 = 6(4)+4$,
2. $8 \odot_6 5 = 4$, since $8 \times 5 = 6(6)+4$.

Example 7. *Prove that the set* $G = \{0, 1, 2, 3, 4, 5\}$ *is a finite Abelian group under ordinary addition with modulo 6 as the composition.*

Solution. Here we shall make the following composition table.

$\oplus_6$ /	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

(*i*) *Closure property.* The system is closed under $\oplus$ because all the elements resulting from the operation $\oplus_6$ in the set {0, 1, 2, 3, 4, 5} are also the elements of the set.

(*ii*) *Associative.* The composition is associative because $(a \cdot b)+c$ and $a+(b+c)$ both will have the same positive remainder when divided by 6, *e.g.*,

$$(3\oplus_6 4)\oplus_6 5=0=3\oplus_6(4\oplus_6 5)$$

(*iii*) *Identity element.* Clearly the element 0 of the set is the identity element for the composition.

(*iv*) *Inverse element.* In order to find the inverse of element, say 5, look to the row headed by 5 where 0 is there, then the element at the head of this column, *i.e.*, 1 will be the inverse of 5. Similarly we can show that the inverse of the elements 0, 1, 2, 3, 4, 5 are 0 5, 4, 3, 2, 1 respectively.

(*v*) *Commutative.* It can be seen from the table that

$$a\oplus_6 b=b\oplus_6 a \text{ for any } a, b\in G$$

Hence the set G under ordinary addition with modulo 6 is a finite Abelian group.

Example 8. *Is the set {1, 2, 3, 4, 5, 6, 7} a group under addition modulo 8.*

Solution.

$\oplus_8$	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
4	5	6	7	0	1	2	3
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

The abobe operation is not a binary operation because 0 or additive identity element does not belong to the set.

Example 9. *On the set Z, we introduce a operation * defined as follows :*

$$a*b=a+b+1, \text{ where } + \text{ is the ordinary addition.}$$

Show that (Z,) is a group.*

Solution. We list the following properties to show that $(Z, *)$ is group.

(*i*) *Closure.* If a, b are any two elements from $(Z, *)$ then

$$a * b = a+b+1 \in Z$$

(*ii*) *Associativity.* If a, b, c, are any three elements from $(Z, *)$ then

$$\begin{aligned}(a*b)*c=(a+b+1)* \quad c &=(a+b+1)+c+1\\ &=(a+b+1+c)+1\\ &=(a+b+c+1)+1\\ &=(a+b+c)+1+1\\ &=(a+b+c)+2\end{aligned}$$

Similary, it can be shown that

$$a*(b*c)=(a+b+c)+2$$

$$\therefore \quad (a*b)*c=a*(b*c)$$

(*iii*) *Identity.* If e is the identity for $(Z,*)$, then we must have

$$a*e=a \forall a \in Z$$

$$\Rightarrow \quad a+e+1=a$$

$$\Rightarrow \quad e+1=0, \text{ where 0 is the additive identity of } Z$$

$$\Rightarrow \quad e=-1, \text{ which is an element from } (Z, *).$$

Thus -1 is the identity for $(Z,*)$

(*iv*) *Inverse.* If b is the inverse of a, then

$$a*b=e$$

$$\Rightarrow \quad a+b+1=-1$$

$$\Rightarrow \quad a+b=-2$$

$$\Rightarrow \quad b=-2-a$$

Thus $-2-a$ is an inverse of all $a \in Z$

Hence $(Z,*)$ forms a group.

Example 10. *Prove that the set* $\{1, 2, 3, 4, 5, 6\}$ *is a finite Abelian oup of order 6 under multiplication modulo 7.*

Solution. The composition table is shown below,

$\odot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(*i*) *Closure property.* From the composition table, we can see that all the entries are the elements of the set.

(*ii*) *Associative law.* We can verify for any three elements of the above set,

$$(a \odot_7 b) \odot_7 c = a \odot_7 (b \odot_7 c)$$

e.g., $(3 \odot_7 5) \odot_7 4 = 4 = 3 \odot_7 (5 \odot_7 4)$

(*iii*) *Identity element.* Clearly $1 \in G$ is the identity, element, since

$$1 \odot_7 a = a = a \odot_7 1 \qquad (a = 1, 2, ., 6)$$

(*iv*) *Existence of inverse.* The inverses of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6, respectively.

(*v*) *Commutative law.* The corresponding rows and columns in the composition table are identical, as such the commutative law holds good.

Hence $(G, \odot_7)$ is a finite Abelian group of order 6 under multiplication modulo 7.

Example 11. *State giving proofs or counter examples, whether the following statements are true or false.*

(*i*) *Given a set S and a commutative binary operation 0 on it, then* $a0(b0c) = (c0b)0a$ *for all a, b, c in S.*

(*ii*) *A group may have more than one identity element.*

(*iii*) *Every finite group of three elements is Abelian.*

(*iv*) *A set* $A = \{1, 2, \ldots\ldots, n-1\}$ *with the operation of multiplication (modulo n) forms a group for all positive integral values of n.*

Solution.

(*i*) True, using commutative property along with associativity.

$$a0(b0c) = (b0c)0a \qquad \text{(associativity)}$$
$$= (c0b)0a \qquad \text{(commutativity)}$$

(*ii*) No, it cannot have two identity elements.

(*iii*) True, a group of three elements say $\{e, a, b\}$ is an Abelian as shown below :

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(*a*) In the above composition, e is an identity element. Since

$$a*e = a, \; b*c = b$$

(*b*) The inverse of a is b because

$$a_* b = e = b_* a$$

(*c*) The composition is commutative, since

$$a_* b = b_* a$$

(*d*) The composition is associative, since

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

(*iv*) True, a set of positive integers given with modulo n has a multiplicative inverse.

5·8 RINGS $(R, \oplus, \odot)$

The algebraic structure of rings has two binary compositions *viz.*, $\oplus$ and $\odot$. We recall that the groups dealt earlier had only one binary operation either $\oplus$ or $\odot$. As regards notations there is no rigidity, some authors use $*$ for $\oplus$ and Δ for $\odot$. It is common practice to use the symbols '$+$' and '$.$' respectively for $*$ and Δ and call these compositions *addition* and *multiplication* respectively. An operation is known by its properties.

We can now define a ring as a non-empty set R with two binary operations $\oplus$ and $\odot$ and indicate it as $(R, \oplus, \odot)$ if the following eight properties hold;

$\mathbf{R}_1$. *Closure law for* $\oplus$:

$$a \oplus b \in R, \forall\ a, b \in R$$

$\mathbf{R}_2$. *Associative law for* $\oplus$:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) \forall a, b, c \in R$$

$\mathbf{R}_3$. *Identity element for* $\oplus$. There exists an element $0 \in R$, called the identity of the composition such that

$$a \oplus 0 = a = 0 \oplus a$$

0, the identity of R for the composition $\oplus$, is called the zero of the ring.

$\mathbf{R}_4$. *Inverse element for* $\oplus$. For every element $a \in R$, there exists an element $b \in R$ such that

$$a \oplus b = 0 = b \oplus a$$

Then b is called inverse of a. The inverse of any element a will be denoted by $(-a)$.

$\mathbf{R}_5$. *Commutative law for* $\oplus$. The composition $\oplus$ is commutative in R, *i.e.*,

$$a \oplus b = b \oplus a, \forall\ a, b \in R$$

$\mathbf{R}_6$. *Closure law for* $\odot$:

$$a \odot b \in R, \forall\ a, b \in R$$

$\mathbf{R}_7$. *Associative law for* $\odot$:

$$(a \odot b) \odot c = a \odot (b \odot c), \forall\ a, b, c \in R$$

It may be noted that for ring there is no necessity for the existence of multiplicative identity, inverse and commutativity.

$\mathbf{R}_8$. *Distributive Laws.* The composition $\odot$ is distributive with respect to $\oplus$, *i.e.*, for all $a, b, c \in R$

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

and

$$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$$

In other words, we may define a ring as follows :

(*i*) R is an Abelian group under $\oplus$,

(*ii*) R is a semi-group under $\odot$, and

(*iii*) $\odot$ is distributive with respect to $\oplus$ in R.

Illustrations 1. The set I of all integers with ordinary addition and multiplication composition is not a ring.

2. The set of natural numbers with ordinary addition and multiplication composition is a ring.

3. The set consisting of the two elements 0, 1 with the following addition and multiplication composition tables :

$\oplus$	0	1
0	0	1
1	1	0

and

$\odot$	0	1
0	0	0
1	0	1

is a ring.

4. The following two tables have been prepared for both the operations on a set of integers {0, 1, 2, 3, 4}. The modulo in this case will be 5 so the ring can formally be called $\{S_1 \oplus_5, \odot_5\}$. The respective tables of the two operations on the same set are :

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Example 12. *State if the set compositions $S=\{a, b\}$ with addition and multiplication defind as follows is of a ring.*

(*i*)

$\oplus$	a	b
a	a	b
b	b	a

(*ii*)

$\odot$	a	b
a	a	a
b	a	b

Solution. In the (*i*) a is the additive identity and b is the additive inverse.

Similarly, in (*ii*) both the closure and associative properties are there. The latter for example is

$$(a \odot b) \odot a = a \odot (b \odot a) = a$$

On checking all the properties of the ring we find that it is a ring.

Example 13. *State if the set $R=\{a, b, c, d\}$ with the operations defined as follows is of a ring :*

$\oplus$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\odot$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

Solution. The set $R=\{a, b, c, d\}$ constitutes a composition of ring because all the eight properties listed above are satisfied. It can be checked taking note of the fact that a is an identity element in (i) and there is no need of identity element for $\odot$.

Sub-Rings. The sub-ring is the ring composition formed by a subset of a set with a ring composition. As shown above $S=\{a, b\}$ constituted a sub-ring of the ring set of $R=\{a, b, c, d\}$.

Commutative Ring. Ring for which multiplication composition is commutative is called commutative ring In other words, a ring $(R, \oplus, \odot)$ is said to be commutative if the $\odot$ composition in R is commutative, *i.e.*,

$$a\odot b=b\odot a \quad \forall\ a, b\in R$$

Ring with Unity. A ring $(R, \oplus, \odot)$ is said to be a ring with unity if it contains an element denoted by 1 such that

$$1\odot a=a=a\odot 1 \qquad \forall\ a\in R$$

For example the ring of all integers is a ring with unity, 1 being the unity of the ring.

Rings with Zero Divisors. In a ring R an element $a\neq 0$ of R is called a divisor of zero if there exists element $b\neq 0$ of R such that

$$a\odot b=0 \text{ and } b\odot a=0.$$

For example, rings I, Q, R, C have no divisors of zero, *i.e.*, have no non-zero element a where $a\odot b=0$ for some $b\odot 0$. In fact $a\odot b=0$ always implies that $a=0$ or $b=0$.

We can prove that if R is a ring with a zero divisor then for all $a\in R$. $a\odot 0=0\odot a=0$.

Since $\quad a\oplus 0=a$

$\therefore \quad a\odot a=(a\oplus 0)\odot a=(a\odot a)\oplus(0\odot a)$

But $\quad a\odot a=(a\odot a)\oplus 0$

Hence $(a\odot a)\oplus(0\odot a)=(a\odot a)\oplus 0$

$\Rightarrow \quad 0\odot a=0$ (Cancellation law)

Similarly $\quad a\odot a=a\odot(a\oplus 0)=(a\odot a)\oplus(a\odot 0)$

Also $\quad a\bar{\odot} a=(aa\odot)\oplus 0$

$\therefore \quad (a\odot a)\oplus(a\odot 0)=(a\odot a)\oplus 0$

By cancellation law

$$a\odot 0=0$$

Integral Domain. An integral Domain is a commutative ring D with unity but having no divisors of zero. For example, the ring I, Q, R and C are all integral domains.

The cancellation law for addition holds in every ring since every element has its inverse. The cancellation law of multiplication holds in every integral domain, as shown below :

If $\quad a\odot c=b\odot c \quad$ and $\quad c\neq 0$

then $\quad a=b$

We have $a \odot c = b \odot c = (a-b) \odot c = 0$

Now since D has no divisor of zero

$$a-b=0 \Rightarrow a=b$$

Example 14. *Prove that if R is a ring with zero element z, then for all $a \in R$, $a \,.\, z = z \,.\, a = z$.*

Solution. Since $a+z=a$

then $$a \,.\, a=(a+z).+a=(a \,.\, a)+z \,.\, a$$

Hence $(a \,.\, a)+z \,.\, a=(a \,.\, a)+z$

Now using the cancellation law, we have

$$z \,.\, a=z$$

Similarly
$$\begin{aligned} a \,.\, a &= a \,.\, (a+z) \\ &= a \,.\, a + a \,.\, z \\ &= a \,.\, z \\ &= z \end{aligned}$$

Example 15. *The two binary compositions $*$, $\triangle$ in the set of I of all integers are defined as follows :*

$$a * b = a+b-1$$

$$a \triangle b = a+b-ab, \text{ for all } a, b \in I$$

Show that $(I, *, \triangle)$ is a ring.

(C.A. Entrance June 1984)

Solution. The set of all integers, I, is a ring for the given two binary compositions $*$, $\triangle$ because.

1. Closure for $*$. The composition is closed because

$$a * b = a+b-1 \in I$$

and
$$b * a = b+a-1 \in I,$$

for all $a, b \in I$.

2. Associative for $*$ The composition is associative because

$$a*(b*c)=(a*b)*c \text{ for all } a, b, c \in I.$$

$\because$
$$\begin{aligned} a * (b * c) &= a * (b+c-1) = a+(b+c-1)-1 \\ &= a+b+c-2 \end{aligned}$$

and
$$\begin{aligned} (a * b) * c &= (a+b-1) * c = (a+b-1)+c-1 \\ &= a+b+c-2 \end{aligned}$$

3. Identity element for $*$. There exists an element $1 \in I$ such that

$$a * 1 = 1 * a = a, \text{ for all } a \in I.$$

4. Inverse element for $*$ There exists an element $(2-a) \in I$ such that

$$a * (2-a) = (2-a) * a = 1, \text{ for all } a \in I.$$

5. **Commutative for *.** The composition is commutative because

$$a * b = b * a,$$

for all $a, b \in I$.

6. **Closure for $\triangle$.** The composition is closed because

$$a \triangle b = a + b - ab \in I$$

and $$b \triangle a = b + a - ba \in I$$

for all $a, b \in I$.

7. **Associative for $\triangle$.** The composition is associative because

$$\begin{aligned} a \triangle (b \triangle c) &= a \triangle (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - ab - ac - bc + abc \end{aligned}$$

$$\begin{aligned} (a \triangle b) \triangle c &= (a + b - ab) \triangle c \\ &= (a + b - ab) + c - (a + b - ab).\ c \\ &= a + b + c - ab - ac - bc + abc. \end{aligned}$$

for all $a, b, c \in I$.

8. **Distributive Laws** The composition * is distributive with respect to $\triangle$, *i.e.*,

$$a * (b \triangle c) = (a * b) \triangle (a * c)$$

$$(b \triangle c) * a = (b * a) \triangle (c * a)$$

for all $a, b, c \in I$.

Therefore $(I, *, \triangle)$ is a ring.

5·9. FIELDS $(F, \oplus, \odot)$

Fields are special types of rings. They also have an algebraic structure with two binary operations, $\oplus$ and $\odot$.

Let $F = \{a, b, c\}$ be a non-empty set with two binary compositions $\oplus$ and $\odot$ If F atisfies the following properties then it is called a field $(F, \oplus, \odot)$

$\mathbf{F}_1$. *Closure law for* $\oplus$: $a \oplus b \in F$, $\forall\, a, b \in F$

$\mathbf{F}_2$. *Associative law for* $\oplus$:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c),\ \forall\ a, b, c \in F$$

$\mathbf{F}_3$. *Identity law for* $\oplus$: There exists an element 0 in F, called the identity for tie composition $\oplus$ such that

$$0 \oplus a = a = a \oplus 0,\ \forall\ a \in F$$

$\mathbf{F}_4$. *Inverse law for* $\oplus$: There exists an element $-a$ in F, called the negative of a, such that

$$(-a) \oplus a = 0 = a \oplus (-a),\ \forall\ a \in F$$

$\mathbf{F}_5$ *Commutative law for* $\oplus$:

$$a \oplus b = b \oplus a,\ \forall\ a,\ b \in F$$

$\mathbf{F}_6$. *Closure law for* $\odot$:

$$a \odot b \in F, \ \forall \ a, b \in F$$

$\mathbf{F}_7$. *Associative law for* $\odot$:

$$(a \odot b) \odot c = a \odot (b \odot c), \ \forall \ a, b, c \in F$$

$\mathbf{F}_8$. *Identity law for* $\odot$: There exists an element 1 in F such that

$$a \odot 1 = a = 1 \odot a, \ \forall \ a \in F$$

$\mathbf{F}_9$. *Inverse law for* $\odot$: For every non-zero element a in F, there exists an element a^{-1} in F called the inverse of a such that

$$a^{-1} \odot a = 1 = a \odot a^{-1}$$

$\mathbf{F}_{10}$. *Commutative law for* $\odot$:

$$a \odot b = b \odot a, \ \forall \ a, b \in F$$

$\mathbf{F}_{11}$. *Distributive laws* : For all $a, b, c \in F$,

$$a \odot (b \oplus c) = (a \odot b) \oplus (c \odot c)$$

$$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$$

In other words, a ring $(F, \oplus, \odot)$ is called a field if it has the following three additional properties :

(*i*) it is commutative, (*ii*) it has a unity and

(*iii*) it is such that every non-zero element has an inverse for the composition $\odot$ in F.

Illustrations. 1. The ring of rational, real and complex numbers with respect to the operations of addition and multiplication is a field.

We are giving below a list of number sets which can have the compositions of a field.

$\{Q, \oplus, \odot\}$	sets of rational numbers
$\{R, \oplus, \odot\}$	set of real numbers
$\{C, \oplus, \odot\}$	set of complex numbers.

2. The set I of all integers forms a ring with respect to addition and multiplication. We can say $(I, \oplus, \odot)$ is a ring. But this ring is not field because with the exception of -1 and 1 no other element of 1 has an inverse with respect to multiplication.

3. The following composition of a set $S = \{a, b, c, d, e, f, g, h\}$ with addition and multiplication as compositions defined by the following, is a field.

$\oplus$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	d	c	f	e	h	g
c	c	d	a	b	g	h	e	f
d	d	c	b	a	h	g	f	e
e	e	f	g	h	a	b	c	d
f	f	e	h	g	b	a	d	c
g	g	h	e	f	c	d	a	b
h	h	g	f	e	d	c	b	a

$\odot$	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	c	d	e	f	g	h
c	a	c	h	f	g	e	b	d
d	a	d	f	g	c	b	h	e
e	a	e	g	c	d	h	f	b
f	a	f	e	b	h	c	d	g
g	a	g	b	h	f	d	e	c
h	a	h	d	e	b	g	c	f

The various properties of the field can be verified. It may be remembered that a is an additive unity or zero element and is a multiplicative unity or 1. Also non-zero elements of the set form an Abelian multiplicative group.

Example 16. *Define a ring and a field. Give an example of ring which is not a field.*

Solution. For definitions see the tezt. The set

$$I=\{\ldots, -3, -2, 0, 1, 2, 3, \ldots\}$$

constitutes a ring but not a field because multiplicative inverses are not there.

Example 17. (*a*) *Define a field and give two examples of a field.* (*b*) *Given that a, b are two members of a field, show that*

$$a(-b)=-(ab) \quad \textit{and} \quad (-a)(-b)=ab$$

Solution. (*a*) Definition and properties are given in the text. The set of rational (Q) and real (R) numbers constitute the compositions of a field.

(*b*) Let there be an element c such that $b+c=0$

So that $c=-b$

But we have $0=a0=a(b+c)=ab+ac$

$\Rightarrow$ $ac=-(ab)$

$\Rightarrow$ $a(-b)=-(ab)$

and $(-a)(-b)=-(a)(-b)=[a(b)]=ab$

EXERCISES

1. (*a*) Define a 'group'. Give one example each of a finite and an infinite group.

(*b*) Define a 'group. When is it Abelian ? Show that the set of all integers, positive or negative, including zero with additive binary operation is an infinite Abelian group.

(*c*) Define a group and examine whether the set N of rational numbers is a group with respect to addition.

(*C.A. Intermediate Nov. 1982*)

2. Is the set of all positive rational numbers, a group in multiplication ? What would be the case if it is a set of all non-zero rational numbers ?

3. (*i*) State if the following is a group in multiplication :

$$S=\{x : x\in R \wedge x>0\}$$

(*ii*) State if the following is a group in addition and multiplication;

$$R=\{2x : x\in Z\}$$

4. State with reasons which of the following sets form a group : In addition

(*i*) $G=\{x : x\in I, x<0\}$

(*ii*) $G=\{3x : x\in I\}$

In multiplication

(*iii*) $G=\{x : x\in I,$ is odd$\}$

(*iv*) $G=\{-2,-1, 1, 2\}$

5. (*a*) Define ring and give two examples.

(*b*) Define a field and give two examples.

6. (*a*) State whether $(N, \oplus, \odot)$ is a ring where N stands for set of natural numbers.

(*b*) State formally the property of a division ring.

7. Determine whether each of the following sets is a ring for ordinary addition and multiplication. In each case justify your answer by proof or by counter-examples :

(*i*) The set of all positive integers,

(*ii*) the set $\{3n : n\in Z\}$.

(*iii*) $\{a+ib : a, b\in Q\}$, and

(*iv*) $\{a+b\sqrt{2} : a, b\in Z\}$.

8. Let * be an operation on the set of real numbers defined by

$$a * b=a+b+a^2b, \forall\ a,b\in R$$

Show that $(R, *)$ is not a group.

9. Prove that the set

$$G=\{\ ..,\ 2^{-4},\ 2^{-3},\ 2^{-2}.\ 2^{-1},\ 1,\ 2,\ 2^2,\ 2^3,\ 2^4,\ .\ \}$$

forms an infinite Abelian group *w.r.t.* multiplication.

10. Prove that the set Q of all rational numbers other that -1 with the operation defind by

$$a * b=a+b+ab \forall a, b\in Q.$$

form a group with respect to binary operation *

11. Prove that the following sets are groups :

(*i*) $G=\{0, 3, 6, 9\}$ for addition modulo 9,

(*ii*) $G=\{1, 5, 7, 11\}$ for multiplication modulo 12.

12. Show that the numbers 1, 2, 3, 4, 6 form a group with respect to the operation of multiplication modulo 7

13. Define an Abelian group.

In the set $S=\{1, 2, 3, 4\}$, let $\odot$ be the composition 'multiplication modulo 5'. Prove that $(S, \odot)$ is an Abelian group.

14. (*a*) Prove that the following operation table defines a group under*.

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(*b*) Show that

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

is group under*.

15. State whether a field possesses more properties than a ring.

16. Do the following sets constitute a field ?
   (*i*) The set of all rational numbers.
   (*ii*) The set of all integers.
   (*iii*) The set of all real numbers.
   (*iv*) The set of all complex numbers.

17. Show that $\{0, 1\}, \oplus, \odot)$ is a field if the compositions $\oplus$, $\odot$ are given by the tables :

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	1
1	0	1

18. Let R be the set of ordered pairs (a, b) of the real numbers. Let addition and multiplication compositions be defined as

$$(a, b)+(c, d)=(a+c, b+d) \quad \text{and}$$
$$(a, b)(c, d)=(ac-bd, bc+ad)$$

Show that R is a field.

19. Prove that the set of all real numbers of the form $a+b\sqrt{2}$, where a and b are rationals forms a field under addition and multiplication.

20. Show that the set $\{a, b, c, d\}$ in which addition and multiplication are defined by the following tables is a finite field.

$\oplus$	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*a*	*d*	*c*
c	*c*	*d*	*a*	*b*
d	*d*	*c*	*b*	*a*

$\odot$	*a*	*b*	*c*	*d*
a	*a*	*a*	*a*	*a*
b	*a*	*b*	*c*	*d*
c	*a*	*c*	*d*	*b*
d	*a*	*d*	*b*	*c*

21. Prove that the set of integers $I=\{0, 1, 2, 3, 4\}$ with addition modulo 5 and multiplication modulo 5 is a composition of a field.

22. Let us define to binary compositions*, $\triangle$ in the set Z of all integers as follows :

$$a * b = a+b-1$$
$$a \triangle b = a+ab-ab \quad \forall \; a, \; b \in Z$$

Show that $(Z, *, \triangle)$ is a commutative ring with unity. What is the zero of this ring ? What is the unity of this ring ?

ANSWERS

1. (*a*) A set of integers forms an infinite group. The following is an example of a group composition with a finite set $S=\{s, m, t, r\}$ which is an Abelian group.

*	s	m	t	r
m	s	m	t	r
s	m	t	r	s
t	t	r	s	m
r	r	s	m	t

(*b*) See the text.

2. No, for the first part, and yes, for the second part.

3. (*i*) Yes, it is set a of non-zero real numbers.
(*ii*) Yes in addition and not in multiplication.

4. (*i*) No, as inverse of each integer is positive,
(*ii*) Yes.
(*iii*) No, as inverse of each element is not there.
(*iv*) No, as product of -2 and 2 is not there.

5. (*a*) The set of integers, real, rational or complex numbers is a ring.

(*b*) The set of real, rational or complex numbers constitute ring.

6. (*a*) No, the additive inverse $-a$ for a is not there.
(*b*) See text.

7. In all except the (*i*) for the reason given in 6(*a*) above

15 Yes.

16. (*i*) Yes, (*ii*) No, (*iii*) Yes. (*iv*) Yes.

21. Hint. If we denote the two compositions by $\oplus_5$ and $\odot_5$ respectively, the composition tables for the two compositions are as shown below.

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the table, we conclude that

(*i*) F is closed under $\oplus_5$

(*ii*) $\odot_5$ is associative in F

(*iii*) 0 is the additive identity

(*iv*) The additive inverse of 0, 1, 2, 3, 4, are 0, 4, 3, 2, 1 respectively.

(*v*) $\oplus_5$ is commutative as the table is symmetric in rows and columns.

(*vi*) F is closed with respect to $\odot_5$

(*vii*) $\odot_5$ is associative in F.

(*viii*) 1 is the multiplicative identity

(*ix*) The inverse of the non-zero elements $1,2,3,4 \in F$ are 4, 3, 2, 1 respectively.

(*x*) $\odot_5$ is commutative as the table is symmetric in rows and columns.

(*xi*) Distributive law holds good in F as

$$a \odot_5 (b \oplus_5 c) = (a \odot_5 b) \oplus_5 (a \odot_5 c)$$

Similarly, $(b \oplus_5 c) \odot_5 a) = (b \odot_5 a) \oplus_5 (c \odot_5 a)$

Hence $(F, \oplus_5, \odot_5)$ is field.

22. **Hint.** (*i*) It can be shown that the set Z is an Abelian group for the composition * defined as given.

(*ii*) *The composition* $\triangle$ *is binary and associative*

Since $(a \triangle b) \triangle = (a+b-ab) \triangle c$

$$= a+b-ab+c-ac-bc+abc$$

Similarly $a \triangle (b \triangle c) = a \triangle (b+c-bc) = a+b+c-bc-ab-ac+abc$

(*iii*) $\triangle$ *is distributive over* *

$\because$ $a \triangle (b * c) = a \triangle (b+c-1)$

$\therefore$ $= a+b+c-1-a(b+c-1) = a+b+c-1-ab-ac+a$

Again $(a \triangle b) * (a \triangle c) = (a+b-ab) * (a+c-ac)$

$$= a+b-ab+a+c-ac-1$$

$\therefore$ $a \triangle (b * c) = (a \triangle b) * (a \triangle c)$

(*iv*) *Commutative*.

$\therefore$ $a \triangle b = a+b-ab = b+a-ba = b \triangle a$

(*v*) *Unity* :

$$a \triangle 0 = a+0-a \,.\, 0 = a$$

$$0 \triangle a = 0+a-0 \,.\, a = a$$

$\therefore$ $a \triangle 0 = a = 0 \triangle c$

Hence, the set is a commutative ring with unity for the two compositions defined as given.