5.4 RING AND FIELD

5.4.1 Ring.

A non-empty set R with two binary operations $\oplus$ and $\odot$ respectively is called ring if the following axioms are satisfied :

I. $(R, \oplus)$ is an abelian group. That is

(i) $a \oplus b \in R \quad \forall\, a, b \in R$

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

(iii) there exist an element, denoted by 0 in R such that $a \oplus 0 = a \quad \forall\, a \in R$.

(iv) to each element a in R there exists an element $-a$ in R such that $a \oplus -a = -a \oplus a = 0$

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

II. $(R, \odot)$ is a semigroup. That is,

(i) $a \odot b \in R \quad \forall\, a, b \in R$

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

III. The composition $\odot$ is distributive i.e. $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ and $(b \oplus c) \odot a = b \odot a \oplus c \odot a \quad \forall\, a, b, c \in R$.

Note. (1) *We say $(R, \oplus, \odot)$ is a ring*

(2) *The two binary operations denoted by $\oplus$ and $\odot$ are not usual addition or multiplication in general.*

(3) *In the future part of the text we use + (called 'addition') and · (called 'multiplication') in place of $\oplus$ and $\odot$ respectively.*

(4) *The identity element w.r.t the binary operation, + in R i.e. 0 is called* ***additive identity element*** *or the* ***zero element*** *in R.*

(5) $-a$ is called *additive inverse* of a.

Illustration. Prove that the set of all matrices of size 2×2 is a Ring with respect to matrix addition and matrix multilication.

Solution. Let S = set of all matrices of size 2×2.

I. We shall show $(S,+)$ is an abelian group:

(i) If A and B be two 2×2 matrices then their sum $A+B$ is also 2×2 matrix.

$\therefore A,B\in S\Rightarrow A+B\in S$

(ii) $A+(B+C)=(A+B)+C$ is well known for matrices.

(iii) The null matrix $O=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\in S$ and we know $A+O=A$ for any 2×2 matrix A. So S has additive identity element 0.

(iv) If $A=\begin{pmatrix}x_1 & x_2\\ y_1 & y_2\end{pmatrix}$ then $-A=\begin{pmatrix}-x_1 & -x_2\\ -y_1 & -y_2\end{pmatrix}\in S$ also Then we see $A+(-A)=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}=0$. Thus A has additive inverse in S.

(v) $A+B=B+A$ is well known for matrix. Thus S is abetion group under $+$.

II. (i) If A and B are two matrices of size 2×2 then AB is also a 2×2 matrices. Thus $A,B\in S$ implies $A,B\in S$.

(ii) $A(BC)=(AB)C$ is well known.

Thus S is a semi group w.r.t matrix multilication,

III. $A(B+C)=AB+AC$ and $(B+C)A=BA+CA$ are established rule for matrix.

Thus all the Axioms of Ring are satisfied by S. So, S is Ring.

Ring with Unit Element.

If in a ring R there exists an element denoted by 1 such that $1\cdot a=a=a\cdot1\ \forall\ a\in R$ then R is called a ring with *unit* element.

Obviously 1 is the *multiplicative identity* of R.

Commutative Ring.

A ring R is said to be commutative if $a \cdot b = b \cdot a$ for all a, b in R.

Illustration. (1) Consider the set Z of all integers. Obviously $(Z,+)$ is a abelian group and $(Z,\cdot)$ is a semi group. Also the multiplication of integers is distributive w.r.t addition of integers i.e.

$a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$, $\forall a,b,c \in Z$

Hence $(Z,+,\cdot)$ is ring.

Since $a \cdot b = b \cdot a \ \forall\, a,b \in Z$, so the ring is commutative. The integer 0 is the zero element of this ring.

Since $1 \in Z$ and $a \cdot 1 = a$ for all a so this is a ring with identity element 1.

(2) Let Z_n be the set of residue classes modulo n where n is a positive integer. Then $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$. Obviously $(Z_n,+)$ is a commutative group where '+' denotes addition of residue class. Also it can be easily verify that $(Z_n, \cdot)$ is a commutative semigroup with unit element $\overline{1}$ where . denotes multiplication of residue class. Again the distributive law holds for this operation multiplication. Therefor $(Z_n,+,\cdot)$ forms a commutative ring and is known as *Ring of integer modulo n.*

5.4.2 Properties of Ring.

Since ring is a group w.r.t + so all the properties of group are valid in ring w.r.t the binary operation +, zero element 0. For instance " the zero element 0 in a ring is unique", " the cancellation property $a+b = a+c \Rightarrow b = c$" are valid in a ring R.

Other Properties of Ring

In a ring $(R,+,\cdot)$

(i) $a \cdot 0 = 0 \cdot a = 0$ for all a in R

(ii) $(-a) \cdot (b) = a \cdot (-b) = -(a \cdot b)$ for all a, b in R

(iii) $(-a) \cdot (-b) = a \cdot b$ for all a, b in R. [*W.B.U.T. 2003*]

Proof. (i) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$

or, $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$ or, $0 = a \cdot 0$ [by cancellation property]

(ii) $(-a) \cdot b + a \cdot b = (-a+a) \cdot b = 0 \cdot b = 0$

So, $(-a) \cdot b = -(a \cdot b)$

(iii) $(-a)\cdot(-b) = -\{(-a)\cdot b\}$ by property (ii)

$= -\{-(a\cdot b)\}$ by property (ii)

$= a\cdot b$ [$\because -(-x) = x$ in Ring]

Trivial and Non-Trivial Ring.

The set R consisting of a single element 0 with two binary operations defined by $0+0=0$ and $0\cdot 0=0$ is a ring. This ring is called the *Zero ring or Trivial ring.*

A ring R consisting of at least two elements is called a *non-trivial ring.*

Ring With or Without Zero Divisors.

A non-zero element a in a ring R is called a zero divisor or divisor of zero if there exist a non-zero element b in R such that $a\cdot b=0$ *or* $b\cdot a=0$. *Then R is said to be a ring with zero divisors.*

On the other hand if in a ring R, $a\cdot b=0\Rightarrow a=0$ or, $b=0$, then R is said to be a *ring without zero divisors.*

Illustration.

The ring of integers $(Z,+,\cdot)$ is a ring without zero divisors, as the product of two non-zero integers cannot be equal to the zero integer.

Cancellation Laws in a Ring.

Cancellation laws hold in a ring if

(i) $a\neq 0$ and $a\cdot b=a\cdot c\Rightarrow b=c$

and (ii) $a\neq 0$ and $b\cdot a=c\cdot a\Rightarrow b=c$ $\forall$ $a,b,c\in R$

Theorem. *A* ring R satisfies cancellation laws if and only if R is without zero divisor. [*W.B.U.T. 2004*]

Proof. Let R be without zero divisor.

Let $a\neq 0$ belongs to R. Now,

$a\cdot b=a\cdot c\Rightarrow a\cdot b+(-a\cdot c)=a\cdot c+(-a\cdot c)$

$\Rightarrow a\cdot b+a\cdot(-c)=0$

$\Rightarrow a\cdot(b+(-c))=0\Rightarrow b+(-c)=0\Rightarrow b=c$.

Conversely, let the cancellation property hold. Let $a\cdot b=0$ and $a\neq 0$.

Then we can write $a \cdot b = a \cdot 0$. Then by cancellation property we have $b = 0$. Similarly if $b \neq 0$ we have $a = 0$. Thus R is without zero divisor.

5.4.3. Subring.

Let $(R, +, \cdot)$ be a ring and S be a non-empty subset of R. Then S is said to be a subring of R if S is itself a ring w.r.t the operations '+' and '$\cdot$'.

Illustration. $(Z, +, \cdot)$ is a subring of $(Q, +, \cdot)$ where Q is set of all rational numbers.

Theorem 1. The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are

(i) $a \in S, b \in S \Rightarrow a - b \in S$ where $a - b = a + (-b)$ and

(ii) $a \in S, b \in S \Rightarrow a \cdot b \in S$

Proof. Beyond the scope of the book.

Illustration. Consider the ring R of all 2×2 matrices with integral elements and S be the subset of matrices of the type $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ of R.

Let $A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \in S$, $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in S$.

Then $A - B = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in S$

and $AB = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in S$

$\therefore$ S is a subring of R.

Theorem 2. The intersection of two subrings is a subring. [*W.B.U.T. 2012, 2004*]

Proof. Let S and T be two subrings of a ring R. Then $S \cap T$ is non-empty as $0 \in S \cap T$.

Let $S \cap T = \{0\}$. Then obviously $S \cap T$ is a trivial subring of R.

Next let $S \cap T \neq \{0\}$ and $a, b \in S \cap T$

Then $a \in S, a \in T, b \in S, b \in T$.

Now, $a \in S,\ b \in S \Rightarrow a-b \in S, a \cdot b \in S$, as S is a subring of R and $a \in T,\ b \in T \Rightarrow a-b \in T, a \cdot b \in T$, as T is a subring of R.

Hence $a-b \in S \cap T,\quad a \cdot b \in S \cap T$

Thus $a \in S \cap T,\ b \in S \cap T \Rightarrow a-b \in S \cap T$ and $a \cdot b \in S \cap T$

$\therefore\ S \cap T$ is a subring of R.

Corollary. An arbitrary intersection of subrings is a subring.

Note. *Union of subrings of ring need not be a subring. For example* $2Z = \{2n : n \text{ is integer}\}$ *and* $3Z = \{3n : n \text{ is integer}\}$ *are two subrings of the ring* Z *but* $2Z \cup 3Z$ *is not subrings because* $4 \in 2Z,\ 3 \in 3Z$ *but* $4-3 = 1 \notin 2Z$ *or* $3Z$.

Illustrative Examples.

Ex. 1. ***Show that the set of all rational numbers is a Ring w.r.t addition and multilication.***

(i) Is this commutative Ring?

(ii) Does this Ring have unit element?

(iii) Is this a Ring without zero divisor?

Let Q =set of all rational numbers. In an Examle of Group (Ex. 1, page 5-4) we have shown Q is Abelian group w.r.t addition.

Since product of two rational number is rational so $a.b \in Q$ if $a,b \in Q$. Since $a.(b.c) = (a.b).c$ is well known so Q is semi group w.r.t the product.

Moreover $a.(b+c) = a.b + a.c$ and $(b+c).a = b.a + c.a$ are well known also. Thus Q satisfies all the Axioms of Ring. Hence $(Q, +, \bullet)$ is a Ring.

(i) Since $a.b = b.a$ is well known so Q is commutative Ring.

(ii) $1 \in Q$ and we know $a.1 = a$. So Q has unit element which is 1.

(iii) Since $a.b = 0$ implies either $a = 0$ or $b = 0$ so Q is without zero divisor.

Ex. 2. *Prove that the set S of all real valued continuous functions defined on $[0, 1]$ is a ring. Also show that it is a ring with zero divisor.*

Let $f, g, h \in S$. Then addition and multiplication is defined as $(f+g)x = f(x)+g(x)$, $(fg)(x) = f(x)g(x)$.

(i) $f+g \in S \quad \forall f, g \in S$ as the sum of two real valued continuous function is continuous on the same interval

(ii) $[(f+g)+h](x) = (f+g)(x)+h(x) \quad = (f(x)+g(x))+h(x)$

$= f(x)+(g(x)+h(x)) \quad = f(x)+(g+h)(x) = [f+(g+h)](x)$

$\therefore (f+g)+h = f+(g+h)$

So, the operation addition is associative.

(iii) Let $\theta(x) = 0 \quad \forall x \in [0, 1]$

Then $(\theta+f)(x) = \theta(x)+f(x) = 0+f(x) = f(x)$

$\therefore \theta+f = f$. Similarly $f+\theta = f$

$\therefore \theta$ is the additive identity in S.

(iv) Now $[(-f)+f](x) = -f(x)+f(x) = 0 = \theta(x)$

$\therefore (-f)+f = \theta$ Similarly $f+(-f) = \theta$.

$\therefore -f$ is the inverse of f.

(v) Again $(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$

$\therefore \quad f+g = g+f \quad \forall \quad f, g \in S$.

So S is an additive abelian group.

(vi) $fg \in S \; \forall \; f, g \in S$, as the product of two real valued continuous function is continuous.

(vii) $[(fg)\cdot h](x) = (fg)(x) \; h(x) = [f(x)g(x)]h(x) = f(x)[g(x)\cdot h(x)]$

$= f(x)\cdot[(gh)(x)] = [f\cdot(gh)](x)$

$\therefore (fg)\cdot h = f\cdot(gh) \quad \forall f, g, h \in S$

(viii) Also we have

$$[f\cdot(g+h)](x)=f(x)\cdot(g+h)(x)=f(x)\cdot[g(x)+h(x)]$$

$$=(fg)(x)+(fh)(x)\quad=(fg+fh)\cdot(x)$$

$\therefore\ f\cdot(g+h)=fg+fh$. Similarly $(g+h)\cdot f=gf+hf$

Therefore $(S,+,\cdot)$ is a ring.

To show it is a ring with zero divisor we set the following examples.

Let $f(x)=\begin{cases}\frac{1}{3}-x, & 0\le x\le\frac{1}{3}\\ 0\ , & \frac{1}{3}\le x\le 1\end{cases}$ and $g(x)=\begin{cases}0, & 0\le x\le\frac{1}{3}\\ x-\frac{1}{3}\ , & \frac{1}{3}\le x\le 1\end{cases}$

$\therefore\ f,g\in S$ and $f\neq\theta,\ g\neq\theta$

Now $(fg)(x)=f(x)g(x)$

$$=\begin{cases}\left(\frac{1}{3}-x\right)\cdot 0, & 0\le x\le\frac{1}{3}\\ 0\cdot\left(x-\frac{1}{3}\right), & \frac{1}{3}\le x\le 1\end{cases}$$

$$=0\ \ \forall\ x\in[0,1]$$

$$=\theta(x)$$

$$\therefore\ fg=\theta$$

Hence $(S,+,\cdot)$ is a ring with zero divisors.

Ex. 3. *If $(R,+,\cdot)$ is a ring, then show that*

(i) $a\cdot(b-c)=a\cdot b-a\cdot c$

(ii) $(b-c)\cdot a=b\cdot a-c\cdot a$, where $b-c$ is defined as

$b-c=b+(-c)$

(i) We have $a\cdot(b-c)=a\cdot[b+(-c)]$

$=a\cdot b+a\cdot(-c)$ (by left distribution law)

$=a\cdot b+(-a\cdot c)$, by a previous Theorem

$=a\cdot b-a\cdot c$.

(ii) We have $(b-c)\cdot a=[b+(-c)]\cdot a$

$=b\cdot a+(-c)\cdot a=b\cdot a+(-c\cdot a)\ =b\cdot a-c\cdot a$

Ex. 4. *If $(R,+,\cdot)$ is a ring such that $a^2=a\ \forall\ a\in R$, prove that*

(i) $a+a=0\ \forall\ a\in R$

i.e. each element of R is its own additive inverse

(ii) $a+b=0\Rightarrow a=b$ [W.B.U.T. 2006]

(iii) *R is commutative ring.*

(i) $a\in R\Rightarrow a+a\in R$

$\Rightarrow(a+a)^2=a+a$, by the given condition

$\Rightarrow(a+a)\cdot(a+a)=a+a$

$\Rightarrow(a+a)\cdot a+(a+a)\cdot a=a+a$, using distributive law

$\Rightarrow\left(a^2+a^2\right)+\left(a^2+a^2\right)=a+a\ \left[\because a\cdot a=a^2\right]$

$\Rightarrow\ (a+a)+(a+a)=(a+a)+0\ \ [\because\ a+0=a]$

$\Rightarrow a+a=0$, (by left cancellation law for addition in R)

(ii) Now $a+b=0\quad\Rightarrow a+b=a+a$ [by (i)]

$\Rightarrow b=a$ (by left cancellation law)

(iii) We have, $(a+b)^2=a+b$

$\Rightarrow\ (a+b)\cdot(a+b)=a+b$

$\Rightarrow\ (a+b)\cdot a+(a+b)\cdot b=a+b$ (by distributive law)

$\Rightarrow\ a^2+b\cdot a+a\cdot b+b^2=a+b$ (by distributive law)

$\Rightarrow\ (a+b\cdot a)+(a\cdot b+b)=a+b$ (by given condition)

$\Rightarrow\ (a+b)+(b\cdot a+a\cdot b)=(a+b)+0$, using commutative and associative property

$\Rightarrow\ b\cdot a+a\cdot b=0$, by left cancellation law

$\Rightarrow\ a\cdot b=b\cdot a$ by (ii)

$\therefore\ R$ is a commutative ring.

Ex. 5. *If R be a ring and $a, b, c \in R$ then show that*

(i) $-(a+b) = -a-b$ (ii) $a-(b+c)=(a-b)-c$.

(i) We have $(a+b)+(-a-b) = a+[b+(-a-b)]$

$= a+[b+\{(-b)+(-a)\}] = a+[\{b+(-b)\}+(-a)]$

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

Hence $-(a+b) = -a-b$.

(ii) We have $a-(b+c) = a+(-b-c)$, by (i)

$= a+\{(-b)+(-c)\} = \{a+(-b)\}+(-c) = (a-b)-c$.

Ex. 6. *If in a ring R with unity, $(xy)^2 = x^2y^2 \ \forall\ x, y \in R$, then show that R is commutative.* [*W.B.U.T. 2007*]

Since the unity of ring $1 \in R$, so for all $x, y \in R$,

$[x(y+1)]^2 = x^2(y+1)^2$, by given condition

or, $[x(y+1)]\ [x(y+1)] = x^2(y+1)(y+1)$

or, $(xy+x)(xy+x) = x^2[y(y+1)+(y+1)]$, by distributive law

or, $xy(xy+x)+x(xy+x) = x^2[y^2+y+y+1]$

or, $(xy)^2+xyx+xxy+x^2 = x^2y^2+x^2y+x^2y+x^2$

or, $x^2y^2+xyx+x^2y+x^2 = x^2y^2+x^2y+x^2y+x^2$

or, $xyx+x^2y = x^2y+x^2y$

or, $xyx = x^2y$ ... (1)

Replacing x by $x+1$, we get

$(x+1)y(x+1) = (x+1)^2y$

or, $(xy+y)(x+1) = (x+1)(x+1)y$

or, $(xy+y)x+(xy+y)1 = \{x(x+1)+1(x+1)\}y$

or, $xyx+yx+xy+y = (x^2+x+x+1)y$

or, $x^2y+yx+xy+y = x^2y+xy+xy+y$, by (1)

or, $yx+xy = xy+xy$ or, $yx = xy$

Hence R is a commutative ring.

Ex. 7. *Assuming that the set R of all ordered pairs of the form (a, b) of real numbers form a group under the operation addition, show that R is a ring under the addition and multiplication of ordered pairs defined as*

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

$(a,b)\cdot(c,d)=(ac,\ bd)\ \ \forall\,(a,b)$ *and* $(c,d)\in R$

(i) Obviously $(a,b)\cdot(c,d)=(ac,bd)\in R$, as ac, bd are real numbers, so R is closed w.r.t the operation multiplication.

(ii) Let $(a,b),(c,d),(e,f)\in R$. Then

$[(a,b)\cdot(c,d)\cdot(e,f)=(ac,bd)\cdot(e,f)]$

$=((ac)e,(bd)f)=(a(ce),b(df))$

$=(a,b)\cdot(ce,df)=(a,b)\cdot[(c,d)\cdot(e,f)]$

So the operation multiplication is associative.

(iii) Now $(a,b)\cdot[(c,d)+(e,f)]\ =(a,b)\cdot(c+e,\ d+f)$

$=(a(c+e),\ b(d+f))\ \ =(ac+ae,\ bd+bf)$

$=(ac,bd)+(ae,bf)\ \ =(a,b)\cdot(c,d)+(a,b)\cdot(e,f)$

Similarly we can show that the other distributive law holds good.

Hence R is a ring w.r.t the given operations.

Ex. 8. *Prove that the subset S of all matrices of the form* $\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$ *with α,β integers, forms a subring of the ring R of all 2×2 matrices having elements as integers.*

Let $A=\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}\in S,\ B=\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}\in S$ where $\alpha_1,\alpha_2,\beta_1,\beta_2$ are integers

Then $A-B=\begin{pmatrix}\alpha_1-\alpha_2 & 0\\ 0 & \beta_1-\beta_2\end{pmatrix}\in S$, as $\alpha_1-\alpha_2,\beta_1-\beta_2$ are integers.

Also $AB=\begin{pmatrix}\alpha_1 & 0\\ 0 & \beta_1\end{pmatrix}\begin{pmatrix}\alpha_2 & 0\\ 0 & \beta_2\end{pmatrix}=\begin{pmatrix}\alpha_1\alpha_2 & 0\\ 0 & \beta_1\beta_2\end{pmatrix}\in S$, as $\alpha_1\alpha_2, \beta_1\beta_2$ are integers.

$\therefore$ S is a subring of R.

5.4.4. Integral Domain.

A ring is called an integral domain if it (i) is commutative (ii) has unit element (iii) is without zero divisors

[*W.B.U.T. 2004*]

Illustration (i) The ring of integers $(Z, +, \cdot)$ is an integral domain, as the ring is commutative with unit element 1 and $m \cdot n = 0$ implies either $m = 0$ or $n = 0$.

(ii) The ring Z_6 of integer modulo 6 is not an integral domain, as $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ and $\bar{2} \times \bar{3} = \bar{0}$, $\bar{3} \times \bar{4} = \bar{0}$ though $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$ etc.

Theorem 1. For any positive integer n, the ring Z_n of all integers modulo n is an integral domain if and only if n is prime integer.

Proof. Let Z_n be an integral domain.

Then $\bar{1} \neq \bar{0}$ in Z_n and hence $n > 1$.

If n is not prime, then $n = rs$ for some integers r, s where $1 < r, s < n$. Then $\bar{r} \cdot \bar{s} = \bar{n} = \bar{0}$ but neither $\bar{r}$ nor $\bar{s}$ is zero element of the ring Z_n which contradicts that Z_n is an integral domain. Hence n is a prime integer.

Conversly, consider Z_n for a prime intger n. Let $\bar{x}, \bar{y} \in Z_n - \{\bar{0}\}$, so $\bar{x} \neq \bar{0}, \bar{y} \neq \bar{0}$.

Now if $\bar{x} \cdot \bar{y} = \bar{0}$, then $\overline{xy} = \bar{0}$ and so xy is a divisor of n. As n is prime so we must have either x is a divisor of n or y is a divisor of n which are not possible as $\bar{x} \neq \bar{0}$, $\bar{y} \neq \bar{0}$. Hence Z_n is an integral domain.

Theorem 2. A commutative ring R with unit element is an integral domain if and only if for every non-zero element $a \in R$,

$a \cdot u = a \cdot v \Rightarrow u = v$ for all $u, v \in R$.

Proof. Beyond the scope of the book.

5.4.5. Field.

A ring R with at least two elements is called a field if it (i) is commutative (ii) has unit element (iii) is such that each non-zero element possesses multiplicative inverse.

[*W.B.U.T. 2003*]

Thus a non-empty set F with two binary operations addtion $+$ and multiplication $\cdot$ is called field if F has more than one element and the following axioms are satisfied :

I. $(F,+)$ is an abelian group

that is (i) $a+b \in F \quad \forall\, a,b \in F$

(ii) $(a+b)+c = a+(b+c) \quad \forall\, a,b,c \in F$

(iii) there exist an element, denoted by 0 in F such that $0+a = a+0 = a \quad \forall\, a \in F$.

(iv) to each element a in F there exists an element $-a$ in F such that $a+(-a) = (-a)+a = 0$.

(v) $a+b = b+a \quad \forall\, a,b \in F$

II. The subset of all non-zero elements of F is an abelian group w.r.t the operation.

that is (i) $a \cdot b \in F \quad \forall\, a,b \in F$

(ii) $(a \cdot b)\cdot c = a \cdot (b \cdot c) \quad \forall\, a,b,c \in F$

(iii) there exist an element 1 called unit element in F such that

$$a \cdot 1 = 1 \cdot a = a \quad \forall\, a \in F$$

(iv) for each non-zero element $a \in F$, there exist an element $a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

(v) $a \cdot b = b \cdot a \quad \forall\, a,b \in F$.

III. The multiplication is distributive i.e.

$a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall\, a,b,c \in F$.

Illustration. (i) The ring of rational numbers $(Q,+,\cdot)$ is a field, as it is commutative ring with unit element and each non-zero element has multiplicative inverse.

(ii) Consider the ring Z_5 of integers modulo 5 where $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. This is a commutative ring with the unit element $\bar{1}$. Also $\bar{1}\cdot\bar{1} = \bar{1}$, so, $(\bar{1})^{-1} = \bar{1}$, $\bar{2}\cdot\bar{3} = \bar{6} = \bar{1}$, so $(\bar{2})^{-1} = \bar{3}$, and $(\bar{3})^{-1} = \bar{2}$, $\bar{4}\times\bar{4} = \overline{16} = \bar{1}$, so $(\bar{4})^{-1} = \bar{4}$. Thus each non-zero element has multiplicative inverse. Hence Z_5 is a field.

Theorem 1. Every field is an integral domain.

Proof. Let $(F, +, \cdot)$ be a field. Then F is a commutative ring with unit element and each non-zero element of F has multiplicative inverse.

Let $a, b \in F$ and $ab = 0$. Also let $a \neq 0$. Then $a^{-1} \in F$

$$\therefore\ ab = 0 \Rightarrow a^{-1}\cdot(ab) = a^{-1}\cdot 0 \qquad \Rightarrow (a^{-1}a)\cdot b = 0$$

$$\Rightarrow 1\cdot b = 0 \ (\because a^{-1}a = 1) \qquad \Rightarrow b = 0$$

Next let $b \neq 0$. Then $b^{-1} \in F$.

$$\therefore\ ab = 0 \Rightarrow (ab)b^{-1} = 0\cdot b^{-1} \qquad \Rightarrow a(bb^{-1}) = 0$$

$$\Rightarrow a\cdot 1 = 0 \Rightarrow a = 0.$$

Thus $ab = 0 \Rightarrow$ either $a = 0$ or, $b = 0$

Hence the field F has no zero divisor.

Thus the field F is an integral domain.

Note : *Converse of the above theorem is not true i.e. every integral domain is not field e.g. the ring of integers $(Z, +, \cdot)$ is an integral domain but not a field, as the inverse of each non-zero element of Z does not exist.*

Theorem 2. Every finite integral domain is a field.

[*W.B.U.T. 2003, 2004, 2006, 2008, 2012, 2014, 2016*]

Proof. Let D be a finite integral domain with n distinct elements, say $a_1, a_2, \cdots, a_n$. Since D is an integral domain it is a commutative using with unity and without zero divisor.

Let $a \neq 0 \in D$. Consider n products $a\cdot a_1, a\cdot a_2, \cdots, a\cdot a_n$. All these are distinct elements of D. For suppose that

$$a\cdot a_i = a\cdot a_j \text{ for } i \neq j.$$

Then $a_i \neq a_j$, since D is without zero divisor and $a \neq 0$.

$\therefore a \cdot a_1, a \cdot a_2, \cdots, a \cdot a_n$ are all n distinct elements of D placed in some order. Since D has an unity element 1, so there exists a non-zero element, say a_k such that

$$a \cdot a_k = 1$$

and so by commutativity, $a \cdot a_k = a_k \cdot a = 1$. Therefore a_k is the multiplicative inverse of the non-zero element $a \in D$. Thus every non-zero element of D is invertible.

Hence D is a field.

Finite Field. A field having only a finite number of elements is called a finite field.

Illustration. The ring Z_p of integers modulo p is a field when p is a prime number. This field has p elements and so it is an example of a finite field.

Theorem 3. The multiplicative group of non-zero elements of a finite field is cyclic.

Proof. Beyond the scope of the book.

Illustrative Examples.

Ex. 1. *Examine whether the following sets form an integral domain with respect to ordinary addition and multiplication ? If so state if they are fields.*

(i) *The set of even integers.* [*W.B.U.T. 2005*]

(ii) *the set of positive integers.*

Let E be the set of all even integers. Then it can be easily verified that the set E is a ring w.r.t addition and multiplication. Also the multiplication is a commutative composition and is without zero divisor as the product of two non-zero even integers cannot be equal to zero. But the ring has no unit element. Hence the set E of even integers is not an integral domain.

But the set E is not a field as the multiplicative identity does not exist and hence every non-zero element does not possesses multiplicative inverse.

(ii) Let N be the set of all positive integers. Then $0 \notin N$ and hence additive identity does not exist. Therefore N is not a ring and so is not an integral domain.

Ex. 2. *Assuming that the set F of all real numbers of the form $a+b\sqrt{2}$ with a,b are integers form a ring w.r.t the ordinary addition and multiplication, show that F is an integral domain. Is it a field ?*

Let $a+b\sqrt{2} \in F$ and $c+d\sqrt{2} \in F$, where a,b,c,d are integers.

(i) Now $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$

and $(c+d\sqrt{2})(a+b\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$

$\therefore (a+b\sqrt{2})(c+d\sqrt{2}) = (c+d\sqrt{2})(a+b\sqrt{2})$.

So the multiplication is commutative.

(ii) $1+0\cdot\sqrt{2} \in F$ and hence the unit element exist in F.

(iii) Let $(a+b\sqrt{2})(c+d\sqrt{2}) = 0+0\sqrt{2}$, the zero element of F

Then $ac+2bd=0,\ ad+bc=0$

$\Rightarrow$ either $a=0$ and $b=0$ or, $c=0$ and $d=0$

Thus $(a+b\sqrt{2})(c+d\sqrt{2}) = 0+0\sqrt{2} \Rightarrow$ either $a+b\sqrt{2}=0$ or, $c+d\sqrt{2}=0$. Thus the ring F is without zero divisors.

Therefore the set F is an integral domain.

Next let $a+b\sqrt{2}$ be a non-zero element of F. Then the inverse of $a+b\sqrt{2}$ is

$$\frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \notin F,$$ as $\frac{a}{a^2-2b^2}, \frac{b}{a^2-2b^2}$ are not always integers.

Hence F is not a field.

Ex. 3. *Let C be the set of all complex numbers of the form $a+ib$, Assuming that the set C is a ring w.r.t addition and multiplication, prove that C is a field.*

Let $a+ib, c+id \in C$

Then, (i) $(a+ib)(c+id) = (ac-bd)+i(ad+bc)$

and $(c+id)(a+ib) = (ac-bd)+i(ad+bc)$

$\therefore (a+ib)(c+id) = (c+id)(a+ib)$

Thus the multiplication is commutative in C.

(ii) Now, $1 = 1 + i \cdot 0 \in C$ and $(a+ib)1 = a+ib \quad \forall \ a+ib \in G$.

So, 1 is the unity element of C.

(iii) Let $a+ib$ be any non-zero element of C and

$(a+ib)(c+id) = 1 + i \cdot 0$

Then $(ac-bd)+i(bc+ad) = 1+i\cdot 0 \quad \Rightarrow ac - bd = 1,\ bc + ad = 0$

Solving these equations for c,d we get $c = \frac{a}{a^2+b^2},\ d = \frac{b}{a^2+b^2}$

As $a \neq 0,\ b \neq 0$, so $a^2 + b^2 \neq 0$,

so, $\left(\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of $a+ib$.

Thus each non-zero element of C possesses multiplicative inverse. Hence $(C, +, \cdot)$ is a field.

Ex. 4. *Prove that the ring of matrices of the form* $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ *of real numbers is a field.*

Let $M = \left\{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in R\right\}$

Then $(M, +, \cdot)$ is a ring (given)

Let $A = \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \in M,\ B = \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} \in M$

Then (i) $AB = \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + y_1x_2 \\ -x_2y_1 - x_1y_2 & -y_1y_2 + x_1x_2 \end{pmatrix}$

$$BA = \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + y_1x_2 \\ -x_2y_1 - x_1y_2 & -y_1y_2 + x_1x_2 \end{pmatrix}$$

$\therefore AB = BA \quad \forall A, B \in M$.

So multiplication is commutative.

(ii) Now $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ is an unity element,

as $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$.

(iii) Let $A=\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ be a non-zero element of M.

Then x and y are not simultaneously 0.

Now det $(A)=x^2+y^2\neq 0$.

So A^{-1} exists and $A^{-1}=\frac{1}{x^2+y^2}\begin{pmatrix} x & -y \\ y & x \end{pmatrix}\in M$.

Thus the multiplicative inverse of each non-zero element of M exists.

Hence the ring $(M,+,\cdot)$ is a field.

Ex. 5. *Prove that the set Z_5 of integers modulo 5 forms a field under addition and multiplication of modulo class.*

Here $Z_5=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$. We shall show that $(Z_5,+,\times)$ forms a field. Let us construct the following additive and multiplicative composition table :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

From the above tables it is obvious that

(i) Z_5 is closed w.r.t addition modulo 5

(ii) Addition modulo 5 is associative in Z_5

e.g. $(\bar{2}+\bar{4})+\bar{3}=\bar{1}+\bar{3}=\bar{4}$ and $\bar{2}+(\bar{4}+\bar{3})=\bar{2}+\bar{2}=\bar{4}$

$\therefore\ (\bar{2}+\bar{4})+\bar{3}=\bar{2}+(\bar{4}+\bar{3})$

(iii) $\bar{0}$ is the additive identity

(iv) the inverse of $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$ are $\bar{0},\bar{4},\bar{3},\bar{2},\bar{1}$ respectively. So inverse of each element exist

(v) the operation addition modulo 5 is commutative e.g.,

$$\bar{1}+\bar{4}=\bar{0}=\bar{4}+\bar{1}\cdot$$

(vi) Z_5 is closed w.r.t multiplication modulo 5

(vii) multiplication modulo 5 is associative in Z_5 e.g.

$$(\bar{1}\times\bar{4})\times\bar{3}=\bar{4}\times\bar{3}=\bar{2},\quad \bar{1}\times(\bar{4}\times\bar{3})=\bar{1}\times\bar{2}=\bar{2}$$

$$\therefore (\bar{1}\times\bar{4})\times\bar{3}=\bar{1}\times(\bar{4}\times\bar{3})$$

(viii) $\bar{1}$ is the multiplicative identity

(ix) the inverse of $\bar{1},\bar{2},\bar{3},\bar{4}$ are $\bar{1},\bar{3},\bar{2},\bar{4}$ respectively. Thus the inverse of each non-zero element exist.

(x) the operation multiplication is commutative

(xi) the distributive property holds good in Z_5, e.g.

$$\bar{2}\times(\bar{3}+\bar{4})=\bar{2}\times\bar{2}=\bar{4},\ (\bar{2}\times\bar{3})+(\bar{2}\times\bar{4})=\bar{1}+\bar{3}=\bar{4}$$

$$\therefore\ \bar{2}\times(\bar{3}+\bar{4})=(\bar{2}\times\bar{3})+(\bar{2}\times\bar{4})$$

Hence $(Z_5,+,\times)$ is a field.

Ex. 6. *Prove that in a field F, the equations* $a\cdot x=b$ *and* $y\cdot a=b$ *have unique solutions where* $a,b\in F$ *and* $a\neq 0$

[*W.B.U.T. 2008*]

Since $a\neq 0$. $\therefore a^{-1}$ exists in F. So, from the equation $a\cdot x=b$ we get $a^{-1}\cdot a\cdot x=a^{-1}\cdot b$ or, $e\cdot x=a^{-1}\cdot b\ \therefore x=a^{-1}\cdot b$. So, $x=a^{-1}\cdot b$ is a solution of the equation $a\cdot x=b$.

Now $a\neq 0\Rightarrow a^{-1}\in F\Rightarrow a^{-1}\cdot b\in F$ $\therefore$ The solution $\in F$.

Next let x_1 and x_2 be two solutions of $a\cdot x=b$. Then

$a\cdot x_1=b,\ a\cdot x_2=b \quad\therefore\ a\cdot x_1=a\cdot x_2$

$\Rightarrow x_1=x_2\ \ (\because a\neq 0)$

Thus the solution of the equation $a\cdot x=b$ is unique and is $a^{-1}\cdot b$.

Similarly the solution of $y\cdot a=b$ is unique and is $b\cdot a^{-1}$.

Ex. 7. *Let* $(F,+,\cdot)$ *be a field and* $a,b\in F$ *with* $b\neq 0$. *Then show that* $a=1$ *when* $(ab)^2=ab^2+bab-b^2$

We have $(ab)^2 = ab^2 + bab - b^2$

$\Rightarrow (ab)(ab) = (ab)b + bab - b \cdot b$

$\Rightarrow (aba) \cdot b = (ab + ba - b) \cdot b$

$\Rightarrow a(ba) = ab + ba - b$, by right cancellation law

$\Rightarrow a(ab) = ab + ab - b \ [\because ab = ba]$

$\Rightarrow (a\,a)b = 2ab - b \Rightarrow (aa)b = (2a - 1)b$

where 1 is unit element of F

$\Rightarrow aa = 2a - 1 \Rightarrow aa = a + a - 1$

$\Rightarrow aa - a - a + 1 = 0 \Rightarrow (a-1) \cdot (a-1) = 0$

$\Rightarrow a - 1 = 0$

$\therefore a = 1$.

Ex. 8. *In a field F, prove that* $a^2 = b^2$ *implies either* $a = b$ *or* $a = -b \ \forall\, a, b \in F$.

Now $(a-b) \cdot (a+b) = (a-b) \cdot a + (a-b) \cdot b$,

by Right Distributive Law

$= a \cdot a - b \cdot a + a \cdot b - b \cdot b$, by left distributive law

$= a^2 - a \cdot b + a \cdot b - b^2 \ [\because a \cdot b = b \cdot a \ \forall a, b \in F]$

$= a^2 - b^2 \quad = a^2 - a^2 \ [\because a^2 = b^2]$

$= 0$

$\therefore$ Either $a - b = 0$ or $a + b = 0$ [$\therefore$ Field has no divisor of 0]

i.e., either $a = b$ or $a = -b$.

EXERCISE

I. Short Answer Questions

1. (a) Define a ring and give an example of a ring.
   (b) Show that the set of all integers is a ring under + and ×.
2. Show that the set C of all complex numbers is a commutative ring with unity, the addition and multiplication of complex numbers being the two ring compositions.