RINGS

Prepared
by
K.Shalini
Lecturer in Mathematics
SKR & SKR College for Women,
Kadapa

Contents

Rings Definition

- Let R be a non empty set and +, .be two binary operations in R. (R,+,.) is said to be a ring

i) (R,+) is an Abelian group

a. Closure Law

b. Associative Law

c. Identity Law

d. Inverse Law

e. Commutative law

i) (R,.) is a Semi group

ii) Distributive laws holds

Boolean Rings

- In a ring if $a^2 = a$ then that ring is called a Boolean Ring.
- Every Boolean Ring is abelian

Proof:- for a,b$\in R \rightarrow a + b \in R$

$$\rightarrow (a+b)^2 = a + b$$
$$\rightarrow (a+b)(a+b) = a + b$$
$$\rightarrow (a+b) + (ab + ba) = (a+b) + 0$$
$$\rightarrow (ab + ba) = 0$$
$$\rightarrow ab = ba$$

Hence R is abelian

Problems on Rings

Ex. 2. *Prove that the set of even integers is a ring, commutative without under usual addition and multiplication of integers.*

Sol. Let R = the set of even integers. Then $R = \{2x \mid x \in Z\}$.

$a, b, c \in R \Rightarrow a = 2m, b = 2n, c = 2p$ where $m, n, p \in Z$.

$(R, +)$ is a commutative group. (see ex. in groups)

$a \cdot b = (2m)(2n) = 2l$ where $l = 2mn \in Z$

$\therefore$ Multiplication $(\bullet)$ of integers is a binary operation in R.

$(a \cdot b) \cdot c = (2m \cdot 2n) \cdot 2p = 8mnp$ and $a \cdot (b \cdot c) = 2m \cdot (2n \cdot 2p) = 8mnp$

$\therefore (a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\Rightarrow$ Multiplication $(\bullet)$ is associative in R.

$a \cdot (b + c) = 2m(2n + 2p) = 2m \cdot 2n + 2m \cdot 2p = a \cdot b + a \cdot c$

Similarly, $(b + c) \cdot a = b \cdot a + c \cdot a$

$\therefore$ Distributive laws hold in R. Hence $(R, +, \bullet)$ is a ring.

Since '1' is not an even integer; $1 \notin R$ and hence R has no unity element.

Zero Divisors of a Ring

- Two non zero elements a, b of a ring R are said to be zero divisors if ab=0

and $a \neq 0, ba = ca$

Theorem. ***A ring R has no zero divisors if and only if the cancellation hold in R.***

(A. N. U. M15, S. K. D. 04, K. U. 03, 08, S. V.

Proof. Let the ring have no zero divisors. We prove that cancellation laws ho

$a, b, c \in R$ and $a \neq 0, ab = ac \Rightarrow ab - ac = 0$

$\Rightarrow a(b-c) = 0 \Rightarrow b - c = 0 \quad (\because a \neq 0) \Rightarrow b = c$

Similarly we can prove $a \neq 0, ba = ca \Rightarrow b = c$

Conversely, let the cancellation laws hold in R. We prove that R has no zero di

If possible, suppose that there exist $a, b \in R$ such that $a \neq 0, b \neq 0$ and $ab = 0$.

$ab = 0 \Rightarrow ab = a0 \Rightarrow b = 0$ (By cancellation law)

This is a contradiction. $\therefore$ $a \neq 0, b \neq 0$ and $ab = 0$ is not true in R.

$\therefore$ R has no zero divisors.

Integral Domain

- A commutative Ring with unity containing no zero divisors is an Integral Domain.

Ex. 9. *Prove that the set* $Z[i] = \{a+bi \mid a,b \in Z, i^2 = -1\}$ *of Gaussian integers is an integral domain with respect to addition and multiplication of numbers. Is it a field ?* **(S. V. U. M15, 01, O.U. 01, N.U. 04)**

Sol. Let $Z(i) = \{a+bi \mid a,b \in Z\}$.

Let $x, y \in Z(i)$ so that $x = a+bi, y = c+di$ where $a,b,c,d \in Z$

18

$x+y = (a+c)+(b+d)i = a_1 + b_1 i$ where $a_1 = a+c, b_1 = b+d \in Z$

$x \cdot y = (ac-bd)+(ad+bc)i = a_2 + b_2 i$ where $a_2 = ac-bd$, $b_2 = ad+bc \in Z$

$\therefore$ $+, \cdot$ are binary operations in $Z(i)$.

Since the elements of $Z(i)$ are complex numbers we have that

(*i*) addition and multiplication are commutative in $Z(i)$,

(*ii*) addition and multiplication are associative in $Z(i)$ and

(*iii*) multiplication is distributive over addition in $Z(i)$.

Clearly zero element $= 0+0i = 0$ and unity element $= 1+0i = 1$.

Further, for every $x = a+ib \in Z(i)$ we have $-x = (-a)+i(-b) \in Z(i)$

so that $x+(-x) = \{a+(-a)\}+i\{b+(-b)\} = 0+i0 = 0$

$\Rightarrow$ Additive inverse exists. $\therefore$ $Z(i)$ is a commutative ring with unity element.

For $x, y \in Z(i)$, $x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$ since x, y are complex numbers.

Hence $Z(i)$ is an integral domain with unity element.

Field

- Def: A commutative ring with unity is called a filed if
  i) i) R is a ring ii) R is Commutative iii) R has unity element iv) every non zero element of R is invertible

Theorem. 5. ***Every field is an integral domain.***

(K. U. M15, N. U. 12, 01, O. U. 03, S. K. U. 07, S. V. U. M 14, 08)

Proof. Let $(F, +, \cdot)$ be a field. Then the ring F is a commutative ring with unity and having every non - zero element as unit.

But an integral domain is a commutative ring with unity and having no zero divisors.

So, we have to prove that F has no zero divisors.

(Write the proof of the above Theorem (3))

Note. The converse of the above theorem need not be true. But an integral domain with finite number of elements can become a field.

Problems on Fields

So, every non-zero ...

Ex. 10. *Prove that* $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$ *is a field with respect to ordi addition and multiplication of numbers.*

(A. U. M14, S. K. U. M15, A. N. U. 12, S. V. U. 00, K. U

Sol. Let $x, y, z \in Q[\sqrt{2}]$ so that

$x = a_1 + b_1\sqrt{2}, y = a_2 + b_2\sqrt{2}, z = a_3 + b_3\sqrt{2}$ where $a_1, b_1, a_2, b_2, a_3, b_3 \in Q$

$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = a + b\sqrt{2}$ where $a_1 + a_2 = a, b_1 + b_2 = b \in Q$

$x \cdot y = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} = c + d\sqrt{2}$ where $c = a_1a_2 + 2b_1b_2 \in Q$

and $d = a_1b_2 + a_2b_1 \in Q$

$\therefore$ Addition $(+)$ and multiplication $(\bullet)$ of numbers are binary operations in $Q[\sqrt{2}]$

$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = (a_2 + a_1) + (b_2 + b_1)\sqrt{2}$

$= (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2}) = y + x \Rightarrow$ Addition is commutative.

$(x + y) + z = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2}$

and $x + (y + z) = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2}$

$\Rightarrow (x + y) + z = x + (y + z) \Rightarrow$ Addition is associative.

For $0 \in Q$ we have $0 + 0\sqrt{2} = 0 \in Q[\sqrt{2}]$ so that

$x+0=x$ for $x \in Q[\sqrt{2}] \Rightarrow 0 \in Q[\sqrt{2}]$ is the zero element.

For $x=a_1+b_1\sqrt{2} \in Q[\sqrt{2}]$ we have

$-x=(-a_1)+(-b_1)\sqrt{2} \in Q[\sqrt{2}]$ so that $x+(-x)=0 \Rightarrow$ Additive inverse exists.

$\therefore (Q[\sqrt{2}],+)$ is a commutative group.

$x \cdot y=(a_1+b_1\sqrt{2}) \cdot (a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$

$=(a_2a_1+2b_2b_1)+(a_2b_1+b_2a_1)\sqrt{2}=y \cdot x \Rightarrow$ Multiplication is commutative.

$(x \cdot y) \cdot z=(\overline{a_1a_2+2b_1b_2}+\overline{a_1b_2+a_2b_1}\sqrt{2}) \cdot (a_3+b_3\sqrt{2})$

$=(a_1a_2a_3+2b_1b_2a_3+2a_1b_2b_3+2a_3b_1b_3)+(a_1a_2b_3+2b_1b_2b_3+a_1a_3b_2+a_2a_3b_1)\sqrt{2}$

and $x \cdot (y \cdot z)=(a_1+b_1\sqrt{2})(\overline{a_2a_3+2b_2b_3}+\overline{a_2b_3+a_3b_2}\sqrt{2})$

$=(a_1a_2a_3+2a_1b_2b_3+2a_2b_1b_3+2a_3b_1b_2)+(a_1a_2b_3+a_1a_3b_2+a_2a_3b_1+2b_1b_2b_3)\sqrt{2}$

$\therefore (x \cdot y) \cdot z=x \cdot (y \cdot z) \Rightarrow$ Multiplication is associative.

$x \cdot (y+z)=(a_1+b_2\sqrt{2})(\overline{a_2+a_3}+\overline{b_2+b_3}\sqrt{2})$

$=(a_1a_2+a_1a_3+2b_1b_2+2b_1b_3)+(a_1b_2+a_1b_3+a_2b_1+a_3b_1)\sqrt{2}$

and $x \cdot y+x \cdot z=(\overline{a_1a_2+2b_1b_2}+\overline{a_1b_2+a_2b_1}\sqrt{2})+(\overline{a_1a_3+2b_1b_3}+\overline{a_1b_3+a_3b_1}\sqrt{2})$

$=(a_1a_2+2b_1b_2+a_1a_3+2b_1b_3)+(a_1b_2+a_2b_1+a_1b_3+a_3b_1)\sqrt{2}$

$\therefore x \cdot (y+z)=x \cdot y+x \cdot z \Rightarrow$ Distributivity is true. Hence $(Q[\sqrt{2}],+,\cdot)$ is a ring.

$1=1+0\sqrt{2} \in Q[\sqrt{2}]$ so that $x \cdot 1=(a_1+b_1\sqrt{2})(1+0\sqrt{2})=x \ \forall \ x \in Q[\sqrt{2}]$.

$\therefore Q[\sqrt{2}]$ is a commutative ring with unity element.

To show that $Q[\sqrt{2}]$ is a field we have to prove further every non-zero element in $Q[\sqrt{2}]$ has multiplicative inverse.

Let $a+b\sqrt{2} \in Q[\sqrt{2}]$ and $a \neq 0$ or $b \neq 0$

Then $\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\left(\frac{a}{a^2-2b^2}\right)+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$

since $a^2-2b^2 \neq 0$ for $a \neq 0$ or $b \neq 0$. $\quad a,b \in Q \Rightarrow \frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in Q$

For $a+b\sqrt{2} \neq 0 \in Q[\sqrt{2}]$ there exists $\left(\frac{a}{a^2-2b^2}\right)+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in Q[\sqrt{2}]$ such that

$(a+b\sqrt{2})\left[\left(\frac{a}{a^2-2b^2}\right)+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}\right]=1=1+0\sqrt{2}$

$\therefore$ Every non-zero element of $Q[\sqrt{2}]$ is invertible. Hence $Q[\sqrt{2}]$ is a field.

Characteristic of a Ring

- The characteristic of a ring R is defined as the least positive integer p such that pa=0 for all a∈ R. In case such a positive integer p does not exist then we say that the characteristic of R is zero or infinite

Theorem: The characteristic of a Integral Domain is either prime or zero

Proof. Let $(R, +, \cdot)$ be an integral domain. Let the characteristic of $R = p\ (\neq 0)$.

If possible, suppose that p is not a prime. Then $p = mn$ where $1 < m, n < p$.

$a \neq 0 \in R \Rightarrow a \,.\, a = a^2 \in R$ and $a^2 \neq 0$ ($\because$ R is integral domain)

$pa^2 = 0 \Rightarrow (mn)\, a^2 = 0 \Rightarrow (ma)\,(na) = 0$

$\Rightarrow ma = 0$ or $na = 0$ ($\because$ R is integral domain)

Let $ma = 0$. For any $x \in R$, $(ma)\, x = 0 \Rightarrow a\,(mx) = 0 \Rightarrow mx = 0$ ($\because a \neq 0$)

This is absurd, as $1 < m < p$ and characteristic of $R = p$.

$\therefore\ ma \neq 0$. Similarly, we can prove that $na \neq 0$.

This is a contradiction and hence p is a prime.

Subrings

- Def: Let (R,+,.) be a ring and S be a non-empty subset of R. If (S,+,.) is also a ring w.r.to operations then (S,+,.) is a subring of R

Theorem: Let S be a non empty subset of a ring R. Then S is a subring of R iff a-b∈S and ab ∈S

Proof. Let S be a subring of R.

We now prove that $a-b \in S$ and $ab \in S \ \forall \ a,b \in S$.

Since S is a subring of R, S is a ring with respect to the addition and multiplication operations in R.

$\therefore \ a,b \in S \Rightarrow a,-b \in S \Rightarrow a+(-b)=a-b \in S$ and $a,b \in S \Rightarrow ab \in S$

Let $a-b \in S$ and $ab \in S \ \forall \ a,b \in S$.

We now prove that S is a ring.

Since S is a non empty subset of the commutative group $(R,+)$ with the condition $a-b \in S \ \forall \ a,b \in S$; by group theory $(S,+)$ is a commutative subgroup of $(R,+)$.

Since $ab \in S \ \forall \ a,b \in S$, multiplication $(\bullet)$ is a binary operation in S.

Also, $a,b,c \in S \Rightarrow a,b,c \in R \Rightarrow a(bc)=(ab)c$

Further $a,b,c \in S \Rightarrow a,b,c \in R \Rightarrow a(b+c)=ab+ac$ and $(b+c)a=ba+ca$

$\therefore \ (S,+,\bullet)$ is a ring and hence $(S,+,\bullet)$ is a subring of R.

- Theorem: The intersection of two subrings of a ring is also a subring of R

Proof. Let S_1, S_2 be two subrings of R. Let $0 \in R$ be zero element.

Since every subring contains atleast zero element of the ring, $0 \in S_1$ and $0 \in S_2$

$\therefore 0 \in S_1 \cap S_2$ and hence $S_1 \cap S_2 \neq \phi$ and $S_1 \cap S_2 \subset R$.

Let $a, b \in S_1 \cap S_2$. Then $a, b \in S_1$ and $a, b \in S_2$.

$a, b \in S_1$ and S_1 is a subring of $R \Rightarrow a - b \in S_1$ and $ab \in S_1$

$a, b \in S_2$ and S_2 is a subring of $R \Rightarrow a - b \in S_2$ and $a, b \in S_2$

From (1) and (2) we have $a, b \in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$

$\therefore S_1 \cap S_2$ is a subring of R.

Ideals

- Def: Let (R,+,.) be a ring. A non empty susbset U of R is called an Ideal if i)a,b∈U→ a-b ∈U ii) a ∈U and r ∈R→ar,ra ∈U
- The intersection of two ideals of a ring R is an ideal of R

Proof. Let U_1, U_2 be two ideals of the ring R.

If $0 \in R$ is the zero element, then $0 \in U_1$ and $0 \in U_2$.

$\therefore\ 0 \in U_1 \cap U_2$ and hence $U_1 \cap U_2 \neq \phi$

Let $a,b \in U_1 \cap U_2$ and $r \in R$. Then $a,b \in U_1$ and $a,b \in U_2$.

$a,b \in U_1, r \in R$ and U_1 is an ideal $\Rightarrow a-b \in U_1$ and $ar, ra \in U_1$ .... (1)

$a,b \in U_2, r \in R$ and U_2 is an ideal $\Rightarrow a-b \in U_2$ and $ar, ra \in U_2$ .... (2)

From (1) and (2) : $a-b \in U_1 \cap U_2$ and $ar, ra \in U_1 \cap U_2$

Hence $U_1 \cap U_2$ is an ideal of R.

- If U1 and U2 are two ideals of a ring R then U1UU2 is an ideal of R if and only if U1⊂U2 of U2 ⊂U1

Proof. Let $U_1 \cup U_2$ be an ideal of R. We now prove that $U_1 \subset U_2$ or $U_2 \subset U_1$

If possible, suppose that $U_1 \not\subset U_2$ and $U_2 \not\subset U_1$.

Since $U_1 \not\subset U_2$ there exists an element $a \in U_1$ and $a \notin U_2$.

Since $U_2 \not\subset U_1$ there exists an element $b \in U_2$ and $b \notin U_1$.

$a \in U_1$ and $b \in U_2 \Rightarrow a, b \in U_1 \cup U_2$

$a, b \in U_1 \cup U_2$ and $U_1 \cup U_2$ is an ideal $\Rightarrow a - b \in U_1 \cup U_2$

$\Rightarrow a - b \in U_1$ or $a - b \in U_2$

But $a - b \in U_1 \Rightarrow a - (a - b) = b \in U_1$ ... (1)

$a - b \in U_2 \Rightarrow b + (a - b) = a \in U_2$ ... (2)

Both (1) and (2) contradict $a \notin U_2, b \notin U_1$

$\therefore$ Our supposition is wrong. Hence $U_1 \subset U_2$ or $U_2 \subset U_1$.

Conversely, let $U_1 \subset U_2$ or $U_2 \subset U_1$

Then $U_1 \cup U_2 = U_2$ or U_1 and hence $U_1 \cup U_2$ is an ideal.

Principal Ideals

- Let R be a commutative ring with unity and a∈R. The Ideal$\{ra/r \in R\}$of all multiples of a is called the principal ideal generated by 'a' and it is denoted by (a).

- Principal Ideal Ring: A commutative ring R with unity is a principal ideal ring if every ideal in R is a principal ideal

- Theorem: The ring of Integers is a principal ideal ring.

Proof. Let U be ideal of Z and $U = \{0\}$. Then U is generated by the zero element.

$\therefore U = \langle 0 \rangle$ is a principal ideal.

Let U be an ideal of Z and $U \neq (0)$.

$\therefore$ there exists $a \in U$ so that $a \neq 0$. $a \in U, U$ is an ideal $\Rightarrow -a \in U$.

Since $U \subset Z$, one of $a, -a$ must be a positive integer.

$\therefore$ the set of positive integers U^+ in U is non - empty.

$\therefore$ by well - ordering principle U^+ has a least member, say, b.

We now prove that $U = \langle b \rangle =$ the principal ideal generated by 'b'.

Let $x \in U$. Since x, b are integers and $b \neq 0$ there exist $q, r \in Z$ such that $x = bq + r;\ 0 \leq r < b$ (Division algorithm).

$b \in U, q \in Z$ and U is an ideal $\Rightarrow bq \in U$. $x \in U, bq \in U \Rightarrow x - bq = r \in U$.

Now $r \in U, 0 \leq r < b$ and b is the least member in $U^+ \Rightarrow r = 0$.

$\therefore x - bq = r \Rightarrow x - bq = 0 \Rightarrow x = bq$.

Hence $x \in U \Rightarrow x = bq$ for $q \in Z \Rightarrow U = \{bq \mid q \in Z\} = \langle b \rangle$.

$\therefore$ every ideal U of Z is a principal ideal. Hence Z is a principal ideal ring.

Note 1.

Euclidean Rings

- Def: An Integral Domain R is said to be Euclidean ring if every $a \neq 0 \in R$ there is defined a non negative integer d(a) such that

1) For all $a,b \in R$, $d(a) \leq d(ab)$

2) For any $a,b \in R$, there exist $q,r \in R$ such that $a=bq+r$ where either $r=0$ or $d(r)<d(b)$

Theorem: Every field is a Euclidean Ring

Proof. Let F be a field and F^* be the set of all non-zero elements of F.

Since F is a field, F is an integral domain.

Define the mapping $d : F^* \to Z$ by $d(a) = 0$ (zero integer) $\forall a \in F^*$

$\therefore\ d(a) \geq 0\ \forall\ a \in F^*$

Let $a, b \in F^*$. Then a, b and ab are non zero elements of F.

$\therefore\ d(a) = 0$ and $d(ab) = 0 \Rightarrow d(a) \leq d(ab)$

Let $a \in F$ and $b \in F^*$. Now $a = a1$ where 1 is the unity element of F.

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

$= (ab^{-1})\, b + 0$ where '0' is the zero element of the field F.

$\therefore\ a = qb + r$ where $q = ab^{-1}, r = 0$

Hence, for $a \in F, b \in F^*$ there exist $q, r \in F$ so that $a = qb + r$ where $r = 0$.

$\therefore\ F$ is an Euclidean ring.

THANK YOU