2:45

Impressions

Date ....

Page ....

Rings.

Ring → Let R be a non-empty set with two binary composition addition (+) & multiplication (·) then R is called Ring iff it satisfies the following:

I) R is an abelian group under + i.e.

(i) for $a, b \in R \Rightarrow a+b \in R$ i.e. R is closed under addition.

ii) for $a, b, c \in R$
$a+(b+c) = (a+b)+c$ i.e. associativity under addition holds in R.

iii) for each $a \in R$, $\exists\ 0 \in R$ s.t. $a+0 = a = 0+a$ i.e. R has additive identity.

iv) for each $a \in R$ $\exists\ -a \in R$ s.t.

$a+(-a) = 0$ i.e. R has additive inverse.

v) for each $a, b \in R$
$a+b = b+a$ i.e. R is commutative under addition.

II) for each $a, b \in R$, $a \cdot b \in R$ i.e. R is closed under multiplication

III) for $a, b, c \in R$,
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ i.e. associativity under multiplication holds in R.

IV) for $a, b, c \in R$.

(i) $a \cdot (b+c) = a \cdot b + a \cdot c$ (Left distributive law)
$(a+b) \cdot c = ac + bc$ (Right distributive law)

for eg. Set of integers $(Z, +, \cdot)$ is a ring.

Commutative Ring → A ring R is called a commutative ring if $a \cdot b = b \cdot a$ $\forall$ $a, b \in R$.

Ring with Unity → A ring R is called ring with unity if for each $x \in R$, $\exists$ $1 \in R$ s.t. $1 \cdot x = x = x \cdot 1$. The element 1 is called multiplicative identity of R.

$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$AB = 0$

Impressions
Date
Page

Ring with Zero divisors → Let R be a ring $0 \neq a, b \in R$ then R is called ring with zero divisor if $a.b = 0$ i.e. If product of two non-zero elements in a ring R is zero then R is called ring with zero divisors.

Also we can say that the element a is zero divisor of b or b is zero divisor of a.

Ring without zero divisor → A ring R is called ring without zero divisors if whenever

$a.b = 0 \Rightarrow a = 0$ or $b = 0$ $\forall$ $a, b \in R$.

Boolean ring → A ring R is called boolean ring if $x^2 = x$ $\forall$ $x \in R$

for e.g. The Ring $\{0, 1, +_2, \times_2\}$ under addition and multiplication modulo 2 is a boolean ring.

Impressions
Date
Page

Q. If R is a ring s.t $a^2 = a \ \forall \ a \in R$.
show that:
(i) $a + a = 0 \ \forall a \in R$
ii) $a + b = 0 \Rightarrow a = b$
iii) R is Commutative.

Solⁿ: Given R is a ring s.t $a^2 = a, \forall a \in R$
Since $a^2 = a \ \forall \ a \in R$
$\Rightarrow (a+a)^2 = a + a$
$\Rightarrow (a+a)(a+a) = a+a$
$\Rightarrow a \cdot (a+a) + a \cdot (a+a) = a + a$ (Distributive)
$\Rightarrow a \cdot a + a \cdot a + a \cdot a + a \cdot a = a + a$
$\Rightarrow a + a + a + a = a + a$ $\because [a^2 = a \Rightarrow a \cdot a = a]$
$\Rightarrow \boxed{a + a = 0 \ \forall \ a \in R}$ (left Cancellation law)

ii) let $a + b = 0 = a + a$ $\because$ (of part a)
$\Rightarrow \boxed{b = a}$ (left Cancellation law)

iii) Given $a^2 = a \ \forall \ a \in R$
$\Rightarrow (a+b)^2 = a + b$
$\Rightarrow (a+b)(a+b) = a + b$
$\Rightarrow a \cdot a + b \cdot a + a \cdot b + b \cdot b = a + b$

$a^2 + b.a + a.b + b^2 = a+b$

$\Rightarrow a + b.a + a.b + b = a+b \quad \because (a^2 = a \ \forall a \in R)$

$\Rightarrow b a + a.b + b = b$ (left canc law)

$\Rightarrow b a + a.b = 0$ (right canc law)

$\Rightarrow \boxed{ba = ab}$ [from ii) part. $a+b=0 \Rightarrow a=b$]

hence R is commutative.

Morphism of Rings

The word morphism is combination of various terms like ring homomorphism, ring isomorphism etc.

Ring Homomorphism

Let $(R, +, \cdot)$ and $[R', +', \cdot']$ be two rings. then mapping $f: R \to R'$ is called a ring homomorphism

(i) $f(a+b) = f(a) +' f(b) \ \forall \ a, b \in R$

$f(a \cdot b) = f(a) \cdot' f(b) \quad \forall a, b \in R.$

Also a ring homomorphism and one one is called monomorphism.
A ring homomorphism f onto is called epimorphism.

Further if in addition f is one-one onto then f is called an isomorph
& R and R' are said to be isomorp
& we write $R \cong R'$.

Integral Domain → A non zero Elem

$a \in R$ is called a zero divisor if there exist a non-zero Element $b \in R$ s.t. $ab = 0$.

A Commutative Ring R is called an integral domain if for every $0 \neq a, b \in R$, $ab = 0$
$\Rightarrow a = 0$ or $b = 0$

Thus a Commutative ring is called

Impressions
Date
Page

an integral domain if R has no zero divisor.

Q. find all zero divisors of Z_{15}, Z_6, Z_{20}.

Sol^n $Z_{15} = \{0, 1, 2 \cdots 14; +_{15}, \times_{15}\}$

We know that an Element m in $[Z_n, +_n, \times_n]$ is a zero divisor iff m is not relative prime to n.

Here $n = 15$. The only no which are not relatively prime to 15 are 3, 5, 6, 9, 10, 12,

hence 3, 5, 6, 9, 10, 12 are zero divisors.

Also $3 \times_{15} 5 = 0$ $9 \times_{15} 10 = 0$.
& $5 \times_{15} 6 = 0$ $10 \times_{15} 12 = 0$ etc.

ii) $Z_6 = \{0, 1, 2, 3, 4, 5, +_6, \times_6\}$
The only Element which are not relatively prime to 6 are 2, 3, 4
∴ Zero divisors of Z_6 are 2, 3, 4.

Also $2 \times_6 3 = 0$, $3 \times_6 4 = 0$ etc

(iii) $Z_{20} = \{0, 1, 2, 3 \ldots 19, +_{20}, \times_{20}\}$

Elements which are not relative prime to 20 are 2, 4, 6, 8, 10, 12, 14, 16, 18

hence Zero divisor of Z_{20} are
2, 4, 6, 8, 10, 12, 14, 16, 18.

<u>field</u>: A Commutative Ring F with unity s.t each non-zero element has a multiplicative inverse i.e. $\exists\, a^{-1} \in F$ s.t
$a a^{-1} = 1 = a^{-1} a$ is called field.
It is denoted by F.

Alternatively F is a field if its non zero elements form a group under multiplication.

e.g. $[Q, +, \cdot]$, $[R, +, \cdot]$ are fields.

Thm Every field is an integral domain but converse is not true.

Proof let F be a field.
We show that F is an integral domain.
Since F is field, F must be commutative. We show F is without zero divisors.

let $a, b \in F$ s.t. $a \cdot b = 0 \rightarrow (1)$

If $a \neq 0$ then as F is field so each non zero element of F has multiplicative inverse i.e. for $a \in F$ there exists $a^{-1} \in F$ s.t. $aa^{-1} = 1 = a^{-1}a$

from (1) $a \cdot b = 0$

$\Rightarrow \vec{a}\,(a \cdot b) = \vec{a} \cdot 0$

$\Rightarrow (\vec{a}a) \cdot b = 0$ $[a \cdot 0 = 0 \ \forall a \in R]$

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow \boxed{b = 0}$.

Hence if $a \neq 0$ then $b = 0$

llly if $b \neq 0$ then $a = 0$.

Hence F is without zero divisors.

consequently F is an integral domain

The Converse is however not true for e.g. Z is an integral domain but for $2 \in Z$ there is no $a \in Z$ s.t $2 \cdot a = 1 = a \cdot 2$ i.e. 2 has no multiplicative inverse.

$\therefore$ Z cannot be a field

Impressions
Date ....
Page ....

Quotient Ring :→ Let R is a ring and I is an ideal of R. Define R/I by

$$R/I = \{x+I,\ x \in R\}$$

then R/I is also ring under addition & multiplication defined by

$$(r+I)+(s+I) = r+s+I,\ \forall\ r,s \in R$$

$$(r+I)(s+I) = rs+I\ \ \forall\ r,s \in R$$

The ring defined by R/I is known as quotient ring.

---

eg. (i) If R is Commutative, then R/I is also Commutative.

ii) If R is a ring with identity then R/I is also a ring with I as identity when I is an ideal of R.

Impressions
Date ....
Page ....

(i) By definition, if I is an ideal of R then $R/I = \{a+I : a \in R\}$

Let $a+I, b+I \in R/I$ & Consider

$$(a+I)(b+I) = ab+I$$
$$= ba+I \quad (a,b \in R \text{ \& } R \text{ is commutative})$$
$$= (b+I)(a+I)$$

$\therefore R/I$ is commutative.

ii) Let $1 \in R$ be identity & if $a+I \in R/I$ then Consider

$$(a+I)(1+I) = a \cdot 1 + I = a+I$$
$$= 1 \cdot a + I$$
$$= (1+I)(a+I)$$

$\therefore 1+I$ is identity of R/I.

Impressions
Date
Page

The integer modulo m $(m \geq 1)$

The integer modulo m denoted by Z_m is set given by

$Z_m = \{0, 1, 2, 3 --- m-1; +_m, \times_m\}$

where the operation $+_m$ (read as addition modulo m) & $\times_m$ (read as multipliation modulo m) are defined as

$a +_m b$ = remainder after $a+b$ is divided by m.

$a \times_m b$ = remainder after ab is divided by m.

Order of a group → The order of a group G is the no. of elements in the group G. It is denoted by $O(G)$ or $|G|$.