Rings: Handwritten notes

by

Atiq ur Rehman

http://www.MathCity.org/atiq

Partial Contents

Ring:-

def:- An order triple $(R,+,\cdot)$ is called a ring if it satisfy the following axioms.

i) R is abelian group under addition.

ii) R is semi-group under multiplication.

iii) Distributive law holds in R

i.e for $a,b,c \in R$

$a(b+c) = ab + ac$; Left Distributive law

$(a+b)c = ac + bc$; Right Distributive law.

Examples.

$(\mathbb{Z},+,\cdot)$ is a ring

$(\mathbb{Q},+,\cdot)$ is a ring.

$(\mathbb{Z}_n,\oplus,\otimes)$ is a ring.

Lemma:-

If $(R,+,\cdot)$ is a ring, ~~$a,b \in R$~~ then ~~for~~ $a,b \in R$, we have

i) $0\cdot a = a\cdot 0 = 0$

ii) $a(-b) = (-a)b = -(ab)$

iii) $(-a)(-b) = ab$

iv) if $1 \in R$ then $(-1)a = -a$.

Proof.

$\because \quad 0 = 0 + 0$

$\Rightarrow \quad a\cdot 0 = a\cdot(0+0)$

$\Rightarrow \quad a\cdot 0 = a\cdot 0 + a\cdot 0$ by distributive law

$\Rightarrow \quad 0 + a\cdot 0 = a\cdot 0 + a\cdot 0$

$\Rightarrow \quad 0 = a\cdot 0$ by cancellation law.

Again

$0\cdot a = (0+0)\cdot a$

$\Rightarrow \quad 0\cdot a = 0\cdot a + 0\cdot a$

$\Rightarrow \quad 0 + 0\cdot a = 0a + 0\cdot a$

$\Rightarrow \quad 0 = 0\cdot a$ by cancellation law.

ii) As $a(-b)+ab = a(-b+b)$ by distributive law

$= a.0$

$\Rightarrow a(-b)+ab = 0$

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

And

$(-a)b + ab = (-a+a)\,b$

$= 0\cdot b$

$= 0$

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

iii) To prove $(-a)(-b) = ab$

$(-a)(-b) = -(a(-b))$ by (ii)

$= -(-(ab))$

$= ab$

iv) $\because$ $(-1)\cdot a + a = (-1)a + 1\cdot a$

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

$= 0\cdot a$

$= 0$

$\Rightarrow (-1)\cdot a = -a$

Question

In a ring R prove that for $a, b \in R$

$(a+b)^2 = a^2 + ab + ba + b^2$

Solution:-

$(a+b)^2 = (a+b)(a+b)$

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

$= a\cdot a + a\cdot b + b\cdot a + b\cdot b$

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

$\neq a^2 + 2ab + b^2$ $\because$ '$\cdot$' is not commutative

Question:-

Solve, in a ring R, for $a, b \in R$.

$(a+b)^3$

Do yourself.

Lemma:-

If R is a system with 1, satisfying all axiom of a ring except possibly $a+b=b+a$, for $a, b \in R$. Show that R is a ring.

Proof:

We have to prove

$$a+b=b+a \text{ only.}$$

$\because$

$$\begin{aligned}(a+b)(1+1) &= (a+b)\cdot 1+(a+b)\cdot 1\\ &= a\cdot 1+b\cdot 1+a\cdot 1+b\cdot 1\\ &= a+b+a+b \quad \text{---} \quad (i)\end{aligned}$$

Also

$$\begin{aligned}(a+b)(1+1) &= a(1+1)+b\cdot(1+1)\\ &= a\cdot 1+a\cdot 1+b\cdot 1+b\cdot 1\\ &= a+a+b+b \quad \text{---} \quad (ii)\end{aligned}$$

from (i) & (ii)

$$a+a+b+b = a+b+a+b$$

$\Rightarrow \quad a+b+b = b+a+b$ by left cancellation law

$\Rightarrow \quad a+b = b+a$ by right cancellation law.

Question

If $a^2=0$ in a ring R

Show that $ax+xa$ commute with $a \in R$.

Solution:-

$$\begin{aligned}\because \; a\cdot(ax+xa) &= a\cdot ax+axa \quad \text{by distributive law}\\ &= a^2x+axa\\ &= 0\cdot x+axa \quad \because a^2=0\\ &= 0+axa = axa \quad \text{---} \quad (i)\end{aligned}$$

and $(ax + xa) \cdot a = axa + xa \cdot a$

$= axa + xa^2$

$= axa + x \cdot 0 \quad \because a^2 = 0$

$= axa + 0$

$= axa$ ——— (ii)

From (i) and (ii)

$$a \cdot (ax + xa) = (ax + xa) \cdot a$$

as desire.

Commutative Ring:-

def:- A ring in which multiplication is ~~comm~~ commutative is called a commutative ring.

Ring with Unity:-

def:- A ring $(R, +, \cdot)$ with a multiplicative identity 1. such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$, is called a ring with unity.

Boolean's Ring:-

def:- If $x^2 = x \quad \forall \; x \in R$ then R is called Boolean ring.

Division Ring:-

def:- Let $(R, +, \cdot)$ is a ring with unity then an element $a \in R$ is called unit if it has multiplicative inverse in R.

If every non-zero element of R has multiplicative inverse in R. then R is called division ring.

Zero Divisor :-

def.- If $(R, +, \cdot)$ is a commutative ring then an element $a \in R$, $a \neq 0$ is called zero divisor if there is an element $b \neq 0$, $b \in R$ such that $a \cdot b = 0$

Example:-

i) let $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

as $\bar{2} \times \bar{3} = 0$

$\therefore$ $\bar{2}$ & $\bar{3}$ are zero divisor.

ii) The ring of all $m \times n$ matrix also have zero divisor

e.g

$$\begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O.$$

Integral Domain :-

def.- A commutative ring R is called integral domain if it has no zero divisor

OR

R is integral domain iff $a, b \in R$

$a \cdot b = 0 \Rightarrow$ atleast one of a or b is zero.

e.g. Set of integers Z is integral domain.

Lemma :-

A commutative ring R is an integral domain iff cancellation laws under multiplication holds in R.

Proof:-

Suppose cancellation law under multiplication holds in R.

and let for $a, b \in R$ and $a \neq 0$.

$a \cdot b = 0$

$\Rightarrow a.b = a.0 \quad \because a.0 = 0$

$\Rightarrow b = 0$ by cancellation law.

So $a.b = 0 \Rightarrow b = 0$ and $a \neq 0$.

implies R is integral domain.

Conversely, let R is integral domain.

i.e $a.b = 0$, $a = 0$ or $b = 0$.

Let $a.b = 0$; $a \neq 0$.

Now if $a.b = a.c$; $c \in R$

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

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

$\because$ R is integral domain

$\therefore b - c = 0$ as $a \neq 0$

$\Rightarrow b = c$

i.e $ab = ac \Rightarrow b = c$

hence cancellation law holds.

Review :-

i) If $x^2 = x \ \forall \ x \in R$ (ring) then R is called boolean ring.

****

Available online at http://www.MathCity.org

****

Lemma:-

A boolean ring is commutative.

Proof:-

Let R be boolean ring and $x, y \in R$

then $x^2 = x$, $y^2 = y$, $(x+y)^2 = (x+y)$.

$\because$ $(x+y) = (x+y)^2$

$\Rightarrow$ $x + y = x^2 + xy + yx + y^2$

$\Rightarrow$ $x + y = x + xy + yx + y$ $\quad \because x^2 = x$, $y^2 = y$

$\Rightarrow$ $0 = xy + yx$ by left and right cancellation law in R under '$+$'.

Now

$x \cdot 0 = x(xy + yx)$

$\Rightarrow$ $0 = x^2 y + xyx$

$\Rightarrow$ $0 = xy + xyx$ ——— (i)

and

$0 \cdot x = (xy + yx)x$

$\Rightarrow$ $0 = xyx + yx^2$

$\Rightarrow$ $0 = xyx + yx$ ——— (ii)

By (i) and (ii)

$xy + xyx = xyx + yx$

$\Rightarrow$ $xy + xyx = yx + xyx$ $\quad \because (R, +)$ is an abelian group.

$\Rightarrow$ $xy = yx$ by cancellation law in $(R, +)$.

i.e R is commutative.

Field:-

def:- The order triple $(F,+,\cdot)$ is a field if it satisfy the following axioms

i) F is abelian group under addition.

ii) $F-\{0\}$ is abelian group under multiplication.

iii) Right distributive property holds in R.

i.e for $a,b,c \in F$

$$(a+b)c = ac+bc$$

Example:-

$(\mathbb{Q},+,\cdot)$; $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are fields.

If $S=\{a+b\sqrt{3} \ ; \ a,b\in\mathbb{R}\}$ then S is a field.

Lemma:-

Every field is an integral domain.

Proof:-

Consider $a,b \in F$ where F is field and $a\neq 0$.

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

i.e if $ab=0$ then $a\neq 0$, $b=0$

$\Rightarrow$ field is an integral domain.

Example:-

$(Z_{12}, \oplus, \odot)$ is a ring.

For zero divisor

$\bar{2} \times \bar{6} = \bar{3} \times \bar{4} = \bar{3} \times \bar{8} = \bar{4} \times \bar{6} = \bar{4} \times \bar{9} = \bar{6} \times \bar{6}$
$= \bar{6} \times \bar{8} = \bar{6} \times \bar{10} = \bar{8} \times \bar{9} = 0$

i.e $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$ are zero divisor.

They are not relatively prime with $\bar{12}$.

Theorem:-

In a ring $(Z_n, \oplus, \odot)$, the zero divisor are precisely (strictly) those elements which are not relatively prime to n.

Proof:-

Let $m \in Z_n$ and $m \neq 0$, m and n are not relatively prime.
Let G.C.D of m and n is $d \neq 1$.
then

$$\frac{mn}{d} = \left(\frac{m}{d}\right)n = 0 \Rightarrow m\left(\frac{n}{d}\right) = 0$$

here $m \neq 0$, $\frac{n}{d} \neq 0$

Let $m \in Z_n$, $m \neq 0$ is relatively prime to n.
if for $s \in Z_n$, we have $ms = 0$
then $n \mid ms$.
As m & n are relatively prime
$\Rightarrow n \mid s \Rightarrow s = 0$
i.e m is not zero divisor.
$\therefore$ zero divisor of Z_n are not relatively prime to n.

Sub-ring:-

def:— Let S is a subset of a ring R.
if S is also a ring then S is called sub-ring of R

Theorem:-

A non-empty subset S of a ring R is a subring iff $a, b \in S \Rightarrow a-b \in S$, $ab \in S$.

Proof:

Let S be a subring then S itself is a ring.

Let $a, b \in S \Rightarrow a, -b \in S$

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

Conversely, Suppose $a, b \in S \Rightarrow a-b \in S$ and $ab \in S$.

as $a, b \in S \Rightarrow a+(-b) = a-b \in S$

$\Rightarrow S$ is subgroup under addition.

Also $a, b \in S \Rightarrow ab \in S$

i.e. S is closed under '$\cdot$'.

Let $a, b, c \in S \Rightarrow a, b, c \in R$

$\Rightarrow a(bc) = (ab)c \quad \because R$ is ring.

as $bc \in S$ for $b, c \in S$

$\Rightarrow a\cdot(bc) \in S$ by closure property.

and $(ab)\cdot c \in S$ for $ab, c \in S$

$\Rightarrow S$ is associative under '$\cdot$'.

Also as distributive law holds in R therefore it holds in S.

$\therefore S$ is a ring and hence a subring.

Theorem:-

A finite commutative ring with more then one element and without zero divisor is a field.

Or: every finite integral domain is a field.

Proof:-

Let R be commutative ring without zero divisor. i.e R is integral domain.

we show that R contains identity element and inverse of its every element under multiplication.

Let $a_1, a_2, \ldots, a_n$ be distinct element of R.

Let $a \in R$, $a \neq 0$ then $aa_i \in R$.

and so $\{aa_1, aa_2, \ldots, aa_n\} \subseteq R$

Further if $aa_i = aa_j$

$\Rightarrow aa_i - aa_j = 0$

$\Rightarrow a(a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0 \quad \because a \neq 0$

$\Rightarrow a_i = a_j$

hence

$\{aa_1, aa_2, \ldots, aa_n\} = R$

$\because a \in R$ so one of the product in R must be equal to a,

i.e $a = aa_i = a_i a$ (say)

i.e a_i is dealing as an identity element

to see this let $b \in R$ is any other element

then $b = aa_j$

Now $ba_i = a_i b$

$= a_i(aa_j)$

$= (a_i a) a_j$

$= aa_j \quad \because a = a_i a$

$\Rightarrow ba_i = b$

$\therefore a_i$ is the identity element.

and we take it equal to 1 i.e $a_i = 1$.
so $1 \in R$.
As $1 \in R = \{aa_1, aa_2, \ldots\ldots, aa_n\}$.
so one of the product element say aa_k must be equal to 1
i.e $aa_k = 1$
i.e a_k is the inverse of a.
$a^{-1} = a_k$
i.e each element in R is unit element.
so R is field.

Characteristic of ring:-

def:- Let R be a ring, If there exist a positive integer n such that $na = 0 \ \forall \ a \in R$. where n is least, then n is called characteristic of R. If there is no such +ive integer for which $na = 0$, then R is of characteristic zero.

e.g
i) the ring $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of zero characteristic.
ii) Z_n is a ring of characteristic n.

e.g
for $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$2[3] = [6] = 0$
$3[2] = [6] = 0$.

But $6[a] = 0 \quad \forall \ a \in Z_6$.
i.e characteristic of Z_6 is 6
(6 is least +ive integer).

Theorem

Let R be a ring with unity, then R has characteristic $n > 0$ iff n is least +ive integer such that $n \cdot 1 = 0$.

Proof:-

Let $n > 0$ be characteristic of R

then $na = 0 \ \forall \ a \in R$, n is least +ive integer.

and in particular $n \cdot 1 = 0$.

Further if $m \cdot 1 = 0$, $0 < m < n$

then $m \cdot a = m(1 \cdot a)$

$= (m \cdot 1) a$

$= 0 \cdot a = 0$

$\Rightarrow m \cdot a = 0$, a contradiction as n is least.

hence $n \cdot 1 = 0$.

Conversely, let $n \cdot 1 = 0$ where n is least +ive integer ~~then $\forall a \in R$~~.

then $\forall \ a \in R$

$n \cdot a = n \cdot (1 \cdot a)$

$= (n \cdot 1) \cdot a$

$= 0 \cdot a = 0$

i.e R is of characteristic n.

which complete the proof

Theorem

The characteristic of an integral domain R is either zero or prime.

Proof:-

If there does not exist any least +ive integer n, such that $na = 0 \ \forall \ a \in R$.
then R is of characteristic zero.

But if there exist least +ive integer then let m is a least +ive integer such that
$$ma = 0 \quad \forall \ a \in R$$
and in particular $m \cdot 1 = 0$

If m is not prime, then there are integers m_1 and m_2 such that
$$m > m_1, m_2 > 0$$
and $m = m_1 m_2$

As $m \cdot 1 = 0$

$\Rightarrow (m_1 m_2) \cdot 1 = 0$

$\Rightarrow (m_1 \cdot 1)(m_2 \cdot 1) = 0$

and since R is integral domain therefore
either $m_1 \cdot 1 = 0$ or $m_2 \cdot 1 = 0$
a contradiction as m is least +ive integer such that $m \cdot 1 = 0$

Hence m is prime.

Question

Intersection of any number of subrings is a subring.

— Do yourself —

Theorem:-

Let R be a boolean ring then characteristic of R is 2 and R is commutative.

Proof:-

Let $x \in R$, $x^2 = x$

then $(x+x)^2 = x + x$

$\Rightarrow (x+x)(x+x) = x + x$

$\Rightarrow x(x+x) + x(x+x) = x + x$

$\Rightarrow x^2 + x^2 + x^2 + x^2 = x + x$

$\Rightarrow x + x + x + x = x + x$

$\Rightarrow x + x = 0$

$\Rightarrow 2x = 0$

and so $2 \cdot 1 = 0$ for $x = 1$

$\Rightarrow$ 2 is characteristic of R.

To prove R is commutative

Let $x, y \in R$

$\Rightarrow x + y = (x+y)^2$

$= (x+y)(x+y)$

$= x(x+y) + y(x+y)$

$= x^2 + xy + yx + y^2$

$= x + xy + yx + y$ $\quad \because x^2 = x$, $y^2 = y$

$\Rightarrow 0 = xy + yx$

Now $xy + 0 = xy + xy + yx$

$= 2xy + yx$

$\because 2xy = 0$ as R has characteristic 2

$\therefore xy = yx$

$\Rightarrow R$ is commutative

Regular Ring:-

Let R be a ring and $x \in R$ then the element x is called regular element if there exist $y \in R$ such that $x = xyx$

If all elements of a ring are regular then R is regular ring.

e.g: In Z only $0, 1, -1$ are regular element

$\because$ $0 = 0x0 \quad \forall\ x \in Z$

$1 = 1\cdot 1\cdot 1$

$-1 = (-1)(-1)(-1)$

Example

Let R be a field of real numbers and

$$R\times R = \{(x,y) \mid x, y \in R\}$$

Define '+' and '·' on $R\times R$ by

$$(x,y) + (z,w) = (x+z,\ y+w)$$

$$(x,y)\cdot(z,w) = (xz,\ yw)$$

i) Is $R\times R$ commutative ring?

ii) Is $R\times R$ a field.

iii) Is $R\times R$ a regular ring, provided that $R\times R$ is a ring.

Sol: i) & ii) Do yourself

iii) To check $R\times R$ is regular

Let $(x,y) \in R\times R$

if $x = 0$, $y = 0$

$(x,y) = (x,y)(x,y)(x,y)$

if $x \neq 0$, $y = 0$

$(x,y) = (x,y)(x^{-1}, y)(x,y)$

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

$= (x, y^3) = (x,y) \quad \because y = 0$

*

if $x \neq 0$, $y \neq 0$

$(x,y) = (x,y)(x^{-1}, y^{-1})(x,y)$

$= (1,1)(x,y)$

$= (x,y)$

Hence $R\times R$ is regular

* **Example:-**

$M_2(R)$ = Set of all metrices of 2x2 order over $\mathbb{R}$.
$M_2(\mathbb{R})$ is non-commutative ring with unity.
'+' is usual addition and '.' is multiplication of matrices.
Prove that $M_2(\mathbb{R})$ is a regular ring.

Solution:-

Let $A = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(\mathbb{R})$

if $xw - zy \neq 0$

$$B = \frac{1}{xw-zy}\begin{bmatrix} w & -y \\ -z & x \end{bmatrix} = \begin{bmatrix} \frac{w}{xw-zy} & \frac{-y}{xw-zy} \\ \frac{-z}{xw-zy} & \frac{x}{xw-zy} \end{bmatrix}$$

and

$$ABA = \begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} \frac{w}{xw-zy} & \frac{-y}{xw-zy} \\ \frac{-z}{xw-zy} & \frac{x}{xw-zy} \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix} = A$$

if $xw - zy = 0$

there are two cases

Case I: If all of x, y, z, w are zero.

then $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

then $\forall\ B \in M_2(R)$, we have $ABA = A$

Case II: if $x \neq 0$ then take $B = \begin{bmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{bmatrix}$

$$ABA = \begin{bmatrix} x & y \\ z & \omega \end{bmatrix} \begin{bmatrix} 1/x & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & \omega \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ z & \omega \end{bmatrix} \begin{bmatrix} 1 & y/x \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & y \\ z & \frac{zy}{x} \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ z & \omega \end{bmatrix} = A \qquad \because x\omega - zy = 0$$

$$x\omega = zy$$

$$\omega = \frac{zy}{x}$$

Similarly if $y \neq 0$ or $z \neq 0$ or $\omega \neq 0$ we can find B such that $A = ABA$.

Hence $M_2(\mathbb{R})$ is a regular ring.

Note:-

$M_2(R)$ is not a division ring.

so a regular ring need not be a division ring.

But a division ring is always regular ring.

Theorem

Let R be a regular ring with more than one element. Let for all $x \in R$, there exists a unique $y \in R$ such that $x = xyx$, then

i) R has no zero divisor

ii) if $x \neq 0$ and $x = xyx$, then $y = yxy$ $\forall$, $x, y \in R$.

iii) R contains an identity element.

iv) R is division ring.

Proof:

i) Let $0 \neq x \in R$ and $xz = 0$

$\because x \in R$ there exist a unique $y \in R$ such that

$$x = xyx$$

Now
$$\begin{aligned} x(y-z)x &= xyx - xzx \\ &= xyx - 0 \cdot x \\ &= xyx \qquad \because 0 \cdot x = 0 \\ &= x \end{aligned}$$

$\because xyx = x \Rightarrow y$ is unique

$\Rightarrow y - z = y \Rightarrow z = 0$

Hence R has no zero divisor.

ii) Let $x \neq 0$, $x = xyx$

Now
$$\begin{aligned} x(y - yxy) &= xy - x(yxy) \\ &= xy - (xyx)y \\ &= xy - xy \\ &= 0 \end{aligned}$$

Since R has no zero divisor

and $x \neq 0 \Rightarrow y - yxy = 0$

$\Rightarrow y = yxy$.

iii) Let $x (\neq 0) \in R$ then there is unique $y \in R$ such that $x = xyx$

Let $e = yx$

if $e = 0$ then $x = xyx \Rightarrow x = 0$

a contradiction so $e \neq 0$

Also $e^2 = (yx)(yx) = y(xyx) = yx = e$

Let $z \in R$

$(ze - z)e = ze^2 - ze$

$= ze - ze = 0 \quad \because e^2 = e$

$\because e \neq 0 \Rightarrow ze - z = 0$

$\Rightarrow ze = z$

also $e(ez - z) = e^2 z - ez$

$= ez - ez = 0$

As $e \neq 0 \Rightarrow ez - z = 0 \Rightarrow ez = z$

Hence $ze = ez = z$

so e is identity of R.

iv) To prove R is a division ring

we have to prove that every non-zero element of R contain inverse in R.

For $x \neq 0 \in R$, we have

$x = xyx$, where $y \in R$ is unique.

Since $xyx = x$

$\Rightarrow xyx = xe$ as R contains identity.

$\Rightarrow xyx - xe = 0$

$\Rightarrow x(yx - e) = 0$

$\because x \neq 0 \Rightarrow yx - e = 0 \quad \because R$ contains no zero divisor

$\Rightarrow yx = e$

Also $xyx = ex$

$\Rightarrow xyx - ex = 0$

$\Rightarrow (xy - e)x = 0$

As $x \neq 0 \Rightarrow xy - e = 0$

$\Rightarrow xy = e$

i.e $yx = xy = e$

i.e inverse of each element exists in R.

This complete the proof

Question: Prove that $C(R)$ is a subring of a ring R. where $C(R)$ is centre of R.

Solution

Let $a, b \in C(R)$

to prove $C(R)$ is subring we prove $a-b, ab \in C(R)$

As $a, b \in C(R)$

$\Rightarrow ax = xa \;,\; bx = xb \quad \forall\; x \in R.$

and

$$\begin{aligned}(a-b)x &= ax - bx \\ &= xa - xb \qquad \because ax = xa \;\&\; bx = xb \\ &= x(a-b)\end{aligned}$$

$\Rightarrow a-b \in C(R)$

also

$$\begin{aligned}(ab)x &= a(bx) \\ &= a(xb) \\ &= (ax)b = (xa)b \\ &= x(ab)\end{aligned}$$

$\Rightarrow ab \in C(R)$

Hence $C(R)$ is a subring.

Question:

Let R be a ring such that $a^2 + a \in C(R) \;\forall\; a \in R$ show that R is commutative

Solution

Let $x, y \in R \Rightarrow x + y \in R$

$\Rightarrow (x+y)^2 + (x+y) \in C(R)$

$\Rightarrow x^2 + y^2 + xy + yx + x + y \in C(R)$

$\Rightarrow x^2 + x + y^2 + y + xy + yx \in C(R)$

$\because x^2 + x,\; y^2 + y \in C(R)$

$\Rightarrow xy + yx \in C(R) \qquad \because C(R)$ is subring

$\Rightarrow x(xy + yx) = (xy + yx)x$

$\Rightarrow x^2y + xyx = xyx + yx^2$

$\Rightarrow x^2y + xyx = yx^2 + xyx$

$\Rightarrow x^2 y = y x^2$

As $x^2+x \in C(R)$

$\Rightarrow y(x^2+x) = (x^2+x)y$ by definition of $C(R)$

$\Rightarrow yx^2 + yx = x^2 y + xy$

$\Rightarrow yx^2 + yx = yx^2 + xy$ $\because x^2 y = y x^2$

$\Rightarrow yx = xy$

$\Rightarrow R$ is commutative.

Question

Find all subrings of the ring of integer Z.

Solution:

Let n be a non-negative integer and

$T_n = nZ = \{nt, t \in Z\}$

As $0 \in T_n \Rightarrow T_n$ is non-empty.

Let $a, b \in T_n$

then $a = nt$, $b = ns$ for some $t, s \in Z$

$a - b = nt - ns = n(t-s) \in T_n$ | $\because t, s \in Z$, $t - s \in Z$

and also

$ab = (nt)(ns) = n(t(ns)) \in T_n$

Hence T_n is a subring

Let A be any other subring of Z

If $A = \{0\}$ then $A = 0.Z$.

Let $A \neq \{0\}$,

if $m(\neq 0) \in A$. then $-m \in A$

i.e A contains ~~pve~~ integer.

and Let $n \in A$ be least $+$tive integer

$\Rightarrow nZ \subseteq A$ ——— (i)

Let $m \in A$

then by division algorithm there are integer q and r such that

$m = nq + r$, $r < n$

As $m \in A$, $n \in A$, $nq \in A$
$\Rightarrow m - nq \in A$
i.e $r \in A$
which is a contradiction as n is least

$\Rightarrow r = 0$
$\Rightarrow m = nq \in nZ$
$\Rightarrow A \subseteq nZ$ ——— (ii)

by (i) and (ii)
$A = nZ = T_n$

Hence all subrings of Z are of the form nZ.

17-4-04

Ideals

def:- A subring S of a ring R is called right ideal in R if $s \in S$ and $a \in R \Rightarrow sa \in S$
Similarly, if $as \in S$ then S is left ideal
If a subring is left ideal as well as right ideal then it is simply called ideal.

OR

A non-empty subset S of a ring R is ideal if for $s_1, s_2 \in S$, $a \in R$
$s_1 - s_2 \in S$ & $as, sa \in S$.

Note:
Every ring has atleast two ideals, one is $\{0\}$ and second is R itself.
ideal $\{0\}$ is called null ideal and R itself is called unit ideal or improper ideal
For an ideal S if $S \neq R$ then S is called proper ideal.

Lemma:

A field F contain no proper ideal other than null ideal.

Proof:

Let I be an ideal of a field F such that $I \neq \{0\}$

Let $a \neq 0 \in I$, $a^{-1} \in F$

$\Rightarrow a^{-1}a \in I$ by definition of ideal.

i.e $1 \in I$

Now $1 \in I$ and $x \in F$

$x \cdot 1 \in I$ by definition of ideal

i.e $x \in I$

$\Rightarrow F \subseteq I$ ——— (i)

but

$I \subseteq F$ ——— (ii) $\because$ I is subset of F

From (i) and (ii)

$I = F$

Hence field F has no proper ideal other than $\{0\}$.

Theorem

A non-zero commutative ring with unity is a field if it has no proper ideal.

Proof:

Let R be a non-zero commutative ring with unity and $a(\neq 0) \in R$

then the set Ra is an ideal of R, ~~because~~

For $x, y \in Ra$

$\Rightarrow x = r_1 a \,,\; y = r_2 a$ for some $r_1, r_2 \in R$

$x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a \in Ra \quad \because r_1 - r_2 \in R$

and if $r \in R$

then $rx = r(r_1 a) = (r r_1) a \in Ra$

$\Rightarrow Ra$ is an ideal.

Now if R has no proper ideal then

$Ra = R$

For $1 \in R = Ra \quad \exists$ an element $b \in R$

such that $ba = 1$

i.e R contains inverse of each element

So R is field.

4-2004

Quotient Ring:-

def:- Let S be an ideal of a ring R. Then for $a \in R$, the set

$R/S = \{ S + a \,,\; a \in R \}$ with the following two operation

(i) $(S+a) + (S+b) = S + (a+b)$

$(S+a)\cdot(S+b) = S + ab$

is called Quotient ring.

Homomorphism of a Ring:-

def:- A mapping $\phi : R \to R'$ is called homomorphism if

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\cdot\phi(b)$$

Kernel of Homomorphism:-

def:- Let ϕ be a homomorphism of a ring R onto a ring R'. those element of R which map onto 0 is called $\ker\phi$.

i.e $\forall\ a \in R$ such that $\phi(a) = 0$

Lemma:-

If S is an ideal of a ring R, then the mapping $\phi : R \to R/S$ defined by

$$\phi(a) = S + a \text{ is homomorphism.}$$

Solution

For $a, b \in R$

$$\phi(a+b) = S + (a+b)$$
$$= (S+a) + (S+b)$$
$$= \phi(a) + \phi(b)$$

and

$$\phi(ab) = S + ab$$
$$= (S+a)\cdot(S+b)$$
$$= \phi(a)\cdot\phi(b)$$

hence ϕ is homomorphism.

Lemma:-

If φ is a homomorphism of R into R', then $\ker\varphi$ is a subring of R.

Proof:

Let $a, b \in \ker\varphi$

$\Rightarrow \varphi(a) = 0 \quad , \varphi(b) = 0$.

Now $\varphi(a-b) = \varphi(a) - \varphi(b) \quad \because \varphi$ is homomorphism

$= 0 - 0 = 0$

$\Rightarrow a - b \in \ker\varphi$.

Also

$\varphi(ab) = \varphi(a)\cdot\varphi(b) \quad \because \varphi$ is homomorphism

$= 0 \cdot 0 = 0$

$\Rightarrow ab \in \ker\varphi$

i.e $a-b, ab \in \ker\varphi \Rightarrow \ker\varphi$ is subring.

Lemma:-

A homomorphism φ from a ring R onto a ring R' is isomorphism iff $\ker\varphi = \{0\}$.

Proof:

Let $\ker\varphi = \{0\}$

For $a, b \in R$

if $\varphi(a) = \varphi(b)$

$\Rightarrow \varphi(a) - \varphi(b) = 0$

$\Rightarrow \varphi(a-b) = 0 \quad \because \varphi$ is homomorphism

$\Rightarrow a - b \in \ker\varphi = \{0\}$

$\Rightarrow a - b = 0$

$\Rightarrow a = b \Rightarrow \varphi$ is one-one

hence φ is isomorphism.

Conversely,

Let φ is isomorphism

Let $a \in \ker\varphi$

$\Rightarrow \varphi(a) = 0 = \varphi(0) \Rightarrow a = 0 \quad \because \varphi$ is one-one *

* $\Rightarrow \ker\varphi = \{0\}$

proved.

Lemma:-

If ϕ is homomorphism of R onto R'
then (i) $\phi(0) = 0$
(ii) $\phi(-a) = -\phi(a)$

Proof.

i) $\phi(a+0) = \phi(a) + \phi(0)$
$\Rightarrow \phi(a) = \phi(a) + \phi(0)$
$\Rightarrow 0 = \phi(0)$ by cancellation law.

ii) $\phi(a-a) = \phi(a+(-a))$
$\Rightarrow \phi(0) = \phi(a) + \phi(-a)$
$\Rightarrow 0 = \phi(a) + \phi(-a)$
$\Rightarrow \phi(-a) = -\phi(a)$

proved.

Question:- Let $\phi : R \rightarrow R'$ be a homomorphism then Show that $\ker\phi$ is an ideal of R.

Solution:

Let $x \in \ker\phi$ and $a \in R$
then $\phi(x) = 0$
Now $\phi(ax) = \phi(a).\phi(x)$ $\because \phi$ is homomorphism
$= \phi(a)\cdot 0 = 0$
$\Rightarrow ax \in \ker\phi$
and $\phi(xa) = \phi(x).\phi(a)$ $\because \phi$ is homomorphism.
$= 0\cdot\phi(a) = 0$
$\Rightarrow xa \in \ker\phi$.

$\Rightarrow \ker\phi$ is an ideal of R.

* Also prove that it is a subring.

Question:

If U and V are ideals of R, prove that
$U+V = \{u+v : u \in U \wedge v \in V\}$ is also ideal of R.

Solution:-

For $a_1, a_2 \in U$ and $b_1, b_2 \in V$
consider $a_1+b_1,\ a_2+b_2 \in U+V$
then $(a_1+b_1)-(a_2+b_2) = (a_1-a_2)+(b_1-b_2) \in U+V$
as U and V are ideal of R
$a_1, a_2 \in U \Rightarrow a_1-a_2 \in U$ and $b_1, b_2 \in V \Rightarrow b_1-b_2 \in V$
$\Rightarrow U+V$ is a subgroup of R under addition
Now
for $r \in R$ and $a+b \in U+V$
$r(a+b) = ra+rb \in U+V$
because $r \in R,\ a \in U \Rightarrow ra \in U$
and $r \in R,\ b \in V \Rightarrow rb \in V$
Similarly
$(a+b)r = ar+br \in U+V$

Hence $U+V$ is an ideal of R.

Question:

If U, V are ideals of a ring R, then prove that the set UV of all elements that can be written as finite sum of elements of the form uv where $u \in U$ and $v \in V$ is also an ideal of R.

Solution:-

Consider $x, y \in UV$ such that
$$x = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$
$$y = a_1'b_1' + a_2'b_2' + \cdots + a_n'b_n'$$
where $a_i, a_i' \in U$ and $b_i, b_i' \in V$ for each i
Now
$$x-y = (a_1b_1 + \cdots + a_nb_n) - (a_1'b_1' + \cdots + a_n'b_n')$$
$$= a_1b_1 + \cdots + a_nb_n + (-a_1')b_1' + \cdots + (-a_n')b_n' \in UV$$

Question:

If I_1 and I_2 are ideal of a ring R then prove that $I_1 I_2 \subseteq I_1 \cap I_2$

Solution

Consider $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in I_1 I_2$

where $a_i \in I_1$ and $b_i \in I_2$

then

$a_i b_i \in I_1$ since I_1 is an ideal, $b_i \in I_2 \subseteq R$.

$\Rightarrow a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in I_1$ ——— (i)

Also

$a_i b_i \in I_2$ as I_2 is ideal and $a_i \in I_1 \subseteq R$.

$\Rightarrow a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in I_2$ ——— (ii)

From (i) and (ii)

$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in I_1 \cap I_2$

Hence $I_1 I_2 \subseteq I_1 \cap I_2$

Principal Ideal

—: An ideal I of a ring R is said to be a principal ideal if $I = aR$ and is usually denoted by $\langle a \rangle$.

Principal Ideal Ring:

—: A principal ideal ring is a ring in which every ideal is principal ideal. ~~we shall write~~

Theorem

—: The proper ideal of a ring can not contain the identity element.

Proof:

Find yourself.

****

Maximal Ideal

def:- A maximal ideal of ring R is an ideal M different from R such that there is no proper ideal N of R containing M.

Explanation:-

In other word, an ideal of R is a maximal ideal if it is impossible to squeeze an ideal between it and the full ring. Given a ring there is no guarantee that it has any maximal ideals in a ring R. Also there may be many distinct maximal ideal in a ring R

Example:

In the set of integers

$$\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \ldots\}$$

$\langle 2 \rangle = 2\mathbb{Z} = \{0, \pm2, \pm4, \pm6, \ldots\}$ is a maximal ideal

and $\langle 4 \rangle = \{0, \pm4, \pm8, \ldots\}$ is not a maximal ideal.

Since $\langle 4 \rangle \subseteq \langle 2 \rangle \subset \mathbb{Z}$

Lemma

-: In a ring of integers the ideal $\langle n \rangle$, where $n \geq 1$, is maximal iff n is prime

Proof:

Let $\langle n \rangle$ is maximal in $\mathbb{Z}$, we have to show that n is prime.

Let us suppose that n is not prime then obviously n is composite

Let $n = n_1 \cdot n_2$, where n_1, n_2 are prime and we choose them such that $1 < n_1 < n_2$

and $1 < n_1 < n_2 < n$

$$\Rightarrow \langle n \rangle \subset \langle n_1 \rangle \subseteq \mathbb{Z}$$

but $\langle n \rangle$ is maximal so we have a contradiction to the fact that $\langle n \rangle$ is maximal so our supposition that n is composite is wrong hence n is prime.

Conversely, we have that $\langle n \rangle$ is prime and we have to show that $\langle n \rangle$ is maximal.

Let us suppose that $\langle n \rangle$ is not maximal and let $\langle m \rangle$ be maximal ideal then

$$\langle n \rangle \subset \langle m \rangle$$

$$\Rightarrow m \mid n.$$

But n is prime, hence we have a contradiction

$$\Rightarrow \langle n \rangle \text{ is a maximal ideal.}$$

Ideal generated by $I \cup \langle a \rangle = (I, a)$

—: Let R be a ring and, I and J be the ideals of R. Then their sum

$$I + J = \{a + b \mid a \in I, b \in J\}$$

is an ideal of R, which contains both the ideal I and J and is called the ideal generated by $I \cup J$.

Let us take $a \in R$, then $aR = \langle a \rangle = \{ar \mid r \in R\}$ is also an ideal of R, called the ideal of R generated by the element a.

Let I be an ideal of R and $a \in R$, $a \notin I$ then $I + \langle a \rangle$ is an ideal of R, whose elements are of this type $I + \langle a \rangle = \{i + ar \mid i \in I, r \in R\}$ called the ideal generated by $I \cup \langle a \rangle$. This ideal will be denoted by (I, a).

Theorem

:- I is maximal in R iff $(I,a)=R$ for $\forall$ $a\in R, a\notin I$.

Proof

Let I is maximal in R, we have to show that $(I,a)=R$ for $a\in R$, $a\notin I$.

We know that

$$I\subseteq (I,a)\subseteq R \quad \text{for } a\notin I, a\in R.$$

Since I is maximal

therefore $(I,a)=R$

Conversely, Let $(I,a)=R$ $\forall$ $a\in R$, $a\notin I$.

we have to show that I is maximal.

Let I is not maximal J is maximal ideal

then $I\subseteq J$.

$\Rightarrow I\subseteq J\subseteq R$

we have to show that $J=R$

Let $a\in J$, $a\notin I$

$\Rightarrow I\subset (I,a)\subseteq J\subseteq R$.

$\Rightarrow R\subseteq J\subseteq R \quad \because (I,a)=R$

$\Rightarrow J=R$

$\Rightarrow I$ is a maximal ideal

Theorem

:- Let R be commutative ring with unity Let M be an proper ideal of R, then M is maximal iff R/M is Field.

Proof:

Suppose M is a maximal ideal in R. It is easy to see that if R is a commutative ring with unity, then R/M is also a commutative ring with unity if $M\neq R$, which is the case when M is maximal.

Let $a+M\in R/M$, with $a\notin M$, so that

$a+M$ is not the additive identity of R/M;
we have to show that $a+M$ has a multiplicative inverse in R/M.

Since M is maximal in $R \Rightarrow (M, a) = R$
The elements of (M,a) are of the form
$$(M,a) = \{m + ar : m \in M, r \in R\}$$
$\because 1 \in R \Rightarrow 1 \in (M,a)$
$\Rightarrow 1 = m + ar$ for some $m \in M$, $r \in R$.
$\Rightarrow 1 - ar = m \in M$
$\Rightarrow 1 + M = ar + M$ $\quad \because ab^{-1} \in H \Rightarrow aH = bH$
$\Rightarrow 1 + M = (a+M)(r+M)$
$\because 1+M$ is identity w.r.t multiplication of R/M
$\therefore a+M$ is multiplicative inverse of $r+M$
$\Rightarrow R/M$ is a field.

Conversely, suppose that R/M is a field. To show M is maximal we suppose that M is not maximal. Let J be the maximal ideal such that $M \subset J \subset R$.
Let $a \notin M$, $a \in J$
$\Rightarrow a + M$ is non-zero element
$\therefore$ it has multiplicative inverse in R/M as it is field.
Let $b + M$ is its multiplicative inverse
where $b \notin M$, $b \in J$.

Then $(a+M)(b+M) = 1 + M$
$\Rightarrow ab + M = 1 + M$
$\Rightarrow -ab + 1 \in M$
Now $1 = ab + (-ab + 1)$
$\because -ab + 1 \in M \subset J$, $ab \in J$ as $a, b \in J$
$\Rightarrow 1 \in J$
but we know that proper ideal can not contain the identity element $\Rightarrow J$ is improper (Theorem)
$\Rightarrow J = R$
$\Rightarrow M$ is a maximal ideal.

Theorem (Fundamental Homomorphism Theorem).

Let ϕ be a homomorphism of a ring R into ring R' with kernel K. Then $\phi(R)$ is a ring and $\phi(R) \cong R/K$

Proof:

$\because$ R is ring.

i.e R is abelian group under addition

R is semi-group under multiplication

and Distributive Law holds in R.

$\because$ $\phi(R)$ is homomorphic image of R

and homomorphic image of a group is a group

$\therefore$ $\phi(R)$ is abelian group under addition

$\phi(R)$ is semi-group under multiplication

and for distributive law

Let $a, b, c \in R \Rightarrow \phi(a), \phi(b), \phi(c) \in \phi(R)$

Now $\phi(a)[\phi(b)+\phi(c)] = \phi(a)[\phi(b+c)]$ $\because \phi$ is homomorphism

$= \phi[a(b+c)]$

$= \phi[ab+ac]$ $\because a, b, c \in R$ (ring)

$= \phi(ab) + \phi(ac)$

$= \phi(a).\phi(b) + \phi(a).\phi(c)$

i.e left distributive law holds

Similarly we can prove for right distributive law

$\Rightarrow \phi(R)$ is a ring.

Now to prove $R/K \cong \phi(R)$ or $\phi(R) \cong R/K$

define a mapping $\psi : R/K \rightarrow \phi(R)$

by $\psi(a+K) = \phi(a)$; $a \in R$.

then ψ is well define as

if $a+K = b+K$

$\Rightarrow a = b+K$

Now $\psi(a+K) = \phi(a)$

$= \phi(b+K)$ $\because a = b+K$

$\Rightarrow \psi(a+K) = \phi(b) + \phi(K)$

$\Rightarrow \phi(b) + 0'$ $\because \phi(K) = 0'$

$= \phi(b)$

$= \psi(b+K) \Rightarrow \psi$ is well define.

Obviousely, ψ is onto as each $\phi(a) \in \phi(R)$ is an image of $a+K \in R/K$

ψ is one-one as

if $\psi(a+K) = \psi(b+K)$

$\Rightarrow \phi(a) = \phi(b)$

$\Rightarrow \phi(a) - \phi(b) = 0$

$\Rightarrow \phi(a-b) = 0$

$\Rightarrow a-b \in K$ i.e. $a \in b+K$

hence $a+K = b+K \Rightarrow \psi$ is one-one

Now

$\psi[(a+K)+(b+K)] = \psi[(a+b)+K]$

$= \phi(a+b)$

$= \phi(a) + \phi(b)$ $\because \phi$ is homomorphism

$= \psi(a+K) + \psi(b+K)$

and

$\psi[(a+K)(b+K)] = \psi[ab+K]$

$= \phi(ab)$

$= \phi(a)\cdot\phi(b)$ $\because \phi$ is homo.

$= \psi(a+K)\cdot\psi(b+K)$

Thus ψ is homomorphism

~~and~~ Hence $R/K \cong \phi(R)$.

****

Available online at *http://www.MathCity.org*

****