P.R. GOVT COLLEGE (A)
KAKINADA

GUNNAM PRASADA RAO

LECTURER IN MATHEMATICS

RING THEORY-SEM-IV

INTRODUCTION TO RINGS, SUBRINGS, IDEALS, HOMOMORPHISM, POLYNOMIAL RINGS

UNIT-1: RINGS AND FIELDS

Ring: A system $(R;\ +,\cdot)$ where R is a non-empty set and $+,\cdot$ are two binary operations on R is a ring if it satisfies the following conditions. (i) $(R,+)$ is an abelian group. (ii) $(R,\ \cdot)$ is a semi-group. (iii) Multiplication is distributive under addition. Here '0' is called additive identity.

Ex: 1. $(\mathbb{Z};\ +,\cdot)$ $(\mathbb{Q};\ +,\cdot)$ $(\mathbb{R};\ +,\cdot)$ $(\mathbb{C};\ +,\cdot)$ are all rings.

2. $< R = \{0,1,2,3,4,5\} +_6, \times_6 >$ is a ring.

3. $< Z_6 = \{\bar{0}, \bar{1}, \bar{2}\ \bar{3}, \bar{4}, \bar{5}\} \oplus \odot >$ is a ring

4. $E =$ The set of even integer's $= \{2n\ /\text{n}\in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4\ \ldots\}$ form a ring.

5. O = The set of all odd integers$= \{2n+1\ /\text{n}\in \mathbb{Z}\} = \{\ldots, -3, -1, 1, 3\ \ldots\}$ is not a ring.

6. The set M of 2x2 matrices whose elements are integers. i.e. $M = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in \mathbb{Z}\right\}$ then $(M;\ +,\cdot)$ is a ring.

Commutative ring: A ring $(R;\ +,\cdot)$ is said to be commutative ring if $a \cdot b = b \cdot a \quad \forall a, b \in R$

Ring with unity: A ring $(R;\ +,\cdot)$ is said to be ring with unity if there exists '1'$\in R$ such that $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$. Here '1' is called unity element in R

Commutative ring with unity: A ring $(R;\ +,\cdot)$ is said to be commutative ring with unity if

(i) $a \cdot b = b \cdot a \quad \forall a, b \in R$ (ii) if there exists '1'$\in R$ such that $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$.

Ex: 1. $(\mathbb{Z};\ +,\cdot)$ $(\mathbb{Q};\ +,\cdot)$ $(\mathbb{R};\ +,\cdot)$ $(\mathbb{C};\ +,\cdot)$ are all commutative rings with unity.

2. $E =$ The set of even integer's $= \{2n\ /\text{n}\in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4\ \ldots\}$ form a commutative ring without unity.

Boolean ring: A ring $(R;\ +,\cdot)$ is said to be Boolean ring if $a \cdot a = a \quad \forall a \in R$

$i.e.\ a^2 = a \quad \forall a \in R$ (In a ring R every element is idempotent then R is said to be Boolean ring)

Cancellation laws hold in *R*: Let $(R;\ +,\cdot)$ be ring. For $a, b, c \in R$

$(i) a \neq 0 \quad ab = ac \Longrightarrow b = c\ \ (left\ cancellation\ law)\ and$

$(ii) a \neq 0 \quad ba = ca \Longrightarrow b = c\ \ (right\ cancellation\ law)$ Then we say that Cancellation laws hold in R

Ring with zero divisors: A ring$(R;\ +,\cdot)$ is said to have zero divisors if there exists $a, b, \in R$ so that $a \neq 0, b \neq 0\ and\ \ ab = 0$

Ring with zero divisors: A ring$(R;\ +,\cdot)$ is said to have zero divisors if there exists $a, b, \in R$ so that $a \neq 0, b \neq 0\ and\ \ ab = 0$

Ex: 1.The ring $< R = \{0,1,2,3,4,5\}\ +_{6,}\ \times_6 >$ has zero divisors. Since $2,3 \in R\ \ and\ 2 \neq 0,\ 3 \neq 0\ and\ 2 \times_6 3 = 0$ also $3,4 \in R\ \ and\ 3 \neq 0,\ 4 \neq 0\ and\ 3 \times_6 4 = 0$

So the set of zero divisors of R = {2, 3, 4}

2. The ring $< R = \{0,1,2,3,4,5,6\}\ +_{7,}\ \times_7 >$ has no zero divisors. Since $1,3 \in R\ \ni\ 1 \neq 0,\ 3 \neq 0\ and\ 1 \times_7 3 = 3 \neq 0$

Ring without zero divisors: A ring$(R;\ +,\cdot)$ is said to have no zero divisors if $\forall a, b \in R$ so $and\ \ ab = 0\ then\ either\ a = 0\ or\ b = 0.$

Ex: 1. $(\mathbb{Z};\ +,\cdot)$ $(\mathbb{Q};\ +,\cdot)$ $(\mathbb{R};\ +,\cdot)$ $(\mathbb{C};\ +,\cdot)$ are all have no zero divisors.

2. The ring $< R = \{0,1,2,3,4,5,6\}\ +_{7,}\ \times_7 >$ has no zero divisors. Since $1,3 \in R\ \ni\ 1 \neq 0,\ 3 \neq 0\ and\ 1 \times_7 3 = 3 \neq 0$

Integral domain: A ring$(R;\ +,\cdot)$ is said to be an integral domain if (i) multiplication is commutative in R (ii) $R\ has\ no\ zero\ divisors$.

Note: (i) In a ring R, the additive identity is called zero element of R

(ii) In a ring R, the multiplicative identity is called unity element of R

Ex: 1. $(\mathbb{Z};\ +,\cdot)$ $(\mathbb{Q};\ +,\cdot)$ $(\mathbb{R};\ +,\cdot)$ $(\mathbb{C};\ +,\cdot)$ are all integral domain.

2. The ring $< R = \{0,1,2,3,4,5,6\}\ +_{7,}\ \times_7 >$ is an I.D

Division ring (Skew field): A ring $(R;\ +,\cdot)$ with at least two elements is said to be division ring if (i) R has unity element (ii) every non-zero element of R is invertible under multiplication.

i.e. $\forall a \neq 0\ so\ \exists b \in R\ \ni\ a \cdot b = b \cdot a\ \ = 1\ \ \therefore b\ is\ called\ inverse\ of' a'\ in\ R$

Ex: 1. $(\mathbb{Z};\ +,\cdot)$ is not division ring. (ii) $(\mathbb{Q};\ +,\cdot)$ $(\mathbb{R};\ +,\cdot)$ $(\mathbb{C};\ +,\cdot)$ are all division rings.

(iii) The ring $< R = \{0,1,2,3,4,5,6\}\ +_{7,}\ \times_7 >$ is a division ring.

Field: A ring $(R;\ +,\cdot)$ with atleast two elements is said to be field if (i) Multiplication is commutative in R (ii) R has unity element in R (iii) every non-zero element of R is invertible under multiplication.

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

Theorem 1: If R is a Boolean ring then (i) $a + a = 0 \quad \forall a \in R$ (ii) $a + b = 0 \Longrightarrow a = b$

(iii) R is commutative under multiplication (0R) If R is Boolean ring then show that R is a commutative ring.

Proof: (i) $a \in R \Longrightarrow a + a \in R$ [$\because$ $(R, +)$ is a group]

Since R is a Boolean ring so $(a + a)^2 = a + a$

$(a + a)^2 = a + a \Longrightarrow (a + a)(a + a) = (a + a)$

$\Longrightarrow a(a + a) + a(a + a) = (a + a)$ [By R.D.L]

$\Longrightarrow (a.a + a.a) + (a.a + a.a) = (a + a)$ [By L.D.L]

$\Longrightarrow (a + a) + (a + a) = (a + a)$ [$\because$ $a^2 = a \quad \forall a \in R$]

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

$\Longrightarrow (a + a) = 0$ [By R.C.L of group $(R, +)$]

(ii) $a + b = 0 \Longrightarrow a + b = a + a \quad By\ (i)$

$\Longrightarrow b = a$ [By R.C.L of group $(R, +)$]

$\Longrightarrow a = b$

(iii) $a, b \in R \Longrightarrow a + b \in R$ since R is a Boolean ring so $(a + b)^2 = a + b$

Now $(a + b)^2 = a + b \Longrightarrow (a + b)(a + b) = a + b$

$\Longrightarrow a(a + b) + b(a + b) = a + b$ [By R.D.L]

$\Longrightarrow (a.a + a.b) + (b.a + b.b) = a + b$ [By L.D.L]

$\Longrightarrow (a + a.b) + (b.a + b) = a + b$ [$\because$ $a^2 = a,\ b^2 = b \ , \forall a, b \in R$]

$\Longrightarrow (a + b) + (a.b + b.a) = a + b$ [$+ \ is \ Ass \ and \ com \ in R$]

$\Longrightarrow (a + b) + (a.b + b.a) = (a + b) + 0$

$\Longrightarrow ab + ba = 0$ [By L.C.L of group $(R, +)$]

$\Longrightarrow ab = ba$ By (ii)

$\therefore$ R is commutative under multiplication

Theorem 2: A ring R has no zero divisors iff cancellation laws holds in R

Proof: Necessary condition :($\Longrightarrow$) we can assume that R has no zero divisors

To prove cancellation laws holds in R

(i) For $a, b, c \in R \; such \; that \; a \neq 0, \quad ab = ac$

$a \neq 0, \quad ab = ac \Longrightarrow ab - ac = 0 \Longrightarrow a(b - c) = 0$

$\Longrightarrow b - c = 0 \; [\because a \neq 0 \; and \; R \; has \; no \; zero \; divisors]$

$\Longrightarrow b = c \quad \therefore \; left$ cancellation laws holds in R

(i) For $a, b, c \in R \; such \; that \; a \neq 0, \quad ba = ca$

$a \neq 0, \quad ba = ca \Longrightarrow ba - ca = 0 \Longrightarrow (b - c)a = 0$

$\Longrightarrow b - c = 0 \; [\because a \neq 0 \; and \; R \; has \; no \; zero \; divisors]$

$\Longrightarrow b = c \quad \therefore \; right$ cancellation laws holds in R

$Hence$ cancellation laws holds in R

Sufficient condition :($\Longleftarrow$) we can assume that cancellation laws hold in R

To prove that R has no zero divisors

If possible suppose R has zero divisors. i.e. $\exists \; a, b \; \in R \; so \; that \; \; a \neq 0, b \neq 0 \; and \; \; ab = 0$

$a \neq 0, and \; \; ab = 0 \Longrightarrow a \neq 0, and \; \; ab = a.0 \Longrightarrow b = 0$

$(By \; l.c.l) \; which \; is \; contradict \; to \; b \neq 0$

$\therefore \; R$ has no zero divisors

Theorem 3: A division ring has no zero divisors

Proof: Let $(R; \; +, \cdot)$ be division ring. To prove that R has no zero divisors. i.e. $a, b \; \in R \; and \; ab = 0 \Longrightarrow a = 0 \; or \; b = 0$

(i) Let $a, b \; \in R \; , \; a \neq 0, \; \; and \; ab = 0$

$since \; a \neq 0 \; , R \; is \; a \; division \; ring$

$\Longrightarrow \; \exists \; a^{-1} \in R \ni aa^{-1} = a^{-1}a = 1 \; [\; Every \; non \; zero \; element \; has \; multiplicative \; inverse]$

$ab = 0 \Longrightarrow a^{-1}(ab) = a^{-1}.0 \Longrightarrow (a^{-1}a)b = 0 \Longrightarrow 1.b = 0 \Longrightarrow b = 0$ $[R\ has\ unity\ element\ ]$

(ii) Let $a, b \in R$, $b \neq 0$, $and\ ab = 0$

$since\ b \neq 0\ , R\ is\ a\ division\ ring$

$\Longrightarrow \exists\ b^{-1} \in R \ni bb^{-1} = b^{-1}b = 1$ [$Every\ non\ zero\ element\ has\ multiplicative\ inverse$]

$ab = 0 \Longrightarrow (ab)b^{-1} = 0.b^{-1} \Longrightarrow a(bb^{-1}) = 0 \Longrightarrow a.1 = 0 \Longrightarrow a = 0$ $[R\ has\ unity\ element\ ]$

Hence $a, b \in R\ and\ ab = 0 \Longrightarrow a = 0\ or\ b = 0$ $\therefore$ R has no zero divisors

Theorem 4: A field has no zero divisors

Proof: Let $(F;\ +,\cdot\ )$ be field.

(i) Let $a, b \in F$, $a \neq 0$, $and\ ab = 0$

$since\ a \neq 0\ , F\ is\ a\ field \Longrightarrow \exists\ a^{-1} \in F \ni aa^{-1} = a^{-1}a = 1$

$a \neq 0$, $ab = 0 \Longrightarrow a^{-1}(ab) = a^{-1}.0 \Longrightarrow (a^{-1}a)b = 0 \Longrightarrow 1.b = 0 \Longrightarrow b = 0$

Thus $a, b \in F$, $a \neq 0$, $and\ ab = 0 \Longrightarrow b = 0$

(ii) Let $a, b \in F$, $b \neq 0$, $and\ ab = 0$

$since\ b \neq 0\ , F\ is\ a\ field \Longrightarrow \exists\ b^{-1} \in F \ni bb^{-1} = b^{-1}b = 1$

$b \neq 0$, $\quad ab = 0 \Longrightarrow (ab)b^{-1} = 0.b^{-1} \Longrightarrow a(bb^{-1}) = 0 \Longrightarrow a.1 = 0 \Longrightarrow a = 0$

Hence $a, b \in F\ and\ ab = 0 \Longrightarrow a = 0\ or\ b = 0$ $\therefore$ F has no zero divisors

Theorem5: Every field is an integral domain. Is the converse true?

Proof: To prove that every field is an integral domain. For this we have to show that a field F has no zero divisors.

(i) Let $a, b \in F$, $a \neq 0$, $and\ ab = 0$

$since\ a \neq 0\ , F\ is\ a\ field \Longrightarrow \exists\ a^{-1} \in F \ni aa^{-1} = a^{-1}a = 1$

$a \neq 0$, $ab = 0 \Longrightarrow a^{-1}(ab) = a^{-1}.0 \Longrightarrow (a^{-1}a)b = 0 \Longrightarrow 1.b = 0 \Longrightarrow b = 0$

Thus $a, b \in F$, $a \neq 0$, $and\ ab = 0 \Longrightarrow b = 0$

(ii) Let $a, b \in F$, $b \neq 0$, $and\ ab = 0$

$since\ b \neq 0\ , F\ is\ a\ field \Longrightarrow \exists\ b^{-1} \in F \ni bb^{-1} = b^{-1}b = 1$

$b \neq 0, \quad ab = 0 \Longrightarrow (ab)b^{-1} = 0.b^{-1} \Longrightarrow a(bb^{-1}) = 0 \Longrightarrow a.1 = 0 \Longrightarrow a = 0$

Hence $a, b \in F \; and \; ab = 0 \Longrightarrow a = 0 \; or \; b = 0 \; \therefore \; F$ has no zero divisors

The converse of the theorem need not be true. i.e. An integral domain need not be field.

For example, the ring of integers $(\mathbb{Z};\ +,\cdot)$ is an integral domain but it is not a field because

$4 \neq 0 \in \mathbb{Z} \; has \; no \; multiplicative \; inverse \; in \; \mathbb{Z}.$

Theorem6: A finite integral domain is a field.

Proof: Let $(D;\ +,\cdot)$ be an integral domain with ' n' elements.

To prove that D is a field. We have to show that (i) D has a unity element (ii) every non zero element has multiplicative inverse.

Let $D = \{ x_1, x_2, x_3 \ldots, x_n\}$ and $a \neq 0 \in D$,

Consider the set $aD = \{ ax_1, ax_2, ax_3 \ldots, ax_n\}$

Let $p \in aD \; then \; p = ax_r \quad where \; x_r \in D \quad 1 \leq r \leq n$

Since $a \in D, \quad x_r \in D \; \; and \; D \; is \; an \; integraldomain \Longrightarrow ax_r \in D \Longrightarrow p \in D \Longrightarrow aD \subseteq D$

If possible, suppose $ax_i = ax_j \quad for \; 1 \leq i, j \leq n \quad and \; \; i \neq j$

$\Longrightarrow a(x_i - x_j) = 0 \Longrightarrow x_i - x_j = 0 \Longrightarrow x_i = x_j \quad [\because \; a \neq 0 \; and \; D \; has \; no \; zero \; divisors]$

Which is contradiction to D has 'n 'distinct elements.
So $aD \; has \; 'n' \; distinct \; elements, D \; has \; 'n' distinct \; elements \; \; and \; \; aD \subseteq D \quad so \; \; \therefore aD = D$

For $a \neq 0 \in D \; , since \; aD = D \Longrightarrow a \in aD \Longrightarrow a = ax_e \quad forsome \; x_e \in D$

Since $D \; is \; commutative \quad \therefore \; a = ax_e = x_e a$

We now prove that x_e is the unity element. Let $y \in D \quad \therefore \; y \in aD \Longrightarrow y = ax_k \quad forsome \; x_k \in D$

$x_e y = x_e(ax_k \;) = (x_e a)x_k = ax_k = y$ Since $D \; is \; commutative \quad y = x_e y = yx_e$

$\therefore \; x_e(= 1)$ is the unity element.

$\therefore 1 \in D \; , we \; have \; 1 \in aD \Longrightarrow 1 = ax_l \quad forsome \; x_l \in D$

$\therefore a \neq 0 \in D \; \exists \; x_l \in D \ni ax_l = x_l a = 1$ [Since $D \; is \; commutative$]

$\Longrightarrow Every \; non \; zero \; element \; has \; multiplicative \; inverse.$ Hence $D \; is \; a field.$

Problems:

1. Show that $R = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$ form a field under usual addition and multiplication.

Sol: $R = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$. Let $x, y, z \in R$ *so that* $x = a_1 + b_1\sqrt{2}$,

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

I: $(R, +)$ *is an abelian group*

(i) Closure property: $x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = a + b\sqrt{2} \in R$

where $a = a_1 + a_2 \in \mathbb{Q}$ $\quad$ *and* $\quad b = b_1 + b_2 \in \mathbb{Q}$

(ii) Commutative property:

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

(iii) Associative property: $(x + y) + z = [(a_1 + a_2) + a_3] + [(b_1 + b_2) + b_3]\sqrt{2}$

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

(iv) Clearly $0 = 0 + 0\sqrt{2}$ *is the additive identity*

(v) Clearly $(-a) + (-b)\sqrt{2}$ *is the inverse of* $a + b\sqrt{2}$

II: $(R, \cdot)$ *is semi group*

(vi) $xy = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ also $xy = yx \ \forall x, y \in \mathbb{Q}(\sqrt{2})$

(vii) $(xy)z = \left[(a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\right].\left(a_3 + b_3\sqrt{2}\right)$

$= (a_1a_2a_3 + 2b_1b_2a_3 + 2a_1b_2b_3 + 2a_2b_1b_3) + \sqrt{2}(a_1b_2a_3 + a_2b_1a_3 + a_1a_2b_3 + 2b_1b_2b_3)$

similarly we can prove that $\quad x(yz) = (a_1a_2a_3 + 2b_1b_2a_3 + 2a_1b_2b_3 + 2a_2b_1b_3)$

$+\sqrt{2}(a_1b_2a_3 + a_2b_1a_3 + a_1a_2b_3 + 2b_1b_2b_3)$ $\quad \therefore (xy)z = x(yz)$

III: Distributive laws

$x.(y + z) = \left(a_1 + b_1\sqrt{2}\right).\left[(a_2 + a_3) + (b_2 + b_3)\sqrt{2}\right] = [a_1a_2 + a_1a_3 + 2(b_1b_2 + b_1b_3)$

$+\sqrt{2}(a_2b_1 + a_3b_1 + a_1b_2 + a_1b_3)$

$xy + xz = \left[(a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\right] + (a_1a_3 + 2b_1b_3) + (a_1b_3 + a_3b_1)\sqrt{2}$

$\therefore x(y+z) = xy + xz \quad also\ we\ can\ prove\ (y+z).x = yx + zx$

IV: unity element: Let $1 = 1 + 0\sqrt{2}\ then\ for\ any\ x = a + b\sqrt{2}$

$we\ have\ x.1 = 1.x = x \qquad \forall x \in \mathbb{Q}(\sqrt{2})$

V: Inverse property: Let $a + b\sqrt{2} \neq 0 \in \mathbb{Q}(\sqrt{2})\ then\ \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \sqrt{2}\left(-\frac{b}{a^2-2b^2}\right)$

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

$\therefore Every\ non\ zero\ element\ has\ multiplicative\ inverse$

$So\ (\mathbb{Q}(\sqrt{2}), +, \cdot) is\ a\ field.$

2. Give an example of division ring which is a not a field

Sol: Consider the set $M = \left\{\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix} / a, b, c, d \in \mathbb{R}\right\} of\ 2 \times 2$ matrices whose elements are complex numbers.

We know that $(M;\ +, \cdot)$ is a ring under matrices addition and multiplication.

(i) $\begin{bmatrix} a_1+ib_1 & c_1+id_1 \\ -c_1+id_1 & a_1-ib_1 \end{bmatrix} + \begin{bmatrix} a_2+ib_2 & c_2+id_2 \\ -c_2+id_2 & a_2-ib_2 \end{bmatrix}$

$= \begin{bmatrix} (a_1+a_2)+i(b_1+b_2) & (c_1+c_2)+i(d_1+d_2) \\ (-c_1-c_2)+i(d_1+d_2) & (a_1+a_2)-i(b_1+b_2) \end{bmatrix} = \begin{bmatrix} p+iq & r+is \\ -r+is & p-iq \end{bmatrix} \in M$

$where \quad p = (a_1+a_2), \qquad q = (b_1+b_2) \quad r = (c_1+c_2), \quad s = (d_1+d_2) \in \mathbb{R}$

$\therefore\ '+' is\ binary\ operation\ on\ M$

(ii) We know that matrices addition is commutative and associative.

(iii) Clearly $0 = \begin{bmatrix} 0+i0 & 0+i0 \\ -0+i0 & 0-i0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

(iv) Let $A \in M\ where\ A = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}\ then - A = \begin{bmatrix} -(a+ib) & -(c+id) \\ -(-c+id) & -(a-ib) \end{bmatrix} \in M$

We have $A + (-A) = (-A) + A = 0$

(v) Clearly $A.B = \begin{bmatrix} a_1+ib_1 & c_1+id_1 \\ -c_1+id_1 & a_1-ib_1 \end{bmatrix} . \begin{bmatrix} a_2+ib_2 & c_2+id_2 \\ -c_2+id_2 & a_2-ib_2 \end{bmatrix} = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix} \in M$

(vi)We know that matrices multiplication is associative

(vii) We know that matrices multiplication is distributive under addition

(viii)Clearly $\begin{bmatrix} 1+i0 & 0+i0 \\ -0+i0 & 1-i0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the unity element

(ix) Let $A \neq 0 \in M \ni A = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$ $where\ \ a,b,c,d \in \mathbb{R}$

$detA = (a+ib)(a-ib) - (c+id)(-c+id) = a^2+b^2 — (-c^2-d^2)$

$= a^2+b^2+c^2+d^2 \neq 0$

$Every\ A \neq 0 \in M\ is\ a\ non-singular\ matrices\ and\ hence\ invertiable$

$M\ is\ a\ division\ ring\ but\ not\ field\ because\ matrix\ multiplication\ is\ not\ a\ commutative.$

3. Show that the set $z[i] = \{a+ib/a\,, b \in \mathbb{Z}\}$of Gaussian integers is an integral domain under usual addition and multiplication. Is it a field?

Sol: $z[i] = \{a+ib/a\,, b \in \mathbb{Z}\}$ $Let\ x,y,z \in z[i]$

$so\ that \quad x = a_1+ib_1,\ \ y = a_2+ib_2,\ \ z = a_3+ib_3\ where\ a_1,a_2,a_3,b_1,b_2,b_3 \in \mathbb{Z}$

Now $x+y = (a_1+ib_1)+(a_2+ib_2) = (a_1+a_2)+i(b_1+b_2) = p+iq \in z[i]$

$where\ p = (a_1+a_2) \in \mathbb{Z}, \qquad q = (b_1+b_2) \in \mathbb{Z}$

$\therefore\ '+'is\ binary\ operation\ on\ z[i]$

$xy = (a_1+ib_1).(a_2+ib_2) = (a_1a_2-b_1b_2)$+i$((a_1b_2+b_1a_2) = c+id \in z[i]$

$where\ c = (a_1a_2-b_1b_2), \quad d = (a_1b_2+b_1a_2) \in \mathbb{Z}$

$\therefore\ \ '\cdot'is\ binary\ operation\ on\ z[i]$

Since the elements of $z[i]$ are also complex numbers. We have that

(i) Addition and multiplication are commutative in $z[i]$

(ii) Addition and multiplication are associative in $z[i]$

(iii) Multiplication is distributive under addition in $z[i]$

(iv) Clearly the zero elements $0+i(0)$, $the\ unity\ element\ 1+i(0)$

(v) For every $x = a+ib \in z[i]$,

$we\ have\ \ -x = -(a+ib) so\ that\ x + (-x) = [a + (-a) + i[b + (-b)] = 0 + i(0)$

$\therefore$ ($z[i]$; $+, \cdot$) is a commutative ring with unity.

For $x, y \in z[i]\ \ and\ xy = 0 \Longrightarrow x = 0\ or\ y = 0\ since\ \ x, y\ are\ comple\ numbers$

$\therefore$ ($z[i]$; $+, \cdot$) is an integral domain with unity.

Let $a = 3 + 4i \neq 0 \in z[i]\ \ we\ have\ b = \frac{3}{25} + i\left(-\frac{4}{25}\right) so\ that\ a.b = (3+4i)\left[\frac{3}{25} + i\left(-\frac{4}{25}\right)\right]$

$= \frac{9}{25} + \frac{16}{25} + i\left(\frac{12}{25} - \frac{12}{25}\right) = 1 + i(0), \qquad but\ \frac{3}{25} + i\left(-\frac{4}{25}\right) \notin z[i]\ \ as \frac{3}{25}, -\frac{4}{25} \notin \mathbb{Z}$

$\therefore Every\ non\ zero\ element\ in\ \mathbb{Z}\ is\ not\ a\ invertiable\ and\ hence\ z[i]\ \ \ is\ not\ field.$

Characteristic of ring : The characteristic of a ring $\boldsymbol{R}$ is defined as the least positive integer p such that $pa = 0\ \ \forall a \in R$. In case such a positive integer does not exist then we say that the characteristic of $R$is zero or infinite.

Ex: 1. $R = \{0,1,2,3,4,5,\}$ is a $ring\ under\ +_6, \times_6$. So the cha of $R = 6$.

2. The char of a ring $(\mathbb{Z};\ +, \cdot\ )$ is zero. Since$\exists\ does\ not\ exist\ a\ positive\ integer$

$such\ that\ na = 0\ \ \forall a \in \mathbb{Z}$

Theorem1: If R is a non-zero ring such that $a^2 = a\ \ \forall a \in R$ then char of R is 2.

Proof: $Let\ a \in R,\ \ a \in R, and\ R\ is\ a\ group \Longrightarrow a + a \in R$

$since\ a^2 = a\ \ \forall a \in R$

$\therefore (a+a)^2 = a + a \Longrightarrow (a+a)(a+a) = a + a$

$\Longrightarrow a(a+a) + a(a+a) = a + a$ [by R.D.L]

$\Longrightarrow (a.a + a.a) + (a.a + a.a) = (a + a)$ [by L.D.L]

$\Longrightarrow (a+a) + (a+a) = (a+a)$ [since $a^2 = a$]

$\Longrightarrow (a+a) + (a+a) = (a+a) + 0$ (by l.cl of a group (R, +)]

$\Longrightarrow (a+a) = 0 \Longrightarrow 2a = 0$

Further $a \neq 0 \quad 1.a = a \neq 0 \Longrightarrow 1.a \neq 0 \quad [If\ 1.a = 0\ \forall a \in R\ then\ R = \{0\}]$

$\therefore 2\ is\ the\ least\ positive\ intege\ such\ that\ 2.a = 0\ \ \forall a \in R$

Theorem2: If char of R is 2 and a, b such that a and b are commute then

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

Proof: $a, b \in R \Longrightarrow a + b \in R$

$\therefore (a+b)^2 = (a+b)(a+b) = (a+b)a + (a+b).b$

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

$= a^2 + 2ab + b^2$ [since $a, b \in R \Longrightarrow ab \in R$ *and char of* $R = 2$ *so* $2ab = 0$]

$= a^2 + b^2$

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

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

Theorem3: The characteristic of an integral domain is either a prime number or a zero.

Proof: Let $(R;\ +,\cdot)$ be an integral domain and $a \neq 0 \in R$

Case (i): If $o(a) = 0$ a *is consider as an element of the group* $(R;+)$

$\therefore$ *char of* $R = 0$ [$\because$ *If any element of a ring* R *is order zero, regarded as a member of the additive group of* R *the char of* R *is zero*]

Case (ii): If $o(a) =$ is finite, Let $o(a) = p$ where p is the positive integer

By known theorem; The char of an integral domain is the order of any non-zero element of R, regarded as a member of additive group (R; +).

$\therefore$ *char of* $R = p$ To prove that P is prime

If possible, suppose P is not a prime.

$\therefore p = p_1 p_2$ *where* $p_1 \neq 1, p_2 \neq 1$ *and* $p_1 < p$ *also* $p_2 < p$

Since R has no zero divisors, the product of any non-zero elements cannot be zero.

$\therefore a \neq 0 \Longrightarrow a.a \neq 0 \Longrightarrow a^2 \neq 0 \in R$

$\therefore o(a^2) = p \Longrightarrow p$ *is the least positive integer such that* $pa^2 = 0$

$\Longrightarrow (p_1 p_2)a^2 = 0 \Longrightarrow (p_1 a)(p_2 a) = 0$

$\Longrightarrow p_1 a = 0$ *or* $p_2 a = 0$ $(since\ R\ has\ no\ zero\ divisors)$

This is a contradiction [$\therefore o(a) = p \; and \;\; p_1 < p \, , \;\; p_2 < p \Longrightarrow pa = 0 \; but \; p_1 a \neq 0, p_2 a \neq 0$]

$\therefore$ Our supposition is wrong so P is a prime.

Hence the char of R is either a prime or a zero.

Theorem4: The characteristic of a field/ division ring is either a prime number or a zero

Proof: we know that every field is an integral domain. And write the proof of above theorem.