11 Years
Solved Papers
2009-2019

MADE EASY
Publications

Civil Services
Main Examination

TOPICWISE PREVIOUS YEARS' SOLVED PAPERS

Mathematics
Paper-II

1 Modern Algebra

1. Groups

1.1 If $\mathbb{R}$ is the set of real number and $\mathbb{R}_+$ is the set of positive real numbers, show that $\mathbb{R}$ under addition $(\mathbb{R}, +)$ and $\mathbb{R}_+$ under multiplication $(\mathbb{R}, +)$ are isomorphic. Similarly, if $\mathbb{Q}$ is the set of rational numbers and $\mathbb{Q}_+$ the set of positive rational numbers, are $(\mathbb{Q}, +)$ and $(\mathbb{Q}_+, \cdot)$ isomorphic? Justify your answer.

(2009 : 4+8=12 Marks)

Solution:

Let $\mathbb{R}$ be the set of real number and $\mathbb{R}_+$ be the set of positive real number.

We have to show

$$(\mathbb{R},+) \cong (\mathbb{R}_+,\cdot)$$

Define $f: \mathbb{R} \to \mathbb{R}_+$ as

$$f(x) = a^x; \text{ where } a > 0.$$

We will show f is one-one.

Consider,

$$\ker f = \{x \in R \mid f(x) = 1\}$$
$$= \{x \in \mathbb{R} \mid a^x = 1\}$$
$$= \{x \in \mathbb{R} \mid x = \log_a^1\}$$
$$= \{x \in \mathbb{R} \mid x = 0\}$$
$$= \{0\}$$

$\therefore$ f is 1 – 1.

We will show f is homomorphism.

Let $x, y \in R$

Consider

$$f(x + y) = a^{x+y}$$
$$= a^x.a^y = f(x).f(y)$$

$\therefore$ f is homomorphism. We will show f is onto, i.e., we have to find for any positive real number 'y' some real number x such that

$$f(x) = y$$

i.e., $a^x = y$

As $a^x = y$

On taking log both sides

$\Rightarrow$ $x = \log_a y$

$\therefore$ $f(x) = y$

Hence, f is onto.

$\therefore$ $(\mathbb{R},+) \cong (\mathbb{R}_+,\cdot)$

Let Q be the set of rational numbers and Q_+ be the set of positive rational number.

If f is homomorphism from Q to Q_+, then

$\phi: \mathbb{R} \to \mathbb{R}^+$

$\phi(x) = e^x, \forall x \in R$

$$f(x, y) = f(x)f(y) \ \forall \ x, y \in Q$$

And if image of 1 is known then the image of every element will be known.

$$\therefore \quad f(x) = a^x \text{ where } a = f(1)$$

If $a = 1$,

$$f(x) = 1$$

$\therefore$ f is trivial homomorphism.

If $a \neq 1$,

$$f(x) = 1$$

then

$$f(x) = a^x \in Q_+ \forall \ x \in Q$$

which is a contradiction.

Hence, only trivial homomorphism is possible.

$$\therefore \quad (Q, +) \not\cong (Q_+, .)$$

1.2 Determine the number of homomorphisms from the additive group Z_{15} to the additive group Z_{10}. (Z_n is the cyclic group of order n).

(2009 : 12 Marks)

Solution:

Let $\phi : \mathbb{Z}_{15} \to \mathbb{Z}_{10}$ be a homomorphism.

As $\mathbb{Z}_{15}$ is a cyclic group of order 15.

$$\mathbb{Z}_{15} = \langle 1 \rangle$$

Under homomorphism, if element 1 will be mapped then remaining elements will get mapped themselves ($\because$ G is cyclic)

Suppose, $\phi(1) = x$

As we know, if f is homomorphism from G to G' then $O(f(a))/0(a)$ where $a \in G$.

As $\phi(1) = x$.

$$\therefore \quad O(x)/O(a) = 15$$

And order of element divides order of group

$\therefore$ $O(x)/10$ As $O(x)/15$

$O(x)/15 \Rightarrow O(x) | g.c.d(15, 10) O(x) | 5$

$$\therefore \quad O(x) = 1 \text{ or } O(x) = 5$$

If $O(x) = 1$. Then it is trivial homomorphism. And if $O(x) = 5$.

Note : In $\mathbb{Z}_n$, number of elements of order $k = \phi(k)$; provided $k | n$.

$\therefore$ In $\mathbb{Z}_{10}$, number of elements of order $5 = \phi(5) = 4$.

$\therefore$ We have 4 possibilities for x.

Total number of homomorphism = 4 + 1 = 5.

1.3 Show that the alternating group on four letters A_4 has no subgroup of order 6.

(2009 : 15 Marks)

Solution:

Consider the alternating group A_4.

$$\sigma(A_4) = \frac{\dot{\sigma}(S_4)}{2} = \frac{|4}{2} = 12$$

We show although $6 | 12$, A_4 has no subgroup of order 6. Suppose H is a subgroup of A_4 and $\sigma(H) = 6$.

By previous problem the number of distinct 3-cycles in S_4 is

$$\frac{1}{3} \cdot \frac{4!}{(4-3)!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 1} = 8$$

Again, as each 3-cycle will be even permutation all these 3-cycles are in A_4. Obviously then, at least one 3-cycle, say s does not belong to $H(\sigma(H) = 6)$.

Now, $\sigma \in H \Rightarrow \sigma^2 \in H$, because if $\sigma^2 \in H$.

Then, $\sigma^4 \in H$

$\Rightarrow$ $\sigma \in H$

As $\sigma^3 = I as \sigma(\sigma) = 3$

Let $K = <\sigma> = \{I, \sigma, \sigma 2\}$ then, $\sigma K = 3(= \sigma(\sigma))$

and $H \cap K = \{1\}$ $(\sigma, \sigma^2 \notin H)$

$$\Rightarrow \quad \sigma(HK) = \frac{\sigma(H) \cdot \sigma(K)}{\sigma(H \cap K)} = \frac{6.3}{1} = 18,$$

not possible as $HK \subseteq A_4$ and $\sigma(A_4) = 12$.

1.4 Let $G = R - \{-1\}$ be the set of all real numbers omitting –1. Define the binary relation $*$ on G by $a*b = a + b + ab$. Show $(G, *)$ is a group and it is abelian.

(2010 : 12 Marks)

Solution:

Given : Binary relation $*$ as

$$a*b = a + b + ab, \text{ where } a, b \in G.$$

Closure : Let $a, b \in G$

$\therefore$ $a*b = a + b + ab$.

if $a + b + ab = -1$, then

$$a + b + ab + 1 = 0$$

$\Rightarrow$ $(1 + a) + b(1 + a) = 0$

$\Rightarrow$ $(1 + a) + (1 + b) = 0$

$\Rightarrow$ either $1 + a = 0 \Rightarrow a = -1$

or $1 + b = 0 \Rightarrow b = -1$

$\because$ both $a, b \in G$

$\therefore$ $a \neq -1$ and $b \neq -1$

$\therefore$ $a + b + ab \neq -1$ for any $a, b \in G$

$\therefore$ $a + b + ab \neq -1$ for any $a, b \in G$

$\therefore$ $a*b \in G$

So, closure is satisifed.

Associative : Let $a, b, c \in G$

$\therefore$ $(a*b)*c = (a + b + ab)*c$

$= a + b + ab + c + (a + b + ab)c$

$= a + b + ab + c + ac + bc + abc$

$= a + b + c + ab + ac + bc + abc$

Also, $a*(b*c) = a*(b + c + bc)$

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

$= a + b + c + ab + bc + ac + abc$

as $(a*b)*c = a*(b*c)$

$\therefore$ Associative property is satisfied.

Identity :

Let $a*b = a = a + b + ab$

$\Rightarrow \quad a + b + ab = a$

$\Rightarrow \quad b(1 + a) = 0$

as $\quad a \neq -1 \Rightarrow b = 0$

$\therefore$ $b = 0$ is an identity and as $O \in G$.

$\therefore$ identity exists.

Inverse :

Let $\quad a*b = 0 = a + b + ab$

$\Rightarrow \quad a(1 + b) = -b \Rightarrow a = \dfrac{-b}{1+b} \qquad (b \neq -1)$

Also, $\quad \dfrac{-b}{1+b} \in G$

$\therefore$ Inverse exists.

As closure, associative property, identity, inverse conditions are satisfied. $\therefore$ $(G, *)$ is a group.

Now, $\quad a*b = a + b + ab$

$b*a = b + a + ba = a + b + ab$

as $\quad a*b = b*a$

$\therefore$ $(G, *)$ is abelian.

1.5 Show that a cyclic group of order 6 is isomorphic to the product of a cyclic group of order 2 and a cyclic group of order 3. Can you generalize this? Justify.

(2010 : 12 Marks)

Solution:

Let $\quad z_6$ is cyclic group of order 6

z_2 is cyclic group of order 2

z_3 is cyclic group of order 3

Now, we know that

$$Z_m \times Z_n \cong Z_{mn}$$

when m and n are co-prime.

Here, $\quad m = 2, n = 3$

$\therefore \quad z_2 \times z_3 \cong z_6$

1.6 Let $(\mathbb{R}^*, \cdot)$ be the multiplicative group of non-zero reals and $((GL(n, \mathbb{R}), X)$ be the multiplicative group of $n \times n$ non-singular real matrices. Show that the quotient group $GL(n, \mathbb{R}) / SL(n, \mathbb{R})$ and $(\mathbb{R}^*, \cdot)$ are isomorphic where

$$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) / \det A = 1\}$$

What is the centre of $GL(n, \mathbb{R})$?

(2010 : 15 Marks)

Solution:

Given, $(GL(n,\mathbb{R}), X)$ is multiplicative group of real matrices.

Let f : $GL(n,\mathbb{R}) \rightarrow (\mathbb{R}^*, \cdot)$ be a no morphism where for any $A \in G$.

$$\phi(A) = |A|$$

$\therefore \quad \phi(A \times B) = |AB| = |A|\,|B|$

Now, let Ker(ϕ) contains matrices such it $B \in$ Ker (ϕ)
then $\phi(AB) = A$
$\therefore$ $|B| = 1$
$\therefore$ Ker(ϕ) contains matrices such that $|B| = 1$ if $B \in$ Ker (ϕ).
$\therefore$ By first fundamental theorem of homomorphism,

$$\frac{GL}{Ker(\phi)} \equiv (\mathbb{R}^*, \cdot)$$

Given, $SL(n,\mathbb{R}) = \{A \in GL(n,\mathbb{R}) / |A| = 1\}$

i.e., $SL(n,\mathbb{R})$ is Ker(ϕ).

$\therefore$ $$\frac{GL(n,\mathbb{R})}{SL(n,\mathbb{R})} \cong (\mathbb{R}^*, \cdot)$$

Now, let z be the centre of $GL(n,\mathbb{R})$.

for $x \in z$ where $X = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$

$\forall A \in GL(n,\mathbb{R})$, $AX = XA$

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $A \in GL(n,\mathbb{R})$

Now, $$AX = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$$

$$XA = \begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ap+qc & pb+qd \\ ar+cs & br+ds \end{bmatrix}$$

$\therefore$ for $XA = AX$

$$\begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix} = \begin{bmatrix} ap+qc & pb+qd \\ ar+cs & br+ds \end{bmatrix}$$

Holds true when $p = q = r = s$
or $p = s, q = r = 0$

$\therefore$ $$z = \left\{\begin{bmatrix} p & p \\ p & p \end{bmatrix}, \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix} \middle| p \in R\right\}$$

1.7 Show that the set

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

of six transformations on the set of Complex numbers defined by

$$f_1(z) = z,\ f_2(z) = 1 - z,\ f_3(z) = \frac{z}{(z-1)},$$

$$f_4(z) = \frac{1}{z},\ f_5(z) = \frac{1}{(1-z)} \text{ and } f_6(z) = \frac{(z-1)}{z}$$

is a non-abelian group of order 6 w.r.t. composition of mappings.

(2011 : 12 Marks)

Solution:

Let us construct the following table of the elements of G w.r.t. composition of mappings :

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	z	$1-z$	$\frac{z}{z-1}$	$\frac{1}{z}$	$\frac{1}{1-z}$	$\frac{z-1}{z}$
f_2	$1-z$	z	$\frac{1}{1-z}$	$\frac{z-1}{z}$	$\frac{z}{z-1}$	$\frac{1}{z}$
f_3	$\frac{z}{z-1}$	$\frac{z-1}{z}$	z	$\frac{1}{1-z}$	$\frac{1}{z}$	$1-z$
f_4	$\frac{1}{z}$	$\frac{1}{1-z}$	$\frac{z-1}{z}$	z	$1-z$	$\frac{z}{z-1}$
f_5	$\frac{1}{1-z}$	$\frac{1}{z}$	$1-z$	$\frac{z}{z-1}$	$\frac{z-1}{z}$	z
f_6	$\frac{z-1}{z}$	$\frac{z}{z-1}$	$\frac{1}{z}$	$1-z$	z	$\frac{1}{1-z}$

From the table it is clear that

$$(f_i \circ f_i)(z) = (f_i \circ f_i)(z) \ \forall\ z \in C, 1 \le i \le 6$$

$\therefore$ f_i is the identity of G.

Also, $f_1^{-1} = f_1;\ f_2^{-1} = f_2;\ f_3^{-1} = f_3,\ f_4^{-1} = f_4^1 = f_5^{-1} = f_6;\ f_6^{-1} = f_5$

$\Rightarrow$ G is a group.

But $(f_2 \circ f_3)(z) = \frac{1}{1-z}$

and $(f_3 \circ f_2)(z) = \frac{z-1}{z}$

$\therefore$ G is a non-abelian group.

1.8 (i) Prove that a group of Prime order is abelian.

(2011 : 6 Marks)

(ii) How many generators are there of the cyclic group (G, .) of order 8?

(2011 : 6 Marks)

Solution:

(i) Let $O(G) = P$, where P is a prime number.

Let $a \in h$ be any element.

Since order of an element divides the order of the group.

$\therefore$ $O(a) \mid O(G) = P$

$\Rightarrow$ $O(a) = 1$ or $O(a) = P$

If $a \neq e$, then $O(a) = P$

Let $H = (a)$

$\Rightarrow$ $O(H) = O(a) = P$ and $H \subseteq G$

$\therefore$ $H = G = (a)$

$\Rightarrow$ G is cyclic.

$\Rightarrow$ G is abelian **(as every cyclic group is abelian).**

(ii) Let G be a cyclic group of order 8.

$\therefore$ $\exists$ can element $a \in G$ such that $O(a) = 8$

We know that, $O(a^n) = \frac{O(a)}{(O(a), n)}$

$\therefore$ $O(a^n) = O(a) \Rightarrow (O(a), n) = 1$

Number of elements of G whose order is co-prime to

$$O(a) = \phi(O(a)) = \phi(8) = \phi(2^3) = 4 \quad (\because \phi(P^n) = P^n - P^{n-1})$$

$\therefore$ Number of generators of cyclic group of order 8 = 4.

1.9 Give an example of a group G in which every proper subgroup is cyclic but the group itself is not cyclic.

(2011 : 15 Marks)

Solution:

Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Define product on G by usual multiplication together with

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

Then G forms a group.

But G is not abelian as $ij \neq ji$.

$\Rightarrow$ G can not be cyclic as every cyclic group is abelian.

Let

$$H_1 = [1] = \langle 1 \rangle$$
$$H_2 = [\pm 1] = \langle -1 \rangle$$
$$H_3 = [\pm 1, \pm i] = \langle i \rangle = \langle -i \rangle$$
$$H_4 = [\pm 1, \pm j] = \langle j \rangle = \langle -j \rangle$$
$$H_5 = [\pm 1, \pm k] = \langle k \rangle = \langle -k \rangle$$

Thus, H_1 to H_5 are proper subgroups of G and all there are cyclic. Hence the result.

1.10 Let a and b be elements of a group, with $a^2 = e$, $b^6 = e$ and $ab = b^4a$. Find the order of ab, and express its inverse in each of the forms $a^m b^n$ and $b^m a^n$.

(2011 : 20 Marks)

Solution:

Given : $a^2 = e$, $b^6 = e$ and $ab = b^4a$

$\therefore$ $ab = b^4a$

$\Rightarrow$ $aba^{-1} = b^4aa^{-1} = b^4e = b^4$

Again, $b^8 = b^4 \cdot b^4 = (aba^{-1})(aba^{-1}) = ab^2a^{-1}$

$\Rightarrow$ $b^{16} = b^8 \cdot b^8 = (ab^2a^{-1})(ab^2a^{-1})$

$= ab^4a^{-1}$

$= a(aba^{-1})a^{-1}$ $(\because b^4 = aba^{-1})$

$= a^2ba^{-2}$

$= a^2b(a^2)^{-1}$

$= ebe = b$

$\Rightarrow$ $b^{16} = b \Rightarrow b^{15} = e$

$\Rightarrow$ $O(b) = 1, 3, 5 \text{ or } 15$ ...(i)

Also, given $b^6 = e$

$\Rightarrow$ $O(b) = 1, 2, 3 \text{ or } 6$ ...(ii)

$\therefore$ From (i) and (ii)

$O(b) = 3$

And $ab = b^4a = b^3ba = eba = ba$

$\therefore$ Number of conjugacy classes = 7.

An element of 1st class = (1)

An element of 2nd class = (1 2)

An element of 3rd class = (1 2 3)

An element of 4th class = (1 2 3 4)

An element of 5th class = (1 2 3 4 5)

An element of 6th class = (1 2)(3 4)

An element of 7th class = (1 2 3)(4 5)

1.13 Give an example of an infinite group in which every element has finite order.

(2013 : 10 Marks)

Solution:

Consider $\left\langle \frac{Q}{Z}, t \right\rangle$, i.e., the quotient group of rationals with respect to integers under addition.

Any element of $\frac{Q}{Z}$ is of form $\frac{p}{q}+z$ where $\frac{p}{q} \in Q$ is in lowest form.

$$q\left(\frac{p}{q}+z\right) = \underbrace{\frac{p}{q}+.....+\frac{p}{q}}_{q \text{ times}}+z = p+z$$

$$= z$$

$\therefore$ $$O\left(\frac{p}{q}+z\right) \le q$$

So, order of all elements are finite. But there are infinitely elements in $\frac{Q}{Z}$ as there are infinite rationals in [0, 1) and none of them are equal in $\frac{Q}{Z}$.

$$= f(a+ib)+f(c+id)$$

And $$f[(a+ib)(c+id)] = f[ac-bd+i(ad+bc)]$$

$$= \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$

$$= f(a+ib)\cdot f(c+id)$$

f is one-one

$$a+ib = c+id \Rightarrow a = c \text{ and } b = d \Rightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & a \end{bmatrix}$$

$\Rightarrow$ $$f(a+ib) = f(c+id)$$

f is onto

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in S \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = f(a+ib)$$

$\therefore$ f is a one-one onto linear map and so an isomorphism.

1.14 What are the orders of the following permutations in S_{10}.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 7 & 3 & 10 & 5 & 4 & 2 & 6 & 9 \end{pmatrix}$$ **and (1 2 3 4 5) (6 7)**

(2013 : 10 Marks)

Solution:

Approach : This and the next part uses the fact that order of any permutation written as disjoint cycles in LCM of the order of the cycle. And order of any cycle is its length.

Writing the permutation as product of disjoint cycles.

(2 8) (3 7 4) (5 10 9 6)

Order = L.C.M. (2, 3, 4) = 12

(1 2 3 4 5)(6 7)

Order = L.C.M. (5, 2) = 10

1.15 What is the maximal possible order of an element in S_{10}? Why? Give an example of that element? How many elements will be there in S_{10} of that order?

(2013 : 13 Marks)

Solution:

Any permutation in S_{10} can be written as product of disjoint cycles. Let $n_1, n_2, ..., n_r$ be size of these cycles. Then they are also the order of respective cycles.

$$n_1 + n_2 + ... + n_r = 10$$

and Order = L.C.M. $(n_1, n_2, ..., n_r)$

The order will be maximised if n_i's are relative primes.

The primes less than 10 are 2, 3, 5, 7.

Taking $n_1 = 3$, $n_2 = 7$, Order = 21; $n_1 = 2$, $n_2 = 3$, $n_3 = 3$, Order = 30.

∴ The highest order is 30 for cycles of length 2, 3 and 5.

An example : (1, 2)(3 4 5)(6 7 8 9 10)

Number of Such Elements :

${}^{10}C_2$ ways of picking 2 elements for 1st cycle and they can be written (2 – 1)! = 1 way.

${}^{8}C_3$ ways of picking 3 elements from rest 8 elements and can be written in (3 – 1)! = 2 ways.

Rest 5 elements can be written in (5 – 1)! = 24 ways.

$$\text{Total number of elements} = {}^{10}C_2 \times 1 + {}^{8}C_3 \times 2 + 1 \times 24$$

$$= \frac{10\times9}{2} + \frac{8\times7\times6}{3\times2} \times 2 + 24$$

$$= 45 + 56 + 24 = 135 \text{ elements.}$$

1.16 Let G be the set of all real 2×2 matrices $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$, where $xz \neq 0$. Show that G group under matrix multiplication. Let N denote the subset $\left\{\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in \mathbb{R}\right\}$. Is N a normal subgroup of G? Justify your answer.

(2014 : 10 Marks)

Solution:

Let $(G, *)$ be an algebraic structure. Where I∗I implies multiplication between its element in 'G' is the set of all 2×2 matrices of type $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$; $xz \neq 0, x, y, z \in R$

$$G = \left\{\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}; xz \neq 0; x, y, z \in R\right\}$$

(i) Closure Property:

$$\forall \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G$$

$$x, y, z, a, b \in 1R \quad \text{...(i)}$$

$$xz \neq a, ac \neq 0 \quad \text{...(ii)}$$

$$\Rightarrow \quad \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} * \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} ax & xb+yc \\ 0 & zc \end{bmatrix} = A$$

$ax \in 1R$

$$(ax).(cz) = (ac)(xz) \neq 0 \text{ from (ii)}$$

$xb + yc \in 1R$

$$zc \in 1R \text{ from (i)}$$

$$\therefore \quad A \in G \Rightarrow (G, *) \text{ is closed}$$

(ii) Associative Property :

$$\forall \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, \begin{bmatrix} p & a \\ 0 & r \end{bmatrix} \in G$$

$$x, y, z, a, b, c, p, r \in 1R$$

$$xz \neq 0, ac \neq 0, Pr \neq 0$$

$$\Rightarrow \quad \left(\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} * \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) * \begin{bmatrix} p & a \\ 0 & r \end{bmatrix} = \begin{bmatrix} ax & bx+yc \\ 0 & zc \end{bmatrix} * \begin{bmatrix} p & a \\ 0 & r \end{bmatrix}$$

$$= \begin{bmatrix} apx & aqx+bxr+ycr \\ 0 & zcr \end{bmatrix} \quad \text{...(iii)}$$

$$\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} * \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} * \begin{bmatrix} p & q \\ 0 & r \end{bmatrix}\right) = \begin{bmatrix} apx & aqx+bxr+ycr \\ 0 & zcr \end{bmatrix} \quad \text{...(iv)}$$

Here, (iii) = (iv)

i.e. $$\left(\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} * \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) * \begin{bmatrix} p & q \\ 0 & r \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} * \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} * \begin{bmatrix} p & a \\ 0 & r \end{bmatrix}\right)$$

$\therefore$ (G, x) satisfy associative property.

(iii) Existence of Left Identity :

Let $$\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in G, \text{ where } xz \neq 0, x, y, z \in 1R \quad \text{...(v)}$$

Let $$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G, \text{ where } ac \neq 0, a, b, c \in 1R \quad \text{...(vi)}$$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} * \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$$

$$\begin{bmatrix} ax & ay+bz \\ 0 & cz \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$$

equating its element, $cz = z \Rightarrow z(c-1) = 0$

From (vi), $ac \neq 0 \Rightarrow a \neq 0.\ c \neq 0$

From (v) $xz \neq 0 \Rightarrow x \neq 0, z \neq 0$

$\therefore$ $c - 1 = 0 \Rightarrow c = 1$

$ax = x \Rightarrow x(1-a) = 0$

From (v) $x \neq 0$ $\quad 1 - a = 0$ $\quad a = 1$

$ay + bz = y$ $\quad y + bz = y$

$\Rightarrow$ $\quad bz = 0$ From (v) $\quad z \neq 0$

$\therefore$ $\quad b = 0$ $\quad \therefore \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow$ left identity.

(iv) Existence of left inverse:

Let $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, \begin{bmatrix} p & q \\ 0 & r \end{bmatrix} \in G$

Where, $xz \neq 0, pr \neq 0$

$x, y, z, p, q, r \in 1R$

$\neq 0$

$$\begin{bmatrix} p & q \\ 0 & r \end{bmatrix} * \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} px & py + qz \\ 0 & rz \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

equating the elements,

$$px = 1 \qquad p = \frac{1}{x}$$

$$rz = 1 \qquad r = \frac{1}{z}$$

$$py + az = 0 \qquad \frac{y}{x} + az = 0$$

$$q = -\left(\frac{y}{xz}\right)$$

$\therefore$ $\begin{bmatrix} p & q \\ 0 & r \end{bmatrix} = \begin{bmatrix} \frac{1}{x} & \frac{-y}{xz} \\ 0 & \frac{1}{2} \end{bmatrix}$ left inverse of $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$ ...(vii)

$\therefore$ $(G, *)$ is a group,

$$N = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}; a \in 1R \right\} \subset G$$

$$e = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in N;\ N \neq \phi$$

Let, $\quad A = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \in N;\ x \in 1R$

$$A^{-1} = \begin{bmatrix} \frac{1}{1} & -\frac{x}{1} \\ 0 & \frac{1}{1} \end{bmatrix} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}$$ From (vii)

(i) $A^{-1} \in N$

(ii) Let, $\quad B = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} \in N;\ y \in 1R$

$$A * B = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y + x \\ 0 & 1 \end{bmatrix} \in N$$

$\therefore$ $N < G$ ('N' is subgroup of G).

For 'N' to be a normal subgroup.

$$\forall X \in G \Rightarrow X * n * X^{-1} \in N$$
$$n \in N$$

Let, $$x = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, x^{-1} = \begin{bmatrix} \frac{1}{x} & \frac{-y}{xz} \\ 0 & \frac{1}{z} \end{bmatrix}$$

$$XnX^{-1} = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{x} & \frac{-y}{xz} \\ 0 & \frac{1}{z} \end{bmatrix}$$

$$= \begin{bmatrix} x & xx+y \\ 0 & z \end{bmatrix} * \begin{bmatrix} \frac{1}{x} & \frac{-y}{xz} \\ 0 & \frac{1}{z} \end{bmatrix} = \begin{bmatrix} 1 & \frac{-xy}{xz} + \frac{xx}{z} + \frac{y}{z} \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \frac{xx}{z} \\ 0 & 1 \end{bmatrix} \in N$$

$\therefore$ $N \trianglelefteq G$. (Normal subgroup of G).

1.17 (i) How many generators are there of cyclic group G of order 8. Explain.

(2015 : 5 Marks)

(ii) Taking a group $\{e, a, b, c\}$ of order 4, where e is the identity, construct composition tables showing that one is cyclic while other is not.

(2015 : 5 Marks)

Solution:

(i) Let a be a generator of group G with order 8. $\therefore$ a^i is generator of G if i and 8 are co-prime numbers, co-prime to 8 are 1, 3, 5, 7.

$\therefore$ Number of generators of G are 4.

(ii) **Cyclic Group :** Let a be the generator, such that $a^1 = a$, $a^2 = b$, $a^3 = c$ and $a^4 = e$.

$\therefore$ Table is

x	e	a	b	c
e	e	a	b	c
a	a	a^2	$ab = a^3$	$ac = a^4 = e$
b	b	$ba = a^3$	$b^2 = e$	$bc = a^5 = a$
c	c	$ca = e$	$cb = a$	$c^2 = a^2$

So, table is

x	e	a	$b = a^2$	$c = a^2$
e	e	a	a^2	a^3
a	a	a^2	a^3	e
$b = a^2$	a^2	a^3	e	a
$c = a^3$	a^3	e	a	a^2

The above table is a group as e occurs in every row and column. Further, transpose of elements does not change the table.

Non-Cyclic : Let $a = \{e, a, b, c\}$ such that $a^2 = b^2 = c^2 = e$.

$\therefore$ table is

x	e	a	b	c
e	e	a	b	c
a	a	e	ab	ac
b	b	ab	e	bc
c	c	ac	bc	e

Above table is a group as e is present in each row and column.

1.18 Let p be a prime number and z_p denote the additive group of integers modulo p. Show that every non-zero element of z_p generates z_p.

(2016 : 15 Marks)

Solution:

Let z_p the additive group, where p is a prime number.

$\therefore$ $z_p = \{0, 1, 2, 3, ... p-1\}$

Let $a \neq 0 \in z_p$ and a be the group formed by a.

$a = <a> = \{a, 2a, 3a, ...\}$

Now, a will form a subgroup of z_p.

By Lagrange's theorem

$o(a) \mid o(z_p)$

Here, $o(z_p) = p$ = prime number

$\therefore$ $o(a) = 1$ or $o(a) = p$

as $a \neq 0$, $o(a) \neq 1$

$\therefore$ $o(a) = p$

$\Rightarrow$ $a = z_p$

$\therefore$ a generates z_p.

So, every non-zero element of z_p generates z_p.

1.19 Let G be a group of order n. Show that G is isomorphic to a subgroup of the permutation group S_n.

(2017 : 10 Marks)

Solution:

S_n = Group of all permutations of set G. For any $a \in G$, define a mapping.

$f_a : G \to G$ s.t. $f_a(x) = ax$, then

f_a is well defined as $x = y \Rightarrow f_a(x) = f_a(y)$.

f_a is one-one as $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$

Also, for any $y \in G$, since $f_a(a^{-1}y) = a(a^{-1}y) = y$, we find $a^{-1}y$ is pre-image of $y \Rightarrow f_a$ is onto.

Hence, f_a is permutation on G. $\therefore f_a \in S_n$.

Let K be the set of all such permutations.

To show, $K \subseteq S_n$: $K \neq \phi$ as $f_e \in K$.

Let $f_a, f_b \in K$ be any members, then

$$f_b \circ f_{b^{-1}}(x) = f_b(f_{b^{-1}}(x)) = f_b(b^{-1}x) = b(b^{-1}x) = ex = f_e(x)$$

$\therefore$ $f_{b^{-1}} = (f_b)^{-1}$ ($f_e = I$ is identify of S_n)

Also, $(f_a \circ f_b)x = f_a(bx) = a(bx) = f_{ab}(x)$ $\forall$ x

i.e., $f_{ab} = f_a \circ f_b$

$f_a \circ (f_b)^{-1} = f_a \circ f_{b^{-1}} = f_{ab^{-1}} \in K$ shows $K \subseteq S_n$

Now, define $\phi : G \to K$ s.t. $\phi(a) = f_a$

then ϕ is well defined, 1–1 map as

$a = b \Leftrightarrow ax = bx \Leftrightarrow f_a(x) = f_b(x) \ \forall \ x$

$\Leftrightarrow f_a = f_b \Leftrightarrow f(a) = f(b)$

ϕ is obviously onto and as $\phi(ab) = f_{ab} = \phi(a)\phi(b)$.

ϕ is isomorphism.

1.20 Show that the graphs $\mathbb{Z}_5 \times \mathbb{Z}_7$ and $\mathbb{Z}_{35}$ are isomorphic.

(2017 : 15 Marks)

Solution:

We prove that $\mathbb{Z}_5 \times \mathbb{Z}_7 = \{(x, y) \cdot x \in \mathbb{Z}_5, y \in \mathbb{Z}_7\}$ is a cyclic group of order 35. To differentiate between the identity element perpendicular of $\mathbb{Z}_5$ and $\mathbb{Z}_7$, we denote them by e_5 and e_7 respectively.

Then, $|e_5| = 5$ and $|e_7| = 7$

Clearly, $(e_5, e_7) = (1,1) \in \mathbb{Z}_5 \times \mathbb{Z}_7$

We claim that $|(e_5, e_7)| = 35$

Clearly, $35(e_5, e_7) = (0, 0)$

Now, let $t(e_5, e_7) = (0, 0)$

$\Rightarrow (te_5, te_7) = (0, 0)$

$\Rightarrow te_5 = 0$ and $te_7 = 0$

$\Rightarrow 5/t$ and $7/t$

$\Rightarrow 35/t \ \because \ gcd(5, 7) = 1$

Thus, 35 is the least positive integer such that $35(e_5, e_7) = (0, 0)$.

$\therefore |(e_5, e_7)| = 35$ so $\mathbb{Z}_5 \times \mathbb{Z}_7 = \langle (e_5, e_7) \rangle$

Now, every cyclic finite group of order 35 is isomorphic to $\mathbb{Z}_{35} \cdot 12$.

1.21 Show that the quotient group of (R_1+) modulus z is isomorphic to the multiplicative group of complex numbers on unit circle in the complex plane. Here, R is set of real numbers and z is the set of integers.

(2018 : 15 Marks)

Solution:

Let $\frac{R}{z} = \{z + a \mid a \in R\}$ be the quotient group in addition modulo z.

Define a group $A = \left\{e^{i2\pi a} = x + iy \middle| \sqrt{x^2 y^2} = 1\right\}$

$\therefore A$ is a group of complex numbers on unit circle.

Now, define a mapping f such that

$f : R \to A$

and $f(a) = e^{i2\pi a}$, where $a \in R$

f is well defined :

Let $a = b$

$\therefore i2\pi a = i2\pi b$

$\Rightarrow e^{i2\pi a} = e^{i2\pi b}$

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

$\therefore$ f is well defined.

f is onto :

For every element $e^{i2\pi a}$, $\exists\, a \in R$ such as

$f(a) = e^{i2\pi a}$ .... f is onto.

f is homo-morphism :

$$f(a+b) = e^{i2\pi(a+b)} = e^{i2\pi a}.e^{i2\pi b} = f(a)\cdot f(b)$$

$\therefore$ f is homomorphism.

So, by first fundamental theorem of homo-morphism, $\frac{R}{K} \cong A$

where, $K = \text{Kerf}\{a \in R \mid f(a) = 1\}$

$K = \{a \mid e^{i2\pi a} = 1\} = z$

$\therefore$ $\frac{R}{Z} \cong A$

1.22 Find all the proper subgroups of multiplication group of the field (Z_{13}, T_{13}, X_{13}), where T_{13} and X_{13} represent addition modulo 13 and multiplication modulo 13 respectively.

(2018 : 20 Marks)

Solution:

Given: $\{Z_{13}, X_{13}\} = \{1, 2, 3, ..., 12\}$

$\therefore$ 13 is a prime number. $\therefore$ Z_{13} is a cyclic group.

Now, $2^1 = 2, 2^2 = 4, 2^3 = 8$

$2^4 = 16 = 3, 2^5 = 32 = 6, 2^6 = 64 = 12$

$2^7 = 128 = 11, 2^8 = 9, 2^9 = 5$

$2^{10} = 10, 2^{11} = 7, 2^{12} = 1$

i.e., 2 is a generator of (Z_{13}, X_{13}).

By Lagrange's theorem, order of a subgroup divides order of group.

Divisors of 12 are 1, 2, 3,4, 6, 12.

$\therefore$ by fundamental theorem of cyclic group the subgroups are $<2^1> = <2>$, $<2^2> = <4>$, $<2^3> = ...$, $<2^4> = <3>$, $<2^6> = <12>$, $<2^{12}> = <1>$.

So, proper subgroups are <2>, <4>, <3>, <8>, <12>.

1.23 Let G be a finite group, H and K subgroups of G such that $K \subset H$. Show that $(G : K) = (G : H)(H : K)$.

(2019 : 10 Marks)

Solution:

Since, $K \subset H \subseteq G$ and H, K are subgroups of G, therefore K is a subgroup of H.

By Lagrange's theorem

$$(G : K) = \frac{O(G)}{O(K)}$$

Similarly, $$(G : H) = \frac{O(G)}{O(H)}$$

$$(H : K) = \frac{O(H)}{O(K)}$$

Hence, $$(G : H)(H : K) = \frac{O(G)}{O(H)} \times \frac{O(H)}{O(K)}$$

$$= \frac{O(G)}{O(K)}$$
$$= (G : K)$$

Hence, the result.

1.24 If G and H are finite groups whose orders are relatively prime, then prove that there is only one homomorphism from G to H, the trivial one.

(2019 : 10 Marks)

Solution:

Let G and H be finite groups such that orders of G and H are relatively prime to each other. Consider $\phi - G \to H$ to be a homomorphism.

To show that ϕ must be trivial.

As $f(G)$ is a subgroup of H.

$\Rightarrow$ Order of $f(G)$ divides order of H.

Also, $\phi(G)$ is a quotient of G.

$\Rightarrow$ Order of $\phi(G)$ divides order of G.

$\because$ Orders of G and H are coprimes.

$\Rightarrow \phi(G)$ is trivial. Hence the result.

1.25 Write down all quotient groups of the group Z_{12}.

(2019 : 10 Marks)

Solution:

Let $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ be a group.

Clearly, Z_{12} is a cylic group and generated by '1', i.e., $Z = (i)$ so that $0(1) = 12 = 0(Z_{12})$

$\therefore$ The subgroups of Z_{12} are precisely the subgroup generated by $m(1)$, where m divides 12.

Since, $\frac{12}{m} \Rightarrow m = 1, 2, 3, 4, 5$ and 12.

$\therefore$ <1>, <2(1)>, <3(1)>, <4(1)>, <6(1)> and <12(1)> are cyclic subgroups of Z_{12}.

i.e., <1>, <2>, <3>, <4>, <6> and <2>.

Since, Z_{12} is cyclic. $\therefore$ Its every subgroup is normal.

Thus, the normal subgroups of Z_{12} are given by $<1> = Z_{12}$, $<2> = \{2s \mid s \in I\}$

$= \{2, 4, 6, 8, 10, 0, ...\}$

$<3> = \{0, 2, 6, 9\}$, $<4> = \{0, 4, 8\}$

$<6> = \{0, 6\}$ and $<12> = \{0\} = <0>$

Finally, the quotient groups of Z_{12} are given by

$$Z_{12} = \left\{\frac{<1> + n}{NZ_{12}}\right\}$$

$$<1> = \{<1>\}$$

$$Z_{12} = \left\{\frac{<2> + \lambda}{NZ_{12}}\right\}$$

$$<2> = \{<2>, <2> + 1\}$$

$$\frac{Z_{12}}{<3>} = \{<3>, <3> + 1, <3> + 2\}$$

$$\frac{Z_{12}}{<4>} = \{<4>, <4> + 1, <4> + 2, <4> + 3\}$$

$$\frac{Z_{12}}{<6>} = \{<6>, <6>+1, <6>+2, <6>+3, <6>+4, <6>+5\}$$

and

$$\frac{Z_{12}}{<12>} = \{<12>, <12>+1, <12>+2, <12>+3, <12>+4, <12>+5, <12>+6, <12>+7 \text{ and } <12>+8, <12>+9, <12>+10, <12>+11\}$$

Hence, the result.

2. Rings

2.1 How many proper, non-zero ideals does the ring $\mathbb{Z}_{12}$ have? Justify your answer. How many ideals does the ring $\mathbb{Z}_{12} \odot \mathbb{Z}_{12}$ have? Why?

(2009 : 2+3+4+6=15 Marks)

Solution:

Let $(\mathbb{Z}_m, \oplus_m)$ be a cyclic group of order m.

Let I be a subgroup of $\mathbb{Z}_m$.

$\therefore$ $I = (\alpha) = n\alpha$, f.s. $n \in \mathbb{Z}$

We will show I is an ideal of $\mathbb{Z}_m$.

Let $x, y \in I$.

$\therefore$ $x = n_1\alpha$ and $y = n_2\alpha$

So, $x - y = n_1\alpha - n_2 = (n_1 - n_2)\alpha \in I$ ...(i)

and let $x \in I$; $r \in \mathbb{Z}_m$.

Consider $rx = rn_1\alpha(rn_1)\alpha \in I$ ...(ii)

From (i) and (ii)

I is an ideal of $\mathbb{Z}_m$.

And number of subgroup of $\mathbb{Z}_m = \tau(m)$

$\therefore$ Number of ideal of $\mathbb{Z}_m = \tau(m)$

$\therefore$ Number of ideal of $\mathbb{Z}_{12} = \tau(12)$

$= \tau(3.4) = 4$

$\therefore$ Number of proper non-zero ideal of $\mathbb{Z}_{12}$

$= 4 - 2 = 2$

Using the results, "If I is an ideal of ring R and J is an ideal of ring S then $I \times J$ is a ideal of $R \times S$."

$\therefore$ Number of ideals of

$$\mathbb{Z}_{12} \times \mathbb{Z}_{12} = \tau(12) \times \tau(12)$$
$$= 4 \times 4 = 16$$

2.2 Show that $\mathbb{Z}[X]$ is a unique factorization domain that is not a principal ideal domain ($\mathbb{Z}$ is the ring of integers). Is it possible to give an example of principal ideal domain that is not a unique factorization domain? $\mathbb{Z}[X]$ is the ring of polynomials in the variable X with integers).

(2009 : 15 Marks)

Solution:

We have to show $\mathbb{Z}[x]$ is U.F.D.

As we know, if R is U.F.D., then $R(x)$ is U.F.D. (*)

We know, every P.I.D. is U.F.D.

$\because \mathbb{Z}$ is P.I.D.

$\Rightarrow \mathbb{Z}$ is U.F.D.

$\Rightarrow \mathbb{Z}[x]$ is U.F.D. (from (*))

In P.I.D.; $\alpha \neq 0$ and non-unit is irreducible.

$\Leftrightarrow$ $<a>$ is maximal.

In $\mathbb{Z}[x]$, x is irreducible.

$$x = b.c$$

Here we have two possibilities, b is constant and c is of degree 1, or c is constant and b is constant and b is of degree 1.

Case I : b is constant, c is of degree 1.

$$x = b(\alpha x + \beta)$$
$$= b\alpha x + \beta b$$

On comparing co-efficients,

$$b\alpha = 1 \text{ and } \beta\alpha = 0$$
$$\Rightarrow \quad b\alpha = 1 \text{ and } \beta = 0 \qquad (\because b \text{ is constant})$$

$\Rightarrow b$ is unit.

Similarly in **Case II :** c is unit.

$\therefore x$ is irreducible.

As $\langle x \rangle \subseteq \langle x, 2 \rangle \subseteq [x]$. But $\langle x \rangle$ is not maximal.

From (*), $\langle x \rangle$ is not.maximal but x is not irreducible.

$\therefore \mathbb{Z}[x]$ is not P.I.D.

Further, no it is not possible to give an example of P.I.D. that is not U.F.D. because every P.I.D. is U.F.D.

2.3 How many elements does the quotient ring $\frac{\mathbb{Z}_5[X]}{(X^2+1)}$ have? Is it an integral domain? Justify your answer.

(2009 : 15 Marks)

Solution:

Let $$R = \frac{\mathbb{Z}_5[x]}{\langle x^2+1 \rangle}$$

$$R = \frac{\mathbb{Z}_5[x]}{\langle x^2+1 \rangle} = \left\{ f(x) + \langle x^2+1 \rangle : f(x) \in \mathbb{Z}_5(x) \right\}$$

By division algorithm on $f(x)$ and $x^2 + 1$

$\Rightarrow q(x)$ and $r(x)$

$$f(x) = q(x)(x^2+1) + r(x); \text{ where } r(x) = 0$$
$$\deg r(x) < \deg(x^2+1)$$
$$f(x) + \langle x^2+1 \rangle = q(x)\langle x^2+1 \rangle + r(x) + \langle x^2+1 \rangle$$
$$= q(x)\langle x^2+1 \rangle + \langle x^2+1 \rangle + r(x) + \langle x^2+1 \rangle$$
$$= \langle x^2+1 \rangle + r(x) + \langle x^2+1 \rangle$$
$$= r(x) + \langle x^2+1 \rangle$$

$\therefore$ $$R = \left\{ r(x) + \langle x^2+1 \rangle : r(x) \in \mathbb{Z}_5[x] \deg r(x) = 1 \right\}$$

$$= \{a + bx + \langle x^2 + 1\rangle : a, b \in \mathbb{Z}_5$$

Thus, we have five choices for 'a' as well as five choices for 'b'.

$\therefore$ $|R| = 5 \times 5 = 25$

As $x^2 + 1$ is reducible over $\mathbb{Z}_5$, because

$$x^2 + 1 = (x + 2)(x + 3)$$

$\therefore$ By Chinese Remainder theorem;

$$\frac{\mathbb{Z}_5[x]}{\langle x^2+1\rangle} = \frac{\mathbb{Z}_5[x]}{\langle x+2\rangle\langle x+3\rangle} \cong \frac{\mathbb{Z}_5[x]}{\langle x+2\rangle} \times \frac{\mathbb{Z}_5[x]}{\langle x+3\rangle} \quad (\because g.c.d.(x+2), (x+3) = 1)$$

$\therefore$ $\mathbb{Z}_5$ is field and $x + 2$ is irreducible polynomial over $\mathbb{Z}_5$.

$\therefore$ $\dfrac{\mathbb{Z}_5[x]}{\langle x+2\rangle}$ is field.

And $$\frac{\mathbb{Z}_5[x]}{\langle x+2\rangle} = \{a_0 + \langle x+2\rangle : a_0 \in \mathbb{Z}_5\}$$

$\therefore$ $$\left|\frac{\mathbb{Z}_5[x]}{\langle x+2\rangle}\right| = 5$$

$\therefore$ $$\frac{\mathbb{Z}_5[x]}{\langle x+2\rangle} \cong \mathbb{Z}_5$$

Similarly, $$\frac{\mathbb{Z}_5[x]}{\langle x+3\rangle} \cong \mathbb{Z}_5$$

$\therefore$ $$\frac{\mathbb{Z}_5[x]}{\langle x+1\rangle} \cong \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$a = (1,0) \in \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$b = (0,1) \in \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$a, b = (1, 0).(0, 1) = (0, 0)$$

$\therefore$ $\mathbb{Z}_5 \times \mathbb{Z}_5$ is not an I.D.

2.4 Let $C = \{f : I = [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$. Show C is a commutative ring with 1 under pointwise addition and multiplication. Determine whether C is an integral domain. Explain.

(2010 : 15 Marks)

Solution:

Given $C = \{f : I = [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$

Let $f, g, h \in C$

A. Addition :

I. Closure : $(f + g)a = f(a) + g(a) \in R \ \forall \ a \in I$ as f & g are continuous functions.

$\therefore$ Closure is satisfied.

II. Associative :

$$((f + g) + h)a = f(a) + g(a) + h(a)$$
$$= (f + (g + h))a \text{ as } f, g, h \text{ are continuous.}$$

$\therefore$ Associative property is satisifed.

III. Identity :

$$(f + g)a = f(a) + g(a)$$

Let g is such that $g(a) = 0 \ \forall \ a \in R$

Such g can exist MC, so inverse exist.

IV. **Commutative :**

$$(f + g)a = f(a) + g(a) = g(a) + f(a) = (g + f)a$$

$\therefore$ C is abelian.

So, C is abelian group.

B. **Multiplication :**

I. **Closure :** $f(g(a)) \in R \Rightarrow$ Closure is satisfied.

II. **Associative :** $f(g(h))$ follows associative law due to continuity.

C. **Distributive :** $(f(g + h))a = f(g(a)) + f(h(a)$ as f, g, h are continuous.

$\therefore$ Distributive law is satisfied.

D. **Commutative :** $f(g(a)) = g(f(a))$ as f, g are continuous.

So, commutative property is satisfied.

Now, let $g(a) = 1$ be a function $\forall a \in I$

$\therefore$ $g(a) \in C$

So, C is a commutative ring with unity.

Now, let $f, g \in C$.

Let $f.g = 0$, i.e., $f(g(a)) = 0$ for some $a \in I$. Possibly only if f has 0 in its range. $\therefore$ **C is an integral domain (no zero divisors).**

2.5 Show that the quotient ring $\frac{z(i)}{(1+3i)}$ is isomorphic to the ring $\frac{z}{10z}$ where $z[i]$ denotes the ring of Gaussian integers.

(2010 : 15 Marks)

Solution:

Let $f: z[i] \to \frac{z}{10z}$ be an isomorphism such that

$$f(a + bi) = 10z + |a + bi| \text{ for } (a + bi) \in z[i]$$

f: well defined

Let $a + bi, c + di \in z[i]$

where $a + bi = c + di$

$\therefore$ $|a + bi| = |c + di|$

$\Rightarrow$ $10z + |a + bi| = 10z + |c + di|$

$\therefore$ f is well defined.

f is onto as

$10z + |a + bi| \in \frac{z}{10z} \ \forall a + bi \in z[i]$

$\therefore$ f is a homomorphism.

Now, $\ker(f) = \{a + bi \in z[i] \mid f(a + bi) = 10z\}$

$\therefore$ $10z + |a + bi| \in 10z$

i.e., $|a + bi| = 0$

$\Rightarrow$ $a^2 + b^2 = 10$, only possible if $a = 1, b = 3$ or $a = 3, b = 1$.

$\therefore$ $1 + 3i \in \ker(f)$

So, **by first fundamental theorem of homomorphism,**

$$\frac{z[i]}{1+3i} \cong \frac{z}{10z}$$

2.6 Let F be the set of all real valued continuous functions defined on the closed interval $[0, 1]$. Prove that $(F, +, .)$ is a Commutative Ring with unity with respect to addition and multiplication of functions defined pointwise as below :

$$\left.\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ \text{and}\quad (f\cdot g)(x) &= f(x)\cdot g(x)\end{aligned}\right\} x \in [0,1]$$

where $f, g \in F$.

(2011 : 15 Marks)

Solution:

First, we will prove that (F, t) is an abelian group.

Let $f, g \in F$.

$\Rightarrow f$ and g are real valued continuous function on $[0, 1]$ and sum of two real valued continuous functions is also a real valued continuous function.

$\therefore \quad f + g \in F$

Let $f, g, h \in F$

Then,
$$\begin{aligned}[(f+g)+h](x) &= (f+g)(x)+h(x)\\ &= (f(x)+g(x))+h(x)\\ &= f(x)+(g(x)+h(x))\end{aligned}$$

[$\because f(x), g(x), h(x)$ are real numbers and real numbers are associative]

$$\begin{aligned}&= f(x)+(g+h)(x)\\ &= [f+(g+h)](x)\end{aligned}$$

$\Rightarrow \quad (f+g)+h = f+(g+h)$

$\therefore$ Associative property holds.

Let $f \in F$.

$\therefore f$ is continuous on $[0, 1]$

Define $O : [0, 1] \to R$ such that

$$O(x) = 0;\ \forall\ x \in [0, 1]$$

Then
$$f(x) + O(x) = f(x) = O(x) + f(x)\ \forall\ f \in F$$

Hence, zero mapping is the identity map for (F, f).

Again, let $f \in F$.

$\Rightarrow f$ is continuous on $[0, 1]$

$\Rightarrow -f$ is continuous on $[0, 1]$

Further,
$$f(x) + (-f(x)) = O(x) = (-f(x) + f(x)\ \forall\ f \in F$$

$\therefore -f$ is the inversre function on f.

Let $f, g \in F$.

Then,
$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ &= g(x)+f(x)\end{aligned}$$

($\because f(x)$ and $g(x)$ are real numbers and real numbers are commutative)

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

$\Rightarrow$
$$f + g = g + f\ \forall\ f, g \in F$$

Commutative property holds.

If f and g are two real valued continuous functions on $[0, 1]$, then

$(fg)(x) = f(x)g(x)$ is also a real valued continuous function on $[0, 1]$

$\Rightarrow fg \in (F_{g+g})$

$\Rightarrow$ Closure property under multiplication holds.

Since, for $f, g, h \in (F_{g+g})$,

$$[(f\cdot g)\cdot h](x) = (fg)(x)h(x)$$
$$= (f(x)g(x))h(x)$$
$$= f(x)(g(x)h(x)) \quad [\because f(x), g(x), h(x) \text{ are real numbers}]$$
$$= f(x)(gh)(x)$$
$$= [f(gh)](x)$$
$$\Rightarrow (fg)h = f(gh)$$

$\therefore$ Associativity under multiplication holds.

Again
$$[f\cdot(g+h)](x) = f(x)\cdot[(g+h)(x)]$$
$$= f(x)\cdot[g(x)+h(x)]$$
$$= f(x)\cdot g(x) + f(x)\cdot h(x)$$
$$= (fg)(x) + (fh)(x)$$
$$= (fg+fh)(x)$$
$$\Rightarrow f\cdot(g+h) = fg + fh$$

Similarly,
$$(g+h)\cdot f = g\cdot f + h\cdot f$$

$\forall\ f, g, h \in (F_{g+g})$

$\therefore (F_{g+g})$ is

(i) an abelian group under addition.

(ii) a semi-group under multiplication.

(iii) holds distributive property.

$\therefore (F_{g+g})$ is a ring.

Also,
$$(fg)(x) = f(x)g(x)$$
$$= g(x)f(x) \quad (\because f(x), g(x) \text{ are real numbers})$$
$$= (gf)(x)$$
$$\Rightarrow fg = gf\ \forall\ f, g \in F$$

$\Rightarrow F$ is a commutative ring.

Define $I : [0, 1] \to R$ such that
$$I(x) = 1\ \forall\ x \in [0, 1]$$

Then
$$(fI)(x) = f(x)I(x)$$
$$= f(x)\cdot I = f(x)$$

and
$$(If)(x) = I(x)F(x)$$
$$= f(x)$$
$$\Rightarrow If = f = fI$$

$\Rightarrow I$ is the unity of (F_{g+g}).

2.7 Is the ideal generated by 2 and X in the polynomial ring $Z[X]$ of polynomials in a single variable X with coefficients in the ring of integers Z, a principal ideal? Justify your answer.

(2012 : 15 Marks)

Solution:

Principal Ideal : An ideal I of a ring R is called principal ideal if there is an element a of R such that
$$I = aR = \{ar : r \in R\}$$
i.e., I is generated by the element a.

Let
$$I = \{Xf(X) + 2g(X) \mid f(X), g(X) \in Z[X]\}$$
$$(Xf_1(X) + 2g_1(X)) - (Xf_2(X) + 2g_2(X)) = X(f_1(X) - f_2(X)) + 2(g_1(X) - g_2(X)) \in A \quad \ldots(i)$$
$(\because f_1(X) - f_2(X) \in Z[X],\ g_1(X) - g_2(X) \in Z[X])$

Again for $h(X) \in Z[X]$
$$[Xf(X) + 2g(X)]h(X) = Xf(X)h(X) + 2g(X)h(X) \in A \quad \ldots(ii)$$

$\therefore$ from (i) and (ii), A is an ideal of $Z(X)$.

We claim, $A \neq Z(X)$

Because if $A = Z(X)$, then $1 \in Z(X)$,

$\Rightarrow 1 \in A \Rightarrow$ $1 = Xf(X) + 2g(X)$

$\Rightarrow$ $1 = X(G_0 + G_1X + ... + G_pX^p) + 2(b_0 + b_1X + ... + b_qX^q)$

$\Rightarrow 1 = 2b_0 \Rightarrow$ $b_0 = \frac{1}{2}$, which is a contradiction, as $b_0 \in Z$, the set of integers.

$\therefore$ $A \neq Z(X)$

2.8 Let $J = \{a + bi \mid a, b \in z\}$ be the ring of Gaussian integers (subtring of C). Which of the following is J : Euclidean domain, Principal ideal domain, Unique factorization domain? Justify your answer. (2013 : 15 Marks)

Solution:

J is a Euclidean domain.

Proof : First we show that J is an ideal domain.

$$(a + bi)(c + di) = 0$$

$\Rightarrow$ $$(ac - bd) + i(ad + bc) = 0$$

$\Rightarrow$ $$ac - bd = 0$$

$$ad + bc = 0 \quad ...(i)$$

Let $$c + id \neq 0 \Rightarrow c \neq 0 \ \& \ d \neq 0 \quad ...(ii)$$

Multiplying (i) by c and (ii) by d and adding

$$a(c^2 + d^2) = 0 \Rightarrow a = 0$$

This gives $b = 0$ as well.

$\therefore$ $$a + ib = 0$$

So J has no zero divisors.

For $a + ib \in J$ define

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

Then $a, b \in z \Rightarrow a^2 + b^2 \in z \Rightarrow d(a + ib) \in z$

$$d[(a + ib)(c + id)] = d[(ac - bd) + i(ad + bc)]$$

$$= (ac - bd)^2 + (ad + bc)2$$

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

$\therefore$ $$d(xy) \geq d(x) \text{ if } y \neq 0 \quad ...(i)$$

as if $y \neq 0 \Rightarrow c \neq 0$ or $d \neq 0 \Rightarrow c^2 + d^2 \geq 1$

$\Rightarrow$ $$d(y) \geq 1$$

And finally we prove the euclidian algorithm of J.

i.e., $x, y \in J, x \neq 0$ and $y \neq 0$ $\exists$ t and $r \in J$ such that

$$x = yt + r$$

Let $y = n \in J$ be an integer. (We first prove it for this special case).

and $$x = a + ib; \ a, b \in z$$

By euclidean algorithm for z, $\exists$ $t, r \in z$

$$a = nt + r$$

where $r = 0$ or $r < n$.

Now $r < \frac{n}{2}$ or $r \geq \frac{n}{2}$

If $r \geq \frac{n}{2}$,

$$r_1 = n - r < \frac{n}{2}$$

$$a = n(t + 1) - n + r$$

$$= n(t + 1) - r_1$$

Either way a can be written as

$$a = nt_1 + k_1 \text{ where } |k_1| < \frac{n}{2} \text{ or } k_1 = 0$$

Similarly b can be written as

$$b = nt_2 + k_2 \text{ where } |k_2| < \frac{n}{2} \text{ or } k_2 = 0$$

$$\therefore \quad a + ib = n(t_1 + it_2) + k_1 + ik_2$$

where $k_1 + ik_2 = 0$

or $$d(k_1 + ik_2) = k_1^2 + k^2 < \frac{n^2}{4} + \frac{n^2}{4} < n^2 = d(n)$$

So, in this case the result is proved.

Again consider $x, y \in J$ be any two non-zero members.

$$y\bar{y} = c^2 + d^2 \in z$$

$\therefore \exists\, t, r \in J$ such that

$$x\bar{y} = y\bar{y}t + r$$

If $r = 0 \Rightarrow$ $\quad x\bar{y} = ty\bar{y} \Rightarrow x = ty$

If $d(r) < d(y\bar{y}) \Rightarrow$ $\quad d(x\bar{y} - ty\bar{y}) < d(y\bar{y})$

$\Rightarrow$ $\quad d(x - ty)d(\bar{y}) < d(y)d(\bar{y})$ [from (i)]

$$d(x - ty) < d(y)$$

Let $x - ty = r$

Then $x = ty + r$ where $d(r) < d(y)$

$\therefore$ The result follows for general case.

So, J is a Euclidean Domain.

Now, every *ED* is a *PID*. So J is a *PID* and every *PID* is a *UFD*. So J is a *UFD* as well.

2.9 Let R^r = Ring of all real valued functions on [0, 1] under the operations.

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

Let $$M = \left\{ f \in R^C \middle| f\left(\frac{1}{2}\right) = 0 \right\}$$

Is M a maximal ideal of R? Justify your answer.

(2013 : 15 Marks)

Solution:

First we need to prove that M is an ideal of R^C.

Define $g : R[0, 1] \to R$

$$g(x) = 0 \quad \forall x \in [0,1]$$

Then $g(x)$ is real valued and continuous and $g(1/2) = 0$

$\Rightarrow g \leftarrow M \Rightarrow M \neq \phi$, i.e., non empty.

Again, $f, g \in M \Rightarrow$ $\quad f\left(\frac{1}{2}\right) = g\left(\frac{1}{2}\right) = 0$

$$f\left(\frac{1}{2}\right) - g\left(\frac{1}{2}\right) = 0 - 0 = 0$$

so $f - g \in M$.
and $f \in M, h \in R^C$

$$fh\left(\frac{1}{2}\right) = f\left(\frac{1}{2}\right)h\left(\frac{1}{2}\right) = 0 \cdot h\left(\frac{1}{2}\right) = 0$$

$\therefore$ $fh \in M$

So, M is an ideal of R^C.
Let I be another ideal of R^C and $MCI \leq R^C$.
If $M \neq I$, i.e., M is a proper subset of I then $\exists\, \lambda \in I$ such that $\lambda \notin M$

$\lambda \notin M \Rightarrow$ $$\lambda\left(\frac{1}{2}\right) = C \neq 0$$

Define $y : [0, 1] \to R$ such that

$$y(x) = C \ \forall x \in [0,1]$$

Then $y \in R^C$
Also let $\beta : y - \lambda \in R^C$

and $$\beta\left(\frac{1}{2}\right) = y\left(\frac{1}{2}\right) - \lambda\left(\frac{1}{2}\right) = C - C = 0$$

$\therefore$ $\beta \in M$

$\Rightarrow \beta \in I$ as $M \subset I$
$\Rightarrow y \in I$ as $\lambda \in I \Rightarrow \beta + \lambda \in I$
Finally let $\alpha : [0, 1] \to R$

$$\alpha(x) = \frac{1}{C} \ \forall\, x \in [0,1]$$

Then $\alpha \in R^C$ as it is continuous.
And $y \in I$
$\Rightarrow \alpha y \in I$ as I is an ideal.

But $$\alpha y(x) = \frac{1}{C} \cdot C = 1 \ \forall\, x \in [0,1]$$

i.e., αy is identity of R^C.
$\Rightarrow$ Identity of $R^C \in I$
$\Rightarrow$ $$R^C = I$$
So, M is a maximal ideal.

2.10 Prove that the set $Q(\sqrt{5}) = \left\{\frac{a + b\sqrt{5}}{a, b \in Q}\right\}$ is a commutative ring with identity.

Solution: (2014 : 15 Marks)

Given that :

$$Q(\sqrt{5}) = \left\{\frac{a + b\sqrt{5}}{a, b \in Q}\right\}$$

To prove $Q(\sqrt{5})$ is a commutative ring with identity, it must satisfies the following properties :

I. To prove $(Q\sqrt{5}, +)$ is an aselian group :

(i) **Closure Prop :**

Let $a + b\sqrt{5}$, $c + d\sqrt{5} \in Q(\sqrt{5})$, $a, b, c, d \in Q$.
$\therefore$ Closure property is satisfied. ($\because a + c, b + d \in Q$)

(ii) **Asso. Prop :**

Let $x, y, z \in Q(\sqrt{5})$

Choosing $x = a+b\sqrt{5}$, $y = c+d\sqrt{5}$, $z = e+f\sqrt{5}$ where $a, b, c, d, e, f \in Q$

$\therefore$ $(x + y) + z = x + (y + z)$ (By associative property of R)

$\therefore$ Associative Property is satisfied.

(iii) **Existence of Rest Identity :**

$$\forall x = a+b\sqrt{5} \in Q(\sqrt{5})$$

$$y = 0+0\sqrt{5} \in Q(\sqrt{5}) \text{ where } a, b \in Q.$$

such that

$$y = (0+0\sqrt{5})+(a+b\sqrt{5})$$

$$= (0 + a) + (0 + b)\sqrt{5}$$

$$= a+b\sqrt{5}$$

$$= x$$

$\therefore$ The identity element is $0+0\sqrt{5} = 0 \in Q(\sqrt{5})$

(iv) **Existence of left inverse :**

For each $a+b\sqrt{5} \in Q[\sqrt{5})$ if $-(-b) \in Q(\sqrt{5}) = 0+0\sqrt{5}$

$\therefore$ Inverse of $a+b\sqrt{5} = -a-b\sqrt{5} \in Q(\sqrt{5})$

(v) **Commutative Property :**

$-\forall x, y \in Q[\sqrt{5}]$ where $x = a+b\sqrt{5}$, $y = c+d\sqrt{5}$

$\Rightarrow$ $x + y = y + x$ (by commutative property in Q)

$\therefore$ Commutative property is satisfied.

$\because$ $(Q\sqrt{5}, +)$ is an abelian group.

II. To prove $(Q\sqrt{5})$ is a semigroup :

(i) **Closure Prop :**

Let $x = a+b\sqrt{5}$, $y = c+d\sqrt{5} \in Q\sqrt{5}$, $a, b, c, d, \in Q$

then $x \cdot y = (a+b\sqrt{5})(c+d\sqrt{5})$

$= (ac+5bd)+(ad+bc)+5 \in Q(\sqrt{5})$ ($\because$ $ac + 5bd$, $ad + btQ$)

$\therefore$ Closure properties is satisfied.

(ii) Let $x, y, z \in Q(\sqrt{5})$

Choosing $x = a+b\sqrt{5}$, $y = c+d\sqrt{5}$, $z = e+f\sqrt{5}$, $a, b, c, d, e, f \in Q$.

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$\therefore$ Associative Property is satisfied.

2.11 Give an example of a ring having identity but a subring of this having a different identity.

(2015 : 10 Marks)

Solution:

Let R be a ring such that

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a,b,c,d \in R \right\}$$

Clearly, R is a ring and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an identity in R.

Now, consider subring $R_1 = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} ; x \in R \right\}$

R_1 is a subring of R_1. However, $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is an identity of R_1.

Thus, R_1 which is a subring has different identity from R.

2.12 If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R' that $\phi(1)$ is unit element of R'. (2015 : 15 Marks)

Solution:

Given : $f: R \to R'$ be a homomorphic.

1 is unit in R.

Let $x \in R$ be an element.

$\therefore x = 1 \cdot x$ as 1 is a unit.

$\therefore \quad \phi(x) = \phi(1 \cdot x) = \phi(1) \cdot \phi(x)$

$\Rightarrow \quad \phi(x) = \phi(1) \cdot \phi(x)$ ...(i)

Similarly, $x = x \cdot 1$

$\therefore \quad \phi(x) = \phi(x \cdot 1) = \phi(x) \cdot \phi(1)$

$\Rightarrow \quad \phi(x) = \phi(x) \cdot \phi(1)$ ...(ii)

From (i) and (ii), it can be concluded that $\phi(1)$ is a unit element in R'.

2.13 Do the following sets form integral domains with respect to ordinary addition and multiplication? If so, state if they are fields :

(i) The set of numbers of the form $b\sqrt{2}$ with b rational.

(ii) The set of even integers.

(iii) The set of positive integers.

Solution: (2015 : 5+6+4 = 15)

An integral domain is a commutative ring with unity without zero divisors.

(i) Given, $G = \{b\sqrt{2} \mid b \in Q\}$ (assume)

Now, 1 is a unit of $b\sqrt{2} \quad \forall b \in Q$ but $1 \notin G$

$\therefore \quad G = \{b\sqrt{2} \mid b \in Q\}$ is not an integral domain.

(ii) Let $G = \{2n \mid n \in N\}$

Now, $1 \notin G$ which is a unity of even integers.

$\therefore G$ = set of even integers is not an integral domain.

(iii) Let G = {0, 1, 2, 3, ...} = set of positive integers.

Clearly, G is commutative.

$1 \in G \Rightarrow$ unity belongs to G.

Let $a \in G$, for some $b \in G$

if

$a \cdot b = 0$

$\Rightarrow$ $b = 0$ as a, b are integers.

So, it is an integral domain.

Now, suppose $a, b \in G$ such that

$$a \cdot b = 1$$

$\Rightarrow$ $b = \left(\frac{1}{a}\right)$ but $b \notin G$ if $a \neq 1$

$\therefore$ no element of G has its multiplicative inverse except 1.

$\therefore$ G is not a field.

So, (i) and (ii) are neither integral domains nor a field.

(iii) is an integral domain but not a field.

2.14 Let K be a field and $K[X]$ be the ring of polynomials over K in a single variable X. For a polynomial $f \in K[X]$; let $<f>$ denote the ideal in $K[X]$ generated by f. Show that $<f>$ is a maximum ideal in $K[X]$ if and only if f is an irreducible polynomial over K.

(2016 : 10 Marks)

Solution:

Given, K is a field and $K[X]$ is ring of polynomials. Let F be an ideal generated by f, $f \in K[X]$.

$\therefore$ $F = <f>, f \neq 0$

Let $F = <f>$ is a maximal ideal.

Let $f = g \cdot h$, where $g, h \in K[X]$, $g, h \neq 0$.

Let a be an ideal generated by g.

$\therefore$ $a = <g>$

$\therefore$ $F < G < K[X]$

but F is maximal ideal by our assumption.

$\therefore$ either $F = G$ or $G = K[X]$

Case 1 :

If $G = K[X]$, then

$1 \in G$

$\therefore$ $1 = g \cdot h$, for some $h_2 \in K[X]$

$\Rightarrow$ $(\deg 1) = \deg g + \deg h_1 \Rightarrow 0 = \deg g + \deg h_1$

$\Rightarrow$ $\deg g = 0 \Rightarrow g =$ constant polynomial

Case 2 :

If $F = G$

$\therefore$ For some $h_2 \in K[X]$

$g = f \cdot h_2$

$\therefore$ $f = g \cdot h$

$\Rightarrow$ $gh = f \Rightarrow f \cdot h_2 \cdot h = f$

$\Rightarrow$ $f(1 - h_2 h) = 0$

as $f \neq 0$, $1 - h_2 h = 0$ ($K[X]$ is integral domain)

$\Rightarrow$ $h_2 \cdot h = 1 \Rightarrow \deg(h) = 0$

$\Rightarrow h$ is a constant polynomial.

Thus, from both case (1) and case (2), either g or h is a constant polynomial and $g, h \neq 0$.

$\Rightarrow f$ is an irreducible polynomial over K.

Conversely : Let f is an irreducible polynomial over K.

Let $<f>$ is not a maximal ideal and $I = <d>$, $d \in K[x]$, such that

$$F < I < K[x]$$

Now, for some $t \in K[x]$,

$$f = d \cdot t$$

as f is an irreducible polynomial.

$\therefore$ either d or t is a constant polynomial.

Case 1 : If deg $t = 0$

then, $d = \frac{1}{t} \cdot (f)$

$\Rightarrow$ $\langle d \rangle < \langle f \rangle$

$\Rightarrow$ $I < F$

But $F < I$ as per our assumption.

$\Rightarrow$ $I = F$

Case 2 : If deg $(d) = 0$

$\therefore$ for some $P \in K[X]$, $d \cdot p = 1$

$\Rightarrow$ $1 \in I$

From case (1) and case (2), it can be inferred that I is not maximal.

$\therefore$ F is a maximal ideal.

2.15 Let F be a field and $F[x]$ denote the ring of polynomials over F in a single variable x. For $f(x)$, $g(x) \in F[x]$ with $g(x) \neq 0$, show that there exists $q(x)$, $r(x) \in F(x)$ such that degree of $(r(x))$ < degree $(g(x))$ and, $f(x) = q(x)g(x) + r(x)$.

(2017 : 20 Marks)

Solution:

To show the existence of $q(x)$ and $r(x)$. If $f(x) = 0$ or deg $f(x) <$ deg $g(x)$, we simply say $q(x) = 0$ and $r(x) = f(x)$.

So, we assume that

$$n = \deg f(x) \geq \deg g(x) = m \text{ and}$$

Let $f(x) = a_n x^n + \ldots + a_0$ and

$g(x) = b_m x^m + \ldots + b_0$

We use the idea of 'long division' of $f(x)$ by $f(x)$, then use the second PMI on deg $f(x)$.

So, by long division, let

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

Then, $f_1(x) = 0$ or deg $f_1(x) <$ deg $f(x)$

by our induction hypothesis, there exist $q_1(x)$ and $r_1(x)$ in $F[x]$ s.t.

$$f_1(x) = q_1(x)g(x) + r_1(x),$$

where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$

Hence,

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + f_1(x) \\ &= a_n b_m^{-1} x^{n-m} g(x) + q_1(x)g(x) + r_1(x) \\ &= [a_n b_m^{-1} x^{n-m} + q_1(x)]g(x) + r_1(x) \end{aligned}$$

So, the polynomials, $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$

and $r(x) = r_1(x)$ have the desired properties.

To prove the uniqueness, suppose that $f(x) = g(x)q(x) + r(x)$ and $f(x) = g(x)\bar{q}(x) + \bar{r}(x)$, where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$ and $\bar{r}(x) = 0$ or deg $\bar{r}(x) <$ deg $g(x)$.

Subtracting these two equations,

$$0 = g(x)[q(x) - \bar{q}(x)] + [r(x) - \bar{r}(x)]$$

or $$\bar{r}(x) - r(x) = g(x)[q(x) - \bar{q}(x)]$$

Thus, $\bar{r}(x) - r(x)$ is 0, or the deg $(\bar{r}(x) - r(x))$ is at least that of $g(x)$.

Since, second case is impossible.

$\therefore$ $\bar{r}(x) = r(x)$ and $q(x) = \bar{q}(x)$

2.16 Let R be an integral domain with unit element. Show that any unit in $R[x]$ is a unit in R.

Solution: (2018 : 10 Marks)

Let $f(x) \in R[x]$ be a unit in $R[x]$.

$\therefore \exists\ g(x) \in R[x]$ such that $f(x) \cdot g(x) = 1$

Now, therefore $\deg(f(x) \cdot g(x) = \deg(1) = 0$

$\because$ R is an integral domain, i.e., it has no zero divisors. Therefore,

So, $\deg(f(x) \cdot g(x) = \deg f(x) + \deg g(x)$

i.e., $\deg f(x) + \deg g(x) = 0$

Let $\deg f(x) = \deg g(x) = 0$

So, $f(x) = a_0$ where a_0, b_0 are constants.

$\therefore$ $g(x) = b_0$

$\because a_0, b_0 \in R, \therefore a_0$ is a unit. $f(x) \cdot g(x) = a_0 \cdot b_0 = 1$

$\therefore f(x) = a_0$ is unit in $R[x]$ and a_0 is also a unit in R.

2.17 Let a be an irreducible element of the Euclidean ring R, then prove that $R/(a)$ is a field.

Solution: (2019 : 10 Marks)

Let $A = (a)$, where a is an irreducible element of R.

We shall show that A is a maximal ideal of R. Let I be any ideal of R such that $A \subseteq I \subseteq R$. Since R is an Euclidean ring and E.D. $\Rightarrow$ P.I.D.

$\therefore$ We have, R is a PID.

Let $I = \langle d \rangle$, for some $d \in R$

Case (i) : Let $d \in A = (a)$. Then $d = ax$ for some $x \in R$.

for any $r \in I = (d)$, $n = dy$ for some $y \in R$.

$\Rightarrow$ $r = (ax)_y = a(xy)$

$\Rightarrow r \in A$

$\Rightarrow ISA$

Also, $A \subseteq I$

$\therefore$ $A = I$

Case (ii) : Let $d \in A$

Since $a \in A$ and $A \subset I = (d)$

So, $a = dt$ for some $t \in R$

Since, R is irreducible, either d or t is a unit.

If t is a unit, then $t^{-1} \in R$ and so $d = at^{-1}$.

Since, $a \in A$, which is a contradiction. Consequently, d must be a unit, i.e., $d^{-1} \in R$.

Now, $d \in I$ and $d^{-1} \in R \Rightarrow$ $1 = dd^{-1} \in I$

$\Rightarrow$ $I = R$

Hence, $ASISR$

$\Rightarrow$ $A = I$ or $I = R$

$\Rightarrow A$ is a maximal ideal of R, i.e., since (a) is a maximal ideal of R.

Therefore, $R(a)$ is a field. Hence proved.

3. Fields

3.1 Consider the polynomial ring $Q[x]$. Show $P(x) = x^3 - 2$ is irreducible over Q. Let I be the ideal in $Q[x]$ generated by $P(x)$. Then show that $Q[x]/I$ is a field and that each element is of the form $a_0 + a_1t + a_2t^2$ with a, a_1, a_2 in Q and $t = x + I$. (2010 : 15 Marks)

Solution:

Given : $P(x) = x^3 - 2$

Let $f(x), g(x) \in Q[x]$, and $p(x)$ is reducible such that

$$p(x) = f(x).g(x)$$

Suppose, $f(x) = x + a$

$$g(x) = x^2 + bx + c$$

$\therefore$ $p(x) = x^3 - 2 = (x + a)(x^2 + bx + c)$

$\Rightarrow$ $x^3 - 2 = x^3 + bx^2 + cx + ax^2 + bx + ac$

Comparing LHS & RHS, we get

$$a + b = 0 \Rightarrow a = -b$$

$$ab + c = 0$$

$\Rightarrow$ $-a^2 + c = 0 \Rightarrow c = a^2$

$$ac = -2$$

$\Rightarrow$ $a^3 = -2 \Rightarrow a = -2^{1/3}$ which is not a rational number

i.e., $a \notin Q \Rightarrow b, c \notin Q$

$\therefore$ $p(x)$ is irreducible over Q.

Now, I is ideal generated by $p(x)$

i.e., $I = \langle p(x) \rangle$

$\therefore$ $\frac{Q(x)}{I}$ is a field as $p(x)$ is irreducible (theorem)

$\therefore$ $$\frac{Q(x)}{I} = \langle p(x) \rangle + b_0 + b_1x + b_2x^2 = I + b_0 + b_1x + b_2x^2 \quad ...(1)$$

as $\deg.(b_0 + b_1x + b_2x^2) < \deg.(p(x))$

$\downarrow$

remainder term

where $b_0, b_1, b_2 \in Q$.

Now, $t = x + I$

$$a_0 + a_1t + a_2t^2 = a_0 + a_1(x + I) + a_2(x + I)^2$$
$$= a_0 + a_1(x + I) + a_2(x + I)(x + I)$$
$$= a_0 + a_1(x + I) + a_2(x^2 + I)$$
$$= a_0 + a_1x + a_2x^2 + I \text{ which is equivalent to eqn. (1)}$$

$\therefore$ $\frac{q(x)}{I}$ can be written as $a_0 + a_1t + a_2t^2$ where $t = x + I$.

3.2 Show that the set of matrices $S = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} a, b \in R \right\}$ is a field under the usual binary operations of matrix addition and matrix multiplication. What are the additive and multiplicative identities and what

is the inverse of $\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}$? Consider the map $f: C \to S$ defined by $f(a+ib) = \begin{bmatrix}a & -b\\ b & a\end{bmatrix}$. Show that f is an isomorphism (Here R is the set of real numbers and C is the set of complex numbers)?

(2013 : 10 Marks)

Solution:

Approach : Prove only the important parts in actual exam.

$SCM(2, r)$ where $M(2, R)$ is the ring of 2×2 matrices with entries from R.

To show S is a field

$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix} \in S \Rightarrow \begin{bmatrix}a & -b\\ b & a\end{bmatrix}^{-1} = \begin{bmatrix}\frac{a}{a^2+b^2} & \frac{b}{a^2+b^2}\\ \frac{-b}{a^2+b^2} & \frac{a}{a^2+b^2}\end{bmatrix}^{-1} \in S$$

and
$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix}\begin{bmatrix}c & -d\\ d & c\end{bmatrix}^{-1} = \begin{bmatrix}a & -b\\ b & a\end{bmatrix}\begin{bmatrix}\frac{c}{c^2+d^2} & \frac{d}{c^2+d^2}\\ \frac{-d}{c^2+d^2} & \frac{c}{c^2+d^2}\end{bmatrix} = \begin{bmatrix}\frac{ac+bd}{c^2+d^2} & \frac{-(bc-ad)}{c^2+d^2}\\ \frac{bc-ad}{c^2+d^2} & \frac{ac+bd}{c^2+d^2}\end{bmatrix} \in S$$

So, S is closed w.r.t. multiplication and has multiplicative inverse.

Also,
$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix}\begin{bmatrix}c & -d\\ d & c\end{bmatrix} = \begin{bmatrix}ac-bc & -(bc+ad)\\ bc+ad & ac-bd\end{bmatrix} = \begin{bmatrix}c & -d\\ d & c\end{bmatrix}\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$$

i.e., multiplication is commutative.

That addition is commutative, closed and has inverse follows from S being subset of $M(2, R)$.

$\therefore$ S is a field.

Additive identity :

$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix}+\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix} = \begin{bmatrix}a & -b\\ b & a\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}+\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$$

$\therefore \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix} \in S$ is additive identity.

Similarly, $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = I_2$ is multiplicative identity.

$$\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}^{-1} = \begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{-1}{2} & \frac{1}{2}\end{bmatrix} \in S$$

$$f(a+ib) = \begin{bmatrix}a & -b\\ b & a\end{bmatrix}$$

To show f is isomorphism, f is linear.

$$f[(a+ib)+(c+id)] = f(a+c+i(b+d)]$$
$$= \begin{bmatrix}a+c & -(b+d)\\ b+d & a+c\end{bmatrix} = \begin{bmatrix}a & -b\\ b & a\end{bmatrix}+\begin{bmatrix}c & -d\\ d & c\end{bmatrix}$$

3.3 Show that Z_7 is a field. Then find $([5] + [6])^{-1}$ and $(-[4])^{-1}$ in Z_7. (2014 : 15 Marks)

Solution:

$$z_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$$

For z_7 to be a field, it should satisfy

(i) $(z_7, +)$ is an abelian.

(ii) $(z_7, \times)$ is an abelian group, where $z_7^* = z_7 - \{0\}$

(iii) Distributive law.

(i) $(Z_7, +)$

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

- All elements belong to z_7 – closure property.
- First row coincide with the top row, then [0] is identity element.
- [0] is in every row & column
  ∴ Inverse property satisfied.
- $([a] + [b] + [c] = [a + b] + [c] = [a + b + c] = [a] + [b + c] = [a] + ([b] + [c])$
  ∴ Associative property satisfied.
- Transpose of matrix equal to original matrix.
  ∴ Commutative property satisfy.

(ii) (Z_7^*, x)

×	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

- Every element belong to z_7^*-closure property.
- Top row co-incide with first row, Hence [1] is an identity element.
- [1] is in every row & column.
  ∴ Inverse property satisfied.
- $([a] \times [b] \times [c] = [(a \times b) \times [c] = [a \times b \times c] = [a] \times [b \times c] = [a] \times ([b] \times [c])$.
- Associative property satisfed.
- Transpose of matrix is equal to original matrix.
  ∴ Commutative property satisfy.

(iii) **Distributivity :**

$$[a] \times ([b] \times [c]) = [a] \times ([b + c]) = [a(b + c)]$$
$$= [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$$

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

Similarly

$$\Rightarrow \quad ([5]+[6])^{-1} = [4]^{-1} = [2]$$

$$\Rightarrow \quad (-[4])^{-1} = ([3])^{-1} = [5]$$

3.4 Show that the set $\{a + b\omega : \omega^3 = 1\}$, where a and b are real numbers, is a field with respect to usual addition and multiplication.

(2014 : 15 Marks)

Solution:

Let $G = \{(a + bw); w^3 = 1 ; a, b \in |R\}$

(i) Let $(G, +)$ be an algebraic structure.

$\forall (a + bw), (c + dw) \in G.$

$$(a + bw) + (c + dw) = (a + c) + (b + d)w$$
$$= p + qw - (a + c) \in |R$$

$\therefore$ Closure property satisfy.

(ii) Let, $(a + bw), (c + dw), (e + fw) \in G.$

$$[(a + bw) + (c + dw)] = ((a + c) + (b + d)w) + (e + fw)$$
$$= (a + c + e) + (b + d + f)w \quad \text{... (i)}$$

$(a + c + e) \in |R$

$(b + d + f) \in |R$

$$a + bw) + [(c + dw) + (e + fw)] = (a + bw) + [(c + e) + (d + f)w]$$
$$= (a + c + e) + (b + d + f)w \quad \text{...(ii)}$$

From (i) & (ii) $\Rightarrow$ Associative property satisfy.

(iii) Let $(a + bw) \in G, 0 \in G.$

$$(a + bw) + 0 = (a + bw)$$

$\therefore$ '0' is the identity element of $(G, +)$.

(iv) Let $(a + bw) \in G, (-a - bw) \in G$

$$(a + bw) + (-a - bw) = (a - a) + (b - b)w = 0$$

$\therefore$ Inverse property satisfied.

(v) Let $(a + bw), (c + dw) \in G.$

$\therefore$
$$a + bw + c + dw = (a + c) + (b + d)w$$
$$= (c + a) + (d + b)w$$
$$= c + dw + a + bw$$

$\therefore$ Commutative property satisfied.

$\therefore$ $(G, +)$ is an abelian group.

(ii) $(G^*, \times)$; G^* denote $G - \{0\}$

(i) Let $(a + bw), (c + dw) \in G.$

$$(a + bw) \times (c + dw) = ac + bdw^2 + (ad + bc)w$$
$$= ac + bd(-1-w) + (ad + bc)w$$
$$= (ac - bd) + w(ad + bc - bd) \in G$$

$\therefore$ Closure property satisfied.

(ii) Associative property is satisfies over complex numbers.

(iii)
$$(a + bw)(c + dw) = (a + bw)$$

Let,
$$c = 1; d = 0$$
$$(a + bw)(1) = (a + bw) \quad 1 \in G^*$$

$\therefore$ Identity property satisfied.

(iv)
$$(a + bw)(c + dw) = 1$$
$$(ac - bd) + w(bc + ad - bd) = 0$$

$$c + dw = \frac{1}{a+bw} \times \frac{a+bw^2}{a+bw^2}$$

$$= \frac{a+bw^2}{a^2+b^2w^3+ab(w+w^2)}$$

$$= \frac{a+b(-1-w)}{a^2+b^2+ab(-1)} = \frac{a-b-bw}{a^2+b^2+(-ab)}$$

$$= \frac{(a-b)}{a^2+b^2-ab} + \frac{(-bw)}{a^2+b^2-ab}$$

$$\therefore \quad c + dw = l + pw$$

where,

$$l = \frac{a-b}{a^2+b^2-ab}$$

$$p = \frac{-b}{a^2+b^2-ab}$$

$(a-b)^2 \geq 0,\ a^2+b^2 \geq 2ab > ab,\ a \leq a,\ b \neq 0$

$\therefore$ Inverse exists.

(v) $$(a+bw).(c+dw) = ac + bcw + adw + bdw^2$$
$$= c(a+bw) + d(aw+bw^2)$$
$$= (c+dw).(a+bw)$$

$\therefore$ commutative satisfy.

$\therefore$ $(G^*, \times)$ is an abelian group.

(iii) **Distributive Property :**

$$(a+bw) \times [(c+dw) + (e+fw)] = (a+bw) \times [(c+e) + (d+f)w]$$
$$= ac + ae + bcw + bew + (ad+af)w + (bd+bf)w^2$$
$$= (a+bw) \times (c+dw) + (a+bw) \times (e+fw)$$

3.5 Let K be an extension of a field F. Prove that the elements of K which are algebraic over F, from a subfield of K. Further, if $F < K < L$ are fields, L is algebraic over K and K is algebraic over F, then prove that L is algebraic over F.

(2016 : 20 Marks)

Solution:

Given, K is an extension of F.

Let $a, b \in K$ and a, b are algebraic over F. Then $F(a, b)$ is a finite extension of F. So, all elements of $F(a, b)$ are algebraic over F.

$\therefore$ $a + b,\ ab,\ ab^{-1}$ (if $b \neq 0$) are algebraic over F.

$\therefore$ elements of K which are algebraic over F form a subfield of K.

Now, given $F < K < L$ and $\frac{K}{F}$ and $\frac{L}{K}$ are algebraic.

Let $a \in L$. Since L is algebraic over K, a is algebraic over K.

$\therefore$ $\exists\ 0 \neq f(x) \in K[x]$ such that $f(a) = 0$

Let $$f(x) = \alpha_0 + \alpha_1 x + \ldots\ldots + \alpha_n x_n,\ \alpha_i \in K$$

Since K is algebraic over F, each $\alpha_i \in K$ is algebraic over F. We know that if $a_1, a_2, \ldots\ldots, a_n \in K$ are algebraic over F then $F(a_1, a_2, \ldots\ldots a_n)$ is finite extension of F and so is algebraic over F.

$\therefore$ $$[F(\alpha_0, \alpha_1, \ldots, \alpha_n)F] = \text{Finite}$$

Let $$M = F(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n)$$

Then, $[M : F]$ is finite and so M is algebraic over F. Clearly each $a_i \in M$. Thus, $f(x) \in M[x]$, i.e., a is algebraic over M.

Now, we knw that if $a \in K$ be algebraic over F, then $[F(a) : F]$ = Finite = deg Irr(F, a) and so $F(a)$ is an algebraic extension of F.

$\therefore$ $M(a)$ is finite extension of M.

$\Rightarrow$ $[M(a) : F] = [M(a) : M]\,[M : F]$ = Finite

$\Rightarrow$ $M(a)$ is algebraic over F.

$\Rightarrow$ $a \in M(a)$ is algebraic over F.

Since a is an arbitrary element of L. $\therefore$ L is an algebraic extension of F or L is algebraic over F.

3.6 Show that every algebraically closed field is infinite.

(2016 : 15 Marks)

Solution:

We know that any field, say F is called as algebraically closed if each non-constant polynomial in $F[x]$ has a root in F.

Now, let $a_i \in F$, where F is a finite field.

Consider $f(x) = 1 + \underset{a_i \in F}{\pi}(x - a_i)$ $\{a_1, a_2, \ldots\ldots \in F\}$

The coefficients of $f(x)$ lie in the field F and so, $f(x) \in F(x)$. Also, $f(x)$ is a non-constant polynomial.

Now, for each $a_i \in F$, we have

$$f(a_i) = 1 \neq 0$$

$\therefore$ $f(x)$ has no root in F, as any value a_i is not a root. As F is finite, so we cannot choose any value outside a_i.

$\therefore$ F is not algebraically closed.

As any finite field F is not algebraically closed, $\therefore$ any algebraically closed field shoudl be finite.

■■■■