IAS-2000

2000 / 20M → A finite commutative ring without zero divisors is a field.

2(c). Soln: Let F be a finite commutative ring without zero divisors.

Let $F = \{a_1, a_2, \ldots a_n\}$ and F contains 'n' distinct elements.

TO prove that F is a field.

for this we are enough to prove that an element $1 \in F$ such that $1 \cdot a = a \cdot 1 = a \ \forall a \in F$ and also for every element $a \neq 0 \in F$, there exists an element $b \in F$ such that $ab = ba = 1$.

Let $a \neq 0 \in F$.

$\therefore aa_1, aa_2, \ldots aa_n \in F$ (by closure prop of F)

All these elts are distinct.

because, if possible

let $aa_i = aa_j$; $a_i, a_j \in R$

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

$\Rightarrow a_i - a_j = 0$ ($\because a \neq 0$ & F is ID)

$\Rightarrow a_i = a_j$

which is contradiction to hyp. that F contains n distinct elts.

$\therefore aa_1, aa_2, \ldots aa_n$ are n distinct elts in F which has exactly 'n' elts.

$\therefore$ By the pigeon-hole principle every element F can be written as aa_i for some $a_i \in F$.

since $a \neq 0 \in F$, we have $a = aa_i$ for some $a_i \in F$.

Since F is commutative:

$\therefore a = aa_i = a_i a$.

we now prove that a_i is unit element.

Let $y \in F$ then $y = aa_j$ for some $a_j \in F$.

$$\Rightarrow a_i y = a_i(aa_j) = (a_i a)a_j = aa_j = y$$

$$\Rightarrow a_i y = 1 \cdot y \Rightarrow a_i = 1 \quad \text{(by RCL)}$$

$\therefore a \in F \ \exists\ 1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$.

$\therefore$ 1 is the unit element in F.

since $1 \in F$

$1 = aa_k$ for some $a_k \in F$.

$\therefore$ for $a \neq 0 \in F$, $\exists\ a_k \in F$ such that $aa_k = 1 = a_k a$.

($\because$ F is comm.)

$\therefore a \neq 0 \in D$ has x^{ve} inverse in F.

$\therefore$ F is a field.

HEAD OFFICE:25/8, Old Rajinder Nagar Market, Delhi-60. (M) 9999197625, 011-45629987. BRANCH OFFICE(DELHI): 105-106, Top Floor, Mukherjee Tower, Mukherjee Nagar, Delhi-9. BRANCH OFFICE(HYDERBAD): H.No. 1-10-237, 2nd Floor, Room No. 202 R.K'S-Kancham's Blue Sapphire Ashok Nagar Hyd-20. (M) 09652351152, 09652661152

2001 / 12M **1(b).** Prove that the polynomial $1+x+x^2+\cdots\cdots+x^{p-1}$ where p is a prime number, is irreducible over the field of rational numbers.

Soln: Let $f(x) = 1+x+x^2+\cdots\cdots+x^{p-1}$

$= \frac{x^p-1}{x-1}$ $\left(\because 1+x+x^2 = \frac{x^3-1}{x-1} = \frac{(x-1)(x^2+x+1)}{x-1} = x^2+x+1\right)$

Replacing x by x+1, we get

$f(x+1) = \frac{(1+x)^p-1}{x}$

$= \frac{1}{x}\left[1+{}^pC_1 x+{}^pC_2 x^2+\cdots {}^pC_{p-1}x^{p-1}+x^p-1\right]$

$= p+\frac{1}{2}p(p-1)x+\cdots+px^{p-2}+1.x^{p-1}$

we write $a_0 = p$, $a_1 = \frac{1}{2}p(p-1)\cdots\cdots a_{p-1} = p$,

$a_p = 1$.

(by comparing with $a_0+a_1x+a_2x^2+\cdots+a_nx^n$)

Then p divides $a_0, a_1, \cdots\cdots a_{p-1}$; but p doesnot divide a_p and p^2 doesnot divide a_0.

By Eisenstein criterion of irreducibility, $f(x+1)$ is irreducible over $\mathbb{Q}$.

Now we show that $f(x)$ is irreducible over $\mathbb{Q}$.

Suppose this is false.

Then we can write

$f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$

and $\deg g(x) > 0$ and $\deg h(x) > 0$.

$\therefore f(x+1) = g(x+1)h(x+1)$

where $g(x+1)$, $h(x+1) \in \mathbb{Q}[x]$; $\deg g(x+1) > 0$ and $\deg h(x+1) > 0$.

It means that $f(x+1)$ is not irreducible over $\mathbb{Q}$,

which is a contradiction.

Hence $f(x)$ irreducible over $\mathbb{Q}$.

2(a). 2001 → Let N be a normal subgroup of G. Show that $\frac{G}{N}$ is abelian iff $xy\bar{x}^{1}\bar{y}^{1} \in N$ for all $x, y \in G$.

Soln: Let $x, y \in \frac{G}{N}$ then $x = Nx$, $y = Ny$; for some $x, y \in G$.

$\frac{G}{N}$ is abelian $\Leftrightarrow xy = yx$ $\forall x, y \in \frac{G}{N}$.

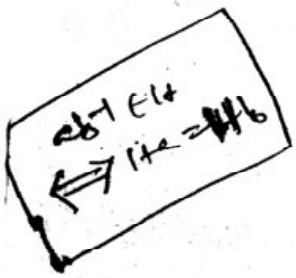
$\Leftrightarrow NxNy = NyNx$ $\forall x, y \in G$.

$\Leftrightarrow Nxy = Nyx$ $\forall x, y \in G$,

$\Leftrightarrow (xy)(yx)^{-1} \in N$ $\forall x, y \in G$

$\Leftrightarrow (xy)(\bar{x}^{1}\bar{y}^{1}) \in N$ $\forall x, y \in G$.

$\Leftrightarrow xy\bar{x}^{1}\bar{y}^{1} \in N$ $\forall x, y \in G$



1988
2001 → If R is a commutative ring with unity, then an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

2(b)

Proof: Given that R is a commutative ring with unity and M is an ideal.

$\therefore$ The quotient ring $\frac{R}{M} = \{a+M / a \in R\}$ is a commutative ring and has unity.

Zero element of $\frac{R}{M}$ is $0+M = M$ where $0 \in R$ is zero element in R.

Unit element of $\frac{R}{M}$ is $1+M$ where $1 \in R$ is the unity element in R.

Now suppose that M is a maximal ideal of R.

We prove that $\frac{R}{M}$ is a field.

To prove that $\frac{R}{M}$ is a field, we have to show that every non-zero element of $\frac{R}{M}$ has multiplicative inverse.

Let $a+M \in \frac{R}{M}$ and $a+M$ be non-zero element

$\therefore a+M \neq M$

$\Rightarrow a \notin M$ $\left(\because a+M \neq M \Leftrightarrow a \notin M \text{ (or) } M+a \neq M \Leftrightarrow a \notin M\right)$

If $\langle a \rangle = \{ar / r \in R\}$ is a principal ideal of R then $\langle a \rangle + M$ is also an ideal of R (Since the sum of two ideals is again an ideal of R) ✓

Again $a = a \cdot 1 + 0 \in \langle a \rangle + M$ and $a \notin M$

$\therefore M \subset \langle a \rangle + M \subseteq R$

Since M is a maximal ideal of R

$\therefore \langle a \rangle + M = R$

Since $1 \in R \Rightarrow 1 \in \langle a \rangle + M$

$\Rightarrow 1 = ar + m$ for some $r \in R, m \in M$.

HEAD OFFICE:25/8, Old Rajinder Nagar Market, Delhi-60. (M) 9999197625, 011-45629987. BRANCH OFFICE(DELHI): 105-106, Top Floor, Mukherjee Tower, Mukherjee Nagar, Delhi-9. BRANCH OFFICE(HYDERBAD): H.No. 1-10-237, 2nd Floor, Room No. 202 R.K'S-Kancham's Blue Sapphire Ashok Nagar Hyd-20. (M) 09652351152, 09652661152

$\Rightarrow 1+M = (ar+m)+M$

$= (ar+M)+(m+M)$

$= (ar+M)+M \quad (\because m \in M \Leftrightarrow m+M = M)$

$= ar+M \quad (\because$ By additive identity prop. of $R/M)$

$= (a+M)(r+M)$

$\therefore (a+M)(r+M) = (r+M)(a+M) = 1 \quad (\because R/M$ is Comm)

$\Rightarrow (a+M)^{-1} = r+M \in \frac{R}{M}$

Hence every non-zero element of $\frac{R}{M}$ is invertible

$\therefore \frac{R}{M}$ is field.

Conversly suppose that $\frac{R}{M}$ is a field.

We prove that M is maximal ideal of R.

Let U be any ideal of R such that

$M \subset U \subseteq R$ and $M \neq U$

Now we shall show that $U = R$

Since $M \subset U$ and $M \neq U, \exists p \in U$ s.t $p \notin M$

$\Rightarrow$ i.e. $p+M \neq M \quad (\because p+M = M \Leftrightarrow p \in M)$

i.e $p+M$ is non-zero element of $\frac{R}{M}$.

Since $\frac{R}{M}$ is a field

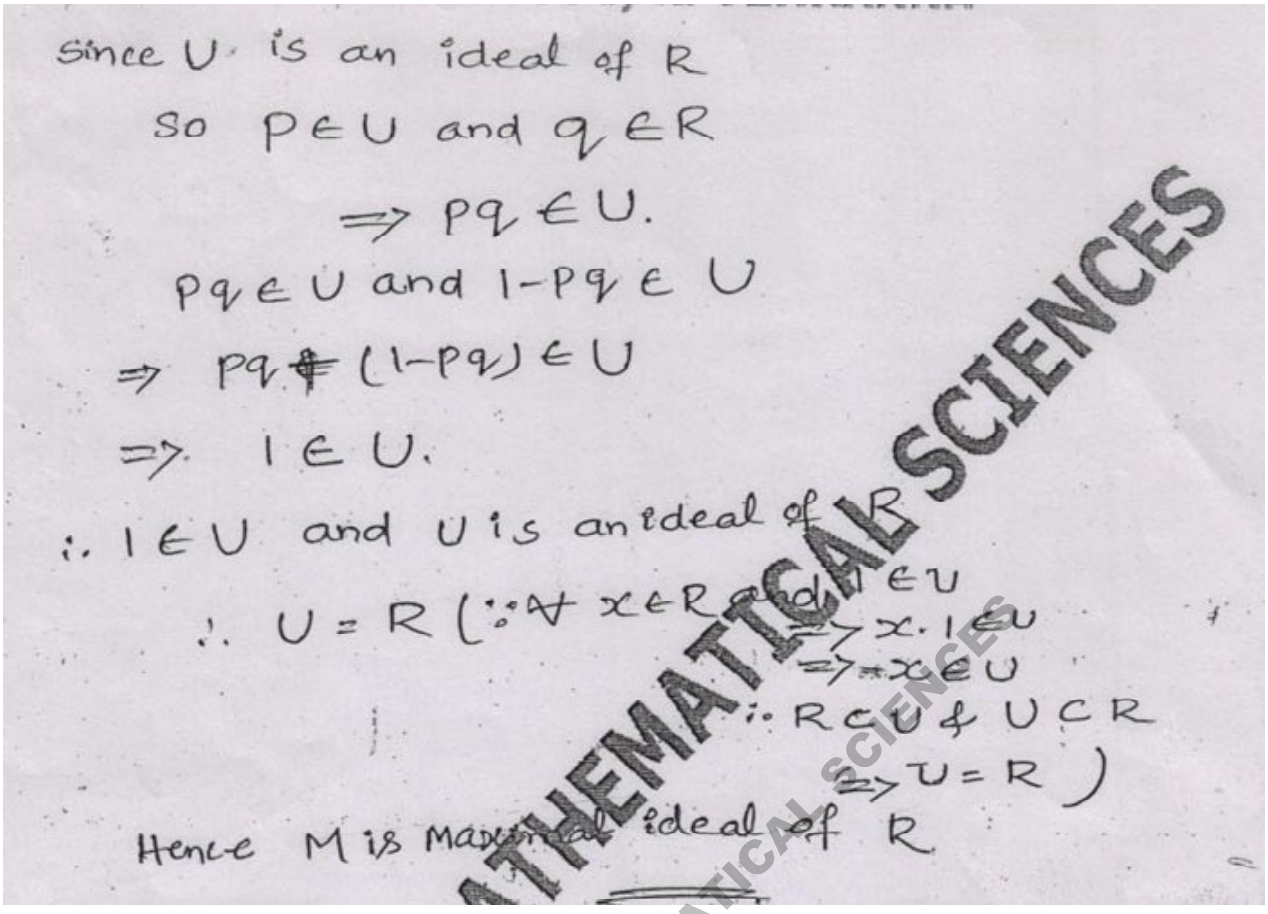
and $p+M$ is non-zero element of $\frac{R}{M}$

$\Rightarrow p+M$ has multiplicative inverse, say $q+M$

$\therefore (p+M)(q+M) = 1+M$

$\Rightarrow pq+M = 1+M$

$\Rightarrow 1-pq \in M \quad (\because a+M = b+M \Leftrightarrow (-a)+b \in M$



Since U is an ideal of R

So $p \in U$ and $q \in R$

$\Rightarrow pq \in U.$

$pq \in U$ and $1-pq \in U$

$\Rightarrow pq + (1-pq) \in U$

$\Rightarrow 1 \in U.$

$\therefore 1 \in U$ and U is an ideal of R

$\therefore U = R$ ($\because \forall x \in R$ and $1 \in U$

$\Rightarrow x \cdot 1 \in U$

$\Rightarrow x \in U$

$\therefore R \subseteq U$ & $U \subseteq R$

$\Rightarrow U = R$)

Hence M is Maximal ideal of R

IAS-2002

2002 IOM

2(a)i If $O(G)=p^2$, where p is prime number then G is abelian.

proof: Since $O(G)=p^2$, p is prime

$\therefore Z \neq \{e\}$, i.e., $O(Z)>1$

By Lagranges theorem

$O(Z)$ divides $O(G)=p^2$

i.e. $\frac{O(G)}{O(Z)}$ i.e. $\frac{p^2}{O(Z)}$

$\therefore O(Z)=p^2$ or p.

Case(i) Let $O(Z)=p^2$

then $O(Z)=O(G) \Rightarrow Z=G$ $(\because Z \subset G)$

10

Since $\forall a \in G \Rightarrow a \in Z \Rightarrow ax=xa \quad \forall x \in G$

$\therefore G$ is abelian.

Case(ii): Let $O(Z)=p$

Since $O(G)=p^2>p$

i.e, $p<p^2$

i.e, $O(Z)<O(G)$

$\therefore Z$ is proper subgroup of G.

So that there exists some $a \in G$ such that $a \notin Z$

w.k.T $N(a)=\{x \in G / xa=ax\}$ is a subgroup of G and $a \in N(a)$.

Also $x \in Z \Rightarrow x \in N(a)$

$\therefore Z \subseteq N(a)$.

$a \notin Z \Rightarrow o(Z) < o(N(a))$

$\Rightarrow p < o(N(a))$

By Lagrange's theorem

$o(N(a))$ divides $o(G) = p^2$ i.e. $\frac{o(G)}{o(N(a))}$

and $o(N(a)) > p$.

$\therefore o(G) = p^r \Rightarrow o(N(a)) = o(G)$.

$\Rightarrow N(a) = G \quad (\because N(a) \subseteq G)$

$\Rightarrow x \in N(a) \ \forall x \in G$.

$\Rightarrow a \in Z$.

which is a contradiction.

$\therefore o(Z) = p$ is impossible.

$\therefore o(Z) = p^r$.

In this case we have already proved that G is abelian.

2007 & 10M → A finite integral domain is a field..

2(c)i. Sol^{n}: Let F be the finite I.D.

Let $F = \{a_1, a_2, \ldots a_n\}$ and F contains 'n' distinct elements.

To prove that F is a field

for this we are enough to prove that the non-zero elements of F have x^{ve} inverse.

Let $a \neq 0 \in F$

$\therefore aa_1, aa_2, \ldots aa_n \in F$ (by Closure prop.)

All these elements are distinct.

because: If possible

Let $aa_i = aa_j$; $a_i, a_j \in F$

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

$\Rightarrow a_i - a_j = 0$ ($\because a \neq 0$ & F is an ID i.e, F does not contain zero divisors)

$\Rightarrow a_i = a_j$

This is a contradiction to hypothesis that F contains n distinct elements.

$\therefore$ Our assumption that $aa_i = aa_j$ is wrong.

$\therefore aa_1, aa_2, \ldots aa_n$ are all distinct elements in F which has exactly 'n' elements.

By the pigeon-hole principle, one of these products must be equal to one. ($\because$ F is an ID)

Let $aa_r = 1$ for some $a_r \in F$.

$\therefore a^{-1} = a_r$.

$\therefore$ Every non-zero element of F has x^{ve} inverse.

$\therefore$ F is a field.

IAS-2003

1(a). 2003 TPM → If H is a subgroup of a group G such that $x^2 \in H$ for every $x \in G$, prove that H is a normal subgroup of G.

Sol^n: Let $g \in G$, so that $g^{-1} \in G$.

then $(g^{-1})^2 \in H$ (by hyp).

$\Rightarrow g^{-2} \in H$

and $h^{-1}g^{-2} \in H \ \forall h \in H$. ($\because$ H is subgroup & $h^{-1} \in H$)

Since $gh \in G \Rightarrow (gh)^2 \in H$. (by hypothesis)

Now $(gh)^2 \in H$ and $h^{-1}g^{-2} \in H$

$\Rightarrow (gh)^2 h^{-1}g^{-2} \in H$ ($\because H < G$).

$\Rightarrow ghgh\,h^{-1}g^{-1}g^{-1} \in H$

$\Rightarrow ghge\,g^{-1}g^{-1} \in H$

$\Rightarrow ghgg^{-1}g^{-1} \in H$

$\Rightarrow ghg^{-1} \in H \ \forall g \in G, h \in H$

($\because geg^{-1} = gg^{-1} = e$)

Hence H is normal subgroup of G.

2003 12M.

1(b). Show that the ring $Z[i] = \{a+ib / a, b \in Z, i = \sqrt{-1}\}$ of Gaussian integers is a Euclidean domain.

Sol^n: We know that $Z[i] = \{a+ib / a, b \in Z, i = \sqrt{-1}\}$ of Gaussian integers is an integral domain w.r.t $+^n$ and $\times^n$.

Let us define the mapping $d: Z[i]-\{0\} \to Z$ by $d(x+iy) = x^2+y^2 \ \forall\ x+iy \in Z[i]-\{0\}$. (2)

i.e $d(x+iy) = |x+iy|$
$= x^2+y^2 \ \forall\ x+iy \in Z[i]-\{0\}$ (1).

We have $x \neq 0$ or $y \neq 0$ and hence $x^2+y^2 \geq 1$.

$\therefore d(z) = d(x+iy) \geq 0 \ \forall\ z \in Z[i]-\{0\}$.

Let $z_1, z_2 \in Z[i]-\{0\}$ then we have $z_1 = a+ib$, $z_2 = c+id$ where $a, b, c, d \in Z$ and $a \neq 0$ or $b = 0$; $c \neq 0$ or $d \neq 0$.

$\therefore z_1 z_2 = (ac-bd)+i(ad+bc)$.

Now we have $d(z_1 z_2) = (ac-bd)^2+(ad+bc)^2$
$= (a^2+b^2)(c^2+d^2)$.
$\geq a^2+b^2 = d(z_1)$
$(\because c^2+d^2 \geq 1)$

$\therefore \boxed{d(z_1) \leq d(z_1 \cdot z_2).}$

Now we have

$$\frac{z_1}{z_2} = \frac{a+ib}{c+id}$$
$$= \frac{ac+bd}{c^2+d^2} + i\left[\frac{bc-ad}{c^2+d^2}\right]$$

$\frac{z_1}{z_2} = p+iq$ (say)

where $p = \frac{ac+bd}{c^2+d^2}$; $q = \frac{bc-ad}{c^2+d^2}$ are rational numbers.

Corresponding to the rational numbers p and q, we can find suitable integers p' and q' such that-

$|p'-p| \le \frac{1}{2}$ and $|q'-q| \le \frac{1}{2}$

Let $t = p' + q'i$ then $t \in Z[i]$

and $\frac{z_1}{z_2} = \lambda$, where $\lambda = p + qi$

$\Rightarrow z_1 = \lambda z_2$

$= (\lambda - t) z_2 + t z_2$

$\boxed{z_1 = t z_2 + r}$ where $r = (\lambda - t) z_2$

NOW $z_1, z_2, t \in Z[i]$

$\Rightarrow z_1 - t z_2 \in Z[i]$

$\Rightarrow r \in Z[i]$.

$\therefore \exists\ t, r \in Z[i]$ s.t $z_1 = t z_2 + r$ where

$r = 0$, or

$d(r) = d[(\lambda - t) z_2]$

$= d[(p+qi) - (p'+q'i)] d(z_2)$

$= d[(p-p') + (q-q')i] d(z_2)$.

$= [(p-p')^2 + (q-q')^2] d(z_2)$.

$\le \left[\frac{1}{4} + \frac{1}{4}\right] \cdot d(z_2)$

$= \frac{1}{2} d(z_2)$

$< d(z_2)$.

Thus $\exists\ t, r \in Z[i]$ s.t $z_1 = t z_2 + r$

where $r = 0$ (or) $d(r) < d(z_2)$.

HEAD OFFICE:25/8, Old Rajinder Nagar Market, Delhi-60. (M) 9999197625, 011-45629987. BRANCH OFFICE(DELHI): 105-106, Top Floor, Mukherjee Tower, Mukherjee Nagar, Delhi-9. BRANCH OFFICE(HYDERBAD): H.No. 1-10-237, 2nd Floor, Room No. 202 R.K'S-Kancham's Blue Sapphire Ashok Nagar Hyd-20. (M) 09652351152, 09652661152

2003 Let R be the ring of all the real valued continuous functions on the closed unit interval. Show that $M = \{f \in R \mid f(\tfrac{1}{3}) = 0\}$ is maximal ideal of R.

2(a)i.

Soln: Given that R be the ring of all the real valued continuous functions on the closed unit interval.

i.e., $R = \{f \mid f : [0,1] \longrightarrow \mathbb{R} \text{ is continuous on } [0,1]\}$

where $\mathbb{R}$ denote the set of all real numbers.

Here R is a ring w.r.t compositions:

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

$(fg)(x) = f(x)\,g(x)$ $\forall x \in [0,1]$ and $f, g \in R$

Now we shall show that

$M = \{f \in R \mid f(\tfrac{1}{3}) = 0\}$ is maximal ideal.

first of all we shall show that M is an ideal of R.

Now for this, first of all we observe that M is non-empty because the real valued function 'e' on $[0,1]$ defined by $e(x) = 0$ $\forall x \in [0,1]$.

$\therefore e \in M$.

$\therefore M$ is non-empty subset of R.

Now let $f, g \in M$ then $f(\tfrac{1}{3}) = 0$, $g(\tfrac{1}{3}) = 0$.

we have $(f-g)(\tfrac{1}{3}) = f(\tfrac{1}{3}) - g(\tfrac{1}{3})$

$= 0 - 0$

$= 0$

2(a)ii.

2003 → The union of two ideals of a ring R is an ideal of R if and only if one is contained in the other.

Proof: Let S_1 and S_2 be two ideals of the ring R.

Let $S_1 \subset S_2$ or $S_2 \subset S_1$.

if $S_1 \subset S_2$ then $S_1 \cup S_2 = S_2$ (S_2 is an ideal of R)

if $S_2 \subset S_1$ then $S_1 \cup S_2 = S_1$ (S_1 is an ideal of R)

$\therefore S_1 \cup S_2$ is an ideal of R.

Conversely suppose that $S_1 \cup S_2$ is an ideal of R.

Now we prove that $S_1 \subset S_2$ or $S_2 \subset S_1$

If possible, suppose that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$

since $S_1 \not\subset S_2$

Let $a \in S_1$ but $a \notin S_2$

since $S_2 \not\subset S_1$

Let $b \in S_2$ but $b \notin S_1$

Now $a \in S_1$ and $b \in S_2 \Rightarrow a, b \in S_1 \cup S_2$

$\Rightarrow a-b \in S_1 \cup S_2$ ($\because S_1 \cup S_2$ is an ideal of R)

$\Rightarrow a-b \in S_1$ or $a-b \in S_2$

Now $a \in S_1$ and $a-b \in S_1$

$\Rightarrow a-(a-b) = b \in S_1$ ($\because S_1$ is an ideal of R)

$\therefore$ which is contradiction to the fact $b \notin S_1$.

Now $b \in S_2$, $a-b \in S_2$

$\Rightarrow b+(a-b) \in S_2$ ($\because S_2$ is an ideal of R)

$\Rightarrow a \in S_2$

which is contradiction to fact $a \notin S_2$

$\therefore$ our supposition is wrong.

Hence $S_1 \subset S_2$ or $S_2 \subset S_1$.

$f, g \in M$

$\therefore (M,+)$ is a subgroup of $(R,+)$

Let $f \in M$ and $h \in R$ then $f(\frac{1}{3}) = 0$.

Now we have

$$(fh)(\tfrac{1}{3}) = f(\tfrac{1}{3})\, h(\tfrac{1}{3}) = 0 \cdot h(\tfrac{1}{3}) = 0.$$

$\Rightarrow fh \in M$

Similarly $hf \in M$

$\therefore M$ is an ideal of R.

Finally we shall show that M is a maximal ideal of R.

Let us define a function $\theta : [0,1] \to \mathbb{R}$ such that $\theta(x) = 1 \quad \forall x \in [0,1]$

then θ is a continuous function.

$\therefore \theta \in R$. (wrong)

But $\theta \notin M$ as $\theta(\frac{1}{3}) = 1 \neq 0$

$\therefore M \neq R$.

Let U be any other ideal of R such that $M \subset U \subseteq R$ and $M \neq U$.

we need to show that $U = R$.

Since $M \subset U$ and $M \neq U$,

there exists a function $\lambda \in U$ such that

$\lambda \notin M$ i.e $\lambda(\frac{1}{3}) \neq 0$

Let $\lambda(\frac{1}{3}) = c \neq 0$.

Let us define a function $\rho : [0,1] \to \mathbb{R}$ s.t

$\rho(x) = c \quad \forall x \in [0,1]$.

then $\rho \in R$

Let $\psi = \lambda - \rho$ then $\psi(\frac{1}{3}) = \lambda(\frac{1}{3}) - \rho(\frac{1}{3})$

$= c - c$

$= 0$.

$\Rightarrow \psi \in M$

$\Rightarrow \psi \in U$ as $M \subset U$

i.e $\rho = \lambda - \psi \in U \quad (\because \lambda, \psi \in U)$

If γ be a function from $[0,1]$ to $\mathbb{R}$

s.t $\gamma(x) = \frac{1}{c}$, $(c \neq 0)$

Then $\gamma \in R$.

Now we have

$(\gamma\rho)(x) = \gamma(x)\,\rho(x)$

$= \frac{1}{c} \cdot c$

$= 1$

$= \theta(x) \quad \forall x.$

$\Rightarrow \gamma\rho = \theta$

Since $\rho \in U$, $\therefore \gamma\rho \in U$

we find $\theta \in U$

But θ is the unity of the ring R.

thus U is an ideal containing unity.

$\Rightarrow U = R$

Hence M is maximal ideal of the ring R.

Method(2) that M is maximal ideal can also be proved by using the fundamental theorem of homomorphism.

HEAD OFFICE:25/8, Old Rajinder Nagar Market, Delhi-60. (M) 9999197625, 011-45629987. BRANCH OFFICE(DELHI): 105-106, Top Floor, Mukherjee Tower, Mukherjee Nagar, Delhi-9. BRANCH OFFICE(HYDERBAD): H.No. 1-10-237, 2nd Floor, Room No. 202 R.K'S-Kancham's Blue Sapphire Ashok Nagar Hyd-20. (M) 09652351152,09652661152

Let us define function

$\Theta : R \longrightarrow \mathbb{R}$ such that

$\Theta(f) = f(1/3) \quad \forall f \in R$ ——— (1)

where $\mathbb{R}$ = set of real numbers.

Then Θ is a homomaphism as

$\Theta(f+g) = (f+g)(1/3)$

$= f(1/3) + g(1/3)$

$\boxed{\Theta(f+g) = \Theta(f) + \Theta(g)}$

&

$\Theta(fg) = (fg)(1/3)$

$= f(1/3)\, g(1/3)$

$\boxed{\Theta(fg) = \Theta(f)\, \Theta(g).}$

To check ontoness,

if $r \in \mathbb{R}$ be any element we can define another map $\phi : [0,1] \longrightarrow \mathbb{R}$ s.t

$\phi(x) = r \quad \forall \; x \in [0,1]$.

Then ϕ being constant function will be continuous.

Thus $\phi = R$.

Also $\Theta(\phi) = \phi(1/3)$,

showing that ϕ is pre-image of r under Θ.

i.e Θ is onto.

Thus by fundamental theorem of homomorphism

$$\frac{R}{\ker\phi} \cong \mathbb{R}$$

Now $f \in \ker\phi \Leftrightarrow \phi(f) = 0$

$\Leftrightarrow f(1/3) = 0$

$\Leftrightarrow f \in M.$

$\Rightarrow \ker\phi = M$

Hence $\frac{R}{M} \cong \mathbb{R}$, but $\mathbb{R}$ being a field, $\frac{R}{M}$ will be a field

i.e. M is a maximal ideal of R.

(∵ If R is a commutative ring with unity. An ideal M of R is maximal ideal of $R \Leftrightarrow \frac{R}{M}$ is a field.)

HEAD OFFICE:25/8, Old Rajinder Nagar Market, Delhi-60. (M) 9999197625, 011-45629987. BRANCH OFFICE(DELHI): 105-106, Top Floor, Mukherjee Tower, Mukherjee Nagar, Delhi-9. BRANCH OFFICE(HYDERBAD): H.No. 1-10-237, 2nd Floor, Room No. 202 R.K'S-Kancham's Blue Sapphire Ashok Nagar Hyd-20. (M) 09652351152,09652661152

2003
1992, 96
[15M]

2(b)ii. prove that x^2+x+4 is irreducible over F, the field of integers modulo 11. and prove further that $\frac{F[x]}{x^2+x+4}$ is a field having 121 elements.

Soln: we have

$F = Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$.

Now we prove that the irreducibility of x^2+x+4 over F.

we observe that $f(x) = x^2+x+4$ is not satisfied by the elements of Z_{11}, $f(x) \neq 0$ for each $\alpha \in F$.

consequently x^2+x+4 is not expressible a product of two linear factors in $F[x]$.

Hence x^2+x+4 is irreducible over F.

By another theorem, [Let F be a field. The ideal $A = \langle p(x) \rangle = \{p(x) f(x) : f(x) \in F[x]\}$ in $F[x]$ is a maximal ideal iff $p(x)$ is an irreducible polynomial over F.

and by theorem if R is commutative ring with unity, then an ideal M of R is maximal iff R/M is a field.]

$\frac{F[x]}{\langle x^2+x+4 \rangle}$ is a field.

Any element of this field of the form $f(x) + \langle x^2+x+4 \rangle$, where $f(x) \in F[x]$.

By Division algorithm in $F[x]$, there exist $t(x), r(x) \in F[x]$ such that

$$f(x) = t(x)(x^2+x+4) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg(x^2+x+4) = 2$

we may take $r(x) = \alpha x + \beta \in F[x]$.

Since $t(x)(x^2+x+4) \in \langle x^2+x+4 \rangle$,

therefore $f(x) + \langle x^2+x+4 \rangle = r(x) + \langle x^2+x+4 \rangle$

$$= \alpha x + \beta + \langle x^2+x+4 \rangle. \quad \text{---(1)}$$

In the above expression $\alpha, \beta \in F = Z_{11}$ and $O(Z_{11}) = 11$.

consequently, each of α and β can be selected in 11 ways. Hence, by (1), the number of elements of the field $\frac{F[x]}{\langle x^2+x+4 \rangle}$ is $11^2 = 121$.

IAS-2004

2004 | 12M

1(b). G is an abelian group. If $a, b \in G$ such that $o(a) = m$, $o(b) = n$ and $(m, n) = 1$ then $o(ab) = mn$.

Given that G is an abelian group and $a, b \in G$ such that $o(a) = m$ & $o(b) = n$

Since $o(a) = m$;
i.e, m is the least +ve integer such that $a^m = e$.

and $o(b) = n$
i.e, n is the least +ve integer such that $a^n = e$

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

Let $o(ab) = p$

Now $(ab)^{mn} = a^{mn} b^{mn}$ ($\because$ G is abelian)

$= (a^m)^n (b^n)^m$

$= e^n e^m$

$= e$

$\therefore (ab)^{mn} = e$

$\Rightarrow o(ab) / mn$

i.e, p / mn —— (1)

Also $(ab)^{pn} = [(ab)^p]^n$

$= e^n$

$= e$

and $(ab)^{pn} = a^{pn} b^{pn}$

$= a^{pn}(b^n)^p$

$= a^{pn} \cdot e$

$= a^{pn}$

$\therefore a^{pn} = e \quad (\because (ab)^{pn} = e)$

$\Rightarrow o(a) / pn$

i.e, m / pn.

Since $(m, n) = 1$

$\Rightarrow m / p$. ——(2)

Similarly we can prove n / p ——(3)

from (2) & (3) and $(m, n) = 1$

we have mn / p ——(4)

$\therefore$ from (1) & (4)

we have $mn = p$

$\therefore o(ab) = p = mn$

$= o(a) \cdot o(b)$.

IAS-2005

Theorem
2005 12M

1(a). If M, N are two normal subgroups of G such that $M \cap N = \{e\}$. Then every element of M commutes with every element of N.

Proof: Let $m \in M$ and $n \in N$.

To prove that $nm = mn$.

Since $n \in N$, $\bar{n}^1 \in N$. ($\because N$ is normal subgroup of G)

and $m \in G$

we have $m(\bar{n}^1)\bar{m}^1 \in N$.

Also by closure in N

$$nm\bar{n}^1\bar{m}^1 \in N \quad \text{---} (1)$$

Since M is normal.

$$nm\bar{n}^1 \in M \quad (\because n \in G)$$

By closure in M,

$$nm\bar{n}^1\bar{m}^1 \in M \quad \text{---} (2).$$

From (1) & (2) we have

$$nm\bar{n}^1\bar{m}^1 \in M \cap N$$

But $M \cap N = \{e\}$.

$\therefore nm\bar{n}^1\bar{m}^1 = e$

$\Rightarrow mn\bar{n}^1 = m$

$\Rightarrow nm = mn$

$\therefore$ Every element of M commutes with every element of N.

2005 ISM → If H & K are subgroups of a finite group

2(a)i. G and $o(H) > \sqrt{o(G)}$

$o(K) > \sqrt{o(G)}$ then $o(H \cap K) > 1$

i.e., $H \cap K \neq \{e\}$

proof: Given that H & K are two subgroups of a finite group G.

$\therefore HK \subseteq G$,

$\therefore o(HK) \leq o(G)$

$\Rightarrow o(G) \geq o(HK)$

$$= \frac{o(H) \cdot o(K)}{o(H \cap K)}$$

$$> \frac{\sqrt{o(G)} \cdot \sqrt{o(G)}}{o(H \cap K)} \quad \text{(by hyp)}$$

$$= \frac{o(G)}{o(H \cap K)}$$

$$\therefore o(G) > \frac{o(G)}{o(H \cap K)}$$

$\Rightarrow o(H \cap K) > 1$

Hence $H \cap K \neq \{e\}$

2(a)ii.

Theorem 2005 IBM: If $f: G \to G'$ is an isomorphism (i.e, $o(f(a))$ divides order of 'a', $a \in G$), then the order of $a \in G$ is equal to the order of its image $f(a)$.

Proof: Let $o(a) = n$; $a \in G$ then $a^n = e$. where n is the least +ve integer.

$\therefore f(a^n) = f(e)$

$\Rightarrow f(a \cdot a \cdot \ldots \cdot n \text{ times}) = f(e)$

$\Rightarrow f(a) \cdot f(a) \cdot \ldots \cdot n \text{ times} = f(e)$ ($\because f$ is homo).

$\Rightarrow [f(a)]^n = f(e) = e'$ where e' is identity in G'.

$\Rightarrow o[f(a)] \leq n$ ——①

Let $o[f(a)] = m$ then

$[f(a)]^m = e'$ where m is the least +ve integer

$\Rightarrow f(a) \cdot f(a) \cdot \ldots \cdot m \text{ times} = e'$

$\Rightarrow f(a \cdot a \cdot \ldots \cdot m \text{ times}) = f(e)$

$\Rightarrow f(a^m) = f(e)$

$\Rightarrow a^m = e$ ($\because f$ is 1-1)

$\Rightarrow o(a) \leq m$ ——②

from ① & ② we have

$m \leq n$ & $n \leq m$.

$\Rightarrow m = n$

$\Rightarrow o[f(a)] = o(a)$.

IAS-2006

1(a). Let S be the set of all real numbers except -1. Define $*$ on S by $a*b = a+b+ab$

a) Show that $*$ gives a binary operation on S.

b) Show that $(S, *)$ is a group.

c) Find the solution of the equation $2*x*3=7$ in S.

Soln:

(a) Since S is the set of all real numbers except -1 and $*$ is an operation defined in $S=\mathbb{R}-\{-1\}$ such that

$a*b = a+b+ab \quad \forall a,b \in S$

when $a,b \in S$

$a*b = a+b+ab \in S$.

$\therefore a*b \in S$

$\therefore *$ is a b-o on S.

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

$\forall a,b \in S$.

If possible let $a*b=-1$

$\Rightarrow a+b+ab=-1$

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

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

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

$\Rightarrow a=-1$ or $b=-1$ (1)

clearly which is contradiction to hypo. that $a \neq -1, b \neq -1$ $\forall a,b \in S$.

(b) (i) Closure proof:

$\forall a,b \in S$

$a*b = a+b+ab \in S$ by (1)

$\therefore S$ is closed under $*$.

(ii) Associative prop:

$\forall a, b, c \in S \Rightarrow (a * b) * c = (a+b+ab) * c$

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

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

Similarly $a*(b*c) = a+b+c+ab+bc+ca+abc$.

$\therefore (a*b)*c = a*(b*c)$.

$\therefore$ Associative law holds.

(iii) Existence of left Identity:

Let $a \in S$, $e \in S$ then $e*a = a$

Now $e*a = a$

$\Rightarrow e+a+ea = a$

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

$\Rightarrow e = 0 \in S \ (\because a \neq -1)$

$\therefore e*a = 0*a$

$= 0+a+0(a)$

$= a$

$\therefore \forall a \in S \ \exists \ 0 \in S$ such that $0*a = a$.

$\therefore 0$ is the left identity in S.

(iv) Existence of left inverse:

Let $a \in S$, $b \in S$ then $b*a = e$

Now $b*a = e$

$\Rightarrow b+a+ba = 0 \quad (\because e = 0)$

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

$\Rightarrow b = \frac{-a}{1+a} \in S \ (\because a \neq -1)$

$\therefore b*a = \frac{-a}{1+a} * a$

$$= \frac{-a}{1+a} + a + \left(\frac{-a}{1+a}\right) a$$

$$= \frac{-a}{1+a} + a - \frac{a^2}{1+a}$$

$$= \frac{-a + a(1+a) - a^2}{1+a}$$

$$= 0$$

for each $a \in S$ $\exists$ $b = \frac{-a}{1+a} \in S$ such that $\frac{-a}{1+a} * a = 0$

$\therefore b = \frac{-a}{1+a}$ is left inverse of a in S w.r.t $*$.

$\therefore (S, *)$ is a group.

(c) $2 * x * 3 = 7$

$\Rightarrow (2 + x + 2x) * 3 = 7$ by (1)

$\Rightarrow (2 + 3x) * 3 = 7$

$\Rightarrow (2+3x) + 3 + (2+3x)\,3 = 7$ by (1)

$\Rightarrow 5 + 3x + 6 + 9x = 7$

$\Rightarrow 11 + 12x = 7$

$\Rightarrow 12x = -4$

$\Rightarrow x = -\frac{1}{3} \in S$

Now $2 * \left(-\frac{1}{3}\right) * 3 = \left[2 + \left(-\frac{1}{3}\right) + 2\left(-\frac{1}{3}\right)\right] * 3$ by (1)

$= \left(\frac{5}{3} - \frac{2}{3}\right) * 3$

$= 1 * 3$

$= 1 + 3 + 3$

$= 7$

$\therefore x = -1/3$ is a solution of the equation $2 * x * 3 = 7$ in S

2006 1.0M → Let G be the set of all those ordered pairs (a, b) of real numbers for which $a \neq 0$ and define in G, an operation $\otimes$ as follows:

2(a)ii.

2006. 10 M → Let G be the set of all those ordered pairs (a,b) of real numbers for which $a \neq 0$ and define in G, an operation $\otimes$ as follows:

$$(a,b) \otimes (c,d) = (ac, bc+d)$$

Examine whether G is a group w.r.t the operation $\otimes$. If it is a group, is G abelian?

Soln: Let $G = \{(a,b) / a \neq 0, b \in \mathbb{R}\}$ and an operation $\otimes$ defined by

$$(a,b) \otimes (c,d) = (ac, bc+d) \quad \text{---} (1)$$

(i) Closure prop:

$\forall (a,b), (c,d) \in G$; $a, b, c, d \in \mathbb{R}$ & $a \neq 0$, $c \neq 0$.

$\Rightarrow (a,b) \otimes (c,d) = (ac, bc+d) \in G$

($\because a \neq 0, c \neq 0 \Rightarrow ac \neq 0$ & $bc+d \in \mathbb{R}$)

$\therefore G$ is closed under $\otimes$.

(ii) Asso. prop:

$\forall (a,b), (c,d), (e,f) \in G$ where $a, b, c, d, e, f \in \mathbb{R}$ & $a, c, e \neq 0$

$$\Rightarrow [(a,b) \otimes (c,d)] \otimes (e,f) = (ac, bc+d) \otimes (e,f) \quad \text{by (1)}$$

$$= (ace, (bc+d)e+f)$$

$$= (ace, bce+de+f)$$

Similarly $(a,b) \otimes [(c,d) \otimes (e,f)] = (ace, bce+de+f)$

$\therefore$ Asso. law holds.

(iii) Existence of left identity:

Let $(a,b) \in G$ where $a \neq 0$

Let $(x,y) \in G$, where $x \neq 0$ such that

$$(x,y) \otimes (a,b) = (a,b)$$

Now $(x,y) \otimes (a,b) = (a,b)$

$\Rightarrow (xa, ya+b) = (a,b)$ by (1)

$\Rightarrow xa = a$ & $ya+b = b$

$\Rightarrow x=1$ & $ya=0$

$\Rightarrow y=0 \quad (\because a\neq 0)$

$\therefore x=1$ & $y=0$

$\therefore (1,0)\in G$ such that $(1,0)\otimes(a,b)=(a,b)$

$\therefore (1,0)$ is the left identity in G.

(iv) Existence of left inverse:

Let $(a,b)\in G$ where $a\neq 0$

Let $(x,y)\in G$ where $x\neq 0$ such that

$(x,y)\otimes(a,b)=(1,0)$

Now $(x,y)\otimes(a,b)=(1,0)$

$\Rightarrow (xa, ya+b)=(1,0)$

$\Rightarrow xa=1 \; ; \; ya+b=0$

$\Rightarrow x=\frac{1}{a} \; ; \; y=-\frac{b}{a} \quad (\because a\neq 0)$

$\therefore (x,y)=\left(\frac{1}{a},-\frac{b}{a}\right)\in G$ such that

$\left(\frac{1}{a},-\frac{b}{a}\right)\otimes(a,b)=(1,0)$

$\therefore \left(\frac{1}{a},-\frac{b}{a}\right)$ is the left inverse of (a,b)

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

(v) Comm. prop:

$\forall (a,b),(c,d)\in G \; ; \; a,b,c,d\in R \; ; \; a\neq 0, c\neq 0$

$(a,b)\otimes(c,d)=(ac,bc+d)$ (by (i))

and: $(c,d)\otimes(a,b)=(ca,da+b)$

$\therefore (a,b)\otimes(c,d)\neq(c,d)\otimes(a,b)$

$\therefore G$ is not commutative under $\otimes$

$\therefore$ the group $(G,\otimes)$ is not an abelian group. ✓

2006 Show that $\mathbb{Z}[\sqrt{2}] = \{m+n\sqrt{2} : m, n \in \mathbb{Z}\}$ is a Euclidean domain.

2(b).

Soln: We know that $\mathbb{Z}[\sqrt{2}]$ is an integral domain with unity $1 = 1+\sqrt{2}\cdot 0$.

Let us define a mapping

$d : \mathbb{Z}[\sqrt{2}] - \{0\} \longrightarrow \mathbb{Z}$ by

$d(m+n\sqrt{2}) = |m^2-2n^2| \quad \forall\ m+n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]-\{0\}$.

we have $m \neq 0$ or $n \neq 0$.

$\therefore d(m+n\sqrt{2})$ is a +ve integer.

for each $m+n\sqrt{3} \in \mathbb{Z}[\sqrt{2}]-\{0\}$.

$\therefore d(m+n\sqrt{2}) \geq 0$.

Now let: $a = m+n\sqrt{2} \neq 0$, $b = m_1+n_1\sqrt{2} \neq 0$ in $\mathbb{Z}[\sqrt{2}]$;

$m \neq 0$ or $n \neq 0$; $m_1 \neq 0$ or $n_1 \neq 0$.

Then we have

$ab = (mm_1+2nn_1) + (mn_1+nm_1)\sqrt{2}$

and $d(ab) = |(mm_1+2nn_1)^2 - 2(mn_1+nm_1)^2|$

(by defn)

$= |m^2m_1^2 + 4n^2n_1^2 - 2(m^2n_1^2+n^2m_1^2)|$

$= |(m^2-2n^2)(m_1^2-2n_1^2)|$

$= |m^2-2n^2|\,|m_1^2-2n_1^2|$.

$\geq |m^2-2n^2| \quad (\because |m_1^2-2n_1^2| \geq 1)$

$= d(a)$.

$\therefore\ d(a) \le d(ab)$,

Now we have .....

$$\frac{a}{b} = \frac{m+n\sqrt{2}}{m_1+n_1\sqrt{2}} = \frac{(m+n\sqrt{2})(m_1-n_1\sqrt{2})}{(m_1+n_1\sqrt{2})(m_1-n_1\sqrt{2})}$$

$$= \left(\frac{mm_1-2nn_1}{m_1^2-2n_1^2}\right) + \left(\frac{m_1n-mn_1}{m_1^2-2n_1^2}\right)\sqrt{2}$$

$$= p+q\sqrt{2}$$

where $p = \frac{mm_1-2nn_1}{m_1^2-2n_1^2}$ & $q = \frac{m_1n-mn_1}{m_1^2-2n_1^2}$ are rational numbers.

corresponding to the rational numbers p and q, we can find two integers p' and q' such that $|p'-p| \le \frac{1}{2}$ and $|q'-q| \le \frac{1}{2}$

Let $t = p'+q'\sqrt{2}$.

Then $t \in \mathbb{Z}[\sqrt{2}]$

we have $\frac{a}{b} = \lambda$, where $\lambda = p+q\sqrt{2}$

$\Rightarrow a = \lambda b = (\lambda - t)b + tb$

$= tb + r$, where $r = (\lambda - t)b$

Now $a, b, t \in \mathbb{Z}[\sqrt{2}]$

$\Rightarrow a - tb \in \mathbb{Z}[\sqrt{2}]$

$\Rightarrow r \in \mathbb{Z}[\sqrt{2}]$

$\therefore \exists\ t, r \in \mathbb{Z}[\sqrt{2}]$ such that

$a = tb + r$; where $r = 0$ (or)

$$d(r) = d\{(a-b)b\}$$

$$= d\{(p+q\sqrt{2}) - (p'+q'\sqrt{2})\}\, d(b)$$

$$= d\{(p-p') + (q-q')\sqrt{2}\}\, d(b)$$

$$= |(p-p')^2 - 2(q-q')^2|\, d(b)$$

$$\leq |(p-p')^2 + 2(q-q')^2|\, d(b)$$

$$\leq \left(\frac{1}{4} + \frac{2}{4}\right) d(b)$$

$$= \frac{3}{4}\, d(b)$$

$$< d(b).$$

$\therefore \mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

IAS-2007

1(a).

→ If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$ find $o(b)$.

Sol^n: we have

$$(aba^{-1})^2 = (aba^{-1})aba^{-1}$$
$$= ab(a^{-1}a)ba^{-1}$$
$$= abeba^{-1}$$
$$= ab^2a^{-1}$$
$$= aababa^{-1}a^{-1} \quad (\because aba^{-1} = b^2)$$
$$= a^2ba^{-2}$$

Now $(aba^{-1})^4 = \{(aba^{-1})^2\}^2$

$$= (a^2ba^{-2})^2$$
$$= a^2ba^{-2} \cdot a^2ba^{-2}$$
$$= a^2b(a^{-2}a^2)ba^{-2}$$
$$= a^2beba^{-2}$$
$$= a^2b^2a^{-2}$$
$$= a^2ababa^{-1}a^{-2}$$
$$= a^3ba^{-3}$$

Now $(aba^{-1})^8 = \{(aba^{-1})^4\}^2$

$$= (a^3ba^{-3})^2$$
$$= a^3ba^{-3} \cdot a^3ba^{-3}$$
$$= a^3b(a^{-3}a^3)ba^{-3}$$
$$= a^3b^2a^{-3}$$
$$= a^3ababa^{-1}a^{-3}$$
$$= a^4ba^{-4}$$

Now $(aba^{-1})^{16} = \{(aba^{-1})^8\}^2$

$$= (a^4ba^{-4})^2$$
$$= a^4ba^{-4} \cdot a^4ba^{-4}$$
$$= a^4b(a^{-4}a^4)ba^{-4}$$
$$= a^4b^2a^{-4}$$
$$= a^4ababa^{-1}a^{-4}$$
$$= a^5ba^{-5}.$$

$= ebe^{-1} \quad (\because a^5 = e)$

$= be$

$= b$

$\therefore (aba^{-1})^{16} = b$

$\Rightarrow (b^2)^{16} = b \quad (\because aba^{-1} = b^2)$

$\Rightarrow b^{32} = b$

$\Rightarrow b^{32} = b$

$\Rightarrow b^{31} = e.$

Since $b^m = e \Rightarrow o(b)/m$ i.e $^{?}/_{an}$

$\therefore o(b)/31$

But 31 is prime integer

$\therefore o(b) = 1$ or 31

if $b = e$ then $o(b) = 1$

if $b \neq e$ then $o(b) = 31$

2007 U4 → Let $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in Z\right\}$. show that R is a ring under matrix addition and multiplication.

1(b). Let $A=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} / a,b \in Z\right\}$. Then show that A is a left ideal of R but not a right ideal of R.

Sol'n: Let $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in Z\right\}$

Now we show that R is a ring w.r.t $+^n$ and $\times^n$.

(i) Closure Prop:

$\forall\ A,B \in R \Rightarrow A+B \in R$

$\therefore$ R is closed under $+^n$.

(ii) Associative Prop: $\forall\ A,B,C \in R \Rightarrow (A+B)+C = A+(B+C)$

$\therefore$ R is associative under $+^n$.

(iii) Existence of left identity:

Let $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$; $a,b,c,d \in Z$

$O=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$, $0 \in Z$ then

$$O+A=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}+\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

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

$$=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (\because 0,a \in Z \Rightarrow 0+a=a)$$

$$=A$$

$\therefore \forall\ A \in R$, $\exists\ 0$ (null matrix) $\in R$ such that $0+A=A$.

$\therefore$ Identity prop. is satisfied w.r.t $+^n$.

Here 0 (null matrix) is the left identity in R

(iv) Existence of left Inverse:

Let $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$, $a,b,c,d \in Z$

HEAD OFFICE:25/8, Old Rajinder Nagar Market, Delhi-60. (M) 9999197625, 011-45629987. BRANCH OFFICE(DELHI): 105-106, Top Floor, Mukherjee Tower, Mukherjee Nagar, Delhi-9. BRANCH OFFICE(HYDERBAD): H.No. 1-10-237, 2nd Floor, Room No. 202 R.K'S-Kancham's Blue Sapphire Ashok Nagar Hyd-20. (M) 09652351152,09652661152

$B = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in R$, $-a, -b, -c, -d \in Z$ then

$$B+A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a+a & -b+b \\ -c+c & -d+d \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (\because -a+a = -b+b = -c+c = -d+d = 0)$$

$$= 0$$

$\therefore \forall A \in R, \exists B = -A \in R$ such that

$B+A = 0$

$\therefore B = -A$ is left inverse of A in R w.r.t $+$.

(V) Commutative Prop:

$\forall A, B \in R \Rightarrow A+B = B+A$

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

(III) (i) Closure Prop:

$\forall A, B \in R \Rightarrow A \cdot B \in R$

(ii) Associative Prop:

$\forall A, B, C \in R \Rightarrow (A \cdot B)C = A(B \cdot C)$

$\therefore (R, \cdot)$ is a semigroup.

(iii) Distributive laws:

$\forall A, B, C \in R$

$\Rightarrow A \cdot (B+C) = A \cdot B + A \cdot C$

R satisfies DL

$\therefore (R, +, \cdot)$ is a ring.

Given that $A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\} \subseteq R$

Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in A$

$\therefore A \neq \phi$.

Now let $A_1, A_2 \in A$ choosing $A_1 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$

then $A_1 - A_2 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ $a_1, b_1, a_2, b_2, 0 \in Z$

$$= \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in A \quad (\because a_1 - a_2, b_1 - b_2 \in Z)$$

$\therefore A$ is a subgroup of R.

Let $A_1 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \in A$, $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$

$a_1, b_1 \in Z$ $\quad a, b, c, d \in Z$

then $= \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} = \begin{bmatrix} aa_1+bb_1 & 0 \\ ca_1+db_1 & 0 \end{bmatrix}$

$\in A \quad (\because aa_1+bb_1, ca_1+db_1 \in Z)$.

$\therefore A$ is the left ideal in R.

Now $A_1B = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$= \begin{bmatrix} a_1a & a_1b \\ b_1a & b_1b \end{bmatrix} \notin A$

$\therefore A$ is not the right ideal in R