Hence $p|ab \Rightarrow p|a$ or $p|b$

That is p is a prime element in D.

Hence it proofed the theorem.

P-26 X → Ex. 5

Thm: Prove that every irreducible element of a principal ideal domain is prime.

Proof: Let D be a principal ideal domain and p an irreducible element in D.

Then $p \neq 0$ and p is not a unit.

Let $p \mid ab$ such that p is not a divisor of a

Let us denote by (p) and (b) the principal ideals generated by p and b respectively.

Then $(p) + (b)$ is also a principal ideal of D generated by an element $d \in D$.

Then $(p) + (b) = (d)$

consequently, $(p) \subseteq (d)$ and therefore $p \in (d)$

So, $p = dx$ for some $x \in D$.

But p being an irreducible element, so either d or x is unit.

Now if d is a unit, then

$$(p) + (b) = (d) \Rightarrow px_1 + bx_2 = 1 \text{ for some } x_1, x_2$$

$$\Rightarrow apx_1 + abx_2 = a$$

$$\Rightarrow p \mid a \quad [\because p \mid ab]$$

This contradicts our assumption.

similarly if $p \mid ab$ & p is not a divisor of b then there will be a contradiction.

Units in integral domain:

Let D be an integral domain. Then each such element of D, which is a divisor of every non-zero element of D is called a unit in D.

Th^m: Prove that in an integral domain every prime element is irreducible.

Proof: Let D be an integral domain and p is a prime element in D. Then p is not a unit.

Now let $p = ab$, for some $a, b \in D$

Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ [$\because$ p is prime]

Now $p \mid a$, then $a = pd$ for some $d \in D$

$\therefore p = ab = (pd)b = p(db)$

$\Rightarrow p = p(db)$

$\Rightarrow db = 1$

This shows that b is a unit.

Similarly, $p \mid b \Rightarrow a$ is a unit.

Thus, $p = ab \Rightarrow$ one of a & b must be a unit

Hence p is irreducible.

15/11/23

⊛ Unique factorisation Polynomial

P-253

Thm → unique factorisation theorem for polynomials over

⊛ Irreducible element & Prime element

Thm → ① In an integral domain every prime element is irreducible.

② Every irreducible element of a principal ide domain is prime.

29.11.202

Irreducible Polynomial

A non-zero polynomial $f(x)$ in the polynomial domain $F[x]$ of a field F is said to be an ir polynomial, if $f(x)$ has no proper divisors.

Irreducible Elements:

Let R be a commutative ring with unity & n zero element $p \in R$ is said to be irreducible if $p = ab \Rightarrow$ one of a and b must be a uni

Prime Elements:

Let R be a commutative rin with unity. A non-zero element $p \in R$ is said to be a prime element of R. if p is not a unit and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ $\forall a, b \in R$.

$\Rightarrow r \in S \quad [\because a = bq + r]$

$\Rightarrow r = 0 \quad [\because d(b)$ being least, so if $d(r) \neq d(b)]$

Thus $a = bq$ for some $q \in R$

That is, each element a of S is generated by b

So, $S = \langle b \rangle$

Thus every ideal of R is a principal ideal.

Let $R = \langle c \rangle$

Then each element of R is of the form

cx for some $x \in R$.

That is $c = cx$ for some $x \in R$

Let $a \in R$ be any element

Then $\exists\ t_1 \in R$ s.t. $a = t_1 c$

But $a = t_1 c$

$\Rightarrow at = (t_1 c)t$

$\Rightarrow at = t_1 (ct)$

$\Rightarrow at = t_1 c \quad [\because ct = c]$

$\Rightarrow at = a \quad [\because t_1 c = a]$

$\Rightarrow t$ is the unity element of R

Hence R is a principal ideal ring.

Proof: Let R be an Euclidean ring and Let d be the corresponding Euclidean valu

Let S be any ideal of R.

If $S = \{0\}$, then S is a principal ideal generated by 0.

Let S be a non-zero ideal of R, so that it contains at least one non-zero element of R.

Consider the set $T = \{d(a) : a \in R \ \& \ a \neq 0\}$

Let T has least element k s.t. $k = d(b)$ for some non-zero element $b \in S$.

we have to show that $S = \langle b \rangle$

Let a be a non-zero arbitrary of S, then by Euclidean valuation $\exists\ q, r \in R$ where $r = 0$ or $d(r) < d(b)$

$a = bq + r$,

Since $b \in S$ and $q \in R \Rightarrow bq \in S$ [$\because S$ is an ideal]

again $a \in S$, $bq \in S$ $a - bq \in S$ ["]

(i) $a=0 \Rightarrow |a|=0 \Rightarrow d(a)=0$

(ii) If a and b two non-zero elements of $\mathbb{Z}$, then

$$d(ab) = |ab| = |a|\cdot|b| \geq |a| = d(a)$$

$$\Rightarrow d(a) \leq d(ab) \quad \forall \text{ non-zero } a, b \in \mathbb{Z}$$

(iii) If a and b two non-zero elements in $\mathbb{Z}$, then by division algorithm $\exists$ integers q and r in $\mathbb{Z}$ s.t. $a = bq + r$, where either $r=0$ or $0 < r < |b|$

that is, either $r=0$ or $|r| < |b|$

" " , " $r=0$ or $d(r) < d(b)$

Thus d is an Euclidean valuation.

consequently $\mathbb{Z}$ is an Euclidean ring.

Thm: Prove that every field is an Euclidean ring.

$d : F \to W$ s.t.

$d(a) = 0 \quad \forall a \in F$

Thm: Prove that every ~~field~~ Euclidean ring is a principal ideal ring.

21.11.2023

* Euclidean Ring:

Let R be a commutating ring without zero divisors. Then R is said to be an Euclidean ring if there exists a mapping d of R into w of whole numbers in such a way that,

(1) $a=0 \Rightarrow d(a)=0$

(2) $d(a) \leq d(ab)$. $\forall$ non zero elements $a, b \in R$

(3) Corresponding to each pair of non-zero elements $a, b \in R$

$\exists$ elements q and $r \in R$, s.t.

$a=bq+r$ where either $r=0$ or $d(r) < d(b)$

Then d is called the Euclidean valuation a the property (III) is called Euclidean abor

Thm: Proove that $\mathbb{Z}$, the ring of all integers is a Euclidean ring.

Proof: Let us define a mapping

$d: \mathbb{Z} \to W$, where $W = \mathbb{Z}^+ \cup \{0\}$

s.t. $d(a) = |a|$, $\forall a \in \mathbb{Z}$

Then d satisfies the following properties.

$2 = g_1(x)\, g(x)$ and $x = g_2(x) \cdot g(x)$

$\Rightarrow 2x = g_1(x)\, g(x)$ and $2x = 2g_2(x) \cdot g(x)$

So, $[g_1(x) \cdot g(x)]\, x = 2g_2(x) \cdot g(x)$ [$\because \mathbb{Z}[x]$ is commutative]

$\therefore 2g_2(x) = x g_1(x)$

It follows that each coefficient of $g_1(x)$ is an even integer. So $g_1(x) = 2h(x)$ for some $h(x) \in \mathbb{Z}[x]$

$\therefore 2 = 2h(x) \cdot g(x)$ or $h(x) \cdot g(x) = 1$

This shows that $1 \in (g(x))$, that is $1 \in S$

But this is not possible, since $1 \in S \Rightarrow 1 = 2f(x) + g(x)$, for some $f(x)$ & $g(x) \in \mathbb{Z}[x]$

$\Rightarrow 1 = 2[a_0 + a_1(x) + \cdots + x^n(b_0 + b_1 x + \cdots)]$

$\Rightarrow 1 = 2q_0$ for some integer a_0, which is a contradiction

$\Rightarrow r(x) \in S \quad [\because f(x) = q(x) \cdot g(x) = r(x)]$

But when $\deg r(x) < \deg g(x)$

$r(x) \notin S$, since $g(x)$ is a non-zero ideal of lowest degree in S.

So, $r(x) \in S \Rightarrow r(x) = 0$

$\therefore f(x) = q(x) \cdot g(x)$

Thus S is an ideal generated by $g(x)$

That is $S = (g(x))$

So, S is a principal ideal generated

Hence $F[x]$ is a principal ideal ring.

Soln of the Problem:

Let $S = \{2f_1(x) + 2f_2(x) : f_1(x), f$

be the ideal of $\mathbb{Z}[x]$ generated by 2 and

of $\mathbb{Z}[x]$ and if possible let S be

principal ideal of $\mathbb{Z}[x]$.

Then $\exists$ a non-zero ideal $g(x)$ in $\mathbb{Z}[x]$ s.t.

$S = (g(x))$

In this case, $2 \in S, 2 \in S \Rightarrow 2 \in (g(x))$ and

and therefore $\exists\ g_1(x), g_2(x) \in \mathbb{Z}[x]$ s.t.

and so $q(x) = 0$ and $r(x) = f(x)$ are the polynomials in $F[x]$ s.t.

$$f(x) = q(x) \cdot g(x) + r(x)$$ where $\deg(r(x)) < \deg(g(x))$

Mid → 14/11/2023

Syllabus → Polynomial ring পর্যন্ত।

08-11-2023

**Thm: Prove that a polynomial ring over a arbitrary field is a principal ideal ring.

**Problem: Show that the polynomial ring $Z[x]$ is not a principal ideal ring.

Proof: Let $F[x]$ be a polynomial ring over a arbitrary field F.

Let S be an arbitrary non-zero ideal of $F[x]$ and $g(x)$ be a non-zero poly of lowest degree in S.

Let $f(x) \in S$ be any polynomial.

Then by division algorithm $\exists\ q(x), r(x) \in F[x]$ s.t. $f(x) = q(x) \cdot g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Note, S being an ideal,

$g(x) \in S,\ q(x) \in F[x] \Rightarrow g(x) \cdot q(x) \in S$

$\Rightarrow f(x) - g(x) \cdot q(x) \in S$

Hence no non-zero polynomial of degree greater than zero, in $F[x]$ possess its multiplicative inverse.

Hence $F[x]$ is not a field.

Division Algorithm

Statement: Let $f(x)$ be any polynomial and $g(x)$ a non-zero polynomial in the polynomial domain $F[x]$ over a field F. Then $\exists$ unique polynomials $q(x)$ and $r(x)$ in $F[x]$ s.t. $f(x) = q(x) \cdot g(x) + r(x)$ where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

Proof: If $f(x) = 0$ then $\exists$ $q(x)$, $r(x) \in F(x)$ s.t. $q(x) = 0$, $r(x) = 0$ and $f(x) = q(x) \cdot g(x) + r(x)$ where $r(x)$

Let $f(x) \neq 0$ and $g(x) \neq 0$ and let,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m, \quad a_m \neq 0.$$

and $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n, \quad b_n \neq 0.$

Thus $\deg(f(x)) = m$ and $\deg(g(x)) = n$

Case-I: when $\deg(f(x)) < \deg(g(x))$ that is $m < n$

then, $f(x) = 0 \cdot g(x) + f(x)$, where $\deg(f(x)) < \deg(g(x))$

17.10.2023

$\#\, f(x) \in F[x]$ s.t. $f(x) \neq 0$

$\exists\, g(x) \in F[x]$ s.t. $f(x) \cdot g(x) = I(x)$.

Thm If F is a field, then the set $F[x]$ of all polynomials over F is an integral domain but $F[x]$ is not a field.

Proof: We know every field is an integral domain since F is a field, so F is an integral domain and consequently $F[x]$, the set of all polynomials in x an integral domain.

Now we have prove that $F[x]$ is not a field.

Let us consider a polynomial $f(x) \in F[x]$ such that $\deg[f(x)] > 0$

Then the product of $f(x)$ with any non-zero polynomial $g(x) \in F[x]$ can never be the unity element $I(x) = 1 \cdot x^0$,

Since F being an integral domain,

$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)) > 0$ [$\because \deg(f(x)) > 0$ & $\deg(g(x)) > 0$]

& the degree of $I(x)$ is 0.

Polynomial Rings:

Let R be an arbitrary ring and R[x] be the set of all polynomials over R. Then R[x] forms a ring with the operations polynomial addition and polynomial multiplication. The ring R[x] is called the polynomial over R.

Thm-1 Let R be an arbitrary ring and R[x] be the set of all polynomials over R. Then prove that R[x] forms a ring with the operation polynomial of addition &

Thm-2 Let R be an integral domain and R[x] be the set of all polynomials over R. Then prove that R[x] is also an integral domain with the operations of polynomial addition and polynomial multiplication.

Thm-3 (P-247 Thm 2)

If F is a field, then the set of all polynomials F[x] is an integral domain over F but the polynomial domain F[x] is not a field.

15.10.2023

R is a ring

$a_0, a_1, a_2, \ldots, a_n, \ldots \in R$

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots \in R[x]$ Polynomial

$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m + \cdots \in K[x]$

$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$

$f(x) \cdot g(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots$

$= c_0 + c_1 x + c_2 x^2 + \cdots$

where, $c_i = \sum_{i+k=i} a_i b_k$

(Page-241) $0(x) = 0 + 0x + \cdots$

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots \in R[x]$

$(-a_0) + (-a_1)x + (-a_2)x^2 + \cdots + (-a_n)x^n + \cdots \in R[x]$

$= -(a_0 + a_1 x + a_2 x^2 + \cdots) \in R[x]$

$= -f(x) \in R[x]$

$\therefore f(x) + (-f(x))$

$= (a_0 + (-a_0)) + (a_1 + (-a_1))x + \cdots$

$= 0 + 0x + \cdots$

$= 0(x)$

$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$

$= (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 + \cdots$

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

Now, consider the mapping,

$f: T \to \frac{(S+T)}{S} : f(a) = S+a \quad \forall\, a \in T.$

The mapping f preserves both the compositions,

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

and
$$f(ab) = (S+ab)$$
$$= (S+a)(S+b)$$
$$= f(a) \cdot f(b) \quad \forall\, a, b \in T$$

Also, f is onto, since

$(S+a) \in (S+T)/S \Rightarrow a \in S+T$

$\Rightarrow a \in s+t$ for some $s \in S$ & $t \in$

$\Rightarrow (S+a) = (S+s) + (S+t)$

$\Rightarrow (S+a) = S + (S+t) = (S+t)$ [$\because s \in S \Rightarrow$

$\Rightarrow (S+a) = f(t)$ where $t \in T$

Thus $(S+T)/S$ is the homomorphic image of T under

Also $\ker f = \{t \in T : f(t) = S$, the zero of $(S+T)/S\}$

$= \{t \in T : S+t = S\}$

$= S \cap T$ [$\because S+t = S \Rightarrow t \in S$]

By the first law of isomorphism, we have

$(S+T)/S \cong T/(S \cap T)$.

Now, $\ker f = \{ s+a : f(s+a) = T \text{ the zero of } R/T \}$

$= \{ s+a : T+a = T \}$

$= \{ s+a : a \in T \}$

$= T/S$

Hence by the first law of isomorphism, we have

$$R/T \cong \frac{R/S}{T/S}.$$

(Third Law → ~~बाएगा तीसरा नियम~~)

Statement: If S is an ideal of a ring R and T is any subring of R, then $\frac{S+T}{S} \cong \frac{T}{S \cap T}$

Proof: S is an ideal & T is a subring of R

So $S+T$ be elements of $S+T$. Then

Let (t_1+a_1) & (t_2+a_2)

$$(t_1+a_1)-(t_2+a_2) = \underbrace{(t_1-t_2)}_{\in T} + \underbrace{(a_1-a_2)}_{\in S}$$

$$\& \quad (t_1+a_1)(t_2+a_2) = \underbrace{t_1 t_2}_{\in T} + \underbrace{t_1 a_2 + t_2 a_1 + a_1 a_2}_{\in S}$$

Hence $S+T$ is a subring of R.

Now, S is an ideal of $S+T$.

So, $(S+T)/S$ is a quotient ring.

$\Rightarrow (S+a)(s+b) \in T/S$ & $(S+b)(S+a) \in T/S$

$\Rightarrow T/S$ is an ideal of R/S.

Thus $\frac{R/S}{T/S}$ is a quotient ring.

Now let us consider a mapping

$f: R/S \to R/T$ such that,

$f(S+a) = T+a$, $\forall\, a \in R$

Then $f[(S+a)+(S+b)] = f[S+(a+b)] = T+(a+b)$

$= (T+a)+(T+b)$

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

Similarly, $f[(S+a)(S+b)] = f[S+(ab)] = T+(ab)$

$= (T+a)(T+b)$

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

Thus f is homomorphism.

Also for each $T+a \in R/T$ $\exists$ an element $S+a \in R/S$ such that $f(S+a) = T+a$

so f is onto.

$\therefore f$ is homomorphism of R/S onto R/T

That is, $R/S \simeq R/T$

11.10.2023

2nd Law of isomorphism:

Statement: If S is an ideal of a ring R and T is an ideal of R containing S then $\frac{R}{T} \cong \frac{R/S}{T/S}$

Proof: Since S and T are ideals of R

So, $\frac{R}{S}$, $\frac{R}{T}$ are quotient rings.

Now $S \subset T \subset R$, So, S is a subring of T.

Since $r \in T$, $s \in S \Rightarrow rs \in S$ and $sr \in S$

$\Rightarrow S$ is an ideal of T.

Thus T/S is a quotient ring.

Since $S+a \in T/S \Rightarrow a \in T \Rightarrow a \in R$

$\Rightarrow S+a \in R/S$

So, $T/S \subset R/S$

Again, $S+a \in T/S$, $S+b \in T/S \Rightarrow a \in T, b \in T$

$\Rightarrow a-b \in T, ab \in T$

$\Rightarrow a-b \in R, ab \in R$

$\Rightarrow S+(a-b) \in R/S, S+ab \in R/S$

$\Rightarrow (S+a)-(S+b) \in R/S, (S+a)(S+b) \in R/S$

$\Rightarrow T/S$ is a subring of R/S.

∵ T is an ideal of R ⇒ T is a subring of R

Also, $S+a \in T/S$, $S+r \in R/S \Rightarrow a \in T, r \in R$

$\Rightarrow ar \in T, ra \in T$

$\Rightarrow S+ar \in T/S$ and $S+ra \in T/S$

and $\phi[(s+a)(s+b)] = \phi[s+ab]$

$= f(ab)$

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

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

Hence ϕ is an isomorphism of R/s onto R'.

Hence it is proved that,

If $f: R \to R'$ is a ring homomorphism

then ~~prove~~ ~~that~~ $\frac{R}{S} \cong R'$.

$\Rightarrow f(a) - f(b) = 0'$ [$\because$ f is homomorphism]

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

$\Rightarrow \varphi(S+a) = \varphi(S+b)$ [" "]

$\Rightarrow \varphi$ is well defined.

(ii) φ is one-one:

Let $\varphi(S+a) = \varphi(S+b)$

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

$\Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a-b) = 0'$

$\Rightarrow a-b \in \ker f$

$\Rightarrow a-b \in S$

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

$\Rightarrow S+a = S+b$

$\Rightarrow \varphi$ is one-one.

φ is onto, for, if $a' \in R'$, then f being onto $\exists\ a \in R$ such that $a' = f(a)$ and so $S+a \in R/S$ s.t.

$$\varphi(S+a) = f(a)$$

Finally φ preserves both the compositions, as

$$\begin{aligned}\varphi[(S+a)+(S+b)] &= \varphi[S+(a+b)] \\ &= f(a+b) \\ &= f(a) + f(b) \\ &= \varphi(S+a) + \varphi(S+b)\end{aligned}$$

Hence R' is a ring without zero divisors.

1st Law of isomorphism

Statement: Every homomorphic image of a ring is isomorphic to some quotient ring of that ring.

$f: R \to R' \Rightarrow R' \cong \frac{R}{S}$

$\varphi: \frac{R}{S} \to R' \quad \varphi(S+a) = f(a)$

(i) φ is well defined
(ii) φ is one-one
(iii) φ is onto
(iv) φ is homomorphism

State & prove 1st law of isomorphism.

Or, If $f: R \to R'$ is a ring homomorphism then prove that $\frac{R}{S} \cong R'$.

Proof: Let $f: R \to R'$ be a ring homomorphism and R' is the homomorphic image of R.

Let $\ker f = S$ and $\varphi: \frac{R}{S} \to R'$ is a mapping defined by $\varphi(S+a) = f(a) \quad \forall S+a \in \frac{R}{S}$.

(i) φ is well defined: Let $S+a = S+b$

Then $S + (a-b) = S$

$\Rightarrow a - b \in S$

$\Rightarrow a - b \in \ker f$

$\Rightarrow f(a-b) = 0'$

10.10.2023

(p-227)

Theorem: Prove that ① isomorphic image of a commutative ring is commutative

② isomorphic image of a ring with unity is a ring with unity.

③ isomorphic image of a ring without zero divisors is a ring without zero divisors.

④ isomorphic image of an integral domain is an integral domain.

Proof ②: Let $f: R \to R'$ be a ring isomorphism.

Suppose R is a ring with unity.

Then $\forall a \in R \Rightarrow a \cdot 1 = 1 \cdot a = a$

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

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

This shows that $f(1)$ is the unity element of R'

Hence R' is the ring with unity.

Proof ③: Let $f: R \to R'$ be a ring isomorphism.

Suppose R is a ring without zero divisors.

Then $f(0) = 0'$, where $0 \in R$ and $0' \in R'$

Since R is a ring without zero divisors, so,

$a \neq 0, b \neq 0 \Rightarrow ab \neq 0$

$\Rightarrow f(ab) \neq f(0)$

Since $a \neq 0, b \neq 0 \Rightarrow f(a) \cdot f(b) \neq f(0)$ $\therefore f$ is a homomorphism

$\Rightarrow f(a) \neq 0, f(b) \neq 0$

The matrices in $A \cap B$ have the form:

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

Now let $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ in R.

Now consider $(A \cap B) \cdot X$:

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} a \cdot x_{11} & a \cdot x_{12} \\ 0 & 0 \end{bmatrix} \notin A \cap B$$

Similarly

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x_{11} a & 0 \\ x_{21} a & 0 \end{bmatrix} \notin A \cap B$$

Hence it prove the theorem.

Now let's consider the sum of these two ideals $A+B$, which consists of all possible sums of matrices from A & matrices from B:

$$A+B = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$$

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

Now let's consider the element $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in R$. If $A+B$ were a left ideal of R it should be closed under left multiplication by elements of R.

Now, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a+c & d \\ b & 0 \end{bmatrix} = \begin{bmatrix} a+c & d \\ 0 & 0 \end{bmatrix} \notin A+B$

Similarly we can show that

$$\begin{bmatrix} a+c & d \\ b & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a+c & 0 \\ b & 0 \end{bmatrix} \notin A+B$$

Hence it is proved.

(8) If A is a left ideal of a ring R & B is a right ideal of R then $A \cap B$ need not be even a one sided ideal of R.

Proof: Consider $A = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ & $B = \left\{ \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : c, d \in \mathbb{Z} \right\}$

Now let's find the intersection $A \cap B$. It consists of all matrices that belong to both A & B:

$$A \cap B = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\} \cap \left\{ \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : c, d \in \mathbb{Z} \right\}$$

⑥ If S is an ideal of a ring R with unity elem... 1 and if $1 \in S$, then show that $R = S$.

Proof: Let x be an arbitrary element of R. We want to show that $x \in S$.

Since $1 \in S$ & $x \in R$ we can express $x = 1 \cdot x$

Now S is an ideal which means it is closed und... left multiplication by elements of R.

Therefore $1 \cdot x \in S$.

$\therefore R \subseteq S$ ... ①

Again, Let $y \in S$ we want to show $y \in R$.

Since S is an ideal of R then $S \subseteq R$ by defin...

Therefore $y \in R$

$\therefore S \subseteq R$ ... ②

From ① & ② we can say $R = S$.

⑦ If A is a left ideal of a ring R and B is a rig... ideal of R, then $A+B$ need not be even a one sided ideal of R.

Hint: In the ring R of all 2×2 matrices over Z.

consider $A = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in Z \right\}$ & $B = \left\{ \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : c, d \in Z \right\}$

Proof: consider the left ideal $A = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in Z \right\}$ and right ideal $B = \left\{ \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : c, d \in Z \right\}$ in the ring R of 2×2 matrices over Z.

(5) Show that the set E of all even integers is an ideal of the ring of integers.

Proof: Containment of the Additive Identity

The additive identity in the ring of integers is 0, which is an even integer. Therefore $0 \in E$.

Closure under Addition

Let a & b be two even integers. We want to show $a+b \in E$. Let $a = 2m$ & $b = 2n$

$\therefore a+b = 2m + 2n = 2(m+n)$

Since $(m+n)$ is an integer & $(a+b)$ is divisible by 2.

$\therefore a+b \in E$.

Closure under Left Multiplication

Let a be an even integer & r be any integer.

we have to show ra is even & $ra \in E$.

Let $a = 2m$ for some integer m.

$\therefore ra = r(2m) = 2(rm)$

Since rm is an integer & ra is divisible by 2.

$\therefore ra \in E$

Hence it is proved that E is an ideal of the ring of integers.

Proof: Containment of the Additive Identity

Since $0 \cdot s = 0$ for any element s in S, it follows that $0 \cdot x = 0$, $\forall x$ in R. Therefore $0 \in S:t$ as x

Closure under addition

Let $x, y \in S:t$ then $xs \subseteq t$ & $ys \subseteq t$ $\forall s$ in S.

we want to show that $x+y$ is also in $S:t$

meaning $(x+y)s \subseteq t$ $\forall s$ in S.

Consider $(x+y)s$. since $xs \subseteq t$ & $ys \subseteq t$ we

$(x+y)s = xs + ys$

Now since t is an ideal it is closed under ad

Therefore $xs + ys$ is in t which means

$(x+y)s \subseteq t$ $\forall s$ in S.

Hence $x+y$ is in $S:t$ & $S:t$ is closed under

Closure under Left Multiplication

Let $x \in S:t$ & $r \in R$ we want to show that r

is also in $S:t$, meaning $(rx)s \subseteq t$ for all s in S.

Consider $(rx)s$. since $xs \subseteq t$ $\forall s \in S$ we have

$(rx)s = r(xs)$

Now $xs \subseteq t$ implies that $r(xs)$ is also in t becau

t is closed under left multiplication by elements of R

Therefore $(rx)s \subseteq t$ $\forall s \in S$

$\therefore rs \in S:t$.

Thus $S:t$ is closed under left multiplication.

Hence $S:t$ is an ideal of R.

$a(-x) = -(ax) = -0 = 0$
So $-x \in S$ & S is closed under additive inverse.

ⓒ Closure under right multiplication
Let $x \in S$ & r be any element of R. We want to show that $xr \in S$. Using the associativity of ring multiplication we have:
$a(xr) = (ax)r = 0 \cdot r = 0$.
So $xr \in S$ & S is closed under right multiplication.
Therefore S is a right ideal of the ring R.

(ii) $t = \{x \in R : xa = 0\}$ is a left ideal of R.
ⓐ & ⓑ → closure under addition & additive inverse same as before.

ⓒ Closure under left multiplication
Let $x \in t$ and r be any element of R. We want to show that $rx \in t$. Using the associativity of ring multiplication we have:
$(rx)a = r(xa) = r \cdot 0 = 0$
So $rx \in t$ & t is closed under left multiplication.
Therefore t is a left ideal of the ring R.

④ If S & T are ideals of a ring R, define $S:T = \{x \in R : xS \subseteq T\}$. Show that $S:T$ is an ideal of R.

Hint: $S:T = \{x \in R : xS \in T, \forall s \in S\}$.

Since this set is a subset of the 2×2 matrices with integral entries, it inherits the property of containing additive inverses for each element.

$\therefore S$ is a subring of R.

Now Let $A=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$ & $B=\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$ in S then

$AB=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ where $A\neq 0$ & $B\neq 0$

So S is containing zero divisors.

$\therefore S$ is not an integral domain.

(3) Let a be an arbitrary element of a ring R. Show that:-

(i) $S=\{x\in R : ax=0\}$ is a right ideal of R

(ii) $T=\{x\in R : xa=0\}$ is a left ideal of R

Proof:- (i) $S=\{x\in R : ax=0\}$ is a right ideal of R.

(a) Closure under addition

Let $x, y\in S$. This means $ax=0$ & $ay=0$

Now consider $x+y$. We want to show that $(x+y)\in S$.

Using the distributive property of rings, we have:

$a(x+y)=ax+ay=0+0=0$

So $(x+y)\in S$ & S is closed under addition.

(b) Closure under additive inverse.

Let $x\in S$ which means $ax=0$. We want to show that $-x\in S$. Using the distributive property and the fact that 0 is the additive identity of R, we have:

Soln: **Subring:** A sub-ring is a non-empty subset of a ring that is itself a ring under the inherited operations.

Properties:

* A sub-ring contains the additive identity (0) of the original ring.
* A sub-ring is closed under addition & multiplication.
* A sub-ring may or may not contain the multiplicative identity (1)
* The sub-ring must be closed under additive inverse.

Ideal: An ideal is a special type of sub-ring that has additional properties.

Properties:

* An ideal contains the additive identity (0) of the ring.
* It is closed under addition & subtraction.
* It is closed under multiplication by elements from the larger ring.
* It may or may not contain the multiplicative identity (1) of the larger ring.

Let R be a ring of 2×2 matrices with their elements as integers

Let $S = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$

Then for any two matrices $A = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ & $B = \begin{bmatrix} d & 0 \\ e & f \end{bmatrix}$ in S

$$A + B = \begin{bmatrix} a+d & 0 \\ b+e & c+f \end{bmatrix} \in S$$

$\therefore$ S is closed under addition.

$$AB = \begin{bmatrix} ad & 0 \\ bd+ce & cf \end{bmatrix} \in S$$

$\therefore$ S is closed under multiplication

we know the additive identity for 2×2 matrices is the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ & it is clearly in S.

(H.W) Exercise - X.3

(1) Prove that the set S of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ with a & b as integers forms a subring of the ring R of all 2×2 matrices having elements as integers. Prove further that S is neither a right nor a left ideal in R.

Proof: Let R be a ring of all 2×2 matrices with their elements as integers.

Let $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in Z \right\}$

Then for any two matrices $A = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}$ & $B = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix}$ in S

$$A-B = \begin{bmatrix} a_1-a_2 & 0 \\ 0 & b_1-b_2 \end{bmatrix} \in S \quad \& \quad AB = \begin{bmatrix} a_1a_2 & 0 \\ 0 & b_1b_2 \end{bmatrix} \in S$$

Thus $A, B \in S \Rightarrow A-B \in S$ & $AB \in S$

So S is a sub-ring of R.

Moreover if $A = \begin{bmatrix} p & 0 \\ 0 & q \end{bmatrix} \in S$ & $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$ then

$$TA = \begin{bmatrix} ap & bq \\ cp & dq \end{bmatrix} \notin S \qquad AT = \begin{bmatrix} pa & bp \\ eq & dq \end{bmatrix} \notin S$$

This shows that S is not a left nor a right ideal of R.

(2) Distinguish between subrings & ideals in a ring. Show that $S = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in Z \right\}$ is a sub-ring & Further show that it is not an integral domain.

Thus, n is the least positive integer s.t. $na = 0 \ \forall a \in R$.
Hence, the characteristic of R is n.

As a consequence of the above theorem, it follows that the characteristic of the integral domain D is the least positive integer n, if it exists s.t. $n \cdot 1 = 0$ where 1 is the unity of D; and 0 is the zero of D. If such an n does not exist, characteristic of D is zero or infinite.

The characteristic of a field is defined to be the characteristic of the field regarded as an integral domain.

Thm-①: The characteristic of a ring R with unity is 0 or a positive integer n, according as the unity element of R regarded as a member of the additive group R has the order 0 or n.

Proof: Let R be a ring with unity element 1.

Let $O(1)=0$, when 1 is regarded as a member of $(R,+)$. Then $\exists$ no positive integer n for which $n\cdot 1=0$ & therefore, $na\neq 0 \ \forall\ a\in R$.

Thus, $\exists$ no positive integer n for which $na=0\ \forall a\in R$.

Accordingly, R is a ring of zero or infinite characteristic.

Again, let $O(1)=n$, when 1 is regarded as a member of $(R,+)$.

Then n is the least positive integer such that $n\cdot 1=0$.

Now if $a\in R$, then

$$\begin{aligned} na &= a+a+\cdots \text{ to } n \text{ terms} \\ &= 1\cdot a+1\cdot a+\cdots \text{ to } n \text{ terms} \\ &= (1+1+\cdots \text{ to } n \text{ terms})\,a \\ &= (n\cdot 1)\,a \\ &= 0\cdot a \\ &= 0. \end{aligned}$$

⊕① $f: R \to R'$

$\forall\, a', b' \in R'$ $\exists\, a, b \in R$ s.t. $f(a) = a'$, $f(b) = b'$

$a' \cdot b' = f(a) \cdot f(b)$

$= f(ab)$

$= f(ba)$

$= f(b)\, f(a)$ [f is homomorphism]

$= b' \cdot a'$

Hence R' is commutative.

20.09.2023

$Z_x = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$

$x \times 0 = 0$ $\quad x \times 4 \neq 0$

$x \times 1 = 0$ $\quad x \times 5 = 0$

$x \times 2 = 0$ $\quad x \times 6 \neq 0$

$x \times 3 = 0$

Characteristic of a ring:

The characteristic of a ring R if it exists is the smallest positive integer n s.t. $na = 0 \;\forall\, a \in R$

If there exists no positive integer then the characteristic of R is either zero or finite characteristic.

Thm — 1, 3, 4, 5 (P-205)

(iii) f is onto

For each $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M$

$\exists\ a+ib \in \mathbb{C}$ such that $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

that is $f(a) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

Thus f is onto

Hence it is proved.

Problem (P-235)

If $\mathbb{C}$ is the ring of the complex numbers then the mapping $f: \mathbb{C} \to \mathbb{C}$ defined by $f(x+iy) = x-iy$, $\forall x+iy \in \mathbb{C}$ is an automorphism.

P-226 (Ex-2)

Consider the mapping $f: \mathbb{Z} \to E$ defined by $f(a) = 2a$ $\forall a \in \mathbb{Z}$ where E is the set of all even integer and $a*b = \frac{ab}{2}$ $\forall a, b \in E$ and $(E, +, *)$ is a ring. Then show that f is isomorphism.

P-227 (Th^m-2)

(i) Prove that isomorphic image of a commutative r is commutative.

(ii) Every isomorphic image of a ring with unity is ring with unity.

(iii) Every isomorphic image of a ring without zero divisors is a ring without zero divisors.

19.09.2023

(226)

Thm: Let $f: R \to R'$ be a ring isomorphism. Then prove that

(i) $f(0) = 0'$

(ii) $f(-a) = -f(a)$

(iii) $f(R)$ is a subring of R'.

(225)(Ex-1)

Problem: Let $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in R \right\}$ and $f: \mathbb{C} \to M$ defined by $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $\forall\, a+ib \in \mathbb{C}$. Then show that f is isomorphism.

Soln: (i) f is homomorphism

Let $z = a+ib$ & $w = c+id$ be any two elements of $\mathbb{C}$ where $a, b, c, d \in R$

Then $f(z+w) = f[(a+c)+i(b+d)]$

$= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}$ $\left[\because f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right]$

$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$= f(z) + f(w)$

Similarly $f(zw) = f(z) \cdot f(w)$ $\forall\, z, w \in \mathbb{C}$

$\therefore f$ is homomorphism.

(ii) f is one-one

Let $f(z) = f(w)$, $z, w \in \mathbb{C}$

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

$\Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \Rightarrow a = c,\ b = d$

$\Rightarrow a+ib = c+id$

$\Rightarrow z = w \Rightarrow f$ is one-one.

$\therefore f(a-b) = f(a+(-b))$

$= f(a) + f(-b)$ [$\because$ f is homomorphism]

$= f(a) - f(b)$ [$\because$ u]

$= 0' - 0'$

$= 0'$

$\Rightarrow a-b \in \ker f$

Again, $f(ab) = f(a) \cdot f(b)$

$= 0' \cdot 0'$

$= 0'$

$\Rightarrow ab \in \ker f$

Thus $\ker f$ is a subring of R.

Now for any $a \in \ker f$ & $r \in R$

$f(ar) = f(a) \cdot f(r)$ [$\because$ f is homomorphism]

$= 0' \cdot f(r)$ [$\because a \in \ker f \Rightarrow f(a) = 0'$]

$= 0'$

and $f(ra) = f(r) f(a)$

$= f(r) \cdot 0'$

$= 0'$

Thus $a \in \ker f$ & $r \in R$

$\Rightarrow ar, ra \in \ker f$

Hence $\ker f$ is an ideal of R.

Kernel of a ring homomorphism:

Let $f: R \to R'$ be a ring homomorphism then the kernel of f is denoted by $\ker f$ and defined by

$$\ker f = \{x \in R : f(x) = 0'\}$$

where $0'$ is the additive identity of R'

Thm: Prove that kernel of a ring homomorphism is an ideal of its domain and image is a subring of its codomain. ⟶ (H.W)

Range / Image of a ring homomorphism:

Let $f: R \to R'$ be a ring homomorphism then the image of f is denoted by $\text{im} f$ and defined by

$$\text{Im} f = \{y \in R' : \exists\, x \in R \text{ s.t. } f(x) = y,\ x \in R\}$$

Proof: Let $f: R \to R'$ be a ring isomorphism then

$$\ker f = \{x \in R : f(x) = 0'\}$$

Since $f: R \to R'$ is homomorphism

So, $f(0) = 0'$ therefore $0 \in \ker f$

$\therefore \ker f \neq \emptyset$

Now, let $a, b \in \ker f$ be any two elements

then $f(a) = 0'$ & $f(b) = 0'$

17.09.2023

Thm: An ideal S of a commutative ring R with unity is maximal iff the residue class ring R/S is a field. → (H.W) | 221 Page Thm 2

Homomorphism of Rings:

$$f: G \longrightarrow G'$$

$$f(a*b) = f(a) * f(b) \quad \forall\, a, b \in G$$

Let R and R' be two rings and $f: R \to R'$ then f is called a homomorphism if

$$\left.\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a) \cdot f(b) \end{aligned}\right\} \forall\, a, b \in R.$$

Isomorphism of Rings:

Let R & R' be two rings and $f: R \to R'$ then f is called an isomorphism if

1) f is homomorphism
2) f is one-one
3) f is onto

Th^m: Let R be a commutative ring with unity and S be an ideal of R. Prove that R/S is an integral domain iff S is a prime ideal.

Proof: Since S is an ideal of a commutative ring R with unity so R/S is also a commutative ring with unity.

Now, first suppose that S is a prime ideal. Then

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

$\Rightarrow ab \in S$

$\Rightarrow a \in S$ or $b \in S$ [$\because S$ is prime]

$\Rightarrow S+a = S$ or $S+b = S$.

This shows that R/S is without zero divisors & hence it is an integral domain.

Again, suppose that $(S+a)(S+b) = S \Rightarrow S+a = S$ or $S+b = S$.

Then, $S+ab = S \Rightarrow S+a = S$ or $S+b = S$

i.e. $ab \in S \Rightarrow a \in S$ or $b \in S$.

This proves that S is prime.

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

$= N + abc$

$= N + a(bc) = (N+a)(N+bc)$

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

(viii) $(N+a)((N+b)+(N+c)) = (N+a)(N+(b+c))$

$= N + a(b+c)$

$= N + (ab + ac)$

$= (N+ab) + (N+ac)$

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

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

$= N + (a+b)c$

$= N + (ac + bc)$

$= (N+ac) + (N+bc)$

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

Hence prove the theorem.

Proof: $\frac{R}{N} = \{N+a : a \in R\}$

$\forall\ N+a,\ N+b \in \frac{R}{N}$

(I) $(N+a)+(N+b) = N+(a+b) \in \frac{R}{N}$ [$\because a, b \in R \Rightarrow a+b \in R$]

(II) $((N+a)+(N+b))+(N+c) = (N+(a+b))+(N+c) = N+(a+b+c)$

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

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

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

(III) Since $0 \in R \Rightarrow N+0 = N \in \frac{R}{N}$

& $\forall\ N+a \in \frac{R}{N}$

$(N+a)+(N+0) = N+(a+0) = N+a$

& $(N+0)+(N+a) = N+(0+a) = N+a$

(IV) for each $N+a \in \frac{R}{N}$ $\exists\ N+(-a) \in \frac{R}{N}$ [$\because a \in R \Rightarrow -a \in R$]

s.t. $(N+a)+(N+(-a)) = N+(a+(-a)) = N+0 = N$

& $(N+(-a))+(N+a) = N+(-a+a) = N+0 = N$

So, the additive inverse of $N+a$ is $N+(-a)$

(V) $(N+a)+(N+b) = N+(a+b) = N+(b+a) = (N+b)+(N+a)$

$\forall\ N+a,\ N+b \in \frac{R}{N}$

Similarly for multiplication.

(VI) $\forall\ N+a,\ N+b \in \frac{R}{N}$

$(N+a)(N+b) = N+ab \in \frac{R}{N}$ [$\because a, b \in R \Rightarrow ab \in R$]

Page-219 : Th^m - 9

An ideal S of a ring Z is a maximal ideal of Z iff S is generated by a prime integer p.

Page-220 : Th^m - 10

Let S_1 & S_2 be any two ideals of a ring. Then $S_1 + S_2$ is the ideal generated by $S_1 \cup S_2$.

13.09.2023

Quotient Ring: Let R be a ring and N be an ideal of R. Then the set of all additive cosets of N, denoted by $\frac{R}{N} = \{N+a : a \in R\}$, forms a ring with the binary operations defined by

$$(N+a) + (N+b) = N + (a+b)$$
$$\& \quad (N+a)(N+b) = N + ab \quad \Big\} \forall\, a, b \in R$$

The ring $\frac{R}{N}$ is called a quotient ring or factor ring of R modulo N.

Th^m: Let R be a ring and N be an ideal of R. Then prove that the set of all additive cosets of N; that is $\frac{R}{N} = \{N+a : a \in R\}$, forms a ring with the binary operations defined by

$$(N+a) + (N+b) = N + (a+b)$$
$$\& \quad (N+a)(N+b) = N + ab \quad \Big\} \forall\, a, b \in R.$$

Let s be the least positive integer in S.

Then $\mathbb{Z}s$ is a principal ideal of $\mathbb{Z}$.

We have to show that $\mathbb{Z}s = S$

Clearly, $\mathbb{Z}s \subseteq S$ [$\because as \in \mathbb{Z}s \Rightarrow a \in \mathbb{Z}, s \in S \Rightarrow as \in S$]

Now let $n \in S$

By division algorithm, $\exists$ integers $q, r \in \mathbb{Z}$ s.t.

$n = qs + r$ where $r = 0$ or $0 < r < s$

$\Rightarrow n - qs = r$

Now $s \in S, q \in \mathbb{Z} \Rightarrow qs \in S$ [$\because S$ is an ideal of $\mathbb{Z}$]

Again $n \in S, qs \in S \Rightarrow n - qs \in S$

$\Rightarrow r \in S$

Since s is the least positive integer of S. Thus $0 < r < s$ is not possible. So, $r = 0$

and $n - qs = 0$

or, $n = qs \in \mathbb{Z}s$

Then $n \in S \Rightarrow n \in \mathbb{Z}s$

So, $S \subseteq \mathbb{Z}s$

Hence, $S = \mathbb{Z}s$ and therefore S is a principal ideal of $\mathbb{Z}$

Thus every ideal in $\mathbb{Z}$ is a principal ideal and therefore $\mathbb{Z}$ is a principal ideal ring.

Now, let S be any ideal of R containing a.

Now, if $ra \in Ra$, then $r \in R$ and therefore, $a \in S$, $r \in R \Rightarrow ra \in S$ [$\because$ S is an ideal containing

Consequently, $ra \in Ra \Rightarrow ra \in S$ and therefore, $Ra \subseteq S$

Thus, Ra is contained in every ideal containing a and therefore it is smallest ideal containing a.

Hence Ra is the principal ideal generated by a.

1st Mid → 27-09-2023

12.09.2023

Thm: Prove that the ring of integers $\mathbb{Z}$ is a principal ideal ring.

Prove that every ideal in the ring of integers $\mathbb{Z}$ is a principal ideal.

Proof: We know that $\mathbb{Z}$ is a commutative ring with unity. Let S be any ideal of $\mathbb{Z}$.

If $S = \{0\}$, then it is clearly a principal ideal

If $S \neq \{0\}$, let $a \in S$ then $-a \in S$.

Thus S contains at least one positive integer.

Thm: If R is a commutative ring and $a \in R$, then prove that $Ra = \{ra : r \in R\}$ is an ideal of R.

Proof: since $r \in R$ & $a \in R \Rightarrow ra \in R$ [by closure law of multiplication]

Thus $Ra \subseteq R$

Now let $r_1a, r_2a \in Ra$ be any two elements, where $r_1, r_2 \in R$

Then $r_1a - r_2a = (r_1 - r_2)a \in Ra$ [$\because r_1 - r_2 \in R$]

and $(r_1a)(r_2a) = [(r_1a)r_2]a \in Ra$ [$\because (r_1a)r_2 \in R$]

$\therefore Ra$ is a subring of R.

Now if $r_1a \in Ra$ and $r \in R$ [be any elements]

Then $r(r_1a) = (rr_1)a \in Ra$ [$\because r, r_1 \in R \Rightarrow rr_1 \in R$]

and $(r_1a)r = r_1(ar) = r_1(ra)$ [$\because R$ is commutative]

$= (r_1r)a \in Ra$ [$\because r_1, r \in R \Rightarrow r_1r \in R$]

Hence Ra is an ideal of R.

(H.W) → R is a principle ideal.

(H.W) → It has already been shown that Ra is an ideal of R

Also, $a \in Ra$ [$\because 1 \in R \Rightarrow 1.a \in Ra$]

Thus, Ra is an ideal of R containing a.

Thm: A field has no proper ideal.

or,

If F is a field, then the only non-zero ideal of F is F itself.

Proof: Let S be a non-zero ideal of a field F.

Suppose $a \in S$ be any element s.t. $a \neq 0$

Then $a \in F$ [$\because S \subseteq F$]

$\Rightarrow a^{-1} \in F$ [$\because F$ is a field]

Now, $a \in S$, $a^{-1} \in F \Rightarrow a a^{-1} \in S$ [$\because S$ is an ideal of F]

$\Rightarrow 1 \in S$

Then for any $x \in F$, we have

$1 \in S$, $x \in F$

$\Rightarrow 1 \cdot x \in S$ [$\because S$ is an ideal of F]

$\Rightarrow x \in S$

$\therefore F \subseteq S$ ..... (1)

but S is an ideal of F, so, $S \subseteq F$ ..... (2)

From (1) & (2) we get, $S = F$.

Hence A field has no proper ideal.

That is the only non-zero ideal of a field F is F itself.

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

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

Thus, $a \in S, b \in S \Rightarrow a - b \in S$ & $ab \in S$

S is a sub-ring of R, satisfying (II)

Hence, S is an ideal of R.

05.09.2023

Arbitrary intersection of ideals of a ring R is an ideal of R. → 216 P. (Th^m - 2)

$(\mathbb{Z}, +, \cdot)$ is a principle ideal ring $S = \{\ldots -10, -5, 0, 5, 10, \ldots\}$ is maximal ideal.

$S_1 = \{\ldots -20, -10, 0, 10, 20, \ldots\}$

$S_2 = \{\ldots -15, -10, -5, 0, 5, 10, 15, \ldots\}$

① S_1 ⊂ S_2 তাহলে S_1 maximal নয় but S_2 maximal.

Prime ideal:

$S_1 = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$

$ab \in S_1 \Rightarrow a \in S_1$ or $b \in S_1$

[$\because 5 | a$ or $5 | b$]

Also $S \subseteq R$.

So, the commutative of addition
the associative of "
the " of multiplication
& the distributive laws hold in S.

Hence S is a subring of R.

** def. → book: Page-217

Principal ideal

An ideal S of a ring R is said to be a principal ideal of a ring R if it is generated by single element $S = \{a\}$

Principal ideal ring

A commutative ring with unity without zero divisor is called a principal ideal ring & every ideal is principal ideal

Maximal ideal

$S \neq \{0\}$
$S \neq R$
A non-zero ideal S s.t. $S \neq R$ then S is said to be maximal ideal if $\nexists$ no ideal greater than S then S is maximal ideal

Prime

$ab \in$
$a \in$
$b \in$

(H.W)

Proof (2): Let S be an ideal of a ring R. Then, S is sub-ring of R. In particular, S is a subgroup of a additive group of R.

(i) $a \in S,\ b \in S \Rightarrow a - b \in S$

Also, by definition of an ideal,

(ii) $a \in S,\ r \in R \Rightarrow ar \in S$ and $ra \in S$.

Conversely, let S be a non-empty subset of ring R such that conditions (i) and (ii) are satisfi

03.09.2023

**Thm 1: The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R if $a \in S, b \in S \Rightarrow a-b \in S$ and $ab \in S$, $\forall a, b \in S$.

**Thm 2: The necessary and sufficient conditions for a non-empty subset S of a ring R to be an ideal of R if i) $a \in S, b \in S \Rightarrow a-b \in S$
ii) $a \in S, r \in R \Rightarrow ar \in S$ and $ra \in S$

Proof ⇒: Let S be a subring of R
Then $\forall a \in S, b \in S \Rightarrow a \in S, -b \in S$ [∵ S is an additive abelian group]
$\Rightarrow a + (-b) \in S$ [by (i)]
$\Rightarrow a - b \in S$

Also given that $\forall a \in S, b \in S \Rightarrow ab \in S$ [∵ S is a subring of R]

Conversely, let S be a non-empty subset of R s.t.
$\forall a, b \in S \Rightarrow a-b \in S$ ... (i) & $ab \in S$ ... (ii) (w.k.t)
Then $a \in S, a \in S \Rightarrow a-a \in S \Rightarrow 0 \in S$ by (i)
and $0 \in S, a \in S \Rightarrow 0-a \in S \Rightarrow -a \in S$ by (i)
Also, $a \in S, b \in S \Rightarrow a \in S, -b \in S$
$\Rightarrow a-(-b) \in S$ by (i)
$\Rightarrow a+b \in S$
and $a \in S, b \in S \Rightarrow ab \in S$ by (ii)
Thus S is closed under addition and multiplication.
Also, the additive identity in S & every element in S has its negative in S.

Ex-2 (P-215) (H.W)

Proof: Let R be ring of all 2×2 matrices with their elements as integers.

Let $S=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z}\right\}$

Then, for any two matrices $A=\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$ & $B=\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ i

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

& $AB=\begin{bmatrix} a_1 a_2 & 0 \\ b_1 b_2 & 0 \end{bmatrix} \in S \quad [\because a_1, a_2, b_1, b_2 \in \mathbb{Z}]$

Thus $A \in S$, $B \in S \Rightarrow A-B \in S$ & $AB \in S$.

So, S is a sub-ring of R.

Moreover if $A=\begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix} \in S$ & $T=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$ be arbitrary. Then

$$TA=\begin{bmatrix} ap+bq & 0 \\ cp+dq & 0 \end{bmatrix} \in S \quad [\because ap+bq, cp+dq \in \mathbb{Z}]$$

Thus $A \in S$, $T \in R \Rightarrow TA \in S$

This shows that S is a left ideal of R.

However, it is clear that,

$B=\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in S$ & $C=\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \in R$

But $BC=\begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix} \notin S$

This shows that S is not a right ideal of R.

(H.W)

* If R is ring with unity & $(xy)^2 = x^2y^2 \ \forall\ x, y \in R \Rightarrow R$ is commutative

Proof: We have, $(xy)^2 = x^2y^2 \ \forall\ x, y \in R \quad \cdots (1)$

Replacing y by $y+1 \in R$ in (1) where 1 is unity.

$$[x(y+1)]^2 = x^2(y+1)^2$$

$$\Rightarrow (xy+x)^2 = x^2(y^2+2y+1) \quad \left[\because \begin{array}{l} \text{R.D.P. \& L.D.P} \\ (y+1)(y+1) = y(y+1)+(y+1) \\ = y^2+y+y+1 \\ = y^2+2y+1 \end{array}\right]$$

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

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

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

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

(by cancellation law)

$$\Rightarrow (xy)x = x^2y \quad \forall\ x, y \in R \quad \cdots (2)$$

Replacing x by $(x+1)$ $\left[\because \begin{array}{l} (xy)x = x^2y \\ x(yz) = x(xy) \end{array}\right]$

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

$$\Rightarrow (x+1)(yx+y) = (x+1)(xy+y)$$

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

$\Rightarrow$ by eqn (2) and cancellation law

$$\Rightarrow yx = xy \quad \forall\ x, y \in R$$

Hence R is commutative ring.

Subring: Let $(R,+,\cdot)$ be a ring and S be a non-empty subset of R then S is said to be a subring of R if $a+b \in S$, $ab \in S$, $\forall a,b \in S$ and S is itself a ring with respect to the operation.

Example: $2\mathbb{Z}$ is a subring of $\mathbb{Z}$

$2\mathbb{Z}$ is a subring of R

$S = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$ is a subring of $R = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}\right\}$

Ideals: A subring S of a ring R is called an ideals of R if $\forall a \in S$ and $\forall r \in R$ implies that $ar \in S$ (R.I) $ra \in S$. (L.I)

Example: $n\mathbb{Z}$ is an ideals of $\mathbb{Z}$.

P-215

Ex.2: $S = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$ show that

i) S is a subring of $R \longrightarrow \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}\right\}$ (W.H)

ii) S is a left ideal of R

iii) S is not a right ideal of R

Note: If $S = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$

then (iii) satisfy but not

(ii) → S is right ideal

not left ideal

P-223

↳ Ex: 1 to 8 (H.W)

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

[by commutativity & associativity of addition in R]

$\Rightarrow ba+ab = 0$ [by cancellation law of addition]

$\Rightarrow ba+ab = ba+ba$ [$\because x+x=0 \ \forall x \in R$ & $ba \in R$]

$\Rightarrow ab = ba$ [by left cancellation law of addition in R]

Hence R is a commutative ring.

The converse of the above statement is not true since the ring $\mathbb{Z}$ of all integers is a commutative ring but each of its elements is not idempotent.

(#) Let R be a ring with unity s.t. $(ab)^2 = a^2b^2 \ \forall a,b \in R$ show that R is a commutative.

Proof: (H.W)

30.08.2023

✱ An element of a ring R is said to be idempotent if $a^2 = a$ ⟷ Nilpotent if $a^n = 0$.

(H.W)

Th^m: If each element of a ring R is idempotent show that R must be a commutative ring. What do you say about the converse.

Proof: Let R be a ring s.t. $x^2 = x \ \forall x \in R$

First we show that, $x + x = 0 \ \forall x \in R$.

Now, $x \in R \Rightarrow (x+x) \in R \Rightarrow (x+x)^2 = (x+x)$.

Now, $(x+x)^2 = (x+x)$

$\Rightarrow (x+x)(x+x) = (x+x)$ [by distributive law]

$\Rightarrow (x^2 + x^2) + (x^2 + x^2) = (x+x)$ [$\because x^2 = x$]

$\Rightarrow (x+x) + (x+x) = (x+x) + 0$

$\Rightarrow (x+x) = 0$

Thus $x + x = 0 \ \forall x \in R$

Now let a & b any arbitrary elements of R s.t. $a^2 = a$ & $b^2 = b$

Also $a \in R, b \in R \Rightarrow (a+b) \in R \Rightarrow (a+b)^2 = (a+b)$

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

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

$\Rightarrow (a+b)a + (a+b)b = (a+b)$ [by distributive law]

$\Rightarrow (a^2 + ba) + (ab + b^2) = (a+b)$ [$\because$]

$\Rightarrow (a + ba) + (ab + b) = (a+b)$

Thm: A finite commutative ring without zero divisors is a field.

Proof: Let D be a finite commutative ring without zero divisors.

Let $a \in D$ s.t. $a \neq 0$

Suppose $D^* = \{ax : x \in D \text{ & } x \neq 0\}$

Then each element of D^* is a non-zero elements of D.

Moreover all the elements of D^* are distinct

since $ax = ay$, $a \neq 0 \Rightarrow x = y$

Thus D^* has $(n-1)$ non-zero elements of D.

since $a \in D$ and $a \neq 0$

so, $\exists\ ax \in D$ s.t. $a \cdot x = a$

$\Rightarrow ax = xa \quad [\because D \text{ is commutative}]$

$\Rightarrow ax = a(1)$

$\Rightarrow x = 1 \in D$

since $1 \in D$, so $\exists\ ax \in D$ s.t. $ax = 1$

$\Rightarrow ax = xa = 1 \quad [\because D \text{ is commutative}]$

$\Rightarrow a^{-1} = x$

$\Rightarrow$ every non-zero element of D has a multiplicative inverse

Hence D is a field.

Th^m: A finite integral domain is a field.

Proof: Let D be a finite integral domain with n elements. Then D is a commutative ring with unity & without zero divisors.

Let $a \in D$ s.t. $a \neq 0$.

Suppose $D^* = \{ax : x \in D \text{ & } x \neq 0\}$

Then each element of D^* is a non-zero element of D.

Moreover, all the elements of D^* are distinct

Since $ax = ay$, $a \neq 0 \Rightarrow x = y$

Then D^* has $(n-1)$ non-zero elements of D.

Since $1 \in D$, thus $\exists\, ax \in D^*$ s.t.

$ax = 1$ for some $x \in D$.

$\Rightarrow ax = xa = 1$ [$\because D$ is a commutative ring]

$\Rightarrow a^{-1} = x$

$\Rightarrow$ every non-zero element of D has a mult. inv.

Hence D is a field.

Note: If the integral domain is finite then it is a field.

29.08.2023

Thm: A field has no zero divisors.

Alternative Proof:

Let F be a field and $a, b \in F$ s.t. $ab = 0$

If possible let $a \neq 0$ then a^{-1} exists. [$\because$ F is a field so every non-zero element of F has a multiplicative inverse]

Now, $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1} \cdot 0$

$\Rightarrow (a^{-1}a)b = 0$

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0$

Similarly, $ab = 0$, $b \neq 0$

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

$\Rightarrow a(bb^{-1}) = 0$

$\Rightarrow a \cdot 1 = 0$

$\Rightarrow a = 0$

Hence $ab = 0 \Rightarrow a = 0$ or $b = 0$

and therefore F has no zero divisors.

If the qst. is → Every field is an integral domain.

Then Extra two line.

Since every field is a commutative ring with unity, it follows that every field is an integral domain.

Note: If the integral domain is finite than it is a field.

Existence of zero divisors:

Consider matrices $A=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$ & $B=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\in$

Then $AB=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ which is

zero matrix. But both $A\neq\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ & $B\neq$

So after all those condition we can say

M is a non-commutative ring without unit

and with zero divisors.

$\therefore AB = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & ad \\ 0 & bd \end{pmatrix} \in M.$

Associative law: $\forall A, B, C \in M \Rightarrow (AB)C = A(BC)$

As matrix multiplication satisfy associative law.

So it satisfy that $(M, +, \cdot)$ is a ring.

→ Distributive law: ....

Non-commutativity: $\forall A, B \in M \quad AB \neq BA$ unless

$a = c = 0$ or $b = d = 0$

if $A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ $B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix}$ then $AB \neq BA$

So $AB = \begin{pmatrix} 0 & ad \\ 0 & bd \end{pmatrix}$ $BA = \begin{pmatrix} 0 & cb \\ 0 & bd \end{pmatrix}$

So $(M, +, \cdot)$ is a non commutative ring.

Ring with Unity check:

For a matrix multiplication the identity must be an identity matrix but in M there is no chance to build an identity matrix as $M = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ & $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

So $(M, +, \cdot)$ is ring without unity.

Identity Element: $\exists$ a matrix $E = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M$

s.t. $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$

Here E is the identity.

Inverse Element: $\forall \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \exists \begin{pmatrix} 0 & -a \\ 0 & -b \end{pmatrix}$ s.t.

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

Commutative Law: $\forall A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, $B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \in M$

s.t. $A+B = B+A$

As $A+B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} + \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & a+c \\ 0 & b+d \end{pmatrix}$

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

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

$= B+A.$

(2) $(M, \cdot)$ is a semi group.

Closure law: $\forall A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, $B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \in M$

Let $z_1 = a_1 + b_1\sqrt{2}$ s.t. $z_1 \cdot y = e$

$\Rightarrow (a_1 + b_1\sqrt{2}) \cdot y = 1$

$\Rightarrow y = \frac{1}{(a_1 + b_1\sqrt{2})} \in S$

$\therefore S$ is a field, as it satisfied all the conditions.

(H.W) Show that $M = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in R \right\}$ is a non-commutative ring without unity and with zero divisors.

Soln: ① $(M, +)$ is an abelian group.

Closure law: Let $A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ & $B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix}$ be two matrices from the set M then

$$(A+B) = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} + \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & a+c \\ 0 & b+d \end{pmatrix} \in M.$$

Associative law: Let $A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, $B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix}$, $C = \begin{pmatrix} 0 & e \\ 0 & f \end{pmatrix} \in M$

Then $(A+B)+C = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} + \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \right\} + \begin{pmatrix} 0 & e \\ 0 & f \end{pmatrix}$

$$= \begin{pmatrix} 0 & a+c \\ 0 & b+d \end{pmatrix} + \begin{pmatrix} 0 & e \\ 0 & f \end{pmatrix}$$

$$= \begin{pmatrix} 0 & a+c+e \\ 0 & b+d+f \end{pmatrix} = \begin{pmatrix} 0 & a+(c+e) \\ 0 & b+(d+f) \end{pmatrix} = A+(B+C)$$

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

④ $(S, +, \cdot)$ is a commutative ring!

$\forall x, y \in S \Rightarrow xy = yx$

Let $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2} \in S$

$$\therefore xy = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$$

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

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

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

$$\therefore xy = yx$$

⑤ $(S, +, \cdot)$ is a ring with unity.

$\forall x \in S, \exists\ e \in S \Rightarrow x \cdot e = e \cdot x = x$

Let $x = a_1 + b_1\sqrt{2} \in S$.

$$x \cdot e = x$$

$$\Rightarrow (a_1 + b_1\sqrt{2}) \cdot e = (a_1 + b_1\sqrt{2})$$

$$\Rightarrow e = 1$$

⑥ Every non-zero element has multiplicative inverse

$\forall x \in S, \exists\ y \in S \Rightarrow xy = e \quad (e = 1)$

Associative Law: $\forall x, y, z \in S \Rightarrow (xy)z = x(yz)$

Let $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2}$, $z = a_3 + b_3\sqrt{2} \in S$

$$(xy)z = \{(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})\}(a_3 + b_3\sqrt{2})$$

$$= \{(a_1a_2 + 2b_1b_2) + \sqrt{2}(a_1b_2 + a_2b_1)\}(a_3 + b_3\sqrt{2})$$

$$= (a_1a_2a_3 + 2b_1b_2a_3) + 2(a_1b_2 + a_2b_1)b_3 + [(a_1b_2 + a_2b_1)a_3 + (a_1a_2 + 2b_1b_2)a_3]\sqrt{2}$$

Similarly,

$$x(yz) = (a_1 + b_1\sqrt{2})\{(a_2 + b_2\sqrt{2})(a_3 + b_3\sqrt{2})\}$$

$$= (a_1a_2 + 2b_1b_2)a_3 + 2(a_1b_2 + a_2b_1)b_3 + [(a_1b_2 + a_2b_1)a_3 + (a_1a_2 + 2b_1b_2)a_3]\sqrt{2}.$$

③ Distributive Law:

I Left Distributive Law: $\forall x, y, z \in S$

$$x \cdot (y + z) = xy + xz$$

Let $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2}$, $z = a_3 + b_3\sqrt{2} \in S$

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

$$= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2})(a_3 + b_3\sqrt{2})$$

$$= xy + xz$$

Similarly we can prove the right distributive law.

Inverse Element: $\forall x \in S \Rightarrow \exists$ an element $-x \in S$

s.t. $x + (-x) = (-x) + x = e$

Let, $x = a_1 + b_1\sqrt{2} \in S$ then $-x = -a_1 - b_1\sqrt{2} \in$

$\therefore x + (-x) = a_1 + b_1\sqrt{2} + (-a_1 - b_1\sqrt{2}) = 0 = e.$

Commutative Law: $\forall x, y \in S \Rightarrow x + y = y + x$

Let $x = a_1 + b_1\sqrt{2} \in S$ $y = a_2 + b_2\sqrt{2} \in S$

$\therefore x + y \Rightarrow a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}$

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

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

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

② $(S, \cdot)$ is semigroup

closure law: $\forall x, y \in S \Rightarrow x \cdot y \in S$

Let $x = a_1 + b_1\sqrt{2}$ & $y = a_2 + b_2\sqrt{2} \in S$

Then $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + \sqrt{2}(a_1b_2 + a$

Here, $a_1a_2 + 2b_1b_2 \in S$ & $a_1b_2 + a_2b_1 \in S$

Let $a_1 + a_2 + 2b_1b_2 = a_3$ $a_1b_2 + a_2b_1 = b_3$

$\therefore a_3 + b_3\sqrt{2} \in S.$

(HW) Show that $S = \{a+b\sqrt{2} : a, b \in \mathbb{R}\}$ is a field.

Soln: ① $(S, +)$ is an abelian group

Commutative law: $\forall\, x, y \in S$ s.t. $x+y \in S$

Let $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2}$

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

$\because a_1, a_2 \in \mathbb{R} \Rightarrow a_1+a_2 \in \mathbb{R}$

& $b_1, b_2 \in \mathbb{R} \Rightarrow b_1+b_2 \in \mathbb{R}$

Let $a_1+a_2 = a_3 \in S$ $\quad b_1+b_2 = b_3 \in S$

then $a_3 + b_3\sqrt{2} \in S$.

Associative law: $\forall\, x, y, z \in S \Rightarrow (x+y)+z = x+(y+z)$

Let $x = a_1+b_1\sqrt{2}$, $y = a_2+b_2\sqrt{2}$, $z = a_3+b_3\sqrt{2}$

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

$= (a_1+a_2+a_3) + (b_1+b_2+b_3)\sqrt{2}$

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

$= (a_1+a_2+a_3) + (b_1+b_2+b_3)\sqrt{2}$

Identity Element: $\forall\, x \in S \Rightarrow \exists\, e \in S$ s.t. $x+e = x$

Let $x = a_1+b_1\sqrt{2} \in S$ For $e = 0$

$\therefore (a_1+b_1\sqrt{2}) + (0+0\sqrt{2}) = a_1+b_1\sqrt{2} = x$.

& $(0+0\sqrt{2}) + (a_1+b_1\sqrt{2}) = a_1+b_1\sqrt{2} = x$.

⑤ Commutative Law for $\times_5$:

For any two element in R s.t. 2, 3 we have

$(2 \times_5 3) = 1$ & $(3 \times_5 2) = 1$

So $(R, +_5, \times_5)$ is a commutative ring.

⑥ $(R, +_5, \times_5)$ is a ring with unity:

$\exists\ 1 \in R$ such that $1 \times_5 2 = 2$ $\quad 1 \times_5 4 = 4$

$1 \times_5 3 = 3$ $\quad 1 \times_5 0 = 0$.

So $(R, +_5, \times_5)$ is ring with unity.

⑦ Multiplicative Inverse of every non zero element:

In R 1, 2, 3, 4 are non-zero elements.

1 has its multiplicative inverse 1

2 " " " 3

3 " " " 2

4 " " " 4

So after all these conditions we have proved that $(R, +_5, \times_5)$ is a field.

② R is closed under the operation $\times_5$ since if we build up the table we get,

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

So R is closed under $\times_5$.

③ Associative law under the operation $\times_5$:

For any three element in R s.t 1, 2, 3 we get, $(1\times_5 2)\times_5 3 = 2\times_5 3 = 1$

$1\times_5 (2\times_5 3) = 1\times_5 1 = 1$

④ Distributive Law:

□ Left distributive Law: for any three element in R s.t. 1, 2, 3 we have

$1\times_5 (2+5 3) = 1\times_5 0 = 0$

& $(1\times_5 2)+_5 (1\times_5 3) = 2+_5 3 = 0$

□ Right distributive Law: For 2, 3, 4 in R we get

$(2+_5 3)\times_5 4 = 0\times_5 4 = 0$

$(2\times_5 4)+_5 (3\times_5 4) = 3+_5 2 = 0$.

+5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

if a, b any element belongs to R then from the table; $a +_5 b \in R$ as $1 +_5 2 = 3 \in R$.

Associative law: $\forall a, b, c \in R$, $(a +_5 b) +_5 c = a +_5 (b +_5 c)$

$(1 +_5 2) +_5 3 = 3 +_5 3 = 1$

$1 +_5 (2 +_5 3) = 1 +_5 0 = 1$

Identity Element: $\exists\, 0 \in R$ s.t. $1 +_5 0 = 1$, $2 +_5 0 = 2$, $3 +_5 0 = 3$, $4 +_5 0 = 0$, $0 +_5 0 = 0$ so 0 is the identity element.

Inverse Element: From the tables every element has its inverse. Inverse of 0 is 0, 1 is 4, 2 is 3, 3 is 2, 4 is 1.

Commutative Law: Any two element 1, 2 we get $1 +_5 2 = 3$ & $2 +_5 1 = 3$ which satisfied commutative

Similarly we can show that, $(a*b)\circ c = (a\circ c)*(b\circ c)$.

$\therefore (\mathbb{Z}, *, \circ)$ is a ring.

⑤ Commutative law: $\forall a, b \in \mathbb{Z}$, $(a\circ b) = a+b-ab$

$= b+a-ba$ [$\because (\mathbb{Z},+)$ is a commutative ring]

$= (b\circ a)$

So, $(\mathbb{Z}, *, \circ)$ is a commutative ring.

⑥ $(\mathbb{Z}, *, \circ)$ is ring with Unity:

Let e be the unity element in $(\mathbb{Z}, *, \circ)$

So, for each $a \in \mathbb{Z} \Rightarrow a\circ e = e\circ a = a$

$\Rightarrow a+e-ae = a$

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

$\Rightarrow e = \frac{0}{1-a} = 0 \in \mathbb{Z}$ [$\because a \neq 1$]

So 0 is the unity element in $(\mathbb{Z}, *, \circ)$.

H.W. Consider the algebric structure, $(R = \{0,1,2,3,4\}, +_5, \times_5)$ show that R is a field.

Soln: ① $(R, +_5)$ is an abelian group.

Closure law: If we build up the table for $+_5$ then we get,

② $\mathbb{Z}$ is closed under the operation $\circ$

Since $\forall a, b \in \mathbb{Z} \Rightarrow a \circ b = a+b-ab \in \mathbb{Z}$

So, $\mathbb{Z}$ is closed under $\circ$

③ Associative law under the operation $\circ$

$\forall a, b, c \in \mathbb{Z}$, $a \circ (b \circ c) = a \circ (b+c-bc)$

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

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

and $(a \circ b) \circ c = (a+b-ab) \circ c$

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

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

$\therefore a \circ (b \circ c) = (a \circ b) \circ c$

So $(\mathbb{Z}, \circ)$ is associative.

④ Distributive laws:

i) Left distributive law:

$\forall a, b, c \in \mathbb{Z}$, $a \circ (b * c) = a \circ (b+c-1)$

$= a+b+c-1-a(b+c-$

$= a+b+c-1-ab-ac$

$= 2a+b+c-1-ab-$

Again, $(a \circ b) * (a \circ c) = (a+b-ab) * (a+c-ac)$

$= a+b-ab+a+c+ac-1$

$= 2a+b+c-1-ab-ac$

$\therefore a \circ (b * c) = (a \circ b) * (a \circ c)$ $\forall a, b, c \in \mathbb{Z}$

27.08.2023

Q① Let $\mathbb{Z}$ be the set of all integers. Two operation $*$ and $\circ$ are defined as, $a*b = a+b-1$ & $a\circ b = a+b-ab$ $\forall a, b \in \mathbb{Z}$. Prove that the algebric system $(\mathbb{Z}, *, \circ)$ is a commutative ring with unity.

Q② Let R be a ring with unity. Two operations, $*$ and $\circ$ are defined on R

$a*b = a+b+1$ & $a\circ b = a+b+ab$, $\forall a, b \in R$

Prove that the algebric system $(R, *, \circ)$ is a commutative ring with unity.

Soln①: ① $(\mathbb{Z}, *)$ is an abelian group

Closure law: $\forall a, b \in \mathbb{Z}$ s.t. $a*b = a+b-1 \in \mathbb{Z}$

Associative law: $\forall a, b, c \in \mathbb{Z}$ s.t. $(a*b)*c = (a*b)+c-1$

$= a+b-1+c-1$

$= a+(b+c-1)-1$

$= a*(b*c)$

Identity Element: $\exists\, 1 \in \mathbb{Z}$ s.t. $a*1 = a+1-1 = a$

Inverse Element: $\exists b \in \mathbb{Z}$ s.t. $a*b = 1$

$\Rightarrow a*b-1 = 1$

$\Rightarrow b = (2-a) \in \mathbb{Z}$

Commutative law: $\forall a, b \in \mathbb{Z}$ s.t. $a*b = a+b-1$

$= b+a-1$

$= b*a.$

Thm: Prove that a field has no zero divisors.

Or,

Prove that every field is an integral domain.

(H.W)

Proof: Let R be a field. Then it is a commutative ring with unity and every non-zero element in R has a multiplicative inverse.

Let $a, b \in R$ such that $ab = 0$ & if possible, let $a \neq 0$.

Then a^{-1} exists and therefore, in this case,

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

$$\Rightarrow eb = 0$$

$$\Rightarrow b = 0$$

Thus $ab = 0, a \neq 0 \Rightarrow b = 0$.

Similarly $ab = 0,\ b \neq 0 \Rightarrow a = 0$

Hence R is without zero divisors.

③ $(-a)(-b) = ab$

Let, $-b = c$

$\therefore (-a)(-b) = (-a)\cdot c$

$= -(ac)$ by ②

$= -(a(-b))$

$= -(-ab)$ by ②

$= ab$

Thm: Prove that a ring $(R, +, \cdot)$ is without zero divisors iff the cancellation laws hold in it.

Proof: Let R is without zero divisors.

Suppose $a, b, c \in R$ s.t. $a \neq 0$, $ab = ac$.

Then $ab - ac = 0$, $a \neq 0 \Rightarrow a(b-c) = 0$, $a \neq 0$

$\Rightarrow b - c = 0$ [$\because$ R is without zero divisor & $a \neq 0$]

$\Rightarrow b = c$

Similarly, $a \neq 0$ and $ba = ca \Rightarrow b = c$

Thus cancellation laws holds in R.

Conversely, let cancellation laws hold in R.

Suppose $ab = 0$ & $a \neq 0$

Then $ab = a \cdot 0$ and $a \neq 0$

$\Rightarrow b = 0$ [by left cancellation law]

Similarly, $ab = 0$, $b \neq 0 \Rightarrow ab = 0 \cdot b$, $b \neq 0$

$\Rightarrow a = 0$ [by right cancellation law]

Thus $ab = 0 \Rightarrow a = 0$ or $b = 0$

Hence R is without zero divisors.

3. a divison ring which is not a field → $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

4. a non-commutative ring without unity → $M_n(\mathbb{R})$, ($n \times n$) matrix in

Endomorphism Rings.

23.08.2023

If $(R, +, \cdot)$ is a ring and $a, b, c \in R$ then prove that,

i) $a \cdot 0 = 0 \cdot a = 0$, $\forall a \in R$

ii) $a(-b) = (-a) \cdot b = -(ab)$, $\forall a, b \in R$

iii) $(-a)(-b) = ab$, $\forall a, b \in R$

① $0 + 0 = 0$

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

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

$\Rightarrow a \cdot 0 = 0$

② $a \cdot (-b) = -ab$

$b + (-b) = 0$

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

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

$\Rightarrow (-(ab) + ab) + a(-b) = -(ab) + 0$ [$\because a \cdot 0 = 0$]

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

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

Ring without Zero Divisors:

A ring $(R,+,\cdot)$ is said to be a ring without zero divisors if $ab=0 \Rightarrow a=0$ or $b=0$

$a\neq 0$ & $b\neq 0 \Rightarrow ab\neq 0$

Ex: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings without zero divisors.

#	Integral Domain	Divison Ring or Skew field	Field
Properties	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	set of all (2×2) matrix	$\mathbb{R}, \mathbb{Q}, \mathbb{C}$
Commutative	✓	✗	✓
Ring with Unity	✓	✓	✓
Without zero divisors	✓	✗	✗
Every non zero elements has a multiplicative inverse	✗	✓	✓

* All field is divison ring, but converse is not true.

Show that $S=\{a+b\sqrt{2} : a,b\in\mathbb{R}\}$ is a field.

Show that $M=\left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a,b\in\mathbb{R}\right\}$ is a non-commutative ring without unity and with zero divisors.

Give an example of

1. a commutative ring with unity → $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. a non " " " → set of all (2×2) matrix in $\mathbb{R}$

* Set of $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ is a Ring but $\mathbb{N}$ is not.

* None commutative Ring is Matrix multiplication.

* Set of even integer is not ring with unity.

$E = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$S = \{ma : a \in \mathbb{Z}\}$

$m \neq 1$ and fixed positive integer.

22.08.2023

* The smallest ring is 0 or $R = \{0\}$.

* $R, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$ without 0 divisor.

Commutative Ring:

A ring $(R, +, \cdot)$ is said to be commutative if

$\forall a, b \in R \Rightarrow ab = ba$.

Ring with Unity:

A ring $(R, +, \cdot)$ is said to be a ring with unity if $\exists\ 1 \in R$ s.t. $1 \cdot a = a$, $\forall a \in R$.

Ring with zero Divisors:

A ring $(R, +, \cdot)$ is said to be ring with zero divisors if $\exists\ a \neq 0,\ b \neq 0 \in R$ s.t. $ab = 0$

Ex: $M = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}\right\}$ is a ring with zero

16.08.2023

#Ring: An algebraic system $(R, +, \cdot)$ with a non-empty set R and two binary operations, addition $(+)$ and multiplication $(\cdot)$ is said to be a ring if the following properties are satisfied:

1. $(R,+)$ is an abelian group:

A1: Closure law for addition: $\forall a, b \in R \Rightarrow a+b \in R$

A2: Associative " " " : $\forall a, b, c \in R \Rightarrow (a+b)+c = a+(b+c)$

A3: Existance of additive identity: $\exists 0 \in R$ s.t. $a+0 = 0+a = a \quad \forall a \in R$

A4: Existance of inverse addition: $\forall a \in R \; \exists -a \in R$ s.t. $a+(-a) = -a+a = 0$

A5: Commutative Law: $\forall a, b \in R \Rightarrow a+b = b+a$

2. R is closed under multiplication:
that is $\forall a, b \in R \Rightarrow a \cdot b \in R$

3. $(R, \cdot)$ is associative: that is, $\forall a, b, c \in R \Rightarrow (ab)c = a(bc)$

4. $(R, +, \cdot)$ is distributive: that is, (i) $a(b+c) = ab + ac \quad \forall a, b, c \in R$
[Left distributive law]

(ii) $(a+b)c = ac + bc \quad \forall a, b, c \in R$
[Right distributive Law]

* যদি 1 থাকে অর্থাৎ multiplicative identity থাকে তাকে Ring with unity বলে।

* যদি multiplicative commutative hold করে তাকে Commutative Ring.

Example: 0 is a Ring. [only one element 0].