(1) Algebra, Dr Satish Kumar

Q(1) Let Define an ideal of a commutative ring. Give one example.

Ans. Let $(R, +, \cdot)$ be a commutative ring.

Let $S \subseteq R$ then S is called an ideal if

(1) $(S, +)$ is a subgroup of R

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

(2) Let $r \in R$, $s \in S$ then $rs \in S$ and $sr \in S$ $\forall r \in R$ and $\forall s \in S$.

Example: $(I, +, \cdot)$ is a ring, $(2I, +, \cdot)$ is an ideal of $(I, +, \cdot)$.

Q2. If U is an ideal of a ring R with unity and $1 \in U$ then prove $U = R$

Ans Let U be an ideal of a ring R.

Let $1 \in U$.

To prove $U = R$

Clearly $U \subseteq R$ —— (1)

To prove $R \subseteq U$

Let $x \in R, 1 \in U \Rightarrow x.1 \in U$ [$\because U$ is an ideal of R]

$\Rightarrow x \in U$

$\Rightarrow x \in R \Rightarrow x \in U$

$\Rightarrow R \subseteq U$ —— (2)

from (1) and (2) $R = U$.

Q3. For any given element a of a commutative ring R.

Let $Ra = \{xa \mid x \in R\}$

Prove Ra is an ideal of a ring R.

Ans. Let $(R, +, \cdot)$ be a ~~ring~~ commutative ring.

Let $a \in R$ then

To prove $Ra = \{xa \mid x \in R\}$ is an ideal.

Let $\alpha \in Ra \Rightarrow \alpha = x_1 a$, $\forall x_1 \in R$

$\beta \in Ra \Rightarrow \beta = x_2 a$, $\forall x_2 \in R$

$\Rightarrow \alpha - \beta = x_1 a - x_2 a = (x_1 - x_2) a \in Ra$

$\Rightarrow (\alpha - \beta) \in Ra \Rightarrow (Ra, +)$ is a subgroup of R.

Let $r \in R$, $\alpha \in Ra \Rightarrow \alpha = x_1 a$, $\forall x_1 \in R$.

then $r\alpha = r(x_1 a) = (r x_1) a \in Ra$

and $\alpha r = (x_1 a) r$

$= x_1 (a r)$ Associatively

$= x_1 (r a)$ (Commutativity)

$\alpha r = (x_1 r) a \in Ra$ (Associativity)

$\therefore$ $r\alpha$ and $\alpha r \in Ra$

$\therefore$ Ra is an ideal of a ring

Q 4. Prove that a field has no proper ideals.

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

To prove F has no proper ideals.

Let S be an ideal of a field R

then two cases arise.

(1) $S = (0)$ (2) $S \neq (0)$

if $S = (0) \Rightarrow S$ is not proper ideals.

(2) if $S \neq (0)$

Let $0 \neq a \in S \Rightarrow a^{-1} \in S \Rightarrow a^{-1} \in F$ [$\because S \subseteq F$]

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

$\Rightarrow 1 \in S$ [$\because a a^{-1} = 1$]

Now,

$x \in F, 1 \in S \Rightarrow x \cdot 1 \in S$ [~~$x \in S$~~

$\Rightarrow x \in S$ [$\because S$ is an ideal]

$\Rightarrow x \in F \Rightarrow x \in S$

$\Rightarrow F \subseteq S$

But $S \subseteq F$

$\Rightarrow S = F$

$\Rightarrow$ S is not proper ideal

$\therefore$ F has no proper ideals.

(5) A commutative ring with unity is a field if it has no proper ideals.

2018

Proof. Let $(R, +, \cdot)$ be a commutative ring with unity.

Let R has no proper ideals

To prove $(R, +, \cdot)$ is a field

We know if ~~$a \in R$ then~~ $0 \neq a \in R$

$Ra = \{xa \mid x \in R\}$ is an ideal of R

Since let $d \in Ra \Rightarrow d = xa$

$\Rightarrow d = a$ if $x = 1 \in R$

$\Rightarrow a \in Ra$ & $0 \neq a \in R$

Now, $0 \neq a \in Ra \Rightarrow Ra \neq (0)$

$\Rightarrow Ra = R$ [$\because R$ has no proper ideals]

$\Rightarrow$ Elements of R are multiple of a

let $R = \{r_1 a, r_2 a, r_3 a, r_4 a, \ldots\}$

Since $1 \in R \Rightarrow \exists\, r_i a \in R$ for some i

such that $r_i a = 1$

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

$\Rightarrow$ multiplicative inverse of a is r_i

$\Rightarrow (R, +, \cdot)$ is a field. proved.

Q6 Define Principal ideal. Give example of it.

Ans An ideal S of a ring R is said to be principle ideal if there exist an element a of S such that any ideal T containing a contains S.

Note. Any ideal generated by its element is called principle ideal.

Ex. $(I, +, \cdot)$ is a ring, $S \in I$ then $S = \{sa \mid a \in I\}$ is principal ideal.

$S = \{5a \mid a \in I\}$

$S = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$

$\Rightarrow S = (5)$ is principle ideal

since S is generated by its element namely 5, and $5 \in S$.

<u>Theorem.</u> Prove that the ring of integers is a principal ideal ring.

Proof. Let $(I, +, \cdot)$ be a ring of integers

Now I will be principal ideal of every ideal of I is a principal ideal.

Let S be an ideal of I

than two cases arise:

(1) $S = (0)$ (2) $S \neq (0)$

<u>case (1)</u> $S = (0) \Rightarrow S$ is a principal ideal generated by 0 element and $0 \in S$.

<u>case (2)</u> Let $S \neq (0)$

Let $0 \neq a \in S \Rightarrow -a \in S$

Let S^+ = set of all positive numbers

Let $\Rightarrow \exists$ least positive number say $s \in S^+$ (by well ordering principal)

$\Rightarrow s \in S$ [$\because S^+ \subseteq S$]

Let $n \in S$, $s \in S \Rightarrow$ by division algorithm

$\exists\, q \in I$, $r \in I$ such that

$n = sq + r$ where $0 \leq r < s$

Now $s \in S, q \in I \Rightarrow sq \in S$ [$\because S$ is an ideal of I]

$\Rightarrow -sq \in S$ [$(S, +)$ is a subgroup]

Now, $n \in S$, $-sq \in S \Rightarrow (n - sq) \in S \Rightarrow r \in S$ [$\because n - sq = r$]

Now, $r \in S$ & $r < s$

$\Rightarrow r$ must be zero [$\because s$ is least]

$\therefore n = sq \Rightarrow$ elements of S are multiple of s

$\Rightarrow S = (s)$ [$\because S$ is generated by its element s & $s \in S$]

$\Rightarrow S$ is principal ideal.

ii $(I, +, \cdot)$ is a principal ideal
[$\because$ S was arbitrary].

<u>Theorem.</u> Prove that a polynomial domain $F[x]$ over a field F is a principal ideal ring.

Proof. Let $\{F(x), +, \cdot\}$ be a polynomial domain over a field F.

To prove $F(x)$ is a principal ideal ring
We shall prove its every ideal is a principal ideal.

Let S be an ideal of $F(x)$
then two cases arise (1) $S = (0)$ (2) $S \neq (0)$

<u>case</u> (1) If $S = (0)$ i.e S is generated by zero polynomial
$\Rightarrow$ S is a principal ideal

<u>Case (2)</u> If $S \neq (0)$ $\Rightarrow \exists$ non-zero polynomial say $g(x) \in S$
let $\deg g(x)$ is lowest

Let $f(x) \in S$, let $g(x) \in S$ then by division algorithm $\exists$ $q(x) \in F(x)$ and $r(x) \in F(x)$ such that
$f(x) = g(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Now, $g(x) \in S$, $q(x) \in F(x) \Rightarrow g(x)q(x) \in S$
[$\because$ S is an ideal]
$\Rightarrow -g(x)q(x) \in S$
[$\because$ S is a subgroup]

Now, $f(x) \in S$, $-g(x)q(x) \in S$
$\Rightarrow [f(x) - g(x)q(x)] \in S$
$\Rightarrow r(x) \in S$ [$\because r(x) = f(x) - g(x)q(x)$]

Now $r(x) < g(x)$ & $\deg g(x)$ is lowest.
$\Rightarrow r(x)$ must be ~~of~~ zero polynomial
$\Rightarrow f(x) = g(x)q(x)$

$\Rightarrow$ Elements of S will be multiple of $g(x)$

i.e. $S = (g(x))$ and $g(x) \in S$

$\Rightarrow$ S will be ~~an~~ principal ideal

& S is arbitrary

$\therefore$ Every ideal of $F(x)$ is principal ideal

$\Rightarrow [F(x), +, \cdot]$ is a principal ideal ring.

<u>Theorem</u>, Let F be a field and $f(x)$ and $g(x)$ be any two polynomials in $F(x)$, not both of which are zero. Then $f(x)$ and $g(x)$ have a greatest common divisor $d(x)$ which can be expressed in the form

$$d(x) = m(x) f(x) + n(x) g(x) \text{ where } m(x), n(x) \in F(x).$$

Proof. Let $[F(x), +, \cdot]$ be a polynomial domain over the field F.

Let $0 \neq f(x), 0 \neq g(x) \in F(x)$

then to prove $f(x)$ and $g(x)$ have greatest common divisor $d(x)$ such that

$$d(x) = m(x) f(x) + n(x) g(x), \text{ where } m(x), n(x) \in F(x)$$

Suppose we claim

$$S = \{ s(x) f(x) + t(x) g(x) \mid s(x), t(x) \in F(x) \} \quad \text{--- (1)}$$

is an ideal of $F(x)$

Now we shall prove S is an ideal of $F(x)$

Let $\alpha(x) \in S, \beta(x) \in S \Rightarrow \alpha(x) = s_1(x) f(x) + t_1(x) g(x)$

and $\beta(x) = s_2(x) f(x) + t_2(x) g(x)$

where $s_1(x), s_2(x), t_1(x), t_2(x) \in F(x)$

$\therefore [\alpha(x) - \beta(x)] = [s_1(x) - s_2(x)] f(x) + [t_1(x) - t_2(x)] g(x)$

$\Rightarrow [\alpha(x) - \beta(x)] \in S$ as $[s_1(x) - s_2(x)], [t_1(x) - t_2(x)] \in F(x)$.

Let $c(x) \mid g(x) \Rightarrow c(x) \mid n(x) g(x)$ —— (5)

(4) & (5) $\Rightarrow$

$$c(x) \mid [m(x) f(x) + n(x) g(x)]$$

$$\Rightarrow c(x) \mid d(x) \quad \text{—— (6)}$$

$$[\because d(x) = m(x) f(x) + n(x) g(x)]$$

$\therefore$ $d(x)$ is a g.c.d of $f(x)$ and $g(x)$ such that

$$d(x) = m(x) f(x) + n(x) g(x)$$, proved.

<u>Theorem.</u> Let $f(x)$, $g(x)$ and $h(x) \in F(x)$, polynomial domain over field F. If $f(x) \mid g(x) h(x)$ and g.c.d of $f(x)$, $g(x)$ is 1 then $f(x) \mid h(x)$

Proof. Let $\{F(x), +, \cdot\}$ be a polynomial domain over F

Let $f(x), g(x), h(x) \in F(x)$

Let g.c.d of $f(x)$ and $g(x)$ is 1

then $\exists\ m(x), n(x) \in F(x)$ such that

$$1 = m(x) f(x) + n(x) g(x) \quad \text{—— (1)}$$

Also given $f(x) \mid g(x) h(x)$

$\Rightarrow \exists\ k_1(x) \in F(x)$ such that

$$g(x) h(x) = f(x) k_1(x) \quad \text{—— (2)}$$

multiplying ~~h(x)~~ (1) by $h(x)$, we get

$$h(x) = m(x) f(x) h(x) + n(x) \underline{g(x) h(x)}$$

$$\Rightarrow h(x) = m(x) f(x) h(x) + n(x) \cdot f(x) k_1(x) \quad [\text{by } (2)]$$

$$\Rightarrow h(x) = f(x) [m(x) h(x) + n(x) k_1(x)]$$

$\Rightarrow f(x) \mid h(x)$, proved.

Theorem. If $f(x)$ is an irreducible polynomial in $F(x)$ for a field F and $f(x) \mid g(x)h(x)$ where $g(x), h(x) \in F(x)$ then $f(x)$ divides atleast one of $g(x)$ or $h(x)$.

Proof. Let $(F(x), +, \cdot)$ be a polynomial domain over field F.

Let $f(x)$ be irreducible polynomial in $F(x)$

Let $f(x) \mid g(x)h(x)$

Then two cases arise

(1) $[f(x), g(x)] = 1 \Rightarrow f(x) \mid h(x)$

(2) $[f(x), h(x)] = 1 \Rightarrow f(x) \mid g(x)$, proved.

Theorem. State and prove unique factorization Theorem

Statement. Let $\{F(x), +, \cdot\}$ be a polynomial domain over field F. Let $0 \neq f(x) \in F(x)$ then either $f(x)$ is unit or $f(x) = a\, p_1(x)\, p_2(x) \cdots p_m(x)$ where each $p_i(x)$, $1 \leq i \leq m$ is an irreducible polynomial in $F(x)$ and $a \in F$ is the leading coefficient of $f(x)$.

Also the above representation is unique except for the order.

Proof. Let $\{F(x), +, \cdot\}$ be a polynomial domain over a field F.

Let $0 \neq f(x) \in F(x)$ then to prove

(1) Either $f(x)$ is unit or

(2) $f(x) = a\, p_1(x)\, p_2(x) \cdots p_m(x)$

where each $p_i(x)$ is irreducible polynomial and this representation is unique

We shall prove this theorem by mathematical induction

(1) If $f(x)$ is unit we are nothing to prove

(2) If $\deg f(x)$ is one

i.e let $f(x) = ax + b$

$\Rightarrow f(x) = a[x + a^{-1}b]$

$f(x) = a f_1(x)$ where a is leading coefficient

$\Rightarrow$ theorem is true in this case.

Now, Suppose the theorem is true for all polynomials each of whose degree is less than degree of $f(x)$. then we shall prove it will be also true for $f(x)$.

(i) If $f(x)$ is irreducible we are nothing to prove

(ii) If $f(x)$ is not irreducible

$\Rightarrow \exists\ g(x) \in F(x),\ h(x) \in F(x)$ such that

$f(x) = g(x)h(x)$ where neither $g(x)$ is unit nor $h(x)$ is unit and degree of $g(x) < \deg f(x)$

degree of $h(x) < \deg f(x)$

$\because$ degree of $g(x) < \deg f(x)$

$\Rightarrow g(x) = c\,\alpha_1(x)\alpha_2(x) \ldots\ldots \alpha_s(x)$ where each $\alpha_i(x)$ is prime

c is leading coefficient (c by supposition)

Also

$h(x) = d\,\beta_1(x)\beta_2(x) \ldots \beta_t(x)$ where each $\beta_j(x)$ is prime & d is leading coefficient (c by supposition)

$\Rightarrow g(x)h(x) = cd\,\alpha_1(x)\alpha_2(x) \ldots \alpha_s(x)\beta_1(x) \ldots \beta_t(x)$

$\Rightarrow f(x) = cd\,\alpha_1(x)\alpha_2(x) \ldots \alpha_s(x)\beta_1(x) \ldots \beta_t(x)$

$\Rightarrow f(x) = a\,\alpha_1(x)\alpha_2(x) \ldots \alpha_s(x)\beta_1(x) \ldots \beta_t(x)$ [where $a = cd$]

So theorem is proved

<u>Uniqueness.</u> Suppose $f(x)$ has two different representations namely

$f(x) = a\,p_1(x)p_2(x) \ldots p_m(x)$ —— (1)

$f(x) = a\,q_1(x)q_2(x) \ldots q_n(x)$ —— (2)

(1) & (2) $\Rightarrow$

$$p_1(x)\,p_2(x)\cdots p_m(x) = q_1(x)\,q_2(x)\cdots q_n(x) \quad \text{--- (3)}$$

Suppose

$$p_1 \mid p_1(x)\,p_2(x)\cdots p_m(x)$$

$$\Rightarrow p_1 \mid q_1(x)\,q_2(x)\cdots q_n(x) \quad \text{--- (from (3))}$$

Let $p_1 \mid q_1(x) \Rightarrow q_1(x) = u\,p_1(x)$ --- (4)

$\Rightarrow$ ~~(4) $\Rightarrow$~~

~~$p_1 \mid u\,p_1(x)\,q_2(x)\,q_3(x)\cdots q_n(x)$~~

put $q_1(x) = u\,p_1(x)$ in (3)

$$\cancel{p_1(x)}\,p_2(x)\cdots p_m(x) = u_1\,\cancel{p_1(x)}\,q_2(x)\cdots q_n(x) \quad \text{--- (5)}$$

Again $p_2(x) \mid p_2(x)\,p_3(x)\cdots p_m(x)$

$\Rightarrow p_2(x) \mid u_1 q_2(x)\,q_3(x)\cdots q_n(x)$ by (5)

Let $p_2(x) \mid q_2(x) \Rightarrow q_2(x) = u_2\,p_2(x)$ --- (6)

$\therefore$ (5) & (6) $\Rightarrow$

$$\cancel{p_2(x)}\,p_3(x)\cdots p_m(x) = u_1 u_2\,\cancel{p_2(x)}\,q_3(x)\cdots q_n(x)$$

$$\Rightarrow p_3(x)\,p_4(x)\cdots p_m(x) = u_1 u_2\,q_3(x)\cdots q_n(x)$$

After m steps (if $m < n$), we have

$$1 = u_1 u_2 \cdots u_m\,q_{m+1}\,q_{m+2}\cdots q_n(x)$$

which is not possible

$\Rightarrow n \le m$ --- (7) $[\because m \ne n]$

Interchanging the role of m & n, we have

$m \le n$ --- (8)

(7) & (8) $\Rightarrow m = n$

$\therefore$ representation is unique. Hence the theorem

Let $r(x) \in F(x)$

$\alpha(x) \in S$ then $\alpha(x) = s_1(x) f(x) + t_1(x) g(x)$, $s_1(x), t_1(x) \in F(x)$

Now

$r(x)\alpha(x) = r(x)[s_1(x) f(x) + t_1(x) g(x)]$

$= [r(x) s_1(x)] f(x) + [r(x) t_1(x)] g(x)$

$\Rightarrow r(x)\alpha(x) \in S$ as $r(x)s_1(x), r(x)t_1(x) \in F(x)$.

$\therefore$ S is an ideal of $f(x)$

Now since every ideal is ~~an~~ principal ideal of $f(x)$

$\therefore$ S is a ~~principle~~ principal ideal $\Rightarrow \exists\, d(x) \in S$ such that

~~$d(x) = m(x)$~~

every element of S is a multiple of $d(x)$.

Since $d(x) \in S \Rightarrow \exists\, m(x) \in F(x), n(x) \in F(x)$ such that

$d(x) = m(x) f(x) + n(x) g(x)$

Now ~~put $s(x) = 1, t(x) = 0$ in (1) $\Rightarrow$~~

(1) $\Rightarrow s(x) f(x) + t(x) g(x) \in S$

$\Rightarrow [1 \cdot f(x) + 0\, g(x)] \in S$ [put Take $s(x) = 1$, $t(x) = 0$]

$\Rightarrow f(x) \in S$

$\Rightarrow f(x)$ is a multiple of $d(x) \Rightarrow d(x) \mid f(x)$ —— (2)

Again (1) $\Rightarrow$ $[0 \cdot f(x) + 1 \cdot g(x)] \in S$ [Take $s(x) = 0$, $t(x) = 1$]

$\Rightarrow g(x) \in S \Rightarrow g(x)$ is a multiple of $d(x)$

$\Rightarrow d(x) \mid g(x)$ —— (3)

Let $c(x) \in F(x)$ such that

$c(x) \mid f(x) \Rightarrow c(x) \mid m(x) f(x)$ —— (4)