CH-05 (1) Algebra, Dr Satish Kumar

Theorem. Let S be an ideal of a ring R then $\frac{R}{S} = \{(S+a) \mid a \in R\}$ forms a ring with respect to "+" and "·" defined in $\frac{R}{S}$ as

(i) $S+a + S+b = S+a+b$ [Addition is binary in $\frac{R}{S}$]

(ii) $(S+a)\cdot(S+b) = S+ab$ [multiplication is binary in $\frac{R}{S}$,

"+" is associative Let $S+a_1, S+a_2, S+a_3 \in \frac{R}{S}$, $a_1, a_2, a_3 \in R$

To show

$$\{(S+a_1)+(S+a_2)\}+(S+a_3) = (S+a_1)+\{(S+a_2)+(S+a_3)\}$$

$$\begin{aligned}
LHS &= \{(S+a_1)+(S+a_2)\}+(S+a_3) \\
&= [S+(a_1+a_2)]+(S+a_3) \\
&= S+(a_1+a_2)+a_3 \\
&= S+a_1+(a_2+a_3) \quad [\because (a_1+a_2)+a_3 = a_1+(a_2+a_3) \text{ in } R] \\
&= S+a_1+S+(a_2+a_3) \\
&= S+a_1+\{(S+a_2)+(S+a_3)\}
\end{aligned}$$

LHS = RHS

Existance of additive identity in $\frac{R}{S}$.

Let $(S+a) \in \frac{R}{S}$ then $\exists (S+0) \in \frac{R}{S}$ called zero identity in $\frac{R}{S}$ such that

$$\begin{aligned}
S+a+S+0 &= S+a+0 \\
&= S+a
\end{aligned}$$

$\Rightarrow (S+0)$ is zero identity in $\frac{R}{S}$. [Note. $S+0=S$]

Existance of additive inverse

Let $(S+0) \in \frac{R}{S}$ (zero identity). Let $(S+a) \in \frac{R}{S}$

Then $\{S+(-a)\} \in \frac{R}{S}$ called inverse of $(S+a)$ such that

$$\begin{aligned}
(S+a)+S+(-a) &= S+a+(-a) \\
&= S+a-a \\
&= S+0.
\end{aligned}$$

"+" is commutative. Let $(s+a), (s+b) \in \frac{R}{s}$, $a, b \in R$

then

To show $(s+a)+(s+b) = (s+b)+(s+a)$

$LHS = (s+a)+(s+b)$

$LHS = s+a+b$ $[\because a+b = b+a$, in $R]$

$LHS = s+b+a$

$LHS = (s+b)+(s+a)$

$LHS = RHS$

"$\cdot$" is binary. Let $(s+a), (s+b) \in \frac{R}{s}$

then $(s+a).(s+b) = (s+ab) \in \frac{R}{s}$ as $(a.b) \in R$

"$\cdot$" is associative. Let $(s+a), (s+b), (s+c) \in \frac{R}{s}$, $a, b, c \in R$

then To show $\{(s+a)(s+b)\}(s+c) = (s+a)\{(s+b)(s+c)\}$

$LHS = \{(s+a)(s+b)\}(s+c)$

$LHS = (s+ab)(s+c)$

$LHS = s+(ab)c$

$LHS = s+a(bc)$ $[\because (ab)c = a(bc)$ in $R]$

$LHS = (s+a)(s+bc)$

$LHS = (s+a)\{(s+b)(s+c)\}$

$LHS = RHS$

Distributive properties. Let $(s+a), (s+b), (s+c) \in \frac{R}{s}$, $a, b, c \in R$

To show

(i) $(s+a).[(s+b)+(s+c)] = (s+a).[s+b]+(s+a).(s+c)$

(ii) $[(s+b)+(s+c)](s+a) = (s+b).(s+a)+(s+c).(s+a)$

(i) $LHS = (s+a).[(s+b)+(s+c)$

$LHS = (s+a).[s+b+c]$

$LHS = s+a(b+c)$

$LHS = s+ab+ac$ — (1)

$RHS = (s+a).(s+b) + (s+a).(s+c)$

$RHS = (s+ab) + (s+ac)$

$RHS = s + ab + ac$ —— (2)

(1) and (2) $\Rightarrow$ $LHS = RHS$.

Similarly we can prove (ii) part.

Therefore, $\left\{\frac{R}{s}, +, \cdot\right\}$ is a ring.

Theorem. If f is a homomorphism of a ring R into a ring R' with kernel S, Then prove that S is an ideal of R

Proof. Let R and R' be any two rings.

Let $f: R \longrightarrow R'$ be homomorphism

Let S be the kernel of f then

$S = \{x \in R \mid f(x) = 0'$, $0'$ is identity element in $R'\}$

To show S is an ideal

Let $\alpha \in S \Rightarrow f(\alpha) = 0$

$\beta \in S \Rightarrow f(\beta) = 0$

To show $(\alpha - \beta) \in S$

$f(\alpha - \beta) = f[\alpha + (-\beta)]$

$f(\alpha - \beta) = f(\alpha) + f[-\beta]$ [$\because f$ is homomorphism]

$f(\alpha - \beta) = f(\alpha) - f(\beta)$

$f(\alpha - \beta) = 0' - 0'$

$f(\alpha - \beta) = 0'$

$\Rightarrow (\alpha - \beta) \in S \Rightarrow (S, +)$ is a subgroup.

CH-05 (4) Ring Dr. Satish Kumar

Let $r \in R$, $\alpha \in S \Rightarrow f(\alpha) = 0'$

To show $r\alpha$ and $\alpha r \in S$

$$f(r\alpha) = f(r) f(\alpha) = f(r) \cdot 0' = 0'$$

$\Rightarrow r\alpha \in S$

Again $f(\alpha r) = f(\alpha) f(r) = 0' \cdot f(r) = 0'$

$\Rightarrow \alpha r \in S$

$\therefore (S, +, \cdot)$ is an ideal of $(R, +, \cdot)$.

Theorem. State and prove fundamental theorem of homomorphism on rings.

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

Proof. Let R and R' be any two rings.

Let $f: R \longrightarrow R'$ be homomorphism

then $R' = \{ f(a) \mid a \in R \}$ be homomorphic image of R.

Let S be a kernel of f then

$S = \{ x \in R \mid f(x) = 0', \ 0' \text{ is zero identity in } R' \}$

then clearly S is an ideal of R.

$\Rightarrow \frac{R}{S} = \{ (S+a) \mid a \in R \}$ is a ring, called quotient ring

To show $\frac{R}{S} \cong R'$.

Define a new mapping

$$\phi : \frac{R}{S} \longrightarrow R' \text{ such That}$$

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

Clearly ϕ is well defined

To show ϕ is one-one. Let $(S+a), (S+b) \in \frac{R}{S}$

$\phi(S+a) = \phi(S+b) \Rightarrow f(a) = f(b)$

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

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

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

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

$\Rightarrow S+a = S+b$

$\Rightarrow \phi$ is one-one

To show ϕ is onto. Let $f(a) \in R'$ then $\exists (S+a) \in \frac{R}{S}$ such that $\phi(S+a) = f(a), \forall a \in R$.

$\Rightarrow \phi$ is onto.

To show
(i) $\phi[(S+a)+(S+b)] = \phi(S+a) + \phi(S+b)$
(ii) $\phi[(S+a)(S+b)] = \phi(S+a)\,\phi(S+b)$

(i) Let $S+a, S+b \in \frac{R}{S}$

$\phi[S+a+S+b] = \phi[S+a+b]$ $[\phi(S+a) = f(a)]$

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

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

$\phi[(S+a)+(S+b)] = \phi(S+a) + \phi(S+b)$

(ii) $\phi[(S+a)(S+b)] = \phi[S+ab]$ $[\because \phi(S+a) = f(a)]$

$\phi[(S+a)(S+b)] = f(ab)$ $[\because f$ is homomorphism$]$

$\phi[(S+a)(S+b)] = f(a)f(b)$ $[\because f(a) = \phi(S+a)$ etc$]$

$\phi[(S+a)(S+b)] = \phi(S+a)\cdot\phi(S+b)$

Therefore, ϕ is an isomorphism.

Hence $R' \cong \frac{R}{S}$, proved.

CH-05 (06) Ring Dr Satish Kumar

Q. Define maximal ideal

Ans An ideal S ($S \neq R$) in a ring R is called maximal ideal of R if there exists another ideal T of R such that

$$S \subseteq T \subseteq R$$

then either $T = S$ or $T = R$.

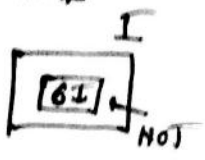
Example. (1) Let $(I, +, \cdot)$ be a ring then $(5I, +, \cdot)$ is maximal ideal of $(I, +, \cdot)$ as there exists no ideal T such that

$$5I \subseteq T \subseteq I.$$ [अर्थात 5I से बड़ा ideal व I से छोटा ideal exist नहीं करता]

Note. Because $\nexists$ no T containing $5I$.

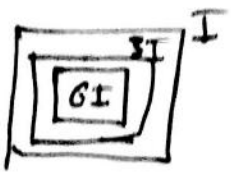
(2) $(I, +, \cdot)$ is a ring

$(6I, +, \cdot)$ is an ideal but not maximal



as $6I \subseteq 3I \subseteq I$

Here $3I$ contains ~~property~~ $6I$ property.



नोट: ex. (1) में $5I$ व I के बीच $5I$ को contain करने वाला कोई ideal exist नहीं करता जबकि ex. (2) में $6I$ को contain करने वाला $3I$ ideal exist करता है।

Theorem. An ideal S of the ring of integers I is maximal iff S is generated by some prime integer

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

Let S is an ideal generated by p, p is a prime

"If part" Suppose p is prime

To show $S = (p)$ is maximal

Let T be an ideal such that $S \subseteq T \subseteq I$

To prove either $T = S$ or $T = I$

Let $T = (q)$, q is some integer

Now $S \subseteq T \Rightarrow (p) \subseteq T$

Let $p \in S \Rightarrow p \in T$ $[\because S \subseteq T]$

$\Rightarrow p = rq$ $[\because T = (q) = \{rq \text{ for some integer } r\}]$

Since p is prime it means as S is prime $[S = 1 \times S$ OR $S = S \times 1]$

two cases arise

(1) $q = 1$

(2) $q = p$

(1) If $q = 1$

$\Rightarrow p = r$ i.e $T = I$

(2) If $q = p$ then $T = S$

$\therefore S \subseteq T \subseteq I \Rightarrow T = S$ or $T = I$

$\Rightarrow S$ is is maximal ideal.

<u>Only if part</u> Suppose $S = (p)$ is maximal

To prove p is prime

Suppose if possible p is not prime

then $\exists\ m, n \in I$ such that

$p = mn$ where neither $m \neq 1$ nor $n \neq 1$

Now, it is ~~obvious~~ obvious

$(p) \subseteq (m) \subseteq I$

$\Rightarrow$ Either $(m) = I$ or $(m) = (p)$.

(i) if $(m) = I \Rightarrow m = 1$ which is a contradiction

(ii) if $(m) = (p) \Rightarrow m$ is a multiple of p

$\Rightarrow m = lp$ for some $l \in I$

$\therefore p = mn$

$\Rightarrow p = lpn$

$\Rightarrow p(1 - ln) = 0$

$\Rightarrow 1 - ln = 0$ as $p \neq 0$ & I is without zero divisors

$\Rightarrow ln = 1$ which is a contradiction as $\exists$ no integers namely l & n whose product is 1.

$\therefore$ p must be prime.

Theorem. Let S_1 and S_2 be two ideals of a ring R

Let $S_1 + S_2 = \{ s_1 + s_2 \mid s_1 \in S_1, s_2 \in S_2 \}$

Then $(S_1 + S_2)$ is an ideal generated by $(S_1 \cup S_2)$

Proof. Let S_1 and S_2 be any two ideals of a ring R.

To prove $(S_1 + S_2)$ is an ideal generated by $(S_1 \cup S_2)$

We know

$$S_1 + S_2 = \{ (s_1 + s_2) \mid s_1 \in S_1, s_2 \in S_2 \}$$

Let $\alpha \in S_1 + S_2 \Rightarrow \alpha = a_1 + a_2$, $a_1 \in S_1$, $a_2 \in S_2$

$\beta \in S_1 + S_2 \Rightarrow \beta = b_1 + b_2$, $b_1 \in S_1$, $b_2 \in S_2$

Now, $\alpha - \beta = (a_1 - b_1) + (a_2 - b_2)$

$\Rightarrow (\alpha - \beta) \in (S_1 + S_2)$ as $(a_1 - b_1) \in S_1$, $(a_2 - b_2) \in S_2$

Now, Let $r \in R$, $\alpha \in (S_1 + S_2) \Rightarrow \alpha = a_1 + b_1$, $a_1 \in S_1$, $b_1 \in S_2$

$r\alpha = r(a_1 + b_1)$

$r\alpha = ra_1 + rb_1 \Rightarrow r\alpha \in (S_1 + S_2)$ as $ra_1 \in S_1$, $rb_1 \in S_2$

Similarly $\alpha r \in (S_1 + S_2)$

$\therefore (S_1 + S_2)$ is an ideal of a ring R.

Since $0 \in S_1$, $0 \in S_2$

$\Rightarrow S_1 \subseteq S_1 + S_2$

and $S_2 \subseteq S_1 + S_2$

$\Rightarrow S_1 \cup S_2 \subseteq (S_1 + S_2)$ $\left[\because \begin{matrix} A \subseteq C \\ B \subseteq C \end{matrix} \Big| \Rightarrow (A \cup B) \subseteq C \right]$

$\Rightarrow (S_1 + S_2)$ is the smallest ideal containing $S_1 \cup S_2$

as if S is an ideal containing $(S_1 \cup S_2)$

then S must contain $S_1 + S_2$ $(\because (S_1 \cup S_2) \subseteq (S_1 + S_2))$

$\therefore S_1 + S_2 = (S_1 \cup S_2)$, proved.

Theorem. An ideal S of a commutative ring R with unity is maximal iff the quotient ring $\frac{R}{S}$ is a field.

Proof. Let S be an ideal of a commutative ring R with unity.

"If part" suppose S is maximal

To prove $\frac{R}{S}$ is a field

We ~~have~~ know

$\frac{R}{S} = \{S+a \mid a \in R\}$ is a commutative ring with unit element as $S+1$. and zero element as S.

In order to prove $\frac{R}{S}$ is a field we shall prove every non zero element of $\frac{R}{S}$ has its multiplicative inverse.

Let $(S+b)$ be any non-zero element of $\frac{R}{S}$

$\Rightarrow S+b \neq S$ [$\because$ S is zero element of $\frac{R}{S}$]

$\Rightarrow b \notin S$

Let $T = (b)$ is principal ideal of R generated by b, $b \in T$.

$\Rightarrow S \subseteq (S+T)$ and $(S+T) \subseteq R$

But S is maximal

$\Rightarrow S+T = R$

$S+T = \{S+b\alpha \mid \alpha \in R\}$

Let $S+b\alpha \in (S+T) \Rightarrow S+b\alpha \in R$ [$\because S+T=R$]

Since $1 \in R$

$\Rightarrow a+b\alpha = 1$ where $a \in S$

$\Rightarrow a = 1-b\alpha$

$\Rightarrow (1-b\alpha) \in S$ [$\because a \in S$]

$\Rightarrow S+1 = S+b\alpha$ $\quad [Ha = Hb \Leftrightarrow ab^{-1} \in H]$

$\Rightarrow S+1 = (S+b)(S+\alpha)$

$\Rightarrow (S+\alpha)$ is the multiplicative inverse of $(S+b)$

$\Rightarrow \left(\frac{R}{S}, +, \cdot\right)$ is a field [$\because (S+b)$ is arbitrary].

"Only if part" Suppose $\left(\frac{R}{S}, +, \cdot\right)$ is a field

To prove S is maximal

Let S' be an ideal of R such that

$$S \subseteq S' \subseteq R \quad \& \quad S \neq S'$$

$\Rightarrow$ ~~$S' \subseteq R$~~ S will be maximal if $S' = R$

clearly $S' \subseteq R$ —— (1)

To prove $R \subseteq S'$

Let $\alpha \in R$ such that $\alpha \notin S$

$\Rightarrow S+\alpha \neq S$

$\Rightarrow S+\alpha$ is non zero element of $\frac{R}{S}$

Since $S \subseteq S' \Rightarrow \exists\ \beta \in S'$ such that $\beta \notin S$

$\Rightarrow S+\beta \in \frac{R}{S}$ is also a non zero element

We know $\left(\frac{R}{S}, \cdot\right)$ is a group

$\therefore \exists\ (S+r) \in \frac{R}{S}$ such that

$(S+r)(S+\beta) = S+\alpha, \quad r \in R$

$\Rightarrow S+r\beta = S+\alpha \Rightarrow (\alpha - r\beta) \in S$ —— (2)

$\Rightarrow \alpha - r\beta \in S'$ [$\because S \subseteq S'$] —— (1)

Also $r \in R, \beta \in S' \Rightarrow r\beta \in S'$ —— (2)

(1) & (2) $\alpha - r\beta + r\beta \in S'$

$\Rightarrow \alpha \in S'$

$\therefore \alpha \in R \Rightarrow \alpha \in S' \Rightarrow R \subseteq S'$ —— (3)

(1) & (3) $\Rightarrow S' = R$

$\therefore S$ is maximal ideal of R.

Theorem. Let R be a commutative ring and S be any ideal of R then $\frac{R}{S}$ is an integral domain iff S is prime ideal.

Proof. Let R be a commutative ring and S be an ideal of R then

$\frac{R}{S} = \{ S+a \mid a \in R \}$ is a ring, called quotient ring

Also $\frac{R}{S}$ is commutative as

$(S+a)(S+b) = (S+b)(S+a)$ $[\because ab = ba]$

If part: Suppose S is prime ideal

to prove $\frac{R}{S}$ is an integral domain

To prove $\frac{R}{S}$ is without zero divisors

We know zero element of $\frac{R}{S}$ is S

So let $S+a$ and $S+b$ be any two ~~non zero~~ elements of $\frac{R}{S}$ where $a, b \in R$ but $a \notin S$, $b \notin S$

Now ~~$(S+a) \neq S$~~ To show

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

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

(i) if $S+a = S \Rightarrow a \in S$ which is a contradiction

(ii) if $S+b = S \Rightarrow b \in S$ which is again a contradiction

~~$\therefore (S+a)(S+b) = S$.~~

$\Rightarrow$

$S+ab = S \Rightarrow ab \in S$

$\Rightarrow$ Either $a \in S$ (i) or $b \in S$ (ii) [$\because S$ is prime ideal]

(i) $a \in S \Rightarrow S+a = S$

(ii) $b \in S \Rightarrow S+b = S$

$\therefore (S+a)(S+b) = S \Rightarrow$ Either $S+a = S$ or $S+b = S$

$\Rightarrow \frac{R}{S}$ is without zero divisors.

$\Rightarrow \frac{R}{S}$ is an integral domain.

"Only if part" suppose $\left(\frac{R}{S}, +, \cdot\right)$ is an integral domain

to prove S is prime ideal.

Let $a, b \in R$ such that $(ab) \in S$

To prove either $a \in S$ or $b \in S$

It is given $\frac{R}{S}$ is without zero divisors

let $S+a$, $S+b$ be any two ~~non-zero~~ elements of $\frac{R}{S}$

$(S+a)(S+b) = S$ [$\because$ S is zero element of $\frac{R}{S}$]

$\Rightarrow$ Either $\underset{(i)}{S+a=S}$ or $\underset{(ii)}{S+b=S}$

(i) $S+a=S \Rightarrow a \in S$

(ii) $S+b=S \Rightarrow b \in S$

$\therefore$ $(ab) \in S \Rightarrow$ Either $a \in S$ or $b \in S$

$\Rightarrow S$ is prime ideal.

proved