$O(a) = 2 \quad O(b) = 2$

$H = \{e, a\} \quad K = \{e, ab\}$

$HK = \{e, a, b, ab\}$; is a commutative group.

$|HK| \mid |G|$

$\therefore |4| = 4n$

(a) **Ring** →

$R \neq \phi$. $(R, +, \cdot)$ → 2 binary operations.

where

$+ : R \times R \to R$

$\cdot : R \times R \to R$.

$(a,b) \to a+b$

$(a,b) \to a \cdot b$

Ring iff.

(i) $(R, +)$ is a commutative group.

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

(iii) $a \cdot (b+c) = a \cdot b + a \cdot c$ → left distributive property

$(b+c) \cdot a = a \cdot c + b \cdot c$ → Right distributive property.

$\forall a, b, c \in R$.

Examples:

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

→ forms a ring.

A Ring R is commutative ring, if $ab = ba$.

$\forall ab \in R$.

If 0_R 0 → zero element (commutative wrt product).

✓ $M_{n \times n}(\mathbb{R})$ forms a ring.

but $M_{m \times n}(\mathbb{R})$ does not form a ring.

$m \neq n$

Scanned by CamScanner

$M_{n\times n}(\mathbb{Z}_n)$ $\quad \mathbb{Z}_n = \{[0], [1], \ldots, [n+1]\}$.

$[a] + [b] = [a+b]$

$[a][b] = [a\cdot b]$ $\quad \forall\ [a], [b] \in \mathbb{Z}_n$

$[a][b] = [b][a]$

finite commutative ring

finite non-commutative ring.

Ring has identity element if it has identity with respect to $\otimes$ product

$1_R, 1$

if $1_R\, a = a\, 1_R = a \quad \forall\ a \in R$.

$(2\mathbb{Z}, +, \cdot)$ — even integers

[$GL(2, \mathbb{R})$ does not form ring as closure property is not there.]

$(n\mathbb{Z}, +, \cdot)$ $n \neq 1$.

finite ring without identity, $(\mathbb{Z}_n - \{[1]\}, +, \cdot)$

$(P(X), \triangle, \cap)$

$A + B = A \triangle B = (A \setminus B) \cup (B \setminus A)$

$A \cdot B = A \cap B$

Subring →

Ring of continuous functions →

Scanned by CamScanner

Ring of continuous functions →

Let, $C[0,1] = \{ f : [0,1] \to \mathbb{R} \mid$ where f is continuous function $\}$

↳ $C[a,b]$

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

$\forall\ f,g \in C[0,1]$

$x \in [0,1]$

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

$x \in [0,1]$

$f(g(x))$

↳ does not form ring.

so, pointwise mapping must be taken.

Let, $D[0,1] = \{ f : [0,1] \to \mathbb{R} \mid$ where f is Differentiable $\}$.

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

$(f \cdot g)(x) = f(x)\,g(x) \ \forall\ f,g \in D[0,1]$

$x_0 \in [0,1]$.

□ Integral domain

Let R be commutative ring with identity

zero divisor
Divisor of zero

Def, $a,b \in R$ s.t

iff $ab = 0$

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

then a Ring R with no divisor of zero.

if $ab = 0$ when $a \neq 0$ or $b \neq 0$ then a has divisor of zero

Ring → Division Ring → Field.

Scanned by CamScanner

take $M_2(\mathbb{R})$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\neq 0$ $\neq 0$ $= 0$

n divisor of zero.

Ring R is said to be integer domain if, R is commutative ring with identity. Then R is called an integral domain if R has no divisor of zero $(\mathbb{Z}, +, \cdot)$.

$(\mathbb{Z}_n, +, \cdot)$ is integer domain if n is prime

Scanned by CamScanner

$$\rightarrow \quad \bar{r}_{OC} \times \left[\bar{F}_{CA} + \bar{F}_{CB}\right] + \bar{r}_{OE} \times \left[240\times 9.8\,\hat{k}\right]$$

$$= 0$$

Integral domain

R → commutative ring with identity. in which there is no divisor of zero.

$$ab = 0$$

$$\Rightarrow a = 0 \text{ or } b = 0$$

Division Ring →

Ring with identity 1 then R is said to be a Division ring if for any $a \neq 0 \in R$ $\exists\, b \in R$ s.t

$ab = ba = 1$ ∃ inverse wrt product.

Field

Let R be a commutative ring with identity 1, R is called a field if every $a \neq 0 \in R$, $\exists\, b \in R$ s.t,

$ab = ba = 1$

Commutative division ring is a field.

Field is a Division ring as well as Integral domain.

$ab = 0 \quad a \neq 0$

$a^{-1}(ab) = 0$ | integral domain.

$\Rightarrow b = 0.$

Scanned by CamScanner

Field $\Rightarrow$ Division ring

$\not\Leftarrow$

Division ring $\Rightarrow$ Field

$\not\Leftarrow$

$$R = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}_{2\times 2} : u, v \in \mathbb{C} \right\}.$$

$u = x + iy \quad v = a + ib \quad \bar{u} = x - iy$

$\bar{v} = a - ib$

↳ this forms a division ring but not field.

✓ Finite division ring is always a field.

$(\mathbb{Z}, +, \cdot) \longrightarrow$ ID but not field.

✓ Finite integral domain is always a field.

Let R be a finite integral domain,

$R = \{a_1, a_2, \cdots, a_n\}$. → this set contains

Let $a_1 \neq 0 \in R$.

consider a set, this

$S = \{a_1 a_1, a_1 a_2, \cdots, a_1 a_n\}$.

Let, $a_1 a_i = a_1 a_j \quad i \neq j$ all distinct.

$\Rightarrow a_1 (a_i - a_j) = 0$

$\because a_1 \neq 0$, and R is integral domain

$a_i - a_j = 0$

$\Rightarrow a_i = a_j$

$S \subseteq R \quad |S| = |R|$

$\exists \; a_1 a_i = 1$

we can define a bijection from $R \to S$.

$a_1 a_i = 1 = a_i a_1$ → commutative ∴ R is a field

∴ R is ID

Let R be a finite ID.

Let, $a(\neq 0) \in R$

Define a mapping $f_a : R \to R$ by

$f_a(x) = ax$ for $\forall x \in R$.

$f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

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

$\Rightarrow (x-y) = 0$

or, $x = y$. $\left(\because a \neq 0 \text{ \& } R \text{ is an ID}\right)$.

✓ Cardinality same and finite then injective map means surjective.

Since R is finite, it follows f_a is surjective.

Since, f_a is surjective $\because 1 \in R$.

$\therefore \exists\, x \in R$

s.t, $f_a(x) = ax = 1$

$\because$ R is commutative,

$xa = 1$.

$\therefore$ R is a field.

take $(\mathbb{Z}, +, \cdot), (\mathbb{Z}_n, +, \cdot)$

$\mathbb{Z}_n$ is ID iff n is prime.

✓ $\mathbb{Z}_p$ are all fields.

Scanned by CamScanner

if F is any finite field,

$|F| = p^n$ for some prime p & $n \in \mathbb{N}$

$|R| = 6$, $R \to$ ID.

$|(R,+)| = 6 = (2 \cdot 3)$ | from Cauchy's theorem

$\exists\ a \in R$ s.t. $o(a) = 2$

$2a = 0$

$\exists\ b \in R$, $o(b) = 3$

$3b = 0$

$(2a)(b) = 0$

$\Rightarrow (a2b) = 0$ commut

$\Rightarrow (a)(2b) = 0 \Rightarrow 2b = 0$ contradiction

both non zero & not ID. Bcoz $3b = 0$

Subring.

Let, $(R, +, \cdot)$ and $S \subseteq R$

$S \neq \phi$

then S is subring of R is S itself forms a ring where, $(S, +, \cdot) \to$

$(+) : S \times S \to S$ } restricted
$(\cdot) : S \times S \to S$ } binary operation

S forms a subring of R,

iff $ab \in S$, $a - b \in S$ for $\forall\ a, b \in S$.

Let R be a ring and S be a subring of R — necessary and sufficient condition.

$(R,+,\cdot)$ $(\mathbb{R},+,\cdot)$ $(\mathbb{Z},+,\cdot)$ $(m\mathbb{Z},+,\cdot)$

$(\mathbb{Q},+,\cdot)$

Subrings.

$R = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in R \right\}$ $(R/\{0\},\cdot)$ → forms a group

↳ forms a Field.

Scanned by CamScanner

✓ S may have identity but R has no identity

✓ S has different identity than R.

✓ S has no identity and R has identity

All possibility,

$R \to$ $\quad S \to I_S$

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

this forms ring wrt addition and multiplication.

identity $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$,

R has no identity

but, S has this identity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

$R \to 1_R \quad S \to I_S$

let $1_R \neq 1_S$

$R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in R \right\}$.

$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

$1_S = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

$1_R \neq 1_S$

Scanned by CamScanner

$R_1 \times R_2 = \{(a,b) : a \in R, b \in R\}$.

$(a,b) + (c,d) = (ac, bcd)$

$(a,b)(c,d) = (ac, bd)$

$1_R = (1,1)$

$S = \mathbb{Z} \times \{0\}$

$1_S = (1,0)$

for, R is ID and S is subring of R.

$1_R = 1_S$

$(a,0) \in S$.

$a \cdot 1_R = a$

$a \cdot 1_S = a$

$a \cdot 1_R = a \cdot 1_S$

$a(1_R - 1_S) = 0$

$R \to 1_R$ $\quad S \to 1_S$

$R = (\mathbb{R}, +, \cdot)$ $\quad S = (\mathbb{Z}, +, \cdot)$

$1_R = 1$ $\quad 1_S = 1$

$R \to \mathbb{Z}$ $\quad S \to \mathbb{Z}$

no identity

Quotient ring.

Scanned by CamScanner

Ideal

Let R be a ring and I be a subring of R.

Then I is ideal

(i) a left ideal of R if $rI \subseteq I$ $\forall r \in R$ and $a \in I$

(ii) a right ideal of R if $ar \in I$ $\forall r \in R$, $a \in I$

(iii) an ideal of R if I is left ideal as well as right ideal.

An ideal I of a ring R is called a proper ideal of R if $I \neq R$.

$\{0\} \subset R$.

↳ proper ideal.

for a field $\{0\}$ is maximal ideal.

If a ring R has identity 1 and $1 \in I$ implies that $I = R$

$I \subseteq R$ $R \subseteq I$

Let $r \in R$ then $r = r \cdot 1 \in I$ we have chosen I as the ideal.

$R \subseteq I$

if I is proper ideal then I does not contain 1.

Let R be a ring. and I_1 and I_2 be two ideals of R, $(I_1 + I_2) = \{a + b : a \in I_1, b \in I_2\}$.

$I_1 + I_2$ is also an ideal of R.

$R = (Z, +, \cdot)$

$I = nZ$, $n \in N$ $n = 0$

$a - b \in I$

$ra \in I$ $ab \in I$

$a \in I_1 \cap I_2$ $r \in R$

Scanned by CamScanner

$ab \in I_1$ $ab \in I_2$ $a-b \in I$

$I_1 = 2\mathbb{Z}$

$I_2 = 3\mathbb{Z}$ $2 \in I_1$ $a-b \in (I_1 \cap I_2)$

$\subset I_1 \cup I_2$

$3 \in I_2$ $\subset I_1 \cup I_2$

$2+3 = 5 \notin I_1 \cup I_2$

$I_1 \cup I_2$ is not the ideal of ring R. $I_1 \cap I_2$ is ideal.

$I_1 I_2 = \{ ab : a \in I_1, b \in I_2 \}$ $(a+b)$

does not form closure under addition.

$ab + cd \neq ef$ → may not be written from

$I_1 I_2 = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I_1, b_i \in I_2 \right\}$

cannot be taken infinite sums because the sum may not exist.

Principle ideal.

Single element generated ideal.

$S (\neq \phi) \subseteq R$

$\langle S \rangle = \bigcap_{S \in I_i} I_i$ ideal generated by S.

$S = \{a\}$

$I = \langle a \rangle$ → principle ideal.

$\langle a \rangle = \{ ra + na : r \in R, n \in \mathbb{Z} \}$ → needed to construct a if there is no identity in R.

$ra : r \in R$ → if there is identity.

$= Ra$

$\langle a \rangle_r = \{ as + n'a : s \in R, n' \in \mathbb{Z} \}$ → if there is no identity

$as : s \in R \} = aR$

→ if there is identity.

Scanned by CamScanner

$\langle a \rangle = \{ ra + as + \sum_{i=1}^{n} r_i a s_i + na : n \in \mathbb{Z} \}$ → with + identity

$r, s, r_i, s_i \in R$.

$= \{ \sum_{i=1}^{n} r_i a s_i \}$ $r_i, s_i \in R$.

↳ with identity $1 \in R$

$= RaR$

$Ra = aR = RaR$] commutative ring.

$\langle a \rangle_L = \langle a \rangle_R$

$Ra = aR$

Quotient ring →

R = field.

$\{0\}$, R (iff)

[Let R be commutative ring with identity then R is field iff R has only two ideals $\{0\}$ and R.]

- $I \neq \{0\}$

$a \neq 0 \in I$

$a^{-1}a = 1 \in I$

for $a \in I$

$a^{-1} \in$ Field R

$I = R$

prove the converse,

Let $(a \neq 0) \in R$,

$Ra = \{ra : r \in R\}$.

Consider Ra.

Then Ra is a non zero ideal,

$Ra \neq \{0\}$.

R has only two ideals $\{0\}$ & R

Since $Ra = R$,

Since $1 \in R$ ∃ $r \in R$ s.t. $ra = 1$

Since R is commutative $ar = 1$

$ra = ar = 1$

Scanned by CamScanner

from groups we check a normal subgroup

$G/H = \{aH : a \in G\}$

$(ab)H = (bH)$ $\Leftarrow$ $(ab)H$

Let R be a ring and I be ideal of R.

$R/I = \{a+I : a \in R\}$.

$a \sim_I b \Rightarrow a - b \in I$

$[a]_{\sim_I} = a + I$

$[a]_{\sim_I} = \{b \in R : a - a \in I$

$b - a = i$

$b = a + i \in a + I$

$(a + I) + (b + I) = (a + b) + I$

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

✓ for rings the congruence classes are I

If R is commutative ring with identity and I is a ideal of R then R/I is a commutative ring with identity

$1 + i$

When ring is commutative R/I is also commutative.

$a + I, b + I \in R/I$.

$(a + I)(b + I)$

$= ab + I$

$= ba + I = (b + I)(a + I)$.

Let, R be a finite commutative ring with identity then for any non-zero a in R, a is either a zero divisor or a unit (invertible) in R.

R/I is commutative $\Leftrightarrow ab - ba \in I \; \forall a, b \in R$,

~~$ab + I = ba + I$~~

$a + I = b + I$

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

Scanned by CamScanner

$(a+I)(b+I) = (b+I)(a+I)$

$(ab+I) = (ba+I)$

$\Rightarrow (ab-ba) \in I$

R is commutative.

$\therefore ab - ba \in I \quad \forall a, b \in R$

let $a(\neq 0) \in R$,

$ab = ba = 1$

$ab = 0$

$(\mathbb{Z}_n, +, \cdot)$

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

$\gcd(a, b) = 1 \qquad [a][b] = 1$

$f_a : R \to R$ by

$f_a(a) = ax$

If not injective

$f(u) = f(v)$

$u \neq v$ in R

$au = av$

$\Rightarrow u \in R \quad a(u-v) = 0$

$\therefore R$ is finite,

f_a is surjective

$\exists\ x \in R$ s.t.

$f_a(x) = 1$

$ax = 1$

$xa = 1$

$ax = xa = 1$

$u \neq v$

so, a is a divisor of zero.

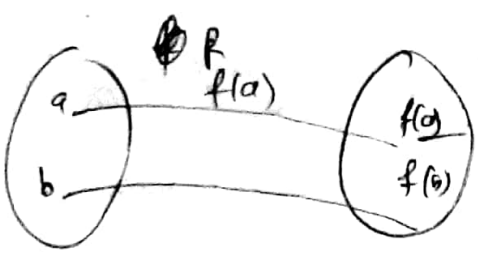
Scanned by CamScanner

Homomorphism of a ring

Let R and R' be two rings $f: R \to R'$ is called a Homomorphism if $(R, +, \cdot)$ $(R', +', \cdot')$

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

(ii) $f(ab) = f(a)\, f(b)$ $\forall a, b \in R$



if $f: R \to R$.

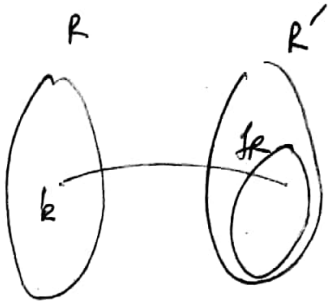
Endomorphism, homomorphism to itself.

homomorphism with surjection → epimorphism.

from an graph.

$f: R \to R'$

↳ isomorphism → $R \cong R'$



$f: G \to G'$

$f(e_G) = e_{G'}$ in group

for ring →

$f: R \to R'$

(i) $f(0_R) = 0_{R'}$

(ii) $f(1_R) = 1_{f(R)} = 1_{R'}$ ← this happen when f is surjective

if f is surjective. } if identity does not exist.

$f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

$f(a) = (a, a)$ → if defined like this. Identity go to identity.

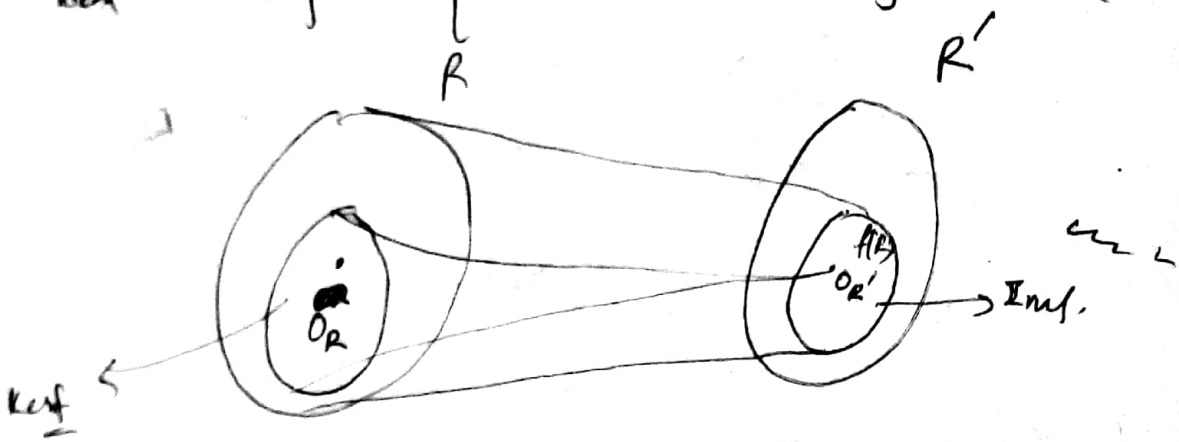
$f(a) = (a, 0)$ → if defined like this then identity does not go to identity.

Scanned by CamScanner

$f: R \to R'$ ring homomorphism

$\text{Im } f = \{ f(x) : x \in R \}$.

ideal $\quad \ker f = \{ x \in R : f(x) = 0_{R'} \}$, a



$x, y \in \ker f$

$x - y \in \ker f$.

$xy \in \ker f$.

Since $x, y \in \ker f \quad f(x) = f(y) = 0_{R'}$.

$$f(x-y) = f(x) - f(y)$$

$$= 0_{R'} - 0_{R'}$$

$$= 0_{R'}$$

$\Rightarrow (x-y) \in \ker f$.

$$f(xy) = f(x) \cdot f(y)$$

$$= 0_{R'} \cdot 0_{R'}$$

$$= 0_{R'}$$

$\therefore xy \in \ker f$

Scanned by CamScanner

$rx, xr \in \ker f$. ($rx = xr$)

$f(rx) = f(r) f(x)$ $\quad \because x \in \ker f$

$= f(r) 0_{R'}$ $\quad f(x) = 0_{R'}$

$= 0_{R'}$

$\Rightarrow rx \in \ker f$.

$f(xr) = f(x) \cdot f(r)$

$= 0_{R'} f(r) = 0_{R'}$

$\Rightarrow xr \in \ker f$.

Let R be a ring, I be a ideal of R.

$R/I = \{ a+I ; a \in R \}$

Define a mapping $f : R \to R/I$ by

$f(r) = r + I \quad \forall r \in R$.] natural epimorphism.

$f(r_1 + r_2) = (r_1 + I) + (r_2 + I) \quad (r_1 + r_2) + I$

$= (r_1, I) + (r_2, I)$

$= f(r_1) + f(r_2)$

$f(r_1 r_2) = r_1 r_2 + I = (r_1 + I)(r_2 + I)$.

$= f(r_1) f(r_2)$

$\ker f = \{ r \in R : f(r) = 0 + I \}$.

$= \{ r \in R : r + I = 0 + I \}$.

$= \{ r \in R : r \in I$

$= I$.

Scanned by CamScanner

non empty subset I be an ideal of R then it must be kernal of some homomorphism.

$f: G \to G'$ → monomorphism.] for

homomorphism iff $\ker f = \{e_G\}$.

iff $\ker f = \{e_G\}$

Homomorphism of a ring.

Let R and R' be two rings.

Let $f: R \to R'$ be a homomorphism.

Then f is a monomorphism iff $\ker f = \{0_R\}$

First suppose that, f is a monomorphism.

let, $x \in \ker f$. if we show, x is 0_R be,

Then,

$f(x) = 0_{R'} = f(0_R)$

↳ ∵ f is homomorphism.

$f: R \to R'$

$0_R + 0_R = 0_R$

$f(0_R + 0_R) = f(0_R)$

$R_1 +$

$\Rightarrow f(0_R) + f(0_R) = f(0_R) + 0_{R'}$

$\Rightarrow f(0_R) = 0_{R'}$

∵ f is monomorphism,

$\Rightarrow x = 0_R$. ∵ f is injective.

Scanned by CamScanner

$\therefore$ Kerf contains 0_R.

Conversely,

Let, Kerf $= \{0_R\}$.

Let $a, b \in R$, be s.t, $f(a) = f(b)$

$\Rightarrow f(a) - f(b) = 0_{R'}$

$\Rightarrow f(a-b) = 0_{R'}$

$a - b \in \text{Kerf} = \{0_R\}$.

$\Rightarrow a - b = 0_R$

$\Rightarrow a = b$.

First isomorphism theorem.

Let R and R' be two rings and $f: R \to R'$ be an epimorphism. Then $R/\text{kerf} \cong R'$.

Define a mapping $\phi: R/\text{kerf} \to R'$ by

$$\phi(a + \text{kerf}) = f(a) \quad \forall\ a + \text{kerf} \in R/\text{kerf}.$$

to show first well defined: $a = b \Rightarrow f(a) = f(b)$.

Let, $a + \text{kerf} = b + \text{kerf}$.

$a + I = b + I$ if $a - b \in I$.

~~$\phi(a + \text{kerf}) = \phi(b + \text{kerf})$~~.

$\Leftrightarrow a - b \in \text{kerf}$.

$\Leftrightarrow f(a-b) = 0_{R'}$

$\Leftrightarrow f(a) - f(b) = 0_{R'}$

$\Leftrightarrow f(a) = f(b)$.

$\Leftrightarrow \phi(a + \text{kerf}) = \phi(b + \text{kerf})$.

Scanned by CamScanner

Let $y \in R'$

$\because f$ is epimorphism.

$\exists\ x \in R$ s.t. $f(x) = y$.

$\Rightarrow \phi(x + \ker f) = y$

$\therefore\ x + \ker f \in R/\ker f$ s.t.

$\phi(x + \ker f) = y$.

now to show ϕ is homomorphism.

$$\phi[(a+\ker f) + (b+\ker f)]$$

$$= \phi[(a+b)\ker f] \quad [\because \text{from definition of quotient}].$$

$$= f(a+b)$$

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

$$= \phi(a+\ker f) + \phi(b+\ker f).$$

$$\phi[(a+\ker f)(b+\ker f)]$$

$$= \phi((ab)+\ker f)$$

$$= f(ab)$$

$$= f(a) f(b) = \phi(a\ker f)\,\phi(b\ker f).$$

Scanned by CamScanner

prime ideal and maximal ideal of a commutative ring with identity →

$\mathbb{Z}$

$\langle p \rangle$ P is prime.

$I = \langle n \rangle = n\mathbb{Z}$ $n=0$, $n \in \mathbb{N}$.

$\langle p \rangle = p\mathbb{Z}$

$ab \in \langle p \rangle = p\mathbb{Z}$

$ab = pt$, $t \in \mathbb{Z}$.

$\Rightarrow p \mid ab$

from the property of prime

either $p \mid a$ or $p \mid b$

$\Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$

$a = pe \in e\langle p \rangle$ $b = pd \in \langle p \rangle$.

Let R be a commutative ring with identity and P be a proper ideal of R. ie $P \neq R$. Then P is called a prime ideal of R if for $a,b \in R$ $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$

$\{0\} \neq R$ $a,b \in R$.

$ab \in \{0\}$

$ab = 0$ or $a = 0$ or $b = 0$] for integral domain,

either $a \in \{0\}$ or $b \in \{0\}$

0 ideal is always a prime ideal for integer domain.

$\{0\}$, $p\mathbb{Z}$ are prime ideal of $\mathbb{Z}$.

maximal ideal →

Let R be a commutative ring with identity. A proper ideal M is called a maximal ideal of R if there doesn't exist an ideal I of R s.t, $M \subset I \subset R$.

the maximum ideal is R. if $M \subset I \subseteq R$

then $I = R$.

the M is maximal.

Scanned by CamScanner

$p\mathbb{Z}$ → maximal ideal.

$\{0\}$ is a maximal ideal of a commutative ring with identity iff R is a field.

$\{0\}, F$

Prime ideal of $\mathbb{Z}$ but not a maximal ideal of $\mathbb{Z}$.

$I \neq \{0\} \subseteq F$

at I $a^{-1} \in F$, $a^{-1}a \in I$ $\therefore I = F$

Let R be a commutative ring with identity.
Let M be a maximal ideal of R then M is a prime ideal of R.

Let for any $ab \in R$, $ab \in M$ s.t, $a \notin M$.

$a, b \in R$

$P \neq R$,
$ab \in I \Rightarrow a \in P$ or $b \in P$.

consider the set

$J = \{x + ra : x \in M, \& r \in R\}$.

$\exists\ a = 0 + 1 \cdot a \in J$ but $a \notin M$.

so, then $M \subset J$

$x = x + 0 \cdot a \in J$.

$\therefore$ M is maximal so, J must be equal to the whole ring R. $(J = R)$.

Now $1 \in R$. so, $1 \in J$.

$\exists\ x \in M$ $r \in R$, $1 = x + ra$.

$b = xb + rab \in M$.

so, $b \in M$

$\therefore$ M is a maximal ideal ideal of ring R.

Eg Every maximal ideal is the prime ideal but converse not true. Ex $\{0\}$

Scanned by CamScanner

Let R be commutative ring with identity.

Let P be a proper ideal of R. Then P is a prime ideal of R if R/P is an integral domain.

Let M be a proper ideal of R. Then M is a maximal ideal of R iff R/M is a field.

M is a maximal ideal of R ⇒ R/M is a integral domain ✓

⇔ M is a prime ideal of R.

For commutative ring maximal ideal exists. So, prime ideal exists.

$\mathbb{Z}$ ⇒ PID $I = \langle a \rangle = Ra$.

$\{0\}$ PID prime ideal.

PID maximal (non zero consider)

R is finite R/M is also finite.

$R/M = \{ a + M : a \in R \}$.

M is a maximal ideal of R ⇔ R/M is a field (⇔ R/M is an finite integral dom ⇔ M is a prime ideal of R.

Polynomial ring →

$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ $a_0, a_1, a_2, \dots a_n \in R$.

Let R be ring with identity.

Let $R[x] = \{ f(x)$ is a polynomial in $R \}$.

$f(x) + g(x) \in R[x]$

$f(x)\, g(x) \in R[x]$ $g(x) = b_0 + b_1 x + \dots + b_m x^m$.

forms a ring wrt, (+) and (·) $f(x), g(x) \in R[x]$

(+) adding two poly

(·) product of two poly.

If R is a commutative ring with identity then R[x] is a commutative ring with identity.

(i) R is a commutative ring with identity then R[x] is a commutative ring with identity.

Scanned by CamScanner

R → I.D
R[x] → I.D
R → field R[x] need not be a field.
f(x) = a. only constant function will be invertible

Let R be a commutative ring with identity. Then $R[X]/\langle X\rangle \simeq R$.

$\langle x\rangle = \{x f(x) : f(x) \in R[x]\}$. $\langle a\rangle = Ra$, $R = R[x]$ poly ring.

$= \{x f(x) : f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \in R[x]\}$.

$= \{a_0 x + a_1 x^2 + \dots + a_n x^{n+1} ; a_i \in R\}$.

$= \{g(x) :$ constant term of $g(x)$ is zero$\}$.

Define a mapping $\phi : R[x] \to R$ by.

$\phi(a_0 + a_1 x + \dots + a_n x^n) = a_0$.

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

$\phi(f(x) g(x)) = \phi(f(x))\, \phi(g(x))$

This is a surjection as, for any $a \in R$,

$\phi(a + bx) = a$

So, $R[x]/\ker\phi \simeq R$.

$f(x) \in \ker\phi \iff \phi(f(x)) \iff 0$

$\iff a_0 \iff 0$

$\iff f(x) \in \langle x\rangle$

$\langle x\rangle$ is a prime ideal of $Z[x]$ but $\langle x\rangle$ is not a maximal ideal of $Z[x]$.

$Z[x]/\langle x\rangle \simeq Z$

I.D. ... I.D

prime ideal of Z.

if $\langle x\rangle$ is maximal ideal. then Z and Z(x) has to field. but they are not,

Let R be a commutative ring with identity and I be an ideal.

Then $R[x]/I[x] \simeq (R/I)[x]$

I is a prime ideal of R
$\Leftrightarrow$ R/I is an I.D
$\Leftrightarrow (R/I)[x]$ - ID

I is an ideal of R.
$\Rightarrow$ I[x] is an ideal of R[x]

P is a prime ideal of R.
$\Rightarrow$ P[x] is a prime ideal of R[x]

M is a maximal ideal of R.
$\Rightarrow$ M[x] is a maximal ideal of R[x].

$\phi : R[x] \to R/I[x]$

$\phi(a_0 + a_1 x + \dots + a_n x^n) = (a_0 + I) + (a_1 + I)x + (a_2 + I)x^2 + \dots + (a_n + I)x^n$.

Field Extension →

Let F be a field and K be a subfield of F then F/K is called field extension. $K \subseteq F$

this is just a notation.

F field K = subfield $a, b \in K$

$a - b \in K$.

$a \in K$, $b (\neq 0) \in K$, $ab^{-1} \in K$

$(V, +)$ $(F, +, \cdot)$

$\cdot : F \times V \to V$

$+ : (\alpha, V) \to \alpha \cdot V$

$[F : K]$ degree of dimension of field extension in F/K.

$[\mathbb{C} : \mathbb{R}] = 2$

Basis of $\mathbb{C}$ is $\{1, i\}$.

$\{a + ib : a, b \in \mathbb{R}\}$.

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$.

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

$x^2 - 2$ $\quad x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$

$\{1, \sqrt{2}\}$

Scanned by CamScanner