Ex. (6) Pg-224 S.K. Hapa

Prove that the matrices $\left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} : a, b \in Q\right\}$ forms a field under matrix addition & multiplication. Also show that it is an I.D. (See in the next page).

Soln: Let $S = \left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} : a, b \in Q\right\}$.

$(S, +, \cdot)$ forms a ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ → Show it.

Let $X = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \in S$, $Y = \begin{pmatrix} p & q \\ 3q & p \end{pmatrix} \in S$.

Then $X \cdot Y = Y \cdot X$ for all $X, Y \in S$. → verify it.

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

Let X be a non-zero element of S. Then $a, b \in Q$ and ~~Then~~ $(a, b) \neq (0, 0)$, $\det X = a^2 - 3b^2 \neq 0$, since $(a, b) \neq (0, 0)$ and a, b are rational $(\in Q)$.

[otherwise, if $a^2 - 3b^2 = 0$, then $a = \sqrt{3}b \Rightarrow a \notin Q$.]

$\therefore$ $\det X \neq 0 \Rightarrow X^{-1}$ exists and

$$X^{-1} = \frac{1}{\det X}\begin{pmatrix} a & -b \\ -3b & a \end{pmatrix}$$

$$= \frac{1}{a^2 - 3b^2}\begin{pmatrix} a & -b \\ -3b & a \end{pmatrix} \in S.$$

$\therefore$ Each non-zero element of S is a unit.

Hence $(S, +, \cdot)$ forms a field. (proved).

Ex. 14 Pg-231 (ii) Prove that the set $S = \{a + b\sqrt{-5} : a, b \in Z\}$ is an I.D.

Show first $(S, +, \cdot)$ is a Commutative ring with unity $1 (= 1 + 0\sqrt{-5})$.

To shows that $(S, +, \cdot)$ contains no divisor of zero, we take $p = (a + b\sqrt{-5}) \in S$ be a non-zero element.

Then $a, b \in Z$ and $(a, b) \neq (0, 0)$

Let $q = (c + d\sqrt{-5})$ and let $pq = 0$ $[0 + 0\sqrt{-5}]$

Then $(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = 0 \Rightarrow (ac - 5bd) + (ad + bc)\sqrt{5} = 0 + 0\sqrt{-5}$

$\Rightarrow$ $ac - 5bd = 0$ & $bc + ad = 0$ } Homogeneous system giving non-zero solns for c, d, if $\begin{vmatrix} a & -5b \\ b & a \end{vmatrix} = 0$,

i.e., if $a^2 + 5b^2 = 0$.

Since $a, b \in Z$ & $(a, b) \neq (0, 0)$, $a^2 + 5b^2 \neq 0 \Rightarrow c$ & d both zero.

i.e., $c + d\sqrt{-5}$ is a zero element. Hence $(S, +, \cdot)$ is an I.D.

Ex. Examine if the ring of matrices $\left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} : a, b \in \mathbb{Q}\right\}$ is an I.D.

Let $S = \left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} ; a, b \in \mathbb{Q}\right\}$

$(S, +, \cdot)$ forms a commutative ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $X = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$ be a non-zero element of S.

Then $a, b \in \mathbb{Q}$ and $(a, b) \neq (0, 0)$.

Let $XY = 0$, where $Y = \begin{pmatrix} p & q \\ 3q & p \end{pmatrix}$

$\Rightarrow \left.\begin{aligned} ap + 3bq &= 0 \\ bp + aq &= 0 \end{aligned}\right\}$ homogeneous system giving zero solutions for p, q, if $\begin{vmatrix} a & 3b \\ b & a \end{vmatrix} \neq 0$

$a,\ a^2 - 3b^2 \neq 0$ for $a, b \in \mathbb{Q}$ & $(a, b) \neq (0, 0)$.

[otherwise, if $a^2 - 3b^2 = 0$, then $a = \sqrt{3}b \Rightarrow a \notin \mathbb{Q}$].

$\therefore Y \in S$ is a zero element of S.

$\therefore (S, +, \cdot)$ contains no-divisor of zero.

$\therefore$ $(S, +, \cdot)$ is an I.D.

Ex. Find the units in the ring of integral quaternions.

Let $H = \left\{\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} ; a, b, c, d \in \mathbb{Z}\right\}$, set of all integral quaternions

Let $A = \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$ be a unit in the ring H.

Then $A^{-1} \in H$. $\Rightarrow \det A \neq 0 \Rightarrow a^2 + b^2 + c^2 + d^2 \neq 0$.

$\therefore A^{-1} = \frac{1}{(a^2+b^2+c^2+d^2)} \begin{pmatrix} a-ib & -c-id \\ c+id & a+ib \end{pmatrix}$.

Since $A^{-1} \in H$, $a, b, c, d \in \mathbb{Z}$, then $a^2 + b^2 + c^2 + d^2 = 1$.

$\therefore$ $\left.\begin{aligned} a &= 1, b = c = d = 0 \\ a &= -1, b = c = d = 0 \\ b &= 1, a = c = d = 0 \\ b &= -1, a = c = d = 0 \\ c &= \pm 1, a = b = d = 0 \\ d &= \pm 1, a = b = c = 0 \end{aligned}\right\}$ So there are 8 units:

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$.

SKEW FIELD / DIVISION RING

A non-trivial ring S with unity is said to be a skew field if every non-zero element of S is a unit.

Theorem: A skew field contains no divisor of zero.

Proof:- Let S be a skew field and $a(\neq 0) \in S$ $\therefore a^{-1} \in S$.
Let $a \cdot b = 0$ where $b \in S$.
$\Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow (a^{-1} \cdot a) \cdot b = 0 \Rightarrow I \cdot b = 0 \Rightarrow b = 0$.
$\Rightarrow$ a is NOT a left divisor of zero.
~~Let $b(\neq 0) \in S$, $\therefore b^{-1} \in S$.~~
Let $b \cdot a = 0$ where $a(\neq 0) \in S$. $\Rightarrow a^{-1} \in S$
$\Rightarrow b^{-1} \cdot (b \cdot a) = b^{-1} \cdot 0 \Rightarrow (b \cdot b^{-1}) \cdot a = 0 \Rightarrow b \cdot I = 0 \Rightarrow b = 0$
Consequently, a is not a divisor of zero.
$\therefore$ S contains no divisor of zero.

Theorem: The cancellation law holds in a skew field
Let S be a skew field and let $a, b, c \in S$ and $a \cdot b = a \cdot c$ where $a \neq 0$. $\therefore a^{-1}$ exists in S.
Then $a \cdot (b - c) = 0 \Rightarrow a^{-1} \cdot [a \cdot (b - c)] = a^{-1} \cdot 0$
$\Rightarrow (a^{-1} \cdot a) \cdot (b - c) = 0$
$\Rightarrow I \cdot (b - c) = 0 \Rightarrow \underline{b = c}$.
$\therefore$ left cancellation law holds in S.
Again, let $b \cdot a = c \cdot a$ where $a \neq 0$. $\therefore a^{-1} \in S$.
Then $(b - c) \cdot a = 0 \Rightarrow [(b - c) \cdot a] \cdot a^{-1} = 0 \cdot a^{-1} = 0$
$\Rightarrow (b - c) \cdot (a \cdot a^{-1}) = 0 \Rightarrow (b - c) \cdot I = 0$
$\Rightarrow \underline{b = c}$.
$\therefore$ Right cancellation law holds in S.

Field: A commutative skew field is a field.
eg: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$
① $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, ... are fields, w.r.t. $+, \cdot$.
② Finite fields $(\mathbb{Z}_5, +, \cdot)$, $(\mathbb{Z}_3, +, \cdot)$, $(\mathbb{Z}_7, +, \cdot)$.

A field is an I.D. but the converse is NOT True.
Let F be a field and $a(\neq 0) \in F$.
Then $a^{-1} \in F$. Let $a \cdot b = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow b = 0$.
$\therefore$ a is ~~not~~ not a left divisor of zero, also is not a right divisor of zero, as F is commutative.

Converse Example:- $(\mathbb{Z}, +, \cdot)$ is an I.D. but not a field

$pI = 0 \Rightarrow$ char D is either p or $< p$
$qI = 0 \Rightarrow$ char D " " q or $< q$.
In either case, char D = m is contradicted.
$\therefore$ m is not a composite number.
$\therefore$ m is a prime number.
If, however, $\exists$ no +ve integer n for which $nI = 0$ holds, then char D = 0.

Theorem:- If the characteristic of an I.D. D be a non-zero number p, then the order of every non-zero element in the group $(D, +)$ is p.

Proof: Since char D = p, p is a prime number.
Let x be a non-zero element of D.

Then $px = x + x + \cdots + x$ (p times)
$= (I + I + \cdots + I).x$, I being the unity
$= (pI).x = 0.x = 0$.

$\Rightarrow$ order of x in the group $(D, +)$ is a divisor of p.
The only divisors of p are 1 and p.
The identity/zero element in the group $(D, +)$ is the only element of order 1.
Hence the order of x is p.

Field: Let F be a field and let $F^* = F - \{0\}$.
Then F^* forms a commutative group w.r.t. multiplication

Theorem: A finite I.D. is a field.

Let D be a finite I.D. containing $a_0 (= 0), a_1, a_2, \cdots, a_{n-1}$.
To prove: $a_1, a_2, \cdots, a_{n-1}$ are all units,
Let a_q be not the unity in D. Let us consider the products: $a_q \cdot a_1, a_q \cdot a_2, \cdots, a_q \cdot a_{n-1} \in D$ and none of them is zero, since D contains no divisor of zero. These are all distinct also
Let $a_q \cdot a_p = I = a_p \cdot a_q$ [$\because$ D is commutative]
$\Rightarrow a_q$ is a unit in D.
If however, a_q is the unity then also a_q is a unit in D.
This proves that each non zero element is a unit and proving that D is a field.

Ideals of a ring

Definition →

A subring S of a ring R is said to be

(i) a left ideal of R if $a \in S, r \in R \Rightarrow r.a \in S$;

(ii) a right " " " " " " $\Rightarrow a.r \in S$

(iii) an ideal (bothsided) " " " $\Rightarrow r.a \in S, a.r \in S$.

Improper Ideal of R is R itself

Trivial Ideal of R is the subring $\{0\}$, also it is trivial ring/subring. (null ideal)

Theorem :- A non-empty subset S of a ring $(R, +, \cdot)$ is an ideal of R if and only if

(i) $(S, +)$ is a subgroup of the group $(R, +)$; and

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

Proof: Let S be an ideal of R.

Then S is a subring of R. Therefore,

(i) $(S, +)$ is a subgroup of the group $(R, +)$.

(ii) $a \in S, r \in R \Rightarrow r.a \in S, a.r \in S$, since S is an ideal of R.

Conversely, let S be a non-empty subset of R where (i) & (ii) both hold.

Let $a \in S, b \in S \Rightarrow a \in S, b \in R \Rightarrow a.b \in S$

$\therefore (S, +)$ is a subgroup of the group $(R, +)$

and $a \in S, b \in S \Rightarrow a.b \in S$

$\therefore$ S is a subring of R with (ii) holds.

$\therefore$ S is an ideal of R.

Theorem :- A non-empty subset S of a ring $(R, +, \cdot)$ is an ideal of R if and only if

(i) $a \in S, b \in S \Rightarrow a - b \in S$; (ii) $a \in S, r \in R \Rightarrow r.a \in S, a.r \in S$.

Proof :- Let S be an ideal of R. Then S is a subring of R such that $a \in S, r \in R \Rightarrow r.a \in S, a.r \in S$

Since S is a ring, $(S, +)$ is an abelian group,

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

$\therefore$ Both (i) & (ii) hold in S.

Conversely, let S be a non-empty subset of R such that (i) & (ii) both hold.

(i) $\Rightarrow$ $(S, +)$ is a subgroup of the group $(R, +)$

(ii) $\Rightarrow$ $a \in S, b \in S \Rightarrow a \in S, b \in R \Rightarrow a.b \in S$.

$\therefore$ S is a subring of R with (ii) holds.

$\Rightarrow$ S is an ideal of R.

Ex.1. Every subring of the ring Z is an ideal.

The subrings of the ring Z are mZ, m being a non-negative integer.

$m = 0$. Then mZ is the null ideal $\{0\}$.

Let m be a (+ve) integer. Let $S = mZ$.

Let $p \in S$. Then $p = mu$ for some $u \in Z$.

For an arbitrary $r \in Z$, $pr = m(ur) \in S$, since (ur) is an integer.

$\therefore p \in S, r \in Z \Rightarrow pr \in S, rp \in S$

$\therefore$ S is an ideal of the ring Z.

Thus every subring of the ring Z is an ideal.

Ex.2. Every subring of the ring Z_n is an ideal.

The subrings of the ring Z_n are precisely the cyclic subgroups of the group $(Z_n, +)$ generated by positive divisors (d) of n.

when $d = 1$, the subring is Z_n itself (improper ideal)

when $d = n$, " " " $\{\bar{0}\}$, the trivial subring (null ideal)

Let m be a proper +ve divisor of n and $n = md$ $(1 < d < n)$.

Then $S = \{\bar{m}, 2\bar{m}, 3\bar{m}, \cdots, (d-1)\bar{m}, \bar{0}\}$ is a subring of the ring Z_n.

Let $a \in S$, $\bar{p} \in Z_n$. Then $a = s\bar{m}$, $1 \le s \le d$; $1 \le p \le n$.

$ps = qd + r$, $0 \le r < d$

Then $pa = ps\bar{m} = qd\bar{m} + r\bar{m} = r\bar{m} \in S$.

$\Rightarrow ap \in S$ [$\because$ Z_n is a commutative ring].

$\therefore$ S is an ideal of the ring Z_n.

Thus every subring of the ring Z_n is an ideal.

(3) $(Z, +, \cdot)$ is a subring of the ring $(Q, +, \cdot)$.

But $(Z, +, \cdot)$ is not an ideal of $(Q, +, \cdot)$, since $a \in Z$, $q \in Q$ does not necessarily imply $qa \in Z$.

(4). Let R be the ring of all real valued continuous fns. defined on $[0, 1]$ and let $S = \{f \in R : f(\frac{1}{2}) = 0\}$. Then S is an ideal of R.

S is non-empty subset of R, since the zero fn. $0 \in S$.

$f - g$ is continuous fn. on $[0, 1]$ and $(f-g)(\frac{1}{2}) = 0$.

$\Rightarrow f - g \in S$.

Let $h \in R$, $f(\frac{1}{2}) = 0 = fh(\frac{1}{2}) \Rightarrow hf \in S$, $fh \in S$.

$\therefore$ $f \in S$, $h \in R \Rightarrow hf \in S$ and $fh \in S$.

$\therefore$ S is an ideal of R.

Th: Let S and T be two ideals of a ring R. Then $S \cap T$ is an ideal of R.

Note: The intersection of a family of ideals of R is an ideal of R.

Note: The union of two ideals of a ring R may not be an ideal of R.

Let $R = (\mathbb{Z}, +, \cdot)$, $S = (2\mathbb{Z}, +, \cdot)$, $T = (3\mathbb{Z}, +, \cdot)$
Then S and T are ideals of R but $S \cup T$ is not an ideal of R, since $3 \in S \cup T$, $2 \in S \cup T$ but $3-2 \notin S \cup T$.

Th: $S \cup T$ is an ideal of R iff either $S \subset T$ or $T \subset S$.

Conversely, Let $S \cup T$ be an ideal of R.
Let us suppose that neither $T \subset S$ nor $S \subset T$.
Then both $T - S$ and $S - T$ are non-empty.
Let $x \in T - S$, $y \in S - T$.
$x \in S \cup T$, $y \in S \cup T \Rightarrow x - y \in S \cup T$.
If $x - y \in S$, $(x-y) + y \,(= x) \in S$, a contradiction.
If $x - y \in T$, $x - (x-y)\,[= y] \in T$, " "
$\therefore$ our assumption is wrong.

Th: $S + T = \{s + t : s \in S, t \in T\}$ is an ideal of R and it is the smallest ideal of R containing both S & T.
$0 \in S$, $0 \in T \Rightarrow 0 \in S+T \Rightarrow S+T$ is non-empty.
$a \in S+T$, $b \in S+T \Rightarrow a - b \in S+T$.
Let $r \in R$ be arbitrary, $ar = (s_1 + t_1)r = s_1 r + t_1 r \in S+T$.
Also $ra \in S+T$.
$\therefore$ $S+T$ is an ideal of R.
To prove the smallest ideal:
Let P be any ideal containing both S & T.
Let $x \in S+T$, let $x = s_1 + t_1$, $T \subset P \Rightarrow t_1 \in P \Rightarrow s_1 + t_1 \in P$.
$S \subset P \Rightarrow x \in P$. $[s_1 \in P, T \subset P \Rightarrow t_1 \in P \Rightarrow s_1 + t_1 \in P$.
$\therefore x \in S+T \Rightarrow x \in P \Rightarrow S+T \subset P$.

Th: If an ideal S of a ring R with unity contains a unit of R, then $S = R$.
Let S contains a unit u of R. $\Rightarrow u^{-1} \in R$.
$u u^{-1} = u^{-1} u = 1$.
$u \in S$ $u^{-1} \in R \Rightarrow u u^{-1} \in S \Rightarrow 1 \in S$.
Let $a \in R$. $a \in R$, $1 \in S \Rightarrow a \in S \Rightarrow R \subset S$. Also $S \subset R$
$\therefore S = R$.

Subring:

Let $(R,+,\cdot)$ be a ring and S be a non-empty subset of R s.t. S is stable under $+$ and $\cdot$, i.e.,

$a,b \in S \Rightarrow a+b \in S,\ a\cdot b \in S.$

The restriction maps $\oplus, \odot$ of $+,\cdot : \oplus, \odot : S\times S \to S$, defined by $a \oplus b = a+b$, $\forall\ a,b \in S$.
& $a \odot b = a\cdot b$ " "

If S forms a ring under $\oplus$ & $\odot$, S is said to be a subring of R.

Definition: A non-empty subset S of R is said to be a subring of $(R,+,\cdot)$ if S forms a ring under the compositions $+$ and $\cdot$ restricted to S.

Improper Subring
Trivial "

eg: $(\mathbb{Z},+,\cdot)$ is a ring. $(2\mathbb{Z},+,\cdot)$ is a subring.

Ideals.

Ex. The ideal $p\mathbb{Z}+q\mathbb{Z}$ of the ring $\mathbb{Z}$ is the ideal $\mathbb{Z}$ itself, where $\gcd(p,q)=1$. p,q are +ve integers.

$\gcd(p,q)=1 \Rightarrow pu+qv=1$ for some $u,v \in \mathbb{Z}$

Since $u\in\mathbb{Z}$, $pu \in p\mathbb{Z}$, since $v\in\mathbb{Z}$, $qv \in q\mathbb{Z}$.

$\therefore pu+qv \in p\mathbb{Z}+q\mathbb{Z} \Rightarrow 1 \in p\mathbb{Z}+q\mathbb{Z}$.

As the ideal $p\mathbb{Z}+q\mathbb{Z}$ of the ring contains the identity element of $\mathbb{Z}$, $p\mathbb{Z}+q\mathbb{Z}=\mathbb{Z}$., because.

$1 \in p\mathbb{Z}+q\mathbb{Z}$, and $a\in\mathbb{Z} \Rightarrow 1.a \in p\mathbb{Z}+q\mathbb{Z}$.

$\therefore \mathbb{Z} \subset p\mathbb{Z}+q\mathbb{Z} \Rightarrow \mathbb{Z} = p\mathbb{Z}+q\mathbb{Z}$ [$\because p\mathbb{Z}+q\mathbb{Z} \subset \mathbb{Z}$]

A division ring/field has no non-trivial proper ideals

Let S be a non-trivial ideal of R.
Then S contains a non-zero element of R which is also a unit in R.
Since S is an ideal of R with unity and S contains a unit of R. $\Rightarrow S=R$.
$\therefore R$ has no non-trivial proper ideal.

Note: Simple ring $\longrightarrow$ if it has no non-trivial proper ideals

Subrings & Ideals..

Subrings of the ring Z_n:

Let $(T,+,\cdot)$ be a subring of the ring Z_n. Then the group $(T,+)$ must be a subgroup of the group $(Z_n,+)$. As the group $(Z_n,+)$ is cyclic, the subgroup $(T,+)$ is also cyclic.

For every +ve divisor d of n, there is one and only one subgroup of $(Z_n,+)$ of order d and it is generated by n/d, a divisor of n.

Let d be a +ve divisor other than 1 and n.

Let $n = md$ $(1<m<n)$. Then m is a +ve divisor of n and $\bar{m} \in Z_n$ generates the additive cyclic subgroup $S = \{\bar{m}, 2\bar{m}, 3\bar{m}, 4\bar{m}, \cdots, (d-1)\bar{m}, \bar{0}\}$ of order d.

We prove that S is a subring of Z_n.

Let $x, y \in S$. Then $x = p\bar{m}$, $y = q\bar{m}$ for $p, q \in Z$ s.t. $0 \le p, q < d$.

Then $x.y = p\bar{m} \cdot q\bar{m}$

Now, let $pqm = \lambda d + \mu$, where $\lambda, \mu \in Z$ s.t. $0 \le \mu < d$.

Then $(pm)(qm) = \lambda md + \mu m = \lambda n + \mu m$.

$\Rightarrow (p\bar{m})(q\bar{m}) = \mu\bar{m}$

$\therefore x.y = \mu\bar{m} \in S$, since $0 \le \mu < d$.

$\therefore (S,+,\cdot)$ is a subring of the ring Z_n.

If $d = 1$ or $d = n$, then we have the trivial subring $\{\bar{0}\}$ or the improper subring Z_n resp.

$\therefore$ The all subrings of the ring Z_n is same as the " cyclic subgroups of the group $(Z_n,+)$ generated by +ve divisor of n.

eg: The subrings of the ring Z_6 are: $Z_6, \{\bar{2}, \bar{4}, \bar{0}\}, \{\bar{3}, \bar{0}\}$ and $\{\bar{0}\}$ corres. to the divisors 1, 2, 3 & 6.

The subrings of the ring Z_8 are:
$Z_8, \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\}, \{\bar{4}, \bar{0}\}$ and $\{\bar{0}\}$ corres. to the divisors 1, 2, 4 & 8.

$o(a) = d$

Every subring of the ring Z_n is an ideal.

We have the subrings of the ring Z_n are the cyclic subgroups of the group $(Z_n, +)$ generated by +ve divisors of n.

We have the improper ideal Z_n and the null ideal $\{\bar{0}\}$ corres. to the improper divisors 1 and n.

Let m be a proper +ve divisor of n and $n = md$ $(1 < d < n)$

Then $S = \{\bar{m}, 2\bar{m}, 3\bar{m}, \ldots, (d-1)\bar{m}, \bar{0}\}$ is a subring of Z_n.

Let $a \in S$ and $\bar{p} \in Z_n$ then $a = u\bar{m}$ for $u \in Z$ s.t. $1 \le u \le d$ and $1 \le p \le n$.

pu is a +ve integer. By D.A., $pu = qd + r$, $0 \le r < d$

Then $pa = pu\bar{m} = qd\bar{m} + r\bar{m} = r\bar{m} \in S$

$\therefore pa \in S \Rightarrow ap \in S$, since Z_n is a Commutative ring

$\therefore S$ is an ideal of the ring Z_n.

Thus every subring of the ring Z_n is an ideal.

Principal ideal in a ring:

Let S be a non-empty subset of a ring R. The intersection of all ideals of R containing S is the smallest ideal of R containing S. This is called the ideal generated by S.

In particular, if S be a single element of R, then the ideal generated by the element is called a principal ideal of R.

$\therefore$ Corresponding to each element of a ring R there is a principal ideal of R.

Definition → The smallest ideal of R containing the element $a \in R$, is said to be a principal ideal of R. It is said to be the ideal generated by a and is denoted by $\langle a \rangle$.

Alternatively, an ideal U of a ring R is said to be a principal ideal of R if $U = \langle a \rangle$ for some $a \in R$.

Examples:

① Let R be a ring. The null ideal $\{\bar{0}\}$ is the smallest ideal of R containing the element 0. The null ideal $\{\bar{0}\}$ is a principal ideal of R

② Let R be a ring with unity 1. Let U be the smallest ideal of R containing the element 1. Since U is an ideal $a \in R, 1 \in U \Rightarrow 1.a \in U \Rightarrow a \in U \Rightarrow U = R$, R is the principal ideal.

(3) In the ring $(\mathbb{Z}, +, \cdot)$, the subring/ideal $m\mathbb{Z}$, is a principal ideal (m being a +ve integer). We show that the ideal $m\mathbb{Z}$ is the smallest ideal containing the element m.

Let U be any ideal of the ring $\mathbb{Z}$ containing m.

Then $ma \in U$, as $m \in U, a \in \mathbb{Z} \Rightarrow ma \in U, \forall a \in \mathbb{Z}$.

$\Rightarrow m\mathbb{Z} \subset U$.

This proves that $m\mathbb{Z}$ is a principal ideal of the ring $\mathbb{Z}$.

Here, all ideals of the ring $\mathbb{Z}$ are principal ideals $m\mathbb{Z} (m \in \mathbb{Z}, m \geq 0)$.

eg. In the ring $2\mathbb{Z}$, the subring $\{0, \pm 1, \pm 8, \pm 12, \ldots\}$ is an ideal. It is the smallest ideal containing the element 1. It is the principal ideal $\langle A \rangle$.

(4) Let us consider the ring $R = \mathbb{Z} \times \mathbb{Z}$, where

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

$(a,b) \cdot (c,d) = (ac, bd)$, $\forall (a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}$.

The subring S of all ordered pairs $\{(a,0) : a \in \mathbb{Z}\}$ is an ideal of R, which is the smallest ideal containing the element $(1,0)$ of R.

Let U be any ideal of R containing $(1,0)$.

Let $(p,0) \in S$. Then $(p,b) \in R$, $\forall b \in \mathbb{Z}$.

$(1,0) \in U, (p,b) \in R \Rightarrow (1,0) \cdot (p,b) = (p,0) \in U$.

$\therefore S \subset U$.

Hence S is a principal ideal.

Theorem: Let R be a commutative ring with unity and $a \in R$. Then the set $Ra = \{ra : r \in R\}$ is a principal ideal of R generated by a.

First to prove: Ra is an ideal of R.

$0 \in R \Rightarrow 0a \in Ra \Rightarrow 0 \in Ra \Rightarrow Ra$ is a non-empty subset of R.

Let $p = r_1 a \in Ra$, $q = r_2 a \in Ra$ for $r_1, r_2 \in R$.

$\therefore p - q = (r_1 - r_2)a \in Ra$, $\because r_1 - r_2 \in R$

Let $r \in R$, $p = r_1 a \in Ra$. Then $rp = r(r_1 a) = (rr_1)a \in Ra$.

Also $pr \in Ra$ since R is a commutative ring.

$\therefore Ra$ is an ideal of R.

To prove: Ra is a principal ideal of R and $Ra = \langle a \rangle$

Let U be any ideal of R containing a, and let $ra \in Ra$ for some $r \in R$.

$\therefore r \in R, a \in U \Rightarrow ra \in U$, since U is an ideal.

$\therefore Ra \subset U \Rightarrow Ra$ is a principal ideal generated by a

Principal Ideal Ring:

A ring is said to be a principal ideal ring if every ideal of the ring is a principal ideal.

Examples:

① The ring $\mathbb{Z}$ is a principal ideal ring.

The ideals are: $m\mathbb{Z}$ where m is a non-negative integer.

Let $m = 0$. Then $m\mathbb{Z}$ is the null ideal $\{\bar{0}\}$. It is the principal ideal $\langle 0 \rangle$.

Let m be a +ve integer and let $U = m\mathbb{Z}$, m being the least +ve integer in U. $U = \{rm : r \in \mathbb{Z}\}$ is the principal ideal generated by m, since $\mathbb{Z}$ is a commutative ring with unity and $U = \{rm : r \in \mathbb{Z}\}$.

Thus every ideal in $\mathbb{Z}$ is a principal ideal, being $\mathbb{Z}$ is a principal ideal ring.

② Show that the ring $\mathbb{Z}_n$ is a principal ideal ring.

Let U be an ideal of $\mathbb{Z}_n$.

If U be the null ideal then $U = \langle \bar{0} \rangle$ and it is the principal ideal

If $U = \mathbb{Z}_n$, then $U = \langle \bar{1} \rangle$ and it is the principal ideal.

In the ring $\mathbb{Z}_n$, every subring is an ideal and the subrings are the cyclic subgroups of $(\mathbb{Z}_n, +)$ generated by positive divisors of n.

Let $U = \{\bar{m}, 2\bar{m}, 3\bar{m}, \ldots, (d-1)\bar{m}, \bar{0}\}$, where m is a proper +ve divisor of n and $n = md$. Then $1 < d < n$ and U becomes an ideal in $\mathbb{Z}_n$.

Let m is the least +ve integer s.t. $\bar{m} \in U$.

$$U = \{p\bar{m} : 1 \le p \le d\}$$

Let $H = \{r\bar{m}, r \in \mathbb{Z}_n\}$

$\bar{m} \in U, r \in \mathbb{Z}_n \Rightarrow r\bar{m} \in U$

$\therefore H \subset U$.

Again $U \subset H$ $\Rightarrow U = H$

U is the principal ideal generated by m.

* Since $\mathbb{Z}_n$ is a commutative ring with unity, and $U = \{r\bar{m} : r \in \mathbb{Z}_n\}$,

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

Prime ideal in a ring:

In a ring R, an ideal $P \neq R$ is said to be a prime ideal if for $a, b \in R$, $a \cdot b \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Maximal ideal in a ring:

In a ring R, an ideal $M \neq R$ is said to be a maximal ideal in R if for any ideal U of R satisfying $M \subset U \subset R$, either $U = M$ or $U = R$.

i.e., a maximal ideal M of a ring R is such that there exists no proper ideal of R strictly containing M.

Examples:

① In the null ideal $\{0\}$ in the ring $\mathbb{Z}$ is a prime ideal, since for $a, b \in \mathbb{Z}$, $a \cdot b \in \{0\} \Rightarrow a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0 \Rightarrow a \in \{0\}$ or $b \in \{0\}$.

② The ideal $2\mathbb{Z}$ in the ring $\mathbb{Z}$ is a prime ideal

Let $a \cdot b \in 2\mathbb{Z}$ for some $a, b \in \mathbb{Z}$.

$\Rightarrow a \cdot b = 2m$, $m \in \mathbb{Z}$.

$\Rightarrow 2 \mid a \cdot b \Rightarrow 2 \mid a$ or $2 \mid b$.

$2 \mid a \Rightarrow a \in 2\mathbb{Z}$, $2 \mid b \Rightarrow b \in 2\mathbb{Z}$.

$\therefore ab \in 2\mathbb{Z} \Rightarrow$ either $a \in 2\mathbb{Z}$ or $b \in 2\mathbb{Z}$

$\Rightarrow 2\mathbb{Z}$ is a prime ideal in the ring $\mathbb{Z}$

③ BUT, the ideal $4\mathbb{Z}$ in the ring $2\mathbb{Z}$ is not a prime ideal, since $2 \cdot 2 \in 4\mathbb{Z}$, where $2 \notin 4\mathbb{Z}$.

④ The ideal $4\mathbb{Z}$ in the ring $\mathbb{Z}$ may not be a prime ideal, since $a \cdot b \in 4\mathbb{Z} \Rightarrow a \cdot b = 4m$, $m \in \mathbb{Z}$,

$\Rightarrow 4 \mid a \cdot b \Rightarrow$ either $4 \mid a$ or $4 \mid b$

$\Rightarrow$ or ~~either~~ $2 \mid a$ and $2 \mid b$

$\Rightarrow 2 \mid a \Rightarrow a \in 2\mathbb{Z}$, $2 \mid b \in b \in 2\mathbb{Z}$.

$\therefore a \cdot b \in 4\mathbb{Z} \Rightarrow a \in 2\mathbb{Z}$ & $b \in 2\mathbb{Z}$

$a \notin 4\mathbb{Z}$ or $b \notin 4\mathbb{Z}$.

$\therefore 4\mathbb{Z}$ may not be a prime ideal.

⑤ But the ideal $5\mathbb{Z}$ in the ring $2\mathbb{Z}$ is a prime ideal, since $a \cdot b \in 5\mathbb{Z} \Rightarrow$ either $a \in 5\mathbb{Z}$ or $b \in 5\mathbb{Z}$,

$\Rightarrow 5\mathbb{Z}$ is a prime ideal in the ring $\mathbb{Z}$.

Infact, the prime ideals in the ring $\mathbb{Z}$ are the ideals $p\mathbb{Z}$, where p is either 0 or a prime.

Let p be a prime.

To prove: $p\mathbb{Z}$ is a prime ideal.

Let $a, b \in \mathbb{Z}$ s.t. $a \cdot b \in p\mathbb{Z}$. Then

$a \cdot b = pm$ for some $m \in \mathbb{Z}$.

$\Rightarrow p \mid a \cdot b \Rightarrow$ either $p \mid a$ or $p \mid b$ [Since p is prime]

$p \mid a \Rightarrow a = pu$ for some $u \in \mathbb{Z}$, hence $a \in p\mathbb{Z}$

$p \mid b \Rightarrow b \in p\mathbb{Z}$.

Thus $a \cdot b \in p\mathbb{Z} \Rightarrow$ either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$

$\therefore p\mathbb{Z}$ is a prime ideal in the ring $\mathbb{Z}$.

Conversely, let $p\mathbb{Z}$ be a non-null prime ideal in $\mathbb{Z}$.

$\therefore p \neq 0$. Since $p\mathbb{Z}$ is a prime ideal, $p\mathbb{Z} \neq \mathbb{Z}$ and hence $p \neq 1$.

Let $p \mid ab$ for $a, b \in \mathbb{Z}$.

$\Rightarrow a \cdot b = p \cdot u$ for $u \in \mathbb{Z}$. $\Rightarrow a \cdot b \in p\mathbb{Z} \Rightarrow$ either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$

$a \in p\mathbb{Z} \Rightarrow p \mid a$, $b \in p\mathbb{Z} \Rightarrow p \mid b$

$\therefore p \mid a \cdot b \Rightarrow$ either $p \mid a$ or $p \mid b \Rightarrow$ p is a prime.

Th: P, Q are prime ideals of a commutative ring R. Then $P \cap Q$ is a prime ideal of R iff either $P \subset Q$ or $Q \subset P$.

Let $P \cap Q$ be a prime ideal.

To prove; either $P \subset Q$ or $Q \subset P$, i.e.,

" $P - Q$ or $Q - P$ is empty.

If possible, let $x \in P - Q$, $y \in Q - P$.

$\therefore x \in P$, $x \notin Q$; $y \in Q$, $y \notin P$.

Since P is an ideal of R, $x \in P$, $y \in Q - P \subset R \Rightarrow x \cdot y \in P$

" Q " " " " " , $y \in Q$, $x \in P - Q \subset R \Rightarrow x \cdot y \in Q$.

$\therefore xy \in P \cap Q \Rightarrow$ either $x \in P \cap Q$ or $y \in P \cap Q$.

But $x \notin Q$ & $y \notin P$, $\therefore$ it is a contradiction,

$\therefore P - Q$ or $Q - P$ is empty; either $P \subset Q$ or $Q \subset P$.

Conversely: Let either $P \subset Q$ or $Q \subset P$.

If $P \subset Q$, then $P \cap Q = P$, } which are prime ideals

& if $Q \subset P$, " $P \cap Q = Q$ }

$\therefore P \cap Q$ is a prime ideal of R.