Chapter - 14th
Ideals and Factor Rings

Ideal :- A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$, both ra and ar are in A.

Or

A non empty subset A of R is called a (two-sided) ideal of R if

(i) $a - b \in A \quad \forall\, a, b \in A$

(ii) $ra, ar \in A \quad \forall\, r \in R,\ a \in A$.

Note :- (i) An ideal A of R is called a proper ideal of R if A is a proper subset of R.

(ii) Every ideal is a subring but not conversely.

for e.g. :- $\mathbb{Q}$, the set of rational numbers is a ring under usual addition and usual multiplication.

$\mathbb{Z} \subseteq \mathbb{Q}$ is subring of $\mathbb{Q}$, but $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$ because $\frac{1}{2} \in \mathbb{Q}$, $3 \in \mathbb{Z} \Rightarrow \frac{3}{2} \notin \mathbb{Z}$.

(iii) Let R be a ring with unity and I be an ideal of R. Let u be a unit in R.

Claim: If $u \in I$, then $I = R$.

Let $u \in I$. Since $u^{-1} \in R$, then $u^{-1}u \in I \Rightarrow 1 \in I$

Since $1 \in I$, let $r \in R$ be any element, then

$$r1 \in I \Rightarrow r \in I \Rightarrow R \subseteq I \Rightarrow I = R.$$

So we conclude that if a unit belongs to an ideal I, then $I = R$.

Examples of Ideal :

Example 1: For any ring R, $\{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the trivial ideal.

Example: 2 For any positive integer n, the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, --\}$ is an ideal of $\mathbb{Z}$.

Example 3: Let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra : r \in R\}$ is an ideal of R, called the principal ideal generated by a.

Solution: $\langle a \rangle = \{ra : r \in R\}$. Clearly $\langle a \rangle$ is non empty as $0a = 0 \in \langle a \rangle$.

(i) $r_1 a, r_2 a \in \langle a \rangle$ where $r_1, r_2 \in R$

$r_1 a - r_2 a = (r_1 - r_2) a \in \langle a \rangle$ because $r_1 - r_2 \in R$.

(ii) Let $s \in R$ and $ra \in \langle a \rangle$.

$s(ra) = (sr)a \in \langle a \rangle$ because $sr \in R$ and

$(ra)s = s(ra) = (sr)a \in \langle a \rangle$ ($\because R$ is commutative)

$\therefore$ $s(ra)$ and $(ra)s$ both are in $\langle a \rangle$.

$\Rightarrow \langle a \rangle$ is an ideal of R generated by a.

Example ⇒ 4. Let $\mathbb{R}[x]$ denote the set of all polynomials with real coefficients and let A denote the subset of all polynomials with constant term 0. Show that A is an ideal of $\mathbb{R}[x]$ and $A = \langle x \rangle$.

Solution ⇒ To show ⇒ A is an ideal of $\mathbb{R}[x]$ and $A = \langle x \rangle$.

Note that $A = \{ f(x) \in \mathbb{R}[x] : f(0) = 0 \}$

Clearly zero polynomial belongs to A, so $A \neq \phi$.

(i) Let $f(x), g(x) \in A \Rightarrow f(0) = 0, g(0) = 0$

Now $f(0) - g(0) = 0 \Rightarrow f(x) - g(x) \in A$.

(ii) Let $r(x) \in \mathbb{R}[x]$ and $f(x) \in A \Rightarrow f(0) = 0$.

$\Rightarrow r(0) f(0) = (r(0)) 0 = 0 \Rightarrow r(x) f(x) \in A$.

Also $f(0) r(0) = 0 \Rightarrow f(x) r(x) \in A \Rightarrow$ A is an ideal.

Now Claim: $A = \langle x \rangle = \{ r(x) . x : r(x) \in \mathbb{R}[x] \}$.

Since A contains all polynomials with constant term 0,

let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x \in A$

$= (a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_2 x + a_1) x$

$\Rightarrow f(x) \in \langle x \rangle$ as $a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_2 x + a_1 \in \mathbb{R}[x]$

$\therefore A \subseteq \langle x \rangle$.

Let $s(x) \in \langle x \rangle$, then $s(x)$ must be of the form

$s(x) = (r(x)) x \Rightarrow$ clearly $s(x)$ has no constant term

$\Rightarrow s(x) \in A$.

$\therefore\ A = \langle x \rangle$

or A is a principal ideal generated by x.

Example:- 5. Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n \in R$. Then $I = \langle a_1, a_2, \ldots, a_n \rangle$

$= \{ r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_i \in R \}$ is an ideal of R, called ideal generated by $a_1, a_2, \ldots, a_n$.

Solution:- Proof is similar to Example 3. Do yourself.

Example: 6 Let $\mathbb{Z}[x]$ denote the ring of all polynomials with integer coefficients. Let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant term. Show that I is an ideal of $\mathbb{Z}[x]$ and $I = \langle x, 2 \rangle$.

Solution:- Note that $I = \{ f(x) \in \mathbb{Z}[x] : f(0) \text{ is even integer} \}$.

Clearly zero polynomial belongs to $I \Rightarrow I \neq \phi$.

(i) Let $f(x), g(x) \in I \Rightarrow f(0), g(0)$ both are even integers.

Now $f(0) - g(0)$ is even integer $\Rightarrow f(x) - g(x) \in I$.

(ii) Let $r(x) \in \mathbb{Z}[x]$ and $f(x) \in I \Rightarrow f(0)$ is even integer.

Note that $r(0) f(0)$ is even integer $\Rightarrow r(x) f(x) \in I$

Also $f(0) r(0)$ is also an even integer $\Rightarrow f(x) r(x) \in I$

Hence I is an ideal of $\mathbb{Z}[x]$.

Next Claim : $I = \langle x, 2 \rangle$.

Note that $\langle x, 2\rangle = \{r(x)\,x + (s(x))\,2 \;:\; r(x), s(x) \in \mathbb{Z}[x]\}$

by definition given in Example 5.

Let $f(x) \in \langle x,2\rangle$, then $f(x)$ must be of the form

$(r(x))\,x + (s(x))\,2$.

Suppose that $f(x) = \underbrace{(p(x))\,x}_{\text{No Constant term}} + \underbrace{(q(x))\,2}_{\text{Constant term must be even (if exists).}}$ for some $p(x), q(x) \in \mathbb{Z}[x]$.

$\therefore f(x) \in I. \Rightarrow \langle x,2\rangle \subseteq I$ - (1)

On other hand, suppose that $f(x) \in I$

$\Rightarrow f(x)$ is a polynomial with constant term even.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + \underbrace{a_0}_{\text{must be even}}$

$$= (a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_2 x + a_1)\,x + 2a_0'$$

$\left[\because a_0 = 2a_0' \text{ for some integer } a_0'\right]$

$\Rightarrow f(x)$ is of the form $(r(x))\,x + (s(x))\,2$

$\Rightarrow f(x) \in \langle x,2\rangle \Rightarrow I \subseteq \langle x,2\rangle$ - (2)

Hence from (1), (2) $I = \langle x,2\rangle$.

Example 7. Let R be the ring of all real-valued functions of a real variable. The subset S of all differentiable functions is a subring of R but not an ideal of R.

Solution: $S = \{ f \in R : f : \mathbb{R} \to \mathbb{R}$ is a differentiable function $\}$

Prove yourself, S is a subring of R.

Let $f \in S$ be a differentiable function from $\mathbb{R}$ to $\mathbb{R}$ given by $f(x) = x \;\; \forall x \in \mathbb{R}$.

and $r \in R$ be a function from $\mathbb{R}$ to $\mathbb{R}$ given by

$$r(x) = \begin{cases} x^{3/2} & ; x \geq 0 \\ x^{-3/2} & ; x < 0 \end{cases}$$

Now
$$r(x) f(x) = \begin{cases} x^{5/2} & ; x \geq 0 \\ x^{-1/2} & ; x < 0 \end{cases}$$

is not differentiable at $x = 0$.

$\Rightarrow rf \notin S \Rightarrow S$ is not an ideal of R.

Example 8. Let $R = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} : a_i \in \mathbb{Z} \right\}$ is a ring with usual addition and multiplication of matrices.

I be a subset of R consisting of matrices with even entries.

$$I = \left\{ \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} : b_1, b_2, b_3, b_4 \text{ are even integers} \right\}$$

Prove yourself that I is an ideal of R.

Example:- 9 $\mathbb{Z}_6$ is a ring. Let $S = \{0, 2, 4\} \subseteq \mathbb{Z}_6$.

S is a subring of $\mathbb{Z}_6$ (Discussed in Chapter 12)

Let $r \in \mathbb{Z}_6$ and $a \in S$., note that $ra, ar \in S$.

So S is also an ideal of $\mathbb{Z}_6$.

Factor Ring:

Theorem:- 14.2 Let R be a ring and A be a subring of R. The set of cosets $\{r + A : r \in R\}$ is a ring under the operations $(s+A) + (t+A) = (s+t) + A$ and $(s+A)(t+A) = st + A$ iff A is an ideal of R.

Proof:- Consider A is an ideal of R.

To prove:- $X = \{r + A : r \in R\}$ is a ring.

Since A is a normal subgroup of R under addition.

$\therefore$ X is clearly an Abelian group under addition

Now we show multiplication of any two cosets in X is well defined.

Let $(s+A,\ t+A) = (s'+A,\ t'+A)$

<u>To show</u>: $st+A = s't'+A$

Since $s+A = s'+A$ and $t+A = t'+A$

$\Rightarrow s-s' \in A$ and $t-t' \in A$

$\Rightarrow s-s' = a_1$ and $t-t' = a_2$ for some $a_1, a_2 \in A$

$\Rightarrow s = s'+a_1$ and $t = t'+a_2$

Now $st+A = (s'+a_1)(t'+a_2)+A = s't'+s'a_2+a_1t'+a_1a_2+A$

$= s't'+A \quad (\because s'a_2+a_1t'+a_1a_2 \in A)$

$\therefore st+A = s't'+A \Rightarrow$ Multiplication is well defined.

It is trivial to prove that multiplication is associative and distributive property. Hence X forms a ring under the given operations.

<u>Conversely</u> $\Rightarrow$ Let if possible A is a subring but not an ideal. Then there must exist elements $a \in A$ and $r \in R$ such that $ar \notin A$ or $ra \notin A$. Say $ar \notin A$. Consider the elements $a+A = 0+A$ and $r+A$ in X.

Clearly $(a+A)(r+A) = ar+A$ is a non zero element of X as $ar \notin A$, but $(0+A)(r+A) = 0r+A = A$.

Since $ar+A \neq 0+A \Rightarrow$ multiplication is not well defined $\Rightarrow$ X is not a ring which is a contradiction

Hence A is an ideal.

Note:⇒ 1. Let A be an ideal of R, then the set of cosets $\{r+A : r \in R\}$ forms a ring under the operations $(s+A)+(t+A)=(s+t)+A$ and $(s+A)(t+A) = st+A$. This ring is called <u>Factor ring</u> and denoted by <u>R/A</u>.

Note:- 2. In factor ring R/A, notice that $0+A$ is <u>addition identity</u> (zero element) and $(-r)+A$ is <u>additive inverse</u> of element $r+A$.

Imp

Note:- 3. Let A be an ideal of ring R, then

$$r+A = A \text{ iff } r \in A.$$

Proof:- Firstly we know that every ideal is a normal subgroup of R under addition.

Now consider $r+A=A$. <u>To show</u>: $r \in A$.

Since $r+A=A$, $r+0 \in r+A = A \Rightarrow r \in A$.

Conversely:⇒ Consider $r \in A$. <u>To prove</u>: $r+A=A$.

Let $r+a \in r+A \Rightarrow r+a \in A$ [$\because r, a \in A$ and A is a normal subgp of R under addition]

$\Rightarrow r+A \subseteq A$

Now let $a \in A \Rightarrow r+((-r)+a) \in r+A$ [$\because r \in A \Rightarrow -r \in A \Rightarrow -r+a \in A$]

$\Rightarrow a \in r+A$

$\Rightarrow A \subseteq r+A$, Hence $r+A=A$.

Note :- 4. Let A be an ideal of R, then

$$r + A = s + A \text{ iff } r - s \in A.$$

Proof :- Prove yourself

Note :- 5 Let R be a ring with unity and A be an ideal of R, then R/A also has unity.

Proof :- Let 1 be unity of R.

Claim :- $1 + A$ is unity of factor ring R/A.

Let $r + A$ be any element of R/A.

Now $(r+A)(1+A) = r1 + A = r + A$ and

$(1+A)(r+A) = 1r + A = r + A$.

Hence proved.

Note :- 6 Let R be a commutative ring and A be an ideal of R, then R/A is also commutative ring.

Note :- 7 Let R be a ring with unity and u be a unit in R, and A be an ideal of R, then $u + A$ is unit in R/A provided $A \neq R$.

Prove yourself Note 6, Note 7. Very easy proofs.

Examples of Factor Rings.

Example :- $4\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Then

$\mathbb{Z}/4\mathbb{Z} = \{a + 4\mathbb{Z} : a \in \mathbb{Z}\}$ is a factor ring.

First of all, we find the elements of $\mathbb{Z}/4\mathbb{Z}$.

Let $a+4\mathbb{Z}$ be any element of $\mathbb{Z}/4\mathbb{Z}$

By division algorithm

$\exists$ $q, r \in \mathbb{Z}$ such that

$$a = 4q + r, \quad 0 \le r \le 3.$$

$$\therefore a + 4\mathbb{Z} = r + 4q + 4\mathbb{Z} = r + 4\mathbb{Z}, \; 0 \le r \le 3$$

$$[\because 4q \in 4\mathbb{Z} \Rightarrow 4q + 4\mathbb{Z} = 4\mathbb{Z}]$$

$\therefore$ $\mathbb{Z}/4\mathbb{Z}$ has only elements $0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}$

or $\mathbb{Z}/4\mathbb{Z} = \{r + 4\mathbb{Z} : r = 0, 1, 2, 3\}$ is a factor ring. Also note that $\mathbb{Z}/4\mathbb{Z}$ is commutative ring with unity $(1+4\mathbb{Z})$.

Take two elements $2+4\mathbb{Z}, 3+4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$.

We see how to add and multiply these elements

$$(2+4\mathbb{Z}) + (3+4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$$

and
$$(2+4\mathbb{Z})(3+4\mathbb{Z}) = 2\cdot 3 + 4\mathbb{Z} = 6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z} = 2 + 4\mathbb{Z}.$$

$\therefore$ $\mathbb{Z}/4\mathbb{Z}$ is a finite commutative factor ring with unity. (Is $3+4\mathbb{Z}$ a unit?)

Example → $6\mathbb{Z}$ is an ideal of $2\mathbb{Z}$.

So factor ring $2\mathbb{Z}/6\mathbb{Z} = \{a+6\mathbb{Z} : a \in 2\mathbb{Z}\}$.

Firstly we find elements of $2\mathbb{Z}/6\mathbb{Z}$.

By division algorithm, $\exists\ q, r \in \mathbb{Z}$ such that

$a = 6q + r$, $0 \le r \le 5$ and r is even

$\therefore\ a + 6\mathbb{Z} = 6q + r + 6\mathbb{Z} = r + 6\mathbb{Z}$ as $6q \in 6\mathbb{Z}$.

$$\therefore\ 2\mathbb{Z}/6\mathbb{Z} = \{r + 6\mathbb{Z} : 0 \le r \le 5,\ r \text{ is even}\}$$
$$= \{0+6\mathbb{Z},\ 2+6\mathbb{Z},\ 4+6\mathbb{Z}\}.$$

So $2\mathbb{Z}/6\mathbb{Z}$ is a finite (three elements) factor ring which is commutative clearly.

Is $2\mathbb{Z}/6\mathbb{Z}$ a ring with unity? If yes, what is the unity element?

Example → See Example 10 in Book at P. 251.

$$R/I = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + I : \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in R \right\}$$

$$= \left\{ \begin{bmatrix} 2q_1+r_1 & 2q_2+r_2 \\ 2q_3+r_3 & 2q_4+r_4 \end{bmatrix} + I : q_i \in \mathbb{Z},\ r_i \in \mathbb{Z} \text{ and } 0 \le r_i \le 1 \right\}$$

$$R/I = \left\{ \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + \begin{bmatrix} 2q_1 & 2q_2 \\ 2q_3 & 2q_4 \end{bmatrix} + I : q_i \in \mathbb{Z}, r_i \in \mathbb{Z}, \ 0 \le r_i \le 1 \right\}$$

$$= \left\{ \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I : 0 \le r_i \le 1 \right\}$$

$\therefore$ R/I is a commutative factor ring with unity $\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$ and R/I has 16 elements.

Now identify $\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + I$.

See $\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 0 \\ 4 & -4 \end{bmatrix} + I$

$= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + I$ as $\begin{bmatrix} 6 & 0 \\ 4 & -4 \end{bmatrix} \in I$.

Imp

Example:- Let $\mathbb{R}[x]$ be the ring of polynomials with real coefficients and let $\langle x^2+1 \rangle$ denote the principal ideal generated by x^2+1.

$$\langle x^2+1 \rangle = \{ f(x)(x^2+1) : f(x) \in \mathbb{R}[x] \}$$

Now $\mathbb{R}[x] / \langle x^2+1 \rangle = \{ g(x) + \langle x^2+1 \rangle : g(x) \in \mathbb{R}[x] \}$

Since $g(x)$ is any element of $\mathbb{R}[x]$, we can write

$g(x) = (x^2+1)\, q(x) + r(x)$ where $0 \le \deg r(x) \le 1$

$\therefore \mathbb{R}[x]/\langle x^2+1\rangle = \{ r(x) + q(x)(x^2+1) + \langle x^2+1\rangle : q(x), r(x) \in \mathbb{R}[x]$ and $0 \le \deg r(x) \le 1 \}$

$= \{ r(x) + \langle x^2+1\rangle : r(x) \in \mathbb{R}[x]$ and $0 \le \deg r(x) \le 1 \}$

$[\because q(x)(x^2+1) \in \langle x^2+1\rangle]$

$= \{ (ax+b) + \langle x^2+1\rangle : a, b \in \mathbb{R} \}$

Final form of elements of $\mathbb{R}[x]/\langle x^2+1\rangle$ is $(ax+b)+\langle x^2+1\rangle$.

In factor Ring $\mathbb{R}[x]/\langle x^2+1\rangle$, multiplication is done using the fact that $(x^2+1) + \langle x^2+1\rangle = 0 + \langle x^2+1\rangle$.

One should think x^2+1 as 0 or equivalently $x^2=-1$ in factor ring $\mathbb{R}[x]/\langle x^2+1\rangle$.

For e.g. $((x+3)+\langle x^2+1\rangle)((2x+5)+\langle x^2+1\rangle)$

$= (x+3)(2x+5) + \langle x^2+1\rangle = 2x^2+11x+15+\langle x^2+1\rangle$.

$= (11x+13) + \langle x^2+1\rangle \quad [\because x^2=-1]$

Example → Consider an ideal $\langle 2-i\rangle$ generated by an element $2-i$ in ring of Gaussian integers $\mathbb{Z}[i]$. We are to find the elements of $\mathbb{Z}[i]/\langle 2-i\rangle$.

Scanned with CamScanner

Elements of $\mathbb{Z}[i]/\langle 2-i\rangle$ will be of the form

$(a+ib)+\langle 2-i\rangle$, where $a+ib \in \mathbb{Z}[i]$

Note that $(2-i)+\langle 2-i\rangle = 0+\langle 2-i\rangle$.

So when we are dealing with coset representatives we may treat $2-i=0$ i.e. $2=i$. For example the coset $3+4i+\langle 2-i\rangle = 3+8+\langle 2-i\rangle = 11+\langle 2-i\rangle$.

$\therefore$ All elements of $\mathbb{Z}[i]/\langle 2-i\rangle$ can be expressed as

$a+\langle 2-i\rangle$ where a is an integer.

We can further reduce the distinct elements of $\mathbb{Z}[i]/\langle 2-i\rangle$ using $2=i \Rightarrow 4=-1 \Rightarrow 5=0$.

Therefore $(3+4i)+\langle 2-i\rangle = 3+8+\langle 2-i\rangle = 11+\langle 2-i\rangle$

$= 1+5+5+\langle 2-i\rangle$

$= 1+\langle 2-i\rangle$

$\therefore$ We can claim that the only distinct elements in $\mathbb{Z}[i]/\langle 2-i\rangle$ are $0+\langle 2-i\rangle$, $1+\langle 2-i\rangle$, $2+\langle 2-i\rangle$, $3+\langle 2-i\rangle$, $4+\langle 2-i\rangle$.

We show that $1+\langle 2-i\rangle$ has additive order 5.

Note that $5(1+\langle 2-i\rangle) = 5+\langle 2-i\rangle = 0+\langle 2-i\rangle$.

$\Rightarrow$ order of $1+\langle 2-i\rangle$ is either 1 or 5.

Let if possible additive order of $1+\langle 2-i\rangle$ is one.

$\Rightarrow 1+\langle 2-i\rangle = 0+\langle 2-i\rangle \Rightarrow 1 \in \langle 2-i\rangle$

$\Rightarrow 1 = (a+ib)(2-i) \Rightarrow 1 = (2a+b)+i(2b-a)$

$\Rightarrow 2a+b=1$ and $-a+2b=0 \Rightarrow b=\frac{1}{5}$

Which is not possible as $a, b \in \mathbb{Z}$.

$\therefore$ Additive order of $1+\langle 2-i\rangle$ is 5.

$$\therefore \mathbb{Z}[i]/\langle 2-i\rangle = \left\{ \begin{array}{c} 0+\langle 2-i\rangle,\ 1+\langle 2-i\rangle,\ 2+\langle 2-i\rangle, \\ 3+\langle 2-i\rangle,\ 4+\langle 2-i\rangle \end{array} \right\}$$

Prime Ideal :- A proper ideal A of a commutative ring R is said to be prime ideal of R if for any $a, b \in R$ whenever $ab \in A$ implies $a \in A$ or $b \in A$.

Example :- Trivial ideal $\{0\}$ in $\mathbb{Z}$ is prime ideal.

Sol^n :- Let $ab \in \{0\}$ where $a, b \in \mathbb{Z}$

$\Rightarrow ab = 0 \Rightarrow a=0$ or $b=0$ $[\because \mathbb{Z}$ is I.D.$]$

$\Rightarrow \{0\}$ is Prime ideal.

Example :- Let n be a positive integer. Then in the ring of integers $\mathbb{Z}$, prove that $n\mathbb{Z}$ is prime ideal iff n is prime.

Solution:→ Consider n is prime

To prove: $n\mathbb{Z} = \{0, \pm n, \pm 2n, ---\}$ is prime ideal.

For any $a, b \in \mathbb{Z}$, let $ab \in n\mathbb{Z}$

$\Rightarrow ab$ is multiple of $n \Rightarrow n | ab$

$\Rightarrow n|a$ or $n|b$ ($\because n$ is prime)

$\Rightarrow a$ is multiple of n or b is multiple of n

$\Rightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z} \Rightarrow n\mathbb{Z}$ is prime ideal.

Conversely:→ Consider $n\mathbb{Z}$ is prime ideal.

To show: n is prime.

Let if possible n is composite.

$\Rightarrow n = rs$ where $r, s \in \mathbb{N}$ and $1 < r, s < n$

Now $n \in n\mathbb{Z} \Rightarrow rs \in n\mathbb{Z}$ but neither $r \in n\mathbb{Z}$ nor $s \in n\mathbb{Z}$

$\Rightarrow n\mathbb{Z}$ is not prime ideal which is a contradiction.

$\therefore$ n is prime.

Maximal Ideal:→ A proper ideal A of R is said to be a maximal ideal of R if whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

i.e. the only ideal that properly contains a maximal ideal is the entire ring.

Scanned with CamScanner

<u>Example</u>:- $4\mathbb{Z}$ is not maximal ideal of $\mathbb{Z}$ because

$$4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$$

<u>Example</u>:- $2\mathbb{Z}$ is maximal ideal of $\mathbb{Z}$.

<u>Solution</u>:- Let B be an ideal that properly contains $2\mathbb{Z}$. That is $2\mathbb{Z} \subsetneq B$. Therefore $\exists$ an element $a \in B$ but $a \notin 2\mathbb{Z}$.

$\therefore$ a must be odd. $\Rightarrow$ $a+1$ is even $\Rightarrow (a+1) \in 2\mathbb{Z} \subseteq B$

$\Rightarrow a, a+1 \in B \Rightarrow (a+1) - a \in B \Rightarrow 1 \in B$.

Hence $B = \mathbb{Z}$.

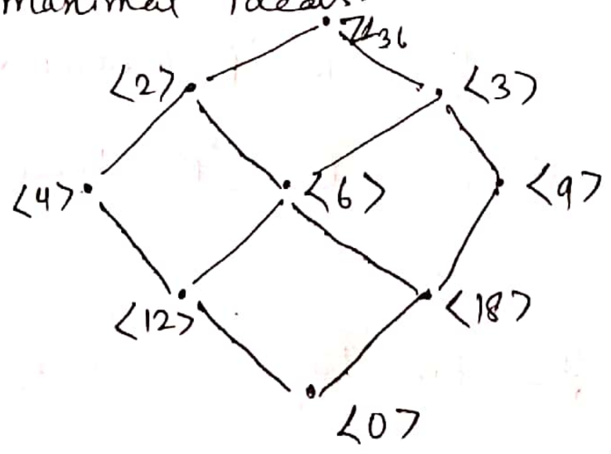
Therefore any ideal B that properly contains $2\mathbb{Z}$ is entire ring $\mathbb{Z}$ itself. Hence $2\mathbb{Z}$ is maximal.

<u>Example</u>:- $\{0\}$ is not maximal ideal in $\mathbb{Z}$ as

$$\{0\} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$$

But $\{0\}$ is prime ideal of $\mathbb{Z}$.

<u>Example</u>:- In ring $\mathbb{Z}_{36}$, Note that only $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals.



Here we see the lattice of ideals of $\mathbb{Z}_{36}$.
We see that only ideals $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals because the ideal that contains properly these ideals is entire ring $\mathbb{Z}_{36}$.

Note :- From the above example, we can generalize that the only Maximal ideals of $\mathbb{Z}_n$ are those which are generated by prime divisors of n.

V.Imp
Example :- Show that $\langle x^2+1 \rangle$ is maximal ideal in $\mathbb{R}[x]$.

Solution :- We have to show that $\langle x^2+1 \rangle$ is maximal.
Let B be an ideal which properly contains $\langle x^2+1 \rangle$.
i.e. $\langle x^2+1 \rangle \subseteq B$ but $\langle x^2+1 \rangle \neq B$.
$\therefore \exists \; f(x) \in B$ but $f(x) \notin \langle x^2+1 \rangle$.

Now $f(x) = q(x)(x^2+1) + r(x)$ where $q(x), r(x) \in \mathbb{R}[x]$ — (1)
and $0 \leq \deg r(x) \leq 1$ and $r(x) \neq 0$.

Here $r(x) \neq 0$ as if $r(x) = 0 \Rightarrow f(x) \in \langle x^2+1 \rangle$. which is not possible.

$\Rightarrow r(x)$ is of the form $ax+b$. where a and b not both zero
from (1)
$r(x) = ax+b = f(x) - q(x)(x^2+1) \in B$

$\Rightarrow ax+b \in B \Rightarrow (ax+b)(ax-b) \in B$

$\Rightarrow a^2x^2 - b^2 \in B$ ($\because B$ is an ideal and $ax-b \in \mathbb{R}[x]$)

Since $\langle x^2+1\rangle \subseteq B \Rightarrow x^2+1 \in B \Rightarrow a^2(x^2+1) \in B$

$\therefore\ a^2(x^2+1) - a^2x^2+b^2 = a^2+b^2 \in B$

$\Rightarrow a^2+b^2 \neq 0$ and $a^2+b^2 \in B$.

Note that every non zero constant polynomial in $\mathbb{R}[x]$ is unit, so a^2+b^2 is a unit and $a^2+b^2 \in B$

$$\Rightarrow \frac{1}{a^2+b^2}(a^2+b^2) \in B \Rightarrow 1 \in B \Rightarrow B = \mathbb{R}[x]$$

$\therefore\ \langle x^2+1\rangle$ is maximal ideal in $\mathbb{R}[x]$.

Imp

Example:– Prove that $\langle x\rangle$ is a prime ideal in $\mathbb{Z}[x]$ but not maximal ideal.

Sol^n:– Try yourself. For Hint: See Example 17 at Page 255.

M. Imp

Theorem:– 14.3 Let R be a commutative ring with unity and let A be an ideal of R, then show that R/A is an integral domain iff A is prime ideal.

Proof:– Assume that R/A is an I.D.

To show: A is prime ideal.

Let $ab \in A$ where $a, b \in R$.

$\Rightarrow ab + A = 0 + A$

$\Rightarrow (a+A)(b+A) = 0 + A$

Since R/A has no zero divisors

Therefore $\therefore$ $a+A = 0+A$ or $b+A = 0+A$

$\Rightarrow a \in A$ or $b \in A$

Thus $ab \in A \Rightarrow a \in A$ or $b \in A$, hence A is prime ideal.

Conversely :- Assume that A is a prime ideal.

To show: R/A is an I.D.

Since R is a commutative ring with unity, R/A is commutative ring with unity.

Claim: R/A has no zero divisors.

Consider $(a+A)(b+A) = 0+A$

$\Rightarrow ab + A = 0 + A \Rightarrow ab \in A$

$\Rightarrow a \in A$ or $b \in A$ ($\because$ A is prime ideal)

$\Rightarrow a+A = 0+A$ or $b+A = 0+A$.

$\Rightarrow R/A$ has no zero divisors

$\Rightarrow R/A$ is an Integral domain.

(M. Imp)

Theorem :- 14.4 Let R be a commutative ring with unity and let A be an ideal of R, then show that R/A is a field iff A is maximal ideal.

Proof : Assume that R/A is a field. Here $1+A$ is multiplicative identity (unity) of R/A.

Let B be an ideal properly containing A.

Claim:- $B = R$

Since B properly contains A, $\exists\ x \in B$ but $x \notin A$.

Now $x + A \neq 0 + A$ and R/A is a field, so $x + A$ is a unit in R/A.

$\exists\ y + A \in R/A$ such that $(x+A)(y+A) = 1 + A$

$$\Rightarrow xy + A = 1 + A \Rightarrow xy - 1 \in A \subseteq B.$$

$\therefore xy - 1 \in B$, also $xy \in B$ ($\because x \in B$ and B is an ideal)

$$\therefore (xy) - (xy - 1) \in B \Rightarrow 1 \in B.$$

$$\Rightarrow B = R.$$

$\therefore A$ is maximal ideal of R.

Conversely:- Consider A is maximal ideal of R.

To prove:- R/A is a field.

Since R is commutative ring with unity, R/A is a commutative ring with unity.

Only thing to prove is that every non zero element of R/A is a unit.

Let $x + A \neq 0 + A$ i.e. $x \notin A$

Consider $B = \{xr + a : r \in R, a \in A\}$

We show that B is an ideal of R and properly contains A.

Let $p = xr_1 + a_1$ and $q = xr_2 + a_2$ be two elements of B, then $p - q = x(r_1 - r_2) + (a_1 - a_2)$ also belongs to B as $r_1 - r_2 \in R$ and $a_1 - a_2 \in A$.

Now let $p = xr_1 + a_1 \in B$ and $r \in R$.

$rp = r(xr_1 + a_1) = rxr_1 + ra_1 = x(rr_1) + ra_1$

$\Rightarrow rp \in B$ ($\because$ A is an ideal and R is commutative ring)

$\therefore$ B is an ideal of R and properly contains A.

($\because$ $x \in B$ but $x \notin A$)

Since A is maximal ideal, $B = R$.

$\Rightarrow 1 \in B \Rightarrow 1 = xr + a$ for some $r \in R, a \in A$.

Now $1 + A = xr + a + A = xr + A$

$= (x + A)(r + A)$ ($\because$ $a \in A$)

$\therefore$ $(x + A)(r + A) = 1 + A$.

$\Rightarrow$ $r + A$ is multiplicative inverse of $x + A$.

$\therefore$ Every non zero element of R/A is a unit.

Hence R/A is a field.

Result: Prove that every maximal ideal is prime ideal in a commutative ring with unity but converse is not true.

Proof: Let M be a maximal ideal of a commutative ring with unity R.

By Theorem 14.4, R/M is a field.

We know that every field is an Integral domain.

$\Rightarrow$ R/M is an I.D and using Theorem 14.3

M is prime ideal.

Converse is not true: $\{0\}$ is prime ideal in $\mathbb{Z}$

but $\{0\}$ is not maximal ideal of $\mathbb{Z}$ (Already proved)

There is one more counterexample i.e Example 17 at Page 255.

Exercises

Exercise 8 If A and B are ideals of a ring R, show that the sum of A and B, $A+B=\{a+b : a\in A, b\in B\}$, is an ideal.

Proof: It is very simple, just use definition of ideal.

Since $0 \in A$, $0 \in B \Rightarrow 0+0=0 \in A+B$
$\Rightarrow A+B \neq \phi$.

(i) Let $x = a_1 + b_1$ and $y = a_2 + b_2$ be two elements of $A+B$, where $a_1, a_2 \in A$, $b_1, b_2 \in B$.

$$x - y = (a_1+b_1) - (a_2+b_2) = (a_1-a_2) + (b_1-b_2) \in A+B$$

[$\because a_1, a_2 \in A$ and A is an ideal. $\Rightarrow a_1 - a_2 \in A$. Similarly for B]

$\therefore x - y \in A+B$.

(ii) Let $x = a+b \in A+B$ where $a \in A$, $b \in B$, and let $r \in R$.

Now $rx = r(a+b) = ra + rb \in A+B$.

and $xr = (a+b)r = ar + br$

[$\because a \in A$ and $r \in R$, and A is an ideal $\Rightarrow ra$ and $ar \in A$. Similarly for B]

$\therefore rx, xr \in A+B$

Hence $A+B$ is an ideal.

Exercise:- 7 Prove that intersection of any set of ideals of a ring is an ideal.

(Imp)

Exercise:-9 In the ring of integers $\mathbb{Z}$, find a positive integer a such that $\langle a \rangle = \langle m \rangle + \langle n \rangle$.

Solution :- Claim: $a = \gcd\{m, n\}$.

For $a = \gcd\{m,n\}$, we prove that $\langle m \rangle + \langle m \rangle = \langle a \rangle$.

Since $a = \gcd\{m,n\}$, $\exists$ $p, q \in \mathbb{Z}$ such that

$$a = mp + nq \in \langle m \rangle + \langle n \rangle.$$

$$\Rightarrow a \in \langle m \rangle + \langle n \rangle \Rightarrow \langle a \rangle \subseteq \langle m \rangle + \langle n \rangle \quad \text{— (1)}$$

Since $a = \gcd\{m,n\} \Rightarrow a \mid m$ and $a \mid n \Rightarrow m = ak, n = al$ for some $k, l \in \mathbb{Z}$.

Let $x \in \langle m \rangle + \langle n \rangle \Rightarrow x = mr + ns$

$$\Rightarrow x = akr + als = a(kr + ls)$$

$$\Rightarrow x \in \langle a \rangle.$$

$$\therefore \langle m \rangle + \langle n \rangle \subseteq \langle a \rangle \quad \text{— (2)}$$

From (1), (2) $\langle a \rangle = \langle m \rangle + \langle n \rangle$ where $a = \gcd\{m,n\}$.

In particular $\langle 3 \rangle + \langle 6 \rangle = \langle 3 \rangle$ as $\gcd\{3,6\} = 3$.

$\langle 2 \rangle + \langle 3 \rangle = \langle 1 \rangle$. as $\gcd\{2,3\} = 1$

Exercise: 10 If A and B are ideals of a ring, show that product of A and B,

$AB = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n : a_i \in A, b_i \in B, n \in \mathbb{N}\}$ is an ideal.

Proof: Since $0 \in A$ and $0 \in B \Rightarrow 0 \cdot 0 = 0 \in AB$

$\Rightarrow AB$ is non empty.

(i) $x, y \in AB \Rightarrow x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$ and

$y = c_1 d_1 + c_2 d_2 + \cdots + c_n d_m$ for some $a_i, c_i \in A$, $b_i, d_i \in B$.

$$x - y = (a_1 b_1 + a_2 b_2 + - + a_n b_n) - (c_1 d_1 + c_2 d_2 + - + c_m d_m)$$

$$= a_1 b_1 + a_2 b_2 + - + a_n b_n + (-c_1) d_1 + (-c_2) d_2 + - + (-c_m) d_m$$

$$\Rightarrow x - y \in AB \quad [\because -c_i \in A \text{ as } c_i \in A]$$

(ii) Let $x = a_1 b_1 + a_2 b_2 + - + a_n b_n \in AB$ where $a_i \in A$, $b_i \in B$, $n \in \mathbb{N}$ and $r \in R$.

$$rx = r(a_1 b_1 + a_2 b_2 + - + a_n b_n) = (ra_1) b_1 + (ra_2) b_2 + - + (ra_n) b_n$$

$$\Rightarrow rx \in AB \quad [\because a_i \in A \Rightarrow r a_i \in A \text{ as } A \text{ is an ideal}]$$

Also $xr = (a_1 b_1 + a_2 b_2 + - + a_n b_n) r = a_1 (b_1 r) + a_2 (b_2 r) + - + a_n (b_n r)$.

$$\therefore xr \in AB \quad [\because b_i \in B \text{ and } r \in R \Rightarrow b_i r \in B \text{ as } B \text{ is an ideal}]$$

$$\therefore xr, rx \in AB \quad \forall x \in AB, r \in R$$

$\therefore$ AB is an ideal of R.

<u>Exercise</u> :- 11.(a) Find a positive integer a such that $\langle a \rangle = \langle 3 \rangle \langle 4 \rangle$.

<u>Solution</u> :- <u>Claim</u> :- $a = 3 \cdot 4 = 12$.

Let $x \in \langle 3\rangle\langle 4\rangle$.

$x = (3s_1)(4t_1) + (3s_2)(4t_2) + \text{---} + (3s_n)(4t_n)$ where $s_i, t_i \in \mathbb{Z}$

$= 12s_1t_1 + 12s_2t_2 + \text{---} + 12s_nt_n$

$= 12(s_1t_1 + s_2t_2 + \text{---} + s_nt_n) \in \langle 12\rangle$.

$\therefore x \in \langle 12\rangle \Rightarrow \langle 3\rangle\langle 4\rangle \subseteq \langle 12\rangle$ — (1)

Let $x \in \langle 12\rangle \Rightarrow x = 12t$ where $t \in \mathbb{Z}$

$\Rightarrow x = (3\cdot 1)(4t) \in \langle 3\rangle\langle 4\rangle$.

$\therefore \langle 12\rangle \subseteq \langle 3\rangle\langle 4\rangle$ — (2)

From (1), (2) $\langle 12\rangle = \langle 3\rangle\langle 4\rangle$.

11 (b) $a = 48$ (c) $a = mn$.

Exercise :- 12 Let A and B be ideals of a ring R, then show that $AB \subseteq A \cap B$.

Proof :- Let $x \in AB$

$\Rightarrow x = a_1b_1 + a_2b_2 + \text{---} + a_nb_n$ where $a_i \in A$, $b_i \in B$ and $n \in \mathbb{N}$.

Since $a_i \in A$ and A is an ideal $\Rightarrow a_ib_i \in A$, $i = 1$ to n.

$\Rightarrow a_1b_1 + a_2b_2 + \text{---} + a_nb_n \in A$ as A is an ideal.

$\Rightarrow x \in A$ — (1)

Since $b_i \in B$ and B is an ideal $\Rightarrow a_ib_i \in B$, $i = 1$ to n

$\Rightarrow a_1b_1 + a_2b_2 + \text{---} + a_nb_n = x \in B$ — (2)

From (1) and (2) $x \in A \cap B \Rightarrow AB \subseteq A \cap B$.

(qub)
Exercise:- 13 If A and B are ideals of a commutative ring R with unity and $A+B=R$, then show that $A \cap B = AB$.

Proof:- Firstly we have to prove Exercise 12.

$\therefore AB \subseteq A \cap B$ — (1) (Done in Exercise 12).

Claim:- $A \cap B \subseteq AB$.

Let $x \in A \cap B \Rightarrow x \in A$ and $x \in B$.

Now given that $A+B=R \Rightarrow 1 \in A+B$

$\Rightarrow 1 = a+b$ where $a \in A$, $b \in B$.

$\Rightarrow x \cdot 1 = xa + xb$

$\Rightarrow x = xa + xb = ax + xb$ ($\because R$ is commutative)

$\therefore x = ax + xb \in AB$

ax: belongs to A, belongs to B; x: Belongs to A; b: Belongs to B

$\therefore A \cap B \subseteq AB$ — (2)

From (1), (2)

$\boxed{A \cap B = AB}$

Exercise → 25. Let R be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Show that $A = \{f \in R : f(0) = 0\}$ is maximal ideal of R.

Solution ⇒ $A = \left\{ f \in R : f : \mathbb{R} \to \mathbb{R} \text{ is a map with } f(0) = 0 \right\}$

A is non empty as zero function belongs to A.

(i) $f, g \in A \Rightarrow f(0) = 0,\ g(0) = 0 \Rightarrow (f-g)(0)$
$= f(0) - g(0) = 0$

$\Rightarrow f - g \in A$

(ii) Let $f \in A$ and $r \in R$. Since $f \in A \Rightarrow f(0) = 0$

$(rf)(0) = r(0) f(0) = r(0) \cdot 0 = 0 \Rightarrow rf \in A$

Similarly $fr \in A$

$\therefore rf, fr \in A \ \forall\, r \in R, f \in A$

Therefore A is an ideal of R.

Claim → A is maximal ideal.

Let B be an ideal of R which properly contains A.

$\therefore \exists\ g \in B$ but $g \notin A$.

$\Rightarrow g(0) \neq 0$

Note that $g(x) - g(0)$ is a map which gives 0 at $x=0 \Rightarrow g(x) - g(0) \in A \subseteq B$.

$\Rightarrow g(x) - g(0), \; g(x) \in B \Rightarrow (g(x)) - (g(x) - g(0)) \in B$

$\Rightarrow g(0) \in B$, Here $g(0)$ is a constant non zero function from $\mathbb{R} \to \mathbb{R}$. So $g(0)$ is a unit and $g(0) \in B$.

$\Rightarrow g(0) \cdot \frac{1}{g(0)} \in B \Rightarrow 1 \in B \Rightarrow B = R$.

$\therefore A$ is a maximal ideal of R.

Imp

Exercise:- 34. An integral domain D is called a Principal Integral domain if every ideal of D is of the form $\langle a \rangle = \{ad : d \in D\}$. Show that $\mathbb{Z}$ is a Principal integral domain.

Proof:- We are to prove that every ideal of $\mathbb{Z}$ is Principal ideal. (Recall definition of Principal ideal).

i.e We are to show that every ideal of $\mathbb{Z}$ is of the form $\langle a \rangle$. ($\because \mathbb{Z}$ is already an Integral domain).

Let I be an ideal in $\mathbb{Z}$.

If $I = \{0\} \Rightarrow I = \langle 0 \rangle$.

So let $I \neq \{0\}$, then I must have both +ve and -ve integers.

Let a be the least +ve integer such that $a \in I$

Claim: $I = \langle a \rangle$.

Let $x \in I$, by division algorithm $\exists$ q and r such that $x = aq + r$, $0 \le r \le a-1$ — (1)

Since $x, a \in I \Rightarrow x, aq \in I$ ($\because$ I is an ideal)

$\Rightarrow r = x - aq \in I$

$\Rightarrow r \in I$, $0 \le r \le a-1$

$r = 0$ as a is least +ve integer such that $a \in I$.

From (1)

$x = aq \Rightarrow$ Every element x of I is of the form $aq \Rightarrow I = \langle a \rangle = \{aq : q \in \mathbb{Z}\}$.

Hence Every ideal of $\mathbb{Z}$ is Principal ideal.

$\Rightarrow \mathbb{Z}$ is a Principal Integral domain.

Exercise :- 33. In $\mathbb{Z}_5[x]$, let $I = \langle x^2+x+2 \rangle$. Find multiplicative Inverse of $(2x+3)+I$ in factor ring $\mathbb{Z}_5[x]/I$.

Sol^n:- Here $\mathbb{Z}_5[x]$ is commutative ring with unity.

$\Rightarrow \mathbb{Z}_5[x]/I$ is commutative ring with unity.

We are to find multiplicative inverse of $(2x+3)+I$ (if exists).

Note that $\mathbb{Z}_5[x] / \langle x^2+x+1 \rangle$ has elements of the form $(ax+b)+\langle x^2+x+1\rangle$ and $(x^2+x+1)+\langle x^2+x+1\rangle$
$= 0 + \langle x^2+x+1\rangle$

i.e. $x^2+x+1 = 0$ in $\mathbb{Z}_5[x]/\langle x^2+x+1\rangle$.

We use this fact $x^2+x+1=0$ in multiplication calculation.

Now let $(ax+b)+I$ be inverse (multiplicative) of $(2x+3)+I$. (Make sure all calculation will be for modulo 5 i.e. in $\mathbb{Z}_5$)

$$\therefore ((ax+b)+I)((2x+3)+I) = 1+I$$

$$\Rightarrow (ax+b)(2x+3)+I = 1+I$$

$$\Rightarrow (2ax^2+(3a+2b)x+3b)+I = 1+I$$

$$\Rightarrow 2a(-x-1)+(3a+2b)x+3b+I = 1+I$$

(use $x^2=-x-1$)

$$\Rightarrow (a+2b)x+(3b-4a)+I = 1+I$$

$$\Rightarrow a+2b=0$$
$$-4a+3b=1$$

by solving a, b
$a=3, b=1$

$\therefore$ $(3x+1)+I$ is multiplicative inverse of $(2x+3)+I$.

$\therefore$ $(3x+1)+I$ is a unit in $\mathbb{Z}_5[x]/I$.

Exercises 1, 2, 3, 4, 5, 16, 20, 22, 23, 27, 32, 43, 45.

These above exercises are similar to those, I have done already in this chapter-14th.

Try yourself these exercises.