Ex. 1.1

① Let A be an ideal of R. prove that the set of all those polynomials in $R[x]$ whose constant term are arbitrary but other coefficient belong to A is a subring of $R[x]$.

② Let R be a commutative ring with unity and S be a subring of R that contains the unity of R. Let $f(x) \in R[x]$. If there exist a polynomial $g(x) \in S[x]$ whose leading coeff. is a unit in S such that ~~f g~~ $f(x)g(x) \in S[x]$ then prove that $f(x) \in S[x]$

Ex. soln.

R commutative ring with unity.

S - subring of R containing the unity of R.

$f(x) \in R[x]$. If $\exists\, g(x) \in S[x]$ whose leading coefficient is a unit in S s.t.

$f(x)g(x) \in S[x]$ then prove that $f(x) \in S[x]$.

Soln. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$

where $a_i \in R$ $\forall i = 0, 1, \ldots m$.

$a_m \neq 0$

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$

where $b_j \in S$, $\forall j = 0, 1, \ldots n$

$b_n \neq 0$.

by the given condition (i) b_n is a unit in S.

(ii) $f(x)g(x) \in S[x]$

To prove $f(x) \in S[x]$

i.e. to show $a_i \in S$ $\forall i = 0, 1, \ldots m$

$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + \cancel{c_{m+n}x^{m+n}} + c_lx^l$

where $l \le m+n$

Since $c_k = \sum_{i+j=k} a_i b_j$, $c_k \in S$ $\forall k = 0 \ldots t$

Hence $c_{m+n} = a_m b_n \neq 0$ — for b_n is a unit in S.

[if $a_m b_n = 0 \Rightarrow a_m = 0$ $\Rightarrow (a_m b_n) b_n^{-1} = 0$ which is not true]

$\Rightarrow$ ~~$t = m + n$~~

Now $c_{m+n} \in S$

$\Rightarrow a_m b_n \in S \Rightarrow a_m b_n = s_1$ for some $s_1 \in S$

$\Rightarrow a_m = s_1 b_n^{-1} \in S$

Next we consider c_{m+n-1}

~~$c_{m+n-1} = a_m b_{n-1} + a_{m-1} b_n$~~

$c_{m+n-1} = a_{m-1} b_n + a_m b_{n-1}$

Since $c_{m+n-1} \in S \Rightarrow a_{m-1} b_n + a_m b_{n-1} = s_2$ for some $s_2 \in S$

$\Rightarrow a_{m-1} b_n = s_2 - a_m b_{n-1} \in S$

$\Rightarrow a_{m-1} b_n = s_3$ for some $s_3 \in S$

$\Rightarrow a_{m-1} = s_3 b_n^{-1} \in S$

$\Rightarrow a_{m-1} \in S$

Similarly considering c_{m+n-2} we get $a_{m-2} \in S$

c_{m+n-3}, we get a_{m-3} … c_1, c_0 we get $a_1, a_0 \in S$.

$\therefore$ hence $a_i \in S$ $\forall i = 0, 1, \ldots m$.

Thus $f(x) \in S[x]$

Unit 5

Prerequisites:-

Defination:- Let R be a commutative ring with unity. Let $a, b \in R$. Then a and b are called associates if $a = bu$ where u is a unit in R.

eg. In Z' 3, -3 are associates.

$n, -n$ " " , $n \in Z'$

Defination:- prime element.

Let R be a commutative ring with unity. An element $p \in R$ is called a prime element if the following conditions are satisfied -

(i) $p \neq 0$ and p is not a unit in R,

(ii) If $p \mid ab$ Then either $p \mid a$ or $p \mid b$ for $a, b \in R$.

eg. In Z', The prime numbers are prime elements of Z'.

$3 \neq 0$, 3 is not a unit

$3 \mid ab \Rightarrow 3 \mid a$ or $3 \mid b$.

Defination:- Irreducible element:- Let R be a commutative ring with unity. An element $p \in R$ is called an irreducible element if it satisfies the following conditions -

(i) $p \neq 0$ and p is not a unit in R.

(ii) if $p = ab$ Then one of a and b must be unit, $a, b \in R$.

eg. In Z', the prime numbers are irreducible element in Z

$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

is called ring of Gaussian integers.

$\mathbb{Z}[i]$ is a commutative ring with unity

Also $\mathbb{Z}[i]$ has no proper zero divisors.

$\therefore$ $\mathbb{Z}[i]$ is an integral domain unity.

Ex. Find all the units of $\mathbb{Z}[i]$.

Soln Let $a+bi \in \mathbb{Z}[i]$ be a unit, then $\exists$ $c+di \in \mathbb{Z}[i]$ such that

$(a+bi)(c+di) = 1 \rightarrow$ (i)

So $(a-bi)(c-di) = 1 \rightarrow$ (ii)

~~(i) x ii~~ From (i) & (ii)

$(a^2+b^2)(c^2+d^2) = 1$

$\Rightarrow a^2+b^2 = 1, \; c^2+d^2 = 1$ $\quad \boxed{a, b \in \mathbb{Z}}$

$a^2+b^2 = 1 \Rightarrow a^2 = 1, b^2 = 0$
or $a^2 = 0, b^2 = 1$

i.e. $a = \pm 1, b = 0$, or $a = 0, b = \pm 1$

$\Rightarrow$ the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$

i.e. $1, -1, i, -i$

Ex. Find all the units of $\mathbb{Z}[\sqrt{-5}]$

$\mathbb{Z}[\sqrt{-5}]$ is an integral domain with unity

$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

Ans ± 1 are the only units.

Ex. Show that $1+i$ is an irreducible element in $\mathbb{Z}[i]$.

Solⁿ:- $1+i$ is not a unit in $\mathbb{Z}[i]$ and $1+i \neq 0$.

Let ~~$1+i = (a+ib)(c+id)$~~

$1+i = (a+bi)(c+di)$, $a,b,c,d \in \mathbb{Z}$.

$= xy$ when $x = a+bi$, $y = c+di$

$1+i = (a+bi)(c+di) \rightarrow$ (i)

So $1-i = (a-bi)(c-di) \rightarrow$ (ii).

From (i) & (ii) we get,

$1^2 - i^2 = 2 = (a^2+b^2)(c^2+d^2)$

$\Rightarrow a^2+b^2 = 1$ or $c^2+d^2 = 2$ or $a^2+b^2 = 2$, $c^2+d^2 = 1$

if $a^2+b^2 = 1 \Rightarrow (a+bi)(a-bi) = 1$

$\Rightarrow a+bi$ is a unit.

if $c^2+d^2 = 1 \Rightarrow (c+di)(c-di) = 1$.

$\Rightarrow c+di$ is unit.

$\Rightarrow$ either $a+bi$ is a unit or $c+di$ is a unit.

$\Rightarrow$ either x is a unit or y is a unit.

Hence $1+i$ is an irreducible element.

Ex. Show that 2 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$ but 2 is not a prime element in $\mathbb{Z}[\sqrt{-5}]$.

Scanned with CamScanner

Soln: Unit of $Z[\sqrt{-5}]$ is ± 1.

~~$\therefore$ 3 is not a unit~~

$\therefore$ 3 is a non zero elt. which is not a unit in $Z[\sqrt{-5}]$

Let $3 = xy$, $x, y \in Z[\sqrt{-5}]$

where $x = a + b\sqrt{-5}$

$y = c + d\sqrt{-5}$

$\therefore 3 = (a+b\sqrt{-5})\cdot(c+d\sqrt{-5}) \to (i)$

$= \cancel{(a+b\sqrt{5}i)(c+d\sqrt{5}i)} \to (i)$

So $3 = (a - b\sqrt{-5})(c - d\sqrt{-5}) \to (ii)$

From (i) & (ii)

$9 = (a^2+5b^2)(c^2+5d^2)$

$\therefore a^2+5b^2 = 9$, $c^2+5d^2=1$ or $a^2+5b^2=1$, $c^2+5d^2=9$

or $a^2+5b^2 = 3$, $c^2+5d^2=1$ ~~$a^2+5b^2=3$, $c^2+5d^2=3$~~ or ~~$a^2+5b^2=\ldots$~~ ~~$c^2+5d^2=3$~~

but no integer satisfies the condition.

If $c^2+5d^2=1 \Rightarrow (c+d\sqrt{-5})(c-d\sqrt{-5})=1$

$\therefore c+d\sqrt{-5}$ is a unit.

if $a^2+5b^2=1 \Rightarrow (a+b\sqrt{-5})(a-b\sqrt{-5})=1$

$\therefore a+b\sqrt{-5}$ is a unit.

if leave either $a+b\sqrt{-5}$ is a unit or $c+d\sqrt{-5}$ is a unit.

$\therefore$ 3 is an irreducible elt.

2nd part:- To show 3 is not a prime element

We know $(2+\sqrt{-5})(2-\sqrt{-5}) = 9$

Now $3 \mid 9 \Rightarrow 3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$

But $3 \nmid 2+\sqrt{-5}$ or $3 \nmid 2-\sqrt{-5}$

For if $3 \mid 2+\sqrt{-5}$

Then $(2+\sqrt{-5}) = 3(x+s\sqrt{-5})$, $x, s \in \mathbb{Z}$

$\Rightarrow 3x = 2$, $3s = 1$

$\exists$ no integer which satisfies this, a

is a contradiction.

$\therefore 3 \nmid 2+\sqrt{-5}$, lly $3 \nmid 2-\sqrt{-5}$

$\therefore$ 3 is not a prime.

Show that in Z_6', $\bar{2}$ is a prime element but not irreducible.

$Z_6' = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, is a ring under addition and multiplication modulo 6.

(Z_6' is not an integral domain).

Only unit are $\bar{1}$ and $\bar{5}$ (and $\bar{1}$ is the unity)

Here $\bar{2} \cdot \bar{4} = \bar{2}$

but $\bar{2}$ and $\bar{4}$ not units.

$\Rightarrow \bar{2}$ is not an irreducible elt.

It can be easily verified $\bar{2}$ is a prime elt.

(Try)

Scanned with CamScanner

Let $\bar{2} \mid ab$. To show $\bar{2}$ is a prime we have to show that either $\bar{2} \mid a$ or $\bar{2} \mid b$.
Suppose if possible neither $\bar{2} \mid a$ nor $\bar{2} \nmid b$. Then $a = \bar{2}m + 1$, $b = \bar{2}n + 1$
so $ab = (\bar{2}m + 1)(\bar{2}n + 1) = \bar{4}mn + \bar{2}(m+n) + 1$. But $\bar{2} \mid ab$
$\bar{2} \mid \bar{4}mn$, $2 \mid \bar{2}(m+n)$ so $\bar{2} \mid 1$. Which is a contradiction. This
contradiction implies that ~~$\bar{2} \mid a$~~ either $\bar{2} \mid a$ or $\bar{2} \mid b$. So $\bar{2}$ is prime.

5.1.1. In an integral domain with unity every prime element is irreducible.

Pf. Let R be an integral domain with unity and P be a prime element in R.

Show p is an irreducible element.

Since P is a prime element, $P \neq 0$ and P is not ~~a~~ a unit in R.

For $a, b \in R$ let $P = ab$

$P \mid P \Rightarrow P \mid ab$

$\Rightarrow P \mid a$ or $P \mid b$ [$\because p$ is prime]

Let $P \mid a$

Then $\exists\, x \in R$ s.t. $a = px$

Now $P = ab \Rightarrow$ ~~pxb~~ $p = pxb$

$\Rightarrow 1 = xb$ [By Cancellation law]

$\Rightarrow xb = 1$

$\Rightarrow b$ is a unit.

Similarly, if $P \mid b$ then it can be shown that a is a unit.

Thus $P = ab \Rightarrow$ One of a and b is a unit.

$\Rightarrow P$ is an irreducible element.

Note:- In a ring, a prime element may not be an irreducible element.

eg. Z_6 is a ring. In Z_6, $\bar{2}$ is a prime element which is not irreducible.

(Z_6 is not an integral domain)