E-Learning Materials for Sem - 6(I)

Unit - 1, CC - 14

Topic - Ring theory and Linear Algebra - II

Date - 04. 04. 2020.

Prepared by - Dr. Alauddin Dafadar.

It follows that an associate of an irreducible element in D is also an irreducible in D. 7

Ex: In the integral domain $\mathbb{Z}$, 5 and -5 are irreducible elements, but 6 is not.

Because $5 = 5 \cdot 1$ $-5 = 5 \cdot (-1)$

In here ① 5 and -5 is not unit.

② and only divisors of 5 and -5 are 1 and -1

and 5 and -5 are an associate of 5 and -5.

Ex: A field F is an integral domain where every non-zero element is a unit.

$\therefore$ There is a no irreducible element in a field.

Ex: $5 = [= (2+i)(2-i)]$ is not an irreducible element in the domain $\mathbb{Z}[i]$ but it is irreducible element in a field. in the subdomain $\mathbb{Z}$.

Ex.6: Show that 3 is an irreducible element in the integral domain $\mathbb{Z}[i]$.

$\Rightarrow$ Let $3 = (a+bi)(c+di)$. Then $N(3) = N(a+bi)N(c+di)$ gives $(a^2+b^2)(c^2+d^2) = 9$ for integers a, b, c, d.

This is possible if either i) $a^2+b^2 = 1$ and $c^2+d^2 = 9$ ii) $a^2+b^2 = 3$, $c^2+d^2 = 3$, iii) $a^2+b^2 = 9$ and $c^2+d^2 = 1$

In i) $a^2+b^2 = 1 \Rightarrow (a+bi)(a-bi) = 1 \Rightarrow a+bi$ is a unit

In iii) $c^2+d^2 = 1 \Rightarrow (c+di)(c-di) = 1 \Rightarrow c+di$ is a unit

The possibility ii) can not happen.

$\therefore$ If $3 = (a+bi)(c+di)$ then either $a+bi$ is a unit or $c+di$ is a unit. This proves that 3 is an irreducible in the domain $\mathbb{Z}[i]$.

Ex. 7 Show that 2 is an irreducible element in the domain $D = \mathbb{Z}[\sqrt{-5}]$

⇒ Let us define a norm function N on D by $N(a + b\sqrt{-5}) = a^2 + 5b^2$

Let $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then

$N(2) = N(a + b\sqrt{-5})\, N(c + d\sqrt{-5})$

$\Rightarrow 4 = (a^2 + 5b^2)(c^2 + 5d^2)$, for integers a, b, c, d

This is possible if either i) $a^2 + 5b^2 = 1$ and $c^2 + 5d^2 = 4$ ii) $a^2 + 5b^2 = 2$, and $c^2 + 5d^2 = 2$ iii) $a^2 + 5d^2 = 4$, $c^2 + 5d^2 = 1$

In i) $a^2 + 5b^2 = 1 \Rightarrow$ ~~that~~ $a = \pm 1, b = 0$ so $a + b\sqrt{-5}$ is a unit

In iii) $c^2 + 5d^2 = 1 \Rightarrow c = \pm 1, d = 0$ so $c + d\sqrt{-5}$ is a unit.

The possibility ii) cannot happen

∴ If $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then either $a + b\sqrt{-5}$ is a unit or $c + d\sqrt{-5}$ is a unit.

This prove that 2 is a irreducible in D.

Prime element :⇒

A non-zero element p in an integral domain D is said to be a prime element in D if

i) p is not a unit and

ii) $p \mid ab$ implies either $p \mid a$ or $p \mid b$, for a, b in D.

Theorem 01: In an integral domain, every prime elements is an irreducible. 9

$\Rightarrow$ Let P be a prime element in an integral domain D. Then $P \neq 0$ and P is not a unit in D.

Let $a \in D$ and a is a divisor of P. Then $P = ab$ for some b in D.

$P = ab \Rightarrow P \mid ab$ and since P is prime, either $P \mid a$ or $P \mid b$

i) $P \mid a$, then we have $a \mid P$ and $P \mid a$ and this shows that a is an associate of P.

ii) If $P \mid b$, then $b = pd$ for some d in D.

$\therefore$ $P = ab = apd$ and this gives $P - apd = 0$

$\Rightarrow P(1 - ad) = 0$,

and D contains no divisor of zero

Since $P \neq 0$, Then $ad = 1$

This shows that a is a unit in D.

Thus a is a divisor of P implies either a is an associate of P or a is a unit in D.

$\therefore$ P is an irreducible in D.

Ex. 8 In an integral domain, an irreducible element may not be a prime.

$\Rightarrow$ Example, in the integral domain $D = \mathbb{Z}[\sqrt{-5}]$,

$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$,

2 is an irreducible in D and $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$.

But 2 is neither a divisor of $1 + \sqrt{-5}$ nor a divisor of $1 - \sqrt{-5}$. So 2 is not a prime in D.

Ex. 9 Show that 3 is an irreducible element but is not a prime element in the integral domain $Z[\sqrt{-5}]$ 10

⇒ Let $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then $N(3) = N(a+b\sqrt{-5})\,N(c+d\sqrt{-5})$ giving $(a^2+5b^2)(c^2+5d^2) = 9$ for integers a, b, c, d

This is possible if either

i) $a^2+5b^2 = 1$ and $c^2+5d^2 = 9$

ii) $a^2+5b^2 = 3$ and $c^2+5d^2 = 3$

iii) $a^2+5b^2 = 9$ and $c^2+5d^2 = 1$.

In i) $a^2+5b^2 = 1 \Rightarrow a = \pm 1,\ b = 0$ so $a+b\sqrt{-5}$ is a unit

In iii) $c^2+5d^2 = 1 \Rightarrow c = \pm 1,\ d = 0$ so $c+5d\sqrt{-5}$ is a unit

The possibility (ii) cannot happen.

Therefore if $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ Then

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

This prove that 3 is an irreducible element in the integral domain $Z[\sqrt{-5}]$

We have $3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$ in the integral domain $Z[\sqrt{-5}]$

$\therefore$ 3 is a divisor of $(1+2\sqrt{-5})(1-2\sqrt{-5})$ but 3 is neither a divisor of $(1+2\sqrt{-5})$ nor a divisor of $(1-2\sqrt{-5})$.

Hence 3 is not a prime element in the integral domain $Z[\sqrt{-5}]$.

Unique factorization domain (UFD) :⇒

i) Every non-zero and non-unit element in D can be expressed as the product of a finit numbers of irreducible elements, and

ii) The decomposition is unique upto the order and associates of the irreducibles. [That is ~~iff~~ if $P_1 P_2 P_3 \cdots P_r$ and $q_1 q_2 \cdots q_s$ be the two factorizations of the same element in D, then $r = s$ and P_i, q_j are associates for some i, j]

Ex.10 Prove that the integral domain $\mathbb{Z}$ is UFD.

⇒ Every non-zero element other than 1 and -1 in $\mathbb{Z}$ can be expressed as the product of a finit number of irreducible elements in $\mathbb{Z}$ and the factorization is unique except for the order of the factors.

$36 = 3 \cdot 3 \cdot 2 \cdot 2 = (-2) \cdot 2 (-3)(-3) = (-2)(-3) \cdot 2 \cdot 3.$

Here 2. and -2 associates, 3 and -3 associates.

~~Ex-11~~ **Theorem 02:** P- 261

In a UFD (unique factorization domain), every irreducible element is a prime.

⇒ Let P be an irreducible element in a unique factorizatio domain D. Then P is neither zero nor a unit in D.

Let $P \mid ab$, $a, b \in D$. Then $ab = Pc$ for some c in D.

Since p is a non-unit and $P \mid ab$, at least one of a, b must be non-unit.

Case-1 Let one of a and b non-unit

If a be a unit and b be a non-unit then $a^{-1} \in D$ and $b = Pc(a^{-1})$ and therefore $P \mid b$.

If ~~b~~ b be a unit and a be a non-unit then $b^{-1} \in D$ and $a = p(cb^{-1})$ and therefore $p|a$.

So in this case $p|a$ or $p|b$.

Case-II

Let both of a and b be non-units.

Let $a = p_1p_2 \cdots p_r$ and $b = q_1q_2 \cdots q_s$, where $p_1, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ are irreducible in D.

If c be a unit, then $ab = pc$ implies ab is an associate of p and therefore ab is an irreducible. But it is not so

∴ c is a non-unit

Let $c = t_1t_2 \cdots t_k$, where $t_1, t_2, \ldots, t_k$ are irreducible in D.

$ab = pc$ gives $p_1p_2 \cdots p_r q_1 q_2 \cdots q_s = p t_1 t_2 \cdots t_k$

By uniqueness of the factorization of ab into irreducible it follows that p must be an associate of one of $p_1, p_2, p_3, \ldots, p_r$ or one of $q_1, q_2, \ldots, q_s$.

In this former case, $p|a$ and in the latter $p|b$.

So in this case $p|a$ or $p|b$.

Hence in any case $p|ab$ implies either $p|a$ or $p|b$.

So p is ~~an~~ prime element in D.

Ex. 11 Show that the elements $1+2i$ and $3+5i$ in the integral domain $Z[i]$ are prime to each other.

⇒ The integral domain $Z[i]$ is a UFD. $1+2i$ and $3+5i$ belong to $Z[i]$ and

$2(3+5i)+(-5)(1+2i) = 1$, 1 being the identity element in the domain.

This shows that $1+2i$ and $3+5i$ are prime to each other.

References – Higher Algebra – (8)
S.K. Mapa