E-Learning Materials for Sem - 6(I)

Unit - 1, CC - 14

Topic - Ring theory and Linear Algebra - II

Date - 09. 04. 2020.

Prepared by - Dr. Alauddin Dafadar.

1

Principal ideal domain (PID) :-> p-264

An integral domain is said to be a principal ideal domain if every ideal of the domain is a principal ideal

Principal ideal in a ring:

[Let S be a non-empty subset of R. The intersection of all ideals of R containing the subset S is an ideal of R and it is smallest ideal of R containing the subset S. This is said to be ideal generated by S. and it's called principal ideal of R.]

Ex.12 The ring Z is an integral domain and it is a ~~said to~~ be principal ideal domain.

=> In the ring Z, the ring of all integers, the ~~subring mZ (m being a positive integer) is a principal ideal~~.

Let mZ be a subring of Z., m being a positive integer.
The subring mZ is an ideal of the ring Z.

Let U be any ideal of Z containing the element m. Then $ma \in U$ for all $a \in Z$.

In other words, $mZ \subset U$.

This prove that the ideal mZ is the smallest ideal of Z containing the element m.

$\therefore$ mZ is a principal ideal of the ring Z.

Since all ideals in the ring Z are given by mZ where m is an integer ≥ 0.
It follows that all ideals of the ring Z are principal ideals, therefore the ring Z is PID.

Ex. 13 The ring $\mathbb{Z}[x]$ is an integral domain and it is not a principal ideal domain (PID).

$\Rightarrow$ Let us consider the ideal S of $\mathbb{Z}[x]$ generated by the element 2 and x of $\mathbb{Z}[x]$. Then

$$S = 2f(x) + xg(x) : f(x) \in \mathbb{Z}[x],\ g(x) \in \mathbb{Z}[x].$$

Let S be principal ideal of $\mathbb{Z}[x]$, say $\langle h(x) \rangle$ for some $h(x) \in \mathbb{Z}[x]$.

$2 \in S \Rightarrow 2 \in \langle h(x) \rangle \Rightarrow 2 = h(x)h_1(x)$ for some $h_1(x) \in \mathbb{Z}[x]$

$x \in S \Rightarrow x \in \langle h(x) \rangle \Rightarrow x = h(x)h_2(x)$ for some $h_2(x) \in \mathbb{Z}[x]$

$\therefore\ 2h_2(x) = xh_1(x)$.

This shows that each co-efficient of $h_1(x)$ is an even integer. So $h_1(x) = 2p(x)$ for some $p(x) \in \mathbb{Z}[x]$

consequently, $2 = 2h(x)p(x)$, therefore $h(x)p(x) = 1$

$h(x)p(x) = 1 \Rightarrow 1 \in \langle h(x) \rangle$ i.e.; $1 \in S$

$1 \in S \Rightarrow 1 = 2q(x) + x\,r(x)$ for some $q(x), r(x) \in \mathbb{Z}[x]$

Let $q(x) = a_0 + a_1x + a_2x^2 + \ldots$, $r(x) = b_0 + b_1x + b_2x^2 + \ldots$

Then $1 = 2(a_0 + a_1x + a_2x^2 + \ldots) + x(b_0 + b_1x + b_2x^2 + \ldots)$

$\therefore\ 1 = 2a_0$, an impossibility, since a_0 is an integer.

$\therefore$ S is not a principal ideal of $\mathbb{Z}[x]$.

Hence $\mathbb{Z}[x]$ is not a principal ideal domain.

In a principal ideal domain D, a non null ~~principal~~ ideal P or $\langle P \rangle$ is maximal if and only if P is an irreducible in D.

$\Rightarrow$ Let a non-null ideal $\langle P \rangle$ be maximal in D.

Then $\langle P \rangle \neq \langle 0 \rangle$, $\langle P \rangle \neq D$. i.e.; $P \neq 0$ and P is not a unit

Let $a \in D$ and a is divisor of P. $a | P$ implies $\langle P \rangle \subset \langle a \rangle$.
i.e.; either $\langle P \rangle = \langle a \rangle$ or $\langle P \rangle$ is properly contained in $\langle a \rangle$

If $\langle P \rangle = \langle a \rangle$, then a and p are associates.
If $\langle P \rangle$ is properly contained in $\langle a \rangle$, then $\langle a \rangle = D$, [since P is maximal]

$\langle a \rangle = D$
$\Rightarrow$ a is unit

Thus a is a divisor of P implies either a is an associates of P or a is a unit

Hence P is an irreducible in D.

Conversely,

Let P be an irreducible in D.

Let U be an ideal of D such that $\langle P \rangle \subset U \subset D$.

Since D is a PID, U is a principal ideal, ~~say $\langle q \rangle$ for~~ say $\langle q \rangle$, for some q in D.

$\langle P \rangle \subset U$

$\Rightarrow P \in \langle q \rangle$

$\Rightarrow P = qr$, for some $r \in D$.

Since P be an irreducible in D, $P = qr$ implies either q is a unit or q is an associate of P.

If q is a unit then $\langle q \rangle = D$. If q is an associate of P then $\langle q \rangle = \langle P \rangle$.

$\therefore \langle p \rangle \subset U \subset D$

$\Rightarrow$ Either $U = D$ or $U = \langle p \rangle$

This prove that $\langle p \rangle$ is maximal.

This complet the proof.

Theorem 04   P - 265

In a PID, any two non zero element a, b have a g, and if d be a gcd, then $d = ua + vb$ for some u, v in the domain.

$\Rightarrow$ Let us consider the principal ideals $\langle a \rangle$, $\langle b \rangle$ in D.

$\langle a \rangle + \langle b \rangle$ is also an ideal in D.

Since D is a PID, $\langle a \rangle + \langle b \rangle = \langle d \rangle$, for some d in

$\langle a \rangle + \langle b \rangle = \langle d \rangle$

$\Rightarrow \langle a \rangle \subset \langle d \rangle$ and $\langle b \rangle \subset \langle d \rangle$

$\langle a \rangle \subset \langle d \rangle$ or $\langle b \rangle \subset \langle d \rangle$

$\Rightarrow d \mid a$ $\Rightarrow d \mid b$

Thus d is a common divisor of a and b.

Let $e \mid a$ and $e \mid b$.

Then $\langle a \rangle \subset \langle e \rangle$ and $\langle b \rangle \subset \langle e \rangle$

$\Rightarrow \langle a \rangle + \langle b \rangle \subset \langle e \rangle$

$\therefore e \mid d$

Therefore d is a gcd of a and b.

2nd part

$\langle d \rangle = \langle a \rangle + \langle b \rangle$

$\Rightarrow d = au + bv$ for some u, v in D.

* In a UFD, any two non-zero element a, b have a gcd and if d be a gcd. then d may not be expressed as $ua + bv$. for some u, v in D 17

⇒ For example.

The polynomial ring $Z[x]$ is a UFD and 1 is a gcd of the elements 2 and x in $Z[x]$.

Let $1 = 2f(x) + xg(x)$ for some $f(x), g(x)$ in $Z[x]$.

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$, $g(x) = b_0 + b_1x + b_2x^2 + \cdots$

Then $1 = 2(a_0 + a_1x + a_2x^2 + \cdots) + x(b_0 + b_1x + b_2x^2 + \cdots)$

$\therefore 1 = 2a_0$ but this is not possible, since a_0 is an integer

So 1 (i.e., gcd of 2 and x) cannot be expressed as $2f(x) + xg(x)$ for some $f(x), g(x)$ in $Z[x]$.

Theorem 05 P - 266

In a principal ideal domain D, any two non-zero element a, b have an lcm.

⇒ Let us consider the principal ideal $\langle a \rangle$ and $\langle b \rangle$ in D.

$\langle a \rangle \cap \langle b \rangle$ is also an ideal in D.

Since D is PID, $\langle a \rangle \cap \langle b \rangle = \langle l \rangle$ for some l in D.

$\langle a \rangle \cap \langle b \rangle = \langle l \rangle$ ⑥

$\Rightarrow \langle l \rangle \subset \langle a \rangle$ and $\langle l \rangle \subset \langle b \rangle$

$\Rightarrow a | l$ and $b | l$

Thus l is a common multiple of a and b.

Let $a | m$ and $b | m$

$\Rightarrow \langle m \rangle \subset \langle a \rangle$ and $\langle m \rangle \subset \langle b \rangle$

$\Rightarrow \langle m \rangle \subset \langle a \rangle \cap \langle b \rangle$

i.e., $\langle m \rangle \subset \langle l \rangle$

Therefore $l \mid m$ and therefore l is an lcm of a and b.

This completes the proof.

<u>Ex. 14</u> Express the ideal $4\mathbb{Z} + 6\mathbb{Z}$ as a principal ideal in the integral domain $\mathbb{Z}$.

$\Rightarrow$ Since every ideal in the domain $\mathbb{Z}$ is a principal ideal the ideal $4\mathbb{Z} + 6\mathbb{Z}$ is a principal ideal.

Let $p\mathbb{Z} = 4\mathbb{Z} + 6\mathbb{Z}$.

Then $4\mathbb{Z} \subset p\mathbb{Z}$ and, $6\mathbb{Z} \subset p\mathbb{Z}$

$\Rightarrow p \mid 4$ and $p \mid 6$

So p is a common divisor of 4 and 6.

Let d be any common divisor of 4 and 6.

Then $d \mid 4$ and $d \mid 6$.

$d \mid 4$ implies that the ideal $4\mathbb{Z} \subset d\mathbb{Z}$ and

$d \mid 6$ implies that the ideal $6\mathbb{Z} \subset d\mathbb{Z}$

$\therefore 4\mathbb{Z} + 6\mathbb{Z} \subset d\mathbb{Z}$

i.e; $p\mathbb{Z} \subset d\mathbb{Z}$

$\Rightarrow d \mid p$

Thus p is a greatest common divisor of 4 and 6 i.e; $p = 2$

Hence $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

<u>Ex. 15</u> Express the ideal $8\mathbb{Z} \cap 12\mathbb{Z}$ as a principal ideal in the integral domain $\mathbb{Z}$.

$\Rightarrow$ Since every ideal in the domain $\mathbb{Z}$ is a principal ideal, the ideal $8\mathbb{Z} \cap 12\mathbb{Z}$ is a principal ideal

Let $p\mathbb{Z} = 8\mathbb{Z} \cap 12\mathbb{Z}$

Then $p\mathbb{Z} \subset 8\mathbb{Z}$ and $p\mathbb{Z} \subset 12\mathbb{Z}$

$\Rightarrow 8 \mid p$ and $12 \mid p$

So p is common multiple of 8 and 12,

Let m be any common multiple of 8 and 12.

Then $8 | m$ and $12 | m$

$\Rightarrow$ The ideal $m\mathbb{Z} \subset 8\mathbb{Z}$ and the ideal $m\mathbb{Z} \subset 12\mathbb{Z}$.

$\Rightarrow$ $m\mathbb{Z} \subset 8\mathbb{Z} \cap 12\mathbb{Z}$

i.e; $m\mathbb{Z} \subset p\mathbb{Z}$

$\Rightarrow$ $p | m$.

Thus p is a least common multiple of 8 and 12 i.e; $p = 24$

Hence $8\mathbb{Z} \cap 12\mathbb{Z} = 24\mathbb{Z}$.

Ex. 16 Show that every proper ideal in a PID is contained in a maximal ideal.

Euclidean Domain :→ P – 270

v: non-zero element of D → non negative integer.

An integral domain D is said to be a Euclidean domain if there exist a function v that maps the non-zero elements of D into the non-negative integers satisfying the following conditions ——

1) $v(a) \leq v(ab)$ for all non-zero $a, b \in D$; and
2) for all $a, b \in D$ with $b \neq 0$, $\exists$ q and r in D such that $a = bq + r$, where either $r = 0$ or $v(r) < v(b)$

The function v is said to be a Euclidean valuation ~~function~~ on D

Ex. 17 The integral domain $\mathbb{Z}$ is a Euclidean domain.

⇒ Let us define a function v by $v(a) = |a|$ for all non-zero a in $\mathbb{Z}$.

i) Let a, b non-zero element in $\mathbb{Z}$. Then $ab \in \mathbb{Z}$ and ab

$v(ab) = |ab|$, $v(a) = a$, $v(b) = b$

$\therefore$ $v(ab) = v(a)\, v(b)$

ii) Let $a, b \in \mathbb{Z}$ and $b \neq 0$.

By division algorithm, $\exists$ integers q and r such that $a = bq + r$ with either $r = 0$ or $0 < r < |b|$.

$0 < r < |b| \Rightarrow |r| < |b| \Rightarrow v(r) < v(b)$

$\therefore$ For $a, b \in \mathbb{Z}$ and $b \neq 0$, $\exists$ element q and r in $\mathbb{Z}$ such that $a = bq + r$ with either $r = 0$ or $v(r) < v(b)$

Thus v satisfies both the conditions of Euclidean valuation on $\mathbb{Z}$ and $\mathbb{Z}$ becomes a Euclidean domain.

Ex 18 A field F is a Euclidean domain.

⇒ Let us define a function v by $v(a)=1$ for all non-zero a in F.

i) Let a, b be non-zero elements in F. Then $ab \in F$ & $ab \neq 0$

$v(ab) = 1$. $v(a) = 1$, $v(b) = 1$

$\therefore v(ab) = v(a)\, v(b)$

ii) Let $a, b \in F$ and $b \neq 0$. Then $b^{-1} \in F$ and $a = (bb^{-1})a$.

$= b(b^{-1}a)$

$= bq + r$,

where $q = b^{-1}a$, $r = 0 \in F$

Thus v satisfies both the conditions of a Euclidean valuation on F and F becomes a Euclidean domain.

Ex 19 Show that $Z[i]$ is a Euclidean domain.

⇒ Let us define a function v by $v(\alpha) = N(\alpha)$ for all non-zero α in $Z[i]$.

where $N(a+bi) = a^2+b^2$

i) If $\alpha = a+bi$ and $\beta = c+di$ be non-zero element in $Z[i]$.

Then $N(\alpha\beta) = N(\alpha)N(\beta) = (a^2+b^2)(c^2+d^2) \geq (a^2+b^2) = N(\alpha)$.

ii) Let $a+bi$, $c+di$ belong to $Z[i]$ with $(c+di) \neq 0$.
i.e., $c \neq 0, d \neq 0$.

Let $\frac{a+bi}{c+di} = p+qi$ —— ⓐ

Then $p \left[= \frac{ac+bd}{c^2+d^2}\right]$, $q = \left[\frac{bc-ad}{c^2+d^2}\right]$ are rational number.

There exist integers m, n such that

$|p-m| \leq \frac{1}{2}$, $|q-n| \leq \frac{1}{2}$.

Let $p-m = \alpha$, $q-n = \beta$ Then α, β are rational and
$|\alpha| \leq \frac{1}{2}$, $|\beta| \leq \frac{1}{2}$

we have $(a+bi) = (c+di)(p+qi)$ by (a)

$= (c+di)(m+\alpha + ni + \beta i)$

$= (c+di)(m+ni) + r$, where $m+ni \in \mathbb{Z}[i]$

$r = (\alpha+\beta i)(c+di)$

Let $r = s+ti$ for some $s, t \in \mathbb{Z}$

Either $r=0$, or $v(r) = N(s+ti) = s^2+t^2 = (c^2+d^2)(\alpha^2+\beta^2)$ since $|\alpha| \le \frac{1}{2}$, $|\beta| \le \frac{1}{2}$

$\Rightarrow v(r) \le (c^2+d^2)\left(\frac{1}{4}+\frac{1}{4}\right)$

$\Rightarrow v(r) < (c^2+d^2)$

$\Rightarrow v(r) < v(c+di)$

Thus $a+bi = (c+di)(m+ni) + r$, where $m+ni, r \in \mathbb{Z}[i]$

and either $r=0$ or $v(r) < v(c+di)$.

Hence $\mathbb{Z}[i]$ is Euclidean domain under the Euclidean valuation v.

Theorem 06 :⇒ p - 273

Every Euclidean domain is a PID.

⇒ Let D be an Euclidean domain with a Euclidean valuation v.

Let U be an ideal of D.

Case - I

Let $U = \{0\}$, the null ideal.

Then $U = \langle 0 \rangle$, a principal ideal.

Case - II

Let U be a non-null ideal

Then $\exists$ a non-zero element b in U such that $v(b)$ is the least of all $v(x)$ for all non-zero x in U.

Such an element b exist by the well ordering

---

property of the set ... Let $a \in U$. Then by the condit... there exist element... where either r = ... Since U is an ...

$\therefore v(r) < v(b)$, ...

$\therefore r = 0$ and a ...

Since a is a...

$U = \langle b \rangle$, a ...

Thus every ...

$\therefore D$ is a P...

This complet...

Theorem 07

Let D be ... v. Then

i) $v(1)$ is ...

ii) an el...

...erty of the set $\mathbb{N}$

...t $a \in U$.

...hen by the condition ii) of the Euclidean valuation v,
...here exist elements q and r in D such that $a = bq + r$.
where either $r = 0$ or $v(r) < v(b)$.

Since U is an ideal $a \in U$, $b \in U \Rightarrow a - bq \in U$,

$\Rightarrow r \in U$

$\therefore$ $v(r) < v(b)$, is not possible, by the choice of b.

$\therefore$ $r = 0$ and $a = bq$ for some $q \in D$.

Since a is an arbitrary element in U,
$U = \langle b \rangle$, a principal ideal.

Thus every ideal in D is a principal ideal.

$\therefore$ D is a PID.
This complete the proof.

Theorem 07

Let D be a Euclidean domain with a Euclidean valuation v. Then

i) $v(1)$ is minimal along all $v(a)$ for non-zero a in D.
ii) an element u in D is a unit if and only if $v(u) = v(1)$.

Polynomial Rings :⇒ P – 292

Let R be a ring and x be underterminate.

A polynomial in x over R is $f(x)$

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots, \; a_i \in R$

① If for some $n \geq 0$, $a_n \neq 0$ and $a_i = 0$ for all $i > n$ then a_n is said to be $\boxed{\text{leading coefficent}}$ of $f(x)$.
n is said to be the degree of $f(x)$, $\deg(f) = n$ or $\deg(f(x)) = n$

② If n such exist, then the polynomial is of the form
$f(x) = a_0 + 0x + 0x^2 + \cdots \cdots$, it is be a constant polynomial
$\deg(f(x)) = 0$.

③ If $a_i = 0$, for all $i = 0, 1, 2, \ldots \ldots$, it is be a zero-polynomial. and no degree assigned to it.

Theorem 09 :⇒

If R be a ring with no divisor of zero, then the ring $(R[x], +, \cdot)$ is a ring with no divisor of zero.

⇒ Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ and
$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ be non-zero element in $R[x]$ with leading coffiecents a_m, b_n respectively.

Let us consider the product $f(x) \cdot g(x)$.
The co-efficent of x^{m+n} in the product $f(x) \cdot g(x)$. is $a_m b_n$ and it is non-zero,

Since R contains no divisor of zero.
$\therefore$ $f(x) \cdot g(x)$ is a non-zero polynomial in $R[x]$.
This prove that the ring $(R[x], +, \cdot)$ contain no divisor of zero.

Division Algorithm :⇒

Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = g(x)\,q(x) + r(x)$$

where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

i) $q(x)$ is called the <u>quotient</u>, $r(x)$ is called the <u>remainder</u> in the division of $f(x)$ by $g(x)$.

Zero or root :⇒

An element a in a field F is said to be zero (or root) of a polynomial $f(x)$ in $F[x]$ if $f(a) = 0$ in F.

Ex:⇒ $\bar{1}$ in $\mathbb{Z}_5$ is a zero ~~element~~ of the polynomial

$$f(x) = x^3 + \bar{2}x^2 + x + \bar{1}$$

$$= (\bar{1})^3 + \bar{2}(\bar{1})^2 + \bar{1} + \bar{1}$$

$$= \bar{1} + \bar{2} + \bar{1} + \bar{1}$$

$$= \bar{5}$$

$$= \bar{0}.$$

Irreducible polynomial :⇒

Let f be a field. A nonconstant polynomial $f(x)$ in $F[x]$ is said to be an <u>irreducible polynomial</u> in $F[x]$ if $f(x)$ <u>cannot be expressed</u> as the product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree them ~~f(x)~~ $\deg(f(x))$..

** [Since F is a field, $F[x]$ is UFD and therefore there is no distinction between a prime element and an irreducible element in $F[x]$.]

** [A polynomial ... field F, bu... large field

Ex:⇒ The pol... but is not ... because $x^2 - 2$ ...

Theorem 12 :

Let $f(x)$ be ... Then $f(x)$ i... a zero in ...

⇒ Let $f(x)$ ... where deg(... Since deg ... Then one ... If say ... Then g(x ... clearly ... $f(x)$ – a ...

Conversely, Let $a \in$ ... Then $x -$ ... $f(x)$ i... This c...

Ex:⇒ Since the ... polynom...

NB: [A polynomial $f(x)$ in $F[x]$ may be irreducible over the field F, but it may not be irreducible over a large field K containing F as a subfield.]

Ex: The polynomial x^2-2 is irreducible over the field $\mathbb{Q}$ but is not irreducible over the field $\mathbb{R}$.

because $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ in $\mathbb{R}$.

Theorem 12: P – 297

Let $f(x)$ be a polynomial in $F[x]$ of degree 2 or 3. Then $f(x)$ is $\boxed{\text{reducible}}$ over F if and only if it has a zero in F.

$\Rightarrow$ Let $f(x)$ be reducible over F. Then $f(x) = g(x)\,h(x)$ where $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$.

Since $\deg(f(x))$ is either 2 or 3.

Then one of $g(x)$ and $h(x)$ must be of degree 1.

If say $g(x)$ is of degree 1.

Then $g(x) = ax+b$, $a \neq 0$, $a, b \in F$.

clearly $g(x)$ has a zero $-a^{-1}b$, in F and consequently $-a^{-1}b$ is a zero of $f(x)$.

Conversely,

Let $a \in F$ be a zero of the polynomial $f(x)$ in $F[x]$.

Then $x-a$ is a factor of $f(x)$ and this proves that $f(x)$ is reducible over F.

This completes the proof.

Ex: $f(x) = x^3+x+1$ is irreducible over $\mathbb{Z}_2$, because since the polynomial $f(x)$ is of degree 3 and none of the elements of the field $\mathbb{Z}_2$ is a zero of the polynomial.

Refenencea — Highen Algebra — (8)
S.K. Mapa.