Ring Theory 12

19 May 2024 16:29

Def:- A ring R is a PID if it is an integral domain and every ideal of R is principal ideal.

Example:- Ring of integers $\mathbb{Z}$ is a PID

Proposition:- If $\mathbb{F}$ is a field then it is a PID

Proof:- I be a ideal of $\mathbb{F}$

If $a \in I$ and $a \neq 0$.

$aa^{-1} \in I \Rightarrow 1 \in I$

$\Rightarrow r1 \in I$ for $r \in \mathbb{F}$ and $\{0\} = \langle 0 \rangle$

$\Rightarrow \mathbb{F} = I$ // $\Downarrow$

$\Rightarrow$ Ideal of $\langle 1 \rangle$ and $\langle 0 \rangle$

Prop:- If $\mathbb{F}$ is a field then the ring of polynomials $\mathbb{F}[x]$ is a PID

- $\mathbb{Z}[x]$ is not a PID as $I = \langle 2, x \rangle$ is not principle

Prop:- If R is an Euclidean domain then R is a PID

Proof:- Let I be ideal of R.

$0 \neq a \in I$ and $N(a) < N(b)$ $\forall\, b \in I$ and $b \neq 0$

Let $x \in I$, $x = qa + r \Rightarrow r = 0$ or $N(r) < N(a)$ ✗ not true

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

$\Rightarrow I = \langle a \rangle$

- a and b are associates if $\langle a \rangle = \langle b \rangle$, i.e., $a | b$ and $b | a$

- In $\mathbb{Z}$, the units are $+1, -1$. For $a \in \mathbb{Z}$, $a, -a$ are associates

- Let $\mathbb{F}$ be a field. In $\mathbb{F}[x]$, the units are the polynomials of degree 0 $0 \neq a \in \mathbb{F}$. $a, -a$ are associates.

- > Let $\mathbb{F}$ be a field. In $\mathbb{F}[x]$, the units are the non-zero polynomial of degree 0. $0 \neq a \in \mathbb{F}$, $a, -a$ are associates.

$S = (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1)$ $\quad mS$, $m \in \mathbb{F}$, $m \neq 0$

So, S, mS are associates.

<u>Def</u>:- Let $a \in R$. A factorization of a is a pair $b, c \in R$ such that $a = bc$. When c is a unit then a and b are associates.

<u>Lemma</u>:- Let $a \in R$ be an element which is not a unit. If $a \neq 0$ then the followings are equivalent:-

(i) Every factorization of a is trivial

(ii) The only divisors of a are associates and units

(iii) The ideal $\langle a \rangle$ is maximal in the set,
$\{ I \trianglelefteq R \mid \langle 0 \rangle \neq I \neq R,\ I \text{ is principal} \}$

When these are true we get that a is irreducible, otherwise, a is reducible.

<u>Example</u>:- In $\mathbb{Q}[x]$ $x^2 - 3$ is irreducible, but it is reducible in $\mathbb{R}$.

<u>Definition</u>:- Let R be an integral domain. Then R is a UFD if:

(i) $\forall\, a \in R$ and $a \neq 0$, a not a unit we can get a as a product of irreducibles

(ii) This factorization of a is unique upto reodering and associates.

<u>Example</u>:- $\mathbb{Z}$ is a UFD, $\mathbb{Q}$ is a UFD

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

$(\quad)(\quad) = a^2 - 5b^2$

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

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

$a = 3,\ b = 1 \Rightarrow 4 = 2 \times 2 = (3+\sqrt{5})(3-\sqrt{5})$

So $\mathbb{Z}[\sqrt{5}]$ is not a UFD

Quadratic Rings :- D is not a square

$\mathbb{Z}[\sqrt{D}]$

$\alpha = a - b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ $\quad N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$

$N(\alpha) = a^2 - Db^2 = \alpha\bar{\alpha}$

$N(\alpha\beta) = N(\alpha)N(\beta)$ $\Rightarrow$ N is a ring homomorphism on multiplication operations

$\forall \alpha, \beta \in \mathbb{Z}[\sqrt{D}]$

$N(\alpha) = 0$ iff $\alpha = 0$

α is a unit iff $N(\alpha) = \pm 1$

If $\alpha \mid \beta$ in $\mathbb{Z}[\sqrt{D}]$ then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$

$\hookrightarrow \beta = a\alpha$, $a \in \mathbb{Z}[\sqrt{D}]$

$N(\beta) = N(a)N(\alpha)$

- Let S be the set of all formal function, $f : \mathbb{R} \to \mathbb{R}$ which are of the form,

$$f(x) = a_0 + a_1 x^{q_1} + a_2 x^{q_2} + \cdots + a_m x^{q_m}$$

for some $m \in \mathbb{N}$, $a_0, \ldots, a_m \in \mathbb{R}$, $q_1, \ldots q_m \in \mathbb{Q}$

$\Rightarrow \quad q_1 = \frac{r_1}{s_1}, \quad \ldots, \quad q_m = \frac{r_m}{s_m}$

$f(x)^{-1} = \frac{1}{f(x)} \Leftarrow$ If $a_0 \neq 0$ then $f(x)$ is invertible

$f(x)\frac{1}{f(x)} = 1$

$f(x) = g(x)h(x) = p(x)q(x)$

upto associates this factorization is unique

$\Rightarrow S$ is a UFD

Lemma:- Let R be an integral domain. Let $a, b \in R$. Assume that d is one gcd of a and b. Let $x \in R$ be another element. Then x is another gcd of a and b iff x and d are associates.

Definition:- R be an integral domain is also a GCD-domain if

(i) $\forall\, a, b \in R,\ a, b \neq 0\ \exists$ a gcd of a and b

(ii) $\gcd(a, b) = d \Rightarrow d = xa + yb$ for some $x, y \in R$

Lemma:- Every UFD is a GCD-domain

Proof.- $a, b \in$ UFD

$a = u_a p_1 p_2 \cdots p_n$

$b = u_b q_1 q_2 \cdots q_m$

$\Rightarrow p_i$'s and q_i's are irreducible

Let $d | a$, $d | b$

arrange to, p

$a = u_a \underbrace{(p_1 \cdot\, p_t)}_{d}\, \overbrace{p_{t+1} \cdots p_n}$

$b = u_b \underbrace{(q_1 \cdots q_t)}_{d}\, \underbrace{q_{t+1} \cdots q_m}_{q}$

$\Rightarrow p_i$ and q_i upto t are associates and $t+1$ to rest is not

so d is a gcd

Let d' be another gcd of a, b. $\Rightarrow d' | a$, $d' | b$

If d' is a unit $\Rightarrow d' | d$

Now suppose $d' \nmid d \Rightarrow d | d' \Rightarrow d$ has a unique factorization in d'

complete factorization of d' will have some subpart that $\nmid d$

but $d' | a$ and $d' | b \Rightarrow$ (all subparts of d') $| a, b$

$\Rightarrow \Leftarrow$ contradiction

$\Rightarrow d' | d \Rightarrow d'$ and d are associates

$\Rightarrow d' | d$ $\Rightarrow d'$ and d are associates

Using Euclid's lemmas we can get x, y