Ring Theory

Lecture 23

Prop. Let R be an int domain.

TFAE

(1) For every non-zero elt which is not a unit, the process of factoring a terminates after finitely many steps and results a factorization of a into irreducible elts.

(2) R doesn't contain an infinite increasing chain of principal ideals

$(a_1) \subsetneq (a_2) \subsetneq \cdots$

Pf: Suppose R contains an infinite increasing seq^n of principal ideals

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

Then $(a_n) \subsetneq (1) \quad \forall n.$

$$a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2$$

$$= \cdots$$

which leads to the factorization of a_1 as a product of infinitely many elts.

Converse follows similarly.

Example. Consider the poly $F[x_1]$ and adjoin all 2^k-th roots of x_1 to the poly ring $F[x_1]$.

Let $R = F[x_1, x_2, x_3, \ldots]$

where $x_2^2 = x_1$, $x_3^2 = x_2$, $x_4^2 = x_3$.

and so on. $\ldots$

$\therefore$ We can factor x_1 indefinitely in the ring R and we get an infinite chain of principal ideals

$$(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$$

Propn: Let a & b be two non-zero elts of an UFD R. and let $a = u p_1^{e_1} \cdots p_n^{e_n}$

$b = v p_1^{f_1} \cdots p_n^{f_n}$ are prime factorization of a & b where u & v are units the primes $p_1, \ldots, p_n$ are distinct & $e_i, f_i \geq 0$ are exponent.

Then the elt $d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$

is the gcd of a, b.

Ex pf of the propn

In $\mathbb{Z}$. $a, b \in \mathbb{Z}$.

Let $d = \gcd(a, b)$

$\Leftrightarrow$ $d = ap + bq$ for some $p, q \in \mathbb{Z}$.

Q Is it possible to write down the gcd of two elts as a above for any UFD?

Example $\mathbb{Z}[x]$ is an UFD.

$\gcd(2, x) = 1$. but 1 is not a combination of 2 & x.

Defn. An int domain R is called principal ideal domain (PID) if every ideal of R is principal.

Example (1) $F[x]$ where F is a field is a PID

(2) $\mathbb{Z}$ is a PID.

Propn: Let R be a FD. Then it is an UFD iff every irreducible element is prime.

Pf: ($\Leftarrow$) Let every irreducible elt is prime. Let $0 \neq a \in R$ be a non unit elt

Let $a = p_1 \cdots p_m = q_1 \cdots q_n$

where p_i, q_i are primes.

We may assume $m \leq n$.

Since (p_1) is a prime ideal

$\exists\, q_j$ s.t $q_j \in (p_1)$.

Here $q_j = p_1 r_j$ for some $r_j \in R$

$$p_1 \cdots p_m = q_1 \cdots q_{j-1} p_1 r_j q_{j+1} \cdots q_n$$

$$\Rightarrow p_2 \cdots p_m = q_1 \cdots q_{j-1} r_j q_{j+1} \cdots q_n.$$

Since q_j is irreducible r_j is a unit. Then the pf is done by induction.

(p_2) is prime ideal.

Let $q_1 \in (p_2)$. then $q_1 = p_2 v_2$

$$p_3 \cdots p_m = v_2 q_2 \cdots q_{j-1} v_j q_j \cdots q_n$$

$$1 = v_1 v_2 \cdots v_l q_l q_{l+1} \cdots q_n$$

$\Rightarrow q_i$ are unit.

But q_i's are prime elt so they can not be unit.

$\therefore \underline{\underline{m = n}}$.

and this prove that a has a unique factorization.

Propn. In a PID irreducible elts are prime.

Pf: Let p be an irreducible elt. WTS (p) is a prime ideal

Let $ab \in (p) \Rightarrow p \mid ab$.

Let $p \nmid a$ WTS $p \mid b$.

Then $(p) \subsetneq (p, a)$

(p) is maximal among proper principal ideals as p is irreducible.

Therefore $(p, a) = R = (1)$

$1 = pc + ad$ for some $c, d \in R$.

$\Rightarrow b = bpc + abd$

$= bpc + pld$ $(\because p \mid ab$ $\therefore ab = pl)$

$= p(bc + ld)$

$\Rightarrow p \mid b$.

$\Rightarrow b \in (p)$.

Hence p is a prime elt.

Remark we observed that in $\mathbb{Z}$ and $F[x]$ every non zero prime ideal is maximal ideal. Is this true in any PID?

Propn: Every non-zero prime ideal in a PID is a maximal ideal.

Pf: Let (p) be a non-zero prime ideal. Let (p) is not maximal ideal. Then $\exists$ a maximal ideal s.t $(p) \subsetneq (m) \Rightarrow p = rm$ for some $r \in R$.

Since (p) is a prime ideal & $rm \in (p)$ then either $r \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(p) = (m)$ is maximal ideal

If $r \in (p)$ then $r = p \cdot s$.

$\therefore \quad p = pm = psm$

$\Rightarrow \quad sm = 1. \quad \Rightarrow m$ is an unit.

which is a contradiction.

Remark. If R is a field then we know that $R[x]$ is a PID.

Q If R is a ring and $R[x]$ is a PID. Can we say R is field?

Prop^n. Let R be any ring and $R[x]$ is a PID. Then R is a field

Pf: Since $R[x]$ is a PID and $R \subset R[x]$ is a subring of $R[x]$. $\therefore$ R must be an int domain.

$R[x]/(x) \cong R$ is an int domain

$\Rightarrow (x)$ is a prime ideal in $R[x]$.

As $R[x]$ is a PID so (x) is a maximal ideal

$\therefore$ R is a field.

Prop A PID is an UFD.

Pf: WTS Existance of factorizati in R which is equivalent to show that R contains no infinite increasing chain of principal ideals.

Suppose $(a_1) \subsetneq (a_2) \subsetneq \cdots$ is an infinite chain of principal ideals. Let I be the union of this chain of principal ideals.

Since R is a PID

$\therefore I = (b)$

Now since b is the union of the ideals (a_n), it is one of

these ideals. Let $b \in (a_n)$

then $(b) \subset (a_n)$

on the other hand

$$(a_n) \subset (a_{n+1}) \subset (b)$$

$\therefore (a_n) = (a_{n+1}) = \cdots = b.$

This contradict $(a_n) \subsetneq (a_{n+1})$

Hence we are done.

<u>Remark</u>. Note that every UFD is not a PID. For example $\mathbb{Z}[x]$ is an UFD but it is not a PID.

Notion of Division algorithm is there in $\mathbb{Z}$ and $F[x]$.

In $\mathbb{Z}$, $b = aq + r$ where either $r = 0$ or $|r| < |a|$.

In $F[x]$, $g(x) = f(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

Let us now abstract the procedure of division algorithm with remainder. To do this we need a notion of size

of an elt in a ring.

In general a size fn on an int domain R will be a fn

$$N : R \setminus \{0\} \longrightarrow \{0, 1, 2, \dots\}$$

from the set of non-zero elts of R to the set of non-negative integers.

Defn An int domain R is an Euclidean domain if there is a size fn. N on R s.t for all $a, b \in R$ s.t $a \neq 0$ ther are elts $q, r \in R$ s.t $b = aq + r$ and either $r = 0$ or $N(r) < N(a)$,

here q is called the quotient and r is called the remainder.

Examples (1) $\mathbb{Z}$ is an ED with

$$N(a) = |a|$$

(2) $F[x]$ where F is a field is an ED with $N(p(x)) = \deg p(x)$

(3) $\mathbb{Z}[i]$ is an ED with

$$N(a+ib) = a^2+b^2.$$

Let $\alpha = a+ib$, $\beta = c+id \neq 0$.

Then $\alpha/\beta = \dfrac{a+ib}{c+id} = \dfrac{(a+ib)(c-id)}{c^2+d^2}$

$$= \frac{ac+bd}{c^2+d^2} + i \cdot \frac{bc-ad}{c^2+d^2}$$

$\alpha/\beta = r + is \in \mathbb{Q}[i]$.

Let $p \approx q$ be integers closest to $r \approx s$

$\therefore |r-p| \approx |s-q|$ are atmost $1/2$.

Let $\theta = (r-p) + (s-q)i$

$\nu = \beta\theta = \beta[(r-p) + i(s-q)]$

$= \beta(r+is) - \beta(p+iq)$

$= \alpha - \beta(p+iq) \in \mathbb{Z}[i]$.

$\therefore \alpha = \beta(p+iq) + \nu$

$N(\nu) = N(\beta\theta) = N(\beta)N(\theta)$

$$N(\gamma) = N(\beta)\,N(\theta)$$

$$= N(\beta)\left[|r-p|^2 + |s-q|^2\right]$$

$$\leq N(\beta)\left[\frac{1}{4}+\frac{1}{4}\right] = \frac{1}{2}N(\beta).$$

$$\Rightarrow N(\gamma) < N(\beta).$$

$\therefore \mathbb{Z}[i]$ is an ED.

Thm. ED are PID.

Pf: Let R be an ED and I be a non-zero ideal of R.

Let us consider the set

$$S = \{N(a) \mid a \in I,\ a \neq 0\}.$$

By well ordering principal S has a minimal elt say $N(b)$...

Then WTS $I = (b)$.

Let $a \in I$ then $a = bq + r$ for $q, r \in R$ & either $r = 0$ or $N(r) < N(b)$.

$r = a - bq \in I$. & $N(b)$ is is minimal in S so $r = 0$.

$\therefore I = (b)$.

Fields $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ Int dom

eg. $\mathbb{Z}$ is an ED which is not a field.

$\mathbb{Z}\left[(1+\sqrt{-19})/2\right]$ is a PID but not an ED.

$\mathbb{Z}[x]$ is an UFD but not a PID.

$\mathbb{Z}[\sqrt{-3}]$ is an int domain but not a UFD.