PID

Lecture 30

Q. In an UFD we know every irreducible elt is prime.

Is the converse true?

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

Pf: ($\Leftarrow$) Assume that every irreducible elt is prime. WTS R is an UFD.

Let $0 \neq a \in R$ be an non-unit elt.

Then $a = p_1 \cdots p_m = q_1 \cdots q_n$ — (*)

where p_i, q_i are prime elts.

We may assume $m \leq n$.

Since (p_1) is a prime ideal $\exists\ q_j$ s.t $q_j \in (p_1)$. Hence $q_j = p_1 x$.

Since q_j is irreducible so p_j' must be an unit. Now substituting $q_j = p_1 p_j'$ in (*) we get

$$p_1 p_2 \cdots p_m = q_1 \cdots p_1 p_j' q_{j+1} \cdots q_n$$

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

Continuing the process we can see that $m = n$ and p_i is associate to some q_j. Hence R is an UFD.

Propn: A PID is an UFD.

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

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

i.e $I = \bigcup_{i=1}^{\infty} (a_i)$.

Note that I is an ideal of R.

Since R is a PID let $I = (b)$

Since $b \in \bigcup_{i=1}^{\infty} (a_i) \Rightarrow b \in (a_n)$ for some n. $\Rightarrow (b) \subset (a_n)$.

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

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

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

Therefore we are done.

Example. $\mathbb{Z}[x]$ is an UFD but it is not a PID. $\mathbb{Z}[x]$ is not a PID because the ideal $(2, x)$ can't be gen by by a single elt.

But $(2,x) \in R[x]$. and

$(2,x) = (1)$ because 2 is a unit in $R[x]$.

Remark We observed that in $\mathbb{Z}$ and $k[x]$ every non-zero prime ideal is a maximal ideal.

Q Is every nonzero prime ideal is a maximal ideal in a 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 $(p) \subset (m)$ $\rightarrow$ is a maximal ideal.

(1) $\Rightarrow$ $p = rm$ for some $r \in R$.

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

if $r \in (p)$ then $r = ps$ — (2)

From eqn (1) & (2) we get $p = psm \Rightarrow (sm-1) = 0 \Rightarrow m$ is a unit which contradiction.

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

Q Is the converse true? If $R[x]$ is a PID then is R a field?

Cor. 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 $\therefore$ R must be an int domain.

Now (x) is a non-zero prime ideal in $R[x]$ since $R[x]/(x) \cong R$, is an int domain.

By previous prop^n every prime ideal

is maximal ideal and hence R is a field.

Euclidean Domain (ED):

Let us now abstract the procedure of division with remainder (division algorithm)

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

$a = bq + r$. either $r = 0$ or $r < |b|$.

$f(x), g(x) \in k[x]$.

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

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

To generalize the notion of division algorithm we need a notion of size of an elt of a ring.

In general a size f.n. on an int domain R will be any f.n

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

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