PID

lecture 29

Defn An int domain R is called a factorization domain (FD) if every non-zero non-unit elt of R can be expressed as a finite product of irreducible elts.

Propn Let R be an int domain. TFAE

(1) For every nonzero elt $a \in R$ which is not a unit, the process of factoring a into irreducible factors terminates after finitely many steps and results a factorization of a into irreducible elts of R.

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

$(a_1) \subset (a_2) \subset \cdots$

Pf: ($\Rightarrow$) Suppose R contains an infinite increasing chain of principal ideals say

$(a_1) \subset (a_2) \subset (a_3) \subset \cdots \subset (a_n) \cdots$

since $(a_{n-1}) \subset (a_n)$ $\therefore a_{n-1} = a_n b_n$ where a_n & b_n are non-units.

$\therefore a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2 = \cdots$

which gives a contradiction.

Prove the converse part similarly.

Example: Consider the poly ring $F[x]$ where F is a field.

Let $R = F[x_1, x_2, x_3, x_4, \cdots]$

where $x_2^2 = x_1$; $x_3^2 = x_2$, $x_4^2 = x_3$ and so on.

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

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

In $\mathbb{Z}$ we can talk about gcd of two integers say a & b.

If $\gcd(a,b) = d$ say

$$d = ra + sb \quad \text{where } r, s \in \mathbb{Z}.$$

Q Does gcd of two elts exists in an UFD?

Q If gcd of two elts exists in an UFD then can we write the gcd as a combination of the two elts?

Prop 2: Let a & b be two non-zero elts of an UFD and let

$a = u p_1^{e_1} \cdots p_n^{e_n}$ and $b = v p_1^{f_1} \cdots p_n^{f_n}$

are factorizations of a & b where u, v are units and the primes $p_1, p_2, \ldots, p_n$ are distinct & $e_i, f_i \geq 0$.

Then the elt $d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_n^{\min(e_n, f_n)}$

is the gcd of a & b.

Pf: Since the exponents of each of the prime occuring in d are no larger than exponent occuring in the factorization of a & b, d divides both a & b.

Let c be any common divisor of a & b. Let $c = q_1^{g_1} \cdots q_m^{g_m}$ be a prime factorization of c. Since q_i divides c hence q_i divides a and b and hence q_i must divides one of the primes p_j.

$\therefore \{q_1, \ldots, q_m\} \subseteq \{p_1, \ldots, p_n\}$.

Similarly, the exponents for the primes occuring in c must be no larger than those occuring in d. This implies c divides d. Therefore d is the gcd of a & b.

Example. However in UFD $\gcd(a,b)$ need not have the form $ra+sb$ for some r, s. For example $\mathbb{Z}[x]$ is an UFD. $\gcd(2, x) = 1$. but 1 is not a linear combination of 2 & x.

Defn An integral domain R is called a principal ideal domain (PID) if every ideal of R is principal (i.e gen by a single elt).

Example $\mathbb{Z}$, $k[x]$ are PID.

Propn. In PID irreducible elts are prime.

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

Let $ab \in (p)$ and $a \notin (p)$.

WLOG $b \in (p)$.

Since $ab \in (p) \Rightarrow p \mid ab$

and $p \nmid a$.

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

Since p is irreducible thus (p) is maximal among proper principal ideals.

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

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

$b = bpc + abd. \in (p)$.

Hence we are done.

Q What is the relation between a PID & an UFD ?

$$b \subset (d).$$

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