# UFD

lecture 28

In $\mathbb{Z}$. $\ni m$

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

where $p_i$'s are prime numbers.
and this representation is unique.

$$k[x] \ni f(x)$$

$$f(x) = f_1(x) \cdots f_r(x).$$

where $f_i(x)$ are irreducible polys.

Consider the ring $R = \mathbb{Z}[\sqrt{-3}]$.

$$= \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

$4 \in R$.

$$2 \cdot 2 = 4 = (1+\sqrt{-3})(1-\sqrt{-3}).$$

# Unique Factorization Domain :

For the rest of the lectures I will assume that $R$ is an integral domain.

**Defn.** We say an elt $a$ divides another elt $b$ (denoted by $a|b$) if $b = aq$ for some $q \in R$.

The elt $a$ is a proper divisor of $b$ if neither $a$ nor $q$ is an unit.

Two elts $a, b$ are called associates if $a = ub$ for some unit $u$.

**Defn.** A nonzero elt $a$ of $R$ is called irreducible if it is not a unit and it has no proper divisor (i.e. if $a = bc$ then either $b$ or $c$ is a unit)

**Defn.** We say an elt $a$ is prime if $(a)$ is a prime ideal.

**Propn.** Let $R$ be an int domain and $0 \neq a \in R$. If $a$ is a prime elt then it is irreducible.

**Pf:** $(a)$ is a prime ideal.

If $a = bc \Rightarrow bc \in (a)$

$\Rightarrow$ either $b \in (a)$ or $c \in (a)$.

WLOG let $b \in (a)$.

Then $b = ad$

$\Rightarrow a = bc = adc$

$\Rightarrow a(1-dc) = 0$

$\Rightarrow dc = 1.$

$\Rightarrow c$ is a unit.

$\therefore a$ is irreducible.

Example The irreducible elts of $\mathbb{Z}$ are prime numbers.

and irreducible elts of $k[x]$ are irreducible polys.

Q Is every irreducible elt is prime?

**Remark**: Irreducible elts need not be prime.

Consider $R = \mathbb{Z}[\sqrt{-3}]$. In $R$ 2 is an irreducible elt but not prime elt.

WTS (2) is not a prime ideal.

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 \in (2)$

Note that $(1+\sqrt{-3})(1-\sqrt{-3}) \in (2)$

But neither $(1+\sqrt{-3})$ nor $(1-\sqrt{-3})$ belongs to (2).

$\therefore$ 2 is not a prime elt.

WTS 2 is an irreducible elt.

Let $2 = (a+ib\sqrt{3})(c+id\sqrt{3})$.

Then $2.\bar{2} = (a+ib\sqrt{3})(a-ib\sqrt{3})$
$(c+id\sqrt{3})(c-id\sqrt{3})$

$\Rightarrow 4 = (a^2+3b^2)(c^2+3d^2)$.

$\therefore a^2+3b^2$ must divide 4

and $a^2+3b^2$ cannot be 2.

Hence $a^2+3b^2=4$ and $c^2+3d^2=1$.

$\Downarrow$

$d=0,\ c=\pm 1$.

Thus one of the factor of 2 is a unit namely $\pm 1$. Hence 2 is irreducible.

**Defn.** A unique factorization domain (UFD) is an integral domain $R$ satisfying that

(1) Every elt $0 \neq a \in R$ can be written as a product of irreducible factors $p_1, \ldots, p_n$ upto a unit namely

$$a = u p_1 \cdots p_n$$

(2) The above factorization is unique i.e if

$$a = u p_1 \cdots p_n = v q_1 \cdots q_m$$

are two factorization into irreducible factors $p_i$ & $q_j$ with

units $u, v$ then $n = m$ and $p_i$ and $q_j$ are associates.

**Prop 2.** In an UFD an elt $a$ is irreducible iff $a$ is prime.

**Pf:** Let $a$ be irreducible elt.

WTS $(a)$ is a prime ideal.

Let $bc \in (a)$. Then $bc = ad$ for some $d \in R$. Since $R$ is an UFD we can decompose $b, c$ & $d$ into irreducible factors.

$$a \cdot u d_1 \cdots d_p = v b_1 \cdots b_s \cdot w c_1 \cdots c_t$$

Since the above factorization is unique $a$ must be associate

to some $c_i$ or $d_i$

$\Rightarrow$ $a$ divides $b$ or $c$.

Hence $(a)$ is a prime ideal.

**Prop:** Let $R$ be an int domain and $a, b \in R$. Then

(1) $a$ is an unit in $R$ iff $(a) = R$.

(2) $a$ and $b$ are associate iff $(a) = (b)$.

(3) $a \mid b$ iff $(b) \subseteq (a)$

(4) $a$ is a proper divisor of $b$ iff $(b) \subsetneq (a) \subsetneq R$.

(5) $a$ is irreducible iff $(a)$ is maximal among proper principal ideals.