Ring Theory

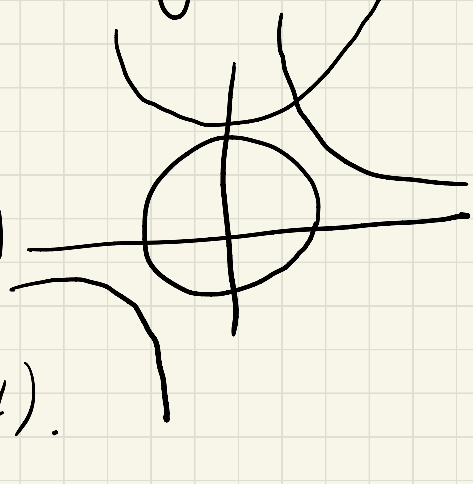
Lecture 22

17/03/2022

Cor. Let $f_1, \dots, f_r$ be polys in $\mathbb{C}[x_1, \dots, x_n]$. This system of eqns $f_1 = 0, f_2 = 0 \dots f_r = 0$ has no soln in $\mathbb{C}^n$ iff

$$(f_1, \dots, f_r) = (1).$$

Example. Consider the ideal gen by $f_1 = x^2 + y^2 - 1$, $f_2 = x^2 - y + 1$, $f_3 = xy - 1$.



Since $Z(f_1, f_2, f_3) = \phi$

thus $(f_1, f_2, f_3) = (1)$.

Grobner basis.

Remark 1: Let R be a ring. Every ideal I of R which is not the unit ideal is contained in a maximal ideal.

Remark 2: The only ring R having no maximal ideal is the zero ring.

$\mathbb{Z} \ni n = p_1 p_2 \cdots p_n$ uniquely.

Unique Factorization Domain:

Let R be an int domain throughout

Defn: We say an elt a divides another elt b $(a \mid b)$ if $b = aq$ for some $q \in R$.

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

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

eg. $\mathbb{R} \rightsquigarrow 6 \rightsquigarrow$ unit. (irreducible).

$\mathbb{Z} \rightsquigarrow 6 = 2 \cdot 3$. (reducible).

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

Defn 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 prime elt then it is irreducible.

Pf: (a) is a prime ideal.

If $a = bc$ then either $b \in (a)$ or $c \in (a)$. WLOG let $b \in (a)$.

then $b = ad$. $\Rightarrow a = adc$

$\Rightarrow dc = 1$.

$\Rightarrow c$ is an unit

Hence a is irreducible.

Q Is every irreducible elt prime?

In $\mathbb{Z}$ the irreducible elts are prime number and so they are prime elts.

In $k[x]$ the irreducible elts are irreducible polys and hence they are prime elts.

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

We see here that irreducible elt need not be prime.

In R consider the elt 2.

<u>WTS</u> 2 is irreducible.

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

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

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

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

$a^2 + 3b^2$ can not be 2.

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

$\Downarrow$

$c = \pm 1$

$d = 0$.

Thus one of the factor of 2 is unit namely ± 1. Hence 2 is irreducible.

<u>WTS</u> 2 is not a prime elt.

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

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

Hence (2) is not a prime ideal.

<u>Defn</u>. A unique factorization domain (UFD) is an int domain R satisfying that

1. Every elt $0 \neq a \in R$ can be written as a product of irreducible factors $p_1, \dots, p_n$ up to 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 associate.

<u>Propn</u>. In a UFD an elt a is irreducible iff a is prime.

<u>Pf</u>: Let a be irreducible

wTS (a) is a prime ideal.

Let $bc \in (a)$

$\Rightarrow$ $bc = ad$ for some $d \in R$.

Since R is an UFD we can decompose b, c & d into irreducibles

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

Since the factorization is unique a must be associate to some c_i or b_i

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

$\Rightarrow$ (a) is a prime ideal.

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

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

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

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

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

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

Defn: An int domain R is called a factorization domain (FD) if every nonzero elt of R can be expressed as product of irreducible elts.