Lec 11/14

Wednesday, November 14, 2018 11:31

Observation: $f(x) \in K[x]$; $\alpha \in K$.

derivative as defined in Calculus

$(x-\alpha)$ divides $f(x) \iff f(\alpha) = 0$.

$(x-\alpha)^N$ divides $f(x) \iff f(\alpha) = f'(\alpha) = \dots = f^{(N-1)}(\alpha) = 0$

A polynomial of degree N cannot have more than N distinct roots.

(we have used this before: $\mathrm{Aut}_{gp}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^\times$ is cyclic)

eg $\overset{f(x)}{\overset{\shortparallel}{x^2 + x + 1}} \in \mathbb{F}_2[x]$ is irreducible since $f(\alpha) = \overset{0}{\overset{\nparallel}{1}}$ for $\alpha = 0, 1$.

Lectures 31-44 will be what's on the midterm.

Polynomial rings in $\overset{1}{\overset{\shortparallel}{\text{many}}}$ variables w/ coefficients from a field, $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

Let $n \in \mathbb{Z}_{\geq 1}$, $R = K[x_1, \dots, x_n]$.

Cor. of Hilbert Basis Theorem: R is Noetherian

i.e. every ideal in R is finitely generated.

$R = (\underbrace{K[x_1, \dots, x_{n-1}]}_{A})[x_n]$. rename it to u. $R = A[u]$. A is Noeth. by ind. hyp.

Hilbert's proof (sketch): Take $I \subsetneq A[u]$.

Step 1. take leading coeffs: $L(I) \subset A$ ideal

$L(I) = (a_1, \dots, a_k)$.

Pick $p_1(u), \dots, p_k(u) \in I$ s.t. $L(p_i(u)) = a_i$.

Prove: modulo $(P_1(u), \ldots, P_k(u))$, we can assume that an element of I has degree $< \mathrm{Max}\{\deg(P_i)\} = D$.

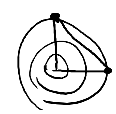
Step 2. Pick finitely many "generators" of $I_{<D} = \{p(u) \in I \mid \deg(p(u)) < D\}$.

Not really Computable/algorithmic.

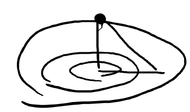
but what's special about x_n? any variable can be used.

Gröbner Basis Theory –

Optimization problems : Maximize $x^2 + y^2$ when $x \geq 0, y \geq 0, x + y \leq 3$.



$x^2 + 2y^2$



In general: Constraints $f_1(x_1, \ldots, x_n) \leq 0$

$f_2(x_1, \ldots, x_n) \leq 0$

$\vdots$

Monomial = polynomial w/ one term. eg $4x_1^2 x_2 x_3^4 \in K[x_1, x_2, x_3]$.

$x_1 + x_2 x_3$ is not a monomial.

Polynomials in $K[x_1, x_2]$ is of the form $\sum_{k_1, k_2 \geq 0}^{\text{finite}} C(k_1, k_2)\, x_1^{k_1} x_2^{k_2}$

Notation: $x_1, \dots, x_n$ just write $\underline{x}$

$\alpha_1, \dots, \alpha_n \in \mathbb{Z}_{\geq 0}$ just write $\underline{\alpha}$

So $\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ [monomial].

Polynomials in $K[x_1, \dots, x_n]$ are of the form

$$\sum_{\underline{\alpha} \in (\mathbb{Z}_{\geq 0})^n}^{\text{finite}} C(\underline{\alpha}) \cdot \underline{x}^{\underline{\alpha}}$$

$$\{ \underline{x}^{\underline{\alpha}} : \underline{\alpha} \in \mathbb{Z}_{\geq 0}^n \}$$
$$\parallel$$

We have to fix an order on the set of monomials.

Such that $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}} \implies \underline{x}^{\underline{\alpha}+\underline{\gamma}} \leq \underline{x}^{\underline{\beta}+\underline{\gamma}}$ for all $\underline{\gamma} \in \mathbb{Z}_{\geq 0}^n$.

Constants are less than everybody, but have no internal order.

eg Lexicographic Ordering (or dictionary ordering):

- pick (arbitrary) ordering on alphabet $\{x_1, \dots, x_n\}$
- ordering on monomials = according to dictionary

eg if $x_1 > x_2 > x_3$ $\quad x_1^{k_1} x_2^{k_2} x_3^{k_3} > x_1^{l_1} x_2^{l_2} x_3^{l_3}$

$\Rightarrow$ $k_1 > l_1$ or $k_1 = l_1$ and $k_2 > l_2$ or $k_1 = l_1$ and $k_2 = l_2$ and $k_3 = l_3$.

$$R = K[x_1, \dots, x_n] \ni f(x_1, \dots, x_n) = \sum_{\underline{\alpha} \in \mathbb{Z}_{\geq 0}^n}^{\text{finite}} C(\underline{\alpha}) \, \underline{x}^{\underline{\alpha}}.$$

Let $\leq$ be monomial order. Let $LT(f)$ = Largest monomial in $f(x_1, \dots, x_n)$.

$LT(f) = C(\underline{\alpha}_0) \, \underline{x}^{\underline{\alpha}_0}$ where $C(\alpha_0) \neq 0$ and $\underset{C(\alpha)}{\cancel{\Uparrow}}\; C(\alpha) \neq 0 \Rightarrow \underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\alpha}_0}$

For $I \subsetneq R$ ideal ; $LT(I) \overset{\text{defn}}{:=}$ ideal generated by $\{LT(f) : f \in I\}$ in R again.

$$\underline{x}^{\alpha} \mid \underline{x}^{\beta} \iff \alpha_i \le \beta_i \quad \forall i.$$

Some examples:

(1) say $n=2$. call our variables x and y.

$$R = K[x,y].$$

$x > y \rightsquigarrow$ Lexicographical monomial ordering.

$f(x,y) = x^2y + xy^3 + 3$ so $LT(f(x,y)) = x^2y$.

(if we started w/ $x<y$, $LT(f(x,y)) = xy^3$).

$I = (f_1, \dots, f_\ell)$. $\quad LT(I) \supseteq (LT(f_1), \dots, LT(f_\ell))$.

not necessarily equal.

If it's equal, $(f_1, \dots, f_\ell)$ is a Gröbner basis.

eg

$$f(x,y) = x^3y - xy^2 + 1$$
$$g(x,y) = x^2y^2 - y^3 - 1$$

$I = (f(x,y), g(x,y)) \subset R$ ideal.

$LT(f(x,y)) = x^3y, \quad LT(g(x,y)) = x^2y^2.$

"monomials"

$\rightsquigarrow (LT(f), LT(g)) \ni h(x,y) \Rightarrow h$ has all terms of degree at least 4

but $x \in LT(I)$ since $yf(x,y) - xg(x,y) = x+y$, $LT(x+y) = x$.

"Initial ideal"