Lecture 51

(51.0) Recall that we discussed (in last lecture) irreducibility of a polynomial (one variable; coefficients from a unique factorization domain). We also made the following observation:

Observation: Let K be a field (e.g. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ ($p \in \mathbb{Z}_{\geq 2}$ prime))

Let $f(x) \in K[x]$, $\alpha \in K$. Then

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

Proof. - ($\Rightarrow$) If $f(x) = (x-\alpha)\cdot g(x)$ then $f(\alpha) = 0 \cdot g(\alpha) = 0$.
(for some $g(x) \in K[x]$)

($\Leftarrow$) Write $f(x) = (x-\alpha)\cdot q(x) + r(x)$ using division, (divide $f(x)$ by $x-\alpha$)
so that degree $(r(x)) <$ degree $(x-\alpha) = 1$.
i.e. $r(x) = r \in K$.

Now $\left.\begin{cases} f(\alpha) = 0 \cdot q(\alpha) + r = r \\ f(\alpha) = 0 \quad \text{(given)} \end{cases}\right\} \Rightarrow f(x) = (x-\alpha)\cdot q(x)$.

[Ex.] Carry out the same argument to prove:

$(x-\alpha)^N$ divides $f(x) \iff f(\alpha) = \underbrace{f'(\alpha) = f''(\alpha) \ldots = f^{(N-1)}(\alpha)}_{\text{derivatives of } f, f', \ldots} = 0$

[Recall $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$

$\Rightarrow f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2a_2 x + a_1$.]

Corollary of Observation : (Again $f(x) \in K[x]$).

$f(x)$ has m distinct roots in $K \Rightarrow m \leq n$.

[side note : we actually proved & used this result in Lecture 21 - see page 4 §21.3 - to conclude that

$$\underset{gp}{\mathrm{Aut}}\,(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^{\times} \text{ is cyclic.} \;]$$

Example. Let $x^2 + x + 1 \in \mathbb{F}_2[x]$. Then $\alpha \in \mathbb{F}_2$ can only be 0 or 1. $f(0) = 1$ and $f(1) = 3 \equiv 1 \pmod 2$ i.e. $\forall\, \alpha \in \mathbb{F}_2$, $f(\alpha) \neq 0$. Thus $f(x)$ cannot be written as a product of <u>two linear factors</u> in $\mathbb{F}_2[x]$; hence it is irreducible.

(51.1) <u>Polynomial rings in many variables - coefficients from a field K</u> (many ≥ 1).

Let $n \geq 1$ and let us consider

$$R = K[x_1, x_2, \ldots, x_n]$$

ring of polynomials in n variables with coefficients from a field K.

Let us quickly review our proof of Hilbert Basis Theorem which implies that R is Noetherian (i.e., every ideal in R is finitely generated).

$$R = K[x_1, \dots, x_n] = \underbrace{\left(K[x_1, \dots, x_{n-1}]\right)}_{\text{call it } A}[x_n]$$

call this variable u for now.

$$R = A[u]$$

$+U$
I ideal $\rightsquigarrow$ ideal in A generated by leading coefficients of $p(u) \in I \subset_{+} A[u]$

say $L(I) \subset A$

Step 1. - Use the fact that A is Noetherian to get

$(a_1, \dots, a_k) = L(I)$ in A

Pick $p_1(u), \dots, p_k(u) \in A[u]$ so that

Leading Coeff. of $p_j(u) = a_j$

Division algorithm $\Rightarrow$ modulo $p_1(u), \dots, p_k(u)$

degree of any $q(u) \in A[u]$

can be brought down to be

(strictly) less than $\operatorname{Max}_{1 \le j \le k} \{\deg(p_j(u))\}$

!! ☺

Step 2 – Pick "generators" of $I_{<D}$ (finitely many)

$$\| \quad \{ p(u) \in I \mid \deg(p(u)) < D \}$$

Note: (1) by writing $u = x_n$ we made a choice: x_n is "better" than $x_1, \dots, x_{n-1}$ (NOT democratic).

(2) Step 2 is not as "algorithmic" as Step 1.

We will fix these issues now.

(51.2) Monomials, orderings and related notation.

Monomial = Polynomial with only one term

(e.g. $x_1^2 x_2 \in K[x_1, x_2]$).

We can write a polynomial in $K[x_1, \dots, x_n]$ as finite sum of monomials

(e.g. typical poly. in $K[x_1, x_2]$ is of the form

$$\sum_{k,\ell \geq 0} c(k,\ell)\, x_1^k x_2^\ell \quad . \ )$$

finite (i.e. $k, \ell \leq N$ for some $N \in \mathbb{Z}_{\geq 0}$)

Convenient short-hand: $\underline{x}$ for $x_1, \dots, x_n$

$\underline{\alpha} = \alpha_1, \dots, \alpha_n$ "exponents" ; $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_{\geq 0}$

$\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$: typical monomial. } in $K[x_1, \dots, x_n]$

$\sum_{\underline{\alpha} \in (\mathbb{Z}_{\geq 0})^n} c(\underline{\alpha})\, \underline{x}^{\underline{\alpha}}$: typical polynomial.

finite sum

Definition: A monomial order is a total order on the set of monomials $\left\{ \underline{x}^{\underline{\alpha}} \mid \underline{\alpha} \in (\mathbb{Z}_{\geq 0})^n \right\}$

s.t. $\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\beta}}$

$\Rightarrow \underline{x}^{\underline{\alpha}+\underline{\gamma}} \leq \underline{x}^{\underline{\beta}+\underline{\gamma}} \quad \forall\ \underline{\gamma} \in (\mathbb{Z}_{\geq 0})^n$

(51.3) For example:

Dictionary order or lexicographic order - we fix an arbitrary ordering on variables, and then decide which monomial is "bigger" according to the following rule (how to look up words in a dictionary!)

$$x_1^{k_1} x_2^{k_2} x_3^{k_3} \geq x_1^{l_1} x_2^{l_2} x_3^{l_3}$$

iff $k_1 > l_1$

or $k_1 = l_1$ and $k_2 > l_2$

or $k_1 = l_1$; $k_2 = l_2$ and $k_3 > l_3$

(to fix ideas - our language has 3 alphabets x_1, x_2, x_3)

$\Vert$ x_1 comes before x_2.
$\Vert$ x_2 comes before x_3.

(our choice - can be changed).

$x_1 > x_2 > x_3$

e.g. $x_1^2 x_2^1 x_3^1 \geq x_1^2 x_2^1 x_3^0$

(51.4) Leading term :- Let us assume we fixed a monomial order for monomials in $K[x_1, \ldots, x_n]$.

For $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$

$\Vert$

$$\sum c(\alpha)\, x^{\alpha}$$

$$LT(f) = c(\alpha_0)\, x^{\alpha_0}$$

where α_0 is such that

- $c(\alpha_0) \neq 0$
- $c(\alpha) \neq 0 \Rightarrow \alpha_0 \geq \alpha$

$LT(f)$ leading term of f

Convention: $LT(0) = 0$

Let $I \subsetneq K[x_1, \ldots, x_n]$ be (an) ideal. Define, similarly

$$LT(I) = \text{ideal in } K[x_1, \ldots, x_n] \text{ generated by}$$

$$\{LT(f) \mid f \in I\}$$

(51.5) Example. Say $n = 2$ and let us just write x & y for our variables. So, $R = K[x, y]$. Let us also choose lexicographic order, with $x > y$.

$$f(x, y) = x^3y - xy^2 + 1 \quad \Rightarrow LT(f) = x^3y$$

$$g(x, y) = x^2y^2 - y^3 - 1 \quad \Rightarrow LT(g) = x^2y^2$$

Catch: $LT(f)$, $LT(g)$ do not generate $LT(I)$ if $I = (f, g) \subset K[x, y]$.

e.g. $x + y = y \cdot f - x \cdot g \in I$

$\Rightarrow LT(I) \ni x$