Lec 9/28

Thursday, September 28, 2017 10:21

Thm $\exists!$ GCD $(f_1, \ldots, f_m)$, $f_1, \ldots, f_m \in F[X]$

Proof $I = \{ \sum_{i=1}^{m} g_i f_i : g_1, \ldots, g_m \in F[X] \}$

$gI = I$ for $g \in F[X]$, (better than subring; ideal)

Let $h \in I$ of least degree.

$f_j = Qh + R$

$\deg R < \deg h$ or $R = 0$. $\deg R \geq \deg h$ since $R = f_j - Qh \in I$

and any other common divisor of $\{f_1, f_2, \ldots, f_m\}$ divides h since h is a combination of the polynomials.

$h' \mid h$ and $h \mid h' \to h = \epsilon_0 h'$ for a unit ϵ_0 and so h is unique.

Cor $\{f_1, \ldots, f_m\}$ are relatively prime $\Leftrightarrow \exists g_1, \ldots, g_m$ s.t. $g_1 f_1 + \cdots + g_n f_m = 1$.

Prop Let $p \in F[X]$ be prime. assume $p \mid fg$. then $p \mid f$ or $p \mid g$.

Proof say $p \nmid f$. Then $1 = kp + lf$. Then $g = kpg + lfg$.

p divides fg so p divides g.

PFThm. Let $f \in F[X]$. Then either f is a unit or $\exists$ a unique (up to units) factorization of $f = p_1 p_2 \cdots p_m$ with $p_1, \ldots, p_m$ prime. If $f = q_1 q_2 \cdots q_s$

then $m = s$ and after reindexing, $p_i \cong q_i$ $\forall i$ ($p_i = \epsilon_i q_i$ for a unit ϵ_i).

Proof: $\exists$: induction on degree of f (easy).

!: Induction on # of primes (easy).

Ex: $f \in F[X]$ $\deg(f) \leq 3$. f is prime $\Leftrightarrow$ f has no roots in F.

Note: $f = X^2 + 1 = (X+1)^2$ in F_2.

$$(X+1)^2 = X^2 + \underbrace{2X}_{= 0X} + 1 = X^2 + 1$$

Proof $\deg f = 1 \Leftrightarrow f$ prime. $\deg f = 2,3$ and f has a root $\xi \Leftrightarrow f = P(X - \xi)$ and is not prime.

(doesn't work for $\deg > 3$: $(X^2+1)^2$

$f = p_1^{k_1} \cdots p_m^{k_m}$ uniquely where $p_i \in F[X]$ prime and $k_i \geq 0$ ($\in \mathbb{Z}$).

$g = p_1^{l_1} \cdots p_m^{l_m}$

$(f, g) = p_1^{\min(l_1, k_1)} \cdots p_m^{\min(l_m, k_m)}$

turn $F(X)$ into a field. (inject it)

$F[X] \hookrightarrow F(X)$ rational

Paralleling $\mathbb{Z} \hookrightarrow \mathbb{Q}$

$(f_1, g_1), (f_2, g_2) \in F[X] \times F[X]$

$(f_1, g_1) \sim (f_2, g_2)$ iff $f_1 g_2 = f_2 g_1$

$\sim$ is an equivalent relation:

(symmetric, reflexive, transitive)