MATH 407

5/7/18

Thm. $f \in F[x]$ has a repeated factor iff $\gcd(f, f') = d$ has $\deg(d) \geq 1$

Pf. $f = a^k b$, $\deg(a) \geq 1$, $k > 1$

$f' = ka^{k-1}a'b + a^k b'$

$= a(ka^{k-1}a'b + a^{k-1}b')$

Suppose $\deg(d) \geq 1$

Let p be an irreducible factor of d.

$f = ap$, some a

$f' = a'p + ap'$

Lemma If p irreducible f any poly $0 \leq \deg(f) < \deg(p)$

$\gcd(f, p) = 1$

$\gcd(p', p) = 1$

$p \mid d \mid f'$ thus $f' = bp$

$bp - a'p = ap'$

$(b - a')p = ap'$

$p \mid ap'$

Thus $p \mid a$, $a = cp$

*If $f(x) = a_0 + a_1 x^1 + \ldots + a_k x^k + \ldots + a_n x^n$

then $f^{(k)}(x) = a_k k!\,(1 + \ldots + a_n x^{n-k})$

$f^k(0) = a_k k!$

$\dfrac{f^k(0)}{k!} = a_k$

(2)

$$= \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} (x-0)^k$$

$$f(x) = \sum_{k=0}^{n} a_k (x-c)^k = \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!} (x-c)^k$$

* Modular Arithmetic for $F[x]$ (mod f)

$a(x) \equiv b(x) \pmod f$ iff $f \mid (a-b)$

iff $a-b \equiv 0 \pmod f$

iff when $a = fq_a + r_a$, $b = fq_b + r_b$,

$\deg(r_a) < \deg(f)$

$\deg(r_b) < \deg(f)$

$r_a = r_b$

* $\equiv \pmod f$ is an equivalence relation

$$[a]_f = \{b : a \equiv b \pmod f\}$$

$$[0]_f = [f]_f = \langle f \rangle = fF[x]$$

$$[a]_f [b]_f = [ab]_f$$

$$[a]_f = [r_a]_f, \ \deg(r_a) < \deg(f)$$

$$r_a - \hat{r}_a = 0$$

Each equivalent class has one polynomial of deg $< f$

* For any $\lambda \in F$

$$[\lambda a]_f = \lambda [a]_f$$
$$= \{\lambda b : a \equiv b \pmod f\}$$

$\lambda \in F[x]$

<u>Thm.</u> $F[x]/\langle f\rangle$ vector space over F w/ basis $\{[1], [x], [x^2], \ldots, [x^{k-1}]\}$, $\deg(f) = k$.

Note: $F[x]/\langle f\rangle = \{[a]_f : a \in F[x]\}$

If $g(x) = b_0 + b_1 x^1 + \ldots + b_{k-1} x^{k-1}$

$$[g]_f = [b_0] + [b_1 x^1] + \ldots + [b_{k-1} x^{k-1}]$$
$$= b_0[1] + b_1[x] + \ldots + b_{k-1}[x^{k-1}]$$
$$\overset{?}{=} [c_0] + [c_1 x^1] + \ldots + [c_{k-1} x^{k-1}]$$

No, because

$$\Rightarrow [c_0 + c_1 x^1 + \ldots + c_{k-1} x^{k-1}]$$
$$\Rightarrow (b_0 - c_0) + (b_1 - c_1) x + \ldots + (b_{k-1} - c_{k-1}) x^{k-1} \equiv 0 \pmod f$$

$b_i - c_i = 0 \ \forall i$

Look at $a_0 + a_1 x^1 + \ldots + a_k x^k = f$, $f \equiv 0 \pmod f$

$$\Rightarrow a_0 + a_1 x^1 + \ldots + a_k x^k \equiv 0 \pmod f$$

1) if $a_0 = 0$, $x(a_1 + a_2 x^1 + \ldots + a_k x^{k-1}) \equiv 0 \pmod f$

$$[x][a_1 + \ldots + a_k x^{k-1}] = 0$$

(4)

$$-a_0 = a_1 x^1 + \dots + a_k x^k$$

$$1 = -x\left(\frac{a_1}{a_0} + \dots + \frac{a_k}{a_0} x^{k-1}\right)$$

$$[1]_f = [x]_f \left[-\frac{a_1}{a_0} - \dots - \frac{a_k}{a_0} x^{k-1}\right]_f$$