Lecture 16: Multiple roots and separable polynomials.

$f(x) \in F[x]$ monic. Over the splitting field of f,

have $f(x) = (x-\alpha_1)^{k_1} \cdots (x-\alpha_n)^{k_n}$ ← multiplicities

with α_i distinct. If $k_i = 1$, call α_i a <u>simple root</u>; otherwise α_i is a <u>multiple root</u>.

$f(x)$ is <u>separable</u> if all roots are simple

<u>Ex</u>: x^2-1, x^2+1 in $\mathbb{Q}[x]$

<u>Non ex</u>: ① $x^2+2x+1 = (x+1)^2$ in $\mathbb{Q}[x]$

② $x^2+t \in \underbrace{\mathbb{F}_2(t)}_{\text{field of rat'l fns.}}[x]$

ⓐ Irreducible by Eisenstein with ideal (t).

ⓑ Let α be a root in the splitting field, so $\alpha^2 = t$

Then $(x-\alpha)^2 = x^2 - 2\alpha x + t = x^2+t$

So α is a multiple root.

Thm: If F has char 0 or F is finite, then every irreducible $f \in F[x]$ is separable.

[Will show char 0 part today, finite case next time. First a basic tool...]

For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $F[x]$, define

$$f'(x) = n \cdot a_n x^n + (n-1) a_{n-1} x^{n-1} + \cdots + a_1$$

[This derivative is also in $F[x]$, but is "formal" as notions of limit used to define the derivative in calculus may make no sense here. Has the usual props:

$$(f+g)' = f' + g' \quad \text{and} \quad (fg)' = f'g + fg'$$

Lemma 1: A root α of $f(x)$ is a mult. root iff $f'(\alpha) = 0$.

Lemma 2: $f(x) \in F[x]$ is separable iff $\gcd(f(x), f'(x)) = 1$ in $F[x]$.

Ex: ① $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$. $f'(x) = 2x \Rightarrow$ separable

② $f(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$. $f'(x) = 2x + 2 = 2(x+1)$

$$\Rightarrow \gcd(f, f') = x + 1.$$

(3) $f(x) = x^2 + t$ in $\mathbb{F}_2(t)[x]$ $\quad f'(x) = 2x = 0.$

($\Rightarrow$ $\gcd = x^2+t$!)

Pf of Lemma 1: Consider $g(x) = f(x-\alpha)$. Then a mechanical check gives $g'(x) = f'(x-\alpha)$. So have reduced to case $\alpha = 0$. Then

$g(x) = x^k h(x)$ where $k > 0$ and $h(x)$ has non-zero constant term

Then

$$g'(x) = \underset{\substack{\uparrow \\ \text{nonzero at } x=0}}{k x^{k-1} h(x)} + \underbrace{x^k h'(x)}_{0 \text{ at } x=0}$$

Thus

$$g'(0) = \begin{cases} 0 & k > 0 \quad (\Rightarrow \text{multiple root}) \\ h(0) & k = 1 \quad (\Rightarrow \text{simple root}). \end{cases}$$

$\square$

Pf of Lemma 2: Will show for $p, q \in F[x]$ have

$\gcd(p,q) = 1 \iff p, q$ have no common roots in an ext K/F where both split completely.

Case p, q have a common root α. Then p and q are both divisible by $m_{\alpha,F}(x) \Rightarrow \gcd(p,q) \neq 1$.

Case no common root. If $\gcd(p,q) = r(x)$ nonconst, then any root of $r(x)$ is a common root of p and q. $\square$

<u>Thm</u>: If $\mathrm{char}(F) = 0$, then every irreducible $f(x) \in F[x]$ is separable.

<u>Pf</u>: $n = \deg f(x) \geq 2$. Then $\deg f' = n-1$. As $f(x)$ is irreducible, only divisors are $f(x)$ and 1.

Hence $\gcd(f(x), f'(x)) = 1$. $\square$

<u>Q</u>: Where did I use $\mathrm{char}(F) = 0$?

<u>A</u>: To show $\deg f' = n-1$. In char p, can have $f' = 0$, as did in the case $X^2 + t$ above. Another example is $f = X^p + 1$ in $\mathbb{F}_p[x]$. [Thm on sep still holds for F finite]

<u>Frobenius map</u>: F a field of char p.

$$\varphi : F \to F \quad \text{by} \quad \varphi(a) = a^p$$

<u>Key</u>: φ is a 1-1 homomorphism of fields.

<u>Check</u>:
$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$
$$\varphi(a+b) = (a+b)^p = a^p + pa^{p-1}b + \cdots + pab^{p-1} + b^p$$
$$= a^p + b^p = \varphi(a) + \varphi(b)$$

φ is 1-1 as $\varphi(1) = 1$ and hence φ is nontrivial.

<u>Cor</u>: If F is finite, then φ is an isomorphism

<u>Pf</u>: A 1-1 map of a finite set to itself is onto. $\square$

<u>Contrast</u>: φ is not onto for $\mathbb{F}_p(t)$. What is an elt not in the image? <u>Ans</u>: t

<u>Thm</u>: F finite. Every irreducible f in $F[x]$ is separable.

<u>Pf</u>. Suppose f has a repeat root $\Rightarrow f'(x) = 0 \Rightarrow$

$$f(x) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0$$

$$= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p$$

b_i exist as Frob is onto.

$$= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)^p$$

$\square$

$\Rightarrow f$ is reducible.