Lecture 16: Multiple roots and separable polynomials.

\[ f(x) \in F[x] \text{ monic. Over the splitting field of } f, \]
\[ \text{have } f(x) = (x - \alpha_1)^{k_1} \cdots (x - \alpha_n)^{k_n} \text{ } \leftarrow \text{multiplicities} \]
\[ \text{with } \alpha_i \text{ distinct. If } k_i = 1, \text{ call } \alpha_i \text{ a simple root; otherwise } \alpha_i \text{ is a multiple root.} \]

\[ f(x) \text{ is separable if all roots are simple} \]

Ex: \( x^2 - 1, \ x^2 + 1 \text{ in } \mathbb{Q}[x] \)

Non ex: \( x^2 + 2x + 1 = (x + 1)^2 \text{ in } \mathbb{Q}[x] \)

2. \( x^2 + t \in \mathbb{F}_2[t][x] \)
   \[ \text{field of nat'l fs.} \]
   \[ \text{a) Irreducible by Eisenstein with ideal } (t). \]

b) let \( \alpha \) 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 \( \alpha \) 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 $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ in $F[x]$, define

$$f'(x) = n \cdot a_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$$

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

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

$\Rightarrow \gcd(f, f') = x + 1$. 
\( f(x) = x^2 + t \) in \( F_2(t)[x] \)  \( f'(x) = 2x = 0. \)  \( (\Rightarrow \gcd = x^2 + t !) \)

**Proof 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
\[
g(x) = x^k h(x) \text{ where } k > 0 \text{ and } h(x) \text{ has non-zero constant term}
\]
Then
\[
g'(x) = k x^{k-1} h(x) + x^k h'(x)
\]
Thus \( g'(0) = \begin{cases} 0 & k > 0 \ (\Rightarrow \text{multiple root}) \\ h(0) & k = 1 \ (\Rightarrow \text{simple root}) \end{cases} \)

**Proof Lemma 2:** We will show for \( p, q \in F[x] \) have
\[
\gcd(p, q) = 1 \iff p, q \text{ have no common roots in an ext } K/F \text{ where both split completely.}
\]
Case \( p, q \) have a common root \( \alpha \). 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 \( q \). \( \square \)
Thm: If \( \text{char}(F) = 0 \), then every irreducible \( f(x) \in F[x] \) is separable.

**Pf:** \( n = \deg f(x) \geq 2 \). Then \( \deg f' = n - 1 \). As \( f(x) \) is irreducible, only divisors are \( f(x) \) and \( 1 \). Hence \( \gcd(f(x), f'(x)) = 1 \). \( \square \)

Q: Where did I use \( \text{char}(F) = 0 \)?

A: To show \( \deg f' = n - 1 \). In \( \text{char} p \), can have \( f' = 0 \), as did in the case \( x^2 + t \) above. Another example is \( f = x^{p+1} \) in \( F_p[x] \). [Thm on sep still holds for \( F \) finite]

**Frobenius map:** \( F \) a field of \( \text{char} p \).

\[ \sigma : F \to F \text{ by } \sigma(a) = a^p \]

Key: \( \sigma \) is a 1-1 homomorphism of fields.

Check: \( \sigma(ab) = (ab)^p = a^p b^p = \sigma(a) \sigma(b) \)

\[ \sigma(a + b) = (a + b)^p = a^p + p a^{p-1} b + \ldots + p a b^{p-1} + b^p = a^p + b^p = \sigma(a) + \sigma(b) \]
$\phi$ is $1$-$1$ as $\phi(1) = 1$ and hence $\phi$ is nontrivial.

**Cor.** If $F$ is finite, then $\phi$ is an isomorphism.

**Pf.** A $1$-$1$ map of a finite set to itself is onto. \( \square \)

**Contrast:** $\phi$ is not onto for $\mathbb{F}_p(t)$. What is an elt not in the image? \textit{Ans.:} $t$

**Thm.** $F$ finite. Every irreducible $f$ in $F[x]$ is separable.

**Pf.** Suppose $f$ has a repeat root $\Rightarrow f'(x) = 0 \Rightarrow$

$$f(x) = a_n x^{p^n} + a_{n-1} x^{p^{n-1}} + \ldots + a_1 x^p + a_0 \quad \text{b; exist}$$

$$= b_n x^{p^n} + b_{n-1} x^{p^{n-1}} + \ldots + b_1 x^p + b_0 \quad \text{as Frob}$$

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

$\Rightarrow f$ is reducible. \( \square \)