Lecture 16: Separable Extensions

Def: \( f(x) \in F[x] \) separable if its roots in some splitting field are simple, i.e. no multiple roots.

Lemma: \( f(x) \) is separable iff it has no common root with \( f'(x) \) iff \( \gcd(f(x), f'(x)) = 1 \).

Then: If char \((F) = 0\), then any irreducible \( f(x) \in F[x] \) is separable.

Proof: \( n = \deg f > 2 \). Then \( \deg f' = n-1 \). As \( f(x) \) is irreducible, only factors are \( f(x) \) and \( 1 \). Thus \( \gcd(f(x), f'(x)) = 1 \).

Q: Where did cl use that char \((F) = 0\)?

A: To show \( \deg f' = n-1 \). With char \( p \), degree can drop more, all the way to \( f' = 0 \), in which case \( \gcd(f, f') = f \).

\[ \text{Ex: } f = x^p + 1 \text{ in } F_p[x] \]
\[ f' = px^{p-1} = 0. \]

Then still holds for \( F \) finite, as well now see...
Frobenius map: $F$ a field of char $p$.

$p: F \rightarrow F$ by $p(a) = a^p$

Key: $p$ is a 1-1 homomorphism of fields.

Check: $p(ab) = (ab)^p = a^p b^p$

$p(a+b) = (a+b)^p = a^p + b^p = p(a) + p(b)$

Cor: if $F$ is finite, then $p$ is an isomorphism.

Pf: A 1-1 map of a finite set to itself is onto.

Contrast: $p$ is not onto for $F_p(t)$.

Q: What is an elt not in the image? A. t

Thm: $F$ finite. Then every irreducible $f \in F[x]$ is separable.

Proof: Suppose $f(x)$ is inseparable.
Then \( f'(x) = 0 \Rightarrow \) all terms of the form \( x^n \) with \( p \nmid n \).

So \( \exists g(x) \in F[x] \) with \( f(x) = g(x^p) \).

Then
\[
f(x) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \ldots + a_1 x^p + a_0 \]
\[
= b_n x^{pn} + b_{n-1} x^{p(n-1)} + \ldots + b_1 x^p + b_0
\]
for some \( b_i \in F \) since the Frobenius map is onto.

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

And so \( f \) is reducible.

\[\text{Def: A field is perfect if}
\begin{align*}
(\&) & \quad \text{char} = 0 \\
(\&\&) & \quad \text{char} = p \text{ and } x \mapsto x^p \text{ is an isom.}
\end{align*}\]

\[\text{Thm: If } F \text{ perfect, then every indep. poly is separable.}\]
Finite fields:

Basic: \( F_p = \mathbb{Z}/p\mathbb{Z} \)

Others: \( x^2 + x + 1 \) is irreducible in \( \mathbb{F}_2[x] \).

\[ F = \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)} \]

Then as an \( \mathbb{F}_2 \)-vector space, \( F \cong \mathbb{F}_2^2 \), \( \mathbb{F}_2^2 \)

\( \Rightarrow |F| = 4 \).

Thm: \( p \) prime, \( m \geq 1 \). Then \( \exists \) unique finite

field \( \mathbb{F}_{p^m} \) with \( p^m \) elts.

Q: How many have seen this?

Construction: Let \( K = \) splitting field of

\( f(x) = x^{p^n} - x \) over \( \mathbb{F}_p \)

\( \text{separable as } f' = -1 \).

Set \( S = \{ \text{all roots of } f(x) \text{ in } K \} \)
Notes:
1. \( \mathbb{F}_p \subseteq S \).
2. \( S \) is a subring
   * \( a, b \in S \) then \( a^p = a \), \( b^p = b \)
   So \( f(ab) = a^p b^p = a \cdot b = 0 \).
   and \( f(a+b) = (a+b)^p = a+b \)
   \( = (a^p + b^p) - a - b = 0 \).

\( \Rightarrow S \) is a field (by old argument or since \( S \) is finite).
\( \Rightarrow S = K \) and \( |K| = p^n \).

Uniqueness: Suppose \( K/\mathbb{F}_p \) with \( p^n \) elts.
Then \( (K \setminus \{0\}, \times) \) is a group of order \( p^n - 1 \).
\( \Rightarrow \forall a \neq 0 \text{ in } K \text{ that } a^{p^n-1} = 1 \iff a^p - a = 0 \).
Thus \( K \) is a splitting field for \( x^{p^n} - x \) as well.