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

Thm: If $\text{char}(F) = 0$, then any irreducible $f(x) \in F[x]$ is separable.

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

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

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

Ex: $f = x^p + 1$ in $\mathbb{F}_p[x]$

$f' = px^{p-1} = 0$.

[Thm still holds for F finite, as we'll now see...]

Frobenius map: F a field of char p.

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

Key: φ is a 1-1 homomorphism of fields.

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

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

Cor: If F is finite, then φ is an isomorphism.

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

Contrast: φ is not onto for $\mathbb{F}_p(t)$.

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 $p \mid n$.

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

Then

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

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

for some $b_i \in F$ since the Frob. map is onto.

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

And so f is reducible. ▨

Def: A field is perfect if

(a) $\mathrm{Char} = 0$

(b) $\mathrm{Char} = p$ and $x \mapsto x^p$ is an isom.

} $\mathbb{Q}, \mathbb{R}, \mathbb{F}_p$

Thm: F perfect, then every irred. poly is separable.

Finite fields:

Basic: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Others: x^2+x+1 is irred in $\mathbb{F}_2[x]$.

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

Then as an $\mathbb{F}_2$-vector space, $F \cong \mathbb{F}_2^{[F:\mathbb{F}_2]} = \mathbb{F}_2^2$

$\Rightarrow |F| = 4.$

Thm: p prime, $n \geq 1$. Then $\exists$ a unique finite field $\mathbb{F}_{p^n}$ with p^n elts.

[Q: How many have seen this?]

Construction: Let K = splitting field of $f(x) = \underbrace{x^{p^n} - x}$ over $\mathbb{F}_p$

separable as $f' = -1$.

Set $S = \{$all roots of $f(x)$ in $K\}$

Notes: ① $\mathbb{F}_p \subseteq S$.

② S is a subring

- $a, b \in S$ then $a^{p^n} = a \quad b^{p^n} = b$

So $f(ab) = a^{p^n} b^{p^n} - ab = ab - ab = 0$.

and
$$f(a+b) = (a+b)^{p^n} - a - b$$
$$= (a^{p^n} + b^{p^n}) - a - b = 0.$$

$\Rightarrow$ 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 $p^n - 1$.

$\Rightarrow \forall a \neq 0$ in K that $a^{p^n - 1} = \underline{1} \Leftrightarrow a^{p^n} - a = 0$.

Thus K is a splitting field for $x^{p^n} - x$ as well.

$\blacksquare$