Lecture 24

<u>defn.</u> K is <u>separable</u> over F if for every $\alpha \in K$, $m_{\alpha,F}(x)$ is separable.

Otherwise, K/F is inseparable.

How to check whether a polynomial has multiple roots.

<u>defn.</u> If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$.

the <u>derivative</u> of $f(x)$ is

$$D_x f(x) = n a_n x^{n-1} + \dots + 2a_2 x + a_1$$

⚠ Entirely formal! But satisfies all the usual properties

- linearity $D_x(f+g) = D_x f + D_x g$
- Leibniz rule $D_x(fg) = f(D_x g) + (D_x f) g$.

<u>Prop.</u> A polynomial $f(x)$ has a multiple root α <u>iff</u> α is also a root of $D_x f(x)$.

↳ ie. $m_{\alpha,F}(x) \mid$ both $f(x)$ and $D_x f(x)$

↳ ie $f(x)$ is separable <u>iff</u> $\gcd(f(x), D_x f(x)) = 1$

<u>note</u> we are working in a ED.

Pf.

$\boxed{\Longrightarrow}$ Suppose α is a multiple root of $f(x)$.

Then over some splitting field,

$$f(x) = (x-\alpha)^n g(x) \quad \text{where } n \geq 2.$$

Then

$$D_x f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x)$$

$\Rightarrow \alpha$ is also a root of $D_x f(x)$ $\quad (x-\alpha) \mid D_x f(x)$.

$\boxed{\Leftarrow}$ Suppose $f(x)$ and $D_x f(x)$ have α has a root.

Then $f(x) = (x-\alpha)\, h(x)$ (over a splitting field)

$$D_x f(x) = h(x) + (x-\alpha) D_x h(x)$$

$\Rightarrow (x-\alpha) \mid h(x) \Rightarrow h(x) = (x-\alpha) = h_1(x).$

$\Rightarrow f(x) = (x-\alpha)^2 h_1(x) \Rightarrow \alpha$ is a multiple root.

Rmk. gcd condition: Let α be a root of a common factor of $f(x)$ and $D_x f(x) \rightsquigarrow f(x)$ is inseparable.

eg. $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

$D_x f(x) = p^n x^{p^n - 1} - 1 = -1$. No roots!

$\Rightarrow f(x)$ is separable

$\Bigg\}$ will see again later.

Cor. Every irred. polyn over a field of char 0 is separable.

Pf. If $f(x)$ has degree n, then $D_x f(x)$ has degree $n-1$.

$f(x)$ irred $\Rightarrow$ only factors (up to a constant) are 1 and $f(x)$.

But clearly $f(x) \nmid D_x f(x)$

//

Observation Now consider F with char $F = p > 0$, and let $f(x) \in F[x]$ be monic irreducible. $\Rightarrow$ for any root β of $f(x)$, $m_{\beta,F}(x) = f(x)$

If f is inseparable, ie has a multiple root α, then

$f(x) = m_{\alpha,F}(x) \mid D_x f(x) \quad \Rightarrow D_x f(x) = 0.$

$\Rightarrow$ all powers of x in $f(x)$ are powers of x^p

ie. $f(x) = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \dots + a_1 x^p + a_0$

The Frobenius Endomorphism $\qquad \varphi(a) = a^p$

prop. Let F be a field of char p. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p \qquad \text{and} \qquad (ab)^p = a^p b^p.$$

In other words, $\varphi(a) = a^p$ is an injective field hom. $F \to F$

(because $\ker \varphi \neq 0$)

Pf. Binomial Theorem:

$$(a+b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1}}_{\text{all these coefficients are divisible by } p.} + b^p$$

$\blacksquare$

defn. Let F be a field of characteristic p.

$\varphi : F \to F$, $a \mapsto a^p$ is called the <u>Frobenius endomorphism</u> of F.

Cor. Let $\mathbb{F}$ be a <u>finite</u> field of characteristic p.

Then every element of $\mathbb{F}$ is a p^{th} power: $\mathbb{F} = \mathbb{F}^p$.

Pf. φ is injective $\Rightarrow$ surjective. //

- Why was the first example we saw of an inseparable extension over such a big field $\mathbb{F}_2(t)$?

prop. Every irred. polynomial over a finite field $\mathbb{F}$ is separable.

$\Rightarrow$ positive characteristic

$\hookrightarrow$ Rmk. And in general, a polyn in $F[x]$ is separable iff it's the product of distinct irreducibles (clear)

$\hookrightarrow$ distinct irred don't have roots in common b/c minimal polynomials are unique.

pf.

Let $\mathbb{F}$ be a finite field. Let $p = \text{char}\, \mathbb{F}$.

BWOC, suppose $f(x) \in \mathbb{F}[x]$ is an irreducible inseparable polyn.

From Observation, f irred, insep $\Rightarrow f(x) = g(x^p)$

$= a_m (x^p)^m + a_{m-1}(x^p)^{m-1} + \dots + a_1 (x^p) + a_0$

and these coeffs are also pth powers, so we can write

$= b_m^p (x^p)^m + b_{m-1}^p (x^p)^{m-1} + \dots + b_1^p (x^p) + b_0^p$

$= (b_m x^m + b_{m-1} x^m + \dots + b_1 x + b_0)^p$

contradicting the assumption that $f(x)$ was irreducible. ☒

defn. (Perfect fields) $\boxed{\text{perfect} \Longrightarrow \text{separable.}}$

- Fields of char p where every element $\alpha \in K$ is a pth power, ie $\alpha = \beta^p$ for some $\beta \in K$ are called perfect fields.
  - eg. finite fields of char p.
- char 0 fields are also perfect

eg. infinite, char p, perfect : $\overline{\mathbb{F}_p}$

Finite Fields

Let $n \in \mathbb{N}$. Consider $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

- $f(x)$ is separable: $D_x f(x) = p^n x^{(p^n-1)} - 1 = -1$

  $\Rightarrow$ has p^n distinct roots

- Let α, β be two roots of $f(x)$. $\Rightarrow \alpha^{p^n} = \alpha, \ \beta^{p^n} = \beta$

  Claim: The set of roots forms a field

  - $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$
  - $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$
  - $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$

  $\Rightarrow$ This is the splitting field K of $f(x)$.

  This has p^n elements $\Rightarrow [K : \mathbb{F}_p] = n$.

- Now let $\mathbb{F}$ be a finite field of characteristic p.

  If $[\mathbb{F} : \mathbb{F}_p] = n$, then $|\mathbb{F}| = p^n$. * Only orders of finite fields is p^n.

  prime subfield

  Since $|\mathbb{F}^\times| = p^n - 1$, $\forall \alpha \in \mathbb{F}^\times$, $\alpha^{p^n-1} = 1 \Rightarrow \alpha^{p^n} = \alpha$.

  $\Rightarrow \mathbb{F} \cong$ splitting field of $x^{p^n} - x$.

$\Rightarrow$ Finite fields of order p^n exist and are unique up to $\cong$.

Lemma. $\mathbb{F}_{p^n}^\times$ is actually cyclic:

Let $m = \operatorname{lcm}\{|\alpha| : 0 \neq \alpha \in \mathbb{F}_{p^n}^\times\}$ $(\leq p^n - 1)$

Then $\exists \beta \in \mathbb{F}_{p^n}^\times$ s.t. $|\beta| = m$ (gp thy - take product of elements w/ coprime order)

$\Rightarrow \forall \alpha \neq 0$, $\underbrace{\alpha^m = 1}$

The equation $x^m = 1$ has at most m distinct roots. $\Rightarrow m \geq p^n - 1$.

$\Rightarrow m = p^n - 1. \Rightarrow \mathbb{F}_{p^n}^\times = \langle \beta \rangle$.