My OH this week will be canceled

Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

Remember that K/F is separable if $\forall \alpha \in K$,

$m_{\alpha,F}$ is separable

↳ a polynomial is separable if its roots are distinct.

If f is reducible, f can "easily" be inseparable

e.g. $f(x) = (x-2)^2$

repeated factor ⟶ repeated root.

So the polynomials that can be inseparable in a non-silly way are the irreducible polynomials,

This is all in D&F Section 13.5

Recall: Proposition 33:

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

Are there irreducible and inseparable polynomials?

Yes.

Let f be irreducible and inseparable / F

Then $\gcd(f, f') \neq 1$

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

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

this is a polynomial of degree $< n$

f' is of degree $n-1$ iff $n \neq 0$ in F.

Since f is irreducible, for any polynomial

$$\gcd(f, p) = 1 \text{ or } f$$

If $\gcd(f, f') \neq 1$, then $\gcd(f, f') = f$

$\Rightarrow f \mid f'$ but $\deg f' < \deg f$.

The only time a polynomial of higher divides a polynomial of lower degree is if the lower-degree polynomial is 0.

0 is divisible by everything: $0 = f \cdot 0$

Note that if $f' \neq 0$ and f is irreducible then

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

So the only irreducible inseparable polynomials have derivative equal to 0.

$$f'(x) = \boxed{na_n} x^{n-1} + \boxed{(n-1)a_{n-1}} x^{n-2} + \dots + \boxed{a_1}$$

all have to be zero

The only this can happen is:

If $f(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + \dots + a_0$

then $a_k \neq 0 \Rightarrow k = 0$ in F

$\Rightarrow \mathrm{char}(F) = p$ prime and $p \mid k$

Example $f(x) = x^2 - t \in \mathbb{F}_2(t)[x]$ nonconstant polynomial

$f'(x) = 2x = 0$ zero derivative.

If $f \in F[x]$ is irreducible and inseparable then

- $\text{char}(F) = p \neq 0$
- $f(x) = \sum_{k=0}^{n} a_{pk} x^{pk} = a_{np} x^{np} + a_{(n-1)p} x^{(n-1)p} + \dots + a_0$

Corollary: If K/F is inseparable and finite, then $\text{char}(F) = p$ and $p \mid [K:F]$

proof: If $K|F$ is inseparable then $\exists\, \alpha \in K$ with $m_{\alpha,F}$ inseparable and irreducible so $p \mid \deg m_{\alpha,F}$

```tikzcd
 & K \arrow[dl, dash] \arrow[d, dash] \\
F(\alpha) \arrow[r, dash] & F
```

$$[K:F] = [K:F(\alpha)]\,[F(\alpha):F]$$

Note: If $\operatorname{char} F = p$ and $p \mid [K:F]$ it does not mean that $K|F$ is inseparable

Going back: f irred + insep.

$$f(x) = a_{np}x^{np} + \dots + a_p x^p + a_0$$

$$= a_{np}(x^p)^n + \dots + a_p(x^p) + a_0$$

$$= f_1(x^p)$$

look at f_1 if separable, done

if inseparable $f_1 = b_{mp}x^{mp} + \dots + b_1 x^p + b_0$

$f(x) = f_1(x^p)$

$= f_2(x^{p^2})$

$f_1(x) = f_2(x^p)$

If f_2 is separable, done if not, repeat. and so on,

Proposition 38

Let f be irred over F, char$(F)=p$, then $\exists$ a unique integer k and a sep poly f_{sep} with

$$f(x) = f_{sep}(x^{p^k})$$

Example $f(x) = x^2 - t$ $F = \mathbb{F}_2(t)$ $p=2$

$f_1(x) = x - t$ separable (unique root t)

$$f(x) = f_1(x^2)$$

Example 2 $f(x) = x^6 + x^2 + t$

$f_1(x) = x^3 + x + t$ separable

$f(x) = f_1(x^2)$ $f_1'(x) = 3x^2 + 1 \neq 0$

Example: $f_2(x) = x^3 + x + t$

$$\boxed{f(x) = x^{12} + x^4 + t} = (x^2)^6 + (x^2)^2 + t$$

$$f(x) = f_2(x^4)$$

still inseparable

$$f_1(x) = x^6 + x^2 + t$$
$$= (x^2)^3 + (x^2) + t$$

$$f_2(x) = x^3 + x + t$$

HW

$f(x) = x^4 + 2x^2 + 5$

$y = x^2 \quad y^2 + 2y + 5$

$x = \pm\sqrt{y}$

K
$|$
$F(y)$
$|$
F

Corollary: Every splitting field K/F can be written as

$$\begin{array}{c} K \\ | \\ K^{sep} \\ | \\ F \end{array}$$

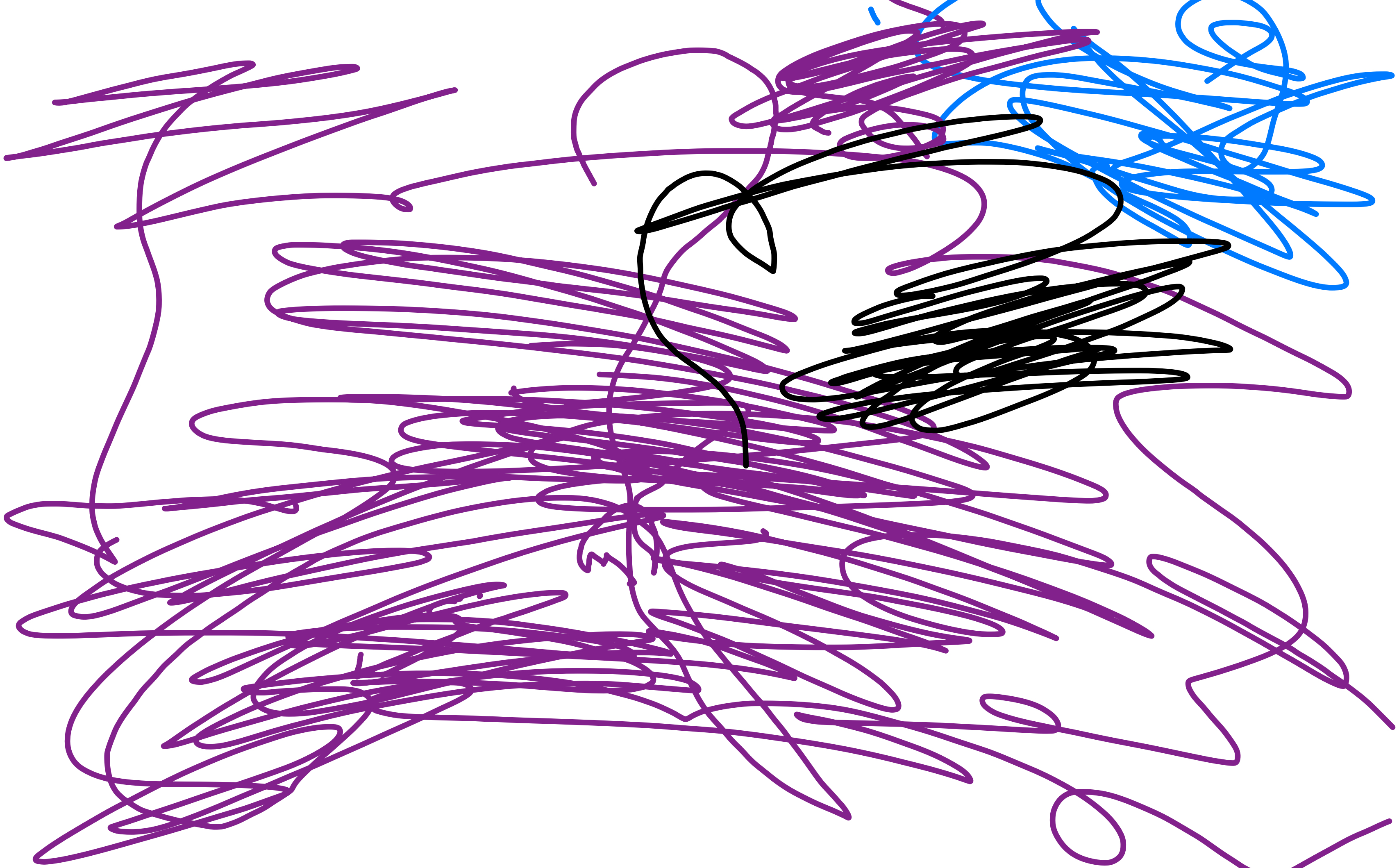
$K = K^{sep}(\alpha^{1/p^k})$

separable

splitting field of f_{sep}

$f(x) = f_{sep}(x^{p^k})$

$$\deg f = \underbrace{\deg_i f}_{= p^k} \cdot \underbrace{\deg_s f}_{= \deg f_{sep}}$$



No classes on Wednesday!

That's all for today!