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.

Section 13.5: Separable + inseparable extensions

K/F (alg) is separable if $\forall \alpha \in K$ $m_{\alpha,F}$ is separable

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

super weird + hard

then $\text{char}(F) = p \neq 0$

and $f'(x) = 0$ ($\deg f' < \deg f$ but also $f \mid f'$)

$\Downarrow$ every exponent appearing in f is divisible by p.

Example $f(x) = x^{64} + x^{24} + x^{16} + 1 \in F[x]$ char$(F) = 2$

assume irreducible

$$f'(x) = \underbrace{64}_{=0} x^{63} + \underbrace{24}_{=0} x^{23} + \underbrace{16}_{=0} x^{15} = 0$$

in F

$$f(x) = f_1(x^2) = (x^2)^{32} + (x^2)^{12} + (x^2)^8 + 1$$

$f_1(x) = x^{32} + x^{12} + x^8 + 1$ $\quad f_1'(x) = 0$ insep

$$= f_2(x^2) = (x^2)^{16} + (x^2)^6 + (x^2)^4 + 1$$

$f_2(x) = x^{16} + x^6 + x^4 + 1$ $\quad f_2'(x) = 0$ insep

$$f(x) = f_1(x^2) = (x^2)^{32} + (x^2)^{12} + (x^2)^8 + 1$$

$$f_1(x) = x^{32} + x^{12} + x^8 + 1 \qquad f_1'(x) = 0 \quad \text{insep}$$

$$= f_2(x^2) = (x^2)^{16} + (x^2)^6 + (x^2)^4 + 1$$

$$f_2(x) = x^{16} + x^6 + x^4 + 1 \qquad f_2'(x) = 0 \quad \text{insep}$$

$$f_2(x) = f_3(x^2) = (x^2)^8 + (x^2)^3 + (x^2)^2 + 1$$

$$f_3(x) = x^8 + x^3 + x^2 + 1 \qquad f_3'(x) = x^2 \quad \text{sep}$$

$$f(x) = f_3(x^8) = f_3(x^{2^3})$$

If f is irreducible and inseparable, $f \in F[x]$, $\text{char}(F) = p \neq 0$, there exists k a positive integer

unique such that

f_{sep} separable polynomial with

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

is separable

Changing gears for a minute

Let F be a field with $\mathrm{char}(F) = p \neq 0$.

then $\sigma_p : F \to F$, $\alpha \mapsto \alpha^p$ is a field homomorphism

respect $+$ and $\times$

if $\mathrm{char}(F) = p$ then $(\alpha+\beta)^p = \alpha^p + \beta^p$ $\quad \sigma_p(\alpha+\beta) = \sigma_p(\alpha) + \sigma_p(\beta)$

$(\alpha\beta)^p = \alpha^p \beta^p$ $\quad \sigma_p(\alpha\beta) = \sigma_p(\alpha)\sigma_p(\beta)$.

In fact σ_p is always (if $\mathrm{char}(F) = p \neq 0$) injective!

$$\sigma_p : F \to F$$
$$\alpha \mapsto \alpha^p$$
$$?? \mapsto 1$$

$\sigma_p(x) = 1 \iff x^p = 1$

Injective means that each element of F has a unique preimage. In particular 1 has a unique premage i.e. if $\mathrm{char}(F) = p$ the equation

$x^p = 1$ ← the preimage of 1 under σ_p are the solutions to this equation

$$x^p - 1 = (x-1)^p$$

Solving $x^p = 1$ in a field F with $\mathrm{char}(F) = p$

$$x^p - 1 = 0$$

$$(x-1)^p = 0 \longrightarrow \text{only solution is } 1!$$

This is different from $\mathbb{Q}$! Recall that ζ_p is a root of $x^p - 1$ that is not 1 and $x^p - 1$ has p roots in char 0. (In fact, has p roots in char $\ell \neq p$)

In char p, there are not n n^{th} roots of unity if $p \mid n$ (but there are otherwise)

Another way to think about it:

$x^n - 1$ is separable if $\mathrm{char}(F) \nmid n$

(derivative is $nx^{n-1} \neq 0$)

so n distinct roots

$x^n - 1$ is not separable if $\mathrm{char}(F) \mid n$

because then derivative is 0

so fewer than n distinct roots.

Going back to what we were saying:

Let F be a field, $\text{char}(F) = p \neq 0$, then $\sigma_p : F \to F$
$\sigma_p(\alpha) = \alpha^p$ is an injective field homomorphism.

Definition: We say F is <u>perfect</u> if σ_p is also surjective.

Definition: If $\text{char}(F) = 0$ we also say F is perfect.

Big result: F has inseparable extensions iff it is not perfect.

$\exists$ inseparable irred poly

σ_p is not surjective.

Connection: say $\mathrm{char}(F)=p$ and F is perfect

$f(x)\in F[x]$ with $f'(x)=0$

Claim: f is reducible i.e. no irreducible inseparable polynomials.

We know that if $f'(x)=0$ then

$$f(x)=f_1(x^p) \quad \text{for some } f_1 \in F[x]$$

Write $f(x)=\sum_{k=0}^{n} a_k x^{pk} = a_n x^{np} + a_{n-1} x^{(n-1)p} + \dots + a_1 x^p + a_0$

If $a_0=0$ then f is reducible since $x \mid f(x)$

If $a_0 \neq 0$, recall that $a_0 \in F$ and σ_p is surjective so there is $\alpha_0 \in F$ with $\alpha_0^p = a_0$

$$f(x) = a_n x^{np} + a_{n-1} x^{(n-1)p} + \dots + a_1 x^p + \alpha_0{}^p$$

$$= \left(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + \alpha_0\right)^p$$

So f is not irreducible!

Example: $F = \mathbb{F}_3(t) \ni \dfrac{t^3+2t+1}{t+2}$

$$\psi \quad \frac{p(t)}{q(t)} \qquad p, q \in \mathbb{F}_3[t]$$

$$\alpha = \frac{p(t)}{q(t)}$$

Note that F is not perfect: $\quad \sigma_3 : F \to F$, $\alpha \mapsto \alpha^3$

there is no $\alpha \in F$ with $\alpha^3 = t$

$$\left(\frac{p(t)}{q(t)}\right)^3 = t$$

So this gives an irreducible inseparable polynomial:

$$f(x) = x^3 - t \in F[x] = \mathbb{F}_3(t)[x]$$

- f is irreducible since it's degree 3 and has no linear factor.

- $f'(x) = 0 = \frac{d}{dx} f(x) = 3x^2 = 0 \Rightarrow \gcd(f, f') = f \neq 1$

So f is inseparable.

$F = \mathbb{F}_3(t)$

$$[\mathbb{F}_3(t^{1/3}) : \mathbb{F}_3(t)] = \deg \underbrace{m_{t^{1/3}, F}}_{= x^3 - t} = 3$$

only one root (namely $t^{1/3}$)

so $\sigma \in \mathrm{Aut}$ must fix $t^{1/3}$

$$\begin{array}{c} \mathbb{F}_3(t^{1/3}) \\ | \; 3 \\ \mathbb{F}_3(t) \end{array}$$

basis $1, t^{1/3}, t^{2/3}$

$$\mathrm{Aut}(\mathbb{F}_3(t^{1/3}) / \mathbb{F}_3(t)) = 1$$

this is the splitting field of $x^3 - t = (x - t^{1/3})^3$

Proposition: If F is a finite field, then F is perfect.
(i.e. every finite extension of a finite field is separable)

we actually showed more

we've shown it's Galois.

proof: $\operatorname{char}(F) = p$

$\sigma_p : F \to F$ this is an injective map between finite sets so it must be surjective.

$\square$

$F = \mathbb{F}_5$

$$f(x) = x^5 - 3$$
$$= (x-\alpha)^5$$
$$= (x-3)^5$$
$$= f_1(x^5)$$

$f_1(x) = x - 3$

know $\exists\, \alpha \in \mathbb{F}_5$ with $\alpha^5 = 3$

if $\beta \in \mathbb{F}_5$ then $\beta^5 = \beta$

That’s all for today!