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.

We saw that if $f \in F[x]$ is inseparable and irreducible

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

and all of the exponents in f are divisible by p

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

Why? f sep iff $\gcd(f, f') = 1$

but if f is irreducible $\gcd(f, g) = 1$ or f

and the only polynomial g with $\deg g < \deg f$ and

$f \mid g$ is $g = 0$

In other words if f irred + insep

f divides f', a polynomial with $\deg f' < \deg f$

$\Rightarrow f' = 0$

But in char p, can have $f' = 0$ without $f = c$ if all exponents are divisible by p

This discussion also shows that if

K/F is finite inseparable

then $\mathrm{char}(F) = p \neq 0$ and $p \mid [K:F]$,

Because: $\exists\, \alpha \in K$ with $m_{\alpha,F}$ irreducible + insep

$\Rightarrow p \mid \deg m_{\alpha,F}$

and since $F(\alpha) \subseteq K$ we have

$$\begin{array}{c} K \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

$$[K:F] = [K:F(\alpha)]\underbrace{[F(\alpha):F]}_{\text{div by } p.}$$

Caution: If $\mathrm{char}(F) = p \neq 0$ and $p \mid [K:F]$ then K/F may or may not be separable.

Last time: We saw that F has finite inseparable extensions iff F is not perfect

Recall: We say F is <u>perfect</u> if either

- $\mathrm{char}(F) = 0$
- or if $\mathrm{char}(F) = p \neq 0$, the map $\sigma_p : F \to F$ given by $\sigma_p(\alpha) = \alpha^p$ is <u>surjective</u>

Why? If f has all of its exponents divisible by p and $f \in F[x]$ $\text{char}(F) = p \neq 0$

then $f(x) = (g(x))^p$ $g(x) \in F[x]$ iff the constant term of f is a p^{th} power.

$h(x) = a_n x^n + \dots + a_0$

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

$$= (\underbrace{a_n x^n + a_{n-1} x^{(n-1)} + \dots + a_1 x + a_0^{1/p}}_{g(x) \in F[x] \text{ iff } a_0^{1/p} \in F})^p = (g(x))^p$$

If F is perfect: can always do this, so there are no polynomials with $f(x)=g(x^p)$

equivalent to: all exponents div by p

and $f(x)$ is irreducible.

$\Rightarrow$ so no irred insep polynomials

If F is not perfect then there is $\alpha \in F$ with $\alpha^{1/p} \notin F$ so $x^p - \alpha$ is irred and insep

$$\begin{aligned} F &\to F \\ \beta &\mapsto \beta^p \neq \alpha \end{aligned}$$

so $F(\alpha^{1/p})$ is insep extension.

Moving back to <u>finite</u> fields

So σ_p ("Frobenius map") is surjective because it is injective.

(σ_p on any field is injective)

<u>So</u> finite fields are perfect

not unique

~~the~~ most famous inseparable extension

$$\begin{array}{c} \mathbb{F}_p(t^{1/p}) \\ | \\ \mathbb{F}_p(t) \end{array} \qquad x^p - t$$

We knew that because we showed that every finite extension of a finite $\mathbb{F}_q$ $q=p^r$ p prime, r positive integer is the splitting field of $x^{q^n}-x$ for some positive integer n. This is a separable polynomial (its derivative is $-1 \neq 0$) so $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois hence separable.

Note: Every extension of $\mathbb{Q}$ is separable but they are not all Galois!!

Let K be a finite extension of $\mathbb{F}_q$

say $[K:\mathbb{F}_q]=n$

Then K is the splitting field of $x^{q^n}-x$ over $\mathbb{F}_q$.

$\#K=5^3$

Example if $[K:\mathbb{F}_5]=3$ then K is the splitting field of $x^{5^3}-x$ over $\mathbb{F}_5$

$$x^{5^3}-x = x^{125}-x$$

$$K\cong\mathbb{F}_{125}=\mathbb{F}_{5^3}$$

Where we left off a long time ago:

Let $q = p^r$; $\mathbb{F}_{q^n}/\mathbb{F}_q$ is finite and separable so there is a primitive element α: $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$

Note: $\mathbb{F}_{q^n} = \mathbb{F}_{(p^r)^n} = \mathbb{F}_{p^{rn}}$

$$\begin{array}{c} \mathbb{F}_{p^{rn}} \\ \cup\!\mid \\ \mathbb{F}_{p^r} \end{array}$$

That’s all for today!