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.

Last time: Field extensions

- algebraic field extensions

  K/F alg if $\forall \alpha \in K$, α is a root of a polynomial $f(x) \in F[x]$

- splitting fields

  K/F is the splitting of $f(x) \in F[x]$ if f factors completely in $K[x]$ but not over any intermediate field

Example: $\mathbb{C}/\mathbb{Q}$ is a field extension

$$\begin{array}{c}\mathbb{C}\\ \Big| \\ \mathbb{Q}(i) \\ \Big|\,2 \\ \mathbb{Q}\end{array}$$

$f(x) = x^2 + 1 \in \mathbb{Q}[x]$

$f(x) = (x-i)(x+i) \in \mathbb{C}[x]$

splits completely

but $\mathbb{C}$ is not the splitting field of f over $\mathbb{Q}$ because it's too big.

splitting field because smallest where f factors

We say that K/F is <u>normal</u> if K is the splitting field of a polynomial $f(x) \in F[x]$.

x^3-2 factors more than before but not all the way

Ex: $\mathbb{Q}(\sqrt[3]{2})$ is not normal

we still have $(x-2)(x+1) = x^2-x-2$

$\hookrightarrow$ every polynomial that factors completely here, already factored completely in a smaller field

Section 13.5 Separable + Inseparable extensions

→ lots of finite field stuff there

Definition: f is separable if all of its roots (which can possibly be in larger fields) are distinct

e.g. $f(x) = x^4 - 4x^2 + 4$ not separable

$= (x^2 - 2)^2$ roots $\{\sqrt{2}, \sqrt{2}, -\sqrt{2}, -\sqrt{2}\}$

If f is not separable, it's inseparable

derivative

Prop 33 f has a multiple root α iff $f'(\alpha)=0$ also

To put it another way, f is separable iff $\gcd(f, f') = 1$

Note that if $f(\alpha)=0$ and $f'(\alpha)=0$ then $x-\alpha$ divides both f and f' so $\gcd \neq 1$

Example $f(x) = (x^2-2)^2 = x^4 - 4x^2 + 4$

$$f'(x) = 4x^3 - 8x = 4x(x^2-2)$$

$$\gcd(f, f') = x^2 - 2$$

so $f(\sqrt{2}) = f'(\sqrt{2}) = 0$

$f(-\sqrt{2}) = f'(-\sqrt{2}) = 0$

and indeed both $\sqrt{2}$ and $-\sqrt{2}$ are double roots of f

Proof: Say α is a multiple root of f

$$f(x) = (x-\alpha)^2 g(x)$$

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

$$= (x-\alpha)\left[2g(x) + (x-\alpha)g'(x)\right]$$

finish other direction yourself!

Corollary 3.4

If $\mathrm{char}(F)=0$ and $f \in F[x]$ is irreducible, then f is separable

→ So in char 0, the only way to get an inseparable polynomial is to take a power of a polynomial

$$f(x) = (x-2)^2 (x+3) \quad \text{not sep}$$

Another way to say this is that in char 0, f is separable iff it is a product of distinct irreducible polynomials.

Note that in characteristic p, there are irreducible inseparable polynomials

Let t be transcendental over $\mathbb{F}_p$

then $x^p - t$ is irred over $\mathbb{F}_p(t)$ + insep.

Definition: K/F is a separable extension if

$\forall \alpha \in K$, $m_{\alpha,F}$ is separable

irreducible

Section 13.6 Cyclotomic extensions

↳ we'll have problems on these

Wednesday #6 of HW8

Chapter 14 - Galois theory

"Galois" is a kind of extension

Definition

K/F is Galois if

- $[K:F] < \infty$ ($\Rightarrow$ algebraic)
- normal / a splitting field
- separable

One more equivalent definition

K/F is Galois if K is the splitting field of a separable polynomial $f(x) \in F[x]$.

$\Rightarrow$ if $\deg f = n$ then $[K:F] \leq n!$ $\quad [K:F] \mid n!$

See book for proof that every element of K is separable.

Theorem 13 of Section 14.2

If K/F is Galois (finite, normal, separable) and $f(x) \in F[x]$ is irreducible. Then f has a root in K iff it splits completely in K.

If K/F is Galois, whenever K contains one root of an irred polynomial, it contains them all.

$\sigma : K \to K$ is a field automorphism

means that σ is a field homomorphism

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = \sigma(a)\sigma(b)$$

and σ is a bijection

We write $\sigma \in \mathrm{Aut}(K)$

If K/F is a fld extension, we write

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) : \sigma \text{ fixes } F \text{ pointwise}\}$$

(not as a set)

Example:
$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ | \\ \mathbb{Q} \end{array}$$

$\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$

$\sigma(\sqrt{2}) = -\sqrt{2}$

$\sigma(\sqrt{3}) = \sqrt{3}$

σ fixes $\mathbb{Q}$ also

① Every field automorphism always fixes the prime subfield.

That's because a fld hom sends 1 to 1

$$
\begin{array}{ccl}
K & \xrightarrow{\sigma} & K \\
1 & \longmapsto & 1 \\
2 & \overset{?}{\longmapsto} & \sigma(2)=\sigma(1+1)=\sigma(1)+\sigma(1)=2 \\
\frac{1}{2} & \overset{?}{\longmapsto} & 1=\sigma(1)=\sigma(\frac{1}{2}\cdot 2)=\sigma(\frac{1}{2})\cdot\sigma(2) \\
 & & =\sigma(\frac{1}{2})\,2
\end{array}
$$

$\Rightarrow \sigma(\frac{1}{2})=\frac{1}{2}$

② If α is a root of an irreducible poly f then a field aut σ sends α to another root of f

EX: $\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$

this is a root of $x^2 - 3$

Notice that $\sigma((\sqrt{3})^2 - 3)$

Notice that $\sigma\left((\sqrt{3})^2-3\right) = \sigma(0)=0$ since $(\sqrt{3})^2-3=0$

$$\begin{aligned} &\;\;\parallel \\ &\left(\sigma(\sqrt{3})\right)^2 - \sigma(3) \quad \leftarrow \sigma \text{ respects operations} \\ &\;\;\parallel \\ &\left(\sigma(\sqrt{3})\right)^2 - 3 \quad \leftarrow \sigma(3)=3 \text{ since } 3\in\mathbb{Q} \end{aligned}$$

$\Rightarrow \sigma(\sqrt{3})$ satisfies the polynomial x^2-3

$\left(\sigma(\sqrt{3})\right)^2-3=0 \qquad \Rightarrow \sigma(\sqrt{3})=\sqrt{3}$ OR $-\sqrt{3}$

By Wednesday   Read   14.1 + 14.2

That’s all for today!