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.

Galois extensions

A field extension K/F is <u>Galois</u> if it is

- finite: $[K:F] < \infty$
- separable: $\forall \alpha \in K$ $m_{\alpha,F}$ has distinct roots
- normal: K is the splitting fld of a poly/F

Equivalently K/F is Galois if K is the splitting field of a separable polynomial in $F[x]$

Category theory for the working mathematician

What should amaze you is

K splitting field of sep poly $\Rightarrow$ K is separable

Theorem 13 of Section 14.2

If K/F is Galois then if $f(x) \in F[x]$ is irreducible with one root in K, then all its roots are in K

If $f \in F[x]$ is irred then
- Splits completely in K
- or no roots in K

Now shift our attention to field automorphisms

$$\mathrm{Aut}(K) := \{ \sigma : K \to K, \ \sigma \text{ field homomorphism}, \ \sigma \text{ bijection} \}$$

If K/F is an extension

$$\mathrm{Aut}(K/F) := \{ \sigma \in \mathrm{Aut}(K) : \sigma(a) = a \ \forall a \in F \}$$

$\mathrm{Aut}(K)$ is a gp, $\mathrm{Aut}(K/F)$ is a subgp under composition

Lemma

Let $f(x) \in F[x]$ and $\sigma \in \mathrm{Aut}(K/F)$, $\alpha \in K$ is such that $f(\alpha) = 0$. Then $\sigma(\alpha)$ is ~~another~~ a root of f.

same or different

An element of $\mathrm{Aut}(K/F)$ permutes the roots of polynomials with coefficients in F.

proof: We have $0 = f(\alpha)$

Say $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$a_i \in F$

Apply σ to the equation $0 = f(\alpha)$

$$0 = \sigma(0) = \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n)$$

because a field map always sends $0 \mapsto 0$, $1 \mapsto 1$

$$0 = \sigma(0) = \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n)$$

because a field map always sends $0 \mapsto 0$, $1 \mapsto 1$

$\sigma(a+b) = \sigma(a) + \sigma(b)$ $\forall a, b \in K$

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

$\Downarrow$

if $a \in F$ $\sigma(a) = a$

$$= \sigma(a_0) + \sigma(a_1\alpha) + \sigma(a_2\alpha^2) + \dots + \sigma(a_n\alpha^n)$$

$$= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \sigma(a_2)\sigma(\alpha)^2 + \dots + \sigma(a_n)\sigma(\alpha)^n$$

$$= a_0 + a_1\sigma(\alpha) + a_2\sigma(\alpha)^2 + \dots + a_n\sigma(\alpha)^n$$

$$0 = \sigma(0) = \sigma\left(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n\right)$$

because a field map always sends $0 \mapsto 0$, $1 \mapsto 1$

$$= \sigma(a_0) + \sigma(a_1\alpha) + \sigma(a_2\alpha^2) + \dots + \sigma(a_n\alpha^n)$$

$\sigma(a+b) = \sigma(a) + \sigma(b)$ $\forall a, b \in K$

$$= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \sigma(a_2)\sigma(\alpha)^2 + \dots + \sigma(a_n)\sigma(\alpha)^n$$

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

if $a \in F$ $\sigma(a) = a$

$$= a_0 + a_1\sigma(\alpha) + a_2\sigma(\alpha)^2 + \dots + a_n\sigma(\alpha)^n$$

$$0 = f(\sigma(\alpha)) \Rightarrow \sigma(\alpha) \text{ is a Root of } f$$

In particular, $m_{\alpha,F} \in F[x]$ with $m_{\alpha,F}(\alpha) = 0$

So if $\sigma \in \mathrm{Aut}(K/F)$ then $\sigma(\alpha)$ is also a root of $m_{\alpha,F}$

(remember that if $f \in F[x]$ and $f(\alpha) = 0$ then be told $m_{\alpha,F} \mid f$)

Example: $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$

Let α be a root of f: $f(x) = (x^2-2)(x^2-3)$

So $\alpha = \sqrt{2}$ or $-\sqrt{2}$ or $\sqrt{3}$ or $-\sqrt{3}$

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

contains the roots of f

then $\sigma(\alpha)$ is a root of f

But if $\alpha = \pm\sqrt{2}$ then $\sigma(\alpha) = \pm\sqrt{2}$

If $\sigma \in \mathrm{Aut}(K/F)$ and $\alpha \in K$ then

$\sigma(\alpha)$ is a Root of $m_{\alpha, F}$

Another way to think of it: if $\sigma(\sqrt{2}) = \sqrt{3}$

then $(\sigma(\sqrt{2}))^2 = 3$

$\neq$

$\sigma((\sqrt{2})^2) = \sigma(2) = 2$ because σ fixes $\mathbb{Q}$

Let K/F be a Galois extension, then by the Primitive Element Theorem (Theorem 25 of Section 14.4) $\exists \alpha \in K$ s.t. $K = F(\alpha)$

Example: $\mathbb{Q}(\underbrace{\sqrt{2}}_{\alpha_1}, \underbrace{\sqrt{3}}_{\alpha_2})/\mathbb{Q}$

$$\| $$

$$\mathbb{Q}(\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha})$$

finite + separable

↳ deg 4

↳ every extension of $\mathbb{Q}$ is separable

K/F finite separable $K = F(\alpha)$

From the discussion we just had

- if $\sigma \in \mathrm{Aut}(K/F)$ then $\sigma(\alpha)$ is a root of $m_{\alpha,F}$

- if $\sigma \in \mathrm{Aut}(K/F)$ then σ is completely determined by the value of $\sigma(\alpha)$

Why? well $F(\alpha)$ means that an element of $F(\alpha)$ is of the form $\frac{p(\alpha)}{q(\alpha)}$ where

$p, q \in F[x]$.

↑ all the elements that are $+, -, \times, \div$ of elements of F and α

$p(x) = 5x^2 + 2$

$q(x) = 10x^3 + 5x + 1$

$$\frac{p(\alpha)}{q(\alpha)} = \frac{5\alpha^2 + 2}{10\alpha^3 + 5\alpha + 1} \in F(\alpha)$$

Now $\sigma \in \mathrm{Aut}(K/F)$

$\beta \in K \Rightarrow \beta = \dfrac{p(\alpha)}{q(\alpha)}$ so $\sigma(\beta) = \sigma\left(\dfrac{p(\alpha)}{q(\alpha)}\right)$

$p, q \in F[x]$

$= \dfrac{\sigma(p(\alpha))}{\sigma(q(\alpha))} = \dfrac{p(\sigma(\alpha))}{q(\sigma(\alpha))}$

So if $\sigma_1(\alpha) = \sigma_2(\alpha)$

then $\sigma_1(\beta) = \sigma_2(\beta) \quad \forall \beta \in K$

$\sigma_1 =$

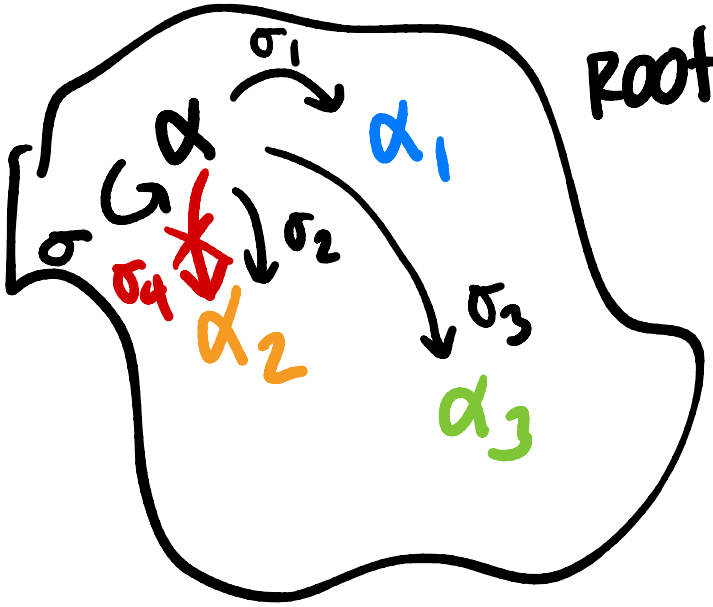
Eg $\beta = 5\alpha^2 + 1$

$\sigma(\beta) = 5\,\sigma(\alpha)^2 + 1$

Let K/F finite separable, $K = F(\alpha)$

then $\#\,\mathrm{Aut}(K/F) \leq \deg m_{\alpha,F}(x)$

proof: if $\sigma \in \mathrm{Aut}(K/F)$ then $\sigma(\alpha)$ is a root of $m_{\alpha,F}$. $m_{\alpha,F}$ has $\deg m_{\alpha,F}$ different roots because its separable and so there are at most $\deg m_{\alpha,F}$ different choices for $\sigma(\alpha)$



roots of $m_{\alpha,F}$

max number of possible $\sigma \in \mathrm{Aut}(K/F)$ is to have one σ for each root.

cannot have more σs

$\Rightarrow \sigma_2 = \sigma_4$

Note that $\deg m_{\alpha,F} = [K:F]$ since $K = F(\alpha)$

so $\#\mathrm{Aut}(K/F) \leq [K:F]$

Alternative definition

K/F is Galois iff $\#\mathrm{Aut}(K/F) = [K:F]$

i.e. $\mathrm{Aut}(K/F)$ is as big as possible.

That's all for today!

Friday: finish this discussion
then HW8 #1
then if we can #6