Galois Theory

Recap:

- $\mathrm{Aut}(K/F) = \{ \sigma : K \to K \text{ auto.}$
  $\sigma|_F = id_F \}$.
- K/F is called <u>Galois</u> if

$[K:F] = |\mathrm{Aut}(K/F)|$

in which we write $\mathrm{Gal}(K/F)$ for $\mathrm{Aut}(K/F)$

In lectures you showed
$|\mathrm{Aut}(K/F)| \leq [K:F]$.

Def: $H \leq \mathrm{Aut}(K)$ the <u>fixed field</u> of $H = K^H$
$= \{ x \in K : \sigma(x) = x$ forall
$\sigma \in H \}$

Thm: (Artin) $H \leq \mathrm{Aut}(K)$ finite

1.) $[K : K^H] = |H|$

2.) $K|K^H$ is Galois

3.) $\mathrm{Gal}(K|K^H) = H$

Idea of Galois theory:

$$\{\text{Subgps of } \mathrm{Gal}(K|F)\} \qquad\qquad H$$
$$\updownarrow \qquad\qquad\qquad\qquad \downarrow$$
$$\{\text{intermediate extension } L \text{ of } K|F\} \qquad\qquad K^H$$

Cor: $H_1, H_2 \leq \mathrm{Aut}(K)$ finite

$$H_1 = H_2 \iff K^{H_1} = K^{H_2}.$$

Big thm will see later.

$K|F$ Galois $\iff$ separable + normal

$\iff$ s.f. of a separable poly.

Rmk: What $K^{Gal(K|F)}$?

$$[K : K^{Gal(K|F)}] = |Gal(K|F)|$$
$$= [K : F]$$
$$=$$
$$[K : K^{Gal(K|F)}] \cdot [K^{Gal(K|F)} : F]$$

$\Rightarrow [K^{Gal(K|F)} : F] = 1$

$\Rightarrow \quad K^{Gal(K|F)} = F.$

Examples of Galois Group computations

1.) $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is Galois
b/c it's a s.f. of $x^2 - 2$.

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$ So $Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$

Explicitly:

any $\sigma \in Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is determined by what it does to $\sqrt{2}$.

$$\sigma(\sqrt{2}) = \pm\sqrt{2}.$$

this means ≤ 2 auto.

but ext^n is Galois, so exactly 2.

this means both choices work!!

$1 : \sqrt{2} \longrightarrow \sqrt{2}$ identity

$\sigma : \sqrt{2} \longrightarrow -\sqrt{2}$

$$Gal(\mathbb{Q}(\sqrt{2}), \mathbb{Q}) = \{1, \sigma\}$$

2.) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois b/c it's the s.f. of $(x^2-2)(x^2-3)$.

We know that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

So $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ is a group of order 4.

Any $\sigma \in Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ is determined by what it does to $\sqrt{2}, \sqrt{3}$.

$$\sigma : \begin{array}{l} \sqrt{2} \longrightarrow \pm\sqrt{2} \\ \sqrt{3} \longrightarrow \pm\sqrt{3} \end{array}$$

So ≤ 4 auto. $\Longrightarrow$ all work!

$$\sigma : \begin{array}{l} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{array} \qquad \tau : \begin{array}{l} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{array}$$

$$\sigma\tau : \begin{array}{l} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{array}$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$\langle \sigma, \tau \mid \sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle$

Subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$	Fixed fields
$\{1\}$	$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ $\quad a,b,c,d \in \mathbb{Q}$.

Let's say this is fixed by σ.

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = a+b\sigma(\sqrt{2})+c\sigma(\sqrt{3}) + d\sigma(\sqrt{6})$$

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$

$$\Rightarrow \quad 2b\sqrt{2}+2d\sqrt{6} = 0$$

$\Rightarrow$ $b=d=0$ b/c $\sqrt{2},\sqrt{6}$ l.i. over $\mathbb{Q}$ b/c part of basis for this ext^n.

So fixed field is

$$\{a+c\sqrt{3} : a,c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3}).$$

3.) $f(x) = x^4 - 2x^2 - 2$. $f(x)$ is irred. over $\mathbb{Q}$ b/c eisenstein at 2.

Roots of f:

$\pm\alpha, \pm\beta$

$\alpha = \sqrt{1+\sqrt{3}}$ $\qquad \alpha\beta = i\sqrt{2}$

$\beta = \sqrt{1-\sqrt{3}}$

s.f. of $f(x)$ is $\mathbb{Q}(\alpha, i\sqrt{2})$

$$\mathbb{Q}(\alpha, i\sqrt{2})$$
$$\Big|\ 2 \qquad \text{b/c } i\sqrt{2} \notin \mathbb{R}$$
$$\mathbb{Q}(\alpha)$$
$$\Big|\ 4 \qquad \text{b/c } f \text{ is irred.}$$

(4)

$\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q}$ is Galois b/c s.f. of $f(x)$.

$Gal(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$ is a gp of order 8.

Any $\sigma \in Gal(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$ is determined by what it does to α, $i\sqrt{2}$.

$$\alpha \longrightarrow \pm\alpha, \pm\beta$$

$$i\sqrt{2} \longrightarrow \pm i\sqrt{2}$$

≤ 8 auto. we have exactly 8

So all work!

$\sigma: \alpha \longrightarrow \beta$ $\qquad\qquad$ $\tau: \alpha \longrightarrow \alpha$

$\quad\; i\sqrt{2} \longrightarrow -i\sqrt{2}$ $\qquad\qquad$ $\quad i\sqrt{2} \longrightarrow -i\sqrt{2}$

	1	σ	σ^2	σ^3	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
α	α	β	$-\alpha$	$-\beta$	α	$-\beta$	$-\alpha$	β
$i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$

$$\beta = \frac{i\sqrt{2}}{\alpha} \implies \sigma(\beta) = \frac{\sigma(i\sqrt{2})}{\sigma(\alpha)} \text{ etc.}$$

$$\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$$

$$= \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \; \tau\sigma\tau = \sigma^3 \rangle$$

Check relation

$$\cong D_8.$$

Application 1

Prop: $K|F$ $\alpha \in K$. Then

$$m_\alpha(x) = \prod (x - \sigma(\alpha))$$

where the product runs through all distinct values of $\sigma(\alpha)$ for $\sigma \in Gal(K|F)$.

Proof: α a root of $m_\alpha(x) \in F[x]$

$\Rightarrow$ $x - \alpha \mid m_\alpha(x)$ in $K[x]$.

$m_\alpha(x) = (x-\alpha)\, g(x)$ for some $g(x) \in K[x]$.

$$m_\alpha(x) = (x - \sigma(\alpha))(\sigma g)(x)$$

for any $\sigma \in Gal(K/F)$

$$\Rightarrow \prod (x - \sigma(\alpha)) \mid m_\alpha(x) \text{ in } K[x].$$

$$p(x) = \prod (x - \sigma(\alpha))$$

hitting $p(x)$ w/ σ just permutes the list $\{\sigma(\alpha)\}$

$$\Rightarrow (\sigma p)(x) = p(x)$$

i.e. all coeff. are fixed by

$Gal(K|F) \implies$ in F.

$\implies m_\alpha(x) = \prod (x - \sigma(\alpha))$

by minimality.

<u>Ex:</u> $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ has degree 8. It's Galois gp is D_8 with generators

$\sigma: 2^{1/4} \longrightarrow i2^{1/4}$ $\quad$ $\tau: 2^{1/4} \longrightarrow 2^{1/4}$

$\quad\; i \longrightarrow i$ $\quad\quad\quad\quad\quad\quad\; i \longrightarrow -i$

(check!)

	1	σ	σ^2	σ^3	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
$2^{1/4}$	$2^{1/4}$	$i2^{1/4}$	$-2^{1/4}$	$-i2^{1/4}$	$2^{1/4}$	$-i2^{1/4}$	$-2^{1/4}$	$i2^{1/4}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

$$\alpha = 1+\sqrt{2}+\sqrt[4]{2}$$

the Gulois conjugates of α:

$1+\sqrt{2}+\sqrt[4]{2}$, $1-\sqrt{2}+i\sqrt[4]{2}$, $1+\sqrt{2}-\sqrt[4]{2}$, $1-\sqrt{2}-i\sqrt[4]{2}$

this tells us that $\deg m_\alpha(x) = 4$

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ \mid\ 4 \\ \mathbb{Q} \end{array}$$

Note $\alpha \in \mathbb{Q}(\sqrt[4]{2})$

$\Longrightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[4]{2})$.