May 12

Let $K \subset L$ be a finite field ext

The Galois group

$$\mathrm{Gal}(L/K) = \{\text{automorphisms } \sigma : L \to L \text{ s.t. } \forall x \in K\ \sigma(x) = x\}$$

"auts of L over K"

Notation: $\mathrm{Gal}_K(L) \longleftrightarrow \mathrm{Gal}(L/K)$

Hungerford: $F \subset K \longleftrightarrow K \subset L$

Properties

1. $\mathrm{Gal}(L/K)$ is a group under composition
2. If $x \in L$ has min poly $f(x) \in K[x]$ then $\forall \sigma \in \mathrm{Gal}(L/K)$, $\sigma(x)$ is also a root of $f(x)$

$\rightsquigarrow$ $\mathrm{Gal}(L/K)$ acts on the roots of $f(x)$.

3. If $u, v \in L$ have same min poly, $\exists \sigma \in \mathrm{Gal}(L/K)$ s.t. $\sigma(u) = v$.
4. Upshot: If $K \subset L$ is the splitting field of $f(x)$ and $K \subset L$ is separable and $n = \deg f$, then

$$\mathrm{Gal}(L/K) \subset S_n \text{ subgp}$$

$\rightsquigarrow$ $\mathrm{Gal}(L/K)$ acts on roots of $f(x)$ via permutation.

Cor: $|\mathrm{Gal}(L/K)| \mid n!$

Recall: We know $|L:K| \mid n!$

Fact (to be proven)

Let $K \subset L$ be a finite field ext

Then $\#\mathrm{Gal}(L/K) \leq |L:K|$

with equality iff

$K \to L$ is separable & normal.

Defn Say $K \to L$ is Galois if

$K \to L$ finite, separable & normal

The Galois group $\mathrm{Gal}(L/K)$ carries the most information when $K \subset L$ is Galois!

$\rightsquigarrow$ Sometimes people will only write $\mathrm{Gal}(L/K)$ if it's $K \subset L$ is Galois & otherwise write $\mathrm{Aut}(L/K)$

Ex 1 $\mathbb{R} \to \mathbb{C}$

$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, \sigma\}$

where $\sigma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$

$|\mathbb{C} : \mathbb{R}| = 2 = \#\mathrm{Gal}(\mathbb{C}/\mathbb{R})$

note: $\mathbb{R} \to \mathbb{C}$ is sep & normal

Ex 2 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{11})$

$\mathrm{Gal}(\mathbb{Q}(\sqrt{11})/\mathbb{Q}) = \{id, \sigma\}$

$\sigma : \mathbb{Q}(\sqrt{11}) \to \mathbb{Q}(\sqrt{11})$

$a + b\sqrt{11} \mapsto a - b\sqrt{11}$

note: min poly of $\sqrt{11}$ is $x^2 - 11$

Two ways to write a field ext

$$\underbrace{K \subset L}_{K \to L} \qquad \underbrace{K \xrightarrow{\tau} L}_{\tau(K) \subset L}$$

Ex 3 $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$

What is $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$?

$\rightsquigarrow$ min poly of $\sqrt[3]{2}$ is x^3-2

Other roots are $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

$\omega = e^{2\pi i/3}$

Claim: $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$

b/c if $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ is aut, then $\sigma(\sqrt[3]{2})$ is also a root of x^3-2.

But the only root in $\mathbb{Q}(\sqrt[3]{2})$ is $\sqrt[3]{2}$.

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

$$\underbrace{\#\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})}_{=1} \leq \underbrace{|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|}_{=3}$$

Ex 4

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) = L$

splitting field of x^3-2

Fact $\rightsquigarrow$ $|\mathrm{Gal}(L/\mathbb{Q})| = 6 = |L:\mathbb{Q}|$

Know $\mathrm{Gal}(L/\mathbb{Q}) \subset S_3$

$(3 = \deg(x^3-2))$

basis of $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ $\quad \omega^2+\omega+1=0$

$\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$

Know: If $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$,

$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

$\sigma(\sqrt{3}i) = \sqrt{3}i, -\sqrt{3}i$

These images determine σ.

Claim: Each of the 6 options defines a well defined field aut

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$$

keep constant

If $\sqrt{3}i \overset{\sigma}{\longmapsto} -\sqrt{3}i$,

$\omega \longmapsto \omega^2$

Here σ is complex conj

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow[z \longmapsto \bar{z}]{} & \mathbb{C} \\ \cup & & \cup \\ \sigma : \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) & \longrightarrow & \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) \end{array}$$