May 10 : Galois groups

Évariste Galois
1811 - 1832

Maryam Mirzakhani
1977 - 2017

Galois Theory

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

- An automorphism of L over K is a field isomorphism $\phi : L \to L$ that preserves K, i.e. $\forall x \in K$ $\phi(x) = x$.

Ex: complex conj. $\mathbb{C} \to \mathbb{C}$
$a+ib \mapsto a-ib$
is an automorphism of $\mathbb{C}$ over $\mathbb{R}$

- The Galois group (or automorphism group) of L over K

$$\mathrm{Gal}(L/K) = \{\phi : L \to L \text{ automorphism of } L \text{ over } K\}$$

Notation: Some people reserve "Galois group" only when $K \subset L$ is normal & separable.

HW (7.5)(a) $\mathrm{Gal}(L/K)$ is a group under composition

(b) Let $\alpha \in L$ is a root of a polynomial $f(x) \in K[x]$. For any $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\alpha)$ is also a root of $f(x)$.

Key idea: Elements $\sigma \in \mathrm{Gal}(L/K)$ take roots to other roots.
$\rightsquigarrow$ action of $\mathrm{Gal}(L/K)$ on the roots of $f \in K[x]$

Ex: What is $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$?

Note $\mathbb{C}$ is splitting field of x^2+1
$\to \mathbb{C} = \mathbb{R}(i)$

Let $\sigma : \mathbb{C} \to \mathbb{C}$ aut. over $\mathbb{R}$

Two examples: $\sigma = \mathrm{id}$ or $\sigma = $ conjugation
Are there others?

Fran: No!

Reason:

Any $\sigma: \mathbb{C} \to \mathbb{C}$ aut over $\mathbb{R}$ takes any root x^2+1 to another root.

Therefore, $\sigma(i) = \pm i$

Also, since $\mathbb{C} = \mathbb{R}(i)$, the field auto. σ is determined by where it sends i.

(if $z \in \mathbb{C}$, $z = a + ib$ where $a, b \in \mathbb{R}$
$\sigma(z) = a \pm ib$)

Prop Let $K \subset L = K(\alpha_1, \dots, \alpha_n)$

Then any $\sigma \in Gal(L/K)$ is determined by the images $\sigma(\alpha_i)$.

Pf: It suffices to show that if $\sigma(\alpha_i) = \alpha_i$ for all i, then σ is the identity.

- Any element $x \in L$ can be written as an expression involving elements of K and products, sums, diff., quotients of α_i. eg. $x = 4\alpha_1 + \frac{\alpha_2 \alpha_3}{\alpha_6 - 1} + \cdots$

Since σ is a field isom & preserves K, $\sigma(x) = x$

Prop. Let L be splitting field of $f(x) \in K[x]$. So $K \subset L$.

- Let $u, v \in L$

Then there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(u) = v$ if and only if u and v have the same min poly.

Proof ($\Longrightarrow$) If $\exists \sigma$ w/ $\sigma(u) = v$ and let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ min poly of u.

$$\rightsquigarrow g(u) = u^n + \underbrace{a_{n-1}}_{\text{in } K} u^{n-1} + \cdots + \underbrace{a_0}_{\text{in } K} = 0$$

Apply σ,

$$\sigma(u)^n + a_{n-1}\sigma(u)^{n-1} + \cdots + a_0 = 0$$

$\Longrightarrow v = \sigma(u)$ is also a root of g

$\Longrightarrow$ min poly of v divides g

In reverse, g (min poly of u) divides min poly of v.

($\Longleftarrow$) Say u & v are min poly of $f(x) \in K[x]$

$$\begin{tikzcd}
L \arrow[r, dashed, "\exists"] & L \\
K(u) \arrow[u, dash] \arrow[r, "\sigma"] & K(v) \arrow[u, dash] \\
K \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

$$K(u) = K[x]/f(x) = K(v)$$

$\rightsquigarrow$ Gives isom $K(u) \xrightarrow{\sigma} K(v)$

By properties of splitting fields, $\exists\, \tilde{\sigma} : L \to L$ extending σ

$\Longrightarrow \tilde{\sigma} \in \mathrm{Gal}(L/K)$ and $\tilde{\sigma}(u) = v$.

Cor: Let $K \subset L$ be the splitting field of $f(x) \in K[x]$ of degree n.
Then $Gal(L/K) \subset S_n$ is a subgroup.

Proof We know $f(x)$ splits$/L$
i.e. $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$
where $\alpha_i \in L$
And $L = K(\alpha_1, \dots, \alpha_n)$.
Construct a group hom

$$\psi : Gal(L/K) \longrightarrow S_n$$
$$\sigma \longmapsto \left(\begin{array}{l} \{1,\dots,n\} \longrightarrow \{1,\dots,n\} \\ i \longmapsto j \text{ where } \sigma(\alpha_i) = \alpha_j \end{array} \right)$$

In other words, σ permutes the roots.

Since any $\sigma \in Gal(L/K)$ is determined by its image $\sigma(\alpha_i)$
ψ is injective!

$$Gal(L/K) \subset S_n.$$

Comment: If f is not separable, then α_i may not be distinct, ambiguous

$k \le n$

Let $\alpha_1, \dots, \alpha_k$ distinct roots

$\rightarrow Gal(L/K) \subset S_k \subset S_n$