Galois theory

What is it good for ?

Example - Constructible $\iff$ member of $\mathbb{Q} \subset K$ such that

$$\underbrace{\mathbb{Q} \subset K_1}_{\deg 2} \underbrace{\subset K_2}_{\deg 2} \underbrace{\subset \cdots}_{\deg 2} \subset K_n = K$$

Given $\mathbb{Q} \subset K$, is there a chain of deg 2 ext^n as above ?

Galois theory answers this question.

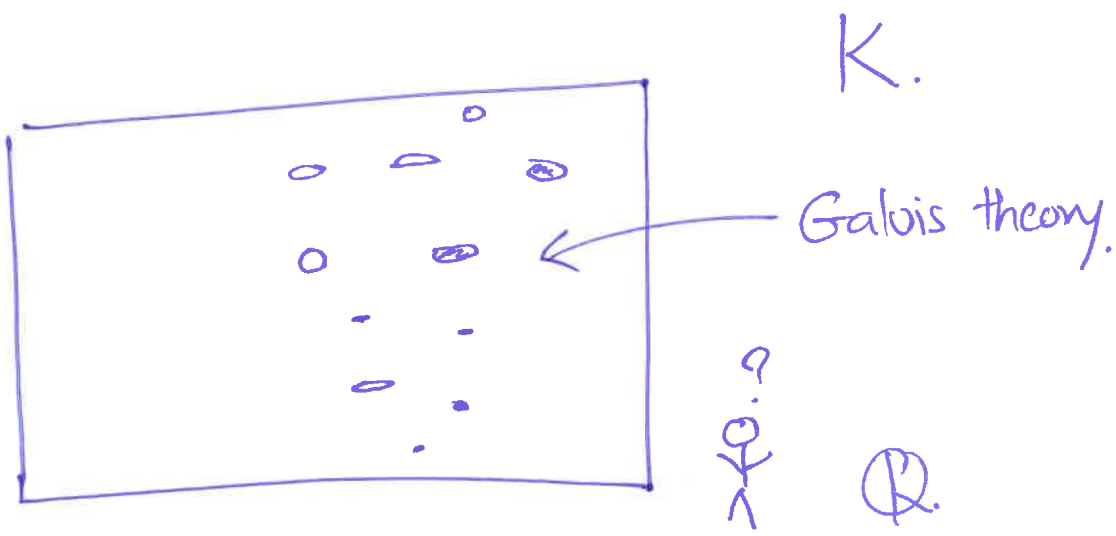
Given $\mathbb{Q} \subset K$:

Galois theory $\Rightarrow$ All intermediate extensions

$$\begin{tikzcd}
 & K & \\
 & K_3 \arrow[u] & \\
K_2 \arrow[ur] & & K_1 \arrow[ul] \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Arrow
$\parallel$
subfield.

Given $\mathbb{Q} \subset K$ $\xrightarrow[\text{Theory.}]{\text{Galois}}$ Diagram of ~~sub~~ intermediate fields.



Slogan: A field extension $F \subset K$ is governed by its symmetries.

A symmetry of a field K is an automorphism
$$\varphi: K \to K.$$

(invertible homomorphism).

Ex. $\varphi: \mathbb{C} \to \mathbb{C}$ $\quad z \mapsto \bar{z}$

Ex. $\varphi: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ $\quad x \mapsto x^p$

A symmetry of an extension $F \subset K$ is an aut. $\varphi: K \to K$ such that $\varphi|_F = \text{identity}$.

Ex. $F = \mathbb{Q}[\sqrt{2}] \subset K = \mathbb{Q}[\sqrt{2}, i]$

$\varphi : K \to K \qquad z \mapsto \bar{z}$

is a symmetry of $F \subset K$.

Given $F \subset K$, let
$$G = \mathrm{Aut}(F \subset K) = \mathrm{Aut}(K/F) = \mathrm{Aut}_F(K).$$

G is a group, operation = composition.

Governs everything.

Theorem: Let $F \subset K$ be a finite extension satisfying ...

There is a bijection between intermediate fields of $F \subset K$ and subgroups of $G = \mathrm{Aut}_F(K)$.

Moreover the diagram of intermediate fields is the same as the diagram of subgroups, reversed.

$$\begin{tikzcd}
 & K & \\
 & K_3 \arrow[u] & \\
K_1 \arrow[ur] & & K_2 \arrow[ul] \\
 & F \arrow[ul] \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{id\} \arrow[d] & \\
 & H_3 \arrow[dl] \arrow[dr] & \\
H_1 \arrow[dr] & & H_2 \arrow[dl] \\
 & G &
\end{tikzcd}$$

degree. $\longleftrightarrow$ index

$F \subset K_i \mapsto \mathrm{Aut}(K/K_i)$

$\left\{ x \in K \mid \forall \sigma \in H \ \ \sigma(x) = x \right\} \longleftarrow H$

Ex. $F = \mathbb{Q} \subset \mathbb{Q}[\sqrt{2}, i] = K$.

$G = \mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

↳ has 4 elts.

$\sqrt{2} \mapsto \sqrt{2}$ $i \mapsto i$	$\sqrt{2} \mapsto -\sqrt{2}$ $i \mapsto i$	$\sqrt{2} \mapsto \sqrt{2}$ $i \mapsto -i$	$\sqrt{2} \mapsto -\sqrt{2}$ $i \mapsto -i$
$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$.

$$\begin{tikzcd}
 & \mathbb{Q}[\sqrt{2}, i] & \\
\mathbb{Q}[\sqrt{2}] \arrow[ur] & \mathbb{Q}[i] \arrow[u] & \mathbb{Q}[\sqrt{2}i] \arrow[ul] \\
 & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \{(0,0)\} \arrow[dl] \arrow[d] \arrow[dr] & \\
\{(0,0),(0,1)\} \arrow[dr] & \{(0,0),(1,0)\} \arrow[d] & \{(0,0),(1,1)\} \arrow[dl] \\
 & \mathbb{Z}_2 \times \mathbb{Z}_2 &
\end{tikzcd}$$