Galois Theory.

Motivation: How to solve a polynomial equation?

$n=2$

$$f(x) = ax^2 + bx + c = 0 \qquad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$n=3$ (1500+)

$$f(x) = ax^3 + bx^2 + cx + d = 0$$

$$\Delta_0 = b^2 - 3ac$$

$$\Delta_1 = 2b^3 - 9abc + 27a^2 d$$

$$C = \sqrt[3]{\frac{\Delta_1 \pm \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}}$$

$$r_k = -\frac{1}{3a} \cdot \left(b + C \cdot \xi^k + \frac{\Delta_0}{\xi^k \cdot C} \right)$$

$k = 0, 1, 2 \qquad \xi = \xi_3.$

$n=4$ $f(x) = ax^4 + bx^3 + cx^2 + dx + e = 0$ (1500+)

Q: Can you still find a formula for a generic quartic polynomial? (Ask google/wiki).

Ans: Yes.

$n=5$. $f(x) = \sum_{n \leq 5} a_n x^n$

Galois ($n \geq 5$): Ans: No.

Such a formula does not exist for $n > 4$. (1800+)

Def (F-automorphism of K) Given a field extension K/F,

$$\mathrm{Aut}(K/F) := \left(\left\{ \sigma : K \to K \;\middle|\; \begin{array}{l} \sigma(a) = a \quad \forall a \in F \\ \underbrace{\sigma \text{ is an isomorphism}}_{\sigma \text{ is called } F\text{-automorphism of } K} \text{ ring} \end{array} \right\}, \text{ composition} \right)$$

is a grp.

eg. $\begin{array}{c} \mathbb{F}_q \\ | \\ \mathbb{F}_p \end{array}$ $\{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma \text{ is a ring isomorphism}\}$ forms a grp under composition.

$1 \to 1$ $\quad \mathbb{F}_p \xrightarrow{id} \mathbb{F}_p$

eg. $\begin{array}{c} \mathbb{Q}[\sqrt{2}] \\ | \\ \mathbb{Q} \end{array}$ Galois

$\mathbb{Q} \xrightarrow{id} \mathbb{Q}$

$\sigma : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$

σ has to fix $\mathbb{Q}$ element-wisely.

$\sigma : \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}]$

$\sigma(\sqrt{2}) \longrightarrow -\sqrt{2}$

then $\exists!$ field isomorphism. s.t. $\sigma(\sqrt{2}) = -\sqrt{2}$.

$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

uniqueness $\to$ $\sigma(a + b\sqrt{2}) = \sigma(a) + \sigma(b\sqrt{2}) = \sigma(a) + \sigma(b) \cdot \sigma(\sqrt{2})$

$= a + b \cdot \sigma(\sqrt{2})$

existence $\to$ $\underset{T}{\underline{\sigma(\sqrt{2})}}^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2$

$T^2 - 2 = 0 \qquad T = \sqrt{2} \text{ or } -\sqrt{2}$.

$F = \mathbb{Q}[\sqrt{2}]$ is defined by $f(x) = x^2 - 2$

$\forall \alpha \in F$ if $\alpha^2 - 2 = 0$, then

$$\sigma(\alpha^2 - 2) = \sigma(0)$$
$$\parallel$$
$$\sigma(\alpha)^2 - 2$$

σ has to map a root to another root.

For $F = \mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, we actually prove that.

$$\mathrm{Aut}(F/\mathbb{Q}) = \left\{ \begin{array}{l} id: \sqrt{2} \to \sqrt{2} \\ \sigma: \sqrt{2} \to -\sqrt{2} \end{array} \right\} \simeq C_2$$

$\leftarrow$ cyclic grp of order 2.

$$\underline{\sigma \circ \sigma}: \quad \sqrt{2} \xrightarrow{\sigma} -\sqrt{2} \xrightarrow{\sigma} -(-\sqrt{2}) = \sqrt{2}$$

eg. $F = \mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$. $\qquad \mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[x]/\langle x^3 - 2 \rangle$

$$\begin{array}{c} F \\ \big| \, 3 \\ \mathbb{Q} \end{array}$$

not Galois

$\mathrm{Aut}(F/\mathbb{Q}) = ?$

$$\mathbb{Q}[\sqrt[3]{2}] = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \}.$$

If σ fixes $\mathbb{Q}$. then

$$\sigma(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\,\sigma(\sqrt[3]{2}) + c \cdot \sigma(\sqrt[3]{2})^2$$

The value of $\sigma(\sqrt[3]{2})$ completely pin down the value of σ(any field element)

Where can I map $\sqrt[3]{2}$ to ?

$\sqrt[3]{2}$ is root $x^3 - 2 = 0$

$$\sigma\left((\sqrt[3]{2})^3 - 2\right) = \sigma(0) = 0$$

$$\boxed{\sigma(\sqrt[3]{2})}^3 - 2 = 0, \quad \sigma(\sqrt[3]{2}) = T$$

$$T^3 - 2 = 0$$

$$= (T - \underbrace{\sqrt[3]{2}}_{r_1})(T - \underbrace{\sqrt[3]{2} \cdot \zeta_3}_{r_2}) \cdot (T - \underbrace{\sqrt[3]{2} \cdot \zeta_3^2}_{r_3}) = 0$$

So we have at most 3 choices for $\sigma(\sqrt[3]{2})$.

if $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ this induces identity on $F \xrightarrow{id} F$.

$$\sigma(\sqrt[3]{2}) \overset{?}{=} \sqrt[3]{2} \cdot \zeta_3 \notin F$$
$\star$

Therefore $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ is the only choice.

$\mathrm{Aut}(F/\mathbb{Q}) = \{e\}$.

This motivate the concept of Galois extension.

Def (normal extension): A finite field extension K/F is called normal if $\forall f(x)$ irreducible in $F[x]$

$f(x)$ has a root in $K \iff f(x)$ has all roots in K.

Rmk: All finite extensions over $\mathbb{F}_q$ are Galois. (see hw 8).

Def (Galois extension over $\mathbb{Q}$) A finite extension K over $\mathbb{Q}$ is called Galois extension over $\mathbb{Q}$ if $K/\mathbb{Q}$ is normal.

Suppose 1) $K/\mathbb{Q}$ is Galois. 2) $K = \mathbb{Q}[\alpha]$ $\alpha \in \mathbb{C}$

algebraic number

$K = \mathbb{Q}[\alpha]$

$\mathbb{Q}$

$\{\underbrace{1, \alpha, \alpha^2 \dots}\ \alpha^k\}$ is.

$\exists$ smallest k s.t. linearly dependent.

this $\Sigma a_i \cdot \alpha^i = 0$ gives a

$f(x) = \Sigma a_i x^i$

irreducible in $\mathbb{Q}[x]$.

Then $\mathbb{Q}[\alpha] = \{a_0 \cdot 1 + a_1\alpha + \dots + a_{k-1}\alpha^{k-1} \mid a_i \in \mathbb{Q}\}$.

$a_k \alpha^k$

Q: $\mathrm{Aut}(K/\mathbb{Q}) = ?$

$$f(x) = (x - \overset{\alpha}{\overset{\shortparallel}{\alpha_1}})(x - \alpha_2) \cdots (x - \alpha_k) \in K[x]$$

$$f(\alpha) = \Sigma a_i \alpha^i = 0$$

$\downarrow \sigma$

$$\sigma(f(\alpha)) = \Sigma a_i \cdot \underbrace{\sigma(\alpha)}_{T}{}^i$$

$\Sigma a_i T^i = 0$ T must be a root of $f(x)$.

T must be α_i for some i.

T has most k choices: $\alpha \to \alpha_i$

$i = 1, \dots, k$.

We can prove all choices $\exists$!

a ring isomorphism of $\sigma_i : K \to K$. s.t $\sigma_i(\alpha) = \alpha_i$.

$|\mathrm{Aut}(K/\mathbb{Q})| = K.$

Ex: 1). $f(x) \in \mathbb{Q}[x]$ is irreducible, then $f(x)$ has no double roots. $f'(x)$, $f(x)$ has common roots.

check mid-term

2) For each specification of α, $\sigma_i(\alpha) = \alpha_i$, σ_i really extend to a field isomorphism.

Def: (Galois Grp). If $K/\mathbb{Q}$ is a Galois extension, then.

$\mathrm{Gal}(K/\mathbb{Q}) := \mathrm{Aut}(K/\mathbb{Q})$

is called the Galois grp.

Lemma (Primitive Element Thm) Every finite extension over $\mathbb{Q}$ can be written as $\mathbb{Q}[\alpha]$ for a root α of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. $\deg(f) = [\mathbb{Q}[\alpha] : \mathbb{Q}]$.

Rmk: does not require ext to be Galois.

Check hw. $\mathbb{Q}[\sqrt{2} + \sqrt{5}] = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$.

$$\mathbb{Q}[\sqrt{2}, \sqrt{5}] = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$$
$$|$$
$$\mathbb{Q}[\sqrt{2}]$$
$$|$$
$$\mathbb{Q}$$

Thm. If $K/\mathbb{Q}$ is Galois, then

$|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$.