Galois Theory (An overview)

Assume all fields are subfields of $\mathbb{C}$ during this lecture.

Let $F \subset \mathbb{C}$ be a subfield and $f(x) \in F[x]$.

Assume $f(x) = a \prod_{i=1}^{n} (x - \alpha_i)$ where $a \in F$, $\alpha_i \in \mathbb{C}$.

Definition $F_f := F(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ is called the splitting field of $f(x)$.

minimal subfield of $\mathbb{C}$ containing F and $\{\alpha_1, \ldots, \alpha_n\}$

Example $F = \mathbb{Q}$, $f(x) = x^3 - 2$

$$f(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}e^{\frac{2\pi i}{3}})(x - \sqrt[3]{2}e^{\frac{4\pi i}{3}})$$

$$\Rightarrow \quad \mathbb{Q}_f = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}) = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$$

More general: $f(x) = x^n - a \quad (a \in \mathbb{Q})$

$$\Rightarrow \quad \mathbb{Q}_f = \mathbb{Q}(\sqrt[n]{a}, e^{\frac{2\pi i}{n}}) \quad (\sqrt[n]{a} \in \mathbb{C} \text{ is a single } n^{\text{th}} \text{ root of } a)$$

Definition Let E/F be a field extension. We say E/F is Galois if $\exists\, f(x) \in F[x]$ s.t. $E = F_f$, i.e. if E is the splitting field of some polynomial in $F[x]$.

Examples: $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})/\mathbb{Q}$ is Galois.

Remarks 1/ For characteristic p field extensions there is an extra condition required. We've dealing only with subfields of $\mathbb{C}$ so we don't need to worry about it.

2/ E/F Galois $\Leftrightarrow$ given $g(x) \in F[x]$ irreducible, either $g(x)$ has no roots in E, or it splits into linear factors in $E[x]$.

$\Rightarrow$ $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is <u>not</u> Galois. $g(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, has a root in $\mathbb{Q}(\sqrt[3]{2})$ but cannot split into linear factors as $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$.

3/ E/K, K/F field extensions.

E/F Galois $\Rightarrow$ E/K Galois

$$\text{Galois}\left\{\begin{array}{l} E \\ | \\ K \\ | \\ F \end{array}\right. \begin{array}{l} \} \text{ Galois} \\ \\ \} \text{ Not necessarily Galois.} \end{array}$$

Example: $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) / \mathbb{Q}(e^{2\pi i/3})$ Galois.

Definition Let E/F be a Galois extension.

$$\mathrm{Gal}(E/F) = \left\{ \sigma : E \to E \;\middle|\; \begin{array}{l} \sigma \text{ is a field automorphism} \\ \sigma(a) = a \quad \forall a \in F \end{array} \right\}$$

Galois group of E/F

Remarks 1/ $\mathrm{Gal}(E/F)$ is a group under composition.

2/ $|\mathrm{Gal}(E/F)| = [E:F]$ $\leftarrow$ not obvious

How can we concretely think about $\mathrm{Gal}(E/F)$?

E/F Galois $\Rightarrow$ $E = F_f$ for some $f(x) \in F[x]$.

Let $f(x) = a_0 + a_1 x + \dots + a_n x^n = a_n \prod_{i=1}^{n} (x - \alpha_i)$

$a_j \in F$, $\alpha_i \in \mathbb{C}$. $\Rightarrow$ $E = F(\alpha_1, \dots, \alpha_n)$

If $\sigma \in \mathrm{Gal}(E/F)$ $\Rightarrow$ $\sigma(a) = a$ $\forall a \in F$ $\Rightarrow$ σ is completely determined by what it does to $\alpha_1, \dots, \alpha_n$.

$$f(\alpha_i) = 0 = a_0 + a_1\alpha_i + \dots + a_n \alpha_i^n$$

$$\Rightarrow \sigma(0) = \sigma(a_0 + a_1 \alpha_i + \dots + a_n \alpha_i^n)$$
$$= a_0 + a_1(\sigma(\alpha_i)) + \dots + a_n(\sigma(\alpha_i))^n = 0$$

$\Rightarrow$ $f(\sigma(\alpha_i)) = 0$ $\Rightarrow$ $\sigma(\alpha_i) = \alpha_j$ for some j.

$\Rightarrow$ $Gal(E/F)$ acts faithfully on $\{\alpha_1, \dots, \alpha_n\}$

This induces an injective homomorphism $Gal(E/F) \to Sym_n$.

Example $E = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$ $E = \mathbb{Q}_f$ where

$$f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

Note that $-1 \in \mathbb{Q}(\sqrt{2}) \Rightarrow -\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ($x^2 - 2$ is minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$)

$\Rightarrow$ There is an injective hom $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \longrightarrow Sym_2$

and $|Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$ $\Rightarrow$ $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong Sym_2$

Fact: Let. $E = F_f$ and $f(x) = f_1(x) \cdots f_m(x) \in F[x]$

$f_i(x) \in F[x]$ irreducible. Assume $\alpha \in E$ is a root of $f_i(x)$. $\Rightarrow$ $\underset{\substack{\uparrow \\ \text{under action of } Gal(E/F)}}{orb}(\alpha)$ = All roots of $f_i(x)$ in E

This means that in general $Gal(E/F) \not\cong Sym_n$

In fact, even if $f(x)$ irreducible it's still possible that $Gal(E/F) \not\cong Sym_n$

Example $E = \mathbb{Q}(\sqrt[4]{2}, i)$, $F = \mathbb{Q}$ $\Rightarrow$

$E = \mathbb{Q}_f$ where $f(x) = x^4 - 2$. $\leftarrow$ irreducible in $\mathbb{Q}[x]$

$\Rightarrow E = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2})$ Non-trivial polynomial relationship between roots

Observe $(\sqrt[4]{2})^2 + (i\sqrt[4]{2})^2 = 0$.

$\sigma \in Gal(E/\mathbb{Q}) \Rightarrow (\sigma(\sqrt[4]{2}))^2 + (\sigma(i\sqrt[4]{2}))^2 = \sigma(0) = 0$

must be preserved

$(\sqrt[4]{2})^2 + (-\sqrt[4]{2})^2 \neq 0$

$\Rightarrow \nexists\, \sigma \in Gal(E/\mathbb{Q})$ such that $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma(i\sqrt[4]{2}) = -\sqrt[4]{2}$

$\Rightarrow \ \mathrm{Gal}(E/\mathbb{Q}) \not\cong \mathrm{Sym}_4$

Conclusion:

$\mathrm{Gal}(E/F)$ = Permutations of roots of splitting polynomial which preserve all polynomial relationships between them.

Fundamental Theorem of Galois Theory

E/F Galois. There is a bijection of sets:

$$\left\{ \begin{matrix}\text{Intermediate} \\ \text{subfields}\end{matrix} \ F \subset K \subset E \right\} \longleftrightarrow \{\text{subgroups } H \subset \mathrm{Gal}(E/F)\}$$

$$K \longrightarrow \left\{ \sigma \in \mathrm{Gal}(E/F) \mid \begin{matrix}\sigma(k) = k \\ \forall k \in K\end{matrix} \right\} = \mathrm{Gal}(E/K)$$

K/F Galois $\Longleftrightarrow$ $\mathrm{Gal}(E/K) \triangleleft \mathrm{Gal}(E/F)$
and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$

Solving an Equation by Radicals

Q/ Does there exist a version of quadratic formula for polynomials of degree ≥ 3?

Examples

1. $f(x) = x^2 - x - 1$. Quadratic formula $\Rightarrow \frac{1 \pm \sqrt{5}}{2}$ are roots
$\Rightarrow \ \mathbb{Q}_f = \mathbb{Q}(\sqrt{5})$

2/ $f(x) = x^3 - 2 \Rightarrow \mathbb{Q}_f = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$

$$\mathbb{Q} \subset \mathbb{Q}(e^{\frac{2\pi i}{3}}) \subset \mathbb{Q}(e^{\frac{2\pi i}{3}})(\sqrt[3]{2})$$
$$= \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$$

Notice in both cases we can get to splitting field by sucessively adjoing n^{th} roots of elements. radicals

<u>Observation</u> If there is a version of the quadratic formula for any $f(x) \in \mathbb{Q}[x]$ all roots can can be constructed by doing basic algebraic operations and sucessively taking radicals.

<u>Definition</u> A <u>tower of radical extensions</u> of $\mathbb{Q}$ is a nested chain of field extensions:

$$\underset{K_0}{\overset{\|}{\mathbb{Q}}} \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

s.t.

Say K_{i+1}/K_i a radical extension

1/ $K_{i+1} = K_i(\alpha_i)$ where α_i is a root of a polynomial of the form $x^{n_i} - b_i \in K_i[x]$.

2/ $e^{\frac{2\pi i}{n}} \in K_1$ where $n = \prod_i n_i$ ← This is a non-standard condition I am imposing to simplify the exposition

and $K_m/\mathbb{Q}$ Galois.

<u>Fact</u> : K_i/K_{i-1} Galois and $Gal(K_i/K_{i-1})$ <u>Abelian</u>.

<u>Definition</u> We say $f(x)$ is <u>soluble by radicals</u> if $\mathbb{Q}_f \subset K_m$ for some tower of radical extensions

Succession of radical extensions as above

<u>Fundamental Theorem</u> $\Rightarrow$

$$K_m \supset K_{m-1} \supset \cdots\cdots K_2 \supset K_1 \supset \mathbb{Q} = K_0$$

$$\Updownarrow$$

$$\{e\} \lhd \mathrm{Gal}(K_m/K_{m-1}) \lhd \cdots \mathrm{Gal}(K_m/K_2) \lhd \mathrm{Gal}(K_m/K_1) \lhd \mathrm{Gal}(K_m/\mathbb{Q})$$

where $\dfrac{\mathrm{Gal}(K_m/K_{i-1})}{\mathrm{Gal}(K_m/K_i)} \cong \mathrm{Gal}(K_i/K_{i-1}) = \text{Abelian}$

$\Rightarrow$ <u>Simple components</u> of $\mathrm{Gal}(K_m/\mathbb{Q})$ are <u>cyclic</u> (ie $\mathbb{Z}/p\mathbb{Z}$, p prime)

We call such groups <u>solvable</u>.

Abelian $\Rightarrow$ Solvable , Solvable $\not\Rightarrow$ Abelian.

structure theorem for finite Abelian groups

e.g. $\{e\} \subsetneq \mathrm{Alt}_3 \subsetneq \mathrm{Sym}_3$

<u>Fact</u> : G solvable $\Rightarrow$ All subgroups are solvable <u>and</u> G/H solvable $\forall\, H \lhd G$.

Hence, $\mathbb{Q} \subset \mathbb{Q}_f \subset K_m$

$$\Rightarrow \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \cong \frac{\mathrm{Gal}(K_m/\mathbb{Q})}{\mathrm{Gal}(K_m/\mathbb{Q}_f)}$$

$\Rightarrow \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ solvable finite group.

<u>Conclusion</u>

$\exists$ version of quadratic formula for $f(x) \in \mathbb{Q}[x]$ $\Rightarrow$ $\mathbb{Q}_f$ contained in a tower of radical extensions $\Rightarrow$ $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ Solvable

f soluble by radicals

Said another way :

Gal ($\mathbb{Q}_f / \mathbb{Q}$) <u>not</u> solvable $\Rightarrow$ $\nexists$ version of the quadratic formula for $f(x) \in \mathbb{Q}[x]$

<u>Fact</u> : If $f(x) \in \mathbb{Q}[x]$, $\deg(f(x)) = 5$, irreducible, has exactly 3 real roots then $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \cong \mathrm{Sym}_5$.

For example, $f(x) = x^5 + x^2 - 1/4$.

Recall $\{e\} \triangleleft \mathrm{Alt}_5 \triangleleft \mathrm{Sym}_5$ and

$\mathrm{Sym}_5 / \mathrm{Alt}_5 \cong \mathbb{Z}/2\mathbb{Z}$, Alt_5 are simple

$\Rightarrow$ Simple components of $\mathrm{Gal}(K_f/\mathbb{Q})$ are $(\mathbb{Z}/2\mathbb{Z}, \mathrm{Alt}_5)$.

non-abelian

$\Rightarrow$ $\mathrm{Gal}(K_f/\mathbb{Q})$ not solvable

$\Rightarrow$ $f(x) = x^5 - x^2 - 1/4$ <u>not</u> solvable by radicals.

$\Rightarrow$ There is no version of quadratic formula for degree 5 polynomials $\leftarrow$ Same for all degrees ≥ 5

<u>Conjecture</u>: Given <u>any</u> finite group G, $\exists$ $E/\mathbb{Q}$ a Galois extension s.t. $G \cong \mathrm{Gal}(E/\mathbb{Q})$.

ie all finite symmetries can be realized by by considering zeroes of polynomials with rational coefficients.