Groups & Rings: Lecture #25

Galois theory

- Statement of fundamental theorem
- Automorphisms and fixed field
- The Galois correspondence
- Example: finite fields
- ~~Example: cyclotomic extensions of $\mathbb{Q}$~~
- ~~On the proof of the correspondence~~
- Application: solvability by radicals (early 1800's)
- ~~Application: $\mathbb{C}$ is algebraically closed~~

Statement of the fundamental theorem

Def: Let E/F be a field extension.

(i) E/F separable if the minimal polynomial of any $\alpha \in E$ has no repeated roots (in splitting field of α).

(all ext's in char 0 are separable as well as ext. of finite fields)

(ii) E/F normal if the minimal polynomial of any $\alpha \in E$ has all its roots in E (i.e., E contains a splitting field of α).

(iii) E/F Galois if finite + separable + normal.

Rmk: If $E/K/F$ $(F \subset K \subset E)$ then

E/F Galois $\Rightarrow$ E/K Galois (but K/F need not be Galois)

Later, we will to every Galois extension E/F associate a group $Gal(E/F)$, the Galois group.

Theorem 23.22 (Fundamental theorem of Galois theory)

Let E/F Galois extension. There is a one-to-one corr.

$$\left\{ \begin{array}{c} \text{intermediate field ext's} \\ E/K/F \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{subgroups} \\ H \leq Gal(E/F) \end{array} \right\}$$

subgroup

Moreover:

(i) K/F normal $\Leftrightarrow$ H normal subgroup

(ii) $[E:F] = |Gal(E/F)|$ and more precisely $[E:K] = |H|$

(iii) $K = E \longleftrightarrow H = \{e\}$ trivial

$K = F \longleftrightarrow H = Gal(E/F)$ improper

Automorphisms and fixed fields

Def/Prop 23.2: Let E/F field extension. The set

$$\mathrm{Aut}(E/F) = \{\sigma : E \to E \text{ isomorphism of fields} : \overbrace{\sigma|_F = id_F}^{\sigma(a)=a\ \forall a\in F}\}$$

of automorphisms of E fixing F is a group under composition.
↑ exercise

Def: If E/F is Galois, then $\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$.

Examples:

(1) $\mathbb{C}/\mathbb{R}$ is Galois $\left(\text{min pol of } \alpha\in\mathbb{C},\ \alpha\notin\mathbb{R} \text{ is } (z-\alpha)(z-\bar\alpha) = z^2 - \mathrm{Re}(\alpha)z - |\alpha|^2\right)$

basis $1, i$

$\sigma : \mathbb{C} \to \mathbb{C}$ $\quad \sigma \in \mathrm{Aut}(E/F)$

$1 \mapsto 1$ (b/c σ fixes $\mathbb{R}$)

$i \mapsto \pm i$ (b/c ring homo: roots of x^2+1)

$0 = \sigma(0) = \sigma(i^2+1) \overset{\text{ring homo}}{=} \sigma(i)^2 + 1 \Rightarrow \sigma(i) = \pm i$

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{id, \tau\} = \langle\tau\rangle = \mathbb{Z}/2\mathbb{Z}$$
$$[\mathbb{C}:\mathbb{R}] = |\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2$$

↑ complex conj.

(2) $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ also Galois. $\quad \sigma : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}(\sqrt{D})$

basis $1, \sqrt{D}$

$1 \mapsto 1$

$\sqrt{D} \mapsto \pm\sqrt{D}$

with Galois group $\mathbb{Z}/2 = \langle\tau\rangle$

↑ conjugation: $\tau(\sqrt{D}) = -\sqrt{D}$

(3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ not Galois (not normal)

basis $1, \sqrt[3]{2}, \sqrt[3]{4}$ $\quad$ min pol of $\sqrt[3]{2}$ is x^3-2 $\quad$ roots: $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$ (ζ: 3^{rd} root of unity)

$\zeta = e^{\frac{2\pi i}{3}} \in \mathbb{C}\setminus\mathbb{R} \Rightarrow \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$

$\Rightarrow$ extension not normal

$$\sigma : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2})$$

only 1 root in $\mathbb{Q}(\sqrt[3]{2})$

$$1 \longmapsto 1$$
$$\sqrt[3]{2} \longmapsto \text{root of } x^3-2 = \sqrt[3]{2}$$
$$\sqrt[3]{4} = (\sqrt[3]{2})^2 \longmapsto (\sqrt[3]{2})^2 = \sqrt[3]{4}$$

$$\Rightarrow \mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right) = \{id\}$$

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 1 = \left|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})\right|$$

"too few automorphism" (similar problem if E/F inseparable)

<u>Def/Cor 23.14</u>: Let E/F be a field extension and $H \leq \mathrm{Aut}(E/F)$.
The fixed set of H is

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \ \ \forall \sigma \in H\} \subseteq E$$

a field containing F (so an intermediate extension $E/E^H/F$).

exercise

In Examples (1) & (2): $\mathrm{Gal}(E/F) = \mathbb{Z}/2\mathbb{Z} = \langle \tau \rangle$ conjugation

and $E^{\mathbb{Z}/2\mathbb{Z}} = \{\alpha \in E : \tau(\alpha) = \alpha\} = F$. Indeed:

(1) $\alpha \in \mathbb{C}$, $\tau(\alpha) := \boxed{\overline{\alpha} = \alpha} \Leftrightarrow \alpha \in \mathbb{R}$

(2) $\tau(\underbrace{a + b\sqrt{D}}_{\alpha}) := \boxed{\underbrace{a - b\sqrt{D}}_{\overline{\alpha}} = \underbrace{a + b\sqrt{D}}_{\alpha}} \Leftrightarrow b = 0 \Leftrightarrow \alpha \in \mathbb{Q}$.

But in example (3) (not Galois):

(3) $\mathrm{Aut}(E/F) = \{e\}$, $E^{\mathrm{Aut}(E/F)} = E$ and not F "too few auto."

Ex: $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

deg 4, basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})}_{\substack{\text{deg } 2 \\ \text{basis: } 1, \sqrt{2}}} \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$$

$$\mathbb{Q} \subset \underbrace{\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})}_{\substack{\text{deg } 2 \\ \text{basis: } 1, \sqrt{3}}}$$

$\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

$$\sigma : \mathbb{Q}(\sqrt{2},\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$$

$$\begin{aligned} 1 &\longmapsto 1 \\ \sqrt{2} &\longmapsto \pm\sqrt{2} = \alpha \\ \sqrt{3} &\longmapsto \pm\sqrt{3} = \beta \\ \sqrt{2}\sqrt{3} = \sqrt{6} &\longmapsto \alpha\beta \end{aligned}$$

$\sigma_2(\sqrt{2}) = -\sqrt{2}, \quad \sigma_2(\sqrt{3}) = \sqrt{3}$

$\sigma_3(\sqrt{3}) = -\sqrt{3}, \quad \sigma_3(\sqrt{2}) = \sqrt{2}$

$$\mathrm{Aut}(\,---\,) = \{ id, \sigma_2, \sigma_3, \underbrace{\sigma_2 \circ \sigma_3 = \sigma_3 \circ \sigma_2}_{\substack{\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3}}} \} \cong \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Verify that extension is Galois.

$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle \sigma_2 \rangle} = \{ \alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3}) : \sigma_2(\alpha) = \alpha \} = \mathbb{Q}(\sqrt{3})$$

$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle \sigma_3 \rangle} = \{ \alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3}) : \sigma_3(\alpha) = \alpha \} = \mathbb{Q}(\sqrt{2})$$

$$\begin{aligned} \mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle \sigma_2 \circ \sigma_3 \rangle} &= \{ \alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3}) : \sigma_2 \circ \sigma_3(\alpha) = \alpha \} = \mathbb{Q}(\sqrt{6}) \\ &= \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : b = -b,\ c = -c \} \\ &= \{ a + d\sqrt{6} \} \end{aligned}$$

Intermediate fields

$$\begin{array}{ccccc} & \subset & \mathbb{Q}(\sqrt{2}) & \subset & \\ \mathbb{Q} & \subset & \mathbb{Q}(\sqrt{3}) & \subset & \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ & \subset & \mathbb{Q}(\sqrt{6}) & \subset & \end{array}$$

Subgroups

$$\begin{array}{ccccc} & \geqslant & \langle \sigma_3 \rangle & \geqslant & \\ \mathbb{Z}/2 \times \mathbb{Z}/2 & \geqslant & \langle \sigma_2 \rangle & \geqslant & \{e\} \\ & \geqslant & \langle \sigma_2 \circ \sigma_3 \rangle & \geqslant & \end{array}$$

$$E^H \longleftarrow\!\!| \quad H \leq \mathrm{Gal}(E/F)$$

The Galois correspondence

Let E/F Galois extension. The Galois correspondence:

$$\{E/K/F\} \longleftrightarrow \{H \leq \mathrm{Gal}(E/F)\}$$

$$E^H \longleftarrow\!\!| \quad H$$

$$K \longmapsto \mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$$

<u>Rmk</u>: Small/big field extension $\longleftrightarrow$ Big/small subgroup.

smallest $K = F$ $\longleftrightarrow$ $\mathrm{Gal}(E/F)$ whole group

biggest $K = E$ $\longleftrightarrow$ $\mathrm{Gal}(E/E) = \{id\}$ trivial subgroup

<u>Reason</u>: Galois correspondence is inclusion-reversing:

$$F \subset K \subset L \subset E \longleftrightarrow \mathrm{Gal}(E/F) \geq \mathrm{Gal}(E/K) \geq \mathrm{Gal}(E/L) \geq \mathrm{Gal}(E/E)$$

<u>Rmk</u>: $[K:F] = \dfrac{[E:F]}{[E:K]} = \dfrac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/K)|} = [\mathrm{Gal}(E/F) : \underbrace{\mathrm{Gal}(E/K)}_{H}]$

degree (K/F) = index (H in $\mathrm{Gal}(E/F)$)

Example: finite fields

$F = \mathbb{F}_{p^f} \subseteq E = \mathbb{F}_{p^e}$ $\quad e \geq f$ $\quad$ (actually $f | e$, $p^e = (p^f)^{[E:F]}$)

$\Rightarrow e = f[E:F]$

Claim (Cor 23.8) E/F is Galois and $Gal(E/F) \cong \mathbb{Z}/p^{e-f}\mathbb{Z}$

is cyclic and generated by the f^{th} Frobenius:

$$\phi : E \longrightarrow E$$
$$a \longmapsto a^{p^f}$$

To see this:

(1) $|Gal(E/F)| = [E:F] = p^{e-f}$ so order of group correct.

(2) $\phi \in Aut(E/F)$ because $a \in F \Rightarrow a^{p^f} = a \Rightarrow \phi(a) = a$

and ϕ ring homo b/w fields $\Rightarrow$ injective $\xRightarrow{|E| \text{ finite}}$ surjective.

(3) $\{id, \phi, \phi^2, \phi^3, \dots, \phi^{p^{e-f}-1}\}$ all different

b/c $\phi^n \neq id$ if $n = 1, 2, \dots, p^{e-f}-1$.

Indeed, $\phi^n = id$ means $\underbrace{x^{np^f} = x}_{\text{has } np^f \text{ roots}}$ $\forall x \in \underbrace{E}_{\text{has } p^{e-f} \text{ elts}}$ which is impossible.

(4) $\phi^{p^{e-f}} = id$ b/c $(x^{p^f})^{p^{e-f}} = x^{p^e} = x$ $\quad \forall x \in E$.

Conclusion: $\underbrace{Aut(E/F)}_{\text{order } p^{e-f}} \geq \langle \phi \rangle = \underbrace{\{1, \phi, \dots, \phi^{p^{e-f}-1}\}}_{p^{e-f} \text{ elts}}$

Consequence: $\mathbb{F}_{p^e} / K / \mathbb{F}_{p^f} \longleftrightarrow$ subgroups of $\mathbb{Z}/p^{e-f}\mathbb{Z}$

$\updownarrow$

divisors of $e-f$

Solvability by radicals

Ex: $x^2 + px + q = 0 \iff x = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$

Ex: $x^3 + px + q = 0$ has solutions: (Cardano's formula 1545)

no x^2-term (can be eliminated by $x \mapsto x + d$)

$$x = \sqrt[3]{\underbrace{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}_{\alpha_1}} + \sqrt[3]{\underbrace{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}_{\alpha_2}}$$

+ 2 more complex roots

$x = \sqrt[3]{\alpha_1} + \sqrt[3]{\alpha_2}$, α_1, α_2 roots of $z^2 + qz - p^3/27$

other roots: $x = \zeta \sqrt[3]{\alpha_1} + \zeta^2 \sqrt[3]{\alpha_1}$, where $\zeta^3 = 1$

Remark: Solving $p(x) = 0$ by radicals

$\iff$ splitting field of $p(x)$ over $\mathbb{Q}$ is contained in an iterated extension of the form $F(\sqrt[n]{\alpha})/F$.

Facts: (If F contains all roots of unity then)

- Splitting field E of $x^n - \alpha$ $(\alpha \in F)$ has **abelian** Galois group $Gal(E/F)$
- If E/F Galois and $Gal(E/F)$ cyclic $\Rightarrow$ E/F is radical extension

Consequence: Let $p(x) \in \mathbb{Q}[x]$ and let E be its splitting field.

Then $p(x)$ can be solved with radicals $\iff$ $Gal(E/F)$ is solvable

<u>Def</u>: A group G is solvable if it is an iterated extension of abelian groups, that is, $\exists \{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ such that G_i/G_{i-1} abelian for $i = 1, 2, \dots, n$.

(Lecture #8?)

<u>Fact</u>: S_5 is <u>not solvable</u> because $A_5 \triangleleft S_5$ and A_5 is <u>simple</u>

$\Longrightarrow$ in general, quintics cannot be solved by radicals ($\exists\, p(x) \in \mathbb{Q}[x]$ of deg 5 w/ $Gal(E/\mathbb{Q}) = S_5$.)

<u>Explicit example</u>: $p(x) = x^5 - x - 1$

The Galois group of the splitting field of $p(x)$, $\deg p(x) \leq 4$ is a subgroup of S_4 and these are always solvable.

<u>Example</u>: S_4 is solvable (an iterated ext of abelian groups):

$$\{e\} \triangleleft H \triangleleft A_4 \triangleleft S_4$$

1   4   12   24

- A_4 = even permutations
- $H = \{id, (12)(34), (13)(24), (14)(23)\}$

$$\boxed{\begin{aligned} S_4/A_4 &\simeq \mathbb{Z}/2 \\ A_4/H &\cong \mathbb{Z}/3 \\ H/\{e\} &\cong \mathbb{Z}/2 \times \mathbb{Z}/2 \end{aligned}}$$

abelian