Eine Woche, ein Beispiel

7.30. Galois correspondence

This is a continuation of [2023.06.04]. I think maybe it is better to make it a series (since this topic is a bit too fundamental and basic), but I am still not sure if I will keep updating this series. Let us see.

Last time.
- field extension
- Galois = normal + seperable
- $\mathrm{Gal}(E/F) := \mathrm{Aut}_{F\text{-alg}}(E)$

Today
- compliment of last time
- Galois correspondence.

Ex. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois (why?), and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

A. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[T]/(T^2-2)$

$$\phi: \mathbb{Q}[T]/(T^2-2) \longrightarrow \mathbb{Q}[T]/(T^2-2)$$
$$T \longmapsto \phi(T) = ?$$

The question reduces to solving the equation

$$x^2 - 2 = 0 \quad \text{in} \quad \mathbb{Q}[T]/(T^2-2)$$
$$(x-T)(x+T) = 0$$

ex. Check that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \{T \mapsto T,\ T \mapsto -T\} \cong \mathbb{Z}/2\mathbb{Z}$$

Lemma. Let E/F be field extension, $\phi \in \mathrm{Aut}_{F\text{-alg}}(E)$, $x \in E$. If for some $a_i \in F$,

$$a_n x^n + \cdots + a_0 = 0,$$

then

$$a_n (\phi(x))^n + \cdots + a_0 = 0.$$

Ex. Let $E = \mathbb{F}_2[T]/(T^2+T+1)$, then $E/\mathbb{F}_2$ is Galois, and $\mathrm{Gal}(E/\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$.

⚠ $E \not\cong \mathbb{Z}/4\mathbb{Z}$ as abelian gp!

Ex. $F := \mathbb{F}_2(T)$, $F(\sqrt{T})/F$ is not Galois, and $\mathrm{Aut}_{F\text{-alg}}(F(\sqrt{T})) \cong \{Id\}$.

A. $F(\sqrt{T}) = F[S]/(S^2-T)$

$$\phi: F[S]/(S^2-T) \longrightarrow F[S]/(S^2-T)$$
$$S \longmapsto \phi(S) = ?$$

The question reduces to solving the equation

$$x^2 - T = 0 \quad \text{in} \quad F(\sqrt{T}) = F[S]/(S^2-T)$$
$$(x-S)(x+S) = 0$$

ex. Check that $S = -S$, so $\mathrm{Aut}_{F\text{-alg}}(F(\sqrt{T})) \cong \mathbb{Z}/2\mathbb{Z}$.

Eisenstein criterion [wiki]

Thm. Let $f(T)=a_nT^n+\cdots+a_0\in\mathbb{Z}[T]$, if
$p\nmid a_n$, $p\mid a_{n-1},\dots,a_0$, $p^2\nmid a_0$,
then $f(T)\in\mathbb{Q}[T]$ is irreducible.

E.g. 1) $f(T)=3T^4+15T^2+10 \in\mathbb{Q}[T]$ is irreducible.

2) $f(T)=T^2+T+2 \in\mathbb{Q}[T]$ is irreducible, since
$f(T+3)=T^2+7T+14 \in\mathbb{Q}[T]$ is irreducible.

3) $f(T)=2T^5+4T^2-3 \in\mathbb{Q}[T]$ is irreducible, since
$T^5f(\frac{1}{T})=2+4T^3-3T^5 \in\mathbb{Q}[T]$ is irreducible.

If $f(T)=g(T)h(T)$, then
$f(T+3)=g(T+3)h(T+3)$
$T^5f(\frac{1}{T})=T^5g(\frac{1}{T})h(\frac{1}{T})=T^{\deg g}g(\frac{1}{T})\cdot T^{\deg f}f(\frac{1}{T})$.

E.g. $\Phi_p(T):=\dfrac{T^p-1}{T-1}=T^{p-1}+\cdots+1 \in\mathbb{Q}[T]$ is irreducible, since
$\Phi_p(T+1)=\cdots\cdots \in\mathbb{Q}[T]$ is irreducible.

Rmk. A reminder for Gauss's lemma. [wiki: Gauss's lemma]

Def. $F(T):=a_nT^n+\cdots+a_0\in\mathbb{Z}[T]$ is primitive, if $\gcd(a_n,\dots,a_0)=1$.

Lemma (Primitivity)
$P(T),Q(T)\in\mathbb{Z}[T]$ primitive $\Rightarrow$ $P(T)Q(T)\in\mathbb{Z}[T]$ primitive.

Lemma (Irreducibility) For $F(T)\in\mathbb{Z}[T]$ nonconstant,
$$F(T)\in\mathbb{Z}[T]\text{ is irr}\iff\begin{cases}F(T)\in\mathbb{Q}[T]\text{ is irr}\\ F(T)\in\mathbb{Z}[T]\text{ is primitive}\end{cases}$$

Continuation of examples.

$\mathbb{Q}(\zeta_p)=\mathbb{Q}[T]/(\Phi_p(T))$ $\qquad Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong(\mathbb{Z}/p\mathbb{Z})^\times$

$\mathbb{Q}(\sqrt{2+\sqrt{2}})=\mathbb{Q}[T]/((T^2-2)^2-2)$ $\qquad Gal(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})\cong\mathbb{Z}/4\mathbb{Z}$

Suppose $\operatorname{char}F=p$, $a\in F$, $x^p-x-a\in F[x]$ irr.
Let $E:=F[T]/(T^p-T-a)$, then $Gal(E/F)\cong\mathbb{Z}/p\mathbb{Z}$.

We do the rest of examples in Galois correspondence.

Thm (Galois correspondence / Fundamental theorem of Galois theory)

Let E/F be any (finite) Galois extension.

We have one-to-one correspondence

$$\{L/F \text{ field extension}, L \subseteq E\} \xleftrightarrow{1:1} \{H \leqslant \mathrm{Gal}(E/F) \text{ closed subgp}\}$$

$$\cup \qquad\qquad\qquad\qquad \cup$$

$$\{L/F \text{ normal extension}, L \subseteq E\} \xleftrightarrow{1:1} \{H \triangleleft \mathrm{Gal}(E/F) \text{ closed subgp}\}$$

↑ comes from "normal subgp"

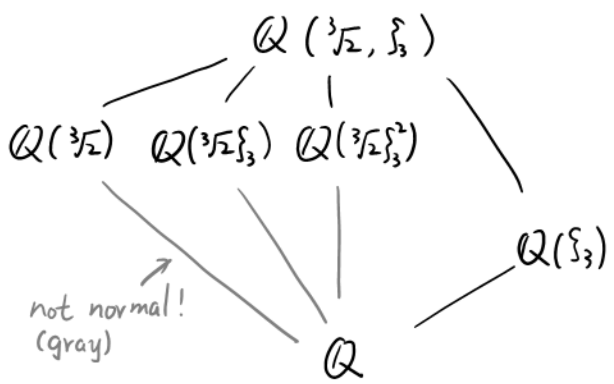
also considered as data

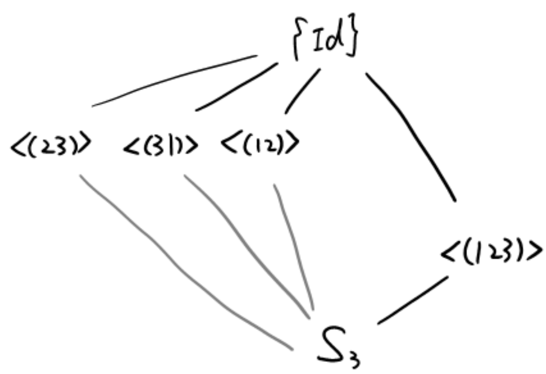
$$L \longmapsto \mathrm{Gal}(E/L)$$

$$E^H \longleftarrow\!\shortmid\; H$$

$$\mathrm{Gal}(E/F)\left\{\begin{array}{lll} E & & \\ | & \mathrm{Gal}(E/L) & \text{subgp} \\ L & & \\ | & & \text{quotient} \\ F & & \text{when } L/F \text{ Galois} \end{array}\right. \qquad \begin{array}{ccc} \mathrm{Spec}\,E & E & \{\mathrm{Id}\} \\ \downarrow & | & \cap \\ \mathrm{Spec}\,L & L & \mathrm{Gal}(E/L) \\ \downarrow & | & \cap \\ \mathrm{Spec}\,F & F & \mathrm{Gal}(E/F) \end{array}$$

Eg. $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong S_3 \circlearrowright \{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$

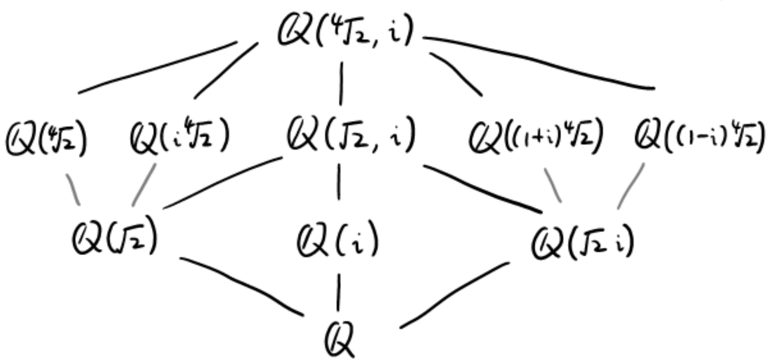


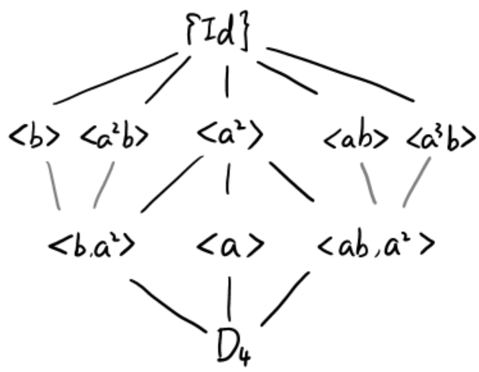


Eg. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4 = \langle a, b \mid a^4 = b^2 = 1,\ bab = a^{-1} \rangle$

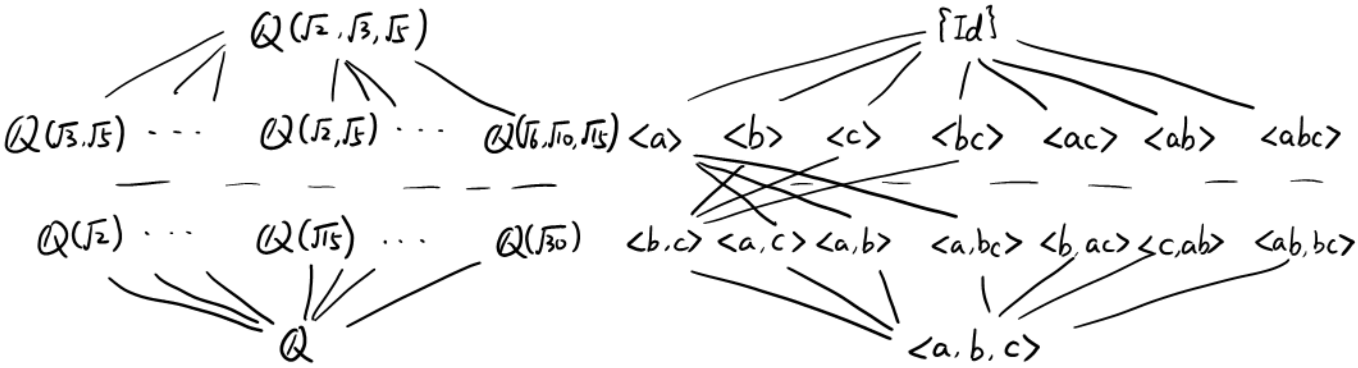
$a: i \longmapsto i,\quad \sqrt[4]{2} \longmapsto i\sqrt[4]{2} \qquad b: i \longmapsto -i,\quad \sqrt[4]{2} \longmapsto \sqrt[4]{2}$





E.g. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}) \cong \underset{a}{\mathbb{Z}/2\mathbb{Z}} \oplus \underset{b}{\mathbb{Z}/2\mathbb{Z}} \oplus \underset{c}{\mathbb{Z}/2\mathbb{Z}}$$



$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},u)/\mathbb{Q}) \cong Q_8$ where $u^2 = (9-5\sqrt{3})(2-\sqrt{2})$ (too technical!)

E.g. $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$a: \zeta_8 \mapsto \zeta_8^3 \quad b: \zeta_8 \mapsto \zeta_8^5$

$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ with intermediate field

$$\mathbb{Q}(\zeta_5) \cap \mathbb{R} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$$

Rmk In general, for $p>3$ prime,

$$\mathbb{Q}(\zeta_p) \supset \mathbb{Q}(\zeta_p) \cap \mathbb{R} \supset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$$

$$\Rightarrow \quad \mathbb{Q}(\zeta_p) \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$$

Conclusion

Galois extension $\underset{\text{Galois inverse problem}}{\overset{\longrightarrow}{\dashleftarrow}}$ Galois group

special field	
finite	finite
simple + sep	finite many subgps
abelian	abelian
cyclic	cyclic
solvable	solvable
without intermediate normal field extension	simple
	semidirect product gp
	Sylow p-subgp

For functional fields, we can translate them as (ramified) covers and discuss unramified field extension as well as unramified subgroup.
You may see this:
https://github.com/ramified/personal_handwritten_collection/blob/main/scattered/%E4%BB%A3%E6%95%B0%E5%9F%BA%E6%9C%AC%E7%BE%A4.pdf