

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 + separable
- $\text{Gal}(E/F) := \text{Aut}_{F\text{-alg}}(E)$

Today

- complement of last time
- Galois correspondence.

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

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

ex. Check that

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

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

If for some $a_i \in F$,

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

then

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

Ex. Let $E = \mathbb{F}_2[T]/(T^2+T+1)$, then E/\mathbb{F}_2 is Galois, and $\text{Gal}(E/\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$.
⚠ $E \not\cong \mathbb{Z}/4\mathbb{Z}$ as abelian gp!

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

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

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

Eisenstein criterion [wiki]

Thm. Let $f(T) = a_n T^n + \dots + a_0 \in \mathbb{Z}[T]$, 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
 $T^5 f(\frac{1}{T}) = 2 + 4T^3 - 3T^5 \in \mathbb{Q}[T]$ is irreducible.

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

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

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

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

Lemma (Primitivity)

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

Lemma (Irreducibility) For $F(T) \in \mathbb{Z}[T]$ nonconstant,

$$F(T) \in \mathbb{Z}[T] \text{ is irr} \Leftrightarrow \begin{cases} F(T) \in \mathbb{Q}[T] \text{ is irr} \\ F(T) \in \mathbb{Z}[T] \text{ is primitive} \end{cases}$$

Continuation of examples.

$$\begin{aligned} \mathbb{Q}(\sqrt{p}) &= \mathbb{Q}[T]/(\Phi_p(T)) & \text{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) &\cong (\mathbb{Z}/p\mathbb{Z})^\times \\ \mathbb{Q}(\sqrt{2+\sqrt{2}}) &= \mathbb{Q}[T]/((T^2-2)^2-2) & \text{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}) &\cong \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

Suppose $\text{char } F = p$, $a \in F$, $x^p - x - a \in F[x]$ irr.

Let $E = F[T]/(T^p - T - a)$, then $\text{Gal}(E/F) \cong \mathbb{Z}/p\mathbb{Z}$.

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

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

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

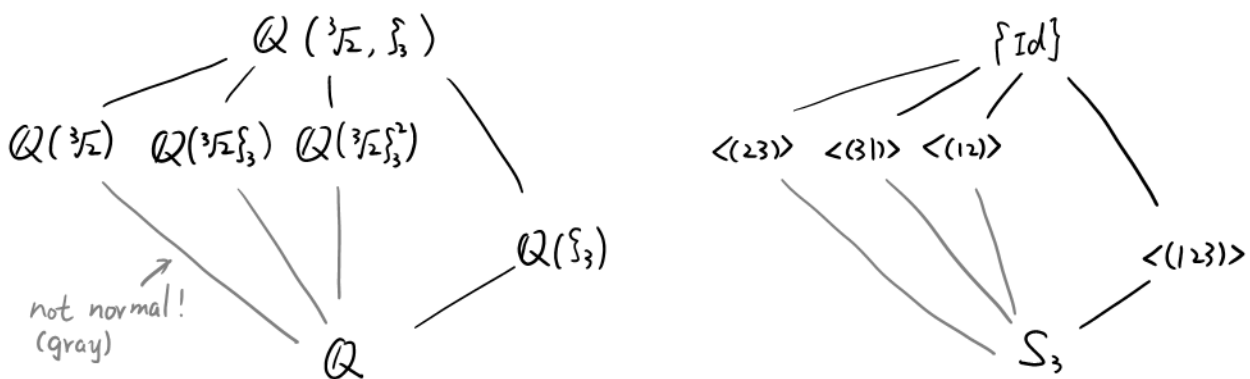
↑ comes from "normal subgroup"

$$\begin{array}{ccc} L & \xrightarrow{\quad} & \text{Gal}(E/L) \\ E^H & \xleftarrow{\quad} & H \end{array}$$

also considered as data

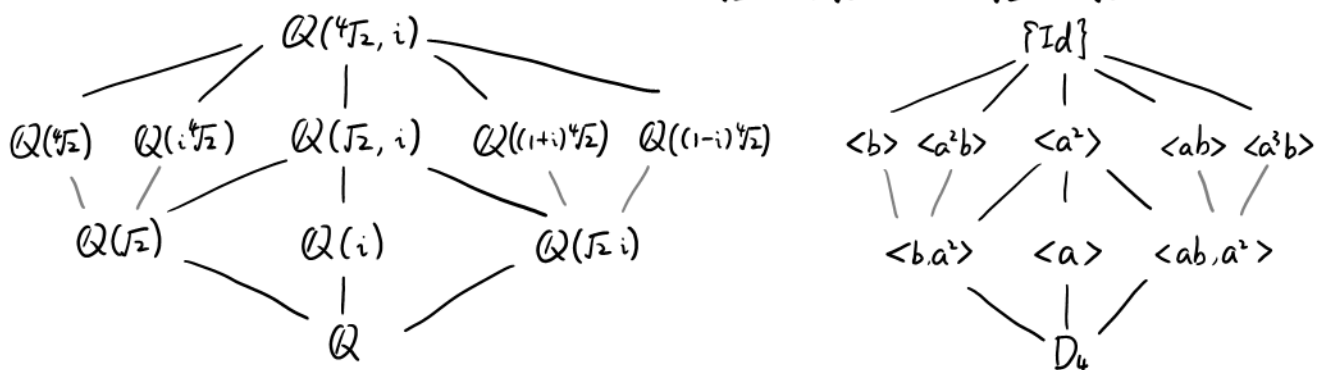
$$\begin{array}{ccccc} \text{Gal}(E/F) & \left\{ \begin{array}{l} E \\ | \\ \text{Gal}(E/L) \text{ subgroup} \\ | \\ L \\ | \\ F \end{array} \right. & & \begin{array}{ccc} \text{Spec } E & E & \{Id\} \\ \downarrow & | & \cap \\ \text{Spec } L & L & \text{Gal}(E/L) \\ \downarrow & | & \cap \\ \text{Spec } F & F & \text{Gal}(E/F) \end{array} \\ & & \text{quotient} & & \\ & & \text{when } L/F \text{ Galois} & & \end{array}$$

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

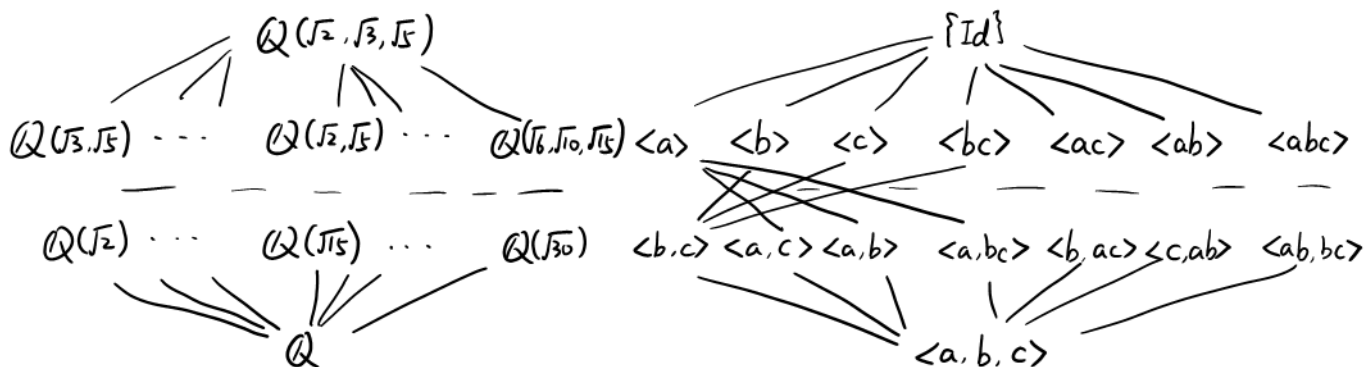


Eg. $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
 $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$

$$\begin{array}{ll} a: i \mapsto i & b: i \mapsto -i \\ \sqrt[4]{2} \mapsto i\sqrt[4]{2} & \sqrt[4]{2} \mapsto \sqrt[4]{2} \end{array}$$



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



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

E.g. $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
 $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ with intermediate field $\mathbb{Q}(\zeta_5) \cap \mathbb{R} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$
 $a: \zeta_8 \mapsto \zeta_8^3 \quad b: \zeta_8 \mapsto \zeta_8^5$

Rmk In general, for $p > 3$ prime,
 $\mathbb{Q}(\zeta_p) \supset \mathbb{Q}(\zeta_p) \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$
 $\Rightarrow \mathbb{Q}(\zeta_p) \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$

People have methods to compute many Galois groups, see here:
<https://mathoverflow.net/questions/22923/computing-the-galois-group-of-a-polynomial>

Conclusion

Galois extension	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

Examples

1. Finite field

In this section, F/\mathbb{F}_p fin extension, $\#F = p^n$.

Prop 1. F^\times is a cyclic gp.

Reason. 1) F^\times is abelian, $\#F^\times = p^n - 1$

\Rightarrow can use classifications of f.g. abelian gp

2) $x^{p^n-1} - 1 = \prod_{\alpha \in F^\times} (x - \alpha)$ \Rightarrow $\# 0 < k < p^n - 1, k \mid p^n - 1$ s.t.
 $x^k - 1$ has at most k roots $\forall \alpha \in F^\times, \alpha^k - 1 = 0$

Def. $\alpha \in F^\times$ is primitive, if $\langle \alpha \rangle_{gp} = F^\times$.

For $k \in \mathbb{N}_{>0}$ and a general field F s.t. $\mu_k(F^\times) \cong \mathbb{Z}/k\mathbb{Z}$,

$\alpha \in F^\times$ is a primitive k -th root of unity, if $\langle \alpha \rangle_{gp} = \mu_k(F^\times)$

We fix $\zeta_k \in F^\times$ as a primitive k -th root of unity later on.

Cor. $F \cong \mathbb{F}_p(\zeta_{p^n-1})$

Rmk <https://math.stackexchange.com/questions/295679/roots-of-unity-in-mathbb-q-p>

In ptc. in $\mathbb{Q}_p, p \neq 2$,

$k \mid p-1 \iff \exists$ some primitive k -th root of unity.

Prop 2. $\exists!$ field of size p^n (as abstract field)

To be exact, let

$F' :=$ the splitting field of $x^{p^n} - x$ over \mathbb{F}_p ,

then $\#F' = p^n$, and $F \cong F'$.

Reason. $\#F' = p^n$:

$F'' := \{x \in F' \mid x^{p^n} = x\} \subseteq F'$ is a subfield with $\#F'' = p^n$.

$x^{p^n} - x$ splits over $F'' \xrightarrow{\text{def of } F'} F'' = F'$

$F \cong F', x^{p^n} - x$ splits over $F \xrightarrow{\#F' = \#F = p^n} F' \hookrightarrow F$
 $\xrightarrow{\#F' = \#F = p^n} F' \cong F$

Cor. $\exists \mathbb{F}_{p^r} \hookrightarrow \mathbb{F}_{p^s} \iff r \mid s$

Prop 3. $\text{Gal}(F/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ is generated by

$\text{Frob}: F \longrightarrow F \quad x \longmapsto x^p$

Reason: $F^{\text{Frob}} = \mathbb{F}_p$

Prop 4. Fix p prime. For $d \in \mathbb{N}_{\geq 1}$, let

$$\mathcal{P}_d := \{f(x) \in \mathbb{F}_p[x] \mid f \text{ monic irr, } \deg f = d\} \quad N_p(d) := \#\mathcal{P}_d$$

then

$$1) \quad x^{p^n} - x = \prod_{d|n} \prod_{f(x) \in \mathcal{P}_d} f(x)$$

$$2) \quad N_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} = \frac{p^n}{n} + O\left(\frac{p^{\frac{n}{2}}}{n}\right)$$

Reason:

$$1) \quad x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha) = \prod_{d|n} \prod_{f(x) \in \mathcal{P}_d} \prod_{\min(\alpha, F) = f} (x - \alpha) = \prod_{d|n} \prod_{f(x) \in \mathcal{P}_d} f(x)$$

$$2) \quad 1) \Rightarrow p^n = \sum_{d|n} d N_p(d)$$

$$\xrightarrow{\text{Möbius}} N_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

Ex. For $i \in \mathbb{N}_{>0}$, show that

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} 0, & (q-1) \nmid i \\ -1, & (q-1) \mid i \end{cases} \quad \text{in } \mathbb{F}_q$$

e.g. for $x \in \mathbb{F}_q^n$, denote $x^I := x_1^{i_1} \cdots x_n^{i_n}$. When $\exists i_k, 0 \leq i_k < q-1$,

$$\sum_{x \in \mathbb{F}_q^n} x^I = 0 \quad \text{in } \mathbb{F}_q$$

Ex. \mathbb{F}_q is a C_1 -field, i.e.,

for $d < n$, $f(z_1, \dots, z_n) \in \mathbb{F}_q[z_1, \dots, z_n]_d$, $\exists x \in \mathbb{F}_q^n - \{0\}$ s.t. $f(x) = 0$.

$$\text{IA: } 0 = \sum_{x \in \mathbb{F}_q^n} (1 - (f(x_1, \dots, x_n)^{q-1})) = \#\{x \in \mathbb{F}_q^n \mid f(x) = 0\} \pmod{p}.$$

In general: https://en.wikipedia.org/wiki/Chevalley%E2%80%93Warning_theorem

degree 3 Galois extension:

<https://math.stackexchange.com/questions/2017810/galois-group-of-the-irreducible-cubic-equation-x3-3x1>

cyclic field:

<https://math.stackexchange.com/questions/4038049/necessity-for-n-th-roots-of-unity-in-simple-kummer-extension>