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.

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

<u>Today</u>
- 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 $\mathrm{Aut}_{F\text{-alg}}(F(\sqrt{T})) \cong \{\mathrm{Id}\}$.

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

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

E.g. $\Phi_p(T) := \frac{T^p - 1}{T - 1} = T^{p-1} + \cdots + 1 \in \mathbb{Q}[T]$ 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. $F(T) := a_n T^n + \cdots + a_0 \in \mathbb{Z}[T]$ 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

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

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

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

↑ comes from "normal subgp"

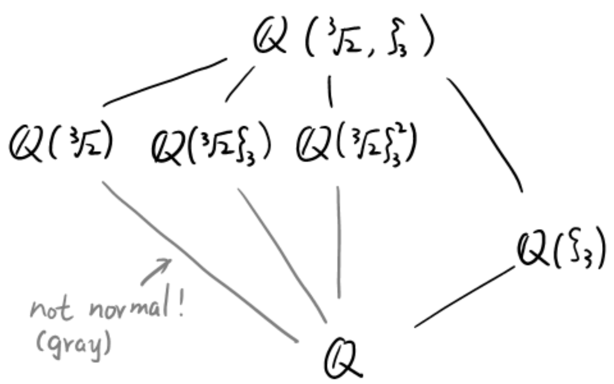
$$L \longmapsto Gal(E/L)$$

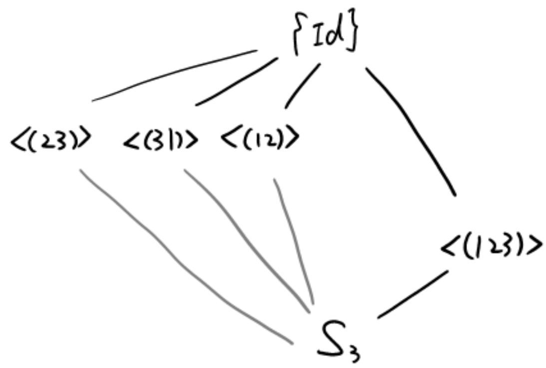
$$E^H \longleftarrow\!\shortmid\; H$$

also considered as data

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

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

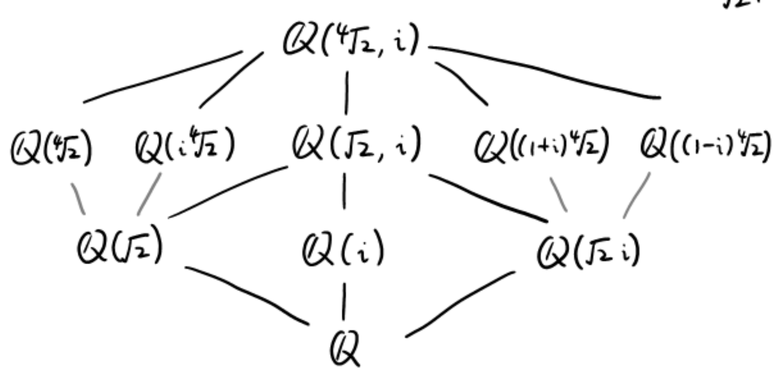


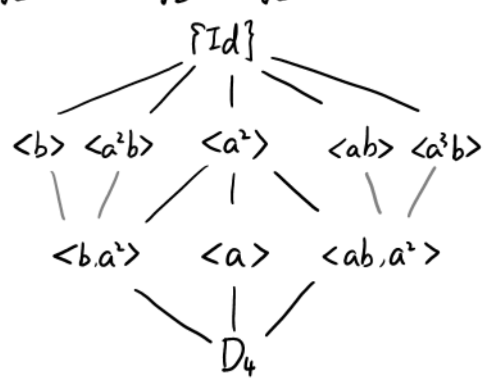


Eg. $Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

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

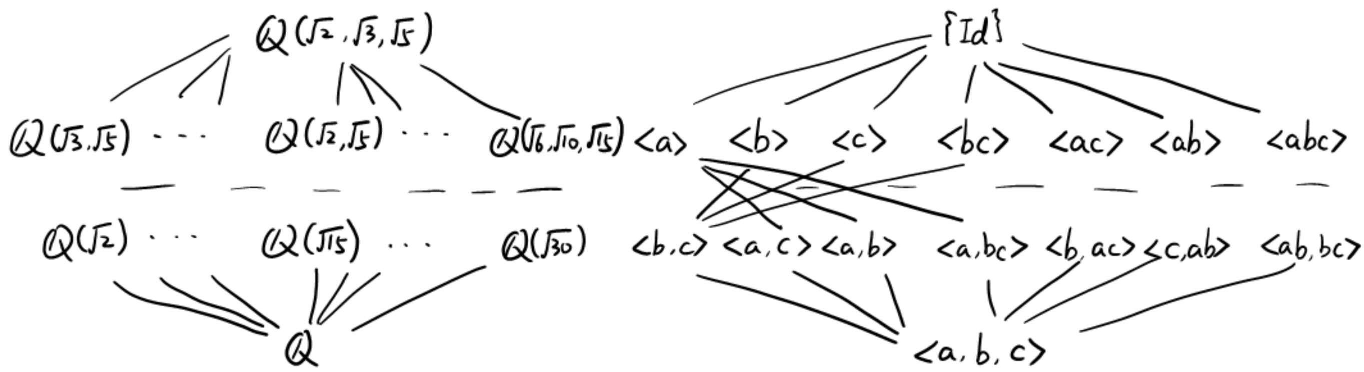
$a: i \mapsto i, \quad \sqrt[4]{2} \mapsto i\sqrt[4]{2} \qquad b: i \mapsto -i, \quad \sqrt[4]{2} \mapsto \sqrt[4]{2}$





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

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



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

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

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

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 $\xrightarrow{}$ Galois group

$\xleftarrow{\text{Galois inverse problem}}$

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) $\left.\begin{array}{l} x^{p^n-1} - 1 = \prod_{\alpha \in F^\times}(x-\alpha) \\ x^{p^n-1} - 1 \text{ seperable} \end{array}\right\} \Rightarrow \begin{array}{l} \nexists\ 0 < k < p^n - 1 \quad \text{s.t.} \\ \forall \alpha \in F^\times,\ \alpha^k - 1 = 0 \end{array}$

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

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

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

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 $\mathbb{Q}_p$, $p \neq 2$,

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

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

To be exact, let

$F' := $ the spliting 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 $F \Longrightarrow F' \hookrightarrow F \xRightarrow{\# F' = \# F = p^n} F' \cong F$

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

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

$\mathrm{Frob}: F \longrightarrow F \qquad x \longmapsto x^p$

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

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

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

then

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

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

Reason:

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

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

$$\xRightarrow{\text{Möbius}} \quad N_p(n) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, p^{\frac{n}{d}}$$

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

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

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

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

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. $f(x) = 0$.

/A: $$0 = \sum_{x \in \mathbb{F}_q^n} \left(1 - (f(x_1, \dots, x_n))^{q-1}\right) = \# \{ x \in \mathbb{F}_q^n \mid f(x) = 0 \} \mod p.$$

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

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