3.4 An example: $L = \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$

→ Since char $\mathbb{Q} = 0$, $L/\mathbb{Q}$ is separable.

→ L is the splitting field of $\{T^2+1, T^2-2\} \subset \mathbb{Q}[T]$:

$$T^2+1 = (T-i)(T+i) \quad \text{and} \quad T^2-2 = (T-\sqrt{2})(T+\sqrt{2}).$$

$\Rightarrow$ $L/\mathbb{Q}$ is normal.

→ $[\mathbb{Q}(i):\mathbb{Q}] = 2$ since $\mathrm{Mipo}_i = T^2+1$ has degree 2
$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ since $\mathrm{Mipo}_{\sqrt{2}} = T^2-2$ has degree 2

→ Since $\sqrt{2} \notin \mathbb{Q}(i)$, T^2-2 is also the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(i)$.

Thus
$$[L:\mathbb{Q}] = [L:\mathbb{Q}(i)] \cdot [\mathbb{Q}(i):\mathbb{Q}] = 2 \cdot 2 = 4.$$

$\Rightarrow$ $\#\,\mathrm{Gal}(L/\mathbb{Q}) = 4$.

→ We find the 4 $\mathbb{Q}$-linear automorphisms

$$L \xrightarrow{id} L, \quad L \xrightarrow{\sigma_i} L, \quad L \xrightarrow{\sigma_{\sqrt{2}}} L, \quad L \xrightarrow{\sigma_{i\sqrt{2}}} L$$
$$i \mapsto i \qquad\quad i \mapsto -i \qquad\quad i \mapsto i \qquad\quad i \mapsto -i$$
$$\sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{2} \mapsto -\sqrt{2}$$

$\Rightarrow$ $G = \mathrm{Gal}(L/\mathbb{Q}) = \{id, \sigma_i, \sigma_{\sqrt{2}}, \sigma_{i\sqrt{2}}\}$

Since $\sigma^2 = id$ for all $\sigma \in G$, $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

→ Hasse diagram of G:

$$\begin{tikzcd}
 & G \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle \sigma_i \rangle \arrow[dr, dash, "2"'] & \langle \sigma_{\sqrt{2}} \rangle \arrow[d, dash, "2"] & \langle \sigma_{i\sqrt{2}} \rangle \arrow[dl, dash, "2"] \\
 & \{id\} &
\end{tikzcd}$$

→ Fixed fields:

$$L^{\langle \sigma_i \rangle} = \mathbb{Q}(\sqrt{2}), \quad L^{\langle \sigma_{\sqrt{2}} \rangle} = \mathbb{Q}(i), \quad L^{\langle \sigma_i \sigma_{\sqrt{2}} \rangle} = \mathbb{Q}(i\sqrt{2})$$

⇒ all intermediate fields of $L/\mathbb{Q}$ are:

$$\begin{tikzcd}
 & L \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(i) \arrow[d, dash, "2"] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

3.5 Finite fields

Thm 1: p prime number

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ finite field with p elements

$\overline{\mathbb{F}}_p$ its algebraic closure

(1) For every $n \geq 1$, there is a unique subfield $\mathbb{F}_{p^n}$ of $\overline{\mathbb{F}}_p$ with p^n elements, and all finite subfields of $\overline{\mathbb{F}}_p$ are of this form.

(2) $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ iff. $n \mid m$. In this case $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is Galois and primitive. Its Galois group is cyclic of order $\frac{m}{n}$, generated by

$$\begin{aligned} \mathrm{Frob}_{p^n} : \mathbb{F}_{p^m} &\longrightarrow \mathbb{F}_{p^m} \\ a &\longmapsto a^{(p^n)} \end{aligned} \qquad (\underline{n\text{-th power Frobenius}})$$

(3) $\mathbb{F}_{p^n}^{\times}$ is cyclic of order $p^n - 1$.

proof: (1) • Every finite subfield $K \subset \overline{\mathbb{F}}_p$ contains $\mathbb{F}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$.

$\Rightarrow K$ is an $\mathbb{F}_p$-vector space of positive dimension n

$\Rightarrow \# K = p^n$

• <u>Existence of $\mathbb{F}_{p^n}$:</u>

Let $L \subset \overline{\mathbb{F}}_p$ be the splitting field of $f = T^{(p^n)} - T$ over $\mathbb{F}_p$. Then $f = \prod_{i=1}^{p^n} (T - a_i) \in L[T]$.

<u>claim:</u> $L = \{a_1, \ldots, a_{p^n}\}$.

Note that $f(a) = 0$ iff. $a^{(p^n)} = a$ for $a \in \overline{\mathbb{F}}_p$.

We have for all i, j:

- $(a_i \cdot a_j)^{(p^n)} = a_i^{(p^n)} \cdot a_j^{(p^n)} = a_i \cdot a_j$,
- $(a_i^{-1})^{(p^n)} = (a_i^{(p^n)})^{-1} = a_i^{-1}$ (if $a_i \neq 0$)
- $(a_i + a_j)^{(p^n)} = a_i^{(p^n)} + a_j^{(p^n)} = a_i + a_j$ (little Fermat thm),
- $(-a_i)^{(p^n)} = (-1)^{p^n} a_i^{p^n} = \begin{cases} -a_i & \text{if } p \text{ is odd}, \\ a_i = -a_i & \text{if } p \text{ is even}. \end{cases}$

Thus $\{a_1, \ldots, a_{p^n}\}$ forms a subfield of $\overline{\mathbb{F}}_p$ and thus $L = \{a_1, \ldots, a_{p^n}\}$. ↯

Since

$$\sum_{i=1}^{p^n} \prod_{j \neq i} (T - a_j) \underset{\begin{pmatrix}\text{Leibniz}\\ \text{rule}\end{pmatrix}}{=} f' = p^n T^{p^n - 1} - 1 = -1$$

has no root in common with f,

f has no multiple roots, i.e.

$\# L = \# \{a_1, \ldots, a_{p^n}\} = p^n$, and $L/\mathbb{F}_p$ is separable.

Thus $\mathbb{F}_{p^n} := L$ is Galois over $\mathbb{F}_p$ with p^n elts.

- <u>Uniqueness of $\mathbb{F}_{p^n}$:</u>

  Consider $L \subset \overline{\mathbb{F}_p}$ with p^n elements.

  $\Rightarrow \# L^\times = p^n - 1$

  $\Rightarrow a^{p^n-1} = 1$ for all $a \in L^\times$ (Lagrange's thm)

  $\Rightarrow f(a) = 0$ for all $a \in L$ where $f = T^{p^n} - T = T(T^{p^n-1} - 1)$

  $\Rightarrow L$ is the splitting field of f over $\mathbb{F}_p$

  $\Rightarrow L = \mathbb{F}_{p^n}$

<u>(2):</u> · If $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, then $\mathbb{F}_{p^m}$ is a $\mathbb{F}_{p^n}$-vector space and $p^m = (p^n)^d = p^{nd}$ for some $d \geq 1$. Thus $n | m$.

· Conversely, if $m = dn$, then for all $a \in \mathbb{F}_{p^n}$.

$$a^{(p^m)} = a^{\underbrace{(p^n \cdots p^n)}_{d\text{-times}}} = (\cdots (a^{(p^n)})^{(p^n)} \cdots)^{(p^n)} = a.$$

Thus $a \in \mathbb{F}_{p^m} \Rightarrow \mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$.

· Since $\mathbb{F}_{p^m} / \mathbb{F}_p$ is Galois, $\mathbb{F}_{p^m} / \mathbb{F}_{p^n}$ is so too.

$\mathbb{F}_{p^m}$ has at most one subfield of cardinality p^i for $i = 1 \ldots m-1$. Since $p \geq 2$,

$$\# \Big(\mathbb{F}_{p^m} - \bigcup_{E \subsetneq \mathbb{F}_{p^m}} E \Big) \geq p^m - \sum_{i=1}^{m-1} p^i > 1,$$

i.e. $\mathbb{F}_{p^m}$ contains an element a that is not contained in any proper subfield.

Thus $\mathbb{F}_{p^m} = \mathbb{F}_{p^n}(a)$ is primitive.

· $\# \operatorname{Gal}(\mathbb{F}_{p^m} / \mathbb{F}_{p^n}) = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = \frac{m}{n} =: d$.

$\operatorname{Frob}_{p^n} \in G = \operatorname{Gal}(\mathbb{F}_{p^m} / \mathbb{F}_{p^n})$ (exercise)

Let $e = \operatorname{ord}(\operatorname{Frob}_{p^n})$.

$\Rightarrow e \leq d$ and $a^{(p^{en})} = (a^{(p^n)})^e = (\mathrm{Frob}_{p^n}(a))^e = 1 \quad \forall a \in \mathbb{F}_{p^m}$

$\Rightarrow a$ is a root of $f = T^{(p^{ne})} - T$

Since f is separable,

$p^{ne} = \deg f \geq \# \mathbb{F}_{p^m} = p^m$

$\Rightarrow e \geq \frac{m}{n} = d$

Thus $\mathrm{ord}(\mathrm{Frob}_{p^n}) = d$ and $G = \langle \mathrm{Frob}_{p^n} \rangle$.

(3): $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$ is of order n

$\Rightarrow a^{p^n-1} = 1$ for all $a \in \mathbb{F}_{p^n}^\times$, and

$\forall k < p^n-1 \ \exists a \in \mathbb{F}_{p^n}^\times$ s.t. $a^k \neq 1$

Since $\mathbb{F}_{p^n}^\times$ is finite abelian,

$$\mathbb{F}_{p^n}^\times \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$$

for some prime powers $q_1 - q_r$, by the structure thm. of finitely generated abelian groups.

Thus $p^n - 1 = q_1 \cdots q_r$ and

$p^n - 1 = \min\{k \in \mathbb{N} \mid a^k = 1 \text{ for all } a \in \mathbb{F}_{p^n}^\times\}$

$= \mathrm{lcm}(q_1 - q_r)$,

which is only possible if $q_1 - q_r$ are pairwise coprime. Thus

$$\mathbb{F}_{p^n}^\times \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z} \simeq \mathbb{Z}/(p^n-1)\mathbb{Z}.$$

(Chinese remainder theorem) $\square$

4 Applications of Galois theory

4.1 The central result

For simplicity, we assume that all fields in this section are of characteristic 0.

<u>Def:</u> A finite extension L/K (in char. 0) is a <u>radical extension</u> if there exists a sequence

$$K = K_0 \subset K_1 = K_0(a_1) \subset K_2 = K_1(a_2) \subset \ldots \subset K_r = K_{r-1}(a_r) = L$$

such that $b_i = a_i^{n_i} \in K_{i-1}$ for $i = 1 \ldots r$ and some $n_i \geq 1$, i.e. "$a_i = \sqrt[n_i]{b_i}$".

<u>Def:</u> A finite group G is <u>solvable</u> if there exists a sequence of subgroups

$$\{e\} = G_0 < G_1 < \ldots < G_r = G$$

such that
- $G_{i-1} \lhd G_i$ for $i = 1 \ldots r$,
- $G_i / G_{i-1} \cong \mathbb{Z}/_{n_i \mathbb{Z}}$ for some $n_i \geq 1$.

<u>Thm:</u> L/K finite of char. 0

L^{norm} normal closure of L/K

Then L is contained in a radical extension L' of K iff. $\mathrm{Gal}(L^{norm}/K)$ is solvable.