2.2. Fundamental theorem

Fund. thm. of infinite Galois theory

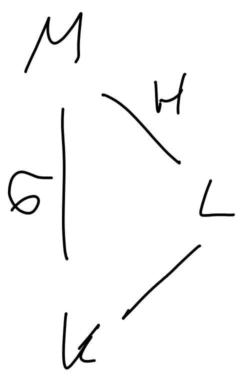
Let $M|K$ be a ~~finite~~ Gal. ext. with $G = \mathrm{Gal}(M|K)$.
Then, there is a bijection

$$\{\text{field } K \subseteq L \subseteq M\} \longleftrightarrow \{\text{closed subgroup } H \subseteq G\}$$

$$L \longmapsto \mathrm{Gal}(M|L) = \{\sigma \in G \mid \sigma(x) = x \ \forall x \in L\}$$

(Krull top. is subspace top. from Krull top. on $G = \mathrm{Gal}(M|K)$)

$$M^H = \{x \in M \mid \sigma(x) = x \ \forall \sigma \in H\} \longleftarrow H$$



$M|L$ is always Galois.
$L|K$ is Galois if and only if H is a normal subgroup of G. Then, H is the kernel of $G \longrightarrow \mathrm{Gal}(L|K)$, $\sigma \mapsto \sigma|_L$

so $\mathrm{Gal}(L|K) \cong G/H$.

(Krull top. = quotient top.)

For any subgroup $H \subseteq G$, $\mathrm{Gal}(M|M^H) = \overline{H}$, the closure of H in G.

What goes wrong for infinite Galois extensions?

We might have $Gal(M|M^H) \supsetneq H$.

Not every $H \leq G$ is of the form $Gal(M|L)$ for some L.

<u>Ex</u> $G = Gal(\overline{\mathbb{F}_q}|\mathbb{F}_q) \cong \hat{\mathbb{Z}}$

$$\begin{array}{ccc} G = Gal(\overline{\mathbb{F}_q}|\mathbb{F}_q) & \cong & \hat{\mathbb{Z}} \\ \cup\!\!\!\mid & & \cup\!\!\!\mid \\ H = \langle \varphi_q \rangle & \cong & \mathbb{Z} \\ \varphi_q & \longrightarrow & 1 \end{array}$$

$$\overline{\mathbb{F}_q}^H = \{x \in \overline{\mathbb{F}_q} \mid \varphi_q(x) = x\}$$
$$= \{x \in \overline{\mathbb{F}_q} \mid x^q = x\}$$
$$= \mathbb{F}_q$$

$$\Rightarrow Gal(\overline{\mathbb{F}_q}|\overline{\mathbb{F}_q}^H) = Gal(\overline{\mathbb{F}_q}|\mathbb{F}_q) = G \supsetneq H.$$

$$G = \overline{\mathbb{Z}} \leftarrow \boxed{\mathbb{Z} \text{ dense in } \hat{\mathbb{Z}}}$$

Note For $K \subseteq L \subseteq M$, we have

$$\mathrm{Gal}(M|L) = \{\sigma \in \mathrm{Gal}(M|K) \mid \sigma(x) = x \ \forall x \in L\}$$

$$= \bigcap_{x \in L} \mathrm{Gal}(M|K(x))$$

$$= \bigcap_{\substack{L' \subseteq L \\ \text{finite ext. of } K}} \mathrm{Gal}(M|L')$$

$$= \bigcap_{\substack{L' \subseteq L \\ \text{any ext. of } K}} \mathrm{Gal}(M|L').$$

Idea In topology, intersections of closed sets are closed.

$\rightsquigarrow$ Look for topology on $\mathrm{Gal}(M|K)$ s.t.

$H \subseteq G$ closed $\Leftrightarrow$ $H = \mathrm{Gal}(M|L)$ for some L.

Def The Krull topology on $G = \mathrm{Gal}(M|K)$ has the following base of open sets:

$$U_{\sigma, L} = \sigma\, \mathrm{Gal}(M|L) = \{\tau \in G \mid \tau|_L = \sigma\}$$

for $L \subseteq M$ finite Galois ext. of K,

$\sigma \in \mathrm{Gal}(L|K)$.

Roughly: $\sigma, \tau \in G$ "close" if they agree on a "large" finite Galois ext. $L \subseteq M$ of K.

Ex If $M|K$ is a finite ext., we get the discrete top:

$U_{\sigma, M} = \{\sigma\}$, so any set is open.

Rmk The Krull top. on $Gal(M|K) = \varprojlim_{L\in\mathcal{L}} Gal(L|K)$

$$\subseteq \prod_{L\in\mathcal{L}} Gal(L|K)$$

(where $\mathcal{L}$ consists of fin. ~~Gal~~. ext. $L \subseteq M$ of K) agrees with the subspace top. of the prod. top. of the disc. top.

Rmk G is a topological group: $G\times G \to G$, $(x,y)\mapsto xy$ and $G\to G$, $x\mapsto x^{-1}$ are continuous.

Ex The isom. $Gal(\overline{\mathbb{F}_q}\,|\,\mathbb{F}_q)\cong\hat{\mathbb{Z}}$, $Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q})\cong\hat{\mathbb{Z}}^\times$ defined earlier are homeomorphisms.

Ese $\quad Gal(\overline{\mathbb{F}_q} \mid \mathbb{F}_q) = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$

Finite index closed subgroups: $\quad H = n \cdot \hat{\mathbb{Z}} \quad , n \geq 1$
(= open)

$\wr$

Fin. (Gal.) ext. of $\mathbb{F}_q$: $\quad L = \mathbb{F}_{q^n}$

Closed subgroups: $H = \prod_p p^{e_p} \mathbb{Z}_p$ with $e_p = \{0, 1, \dots, \infty\}$
$(p^\infty = 0)$

(Take any closed H, $e_p := \min \{ v_p(x_p) \mid x = (x_p)_p \in H \}$.

$$x \in H \Rightarrow x \cdot \mathbb{Z} \subseteq H \underset{\substack{\uparrow \\ H \text{ closed}}}{\Longrightarrow} x \cdot \hat{\mathbb{Z}} \subseteq H \Rightarrow \underbrace{x_p \mathbb{Z}_p}_{= p^{e_p} \mathbb{Z}_p} \subseteq H$$

$\Downarrow$

$\prod_p p^{e_p} \mathbb{Z}_p \subseteq H$

$\Downarrow$

$\dots = H$)

Gal. ext. of $\mathbb{F}_q$: $L = \bigcup_{\substack{n \geq 1: \\ H \subseteq Gal(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \\ = n \cdot \hat{\mathbb{Z}}}} \mathbb{F}_{q^n} = \bigcup_{\substack{n \geq 1: \\ \forall p: v_p(n) \leq e_p}} \mathbb{F}_{q^n}$

$\left(\text{"} = \mathbb{F}_{q^N} \text{ with } N = \underbrace{\prod_p p^{e_p}}_{\text{not necessarily a number}} \text{"} \right)$

Pf of fund. thm. of infinite Galois theory

$M^{Gal(M|L)} = L$ for any $K \subseteq L \subseteq M$

"$\supseteq$" clear

"$\subseteq$" Let $x \in M \setminus L$. Let L_x be a fin. Gal. ext. of L containing x. $\underset{\substack{\uparrow \\ \text{fund. thm.} \\ \text{of fin. Gal. theory}}}{\Rightarrow}$ $\exists\, \bar\sigma \in Gal(L_x|L)$: $\bar\sigma(x) \neq x$.

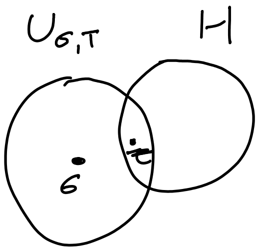
We know that $Gal(C|A) \to Gal(B|A)$ is surj. for any finite Gal. ext. $C|B$.

$\Rightarrow$ By Zorn's lemma, there is an ext. σ of $\bar\sigma$ to M. (The map $Gal(M|L) \to Gal(L_x|L)$ is surj.)

But $\sigma(x) \neq x$.

$Gal(M|M^H) = \overline{H}$ for all $H \leq G$

"$\subseteq$" Let $\sigma \in Gal(M|M^H)$. For any fin. Galois ext. $T \subseteq M$ of K, we have



$$\sigma|_T \in Gal(T|T^H) = \text{"}H|_T\text{"} = \{\tau|_T : \tau \in H\}.$$

$\Rightarrow U_{\sigma,T} \cap H \neq \emptyset$ for all T

$\Rightarrow \sigma \in \overline{H}$.

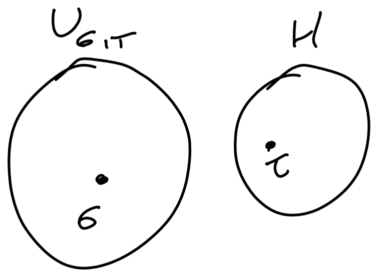
"$\supseteq$" Let $\sigma \notin Gal(M|M^H)$. $\Rightarrow \exists x \in M^H$: $\sigma(x) \neq x$.

Let $T \subseteq M$ be a fin. Gal. ext. of K containing x.

$x \in M^H \Rightarrow \forall \tau \in H$: $\tau(x) = x$

Since $\sigma(x) \neq x$, we conclude that $\sigma|_T \neq \tau|_T \ \forall \tau \in H$.

$\Rightarrow U_{\sigma,T} \cap H = \emptyset$. $\Rightarrow \sigma \notin \overline{H}$.



<u>$Gal(M|L) \subseteq Gal(M|K)$ carries the subspace top.</u>

Let $\sigma \in Gal(M|K)$, $T \subseteq M$ fin. Gal. ext.

$$U_{\sigma,T} \cap Gal(M|L) = \{\tau \in G \mid \tau|_T = \sigma|_T, \ \tau|_L = id_L\}$$

$$= \begin{cases} U_{\sigma',L\cdot T}, & \exists \sigma' \in Gal(L\cdot T|K): \sigma'|_T = \sigma|_T, \ \sigma'|_L = id_L \\ \emptyset, & \text{otherwise.} \end{cases}$$

$\vdots$

"$\square$"

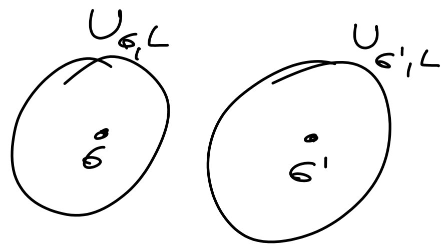
Thm $G = \mathrm{Gal}(M|K)$ is Hausdorff, totally disconnected, compact.

Pf Hausdorff + tot. disconn.

Take any $\sigma \neq \sigma' \in G$.

$\Rightarrow \sigma|_L \neq \sigma'|_L$ for some finite Gal. ext. $L \subseteq M$ of K.

$\Rightarrow U_{\sigma,L} \cap U_{\sigma',L} = \emptyset$ ($\Rightarrow$ Hausdorff)



In fact, $\displaystyle G \setminus U_{\sigma,L} = \bigcup_{\substack{\tau \in G: \\ \tau|_L \neq \sigma|_L}} U_{\tau,L}$ is open

($\Rightarrow$ tot. disconnected)

compact

$$\underbrace{\mathrm{Gal}(M|K) = \varprojlim_{\substack{L \subseteq M \\ \text{fin. Gal. ext.} \\ \text{of } K}} \mathrm{Gal}(L|K) \underset{\text{closed}}{\subseteq}}_{\text{compact}} \underbrace{\prod_{L} \underbrace{\mathrm{Gal}(L|K)}_{\substack{\text{finite} \\ \Downarrow \\ \text{compact}}}}_{\text{compact}}$$

$\square$

Reminder: compact $\Rightarrow$ ~~every sequence has a convergent subsequence~~

Hausdorff $\Rightarrow$ limits are unique (if they exist), all finite subsets are closed.

Thm If G is a compact top. group, $H \subseteq G$ is any subgroup:

H open $\Leftrightarrow$ H closed and $[G:H] < \infty$.

Pf G is the disjoint union of the left cosets of H. $\square$

2.3. Dedekind domains

Let $\mathcal{O}_K$ be a Ded. dom., $L|K$ any Gal. ext., $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L. (Might not be a Ded. dom. if $L|K$ is infinite!)

Let $\mathfrak{q}$ be a prime in $\mathcal{O}_K$.

Thm $Gal(L|K)$ acts transitively on $\{\mathfrak{P}$ max. id. of $\mathcal{O}_L$ lying above (= containing) $\mathfrak{q}\}$.

$$\begin{array}{ccc} L & \mathcal{O}_L & \mathfrak{P} \; \ldots \\ G \big| & \big| & //// \\ K & \mathcal{O}_K & \mathfrak{q} \end{array}$$

Def Decomposition group $D(\mathfrak{P}|\mathfrak{q}) = Stab(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$

Thm $\kappa(\mathfrak{P})|\kappa(\mathfrak{q})$ is normal.

Cor If $\kappa(\mathfrak{q})$ is a perfect (e.g. finite) field, then $\kappa(\mathfrak{P})|\kappa(\mathfrak{q})$ is Galois.

Thm $D(\mathfrak{P}|\mathfrak{q}) \longrightarrow Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{q}))$ is surjective.

Def Inertia group $= \ker(\ldots) = \{\sigma \in D(\mathfrak{P}|\mathfrak{q}) \mid \sigma(x) \equiv x \bmod \mathfrak{P} \; \forall x \in \mathcal{O}_L\}$.

Rmk $\mathfrak{P}|\mathfrak{q}$ is unramified if and only $I(\mathfrak{P}|\mathfrak{q}) = 1$.

Def If $\mathfrak{P}|\mathfrak{q}$ is unramified and $\kappa(\mathfrak{q}) = \mathbb{F}_q$, write

$$D(\mathfrak{P}|\mathfrak{q}) \xrightarrow{\sim} \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{q}))$$

$$\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) \longrightarrow \varphi_q : x \mapsto x^q$$

(Frobenius)

Rmk $D(\sigma\mathfrak{P}|\mathfrak{q}) = \sigma D(\mathfrak{P}|\mathfrak{q}) \sigma^{-1}$

$I \qquad\qquad I$

$\mathrm{Frob} \qquad\qquad \mathrm{Frob}$

Cor $\mathrm{Frob}(\mathfrak{q}) = \{\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) : \mathfrak{P} \ni \mathfrak{q}\}$ is a conj. class in G

Lemma D, I are closed subgroups of G.

Pf $D(\mathfrak{P}|\mathfrak{q}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$

$$= \{\sigma \in G \mid \underbrace{\sigma(\mathfrak{P} \cap F) = \mathfrak{P} \cap F}_{\text{only depends on } \sigma|_F} \ \forall F \subseteq L \text{ fin. Gal. ext. of } K\}$$

$$= \bigcap_F \text{closed set}$$

is closed

$I = \_\_\_$ $\square$