5-23-25 (WEEK 14)

Shun/翔海(@shun4midx)

INFINITE GALOIS GROUPS (Welcome to Shun's insanity :D)

PROPOSITION 1

Let L/K be algebraic. TFAE:

(A) L/K is normal

(B) L is a splitting field of some set S (possibly infinite)

(C) $\forall \sigma: L \hookrightarrow \overline{K}$ which fixes K induces an automorphism of L

Proof

"(A)⇒(B)": $S=\{m_{\alpha,K} \mid \alpha \in L\}$

On one hand, $\because m_{\alpha,K}$ splits over L $\therefore$ All roots of $m_{\alpha,K}$ lie in L

On the other hand, if $K \subseteq L' \subsetneq L$, then $\forall \alpha \in L \setminus L'$, $m_{\alpha,K}$ can't split over L' (at least, $\alpha \notin L'$)

$\therefore$ L is the smallest among $^{\text{field}}/_{K}$ which contains all roots of $f \in S$

"(B)⇒(A)": Let $A=\{\alpha \in L \mid f(\alpha)=0 \text{ for some } f \in S\}$. Then, $L=K(A)$

$\forall \beta \in L$, say $\beta \in K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in A$.

If L' is a splitting field of $f(x)=m_{\alpha_1,K} \cdots m_{\alpha_n,K}$ over K, then $m_{\beta,K}$ also splits over L'. Here, $\forall i$, $m_{\alpha_i,K} \mid f_i$ for some $f_i \in S$

Certainly, $L' \subseteq L$

"(A)⇒(C)". $\forall \alpha \in L$, $\sigma(\alpha)$ is also a root of $m_{\alpha,K}$, so $\sigma(\alpha) \in L$

Hence, $\sigma: L$ "$\hookrightarrow$" L' fixes K + "L/K is algebraic" ⇒ σ is onto, so $\sigma(L)=L$

"(C)⇒(A)": For $\alpha \in L$, β is a root of $m_{\alpha,K}$. Then $\exists$

$$\begin{tikzcd} \tau: K(\alpha) \arrow[r] & K(\beta) \arrow[r, hook] & \overline{K} \\ \overset{\neq}{0} \quad \alpha \arrow[r, mapsto] & \beta & \end{tikzcd}$$

We know τ can be extended to $\sigma: L \hookrightarrow \overline{K}$. By assumption, $\sigma(L)=L$ and $\beta=\tau(\alpha)=\sigma(\alpha) \in L$ □

THE FUNDAMENTAL THEOREM OF GALOIS THEORY DOES NOT HOLD FOR INFINITE ALGEBRAIC EXTENSIONS

EXAMPLE

Let $A=\{\sqrt{p} \mid p: \text{prime}\}$ and $L=\mathbb{Q}(A)$

- $L/\mathbb{Q}$ is normal: L is a splitting field of $\{x^2-p \mid p: \text{prime}\}$
- $L/\mathbb{Q}$ is separable: $\because \operatorname{char} \mathbb{Q}=0$
- $\operatorname{Gal}(L/\mathbb{Q})$ has uncountably many groups of index 2 (There are only countably many quadratic field extensions of $\mathbb{Q}$ in L)

  $\ulcorner$ $\mathbb{Q}(\sqrt{q})$, q: square free

  ↳ $\forall \sigma \in \operatorname{Gal}(L/\mathbb{Q})$, $\sigma: \sqrt{p} \longmapsto \sqrt{p}$ or $-\sqrt{p}$, $\sigma^2=id$, so $\operatorname{Gal}(L/\mathbb{Q})$ is abelian

  $\cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ can be seen as a $\mathbb{Z}/2\mathbb{Z}$ vector space V

  We know $V^*=\{\phi: V \longrightarrow \mathbb{Z}/2\mathbb{Z} \mid \phi \text{ is a } \mathbb{Z}/2\mathbb{Z}\text{-linear transformation}\} \leftrightarrow \operatorname{Ker}\phi \leq V$ is uncountable

  $\therefore$ $\{\operatorname{Ker}\phi \mid \phi \in V^*\}$ (index 2) is uncountable

GOAL

Consider a Galois extension L/K,

$$\begin{tikzcd} \mathcal{F}=\{E \mid L \supseteq E \supseteq K\} \arrow[r] & \mathcal{G}=\{H \mid H \leq \operatorname{Gal}(L/K)\} \\ E \arrow[r, mapsto] & \operatorname{Gal}(L/E) \\ L^H & H \arrow[l, mapsto] \end{tikzcd}$$

FACT 1

$E \mapsto \operatorname{Gal}(L/E) \rightarrow E = L^{\operatorname{Gal}(L/E)}$

Proof

For $\alpha \in L \setminus E$, let E_1 be a splitting field of $m_{\alpha,E}$.

Then, we have E_1/E: finite Galois ⇒ $E_1^{\operatorname{Gal}(E_1/E)}=E$ ⇒ $\exists \tau \in \operatorname{Gal}(E_1/E)$, $\alpha \notin E$, $\tau(\alpha) \neq \alpha$

Extend, then we have $\sigma \in \operatorname{Gal}(L/E)$, $\sigma(\alpha) \neq \alpha$

FACT 2

Let L/K be Galois and $G=\operatorname{Gal}(L/K)$

If E/K is Galois and $H=\operatorname{Gal}(L/E)$, then $\operatorname{Gal}(E/K) \cong G/H$

Proof

Define $\varphi: G \twoheadrightarrow \mathrm{Gal}(E/K)$

$\sigma \longmapsto \sigma|_E$ ← well-defined since E/K is normal

It is onto due to the important extension property

By extension, $\mathrm{Ker}\,\varphi = H \Rightarrow G/H \cong \mathrm{Gal}(E/K)$ □

GOAL

To find a good formulation for $\mathrm{Gal}(L/K) = G$

STRATEGY

$\{K \subseteq E_i \subseteq L \mid E_i/K : \text{finite Galois}\} = \{E_i \mid i \in I\}$

$\forall i$, $H_i := \mathrm{Gal}(L/E_i) \trianglelefteq G$, $G_i := G/H_i \cong \mathrm{Gal}(E_i/K)$ ← $|G_i| < \infty$ ⇝ $\overset{\overset{G}{\swarrow}}{\{G_i \mid i \in I\}}$

- $i \leq j \Leftrightarrow E_i \subseteq E_j \Leftrightarrow H_i \supseteq H_j$, $\varphi_{ji}: G_j = \overset{\text{big}}{G/H_j} \longrightarrow \overset{\text{small}}{G_i := G/H_i}$

$\sigma \in \mathrm{Gal}(E_j/K)$ $\bar{\sigma} \longmapsto \bar{\sigma}$ $\mathrm{Gal}(E_i/K) \ni \sigma|_{E_i}$

MAIN THEOREM

Let L/K be Galois. Then, $\mathrm{Gal}(L/K) \cong \underset{i}{\varprojlim} G_i$ ← inverse limit

Proof

$\forall i$,

$$\begin{tikzcd}
\mathrm{Gal}(L/K) \arrow[rr, "\rho_i"] \arrow[dddr, "\rho_{id}"] & & \mathrm{Gal}(E_i/K) \cong G_i \\
\sigma \arrow[rr, mapsto] \arrow[dddr, mapsto] & & \sigma|_{E_i} \\
& & \\
& \mathrm{Gal}(E_j/K) \cong G_j \arrow[uuur, "\underset{E_i \subseteq E_j}{\varphi_{ji}}"'] & \\
& \sigma|_{E_j} \arrow[uuur, mapsto] &
\end{tikzcd}$$

By the universal property of $\varprojlim G_i$, $\exists !\, f: \mathrm{Gal}(L/K) \longrightarrow \varprojlim G_i$, s.t $\varphi_i \circ f = \rho_i$

$\sigma \longmapsto (\sigma|_{E_i})_{i \in I}$

- f is 1-1: $\sigma \in \mathrm{Ker} f \Leftrightarrow \sigma|_{E_i} = \mathrm{id}_{E_i}\ \forall i \in I \Leftrightarrow \sigma = \mathrm{id}_L$

  Claim: $\forall \alpha \in L, \exists i \in I$, s.t. $\alpha \in E_i$

  $\cap$

  $K(\beta_1, \dots, \beta_n) = E_i$

- f is onto: For $(\sigma_i)_{i \in I} \in \underset{i}{\varprojlim} G_i$, define $\sigma: L \longrightarrow L$

  $E_i \ni \alpha \longmapsto \sigma_i(\alpha)$

  ↳ Well-defined: If $\alpha \in E_j$ too, then $\alpha \in E_i \cap E_j = E_t$, $\sigma_i(\alpha) = \sigma_i|_{E_t}(\alpha) = \sigma_t(\alpha) = \sigma_j|_{E_t}(\alpha) = \sigma_j(\alpha)$ ✓

  ↳ Homo: $\alpha, \beta \in L$, say $\alpha \in E_i$, $\beta \in E_j$, then, $\alpha, \beta \in E_i E_j = E_k$, so $\sigma(\alpha\beta) = \sigma_k(\alpha\beta) \overset{\sigma_k \text{ is homo}}{=} \sigma_k(\alpha)\sigma_k(\beta) = \sigma(\alpha)\sigma(\beta)$

  ↙σ_i is autom

  ↳ 1-1: If $\sigma(\alpha) = 0$, $\alpha \in E_i$, then $\sigma_i(\alpha) = 0 \Rightarrow \alpha = 0$

  ↳ Onto: $\forall \beta \in L$, say $\beta \in E_i$ and $\sigma_i(\alpha) = \beta \Rightarrow \sigma(\alpha) = \beta$ ✓

p-ADIC INTEGERS

(Yes, I've gone insane stfu this is typical Shun <2 weeks before finals)

$I = \mathbb{N}$, for $i \leq j$, $\varphi_{ji}: \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ ⇝ $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \dots$

$\bar{a} \longmapsto \bar{a}$ $\quad a_0 + p\mathbb{Z} \longleftarrow a_0 + a_1 p + a_2 p^2 + p^3\mathbb{Z}$

$\therefore \varprojlim \mathbb{Z}/p^i\mathbb{Z} = \{a_0 + a_1 p + a_2 p^2 + \dots + a_i p^i \mid 0 \leq a_i \leq p-1\} =: \mathbb{Z}_p$ (that's why we shouldn't write $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{Z}_p$ lol... $\mathbb{F}_p$ is better)

LIMITS IN ALGEBRA

(From here on, everything goes downhill, pls don't reference this, I'm 99% sure it's wrong)

Consider a sequence of objects $\dots \to X_n \to X_{n-1} \to \dots \to X_1$ in $\mathcal{C}$, we want to consider a "X_∞"

but I don't wanna erase this lol so enjoy my insanity :)

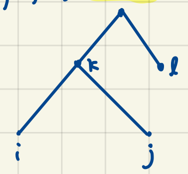
General: 1. A directed set I

2. $\{X_i\}_{i \in I}$ objects in a category

だからボクは代数学を辞めた

DEFINITION (POSET)

$(I, \leq)$ is directed if $\forall i, j \in I$, $\exists k \in I$, $k \geq j$, $k \geq i$



$$\lim_{n} x_n = \lim_{n \geq k} x_n$$

DEFINITION (FAMILIES)

$\mathcal{C}$: A category, I: A directed set $(\mathbb{N}, \geq)$

Then, $A = \{A_i \in \mathcal{C}\}_{i \in I}$ is directed if $\forall i \leq j$ in I, $i \leq j \leq k$, we have the universal property

$$\begin{tikzcd} A_i \arrow[rr, "f_j^i"] \arrow[dr, "f_k^i"'] & \arrow[d, phantom, "\circlearrowright"] & A_j \arrow[dl, "f_k^j"] \\ & A_k & \end{tikzcd}$$

Note: "inversely directed": → ⇒ ←

LIMIT BY UNIVERSAL PROPERTY (ACTUALLY JUST UNION/INTERSECTION)

$$\text{"}\cap A_i\text{"} \to \dots \to A_i \to A_{i-1} \to \dots \to A_1$$

$$B_1 \dots \to B_{i-1} \to B_i \to \dots \to \text{"}\cup B_i\text{"}$$

DEFINITION (UNIVERSAL PROPERTY)

A is inversely directed if

$$\begin{tikzcd} Y \arrow[rr, "g_j"] \arrow[dr] & \arrow[d, phantom, "\circlearrowright"] & A_{j \geq i} \arrow[dl] \\ & A_i & \end{tikzcd}$$

$$\begin{tikzcd} \mathcal{C} \ni Y \arrow[r, "\exists!"] \arrow[rr, bend right, "g_i"'] & \varprojlim A \arrow[r] & A_i \end{tikzcd}$$

Directed:

$$\begin{tikzcd} Y & & A_{i \geq j} \arrow[ll] \arrow[dl] \\ & A_j \arrow[ul] & \end{tikzcd}$$

, $Y \leftarrow \varinjlim A$

- $\varprojlim A \in \mathcal{C}$
- $$\begin{tikzcd} \varprojlim A \arrow[r] \arrow[dr, "\exists"] & A_i \arrow[d, "i \geq j"] \arrow[dl, phantom, "\circlearrowleft"] \\ Y \arrow[u, "="] & A_j \end{tikzcd}$$

EXAMPLE

Let $I = \mathbb{N}$, $A_n := \mathbb{Z}/p^n\mathbb{Z}$

Inversely directed: $\mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$
$\bar{z} \longmapsto \bar{z}$
$\Rightarrow$ limit $= \{a_0 + pa_1 + p^2a_2 + \dots \mid 0 \leq a_i \leq p-1\} = \mathbb{Z}_p$

Directed: $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$
$\bar{z} \longmapsto \overline{pz}$

$\cong$

$\frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \longrightarrow \frac{1}{p^{n+1}}\mathbb{Z}/\mathbb{Z} \Rightarrow \varinjlim A = \bigcup_{n \in \mathbb{N}} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$

THEOREM (EXISTENCE)

Inverse limit exists uniquely in Mod, groups, rings

Proof

Let A be an inversely directed family

A has $\begin{cases} I\text{: direct set} \\ A_i \in \mathcal{C},\ i \in I \\ i \leq j,\ A_j \xrightarrow{\phi_i^j} A_i \end{cases}$

$\phi_j^k \circ \phi_i^j = \phi_i^k$

$$\begin{tikzcd} & & A_{i \leq j} \\ Y \arrow[urr, "g_i"] \arrow[drr, "g_j"'] & \varprojlim A \arrow[l] & \\ & & A_i \arrow[uu, "\phi_i^j"'] \end{tikzcd}$$

$\Rightarrow$ $Y \longmapsto \prod_{i \in I} A_i = \{I \xrightarrow{\pi} \bigsqcup_{i \in I} A_i \mid \pi(i) \in A_i\}$
$y \longmapsto (g_i(y))_i$

Shun/翔海(@shun4midx)

Define $\varprojlim A = \{(a_i) \in \prod_i A_i \mid a_i = \phi^i_j(a_j)\ \forall_j \le i\}$

$$\begin{tikzcd} \varprojlim A & \prod_i A_i \arrow[d] \\ Y \arrow[u] & A_i \end{tikzcd}$$

$\Rightarrow$ Satisfies universal property ✓

In other words, we can think of "inverse limit" as "consists of compatible tuples $(a_i)_i$"

DIRECT LIMIT

$A = \{A_i\}$: direct family, then we define the following:

$$\begin{tikzcd} A_i \arrow[rr] \arrow[dr] & \circlearrowleft & \varinjlim A \\ & A_j \arrow[ur] & \end{tikzcd}$$

$\varinjlim A = \sqcup A_i / a_i \sim f^i_j(a_j)$ ← can prove it is an equivalence relation

We define $[a_i] + [a_j] = [f^i_k a_i + f^j_k a_j]$ if $k \geq i, j$

EXAMPLE

K: field, $I = \{K \hookrightarrow L$: finite Galois extension$\}$

$$\begin{tikzcd}[row sep=small] L \arrow[d, dash] & \le & L' \arrow[d, dash] & \equiv & K \arrow[r, dash] \arrow[rr, dash, bend right, "\circlearrowleft"'] & L \arrow[r, dash] & L' \\ K & & K & & & & \end{tikzcd}$$

$L \subseteq L'$

wtf is this

Directed:

$$\begin{tikzcd} & LL' \arrow[dl, dash] \arrow[dr, dash] \arrow[d, dash] & \\ L \arrow[dr, dash] & {} \arrow[d, dash] & L' \arrow[dl, dash] \\ & K & \end{tikzcd}$$

$\mathrm{Gal}(L'/K) \longrightarrow \mathrm{Gal}(L/K)$

$\sigma \longmapsto \sigma|_{L}$

$\Rightarrow \mathrm{Gal}(K^{sep}/K) = \varprojlim \underbrace{\mathrm{Gal}(L/K)}_{\text{finite}}$

EXAMPLE

$P \in \mathrm{Spec}\, A \Rightarrow A_P = \varinjlim_{f \notin P} A_f$ idk don't ask me why

EXAMPLE

$\mathbb{Z}_{10} = \cdots 99999 = -1$ $(\because \cdots\cdots 99999 + 1 = 0)$