20. Galois 理論

20–1. **自己同型群・固定体.** 体の拡大 L/K に対し、
$G := \mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) | \sigma|_K = \mathrm{id}\}$ とするとき、

- $H \subset G$: 部分群に対し、
  $L^H := \{x \in L | \forall \sigma \in H : \sigma(x) = x\}$: H の**固定体 (fixed field)**
- M : L/K の中間体に対し、
  $\mathrm{Aut}(L/M) = \{\sigma \in G | \forall x \in M : \sigma(x) = x\}$: L の M 上の自己同型群
- 自明に、$\mathrm{Aut}(L/L^H) \supset H, L^{\mathrm{Aut}(L/M)} \supset M$

20–2. **Galois 拡大.** 有限次 (代数) 拡大 L/K に対し、

- L/K : **Galois 拡大 (Galois extention)** $\overset{\leftarrow}{\iff} L/K$: 正規かつ分離的
  $\iff \#\mathrm{Aut}(L/K) = \#\mathrm{Emb}_K(L, \overline{K}) = [L : K] \iff L^{\mathrm{Aut}(L/K)} = K$

L/K : Galois 拡大の時、特に $\mathrm{Aut}(L/K)$ を $\mathrm{Gal}(L/K)$ と書き、L/K の **Galois 群 (Galois group)** と呼ぶ。

- L/K : Galois 拡大で、$G = \mathrm{Gal}(L/K)$ が＊＊群である時、L/K を**＊＊拡大**と呼ぶ。(＊＊= abel・巡回・可解・冪零・p など)

20–3. **Galois 理論の基本定理.** L/K を Galois 拡大、$G := \mathrm{Gal}(L/K)$ をその Galois 群とし、$\mathcal{H}_G := \{H | G \text{ の部分群}\}, \mathcal{M}_{L/K} := \{M | L/K \text{ の中間体}\}$ とおく。

$$\Phi : \mathcal{M}_{L/K} \longrightarrow \mathcal{H}_G \qquad \Psi : \mathcal{H}_G \longrightarrow \mathcal{M}_{L/K}$$
$$M \longmapsto \mathrm{Aut}(L/M) \qquad H \longmapsto L^H$$

- Φ, Ψ :共に全単射で、互いに逆写像 $(\Phi \circ \Psi = \mathrm{id}_{\mathcal{H}_G}, \Psi \circ \Phi = \mathrm{id}_{\mathcal{M}_{L/K}})$
- Φ, Ψ :共に包含関係に関して順序逆同型 $(H_i \leftrightsquigarrow M_i$ のとき、$H_1 \subset H_2 \Leftrightarrow M_1 \supset M_2)$
- $H_i \leftrightsquigarrow M_i$ のとき、$H_1 \cap H_2 \leftrightsquigarrow M_1 M_2, \langle H_1, H_2 \rangle \leftrightsquigarrow M_1 \cap M_2$
- $M \in \mathcal{M}_{L/K}$ に対し、L/M : Galois で、$\mathrm{Gal}(L/M) = \Phi(H)$
- $\forall \sigma \in G$ に対し、$\sigma H \sigma^{-1} \leftrightsquigarrow \sigma(M)$
- 特に、$H \lhd G \iff M/K$: Galois で、この時、$G/H \simeq \mathrm{Gal}(M/K)$

Φ, Ψ による部分群と中間体との対応を **Galois 対応 (Galois correspondence)** と呼ぶ。

- L/K : 分離代数拡大に対し、L の K 上の正規閉包 $\widetilde{L}$ は、L を含む K の最小の Galois 拡大 (L/K の **Galois 閉包 (Galois closure)** という)

20–4. **推進定理.** L/K:Galois 拡大、M/K:任意の体拡大 (超越でも非分離でも可) に対し、

- LM/M : Galois 拡大で、$\mathrm{Gal}(LM/M) \simeq \mathrm{Gal}(L/L \cap M)$

特に、L_1, L_2 : 共に Galois 拡大の時、

- $L_1 L_2, L_1 \cap L_2$: 共に K 上の Galois 拡大
- $\mathrm{Gal}(L_1 L_2/K) \simeq \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) | \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}\}$
- $\mathrm{Gal}(L_1 L_2/L_1 \cap L_2) \simeq \mathrm{Gal}(L_1/L_1 \cap L_2) \times \mathrm{Gal}(L_2/L_1 \cap L_2)$

20–5. **例: $\boldsymbol{Q}$ の円分拡大.** $n \geq 1$ に対し、$\zeta_n \in \overline{\boldsymbol{Q}}$: 1 の原始 n 乗根の一つとする (例えば、$\boldsymbol{C}$ 内で考えれば $\zeta_n = e^{2\pi i/n}$ など)。

- $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$: $\boldsymbol{Q}$ の **(第 n) 円分拡大 (cyclotomic extention)**。$[\boldsymbol{Q}(\zeta_n) : \boldsymbol{Q}] = \varphi(n)$
- $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$: Galois 拡大で、$\mathrm{Gal}(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}) \simeq (\boldsymbol{Z}/n\boldsymbol{Z})^\times$
  $$(\sigma_a : \zeta_n \mapsto \zeta_n^a) \leftrightsquigarrow a \bmod n$$

20–6. **例: 有限体の拡大.** p : 素数とし、$r \geq 1, q := p^r$ とする。$n \geq 1$ に対し、

- q 元体 $\boldsymbol{F}_q$ の (唯一の) n 次拡大 $\boldsymbol{F}_{q^n}/\boldsymbol{F}_q$ は Galois 拡大で、
  $\mathrm{Gal}(\boldsymbol{F}_{q^n}/\boldsymbol{F}_q) = \langle \mathrm{Frob}_q \rangle \simeq \boldsymbol{Z}/n\boldsymbol{Z}$ (ここに $\mathrm{Frob}_q : x \mapsto x^q$: q 乗 Frobenius 写像)

特に、有限体の有限次拡大はすべて巡回拡大である。