体論 (第12回)

12. ガロアの基本定理の証明

前回, ガロアの基本定理について説明し, いくつかの具体例を紹介しました. 今回はこの証明についてみていきます. まずは定理の主張を復習しておきます.

定理 11-2 (ガロア理論の基本定理)
L/K を有限次ガロア拡大とする. $\mathbb{M}$ を L/K の中間体全体, $\mathbb{H}$ を $G = \mathrm{Gal}(L/K)$ の部分群全体とし, 写像

$$\Phi : \mathbb{H} \longrightarrow \mathbb{M} \quad (H \longmapsto L^H), \quad \Psi : \mathbb{M} \longrightarrow \mathbb{H} \quad (M \longmapsto H(M))$$

を考える. このとき,

$$\Phi \circ \Psi = \mathrm{Id}_{\mathbb{M}}, \quad \Psi \circ \Phi = \mathrm{Id}_{\mathbb{H}}.$$

さらに次が成り立つ.

(1) $H_1, H_2 \in \mathbb{H}$ とし, $M_1 = \Phi(H_1)$, $M_2 = \Phi(H_2)$ と置く. このとき,

$$H_1 \subseteq H_2 \iff M_2 \subseteq M_1.$$

特に $\Phi(G) = K$, $\Phi(\{\mathrm{Id}_L\}) = L$.

(2) $\Phi(H) = M$ とする. このとき, $|H| = [L : M]$ であり, さらに

$$H \text{ が } G \text{ の正規部分群} \iff M/K \text{ はガロア拡大}$$

が成り立つ.

$\Phi \circ \Psi = \mathrm{Id}_{\mathbb{M}}$ の証明
$M \in \mathbb{M}$ に対して,

$$(\Phi \circ \Psi)(M) = \Phi(\mathrm{Gal}(L/M)) = L^{\mathrm{Gal}(L/M)}$$

であるので $L^{\mathrm{Gal}(L/M)} = M$ を示せばよい.
定義より $M \subseteq L^{\mathrm{Gal}(L/M)}$ は明らか. $x \in L^{\mathrm{Gal}(L/M)}$ とする. 定理 9-2 から x の M 上共役全体は

$$\{\sigma(x) \mid \sigma \in \mathrm{Gal}(L/M)\} = \{x\}.$$

従って x の M 上共役はただ 1 つしかないので $x \in M$. よって $L^{\mathrm{Gal}(L/M)} \subseteq M$.

□

次に $\Psi \circ \Phi = \mathrm{Id}_{\mathbb{H}}$ を示します. このために次の補題を準備します.

補題 12-1

L/K を有限次ガロア拡大とし, H を $\mathrm{Gal}(L/K)$ の部分群とする. $\alpha \in L$ に対して

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

と置けば, $f(x) \in L^H[x]$ となる.

[証明]

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ $(a_i \in L)$ と表す. $\tau \in H$ に対して,

$$f^{(\tau)}(x) = \prod_{\sigma \in H} \Big(x - (\tau \circ \sigma)(\alpha)\Big)$$

と置くと, τ は環準同型より

$$f^{(\tau)}(x) = x^n + \tau(a_{n-1})x^{n-1} + \cdots + \tau(a_0).$$

一方, H は群より $\{\tau \circ \sigma \mid \sigma \in H\} = H$ が成り立つ. 従って

$$f^{(\tau)}(x) = \prod_{\sigma \in H} \Big(x - (\tau \circ \sigma)(\alpha)\Big) = \prod_{\sigma \in H} \Big(x - \sigma(\alpha)\Big) = f(x).$$

これより, $\tau(a_i) = a_i$ $(0 \leq i \leq n-1)$. 従って $a_i \in L^H$ であり, $f(x) \in L^H[x]$ を得る.

□

問題 12-1　$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ とし, $G = \mathrm{Gal}(L/\mathbb{Q})$ とする. また $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = -\sqrt{3}$ を満たす $\sigma \in G$ を取り, $H = <\sigma>$ と置く. $\alpha = \sqrt{2} + \sqrt{3}$ に対して, 補題 12-1 が成り立つことを確認せよ.

$\Psi \circ \Phi = \mathrm{Id}_{\mathbb{H}}$ の証明

$H \in \mathbb{H}$ に対して,

$$(\Psi \circ \Phi)(H) = \Psi(L^H) = \mathrm{Gal}(L/L^H).$$

従って $H = \mathrm{Gal}(L/L^H)$ を示せばよい .

定義から $H \subseteq \mathrm{Gal}(L/L^H)$ は直ちに従う. 従って $|H| \leq |G(L/L^H)| = [L : L^H]$. 定理 9-1 より $L = L^H(\alpha)$ $(\alpha \in L)$ と表せる. このとき,

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

と置けば, 補題 12-1 より $f(x) \in L^H[x]$ となる. $f(\alpha) = 0$ より, α の L^H 上の最小多項式を $g(x)$ とすると,

$$|H| = \deg f \geq \deg g = [L^H(\alpha) : L^H] = [L : L^H].$$

よって $|H| = |\mathrm{Gal}(L/L^H)|$. これと $H \subseteq \mathrm{Gal}(L/L^H)$ を合わせると $H = \mathrm{Gal}(L/L^H)$ が従う.

定理 11-2 (1) の証明

$H_1 \subseteq H_2$ のとき,

$$L^{H_1} = \{x \in L \mid \sigma(x) = x\ (\forall \sigma \in H_1)\} \supseteq \{x \in L \mid \sigma(x) = x\ (\forall \sigma \in H_2)\} = L^{H_2}.$$

従って $M_1 \supset M_2$. 逆は問題にしておく.

□

問題 12-2　定理 11-2 (1) の状況を考える. $M_2 \subseteq M_1$ のとき, $H_1 \subseteq H_2$ を示せ.

定理 11-2 (2) の証明

$\Psi \circ \Phi = \mathrm{Id}_{\mathbb{H}}$ より

$$[L : M] = |\mathrm{Gal}(L/M)| = |\Psi(M)| = |\Psi(\Phi(H))| = |H|.$$

次に

$$H \text{ が } G \text{ の正規部分群} \iff M/K \text{ はガロア拡大}$$

を示す. まず, M/K をガロア拡大とする. このとき,

$$\varphi : G \to \mathrm{Gal}(M/K) \quad (\sigma \mapsto \sigma|_M) \qquad \text{(eq 1)}$$

は群の準同型で,

$$\ker \varphi = \{\sigma \in G \mid \sigma|_M = \mathrm{Id}_M\} = \mathrm{Gal}(L/M) = H.$$

従って H は G の正規部分群である.

逆に H が G の正規部分群とする. $\tau \in \mathrm{Hom}_K(M, \mathbb{C})$ とすると, 補題 9-1 より $\sigma|_M = \tau$ を満たす $\sigma \in \mathrm{Hom}_K(L, \mathbb{C}) = G$ が取れる. このとき, $\sigma H \sigma^{-1} = H(\sigma(M))$ が成り立つ (問題 12-3). H は G の正規部分群なので,

$$\Psi(\sigma(M)) = H(\sigma(M)) = \sigma H \sigma^{-1} = H = \Psi(M).$$

Ψ は単射より $\sigma(M) = M$. これより $\tau(M) = M$. 従って M/K はガロア拡大である.

□

[**補足**] 補題 9-1 より (eq 1) の φ は全射であることが分かる. 従って, 準同型定理から群の同型

$$G/H(M) \simeq \mathrm{Gal}(M/K)$$

が得られる.

問題 12-3 定理 11-2 (2) の証明において, $\sigma H \sigma^{-1} = H(\sigma(M))$ を示せ.