体論 (第 11 回)

11. ガロア理論

今回はガロア理論の基本定理とその使い方について解説します.

定理 11-1

L/K を有限次ガロア拡大, そのガロア群を G とする.

(1) G の部分群 H に対して,

$$L^H = \{x \in L \mid \sigma(x) = x \quad (\forall \sigma \in H)\}$$

は L/K の中間体となる. L^H を H **の固定体**という.

(2) M を L/K の中間体とすると, L/M はガロア拡大となる. $H(M) = \mathrm{Gal}(L/M)$ と置くと, $H(M)$ は G の部分群で,

$$H(M) = \{\sigma \in G \mid \sigma|_M = \mathrm{Id}_M\}$$

となる. $H(M)$ **を** M **の固定群**という.

[証明]

(1) 定理 1-1 の (i)-(iv) を示せばよい. ここでは, (i) のみ確認しておく. つまり,

$$x, y \in L^H \implies x - y \in L^H$$

を言えばよい. $\sigma \in H$ に対して, $\sigma(x) = x$, $\sigma(y) = y$ であり, σ は環準同型だから

$$x - y = \sigma(x) - \sigma(y) = \sigma(x - y).$$

従って $x - y \in L^H$ である.

(2) $x \in L$ をとる. y を x の M 上共役とすると, 定理 7-1 (2) から x の K 上共役でもある. L/K はガロア拡大より $y \in L$ となる. 従って L/M はガロア拡大である. 後半の主張は

$$H(M) = \mathrm{Hom}_M(L, L) \subseteq \mathrm{Hom}_K(L, L) = G$$

から従う.

□

例題 11-1

$L = \mathbb{Q}(\sqrt{2})$ とすると, $L/\mathbb{Q}$ のガロア群は

$$G = G(L/\mathbb{Q}) = \{\mathrm{Id}_L,\ \sigma\}$$

で与えられる. ただし, σ は $\sigma(\sqrt{2}) = -\sqrt{2}$ を満たすものとする.

(1) L, $\mathbb{Q}$ のそれぞれの固定群を求めよ.

(2) $H = \{\mathrm{Id}_L\}$, G のそれぞれの固定体を求めよ.

(解答)

(1) について.

$$\begin{aligned} H(L) &= G(L/L) = \{\sigma \in G \mid \tau\,|_L = \mathrm{Id}_L\} = \{\mathrm{Id}_L\}, \\ H(\mathbb{Q}) &= G(L/\mathbb{Q}) = G. \end{aligned}$$

(2) について.

$$L^H = \{x \in L \mid \mathrm{Id}_L(x) = x\} = L.$$

次に L^G について考える.

$$L^G = \{x \in L \mid \tau(x) = x\ (\forall \tau \in G)\} = \{x \in L \mid \sigma(x) = x\}$$

に注意する. $x = a + b\sqrt{2} \in L\ (a, b \in \mathbb{Q})$ を取ると,

$$\sigma(x) = x \iff a - b\sqrt{2} = a + b\sqrt{2} \iff b = 0 \iff x \in \mathbb{Q}.$$

従って $L^G = \mathbb{Q}$.

□

上の例題から, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ の部分体と $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ の部分群とは一対一に対応していることが分かります.

$$L \longleftrightarrow \{\mathrm{Id}_L\}, \qquad \mathbb{Q} \longleftrightarrow G.$$

このような性質を一般化したのがガロア理論の基本定理です.

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 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,

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

が成り立つ. つまり, 上記の写像は L/K の中間体と G の部分群の間に一対一対応を与える. 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.

$$\begin{tikzcd}
L \arrow[d, dash, "{[L:M]}"'] & & \{\mathrm{Id}_L\} \arrow[d, dash, "{|H|}"] \\
M \arrow[d, dash] \arrow[rr, leftrightarrow, dashed, "1 : 1"] & & H \arrow[d, dash] \\
K & & G
\end{tikzcd}$$

定理 11-2 は次回証明を与えます. 今回は定理の使い方を確認していきます.

例題 11-2

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ のとき, $L/\mathbb{Q}$ の中間体をすべて求めよ.

[解答]

定理 10-3 より, $L/\mathbb{Q}$ は 4 次ガロア拡大で, そのガロア群は

$$G = G(L/\mathbb{Q}) = \{\sigma_1 = \mathrm{Id}_L, \sigma_2, \sigma_3, \sigma_4\}$$

で与えられる. ただし, $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ は

$$\begin{aligned}
\sigma_1(\sqrt{2}) &= \sqrt{2}, & \sigma_1(\sqrt{3}) &= \sqrt{3}, \\
\sigma_2(\sqrt{2}) &= \sqrt{2}, & \sigma_2(\sqrt{3}) &= -\sqrt{3}, \\
\sigma_3(\sqrt{2}) &= -\sqrt{2}, & \sigma_3(\sqrt{3}) &= \sqrt{3}, \\
\sigma_4(\sqrt{2}) &= -\sqrt{2}, & \sigma_4(\sqrt{3}) &= -\sqrt{3}
\end{aligned}$$

を満たすものとする. $G \simeq C_2 \times C_2$ より, G の部分群は次の 5 つである.

$$G, \quad H_2 =< \sigma_2 >, \quad H_3 =< \sigma_3 >, \quad H_4 =< \sigma_4 >, \quad \{\mathrm{Id}_L\}.$$

これらに対応する中間体を求めればよい. ここでは, H_2 に対応する中間体のみ考察する.

$$\begin{aligned}
L^{H_2} &= \{x \in L \mid \sigma(x) \quad (\forall \sigma \in H_2)\} \\
&= \{x \in L \mid \sigma_2(x) = x\}.
\end{aligned}$$

$L/\mathbb{Q}$ の基底は $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ であるから, L の元を $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in L$ $(a, b, c, d \in \mathbb{Q})$ で表すと,

$$\begin{aligned}
x = \sigma_2(x) \quad &\iff \quad a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
&\iff \quad c = d = 0 \\
&\iff \quad x \in \mathbb{Q}(\sqrt{2}).
\end{aligned}$$

従って $L^{H_2} = \mathbb{Q}(\sqrt{2})$ が従う. 他の部分群に対応する中間体は次のようになる.

$$L^G = \mathbb{Q}, \quad L^{H_3} = \mathbb{Q}(\sqrt{3}), \quad L^{H_4} = \mathbb{Q}(\sqrt{6}), \quad L^{\{\mathrm{Id}_L\}} = L.$$

□

問題 11-1 例題 11-2 の状況を考える.

(1) 例題 11-2 と同様にして, $L^{H_3} = \mathbb{Q}(\sqrt{3})$ を証明せよ.

(2) $\Psi(\mathbb{Q}(\sqrt{6}))$ を計算し, $L^{H_4} = \mathbb{Q}(\sqrt{6})$ を確認せよ.

例題 11-3

$\alpha = e^{\frac{2\pi i}{5}} = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ とし，$L = \mathbb{Q}(\alpha)$ と置く．

(1) $L/\mathbb{Q}$ が 4 次ガロア拡大であることを示せ．

(2) G を $L/\mathbb{Q}$ のガロア群とし，$\sigma(\alpha) = \alpha^2$ を満たす $\sigma \in G$ を取る．このとき，$G =< \sigma >$ を示せ．

(3) $L/\mathbb{Q}$ の中間体をすべて求めよ．

(1) α の $\mathbb{Q}$ 上の最小多項式は

$$(1) f(x) = x^4 + x^3 + x^2 + x + 1 = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$$

である (問題 3-3)．よって $[L : \mathbb{Q}] = 4$．また $\alpha, \alpha^2, \alpha^3, \alpha^4$ はすべて L に含まれので，$L/\mathbb{Q}$ はガロア拡大である．

(2) $G = \{\sigma_1, \sigma_2,\ \sigma_3, \sigma_4\}$ と表す．ただし，$\sigma_1, \sigma_2,\ \sigma_3, \sigma_4$ は次を満たすものとする．

$$\sigma_1(\alpha) = \alpha,\quad \sigma_2(\alpha) = \alpha^2,\quad \sigma_3(\alpha) = \alpha^3,\quad \sigma_4(\alpha) = \alpha^4.$$

$\alpha^5 = 1$ に注意すれば，

$$\begin{array}{rcl} \sigma(\alpha) & = & \alpha^2, \\ \sigma^2(\alpha) & = & \sigma(\sigma(\alpha)) = \sigma(\alpha^2) = \alpha^4, \\ \sigma^3(\alpha) & = & \sigma(\sigma^2(\alpha)) = \sigma(\alpha^4) = \alpha^8 = \alpha^3, \\ \sigma^4(\alpha) & = & \sigma(\sigma^3(\alpha)) = \sigma(\alpha^3) = \alpha^6 = \alpha. \end{array}$$

よって $\sigma_1 = \sigma^4,\ \sigma_2 = \sigma,\ \sigma_3 = \sigma^3,\ \sigma_4 = \sigma^2$．従って $G =< \sigma >$．

(3) (2) より G は σ で生成される位数 4 の巡回群である．よって，G の部分群は次の 3 つである．

$$G =< \sigma >,\quad H =< \sigma^2 >,\quad \{\mathrm{Id}_L\}.$$

定理 11-2 から $L/\mathbb{Q}$ の中間体はちょうど 3 つ存在し，$L^G = \mathbb{Q},\quad L^{\{\mathrm{Id}_L\}} = L$ である．また

$$\frac{-1+\sqrt{5}}{4} = \cos\left(\frac{2\pi}{5}\right) = \frac{1}{2}\Big(\alpha + \frac{1}{\alpha}\Big) \in L$$

より，$\mathbb{Q}(\sqrt{5})$ は $L/\mathbb{Q}$ の中間体であり，$L^H = \mathbb{Q}(\sqrt{5})$ でなければならない．以上より，$L/\mathbb{Q}$ の中間体は $L,\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}$ の 3 つである．

□

問題 11-2　$\alpha = \sqrt{2+\sqrt{2}}$ とし, $L = \mathbb{Q}(\alpha)$ と置く. このとき, $L/\mathbb{Q}$ の中間体を求めよ (問題 10-3 を参照のこと).

問題 11-3　$L/\mathbb{Q}$ は奇数次のガロア拡大とするとき, $L \subseteq \mathbb{R}$ を示せ.