体論 (第10回)

10. ガロア拡大とガロア群

今回はガロア拡大とガロア群について解説します.

定義 10-1 (ガロア拡大)
L を $\mathbb{C}$ の部分体とし, L/K を代数拡大とする. 任意の $\alpha \in L$ の K 上共役がすべて L に含まれるとき L/K を**ガロア拡大**と言う.

[**注意**] 一般的には, 代数拡大 L/K に対して, 任意の $\alpha \in L$ の K 上共役がすべて L に含まれるとき, L/K を**正規拡大**と言い, さらに分離拡大でもあるとき, ガロア拡大と言う. 定理 7-2 から L が $\mathbb{C}$ の部分体の場合, L/K は常に分離拡大なので, 本資料では簡単のためガロア拡大の定義を上記のようにしている.

$L = \mathbb{Q}(\sqrt{2})$ を考える. $x = a + b\sqrt{2} \in L$ $(a, b \in \mathbb{Q})$ を取る. $x \in \mathbb{Q}$ のとき, x の $\mathbb{Q}$ 上共役は $x = a \in L$. $x \notin \mathbb{Q}$ のとき, x の $\mathbb{Q}$ 上共役は $a \pm b\sqrt{2} \in L$. どちらの場合でも x の $\mathbb{Q}$ 上共役は L に含まれるので, $L/\mathbb{Q}$ はガロア拡大である.

定理 10-1
K を $\mathbb{C}$ の部分体とする. $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ を K 上代数的な元とし, $L = K(\alpha_1, \ldots, \alpha_n)$ と置く. このとき, 次の二つは同値である.

(i) L/K がガロア拡大.

(ii) $\alpha_1, ..., \alpha_n$ の K 上共役はすべて L に含まれる.

[**証明**]
(i)⇒(ii) はガロア拡大の定義から従う.
(ii)⇒(i) について. $\beta \in L$ とし, その K 上共役 γ を考える. 定理 9-2 より $\sigma(\beta) = \gamma$ となる $\sigma \in \mathrm{Hom}_K(L, \mathbb{C})$ が存在する. σ は K-準同型より

$$\gamma = \sigma(\beta) \in K(\sigma(\alpha_1), \sigma(\alpha_2), ..., \sigma(\alpha_n)).$$

各 $\sigma(\alpha_i)$ は α_i の K 上共役より $\sigma(\alpha_i) \in L$. 従って $\gamma \in L$ である.

□

例 10-1

(1) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ はガロア拡大である.

(2) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ はガロア拡大でない.

[証明]
(1) $\sqrt{2}$, $\sqrt{3}$ の $\mathbb{Q}$ 上共役はそれぞれ $\pm\sqrt{2}$, $\pm\sqrt{3}$ である. $\pm\sqrt{2}$, $\pm\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ より定理 10-1 から $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ はガロア拡大である.

(2) $\sqrt[4]{2}$ の $\mathbb{Q}$ 上共役は $\pm\sqrt[4]{2}$, $\pm\sqrt[4]{2}i$ である. $\sqrt[4]{2}i \notin \mathbb{Q}(\sqrt[4]{2})$ より $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ はガロア拡大でない.

□

問題 10-1 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ はガロア拡大であることを示せ. ただし, $\omega = e^{\frac{2\pi i}{3}}$ は 1 の原始 3 乗根である.

定理 10-2
L を $\mathbb{C}$ の部分体とし, L/K を有限次ガロア拡大とする.

(1) $\mathrm{Hom}_K(L, \mathbb{C}) = \mathrm{Hom}_K(L, L)$.

(2) $\sigma \in \mathrm{Hom}_K(L, L)$ は環の同型写像.

[証明]
(1) $\subseteq$ を示せば十分である. $\alpha \in L$ とする. $\sigma(\alpha)$ は α の K 上共役で, L/K はガロア拡大より $\sigma(\alpha) \in L$. 従って $\sigma(L) \subseteq L$ となる.

(2) σ が全単射であることを確認する.

(i) L は体より $\ker\sigma$ は $\{0\}$ または L のいずれか. $1 \notin \ker\sigma$ より $\ker\sigma = \{0\}$. 従って σ は単射.

(ii) σ は K-線形写像であることに注意する. $\ker\sigma = \{0\}$ より,

$$\dim_K L = \dim_K \sigma(L) + \dim_K(\ker\sigma) = \dim_K \sigma(L).$$

$\sigma(L) \subseteq L$ であるから, $\sigma(L) = L$. 従って σ は全射.

□

定義 10-2 (ガロア群)

L を $\mathbb{C}$ の部分体とする. 有限次ガロア拡大 L/K に対して,

$$G(L/K) = \mathrm{Hom}_K(L, L)$$

と置く. このとき, $G(L/K)$ には写像の合成 $\circ$ で群構造が入る. この群を L/K の**ガロア群**と言う. 単位元は Id_L, また $\sigma \in G(L/K)$ の逆元は逆写像 σ^{-1} である.

[補足] 定理 10-2 から, $|G(L/K)| = |\mathrm{Hom}_K(L, \mathbb{C})| = [L : K]$.

$L = \mathbb{Q}(\sqrt{2})$ を考える. $L/\mathbb{Q}$ は 2 次ガロア拡大で, $G(L/\mathbb{Q}) = \{\mathrm{Id}_L,\ \sigma\}$ である. ここで, σ は $\sigma(\sqrt{2}) = -\sqrt{2}$ を満たすものとする. σ^2 を計算してみる.

$$\sigma^2(\sqrt{2}) = \sigma(\sigma(\sqrt{2})) = \sigma(-\sqrt{2}) = -\sigma(\sqrt{2}) = \sqrt{2}.$$

従って $\sigma^2 = \mathrm{Id}_L$ である.

□

定理 10-3

相異なる整数 $m,\ n \neq 0, 1$ は平方因子を持たず, また互いに素と仮定する. $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ と置く.

(1) $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$.

(2) $[L : \mathbb{Q}] = 4$.

(3) $\{1, \sqrt{m}, \sqrt{n}, \sqrt{mn}\}$ は $L/\mathbb{Q}$ の基底である.

(4) $L/\mathbb{Q}$ はガロア拡大である.

(5) 次の写像 φ は全単射である.

$$\varphi : G(L/\mathbb{Q}) \to \left\{\pm\sqrt{m}\right\} \times \left\{\pm\sqrt{n}\right\} \quad \left(\sigma \mapsto \left(\sigma(\sqrt{m}), \sigma(\sqrt{n})\right)\right)$$

(6) 群の同型 $G(L/\mathbb{Q}) \simeq C_2 \times C_2$ が成り立つ. ここで, C_n は位数 n の巡回群を表す.

※ 整数 x がどのような素数 p に対しても $p^2 \nmid x$ を満たすとき, x は**平方因子を持たない**と言う.

[補足] (5) より $G(L/\mathbb{Q})$ の 4 つの元を持ち, それらは次で特徴付けられる.

$$\begin{aligned}
&\sigma_1(\sqrt{m}) = \sqrt{m}, \qquad \sigma_1(\sqrt{n}) = \sqrt{n},\\
&\sigma_2(\sqrt{m}) = \sqrt{m}, \qquad \sigma_2(\sqrt{n}) = -\sqrt{n},\\
&\sigma_3(\sqrt{m}) = -\sqrt{m}, \quad \sigma_3(\sqrt{n}) = \sqrt{n},\\
&\sigma_4(\sqrt{m}) = -\sqrt{m}, \quad \sigma_4(\sqrt{n}) = -\sqrt{n}.
\end{aligned}$$

$G(L/\mathbb{Q})$ の単位元 Id_L は σ_1 である.

[定理 10-3 の証明]

(1) $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$ と仮定する. $\sqrt{n} = a + b\sqrt{m}$ $(a, b \in \mathbb{Q})$ と表す. $n = (a^2 + mb^2) + 2ab\sqrt{m}$ より, $a^2 + mb^2 = n$ および $2ab = 0$.

(i) $b = 0$ のとき, $n = a^2$ となり仮定に矛盾する.

(ii) $b \neq 0$ のとき, $a = 0$ である. $b = c/d$ $(c, d \in \mathbb{Z}, \gcd(c, d) = 1)$ と表すと, $d^2 n = c^2 m$. $\gcd(m, n) = \gcd(c, d) = 1$ より $m = \pm d^2$, $n = \pm c^2$ となる. m, n は平方因子を持たないので $m = n = -1$ となり矛盾.

以上より $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$ が示せた.

(2) $K = \mathbb{Q}(\sqrt{m})$ と置く. $\sqrt{n} \notin K$ より, $x^2 - n$ が $\sqrt{n}$ の K 上の最小多項式である. よって

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = [K(\sqrt{n}) : K][K : \mathbb{Q}] = 4.$$

(3) $\dim_{\mathbb{Q}} L = 4$ より, $\{1, \sqrt{m}, \sqrt{n}, \sqrt{mn}\}$ が $\mathbb{Q}$ 上 1 次独立であることを示せば十分である.

$$a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn} = 0 \ (a, b, c, d \in \mathbb{Q})$$

とすると,

$$a + b\sqrt{m} + \sqrt{n}(c + d\sqrt{m}) = 0.$$

$\{1, \sqrt{n}\}$ は K 上 1 次独立であるから,

$$a + b\sqrt{m} = 0, \quad c + d\sqrt{m} = 0.$$

従って $a = b = c = d = 0$. 以上より $\{1, \sqrt{m}, \sqrt{n}, \sqrt{mn}\}$ は $\mathbb{Q}$ 上 1 次独立である.

(4) $\sqrt{m}, \sqrt{n}$ の $\mathbb{Q}$ 上共役はそれぞれ $\pm\sqrt{m}$, $\pm\sqrt{n}$ である. $\pm\sqrt{m}$, $\pm\sqrt{n} \in L$ より, 定理 10-1 から $L/\mathbb{Q}$ はガロア拡大である.

(5) φ が単射であることを示す. $\sigma, \tau \in G(L/\mathbb{Q})$ $(\varphi(\sigma) = \varphi(\tau))$ とする. このとき,

$$\sigma(\sqrt{m}) = \tau(\sqrt{m}), \quad \sigma(\sqrt{n}) = \tau(\sqrt{n}).$$

$x \in L$ とし, $x = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn}$ $(a, b, c, d \in \mathbb{Q})$ で表すと,

$$\begin{aligned} \sigma(x) &= a + b\sigma(\sqrt{m}) + c\sigma(\sqrt{n}) + d\sigma(\sqrt{m})\sigma(\sqrt{n}) \\ &= a + b\tau(\sqrt{m}) + c\tau(\sqrt{m}) + d\tau(\sqrt{m})\tau(\sqrt{n}) \\ &= \tau(x). \end{aligned}$$

よって $\sigma = \tau$ であり, φ は単射である. また $|G(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4$ より φ は全射でもある.

(6) $G(L/\mathbb{Q})$ は位数 4 の群より $C_2 \times C_2$ または C_4 と同型である. 任意の $\sigma \in G(L/\mathbb{Q})$ に対して, $\sigma(\sqrt{m}) = \pm\sqrt{m}$, $\sigma(\sqrt{n}) = \pm\sqrt{n}$ であるから

$$\sigma^2(\sqrt{m}) = \sqrt{m}, \quad \sigma^2(\sqrt{n}) = \sqrt{n}.$$

従って $\sigma^2 = \mathrm{Id}_L$. これより $G(L/\mathbb{Q}) \simeq C_2 \times C_2$ である.

□

問題 10-2 定理 10-3 とその補足の記号のもとで考える.

(1) $\sigma_2 \circ \sigma_3$, σ_3^2, σ_4^{-1} はそれぞれ σ_1, σ_2, σ_3, σ_4 のいずれかを答えよ.

(2) $\beta = \sqrt{m} + \sqrt{n} + \sqrt{mn}$ の $\mathbb{Q}$ 上共役をすべて求めよ.

問題 10-3 $\alpha = \sqrt{2 + \sqrt{2}}$ とする.

(1) α の $\mathbb{Q}$ 上の最小多項式を求めよ.

(2) α の $\mathbb{Q}$ 上共役をすべて求めよ.

(3) $\mathbb{Q}(\alpha)/\mathbb{Q}$ がガロア拡大であることを示せ.

(4) $G(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq C_4$ を示せ.