

## §12. ガロア対応の例

**例 12.1 ( $\mathbf{Q}$  上の 2 次拡大)**  $\mathbf{Q}$  上の 2 次拡大体  $L$  は  $\mathbf{Q}$  上ガロアであり,  $\alpha \notin \mathbf{Q}$  をみたく任意の  $\alpha \in L$  をとれば,  $L = \mathbf{Q}(\alpha)$  である.  $\alpha$  の  $\mathbf{Q}$  上の最小多項式を

$$f(X) = X^2 + bX + c \quad (b, c \in \mathbf{Q})$$

とすると,  $\alpha$  は

$$\frac{-b + \sqrt{b^2 - 4c}}{2}, \quad \frac{-b - \sqrt{b^2 - 4c}}{2}$$

のどちらかであり, どちらであっても  $L = \mathbf{Q}(\sqrt{b^2 - 4c})$  である. 有理数  $b^2 - 4c$  の分母を  $s$  とすれば,  $s^2(b^2 - 4c) \in \mathbf{Z}$  かつ  $L = \mathbf{Q}(\sqrt{s^2(b^2 - 4c)})$  でもあるから,

$$L = \mathbf{Q}(\sqrt{m}) \quad (m \in \mathbf{Z})$$

と表すことができる. ここで, もし  $m$  が平方数  $l^2$  で割れて  $m = l^2 m'$  ならば  $L = \mathbf{Q}(\sqrt{m'})$  とできる. そこで, はじめから  $m$  は平方因子をもたない, つまり

$$m = -1 \text{ または } \pm p_1 p_2 \dots p_r \quad (p_i \text{ は相異なる素数})$$

の形をした整数であるとしてよい (このような整数は square-free な整数と呼ばれる).

さて,  $\sqrt{m}$  の  $\mathbf{Q}$  上の共役元は,  $\sqrt{m}$ ,  $-\sqrt{m}$  なので, 定理 6.11 より, 2 つの同型写像, すなわち  $\text{Gal}(L/\mathbf{Q})$  の元で

$$\sqrt{m} \mapsto \sqrt{m}, \quad \sqrt{m} \mapsto -\sqrt{m}$$

をみたくものがそれぞれ存在する. 前者は恒等写像  $\text{id}_L$  である. 後者を  $\sigma$  とすると,  $\sigma(\sqrt{m}) = -\sqrt{m}$ , より詳しく

$$\sigma : L \longrightarrow L, \quad a + b\sqrt{m} \mapsto a - b\sqrt{m} \quad (a, b \in \mathbf{Q})$$

となっている. ここで,

$$\sigma^2(a + b\sqrt{m}) = \sigma(a - b\sqrt{m}) = a - b(-\sqrt{m}) = a + b\sqrt{m}$$

より  $\sigma^2 = \text{id}_L$  が成り立っている. 以上をまとめて, 2 次拡大  $L/\mathbf{Q}$  のガロア群として位数 2 の巡回群

$$\text{Gal}(L/\mathbf{Q}) = \langle \sigma \rangle = \{1, \sigma\}$$

が得られたことになる (ただし,  $\text{id}_L = 1$  と略記した).

例 12.2 ( $\mathbf{Q}$  上の巡回拡大でない 4 次アーベル拡大)  $\mathbf{Q}$  上の拡大体

$$L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

を考える.  $\alpha = \sqrt{2} + \sqrt{3}$  とおけば  $L = \mathbf{Q}(\alpha)$  と書ける (例 2.4 参照).  $\sqrt{2}, \sqrt{3}$  の  $\mathbf{Q}$  上の共役元は, それぞれ  $\pm\sqrt{2}, \pm\sqrt{3}$  だから,  $\alpha$  の  $\mathbf{Q}$  上の共役元は  $\pm\sqrt{2} \pm \sqrt{3}$  (復号任意) のどれかである. 一方,

$$|\text{Conj}(\alpha, \mathbf{Q})| = [L : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4$$

より

$$\text{Conj}(\alpha, \mathbf{Q}) = \left\{ \sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3} \right\}$$

でなければならない. よって,

$$\text{Conj}(\alpha, \mathbf{Q}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\alpha) = L$$

がいえて,  $L/\mathbf{Q}$  は正規拡大であることがわかる. したがって  $L/\mathbf{Q}$  はガロア拡大である (多項式  $(X^2 - 2)(X^2 - 3)$  の  $\mathbf{Q}$  上の最小分解体であることからわかる).  $G$  をガロア群とする;  $G = \text{Gal}(L/\mathbf{Q})$ .  $L/\mathbf{Q}$  の中間体

$$M_2 = \mathbf{Q}(\sqrt{2}), \quad M_3 = \mathbf{Q}(\sqrt{3})$$

に対応する  $G$  の部分群を  $H_2, H_3$  とする. すなわち

$$H_2 = \text{Gal}(L/M_2), \quad H_3 = \text{Gal}(L/M_3),$$

または, これらと同値だが

$$M_2 = L^{H_2}, \quad M_3 = L^{H_3}$$

が成り立っている.

$$[L : M_2] = \frac{[L : \mathbf{Q}]}{[M_2 : \mathbf{Q}]} = \frac{4}{2} = 2, \quad [L : M_3] = \frac{[L : \mathbf{Q}]}{[M_3 : \mathbf{Q}]} = \frac{4}{2} = 2$$

より,  $H_2, H_3$  はどちらも位数 2 の群, したがって巡回群である. そこで, それらの生成元をそれぞれ  $\tau, \sigma \in G$  とする;

$$H_2 = \langle \tau \rangle, \quad H_3 = \langle \sigma \rangle.$$

このとき  $\sqrt{2} \in M_2 = L^{H_2}$  より  $\tau(\sqrt{2}) = \sqrt{2}$  が成り立つが, もし  $\tau(\sqrt{3}) = \sqrt{3}$  でもあるとすると,  $L$  全体が  $H_2$  で不変になるから,  $M_2 = L^{H_2} = L$  となって矛盾する. よって  $\tau(\sqrt{3}) = -\sqrt{3}$  でなければならない.  $H_3$  についても同様に考えて,

$$\begin{aligned} \sigma(\sqrt{2}) &= -\sqrt{2}, & \sigma(\sqrt{3}) &= \sqrt{3}, \\ \tau(\sqrt{2}) &= \sqrt{2}, & \tau(\sqrt{3}) &= -\sqrt{3}, \end{aligned}$$

したがって

$$\sigma(\alpha) = -\sqrt{2} + \sqrt{3}, \quad \tau(\alpha) = \sqrt{2} - \sqrt{3}$$

を得る. ここで,  $\sigma \neq \tau$  はあきらかだが,

$$\begin{aligned} \sigma\tau(\alpha) &= \sigma(\tau(\alpha)) = \sigma(\sqrt{2} - \sqrt{3}) = -\sqrt{2} - \sqrt{3}, \\ \tau\sigma(\alpha) &= \tau(\sigma(\alpha)) = \tau(-\sqrt{2} + \sqrt{3}) = -\sqrt{2} - \sqrt{3} \end{aligned}$$

より,  $\sigma\tau = \tau\sigma$  が成り立つ. したがって  $G$  はアーベル群である. また,  $\sigma\tau$  は  $\sigma$  とも  $\tau$  とも異なる  $G$  の元である.  $G$  の位数が体次数  $[L:\mathbf{Q}] = 4$  と一致することに注意すれば,

$$G = \{1, \sigma, \tau, \sigma\tau\} = \langle \sigma, \tau \rangle$$

と表され, 位数 4 のアーベル群であることがわかる. さらに  $G$  は位数 4 の元をもたないから巡回群ではない. 実際,  $G$  は位数 2 の巡回群の直積  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  と同型である. (加法群  $\mathbf{Z}/2\mathbf{Z}$  は位数 2 の巡回群 (生成元は  $\bar{1} = 1 + 2\mathbf{Z}$ ) であり, 同型写像

$$\varphi: G \longrightarrow \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

が

$$\varphi(\sigma) = (\bar{1}, \bar{0}), \quad \varphi(\tau) = (\bar{0}, \bar{1})$$

によって与えられる.)

**例 12.3 (Q 上の 6 次非アーベル拡大)**  $\alpha$  を  $X^3 - 5$  の実数根とし,  $\omega$  を 1 の原始 3 乗根とする ( $\omega = e^{\frac{2\pi i}{3}}$  と思ってよい). アイゼンシュタインの定理より,  $X^3 - 5$  は  $\mathbf{Q}$  上既約, したがって  $\alpha$  の  $\mathbf{Q}$  上の最小多項式である. さらに

$$X^3 - 5 = (X - \alpha)(X - \alpha\omega)(X - \alpha\omega^2)$$

より  $\text{Conj}(\alpha, \mathbf{Q}) = \{\alpha, \alpha\omega, \alpha\omega^2\}$  であって,  $X^3 - 5$  の  $\mathbf{Q}$  上の最小分解体  $L$  は

$$L = \mathbf{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbf{Q}(\alpha, \omega)$$

で与えられる.  $L/\mathbf{Q}$  のガロア群を  $G = \text{Gal}(L/\mathbf{Q})$  とおく. いま, 2つの中間体

$$K = \mathbf{Q}(\alpha), \quad F = \mathbf{Q}(\omega)$$

について

$$[K:\mathbf{Q}] = 3, \quad [F:\mathbf{Q}] = [\mathbf{Q}(\sqrt{-3}):\mathbf{Q}] = 2$$

に注意する (後者は  $\omega$  が  $X^2 + X + 1$  の根, すなわち  $(-1 \pm \sqrt{-3})/2$  であることからわかる). このことから,  $[L:\mathbf{Q}] = 6$ , したがって  $G$  の位数は 6 である.  $K, F$  に対応する  $G$  の部分群をそれぞれ  $H, N$  とする;

$$\begin{aligned} K &= L^H, & H &= \text{Gal}(L/K), \\ F &= L^N, & N &= \text{Gal}(L/F). \end{aligned}$$

このとき,

$$|H| = [L : K] = \frac{[L : \mathbf{Q}]}{[K : \mathbf{Q}]} = \frac{6}{3} = 2, \quad |N| = [L : F] = \frac{[L : \mathbf{Q}]}{[F : \mathbf{Q}]} = \frac{6}{2} = 3,$$

したがって,  $H$  は位数 2 の巡回群,  $N$  は位数 3 の巡回群である. それぞれの生成元を  $\tau, \sigma$  とする;

$$H = \langle \tau \rangle = \{1, \tau\}, \quad N = \langle \sigma \rangle = \{1, \sigma, \sigma^2\}.$$

ここで,  $\tau(\omega) = \bar{\omega} = \omega^2$  である. 実際, そうでないとすると  $\tau(\omega) = \omega$  だが,  $\alpha \in K$  より  $\tau(\alpha) = \alpha$  でもあるから,  $L = \mathbf{Q}(\alpha, \omega)$  が  $H$  の不変体となって矛盾する. 一方,  $\sigma(\alpha) = \alpha$  とすると, 今度は  $L$  が  $N$  の不変体となって矛盾するから,  $\sigma(\alpha) = \alpha\omega$  または  $\alpha\omega^2$  である. 後者の場合,

$$\sigma^2(\alpha) = \sigma(\alpha\omega^2) = \sigma(\alpha)\sigma(\omega)^2 = \alpha\omega^2\omega^2 = \alpha\omega^4 = \alpha\omega$$

であって, かつ  $N = \langle \sigma^2 \rangle$  でもあるから,  $\sigma^2$  をあらためて  $\sigma$  とおくことによって

$$\begin{aligned} \sigma(\alpha) &= \alpha\omega, & \sigma(\omega) &= \omega, \\ \tau(\alpha) &= \alpha, & \tau(\omega) &= \omega^2 \end{aligned}$$

であるとしてよい. このとき,

$$\begin{aligned} \tau\sigma(\alpha) &= \tau(\alpha\omega) = \alpha\omega^2, & \sigma^2\tau(\alpha) &= \sigma^2(\alpha) = \alpha\omega^2, \\ \tau\sigma(\omega) &= \tau(\omega) = \omega^2, & \sigma^2\tau(\omega) &= \sigma^2(\omega^2) = \omega^2 \end{aligned}$$

より  $\tau\sigma = \sigma^2\tau$  が示される. 次に, 定理 11.2 より,

$$\begin{aligned} \sigma(K) &= \mathbf{Q}(\sigma(\alpha)) = \mathbf{Q}(\alpha\omega) \text{ に対応する部分群は } \sigma H \sigma^{-1} = \langle \sigma\tau\sigma^{-1} \rangle, \\ \sigma^2(K) &= \mathbf{Q}(\sigma^2(\alpha)) = \mathbf{Q}(\alpha\omega^2) \text{ に対応する部分群は } \sigma^2 H \sigma^{-2} = \langle \sigma^2\tau\sigma^{-2} \rangle. \end{aligned}$$

さらに,  $\tau^2 = \sigma^3 = 1$  と  $\tau\sigma = \sigma^2\tau$  を使えば,

$$\sigma\tau\sigma^{-1} = \sigma^2\tau, \quad \sigma^2\tau\sigma^{-2} = \sigma\tau$$

および

$$G = \langle \sigma, \tau \rangle = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

が成り立つことがわかる. したがって,  $G$  は 3 次対称群  $S_3$  と同型な非アーベル群である.  $(G : N) = 2$  より  $N$  は  $G$  の正規部分群であり,  $F$  は  $\mathbf{Q}$  上のガロア拡大体である. これは  $[F : \mathbf{Q}] = 2$  からわかる (命題 9.3 参照). 一方,  $\text{Conj}(\alpha, \mathbf{Q}) \not\subseteq K = \mathbf{Q}(\alpha)$  より,  $K$  は  $\mathbf{Q}$  上ガロアではなく, したがって,  $H$  は  $G$  の正規でない部分群である. このことは,  $\sigma\tau\sigma^{-1} = \sigma^2\tau \notin H$  から直接確かめられる.