§12. ガロア対応の例

例 12.1（$\boldsymbol{Q}$ 上の 2 次拡大） $\boldsymbol{Q}$ 上の 2 次拡大体 L はガロア拡大であり，$\alpha \notin \boldsymbol{Q}$ である $\alpha \in L$ をとれば，$L = \boldsymbol{Q}(\alpha)$ である． α の $\boldsymbol{Q}$ 上の最小多項式を

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

とする． したがって，α は

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

のどちらかであり，どちらにしろ，$L = \boldsymbol{Q}\big(\sqrt{b^2 - 4c}\big)$ である． 有理数 $b^2 - 4c$ の分母を s とすれば，$s^2(b^2 - 4c) \in \boldsymbol{Z}$ かつ $L = \boldsymbol{Q}\Big(\sqrt{s^2(b^2 - 4c)}\Big)$ でもあるから，

$$L = \boldsymbol{Q}\big(\sqrt{m}\big) \qquad (m \in \boldsymbol{Z})$$

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 $L = \boldsymbol{Q}\big(\sqrt{m'}\big)$ とできる． そこで，はじめから m は平方因子を持たない，つまり

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

と表される整数であるとしてよい．

さて，$\sqrt{m}$ の $\boldsymbol{Q}$ 上の共役元は，$\sqrt{m}, -\sqrt{m}$ なので，定理 6.12 より，2 つの同型写像，すなわち $\mathrm{Gal}(L/\boldsymbol{Q})$ の元で

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

をみたすものが存在する． 前者は恒等写像 $\mathrm{id}_L (= 1$ と略す$)$ である． 後者を σ とすると，$\sigma(\sqrt{m}) = -\sqrt{m}$，より詳しく

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

となっている． ここで，

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

より $\sigma^2 = \mathrm{id}_L = 1$ が成り立っている． 以上をまとめて，2 次拡大 $L/\boldsymbol{Q}$ のガロア群として位数 2 の巡回群

$$\mathrm{Gal}(L/\boldsymbol{Q}) = \{1, \sigma\}$$

が得られたことになる．

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

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

を考える． $\alpha = \sqrt{2} + \sqrt{3}$ とおけば，$L = \boldsymbol{Q}(\alpha)$ と書ける． $\sqrt{2}, \sqrt{3}$ の $\boldsymbol{Q}$ 上の共役元は，それぞれ $\pm\sqrt{2}, \pm\sqrt{3}$ だから，α の $\boldsymbol{Q}$ 上の共役元は $\pm\sqrt{2} \pm \sqrt{3}$ (複号任意) のどれかである． 一方，$|\mathrm{Conj}(\alpha, \boldsymbol{Q})| = [L : \boldsymbol{Q}] = \big[\boldsymbol{Q}\big(\sqrt{2}, \sqrt{3}\big) : \boldsymbol{Q}\big] = 4$ だから，

$$\mathrm{Conj}(\alpha, \boldsymbol{Q}) = \Big\{\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3}\Big\}$$

でなければならない． これら 4 つの共役元はあきらかに $L = \boldsymbol{Q}\big(\sqrt{2}, \sqrt{3}\big)$ に属する（このことは

$$-\sqrt{2} + \sqrt{3} = \frac{\sqrt{3} - \sqrt{2}}{\sqrt{3}^2 - \sqrt{2}^2} = \frac{1}{\alpha}, \quad \sqrt{2} - \sqrt{3} = -\frac{1}{\alpha}, \quad -\sqrt{2} - \sqrt{3} = -\alpha$$

からもわかる）ので，$L/\boldsymbol{Q}$ は正規拡大であり，したがってガロア拡大である（標数 0 なので分離拡大である）． G をガロア群とする; $G = \mathrm{Gal}(L/\boldsymbol{Q})$． $L/\boldsymbol{Q}$ の中間体

$$M_2 = \boldsymbol{Q}\Big(\sqrt{2}\Big), \qquad M_3 = \boldsymbol{Q}\Big(\sqrt{3}\Big)$$

に対応する G の部分群を H_2, H_3 とする． すなわち

$$H_2 = \mathrm{Gal}(L/M_2), \qquad H_3 = \mathrm{Gal}(L/M_3),$$

または，これらと同値だが

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

が成り立っている．

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

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;

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

$\sqrt{2} \in M_2$ かつ M_2 は H_2 の不変体だから，$\tau(\sqrt{2}) = \sqrt{2}$ である． ここで，もし $\tau(\sqrt{3}) = \sqrt{3}$ だとすると，L 全体が H_2 で不変になるから，$M_2 = K^{H_2} = L$ 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，

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

したがって

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

を得る． ここで，$\sigma \neq \tau$ はあきらかだが，

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

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 σ とも τ とも異なる G の元である． G の位数が体次数 $[L : \boldsymbol{Q}] = 4$ 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． 加法群 $\boldsymbol{Z}/2\boldsymbol{Z}$ は位数 2 の巡回群（生成元は $\bar{1} = 1 + 2\boldsymbol{Z}$）であり，同型写像

$$\delta : G \longrightarrow \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$$

が

$$\delta(\sigma) = (\bar{1}, \bar{0}), \qquad \delta(\tau) = (\bar{0}, \bar{1})$$

によって与えられる．

例 12.3 （$\boldsymbol{Q}$ 上の 6 次非アーベル拡大） α を $X^3 - 5$ の実数根とし，ω 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 $\boldsymbol{Q}$ 上既約，したがって α の $\boldsymbol{Q}$ 上の最小多項式である． さらに

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

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

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

で与えられる．$L/\boldsymbol{Q}$ のガロア群を $G = \mathrm{Gal}(L/\boldsymbol{Q})$ とおく． 中間体 $K = \boldsymbol{Q}(\alpha)$ および $F = \boldsymbol{Q}(\omega)$ について

$$[K : \boldsymbol{Q}] = 3, \qquad [F : \boldsymbol{Q}] = \big[\boldsymbol{Q}\big(\sqrt{-3}\big) : \boldsymbol{Q}\big] = 2$$

に注意する（後者は ω 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，$[L : \boldsymbol{Q}] = 6$，したがって G の位数は 6 であることもわかる． いま，$K = \boldsymbol{Q}(\alpha)$ に対応する G の部分群を H とし，$F = \boldsymbol{Q}(\omega)$ に対応する G の部分群を N とすると，

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

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 τ, σ とする;

$$H = \langle \tau \rangle, \qquad N = \langle \sigma \rangle.$$

ここで，$\tau(\omega) = \omega^2$ 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，$L = \boldsymbol{Q}(\alpha, \omega)$ 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，

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

であって，かつ $N = \langle \sigma^2 \rangle$ でもあるから，σ^2 をあらためて σ 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 11.1 より，

$\sigma K = \boldsymbol{Q}(\sigma(\alpha)) = \boldsymbol{Q}(\alpha\omega)$ に対応する部分群は $\sigma H\sigma^{-1} = \langle \sigma\tau\sigma^{-1} \rangle$,
$\sigma^2 K = \boldsymbol{Q}\big(\sigma^2(\alpha)\big) = \boldsymbol{Q}\big(\alpha\omega^2\big)$ に対応する部分群は $\sigma^2 H\sigma^{-2} = \langle \sigma^{-1}\tau\sigma \rangle$.

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

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

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． $F/\boldsymbol{Q}$ は 2 次ガロア拡大だから，$N = \langle \sigma \rangle$ は G の正規部分群である．実際，

$$\begin{aligned} \tau^{-1}\sigma\tau(\alpha) &= \tau\sigma(\alpha) = \tau(\alpha\omega) = \alpha\tau(\omega) = \alpha\omega^2 = \sigma^2(\alpha), \\ \tau^{-1}\sigma\tau(\omega) &= \tau\sigma(\omega^2) = \tau(\omega)^2 = \omega^4 = \omega = \sigma^2(\omega) \end{aligned}$$

より，$\tau^{-1}\sigma\tau = \sigma^2 \in N$，よって $\tau^{-1}N\tau = N$ が成り立つ． 一方，$K/\boldsymbol{Q}$ はガロア拡大ではないから，H は G の正規でない部分群である．