§9. 正規拡大

定理 9.1 代数拡大 L/K について，次は同値である．

(i) すべての $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して $\sigma(L) \subset L$.

(ii) すべての $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して $\sigma(L) = L$.

(iii) すべての $\alpha \in L$ に対して $\mathrm{Conj}(\alpha, K) = \{\, \sigma(\alpha) \mid \sigma \in \mathrm{Aut}(L/K) \,\}$.

(iv) すべての $\alpha \in L$ に対して $\mathrm{Conj}(\alpha, K) \subset L$.

証明 (i)⇒(ii): $\sigma \in \mathrm{Aut}(\overline{K}/K)$ ならば，$\sigma^{-1} \in \mathrm{Aut}(\overline{K}/K)$ でもあるから，$\sigma^{-1}(L) \subset L$ が (i) より得られ，$L = \sigma(\sigma^{-1}(L)) \subset \sigma(L)$． よって (ii) が導かれた．
(ii)⇒(iii): $\alpha \in L$ とし，その K 上の最小多項式を $f(X)$ とする． 任意の $\sigma \in \mathrm{Aut}(L/K)$ に対して，$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ より，$\sigma(\alpha) \in \mathrm{Conj}(\alpha, K)$,

$$\therefore \quad \{\, \sigma(\alpha) \mid \sigma \in \mathrm{Aut}(L/K) \,\} \subset \mathrm{Conj}(\alpha, K).$$

逆の包含関係を示すために，$\beta \in \mathrm{Conj}(\alpha, K)$ とすると，定理 6.12（または系 6.13）から，$\beta = \tau(\alpha)$ をみたす $\tau \in \mathrm{Aut}(\overline{K}/K)$ がとれる． このとき (ii) より $\tau(L) = L$ なので，$\sigma = \tau|_L$ とおけば，$\sigma \in \mathrm{Aut}(L/K)$ であって，かつ $\beta = \tau(\alpha) = \sigma(\alpha)$ であるから，逆の包含関係が示された．
(iii)⇒(iv): $\alpha \in L$ ならば $\{\, \sigma(\alpha) \mid \sigma \in \mathrm{Aut}(L/K) \,\} \subset L$，よって (iii) より (iv) を得る．
(iv)⇒(i): $\alpha \in L$ とすると，系 6.13 より，$\sigma \in \mathrm{Aut}(\overline{K}/K)$ のとき $\sigma(\alpha) \in \mathrm{Conj}(\alpha, K)$. よって (iv) より $\sigma(\alpha) \in L$ となり，(i) が得られた． □

定義 9.2 前定理の条件が成り立つような代数拡大 L/K を**正規拡大**という． L は K 上**正規**であるともいう．

定義 9.3 体 K 上の多項式 $f(X)$ に対して，その根すべてを K に添加して得られる体を $f(X)$ の K 上の**最小分解体**という（それは K の代数拡大体，すなわち $\overline{K}$ の部分体になっている）．

例 9.4 α が K 上代数的であるとき，α の K 上の最小多項式の K 上の最小分解体は $K(\mathrm{Conj}(\alpha, K))$ で与えられる．

定理 9.5 代数拡大 L/K について，次は同値である．

(i) L/K は有限次正規拡大である．

(ii) L は K 上のある多項式の K 上の最小分解体である．

証明 (i)⇒(ii): L/K は有限次拡大だから，K 上代数的な有限個の $\alpha_1, \ldots, \alpha_n$ によって $L = K(\alpha_1, \ldots, \alpha_n)$ と表される．L/K が正規であるという仮定より $\mathrm{Conj}(\alpha_i, K) \subset L$ が成り立つ．一方，$f_i(X)$ を α_i の K 上の最小多項式とすると，$\mathrm{Conj}(\alpha_i, K)$ は $f_i(X)$ の根全体の集合と一致する．したがって，

$$f(X) = f_1(X) \cdots f_n(X)$$

とおくと，その K 上の最小分解体は

$$K(\mathrm{Conj}(\alpha_1, K) \cup \cdots \cup \mathrm{Conj}(\alpha_n, K)) \subset L$$

であるが，左辺が $K(\alpha_1, \ldots, \alpha_n) = L$ を含むのはあきらかなので (ii) が得られた．
(ii)⇒(i): L が $f(X) \in K[X]$ の K 上の最小分解体であるとする．すなわち，$f(X)$ の根全体の集合を A とすれば，$L = K(A)$ が成り立つ．いま，$\sigma \in \mathrm{Aut}(\overline{K}/K)$ を任意にとる．$\alpha \in A$ ならば，定理 6.12 より $\sigma(\alpha) \in \mathrm{Conj}(\alpha, K)$ であり，さらに α の K 上の最小多項式は $f(X)$ の因子だから，$\mathrm{Conj}(\alpha, K) \subset A$，よって $\sigma(A) \subset A$ が成り立つ（実際には $\sigma(A) = A$ がいえる）．したがって，定理 9.1 の (i) より，L は K 上正規である．□

例 9.6 ω を 1 の原始 3 乗根とし，

$$K = \boldsymbol{Q}(\omega), \quad M = \boldsymbol{Q}\left(\sqrt[3]{5}\right), \quad L = KM = \boldsymbol{Q}\left(\omega, \sqrt[3]{5}\right)$$

とおく．$K = \boldsymbol{Q}\left(\sqrt{-3}\right)$, $L = \boldsymbol{Q}\left(\sqrt[3]{5}, \sqrt{-3}\right)$ とも表せることに注意.

(a) K は，$X^2 + X + 1$ の $\boldsymbol{Q}$ 上の最小分解体であり，$\boldsymbol{Q}$ 上正規である.
(b) L は，$X^3 - 5$ の $\boldsymbol{Q}$ 上の最小分解体であり，$\boldsymbol{Q}$ 上正規である.
(c) M は，$\mathrm{Conj}(\sqrt[3]{5}, \boldsymbol{Q}) = \left\{\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega\sqrt[3]{5},\right\} \not\subset M$ より，$\boldsymbol{Q}$ 上正規ではない.

定理 9.7 α が体 K 上代数的であるとき，次は同値である.

(i) $K(\alpha)/K$ は正規拡大である.
(ii) $K(\alpha)$ は α の K 上の最小多項式の K 上の最小分解体である.
(iii) $K(\alpha) = K(\mathrm{Conj}(\alpha, K))$ が成り立つ.
(iv) $|\mathrm{Aut}(K(\alpha)/K)| = |\mathrm{Conj}(\alpha, K)|$ が成り立つ.

証明 (i)⇒(iv): 定理 6.14 の証明で見たように，単射

$$\Phi : \mathrm{Aut}(K(\alpha)/K) \longrightarrow \mathrm{Conj}(\alpha, K), \qquad \sigma \mapsto \sigma(\alpha)$$

が定まる．いま，$\beta \in \mathrm{Conj}(\alpha, K)$ を任意にとれば，仮定 (i) より $\beta \in K(\alpha)$ だから $K(\beta) \subset K(\alpha)$，さらに K 上の次数を考えることにより $K(\beta) = K(\alpha)$ である．一方，定理 6.12 より $\tau(\alpha) = \beta$ をみたす $\tau \in \mathrm{Aut}(\overline{K}/K)$ が存在する．そこで，$\sigma = \tau|_{K(\alpha)}$ とおけば，

$$\sigma(K(\alpha)) = K(\sigma(\alpha)) = K(\beta) = K(\alpha),$$

よって $\sigma \in \mathrm{Aut}(K(\alpha)/K)$ であって，もちろん $\sigma(\alpha) = \beta$． したがって，上記写像 Φ が全単射であることがわかり，(iv) を得る．
(iv)⇒(iii): 上で定めた Φ は，仮定 (iv) より全単射である． すなわち，$\beta \in \mathrm{Conj}(\alpha, K)$ ならば，$\sigma(\alpha) = \beta$ をみたす $\sigma \in \mathrm{Aut}(K(\alpha)/K)$ が存在し，とくに $\beta \in K(\alpha)$． したがって

$$K(\mathrm{Conj}(\alpha, K)) \subset K(\alpha).$$

逆の包含関係はあきらかだから，(iii) が示された．

(iii)⇒(ii): は最小分解体の定義より直ちにわかる．

(ii)⇒(i): も定理 9.5 よりあきらかである． □

例 9.8 (1) 任意の体 K の任意の 2 次拡大体は K 上正規である．

(2) $\boldsymbol{Q}(\alpha)/\boldsymbol{Q}$ を 3 次拡大とすると，α の $\boldsymbol{Q}$ 上の最小多項式 $f(X)$ は 3 次式である．

(a) $\boldsymbol{Q}(\alpha)/\boldsymbol{Q}$ が正規拡大ならば，$f(X)$ の 3 根はすべて実数である．

(b) $f(X)$ の実根がただひとつならば，$\boldsymbol{Q}(\alpha)/\boldsymbol{Q}$ は正規ではない．

例 9.9 3 次既約多項式 $g(X) = X^3 - 3X + 1$ の任意のひとつの根を β とすると，$\boldsymbol{Q}(\beta)/\boldsymbol{Q}$ は正規拡大である． 実際,

$$g\left(\frac{1}{1-\beta}\right) = -\frac{g(\beta)}{(1-\beta)^3} = 0, \qquad g\left(1 - \frac{1}{\beta}\right) = -\frac{g(\beta)}{\beta^3} = 0$$

より，$g(X)$ の他の 2 根が $\dfrac{1}{1-\beta}$, $1 - \dfrac{1}{\beta}$ であることが確かめられるので，$\boldsymbol{Q}(\beta)$ は $g(X)$ の $\boldsymbol{Q}$ 上の最小分解体，よって定理 9.7 より正規であることがわかる．

例 9.10 自然数 n に対して ζ_n を 1 の原始 n 乗根とする． すなわち，$\zeta_n \in \boldsymbol{C}^\times$ であって，その（乗法群 $\boldsymbol{C}^\times$ における）位数が n であるとする（$\zeta_n = e^{2\pi i/n}$ であるとしてよい）． このとき，$\boldsymbol{Q}(\zeta_n)$ は $\boldsymbol{Q}$ 上正規である． 実際，$\boldsymbol{Q}(\zeta_n)$ は $X^n - 1$ の $\boldsymbol{Q}$ 上の最小分解体である．

例 9.11 $\boldsymbol{Q}$ 上の拡大体 K が $\zeta_n \in K$ をみたすとき，任意の $a \in K$ に対して $K(\sqrt[n]{a})/K$ は正規拡大である． 実際，L を $X^n - a$ の K 上の最小分解体とすると，

$$L = K\big(\sqrt[n]{a},\ \zeta_n \sqrt[n]{a},\ \ldots,\ \zeta_n^{n-1} \sqrt[n]{a}\big).$$

ここで，$\zeta_n \in K$ に注意すれば，任意の $j = 0, 1, \ldots, n-1$ に対して $\zeta_n^j \sqrt[n]{a} \in K(\sqrt[n]{a})$，よって $L = K(\sqrt[n]{a})$ であり，これは K 上正規である．

定理 9.12 L/K を正規拡大とすると，任意の中間体 M に対して L/M は正規拡大である．

証明 $\alpha \in L$ のとき，$\mathrm{Conj}(\alpha, M) \subset \mathrm{Conj}(\alpha, K)$ だから，定理 9.1 (iv) を使えばよい． $\square$

注意 正規拡大 L/K の中間体 M は，一般には K 上正規にはならない． 例 9.6 を参照.

定理 9.13 L, E がともに K 上正規ならば，LE, $L \cap E$ はどちらも K 上正規である．

証明 定理 9.1 の条件 (i) を使う． $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して，仮定より $\sigma(L) \subset L$, $\sigma(E) \subset E$． よって，$\sigma(LE) \subset \sigma(L)\sigma(E) \subset LE$ かつ $\sigma(L \cap E) \subset \sigma(L) \cap \sigma(E) \subset L \cap E$ よりＯＫ. $\square$

定理 9.14 L/K を正規拡大とすると，任意の拡大 F/K に対して LF/F は正規拡大である．

証明 $\sigma \in \mathrm{Aut}(\overline{F}/F)$ に対して，$\sigma|_{\overline{K}} \in \mathrm{Aut}(\overline{K}/K)$ が成り立つことを確かめるのは難しくない． よって，L/K が正規であるという仮定より $\sigma(L) \subset L$ となるので，$\sigma(LF) = \sigma(L)\sigma(F) \subset LF$ が得られ，LF/F は正規である． $\square$

定義 9.15 代数拡大 L/K に対して，L を含む K 上の最小の正規拡大体を L/K の**正規閉包**という．

命題 9.16 α が K 上代数的であるとき，$K(\alpha)/K$ の正規閉包は $K(\mathrm{Conj}(\alpha, K))$ である．

証明 L を $K(\alpha)$ の正規閉包とする． 例 9.4 と定理 9.5 より，$K(\mathrm{Conj}(\alpha, K))$ は K 上正規だから，最小の正規拡大である L は $K(\mathrm{Conj}(\alpha, K))$ に含まれる． 一方，$\alpha \in L$ だから，定理 9.1 の条件 (iv) より，$\mathrm{Conj}(\alpha, K) \subset L$，したがって $K(\mathrm{Conj}(\alpha, K)) \subset L$． よって $L = K(\mathrm{Conj}(\alpha, K))$ を得る． $\square$