

## §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  $\sigma \in \text{Aut}(\overline{K}/K)$  に対して  $\sigma(L) \subset L$ .
- (ii) すべての  $\sigma \in \text{Aut}(\overline{K}/K)$  に対して  $\sigma(L) = L$ .
- (iii) すべての  $\alpha \in L$  に対して  $\text{Conj}(\alpha, K) = \{\sigma(\alpha) \mid \sigma \in \text{Aut}(L/K)\}$ .
- (iv) すべての  $\alpha \in L$  に対して  $\text{Conj}(\alpha, K) \subset L$ .

**証明** (i) $\Rightarrow$ (ii):  $\sigma \in \text{Aut}(\overline{K}/K)$  ならば,  $\sigma^{-1} \in \text{Aut}(\overline{K}/K)$  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) $\Rightarrow$ (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  $\sigma \in \text{Aut}(L/K)$  に対して,  $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$  より,  $\sigma(\alpha) \in \text{Conj}(\alpha, K)$ ,

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

逆の包含関係を示すために,  $\beta \in \text{Conj}(\alpha, K)$  とすると, 定理 6.12 (または系 6.13) から,  $\beta = \tau(\alpha)$  をみたす  $\tau \in \text{Aut}(\overline{K}/K)$  がとれる. このとき (ii) より  $\tau(L) = L$  なので,  $\sigma = \tau|_L$  とおけば,  $\sigma \in \text{Aut}(L/K)$  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) $\Rightarrow$ (iv):  $\alpha \in L$  ならば  $\{\sigma(\alpha) \mid \sigma \in \text{Aut}(L/K)\} \subset L$ , よって (iii) より (iv) を得る.

(iv) $\Rightarrow$ (i):  $\alpha \in L$  とすると, 系 6.13 より,  $\sigma \in \text{Aut}(\overline{K}/K)$  のとき  $\sigma(\alpha) \in \text{Conj}(\alpha, K)$ . よって (iv) より  $\sigma(\alpha) \in L$  となり, (i) が得られた.  $\square$

**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**  $\alpha$  が  $K$  上代数的であるとき,  $\alpha$  の  $K$  上の最小多項式の  $K$  上の最小分解体は  $K(\text{Conj}(\alpha, K))$  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) $\Rightarrow$ (ii):  $L/K$  は有限次拡大だから,  $K$  上代数的な有限個の  $\alpha_1, \dots, \alpha_n$  によって  $L = K(\alpha_1, \dots, \alpha_n)$  と表される.  $L/K$  が正規であるという仮定より  $\text{Conj}(\alpha_i, K) \subset L$  が成り立つ. 一方,  $f_i(X)$  を  $\alpha_i$  の  $K$  上の最小多項式とすると,  $\text{Conj}(\alpha_i, K)$  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

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

であるが, 左辺が  $K(\alpha_1, \dots, \alpha_n) = L$  を含むのはあきらかなので (ii) が得られた.

(ii) $\Rightarrow$ (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,  $\sigma \in \text{Aut}(\bar{K}/K)$  を任意にとる.  $\alpha \in A$  ならば, 定理 6.12 より  $\sigma(\alpha) \in \text{Conj}(\alpha, K)$  であり, さらに  $\alpha$  の  $K$  上の最小多項式は  $f(X)$  の因子だから,  $\text{Conj}(\alpha, K) \subset A$ , 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.  $\square$

**例 9.6**  $\omega$  を 1 の原始 3 乗根とし,

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

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

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

**定理 9.7**  $\alpha$  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  $\alpha$  の  $K$  上の最小多項式の  $K$  上の最小分解体である.
- (iii)  $K(\alpha) = K(\text{Conj}(\alpha, K))$  が成り立つ.
- (iv)  $|\text{Aut}(K(\alpha)/K)| = |\text{Conj}(\alpha, K)|$  が成り立つ.

**証明** (i) $\Rightarrow$ (iv): 定理 6.14 の証明で見たように, 単射

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

が定まる. いま,  $\beta \in \text{Conj}(\alpha, K)$  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  $\tau \in \text{Aut}(\bar{K}/K)$  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  $\sigma \in \text{Aut}(K(\alpha)/K)$  であって、もちろん  $\sigma(\alpha) = \beta$ . したがって、上記写像  $\Phi$  が全単射であることがわかり、(iv) を得る.

(iv) $\Rightarrow$ (iii): 上で定めた  $\Phi$  は、仮定 (iv) より全単射である. すなわち、 $\beta \in \text{Conj}(\alpha, K)$  ならば、 $\sigma(\alpha) = \beta$  をみたす  $\sigma \in \text{Aut}(K(\alpha)/K)$  が存在し、とくに  $\beta \in K(\alpha)$ . したがって

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

逆の包含関係はあきらかだから、(iii) が示された.

(iii) $\Rightarrow$ (ii): は最小分解体の定義より直ちにわかる.

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

(a)  $\mathbf{Q}(\alpha)/\mathbf{Q}$  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、 $\mathbf{Q}(\alpha)/\mathbf{Q}$  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  $\beta$  とすると、 $\mathbf{Q}(\beta)/\mathbf{Q}$  は正規拡大である. 実際、

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

より、 $g(X)$  の他の 2 根が  $\frac{1}{1-\beta}$ ,  $1 - \frac{1}{\beta}$  であることが確かめられるので、 $\mathbf{Q}(\beta)$  は  $g(X)$  の  $\mathbf{Q}$  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  $\zeta_n$  を 1 の原始  $n$  乗根とする. すなわち、 $\zeta_n \in \mathbf{C}^\times$  であって、その (乗法群  $\mathbf{C}^\times$  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、 $\mathbf{Q}(\zeta_n)$  は  $\mathbf{Q}$  上正規である. 実際、 $\mathbf{Q}(\zeta_n)$  は  $X^n - 1$  の  $\mathbf{Q}$  上の最小分解体である.

**例 9.11**  $\mathbf{Q}$  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、

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

ここで、 $\zeta_n \in K$  に注意すれば、任意の  $j = 0, 1, \dots, n-1$  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,  $\text{Conj}(\alpha, M) \subset \text{Conj}(\alpha, K)$  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.  $\sigma \in \text{Aut}(\overline{K}/K)$  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**  $\sigma \in \text{Aut}(\overline{F}/F)$  に対して,  $\sigma|_{\overline{K}} \in \text{Aut}(\overline{K}/K)$  が成り立つことを確かめるのは難しい. 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**  $\alpha$  が  $K$  上代数的であるとき,  $K(\alpha)/K$  の正規閉包は  $K(\text{Conj}(\alpha, K))$  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,  $K(\text{Conj}(\alpha, K))$  は  $K$  上正規だから, 最小の正規拡大である  $L$  は  $K(\text{Conj}(\alpha, K))$  に含まれる. 一方,  $\alpha \in L$  だから, 定理 9.1 の条件 (iv) より,  $\text{Conj}(\alpha, K) \subset L$ , したがって  $K(\text{Conj}(\alpha, K)) \subset L$ . よって  $L = K(\text{Conj}(\alpha, K))$  を得る.  $\square$