

## §4. 代数拡大

**定義 4.1**  $L/K$  を体の拡大とする.  $L$  の任意の元が  $K$  上代数的であるとき,  $L$  は  $K$  上代数的であるという. また,  $L/K$  を**代数拡大**という.  $L$  が  $K$  上代数的でないとき,  $L$  は  $K$  上**超越的**であるといい,  $L/K$  を**超越拡大**という.

**命題 4.2** 有限次拡大は代数拡大である.

**証明**  $L/K$  を有限次拡大とする. 任意の  $\alpha \in L$  に対して,  $L/K$  の中間体である  $K(\alpha)$  は, 定理 2.9 より  $K$  上の有限次拡大体だから, 定理 3.7 によって,  $\alpha$  は  $K$  上代数的である.  $L$  の任意の元が  $K$  上代数的であることが示されたから,  $L/K$  は代数拡大である.  $\square$

**命題 4.3** 体の拡大  $L/K$  に対して次は同値である.

- (i)  $L/K$  は有限次拡大である.
- (ii)  $K$  上代数的な有限個の元  $\alpha_1, \dots, \alpha_n \in L$  が存在して,  $L = K(\alpha_1, \dots, \alpha_n)$  が成り立つ.

**証明** (i) のとき, ベクトル空間としての  $L$  の  $K$  上の基底  $\alpha_1, \dots, \alpha_n$  をとれば, 前命題よりこれらはすべて  $K$  上代数的であり, (ii) が導かれる. 逆に, (ii) のときは,

$$K_0 = K, \quad K_1 = K_0(\alpha_1), \quad K_2 = K_1(\alpha_2), \quad \dots, \quad K_n = K_{n-1}(\alpha_n)$$

とおけば, 各  $i = 1, \dots, n$  について,  $\alpha_i$  は  $K_{i-1}$  上代数的だから, 定理 3.7 より  $K_i/K_{i-1}$  は有限次, よって, 定理 2.9 から  $L = K_n$  は  $K$  上有限次であり, (i) を得る.  $\square$

**定理 4.4**  $M$  を体の拡大  $L/K$  の中間体とすると, 次は同値である.

- (i)  $L/K$  は代数拡大である.
- (ii)  $L/M, M/K$  はともに代数拡大である.

**証明** (i) ならば (ii) が成り立つのはあきらかなので, 以下, (ii) を仮定して (i), すなわち, 任意の  $\alpha \in L$  が  $K$  上代数的であることを確かめればよい. (ii) より  $L/M$  は代数的だから,  $\alpha$  は  $M$  上代数的, したがって,  $\alpha$  を根とする  $M$  上の零でない多項式

$$g(X) = c_0 + c_1X + \dots + c_nX^n \quad (c_i \in M)$$

が存在する. いま,  $M_0 = K(c_0, c_1, \dots, c_n)$  とおくと,  $\alpha$  は  $M_0$  上代数的であるから, 定理 3.7 より  $M_0(\alpha)/M_0$  は有限次である. 一方, 仮定 (ii) より  $M/K$  も代数的なので  $c_i$  は  $K$  上代数的, よって, 前命題より  $M_0/K$  は有限次である. したがって, 定理 2.9 から,  $M_0(\alpha)/K$  は有限次拡大であり, さらに命題 4.2 から代数拡大でもある. とくに  $\alpha$  は  $K$  上代数的である.  $\square$

**例 4.5** 自然数  $n$  に対して,  $X^n - 1 = 0$  の根である複素数全体を  $W_n$  とする;

$$W_n = \{z \in \mathbf{C} \mid z^n = 1\}.$$

いま,

$$\zeta_n = e^{\frac{2\pi\sqrt{-1}}{n}} = \cos \frac{2\pi}{n} + \sqrt{-1} \sin \frac{2\pi}{n}$$

とおけば,  $W_n = \{\zeta_n^j \mid j = 0, 1, \dots, n-1\}$  と具体的にかけ, これが  $X^n - 1$  の根全体の集合と一致する. よって, 命題 4.3 より  $\mathbf{Q}(W_n)/\mathbf{Q}$  は有限次, したがって, 命題 4.2 より代数拡大である (実際には,  $\mathbf{Q}(W_n) = \mathbf{Q}(\zeta_n)$  が成り立っているので, 命題 4.3 は必要とせず, 定理 3.7 を使えばよい). とくに  $n$  が素数  $p$  の場合,  $\zeta_p$  は  $X^p - 1$  の既約因子  $X^{p-1} + X^{p-2} + \dots + X + 1$  の根だから, 定理 3.8 より,

$$[\mathbf{Q}(W_p) : \mathbf{Q}] = [\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1.$$

この等式は, 任意の自然数  $n$  に対して, オイラー関数  $\varphi$  を用いた等式

$$[\mathbf{Q}(W_n) : \mathbf{Q}] = [\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n)$$

に拡張されるが, 証明は少し難しい.

**補題 4.6**  $L/K$  を体の拡大とし,  $A \subset L$  とすると,  $K(A)$  は  $A$  の有限部分集合  $B$  のすべてを走らせることにより

$$K(A) = \bigcup_B K(B)$$

と表される. すなわち, 任意の  $\alpha \in K(A)$  に対して,  $\alpha \in K(\beta_1, \dots, \beta_n)$  であるような有限個の  $\beta_1, \dots, \beta_n \in A$  がとれる.

**証明**  $M = \bigcup_B K(B)$  とおく. このとき,  $M \subset K(A)$  は直ちにわかる. 一方, あきらかに  $K \subset M$  であり, また  $A \subset M$  もすぐにわかるから,  $M$  が体であれば  $K(A) \subset M$ , したがって補題を得る. 以下,  $M$  が体であることを確かめる.  $M$  の任意の元  $\beta, \gamma \neq 0$  に対して,  $\beta \in K(B)$ ,  $\gamma \in K(C)$  をみたす  $A$  の有限部分集合  $B, C$  がとれる.  $D = B \cup C$  とおけば,  $D$  も  $A$  の有限部分集合であって  $\beta, \gamma \in K(D)$  であるが,  $K(D)$  は体なので,  $\beta, \gamma$  の和, 差, 積, 商は  $K(D)$  に属する. さらに  $K(D) \subset M$  なので, これらは  $M$  に属する. よって,  $M$  は体である.  $\square$

**定理 4.7**  $L/K$  を体の拡大とし,  $A \subset L$  とする.  $A$  の任意の元が  $K$  上代数的ならば  $K(A)/K$  は代数拡大である.

**証明** 任意の  $\alpha \in K(A)$  に対して, 前補題から,  $\alpha \in K(\beta_1, \dots, \beta_n)$  をみたす  $\beta_i \in A$  がとれる. 仮定より  $\beta_i$  は  $K$  上代数的だから, 拡大  $K(\beta_1, \dots, \beta_n)/K$  は, 命題 4.3 より有限次, よって命題 4.2 より代数的, とくに  $\alpha$  は  $K$  上代数的である.  $\square$

**系 4.8**  $L/K$  を体の拡大とする.  $\alpha, \beta \in L$  ( $\beta \neq 0$ ) がともに  $K$  上代数的ならば, それらの和と差  $\alpha \pm \beta$ , 積  $\alpha\beta$ , 商  $\alpha/\beta$  はどれも  $K$  上代数的である.

**証明** 前定理より  $K(\alpha, \beta)$  は  $K$  上代数的であり,  $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha, \beta)$  だから結論を得る.  $\square$

**例 4.9** 複素数平面における単位円を  $S$  とする. また, ある自然数  $n$  に対して,  $z^n = 1$  をみたす複素数全体を  $W$  で表す.

$$S = \{z \in \mathbf{C} \mid |z| = 1\} = \{x + iy \in \mathbf{C} \mid x, y \in \mathbf{R}, x^2 + y^2 = 1\},$$

$$W = \{z \in \mathbf{C} \mid \exists n \in \mathbf{N} \text{ s.t. } z^n = 1\} = \bigcup_{n=1}^{\infty} W_n.$$

すべての  $n \in \mathbf{N}$  について,  $W_n \subset W \subset S$ , したがって  $\mathbf{Q}(W_n) \subset \mathbf{Q}(W) \subset \mathbf{Q}(S)$ . このとき, 以下が成り立つ.

- (1)  $\mathbf{Q}(W)/\mathbf{Q}$  は有限次ではない代数拡大である.
- (2)  $\mathbf{Q}(S)/\mathbf{Q}$  は超越拡大である. したがって  $\mathbf{Q}(S)/\mathbf{Q}(W)$  も超越拡大である.

(1) は, 定理 4.7 および例 4.5 から容易に証明できる. また,  $0 < \varepsilon < 1$  をみたす  $\mathbf{Q}$  上超越的な実数  $\varepsilon$  (たとえば  $\varepsilon = \pi/4$  など...) をとれば,  $\sqrt{1-\varepsilon^2} + \varepsilon i$  は  $S$  に属し,  $\mathbf{Q}$  上超越的であることが確かめられるから, (2) も示される.

**命題 4.10**  $L/K$  を体の拡大とし,  $M$  をその中間体とする.  $\alpha \in L$  が  $K$  上代数的であるとき,

$$[M(\alpha) : M] \leq [K(\alpha) : K]$$

が成り立つ.

**証明**  $\alpha$  の  $K$  上の最小多項式を  $f(X)$  とすると,  $\deg f = [K(\alpha) : K]$ . 一方,  $f(X)$  は  $M$  上の多項式でもあるから, 補題 3.5 より,  $[M(\alpha) : M] \leq \deg f$  であり, 求める不等式を得る.  $\square$

**例 4.11**  $X^3 - 1$  の 1 でない根のひとつを  $\omega$  とする (1 の原始 3 乗根). このとき,  $\omega, \omega^2$  は  $X^2 + X + 1$  の 2 根である.  $X^3 - 2$  の実根を  $\alpha$  とすれば, 他の根は  $\alpha\omega, \alpha\omega^2$  で与えられる.  $X^3 - 2$  は  $\mathbb{Q}$  上既約だから, 定理 3.8 より  $\mathbb{Q}(\alpha)/\mathbb{Q}$  は 3 次拡大である. このとき,

$$(a) \quad M_1 = \mathbb{Q}(\omega) \text{ とおけば, } [M_1(\alpha) : M_1] = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

$$(b) \quad M_2 = \mathbb{Q}(\alpha\omega) \text{ とおけば, } [M_2(\alpha) : M_2] = 2 < 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

が成り立ち, それぞれ, 前命題において, 等号が成り立つ例, 成り立たない例となっている.

**定義 4.12**  $\Omega/K$  を体の拡大とし,  $L, M$  をその中間体とすると,  $L, M$  をともに含む  $\Omega$  の最小の部分体を  $L, M$  の**合成体**といい  $LM$  で表す. すなわち,  $LM = L(M) = M(L)$  である.

**定理 4.13**  $L, M$  を体の拡大  $\Omega/K$  の中間体とする.  $L/K$  が有限次拡大ならば,

$$[LM : M] \leq [L : K]$$

が成り立ち, とくに,  $LM/M$  も有限次拡大である.

**証明** 命題 4.3 より,  $L = K(\alpha_1, \dots, \alpha_n)$  をみたす  $K$  上代数的な元  $\alpha_i$  がとれる. そこで, 体の拡大列  $K_0 \subset K_1 \subset \dots \subset K_n$  および  $M_0 \subset M_1 \subset \dots \subset M_n$  を

$$K_0 = K, \quad K_1 = K_0(\alpha_1), \quad K_2 = K_1(\alpha_2), \quad \dots, \quad K_n = K_{n-1}(\alpha_n)$$

$$M_0 = M, \quad M_1 = M_0(\alpha_1), \quad M_2 = M_1(\alpha_2), \quad \dots, \quad M_n = M_{n-1}(\alpha_n)$$

と定めれば, 命題 4.10 より  $[M_i : M_{i-1}] \leq [K_i : K_{i-1}]$ . さらに,  $L = K_n$  かつ  $LM = M_n$  だから, 定理 2.9 を何度か適用して

$$[LM : M] = [M_n : M_{n-1}] \cdots [M_1 : M_0] \leq [K_n : K_{n-1}] \cdots [K_1 : K_0] = [L : K]$$

が導かれる.  $\square$