

## §2. 体の拡大, 拡大次数

**定義 2.1** 体  $K$  が体  $L$  の部分体, つまり

$$K \subset L$$

のとき,  $L$  を  $K$  の**拡大体**という. このとき, 体の**拡大**  $L/K$  ということが多い. また,  $M$  が  $K$  の拡大体で, かつ  $L$  が  $M$  の拡大体, つまり

$$K \subset M \subset L$$

であるとき,  $M$  を拡大  $L/K$  の**中間体**という.

**定義 2.2**  $L/K$  を体の拡大とする.

- (1)  $L$  の部分集合  $A$  に対して,  $A$  を含む最小の  $L/K$  の中間体を  $K(A)$  と表し,  $K$  に  $A$  を**添加した体**という.
- (2) とくに  $A$  が有限集合で  $A = \{\alpha_1, \dots, \alpha_n\}$  のとき,  $K(A)$  を  $K(\alpha_1, \dots, \alpha_n)$  と略記する.
- (3) ただひとつの  $\alpha \in L$  により  $K(\alpha)$  と表される体を  $K$  の**単純拡大体**という. この場合,  $\alpha$  を拡大  $K(\alpha)/K$  の**原始元**という.

**命題 2.3**  $L/K$  を体の拡大とする.  $\alpha \in L$  に対して,  $K(\alpha)$  は  $K$  上  $\alpha$  で生成される可換環 (すなわち,  $K$  と  $\alpha$  を含む  $L$  の最小の部分環)

$$K[\alpha] = \{ g(\alpha) \mid g(X) \in K[X] \}$$

の商体である. したがって

$$K(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(X), h(X) \in K[X], h(\alpha) \neq 0 \right\}$$

が成り立つ.

**証明**  $K(\alpha)$  は  $K$  と  $\alpha$  を含む体だから,  $g(X), h(X) \in K[X]$  とすると  $g(\alpha), h(\alpha) \in K(\alpha)$ , さらに  $h(\alpha) \neq 0$  であれば  $g(\alpha)/h(\alpha) \in K(\alpha)$ . 一方,

$$\left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(X), h(X) \in K[X], h(\alpha) \neq 0 \right\}$$

は  $L$  の部分体なので,  $K(\alpha)$  の最小性から命題の主張は正しいことがわかる.  $\square$

例 2.4 有理数体  $\mathbf{Q}$  の拡大体について、いくつかの例をあげる.

$$(1) \mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\sqrt{2}-1) = \mathbf{Q}\left(\frac{1}{\sqrt{2}}\right) = \mathbf{Q}\left(\frac{1+3\sqrt{2}}{5-7\sqrt{2}}\right)$$

最初の等号は,

$$\sqrt{2}-1 \in \mathbf{Q}(\sqrt{2}) \text{ だから } \mathbf{Q}(\sqrt{2}-1) \subset \mathbf{Q}(\sqrt{2}),$$

$$\sqrt{2} = (\sqrt{2}-1) + 1 \in \mathbf{Q}(\sqrt{2}-1) \text{ だから } \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}-1)$$

よりわかる. 真ん中の等号はどうよ? 最後の等号は,

$$\alpha = \frac{1+3\sqrt{2}}{5-7\sqrt{2}} \text{ とおけば } \sqrt{2} = \frac{5\alpha-1}{7\alpha+3} \in \mathbf{Q}(\alpha)$$

となることを使えばわかるはず.

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

$\sqrt{2}+\sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$  より  $\mathbf{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$  は OK. 一方,  $\beta = \sqrt{2}+\sqrt{3}$  とおけば,  $\frac{1}{\beta} = \sqrt{3}-\sqrt{2}$  が成り立ち,

$$\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\beta) = \mathbf{Q}\left(\frac{1}{\beta}\right) = \mathbf{Q}(\sqrt{2}-\sqrt{3}).$$

さらに,

$$\sqrt{2} = \frac{\beta - \frac{1}{\beta}}{2} \in \mathbf{Q}(\beta), \quad \sqrt{3} = \frac{\beta + \frac{1}{\beta}}{2} \in \mathbf{Q}(\beta)$$

よって,  $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbf{Q}(\beta) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$ .

$$(3) \mathbf{Q}(\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{4})$$

$\gamma = \sqrt[3]{2}$ ,  $\delta = \sqrt[3]{4}$  とおけば,  $\delta = \gamma^2$  より  $\mathbf{Q}(\delta) \subset \mathbf{Q}(\gamma)$ . 逆に,  $\gamma = \frac{\delta^2}{2}$  より  $\mathbf{Q}(\gamma) \subset \mathbf{Q}(\delta)$ .

$$(4) \mathbf{Q}(\mathbf{Z}) = \mathbf{Q}, \quad \mathbf{Q}(\mathbf{R}) = \mathbf{R}, \quad \mathbf{Q}(\mathbf{R}, \sqrt{-1}) = \mathbf{C}, \quad \mathbf{Q}(\sqrt{-1}) \subsetneq \mathbf{C}$$

**定義 2.5**  $L/K$  を体の拡大とすると,  $L$  は  $K$  上のベクトル空間ともみなすことができる ( $L$  における和をベクトルの和,  $K$  の元に  $L$  の元をかける操作をスカラー倍とする). このとき,  $K$  上のベクトル空間としての  $L$  の次元を拡大  $L/K$  の次数といい

$$[L:K]$$

で表す.  $[L:K]$  が有限のとき,  $L/K$  は有限次拡大であるといい, そうでないとき無限次拡大であるという.

**例 2.6** (1)  $\mathbb{Q}(\sqrt{7})$  は  $\mathbb{Q}$  上 2 次拡大である,  $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$ .

だって,  $1, \sqrt{7}$  は,  $\mathbb{Q}$  上 1 次独立だし,  $\mathbb{Q}$  上  $\mathbb{Q}(\sqrt{7})$  を生成してるから,  $\mathbb{Q}$  上  $\mathbb{Q}(\sqrt{7})$  の基底だもん.

(2)  $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$  は 3 次拡大である,  $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ .

なぜかという,  $1, \sqrt[3]{5}, \sqrt[3]{25}$  は  $\mathbb{Q}(\sqrt[3]{5})$  の  $\mathbb{Q}$  上の基底だから.

**補題 2.7**  $M$  を体の拡大  $L/K$  の中間体とし,  $\alpha_1, \dots, \alpha_m \in M$ ,  $\beta_1, \dots, \beta_n \in L$  とする.

$\alpha_1, \dots, \alpha_m$  が  $K$  上 1 次独立であり, かつ  $\beta_1, \dots, \beta_n$  が  $M$  上 1 次独立

ならば,  $mn$  個の  $L$  の元  $\alpha_i\beta_j$  ( $i = 1, \dots, m, j = 1, \dots, n$ ) は  $K$  上 1 次独立である.

**証明**  $mn$  個の元  $\alpha_i\beta_j$  に  $K$  上の線形関係

$$\sum_{i=1}^m \sum_{j=1}^n c_{ij} \alpha_i \beta_j = 0 \quad (c_{ij} \in K)$$

があったとする. このとき, すべての  $i, j$  に対して  $c_{ij} = 0$  が成り立つことを確かめればよい. いま, 上式を書き換えて

$$\sum_{j=1}^n \left( \sum_{i=1}^m c_{ij} \alpha_i \right) \beta_j = 0$$

を考えると,  $\sum_{i=1}^m c_{ij} \alpha_i \in M$  であり,  $\beta_1, \dots, \beta_n$  が  $M$  上 1 次独立という仮定から,

$$\sum_{i=1}^m c_{ij} \alpha_i = 0 \quad (j = 1, \dots, n)$$

を得る. さらに,  $c_{ij} \in K$  であり, かつ  $\alpha_1, \dots, \alpha_m$  が  $K$  上 1 次独立という仮定から

$$c_{ij} = 0 \quad (i = 1, \dots, m, j = 1, \dots, n)$$

が導かれる. □

**補題 2.8**  $M$  を体の拡大  $L/K$  の中間体とし,  $\alpha_1, \dots, \alpha_m \in M$ ,  $\beta_1, \dots, \beta_n \in L$  とする.

$\alpha_1, \dots, \alpha_m$  が  $K$  上  $M$  を生成し, かつ  $\beta_1, \dots, \beta_n$  が  $M$  上  $L$  を生成する

ならば,  $mn$  個の  $L$  の元  $\alpha_i\beta_j$  ( $i = 1, \dots, m, j = 1, \dots, n$ ) は  $K$  上  $L$  を生成する.

**証明** 任意の  $\gamma \in L$  が,  $mn$  個の元  $\alpha_i\beta_j$  の  $K$  上の 1 次結合で表されることを確かめる. いま,  $\beta_1, \dots, \beta_n$  が  $M$  上  $L$  を生成するので,

$$\gamma = \sum_{j=1}^n b_j \beta_j$$

をみたく  $b_j \in M$  が存在する. さらに,  $\alpha_1, \dots, \alpha_m$  が  $K$  上  $M$  を生成するという仮定から,

$$b_j = \sum_{i=1}^m a_{ij} \alpha_i \quad (j = 1, \dots, n)$$

となる  $a_{ij} \in K$  がとれる. よって,

$$\gamma = \sum_{j=1}^n \left( \sum_{i=1}^m a_{ij} \alpha_i \right) \beta_j = \sum_{i=1}^m \sum_{j=1}^n a_{ij} \alpha_i \beta_j$$

と書け,  $\gamma$  が  $\alpha_i\beta_j$  たちの  $K$  上の 1 次結合で表されることがいえた.  $\square$

**定理 2.9**  $M$  を体の拡大  $L/K$  の中間体とすると,

$$[L : K] = [L : M][M : K]$$

が成り立つ. とくに,  $L/K$  が有限次拡大であるためには,  $L/M$ ,  $M/K$  がともに有限次拡大であることが必要十分である.

**証明**  $\alpha_1, \dots, \alpha_m$  を  $M$  の  $K$  上の基底,  $\beta_1, \dots, \beta_n$  を  $L$  の  $M$  上の基底とすると,

$$m = [M : K], \quad n = [L : M].$$

ここで, 補題 2.7 より,  $mn$  個の元  $\alpha_i\beta_j$  は  $K$  上 1 次独立だから

$$[L : K] \geq mn = [L : M][M : K],$$

一方, 補題 2.8 より,  $L$  は  $K$  上  $mn$  個の元によって生成されるから,

$$[L : K] \leq mn = [L : M][M : K]$$

が成り立ち, したがって等式が導かれる.  $\square$