# §8.　分離拡大

定理 6.3 より，体 $K$ 上の多項式 $f(X)$ は，$\overline{K}$ において $X-\alpha$ の形の 1 次式の積に分解される．同じ 1 次式をまとめてしまえば

$$
\begin{aligned}
&f(X) = c\,(X-\alpha_1)^{m_1}\,(X-\alpha_2)^{m_2}\cdots(X-\alpha_r)^{m_r}\\
&\text{ただし}\quad c\in K,\ \ \alpha_i\in\overline{K},\ \ m_i\in\boldsymbol{N}
\end{aligned}
$$

と表すことができる．ここで，$\alpha_1,\ldots,\alpha_r$ は $f(X)$ の相異なる根になっている．このとき，$m_i=1$ であるような $\alpha_i$ を $f(X)$ の**単根**といい，$m_i\geq 2$ である $\alpha_i$ を **重根**という．

**定義 8.1**　体 $K$ 上の多項式 $f(X)$ について，$\overline{K}$ におけるすべての根が単根であるとき，**分離的**であるという．一方，$\overline{K}$ において重根をもつとき，**非分離的**であるという．分離的な多項式を**分離多項式**，非分離的な多項式を**非分離的多項式**ともいう．

**定理 8.2**　$K$ を標数 0 の体，または有限体とすると，$K$ 上の任意の既約多項式は分離的である．

**証明**　$K$ 上の既約多項式 $f(X)$ が重根 $\alpha$ をもつとする．このとき

$$f(X)=(X-\alpha)^2 g(X)\qquad (g(X)\in\overline{K}[X])$$

とかけるが，微分すれば

$$f'(X)=2(X-\alpha)g(X)+(X-\alpha)^2 g'(X),$$

したがって，$f(\alpha)=f'(\alpha)=0$ となる．ここで，$K$ が標数 0 の体ならば，$f'(X)$ は零多項式ではなく，$\deg f'(X)<\deg f(X)$ が成り立つ．一方で，$f(X)$ は $\alpha$ の $K$ 上の最小多項式（の定数倍）なので矛盾する．そこで以下，$K$ の標数は $p>0$ であるとする．この場合でも，$f'(X)$ が零多項式でなければ同様に矛盾する．$f'(X)$ が零多項式であるとすると，簡単な考察から

$$f(X)=c_0+c_1X^p+c_2X^{2p}+\cdots+c_mX^{mp}\qquad (c_i\in K)$$

と書けることが確かめられる．さらに，$K$ が有限体で $|K|=p^n$ $(n\geq 1)$ であれば，任意の $c\in K$ に対して $c^{p^n}=c$ が成り立つから，とくに $c_i=b_i^p$ $(b_i\in K)$ と表すことができ，したがって

$$f(X)=b_0^p+b_1^pX^p+b_2^pX^{2p}+\cdots+b_m^pX^{mp}=\bigl(b_0+b_1X+b_2X^2+\cdots+b_mX^m\bigr)^p$$

となって，$f(X)$ の既約性に矛盾する．　□

**定義 8.3**　$K$ を体とする．$\alpha \in \overline{K}$ の $K$ 上の最小多項式が分離的であるとき，$\alpha$ は $K$ 上**分離的**であるという．

定理 6.14 の直後の注意から，次の定理を得る．

**定理 8.4**　$K$ を体とする．$\alpha \in \overline{K}$ について，次は同値である．

(i) $\alpha$ は $K$ 上分離的である．

(ii) $|\mathrm{Conj}(\alpha, K)| = [K(\alpha) : K]$ が成り立つ．

**補題 8.5**　$K$ を体とし，$\beta, \gamma \in \overline{K}$ とする．$\beta$ が $K$ 上分離的ならば，

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

をみたす $\alpha \in K(\beta, \gamma)$ が存在する．

**証明**　<u>$K$ が有限体のとき:</u>　$K$ の有限次拡大体である $K(\beta, \gamma)$ も有限体なので，§15 補遺で証明される命題 15.1『体の乗法群の有限部分群は巡回群である』を使えば，$K(\beta, \gamma)^{\times}$ は巡回群である．$\alpha$ をその生成元とすれば，$K(\beta, \gamma) = K(\alpha)$ が成り立つ．
<u>$K$ が無限体のとき:</u>　$\beta, \gamma$ から定まる $\overline{K}$ の有限部分集合

$$S = \left\{ \frac{\gamma - \gamma'}{\beta' - \beta} \;\middle|\; \beta \neq \beta' \in \mathrm{Conj}(\beta, K),\ \gamma' \in \mathrm{Conj}(\gamma, K) \right\}$$

に属さない $s \in K$ がとれる．$\alpha = \gamma + s\beta$ とおく．このとき $K(\alpha) \subset K(\beta, \gamma)$ であるが，一方で，もし $\beta \in K(\alpha)$ が示されれば，$\gamma = \alpha - s\beta \in K(\alpha)$ がいえて $K(\beta, \gamma) = K(\alpha)$ が得られる．そこで，以下，$\beta \notin K(\alpha)$ を仮定して矛盾を導く．さて，$\beta$ は $K$ 上分離的だから $K(\alpha)$ 上も分離的であり，したがって定理 8.4 より

$$|\mathrm{Conj}(\beta, K(\alpha))| = [K(\alpha, \beta) : K(\alpha)]$$

が成り立つが，$\beta \notin K(\alpha)$ を仮定したから右辺は 1 より大きくなっている．よって，$\beta' \neq \beta$ である $\beta' \in \mathrm{Conj}(\beta, K(\alpha))$ がとれる．いま，$g(X)$ を $\gamma$ の $K$ 上の最小多項式とし，$G(X) = g(\alpha - sX)$ とおくと，$G(X)$ は $K(\alpha)$ 上の多項式であって

$$G(\beta) = g(\alpha - s\beta) = g(\gamma) = 0.$$

よって，$G(X)$ は $\beta$ の $K(\alpha)$ 上の最小多項式で割り切れ，したがって $G(\beta') = 0$ が成り立つ．よって，$g(\alpha - s\beta') = 0$ より，$\alpha - s\beta' \in \mathrm{Conj}(\gamma, K)$．そこで $\gamma' = \alpha - s\beta'$ とおけば

$$\gamma' = (\gamma + s\beta) - s\beta', \qquad \therefore\ s = \frac{\gamma - \gamma'}{\beta' - \beta} \in S$$

となるが，$\beta' \in \mathrm{Conj}(\beta, K(\alpha)) \subset \mathrm{Conj}(\beta, K)$ に注意すれば，$s$ の取り方に矛盾する．$\square$

**定義 8.6**　代数拡大 $L/K$ において，すべての $\alpha \in L$ が $K$ 上分離的であるとき，$L/K$ を**分離拡大**という．また，このとき $L$ は $K$ 上**分離的**であるともいう．

**定理 8.7 (原始元定理)** 任意の有限次分離拡大は単純拡大である．すなわち $L/K$ が有限次分離拡大ならば，$L = K(\alpha)$ をみたす $\alpha \in L$ が存在する．

**証明**　次数 $[L:K]$ に関する数学的帰納法で示す．$[L:K] = 1$ すなわち $L = K$ のときはあきらか．以下，$[L:K] > 1$ とし，次数が $[L:K]$ より小さい場合は成り立つと仮定する（帰納法の仮定）．$[L:K] > 1$ より，$\beta \notin K$ である $\beta \in L$ が存在する．このとき

$$[L:K(\beta)] < [L:K] \quad \text{かつ} \quad L/K(\beta) \text{ は分離拡大}$$

だから，帰納法の仮定より $L = K(\beta, \gamma)$ をみたす $\gamma \in L$ が存在する．そこで，前補題を適用すれば，定理の主張を得る．□

**定理 8.8**　$K$ を標数 0 の体，または有限体とする．

(1) $K$ 上のすべての既約多項式は分離的である．
(2) $K$ 上のすべての代数拡大体は分離的である．
(3) $K$ 上のすべての有限次拡大体は単純である．

**証明**　定理 8.2 および定理 8.7 からすぐに得られる．□

次の補題は，定理 6.11 を使って証明される（§15 補遺を参照）．

**補題 8.9**　体 $K$ 上代数的である $\alpha, \beta$ が，$\beta \in K(\alpha)$ をみたすならば，

$$|\mathrm{Conj}(\alpha, K)| = |\mathrm{Conj}(\alpha, K(\beta))|\,|\mathrm{Conj}(\beta, K)|$$

が成り立つ．

**命題 8.10**　体 $K$ 上分離的である $\alpha$ に対して，$K(\alpha)/K$ は分離拡大である．

**証明**　任意の $\beta \in K(\alpha)$ について，$\beta$ が $K$ 上分離的であることを確かめればよい．そのために，まず，定理 6.14 より，

$$|\mathrm{Conj}(\alpha, K(\beta))| \leq [K(\alpha):K(\beta)], \qquad |\mathrm{Conj}(\beta, K)| \leq [K(\beta):K].$$

よって，前補題から

$$|\mathrm{Conj}(\alpha, K)| \leq [K(\alpha):K(\beta)][K(\beta):K] = [K(\alpha):K]$$

であるが，$\alpha$ は $K$ 上分離的だから，定理 8.4 より最左辺は $[K(\alpha):K]$ に等しく，したがって，3 つの不等号はすべて等号に置き換わる．とくに $|\mathrm{Conj}(\beta, K)| = [K(\beta):K]$ だから，再び定理 8.4 より $\beta$ は $K$ 上分離的である．□

**定理 8.11**　$M$ を代数拡大 $L/K$ の中間体とするとき，次は同値である．

(i) $L/K$ は分離拡大である．

(ii) $L/M$, $M/K$ はともに分離拡大である．

**証明**　(i) ならば (ii) は明らかなので，以下では (ii) を仮定して (i)，すなわち，任意の $\gamma \in L$ が $K$ 上分離的であることを示す．
$M/K$ が有限次拡大の場合:　$M/K$ が有限次分離拡大だから，原始元定理（定理 8.7）より，$M = K(\beta)$ をみたす $\beta \in M$ が存在する．このとき $M(\gamma) = K(\beta, \gamma)$ であるが，(ii) より $\beta$ は $K$ 上分離的なので，補題 8.5 より，$M(\gamma) = K(\alpha)$ をみたす $\alpha \in M(\gamma)$ が存在する．$M(\alpha) \subset M(\gamma) = K(\alpha) \subset M(\alpha)$ より $M(\alpha) = K(\alpha)$ であり，さらに (ii) から $\alpha$ が $M$ 上分離的であることもわかるから，定理 8.4 より

$$|\mathrm{Conj}(\beta, K)| = [K(\beta) : K], \qquad |\mathrm{Conj}(\alpha, M)| = [M(\alpha) : M] = [K(\alpha) : K(\beta)].$$

ここで，$\beta \in K(\alpha)$ であることから，補題 8.9 が適用できることに注意して

$$\begin{aligned}[K(\alpha) : K] &= [K(\alpha) : K(\beta)][K(\beta) : K] \\ &= |\mathrm{Conj}(\alpha, K(\beta))|\,|\mathrm{Conj}(\beta, K)| = |\mathrm{Conj}(\alpha, K)|\,.\end{aligned}$$

よって，定理 8.4 と命題 8.10 から，$K(\alpha) = M(\gamma)$ は $K$ 上分離的，とくに $\gamma$ は $K$ 上分離的であることが確かめられた．
$M/K$ が無限次拡大の場合:　$\gamma$ の $M$ 上の最小多項式の係数をすべて $K$ に添加した体を $M_0$ とする．$M_0$ は $M/K$ の中間体であり，仮定 (ii) より，$\gamma$ は $M_0$ 上分離的，かつ $M_0/K$ は有限次分離拡大である．そこで，$M$ を $M_0$ に置き換えて上の議論を適用すればよい．□

**命題 8.12**　$K$ を体とし，$\alpha, \beta \in \overline{K}$ が $K$ 上分離的であるとする．このとき，$K(\alpha, \beta)/K$ は分離拡大である．とくに，$\alpha \pm \beta, \alpha\beta, \alpha/\beta$ はどれも $K$ 上分離的である．

**証明**　命題 8.10 より，$K(\alpha)/K$ は分離拡大，さらに，$\beta$ は $K(\alpha)$ 上も分離的だから，$K(\alpha, \beta)/K(\alpha)$ も分離拡大である．よって，前定理より結論を得る．□

**定理 8.13**　$L$, $E$ がともに $K$ 上分離的ならば，$LE$, $L \cap E$ はどちらも $K$ 上分離的である．

**証明**　$LE$ の元は $L \cup E$ の有限個の元から加減乗除によって表されるから，前命題によって $K$ 上分離的であることがわかり，したがって $LE/K$ は分離拡大である．$(L \cap E)/K$ が分離拡大であることは明らかである．□