§7. 標数と分離性

K を体とする．自然数 n に対して $1 \in K$ の n 個の和を $\Gamma(n)$ とする;

$$\Gamma(n) = \underbrace{1 + \cdots + 1}_{n}$$

さらに，$\Gamma(-n) = -\Gamma(n)$，$\Gamma(0) = 0$ と定めれば，整数環 $\mathbb{Z}$ から体 K への準同型写像 $\Gamma : \mathbb{Z} \to K$ が定義される． 核 $\operatorname{Ker}\Gamma$ は $\mathbb{Z}$ の素イデアルなので，$\operatorname{Ker}\Gamma = (p)$ (ただし $p = 0$ または素数) となる．

定義 7.1 体 K に対して，$\operatorname{Ker}\Gamma = (p)$ をみたす $p \geq 0$ を K の**標数**という． 上述のように K の標数は 0 または素数である．

定義 7.2 素数 p に対して

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

とおく． $\mathbb{F}_p$ は p 個の元からなる有限体であって，標数は p である．

定理 7.3 (1) 体 K の標数が 0 ならば，単射準同型

$$\mathbb{Q} \longrightarrow K$$

が一意的に存在する． すなわち，K は有理数体 $\mathbb{Q}$ と同型な部分体をもつ．
(2) 体 K の標数が p ならば，単射準同型

$$\mathbb{F}_p \longrightarrow K$$

が一意的に存在する． すなわち，K は有限体 $\mathbb{F}_p$ と同型な部分体をもつ．

定義 7.4 体 K 上の多項式

$$f(X) = \sum_{j=0}^{n} c_j X^j = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0, \qquad c_j \in K$$

に対して，

$$f'(X) = \sum_{j=1}^{n} j c_j X^{j-1} = n c_n X^{n-1} + (n-1) c_{n-1} X^{n-2} + \cdots + c_1$$

を $f(X)$ の**形式的微分**（または単に**微分**）という．

命題 7.5　体 K 上の多項式 $f(X), g(X)$ に対して次が成り立つ．
(1) 任意の $a \in K$ に対して $\{af(X)\}' = af'(X)$,
(2) $\{f(X) + g(X)\}' = f'(X) + g'(X)$,
(3) $\{f(X)g(X)\}' = f'(X)g(X) + f(X)g'(X)$,
(4) $\{f(g(X))\}' = f'(g(X))g'(X)$.

定義 7.6　体 K 上の多項式 $f(X)$ が $\overline{K}$ において重根をもたないとき，$f(X)$ は**分離的**であるという． 分離的な多項式を**分離多項式**ともいう．

補題 7.7　体 K 上の多項式 $f(X)$ に対して次の (i), (ii) は同値である．
(i) $f(X)$ は分離的でない．
(ii) $f(\alpha) = f'(\alpha) = 0$ をみたす $\alpha \in \overline{K}$ が存在する．

さらに $f(X)$ が K 上既約ならば，次とも同値である．
(iii) $f'(X)$ は零多項式である．

定理 7.8　K を標数 p の体とし，$f(X)$ を K 上の既約多項式とする．
(1) $p = 0$ のとき，$f(X)$ は分離的である．
(2) $p > 0$ のとき，$f(X)$ が分離的であるためには，$f(X) = g(X^p)$ をみたす K 上の多項式 $g(X)$ が存在しないことが必要十分である．

定義 7.9　K を体とする．
(1) $\alpha \in \overline{K}$ の K 上の最小多項式が分離的であるとき，α は K 上**分離的**であるという．
(2) 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 7.10　K を体とする． $\alpha \in \overline{K}$ について，次は同値である．
(i) α は K 上分離的である．
(ii) $|\mathrm{Conj}(\alpha, K)| = [K(\alpha) : K]$ が成り立つ．

補題 7.11　K を体とし，$\alpha, \beta \in \overline{K}$ とする． α が K 上分離的ならば，$K(\alpha, \beta) = K(\gamma)$ をみたす $\gamma \in \overline{K}$ が存在する．

定理 7.12　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．

定理 7.13　標数 0 の体 K について次が成り立つ．
(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．