

§7. 標数

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, $\Gamma(-n) = -\Gamma(n)$, $\Gamma(0) = 0$ と定める.

補題 7.1 上で定めた写像

$$\Gamma: \mathbf{Z} \longrightarrow K$$

は, 可換環の準同型写像であり, その核は, $p = 0$ または素数によって, $\text{Ker } \Gamma = (p)$ と表される ($\text{Ker } \Gamma = p\mathbf{Z}$ と表してもよい).

証明 【準同型であること】 すべての $m, n \in \mathbf{Z}$ に対して

$$\Gamma(m+n) = \Gamma(m) + \Gamma(n), \quad \Gamma(mn) = \Gamma(m)\Gamma(n)$$

が成り立つことを確かめればよい. m, n のどちらかが 0 のときはあきらかに成り立つ. $m, n > 0$ のときは数学的帰納法を用いて確認できる. $n < 0$ のときは $\Gamma(-n) = -\Gamma(n)$ を使って正のときに帰着させればよい. $m < 0$ のときも同様である.

【核について】 Γ の像は体 K の部分環なので整域である. よって, 準同型定理より Γ の核は $\mathbf{Z}$ の素イデアル, したがって $\text{Ker } \Gamma = (0)$, または素数 p を用いて $\text{Ker } \Gamma = (p)$ と表される. $\square$

定義 7.2 体 K に対して, $\text{Ker } \Gamma = (p)$ をみたす $p \geq 0$ を K の**標数**という.

補題 7.1 より, K の標数は 0 または素数である. さらに, 整域 R に対しても同様にして標数を定義することができ, その場合でも, 標数は 0 または素数である.

写像 Γ を用いず直接的に標数を定義することもできる. K の単位元 1 を 2 個以上 p 個足し合わせて初めて 0 となる (すなわち

$$\underbrace{1 + \cdots + 1}_p = 0$$

となる) とき, p は素数である (証明してみよ). この p を K の標数とする. 1 をいくつ足し合わせても 0 にならないとき, K の標数を 0 とする.

定義 7.3 素数 p に対して

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

とかく. $\mathbf{F}_p$ 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 7.4 K を標数 p の体とする.

(1) $p = 0$ ならば, 単射準同型

$$\mathbf{Q} \longrightarrow K$$

が一意的に存在する. すなわち, K は有理数体 $\mathbf{Q}$ と同型な部分体をもつ.

(2) $p > 0$ すなわち p が素数ならば, 単射準同型

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

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

証明 (1) $n \neq 0$ ならば $\Gamma(n) \neq 0$ なので, $a = \frac{m}{n} \in \mathbf{Q}$ ($m, n \in \mathbf{Z}, n \neq 0$) のとき,

$$\tilde{\Gamma}(a) = \frac{\Gamma(m)}{\Gamma(n)}$$

とおくことによって

$$\tilde{\Gamma} : \mathbf{Q} \longrightarrow K$$

を定めることができる. $\tilde{\Gamma}$ が準同型写像であることを示すのは難しくない. よって $\tilde{\Gamma}$ は単射準同型写像である. 次に一意性を示すために,

$$\Delta : \mathbf{Q} \longrightarrow K$$

も単射準同型であるとする. このとき, $\tilde{\Gamma}(1) = 1 = \Delta(1)$ であり, 数学的帰納法を用いて $\tilde{\Gamma}(n) = \Delta(n)$ がすべての $n \in \mathbf{N}$ に対して成り立つことがわかる. このことから, すべての $a \in \mathbf{Q}$ に対して $\tilde{\Gamma}(a) = \Delta(a)$ を示すことは難しくない.

(2) $\Gamma : \mathbf{Z} \rightarrow K$ の核が $(p) = p\mathbf{Z}$ であることから, 準同型定理を適用すれば, 単射準同型写像

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \longrightarrow K$$

が得られる. 一意性については, $\mathbf{F}_p$ の元が $1 + \cdots + 1$ と表されることを使えば, すぐにわかる. $\square$

定理 7.5 K が有限体ならば, K の標数 p は素数であり, K は $\mathbf{F}_p$ の有限次拡大体と同型である. とくに, K が $\mathbf{F}_p$ の n 次拡大体と同型ならば, K は p^n 個の元からなる有限体である.

証明 前半は前定理からあきらかなので, 後半のみ示す. K は $\mathbf{F}_p$ の n 次拡大体であるとしてよい. $\alpha_1, \dots, \alpha_n$ を K の $\mathbf{F}_p$ 上の基底とすれば, K の任意の元は

$$c_1\alpha_1 + \cdots + c_n\alpha_n \quad (c_i \in \mathbf{F}_p)$$

の形に一意的に表され, 各 c_i の取り方は p 通りだから, K の元の個数は p^n である. $\square$

命題 7.6 p を素数とする.

(1) 体 K の標数が $p > 0$ ならば, 任意の $a, b \in K$ に対して

$$(a + b)^p = a^p + b^p$$

が成り立つ.

(2) $\mathbf{F}_p$ 上の多項式 $f(X)$ に対して,

$$f(X)^p = f(X^p)$$

が成り立つ.

証明 (1) 二項定理より

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p.$$

ここで, p は素数なので, $1 \leq j \leq p-1$ のときの二項係数は

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} \equiv 0 \pmod{p}.$$

よって, K において $\binom{p}{j}a^j b^{p-j} = 0$ となり, 求める等式を得る.

(2) $f(X)$ を具体的に

$$f(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \quad (c_i \in \mathbf{F}_p)$$

と表せば, (1) の証明と同様の議論を繰り返し使って

$$f(X)^p = c_n^p X^{np} + c_{n-1}^p X^{(n-1)p} + \cdots + c_1^p X^p + c_0^p.$$

ここで, **フェルマーの定理**より $c_i^p = c_i$ が成り立つから,

$$f(X)^p = c_n (X^p)^n + c_{n-1} (X^p)^{n-1} + \cdots + c_1 X^p + c_0 = f(X^p)$$

を得る. □

例 7.7 -1 は 3 を法として平方非剰余なので, $X^2 + 1$ は $\mathbf{F}_3$ 上既約である. したがって, §5 の考察から, 2 次拡大 $K/\mathbf{F}_3$ がとれて, K において $X^2 + 1$ は根をもつ. 実際には K は剰余環 $\mathbf{F}_3[X]/(X^2 + 1)$ と同型であり, X の属する類に対応する K の元を α とすると, 具体的に

$$K = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}.$$

と書ける. ただし, $\mathbf{F}_3 = \{0, 1, 2\}$ とする. このとき, $\alpha^2 = -1$ に注意すれば

$$(1 + \alpha)(2\alpha) = 2\alpha + 2\alpha^2 = 2\alpha - 2 = 1 + 2\alpha$$

のように積が計算できる (すべての積をチェックして, K の乗積表を作成してみよ).

例 7.8 任意の素数 p に対して, F_p 上の 2 次拡大が存在することが以下のようにしてわかる.

- (1) p が奇素数の場合, p を法として平方非剰余である整数 u が存在するから, 前の例と同様にして, $F_p[X]/(X^2 - u)$ と同型な F_p 上の 2 次拡大が存在する.
- (3) $p = 2$ の場合, $X^2 + X + 1$ が F_2 上既約であるから, やはり F_2 上の 2 次拡大が存在する.

例 7.9 p を素数とし, K/F_p を有限次拡大で $n = [K : F_p]$ とする. 写像 ϕ を

$$\phi : K \longrightarrow K, \quad \alpha \mapsto \alpha^p$$

によって定める. このような ϕ を K の**フロベニウス写像**という.

- (1) ϕ は K から K への準同型写像である.

なぜなら, $\alpha, \beta \in K$ に対して, $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ はあきらかであり, さらに定理 7.6 から $\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$ もいえるから.

- (2) ϕ は F_p 上の同型写像である. すなわち $\phi \in \text{Aut}(K/F_p)$.

なぜなら, $a \in F_p$ に対して $\phi(a) = a^p = a$ がいえるから (フェルマーの定理).

- (3) 自然数 j に対して, ϕ の j 個の合成を ϕ^j とする;

$$\phi^j = \underbrace{\phi \circ \cdots \circ \phi}_j$$

さらに $\phi^0 = \text{id}$ (恒等写像) とする. $\phi^j \in \text{Aut}(K/F_p)$ である.

- (4) $0 < j < n$ のとき, $\phi^j \neq \text{id}$.

なぜなら, もし $\phi^j = \text{id}$ ならば, すべての $\alpha \in K$ に対して $\alpha = \phi^j(\alpha) = \alpha^{p^j}$ だから, K のすべての元は多項式 $X^{p^j} - X$ の根である. しかし, 定理 7.5 より, K の元の個数は p^n なので, p^j 次多項式の根だけでは尽くせないはずなので矛盾.

- (5) ϕ^j ($0 \leq j < n$) は互いに相異なる.

なぜなら, もし $\phi^j = \phi^k$ ($0 \leq j < k < n$) ならば $\phi^{k-j} = \text{id}$ となって (4) に反する.

- (6) $\text{Aut}(K/F_p) = \{\text{id}, \phi, \phi^2, \dots, \phi^{n-1}\}$.

なぜなら, あきらかに $\text{Aut}(K/F_p) \supset \{\text{id}, \phi, \phi^2, \dots, \phi^{n-1}\}$. (5) より右辺は n 個の元をもつから $|\text{Aut}(K/F_p)| \geq n$. 一方, 命題 15.1 (§15 補遺参照) より, $K^\times$ は巡回群であり, その生成元を γ とすれば $K = F_p(\gamma)$ なので, 定理 6.14 が適用できて $|\text{Aut}(K/F_p)| \leq [K : F_p] = n$. よって, 不等式はすべて等号に置き換わり, 上の包含関係も等号で結ばれることがわかる.

- (7) $\phi^n = \text{id}$.

なぜなら, $\phi^n \in \text{Aut}(K/F_p)$ だから, (6) より $\phi^n = \phi^j$ ($0 \leq j < n$) をみたす j がある. もし $j > 0$ ならば, $\phi^{n-j} = \text{id}$ かつ $0 < n-j < n$ であり (4) に反する. したがって $j = 0$ であり $\phi^n = \phi^0 = \text{id}$.