

§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. そこで, m, n がどちらも正のとき, どちらか一方が負のとき, どちらも負のときの場合分けし, 厳密には数学的帰納法を用いて確認する (というわけで, あとはキミたちにおまかせっっちゃうわけ).

【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.

注意 補題 7.1 より, K の標数は 0 または素数である. 以下のように, 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 となる時 (すなわち $\underbrace{1 + \cdots + 1}_p = 0$ のとき), 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. さらに, 整域 R に対しても, 上と同様にして標数を定義することができる. この場合も, 整域 R の標数は 0 または素数である.

定義 7.3 素数 p に対して

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

とおく. \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. これが単射準同型写像であることを示すのは難しくない. 次に一意性を示すために, $\Delta : \mathbf{Q} \rightarrow K$ も単射準同型であるとする. このとき, $\tilde{\Gamma}(1) = 1 = \Delta(1)$ である. いま, $1 \in \mathbf{Q}$ から始めて四則演算を繰り返して得られる集合が \mathbf{Q} に一致することと, $\tilde{\Gamma}, \Delta$ がともに準同型であることを合わせて考えれば, すべての $a \in \mathbf{Q}$ に対して $\tilde{\Gamma}(a) = \Delta(a)$ が示され, 一意性を得る.

(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, $1 \in \mathbf{F}_p$ から始めて四則演算を繰り返して得られる集合が \mathbf{F}_p に一致すること以外は上と同様である. \square

定義 7.5 体 K に対して, 前定理から定まる, \mathbf{Q} または \mathbf{F}_p と同型な部分体を, K の素体という.

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) 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. □

定理 7.7 p を素数, K/\mathbf{F}_p を n 次拡大とすると, K の元の個数は p^n である.

証明 $\alpha_1, \dots, \alpha_n$ 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. □

例 7.8 -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 7.9 任意の素数 p に対して, F_p 上の 2 次拡大体が存在することが以下のよう
にしてわかる.

(1) 任意の奇素数 p に対して, 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 次拡大体が存在
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
大体が存在する.

例 7.10 p を素数とする. $f(X)$ を F_p 上の既約多項式, α をその根とすると
 $K = F_p(\alpha)$ は F_p 上の n 次拡大体である. 写像 ϕ を以下のように定める.

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

(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, 例 7.7 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, (5) より右辺は n 個の元を持ち, それらが左辺に属しているので,
 $|\text{Aut}(K/F_p)| \geq n$. 一方, 定理 6.14 より $|\text{Aut}(K/F_p)| \leq [K : F_p] = n$ だから,
不等式はすべて等号であり, $\text{Aut}(K/F_p)$ は $\{\phi^j \mid j = 0, 1, \dots, n-1\}$ と一致する.

(7) ϕ を F_p 上のフロベニウス写像という.