

8 第8回

8.1 ベキ表現の続き

$GF(p^m)$ の元が原始元 β のべき表現で表されている場合、乗算は $\beta^{p^m-1} = 1$ であることを用いて

$$\beta^i \cdot \beta^j = \beta^{R_{p^m-1}[i+j]}$$

によって簡単に行える。また、 β^i の乗法逆元は β^{p^m-1-i} で与えられる。なぜなら

$$\beta^i \cdot \beta^{p^m-1-i} = \beta^{p^m-1} = 1$$

例 $GF(4) = \{0, 1, \alpha, \alpha + 1\}$ において $\alpha + 1 = \alpha^2$ なので、

$$(\alpha + 1) \cdot (\alpha + 1) = \alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha$$

8.2 標数

有限体 F の零元を 0、(乗法) 単位元を 1 とする。さて、単位元 1 を n 個加えた結果を $\bar{n}$ とすれば

$$\bar{n} = \underbrace{1 + 1 + \cdots + 1}_{n \text{ 個}}$$

であり、 F は要素数が有限なので

$$\bar{1}, \bar{2}, \bar{3}, \dots, \bar{n}, \dots$$

が全て異なることはない。すなわち

$$\bar{m} = \bar{n} = \underbrace{1 + 1 + \cdots + 1}_{m \text{ 個}} = \underbrace{1 + 1 + \cdots + 1}_{n \text{ 個}}$$

が成り立つ自然数 m, n ($0 < m < n$) が存在する。この式の両辺に -1 (1 の加法逆元) を m 個加えると

$$\underbrace{1 + 1 + \cdots + 1}_{n-m \text{ 個}} = \overline{n-m} = 0$$

が得られる。ここで、 $\overline{n-m} = 0$ となる最小の自然数 $n - m = d_0$ を体 F の「標数」という。

例 $GF(2^2) = \{0, 1, \alpha, \alpha + 1\}$ の標数は、 $1 + 1 = 0$ から 2 である。 $GF(5) = \{0, 1, 2, 3, 4\}$ の標数は、 $1 + 1 = 2, 1 + 1 + 1 = 3, 1 + 1 + 1 + 1 = 4, 1 + 1 + 1 + 1 + 1 = 0$ から 5 である。

補題 2 有限体 F の標数 d_0 は素数である。

証明 標数 d_0 が合成数であったとして矛盾を示す。 $d_0 = d_1 d_2$ ($d_1 > 1, d_2 > 1$) とすれば、分配則から

$$\begin{aligned} 0 = \overline{d_0} &= \underbrace{1 + 1 + \cdots + 1}_{d_0} \\ &= \underbrace{(1 + 1 + \cdots + 1)}_{d_1} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{d_2} \\ &= \overline{d_1} \cdot \overline{d_2} \end{aligned}$$

が得られる。両辺に $(\overline{d_2})^{-1}$ を乗じれば

$$0 = \overline{d_1} \cdot \overline{d_2} \cdot (\overline{d_2})^{-1} = \overline{d_1}$$

となる。 $d_1 < d_0$ なので、 d_0 を標数とした仮定に矛盾する。

8.3 最小多項式

$GF(p^m)$ の元 β に対し、 $m(\beta) = 0$ となる $GF(p)$ 上の最小次数のモニック多項式 $m(x)$ を β の $GF(p)$ 上の最小多項式という。

定理 19 $\forall \beta \in GF(p^m)$ に対して β の $GF(p)$ 上の最小多項式は一意に存在する。

証明 $GF(p^m)$ の任意の元は、多項式 $f(x) = x(x^{p^m-1} - 1)$ の根である。また、 $f(x)$ は

$$f(x) = x(x^{p^m-1} - 1) = m_1(x)m_2(x) \cdots m_L(x)$$

と一意的に因数分解される。但し、 $m_l(x)$ ($l = 1, 2, \dots, L$) は $GF(p)$ 上の素多項式である。 β は $f(x)$ の単根であるので、 $m_1(x) \sim m_L(x)$ のいずれか 1 つの多項式の根でなければならない。従って、ある l について $m_l(x) = 0$ が成り立つ。 $m_l(x)$ は素多項式なので、最小多項式である。

他方、 β を根とする最小次数のモニック多項式が 2 つ存在したとし、それらを $m_1(x) \neq m_2(x)$ とすれば

$$m(x) = m_1(x) - m_2(x)$$

もまた β を根として有し、

$$\deg m(x) < \deg m_1(x) = \deg m_2(x)$$

となる。これは、次数の最小性に矛盾する。従って、 $m_1(x) = m_2(x)$ でなければならない。

例 $p(x) = x^3 + x + 1$ の根の 1 つ α によって作られる $GF(2^3)$ において、 α の $GF(2)$ 上の最小多項式を求めよう。

$$\begin{aligned} x(x^7 - 1) &= x(x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \\ &\parallel \\ &p(x) \end{aligned}$$

従って、 α の最小多項式は $x^3 + x + 1$ である。一方、 $(\alpha + 1)$ の $GF(2)$ 上の最小多項式の候補は、 $x^3 + x + 1$ と $x^3 + x^2 + 1$ であり、代入して計算を行うと

$$\begin{aligned} (\alpha + 1)^3 + (\alpha + 1) + 1 &= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha + 1) + 1 \\ &= \alpha^3 + \alpha^2 + 1 \\ &= \alpha + 1 + \alpha^2 + 1 = \alpha + \alpha^2 \\ (\alpha + 1)^3 + (\alpha + 1)^2 + 1 &= (\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^2 + 1 + 1 \\ &= \alpha^3 + \alpha + 1 = 0 \end{aligned}$$

が得られる。従って、 $(\alpha + 1)$ の最小多項式は $x^3 + x^2 + 1$ である。

8.4 線形符号

[定義] F を体とすると、 $V = F^n$ の線形部分空間 C を線形符号という。 C の次元を k とし、 C の基底を $\{e_1, e_2, \dots, e_k\}$ とする。このとき、

$$G = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix} \quad (e_i \text{ は行ベクトル})$$

を生成行列という。また

$$C = \left\{ (i_1, i_2, \dots, i_k)G \mid (i_1, i_2, \dots, i_k) \in F^k \right\}$$

と書け、 C の要素を符号語という。

この定義から直ちに、 $v_1 = i_1 G, v_2 = i_2 G$ ならば、 $\forall \alpha, \beta \in F$ に対し

$$\alpha v_1 + \beta v_2 = (\alpha i_1 + \beta i_2)G \in C$$

が成り立つ。すなわち、線形符号の符号語の線形結合もまた符号語となっている。

[定義](ハミング重み) ベクトル $\mathbf{v} \in F^n$ のハミング重み $\overline{W}_H(\mathbf{v})$ は $\mathbf{v}$ 中の非零の要素数に等しい。すなわち

$$\overline{W}_H(\mathbf{v}) = D_H(\mathbf{v}, \mathbf{0}) \quad \mathbf{0} : \text{零ベクトル}$$

である。但し、 D_H はハミング距離を表す。

[定義] 線形符号 C の最小距離 d は

$$d = \min_{\substack{\mathbf{v} \in C \\ \mathbf{v} \neq \mathbf{0}}} \overline{W}_H(\mathbf{v})$$

を満足する。すなわち、線形符号の最小距離は非零の符号語の最小ハミング重みに等しい。

証明

$$\begin{aligned} d &= \min_{\substack{\mathbf{v}_i, \mathbf{v}_j \in C \\ \mathbf{v}_i \neq \mathbf{v}_j}} D_H(\mathbf{v}_i, \mathbf{v}_j) \\ &= \min_{\mathbf{v}_i \neq \mathbf{v}_j} D_H(\mathbf{v}_i - \mathbf{v}_j, \mathbf{0}) \\ &= \min_{\mathbf{v}_i \neq \mathbf{v}_j} \overline{W}_H(\mathbf{v}_i - \mathbf{v}_j) \end{aligned}$$

ここで、 $\mathbf{v}_i - \mathbf{v}_j = \mathbf{w} \in C$ であり、 $\mathbf{v}_j$ を固定したとき

$$\{\mathbf{w} = \mathbf{v}_i - \mathbf{v}_j \mid \forall \mathbf{v}_i \in C, \mathbf{v}_i \neq \mathbf{v}_j\} = \{\mathbf{w} \in C \mid \mathbf{w} \neq \mathbf{0}\}$$

が成り立つので、

$$d = \min_{\substack{\mathbf{w} \in C \\ \mathbf{w} \neq \mathbf{0}}} \overline{W}_H(\mathbf{w})$$

が得られる。

例 生成行列

$$G = \begin{bmatrix} 1110 \\ 0111 \end{bmatrix}$$

によって定まる $GF(2)$ 上の線形符号 C を考える。このとき、 C の符号語は

$$C = \{(0000), (1110), (0111), (1001)\}$$

なので、最小距離は2となる。