

代数系と符号理論 (O) 第8回板書プリント

制作：植松友彦

2014.6.4

第7回の復習

- 体の定義
- 有限体 $\mathbb{F}_p$
- 多項式環 $F[x]$
- 既約多項式
- 多項式環を基礎とした有限体 $\mathbb{F}_{p^m}$
- 元の位数と原始元

1 有限体の構造

[定義 9.1] 体 F の部分集合 S が体 F と同一演算の下で体をなすとき、 S を F の部分体という。逆に、 F を S の拡大体という。

[定理 9.1]

$$x^m - 1 \text{ が } x^n - 1 \text{ を割り切る} \Leftrightarrow m \text{ が } n \text{ を割り切る}$$

$$2^m - 1 \text{ が } 2^n - 1 \text{ を割り切る} \Leftrightarrow m \text{ が } n \text{ を割り切る}$$

[定理 9.2]

$$\mathbb{F}_{2^m} \text{ が } \mathbb{F}_{2^n} \text{ の部分体} \Leftrightarrow m \text{ が } n \text{ を割り切る}$$

[定義 9.2] (標数) 体 F において乗法単位元 1 について

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ 個の和}} = 0$$

となる非零の最小の自然数 n を体 F の標数という。尚、このような有限の n がないとき、体の標数を 0 と定義する。

[定理 9.3] 全ての有限体 F の標数は素数である。

[定義 9.3] (最小多項式) $\beta \in \mathbb{F}_{p^m}$ に対して、 $m(\beta) = 0$ となる $\mathbb{F}_p$ 上の最小次数のモノック多項式 $m(x) \in \mathbb{F}_p[x]$ を β の $\mathbb{F}_p$ 上の「最小多項式 (minimum polynomial)」という。

[例 1] 例 9.2 の $\mathbb{F}_4$ において、元 0 の最小多項式は x であり、元 1 の最小多項式は $x+1$ である。一方、元 x の最小多項式については、この表記のままでは考えにくいので (x が有限体の元なのか、それとも多項式の変数を表すのかについて混同が生じる)、有限体の多項式表現のところで述べる。

[定理 9.4] 最小多項式は次の性質を有する。

1. 任意の $\beta \in \mathbb{F}_{p^m}$ に対して、 β の $\mathbb{F}_p$ 上の最小多項式は常に存在する。また、最小多項式は既約である。
2. 最小多項式は唯一つである。
3. $\beta \in \mathbb{F}_{p^m}$ が多項式 $f(x) \in \mathbb{F}_p[x]$ の根であるとき、すなわち $f(\beta) = 0$ であるとき、 β の $\mathbb{F}_p$ 上の最小多項式 $m(x)$ は $f(x)$ を割り切る。
4. $x^{p^m} - x$ は $\mathbb{F}_{p^m}$ の元の相異なる最小多項式の積である。

[定理 14.2] (最小多項式の性質) p を素数とすると、 $\mathbb{F}_p$ 上のある多項式 $m(x)$ が β を根として持てば、 β^p もまた $m(x)$ の根である。

(証明) 簡単のため、 $p = 2$ の場合について証明するが、 $p \neq 2$ の場合も同様に行える。まず、 $f_1(x), f_2(x) \in \mathbb{F}_2[x]$ とするとき、

$$(f_1(x) + f_2(x))^2 = (f_1(x))^2 + (f_2(x))^2 \quad (1)$$

が成り立つことに注意する。 $m(x)$ の次数が n であり、

$$m(x) = \sum_{i=0}^n m_i x^i$$

と書けるとすれば、式 (1) を繰り返し用いることで、

$$\begin{aligned} (m(x))^2 &= \left(m_n x^n + \sum_{i=0}^{n-1} m_i x^i \right)^2 \\ &= m_n^2 x^{2n} + \left(\sum_{i=0}^{n-1} m_i x^i \right)^2 \\ &= m_n^2 x^{2n} + \left(m_{n-1} x^{n-1} + \sum_{i=0}^{n-2} m_i x^i \right)^2 \\ &= m_n^2 x^{2n} + m_{n-1}^2 x^{2(n-1)} + \left(\sum_{i=0}^{n-2} m_i x^i \right)^2 \\ &= m_n^2 x^{2n} + m_{n-1}^2 x^{2(n-1)} + \dots + m_0^2 \\ &= \sum_{i=0}^n m_i^2 x^{2i} \\ &= \sum_{i=0}^n m_i x^{2i} \\ &= m(x^2) \end{aligned}$$

が得られる。但し、最後から2番目の等式は $m_i \in \mathbb{F}_2$ から $m_i^2 = m_i$ が成り立つことを用いた。従って、 $m(\beta) = 0$ ならば、 $m(\beta^2) = (m(\beta))^2 = 0$ である。 Q.E.D.

[定理 14.3](最小多項式の求め方) $\beta \in \mathbb{F}_{p^m}$ の $\mathbb{F}_p$ 上の最小多項式 $m(x)$ は

$$m(x) = (x - \beta)(x - \beta^p)(x - \beta^{p^2}) \cdots (x - \beta^{p^{l-1}})$$

で与えられる。但し、 l は $\beta^{p^l} = \beta$ をみたす最小の正の整数である。特に、 $\beta \in \mathbb{F}_{p^m}$ から $\beta^{p^m} = \beta$ が成り立つので $l \leq m$ である。

[例 2] 既約多項式 $p(x) = x^3 + x + 1$ によって定まる有限体 $\mathbb{F}_{2^3}$ において、元 x の $\mathbb{F}_2$ 上の最小多項式を求めてみよう。定理 14.3 に従って、 $x^{2^m} = x$ となる最小の m を求めると

$$x^2 = x^2, x^{2^2} = x^4 = x^2 + x, x^{2^3} = (x^2 + x)^2 = x$$

から $m = 3$ である。最小多項式の変数を y によって表せば、 x の最小多項式

$$\begin{aligned} (y - x)(y - x^2)(y - x^2) &= (y^2 + (x^2 + x)y + x^3)(y + x^4) \\ &= (y^2 + (x^2 + x)y + x + 1)(y + x^2 + x) \\ &= y^3 + (x^2 + x + x^2 + x)y^2 + ((x^2 + x)^2 + x + 1)y + (x + 1)(x^2 + x) \\ &= y^3 + y + 1 \end{aligned}$$

が得られる。

[定義 9.5] (原始多項式) $\mathbb{F}_{p^m}$ の原始元 α の $\mathbb{F}_p$ 上の最小多項式を「原始多項式 (primitive polynomial)」と呼ぶ。

[定理 9.5] $\mathbb{F}_p$ の拡大体 $\mathbb{F}_{q'}$ を考え、 $\mathbb{F}_{q'}$ の原始元 α の $\mathbb{F}_p$ 上の最小多項式 (原始多項式) を $m(x)$ とする。 $m(x)$ の次数が ℓ ならば、 $\mathbb{F}_{q'}$ の位数 q' は

$$q' = p^\ell$$

を満たす。また、 $\mathbb{F}_{q'}$ の任意の元 β は、

$$\beta = a_{\ell-1}\alpha^{\ell-1} + a_{\ell-2}\alpha^{\ell-2} + \cdots + a_0 \quad (2)$$

によって表される。但し、 a_i ($i = 0, 1, \dots, \ell$) は $\mathbb{F}_p$ の元である。

[系 9.1] 全ての有限体 $\mathbb{F}_q$ の要素数 q は素数のべき乗である。すなわち、 p を素数、 m を自然数として、 $q = p^m$ と書ける。

2 有限体の構造のまとめ

$x^{63} - 1$ の $\mathbb{F}_2$ 上での因数分解を例に取って有限体の性質について整理を行なう。有限体 $\mathbb{F}_{64}$ の非零の元は、任意の原始元のべき乗で表現される。従って、これらの元は、 $0, 1, \alpha, \alpha^2, \dots, \alpha^{62}$ と書ける。従って、

$$x^{63} - 1 = (x - 1)(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{62})$$

である。ここで、単純な計算により、

$$(\alpha^{21})^3 = \alpha^{63} = 1$$

であるので、 α^{21} の位数は 3 である。同様に、 α^{42} の位数も 3 である ($42 = 21 \times 2$ に注意)。他方、 $(\alpha^9)^7 = \alpha^{63} = 1$ であり、 α^9 の位数は 7 である。同様に、 $\alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}$ の位数は 7 である ($18 = 9 \times 2, 27 = 9 \times 3, \dots, 54 = 9 \times 6$ に注意)。最後に、 $(\alpha^{21})^3 = 1$ に注意すれば、 $\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{35}, \alpha^{49}, \alpha^{56}$ の位数は 9 である ($14 = 7 \times 2, 21 = 7 \times 3, \dots, 56 = 7 \times 8$ だが、 α^{21} と α^{42} の位数は 3)。残りの 36 個の元の位数は全て 63 である。

さて、 $\beta_1, \beta_2, \dots, \beta_r$ を位数 i の元全体とすると、円分多項式 $\psi_i(x)$ を

$$\psi_i(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r)$$

によって定義する。このとき、

$$x^{63} - 1 = \psi_1(x)\psi_3(x)\psi_7(x)\psi_9(x)\psi_{21}(x)\psi_{63}(x)$$

と因数分解される。多項式 $x^{21} - 1$ は $x^{63} - 1$ を割り切り、 $\beta^{21} = 1$ を満足する全ての元 β を根としてもつから、 $x^{21} - 1$ は、21 を割り切る $i (= 1, 3, 7, 21)$ について $\psi_i(x)$ で割り切れる。従って、

$$x^{21} - 1 = \psi_{21}(x)\psi_7(x)\psi_3(x)\psi_1(x)$$

が成り立つ。同様に、

$$\begin{aligned} x^9 - 1 &= \psi_9(x)\psi_3(x)\psi_1(x) \\ x^7 - 1 &= \psi_7(x)\psi_1(x) \\ x^3 - 1 &= \psi_3(x)\psi_1(x) \\ x - 1 &= \psi_1(x) \end{aligned}$$

が成り立つ。従って、この式から、

$$\begin{aligned} \psi_1(x) &= x - 1 \quad (1 \text{ 次}) \\ \psi_3(x) &= \frac{x^3 - 1}{\psi_1(x)} = x^2 + x + 1 \quad (2 \text{ 次}) \\ \psi_7(x) &= \frac{x^7 - 1}{\psi_1(x)} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \quad (6 \text{ 次}) \\ \psi_9(x) &= \frac{x^9 - 1}{\psi_1(x)\psi_3(x)} \quad (6 \text{ 次}) \\ \psi_{21}(x) &= \frac{x^{21} - 1}{\psi_1(x)\psi_3(x)\psi_7(x)} \quad (12 \text{ 次}) \\ \psi_{63}(x) &= \frac{x^{63} - 1}{\psi_1(x)\psi_3(x)\psi_7(x)\psi_9(x)\psi_{21}(x)} \quad (36 \text{ 次}) \end{aligned}$$

が得られる。 $\psi_i(x)$ の次数は、位数 i の元の個数に等しく、これは既に計算済みである。他方、もし元の位数を知らなくても、上の方法によって、円分多項式の次数を求めることができる。まず、 $\psi_1(x)$ の次数は明らかに 1 であり、 $\psi_3(x)$ の次数は $x^3 - 1$ の次数から $\psi_1(x)$ の次数を引いたものである。以下、順に円分多項式 $\psi_i(x)$ の次数を定めることができる。

円分多項式を既約多項式に分解することを考えよう。位数 3 の元の $\mathbb{F}_2$ 上の最小多項式の次数は 2 である。なぜならば、これらの元は $x^3 - 1 = x^{2^2-1} - 1 = 0$ の根であり、このことは $\mathbb{F}_{2^2}$ の元であることを意味するからである。従って、 $\psi_3(x)$ は $\mathbb{F}_2$ 上で既約である。事実、 $x^3 - 1$ の根は $1, \alpha^{21}, \alpha^{42}$ である。同様に、位数 7 の元は $\mathbb{F}_{2^3}$ に属し、最小多項式の次数は 3 である。従って、

$\psi_7(x)$ は 3 次の既約多項式 2 個に分解される。他の $\mathbb{F}_{2^6}$ の元は、部分体の要素ではない。従って、これらの最小多項式の次数は全て 6 である。従って、 $\psi_9(x)$ は既約多項式であり (根の位数が 9 なので、原始既約多項式ではないことに注意)、 $\psi_{21}(x)$ は 6 次の既約多項式 2 個に、 $\psi_{63}(x)$ は 6 次の既約多項式 6 個に、それぞれ因数分解される。尚、 $\psi_{63}(x)$ の因数となる最小多項式は全て原始既約多項式である。

更に、これらの既約多項式を因数分解せずに計算することもできる。もし、 β を 6 次の既約多項式 $p(x)$ の元とすると、この多項式の他の根は、 $\beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32}$ である。そこで、 $m_i(x)$ によって α^i の最小多項式を表すと、

$$m_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32})$$

および、

$$m_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48})(x - \alpha^{33})$$

などが得られる。ここで、 $\alpha^{63} = 1$ から $(\alpha^{48})^2 = \alpha^{96} = \alpha^{33}$ であることに注意する。また、 $(\alpha^{32})^2 = \alpha^{64} = \alpha$ であり、 $m_1(x)$ の相異なる根は全て、 α^1 に対して 2 乗演算を繰り返すことで得られる。同様に、 $(\alpha^{33})^2 = \alpha^{66} = \alpha^3$ が成り立つので、 $m_3(x)$ の全ての根もまた、 α^3 に対して 2 乗演算を繰り返すことで得られる。他方、

$$(\alpha^9)^2 = \alpha^{18}, (\alpha^{18})^2 = \alpha^{36}, (\alpha^{36})^2 = \alpha^{72} = \alpha^9$$

であるので、 $m_9(x)$ の相異なる根は 3 個であり、このことは $m_9(x)$ が次数 3 の多項式であることに一致している。以上の結果をまとめて、次の表を得る。尚、表では便宜上 α は原始多項式 $x^6 + x + 1$ の根として展開を行って $\mathbb{F}_2$ 上の多項式を得ている (α が他の原始多項式の根ならば展開して得られる多項式が異なることに注意)。

$x^{63} - 1$ の因数分解

$$x^{63} - 1 = \psi_1(x)\psi_3(x), \psi_7(x), \psi_9(x)\psi_{21}(x)\psi_{63}(x)$$

$$\psi_1(x) = x - 1$$

$$\psi_3(x) = m_{21}(x)$$

$$m_{21}(x) = (x - \alpha^{21})(x - \alpha^{42}) = x^2 + x + 1$$

$$\psi_7(x) = m_9(x)m_{27}(x)$$

$$m_9(x) = (x - \alpha^9)(x - \alpha^{18})(x - \alpha^{36}) = x^3 + x^2 + 1$$

$$m_{27}(x) = (x - \alpha^{27})(x - \alpha^{54})(x - \alpha^{45}) = x^3 + x + 1$$

$$\psi_9(x) = m_7(x)$$

$$m_7(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{28})(x - \alpha^{56})(x - \alpha^{49})(x - \alpha^{35}) = x^6 + x^3 + 1$$

$$\psi_{21}(x) = m_3(x)m_{15}(x)$$

$$m_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{48})(x - \alpha^{33}) = x^6 + x^4 + x^2 + x + 1$$

$$m_{15}(x) = (x - \alpha^{15})(x - \alpha^{30})(x - \alpha^{60})(x - \alpha^{57})(x - \alpha^{51})(x - \alpha^{39}) = x^6 + x^5 + x^4 + x^2 + 1$$

$$\psi_{63}(x) = m_1(x)m_5(x)m_{11}(x)m_{13}(x)m_{23}(x)m_{31}(x)$$

$$m_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})(x - \alpha^{32}) = x^6 + x + 1$$

$$m_5(x) = (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^{40})(x - \alpha^{17})(x - \alpha^{34}) = x^6 + x^5 + x^2 + x + 1$$

$$m_{11}(x) = (x - \alpha^{11})(x - \alpha^{22})(x - \alpha^{44})(x - \alpha^{25})(x - \alpha^{50})(x - \alpha^{37}) = x^6 + x^5 + x^3 + x^2 + 1$$

$$m_{13}(x) = (x - \alpha^{13})(x - \alpha^{26})(x - \alpha^{52})(x - \alpha^{41})(x - \alpha^{19})(x - \alpha^{38}) = x^6 + x^4 + x^3 + x + 1$$

$$m_{23}(x) = (x - \alpha^{23})(x - \alpha^{46})(x - \alpha^{29})(x - \alpha^{58})(x - \alpha^{53})(x - \alpha^{43}) = x^6 + x^5 + x^4 + x + 1$$

$$m_{31}(x) = (x - \alpha^{31})(x - \alpha^{62})(x - \alpha^{61})(x - \alpha^{59})(x - \alpha^{55})(x - \alpha^{47}) = x^6 + x^5 + 1$$

中間テスト

6月25日(水)の授業時間中に中間テストを行う。範囲は、教科書116ページまでと板書プリント8回までとする。教科書・ノート・プリント参照不可。