

代数系と符号理論 第8回板書プリント

植松友彦 2007.5.22

1 有限体の続き

1.1 有限体の別の考え方

いままでは、 F_{2^m} を構成するとき、 F_2 上の多項式環 $F_2[x]$ に対して、 m 次の既約多項式 $p(x)$ による法演算を導入することで有限体を構成してきた。

ここでは、有限体の構成法の別の見方について述べる。有理数体 Q に $x^2 - 2$ の根 $\sqrt{2}$ を付け加えた集合 $Q(\sqrt{2})$ を考えよう。集合 $Q(\sqrt{2})$ の全ての元は $a + b\sqrt{2}$ と書ける。但し、 a, b は有理数である。集合 $Q(\sqrt{2})$ が和と差について閉じているのは自明であるし、積については

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in Q(\sqrt{2})$$

であり、また非零の元 $a + b\sqrt{2}$ の逆元は

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in Q(\sqrt{2})$$

である。従って、集合 $Q(\sqrt{2})$ は体となる。

有理数にある多項式の根を付け加えるという方法と同様にして、有限体が構成できることについて述べよう。いま、 F_2 上の $m(=3)$ 次の既約多項式 $p(x) = x^3 + x + 1$ の根 α を F_2 に付け加えてできる集合 F を考えよう。この集合 F の要素は、全て

$$F = \{a_2\alpha^2 + a_1\alpha + a_0 : a_i \in F_2, i = 0, 1, 2\}$$

と書ける。ここで、 α の3次以上の項がないのは、 α が

$$\alpha^3 + \alpha + 1 = 0$$

をみたし、 α^3 は α と1の線形結合で書けるからである ($\alpha^2, \alpha, 1$ は一次独立であり、 $\alpha^3, \alpha^4, \dots$ はこれらの線形結合で書ける)。

次に、集合 F での演算を考えよう。加法については、

$$(a_2\alpha^2 + a_1\alpha + a_0) + (b_2\alpha^2 + b_1\alpha + b_0) = (a_2 + b_2)\alpha^2 + (a_1 + b_1)\alpha + (a_0 + b_0)$$

から閉じていることはすぐ分かるし、加法の逆元は自分自身である。他方、乘法については、再び $\alpha^3 + \alpha + 1 = 0$ に注意すれば、たとえば、

$$(\alpha^2 + \alpha)(\alpha + 1) = \alpha^3 + \alpha = (\alpha + 1) + \alpha = 1$$

が得られ、積が F の元であることは容易に分かる。元 a の逆元については、 α を未知数をみなして、多項式に関するユークリッドの互除法を適用することで求めることが出来る。例えば、 α^2 の逆元は、 α^2 と $p(\alpha) = \alpha^3 + \alpha + 1$ の間で互除法を行うことで、関係式

$$\alpha^2(1 + \alpha + \alpha^2) + (\alpha + 1)(\alpha^3 + \alpha + 1) = 1$$

が得られる。ここで、 $p(\alpha) = 0$ を用いると、左辺の 2 項目が零になり

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

が得られ、この式は、 α^2 の逆元が $(1 + \alpha + \alpha^2)$ であることを意味する。従って、集合 F は体となる。

尚、このようにして得られた体は、前回説明した体の構成法、すなわち多項式環 $F_2[x]$ に既約多項式 $p(x)$ による法演算によって加法と乗法を定めた有限体において、 x を形式的に α に書き直したものと一致していることに注意しておく。

1.2 拡大体と部分体

p を素数、 m, n を正の整数とすると、有限体 F_{p^m} と F_{p^n} について、 $m|n$ ならば F_{p^n} を F_{p^m} の拡大体と呼ぶ。また、 $m|n$ ならば F_{p^m} は F_{p^n} の部分体である。

[例 1] F_{2^2} は F_2 の拡大体である。他方、 F_2 は F_{2^2} の部分体である。 F_{2^5} は F_2 の拡大体であるが、 F_2 と自分自身以外の部分体を持たない。 F_{2^6} の部分体は、 $F_2, F_{2^2}, F_{2^3}, F_{2^6}$ の 4 個である。 F_{2^2} の拡大体は、 $F_{2^4}, F_{2^6}, F_{2^8}$ などがある。

[定義 1] (原始既約多項式) 既約多項式の根 α が原始元であるとき、その既約多項式を原始既約多項式という。

[例 2] $x^4 + x^3 + x^2 + x + 1$ は既約多項式だが、原始既約多項式ではない。なぜなら、この多項式の根を α とすると、

$$\alpha^5 = (\alpha + 1) \underbrace{(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)}_{=0} + 1 = 1$$

であり、根 α の位数は 5 である。

2 有限体の構造—まとめ

$x^{63} - 1$ の 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 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。同様にして、 $\alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}$ 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 $\beta^{21} = 1$ 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。同様にして、

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

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 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 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 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 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 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、

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

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。

$x^{63} - 1$ の因数分解

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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