代数系と符号理論　第7回板書プリント

植松友彦 2007.5.16

1　有限体の続き

1.1　元の位数の性質

[定義 **2.1.2**] 有限体 F において、$a \in F \setminus \{0\}$ は非零の元であるとする。このとき、a の位数 $\mathrm{ord}(a)$ とは、$a^s = 1$ となる最小正整数 s である。

[例 **1**] 有限体 $F_5 = \{0, 1, 2, 3, 4\}$ において、元 1 の位数は 1 であり、元 2 の位数は、

$$2^2 = 4,\ 2^3 \bmod 5 = 3,\ 2^4 \bmod 5 = 1$$

から 4 である。また同様な計算によって、$\mathrm{ord}(3) = \mathrm{ord}(4) = 4$ であることが分かる。

[例 **2**] 有限体 $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$ において、非零の各元の位数を求めると、

$$\mathrm{ord}(1) = 1,\ \mathrm{ord}(2) = 3,\ \mathrm{ord}(3) = 6,\ \mathrm{ord}(4) = 3,\ \mathrm{ord}(5) = 6,\ \mathrm{ord}(6) = 2$$

である。

[補題 **2.1.1**] F を有限体とし、$a, b \in F \setminus \{0\}$ とする。このとき、以下が成り立つ。

1. $\mathrm{ord}(a) = s \Rightarrow a, a^2, \cdots, a^s$ は全て相異なる。
2. $a^j = 1 \Leftrightarrow \mathrm{ord}(a) | j$　($\mathrm{ord}(a)$ は j を割り切る。)
3. $\mathrm{ord}(a^j) = \frac{\mathrm{ord}(a)}{(\mathrm{ord}(a), j)}$
4. $\mathrm{ord}(a) = s, \mathrm{ord}(b) = j, (s, j) = 1 \Rightarrow \mathrm{ord}(ab) = sj$

(証明)　a の位数を s とする。

1. 位数の定義から自明。
2. s が j を割り切るならば、$j = sh$ となる整数 h が存在し、$a^{sh} = (a^s)^h = 1^h = 1$ が成り立つ。逆に $a^j = 1$ を仮定すると、$j = sh + r$ となるような h と $0 \leq r < s$ が存在する。このとき、

   $$1 = a^j = a^{sh+r} = (a^s)^h a^r = a^r$$

   となる。このとき $r > 0$ ならば、a の位数は $r(< s)$ 以下となり、位数 s の定義に矛盾するので、$r = 0$ でなければならず、$s | j$ である。

3. $\mathrm{ord}(a) = s$ かつ $\mathrm{ord}(a^j) = l$ とおき、$(s, j) = m$ とする。

$$1 = (a^j)^l = a^{jl}$$

と 2. から s が jl を割り切る。このことは、s/m が jl/m を割り切ることを意味し、s/m と j が互いに素なので、s/m が l を割り切る ことが分る。また逆に、

$$(a^j)^{s/m} = (a^s)^{j/m} = 1$$

であり、再び、2. から l が s/m を割り切る。従って、$l = s/m$ が得られる。

4. $\mathrm{ord}(a) = s, \mathrm{ord}(b) = j$ に注意すると、$(ab)^{sj} = (a^s)^j (b^j)^s = 1 \cdot 1 = 1$ である。従って、2. により $\mathrm{ord}(ab)$ は sj を割り切るが、$(s, j) = 1$ であるから、このことは、s を割り切るある整数 l_1 および j を割り切るある整数 l_2 が存在して、

$$\mathrm{ord}(ab) = l_1 \cdot l_2$$

すなわち、$(ab)^{l_1 l_2} = 1$ を意味する。従って、

$$1 = [(ab)^{l_1 l_2}]^{s/l_1} = (a^s)^{l_2} b^{s l_2} = b^{s l_2}$$

である。再び 2. より、j が $l_2 s$ を割り切り、$(j, s) = 1$ であることから j は l_2 を割り切る ので、$j = l_2$ が分る。同様にして、$s = l_1$ が得られるので、

$$\mathrm{ord}(ab) = sj$$

である。 Q.E.D.

1.2 位数と原始元

[定理 **2.1.2**] **(原始元の存在)** F を要素数 q の有限体であるとする。このとき、F は位数 $q-1$ の元 α を持つ。このような元 α を「**原始元 (primitive element)**」という。

原始元 α を用いると、F の非零の元は、

$$\alpha, \alpha^2, \cdots, \alpha^{q-2}, \alpha^{q-1} = 1$$

によって表される。このような有限体の元の表現を「べき表現」という。べき表現を用いれば、乗算は、

$$\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod (q-1)}$$

によって簡単に計算できる。

[注意] この定理は原始元の存在を保証しているが、原始元は通常試行錯誤で求めるしかない。

(証明) α を最大位数の元で $\mathrm{ord}(\alpha) = r$ とすると、補題 2.1.1 の 1. から

$$|F \setminus \{0\}| = q - 1 \Longrightarrow r \leq q - 1 \quad (\text{位数は } q-1 \text{ 以下 !}) \tag{1}$$

である。

次に、$\forall\beta \in F \setminus \{0\}$ の位数 $\mathrm{ord}(\beta) = s$ が $s|r$ を満たすことを示す。もし s が r を割り切らないならば、ある素数 p と自然数 i, j が存在して、

$$r = p^i a,\ s = p^j b,\ i < j,\ (a, p) = (b, p) = 1$$

と書ける。例えば、$r = 15 = 3 \cdot 5,\ s = 6 = 2 \cdot 3$ ならば、

$$r = 2^0 \cdot 15,\ s = 2^1 \cdot 3$$

から、$p = 2, j = 1, i = 0$ と選ぶことができる。$r = p^i a$、$s = p^j b$ と補題 2.1.1 の 3. から、

$$\begin{aligned} \mathrm{ord}(\alpha^{p^i}) &= \frac{r}{(r, p^i)} = \frac{p^i a}{p^i} = a \\ \mathrm{ord}(\beta^b) &= \frac{s}{(s, b)} = \frac{p^j b}{b} = p^j \end{aligned}$$

が得られる。一方、$(a, p^j) = 1$ であるから、補題 2.1.1 の 4 と $j > i$ から

$$\mathrm{ord}(\alpha^{p^i} \cdot \beta^b) = a \cdot p^j > a \cdot p^i = r$$

となり、r が最大の位数であることに矛盾する。従って、$s|r$ である。

このことと $\beta^r = (\beta^s)^{(r/s)} = 1$ から、$F \setminus \{0\}$ の $q - 1$ 個の全ての元が多項式 $x^r - 1$ の根であることが分かる。しかも、定理 2.2.2(後述) から次数 r の多項式は高々r 個の根しか持たないこととから、$r \geq q - 1$ が得られ、式 (1) と組み合わせることで $r = q - 1$ を得る。 Q.E.D.

[系 **2.1.1**] 要素数 q をもつ有限体の任意の非零元の位数は $q - 1$ を割り切る。

[系 **2.1.2**] 要素数 q をもつ有限体の任意の元 γ は、等式 $\gamma^q - \gamma = 0$ を満たす。

(証明)　F_q の非零の元は、$x^{q-1} - 1 = 0$ の根である。従って、全ての元は、$x(x^{q-1} - 1) = 0$ の根である。 Q.E.D.

[例 **2.1.3**] 3 は F_{17} の原始元である。なぜなら、F_{17} の非零の元の可能な位数は、$17 - 1 = 16$ の約数 $1, 2, 4, 8, 16$ のいずれかであり、

$$3^2 = 9,\ 3^4 = 13,\ 3^8 = 16$$

なので、3 の位数は 16 でなければならない。

1.3　有限体 F_{p^m}

F を体とする。$F[x]$ によって、体 F の元を係数としてもつ多項式 (体 F 上の多項式)

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \quad a_i \in F$$

の集合（多項式環）を表す。多項式の次数 (deg)、加算、乗算は既知であるとする。

[定理 **2.2.1**] $a(x), b(x) \in F[x]\ \ b(x) \neq 0$ とする。このとき、次の等式を満たし、かつ次数が $\deg(r(x)) < \deg(b(x))$ となる多項式の組 $q(x), r(x)$ が一意的に存在する。

$$a(x) = q(x)b(x) + r(x)$$

証明は、実数等に対する通常の剰余定理の証明を、係数が有限体であることに注意して適用すれば良い。

[定理 **2.2.2**] 次数 n の多項式は、F 上で高々n 個の（相異なる）根を持つ。

(証明) $a \in F$ を多項式 $f(x) \in F[x]$ の根とする。このとき、定理 2.2.1 から

$$f(x) = q(x)(x-a) + r(x)$$

となる多項式 $q(x), r(x)$ が唯一組存在する。$r(x)$ は定数であり、かつ $f(a) = 0$ であるので、

$$0 = f(a) = r(x)$$

が成り立つ。従って、

$$f(x) = q(x)(x-a), \quad \deg(q(x)) = n-1$$

となる。以下、$q(x)$ について同様の議論を行えば良い。 Q.E.D.

多項式 $f(x) \in F[x]$ が因数分解できない、すなわち $f(x) = a(x)b(x)$ が成り立つのは $\deg(a(x)) = 0$ または $\deg(b(x)) = 0$ に限るとき、$f(x)$ は既約であるといわれる。

既約多項式は、$F[x]$ において、整数中の素数がなすのと同じ働きをする。従って、任意の多項式が既約多項式の積として、（一意に）表されることを示すことができる。証明は、整数の場合と同様に行える。

任意の正整数 m に対し、有限体 F_2 の元を係数とする次数 m の既約多項式が存在することを証明することができる。興味のある者は、代数学や符号理論の教科書を参照されたい。

[例 **2.2.1**] （F_2 上の 5 次以下の既約多項式）

次数	既約多項式	既約である理由
1	$x,\ x+1$	
2	x^2+x+1	x でも $x+1$ でも割れない (定数項があり、項の数が奇数個)
3	$x^3+x+1,\ x^3+x^2+1$	同上
4	$x^4+x+1,\ x^4+x^3+1$ $x^4+x^3+x^2+x+1$	$x, x+1, x^2+x+1$ で割れない (x^4+x^2+1 は x^2+x+1 で割れる)
5	$x^5+x^2+1,\ x^5+x^4+x^3+x^2+1$ $x^5+x^4+x^2+x+1,\ x^5+x^3+x^2+x+1$ $x^5+x^4+x^3+x+1, x^5+x^3+1$	同上

既約多項式を用いると、$q = 2^m$ 個の元を持つ有限体を次のようにして構成できる。この体を F_q あるいは F_{2^m} と書く。更に、この体 F_q が既約多項式 $f(x)$ の選び方によらず、全て同型であることも証明できる。

【体 F_{2^m} の構成法】

- 既約多項式：F_2 上の m 次既約多項式 $f(x)$ を一つ定める。
- 元：F_2 上の m 次元ベクトル $a = (a_{m-1}, \cdots, a_0)$ または $m-1$ 次以下の多項式

$$a(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0 \in F_2[x]$$

として表現される 2^m 個のベクトルまたは多項式。以下では、２つの元の表示の間には、

$$a = (a_{m-1}, \cdots, a_0) \Longleftrightarrow a(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0$$

という一対一対応があるとする。

- 加法：ベクトルの和（多項式の和）
- 加法の単位元：$0 = (0, 0, \cdots, 0)$
- 加法の逆元：$a + a = 0$ から、逆元は自分自身。
- 乗法：既約多項式 $f(x)$ を用い、

  $$a(x)b(x) \bmod f(x)$$

  によって定める。
- 乗法の単位元：1
- 乗法の逆元：多項式に対するユークリッドの互除法から、任意の $a(x) \in F_2[x]$ について、

  $$a(x)p(x) + f(x)q(x) = (a(x), f(x)) = 1$$

  を満たす多項式 $p(x), q(x) \in F_2[x]$ が存在する。但し、$(a(x), f(x))$ は、$a(x)$ と $f(x)$ の最大公約多項式を表す。両辺の $f(x)$ に関する剰余を取ることで、

  $$a(x)(p(x) \bmod f(x)) = 1 \bmod f(x)$$

  が得られ、$(p(x) \bmod f(x))$ は $a(x)$ の逆元である。
- 分配法則の成立は明らか。

[例 **2.2.2**] 有限体の例
既約多項式 $f(x) = x^2 + x + 1$ によって定まる有限体 $F_4 = \{0, 1, x, x+1\}$ （教科書 p.27 の表の ab を $bx + a$ と書き直したものと同一）

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

原始元は、x と $x+1$ である。なぜなら、

$$x^2 = x + 1,\ x^3 = x^2 \cdot x = (x+1) \cdot x = 1$$
$$(x+1)^2 = x,\ (x+1)^3 = (x+1)^2 \cdot (x+1) = x \cdot (x+1) = 1$$

が成り立つからである。

1.4 有限体での加算と乗算

- 元を多項式表示すれば、加算は容易に行える。
- 有限体 F_q の原始元 α が与えられたとき、べき表示を用いれば乗算は容易に行える。

$$\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod (q-1)} \quad (\alpha^{q-1} = 1 \text{ を思い出すこと！!})$$

従って、F_{2^m} 上の計算をするためには、多項式表示とべき表示の間の対応表を用意すると良い。

[例 **3**] 有限体 F_8 を構成しよう。$8 = 2^3$ なので、F_2 上の 3 次の既約多項式として、$x^3 + x + 1$ を選ぶ。このとき、系 2.1.1 と $q - 1 = 8 - 1 = 7$ から、1 以外の元の位数は全て 7 となる。従って、$\alpha = x$ や $\beta = x + 1$ は原始元である。事実、べき乗を計算すると、

べき表示	多項式表示	α による表示	べき表示	多項式表示
α	x	α	β	$x+1$
α^2	x^2	α^2	β^2	$(x+1)^2 = x^2+1$
α^3	$x^3 = x+1$	$\alpha+1$	β^3	$(x^2+1)(x+1) = x^2$
α^4	$(x+1)x = x^2+x$	$\alpha^2+\alpha$	β^4	$x^2(x+1) = x^2+x+1$
α^5	$(x^2+x)x = x^2+x+1$	$\alpha^2+\alpha+1$	β^5	$(x^2+x+1)(x+1) = x$
α^6	$(x^2+x+1)x = x^2+1$	α^2+1	β^6	$x(x+1) = x^2+x$
α^7	$(x^2+1)x = 1$	1	β^7	$(x^2+x)(x+1) = 1$

が得られ、両者は異なる対応ではあるが、いずれも非零の元のべき乗表現を与えることが分かる。この表によれば、べき表示の加算や多項式表示の乗算も

$$\alpha^3 + \alpha^2 = \underbrace{(x^2) + (x+1) = x^2 + x + 1}_{\text{多項式表示で計算}} = \alpha^5$$

$$(x^2+1)(x^2+x+1) = \underbrace{\alpha^6\alpha^5 = \alpha^{11}}_{\text{べき表示で計算}} = \alpha^4 = x^2 + x$$

のようにして容易に行える。β を用いたとしても

$$(x^2+1)(x^2+x+1) = \beta^2\beta^4 = \beta^6 = x^2 + x$$

が得られ、当然ながら同一の演算結果が得られる。

尚、多項式表示において、$\alpha = x$ が原始元の場合、多項式を既約多項式 $f(x)$ の根 α の多項式として表すことが多い。すなわち、この表示では多項式表示における x の代わりに α を用いる。(左側の表の「α による表示」)。この場合、α は $f(\alpha) = 0$ を満足するので、この式を利用すれば、α^4 に対応する多項式表示の計算は $f(\alpha) = 0$ を用いた簡約

$$\alpha^4 = \alpha f(\alpha) + (\alpha^2 + \alpha) = \alpha^2 + \alpha$$

と見なすこともできる。