7　第7回

p を素数とするとき、$GF(p)$ 上の $m-1$ 次以下の多項式の集合に対し、m 次の素多項式を法とする演算を導入することで $GF(p^m)$ は構成できる。
$GF(p^m)$ ： $GF(p)$ の m 次の拡大体
$GF(p)$ ： $GF(p^m)$ の基礎体

定理 17 任意の素数 p と任意の正整数 m について、$GF(p)$ 上の m 次素多項式が存在する。

(証明は省略)
この定理と前に述べた結果を用いると、次の系を得る。

系 3 元の数が素数 p のべき乗となる有限体 $GF(p^m)$ が存在する。

一般には、この逆、すなわち元の数が素数のべき乗以外の有限体が存在しないことも証明されている。従って $GF(6)$ や $GF(12)$ は存在しない。

7.1　有限体の表現

$GF(4)$ において x は単なる変数ではなく、有限体の元である。そこで、m 次の素多項式 $p(x)$ で生成される $GF(p^m)$ の元 x を変数と区別するために、α とおく。このとき、$R_{p(x)}[p(x)]=0$ から $p(\alpha)=0$ が成り立つので、α は素多項式 $p(x)$ の根とも考えることができる。

(例)　$GF(2)$ 上の素多項式 $p(x)=x^2+x+1$ の 1 つの根を α とすれば、$GF(4)=\{0,1,\alpha,\alpha+1\}$ と書ける。このとき、

$$\alpha(\alpha+1)=\alpha^2+\alpha=(\alpha^2+\alpha+1)+1=0+1=1$$

となり、これは $R_{p(\alpha)}[\alpha\cdot(\alpha+1)]=1$ と一致する。

$GF(p)$ 上の m 次素多項式 $p(x)$ の 1 つの根を α とすると、$GF(p^m)$ の元は α の $m-1$ 次以下の多項式

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{m-1}\alpha^{m-1}\quad(a_i\in GF(p))$$

によって表せる。このような元の表現を「多項式表現」と呼び、$\{1,\alpha,\cdots,\alpha^{m-1}\}$ を $GF(p^m)$ の多項式基底という。

$GF(p^m)$ の元 $a_0+a_1\alpha+\cdots+a_{m-1}\alpha^{m-1}$ をその係数を並べて得られる $GF(p)$ 上の m 次元ベクトル $(a_0, a_1, \cdots, a_{m-1})$ で表すことを「ベクトル表現」と呼ぶ。$GF(p^m)$ の元の加算は

$$\begin{aligned} & (a_0, a_1\alpha, +\cdots+a_{m-1}\alpha^{m-1}) + (b_0+b_1\alpha+\cdots+b_{m-1}\alpha^{m-1}) \\ = \ & (a_0+b_0)+(a_1+b_1)\alpha+\cdots+(a_{m-1}+b_{m-1})\alpha^{m-1} \end{aligned}$$

なので、これをベクトル表現で書けば

$$\begin{aligned} & (a_0, a_1, \cdots, a_{m-1}) + (b_0, b_1, \cdots, b_{m-1}) \\ = \ & (a_0+b_0, a_1+b_1, \cdots, a_{m-1}+b_{m-1}) \end{aligned}$$

となり、ベクトル表現において加算はベクトルの加算と一致する。

これから、$GF(p^m)$ は加法について、$GF(p)$ 上の m 次元ベクトル空間をなすことが分かる。

(例) $GF(4)=\{0, 1, \alpha, \alpha+1\}$ の基底 $\{1, \alpha\}$ によるベクトル表現は

多項式表現	ベクトル表現
0	$(0,0)$
1	$(1,0)$
α	$(0,1)$
$\alpha+1$	$(1,1)$
	$\uparrow\uparrow$
基底 :	$1\ \alpha$

7.2 べき表現

有元体の任意の元 a について

$$\begin{aligned} a^0 &= 1 \\ a^1 &= a \\ &\vdots \\ a^i &= a^j \end{aligned}$$

となる (i¿j) が存在する。このとき、両辺を a^j で割れば $a^{i-j}=1$ となる。従って、$a^i=1$ となる正整数が存在する。特に、$a^e=1$ となる最小の正整数 e を a の位数 (order) という。このとき、$1, a, \cdots, a^{e-1}$ は全て異なる。

補題 1 $GF(p^m)$ において、任意の元 $a\neq 0$ は

$$a^{p^m-1}=1$$

をみたす。逆に、$GF(p^m)$ の非零の元の全体は

$$f(x) = x^{p^m-1} - 1]$$

の根全体に等しい。

また、$a \in GF(p^m), a \neq 0$ とすれば、a の位数は $p^m - 1$ を割り切る。

(証明) $F = GF(p^m)$ から零元をのぞいたものを $F^\times$ とする。
このとき、

$$a \cdot F = \{ac | c \in F^\times\} = F^\times$$

が成り立つ。なぜならば、$a, b, c \in F^\times$ とし、$b \neq c$ ならば
$ab \neq ac$ が成り立つからである。従って

$$\underbrace{\prod_{c \in F^\times} c}_{\substack{\uparrow \\ F^\times \text{ の全ての元の積}}} = \prod_{c \in F^\times} a \cdot c = a^{\underbrace{p^m-1}_{\substack{\uparrow \\ F^\times \text{ の元の数}}}} \cdot \prod_{c \in F^\times} c$$

$$\therefore a^{p^m-1} = 1$$

一方、$\deg f(x) = p^{m-1}$ であるので、$f(x)$ の根の総数は高々$p^m - 1$ である。また、$|F^\times| = p^m - 1$ であるので、$F^\times$ の要素は $f(x) = 0$ の根全体と一致しなければならない。

a の位数を k_0 とし、

$$p^m - 1 = nk_0 + r, 0 \leq r < k_0$$

とする。このとき、$a^{p^m-1} = 1$ と $a^{k_0} = 1$ から

$$1 = a^{p^m-1} = a^{nk_0+r} = (a^{k_o})^n \cdot a^r = a^r$$

となる。ここで、k_0 の最小性から、$r = 0$ が分かり、$p^m - 1 = nk_0$ を得る。

定理 18 $GF(p^m)$ には位数 $p^m - 1$ の元 β が存在して

$$GF(p^m) = \{0, 1, \beta, \beta^2, \cdots, \beta^{p^m-2}\}$$

と表せる。特に、元 β を原始元といい、β を根としてもつ最小次数のモニック多項式を原始多項式という。

この定理から、$GF(p^m)$ の非零の元全てが β のべき乗によって表せる。このような表現を $GF(p^m)$ の元の「べき表現」という。

(例)　$p(x) = x^2 + x + 1$ の根の 1 つを α とすれば $GF(4) = \{0, 1, \alpha, \alpha + 1\}$ である。このとき、$\alpha^2 = \alpha + 1$ なので $GF(4) = \{0, 1, \alpha, \alpha^2\}$ とべき表現される。また

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

なので、α の位数は 3 であり、α は原始元である。

(定理 18 の証明)　素多項式 $p(x) = x^4 + x^3 + 1$ によって作られる $GF(2^4)$ について証明する。他の有元体についてもほぼ同様に示せる。$h = 2^4 - 1 = 15$ を素因数分解すると $h = 3 \times 5$ となる。$x^3 - 1$ の根でない $GF(2^4)$ の元を 1 つ選ぶ。$p(x) = 0$ の根の 1 つを α とすると α は $x^3 - 1$ の根ではない。そこで

$$\beta_1 = \alpha^{h/3} = \alpha^5 (\neq 1)$$

とおくと、$\beta_1^3 = (\alpha^5)^3 = \alpha^{15} = 1$ であり、β_1 の位数は 15 の約数でなければならないので、β_1 の位数は 3 である。

同様にして、$x^5 - 1$ の根でない $GF(2^4)$ の元として、α を選ぶ。
$(\because \alpha^5 + 1 = (\alpha + 1)p(x) + \alpha^3 + 1 = \alpha^3 + 1)$

$$\beta_2 = \alpha^{h/5} = \alpha^3 (\neq 1)$$

とおくと、$(\beta_2)^5 = \alpha^{15} = 1$ であり、β_2 の位数が 5 であることが分かる。このとき $\beta = \beta_1\beta_2$ は原始元となる。なぜならば、β の位数は補題 1 から、15 の約数であり、

$$\begin{aligned} \beta &= \alpha^5 \cdot \alpha^3 = \alpha^8 \neq 1 \\ \beta^3 &= (\beta_1)^3(\beta_2)^3 = \beta_2^3 \neq 1 \\ \beta^5 &= (\beta_1)^5(\beta_2)^5 = \beta_1^5 = \beta_1^2 \neq 1 \end{aligned}$$

から、β の位数が 15 であることが分かる。