情報数学 II-B 演習　No.5 略解

問題 1. GF(2) を位数が 2 の有限体とする．GF(2) $= \{0, 1\}$ とし，GF(2) 上の 2 つの既約多項式をそれぞれ $m_1(x) = x^3 + x + 1$, $m_2(x) = x^3 + x^2 + 1$ とする．また $m_1(x)$ で拡大した体を K, $m_2(x)$ で拡大した体を G とするとき次の問いに答えよ．

(1) $m_2(x) = 0$ の根を α とする．α が拡大体 G の原始元であることを示せ．

$$G = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

$$\begin{aligned}
\alpha &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^2 + 1 \\
\alpha^4 &= \alpha^2 + \alpha + 1 \\
\alpha^5 &= \alpha + 1 \\
\alpha^6 &= \alpha^2 + \alpha \\
\alpha^7 &= 1
\end{aligned}$$

よって α 原始元である．

(2) G の各元の GF(2) 上の最小多項式を求めよ．
講義ノートの定理 16 を用いれば，β が GF(2) 上のある多項式 $m(x)$ の根であるならば，$\beta^2, \beta^{2^2}, \ldots$ も $m(x)$ の根であることが分かり，多項式の次数は根の個数と一致することから，求めたい最小多項式の次数を確定できる．

G	$m(x)$
0	x
1	$x+1$
α	x^3+x^2+1
α^2	x^3+x^2+1
α^3	x^3+x+1
α^4	x^3+x^2+1
α^5	x^3+x+1
α^6	x^3+x+1

(3) $m_2(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$, $m_1(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5)$ が成り立つことを確認せよ．

$$\begin{aligned}
m_2(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4) \\
&= x^3 - (\alpha + \alpha^2 + \alpha^4)x^2 + (\alpha^3 + \alpha^5 + \alpha^6)x - \alpha^7 \\
&= x^3 + x^2 + 1 \\
m_1(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) \\
&= x^3 - (\alpha^3 + \alpha^6 + \alpha^5)x^2 + (\alpha^9 + \alpha^11 + \alpha^8)x - \alpha^14 \\
&= x^3 + x + 1
\end{aligned}$$

(4) K と G が同型であることを確かめよ.

$m_1(x) = 0$ の根を β とする

$$K = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}$$

$$\begin{aligned}
\beta &= \beta \\
\beta^2 &= \beta^2 \\
\beta^3 &= \beta + 1 \\
\beta^4 &= \beta^2 + \beta \\
\beta^5 &= \beta^2 + \beta + 1 \\
\beta^6 &= \beta^2 + 1 \\
\beta^7 &= 1
\end{aligned}$$

ここで, 以下のように定義する

$$\begin{array}{cccc} \phi : & K & \to & G \\ & \beta^k & \mapsto & \alpha^{3k} \end{array}$$

問題 2. GF(3) を位数が 3 の有限体とする．GF(3) = $\{0, 1, 2\}$ とし，GF(3) 上の既約多項式を $m(x) = x^2 + 1$ とする．このとき $m(x) = 0$ の根を α とし，$K = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$ とおく.

(1) K の原始元を 1 つ求めよ.（この原始元を β とする）

$$\beta = \alpha + 1$$

とすると

$$\begin{aligned}
\beta^1 &= \alpha + 1 \\
\beta^2 &= 2\alpha \\
\beta^3 &= 2\alpha + 1 \\
\beta^4 &= 2 \\
\beta^5 &= 2\alpha + 2 \\
\beta^6 &= \alpha \\
\beta^7 &= \alpha + 2 \\
\beta^8 &= 1
\end{aligned}$$

(2) K の各元の最小多項式を求めよ.

G	$m(x)$
0	x
1	$x+2$
β	x^2+x+2
β^2	x^2+1
β^3	x^2+x+2
β^4	$x+1$
β^5	x^2+2x+2
β^6	x^2+1
β^7	x^2+2x+2

(3) $x^9 - x = x(x-1)(x-2)m_1(x)m_2(x)m_3(x)$ が成り立つことを示せ．(ただし，$m_i(x)$ は 2 次の既約多項式とする.$(i=1,2,3)$)

問題 3. GF(2^4) の原始元 α の最小多項式 $m_1(x) = x^4 + x + 1$ とする．

(1) GF(2^4) の 0 以外の元を，α のベキ表現，α の 3 次以下の多項式表現， 4 次元ベクトルで表現せよ.

解答.

慎重に計算していけば，次の表が得られるはずである.

表 1: GF(2^4) の各表現によって得られる表

べき	多項式	ベクトル	べき	多項式	ベクトル
1	1	$(0,0,0,1)$			
α	α	$(0,0,1,0)$	α^8	α^2+1	$(0,1,0,1)$
α^2	α^2	$(0,1,0,0)$	α^9	$\alpha^3+\alpha$	$(1,0,1,0)$
α^3	α^3	$(1,0,0,0)$	α^{10}	$\alpha^2+\alpha+1$	$(0,1,1,1)$
α^4	$\alpha+1$	$(0,0,1,1)$	α^{11}	$\alpha^3+\alpha^2+\alpha$	$(1,1,1,0)$
α^5	$\alpha^2+\alpha$	$(0,1,1,0)$	α^{12}	$\alpha^3+\alpha^2+\alpha+1$	$(1,1,1,1)$
α^6	$\alpha^3+\alpha^2$	$(1,1,0,0)$	α^{13}	$\alpha^3+\alpha^2+1$	$(1,1,0,1)$
α^7	$\alpha^3+\alpha+1$	$(1,0,1,1)$	α^{14}	α^3+1	$(1,0,0,1)$

(2) α^3 の最小多項式 $m_3(x)$ を求めよ.

解答.

問題 2 のときと同様に考えればよい．α^3 のべきを考えてみる．$(\alpha^3)^2 = \alpha^6, (\alpha^3)^{2^2} = \alpha^{12}, (\alpha^3)^{2^3} = \alpha^9$ であるから，$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ は同じ最小多項式をもち，その多項式は次数が 4 であることが分かる．これを，

$$m_3(x) = x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \quad (c_0, c_1, c_2, c_3 \in \mathrm{GF}(2))$$

とおこう．α^3 は最小多項式の定義より $m_3(x)$ の根であるから，

$$\begin{aligned}m_3(\alpha^3) &= (\alpha^3)^4 + c_3(\alpha^3)^3 + c_2(\alpha^3)^2 + c_1\alpha^3 + c_0 \\ &= \alpha^{12} + c_3\alpha^9 + c_2\alpha^6 + c_1\alpha^3 + c_0 \\ &= (\alpha^3 + \alpha^2 + \alpha + 1) + c_3(\alpha^3 + \alpha) + c_2(\alpha^3 + \alpha^2)c_1\alpha^3 + c_0 \\ &= (c_3 + c_2 + c_1 + 1)\alpha^3 + (c_2 + 1)\alpha^2 + (c_3 + 1)\alpha + (c_0 + 1) = 0\end{aligned}$$

が成り立つ．さて，この式が恒等的に成り立つようにするためには，

$$\begin{cases} c_3 + c_2 + c_1 + 1 = 0 \\ c_2 + 1 = 0 \\ c_3 + 1 = 0 \\ c_0 + 1 = 0 \end{cases}$$

を解けばよい．結果として $c_3 = c_2 = c_1 = c_0 = 1$ が得られる．以上より，α^3 の最小多項式は $m_3(x) = x^4 + x^3 + x^2 + x + 1$ である．

(3) α^5 の最小多項式 $m_5(x)$ を求めよ.
α^5 の最小多項式は $m_5(x) = x^2 + x + 1$ である．

(4) α^7 の最小多項式 $m_7(x)$ を求めよ.
α^7 の最小多項式は $m_7(x) = x^4 + x^3 + 1$ である．

(5) $x^{16} - x = x(x-1)m_1(x)m_3(x)m_5(x)m_7(x)$ が成り立つことを確認せよ.