代数系と符号理論 (O) [第 2 回宿題]

通信情報工学専攻 植松友彦

提出方法

- 必ず宿題用ノートを用意し, ノートを提出すること. レポート用紙, ルーズリーフ等はたとえ綴じてあっても不可. ノートの表紙に必ず学籍番号と氏名を記入すること.
- 答えを見て自己採点 (◯か×) をすること.
- 締切: 6 月 18 日 (水) の演習終了時

(問題 1)

$\mathbb{F}_2$ 上の 4 次既約多項式 $f(x) = x^4 + x^3 + 1$ の根 α を用いて構成される $\mathbb{F}_{2^4}$ について, 次の問いに答えよ.

1) α が原始元であることを下記の表の空欄を埋めることで示せ.

べき表示	多項式表示		べき表示	多項式表示
α	α		α^9	
α^2	α^2		α^{10}	
α^3	α^3		α^{11}	
α^4			α^{12}	
α^5			α^{13}	
α^6			α^{14}	
α^7			α^{15}	1
α^8			——	——

2) 次の乗算表の空欄を多項式表示で埋めよ.

	α^2+1	$\alpha^3+\alpha$	α^3	α^3+1
α^3+1				
α^2				
α				
$\alpha+1$				
α^2+1				
$\alpha^2+\alpha+1$				
$\alpha^2+\alpha$				
$\alpha^3+\alpha$				

	$\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2
α^3+1				
α^2				
α				
$\alpha+1$				
α^2+1				
$\alpha^2+\alpha+1$				
$\alpha^2+\alpha$				
$\alpha^3+\alpha$				

3) 各元の位数を求めよ.

元	位数		元	位数
1			α^8	
α			α^9	
α^2			α^{10}	
α^3			α^{11}	
α^4			α^{12}	
α^5			α^{13}	
α^6			α^{14}	
α^7			——	——

4) 次の計算を行え.

(a) $(y+\alpha)(y+\alpha^2)(y+\alpha^4)(y+\alpha^8)$

(b) $(y+\alpha^3)(y+\alpha^6)(y+\alpha^{12})(y+\alpha^9)$

(c) $(y+\alpha^5)(y+\alpha^{10})$

(d) $(y+\alpha^7)(y+\alpha^{14})(y+\alpha^{13})(y+\alpha^{11})$

(問題2)

$\mathbb{F}_2$ 上の 4 次既約多項式 $f(x)=x^4+x^3+x^2+x+1$ の根 α を用いて構成される $\mathbb{F}_{2^4}$ について, 次の問いに答えよ.

1) α が原始元でないことを下記の表の空欄を埋めることで示せ.

べき表示	多項式表示		べき表示	多項式表示
α	α		α^9	
α^2	α^2		α^{10}	
α^3	α^3		α^{11}	
α^4			α^{12}	
α^5			α^{13}	
α^6			α^{14}	
α^7			α^{15}	1
α^8			——	——

2) 原始元 β を一つ求め, 下記の表の空欄を埋めよ.

べき表示	α の多項式表示		べき表示	α の多項式表示
β			β^9	
β^2			β^{10}	
β^3			β^{11}	
β^4			β^{12}	
β^5			β^{13}	
β^6			β^{14}	
β^7			β^{15}	1
β^8			——	——

3) 次の乗算表の空欄を α の多項式表示で埋めよ.

	α^2+1	$\alpha^3+\alpha$	α^3	α^3+1
α^3+1				
α^2				
α				
$\alpha+1$				
α^2+1				
$\alpha^2+\alpha+1$				
$\alpha^2+\alpha$				
$\alpha^3+\alpha$				

	$\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2
α^3+1				
α^2				
α				
$\alpha+1$				
α^2+1				
$\alpha^2+\alpha+1$				
$\alpha^2+\alpha$				
$\alpha^3+\alpha$				

4) 各元の位数を求めよ.

元	位数		元	位数
1			β^8	
β			β^9	
β^2			β^{10}	
β^3			β^{11}	
β^4			β^{12}	
β^5			β^{13}	
β^6			β^{14}	
β^7			――	――

5) 次の計算を行え.

(a) $(y+\alpha)(y+\alpha^2)(y+\alpha^4)(y+\alpha^8)$

(b) $(y+\alpha^3)(y+\alpha^6)(y+\alpha^{12})(y+\alpha^9)$

(c) $(y+\alpha^5)(y+\alpha^{10})$

(d) $(y+\alpha^7)(y+\alpha^{14})(y+\alpha^{13})(y+\alpha^{11})$

(問題 3)

$\mathbb{F}_2$ 上の 5 次既約多項式 $f(x)=x^5+x^2+1$ の根 α を用いて構成される $\mathbb{F}_{2^5}$ について, 次の問いに答えよ.

1) α が原始元であることを下記の表の空欄を埋めることで示せ.

べき表示	多項式表示		べき表示	多項式表示
α	α		α^{17}	
α^2	α^2		α^{18}	
α^3	α^3		α^{19}	
α^4	α^4		α^{20}	
α^5			α^{21}	
α^6			α^{22}	
α^7			α^{23}	
α^8			α^{24}	
α^9			α^{25}	
α^{10}			α^{26}	
α^{11}			α^{27}	
α^{12}			α^{28}	
α^{13}			α^{29}	
α^{14}			α^{30}	
α^{15}			α^{31}	
α^{16}			—	—

2) 次の乗算表の空欄を多項式表示で埋めよ.

	α^2+1	$\alpha^4+\alpha^3+\alpha$	α^3	$\alpha^4+\alpha^3+1$
α^3+1				
$\alpha^4+\alpha^2$				
α				
$\alpha^4+\alpha+1$				
α^2+1				
$\alpha^4+\alpha^2+\alpha+1$				
$\alpha^2+\alpha$				
$\alpha^4+\alpha^3+\alpha$				

	$\alpha^4+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^4+\alpha^2+\alpha+1$	α^2
α^3+1				
$\alpha^4+\alpha^2$				
α				
$\alpha^4+\alpha+1$				
α^2+1				
$\alpha^4+\alpha^2+\alpha+1$				
$\alpha^2+\alpha$				
$\alpha^4+\alpha^3+\alpha$				

3) 次の計算を行え.

(a) $(y+\alpha)(y+\alpha^2)(y+\alpha^4)(y+\alpha^8)(y+\alpha^{16})$

(b) $(y+\alpha^3)(y+\alpha^6)(y+\alpha^{12})(y+\alpha^{24})(y+\alpha^{17})$

(c) $(y+\alpha^5)(y+\alpha^{10})(y+\alpha^{20})(y+\alpha^9)(y+\alpha^{18})$

(d) $(y+\alpha^7)(y+\alpha^{14})(y+\alpha^{28})(y+\alpha^{25})(y+\alpha^{19})$

(e) $(y+\alpha^{11})(y+\alpha^{22})(y+\alpha^{13})(y+\alpha^{26})(y+\alpha^{21})$

(f) $(y+\alpha^{15})(y+\alpha^{30})(y+\alpha^{29})(y+\alpha^{27})(y+\alpha^{23})$

代数系と符号理論 (O) [第 2 回宿題の解答]

通信情報工学専攻 植松友彦

(問題 1 の解答)

1) 次の表から α が原始元であることが示された.

べき表示	多項式表示		べき表示	多項式表示
α	α		α^9	α^2+1
α^2	α^2		α^{10}	$\alpha^3+\alpha$
α^3	α^3		α^{11}	$\alpha^3+\alpha^2+1$
α^4	α^3+1		α^{12}	$\alpha+1$
α^5	$\alpha^3+\alpha+1$		α^{13}	$\alpha^2+\alpha$
α^6	$\alpha^3+\alpha^2+\alpha+1$		α^{14}	$\alpha^3+\alpha^2$
α^7	$\alpha^2+\alpha+1$		α^{15}	1
α^8	$\alpha^3+\alpha^2+\alpha$		——	———

2) 表は以下の通り.

	α^2+1	$\alpha^3+\alpha$	α^3	α^3+1
α^3+1	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$
α^2	$\alpha^3+\alpha^2+1$	$\alpha+1$	$\alpha^3+\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$
α	$\alpha^3+\alpha$	$\alpha^3+\alpha^2+1$	α^3+1	$\alpha^3+\alpha+1$
$\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	1	α
α^2+1	α^3	α^3+1	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha+1$	α	α^2	$\alpha^3+\alpha$	$\alpha^3+\alpha^2+1$
$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	α	α^2
$\alpha^3+\alpha$	α^3+1	$\alpha^3+\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$

	$\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2
α^3+1	α^2	$\alpha^3+\alpha$	$\alpha^3+\alpha^2+1$	$\alpha^3+\alpha^2+\alpha+1$
α^2	1	$\alpha^3+\alpha^2+\alpha$	α^2+1	α^3+1
α	$\alpha^3+\alpha^2$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	α^3
$\alpha+1$	$\alpha^3+\alpha$	α^3	α^3+1	$\alpha^3+\alpha^2$
α^2+1	$\alpha^2+\alpha+1$	1	α	$\alpha^3+\alpha^2+1$
$\alpha^2+\alpha+1$	$\alpha^3+\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	α^2+1
$\alpha^2+\alpha$	$\alpha^3+\alpha^2+1$	α^3+1	$\alpha^3+\alpha+1$	1
$\alpha^3+\alpha$	$\alpha^3+\alpha^2+\alpha$	α	α^2	$\alpha+1$

3) 位数は以下の通り.

元	位数		元	位数
1	1		α^8	15
α	15		α^9	5
α^2	15		α^{10}	3
α^3	5		α^{11}	15
α^4	15		α^{12}	5
α^5	3		α^{13}	15
α^6	5		α^{14}	15
α^7	15		——	——

4) (a)

$$\begin{aligned}
&(y+\alpha)(y+\alpha^2)(y+\alpha^4)(y+\alpha^8)\\
&= \{y^2+(\alpha+\alpha^2)y+\alpha^3\}\{y^2+(\alpha^4+\alpha^8)y+\alpha^{12}\}\\
&= (y^2+\alpha^{13}y+\alpha^3)(y^2+\alpha^7y+\alpha^{12})\\
&= y^4+(\alpha^{13}+\alpha^7)y^3+(\alpha^3+\alpha^{12}+\alpha^{20})y^2+(\alpha^{156}+\alpha^{21})y+\alpha^{15}\\
&= y^4+y^3+1
\end{aligned}$$

(b)

$$\begin{aligned}
&(y+\alpha^3)(y+\alpha^6)(y+\alpha^{12})(y+\alpha^9)\\
&= (y+\alpha^3)(y+\alpha^{12})(y+\alpha^6)(y+\alpha^9)\\
&= \{y^2+(\alpha^3+\alpha^{12})y+\alpha^{15}\}\{y^2+(\alpha^6+\alpha^9)y+\alpha^{15}\}\\
&= (y^2+\alpha^5y+1)(y^2+\alpha^{10}y+1)\\
&= (y^2+1)^2+(\alpha^5+\alpha^{10})y(y^2+1)+\alpha^{15}y^2\\
&= y^4+1+y^3+y+y^2\\
&= y^4+y^3+y^2+y+1
\end{aligned}$$

(c)

$$\begin{aligned}
(y+\alpha^5)(y+\alpha^{10}) &= y^2+(\alpha^5+\alpha^{10})y+\alpha^{15}\\
&= y^2+y+1
\end{aligned}$$

(d)

$$\begin{aligned}
&(y+\alpha^7)(y+\alpha^{14})(y+\alpha^{13})(y+\alpha^{11})\\
&= \{y^2+(\alpha^7+\alpha^{14})y+\alpha^{21}\}\{y^2+(\alpha^{13}+\alpha^{11})y+\alpha^{24}\}\\
&= (y^2+\alpha^5y+\alpha^6)(y^2+\alpha^5y+\alpha^9)\\
&= (y^2+\alpha^5y)^2+(\alpha^6+\alpha^9)(y^2+\alpha^5y)+\alpha^{15}\\
&= y^4+\alpha^{10}y^2+\alpha^{10}y^2+\alpha^{15}y+1\\
&= y^4+y+1
\end{aligned}$$

(問題 2 の解答)

1) 表から α が原始元でないことが示された.

べき表示	多項式表示		べき表示	多項式表示
α	α		α^9	$\alpha^3+\alpha^2+\alpha+1$
α^2	α^2		α^{10}	1
α^3	α^3		α^{11}	α
α^4	$\alpha^3+\alpha^2+\alpha+1$		α^{12}	α^2
α^5	1		α^{13}	α^3
α^6	α		α^{14}	$\alpha^3+\alpha^2+\alpha+1$
α^7	α^2		α^{15}	1
α^8	α^3		——	——

2) 原始元 $\beta=\alpha+1$ とすると, 表は以下の通り.

べき表示	α の多項式表示		べき表示	α の多項式表示
β	$\alpha+1$		β^9	α^2
β^2	α^2+1		β^{10}	$\alpha^3+\alpha^2$
β^3	$\alpha^3+\alpha^2+\alpha+1$		β^{11}	$\alpha^3+\alpha+1$
β^4	$\alpha^3+\alpha^2+\alpha$		β^{12}	α
β^5	$\alpha^3+\alpha^2+1$		β^{13}	$\alpha^2+\alpha$
β^6	α^3		β^{14}	$\alpha^3+\alpha$
β^7	$\alpha^2+\alpha+1$		β^{15}	1
β^8	α^3+1		——	——

3) 表は以下の通り.

	α^2+1	$\alpha^3+\alpha$	α^3	α^3+1
α^3+1	$\alpha^3+\alpha^2$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha$	$\alpha+1$
α^2	$\alpha^3+\alpha+1$	α^3+1	1	α^2+1
α	$\alpha^3+\alpha$	$\alpha^3+\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$
$\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$	1	$\alpha^2+\alpha+1$	α^2
α^2+1	$\alpha^3+\alpha^2+\alpha$	$\alpha+1$	α^3+1	$\alpha^3+\alpha^2$
$\alpha^2+\alpha+1$	α^2	α^3	$\alpha^2+\alpha$	1
$\alpha^2+\alpha$	1	α	$\alpha^3+\alpha^2+\alpha$	α^3
$\alpha^3+\alpha$	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2+1$	$\alpha^2+\alpha+1$

	$\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2
α^3+1	α^3	$\alpha^3+\alpha+1$	1	α^2+1
α^2	$\alpha^2+\alpha+1$	α	$\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$
α	$\alpha^3+\alpha^2$	1	$\alpha^3+\alpha^2+\alpha$	α^3
$\alpha+1$	$\alpha^3+\alpha$	$\alpha^3+\alpha^2+\alpha$	α^3+1	$\alpha^3+\alpha^2$
α^2+1	1	$\alpha^3+\alpha^2+1$	α^2	$\alpha^3+\alpha+1$
$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	$\alpha^3+\alpha^2$	$\alpha^3+\alpha$	$\alpha+1$
$\alpha^2+\alpha$	$\alpha^3+\alpha+1$	$\alpha+1$	$\alpha^3+\alpha^2+1$	$\alpha^2+\alpha+1$
$\alpha^3+\alpha$	α	α^2+1	α^3	α^3+1

4) 位数は以下の通り.

元	位数		元	位数
1	1		β^8	15
β	15		β^9	5
β^2	15		β^{10}	3
β^3	5		β^{11}	15
β^4	15		β^{12}	5
β^5	3		β^{13}	15
β^6	5		β^{14}	15
β^7	15		——	——

5) (a)

$$\begin{aligned}
&(y+\alpha)(y+\alpha^2)(y+\alpha^4)(y+\alpha^8)\\
&= (y+\alpha)(y+\alpha^4)(y+\alpha^2)(y+\alpha^3)\\
&= \{y^2+(\alpha+\alpha^4)y+\alpha^5\}\{y^2+(\alpha^2+\alpha^3)y+\alpha^5\}\\
&= (y^2+\beta^5 y+1)(y^2+\beta^{10}y+1)\\
&= (y^2+1)^2+(\beta^5+\beta^{10})y(y^2+1)+\beta^{15}y^2\\
&= y^4+1+y^3+y+y^2\\
&= y^4+y^3+y^2+y+1
\end{aligned}$$

(b)

$$\begin{aligned}
&(y+\alpha^3)(y+\alpha^6)(y+\alpha^{12})(y+\alpha^9)\\
&= (y+\alpha^3)(y+\alpha^1)(y+\alpha^2)(y+\alpha^4)\\
&= y^4+y^3+y^2+y+1
\end{aligned}$$

(c)

$$\begin{aligned}
(y+\alpha^5)(y+\alpha^{10}) &= (y+1)^2\\
&= y^2+1
\end{aligned}$$

(d)

$$
\begin{aligned}
&(y+\alpha^7)(y+\alpha^{14})(y+\alpha^{13})(y+\alpha^{11})\\
&\quad= \quad (y+\alpha^2)(y+\alpha^4)(y+\alpha^3)(y+\alpha^1)\\
&\quad= \quad y^4+y^3+y^2+y+1
\end{aligned}
$$

(問題 3 の解答)

1) 表は以下の通りとなり, α が原始元であることが示された.

べき表示	多項式表示		べき表示	多項式表示
α	α		α^{17}	$\alpha^4+\alpha+1$
α^2	α^2		α^{18}	$\alpha+1$
α^3	α^3		α^{19}	$\alpha^2+\alpha$
α^4	α^4		α^{20}	$\alpha^3+\alpha^2$
α^5	α^2+1		α^{21}	$\alpha^4+\alpha^3$
α^6	$\alpha^3+\alpha$		α^{22}	$\alpha^4+\alpha^2+1$
α^7	$\alpha^4+\alpha^2$		α^{23}	$\alpha^3+\alpha^2+\alpha+1$
α^8	$\alpha^3+\alpha^2+1$		α^{24}	$\alpha^4+\alpha^3+\alpha^2+\alpha$
α^9	$\alpha^4+\alpha^3+\alpha$		α^{25}	$\alpha^4+\alpha^3+1$
α^{10}	α^4+1		α^{26}	$\alpha^4+\alpha^2+\alpha+1$
α^{11}	$\alpha^2+\alpha+1$		α^{27}	$\alpha^3+\alpha+1$
α^{12}	$\alpha^3+\alpha^2+\alpha$		α^{28}	$\alpha^4+\alpha^2+\alpha$
α^{13}	$\alpha^4+\alpha^3+\alpha^2$		α^{29}	α^3+1
α^{14}	$\alpha^4+\alpha^3+\alpha^2+1$		α^{30}	$\alpha^4+\alpha$
α^{15}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$		α^{31}	1
α^{16}	$\alpha^4+\alpha^3+\alpha+1$		——	——

2) 表は以下の通り.

	α^2+1	$\alpha^4+\alpha^3+\alpha$	α^3	$\alpha^4+\alpha^3+1$
α^3+1	α^3	$\alpha^4+\alpha^2$	α	$\alpha^3+\alpha^2+\alpha+1$
$\alpha^4+\alpha^2$	$\alpha^3+\alpha^2+\alpha$	$\alpha^4+\alpha^3+\alpha+1$	α^4+1	α
α	$\alpha^3+\alpha$	α^4+1	α^4	$\alpha^4+\alpha^2+\alpha+1$
$\alpha^4+\alpha+1$	$\alpha^4+\alpha^2+1$	$\alpha^4+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2$	$\alpha^2+\alpha+1$
α^2+1	α^4+1	$\alpha^4+\alpha^3+\alpha^2+1$	$\alpha^3+\alpha^2+1$	$\alpha^4+\alpha$
$\alpha^4+\alpha^2+\alpha+1$	1	α^4	α^3+1	$\alpha^3+\alpha^2$
$\alpha^2+\alpha$	$\alpha^4+\alpha^3+\alpha^2+\alpha$	$\alpha^4+\alpha^2+\alpha$	$\alpha^4+\alpha^2+1$	$\alpha^4+\alpha^3+\alpha^2$
$\alpha^4+\alpha^3+\alpha$	$\alpha^4+\alpha^3+\alpha^2+1$	$\alpha+1$	$\alpha^3+\alpha^2+\alpha$	α^3

	$\alpha^4+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^4+\alpha^2+\alpha+1$	α^2
α^3+1	$\alpha^4+\alpha^2+\alpha+1$	$\alpha^4+\alpha^3$	$\alpha^4+\alpha^3+\alpha^2+\alpha$	1
$\alpha^4+\alpha^2$	α^4	$\alpha^4+\alpha$	α^2	$\alpha^4+\alpha^3+\alpha$
α	α^3+1	$\alpha^4+\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha+1$	α^3
$\alpha^4+\alpha+1$	$\alpha^4+\alpha^3+\alpha^2+1$	$\alpha^4+\alpha^3+\alpha$	$\alpha^3+\alpha^2+\alpha$	$\alpha^2+\alpha$
α^2+1	α^2	$\alpha^4+\alpha^2+\alpha$	1	$\alpha^4+\alpha^2$
$\alpha^4+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^4+\alpha^3$	$\alpha^4+\alpha^2+\alpha$
$\alpha^2+\alpha$	$\alpha^4+\alpha^3+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^4+\alpha^3+\alpha^2+1$	$\alpha^4+\alpha^3$
$\alpha^4+\alpha^3+\alpha$	$\alpha^3+\alpha$	α	α^4	$\alpha^2+\alpha+1$

3) (a) y^5+y^2+1

(b) $y^5+y^4+y^3+y^2+1$

(c) $y^5+y^4+y^2+y+1$

(d) $y^5+y^3+y^2+y+1$

(e) $y^5+y^4+y^3+y+1$

(f) y^5+y^3+1