5 4つの元からなる体 $\mathbb{F}_4$

入学年度		学部	学 科		組		番　号			検	フリガナ	
		B		1							氏 名	

これまでに，各素数 p について，p 個の元からなる体，p 元体 $\mathbb{F}_p$ があることを知った．それでは，元の個数が 4 である体は存在するだろうか．すでに見たように，合成数 4 を法とする剰余環 $\mathbb{Z}/4\mathbb{Z}$ は 4 個の元からなるが，必ずしも除法が可能ではないので，$\mathbb{Z}/4\mathbb{Z}$ は体ではない．しかし，結論から言うと 4 つの元からなる体 $\mathbb{F}_4$ は存在する．それはどのようなものかを見てみよう．

4 つの元からなる体を $\mathbb{F}_4$ とすると，その中に 0 と 1 が含まれるから，$\mathbb{F}_4 = \{0, 1, a, b\}$ と書ける．このとき，$0, 1, a, b$ は相異なる元である．まず，$\mathbb{F}_4$ の乗法表を作るとの表 1 のようになるはずである．

$\times$	1	a	b
1	1	a	b
a	a	a^2	ab
b	b	ab	b^2

表 1　$\mathbb{F}_4$ の乗法表

1　a)　$a^2 = b$ は $ab = 1$ であることを示せ．
［乗法表の a の行 (a, a^2, ab) は $1, a, b$ を並べ直したもの（置換という）だが，一番左端は a で決まっているので，$(a^2, ab) = (1, b)$，または $(b, 1)$．この後，縦の列についても異なる元が並ぶこと用いる．］

b)　前問より，$a^3 = 1$ が成り立つことを示せ．［$ab = 1$ に $b = a^2$ を代入する．］

c)　a は $x^2 + x + 1 = 0$ の解であることを示せ．
［方程式 $x^3 - 1 = 0$ は通常通り $(x - 1)(x^2 + x + 1) = 0$ と因数分解できる．$a \neq 1$ だから，a は $x^2 + x + 1 = 0$ の解である．a^2 も同様に $x^3 - 1 = 0$ をみたす．］

d)　a^2 も $x^2 + x + 1 = 0$ の解であることを示し，$\mathbb{F}_4$ 上では $(x^2 + x + 1) = (x - a)(x - a^2)$ と因数分解できることを示せ．［$x^2 + x + 1 = 0$ に a^2 を代入し，$a^3 = 1$ であることを用いる．］

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	$1+1$	$a+1$	a^2+1
a	a	$a+1$	$a+a$	$a+a^2$
a^2	a^2	a^2+1	$a+a^2$	a^2+a^2

表 2　$\mathbb{F}_4$ の加法表

e)　上の加法表で，「1」の行 $(1, 1+1, a+1, a^2+1)$ には必ず 0 が含まれるが，$a+1$, a^2+1 はともに 0 ではあり得ないことを示し，$1 + 1 = 0$ であることを示せ．［$a + 1 = 0$ なら，d) より $a + a^2 + 1 = 0$ だから，$a^2 = 0$ となり矛盾．$a^2 + 1$ についても同様．］

f)　加法表の「1」の行は $(1, 0, a^2, a)$ となることを示せ．［縦の列についても，すべての異なる元が並ぶことによる．］

g)　分配法則を用いて $a + a = 0$ を示せ．［$(1 + 1)a = a + a$ による．］

h)　$\mathbb{F}_4$ の加法表と乗法表を完成せよ．（加法表には 0, 1, a, $a + 1$ を，乗法表には 1, a, a^2 を用いよ．）

$+$	0	1	a	$a+1$
0				
1				
a				
$a+1$				

$\times$	1	a	a^2
1			
a			
a^2			

表 3　$\mathbb{F}_4$ の加法・乗法表

【裏に続く】

表で得られた結果をまとめると

- $1+1=0$ である．これにより，すべての元 a について $2a=0$ になる．
- 減法は加法と一致する．なぜなら，$a+a=0$ より，$-a=a$ が得られ，$b-a=b+(-a)=b+a$ となるからである．
- $\mathbb{F}_4$ の 0 以外の元はすべて $x^3=1$ をみたす．（フェルマーの小定理の類似）
- $\mathbb{F}_4$ の $0,\ 1$ 以外の元の一つを a と書く代わりに ω と書くと，$\omega^2+\omega+1=0$ であり，もう一つの 0 と 1 以外の $\mathbb{F}_4$ の元は ω^2 と表され，これは $\omega+1$ と一致する．すなわち，ω は複素数の $\omega=\frac{-1+\sqrt{3}i}{2}$ と類似の性質を持つ．複素数の場合は $\omega^2=-\omega-1$ であるが，$\mathbb{F}_4$ では，'+' = '−' であるから，$\omega^2=\omega+1$ となる．また，$\omega^3=1$ より，$\omega^2=\omega^{-1}$ も成り立つ．

$\mathbb{F}_4$ の加法表・乗法表は下のようになる．加法表では第 4 の元を $\omega+1$, 乗法表では ω^2 と表す方が都合がよいので，そのように表した．

$+$	0	1	ω	$\omega+1$
0	0	1	ω	$\omega+1$
1	1	0	$\omega+1$	ω
ω	ω	$\omega+1$	0	1
$\omega+1$	$\omega+1$	ω	1	0

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

表 4　$\mathbb{F}_4$ の加法・乗法表

2　$\mathbb{F}_4$ の $0,\ 1$ 以外の元の一つを ω としたとき，次の各元を $a\omega+b$ $(a,b=0$ または $1)$ の形に表せ．

a）$\dfrac{1}{\omega+1}$　　b）$\omega(\omega+1)$　　c）$\omega^2-(\omega-1)$

d）$\dfrac{\omega}{\omega+1}$　　e）ω^4　　f）$\dfrac{\omega^2}{\omega-1}$

体 K の元を係数とする多項式を K 上の多項式という．K 上の多項式間の四則演算は通常の多項式のときと同じにように行うことができる．体 K 上の多項式で，それよりも次数の低い K 上の多項式に因数分解できない多項式を K 上の**既約多項式**という．

例 1　$\mathbb{F}_2=\{0,1\}$ 上の多項式として $x,\ x+1$ は既約多項式であるが，x^2+1 は既約多項式ではない．なぜなら，$f(x)=x^2+1$ とおくと，$f(1)=1^2+1=1+1=0$ なので，因数定理により，$f(x)$ は $x-1$ で割り切れるからである．実際，$(x-1)^2=x^2-2x+1=x^2+1$ である．$\mathbb{F}_2$ 上では $x-1=x+1$ なので，$x^2+1=(x+1)^2$ でもあることに注意．一方，x^2+x+1 は $\mathbb{F}_2$ 上では既約である．

例 2　$\mathbb{F}_4=\{0,1,\omega,\omega^2\}$ 上の多項式としては x^2+x+1 は $x^2+x+1=(x-\omega)(x-\omega^2)$ と因数分解できるので，既約ではない．

3　a）$\mathbb{F}_2$ 上の 3 次の多項式をすべて挙げよ．そのうち，既約であるものは因数分解せよ．

b）$\mathbb{F}_2$ 上の 4 次の多項式のうち，既約であるものはいくつあるか．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)