4 4つの元からなる体 $\mathbb{F}_4$

2026年度前期　情報数学特論2（木曜4限）

入学年度	学部	学科	組	番号	検	フリガナ	
		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 $\mathbb{F}_p$ について調べた．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，零因子を持ち，除法が必ずしも可能ではないので，$\mathbb{Z}/4\mathbb{Z}$ 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考えてみよう．

4 つの元からなる体が存在するとして，それを $\mathbb{F}_4$ と書く．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．ここで，$0, 1, a, b$ は相異なる元である．以下に示す体の定義から，F_4 が持つべき性質を導き出してみよう．

「体」の定義

集合 K の任意の二つの元 a, b に対し，その**和** $a+b$ と**積** ab と呼ばれる K の元がそれぞれ定義され，次の（K 1）から（K 10）までの条件をみたすとき，K は**体**であるという．

(K 1)　【和の交換律】任意の a, b について，$a+b=b+a$.
(K 2)　【和の結合律】任意の a, b, c について $(a+b)+c=a+(b+c)$.
(K 3)　【加法の単位元 0 の存在】0 で表される K の元が存在し，すべての K の元 a に対して $a+0=a$ をみたす．
(K 4)　【加法の逆元の存在】任意の K の元 a に対して $-a$ で表される K の元が存在し，$a+(-a)=0$ をみたす．
(K 5)　【積の交換律】任意の a, b について，$ab=ba$.
(K 6)　【積の結合律】任意の a, b, c について，$(ab)c=a(bc)$.
(K 7)　【分配律】 任意の a, b, c について，$a(b+c)=ab+ac$.
(K 8)　【乗法の単位元 1 の存在】1 で表される K の元が存在し，すべての K の元 a に対して $a1=a$ をみたす．
(K 9)　【乗法の逆元の存在】0 でない任意の $\mathbb{R}$ の元 a に対して a^{-1} で表される K の元が存在し，$aa^{-1}=1$ をみたす．
(K 10)　【0 以外の元の存在】 $1 \neq 0$.

まず，$\mathbb{F}_4$ から 0 を除いた集合 $\mathbb{F}_4^\times = \{1, a, b\}$ を考える．$\mathbb{F}_4^\times$ は乗法について閉じており，$\mathbb{F}_4^\times$ 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　$\mathbb{F}_4^\times$ の乗法表

1　a)　$x \in \mathbb{F}_4^\times$ に対し，$m_a(x)=ax$ で定義される写像 $m_a : \mathbb{F}_4^\times \to \mathbb{F}_4^\times$ は全単射であることを (K 9) を用いて示せ．

b)　乗法表の a の行に着目する．a) により，(a, a^2, ab) は $(1, a, b)$ の置換になっていることがわかる．さらに，$a^2=b, ab=1$ であること，すなわち $(a, a^2, ab)=(a, b, 1)$ であることを示せ．

c)　b) により，a, a^2 はともに $x^3-1=0$ の解であることを示せ．

d)　a, a^2 はともに $x^2+x+1=0$ の解であることを示し，$x^2+x+1=(x-a)(x-a^2)$ と因数分解できることを示せ．［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 $a^2+a+1=0$ を満たす．a^2 も同様．］

ここまでで，$\mathbb{F}_4 = \{0, 1, a, a^2\}$ と表すことができることがわかった．この時点で，乗法表と加法表は以下のようにあらわされることがわかる．

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

$+$	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　$\mathbb{F}_4$ の乗法表と加法表

【裏に続く】

e) $x \in \mathbb{F}_4$ に対し，$\alpha_1(x) = x + 1$ で定義される写像 $\alpha_1 : \mathbb{F}_4 \to \mathbb{F}_4; x \mapsto x + 1$ は (K 4) により全単射である．これを用い，$1 + 1 = 0$ を示せ．［ $\alpha_1(a) = 0$ すなわち，$a + 1 = 0$ であるとすると，両辺に a^2 を加え，$a^2 + a + 1 = a^2$ となるが，これは $a^2 + a + 1 = 0$ と矛盾する．その他の場合も同様．］

f) 分配法則を用い，任意の $x \in \mathbb{F}_4$ について，$x + x = 0$，および $-x = x$ が成り立つことを示せ．［ $(1 + 1)x = x + x$ による．］

g) $\mathbb{F}_4$ 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　$\mathbb{F}_4$ の加法表と乗法表

これまでに得られた結果をまとめると以下のようになる．

- $1 + 1 = 0$ である．これにより，すべての元 x について $2x = 0$ になる．
- 減法は加法と一致する．なぜなら，$x + x = 0$ より，$-x = x$ が得られ，$b - x = b + (-x) = b + x$ 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，$0, 1$ 以外のもう一つの $\mathbb{F}_4$ 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 $\omega = \frac{-1+\sqrt{-3}}{2}$ 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，‘+’ と ‘−’ は同値であるから，$\omega^2 = \omega + 1$ となる．また，$\omega^3 = 1$ より，$\omega^2 = \omega^{-1}$ も成り立つ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)

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，既約でない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．