5 4つの元からなる数の体系

入学年度		学部	学科		組		番号			検	フリガナ	
2	3	B		1							氏名	

日頃我々が「数」と呼ぶものを特徴づける最も重要な性質は四則演算ができることである．とくに，有理数や実数は 0 以外の数による除法が必ずできる．このように，除法まで含めた四則演算について閉じている集合が他にもあれば，それもまた一つの数の体系と見做すのが現代数学である．前々回に見たように，「素数 p を法とする合同類」は四則演算について閉じた集合であり，これも新たな「数」の体系と見做される．さらに別の数の体系も作りたいが，そのためには，そもそも四則演算とは何か，そしてそれについて閉じている集合とはいかなるものかを，抽象的・形式的に定義しておかなければならない．そのような集合は「体」（独：Korper，仏：corps，英：field）と呼ばれ，ある種の「数の体系」とみなされる．

「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 $\mathbf{R}$ 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 $\mathbf{R}$ の元 a に対して a^{-1} または $1/a$ で表される $\mathbf{R}$ の元が存在し，$aa^{-1}=1$ をみたす.
(K 10)【0 以外の元の存在】 $1 \neq 0$.

(K 3), (K 8), (K 10) により，体 K は必ず 0 と 1 という異なる元をもつから，素数 2 を法とする合同類 $\mathbf{F}_2=\{0,1\}$ は最も小さい体ということになる．$\mathbf{F}_3, \mathbf{F}_5$ など，元の個数が 3 や 5 である体もある．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 を法とする合同類では必ずしも除法が可能ではないので，これは体ではない．結論から言うと，4 つの元からなる体 $\mathbf{F}_4$ は存在する．それはどのようなものかを見てみよう．

$\mathbf{F}_4$ は 4 つの元からなるが，その中に 0 と 1 が含まれるから，$\mathbf{F}_4=\{0,1,a,b\}$ と書ける．まず，$\mathbf{F}_4$ の乗法表を作るとの表 1 のようになる．

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

表 1　$\mathbf{F}_4$ の乗法表

1 a)　b は a の逆元であることを示せ.
［乗法表の a の行の中には 1 が現れないといけないが，$a=1$ または $a^2=1$ とすると矛盾が出る.］

b)　$a^2=a^{-1}$ であることを示し，$a^3=1$ が成り立つことを示せ.
［乗法表の b を a^{-1} と書き直す．a の行の中には $1, a, a^{-1}$ が 1 度ずつ現れるなければいけない.］

c)　a, a^{-1} はともに $x^2+x+1=0$ 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^{-1} も $x^3-1=0$ をみたす.］

d)　解と係数の関係を用いて，$a+a^{-1}+1=0$ であることを示せ.
［$\mathbf{F}_4$ 上では $(x^2+x+1)=(x-a)(x-a^{-1})$ と因数分解できる.］

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

$+$	0	1	a	a^{-1}
0	0	1	a	a^{-1}
1	1	2	$a+1$	$a^{-1}+1$
a	a	$a+1$	$2a$	$a+a^{-1}$
a^{-1}	a^{-1}	$a^{-1}+1$	$a+a^{-1}$	$2a^{-1}$

表 2　$\mathbf{F}_4$ の加法表

【裏に続く】

以上をまとめると

- $2 = 0$ である．これは $1 + 1 = 0$ とも言い換えられる．これにより，すべての元の 2 倍は 0 になる．
- 減法は加法と一致する．なぜなら，$a + b, a - b$ のそれぞれに b を加えると，いずれも a となり等しくなるからである．
- $\mathbf{F}_4$ 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）
- $\mathbf{F}_4$ の 0, 1 以外の元の一つを ω とおくと，$\omega^2 + \omega + 1 = 0$ であり，もう一つの 0, 1 以外の $\mathbf{F}_4$ の元は ω^2 と表され，これは $\omega + 1$ と一致する．（ω という文字は，この元が複素数の $\omega = \frac{-1+\sqrt{3}i}{2}$ と類似の性質を持つことによる．複素数の場合は $\omega^2 = -\omega - 1$ であるが，$\mathbf{F}_4$ では，‘+’ = ‘−’ であるから，$\omega^2 = \omega + 1$ となる．）

$\mathbf{F}_4$ 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 3　$\mathbf{F}_4$ の加法・乗法表

2　$\mathbf{F}_4$ 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. $\mathbf{F}_2 = \{0, 1\}$ 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，$f(x)$ は $x - 1$ $(= x + 1)$ 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．

3　a）$\mathbf{F}_2$ 上の 2 次の多項式をすべて挙げよ．そのうち，既約であるものをすべて言え．

b）$\mathbf{F}_2$ 上の 3 次の多項式をすべて挙げよ．そのうち，既約であるものをすべて言え．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)