入学年度		学部	学 科		組		番 号			検	フリガナ	
2	3	B		1							氏 名	

前回，4 つの元からなる体 $\mathbf{F}_4$ が存在することをみた．$\mathbf{F}_4$ は 0 と 1 のみからなる体 $\mathbf{F}_2 = \{0, 1\}$ に，$\omega^2 + \omega + 1 = 0$ をみたす “虚数”ω を付け加えて得られるのであった．今回は，$\mathbf{F}_2 = \{0, 1\}$ からはじめて 8 個の元からなる新たな体 $\mathbf{F}_8$ を構成する仕方を見てみる．基本的な考え方は，$\mathbf{F}_2$ に ω とは別の “虚数” を付け加えることによる．

$\mathbf{F}_2$ 上の既約な 3 次多項式は $x^3 + x + 1$ と $x^3 + x^2 + 1$ の 2 つであった．このうち，どちらを選んでも同じなのであるが，ここでは前者を選び，$\mathbf{F}_2$ に $\alpha^3 + \alpha + 1 = 0$ をみたす元を付け加える．$\mathbf{F}_2$ では $1 + 1 = 0$ が成り立つので，多項式の計算でも 2 倍すれば 0 になるし，足し算と引き算は同値になる．したがって，$\alpha^3 + \alpha + 1 = 0$ から $\alpha^3 = \alpha + 1$ が導かれ，α の 3 次以上の式は α^3 が現れるごとに $\alpha + 1$ に置き換えることによってすべて 2 次以下の式に変形することができる．言い換えると，$0, 1$ と α から加法・乗法を組み合わせて出来る数はすべて $k\alpha^2 + l\alpha + m$（$k, l, m = 0$ または 1) の形に表される．これら全体の集合が $\mathbf{F}_8$ である．すなわち，

$$\mathbf{F}_8 = \left\{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\right\}$$

$\mathbf{F}_8$ の 2 つの元の乗法は，例えば $(\alpha^2+1)\times(\alpha+1)$ を求めたければ，まずこれを展開し $(\alpha^2+1)\times(\alpha+1) = \alpha^3 + \alpha^2 + \alpha + 1$ を得る．そして $\alpha^3 = \alpha + 1$ を用いて，α^3 が現れるごとに $\alpha + 1$ に置き換え，

$$(\alpha^2 + 1) \times (\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1 = (\alpha + 1) + \alpha^2 + \alpha + 1 = \alpha^2 + (\alpha + \alpha) + (1 + 1) = \alpha^2$$

を得る．すなわち，$(\alpha^2 + 1) \times (\alpha + 1) = \alpha^2$ である．（これは，多項式 $(x^2 + 1)(x + 1)$ を $x^3 + x + 1$ で割ったときの余りが x^2 になることからも計算出来る．）

1 次の，$\mathbf{F}_8$ の乗法に関する表を手計算によって埋めよ．

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

次に，$\mathbf{F}_8$ についても，Fermat の小定理の類似が成り立つことをみる．そこで，$\alpha^1, \alpha^2, \ldots, \alpha^n, \ldots$ をつぎつぎに計算し $k\alpha^2 + l\alpha + m$ の形に直してみよう．

2 次の数を α の 2 次式の形に表せ．

$\alpha^0 = 1$

$\alpha^1 = \alpha$

$\alpha^2 =$

$\alpha^3 =$

$\alpha^4 =$

$\alpha^5 =$

$\alpha^6 =$

$\alpha^7 =$

α^n の形で表される数同士のの乗法は指数法則 $\alpha^m \times \alpha^n = \alpha^{m+n}$ により，指数の足し算として計算できる．そこで，上で得た結果をもとに $k\alpha^2 + l\alpha + m$ の形の数を α^n の形に直して乗法を計算することを考える．例えば次のように計算できる

$$(\alpha^2 + 1) \times (\alpha + 1) = \alpha^{\square} \times \alpha^{\square} = \alpha^{\square}$$

3 次の形の乗法の表を完成させよ．

$\times$	$\alpha^0 = 1$	$\alpha^1 = \alpha$	$\alpha^2 = \alpha^2$	$\alpha^3 = \square$	$\alpha^4 = \square$	$\alpha^5 = \square$	$\alpha^6 = \square$
$\alpha^0 = 1$							
$\alpha^1 = \alpha$							
$\alpha^2 = \alpha^2$							
$\alpha^3 = \square$							
$\alpha^4 = \square$							
$\alpha^5 = \square$							
$\alpha^6 = \square$							

【裏に続く】

4 次の元の逆元を求めよ.

a) α^2+1　　b) $\alpha^2+\alpha$　　c) α^5

5 次の元の逆元を求めよ.

a) $\dfrac{\alpha^2}{\alpha^2+\alpha}$　　b) $\dfrac{\alpha^2+\alpha+1}{\alpha^4}$　　c) $\dfrac{\alpha^5+\alpha^6}{\alpha^2+1}$

6 $f(x)=x^3+x+1$ を $\mathbf{F}_8$ 上で因数分解せよ.

[因数定理を用いる. $f(x)$ に α^k を次々に代入し, 0 になるものを見つければよい.]

7 元の個数がさらに 2 倍の $\mathbf{F}_{16}$ も同様に構成される. $\mathbf{F}_{16}$ は $\mathbf{F}_2$ に 4 次式 $\beta^4+\beta+1=0$ をみたす, α とは別の「数」β を付け加えて出来る. $\mathbf{F}_{16}$ に属する数は $k\beta^3+l\beta^2+m\beta+n$ $(k,l,m,n=0,1)$ の形に表される. $\mathbf{F}_8$ のと気と同様に $\beta^1,\beta^2,\ldots,\beta^n,\ldots$ を計算し β の 3 次以下の式の形に直して見てみよう.

$\beta^0=$

$\beta^1=$

$\beta^2=$

$\beta^3=$

$\beta^4=$

$\beta^5=$

$\beta^6=$

$\beta^7=$

$\beta^8=$

$\beta^9=$

$\beta^{10}=$

$\beta^{11}=$

$\beta^{12}=$

$\beta^{13}=$

$\beta^{14}=$

$\beta^{15}=$

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)