

前回までに、 $\mathbb{F}_2 = \{0, 1\}$ に加えて、それぞれ4個、8個の元からなる体 $\mathbb{F}_4$, $\mathbb{F}_8$ について詳しく調べた。元の個数がさらに2倍の $\mathbb{F}_{16}$ も同様に構成される。 $\mathbb{F}_{16}$ は $\mathbb{F}_2$ に4次式

$$\beta^4 + \beta + 1 = 0$$

をみたす、 ω や α とは別の「虚数」 β を付け加えて得られる。 β の4次以上の式は β^4 が現れるごとに $\beta + 1$ に置き換えることによってすべて3次以下の式に変形することができるので、 $\mathbb{F}_{16}$ に属する数は

$$k\beta^3 + l\beta^2 + m\beta + n \quad (k, l, m, n \text{ は } 0 \text{ または } 1)$$

の形に表される。いま、この多項式 $k\beta^3 + l\beta^2 + m\beta + n$ を “ $klmn$ ” と書き、これを2進数で表された整数と考える。例えば、 $\beta^3 + \beta + 1$ を 1011 と表し、これを2進数 $1011_{(2)}$ とみて、それを10進法で表し 11 を対応させる。すなわち、

$$\beta^3 + \beta + 1 \mapsto 1 \cdot \beta^3 + 0 \cdot \beta^2 + 1 \cdot \beta + 1 \mapsto 1011 \mapsto 1011_{(2)} = 11$$

1 以下の表を完成させよ。

指数 k	β^k	3次以下の式	2進法	10進法
0	β^0	1	1	1
1	β^1			
2	β^2			
3	β^3			
4	β^4			
5	β^5			
6	β^6			
7	β^7	$\beta^3 + \beta + 1$	1011	11
8	β^8			
9	β^9			
10	β^{10}			
11	β^{11}			
12	β^{12}			
13	β^{13}			
14	β^{14}			

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

2 前ページの表を並べ替え、以下の表を完成させよ。

10進法	2進法	3次以下の式	β^k	指数 k
1	1	1	β^0	0
2				
3				
4				
5				
6				
7				
8				
9				
10				
11	1011	$\beta^3 + \beta + 1$	β^7	7
12				
13				
14				
15				

この表を用いると、3次以下の式で表された $\mathbb{F}_{16}$ の2つの数のかけ算を、それぞれの数を β^k の形に表した上で、指数の足し算として計算し、それをまた β の3次以下の式に直すことで計算できる。

3 次のかけ算を、指数の足し算に直した上で計算させよ。

a) $(\beta^3 + \beta + 1)(\beta + 1) =$

b) $(\beta^3 + \beta^2 + 1)(\beta^2 + \beta + 1) =$

c) $(\beta^2 + \beta + 1)(\beta^2 + 1) =$

d) $(\beta^3 + \beta + 1)(\beta^3 + 1) =$

● Mathematica® を使ってやってみよう!

β の多項式 $f(\beta)$ を 3 次以下の式に直すことは, $f(\beta)$ を $\beta^4 + \beta + 1$ で割った余りを求めることに他ならない. しかし, 手計算で β の多項式を 3 次以下の式に直すのは大変なので, これを Mathematica® を用いて計算することを考える. 基本的には, 多項式の割り算である **PolynomialMod** を用いればよいが, 今の場合, $2 = 0$ であること (標数が 2 であること) も勘定に入れなければならない. そこで, 例えば β^7 を β の 3 次以下の式に直すには, 次のようにする.

```
PolynomialMod[b^7, b^4 + b + 1, Modulus -> 2]
```

(+ は Shift キーと Enter キーを同時に押し, コマンドを実行することを意味する.)

k をいろいろ変えて, β^k を一度に計算するには **Table** コマンドを使うとよい. このコマンドについての詳しい説明は, Mathematica® のヘルプと次のサイトを参照するとよい.

<https://www1.econ.hit-u.ac.jp/kawahira/courses/mathematica/03.pdf>

4 Mathematica のコマンド **PolynomialMod** と **Table** を用いて, β^k を計算せよ.

Mathematica には有限体の計算を実行できる “**Finite Fields**” というパッケージが含まれている. これを用いると問題 1 の表が簡単に作れる.

```
<< FiniteFields'
```

```
F16 = GF[2, {1, 1, 0, 0, 1}];
```

```
Table[{i, b^i,  
  ElementToPolynomial[Power[F16[{0, 1, 0, 0}], i], b] //  
  TraditionalForm,  
  BaseForm[  
    ElementToPolynomial[Power[F16[{0, 1, 0, 0}], i], b] /. b -> 2, 2],  
    ElementToPolynomial[Power[F16[{0, 1, 0, 0}], i], b] /. b -> 2},  
  {i, 1, 15}] // TableForm
```

ここで, Mathematica では多項式を昇べきの順に表示するのが標準となっていることに注意しておく. すなわち, $b^4 + b + 1$ は Mathematica では $1 + b + b^4$ と表示される. 上の $\text{GF}[2, \{1, 1, 0, 0, 1\}]$ 中の $\{1, 1, 0, 0, 1\}$ はこの慣習を反映して $1 + b + b^4$ を表している. また, **TraditionalForm** と指定することにより, 多項式を我々の慣れた降べきの順に表すこともできる.

QR-コードなどに実際に使われるのは $2^8 = 256$ 個の数からなる体 $\mathbb{F}_{256}$ である. この体は $\mathbb{F}_2$ に $g^8 + g^4 + g^3 + g^2 + 1 = 0$ をみたす虚数 g を付け加えて得られる体である. $\mathbb{F}_{256}$ について上の表と同じ表を作るには上の式を少し変更して次のようにすればよい. (すでに **FiniteFields** パッケージはロードされているとする.)

```
F256 = GF[2, {1, 0, 1, 1, 1, 0, 0, 0, 1}];
```

```
Table[{i, g^i,  
  ElementToPolynomial[Power[F256[{0, 1, 0, 0}], i], g] //  
  TraditionalForm,  
  BaseForm[  
    ElementToPolynomial[Power[F256[{0, 1, 0, 0}], i], g] /. g -> 2, 2],  
    ElementToPolynomial[Power[F256[{0, 1, 0, 0}], i], g] /. g -> 2},  
  {i, 1, 255}] // TableForm
```