

入学年度	学部	学 科	組	番 号	検	フリガナ
	B	1				氏名

有限体 \mathbb{F}_8 は \mathbb{F}_2 に $\alpha^3 + \alpha + 1 = 0$ をみたす数 α を加えて得られる数の体系であった。 \mathbb{F}_8 の元はすべて α の 2 次以下の多項式として表され (加法表示), 0 を除く 7 個の元は α^k ($0 \leq k \leq 6$) と表せる (乗法表示) のであった。 α の多項式 $P(\alpha)$ を 3 次以下の式に直すことは, $P(\alpha)$ を $\alpha^3 + \alpha + 1$ で割った余りを求めることに他ならない。これを Mathematica™ を用いて計算することを考える。基本は多項式の割り算である **PolynomialMod** を用いればよいが, 今の場合, $1 + 1 = 0$ という計算ルールのもとで計算することも勘定に入れなければならない。そこで, 例えば α^7 を α の 3 次以下の式に直すには, 次のようにすればよい。(α を Mathematica™ で入力するのが面倒であれば **a** を用いてもよい。)

```
PolynomialMod[ $\alpha^7, \alpha^4 + \alpha + 1, \text{Modulus} \rightarrow 2$ ] ⌘+↵
```

(⌘+↵) 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, α^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のこと。

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

まず, 次のようにすると結果が 1 行になって出てくる。

```
Table[PolynomialMod[ $\alpha^k, \alpha^3 + \alpha + 1, \text{Modulus} \rightarrow 2$ ], {k, 0, 7}] ⌘+↵
```

ここで, **TableForm** というコマンドを使うと, 結果が縦書きになる。

```
Table[PolynomialMod[ $\alpha^k, \alpha^3 + \alpha + 1, \text{Modulus} \rightarrow 2$ ], {k, 0, 7}] // TableForm ⌘+↵
```

さらに, 次のようにすると, α^k とその計算結果を並べて表示できる。

```
Table[{ $\alpha^k, \text{PolynomialMod}[\alpha^k, \alpha^3 + \alpha + 1, \text{Modulus} \rightarrow 2]$ }, {k, 0, 7}] // TableForm ⌘+↵
```

① 有限体 \mathbb{F}_{16} は \mathbb{F}_2 に $\beta^4 + \beta + 1 = 0$ をみたす数 β を加えて得られる。 \mathbb{F}_{16} の元はすべて β の 3 次以下の多項式として表される。上の計算を真似して, $k = 0, 1, 2, \dots, 15$ について β^k を β の 3 次以下の多項式として表示する表を作れ。

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[{k,  $\beta^k$ ,
ElementToPolynomial[Power[F16[{0, 1, 0, 0}], k],  $\beta$ ] // TraditionalForm,
BaseForm[
ElementToPolynomial[Power[F16[{0, 1, 0, 0}], k],  $\beta$ ]
/.  $\beta \rightarrow 2$ , 2],
ElementToPolynomial[Power[F16[{0, 1, 0, 0}], k],  $\beta$ ]
/.  $\beta \rightarrow 2$ ],
{k, 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, $\beta^4 + \beta + 1$ は Mathematica™ では $1 + \beta + \beta^4$ と表示される。上の $\text{GF}[2, \{1, 1, 0, 0, 1\}]$ の中の $\{1, 1, 0, 0, 1\}$ はこの Mathematica™ の慣習を反映して $1 + \beta + \beta^4$ を表している。また, **TraditionalForm** と指定することにより, 多項式をいつもの慣れた降べきの順に表すこともできる。

上の式で得られた結果の第 3 列目は β の 3 次以下の式の係数を並べて得た数を 2 進法表示した整数とみなしたものである。例えば, $\beta^2 + 1$ は $\beta^2 + 0\beta + 1$ とみて 101 とし, それを 2 進法表示した整数 101_2 とみたものである。そして, 第 4 列目はその整数を 10 進表示, すなわち普通の表示に直したものである。

② QR コードなどの実用上は $2^8 = 256$ 個の元を持つ有限体 \mathbb{F}_{256} が使われることが多い。 \mathbb{F}_{256} は \mathbb{F}_2 に $\gamma^8 + \gamma^4 + \gamma^3 + \gamma^2 + 1 = 0$ をみたす数 γ を加えて得られる。 \mathbb{F}_{256} の元はすべて γ の 7 次以下の多項式として表される。上の計算を真似して, $k = 1, 2, \dots, 255$ について γ^k を β の 7 次以下の多項式として表示する表を作れ。

BCH 符号

次に, 前々回に扱った, BCH 符号の符号多項式を Mathematica™ で計算してみる。

まず, (7, 4) 型の BCH 符号では, 情報語は 4bit であり, 0 から 15 までの数を 2 進法表示した 0000 から 1111 までの 16 語である。まず, これらをベクトルとみる。たとえば, 5 は 2 進法表示すると 0101 となるので, これをベクトル $(0, 1, 0, 1)$ と同一視する。さらに, これとベクトル $(x^3, x^2, x, 1)$ の内積をとると,

$$(0, 1, 0, 1) \cdot (x^3, x^2, x, 1) = 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1 \cdot 1 = x^2 + 1$$

となる。 [平面的ベクトル $\vec{a} = (a_1, a_2)$ と $\vec{b} = (b_1, b_2)$ の内積 $\vec{a} \cdot \vec{b}$ は $\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2$ と定義されるのであった。 n 次元ベクトルの内積も

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = a_1 b_1 + a_2 b_2 + \dots + a_n b_n$$

と定義される。]

まず、0から15までの数 n を4桁の2進法表示し、それを4次元ベクトルにする関数 f を定義する。

```
f[n_] := (  
  n1 = n;  
  vect = {};  
  While[n1 > 0,  
    vect = Prepend[vect, Mod[n1, 2]];  
    n1 = Quotient[n1, 2];  
  Return[PadLeft[vect, 4]];  
)
```

ここで例えば、

```
f[5].Table[x^(3 - k), {k, 0, 3}]
```

とすると、 $1 + x^2$ という答えが出るはずである。(表示の順序は昇べきの順になってしまう。)

情報語から符号語を作る方法を思い出したみと、多項式 $q(x)$ に対して $u(x)$ を

$$u(x) = (q(x))x^3 + (q(x)x^3 \text{ を } x^3 + x + 1 \text{ で割った余り})$$

と定義するのであった。Mathematica™ を用いて上で得た $1 + x^2$ から符号語を作るには、

```
Expand[(1 + x^2)*x^3] + PolynomialMod[(1 + x^2)*x^3, x^3 + x + 1,  
  Modulus -> 2]
```

とすればよい。 $x^2 + x^3 + x^5$ という答えが得られるはずである。ここまでの計算を自動化して表にするには次のようにする。

```
Table[{k, BaseForm[k, 2],  
  Expand[f[k].{x^3, x^2, x, 1}] // TraditionalForm,  
  Expand[f[k].{x^3, x^2, x, 1}*x^3] +  
  PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,  
  Modulus -> 2] // TraditionalForm},  
 {k, 0, 15}] // TableForm
```

さらに、最後の列の x の6次以下の多項式を7次元ベクトルに変えて表示するには次のようにすればよい。

```
Table[{k, BaseForm[k, 2],  
  Expand[f[k].{x^3, x^2, x, 1}] // TraditionalForm,  
  Expand[f[k].{x^3, x^2, x, 1}*x^3] +  
  PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,  
  Modulus -> 2] // TraditionalForm,  
  PadLeft[Reverse[CoefficientList[  
    Expand[f[k].{x^3, x^2, x, 1}*x^3] +  
    PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,  
    Modulus -> 2], x]  
  ], 7] // StandardForm},  
 {k, 0, 15}] // TableForm
```

3 前々回に作った符号多項式の表と、上で得られた結果と比較せよ。

ここで、最後の列の7次元ベクトルだけを取りだし、それらの間の Hamming 距離を計算し、表にしてみる。

```
words = Table[  
  PadLeft[Reverse[CoefficientList[  
    Expand[f[k].{x^3, x^2, x, 1}*x^3]  
    + PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,  
    Modulus -> 2], x]], 7],  
  {k, 0, 15}];  
Table[Table[HammingDistance[words[[i]], words[[j]]], {j, 1, 16}], {i, 1, 16}]
```

4 上の結果から16個の符号語間の Hamming 距離の最小値を求めよ。