

入学年度	学部	学科	組	番号	検	フリガナ	
	D	1				氏名	

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

$\mathbb{F}_2$  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、  $\mathbb{F}_2$  に  $\alpha^3 + \alpha + 1 = 0$  をみたす元  $\alpha$  を付け加える。  $\mathbb{F}_2$  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 にり、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、  $\alpha$  の 3 次以上の式は  $\alpha^3$  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  $\alpha$  から加法・乗法を組み合わせて出来る数はすべて

$$k\alpha^2 + l\alpha + m \quad (k, l, m = 0 \text{ または } 1)$$

の形に表され、これら全体の集合が  $\mathbb{F}_8$  である。すなわち、

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

$\mathbb{F}_8$  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、  $\alpha^3$  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  $x^2$  になることから計算出来る。)

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

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

次に、  $\mathbb{F}_8$  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、  $\alpha^1, \alpha^2, \dots, \alpha^n, \dots$  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  $\alpha$  の 2 次式の形に表せ。

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 =$$

$$\alpha^3 =$$

$$\alpha^4 =$$

$$\alpha^5 =$$

$$\alpha^6 =$$

$$\alpha^7 =$$

$\alpha^n$  の形で表される数同士の乗法は指数法則  $\alpha^m \times \alpha^n = \alpha^{m+n}$  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  $\alpha^n$  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。

$\times$	$\alpha^0 = 1$	$\alpha^1 = \alpha$	$\alpha^2 = \alpha^2$	$\alpha^3 =$ <input type="text"/>	$\alpha^4 =$ <input type="text"/>	$\alpha^5 =$ <input type="text"/>	$\alpha^6 =$ <input type="text"/>
$\alpha^0 = 1$							
$\alpha^1 = \alpha$							
$\alpha^2 = \alpha^2$							
$\alpha^3 =$ <input type="text"/>							
$\alpha^4 =$ <input type="text"/>							
$\alpha^5 =$ <input type="text"/>							
$\alpha^6 =$ <input type="text"/>							

4] 次の元の逆元を求めよ.

a)  $\alpha^2 + 1$

b)  $\alpha^2 + \alpha$

c)  $\alpha^5$

5] 次の元の逆元を求めよ.

a)  $\frac{\alpha^2}{\alpha^2 + \alpha}$

b)  $\frac{\alpha^2 + \alpha + 1}{\alpha^4}$

c)  $\frac{\alpha^5 + \alpha^6}{\alpha^2 + 1}$

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

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

7] 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  $\beta^4 + \beta + 1 = 0$  をみたとす,  $\alpha$  とは別の「数」 $\beta$  を付け加えて出来る.  $\mathbb{F}_{16}$  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.  $\mathbb{F}_8$  のと気と同様に  $\beta^1, \beta^2, \dots, \beta^n, \dots$  を計算し  $\beta$  の 3 次以下の式の形に直して見てみよう.

$$\beta^0 =$$

$$\beta^1 =$$

$$\beta^2 =$$

$$\beta^3 =$$

$$\beta^4 =$$

$$\beta^5 =$$

$$\beta^6 =$$

$$\beta^7 =$$

$$\beta^8 =$$

$$\beta^9 =$$

$$\beta^{10} =$$

$$\beta^{11} =$$

$$\beta^{12} =$$

$$\beta^{13} =$$

$$\beta^{14} =$$

$$\beta^{15} =$$