4 p 元体

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

今後，特に断りのない限り，p と書けばそれは素数を表すこととする．p を法とする合同類からなる剰余環 $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ については，前回の練習問題の内容を言い換えると，次の性質が成り立つ．

(1) $\mathbb{Z}/p\mathbb{Z}$ は零因子を持たない．
(2) $\overline{a} \neq \overline{0}$ ならば，$\overline{a}\,\overline{x} = \overline{1}$ をみたす $\overline{x}$ が存在する．
(3) $\overline{a} \neq \overline{0}$ ならば，任意の $\overline{b}$ に対して $\overline{a}\,\overline{x} = \overline{b}$ をみたす $\overline{x}$ が存在する．

例えば，$p = 7$ とすると，$2 \times 4 \equiv 1 \pmod 7$ であるから，$\overline{2} \times \overline{4} = \overline{1}$ と書くことができる．これは，$\overline{4}$ が $\overline{2}$ の「逆数」の役割を担っていることを意味する．一般に，$\overline{a}\,\overline{x} = \overline{1}$ をみたす $\overline{x}$ を $\overline{a}$ の**逆元**といい，$\overline{a}^{-1}$ と表す．たとえば，$\overline{4} = \overline{2}^{-1}$ である．もちろん $\overline{2} = \overline{4}^{-1}$ でもある．誤解の恐れがない場合は，$\overline{\ }$ をとって，「$\mathbb{Z}/7\mathbb{Z}$ において $2^{-1} = 4$ である」と表す．

1 $\mathbb{Z}/7\mathbb{Z}$ の 0 以外の各々の元について、その逆元を求めよ．

$1^{-1} =$　　$2^{-1} =$　　$3^{-1} =$　　$4^{-1} =$　　$5^{-1} =$　　$6^{-1} =$

普通，1 次方程式 $ax = b$ を解くには，両辺を a で割って，$x = \frac{b}{a}$ とするが，これは両辺に逆数 a^{-1} をかけ $x = ba^{-1}$ とすることと言い換えられる．$\mathbb{Z}/7\mathbb{Z}$ 内の方程式 $ax = b$ についても同様に，方程式の両辺に a の逆元 a^{-1} をかけて解くことができる．すなわち，$x = ba^{-1}$ が解である．例えば，$3x = 4$ であれば，この両辺に $3^{-1} = 5$ をかけて，$x = 4 \times 3^{-1} = 4 \times 5 = 20 = 6$ となる．実際，$x = 6$ のとき，$3x \equiv 3 \times 6 \equiv 18 \equiv 4 \pmod 7$ であり，確かに解である．

2 $p = 11$ として，$\mathbb{Z}/11\mathbb{Z}$ について考える．

a) $\mathbb{Z}/11\mathbb{Z}$ の 0 以外の各々の元に付いて，その逆元を求めよ．

$1^{-1} =$　　$2^{-1} =$　　$3^{-1} =$　　$4^{-1} =$　　$5^{-1} =$

$6^{-1} =$　　$7^{-1} =$　　$8^{-1} =$　　$9^{-1} =$　　$10^{-1} =$

b) $\mathbb{Z}/11\mathbb{Z}$ における次の方程式を解け．

a）$3x = 4$　　b）$5x = 10$　　c）$7x = 6$

一般に，p を法とする剰余環 $\mathbb{Z}/p\mathbb{Z}$ は $\mathbb{F}_p$ はとも表され，p **元体**と呼ばれる．混同の恐れがないときは，$\overline{\ }$ をとって簡単に表すので，

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$$

である．$\mathbb{F}_p$ は加法・減法について閉じている．さらに，$\mathbb{F}_p$ から $\overline{0} = 0$ を除いた集合

$$\mathbb{F}_p^{\times} = \{1, 2, \ldots, p-1\}$$

は乗法についても閉じており，上の性質 (2) により各元が逆元を持つことから，除法についても閉じていることが示される．

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「数の体系」であると考える．現代数学では，このような四則演算ができる集合は，それもまた一つの数の体系と見做す．$\mathbb{F}_p$ 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．このように四則演算が定義された集合は「**体**」（独：Korper，仏：corps，英：field）と呼ばれる．$\mathbb{F}_p$ は p 個の元（要素）をもつ体であることから p 元体と呼ばれる．

もう少し抽象的・形式的に正確に定義すると，体とは以下のように定義される．

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

有理数全体の集合 $\mathbb{Q}$，実数全体の集合 $\mathbb{R}$，複素数全体の集合 $\mathbb{C}$ はすべて体である．一方，整数全体の集合 $\mathbb{Z}$ は体ではない．剰余環 $\mathbb{Z}/m\mathbb{Z}$ は m が素数であるときに限り (K 4) をみたし，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は体である．

(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，空集合 ϕ や $\{0\}$ は体ではない．したがって，$\mathbb{F}_2 = \{0, 1\}$ が最も小さい体ということになる

3 $F = \{a + b\sqrt{2} \mid a, b$ は有理数 $\}$ とする．F は (K 9) をみたすことを示せ．(ヒント：「分母の有理化」)

（実際，F は $\mathbb{Q}(\sqrt{-2})$ とあらわされ，体であることが示される．このように，$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$，以外にも体はたくさんあることが知られている）．

【裏に続く】

高校数学で扱う多項式（= 整式）と同様，$\mathbb{F}_p$ の元を係数とする多項式（$\mathbb{F}_p$ 上の多項式と呼ぶ）についても，除法が可能である．すなわち，$\mathbb{F}_p$ 係数の多項式 $A(x)$，$B(x)$ について，

$$A(x) = B(x)Q(x) + R(x), \qquad \deg R(x) \leqq \deg Q(x)$$

をみたす $\mathbb{F}_p$ 係数の多項式 $Q(x)$ と $R(x)$ が求まる．また，高校数学の場合と同様に「剰余の定理」「因数定理」も同様に成り立つ．

例えば，$p = 5$ として，$\mathbb{F}_5$ 係数の多項式 $F(x) = x^2+2x+2$ を考える．いま，$F(1) = 1+2+2 = 5 \equiv 0 \pmod 5$, $F(2) = 4+4+2 = 10 \equiv 0 \pmod 5$ であるから，因数定理により，$x-1, x-2$ が $F(x)$ の因数であることがわかる．$F(x)$ の次数と，x^2 の係数を考慮して

$$x^2 + 2x + 2 = (x-1)(x-2) \qquad (\mathbb{F}_5 \text{ 係数の多項式として})$$

が成り立つ．これはまた $x^2 + 2x + 2 = (x+4)(x+3)$ とも表せることに注意．

4 次の $\mathbb{F}_5$ 係数の多項式を因数分解せよ．

a) $x^2 + x + 3$

b) $x^2 + 1$

c) $x^2 + x + 1$

d) $x^2 + x + 4$

e) $x^3 + x^2 + x + 1$

f) $x^4 - 1$

5 次の $\mathbb{F}_7$ 係数の多項式を因数分解せよ．

a) $x^2 + x + 1$

b) $x^2 + 1$

c) $x^2 - x + 1$

d) $x^6 - 1$

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)

6 $x^2 - 1$ を $\mathbb{F}_p$ 上の多項式とみる．p がどんな素数であっても，明らかに $x^2 - 1 = (x-1)(x+1)$ は成り立つ．ただし，$p = 2$ の場合は $-1 \equiv 1 \pmod 2$ なので，$\mathbb{F}_2$ 上では $x^2 - 1 = (x-1)^2$ である．以下では p は 2 以外の素数とする．

a) $\mathbb{F}_p^\times$ の元 a で，$a^2 = 1$ となるものは $a = 1$ または $a = p-1$ に限ることを示せ．

b) $\mathbb{F}_p^\times$ の元 a で，$a = a^{-1}$ となるものは $a = 1$ または $a = p-1$ に限ることを示せ．

c) $\mathbb{F}_p^\times$ の元は，$\{1\}, \{p-1\}$ および $\frac{p-3}{2}$ 個の $\{a, a^{-1}\}$ という形の集合に分割される．$p = 13$ の場合に $\mathbb{F}_{13}^\times$ を実際にこのように分割してみよ．

d) 【次週以降の話題に向けて】 p を法とする合同類から 0 の類を除いて作ったのかけ算の表の各行には 1 から $p-1$ までの数が各 1 回ずつ現れる．これより

$$1 \times 2 \times 3 \times \cdots \times (p-1) \equiv -1 \pmod p$$

であることを示せ．