

## 代数入門演習 (第一回 2011/04/11)

- $A = \{1, 2\}$ ,  $B = \{x, y\}$  とする。
  - $A$  から  $B$  への写像をすべて書け。
  - $B \times B$  から  $B$  への写像  $f$  で、

「任意の  $a, b, c \in B$  に対して  $f(a, f(b, c)) = f(f(a, b), c)$  が成り立つ」  
ものを一つ見つけよ。
- 以下のような写像の例を具体的に構成せよ。
  - 単射であって全射ではない。
  - 全射であって単射ではない。
- $A, B, C$  を集合とし、二つの写像  $f: A \rightarrow B$ ,  $g: B \rightarrow C$  を考える。
  - $f$  と  $g$  が共に単射ならば合成写像  $g \circ f$  も単射であることを示せ。
  - $f$  と  $g$  が共に全射ならば  $g \circ f$  も全射であることを示せ。
  - $g \circ f$  が全射ならば  $g$  は全射であることを示せ。
  - $g \circ f$  が単射ならば  $f$  は単射であることを示せ。
- 写像  $f: A \rightarrow B$ ,  $g: B \rightarrow A$  について  $f \circ g$ ,  $g \circ f$  が共に全単射であるとする。このとき  $f$  は全単射であることを示せ。
- 三つの写像  $f: A \rightarrow B$ ,  $g: A \rightarrow B$ ,  $h: B \rightarrow C$  を考える。  $h \circ f = h \circ g$  かつ  $h$  は単射であるとする。このとき  $f = g$  であることを示せ。
- 写像  $f: A \rightarrow B$  を考える。  $A$  の部分集合  $X, Y$  について  $f(X \cup Y) = f(X) \cup f(Y)$  が成り立つかどうかを考え、成り立つならばそれを証明し、成り立たないならば反例を一つ構成せよ。
- 写像  $f: A \rightarrow B$  を考える。  $A$  の部分集合  $X, Y$  について  $f(X \cap Y) = f(X) \cap f(Y)$  が成り立つかどうかを考え、成り立つならばそれを証明し、成り立たないならば反例を一つ構成せよ。
- $A = (a_{ij})$ ,  $B = (b_{ij})$ ,  $C = (c_{ij})$  をそれぞれ  $n$  次正方行列とする。  
 $(AB)C = A(BC)$  が成り立つことを示せ。

## 代数入門演習 (第二回 2011/04/18)

1. 同値関係の定義を書け。
2.  $n$  を自然数とし固定する。 $a, b \in \mathbb{Z}$  に対して、ある  $\ell \in \mathbb{Z}$  が存在して  $a - b = n\ell$  となるとき  $a \equiv b \pmod{n}$  と定める。この関係  $\equiv \pmod{n}$  は  $\mathbb{Z}$  上の同値関係であることを示せ。
3.  $M_n(\mathbb{C})$  を複素数を成分とする  $n$  次正方形行列全体の集合とする。 $A, B \in M_n(\mathbb{C})$  に対して、ある正則行列  $P$  があって  $B = P^{-1}AP$  となるとき  $A \sim B$  と書いて  $A$  と  $B$  は相似であるという。関係  $\sim$  は同値関係であることを示せ。
4.  $V$  を  $\mathbb{R}$  上のベクトル空間とし  $W$  をその部分空間とする。 $v, v' \in V$  に対して  $v - v' \in W$  のとき  $v \sim v'$  と書くことにする。このとき関係  $\sim$  は  $V$  上の同値関係であることを示せ。
5. 前問の記号を続けて用いる。 $v \sim v'$  かつ  $u \sim u'$  であるならば  $v + u \sim v' + u'$  であることを示せ。(これによって同値類の集合  $V/W$  に加法が矛盾なく定義される。)
6. 順序関係の定義を答えよ。
7. 全順序集合ではない順序集合の例を一つ挙げよ。
8.  $a, b \in \mathbb{N}$  に対して  $a \mid b$  とは  $a$  が  $b$  の約数であることとする。
  - (1) 関係  $\mid$  は  $\mathbb{N}$  の順序であることを示せ。
  - (2)  $A = \{1, 2, \dots, 10\}$  とし、 $A$  を上の関係で  $\mathbb{N}$  の順序部分集合と見る。このとき  $A$  の極大元、極小元をすべて求めよ。また  $A$  に最大元、最小元が存在するならば、それを答えよ。
9. 順序集合の最大元は極大元であることを示せ。
10. 整列集合の定義を書け。また整列集合の例、整列集合ではない全順序集合の例を書け。
11. ツェルメロの整列可能定理を書け。
12. ツォルンの補題を書け。

## 代数入門演習 (第三回 2011/04/25)

1.  $A = \{0, 1\}$  は通常の乘法によって半群になっている。このとき演算表 (乘法表) を

	0	1
0	0	0
1	0	1

のように書く。 $A = \{0, 1, -1\}$  も通常の乘法によって半群になっている。この半群の乘法表を書け。

2.  $\mathbb{Z}/3\mathbb{Z}$  に  $(a + 3\mathbb{Z}) + (b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z}$  で加法を定義する。このときの演算表を書け。また  $\mathbb{Z}/3\mathbb{Z}$  に  $(a + 3\mathbb{Z})(b + 3\mathbb{Z}) = ab + 3\mathbb{Z}$  で乘法を定義したときの演算表を書け。
3.  $A = \{a, b\}$  を半群とする。  $aa = b, ab = a$  とするとき  $ba, bb$  を求めよ。またこの半群の乘法表を書き、それがモノイドかどうかを判定せよ。
4.  $A$  の演算を任意の  $a, b \in A$  に対して  $ab = a$  で定める。このとき、この演算が結合法則を満たすことを示せ。また、これがモノイドであるかどうかを判定せよ。
5.  $P = \{(x, y) \mid x, y \in \mathbb{R}\}$  に次のような演算を定義する。

$$(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$$

- (1)  $P$  はこの演算でモノイドになることを示せ。また単位元を求めよ。
- (2)  $P$  の正則元を決定し、その逆元を求めよ。
6.  $Q = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$  に次のような演算を定義する。

$$(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1x_2, x_1y_2 + y_1z_2, z_1z_2)$$

- (1)  $Q$  はこの演算でモノイドになることを示せ。また単位元を求めよ。
- (2)  $Q$  は可換ではないことを示せ。
- (3)  $Q$  の正則元を決定し、その逆元を求めよ。
7. モノイドの単位元はただ一つであることを示せ。
8.  $\mathbb{N} \times \mathbb{N}$  に以下のような関係  $\leq$  を定める。  $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$  に対して
- (1)  $a < c$  ならば  $(a, b) \leq (c, d)$
- (2)  $a = c$  かつ  $b \leq d$  ならば  $(a, b) \leq (c, d)$

このとき  $\mathbb{N} \times \mathbb{N}$  上の関係  $\leq$  が順序であることを示せ。またこれが整列順序であることを示せ。(この順序を辞書式順序という。)

## 代数入門演習 (第四回 2011/05/02)

1. 以下のものは、半群、モノイド、群、そのいずれでもないか、最も適当なものをそれぞれ答えよ。

- (1) 集合  $\{0, 1\}$  で通常 addition を演算とするもの。
- (2) 集合  $\{0, 1\}$  で通常 multiplication を演算とするもの。
- (3) 集合  $\{-1, 1\}$  で通常 multiplication を演算とするもの。
- (4) 集合  $\{-1, 0, 1\}$  で通常 multiplication を演算とするもの。
- (5) 実数を成分とする  $n$  次正方形行列の全体で通常 addition を演算とするもの。
- (6) 実数を成分とする  $n$  次正方形行列の全体で通常 multiplication を演算とするもの。

2.  $R = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$  に次のような演算を定義する。

$$(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1x_2, x_1y_2 + y_1x_2, x_1z_2 + y_1y_2 + z_1x_2)$$

- (1)  $R$  はこの演算でモノイドになることを示せ。また単位元を求めよ。
  - (2)  $R$  の正則元を決定し、その逆元を求めよ。
3. 有理整数全体の集合  $\mathbb{Z}$  は乘法に関してモノイドである。 $\mathbb{Z}$  の正則元を決定せよ。
4.  $M_n(\mathbb{Z})$  で整数を成分とする  $n$  次正方形行列全体の集合を表す。 $M_n(\mathbb{Z})$  は通常行列の積によってモノイドとなる。 $M_n(\mathbb{Z})$  の正則元を決定せよ。(難しければ、まず  $n = 2$  として考えよ。)
5.  $A$  をモノイドとし  $U$  をその単数群とする。 $a, b \in A$  に対して、ある  $x \in U$  が存在して  $b = x^{-1}ax$  となるとき  $a \sim b$  と書く。このとき  $\sim$  は  $A$  上の同値関係であることを示せ。
6.  $G$  を群とする。写像  $f: G \rightarrow G$  を  $f(a) = a^{-1}$  で定めると、これは全単射であることを示せ。
7.  $G$  を群とする。 $g \in G$  を一つ固定して写像  $f: G \rightarrow G$  を  $f(a) = ag$  で定めると、これは全単射であることを示せ。
8. 問 7 で、 $G$  が群ではなくモノイドと仮定したときには  $f$  は全単射とは限らない。このような例を作れ。

## 代数入門演習 (第五回 2011/05/09)

1.  $\mathbb{C}$  から  $\mathbb{C}$  への写像  $f_i$  ( $i = 1, \dots, 6$ ) を次のように定める。

$$f_1(z) = z, \quad f_2(z) = 1 - z, \quad f_3(z) = \frac{1}{z},$$

$$f_4(z) = \frac{1}{1-z}, \quad f_5(z) = \frac{z-1}{z}, \quad f_6(z) = \frac{z}{z-1}$$

(0 で割ることがあっても気にしなくてよい。)

$G = \{f_i \mid i = 1, \dots, 6\}$  とおき、写像の合成を演算とする演算表を作れ。またそれが群になることを確認せよ。

ヒント. 例えば

$$f_3 \circ f_2(z) = f_3(f_2(z)) = f_3(1-z) = \frac{1}{1-z} = f_4(z)$$

なので  $f_3 f_2 = f_4$  である。

2.  $A = \{1, 2, \dots, n\}$  とする。  $A$  から  $A$  への全単射を  $A$  上の置換という。置換  $\sigma$  を

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

と表すことにする。

- (1)  $n = 3$  とするとき  $A$  上の置換を全て書け。
  - (2) 写像の合成で置換の積を定義する。  $n = 3$  として、このときの乗法表を作れ。
  - (3) 乗法表から気付くことを何でもよいので書け。
3.  $G$  を群とする。  $a \in G$  に対して、ある  $x \in G$  があって  $ax = x$  が成り立つならば  $a$  は  $G$  の単位元であることを示せ。
4.  $G$  を群とする。  $a, b \in G$  が  $ab = 1$  を満たすならば、  $b$  は  $a$  の逆元であることを示せ。
5.  $G$  を群とし  $a \in G$  を固定する。写像  $f : G \rightarrow G$  を  $f(x) = a^{-1}xa$  で定める。このとき、任意の  $x, y \in G$  に対して  $f(xy) = f(x)f(y)$ ,  $f(x^{-1}) = f(x)^{-1}$  であることを示せ。
6.  $G, H$  を群とし、写像  $f : G \rightarrow H$  を考え、任意の  $x, y \in G$  に対して  $f(xy) = f(x)f(y)$  が成り立つとする。このとき  $f(1_G) = 1_H$  であり、任意の  $x \in G$  に対して  $f(x^{-1}) = f(x)^{-1}$  であることを示せ。

## 代数入門演習 (第六回 2011/05/16)

1. 自然数  $n$  に対して  $n\mathbb{Z} = \{n\ell \mid \ell \in \mathbb{Z}\}$  とおけば、 $n\mathbb{Z}$  は加法群  $\mathbb{Z}$  の部分群であることを示せ。
2.  $G$  を群とし  $H$  をその部分群とする。 $a, b \in G$  に対して  $a^{-1}b \in H$  であるときに  $a \sim b$  と書くことにする。このとき  $\sim$  は  $G$  上の同値関係であることを示せ。
3.  $G$  を群とする。 $a \in G$  に対して  $C_G(a) = \{x \in G \mid ax = xa\}$  とおいてこれを  $G$  における  $a$  の中心化群という。
  - (1)  $C_G(a)$  は  $G$  の部分群であることを示せ。
  - (2)  $x, y \in G$  に対して以下の条件は同値であることを示せ。
    - (a)  $x^{-1}ax = y^{-1}ay$
    - (b)  $xy^{-1} \in C_G(a)$
    - (c)  $C_G(a)x = C_G(a)y$
  - (3)  $G$  が有限群であるとき  $\{x^{-1}ax \mid x \in G\}$  はちょうど  $|G|/|C_G(a)|$  個の元を含むことを示せ。
4. 2次元ユークリッド空間  $\mathbb{R}^2$  において

$$A = (1, 1), B = (-1, 1), C = (-1, -1), D = (1, -1)$$

とする。正方形  $ABCD$  を考え、それをそれ自身に移すような変換を考える。これは  $\{A, B, C, D\}$  上の置換と考えられる。例えば

$$x = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} \quad y = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}$$

はそのようなものである。

- (1) 正方形  $ABCD$  をそれ自身に移すような  $\{A, B, C, D\}$  上の置換をすべて書け。
- (2) (1) で求めたものはすべて  $x, y$  の積で書けることを確認せよ。(群の任意の元が  $x$  と  $y$  の積で書けるので  $\{x, y\}$  を群の生成系という。 $x, y$  を生成元という。)
- (3)  $x^4 = y^2 = 1, yx = x^3y$  を確認せよ。(生成元の間になり立つ関係を基本関係という。このとき  $G = \langle x, y \mid x^4 = y^2 = 1, yx = x^3y \rangle$  と書く。)
- (4)  $x, y$  の任意の積は  $x^i y^j$  ( $0 \leq i < 4, 0 \leq j < 2$ ) と書けることを示せ。
- (5) (1) で求めたものを  $\mathbb{R}^2$  上の一次変換と見て行列で表せ。ただし  $\mathbb{R}^2$  は列ベクトルの空間と見て、行列は左からかけるものとする。
- (6) 置換の積と (5) で求めた行列の積との関係を調べよ。

## 代数入門演習 (第七回 2011/05/23)

1. 第六回演習問 4 を答えよ。(この群を位数 8 の二面体群といい  $D_8$  で表す。)
2.  $\mathbb{R}$  上の一般線型群  $GL_n(\mathbb{R})$  を考え、 $O(n) = \{T \in GL_n(\mathbb{R}) \mid {}^tTT = E\}$  とおく。このとき  $O(n)$  は  $GL_n(\mathbb{R})$  の部分群であることを示せ。ただし  $E$  は単位行列を表し  ${}^tT$  は  $T$  の転置行列を表すものとする。(  $O(n)$  を  $n$  次直交群という。 )
3.  $S_n$  を集合  $\{1, \dots, n\}$  上の対称群とする。  $H = \{\sigma \in S_n \mid \sigma(1) = 1\}$  とおくと  $H$  は  $S_n$  の部分群であることを示せ。
4.  $n$  を自然数とし  $\mathbb{Z}/n\mathbb{Z}$  に次のように積を定義する。

$$(s + n\mathbb{Z})(t + n\mathbb{Z}) = st + n\mathbb{Z}$$

このとき次の間に答えよ。

(  $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \mid r \in \mathbb{Z}\}$ ,  $r + n\mathbb{Z} = \{qn + r \mid q \in \mathbb{Z}\}$  である。 )

- (1) 積が矛盾なく定義されていることを確認せよ。
  - (2)  $\mathbb{Z}/n\mathbb{Z}$  はこの積に関してモノイドであることを示せ。
  - (3) モノイド  $\mathbb{Z}/6\mathbb{Z}$ ,  $\mathbb{Z}/7\mathbb{Z}$ ,  $\mathbb{Z}/8\mathbb{Z}$  について、その単数群を求めよ。
5.  $G$  を群とする。  $a, b \in G$  に対して、ある  $x \in G$  があって  $b = x^{-1}ax$  となるとき  $a \sim b$  として、  $G$  上の関係  $\sim$  を定める。  $\sim$  は同値関係であることを示せ。(この関係  $\sim$  による同値類を  $G$  の共役類という。  $a$  を含む共役類に含まれる元数が  $|G|/|C_G(a)|$  であることが第六回問 3 で示されている。 )
  6.  $G$  を位数 8 の二面体群  $G = D_8 = \langle x, y \mid x^4 = y^2 = 1, yx = x^3y \rangle$  (第六回問 4) とし  $H = \langle y \rangle$  とする。  $G$  の元は  $x^i y^j$  ( $0 \leq i < 4, 0 \leq j < 2$ ) で表すものとする。
    - (1)  $H$  を集合として求めよ。
    - (2)  $G$  の  $H$  による左剰余類をすべて求めよ。
    - (3)  $G$  の  $H$  による右剰余類をすべて求めよ。
    - (4)  $K = \langle x^2 \rangle$  として、同様に左剰余類、右剰余類を求めよ。

## 代数入門演習 (第八回 2011/06/06)

1.  $R$  を整域とする。  $a, b, x \in R$  とし  $x \neq 0$  とする。このとき  $ax = bx$  ならば  $a = b$  であることを示せ。
2. 整域  $R$  が集合として有限集合であるならば  $R$  は体であることを示せ。
3. 整域であって体ではないものの例を一つ答えよ。
4.  $m, n$  を自然数とする。  $f: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  ( $f(a+m\mathbb{Z}) = a+n\mathbb{Z}$ ) が矛盾なく定義されるための  $m, n$  に関する必要十分条件を求めよ。 ( $\mathbb{Z}/m\mathbb{Z}$  の定義などは講義ノートなどを参照。)
5.  $R$  を環とする。  $e \in R$  で  $e^2 = e$  となるものを  $R$  のべき等元という。  $R$  が単位元  $1$  をもつとし、  $e$  が  $R$  のべき等元であるならば  $1 - e$  もべき等元であることを示せ。
6.  $R$  を単位元  $1$  をもつ環とする。  $x \in R$  に対してある自然数  $n$  があって  $x^n = 0$  であるとする (このような  $x$  をべき零元という)。このとき  $1 - x$  は正則元であることを示せ。
7.  $\mathbb{C}$  上 2 次の全行列環  $M(2, \mathbb{C})$  の元で、零元でも単位元でもないべき等元を一つ見つけよ。また零元でないべき零元を一つ見つけよ。
8.  $R_1, R_2$  を単位元をもつ環とする。集合としての直積  $R_1 \times R_2$  に以下のように加法と乗法を定める。

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2), \quad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

このとき、この演算によって  $R_1 \times R_2$  は環になる。これを  $R_1$  と  $R_2$  の直和といい  $R_1 \oplus R_2$  と書く。

- (1)  $R_1 \oplus R_2$  の零元と (乗法に関する) 単位元を求めよ。
  - (2)  $R_1 \oplus R_2$  の正則元と左 (右) 零因子を  $R_1, R_2$  の正則元と左 (右) 零因子を用いて決定せよ。
9. 可換環  $R = \mathbb{Z}/12\mathbb{Z}$  を考え  $S = 3\mathbb{Z}/12\mathbb{Z} = \{3a + 12\mathbb{Z} \mid a \in \mathbb{Z}\}$  とする。
    - (1)  $S$  の元をすべて書け。また  $S$  は  $R$  の部分環であることを示せ。
    - (2)  $R$  と  $S$  に単位元が存在するかどうか調べ、存在するならばそれを求めよ。



## 代数入門演習 (第九回 2011/6/13)

1.  $R$  を環とし  $a \in R$  とする。  $S = \{r \in R \mid ar = ra\}$  とおくと  $S$  は  $R$  の部分環であることを示せ。
2.  $R$  を環とする。  $C = \{r \in R \mid ar = ra \text{ for } \forall a \in R\}$  とおくと  $C$  は  $R$  の部分環であることを示せ。
3.  $R = M_2(\mathbb{R})$  は実数体  $\mathbb{R}$  上 2 次の全行列環とする。すなわち  $\mathbb{R}$  の元を成分とする 2 次の正方行列の全体である。

$$\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R \mid a \in \mathbb{Q}, b \in \mathbb{R}, c \in \mathbb{Q} \right\}$$

のような記号を用いる。以下の集合が  $R$  の部分環であるかどうかを判定せよ。

$$\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix}, \begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{Q} \\ 0 & \mathbb{R} \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ \mathbb{R} & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{R} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{R} \end{pmatrix}$$

4.  $R$  を単位元をもつ環とし  $a \in R$  を固定する。写像  $f : R \rightarrow R$  を  $f(x) = xa$  で定める。このとき次を示せ。
  - (1)  $f^{-1}(0) = \{0\}$  と  $f$  が単射であることは同値である。 ( $f^{-1}$  は写像ではない。  $f^{-1}(0) = \{x \in R \mid f(x) = 0\}$  である。)
  - (2)  $1 \in f(R)$  と  $f$  が全射であることは同値である。
5.  $m$  と  $n$  を互いに素な二つの自然数とする。すなわち、 $m$  と  $n$  の最大公約数が 1 であるとする。このとき  $f : \mathbb{Z}/mn\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$  を  $f(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$  で定める。ただし  $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$  は集合としての直積である。
  - (1)  $f$  が矛盾なく定義されていることを示せ。
  - (2) [中国剰余定理]  $f$  が単射であることを示せ。(このとき元数が等しい有限集合の間の単射なので、実は全単射となる。)
  - (3)  $m = 3, n = 4$  として、実際にすべての元の像を書くことによって  $f$  が全単射であることを確認せよ。
  - (4) 3 で割ると 1 余り、4 で割ると 2 余る最小の自然数を求めよ。

## 代数入門演習 (第十回 2011/06/20)

1.  $I$  を環  $R$  のイデアルとする。  $I$  は  $R$  の部分環であることを示せ。
2. 有理整数環  $\mathbb{Z}$  のイデアルを考える。  $n \in \mathbb{Z}$  に対して  $n\mathbb{Z} = \{n\ell \mid \ell \in \mathbb{Z}\}$  は  $\mathbb{Z}$  のイデアルであることを示せ。
3. 有理整数環  $\mathbb{Z}$  において、任意の  $n \in \mathbb{Z}$  に対して  $n\mathbb{Z} = \{n\ell \mid \ell \in \mathbb{Z}\}$  は  $\mathbb{Z}$  のイデアルである (問 2)。逆に  $\mathbb{Z}$  のイデアルはこの形のものに限ることを以下の方針で示せ。
  - $I$  を  $\mathbb{Z}$  のイデアルとする。  $I = \{0\}$  ならば  $I = 0\mathbb{Z}$  である。
  - $I$  を  $\mathbb{Z}$  の  $\{0\}$  でないイデアルとすると  $I$  は正の数を含む。
  - $n$  を  $I$  に含まれる最小の正の数とすると  $I = n\mathbb{Z}$  である。
4.  $R$  を環とし  $I, J$  をそのイデアルとする。このとき  $I \cap J, I + J$  も  $R$  のイデアルであることを示せ。ただし  $I + J = \{i + j \mid i \in I, j \in J\}$  である。また  $I \cup J$  はイデアルとは限らない。そのような例を具体的に一つ示せ。
5.  $m, n \in \mathbb{N}$  に対して  $m\mathbb{Z} \cap n\mathbb{Z}$  と  $m\mathbb{Z} + n\mathbb{Z}$  は何であるかを考察せよ。(分かりにくければ、まず  $m = 4, n = 6$  として考えよ。)
6.  $R$  を環とし  $a \in R$  とする。  $aR = \{ar \mid r \in R\}$  は  $R$  の右イデアルであることを示せ。また  $\{rar' \mid r, r' \in R\}$  は  $R$  のイデアルであるとは限らないことを反例をあげることによって示せ。
7.  $I$  を可換環  $R$  のイデアルとする。

$$\sqrt{I} = \{x \in R \mid \text{ある } n \in \mathbb{N} \text{ が存在して } x^n \in I\}$$

とおく。このとき  $\sqrt{I}$  は  $R$  のイデアルであることを示せ。(  $\sqrt{I}$  を  $I$  の根基イデアルという。 )

8.  $I$  を単位元をもつ環  $R$  のイデアルとする。このとき  $1 \in I$  であることと  $I = R$  であることは同値である。これを示せ。
9. 環  $R$  のイデアル  $I$  が極大イデアルであるとは、  $I$  を含む  $R$  のイデアルが  $I$  と  $R$  以外に存在しないことである。  
 $R$  を単位元をもつ環とする。  $R$  は少なくとも一つの極大イデアルをもつことを示せ。(Zorn の補題を用いる。)

## 代数入門演習 (第十一回 2011/06/27)

- $F = \mathbb{Z}/5\mathbb{Z}$  とすると、これは体である。多項式環  $F[x]$  で  $f(x) = x^5 + 2x + 3$  を  $g(x) = 2x^3 + 1$  で割った商と余りを求めよ。
- $K$  を体とする (分かりにくければ  $\mathbb{R}$  や  $\mathbb{C}$  と思ってもよい)。  $K$  上の一変数多項式環  $K[x]$  の任意のイデアルが単項イデアルであることを以下の方針で示せ。
  - $I$  を  $K[x]$  のイデアルとする。  $I = 0$  ならば  $I = 0K[x]$  である。
  - $I \neq 0$  とする。  $I$  に含まれる 0 でない多項式のうち、次数最小のものを一つ取り、これを  $h(x) = a_0 + a_1x + \cdots + a_nx^n$  ( $a_n \neq 0$ ) とする。
  - 任意の  $f(x) \in K[x]$  に対して  $f(x)h(x) \in I$  である。よって  $h(x)K[x] \subset I$  となる。
  - $f(x) \in I$  とする。  $f(x) = q(x)h(x)$  となる  $q(x) \in K[x]$  が存在する。よって  $f(x) \in h(x)K[x]$  となり  $h(x)K[x] \supset I$  となる。
- $f(x) = x^2 + 1, g(x) = x^3 - 1$  とする。  $f(x)a(x) + g(x)b(x) = 1$  となる  $a(x), b(x) \in \mathbb{R}[x]$  を見つけよ。 ( $\mathbb{Z}$  におけるユークリッドの互除法を参考にせよ。)
- 多項式としては等しくないが、それが定める関数が等しくなるような例を構成せよ。
- 実数体  $\mathbb{R}$  上の一変数多項式環  $\mathbb{R}[x]$  を考える。非負整数  $\ell$  に対して、 $\mathbb{R}[x]$  のイデアル  $I = x^{\ell+1}\mathbb{R}[x]$  を考え、剰余環  $\mathbb{R}[x]/I$  を考える。  $\mathbb{R}[x]/I$  の演算は、多項式の  $(\ell + 1)$  次以上の項を無視するものと考えてよい。
  - $\mathbb{R}[x]/I$  の単数を決定せよ。
  - $\mathbb{R}[x]/I$  のイデアルをすべて決定せよ。(難しければ、まず  $\ell = 1, 2$  あたりで考えよ。)
- $R$  を整域とし、多項式環  $R[x]$  を考える。  $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$  に対して  $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$  を  $f(x)$  の形式的微分という。
  - $f(x) = x^\ell, g(x) = x^m$  として微分公式  $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$  を示せ。(一般に  $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$  が成り立つが、証明はやや難しいので省略してよい。次の問題ではこれを用いてよい。)
  - $\alpha \in R$  が  $f(x)$  の重根であるとは  $(x - \alpha)^2 \mid f(x)$  であることとする。 $\alpha \in R$  が  $f(x)$  の重根であることと  $f(\alpha) = f'(\alpha) = 0$  であることは同値であることを示せ。

## 代数入門演習 (第十二回 2011/07/04)

1.  $F = \mathbb{Z}/7\mathbb{Z}$  とすると、これは体である。多項式環  $F[x]$  で  $f(x) = 2x^3 + x^2 + 1$  を  $g(x) = 3x^2 + 1$  で割った商と余りを求めよ。
2.  $K$  を有限体、すなわち  $|K| < \infty$  なる体、とし、その標数を  $p$  とする。 $f: K \rightarrow K$  ( $f(a) = a^p$ ) を考える。
  - (1) 任意の  $a, b \in K$  に対して  $f(a+b) = f(a) + f(b)$ ,  $f(ab) = f(a)f(b)$  となることを示せ。
  - (2)  $f$  は全単射であることを示せ。
3.  $f(x) = x^2 + x + 1$ ,  $g(x) = x - 1$  とする。剰余環  $\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$  において  $\bar{g}(x) = g(x) + f(x)\mathbb{Q}[x]$  の逆元を求めよ。
4.  $\alpha \in \mathbb{C}$  をある一変数有理数係数多項式の根の一つとする。 $f(x) \in \mathbb{Q}[x]$  を  $f(\alpha) = 0$  となる次数最小、かつ最高次係数が 1 である多項式とする。(これを  $\alpha$  の最小多項式という。)
  - (1)  $g(x) \in \mathbb{Q}[x]$  が  $g(\alpha) = 0$  をみたすならば  $g(x)$  は  $f(x)$  で割り切れることを示せ。
  - (2)  $\sqrt{2} + \sqrt{3}$  の最小多項式を求めよ。
5.  $\mathbb{R}^4$  に以下のように積を定める。

$$\begin{aligned} & (a_1, b_1, c_1, d_1)(a_2, b_2, c_2, d_2) \\ &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, a_1b_2 + a_2b_1 + c_1d_2 - c_2d_1, \\ & a_1c_2 + a_2c_1 + d_1b_2 - d_2b_1, a_1d_2 + a_2d_1 + b_1c_2 - b_2c_1) \end{aligned}$$

また加法は通常のベクトルのように対応する成分同士で行うこととする。

- (1)  $x(y+z) = xy + xz$  が成り立つことを確認せよ。(分配法則を確認するには  $(x+y)z = xz + yz$  も確認する必要がある。)
- (2) 乗法の結合法則などが確認でき、この演算で  $\mathbb{R}^4$  は環になる。(確認しなくてもよい。) これが非可換環であることを確認せよ。
- (3) この環の零元 (加法に関する単位元) と単位元 (乗法に関する単位元) を求めよ。
- (4)  $(a, b, c, d)(a, -b, -c, -d)$  を計算せよ。
- (5) (4) を用いて、この環が斜体であることを示せ。(これをハミルトンの四元数体といい  $\mathbb{H}$  という記号で書かれることが多い。)

## 代数入門演習 (第十三回 2011/07/11, 修正版)

1.  $K$  を体とする。多項式  $f(x) \in K[x]$  は写像  $f^* : K \rightarrow K, f^*(a) = f(a)$  を定める。このように多項式で定義される写像を多項式写像という。以下、 $K = \mathbb{Z}/2\mathbb{Z}$  とする。
  - (1)  $K$  上の次数が 1 以下の多項式をすべて書け。
  - (2) (1) の多項式が定める写像をすべて書け。
  - (3)  $K$  から  $K$  への任意の写像は多項式写像であることを確認せよ。(同じことが任意の有限体上で成り立つ。)
2.  $\mathbb{Q}$  上で多項式  $x^6 - 1$  を既約多項式の積に分解せよ。
3.  $K = \mathbb{Z}/5\mathbb{Z}$  上で多項式  $x^5 - 1$  を既約多項式の積に分解せよ。
4.  $R = \{A(a_0, a_1, \dots, a_n) \mid a_i \in \mathbb{R}\}$ , ただし

$$A(a_0, a_1, \dots, a_n) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n \\ 0 & a_0 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_0 & a_1 \\ 0 & 0 & \cdots & 0 & a_0 \end{pmatrix} \in M_{n+1}(\mathbb{R}),$$

とおく。

- (1)  $R$  は  $M_{n+1}(\mathbb{R})$  の部分環であることを示せ。
  - (2)  $R$  の単数を決定せよ。
  - (3)  $R$  のイデアルをすべて決定せよ。
- (ヒント.  $a_0, \dots, a_n$  のうち、一つの値だけが 1 で、他が 0 となるものを考え、それらの積を調べよ。)
5.  $K = \mathbb{Z}/5\mathbb{Z}$  とする。
    - (1)  $K$  の乗法表を書け。
    - (2)  $K$  の単数群を求め、単数群の元、それぞれに対して、その位数を求めよ。
    - (3)  $K$  の単数群の構造を考察せよ。
    - (4)  $K$  の任意の元  $a$  に対して  $a^5 - a = 0$  であることを確認せよ。
- (一般に、任意の素数  $p$  に対して、 $\mathbb{Z}/p\mathbb{Z}$  の任意の元  $a$  は  $a^p - a = 0$  をみたす。)