# 7　代数系 2

前回に引き続いて，代数系について学ぶ．今回は環(かん)と体(たい)について説明する．

## 7.1　環

環とは，$\mathbb{Z}$ のように，加法と乗法が定義された代数系である．正確な定義は次のようになる．

**定義 1.** 代数系 $(R, +, \cdot)$ が次の (i)–(vii) を満たすとき，$(R, +, \cdot)$ を**環**[*1]という．

(i) （**加法の結合律**）任意の $a, b, c \in R$ に対して，$(a + b) + c = a + (b + c)$ が成り立つ．
(ii) （**加法の交換律**）任意の $a, b \in R$ に対して，$a + b = b + a$ が成り立つ．
(iii) （**零元の存在**）ある元 $o \in R$ が存在して，任意の $a \in R$ に対して，$a + o = o + a = a$ が成り立つ．この $o$ を $(R, +, \cdot)$ の**零元**という．
(iv) （**加法に関する逆元の存在**）(iii) の零元 $o \in R$ について，任意の $a \in R$ に対して，ある元 $x \in R$ が存在して，$a + x = x + a = o$ が成り立つ．この $x$ を加法に関する $a$ の逆元といい，$-a$ で表す．
(v) （**乗法の結合律**）任意の $a, b, c \in R$ に対して，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ．
(vi) （**単位元の存在**）ある元 $e \in R$ が存在して，任意の $a \in R$ に対して，$a \cdot e = e \cdot a = a$ が成り立つ．この $e$ を $(R, +, \cdot)$ の（乗法に関する）**単位元**という．
(vii) （**分配律**）任意の $a, b, c \in R$ に対して，$a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ が成り立つ．

環 $(R, +, \cdot)$ が次の (viii) を満たすとき，$(R, +, \cdot)$ を**可換環**という．

(viii) （**乗法の交換律**）任意の $a, b \in R$ に対して，$a \cdot b = b \cdot a$ が成り立つ．

定義 1 の (i)–(iv) は，代数系 $(R, +)$ が可換群であることと同値である．

$(R, +, \cdot)$ が環のとき，演算を省略して $R$ は環であるということが多い．また，乗法の $\cdot$ も省略して，$a \cdot b$ を $ab$ と表す．

$(R, +, \cdot)$ が環であるとき，$(R, +)$ は群だから，零元はただ 1 つである．また，任意の $a \in R$ に対して，$a$ の加法に関する逆元もただ 1 つである．また，同様の議論によって，単位元もただ 1 つであることがわかる．$R$ の零元を 0 あるいは $0_R$ で表し，$R$ の単位元を 1 あるいは $1_R$ で表すことが多い．

群の場合と同様に，$a, b, c \in R$ に対して，結合律によって，$(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$ だから，括弧を省略してこれらをそれぞれ $a + b + c$, $abc$ と書く．4 個以上の元についても，括弧をどのように付けても演算の結果が等しいことが証明できるので，同様に括弧を省略して書く．

**注意 2.** 環の定義において，単位元の存在 (vi) を仮定しない場合もある．

**例 3.**　(1) $\mathbb{Z}$ と加法 $+$，乗法 $\cdot$ の組 $(\mathbb{Z}, +, \cdot)$ は可換環である．
(2) (1) と同様に，$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は可換環である．
(3) $n$ 次実行列全体を $M_n(\mathbb{R})$ で表す．$M_n(\mathbb{R})$ は環であるが，$n \geqq 2$ のとき可換環ではない．

[*1] 環を英語で ring というので，環を表すのに $R$ を用いている．

表 1　環 $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ の演算表

| $+$ | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ |
| $[1]$ | $[1]$ | $[2]$ | $[0]$ |
| $[2]$ | $[2]$ | $[0]$ | $[1]$ |

| $\cdot$ | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $[0]$ | $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ | $[2]$ |
| $[2]$ | $[0]$ | $[2]$ | $[1]$ |

環の重要な例として，$\mathbb{Z}/m\mathbb{Z}$ を考える．$m$ を正の整数とする．$\mathbb{Z}$ の上の同値関係 $\equiv_m$ を

$$x \equiv_m y \overset{\text{def}}{\iff} m \mid (x - y)$$

で定義する．集合 $\mathbb{Z}/m\mathbb{Z}$ は，同値関係 $\equiv_m$ による $\mathbb{Z}$ の商集合であった．したがって，

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\equiv_m = \{[0], [1], \ldots, [m-1]\}$$

となる．$\mathbb{Z}/m\mathbb{Z}$ の上に加法 $+$ を定義すると $(\mathbb{Z}/m\mathbb{Z}, +)$ が可換群になることは前回述べた．

前回と同様に，$\mathbb{Z}/m\mathbb{Z}$ の上の加法 $+$，乗法 $\cdot$ を次のように定義する．

$$[a] + [b] := [a + b], \quad [a] \cdot [b] := [ab].$$

これらが代表元 $a, b$ の選び方に依存しないことは前回と同様に証明される．このとき，代数系 $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ は可換環である．

**例 4.** $m = 3$ の場合を考える．環 $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ の演算 $+, \cdot$ は次のように計算される．

$$\begin{aligned}
&[0] + [0] = [0], && [0] + [1] = [1], && [0] + [2] = [2],\\
&[1] + [0] = [1], && [1] + [1] = [2], && [1] + [2] = [3] = [0],\\
&[2] + [0] = [2], && [2] + [1] = [3] = [0], && [2] + [2] = [4] = [1],\\
&[0] \cdot [0] = [0], && [0] \cdot [1] = [0], && [0] \cdot [2] = [0],\\
&[1] \cdot [0] = [0], && [1] \cdot [1] = [1], && [1] \cdot [2] = [2],\\
&[2] \cdot [0] = [0], && [2] \cdot [1] = [2], && [2] \cdot [2] = [4] = [1]
\end{aligned}$$

この結果を表にすると表 1 のようになる．

**例 5.** $m = 1$ の場合を考える．このとき，$\mathbb{Z}/1\mathbb{Z} = \{[0]\}$ となり，演算は次のようになる．

$$[0] + [0] = [0], \quad [0] \cdot [0] = [0].$$

この場合，零元と乗法に関する単位元は一致している．このように，ただ 1 つの零元のみからなる環を**零環**という．

環の基本的な性質として，次の定理が成り立つ．

**定理 6.** $R$ を環とする．任意の $a \in R$ に対し，次の等式が成り立つ．

(i) $0 \cdot a = a \cdot 0 = 0$.
(ii) $(-1) \cdot a = a \cdot (-1) = -a$.

**証明.** (i) $0 = 0 + 0$ である．分配律より，

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a.$$

$0 \cdot a$ の加法に関する逆元 $-(0 \cdot a) \in R$ が存在するから，

$$0 = 0 \cdot a + (-(0 \cdot a)) = (0 \cdot a + 0 \cdot a) + (-(0 \cdot a)) = 0 \cdot a + (0 \cdot a + (-(0 \cdot a))) = 0 \cdot a + 0 = 0 \cdot a.$$

よって，$0 \cdot a = 0$ である．$a \cdot 0 = 0$ も同様に証明される．
(ii) (i) の結果から，

$$\begin{aligned} -a = -a + 0 = -a + 0 \cdot a = -a + (1 + (-1)) \cdot a = -a + (1 \cdot a + (-1) \cdot a) \\ = -a + (a + (-1) \cdot a) = (-a + a) + (-1) \cdot a = 0 + (-1) \cdot a = (-1) \cdot a \end{aligned}$$

ゆえに，$(-1) \cdot a = -a$ である．$a \cdot (-1) = -a$ も同様に証明される． □

## 7.2 体

体とは，$\mathbb{Q}, \mathbb{R}$ のように，加減乗除が定義されている代数系である．体は環に条件を付け加えたものとして，次のように定義される．

**定義 7.** 代数系 $(F, +, \cdot)$ が零環でない可換環であるとする．次の条件が成り立つとき，$(F, +, \cdot)$ を**体**[*2]という．

(i) **（乗法に関する逆元の存在）** 0 でない任意の $a \in K$ に対して，ある $x \in K$ が存在して，$a \cdot x = x \cdot a = 1$ が成り立つ．この $x$ を $a$ の（乗法に関する）**逆元**といい，$a^{-1}, 1/a$ などで表す．

$(F, +, \cdot)$ を体とする．$F^\times := F - \{0\}$ とおくと，定義から，$(F^\times, \cdot)$ は可換群になる．逆に，体を次のように定義することもできる．

**定義 7′.** 代数系 $(F, +, \cdot)$ が次の (i)–(iii) を満たすとき，$(F, +, \cdot)$ を**体**という．

(i) $(F, +)$ は可換群である．
(ii) $F^\times := F - \{0\}$ とする．$(F^\times, \cdot)$ は可換群である．
(iii) **（分配律）** 任意の $a, b, c \in F$ に対して，$a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ が成り立つ．

**例 8.** (i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である．
(ii) $\mathbb{Z}$ は体ではない．実際，2 の逆元 $1/2$ は整数でなく，$\mathbb{Z}$ の元でない．

**注意 9.** 体の定義において，乗法が可換であることを除いたものを**斜体**という．ハミルトン[*3]の 4 元数体が代表的な例であるが，詳細は省略する．

環 $\mathbb{Z}/m\mathbb{Z}$ が体であるかどうかは $m$ の性質に依存する．例えば，例 4 で述べた $m = 3$ の場合，$\mathbb{Z}/3\mathbb{Z}$ が体であることは表 1 から直ちに分かる．実際，

$$[1] \cdot [1] = [1], \quad [2] \cdot [2] = [1]$$

[*2] 体を英語で field というので，体を表すのに $F$ を用いている．ドイツ語では Körper というので，体を $K$ で表すことも多い．
[*3] William Rowan Hamilton (1805–1865) : アイルランドの数学者・理論物理学者.

である．

一方，$m = 4$ の場合を考えると，$\mathbb{Z}/4\mathbb{Z}$ において，

$$[2] \cdot [0] = [0], \quad [2] \cdot [1] = [2], \quad [2] \cdot [2] = [4] = [0], \quad [2] \cdot [3] = [6] = [2]$$

となるから，$[2] \in \mathbb{Z}/4\mathbb{Z}$ は逆元を持たない．したがって，$\mathbb{Z}/4\mathbb{Z}$ は体ではない．

一般に，次の定理が成り立つ．

**定理 10.** 環 $\mathbb{Z}/m\mathbb{Z}$ が体であるための必要十分条件は，$m$ が素数であることである．

**証明.** $m = 1$ のとき，素数の定義[*4]から $m$ は素数でない．また，$\mathbb{Z}/m\mathbb{Z}$ は零環となるので体ではない．

$m$ が合成数のとき，$m$ の約数 $d$ で $1 < d < m$ となるものが存在する．このとき，$\mathbb{Z}/m\mathbb{Z}$ において $d$ は逆元を持たない．実際，$[d] \cdot [x] = [1]$ であるとすると，$dx - 1 = km$ となる整数 $k$ が存在する．ところが，$1 = dx - km$ となり，左辺は $d$ の倍数でないが，右辺は $d$ の倍数となり矛盾する．よって，$\mathbb{Z}/m\mathbb{Z}$ は体ではない．

$m$ が素数のとき，$\mathbb{Z}/m\mathbb{Z}$ が体になることを示す．$a$ を整数として，$[a] \neq [0]$ とする．このとき $a$ は $m$ の倍数ではない．写像 $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ を

$$f(x) = [a] \cdot x \quad (x \in \mathbb{Z}/m\mathbb{Z})$$

で定義する．

まず $f$ が単射であることを示す．$[b], [c] \in \mathbb{Z}/m\mathbb{Z}$ に対して $f([b]) = f([c])$ であるとすると，$[a] \cdot [b] = [a] \cdot [c]$ より，$[a(b-c)] = [0]$，すなわち，$a(b-c)$ は $m$ の倍数である．$m$ は素数であり，$a$ は $m$ の倍数でないから，$b - c$ は $m$ の倍数である．よって，$[b] = [c]$ となり，$f$ は単射である．

次に $f$ が全射であることを示す．$f$ が全射でないと仮定すると，$f$ の像 $\mathrm{Im}f = f(\mathbb{Z}/m\mathbb{Z})$ は $\mathrm{Im}f \subsetneqq \mathbb{Z}/m\mathbb{Z}$ を満たす．したがって，$|\mathrm{Im}f| < |\mathbb{Z}/m\mathbb{Z}|$ である．ところが，$f$ は単射だから，$|\mathrm{Im}f| = |\mathbb{Z}/m\mathbb{Z}|$ であり矛盾する．ゆえに，$f$ は全射である．

$f$ は全射だから，$f(x) = [1]$ となる $x \in \mathbb{Z}/m\mathbb{Z}$ が存在する．よって，$[a]$ は逆元 $x$ を持つ．以上で $\mathbb{Z}/m\mathbb{Z}$ が体になることが示された． □

**注意 11.** 上の証明では $\mathbb{Z}/m\mathbb{Z}$ において逆元を具体的に計算する方法は与えられていない．実際には，ユークリッドの互除法と呼ばれるアルゴリズムを用いることで逆元を高速に計算することができる．

$p$ が素数のときの $\mathbb{Z}/p\mathbb{Z}$ のように，要素の個数が有限個である体を**有限体**という．暗号理論や符号理論において，有限体は重要な役割を果たしている．

## 演習問題

1. 環 $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ の演算表を書け．
2. $F$ を体とする．$a, b \in F$ が $ab = 0$ を満たすならば，$a = 0$ または $b = 0$ であることを示せ．

[*4] 正の整数 $p$ が素数であるとは，$p \geqq 2$ であり，$p$ の正の約数が 1 と $p$ のみであることをいう．