4　代数系の基礎 (1) –整数の合同の概念 $\mathbb{Z}/m\mathbb{Z}$–

• 4-1 : 同値関係

集合 A, B に対して, その直積集合 $A\times B$ の部分集合を A から B への **二項関係** と呼ぶ. 二項関係 $R \subset A\times B$ の元は (a, b) のように順序のついた対である. 二項関係 R が与えられたとき, $(a, b) \in R$ であることを aRb あるいは $a \sim_R b$, または単に $a \sim b$ などと表す. 集合 A に対して, A から A 自身への二項関係を A 上の **関係** と呼ぶ.

例 4-1　(1) 集合 A を $A = \Big\{2, 4, 5, 8\Big\}$ とする. A 上の関係 R を

$$R = \Big\{(a, b) \in A \times A \mid a|b, \text{つまり}, a \text{ は } b \text{ を割り切る}. \Big\}$$

と定める. このとき, $R = \Big\{(2, 2), (2, 4), (2, 8), (4, 4), (4, 8), (5, 5), (8, 8)\Big\}$ である.

(2) 実数全体の集合 $\mathbb{R}$ に対して, $\mathbb{R}^2$ の部分集合 $R = \Big\{(x, y) \mid x \geq y\Big\}$, $R' = \Big\{(x, y) \mid x = y\Big\}$, $R'' = \Big\{(x, y) \mid x > y\Big\}$ などは $\mathbb{R}$ 上の関係である.

集合 A 上の関係 $\sim$ を考えよう.

(a) 任意の $a \in A$ に対して, $a \sim a$ が成り立つとき, 関係 $\sim$ は **反射律を満たす** という.
(b) 任意の $a, b \in A$ に対して, $a \sim b$ ならば $b \sim a$ が成り立つとき, 関係 $\sim$ は **対称律を満たす** という.
(c) 任意の $a, b, c \in A$ に対して, $a \sim b$ かつ $b \sim c$ ならば $a \sim c$ が成り立つとき, 関係 $\sim$ は **推移律を満たす** という.

例 4-2　(1) $\mathbb{R}$ 上の関係 $a \sim b$ であることを $a \geq b$ と定義する. このとき, 任意の $a \in \mathbb{R}$ に対して $a \geq a$ なので関係は反射律を満たす. この関係は対称律を満たさない. 例えば, $2 \geq 1$ だが, $1 \geq 2$ ではない. 任意の $a, b, c \in \mathbb{R}$ に対して, $a \geq b$ かつ $b \geq c$ ならば $a \geq c$ なので関係は推移律を満たす.

(2) $m > 0$ を整数とする. このとき, $\mathbb{Z}$ 上の関係 $a \sim b$ を「$a - b$ が m で割り切れる」と定義しよう. 任意の $a \in \mathbb{Z}$ に対して $a - a = 0$ なので反射律を満たす. また, 任意の $a, b \in \mathbb{Z}$ で $a \sim b$ ならば $a - b = mk$ となる整数 k がとれる. このとき $b - a = m \cdot (-k)$ とかけるので $b \sim a$ が成り立つ. すなわち対称律も満たす. 最後に, 任意の $a, b, c \in \mathbb{Z}$ で $a \sim b$ かつ $b \sim c$ であるとする. このとき, 整数 k, k' で $a - b = mk$, $b - c = mk'$ とかける. このとき,

$$a - c = a - b + b - c = mk + mk' = m(k + k')$$

だから $a - c$ も m で割り切れる. つまり $a \sim c$ だから推移律も満たされることがわかった.

集合 A 上の関係 R が反射律, 対称律, 推移律を満たしているとき, R を A 上の **同値関係** と呼ぶ. **例 4-2** (2) の関係は同値関係である.

レポート 4-1　集合 $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ 上の関係を次のように定義する.

$$(m, n) \sim (m', n') \quad \overset{\text{def}}{\Longleftrightarrow} \quad mn' = m'n$$

こうして定義された関係 $\sim$ は同値関係であることを示せ.

担当：茨城大学 情報科学領域　宮本 賢伍

- **4-2 : 商集合**

集合 A 上の同値関係 $\sim$ があるとき, $x \in A$ と同値関係にある A の元全体

$$\overline{x} = \left\{ y \in A \mid x \sim y \right\}$$

を x の **同値類** といい, x を **代表元** という. A の同値類を全て集めた集合族を A の同値関係 $\sim$ に関する **商集合** といい, $A/\sim$ で表す.

$$A/\sim := \left\{ \overline{x} \mid x \in A \right\}$$

命題 4.1. 集合 A 上の関係 $\sim$ が同値関係であるとする. このとき, 次が成立する.

(1) 任意の $x \in A$ に対して, $x \in \overline{x}$ である.
(2) A の元 $x, y \in A$ に対して, $\overline{x} = \overline{y}$ と $x \sim y$ は同値である.
(3) A の元 $x, y \in A$ に対して, $\overline{x} \neq \overline{y}$ であれば, $\overline{x} \cap \overline{y} = \varnothing$ である.

証明. (1) 関係 $\sim$ は A 上の同値関係であるから, 任意の $x \in A$ に対して $x \sim x$ である. よって $x \in \overline{x}$ となる.

(2) 任意の $x, y \in A$ をとる. $\overline{x} = \overline{y}$ であると仮定する. このとき, (1) より $y \in \overline{y} = \overline{x}$ なので $y \sim x$ である. 関係 $\sim$ は A 上の同値関係なので $x \sim y$ となる.

逆に $x \sim y$ であると仮定する. 2 つの集合 $\overline{x}$ と $\overline{y}$ が等しいことを示そう. 任意に $z \in \overline{x}$ をとれば, $x \sim z$ であるので対称律を用いて $z \sim x$ が成り立つ. 仮定から $x \sim y$ だから推移律を用いて $z \sim y$ となる. 対称律を用いて $y \sim z$ だから $z \in \overline{y}$ である. 従って $\overline{x} \subset \overline{y}$ である. x と y の役割を入れ替えれば同様にして $\overline{y} \subset \overline{x}$ が成り立つことがわかる. 以上で $\overline{x} = \overline{y}$ である.

(3) A の元 $x, y \in A$ に対して, $\overline{x} \neq \overline{y}$ であると仮定する. このとき, (2) より $x \sim y$ とはならない. $\overline{x} \cap \overline{y} \neq \varnothing$ と仮定すると, ある元 $z \in \overline{x} \cap \overline{y}$ がとれる. このとき, $x \sim z$ かつ $y \sim z$ が成り立つ. 対称律と推移律を用いれば $x \sim y$ である. これは仮定に反するので矛盾である. 従って $\overline{x} \cap \overline{y} = \varnothing$ である. □

- **4-3 : 整数に対する合同の概念**

自然数 m をひとつとる. このとき, $\mathbb{Z}$ 上の関係 $\sim$ を次のように定義しよう.

$$a \sim b \quad \overset{\text{def}}{\iff} \quad m \mid (a - b)$$

すなわち, $a - b$ が m の倍数であるときに $a \sim b$ と定義するのである. このとき, $a \sim b$ を

$$a \equiv b \pmod{m}$$

とかいて, a と b は **m を法として合同** という.

命題 4.2. $m \in \mathbb{N}$ を固定する. このとき, $\mathbb{Z}$ 上で定義される m を法として合同という関係は同値関係である.

証明. 任意の整数 $a \in \mathbb{Z}$ に対して, $a - a = 0$ なので $a \equiv a \pmod{m}$ である. よって反射律を満たす. また, 整数 $a, b \in \mathbb{Z}$ に対して, $a \equiv b \pmod{m}$ であれば $a - b = qm$ となる $q \in \mathbb{Z}$ が存在する. このとき, $b - a = (-q) \cdot m$ である. $-q \in \mathbb{Z}$ だから $b \equiv a \pmod{m}$ である. よって対称律を満たす. 最後に, 整数 $a, b, c \in \mathbb{Z}$ に対して, $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ であるとする. すると, $a - b = qm$, $b - c = rm$ となるような $q, r \in \mathbb{Z}$ が存在する. このとき,

$$a - c = (a - b) + (b - c) = pm + rm = (p + r)m$$

であり, $p + r \in \mathbb{Z}$ だから $a \equiv c \pmod{m}$ であるから推移律を満たす. 以上で m を法として合同という関係は $\mathbb{Z}$ 上の同値関係である. □

担当：茨城大学 情報科学領域　宮本 賢伍

$m \geq 2$ を自然数とする．$\mathbb{Z}$ 上の, m を法とする合同という同値関係による商集合を $\mathbb{Z}/m\mathbb{Z}$（あるいは $\mathbb{Z}_m$）とかく．この同値関係による整数 $a \in \mathbb{Z}$ の同値類を $\overline{a}$ とかくことにすると

$$\mathbb{Z}/m\mathbb{Z} = \left\{ \overline{a} \mid a \in \mathbb{Z} \right\}$$

である．

命題 4.3. $m \in \mathbb{N}$ を 2 以上とする．このとき, $\mathbb{Z}/m\mathbb{Z} = \left\{ \overline{0}, \overline{1}, \ldots, \overline{m-1} \right\}$ である．

証明. $A = \left\{ \overline{0}, \overline{1}, \ldots, \overline{m-1} \right\}$ とおく．明らかに $A \subset \mathbb{Z}/m\mathbb{Z}$ だから $\mathbb{Z}/m\mathbb{Z} \subset A$ を示せば良い．任意に $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ をとる．このとき, 除法の原理より

$$a = qm + r \quad (0 \leq r < m)$$

となるような $q, r \in \mathbb{Z}$ が存在する．このとき, $a - r = qm$ なので $a \equiv r \pmod{m}$ である．**命題 4.1** (2) より $\overline{a} = \overline{r}$ である．このとき, $0 \leq r < m$ だから $\overline{r} \in A$ である．よって $\mathbb{Z}/m\mathbb{Z} \subset A$ が従う．以上より $\mathbb{Z}/m\mathbb{Z} = \left\{ \overline{0}, \overline{1}, \ldots, \overline{m-1} \right\}$ である． □

- **4-4 : $\mathbb{Z}/m\mathbb{Z}$ 上の和と積, 写像の well-defined**

$m > 1$ を自然数とする．高校で学んだように, 整数 $a, b, c \in \mathbb{Z}$ に対して,

$$a \equiv b \pmod{m} \quad \Longrightarrow \quad a + c \equiv b + c \pmod{m}, \quad ac \equiv bc \pmod{m}$$

であった．$a \equiv b \pmod{m}$ であることは, a と b は m を法として合同という同値関係 $\sim$ で $a \sim b$ ということと同じであるから, 次の命題が成り立つということである．

命題 4.4. $m > 1$ を自然数とする．$\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/m\mathbb{Z}$ に対して

$$\overline{a} = \overline{b} \quad \Longrightarrow \quad \overline{a + c} = \overline{b + c}, \quad \overline{a \cdot c} = \overline{b \cdot c}$$

である．

証明. $\overline{a} = \overline{b}$ と仮定すれば, $a - b = qm$ となるような整数 $q \in \mathbb{Z}$ が存在する．このとき,

$$(a + c) - (b + c) = a - b = qm$$

なので $\overline{a + c} = \overline{b + c}$ である．積についても同様である． □

レポート 4-2　命題 4.4 の積についての主張を証明せよ．

商集合 $\mathbb{Z}/m\mathbb{Z}$ には, 通常の整数と同様に和と積を定めることができることを確認しよう．任意に $x, y \in \mathbb{Z}/m\mathbb{Z}$ をとる．このとき, x と y はある代表元 $a, b \in \mathbb{Z}$ を用いて, $x = \overline{a}$ および $y = \overline{b}$ と表せる．このとき,

$$x + y := \overline{a + b}, \quad x \cdot y := \overline{a \cdot b}$$

と定義する．このとき注意しなければならないのは, $x + y$ や $x \cdot y$ は代表元 a と b を用いて定義されていることである．代表元はさまざまな取り方があるのが普通である．例えば, $\mathbb{Z}/3\mathbb{Z}$ において $\overline{0} = \overline{3} = \overline{6} = \overline{9} = \cdots$ と $\overline{0}$ の代表元として 3 の倍数はなんでも取れる．しかし, これらは代表元の選び方に依存しない．実際, $x = \overline{a} = \overline{a'}$, $y = \overline{b} = \overline{b'}$ というように, それぞれを 2 つの代表元を用いて表すことができたとすると, **命題 4.4** により

$$\overline{a + b} = \overline{a + b'} = \overline{b' + a} = \overline{b' + a'} = \overline{a' + b'}$$
$$\overline{a \cdot b} = \overline{a \cdot b'} = \overline{b' \cdot a} = \overline{b' \cdot a'} = \overline{a' \cdot b'}$$

である．こうして，$x+y$, $x\cdot y\in\mathbb{Z}/m\mathbb{Z}$ が代表元の選び方に依らずに定まることが示された．

$\mathbb{Z}/m\mathbb{Z}$ 上の和や積のように，既に定められた概念から新たな概念を定める際に，元ある概念が複数の表示の仕方を持つ場合，それらのうち 1 つを用いて定義をすることは数学ではよくある．このとき，これから定めようとする概念が，どの表示を用いても 1 つに確定してしまうとき，その定義は **well-defined** であると表現する．日本語では「矛盾なく定義されている」と訳すが，数学の慣習で「well-defined である」と表現することが多い．

命題 4.5. $m>1$ を自然数とする．このとき，以下の性質が成り立つ．

(1) 任意の $x,y,z\in\mathbb{Z}/m\mathbb{Z}$ に対して，$(x+y)+z=z+(y+z)$ である．
(2) 任意の $x\in\mathbb{Z}/m\mathbb{Z}$ に対して，$x+\overline{0}=\overline{0}+x=x$ である．
(3) 任意の $x\in\mathbb{Z}/m\mathbb{Z}$ に対して，ある $y\in\mathbb{Z}/m\mathbb{Z}$ で $x+y=\overline{0}=y+x$ となるものが存在する．

証明. (1) 任意の $x,y,z\in\mathbb{Z}/m\mathbb{Z}$ に対して，$x=\overline{a}$, $y=\overline{b}$, $z=\overline{c}$ となるような $a,b,c\in\mathbb{Z}$ が存在する．このとき，

$$(x+y)+z=(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{b+c}=\overline{a}+(\overline{b}+\overline{c})=x+(y+z).$$

(2) 任意の $x\in\mathbb{Z}/m\mathbb{Z}$ に対して，$x=\overline{a}$ となるような $a\in\mathbb{Z}$ が存在する．このとき，

$$x+\overline{0}=\overline{a}+\overline{0}=\overline{a+0}=\overline{a}=x,\quad \overline{0}+x=\overline{0}+\overline{a}=\overline{0+a}=\overline{a}=x.$$

(3) 任意の $x\in\mathbb{Z}/m\mathbb{Z}$ に対して，$x=\overline{a}$ となるような $a\in\mathbb{Z}$ が存在する．このとき，$y=\overline{-a}\in\mathbb{Z}/m\mathbb{Z}$ を考えれば

$$x+y=\overline{a}+\overline{-a}=\overline{a-a}=\overline{0},\quad y+x=\overline{-a}+\overline{a}=\overline{-a+a}=\overline{0}.$$

以上で (1), (2), (3) が証明された． □

例 4-3　$m=5$ としよう．このとき，**命題 4.3** より $\mathbb{Z}/5\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$ である．このとき，$\mathbb{Z}/5\mathbb{Z}$ のそれぞれの元に対する和を計算すると，以下の表のようになる．ただし，1 列目の $\overline{a}$ と 1 行目の $\overline{b}$ の和 $\overline{a+b}$ をそれぞれ計算したものを表している．このように，演算の結果を表にしてまとめたものを **演算表** という．

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

レポート 4-3　$\mathbb{Z}/5\mathbb{Z}$ の積に関する演算表をかけ．

担当：茨城大学 情報科学領域　宮本 賢伍