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

• 3-1 : 同値関係

定義 3.1. 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 が与えられたとき, $(a, b) \in R$ であることを aRb , または単に $a \sim b$ と表す. $(a, b) \notin R$ のとき, $a \not\sim b$ 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 3-1 $A = \{2, 4, 5, 8\}$ とする. A 上の関係 R を

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

と定める. このとき, $R = \{(2, 2), (2, 4), (2, 8), (4, 4), (4, 8), (5, 5), (8, 8)\}$ である. 記号 $\sim$ を使えば $2 \sim 2$, $2 \sim 4$, $4 \sim 8$ などである.

定義 3.2. R を集合 A 上の関係とする.

- (a) 任意の $a \in A$ に対して, $a \sim a$ が成り立つとき, R 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, R 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, R は **推移律を満たす** という.

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.

命題 3.3. $m > 0$ を自然数とする. このとき, $\mathbb{Z}$ 上の関係 R を

$$a \sim b \stackrel{\text{def}}{\iff} a - b \text{ が } m \text{ で割り切れる}$$

と定義する. このとき, R は同値関係である.

証明. 関係 R が反射律, 対称律, 推移律を満たすことを確認すれば良い.

- (a) 任意の $a \in \mathbb{Z}$ に対して $a - a = 0$ なので, 関係 R は反射律を満たす.
 (b) 任意の $a, b \in \mathbb{Z}$ で $a \sim b$ ならば $a - b = mk$ となる整数 $k \in \mathbb{Z}$ 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. すなわち関係 R は対称律を満たす.
 (c) 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 $k, k' \in \mathbb{Z}$ 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 $a \sim c$ だから関係 R は推移律も満たす.

以上で, 関係 R は $\mathbb{Z}$ 上の同値関係である. □

定義 3.4. 集合 A 上の同値関係 R があるとき, $x \in A$ と **同値関係にある A の元全体の集合**

$$[x] := \{y \in A \mid x \sim y\}$$

を x の **同値類** といい, x を $[x]$ の **代表元** という. A の同値類を全て集めた集合族を

$$A/\sim := \{[x] \mid x \in A\}$$

で表し, これを A の同値関係 R による **商集合** という.

集合 A 上の同値関係があるとき, この同値関係は次の性質をみたすことがわかる.

命題 3.5. 集合 A 上の関係 R が同値関係であるとする. このとき, 次が成り立つ.

- (1) $\forall x \in A, x \in [x]$.
- (2) $\forall x \in A, \forall y \in A, [x] = [y] \iff x \sim y$.
- (3) $\forall x \in A, \forall y \in A, [x] \neq [y] \iff [x] \cap [y] = \emptyset$.

● 3-2 : 整数に対する合同の概念

自然数 m に対して, $\mathbb{Z}$ 上の関係 R を

$$a \sim b \stackrel{\text{def}}{\iff} a - b \text{ が } m \text{ で割り切れる}$$

と定義すれば, **命題 3.3** によって R は同値関係となった. 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. $a \equiv b \pmod{m}$ であるとき, ある $k \in \mathbb{Z}$ が存在して $a - b = km$ とできるということなので, これは

$$\text{「} a \text{ を } m \text{ で割った余り} \text{」} = \text{「} b \text{ を } m \text{ で割った余り} \text{」}$$

ということを述べていることに注意しよう. 整数 $a \in \mathbb{Z}$ に対して, $a \in \mathbb{Z}$ の同値類は

$$[a] = \{a + mk \mid k \in \mathbb{Z}\}$$

で与えられる. なぜならば, 任意の $x \in [a]$ に対して, $a - x = mk$ となる $k \in \mathbb{Z}$ が存在するので, $x = a - mk$ となるからである. $\mathbb{Z}$ 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 $\mathbb{Z}_m$) で表す. すなわち,

$$\mathbb{Z}/m\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\}$$

である.

命題 3.6. $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$ が成り立つ.

証明. $A = \{[0], [1], \dots, [m-1]\}$ 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 $[a] \in \mathbb{Z}/m\mathbb{Z}$ 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. すると, $a - r = qm$ なので $a \equiv r \pmod{m}$ である. **命題 3.5** (2) より $[a] = [r]$ である. このとき, $0 \leq r < m$ だから $[r] \in A$ である. よって $\mathbb{Z}/m\mathbb{Z} \subset A$ が従う. 以上より $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$ となることが示された. $\square$

つまり, **命題 3.6** は $\mathbb{Z}/m\mathbb{Z}$ の代表元として $0, 1, \dots, m-1$ を選べば十分であることを述べている.

例 3-2 $m = 3$ とする. **命題 3.6** によって, $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ である. **命題 3.5** と合わせると

- $[0] = \{3k \mid k \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\} = [-6] = [-3] = [3] = [6] = \dots$
- $[1] = \{3k + 1 \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\} = [-5] = [-2] = [4] = [7] = \dots$
- $[2] = \{3k + 2 \mid k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\} = [-4] = [-1] = [5] = [8] = \dots$

などのように, 代表元の取り方には自由度がある.

• 3-3 : $\mathbb{Z}/m\mathbb{Z}$ 上の和と積の定義

$\mathbb{Z}/m\mathbb{Z}$ には, 和と積を定義することができる. そのために, $m = 3$ の場合で観察しておこう.

まず, 加法について考える. 例えば, $\mathbb{Z}/3\mathbb{Z}$ において, $22 \in [1]$ と $17 \in [2]$ について

$$22 + 17 = 39 \in [39] = [0]$$

となる. 一般に, $a \in [1], b \in [2]$ をとれば, ある整数 $k, k' \in \mathbb{Z}$ を用いて $a = 3k + 1, b = 3k' + 2$ と表すことができるので,

$$a + b = 3k + 1 + 3k' + 2 = 3(k + k' + 1) \in [3(k + k' + 1)] = [0]$$

である. これを

$$[1] + [2] = [0]$$

と表すことにしよう. この $+$ は通常の和ではなく, あくまで $\mathbb{Z}/3\mathbb{Z}$ における和 (すなわち, 同値類に属する全ての元について, この関係が成り立つという意味の記号) である. とところで, $[0] = [3]$ なので, 上の関係は

$$[1] + [2] = [1 + 2] = [0]$$

ということになる.

また, 積についても考察すると

$$ab = (3k + 1)(3k' + 2) = 9kk' + 6k + 3k' + 2 = 3(3kk' + 2k + k') + 2 \in [3(3kk' + 2k + k') + 2] = [2]$$

であるから,

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

が成り立っている.

そこで, $\mathbb{Z}/m\mathbb{Z}$ における和 $+$ と積 $\cdot$ を $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$ に対して,

$$\text{(和)} \quad [a] + [b] := [a + b]$$

$$\text{(積)} \quad [a] \cdot [b] := [a \cdot b]$$

と定義すると良さそうである. このとき注意しなければならないのは, 和 $+$ や積 $\cdot$ は代表元 a と b を用いて定義しようとしていることである. 例えば, $\mathbb{Z}/3\mathbb{Z}$ において $[0] = [3] = [6] = [9] = \dots$ と $[0]$ の代表元として 3 の倍数はなんでも取れる. 従って, この定義を正当化するには, 次の疑問を解決しなければならない.

m を自然数とする. $\mathbb{Z}/m\mathbb{Z}$ において, $[a] = [a'], [b] = [b']$ であるとする. このとき, 常に

$$[a + b] = [a' + b'], \quad [ab] = [a'b']$$

が成り立つだろうか.

命題 3.7. $\forall [a] \in \mathbb{Z}/m\mathbb{Z}, \forall [b] \in \mathbb{Z}/m\mathbb{Z}, \forall [c] \in \mathbb{Z}/m\mathbb{Z},$

$$[a] = [b] \implies [a + c] = [b + c], \quad [a \cdot c] = [b \cdot c]$$

である.

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

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

なので $[a + c] = [b + c]$ である. 積についても同様である. □

命題 3.7 によって、先の疑問の答えは「成り立つ」となることがわかる。実際、 $[a] = [a']$, $[b] = [b']$ 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、命題 3.7 より

$$[a + b] = [a + b'] = [b' + a] = [b' + a'] = [a' + b']$$

$$[a \cdot b] = [a \cdot b'] = [b' \cdot a] = [b' \cdot a'] = [a' \cdot b']$$

である。こうして、 $\mathbb{Z}/m\mathbb{Z}$ の和 $+$ と積 $\cdot$ が代表元の選び方に依らずに定まることが示された*1。ここで定義した $\mathbb{Z}/m\mathbb{Z}$ の和 $+$ を **剰余の和**, 積 $\cdot$ を **剰余の積** と呼ぶ。

例 3-3 $m = 5$ としよう。このとき、命題 3.6 より $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$ である。このとき、 $\mathbb{Z}/5\mathbb{Z}$ のそれぞれの元に対する剰余の和を計算すると、以下の表のようになる。ただし、1 列目の $[a]$ と 1 行目の $[b]$ の和 $[a + b]$ 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。

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

また、 $\mathbb{Z}/5\mathbb{Z}$ のそれぞれの元に対する剰余の積の演算表は次のようになる。

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

*1 $\mathbb{Z}/m\mathbb{Z}$ 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。

小テスト 3-1 以下に示す $\mathbb{N}$ 上の関係 R が反射律, 対称律, 推移律のうち成り立っているものを全て選べ.

- (1) $x \sim y$ を $x \leq y$ と定める.
- (2) $x \sim y$ を $x + y$ が 3 で割り切れる.
- (3) $R = \{(n, n) \mid n \in \mathbb{N}\}$
- (4) $R = \{(x, y) \mid x < y, x, y \in \mathbb{N}\}$
- (5) $R = \{(x, y) \mid |x - y| = 3, x, y \in \mathbb{N}\}$

小テスト 3-2 $\mathbb{Z}/6\mathbb{Z}$ における和と積の演算表を完成させよ. ただし, $a_i, b_i \in \{0, 1, 2, 3, 4, 5\}$ ($i = 1, 2, 3, 4, 5$) で答えること.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	$[a_5]$	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	$[a_1]$	[1]
[3]	[3]	[4]	$[a_4]$	$[a_3]$	$[a_2]$	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	$[b_1]$	$[b_2]$	[4]
[3]	[0]	[3]	$[b_3]$	$[b_4]$	[0]	[3]
[4]	[0]	[4]	$[b_5]$	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

演習問題 3-1 集合 $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ 上の関係を次のように定義する.

$$(m, n) \sim (m', n') \stackrel{\text{def}}{\iff} mn' = m'n$$

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.

演習問題 3-2 $\mathbb{Z}/7\mathbb{Z}$ の和と積における演算表をかけ.

演習問題 3-3 集合 $\{0, 1\}$ 上の関係全体の集合を $\mathcal{R}$ とおく.

- (1) $|\mathcal{R}|$ を求めよ.
- (2) $\mathcal{R}$ のうち, 同値関係であるものをすべて与えよ.

● 3-A : 命題 3.5 の証明

命題. 集合 A 上の関係 R が同値関係であるとする. このとき, 次が成り立つ.

- (1) $\forall x \in A, x \in [x]$.
- (2) $\forall x \in A, \forall y \in A, [x] = [y] \iff x \sim y$.
- (3) $\forall x \in A, \forall y \in A, [x] \neq [y] \iff [x] \cap [y] = \emptyset$.

証明. (1) 関係 R 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 $x \in [x]$ となる.

(2) 任意の $x, y \in A$ をとる. $[x] = [y]$ であると仮定する. このとき, (1) より $y \in [y] = [x]$ なので $y \sim x$ である. 関係 R 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 $[x]$ と $[y]$ が等しいことを示そう. 任意に $z \in [x]$ 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 $z \in [y]$ である. 従って $[x] \subset [y]$ である. x と y の役割を入れ替えれば同様にして $[y] \subset [x]$ が成り立つことがわかる. 以上で $[x] = [y]$ である.

(3) A の元 $x, y \in A$ に対して, $[x] \neq [y]$ であると仮定する. このとき, (2) より $x \sim y$ とはならない. $[x] \cap [y] \neq \emptyset$ と仮定すると, ある元 $z \in [x] \cap [y]$ 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 $[x] \cap [y] = \emptyset$ である. また, $[x] \cap [y] = \emptyset$ であれば, $[x] \neq [y]$ は明らかである. □

命題 3.5 が述べているのは, 集合 A 上に同値関係が与えられたとき, その同値関係による同値類によって A が集合として分割されている, ということである.