

3 2 項関係と同値関係

• 3-1 : 2 項関係

定義 3.1. A, B を集合とする. $A \times B$ の部分集合 $R \subset A \times B$ を, A から B への **2 項関係 (binary relation)** という. 特に $A = B$ のとき, A 上の 2 項関係という. $(a, b) \in R$ であることを $a R b$ と書き, a と b は R によって **関係する** という. $(a, b) \notin R$ のときは $a \not R b$ と書く.

例 3-1 以下はいずれも 2 項関係の典型例である.

- (1) **大小関係** : $R_{\leq} = \{(a, b) \in \mathbb{R}^2 \mid a \leq b\}$ は \mathbb{R} 上の 2 項関係である. 例えば $2 \leq 5$ は $(2, 5) \in R_{\leq}$ を意味する.
- (2) **整除関係** : 自然数 a, b に対して, $a \mid b$ とは, ある $k \in \mathbb{N}$ が存在して $b = ka$ と書けることをいう. 例えば $3 \mid 12, 2 \mid 8, 4 \nmid 7$ である.
- (3) **合同関係** : 整数 a, b と正整数 n に対して, $n \mid (a - b)$ であるとき, $a \equiv b \pmod{n}$ と書く. これを「 a と b は n を法として **合同**」という. 例えば $7 \equiv 1 \pmod{3}, -5 \equiv 1 \pmod{3}, 10 \equiv 4 \pmod{6}$ である.

2 項関係には次の基本的な性質がある.

定義 3.2. A 上の 2 項関係 R について,

- (a) **反射的 (reflexive)** : 任意の $a \in A$ に対して $a R a$ が成り立つ.
- (b) **対称的 (symmetric)** : $a R b$ ならば $b R a$ が成り立つ.
- (c) **反対称的 (antisymmetric)** : $a R b$ かつ $b R a$ ならば $a = b$ が成り立つ.
- (d) **推移的 (transitive)** : $a R b$ かつ $b R c$ ならば $a R c$ が成り立つ.

例 3-2 各 2 項関係についての性質を確認する (✓ : 満たす).

2 項関係	反射的	対称的	反対称的	推移的
\leq (\mathbb{R} 上)	✓		✓	✓
$<$ (\mathbb{R} 上)			✓	✓
\mid (\mathbb{N} 上の整除)	✓		✓	✓
$\equiv \pmod{n}$ (\mathbb{Z} 上)	✓	✓		✓
$=$ (集合 A 上)	✓	✓	✓	✓

例えば, \leq が対称的でないことは「 $2 \leq 3$ であるが $3 \not\leq 2$ 」から確認できる. $<$ が反射的でないことは $1 \not< 1$ から確認できる. $\equiv \pmod{n}$ が反対称的でないことは, $n = 3$ のとき $1 \equiv 4 \pmod{3}$ かつ $4 \equiv 1 \pmod{3}$ であるが $1 \neq 4$ から確認できる.

• 3-2 : 同値関係

定義 3.3. A 上の 2 項関係 \sim が **反射的・対称的・推移的** をすべて満たすとき, \sim を A 上の **同値関係 (equivalence relation)** という.

例 3-3

- (1) **合同関係 $\equiv \pmod{n}$ は \mathbb{Z} 上の同値関係** である. 各性質を確認してみよう.

- (i) (反射的) 任意の $a \in \mathbb{Z}$ に対して $n \mid (a - a) = 0$ より $a \equiv a \pmod{n}$.
- (ii) (対称的) $a \equiv b \pmod{n}$ ならば $n \mid (a - b)$, よって $n \mid -(a - b) = b - a$ より $b \equiv a \pmod{n}$.
- (iii) (推移的) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ ならば $n \mid (a - b)$ かつ $n \mid (b - c)$, よって $n \mid (a - b) + (b - c) = a - c$ より $a \equiv c \pmod{n}$.

(2) 平面 \mathbb{R}^2 上の直線の集合を \mathcal{L} とする. 「 $l_1 = l_2$ または $l_1 \parallel l_2$ 」(l_1 と l_2 は一致するか平行) という関係は \mathcal{L} 上の同値関係である.

(3) 整数全体 \mathbb{Z} 上で「 a と b は偶奇性が等しい」という関係は同値関係である ($a - b$ が偶数, すなわち $\equiv \pmod{2}$).

例 3-4 次の関係は同値関係ではない.

- (1) \mathbb{R} 上の $<$ は, $1 < 1$ が成り立たないので **反射的でない**.
- (2) \mathbb{N} 上の整除関係 \mid は, $2 \mid 6$ であるが $6 \nmid 2$ なので **対称的でない**.
- (3) \mathbb{Z} 上の 「 $|a - b| \leq 1$ 」 は, $1R2$ かつ $2R3$ であるが $|1 - 3| = 2 > 1$ より $1R/3$ なので **推移的でない**.

● 3-3 : 同値類と商集合

定義 3.4. \sim を集合 A 上の同値関係とする. $a \in A$ に対して,

$$[a]_{\sim} = \{b \in A \mid a \sim b\}$$

を a の **同値類 (equivalence class)** といい, a をその **代表元** という (単に $[a]$ と書くことも多い). 同値類の全体からなる集合

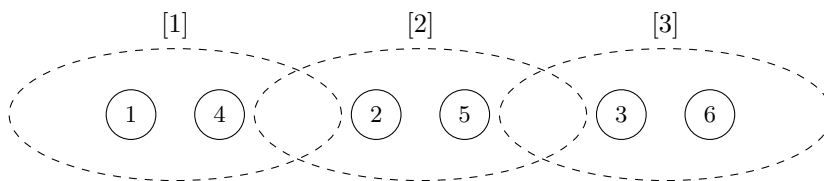
$$A/\sim = \{[a] \mid a \in A\}$$

を **商集合 (quotient set)** という.

例 3-5 $A = \{1, 2, 3, 4, 5, 6\}$ 上の合同関係 $\equiv \pmod{3}$ の同値類を求める.

$$[1] = \{b \in A \mid b \equiv 1 \pmod{3}\} = \{1, 4\}, \quad [2] = \{b \in A \mid b \equiv 2 \pmod{3}\} = \{2, 5\}, \\ [3] = \{b \in A \mid b \equiv 0 \pmod{3}\} = \{3, 6\}.$$

なお, $[4] = [1]$, $[5] = [2]$, $[6] = [3]$ である. 商集合は $A/\sim = \{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$ である.



定理 3.5. \sim を集合 A 上の同値関係とする. 任意の $a, b \in A$ に対して, 以下が成り立つ.

- (1) $a \in [a]$ (各同値類は空でない).
- (2) $a \sim b \iff [a] = [b]$.
- (3) $[a] \cap [b] = \emptyset$ または $[a] = [b]$ (任意の 2 つの同値類は一致するか, 交わらない).

証明. (1) \sim の反射性より $a \sim a$ だから $a \in [a]$.

(2) (\implies) $a \sim b$ とする. $c \in [a]$ ならば $a \sim c$, 対称性から $b \sim a$, 推移性から $b \sim c$ より $c \in [b]$, よって $[a] \subset [b]$. $b \sim a$ に対して同様の議論を行うと $[b] \subset [a]$. よって $[a] = [b]$.

(\impliedby) $[a] = [b]$ とすると, (1) より $b \in [b] = [a]$ だから $a \sim b$.

(3) $[a] \cap [b] \neq \emptyset$ と仮定し, $c \in [a] \cap [b]$ をとる. $a \sim c$ かつ $b \sim c$ より対称性・推移性から $a \sim b$, (2) より $[a] = [b]$. □

この定理から、 A の各元はちょうど一つの同値類に属し、 A は同値類によって互いに交わらないグループに分割されることがわかる。この分割を A の分割 (partition) という。

例 3-6 \mathbb{Z} 上の合同関係 $\equiv \pmod{3}$ による同値類と商集合を求める。3 で割った余りは 0, 1, 2 の 3 通りしかないので、同値類はちょうど 3 つである。

$$\begin{aligned}[0] &= \{\dots, -6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}, \\ [1] &= \{\dots, -5, -2, 1, 4, 7, \dots\} = 3\mathbb{Z} + 1, \\ [2] &= \{\dots, -4, -1, 2, 5, 8, \dots\} = 3\mathbb{Z} + 2.\end{aligned}$$

例えば $[-1] = [2]$, $[4] = [1]$, $[-6] = [0]$ が確認できる。商集合は $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ である。

補足 3.6. 一般に、 n を正整数とすると、 \mathbb{Z} 上の合同関係 $\equiv \pmod{n}$ による商集合は

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \dots, [n-1]\}$$

であり、ちょうど n 個の同値類からなる。この $\mathbb{Z}/n\mathbb{Z}$ は整数論・代数学において重要な代数構造 (環) をもち、暗号理論などにも応用される。

小テスト

小テスト 3-1 次の各 2 項関係について、定義 3.2 の性質 (a)~(d) のうちどれを満たすか判定し、理由を簡潔に述べよ。

- (1) $A = \mathbb{Z}$ 上の関係 $R: aRb$ とは $|a - b| \leq 1$ (差の絶対値が 1 以下)
- (2) $A = \mathbb{Z}$ 上の関係 $S: aSb$ とは $a + b$ が偶数
- (3) $A = \{1, 2, 3, 4, 5, 6\}$ 上の関係 $T: aTb$ とは $\gcd(a, b) > 1$ (最大公約数が 1 より大きい)

小テスト 3-2 \mathbb{Z} 上の合同関係 $\equiv \pmod{4}$ について答えよ。

- (1) すべての同値類を求めよ。
- (2) 商集合 $\mathbb{Z}/4\mathbb{Z}$ を書け。
- (3) 整数 $-7, 0, 11, 18, -3$ はそれぞれどの同値類に属するか答えよ。

小テスト 3-3 $A = \{a, b, c, d\}$ 上の関係

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (c, d), (d, c)\}$$

について答えよ。

- (1) R が同値関係であることを、反射的・対称的・推移的の各性質を確認することで示せ。
- (2) $[a], [b], [c], [d]$ をそれぞれ求めよ。
- (3) 商集合 A/R を求めよ。