# 情報数学 I

## 第 5 回「関係-同値関係の性質、合同関係」

〇同値関係の性質

$R$を集合$S$上の同値関係としたとき、次の定理が成り立つ。

[定理 1] $\forall a \in S$ に対して、$a \in C_a$が成り立つ。

[定理 2] $\forall a, x, y \in S$に対し、$x, y \in C_a \Longrightarrow xRy$が成り立つ。

[定理 3] $\forall a, b \in S$ に対し、$aRb \Longrightarrow C_a = C_b$が成り立つ。

[定理 4] $S/R$は$S$の分割である。

〇合同関係

合同関係: $a, b \in \mathbb{Z}$ (整数の集合), $m \in \mathbb{N}$(自然数の集合)に対して、$a - b$は$m$で割り切れる($a - b$は$m$の倍数である)とき、“$a$は$b$と$m$を法とする合同関係にある”といい、$a \equiv b \pmod m$と書く(または$a \equiv_m b$とも書く)。

合同関係は$a$を$m$で割った余りと$b$を$m$で割った余りが等しい関係でもある。

この合同関係は、数学者ガウス(1777 年～1855 年)が定義した。

(例 1) $x, y \in \mathbb{Z}$に対する関係$R$を$x \equiv y \pmod m$とする。$R$が同値関係であることを示せ。

(解) 集合$\mathbb{Z}$の合同関係≡が反射的かつ対称的かつ推移的であることを示せばよい。

(1) $\forall x \in \mathbb{Z}$に対し、$x - x = 0$は$m$で割り切れる。従って、$x \equiv x \pmod m$が成り立つ。よって、合同関係≡は反射的である。

(2) $\forall x, y \in \mathbb{Z}$に対して、$x \equiv y \pmod m$が成り立っているとする。そうすると、$x - y$は$m$で割り切れる。$-(x - y) = y - x$は$m$で割り切れる。すなわち、$y \equiv x \pmod m$が成り立つ。よって、合同関係≡は対称的である。

(3) $x, y, z \in \mathbb{Z}$に対して、$x \equiv y \pmod m, y \equiv z \pmod m$が成り立つとする。すると、$x - y$と$y - z$は$m$で割り切れる。$(x - y) + (y - z) = x - z$も$m$で割り切れる。すなわち$x \equiv z \pmod m$が成り立つ。よって、合同関係≡は推移的である。

(1), (2), (3)より、合同関係≡は同値関係である。

(例 2) 集合$\mathbb{Z}$上の合同関係≡は同値関係である。この合同関係≡による集合$\mathbb{Z}$の商$\mathbb{Z}/\equiv$すなわち$\mathbb{Z}$の同値類への分割を求めよ。

(解)

$0 \in \mathbb{Z}$と合同関係≡にある同値類$C_0$は

$$\begin{aligned} C_0 &= \{x | x \equiv 0 \pmod{m}, x \in \mathbb{Z}\} \\ &= \{x | x - 0 \text{ は} m \text{で割り切れる}\} \\ &= \{\cdots, -2m, -m, 0, m, 2m, \cdots\} \end{aligned}$$

$1 \in \mathbb{Z}$と合同関係≡にある同値類$C_1$は

$$\begin{aligned} C_1 &= \{x | x \equiv 1 \pmod{m}, x \in \mathbb{Z}\} \\ &= \{x | x - 1 \text{ は} m \text{で割り切れる}\} \\ &= \{\cdots, -2m + 1, -m + 1, 1, m + 1, 2m + 1, \cdots\} \end{aligned}$$

$k \in \mathbb{Z}$と合同関係≡にある同値類$C_k$は

$$\begin{aligned} C_k &= \{x | x \equiv k \pmod{m}, x \in \mathbb{Z}\} \\ &= \{x | x - k \text{は} m \text{で割り切れる}\} \\ &= \{\cdots, -2m + k, -m + k, k, m + k, 2m + k, \cdots\} \end{aligned}$$

$m - 1 \in \mathbb{Z}$と合同関係≡にある同値類$C_{m-1}$は

$$\begin{aligned} C_{m-1} &= \{x | x \equiv m - 1 \pmod{m}, x \in \mathbb{Z}\} \\ &= \{\cdots, -m - 1, -1, m - 1, 2m - 1, 3m - 1, \cdots\} \end{aligned}$$

従って、$\mathbb{Z}/\equiv = \{C_0, C_1, C_2, \cdots, C_{m-1}\}$となる。

集合$\mathbb{Z}$上の$m$を法とする合同関係≡は周期が$m$である周期構造を構成する。

| $C_0$ ↓ | $C_1$ ↓ | $C_2$ ↓ | | $C_k$ ↓ | | $C_{m-1}$ ↓ |
|---|---|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | | ⋮ | | ⋮ |
| $-2m$ | $-2m + 1$ | $-2m + 2$ | $\cdots$ | $-2m + k$ | $\cdots$ | $-m - 1$ |
| $-m$ | $-m + 1$ | $-m + 2$ | $\cdots$ | $-m + k$ | $\cdots$ | $-1$ |
| $0$ | $1$ | $2$ | $\cdots$ | $k$ | $\cdots$ | $m - 1$ |
| $m$ | $m + 1$ | $m + 2$ | $\cdots$ | $m + k$ | $\cdots$ | $2m - 1$ |
| $2m$ | $2m + 1$ | $2m + 2$ | $\cdots$ | $2m + k$ | $\cdots$ | $3m - 1$ |
| ⋮ | ⋮ | ⋮ | | ⋮ | | ⋮ |

〇同値関係の性質と証明

$R$を集合$S$上の同値関係としたとき、次の定理が成り立つ。

[定理 1] $\forall a \in S$ に対して、$a \in C_a$が成り立つ。

[定理 2] $\forall a, x, y \in S$に対し、$x, y \in C_a \Longrightarrow xRy$が成り立つ。

[定理 3] $\forall a, b \in S$ に対し、$aRb \Longrightarrow C_a = C_b$が成り立つ。

[定理 4] $S/R$は$S$の分割である。

関係$R$は、同値関係であるから、反射的かつ対称的かつ推移的である。そこで、$\forall a, b, c \in S$に対して、$aRa, aRb \Longrightarrow bRa, aRb \wedge bRc \Longrightarrow aRc$ が成り立つことを用いて、証明すればよい。

(定理 1 の証明) $\forall a \in S$に対して$R$は反射的であるから$aRa$である。従って、$a \in C_a$が成り立つ。(なぜならば $C_a = \{b | aRb, a \in S, b \in S\}$ )

(定理 2 の証明) $\forall x, y \in S$に対し$x \in C_a$と$y \in C_a$が成り立つとすると、$xRa$と$yRa$が成り立つ。対称律と推移律より、$xRa \wedge aRy \Longrightarrow xRy$であるため、$xRy$が成り立つ。

(定理 3 の証明) いま、$aRb$が成り立つとする。$R$は対称的であるから$bRa$が成り立つ。$c \in C_a$であるならば$a$は$c$と同値関係にあるから$aRc$が成り立つ。$R$は推移的であるから、$bRa \wedge aRc \Longrightarrow bRc$が成り立つ。よって、$c \in C_b$となる。すなわち、$c \in C_a$ならば$c \in C_b$が成り立つ。従って、$aRb$が成り立つならば、$C_a \subseteq C_b \cdots (A)$が成り立つ。一方、$c \in C_b$であるならば$b$は$c$と同値関係にあるから、$bRc$が成り立つ。$R$は推移的であるから、$aRb \wedge bRc \Longrightarrow aRc$が成り立つ。よって、$c \in C_a$となる。すなわち、$c \in C_b$ならば$c \in C_a$が成り立つ。従って、$aRb$が成り立つならば、$C_b \subseteq C_a \cdots (B)$が成り立つ。$(A), (B)$より、$aRb$が成り立つならば$C_a = C_b$が成り立つ。

(定理 4 の証明) $S/R$が$S$の分割であることを示すには、次の(1)～(2)が成り立つことを示せばよい。

(1) $S$の全ての要素を$C_{a_1}, C_{a_2}, \cdots, C_{a_n}$としたとき、$C_{a_1} \cup C_{a_2} \cup \cdots \cup C_{a_n} = S$が成り立つ。

(2) $\forall a, b \in S$ に対し、$C_a = C_b$もしくは$C_a \cap C_b = \phi$が成り立つ。

(1)の証明: 定理 1 より、$\forall a \in S$ に対して、$a \in C_a$が成り立つ。同値類の要素も$S$の要素であるから、$C_{a_1} \cup C_{a_2} \cup \cdots \cup C_{a_n} = S$が成り立つ。

(2)の証明: $C_a \cap C_b \neq \phi$とするならば$C_a \cap C_b$の要素$c$が存在する。従って、その要素$c$は$c \in C_a$であるので、$aRc$が成り立つ。また、$c \in C_b$であるので、$bRc$が成り立つ。一方、$R$は対称的であるので、$bRc \Longrightarrow cRb$が成り立つ。$R$は推移的であるので、$aRc \wedge cRb \Longrightarrow aRb$が成り立つ。従って、定理 3 より$C_a = C_b$が成り立つ。すなわち、$C_a \cap C_b \neq \phi$であるならば、$C_a = C_b$が成り立つ。

# 同値関係$R$による集合$S$の分割法のフローチャート