

関係と順序

離散数学・オートマトン

2024 年後期

佐賀大学理工学部 只木進一

- ① 二項関係: Binary relations
- ② 関係の演算: Operations of relations
- ③ 同値関係: Equivalence relations
- ④ 順序: Order

二項関係: Binary relations

- 2つのモノを結びつける関係
- 集合 A と B の直積 $A \times B$ の部分集合 R
 - A から B への二項関係 (A から B への関係)
 - $R: A \rightarrow B$
 - $(a, b) \in R$: a と b は R の関係にある: aRb
 - $R(a) = \{b \mid aRb\}$: a と R の関係にある全体
- $R: A \rightarrow A$: A の上への関係
- 写像、関数との違い
 - A の一つの要素から B の複数の要素への関係も含む
 - 写像と関数は関係の特殊な場合

関係の定義域、値域

$$R : X \rightarrow Y \quad (1.1)$$

- 定義域 (domain): X
- 値域 (range): Y
- 関数の場合と同じ

逆関係: Inverse relations

aRb の逆関係

- B から A への関係

$$R^{-1} = \{(b, a) \mid a \in A, b \in B, aRb\} \quad (1.2)$$

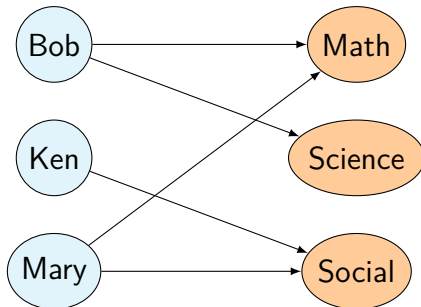
- $b \in B$ と aRb の関係にある a の全体

$$R^{-1}(b) = \{a \in A \mid aRb\} \quad (1.3)$$

- 逆関数との違いに注意

例 1.1: 生徒と得意科目

- $A = \{\text{Bob, Ken, Mary}\}$: 生徒の集合
- $B = \{\text{Math, Science, Social}\}$: 科目の集合



- $R : A \rightarrow B$
 - 生徒 $a \in A$ は、科目 $b \in B$ が得意である
- $R^{-1} : B \rightarrow A$
 - 科目 $b \in B$ を得意な生徒は $a \in A$ である

例 1.2: 関係とグラフ

- $X = \{a, b, c\}$ 上の二項関係

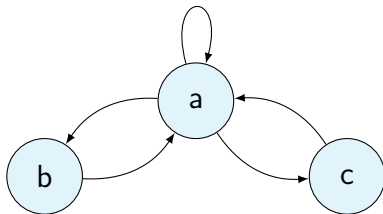
$$R = \{(a, a), (a, b), (a, c), (b, a), (c, a)\} \quad (1.4)$$

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

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

$$R^{-1}(a) = \{a, b, c\}$$

$$R^{-1}(b) = R^{-1}(c) = \{a\}$$



例 1.3: 包含関係

- 集合 X の部分集合上の包含関係 $\subseteq = \{(A, B) \mid A \subseteq B \subseteq X\}$
- $\subseteq^{-1}(B) = 2^B$: B のべき集合
 - B の部分集合全体

$$X = \{a, b\} \quad (1.5)$$

$$2^X = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \quad (1.6)$$

$$\emptyset \subseteq \emptyset$$

$$\emptyset \subseteq \{a\}$$

$$\emptyset \subseteq \{b\}$$

$$\emptyset \subseteq \{a, b\}$$

$$\{a\} \subseteq \{a\}$$

$$\{a\} \subseteq \{a, b\}$$

$$\{b\} \subseteq \{b\}$$

$$\{b\} \subseteq \{a, b\}$$

$$\{a, b\} \subseteq \{a, b\}$$

$$\{a, b\} \subseteq^{-1} \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$$\{a\} \subseteq^{-1} \{\emptyset, \{a\}\}$$

$$\{b\} \subseteq^{-1} \{\emptyset, \{b\}\}$$

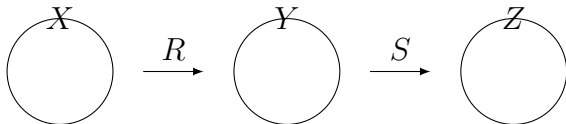
$$\emptyset \subseteq^{-1} \{\emptyset\}$$

関係と関数: Relations and Functions

- 関係 $R : X \rightarrow Y$ が以下を満たすとき、関数と呼ぶ
 - $\forall x \in X$ に対して $|R(x)| = 1$ 、つまり x に対して一つの $y \in Y$ が定まる
- つまり、関数は、関係の特別な場合

関係の結合: Compositions

- 集合 X 、 Y 、 Z に対する関係 $R: X \rightarrow Y$ 及び $S: Y \rightarrow Z$



- 関係の結合

$$S \circ R: X \rightarrow Z \quad (2.1)$$

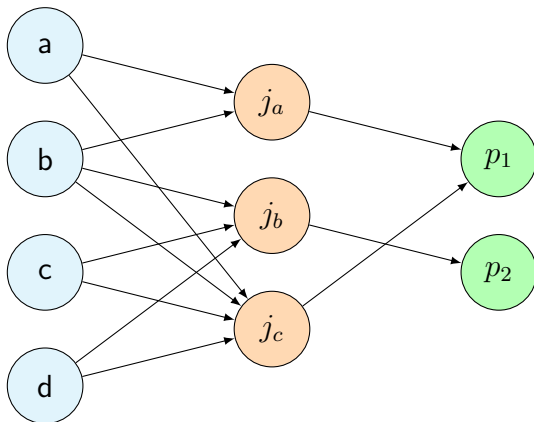
$$S \circ R = \{(x, z) \in X \times Z \mid \exists y \in Y, xRy \wedge ySz\} \quad (2.2)$$

- 結合律

$$R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1 \quad (2.3)$$

例 2.1: 論文著者 \rightarrow 学術誌 \rightarrow 出版社

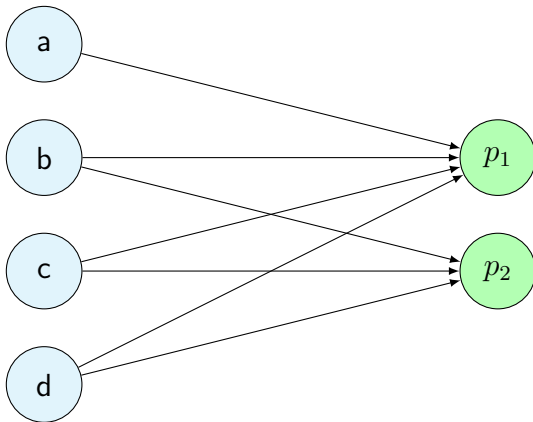
- $R : A \rightarrow J$: 著者 $a \in A$ は $j \in J$ の学術誌に論文を出版した
- $S : J \rightarrow P$: 学術誌 $j \in J$ は $p \in P$ という出版社が出版している。



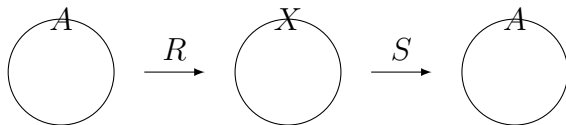
$$R = \{(a, j_a), (a, j_c), (b, j_a), (b, j_b), (b, j_c), (c, j_b), (c, j_d), (d, j_b), (d, j_d)\} \quad (2.4)$$

$$S = \{(j_a, p_1), (j_b, p_2), (j_c, p_1)\} \quad (2.5)$$

$$S \circ R = \{(a, p_1), (b, p_1), (b, p_2), (c, p_1), (c, p_2), (d, p_1), (d, p_2)\} \quad (2.6)$$



例 2.2:

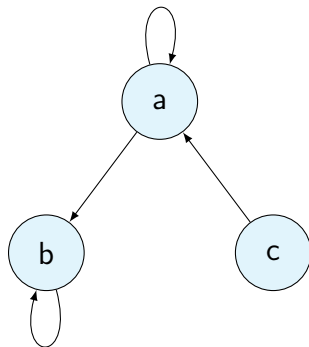
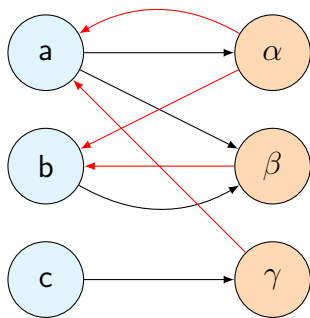


- $A = \{a, b, c\}$ と $X = \{\alpha, \beta, \gamma\}$ に対して

$$R = \{(a, \alpha), (a, \beta), (b, \beta), (c, \gamma)\} \quad (2.7)$$

$$S = \{(\alpha, a), (\alpha, b), (\beta, b), (\gamma, a)\} \quad (2.8)$$

$$\begin{aligned} S \circ R &= \{(x, z) \in A \times A \mid \exists y \in X, xRy \wedge ySz\} \\ &= \{(a, a), (a, b), (b, b), (c, a)\} \end{aligned} \quad (2.9)$$



恒等関係、関係のべき乗

- $R : A \rightarrow A$
 - $R^0 = \Delta_A = \{(a, a) \mid a \in A\}$: 恒等関係: identity
 - $R^{n+1} = R \circ R^n$: べき乗: exponentiation

関係の和、共通部分

- 定義域と値域が共通の二つの関係 $R, S : A \rightarrow B$
 - 和 (union): $R \cup S$
 - 共通部分 (intersection): $R \cap S$
- 反射的推移閉包: reflexive transitive closures

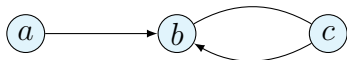
$$R^* = \bigcup_{n=0}^{\infty} R^n \quad (2.10)$$

- 推移閉包: transitive closures

$$R^+ = \bigcup_{n=1}^{\infty} R^n \quad (2.11)$$

例 2.3:

$$R = \{(a, b), (b, c), (c, b)\} \quad (2.12)$$



- R^2

$$aRb \wedge bRc \rightarrow aR^2c$$

$$bRc \wedge cRb \rightarrow bR^2b$$

$$cRb \wedge bRc \rightarrow cR^2c$$

- R^3

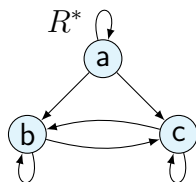
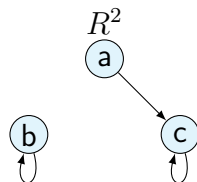
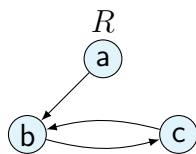
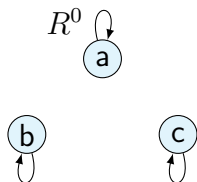
$$aRb \wedge bR^2b \rightarrow aR^3b$$

$$bRc \wedge cR^2c \rightarrow bR^3c$$

$$cRb \wedge bR^2b \rightarrow cR^3b$$

- $R = R^3$ を得る

$$\begin{aligned} R^* &= R^0 \cup R \cup R^2 \\ &= \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, b), (c, c)\} \end{aligned}$$



例 2.4: N 上の二項関係 $nRm \Leftrightarrow n = m + 1$

$$nR^0m \Leftrightarrow n = m$$

$$nR^1m \Leftrightarrow n = m + 1$$

$$nR^2m \Leftrightarrow n = m + 2$$

$$nR^km \Leftrightarrow n = m + k$$

$$nR^*m \Leftrightarrow \exists k \geq 0, nR^km \Leftrightarrow n \geq m$$

$$nR^+m \Leftrightarrow \exists k > 0, nR^km \Leftrightarrow n > m$$

同値関係: Equivalence relations

- $R : A \rightarrow A$
- 以下の三つの性質を全て満たす関係: 同値関係
 - 反射律 (reflexive): $\forall a \in A$ に対して aRa
 - 対称律 (symmetric): $\forall a, b \in A$ に対して $aRb \Leftrightarrow bRa$
 - 推移律 (transitive): $\forall a, b, c \in A$ に対して $aRb \wedge bRc \Leftrightarrow aRc$

例 3.1: m を法とする合同

- $x, y \in N \cup \{0\}$ を $m \in N$ で除した余りが等しい

$$R = \{(x, y) \mid x \equiv y \pmod{m}\} \quad (3.1)$$

- 反射律: xRx は自明
- 対称律: $xRy \rightarrow yRx$ も自明
- 推移律: $xRy \wedge yRz \rightarrow xRz$
 - $k, \ell \in Z$ が存在し、 $x - y = km$ かつ $y - z = \ell m$

$$x - z = (x - y) + (y - z) = (k + \ell)m \quad (3.2)$$

同値類: equivalence classes

- 集合 A 上の同値関係 R によって、集合 A を分ける
- $a \in A$ に対して

$$[a]_R = \{b \in A \mid aRb\} \quad (3.3)$$

- R によって定まる a と同値なものの全体
 - a を代表元という
- 重複は無い

同値類の性質

- 集合 A 上の同値関係 R
- $\forall a, b, c \in A$
- $a \in [a]_R$
- $b, c \in [a]_R \rightarrow bRc$
- $aRb \Leftrightarrow [a]_R = [b]_R$
- $[a]_R = [b]_R$ と $[a]_R \cap [b]_R = \emptyset$ のいずれか一方だけが必ず成り立つ
- $\bigcup_{a \in A} [a]_R = A$

m を法とする剰余類

- $R = \{(x, y) \mid x \equiv y \pmod{m}\}$
- $m = 3$ の場合 ($k \in N \cup \{0\}$)

$$[0] = \{n \mid n = 3k\}$$

$$[1] = \{n \mid n = 3k + 1\}$$

$$[2] = \{n \mid n = 3k + 2\}$$

有限体: Finite fields

- 素数 p で除した余りからなる集合

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\} \quad (3.4)$$

- 加法について $\text{mod } p$ で閉じており、0 を単位元として、全ての要素に逆元がある。
- 乗法について $\text{mod } p$ で閉じており、1 を単位元として、0 以外の要素の逆元がある。
- $\text{mod } p$ で交換則、結合則、分配則が成り立つ。
- Fermat の小定理: p と互いに素な $a \in \mathbb{F}_p$ に対して

$$a^{p-1} \equiv 1 \pmod{p}$$

- 暗号理論の基礎

Fermat の小定理: 数学的帰納法による証明

- $a^p \equiv a \pmod{p}$ を証明
 - $1^p \equiv 1 \pmod{p}$ は明らか
 - a に対して $a^p \equiv a \pmod{p}$ を仮定

$$\begin{aligned}(a+1)^p &\equiv \sum_{k=0}^p \binom{p}{k} a^k 1^{p-k} \pmod{P} \\ &\equiv \left(a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k 1^{p-k} + 1^p \right) \pmod{p} \\ &\equiv (a^p + 1) \pmod{p} \\ &\equiv (a+1) \pmod{p}\end{aligned}\tag{3.5}$$

- $\binom{p}{k} \equiv 0 \pmod{p}$ for $k \in [1, p-1]$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad (3.6)$$

分子は p の倍数、一方分母には因子 p を含まない

- $a^{p-1} \equiv 1 \pmod{p}$

$$\begin{aligned} a^p - a &\equiv 0 \pmod{p} \\ &\equiv a(a^{p-1} - 1) \pmod{p} \end{aligned} \quad (3.7)$$

$$a^{p-1} \equiv 1 \pmod{p} \quad (3.8)$$

例 3.2: $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

$$1 + 4 \equiv 0 \pmod{5}$$

$$2 + 3 \equiv 0 \pmod{5}$$

$$2 \times 3 \equiv 1 \pmod{5}$$

$$4 \times 4 \equiv 1 \pmod{5}$$

$$a = 2 \quad a^2 \equiv 4 \pmod{5} \quad a^3 \equiv 3 \pmod{5} \quad a^4 \equiv 1 \pmod{5}$$

$$a = 3 \quad a^2 \equiv 4 \pmod{5} \quad a^3 \equiv 2 \pmod{5} \quad a^4 \equiv 1 \pmod{5}$$

$$a = 4 \quad a^2 \equiv 1 \pmod{5}$$

順序: Order

- 反対称律: anti-symmetric
 - $\forall a, b \in A$ に対して $aRb \wedge bRa \rightarrow a = b$
- 関係が反射律、推移律、反対称律を満たすとき、半順序 (partial-order) または順序という
 - 大小関係 \leq は半順序
 - 半順序が定義された集合を半順序集合という

全順序: total order

- 全順序: 半順序に加えて、任意の二つの要素について比較可能であるとき
- 全順序集合: 全順序を定義された集合

例 4.1:

- 自然数、整数、有理数、実数に対する大小関係 \leq は全順序
 - 任意の要素を大小関係 \leq で比較可能
- 集合の包含関係 \subseteq は半順序
 - 任意の集合の間に包含関係は成り立たない

例 4.2:

$n, m \in N$ 対する関係「 $n \mid m$: n は m を割り切る」は半順序

- 反射律: $n \mid n$ は自明
- 推移律: $n \mid m \wedge m \mid \ell \rightarrow n \mid \ell$

$$\begin{aligned} (n \mid m \rightarrow m = an, m \mid \ell \rightarrow \ell = bm) \\ \rightarrow \ell = bm = abn \end{aligned} \quad (4.1)$$

- 反対称律

$$\begin{aligned} n \mid m \wedge m \mid n \rightarrow m = an \wedge n = bm \\ \rightarrow a = b = 1 \rightarrow n = m \end{aligned} \quad (4.2)$$

- n と m が互いに素の場合には、関係が成り立たないため、全順序ではない