2009年度 離散数学 講義資料[1] [2]

はしがき

本資料は, 離散数学の講義[3]用資料として作成したものである. 本資料は、参考文献 [1] の内容を中心に [2, 3, 4, 5, 6] を参考にしてまとめたものである.

目 次

1 集合 **2**
- 1.1 集合と元 . . . 2
- 1.2 集合の記法 . . . 2
- 1.3 部分集合 . . . 3
- 1.4 集合の間の演算 . . . 4
- 1.5 直積集合 . . . 7
- 1.6 ベキ集合 . . . 7

2 写像 **10**
- 2.1 写像の定義 . . . 10
- 2.2 単射, 全射, 全単射, 逆写像 . . . 10
- 2.3 写像による像および逆像 . . . 12
- 2.4 合成写像 . . . 14
- 2.5 写像の集合, 鳩の巣原理 . . . 16

3 論理 **19**
- 3.1 命題論理 . . . 19
  - 3.1.1 命題論理 . . . 19
  - 3.1.2 論理記号, 複合命題 . . . 19
  - 3.1.3 論理関数, 主論理和標準形, 主論理積標準形 . . . 22
  - 3.1.4 恒真命題, 論法, 対偶, 背理法 . . . 25
- 3.2 述語と限定記号 . . . 27
  - 3.2.1 述語 . . . 27
  - 3.2.2 全称記号 $\forall$ と存在記号 $\exists$ . . . 27

4 数学的帰納法と再帰的定義 **32**
- 4.1 数学的帰納法 . . . 32
- 4.2 再帰的定義 . . . 35

5 関係 **38**
- 5.1 2 項関係 . . . 38
- 5.2 同値関係 . . . 40
- 5.3 順序関係 . . . 48
- 5.4 関係の閉包 . . . 53
- 5.5 グラフと隣接行列 . . . 55
  - 5.5.1 その 1 (パスの本数) . . . 55
  - 5.5.2 その 2 (三角形の数) . . . 56

[1] ©2007–2009 栗原正純, 電気通信大学情報通信工学科, kuri@ice.uec.ac.jp

[2] 参考 WEB サイト http://www.code.ice.uec.ac.jp/class/
[3] 法政大学 情報科学部, 2009 年度 離散数学 (33: /doc/tex/dismath2009/ : 2009/9/9/20:06)

1 集合

1.1 集合と元

定義 1.1 (集合)

1. 次のような性質をもつ, “もの” の集まりを**集合**という.
   i. あるものが集合に属するか, どうかが, 明確に判断できる.
   ii. 集合に属する 2 つのものが, 同一であるかどうか判断できる.
2. 集合を構成するものを, その集合の**要素** (あるいは**元** (げん)) という.
3. もの x が, 集合 X の要素であることを, x は X に**属する**といい, $x \in X$ または $X \ni x$ と表す. $x_1 \in X, x_2 \in X, \ldots, x_n \in X$ を $x_1, x_2, \ldots, x_n \in X$ と略記することがある. [4]
4. もの x が, 集合 X の要素でないことを, $x \notin X$ または $X \not\ni x$ と表し, x は X に**属さない**という.
5. 集合を要素とする集合を**集合族**という.

1.2 集合の記法

定義 1.2 (集合の記法)

1. 要素 $x_1, x_2, \ldots, x_n$ からなる集合を, $\{x_1, x_2, \ldots, x_n\}$ と表す. (**外延的記法**)
2. $P(x)$ を x に関する条件とする. $P(x)$ を満たす x を要素とし, かつ, そのような x だけを要素とする集合を $\{x|P(x)\}$ と表す. (**内包的記法**)
3. 複数の条件 $P_1(x), \ldots, P_n(x)$ があるとき, $P_1(x), \ldots, P_n(x)$ をすべて満たす x を要素とし, かつ, そのような x だけを要素とする集合を $\{x|P_1(x), \ldots, P_n(x)\}$ と表す.
4. X を集合とするとき, $\{x|x \in X, P(x)\}$ を $\{x|P(x)\}$ と略記することがある.

注意 1.3 1. 集合を表す括弧は, 中カッコ (brace) “{”, “}” を用いること. また, 要素を列挙するときは, コンマ (comma) “,” で区切る.

2. $\{x|P(x)\}$ の中の x は, 括弧 “{” と “}” の中だけで通用する変数であり, もし, 括弧の外に x という記号があっても, それとは何の関わりもない. また, この x を他の記号に置き換えても, 表す集合に変わりはない: たとえば, $\{x|P(x)\} = \{y|P(y)\} = \cdots$.
3. しかし, $\{x|P(x,y)\}$ における y は, 括弧の外の世界と関わりをもつ. つまり, 括弧の外で変数 y にどのような値を設定するかによって, 集合 $\{x|P(x,y)\}$ は異なるものとなる. したがって, このような場合は, y を他の変数に置き換えるときは, 注意を要する.

例題 1.4 1. 自然数全体の集まり: $\{1, 2, \ldots\}$. これは集合である.

2. 10 より小さい素数全体の集まり[5] : $\{2, 3, 5, 7\}$. これは集合である.
3. 十分大きい自然数全体の集まり. これは集合ではない. 集合の定義に示した条件 i を満たさない.
4. 次の集合は空集合である: $\{x|x \in \mathbb{Z}, 2x + 1 = 0\}$.

定義 1.5 要素をもたない集合を**空 (くう) 集合**とよび, 記号 ϕ(ファイ) で表す.

注意 1.6 空集合 ϕ と集合 $\{\phi\}$ は異なる. ϕ は要素をもたない集合 (0 個の要素をもつ集合) であり, $\{\phi\}$ は ϕ という要素をもつ集合 (1 個の要素をもつ集合) である. 空集合を外延的記法で表せば, { } と書くことができるが, 通常は用いない場合が多い. この記述で, $\{\phi\}$ を表せば, { { } } となる.

---

[4] 次の省略記号は, 数学の習慣として用いられる. $x_1, x_2, \ldots, x_n$ に用いられている省略記号 “...” は, 3 個の下付きのドット “.” である. 個数として, 3 個を並べるのが数学での習慣である. 下付きのドットである理由は, 上下方向で, 下側に記述されるコンマ “,” の間での省略であるから. 一方, $1 + 2 + \cdots + n$ のような場合は, 上下方向で中間位置のプラス記号 “+” の間での省略であることより, 中間位置のドット “·” が用いられる.

[5] 素数とは: 1 より大きい整数 x が 1 と x 以外に, 正の約数をもたないとき, x を素数という. 約数とは: a, b を 2 つの整数とする. もし, $a = bq$ となる整数 q が存在するならば, b を a の約数といい, $b|a$ と記す.

1.3 部分集合

定義 1.7 X, Y を集合とする. X の要素がすべて Y の要素であるとき, X は Y の**部分集合**であるといい, $X \subseteq Y$ または $Y \supseteq X$ と表す. X が Y の部分集合であり, かつ, X でない Y の要素が存在するとき, X は Y の**真部分集合**であるといい, $X \subset Y$ または $Y \supset X$ と表す. 言い換えると, $X \subseteq Y$ かつ $X \neq Y$ のとき, X は Y の真部分集合である.

定義 1.8 1. 自然数の全体からなる集合 $\{1, 2, \ldots\}$ を $\mathbb{N}$ と表す.
2. 整数の全体からなる集合: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ を $\mathbb{Z}$ と表す.
3. 有理数の全体からなる集合 $\{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ を $\mathbb{Q}$ と表す.
4. 実数の全体からなる集合を $\mathbb{R}$ と表す.
5. 複素数の全体からなる集合を $\mathbb{C}$ と表す.
6. このとき, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ が成り立つ.

定義 1.9 X, Y を集合とする. $X \subseteq Y$ かつ $X \supseteq Y$ のとき, X と Y は**等しい**といい, $X = Y$ と表す.

定義 1.10 集合 X, Y に対し, $X \subseteq Y$ を証明する基本的な方法は, 「すべての $x \in X$ に対し, $x \in Y$ である」ことを示せばよい.

例題 1.11 次のことを証明せよ.
1. 任意の集合 X に対し, $X \subseteq X$.
2. 任意の集合 X に対し, $\phi \subseteq X$.
3. $\{x | x \in \mathbb{N}, 3 \leq x^2 \leq 17\} = \{x | x \in \mathbb{N}, 2 \leq x \leq 4\}$.
4. $\{2, 3, 1\} \subset \{4, 3, 6, 1, 5, 2\}$.
5. $\{1, 2, 1, 3, 4, 2\} = \{1, 2, 3, 4, 4, 3\}$.

(証明) 1, 2 のみ.
1. 任意の $x \in X$ に対し, $x \in X$ であることは, 明らか. ゆえに, $X \subseteq X$. ∎
2. 「$x \in \phi$ ならば $x \in X$」の対偶 :「$x \notin X$ ならば $x \notin \phi$」を示す. ϕ は, 要素をもたない集合であるから, 常に, $x \notin \phi$ が成り立つ. ∎

集合を外延的記法で表すとき, 要素の順序を入れ換えても, 集合は変化しない. また, 同じ要素を重複して列挙しても, その表す集合は, 重複がない場合と同じである. すなわち, $\{1, 2, 1, 3, 4, 2\} = \{1, 2, 3, 4, 4, 3\} = \{1, 2, 3, 4\}$.

例題 1.12 次のことが正しいかどうかを判定せよ.
1. $\phi \subseteq \phi$
2. $\phi \in \phi$
3. $\phi \subseteq \{\phi\}$
4. $\phi \in \{\phi\}$
5. $\{\phi\} \subseteq \{\phi\}$
6. $\{\phi\} \in \{\phi\}$

(解) 1. 任意の集合 X に対し, $\phi \subseteq X$ であるから, $X = \phi$ とすれば, $\phi \subseteq \phi$. ゆえに, 正しい. 2. ϕ の要素数は 0 であるから, 要素 ϕ を持つことができないことより, 正しくない. 3. 正しい. 4. 集合 X を $X = \{x\}$ とすれば, $x \in X$ であるから, $x = \phi$ とすれば, $\phi \in X = \{\phi\}$. ゆえに, 正しい. 5. 任意の集合 X に対し, $X \subseteq X$. $X = \{\phi\}$ とすれば $\{\phi\} \subseteq \{\phi\}$. ゆえに, 正しい. 6. $\{\phi\}$ の要素は ϕ だけであり, $\{\phi\}$ を要素としてもたない. ゆえに, 正しくない. ∎

1.4 集合の間の演算

本稿では, 記号 ":=" を "定義する" という意味で用いる. 具体的には, $A := B$ とは, 既知の B によって A を新しく定義することを意味する. すなわち, B によって A を定義する. $B =: A$ と記述しても, $A := B$ と同じ意味である.

定義 1.13 集合の間に, 次のような演算を考える. U を集合とし, $X \subseteq U, Y \subseteq U$ とする.

1. $X \cup Y := \{x \mid x \in X$ または $x \in Y\}$. (X と Y の**和集合**)
2. $X \cap Y := \{x \mid x \in X$ かつ $x \in Y\}$. (X と Y の**積集合**, **共通集合**)
3. $X \cap Y = \phi$ のとき, $X \cup Y$ を X と Y の**直和**といい, $X + Y$ と表すことがある.
4. $X^c := \{x \mid x \in U, x \notin X\}$. ($U$ に関する X の**補集合**)
5. $X - Y := X \cap Y^c$. (X と Y の**差集合**)
6. $X \ominus Y := (X - Y) \cup (Y - X)$. ($X$ と Y の**対称差**)

上記定義における集合 U を**全体集合**という. "$x \in X$ または $x \in Y$" というとき, "$x \in X$ かつ $x \in Y$" となる場合を含むことに注意する.

集合を平面上の集合で表すベン図 (Venn diagram) を用いると, 和集合や共通集合などは, 図 1 のように表される.

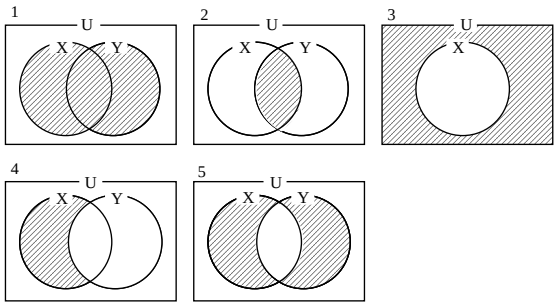


図 1: 1. $X \cup Y$, 2. $X \cap Y$, 3. X^c, 4. $X - Y$, 5. $X \ominus Y$.

例題 1.14 $U = \{1, 2, \ldots, 8\}$, $X = \{3, 4, 5\}$, $Y = \{1, 2, 3, 4, 6\}$ とするとき, $X \cup Y$, $X \cap Y$, X^c, $X - Y$, $X \ominus Y$ をそれぞれ外延的記法で表せ.

(解) $X \cup Y = \{1, 2, 3, 4, 5, 6\}$, $X \cap Y = \{3, 4\}$, $X^c = \{1, 2, 6, 7, 8\}$, $X - Y = \{5\}$, $X \ominus Y = \{1, 2, 5, 6\}$. ∎

定理 1.15 U を全体集合とする. U の任意の部分集合 X に対し, 以下が成立する.

1. $X \cup U = U$, $X \cap U = X$.
2. $X \cup \phi = X$, $X \cap \phi = \phi$.
3. $X \cup X^c = U$, $X \cap X^c = \phi$.
4. $(X^c)^c = X$.

(証明) 1 のみ.

($X \cup U = U$) $\subseteq$) 任意の $x \in X \cup U$ に対し, $x \in U$ より, $X \cup U \subseteq U$. $\supseteq$) 任意の $x \in U$ に対し, $x \in X \cup U$ より, $X \cup U \supseteq U$. 以上より, $X \cup U = U$. ∎

($X \cap U = X$) $\subseteq$) 任意の $x \in X \cap U$ に対し, $X \subseteq U$ より, $x \in X$ は明らか. ゆえに, $X \cap U \subseteq X$. $\supseteq$) 任意の $x \in X$ に対し, $x \in X \subseteq U$ より, $x \in X \cap U$. ゆえに, $X \cap U \supseteq X$. 以上より, $X \cap U = X$. ∎

例題 1.16 X, Y を集合とする. このとき, 次を証明せよ. $X \subseteq Y$ ならば $X \cap Y = X$ が成り立つ. また, $X \cap Y = X$ ならば $X \subseteq Y$ が成り立つ.

定理 1.17 任意の集合 X, Y, Z に対し, 以下の等式が成立する.

1. $X \cup Y = Y \cup X$,
   $X \cap Y = Y \cap X$. (**交換律**)
2. $(X \cup Y) \cup Z = X \cup (Y \cup Z)$,
   $(X \cap Y) \cap Z = X \cap (Y \cap Z)$. (**結合律**)
3. $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$,
   $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$. (**分配律**)
4. $X \cup X = X$,
   $X \cap X = X$. (**ベキ等律**)
5. $(X \cup Y) \cap X = X$,
   $(X \cap Y) \cup X = X$. (**吸収律**)

(証明) 分配律:

$(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$. $A :=$ 左辺, $B :=$ 右辺 とする. まず, $A \subseteq B$ を示す: 任意の $x \in A$ に対し, $x \in X \cup Y$ かつ $x \in Z$. このとき, $x \in X$ または $x \in Y$ である. そこで, i) $x \in X$ かつ $x \in Z$ ならば $x \in X \cap Z$ より, $x \in B$. または, ii) $x \in Y$ かつ $x \in Z$ ならば $x \in Y \cap Z$ より, $x \in B$. したがって, 常に $x \in B$. ゆえに, $A \subseteq B$.

次に, $A \supseteq B$ を示す: 任意の $x \in B$ に対し, $x \in X \cap Z$ または $x \in Y \cap Z$. そこで, i) $x \in X \cap Z$ ならば $x \in X \cup Y$ かつ $x \in Z$ より, $x \in A$. または, ii) $x \in Y \cap Z$ ならば $x \in X \cup Y$ かつ $x \in Z$ より, $x \in A$. したがって, 常に $x \in A$ が成り立つ. ゆえに, $A \supseteq B$. 以上より, $A = B$ が成り立つ. ∎

$(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$: $A :=$ 左辺, $B :=$ 右辺 とする. まず, $A \subseteq B$ を示す: 任意の $x \in A$ に対し, $x \in X \cap Y$ または $x \in Z$. そこで, i) $x \in X \cap Y$ ならば $x \in X \cup Z$ かつ $x \in Y \cup Z$ より, $x \in B$. または, ii) $x \in Z$ ならば $x \in X \cup Z$ かつ $x \in Y \cup Z$ より, $x \in B$. したがって, 常に $x \in B$. ゆえに, $A \subseteq B$.

次に, $A \supseteq B$ を示す: 任意の $x \in B$ に対し, $x \in X \cup Z$ かつ $x \in Y \cup Z$. そこで, i) $x \in Z$ ならば, 明らかに $x \in A$. または, ii) $x \notin Z$ ならば $x \in X$ かつ $x \in Y$ より, $x \in X \cap Y$. ゆえに, $x \in A$. したがって, 常に $x \in A$. ゆえに, $A \supseteq B$. 以上より, $A = B$ が成り立つ. ∎

定理 1.18 (**ド・モルガンの法則**) 和集合, 共通集合, 補集合の間には, 以下のような関係がある.

1. $(X \cup Y)^c = X^c \cap Y^c$.
2. $(X \cap Y)^c = X^c \cup Y^c$.

(証明) 2. $\subseteq$) 任意の $x \in (X \cap Y)^c$ に対し, $x \notin X \cap Y$ であることより, $x \notin X$ または $x \notin Y$ である. すなわち, $x \in X^c$ または $x \in Y^c$ であるから, $x \in X^c \cup Y^c$. ゆえに, $(X \cap Y)^c \subseteq X^c \cup Y^c$. $\supseteq$) $x \in X^c \cup Y^c$ とする. $x \in X^c$ または $x \in Y^c$ である. $x \in X^c$ ならば $x \notin X$ ある. すなわち, $x \notin X \cap Y$. 同様に, $x \in Y^c$ ならば $x \notin Y$ ある. すなわち, $x \notin X \cap Y$. したがって, $x \in (X \cap Y)^c$. ゆえに, $(X \cap Y)^c \supseteq X^c \cup Y^c$. 以上より, $(X \cap Y)^c = X^c \cup Y^c$.

例題 1.19 (ド・モルガンの法則) 全体集合を $U = \{1, 2, \ldots, 8\}$ とする. そして, $X = \{3, 4, 5\}$, $Y = \{1, 2, 3, 4, 6\}$ とするとき, $X \cup Y = \{1, 2, 3, 4, 5, 6\}$, $X \cap Y = \{3, 4\}$, $X^c = \{1, 2, 6, 7, 8\}$, $Y^c = \{5, 7, 8\}$ である. これより, $(X \cup Y)^c = \{7, 8\} = X^c \cap Y^c$. また, $(X \cap Y)^c = \{1, 2, 5, 6, 7, 8\} = X^c \cup Y^c$. ∎

例題 1.20 任意の集合 X, Y, Z に対し, 以下が成り立つことを示せ.

1. $(X \cup Y) - Z = (X - Z) \cup (Y - Z)$
2. $(X - Y) - Z = X - (Y \cup Z)$
3. $X - (Y - Z) = (X - Y) \cup (X \cap Z)$

(証明)

1. $(X \cup Y) - Z = (X \cup Y) \cap Z^c = (X \cap Z^c) \cup (Y \cap Z^c) = (X - Z) \cup (Y - Z)$.
   最初と 3 番目の等号は, 差集合の定義による. 2 番目の等号は, 分配律による.

2. $(X-Y)-Z = (X \cap Y^c)-Z = (X \cap Y^c) \cap Z^c = X \cap Y^c \cap Z^c = X \cap (Y^c \cap Z^c) = X \cap (Y \cup Z)^c = X - (Y \cup Z)$.
3. $X-(Y-Z) = X-(Y \cap Z^c) = X \cap (Y \cap Z^c)^c = X \cap (Y^c \cup Z) = (X \cap Y^c) \cup (X \cap Z) = (X-Y) \cup (X \cap Z)$.

定義 1.21 集合 $X_1, \ldots, X_n$ に対し, 以下を定義する.

1. $\bigcup_{i=1}^{n} X_i := \{x \mid \text{ある } i \in \{1, \ldots, n\} \text{ に対し}, x \in X_i\}$. ($X_1, \ldots, X_n$ の**和集合**)
2. $\bigcap_{i=1}^{n} X_i := \{x \mid \text{すべての } i \in \{1, \ldots, n\} \text{ に対し}, x \in X_i\}$. ($X_1, \ldots, X_n$ の**積集合**, **共通集合**)

以下の定理より, $\cup_{i=1}^{n} X_i$ を $X_1 \cup \cdots \cup X_n$ と表すことが可能である. このとき, $X_1, \ldots, X_n$ をどのように並べ換えても, その表す集合は変わらない. また, 正しい括弧付けならば, どのように括弧をつけても, その表す集合は変わらない. 例えば, $X_1 \cup X_2 \cup X_3 \cup X_4 = X_3 \cup X_1 \cup X_4 \cup X_2 = (X_3 \cup X_1) \cup (X_4 \cup X_2) = ((X_3 \cup X_1) \cup X_4) \cup X_2$. $\cap_{i=1}^{n} X_i$ についても同様である.

定理 1.22 任意の自然数 n と, 任意の n 個の集合 $X_1, \ldots, X_n$ に対し, 以下の等式が成り立つ.

1. $\bigcup_{i=1}^{n} X_i = X_1 \cup \cdots \cup X_n$
2. $\bigcap_{i=1}^{n} X_i = X_1 \cap \cdots \cap X_n$

(証明) 2. 集合の数 n に関する数学的帰納法で示す.

$n = 1$ のとき, $X_1 = X_1$.

$n = k$ のとき, $\cap_{i=1}^{k} X_i = X_1 \cap \cdots \cap X_k$ が成り立つと仮定する.

$n = k+1$ のとき, $\cap_{i=1}^{k+1} X_i = X_1 \cap \cdots \cap X_{k+1}$ が成り立つことを示そう. そのために, まず, $\cap_{i=1}^{k+1} X_i = (\cap_{i=1}^{k} X_i) \cap X_{k+1}$ が成り立つことを示す.

$\subseteq$) $x \in \cap_{i=1}^{k+1} X_i$ とする. 集合 $\cap_{i=1}^{n} X_i$ の定義より, すべての $i \in \{1, \ldots, k+1\}$ に対し, $x \in X_i$. したがって, $x \in \cap_{i=1}^{k} X_i$ かつ $x \in X_{k+1}$ である. すなわち, $x \in \cap_{i=1}^{k} X_i \cap X_{k+1}$. ゆえに, $\cap_{i=1}^{k+1} X_i \subseteq (\cap_{i=1}^{k} X_i) \cap X_{k+1}$.

$\supseteq$) $x \in (\cap_{i=1}^{k} X_i) \cap X_{k+1}$ とする. $x \in \cap_{i=1}^{k} X_i$ より, すべての $i \in \{1, \ldots, k\}$ に対し, $x \in X_i$ であり, さらに, $x \in X_{k+1}$ が成り立つ. したがって, すべての $i \in \{1, \ldots, k+1\}$ に対し, $x \in X_i$ より, $x \in \cap_{i=1}^{k+1} X_i$ である. ゆえに, $\cap_{i=1}^{k+1} X_i \supseteq (\cap_{i=1}^{k} X_i) \cap X_{k+1}$.

以上より, $\cap_{i=1}^{k+1} X_i = (\cap_{i=1}^{k} X_i) \cap X_{k+1}$ が成り立つことが言えた. ゆえに, $n = k$ の仮定より, $\cap_{i=1}^{k+1} X_i = (\cap_{i=1}^{k} X_i) \cap X_{k+1} = X_1 \cap \cdots X_k \cap X_{k+1}$ が成り立つ. ∎

定理 1.23 (拡張されたド・モルガンの法則) 任意の集合 $X_1, \ldots, X_n$ に対し, 以下が成り立つ.

1. $(\bigcup_{i=1}^{n} X_i)^c = \bigcap_{i=1}^{n} X_i^c$.
2. $(\bigcap_{i=1}^{n} X_i)^c = \bigcup_{i=1}^{n} X_i^c$.

定義 1.24 $\mathcal{S}$ を集合族 (すなわち, 集合を要素とする集合) とする.

1. $\bigcup_{X \in \mathcal{S}} X := \{x \mid \text{ある } X \in \mathcal{S} \text{ に対し}, x \in X\}$. (**和集合**)
2. $\bigcap_{X \in \mathcal{S}} X := \{x \mid \text{すべての } X \in \mathcal{S} \text{ に対し}, x \in X\}$. (**積集合**, **共通集合**)

この記法を用いると, ド・モルガンの法則は次のように表される.

定理 1.25 (拡張されたド・モルガンの法則) 任意の集合 $X_1, \ldots, X_n$ に対し, 以下が成り立つ.

1. $(\bigcup_{X \in \mathcal{S}} X)^c = \bigcap_{X \in \mathcal{S}} X^c$.
2. $(\bigcap_{X \in \mathcal{S}} X)^c = \bigcup_{X \in \mathcal{S}} X^c$.

1.5 直積集合

定義 1.26 “もの”$x_1, \ldots, x_n$ に対し, $(x_1, \ldots, x_n)$ を $x_1, \ldots, x_n$ の n **重対** (じゅうつい) という. 特に, (x_1, x_2) を x_1 と x_2 の**順序対**という.

定義 1.27 $X_1, \ldots, X_n$ を集合とする.

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) \mid x_1 \in X_1, \ldots, x_n \in X_n\}$$

を $X_1, \ldots, X_n$ の**直積**, または**直積集合**という. $X_1 = \cdots = X_n = X$ のときは, $X^n := X_1 \times \cdots \times X_n$ と表す.

もし, $X_i = \phi$ ならば, どのような n 重対 $(x_1, \ldots, x_n)$ に対しても, $x_i \notin X_i$ であるから, $(x_1, \ldots, x_n) \notin X_1 \times \cdots \times X_n$ である. これより, $X_i = \phi$ ならば $X_1 \times \cdots \times X_n = \phi$ となる.

例題 1.28 (直積集合)

1. $X = \{2, 1\}$, $Y = \{3, 2, 4\}$ のとき, $X \times Y$ を外延的記法で表せ.
2. $\{(x, y) \mid (x, y) \in \mathbb{N}^2, x^2 + y^2 \leq 8\}$ を外延的記法で表せ.
3. $\{(x, y, z) \mid (x, y, z) \in \mathbb{N}^3, x + y + z = 4\}$ を外延的記法で表せ.
4. 任意の X, Y, Z に対し, 次の等式を証明せよ. $(X \cap Z) \times Y = (X \times Y) \cap (Z \times Y)$
5. X, Y, Z, W を集合とする. このとき, 次の等式を証明せよ. $(X \cap Y) \times (Z \cap W) = (X \times Z) \cap (Y \times W)$

(解)

1. $X \times Y = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$.
2. $\{(1, 1), (1, 2), (2, 1), (2, 2)\}$.
3. $\{(1, 1, 2), (1, 2, 1), (2, 1, 1)\}$.
4. $\subseteq$) 任意の $(a, b) \in (X \cap Z) \times Y$ に対し, $a \in X$ かつ $a \in Z$ かつ $b \in Y$ である. したがって, $(a, b) \in X \times Y$ かつ $(a, b) \in Z \times Y$. ゆえに, $(a, b) \in (X \times Y) \cap (Z \times Y)$. $\supseteq$) 任意の $(a, b) \in (X \times Y) \cap (Z \times Y)$ に対し, $(a, b) \in X \times Y$ かつ $(a, b) \in Z \times Y$. すなわち, $a \in X$ かつ $a \in Z$. さらに, $b \in Y$. ゆえに, $(a, b) \in (X \cap Z) \times Y$. 以上より, 左辺 = 右辺. ∎
5. $\subseteq$) 任意の $(a, b) \in (X \cap Y) \times (Z \cap W)$ に対し, $a \in X \cap Y$ かつ $b \in Z \cap W$. したがって, “$a \in X$ かつ $a \in Y$” かつ “$b \in Z$ かつ $b \in W$.” これより, “$a \in X$ かつ $b \in Z$” かつ “$a \in Y$ かつ $b \in W$.” ゆえに, $(a, b) \in X \times Z$ かつ $(a, b) \in Y \times W$ より, $(a, b) \in (X \times Z) \cap (Y \times W)$. $\supseteq$) 上記証明の逆を示せばよい. 任意の $(a, b) \in (X \times Z) \cap (Y \times W)$ に対し, $(a, b) \in X \times Z$ かつ $(a, b) \in Y \times W$. すなわち, “$a \in X$ かつ $b \in Z$” かつ “$a \in Y$ かつ $b \in W$.” これより, “$a \in X$ かつ $a \in Y$” かつ “$b \in Z$ かつ $b \in W$.” ゆえに, $a \in X \cap Y$ かつ $b \in Z \cap W$ より, $(a, b) \in (X \cap Y) \times (Z \cap W)$. 以上より, 左辺 = 右辺. ∎

1.6 ベキ集合

定義 1.29 X を集合とする. X の部分集合の全体からなる集合を X の**ベキ集合** (冪集合, 巾集合) とよび, 2^X と表す: $2^X := \{Y \mid Y \subseteq X\}$.

ベキ集合 2^X は, X 自身と空集合 ϕ を要素として含むことに注意する.

例題 1.30 (べき集合)

1. $X = \{a\}$ とするとき, 2^X を外延的記法で表せ.
2. $X = \{a, b\}$ とするとき, 2^X を外延的記法で表せ.
3. $X = \{a, b, c\}$ とするとき, 2^X を外延的記法で表せ.
4. $X = \{\phi, \{a\}\}$ とするとき, 2^X を外延的記法で表せ.
5. $\{a\} \neq \{\{a\}\}$ であることに注意する.
6. $2^{\{\phi\}}$ を外延的記法で表せ. (ヒント: $X = \{a\}$ の a を ϕ に置き換えて考える.)

7. $2^{2^{\{\phi\}}}$ を外延的記法で表せ.
8. $X = \{a, b\}$ とするとき, $2^X \times X$ を外延的記法で表せ.

(解)

1. $2^X = \{\phi, X\}$.
2. $2^X = \{\phi, \{a\}, \{b\}, X\}$.
3. $2^X = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, X\}$.
4. $2^X = \{\phi, \{\phi\}, \{\{a\}\}, X\}$.
6. $2^{\{\phi\}} = \{\phi, \{\phi\}\}$.
7. $2^{2^{\{\phi\}}} = \{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\}$.
8. $2^X = \{\phi, \{a\}, \{b\}, X\}$ より, $2^X \times X = \{(\phi, a), (\phi, b), (\{a\}, a), (\{a\}, b), (\{b\}, a), (\{b\}, b), (X, a), (X, b)\}$.

定義 1.31 有限個の要素からなる集合を**有限集合**という. それ以外の集合を**無限集合**という. 有限集合 X の要素数を $|X|$ と表す.

空集合 ϕ は有限集合であり, $|\phi| = 0$ である.

有限集合 X, Y に対し, $X \cap Y = \phi$ ならば, $|X \cup Y| = |X| + |Y|$ が成り立つ. 一般に, 有限集合 $X_1, \ldots, X_n$ に対し, $X_i \cap X_j = \phi$ $(i \neq j)$ ならば, $|X_1 \cup \cdots \cup X_n| = \sum_{i=1}^{n} |X_i|$ が成り立つ.

上記のことから, 有限集合の要素数を数え上げる 1 つの方法として, それを互いに共通部分をもたない, いくつかの部分集合に分割し, それぞれの要素数を数えて足し合わせればよい. 関連する定理を以下に述べる.

定理 1.32 有限集合 X, Y に対し, 以下の等式が成り立つ.

1. $|X \cup Y| = |X| + |Y| - |X \cap Y|$. (**包除原理**)
2. $|X \times Y| = |X| \times |Y|$.
3. $|2^X| = 2^{|X|}$.

(証明)

1. 互いに共通部分をもたないような部分集合で, 集合 X, $X \cup Y$ を次のように表す. $X = (X - Y) \cup (X \cap Y)$, $X \cup Y = (X - Y) \cup Y$. それぞれより, $|X| = |X - Y| + |X \cap Y|$, $|X \cup Y| = |X - Y| + |Y|$. これらより, $|X - Y|$ の項を消すと, $|X \cup Y| = |X| + |Y| - |X \cap Y|$. ∎
2. $X \times Y$ の要素は, X と Y のそれぞれの要素 x, y の順序対 (x, y) である. x と y がとりうる値の個数はそれぞれ $|X|, |Y|$ である. したがって, それらから得られる順序対の全体の個数は $|X| \times |Y|$ となる. ゆえに, $|X \times Y| = |X| \times |Y|$. ∎
3. 仮定より, X は有限集合であるから, $X = \{x_1, \ldots, x_n\}$, $|X| = n$ としても, 一般性は失われない. X の部分集合を決める方法として, 以下のことを考える. 0 と 1 からなる集合を $B = \{0, 1\}$ とし, その n 重の直積集合を B^n とする. B^n の要素は, $(b_1, \ldots, b_n)$ という n 重対となる. そこで, $(b_1, \ldots, b_n)$ を用いて, 次のように X の部分集合を定める. b_i の値が, $b_i = 1$ ならば x_i をその部分集合に含め, $b_i = 0$ ならば x_i をその部分集合に含めないとする. この方法により, B^n の要素から過不足なく, X のすべての部分集合を定めることができる. B^n の要素数は 2^n 個であるから, すべての部分集合の個数も 2^n 個である. ゆえに, $|2^X| = 2^n = 2^{|X|}$. ∎

$|2^X| = 2^{|X|}$ となる問題は, 以下のように考えることもできる. n 個の中から k を選び出す組合せの数は, $\binom{n}{k} = {}_nC_k = \frac{n!}{(n-k)!k!}$ である. したがって, X の部分集合で要素数が k であるものは $\binom{n}{k}$ 個である. これより, X の部分集合の総数は $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ となる.

ここで, 2 項定理 $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ より, その式に $x = y = 1$ を代入することで, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ が得られる.

例題 1.33 n 個の中から k を選び出す組合せの数 $\binom{n}{k}$ が $\frac{n!}{(n-k)!k!}$ と表されることは, 良く知られている. その式には, 割算が含まれていることが分かる. では, その式の値が常に整数になるのは, なぜだろうか. この問題を解くヒントとなる事柄を以下に記載する.

1. 「k, $0 \leq k \leq n$, に対し, $\binom{n}{k}$ は整数になる」ことを示せ.
   上記を命題 $P(n)$ として, n に関する数学的帰納法で証明する方法が考えられる.
2. n 個の中から k 個を選んで得られる順列の総数は
   ${}_nP_k = n(n-1)\cdots(n-(k-1)) = \frac{n!}{(n-k)!}$.
3. n 個の中から k 個を選んで得られる組合せの総数は
   $\binom{n}{k} = {}_nC_k = \frac{{}_nP_k}{k!} = \frac{n!}{(n-k)!k!}$.
4. 「連続する k 個の自然数の積は $k!$ で割り切れる」ことを示せ.
   k に関する数学的帰納法で証明する方法が考えられる.
5. 式 $\frac{n!}{(n-k)!k!}$ において, その分子 $n!$ は連続する n 個の自然数の積である. それは, 連続する $(n-k)$ 個と k 個の自然数の積に分解できる. したがって, 上記のことが正しければ, $\frac{n!}{(n-k)!k!}$ の値は, 常に整数となることが分かる.

例題 1.34 (包除原理) 有限集合 X, Y, Z を有限集合 U の部分集合とするとき, 以下が成り立つことを示せ.

1. $|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$.
   ヒント: 2 個の集合の場合の公式を利用する.
2. $|X \cap Y| = |U| - |X^c| - |Y^c| + |X^c \cap Y^c| = |X| + |Y| + |X^c \cap Y^c| - |U|$.
3. $|X \cap Y \cap Z| = |U| - |X^c| - |Y^c| - |Z^c| + |X^c \cap Y^c| + |X^c \cap Z^c| + |Y^c \cap Z^c| - |X^c \cap Y^c \cap Z^c|$
   ヒント: 2 個の集合の場合の公式を利用する.
4. $|X^c \cap Y^c \cap Z| = |Z| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$.
5. 1 から 250 までの自然数の中で, 2 でも 7 でも割り切れず, かつ 5 で割り切れるものは, いくつあるか. 包除原理を用いて考えよ.

(解)

1. $|(X \cup Y) \cup Z| = |(X \cup Y)| + |Z| - |(X \cup Y) \cap Z| = |X| + |Y| - |X \cap Y| + |Z| - |(X \cap Z) \cup (Y \cap Z)| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$. ここで, $(X \cap Z) \cap (Y \cap Z) = X \cap Y \cap (Z \cap Z) = X \cap Y \cap Z$ より, $|(X \cap Z) \cup (Y \cap Z)| = |X \cap Z| + |Y \cap Z| - |(X \cap Z) \cap (Y \cap Z)| = |X \cap Z| + |Y \cap Z| - |X \cap Y \cap Z|$ となることを使った. ∎
2. $U = (X \cup Y) \cup (X \cup Y)^c = (X \cup Y) \cup (X^c \cap Y^c)$, $U = X \cup X^c$, $U = Y \cup Y^c$. これらより, $|U| = |X \cup Y| + |X^c \cap Y^c| = |X| + |Y| - |X \cap Y| + |X^c \cap Y^c|$. ゆえに, $|X \cap Y| = |X| + |Y| + |X^c \cap Y^c| - |U| = |U| - |X^c| - |Y^c| + |X^c \cap Y^c|$. ∎
3. $|(X \cap Y) \cap Z| = |U| - |(X \cap Y)^c| - |Z^c| + |(X \cap Y)^c \cap Z^c|$. そこで, $|(X \cap Y)^c| = |X^c \cup Y^c| = |X^c| + |Y^c| - |X^c \cap Y^c|$ と $|(X \cap Y)^c \cap Z^c| = |(X^c \cup Y^c) \cap Z^c| = |(X^c \cap Z^c) \cup (Y^c \cap Z^c)| = |X^c \cap Z^c| + |Y^c \cap Z^c| - |(X^c \cap Z^c) \cap (Y^c \cap Z^c)| = |X^c \cap Z^c| + |Y^c \cap Z^c| - |X^c \cap Y^c \cap Z^c|$ より, $|(X \cap Y) \cap Z| = |U| - |X^c| - |Y^c| - |Z^c| + |X^c \cap Y^c| + |X^c \cap Z^c| + |Y^c \cap Z^c| - |X^c \cap Y^c \cap Z^c|$. ∎
4. 集合 $X \cup Y \cup Z$ は共通部分もたない部分集合の和集合で次のように書ける. $(X \cup Y) \cup Z = (X^c \cap Y^c \cap Z) \cup (X \cup Y)$. これより, $|X \cup Y \cup Z| = |X^c \cap Y^c \cap Z| + |X \cup Y| = |X^c \cap Y^c \cap Z| + |X| + |Y| - |X \cap Y|$. そして, $|X \cup Y \cup Z|$ の公式を用いて, $|X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z| = |X^c \cap Y^c \cap Z| + |X| + |Y| - |X \cap Y|$ となる. これを整理すると, $|X^c \cap Y^c \cap Z| = |Z| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$ となる. ∎
5. $U = \{1, \ldots, 250\}$, $X = \{x \mid x \in U, x \text{ は } 2 \text{ で割り切れる }\}$, $Y = \{y \mid y \in U, y \text{ は } 7 \text{ で割り切れる }\}$, $Z = \{z \mid z \in U, z \text{ は } 5 \text{ で割り切れる }\}$. このとき, 求める集合は $X^c \cap Y^c \cap Z$ と表すことができる. $|Z| = 50$, $|X \cap Z| = 25$, $|Y \cap Z| = 7$, $|X \cap Y \cap Z| = 3$. ゆえに, $|X^c \cap Y^c \cap Z| = 50 - 25 - 7 + 3 = 21$ となる. ∎

$|X \cup Y| = |X| + |Y| - |X \cap Y|$ を**包除原理**とよび, 一般に, 集合 $X_1, \ldots, X_n$ に対し, 以下が成り立つ.

$$|X_1 \cup \cdots \cup X_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} |X_{i_1} \cap \cdots \cap X_{i_k}|.$$

また, 直積集合に関しても, $|X_1 \times \cdots \times X_n| = |X_1| \times \cdots \times |X_n|$ が成り立つ.

2 写像

2.1 写像の定義

定義 2.1 X, Y を空でない集合とする.

1. X の各要素に対し, Y の要素が一つずつ対応するとき, この対応を**写像**という.
2. 写像の名前を f とするとき, "$f : X \longrightarrow Y$" または "$X \xrightarrow{f} Y$" と表し, f は X **から** Y **への写像**であるという. X を f の**始集合**, Y を**終集合**とよぶ. 始集合を**定義域**ともいう.
3. f によって $x \in X$ に対応する Y の要素を $f(x)$ と表し, x における f の**値**という. このとき, "$f : x \longmapsto f(x)$" と表す.

写像に関して大切なことは, X のどの要素 x に対しても, その値 $f(x)$ が必ず, しかし唯 1 つ定義されていなければならない.

写像と (1 価) 関数は, ほとんど同義語であるが, 関数というときは, 始集合や終集合が実数や複素数などの数の集合であることが多い.

例題 2.2 図 2 は, $X = \{x_1, x_2, x_3, x_4, x_5\}$, $Y = \{y_1, y_2, y_3, y_4\}$, $f : X \longrightarrow Y$, $f(x_1) = y_2$, $f(x_2) = f(x_4) = y_1$, $f(x_3) = f(x_5) = y_4$ という写像を表している.

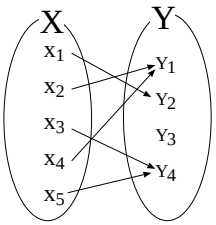


図 2: $f : X \longrightarrow Y$

2.2 単射, 全射, 全単射, 逆写像

定義 2.3 1. $f : X \longrightarrow Y$, $g : X \longrightarrow Y$ とする. f と g が**等しい**とは, 任意の $x \in X$ に対して $f(x) = g(x)$ が成り立つことをいう. f と g が等しいことを $f = g$ と表す.

2. $f : X \longrightarrow Y$ が**定値写像**であるとは, 任意の $x, y \in X$ に対して $f(x) = f(y)$ が成り立つことをいう.
3. $f : X \longrightarrow X$ が**恒等写像**であるとは, 任意の $x \in X$ に対して $f(x) = x$ が成り立つことをいう.
4. $f : X \longrightarrow Y$ が**単射**, あるいは 1 **対** 1 **写像**であるとは, "任意の $x_1, x_2 \in X$ に対し, $x_1 \neq x_2$ ならば $f(x_1) \neq f(x_2)$ が成り立つ" ことをいう. (あるいは, その対偶となる, $f(x_1) = f(x_2)$ ならば $x_1 = x_2$ が成り立つことをいう.)
5. $f : X \longrightarrow Y$ が**全射**, あるいは X から Y の**上への写像**であるとは, "任意の $y \in Y$ に対し, $f(x) = y$ となるような $x \in X$ が存在する" ことをいう.
6. 全射であり, かつ単射である写像を**全単射**という. 集合 X からそれ自身への全単射を X 上の**置換**ともいう.

例題 2.4 図 3 に, 写像 $f : X \longrightarrow Y$ の例を示す.

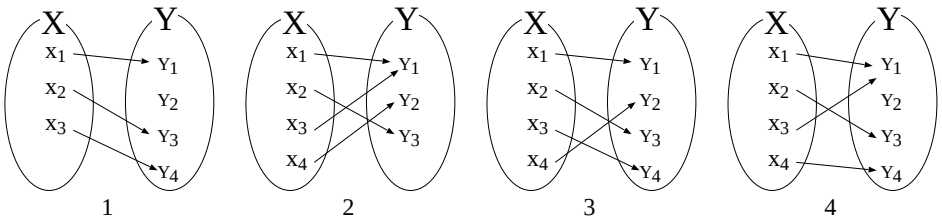


図 3: 1. 単射 (全射ではない), 2. 全射 (単射ではない), 3. 全単射, 4. 全射でも単射でもない写像.

定義 2.5 写像 $f : X \longrightarrow Y$ が全単射であるとき, 任意の $y \in Y$ に対し, $f(x) = y$ となる $x \in X$ が唯 1 つ定まる. $y \in Y$ に, このような $x \in X$ を対応させる Y から X への写像を f の**逆写像**とよび, f^{-1} と表す. すなわち, $f(x) = y$ のとき, かつそのときに限り, $f^{-1}(y) = x$ である.

例題 2.6 図 4 に, 全単射である写像 $f : X \longrightarrow Y$ とその逆写像 $f^{-1} : Y \longrightarrow X$ の例を示す.

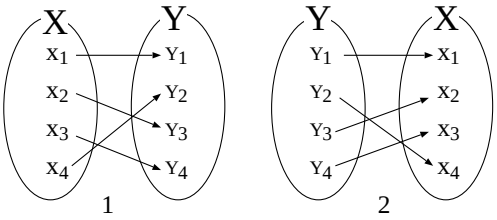


図 4: 1. $f : X \longrightarrow Y$, 2. $f^{-1} : Y \longrightarrow X$.

例題 2.7 全単射 f の逆写像 f^{-1} は全単射であることを示せ.
(証明) $f : X \longrightarrow Y$ とすると, $f^{-1} : Y \longrightarrow X$. 全射) 任意の $x \in X$ に対し, $x = f^{-1}(y)$ となる $y \in Y$ が存在することを示せばよい. f は全単射であるから, この x に対し, $f(x) = y \in Y$ となる y が一意に定まる. ゆえに, 任意の $x \in X$ に対し, $x = f^{-1}(y)$ となる $y \in Y$ が存在する. 単射) 任意の $y_1, y_2 \in Y$ に対し, $f^{-1}(y_1) = f^{-1}(y_2)$ ならば $y_1 = y_2$ となることを示せばよい. 逆写像の定義より, $f(x_1) = y_1$, $f(x_2) = y_2$ となる $x_1, x_2 \in X$ が唯 1 つ定まる. $f^{-1}(y_1) = f^{-1}(y_2)$ ならば $x_1 = f^{-1}(y_1) = f^{-1}(y_2) = x_2$ より $x_1 = x_2$ である. したがって, $x = x_1 = x_2$ とすれば $y_1 = f(x) = y_2$ より $y_1 = y_2$. ゆえに, 任意の $y_1, y_2 \in Y$ に対し, $f^{-1}(y_1) = f^{-1}(y_2)$ ならば $y_1 = y_2$ となる. 以上より, f^{-1} は全単射である. ∎

2.3 写像による像および逆像

定義 2.8 X, Y を空でない集合とし, f を写像 $f : X \longrightarrow Y$ とする.

1. X の部分集合 A に対し,
   $F(A) := \{f(x) \in Y \mid x \in A\}$
   $= \{y \mid y \in Y,\ y = f(x)$ を満たす $x \in A$ が存在する $\}$
   を A の f による**像**という. 特に, $F(X)$ を f の**値域像**という.
2. Y の部分集合 B に対し,
   $F^{-1}(B) := \{x \in X \mid f(x) \in B\}$
   を B の f による**原像**, あるいは**逆像**という.

F と F^{-1} は f と f^{-1} とは異なる. $f : X \longrightarrow Y$ に対し, $F : 2^X \longrightarrow 2^Y$ である. また, $f^{-1} : Y \longrightarrow X$ に対し, $F^{-1} : 2^Y \longrightarrow 2^X$ である. しかし, 記号 F を定義するのに用いた f と同じ記号 f で表し, 記号 F^{-1} をもとの写像 f の逆写像 f^{-1} と同じ記号 f^{-1} で表す習慣がある. 本稿でも, 以下では, 混乱が生じない限り, F, F^{-1} に対し, それぞれ f, f^{-1} を用いる.

例題 2.9 $X = \{1,2,3,4,5\}$, $Y = \{x,y,z,w\}$ とする. 写像 $f : X \longrightarrow Y$ を図 5 のように定義する. このとき, $f(\{1,2,4\})$, $f(\{1,3,5\})$, $f^{-1}(\{x,y,w\})$, $f^{-1}(\{y,z\})$ をそれぞれ外延的記法で表せ.

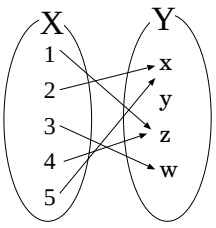


図 5: $f : X \longrightarrow Y$

(解) $f(\{1,2,4\}) = \{x,z\}$, $f(\{1,3,5\}) = \{x,z,w\}$, $f^{-1}(\{x,y,w\}) = \{2,5,3\}$, $f^{-1}(\{y,z\}) = \{1,4\}$.

定理 2.10 X,Y を空でない集合とし, $f : X \longrightarrow Y$ とする. X の任意の部分集合 A,B に対し, 以下のことを示せ.

1. $A \subseteq B$ ならば $f(A) \subseteq f(B)$.
2. $f(A \cup B) = f(A) \cup f(B)$.
3. $f(A \cap B) \subseteq f(A) \cap f(B)$.
4. $f(X - A) \supseteq f(X) - f(A) (= f(X) \cap (f(A))^c)$.
5. $f^{-1}(f(A)) \supseteq A$.

(証明)

1. 任意の $y \in f(A)$ に対し, $f(A)$ の定義より, $f(x) = y$ となる $x \in A$ が存在する. 仮定より, $x \in A \subseteq B$ であるから, $x \in B$. ゆえに, $f(B)$ の定義より, $y = f(x) \in f(B)$.
2. $\subseteq$) 任意の $y \in f(A \cup B)$ に対し, $f(x) = y$ となる $x \in A \cup B$ が存在する. $x \in A$ ならば $y \in f(A)$. また, $x \in B$ ならば $y \in f(B)$. ゆえに, $y \in f(A) \cup f(B)$. $\supseteq$) 任意の $y \in f(A) \cup f(B)$ に対し, $y \in f(A)$ ならば $f(x) = y$ となる $x \in A$ が存在する. また, $y \in f(B)$ ならば $f(x) = y$ となる $x \in B$ が存在する. したがって, $x \in A \cup B$ であり, $y = f(x) \in f(A \cup B)$.
3. 任意の $y \in f(A \cap B)$ に対し, $f(x) = y$ となる $x \in A \cap B$ が存在する. $x \in A$ かつ $x \in B$ より, $y \in f(A)$ かつ $y \in f(B)$. ゆえに, $y \in f(A) \cap f(B)$.
   ($X = \{1,2\}, Y = \{y\}$ とし, X から Y への写像 f を $f(1) = f(2) = y$ とする例により, 一般に, 左辺 $\supseteq$ 右辺 が成り立たないことが分かる.)

4. 任意の $y \in (f(X) - f(A))$ に対し, $y \in f(X)$ かつ $y \notin f(A)$. すなわち, $f(x) = y$ とすると, $x \in X$ かつ $x \notin A$. $x \notin A$ より, $x \in A^c$. したがって, $x \in X \cap A^c = X - A$. ゆえに, $y = f(x) \in f(X - A)$.

   (上記と同じ例により，一般に，左辺 $\subseteq$ 右辺 が成り立たないことが分かる．)

5. 任意の $a \in A$ に対し, $f(a) \in Y$ である. $f(A)$ の定義より, $f(a) \in f(A)$. 次に, $B = f(A)$ と表すと, $f(a) \in F(A) = B$ であるから, $f^{-1}(f(A))$ の定義より, $a \in \{x \mid f(x) = y \in B\} = f^{-1}(B) = f^{-1}(f(A))$. 以上より, $a \in A$ ならば $a \in f^{-1}(f(A))$ が言えた. ゆえに, $f^{-1}(f(A)) \supseteq A$ が成り立つ.

   (f が単射ならば $f^{-1}(f(A)) = A$ が成り立つ.) $\supseteq$) が成り立つことは上記の証明から明らか. $\subseteq$) を示す. $B = f(A)$ とする. 任意の $a \in f^{-1}(f(A)) = f^{-1}(B)$ に対し, $f^{-1}(B)$ の定義より, $f(a) \in B$. 次に, $f(A)$ の定義より, $f(a) = f(x)$ となる $x \in A$ が存在する. そこで, f は単射であるから, $f(a) = f(x)$ ならば $a = x$ であるから, $a = x \in A$ となる. したがって, $a \in f^{-1}(f(A))$ ならば $a \in A$ が言えるので, $f^{-1}(f(A)) \subseteq A$ が成り立つ. 以上より, $\supseteq$ と $\subseteq$ の両方が成り立つから, $(f(A)) = A$ が成立する.

定理 2.11 X,Y を空でない集合とし, $f : X \longrightarrow Y$ とする. Y の任意の部分集合 A,B に対し, 以下のことを示せ.

1. $A \subseteq B$ ならば $f^{-1}(A) \subseteq f^{-1}(B)$.
2. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
3. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
4. $f^{-1}(Y - B) = f^{-1}(Y) - f^{-1}(B)(= f^{-1}(Y) \cap (f^{-1}(B))^c)$.
5. $f(f^{-1}(B)) \subseteq B$.

(証明)

1. 任意の $x \in f^{-1}(A)$ に対し, $f^{-1}(A)$ の定義より, $f(x) \in A$. 仮定より, $f(x) \in A \subseteq B$ であるから, $f(x) \in B$. ゆえに, $f^{-1}(B)$ の定義より, $x \in f^{-1}(B)$.
2. $\subseteq$) 任意の $x \in f^{-1}(A \cup B)$ に対し, $f^{-1}(A \cup B)$ の定義より, $f(x) \in A \cup B$. $f(x) \in A$ ならば $x \in f^{-1}(A)$. また, $f(x) \in B$ ならば $x \in f^{-1}(B)$. 以上より, $x \in f^{-1}(A) \cup f^{-1}(B)$. $\supseteq$) 任意の $x \in f^{-1}(A) \cup f^{-1}(B)$ に対し, $f^{-1}(A)$ の定義より, $x \in f^{-1}(A)$ ならば $f(x) \in A$. また, $f^{-1}(B)$ の定義より, $x \in f^{-1}(B)$ ならば $f(x) \in B$. したがって, $f(x) \in A \cup B$. ゆえに, $f^{-1}(A \cup B)$ の定義より, $x \in f^{-1}(A \cup B)$.
3. $\subseteq$) 任意の $x \in f^{-1}(A \cap B)$ に対し, $f^{-1}(A \cap B)$ の定義より, $f(x) \in A \cap B$. したがって, $f(x) \in A \cap B$ ならば $x \in f^{-1}(A)$ かつ $x \in f^{-1}(B)$. ゆえに, $x \in f^{-1}(A) \cap f^{-1}(B)$. $\supseteq$) 任意の $x \in f^{-1}(A) \cap f^{-1}(B)$ に対し, $f^{-1}(A)$ と $f^{-1}(B)$ の定義より, $f(x) \in A$ かつ $f(x) \in B$. したがって, $f(x) \in A \cap B$. ゆえに, $f^{-1}(A \cap B)$ の定義より, $x \in f^{-1}(A \cap B)$.
4. $\subseteq$) 任意の $x \in f^{-1}(Y - B)$ に対し, $f^{-1}(Y - B)$ の定義と差集合の定義より, $f(x) \in Y - B = Y \cap B^c$. すなわち, $f(x) \in Y$ かつ $f(x) \in B^c$. $f^{-1}(Y)$ の定義より, $x \in f^{-1}(Y)$. また, $f(x) \in B^c$ ならば $f(x) \notin B$. さらに, f^{-1} の定義より, $f(x) \notin B$ ならば $x \notin f^{-1}(B)$. したがって, $x \in (f^{-1}(B))^c$. ゆえに, $x \in f^{-1}(Y)$ かつ $x \in (f^{-1}(B))^c$. 以上より, $x \in f^{-1}(Y) \cap (f^{-1}(B))^c = f^{-1}(Y) - f^{-1}(B)$.

   $\supseteq$) 任意の $x \in f^{-1}(Y) - f^{-1}(B) = f^{-1}(Y) \cap (f^{-1}(B))^c$ に対し, f^{-1} の定義より, $f(x) \in Y$. $x \in (f^{-1}(B))^c$ より, $x \notin f^{-1}(B)$ であり, f^{-1} の定義より, $f(x) \notin B$. すなわち, $f(x) \in B^c$. したがって, $f(x) \in Y$ かつ $f(x) \in B^c$. ゆえに, $f(x) \in Y \cap B^c = Y - B$. 最後に, f^{-1} の定義より, $x \in f^{-1}(Y - B)$.
5. $A = f^{-1}(B)$ とする. 任意の $b \in f(f^{-1}(B)) = f(A)$ に対し, $f(A)$ の定義より, $f(a) = b$ となる $a \in A = f^{-1}(B)$ が存在する. 次に, $f^{-1}(B)$ の定義より, $b = f(a) \in B$. 以上より, $b \in f(f^{-1}(B))$ ならば $b \in B$ が言えた. ゆえに, $f(f^{-1}(B)) \subseteq B$ が成り立つ.

   (f が全射ならば, $f(f^{-1}(B)) = B$ が成り立つ.) $\subseteq$) が成り立つことは上記証明より明らか. 次に, $\supseteq$) を示す. $A = f^{-1}(B)$ とする. 任意の $b \in B \subseteq Y$ に対し, f は全射であるか

ら, $f(a) = b \in B$ となる $a \in X$ が存在する. さらに, $f^{-1}(B)$ の定義より, $f(a) \in B$ ならば $a \in f^{-1}(B) = A$. 次に, $f(A)$ の定義より, $a \in A$ ならば $b = f(a) \in A = f(f^{-1}(B))$ である. したがって, $b \in B$ ならば $b \in f(f^{-1}(B))$ が言えるので, $f(f^{-1}(B)) \supseteq B$ が成り立つ. 以上より, $\subseteq$ と $\supseteq$ の両方が成り立つから, $f(f^{-1}(B)) = B$ が成立する.

例題 2.12 $X = \{1,2,3,4,5,6\}$, $Y = \{x,y,z,u\}$ とする. 写像 $f : X \longrightarrow Y$ を図 6 のように定義する.

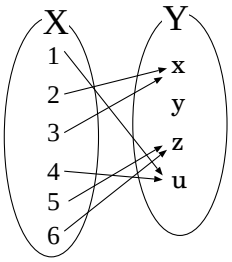


図 6: $f : X \longrightarrow Y$

1. $A = \{2,4,5\}$, $B = \{1,4,6\} \subseteq X$ とするとき, $f(A \cup B) = f(A) \cup f(B)$, $f(A \cap B) \subseteq f(A) \cap f(B)$ が成り立つことを確かめよ.
2. $A = \{x,y\}$, $B = \{y,u\} \subseteq Y$ とするとき, $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ が成り立つことを確かめよ.

2.4 合成写像

定義 2.13 X, Y, Z を空でない集合とする. 写像 $X \xrightarrow{f} Y \xrightarrow{g} Z$ に対し, それらの**合成写像** $X \xrightarrow{g \circ f} Z$ を, $x \in X$ に対し, $(g \circ f)(x) := g(f(x))$ と定義する.

例題 2.14 $X = \{x_1, x_2, x_3\}$, $Y = \{y_1, y_2, y_3, y_4\}$, $Z = \{z_1, z_2, z_3\}$ とする. 写像 $X \xrightarrow{f} Y \xrightarrow{g} Z$ を図 7 のように定義する. $(g \circ f)(x_1)$, $(g \circ f)(x_2)$, $(g \circ f)(x_3)$ を求めよ.

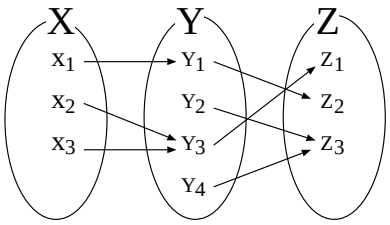


図 7: $f : X \longrightarrow Y$

(解答) $(g \circ f)(x_1) = g(f(x_1)) = g(y_1) = z_2$ より, $(g \circ f)(x_1) = z_2$. 同様にして, $(g \circ f)(x_2) = (g \circ f)(x_3) = z_1$.

定理 2.15 X, Y, Z, W を空でない集合とする. 写像 $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$ に対し, $(h \circ g) \circ f = h \circ (g \circ f)$ が成り立つ. すなわち, 結合律が成り立つ.
(証明) 任意の $x \in X$ に対し, $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$ が成り立つことを示せばよい.
$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

例題 2.16 写像 $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ がそれぞれ全単射ならば, 次のことが成り立つことを示せ.

1. $g \circ f$ は全単射
2. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

(証明)2. まず，$g \circ f$ は全単射であるから逆写像 $(g \circ f)^{-1}$ を定義でき，$z \in Z$ に対し，$(g \circ f)^{-1}(z) = x$ とする．すなわち，$z = (g \circ f)(x) = g(f(x))$. g は全単射であるから，$g^{-1}(z) = f(x)$. さらに，f も全単射であることより，$f^{-1}(g^{-1}(z)) = x$. したがって，$x = f^{-1}(g^{-1}(z)) = (f^{-1} \circ g^{-1})(z)$. ゆえに，$(g \circ f)^{-1}(z) = x = (f^{-1} \circ g^{-1})(z)$ が成り立つ． ∎

例題 2.17 X, Y, Z を空でない集合とし, $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ とする．このとき, 次のことが成り立つことを示せ.

1. $g \circ f$ が単射ならば, f は単射である．
2. $g \circ f$ が全射ならば, g は全射である．
3. $g \circ f$ が単射, かつ f が全射ならば, g は単射である．
4. $g \circ f$ が全射, かつ g は単射ならば, f は全射である．

(証明)

1. 任意の $a, b \in X$ に対し，$f(a) = f(b)$ ならば，$g(f(a)) = g(f(b))$ であり，$g \circ f$ は単射であるという仮定より，$a = b$ である．ゆえに，$f(a) = f(b)$ ならば $a = b$ が言えるので，f は単射である．
2. $g \circ f$ が全射であることより，任意の $z \in Z$ に対し，$(g \circ f)(x) = z$ となる $x \in X$ が存在する．すると，$z = (g \circ f)(x) = g(f(x))$ となる $y = f(x) \in Y$ が存在する．ゆえに，$z \in Z$ に対し，$g(y) = g(f(x)) = z$ となる $y \in Y$ が存在することより，g は全射である．
3. 任意の $y_1, y_2 \in Y$ に対し，$g(y_1) = g(y_2)$ ならば $y_1 = y_2$ を示せばよい．f は全射であるから，$y_1, y_2 \in Y$ に対し，$f(x_1) = y_1, f(x_2) = y_2$ となる $x_1, x_2 \in X$ が存在する．一方，$g(y_1) = z_1, g(y_2) = z_2$ とすると，$g \circ f$ は単射であるから，$z_1 = z_2$ ならば $x_1 = x_2$ である．したがって，$y_1 = f(x_1) = f(x_2) = y_2$ となる．すなわち，$g(y_1) = z_1 = z_2 = g(y_2)$ ならば $y_1 = y_2$. ゆえに，g は単射である．
4. 任意の $y \in Y$ に対し，$f(x) = y$ となる $x \in X$ が存在することを示せばよい．$y \in Y$ に対し，$g(y) = z \in Z$ とする．$g \circ f$ は全射であるから $z \in Z$ に対し，$(g \circ f)(x) = z$ となる $x \in X$ が存在する．このとき，$g(f(x)) = z = g(y)$ であり，g は単射であることより，$f(x) = y$. したがって，$y \in Y$ に対し，$f(x) = y$ となる $x \in X$ が存在する．ゆえに，f は全射である．

定義 2.18 X を空でない集合とする．このとき, $X \times X$ から X への写像を X 上の **2 項演算**という．

実数の加法 “+” や乗法 “×” は, 2 つの実数に対して 1 つの実数を対応させる写像である．したがって, これらは $\mathbf{R}$ 上の 2 項演算である．

2.5 写像の集合, 鳩の巣原理

定義 2.19 集合 X から集合 Y への写像の全体からなる集合を
$Y^X := \{f \mid f : X \longrightarrow Y\}$
と表す.

例題 2.20 $X = \{x_1, x_2\}$, $Y = \{y_1, y_2\}$ に対し, 集合 Y^X を外延的記法で表せ.
(解答) $Y^X = \{f_1, f_2, f_3, f_4\}$. ただし, f_1, f_2, f_3, f_4 は図 8 のような写像である.

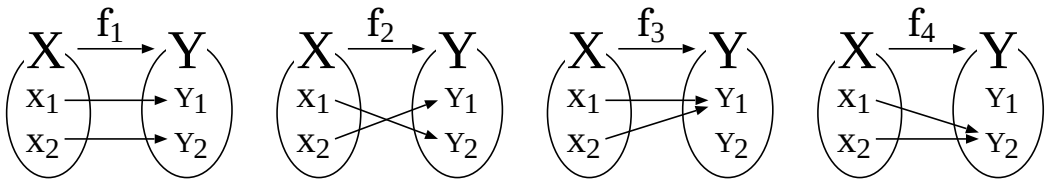


図 8: 写像 f_1, f_2, f_3, f_4.

定理 2.21 X,Y を空でない有限集合とし, $|X| = m$, $|Y| = n$ とする. X から Y への写像の数に関し, 以下のことが成り立つ.

1. 写像の総数 : $|\{f \mid f : X \longrightarrow Y\}| = |Y^X| = n^m = |Y|^{|X|}$
2. 単射の総数 : $|\{f \mid f : X \longrightarrow Y,\ f \text{ は単射 }\}|$
$$= \begin{cases} n(n-1)(n-2)\cdots(n-(m-1)) = \frac{n!}{(n-m)!}, & (m \leq n) \\ 0, & (m > n) \end{cases}$$
3. 全射の総数 : $|\{f \mid f : X \longrightarrow Y,\ f \text{ は全射 }\}|$
$$= \begin{cases} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^m, & (m \geq n) \\ 0, & (m < n) \end{cases}$$

(証明) X, Y は有限集合であるから, $X = \{x_1, \ldots, x_m\}$, $Y = \{y_1, \ldots, y_n\}$ としても一般性は失われない.

1. 各 x_i に対し, $f(x_i) = y_j$ となる対応を指定することで写像は定まる. x_i に対し, そのような対応を指定する仕方は n 通り. したがって, m 個の x_i, $i = 1, \ldots, m$ に対し, $f(x_i) = y_j$ の値を定める組合せは n^m 通りある. ゆえに, $|Y^X| = n^m = |Y|^{|X|}$.
2. 単射であるから, 任意の $x_1, x_2 \in X$ に対し, $x_1 \neq x_2$ ならば $f(x_1) \neq f(x_2)$. したがって, これを満たすには, $m \leq n$ でなければならない. したがって, $m > n$ のときには 0 個となる. $m \leq n$ の場合について考える. 求める個数は, x_1 から x_m に対し, 順に $f(x_1), \ldots, f(x_m)$ の値を $y_1, \ldots, y_n$ の中から定める数である. ただし, 単射であるから $x_1 \neq x_2$ ならば $f(x_1) \neq f(x_2)$ を満たす必要がある. すなわち, n 個の中から m 個を順に取り出す順列の数である. ゆえに, 求める個数は, $n(n-1)(n-2)\cdots(n-(m-1)) = \frac{n!}{(n-m)!}$ となる.
3. 全射であるから, 任意の $y \in Y$ に対し, $f(x) = y$ となる $x \in X$ が存在する. $m < n$ であるとすると, $y_1 \neq y_2$ である $y_1, y_2 \in Y$ に対し, $y_1 = f(x) = y_2$ となる $x \in X$ が少なくとも 1 つは存在することになる. しかし, これは, 写像の定義である, $f(x)$ の値が唯 1 つ定まるということに矛盾する. ゆえに, $m < n$ のときは, 0 個である. $m \geq n$ の場合については, 別途示す.

系 2.22 X, Y を空でない有限集合とする.

1. "X から Y への単射が存在する" ことと, "$|X| \leq |Y|$" は同値である.
2. "X から Y への全射が存在する" ことと, "$|X| \geq |Y|$" は同値である.
3. "X から Y への全単射が存在する" ことと, "$|X| = |Y|$" は同値である.

(証明)

1. 単射が存在するならば, その個数は 1 以上であるから, $|X| > |Y|$ ではない. すなわち, $|X| \leq |Y|$ である. 逆に, $|X| \leq |Y|$ ならば, $|Y|!/(|Y| - |X|)!(> 0)$ 個の単射を定義できるので, 単射が存在する.

2. 全射が存在するならば, その個数は 1 以上であるから, $|X| < |Y|$ ではない. すなわち, $|X| \geq |Y|$ である. 逆に, $|X| \geq |Y|$ ならば, 上記定理より, $\sum_{k=0}^{|Y|}(-1)^{|Y|-k}\binom{|Y|}{k}k^{|X|}(> 0)$ 個の全射を定義できるので, 全射が存在する.
3. 全単射が存在するならば, 上記 1,2 より, $|X| = |Y|$ である. 逆に, $|X| = |Y|$ ならば, $X = \{x_1, \ldots, x_{|X|}\}$, $Y = \{y_1, \ldots, y_{|X|}\}$ に対し, $f(x_i) = y_i$, $i = 1, \ldots, |X|$ とすることで, f は全単射となる. ゆえに, 全単射が存在する.

鳩の巣原理: $|X| > |Y|$ ならば X から Y への単射は存在しない. したがって, $f(x_1) = f(x_2)$ となる, 異なる $x_1, x_2 \in X$ が存在する. これを, 一般に, **鳩の巣原理**という.

実数 x に対し, x 以上の最小の整数を $\lceil x \rceil$ と表し, x の天井 (ceiling) という. 一方, x 以下の最大の整数を $\lfloor x \rfloor$ と表し, x の床 (floor) という. たとえば, $x = 2.3$ ならば, $\lceil 2.3 \rceil = 3$, $\lfloor 2.3 \rfloor = 2$ となる. このとき, $\lceil x \rceil - x < 1$, $x - \lfloor x \rfloor < 1$ が成り立つことに注意する.

定理 2.23 X, Y を空でない有限集合とする. $k = \lceil \frac{|X|}{|Y|} \rceil$ とするとき, X から Y への任意の写像 f に対し, $f(x_1) = \cdots = f(x_k)$ を満たす k 個の異なる $x_1, \ldots, x_k$ が存在する.
(証明) 背理法を用いて証明する. $|X| > |Y|$ とする. このとき, $k > 0$ である. X から Y への任意の写像 f に対し, $f(x_1) = \cdots = f(x_k)$ を満たす k 個の異なる $x_1, \ldots, x_k$ が存在しないと仮定する. すなわち, すべて k 個より少ないとする. すると, $|X| \leq (k-1)|Y| = (\lceil \frac{|X|}{|Y|} \rceil - 1)|Y| < \frac{|X|}{|Y|}|Y| = |X|$ より, $|X| < |X|$ となり, 矛盾. ゆえに, $f(x_1) = \cdots = f(x_k)$ を満たす k 個の異なる $x_1, \ldots, x_k$ が存在する.

例題 2.24 13 人以上の人がいれば, 必ず同じ生まれ月の人がいることを示せ.
(解答) 13 人以上の人の集合を X, 月の集合を $Y = \{1, \ldots, 12\}$ とする. そして, X に属する人に, その生まれ月を対応させる写像を考える. $|X| \geq 13 > 12 = |Y|$ であるから, 鳩の巣原理の定理より, 少なくとも $\lceil \frac{13}{12} \rceil = 2$ 人の人が同じ生まれ月になる.

定理 2.25 X, Y を空でない有限集合とし, $|X| = |Y|$ とする. このとき, X から Y への写像が全射であることと, 単射であることは同値である.
(証明) 写像を f とする. 全射 $\rightarrow$ 単射) 全射より, 任意の $y \in Y$ に対し, $f(x) = y$ となる $x \in X$ が存在する. そこで, $f(x_1) = f(x_2)$ かつ $x_1 \neq x_2$ となる $x_1, x_2 \in X$ が存在すると仮定すると, $|X| > |Y|$ となる. これは, $|X| = |Y|$ に矛盾. ゆえに, $f(x_1) = f(x_2)$ ならば $x_1 = x_2$ である. すなわち, f は単射である. 全射 $\leftarrow$ 単射) 単射より, $x_1 \neq x_2$ となる任意の $x_1, x_2 \in X$ に対し, $f(x_1) \neq f(x_2)$ である. $|X|$ 個の $f(x) \in Y$ はすべて異なり $|X|$ 個ある. $|X| = |Y|$ であるから $Y = \{f(x_i) \mid i = 1, \ldots, |X|,$ もし $i \neq j$ ならば $f(x_1) \neq f(x_2)\}$ と定めることができる. ゆえに, 任意の $y \in Y$ に対し, $f(x) = y$ となる $x \in X$ が存在する. すなわち, f は全射である.

集合 X から集合 Y への全単射が存在するとき, X と Y は**対等**であるという. 対等な集合は等しい**濃度**をもつという. 集合 X の濃度を $|X|$ と表す. 有限集合の濃度 $|X|$ は元の個数を表す. したがって, 集合の濃度という概念は, 元の個数という概念の拡張である.

自然数または 0 で表される有限集合の濃度を**有限の濃度**といい, 無限集合の濃度を**無限の濃度**という. 自然数全体の集合 $\mathbb{N}$ の濃度は, 1 つの無限の濃度である. これを**可算の濃度**といい, 記号 $\aleph_0$ と表す. ($\aleph_0$ はアレフ・ゼロとよむ) 実数全体の集合 $\mathbb{R}$ の濃度も 1 つの無限の濃度である. これを**連続の濃度**といい, 記号 $\aleph$ と表す. ($\aleph$ はアレフとよむ)

濃度 $\aleph_0$ をもつ集合を**可算集合**といい, 自然数全体の集合 $\mathbb{N}$ 以外に, 整数数全体の集合 $\mathbb{Z}$ や有理数全体の集合 $\mathbb{Q}$ も可算集合であることが証明できる.

有限集合 X, Y に対し, 系 2.22 より, X と Y が等しい濃度をもつことと, $|X| = |Y|$ は同値である.

集合 X から集合 Y への全射が存在するとき, $|X|$ は $|Y|$ 以上であるといい, $|X| \geq |Y|$ と表す. $|X| \geq |Y|$ かつ $|X| \neq |Y|$ のとき, $|X|$ は $|Y|$ より大きいといい, $|X| > |Y|$ と表す.

濃度が $|X| < \aleph_0$ であるような集合 X を, **たかだか可算な集合**という. 可算の濃度 $\aleph_0$ と連続の濃度 $\aleph$ との関係として, $\aleph_0 < \aleph$ が成り立つことが証明できる.

さらに, 任意の集合 X に対し, 集合 X とベキ集合 2^X の濃度に関しては, $|X| < |2^X|$ が成り立つことが証明できる. つまり, いかなる濃度に対しても, それより大きい濃度が必ず存在することが証明されている.

例題 2.26 空でない有限集合 X, Y に対し，$|X| = m, |Y| = n$ とする. このとき，X から Y への全射の総数は $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m$ と書けることを，以下に厳密な証明ではないが，スケッチする.

1. まず，X から Y への写像の総数は n^m である.
2. 要素数 m の集合 X から要素数 k の部分集合 $B(\subseteq Y)$ への全射の総数を $F(m,k)$ と表す.
3. このとき，n^m 個の写像の中で値域 (終集合) が要素数 k 個の部分集合 $B \subseteq Y$ になるような写像の総数は $\binom{n}{k}F(m,k)$ である.
4. したがって，写像の総数は $n^m = \sum_{k=1}^{n}\binom{n}{k}F(m,k)$ と書ける.
5. すると，$F(m,n) = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m$ を n に関する数学的帰納法で証明できる. 方針は，$n = 1$ のとき，正しいことを示し，$n-1$ まで，正しいと仮定する. テクニカルな式変換を用いることで次式を示すことができ，n のときでも，正しいことを示すことができる. (テクニカルな部分の内容は，文献 [2] の第 1 章末の問題 19(p.41) の解答に書かれいるものを参照.)

$$F(m,n) = n^m - \sum_{j=1}^{n-1}\binom{n}{j}F(m,j) = n^m - \sum_{j=1}^{n-1}\binom{n}{j}\left(\sum_{k=0}^{j}(-1)^{j-k}\binom{j}{k}k^m\right) = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m.$$

例題 2.27 有限集合 X の分割とは X の部分集合を要素とする集合 $\{A_1, \ldots, A_n\}$ で, 次の条件を満たすもののことである.

1. $A_i \neq \phi$ $(i = 1, \ldots, n)$,
2. $\cup_{i=1}^{n} A_i = X$,
3. $i \neq j \rightarrow A_i \cap A_i = \phi$.

各 A_i を分割ブロックという. X から集合 $\{1, \ldots, n\}$ への全射の総数を与える公式を用いて, X を n 個のブロックに分ける分割の総数を示せ.

(解) $\frac{1}{n!}F(|X|, n)$.

3 論理

3.1 命題論理

3.1.1 命題論理

命題とは, “**真** (しん)” か “**偽** (ぎ)” かが明確に定まっている陳述のこと. ここで, 真とは, “正しい” こと, 偽とは, “正しくない” こと, 陳述とは, これはこうであるというような “主張” である, と理解しておけばよい.

真か偽かが明確に定まっていることと, それが証明できるということは, 別である. “π が無理数である” という陳述は, それが仮に証明できなくても, 真か偽のいずれかである.

命題が真であるとき, それが**成り立つ**, あるいは, **成立する**ともいう.

例題 3.1 次の陳述は命題である.

1. $1+2=5$.
2. 三角形の内角の和は 180 度である.
3. 各桁の数字の和が 3 で割り切れる数は, 3 で割り切れる.
4. 犬と猿は仲がよくない. この陳述は, 真偽がはっきりしないので命題ではない.
5. 風が吹けば桶屋が儲かる. この陳述も, 真偽がはっきりしないので命題ではない.

命題論理とは, 数学で用いる, “かつ”, “または”, “ならば” などの自然言語で表される論理を, 記号を用いて形式化したもの.

3.1.2 論理記号, 複合命題

定義 3.2 (**論理記号**) 与えられた命題から新たな命題を作る**命題結合記号**とよばれる**論理記号** $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\neg$ を次の**真理値表**によって定義する. ただし, p, q は命題, T は真 (True), F は偽 (False) を表す. T, F を真理値という.

p	q	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftarrow q$	$p \Leftrightarrow q$	$\neg p$
T	T	T	T	T	T	T	F
T	F	T	F	F	T	F	F
F	T	T	F	T	F	F	T
F	F	F	F	T	T	T	T

1. $p \vee q$: p と q の**論理和** (あるいは選言) という. “p または q” という意味を表す. これに対し, $p \oplus q := (p \wedge \neg q) \vee (\neg p \wedge q)$ で定義される p と q の**排他的論理和**がある. 論理和と排他的論理和の違いは, p と q がともに T であるとき, それぞれ T と F になることである.

p	q	$(p \wedge \neg q) \vee (\neg p \wedge q)$
T	T	F
T	F	T
F	T	T
F	F	F

2. $p \wedge q$: p と q の**論理積** (あるいは連言) という. “p かつ q” という意味を表す.
3. $p \Rightarrow q$: “p ならば q” という意味を表す. また, “p は q を**含意**する” という. $(p \Rightarrow q) = F$ となるのは, $(p = T) \wedge (q = F)$ のときのみ. 特に, $p = F$ ならば常に $(p \Rightarrow q) = T$ となる.
4. “$(p \Rightarrow q) = T$” のとき, “p は q の**十分条件**である” といい, “q は p の**必要条件**である” という.
5. “$p \Leftrightarrow q$” は “$(p \Rightarrow q) \wedge (p \Leftarrow q)$” と論理的に等しい.
6. “$p \Leftrightarrow q$” が真のとき, p と q は互いに他の**必要十分条件**であるという. また, p と q は**同値**であるという.

7. p と q が同値であることと, p と q の真理値が一致することは同じこと. したがって, "$p \Leftrightarrow q$" を "$p = q$" とも書く.
8. $\neg p$: p の**否定**という.
9. 含意 $p \Rightarrow q$ は, $\neg$ と $\vee$ を用いて, $(p \Rightarrow q) = (\neg p \vee q)$ と表される.

p	q	$\neg p$	$\neg p \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

複合命題とは, 基本命題を論理記号で結合することにより構成される命題である. 何と何が結合されるかを明示するために, カッコ "(", ")" を用いる. ただし, 否定 $\neg$ は最も結合が強いとし, カッコを省略することがある. 例えば, $\neg p \vee q$ は $\neg(p \vee q)$ ではなく, $(\neg p) \vee q$ である.

定理 3.3 任意の命題 p に対し, 以下の等式が成り立つ.

1. $p \vee T = T$, $p \wedge T = p$.
2. $p \vee F = p$, $p \wedge F = F$.
3. $p \vee \neg p = T$, $p \wedge \neg p = F$.
4. $\neg(\neg p) = p$.

p	$p \vee T$	$p \wedge T$	T	$\neg p$	$\neg(\neg p)$
T	T	T	T	F	T
F	T	F	T	T	F

定理 3.4 任意の命題 p, q, r に対し, 以下のことが成り立つ.

1. $p \vee q = q \vee p$,
   $p \wedge q = q \wedge p$. (**交換律**)
2. $(p \vee q) \vee r = p \vee (q \vee r)$,
   $(p \wedge q) \wedge r = p \wedge (q \wedge r)$. (**結合律**)
3. $(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$,
   $(p \wedge q) \vee r = (p \vee r) \wedge (q \vee r)$. (**分配律**)
4. $p \vee p = p$,
   $p \wedge p = p$. (**ベキ等律**)
5. $(p \vee q) \wedge p = p$,
   $(p \wedge q) \vee p = p$. (**吸収律**)

(証明) 論理命題において，同値であること，すなわち，等号 $=$ を示す方法の一つは，それぞれの真理値表を作成し，一致することを示せばよい．ここでは，真理値表を作成するのではなく，場合分けする方法で，同値であることを示す．分配律について示す.

1. $(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$.
   証明の方針として, "左辺 $\Rightarrow$ 右辺 かつ 左辺 $\Leftarrow$ 右辺" が成り立つこと (真であること) を示せばよい．さらに, $p \Rightarrow q$ が真であることを示すには，"$p = T$ のとき，$q = T$ となる" ことを示せば十分であることに注意する．なぜなら，$p = F$ のとき，q の真偽に関係なく $p \Rightarrow q$ は常に真であるから.

   $\Rightarrow$) $((p \vee q) \wedge r) = T$ であるとする．すると，$p = T$ または $q = T$ であり, かつ $r = T$ である．したがって，$p = T$ ならば，$(p \wedge r) = T$. または，$q = T$ ならば，$(q \wedge r) = T$. ゆえに，$((p \wedge r) \vee (q \wedge r)) = T$.

   $\Leftarrow$) 次に，$((p \wedge r) \vee (q \wedge r)) = T$ であるとする．すると，$(p \wedge r) = T$ または $(q \wedge r) = T$ である．したがって，$p = T$ または $q = T$ であり，かつ $r = T$ である．ゆえに，$((p \vee q) \wedge r) = T$.
   以上より，同値であることが言えた. ∎

2. $(p \wedge q) \vee r = (p \vee r) \wedge (q \vee r)$.

⇒) $((p \wedge q) \vee r) = T$ とすると，$(p \wedge q) = T$ または $r = T$ である．したがって，$(p \vee r) = T$ かつ $(q \vee r) = T$ である．ゆえに，$(p \vee r) \wedge (q \vee r)) = T$.

⇐) $(p \vee r) \wedge (q \vee r)) = T$ とすると，$(p \vee r) = T$ かつ $(q \vee r) = T$ である．$r = T$ ならば $((p \wedge q) \vee r) = T$. 逆に，$r = F$ ならば $(p \wedge q) = T$ でなくてはならないから，$((p \wedge q) \vee r) = T$. ゆえに，常に，$((p \wedge q) \vee r) = T$. 以上より，同値であることが言えた. ∎

定理 3.5 (**ド・モルガンの法則**) 任意の命題 p, q に対し, 以下のことが成り立つ.

1. $\neg(p \vee q) = \neg p \wedge \neg q$.
2. $\neg(p \wedge q) = \neg p \vee \neg q$.

(証明) 以下の真理値表にて示す.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
T	T	T	F	F	F	F	T	F	F
T	F	T	F	F	T	F	F	T	T
F	T	T	F	T	F	F	F	T	T
F	F	F	T	T	T	T	F	T	T

(別証明) 前記定理の証明と同じ方法でも示すことかできる. すなわち, ⇒ かつ ⇐ を示せばよい. たとえば, 1. の場合において ⇒ を示すには, $\neg(p \vee q) = T$ とき, $\neg p \wedge \neg q = T$ となることを示せば十分である. ここでは, 1. の場合についての証明を示す.

1. はじめに, $\neg(p \vee q) \Rightarrow \neg p \wedge \neg q$ を示す. $\neg(p \vee q) = T$ ならば $p \vee q = F$. $p \vee q = F$ ならば $p = F$ かつ $q = F$. すなわち, $\neg p = T$ かつ $\neg q = T$ であり, $\neg p \wedge \neg q = T$. ゆえに, $\neg(p \vee q) \Rightarrow \neg p \wedge \neg q$ が成り立つ.

次に, $\neg(p \vee q) \Leftarrow \neg p \wedge \neg q$ を示す. $\neg p \wedge \neg q = T$ ならば $\neg p = T$ かつ $\neg q = T$ であり, $p = F$ かつ $q = F$. したがって, $p \vee q = F$ より, $\neg(p \vee q) = T$ となる. ゆえに, $\neg(p \vee q) \Leftarrow \neg p \wedge \neg q$ が成り立つ.

以上より, $\neg(p \vee q) = \neg p \wedge \neg q$ は成り立つ. ∎

例題 3.6 (論理記号の変換)

1. $p \vee q$ を $p, q, \neg, \wedge$ のみで表せ.
2. $p \vee q$ を $p, q, \neg, \Rightarrow$ のみで表せ.
3. $p \wedge q$ を $p, q, \neg, \vee$ のみで表せ.
4. $p \wedge q$ を $p, q, \neg, \Rightarrow$ のみで表せ.
5. $p \Rightarrow q$ を $p, q, \neg, \vee$ のみで表せ.
6. $p \Rightarrow q$ を $p, q, \neg, \wedge$ のみで表せ.

(解答)

1. ド・モルガンの法則より, $p \vee q = \neg(\neg p \wedge \neg q)$.
2. $(p \Rightarrow q) = (\neg p \vee q)$ より, $p \vee q = \neg(\neg p) \vee q = (\neg p \Rightarrow q)$
3. ド・モルガンの法則より, $p \wedge q = \neg(\neg p \vee \neg q)$.
4. ド・モルガンの法則と上記 2 に結果より, $(p \Rightarrow q) = (\neg p \vee q)$ より, $p \wedge q = \neg(\neg p \vee (\neg q)) = \neg(p \Rightarrow (\neg q))$.
5. $p \Rightarrow q$ を $p, q, \neg, \vee$ のみで表せ. $(p \Rightarrow q) = (\neg p \vee q)$ より, そのもの.
6. ド・モルガンの法則と $(p \Rightarrow q) = (\neg p \vee q)$ より, $(p \Rightarrow q) = (\neg p \vee q) = \neg(\neg(\neg p) \wedge (\neg q)) = \neg(p \wedge (\neg q))$.

集合と論理での記号の対応は以下のように表せる.

集合	論理
$\cup$	$\vee$
$\cap$	$\wedge$
c (補集合)	$\neg$
U (全体集合)	T
ϕ (空集合)	F

例題 3.7 命題 $p \Rightarrow q$ が T であっても, その逆の命題 $q \Rightarrow p$ は必ずしも T でないことを, 真理値表を用いて確かめよ.

例題 3.8 各命題の真理値表を示せ.

1. $p \Rightarrow p$
2. $(p \Rightarrow p) \Rightarrow (p \Rightarrow \neg p)$
3. $(p \vee \neg q) \vee \neg p$
4. $p \Leftrightarrow (\neg p \vee \neg q)$
5. $(\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$

例題 3.9 各命題の真理値表を示せ.

1. $(p \Leftrightarrow \neg p) \Rightarrow (\neg p \wedge q)$
2. $(p \vee \neg q) \Leftrightarrow (q \Rightarrow \neg p)$
3. $[p \wedge (\neg q \Rightarrow p)] \wedge \neg[(p \Leftrightarrow \neg q) \Rightarrow (q \vee \neg p)]$
4. $[q \Leftrightarrow (r \Rightarrow \neg p)] \vee [(\neg q \Rightarrow p) \Leftrightarrow r]$

例題 3.10 各命題を以下のように定義する. そのとき, 次の命題を日本語に翻訳せよ. $p =$ “氷あずきを食べる”, $q =$ “すいかを食べる”, $r =$ “腹痛を起こす”.

1. $(p \wedge q) \Rightarrow r$
2. $r \Rightarrow (p \vee q)$
3. $p \wedge q \wedge \neg r$
4. $r \Rightarrow (p \wedge \neg q)$

例題 3.11 1. 命題 $p \Rightarrow q$ が F であるとき, $(\neg p \vee \neg q) \Rightarrow q$ の値は定まるか. 定まる場合, その値は何か.

2. 命題 $p \Rightarrow q$ が T であるとき, $\neg p \vee (p \Leftrightarrow q)$ の値は定まるか. 定まる場合, その値は何か.

3.1.3 論理関数, 主論理和標準形, 主論理積標準形

p_1, p_2, p_3 を命題とするとき, $(p_1 \vee p_2) \vee p_3$, $p_1 \vee (p_2 \vee p_3)$, $p_2 \vee (p_1 \vee p_3)$ などの真理値はすべて等しいので, これらを $p_1 \vee p_2 \vee p_3$ と表しても混乱は生じない. これも和集合の場合と同じである. 一般に, $p_1, \ldots, p_n$ を命題とするとき, $p_1 \vee \cdots \vee p_n$, $p_1 \wedge \cdots \wedge p_n$ などの意味も明らかであろう. そして,

$$\bigvee_{i=1}^{n} p_i := \begin{cases} T, & \text{ある } i \in \{1, \ldots, n\} \text{ に対し, } p_i = T \text{ のとき;} \\ F, & \text{すべての } i \in \{1, \ldots, n\} \text{ に対し, } p_i = F \text{ のとき.} \end{cases}$$

$$\bigwedge_{i=1}^{n} p_i := \begin{cases} T, & \text{すべての } i \in \{1, \ldots, n\} \text{ に対し, } p_i = T \text{ のとき;} \\ F, & \text{ある } i \in \{1, \ldots, n\} \text{ に対し, } p_i = F \text{ のとき.} \end{cases}$$

とすると, 次の定理が成り立つことも和集合の場合と同様である.

定理 3.12 任意の自然数 n と, n 個の任意の $p_1, \ldots, p_n$ に対し, 以下が成り立つ.

1. $\bigvee_{i=1}^{n} p_i = p_1 \vee \cdots \vee p_n$.
2. $\bigwedge_{i=1}^{n} p_i := p_1 \wedge \cdots \wedge p_n$.

論理関数: 基本命題 $p_1, \ldots, p_n$ から構成される複合命題 $P(p_1, \ldots, p_n)$ は, $\{T, F\}$ に値を取る n 個の変数をもち, $\{T, F\}$ に値を取る写像

P: $\{T, F\}^n \longrightarrow \{T, F\}$

と考えられる. この写像を n 変数**論理関数**とよぶ. $p_1, \ldots, p_n$ を**論理変数**という.

p を論理変数, t を $\{T, F\}$ の要素とするとき,

$$p^t := \begin{cases} p, & t = T \text{ のとき;} \\ \neg p, & t = F \text{ のとき} \end{cases}$$

と定義する.

$(t_1, \ldots, t_n)$ を直積集合 $\{T, F\}^n$ の要素とする n 重対とするとき, $p_1^{t_1} \wedge \cdots \wedge p_n^{t_n}$ を $(t_1, \ldots, t_n)$ に対する $p_1, \ldots, p_n$ の**基本論理積**という.

補題 3.13 $p_1^{t_1} \wedge \cdots \wedge p_n^{t_n} = T$ が成り立つのは, $(p_1 = t_1) \wedge \cdots \wedge (p_n = t_n)$ が成り立つとき, かつ, そのときに限る.
(証明) $(p^t = T) \Leftrightarrow (p = t)$ を示せば十分である. $t = T$ のとき, 定義より, $p^t = p$. $p^t = T$ ならば $t = T = p^t = p$. 逆に, $t = p$ ならば $p^t = p = t = T$. $t = F$ のとき, 定義より, $p^t = \neg p$. $p^t = T$ ならば $\neg t = T = p^t = \neg p$. 逆に, $t = p$ ならば $p^t = \neg p = \neg t = T$. 以上より, $(p^t = T) \Leftrightarrow (p = t)$ が成り立つ. ∎

論理関数 $P(p_1, \ldots, p_n)$ の**真理集合** $\widetilde{P}$ を
$\widetilde{P} := \{(s_1, \ldots, s_n) \mid (s_1, \ldots, s_n) \in \{T, F\}^n,\ P(s_1, \ldots, s_n) = T\}$
と定義する.

すなわち, 論理関数の真理集合は, 論理関数 $P(p_1, \ldots, p_n)$ が T となるような論理変数の組 $(s_1, \ldots, s_n)$ の全体からなる集合である.

定理 3.14 任意の論理関数 $P(p_1, \ldots, p_n)$ は次のように表される. ただし, $\widetilde{P}$ は P の真理集合であり, $\widetilde{P} = \phi$ のときは, 右辺の論理和は F と約束する.
$P(p_1, \ldots, p_n) = \bigvee_{(t_1, \ldots, t_n) \in \widetilde{P}} p_1^{t_1} \wedge \cdots \wedge p_n^{t_n}$.
右辺を論理関数 $P(p_1, \ldots, p_n)$ の**主論理和標準形**という.
(証明) すべての $(p_1, \ldots, p_n) \in \{T, F\}^n$ に対し, 定理の式の右辺と左辺の真理値が一致することを示せばよい.

まず, $\widetilde{P} = \phi$ の場合, 両辺ともに F であるから等式は成り立つ.

次に, $\widetilde{P} \neq \phi$ の場合について考える. $(p_1, \ldots, p_n) \in \widetilde{P}$ ならば, 真理集合の定義より, 左辺 $= T$ である. 一方, $\vee_{(t_1, \ldots, t_n) \in \widetilde{P}} p_1^{t_1} \wedge \cdots \wedge p_n^{t_n}$ において, $(t_1, \ldots, t_n)$ は $\widetilde{P}$ の要素より, $P(t_1, \ldots, t_n) = T$ であり, $\widetilde{P}$ のすべての要素を対象にする. したがって, $P(p_1, \ldots, p_n) = T$ となる $(p_1, \ldots, p_n)$ に対し, $(t_1, \ldots, t_n) = (p_1, \ldots, p_n)$ となる $(t_1, \ldots, t_n) \in \widetilde{P}$ が存在する. したがって, 前記の補題の $(p = t) \Rightarrow (p^t = T)$ より, そのような項に対しては, $(p_1^{t_1} \wedge \cdots \wedge p_n^{t_n}) = T$ となる. 真理値 T をもつ項が存在することより, 右辺 $= T$ である.

次に, $(p_1, \ldots, p_n) \notin \widetilde{P}$ ならば, 真理集合の定義より, 左辺 $= F$ である. 一方, $\vee_{(t_1, \ldots, t_n) \in \widetilde{P}} p_1^{t_1} \wedge \cdots \wedge p_n^{t_n}$ において, $(t_1, \ldots, t_n)$ は $\widetilde{P}$ の要素より, 常に, $P(t_1, \ldots, t_n) = T$ である. したがって, $P(p_1, \ldots, p_n) = F$ となる $(p_1, \ldots, p_n)$ に対し, $(t_1, \ldots, t_n) = (p_1, \ldots, p_n)$ となる $(t_1, \ldots, t_n) \in \widetilde{P}$ は存在しない. したがって, 前記の補題の $(p^t = T) \Rightarrow (p = t)$ より, $(p \neq t) \Rightarrow (p^t \neq T)$, すなわち, $(p^t = F)$ であるから, すべての項に対し, $(p_1^{t_1} \wedge \cdots \wedge p_n^{t_n}) = F$ となる. これより, 右辺 $= F$ である.

以上より, 等式が成り立つことが証明された. ∎

上記の定理は, 任意の論理関数は複合命題として表すことができることを示している.

主論理和標準形に対し, これと**双対**な形の標準形が存在する. それを以下に示そう.

$(t_1, \ldots, t_n)$ を直積集合 $\{T, F\}^n$ の要素とする n 重対とするとき, $p_1^{t_1} \vee \cdots \vee p_n^{t_n}$ を $(t_1, \ldots, t_n)$ に対する $p_1, \ldots, p_n$ の**基本論理和**という. ここで, 関数 p^t の定義より,
$$p^{\neg t} = \begin{cases} \neg p, & t = T \text{ のとき;} \\ p, & t = F \text{ のとき} \end{cases}$$
となることに注意する.

補題 3.15 $p_1^{\neg t_1} \vee \cdots \vee p_n^{\neg t_n} = F$ が成り立つのは, $(p_1 = t_1) \wedge \cdots \wedge (p_n = t_n)$ が成り立つとき, かつ, そのときに限る.
(証明) $(p^{\neg t} = F) \Leftrightarrow (p = t)$ を示せば十分である. ∎

論理関数 $P(p_1, \ldots, p_n)$ の**真理集合** $\widetilde{P}$ の**補集合**を $\overline{P}$ とする. すなわち,
$\overline{P} := \{(s_1, \ldots, s_n) \mid (s_1, \ldots, s_n) \in \{T, F\}^n,\ P(s_1, \ldots, s_n) = F\}$
と定義する.

すなわち, 論理関数の**真理集合の補集合**は, 論理関数 $P(p_1, \ldots, p_n)$ が F となるような論理変数の組 $(s_1, \ldots, s_n)$ の全体からなる集合である.

定理 3.16 任意の論理関数 $P(p_1,\ldots,p_n)$ は次のように表される．ただし, $\overline{P}=\phi$ のときは, 右辺の論理積は T と約束する．

$$P(p_1,\ldots,p_n)=\bigwedge_{(t_1,\ldots,t_n)\in\overline{P}} p_1^{\neg t_1}\vee\cdots\vee p_n^{\neg t_n}.$$

右辺を論理関数 $P(p_1,\ldots,p_n)$ の**主論理積標準形**という．

例題 3.17 次の論理関数 $P(p,q,r)$ の主論理和標準形と主論理積標準形を示せ．

p	q	r	$P(p,q,r)$
T	T	T	F
T	T	F	T
T	F	T	F
T	F	F	T
F	T	T	F
F	T	F	F
F	F	T	T
F	F	F	T

主論理和標準形) 真理集合は $\widetilde{P}=\{(T,T,F),(T,F,F),(F,F,T),(F,F,F)\}$ より, $P(p,q,r)=(p\wedge q\wedge\neg r)\vee(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge\neg q\wedge\neg r)$. 実際に，真理値表を書いて確認する:

p	q	r	$p\wedge q\wedge\neg r$	$p\wedge\neg q\wedge\neg r$	$\neg p\wedge\neg q\wedge r$	$\neg p\wedge\neg q\wedge\neg r$	$P(p,q,r)$
T	T	T	F	F	F	F	F
T	T	F	T	F	F	F	T
T	F	T	F	F	F	F	F
T	F	F	F	T	F	F	T
F	T	T	F	F	F	F	F
F	T	F	F	F	F	F	F
F	F	T	F	F	T	F	T
F	F	F	F	F	F	T	T

主論理積標準形) 真理集合の補集合は $\overline{P}=\{(T,T,T),(T,F,T),(F,T,T),(F,T,F)\}$ より, $P(p,q,r)=(\neg p\vee\neg q\vee\neg r)\wedge(\neg p\vee q\vee\neg r)\wedge(p\vee\neg q\vee\neg r)\wedge(p\vee\neg q\vee r)$. ∎

例題 3.18 一般に，主論理和標準形と主論理積標準形は双対な関係にあるということで，ド・モルガンの法則を利用することで，主論理和標準形の構成法を用いて主論理積標準形を作ることができる．逆に，主論理積標準形の構成法を用いて主論理和標準形を作ることができる．

たとえば，上記の例において，主論理和標準形の構成法を用いて主論理積標準形を作ってみよう．まず，$P(p,q,r)$ の真理値を反転したもの，すなわち，$\neg P(p,q,r)$ を考える．そのとき，$\neg P(p,q,r)$ が T となるのは，$P(p,q,r)$ の真理集合の補集合 $\overline{P}$ の要素に対してのみである．それらの要素に対応するものに対し，主論理和標準形を構成法する．すると，$\neg P(p,q,r)=(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge q\wedge\neg r)$. となる．これより，$\neg(\neg P(p,q,r))$ を考え，ド・モルガンの法則を利用して整理すると，$\neg(\neg P(p,q,r))=(\neg p\vee\neg q\vee\neg r)\wedge(\neg p\vee q\vee\neg r)\wedge(p\vee\neg q\vee\neg r)\wedge(p\vee\neg q\vee r)$. これは確かに，前記の例で得た解と一致する．∎

例題 3.19
1. 3 つの命題 p,q,r のうちの 2 つのみが T であるとき, かつ, そのときに限り T であるような複合命題を構成せよ．
2. 3 つの命題 p,q,r のうち, どれもが T でないか, どれか 1 つが T であるとき, かつ, そのときに限り T であるような複合命題を構成せよ．

3.1.4 恒真命題, 論法, 対偶, 背理法

定義 3.20 常に真である命題を**恒真命題** (Tautology トートロジー) という. また, 常に偽である命題を**矛盾命題** (Contradiction) という.

例題 3.21 p, q, r を命題とするとき, 次の複合命題は恒真命題であることを示せ.

1. $(p \Rightarrow q) = (\neg q \Rightarrow \neg p)$. (等号が成り立てば命題は T, そうでなければ F)
2. $(p \Rightarrow q) = ((p \wedge \neg q) \Rightarrow F)$.
3. $(p \wedge (p \Rightarrow q)) \Rightarrow q$.
4. $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$.

(証明) 真理値表を用いて証明する.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$	$p \wedge \neg q$	$(p \wedge \neg q) \Rightarrow F$
T	T	T	F	F	T	F	T
T	F	F	T	F	F	T	F
F	T	T	F	T	T	F	T
F	F	T	T	T	T	F	T

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg p \Rightarrow \neg q$	$p \wedge \neg q$	$(p \wedge \neg q) \Rightarrow F$	$p \wedge (p \Rightarrow q)$	$p \wedge (p \Rightarrow q) \Rightarrow q$
T	T	T	F	F	T	F	T	T	T
T	F	F	T	F	F	T	F	F	T
F	T	T	F	T	T	F	T	F	T
F	F	T	T	T	T	F	T	F	T

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

∎

例題 3.22 次の命題が恒真命題であるか, 矛盾命題であるか, あるいは, それらのいずれでもないかを判定せよ.

1. $p \vee \neg(p \wedge q)$
2. $(p \vee q) \wedge \neg(p \Rightarrow q)$
3. $(p \wedge q) \wedge \neg(p \vee q)$
4. $p \Rightarrow \neg(p \wedge q)$
5. $[(p \Rightarrow q) \wedge q] \Rightarrow p$

例題 3.23 次の命題が恒真命題であることを示せ.

1. $p \Rightarrow (q \Rightarrow p)$
2. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
3. $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$
4. $p \vee (p \Rightarrow q)$

定義 3.24 **論法**とは, **前提**とよばれる命題 $P_1, \ldots, P_n$ から**結論**とよばれる命題 Q が導かれるという主張であり,

$P_1, \ldots, P_n \vdash Q$

と表される.

論法 $P_1, \ldots, P_n \vdash Q$ が**妥当**であるとは, $(P_1 \wedge \cdots \wedge P_n) \Rightarrow Q$ が恒真命題であることをいう.

このとき, "$(P_1 \wedge \cdots \wedge P_n) \Rightarrow Q$" が恒真命題であると仮定すると, $P_1, \ldots, P_n$ がすべて T ならば Q が T であることが導かれる. なぜなら, $P_1, \ldots, P_n$ がすべて T ならば $(P_1 \wedge \cdots \wedge P_n) = T$. そして, 恒真命題という仮定より, $(T \Rightarrow Q) = T$ と書ける. ゆえに, $Q = T$ が導かれる.

定理 3.25 次の論法は妥当である.

1. **対偶**による証明: $(\neg q \Rightarrow \neg p) \vdash (p \Rightarrow q)$
2. **背理法**による証明: $((p \wedge \neg q) \Rightarrow F) \vdash (p \Rightarrow q)$
3. **三段論法**による証明: $(p \Rightarrow q, q \Rightarrow r) \vdash (p \Rightarrow r)$

(証明)

1. 論法が妥当であることの証明は, その定義より, $(\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$ が恒真命題, すなわち, 常に T であることを示せばよい. 前記の例より, $(\neg q \Rightarrow \neg p)$ と $(p \Rightarrow q)$ の真理値は一致する. また, 含意 $A \Rightarrow B$ は, A と B の真理値が同じ場合, 常に T である. ゆえに, 命題 $(\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$ は常に T であり, 恒真命題である. ∎
2. 上記と同様にして, 命題 $((p \wedge \neg q) \Rightarrow F) \Rightarrow (p \Rightarrow q)$ は恒真命題である. ∎
3. これも上記と同様にして, 命題 $(p \Rightarrow q, q \Rightarrow r) \Rightarrow (p \Rightarrow r)$ は恒真命題である. ∎

例題 3.26 次の主張は, 妥当な論法になっているかどうか, 答えよ.

1. 雨が降るなら学校に行かない. 学校に行かなければ家にいる. よって, 雨が降るなら家にいる.
2. おもしろい授業ならば, それは良い授業である. よって, おもしろくない授業ならば, それは良くない授業である.
3. 良くない授業ならば, それはおもしろくない授業である. よって, おもしろい授業ならば, それは良い授業である.
4. 鯨は哺乳類である. 哺乳類は授乳をする. よって, 鯨は授乳する.

(証明)

1. (三段論法) 命題を $p =$ “雨が降る”, $q =$ “学校に行かない”, $r =$ “家にいる” と表すと, 問いの主張は, 三段論法のかたち $(p \Rightarrow q, q \Rightarrow r) \vdash (p \Rightarrow r)$ と記述できる. ゆえに, その主張は妥当である. ∎
2. $((p \Rightarrow q) \Rightarrow (\neg p \Rightarrow \neg q))$ 命題を $p =$ “おもしろい授業”, $q =$ “良い授業” と表すと, 問いの主張は, $(p \Rightarrow q) \vdash (\neg q \Rightarrow \neg p)$ と記述できる. そこで, 命題 $(p \Rightarrow q) \Rightarrow (\neg p \Rightarrow \neg q)$ を考える. $(p, q) = (F, T)$ のとき, $(p \Rightarrow q) = T$ かつ $(\neg p \Rightarrow \neg q) = F$ より, 命題は F となる. すなわち, 命題は恒真命題ではない. ゆえに, 主張は妥当な論法とはならない. ∎
3. 対偶を用いてい証明する. ∎
4. 三段論法を用いてい証明する. ∎

例題 3.27 (背理法) 最大の素数は存在しないことを示せ.

(証明) 背理法を用いて証明する. そこで, 命題 p を “ 素数は 1 より大きい整数で 1 と自分自身以外の正の約数をもたない” , 命題 q を “ 最大の素数は存在しない” とする. このとき, $((p \wedge \neg q) \Rightarrow F) = T$ となることを示す. すなわち, $(p \wedge \neg q) = F$ を示す. $\neg q$ より, 最大の素数 M が存在すると仮定する. そこで, $2 \sim M$ までのすべての整数を掛け合わせ, 1 を加えた整数 $N = 2 \times \cdots \times M + 1$ を考える. N はその作り方より, $2 \sim M$ の約数をもたない. 従って, N は, N 自身が素数であるか, M より大きい素数の約数をもつかのどちらかである. いずれにしても, M より大きい素数が存在することになり, 仮定に矛盾する. すなわち, $(p \wedge \neg q) = F$. ゆえに, 最大の素数は存在しない. ∎

例題 3.28 次の論法は妥当か.

1. 私は旅行するなら勉強しない.
2. 私は勉強するか, または, 離散数学の試験に合格する.
3. 私は旅行した.

したがって, 私は離散数学の試験に合格した.

(解答) 命題 p, q, r を以下のようにする: $p =$ “旅行する”, $q =$ “勉強する”, $r =$ “離散数学の試験に合格する”.

すると, 問題の論法は, $(p \Rightarrow \neg q) \wedge (q \vee r) \wedge p \vdash r$ となる. すなわち, 論法が妥当であるかどうか判定するには, 命題 $((p \Rightarrow \neg q) \wedge (q \vee r) \wedge p) \Rightarrow r$ が恒真命題になるかどうかを判定すればよい.

まず, $((p \Rightarrow \neg q) \wedge (q \vee r) \wedge p) = F$ の場合, 命題は常に T になる.

次に, $((p \Rightarrow \neg q) \wedge (q \vee r) \wedge p) = T$ の場合, 命題が T になるかどうかを調べる. 仮定より, $(p \Rightarrow \neg q) = T$ かつ $(q \vee r) = T$ かつ $p = T$ である.

$p = T$ より, $(p \Rightarrow \neg q) = T$ ならば, $(\neg q) = T$, すなわち, $q = F$. これより, $(q \vee r) = T$ ならば, $r = T$ でなくてはならない.

したがって, 命題は, $(((p \Rightarrow \neg q) \wedge (q \vee r) \wedge p) \Rightarrow r) = T$ である.

以上より, 命題は恒真命題である. ∎

3.2 述語と限定記号

論理を展開する手段として, 命題以外に述語や限定記号とよばれるものを導入する.

3.2.1 述語

定義 3.29 (**述語**) $X_1, \ldots, X_n$ を集合とする. そのとき, 写像 $P : X_1 \times \cdots \times X_n \longrightarrow \{T, F\}$ を (n 変数) **述語**という.

$P(X_1, \ldots, X_n)$ と書いたとき, これは, $P(X_1, \ldots, X_n) = T$, すなわち, P が $(X_1, \ldots, X_n)$ に対して T であることを主張する.

例題 3.30 1. X を集合とし, $A \subseteq X$ とする. $x \in X$ に対し,

$$P(x) := \begin{cases} T, & x \in A \text{ のとき;} \\ F, & x \in A^c \text{ のとき} \end{cases}$$

と定義される P は, 1 変数述語である. この述語を単に, $x \in A$ と表すことができる.

2. X を集合とする $x, y \in X$ に対し,

$$P(x, y) := \begin{cases} T, & x = y \text{ のとき;} \\ F, & x \neq y \text{ のとき} \end{cases}$$

と定義される P は, 2 変数述語である. この述語を単に, $x = y$ と表すことができる.

3.2.2 全称記号 $\forall$ と存在記号 $\exists$

定義 3.31 (**全称記号**と**存在記号**)

1. P を集合 X 上で定義された述語とする. そのとき, 命題 $\forall x P(x)$ を

$$\forall x P(x) := \begin{cases} T, & X \text{ のすべての } x \text{ に対し, } P(x) = T \text{ のとき;} \\ F, & X \text{ のある } x \text{ に対し, } P(x) = F \text{ のとき} \end{cases}$$

と定義とする. $\forall x$ を x に関する**全称記号**とよぶ. $\forall x P(x)$ は, “すべての x に対し, $P(x)$ は真である” という.

2. P を集合 X 上で定義された述語とする. そのとき, 命題 $\exists x P(x)$ を

$$\exists x P(x) := \begin{cases} T, & X \text{ のある } x \text{ に対し, } P(x) = T \text{ のとき;} \\ F, & X \text{ のすべての } x \text{ に対し, } P(x) = F \text{ のとき} \end{cases}$$

と定義とする. $\exists x$ を x に関する**存在記号**とよぶ. $\exists x P(x)$ は, “$P(x)$ が真であるような x が存在する” という.

3. 全称記号と存在記号を併せて**限定記号**という. 限定記号も論理記号の一つである.
4. $P(x)$ の定義域 X を明示するために, $\forall x P(x)$ を $\forall x \in X : P(x)$, $\exists x P(x)$ を $\exists x \in X : P(x)$ と表すことがある.

例題 3.32 実数 $\mathbb{R}$ 上の関数を $f(x) = x^2 + 3x$ とすると, $f(-2) = -2$ である. このように $f(x)$ が負になるような実数が存在するので, $(\exists x \in \mathbb{R} : f(x) < 0) = T$ である.

他方, $f(1) = 4 > 0$ であることから, すべての実数に対して, $f(x) < 0$ が成立するわけではない. したがって, $(\forall x \in \mathbb{R} : f(x) < 0) = F$ である. ∎

定理 3.33 任意の 1 変数述語に対し, 以下の命題が成り立つ.

1. $\neg(\forall x P(x)) \Leftrightarrow \exists x(\neg P(x))$
2. $\neg(\exists x P(x)) \Leftrightarrow \forall x(\neg P(x))$

(証明) 2. 等号を示すには, 左辺と右辺の真理値が常に一致することを示せばよい.

$(\exists x P(x)) = T$ の場合, まず, $\neg(\exists x P(x)) = F$ である. 次に, $(\exists x P(x)) = T$ は, $P(x) = T$ となるある x が存在するということであるから, $\neg P(x) = F$ となるある x が存在するということである. したがって, すべての x に対し, $\neg P(x) = T$ とはならないことから, $(\forall x(\neg P(x)) = F$ である.

次に, $(\exists x P(x)) = F$ の場合, $\neg(\exists x P(x)) = T$ である. また, $(\exists x P(x)) = F$ は, $P(x) = T$ となるある x が存在しないということであるから, $\neg P(x) = F$ となるある x が存在しないということである. したがって, すべての x に対し, $\neg P(x) = T$ となることから, $(\forall x(\neg P(x)) = T$ である.

以上より, 両辺の真理値は常に一致する. ∎

定義 3.34 1. X_1, X_2 を集合とし, $P : X_1 \times X_2 \longrightarrow \{T, F\}$ を 2 変数述語とする. また, Q_1, Q_2 を $\forall$ または $\exists$ の限定記号とする. このとき, 命題 $Q_1x_1Q_2x_2P(x_1, x_2)$ を $Q_1x_1Q_2x_2P(x_1, x_2) := Q_1x_1(Q_2x_2P(x_1, x_2))$ と定義する.

2. $(Q_2x_2P(x_1, x_2))$ は, x_1 のみを変数とする 1 変数述語である. この述語に, Q_1x_1 を付け加えたものが $Q_1x_1Q_2x_2P(x_1, x_2)$ である.
3. 同様にして, 一般に, $Q_1x_1 \cdots Q_nx_nP(x_1, \ldots, x_n)$ を定義することができる.

注意 3.35 1. $\forall x \exists y P(x, y)$ は, “任意の x に対し, (x ごとに定まる) ある y が存在し, $P(x, y) = T$ となる” という意味の命題である.

2. $\exists x \forall y P(x, y)$ は, “ある x が存在し, (その x を固定したとき,) 任意の y に対し, $P(x, y) = T$ となる” という意味の命題である.
3. 1 変数の場合と同様に, $P(x, y)$ が定義されている集合を明示するために, 命題 $Q_1x_1Q_2x_2P(x_1, x_2)$ を命題 $Q_1x_1 \in X_1, Q_2x_2 \in X_2 : P(x_1, x_2)$ と表すことがある.
4. また, $X_1 = X_2 = X$ のとき, $\forall x_1 \in X, \forall x_2 \in X : P(x_1, x_2)$ と $\exists x_1 \in X, \exists x_2 \in X : P(x_1, x_2)$ をそれぞれ $\forall x_1, x_2 \in X : P(x_1, x_2)$ と $\exists x_1, x_2 \in X : P(x_1, x_2)$ と略記することがある.
5. Q を $\forall$ または $\exists$ の限定記号とする. このとき, 命題 $QxL(x, y, \ldots)$ という形の論理式において, 変数 x は**束縛**されているという. また, $L(x, y, \ldots)$ を x の**適用範囲**という. すなわち, x は, $QxL(x, y, \ldots)$ の中だけで通用する変数であり, 外部とは何の関わりももたない. 同時に, x を他の記号と重複しない記号に置き換えても, 命題の意味は, 変化しない.
6. 例えば, 数式 $\sum_{i=1}^{n} S_i$ において, i はこの式のみで通用するもので, 他の k に置き換えて, $\sum_{k=1}^{n} S_k$ としても式の意味は変わらないことと同じである.
7. どの限定記号によっても束縛されてない変数は**自由**であるという. 自由な変数 y は, $QxL(x, y, \ldots)$ の外部と関わりをもつ.
8. 例えば, 数式 $\exists x \in \mathbb{R} : y = x^2$ において, y は自由な変数である. この命題となる式の真偽は, y にどのような値が与えられるかによって変わってくる.

例題 3.36 論理式 $(\exists y \forall x P(x, y, z)) \wedge (\exists x Q(x, y, z))$ において, 束縛されている変数と自由な変数を示せ.

(解) $(\exists y \forall x P(x, y, z))$ において, x, y は束縛されていて, z は自由である. $(\exists x Q(x, y, z))$ において, x は束縛されていて, y, z は自由である. $(\exists y \forall x P(x, y, z)) \wedge (\exists x Q(x, y, z))$ において, z は自由である. ∎

例題 3.37 命題の真偽を判定せよ.

1. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x = y$
2. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x = y$
3. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x = y$
4. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x = y$

(解) $1.F, 2.T, 3.F, 4.T$.

例題 3.38 命題の真偽を判定せよ.

1. $\forall x \in \mathbb{N}, \exists y \in \mathbb{N} : y = x^2$
2. $\forall y \in \mathbb{N}, \exists x \in \mathbb{N} : y = x^2$
3. $\forall y \in \mathbb{R}, \exists x \in \mathbb{N} : y = x^2$
4. $\forall y \in \mathbb{N}, \exists x \in \mathbb{R} : y = x^2$
5. $\forall y \in \mathbb{R}, \exists x \in \mathbb{R} : y = x^2$

(解) $1.T, 2.F, 3.F, 4.T, 5.F$.

定理 3.39 P を 2 変数の述語とする.

$$\widetilde{Q}_i := \begin{cases} \exists, & Q_i = \forall \text{ のとき;} \\ \forall, & Q_i = \exists \text{ のとき} \end{cases}$$

とするとき, $\neg(Q_1x_1Q_2x_2P(x_1,x_2)) = \widetilde{Q}_1x_1\widetilde{Q}_2x_2(\neg P(x_1,x_2))$ となる.

(証明) すでに, 定理として得られている $\neg(Q_1x_1P(x_1)) = \widetilde{Q}_1x_1(\neg P(x_1))$ を繰り返し用いることで証明できる. ∎

系 3.40 P を n 変数の述語とするとき,

$\neg(Q_1x_1\cdots Q_nx_nP(x_1,\ldots,x_n)) = \widetilde{Q}_1x_1\cdots\widetilde{Q}_nx_n(\neg P(x_1,\ldots,x_n))$

が成り立つ.

例題 3.41 次の 2 つの命題が同じ真理値をもつことを確かめよ.

$\neg(\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x = y)$ と $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x \neq y$.

定理 3.42 P, Q を集合 X 上で定義された 1 変数述語とする. そのとき, 次のことが成り立つ.

1. $(\forall xP(x)) \wedge (\forall xQ(x)) \Leftrightarrow \forall x(P(x) \wedge Q(x))$
2. $(\forall xP(x)) \vee (\forall xQ(x)) \Rightarrow \forall x(P(x) \vee Q(x))$
3. $(\exists xP(x)) \vee (\exists xQ(x)) \Leftrightarrow \exists x(P(x) \vee Q(x))$
4. $\exists x(P(x) \wedge Q(x)) \Rightarrow (\exists xP(x)) \wedge (\exists xQ(x))$

(証明) 1, 2 のみ.

1. $A \Leftrightarrow B$ が T であることを示すには, 同じ真理値をもつ $(A \Rightarrow B) \wedge (A \Leftarrow B)$ が T になることを示せばよい. すなわち, $(A \Rightarrow B) = T$ かつ $(A \Leftarrow B) = T$ を示せばよい.

   $\Rightarrow$) まず, $(A \Rightarrow B) = T$ となることを示そう. $((\forall xP(x)) \wedge (\forall xQ(x))) = T$ とすると, $(\forall xP(x)) = T$ かつ $(\forall xQ(x)) = T$ である. これは, 任意の x に対し, $P(x) = T$ かつ $Q(x) = T$ であることを示している. したがって, 任意の x に対し, $(P(x) \wedge Q(x)) = T$ である. すなわち, $(\forall x(P(x) \wedge Q(x))) = T$.

   $\Leftarrow$) 次に, 逆の $(A \Leftarrow B) = T$ を示す. $(\forall x(P(x) \wedge Q(x))) = T$ とすると, これは, 任意の x に対し, $(P(x) \wedge Q(x)) = T$ である. さらに, $P(x) = T$ かつ $Q(x) = T$ であることを示している. したがって, $(\forall xP(x)) = T$ かつ $(\forall xQ(x))) = T$ となるから $((\forall xP(x)) \wedge (\forall xQ(x))) = T$ である. 以上より, 両辺が同値 $\Leftrightarrow$ であることが示せた. ∎
2. $A \Rightarrow B$ が T であることを示せばよい. すなわち, $(A = T)$ ならば $(B = T)$ を示せばよい. (言い換えると, $(B = F)$ とはならないことを示せばよい.) それ以外の A, B の真理値の組合せでは, 常に $(A \Rightarrow B) = T$ であるから.

   $((\forall xP(x)) \vee (\forall xQ(x))) = T$ であるとする. すると, $(\forall xP(x)) = T$ または $(\forall xQ(x))) = T$ である. $(\forall xP(x)) = T$ ならば, 任意の x に対し, $P(x) = T$ であるから $Q(x)$ の真偽に関わらず, $(P(x) \vee Q(x)) = T$ である. $(\forall xQ(x)) = T$ の場合も同様に, 任意の x に対し, $Q(x) = T$ であるから $P(x)$ の真偽に関わらず, $(P(x) \vee Q(x)) = T$ である. ゆえに, 任意の x に対し, $(P(x) \vee Q(x)) = T$. すなわち, $(\forall x(P(x) \vee Q(x))) = T$ が示せた. 以上より, $((\forall xP(x)) \vee (\forall xQ(x))) = T$ ならば $(\forall x(P(x) \vee Q(x))) = T$ が示せた. ∎

例題 3.43 一般に, 以下のことは成り立たない. 反例を挙げる. $A \Rightarrow B$ に対し, $(A = T)$ のとき, $(B = F)$ を示せば, $(A \Rightarrow B) = F$(成立しないこと) がいえる.

例えば, P, Q を集合 $\{a, b\}$ 上で定義された述語とし, $P(a) = Q(b) = T$, $P(b) = Q(a) = F$ と定める.

1. $\forall x(P(x) \vee Q(x)) \Rightarrow (\forall xP(x)) \vee (\forall xQ(x))$.

   $x = a$ のとき, $(P(a) \vee Q(a)) = (T \vee F) = T$. $x = b$ のとき, $(P(b) \vee Q(b)) = (F \vee T) = T$. ゆえに, $(\forall x(P(x) \vee Q(x))) = T$ である. 一方, $(\forall xP(x)) = F$ かつ $(\forall xQ(x)) = F$ より, $((\forall xP(x)) \vee (\forall xQ(x))) = F$. すなわち, $(\forall x(P(x) \vee Q(x)) \Rightarrow (\forall xP(x)) \vee (\forall xQ(x))) = F$ である. ∎

2. $(\exists x P(x)) \wedge (\exists x Q(x)) \Rightarrow \exists x(P(x) \wedge Q(x))$
   $P(a) = Q(b) = T$ より, $((\exists x P(x)) \wedge (\exists x Q(x))) = T$ である. 一方, $(P(a) \wedge Q(a)) = (T \wedge F) = F$ かつ $(P(b) \wedge Q(b)) = (F \wedge T) = F$ より, $(\exists x(P(x) \wedge Q(x))) = F$ である. ∎

例題 3.44 整数の集合 $\mathbb{Z}$ 上の 1 変数述語 $P(x)$ と $Q(x)$ を次のように定める:

$$P(x) = \begin{cases} T, & \frac{x}{2} \in \mathbb{Z} \text{ のとき;} \\ F, & \frac{x}{2} \notin \mathbb{Z} \text{ のとき} \end{cases} \quad \text{と } Q(x) = \begin{cases} T, & \frac{x+1}{2} \in \mathbb{Z} \text{ のとき;} \\ F, & \frac{x+1}{2} \notin \mathbb{Z} \text{ のとき} \end{cases}$$

このとき，前記の例と同様に，反例になっていることを確かめよ. ∎

例題 3.45 述語 "x さんは y さんが好き" を $L(x, y)$ で表す. このとき, 次の命題はどのような意味を表すか. 意味の違いが分かるように，自然な日本語で表現せよ.

1. $\forall x \exists y : L(x, y)$
2. $\exists y \forall x : L(x, y)$
3. $\exists x \forall y : L(x, y)$
4. $\forall y \exists x : L(x, y)$

(解)

1. 「すべての x に対し，$L(x, y)$ となる y が存在する.」→ 「すべての人 (x) に対し，その人 (x) は好きな人 (y) がいる.」→ 「誰にも，好きな人がいる.」 ∎
2. 「ある y が存在し，すべての x に対し，$L(x, y)$ となる.」→ 「ある人 (y) がいて，すべての人 (x) はその人 (y) が好き.」→ 「誰からも，好かれる人がいる.」 ∎

例題 3.46 次の述語は P は, それぞれ自然数 n のどのような性質を表しているか述べよ.

1. $P(n) = (\exists m \in \mathbb{N} : n = 2m)$
2. $P(n) = (\forall m \in \mathbb{N} : n \neq 2m - 1)$
3. $P(n) = (\exists m \in \mathbb{N} : n = 5(m - 1) + 3)$
4. $P(n) = (\exists \ell \in \mathbb{N}, \exists m \in \mathbb{N} : [(1 < \ell < n) \wedge (1 < m < n) \wedge (n = \ell m)])$

(解)

1. n は 2 の倍数 (偶数) である.
2. n は奇数ではない.
3. $n \in \{3, 8, 13, \ldots\}$ である.
4. n は素数ではない.

例題 3.47 次のことを述語論理式で表現せよ.

1. 自然数 m は自然数 n で割り切れる.
2. x は無理数である.
3. 無理数は存在する.
4. m は素数である
5. どのような自然数よりも大きい素数が存在する.

(解)

1. $P(m, n) = (m \in \mathbb{N}) \wedge (n \in \mathbb{N}) \wedge (\exists k \in \mathbb{N} : m = kn)$
2. $P(x) = (x \in \mathbb{R}) \wedge (\neg(\exists a, b \in \mathbb{Z} : (x = a/b) \wedge (b \neq 0)))$
3. 上記の $P(x)$ を用いて, $\exists x : P(x)$.
4. $Q(m) = (m \in \mathbb{N}) \wedge (m \neq 1) \wedge (\neg(\exists k, \ell \in \mathbb{N} : [(1 < \ell < m) \wedge (1 < k < m) \wedge (m = \ell k)]))$
   または, $Q(m) = (m \in \mathbb{N}) \wedge (m \neq 1) \wedge ((\forall k, \ell \in \mathbb{N} : [(m = \ell k) \Rightarrow ((k = 1) \vee (k = m))]$
5. 上記の $Q(x)$ を用いて, $\forall n \in \mathbb{N}, \exists m \in \mathbb{N} : [Q(m) \wedge (n < m)]$

例題 3.48 k, m, n を自然数とする.

1. k が m, n の公倍数のとき T, そうでないとき F の値をとる 3 変数の述語 $P(k, m, n)$ を構成せよ.
2. k が m, n の最小公倍数のとき T, そうでないとき F の値をとる 3 変数の述語 $Q(k, m, n)$ を構成せよ.

例題 3.49 ある離れ小島があり, その島には「正直村」と「嘘つき村」に分かれている. 正直村の住人のいうことは常に真である (正しく), 嘘つきの住人のいうことは常に偽である (正しくない). 二つの村の住人は, 島の中を自由に歩き回っており, その姿からはどちらの住人かは分からない.

島の住人は皆, ものぐさで, 聞かれたことに対し, 「はい」か「いいえ」かの返事しかしない. しかも, 一回の質問にしか答えてくれない. 正直村の住人は, 質問されたことの答えが真であるならば「はい」と返事をし, 偽ならば「いいえ」と返事をする. 逆に, 嘘つき村の住人は, 質問されたことの答えが真であるならば「いいえ」と返事をし, 偽ならば「はい」と返事をする.

1. さてある冒険家がこの島に上陸した. この島が正直村と嘘つき村に分かれていることは知っている. しかし, 自分が今, 立っているとことろが, 正直村か 嘘つき村か を知りたいが, 分からない. そこへ, ちょうど, 一人の島の住人がやって来た. そこで, ここがどちらの村か尋ねようと思ったが, この人は嘘つき村の住人かもしれないので, 普通の質問, たとえば, 「ここは, 正直村ですか」と尋ねても, 意味はない. さて, それでは, どのような質問をすればよいかを答えよ.
2. 上記の続きで, 冒険家は, この島に「黄金の谷」があることを聞いていた. そこで, その谷を目指して歩きだした. しばらく行くと道が二股に分かれている (左側と右側の道がある). 標識がないのでどちらへ進めばよいか分からず困っていると, 一人の住人がやって来た. そこで, 道を尋ねようと思ったが, この人は嘘つき村の住人かもしれないので, 普通の質問, たとえば, 「右側の道が黄金の谷への道ですか」と尋ねても, 意味はない. さて, それでは, どのような質問をすればよいかを答えよ.

(解答)

1. 命題 p, q を $p =$“ここは, 正直村です”, $q =$“あなたは正直村の住人です” とする. 目標は, p, q を用いた複合命題 $P(p, q)$ で, 真理値表が

p	q	$P(p,q)$
T	T	T
T	F	F
F	T	F
F	F	T

となるものを構成できればよい. 質問の返事の T または F と, 今立っているところが正直村であることの T または F を一致させるように考える. 具体的には, 出会った人が正直村の住人ならば, $q = T$ である. そのとき, 立っている場所が, 正直村ならば $p = T$, そうでなければ $p = F$ である. そして, 複合命題 $P(p, q)$ の真理値が, それぞれ, $((p = T) \wedge (q = T))$ のとき T, $((p = F) \wedge (q = T))$ のとき F というようになればよい. 一方, 出会った人が嘘つき村の住人ならば, $q = F$ である. そのとき, 立っている場所が, 正直村ならば $p = T$, そうでなければ $p = F$ である. そして, 複合命題 $P(p, q)$ の真理値は, それぞれ, $((p = T) \wedge (q = F))$ のとき F, $((p = F) \wedge (q = F))$ のとき T というようになればよい. なぜなら, 嘘つき村の住人であるから, 複合命題 $P(p, q)$ の真理値の反対の真理値を返事するから, $((p = T) \wedge (q = F))$ のとき F ならば「はい (T)」, $((p = F) \wedge (q = F))$ のとき T ならば「いいえ (F)」と返事をする. これは, 今立っているところが正直村であるかないかの真理値と一致する.

そのような複合命題として, $P(p, q) = (p \wedge q) \vee (\neg p \wedge \neg q)$ とすればよい. 日本語の質問にすれば, 「ここは正直村 かつ あなたは正直村の住人 ですか」, または, 「ここは正直村でなく かつ あなたは正直村の住人ではない ですか.」

p	q	$p \wedge q$	$\neg p \wedge \neg q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$	返事をする人と返事
T	T	T	F	T	正直村の人が「はい (T)」と返事する
T	F	F	F	F	嘘つき村の人が「はい (T)」と返事する
F	T	F	F	F	正直村の人が「いいえ (F)」と返事する
F	F	F	T	T	嘘つき村の人が「いいえ (F)」と返事する

嘘つき村の住人は, 複合命題の真理値の逆を答えることに注意する. ∎

例題 3.50 天使は常に真実を述べ, 悪魔は常に嘘をつくとする. A, B は天使か悪魔であることは, はっきりしている. しかし, 彼らが天使か悪魔かは分からない. そこで, A は言いました : 「私が天使ならば B も天使です.」さて, この二人の正体は, それぞれ天使か悪魔か.

(解) 問題を解くヒントは, $p =$「A は天使である」, $q =$「B は天使である」という 2 つの命題を考える. このれらの命題に対し, 命題「私が天使ならば B も天使です」の真偽を場合分けすることで, p, q の可能な真理値を調べる. 答えは, A, B 共に天使である. ∎

4　数学的帰納法と再帰的定義

4.1　数学的帰納法

定理 4.1 $M \subseteq \mathbb{N}$ とする．もし, M が次の条件
1. $1 \in M$,
2. $\forall k \in \mathbb{N} : [k \in M \Rightarrow k+1 \in M]$

を満たすならば, $M = \mathbb{N}$ である．
(証明) 対偶を示す．$M \neq \mathbb{N}$ と仮定する．まず, $1 \notin M$ ならば条件 1 が成り立たないので, 対偶が成り立つ．次に, $1 \in M$ とする．そして, $\mathbb{N} = \{1, 2, \ldots\}$ であるから, 差集合 $\mathbb{N} - M$ には最小値が存在する．それを $m \in \mathbb{N} - M$ とする．すなわち, $m \notin M$．最小であるとした m の選び方より, $m-1 \in M \subset \mathbb{N}$ である．条件 2 において, $m-1 \in \mathbb{N}$ に対し, $m-1 \in M$ ならば $m \in M$ が成立する．これは $m \notin M$ に矛盾する．ゆえに, 条件 2 は成立しない．以上より，$M \neq \mathbb{N}$ ならば条件 1 と 2 は同時に成立しない．ゆえに，対偶は示せた． ∎

定理 4.2 (数学的帰納法 I) P を $\mathbb{N}$ 上で定義された述語とする．もし, 次の条件
1. $P(1)$,
2. $\forall k \in \mathbb{N} : [P(k) \Rightarrow P(k+1)]$

が成り立つならば, $\forall n \in \mathbb{N} : P(n)$ である．
(証明) 条件 1,2 が成立するとする．$M := \{n \in \mathbb{N} \mid P(n)\} (\subset \mathbb{N})$ とする．条件 1 より, $P(1)$ が成立するから, $1 \in M$．さらに, 条件 2 よりと M の定義より, 任意の $k \in \mathbb{N}$ に対し, $k \in M \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow k+1 \in M$．したがって, 前記の定理より, $M = \mathbb{N}$．ゆえに, 任意の $k \in \mathbb{N}$ に対し, $k \in M$ であるから $P(n)$ が成り立つ． ∎

上記の定理の 1. を**帰納法の基礎**, 2. を**帰納ステップ**, 2. の $P(k)$ を**帰納法の仮定**という．

例題 4.3 連続する 3 つの自然数の 3 乗の和は 9 で割り切れることを, 数学的帰納法 I を用いて証明せよ．
(証明) 自然数 n に対し, $f(n) = n^3 + (n+1)^3 + (n+2)^3$ とする．命題 $P(n)$ を, $P(n) =$ "$f(n)$ は 9 で割り切れる" とする．
1. (帰納法の基礎) $1 \in \mathbb{N}$ に対し, $f(1) = 1^3 + 2^3 + 3^3 = 36 = 4 \times 9$ より, $P(1)$ は成り立つ．
2. (帰納ステップ) 自然数 k に対し, $P(k)$ が成り立つと仮定する (帰納法の仮定)．このとき, $P(k+1)$ について調べる．
   $f(k+1) = (k+1)^3 + (k+2)^3 + (k+3)^3 = (k+1)^3 + (k+2)^3 + k^3 + 9k^2 + 27k + 27 = k^3 + (k+1)^3 + (k+2)^3 + 9(k^2 + 3k + 3) = f(k) + 9(k^2 + 3k + 3)$
   これより, $f(k+1)$ は 9 で割り切れる．すなわち, $P(k+1)$ が成り立つ．

以上より，数学的帰納法 I より，任意の自然数 n に対し, $P(n)$ は成り立つ． ∎

例題 4.4 すべての自然数 n に対し，$n^3 + 2n$ は 3 で割り切れることを，数学的帰納法を用いて証明せよ．

数学的帰納法 I では $n=1$ において $P(n)$ が真であることを確かめ, その後, すべての自然数 n に対して $P(n)$ が真であることを導いた. しかし, 帰納法の基礎において, 常に $n=1$ とする必要はなく, 一般の整数でも成り立つことを次の定理にて示す.

定理 4.5 (数学的帰納法 II) $n_0 \in \mathbb{Z}$ を任意に固定した整数とし, P を n_0 以上の整数に対して定義された述語とする. もし, 次の条件

1. $P(n_0)$,
2. $\forall k \geq n_0 : [P(k) \Rightarrow P(k+1)]$

が成り立つならば, $\forall n \geq n_0 : P(n)$ である.

(証明) まず, $n := m-1+n_0$ とする. $Q(m) := P(m-1+n_0)$ とすれば, $Q(m)$ は $\mathbb{N}$ 上で定義された述語となる. そして, 条件 1,2 が成立するならば,

1'. $Q(1) = P(n_0)$ は真である.

2'. $Q(k) = P(k-1+n_0)$ かつ, $Q(k+1) = P((k+1)-1+n_0)$ であり, $P(k-1+n_0) \Rightarrow P((k+1)-1+n_0)$ であるから, $Q(k) \Rightarrow Q(k+1)$ である. したがって, 数学的帰納法 I より, $\forall m \in \mathbb{N} : Q(m)$ が成り立つ. すなわち, $m \geq 1$ かつ $n = m-1+n_0$ かつ $Q(m) = P(m-1+n_0)$ であるから, $\forall n \geq n_0 : P(n)$ が成り立つ. ∎

例題 4.6 3 円と 4 円の切手だけで 6 円以上の任意の郵便代金を支払えることを, 数学的帰納法 II を用いて証明せよ.

(証明) $f(a,b) = 3a+4b$ とする.

$k = 6(= n_0)$ のとき, $(a,b) = (2,0)$ とすれば, $f(2,0) = 6$.

$k \geq 6$ である k に対し, $f(a_1,b_1) = k$ となる (a_1,b_1) が存在すると仮定する. このとき, $k+1$ に対しても $f(a_2,b_2) = k+1$ となる (a_2,b_2) が存在することを示せばよい.

まず, $f(a,b) = 1$ となる (a,b) の組に着目すると, $(a,b) = (-1,1) = (3,-2)$ に対し, $f(a,b) = 1$ となる.

次に, 仮定より, $k+1 = f(a_1,b_1)+1$ である.

$a_1 = 0$ のとき, $k = 4b_1$ であり, $k \geq 6$ より, $b_1 \geq 2$ である. したがって, $k+1 = f(a_1,b_1) + f(3,-2) = f(a_1+3, b_1-2)$. このとき, $a_1+3 \geq 0$ かつ $b_1-2 \geq 0$ が成り立つから, $(a_2,b_2) = (a_1+3, b_1-2)$ とすればよい.

$a_1 > 0$ のとき, $k+1 = f(a_1,b_1) + f(-1,1) = f(a_1-1, b_1+1)$. このとき, $a_1-1 \geq 0$ かつ $b_1+1 \geq 0$ が成り立つから $(a_2,b_2) = (a_1-1, b_1+1)$ とすればよい.

以上のことより, 数学的帰納法 II より, 3 円と 4 円の切手だけで 6 円以上の任意の郵便代金を支払えることが示された. ∎

注意 4.7 一般に, 互いに素な整数 x, y と非負整数 a, b に対し, 整数 $(x-1)(y-1)$ 以上のすべての整数を $ax+by$ のかたちで表現できる. ∎

例題 4.8 5 円と 7 円の切手だけで 24 円以上の任意の郵便代金を支払えることを証明せよ.

定理 4.9 (数学的帰納法 III) P を $\mathbb{N}$ 上で定義された述語とする. もし, 次の条件

1. $P(1)$,
2. $\forall k \in \mathbb{N} : [(1 \leq \forall \ell \leq k : P(\ell)) \Rightarrow P(k+1)]$

が成り立つならば, $\forall n \in \mathbb{N} : P(n)$ である.

(証明) 条件 1,2 が成立するとする. $Q(n) := [1 \leq \forall m \leq n : P(m)]$ とし, $\forall n \in \mathbb{N} : Q(n)$ を数学的帰納法 I で示そう.

1'. $Q(1) = [1 \leq \forall m \leq 1 : P(m)]$ であるから, 条件 1 より, $Q(1)$ は正しい.

2'. $n = k$ のとき $Q(k)$ が正しいと仮定する. そして, $n = k+1$ のとき, $Q(k+1)$ が正しいことを示せばよい. 仮定より, $1 \leq \forall m \leq k : P(m)$ である. さらに, 条件 2 より, $P(k+1)$ は正しい. したがって, $1 \leq \forall m \leq k+1 : P(m)$ は正しい. これは, $Q(k+1)$ が正しいことを示している.

以上のことより, 数学的帰納法 I より, $\forall n \in \mathbb{N} : Q(n)$ が成り立つ. これは, すべての $P(1), P(2), \ldots, P(n)$ が成り立つことを示している. すなわち, 特に, $\forall n \in \mathbb{N} : P(n)$ が成り立つことが示された. ∎

例題 4.10 数列 $a_1, a_2, \ldots$ を

$a_1 = 1,$

$a_n = \sum_{k=1}^{n-1} a_k + 1 \ (n \geq 2)$

と定義する．任意の自然数 n に対し, $a_n = 2^{n-1}$ が成り立つことを数学的帰納法 III により証明せよ．

(証明) $n = 1$ のとき, $a_n = a_1 = 1 = 2^0 = 2^{n-1}$ より, 等式が成り立つ．

$k = 1, 2, \ldots, n-1$ のすべての k に対し, $a_k = 2^{k-1}$ が成り立つと仮定する．そして, n の場合に, $a_n = 2^{n-1}$ が成り立つことを示そう．定義と仮定より,

$a_n = \sum_{k=1}^{n-1} a_k + 1 = \sum_{k=1}^{n-1} 2^{k-1} + 1 = (1 + 2 + \ldots + 2^{n-2}) + 1 = \frac{(1-2^{n-1})}{1-2} + 1 = 2^{n-1}.$

以上のことより, 数学的帰納法 III より, 任意の自然数 n に対し, $a_n = 2^{n-1}$ が成り立つ． ∎

例題 4.11 次の命題が正しいことを示せ．命題: “ 任意の自然数 a, r に対し, a から始まる連続する r 個の整数の積 $a(a+1)(a+2)\cdots(a+r-1)$ は $r!$ で割り切れる． ” ここで, $(a;r) = a(a+1)(a+2)\cdots(a+r-1)$ と記す．また, 整数 x, y に対し, “y は x で割り切れる” ことを $x|y$ と表す．

(証明) まず, 2 つの命題を考える．

$P(r) =$ “任意の自然数 a に対し, $r!|(a;r)$ が成り立つ”,

$Q(a,r) =$ “$r!|(a;r)$ が成り立つ”.

1. $r = 1$ のとき, $P(1)$ は成り立つことは明らか.
2. $r > 1$ のとき, $P(r)$ が成り立つと仮定する．このとき, $P(r+1)$ が成り立つことを示そう．そこで, 任意の自然数 a に対し, $Q(a, r+1)$ が成り立つことを示す.
   i. $a = 1$ のとき, $(a; r+1) = (1; r+1) = (r+1)!$ より, $Q(1, r+1)$ は成り立つ.
   ii. a のとき, $Q(a, r+1)$ が成り立つと仮定する．このとき, $Q(a+1, r+1)$ が成り立つことを示す.

   $(a+1; r+1) = (a+1)((a+1)+1)\cdots((a+1)+(r+1)-2)((a+1)+(r+1)-1) = [(a+1)(a+2)\cdots(a+r)](a+(1+r)) = \underline{a(a+1)(a+2)\cdots(a+r)} + \underline{(a+1)(a+2)\cdots(a+r)(1+r)} = (a; r+1) + (a+1; r)(1+r).$

   $Q(a, r+1)$ が成り立つ仮定より, $(r+1)!|(a; r+1)$ である．また, $P(r)$ が成り立つ仮定より, $r!|(a+1; r)$ であるから, $(r! \times (1+r))|(a+1; r)(1+r) = (r+1)!|(a+1; r)(1+r)$.

   したがって, $(r+1)!|((a; r+1) + (a+1; r)(1+r)) = (r+1)!|(a+1; r+1)$.

   以上より, 数学的帰納法より, 任意の自然数 a に対し, $Q(a, r+1)$ が成り立つことが示された.

   ゆえに, $P(r+1)$ が成り立つことが示された.

したがって, 数学的帰納法より, 任意の自然数 r に対し, $P(r)$ が成り立つ. 以上より, 題意は示された. ∎

例題 4.12 上記の例より, $\frac{(a;r)}{r!} = \frac{a(a+1)(a+2)\cdots(a+r-1)}{r!}$ は整数である．$n = a + r - 1$ とおくと, $n - r = a - 1 \geq 0$ であり, $\frac{(n-(r-1);r)}{r!} = \frac{n(n-1)(n-2)\cdots(n-(r-1))}{r!} = \binom{n}{r}$ となる．$\binom{n}{0} = 1$ と規約する．以上より, n 個の中から r 個を取り出す組合せの総数 $\binom{n}{r}$ は常に整数値となることが理解できる. ∎

4.2 再帰的定義

定義 4.13 (**再帰的定義**) ある種の集合は, 次のように再帰的に定義できる.

1. (**初期ステップ**) 集合 S の要素なるものを幾つか列挙する.
2. (**再帰ステップ**) S の要素であることが分かっているものを用いて, S の新たな要素を定義する.
3. (**限定句**) 上記の 1, 2 で定まるものだけが S の要素であることを述べる. (この条件は, 省略することが多い)

例題 4.14 (再帰的定義) 次のように再帰的に定義される集合 S はどのような集合であるか.

1. A さんを S の要素とする.
2. x さんが S の要素ならば, x さんの子供を S の要素とする.
3. 上記の 1, 2 で定まるものだけを S の要素とする.

1 より, A さんは S に含まれる. 2 より, A さんの子供はすべて S に含まれる. さらに, A さんの子供の子供も S に含まれる. これが繰り返される. 3 より, 上記以外の人は S には含まない. 以上より, 集合 S は A さんの子孫の全体からなる集合である. ∎

前記と同様に, 関数についても再帰的定義を与えることができる.

定義 4.15 ある種の関数 $f : \mathbb{N} \longrightarrow \mathbb{N}$ は, 次のように再帰的に定義できる.

1. (初期ステップ) 幾つかの関数の値 $f(1), f(2), \ldots, f(m)$ を列挙する.
2. (再帰ステップ) $n > m$ に対し, $f(k)$, $1 \leq k \leq m$ の中の幾つかを用いて $f(n)$ を定義する.

再帰的定義の例として, 次の階乗の関数や漸化式があげられる.

例題 4.16 (再帰的定義)

1. (**階乗**) 関数 $f(n) = n!$, $n \in \mathbb{N}$ は, 次のように定義される.
   i. $f(1) = 1$,
   ii. $f(n) = nf(n-1)$, $n \geq 2$
   このとき, $a_n = f(n)$ とすれば, 数列 $\{a_1, a_2, a_3, a_4, \ldots,\}$ は $\{1, 2, 6, 24, \ldots,\}$ となる.
2. 数列 $a_1, a_2, a_3, \ldots,$ は, 次のように定義される.
   i. $a_1 = 3$,
   ii. $a_{n+1} = a_n + 2$, $n \geq 1$
   このとき, 数列は, $\{a_1, a_2, a_3, a_4, \ldots,\} = \{3, 5, 7, 9, \ldots,\}$ となる公差 2 の等差数列である. さらに, $a_n = 3 + 2(n-1)$ となる.
3. (**フィボナッチ数** (Fibonacci number)) 数列 $a_0, a_1, a_2, a_3, \ldots,$ は, 次のように定義される.
   i. $a_0 = 0$, $a_1 = 1$,
   ii. $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$
   このとき, 数列は, $\{a_0, a_1, a_2, a_3, a_4, a_5, a_6, \ldots,\} = \{0, 1, 1, 2, 3, 5, 8, \ldots,\}$ となる.

例題 4.17 次の再帰式で定義されるフィボナッチ数列

i. $a_0 = 0$, $a_1 = 1$,
ii. $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$

に対し, 多項式 $X^2 - X - 1$ を, その特性多項式という. この多項式の 2 根を α, β $(\alpha > \beta)$ とすると, フィボナッチ数列の第 n 項は $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ と表されることを数学的帰納法を用いて証明せよ.

(証明) まず, $X^2 - X - 1$ の根である α, β について, $\alpha + \beta = 1$, $\alpha\beta = -1$ である. また, 解の公式より, $X = \frac{1 \pm \sqrt{5}}{2}$.

1. $n = 0$ のとき, $a_0 = 0 = \frac{1}{\sqrt{5}}(\alpha^0 - \beta^0)$.
   $n = 1$ のとき, $a_1 = 1 = \frac{1}{\sqrt{5}}(\alpha^1 - \beta^1)$.
2. $n = 1, 2, \ldots, k$ のとき, $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ は正しいと仮定する. このとき, $n = k+1$ についても正しいことを示そう.
   $\alpha^{k+1} - \beta^{k+1} = (\alpha^k - \beta^k)(\alpha + \beta) - \alpha\beta(\alpha^{k-1} - \beta^{k-1}) = \sqrt{5}a_k(\alpha + \beta) - \alpha\beta\sqrt{5}a_{k-1} = \sqrt{5}a_k + \sqrt{5}a_{k-1} = \sqrt{5}(a_k + a_{k-1}) = \sqrt{5}a_{k+1}$.
   ゆえに, $a_{k+1} = \frac{1}{\sqrt{5}}(\alpha^{k+1} - \beta^{k+1})$ が成り立つ.

以上より, 数学的帰納法より, 任意の自然数 n について $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ が成り立つ. ∎

例題 4.18 (ハノイの塔 (Tower of Hanoi)) 直径がすべて異なる n 個の円盤があり, 各円盤の中心には棒を通すための穴があけられている. 3 本の棒 b_1, b_2, b_3 が垂直に立っており, 最初, n 個の円盤はすべて小さい円盤ほど上になるように, 棒 b_1 に通して積み重ねられている. これらの円盤を棒 b_2 に移しかえたい. 棒 b_3 は一時的に円盤を積み重ねるために使用してよい. ただし, 一回の操作でただ一つの円盤しか動かすことができず, また, その円盤もそれより小さい円盤の上方にあるように置くことはできない. すなわち, 小さい円盤の上に大きい円盤を置くことはできない.

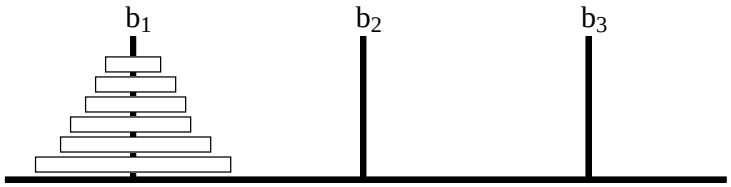


図 9: ハノイの塔

1. n 個の円盤を移し終えるために必要な最小操作回数を $f(n)$ とするとき, $f(n)$ と $f(n-1)$ の間の再帰的な関係を求めよ.
2. $f(n)$ が n のどのような関数になるかを予想し, それを数学的帰納法で証明せよ.

(証明)

1. 具体的に, 少ない個数の場合について考えると, $f(1) = 1$, $f(2) = 3$, $f(3) = 7$, $f(4) = 15$ となる. たとえば, $n = 4$ 個の場合について考える. 3 個の場合の手続きで, 棒 b_1 の上側 3 個を棒 b_3 に移し換える. 1 回の手続きで棒 b_1 の一番下の円盤を b_2 に移し換える. 最後に, 3 個の場合の手続きで, 棒 b_3 にある 3 個の円盤を棒 b_2 に移し換える. したがって, $f(n) = 2f(n-1) + 1$ と書き表すことができる.
2. $f(1) = 1$, $f(2) = 3$, $f(3) = 7$, $f(4) = 15$, $f(5) = 31$ と差 $f(n) - f(n-1)$ を以下のように書き表し, 考察する.

n		$f(n)$	$f(n) - f(n-1)$
1	$1 =$	1	
2	$2 \times 1 + 1 =$	3	$2 = 2^1$
3	$2 \times 3 + 1 =$	7	$4 = 2^2$
4	$2 \times 7 + 1 =$	15	$8 = 2^3$
5	$2 \times 15 + 1 =$	31	$16 = 2^4$

これより, $f(n) = \sum_{k=1}^{n-1} 2^k + 1$, $n \geq 1$ と推測される. さらに, $f(n)$ を整理し, $f(n) = \frac{2^n - 2}{2-1} + 1 = 2^n - 1$ となる. これが正しいことを, 数学的帰納法を用いて以下に示そう.

i. $n = 1$ のとき, $f(1) = 1 = 2^1 - 1$.

ii. $n = k$ のとき, $f(k) = 2^k - 1$ が成り立つと仮定する. このとき, $n = k+1$ でも $f(k+1) = 2^{k+1} - 1$ が成り立つことを示そう.

$$f(k+1) = 2f(k) + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 1.$$

以上より, 数学的帰納法により, 任意の自然数 n に対し, $f(n) = 2^n - 1$ が成り立つ. ∎

例題 4.19 (カタラン数 (Catalan numbers)) カタラン数は, 図のような $n \times n$ の格子上を, 格子点 $(0,0)$ から (n,n) へ至る格子に沿う最短経路で, 下半分の格子点 (i,j), $i \geq j$(図の実線部分) だけを通る経路の総数である.

1. カタラン数 C_n は, 次のような再帰的な関係をもつことを示せ. $C_0 = 1$, $C_1 = 1$, $C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k}$.
2. カタラン数 C_n は, $C_n = \frac{1}{n+1}\binom{2n}{n}$ と表されることを示せ. ここで, $\binom{n}{k}$ は, n 個の中から k 個を選び出す組合せの総数を表す記号である.

(解)

1. 点 (k,k) を経由して, $(0,0)$ から (n,n) に至る最短経路を以下のように考える. まず, $(0,0)$ から (k,k) に至るまでは, 常に通過する点 (i,j) は, $i > j$ を満たす最短経路を考える. このような経路は, $(1,0)$ から $(k,k-1)$ に至る経路で, $i \geq j$ を満たす最短経路と同じであるから, この経路の総数はカタラン数で表すと C_{k-1}. 次に, (k,k) から (n,n) に至るまでは, 常に通過する点 (i,j) は, $i \geq j$ を満たす最短経路を考える. この経路の総数はカタラン数で表すと C_{n-k}. したがって, 上記のような経路で $(0,0)$ から (n,n) に至る最短経路の総数は $C_{k-1}C_{n-k}$.

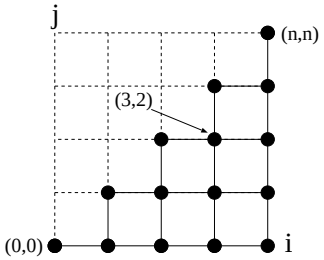


図 10: 格子点と経路 (実線)

そこで，上記のような経路方法をとる場合，$k < m$ を満たす m に対し，点 (m, m) を経由する場合を考えると，そこでの経路の中には, 点 (k, k) を経由する経路は含まれない．なぜなら，$(0, 0)$ から (m, m) までの経路の中で通過するすべての点 (i, j) は $i > j$ を満たすから．

ゆえに，$k = 1, 2, \ldots, n$ までについて考えると，いずれの経路も重複して数えることはないので，求める総数 C_n はそれらの和であり，$C_n = \sum_{k=1}^{n} C_{k-1}C_{n-k}$ となる． ∎

2. 通過点の座標 (i, j) が，$i \geq j$ を満たすという条件を付けないで，単に，$(0, 0)$ から (n, n) に至る最短経路の総数は $\binom{2n}{n}$ である．

   一般に，$(0, 0)$ から (n, m) に至る条件のない最短経路の総数は $\binom{m+n}{n}(= \binom{m+n}{m})$ であることに注意する．

   $(0, 0)$ から (n, n) への条件 $i \geq j$ を満たす最短経路の全体は，i 軸方向に $+1$ ずらすことにより，$(1, 0)$ から $(n + 1, n)$ への最短経路で, 直線 $j = i$ を通らないもの全体に一致する．

   このとき，$(1, 0)$ から $(n + 1, n)$ への条件なしの最短経路は，$(0, 0)$ から (n, n) に至る条件なしの最短経路の総数と同じである．その経路全体の集合を U とする．

   一方，$(1, 0)$ から $(n+1, n)$ への最短経路で, 直線 $j = i$ を通る経路の全体を P と表す．P に含まれる経路の中で $j = i$ を通過するものを考える．そのような経路で, 最初に直線 $j = i$ 上を通過する (直線 $j = i$ と交わる) 点を (k, k) とする．そこで，$(1, 0)$ から (k, k) への経路を直線 $j = i$ で折り返して得られる経路を考える．すると，その経路は，$(0, 1)$ から (k, k) を経由し，$(n + 1, n)$ へ至る経路となる．すなわち，集合 P は $(0, 1)$ から $(n + 1, n)$ へ至る条件なしの最短経路の集合となる．その総数は，$\binom{2n}{n+1}(= \binom{2n}{n-1})$.

   以上より，$(0, 0)$ から (n, n) への条件 $i \geq j$ を満たす最短経路の集合は，全体集合 U における集合 P の補集合 P^c であり，その数は，$|P^c| = C_n$ と書けるから，$C_n = |P^c| = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$ となる． ∎

例題 4.20 4 以上の自然数 n に対し，$2^n < n!$ が成り立つことを，n に関する数学的帰納法を用いて証明せよ．

例題 4.21 任意の有限集合 X に対し, $|2^X| = 2^{|X|}$ が成り立つことを $|X|$ に関する数学的帰納法を用いて証明せよ．

例題 4.22 すべての自然数 n に対し, 次の等式が成り立つことを数学的帰納法を用いて証明せよ．

1. $\sum_{k=1}^{n} k = \frac{1}{2}n(n + 1)$
2. $\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n + 1)(2n + 1)$
3. $\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n + 1)^2$

例題 4.23 以下の等式が成り立つことを確認せよ．それから一般式を予想し，数学的帰納法を用いて証明せよ．

$1^3 = 1,$

$2^3 = 3 + 5,$

$3^3 = 7 + 9 + 11,$

$4^3 = 13 + 15 + 17 + 19.$

5 関係

5.1 2 項関係

定義 5.1 集合 X_1, X_2 に対し, 直積集合 $X_1 \times X_2$ の部分集合を $X_1 \times X_2$ 上の 2 **項関係**という.

さらに, 集合 $X_1, \ldots, X_n$ に対し, 直積集合 $X_1 \times \cdots \times X_n$ の部分集合を $X_1 \times \cdots \times X_n$ 上の n **項関係**として定義できる.

定義 5.2 X, Y を空でない集合とし, R を $X \times Y$ 上の 2 項関係とする. $(x, y) \in R$ に対し, $(x, y) \in R$ を xRy とも表す. xRy が成り立つとき, x **と** y **は** R **の関係がある**という.

X, Y が有限集合のとき, $X \times Y$ 上の 2 項関係は行列で表現できる.

定義 5.3 (2 項関係の行列表現) $X = \{x_1, \ldots, x_m\}$, $Y = \{y_1, \ldots, y_n\}$ に対し, $x_i R y_j$ のとき, かつ, そのときに限り, 行列の (i, j) 成分を 1 とし, それ以外の他の成分を 0 とする.

例題 5.4 有限集合 X, Y を, $X = \{1, 2, 3\}$, $Y = \{a, b, c, d\}$ とする.
2 項関係 $R = \{(1, b), (1, d), (2, a), (2, b), (2, c), (3, c)\} \subseteq X \times Y$ を行列で表現すると次のようになる.

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \left[\begin{array}{cccc} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right] \end{array}$$

例題 5.5 有限集合 X, Y に対し, $X \times Y$ 上の 2 項関係の総数を $|X|, |Y|$ を用いて表せ.
(解答) $|X \times Y| = |X| \times |Y|$ であるから, $|2^{X \times Y}| = 2^{|X \times Y|} = 2^{|X| \times |Y|}$ となる.

定義 5.6 X を集合とするとき, $X \times X$ 上の 2 項関係を X 上の**関係**という.

定義 5.7 (関係のグラフ表現) X 上の関係 R は, これを**有向グラフ**と考えて図示することができる.

グラフ理論では, X の元を**頂点**といい, $(x_i, x_j) \in R$ のとき, 順序対 (x_i, x_j) を**始点** x_i から**終点** x_j に向かう**有向辺**という.

一般に, グラフは, 頂点の集合 V と 辺の集合 $E(\subseteq V \times V)$ を用いて表現でき, それを (V, E) と記す. 本節の場合, $V = X$, $E = R$ となる.

例題 5.8 集合 X を $X = \{a, b, c, d\}$ とし, 関係 R を $R = \{(a, a), (a, b), (b, b), (b, d), (c, a), (c, c), (d, c)\}$ とする. そして, R を有向グラフで図示すると次のようになる (図 11).

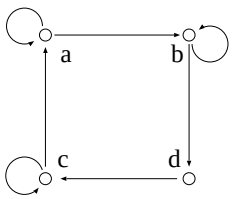


図 11: 関係 R と有向グラフ

定義 5.9 R を集合 X 上の関係とする.

1. (**反射律**) $\forall x \in X : xRx$ が成り立つとき, R は**反射的**であるという.
2. (**対称律**) $\forall x, y \in X : [(xRy) \Rightarrow (yRx)]$ が成り立つとき, R は**対称的**であるという.
3. (**反対称律**) $\forall x, y \in X : [((xRy) \wedge (yRx)) \Rightarrow (x = y)]$ が成り立つとき, R は**反対称的**であるという.
4. (**推移律**) $\forall x, y, z \in X : [((xRy) \wedge (yRz)) \Rightarrow (xRz)]$ が成り立つとき, R は**推移的**であるという.

R を集合 X 上の関係とする. このとき, 上記の各条件を満たす R を表現する行列と有向グラフの関係を以下に示す.

1. R が反射的であることと, 次のそれぞれは同値である:
   i. R を表現する行列の対角成分はすべて 1 である.
   ii. R を表現する有向グラフのすべての頂点 x_i に対し, x_i から x_i へ向かう辺がある.
2. R が対称的であることと, 次のそれぞれは同値である:
   i. R を表現する行列は対称行列である. すなわち, (i,j) 成分に 1 があれば, (j,i) 成分にも 1 がある.
   ii. R を表現する有向グラフにおいて, x_i から x_j へ向かう辺があれば, x_j から x_i へ向かう辺がある.
3. R が反対称的であることと, 次のそれぞれは同値である:
   i. R を表現する行列において, $i \neq j$ ならば, (i,j) 成分と (i,j) 成分が共に 1 になることはない.
   ii. R を表現する有向グラフにおいて, $i \neq j$ ならば, x_i から x_j へ向かう辺と x_j から x_i へ向かう辺の両方が存在することはない.
4. R が推移的であることと, 次のそれぞれは同値である:
   i. R を表現する行列において, (i,j) 成分と (j,k) 成分が共に 1 ならば, (i,k) 成分も 1 である.
   ii. R を表現する有向グラフにおいて, x_i から x_j へ向かう辺と x_j から x_k へ向かう辺が存在するならば, x_i から x_k へ向かう辺が存在する.

例題 5.10 集合 $X = \{a,b,c,d\}$ 上の関係を以下のように定義する.

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

このとき,

1. 関係 R,S,T,U のそれぞれを行列と有向グラフで表せ.
2. 関係 R,S,T,U が, 反射律, 対称律, 反対称律, 推移律 のそれぞれを満たすかどうかを判定せよ.

例題 5.11 X を有限集合とし, $|X| = n$ とする.

1. 集合 X 上の反射的な関係の総数を n を用いて表せ.
2. 集合 X 上の対称的な関係の総数を n を用いて表せ.
3. 集合 X 上の反対称的な関係の総数を n を用いて表せ.
4. 集合 X 上の “ 反射的 ” かつ “ 対称的でない ” 関係の総数を n を用いて表せ.

(解答)

1. 反射的ならば対角成分がすべて 1 になる行列に対応する. そして, $n \times n$ 行列で, 対角成分以外の成分の数は, $n \times n - n = n(n-1)$ 個である. これらの成分は, 0 または 1 をとる. ゆえに, そのような行列の総数は, $2^{n(n-1)}$ 個である. ∎
2. 対称的ならば行列は対称行列である. そのような行列は, 対角成分とそれを除く上三角成分が定まれば一意に定まる. 対角成分の個数は n, 上三角成分の個数は $\frac{n \times n - n}{2}$ である. これらを合わせると, $n + \frac{n \times n - n}{2} = \frac{n(n+1)}{2}$ である. ゆえに, そのような行列の総数は, $2^{\frac{n(n+1)}{2}}$ 個である. ∎
3. 反対称的な関係を表す行列 $A = (a_{i,j})$ の成分 $a_{i,j}$ と $a_{j,i}$ について考える. $i = j$ ならば $a_{i,i} = 0$ または 1 の 2 通りのみである (対角成分). $i \neq j$ ならば $(a_{i,j}, a_{j,i}) = (0,0)$ または $(0,1)$ または $(1,0)$ の 3 通りのみである (対角成分以外). 以上より, 反対称的な関係を表す行列全体の成分について考えると, その組合せの総数は, $2^n \times 3^{\frac{n(n-1)}{2}}$. ∎
4. 反射的な関係より, 対角成分はすべて 1 に決定される. 対角成分以外について, 対称的な関係を考えると上三角成分がどうなるかである. それは, $2^{\frac{n(n-1)}{2}}$ である. ゆえに, 目的の総数は, $2^{n(n-1)} - 2^{\frac{n(n-1)}{2}}$. ∎

5.2 同値関係

定義 5.12 反射律, 対称律, 推移律の 3 つを満たす関係を**同値関係**という.

例題 5.13 次のことを証明せよ.

1. X を任意の集合とするとき,
   $R_{\min} := \{(x, x) \mid x \in X\}$
   は X 上の同値関係になる. このとき, X 上の任意の同値関係 R に対し, $R_{\min} \subseteq R$ が成り立つ.
2. X を任意の集合とするとき,
   $R_{\max} := X \times X$
   は X 上の同値関係になる. このとき, X 上の任意の同値関係 R に対し, $R \subseteq R_{\max}$ が成り立つ.
3. n を任意に固定した整数とするとき,
   $R_{(n)} := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \text{ は } n \text{ の倍数 }\}$
   は $\mathbb{Z}$ 上の同値関係になる. このとき, $xR_{(n)}y$ を “ $x \equiv y \pmod{n}$ ” とも表し, x と y は n を**法として合同**であるという.
4. 上記について, $n = 3$ の場合は以下のようになる.
   $R_{(3)} := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \text{ は } 3 \text{ の倍数 }\}$
   $= \{(0, 3), (3, 0), (4, 1), (1, 4), (2, 5), (5, 2), \ldots\}$
   したがって, $xR_{(3)}y$ を “ $x \equiv y \pmod{3}$ ” と表し, x と y は 3 を**法として合同**であるという.
5. $f : X \longrightarrow Y$ に対し,
   $R_f := \{(x_1, x_2) \in X \times X \mid f(x_1) = f(x_2)\}$
   は X 上の同値関係になる. これを f に付随する同値関係という.

(証明) 3. のみ.

反射律) 任意の $x \in \mathbb{Z}$ に対し, $x - x = 0$ は n の 0 倍となり, $xR_{(n)}x$. ゆえに, $R_{(n)}$ は反射律を満たす.

対称律) 任意の $x, y \in \mathbb{Z}$ に対し, $x - y$ が n の倍ならば, ある整数 $k \in \mathbb{Z}$ が存在して, $x - y = kn$ と表すことができる. 一方, $y - x$ は, $y - x = -kn$ と表すことができ, n の $-k$ 倍となり, $yR_{(n)}x$. ゆえに, $R_{(n)}$ は対称律を満たす.

推移律) 任意の $x, y, z \in \mathbb{Z}$ に対し, $xR_{(n)}y$ かつ $yR_{(n)}z$ ならば, それぞれある整数 $k, m \in \mathbb{Z}$ が存在して, $x - y = kn$ かつ $y - z = mn$ と表すことができる. このとき, $x - z$ は $x - z = kn + mn = (k + m)n$ と表すことができ, n の $(k + m)$ 倍となり, $xR_{(n)}z$. ゆえに, $R_{(n)}$ は推移律を満たす.

以上より, $R_{(n)}$ は $\mathbb{Z}$ 上の同値関係となる. ∎

定義 5.14 R を X 上の同値関係とする. 任意の $x \in X$ に対し, 以下を定義する.

1. $[x] := \{y \in X \mid xRy\} (\subseteq X)$ を R による x の**同値類**という.
2. 各 $[x]$ を R による x の**同値類**という.
3. それぞれの同値類に属する要素を, その同値類の**代表元**という.

例題 5.15 $\mathbb{Z}$ 上の同値関係 $R_{(n)}$ において, $n = 3$ の場合の例を示す.

1. $5 \in \mathbb{Z}$ に対する同値類 $[5]$ は, 次のように表される.
   $[5] = \{y \in \mathbb{Z} \mid 5R_{(3)}y\} = \{y \in \mathbb{Z} \mid 5 - y \text{ は } 3 \text{ の倍数 }\}$
   $= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 5 - y = 3k\}$
   $= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -3k + 5\}$
   $= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -3(k - 1) + 2\}$
   $= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -3k + 2\}$
   $= \{\ldots, -4, -1, 2, 5, \ldots\}$
2. 同値類 $[5]$ において, 5 は $[5]$ の代表元である. また, 2 も $[5]$ の代表元である.

3. 上記と同様に, $0, 1, 2 \in \mathbb{Z}$ に対する同値類 $[0], [1], [2]$ は, 次のように表される.
$$\begin{aligned}
[0] &= \{y \in \mathbb{Z} \mid 0R_{(3)}y\} = \{y \in \mathbb{Z} \mid 0 - y \text{ は } 3 \text{ の倍数 }\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 0 - y = 3k\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -3k\} \\
&= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\
[1] &= \{y \in \mathbb{Z} \mid 1R_{(3)}y\} = \{y \in \mathbb{Z} \mid 1 - y \text{ は } 3 \text{ の倍数 }\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 1 - y = 3k\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -3k + 1\} \\
&= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\
[2] &= \{y \in \mathbb{Z} \mid 2R_{(3)}y\} = \{y \in \mathbb{Z} \mid 2 - y \text{ は } 3 \text{ の倍数 }\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 2 - y = 3k\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -3k + 2\} \\
&= \{\ldots, -4, -1, 2, 5, \ldots\}
\end{aligned}$$
4. 上記の例から, $[2] = \{\ldots, -4, -1, 2, 5, \ldots\} = [5]$ であることが分かる. これより, 同値類 $[2]$ の任意の要素, すなわち, 代表元 $x \in [2]$ に対し, $[2] = [x]$ となることが推測できる.
5. 同値類 $[0], [1], [2]$ のそれぞれの要素をみると, $[0]$ の要素は 3 で割って余りが 0 になる整数, $[1]$ の要素は 3 で割って余りが 1 になる整数, $[2]$ の要素は 3 で割って余りが 2 になる整数であることが分かる.

例題 5.16 1. $R_{(n)}$ で $n = 5$ のとき, $[2]$ と $[8]$ は, それぞれどのような集合になるか考察せよ.
2. また, 任意の $m \in \mathbb{Z}$ に対し, $[m] = [m + 5]$ となることを示せ.

(解答)

1. $$\begin{aligned}
[2] &= \{y \in \mathbb{Z} \mid 2R_{(5)}y\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 2 - y = 5k\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -5k + 2\}, \\
[8] &= \{y \in \mathbb{Z} \mid 8R_{(5)}y\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : 8 - y = 5k\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -5k + 8\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -5k + 3\}.
\end{aligned}$$
以上より, $[2]$ の元は, 5 で割ると 2 余る整数の全体からなる集合である. また, $[8]$ の元は, 5 で割ると 3 余る整数の全体からなる集合である.
2. $$\begin{aligned}
[m + 5] &= \{y \in \mathbb{Z} \mid (m + 5)R_{(5)}y\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : (m + 5) - y = 5k\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -5k + (m + 5)\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : y = -5k + m\} \\
&= \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : m - y = 5k\} \\
&= \{y \in \mathbb{Z} \mid mR_{(5)}y\} = [m].
\end{aligned}$$

定理 5.17 R を X 上の同値関係とする. このとき, 以下のことが成り立つ.

1. $\forall x \in X : x \in [x]$
2. $\forall x, y \in X : (xRy \Leftrightarrow [x] = [y])$
3. $\forall x, y \in X : (x \in [y] \Leftrightarrow [x] = [y])$
4. $\forall x, y \in X : ([x] \cap [y] \neq \phi \Rightarrow [x] = [y])$
5. $\forall x, y \in X : (xRy \Leftrightarrow (\exists z \in X : (x \in [z]) \wedge (y \in [z])))$

(証明)

1. 任意の $x \in X$ に対し, 反射律 xRx が成り立つことから, $x \in [x]$. ∎
2. $\Rightarrow$) xRy とする. 任意の $z \in [x]$ に対し, xRz である. 対称律より, zRx. xRy と推移律より, zRy. 対称律より, yRz. したがって, $z \in [y]$. ゆえに, $[x] \subseteq [y]$. 同様にして, $[x] \supseteq [y]$ も成り立つ. ゆえに, $[x] = [y]$.

⇐) $[x]=[y]$ とする．任意の $z\in[x]=[y]$ に対し，xRz かつ yRz が成り立つ．したがって，対称律と推移律より，xRy が成り立つ． ∎

3. ⇒) $x\in[y]$ とする．任意の $z\in[x]$ に対し，xRz が成り立つ．また，仮定の $x\in[y]$ より，yRx．これらと推移律より，yRz．すなわち，$z\in[y]$．ゆえに，$[x]\subseteq[y]$．同様にして，$[x]\supseteq[y]$ も成り立つ．ゆえに，$[x]=[y]$．

   ⇐) $[x]=[y]$ とする．任意の $z\in[x]=[y]$ に対し，xRz かつ yRz が成り立つ．したがって，対称律と推移律より，yRx が成り立つ．すなわち，$x\in[y]$． ∎

4. ⇒) $[x]\cap[y]\neq\phi$ とする．仮定より，$z\in[x]\cap[y]$ となる z が存在する．上記の 3 より，“$z\in[x]\Rightarrow[z]=[x]$” かつ “$z\in[y]\Rightarrow[z]=[y]$”．したがって，$[x]=[z]=[y]$ より，$[x]=[y]$ が成り立つ．

   (別証明) ⇒) $[x]\cap[y]\neq\phi$ とする．仮定より，$z\in[x]\cap[y]$ となる z が存在する．このとき，$z\in[x]$ より，xRz．さらに，$z\in[y]$ より，yRz．対称律と推移律より，xRy．したがって，上記 2 より，xRy ならば $[x]=[y]$ が成り立つ． ∎

5. ⇒) xRy とする．まず，上記 3 の ⇒ より，$z\in[x]\subseteq X$ に対し，$[z]=[x]$．また，上記 3 の ⇐ より，$[x]=[z]$ ならば $x\in[z]$．次に，仮定の xRy と上記 2 より，$[x]=[y]$ であるから，$[y]=[x]=[z]$ ならば $y\in[z]$．以上より，$(x\in[z])\wedge(y\in[z])$ を満たす $z\in X$ が存在する．

   ⇐) $(x\in[z])\wedge(y\in[z])$ を満たす $z\in X$ が存在すると仮定する．上記 3 より，“$x\in[z]\Rightarrow[x]=[z]$” かつ “$y\in[z]\Rightarrow[y]=[z]$” である．ゆえに，$[x]=[z]=[y]$ である．上記 2 より，$[x]=[y]$ ならば xRy が成り立つ． ∎

定義 5.18 R を X 上の同値関係とする．このとき，

$X/R:=\{[x]\mid x\in X\}$

を X の R による**商集合**という．

例題 5.19 先に定義した同値関係 $R_{\min}$，$R_{\max}$，$R_{(3)}$ について，商集合を求めよ．

(解答)

1. 任意の $x\in X$ に対し，$[x]=\{y\in X\mid yR_{\min}x\}=\{y\in X\mid y=x\}=\{x\}$ より，
   $X/R_{\min}=\{[x]\mid x\in X\}=\{\{x\}\mid x\in X\}$． ∎
2. 任意の $x\in X$ に対し，$[x]=\{y\in X\mid yR_{\max}x\}=\{y\in X\}=X$ より，
   $X/R_{\max}=\{[x]\mid x\in X\}=\{X,X,\ldots\}=\{X\}$． ∎
3. 先の例と同様に，$0,1,2\in\mathbb{Z}$ に対する同値類 $[0],[1],[2]$ は，次のように表される．

$$
\begin{aligned}
[0]&=\{y\in\mathbb{Z}\mid 0R_{(3)}y\}=\{y\in\mathbb{Z}\mid 0-y\text{ は }3\text{ の倍数 }\}\\
&=\{y\in\mathbb{Z}\mid(\exists k\in\mathbb{Z}:0-y=3k)\}\\
&=\{y\in\mathbb{Z}\mid(\exists k\in\mathbb{Z}:y=-3)\}\\
&=\{\ldots,-6,-3,0,3,6,\ldots\},\\
[1]&=\{y\in\mathbb{Z}\mid 1R_{(3)}y\}=\{y\in\mathbb{Z}\mid 1-y\text{ は }3\text{ の倍数 }\}\\
&=\{y\in\mathbb{Z}\mid(\exists k\in\mathbb{Z}:1-y=3k)\}\\
&=\{y\in\mathbb{Z}\mid(\exists k\in\mathbb{Z}:y=-3k+1)\}\\
&=\{\ldots,-5,-2,1,4,7,\ldots\},\\
[2]&=\{y\in\mathbb{Z}\mid 2R_{(3)}y\}=\{y\in\mathbb{Z}\mid 2-y\text{ は }3\text{ の倍数 }\}\\
&=\{y\in\mathbb{Z}\mid(\exists k\in\mathbb{Z}:2-y=3k)\}\\
&=\{y\in\mathbb{Z}\mid(\exists k\in\mathbb{Z}:y=-3k+2)\}\\
&=\{\ldots,-4,-1,2,5,\ldots\}.
\end{aligned}
$$

   任意の $x\in\mathbb{Z}$ は，3 で割ると，その余りは，0, 1, 2 のいずれかである．x を 3 で割った余りが 0 ならば，$x\in[0]$ となる．そして，定理 “ $x\in[y]\Leftrightarrow[x]=[y]$ ” より，$x\in[0]$ ならば $[x]=[0]$ が成り立つ．同様に，$x\in[1]$ ならば $[x]=[1]$，$x\in[2]$ ならば $[x]=[2]$ が成り立つ．ゆえに，
   $\mathbb{Z}/R_{(3)}=\{[x]\mid x\in\mathbb{Z}\}=\{\ldots,[-2],[-1],[0],[1],[2],[3],\ldots\}=\{[0],[1],[2]\}$． ∎

定理 5.20 X を集合とし, R_1, R_2 を X 上の同値関係とする. このとき, 以下のことが成り立つ.
$R_1 = R_2 \Leftrightarrow X/R_1 = X/R_2$.
(証明) 任意の $x \in X$ に対し, x の R_1, R_2 による同値類をそれぞれ $[x]_1, [x]_2$ とすると,
$X/R_1 = \{[x]_1 \mid x \in X\}$, $X/R_2 = \{[x]_2 \mid x \in X\}$.
$\Rightarrow$) $R_1 = R_2$ とする. 任意の $x \in X$ に対し, $[x]_1 = [x]_2$ であるから, $X/R_1 \subseteq X/R_2$ かつ $X/R_1 \supseteq X/R_2$ は明らか. ゆえに, $X/R_1 = X/R_2$.
$\Leftarrow$) $X/R_1 = X/R_2$ とする. $\subseteq$) 任意の $(x, y) \in R_1$ に対し, $[x]_1 = [y]_1$ である. $[x]_1 = [y]_1 \in X/R_1 = X/R_2$ より, $[x]_1 = [y]_1 \in X/R_2$. したがって, $[x]_1 = [y]_1 = [z]_2 (\in X/R_2)$ となる $z \in X$ が存在する. これより, $x, y \in [z]_2$ であり, zR_2x, zR_2y と表される. 対称律と推移律より, xR_2y. すなわち, $(x, y) \in R_2$ となる. ゆえに, $R_1 \subseteq R_2$. $\supseteq$) 同様にして, $R_1 \supseteq R_2$ が成り立つ. 以上より, $R_1 = R_2$ が成り立つ. ∎

定義 5.21 R を X 上の同値関係とする. このとき, 写像 ψ を
$\psi : X \longrightarrow X/R$
$x \longmapsto [x]$
と定義する. ψ を X から X/R への**自然な写像**という.

例題 5.22 $\mathbb{Z}$ 上の同値関係 $R_{(3)}$ において, 自然な写像 $\psi : \mathbb{Z} \longrightarrow \mathbb{Z}/R_{(3)}$ を考える. このとき, $x = 7, 14$ に対する写像の値は以下のようになる.
$\psi(7) = [7] = [1] = \{\ldots, -2, 1, 4, \ldots\}$,
$\psi(14) = [14] = [2] = \{\ldots, -1, 2, 5, \ldots\}$.

定義 5.23 X を空でない集合とする. 集合族 $S(\subseteq 2^X)$ が X の**直和分割**であるとは, 次の 3 つの条件が満たされることをいう.

1. $\phi \notin S$,
2. $\bigcup_{A \in S} A = X$,
3. $\forall A, B \in S : [A \cap B \neq \phi \Rightarrow A = B]$.

直和分割の要素を**ブロック**という.

例題 5.24 集合 $X = \{a, b, c, d, e\}$ とするとき, 集合族 $S = \{\{a\}, \{b, c\}, \{d, e\}\}$ は X の直和分割である. このとき, この直和分割は 3 個のブロックからなる.

定理 5.25 X を空でない集合とし, R を X 上の同値関係とする. このとき, 商集合 X/R は X の直和分割である.
(証明) (X/R が X の直和分割であることを示すには, 直和分割の定義の条件を満たすことを示せばよい.)

1. 任意の $[x] \in X/R$ に対し, $x \in [x]$ より, $[x] \neq \phi$. ゆえに, $\phi \notin \{[x] \mid x \in X\} = X/R$.
2. $\cup_{A \in X/R} A = X$ を示す. $\subseteq$) 任意の $x \in \cup_{A \in X/R} A$ に対し, $x \in A$ となる $A \in X/R$ が存在する. したがって, $x \in A \subseteq X$ より, $x \in X$. ゆえに, $\cup_{A \in X/R} A \subseteq X$. $\supseteq$) 任意の $x \in X$ に対し, $x \in [x] \in X/R$ となる $[x] \in X/R$ が存在する. したがって, $x \in [x] \subseteq \cup_{A \in X/R} A$ より, $x \in \cup_{A \in X/R} A$. ゆえに, $\cup_{A \in X/R} A \supseteq X$. 以上より, $\cup_{A \in X/R} A = X$.
3. 任意の $[x], [y] \in X/R$ に対し, $[x] \cap [y] \neq \phi$ ならば $z \in [x]$ かつ $z \in [y]$ となる $z \in X$ が存在する. そこで, 任意の $a \in [x]$ に対し, xRa と xRz, yRz より, 対称律と推移律を用いて, yRa. ゆえに, $a \in [y]$ より, $[x] \subseteq [y]$ となる. 同様にして, $[x] \supseteq [y]$ も成り立つ. 以上より, 任意の $[x], [y] \in X/R$ に対し, $[x] \cap [y] \neq \phi$ ならば $[x] = [y]$ が成り立つ.

以上より, X/R が X の直和分割であることが示された. ∎

例題 5.26 X を空でない集合とする. 商集合 $X/R_{\min}$, $X/R_{\max}$, $\mathbb{Z}/R_{(3)}$ がそれぞれ X の直和分割であることを確かめよ.

(証明) X/R が X の直和分割であることを示そう.

1. $X/R_{\min}$:
   i. 任意の $x \in X(\neq \phi)$ に対し, $x \in [x] = \{x\}$ より, $[x] \neq \phi$. ゆえに, $\phi \notin X/R_{\min}$.
   ii. $\cup_{A \in X/R_{\min}} A = X$ を示す. $[x] = \{x\}$ より, $\cup_{[x] \in X/R_{\min}} [x] = \cup_{\{x\} \in X/R_{\min}} \{x\} = X$.
   iii. 任意の $[x], [y] \in X/R_{\min}$ に対し, $[x] \cap [y] \neq \phi$ ならば $\{x\} \cap \{y\} \neq \phi$ より, $x = y$. したがって, $[x] = [y]$.

   以上より, $X/R_{\min}$ が X の直和分割であることが示された. ∎
2. $X/R_{\max}$
   i. 任意の $x \in X(\neq \phi)$ に対し, $x \in [x] = X$ より, $[x] \neq \phi$. ゆえに, $\phi \notin X/R_{\max}$.
   ii. $\cup_{A \in X/R_{\max}} A = X$ を示す. $[x] = X$ かつ $X/R_{\max} = \{X\}$ より, $\cup_{A \in X/R_{\max}} A = \cup_{A \in \{X\}} A = X$.
   iii. 任意の $[x], [y] \in X/R_{\max}$ に対し, $X/R_{\max} = \{X\}$ より, $[x] = X = [y]$. したがって, $[x] = [y]$.

   以上より, $X/R_{\max}$ が X の直和分割であることが示された. ∎
3. $\mathbb{Z}/R_{(3)}$:
   i. $\mathbb{Z}/R_{(3)} = \{[0], [1], [2]\}$ であることに注意すると, 任意の $[x] \in \mathbb{Z}/R_{(3)}$ に対し, $x \in [x]$ より, $[x] \neq \phi$. ゆえに, $\phi \notin \mathbb{Z}/R_{(3)}$.
   ii. $\cup_{A \in \mathbb{Z}/R_{(3)}} A = \mathbb{Z}$ を示す. $\subseteq$) $\cup_{[x] \in \mathbb{Z}/R_{(3)}} [x] = [0] \cup [1] \cup [2] \subseteq \mathbb{Z}$ は明らか. $\supseteq$) 任意の $z \in \mathbb{Z}$ に対し, z を 3 で割ったときの余りは 0, 1, 2 のいずれかである. これより, $z \in [0] \cup [1] \cup [2] = \cup_{[x] \in \mathbb{Z}/R_{(3)}} [x]$. すなわち, $\cup_{[x] \in \mathbb{Z}/R_{(3)}} [x] \supseteq \mathbb{Z}$. ゆえに, $\cup_{[x] \in \mathbb{Z}/R_{(3)}} [x] = \mathbb{Z}$.
   iii. 任意の $[x], [y] \in \mathbb{Z}/R_{(3)}$ に対し, $[x] \cap [y] \neq \phi$ ならば $z \in [x]$ かつ $z \in [y]$ となる z が存在する. このことより, そのような z はそれぞれ $z = 3m + x$, $z = 3k + y$ と表される. ただし, $m, k \in \mathbb{Z}$ である. したがって, $x - y = 3(m - k)$ となり, $xR_{(3)}y$ である. ゆえに, $[x] = [y]$.

   以上より, $\mathbb{Z}/R_{(3)}$ が X の直和分割であることが示された. ∎

定理 5.27 X を空でない集合とし, 集合族 S を X の直和分割とする. このとき, 以下が成り立つ.

1. $R := \cup_{A \in S} A \times A$ と定義すると, R は同値関係になる.
2. $X/R = S$.

(証明) (図 12 を参照)

1. R が反射律, 対称律, 推移律を満たすことを示せばよい.
   i. 反射律) 任意の $x \in X$ に対し, S は X の直和分割であるから, $x \in B$ となる $B \in S$ が存在する. したがって, $(x, x) \in B \times B \subseteq \cup_{A \in S} A \times A = R$.
   ii. 対称律) R の定義より, 任意の $x, y \in X$ に対し, xRy ならば $(x, y) \in B \times B$ となる $B \in S$ が存在する. そして, $(y, x) \in B \times B \subseteq \cup_{A \in S} A \times A = R$. ゆえに, yRx が成り立つ.
   iii. 推移律) R の定義より, 任意の $x, y, z \in X$ に対し, "xRy かつ yRz" ならば "$(x, y) \in B \times B$ かつ $(y, z) \in C \times C$" となる $B, C \in S$ が存在する. 仮定より, S は X の直和分割であるから, $y \in B$ かつ $y \in C$ より, $B \cap C \neq \phi$ であるから $B = C$. ゆえに, $(x, y) \in B \times B$ かつ $(y, z) \in B \times B$ より, $x, y, z \in B$ となり, $(x, z) \in B \times B \subseteq \cup_{A \in S} A \times A = R$. ゆえに, xRz が成り立つ.
2. $\subseteq$) i) 任意の $[x] \in X/R$ に対し, $y \in [x]$ ならば xRy. すなわち, $(x, y) \in B \times B$ となる $B \in S$ が存在する. すなわち, $y \in B$. ゆえに, $[x] \subseteq B$. 逆に, ii) $B \in S$ に対し, $x \in B$ とする. このとき, 任意の $y \in B$ に対し, $(x, y) \in B \times B$ であるから xRy となり, $y \in [x]$ である. ゆえに, $[x] \supseteq B$. 以上の i, ii より, $[x] = B \in S$. すなわち, $X/R \subseteq S$ が言えた.

   $\supseteq$) 任意の $B \in S$ に対し, $(x, y) \in B \times B$ とする. すなわち, $x, y \in B$. i) R の定義より, xRy であり, $y \in [x]$. $[x] \supseteq B$. 逆に, ii) 任意の $B \in S$ に対し, $x \in B$ とする. このとき, 任

意の $y \in [x]$ に対し, xRy であるから, $(x,y) \in B \times B$ である. したがって, $y \in B$. ゆえに, $[x] \subseteq B$. 以上の i, ii より, $B = [x] \in X/R$. すなわち, $X/R \supseteq S$ が言えた.

以上より, $X/R = S$ が成り立つ. ∎

この定理の証明から, "$xRy \Leftrightarrow \exists B \in S : x, y \in B$" が成り立つことが分かる.

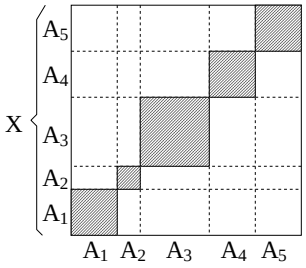


図 12: X の集合族 $S = \{A_1, \ldots, A_5\}$ と直和分割: $R = \cup_{i=1}^{5} A_i \times A_i$, $X/R = S$.

定理 5.28 空でない集合 X に対し, X の直和分割の全体からなる集合を $\widehat{S}$ とし, X 上の同値関係の全体からなる集合を $\widehat{R}$ とする. このとき, 直和分割 $S \in \widehat{S}$ に対し, 同値関係 $R_S = \cup_{A \in S} A \times A$ を対応させる写像は, $\widehat{S}$ から $\widehat{R}$ への全単射である.
(証明) $\widehat{S}$ から $\widehat{R}$ への写像を $F : \widehat{S} \longrightarrow \widehat{R}$; $S \longmapsto R_S = \cup_{A \in S} A \times A$ とする.

単射) 任意の $S_1, S_2 \in \widehat{S}$ に対し, $S_1 \neq S_2$ ならば $F(S_1) \neq F(S_2)$ であることを示せばよい. 任意の $S_1, S_2 \in \widehat{S}$ に対し, $S_1 \neq S_2$ とする. そして, $F(S_1) = R_1, F(S_2) = R_2$ とする. このとき, $F(S_1) = F(S_2)$ と仮定する. 前記の定理 "$X/R_S = S$" より, $S_1 = X/R_1 = X/R_2 = S_2$ となり, $S_1 = S_2$. これは, $S_1 \neq S_2$ に矛盾. ゆえに, $F(S_1) \neq F(S_2)$.

全射) 任意の $R \in \widehat{R}$ に対し, $X/R = \{[x] \mid x \in X\}$ は X の直和分割である. 写像 F の定義より, $F(X/R) = \cup_{x \in X}[x] \times [x]$ である. すると, $(y,z) \in F(X/R) \Leftrightarrow (\exists x \in X : (y,z) \in [x] \times [x]) \Leftrightarrow yRz \Leftrightarrow (y,z) \in R$. ゆえに, $F(X/R) = R$. 以上より, 任意の $R \in \widehat{R}$ に対し, F により R に写される直和分割 X/R が存在する.

以上より, F は全単射であることが示された. ∎

例題 5.29 X を有限集合とすると, X 上の同値関係はいくつあるか.
(解) 上記定理より, 集合 X の直和分割の総数と同じ.

例題 5.30 集合 $\{a,b,c\}$ 上の同値関係をすべて列挙せよ.
(証明) 前記の定理より, 同値関係を列挙するには, 直和分割を列挙し, それを同値関係に写せばよい. 集合 $\{a,b,c\}$ の直和分割は, その分割の個数を $1,2,3$ の順にして, 以下の 5 通りである.

$S_1 = \{\{a,b,c\}\}$,
$S_2 = \{\{a,b\},\{c\}\}$,
$S_3 = \{\{a\},\{b,c\}\}$,
$S_4 = \{\{b\},\{c,a\}\}\}$,
$S_5 = \{\{a\},\{b\},\{c\}\}$.

それぞれの直和分割に対応する同値関係は以下のようになる.

$R_1 = \{a,b,c\} \times \{a,b,c\}$,
$R_2 = (\{a,b\} \times \{a,b\}) \cup (\{c\} \times \{c\})$,
$R_3 = (\{a\} \times \{a\}) \cup (\{b,c\} \times \{b,c\})$,
$R_4 = (\{b\} \times \{b\}) \cup (\{c,a\} \times \{c,a\})$,
$R_5 = (\{a\} \times \{a\}) \cup (\{b\} \times \{b\}) \cup (\{c\} \times \{c\})$.

例題 5.31 集合 $\{a,b,c,d\}$ 上の同値関係をすべて列挙せよ.

定理 5.32 (直和分割の総数) m 個の要素をもつ集合 X を n 個のブロックに分割する直和分割の総数は, 次のように定義される. それは, 第 2 種スターリング数 $S(m,n)$ で与えられる.

$S(m,n) := \frac{1}{n!}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m$.

したがって, 直和分割の総数は, $\sum_{n=1}^{m} S(m,n)$ となる.

(証明) $m \geq n$ と仮定してよい. m 個の要素をもつ集合から n 個の要素をもつ集合への全射の総数は, $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m$ である.

一方, 直和分割の仕方のみを考えるので, 分割したブロックの並び順には関係しない. ゆえに, n 個のブロックに直和分割する総数は, 前式を $n!$ で割った, $\frac{1}{n!}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m$ となり, すなわち, $S(m,n)$ となることが分かる.

最後に, m 個の要素をもつ集合 X を直和分割するブロックの個数 n は, 1 から m であるから, 直和分割の総数は, $\sum_{n=1}^{m} S(m,n)$ となる. ∎

例題 5.33 式 $S(m,n)$ 及び $\sum_{n=1}^{m} S(m,n)$ に対し, $m = 3, 4$ の場合を計算してみよ.

(解答)

$m = 3$ の場合)

n	k	$n!$	$\binom{n}{k}$	k^m	$(-1)^{n-k}\binom{n}{k}k^m$	$S(m,n)$
1	0	1	1	0	0	1
	1		1	1	1	
2	0	2	1	0	0	3
	1		2	1	-2	
	2		1	8	8	
3	0	6	1	0	0	1
	1		3	1	3	
	2		3	8	-24	
	3		1	27	27	

より, $\sum_{n=1}^{3} S(3,n) = 5$.

.

$m = 4$ の場合)

n	k	$n!$	$\binom{n}{k}$	k^m	$(-1)^{n-k}\binom{n}{k}k^m$	$S(m,n)$
1	0	1	1	0	0	1
	1		1	1	1	
2	0	2	1	0	0	7
	1		2	1	-2	
	2		1	16	16	
3	0	6	1	0	0	6
	1		3	1	3	
	2		3	16	-14	
	3		1	81	81	
4	0	24	1	0	0	1
	1		4	1	-4	
	2		6	16	96	
	3		4	81	-324	
	4		1	256	256	

より, $\sum_{n=1}^{4} S(4,n) = 15$. ∎

定義 5.34 S, S' を集合 X の直和分割とする. S が S' の細分であるとは, "$\forall A \in S, \exists B \in S' : A \subseteq B$ " が成り立つことである.

定理 5.35 R, R' を集合 X 上の同値関係とする. $R \subseteq R'$ ならば X/R は X/R' の細分である.

(証明) X/R が X/R' の細分であることを示すには, "$\forall A \in X/R, \exists B \in X/R' : A \subseteq B$ " が成り立つことを示せばよい.

任意の $[x]_R \in X/R$ に対し, $y \in [x]_R$ ならば xRy である. 定理の仮定 $R \subseteq R'$ より, $(x,y) \in R \subseteq R'$ となり, $xR'y$. したがって, $y \in [x]_{R'} \in X/R'$ である. ゆえに, $[x]_R \subseteq [x]_{R'}$.

以上より, $R \subseteq R'$ ならば, 任意の $[x]_R \in X/R$ に対し, $[x]_R \subseteq [x]_{R'}$ を満たす $[x]_{R'} \in X/R'$ が存在する. すなわち, X/R は X/R' の細分である.

例題 5.36 $\mathbb{Z}$ 上の同値関係 $R_{(n)}$ に対し, $n = 2, 4$ とおいて得られる同値関係 $R_{(2)}, R_{(4)}$ を考える. このとき, $R_{(4)} \subseteq R_{(2)}$ であり, $\mathbb{Z}/R_{(4)}$ が $\mathbb{Z}/R_{(2)}$ の細分になっていることを確かめよ.

(解答) 細分になっていることを確かめるには, 任意の $A \in \mathbb{Z}/R_{(4)}$ に対し, $A \subseteq B$ となる $B \in \mathbb{Z}/R_{(2)}$ が存在することを確認すればよい.

まず, 任意の $x \in \mathbb{Z}$ に対し, $[x]_2 \in \mathbb{Z}/R_{(2)}$ は $[x]_2 = \{y \mid \exists m \in \mathbb{Z}\ x - y = 2m\}$, また, $[x]_4 \in \mathbb{Z}/R_{(4)}$ は $[x]_4 = \{y \mid \exists m \in \mathbb{Z}\ x - y = 4m\}$ となる. そして, $\mathbb{Z}/R_{(2)} = \{[0]_2, [1]_2\}$, $\mathbb{Z}/R_{(4)} = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ である. このとき, 以下が成り立つ.

$x \in [0]_4$ に対し, $x = 4m = 2(2m) \in [0]_2$ より, $[0]_4 \subseteq [0]_2$.

$x \in [1]_4$ に対し, $x = 4m + 1 = 2(2m) + 1 \in [1]_2$ より, $[1]_4 \subseteq [1]_2$.

$x \in [2]_4$ に対し, $x = 4m + 2 = 2(2m + 1) \in [0]_2$ より, $[2]_4 \subseteq [0]_2$.

$x \in [3]_4$ に対し, $x = 4m + 3 = 2(2m + 1) + 1 \in [1]_2$ より, $[3]_4 \subseteq [1]_2$.

ゆえに, $\mathbb{Z}/R_{(4)}$ は $\mathbb{Z}/R_{(2)}$ の細分である.

例題 5.37 R と S を集合 X 上の同値関係とする. このとき, $R \cap S$ も X 上の同値関係となることを示せ.

例題 5.38 集合 X 上の反射的関係 R が, " $\forall x, y, z \in X : [(xRy \wedge yRz) \Rightarrow zRx]$ " を満たすならば, R は X 上の同値関係となることを示せ.

例題 5.39 R を集合 X 上の同値関係とし, $S := \{(x, y) \mid \exists z \in X : [xRz \wedge zRy]\}$ とする. このとき, $S = R$ が成り立つことを示せ.

例題 5.40 集合 $X = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 + y^2 \leq 16\}$ とし, X 上の関係 R を, 任意の $(x_1, y_1), (x_2, y_2) \in X$ に対し, "$(x_1, y_1)R(x_2, y_2) \Leftrightarrow x_1 = x_2$" と定義する. このとき, 以下を示せ.

1. R が X 上の同値関係であることを示せ.
2. 商集合 X/R を外延的記法で表せ.

例題 5.41 n 次実正方行列の全体からなる集合を $M(n)$ で表し, $M(n)$ の要素で正則なものの全体からなる集合を $GL(n)$ で表す. $M(n)$ 上の関係 $\sim$ を, 任意の $A, B \in M(n)$ に対し, " $A \sim B \Leftrightarrow \exists C \in GL(n) : A = C^{-1}BC$ " と定義する. このとき, $\sim$ が $M(n)$ 上の同値関係になるを示せ.

例題 5.42 $\mathbb{Z}$ を整数の全体からなる集合とし, $S \subseteq \mathbb{Z}$ とする. 直積集合 $S \times S$ 上の関係 $\sim$ を, 任意の $(a, b), (c, d) \in S \times S$ に対し, " $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$ " と定義する. このとき, 以下を示せ.

1. R が $S \times S$ 上の同値関係であることを示せ.
2. $S = \{1, 2, 3, 4, 5\}$ のとき, 商集合 $(S \times S)/\sim$ の要素数を求めよ.

例題 5.43 $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ 上の関係 $\sim$ を, 任意の $(m_1, n_1), (m_2, n_2) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ に対し, "$(m_1, n_1) \sim (m_2, n_2) \Leftrightarrow m_1 n_2 = m_2 n_1$ " と定義する. このとき, $\sim$ が $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ 上の同値関係になることを示せ.

(分数 a/b とは, $(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ の $\sim$ による同値類のことである. $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim$ は有理数の全体からなる集合である.)

5.3 順序関係

定義 5.44 反射律, 反対称律, 推移律の 3 つを満す関係を**順序関係**, あるいは**半順序関係**と呼ぶ.
順序関係 R が定義されている集合 X を**順序集合**といい, (X, R) と表す.

例題 5.45 S を空でない集合とするとき, $(2^S, \subseteq)$ は順序集合になる. ここで, 記号 $\subseteq$ は集合の包含関係を表す.
(証明) $(2^S, \subseteq)$ が反射律, 反対称律, 推移律を満たすことを示せばよい.
反射律) 任意の $A \in 2^S$ に対し, $A \subseteq A$.
反対称律) 任意の $A, B \in 2^S$ に対し, $A \subseteq B$ かつ $A \supseteq B$ ならば, 集合が等しいことの定義より, $A = B$.
推移律) 任意の $A, B, C \in 2^S$ に対し, $A \subseteq B$ かつ $B \subseteq C$ とする. 任意の $x \in A$ に対し, $x \in B \subseteq C$ より, $x \in C$. ゆえに, $A \subseteq C$ が成り立つ.
以上より, $(2^S, \subseteq)$ は順序集合になる.

R が順序関係のとき, xRy を $x \leq y$ と表すことがある. このとき, y は x より (R の意味で) 大きい, あるいは, x は y より (R の意味で) 小さいという. $x \leq y$ かつ $x \neq y$ のとき, y は x より真に (R の意味で) 大きい, あるいは, x は y より真に (R の意味で) 小さいといい, $x < y$ と表す.
$x < y$ であって, $x < z < y$ を満たす z が存在しないとき, "x は y の**直前の要素である**", あるいは, "y は x の**直後の要素である**" という.

定義 5.46 (**ハッセ図**) $(X, \leq)$ を順序集合とする. X の要素を以下のように作成した図形を**ハッセ図** (Hasse's diagram) という. もし $x < y$ ならば, y を x より上に書く. そして, y が x の直後のとき, かつ, そのときに限り y と x を線で結ぶ.

例題 5.47 順序集合 $(X, \leq)$ を以下のように定義する:
$X = \{a, b, c, d\}$,
$\leq = \{(a, c), (b, c), (c, d), (a, d), (b, d), (a, a), (b, b), (c, c), (d, d)\}$.
このとき, 順序集合 $(X, \leq)$ のハッセ図を記せ.
(解答) 図 13 を参照.

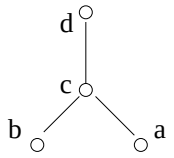


図 13: $(X, \leq)$ のハッセ図

例題 5.48 $S = \{a, b, c\}$ とするとき, 順序集合 $(2^S, \subseteq)$ のハッセ図を示せ.
(解答) 図 14 を参照.

例題 5.49 (X, R) を順序集合とし, $Y \subseteq X$ とする. $R' := R \cap (Y \times Y)$ とすれば, (Y, R') は順序集合となることを示せ. これは, (X, R) において X を Y に制限した順序集合である.
(証明) (Y, R') が反射的, 反対称, 推移的な関係を満たすことを示せばよい. 反射) 任意の $x \in Y$ に対し, $x \in X$ より xRx, すなわち $(x, x) \in R$ である. また, 明らかに, $(x, x) \in Y \times Y$ である. ゆえに, $(x, x) \in R \cap (Y \times Y) = R'$, すなわち, $xR'x$. 反対称) 任意の $x, y \in Y$ に対し, $xR'y$ かつ $yR'x$ ならば, $x, y \in X$ より, xRy かつ yRx であるから $x = y$. 推移律) 任意の $x, y, z \in Y$ に対し, $xR'y$ かつ $yR'z$ ならば, $x, y, z \in X$ より, xRy かつ yRz であり, xRz. また, 明らかに, $(x, z) \in Y \times Y$ である. ゆえに, $(x, z) \in R \cap (Y \times Y) = R'$, すなわち, $xR'z$.

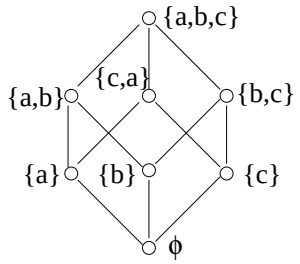


図 14: $(2^S, \subseteq)$ のハッセ図

定義 5.50 $(X, \leq)$ を順序集合とし, Y を X の空でない部分集合とする.

1. (最大元) a が Y の**最大元**であるとは, 次の条件が成り立つときである:
   $a \in Y$ かつ $\forall x \in Y : x \leq a$.
   Y の最大元を $\max Y$ と表す.
2. (最小元) a が Y の**最小元**であるとは, 次の条件が成り立つときである:
   $a \in Y$ かつ $\forall x \in Y : a \leq x$.
   Y の最小元を $\min Y$ と表す.
3. (極大元) a が Y の**極大元**であるとは, 次の条件が成り立つときである:
   $a \in Y$ かつ $\forall x \in X : [(a \leq x \text{ かつ } a \neq x) \Rightarrow x \notin Y]$.
4. (極小元) a が Y の**極小元**であるとは, 次の条件が成り立つときである:
   $a \in Y$ かつ $\forall x \in X : [(x \leq a \text{ かつ } a \neq x) \Rightarrow x \notin Y]$.
5. (上界) a が Y の**上界**であるとは, 次の条件が成り立つときである:
   $a \in X$ かつ $\forall x \in Y : x \leq a$.
6. (下界) a が Y の**下界**であるとは, 次の条件が成り立つときである:
   $a \in X$ かつ $\forall x \in Y : a \leq x$.
7. (上限) a が Y の**上限**であるとは, a が Y の上界の最小元であること. Y の上限を $\sup Y$ と表す.
8. (下限) a が Y の**下限**であるとは, a が Y の下界の最大元であること. Y の下限を $\inf Y$ と表す.

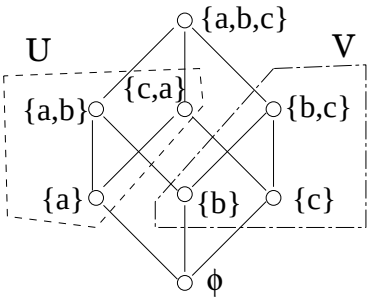
上記の定義より, 上限, 下限は以下のように表すこともできる.

1. $\overline{Y} := \{a \mid a \in X,\ a \text{ は } Y \text{ の上界 }\}$ とする. $\overline{Y}$ の最小元が存在すれば, それが Y の上限である.
2. $\underline{Y} := \{a \mid a \in X,\ a \text{ は } Y \text{ の下界 }\}$ とする. $\underline{Y}$ の最大元が存在すれば, それが Y の上限である.

注意 5.51 有限順序集合において, その部分集合の極大元と極小元は必ず存在する. しかし, 最大元や最小元は存在するとは限らない. また, 極大元 (極小元) は複数存在することもある. しかし, 最大元 (最小元) は存在するとしてもただ 1 つである.

例題 5.52 順序集合 $(X, \leq)$ を例 5.47 と同じものとする. このとき, X の最大元, 最小元, 極大元, 極小元を示せ.
(解答) 最大元: d, 最小元: なし, 極大元: d, 極小元: a, b.

例題 5.53 $S=\{a,b,c\}$ とし, 例 5.48 と同じ順序集合 $(2^S,\subseteq)$ を考える. そこで, 2^S の部分集合として, $U=\{\{a\},\{a,b\},\{c,a\}\}$ と $V=\{\{b\},\{c\},\{b,c\}\}$ とする. このとき, 部分集合 U と V のそれぞれの最大元, 最小元, 極大元, 極小元, 上界, 下界, 上限, 下限を示せ.
(解答)



	U	V
最大元	なし	$\{b,c\}$
最小元	$\{a\}$	なし
極大元	$\{a,b\},\{c,a\}$	$\{b,c\}$
極小元	$\{a\}$	$\{b\},\{c\}$
上界	$\{a,b,c\}$	$\{a,b,c\},\{b,c\}$
下界	$\{a\},\phi$	ϕ
上限	$\{a,b,c\}$	$\{b,c\}$
下限	$\{a\}$	ϕ

例題 5.54 あるクラスの各生徒に関する国語の得点 x と数学の得点 y からなる順序対 $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ を調べると、以下の 9 通りであった。

$$\begin{array}{lll} a=(100,100), & b=(90,90), & c=(80,90),\\ d=(90,70), & e=(60,90), & f=(80,70),\\ g=(90,60), & h=(60,70), & i=(80,60). \end{array}$$

これらの順序対からなる有限集合を

$$X=\{a,b,c,d,e,f,g,h,i\}$$

と定義する. そして, X 上の関係 $\preceq$ を以下のように定義する.
任意の $(x,y),(x',y')\in X$ に対し,

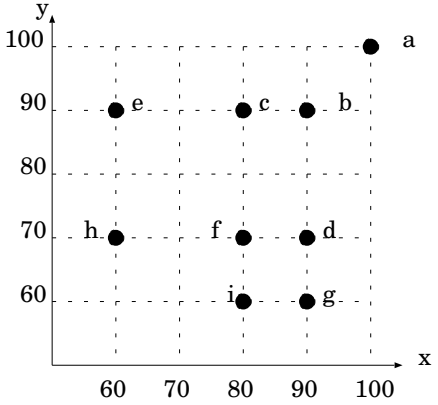
$$\text{“ }(x,y)\preceq(x',y')\text{ ”}\ \Leftrightarrow\ \text{“ }x\le x'\text{ かつ }\ y\le y'\text{ ”}$$

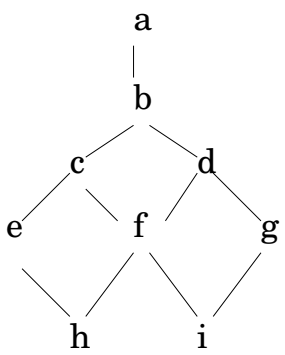
と定義する。ただし、記号 “ $\le$ ” は通常の数の大小関係を表すものとする。このとき, 関係 $\preceq$ は X 上の順序関係になり、$(X,\preceq)$ は順序集合となる。
そこで, X の部分集合 $Y=\{c,d,e,f,h\}$ と $Z=\{c,e,f\}$ を考える. このとき, 以下の問いに解答せよ。

1. 順序集合 $(X,\preceq)$ のハッセ図を示せ.

2. 部分集合 Y と Z のそれぞれの最大元, 最小元, 極大元, 極小元, 上界, 下界, 上限, 下限を示せ.

(解答) まず、各生徒の得点 (x,y) を xy 平面にプロットしてみる。これを参考に、ハッセ図を書くと以下のようになる。





	Y	Z
最大元	なし	c
最小元	h	なし
極大元	c,d	c
極小元	h	e,f
上界	a,b	a,b,c
下界	h	h
上限	b	c
下限	h	h

例題 5.55 $(X, \leq_X), (Y, \leq_Y)$ を順序集合とする. そのとき, $X \times Y$ 上の関係 R を, $(x_1, y_1), (x_2, y_2) \in X \times Y$ に対し, 「“$(x_1, y_1)R(x_2, y_2)$” $\Leftrightarrow$ “$(x_1 \leq_X x_2) \wedge (y_1 \leq_Y y_2)$”」が成り立つときと定義する. このとき, R は $X \times Y$ 上の順序関係になる.

(証明)

(反射律) 任意の $(x, y) \in X \times Y$ に対し、$x \leq x$ かつ $y \leq y$ が成り立つ。ゆえに、$(x, y)R(x, y)$ が成り立つ。

(反対称律) 任意の $(x_1, y_1), (x_2, y_2) \in X \times Y$ に対し、$(x_1, y_1)R(x_2, y_2)$ かつ $(x_2, y_2)R(x_1, y_1)$ ならば、$(x_1, y_1)R(x_2, y_2)$ より、$x_1 \leq x_2$ かつ $y_1 \leq y_2$. さらに、$(x_2, y_2)R(x_1, y_1)$ より、$x_2 \leq x_1$ かつ $y_2 \leq y_1$. したがって、$x_1 \leq x_2$ かつ $x_2 \leq x_1$ より、$x_1 = x_2$. 同様に、$y_1 \leq y_2$ かつ $y_2 \leq y_1$ より、$y_1 = y_2$. ゆえに、$(x_1, y_1) = (x_2, y_2)$ が成り立つ。

(推移律) 任意の $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in X \times Y$ に対し、$(x_1, y_1)R(x_2, y_2)$ かつ $(x_2, y_2)R(x_3, y_3)$ ならば、$(x_1, y_1)R(x_2, y_2)$ より、$x_1 \leq x_2$ かつ $y_1 \leq y_2$. さらに、$(x_2, y_2)R(x_3, y_3)$ より、$x_2 \leq x_3$ かつ $y_2 \leq y_3$. したがって、$x_1 \leq x_2 \leq x_3$ より、$x_1 \leq x_3$. 同様に、$y_1 \leq y_2 \leq y_3$ より、$y_1 \leq y_3$. ゆえに、$(x_1, y_1)R(x_3, y_3)$ が成り立つ。

以上より、R は 反射律、反対称律、推移律を満たし、$X \times Y$ 上の順序関係となる。 □

例題 5.56 自然数の集合 S 上の関係 $|$ を, 任意の整数 $a, b \in S$ に対し,

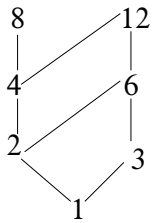
“$a \mid b$ とは, b は a で割り切れる”

と定義する. このとき,

1. 関係 $|$ は順序関係であることを示せ.
2. $S = \{1, 2, 3, 4, 6, 8, 12\}$ のとき, 順序集合 $(S, |)$ に対するハッセ図を示し, S の最大元, 最小元, 極大元, 極小元を示せ.

(解答)

1. 略
2. ハッセ図



	S
最大元	なし
最小元	1
極大元	8, 12
極小元	1

定義 5.57 $(X, \leq)$ を順序集合とする. $x, y \in X$ に対し, $x \leq y$ または $y \leq x$ が成り立つとき, x と y は**比較可能**であるという. そうでないとき, **比較不能**であるという. もし, 任意の 2 要素が比較可能ならば, $\leq$ を**全順序関係**, あるいは, **線型順序関係**と呼ぶ.

例題 5.58 関係 $\leq$ を, 整数の全体 $\mathbb{Z}$ 上の通常の大小関係とすれば, 任意の整数 $x, y \in \mathbb{Z}$ に対し, $x \leq y$ あるいは $y \leq x$ のいずれかが成り立つ. ゆえに, 整数の大小関係 $\leq$ は全順序関係である.

例題 5.59 有限な全順序集合のハッセ図はどのような図形になるか.

(解答) どの 2 要素も比較可能であるから, 順序関係に従って要素を一列に並べることができる. したがって, ハッセ図は, 順序関係で大きいものほど上になるように縦 1 列に並べ, 隣接する要素間を線で結んだ図となる.

例題 5.60 $(X, \leq)$ を全順序集合とする. $X \times X$ の上に関係 $\preceq$ を次のように定義する.

任意の $(x_1, x_2), (y_1, y_2) \in X \times X$ に対し,

「“$(x_1, x_2) \preceq (y_1, y_2)$” $\Leftrightarrow$ “$((x_1 \neq y_1) \wedge (x_1 \leq y_1)) \vee ((x_1 = y_1) \wedge (x_2 \leq y_2))$” 」と定義する。

このとき, 関係 $\preceq$ は $X \times X$ 上の全順序関係になる. このような順序関係を**辞書式順序**という.

定義 5.61 $(X, \leq), (X', \leq')$ をそれぞれ順序集合とする. 写像 $f : X \longrightarrow X'$ が

1. f は全射,
2. $\forall x, y \in X$: $[x \leq y \ \Leftrightarrow \ f(x) \leq' f(y)]$

を満たすとき, f は**順序同型写像**であるという.

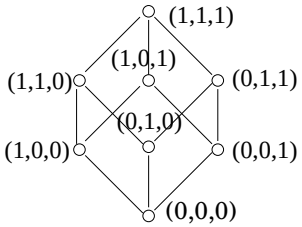
$(X, \leq)$ から $(X', \leq')$ への順序同型写像が存在するとき, $(X, \leq)$ と $(X', \leq')$ は**順序同型**であるという.

順序同型写像の定義より f は全射である. 一方, 任意の $x, y \in X$ に対し, $f(x) = f(y)$ ならば $f(x) \leq f(y)$ より, $x \leq y$. 同様に, $f(y) \leq' f(x)$ より, $y \leq x$. したがって, $x = y$ となり f は単射である. ゆえに, f は全単射である.

例題 5.62 $B = \{0, 1\}$ とする. $B^3 = B \times B \times B$ 上の関係 $\leq$ を次のように定義する: $(x_1, x_2, x_3), (y_1, y_2, y_3) \in B^3$ に対し, 「"$(x_1, x_2, x_3) \leq (y_1, y_2, y_3)$" $\Leftrightarrow$ "$(x_1 \leq y_1) \wedge (x_2 \leq y_2) \wedge (x_3 \leq y_3)$"」を満たすことと定義する.

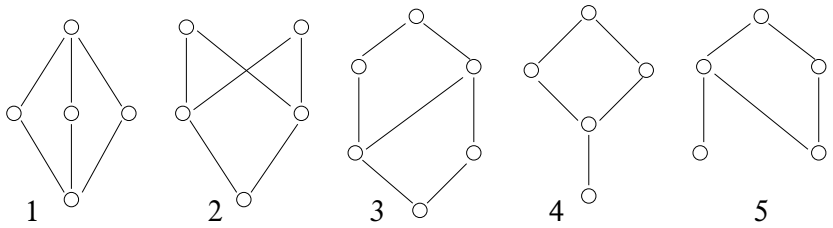
1. 関係 $\leq$ は順序関係であることを示せ.
2. $(B^3, \leq)$ と $(2^S, \subseteq)$ は順序同型であること示せ. ただし, $S = \{a, b, c\}$.

(解答)



定義 5.63 $(X, \leq)$ を順序集合とする. 任意の $x, y \in X$ に対し, 集合 $\{x, y\}$ の $\sup\{x, y\}$ と $\inf\{x, y\}$ が存在するとき, $(X, \leq)$ を**束**という.

例題 5.64 次のハッセ図で示される順序集合は, 束であるかどうか述べよ.



(解) 束である: 1,3,4. 束でない: 2,5.

例題 5.65 X を有限集合とすると, X 上の全順序関係はいくつあるか.
(解) $n!$.

例題 5.66 集合 $\{a, b\}$ 上の順序関係をすべて列挙し, それぞれのハッセ図を示せ.

例題 5.67 R を集合 X 上の同値関係, S を集合 X 上の順序関係とする. このとき, $R \cap S$ は X 上の同値関係となるかどうか答えよ. また, $R \cap S$ は X 上の順序関係となるかどうか答えよ. なるならば証明し, ならないならば反例を述べよ.

5.4 関係の閉包

定義 5.68 R を $X \times Y$ 上の 2 項関係とするとき, $Y \times X$ 上の 2 項関係 R^{-1} を
$R^{-1} := \{(y,x) \mid (x,y) \in R\}$
と定義する. R^{-1} を R の**逆関係**という.

定義 5.69 R を $X \times Y$ 上の 2 項関係, S を $Y \times Z$ 上の 2 項関係とするとき, $X \times Z$ 上の 2 項関係 $R \circ S$ を
$R \circ S := \{(x,z) \mid \exists y \in Y : [((x,y) \in R) \wedge ((y,z) \in S)]\}$
と定義する. $R \circ S$ を R と S の**合成**, あるいは**積**という.

例題 5.70 R, S, T を, それぞれ $X \times Y$, $Y \times Z$, $Z \times W$ 上の 2 項関係とするとき, 結合律 $R \circ (S \circ T) = (R \circ S) \circ T$ が成り立つ.
(証明) $(x,w) \in R \circ (S \circ T) \Leftrightarrow (x,w) \in (R \circ S) \circ T$ を示せばよい.

定義 5.71 R を X 上の関係とする. そのとき, R^+ を以下のように定義する:
1. $R^1 := R$;
2. $n \geq 2$ に対し, $R^n := R^{n-1} \circ R$;
3. $R^+ := \cup_{n=1}^{\infty} R^n$.

例題 5.72 有限集合 X 上の関係 R を表現する行列が与えられているとき, R^2 を表現する行列を求めるにはどうすればよいか. 一般に, R^n を表現する行列を求めるにはどうすればよいか.
(証明) $X = \{x_1, x_2, \ldots, x_n\}$ とし, R を表現する行列を M とする. すると, M の (i,j) 成分 m_{ij} に対し, " $m_{ij} = 1 \Leftrightarrow x_i R x_j \Leftrightarrow (x_i, x_j) \in R$" が成り立つ. このとき, $(x_i, x_k) \in R^2 \Leftrightarrow x_i R^2 x_k \Leftrightarrow x_i (R \circ R) x_k$
$\Leftrightarrow \exists x_j \in X : [(x_i R x_j) \wedge (x_j R x_k)]$
$\Leftrightarrow \exists j \in \{1, 2, \ldots, n\} : [(m_{ij} = 1) \wedge (m_{jk} = 1)]$
$\Leftrightarrow \sum_{j=1}^{n} m_{ij} m_{jk} \neq 0.$
$(m_{i,1}, \ldots, m_{i,n})$ と $(m_{1,j}, \ldots, m_{n,j})$ はそれぞれ M の i 行目と j 行目のベクトルである. そして, $\sum_{j=1}^{n} m_{ij} m_{jk} = (m_{i,1}, \ldots, m_{i,n})(m_{1,j}, \ldots, m_{n,j})^T$ は M^2 の (i,j) 成分である. したがって, R^2 を表現する行列は, i) M^2 の (i,j) 成分が非零ならば 1, ii) そうでなければ 0 と定めた行列となる. R^3 に対応する行列は, $R^2 \circ R$ より, R^2 と R を表現する行列の積で得られたものに, 上記で定めた i) 又は ii) の手続きを行なうことで得られる. 同様の手続きを繰り返すことで, 一般の場合でも得られることが分かる. ∎

R を集合 X 上の関係とする. $x, y \in X$ が xRy を満たすとき, x から y に 1 ステップで**到達可能**であるという. また, $z_1, \ldots, z_n \in X$ が存在し,
$xRz_1 \ \wedge \ z_1 R z_2 \ \wedge \ \cdots \ \wedge \ z_{n-1} R z_n \ \wedge \ z_n R y$
が成り立つとき, x から y に $n+1$ ステップで到達可能であるという. さらに, x から y に有限回数のステップで到達可能であるとき, x から y に到達可能であるという. この言葉を用いて, R^n, R^+ を表すと,
$R^n = \{(x,y) \mid x, y \in X,\ x$ から y に n ステップで到達可能 $\}$,
$R^+ = \{(x,y) \mid x, y \in X,\ x$ から y に到達可能 $\}$.

定理 5.73 R を集合 X 上の関係とするとき, 以下が成り立つ.
1. $R^n = R^{n-k} \circ R^k$. ただし, 非負整数 n, k は $n - k \leq 1$ を満たす.
2. R^+ は推移的な関係である.
3. R' が R を含む推移的な関係ならば, $R^+ \subseteq R'$.

(証明) 3. 任意の $n \geq 1$ に対し, $R^n \subseteq R'$ が成り立つことを, n に関する数学的帰納法で示せばよい.

定義 5.74 P を反射律, 対称律, 推移律などの関係に関するある性質であるとする. 関係 R を含み, 性質 P をもつような関係の中で最小のものを R の**閉包**という. すなわち, 閉包 R' とは,

1. $R \subseteq R'$,
2. R' は P を満たす,
3. “$R \subseteq R''$” かつ “R'' は P を満たす” ならば “$R' \subseteq R''$.”

例題 5.75 R の P 閉包は一意に定まる.
(証明) 「一意である」ことを示すには, R' と R'' を R の P 閉包と仮定すると, $R' = R''$ となることを示せばよい.

定義 5.76 R を集合 X 上の関係とする. 性質 P として, 反射律, 対称律, 推移律をとったとき, R の P 閉包をそれぞれ**反射閉包**, **対称閉包**, **推移閉包**という.

定理 5.77 R を関係とするとき以下が成り立つ.
1. “R が反射的” $\Leftrightarrow$ “R 自身が R の反射閉包”
2. “R が対称的” $\Leftrightarrow$ “R 自身が R の対称閉包”
3. “R が推移的” $\Leftrightarrow$ “R 自身が R の推移閉包”

定義 5.78 R を関係とするとき以下が成り立つ.
1. $R \cup R_{\min}$ は R の反射閉包. ただし, $R_{\min} = \{(x, x) \mid x \in X\}$.
2. $R \cup R^{-1}$ は R の対称閉包. ただし, $R^{-1} = \{(y, x) \mid (x, y) \in R\}$.
3. R^+ は R の推移閉包. ただし, $R^+ = \cup_{n=1}^{\infty} R^n$.

例題 5.79 $X = \{a, b, c, d\}$ とし, $R = \{(a, a), (a, b), (c, a), (c, c), (d, c)\}$ とするとき, R の反射閉包, 対称閉包, 推移閉包のそれぞれを求めよ.
(解答)
1. $R_{\min} = \{(a, a), (b, b), (c, c), (d, d)\}$ より, $R \cup R_{\min} = \{(a, a), (a, b), (c, a), (c, c), (d, c), (b, b), (d, d)\}$.
2. $R^{-1} = \{(a, a), (b, a), (a, c), (c, c), (c, d)\}$ より, $R \cup R^{-1} = \{(a, a), (a, b), (c, a), (c, c), (d, c), (b, a), (a, c), (c, d)\}$.
3. R を表現する行列 M は

	a	b	c	d
a	1	1	0	0
b	0	0	0	0
c	1	0	1	0
d	0	0	1	0

で与えられる. これより, 関係 R^n を表現する行列を $M(R^n)$ と表し, それらを計算すると以下のようになる:

$$M^2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \rightarrow M(R^2) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$M^3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 2 & 1 & 1 & 0 \end{bmatrix} \rightarrow M(R^3) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$M^4 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 4 & 3 & 1 & 0 \\ 3 & 2 & 1 & 0 \end{bmatrix} \rightarrow M(R^4) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$M^5 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 5 & 4 & 1 & 0 \\ 4 & 3 & 1 & 0 \end{bmatrix} \rightarrow M(R^5) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

したがって, $M(R^3) = M(R^4) = M(R^5) = \cdots$ となることが分かる. すなわち, このことは, $R^3 = R^4 = R^5 = \cdots$ を表している. これより, $R^+ = R^1 \cup R^2 \cup R^3$ となる. よって,
$R^2 = \{(a, a), (a, b), (c, a), (c, c), (d, c), (c, b), (d, a)\}$ と
$R^3 = \{(a, a), (a, b), (c, a), (c, c), (d, c), (c, b), (d, a), (d, b)\}$ より,
$R^+ = \{(a, a), (a, b), (c, a), (c, c), (d, c), (c, b), (d, a), (d, b)\}$ となる.

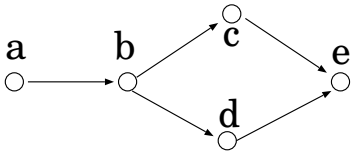
例題 5.80 $X = \{a, b, c, d\}$ とし, X 上の関係を $R = \{(a, a), (a, b), (b, c), (d, d)\}$ とするとき, R^n, $n = 2, 3$ を求めよ. R を含む最小の同値関係を求めよ.

5.5 グラフと隣接行列

5.5.1 その 1 (パスの本数)

前節までは, 与えられた集合 X 上の関係 R を表現する行列やグラフを考えていた. ここでは, 最初に, グラフまたは行列が与えられた場合について考える.

まず, 以下のようなグラフが与えられたとする. 頂点は, a, b, c, d, e の 5 個であることより, 集合



$X = \{a, b, c, d, e\}$. そして, グラフの有向辺より, 関係 $R = \{(a, b), (b, c), (b, d), (c, e), (d, e)\} (\subseteq X^2)$. さらに, この関係を表す行列 M は次のようになる. このように, 有向グラフ上の頂点間の隣接状況を表す行列を, グラフの**隣接行列**という.

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \Leftrightarrow \begin{array}{c|ccccc} & a & b & c & d & e \\ \hline a & 0 & 1 & 0 & 0 & 0 \\ b & 0 & 0 & 1 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 1 \\ d & 0 & 0 & 0 & 0 & 1 \\ e & 0 & 0 & 0 & 0 & 0 \end{array}$$

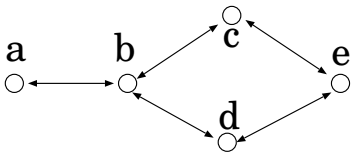
このとき, $R^n = \{(x, y) \mid x, y \in X, x$ から y に n ステップで到達可能 $\}$ に関する内容を, もう少し丁寧に詳しく調べてみる. それには, R^n に隣接行列 M の n 乗 M^n の成分について考える. まずは, M^2, M^3, M^4 を計算してみると以下のようになる.

$$M^2 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad M^3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad M^4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

このとき, 以下のような考察が得られる.

1. 行列 M^2 の (b, e) 成分の値が 2 であるのは, b から e へ 2 ステップで到達するパス (path) が 2 本あることを表す. ここで, 頂点 x から 頂点 y へ到達するパスとは, 有限個の有向辺と頂点を経由することで, x から y へ到達できる経路のこと.
2. 同様に, 行列 M^3 の (a, e) 成分の値が 2 であるのは, a から e へ 3 ステップで到達するパスが 2 本あることを表す.
3. 一方, 行列 M^1 と M^2 の (a, e) 成分の値が 0 で, M^3 で初めて (a, e) 成分が非零な値を取るということは, a から e へは少なくとも 3 ステップを要することを示している.
4. 最後に, M^4 が零行列になっていることは, グラフ上の各頂点から 4 ステップ以上で到達するような頂点がないことを表している.

先のグラフにおいて辺に向きがない場合 (両向きを許す場合) は以下のようになる. 辺に向きがないグラフを無向グラフという. この場合の隣接行列 M および M^2, M^3 は以下のようになる.



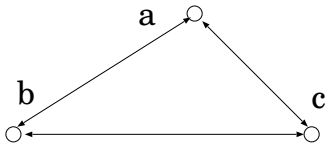
$$M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}, \quad M^2 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 3 & 0 & 0 & 2 \\ 1 & 0 & 2 & 2 & 0 \\ 1 & 0 & 2 & 2 & 0 \\ 0 & 2 & 0 & 2 & 0 \end{bmatrix}, \quad M^3 = \begin{bmatrix} 0 & 3 & 0 & 0 & 2 \\ 2 & 0 & 5 & 5 & 0 \\ 0 & 5 & 0 & 0 & 4 \\ 0 & 5 & 0 & 0 & 0 \\ 2 & 0 & 4 & 4 & 0 \end{bmatrix}.$$

このとき, 以下のような考察が得られる.

1. 隣接行列 M は対称行列になっている.
2. 無向グラフの場合でも, a から e へ到達するには, 少なくとも 3 ステップ必要であることが分かる. なぜなら, 行列 M^1 と M^2 の (a,e) 成分の値が 0 で, M^3 で初めて (a,e) 成分が非零な値を取るから.
3. たとえば, M^3 で (a,b) 成分の値が 3 であることは, a から b へ 3 ステップで到達するパスが 3 本あることを表す. それらのパスは, 次の通り: $(a \to b \to a \to b)$, $(a \to b \to c \to b)$, $(a \to b \to d \to b)$. ここで, 上記の “3 ステップ” と “3 本” の “ 3 ” は, たまたま同じ 3 になっただけで, その関係に深い意味はない.

5.5.2 その 2 (三角形の数)

さて, 次に, 以下のような無向グラフで表された三角形について考えよう. この場合, 集合 $X =$

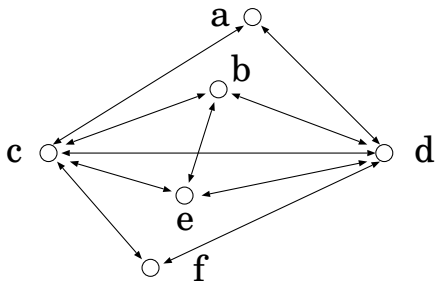


$\{a,b,c\}$, 関係 $R = \{(a,b),(a,c),(b,a),(b,c),(c,b),(c,a)\}(\subseteq X^2)$ となっている. そして, 隣接行列 M および M^2, M^3 を計算すると以下のようになる.

$$M = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad M^2 = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}, \quad M^3 = \begin{bmatrix} 2 & 3 & 3 \\ 3 & 2 & 3 \\ 3 & 3 & 2 \end{bmatrix}.$$

ここでは, 特に, M^3 の対角成分の値に着目する. M^3 の (a,a) 成分の 2 は, a から a に 3 ステップで戻るパスの本数を表す. これらのパスは, $(a \to b \to c \to a)$ と $(a \to c \to b \to a)$ である. これは, 頂点 a を起点とするパスであるが, 一方で, 無向グラフの中で, 頂点 a を含む三角形の数に関係している. 具体的には, (a,a) 成分の 2 は, 無向グラフの中に現れる $\triangle abc$ を 2 重に数えていることになる. 同時に, (b,b) 成分や (c,c) 成分の 2 も同じ$\triangle abc$ を 2 重に数えていることに関連する. したがって, M^3 の対角成分の総和を $6(=2\times 3)$ で割った値 $\frac{1}{6}(2+2+2)=1$ が, 無向グラフの中に現れる三角形の総数を表す.

それでは, 次の無向グラフの中には, 幾つの三角形があるか計算してみよう.



隣接行列 M および M^3 を計算すると以下のようになる.

$$M = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}, \quad M^3 = \begin{bmatrix} 2 & 4 & 9 & 9 & 4 & 2 \\ 4 & 6 & 11 & 11 & 7 & 4 \\ 9 & 11 & 10 & 11 & 11 & 9 \\ 9 & 11 & 11 & 10 & 11 & 9 \\ 4 & 7 & 11 & 11 & 6 & 4 \\ 2 & 4 & 9 & 9 & 4 & 2 \end{bmatrix}.$$

これより, 無向グラフの中の三角形の数は, $\frac{1}{6}(2+6+10+10+6+2)=6$. ∎

参考文献

[1] 尾関和彦, (情報技術者のための) 離散系数学入門, 共立出版, 2004.

[2] 松坂和夫, 集合・位相入門, 岩波書店, 2003.

[3] 松坂和夫, 代数系入門, 岩波書店, 2003.

[4] S. Lipschutz 著, 成嶋弘監訳, 離散数学 (コンピュータサイエンスの基礎数学), オーム社, 2004(H16).

[5] 小倉久和, 情報の基礎離散数学 (– 演習を中心とした –), 近代科学社, 2006.

[6] 町田元, 横森貴, 計算機数学, 森北出版, 1990.