■12 群（電子情報通信基礎）- 2 編（離散数学）

1章 基 礎

（執筆者：高橋俊彦）[2009 年 5 月 受領]

■概要■

本章では集合, 関係, 写像に関する基礎的な概念及び記法の定義を与える. これらは離散数学を議論するための言葉であるにもかかわらず, 文献によって異なる定義が与えられているものが少なくない. 本章で採用した定義は離散数学の教科書及び入門書の比較・検討に基づくものであるが, 特に重要と思われるものを以下に述べておく.

集合は基本的概念であるがゆえにその定義が困難である. 本章では集合を単にものの集まりと定義する. いくつかの文献では, ものは識別可能である[1, 2, 3, 4], あるいは, ものは集まりへの所属が明確である[4, 5]などの条件を付加しているが, いずれにせよ言葉の言い換えの域を脱しない. なお「集合」や「属する」などの言葉を無定義語とする公理論的集合論があることに触れている教科書もある[4, 6, 7].

関係の定義域及び値域を定義している文献は少ないが, 大別して, 関係 $R \subseteq A \times B$ に対し, (a) 集合 A を定義域, 集合 B を値域と定義するもの[8, 9], (b) 集合 $\{a \mid (a,b) \in R$ となる $b \in B$ が存在する $\}$ を定義域, 集合 $\{b \mid (a,b) \in R$ となる $a \in A$ が存在する $\}$ を値域と定義するもの[10, 11, 12] の 2 通りがある. 本章では (a) を採用した.

関係 R と S の合成関係 $\{(a,c) \mid (a,b) \in R, (b,c) \in S\}$ の表記は (c) $R \circ S$ と表すもの[11, 13, 14], (d) $S \circ R$ と表すもの[1, 15, 16] の 2 通りがある. 本章では (d) の定義を採用した.

写像 $f : X \to Y$ の値域の定義及びその日本語と英語の対応には全く統一が見られない. 日本語の値域は, (e) Y と定義するもの[1, 6, 9, 17], (f) X の像 $f(X)$ と定義するもの[3, 4, 8, 10, 11, 12, 18, 19] に大別される.

一方, 値域に対応する英語は codomain あるいは range が用いられており, (g) Y を codomain と定義するもの[7, 9, 14, 16, 19, 20, 21], (h) $f(X)$ を range と定義するもの[3, 4, 8, 9, 10, 11, 12, 15] に大別される. なお, 必ずしも (e) と (g), (f) と (h) が対応しているわけではない. 本章では, (e) 及び (g) を採用した.

有限集合と無限集合の定義については 1-5 節で述べるように 2 通りを示した. これは両者を示し, 比較することに意義があると判断したためである.

濃度は有限集合における要素数の概念を無限集合の場合に拡張したものであるが,「濃度が等しい」ことの定義は与えつつも,「濃度」自体の定義なしに濃度という言葉を使用している文献が少なくない. 本章では濃度の定義の方を与えた.

【本章の構成】

1-1 節は最も基礎的な概念である集合について述べる. 関係と写像はともに 2 集合間の対応であるが, 本章では写像を関係の特別な場合と考え, 1-2 節で関係, 1-3 節で写像について述べる. 1-4 節は数学的帰納法と再帰的定義について述べる. 自然数の集合という無限集合に対する形式的かつ有限長の記述がここで与えられる. 最後に 1-5 節で無限集合について述べる.

■12 群 - 2 編 - 1 章

1-1 集　合

（執筆者：高橋俊彦）[2009 年 5 月 受領]

1-1-1 集　合

集合（set）とはものの集まりである．集合に属するそれぞれのものを要素（element）あるいは元と呼ぶ．a が集合 A の要素である（A に属する）ことを $a \in A$ で表し，そうでないことを $a \notin A$ で表す．集合名はアルファベットの大文字，要素名は小文字により表すことが多い．

(1) 外延的定義と内包的定義

外延的定義（extensional definition）は要素名をすべて書き並べて集合を定義する方法である．要素名を「,」で区切った並びを「{」と「}」で挟む．例えば，集合 $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ は 9 つの自然数 $1, 2, 3, 4, 5, 6, 7, 8, 9$ からなる集合である．ただし，「...」を用いて，記述の一部を省略することがある．例えば，上記の A を $A = \{1, 2, \ldots, 9\}$ などと表す．この省略記号は無限集合に対して濫用される．例えば，すべての自然数の集合を $\{1, 2, 3, \ldots\}$ などと表す．

内包的定義（intensional definition）は要素の性質の記述により集合を定義する方法である．一般には，変数を用いて表される要素とその変数が満たすべき性質を「|」あるいは「:」で区切り，「{」と「}」で挟む．ただし，変数 x と述語（predicate）$P(x)$ を用いて，$\{x \mid P(x)\}$ と表すことが多い．例えば，集合 $A = \{2, 4, 6, 8, 10\}$ は $A = \{x \mid x$ は 2 以上 10 以下の自然数 $\}$ あるいは $A = \{2x \mid x$ は 1 以上 5 以下の自然数 $\}$ などと表すことができる．

集合を定義する方法として，このほかに再帰的定義がある〔本章 1-4-3 参照〕．

(2) 要素数

要素数が有限の集合を有限集合（finite set），無限の集合を無限集合（infinite set）という〔本章 1-5 参照〕．有限集合 A の要素数を $|A|$ あるいは $\#A$ で表す．要素をもたない集合，すなわち要素数 0 の集合を空集合（empty set）と呼び，$\emptyset$ あるいは $\{\}$ で表す．空集合はただ一つ存在する．

(3) 部分集合

集合 A の要素がすべて集合 B の要素であるとき，A を B の部分集合（subset）と呼び，$A \subseteq B$ あるいは $B \supseteq A$ と表す．$A \subseteq B$ かつ $A \supseteq B$，すなわち集合 A と集合 B が同じ要素からなるとき，A と B は等しいといい，$A = B$ と表す．A と B が等しくないことを，$A \neq B$ と表す．

$A \subseteq B$ かつ $A \neq B$ のとき，A は B の真部分集合（proper subset）であるといい，$A \subset B$ と表す．*.

任意の集合 A に対し，以下が成り立つ．

$$\text{反射律}: A \subseteq A. \tag{1・1}$$

$$\text{推移律}: A \subseteq B \text{ かつ } B \subseteq C \text{ ならば } A \subseteq C. \tag{1・2}$$

(4) 集合族

集合を要素とする集合を特に集合族（family）と呼ぶ．集合族 F の任意の要素 $S \in F$ があ

* 記号「$\subset$」を部分集合に対して，すなわち「$\subseteq$」の意味で用いている文献もある[14, 19]．

る集合 A の部分集合であるとき，F を集合 A 上の集合族と呼ぶ．集合 A 上の集合族 F に対し，要素 $a \in A$ が属する F の要素（集合）の数を a の F における位数（order）という．

(5) 数の集合

自然数や有理数など，数の集合は以下に示すような太字のアルファベットで表される．

$\mathbb{N}$: すべての自然数の集合．本章では $\mathbb{N} = \{0, 1, 2, \ldots\}$ とする．

$\mathbb{Z}$: すべての整数の集合．

$\mathbb{Q}$: すべての有理数の集合．

$\mathbb{R}$: すべての実数の集合．

$\mathbb{C}$: すべての複素数の集合．

1-1-2 集合の演算

集合 A, B に対して 2 項演算が定義できる．

(1) 和集合

集合 A, B のいずれかに属する（両方に属する場合も含む）要素全体からなる集合 $\{x \mid x \in A$ または $x \in B\}$ を A と B の和あるいは和集合（union）と呼び，$A \cup B$ と表す．和集合は結びとも呼ばれる．

任意の集合 A, B, C に対して以下の性質が成り立つ．

$$\text{恒等律: } A \cup \emptyset = \emptyset \cup A = A. \tag{1・3}$$

$$\text{べき等律: } A \cup A = A. \tag{1・4}$$

$$\text{交換律: } A \cup B = B \cup A. \tag{1・5}$$

$$\text{結合律: } (A \cup B) \cup C = A \cup (B \cup C). \tag{1・6}$$

結合律により，集合 $A_1, \cdots, A_n$ の和を，括弧を省略して $A_1 \cup \cdots \cup A_n$ と表すことができる．また，集合 I の要素 i に対し，集合 A_i が定まるとき，I のすべての要素 i についての A_i の和を $\bigcup_{i \in I} A_i$ と表す．集合 I は添字集合（index set）と呼ばれる．

(2) 積集合

集合 A, B の両方に属する要素全体からなる集合 $\{x \mid x \in A$ かつ $x \in B\}$ を A と B の積あるいは積集合（intersection）と呼び，$A \cap B$ と表す．積集合は共通部分あるいは交わりとも呼ばれる．

任意の集合 A, B, C に対して以下の性質が成り立つ．

$$\text{支配律: } A \cap \emptyset = \emptyset \cap A = \emptyset. \tag{1・7}$$

$$\text{べき等律: } A \cap A = A. \tag{1・8}$$

$$\text{交換律: } A \cap B = B \cap A. \tag{1・9}$$

$$\text{結合律: } (A \cap B) \cap C = A \cap (B \cap C). \tag{1・10}$$

結合律により，集合 $A_1, \cdots, A_n$ の積を，括弧を省略して $A_1 \cap \cdots \cap A_n$ と表すことができ

る．添字集合 I を用いた表記 $\bigcap_{i\in I} A_i$ も和集合の場合と同様である．

$A \cap B = \emptyset$ であるとき，すなわち A と B が共通要素をもたないとき，それらは互いに素あるいは交わらない（disjoint）と呼ばれる．集合 A,B が互いに素であるとき，$A \cup B$ を $A + B$ と表し，A と B の直和（direct sum）と呼ぶ．

A, B, C を集合とするとき，和と積に関して，以下の分配律が成り立つ．

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{1・11}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{1・12}$$

また，以下の吸収律が成り立つ．

$$A \cap (A \cup B) = A. \tag{1・13}$$

$$A \cup (A \cap B) = A. \tag{1・14}$$

（3）差集合

集合 A に属するが集合 B に属さない要素全体からなる集合 $\{x \mid x \in A$ かつ $x \notin B\}$ を A と B の差あるいは差集合（difference）と呼び，$A - B$ と表す．$A - B$ を $A \backslash B$ と表すこともある．

（4）対称差

集合 A と B のいずれか一方のみに属する要素よりなる集合 $(A - B) \cup (B - A)$ を P と Q の対称差（symmetric difference）と呼び，$P \oplus Q$ と表す．$A \oplus B$ を $A \Delta B$ と表すこともある．

1-1-3 補集合

集合 A が集合 U の部分集合であるとき，$U - A$ を U に関する A の補集合（complement）と呼ぶ．特に U が議論の対象としているすべての要素からなる集合であるとき，U を普遍集合（universal set）あるいは全体集合と呼ぶ．普遍集合 U が明らかである場合，$U - A$ を単に A の補集合といい，$\overline{A}$ と表す．なお，$\overline{A}$ を A^c と表すこともある．

普遍集合 U と集合 $A \subseteq U$ に対して，以下が成り立つ．

$$\overline{\emptyset} = U,\ \overline{U} = \emptyset. \tag{1・15}$$

$$\text{支配律: } \overline{A} \cup A = U,\ \overline{A} \cap A = \emptyset. \tag{1・16}$$

$$\text{復元律: } \overline{\overline{A}} = A. \tag{1・17}$$

1-1-4 ド・モルガンの法則（De Morgan's laws）

A, B を集合とするとき，以下が成り立つ．

$$\overline{A \cap B} = \overline{A} \cup \overline{B}. \tag{1・18}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}. \tag{1・19}$$

ド・モルガンの法則に見られるように，集合の演算に関する公式は $\cup$ と $\cap$ を入れ替え，U

（全体集合）と $\emptyset$ を入れ換えても成り立つ．この性質を双対性と呼ぶ．

1-1-5 べき集合

集合 A のすべての部分集合からなる集合を A のべき集合（power set）といい，2^A あるいは $\mathcal{P}(A)$ と表す．すなわち，$2^A = \{S \mid S \subseteq A\}$ である．例えば，$A = \{1,2,3\}$ に対し，$2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$．特に，$\emptyset \in 2^A, A \in 2^A$ であることに注意．

また，べき集合の要素数について以下が成り立つ．

$$| 2^A | = 2^{|A|}. \tag{1・20}$$

■12 群 - 2 編 - 1 章

1-2 関　係

（執筆者：高橋俊彦）［2009 年 5 月 受領］

1-2-1 順序対と直積

集合 A, B からそれぞれ一つずつ要素 $a \in A, b \in B$ を取り出し，この順番に並べた対 (a, b) を順序対（ordered pair）と呼ぶ．A と B の順序対全体の集合 $\{(a, b) \mid a \in A$ かつ $b \in B\}$ を A と B の直積（direct product）あるいはデカルト積（Cartesian product）と呼び，$A \times B$ と表す．任意の集合 A に対し，

$$A \times \emptyset = \emptyset \times A = \emptyset. \tag{1·21}$$

また，A, B が有限集合のとき，

$$| A \times B | = | A | \times | B | . \tag{1·22}$$

1-2-2 2 項関係

集合 A,B に対し，$A \times B$ の部分集合 R を A から B への 2 項関係（binary relation）あるいは単に関係と呼ぶ．以下では，特に断らない限り関係とは 2 項関係を指す．

A を R の定義域（domain），B を値域（codomain）と呼ぶ．定義域と値域がともに A であるとき，$R \subseteq A \times A$ を A 上の関係と呼ぶ．$(a, b) \in R$ は $R(a, b)$ あるいは aRb とも表される．

R が A から B への関係であるとき，集合 $\{(b, a) \mid (a, b) \in R\}$ は B から A への関係となる．これを R の逆関係（inverse relation）と呼び，R^{-1} と表す．

関係 R, S は定義域，値域がそれぞれ等しく，かつ $R = S$ であるとき*，等しいという．

1-2-3 2 項関係の性質

集合 A 上の 2 項関係が満たす性質のなかで特徴的なものを示す．

(1) 反射律

任意の $a \in A$ に対し，$(a, a) \in R$．このとき R は反射的（reflexive）であるという．

(2) 対称律

$(a, b) \in R$ ならば $(b, a) \in R$．このとき R は対称的（symmetric）であるという．

(3) 反対称律

$(a, b) \in R$ かつ $a \neq b$ ならば $(b, a) \notin R$．このとき R は反対称的（antisymmetric）であるという．

(4) 推移律

$(a, b) \in R, (b, c) \in R$ ならば $(a, c) \in R$．このとき R は推移的（transitive）であるという．

1-2-4 関係の合成

集合 A から集合 B への関係 $R \subseteq A \times B$, 集合 B から集合 C への関係 $S \subseteq B \times C$ に対し，集合

* この等号は集合として R と S が等しい，という意味である．

$\{(a,c) \mid R(a,b)$ かつ $S(b,c)\} \subseteq A \times C$ は関係となる．この関係を R と S の合成（composition）と呼び，$S \circ R$ と表す．

合成は結合律を満たす．すなわち，関係 $R \subseteq A \times B$，$S \subseteq B \times C$，$T \subseteq C \times D$ に対し，

$$T \circ (S \circ R) = (T \circ S) \circ R. \tag{1・23}$$

$n \geq 2$ に対し，関係 R を n 個合成したものを R^n と書く．また，$n = 1$ に対し $R^1 = R$，$n = 0$ に対し $R^0 = \{(a,a) \mid a \in A\}$ とする．R^0 は恒等関係（identity relation）と呼ばれる．

1-2-5 閉　包

R を集合 A 上の関係，S を R を部分集合とする性質 $\mathcal{P}$ を満たす A 上の関係とする．性質 $\mathcal{P}$ を満たす任意の関係 $S' \supseteq R$ に対し，$S' \supseteq S$ であるとき，S を R の $\mathcal{P}$-閉包（$\mathcal{P}$-closure）と呼ぶ．

R の推移的閉包（transitive closure）及び反射的推移的閉包（reflexive transitive closure）はそれぞれ性質 $\mathcal{P}$ を ‘反射的’ 及び ‘反射的かつ推移的’ としたときの $\mathcal{P}$-閉包である．これらはそれぞれ以下の式で与えられる関係 R^+ 及び R^* に等しい．

$$R^+ = R^1 \cup R^2 \cup R^3 \cup \cdots = \bigcup_{i=1}^{\infty} R^i \tag{1・24}$$

$$R^* = R^0 \cup R^1 \cup R^2 \cup \cdots = \bigcup_{i=0}^{\infty} R^i \tag{1・25}$$

1-2-6 同値関係

反射的，対称的，かつ推移的関係を同値関係（equivalence relation）と呼び，記号「≡」で表す*．要素 $a \in A$ に対し，集合 $\{b \in A \mid a \equiv b\}$ を a の同値類（equivalence class）と呼び，$[a]_{\equiv}$ と表す．このとき，a を同値類 $[a]_{\equiv}$ の代表元（representative）と呼ぶ．

和が集合 A となる互いに素な A の部分集合族 F を A の分割（partition）と呼ぶ．すなわち，$\bigcup_{S \in F} S = A$ かつ任意の $S, T \in F$ に対して，$S \neq T$ ならば $S \cap T = \emptyset$ である．

$\equiv$ を集合 A 上の同値関係とする．このとき，任意の要素 $a, b \in A$ に対し，$[a]_{\equiv} = [b]_{\equiv}$ または $[a]_{\equiv} \cap [b]_{\equiv} = \emptyset$ である．したがって，ある $I \subseteq A$ が存在して，集合族 $F = \{[i]_{\equiv} \mid i \in I\}$ は A の分割 $A = \bigcup_{i \in I} [i]_{\equiv}$ となる．集合族 F を A の $\equiv$ による商集合（quotient set）と呼び，$A/\equiv$ と表す．

逆に集合の分割は同値関係を定める．すなわち，集合 A の分割 F に対し，関係 $R = \{(a,b) \mid$ ある $S \in F$ に対し，$a \in S$ かつ $b \in S\}$ は同値関係となる．

1-2-7 半順序関係

反射的，反対称的，かつ推移的な関係を半順序関係（partial order）あるいは単に順序（order）と呼び，しばしば記号「$\preceq$」で表す．集合 A 上に半順序関係 $\preceq$ が定義されているとき，A を半順序集合（partially ordered set, poset）と呼び，$(A, \preceq)$ と表す．

---

* 記号「~」で表すことも多いが[14, 15, 17]，本章では「~」は集合の対等を表すために用いる．

(1) ハッセ図

半順序集合 $(A, \preceq)$ の要素 $a, b \in A$ に対して，$a \preceq b$ かつ $a \neq b$ であるとき，$a \prec b$ と表す†．$(A, \preceq)$ を以下の方法で視覚化した図をハッセ図（Hasse diagram）と呼ぶ．

1. A の各要素に対応した点を描く．ただし，$a \prec b$ ならば a に対応する点は b に対応する点の下方に置かれる．

2. $a \prec b$ である要素 a, b に対し，$a \prec c \prec b$ となる c が存在しないときかつそのときに限り，要素 a, b に対応する点を線分で結ぶ．

図 1·1 は半順序集合 $(2^{\{1,2,3\}}, \subseteq)$ のハッセ図である．

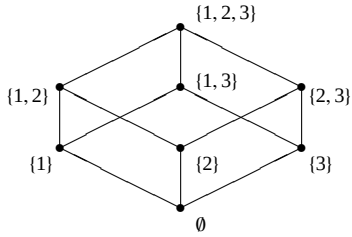

図 1·1　ハッセ図

(2) 比較可能性

要素 a, b に対し，$a \preceq b$ または $b \preceq a$ であるとき，a と b は比較可能（comparable）であるという．そうでないとき，比較不能（incomparable）という．

半順序集合 A の部分集合を S とする．S のどの二つの要素も比較可能であるとき，S を鎖（chain）と呼ぶ．$|S|$ を鎖の長さという．また，S のどの二つの要素も比較不能であるとき，S を反鎖（antichain）と呼ぶ．

(3) 極大元，極小元，最大元，最小元

$B \subseteq A$ とする．要素 $a_0 \in B$ に対し，$a_0 \prec a$ となる要素 $a \in B$ が存在しないとき，a_0 は B で極大（maximal）である，あるいは B の極大元であるという．また，$a \prec a_0$ となる要素 $a \in B$ が存在しないとき，a_0 は B で極小（minimal）である，あるいは B の極小元であるという．

要素 $a_0 \in B$ に対し，a_0 が B のすべての要素と比較可能であり，かつ $a_0 \prec a$ となる要素 $a \in B$ が存在しないとき，a_0 は B で最大（maximum）である，あるいは B の最大元であるという．また，a_0 が B のすべての要素と比較可能であり，かつ $a \prec a_0$ となる要素 $a \in B$ が存在しないとき，a_0 は B で最小（minimum）である，あるいは B の最小元であるという．

1-2-8 全順序関係

どの二つの要素も比較可能であるような半順序関係 $(A, \preceq)$ を全順序関係（total order）あるいは線形順序関係（linear order）と呼ぶ．また，このとき $(A, \preceq)$ を全順序集合（totally ordered set）と呼ぶ．$(A, \preceq)$ が全順序集合であることは A が鎖であることにほかならない．

† 「$\prec$」は擬順序（quasi-order）と呼ばれる．

■12 群 - 2 編 - 1 章

1-3 写　像

（執筆者：高橋俊彦）［2009 年 5 月 受領］

1-3-1 写　像

集合 X のどの要素にも集合 Y のある要素がただ一つだけ対応しているとき，この対応を X から Y への写像（mapping）あるいは関数（函数）（function）と呼び，$f : X \to Y$ と表す．X を定義域（domain），Y を値域（codomain）と呼び，それぞれ $X = \mathbf{dom}(f)$, $Y = \mathbf{codom}(f)$ と表す．

二つの写像 f, g は定義域，値域，各要素の像がいずれも等しいとき，すなわち $\mathbf{dom}(f) = \mathbf{dom}(g)$, $\mathbf{codom}(f) = \mathbf{codom}(g)$, すべての $x \in \mathbf{dom}(f)$ に対して $f(x) = g(x)$ であるとき，等しいといい，$f = g$ と表す．

(1) 制限と拡大

写像 f に対し，定義域を $A \subseteq \mathbf{dom}(f)$ に制限した写像を f の A への制限（restriction）と呼び，$f|_A$ と表す．また，f は $f|_A$ の拡大あるいは拡張（extension）と呼ばれる．

(2) 像と逆像

写像 $f : X \to Y$ によって $x \in X$ に $y \in Y$ が対応づけられているとき，y を x の像（image）と呼び，$y = f(x)$ あるいは $f : x \mapsto y$ と表す．また，$A \subseteq X$ に対し，$f(A) = \{y \mid \text{ある } x \in A \text{ に対し}, y = f(x)\}$ を f による A の像と呼ぶ．特に，$A = X$ のとき，$f(X)$ を写像 f の像と呼び，$\mathbf{range}(f)$ と表す．

写像 $f : X \to Y$ に対し，その像が集合 $B \subseteq Y$ の要素となる X の要素の集合 $\{x \mid x \in X, f(x) \in B\}$ を B の f による逆像（inverse image）あるいは原像（preimage）と呼び，$f^{-1}(B)$ と表す．

1-3-2 合成写像

二つの写像 $f : X \to Y, g : Y \to Z$ に対し，$x \in X$ を $g(f(x))$ に対応させる写像を f と g の合成写像（composition）と呼び，$g \circ f$ と表す．$g \circ f$ の定義域は X，値域は Z，すなわち $g \circ f : X \to Z$ である．任意の写像 f, g, h に対し，合成写像 $g \circ f$ 及び $h \circ g$ が定義されるならば，$h \circ (g \circ f) = (h \circ g) \circ f$ である，すなわち写像の合成は結合律を満たす．

1-3-3 単射，全射，全単射

(1) 単　射

$f : X \to Y$ を写像とする．任意の $x_1, x_2 \in X$ に対し，$x_1 \neq x_2$ ならば $f(x_1) \neq f(x_2)$ が成り立つとき写像 f を単射（injection）あるいは 1 対 1（one-to-one）という．

単射 f, g に対して，合成写像 $g \circ f$ が定義されるならば，それは単射となる．また，写像 f, g の合成写像 $g \circ f$ が単射であるならば，f は単射である（g は単射とは限らない）．

(2) 全　射

$f : X \to Y$ を写像とする．任意の $y \in Y$ に対し，$f(x) = y$ となる $x \in X$ が存在するとき，すなわち $f(X) = Y$ であるとき，f を全射（surjection）あるいは上への（onto）写像という．

全射 f, g に対して，合成写像 $g \circ f$ が定義されるならば，それは全射となる．また，写像 f, g の合成写像 $g \circ f$ が全射であるならば，g は全射である（f は全射とは限らない）．

(3) 全単射

全射かつ単射である写像は全単射あるいは双射（bijection）と呼ばれる．

全単射 f, g に対して，合成写像 $g \circ f$ が定義されるならば，それは全単射となる．また，写像 f, g の合成写像 $g \circ f$ が全単射であるならば，f は単射であり，g は全射である．有限集合 X からそれ自身への全単射 $f : X \to X$ を X の置換（permutation）と呼ぶ．

1-3-4 逆写像

写像 $f : X \to Y$ が全単射であるとき，任意の $y \in Y$ に対し，$y = f(x)$ となる $x \in X$ が一意に定まる．このとき y に x を対応させる写像を f の逆写像（inverse mapping）と呼び f^{-1} で表す．

f^{-1} もまた全単射であり，その逆写像 $(f^{-1})^{-1}$ が定義できる．$(f^{-1})^{-1} = f$ である．

1-3-5 定数関数

すべての $x \in \mathbf{dom}(f)$ に対する像が等しいとき，すなわちある $a \in \mathbf{codom}(f)$ に対し，$f(\mathbf{dom}(f)) = \{a\}$ となるとき，f を定数関数（constant function）あるいは定値写像と呼ぶ．

1-3-6 恒等写像

$f : X \to Y$ を写像とする．すべての $x \in X$ に対し $f(x) = x$ であるとき，f を恒等写像あるいは恒等関数（identity function）と呼ぶ．

■12 群 - 2 編 - 1 章

1-4 数学的帰納法と再帰的定義

（執筆者：高橋俊彦）［2009 年 5 月 受領］

1-4-1 数学的帰納法

$P(n)$ を自然数 n を変数とする述語〔本編 7 章 7-2 参照〕とする．数学的帰納法（mathematical induction）は命題「任意の $n \in \mathbb{N}$ に対して，$P(n)$ が成り立つ」を証明する技法（原理）である．

(1) 数学的帰納法

任意の $n \in \mathbb{N}$ に対して，$P(n)$ が成り立つことを示すためには，次の二つが成り立つことを示せばよい：

1. 命題 $P(0)$ が成り立つ．
2. 任意の n に対し，命題 $P(n)$ が成り立つならば，命題 $P(n+1)$ も成り立つ．

1. を帰納法の基礎，2. を帰納の段階という．また，2 における命題 $P(n)$ が成り立つという仮定を帰納法の仮定という．

(2) 強数学的帰納法

強数学的帰納法は，帰納の段階における仮定が強められているため (1) の数学的帰納法より強力であるが，等価な原理である．

任意の $n \in \mathbb{N}$ に対して，$P(n)$ が成り立つことを示すためには，次の二つが成り立つことを示せばよい：

1. 命題 $P(0)$ が成り立つ．
2. 任意の $k \leq n$ に対し，命題 $P(k)$ が成り立つならば，命題 $P(n+1)$ も成り立つ．

(3) 多重帰納法

多重帰納法は複数の自然数に関する命題を証明する技法（原理）である．例として二重帰納法を示す．

任意の自然数 $m, n \in \mathbb{N}$ に対して，命題 $P(m,n)$ が成り立つことを示すためには，次の二つが成り立つことを示せばよい：

1. 命題 $P(0,0)$ が成り立つ．
2. 任意の m, n に対し，命題 $P(m,n)$ が成り立つならば，命題 $P(m+1,n)$ 及び $P(m,n+1)$ も成り立つ．

1-4-2 ペアノの公理

ペアノ（Giuseppe Peano, 1858–1932）は自然数の集合 $\mathbb{N}$ を公理により定義した．これをペアノの公理（Peano axioms）と呼ぶ．

次の性質を満たす集合 $\mathbb{N}$ を自然数の集合と呼ぶ.

1. $\mathbb{N}$ は 0 と名付けられた要素を含む．すなわち，$0 \in \mathbb{N}$.
2. 以下の性質を満たす写像 $\sigma : \mathbb{N} \to \mathbb{N}$ が存在する．$\sigma(n)$ は n の後者と呼ばれる.
   (a) σ は単射である．すなわち，$m \neq n$ ならば $\sigma(m) \neq \sigma(n)$.
   (b) $\sigma(n) = 0$ となる $n \in \mathbb{N}$ はない． すなわち，0 を後者とする要素はない.
   (c) 集合 $\mathbb{N}$ の部分集合 S が 0 を含み，かつ任意の $n \in S$ に対し，$\sigma(n) \in S$ となるならば，$S = \mathbb{N}$.

数学的帰納法の正当性はペアノの公理の 2(c) に基づく．すなわち，帰納法の基礎と帰納の段階が成立するような数 n の集合 S は公理 2(c) により自然数の集合 $\mathbb{N}$ に等しい.

1-4-3 再帰的定義

再帰的定義（recursive definition）は無限集合 S を有限長の記述により定義する方法の一つであり, 以下のステップからなる：

（a）初期ステップ

S に含まれる要素を有限個列挙する．すなわち，$S_0 \subseteq S (S_0 \neq \emptyset)$ を外延的に定義する.

（b）再帰ステップ

S に含まれる要素により，（新たな）S の要素を定義する.

（c）限定句

S の要素は初期ステップあるいは再帰ステップの有限回の適用により定義されるものに限ることを述べる.

ペアノの公理による自然数の定義は再帰的定義の例である．再帰的定義は帰納的定義（inductive definition）とも呼ばれる.

■12 群 - 2 編 - 1 章

1-5 無限集合

（執筆者：高橋俊彦）［2009 年 5 月 受領］

1-5-1 無限集合

離散数学あるいは情報数学の教科書や入門書における有限集合及び無限集合の定義は大別して以下の 2 通りである．

（1）有限集合でないものを無限集合と定義する[2, 19)]

集合 A とある自然数 n に対する集合 $\{1, 2, \ldots, n\}$ との間に全単射が存在するとき，A を有限集合と呼ぶ．有限集合でない集合を無限集合と呼ぶ．

（2）無限集合でないものを有限集合と定義する[2, 4, 9)]

集合 A とその真部分集合 $A' \subset A$ との間に全単射が存在するとき，A を無限集合と呼ぶ．無限集合でない集合を有限集合と呼ぶ*．例えば，自然数の集合 $\mathbb{N}$ からその真部分集合 $\mathbb{N} - \{0\}$ への写像 $f(n) = n + 1$ は全単射となる．したがって，$\mathbb{N}$ は無限集合である．

(1) の定義は「有限集合はその要素を列挙し尽くせるが無限集合はそうでない」という直観的な理解に近く，分かりやすいように見えるが, 有限集合を定義するために無限集合 $\mathbb{N}$ の存在を仮定していることに注意されたい．

1-5-2 濃　度

集合 A と B の間に全単射が存在するとき，A と B は対等（equipotent）であるといい，$A \sim B$ で表す．

$\sim$ は同値関係であり，すべての集合からなる集合族を同値類に分割する†．各同値類を濃度（cardinality）あるいは基数と呼び，$|A|$ と表す．濃度は大小の比較が可能であるが数ではない．しかし，有限集合に対しては，それがある自然数 n について集合 $\{1, 2, \ldots, n\}$ と対等であるとき，$|A| = n$，すなわち濃度と要素数を同一視する．

自然数の集合 $\mathbb{N}$ の濃度を $\aleph_0$（アレフ・ゼロと読む）と表記する．濃度が $\aleph_0$ である集合を可算集合（countable set）あるいは可算無限集合（countably infinite set）と呼ぶ．有限集合と可算集合をまとめて高々可算集合（at most countable set）と呼ぶ‡．高々可算集合でない集合を非可算集合（uncountable set）と呼ぶ．例えば，実数の集合 $\mathbb{R}$ は非可算である．

■参考文献

1) 守屋 悦朗, “コンピュータサイエンスのための離散数学（Information & computing 61）,” サイエンス社, 1992.
2) C.L. Liu（著）, 成嶋 弘, 秋山 仁（訳）, “コンピュータサイエンスのための 離散数学入門,” オーム社, 1995.
3) 大矢雅則, 佐藤圭子, 井上 啓, “情報数理入門（Information&Computing 別巻 21）,” サイエンス社, 1999.
4) 横森 貴, 小林 聡, “基礎情報数学（ライブラリ新数学大系 E13）,” サイエンス社, 2008.

* デデキント（J. W. R. Dedekind, 1831–1916）による．

† 実際はすべての集合からなる集合族は集合と認められず，より厳密な取り扱い（クラスの概念など）が必要となる．

‡ 高々可算を単に可算と呼ぶ文献もある[14, 20, 21)]

5) 石村園子, “やさしく学べる離散数学,” 共立出版, 2007.
6) 赤間世紀, “離散数学概論—コンピュータサイエンスのための基礎数学,” コロナ社, 1995.
7) R. Garnier and J. Taylor, “Discrete Mathematics for New Technology（2nd edition）,” Taylor & Francis, 2001.
8) 柴田正憲, 浅田由良, “情報科学のための離散数学,” コロナ社, 1995.
9) 佐藤泰介, 高橋篤司, 伊東利哉, 上野修一, “情報基礎数学,” 昭晃堂, 2007.
10) R. Johnsonbaugh, “Discrete Mathematics（The Jk Computer Science and Mathematics Series, 5th edition）,” Prentice Hall College Div., 2000.
11) 牛島和夫, 朝廣雄一, 相 利民, “離散数学（コンピュータサイエンス教科書シリーズ 15）,” コロナ社, 2006.
12) 山崎秀記, “情報科学の基礎—記法・概念・計算とアルゴリズム—Information Science & Engineering F1,” サイエンス社, 2008.
13) 林 晋, 八杉満利子, “情報系の数学入門,” オーム社, 1993.
14) J.L. Hein, “Discrete Mathematics（2nd edition）,” Jones & Bartlett Publishers, 2003.
15) J.K. Truss, “Discrete Mathematics for Computer Scientists（International Computer Science Series, 2nd edition）,” Addison-Wesley, 1999.
16) D.E. Ensley and J.W. Crawley, “Discrete Mathematics, Textbook and Student Solutions Manual: Mathematical Reasoning and Proof with Puzzles, Patterns, and Games,” Wiley, 2006.
17) R.J. McEliece, R.B. Ash, and C. Ash, “Introduction to Discrete Mathematics,” International Edition, 1989.
18) 大山達雄, “パワーアップ離散数学（パワーアップ大学数学シリーズ）,” 共立出版, 1997.
19) 渡辺 治, 北野 晃朗, 木村泰紀, 谷口雅治, “数学の言葉と論理（現代基礎数学 1）,” 朝倉書店, 2008.
20) R.P. Grimaldi, “Discrete and Combinatorial Mathematics: An Applied Introduction（4th edition）,” Addison-Wesley, 1999.
21) K.A. Ross and C.R. Wright, “Discrete Mathematics（5th edition）,” Prentice Hall, 2002.