# 集合論

花木 章秀

信州大学理学部数学科 講義ノート
2022 年度後期 (2022/10/05)

# Chapter 1

# 論理の基本

ここでは数学を学ぶ上で最も基本的である論理学の基本について学ぶ。多くのことは既に知っていることであると思うが、それらを確認しておくということは大事である。勉強をしていて、何かが分からないときには、自分が何を理解していないのかを考えてみると良い。多くの場合、理解できていないのはそのとき勉強していることではなく、もっと前に段階にある。そして、それが実はここで学ぶ論理の部分であるということも少なくはないのである。

## 1.1 命題

それが**真** (true) であるか**偽** (false) であるかがはっきりとしている事柄を**命題**という。例えば以下は命題の例である。

(1) 4 は偶数である。

(2) 偶数は 4 の倍数である。

(3) 犬は動物である。

(4) 猫は犬である。

もちろん (1), (3) は真で (2), (4) は偽である。(2) にはやや注意が必要である。偶数のうちには 4 の倍数も含まれているので (2) は真であったり、偽であったりするように思われる。しかし、(2) は

(2') すべての偶数は 4 の倍数である。

ということを主張していると理解される。したがって一つでも 4 の倍数でない偶数 (例えば 2) があれば偽であるということになる。

以下は命題ではない例である。

(1) 大学生は頭がいい。

(2) 6 は良い数である。

(3) 100 は大きな数である。

(4) 犬と猫は仲が悪い。

(5) プロ野球選手は野球がうまい。

どれも明確な基準が定められておらず、真か偽かを判定できない。

自然数 $n$ に対して

A : $n$ は偶数である。

B : $n$ は 4 の倍数である。

とすると $n$ を定めれば A, B 共に真か偽かが定まり、これらは命題である。真であるか偽であるかが $n$ に依存するので、このような場合は単に A, B とは書かずに A($n$), B($n$) などと書くこともある。

C : (任意の $n$ に対して) A($n$) ならば B($n$) である (偶数は 4 の倍数である)。

D : (任意の $n$ に対して) B($n$) ならば A($n$) である (4 の倍数は偶数である)。

とおくと、これらも命題であり C は偽、D は真である。C や D は $n$ には依存しない命題である。ここで A($n$) や B($n$) は命題であり「A($n$) ならば B($n$) である」というのも命題であることに注意する。

一般に「A ならば B である」ということを $A \Longrightarrow B$ または $B \Longleftarrow A$ と書く。命題 $B \Longrightarrow A$ を命題 $A \Longrightarrow B$ の**逆命題**、または単に**逆**という。ある命題が真であっても、その逆が真であるとは限らない。命題 $A \Longrightarrow B$ が真であるとき A を B の**十分条件**といい、B を A の**必要条件**という。命題 $A \Longrightarrow B$ と命題 $B \Longrightarrow A$ が共に真であるとき A を B の**必要十分条件**といい $A \Longleftrightarrow B$ と書く。明らかに、このとき B は A の必要十分条件でもある。$A \Longleftrightarrow B$ であるとき命題 A と B は**同値である**ともいう。同値な命題を “同じ” 命題と考えることもある。

二つの命題 A, B が同時に真であるときに真であると定めた命題を $A \wedge B$ と書き A **かつ** B と読む。二つの命題 A, B の少なくとも一方が真であるときに真であると定めた命題を $A \vee B$ と書き A **または** B と読む。$A \wedge B$ を A and B、$A \vee B$ を A or B などとも書く。

**例 1.1.1.** 自然数 $n$ に対して

A($n$) : $n$ は 2 の倍数である。

B($n$) : $n$ は 3 の倍数である。

とすれば

$A(n) \wedge B(n)$ : $n$ は 2 の倍数であり、かつ 3 の倍数である。

$A(n) \vee B(n)$ : $n$ は 2 の倍数、または 3 の倍数である。

などとなる。

C($n$) : $n$ は 6 の倍数である。

とおけば

- A($n$) は C($n$) の必要条件
- C($n$) は A($n$) の十分条件
- C($n$) は $A(n) \wedge B(n)$ の必要十分条件

などが成り立つ。

命題 A に対して、A が真のときに偽、偽のときに真と定めた命題を $\neg A$ と書き A **の否定**、A **でない**、または *not* A と読む。明らかに $\neg(\neg A)$ は A の必要十分条件である。

命題 $B \Longrightarrow A$ が真であるとき、命題 $\neg A \Longrightarrow \neg B$ は真となる。これを $B \Longrightarrow A$ の**対偶**という。$\neg A \Longrightarrow \neg B$ の対偶は $B \Longrightarrow A$ となるので、$\neg A \Longrightarrow \neg B$ であることは $B \Longrightarrow A$ となることの必要十分条件である。

ある命題が真であるときに, その対偶が常に真であるということは次のように考えると理解しやすい。$B \Longrightarrow A$ ということは、B が A よりも “強い” ということである。図で表すと Figure 1.1 のようになる。よってこのとき $\neg A$ は $\neg B$ よりも “強く”、$\neg A \Longrightarrow \neg B$ が成り立つのである。

命題 $B \Longrightarrow A$ を考える。A が真であれば、この命題は常に真である。例えば

C : B ならば $1 + 1 = 2$ である。

という命題は B が真であるか偽であるかに関わらず、常に真である。この対偶を考えると $\neg A \Longrightarrow \neg B$ は A が真、すなわち $\neg A$ が偽であれば常に真となる。よって命題 $B \Longrightarrow A$ は B が偽であれば A が真であるか偽であるかに関わらず、常に真である。

以上は感覚的な説明であるが、正確には $B \Longrightarrow A$ を $(\neg A) \vee B$ と同値な命題であると定義する。これは B が真かつ A が偽であるときのみ偽となる命題である。

論理についての基本的な事柄をまとめておく。証明は与えない。類似のことが後に学ぶ集合に対しても成り立つ。

**定理 1.1.2.** (1) $A \wedge (\neg A)$ は常に偽である。

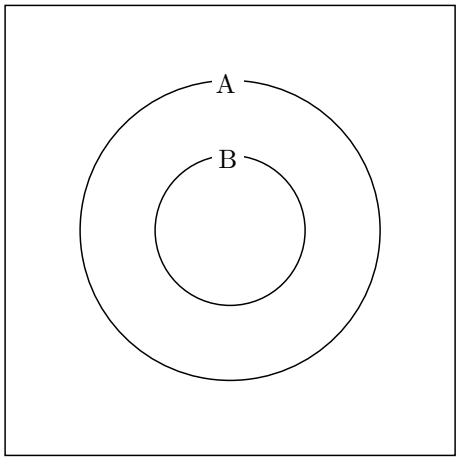


Figure 1.1: $B \Longrightarrow A$

(2) $A \vee (\neg A)$ は常に真である。[1]

(3) $A \Longrightarrow A$ は常に真である。

(4) $A \wedge B \Longrightarrow A$

(5) $A \Longrightarrow A \vee B$

(6) $A \wedge B \Longleftrightarrow B \wedge A$

(7) $A \vee B \Longleftrightarrow B \vee A$

(8) $A \wedge (B \wedge C) \Longleftrightarrow (A \wedge B) \wedge C$

(9) $A \vee (B \vee C) \Longleftrightarrow (A \vee B) \vee C$

(10) $\neg(\neg A) \Longleftrightarrow A$

(11) (ド・モルガンの公式) $\neg(A \wedge B) \Longleftrightarrow (\neg A) \vee (\neg B)$

(12) (ド・モルガンの公式) $\neg(A \vee B) \Longleftrightarrow (\neg A) \wedge (\neg B)$

(13) $A \vee (B \wedge C) \Longleftrightarrow (A \vee B) \wedge (A \vee C)$

(14) $A \wedge (B \vee C) \Longleftrightarrow (A \wedge B) \vee (A \wedge C)$

**例 1.1.3.** $(\neg A) \Longrightarrow A$ は常に偽であるように思われるが、先に述べたように A が真であればこれは真である。$(\neg A) \Longrightarrow A$ は A と同値な命題となる。

## 1.2 真理表

前の節で述べたことを理解するには**真理表**と呼ばれる表を用いるとよい。ある命題が真であることを 1, 偽であることを 0 と表すことにする。二つの命題 A, B を考えるとき、それが真であるか偽であるかの可能性は 4 通りある。A,B によって定まる基本的な命題については以下の通りである。

| A | B | $\neg A$ | $\neg B$ | $A \wedge B$ | $A \vee B$ | $A \Longrightarrow B$ | $B \Longrightarrow A$ | $A \Longleftrightarrow B$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |

このような表を**真理表**と呼ぶ。上の表にある基本的な関係は定義であり説明はできないが、前節の感覚的な説明と矛盾しないようになっている。ここに書いたもの以外の命題の多くは、これらの命題を組み合わせることによって得られる。

[1] 常に真となる命題を**恒真式**、または**トートロジー**という。逆に常に偽となる命題を**矛盾**という。$A \wedge (\neg A)$ は矛盾である。

**例 1.2.1.** 真理表を用いて、ド・モルガンの公式を示してみよう。

| A | B | $\neg(A \wedge B)$ | $(\neg A) \vee (\neg B)$ | $\neg(A \vee B)$ | $(\neg A) \wedge (\neg B)$ |
|---|---|---|---|---|---|
| 1 | 1 | **0** | **0** | 0 | 0 |
| 1 | 0 | **1** | **1** | 0 | 0 |
| 0 | 1 | **1** | **1** | 0 | 0 |
| 0 | 0 | **1** | **1** | 1 | 1 |

$\neg(A \wedge B)$ を表す列と $(\neg A) \vee (\neg B)$ を表す列が等しいことから $\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$ が分かる。$\neg(A \vee B) \iff (\neg A) \wedge (\neg B)$ も同様である。

**例 1.2.2.** 真理表を用いて、ある命題とその対偶が同値であることを示してみよう。

| A | B | $A \Longrightarrow B$ | $\neg A$ | $\neg B$ | $(\neg B) \Longrightarrow (\neg A)$ |
|---|---|---|---|---|---|
| 1 | 1 | **1** | 0 | 0 | **1** |
| 1 | 0 | **0** | 0 | 1 | **0** |
| 0 | 1 | **1** | 1 | 0 | **1** |
| 0 | 0 | **1** | 1 | 1 | **1** |

これによって命題とその対偶の同値性が分かる。

**例 1.2.3.** 命題 $A \Longrightarrow B$ と $B \Longrightarrow C$ が共に真であるとき、$A \Longrightarrow C$ も真である。(これを**三段論法**といい、証明などに頻繁に用いられる。) これを真理表を用いて示してみよう。基本となる命題が 3 つあるので、すべての場合を記述するためには 8 つの行が必要となる。

| A | B | C | $A \Longrightarrow B$ | $B \Longrightarrow C$ | $(A \Longrightarrow B) \wedge (B \Longrightarrow C)$ | $A \Longrightarrow C$ | $(A \Longrightarrow B) \wedge (B \Longrightarrow C) \Longrightarrow (A \Longrightarrow C)$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

$A \Longrightarrow B$ と $B \Longrightarrow C$ が共に 1 である行、すなわち 1, 5, 7, 8 の各行では $A \Longrightarrow C$ も 1 となっている。これは $A \Longrightarrow B$ と $B \Longrightarrow C$ が共に真であるとき、$A \Longrightarrow C$ も真であることを意味している。

**問 1.2.4.** $\neg(A \Longrightarrow B)$ と $A \wedge (\neg B)$ が同値な命題であることを真理表を用いて示せ。

## 1.3 「任意の ···」と「ある ···」

数学では「**任意の** ··· **に対して** ··· **である**」とか「**ある** ··· **が存在して** ··· **である**」などという言い方がよく使われる。これらの意味をきちんと理解していないと証明などが理解できない。まずは例を見てみよう。

A : 任意の実数 $x$ に対して $x^2 \geq 0$ である。

A の否定は何であろうか。A が偽であるということは、一つでも $x^2 \geq 0$ が成り立たない実数 $x$ が存在すればよい。したがって

$\neg$A : ある実数 $x$ が存在して $x^2 < 0$ である。

となる。より自然な言い方をすれば「$x^2 < 0$ となる実数 $x$ が存在する」ということになる。次に実数列 $S = \{a_1, a_2, \cdots\}$ に対して次の命題を考える。

B($S$) : ある自然数 $n$ が存在して $a_n < 0$ である。

この否定は何であろうか。一つでも $a_n < 0$ となる自然数 $n$ が存在すれば B($S$) は真になるので、B($S$) が偽になるためには、すべての自然数 $n$ に対して $a_n \geq 0$ でなければならない。よって

$\neg$B($S$) : 任意の自然数 $n$ に対して $a_n \geq 0$ である。

となる。

以上のように「任意の ··· に対して ··· である」と「ある ··· が存在して ··· である」ということは、否定によって互いに移り会うものなのである。しっかりと覚えておこう。

数学の教科書などでは、先の例のように命題をきちんと文章で表している場合がほとんどであるが、講義などでは適当に省略した記号を用いる場合が多い。この記号が理解できないことも講義が分からなくなる一つの要因である。ここできちんと理解しておこう。

まず、数学でよく用いられる記号を確認する。

$\mathbb{N}$ := 自然数全体の集合 (0 を含める場合もあるが、ここでは含めない)

$\mathbb{Z}$ := 整数全体の集合 (有理整数環。普通の整数は有理整数ともいう。)

$\mathbb{Q}$ := 有理数全体の集合 (有理数体)

$\mathbb{R}$ := 実数全体の集合 (実数体)

$\mathbb{C}$ := 複素数全体の集合 (複素数体)

非負整数全体を $\mathbb{Z}_{\geq 0}$, 負の整数全体を $\mathbb{Z}_{<0}$ などと書くこともある。:= の記号は左辺を右辺で定めるという意味であるが、人によって違う記号を用いる場合もある。また**集合**という言葉は後で説明するが、ここでは単に「自然数全体の集まり」のように理解すればよい。$n$ が自然数であるということを $n \in \mathbb{N}$ と表す。他の記号についても同様である。

さて「任意の自然数 $n$ に対して $\cdots$」ということを記号で「$\forall n \in \mathbb{N}$ に対して $\cdots$」などと書く。「ある自然数 $n$ に対して $\cdots$」ということは記号で「$\exists n \in \mathbb{N}$ に対して $\cdots$」などと書く。$\forall$ は All の A をひっくり返したもの、$\exists$ は Exists の E をひっくり返したものと覚えればよい。次の命題はすべて同じことを言っている。

A : 任意の実数 $x$ に対して $x^2 \geq 0$ である。

A : $\forall x \in \mathbb{R}$ に対して $x^2 \geq 0$ である。

A : $\forall x \in \mathbb{R}$, $x^2 \geq 0$.

A : $x^2 \geq 0$, $\forall x \in \mathbb{R}$.

A : $x^2 \geq 0$ for all $x \in \mathbb{R}$.

A : $x^2 \geq 0$ for every $x \in \mathbb{R}$.

A : $\forall x \in \mathbb{R}$ $(x^2 \geq 0)$.

A : $\forall x$ $(x \in \mathbb{R} \Longrightarrow x^2 \geq 0)$.

all, every は英語としては、その与えるニュアンスが異なるが、論理的には同じと思ってよい。同様に次も同じことである。

$\neg$A : ある実数 $x$ に対して $x^2 < 0$ である。

$\neg$A : $\exists x \in \mathbb{R}$ に対して $x^2 < 0$ である。

$\neg$A : $\exists x \in \mathbb{R}$, $x^2 < 0$.

$\neg$A : $x^2 < 0$, $\exists x \in \mathbb{R}$.

$\neg$A : $x^2 < 0$ であるような $x \in \mathbb{R}$ が存在する。

$\neg$A : $\exists x \in \mathbb{R}$ such that $x^2 < 0$.

$\neg$A : $\exists x \in \mathbb{R}$ s.t. $x^2 < 0$.

$\neg$A : $x^2 < 0$ for some $x \in \mathbb{R}$.

$\neg$A : $\exists x \in \mathbb{R}$ $(x^2 < 0)$.

$\neg$A : $\exists x$ $((x \in \mathbb{R}) \wedge (x^2 < 0))$.

「$\exists x$ such that B」というのは「B であるような $x$ が存在する」ということを英語で言っているだけである。「such that」を省略して「s.t.」と書くことも多い。次の二つの命題を考えよう。

C : $\forall r \in \mathbb{R}, \exists n \in \mathbb{N}, r < n.$

D : $\exists n \in \mathbb{N}, \forall r \in \mathbb{R}, r < n.$

この二つの命題は記述してある順番が違うだけである。同じ意味だろうか。実はこれは全く違う意味なのである。それは文章にして読んでみれば分かる。

C : 任意の $r \in \mathbb{R}$ に対して、ある $n \in \mathbb{N}$ が存在して $r < n$ である。

D : ある $n \in \mathbb{N}$ が存在して、任意の $r \in \mathbb{R}$ に対して $r < n$ である。

C は与えられた $r \in \mathbb{R}$ に対して $n \in \mathbb{N}$ を決めればよいので真である。一方 D は $r \in \mathbb{R}$ に関係なく $n \in \mathbb{N}$ が存在しなければならず偽である。このように省略した記号は便利ではあるが、間違えをおかしやすいものである。試験の答案などにはきちんとした文章を書くことを勧める。

**注意.** 上の命題 C をより自然な言葉で「任意の $r \in \mathbb{R}$ に対して $r < n$ となるような $n \in \mathbb{N}$ が存在する」と読むこともできる。しかしこの場合、

(1) 任意の $r \in \mathbb{R}$ に対して、($r < n$ となるような $n \in \mathbb{N}$ が存在する)

(2) (任意の $r \in \mathbb{R}$ に対して $r < n$)、となるような $n \in \mathbb{N}$ が存在する

と句点を入れてみると (1) は C を、(2) は D を表している。このように命題を記述する場合には、その意味が明らかとなるように細心の注意が必要となる。通常は、句点がない場合にもその文脈からどちらの意味であるかが読み取れることが多いが、少なくとも試験ではきちんと区別しなくてはならない。

上の C, D の否定を求めておく。文章から否定を考えるのはやや難しいが、記号を用いた場合には簡単であることが分かるだろう。

$\neg$C : $\exists r \in \mathbb{R}, \forall n \in \mathbb{N}, r \geq n.$

$\neg$C : ある $r \in \mathbb{R}$ があって、任意の $n \in \mathbb{N}$ に対して $r \geq n$ である。

$\neg$D : $\forall n \in \mathbb{N}, \exists r \in \mathbb{R}, r \geq n.$

$\neg$D : 任意の $n \in \mathbb{N}$ に対して、ある $r \in \mathbb{R}$ があって $r \geq n$ である。

もちろん $\neg$C は偽で $\neg$D は真である。

これをもう少し詳しく説明しよう。命題 C は丁寧に書くと以下のようになる。

C : $\forall r \in \mathbb{R}\ (\exists n \in \mathbb{N}\ (r < n))$.

ここで $(r < n)$ は $r$ と $n$ に関する命題である。$(\exists n \in \mathbb{N}\ (r < n))$ は $r$ のみに関する命題である。なぜならば $n$ はこの中で定義されているので、これは特定の $n$ に関することをいっている訳ではないからである。同様に考えて命題 C はどの変数にも依存しない命題である。$\neg$C は以下のように解釈される。

$\neg$C : $\exists r \in \mathbb{R}\ \neg(\exists n \in \mathbb{N}\ (r < n))$.

$\neg$C : $\exists r \in \mathbb{R}\ (\forall n \in \mathbb{N}\ \neg(r < n))$.

$\neg$C : $\exists r \in \mathbb{R}\ (\forall n \in \mathbb{N}\ (r \geq n))$.

**例 1.3.1** ($\varepsilon$-$\delta$ 論法)**.** 関数 $y = f(x)$ が $x = a$ で**連続**であるとは、以下の条件を満たすこととして定義される。

> [**定義**] 任意の正の数 $\varepsilon$ に対して、ある正の数 $\delta$ があって $|x - a| < \delta$ ならば $|f(x) - f(a)| < \varepsilon$ が成り立つ。

例えば $y = f(x) = 2x$ という関数は任意の $x = a$ において連続であるが、それは以下のように証明される。

> **証明**. $\varepsilon$ を任意の正の数とする。$\delta = \varepsilon/2$ とする。このとき $|x - a| < \delta$ ならば
>
> $$|f(x) - f(a)| = |2x - 2a| = 2|x - a| < 2\delta = \varepsilon$$
>
> である。(証明終り)

ここで重要なのは「ある正の数 $\delta$ があって」といっているので本当に $\delta$ を決めてやる必要があるということである。$\delta = \varepsilon/2$ というのは本質的ではなく、例えば $\delta = \varepsilon/3$ でも構わない。存在することをいいたいのだから、少なくとも一つの例を見つければいいのである。

さて、次に連続でないことを証明してみよう。$y = f(x)$ は $x < 0$ のとき 0 で $x \geq 0$ のとき 1 で定めるとする。このとき、この関数は $x = 0$ で連続でないことは分かるだろう。これを上の定義にしたがって証明する。連続でないことを示したいので定義を否定すればよい。このままで考えるとやや難しいので、連続の定義を記号を用いて書き直してみる。

**[定義]** $\forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}\ (|x - a| < \delta \Longrightarrow |f(x) - f(a)| < \varepsilon)$.

これを否定するので、連続でないということは

$$\exists \varepsilon > 0, \forall \delta > 0\ \exists x \in \mathbb{R}\ \neg(|x - a| < \delta \Longrightarrow |f(x) - f(a)| < \varepsilon).$$

$\neg(|x - a| < \delta \Longrightarrow |f(x) - f(a)| < \varepsilon)$ は「$|x - a| < \delta$ and $|f(x) - f(a)| \geq \varepsilon$」ということである (問 1.2.4)。したがって、いいたいことは

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R}\ ((|x - a| < \delta) \wedge (|f(x) - f(a)| \geq \varepsilon)).$$

ということになる。さて証明をしてみよう。$\exists \varepsilon > 0$ となっているので $\varepsilon$ をきちんと決めてやらなくてはならないことに注意する。$x \in \mathbb{R}$ も同様に決めてやる必要がある。

**証明**. $\varepsilon = 1/2$ とする。任意の $\delta > 0$ に対して $x = -\delta/2$ とすれば $|x - 0| = \delta/2 < \delta$ であって $|f(x) - f(0)| = |0 - 1| = 1 \geq 1/2 = \varepsilon$ である。(証明終り)

この証明で $x$ は $\delta$ によって決まっていることに注意しよう。このような場合「$x$ の取り方は $\delta$ に依存する」などという言い方をする。またこの場合も $\varepsilon$ や $x$ はこのように決めなくてはならないわけではなく、例えば $\varepsilon = 1/4, x = -\delta/5$ などでも構わない。$\varepsilon$ をどのように決めるかは問題によって異なり、自分で考えるしかない。

**注意.** 数学の講義では「命題 1. $\cdots$」などと書かれることが多い。ここで言う命題とは「真である命題」を示している。その意味は「定理」、「補題」などと同じであると思ってよい。確認のため、よく使われる言葉などをまとめておこう。

**命題**：(真の) 命題

**定理**：重要な (真の) 命題

**補題**：それ自身はあまり重要ではないが、定理の証明などに用いられる (真の) 命題

**系**：定理や命題から容易に導かれる (真の) 命題

**定義**：言葉や記号を定めること

**公理**：明らかに成り立つものとして仮定されること (基本的すぎて証明できないと認めるもの)

**予想**：真であることが期待されるが、証明はされていない (真か偽か分からない) 命題 (実は真偽が定まらず、命題でないこともある)

定理などの証明は「証明」や「proof」で始めて書くことが多く、証明の終わりは「Q.E.D.」[2]や「□」などで表される。

[2] ラテン語の “Quod Erat Demonstrandum”（かく示された/これが示されるべき事であった) の略

# Chapter 2

# 集合

集合とは、簡単に言えばものの集まりである。しかし数学的に厳密に考えると色々と問題があることが分かる。集合を厳密に考えて、議論する「集合論」[1] はここではやや難しすぎるので、厳密ではないが実用には十分な理論を解説するにとどめる。ただ、何が問題なのかを分かってもらうために「ラッセルのパラドックス」については解説をする。

## 2.1 集合

**集合** (set) とはものの集まりのことである。しかしものの集まりをすべて集合と呼ぶわけではない。例えば「大きい数の集まり」、「お金持ちの集まり」などはその基準が明確でなく、集合とは言えない。あるものが集合に属するかどうかははっきりとしていなくてはいけないので、その基準は命題である。よって集合は「$x$ に関する命題 $P(x)$ が真となるような $x$ の集まり」という形で記述される。このとき、その集合を

$$\{x \mid P(x)\}$$

のように表す。例えば「100 以上の整数の集まり」であれば

$$\{x \mid x \in \mathbb{Z} \text{ かつ } x \geq 100\}$$

のように表す。「かつ」というのを省略、あるいは英語で表して

$$\{x \mid x \in \mathbb{Z},\ x \geq 100\}, \quad \{x \mid x \in \mathbb{Z} \text{ and } x \geq 100\}$$

のようにも表す。

集合 $S$ に属するもの $x$ を、その集合の**要素** (element)、または**元**という。このとき

$$x \in S, \quad S \ni x$$

などと表す。この記号は既に $\mathbb{Z}, \mathbb{N}$ などに用いていたものである。$x$ が $S$ の要素でないことを

$$x \notin S, \quad S \not\ni x$$

と表す。$S = \{x \mid P(x)\}$ であるとき

$$x \in S \Longleftrightarrow P(x), \quad x \notin S \Longleftrightarrow \neg P(x)$$

である。

集合の要素を列挙することによって集合を定義することもできる。この場合、要素が $x_1, x_2, x_3$ であれば

$$\{x_1,\ x_2,\ x_3\}$$

と表す。例えば「10 以下の素数全体の集合」は

$$\{n \mid n \text{ は素数},\ n \leq 10\} = \{2, 3, 5, 7\}$$

[1]「公理論的集合論」、「ZFC 集合論 (Zermelo-Fraenkel set-theory with the axiom of Choice)」などと呼ばれる。

である。要素の個数が多い場合には適当な省略をする場合もある。例えば「1 から 100 までの整数全体の集合」は

$$\{1, 2, 3, \ldots, 100\}$$

などと表される。また無限個の要素をもつ場合にも同様の省略は用いられ

$$\{1, 2, 3, \ldots\}$$

と書けばすべての自然数の集合という意味である。しかし省略は注意して用いないといけない。例えば $\{1, 2, 3, 5, 9, 10, 100\}$ などという集合を $\{1, 2, \ldots, 100\}$ などと書いても誰も理解してくれないであろう。意味が分かりにくい場合や間違える恐れのある場合には省略はしない方がよい。

集合をこのように要素を並べて表す場合、要素を並べる順番には意味がない。また同じ要素を複数書いても、それは無視される。これは、集合を考えるときには「あるものがその集合に属するか、属さないか」のみが問題とされるからである。例えば次の集合はすべて同じものとして扱われる。

$$\{1, 2, 3\}, \quad \{2, 3, 1\}, \quad \{1, 2, 2, 3, 3, 3, 1, 2\}$$

集合を表すときにこの例のように同じ要素を複数書いても間違いではないが、意味が分かりにくくなるので、なるべく同じ要素は複数書かないようにした方がよい。

二つの集合 $A$, $B$ に対して「$x \in B \Longrightarrow x \in A$」が成り立つとき $B$ を $A$ の**部分集合** (subset) といい $B \subset A$ または $A \supset B$ と書く。$B \subset A$ であり、かつある $x \in A$ があって $x \notin B$ であるとき $B$ を $A$ の**真部分集合** (proper subset) といい $B \subsetneq A$ または $A \supsetneq B$ と書く。

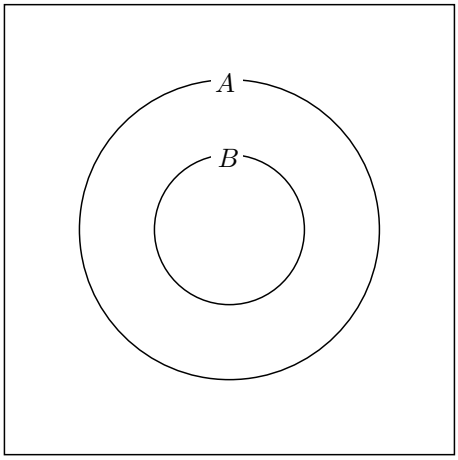


Figure 2.1: $B \subset A$

**注意.** 部分集合であることを $B \subseteq A$, $A \supseteq B$ で表し、真部分集合であることを $B \subset A$, $A \supset B$ と表す場合もある。講義などで分かりにくい場合は質問をして確認するといいだろう。

**定理 2.1.1.** $A \subset B$, $B \subset C$ であるならば $A \subset C$ である。

**証明**. $x \in A$ とする。$A \subset B$ より $x \in B$ である。また $B \subset C$ より $x \in C$ である。よって $A \subset C$ である。 □

$B \subset A$ かつ $A \subset B$ である場合、「$x \in A \Longleftrightarrow x \in B$」である。このとき二つの集合 $A$ と $B$ は**等しい**といい、$A = B$ と書く。$A = B$ のとき、二つの集合 $A$, $B$ は全く同じ要素からなる。

前に「100 以上の整数の集合」を $\{x \mid x \in \mathbb{Z} \text{ かつ } x \geq 100\}$ と表したが、はじめから $\mathbb{Z}$ の部分集合を考えているということを意識する場合は

$$\{x \in \mathbb{Z} \mid x \geq 100\}$$

のような記述もする。

$$\{x \in S \mid P(x)\}$$

という記述は、その集合が $S$ の部分集合として考えられているということと理解すればよい。

集合に含まれる要素の数が有限である場合、その集合を**有限集合** (finite set) といい、要素の数が無限であるとき、その集合を**無限集合** (infinite set) という。有限集合 $A$ の要素の数を $|A|$ や $\sharp A$ などと書く。無限集合の場合は $|A| = \infty$ と書く[2]。$|A| < \infty$ と書かれた場合は $A$ が有限集合であることを意味する。有限集合の部分集合は明らかに有限集合である。有限、無限の定義はやや難しくなるのでここではしない。感覚的に理解しておけば十分である。

**学習のポイント.** 「二つの集合 $A, B$ について $B \subset A$ であることを示せ」という問題を考えよう。試験などでこのような問題ができない場合、何を示せばよいのかが分かっていない場合が多く見られる。「$B \subset A$」の定義は「$x \in B$ ならば $x \in A$」であるから、証明は以下のようになる。

- $x \in B$ とする。このとき $\cdots$。よって $x \in A$ である。したがって $B \subset A$ である。

分かってしまえば簡単なことであるが、きちんと理解しておこう。また「二つの集合 $A, B$ について $A = B$ であることを示せ」という問題は、「$A = B$」の定義が「$A \subset B$ かつ $A \supset B$」であるから、

- $x \in B$ とする。このとき $\cdots$。よって $x \in A$ である。したがって $B \subset A$ である。次に $x \in A$ とする。このとき $\cdots$。よって $x \in B$ である。したがって $A \subset B$ である。以上より $A = B$ である。

となる。この証明は $B \subset A$ を示す部分と $A \subset B$ を示す部分からなり、その両方で同じ文字 $x$ を用いたが、それはまったく違うものである。区別がしにくいと感じるならば、後半では $x$ ではなく $y$ を用いるなどして、紛らわしさがないようにした方がよい。しかし、このような用い方はよくされることなので、ここではあえて同じ記号を用いた。証明などの中で、新しい文字 (記号) を用いるときには、

- それが既に用いられていないか。
- 用いられている場合には、それと混同する恐れはないか。
- それがどの様なものなのかがはっきりとしているか。

などを気にしなければならない。

## 2.2 空集合

**定義 2.2.1** (空集合)**.** 要素を一つも含まないものも集合として扱う。これを**空集合** (empty set) といい $\emptyset$ で表す。記号 $\phi$ も空集合を表すのによく用いられる。任意の $x$ に対して $x \notin \emptyset$ である。

**補題 2.2.2.** 任意の集合 $A$ に対して $\emptyset \subset A$ である。

**証明.** 「$x \in \emptyset \Longrightarrow x \in A$」を示せばよいが $x \in \emptyset$ は常に偽であるから、これは常に真である。 □

**補題 2.2.3.** 空集合 $\emptyset$ は唯一つに定まる。

**証明.** $\emptyset, \emptyset'$ を共に空集合とすると補題 2.2.2 より $\emptyset \subset \emptyset', \emptyset' \subset \emptyset$ であるから $\emptyset = \emptyset'$ である。 □

## 2.3 共通部分

**定義 2.3.1** (共通部分)**.** 二つの集合 $A, B$ に対して $A \cap B = \{x \mid x \in A,\ x \in B\}$ とおいて、これを $A$ と $B$ の**共通部分** (intersection) という。$A \cap B = \emptyset$ であるとき $A$ と $B$ は**共通部分がない**、または**互いに素**であるという。

**例 2.3.2.** $A = \{1, 2, 3\},\ B = \{2, 3, 4, 5\}$ とすると $A \cap B = \{2, 3\}$ である。

集合の共通部分について次が成り立つ。

**定理 2.3.3.** (1) $A \cap B \subset A,\ A \cap B \subset B$

(2) $C \subset A,\ C \subset B \Longleftrightarrow C \subset A \cap B$

(3) $B \subset A \Longleftrightarrow A \cap B = B$

[2]無限集合については後で詳しく扱う。

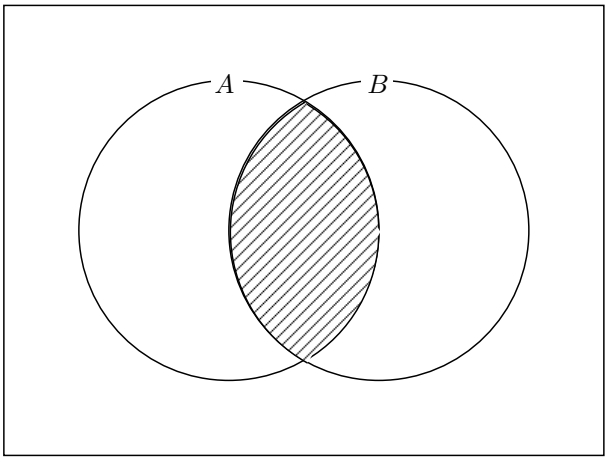


Figure 2.2: $A \cap B$

**証明**. (1), (2) は定義より明らか。

(3) $\Longrightarrow$ を示す。$x \in B$ ならば $B \subset A$ より $x \in A$ なので $x \in A \cap B$ である。よって $B \subset A \cap B$ である。また (1) より $A \cap B \subset B$ である。以上より $A \cap B = B$ である。

$\Longleftarrow$ を示す。$A \cap B = B$ とすると (1) より $A \cap B \subset A$ なので $B \subset A$ である。 □

**定理 2.3.4.** (1) $A \cap B = B \cap A$

(2) $A \cap (B \cap C) = (A \cap B) \cap C$

**証明**. (1) $x \in A \cap B$ とする。定理 2.3.3 (1) より $A \cap B \subset B$ なので $x \in B$ である。同様に $x \in A$ であり、よって $x \in B \cap A$ である。したがって $A \cap B \subset B \cap A$ である。逆も同様に示される。

(2) $x \in A \cap (B \cap C)$ とする。$x \in A$ である。$x \in B \cap C$ であるから $x \in C$ かつ $x \in B$ である。以上より $x \in A \cap B$ かつ $x \in C$ が成り立ち $x \in (A \cap B) \cap C$ である。よって $A \cap (B \cap C) \subset (A \cap B) \cap C$ である。逆も同様に示される。 □

この定理の (1) を $\cap$ の**交換法則** (commutative law) といい (2) を $\cap$ の**結合法則** (associative law) という。この二つの性質により三つ以上の集合の共通部分を考えるとき、カッコをつけなくてもその意味は不明にはならない。以後

$$A \cap B \cap C, \quad A \cap B \cap C \cap D, \quad \cdots$$

などという記号を用いる。また集合の列 $A_1, A_2, \cdots, A_n$ に対して

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

という記号も用いる。無限個の集合の共通部分も考えられる。例えば 集合の列 $A_1$, $A_2$, $\cdots$, $A_i$, $\cdots$ に対して

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots$$

のような記号も用いる。集合の添字が $1, 2, 3, \cdots$ のようになっていなくてもよい。例えば集合 $I$ を添字にもつ集合の族 $\{A_i \mid i \in I\}$ に対しても、その共通部分を

$$\bigcap_{i \in I} A_i$$

のように表す。

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \quad \text{for all } i \in I\}$$

である。したがって $x \in \bigcap_{i \in I} A_i$ を示したければ、任意の $i \in I$ に対して $x \in A_i$ を示せばよい。

**例 2.3.5.** $r \in \mathbb{R}_{>0}$ に対して、閉区間 $I_r = [-r, r]$ を考える。このとき $\bigcap_{r\in\mathbb{R}_{>0}} I_r = \{0\}$ である。

二つの集合が等しいことを示すので、これを示すには $\bigcap_{r\in\mathbb{R}_{>0}} I_r \supset \{0\}$ と $\bigcap_{r\in\mathbb{R}_{>0}} I_r \subset \{0\}$ を示すことになる。

まず 任意の $r \in \mathbb{R}_{>0}$ に対して $0 \in I_r$ は明らかなので $\bigcap_{r\in\mathbb{R}_{>0}} I_r \supset \{0\}$ である。

$\bigcap_{r\in\mathbb{R}_{>0}} I_r \subset \{0\}$ を示すには「$s \in \bigcap_{r\in\mathbb{R}_{>0}} I_r$ ならば $s \in \{0\}$ (すなわち $s = 0$)」を示せばよい。このためにこれの対偶「$s \neq 0$ ならば $s \notin \bigcap_{r\in\mathbb{R}_{>0}} I_r$」を示す。$s \notin \bigcap_{r\in\mathbb{R}_{>0}} I_r$ であることと、ある $r > 0$ があって $s \notin I_r$ であることは同値である。したがって「$s \neq 0$ ならば、ある $r > 0$ があって $s \notin I_r$」を示せばよい。以上より、以下のようにして証明は終わる。

$s \neq 0$ とする。このとき $s \notin I_{|s|/2}$ である。

**注意.** $\bigcap_{i=1}^{\infty} A_i$ の定義は $\bigcap_{i\in\mathbb{N}} A_i$ であって、極限 $\lim_{n\to\infty} \bigcap_{i=1}^{n} A_i$ ではない。この極限は定義されていない。

## 2.4 和集合

**定義 2.4.1** (和集合)**.** 二つの集合 $A$, $B$ に対して $A \cup B = \{x \mid x \in A \text{ または } x \in B\}$ とおいて、これを $A$ と $B$ の**和集合** (union) という。

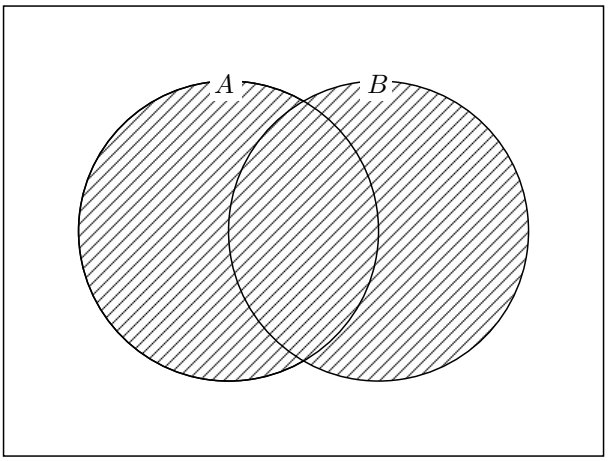


Figure 2.3: $A \cup B$

**例 2.4.2.** $A = \{1, 2, 3\}$, $B = \{2, 3, 4, 5\}$ とすると $A \cup B = \{1, 2, 3, 4, 5\}$ である。

和集合について次が成り立つ。

**定理 2.4.3.** (1) $A \subset A \cup B$, $B \subset A \cup B$

(2) $A \subset C$ かつ $B \subset C \iff A \cup B \subset C$

(3) $B \subset A \iff A \cup B = A$

**定理 2.4.4.** (1) $A \cup B = B \cup A$

(2) $(A \cup B) \cup C = A \cup (B \cup C)$

**証明.** (1) は明らか。(2) を示す。$x \in (A \cup B) \cup C$ とする。$x \in A \cup B$ または $x \in C$ である。まず $x \in C$ とすると $x \in B \cup C$ なので $x \in A \cup (B \cup C)$ である。また $x \in A \cup B$ とすると $x \in A$ または $x \in B$ である。$x \in A$ ならば $x \in A \cup (B \cup C)$ である。$x \in B$ ならば $x \in B \cup C$ なので $x \in A \cup (B \cup C)$ である。以上より、どの場合にも $x \in A \cup (B \cup C)$ となり $(A \cup B) \cup C \subset A \cup (B \cup C)$ である。逆も同様にして示すことができる。 □

この定理の (1) を $\cup$ の**交換法則**といい (2) を $\cup$ の**結合法則**という。この二つの性質により三つ以上の集合の和集合を考えるとき、カッコをつけなくてもその意味は不明にはならない。以後

$$A \cup B \cup C, \quad A \cup B \cup C \cup D, \quad \cdots$$

などという記号を用いる。共通部分の場合と同じように

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$$

$$\bigcup_{i \in I} A_i$$

などの記号も用いる。

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \quad \text{for some } i \in I\}$$

である。

**例 2.4.5.** $r \in \mathbb{R}_{>0}$ に対して、閉区間 $I_r = [-r, r]$ を考える。このとき $\bigcup_{r \in \mathbb{R}_{>0}} I_r = \mathbb{R}$ である。

これを示す。$\bigcup_{r \in \mathbb{R}_{>0}} I_r \subset \mathbb{R}$ は明らかである。任意の $s \in \mathbb{R}$ に対して、$r = |s|$ とすれば $I_r \ni s$ なので $s \in \bigcup_{r \in \mathbb{R}_{>0}} I_r$ である。よって $\bigcup_{r \in \mathbb{R}_{>0}} I_r \supset \mathbb{R}$ である。

和集合 $A \cup B$ において、$A \cap B = \emptyset$ であるとき、これを**共通部分をもたない和**、または**共通部分のない和** (disjoint union) という。三つ以上の和集合 $\bigcup_{i \in I} A_i$ については、任意の $i \neq j$ に対して $A_i \cap A_J = \emptyset$ であるときに共通部分をもたない和という。和が、有限集合であり、かつ共通部分をもたないとき、その要素の数について $\left|\bigcup_{i \in I} A_i\right| = \sum_{i \in I} |A_i|$ が成り立つ。(一般には $\left|\bigcup_{i \in I} A_i\right| \leq \sum_{i \in I} |A_i|$ である。)

## 2.5 差集合と補集合

**定義 2.5.1** (差集合)**.** 二つの集合 $A$, $B$ に対して $A - B = \{x \mid x \in A,\ x \notin B\}$ とおいて、これを $A$ と $B$ の**差集合** (set difference) という。($B \subset A$ でなくてもよい。また差集合を $A \setminus B$ と書くことも多い。)

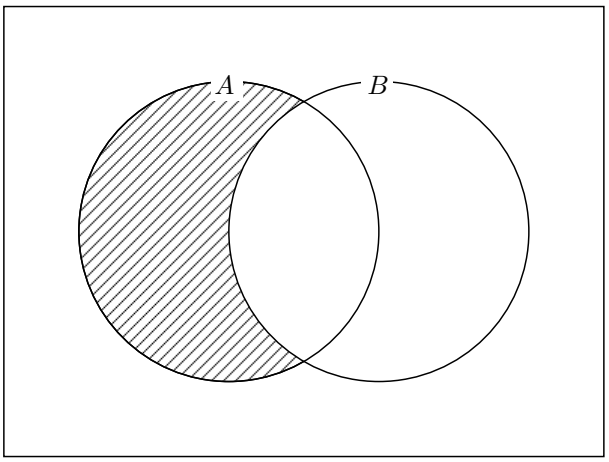


Figure 2.4: $A - B$

明らかに次が成り立つ。

(1) $A - B \subset A$

(2) $x \in A$ ならば $x \in A - B$ または $x \in B$

(3) $x \in B$ ならば $x \notin A - B$

(4) $x \in A - B$ ならば $x \notin B$

(5) $A - \emptyset = A$, $A - A = \emptyset$

**例 2.5.2.** $A=\{1,2,3\},\ B=\{2,3,4,5\}$ とすると $A-B=\{1\},\ B-A=\{4,5\}$ である。

**命題 2.5.3.** $B\subset A$ であることと $A-(A-B)=B$ であることは同値である。

**証明.** $C=A-B$ とおく。

$B\subset A$ とする。$x\in B$ であるならば $x\in A$ であるから $x\in A-C$ または $x\in C$ である。しかし $x\in C=A-B$ とすると $x\notin B$ となり矛盾である。よって $x\in A-C=A-(A-B)$ となり $B\subset A-(A-B)$ である。逆に $x\in A-(A-B)$ とする。$x\in A$ かつ $x\notin A-B$ である。よって $x\in B$ である。したがって $A-(A-B)\subset B$ が成り立ち、以上より $A-(A-B)=B$ である。

$A-(A-B)=B$ とする。このとき $B\subset A$ は明らかである。 □

この定理は以下のように論理式を同値なものに置き換えることによっても証明できる。

命題 2.5.3 の別証明. 以下の論理式の同値が成り立つ。

$$\begin{aligned}
x\in A-(A-B) &\iff (x\in A)\wedge(x\notin(A-B))\\
&\iff (x\in A)\wedge\neg(x\in(A-B))\\
&\iff (x\in A)\wedge\neg((x\in A)\wedge\neg(x\in B))\\
&\iff (x\in A)\wedge(\neg(x\in A)\vee(x\in B))\\
&\iff ((x\in A)\wedge\neg(x\in A))\vee((x\in A)\wedge(x\in B))\\
&\iff (x\in A)\wedge(x\in B)\\
&\iff x\in A\cap B
\end{aligned}$$

したがって $A-(A-B)=A\cap B$ である。定理 2.3.3 (3) より、主張は正しい。 □

**定義 2.5.4** (補集合)**.** $A\subset M$ であるとき、差集合 $M-A$ を $A$ の $M$ における**補集合** (complementary set, complement) という。$M$ が明らかな場合、すなわち $A$ を集合 $M$ の部分集合と見ていることが明らかな場合には $M-A$ を $A^c$ と表し、単に $A$ の**補集合**という。

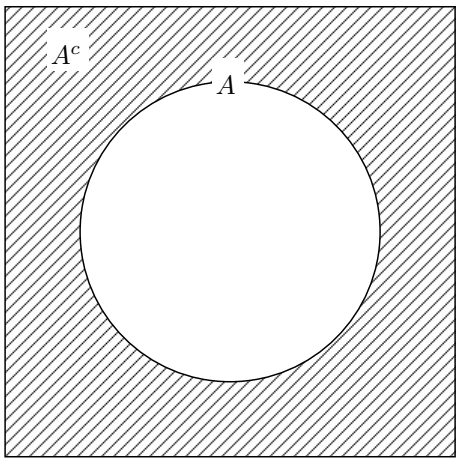


Figure 2.5: $A^c$

$A$ を $M$ の部分集合とするとき、明らかに次が成り立つ。

(1) $x\in M$ ならば $x\in A$ または $x\in A^c$

(2) $x\in A$ ならば $x\notin A^c$

(3) $x\in A^c$ ならば $x\notin A$

(4) $\emptyset^c=M,\ M^c=\emptyset$

(5) $(A^c)^c=A$

$A$ と $B$ が共に $M$ の部分集合で、$M$ における補集号の記号を用いるならば、差集合は $A-B=A\cap B^c$ と表される。

**例 2.5.5.** $A$ を (正の) 奇数全体の集合とし $B$ を (正の) 偶数全体の集合とする。$A$ の $\mathbb{N}$ における補集合は $B$ であり $B$ の $\mathbb{N}$ における補集合は $A$ である。

**例 2.5.6.** $a,b$ を $a\leq b$ である二つの実数とする。$A$ を閉区間 $[a,b]$ とする。$A$ の ($\mathbb{R}$ における) 補集合は $A^c=(-\infty,a)\cup(b,\infty)$ である。

## 2.6 集合の演算

**定理 2.6.1.** $M$ を集合とし $A$, $B$, $C$ はその部分集合とする。補集合は $M$ で考える。このとき次が成り立つ。

(1) $A\cap A^c=\emptyset$

(2) $A\cup A^c=M$

(3) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

(4) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

(5) (ド・モルガンの公式) $(A\cap B)^c=A^c\cup B^c$

(6) (ド・モルガンの公式) $(A\cup B)^c=A^c\cap B^c$

**定理 2.6.2.** $M$ を集合とし、$M$ の部分集合 $A$ と部分集合の族 $\{B_i\}_{i\in I}$ を考える。補集合は $M$ で考える。このとき次が成り立つ。

(1) $A\cap\left(\bigcup_{i\in I}B_i\right)=\bigcup_{i\in I}(A\cap B_i)$

(2) $A\cup\left(\bigcap_{i\in I}B_i\right)=\bigcap_{i\in I}(A\cup B_i)$

(3) $\left(\bigcup_{i\in I}B_i\right)^c=\bigcap_{i\in I}{B_i}^c$

(4) $\left(\bigcap_{i\in I}B_i\right)^c=\bigcup_{i\in I}{B_i}^c$

**証明.** (1) $a\in A\cap\left(\bigcup_{i\in I}B_i\right)$ とする。$a\in\bigcup_{i\in I}B_i$ なので、ある $i\in I$ があって $a\in B_i$ である。よって $a\in A\cap B_i$ となり $a\in\bigcup_{i\in I}(A\cap B_i)$ である。

逆に $a\in\bigcup_{i\in I}(A\cap B_i)$ とする。ある $i\in I$ があって $a\in A\cap B_i$ である。よって $a\in A$ かつ $a\in\bigcup_{i\in I}B_i$ となり $a\in A\cap\left(\bigcup_{i\in I}B_i\right)$ である。

(2) $a\in A\cup\left(\bigcap_{i\in I}B_i\right)$ とする。$a\in A$ ならば、任意の $i\in I$ について $a\in A\cup B_i$ だから $a\in\bigcap_{i\in I}(A\cup B_i)$ である。また $a\in\bigcap_{i\in I}B_i$ とすると、任意の $i\in I$ について $a\in B_i$ だから $a\in A\cup B_i$ となる。よって、このときも $a\in\bigcap_{i\in I}(A\cup B_i)$ である。

$a\in\bigcap_{i\in I}(A\cup B_i)$ とする。$a\in A$ ならば $a\in A\cup\left(\bigcap_{i\in I}B_i\right)$ である。$a\notin A$ とする。このとき、任意の $i\in I$ に対して $a\in A\cup B_i$ より $a\in B_i$ である。よって $a\in\bigcap_{i\in I}B_i$ となり $a\in A\cup\left(\bigcap_{i\in I}B_i\right)$ である。

(3) $a\in\left(\bigcup_{i\in I}B_i\right)^c$ とする。このとき任意の $i\in I$ に対して $a\notin B_i$ であるから $a\in\bigcap_{i\in I}{B_i}^c$ である。

$a\in\bigcap_{i\in I}{B_i}^c$ とする。任意の $i\in I$ に対して $a\notin B_i$ なので $a\in\left(\bigcup_{i\in I}B_i\right)^c$ である。

(4) は (3) とほぼ同じに示される。 □

この定理の (3) の証明はやや雑に書いてあるが、きちんと理解するには次のような論理式の変形を考えればよい。

$$\begin{aligned}
x\in\left(\bigcup_{i\in I}B_i\right)^c &\iff \neg\left(x\in\bigcup_{i\in I}B_i\right)\\
&\iff \neg(\exists\, i\in I\ (x\in B_i))\\
&\iff \forall\, i\in I\ (x\notin B_i))\\
&\iff \forall\, i\in I\ (x\in {B_i}^c))\\
&\iff x\in\bigcap_{i\in I}{B_i}^c
\end{aligned}$$

**問 2.6.3.** 上の定理の (4) を証明せよ。

## 2.7 直積集合

二つのもの $a$ と $b$ を並べたもの $(a,b)$ を $a$ と $b$ から作られた**順序対**という。順序対 $(a,b)$ と $(a',b')$ が等しいことを $a=a'$ かつ $b=b'$ で定め、このとき $(a,b)=(a',b')$ と書く。$(a,b)$ と $(a',b')$ が等しくないことは $(a,b)\neq(a',b')$ と書く。$(a,b)\neq(a',b')$ であることと $a\neq a'$ または $b\neq b'$ が成り立つことは同値である。

$A$, $B$ を集合とする。$a\in A$ と $b\in B$ とから作られた順序対 $(a,b)$ の全体からなる集合を $A$ と $B$ の**直積**、または**直積集合** (direct product, Cartesian product) と呼び $A\times B$ で表す。

$$A\times B=\{(a,b)\mid a\in A,\ b\in B\}$$

三つ以上の集合に対しても直積は定義できる。

$$A\times B\times C=\{(a,b,c)\mid a\in A,\ b\in B,\ c\in C\}$$

などとすればよい。

**注意.** $A\times B$ と $B\times A$ は違うものと考えなくてはならない。

一般に同じ集合いくつかの直積を次のように表す。

$$A^n=\overbrace{A\times\cdots\times A}^{n\text{ 個}}$$

**例 2.7.1.** 座標平面上の点は、その座標を用いて $(x,y)$ のように書くことができる。これは座標平面と直積集合 $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$ が本質的に同じものであることを示している。同様に座標空間は $\mathbb{R}^3$ と思うことができる。

**問 2.7.2.** $A=\{1,2,3\}$, $B=\{a,b\}$ とするとき、直積集合 $A\times B$ の元をすべて書け。

**例 2.7.3.** $A$, $B$ を有限集合とする。このとき直積集合 $A\times B$ も有限集合で

$$|A\times B|=|A|\times|B|$$

が成り立つ。

有限とは限らない集合の族 $\{A_i\}_{i\in I}$ に対しても、その直積集合は定義できる。これを

$$\prod_{i\in I}A_i$$

とかく。

**例 2.7.4.** 集合の族 $\{A_i\}_{i\in I}$ を考える。ある $i\in I$ に対して $A_i=\emptyset$ であるならば $\prod_{i\in I}A_i=\emptyset$ である。

**注意.** 集合の族 $\{A_i\}_{i\in I}$ に対して、任意の $i\in I$ に対して $A_i$ が空でないならば、直積集合 $\prod_{i\in I}A_i$ も空でないように思われる。しかしこれは後で述べる**選択公理**に関することであり、自明ではない。

## 2.8 べき集合

集合 $A$ の部分集合すべての集合を $A$ の**べき集合** (power set) といい $2^A$, または $\mathcal{P}(A)$ と表す。

**例 2.8.1.** (1) $A=\{1,2\}$ に対して $2^A=\{\emptyset,\{1\},\{2\},\{1,2\}\}$ である。

(2) $A=\{1,2,3\}$ に対して $2^A=\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$ である。

集合 $A$ が有限集合である場合には、それぞれの要素が部分集合に含まれるか含まれないかを決めれば部分集合が定まる。したがって $2^A$ の要素の数は $2^{|A|}$ 個あることが分かる。これがべき集合を $2^A$ と書く理由である。

## 2.9 ラッセルのパラドックス

先に述べたように、ここでは厳密な集合の定義はしていない。しかし集合のようなものの集まりでも集合ではないものが存在することに注意しておく。簡単に言えば、あまりにも大きな集まりは集合ではない場合がある。例えば「集合すべての集まり」は集合ではない。これに似た状況から矛盾が生じる「ラッセルのパラドックス」(Russell's paradox) について説明をする。

まず空集合 $\emptyset$ は何も要素を含まないので $\emptyset \notin \emptyset$ である。このように自分自身を要素として含まない集合すべての集まり $A = \{X \mid X \notin X\}$ を考える。$A$ が集合であると仮定する。$\emptyset \in A$ であるから $A \neq \emptyset$ である。

- $A \in A$ か $A \notin A$ のいずれか一方のみが真である。
- $A \notin A$ と仮定する。このとき $A \notin A$ であるから $A \in A$ である。これは矛盾である。
- $A \in A$ と仮定する。このとき $A \in A$ であるから $A \notin A$ である。これは矛盾である。
- 以上より $A \in A$ でも $A \notin A$ でもあり得ない。これはおかしい。

これを「ラッセルのパラドックス」という。この場合 $A$ が集合であるとした部分がおかしく、$A$ は集合ではない。現在の数学ではこのような矛盾の起きないように集合論を構築しているが、その内容はやや難しい。ここで注意しておくことは $\{x \mid P(x)\}$ という形で定義されたものでも集合とは限らないということである。

**注意.** 集合全体の集まりを扱うには**圏** (category) という概念を導入する必要がある。

## 2.10 演習問題

(1) $A \subset B$ とするとき次を示せ。

  (a) $A \cap C \subset B \cap C$
  (b) $A \cup C \subset B \cup C$

(2) $A \cap B = \emptyset$ ならば $(A \cup B) - B = A$ であることを示せ。

(3) $A \cap C = B \cap C$ かつ $A \cup C = B \cup C$ ならば $A = B$ であることを示せ。

(4) 自然数 $\mathbb{N}$ で添字付けられた集合の族 $\{A_n \mid n \in \mathbb{N}\}$ に対して

$$B_m = \bigcup_{j=m}^{\infty} A_j, \quad C_m = \bigcap_{j=m}^{\infty} A_j$$

とおく。このとき次を示せ。

  (a) $\bigcap_{m=1}^{\infty} B_m$ は無数に多くの $A_n$ に含まれる元の全体である。
  (b) $\bigcup_{m=1}^{\infty} C_m$ はある番号以上のすべての $A_n$ に含まれる元の全体である。
  (c) $m > n$ ならば $A_m \subset A_n$ であるとする。このとき $\bigcap_{m=1}^{\infty} B_m = \bigcup_{m=1}^{\infty} C_m$ であることを示せ。

# Chapter 3

# 写像

## 3.1 写像

$A$, $B$ を集合とする。$A$ の各元に対して $B$ の元が一つ定まっているとする。このときこの対応を $A$ から $B$ への**写像** (map) という。$f$ が $A$ から $B$ への写像であることを

$$f : A \to B$$

と表す。このとき $A$ を**定義域** (domain)、$B$ を**値域** (range) という。写像 $f$ によって $a \in A$ に 対応する $B$ の元を $f(a)$ と表し、これを $a$ の $f$ による**像**という。どのように定まる写像なのかを明示したい場合には

$$f : A \to B \quad (a \mapsto f(a))$$

などと書く。

**例 3.1.1.** 通常は $f : A \to B$ と書けば $f$ が写像であることを意味するが、以下の例では簡単のため写像ではないものに対しても同様の記号を用いる。

(1) $f : \mathbb{N} \to \mathbb{N}$ を $f(a) = a + 1$ で定めれば、これは写像である。

(2) $f : \mathbb{N} \to \mathbb{N}$ を $f(a) = a - 1$ で定めると、これは写像ではない。なぜならば $1 \in \mathbb{N}$ に対して $f(1) = 1 - 1 = 0 \notin \mathbb{N}$ であり、1 の $f$ による像が定まらないからである。

(3) $f : \mathbb{R} \to \mathbb{R}$ を $f(a)$ は $a$ の平方根とすると、これは写像ではない。まず正の数について平方根は 2 つあり、このどちらを対応させるのかが定かでない。また負の数については平方根は $\mathbb{R}$ に存在しないので対応が決まらない。

(4) $f : \mathbb{R}_{>0} \to \mathbb{R}$ を $f(a)$ は $a$ の正の平方根とする。すなわち $f(a) = \sqrt{a}$ である。このとき $f$ は写像である。また値域を $\mathbb{R}_{>0}$ としても、これは写像である。

(5) $f : \mathbb{Q} \to \mathbb{N}$ を $f(a)$ は $a$ の分母として定めると、これは写像ではない。なぜならば有理数の書き方は一意的でなく、分母の定義が曖昧だからである。これを「分母が正である既約分数に表したときの分母」とすれば、これは一意的に定まるので写像になる。ただし「整数に対しては分母を 1 とする」などの注意も書き加えた方がよいだろう。当たり前のことに感じるかもしれないが、分母や分子に変数を含むような場合に誤りやすい。

(6) $P(x)$ を実数係数多項式とする。このとき $f : \mathbb{R} \to \mathbb{R}$ を $f(a) = P(a)$ で定めれば、これは写像である。通常はこの写像 $f$ と多項式 $P$ に同じ記号を用いる。

(7) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 1/(x^2 - 1)$ は $x = \pm 1$ で値が定まらないので写像ではない。このとき、定義域を変えて $f : \mathbb{R} - \{\pm 1\} \to \mathbb{R}$, $f(x) = 1/(x^2 - 1)$ とすれば、これは写像となる。$f : \mathbb{R} \to \mathbb{R}$, $f(x) = 1/(x^2 + 1)$ は写像である。

この例を見れば分かるように写像 $f : A \to B$ が定まるためには次のことが必要である。

(1) 任意の $a \in A$ に対して $f(a)$ が定まる。ただし $a \in A$ の記述の仕方が一意的でない場合には、どのような記述に対しても同じ元が対応しなければならない。

(2) (1) で定まった $f(a)$ は $B$ の元である。

$f$ がこの条件を満たすとき $f$ が定まる、または $f$ は**矛盾なく定義される** (well-defined) という。

二つの写像 $f : A \to B$ と $g : C \to D$ が**等しい**とは、$A = C$, $B = D$ であり、任意の $a \in A$ に対して $f(a) = g(a)$ となることとする。このとき $f = g$ と書く。

**例 3.1.2.** $A$ を空でない任意の集合とする。$f : A \to A$ を、任意の $a \in A$ に対して $f(a) = a$ とすれば $f$ は写像である。これを $A$ の**恒等写像** (identity map) といい $\mathrm{id}_A$ と書く。($A$ が空のときも恒等写像は定義できるが、その意味は分かりにくいだろう。)

**例 3.1.3.** $A$ を集合、$B$ を空でない任意の集合とする。$b \in B$ を一つ固定する。$f : A \to B$ を、任意の $a \in A$ に対して $f(a) = b$ とすれば $f$ は写像である。これを**定値写像** (constant map) という。

**例 3.1.4.** $A = \{1, 2, 3\}$, $B = \{a, b\}$ とする。$f : A \to B$ を $f(1) = a$, $f(2) = a$, $f(3) = b$ で定めればこれは写像である。写像 $f : A \to B$ を決めるには $f(1), f(2), f(3)$ を定めればよいので $A$ から $B$ への写像は全部で $2^3 = 8$ 個あることが分かる。

より一般に $A = \{1, 2, \cdots, m\}$, $B = \{1, 2, \cdots, n\}$ とするとき $A$ から $B$ への写像は $n^m$ 個ある。($A$ から $B$ への写像全体の集合を $\mathrm{Map}(A, B)$, または $B^A$ などと書いたりする。)

**問 3.1.5.** $A = \{1, 2\}$, $B = \{1, 2, 3\}$ とするとき $A$ から $B$ への写像をすべて書け。

**問 3.1.6.** $A = \{1, 2\}$ とする。$A$ から $\mathbb{R}$ への写像、$\mathbb{R}$ から $A$ への写像をそれぞれ一つ、具体的に構成せよ。

**例 3.1.7.** $A$ を任意の集合とするとき、空集合 $\emptyset$ から $A$ への写像が唯一つ存在する。実際、写像を決めるには $\emptyset$ の任意の要素に対してその像を決めればよいが、$\emptyset$ は要素をもたないので、何も決めなくても写像は定まる。また二つの写像について、任意の要素 (存在しない) の像が等しいので、それらは等しい。

特に $\emptyset$ から $\emptyset$ への写像は唯一つ存在する。$A \neq \emptyset$ に対しては $A$ から $\emptyset$ への写像は存在しない。

**例 3.1.8.** $A$ を任意の集合とし、$B = \{b\}$ は唯一つの要素をもつ集合とする。このとき $A$ から $B$ への写像が唯一つ存在する。実際、$B$ には要素が一つしかないので、任意の $a \in A$ に対して、その像は $b$ でなければならない。

## 3.2 合成写像

$f : A \to B$, $g : B \to C$ をそれぞれ写像とする。このとき $a \in A$ を $f$ で移して、続けて $g$ で移すという操作が考えられる。このように考えると $A$ から $C$ への新しい写像が得られる。これを $f$ と $g$ の**合成写像** (composite map) といい $g \circ f$ と書く。

$$g \circ f : A \to C \qquad (a \mapsto g(f(a)))$$

はじめに $f$ で移しているのに $g \circ f$ と書くのは、その像が $g(f(a))$ となっているからである。(場合によっては写像の合成を逆の順序で書くこともあるが、この講義ではこの順序で統一する。) このとき $f$ の値域と

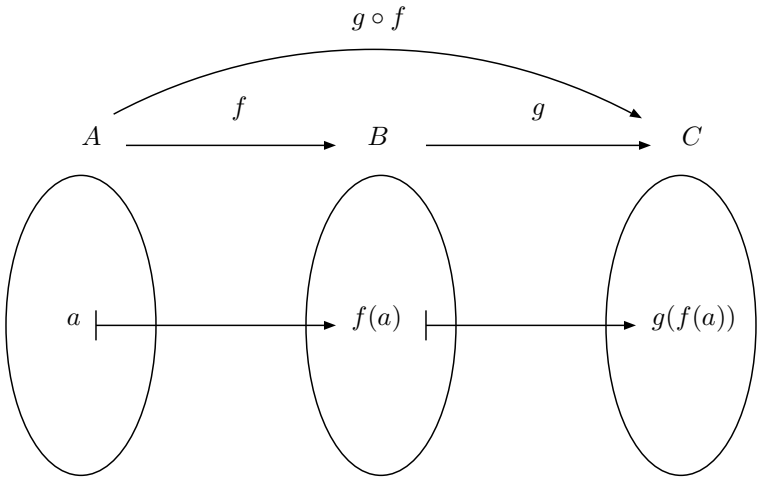


Figure 3.1: $g \circ f$

$g$ の定義域が一致していることが重要で、そうでないときには合成写像は考えられない。(実際には $f$ の値域が $g$ の定義域に含まれていればよいが、正確には後で説明する。)

三つの写像 $f : A \to B$, $g : B \to C$, $h : C \to D$ に対して、写像の合成に関する結合法則

$$(h \circ g) \circ f = h \circ (g \circ f)$$

が成り立つことはすぐに分かるであろう。

**例 3.2.1.** 写像の定義域と値域が一致しているときには、同じ写像の合成を考えることができる。$f : A \to A$ に対して $f^0 = \mathrm{id}_A$, $f^{n+1} = f \circ f^n$ $(n \geq 1)$ として $f^n$ $(n \in \{0\} \cup \mathbb{N})$ を定義することができる。このとき $f^{m+n} = f^m \circ f^n$ が成り立つ。

**例 3.2.2.** $f : \mathbb{R} \to \mathbb{R}$ を $f(x) = x^2 + 1$ で定める。このとき $f^2(x) = f(x^2+1) = (x^2+1)^2 + 1 = x^4 + 2x^2 + 2$ である。

## 3.3 制限写像

写像 $f : A \to B$ を考える。また $C \subset A$ とする。$c \in C$ は $A$ の元でもあるので $f(c) \in B$ が定まる。このようにして写像 $C \to B$ が定義される。これを $f$ の $C$ への**制限** (restriction)、または**制限写像**といい $f|_C$ と書く。

これと似たこととして $f : A \to B$ に対して、すべての像 $f(a)$ が $B$ の部分集合 $C$ に含まれるならば、自然に $f' : A \to C$ $(f'(a) = f(a))$ が定義できる。($f'$ は同じ記号 $f$ を用いて表されることも多い。)

## 3.4 全射

写像 $f : A \to B$ を考える。$C \subset A$ に対して

$$f(C) = \{f(c) \mid c \in C\}$$

とおいて、これを $f$ による $C$ の**像** (image) という。定義から明らかなように $f(C)$ は $B$ の部分集合である。ここで注意するのは $C$ は $A$ の部分集合であって $A$ の元ではないので、今までの意味では $f(C)$ は定

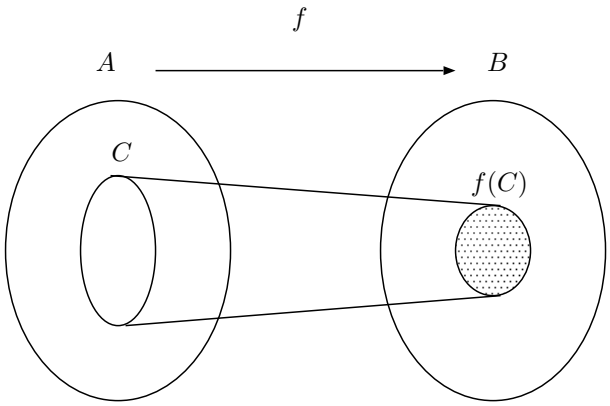


Figure 3.2: $f(C)$

義されない。この場合の $f(C)$ とは新しく定義した記号であり、通常の意味での写像の像ではない。

**注意.** 正確には以下のように考える。$f$ に対して $\widetilde{f} : \mathcal{P}(A) \to \mathcal{P}(B)$ を $\widetilde{f}(C) := \{f(c) \mid c \in C\}$ で定めると、これは写像である。$\widetilde{A} = \{S \in \mathcal{P}(A) \mid |S| = 1\}$ とおくと、$\widetilde{A}$ は自然に $A$ と同じものと考えることができる。同様に $\widetilde{B} = \{T \in \mathcal{P}(B) \mid |T| = 1\}$ とおくと、$\widetilde{B}$ は自然に $B$ と同じものと考えることができる。このように考えれば、制限写像 $\widetilde{f}|_A$ は $f$ と同じものと考えられる。この意味で $\widetilde{f}$ を $f$ と書けば、上で説明したような記号となる。

**例 3.4.1.** 写像 $f : \mathbb{R} \to \mathbb{R}$ を $f(x) = x^2$ で定める。$a, b \in \mathbb{R}$ に対して $(a, b) = \{r \in R \mid a < r < b\}$, $(a, b] = \{r \in R \mid a < r \leq b\}$, $[a, b) = \{r \in R \mid a \leq r < b\}$, $[a, b] = \{r \in R \mid a \leq r \leq b\}$ を、それぞれ開区間、半開区間、半開区間、閉区間という。このとき

$$\begin{aligned} f([1,2)) &= [1,4) \\ f((-1,2)) &= [0,4] \\ f((-\infty,1]) &= [0,\infty) \\ f(\mathbb{R}) &= [0,\infty) \end{aligned}$$

などとなる。

像の定義において、特に $C = A$ としたとき $f(A)$ を単に $f$ の**像** (image) といい $\operatorname{Im} f$ とも書く。$\operatorname{Im} f = B$

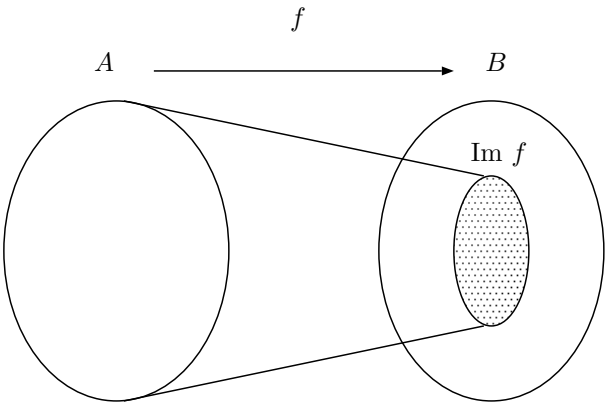


Figure 3.3: $\operatorname{Im} f$

が成り立つとき $f$ を**全射** (surjection) という。すなわち $f : A \to B$ が全射であるとは

- 任意の $b \in B$ に対して、ある $a \in A$ があって $f(a) = b$ となる

ということである。$f$ が全射であることを $f : A \twoheadrightarrow B$ などと書くこともある。

**例 3.4.2.** (1) $f : \mathbb{Z} \to \mathbb{Z}$ $(a \mapsto a + 1)$ は全射である。なぜならば、任意の $b \in \mathbb{Z}$ に対して $b - 1 \in \mathbb{Z}$ であり $f(b - 1) = (b - 1) + 1 = b$ が成り立つからである。

(2) $f : \mathbb{N} \to \mathbb{N}$ $(a \mapsto a + 1)$ は全射ではない。なぜならば、$1 \in \mathbb{Z}$ に対して $f(a) = a + 1 = 1$ となる $a \in \mathbb{N}$ が存在しないからである (そのような $a$ は 0 であるが $0 \notin \mathbb{N}$ である)。

**命題 3.4.3.** $f : A \to B$, $g : B \to C$ を考える。$f$, $g$ がともに全射であるならば $g \circ f : A \to C$ は全射である。

**証明**. $c \in C$ とする。$g$ は全射なので $g(b) = c$ となる $b \in B$ が存在する。$f$ は全射なので $f(a) = b$ となる $a \in A$ が存在する。このとき $g \circ f(a) = g(f(a)) = g(b) = c$ となる。よって $g \circ f$ は全射である。 □

命題 3.4.3 の別証明. $f(A) = B$, $f(B) = C$ であるから $g \circ f(A) = g(f(A)) = g(B) = C$ である。 □

**命題 3.4.4.** $f : A \to B$, $g : B \to C$ を考える。このとき合成写像 $g \circ f : A \to C$ の像について $\operatorname{Im}(g \circ f) \subset \operatorname{Im} g$ が成り立つ。特に $g \circ f : A \to C$ が全射であれば $g$ は全射である。

**証明**. $c \in \operatorname{Im}(g \circ f)$ とする。このとき、ある $a \in A$ があって $g(f(a)) = c$ である。$f(a) \in B$ であるから $c \in \operatorname{Im} g$ である。よってはじめの主張を得る。

$g \circ f$ が全射であるとする。このとき

$$C = \operatorname{Im}(g \circ f) \subset \operatorname{Im} g = g(B) \subset C$$

であるから $g(B) = C$ となり $g$ は全射である。 □

**命題 3.4.5.** 写像 $f : A \to B$ に対して、「任意の集合 $C$ と二つの写像 $g : B \to C, h : B \to C$ について、$g \circ f = h \circ f$ ならば $g = h$ である」という条件を考える。この条件が満たされることと $f$ が全射であることは同値である。

**証明.** $f$ が全射であるとし、$g \circ f = h \circ f$ とする。$b \in B$ を任意にとる。$f$ は全射なので、ある $a \in A$ があって $f(a) = b$ である。このとき

$$g(b) = g(f(a)) = g \circ f(a) = h \circ f(a) = h(f(a)) = h(b)$$

となるので $g = h$ である。

$f$ が全射でないとする。$b_0 \in B$ で $b_0 \notin f(A)$ なるものが存在する。$C = \{x, y\}$ $(x \neq y)$ とおき、任意の $b \in B$ に対して $g(b) = x$ で $g : B \to C$ を定め、

$$h(b) = \begin{cases} x & \text{if } b \neq b_0 \\ y & \text{if } b = b_0 \end{cases}$$

で $h : B \to C$ を定める。このとき $b_0 \notin f(A)$ としているので、任意の $a \in A$ に対して $g \circ f(a) = x = h \circ f(a)$ となる。すなわち $g \circ f = h \circ f$ であるが $g \neq h$ なので、$f$ は命題の条件を満たさない。 □

## 3.5 単射

写像 $f : A \to B$ を考える。$b \in B$ に対して

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

とおいて、これを $f$ による $b$ の**逆像** (inverse image) という。これも単なる記号であり $f^{-1}$ は写像ではない。(正確には $f^{-1} : B \to \mathcal{P}(A)$ である。)

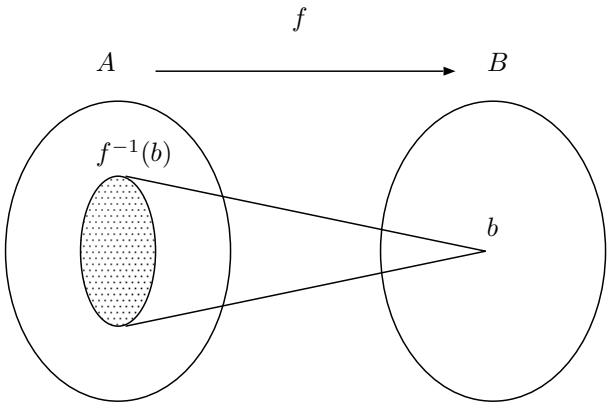


Figure 3.4: $f^{-1}(b)$

$C \subset B$ に対しても

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

とおいて、これを $f$ による $C$ の**逆像** (inverse image) という。(この場合、正確には $f^{-1} : \mathcal{P}(B) \to \mathcal{P}(A)$ である。)

$$f^{-1}(C) = \bigcup_{b \in C} f^{-1}(b)$$

が成り立つことは明らかであろう。

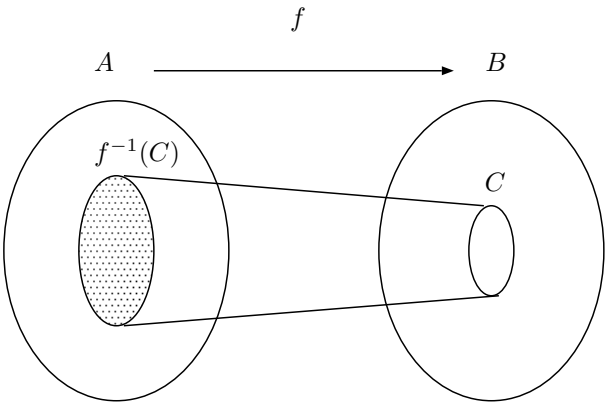


Figure 3.5: $f^{-1}(C)$

**例 3.5.1.** 写像 $f : \mathbb{R} \to \mathbb{R}$ を $f(x) = x^2$ で定める。このとき

$$\begin{aligned} f^{-1}(1) &= \{-1, 1\} \\ f^{-1}(-1) &= \emptyset \\ f^{-1}([1, 4)) &= (-2, -1] \cup [1, 2) \\ f^{-1}([-4, -1)) &= \emptyset \\ f^{-1}((-4, 1)) &= (-1, 1) \\ f^{-1}((-\infty, 1]) &= [-1, 1] \\ f^{-1}(\mathbb{R}) &= \mathbb{R} \end{aligned}$$

などとなる。

**問 3.5.2.** $f : A \to B$ を写像とし $C \subset B$ とする。$f(f^{-1}(C)) \subset C$ であることを示せ。また $f(f^{-1}(C)) = C$ とはならない例を示せ。

**問 3.5.3.** 写像 $f : A \to B$ を考える。$b, b' \in B$, $b \neq b'$ であるとき $f^{-1}(b) \cap f^{-1}(b') = \emptyset$ であることを示せ。

任意の $b \in B$ に対して $f^{-1}(b)$ が高々一つの元しか含まないとき、$f$ を**単射** (injection) という。言い換えると

- $f(a) = f(a')$ ならば $a = a'$ である
- $a \neq a'$ ならば $f(a) \neq f(a)'$ である (上の命題の対偶)

ということである。$f$ が単射であることを $f : A \rightarrowtail B$ などと書くこともある。

**例 3.5.4.** (1) $f : \mathbb{Z} \to \mathbb{Z}$ $(a \mapsto a^2)$ は単射ではない。なぜならば $1 \neq -1$ であるが $f(1) = 1^2 = (-1)^2 = f(-1)$ が成り立つからである。

(2) $f : \mathbb{N} \to \mathbb{N}$ $(a \mapsto a^2)$ は単射である。なぜならば $a \neq a'$ ならば $a^2 \neq (a')^2$ が成り立つからである。

**命題 3.5.5.** $f : A \to B$, $g : B \to C$ を考える。$f$, $g$ がともに単射であるならば $g \circ f : A \to C$ は単射である。

**証明.** $a, a' \in A$ に対して $g \circ f(a) = g \circ f(a')$ とする。$g(f(a)) = g(f(a'))$ で $g$ が単射なので $f(a) = f(a')$ である。また $f$ が単射なので $a = a'$ である。よって $g \circ f$ は単射である。 □

**命題 3.5.6.** $f : A \to B$, $g : B \to C$ を考える。合成写像 $g \circ f : A \to C$ が単射であれば $f$ は単射である。

**証明.** $a, a' \in A$ とし $f(a) = f(a')$ とする。このとき $g \circ f(a) = g(f(a)) = g(f(a')) = g \circ f(a')$ である。$g \circ f$ が単射であるから $a = a'$ である。よって $f$ は単射である。 □

**命題 3.5.7.** 写像 $f : A \to B$ に対して、「任意の集合 $C$ と二つの写像 $g : C \to A$, $h : C \to A$ について、$f \circ g = f \circ h$ ならば $g = h$ である」という条件を考える。この条件が満たされることと $f$ が単射であることは同値である。

**証明.** $f$ が単射であるとし、$f\circ g = f\circ h$ とする。$c\in C$ に対して $f(g(c)) = f\circ g(c) = f\circ h(c) = f(h(c))$ である。$f$ が単射なので $g(c) = h(c)$ となり $g = h$ となる。

$f$ が単射でないとする。$a, a'\in A$, $a\neq a'$ で $f(a) = f(a')$ となるものがある。$C = \{c\}$ とおいて $g(c) = a$, $h(c) = a'$ として $g : C\to A$, $h : C\to A$ を定める。このとき $g\neq h$ であるが $f(g(c)) = f(a) = f(a') = f(h(c))$ となり $f\circ g = f\circ h$ が成り立つ。よって命題の条件はみたされない。 □

**例 3.5.8.** $A\subset B$ であるとき $f : A\to B$ を $f(a) = a$ で定めることができる。これを $A$ の $B$ への**埋め込み** (inclusion)、または**包含写像**という。埋め込は明らかに単射である。

**例 3.5.9.** $f : A\to B$ とする。$B\subset C$ なる $C$ に対して $f' : A\to C$ を $f'(a) = f(a)\in C$ で定めることができる。これは正確には次のように解釈される。$\iota : B\to C$ を埋め込みとし、合成写像 $\iota\circ f : A\to C$ を考えるのである。

**例 3.5.10.** 合成写像のところで $f : A\to B$, $g : C\to D$ で $B\subset C$ ならば、合成写像を考えることができると書いた。これは正確には次のように解釈される。すなわち $\iota : B\to C$ を埋め込みとし、合成写像 $g\circ\iota\circ f : A\to D$ を考えるのである。

## 3.6 全単射

$f : A\to B$ が**全単射** (bijection) であるとは、$f$ が全射かつ単射であることとする。言い換えると

- 任意の $b\in B$ に対して $f(a) = b$ となる $a\in A$ が唯一つ存在する

ということである。このとき「任意の $b\in B$ に対して $f(a) = b$ となる $a\in A$ が存在する」ことから全射、「唯一つ存在する」ということから単射であることが分かる。この言い換えから全単射 $f : A\to B$ に対しては、$b\in B$ に対して $f(a) = b$ となる $a\in A$ を対応させることによって写像 $g : B\to A$ が定まる。この写像 $g$ を $f$ の**逆写像**といって $f^{-1}$ で表す。逆像の定義でも $f^{-1}$ という記号を用いたが、そのときは $f^{-1}$ は単なる記号であった。しかしここでは $f^{-1}$ は写像であるので注意が必要である。

**例 3.6.1.** $A$ を集合とする。恒等写像 $\mathrm{id}_A : A\to A$ $(a\mapsto a)$ は明らかに全単射である。$(\mathrm{id}_A)^{-1} = \mathrm{id}_A$ であることは明らかだろう。恒等写像は $A\subset A$ と見たときの埋め込みに等しい。

**命題 3.6.2.** 全単射 $f : A\to B$ とその逆写像 $f^{-1} : B\to A$ について次が成り立つ。

$$f^{-1}\circ f = \mathrm{id}_A,\qquad f\circ f^{-1} = \mathrm{id}_B$$

**命題 3.6.3.** $f : A\to B$ が全単射であるための必要十分条件は、ある $g : B\to A$ があって $g\circ f$, $f\circ g$ が共に全単射となることである。

**証明.** $f : A\to B$ が全単射であれば $g$ として $f^{-1}$ をとれば命題 3.6.2 より $f^{-1}\circ f = \mathrm{id}_A$, $f\circ f^{-1} = \mathrm{id}_B$ は共に全単射である。

$g : B\to A$ に対して $g\circ f$, $f\circ g$ が共に全単射であるとする。このとき $g\circ f$ が全射であるから命題 3.4.4 より $f$ は全射であり、$f\circ g$ が単射であるから命題 3.5.6 より $f$ は単射である。 □

**定理 3.6.4.** $|A| = |B| < \infty$ とする。このとき写像 $f : A\to B$ について、次は同値である。

(1) $f$ は単射。

(2) $f$ は全射。

(3) $f$ は全単射。

証明のために簡単な補題を用意しよう。補題の証明は定義から明らかである。

**補題 3.6.5.** $f : A\to B$ が全射であるための必要十分条件は、任意の $b\in B$ に対して $|f^{-1}(b)|\geq 1$ となることである。また、単射であるための必要十分条件は、任意の $b\in B$ に対して $|f^{-1}(b)|\leq 1$ となることである。

定理 3.6.4 の証明. (3) $\Longrightarrow$ (1), (3) $\Longrightarrow$ (2) は明らか。(1) $\Longrightarrow$ (2), (2) $\Longrightarrow$ (1) を示せばよい。$A = f^{-1}(B) = \bigcup_{b\in B} f^{-1}(b)$ であり、$b\neq b'$ ならば $f^{-1}(b)\cap f^{-1}(b') = \emptyset$ なので $|A| = \sum_{b\in B}|f^{-1}(b)|$ であることに注意しておく。

$f$ を単射とする。任意の $b \in B$ に対して $|f^{-1}(b)| \leq 1$ である。よって

$$|A| = \sum_{b \in B} |f^{-1}(b)| \leq |B| = |A|$$

となり、任意の $b \in B$ に対して $|f^{-1}(b)| = 1$ である。よって $f$ は全射である。

$f$ を全射とする。任意の $b \in B$ に対して $|f^{-1}(b)| \geq 1$ である。よって

$$|B| \leq \sum_{b \in B} |f^{-1}(b)| = |A| = |B|$$

となり、任意の $b \in B$ に対して $|f^{-1}(b)| = 1$ である。よって $f$ は単射である。 □

**例 3.6.6.** $|A| = \infty$ のときは $f : A \to A$ が全射、または単射であっても全単射とは限らない。例えば $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = 2a$ は単射であるが全射ではない。また $f : \mathbb{N} \to \mathbb{N}$, $f(1) = 1$, $f(a) = a - 1$ $(a > 1)$ とすれば、これは全射ではあるが単射ではない。

**例 3.6.7.** $f : A \to B$ を単射とする。$f' : A \to \mathrm{Im}\, f$ を $f'(a) = f(a)$ で定義することができる。このとき $f'$ は全単射である。

## 3.7 二項演算

整数の足し算とは何だろうか。これは写像を用いて説明される。すなわち、それは写像 $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ に他ならない。$f(a, b)$ を $a + b$ という記号を用いて表しているだけである。

このように、ある集合 $A$ に対して、写像 $f : A \times A \to A$ が与えられるとき、それを $A$ の**二項演算** (binary operation) という。二項演算の像は適当な記号、ここでは仮に $\triangle$ とする、を用いて $f(a, b) = a \triangle b$ のように表される。二項演算 $(a, b) \mapsto a \triangle b$ に対して

**交換法則：** $a \triangle b = b \triangle a$

**結合法則：** $(a \triangle b) \triangle c = a \triangle (b \triangle c)$

などが考えられるが、二項演算がこれらを満たしている必要はない。

**例 3.7.1.** 実数の減法は交換法則も結合法則も満たさない二項演算である。また実数の除法は 0 で割ることができないので、二項演算ではない。

## 3.8 その他

**命題 3.8.1.** 集合 $A$, $B$ に対し $\mathrm{Map}(A, B)$ で $A$ から $B$ への写像全体の集合を表す。$C$ は空でない集合とする。$f : A \to B$ が与えられたとき $f^* : \mathrm{Map}(B, C) \to \mathrm{Map}(A, C)$ を $f^*(\varphi) = \varphi \circ f$ で定義する。このとき

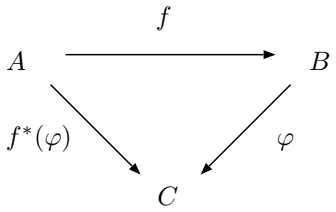


Figure 3.6: $f^*(\varphi) = \varphi \circ f$

次が成り立つ。

(1) $f$ が単射ならば $f^*$ は全射である。

(2) $f$ が全射ならば $f^*$ は単射である。

**証明**. (1) $f$ を単射とする。このとき全単射 $g : A \to \mathrm{Im}\, f$ が得られる。任意の $a \in A$ に対して $g(a) = f(a)$ である。

$\psi \in \mathrm{Map}(A, C)$ を任意にとる。$c \in C$ を一つ固定しておく。$\varphi \in \mathrm{Map}(B, C)$ を $b \in \mathrm{Im}\, f$ に対しては $\varphi(b) = \psi(g^{-1}(b))$ で定め、$b \notin \mathrm{Im}\, f$ に対しては $\varphi(b) = c$ と定める。このとき、任意の $a \in A$ に対して

$$f^*(\varphi)(a) = \varphi(f(a)) = \varphi(g(a)) = \psi(g^{-1}(g(a))) = \psi(a)$$

となる。よって $f^*(\varphi) = \psi$ であり、$f^*$ は全射である。

(2) $f$ を全射とする。$f^*(\varphi) = f^*(\varphi')$ とする。このとき、任意の $a \in A$ に対して $\varphi(f(a)) = \varphi'(f(a))$ である。$f$ が全射なので $\varphi = \varphi'$ となり $f^*$ は単射である。 □

**命題 3.8.2.** $f : B \to C$ とする。$f_* : \mathrm{Map}(A, B) \to \mathrm{Map}(A, C)$ を $f_*(\psi) = f \circ \psi$ で定義する。このとき次

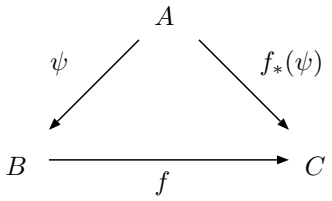


Figure 3.7: $f_*(\psi) = f \circ \psi$

が成り立つ。

(1) $f$ が単射ならば $f_*$ は単射である。

(2) $f$ が全射ならば $f_*$ は全射である。

**証明**. (1) $f$ を単射とする。$f_*(\psi) = f_*(\psi')$ とすれば、任意の $a \in A$ に対して $f(\psi(a)) = f(\psi'(a))$ であるが、$f$ が単射なので $\psi(a) = \psi'(a)$ である。よって $\psi = \psi'$ であり $f_*$ は単射である。

(2) $f$ を全射とする。任意の $\varphi : A \to C$ に対して $\psi : A \to B$ を以下のように定める。$f$ は全射であるから、任意の $c \in C$ に対して $b_c \in f^{-1}(c)$ を選ぶことができる (実はここで後で説明する選択公理を使っている)。$a \in A$ に対して $\psi(a) = b_{\varphi(a)}$ と定める。このとき $(f_*(\psi))(a) = f(\psi(a)) = f(b_{\psi(a)}) = \varphi(a)$ であるから $f_*(\psi) = \varphi$ である。よって $f_*$ は全射である。 □

**問 3.8.3.** $A = \{1, 2, \cdots, m\}$, $B = \{1, 2, \cdots, n\}$ とする。$A$ から $B$ への単射の個数を求めよ。

## 3.9 演習問題

(1) 写像 $f : \mathbb{R} \to \mathbb{R}$ で $|f^{-1}(0)| = 3$ となるものを一つ構成せよ。

(2) 写像 $f : \mathbb{N} \to \mathbb{N} \cup \{0\}$ を、$f(n)$ は $n$ を 5 で割った余りとして定める。$f$ の像 $f(\mathbb{N})$ は何か答えよ。また逆像 $f^{-1}(2)$ と $f^{-1}(\{1, 2\})$ を求めよ。

(3) $A, B$ は集合 $X$ の部分集合、$P, Q$ は集合 $Y$ の部分集合とする。写像 $f : X \to Y$ に対して次を示せ。

(a) $f(A \cup B) = f(A) \cup f(B)$

(b) $f(A \cap B) \subset f(A) \cap f(B)$ (等しくならない例も作れ)

(c) $f(A - B) \supset f(A) - f(B)$ (等しくならない例も作れ)

(d) $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$

(e) $f^{-1}(P \cup Q) = f^{-1}(P) \cup f^{-1}(Q)$

(f) $f^{-1}(P - Q) = f^{-1}(P) - f^{-1}(Q)$

(4) $f : A \to B$, $g : B \to C$ を写像とし $f$ が全単射であるとする。このとき $g$ が単射であることと $g \circ f$ が単射であることは同値である。また $g$ が全射であることと $g \circ f$ が全射であることは同値である。以上のことを示せ。

(5) $f : A \to B, g : B \to C$ を写像とし $g$ が全単射であるとする。このとき $f$ が単射であることと $g \circ f$ が単射であることは同値である。また $f$ が全射であることと $g \circ f$ が全射であることは同値である。以上のことを示せ。

(6) $f : A \to B, g : B \to C, h : C \to A$ に対して $h \circ g \circ f, g \circ f \circ h, f \circ h \circ g$ のうち二つが全射で、残りの一つが単射であるとすると、$f, g, h$ はすべて全単射であることを示せ。また、二つが単射で、残りの一つが全射であるとしても、$f, g, h$ はすべて全単射であることを示せ。

**学習のポイント.** 証明を書くときに気をつけたほうがよいこと、間違いやすいことをまとめておく。

- **仮定と結論**
  証明を書くときには仮定と結論をはっきりと意識して書かなくてはならない。仮定と結論をきちんと意識するためには定義を完全に理解しておく必要がある。当たり前のことであるが、これが出来ていない答案を多く見る。

- **文字の使い方**
  証明中で用いる文字は、どのようなものなのかをきちんと意識して書かなくてはならない。何も言わずに突然新しい文字を用いないようにしよう。「$a \in A$ とすると $\cdots$ である。**任意の** $a \in A$ に対して $\cdots$。」などと書いたときには「任意の」で新たに $a$ を取り直したものと考えられる。既に決まっているものに対して「任意の」などとは書かないはずだからである。

- **「とする」と「とおく」**
  何かを仮定するときには「$\cdots$ とする」、「$\cdots$ と仮定する」などとはっきりと書く。何かを仮定したいときに「$\cdots$ とおく」などと書く学生が少なくないが、「おく」のは既に定義されているものに別名をつけるときなどである。例えば長い数式を繰り返し用いたいときに「$A = \cdots$ とおく」などと用いる。「おく」ことは何かを仮定することではない。「$x \in X$ とおく」のはおかしく、「$x \in X$ とする」が正しい。ただし「$X$ から一つ元を取り、それを $x$ とおく」は正しい。この場合、「おく」前に元が取ってあり、それに名前を付けているからである。

- **「ならば」と「$\Longrightarrow$」**
  記号「$\Longrightarrow$」の用い方を誤っていると思われる答案を多く見る。命題「$A \Longrightarrow B$」が真であることを主張するために $A$ が真である必要はない。「$A$ である。よって $B$ である。よって $C$ である」と言いたいときに「$A \Longrightarrow B \Longrightarrow C$」と書くのは (必ずしも間違えとは言えないが) 不適当である場合が多い。なぜならば $A$ が真であることを知っているのに「$A$ ならば」という必要がないからである。

- **「$\Longleftrightarrow$」**
  記号「$\Longleftrightarrow$」を不用意に用いている答案が多い。当たり前のことであるが「$A \Longleftrightarrow B$」は「$A \Longrightarrow B$」かつ「$B \Longrightarrow A$」という意味である。この記号を用いるときには双方向の命題が真であることをきちんと確認しなければならない。双方向であることが必要ないのに安易に用いている例が少なくない。また、難しい証明では同じ道をたどって双方向の証明が出来るわけではないので、そのような場合には「$\Longleftrightarrow$」で結んで証明を書くことはできない。どうしても「$\Longleftrightarrow$」を用いなければならないことはないので、答案には用いないようにしたほうが無難である。もし用いるとしても、易しいことだけに用いるようにしよう。

- **「題意をみたす」**
  「題意をみたす」という記述を好む学生が少なくない。「題意」は「問題の意味」という意味である。学生が「題意」という言葉を証明中に用いているとき、そのほとんどが用法を間違えている。多くの場合「与えられた条件をみたす」または「要求された性質をもつ」などが適当であろう。「題意」という言葉を使った方がよいときはほとんど無いと思われるが、どうしても用いるときは使い方がおかしくないかをよく考えよう。

# Chapter 4

# 関係

世の中には、色々な “関係” がある。例えば、人と人との関係にも、

- A さんは B さんを知っている
- A さんは B さんのことが好きである
- A さんと B さんは同じ高校を卒業している
- A さんは B さんよりも将棋が強い

など、いくら書いてもきりがない。これは数学的な対象についても同様である。同じ集合に属する二つの元の “関係” について、それを数学的に定義し、議論する。

## 4.1 関係

**定義 4.1.1** (関係)**.** $A$ を集合とする。直積集合 $A \times A$ の部分集合 $R$ を $A$ 上の**二項関係** (binary relation)、または単に**関係** (relation) という。$A$ 上に関係 $R$ が定められていることを明示したい場合には $(A, R)$ と書く。

$R$ を関係とするとき $(x, y) \in R$ であることを $xRy$ とも書くことにする。

**例 4.1.2.** (1) $\leq = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ は $\mathbb{R}$ 上の関係である。

(2) $< = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$ は $\mathbb{R}$ 上の関係である。

(3) 集合 $A$ に対してべき集合 $2^A$ を考える。$\subset = \{(S, T) \in 2^A \times 2^A \mid S \subset T\}$ は $2^A$ 上の関係である。

(4) $\mid = \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n$ は $m$ の約数 $\}$ は $\mathbb{N}$ 上の関係である。

この例において、(1), (2), (3) では “$\leq$” などを定義する右辺で “$\leq$” 自身を使っていて、好ましい記述ではないが、例を理解するには十分であろう。

**例 4.1.3.** $\mathbb{Z}^\sharp = \mathbb{Z} - \{0\}$ とする。$\mathbb{Z}^\sharp \times \mathbb{Z}$ 上に

$$\sim = \{((m, a), (n, b)) \in (\mathbb{Z}^\sharp \times \mathbb{Z}) \times (\mathbb{Z}^\sharp \times \mathbb{Z}) \mid mb = na\}$$

で関係 $\sim$ を定義できる。

ここに挙げた例は (例 4.1.3 を除いて) よく知られた性質を用いて関係を定義しているが、一般に $A$ 上の関係は $A \times A$ の部分集合と言うだけでよいので、自由に関係を定義することができる。

## 4.2 順序関係

通常の生活でも、順序という言葉はよく用いられる。例えば、小学生でも背の低い順に列に並んだりする。この順序について考えよう。順序を表す記号として、よく使われるものを用いると、いろいろな先入観が入りやすいので、ここでは $\preceq$ という、あまり使われない記号を用いることにする。

**定義 4.2.1** (順序関係)**.** 集合 $A$ 上の関係 $\preceq$ が**順序関係** (order)、または単に**順序**であるとは、以下の条件を満たすこととする。

(1) [**反射律**] 任意の $x \in A$ に対して $x \preceq x$

(2) [**推移律**] $x \preceq y,\ y \preceq z$ ならば $x \preceq z$

(3) [**非対称律**] $x \preceq y,\ y \preceq x$ ならば $x = y$

このとき $(A, \preceq)$ を**順序集合** (ordered set) という。

**例 4.2.2.** 「ジャンケン」を考えよう。「グー」は「チョキ」に強く、「チョキ」は「パー」に強く、「パー」は「グー」に強い。これは推移律が成り立たないことを意味しており、ジャンケンにおける「強い」ということは、関係を定めてはいるが、それは順序関係ではない。

**例 4.2.3.** 例 4.1.2 の $(\mathbb{R}, \leq)$, $(\mathbb{N}, \mid)$, $(2^A, \subset)$ はすべて順序集合である。例 4.1.2 の $(\mathbb{R}, <)$ は条件 (1) を満たさないので順序集合ではない。例 4.1.3 $(\mathbb{N} \times \mathbb{Z}, \sim)$ は条件 (3) を満たさないので順序集合ではない。

練習のため例 4.1.2 の $(\mathbb{N}, \mid)$ が順序集合であることを示しておこう。

(1) まず、任意の $n \in \mathbb{N}$ に対して $n$ は $n$ の約数であるから $n \mid n$ である。

(2) $\ell, m, n \in \mathbb{N}$ に対して $\ell \mid m,\ m \mid n$ とすると $\ell$ は $m$ の約数であり $m$ は $n$ の約数であるから $\ell$ は $n$ の約数である。したがって $\ell \mid n$ が成り立つ。

(3) $m, n \in \mathbb{N}$ に対して $m \mid n$ かつ $n \mid m$ とすると $m$ は $n$ の約数で $n$ は $m$ の約数なので $m = n$ である。

以上より $(\mathbb{N}, \mid)$ が順序集合であることが示される。

ここで注意したいのは、例えば 2 と 3 については $2 \mid 3$ も $3 \mid 2$ も成り立たないということである。一般に順序集合の任意の二つの要素について「どちらかが大きい」という順序が定まるわけではない。

**定義 4.2.4** (全順序)**.** 順序集合 $(A, \preceq)$ の任意の二つの要素 $x, y \in A$ に対して $x \preceq y$ または $y \preceq x$ が成り立つとき、この順序を**全順序** (total order) といい、この順序集合を**全順序集合** (totally ordered set) という。単なる順序を全順序とはっきり区別したいときには**半順序** (partial order) という言い方もする。

**例 4.2.5.** 例 4.1.2 $(\mathbb{R}, \leq)$ は全順序集合であるが、例 4.1.2 $(\mathbb{N}, \mid)$ は全順序集合ではない。また $|A| \geq 2$ のとき $(2^A, \subset)$ は全順序集合ではない。

**例 4.2.6.** 前述の「小学生を背の低い順に並べる」ということを考えよう。ある小学校のクラスの生徒を、ある身体測定の際の身長の小さい順に並べるとする。より一般に、集合 $X$ と写像 $f : X \to \mathbb{R}$ が与えられ、$f$ による値によって、集合 $X$ の順序を決めるということを考えよう。自然に考えられる順序 $\preceq$ の決め方として

(1) $f(A) < f(B)$ のとき $A \preceq B$、すなわち

$$\preceq = \{(A, B) \in X \times X \mid f(A) < f(B)\}$$

(2) $f(A) \leq f(B)$ のとき $A \preceq B$、すなわち

$$\preceq = \{(A, B) \in X \times X \mid f(A) \leq f(B)\}$$

が考えられる。(1) は推移律、非対称律をみたすが、反射律をみたさないので順序ではない。(2) は反射律、推移律をみたすが、非対称律をみたさないので、やはり順序ではない。順序を定義するには

$$\preceq = \{(A, A) \in X \times X \mid A \in X\} \cup \{(A, B) \in X \times X \mid f(A) < f(B)\}$$

とすればよい。このとき $A \neq B$ で $f(A) = f(B)$ であるものに対しては $A \preceq B$ でも $B \preceq A$ でもなく、よってこの順序は一般には全順序ではない。

順序集合 $(A, \preceq)$ を考える。$B \subset A$ に対して $B$ の順序を $A$ の順序で定めれば、$B$ はまた順序集合になる。これを**順序部分集合**と呼ぶ。

順序集合 $(A, \preceq)$ の元 $x$ に対して $x \preceq y$ ならば $x = y$ が成り立つとき $x$ を $A$ の**極大元** (maximal element) という。同様に $y \preceq x$ ならば $x = y$ であるとき $x$ を $A$ の**極小元** (minimal element) という。任意の $y \in A$ に対して $y \preceq x$ のとき $x$ を $A$ の**最大元** (largest element) という。任意の $y \in A$ に対して $x \preceq y$ のとき $x$ を $A$ の**最小元** (smallest element) という。

**命題 4.2.7.** 順序集合の最大元は極大元である。また最小元は極小元である。(一般に逆は成り立たない。)

**証明.** $a$ を順序集合 $(A, \preceq)$ の最大元とする。$b \in A$ に対して $a \preceq b$ とする。$a$ は $A$ の最大元なので $b \preceq a$ である。よって順序の定義から $a = b$ である。したがって $a$ は $A$ の極大元である。
最小限についても同様である。 □

**命題 4.2.8.** 順序集合に最大元が存在すれば、それは唯一つに定まる。(最大元が存在するとは限らない。)また最小元も存在すれば唯一つに定まる。

**証明.** $a, b$ を順序集合 $(A, \preceq)$ の最大元とする。$a$ は $A$ の最大元なので $b \preceq a$ である。$b$ は $A$ の最大元なので $a \preceq b$ である。よって順序の定義から $a = b$ である。
最小元についても同様である。 □

**例 4.2.9.** 例 4.1.2 の順序集合 $(2^A, \subset)$ を考える。$2^A$ には最大元 $A$ と最小元 $\emptyset$ が存在する。

**例 4.2.10.** 例 4.1.2 の順序集合 $(2^A, \subset)$ を考え、その順序部分集合 $B = 2^A - \{\emptyset, A\}$ を考える。ここで $|A| > 1$ と仮定する。このとき $B$ には最大元も最小元も存在しない。任意の $a \in A$ に対して $\{a\}$ は $B$ の極小元であり、$A - \{a\}$ は $B$ の極大元である。

**命題 4.2.11.** 全順序集合の極大元 (極小元) は最大元 (最小元) である。

**証明.** 極大元についてのみ示せば、極小元についても同様である。$A$ を全順序集合とし $a \in A$ をその極大元とする。$A$ が全順序集合なので、任意の $b \in A$ に対して $b \preceq a$ または $a \preceq b$ が成り立つが、$a$ が極大であることから $b \preceq a$ である。よって $a$ は最大元である。 □

**定義 4.2.12** (整列順序)**.** 集合 $A$ 上の順序 $\preceq$ が**整列順序** (well order) であるとは任意の空でない部分集合に最小元が存在することである。整列順序によって順序が与えられた順序集合を**整列集合** (well ordered set) という。

**例 4.2.13.** $\mathbb{N}$ や $\{-1, 0\} \cup \mathbb{N}$ は通常の $\leq$ という順序で整列集合である。しかし $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ は整列集合ではない。

**問 4.2.14.** $\{r \in \mathbb{Q} \mid r \geq 0\}$ は整列集合ではないことを示せ。

**例 4.2.15.** $A = \{1, 2\}$ としてべき集合 $2^A$ を考える。このとき $B = \{\{1\}, \{2\}\} \subset 2^A$ を考えれば $B$ に最小元はないので $2^A$ は整列集合ではない。

**命題 4.2.16.** 整列集合は全順序集合である。

**証明.** (対偶を示す。) $A$ を全順序集合ではない順序集合とする。このとき $a \preceq b$ でも $b \preceq a$ でもない $a, b \in A$ が存在する。例 4.2.15 と同じように $B = \{a, b\}$ を考えれば $B$ には最小元は存在しない。したがって $A$ は整列集合ではない。 □

$B = [a_1, a_2, \cdots]$ を順序集合 $A$ の元の列とする。(同じ元を含んでもよい。よって $B$ は部分集合ということではないので異なる記号を用いている。) $B$ が**単調減少列** (**単調増加列**) であるとは $a_{i+1} \preceq a_i$ ($a_i \preceq a_{i+1}$) が任意の $i \in \mathbb{N}$ について成り立つこととする。また $B$ が**狭義単調減少列** (**狭義単調増加列**) であるとは減少列 (増加列) であって $a_i \neq a_{i+1}$ が任意の $i \in \mathbb{N}$ について成り立つこととする。

**命題 4.2.17.** 整列集合には無限の狭義単調減少列は存在しない。

**証明.** 整列集合 $A$ に無限の狭義単調減少列 $B = [a_1, a_2, \cdots]$ が存在したとする。このとき $A$ の部分集合 $C = \{a_1, a_2, \cdots\}$ を考える。$A$ が整列集合だから $C$ には最小元が存在する。$a \in C$ を $C$ の最小元とする。$a \in C$ だから、ある $n \in \mathbb{N}$ があって $a = a_n$ である。しかし $a_{n+1} \preceq a_n = a$, $a_{n+1} \neq a$ となり、$a$ が最小元であることに矛盾する。よって $A$ に無限の狭義単調減少列は存在しない。 □

**例 4.2.18** (辞書式順序)**.** $X = \mathbb{N} \times \mathbb{N}$ に次のように順序を定める。

(1) $a_0 = a_1$ かつ $b_0 \leq b_1$ のとき $(a_0, b_0) \leq (a_1, b_1)$ である。

(2) $a_0 \neq a_1$ かつ $a_0 \leq a_1$ のとき $(a_0, b_0) \leq (a_1, b_1)$ である。

この順序は整列順序である。これを**辞書式順序** (lexicographic order) という。

やや分かりにくいと思うので具体的に書くと以下のようになる。$(a_0, b_0) \leq (a_1, b_1)$ かつ $(a_0, b_0) \neq (a_1, b_1)$ であることを簡単のために $<$ とかく。

$$(1,1) < (1,2) < (1,3) < \cdots < (2,1) < (2,2) < (2,3) < \cdots < (3,1) < \cdots$$

辞書の語順と似ていることも分かるだろう。

これが整列順序であることを示そう。$Y$ を $X$ の空でない部分集合とする。

$$Y_1 = \{a \in \mathbb{N} \mid \text{ある } b \in \mathbb{N} \text{ があって } (a,b) \in Y\}$$

とおく。言い換えれば、写像 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を $f(a,b) = a$ で定めて $Y_1 = f(Y)$ としているのである。$Y$ が空でないから $Y_1$ も空でない。$Y_1$ は $\mathbb{N}$ の部分集合で、$\mathbb{N}$ は整列集合なので $Y_1$ には最小元 $a_1$ が存在する。

$$Y_2 = \{b \in \mathbb{N} \mid (a_1, b) \in Y\}$$

とおく。言い換えれば、写像 $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を $g(a,b) = b$ で定めて $Y_2 = g(f^{-1}(a_1))$ としているのである。$a_1$ の決め方から $Y_2$ は空でない $\mathbb{N}$ の部分集合で、したがって $Y_2$ は最小元 $b_1$ をもつ。このとき $a_1$, $b_1$ の決め方から $(a_1, b_1)$ は $Y$ の最小元である。

**例 4.2.19.** 例 4.2.18 で $\mathbb{N} \times \mathbb{N}$ に辞書式順序を定めたが、これは次のように一般化される。$(A, \leq), (B \leq)$ をそれぞれ整列順序とする。このとき例 4.2.18 と同様に $A \times B$ に順序を定めれば、これも整列順序となる。この順序も**辞書式順序**と呼ばれる。これによって $\mathbb{N}^n$ なども辞書式順序で整列集合と見ることができる。

順序集合 $(A, \preceq)$ の部分集合 $B$ に対して $x \in A$ が $y \preceq x$ $(\forall y \in B)$ を満たすとき、$x$ を $B$ の**上界** (upper bound) という[1]。$B$ の上界が存在するとき $B$ は**上に有界である** (bounded above) という。$B$ の上界全体の集合に最小元が存在するとき、それを $B$ の **上限** (supremum) という[2]。

**例 4.2.20.** 順序集合 $(\mathbb{R} \leq)$ を考える。$B = (0,1)$ (開区間) とすれば、例えば 2 は $B$ の上界であり、よって $B$ は上に有界である。

**定義 4.2.21** (帰納的順序)**.** 集合 $A$ 上の順序 $\preceq$ が**帰納的順序** (inductive order) であるとは $A$ の任意の空でない全順序部分集合が上に有界であることをいう。このとき $A$ を**帰納的順序集合** (inductively ordered set) という。

**命題 4.2.22.** 順序集合 $A$ が最大元をもてば、$A$ は帰納的順序集合である。

**証明**. 最大元は任意の部分集合の上界であるから、任意の部分集合は上に有界である。 □

**例 4.2.23.** $\mathbb{R}$ の開区間 $A = (0,1)$ に自然な順序を考える。$A$ は帰納的ではない。なぜならば $A$ 自身は $A$ の全順序部分集合であるがそれは上界をもたない。

帰納的順序集合は後に学ぶツォルンの補題に現れる。

## 4.3 数学的帰納法と超限帰納法

数学的帰納法の通常の形は以下の通りである。

自然数 $n$ に関する命題は

(1) 1 のとき正しい。

(2) $n$ より小さいすべての自然数に対して正しければ $n$ についても正しい。

が成り立てば、任意の $n$ に対しても正しい。(2) は

(2') $n-1$ に対して正しければ $n$ についても正しい。

という形で考えられることもある。

これは整列集合に一般化される。すなわち $A$ を整列集合とするとき $a \in A$ に関する命題は

(1) $A$ の最小元に対して正しい。

[1] $x \in B$ でなくてもよいことに注意しておく。

[2] **下界** (lower bound)、**下に有界** (bounded below)、**下限** (infimum) も同様に定義されるが、この講義では使わない。

(2) この順序に関して $a$ より小さいすべて元に対して正しければ $a$ についても正しい。

が成り立つとき、任意の $a$ に対しても正しい。これは整列集合には無限の狭義単調減少列が存在しないことによる。すなわち $a \in A$ を決めると、狭義単調減少列は有限回で最小元に達する。したがって命題は有限回の手続きで証明されることになる。数学的帰納法を整列集合に一般化したものを**超限帰納法**という。

**例 4.3.1.** $\mathbb{N} \times \mathbb{N}$ に例 4.2.18 の整列順序を考える。二つの自然数の組 $(a, b)$ に関する命題は

(1) $\mathbb{N} \times \mathbb{N}$ の最小元 $(a, b) = (1, 1)$ で正しい。

(2) $(a_0, b_0) \leq (a, b)$ かつ $(a_0, b_0) \neq (a, b)$ である任意の $(a_0, b_0)$ で正しければ $(a, b)$ で正しい。

が成り立てば、任意の $(a, b)$ で正しい。この形の帰納法を**二重帰納法**ともいう。

考える順序集合が整列集合ではない場合、例えば通常の順序を考えた実数体 $\mathbb{R}$ など、では数学的帰納法や超限帰納法は使えない。

## 4.4 同値関係と類別

**定義 4.4.1** (同値関係)**.** 集合 $A$ 上の関係 $\sim$ が**同値関係**であるとは、以下の条件を満たすこととする。

(1) [**反射律**] 任意の $x \in A$ に対して $x \sim x$

(2) [**対称律**] $x \sim y$ ならば $y \sim x$

(3) [**推移律**] $x \sim y,\ y \sim z$ ならば $x \sim z$

数学においては (数学以外でもそうであると思うが) 色々な意味で「同じである」という概念を用いる。例えば分数 $1/2$ と $3/6$ は同じ数であるが、明らかにその表記は異なる。他にも例えば合同な二つの三角形はある意味では「同じ」と言える。しかし、同じと言う概念をあまり勝手に使うと感覚的に理解しがたいことになる。同値関係は「同じ」という概念を数学的に定式化したものと考えられる。主張していることは

(1) 勝手な要素は自分自身と「同じ」である。

(2) $x$ と $y$ が「同じ」ならば $y$ と $x$ も「同じ」である。

(3) $x$ と $y$ が「同じ」で $y$ と $z$ が「同じ」ならば $x$ と $z$ は「同じ」である。

という当たり前のことである。これが成り立たない場合に「同じ」という言葉を使うのが感覚的に受け入れがたいということも理解できるだろう。

**例 4.4.2.** 例 4.1.3, $\mathbb{Z}^\sharp \times \mathbb{Z}$ 上の関係 $\sim$ は同値関係である。($\mathbb{Z}^\sharp = Z - \{0\}$ である。) これを示そう。

$$\sim = \{((m, a), (n, b)) \in (\mathbb{Z}^\sharp \times \mathbb{Z}) \times (\mathbb{Z}^\sharp \times \mathbb{Z}) \mid mb = na\}$$

であった。

(1) 任意の $(m, a) \in \mathbb{Z}^\sharp \times \mathbb{Z}$ に対して $ma = ma$ は成立するので $(m, a) \sim (m, a)$ である。

(2) $(m, a) \sim (n, b)$ とする。このとき $mb = na$ であるから $na = mb$ である。よって $(n, b) \sim (m, a)$ である。

(3) $(m, a) \sim (n, b),\ (n, b) \sim (\ell, c)$ とする。このとき $mb = na,\ nc = \ell b$ である。よって $mnc = m\ell b = \ell na$ である。ここで $n \in \mathbb{Z}^\sharp$ より $n \neq 0$ なので $mc = \ell a$ が成り立ち $(m, a) \sim (\ell, c)$ である。

以上より $\sim$ は同値関係である。

$\sim$ を集合 $A$ 上の同値関係とする。$x \in A$ に対して

$$C_x = \{y \in A \mid x \sim y\}$$

とおいて、これを $x$ を含む ($\sim$ に関する) **同値類**と呼ぶ。すなわち $C_x$ は $\sim$ に関して $x$ と「同じ」もの全体の集合である。このとき次が成り立つ。

**定理 4.4.3.** $\sim$ を集合 $A$ 上の同値関係とし、$C_x$ を $x \in A$ を含む同値類とする。このとき次が成り立つ。

(1) 任意の $x \in A$ に対して $x \in C_x$

(2) $x, y \in A$ に対して $y \in C_x$ ならば $C_x = C_y$

(3) $x, y \in A$ に対して $C_x \cap C_y \neq \emptyset$ ならば $C_x = C_y$

(4) $x, y \in A$ に対して $C_x \neq C_y$ ならば $C_x \cap C_y = \emptyset$

**証明**. (1) は反射律より明らか。

(2) $y \in C_x$ と仮定する。定義より $x \sim y$ である。また対称律より $y \sim x$ である。
$z \in C_x$ とする。このとき $x \sim z$ である。よって $y \sim x,\ x \sim z$ となり、推移律より $y \sim z$ であり $z \in C_y$ である。したがって $C_x \subset C_y$ である。
$z \in C_y$ とする。このとき $y \sim z$ である。$x \sim y,\ y \sim z$ であるから推移律により $x \sim z$ である。よって $z \in C_x$ であり $C_y \subset C_x$ が成り立つ。
以上より $C_x = C_y$ である。

(3) $C_x \cap C_y \neq \emptyset$ なので $z \in C_x \cap C_y$ とする。このとき $z \in C_x$ なので (2) より $C_x = C_z$ であり、同様に $z \in C_y$ より $C_y = C_z$ である。よって $C_x = C_y$ である。

(4) は (3) の対偶である。 □

**定理 4.4.4.** $\sim$ を集合 $A$ 上の同値関係とし、$C_x$ を $x \in A$ を含む同値類とする。このとき $x, y \in A$ に対して次の条件は同値である。

(1) $x \sim y$

(2) $y \in C_x$

(3) $x \in C_y$

(4) $C_x = C_y$

**証明**. (1) $\Rightarrow$ (2). $x \sim y$ とする。このとき $C_x$ の定義から $y \in C_x$ である。
(2) $\Rightarrow$ (3). $y \in C_x$ とする。$x \sim y$ である。対称律から $y \sim x$ となり $x \in C_y$ である。
(3) $\Rightarrow$ (4). $x \in C_y$ とする。定理 4.4.3 (1) より $x \in C_x$ でもあるから $x \in C_x \cap C_y$ となり $C_x \cap C_y \neq \emptyset$ である。定理 4.4.3 (3) より $C_x = C_y$ である。
(4) $\Rightarrow$ (1). $C_x = C_y$ とする。$y \in C_y = C_x$ であるから $x \sim y$ である。 □

定理 4.4.3 より $A$ の異なる同値類の全体を $\{C_\lambda \mid \lambda \in \Lambda\}$ とおくと

$$A = \bigcup_{\lambda \in \Lambda} C_\lambda, \quad \lambda \neq \mu \text{ ならば } C_\lambda \cap C_\mu = \emptyset$$

となる。これを $A$ の同値関係 $\sim$ による**類別**という[3]。各同値類 $C_\lambda$ から一つずつ元 $a_\lambda$ を選ぶとき $a_\lambda$ を $C_\lambda$ の**代表元**という。また集合 $\{a_\lambda \mid \lambda \in \Lambda\}$ をこの類別の**完全代表系**という。

**例 4.4.5.** 想像しやすい例を見る。あるクラスの学生の集合を $A$ とする。クラスの班分けを考える。ただしメンバーのいない班はないものとし、また複数の班に所属する学生もいないものとする。このとき「同じ班に属する」という $A$ 上の関係 $\sim$ は同値関係となる。学生 $a \in A$ に対して、$a$ の属する同値類 $C_a$ は、$a$ の属する班のメンバーの集合である。クラスを班ごとに分けることが類別である。また班の集合が割った集合 $A/\sim$ となる。各班から班長 (代表者) を選ぶとき、その代表者を集めた集合が完全代表系である。見やすくまとめると以下のようになる。

| 集合 $A$ | クラスの学生 |
|---|---|
| $a$ を含む同値類 | $a$ の属する班 (班のメンバーからなる学生の集合) |
| 類別 | 班分け |
| 完全代表系 | 班長の集合 (学生の集合) |
| 割った集合 $A/\sim$ | 班の集合 (学生の集合を要素とする集合) |

学生 $a$ と $b$ が同じ班に属しているとき、「$a$ の属する班」と「$b$ の属する班」は同一のものであるが呼び方が違い、混乱が起きやすい。完全代表系と割った集合の間には自然な全単射があるが、考えているものは異なる。

[3] あとで説明する商集合を類別としている本などもある。厳密にはその方が正しいかも知れないが、ここでは「部分集合の和集合に書く」ことを類別としておく。

**例 4.4.6.** 例 4.1.3 の同値関係 $\sim$ は実はよく知られたものである。それは $(m,a)$ を含む同値類を $a/m$ と表すと分かる。

$$a/m = b/n \iff (m,a) \sim (n,b) \iff mb = na$$

となっているのである。このとき $a/m$ を有理数と考える。$m \in \mathbb{Z}^\times$ となっているので分母が 0 にならないことにも注意しておく。$a/m$ は分数として $a/m = b/n$ となる $(n,b)$ の全体である。すなわち

$$C_{(m,a)} = \{(n,b) \mid mb = na\} = \{(n,b) \mid a/m = b/n\}$$

である。有理数は既約分数として一意的に書けるので $C_{(m,a)}$ の代表元として、例えば $a/m$ が既約分数であるものを取ることができる。ただし 0 の既約分数表示は $(1,0)$ としておく。したがって既約分数の全体がこの同値関係による類別の完全代表系である[4]。

**注意.** 一般に同値類の代表元の取り方は一意的ではない。この例では既約分数を代表元に取ったが、他の代表元をとっても構わず、その場合には完全代表系も違うものになる。

例 4.4.6 をもう少し考える。$(m,a) \sim (n,b)$ であるとき、有理数としては $a/m = b/n$ であるが $\mathbb{Z}^\sharp \times \mathbb{Z}$ では $(m,a) = (n,b)$ という訳ではない。(ここでは例 4.4.6 とは違い、$a/m$ は同値類ではなく有理数を表すものとする。) 写像 $f : \mathbb{Z}^\sharp \times \mathbb{Z} \to \mathbb{Q}$ $((m,a) \mapsto a/m)$ を定めることは出来るがこれは全単射ではない。同値類全体の集合 $\{C_{(m,a)} \mid (m,a) \in \mathbb{Z}^\sharp \times \mathbb{Z}\}$ を考えれば、写像 $g : \{C_{(m,a)} \mid (m,a) \in \mathbb{Z}^\sharp \times \mathbb{Z}\} \to \mathbb{Q}$ $(C_{(m,a)} \mapsto a/m)$ が矛盾なく定義でき (well-defined) かつ全単射であることを示そう。

$C_{(m,a)} = C_{(n,b)}$ であるならば $(m,a) \sim (n,b)$ であるから $a/m = b/n$ である。したがって $g(C_{(m,a)}) = a/m$ は定まり、写像は矛盾なく定義できる。

任意の有理数 $a/m$ $(a, m \in \mathbb{Z},\ m \neq 0)$ に対して、$(m,a) \in \mathbb{Z}^\sharp \times \mathbb{Z}$ で $g(C_{(m,a)}) = a/m$ である。よって $g$ は全射である。

$g(C_{(m,a)}) = g(C_{(n,b)})$ とすると $a/m = b/n$ であるから $mb = na$、すなわち $(m,a) \sim (n,b)$ であり $C_{(m,a)} = C_{(n,b)}$ が成り立つ。よって $g$ は単射である。

以上より $g$ は矛盾なく定義でき、かつ全単射であることが示された。

この例では $\mathbb{Z}^\sharp \times \mathbb{Z}$ 自身は $\mathbb{Q}$ との間に全単射はないが、その同値類の全体は $\mathbb{Q}$ との間に全単射がある。すなわち一つの同値類を一つのものと見ることが有効である。これは数学では多く見られる方法である。一般に集合 $A$ の上に同値関係 $\sim$ が定義されているとき、その同値類全体の集合を $A/\sim$ と書き、**集合 $A$ を同値関係 $\sim$ で割った集合**、または集合 $A$ の同値関係 $\sim$ による**商集合**という。先の例では $(\mathbb{Z}^\sharp \times \mathbb{Z})/\sim$ と $\mathbb{Q}$ の間に全単射があったのである。

**例 4.4.7.** 2 次元実ベクトル空間 $V = \mathbb{R}^2 = \{(x,y) \in x, y \in \mathbb{R}\}$ とその部分空間 $W = \{(0,y) \mid y \in \mathbb{R}\}$ を考える (定義は線形代数のテキストなどを見ること)。$\boldsymbol{v}, \boldsymbol{v}' \in V$ に対して $\boldsymbol{v} \sim \boldsymbol{v}'$ であることを $\boldsymbol{v} - \boldsymbol{v}' \in W$ であることで定めれば、この関係は $V$ 上の同値関係となることが分かる。言い換えれば $\boldsymbol{v} \sim \boldsymbol{v}'$ であることは、その $x$-成分が一致することである。したがって $\boldsymbol{v}_0 = (x_0, y_0)$ を含む同値類は $\{(x_0, y) \mid y \in \mathbb{R}\}$ となる。これを $\boldsymbol{v}_0 + W$ と表すことにする。この類別の完全代表系として、例えば $\{(x,0) \mid x \in \mathbb{R}\}$ や $\{(x,1) \mid x \in \mathbb{R}\}$ などをとることができる。類別は $\bigcup_{x \in \mathbb{R}} ((x,0) + W)$ となる。

この同値関係で割ったものに自然に加法とスカラー倍が定義され、またベクトル空間になることが確認できる (自明ではないので、次節 (4.4.1) の内容を参考に自分で確認することを勧める)。これを**商空間**といい $V/W$ と表す。(この例の内容は一般のベクトル空間とその部分空間について成り立つ。)

### 4.4.1 整数の合同

$n \in \mathbb{N}$ を一つ固定する。$a, b \in \mathbb{Z}$ に対して

$$a \equiv b \pmod{n} \iff \text{ある } \ell \in \mathbb{Z} \text{ があって } a - b = n\ell$$

という関係を定義する。この関係は同値関係である。

**問 4.4.8.** 上の関係が同値関係であることを示せ。

$a \in \mathbb{Z}$ に対して、この関係による $a$ を含む同値類は $\{a + n\ell \mid \ell \in \mathbb{Z}\}$ と書くことができる。これを $a + n\mathbb{Z}$ と書き $n$ を法とする $a$ を含む**剰余類**という。特に $0 + n\mathbb{Z}$ は単に $n\mathbb{Z}$ とも書かれる。任意の剰余類 $a + n\mathbb{Z}$ に対して、その代表元 $b$ を $0 \leq b < n$ の範囲で取ることができることは明らかだろう。また $0 \leq a < b < n$

[4] 厳密にはこれによって有理数を定義する。有理数との対応を見ることは好ましいことは言えないかも知れないが、あくまでも例として理解して欲しい。

ならば $a+n\mathbb{Z} \neq b+n\mathbb{Z}$ であることも明らかである。したがって $\{0+n\mathbb{Z},\ 1+n\mathbb{Z}, \cdots, (n-1)+n\mathbb{Z}\}$ が同値類のすべてである。この集合を $\mathbb{Z}/n\mathbb{Z}$ と書く。

$\mathbb{Z}/n\mathbb{Z}$ に二項演算 "+" を次のように定義しよう。

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$$

二項演算は写像 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ であるから、これが矛盾なく定義されていることを示そう。$(a+b)+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ は問題ないが、演算が代表元の取り方に依存しないことを示す必要がある。すなわち $a+n\mathbb{Z} = a'+n\mathbb{Z}$, $b+n\mathbb{Z} = b'+n\mathbb{Z}$ であるときに $(a+b)+n\mathbb{Z} = (a'+b')+n\mathbb{Z}$ でなければならない。

$a+n\mathbb{Z} = a'+n\mathbb{Z}$, $b+n\mathbb{Z} = b'+n\mathbb{Z}$ と仮定する。これは、ある $\ell, m \in \mathbb{Z}$ があって $a-a' = n\ell$, $b-b' = nm$ と書けるということである。このとき

$$(a+b)-(a'+b') = (a-a')+(b-b') = n(\ell+m)$$

となるから $(a+b)+n\mathbb{Z} = (a'+b')+n\mathbb{Z}$ である。よって、この演算は矛盾なく定義できる。

**問 4.4.9.** (1) $\mathbb{Z}/n\mathbb{Z}$ に二項演算 "−" を $(a+n\mathbb{Z})-(b+n\mathbb{Z}) = (a-b)+n\mathbb{Z}$ で矛盾なく定義できることを示せ。

(2) $\mathbb{Z}/n\mathbb{Z}$ に二項演算 "×" を $(a+n\mathbb{Z})\times(b+n\mathbb{Z}) = ab+n\mathbb{Z}$ で矛盾なく定義できることを示せ。

(3) 上で定義した $\mathbb{Z}/n\mathbb{Z}$ の加法と乗法は交換法則、結合法則を満たすことを示せ。また減法は一般には交換法則、結合法則を満たさないことを示せ。

## 4.5 演習問題

(1) $X = \{1,2,3,4\}$ とする。

(a) $\preceq = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,4),(3,3),(3,4),(4,4)\}$ は $X$ 上の順序関係であることを確認せよ。この順序は全順序かどうかを判定せよ。また最大元、最小元、極大元、極小元をそれぞれ求めよ。

(b) $\preceq = \{(1,1),(1,2),(2,1),(2,2),(3,3),(3,4),(4,3),(4,4)\}$ は $X$ 上の同値関係であることを確認せよ。またこの同値関係による類別を求めよ。

(2) $\mathbb{R}$ の元を成分に持つ $n$ 次正方行列の全体を $M_n(\mathbb{R})$ と書く。$A, B \in M_n(\mathbb{R})$ に対して、関係 $A \sim B$ を「ある正則行列 $P$ があって $B = P^{-1}AP$ となる」ということで定義する。このとき $\sim$ は同値関係であることを示せ。

(3) (2) の同値関係による同値類の集合 $M_n(\mathbb{R})/\sim$ を考える。$A \in M_n(\mathbb{R})$ を含む同値類を $C_A$ と書くことにする。このとき $\det : M_n(\mathbb{R})/\sim \to \mathbb{R}$ $(\det(C_A) = \det A)$ が矛盾なく定義できることを説明せよ。ただし $\det A$ は $A$ の行列式である。

(4) $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ を $f(a+n\mathbb{Z}) = a+m\mathbb{Z}$ で定義したい。$f$ が矛盾なく定義されるための必要十分条件を求めよ。

(5) $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R} = \{(a,b) \mid a,b \in \mathbb{R}\}$ を考え、$A = \mathbb{R}^2 - \{(0,0)\}$ とする。$A$ に

$$(a,b) \sim (c,d) \iff ad = bc$$

で関係 $\sim$ を定める。$\sim$ は同値関係であり、その同値類の完全代表系として座標平面上の単位円 (半径 1 の円) 上の点 $(a,b)$ のうち $a > 0$ であるもの、および $(a,b) = (0,1)$ からなる集合をとることができる。これを示せ。(この同値類全体の集合を $P^1(\mathbb{R})$ と書いて**射影空間**という。)

# Chapter 5

# 難しいこと

## 5.1 集合の濃度

集合 $S$ が有限集合である場合、$S$ に含まれる要素の数を $S$ の**濃度** (cardinality) という。すなわち、既に定義した記号で $|S|$ が $S$ の濃度である。無限集合に対しても濃度を考えよう。前の定義では、無限集合 $S$ に対してはすべて $|S| = \infty$ と書いた。すべての無限は同じであろうか。これを考えるために、二つの集合に対して濃度が大きい、小さいという概念を定義する。

簡単のために二つの有限集合 $A, B$ を考える。$A$ と $B$ から同時に一つずつ元を取っていき、先に元がなくなった方が濃度は小さいといえる。例えば $A$ が先になくなったとしよう。このとき $A$ の元 $a$ に対して、$a$ と同時に取った $B$ の元 $b_a$ を対応させれば写像 $f : A \to B$ が得られる。また一つの $f(a)$ に対して $a$ と異なる $c \in A$ で $f(c) = f(a)$ となることはないからこの写像は単射である。一般に単射 $f : A \to B$ が存在するとき $A$ の濃度は $B$ の濃度以下である。これを無限集合に対しても適用する。この節では無限集合 $S$ に対して、その濃度を $|A|$ で表すが $|A| = \infty$ という記号は用いないで、無限を区別することにする。

**定義 5.1.1.** 二つの集合 $A$, $B$ に対して単射 $f : A \to B$ が存在するとき $|A| \leq |B|$ と定義する。また $|A| \leq |B|$ であって $|B| \leq |A|$ でないとき $|A| < |B|$ と表す。
全単射 $f : A \to B$ が存在するとき $|A| = |B|$ と定義する。
このようなときに集合の**濃度**が大きい、小さい、等しいなどということにする。

二つの有限集合 $A, B$ に対して $A \subsetneq B$ であるならば $|A| < |B|$ であることは感覚的に理解できるであろう。では無限集合ではどうだろうか。$\mathbb{N}$ を自然数全体の集合として $2\mathbb{N}$ を偶数である自然数全体の集合とする。このとき $2\mathbb{N} \subsetneq \mathbb{N}$ である。しかし写像 $f : \mathbb{N} \to 2\mathbb{N}$ を $f(a) = 2a$ で定めれば、これは全単射である。よって $|\mathbb{N}| = |2\mathbb{N}|$ が成り立つ。したがって無限集合に対しては $A \subsetneq B$ であっても $|A| < |B|$ とは限らないことになる。

**例 5.1.2.** $a, b \in \mathbb{R}$, $a < b$ に対して開区間 $I_{a,b} = (a, b)$ を考える。$a < b$, $c < d$ に対して $|I_{a,b}| = |I_{c,d}|$ である。実際 $f : I_{a,b} \to I_{c,d}$ を

$$f(x) = \frac{c-d}{a-b}x + \frac{ad-bc}{a-b}$$

で定めれば、これは全単射である。

**例 5.1.3.** $|I_{-1,1}| = |\mathbb{R}|$ である。実際 $f : I_{-1,1} \to \mathbb{R}$ を

$$f(x) = \frac{x}{1-x^2}$$

で定めれば、これは全単射である。前の例と合わせると、任意の開区間は $\mathbb{R}$ と同じ濃度をもつ。

集合の濃度に関して

- 任意の集合 $A$ に対して $|A| \leq |A|$ (恒等写像は単射だから)
- $|A| \leq |B|$ かつ $|B| \leq |C|$ ならば $|A| \leq |C|$ (単射の合成は単射だから)

が成り立つ。これは順序の定義の二つの条件 (の類似) であり、残りの半対称律に相当する条件

- $|A| \leq |B|$ かつ $|B| \leq |A|$ ならば $|A| = |B|$

も次のように成り立つ。

**定理 5.1.4** (Bernstein の定理)**.** $|A| \leq |B|$ かつ $|B| \leq |A|$ のとき $|A| = |B|$ である。すなわち二つの単射 $f : A \to B$ と $g : B \to A$ が存在するとき、全単射 $h : A \to B$ が存在する。

**証明**. $A_0 = A$, $B_0 = B$ とおいて、帰納的に

$$A_{n+1} = g(B_n), \quad B_{n+1} = f(A_n)$$

とする。また

$$A_\infty = \bigcap_{n=0}^{\infty} A_n, \quad B_\infty = \bigcap_{n=0}^{\infty} B_n$$

とする。まず

$$A = A_0 \supset A_1 \supset \dots, \quad B = B_0 \supset B_1 \supset \dots$$

となることを示そう。「$A_n \supset A_{n+1}$ かつ $B_n \supset B_{n+1}$ である」ことを $n$ に関する数学的帰納法で示す。$n = 0$ のときは明らかである。「$A_n \supset A_{n+1}$ かつ $B_n \supset B_{n+1}$ である」とする。このとき $B_{n+1} = f(A_n) \supset f(A_{n+1}) = B_{n+2}$ となる。$A_{n+1} = A_{n+2}$ も同様である。

したがって

$$A = A_\infty \cup (A_0 - A_1) \cup (A_1 - A_2) \cup \cdots, \quad B = B_\infty \cup (B_0 - B_1) \cup (B_1 - B_2) \cup \cdots$$

は共通部分のない和集合である。

$g : B \to A$ は単射であるから $g_0 : B \to g(B) = A_1$ を $g_0(b) = g(b)$ で定めればこれは全単射である。よって $a \in A_1$ に対して $g_0^{-1}(a) \in B$ が定義される。

$f(A_\infty) = B_\infty$ を示す。まず、任意の $n \geq 0$ に対して $A_\infty \subset A_n$ であるから $f(A_\infty) \subset f(A_n) = B_{n+1}$ であり、$f(A_\infty) \subset f(A_0) = B_1 \subset B_0$ でもあるから、$f(A_\infty) \subset \bigcap_{n=0}^{\infty} B_n = B_\infty$ である。$b \in B_\infty$ とする。任意の $n \geq 0$ について $b \in B_n$ となる。$n \geq 1$ に対して $b \in B_n = f(A_{n-1})$ なので、ある $a_{n-1} \in A_{n-1}$ が存在して $b = f(a_{n-1})$ となる。しかし $f$ が単射であることから $a_0 = a_1 = \cdots$ となる。これを $a$ とおくと、$a \in \bigcap_{n=0}^{\infty} A_n = A_\infty$ となる。したがって $b = f(a) \in f(A_\infty)$ となり $B_\infty \subset f(A_\infty)$ となる。

$h : A \to B$ を

$$h(x) = \begin{cases} f(x) & \text{ある非負整数 } n \text{ に対して } x \in A_{2n} - A_{2n+1} \text{ のとき} \\ g_0^{-1}(x) & \text{ある非負整数 } n \text{ に対して } x \in A_{2n+1} - A_{2n+2} \text{ のとき} \\ f(x) & x \in A_\infty \text{ のとき} \end{cases}$$

と定める。このとき

$$\begin{aligned} f_n' &: A_{2n} - A_{2n+1} \to B_{2n+1} - B_{2n+2} \quad (f_n'(a) = f(a)) \\ g_n' &: A_{2n+1} - A_{2n+2} \to B_{2n} - B_{2n+1} \quad (g_n'(a) = g_0^{-1}(a)) \\ f' &: A_\infty \to B_\infty \quad (f'(a) = f(a)) \end{aligned}$$

がすべて全単射になることから $h$ は全単射となる。 □

**問 5.1.5.** 上の 3 つの写像が全単射であることを確認せよ。

**例 5.1.6.** 閉区間 $A = [-1, 1]$ と開区間 $B = (-1, 1)$ を考える。

$$f : A \to B \quad \left(f(x) = \frac{1}{2}x\right), \quad g : B \to A \quad (g(x) = x)$$

とすれば $f, g$ は共に単射であり、よって $|A| \leq |B|$ かつ $|A| \geq |B|$ となる。Bernstein の定理はこのとき $|A| = |B|$ であることを主張している。すなわち、全単射 $h : A \to B$ が存在することを意味している。実際にこの全単射を構成してみよう。

$A' = \{\pm 1/2^\ell \mid \ell \text{ は非負整数 }\}$ とおく。$h : A \to B$ を

$$h(x) = \begin{cases} x/2 & x \in A' \text{ のとき} \\ x & x \notin A' \text{ のとき} \end{cases}$$

で定める。すぐにわかるように $h|_{A'}(A') = A' - \{-1, 1\}$ であり、また $h|_{A'}$ は単射である。また $h|_{A-A'}$ が全単射であることは明らかである。よって $h$ は $A$ から $B = A - \{-1, 1\}$ への全単射となる。

**注意.** 全射 $A \to B$ が存在すれば $|A| \geq |B|$ のように思えるが、これは後で紹介する選択公理を用いなければ示すことができない (定理 5.2.1)。

任意の二つの集合 $A, B$ に対して $|A| < |B|$, $|A| = |B|$, $|A| > |B|$ のいずれかが成り立つように思われる。しかしこれも選択公理を用いなければ示すことができない (濃度の比較可能定理：定理 5.2.2)。

自然数全体の集合 $\mathbb{N}$ と同じ濃度をもつ集合を**可算無限集合**という。可算無限集合の濃度を $\aleph_0$ と書き**アレフゼロ**と読む。可算無限集合は無限集合の中で最も小さいものであるといえる。よって $\aleph_0$ は無限濃度のうちで最も小さいものである。可算無限集合と有限集合を合わせて**可算集合** (countable set) という。

**例 5.1.7.** 以下の集合はすべて可算無限集合である。「自然数全体の集合 $\mathbb{N}$」、「偶数全体の集合」、「奇数全体の集合」、「直積集合 $\mathbb{N} \times \mathbb{N}$」「整数全体の集合 $\mathbb{Z}$」、「有理数全体の集合 $\mathbb{Q}$」、「可算無限集合の無限部分集合」

可算集合でない無限集合は存在するのであろうか。以下の命題が可算集合でない無限集合の例を示している。

**命題 5.1.8.** $|\mathbb{N}| < |\mathbb{R}|$ が成り立つ。

実数全体の集合 $\mathbb{R}$ の濃度 $|\mathbb{R}|$ を**連続体濃度**といい $\aleph$ と表す (アレフと読む) 。「$|\mathbb{N}| < |S| < |\mathbb{R}|$ となるような集合 $S$ が存在するか 」という問題は**連続体仮説**と呼ばれ**数学的に証明できないことが証明されている**[1]。では無限集合の濃度は他にあるのだろうか。これには明快に答えることができて、無限集合の濃度はいくらでも存在する。

**命題 5.1.9.** 任意の集合 $A$ に対して、そのべき集合 $2^A$ を考えれば $|A| < |2^A|$ が成り立つ。特に $A$ として無限集合 (例えば可算無限集合) をとれば、無限濃度の列

$$|A| < |2^A| < |2^{(2^A)}| < \cdots$$

が得られる。

**証明.** $2^A$ は $A$ の部分集合全体の集合である。$f : A \to 2^A$ を $f(a) = \{a\}$ で定めればこれは単射であり、よって $|A| \leq |2^A|$ である。

$|A| = |2^A|$ と仮定する。このとき全単射 $f : A \to 2^A$ が存在する。

$$R := \{x \in A \mid x \notin f(x)\}$$

とおく。$R$ は $A$ の部分集合なので $R \in 2^A$ である。$f$ は全単射なので、ある $r \in A$ があって $f(r) = R$ である。ここで

- $r \notin R$ とすると $r \in f(r) = R$ で矛盾。
- $r \in R$ とすると $r \notin f(r) = R$ で矛盾。

よって、このような全単射は存在しない。 □

これを**対角線論法**という。$|\mathbb{N}| < |\mathbb{R}|$ もこれを使って証明される。$I = (0, 1)$ (開区間) として $|\mathbb{N}| < |I|$ を示そう。例 5.1.3 より $|I| = |\mathbb{R}|$ であるから、このことによって $|\mathbb{N}| < |\mathbb{R}|$ が示される。$I$ の任意の元 $a$ は $0.a_1a_2\cdots$ という無限小数として表すことができる[2]。$f : \mathbb{N} \to I$ が全単射であるとする。

$$\begin{aligned} f(1) &= 0.a_1^{(1)}a_2^{(1)}a_3^{(1)}\cdots \\ f(2) &= 0.a_1^{(2)}a_2^{(2)}a_3^{(2)}\cdots \\ f(3) &= 0.a_1^{(3)}a_2^{(3)}a_3^{(3)}\cdots \\ &\cdots \end{aligned}$$

と表すことにする。このとき、$b \in I$ を少数第 $i$ 位が $f(i)$ と異なるように作る。そうすれば $b$ は、どの $f(i)$ とも異なるので $f$ が全単射であることに矛盾する。これが対角線論法と呼ばれる理由も分かって頂けたであろうか。

さて集合の濃度にはいくらでも大きなものが存在し、濃度が一番大きな集合というものは存在しない。「集合すべての集合」というものが存在するとすれば、それは濃度が一番大きな集合となり、ラッセルのパラドックスと同様に矛盾が生じる。

以下のことは証明なしに結果だけ紹介しておく。(証明には以下に述べる選択公理を必要とするものもある。)

[1] 存在するとしても、存在しないとしても無矛盾な数学が構築でき、ほとんどの数学に影響を与えない。

[2] この議論では実数の無限少数教示の一意性が要求されるが、よく知られているように $1.000\cdots = 0.999\ldots$ である。これを避けるためには実数の有限表示 (有限桁で終わる表示、またはある桁から先がすべて 0 となる表示) を禁止すればよい。

**命題 5.1.10.** $A$ が有限集合で $B$ が無限集合であるとき $|A \cup B| = |B|$, $|A \times B| = |B|$ である。また $A$, $B$ ともに無限集合であるとき $|A \cup B| = \max\{|A|, |B|\}$, $|A \times B| = \max\{|A|, |B|\}$ である。すなわち、(有限個の集合の) 和集合や直積集合を作っても、濃度の大きな集合を作ることはできない。

## 5.2 選択公理、整列可能定理、ツォルンの補題

$\{A_1, A_2, \cdots, A_n\}$ を有限個の空でない集合の族とする。このとき各 $A_i$ から一つずつ元 $x_i$ を選ぶことはできる。有限とは限らない集合の族 $\{A_\lambda \mid \lambda \in \Lambda\}$ の場合はどうであろうか。実はこれは他の公理からは証明できないことが知られている。しかしこれは感覚的に正しいように思われる。そこで、これを公理として採用し**選択公理** (または**選出公理**) と呼ぶ。

**選択公理 (the axiom of choice).** 集合の族 $\{A_\lambda \mid \lambda \in \Lambda\}$ において、どの $A_\lambda$ も空でないとする。このとき各 $A_\lambda$ から一つずつ元 $x_\lambda$ を選ぶことができる。

これは次のように言い換えることもできる。

**選択公理 (the axiom of choice).** 集合の族 $\{A_\lambda \mid \lambda \in \Lambda\}$ において、どの $A_\lambda$ も空でないとする。このとき直積集合 $\Pi_{\lambda\in\Lambda} A_\lambda$ も空ではない。

数学の多くの部分で選択公理が利用されているが、選択公理を仮定しない数学もある。(実は写像のところで既に選択公理を利用しているところがあった。探してみるといいだろう。) 選択公理は以下の**ツォルンの補題**、**ツェルメロの整列可能定理**と同値であることが知られている。したがって選択公理を仮定している場合には、これらも成り立つとしてよい。

**ツォルンの補題 (Zorn's lemma).** 順序集合 $A$ が帰納的ならば $A$ に少なくとも一つの極大元が存在する。

**ツェルメロの整列可能定理 (Zermelo's well-ordering theorem).** 任意の集合 $A$ 上に整列順序が定義できる。

整列順序とは、任意の空でない部分集合に最小元が存在する、ということであった。例えば $\mathbb{R}$ は通常の順序で整列集合ではない。整列可能定理は、うまく順序を入れれば $\mathbb{R}$ も整列順序にできる、ということを主張している。これは明らかとは言えないだろう。

以下のことは選択公理を仮定して証明される。

**定理 5.2.1.** 全射 $f : A \to B$ が存在すれば $|A| \geq |B|$ である (単射 $B \to A$ が存在する)。

**証明.** 任意の $b \in B$ に対して $f^{-1}(b) \neq \emptyset$ である。各 $b \in B$ に対して $f^{-1}(b)$ から一つ元を取り、それを $g(b)$ とする (ここで選択公理を使っている)。このとき $g : B \to A$ は単射であり $|A| \geq |B|$ となる。 □

**定理 5.2.2.** [濃度の比較可能定理] 任意の二つの集合 $A$, $B$ に対して $|A| < |B|$, $|A| = |B|$, $|A| > |B|$ のいずれかが成り立つ。

**証明.** $A$, $B$ を集合とする。$A$ または $B$ が空集合ならば明らかなので $A$, $B$ ともに空ではないとする。$\mathcal{S} = \{(X, f) \mid X \subset A, f : X \to B \text{ は単射 }\}$ とおく。$\mathcal{S}$ に次のように順序を定める。$(X, f) \leq (Y, g)$ であるとは、$X \subset Y$ かつ $g|_X = f$ となることである。この順序によって $\mathcal{S}$ は帰納的順序集合となる (あとで示す)。したがってツォルンの補題から $\mathcal{S}$ は極大元 $(X_0, f_0)$ をもつ。

- $X_0 = A$ ならば $f_0 : A \to B$ は単射となり $|A| \leq |B|$ である。
- $f_0(X_0) = B$ とする。$b \in B$ を一つとり $f : A \to B$ を $f(a) = f_0(a)$ ($a \in X_0$ のとき)、$f(a) = b$ ($a \notin X_0$ のとき)、と定めれば $f$ は全射である。定理 5.2.1 より $|A| \geq |B|$ である。
- $X_0 \subsetneq A$, $f_0(X_0) \subsetneq B$ とする。$a_1 \in A - X_0$, $b_1 \in B - f(X_0)$ を選ぶことができる。このとき $X_1 = X_0 \cup \{a\}$ として、写像 $f_1 : X_1 \to B$ を $f_1(a) = f_0(a)$ ($a \in X_0$ のとき)、$f_1(a_1) = b_1$ と定めれば、$f_1$ は単射となり $(X_1, f_1) \in \mathcal{S}$, $(X_0, f_0) \leq (X_1, f_1)$ である。これは $(X_0, f_0)$ の極大性に反する。

したがって $|A| \leq |B|$ または $|A| \geq |B|$ が成り立ち、定理は証明される。 □

**$\mathcal{S}$ が帰納的であることの証明.** $\mathcal{T} = \{(X_\lambda, f_\lambda) \mid \lambda \in \Lambda\}$ を $\mathcal{S}$ の空でない全順序部分集合とする。$X = \bigcup_{\lambda\in\Lambda} X_\lambda$ とし、$f : X \to B$ を次のように定める。$x \in X$ とする。ある $\lambda \in \Lambda$ が存在して $x \in X_\lambda$ である。このとき $f(x) = f_\lambda(x)$ とする。$x \in X_\lambda$ となる $\lambda \in \Lambda$ は一意的でないので $f$ が定義されることを確認しなければならない。$x \in X_\lambda$ かつ $x \in X_\mu$ とする。$\mathcal{T}$ は全順序集合なので $(X_\lambda, f_\lambda) \leq (X_\mu, f_\mu)$ または $(X_\lambda, f_\lambda) \geq (X_\mu, f_\mu)$ である。$(X_\lambda, f_\lambda) \leq (X_\mu, f_\mu)$ とする。このとき $x \in X_\lambda \subset X_\mu$ であり $f_\mu|_{X_\lambda} = f_\lambda$ なの

で $f_\mu(x) = F_\mu|_{X_\lambda}(x) = f_\lambda(x)$ となる。$(X_\lambda, f_\lambda) \geq (X_\mu, f_\mu)$ のときも同様である。これで $f$ が $\lambda$ のとり方に依存しないことが分かる。

$(X, f) \in \mathcal{S}$ であることを示す。$f$ が単射であることを示せばよい。$x, y \in X$ に対して $f(x) = f(y)$ であるとする。ある $\lambda, \mu \in \Lambda$ に対して $x \in X_\lambda$, $y \in X_\mu$ である。$(X_\lambda, f_\lambda) \leq (X_\mu, f_\mu)$ とする。$f_\mu(x) = f_\lambda(x) = f(x) = f(y) = f_\mu(y)$ であり $f_\mu$ が単射であるから $x = y$ となる。$(X_\lambda, f_\lambda) \geq (X_\mu, f_\mu)$ のときも同様である。したがって $f$ は単射となり $(X, f) \in \mathcal{S}$ となる。

$(X, f) \in \mathcal{S}$ は $\mathcal{T}$ の上界である。したがって $\mathcal{S}$ が帰納的順序集合であることが分かる。 □

## 5.3 演習問題

(1) $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を $f(a, b) = 2^{a-1}(2b - 1)$ で定めると、これは全単射であることを示せ。

(2) $\mathbb{R}$ と $\mathbb{R} - \{0\}$ の間の全単射を構成せよ。

# 参考文献

[1] 入門 集合と位相, 竹之内修, 実教出版, 1971.

[2] 数学のロジックと集合論, 田中一之, 鈴木登志雄, 培風館, 2003.

[3] 無限集合 (数学ワンポイント双書 4), 森殻, 共立出版, 1976.

Akihide Hanaki (hanaki@shinshu-u.ac.jp)
2022/08/29