数学入門 AB 集合論と論理学

まえがき

このノートは, 日本大学理工学部数学科の 2012 年度, 2013 年度の 1 年次講義「数学入門 AB」の講義内容をまとめて, 加筆, 修正を加えたものである.

高校の数学と大学の数学での立場の違いとして, 「説明を受ける側」から「説明をする側」に変化することをあげておきたい. 大学の数学科に入学するにあたって, 「学校の先生」を進路として希望する学生は多い. とくに, 大学を卒業したあとに中学校や高校の先生となって, 「説明をする側」に立場がかわることになる. だから, 相手に正しく伝える技術が求められる.

高校までの数学の授業を受ける, とくにテストを受ける立場では, 少しくらいの表現の間違いは気にされず, 計算の結果のみを見てもらえることが多かっただろう. しかし, 大学の数学では, 表現の間違いが内容の間違い, 説明の間違いにつながることが多いため, 正しい表現で証明などを書くことが求められる. それは, 将来に学校の先生となったとき, 必ず必要になる能力でもある. 学校の先生にならないとしても, 相手に正しく説明する能力はどこでも必要である.

集合論を説明するなら, 最初に記号論理学をしっかりと学んで, 論理をきちんと身につけてから, 集合や写像の説明をした方が能率はよい. しかし, このノートではその方法をとらず, 最初に集合や写像の概念を説明して, 数学でよく使われる日本語の言い回しに慣れるようにした. そのために証明がまわりくどくなるところもあるが, はじめのうちは, 「証明を書くための国語」の練習を重視した. そして, 集合や写像の説明のあとに記号論理学に関する説明を加えた. そのため, 記号論理学がなぜ数学に必要となるのかがわかりやすくなっているのではないかと期待する[1].

また, このノートのもう一つの目標として, 「専門書を読むための準備をする」を考えている. 具体的には, 証明の一部を問題として本文中に加えている. 数学科の場合, 卒業論文を作成したり, 実験で一日中実験室にこもるということは, 比較的少ない. そのかわりに, 「卒業研究セミナー」が開講されることが多い. そこでは, 専門書などのテキストを決めて, 学生が先生の立場になって, 卒業研究の担当教員に数学を説明することがよく行われる. このセミナーでは,

[1]記号論理学は数学では是非とも持っていて欲しい知識であるが, 何のためにやっているかが見えにくいため, どのタイミングで勉強するのがよいのか悩むところである.

学生がその専門書を事前に読みこんでおいて, 内容を把握してから説明をするのが普通であり[2], その準備として, 専門書を読むことになるのだが, いろいろな理由で説明が省略されていることがとても多い[3]. 学生は説明が省略されているところもきちんと確認して, 必要に応じて説明を加えなければいけないのだが, 「説明が省略されているところを認識できる」ことが必要になってくる. そのために, このノートでは, 意図的に証明を省略して, 問題にまわしているところがある. これらの問題は解くだけではなく, 「こういう省略があったら, こうやって自分で確認しなければいけない」ということを認識して欲しい.

なお, 問題の解答については, 今後加筆する予定はない. 高校, 特に受験数学では「問題の解答を覚える」ことが数学の勉強だと思っている学生もみられるが, 数学の勉強で重要なことは, 「問題について考えること」である. すぐに答えがでないことを悲観してはいけないのである[4].

このノートはこれからまだ修正や加筆があると思われる. 誤植, 間違い等あれば, 著者の水野[5]に連絡して頂ければ幸いである.

このノートを読むにあたって

- 「定義」は覚えなければいけないものである.
- 定義から導くことができる重要な結果を「定理」という.
- 「例」は定義や定理を理解するために重要である.
- 「注意」は定義や定理で間違いやすいことなどを説明している. 番号のついていない「注意」はやや内容が高度なので, 最初は読み飛ばしてもよい.
- 本文中の「問題」は, 定義や定理を理解しているかを確認するための問題である. 全部に答えられるようになることが望ましい. 各章の章末にある演習問題は, 本文中の問題に比べて難易度が高めの問題である. 理解を深めるために考えてみるとよい.

説明はわかりやすく書いたつもりではあるが, さっと読んだだけでわかるような簡単なものではない. 予習として「定義」, 「定理とその証明」, 「例」を写経のように書き写しながら考えてみることをおすすめする. さらに余裕があれば, 本文中の問題についても考えてみるとよい.

---

[2]事前に準備せずに説明しようとすると, とてもたいへんなことになることが多い.

[3]省略されている内容は, 簡単だから, 書こうとすると長くなるから, **実は間違っているから**などである. このノートについても間違いがあるだろうから注意されたい.

[4]数独などのパズルゲームを解答をみながらやっても, 何もおもしろくはないだろうし, そのパズルゲームの腕があがるとも思えない. 数学も同様に考えれば, 解答をみながら考えても数学の能力があがるわけではないのである.

[5]mizuno atmark math.cst.nihon-u.ac.jp(ただし atmark は@にかえる)

目次

第 1 章

集合

この章では, 集合とは何かということを説明する. さらに, 数学を学ぶ上で必要となる論理学の知識や専門用語, 証明の書き方を説明する. 数学を説明する上で語学, とりわけ国語の知識は欠かすことができない. この章での証明は, 厳密さに気をつけるだけでなく, 日本語としておかしな表現がないように気をつけて書いた. 証明をきちんと書けることは数学を勉強する上で難しいところの一つである. まずは証明を真似してどのように書けば正しい表現となるかを理解して欲しい.

また, この章では, 「かつ」と「または」が入った論理をどのように取り扱えばよいかについて説明する. 「かつ」と「または」は, 高校の数学において混同して使われることが多いが, どちらを使っているのかをはっきり認識する必要がある[1]. 数学の証明を書くためには, 「誰が読んでも同じ意味になる」文章を書く必要があるので, この章では, 「かつ」と「または」に注意しながら読んで欲しい.

1.1. 集合とは何か？

数学は集合を用いて記述される. そこで, 数学を学ぶ上で欠かすことのできない集合を素朴に考えることにする.

定義 1.1 (集合)**.**
ある特定の性質をそなえた「もの」の集まりを**集合**という. 集合 A を構成する一つ一つの「もの」を集合 A の**元**, または**要素**という.

なお, 言葉の意味を定めることを**定義する**という.

例 1.1 (集合の書き方)**.**
集合は普通, アルファベットの大文字で書く. 集合は $\{\cdots\}$ の形で書く.

$$A := \{2, 3, 5, 7\} = \{10 \text{ 以下の素数 }\}.$$

[1] 二次方程式の解として, $x = 1, 3$ と書いたら, $x = 1$ または $x = 3$ と読むであろうが, 一次関数の値として $x = 1$, $y = 3$ と書いたら, $x = 1$ かつ $y = 3$ と読むこともできるであろう.

このとき, 集合 A の元は 2, 3, 5, 7 である. この集合の $=$ については後述する. とりあえずは, 集合が同じものだと思っていればよい. 同じ集合でも書き方, 表現の仕方はいろいろある.

$$\begin{aligned} B &:= \{10000 \text{ 以下の } 3 \text{ で割り切れる自然数 }\} \\ &= \{3, 6, 9, \ldots, 9996, 9999\} \\ &= \{3n : n = 1, 2, \ldots, 3333\}. \end{aligned}$$

厳密さを重視するなら $\{10000$ 以下の 3 で割り切れる自然数 $\}$ であるが, 書くのが面倒だと感じるであろう. $\{3n : n = 1, 2, \ldots, 3333\}$ のように, 変数を使った書き方や, 少し厳密さに欠けるが, 比較的意味がわかりやすい $\{3, 6, \ldots, 9996, 9999\}$ もよく使われる.

注意 1.1.

例 1.1 において, $:=$ は「左を右で**定義**する (決める)」の意味である. 高校までの等号 $=$ は「左と右が**等しい**」の意味と「左を右で**定義**する (決める)」の二つの意味を一緒に用いていた. しかし, これらは区別して使うべきである. そこで, このノートにおいては, $=$ を「左と右が**等しい**」の意味でのみ使うことにする.

例 1.2 (よく使う集合)**.**

次の集合はどの教科書, 専門書でも標準的に使われる.

- $\mathbb{N}$: 自然数全体の集合, すなわち正の整数全体の集合[2]
- $\mathbb{Z}$: 整数全体の集合
- $\mathbb{Q}$: 有理数全体の集合
- $\mathbb{R}$: 実数全体の集合
- $\mathbb{C}$: 複素数全体の集合
- $\emptyset$: 元が一つもない集合 (**空集合**という)
- $(a, b) = \{x : x \text{ は実数}, \ a < x < b\}$: 開区間という.
- $[a, b] = \{x : x \text{ は実数}, \ a \leq x \leq b\}$: 閉区間という.

定義 1.2.

a が集合 A の元であるとき, a は A **に属する**といい, $a \in A$ と書く. また, a が A の元でないとき, $a \notin A$ と書く.

例 1.3.

いくつか具体例をみて, $\in$ の使い方や集合の書き方に慣れて欲しい.

[2]専門書によっては自然数に 0 を入れることがある. どちらかというと洋書に多い.

- $A := \{10\text{ 以下の素数 }\}$ とおくと,

$$3 \in A, \qquad 4 \notin A, \qquad 7 \in A, \qquad 11 \notin A$$

である. なぜなら, 4 は素数ではなく, 11 は 10 より大きいからである.
- $B := \{3n : n = 1, 2, \ldots, 3333\}$ は $B = \{3n : n \in \mathbb{N},\ n \leq 3333\}$ とも書ける. この $\{3n : n \in \mathbb{N},\ n \leq 3333\}$ は厳密な書き方である.
- 集合 X_1, X_2, X_3 をそれぞれ

$$X_1 := \{x \in \mathbb{Q} : x^4 - x^2 - 2 = 0\}$$
$$X_2 := \{x \in \mathbb{R} : x^4 - x^2 - 2 = 0\}$$
$$X_3 := \{x \in \mathbb{C} : x^4 - x^2 - 2 = 0\}$$

とおくと, $X_1 = \emptyset$, $X_2 = \{\pm\sqrt{2}\}$, $X_3 = \{\sqrt{2}, -\sqrt{2}, \sqrt{-1}, -\sqrt{-1}\}$ となる.
- どちらの書き方がわかりやすいかを考えてみてほしい. 計算には左側の方がいいこともあるが, 意味を理解するには右側の方がわかりやすい.

$$\{\pm 1, \pm\sqrt{-1}\} = \{z \in \mathbb{C} : z^4 = 1\}.$$

問題 1.1.
{ 正の偶数 }, { 正の奇数 } を $\in$ を使って厳密に書いてみよ.

次に, 集合が等しいとはどういうことか, つまり, 集合の等号 "=" とはどういうことかを**定義する**[3].

定義 1.3 (包含関係, 集合の等号)**.**
A, B を集合とする. このとき, $A \subset B$ であるとは,

「任意の (すべての)$a \in A$ に対して $a \in B$」

が成り立つことをいう. また, $A \subset B$ でないとき, $A \not\subset B$ と書く. さらに, $A = B$ であるとは

$$A \subset B \text{ かつ } B \subset A$$

が成り立つことをいう.

注意 1.2 (論理記号を使った書き方)**.**
定義 1.3 を論理記号を使って書くと,

$$A \subset B \underset{\text{定義}}{\Leftrightarrow} \text{"}\forall a \in A \text{ に対して } a \in B\text{"}$$

[3]二つの物が等しいということは定義するものである. 例えば, $1 = 0.999\ldots$ が等しいことを示すには, 厳密には, 二つの実数が等しいとはどういうことかを認識する必要がある.

となる. いくつか記号を説明しよう. 詳しくは第 3 章で説明する.

- $\underset{\text{定義}}{\Leftrightarrow}$　左を右で定義する (右を左で定義することもある).
- $\forall$: 「任意の, すべての」を表す記号 (for all, for any の A をひっくりかえしたもの)

例 1.4.

$A := \{9n : n \in \mathbb{Z}\}$, $B := \{6n : n \in \mathbb{Z}\}$, $C := \{3n : n \in \mathbb{Z}\}$ とすると,

$$A \subset C, \quad A \not\subset B$$

となる. $A \subset C$ は「9 の倍数は 3 の倍数である」, $A \not\subset B$ は「9 の倍数は 6 の倍数とは限らない」ということを集合の言葉で書いたものである.

証明.

1. $A \subset C$ を示す.

> 示せばいいことは, 「任意の $a \in A$ に対して $a \in C$ となること」である.

任意の $a \in A$ に対して, ある $n \in \mathbb{Z}$ がとれて, $a = 9n$ と書ける. $9n = 3 \times (3n)$ であり, $3n \in \mathbb{Z}$ だから, $a = 3 \times (3n) \in C$ となる. 従って, $A \subset C$ が成り立つ.

2. $A \not\subset B$ を示す.

> 示せばいいことは, 「任意の $a \in A$ に対して $a \in B$」が成り立たないことである. 従って, 「ある $a \in A$ が存在して $a \notin B$」を示せばよい. すなわち, $a \in A$ となるが $a \notin B$ となる a をみつければよい.

$27 = 9 \times 3$ だから $27 \in A$ である. しかし, 27 は 6 で割り切れないから, $27 \notin B$ である. □

注意 1.3.

上記の枠で囲んだところは実際の証明では書かなくてよいことであるが, 数学を理解するうえでとても大切なことである. 特に, **何を示せばよいか？**を整理してから証明を書くことは大変重要である. 教科書や専門書を自習するにあたって, 証明を読む前, 演習問題を解く前には**何を示せばよいか？**を考えるとよい. **何を示せばよいか？**がはっきりすると, 考える問題はそれほど難しくないことも多い.

注意 1.4 (よくある間違い)**.**

$A \subset C$ の証明の最初の「任意の $a \in A$ に対して」を**書き忘れてはいけない**. $A \subset C$ の定義は「任意の $a \in A$ に対して $a \in C$」だったのだから,「任意の $a \in A$ に対して」は**証明の最初にでてくるはず**である.

注意 1.5.

例 1.4 の証明でででてきた「任意の $a \in A$ に対して $a \in B$」が成り立たないことについて考えてみる.「任意の」は「すべての」とおきかえても同じだから,「すべての $a \in A$ に対して $a \in B$」が成り立たないことは何かということになり, これは「ある $a \in A$ に対しては $a \in B$ が成り立たない」ということである.[4] この「ある」は数学の専門用語で「存在」ということが多い.「存在」を使って言いかえてみると「ある $a \in A$ が存在して, $a \in B$ が成り立たない」, つまり「ある $a \in A$ が存在して, $a \notin B$」となる. このことを論理記号 $\exists$ を用いて,「$\exists a \in A$ s.t $a \notin B$」と書く. 詳しくは第 3 章で説明する.

問題 1.2.

$A := \{2n : n \in \mathbb{Z}\}$, $B := \{4n : n \in \mathbb{Z}\}$, $C := \{6n : n \in \mathbb{Z}\}$ とする.

(1) $B \subset A$ を示せ.

(2) $C \not\subset B$ を示せ.

問題 1.3.

$A := \{n^3 : n \in \mathbb{N}\}$, $B := \{n^6 : n \in \mathbb{N}\}$, $C := \{n^9 : n \in \mathbb{N}\}$ とする.

(1) $B \subset A$ を示せ.

(2) $C \not\subset B$ を示せ.

問題 1.4.

集合 A, B, C が $A \subset B$, $B \subset C$ をみたすとする. このとき, $A \subset C$ を示せ.

1.2. 集合の演算

二つ以上の集合から新しい集合を定義しよう. これは集合にどのような演算を考えるかということでもある. ベン図も用いて説明すると感覚的にはわかりやすいが, ベン図の理解をきちんと証明として記述できるようにして欲しい.

定義 1.4 (差集合)**.**

集合 A, B に対して, **差集合** $A \setminus B$ を

$$A \setminus B := \{a \in A : a \notin B\}$$

[4]「すべての学生が男子である」が成り立たないことは「ある学生が女子である」ということであり,「すべての学生が女子である」というわけではない. つまり, 男子校でないということが女子校であるというわけではない.

で定める. つまり, 差集合は A に入っていて B に入っていない集合である.

例 1.5.
$\mathbb{R} \setminus \mathbb{Q} = \{x \in \mathbb{R} : x \notin \mathbb{Q}\}$ は有理数でない実数, すなわち無理数全体の集合である. また, $\mathbb{C} \setminus \mathbb{R}$ は実数でない複素数である. だから

$$\mathbb{C} \setminus \mathbb{R} = \{x + \sqrt{-1}y : x \in \mathbb{R},\ y \in \mathbb{R}, y \neq 0\}$$

となる.

定義 1.5 (補集合)**.**
集合 A に対して, A の補集合 A^c を

$$A^c := \{a : a \notin A\}$$

で定める.

注意.
通常, 集合 A の補集合を定めるときには, A を部分集合とする全体集合 X が定まっている. すなわち, $A \subset X$ となる集合 X が定まっており, $A^c = X \setminus A$ により定まっている. よって, 定義 1.5 は厳密に書くと $A^c := \{a \in X : a \notin A\}$ となる. 従って, 全体集合 X が異なると, 補集合も異なることがある. 例えば, $X = \mathbb{R}$ で $A = \mathbb{Q}$ のとき, $A^c = \mathbb{Q}^c = \mathbb{R} \setminus \mathbb{Q}$ は無理数全体の集合になるが, $X = \mathbb{C}$ で $A = \mathbb{Q}$ のとき, $A^c = \mathbb{Q}^c = \mathbb{C} \setminus \mathbb{Q}$ は, 複素数の中で, 有理数でない数全体の集合となる. ただし, 全体集合は明らかなために明記されないことも多い. 以下, 補集合については, 常に全体集合 X が定まっていると仮定する.

定義 1.6 (和集合, 共通部分)**.**
A, B を集合とする. このとき, A と B の**和集合** $A \cup B$ と A と B の**共通部分** $A \cap B$ を

$$A \cup B := \{x : x \in A \text{ または } x \in B\}, \quad A \cap B := \{x : x \in A \text{ かつ } x \in B\}$$

で定める.

例 1.6.
差集合や和集合, 共通部分を求めてみる.

- 集合 $A := \{1, 2, 3, 4\}$, $B := \{3, 4, 5, 6\}$ に対して,

$$A \cup B = \{1, 2, 3, 4, 5, 6\},\ A \cap B = \{3, 4\},\ A \setminus B = \{1, 2\},\ B \setminus A = \{5, 6\}.$$

さらに, $C := \{5, 6, 7, 8\}$, $D := \{5, 6, \{1, 2\}\}$ とする (**括弧に注意**). このとき, $A \cap C = \emptyset$, $A \cap D = \emptyset$ である. $A \cap D = \{1, 2\}$ **ではない**.

- $A := \mathbb{N}_0 := \{0, 1, 2, 3, \dots\} = \{0 \text{ 以上の整数 }\}$, $B := \{-n : n \in \mathbb{N}_0\}$ とおく. このとき,

  $$A \cup B = \{x : x \in A \text{ または } x \in B\} = \{0, \pm 1, \pm 2, \dots\} = \mathbb{Z},$$
  $$A \cap B = \{x : x \in A \text{ かつ } x \in B\} = \{0\}$$

  となる.
- $\mathbb{Q} \cap \mathbb{R} = \mathbb{Q}$, $\mathbb{Q} \cup \mathbb{R} = \mathbb{R}$ である.
- $(x^2 - 2)(x^2 + 1) = 0$ をみたす有理数 x, 実数 x は集合を用いて

  $$\{x \in \mathbb{C} : (x^2 - 2)(x^2 + 1) = 0\} \cap \mathbb{Q} = \emptyset,$$
  $$\{x \in \mathbb{C} : (x^2 - 2)(x^2 + 1) = 0\} \cap \mathbb{R} = \{\sqrt{2}, -\sqrt{2}\}$$

  と書くことができる.

問題 1.5.
集合 $A := \{1, 2, 3\}$, $B := \{2, \{3, 4\}\}$ について, $A \setminus B$, $B \setminus A$, $A \cup B$, $A \cap B$ を求めよ.

定理 1.1.
集合 A, B に対して, 次が成り立つ.

(1) $A \subset A \cup B$, $B \subset A \cup B$;
(2) $A \cap B \subset A$, $A \cap B \subset B$;

証明.

> (1) について, 示すべきことは「任意の $a \in A$ に対して $a \in A \cup B$」と「任意の $b \in B$ に対して $b \in A \cup B$」である. (2) について, 示すべきことは「任意の $a \in A \cap B$ に対して $a \in A$」と「任意の $b \in A \cap B$ に対して $b \in B$」である.

(1) $A \subset A \cup B$ のみ示す. 任意の $a \in A$ に対して, 「$a \in A$ または $a \in B$」が成り立つ. 従って, $a \in A \cup B$ となるから, $A \subset A \cup B$ となる.
(2) $A \cap B \subset A$ のみ示す. 任意の $a \in A \cap B$ に対して, 「$a \in A$ かつ $a \in B$」が成り立つ. よって $a \in A$ が成り立つから, $A \cap B \subset A$ となる.

□

注意 1.6.
「または」を示すときには, どちらかが示せればよい. 「または」が仮定さ

れているときには, どちらかが成り立っていることが仮定されているので, 場合わけを使うなど, 証明に工夫がいる.

「かつ」が**仮定されているときには, 両方が成り立っている**ことが仮定されているので, 証明をするためには両方の仮定を使うことができる. 「かつ」を**示すときには, 両方を示せれば**よいので, 二つのことがらを示す必要がある.

注意 1.7 (よくある間違い)**.**

「$a \in A$ または $a \in B$」を「$a \in A$ または B」と**書いてはいけない**. 第 3 章で詳しく説明するが, 「または」の前後には「成り立つか成り立たないか判断できるもの」がないといけない. 「$a \in A$」や「$x \in B$」は成り立つか成り立たないかを判断することができるが, 「B」は**成り立つ, 成り立たないを判断できるものではない.**

質問と答え.

A が空集合ならば, 「任意の $a \in A$」は意味がないのではないか？という質問がありました. たしかに, 空集合ならば元がないのだから, 任意に元を取るということに意味がありません. このような**ちょっと極端かなと思える例を考えてみる**ことは, 内容を理解するうえで非常に重要で, このような質問を思いつくということは非常によいことです.

さて, A が空集合のときにどう考えるかですが, このときは主張「任意の $a \in A$ に対して $a \in A \cup B$」は常に成立すると考えます. このことを説明するために, 背理法を用いて「任意の $a \in A$ に対して $a \in A \cup B$」が成り立たないと仮定してみます. すると, 否定の主張である「ある $a \in A$ が存在して, $a \notin A \cup B$」が成り立つことになりますが, A は空集合だったので, $a \notin A \cup B$ となる $a \in A$ は存在しません. なぜなら, A は空集合ですから, そもそも元が存在しないからです. 従って, 否定の主張が成り立たない, つまり矛盾が得られました. よって, もとの主張である「任意の $a \in A$ に対して $a \in A \cup B$」は成り立つということになります.

主張「任意の $a \in A$ に対して $a \in A \cup B$」が成り立つということを高校で学んだ「背理法」を用いて説明しましたが, 背理法の根底には「排中律」という**ほとんどあたりまえな主張**があります. 排中律とは「命題 p(第 3 章でやります) に対して, p または p の否定のどちらか一方のみが成り立つ」という主張で, 大雑把にいうと, 答えは正しいか正しくないかのどちらかしかないという主張です. 正しそうに見えますが, これが正しいと認めるかそうでないか (つまり, 背理法を証明に使ってよいか, 使ってはいけないか) で, 数学の世界が大きくかわることが知られています.

問題 1.6.
定理 1.1 について, $B \subset A \cup B$ と $A \cap B \subset B$ を示せ.

定理 1.2 (交換法則)**.**
集合 A, B に対して, 次が成り立つ.

(1) $A \cup B = B \cup A$.
(2) $A \cap B = B \cap A$.

定理 1.2 について, 二通りの証明の書き方を説明する. 一つ目は同値の考え方に近い証明である.

定理 1.2 の証明 その 1.

> (1) について, $A \cup B = B \cup A$ を示すのだから, 定義 1.3 から,「$A \cup B \subset B \cup A$」と「$A \cup B \supset B \cup A$」の両方を示す必要がある.「$A \cup B \subset B \cup A$」を示すには,「任意の $a \in A \cup B$ に対して $a \in B \cup A$」を示す必要がある.「$A \cup B \supset B \cup A$」を示すには,「任意の $a \in B \cup A$ に対して $a \in A \cup B$」を示す必要がある. つまり, (1) についてだけでも二つの主張を示す必要がある.

$A \cup B = B \cup A$ のみ示す. そのためには, $A \cup B \subset B \cup A$ と $B \cup A \subset A \cup B$ を示せばよい.

1. $A \cup B \subset B \cup A$ を示す. 任意の $a \in A \cup B$ に対して,「$a \in A$ または $a \in B$」が成り立つ. よって「$a \in B$ または $a \in A$」も成り立つから, $a \in B \cup A$ がわかる. 従って, $A \cup B \subset B \cup A$ となる.

2. $B \cup A \subset A \cup B$ を示す. 任意の $a \in B \cup A$ に対して,「$a \in B$ または $a \in A$」が成り立つ. よって「$a \in A$ または $a \in B$」も成り立つから, $a \in A \cup B$ がわかる. 従って, $B \cup A \subset A \cup B$ となる.

3. **1.** と **2.** より, $A \cup B \subset B \cup A$ と $B \cup A \subset A \cup B$ がわかったので, $A \cup B = B \cup A$ となる. □

注意 1.8.
定理 1.2 の証明で **1.** と **2.** は同じように見えると思う. 実際, 証明に本質的な違いは何もない. しかし, 最初のうちは, **どんなに当たり前だと思うことであっても, きちんと書く癖をつけること**[5]. 特に, **同様である**などで済ますのは, 使わないようにすること. 教科書などで書かれている**「同様である」**は,**「同**

[5]当たり前と思うことに証明をつけることは, 案外難しいことが多い.

様であるから自分で確かめてみよ」という意味である. より専門的な問題では,「同様である」が同様では証明できないことなどがよくある.

問題 1.7.
定理 1.2 において, $A \cap B = B \cap A$ を示せ.

注意 1.9.
教科書によっては, 次のような証明を書いてあることがある.

$$\begin{aligned} x \in A \cup B &\Leftrightarrow x \in A \text{ or } x \in B \\ &\Leftrightarrow x \in B \text{ or } x \in A \\ &\Leftrightarrow x \in B \cup A. \end{aligned}$$

この証明を日本語で書き下したものが「証明 (その 1)」である. このノートでは, この書き方を**推奨しない.** 自分のノートや計算用紙にこの書き方をするのはよいが, 証明として書く時には「証明 (その 1)」のように, 日本語を用いて説明を書くべきである. なぜなら, この書き方は**説明をしたものではない**からである. さらに証明を書く時には「正確な表現」が求められるからである.

定理 1.2 の証明には,「または」がでてくる.「または」はどのように扱うかが見えるようにした証明の書き方をしてみよう.

定理 1.2 の証明 その 2.
$A \cup B \subset B \cup A$ のみ示す. 逆の包含関係 $B \cup A \subset A \cup B$ は各自試みよ.
任意の $a \in A \cup B$ に対して,「$a \in A$ または $a \in B$」が成り立つ. そこで, 場合わけをする.
Case 1. $a \in A$ が成り立つならば,「$a \in B$ または $a \in A$」が成り立つ. よって, $a \in B \cup A$ が成り立つ.
Case 2. $a \in B$ が成り立つならば,「$a \in B$ または $a \in A$」が成り立つ. よって, $a \in B \cup A$ が成り立つ.
よって, どちらの場合についても $a \in B \cup A$ が成り立つ. 従って, $A \cup B \subset B \cup A$ が示された. □

注意 1.10.
「または」が**仮定されている**ときは, どちらかが成り立つから (いいかえると**両方が成り立っていると仮定できない**から), 場合わけを使う必要がある場合が多い. 逆に「または」を**示すとき**には, どちらか片方を示せばよいのだから, どちらか片方のみを示すことを考えればよい.

定理 1.3 (結合法則)**.**
集合 A, B, C に対して, 次が成り立つ.

(1) $(A \cap B) \cap C = A \cap (B \cap C)$;
(2) $(A \cup B) \cup C = A \cup (B \cup C)$.

結合法則についても, 同値の考え方に近い証明の仕方と「かつ」の扱い方が見えるようにした証明の仕方をしてみよう.

定理 1.3 の証明 その 1.
$(A \cap B) \cap C = A \cap (B \cap C)$ のみ示す.
1. $(A \cap B) \cap C \subset A \cap (B \cap C)$ を示す. 任意の $a \in (A \cap B) \cap C$ に対して, 「$a \in A \cap B$ かつ $a \in C$」が成り立つ. よって, 「[$a \in A$ かつ $a \in B$] かつ $a \in C$」も成り立つから「$a \in A$ かつ [$a \in B$ かつ $a \in C$]」となる. よって, 「$a \in A$ かつ $a \in B \cap C$」となるから, $a \in A \cap (B \cap C)$ が成り立つ.
2. $(A \cap B) \cap C \supset A \cap (B \cap C)$ を示す. 任意の $a \in A \cap (B \cap C)$ に対して, 「$a \in A$ かつ $a \in B \cap C$」が成り立つ. よって, 「$a \in A$ かつ [$a \in B$ かつ $a \in C$]」も成り立つから「[$a \in A$ かつ $a \in B$] かつ $a \in C$」となる. よって, 「$a \in A \cap B$ かつ $a \in C$」となるから, $a \in (A \cap B) \cap C$ が成り立つ.
3. 1. と **2.** により, $(A \cap B) \cap C \subset A \cap (B \cap C)$ と $A \cap (B \cap C) \subset (A \cap B) \cap C$ がわかったので, $A \cap (B \cap C) = (A \cap B) \cap C$ となる. □

注意 1.11.
「証明 (その 1)」を論理記号の $\Leftrightarrow$ を用いて簡潔に書くと, 次のようになる. これらの記号の扱い方については第 3 章で詳しく説明する.

$$\begin{aligned} x \in A \cap (B \cap C) &\Leftrightarrow x \in A \text{ and } x \in B \cap C \\ &\Leftrightarrow x \in A \text{ and } (x \in B \text{ and } x \in C) \\ &\Leftrightarrow (x \in A \text{ and } x \in B) \text{ and } x \in C \\ &\Leftrightarrow (x \in A \cap B) \text{ and } x \in C \\ &\Leftrightarrow x \in (A \cap B) \cap C \end{aligned}$$

なお, 注意 1.9 で書いたとおり, このノートでは, この書き方を**推奨しない.**

注意 1.12.
証明を書くときは, 各ステップ毎に**何を示すのか?**を書く方があとで読み返すときや相手に伝えるときにわかりやすい.

定理 1.3 の証明 その 2.
$(A \cap B) \cap C \subset A \cap (B \cap C)$ のみ示す. 逆の包含関係 $A \cap (B \cap C) \subset (A \cap B) \cap C$ は各自試みよ.

任意の $a \in (A \cap B) \cap C$ に対して, 「$a \in A \cap B$ かつ $a \in C$」が成り立つ. よって, 「[$a \in A$ かつ $a \in B$] かつ $a \in C$」が成り立つ. 「$a \in A$ かつ [$a \in B$ かつ $a \in C$]」を示すために, 二つの主張 $a \in A$ と「$a \in B$ かつ $a \in C$」を示す.

1. $a \in A$ を示す. 「$a \in A$ かつ $a \in B$」が成り立つから, とくに $a \in A$ も成り立つ.

2. 「$a \in B$ かつ $a \in C$」を示す. 「$a \in A$ かつ $a \in B$」が成り立つから, とくに $a \in B$ も成り立つ. また $a \in C$ も成り立っていたから, 「$a \in B$ かつ $a \in C$」が成り立つ.

よって, 「$a \in A$ かつ [$a \in B$ かつ $a \in C$]」が成り立つから, 「$a \in A$ かつ $a \in B \cap C$」となるので, $a \in A \cap (B \cap C)$ が示された. □

注意 1.13.

「かつ」が**仮定されている**ときは, 両方が成り立つから, 示したいことにあわせて, 使いたいほうを選んで使ってよい. 逆に「かつ」を**示すとき**には, 両方を示す必要があるから, それぞれの主張を示す必要がある. 従って, 示すことを二つにわける必要がある場合が多い.

問題 1.8.

定理 1.3 において, $(A \cup B) \cup C = A \cup (B \cup C)$ を示せ.

定理 1.4 (分配法則)**.**

集合 A, B, C に対して, 次が成り立つ.

(1) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$;
(2) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

証明.

(1) **1.** $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$ を示す. 任意の $a \in (A \cap B) \cup C$ に対して, 「$a \in A \cap B$ または $a \in C$」が成り立つ. よって「[$a \in A$ かつ $a \in B$] または $a \in C$」となるから「[$a \in A$ または $a \in C$] かつ [$a \in B$ または $a \in C$]」が得られる. だから「$a \in A \cup C$ かつ $a \in B \cup C$」となるので, $a \in (A \cup C) \cap (B \cup C)$ が成り立つ.

2. $(A \cap B) \cup C \supset (A \cup C) \cap (B \cup C)$ を示す. 任意の $a \in (A \cup C) \cap (B \cup C)$ に対して, 「$a \in A \cup C$ かつ $a \in B \cup C$」が成り立つ. よって「[$a \in A$ または $a \in C$] かつ [$a \in B$ または $a \in C$]」が成り立つ. ここから, 「[$a \in A$ かつ $a \in B$] または $a \in C$」が成り立つことを示す.

$a \in C$ のときに「[$a \in A$ かつ $a \in B$] または $a \in C$」は成立しているから, $a \notin C$ のときを考える. このとき, 「$a \in A$ または $a \in C$」から $a \in A$ が成り立つ. また, 「$a \in B$ または $a \in C$」から $a \in B$ も成り立つ. よって, $a \notin C$ のと

きは「$a \in A$ かつ $a \in B$」が成り立つことがわかるので,「[$a \in A$ かつ $a \in B$] または $a \in C$」が成り立つ.

従って,「$a \in A \cap B$ または $a \in C$」となるから $a \in (A \cap B) \cup C$ となる. よって, $(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$ となる.

3. 1. と **2.** により, $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$ と $(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$ がわかったので, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ がわかる.

(2) **1.** $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$ を示す. 任意の $a \in (A \cup B) \cap C$ に対して,「$a \in A \cup B$ かつ $a \in C$」が成り立つ. とくに $a \in A \cup B$ より,「$a \in A$ または $a \in B$」が成り立つ. ここで, 場合わけをする.

もし, $a \in A$ ならば, $a \in C$ だったことから, $a \in A \cap C$ が成り立つ. よって, $a \in (A \cap C) \cup (B \cap C)$ も成り立つ.

逆にもし, $a \in B$ ならば, $a \in C$ だったことから, $a \in B \cap C$ が成り立つ. よって, $a \in (A \cap C) \cup (B \cap C)$ も成り立つ.

いずれにせよ, $a \in (A \cap C) \cup (B \cap C)$ となることがわかったので, $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$ が成り立つ.

2. $(A \cup B) \cap C \supset (A \cap C) \cup (B \cap C)$ を示す. 任意の $a \in (A \cap C) \cup (B \cap C)$ に対して,「$a \in A \cap C$ または $a \in B \cap C$」が成り立つ. ここで場合わけしてみる.

$a \in A \cap C$ ならば,「$a \in A$ かつ $a \in C$」より, $a \in A \cup B$ も成り立つ. よって, $a \in (A \cup B)$ と $a \in C$ がともに成り立つから, $a \in (A \cup B) \cap C$ が成り立つ.

逆に $a \in B \cap C$ ならば,「$a \in B$ かつ $a \in C$」より, $a \in A \cup B$ も成り立つ. よって, $a \in (A \cup B)$ と $a \in C$ がともに成り立つから, $a \in (A \cup B) \cap C$ が成り立つ.

いずれにせよ, $a \in (A \cup B) \cap C$ が成り立つから, $(A \cup B) \cap C \supset (A \cap C) \cup (B \cap C)$ が成り立つ.

3. 1. と **2.** により, $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$ と $(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$ がわかったので, $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ がわかる. □

注意 1.14.

定理 1.4 の証明において, (1) **2.** の議論はやや煩雑である. 第 3 章で,「[$a \in A$ または $a \in C$] かつ [$a \in B$ または $a \in C$]」と「[$a \in A$ かつ $a \in B$] または $a \in C$」は実は同じ主張であることを証明する. しかし, **2.** での証明のアイデアも非常に重要である.「A または B」が成り立つことを示すのに, **B が成り立たないと仮定して A が成り立つことを示す**議論はよく用いられる.

定理 1.5 (de Morgan の法則)**.**

集合 A, B に対して, 次が成り立つ.

(1) $(A \cap B)^c = A^c \cup B^c$;
(2) $(A \cup B)^c = A^c \cap B^c$.

証明.

$(A \cap B)^c = A^c \cup B^c$ のみ示す.

1. 任意の $a \in (A \cap B)^c$ に対して,「$a \notin A \cap B$」だから「[$a \in A$ かつ $a \in B$] の否定」が成り立つ. よって,「$a \notin A$ または $a \notin B$」となるから,「$a \in A^c$ または $a \in B^c$」, すなわち $a \in A^c \cup B^c$ が成り立つ. 従って, $(A \cap B)^c \subset A^c \cup B^c$ が成り立つ.

2. 任意の $a \in A^c \cup B^c$ に対して,「$a \in A^c$ または $a \in B^c$」だから「$a \notin A$ または $a \notin B$」が成り立つ. これは,「[$a \in A$ かつ $a \in B$] の否定」だったことに注意すると,「$a \in A \cap B$ の否定」となるから $a \notin A \cap B$ が成り立つ. 従って, $a \in (A \cap B)^c$ だから, $A^c \cup B^c \subset (A \cap B)^c$ が成り立つ.

3. 1. と **2.** により, $(A \cap B)^c \subset A^c \cup B^c$ と $A^c \cup B^c \subset (A \cap B)^c$ が成り立つから, $A^c \cup B^c = (A \cap B)^c$ が成り立つ. □

問題 1.9.

de Morgan の法則を差集合を用いて記述せよ. 例えば, 集合 X, $A \subset X$, $B \subset X$ について, $(A \cap B)^c = X \setminus (A \cap B)$ がどう書けるか?

問題 1.10.

de Morgan の法則をベン図を用いて説明せよ. ベン図は証明にはならないが, 主張や証明を理解する手助けになる.

注意 1.15.

「$a \in A$ かつ $a \in B$」が成り立たないとはどういうことかに注意して欲しい. 「$a \in A$ かつ $a \in B$」とは「$a \in A$ と $a \in B$ の両方が成り立つこと」だから, これが成り立たないということは,「$a \in A$ と $a \in B$ のどちらか一方は成り立たない」ということである. すなわち「$a \notin A$ か $a \notin B$ のどちらかが成り立つ」ことになる. これは,「$a \notin A$ または $a \notin B$」が成り立つことと同じである.

同じようにして,「$a \in A$ または $a \in B$」が成り立たないということは,「$a \in A$ か $a \in B$ のどちらかが成り立つ」が成立しないことだから「$a \in A$ と $a \in B$ の両方が成り立たない」, つまり「$a \notin A$ かつ $a \notin B$」ということになる.

問題 1.11.

定理 1.5 において, $(A \cup B)^c = A^c \cap B^c$ を示せ.

1.3. 直積集合

平面や空間を考える上で集合の積が重要になる. 高校で学んだ関数のグラフも直積集合の部分集合と考えることができる.

定義 1.7 (直積集合)**.**
集合 A, B に対して, **直積集合** $A \times B$ を

$$A \times B := \{(a, b) : a \in A \text{かつ} b \in B\}$$

で定義する.

例 1.7.
直積集合の具体例をあげる.

- 集合 $A := \{1, 2, 3\}$, $B := \{4, 5\}$ に対して,

  $$A \times B = \{(1, 4),\ (1, 5),\ (2, 4),\ (2, 5),\ (3, 4),\ (3, 5)\}.$$

  A の元の数が 3 個, B の元の数が 2 個, $A \times B$ の元の個数が $3 \times 2 = 6$ 個となっていることに注意して欲しい.
- $\mathbb{R} \times \mathbb{R} = \{(x, y) : x \in \mathbb{R},\ y \in \mathbb{R}\}$ である. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ と書く. $\mathbb{R} \subset \mathbb{R} \times \mathbb{R}$ ではないことに注意せよ.[6]
- $\mathbb{R} \times (0, \infty) = \{(x, y) : x \in \mathbb{R},\ 0 < y < \infty\}$ である. $\mathbb{R}^2_+ := \mathbb{R} \times (0, \infty)$ と書く (半空間という). このとき, $\mathbb{R}^2_+ \subset \mathbb{R}^2$ となる.
- $\mathbb{N} \times \mathbb{R} = \{(n, x) : n \in \mathbb{N},\ x \in \mathbb{R}\}$
- n 次元空間 $\mathbb{R}^n$ を

  $$\mathbb{R}^n := \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ 個}}$$

  で定める.

  $$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) : x_1 \in \mathbb{R},\ x_2 \in \mathbb{R}, \ldots, x_n \in \mathbb{R}\}$$

  である.

例 1.8 (ベクトル空間)**.**
$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ が平面ベクトルのとき, $\vec{a} \in \mathbb{R}^2$ と書く. また, $\vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$ が空間ベクトルのとき, $\vec{b} \in \mathbb{R}^3$ と書く.

2 次の正方行列のなす集合を $M_2(\mathbb{R})$ とかく, すなわち

$$M_2(\mathbb{R}) := \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} : \text{任意の } i, j = 1, 2 \text{ に対して } a_{ij} \in \mathbb{R} \right\}$$

である. 同様にして, 3 次の正方行列のなす集合を $M_3(\mathbb{R})$ と書く.

[6] ただし, $\mathbb{R}$ と $\mathbb{R} \times \{0\}$ を同じものとみなして, $\mathbb{R} \subset \mathbb{R} \times \mathbb{R}$ とみなすことがある.

問題 1.12.

$A := \{1, 2, \{3, 4\}\}$, $B := \{2, 3, 4\}$ とする. このとき, $A \times B$ を求めよ. 元の個数はいくつか？

定理 1.6.

集合 A, B, C について, 次が成り立つ.

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

証明.

$A \times (B \cup C) = (A \times B) \cup (A \times C)$ のみ示す.

1. $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$ を示す.

> 示すべきことは任意の $(a, b) \in A \times (B \cup C)$ に対して, $(a, b) \in (A \times B) \cup (A \times C)$ だから, 「$(a, b) \in (A \times B)$ または $(a, b) \in (A \times C)$」である. 定義 1.7 より $(a, b) \in A \times B$ を示すには,「$a \in A$ かつ $b \in B$」を示せばよい.

任意の $(a, b) \in A \times (B \cup C)$ に対して, 「$a \in A$ かつ $b \in B \cup C$」が成り立つ. よって, とくに「$b \in B$ または $b \in C$」が成り立つ. $(a, b) \in (A \times B) \cup (A \times C)$ を示すために場合わけをする.

$b \in B$ ならば $a \in A$ だったから $(a, b) \in A \times B$ となる. よって, $(a, b) \in (A \times B) \cup (A \times C)$ が成り立つ.

逆に $b \in C$ ならば $a \in A$ だったから $(a, b) \in A \times C$ となる. よって, $(a, b) \in (A \times B) \cup (A \times C)$ が成り立つ. いずれにせよ $(a, b) \in (A \times B) \cup (A \times C)$ が成り立つ.

2. $A \times (B \cup C) \supset (A \times B) \cup (A \times C)$ を示す. 任意の $(a, b) \in (A \times B) \cup (A \times C)$ に対して, 「$(a, b) \in A \times B$ または $(a, b) \in A \times C$」が成り立つ. そこで場合わけして, $(a, b) \in A \times (B \cup C)$ を示す.

$(a, b) \in A \times B$ ならば「$a \in A$ かつ $b \in B$」となるから, とくに定理 1.1 より「$b \in B \subset B \cup C$」となる. よって, $b \in B \cup C$ だから $(a, b) \in A \times (B \cup C)$ である.

逆に $(a, b) \in A \times C$ ならば「$a \in A$ かつ $b \in C$」となるから, とくに定理 1.1 より「$b \in C \subset B \cup C$」となる. よって, $b \in B \cup C$ だから $(a, b) \in A \times (B \cup C)$ である. いずれにせよ $(a, b) \in A \times (B \cup C)$ が得られた. □

問題 1.13.

定理 1.6 において, $A \times (B \cap C) = (A \times B) \cap (A \times C)$ を示せ.

1.4. 応用: 群論の基礎

ここまで集合と演算方法, 証明の書き方について述べたが, そもそもなぜ集合が必要なのか？ということについては触れていない. 集合を最初にしっかりやる理由は, 序文で書いたように証明の書き方を学ぶための題材としての側面もあるが, 数学を考えるときの世界が何か？を決めるためにも使われる[7]. この「考える世界」について説明するために, $\mathbb{Z}$ のたし算について考えてみよう.

$\mathbb{Z}$ のたし算 $+$ には, 次の三つの基本的性質を持っている.

(1) 任意の $a, b, c \in \mathbb{Z}$ に対して, $(a+b)+c = a+(b+c)$ が成り立つ (**結合法則**という).
(2) 任意の $a \in \mathbb{Z}$ に対して $a+0 = 0+a = a$ が成り立つ (この 0 を ($\mathbb{Z}$ の加法に対する) **単位元**という).
(3) 任意の $a \in \mathbb{Z}$ に対して $a+(-a) = (-a)+a = 0$ が成り立つ (この $-a$ を ($\mathbb{Z}$ の加法について a に対する) **逆元**という).

先の三つの性質を持つ集合を**群**という[8]. 代数学でもっとも基礎となる集合であり, この群の性質を調べることが代数学の最初の目標である. しかし, なぜこの性質について調べなければいけないのだろうか？

このことをもう少し見るために, X を変数とする実数係数多項式全体のなす集合を $\mathbb{R}[X]$ と書くことにする. すなわち

$$\mathbb{R}[X] := \{a_0 + a_1X + a_2X^2 + \cdots a_nX^n : n \in \mathbb{N},\ a_0, a_1, a_2, \ldots, a_n \in \mathbb{R}\}$$

と定める. 例えば, $1,\ 2+\sqrt{2}X,\ 4-5X+2X^2 \in \mathbb{R}[X]$ である. この, $\mathbb{R}[X]$ についても, 多項式のたし算が定義できるが, この多項式のたし算についても, 群の性質をみたしている. つまり, 次の三つの性質が成り立つ.

(1) 任意の $f(X), g(X), h(X) \in \mathbb{R}[X]$ に対して[9], $(f(X)+g(X))+h(X) = f(X)+(g(X)+h(X))$ が成り立つ.
(2) 任意の $f(X) \in \mathbb{R}[X]$ に対して $f(X)+0 = 0+f(X) = f(X)$ が成り立つ.
(3) 任意の $f(X) \in \mathbb{R}[X]$ に対して $f(X)+(-f(X)) = (-f(X))+f(X) = 0$ が成り立つ.

---

[7] 中学, 高校ではあまり注意する必要はなかったが, 大学の数学では, どのような世界で考えているか？をある程度明らかにしてから問題を考える必要がある.

[8] さらにいうと, 任意の $a, b \in \mathbb{Z}$ に対して $a+b = b+a$ も成り立つ (**交換法則**という). この性質を持つ群のことを**可換群**とか**アーベル群**という.

[9] $f(X) = a_0 + a_1X + \cdots + a_nX^n$, $g(X) = b_0 + b_1X + \cdots + b_mX^m$, $h(X) = c_0 + c_1X + \cdots + c_kX^k$ と思ってよい. 高校で習った関数 $f(X)$ の記法と同じである. 詳しいことは第 2 章で説明する.

つまり, $\mathbb{Z}$ の足し算も $\mathbb{R}[X]$ の足し算もよく似た性質, つまり群の性質を持っている[10]. この「性質がよく似たもの」, 「群となる性質を持つ集合」を統一的に考えて, 何がわかるか?を調べておけば, 今後の研究対象で別の「性質がよく似たもの[11]」が出てきたときに, 非常に便利である.

ところで, 整数 $\mathbb{Z}$ や多項式 $\mathbb{R}[X]$ には, かけ算が定義できていた. しかし, たし算の性質とかけ算の性質の両方を一緒に調べようとすると, 考えることが多くなって問題が難しくなる[12]. そこで, $\mathbb{Z}$ とか $\mathbb{R}[X]$ とかであったことを忘れて, 集合 G が群の性質を持つときに, どのような性質が得られるか?を問題にするのが群論という研究分野である. 最後に, 集合に対する群の定義を与えることにする. より詳しい内容については, 石田 [**2**], 雪江 [**13**] を参照せよ.

定義 1.8 (群)**.**

集合 G は, 任意の $a, b \in G$ に対して, たし算 $a + b \in G$ が定まっているとする. このたし算が, 次の三つの性質を持つとき, G は (たし算に関する) **群**であるという.

(1) 任意の $a, b, c \in G$ に対して, $(a + b) + c = a + (b + c)$ が成り立つ. この性質を**結合法則**という.
(2) $e \in G$ が存在して, 任意の $a \in \mathbb{Z}$ に対して $a + e = e + a = a$ が成り立つ. この e を (G のたし算に対する) **単位元**という.
(3) 任意の $a \in G$ に対して, $b \in G$ が存在して, $a + b = b + a = e$ が成り立つ. この b を (G のたし算について a に対する) **逆元**といい, $-a := b$ と書く.

問題 1.14.

$\mathbb{R}^\times := \{x \in \mathbb{R} : x \neq 0\}$ とおく. このとき, 実数のかけ算に関して, $\mathbb{R}^\times$ が群になることを示せ.

1.5. 演習問題

問題 1.15.

集合 A, B に対して, $A \setminus B = A$ が成り立つことと $A \cap B = \emptyset$ が同値となることを示せ. つまり, $A \setminus B = A$ が成り立つならば $A \cap B = \emptyset$ が成り立つことと, 逆に $A \cap B = \emptyset$ が成り立つならば $A \setminus B = A$ が成り立つことを示せ.

問題 1.16.

A, B を集合としたとき, 次が互いに同値であることを示せ.

[10] 高校のときから, 「足し算の性質が似ている」はなんとなく感じていただろうと思う.

[11] 例えば, ベクトル全体のなす集合は, 高校で習った足し算で群の性質をみたす. 他にも, アナログ時計の針の動きは群の性質を持っている.

[12] ただし, さらに多くの性質が出てくることからおもしろいともいえる.

(1) $A \subset B$
(2) $A \cup B = B$
(3) $A \cap B = A$
(4) $A \setminus B = \emptyset$

問題 1.17.

A, B を集合としたとき, $A \triangle B := (A \setminus B) \cup (B \setminus A)$ と定める[13]. 集合 A, B, C に対して次を示せ.

(1) $A \triangle B = B \triangle A$
(2) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
(3) $A \triangle A = \emptyset$
(4) $A \triangle \emptyset = A$
(5) 任意の集合 A, B に対して, $A \triangle X = B$ をみたす集合 X がただ一つ存在する.

問題 1.18.

集合 X, Y, $A \subset X$, $B \subset Y$ に対して

$$(X \times Y) \setminus (A \times B) = ((X \setminus A) \times Y) \cup (X \times (Y \setminus B))$$

が成り立つことを示せ.

[13] $A \triangle B$ を A と B の対称差という.

第 2 章

写像

写像というものは, 高校で習った関数をさらに一般化したものである. 数学において, 第 1 章の集合と本章の写像はどの分野であっても基礎となる概念である. この章では写像や関数はどのようにして定義すればよいか, 像と逆像, 全射と単射について説明する. この章の内容は一読しただけではすぐに理解できないかもしれない. しかし, この章を早いうちに理解することで, 今後の数学を勉強, 理解することが易しくなるので, よく考えながら, 模写するように読んで欲しい.

以下, この章ででてくる集合は常に空でないとする.

2.1. 写像とは何か？

高校までに, 二次関数や三次関数を勉強したと思う. また, 三角関数や指数関数, 対数関数も学んだと思う. また, 関数の書き方として, $y = f(x)$ なる書き方もよく使っていた. これらについて, 簡単に復習してみよう.

関数	$f(x)$ の形の典型例	x の範囲	y の範囲
三次関数	$f(x) = x(x+1)(x-1)$	$-\infty < x < \infty$	$-\infty < y < \infty$
三角関数	$f(x) = \sin x$	$-\infty < x < \infty$	$-1 \leq y \leq 1$
指数関数	$f(x) = e^x$	$-\infty < x < \infty$	$0 < y < \infty$
対数関数	$f(x) = \log x$	$0 < x < \infty$	$-\infty < y < \infty$

さて, すぐにわかることとして, 対数関数 $f(x) = \log x$ では x の範囲として $-\infty < x \leq 0$ では定義できない. また, 三角関数 $f(x) = \sin x$ においては, $-\infty < x < \infty$ では, y の範囲は $-1 \leq y \leq 1$ としてもよいことがわかる.

高校の数学で関数とは何か?ということは実は書かれているのだが, 少し曖昧なところがある. この関数というものは何かを厳密に定義しよう.

定義 2.1 (写像)**.**

X, Y を集合とする. f が**集合 X から集合 Y への写像**であるとは, 任意の $x \in X$ に対して, x によって決まるただ一つの元 $y \in Y$ を対応させる規則のことをいう. このとき, $f : X \to Y$ と書き, X を f の**定義域**, Y を f の**値域**とい

う. そして, $x \in X$ に対して, 対応する Y の元 y を $f(x) = y \in Y$ と書き, x における f の値という. さらに, $Y = \mathbb{R}$ のとき, f を (実数値) 関数という.

注意 2.1.

関数や写像とは f のことであって, $f(x)$ のことではない. ただし, 関数 $f(x)$ という書き方をする本はたくさんある. 専門書であっても正しくない表現をしていることがあるので注意すること.[1]

例 2.1 (写像でない例)**.**

大抵の場合は写像しか考えないが, どういうことをすると写像にならないのかを先に説明しよう. 以下, X, Y は定義 2.1 にあらわれる集合とする.

- (定義域に問題がある場合) $X = Y = \mathbb{R}$ として, $f : \mathbb{R} \to \mathbb{R}$ を $x \in \mathbb{R}$ に対して $f(x) := \log x$ により定めようとすると, f は写像にならない. なぜなら, $0, -1 \in \mathbb{R}$ であるが, $f(0) = \log 0$ や $f(-1) = \log(-1)$ を定めることができないからである.
- (値域に問題がある場合) $X = \mathbb{R}$, $Y = (0, \infty)$ として, $f : \mathbb{R} \to (0, \infty)$ を $x \in \mathbb{R}$ に対して $f(x) := \cos x$ により定めようとすると, f は写像にならない. なぜなら, $\pi \in \mathbb{R}$ であるが, $f(\pi) = \cos \pi = -1 \notin (0, \infty)$ だからである.
- (一つずつ対応していない例) $X = Y = \mathbb{C}$ として, $f : \mathbb{C} \to \mathbb{C}$ を $z \in \mathbb{C}$ に対して $f(z) := \sqrt{z}$ により定めようとすると, f は写像にならない. なぜなら, $i = \sqrt{-1}$ として $2i \in \mathbb{C}$ であるが,

$$(1 + i)^2 = 2i, \quad (-1 - i)^2 = 2i$$

より

$$f(2i) = \sqrt{2i} = 1 + i \text{ または } -1 - i$$

となり, $f(2i)$ の値が一つに定まらないからである[2].

例 2.2 (写像の例)**.**

写像の例と, 写像の定義の書き方を述べる. 写像をきちんと定義できることはどの分野でも重要である. 面倒でもきちんと書けるようにすること.

- 写像 $f_1 : (0, \infty) \to \mathbb{R}$ を任意の $x \in (0, \infty)$ に対して

$$f_1(x) := x^2$$

[1] 関数 $f(x)$ という表現を使ってしまうと, 関数を値にとる写像を考えるときに何を考えているのかわからなくなる. 実際に共役空間など, 関数を値にとる写像を考えることがある.

[2] $x \in \mathbb{R}$ の場合, $y = \sqrt{x}$ は $y^2 = x$ となる**非負の数**と定義されていたことに注意せよ. 複素数については, 正負や不等式の概念は, 通常は定義しない

により定める.

- 写像 $f_2 : \mathbb{R} \to \mathbb{R}$ を任意の $x \in \mathbb{R}$ に対して

$$f_2(x) := x^2$$

により定める.

- 写像 $g_1 : \mathbb{R} \to [0, \infty)$ を任意の $x \in \mathbb{R}$ に対して

$$g_1(x) := x^2$$

により定める.

- 写像 $g_2 : \mathbb{R} \to \mathbb{R}$ を任意の $x \in \mathbb{R}$ に対して

$$g_2(x) := x^2$$

により定める.

これらのように写像を定義するときは, **定義域** X, **値域** Y, **任意の** $x \in X$ **に対する** $f(x) \in Y$ の 3 つを明らかにする必要がある. 高校までの数学で関数を定義するときは, 定義域や値域をきちんと明らかにしていなかったこともあるかと思う. **定義域や値域をきちんと決めること**はとくに注意すること.

注意 2.2.

例 2.2 において, f_1 と f_2, g_1 と g_2 は別の写像として考える必要がある. f_1 も f_2 も同じ x^2 で定まっているから, 同じ写像 (関数) と思うかもしれないが, f_1 と f_2 は定義域が異なっている. このことはとても重要な違いで, f_1 は成り立っているが f_2 では成り立っていない性質がある. 同様に, g_1 と g_2 は同じ x^2 で定まっているが, g_1 と g_2 は値域が異なっている. このこともとても重要な違いであり, g_1 は成り立っているが g_2 では成り立っていない性質がある. どのような性質が成り立っていないのかはあとで説明するが, f_1 と f_2, g_1 と g_2 にどのような違いがあるかを考えてみて欲しい.

問題 2.1.

下記は, 高校までの数学でよく見られる関数の書きかたである. 写像 f と g の定義域と値域を定めて, 写像を定義せよ.

$$f(z) = \frac{z+1}{z-1}, \quad g(w) = \sqrt{1-w^2}$$

注意 2.3.

例 2.2 の書き方は厳密ではあるが, 書くことが面倒でもある. そこで, 次のような書き方もよく使う.

(1) $f_1 : (0,\infty) \to \mathbb{R}$ を

$$f_1(x) := x^2 \quad (x \in (0,\infty))$$

により定義する.[3]

(2) $f_1 : (0,\infty) \to \mathbb{R}$ を $f_1 : (0,\infty) \ni x \mapsto x^2 \in \mathbb{R}$ により定義する. 矢印に縦棒がついていることに注意せよ.[4]

問題 2.2.

例 2.2 の写像 f_2, g_1, g_2 を注意 2.3 の書き方を使って書いてみよ.

例 2.2 の f_1 は f_2 の写像の定義域を $(0,\infty) \subset \mathbb{R}$ に制限することによって得られる. このとき, f_1 を $f_2|_{(0,\infty)}$ と書く. より一般の形で述べよう.

定義 2.2 (制限写像)**.**

集合 X, Y と写像 $f : X \to Y$, 部分集合 $A \subset X$ に対して, f の A による**制限** $f|_A : A \to Y$ を $x \in A$ に対して

$$f|_A(x) := f(x)$$

によって定義する.

第 1 章の定義 1.3 で集合が等しいとはどういうことかを定義した. 同じように, 写像が等しいとはどういうことかを定義しよう.

定義 2.3 (写像の等号)**.**

集合 X, Y に対して, 写像 $f : X \to Y$ と $g : X \to Y$ が等しいとは, 任意の $x \in X$ に対して

$$f(x) = g(x)$$

が成り立つことをいう. このとき $f = g$ と書く ($f \equiv g$ と書くこともある). $f = g$ が成り立たないとき $f \neq g$ と書く.

例 2.2 において, $f_1 \neq f_2$ である. なぜなら, f_1 と f_2 は定義域が違うからである. 同様に $g_1 \neq g_2$ である. なぜなら, g_1 と g_2 の値域が違うからである. 写像の定義域や値域が違うときは, 写像が等しくならないことに注意せよ.

例 2.3 (写像の等号の例)**.**

$f : \mathbb{R} \to \mathbb{R}$ と $g : \mathbb{R} \to \mathbb{R}$ を任意の $x \in \mathbb{R}$ に対して

$$f(x) := \sin^2 x, \quad g(x) := 1 - \cos^2 x$$

により定義する. このとき, $f = g$ である.

[3] $f_1(x) := x^2, \quad x \in (0,\infty)$ と丸括弧を書かなくてもよい.

[4] $\in$ を 90 度回転させて縦書きをすることもある.

証明.

> f と g の定義域, 値域がそれぞれ等しいことは明らかだから, 示すことは, 任意の $x \in \mathbb{R}$ に対して $f(x) = g(x)$ であることである.

f と g の定義域と値域はそれぞれ等しい. 任意の $x \in \mathbb{R}$ に対して, $\sin^2 x + \cos^2 x = 1$ だから

$$f(x) = \sin^2 x = 1 - \cos^2 x = g(x)$$

となるので, $f(x) = g(x)$ がわかる. 従って, $f = g$ となる. □

例 2.4 (写像が等号にならないこと)**.**

$f : \mathbb{R} \to \mathbb{R}$ と $g : \mathbb{R} \to \mathbb{R}$ を任意の $x \in \mathbb{R}$ に対して

$$f(x) := \cos x, \quad g(x) := 1 - \frac{1}{2}x^2$$

により定義する. このとき, $f \neq g$ である.

証明.

> f と g の定義域, 値域はそれぞれ等しいから, 示すことは「任意の $x \in \mathbb{R}$ に対して $f(x) = g(x)$」が成り立たないことである. だから, 「ある $x_0 \in \mathbb{R}$ に対して $f(x_0) \neq g(x_0)$」を示せばよい.

$x_0 = \dfrac{\pi}{2} \in \mathbb{R}$ とおくと,

$$f(x_0) = f\left(\frac{\pi}{2}\right) = 0, \quad g(x_0) = g\left(\frac{\pi}{2}\right) = 1 - \frac{\pi^2}{8} \neq 0 = f(x_0)$$

である. 従って, $f \neq g$ である. □

注意.

もし, $1 - \frac{\pi^2}{8} \neq 0$ であることをきちんと証明したいなら, 例えば, 次のようにすればよいだろう. $\pi > 3$ から $\pi^2 > 9$ となる. 従って,

$$1 - \frac{\pi^2}{8} < 1 - \frac{9}{8} = -\frac{1}{8} < 0$$

だから, 特に $1 - \dfrac{\pi^2}{8} \neq 0$ である. このように, 等しくないことを厳密に証明するのは面倒になることが多い.

次に, 二つの写像から新しい写像を定める方法を述べる.

定義 2.4 (合成写像)**.**

X, Y, Z を集合とし, $f : X \to Y$, $g : Y \to Z$ を写像とする. このとき, f と g の合成写像 $g \circ f : X \to Z$ を $x \in X$ に対して

$$g \circ f(x) := g(f(x))$$

によって定める.

例 2.5.

$f : \mathbb{R} \to (0, \infty)$, $g : (0, \infty) \to \mathbb{R}$ を, 任意の $x \in \mathbb{R}$, $y \in (0, \infty)$ に対してそれぞれ

$$f(x) := x^2 + 1, \qquad g(y) := \log y$$

により定める. このとき, f の値域と g の定義域が等しいことから $g \circ f : \mathbb{R} \to \mathbb{R}$ を定めることができて, 任意の $x \in \mathbb{R}$ に対して

$$g \circ f(x) = g(x^2 + 1) = \log(x^2 + 1)$$

となる. また g の値域と f の定義域が等しいことから, $f \circ g : (0, \infty) \to (0, \infty)$ を定めることができて, 任意の $y \in (0, \infty)$ に対して,

$$f \circ g(y) = f(\log y) = \log^2 y + 1$$

となる. しかし, $g \circ g$ は g の値域と g の定義域が異なる, すなわち $(0, \infty) \neq \mathbb{R}$ だから定めることができない.

注意 2.4.

f も定義域と値域が異なるが, $(0, \infty) \subset \mathbb{R}$ だから, 実は $f \circ f$ を定めることができて, 任意の $x \in \mathbb{R}$ に対して

$$f \circ f(x) = (x^2 + 1)^2 + 1$$

となる. 一般に集合 X, Y, Z, W が $Y \subset Z$ をみたすとき, 写像 $f : X \to Y$ と $g : Z \to W$ の合成 $g \circ f$ を定義することができる.

注意.

行列の掛け算が定義できるか否かは, 実は合成写像が定義できるか否かと関係がある. $m, n, l \in \mathbb{N}$ と $(l \times n)$ 行列 A, $(m \times l)$ 行列 B に対して, 積 BA が定義できるが, 積 AB は $(m \neq n$ であれば$)$ 定義できないのであった. これは写像 $g \circ f$ が定義できても $f \circ g$ が定義できるとは限らないことと同じことを主張している. 行列が線形写像の表現になることを勉強することで, この注意の意味を再確認できるであろう.

問題 2.3.
二つの写像 $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$ を任意の $x \in \mathbb{R}$ に対して

$$f(x) := 3x + 1, \qquad g(x) := \frac{1}{x^2 + 1}$$

で与える. $x \in \mathbb{R}$ に対して, 合成写像 $f \circ g(x)$, $g \circ f(x)$, $f \circ f(x)$, $g \circ g(x)$ を求めよ.

問題 2.4.
写像 f, g の値がそれぞれ

$$f(x) := x + \frac{1}{x}, \quad g(y) := \log(1 + y)$$

となるとする.
(1) f と g の定義域と値域を定めて写像を定義せよ.
(2) $f \circ g$ が定められるように, f と g の定義域と値域を定めよ.
(3) $g \circ f$ が定められるように, f と g の定義域と値域を定めよ.

定理 2.1 (写像の合成に関する結合法則)**.**
集合 X, Y, Z, W と写像 $f : X \to Y$, $g : Y \to Z$, $h : Z \to W$ について

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

が成り立つ.

証明.

定義域と値域がそれぞれ等しいことは明らかだから, 示せばいいことは, 任意の $x \in X$ に対して,

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

である.

$h \circ (g \circ f) = (h \circ g) \circ f$ の定義域と値域はそれぞれ等しい. 任意の $x \in X$ に対して,

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

が成り立つ. よって, $(h \circ (g \circ f))(x) = h(g(f(x))) = ((h \circ g) \circ f)(x)$ だから, とくに $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ がわかる. 従って, $h \circ (g \circ f) = (h \circ g) \circ f$ が成り立つ. □

2.2. 像, 逆像

$f : X \to Y$ を写像とする. このときに, 「$x \in X$ の動く範囲におうじて, $y \in Y$ の動く範囲を求めよ」や「$y \in Y$ の動く範囲におうじて, $x \in X$ の動く範囲を求めよ」という問題は一次関数や二次関数の問題として, 中学, 高校で見たことがあるだろう. このことを集合の記法を用いたものが次の像と逆像である.

定義 2.5 (像, 逆像)**.**
$A \subset X$ に対して,

$$f(A) := \{f(a) \in Y : a \in A\}$$

を f による A の**像**という.
$B \subset Y$ に対して

$$f^{-1}(B) := \{x \in X : f(x) \in B\}$$

を f による B の**逆像**という.

例 2.6.
$f : \mathbb{R} \to (-10, \infty)$ を任意の $x \in \mathbb{R}$ に対して

$$f(x) := x^2$$

で定める. $A_1, A_2 \subset \mathbb{R}$, $B_1, B_2 \subset (-10, \infty)$ を

$$A_1 := [-3, 1],\ A_2 := [-1, 2],\ B_1 := [-1, 1],\ B_2 := [1, 9]$$

で定める. このとき,

$$\begin{aligned}
f(A_1) &= \{f(a) \in [0, \infty) : a \in A_1\} \\
&= \{a^2 \in [0, \infty) : a \in [-3, 1]\} = [0, 9], \\
f(A_2) &= \{f(a) \in [0, \infty) : a \in A_2\} = [0, 4], \\
f^{-1}(B_1) &= \{a \in \mathbb{R} : f(a) \in B_1\} \\
&= \{a \in \mathbb{R} : a^2 \in [-1, 1]\} \\
&= \{a \in \mathbb{R} : -1 \le a^2 \le 1\} = [-1, 1], \\
f^{-1}(B_2) &= \{a \in \mathbb{R} : f(a) \in B_2\} \\
&= \{a \in \mathbb{R} : 1 \le a^2 \le 9\} = [-3, -1] \cup [1, 3]
\end{aligned}$$

となる. 「$f(A_1)$ は $-3 \le x \le 1$ を動くときに $y = f(x) = x^2$ が動く範囲」を表している. また, 「$f^{-1}(B_1)$ は $-1 \le y \le 1$ を動くときに $y = f(x) = x^2$ で x が動く範囲」を表している.

問題 2.5.

例 2.6 と同じ記号を用いる. $g : \mathbb{R} \to \mathbb{R}$ を任意の $x \in \mathbb{R}$ に対して

$$g(x) := x^3$$

で定義する. このときに, $g(A_1)$, $g(A_2)$, $g^{-1}(B_1)$, $g^{-1}(B_2)$ を求めよ.

定理 2.2.

$f : X \to Y$ を写像とし, $A_1, A_2 \subset X$, $B_1, B_2 \subset Y$ とする. このとき, 次が成り立つ:

(1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$;
(2) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$;
(3) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;
(4) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;
(5) $A_1 \subset f^{-1}(f(A_1))$;
(6) $f(f^{-1}(B_1)) \subset B_1$;
(7) $f(A_1) \setminus f(A_2) \subset f(A_1 \setminus A_2)$;
(8) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$.

証明.

(1) **1.** $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$ を示す. 任意の $y \in f(A_1 \cup A_2)$ に対して, ある $x \in A_1 \cup A_2$ が存在して, $y = f(x)$ と書ける. 「$x \in A_1$ または $x \in A_2$」だから, 「$f(x) \in f(A_1)$ または $f(x) \in f(A_2)$」が成り立つ. 従って, $y = f(x) \in f(A_1) \cup f(A_2)$ が成り立つ.

2. $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$ を示す. 任意の $y \in f(A_1) \cup f(A_2)$ に対して, 「$y \in f(A_1)$ または $y \in f(A_2)$」が成り立つから,

「$x_1 \in A_1$が存在して $y = f(x_1)$」または「$x_2 \in A_2$が存在して $y = f(x_2)$」

が成り立つ. $x_1 \in A_1$ が存在して $y = f(x_1)$ ならば, $A_1 \subset A_1 \cup A_2$ より, $x_1 \in A_1 \cup A_2$ だから, $y = f(x_1) \in f(A_1 \cup A_2)$ となる. 同様にして, $x_2 \in A_2$ が存在して, $y = f(x_2)$ ならば, $A_2 \subset A_1 \cup A_2$ を使って, $y = f(x_2) \in f(A_1 \cup A_2)$ がわかる. 従って, どちらの場合でも, $y \in f(A_1 \cup A_2)$ が成り立つ.

(2) (1) の証明にならって, 各自, 証明せよ. (1) と違い, 等号が成立しないことに注意.

(3) あとの (4) の証明にならって, 各自, 証明せよ.

(4) **1.** $f^{-1}(B_1 \cap B_2) \subset f^{-1}(B_1) \cap f^{-1}(B_2)$ を示す. 任意の $x \in f^{-1}(B_1 \cap B_2)$ に対して, $f(x) \in B_1 \cap B_2$ が成り立つ. よって, 「$f(x) \in B_1$ かつ $f(x) \in B_2$」が成り立つから, 「$x \in f^{-1}(B_1)$ かつ $x \in f^{-1}(B_2)$」となる. 従って, $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$ が成り立つ.

2. $f^{-1}(B_1) \cap f^{-1}(B_2) \subset f^{-1}(B_1 \cap B_2)$ を示す. 任意の $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$ に対して,「$x \in f^{-1}(B_1)$ かつ $x \in f^{-1}(B_2)$」が成り立つことから,「$f(x) \in B_1$ かつ $f(x) \in B_2$」が成り立つ. よって, $f(x) \in B_1 \cap B_2$ となるから, $x \in f^{-1}(B_1 \cap B_2)$ となる.

(5) 任意の $x \in A_1$ に対して, 示したいことは $x \in f^{-1}(f(A_1))$ だから, $f(x) \in f(A_1)$ であることを示せばよい. $x \in A_1$ だったから, $f(x) \in f(A_1)$ は成立する. 従って, $x \in f^{-1}(f(A_1))$ も成立する.

(6) 任意の $y \in f(f^{-1}(B_1))$ に対して, ある $x \in f^{-1}(B_1)$ がとれて, $y = f(x)$ と書ける. また, $x \in f^{-1}(B_1)$ だから, $f(x) \in B_1$ が成り立つ. 従って, $y = f(x) \in B_1$ が成り立つ.

(7) 各自, 証明せよ.

(8) 各自, 証明せよ.

□

質問と答え.

$f(A_1 \cup A_2) \supset f(A_1) \cup f(A_2)$ の証明のときは, 任意の $y \in f(A_1) \cup f(A_2)$ に対して

「$x_1 \in A_1$が存在して $y = f(x_1)$」または「$x_2 \in A_2$が存在して $y = f(x_2)$」

のように $x_1, x_2 \in X$ の 2 つの文字がでてきました. しかし, $f^{-1}(B_1) \cap f^{-1}(B_2) \subset f^{-1}(B_1 \cap B_2)$ の証明のときには, 任意の $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$ に対して,「$y_1 = f(x)$ かつ $y_2 = f(x)$」と 2 つの文字を出すことはありませんでしたがなぜかという質問がありました. この質問に答えるには「関数, 写像とはなにか？」にたちかえる必要があります.

任意の $y \in f(X)$ にたいして, $y = f(x)$ となる $x \in X$ は **1 つとは限りません.** 例 2.6 で $1 \in f(A_1)$ ですが, $1 = f(a)$ となる $a \in A_1$ は $a = +1$ と $a = -1$ の 2 つがあります. ですから, $y \in f(A_1) \cup f(A_2)$ に対して「$y \in f(A_1)$ または $y \in f(A_2)$」となりますが, このときに x_1 と x_2 **が同じになるかどうかわからないので文字を 2 つ使ったのです.** これを文字 1 つで記述してしまうと, x_1 と x_2 が違う場合を証明することができなくなってしまいます.

これに対して, $x \in X$ を決めると $f(x)$ **はただ一つに決まります.** これは関数や写像が持つ重要な性質です. $x \in f^{-1}(B_1) \cap f^{-1}(B_2)$ としたときに,「$x \in f^{-1}(B_1)$ かつ $x \in f^{-1}(B_2)$」となりますが,「$y_1 = f(x) \in B_1$ かつ $y_2 = f(x) \in B_2$」としなくてもよいのは, $y_1 = f(x) = y_2$, つまり $y_1 = y_2$ となってしまうからです.

問題 2.6.

定理 2.2 において, (2), (3), (7), (8) を証明せよ.

注意 2.5.

定理 2.2 の (2), (5), (6), (7) について, 等号は一般に成立しないことを説明しよう. 例 2.6 の f, $A_1 = [-3, 1]$, $A_2 = [-1, 2]$, $B_1 = [-1, 1]$ について

$$\begin{aligned} f(A_1 \cap A_2) &= f([-1, 1]) = [0, 1] \\ f(A_1) \cap f(A_2) &= [0, 9] \cap [0, 4] = [0, 4] \neq f(A_1 \cap A_2) \\ f^{-1}(f(A_1)) &= f^{-1}([0, 9]) = [-3, 3] \neq A_1 \\ f(f^{-1}(B_1)) &= f([1, 1]) = [0, 1] \neq B_1 \\ f(A_1) \setminus f(A_2) &= [0, 9] \setminus [0, 4] = (4, 9] \\ f(A_1 \setminus A_2) &= f([-3, 1)) = (1, 9] \neq f(A_1) \setminus f(A_2) \end{aligned}$$

となり, 一般に等号が成立しないことがわかる.

問題 2.7.

注意 2.5 のそれぞれの集合の等号を確認せよ.

2.3. 全射, 単射, 逆写像

先の例 2.6 において, $f(1) = f(-1) = 1$ であった. つまり, $1 \in \mathbb{R}$ に対して, $f(x) = 1$ となる $x \in \mathbb{R}$ が二つ (以上) あることになる. つまり, $y = 1$ に対しては, $y = f(x)$ となる x が二つ以上あるから, **逆関数が作れない**ことになる. 逆関数 (より正確には逆写像) が定められるためには写像 f になんらかの条件を課さないといけない. この節では, 逆写像が作れるための条件を考えることにする.

定義 2.6 (単射)**.**

X, Y を集合, $f : X \to Y$ を写像とする. f が**単射**であるとは, 任意の $x_1, x_2 \in X$ に対して $f(x_1) = f(x_2)$ ならば $x_1 = x_2$ が成り立つことをいう[5].

注意 2.6 (間違いやすい例)**.**

単射の定義で「$f(x_1) = f(x_2)$ ならば $x_1 = x_2$ が成り立つ」を「$x_1 = x_2$ ならば $f(x_1) = f(x_2)$ が成り立つ」と, **仮定と結論を逆にしてはいけない.**

注意 2.7.

単射が成り立たないことは, 「ある $x_1, x_2 \in X$ が存在して, $f(x_1) = f(x_2)$

[5]「任意の $x_1, x_2 \in X$ に対して $f(x_1) = f(x_2)$ を**仮定すると** $x_1 = x_2$ が成り立つこと」としてもよい.

かつ $x_1 \neq x_2$」となることである. 一般に「P ならば Q」の否定は, 「P が成り立つが Q が成り立たない」になる[6]. 詳しくは第 3 章で説明する.

注意 2.8.

$f : X \to Y$ が単射であることは, 次と同値である.

(1) 任意の $x_1, x_2 \in A$ に対して,

$$x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$$

が成り立つ. これは, 定義の「ならば」に対して対偶をとったものであり, 意味は定義よりもわかりやすいだろう. しかし, 証明にはあまり向かない. なぜなら, **等しくないことを示すのは, 等しいことを示すよりも難しいことが多いからである**.

(2) 任意の $y \in Y$ に対して, $f^{-1}(\{y\})$ はたかだか一点の集合となる. これをみると, 逆像の記号が逆写像の記号となっていてもそれほど不思議ではないことがわかるだろう. ただし, $f^{-1}(\{y\})$ は空集合もありうる.

例 2.7.

例 2.2 の $f_1 : (0, \infty) \to \mathbb{R}$, $f_2 : \mathbb{R} \to \mathbb{R}$ を例にする. すなわち

$$f_1(x) := x^2 \quad (x \in (0, \infty))$$
$$f_2(x) := x^2 \quad (x \in \mathbb{R})$$

とする. このとき, f_1 は単射であり, f_2 は単射でない.

注意 2.9.

例 2.7 でわかるとおり, 写像の定義域と値域を定めることは重要である. 定義域と値域をきちんと定めないと単射になるか否かを考えることができない.

例 2.7 の証明.

1. f_1 が単射になることを示す.

> 示すことは, 任意の $x_1, x_2 \in (0, \infty)$ に対して, $f_1(x_1) = f_1(x_2)$ **を仮定して,** $x_1 = x_2$ が成り立つことである.

[6]「P ならば Q」ということは, 「P を仮定すると Q が必ず成り立つ」ということである. これが成り立たないということは, 「仮定 P は成立しているが結論 Q は成り立たない」ということになる. もう少し具体的に, 例えば「テストで 90 点以上をとったならば成績が S である」が正しくないとはどういうことになるのか考えてみて欲しい. 85 点だった人の成績が S であるのは, 嘘をつかれたことになるのだろうか？

任意の $x_1, x_2 \in (0, \infty)$ に対して, $f_1(x_1) = f_1(x_2)$ を仮定すると, $x_1^2 = x_2^2$ だから, $(x_1 + x_2)(x_1 - x_2) = 0$ である. ここで, $x_1, x_2 > 0$ **だから** $x_1 + x_2 \neq 0$ であり, $x_1 - x_2 = 0$ が従う. よって, $x_1 = x_2$ が成り立つから, f_1 は単射である.

2. f_2 が単射にならないことを示す.

> 単射でないことを示すには, 否定を示せばよい. つまり, 示すことは「ある $x_1, x_2 \in \mathbb{R}$ が存在して, $f_2(x_1) = f_2(x_2)$ だが $x_1 \neq x_2$」となることである.

$x_1 := 1$, $x_2 := -1 \in \mathbb{R}$ とすると $f_2(x_1) = f_2(1) = f_2(-1) = f_2(x_2)$ だが, $x_1 = 1 \neq -1 = x_2$. よって, f_2 は単射でない. □

注意 2.10.

例 2.7 の単射性の証明は $f(x_1) = f(x_2)$ を仮定して $x_1 = x_2$ を示したが, この証明方法は**「何かが唯一つ存在する」**の証明をするときによく使う方法である. 実際に「何か」が二つ存在したとして, その二つが等しいことを示すことで存在は唯一つということがわかる. このように**唯一つ存在する**を論理記号では $\exists 1$ とか $\exists !$ と書く.

単射の場合では, 写像の値に対する定義域の点が一つしかないことを主張している. 実際に値が同じ点が二つあったとして, その二つが等しいことを示しているので, 写像の値に対する定義域の点が一つしかないことがわかる.

問題 2.8.

X, Y を集合, $f : X \to Y$ を単射とする. このとき, $A_1, A_2 \subset X$ に対して, $f(A_1) \cap f(A_2) \subset f(A_1 \cap A_2)$, $f^{-1}(f(A_1)) \subset A_1$ を示せ. 従って, 単射性は定理 2.2 の (2), (5) の等号が成立する十分条件になっている.

さて, 注意 2.8 において, f が単射であっても, 任意の $y \in Y$ に対して, $f^{-1}(\{y\}) = \emptyset$ がありうることを述べた. 逆写像を作るためには, 任意の $y \in Y$ に対して $y = f(x)$ となる $x \in X$ が存在しなければならない. この性質を述べる.

定義 2.7 (全射)**.**

X, Y を集合, $f : X \to Y$ を写像とする. f が**全射**であるとは, 任意の $y \in Y$ に対して, ある $x \in X$ が存在して $y = f(x)$ が成り立つことをいう.

注意 2.11 (間違いやすい例)**.**

全射の定義で「任意の $y \in Y$ に対して, ある $x \in X$ が存在して」を「ある $x \in X$ が存在して, 任意の $y \in Y$ に対して」と**順序をかえてはいけない.** また,

「任意の $x \in X$ に対してある $y \in Y$ が存在して」と X と Y の役割をかえてはいけない.

注意 2.12.

全射が成り立たないことは, 「任意の $y \in Y$ に対して, ある $x \in X$ が存在して $y = f(x)$」が成り立たないことである. 「任意」を「ある」, 「ある」を「任意」にかえればよかったことに注意すると, 全射が成り立たないことは「ある $y \in Y$ が存在して, 任意の $x \in X$ に対して $y \neq f(x)$」となる.

注意 2.13.

$f : X \to Y$ が全射であることと $f(X) = Y$ が成り立つことは同値である.

問題 2.9.

写像 $f : X \to Y$ について, 次を示せ.

(1) f が全射ならば, $f(X) = Y$ が成り立つ.

(2) $f(X) = Y$ ならば f は全射である.

例 2.8.

例 2.2 の $g_1 : \mathbb{R} \to [0, \infty)$, $g_2 : \mathbb{R} \to \mathbb{R}$ を考える. すなわち

$$g_1(x) := x^2 \quad (x \in \mathbb{R}),$$
$$g_2(x) := x^2 \quad (x \in \mathbb{R})$$

を考える. このとき, g_1 は全射であり, g_2 は全射ではない.

例 2.8 の証明.

1. g_1 が全射となることを示す.

> 示すことは「任意の $y \in [0, \infty)$ に対して, $y = g_1(x) = x^2$ となる $x \in \mathbb{R}$ を**みつけること**」である.

任意の $y \in [0, \infty)$ に対して, $y = g_1(x)$ を $x \in \mathbb{R}$ について解いてみる. すると, $y = x^2$ だから, $x = \sqrt{y}$ または, $x = -\sqrt{y}$ となる. この考察をもとにして, きちんとした証明を書く.

任意の $y \in [0, \infty)$ に対して,

$$x := \sqrt{y} \in \mathbb{R}$$

とおくと,

$$g_1(x) = x^2 = (\sqrt{y})^2 = y$$

となる. 従って, g_1 は全射である.

2. g_2 が全射でないことを示す.

> 示すことは, 全射の否定だから, 「ある $y \in \mathbb{R}$ が存在して, 任意の $x \in \mathbb{R}$ に対して, $g_2(x) = x^2 \neq y$」である.

$y := -1 \in \mathbb{R}$ とすると, 任意の $x \in \mathbb{R}$ に対して $g_2(x) = x^2 \geq 0$ だから, $g_2(x) = -1$ とならない. すなわち, $g_2(x) \neq y$ となる. 従って, g_2 は全射ではない. □

問題 2.10.
X, Y を集合, $f : X \to Y$ を全射とする. このとき, $B \subset Y$ に対して, $B \subset f(f^{-1}(B))$ を示せ. 従って, 全射性は定理 2.2 で (6) の等号が成立する条件となっている.

さて, $f : X \to Y$ が全単射であるとは, f が全射かつ単射であるときをいう. このときは, 全射の性質より, 任意の $y \in Y$ に対して, $f(x) = y$ となる $x \in X$ がとれる. さらに単射の性質より, この x はひとつしかない (一意であるという). 従って, $y \in Y$ に対してただ一つの $x \in X$ がとれて, $y = f(x)$ とできる. そこで, この対応を考える.

定義 2.8 (逆写像)**.**
X, Y を集合, $f : X \to Y$ を全単射とする. このとき, f の逆写像 $f^{-1} : Y \to X$ を $y \in Y$ に対して, $f(x) = y$ となる $x \in X$ により定める.

$f : X \to Y$ を全単射, $f^{-1} : Y \to X$ を f の逆写像とすると, 任意の $x \in X$ と $y \in Y$ に対して

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = x, \tag{2.1}$$

$$f \circ f^{-1}(y) = f(f^{-1}(y)) = y \tag{2.2}$$

が成り立つ (各自). この関係式 (2.1), (2.2) が逆写像のもつ重要な性質である[7].

例 2.9.
逆写像の例を述べる. また, 単射であれば, 逆写像を構成することもできる例を述べる.

---

[7] f を 3 次行列 A, x, y を 3 次元縦ベクトル $\vec{x}, \vec{y}$ とすると, (2.1) と (2.2) は $A^{-1}A\vec{x} = E\vec{x} = \vec{x}$, $AA^{-1}\vec{y} = E\vec{y} = \vec{y}$ とよく似ている (E は 3 次単位行列). これは偶然ではなく, 「行列は (線形) 写像を表現したもの」という線形代数学の深い事実に基づいている.

- $f : (0,\infty) \to (0,\infty)$ を任意の $x \in (0,\infty)$ に対して $f(x) := x^2$ で定めると, f は全単射になる (各自, 確かめよ). 従って, f の逆写像 $f^{-1} : (0,\infty) \to (0,\infty)$ を定義することができる. 実際, よく知られているように, $y \in (0,\infty)$ に対して, $f^{-1}(y) = \sqrt{y}$ である.
- $g : (0,\infty) \to \mathbb{R}$ を, $x \in (0,\infty)$ に対して, $g(x) = x^2$ で定めると, g は単射であるが, 全射ではない (各自, 確かめよ). しかし, $y \in g((0,\infty))$ に対して, $g(x) = y$ をみたす $x \in (0,\infty)$ は一意に決まる. このことから, $h : g((0,\infty)) \to (0,\infty)$ を $y \in g((0,\infty))$ に対して, $g(x) = y$ をみたす $x \in (0,\infty)$ として定めることができる. この写像 h を g^{-1} と書くことがある.

例 2.10.
$\exp : \mathbb{R} \to (0,\infty)$ を $x \in \mathbb{R}$ に対して

$$\exp(x) := e^x$$

と定義すると, exp は全単射になる. exp の逆写像 (逆関数) は対数関数 $\log : (0,\infty) \to \mathbb{R}$ であった[8]. 実際に, $x \in \mathbb{R}$, $y \in (0,\infty)$ に対して

$$\log(\exp(x)) = \log(e^x) = x$$
$$\exp(\log(y)) = e^{\log y)} = y$$

が成り立つ.

例 2.11.
$\sin : \mathbb{R} \to \mathbb{R}$ は単射にも全射にもならない (各自). しかし, 定義域を $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ に制限した制限写像 $\sin|_{[-\frac{\pi}{2},\frac{\pi}{2}]} : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to \mathbb{R}$ が単射になることと $\sin|_{[-\frac{\pi}{2},\frac{\pi}{2}]}\left(\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]\right) = [-1,1]$ となることを用いて, sin の逆関数である逆正弦関数 $\arcsin : [-1,1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ を定めることができる. つまり, $x \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, $y \in [-1,1]$ に対して

$$\arcsin(\sin x) = x$$
$$\sin(\arcsin y) = y$$

をみたすように arcsin を定義する. このときに, $x \in \mathbb{R}$ に対して

$$\arcsin(\sin x) = x$$

[8]対数関数の真数条件は exp の $\mathbb{R}$ による像 $\exp(\mathbb{R})$ が $\exp(\mathbb{R}) = (0,\infty)$ となることからきている

とはならないことに注意すること. 実際に

$$\arcsin\left(\sin\left(\frac{3}{4}\pi\right)\right) = \arcsin\left(\frac{1}{\sqrt{2}}\right) = \frac{1}{4}\pi \neq \frac{3}{4}\pi$$

である.

逆写像に関する関係式 (2.1), (2.2) をみたすような写像がみつかったときに, 写像 f が逆写像を持つのだろうか？これに答えるのが次の定理 2.3 である.

定理 2.3.
X, Y を集合, $f : X \to Y$, $g : Y \to X$ を写像とする. 任意の $x \in X$ に対して, $g \circ f(x) = x$ が成り立つならば, g は全射であり, f は単射である.

系 2.1.
X, Y を集合, $f : X \to Y$, $g : Y \to X$ を写像とする. 任意の $x \in X$ と $y \in Y$ に対して, $g \circ f(x) = x$ かつ $f \circ g(y) = y$ が成り立つならば, f は全単射であり, $f^{-1} = g$ となる.

定理 2.3 の証明.
1. f が単射であることを示す. 任意の $x_1, x_2 \in X$ に対して, $f(x_1) = f(x_2)$ と仮定する. このとき, $g \circ f(x_1) = x_1$ かつ $g \circ f(x_2) = x_2$ より $x_1 = g \circ f(x_1) = g \circ f(x_2) = x_2$ だから, $x_1 = x_2$ が成り立つ.
2. g が全射であることを示す. 任意の $x \in X$ に対して, $y = f(x) \in Y$ とおくと, $g \circ f(x) = x$ より, $g(y) = g(f(x)) = g \circ f(x) = x$ となる. □

問題 2.11.
系 2.1 を証明せよ.

問題 2.12.
集合 X, Y, Z と写像 $f : X \to Y$, $g : Y \to Z$ に対して, 次を示せ.
(1) $g \circ f$ が単射であれば, f は単射である.
(2) $g \circ f$ が全射であれば, g は全射である.

問題 2.13.
$a < b$ に対して, 閉区間 $[0, 1]$ から閉区間 $[a, b]$ への全単射, および開区間 $(0, 1)$ から開区間 (a, b) への全単射を与える関数を構成せよ (ヒント:一次関数を考えよ).

問題 2.14.
A を実数値 n 次正則行列とし, $f : \mathbb{R}^n \to \mathbb{R}^n$ を任意の $x \in \mathbb{R}^n$ に対して

$$f(x) := Ax$$

により定義する.

(1) f が全単射であることを示せ.
(2) f^{-1} を求めよ.

2.4. 応用: 指数関数, 三角関数の定義

この節では, 黒田 [**7**] に従った指数関数, 三角関数の定義について説明する. 高校での指数関数, 三角関数は図や (厳密に定義されていない) 極限に頼った定義であり, 厳密な議論の上には定義されていなかった. そのために, 三角関数や指数関数の微分を計算するときに, 直感に頼った計算をせざるを得なかった. ここでは, 微分積分学におけるいくつかの知識を認めて, 全単射を用いて指数関数の定義を述べる.

まず, 全単射を示すために有用な結果を一つ述べよう.

定理 2.4.

$I = [a, b] \subset \mathbb{R}$ を閉区間, $f : I \to \mathbb{R}$ は連続な狭義単調増加関数とする. このとき, f は単射となり, $f(I)$ は閉区間となる. よって, $g : I \to f(I)$ を任意の $x \in I$ に対して $g(x) = f(x)$ と定義すると, g は全単射となる.

問題 2.15.

定理 2.4 を証明せよ. 証明には, 中間値の定理が必要になる.

2.4.1. 指数関数と対数関数. 自然対数 $e > 0$ はわかっているものとする. $x \in \mathbb{R}$ に対して, 指数関数 e^x はどのように定義すればよいのであろうか？高校数学は, おおよそ次のステップで定義をしていた.

1. 指数法則より $e^2 = e^{1+1} = e^1 e^1 = e \cdot e$, $e^3 = e^{1+1+1} = e \cdot e \cdot e$, $e^4 = \cdots$ **となるように**, $n \in \mathbb{N}$ に対して, e^n を定義する.
2. 指数法則より $e^0 e^1 = e^{0+1} = e$ **となるべき**だから, $e^0 = 1$ と定義する.
3. 指数法則より, $e^{-1}e^1 = e^{-1+1} = e^0 = 1$ **となるべき**だから, $e^{-1} = \dfrac{1}{e}$ と定義する.
4. 指数法則より, $n \in \mathbb{N}$ に対して $(e^{\frac{1}{n}})^n = e^1$ **となるべき**ことを使って, $e^{\frac{1}{n}}$ を定義する.
5. 指数法則より, $n, m \in \mathbb{N}$ に対して $e^{\frac{n}{m}} = (e^{\frac{1}{m}})^n$ **となるべき**ことを使って, $q \in \mathbb{Q}$ に対して, e^q を定義する.
6. 指数関数は**連続になるべき**ことを使って $x \in \mathbb{R}$ に対して e^x を定義する.

つまり, 根底には**指数法則**と**連続性**が成り立つことを仮定して指数関数を定義しているのである. しかし, 指数法則は指数関数から得られるはずのものである. 指数法則を使って指数関数を定義してしまうと, 循環論法に陥いる可能

性もある. また, 指数関数は連続になるべきことを使って, たとえば, $e^{\sqrt{2}}$ を定義するのであるが, このときに, $e^{\sqrt{2}}$ **がきちんと定まるかを考えなければいけない**. さらに, 指数関数の微分を定義から計算するときに, Napier 数 e の定義に戻る必要があるが, Napier 数 e の定義には, 実数の完備性, すなわち Cauchy 列が収束することを用いらなければいけない. つまり, 上記の定義の仕方は**直感的にはわかりやすいのだが**, 厳密な議論をするときには注意をしなければいけないことが多々あるのである.

さて, 指数関数と対数関数については, よく知られているように,

$$g \circ f(x) = \log(e^x) = x \quad (x \in \mathbb{R})$$
$$f \circ g(y) = e^{\log y} = y \quad (y \in (0, \infty))$$

が成り立つ. ここで, $\dfrac{d}{dy} \log y = \dfrac{1}{y}$ だから, 微分積分学の基本定理を用いると

$$\log y = \int_1^y \frac{1}{x}\, dx$$

である. このことを用いて, 対数関数を定義しよう.

定義 2.9 (指数関数, 対数関数)**.**

$\log : (0, \infty) \to \mathbb{R}$ を任意の $y \in \mathbb{R}$ に対して

$$\log y = \int_1^y \frac{1}{x}\, dx$$

で定義する. このとき, log は連続で狭義単調増加だから, 定理 2.4 から全単射になる. そこで, 指数関数 $\exp : \mathbb{R} \to (0, \infty)$ を log の逆関数により定義する.

なお, 対数関数と対数関数を定義すれば, 正の実数の巾乗が定義できることに注意しておこう. 実際に $a > 0$ に対して, $a^x = e^{x \log a}$ だから, これを定義として採用すればよい. すると, $2^{\sqrt{2}}$ など, 無理数の巾乗を $2^{\sqrt{2}} = e^{\sqrt{2} \log 2}$ と定義することができる.

ここで重要なことは, 指数関数と対数関数が**分数関数とその積分だけで定義できている**ことである. 積分は**指数法則や連続性とは無関係**に定義ができる. そして, この定義から, 実際に「指数関数が指数法則をみたすこと」や「指数関数が連続であること」を**証明することができる.**

例 2.12.

$x \in \mathbb{R}$ に対して, $\dfrac{d}{dx} \exp(x) = \exp(x)$ を示してみよう. 逆関数に関する微分

公式から $y = \exp(x)$ とおくと, 微積分の基本定理より

$$\frac{d}{dx}\exp(x) = \frac{1}{\frac{d}{dy}\log y} = \frac{1}{\frac{1}{y}} = y = \exp(x)$$

となる.

2.4.2. 三角関数. 三角関数についても, 指数関数と同じように積分を使って定義する. 円の方程式 $x^2 + y^2 = 1$ を $y \geq 0$ のもとで解くと $y = \sqrt{1 - x^2}$ であるが, このとき, 円上の点 (x, y) と $(1, 0)$ のなす角を $\theta(x)$ と書くとラジアンの定義から, $\theta(x)$ は $(1, 0)$ から (x, y) までの長さであった. これを積分で表すと

$$\theta(x) := \int_x^1 \sqrt{1 + \left(\frac{dy}{dx}(t)\right)^2}\, dt = \int_x^1 \frac{1}{\sqrt{1 - t^2}}\, dt$$

となる. ところで, $x = \cos\theta(x)$ だったから, θ は cos の逆関数である. さらに, 単位円の弧長は 2π だったから, $(1, 0)$ から $(-1, 0)$ までの長さが π, すなわち $\theta(-1) =: \pi$ となる. 以上をまとめて, 次の定義を得る.

定義 2.10 (余弦関数, 逆余弦関数)**.**
$\arccos : [-1, 1] \to [0, \pi]$ を $y \in [-1, 1]$ に対して

$$\arccos(y) := \int_y^1 \frac{1}{\sqrt{1 - x^2}}\, dx$$

により定義する. この関数 arccos は連続で狭義単調減少関数だから, 定理 2.4 を用いると全単射になることがわかる. そこで, $\cos : [0, \pi] \to [-1, 1]$ を arccos の逆関数で定義し, 偶関数になるように周期的に $\mathbb{R}$ に拡張する.

次に, sin を定義する. $\cos^2 x + \sin^2 x = 1$ であり, $0 \leq x \leq \pi$ で $\sin x \geq 0$ だから, $\sin x = \sqrt{1 - \cos^2 x}$ と定義すればよい.

定義 2.11 (正弦関数, 逆正弦関数)**.**
$\sin : [0, \pi] \to [-1, 1]$ を $x \in [0, \pi]$ に対して

$$\sin x := \sqrt{1 - \cos^2 x}$$

により定義する. そして, 奇関数になるように周期的に $\mathbb{R}$ に拡張する. このとき, $\sin : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1]$ は全単射になることがわかるので, この逆関数を $\arcsin : [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ と書く[9].

[9]逆正弦関数や逆余弦関数をすっきりした形で与えるには, 多価関数の理論が必要である. これについては, 複素関数論 (例えば Ahlfors [**14**]) を勉強されたい.

「周期的に拡張する」方法や, 三角関数の諸性質 (加法定理など) は黒田 [**7**] を見よ. 微分積分を論理的に組み立てるには, 何らかの方法で指数関数や三角関数を定義しなければいけない.

なお, Taylor 展開を用いた初等関数の定義の仕方もある. 例えば, 高木 [**9**] などを参照せよ. また, これらの話題は複素数を導入すると, 非常に綺麗な説明ができる. 例えば Ahlfors [**14**] を参照せよ.

2.5. 演習問題

問題 2.16.

$X := \{f : \mathbb{R} \to \mathbb{R}\}$, すなわち, $\mathbb{R}$ から $\mathbb{R}$ への関数全体とし, $f, g \in X$ と $\alpha \in \mathbb{R}$ に対して和 $f+g$ とスカラー倍 αf を $x \in \mathbb{R}$ に対して

$$(f+g)(x) := f(x) + g(x), \qquad (\alpha f)(x) := \alpha f(x)$$

により定義する. このとき X が $\mathbb{R}$ 上の線形空間となることを示せ. すなわち, 次の 8 条件をみたすことを示せ.

(1) (結合法則) 任意の $f, g, h \in X$ に対して $(f+g)+h = f+(g+h)$
(2) (交換法則) 任意の $f, g \in X$ に対して $f+g = g+f$
(3) ある写像 $O \in X$ が存在して, 任意の $f \in X$ に対して $O+f = f$
(4) 任意の $f \in X$ に対して, ある $g \in X$ が存在して $f+g = O$
(5) 任意の $f \in X$ と $\alpha, \beta \in \mathbb{R}$ に対して $(\alpha+\beta)f = \alpha f + \beta f$
(6) 任意の $f, g \in X$ と $\alpha \in \mathbb{R}$ に対して $\alpha(f+g) = \alpha f + \alpha g$
(7) 任意の $f \in X$ と $\alpha, \beta \in \mathbb{R}$ に対して $(\alpha\beta)f = \alpha(\beta f)$
(8) 任意の $f \in X$ に対して, $1f = f$

問題 2.17.

X, Y を**空でない**集合とし, $\pi : X \times Y \to X$ を $(x, y) \in X \times Y$ に対して

$$\pi(x, y) := x$$

で定める. π は全射であることを示せ. この π を**射影** という (ヒント: 空でないことを強調するのには意味がある. よくよく考えてみると実はあたりまえな主張だが, 証明を正しく書こうとすると, 少しやっかいになる).

問題 2.18.

A を実数値 n 次正方行列とし, $f : \mathbb{R}^n \to \mathbb{R}^n$ を $x \in \mathbb{R}^n$ に対して

$$f(x) := Ax$$

により定義する.

(1) f が全射ならば f は単射になることを示せ (ヒント: まず A が正則であることを示せ.).
(2) f が単射ならば f は全射になることを示せ (ヒント: $\vec{e}_1, \ldots, \vec{e}_n \in \mathbb{R}^n$ を単位ベクトルとするときに, $f(\vec{e}_1), \ldots, f(\vec{e}_n)$ が線形独立になることを示せ. 次に, 任意の $\vec{y} \in \mathbb{R}^n$ に対して, $f(\vec{e}_1), \ldots, f(\vec{e}_n), \vec{y}$ が線形従属となることを用いよ).

第 3 章

命題論理と述語論理

第 1 章の注意 1.14 でも述べた通り, 定理 1.4 の証明はやや煩雑であった. それは, 論理学の知識を仮定せずに証明を試みたからであった. この章では, 記号論理学の初歩を説明し, 数学における様々な記述を論理記号を用いて表現してみる. この章については, $\forall$ と $\exists$ の記号を積極的に用いる. 講義の板書やノートでは, これらの記号を使えるようにして欲しい.

3.1. 命題論理

定義 3.1 (命題)**.**
正しいか正しくないかを**客観的**に判断できる主張を**命題**という. 英語では Proposition という. 頭文字をとって, $p, q, r, \ldots$ で表すことが多い.

例 3.1.
数学では命題以外を扱うことはあまりない (と思われる). 少なくとも, 学部の授業では命題以外を扱うことはまずないので, あまり心配をする必要はない.

(1) p:「$1+1=2$」は命題である.
(2) q:「$1+1=3$」は命題である. 内容が正しいか否かと, 命題となるか否かは別であることに注意せよ.
(3) e:数列 $\{a_n\}_{n=1}^{\infty}$ と実数 a に対して, 「n をおおきくしたときに a_n は a に近づく」は命題ではない. n を大きくしたときの大きい n はいくつだろうか? a_n が a に近づくということについて, 近いとはどういうことだろうか? これらは客観的な表現ではない. このことを客観的に述べるために ε-N 論法がうまれたのである.

定義 3.2 (真偽, 真理値)**.**
命題が正しいことを**真**といい, 正しくないことを**偽**という. 真のときは T(True の頭文字) とか 1, 偽のときは F(False の頭文字) とか 0 と略記し, **真理値**という (真偽値ではない).

例 3.2.
例 3.1 において, p の真理値は T, q の真理値は F である.

定義 3.3 (否定)**.**
命題 p に対して, 「p でない」という命題を p の**否定**といい, $\neg p$ と書く.

例 3.3.
例 3.1 の p, q について
(1) $\neg p$: 「$1+1 \neq 2$」
(2) $\neg q$: 「$1+1 \neq 3$」
である.

定義 3.4 (真理表)**.**
命題同士の真理値の対応関係を示した表を**真理表**という.

例 3.4.
命題 p とその否定 $\neg p$ に関する真理表は次の通り

p	$\neg p$
T	F
F	T

定義 3.5 (論理和, 論理積)**.**
命題 p, q に対して, 「p または q」を p と q の**論理和**といい, $p \vee q$ と書く. 「p かつ q」を p と q の**論理積**といい, $p \wedge q$ と書く.

注意 3.1.
記号 $\vee$, $\wedge$ は別の意味で使うこともある. 数学の分野によって, 記号の違いがおこることはよくある

例 3.5.
命題 p, q に対して, $\neg p$ と $\neg q$, $p \vee q$, $\neg(p \vee q)$, $\neg p \wedge \neg q$ の真理表を書くと次のようになる.

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

定義 3.6 (同値)**.**
命題 p, q の真理値がすべて等しいとき, p と q は**同値**であるといい, $p \Leftrightarrow q$ とか $p \underset{\text{同値}}{\Leftrightarrow} q$ と書く.

定理 3.1 (de Morgan の法則)**.**
命題 p, q に対して, 次が成り立つ.

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

(1) については, 例 3.5 によって明らかであろう. (2) については各自, 真理表を作って確かめてみよ.

定義 3.7 (含意, 条件命題)**.**
命題 p, q に対して, $\neg p \vee q$ を $p \to q$ と書き, 「p ならば q」と読み, **条件命題**という. $p \to q$ が真のとき,「$p \Rightarrow q$」と書き, p は q の**十分条件** , q は p の**必要条件**という[1].

例 3.6.
命題 p, q に対して, 条件命題 $p \to q$ などの真理表を書いてみると, 次のようになる.

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

真理表からもわかるように, 「$p \to q$」の否定は「p が成り立ち, q が成り立たない」となる. また「$p \to q$」の否定は「$p \to \neg q$」や「$\neg p \to \neg q$」ではないことに注意すること.

問題 3.1.
命題 p, q に対して, 「$p \to q$」, 「$p \to \neg q$」,「$\neg p \to \neg q$」の真理表を書け. そして, 「$p \to q$」の否定が「$p \to \neg q$」や「$\neg p \to \neg q$」でないことを確かめよ.

定理 3.2.
命題 p, q に対して,

$$「p \Leftrightarrow q」 \Longleftrightarrow 「(p \to q) \wedge (q \to p)」$$

が成り立つ. 右辺は「$p \Rightarrow q$ と $q \Rightarrow p$ が成り立つ」といってもよい.

[1] q が成立するためには, p **が成り立っていれば十分**だから, p を十分条件という. p が成り立っているならば, q **が成り立つことが必要**だから, q を必要条件という. 主格を導く格助詞「が」がどこについているかが重要である. なお, q が成り立つためには, p **が必要というわけではない**. $p \Rightarrow q$ のとき, p が成り立っていなくても, q が成り立つことは有り得ることに注意すること.

証明.
真理表を書いてみればよい. □

問題 3.2.
真理表を書くことで, 定理 3.2 を示せ.

定義 3.8 (逆, 対偶)**.**
命題 p, q に対して, 「$q \to p$」を「$p \to q$」の**逆**といい, 「$\neg q \to \neg p$」を「$p \to q$」の**対偶**という[2].

定理 3.3.
命題 p, q に対して,

$$「p \to q」 \Longleftrightarrow 「\neg q \to \neg p」$$

が成り立つ.

証明.
真理表を書いてみればよい. □

問題 3.3.
真理表を書くことで, 定理 3.3 を示せ.

例 3.7.
第 1 章の定理 1.4 の証明を簡潔に書いてみる.
1. 命題 p, q, r に対して,

$$(p \wedge q) \vee r \underset{\text{同値}}{\Leftrightarrow} (p \vee r) \wedge (q \vee r) \tag{3.1}$$

を示す. 下記の真理表により, $(p \wedge q) \vee r \underset{\text{同値}}{\Leftrightarrow} (p \vee r) \wedge (q \vee r)$ がわかる.

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

[2] $\neg p \to \neg q$ を裏ということがあるが, 数学ではあまり使われない.

2. 集合 A, B, C に対して, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ を示す.
任意の $x \in (A \cap B) \cup C$ に対して, $((x \in A \cap B) \vee x \in C)$ より,

$$((x \in A) \wedge (x \in B)) \vee (x \in C)$$

となるから, (3.1) より

$$((x \in A) \vee (x \in C)) \wedge ((x \in B) \vee (x \in C))$$

となる. よって, $(x \in A \cup C) \wedge (x \in B \cup C)$ だから $x \in (A \cup C) \cap (B \cup C)$ となる.

逆に任意の $x \in (A \cup C) \cap (B \cup C)$ に対して, $(x \in A \cup C) \wedge (x \in B \cup C)$ より

$$((x \in A) \vee (x \in C)) \wedge ((x \in B) \vee (x \in C))$$

となる. (3.1) より

$$((x \in A) \wedge (x \in B)) \vee (x \in C)$$

となるから, $((x \in A \cap B) \vee x \in C)$ より $x \in (A \cap B) \cup C$ がわかる. □

問題 3.4.

命題 p, q, r に対して, 真理表を書いて, 次を示せ.

(1) (結合法則) $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
(2) (結合法則) $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
(3) (分配法則) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
(4) (分配法則) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
(5) (de Morgan の法則) $\neg (p \wedge q) \Longleftrightarrow \neg p \vee \neg q$
(6) (対偶) $(p \to q) \Longleftrightarrow (\neg q \to \neg p)$

問題 3.5.

命題 p, q, r に対して, 次を示せ. 真理表を用いる方法と, 結合法則や分配法則, de Morgan の法則を用いて, 同値をつなげて示す方法の両方で示してみよ.

(1) $((p \vee q) \to r) \Leftrightarrow (p \to r) \wedge (q \to r)$
(2) $((p \wedge q) \to r) \Leftrightarrow (p \to r) \vee (q \to r)$
(3) $(p \to (q \wedge r)) \Leftrightarrow (p \to q) \wedge (p \to r)$
(4) $(p \to (q \vee r)) \Leftrightarrow (p \to q) \vee (p \to r)$

3.2. 述語論理

定義 3.9 (命題関数)**.**

$X_1, \ldots, X_n$ を集合とする. $x_1 \in X_1, \ldots, x_n \in X_n$ に対して, 命題 $p(x_1, \ldots, x_n)$ が定まるとき, $p = p(x_1, \ldots, x_n)$ を**命題関数**という. このとき

$$p(x_1, \ldots, x_n) \quad (x_1 \in X_1, \ldots, x_n \in X_n)$$

と書くことにする.

例 3.8.
次は命題関数である.

(1) X を数学科 1 年生全体として, $x \in X$ に対して

$$p(x)\text{: } x \text{ は男子である.}$$

(2) $X := \mathbb{R}$, $x \in X = \mathbb{R}$ に対して,

$$q(x)\text{: } x + 3 = 1.$$

(3) 集合 X, Y と写像 $f : X \to Y$, $x_1 \in X$, $x_2 \in X$ に対して

$$r(x_1, x_2)\text{: } f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

(4) 集合 X, Y と写像 $f : X \to Y$, $x \in X$, $y \in Y$ に対して

$$s(x, y)\text{: } y = f(x).$$

定義 3.10 (全称命題)**.**
命題関数 $p = p(x)$ $(x \in X)$ に対して, 「任意の (すべての) $x \in X$ に対して, $p(x)$ である」を「$\forall x \in X \quad p(x)$」と書き[3], **全称命題**という.

例 3.9.
例 3.8 の $p(x)$, $q(x)$, $r(x)$ について, 全称命題を考えてみる.

- 例 3.8 の (1) で, 「$\forall x \in X \quad p(x)$」は偽である. なぜなら, 全員男子ではないからである (断っていないが, X の数学科は日本大学理工学部としている). ところで Y を御茶ノ水女子大学の大学生全体としたとき「$\forall y \in Y \quad \neg p(y)$」は真である. 実際, 御茶ノ水女子大学には, 男子大学生はいない (はず) だからである.[4]
- 例 3.8 の (2) で, 「$\forall x \in X \quad q(x)$」は偽である. 実際, $x := -3 \in X$ のとき, $q(-3)$: $-3 + 3 = 1$ は正しくない, つまり, 「すべての $x \in X$ に対して $q(x)$ が正しい」はいえないからである.
- 例 3.8 の (3) で, 「$\forall x_1 \in X, \forall x_2 \in X \quad r(x_1, x_2)$」は単射の定義である.

定理 3.4.
命題関数 $p = p(x, y)$ $(x \in X, y \in Y)$ に対して,

$$\forall x \in X, \forall y \in Y \quad p(x, y) \iff \forall y \in Y, \forall x \in X \quad p(x, y)$$

である. つまり $\forall x$, $\forall y$ の順序は入れかえてよい.

---

[3] 「$\forall x \in X,\ p(x)$」や「$\forall x \in X : p(x)$」, 「$\forall x \in X$ に対して $p(x)$」と書くこともある.
[4] もし, 男子大学生がいるのなら, 著者の勘違いです.

証明は中内 [**10**] を参照せよ. 厳密に証明しようとすると, 数理論理学の知識を必要とする. 感覚的にいうと, 二つの変数 x, y を任意にとるときに, どちらをさきにとってから考えても同じということであり, 直積集合 $X \times Y$ を縦線をひいて埋めつくすか, 横線を引いて埋めつくすかの違いのようなものである.

定義 3.11 (存在命題)**.**
命題関数 $p = p(x)$ $(x \in X)$ に対して, 「ある $x \in X$ が存在して, $p(x)$ である」を「$\exists x \in X \quad p(x)$」と書き, **存在命題**という. 「$\exists x \in X$ s.t. $p(x)$」と書くこともある.

例 3.10.
例 3.8 の $p(x)$, $q(x)$, $r(x)$ について, 存在命題を考えてみる.

- 例 3.8 の (1) で, 「$\exists x \in X \quad p(x)$」は真である. なぜなら, 男子はいるからである. また, Y を御茶ノ水女子大学の大学生全体としたとき「$\exists y \in Y \quad p(y)$」は偽である. 実際, 御茶ノ水女子大学には, 男子大学生はいない (はず) だからである.
- 例 2.6 の (2) で, 「$\exists x \in X \quad q(x)$」は真である. 実際, $x := -2 \in X$ のとき, $q(-2)$: $-2 + 3 = 1$ だからである.
- 例 2.6 の (4) で, 「$\forall y \in Y, \exists x \in X \quad s(x, y)$」は全射の定義である.

定理 3.5.
命題関数 $p = p(x, y)$ $(x \in X, y \in Y)$ に対して,

$$\exists x \in X, \exists y \in Y \quad p(x, y) \iff \exists y \in Y, \exists x \in X \quad p(x, y)$$

である. つまり $\exists x$, $\exists y$ の順序は入れかえてよい.

証明は中内 [**10**] を参照せよ. これも厳密に証明しようとすると, 数理論理学の知識を必要とする. 感覚的にいうと, 直積集合 $X \times Y$ の長方形のどこかに $p(x, y)$ をみたす (x, y) があるわけだから, どちらが先に存在していても同じだということである.

注意 3.2.
定理 3.4 と定理 3.5 より, 「$\forall x \in X, \forall y \in Y$」を「$\forall x \in X, y \in Y$」, 「$\exists x \in X, \exists y \in Y$」を「$\exists x \in X, y \in Y$」と略記することがある.

注意 3.3.
「$\forall x \in X, \exists y \in Y \quad p(x, y)$」を「$\exists y \in Y, \forall x \in X \quad p(x, y)$」と**交換してはいけない.** つまり, $\exists$ と $\forall$ の交換は一般にできない. だから, 例 3.10 の (3.10) で「$\exists x \in X, \forall y \in Y \quad s(x, y)$」は全射の定義ではない.

定理 3.6 (de Morgan の法則)**.**
命題関数 $p = p(x)$ $(x \in X)$ に対して, 次が成り立つ.

(1) $\neg(\forall x \in X \quad p(x)) \Longleftrightarrow \exists x \in X \quad \neg p(x)$,
(2) $\neg(\exists x \in X \quad p(x)) \Longleftrightarrow \forall x \in X \quad \neg p(x)$,

これも証明は中内 [**10**] を参照せよ.

例 3.11 (de Morgan の法則が成り立つ理由)**.**
少し卑近な例で, de Morgan の法則が成り立つことを確かめる.
「すべての学生は男子」を否定すると,「すべての学生は女子」ではなくて,「ある学生は女子」となることはすぐわかるであろう[5]. この「すべて」が $\forall$ に対応していて,「ある」が $\exists$ に対応していたこと,「男子」の否定が「女子」に対応していたことから, 記号的に書くと

$$\neg(\forall x \quad x \text{ は男子}) \Longleftrightarrow (\exists x \quad x \text{ は女子}) \Longleftrightarrow (\exists x \quad \neg(x \text{ は男子}))$$

となることがわかる. 同様に考えれば

$$\neg(\exists x \quad x \text{ は女子}) \Longleftrightarrow (\forall x \quad x \text{ は男子}) \Longleftrightarrow (\forall x \quad \neg(x \text{ は女子}))$$

も感覚的には納得できる.

例 3.12 (ε-N 論法)**.**
$\{a_n\}_{n=1}^{\infty} \subset \mathbb{R}$ を数列とし, $a \in \mathbb{R}$ とする. $\lim_{n\to\infty} a_n = a$ であるとは任意の正数 ε に対して, ある自然数 N をとると任意の自然数 n に対して $n \geq N$ ならば $|a_n - a| < \varepsilon$ である (吹田・新保 [**6**]). これを $\forall$ と ε で書いてみると

$$\forall \varepsilon \in (0, \infty),\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N} \quad p(\varepsilon, N, n)$$

となる. ここで, $p(\varepsilon, N, n)$: $n \geq N \Longrightarrow |a_n - a| < \varepsilon$ である. 次に, $\lim_{n\to\infty} a_n = a$ の否定を考えると, de Morgan の法則から

$$\exists \varepsilon \in (0, \infty),\ \forall N \in \mathbb{N},\ \exists n \in \mathbb{N} \quad \neg p(\varepsilon, N, n)$$

となる. ここで

$$\begin{aligned}
\neg p(\varepsilon, N, n) &\Leftrightarrow \neg(n \geq N \Longrightarrow |a_n - a| < \varepsilon) \\
&\Leftrightarrow \neg(\neg(n \geq N) \vee (|a_n - a| < \varepsilon)) \\
&\Leftrightarrow (n \geq N) \wedge \neg(|a_n - a| < \varepsilon)) \\
&\Leftrightarrow (n \geq N) \wedge (|a_n - a| \geq \varepsilon)
\end{aligned}$$

[5] 男子校の反対は女子校ではなくて, 共学校だということ.

となるから, $\lim_{n\to\infty} a_n = a$ の否定は

$$\exists\varepsilon \in (0,\infty),\ \forall N \in \mathbb{N},\ \exists n \in \mathbb{N} \quad (n \geq N) \wedge (|a_n - a| \geq \varepsilon)$$

となる.

注意 3.4.
$\lim_{n\to\infty} a_n = a$ の否定は

$$\exists\varepsilon \notin (0,\infty),\ \forall N \notin \mathbb{N},\ \exists n \notin \mathbb{N} \quad (n \geq N) \wedge (|a_n - a| \geq \varepsilon)$$

や

$$\exists\varepsilon \in (0,\infty),\ \forall N \in \mathbb{N},\ \exists n \in \mathbb{N} \quad (n \geq N) \Rightarrow (|a_n - a| \geq \varepsilon)$$

ではないことに注意すること.

3.3. 応用: 「存在」, 「ならば」の証明の書き方

大学の数学でたいていの人が難しいと感じることに, 「存在する」と「ならば」を証明することがあげられると思う. そして, この両方がまじっている数列の収束の定義は, 難しく感じられてしまうのだろう. この節では, 数列の極限に関する証明を通して, 「存在する」と「ならば」, 任意と存在を**仮定すること**. **示すこと**とはどういうことかを説明したい.

例 3.13.
$\lim_{n\to\infty} \dfrac{n}{n+1} = 1$ を示してみよう. $\lim_{n\to\infty} \dfrac{n}{n+1} = 1$ の定義は何だったか思い出してみると (例 3.12 も参照)

$$\forall\varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N} \quad n \geq N \Rightarrow \left|\frac{n}{n+1} - 1\right| < \varepsilon$$

であった[6]. だから, ここで難しいところは, $n \geq N \Rightarrow \left|\dfrac{n}{n+1} - 1\right| < \varepsilon$ と $\exists N \in \mathbb{N}$ をどう証明として書くか？である.

$n \geq N \Rightarrow \left|\dfrac{n}{n+1} - 1\right| < \varepsilon$ から説明しよう. 一般に「P⇒Q を示せ」という問題は, 別の言い方をすると「P が成り立つと仮定して, Q が成り立つことを示せ」である. つまり, **示すことは Q** である. だから, P が成り立つかどうかは考えなくてよいのである. 極論すれば, **P が成り立つかどうかはどうでもよい**のである. さて, この問題の場合は, P にあたる部分が $n \geq N$ であり, Q にあたる

[6] $\varepsilon \in (0,\infty)$ は $\varepsilon > 0$ と書くことが多い.

部分が $\left|\dfrac{n}{n+1}-1\right|<\varepsilon$ である. だから, **証明で計算をしっかり書くべきところは** $\left|\dfrac{n}{n+1}-1\right|$ **の計算である.** そこで, この計算をしっかり書いてみると

$$\left|\frac{n}{n+1}-1\right|=\left|1-\frac{1}{n+1}-1\right|=\frac{1}{n+1}\leq\frac{1}{N+1}<\frac{1}{N}$$

となる. 最後から二つ目の不等式 $\leq$ に仮定 $n\geq N$ を使ったことに注意して欲しい. なお, 最後の不等式はたんに分母が小さくなったことによる不等式であるが, これはあとあとのためであり, 別にこの変形はしなくてもよい.

さて, $\exists N\in\mathbb{N}$ をどう考えればよいかを説明しよう. この「存在する」の考え方は「みつけてくる」や「みたすものがある」と言いかえた方がわかりやすいかもしれない. つまり, $\exists$ が出てきたあとの主張「$\forall n\in\mathbb{N}\quad n\geq N\Rightarrow\left|\dfrac{n}{n+1}-1\right|<\varepsilon$」が成り立つように, $N\in\mathbb{N}$ をみつけてこいということである. そこでさきほど, $n\geq N$ の仮定のもとで $\left|\dfrac{n}{n+1}-1\right|<\dfrac{1}{N}$ となったことに注意するともし $\frac{1}{N}<\varepsilon$ **となるような** $N\in\mathbb{N}$ **がみつかったとすると,**

$$\left|\frac{n}{n+1}-1\right|<\frac{1}{N}<\varepsilon$$

となるから, $n\geq N\Rightarrow\left|\dfrac{n}{n+1}-1\right|<\varepsilon$ が成り立つということがわかる. だから, $N\in\mathbb{N}$ を $\dfrac{1}{N}<\varepsilon$, つまり $N>\dfrac{1}{\varepsilon}$ となるように選べばよいが, これは厳密には Archimedes の原理によって示せる.

さて, ここまで考えたところで, 証明を書くときは, 論理記号の順番通りに文字や記号が出てくるように書く.

$\lim\limits_{n\to\infty}\dfrac{n}{n+1}=1$ **の証明**[7]**.**

0. (証明には書かなくてよいことであるがどのようにして $N\in\mathbb{N}$ を選べばよいかを考えるために,)$\forall\varepsilon>0$ に対して, $N\in\mathbb{N}$ を固定しておき, あとで決めることにする. このときに, $\forall n\in\mathbb{N}$ に対して, $n\geq N$ を仮定すると

$$\left|\frac{n}{n+1}-1\right|=\left|1-\frac{1}{n+1}-1\right|=\frac{1}{n+1}\leq\frac{1}{N+1}<\frac{1}{N}$$

[7]この証明に限って, 論理記号を使って証明を記述した.

となるから, $\dfrac{1}{N} < \varepsilon$, すなわち $N > \frac{1}{\varepsilon}$ をみたすように $N \in \mathbb{N}$ を選べばよいことがわかる.

1. $\forall \varepsilon > 0$ に対して, $N \in \mathbb{N}$ を $N \geq \dfrac{1}{\varepsilon}$ をみたすように選ぶ. Archimedes の原理より, このような $N \in \mathbb{N}$ が存在する. このとき, $\forall n \in \mathbb{N}$ に対して, $n \geq N$ ならば[8]

$$\left| \frac{n}{n+1} - 1 \right| = \left| 1 - \frac{1}{n+1} - 1 \right| = \frac{1}{n+1} \leq \frac{1}{N+1} < \frac{1}{N} < \varepsilon$$

となるので, $\lim_{n\to\infty} \dfrac{n}{n+1} = 1$ が成り立つ. □

注意 3.5.

上の証明の **0.** にもあるように**「存在」を証明するときには, とりあえず固定しておいて, どういう条件があればよいかを調べる**のが強力な方法である. このときに, **あとから出てくる文字を使って決めることができない**ことに注意すること.

注意 3.6.

「P ならば Q」を証明するときには, **P を仮定して** Q が成り立つかどうかを調べればよい. **P をうまく変形して Q を示そうとするやり方があるが, このやり方はたいてい間違いである.** P は仮定であり, **示さなければいけないのは Q** だから, 考えるべきことは Q である.

注意 3.7.

上の証明で **0.** のステップは書かなくてよいことであり, 多くの教科書では書かれていない. しかし, **この部分が理解できていないと他の問題を解くことができない.** つまり, 専門書を読むためには, この**著者が記述していない裏側の部分**を埋める必要がある. この作業は非常に難しい上に時間がかかり苦痛にもなると思うが, ここで諦めないことが重要である.

問題 3.6.

$\lim_{n\to\infty} \dfrac{2n-3}{n+1} = 2$ となることを証明せよ.

例 3.14.

数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty} \subset \mathbb{R}$ がそれぞれ $a, b \in \mathbb{R}$ に収束する, すなわち

$$a_n \to a, \quad b_n \to b \qquad (n \to \infty)$$

[8] 「ならば」を「と仮定すると」と書いてもよい.

とする. このとき, 数列 $\{a_n b_n\}_{n=1}^{\infty}$ が ab に収束する, すなわち

$$a_n b_n \to ab \qquad (n \to \infty)$$

を証明してみよう. この証明を書くときによくある間違いが, **証明の 1 行目に**

> $a_n \to a$ より
> $\forall \varepsilon > 0$ に対して $\exists N \in \mathbb{N}$ s.t. $\forall n \in \mathbb{N}$ に対して, $n \geq N \Rightarrow |a_n - a| < \varepsilon$.
> $b_n \to b$ より
> $\forall \varepsilon > 0$ に対して $\exists N \in \mathbb{N}$ s.t. $\forall n \in \mathbb{N}$ に対して, $n \geq N \Rightarrow |b_n - b| < \varepsilon$.

と書いてしまうことである. この文面を最初に書いた段階で, 採点する側からするとこの答案を書いた人は証明したいことが何かわかっていないなと思うのである. ここで証明したいことは

$\forall \varepsilon > 0$ に対して $\exists N \in \mathbb{N}$ s.t. $\forall n \in \mathbb{N}$ に対して, $n \geq N \Rightarrow |a_n b_n - ab| < \varepsilon$.

であって, **仮定である** $a_n \to a$, $b_n \to b$ **をどのように使えばよいか**を問うているのである. **仮定をどのように変形すればよいかを聞いているのではないのである.** 例 3.13 と同じように, どのように N を決めるかが問題であるが, 例 3.13 と違うのは, 具体的な a_n, b_n の形はわからないわけだから, 仮定を使って N を決める必要があるということである.

$a_n \to a$ を仮定していたから

$\forall \varepsilon_1 > 0$ に対して $\exists N_1 \in \mathbb{N}$ s.t. $\forall n_1 \in \mathbb{N}$ に対して, $n_1 \geq N_1 \Rightarrow |a_{n_1} - a| < \varepsilon_1$

が成り立つ. 示すべき主張に関しては添字をつけなかったが, 一緒の文字を使わないようにするために添字をつけておくことに注意しておく. さて,「$\forall \varepsilon > 0$ に対して $\cdots$」が**仮定**されていることから, $\varepsilon_1 > 0$ には**何を選んでもよいのである.** そこで, 何を選んでもよいのであれば, **あとで何にするか決めることにしておけばよい**のである. このことが見やすくなるような証明を書いてみよう.

例 3.14 の証明.

0. $\forall \varepsilon > 0$ に対して, $N \in \mathbb{N}$ を固定してあとで決めることにする. 仮定 $a_n \to a$ かつ $b_n \to b$ より任意の $\varepsilon_1 > 0$ と $\varepsilon_2 > 0$ **をあとで決めることにすると** $\exists N_1,\ N_2 \in \mathbb{N}$ が存在して

$$\forall n_1 \in \mathbb{N} \text{ に対して } n_1 \geq N_1 \Rightarrow |a_{n_1} - a| < \varepsilon_1 \tag{3.2}$$

と

$$\forall n_2 \in \mathbb{N} \text{ に対して } n_2 \geq N_2 \Rightarrow |b_{n_2} - b| < \varepsilon_2 \tag{3.3}$$

が成り立つ. $\forall n \in \mathbb{N}$ に対して $n \geq N$ を仮定すると

$$\begin{aligned} |a_n b_n - ab| &= |(a_n - a)(b_n - b) + (a_n - a)b + a(b_n - b)| \\ &\leq |a_n - a||b_n - b| + |a_n - a||b| + |a||b_n - bj| \end{aligned}$$

となるから, $N \geq N_1$ かつ $N \geq N_2$ を仮定すると (3.2), (3.3) が $n = n_1 = n_2$ とすることで使うことができて

$$|a_n b_n - ab| < \varepsilon_1\varepsilon_2 + |a|\varepsilon_2 + |b|\varepsilon_1$$

となる. $\varepsilon_1\varepsilon_2 + |a|\varepsilon_1 + |b|\varepsilon_1 < \varepsilon$ となるように ε_1, ε_2 を選べばよいのだから, 例えば

$$\varepsilon_1, \varepsilon_2 \leq \sqrt{\frac{\varepsilon}{3}}, \quad \varepsilon_1, \varepsilon_2 \leq \frac{\varepsilon}{3(1 + |a| + |b|)}$$

が成り立てば[9]

$$\begin{aligned} |a_n b_n - ab| &< \varepsilon_1\varepsilon_2 + |a|\varepsilon_2 + |b|\varepsilon_1 \\ &\leq \left(\sqrt{\frac{\varepsilon}{3}}\right)^2 + \frac{|a|\varepsilon}{3(1 + |a| + |b|)} + \frac{|b|\varepsilon}{3(1 + |a| + |b|)} \\ &\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon \end{aligned}$$

となり, 求めたかった不等式が得られる. 整理すると

$$N \geq N_1,\ N_2, \quad \varepsilon_1, \varepsilon_2 \leq \sqrt{\frac{\varepsilon}{3}}, \quad \varepsilon_1, \varepsilon_2 \leq \frac{\varepsilon}{3(1 + |a| + |b|)}$$

が成り立つように, 定めればよい. あとは決める順番であるが, N_1 や N_2 を決めるためには $\varepsilon_1, \varepsilon_2$ を先に指定しなければいけないから, $\varepsilon > 0$ を決めたあとに, $\varepsilon_1, \varepsilon_2$ を決める必要がある.

1. $\forall \varepsilon > 0$ に対して, $a_n \to a$ と $b_n \to b$ より

$$\varepsilon_1 = \varepsilon_2 = \min\left\{\sqrt{\frac{\varepsilon}{3}}, \frac{\varepsilon}{3(1 + |a| + |b|)}\right\} \tag{3.4}$$

ととれば, $\exists N_1,\ N_2 \in \mathbb{N}$ が存在して $\forall n_1, n_2 \in \mathbb{N}$ に対して

$$n_1 \geq N_1 \Rightarrow |a_{n_1} - a| < \varepsilon_1 = \min\left\{\sqrt{\frac{\varepsilon}{3}}, \frac{\varepsilon}{3(1 + |a| + |b|)}\right\} \tag{3.5}$$

[9]分母を $(1 + |a| + |b|)$ としたのは, $|a| = |b| = 0$ のときに無限大になる煩わしさを回避するためである.

と

$$n_2 \geq N_2 \Rightarrow |b_{n_2} - b| < \varepsilon_2 = \min\left\{\sqrt{\frac{\varepsilon}{3}}, \frac{\varepsilon}{3(1+|a|+|b|)}\right\} \tag{3.6}$$

が成り立つ. そこで, この N_1, N_2 に対して $N = \max\{N_1, N_2\}$ とおくと, $\forall n \in \mathbb{N}$ に対して, $n \geq N$ ならば

$$\begin{aligned}
|a_n b_n - ab| &= |(a_n - a)(b_n - b) + (a_n - a)b + a(b_n - b)| \\
&\leq |a_n - a||b_n - b| + |a_n - a||b| + |a||b_n - b| \\
&< \varepsilon_1\varepsilon_2 + |a|\varepsilon_2 + |b|\varepsilon_1 \quad (\because\ (3.5),\ (3.6)) \\
&\leq \left(\sqrt{\frac{\varepsilon}{3}}\right)^2 + \frac{|a|\varepsilon}{3(1+|a|+|b|)} + \frac{|b|\varepsilon}{3(1+|a|+|b|)} \quad (\because\ (3.4)) \\
&\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon
\end{aligned}$$

となる. よって $\{a_n b_n\}_{n=1}^{\infty}$ が ab に収束することが示された. □

注意 3.8.

上の証明の **0.** のように, **「任意の」が仮定されているときは**, その任意となっている対象を**自由に選ぶ**ことができる. そのため, **どのように選んだか？**が重要であることが多い.

問題 3.7.

数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty} \subset \mathbb{R}$ がそれぞれ $a, b \in \mathbb{R}$ に収束する, すなわち

$$a_n \to a, \quad b_n \to b \qquad (n \to \infty)$$

とする. このとき, 数列 $\{a_n + b_n\}_{n=1}^{\infty}$ が $a + b$ に収束する, すなわち

$$a_n + b_n \to a + b \qquad (n \to \infty)$$

を証明せよ.

3.4. 演習問題

問題 3.8.

$f : [0,1] \to \mathbb{R}$ に対して, 次の問に答えよ.

(1) f が $[0,1]$ 上で連続であることの定義とその否定を, 論理記号を用いて表せ.
(2) f が $[0,1]$ 上一様連続であることの定義とその否定を, 論理記号を用いて表せ. 連続と一様連続の違いに注意せよ.
(3) f が $[0,1]$ 上連続ならば, $[0,1]$ 上一様連続であることを論理記号を用いて証明せよ.

問題 3.9.

$\vec{a_1}, \vec{a_2}, \vec{a_3} \in \mathbb{R}^3$ が**線形独立**であるとは, どんな $c_1, c_2, c_3 \in \mathbb{R}$ に対しても, $c_1\vec{a_1} + c_2\vec{a_2} + c_3\vec{a_3} = 0$ ならば, $c_1 = c_2 = c_3 = 0$ となることをいう.

(1) $\vec{a_1}, \vec{a_2}, \vec{a_3} \in \mathbb{R}^3$ が**線形独立**であることの定義とその否定 (**線形従属**という) を, 論理記号を用いて表せ.

(2) 定義に従って, 次のベクトルの組が線形独立か線形従属かを調べよ.

$$\left\{ \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \right\}, \quad \left\{ \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix} \right\}$$

問題 3.10.

$r > 0$, $x_0 \in \mathbb{R}$ に対して, $B_r(x_0) := (x_0 - r, x_0 + r)$ とおく. $U \subset \mathbb{R}$ が開集合であるとは

任意の $x \in U$ に対して, ある正の実数 r が存在して, $B_r(x) \subset U$ が成り立つ

ことをいう.

(1) 論理記号を用いて, 開集合の定義を述べよ.

(2) $U \subset \mathbb{R}$ が開集合でないことを論理記号を用いて述べよ.

(3) 開区間 $(0, 1) \subset \mathbb{R}$ が開集合となることを示せ.

第 4 章

無限個の集合

集合の個数が無限個ある場合の集合の演算について考える. 例えば, 無限個の集合の和集合や共通部分はどう定義されるのかについて述べる. 無限を扱うときには, 有限の場合を「無限の場合でも説明できる」かたちで書き直す必要がある.

4.1. 集合族

第 1 章でも具体例で話題にしていたが, 集合を要素とする集合を考える.

定義 4.1 (集合族)**.**
集合を要素とする集合を**集合族**という. 花文字 (スクリプト体の文字) で書かれることがある.

例 4.1.
集合 X において, その部分集合を集めた集合は集合族になる (このように, 集合 X の部分集合からなる集合族を一般に X 上の集合族という). この集合族を 2^X と書く. すなわち

$$2^X := \{A : A \subset X\}$$

である. 例えば, $X = \{0, 1\}$ のとき,

$$2^X = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$$

である. 元の個数をみると, なぜ 2^X と書くのかがわかると思う.

例 4.2.
$p \geq 2$ を自然数とする. このとき, $a \in \mathbb{Z}$ に対して

$$\overline{a} := \{x \in \mathbb{Z} : x - a \text{ は } p \text{ で割り切れる }\}$$

とおく. このとき, 集合族 $\mathbb{Z}_p$ を

$$\mathbb{Z}_p := \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

で定義する. p が素数の時が特に重要である. これは, p でわった余りで $\mathbb{Z}$ を分割したものとみることもできる. このことは, 第 5 章でさらに詳しく説明する.

例 4.3.
実数上の集合族 $\mathscr{B}$ を

$$\mathscr{B} := \{(a,b) : a,b \in \mathbb{R}, a < b\}$$

で定める. つまり, 開区間全体を集めた集合が $\mathscr{B}$ である. この集合は位相空間を学ぶときに重要となる. また, このあと述べる無限個の集合の例ともなっている

問題 4.1.
$X = \{1,2,3\}$ のときに, 2^X を具体的に求めよ (空集合と全体を忘れないように).

4.2. 無限個の集合の例

集合が無限個ある場合を考えよう. 先の例 4.3 は, 集合の要素が無限個あるわけであるが, 集合の要素が開区間だったから, 開区間が無限個ある, すなわち集合が無限個あることになる. 他の例を挙げよう.

例 4.4.
$n \in \mathbb{N}$ に対して, 集合 $A_n \subset \mathbb{R}$ を

$$A_n := \left(0, 1 - \frac{1}{n}\right)$$

と定める. このとき, $\{A_n\}_{n\in\mathbb{N}}$ は無限個の集合 (集合列ということもある) である.

例 4.5.
$\lambda > 0$ に対して, 集合 $A_\lambda \subset \mathbb{R}$ を

$$A_\lambda := (0, \lambda)$$

と定める. このとき, $\{A_\lambda\}_{\lambda\in(0,\infty)} = \{A_\lambda\}_{\lambda>0}$ は無限個の集合である.

無限個の集合に対して, なんらかのラベル付け (A_n や A_λ の n や λ) があると便利である.

定義 4.2 (添字集合と集合族)**.**
空でない集合 Λ と $\lambda \in \Lambda$ に対して, 集合 A_λ を考える. 集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ を考えたときに, λ を**添字**といい, Λ を**添字集合**という.

例 4.4 では添字集合は $\mathbb{N}$ であり, 例 4.5 では添字集合は $(0,\infty)$ である. また, $n,m\in\mathbb{N}$ に対して

$$A_{n,m}:=\left(-\frac{1}{n},\frac{1}{m}\right)$$

とおけば, $\{A_{n,m}\}_{(n,m)\in\mathbb{N}\times\mathbb{N}}$ となるから, 添字集合は $\mathbb{N}\times\mathbb{N}$ となる.

例 4.6.

実数列 $\{a_n\}_{n=1}^{\infty}$ は, 添字集合 $\mathbb{N}$ のついた実数の部分集合とみなすことができる[1]. そこで, $\{a_n\}_{n=1}^{\infty}\subset\mathbb{R}$ と書くことがある. 同じようにして, 複素数列 $\{z_n\}_{n=1}^{\infty}$ を $\{z_n\}_{n=1}^{\infty}\subset\mathbb{C}$ と書いたり, 実数の部分集合 $A\subset\mathbb{R}$ 上の数列 $\{b_n\}_{n=1}^{\infty}$ を $\{b_n\}_{n=1}^{\infty}\subset A$ と書いたりする.

4.3. 無限個の集合の和集合, 共通部分

話を過度に抽象化しないために, しばらくの間, 考える集合族は $\{A_n\}_{n\in\mathbb{N}}$ として, 添字集合は $\mathbb{N}$ とする. 実際には添字集合はなんでもよい. $\{A_n\}_{n\in\mathbb{N}}$ の和集合 $A_1\cup A_2\cup A_3\cup\cdots$ を考えたいのだが, この定義を定義 1.6 のように

$$A_1\cup A_2\cup A_3\cup\cdots=\{x:x\in A_1\text{または}x\in A_2\text{または}x\in A_3\text{または}\cdots\}\tag{4.1}$$

としようとしても, 右辺の $\cdots$ の意味が定められない. イメージはこれでもいいのだが, 無限に続いてしまうので, この表記では定義できたことにならない. ところで $x\in A_1\cup A_2\cup A_3$ なら (有限個の場合には), $i=1,2,3$ の少なくともどれか一つの i について, $x\in A_i$ が成り立つ. つまり, 数学の言葉を用いれば

$$x\in A_1\cup A_2\cup A_3\underset{\text{同値}}{\Longleftrightarrow}\text{ある }i=1,2,3\text{ が存在して }x\in A_i\tag{4.2}$$

と書きかえができる. (4.1) はの右辺は無限個の場合に意味がわからないが, (4.2) の右辺は無限個の場合でも意味を持つ. すなわち,

$$x\in A_1\cup A_2\cup A_3\cup\cdots\Longleftrightarrow\text{ある }i\in\mathbb{N}\text{ が存在して }x\in A_i$$

を無限個の集合の和集合の定義とすることができる.

定義 4.3 (和集合)**.**

集合族 $\{A_n\}_{n\in\mathbb{N}}$ に対して, 和集合 $\bigcup_{n\in\mathbb{N}}A_n$ を

$$\bigcup_{n\in\mathbb{N}}A_n:=\{x:\text{ある }n\in\mathbb{N}\text{ が存在して }x\in A_n\}$$

で定義する.

[1]正確には $n=1,2,3,\ldots$ と順序が定まっている.

問題 4.2.
Λ を添字集合としたとき, 集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して, 和集合 $\bigcup_{\lambda\in\Lambda} A_\lambda$ の定義は何か？定義 4.3 を参考にして, 記述せよ.

$\{A_n\}_{n\in\mathbb{N}}$ の共通部分 $A_1\cap A_2\cap A_3\cap\cdots$ も同様に考えてみる. 定義 1.6 のように

$$A_1\cap A_2\cap A_3\cap\cdots=\{x : x\in A_1\text{かつ } x\in A_2\text{かつ } x\in A_3\text{かつ}\cdots\}$$

としようとしても, 右辺の $\cdots$ の意味は定められない. ところで $x\in A_1\cap A_2\cap A_3$ なら (有限個の場合には), $i=1,2,3$ のすべての i について, $x\in A_i$ が成り立つ. つまり, 数学の言葉を用いれば

$$x\in A_1\cap A_2\cap A_3 \underset{\text{同値}}{\iff} \text{すべての } i=1,2,3 \text{ に対して } x\in A_i \tag{4.3}$$

と書きかえができる. (4.3) の右辺は無限個の場合でも意味を持つ. すなわち,

$$x\in A_1\cup A_2\cup A_3\cup\cdots \iff \text{すべての } i\in\mathbb{N} \text{ に対して } x\in A_i$$

を無限個の集合の共通部分の定義とすることができる.

定義 4.4 (共通部分)**.**
集合族 $\{A_n\}_{n\in\mathbb{N}}$ に対して, 共通部分 $\bigcap_{n\in\mathbb{N}} A_n$ を

$$\bigcap_{n\in\mathbb{N}} A_n := \{x : \text{すべての } n\in\mathbb{N} \text{ に対して } x\in A_n\}$$

で定義する.

問題 4.3.
Λ を添字集合としたとき, 集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して, 共通部分 $\bigcap_{\lambda\in\Lambda} A_\lambda$ の定義は何か？定義 4.4 を参考にして, 記述せよ.

注意 4.1.
添字集合が $\mathbb{N}$ のときは, $\bigcup_{n\in\mathbb{N}}$ を $\bigcup_{n=1}^{\infty}$, $\bigcap_{n\in\mathbb{N}}$ を $\bigcap_{n=1}^{\infty}$ と書くことがある.

例 4.7.
$n\in\mathbb{N}$ に対して, 集合

$$A_n := \left(0, 2-\frac{1}{n}\right)$$

を考える. このとき,

$$\bigcup_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} \left(0, 2-\frac{1}{n}\right) = (0,2), \qquad \bigcap_{n\in\mathbb{N}} A_n = \bigcap_{n\in\mathbb{N}} \left(0, 2-\frac{1}{n}\right) = (0,1)$$

となる.

例 4.7 の証明.

1. $\bigcup_{n\in\mathbb{N}} A_n = (0,2)$ について, $(0,2) \subset \bigcup_{n\in\mathbb{N}} A_n$ のみ示す. 任意の $x \in (0,2)$ に対して, $2-x>0$ だから, ある $N \in \mathbb{N}$ が存在して, $\frac{1}{N} < 2-x$ とできる[2]. 従って, この $N \in \mathbb{N}$ に対して, $2-\frac{1}{N} > 2-(2-x) = x > 0$ だから $x \in A_N$ となる. 従って, $x \in A_N \subset \bigcup_{n=1}^{\infty} A_n$ となるから, $(0,2) \subset \bigcup_{n\in\mathbb{N}} A_n$ が示された.

2. $\bigcap_{n\in\mathbb{N}} A_n = (0,1)$ について, $\bigcap_{n\in\mathbb{N}} A_n \subset (0,1)$ のみ示す. 任意の $x \in \bigcap_{n\in\mathbb{N}} A_n$ に対して, 任意の $n \in \mathbb{N}$ について $x \in A_n$ だから, $0 < x < 2-\frac{1}{n}$ が成り立つ. 特に $n=1$ とすると $0<x<1$ となるから, $x \in (0,1)$ となる. 従って, $\bigcap_{n\in\mathbb{N}} A_n \subset (0,1)$ が成り立つ. □

問題 4.4.

例 4.7 の証明で, 証明していない逆向きの包含関係を証明せよ.

問題 4.5.

$n \in \mathbb{N}$ に対して, $A_n = \left(0, 1+\frac{1}{n}\right) \subset \mathbb{R}$ とおく. このとき, $\bigcup_{n=1}^{\infty} A_n$ と $\bigcap_{n=1}^{\infty} A_n$ を求めよ ($\bigcap_{n=1}^{\infty} A_n$ は開区間にならないことに注意せよ).

問題 4.6.

$n \in \mathbb{N}$ に対して, $B_n = \left[0, 2-\frac{1}{n}\right] \subset \mathbb{R}$ とおく. このとき, $\bigcup_{n=1}^{\infty} B_n$ と $\bigcap_{n=1}^{\infty} B_n$ を求めよ ($\bigcup_{n=1}^{\infty} B_n$ は閉区間にならないことに注意せよ).

[2]厳密にやるなら Archimedes の原理を使う.

集合の演算に対する結合法則や分配法則, de Morgan の法則や定理 2.2 の主張は, 無限個の集合の和集合, 共通部分についても, ほぼそのまま成り立つ. これらは問題としておく.

問題 4.7 (分配法則)**.**
$\{A_n\}_{n\in\mathbb{N}}$ を集合族, B を集合とする. このとき

$$\left(\bigcup_{n\in\mathbb{N}} A_n\right)\cap B=\bigcup_{n\in\mathbb{N}}(A_n\cap B),\qquad \left(\bigcap_{n\in\mathbb{N}} A_n\right)\cup B=\bigcap_{n\in\mathbb{N}}(A_n\cup B)$$

を示せ.

問題 4.8 (de Morgan の法則)**.**
$\{A_n\}_{n\in\mathbb{N}}$ を集合族とするとき

$$\left(\bigcup_{n\in\mathbb{N}} A_n\right)^c=\bigcap_{n\in\mathbb{N}} A_n^c,\qquad \left(\bigcap_{n\in\mathbb{N}} A_n\right)^c=\bigcup_{n\in\mathbb{N}} A_n^c$$

を示せ.

問題 4.9 (写像と集合の演算)**.**
X, Y を空でない集合, $f: X\to Y$ を写像, $\{A_n\}_{n\in\mathbb{N}}\subset 2^X$ を X 上の集合族, $\{B_n\}_{n\in\mathbb{N}}\subset 2^Y$ を Y 上の集合族とするとき, 次を示せ.

(1) $f\left(\bigcup_{n\in\mathbb{N}} A_n\right)=\bigcup_{n\in\mathbb{N}} f(A_n)$;

(2) $f\left(\bigcap_{n\in\mathbb{N}} A_n\right)\subset\bigcap_{n\in\mathbb{N}} f(A_n)$;

(3) $f^{-1}\left(\bigcup_{n\in\mathbb{N}} B_n\right)=\bigcup_{n\in\mathbb{N}} f^{-1}(B_n)$;

(4) $f^{-1}\left(\bigcap_{n\in\mathbb{N}} B_n\right)=\bigcap_{n\in\mathbb{N}} f^{-1}(B_n)$;

4.4. 無限個の集合の直積と選択公理

ここでも話を抽象化しないために, 考える集合族 $\{A_n\}_{n\in\mathbb{N}}$ として, 添字集合は $\mathbb{N}$ とする. 無限個の集合に対する直積を定義したいのだが, 無限個の集合の和集合と共通部分と同じく, 定義 1.7 をそのまま定義とすることができない. そのために 2 個の直積集合 $A_1\times A_2$ について考え直してみよう. $A_1\times A_2$ は

$$A_1\times A_2=\{(a_1,a_2): a_1\in A_1 \text{ かつ } a_2\in A_2\}$$

であった. そこで, $(a_1, a_2) \in A_1 \times A_2$ に対して, $f : \{1, 2\} \to A_1 \cup A_2$ を

$$f(n) = a_n \quad (n = 1, 2)$$

で定めると $f(n) \in A_n$ をみたす. 逆に $f : \{1, 2\} \to A_1 \cup A_2$ が $n = 1, 2$ に対して, $f(n) \in A_n$ をみたすとすると, $(f(1), f(2)) \in A_1 \times A_2$ となる. このことから

$$T : A_1 \times A_2 \to \{f : \{1, 2\} \to A_1 \cup A_2, f(1) \in A_1, f(2) \in A_2\}$$

を $(a_1, a_2) \in A_1 \times A_2$ と $n = 1, 2$ に対して $T(a_1, a_2)(n) := a_n$ と定めることができて, この写像 T は全単射となる. つまり, $A_1 \times A_2$ と $\{f : \{1, 2\} \to A_1 \cup A_2, f(1) \in A_1, f(2) \in A_2\}$ は (集合として) 同じものとみなすことができる. よって, この後者の写像を用いれば, 無限個の集合に対する直積集合を定義することができる.

定義 4.5 (無限個の集合に対する直積集合)**.**

集合族 $\{A_n\}_{n\in\mathbb{N}}$ に対して直積集合 $\prod_{n\in\mathbb{N}} A_n$ を

$$\prod_{n\in\mathbb{N}} A_n := \left\{ f : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n,\ \text{任意の } n \in \mathbb{N} \text{ に対して } a_n \in A_n \right\} \tag{4.4}$$

で定める.

問題 4.10.

Λ を添字集合としたとき, 集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ に対して, 直積集合 $\prod_{\lambda\in\Lambda} A_\lambda$ の定義は何か？定義 4.5 を参考にして, 記述せよ.

直感的には $a \in \prod_{n\in\mathbb{N}} A_n$ ということは, $a = (a_1, a_2, a_3, \dots)$ と思えばよいのであるが, 点々の部分を厳密に述べようとすると定義 4.5 にようにしなければいけない. さらに, この定義にはもっと重大な問題がある. 有限個の場合とは異なり (4.4) の右辺の集合が空でないことを確かめておかないといけないのである. ある $n \in \mathbb{N}$ が存在して, $A_n = \emptyset$ となっているときは, 右辺は空集合となる (これは写像のときにきちんと述べてはいなかったのだが, 値域が空集合となる写像は存在しない). しかし, 任意の $n \in \mathbb{N}$ に対して, $A_n \neq \emptyset$ のときに (4.4) の右辺はどうなっているのだろうか？直感的に考えれば, (4.4) の右辺は空でない, すなわち $\prod_{n\in\mathbb{N}} A_n$ は空集合ではないと考えるべきであるがこの事実は公理, すなわち証明せずに認める事実とする. このことを**選択公理**という.

選択公理 Λ を添字集合とする. 集合族 $\{A_\lambda\}_{\lambda\in\Lambda}$ は任意の $\lambda\in\Lambda$ に対して, $A_\lambda\neq\emptyset$ を仮定する. このとき, $\prod_{n\in\mathbb{N}} A_n\neq\emptyset$ となる.

このあたりまえに見える公理から, 実に不思議ともいえる結果が得られる. 例えば

- (Lebesgue 測度の意味で) 面積を決定できない集合が存在する.
- 3 次元の球体を適当に分割して, くっつけなおすと, 同じ半径の球体を 2 つ作ることができる (Banach-Tarski のパラドックス). ただし, できた 2 つの球体は (Lebesgue 測度の意味で) 面積を決定できない.

このことから, 選択公理を認めるか否かについては, 様々な意見がある. とりわけ, 面積を決定できない集合が存在することは, 現実的には奇妙とも思えるため, 物理や工学への応用をも念頭においた数学者などで, 「選択公理を使わないようにしている」研究者もいる. 実際に, 選択公理 (と同値な命題) を使うような状況はかなり込み入っていることが多い.

4.5. 応用: 位相空間について

$(0,1)\subset\mathbb{R}$ は開区間というが, 実はこの「開」というのは, もう少し広い概念で使われている. $U\subset\mathbb{R}$ が**開集合**であるとは, 任意の $x\in U$ に対して, ある $\varepsilon>0$ が存在して, $(x-\varepsilon,x+\varepsilon)\subset U$ となることをいう. 例えば, $(0,1)$ などの開区間は開集合であり, 他にも $(0,1)\cup(2,3)$ なども開集合である[3]. 以下, 簡単のために $B_\varepsilon(x):=(x-\varepsilon,x+\varepsilon)$ と書くことにする.

定理 4.1.
次が成り立つ.

(1) $\emptyset,\mathbb{R}$ は開集合である.

(2) $U_1,\dots,U_n$ が開集合ならば, $\bigcap_{k=1}^{n} U_k=U_1\cap U_2\cap\cdots\cap U_n$ も開集合である.

(3) 添字集合を Λ として, 任意の $\lambda\in\Lambda$ に対して, U_λ が開集合ならば, $\bigcup_{\lambda\in\Lambda} U_\lambda$ も開集合である.

[3]感覚的には「こういう感じの集合」と説明できるのだが, この節では, わざとそういう説明をしない. この節の内容は感覚に頼って考えると間違って理解してしまうので, 感覚をいっさい捨てて読んで欲しい.

証明.
(3) のみ示す.

> 示せばいいことは, 任意の $x \in \bigcup_{\lambda\in\Lambda} U_\lambda$ に対して, $B_\varepsilon(x) \subset \bigcup_{\lambda\in\Lambda} U_\lambda$ となる $\varepsilon > 0$ をみつけることである.

任意の $x \in \bigcup_{\lambda\in\Lambda} U_\lambda$ に対して, $\bigcup_{\lambda\in\Lambda} U_\lambda$ の定義から, ある $\lambda \in \Lambda$ が存在して $x \in U_\lambda$ が成り立つ. U_λ は開集合だったから, 開集合の定義より, ある $\varepsilon > 0$ が存在して, $B_\varepsilon(x) \subset U_\lambda$ が成り立つ. $U_\lambda \subset \bigcup_{\lambda\in\Lambda} U_\lambda$ だから (各自考えよ), とくに $B_\varepsilon(x) \subset \bigcup_{\lambda\in\Lambda} U_\lambda$ も成立する. よって, $\bigcup_{\lambda\in\Lambda} U_\lambda$ が開集合となることがわかった. □

問題 4.11.
定理 4.1 の (3) 以外の証明を考えてみよ. なお, 内田 [**5**] を参考にせよ[4].

さて, 開集合の定義で, $B_\varepsilon(x) = (x-\varepsilon, x+\varepsilon)$ としていたが, これは, $B_\varepsilon(x) = \{y \in \mathbb{R} : |y-x| < \varepsilon\}$ ともできることに注意して欲しい. 従って, x と y の二点の距離が定義できていれば, 開集合は定義できるのである. そして, さらに定理 4.1 の主張をじっくりと見てみると, これらの主張はもはや集合の言葉しか使っていないことに注意して欲しい. つまり, $\mathbb{R}$ 上の開集合からなる集合族を $\mathscr{O}$ と書くと

(1) $\emptyset, \mathbb{R} \in \mathscr{O}$.
(2) $U_1, \ldots, U_n \in \mathscr{O}$ ならば, $\bigcap_{k=1}^{n} U_k = U_1 \cap U_2 \cap \cdots \cap U_n \in \mathscr{O}$.
(3) $\{U_\lambda\}_{\lambda\in\Lambda} \subset \mathscr{O}$ ならば, $\bigcup_{\lambda\in\Lambda} U_\lambda \in \mathscr{O}$.

となる. このことをさらに抽象化することで, 次の定義が得られる.

定義 4.6 (位相空間)**.**
X を集合とする. このとき, $\mathscr{O} \subset 2^X$, すなわち X の部分集合からなる集合族 $\mathscr{O}$ が次の 3 条件をみたすとき, $\mathscr{O}$ を X の**位相**といい, $(X, \mathscr{O})$ を**位相空間**という.

[4] この問題が何もみずに解けるようになれば, 位相空間論で苦労することはそれほどないのではないかと思われる.

(1) $\emptyset, X \in \mathscr{O}$.

(2) $U_1, \ldots, U_n \in \mathscr{O}$ ならば, $\bigcap_{k=1}^{n} U_k = U_1 \cap U_2 \cap \cdots \cap U_n \in \mathscr{O}$.

(3) $\{U_\lambda\}_{\lambda\in\Lambda} \subset \mathscr{O}$ ならば, $\bigcup_{\lambda\in\Lambda} U_\lambda \in \mathscr{O}$.

位相空間はたんに, $\mathbb{R}$ を抽象化してみたというだけで考えられた空間ではない[5]. 実数の性質の一つである絶対値の概念が考えられない (ないしは考えにくい) 集合を調べるためには, 位相空間の知識が必須となる. このノートではこれ以上このことには触れないが, 位相空間を勉強するにあたって, 無限個の集合の計算は必須であり, 問題 4.5 や問題 4.6 の具体例は覚えておくことが望ましい.

4.6. 演習問題

問題 4.12.

$\mathbb{N}$ を添字集合とする集合族 $\{A_n\}_{n=1}^{\infty}$ に対して, 次をみたす集合族 $\{B_n\}_{n=1}^{\infty}$ を構成せよ:

$$\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} B_n, \quad B_n \cap B_m = \emptyset \quad (n \neq m)$$

問題 4.13 (上極限集合, 下極限集合)**.**

$\mathbb{N}$ を添字集合とする集合族 $\{A_n\}_{n=1}^{\infty}$ に対して $\{A_n\}_{n=1}^{\infty}$ の**上極限集合**と**下極限集合** $\limsup_{n\to\infty} A_n$ と $\liminf_{n\to\infty} A_n$ を

$$\limsup_{n\to\infty} A_n := \bigcap_{k=1}^{\infty} \left(\bigcup_{n\geq k} A_n \right), \qquad \liminf_{n\to\infty} A_n := \bigcup_{k=1}^{\infty} \left(\bigcap_{n\geq k} A_n \right)$$

でそれぞれ定義する. 集合族 $\{A_n\}_{n=1}^{\infty}$, $\{B_n\}_{n=1}^{\infty}$ に対して, 次を示せ.

(1) $\liminf_{n\to\infty} A_n \subset \limsup_{n\to\infty} A_n$,

(2) $A_n \subset B_n$ ならば

$$\limsup_{n\to\infty} A_n \subset \limsup_{n\to\infty} B_n, \qquad \liminf_{n\to\infty} A_n \subset \liminf_{n\to\infty} B_n.$$

[5]位相空間がとても重要であることの一つの理由として, Poincaré 予想をあげておきたい (もちろん, 他にも重要な理由がたくさんある). この Poincaré 予想は Clay 研究所の 100 万ドル懸賞問題の一つであったのだが, この問題を正しく理解するのには, 位相空間の知識が必要となる. テレビなどの解説では, 位相空間を知らない人向けに苦心して説明がなされているが, 位相空間と幾何学に関する知識がある程度あれば, Poincaré 予想はもっと簡単に理解できる. なお, Poincaré 予想は G. Perelman によって証明された.

注意.

上極限集合 $\limsup_{n\to\infty} A_n$ と下極限集合 $\liminf_{n\to\infty} A_n$ が一致するとき, $\lim_{n\to\infty} A_n$ と書き, 極限集合という. 数列 $\{a_n\}_{n=1}^{\infty}$ に対して $\liminf_{n\to\infty} a_n$ と $\limsup_{n\to\infty} a_n$ が一致するときに $\lim_{n\to\infty} a_n$ が存在することに注意して欲しい.

問題 4.14.

$\mathbb{N}$ を添字集合とする集合族 $\{A_n\}_{n=1}^{\infty}$ が単調増加であるとする. すなわち, 任意の $n \in \mathbb{N}$ に対して, $A_n \subset A_{n+1}$ が成り立つとする. このとき, $\limsup_{n\to\infty} A_n$ と $\liminf_{n\to\infty} A_n$ を求めよ.

第 5 章

同値関係と商集合

$\triangle ABC$ と三角形 $\triangle A'B'C'$ を考える. この二つの三角形が合同のとき,

$$\triangle ABC \equiv \triangle A'B'C'$$

と書いていた. この合同 $\equiv$ は次の性質をみたすことは, ほぼ明らかであろう.

- 同じ三角形は合同 (反射律という)

$$\triangle ABC = \triangle ABC$$

- $\triangle ABC$ と $\triangle A'B'C'$ が合同ならば, $\triangle A'B'C'$ と $\triangle ABC$ も合同 (対称律)

$$\triangle ABC \equiv \triangle A'B'C' \Longrightarrow \triangle A'B'C' \equiv \triangle ABC$$

- $\triangle ABC$ と $\triangle A'B'C'$, $\triangle A'B'C'$ と $\triangle A''B''C''$ のそれぞれが合同ならば, $\triangle ABC$ と $\triangle A''B''C''$ も合同 (推移律)

$$\triangle ABC \equiv \triangle A'B'C',\ \triangle A'B'C' \equiv \triangle A''B''C'' \Longrightarrow \triangle ABC \equiv \triangle A''B''C''$$

これにより, 三角形を分類することができる. ものごとを分類するには, 2 つのものがみたすかみたさないかの規則を考えることが重要になる. また, (通常の実数の等号を考えると) **反射律, 対称律, 推移律**の 3 つの条件はみたしていて欲しい条件といえる. そこで, これらの条件を抽象化して, 集合の上に同値関係を定義し, 集合を分類することを考える.

5.1. 同値関係

定義 5.1 (同値関係)**.**

X を集合とする. $x, y \in X$ に対して, $x \sim y$ か $x \not\sim y$ のどちらかが常に成り立つ規則 $\sim$ が与えられていて, 次をみたすとき, $\sim$ を**同値関係**という.

(1) (反射律) 任意の $x \in X$ に対して $x \sim x$.
(2) (対称律) 任意の $x, y \in X$ に対して $x \sim y$ ならば $y \sim x$.
(3) (推移律) 任意の $x, y, z \in X$ に対して $x \sim y, y \sim z$ ならば $x \sim z$.

例 5.1.

$\mathbb{R}$ 内の等号 $=$ は同値関係となる. また, 不等号 $\leq$ は同値関係ではない. なぜなら, 不等式は対称律をみたさないからである. 例えば $3 \leq 5$ だからといって, $5 \leq 3$ にはならないことから, 不等式が対称律をみたさないことはわかるであろう.

例 5.2.

X を $\mathbb{R}^2$ 内の三角形全体の集合とする. このとき, 合同 $\equiv$ や相似[1] $\sim$ は同値関係である.

例 5.3.

$p \in \mathbb{N}$ を素数とする. $x, y \in \mathbb{Z}$ に対して

$$x \sim y \underset{\text{定義}}{\Leftrightarrow} k \in \mathbb{Z} \text{ が存在して } x - y = kp$$
$$\Leftrightarrow x - y \text{ が } p \text{ でわり切れる } (x, y \text{ を } p \text{ でわったときの余りが同じ})$$

と定める, このとき, $\sim$ は同値関係となる. この同値関係は

$$x \equiv y \pmod{p}$$

と書くことが多い.

証明.

1. 反射律を示す. 任意の $x \in \mathbb{Z}$ に対して, $x - x = 0 = 0p$ となるから, $k = 0$ ととることにより, $x \sim x$ が成り立つ.

2. 対称律を示す. 任意の $x, y \in \mathbb{Z}$ に対して, $x \sim y$ が成り立つと仮定する. このとき, ある $k \in \mathbb{Z}$ が存在して, $x - y = kp$ と書ける. このとき,

$$y - x = -kp = (-k)p$$

であり, $-k \in \mathbb{Z}$ となるから, $y \sim x$ が成り立つ.

3. 推移律を示す. 任意の $x, y, z \in \mathbb{Z}$ に対して, $x \sim y$ かつ $y \sim z$ が成り立つと仮定する. このとき, ある $k_1,\ k_2 \in \mathbb{Z}$ が存在して $x - y = k_1 p$ かつ $y - z = k_2 p$ と書ける. このとき

$$x - z = (x - y) + (y - z) = k_1 p + k_2 p = (k_1 + k_2)p$$

となり, $k_1 + k_2 \in \mathbb{Z}$ となるから, $x \sim z$ が成り立つ. □

問題 5.1.

$p \in \mathbb{N}$ を素数とし, 簡単のために $x, y \in \mathbb{N}$ に対して, $k \in \mathbb{Z}$ が存在して $x - y = kp$ と仮定する. このときに, x と y を p で割った余りが等しいことを

[1] 中学生が使う記号は LaTeX では用意されていないようである

示せ (ヒント: x を p で割った商を q_1, 余りを r_1 と書くと, $x = q_1p + r_1$ かつ $0 \leq r_1 < p$ が成り立つ).

例 5.4.

$\mathbb{R}[X]$ を X を変数する実数係数多項式全体とする. すなわち

$$\mathbb{R}[X] := \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{N}_0,\ a_0, \ldots, a_n \in \mathbb{R}\}$$

とする. $f(X), g(X) \in \mathbb{R}[X]$ に対して

$$f(X) \sim g(X) \underset{\text{定義}}{\Leftrightarrow} h(X) \in \mathbb{R}[X] \text{ が存在して } f(X) - g(X) = (X^2+1)h(X)$$
$$\Leftrightarrow f(X) - g(X) \text{ が } (X^2+1) \text{ でわり切れる}$$

とおく. このとき, $\sim$ は同値関係となる.

証明.

対称律のみ示す. 任意の $f(X), g(X) \in \mathbb{R}[X]$ に対して, $f(X) \sim g(X)$ が成り立つならば, ある $h(X) \in \mathbb{R}[X]$ が存在して, $f(X) - g(X) = (X^2+1)h(X)$ と書ける. このとき

$$g(X) - f(X) = -(X^2+1)h(X) = (X^2+1)(-h(X))$$

となるが, $-h(X) \in \mathbb{R}[X]$ となるので, $g(X) \sim f(X)$ が成り立つ. □

問題 5.2.

例 5.4 について, 反射律と推移律を示せ.

5.2. 同値類と代表元

1 と 4 と 7 は 3 で割った余りが等しい. また, 少し注意が必要だが, $-2 = -1 \times 3 + 1$ や $-5 = -2 \times 3 + 1$ とみることで, -2 や -5 も 3 で割ると余りは 1 となる. よって

$$\cdots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv \cdots \pmod 3$$

がわかる. これら 3 で割った余りが 1 となる整数を集めれば, 新しい集合

$$\{n \in \mathbb{N} : n \equiv 1 \pmod 3\} = \{3m + 1 : m \in \mathbb{Z}\}$$

が定義できる. これを一般化してみよう.

定義 5.2 (同値類, 代表元)**.**

X を集合, $\sim$ を同値関係, $x \in X$ とする. このとき

$$C(x) := \{y \in X : x \sim y\}$$

とおく. $C(x)$ を x の**同値類**, x を**代表元**という.

注意 5.1.

記号 $C(x)$ は内田 [**4**] に従っている. 同値類に対する共通の記号はないようである.

例 5.5.

$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 3$ に対して

$$C(1) = \{n \in \mathbb{Z} : 1 \equiv n \pmod 3\} = \{\ldots, -5, -2, 1, 4, \ldots\} = \{3m + 1 : m \in \mathbb{Z}\}$$
$$C(2) = \{n \in \mathbb{Z} : 2 \equiv n \pmod 3\} = \{\ldots, -4, -1, 2, 5, \ldots\} = \{3m + 2 : m \in \mathbb{Z}\}$$
$$C(3) = \{n \in \mathbb{Z} : 3 \equiv n \pmod 3\} = \{\ldots, -6, -3, 0, 3, 6 \ldots\} = \{3m : m \in \mathbb{Z}\}$$

となる. ところで, $0 \equiv 3 \pmod 3$ より, $0 \in C(3)$ だが

$$\begin{aligned} C(0) &= \{n \in \mathbb{Z} : 0 \equiv n \pmod 3\} \\ &= \{n \in \mathbb{Z} : k \in \mathbb{Z} \text{ が存在して } n - 0 = 3k\} \\ &= \{n \in \mathbb{Z} : k \in \mathbb{Z} \text{ が存在して } n - 3 = 3(k - 1)\} \\ &= \{n \in \mathbb{Z} : 3 \equiv n \pmod 3\} = C(3) \end{aligned}$$

となる. また, $2 \not\equiv 1 \pmod 3$ より $2 \notin C(1)$ だが, このとき, $C(1) \cap C(2) = \emptyset$ となる. なぜなら, もし, $n \in C(1) \cap C(2)$ があったとすると, ある $k_1, k_2 \in \mathbb{Z}$ が存在して, $n = 3k_1 + 1 = 3k_2 + 2$ となるから, $2(k_1 - k_2) = 1$ となるはずである. しかし, 左辺は 3 でわり切れるが, 右辺は 3 でわり切れないので矛盾である. よって, $n \in C(1) \cap C(2)$ は存在しない. いいかえると, $C(1) \cap C(2) = \emptyset$ となる.

この具体例の計算は一般の同値関係に対しても成立する. すなわち次が成り立つ.

定理 5.1.

X を集合, $\sim$ を同値関係, $x, y \in X$ とする.

(1) $x \sim y$ ならば $C(x) = C(y)$.

(2) $x \not\sim y$ ならば $C(x) \cap C(y) = \emptyset$.

証明.

1. (1) を示す. すなわち, $x \sim y$ ならば $C(x) = C(y)$ を示す. だから, 集合の包含関係 $C(x) \subset C(y)$ かつ $C(y) \subset C(x)$ を示せばよい. 任意の $z \in C(x)$ に対して, 同値類の定義より $x \sim z$ となる. 仮定より $x \sim y$ だから, 推移律と対称律より

$$z \sim x \sim y \quad \text{すなわち } z \sim y$$

となる. 従って, 同値類の定義より $z \in C(y)$ となるから, $C(x) \subset C(y)$ となる. 逆の包含関係 $C(y) \subset C(x)$ も証明は同様である.

2. (2) を示す. すなわち, $x \not\sim y$ ならば $C(x) \cap C(y) = \emptyset$ を示す. 空集合であることを示すために, 背理法を用いる. すなわち, $z \in C(x) \cap C(y)$ があったとして矛盾を導く. $z \in C(x)$ かつ $z \in C(y)$ だから, 同値類の定義より $x \sim z$ かつ $y \sim z$ が成り立つ. よって, 推移律と対称律を用いると

$$x \sim z \sim y \quad \text{すなわち } x \sim y$$

となるが, これは仮定 $x \not\sim y$ に矛盾する. よって, $C(x) \cap C(y) = \emptyset$ となる. □

この定理 5.1 の意味については, 次節でより詳しく説明する.

問題 5.3.
上の証明で (同様であるといって) 示さなかった $x \sim y$ ならば $C(y) \subset C(x)$ の証明を補え.

例 5.6.
$\mathbb{R}[X]$ に対して, 例 5.4 の同値関係 $\sim$ を考える. $X^2 + X + 1 \in \mathbb{R}[X]$ に対して, $X^2 + X + 1 \sim X$ だから

$$C(X^2 + X + 1) = C(X)$$

となる. $X^2 + 2 \in \mathbb{R}[X]$ に対して, $X^2 + 2 \sim 1$ だから

$$C(X^2 + 2) = C(1)$$

となる. 一般に $f(X) \in \mathbb{R}[X]$ に対して, 一次多項式 $aX + b \in \mathbb{R}[X]$ が存在して

$$f \sim aX + b$$

となることが知られている[2]. 特に定理 5.1 から $f(X) \in \mathbb{R}[X]$ の同値類 $C(f(X))$ の代表元として, 一次多項式 $aX + b \in \mathbb{R}[X]$ がとれて

$$C(f(X)) = C(aX + b)$$

とできる.

問題 5.4.
例 5.4 の同値関係 $\sim$ を考える. $f(X) \in \mathbb{R}[X]$ が次で与えられたときに, $C(f(X)) = C(aX + b)$ となる $a, b \in \mathbb{R}$ を求めよ.

(1) $f(X) = 3X^2 + 4X + 1$
(2) $f(X) = X^3 + X^2 + X + 1$

[2]環論や単因子論, 割り算と約数の話を使う

5.3. 商集合

$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 3$ について

$$\mathbb{Z} = C(0) \cup C(1) \cup C(2) \tag{5.1}$$

が成り立つ. なぜなら, 整数を 3 でわると, 余りは 0 か 1 か 2 のいずれかだからである. さらに

$$C(n) \cap C(m) = \emptyset \quad (n, m = 0, 1, 2 \quad n \neq m)$$

もいえるから, (5.1) の右辺は $\mathbb{Z}$ を三つの集合にわけていることがわかる. そこで, $\mathbb{Z}/3\mathbb{Z} := \{C(0), C(1), C(2)\}$ と定める. 同値類を集合の元とみて新しい集合を作ることができる.

(5.1) は 3 でわった余りに着目して $\mathbb{Z}$ をわけたのであるが, これは同値関係があればいつでも定義することができる.

定義 5.3 (商集合)**.**

X を集合, $\sim$ を同値関係とする. このとき

$$X/\!\sim := \{C(x) : x \in X\}$$

と定義する. $X/\!\sim$ を X の $\sim$ による**商集合**という.

問題 5.5.

$\sim$ を $\equiv \pmod 3$ とする. このとき $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/\!\sim$ を示せ. 特に, $\mathbb{Z}/\!\sim \subset \mathbb{Z}/3\mathbb{Z}$ を示せ.

ここで, 定理 5.1 の意味について説明する. $x, y \in X$ に対して, $x \sim y$ ならば $C(x) = C(y)$, $x \not\sim y$ ならば $C(x) \cap C(y) = \emptyset$ であった. このことから, $C(x) = C(y)$ または $C(x) \cap C(y) = \emptyset$ のどちらかが成り立つことがわかるのだが, 否定を考えると, $C(x) \neq C(y)$ かつ $C(x) \cap C(y) \neq \emptyset$ の両方が成り立つことはないことがわかる. これにより, $X/\!\sim$ は X を互いに交わらない部分集合で分割していることがわかる.

例 5.7.

$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 5$ に対して

$$\begin{aligned}
\mathbb{Z}/5\mathbb{Z} &= \mathbb{Z}/\!\equiv \pmod 5 \\
&= \{C(n) : n \in \mathbb{Z}\} \\
&= \{\ldots, C(-5), C(-4), C(-3), C(-2), C(-1), \\
&\qquad C(0), C(1), C(2), C(3), C(4), C(5), \ldots\} \\
&= \{C(0), C(1), C(2), C(3), C(4)\}
\end{aligned}$$

となる. 定義通りに書くと, たとえば $C(-5) = C(0) = C(5)$ なので, 同じ元がいくつもあることに注意せよ.

さて, $\phi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ を $n \in \mathbb{Z}$ に対して

$$\phi(n) := C(n)$$

で定義すると, ϕ は全射になる. 実際に任意の $C(n) \in \mathbb{Z}/5\mathbb{Z}$ に対して, 代表元 $n \in \mathbb{Z}$ をとれば, $\phi(n) = C(n)$ がわかる. この写像 ϕ は $\mathbb{Z}/5\mathbb{Z}$ を考えるうえで, もっとも自然にあらわれる写像と考えることができる.

定義 5.4 (射影)**.**

X を集合, $\sim$ を同値関係とする. このとき, $\phi : X \to X/\sim$ を $x \in X$ に対して

$$\phi(x) := C(x)$$

で定義する. この ϕ を X から $X/\sim$ への**標準的射影** (canonical projection) という[3].

問題 5.6.

X を集合, $\sim$ を同値関係とするとき, 自然な射影 $\phi : X \to X/\sim$ は全射になることを示せ.

例 5.8.

$\mathbb{R}[X]$ に対して, 例 5.4 の同値関係 $\sim$ を考える. このとき

$$\mathbb{R}[X]/\sim = \{C(f(X)) : f(X) \in \mathbb{R}[X]\} = \{C(aX + b) : a, b \in \mathbb{R}\}$$

となる. なお, 最後の等式は例 5.6 の事実からわかる. この $\sim$ は $X^2 + 1$ での余りが等しいという意味だったので, $\mathbb{R}[X]/(X^2 + 1) := \mathbb{R}[X]/\sim$ と書く. $\mathbb{R}[X]$ から $\mathbb{R}[X]/(X^2 + 1)$ への標準的射影 ϕ は $f(X) \in \mathbb{R}[X]$ に対して

$$\phi(f(X)) = C(f(X)) = C(a + bX) \quad (f(X) \sim aX + b)$$

となる.

より一般に $h(X) \in \mathbb{R}[X]$ を一つ固定したとき, $f(X), g(X) \in \mathbb{R}[X]$ に対して

$$f(X) \sim g(X) \underset{\text{定義}}{\Leftrightarrow} f(X) - g(X) \text{ が } h(X) \text{ でわりきれる}$$

と定義すると, $\sim$ は同値関係になることが確かめられる (各自確かめよ). この同値関係における商集合を $\mathbb{R}[X]/h(X)$ と書く. 今までの例では $h(X) = X^2 + 1$ で考えていたが, $X^2 + 1$ である必要はない.

[3] 自然な射影ということもある

5.4. 同値類による計算と well-defined

$\mathbb{Z}/3\mathbb{Z} = \{C(0), C(1), C(2)\}$ であった. ここで, 次の問題を考える.

3 でわると 1 余る整数を a, 2 余る整数を b とすると, $a+b$ を 3 でわった余りはいくつか?

この問題は文字と式を用いた中学生のいい演習問題であるが, 証明を書いてみよう.

証明.

ある $n, m \in \mathbb{Z}$ が存在して, $a = 3n+1$, $b = 3m+2$ とできるから

$$a + b = (3n+1) + (3m+2) = 3n + 3m + 3 = 3(n+m+1)$$

より $a+b$ を 3 でわると余りは 0. □

この計算のポイントは余りの和 $1+2=3$ が 3 でわりきれることである. つまり, 余り**だけ**を注意すればよい. だから

$$C(1) + C(2) := C(1+2) = C(3) = C(0)$$

と定義すればよいのではないかと思われる. しかし, これには困ることがいくつかある. 例えば, $C(1) = C(4)$, $C(2) = C(5)$ であったが

$$C(1) + C(2) = C(1+2) = C(3)$$
$$C(4) + C(5) = C(4+5) = C(9)$$

となるが, このときに $C(3) = C(9)$ になっているのだろうか? また, 他の場合ではどうなのだろうか? つまり, 代表元をとりかえたときに, 得られる答えが同じのになっているのかどうかを確かめなければいけない.

そこで問題を整理しよう.

問題 $C(a) = C(a')$ と $C(b) = C(b')$, すなわち $a \equiv a' \pmod 3$ と $b \equiv b' \pmod 3$ を仮定する. このときに, $C(a+a') = C(b+b')$ となるのだろうか, すなわち $a+b \equiv a'+b' \pmod 3$ となるのだろうか? (図 5.1 参照)

$$\begin{array}{ccccc} C(a) & + & C(b) & = & C(a+b) \\ \| & & \| & \Rightarrow & \|? \\ C(a') & + & C(b') & = & C(a'+b') \end{array}$$

図 5.1. 問題を数式で書いてみたもの

問題の証明.

$C(a) = C(a')$ と $C(b) = C(b')$ を仮定すると $a \equiv a' \pmod 3$ と $b \equiv b' \pmod 3$ が成り立つのだから, ある $n, m \in \mathbb{Z}$ が存在して $a - a' = 3n$, $b - b' = 3m$ とできる. このとき

$$(a + b) - (a' + b') = (a - a') + (b - b') = 3n + 3m = 3(n + m)$$

となる. $n + m \in \mathbb{Z}$ だから, $a + b \equiv a' + b' \pmod 3$ がわかる. すなわち, $C(a + b) = C(a' + b')$ が成り立つ. □

このことから, $C(a), C(b) \in \mathbb{Z}/3\mathbb{Z}$ に対して

$$C(a) + C(b) := C(a + b) \tag{5.2}$$

と定義することができる. このとき (5.2) の定義は「問題の証明」より代表元 a, b の選び方には依らずに定まる. このとき, (5.2) の定義は **well-defined** であるという[4].

例 5.9.

$C(a), C(b) \in \mathbb{Z}/5\mathbb{Z}$ に対して, $C(a)$ と $C(b)$ とのかけ算を

$$C(a) \cdot C(b) = C(ab)$$

で定義したとき, この計算は well-defined である. すなわち, $C(a) = C(a')$, $C(b) = C(b')$ ならば $C(ab) = C(a'b')$ となる.

証明.

$C(a) = C(a')$, $C(b) = C(b')$ を仮定すると $a \equiv a'$, $b \equiv b' \pmod 5$ より, ある $n, m \in \mathbb{Z}$ が存在して $a - a' = 5n$, $b - b' = 5m$ とできる. 従って,

$$ab = (a' + 5n)(b' + 5m) = a'b' + 5(a'm + b'n + 5mn)$$

より

$$ab - a'b' = 5(a'm + b'n + 5mn)$$

となる. $a'm + b'n + 5mn \in \mathbb{Z}$ より, $ab \equiv a'b' \pmod 5$ がわかる. 従って $C(ab) = C(a'b')$ となる. □

一般に素数 p と $C(a), C(b) \in \mathbb{Z}/p\mathbb{Z}$ に対して

$$C(a) + C(b) := C(a + b)$$
$$C(a) \cdot C(b) := C(a \cdot b)$$

[4] well-defined のいい和訳はなさそうである.

と定義すると, この定義は well-defined になる (実は p は素数でなくてもよい). p が素数のときは, $C(a) \neq C(0)$ かつ $C(b) \neq C(0)$ ならば $C(a) \cdot C(b) \neq C(0)$ がわかる. 対偶をとっていいかえると

$$C(a) \cdot C(b) = C(0) \Longrightarrow C(a) = 0 \text{ または } C(b) = 0$$

となる[5]. p が素数でないときは, この性質はなりたたない. すなわち, $C(a) \neq C(0)$ かつ $C(b) \neq C(0)$ だが $C(a) \cdot C(b) = C(0)$ となることがある.

問題 5.7.

$C(a), C(b) \in \mathbb{Z}/4\mathbb{Z}$ とする.

(1) $C(a), C(b)$ の和 $C(a) + C(b)$ を

$$C(a) + C(b) := C(a + b)$$

により定義する. この定義が well-defined であることを示せ.

(2) $C(a), C(b)$ の積 $C(a) \cdot C(b)$ を

$$C(a) \cdot C(b) := C(ab)$$

により定義する. この定義が well-defined であることを示せ.

(3) $C(a) \neq C(0)$ かつ $C(b) \neq C(0)$ であるが, $C(a) \cdot C(b) = C(0)$ となる $C(a), C(b) \in \mathbb{Z}/4\mathbb{Z}$ をみつけてみよ.

5.5. 応用: $\mathbb{C}$ や $\mathbb{R}$ の構成

5.5.1. 複素数体 $\mathbb{C}$ の構成. $i = \sqrt{-1}$ とおいて, 複素数を考えたが, そもそも, こんな数は存在するのだろうか?問題をはっきりさせるために, もう少し整理したいい方をすると **$\mathbb{C}$ と同じような構造をもつものは $\mathbb{R}$ から作ることができるのだろうか?**[6]ここでは, $\mathbb{R}[X]$ を用いた複素数 $\mathbb{C}$ の構成を説明する[7].

$f(X) \in \mathbb{R}[X]$ に対して, 例 5.4 で定義した同値関係に関する同値類を $\overline{f(X)}$ とあらわすことにする. すなわち

$$\overline{f(X)} := \{g(X) \in \mathbb{R}[X] : f(X) - g(X) \text{ は } X^2 + 1 \text{ で割り切れる. }\}$$

とおく.

[5]つまり, (代数) 方程式が因数分解を用いて解くことができるということである. なお, たし算とかけ算が定義できて, この性質をみたす集合を整域という. 詳しくは環論で学ぶ.

[6]ここでいう構造というものは代数構造のことをいう. つまり, たし算とかけ算が同じということである.

[7]Stewart [**17**] を参考にした.

命題 5.1.
$\overline{f(X)}, \overline{g(X)} \in \mathbb{R}[X]/(X^2+1)$ に対して, $\overline{f(X)}$ と $\overline{g(X)}$ の和と積を

$$\overline{f(X)} + \overline{g(X)} := \overline{f(X)+g(X)}$$
$$\overline{f(X)} \cdot \overline{g(X)} := \overline{f(X)\cdot g(X)}$$

で定める. この定義は well-defined である.

問題 5.8.
命題 5.1 を示せ.

さて $f(X) = a + bX, g(X) = c + dX \in \mathbb{R}[X]$ に対して, 和 $\overline{f(X)} + \overline{g(X)}$, 積 $\overline{f(X)} \cdot \overline{g(X)}$ を計算してみると

$$\begin{aligned} \overline{f(X)} + \overline{g(X)} &:= \overline{(a+c)+(b+d)X} \\ \overline{f(X)} \cdot \overline{g(X)} &:= \overline{(ac-bd)+(ad+bc)X} \end{aligned} \tag{5.3}$$

となる. ところで, $X = i = \sqrt{-1}$ とおいてみると, (5.3) は複素数のたし算とかけ算によく似ている. 実際に

$$(a+bi)+(b+di) := (a+c)+(b+d)i$$
$$(a+bi)\cdot(b+di) := (ac-bd)+(ad+bc)i$$

となることは知っているであろう. また, とりあえず $\mathbb{C}$ を知っているとすると

$$\mathbb{C} \ni a+bi \mapsto \overline{a+bX} \in \mathbb{R}[X]/(X^2+1)$$

は全単射である. つまり, $\mathbb{R}[X]/(X^2+1)$ は $\mathbb{C}$ の集合としてのコピーになっていて, たし算とかけ算が同じになっていることがわかる[8]. $\mathbb{R}[X]/(X^2+1)$ は $\mathbb{R}$ と多項式の計算だけしか使っていない, 特に $\sqrt{-1}$ を使っていないので, $\mathbb{R}[X]/(X^2+1)$ を $\mathbb{C}$ とみなすことができる.

この小節の最後に, どうしてこういう議論が必要なのかを少しだけ説明しておく. $\mathbb{R}$ の世界で $\mathbb{C}$ と同じものが作れなかったとしよう. すると, $\mathbb{C}$ での計算は $\mathbb{R}$ の世界では虚構の計算, 意味のない計算ということになってしまう. なぜなら, $\mathbb{R}$ の世界で $\mathbb{C}$ と同じものがないのだから, $\mathbb{R}$ の世界とは関係のない計算となってしまうはずだからである. しかし, 我々は通常 $\mathbb{R} \subset \mathbb{C}$ と認識しているし, $\mathbb{C}$ が本質的な役割を果たす物理学もある (量子力学は複素数を本質的に用いている). $\mathbb{R}$ から $\mathbb{C}$ を構成できることによって, $\mathbb{R}$ の世界と $\mathbb{C}$ の世界をつなぐことができるのである.

[8] この部分は代数学における群論や環論における同型という言葉を用いるともっとはっきりと説明できる.

5.5.2. 実数体 $\mathbb{R}$ の構成. この節は, E. Hainar, G. Wanner [**16**] の III.1.2 節に基づいている.

自然数 $\mathbb{N}$ はわかっていることにする. 自然数 $\mathbb{N}$ はたし算とかけ算をすることができるが, ひき算はできない ($3-5$ は自然数にならない). 整数 $\mathbb{Z}$ はたし算, ひき算, かけ算をすることができるが, わり算はできない ($1\div 2$ は整数にならない). そして, 有理数 $\mathbb{Q}$ や実数 $\mathbb{R}$ はたし算, ひき算, かけ算と 0 でないわり算をすることができる. では, $\mathbb{Q}$ と $\mathbb{R}$ は何が違うのだろうか?

例えば, $\sqrt{2}$ が有理数でないことは, ピタゴラスの時代, 紀元前に近い時期から知られていたが, 病的な数字として認識されていなかった. その後, さまざまな発展の後に, 2 次方程式を解くための平方根の知識や, さらに多項式の解としては表すことのできない円周率 π や自然対数の底 e, さらには虚数 $i=\sqrt{-1}$ も Euler の時代 (18 世紀) には認識されていたらしい. ところが, 実数 $\mathbb{R}$ とは何か?という問いは, だれもはっきりした答えを出していなかった (そもそも問題意識になっていなかったと思われる). この問題を認識したのが, Cauchy(19 世紀) で, Cauchy は微分 (導関数) や積分, 無限級数が極限であるとつきつめ, 最後に極限とは何か?を考えることが実数 $\mathbb{R}$ を考えることであると問題提起した. この問題提起や Cauchy の証明の多くのギャップを埋めたのが, Weierstrass や Heine, Cantor などである.[9]

話を $\mathbb{Q}$ と $\mathbb{R}$ の違いにもどそう. $\mathbb{R}$ で重要な性質は $\{a_n\}_{n=1}^{\infty}\subset\mathbb{R}$ が Cauchy 列であるとき, すなわち

「任意の $\varepsilon>0$ に対してある $N\in\mathbb{N}$ が存在して, すべての $n,m\in\mathbb{N}$ に対して $n,m\geq N$ ならば $|a_n-a_m|<\varepsilon$」

が成り立つとき, $\{a_n\}_{n=1}^{\infty}$ はある $a\in\mathbb{R}$ に収束すること, すなわち

「任意の $\varepsilon>0$ に対してある $N\in\mathbb{N}$ が存在して, すべての $n\in\mathbb{N}$ に対して $n\geq N$ ならば $|a_n-a|<\varepsilon$」

とできることである. ここで, 強調したいのは, この性質 (**完備**という) は, $\mathbb{Q}$ では成立しないということである. 例えば,

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ldots\to\sqrt{2}\notin\mathbb{Q}$$

は Cauchy 列であるが, $\mathbb{Q}$ 上で収束していない. つまり, 有理数の Cauchy 列の極限を考えると, 有理数にならないことがある.

[9]つまり, 微分積分学での ε-δ 論法などは, 19 世紀の天才達のアイデアである. そう考えると, すぐに理解できるわけないということも容易に想像がつくだろう. だからといって, あきらめてよいと言いたいわけではなく, 理解しようといろいろ考えをめぐらすなどの努力が大切である.

では, この完備性を証明するにはどうしたらよいのだろうか？この問題は「実数 $\mathbb{R}$ とは何か？」という問題に帰着する非常に難しい問題である. この問題は Dedekind と Cantor, Heine によってそれぞれ独立に答えを出した. 以下, Cantor と Heine のアイデアに従った説明をする. Dedekind による実数の構成 (Dedekind 切断を用いる方法) は, 小林 [**8**] を参照せよ.

集合 X を

$$X := \{\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q} : \text{Cauchy 列 }\}$$

とおく. つまり, X は有理 Cauchy 列全体のなす集合である. 集合 X に同値関係 $\sim$ を $\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty} \in X$ に対して

$$\{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty} \underset{\text{定義}}{\Leftrightarrow} \lim_{n\to\infty} |a_n - b_n| = 0$$

によって定義する. このとき, $\sim$ は実際に集合 X の同値関係になる (各自, 確かめよ). このとき, $\mathbb{Q}/\sim$ を $\mathbb{Q}$ の完備化という. このときに $\mathbb{R} := \mathbb{Q}/\sim$ と定義する.

例えば, $\sqrt{2}$ は有理数列

$$a_1 = 1,\ a_2 = 1.4,\ a_3 = 1.41,\ a_4 = 1.414, \ldots \to \sqrt{2}$$

による同値類として定義する. すなわち $\sqrt{2} = C(\{a_n\}_{n=1}^{\infty})$ とする. このとき, 別の有理数列

$$b_1 = 1,\ b_2 = 1.41,\ b_3 = 1.4142,\ b_4 = 1.414213, \ldots \to \sqrt{2}$$

としても, $\sqrt{2} = C(\{b_n\}_{n=1}^{\infty})$ となるが, このとき, $\{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty}$ がわかる. すなわち

$$\sqrt{2} = C(\{a_n\}_{n=1}^{\infty}) = C(\{b_n\}_{n=1}^{\infty})$$

となる.

この定義によって, 実数が何かというものを定義することができた. 次にすべきことは, この実数にたし算とかけ算を定義して, その定義が well-defined であることや, 結合法則, 交換法則, 分配法則や割り算ができることなどを示すことである. これらの細部まで完全な証明は Landau によって与えられた. 証明の中で Landau は多くの部分が「退屈な仕事 “langweilige Mühe”」と記述している. Landau も退屈な仕事といっているくらいなので, このノートでは証明は略する. 興味があれば, Landau [**15**] などを見よ.

$\mathbb{R} = \mathbb{Q}/\sim$ が完備であることを示すには, 不等式と距離を定義しなければいけない. 不等式を定義するために, もし, 収束する数列 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ が $\lim_{n\to\infty} a_n < \lim_{n\to\infty} b_n$ をみたすならば, ある $\varepsilon_0 > 0$ がとれて $\lim_{n\to\infty} a_n + \varepsilon_0 \le \lim_{n\to\infty} b_n$

となるが, このとき, 十分大きなすべての $n \in \mathbb{N}$ に対して $a_n + \varepsilon_0 \leq b_n$ となることに注意しよう.

定義 5.5 (順序)**.**
実数 $C(\{a_n\}_{n=1}^{\infty}),\ C(\{b_n\}_{n=1}^{\infty}) \in \mathbb{R} = \mathbb{Q}/\sim$ に対して,

$$C(\{a_n\}_{n=1}^{\infty}) < C(\{b_n\}_{n=1}^{\infty})$$

であるとは, ある $\varepsilon > 0$ と $N \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n \geq N$ ならば $a_n + \varepsilon \leq b_n$ が成り立つときをいう. また,

$$C(\{a_n\}_{n=1}^{\infty}) \leq C(\{b_n\}_{n=1}^{\infty})$$

であるとは, $C(\{a_n\}_{n=1}^{\infty}) < C(\{b_n\}_{n=1}^{\infty})$ または $C(\{a_n\}_{n=1}^{\infty}) = C(\{b_n\}_{n=1}^{\infty})$ が成り立つときをいう.

距離を定義するためには, 絶対値が定義できていればよいことが知られている (ここで出てくる距離は, 二つの実数を数直線にプロットしたときの離れ具合いと思ってよい. 数学入門 CD, さらには現代解析学などでの話題である).

定義 5.6 (絶対値)**.**
実数 $C(\{a_n\}_{n=1}^{\infty}) \in \mathbb{R} = \mathbb{Q}/\sim$ に対して, $C(\{a_n\}_{n=1}^{\infty})$ の絶対値 $|C(\{a_n\}_{n=1}^{\infty})|$ を

$$|C(\{a_n\}_{n=1}^{\infty})| := C(\{|a_n|\}_{n=1}^{\infty})$$

で定義する. つまり, 有理数列の**絶対値**による同値類で定義する.

具体例で感覚のみ説明しよう. $-\sqrt{2}$ は有理数列

$$a_1 = -1,\ a_2 = -1.4,\ a_3 = -1.41,\ a_4 = -1.414, \ldots \to -\sqrt{2}$$

による同値類として定義できるが, このとき, $|-\sqrt{2}| = \sqrt{2}$ は

$$a_1 = |-1|,\ a_2 = |-1.4|,\ a_3 = |-1.41|,\ a_4 = |-1.414|, \ldots \to |-\sqrt{2}| = \sqrt{2}$$

として定義したことになる.

さて, 絶対値を定義したことにより, 二つの実数の間の距離が定義できたので, Cauchy 列を考えることができる. 最初の問題であった実数の完備性, すなわち実数列の Cauchy 列は収束列であることを証明しよう.

定理 5.2 (実数の完備性)**.**
$\mathbb{R} := \mathbb{Q}/\sim$ は完備である. すなわち, $\{a_n\}_{n=1}^{\infty} \subset \mathbb{Q}/\sim$ を Cauchy 列としたときに, $a \in \mathbb{Q}/\sim$ が存在して, $\lim_{n\to\infty} a_n = a$ となる.

証明.

1. 各 $n \in \mathbb{N}$ に対して, $a_n = C(\{b_n^i\}_{i=1}^\infty)$ となる $\{b_n^i\}_{i=1}^\infty \in X$ を一つ選ぶ. 任意の $j \in \mathbb{N}$ に対して, $\{a_n\}_{n=1}^\infty$ が Cauchy 列だからある $N_j \in \mathbb{N}$ が存在して任意の $n, k \in \mathbb{N}$ に対して

$$n \geq N_j \Longrightarrow |a_n - a_{n+k}| < \frac{1}{j}$$

とできる. このとき, $|a_n - a_{n+k}| = C(\{|b_n^i - b_{n+k}^i|\}_{i=1}^\infty)$ だったことから, すべての $i \in \mathbb{N}$ に対して $|b_{N_j}^i - b_{N_j+k}^i| \leq \frac{1}{j}$ とできる.[10] そこで, 対角線論法を使って, $c_j := b_{N_j}^j$ とおいてみる. 目標は, $a := C(\{c_j\}_{j=1}^\infty)$ に $\{a_n\}_{n=1}^\infty$ が収束することである.

2. 任意の $j \in \mathbb{N}$ に対して $|a_j - c_j| \leq \frac{1}{j}$ を示す. $|a_j - c_j| = C(\{|b_j^k - c_j|\}_{k=1}^\infty)$ より $k \geq N_j$ ならば

$$|b_j^k - c_j| = |b_j^k - b_j^{N_j}| \leq \frac{1}{j}$$

とできる. よって, $|a_j - c_j| \leq \frac{1}{j}$ がわかる.

3. $\{c_j\}_{j=1}^\infty$ が有理 Cauchy 列である, すなわち $\{c_j\}_{j=1}^\infty \in X$ を示す. $j, k \in \mathbb{N}$ について, 有理数 $|c_j - c_{j+k}|$ は有理数と思っても実数と思っても値がかわらないので, 任意の $\varepsilon > 0$ に対して, $\frac{1}{m_0} < \varepsilon$ をみたす $m_0 \in \mathbb{N}$ をとると, $j \geq N_0 := \max\{m_0, N_{m_0}\}$ ならば

$$\begin{aligned} |c_j - c_{j+k}| &= |c_j - a_j + a_j - a_{j+k} + a_{j+k} - c_{j+k}| \\ &\leq |c_j - a_j| + |a_j - a_{j+k}| + |a_{j+k} - c_{j+k}| \\ &\leq \frac{1}{j} + \frac{1}{m_0} + \frac{1}{j+k} \\ &\leq \frac{1}{m_0} + \frac{1}{m_0} + \frac{1}{m_0} \leq 3\varepsilon \end{aligned} \tag{5.4}$$

とできることから, $\{c_j\}_{j=1}^\infty$ が有理 Cauchy 列であることがわかる. そこで, $a = C(\{c_j\}_{j=1}^\infty)$ とおいてみる. $|c_j - a| = C(\{|c_j - c_{j+k}|\}_{k=1}^\infty)$ だから, (5.4) に注意すると, $j \geq N_0$ ならば $|c_j - a| \leq 3\varepsilon$ となることに注意しておく.

4. 最後に $a_n \to a$ $(n \to \infty)$ を示す. $n \geq N_0$ ならば

$$|a_n - a| \leq |a_n - c_n| + |c_n - a| \leq \frac{1}{n} + 3\varepsilon \leq 4\varepsilon$$

[10] 注意深く考えると, ある $N \in \mathbb{N}$ が存在して, $i \geq N$ でなければ, この不等式はそのままでは成立しないことがわかる. しかし, 代表元となる有理 Cauchy 列をとりかえることにより, この不等式がすべての $i \in \mathbb{N}$ で成立することが示せる.

となるので, $a_n \to a$ $(n \to \infty)$ がわかる. □

5.6. 演習問題

問題 5.9 (有理数の構成)**.**

$m, m' \in \mathbb{Z}$, $n, n' \in \mathbb{N}$ が $\dfrac{m}{n} = \dfrac{m'}{n'}$ ならば $mn' = m'n$ である. $mn' = m'n$ は整数の性質しか使っていないことに注意して, 整数から有理数を構成してみよう. 以下の問題では, **分数をおもてに出さずに考えよ.**

$(m, n), (m', n') \in \mathbb{Z} \times \mathbb{N}$ に対して,

$$(m, n) \sim (m', n') \underset{\text{定義}}{\Leftrightarrow} mn' = m'n$$

で定義する.

(1) $\sim$ が $\mathbb{Z} \times \mathbb{N}$ 上の同値関係となることを示せ (ヒント: 少し難しいのは推移律の証明. もし, $\dfrac{m}{n} = \dfrac{m'}{n'}, \dfrac{m'}{n'} = \dfrac{m''}{n''}$ ならば**両辺に n' をかけることで,** $\dfrac{mn'}{n} = m' = \dfrac{m''n'}{n''}$ となることがわかる. このアイデアを推移律の証明にどう反映させればよいか考えてみよ).

(2) $\overline{(m, n)}$ を $(m, n) \in \mathbb{Z} \times \mathbb{N}$ の $\sim$ に関する同値類とする. このとき, $(m, n), (m', n') \in \mathbb{Z} \times \mathbb{N}$ に対して足し算 $\overline{(m, n)} + \overline{(m', n')}$ と掛け算 $\overline{(m, n)} \cdot \overline{(m', n')}$ を

$$\overline{(m, n)} + \overline{(m', n')} := \overline{(mn' + m'n, nn')}, \quad \overline{(m, n)} \cdot \overline{(m', n')} := \overline{(mm, nn')}$$

で定義する. この足し算と掛け算の定義がそれぞれ well-defined であることを示せ.

以上により, $(\mathbb{Z} \times \mathbb{N})/\sim$ に足し算と掛け算が定義できることがわかった. さらに頑張ると, この演算が結合法則や分配法則などをみたすことが示せる (少し面倒). よって, $\mathbb{Q} := (\mathbb{Z} \times \mathbb{N})/\sim$ と定義することができる.

問題 5.10.

$M_n(\mathbb{R})$ を n 次実数値正方行列のなす集合, $GL_n(\mathbb{R})$ を n 次実数値正則行列のなす集合とする. このとき $A, B \in M_n(\mathbb{R})$ に対して

$$A \sim B \underset{\text{定義}}{\Longleftrightarrow} \text{ある } P \in GL_n(\mathbb{R}) \text{ が存在して } A = P^{-1}BP$$

で定義する. なお, $A, B \in M_n(\mathbb{R})$ に対して, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ となることと $\det(AB) = \det(A)\det(B)$ となることは認めてよい.

(1) $\sim$ は $M_n(\mathbb{R})$ 上の同値関係になっていることを示せ.

(2) $[A]$ を $A \in M_n(\mathbb{R})$ の $\sim$ に関する同値類とする．このとき, $\mathrm{tr}([A]) := \mathrm{tr}(A)$ と定めると, この定義が well-defined であることを示せ.
(3) $\det([A]) := \det(A)$ と定めると, この定義が well-defined であることを示せ.

第 6 章

集合の濃度

無限という言葉は数学のみならず, いろいろなところで聞くことができる. 例えば, 「素数は無限個存在する」は, 背理法のいい練習問題である. また, 実数列が無限大に発散するという表現も微積分ではよく使う. さて, これらの無限というのはすべて同じものであろうか?もう少し問題をわかりやすくいうと, 無限集合 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ の元の個数は同じだろうか？違うのだろうか？この問題に答えるためには, 元の個数を数えることを数学の言葉で表現しなければならない.

集合の元の個数は「集合の濃度」という. 最初に, 集合の濃度の定義といくつかの具体例を説明する. 次に, 無限集合のなかでもとりわけ重要な可算集合について説明する. この章の最後に, 集合全体が集合の濃度について順序付けできることと, その順序が全順序となることを主張する Bernstein の定理について説明する.

6.1. 集合の濃度

素朴に考えるために, 有限個の場合, 例えば二つの集合 $A = \{a, b, c, d, e\}$, $B = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ で個数を数える問題を考える. この集合 A と B の集合の元の個数はどちらも 5 個であることは見れば明らかであるが, これを数学の言葉で表現したい.

そのために, ものさしとなる集合 $C = \{1, 2, 3, 4, 5\}$ を用意する. この集合の元の個数が 5 個であることはわかっていることにする. なぜなら, 集合 C は数を使って作った集合だからである. 次に $f : C \to A$ を

$$f(1) = a, \quad f(2) = b, \quad f(3) = c \quad f(4) = d, \quad f(5) = e$$

で定義する. この写像は, 集合 A の元にそれぞれ番号付けをしたものだと思えばよいだろう. このとき f は全単射になる. なぜなら, 単射は「A のどの 2 つの元も番号が違う」ということであり, 全射は「A のどの元にも番号がついている」ということだからである.

問題 6.1.
上記の写像 $f : C \to A$ が全単射であることを定義にもとづいて示せ.

この全単射写像 f によって, 集合 A の元の個数が 5 個であることが特徴付けられた. つまり, 全単射写像が存在すれば, 元の個数が同じということができる. この特徴を用いて, 集合の濃度を定義しよう.

定義 6.1 (濃度)**.**
集合 X, Y の**濃度が等しい**とは, 全単射写像 $f : X \to Y$ が存在するときをいう. このとき, $X \sim Y$ や $\#X = \#Y$ と書いたりする.

有限集合の場合, 例えば $\#\{1, 2, 3, 4, 5\} = 5$ と書いたりする.

命題 6.1 (同値関係)**.**
集合 A, B, C に対して, 次が成り立つ.

(1) $A \sim A$,
(2) $A \sim B$ ならば $B \sim A$,
(3) $A \sim B$, $B \sim C$ ならば $A \sim C$.

問題 6.2.
命題 6.1 を示せ.

例 6.1.
$n \in \mathbb{N}$, $A = \{1, 2, 3, \ldots, n\}$, $B = \{1, 2, 3, \ldots, n, n+1\}$ とすると, $\#A = n$, $\#B = n+1$ となり, 実際に $\#A \neq \#B$ が示せる. 一般に**有限集合** A, B に対して, $A \subset B$ かつ $A \neq B$ であれば, $\#A \neq \#B$ が成り立つ.

証明 (鳩ノ巣原理).
全単射 $f : A \to B$ が存在したとすると, f は全射だから, ある $a_1 \in A$ が存在して $f(a_1) = 1$ となる. 同様に, $a_2 \in A$ が存在して $f(a_2) = 2$, $a_3 \in A$ が存在して $f(a_3) = 3$,..., ある $a_n \in A$ が存在して $f(a_n) = n$ とできる. このとき, f が単射だから, $i \neq j$ ならば $a_i \neq a_j$ となることに注意すると, a_1 から a_n はすべて違う自然数になるはずである. また $a_{n+1} \in A$ が存在して $f(a_{n+1}) = n+1$ となるが, A の元の個数は n 個だから, a_{n+1} は a_1 から a_n のどれかに等しい. これは f が単射だったことに反する. □

例 6.1 でわかるとおり, 有限集合については濃度は集合の元の個数をそのまま扱っていることがわかる. しかし, 無限集合についての濃度はそれほど自明ではない.

例 6.2.
$A = \{2n : n \in \mathbb{N}\}$ とおくと, $\#A = \#\mathbb{N}$. つまり, 正の偶数全体の集合と, 自然数全体の集合の濃度は等しい.

証明.

$f : \mathbb{N} \to A$ を $n \in \mathbb{N}$ に対して, $f(n) := 2n$ とおくと, f が全単射写像になることを示す. これにより, 全単射写像 $f : \mathbb{N} \to A$ が存在するので, 命題 6.1 とくみあわせて $\#A = \#\mathbb{N}$ がわかる.

1. f が単射になることを示す. 任意の $n, m \in \mathbb{N}$ に対して, $f(n) = f(m)$ ならば, $2n = 2m$ より $n = m$ となる.

2. f が全射になることを示す. 任意の $y \in A$ に対して, $n \in \mathbb{N}$ が存在して $y = 2n$ とかける. よって $f(n) = 2n = y$ となる. □

問題 6.3.

$A := \{2n + 1 : n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}\}$ とおくとき, $\#A = \#\mathbb{N}$ を示せ.

例 6.3.

$\#\mathbb{N} = \#\mathbb{Z}$. つまり, $\mathbb{N}$ と $\mathbb{Z}$ は集合の元の個数が等しい.

証明.

$f : \mathbb{N} \to \mathbb{Z}$ を $n \in \mathbb{N}$ に対して,

$$f(n) := (-1)^n \left[\frac{n}{2}\right]$$

とおく. ここで, $\left[\frac{n}{2}\right]$ は $\frac{n}{2}$ を越えない最大の整数である (Gauss 記号という).

この f は全単射になる. 実際に

$$f(1) = (-1)^1 \left[\frac{1}{2}\right] = 0, \qquad f(2) = (-1)^2 \left[\frac{2}{2}\right] = 1,$$
$$f(3) = (-1)^3 \left[\frac{3}{2}\right] = -1, \qquad f(4) = (-1)^4 \left[\frac{4}{2}\right] = 2,$$
$$f(5) = (-1)^5 \left[\frac{5}{2}\right] = -2, \ldots$$

となる. □

問題 6.4.

例 6.3 の証明で定めた関数 $f : \mathbb{N} \to \mathbb{Z}$ が全単射になることを確かめよ.

例 6.4.

$\#\mathbb{N} = \#(\mathbb{N} \times \mathbb{N})$. つまり, $\#\mathbb{N}$ と $\#(\mathbb{N} \times \mathbb{N})$ の元の個数は等しい[1].

[1] このことから, 濃度は次元を区別できないだろうことが推測される. なぜなら $\mathbb{N}$ と $\mathbb{N}^2$ を同じものと認識してしまっているからである. この事実は例 6.8 で再度説明する.

証明.

$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を $(n, m) \in \mathbb{N}$ に対して

$$f(n, m) := m + \frac{(n + m - 1)(n + m - 2)}{2} = m + \sum_{k=1}^{n+m-2} k$$

と定めると, $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ は全単射になる. □

つまり, 無限集合の場合は $A \subset B$, $A \neq B$ であっても $\#A = \#B$ となることがある. 例 6.3, 例 6.4 のように $\mathbb{N}$ と $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$ の元の個数が同じという, 一見すると不思議に思えることが成り立つ. 直感的には, $\mathbb{Z}$ は $\mathbb{N}$ に比べて, 元の個数が 2 倍くらい多いと思えるだろうし, $\mathbb{N} \times \mathbb{N}$ は $\mathbb{N}$ に比べて, 元の個数が 2 乗くらい多いと思えるだろう. しかし, 無限個の世界を全単射で比較すると, それはたいした差ではないということがわかる.

問題 6.5.

$a, b \in \mathbb{R}$ が $a < b$ をみたすとする. このとき $\#(a, b) = \#(0, 1)$, $\#[-a, b] = \#[0, 1]$ を示せ (ヒント: 一次関数を考える. 問題 2.13 も参考にせよ.).

問題 6.6.

定義に基づいて, 次を示せ.

(1) $\#\mathbb{N} = \#\{2n : n \in \mathbb{Z}\}$
(2) $\#\mathbb{N} = \#\mathbb{N}^3$
(3) $\#\mathbb{R} = \#\mathbb{C}$

6.2. 可算集合

$\mathbb{N}$ と同じ濃度の集合は特別な性質を持っている. つまり, 例 6.3, 例 6.4 でみたように $\mathbb{Z}$ や $\mathbb{N} \times \mathbb{N}$ は特別な性質を持っている.

定義 6.2 (可算集合)**.**

$\#\mathbb{N} = \aleph_0$(アレフゼロと読む) と書く. $\#A = \aleph_0$ となる集合 A を**可算集合**という. また, 集合 A が有限集合か可算集合であるとき, **たかだか可算集合** という.

可算集合のもつ特徴として, 「無限集合として一番小さい」という性質がある. 実際に次の定理が成り立つ.

定理 6.1.

A を可算集合, $B \subset A$ を無限集合とすると, B は可算集合, すなわち $\#B = \aleph_0$ となる.

証明には, 選択公理と (次の節で説明する)Bernstein の定理を用いる. この定理は認めることにする.

例 6.5 (あとで別の証明をする)**.**
$\mathbb{Q}$ は可算集合, すなわち $\#\mathbb{Q} = \aleph_0$ となる.

理由 (厳密な議論ではない).
$\dfrac{p}{q} \in \mathbb{Q}$ を $(p, q) \in \mathbb{Z} \times \mathbb{N}$ とみなすと, $\mathbb{Q} \subset \mathbb{Z} \times \mathbb{N}$ となる. $\mathbb{Q}$ は無限集合で, $\#(\mathbb{Z} \times \mathbb{N}) = \aleph_0$ より $\#\mathbb{Q} = \aleph_0$ である. □

例 6.6.
$\mathbb{R}$ は可算集合ではない. つまり, 可算集合でない無限集合が存在する.

証明 (Cantor の対角線論法).
$\#\mathbb{R}$ が可算集合ならば, その部分集合 $(0, 1] \subset \mathbb{R}$ も可算集合なので, 全単射写像 $a : \mathbb{N} \to (0, 1]$ が存在する. そこで,

$$a(n) = 0, a_{n1}a_{n2}a_{n3}\ldots = \frac{a_{n1}}{10} + \frac{a_{n2}}{10^2} + \frac{a_{n3}}{10^3} + \cdots$$

と無限小数で書くことにする. ただし, a_{ni} は 0 から 9 までの整数であり,

$$1 = 0.9999\ldots, \quad 0.2 = 0.1999\ldots$$

などと書くことにする.

$$\begin{aligned} a(1) &= 0, a_{11}a_{12}a_{13}a_{14}\ldots \\ a(2) &= 0, a_{21}a_{22}a_{23}a_{24}\ldots \\ a(3) &= 0, a_{31}a_{32}a_{33}a_{34}\ldots \\ a(4) &= 0, a_{41}a_{34}a_{43}a_{44}\ldots \end{aligned}$$

と書いたときに, a_{11}, a_{22}, a_{33}, $a_{44}, \ldots$ に着目して, $n \in \mathbb{N}$ に対して

$$b_n = \begin{cases} 1 & a_{nn}\text{が偶数} \\ 2 & a_{nn}\text{が奇数} \end{cases}$$

とおくと, 一つの実数 $b = 0.b_1b_2b_3b_4\ldots \in (0, 1]$ が定まる. このとき, $b = a(n)$ となる $n \in \mathbb{N}$ は存在しない. 実際, 任意の $n \in \mathbb{N}$ に対して, 偶奇が異なるので $a_{nn} \neq b_n$ となるから $a(n) \neq b$ である. 従って a が全単射であったことに矛盾する. □

この証明に使った, 対角成分を選ぶ手法を **Cantor の対角線論法**という. Cantor の対角線論法は, 部分列の存在を示すときによく用いられる.

定義 6.3 (連続濃度, 非可算集合)**.**

$\mathbb{R} = \aleph$(アレフと読む) と書き, **連続濃度**という. 集合 A がたかだか可算集合でないとき, **非可算集合**という.

例 6.7.

$\#(-1,1) = \aleph$.

証明.

$f : \mathbb{R} \to (-1,1)$ を $x \in \mathbb{R}$ に対して

$$f(x) = \frac{2}{\pi}\arctan(x) = \frac{2}{\pi}\int_0^x \frac{1}{1+y^2}\,dy$$

で定めると, f は全単射になることが示される. 証明には, 定理 2.4 を用いる. □

例 6.8.

$\#(\mathbb{R}\times\mathbb{R}) = \#(\mathbb{R}^2) = \aleph$ が成り立つ. つまり, **濃度では次元を区別できない.** これを示すための全単射写像 $f : \mathbb{R} \to \mathbb{R}^2$ はかなり複雑である.

例 6.9.

$\#\mathbb{R} \neq \#2^{\mathbb{R}} = \#\{A : A \subset \mathbb{R}\}$. 一般に集合 X に対して, $\#X \neq \#2^X$. 従って, いくらでも濃度の違う集合が存在する.

問題 6.7.

次の集合は可算集合か否か答えよ.

(1) $\mathbb{Z}$
(2) $\mathbb{Q}$
(3) $\mathbb{R}$
(4) $\mathbb{C}$
(5) $\mathbb{N}\times\mathbb{N}$
(6) $\mathbb{N}\times\mathbb{R}$
(7) $2^{\mathbb{N}}$
(8) $\{f : \mathbb{N} \to \mathbb{R}\}$ ($\mathbb{N}$ から $\mathbb{R}$ への写像全体のなす集合)
(9) $\{A : A$ は整数を成分とする 3 次正方行列 $\} = M_3(\mathbb{Z})$
(10) $\mathbb{R}^3$
(11) $\mathbb{Z}/3\mathbb{Z}$

6.3. Bernstein の定理

$A = \{1,2,3,4,5\}$, $B = \{1,2,3,4,5,6\}$ とおくと, $\#A \leq \#B$ としたくなるだろう. 実際に A の元の個数は 5 個, B の元の個数は 6 個で, A の元の個数より

多いからである. これを数学で表現するために, $f : A \to B$ を

$$f(1) = 1,\ f(2) = 2,\ f(3) = 3,\ f(4) = 4,\ f(5) = 5$$

と定義してみる. このとき, f は単射になることがわかる. 一般に有限集合 A, B に対して $f : A \to B$ が単射であるとき, B の元の個数は A の元の個数より多いことがわかる (鳩の巣原理を使う). そこで, 次の定義を与える.

定義 6.4.
集合 X, Y に対して, $\#X \leq \#Y$ であるとは, 単射 $f : X \to Y$ が存在することである. $\#X < \#Y$ であるとは, $\#X \leq \#Y$ かつ $\#X \neq \#Y$ であることをいう.

例 6.10.
$f : \mathbb{N} \to \mathbb{R}$ を $n \in \mathbb{N}$ に対して $f(n) := n$ と定めると, f は単射になることが容易にわかる. 従って, $\#\mathbb{N} \leq \#\mathbb{R}$ がわかる. 例 6.6 により, $\#\mathbb{N} \neq \#\mathbb{R}$ であったから, $\#\mathbb{N} < \#\mathbb{R}$ もわかる[2].

$x, y, z \in \mathbb{R}$ に対して, 「$x \leq x$ となること」と, 「$x \leq y, y \leq z$ ならば $x \leq z$」は自明であろう[3]. これと同じことは集合の濃度についても成り立つ. すなわち, 次の命題が成り立つ.

命題 6.2.
X, Y, Z を集合とする.

(1) $\#X \leq \#X$,
(2) $\#X \leq \#Y$ かつ $\#Y \leq \#Z$ ならば $\#X \leq \#Z$.

問題 6.8.
命題 6.2 を示せ.

$x, y \in \mathbb{R}$ に対して, 「$x \leq y$ かつ $y \leq x$ ならば $x = y$ となること」は不等式で非常に重要な性質である. この性質が集合の濃度についても成り立つかどうかはまったく自明ではない. つまり, 集合 X, Y に対して, 「$\#X \leq \#Y$ かつ $\#Y \leq \#X$」が成り立つからといって, $\#X = \#Y$, すなわち, X から Y への全単射写像が存在するかどうかは簡単な問題ではない. 幸いにして, 次の定理が知られている.

[2] $\#\mathbb{N} < \#X < \#\mathbb{R}$ となる集合 X が存在しないことを**連続体仮説**という. 連続体仮説は (標準的な数学の枠組みのうえでは) 証明できないことが知られている.

[3] 証明せよといわれると難しい問題である. 実数とは何か? にたちかえらなければならない

定理 6.2 (Bernstein の定理)**.**
集合 X, Y に対して, $\#X \leq \#Y$ かつ $\#Y \leq \#X$ ならば $\#X = \#Y$ が成り立つ. つまり, 単射 $f : X \to Y$ と $g : Y \to X$ が存在すれば, 全単射写像 $F : X \to Y$ が存在する.

証明については, 内田 [**4**] を参照されたい. 命題 6.2 と定理 6.2 より

1. 任意の集合 X に対して $\#X \leq \#X$,
2. 任意の集合 X, Y に対して $\#X \leq \#Y$, $\#Y \leq \#X$ ならば $\#X = \#Y$,
3. 任意の集合 X, Y, Z に対して $\#X \leq \#Y$, $\#Y \leq \#Z$ ならば $\#X \leq \#Z$

が成り立つ. この 3 条件が成り立つとき, $\leq$ を**半順序**とか**半順序関係**という. また, $\mathscr{U}$ を集合全体[4]としたときに, $(\mathscr{U}, \leq)$ を**半順序集合** という. 実は, $X, Y \in \mathscr{U}$ に対して,

$$\#X \leq \#Y \text{ または } \#Y \leq \#X \tag{6.1}$$

のどちらかは必ず成立する[5]. 半順序集合が (6.1) の性質を持つとき, **全順序集合**という. 例えば $(\mathbb{R}, \leq)$ や $(\mathscr{U}, \leq)$ は全順序集合である.

例 6.11.
$\#\mathbb{Q} = \#\mathbb{N}$ であることを Bernstein の定理を使って示せる. 実際に, 単射 $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ を $r = \dfrac{p}{q} \in \mathbb{Q}$ に対して, $f(r) = (p, q)$ と定めればよい. ただし, p, q は既約で, $q \in \mathbb{N}$ とする.

問題 6.9.
例 6.11 のアイデアを用いて, $\mathbb{Q}$ が可算集合であることを示せ.

問題 6.10.
Bernstein の定理を用いて, $\#[0, 1] = \#(0, 1)$, $\#[0, 1) = \#(0, 1)$ を示せ.

問題 6.11.
Bernstein の定理を用いて, $\#\mathbb{R} = \#(\mathbb{R} \times \mathbb{R})$ を示せ (ヒント: $x \in \mathbb{R}$ に対して, $e^x \geq 0$ であることを用いると, $\mathbb{R} \times \mathbb{R}$ から $\mathbb{R}$ への単射が構成できる.).

---

[4]Universe という. 上記の「任意の集合」は,「集合とは何か?」を先に定義しておかないと矛盾がおきることが知られている. なぜ $\mathscr{U}$ を設定しなければいけないかは, 演習問題 6.15(Russell のパラドックス) を考えてみよ.

[5]証明には選択公理を用いる.

6.4. 演習問題

問題 6.12.

$f : [0,1] \to (0,1)$ を $x \in [0,1]$ に対して

$$f(x) := \begin{cases} \dfrac{1}{2} & x = 0 \\ \dfrac{x}{2^2} & x = \dfrac{1}{2^n} \quad (n \in \mathbb{N} \cup \{0\}) \\ x & x \neq 0, \dfrac{1}{2^n} \quad (n \in \mathbb{N} \cup \{0\}) \end{cases}$$

と定めたときに, f が全単射となることを示せ. 従って, $\#[0,1] = \#(0,1)$ となる[6].

問題 6.13.

例 6.4 で定めた関数 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ が全単射になることを示せ (ヒント: 単射の証明は $f(n_1, m_1) = f(n_2, m_2)$ を仮定したときに, $n_1 + m_1 = n_2 + m_2$ かそうでないかで場合わけしてみよ).

問題 6.14.

実数の完備性を示した定理 5.2 は, Cantor の対角線論法と同様の議論を用いている. どのように用いているか考察せよ.

問題 6.15 (Russell のパラドックス)**.**

集合族 $\mathscr{U}$ を

$$\mathscr{U} := \{A : A \text{ は集合で } A \notin A \text{ が成り立つ }\} \tag{6.2}$$

と定義する. このとき, 次を示せ.

(1) $\mathscr{U} \notin \mathscr{U}$ とすると矛盾が成り立つ.

(2) $\mathscr{U} \in \mathscr{U}$ とすると矛盾が成り立つ.

つまり, 集合を素朴に第 1 章の定義で定めると, (6.2) のように定義は一見するとできているようだが, $\mathscr{U} \in \mathscr{U}$ を真とも偽ともできない矛盾が生じる. この矛盾を解消するためには, 先に集合全体が何か？を決めておく必要がある.

[6] 連続な全単射写像 $f : [0,1] \to (0,1)$ は存在しないことが知られている (位相空間論の知識, 特にコンパクトの知識を使う). 従って, $[0,1]$ から $(0,1)$ への全単射な写像は不連続な関数になる.

第 7 章

選択公理とその周辺

$\{A_\lambda\}_{\lambda\in\Lambda}$ を集合族, Λ を添字集合とする (わかりにくければ, $\Lambda=\mathbb{N}$ と思っておいてよい). このときに無限個の直積集合は

$$\prod_{\lambda\in\Lambda} A_\lambda := \left\{ f : \lambda \to \bigcup_{\lambda\in\Lambda} A_\lambda,\ \text{任意の}\lambda\in\Lambda\text{に対して } f(\lambda)\in A_\lambda \right\}$$

と定義するのであった. なお, $\Lambda=\mathbb{N}$ のときは, $a_1\in A_1$, $a_2\in A_2$, $a_3\in A_3\ldots$ に対して

$$(a_1,a_2,a_3,\ldots)\in\prod_{n\in\mathbb{N}} A_n = A_1\times A_2\times A_3\cdots$$

と思っておけばよい. このとき, 選択公理とは「任意の $\lambda\in\Lambda$ に対して, $A_\lambda\neq\emptyset$ ならば, $\prod_{\lambda\in\Lambda} A_\lambda\neq\emptyset$ となる」であった. この選択公理と同値な命題はよく用いられる.

定理 7.1.
以下は同値となる.

(1) 選択公理が成り立つ
(2) 帰納的半順序集合は極大元を持つ (Zorn の補題)
(3) すべての集合は, ある半順序を考えることで整列集合とできる (整列可能定理)

この節での目標は定理 7.1 の主張の理解, 特に Zorn の補題と整列可能定理の主張を理解することである. なお, 定理 7.1 はこのノートでは証明しない. 証明については, 内田 [**4**] を参照せよ.

7.1. Zorn の補題

7.1.1. 順序関係. 同値関係は集合の二つの元が「等しい」ことを抽象化したものであった. 順序関係は集合の二つの元の「大きさが比較できる」ことを抽象化したものである.

定義 7.1 (半順序集合)**.**

X を集合, $x, y \in X$ に対して, $x \leq y$ または $x \not\leq y$ のどちらかが成り立つ規則 $\leq$ が与えられていて次をみたすとき, $\leq$ を**半順序**といい, $(X, \leq)$ を**半順序集合**という.

(1) (反射律) 任意の $x \in X$ に対して $x \leq x$.
(2) (反対称律) 任意の $x, y \in X$ に対して $x \leq y$, $y \leq x$ ならば $x = y$.
(3) (推移律) 任意の $x, y, z \in X$ に対して $x \leq y, y \leq z$ ならば $x \leq z$.

例 7.1.

$\leq$ を $\mathbb{R}$ の通常の不等式とすると, $(\mathbb{R}, \leq)$ は半順序集合になる. 半順序集合は $\mathbb{R}$ の不等式を一般化したものである.

例 7.2.

$\mathscr{U}$ を集合全体としたときに, $(\mathscr{U}, \subset)$ は半順序集合になる. 反対称律は集合の等号の定義そのものである.

例 7.3.

$\leq$ を $\mathbb{R}$ の通常の不等式とすると, $(\mathbb{C}, \leq)$ は半順序集合ではない. 例えば, $i = \sqrt{-1} \leq 1$ などの意味がないことに注意せよ.

半順序集合 $(X, \leq)$ と $x, y \in X$ について, 「$x \leq y$ か $y \leq x$ のどちらかが成り立つ」ことは定義には含まれていない. つまり, x と y のどちらが大きいか? という質問に, 半順序集合は答えを出すことができない. この「x と y のどちらが大きいか?」に答えが出せる集合を定義する.

定義 7.2 (全順序集合)**.**

半順序集合 $(X, \leq)$ が**全順序集合**であるとは, 任意の $x, y \in X$ に対して, $x \leq y$ または $y \leq x$ のどちらかが成り立つことである.

例 7.4.

$(\mathbb{R}, \leq)$ は全順序集合である. 実際に任意の $x, y \in \mathbb{R}$ に対して, $x \leq y$ または $y \leq x$ は成立する (つまり, どちらかが常に大きいという関係があるということ)

例 7.5.

$\mathscr{U}$ を集合全体としたときに, $(\mathscr{U}, \subset)$ は全順序集合にならない. 例えば, $A = \{1, 2, 3\}$, $B = \{3, 4\}$ とすると, $A \not\subset B$ かつ $B \not\subset A$ である.

大きい, 小さいの概念が定まると「上界」や「下界」を考えることができる. 大雑把にいえば, 「いちばん大きいもの」や「いちばん小さいもの」が上限, 下

限であったが, これらは大きい, 小さいの概念があれば定義できた. そこで, 半順序集合における上界や下界, 上限, 下限を定義しよう.

定義 7.3 (上界, 下界, 上限, 下限)**.**
$(X, \leq)$ を半順序集合, $A \subset X$ とする.

- $y \in X$ が A の**上界**であるとは, 任意の $a \in A$ に対して, $a \leq y$ が成り立つことをいう.
- $y \in X$ が A の**下界**であるとは, 任意の $a \in A$ に対して, $y \leq a$ が成り立つことをいう.
- $y \in X$ が A の最大元であるとは, $y \in A$ かつ, 任意の $a \in A$ に対して $a \leq y$ が成り立つことをいう. このとき, $y = \max A$ と書く.
- $y \in X$ が A の最小元であるとは, $y \in A$ かつ, 任意の $a \in A$ に対して $y \leq a$ が成り立つことをいう. このとき, $y = \min A$ と書く.
- $y \in X$ が A の**上限**であるとは, 集合 $\{x \in X : x \text{ は } A \text{ の上界 }\}$ に最小元が存在して

$$y = \min\{x \in X : x \text{ は } A \text{ の上界 }\}$$

となることをいう.

- $y \in X$ が A の**下限**であるとは, 集合 $\{x \in X : x \text{ は } A \text{ の下界 }\}$ に最大元が存在して

$$y = \max\{x \in X : x \text{ は } A \text{ の下界 }\}$$

となることをいう.

例 7.6.
全順序集合 $(\mathbb{R}, \leq)$ の部分集合 $[0, 1) \subset \mathbb{R}$ の上限と下限を調べてみる.

$$\begin{aligned}\{x \in \mathbb{R} : x \text{ は } [0,1) \text{ の上界 }\} &= \{x \in \mathbb{R} : \text{任意の } y \in [0,1),\ y \leq x\} \\ &= [1, \infty), \\ \{x \in \mathbb{R} : x \text{ は } [0,1) \text{ の下界 }\} &= \{x \in \mathbb{R} : \text{任意の } y \in [0,1),\ x \leq y\} \\ &= (-\infty, 0]\end{aligned}$$

となることがわかる. よって,

$$\sup[0,1) = \min\{x \in \mathbb{R} : x \text{ は } [0,1) \text{ の上界 }\} = \min[1, \infty) = 1$$
$$\inf[0,1) = \max\{x \in \mathbb{R} : x \text{ は } [0,1) \text{ の下界 }\} = \max(-\infty, 0] = 0$$

となる. $\mathbb{R}$ の上限, 下限の直感的な理解である「一番大きい値」, 「一番小さい値」に一致していることがわかる.

7.1.2. Zornの補題. さて, Zornの補題を説明するために必要な,「帰納的」と「極大元」について説明しよう.

定義 7.4 (帰納的)**.**
半順序集合 $(X, \leq)$ が**帰納的**であるとは, 任意の $Y \subset X$ に対して, $(Y, \leq)$ が全順序集合ならば, Y は上界を持つことである.

帰納的をどういう意図で専門用語として使うようになったのかは筆者は知らない (wikipedia English を読んだが, 対応する英語はみつからなかった). ただし, 帰納的な半順序集合は数学的帰納法が成り立つような全順序集合を作ることができる. 実際に, $x_1 \in X$ を一つ選ぶと, $(\{x_1\}, \leq)$ は全順序集合になる. よって, 上界をもつから, それを $x_2 \in X$ とおく. すると $(\{x_1, x_2\}, \leq)$ はまた全順序集合になるから, 上界 $x_3 \in X$ が取れる. すると $(\{x_1, x_2, x_3\}, \leq)$ がまた全順序集合になるから, これを繰り返すと, 帰納的に全順序集合を構成することができる.

問題 7.1.
上記の $(\{x_1, x_2\}, \leq)$ や $(\{x_1, x_2, x_3\}, \leq)$ が全順序集合になることを確かめよ.

次に, 極大元を定義しよう.

定義 7.5 (極大元)**.**
半順序集合 $(X, \leq)$ に対して, $a \in X$ が**極大元**であるとは, $a \leq x$ かつ $a \neq x$ となる $x \in X$ が存在しないことである.

$a \in X$ が極大元であるということの直感的な意味は, $a < x$ となる $x \in X$ はないということである. なぜ, このような書き方をしないかというと, $a < x$ という記号を定義していないからである ($a < x$ とは $a \leq x$ かつ $a \neq x$ となることと定義してもよいが, 通常は定義しない).
これらの準備のもとで, Zornの補題の主張を記述することができる.

定理 7.2 (Zornの補題)**.**
$(X, \leq)$ を帰納的半順序集合とする. このとき, X に極大元 $a \in X$ が存在する.

注意 7.1.
Zornの補題は何か具体的に書くことができないもの (関数とか集合とか) の存在を示すときに使うことが多い[1]. 存在を示したいものをみたすような集合を作り, その集合が帰納的な半順序を定義できることを示す.

[1]関数解析学における基本定理ともいえる, Hahn-Banachの定理や, コンパクト位相空間の積位相空間のコンパクト性に関するTychonoffの定理は, Zornの補題を用いて証明される.

7.2. 整列可能定理

定義 7.6 (整列集合)**.**
半順序集合 $(X, \leq)$ が**整列集合**であるとは, 任意の $A \subset X$ に対して, 最小元 $\min A$ が存在することである.

整列集合は, 直感的には $A \subset X$ が小さい順に並べられるということである. $a_1 = \min A$, $a_2 = \min(A \setminus \{a_1\})$, $a_3 = \min(A \setminus \{a_1, a_2\})$ などとすれば, $A = \{a_1, a_2, a_3, \ldots\}$ と小さい順に並べることができる.

命題 7.1.
$(X, \leq)$ が整列集合ならば, $(X, \leq)$ は全順序集合である.

証明.
任意の $x, y \in X$ に対して, $x \leq y$ か $y \leq x$ が成り立つことを示せばよい. そこで $A = \{x, y\} \subset X$ とおくと, $(X, \leq)$ は整列集合だったから, $\min A = \min\{x, y\}$ がある.
もし, $x = \min A$ ならば $y \in A$ に対して $x \leq y$ であり, 反対に $y = \min A$ ならば $x \in A$ に対して $y \leq x$ である. 従って, $x \leq y$ か $y \leq x$ のどちらかが成り立つから, $(X, \leq)$ は全順序集合である. □

命題 7.1 より, $(X, \leq)$ が整列集合であるならば, 全順序集合であり, 全順序集合ならば半順序集合である. つまり, 整列集合が一番条件の厳しい集合である.

例 7.7.
半順序集合 $(\mathbb{N}, \leq)$ は整列集合である. 任意の $A \subset \mathbb{N}$ に対して最小元が存在する.

例 7.8.
$(\mathbb{R}, \leq)$ や $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ は整列集合ではない. 例えば, $(-\infty, 0) \subset \mathbb{R}$ に最小元は存在しない.

$\mathbb{R}$ に通常の不等式 $\leq$ を考えると整列集合にはならないことがわかる. しかし, 別の半順序を考えることによって, 整列集合とできるか? という疑問がでてくる. これを保証するのが, 次の整列可能定理である.

定理 7.3 (整列可能定理)**.**
X を集合とする. このとき, ある X 上の半順序 $\leq$ が存在して, $(X, \leq)$ は整列集合とできる.

例えば, $\mathbb{C}$ には $\mathbb{R}$ の不等式による順序は定義できないが, 別の整列集合となる順序 $\leq$ があることを定理 7.3 は主張している. ただし, その半順序が役に立

つかは別の問題である. また, Banach-Tarski のパラドックスは整列可能定理を用いて証明される.

あとがき

参考文献についていくつかの説明を加える. このノートの多くは, 内田 [**4**] を参考にした. また, 第 2 章 2.4 節の指数関数, 三角関数の定義については黒田 [**7**] に従った. 複素数まで導入して, Taylor 展開を用いた初等関数の定義の仕方もあるが, それについては, 高木 [**9**] を参照されたい. 実際に, 数学科向けの微分積分の教科書においては, Taylor 展開を用いた初等関数の定義がよく用いられている.

第 3 章の論理学については, 中内 [**10**] を参考にした. 論理学は数学において必要不可欠なものだが, これらの内容を初学者向けにまとめた本は (筆者の知る限り) それほど多くはない. このノートを読んで, さらに勉強したい人はとくにお勧めできる本である.

第 5 章 5.5 節は Stewart [**17**] を参考にした. 筆者が学部時代の頃, 環論の演習問題として, $\mathbb{C}$ が $\mathbb{R}[X]/(X^2+1)$ と同型になることを証明したが, 当時はその問題の意図には気がついていなかった. 代数学を勉強することによって, もっとすっきりした $\mathbb{C}$ の構成を勉強して欲しい. 実数の構成 (完備化) については, Hainer-Wanner [**16**] を参照した. 実数とは何か？という問題は非常に難しいが, 数学科に入学したならば, 実数と有理数の違いについては (細部までの証明ができるかはともかく) ある程度説明できるようになって欲しい.

証明の書き方については, 飯高 [**1**] や一樂 [**3**] を参照して欲しい. 証明を書くためには, 「省略のまったくない証明」を真似して, 写経するくらいのことをして, 書き方をまねぶことも大切である. このノートも意図的なところ以外は省略をしないような証明の記述を心掛けたが, どこまで表現として正しいかは少々心配でもある.

このノートで足りないことについては, 内田 [**5, 4**], 森田 [**12**], 松坂 [**11**] を参照して欲しい. これらの参考図書のタイトルにもある通り「位相」は「集合」と切っても切り離せない概念である. そして, この位相を勉強するうえで, 論理学の知識が非常に重要になる. 位相の勉強でつまづいたときに, このノートが役に立つことがあれば幸いである.

索引

参考文献

[1] 飯高 茂, 微積分と集合 そのまま使える答えの書き方, 講談社, 1999.
[2] 石田 信, 代数学入門, 実教出版, 1978.
[3] 一樂 重雄, 集合と位相 そのまま使える答えの書き方, 講談社, 2001.
[4] 内田 伏一, 集合と位相, 裳華房, 1986.
[5] 内田 伏一, 位相入門, 裳華房, 1997.
[6] 吹田 信之, 新保 経彦理工系の微分積分, 学術図書, 1996.
[7] 黒田 成俊, 微分積分, 共立出版, 2002.
[8] 小林 昭七, 微分積分読本 1 変数, 裳華房, 2000.
[9] 高木 貞治, 定本 解析概論, 岩波書店, 2010.
[10] 中内 伸光, 数学の基礎体力をつけるためのろんりの練習帳, 共立出版, 2002.
[11] 松坂 和夫, 集合・位相入門, 岩波書店, 1968.
[12] 森田 茂之, 集合と位相空間, 朝倉書店, 2002.
[13] 雪江 明彦, 代数学 1　群論入門, 日本評論社, 2010.
[14] Lars Valerian Ahlfors, 笠原 乾吉 訳, 複素解析, 現代数学社, 1982.
[15] Edmund Landau, Foundations of analysis. The arithmetic of whole, rational, irrational and complex numbers, Chelsea Publishing Company, 1951.
[16] E. Hainar, G. Wanner, 蟹江幸博 訳, 解析教程 (下), 丸善, 2006.
[17] Ian Stewart, 芹沢 正三 (翻訳), 現代数学の考え方, 筑摩書房, 2012.