数学入門B –集合論–

1. 命題論理と述語論理

1.1. 命題論理.

定義 1.1 (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 1.1.
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) p:「$1+1=3$」は命題である.
(3) e:「新幹線は速い」は命題ではない.

定義 1.2 (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 1.2.
例 1.1 において, p の真理値は T, q の真理値は F である.

定義 1.3 (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 1.3.
例 1.1 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 1.4 (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 1.4.
命題 p とその否定 $\neq p$ に関する真理表は次の通り

p	$\neg p$
T	F
F	T

定義 1.5 (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 1.1.
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 1.5.
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 1.6 (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 1.1 (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 1.5 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 1.7 (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」と読む. $p \to q$ 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.

例 1.6.
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	$\neg p$	$p \to q$ $(\neg p \vee q)$	$\neg(p \to q)$
T	T	F	T	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	F

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.

定理 1.2.
命題 p, q に対して,

$$「p \Rightarrow q」 \Longleftrightarrow 「(p \to q) \vee (q \to p)」$$

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.

証明.
真理表を書いてみればよい. □

定義 1.8 (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.

定理 1.3.
命題 p, q に対して,

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

が成り立つ.

証明.
真理表を書いてみればよい. □

1.2. **述語論理.**

定義 1.9 (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.

例 1.7.
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) $X = \mathbb{N}$, $Y = (0, \infty)$, $n \in \mathbb{N}$, $\varepsilon \in Y$ に対して,

$$r(n, \varepsilon)\text{: } \frac{1}{n} < \varepsilon.$$

定義 1.10 (全称命題)**.**
命題関数 $p = p(x)$ $(x \in X)$ に対して, 「任意の $x \in X$ に対して, $p(x)$ である」を「$\forall x \in X \quad p(x)$」と書き, **全称命題**という.

例 1.8.
例 1.7 の $p(x)$, $q(x)$, $r(x)$ について, 全称命題を考えてみる.

- 例 1.7 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.[1]
- 例 1.7 の (2) で, 「$\forall x \in X \quad q(x)$」は偽である. 実際, $x = -3 \in X$ のとき, $q(-3)$: $-3 + 3 = 1$ だからである.
- 例 1.7 の (3) で, 「$\forall n \in X, \forall \varepsilon \in Y \quad r(x)$」は偽である. 実際, $n = 1 \in X, \varepsilon = 1 \in Y$ のとき, $r(1, 1)$: $\frac{1}{1} < 1$ だからである.

[1] もし, 男子大学生がいるのなら, 著者の勘違いです. すみません. ちなみに大学院生や研究員となると, 男子がいてもおかしくないので, わざわざ大学生と制約をつけています. 御茶ノ水女子大学付属中学などは共学だったと記憶しています.

定理 1.4.
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.

定義 1.11 (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 1.9.
例 1.7 の $p(x)$, $q(x)$, $r(x)$ について, 存在命題を考えてみる.

- 例 1.7 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 1.7 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 1.7 の (3) で,「$\exists n \in X, \exists \varepsilon \in Y \quad r(x)$」は真である. 実際, $n = 1 \in X, \varepsilon = 2 \in Y$ のとき, $r(1, 2)$: $\dfrac{1}{1} < 2$ だからである.

定理 1.5.
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.

注意 1.2.
定理 1.4 と定理 1.5 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 1.3.
「$\forall x \in X, \exists y \in Y \quad p(x, y)$」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.

定理 1.6 (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) $\neg(\forall x \in X \quad p(x)) \iff \exists x \in X \quad \neg p(x)$,
(2) $\neg(\exists x \in X \quad p(x)) \iff \forall x \in X \quad \neg p(x)$,

例 1.10 (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). 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

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

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.

2. 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. § 2.1 では, 集合の濃度の定義といくつかの具体例を説明する. § 2.2 では, 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. § 2.3 では, 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.

2.1. **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 2.1.
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 2.1 (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 2.1 (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 2.2.
命題 2.1 を示せ.

例 2.1.
$n \in \mathbb{N}$, $A = \{1, 2, 3, \ldots, n\}$, $B = \{1, 2, 3, \ldots, n, n+1\}$ 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.

例 2.1 に対して, 無限集合についての濃度はそれほど自明ではない.

例 2.2.
$A = \{2n : n \in \mathbb{N}\}$ とおくと, $\#A = \#\mathbb{N}$.

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 2.1 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. $\forall n, m \in \mathbb{N}$ 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. $\forall y \in A$ に対して, $\exists n \in \mathbb{N}$ が存在して $y = 2n$ とかける. よって $f(n) = 2n = y$ となる. □

問題 2.3.
$A := \{2n + 1 : n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}\}$ とおくとき, $\#A = \#\mathbb{N}$ を示せ.

例 2.3.
$\#\mathbb{N} = \#\mathbb{Z}$. つまり, $\mathbb{N}$ と $\mathbb{Z}$ は集合の元の個数が等しい.

証明の概略.
$f : \mathbb{N} \to \mathbb{Z}$ 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 2.4.
例 2.3 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 2.4.
$\#\mathbb{N} = \#(\mathbb{N} \times \mathbb{N})$. つまり, $\#\mathbb{N}$ と $\#(\mathbb{N} \times \mathbb{N})$ の元の個数は等しい.

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. □

問題 2.5 (難)**.**
例 2.4 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).

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 2.3, 例 2.4 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 4 倍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.

2.2. **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 2.3, 例 2.4 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 2.2 (可算集合)**.**
$\#N = \aleph_0$(アレフゼロ) 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 2.1.
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. この定理はとりあえず認めることにする.

例 2.5 (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.

定理 2.1 を用いた証明.
$\frac{p}{q} \in \mathbb{Q}$ 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 2.6.
$\mathbb{R}$ は可算集合ではない.

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}, ... 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, $\forall n \in \mathbb{N}$ 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 2.3.
$\mathbb{R} = \aleph$ 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 2.7.
$\#(-1,1) = \aleph$.

証明.
$f : \mathbb{R} \to (-1,1)$ を $x \in \mathbb{R}$ に対して

$$f(x) = \arctan\left(\frac{\pi}{2}x\right) = \int_0^{\frac{\pi}{2}x} \frac{1}{1+y^2}\,dy$$

で定めると, f は全単射になることが示される. 証明には, 微分積分の知識を用いる. □

例 2.8.
$\#(\mathbb{R}\times\mathbb{R}) = \#(\mathbb{R}^2) = \aleph$ 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 2.9.
$\#\mathbb{R} \neq \#2^{\mathbb{R}} = \#\{A : A \subset \mathbb{R}\}$. 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.

2.3. Bernstein の定理.

定義 2.4.
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.

命題 2.2.
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 $\#X \leq \#Z$.

定理 2.2 (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.

命題 2.2 と定理 2.2 より
1. $\#X \leq \#X$ $(X$:集合$)$
2. $\#X \leq \#Y$, $\#Y \leq \#X$ ならば $\#X = \#Y$ $(X, Y$:集合$)$
3. $\#X \leq \#Y$, $\#Y \leq \#Z$ ならば $\#X \leq \#Z$ $(X, Y, Z$:集合$)$

が成り立つ. この 3 条件が成り立つとき, $\leq$ を**順序関係**という. また, $\mathscr{U}$ を集合全体[2]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,

$$\#X \leq \#Y \text{ または } \#Y \leq \#X \tag{2.1}$$

のどちらかは必ず成立する. 半順序集合が (2.1) 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 2.10.
$\#\mathbb{Q} = \#\mathbb{N}$ であることを Bernstein の定理を使って示せる.

[2]Universe という. この部分はわざと曖昧に書いてある. なぜ $\mathscr{U}$ を設定しなければいけないかは, Russell のパラドックスを調べてみよ

3. 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.

3.1. 同値関係.

定義 3.1.
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 $x \sim y \Rightarrow y \sim x$.
(3) (推移律) 任意の $x, y, z \in X$ に対して $x \sim y, y \sim z \Rightarrow x \sim z$.

例 3.1.
$\mathbb{R}$ 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. 不等式は対称律をみたさない. 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 3.2.
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[3]$\sim$ は同値関係である.

例 3.3.
$p \in \mathbb{N}$ 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.

[3]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

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 3.1.

$p \in \mathbb{N}$ を素数とし, 簡単のために $x, y \in \mathbb{N}$ に対して, $k \in \mathbb{N}$ 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, $x = q_1 p + r_1$ かつ $0 \leq r_1 < p$ が成り立つ).

例 3.4.

$$\mathbb{R}[X] := \{a_0 + a_1 X + \cdots + a_n X^n : n \in \mathbb{N}_0,\ a_0, \ldots, a_n \in \mathbb{R}\}$$

と定める. つまり, $\mathbb{R}[X]$ は実数係数多項式全体である. $f, g \in \mathbb{R}[X]$ に対して

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

$$\Leftrightarrow x - y \text{ が } (X^2 + 1) \text{ でわり切れる}$$

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

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

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

問題 3.2.

例 3.4 について, 反射律と推移律を示せ.

3.2. **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

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

が定義できる. これを一般化してみよう.

定義 3.2 (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 3.1.
記号 $C(x)$ は参考書 (内田) 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 3.5.
$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 3$ に対して

$$C(1) = \{n \in \mathbb{Z} : 1 \equiv n \pmod 3\} = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} = \{3m + 1 : m \in \mathbb{Z}\}$$
$$C(2) = \{n \in \mathbb{Z} : 2 \equiv n \pmod 3\} = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\} = \{3m + 2 : m \in \mathbb{Z}\}$$
$$C(3) = \{n \in \mathbb{Z} : 3 \equiv n \pmod 3\} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = \{3m : m \in \mathbb{Z}\}$$

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に成り立つ. すなわち次の定理 3.1 が示せる.

定理 3.1.
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. そこで, 任意の $z \in C(x)$ に対して, 同値類の定義より $z \sim x$ 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 $z \sim x$ かつ $z \sim y$ 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 3.1 の意味については, 次節でより詳しく説明する.

問題 3.3.
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 3.6.
$\mathbb{R}[X]$ に対して, 例 3.4 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 $f \in \mathbb{R}[X]$ 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 (環論や単因子論, 割り算と約数の話を使う). 特に定理 3.1 から $f \in \mathbb{R}[X]$ の同値類 $C(f)$ の代表元として, 一次多項式 $aX + b \in \mathbb{R}[X]$ がとれて

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

とできる.

3.3. **商集合.** $\mathbb{Z}$ 上の同値関係 $\equiv \pmod 3$ について

$$\mathbb{Z} = C(0) \cup C(1) \cup C(2) \tag{3.1}$$

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, (3.1) 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, $\mathbb{Z}_3 := \{C(0), C(1), C(2)\}$ 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.

(3.1) 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 3.3 (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 3.4.
$\sim$ を $\equiv \pmod 3$ とする. このとき $\mathbb{Z}_3 = \mathbb{Z}/\sim$ を示せ. 特に, $\mathbb{Z}/\sim \subset \mathbb{Z}_3$ を示せ.

ここで, 定理 3.1 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 3.7.

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

$$\begin{aligned}\mathbb{Z}_5 &= \mathbb{Z}/_{\equiv \pmod 5} \\ &= \{C(n) : n \in \mathbb{Z}\} \\ &= \{C(0), C(1), C(2), C(3), C(4)\} \\ &= \{C(5), C(6), C(7), C(8), C(9)\} \\ &= \{C(0), C(1), C(2), C(3), C(4), C(5), C(6), C(7), C(8), C(9), C(10)\}\end{aligned}$$

となる. 最初と最後の表記は $C(0) = C(5) = C(10)$ なので, 同じ元がいくつもあることに注意せよ.

さて, $\phi : \mathbb{Z} \to \mathbb{Z}_5$ 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 $C(n) \in Z_5$ に対して, 代表元 $n \in \mathbb{Z}$ がとれるから, $\phi(n) = C(n)$ がわかる. この射影は $\mathbb{Z}_5$ を考えるうえで, もっとも自然に表れる写像と考えることができる.

定義 3.4 (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**自然な射影**(canonical projection) という.

例 3.8.

$\mathbb{R}[X]$ に対して, 例 3.4 の同値関係 $\sim$ を考える. このとき

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

となる. 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 $\mathbb{R}[X]/(X^2 + 1)$ への自然な射影 ϕ は $f \in \mathbb{R}[X]$ に対して

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

となる.

3.4. **同値類による計算と well-defined.** $\mathbb{Z}_3 = \{C(0), C(1), C(2)\}$ 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が問題になる.

そこで問題を整理しよう.

> **問題** $a \equiv a' \pmod 3$ と $b \equiv b' \pmod 3$, すなわち $C(a) = C(a')$ と $C(b) = C(b')$ 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?

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, $C(a+a') = C(b+b')$ が成り立つ. □

このことから, $C(a), C(b) \in \mathbb{Z}_3$ に対して

$$C(a) + C(b) := C(a+b) \tag{3.2}$$

と定義することができる. このとき (3.2) 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, (3.2) の定義は **well-defined** であるという[4].

[4] well-defined のいい和訳はなさそうである

例 3.9.
$C(a), C(b) \in \mathbb{Z}_5$ 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, $a \equiv a' \pmod 5$, $b \equiv b' \pmod 5$ ならば $ab \equiv a'b' \pmod 5$ となる.

証明.
$a \equiv a'$, $b \equiv b' \pmod 5$ 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,

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

となるから,

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

となる. $a'm + b'n + 5mn \in \mathbb{Z}$ より, $ab = a'b'$ がわかる. □

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

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

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.

問題 3.5.
$C(a), C(b) \in \mathbb{Z}_4$ 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 $C(a), C(b) \in \mathbb{Z}_4$ をみつけてみよ.

3.5. $\mathbb{C}$ や $\mathbb{R}$ の構成.

[5]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 3 年生の代数学

3.5.1. 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]

答えからいうと, $\mathbb{R}[X]/(X^2+1)$ が $\mathbb{C}$ と同じ構造をもっている. さらに, $\mathbb{R}[X]/(X^2+1)$ は $\mathbb{R}$ だけで作ることができるから, $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$ と定義してしまうことにより, $\mathbb{R}$ から $\mathbb{C}$ が作れたことになる.

3.5.2. 実数体 $\mathbb{R}$ の構成. この節は,

E. Hainar, G. Wanner, 蟹江幸博 訳「解析教程 (下)」, 丸善, 2006

の §III.1.2 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.[7]

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

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n, m \in \mathbb{N} \quad n, m \geq N \Longrightarrow |a_n - a_m| < \varepsilon$$

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

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N} \quad n \geq N \Longrightarrow |a_n - a| < \varepsilon$$

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,

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142, \ldots \to \sqrt{2} \notin \mathbb{Q}$$

である. つまり, 有理数の数列の極限を考えると, 有理数にならないことがある. 上の数列は Cauchy 列になっているが, $\mathbb{Q}$ 上で収束しない.

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,

[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] 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.

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, インターネットなどで調べて欲しい (マンガでだと, 加藤元浩「Q.E.D. 証明終了」の 15 巻とか. たしか 4 ページくらいでざっくりとした説明があったはず)

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, "Foundations of Analysis," 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 $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$ が全ての $n \in \mathbb{N}$ について, $a_n \leq b_n$ ならば $\lim_{n\to\infty} a_n \leq \lim_{n\to\infty} b_n$ となることに注意しよう.

定義 3.5 (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, $C(\{a_n\}_{n=1}^{\infty}) \leq C(\{b_n\}_{n=1}^{\infty})$ であるとは, ある $N \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して,

$$n \geq N \Rightarrow a_n \leq b_n$$

が成り立つときをいう. また, $C(\{a_n\}_{n=1}^{\infty}) \leq C(\{b_n\}_{n=1}^{\infty})$ かつ $C(\{a_n\}_{n=1}^{\infty}) \neq C(\{b_n\}_{n=1}^{\infty})$ であるとき, $C(\{a_n\}_{n=1}^{\infty}) < C(\{b_n\}_{n=1}^{\infty})$ と書く.

注意 3.2.
実は不等式の定義をこれで定めると, 少し困ることがある. この定義を使うと, すべての $a, b \in \mathbb{R}$ に対して, $a \leq b$ か $b \leq a$ のどちらかが成り立つことを示すのが難しくなってしまう. $C(\{a_n\}_{n=1}^{\infty}) < C(\{b_n\}_{n=1}^{\infty})$ を先に定義しておいてから $\leq$ を定義する方が論理的に構成しやすい. 詳しくは「解析教程 (下)」を見よ.

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 3.6.
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.

定理 3.2.
$\mathbb{R} := \mathbb{Q}/\sim$ 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, $a_n = C(\{b_{in}\}_{i=1}^{\infty})$ となる $\{b_{in}\}_{i=1}^{\infty} \in X$ 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, $|a_n - a_{n+k}| = C(\{|b_{in} - b_{i,n+k}|\}_{i=1}^{\infty})$ だったことから, すべての $i \in \mathbb{N}$ に対して $|b_{i,N_j} - b_{N_1+i,N_j+k}| \leq \frac{1}{2j}$ とできる.[8] そこで, 対角線論法を使って, $c_j := b_{jN_j}$ とおいてみる. 目標は, $a := C(\{v_j\}_{j=1}^{\infty})$ 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. $|a_j - c_j| = C(\{|b_{jn} - c_j|\}_{n=1}^{\infty})$ より $n \geq N_j$ ならば

$$|b_{jn} - c_j| = |b_{jn} - b_{jN_j}| \leq \frac{1}{j}$$

とできる. よって, $|a_j - c_j| \leq \frac{1}{j}$ がわかる.

[8] 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.

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, $\dfrac{1}{N_0} < \varepsilon$ をみたす $N_0 \in \mathbb{N}$ をとると, $j \geq \max\{N_0, N_{N_0}\}$ ならば

$$
\begin{aligned}
|c_j - c_{j+k}| &= |c_j - a_j + a_j - a_{j+k} + a_{j+k} - c_{j+k}| \\
&\leq |c_j - a_j| + |a_j - a_{j+k}| + |a_{j+k} - c_{j+k}| \\
&\leq \frac{1}{j} + \frac{1}{N_0} + \frac{1}{j+k} \\
&\leq \frac{1}{N_0} + \frac{1}{N_0} + \frac{1}{N_0} \leq 3\varepsilon
\end{aligned} \tag{3.3}
$$

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, (3.3) に注意すると, $j \geq \max\{N_0, N_{N_0}\}$ 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

$$
|a_n - a| \leq |a_n - c_n| + |c_n - a| \leq \frac{1}{n} + 3\varepsilon \leq 4\varepsilon
$$

となるので, $a_n \to a$ $(n \to \infty)$ がわかる. □

4. 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

$$\prod_{\lambda\in\Lambda} A_\lambda := \left\{ f:\lambda\to\bigcup_{\lambda\in\Lambda} A_\lambda,\ \forall\lambda\in\Lambda\text{に対して } f(\lambda)\in A_\lambda \right\}$$

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「$\forall\lambda\in\Lambda$ 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 4.1.
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 4.1 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.

4.1. Zorn の補題.

4.1.1. 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 4.1 (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 $x\leq y$, $y\leq x\Rightarrow x=y$.
(3) (推移律) 任意の $x,y,z\in X$ に対して $x\leq y, y\leq z\Rightarrow x\leq z$.

例 4.1.
$\leq$ 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 4.2.
$\mathscr{U}$ 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 $=$ そのものである.

例 4.3.
$\leq$ 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.

定義 4.2 (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 4.4.
$(\mathbb{R}, \leq)$ 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 4.5.
$\mathscr{U}$ 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.

定義 4.3 (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, $\forall a \in A$ 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, $\forall a \in A$ 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 $\{x \in X : x \text{ は } Al \text{ の上界 }\}$ に最小元が存在して

  $$y = \min\{x \in X : x \text{ は } Al \text{ の上界 }\}$$

  となることをいう.
- $y \in X$ が A の**下限**であるとは, 集合 $\{x \in X : x \text{ は } Al \text{ の下界 }\}$ に最大元が存在して

  $$y = \max\{x \in X : x \text{ は } Al \text{ の下界 }\}$$

  となることをいう.

例 4.6.
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.

$$\{x \in \mathbb{R} : x \text{ は } [0,1) \text{ の上界 }\} = \{x \in \mathbb{R} : \forall y \in [0,1),\ y \leq x\} = [1, \infty),$$
$$\{x \in \mathbb{R} : x \text{ は } [0,1) \text{ の下界 }\} = \{x \in \mathbb{R} : \forall y \in [0,1),\ x \leq y\} = (-\infty, 0]$$

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.

定義 4.4 (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.

直感的には, どんな全順序部分集合の元よりも大きな元があるということである. 帰納という言葉は数学的帰納法がなじみが深いが, その証明方法は, どんな自然数 n よりも**一つだけ大きな**自然数 $n+1$ があることが重要なことであった (だから, $\mathbb{R}$ では帰納法は使えなかった. 一つだけ大きいという意味がないからである). 帰納的という意味も同じで, 全順序集合の上界が, 一つだけ大きいということに対応している.

定義 4.5 (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).

定理 4.2 (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 4.1.
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. 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.

4.2. 整列可能定理.

定義 4.6 (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 4.1.
$(X, \leq)$ 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 4.1 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 4.7.
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 4.8.
$(\mathbb{R}, \leq)$ 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 4.3 (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 4.3 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.