数学科に入ったら読む本

福井 敏純

2025 年 1 月 9 日

目次

はじめに

友達どうしお互い足を引っ張らずに手を引っ張ろう.
互いに手を引っ張りあえば前に進むではないか!

0.1　数学とは

数学とはどんな学問でしょうか? 数学は諸学問のバックボーンであり，数学的知識を抜きに現代の科学を語ることはできません.

数学は実は単純な学問で，急所さえ徹底的にわからせることができたら，どんな人にもわかるようにできています．残念ながら，日本では数学が嫌いな人が一定数いて，その人達にとっては学校を終えたら一刻も早く忘れてしまいたいものの一つになってしまいました．また学習指導要領がしばらく前に変えられ，体系的な数学の知識が寸断され，知識の断片のみ学ぶ様になっていることも，数学がわからないという学生を増やしていると思います.

数学とは，公式を覚えてそれを当てはめて問題を解くことではありません．確かに公式も数学の一部分ではありますが，その公式のでてきた背景，なぜその公式が成り立つかと言う理由，その公式の持つ意味，などを理解すること事が大切なので，公式を適用して問題を解くと言うのは数学のごく一部でしかありません.

君達は数学の時間では問題の解き方ばかり習って来たと思っているかもしれません．また数学の問題と言うのは考えれば解けるのだと思っているかもしれません．しかし，世の中にはどうやって解いたらよいかわからない問題の方が多いのです．もちろん数学の世界でも,

解き方のわからない問題はたくさんあります.

今までは解き方のわかっている問題ばかりを教わって来たから，数学というのは問題の解き方を教わる学問だと思っているかもしれませんが実は全然違います.

現在解き方のわかっていない未解決の問題に遭遇したとき，数学はその真価を発揮します．問題を論理的に整理して，解決に有効なアイデアをだし，そのアイデアが実際に有効

であることを実地に適用して示す，数学はそれを可能にします．数学の学習にはこういった能力が求められるわけで，これは試行錯誤の連続です．数学的に考えること，論理的に考えることとはどういうことかを，身を持って体験しなければなりません．また数学のアイデアにどういうものがあるのかを，理解しなければなりません．問題を定式化し直すような能力も必要になります．数学科とはそのようなことのできる人材を育てる所です．ですから数学を学習するときは，あせらず，自分に納得のゆくまで，とことん考えることが重要です．

自分を誤魔化し始めると，すぐにいろんなことわからなくなります．

数学科で学ぶ知識は，10 年やそこらで古びるような性質のものではありません．100 年後や 200 年後に，立派に真理として通用する知識です．問題を数学的に定式化し，必要となる数学的なアイデアをだし，問題にアプローチしていく，こういう事ができるようになればあなたの一生の財産になります．大学の 4 年間，あせらず，じっくりと数学に取り組んで欲しいと思います．

0.2　数学をわかるようになるには?

ではどのようにすれば数学が分かるようになるのでしょうか? この問いに答えるのは，たやすいことではありません．こうすれば必ず数学ができるようになるという，万人向けの処方箋もないように思います．ですから，以下に述べるのは一般的なことです．

大学での数学の基礎となるのは，

「微分積分学」と「線形代数学」

です．この 2 つがしっかりわからなければ，おそらく高学年に開講される科目は何も分からないでしょうから，まずはこの 2 つをしっかり習得することが大切です．逆に「微分積分学」と「線形代数学」がわかれば，高学年の科目を理解するのはそれほど難しいことではないと言えるでしょう．

この小冊子は，数学科１年生向けの授業が基になっています．１年生のうちに

１章，２章の１節から４節まで，および 3 章

の内容がわかると進んだ数学を学ぶ基礎ができると思います．この小冊子の他の部分はいろいろなトピックですが勉強が進むにつれて講義等で触れられる事も多いでしょう．本書程度の事は当たり前と省略しながら説明してしまう先生もいるかも知れません．必要に応じて補足的に読んだり，興味に応じて読んでいただければと思っています．

数学の学習の際には自分の頭で考えて，しっかり納得することが一番大切です．しかし

よく考えたけどわからなかったということもあると思います．このことはけっして悪い事ではありません．そのときは友達に聞いてみるなり，先生に質問してみたら良いと思います．そのとき大切なのは間違いを恐れないということです．友達どうしで質問し合い説明し合うのはとてもよい事です．間違えたってよいのです．間違えたらそばにいる先生が直してくれます．大切なのは，前に進もうと努力することです．数学が分かりたいと言う気持があれば自然にいろいろなことが分かって来ます．それから

自分を誤魔化さない

という姿勢です．意識を集中させて話を聞く訓練，工夫してノートをとる練習なども心がけてください．

入門書を読むというのもよいと思います．また「数学セミナー」（日本評論社），「数理科学」（サイエンス社），「現代数学」（現代数学社），「数学」（日本数学会）などの雑誌を見ても数学のいろいろな世界が覗けるはずです．

数学科での 4 年間で有意義に過ごし，しっかり数学を修得して欲しいと思います．

この小冊子が, 皆さんの数学の理解の助けになることを祈っています．

0.3　黒板について

数学科にはセミナー室があり，黒板やホワイトボードが備え付けられています．学年が上がるにつれ利用する機会も増えてくると思いますので，「全国黒板工業連盟」による黒板・ホワイトボードに関する取扱説明を参考に述べておきます．

黒板

1. 常に黒板消しと粉受部に付いたチョークの粉を取り除き，清潔に保って下さい．
2. 黒板面全体をきれいな黒板消しで拭いてチョークの粉を落として下さい．
3. 固く絞ったきれいな濡れ布で黒板面を水拭きして下さい．
4. 乾いたきれいで柔らかな布で黒板面の水分を拭き取って下さい．水拭きの際，洗剤（酸性・アルカリ性・中性を問わず）を使用しないで下さい．

ホワイトボード

1. ボード面は“ホーロー”です．定期的に“水ぶき”をして下さい．特に，光沢度の低い製品はマーカーが消しにくくなりますが，水ぶきで解消します．但し，水拭きの際に“洗剤”(酸性・アルカリ性・中性を問わず) は使用しないで下さい．
2. 常にイレーザーや粉受部に付いたマーカーの粉を取り除き，清潔に保って下さい．
3. かすれたマーカーは，消えにくくなりますので，早めに新品と交換して下さい．

4. イレーザーは水洗いできますが，マーカー粉の付着が著しい物は早めに新品と交換して下さい．

0.4　敬称について

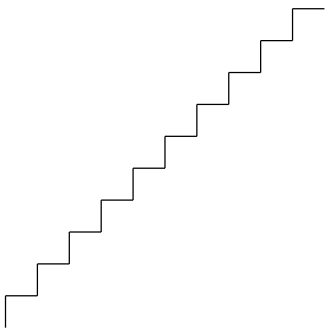
大学の教員には教授，准教授，講師，助教といった職名がついています．なかには，非常勤講師の方もいます．大学の教員に対して「○○教授」と呼びかける学生さんが時々いますが，私は違和感を感じます．その先生が教授であれば間違いではありませんが，もし敬意を表しているつもりでそのような言い方をしているのだとしたら，相手にそのように取られない可能性はかなりあります．教授というのは職名であり，敬称ではないからです．准教授や講師，助教の先生に教授と呼びかけたら明らかに間違いですし，また退職した先生が非常勤講師として教えている事もあるので，その様な先生に「○○教授」と呼びかけたら間違いになります．「○○講師」と呼べば間違いではありませんが，敬意を表しているとは理解されないでしょう．

公式の場で紹介する場面では「○○教授」「○○准教授」と紹介する事もあるでしょうが，これはその職に従事する者として紹介しているので，必ずしも敬意を表した表現ではありません．小学校，中学校，高等学校の正教員の職名は教諭ですので，「○○教諭」と紹介する場面はあるでしょうが，教わる立場の者が「○○教諭」と呼びかけることは多分ないでしょう．ものを教わる相手につける一般的な敬称は「先生」ですので，大学の教員に学生として呼びかけるときも「○○先生」を使うのが無難です[*1]．

[*1] ただし，慶應義塾では，先生というのは創立者たる福澤諭吉先生ひとりに限り，他の教職員はすべて「君（くん）」づけで呼ぶならわしだそうです．もともと「君（くん）」は尊称で，休講掲示なども「○○君休講」という形ででるそうです．

第 1 章

論理



理詰めに議論して人を納得させる「説得術」から数学における証明は生まれたと言われている．しかし「論理に強い」ということは必ずしも「議論に強い」ことを意味しない．論理に強い人でも他人と議論はからきしできない人もいるし，また日常生活では，論理は無茶苦茶でも強弁できる人の方が強く，そのような人の意見が通ってしまうことがしばしばあるからである．論理を学んでも，議論に強くはならないかもしれないが，論理を学ぶことにより，学問の基礎を学習者に強く納得させる効果はあるものと思われる．

ここでは古典的な論理学の基本的な事柄を学習していく．

日本語	英語 (筆記体)	フランス語	ドイツ語	ロシア語
論理	logic (*logic*)	logique	Logik	логика

[*1]

[*1] 参考のため，キーワードの英仏独露語を載せておく．いずれも数学の研究が盛んな国の言葉である．

1.1 命題論理

真または偽である事が決定できる文 (又は文章) を**命題** (proposition) という．たとえば次のようなものは真か偽か判定できるので命題である．

(i) 3 は奇数である．
(ii) $2^{2^5}+1$ は素数である．
(iii) 366 は 5 の倍数である．

しかし次のようなものは命題とは言わない．しばしば真偽を判断する人の主観が入るからである．

(i) この問題は簡単である．
(ii) 永六輔は背が高い．
(iii) 山田花子は美人である．

命題をあつかう論理を命題論理 (propositional logic) という．

命題間の基本的な結合として次の 4 つのものが考えられる．

$\wedge$	かつ (and)	論理積 (conjunction)
$\vee$	または (or)	論理和 (disjunction)
$\neg$	$\cdots$でない (not $\ldots$)	否定 (negation)
$\rightarrow$	ならば (imply)	含意 (implication)

2 つの命題 p, q に対し，「p かつ q」という命題を考え，それを記号 $p \wedge q$ であらわす．「p かつ q」は p, q ともに真のとき真と約束し，それ以外のときは偽と約束する．

また 「p または q」という命題を考え，それを記号 $p \vee q$ であらわす．「p または q」は p, q のうち少なくとも一つが真のとき真と約束し，それ以外のときは偽と約束する．

これを次のように表にまとめて書く．ここで T は 真 (truth), F は 偽 (false) をあらわす．

p	q	$p \wedge q$	$p \vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

このような表を**真理表** (the truth table) とよぶ． また「p が真 (T) で q が真 (T) のと

き，$p \wedge q$ の**真理値**は真 (T) である」,「p が真 (T) で q が偽 (F) のとき，$p \wedge q$ の**真理値**は偽 (F) である」という様にいう．なお T, F の代りに 1, 0 を使う流儀もある．コンピュータにおける論理演算では多くの場合 1, 0 を用いている．

不等号 $\leq$ を次のように約束する．

$$a \leq b \Longleftrightarrow a < b \text{ または } a = b$$

よって 「$1 \leq 2$」は真の命題である．なお $a \leq b$ の代りに $a \leqq b$ を使うこと[*2]もある．

命題 「p の否定」を記号 $\neg p$ であらわす．その真理表は次のようである．

p	$\neg p$
T	F
F	T

「p の否定」を $\neg p$ でなく $\overline{p}$, $\sim p$, p' などと書く流儀もある．

演習 1.1.1. p, q, r を命題とするとき次の命題の真理表を作れ.

(i) $(p \wedge q) \wedge r$
(ii) $(p \wedge q) \vee r$
(iii) $(p \vee r) \wedge (q \vee r)$

ここでの p, q, r は命題であるが p, q, r に任意の命題が代入できる．つまり p, q, r を変数のように考えている訳である．このようにみたとき p, q, r を**命題変数** (propositional variable) という．

2 つの命題 p, q に対し，「p ならば q」という命題を考え，それを記号 $p \to q$ であらわす．命題「p ならば q」 の真理表は次のようになる．

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

これは次のように考える．「p ならば q」が真ということは「『p であってかつ q でない』ことはない」ということだと考えて $p \to q$ は $\neg(p \wedge (\neg q))$ のことと考えその真理値を対応させるのである．

[*2] 文部省がこの記号を指定したという歴史的経緯があり，日本の初等中等教育の教科書ではよく使われている．

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

命題 $p \to q$ に対して $q \to p$ をその命題の**逆** (converse), $(\neg p) \to (\neg q)$ を**裏** (converse of contrapositive), $(\neg q) \to (\neg p)$ を**対偶** (contraposition) という.

演習 1.1.2. $p \to q$ の逆，裏，対偶の真理表を作れ.

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

それに含まれる命題変数が真か偽かに関わりなく常に真理値が T(真) となるような命題を**恒真命題** (tautology) とよぶ

例 1.1.3. $p \vee \neg p$ は恒真命題である.

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

$p \vee \neg p$ を**排中律** (law of excluded middle) とよぶことがある.

$p \wedge \neg p$ を**矛盾律** (contradiction) とよぶことがある．これは常に偽である命題である.

演習 1.1.4. $p \to p$ は恒真命題であることを示せ.

例 1.1.5. $(p \wedge (p \to q)) \to q$ は恒真命題である.

p	q	$p \to q$	$p \wedge (p \to q)$	$(p \wedge (p \to q)) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

演習 1.1.6. $((p \to q) \wedge (q \to r)) \to (p \to r)$ は恒真命題であることを示せ．この命題は

三段論法と呼ばれる．

命題変数 p, q, r, ... を $\wedge$, $\vee$, $\to$, $\neg$ によって有限回結合して得られるものを**論理式** (formula) という．たとえば次の様なものが論理式の例である．

$$p \wedge q, \quad p \vee (p \to \neg q), \quad (p \wedge \neg q) \wedge (q \to \neg p)$$

A, B を p, q, r, ... を命題変数とするような論理式とする．命題「$A \to B$」が恒真命題であるとき，A から B は**推論**されるまたは**演繹**されるといい，記号「$A \Longrightarrow B$」であらわす．これは 「A を真 (T) とするような命題変数 $p, q, r, \ldots$ の真理値に対しては常に B が真 (T) となること」だといいかえられる．

命題 「$(A \to B) \wedge (B \to A)$」 を 「$A \leftrightarrow B$」と略記する．$A \leftrightarrow B$ が恒真命題であるとき 2 つの命題 A, B は**同値**であるといい「$A \iff B$」と書く．これは A と B の真理値が一致する事だと言ってもよい．

演習 1.1.7. $(p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$ は恒真命題であることを示せ．上の約束に従えば，このことを次のように書ける．

$$(p \to (q \to r)) \iff ((p \wedge q) \to r)$$

演習 1.1.8. 次を示せ．これらは分配の法則と呼ばれる．

$$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r),$$
$$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r).$$

演習 1.1.9. 次を示せ．これらは de Morgan[*3] の法則 と呼ばれる．

$$\neg(p \wedge q) \iff (\neg p) \vee (\neg q),$$
$$\neg(p \vee q) \iff (\neg p) \wedge (\neg q).$$

[*3] Augustus de Morgan, 1806 – 1871, は、インド生まれのイギリスの数学者

1.2 述語論理

「x は 3 の倍数である」「y は素数である」のように数学では変数を含む文を考えることが多い．これらは 変数 x, y に具体的な値を代入したら真偽がきまる文である．このような文を**命題関数** (propostional function) または**述語** (predicate) という．「x と y は互いに素である」や「$x^2 + y^2 + z^2 = 1$ 」などのように 2 変数や 3 変数の命題関数を考える事も多い．一般に n 個の変数を含む命題関数を n 変数の**述語** (predicate) という．述語を扱う論理を述語論理 (predicate logic) という．

命題関数または述語を考えるときには表れた変数のとりうる範囲を決めておかなければならない．変数のとりうる範囲を U であらわし**全体集合** (whole set, universe set) または**宇宙** (universe) とよぶ．考えられる U の典型的な例は自然数全体や実数全体などである．U が何であるか本来はいちいち明示すべきであるが, 文脈から明らかなときは略すことにする．たとえば「x は 3 の倍数である」「y は素数である」のような述語を考える場合は，宇宙 U は自然数全体または整数全体である．

述語 (命題関数) に対しても前節と同様に 論理積 $\wedge$, 論理和 $\vee$, 否定 $\neg$, 含意 $\to$ を考えることができる．

変数 x を含む述語 $P(x)$ に対し命題 $\forall x\ P(x)$ と $\exists x\ P(x)$ を次で定める．

$$\forall x\ P(x) : \text{すべての } x \text{ について } P(x) \text{ が真である．}$$
$$\exists x\ P(x) : P(x) \text{ が真なる } x \text{ が存在する．}$$

$\forall$ を**全称記号** (universal quantifier)，$\exists$ を**存在記号** (existental quantifier) といい 両方をあわせて**限定記号** (quantifier) という．それぞれ英語の Any (すべての，任意の) の A, Exist (存在する) の E とをひっくりかえしたものである．

例 1.2.1.「$(x+1)^2 = x^2 + 2x + 1$ は恒等式である．」というのは「$\forall x\ ((x+1)^2 = x^2 + 2x + 1)$」が真の命題であるということである．「方程式 $x^2 = 2$ には解がある」というのは「$\exists x\ (x^2 = 2)$」が真の命題ということである．

注意 1.2.2 (唯一つ存在). 条件 $P(x)$ をみたす x が唯一つだけ存在するとき，次のように書くことがある．

$$\exists| x\ P(x) \quad \text{または} \quad \exists 1\ x\ P(x) \quad \text{または} \quad \exists!\ x\ P(x).$$

このとき「$P(x)$ をみたす x が**一意的に**存在する」という．

例 1.2.3 (4 の倍数は 2 の倍数である).「4 の倍数は 2 の倍数である」という命題を考えてみよう．これは、分解すると「x は 4 の倍数 ならば x は 2 の倍数である」ということ

だから、

$$P(x) : x \text{ は } 4 \text{ の倍数} \qquad\qquad Q(x) : x \text{ は } 2 \text{ の倍数}$$

とおいて述語 (命題関数) 「$P(x) \to Q(x)$」 を考えるということである.

x	$P(x)$	$Q(x)$	$P(x) \to Q(x)$
1	F	F	T
2	F	T	T
3	F	F	T
4	T	T	T
5	F	F	T
6	F	T	T
$\vdots$	$\vdots$	$\vdots$	$\vdots$

なのですべての自然数 x に対し 「$P(x) \to Q(x)$」 は真であることがわかる. よって「$\forall x(P(x) \to Q(x))$」 は真の命題.

演習 1.2.4.「2 の倍数は 4 の倍数である」という命題を同様に解析せよ.

限定記号のついた命題を否定すると次のようになる.

$$\begin{aligned} \neg(\forall x P(x)) &\iff \exists x\ (\neg P(x)) \\ \neg(\exists x P(x)) &\iff \forall x\ (\neg P(x)) \end{aligned}$$

これらは一般化した de Morgan の法則とよばれることがある.

一般化した de Morgan の法則をもちいて次を示すことができる.

$$\begin{aligned} \neg(\forall x(P(x) \to Q(x)) &\iff \exists x\ (P(x) \wedge \neg Q(x)) \\ \neg(\exists x(P(x) \wedge Q(x)) &\iff \forall x\ (P(x) \to \neg Q(x)) \end{aligned}$$

演習 1.2.5. 次の述語の否定を作れ.

(i) $x_1 = x_2 = \cdots = x_n = 0$.
(ii) すべての $i = 1, \ldots, n$ に対し $x_i = 0$.
(iii) $\forall \lambda\ x_\lambda = 0$.

演習 1.2.6. 次の述語の否定を作れ.

(i) $x_1 = 0$ または $x_2 = 0$ または $\ldots$ または $x_n = 0$.
(ii) ある i $(1 \leq i \leq n)$ に対し $x_i = 0$.
(iii) $\exists \lambda\ x_\lambda = 0$.

例 1.2.7.「勉強しないならば叱られる」の対偶をつくってみよう．これを形式的に「叱られないならば勉強する」としてよいだろうか?

$$P(x) : x \text{ は勉強してない} \qquad\qquad Q(x) : x \text{ は叱られている}$$

として $P(x) \to Q(x)$ の対偶をつくると「x は叱られていない ならば x は勉強している」となる．これを日常語に直すと「叱られていないのは勉強しているからだ」となる．

$P(x, y)$ を 2 つの変数 x, y をもつ述語 (命題関数) とする．このとき $\forall y P(x, y)$ や $\exists y P(x, y)$ は x を変数とする命題関数となる．このとき，限定記号 $\forall$ や $\exists$ のついている変数 y を**束縛変数** (bounded variables), なにも限定記号のついてない変数 x を**自由変数** (free variables) という．

$P(x, y)$ を 2 つの変数 x, y をもつ述語 (命題関数) とする．このとき次が成立する．

$$\begin{array}{lcl} \forall x\ \forall y\ P(x, y) & \iff & \forall y\ \forall x\ P(x, y) \\ \exists x\ \exists y\ P(x, y) & \iff & \exists y\ \exists x\ P(x, y) \end{array}$$

したがって最初の条件を 「$\forall x, y\ P(x, y)$」2 番目の条件を「$\exists x, y\ P(x, y)$」 と略記しても混乱は生じない．しかし $\forall$ と $\exists$ が混在するときは，不用意に順番を入れ替えてはいけない．

$\forall x\ \exists y\ (x = y)$	真
$\exists y\ \forall x\ (x = y)$	真でない

$\forall x(P(x) \iff Q(x))$ のとき，単に次の様に書く．

$$P(x) \iff Q(x)$$

演習 1.2.8. 次を示せ．

(i) $(\exists y\ P(x, y)) \wedge Q(x) \iff \exists y\ (P(x, y) \wedge Q(x))$
(ii) $(\exists y\ P(x, y)) \vee Q(x) \iff \exists y\ (P(x, y) \vee Q(x))$
(iii) $(\forall y\ P(x, y)) \wedge Q(x) \iff \forall y\ (P(x, y) \wedge Q(x))$
(iv) $(\forall y\ P(x, y)) \vee Q(x) \iff \forall y\ (P(x, y) \vee Q(x))$

公理、定義、定理. ユークリッドの昔ならいざ知らず，いまどき「公理とは自明の真理である」という考え方をしている人はいないと思う．数学で**公理** (axiom) といえば，各理論体系の出発点として証明をしないで，仮定した事柄である．公理という言葉はユークリッドの「幾何学原本」のなかに現れる「公準」がもとであり，幾何学を組み立てる基礎のようなものであった．そして，誰もが正しいことと認められるべきものと考えられていたのだろう．しかし非ユークリッド幾何の出現によって，公理が自明の真理であるという考え方はなくなった．そして一つの理論において成り立つと仮定または要請されること，と理解されるようになった．その代りに 1 つの理論の基礎になる公理系に対して要請されることは, その公理系から矛盾が出ないこと，すなわちその公理系が無矛盾であることとなった．公理系が無矛盾であるというのは，その公理系からどんな命題 A に対しても A と A の否定が同時に証明されることがないことである．

定義 (definition) とは言葉の意味を規定することである．数学の理論で用いる概念は，その意味を明確にしておかなければならない．したがって，その概念はそれより以前に与えられた概念を用いて論理的に規定されなければならない．その規定のための式とか文章のことを定義というわけである．しかし, それより以前に与えられた概念，それより以前に与えられた概念と, たどっていけば，定義されないで使われる概念に到達する．これらを無定義概念という．たとえばユークリッド幾何学における「点」は無定義概念である．

数学の証明の結果，正しいことがわかった命題を**定理** (theorem) という．通常はその理論の中で重要な位置をしめるものを定理というようである．定理から直ちにわかる正しい命題を，その定理の**系** (corollary) という．**補題** (lemma) というと同じように正しい命題を指すが，別の重要な定理を示すために準備されたものだったり，その理論の構成の鍵になるようなものを指すことが多い．数学的に証明された正しい命題を単に**命題** (proposition) ということもある．定理ほど重要ではないが，意味のあることを主張しているというときに，使う．何を定理と呼び何を補題や命題と呼ぶか，この使い分けは，人によって微妙に違い, これが正しい使い方であると言い切るのは難しいようである．

1.3 解析学から

以後，全体集合 U (考えている変数の動く範囲) は，実数全体または有理数全体とする．このとき

$$\text{「}\forall x\ \big((x>0)\to P(x)\big)\text{」を「}\forall x>0\ P(x)\text{」},$$
$$\text{「}\exists x\ \big((x>0)\wedge P(x)\big)\text{」を「}\exists x>0\ P(x)\text{」}$$

と書くことがある．さらに M を定数とするとき

$$\text{「}\forall x\ \big((x<M)\to P(x)\big)\text{」を「}\forall x<M\ P(x)\text{」},$$
$$\text{「}\exists x\ \big((x<M)\wedge P(x)\big)\text{」を「}\exists x<M\ P(x)\text{」}$$

等と書くこともある．

演習 1.3.1. 次を示せ．

(i)「$\forall x>0\ P(x)$」 の否定は 「$\exists x>0\ \neg P(x)$」.
(ii)「$\exists x>0\ Q(x)$」 の否定は 「$\forall x>0\ \neg Q(x)$」.

命題 1.3.2. $\forall\varepsilon>0\ a<b+\varepsilon \iff a\le b.$

証明. $\forall\varepsilon>0\ a<b+\varepsilon$ は

$$\forall\varepsilon\ (\varepsilon>0 \text{ ならば } a<b+\varepsilon)$$

ということであった．よって $\Longleftarrow$ は明らか $\Longrightarrow$ を示す．$a>b$ とすると $a>b+\varepsilon$ をみたす正の数 ε が存在する．これは左の条件文の否定である． □

□は証明の終わりを表す記号で墓石記号と呼ばれる．最初にこの記号を証明終の意味に用いた数学者に因んでハルモス記号と呼ばれることもある．なお□の代わりに ■ を同じ意味で使う事もある．ラテン語の Quod Erat Demonstrandum (これが示したいことであった) を略して Q.E.D. と書くこと[*4]もあるが，最近は Q.E.D. を使うことは減ってきた．

演習 1.3.3. 上の証明にならって次を示せ．

(i) $\forall\varepsilon>0\quad a\le b+\varepsilon \iff a\le b.$
(ii) $\forall\varepsilon\ge 0\quad a\le b+\varepsilon \iff a\le b.$

[*4] Q.E.D. を使う場合はその直前に示したいことが書いていないとトンチンカンな文章になる事に留意されたい.

(iii) $\forall \varepsilon \geq 0 \quad a < b + \varepsilon \iff a < b.$

命題 1.3.4. $\forall \varepsilon > 0 \quad |a - b| < \varepsilon \iff a = b.$

証明. $\Longleftarrow$ は明らか. $\Longrightarrow$ を示す. $\forall \varepsilon > 0 \quad |a - b| < \varepsilon$ を仮定すると

$$\forall \varepsilon > 0 \quad b - \varepsilon < a < b + \varepsilon.$$

よって $\forall \varepsilon > 0 \quad b < a + \varepsilon, \quad a < b + \varepsilon$. 命題 1.3.2 より $b \leq a$ かつ $a \leq b$, よって $a = b$ を得る. □

これは不等式から等式を導く手品である. 手品の種は正の数 ε をいくらでも小さくとってよいというところにある.

演習 1.3.5. 上の証明にならって次を示せ.

(i) $\forall \varepsilon > 0 \quad |a - b| \leq \varepsilon \iff a = b.$
(ii) $\forall \varepsilon \geq 0 \quad |a - b| \leq \varepsilon \iff a = b.$

例 1.3.6 (数列の収束).「数列 $\{x_n\}$ が α に収束する」という事を論理記号であらわし, さらにその否定を作れ.
解. 解析学では「数列 $\{x_n\}$ が α に収束する」という事は,「任意の正の数 ε に対し, ある自然数 N が存在して $n \geq N$ なるすべての n に対して $|x_n - \alpha| < \varepsilon$ が成り立つ」事であった. これを論理記号であらわすと,

$$\forall \varepsilon > 0 \quad \exists N \ \forall n \ \big((n \geq N) \to (|x_n - \alpha| < \varepsilon)\big)$$

となる. したがって, その否定は次のようになる.

$$\exists \varepsilon > 0 \quad \forall N \ \exists n \ \big((n \geq N) \wedge (|x_n - \alpha| \geq \varepsilon)\big).$$

注意.「$\{x_n\}$ が α に収束する」ことを論理記号と日常語をチャンポンにして次のように書く事が多い.

$$\forall \varepsilon > 0 \quad \exists N \quad \text{s.t. } \forall n \ (n \geq N \text{ ならば } |x_n - \alpha| < \varepsilon)$$

または

$$\forall \varepsilon > 0 \quad \exists N \quad \text{s.t. } |x_n - \alpha| < \varepsilon \ (\forall n \geq N)$$

ここで s.t. は such that の略である. これは次のような英文の略であると考えるとわかりやすい.
For any positive number ε there exists a natural number N such that $|x_n - \alpha| < \varepsilon$ for any n with $n \geq N$.

念の為，筆記体でも書いておこう．
For any positive number ε there exists a natural number N such that $|x_n - \alpha| < \varepsilon$ for any n with $n \geq N$.

例 1.3.7. 数列 $\{a_n\}$ が収束すれば，収束先は一意的である．
解． これは $a_n \to \alpha$ かつ $a_n \to \beta$ ならば $\alpha = \beta$ ということを主張している．仮定より

$$\forall \varepsilon > 0\ \exists N_1 \text{ s.t. } n \geq N_1 \ \text{ ならば } \ |a_n - \alpha| < \varepsilon$$
$$\forall \varepsilon > 0\ \exists N_2 \text{ s.t. } n \geq N_2 \ \text{ ならば } \ |a_n - \beta| < \varepsilon$$

である．任意の $\varepsilon > 0$ に対し，N_1, N_2 を，ここで存在を仮定したものとする．N を N_1, N_2 どちらよりも大きい自然数とすると，$n \geq N$ のとき

$$|\alpha - \beta| = |(\alpha - a_n) + (a_n - \beta)| \leq |\alpha - a_n| + |a_n - \beta| < \varepsilon + \varepsilon = 2\varepsilon$$

ε は任意の正の数であったから，命題 1.3.4 より $\alpha = \beta$.

例 1.3.8 (有界数列).「数列 $\{x_n\}$ が有界である (bounded)」という事を論理記号であらわし，さらにその否定を作れ．
解．「数列 $\{x_n\}$ が有界である」ということは「ある正の数 K が存在してすべての n に対し $|x_n| < K$ が成り立つ」ことであるから，論理記号で書くと

$$\exists K > 0\ \forall n\ (|x_n| < K)$$

となる．これを否定すると

$$\forall K > 0\ \exists n\ (|x_n| \geq K).$$

例 1.3.9 (関数の連続性).「関数 $f(x)$ が $x = a$ で連続である」という事を論理記号であらわし，さらにその否定を作れ．
解． 解析学では「数列 $f(x)$ が $x = a$ で連続である」という事は，「任意の正の数 ε に対し，ある正の数 δ が存在して $|x - a| < \delta$ ならば $|f(x) - f(a)| < \varepsilon$ が成り立つ」事であった．これを論理記号であらわすと，

$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x\ \big((|x - a| < \delta) \to (|f(x) - f(a)| < \varepsilon)\big)$$

となる．したがって，その否定は次のようになる．

$$\exists \varepsilon > 0\ \forall \delta > 0\ \exists x\ \big((|x - a| < \delta) \wedge (|f(x) - f(a)| \geq \varepsilon)\big).$$

注意．「$f(x)$ が $x = a$ で連続である」ことを論理記号と日常語をチャンポンにして次のように書く事が多い．

$$\forall \varepsilon > 0\ \exists \delta > 0 \text{ s.t. } \forall x\ (|x - a| < \delta \text{ ならば } |f(x) - f(a)| < \varepsilon)$$

これは次のような英文の略であると考えられる．
For any positive number ε there exists a positive number δ such that $|f(x)-f(a)|<\varepsilon$ for any x with $|x-a|<\delta$.
筆記体でも書いておこう．
For any positive number ε there exists a positive number δ such that $|f(x)-f(a)|<\varepsilon$ for any x with $|x-a|<\delta$.

なお日常語に近い言葉で論理的な内容を書くときは，「かつ」をあらわす $\wedge$ はカンマ , であらわし，「または」をあらわす $\vee$ は or であらわす事が多い．例えば上に現れた「$f(x)$ が $x=a$ で連続である」の否定はしばしば次のように書く．

$$\exists \varepsilon>0 \text{ s.t. } \big(\forall \delta>0\ \exists x \text{ s.t. } |x-a|<\delta, |f(x)-f(a)|\geq \varepsilon\big).$$

数学的な推論においては，論理記号を用いると厳密ではあるが表現がかたくなって，しばしば読みづらくなる．したがって，「必要に応じて論理記号を用いて数学的な推論をする」というのが望ましい．

注意．カンマの使い方について，少し注意をしておく．例えば「方程式 $x^2=1$ を解け」という問題の解を「$x=1,-1$」と書くが，この場合は、カンマを「または」の意味で使っている．これを見ても解るように，カンマを「かつ」の意味で使うというルールは常に適用される訳ではない．前後の文脈から明らかになっている場合は，「かつ」や「または」は省略して表記する事があると，理解しておくと良い．ただ繰り返しになるが，「『かつ $\wedge$』は省略してカンマを使い，『または $\vee$』 は or で表す」というのは，論理式を扱う時によく使われれる表記法である．

クレタ人は嘘つき．論理に関するパラドックスで，古来有名なものに，クレタ人エピメニデスが述べた「クレタ人はいつも嘘をつく」というのがある (新約聖書「テトスへの手紙」1 章 12-15 節)．この命題が正しいとすると，クレタ人は嘘つきであり，クレタ人エピメニデスが述べたこの命題は偽であり, クレタ人は嘘つきでないことになる．よってクレタ人エピメニデスが述べたこの命題は真であることになる，よってこの命題は真とも偽とも決められない[*5]というのである．このように真と考えても，偽と考えても矛盾の起こる命題を**自己矛盾命題** (self-contradictory proposition) という．同じようなパラドックスをもう一つ紹介しよう．

下の陳述は誤りである．

上の陳述は正しい．

このように，自分自身の真偽に言及するような文の体系を考えると，自己矛盾命題が現れやすいことが経験的にわかっている．このような自己矛盾命題は，論理式を構成するための文法をよく吟味せずに, 論理式をつくってしまったことに原因があると考えられる．自己矛盾命題を数学の中から排除してゆこうというのを主な動機として，論理学が数学の一分野として研究されるようになった.
それによると論理式の定義は次のように与えられる.
まず原子論理式 (atomic formula, atom) と呼ばれるものを定める．次に論理式を次のように定める.

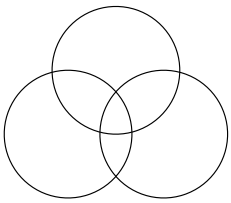
(i) 原子論理式は論理式である.
(ii) p, q が論理式ならば $\neg p$, $p \wedge q$, $p \vee q$, $p \to q$ も論理式である.
(iii) $p(a)$ が自由変数 a を含み, 束縛変数 x を含まない論理式ならば $\forall x\, p(x)$, $\exists x\, p(x)$ は論理式である.
(iv) 原子論理式から (ii), (iii) を繰り返して得られるものだけが論理式である.

われわれは目的に応じて，いろいろの範囲の原子論理式を定めることによりいろいろな範囲の論理式を定めることができるのである．また注意深く原子論理式を定めることにより，上のようなパラドックスを避けることもできるのである.

[*5] 「すべてのクレタ人は嘘つき」を否定すると「あるクレタ人は嘘つきでない」となるので，厳密にはパラドックスとは言えない.

第 2 章

素朴集合論の初歩



数学で「集合」といえば，集まることではなく，「ものの集まり」のことである．例えば「自然数全体の集まり」や「$0 \leq x \leq 1$ であるような実数 x の全体の集まり」等は集合である．しかし日常考える「ものの集まり」には「大きな数の集まり」や「背が高い人の集まり」のようなものもある．しかしこれらは数学では集合とはいわない．数学で「集合」と呼ぶ「ものの集まり」は「どんなものをとってきても，それがその集まりのなかにあるかないかがはっきり定まっている」ものでなければならないのである．

ここではそのように素朴に考えた集合の理論，素朴集合論 (naive set theory) の初歩を学ぶ．

日本語	英語 (筆記体)	フランス語	ドイツ語	ロシア語
集合	set ($\mathcal{S}\mathcal{e}\mathcal{t}$)	ensemble	Menge	множество

2.1 集合

集合は，普通アルファベットの大文字 $A, B, C, \ldots, S, T, \ldots$ を使って表される．A が集合であるとき, A の中に入っている個々の「もの」を A の**元**，または**要素** (英語では element) という．a が集合 A の元であることを

$$a \in A, \quad \text{または} \quad A \ni a$$

と書き，a は集合 A に**属する** (または**含まれる**) という．$a \in A$ の否定は

$$a \notin A, \quad \text{または} \quad A \not\ni a$$

であらわす.

頻繁に現れる基本的ないくつかものは，しばしば固有の記号で表され，固有名詞的に用いられる．代表的なものを挙げておく．

$\mathbb{N}$ = 自然数全体の集合 (the set of natural numbers)
$\mathbb{Z}$ = 整数全体の集合 (the set of integers)
$\mathbb{Q}$ = 有理数全体の集合 (the set of rational numbers)
$\mathbb{R}$ = 実数全体の集合 (the set of real numbers)
$\mathbb{C}$ = 複素数全体の集合 (the set of complex numbers)

なお自然数全体の集合に 0 を含める流儀と，含めない流儀があるので本を読むときや，人の話を聞くときは注意して欲しい．0 を含めないのはアメリカ流で，0 を含めるのはフランスに端を発するようである．しかしこの区別は厳密なものでなく同じ人でも都合によって自然数に 0 を含めたり，含めなかったりする．

$$\mathbb{N} = \{1, 2, 3, \ldots.\}, \quad \text{または} \quad \mathbb{N} = \{0, 1, 2, 3, \ldots.\}.$$

次に，個々の集合を具体的にあらわす記法について説明する．例として「10 より小さい素数の集まり」を考えよう．これを要素を列挙して

$$\{2, 3, 5, 7\}$$

とあらわすことができる．このようにすべての要素を列挙して集合をあらわす表記法を**外延的記法**という．

上の自然数全体の集合の表記 $\mathbb{N} = \{1, 2, 3, \ldots.\}$ も外縁的記法の一種と考えられる．一方，要素の性質を書いて集合を書きあらわすことも考えられる．たとえば，次のようなものである．

$$\{x \mid x \text{ は } 10 \text{ より小さい素数 }\}$$

これを集合の**内包的記法**という．いいかえると $P(x)$ を述語とし，述語 $P(x)$ を真にするようなすべての x 全体の集合を

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

であらわす[*1]のが，集合の**内包的記法**である．「$0 \leq x \leq 1$ であるような実数 x の全体の集合」は内包的記法を用いて

$$\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$$

とあらわすのが普通である．

すべての x について述語 $P(x)$ が偽ということもおこりうる．このような場合も $\{x \mid P(x)\}$ を集合として扱えた方が便利である．そこで元を一つも含まないものも集合と考え，これを**空集合** (empty set) とよび，記号 $\varnothing$ であらわす．例えば

$$\{x \in \mathbb{R} \mid x^2 + 1 = 0\}$$

は空集合である

定義 2.1.1 (部分集合). 集合 A, B において A の元がすべて B の元であるとき，すなわち，

$$\forall x \quad x \in A \Longrightarrow x \in B \tag{2.1}$$

が成り立つならば，A は B の**部分集合** (subset) であるといい，

$$A \subset B \quad \text{または} \quad B \supset A$$

と書く．このことを A は B に**含まれる**，または B は A を**含む**などともいう．

空集合はすべての集合の部分集合である．$A = \varnothing$ とした時、$x \in A$ は常に偽であり、論理式 (2.1) は真であるからである．

$A \subset B$ の否定を

$$A \not\subset B \quad \text{または} \quad B \not\supset A$$

であらわす．これは論理記号で書くと次のようになる．

$$\exists x \quad x \in A \quad x \notin B$$

A が B の部分集合であるというときには，$A = B$ である特別の場合も除外されていない．$A \subset B$ かつ $A \neq B$ のときには A は B の**真部分集合** (proper subset) であるといい，

$$A \subsetneq B, \quad A \subsetneqq B, \quad B \supsetneq A, \quad B \supsetneqq A$$

などと書く．

[*1] $\{x : P(x)\}$ や $\{x\,;P(x)\}$ を使うこともある．

A が B の部分集合であることを $A \subseteq B$ と書き, A が B の真部分集合であることを $A \subset B$ と書く流儀もある．不等号 $<$ の類推からこのように書くのがよいと考えるのであろう．ここで $A \subset B$ を部分集合の意味で使い，真部分集合を表したいときは $A \subsetneq B$ または $A \subsetneqq B$ を使うことにする．

数学の理論を展開するとき，そのとき考えている集合はすべて，ある 1 つの定まった集合 U の部分集合である，ということがわかっているような場合が少なくない．そのような場合 その定まった集合 U のことを**全体集合** (whole set)，または**宇宙** (universe) とよぶ.

変数 x が全体集合 U を動くとする．U の部分集合 A, B を述語 $P(x), Q(x)$ を用いて内包的に次のようにあらわせているとする．

$$A = \{x \in U \mid P(x) \text{ が真 }\}, \quad B = \{x \in U \mid Q(x) \text{ が真 }\}$$

このとき，すべての $x \in U$ に対し $P(x) \Longrightarrow Q(x)$ が成り立つということは $A \subset B$ と同値であることに注意しておこう．

次の命題は明らかであろう．

$$\begin{aligned} A = B &\Longleftrightarrow A \subset B,\ B \subset A \\ &\Longleftrightarrow \forall x\ (x \in A \Leftrightarrow x \in B) \end{aligned}$$

よって 2 つの集合 A と B が等しいことを証明するには, $A \subset B$ であることと，$A \supset B$ であることを証明すればよい．実際，2 つの集合が等しいことの証明は，ほとんどすべての場合に，このようにして行われるのである．

集合算

2 つの集合 A, B が与えられたとき, A の元と B の元を全部合わせて得られる集合を, A と B の**和集合** (union) といい $A \cup B$ であらわす．内包的記法を用いると $A \cup B$ は次のように書きあらわすことができる．

$$A \cup B := \{x \mid x \in A \text{ または } x \in B\}$$

2 つの集合 A, B が与えられたとき, A, B の両方に共通な元全体の集合を, A と B の**共通部分** (intersection) といい $A \cap B$ であらわす．内包的記法を用いると $A \cap B$ は次のように書きあらわすことができる．

$$A \cap B := \{x \mid x \in A, x \in B\}$$

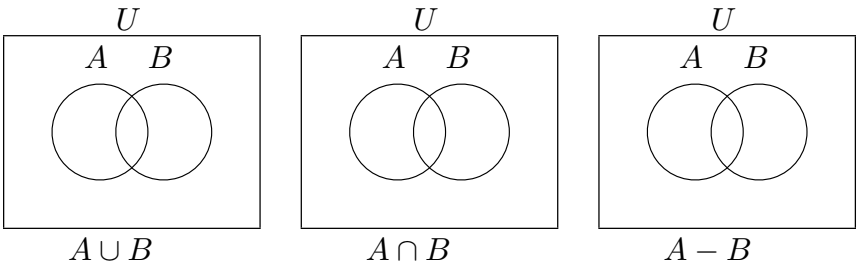
2 つの集合 A, B が与えられたとき, A に属するが，B には属さない様な元全体の集合を, A に対する B の**差集合**といい

$$A - B \quad \text{または} \quad A \setminus B$$

であらわす．内包的記法を用いると $A - B$ は次のように書きあらわすことができる．

$$A - B := \{x \mid x \in A, x \notin B\}$$

演習 2.1.2. 和集合 $A \cup B$, 共通部分 $A \cap B$, 差集合 $A - B$ を，次の Venn 図に図示せよ．



$A \cup B$　　$A \cap B$　　$A - B$

Venn 図[*2]は直観的理解には便利で，よい Venn 図は思考を助けるが，Venn 図による説明だけでは，数学の証明とはいえないことに注意しておこう．

全体集合 U が与えられているとき，集合 A の U に対する差集合 $U - A$ を A の**補集合** (complement) といい，記号 A^c であらわす．

$$A^c = \{x \in U \mid x \notin A\}$$

である．

演習 2.1.3. 全体集合 U の部分集合に対し $A - B = A \cap B^c$ を示せ．

演算 $\cup$, $\cap$ については次の公式が成り立つ．

$$\begin{array}{lrcl}
\text{交換律：} & A \cup B & = & B \cup A, \\
 & A \cap B & = & B \cap A. \\
\text{結合律：} & (A \cup B) \cup C & = & A \cup (B \cup C), \\
 & (A \cap B) \cap C & = & A \cap (B \cap C). \\
\text{分配律：} & (A \cup B) \cap C & = & (A \cap C) \cup (B \cap C), \\
 & (A \cap B) \cup C & = & (A \cup C) \cap (B \cup C). \\
\text{吸収律：} & (A \cup B) \cap A & = & A, \\
 & (A \cap B) \cup A & = & A.
\end{array}$$

演習 2.1.4. 以上を証明せよ．

[*2] John Venn (1834–1923) はイギリスの論理学者

2.2 集合と写像

定理 2.2.1 (de Morgan の法則). U を全体集合，A, B をその部分集合とすると次が成り立つ.

$$(A \cap B)^c = A^c \cup B^c, \quad (A \cup B)^c = A^c \cap B^c.$$

証明. 最初の式だけ示す.

$$\begin{aligned} x \in (A \cap B)^c &\Leftrightarrow x \notin A \cap B \\ &\Leftrightarrow \neg(x \in A \cap B) \\ &\Leftrightarrow \neg(x \in A,\ x \in B) \\ &\Leftrightarrow \neg(x \in A) \text{ または } \neg(x \in B) \\ &\Leftrightarrow x \notin A \text{ または } x \notin B \\ &\Leftrightarrow x \in A^c \text{ または } x \in B^c \\ &\Leftrightarrow x \in A^c \cup B^c \end{aligned}$$

□

演習 2.2.2. de Morgan の法則の 2 番目の式を証明せよ.

対象 a と b の**順序対** (ordered pair) を (a, b) であらわす．すなわち

$$(a, b) = (a', b') \quad \overset{\text{def}}{\Longleftrightarrow} \quad a = a',\ b = b'$$

と約束[*3] して，対 (a, b) を考察の対象とする.

集合 A, B に対して，A の元 a と B の元 b の順序対 (a, b) 全体からなる集合を A と B の**直積集合** (direct product of sets) といい $A \times B$ であらわす．すなわち,

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

である．自分自身との直積集合 $A \times A$ を A^2 と書く．n 個の A の元の組 $(a_1, \ldots, a_n)$ を考え,

$$(a_1, \ldots, a_n) = (a_1', \ldots, a_n') \quad \overset{\text{def}}{\Longleftrightarrow} \quad a_1 = a_1',\ \ldots,\ a_n = a_n'$$

[*3] a' は a プライムと呼ぶ．a ダッシュとよぶ場合もあるが，英語圏では a プライムと呼ぶのが普通である．英語圏でも英国では記号 $'$ をダッシュとする読み方があり，その影響を受けた国（アイルランド，オーストラリア，日本やインドなど）ではダッシュと呼ぶことも多い．日本で定着したダッシュという読みは，明治初頭の技術教育がスコットランド出身のヘンリー・ダイアーやチャールズ・ウェストにより英国風に行われたことに求めることができる．(Wikipedia より)

と約束する．$(a_1, \ldots, a_n)$ 達全体の集合を A の n 個の直積集合といい

$$A^n := \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in A\}$$

と書く．

集合 A のすべての部分集合全体を A の**冪集合** (power set) といい記号 2^A または $\mathfrak{P}(A)$ であらわす．

例 2.2.3. 集合 $A = \{1, 2, 3\}$ のすべての部分集合全体 2^A は次のようになる．

$$2^A = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}$$

演習 2.2.4. 集合 $A = \{1, 2, \ldots, n\}$ のすべての部分集合全体 2^A は次のようになる．

$$2^A = \big\{\varnothing, \{1\}, \{2\}, \ldots, \{n\}, \{1, 2\}, \{1, 3\}, \ldots, \{1, 2, \ldots, n\}\big\}$$

2^A はいくつ元を含むか?

写像

集合 X, Y において，X の各元 x に対して Y のある元を対応させる規則が定まっているとき，X から Y への**写像** (map of X to Y) が定められているという．f が X から Y への写像であることを

$$f : X \to Y \quad \text{または} \quad X \xrightarrow{f} Y$$

のようにあらわす．このとき f によって X の元 x に Y の元 y が対応するとすれば

$$f(x) = y \quad \text{または} \quad x \mapsto y$$

と書いて，y を x の f による**像** (image) という．

写像 $f : X \to Y$ において X を 写像 f の**定義域** (domain) といい

$$f(X) = \{y \in Y \mid \exists x \in X \text{ s.t. } f(x) = y\} = \{f(x) \mid x \in X\}$$

を写像 f の**値域** (range) という．

例 2.2.5. 集合 X に対し $1_X : X \to X$, $x \mapsto x$, を**恒等写像** (identity) という．

例 2.2.6. 集合 X, Y と写像 $f : X \to Y$, $x \mapsto f(x)$, があるとする．X の部分集合 A に対し写像

$$f|_A : A \to Y, \quad a \mapsto f(a)$$

を f の A への**制限写像** (restriction) という．制限写像をあらわすのに記号 $f|_A$, $f|A$ などを用いる．

定義 2.2.7. 写像 $f : X \to Y$ が与えられているとする．X の部分集合 A に対し，

$$f(A) = \{y \in Y \mid \exists x \in A \text{ s.t. } f(x) = y\} = \{f(a) \mid a \in A\}$$

を A の f による**像** (image) という．ここで $f(\varnothing) = \varnothing$ と約束する．また Y の部分集合 B に対し，

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

を B の f による**逆像** (inverse image)（または**原像**）という．ここで $f^{-1}(\varnothing) = \varnothing$ と約束する．また元 $y \in Y$ に対し，$f^{-1}(y)$ を次で定義する．

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

これは $f^{-1}(\{y\})$ のことであり，一般には X の部分集合である．

例 2.2.8. 写像 $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, を考える．$A = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$ とおくと

$$f(A) = \{x \in \mathbb{R} \mid 1 \leq x \leq 4\}$$

となる．$B = \{y \in \mathbb{R} \mid 1 \leq y \leq 4\}$ とおくと，

$$f^{-1}(B) = \{x \in \mathbb{R} \mid -2 \leq x \leq -1\} \cup \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$$

となる．また $f^{-1}(4) = \{2, -2\}$ である．

演習 2.2.9. 写像 $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = x^2 - y^2$, を考える．

(i) $A = \{(x, y) \in \mathbb{R}^2 \mid 1 \leq x \leq 2,\ 1 \leq y \leq 2\}$ とおくとき $f(A)$ を求めよ．
(ii) $B = \{z \in \mathbb{R} \mid 1 \leq z \leq 4\}$ とおくとき，$f^{-1}(B)$ を求めよ．

演習 2.2.10 (線形写像). a, b, c, d を実数とし，次の写像を考える．

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

ここでは $\mathbb{R}^2 = \{\binom{x}{y} \mid x, y \in \mathbb{R}\}$ としている．$0 = \binom{0}{0}$ とおくとき，

(i) $ad - bc \neq 0$ のとき $f^{-1}(0)$ を求めよ．
(ii) $ad - bc = 0$ のとき $f^{-1}(0)$ を求めよ．

集合 X, Y 間の写像 $f : X \to Y$ について，一般に成立する定理をあげておこう．

定理 2.2.11. A, A_1, A_2 を X の部分集合とするとき，次が成り立つ．

(i) $A_1 \subset A_2 \Longrightarrow f(A_1) \subset f(A_2)$.

(ii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
(iii) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
(iv) $f(X - A) \supset f(X) - f(A)$.
(v) $A \subset f^{-1}(f(A))$.

証明. (i): $y \in f(A_1) \iff \exists x \in A_1[f(x) = y] \implies \exists x \in A_2[f(x) = y] \iff y \in f(A_2)$.
(ii): $y \in f(A_1 \cup A_2) \iff \exists x \in A_1 \cup A_2\ [f(x) = y] \iff \exists x\ [(x \in A_1 \vee x \in A_2) \wedge f(x) = y]$
$\iff [\exists x \in A_1(f(x) = y) \vee \exists x \in A_2(f(x) = y)] \iff y \in f(A_1) \cup f(A_2)$
(iii): $y \in f(A_1 \cap A_2) \iff \exists x \in A_1 \cap A_2\ [f(x) = y] \iff \exists x\ [(x \in A_1 \wedge x \in A_2) \wedge f(x) = y]$
$\implies [\exists x_1 \in A_1(f(x_1) = y)] \wedge [\exists x_2 \in A_2(f(x_2) = y)] \iff y \in f(A_1) \cap f(A_2)$
(iv): $y \in f(X) - f(A)$ なる y をとる．$y \in f(X)$ より $f(x) = y$ なる $x \in X$ が存在する．$x \notin A$ を示せばよい．ところで $y \notin f(A)$ より $\forall a \in A\ f(a) \neq y$ なので $x \in A$ とはならない．よって $x \in X - A$.
(v): $x \in A$ より $f(x) \in f(A)$. これは $x \in f^{-1}(f(A))$ を意味している． □

演習 2.2.12. (iii), (iv), (v) で実際に両辺が異なるような例をあげよ．

定理 2.2.13. B, B_1, B_2 を Y の部分集合とするとき，次が成り立つ．

(i) $B_1 \subset B_2 \implies f^{-1}(B_1) \subset f^{-1}(B_2)$.
(ii) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
(iii) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
(iv) $f^{-1}(Y - B) = f^{-1}(Y) - f^{-1}(B)$.
(v) $B \cap f(X) = f(f^{-1}(B))$.

証明. (i): $x \in f^{-1}(B_1) \iff f(x) \in B_1 \implies f(x) \in B_2 \iff f(x) \in B_2$
(ii): $x \in f^{-1}(B_1 \cup B_2) \iff f(x) \in B_1 \cup B_2 \iff (f(x) \in B_1) \vee (f(x) \in B_2)$
$\iff [x \in f^{-1}(B_1)] \vee [x \in f^{-1}(B_2)] \iff x \in f^{-1}(B_1) \cup f^{-1}(B_2)$
(iii): $x \in f^{-1}(B_1 \cap B_2) \iff f(x) \in B_1 \cap B_2 \iff (f(x) \in B_1) \wedge (f(x) \in B_2)$
$\iff [x \in f^{-1}(B_1)] \wedge [x \in f^{-1}(B_2)] \iff x \in f^{-1}(B_1) \cap f^{-1}(B_2)$
(iv): $x \in f^{-1}(Y - B) \iff f(x) \in Y - B \iff f(x) \notin B \iff x \notin f^{-1}(B)$
$\iff x \in X - f^{-1}(B)$
(v): $y \in B \cap f(X) \iff (y \in B) \wedge [\exists x \in X(f(x) = y)]$
$\iff \exists x \in f^{-1}(B)[f(x) = y] \iff y \in f(f^{-1}(B))$ □

2.3 全射と単射

定義 2.3.1 (全射). 写像 $f : X \to Y$ において，$f(X) = Y$ であるとき，f を X から Y の**上への写像** (map of X onto Y) または f は**全射** (surjection) であるという．いいかえると

$$f : \text{全射} \overset{\text{def}}{\iff} \forall\, y \in Y,\ \exists\, x \in X \text{ s.t. } f(x) = y$$

である．全射を $f : X \twoheadrightarrow Y$ のように書くことがある．

surjection は Bourbaki による造語であるらしい．フランス語では on にあたる前置詞が sur なので surjection という言葉が作られたようである．

定義 2.3.2 (単射). 写像 $f : X \to Y$ において，任意の $x, x' \in X$ に対し

$$x \neq x' \quad \text{ならば} \quad f(x) \neq f(x'),$$

または，同じことであるが,

$$f(x) = f(x') \quad \text{ならば} \quad x = x'$$

であるとき，f を**一対一写像** (one-to-one map)，または f は**単射** (injection) であるという．単射を $f : X \hookrightarrow Y$ のように書くことがある．この使い方も Bourbaki による．

注: 病院で injection と言えば注射のことであるが, 数学で injection と言えば単射のことである．

例 2.3.3. 全射や単射のいろいろな例をあげておこう．

(i) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x + 1$, は全射かつ単射.
(ii) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, は全射でもなく単射でもない.
(iii) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 + x$, は全射かつ単射.
(iv) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3 - x$, は全射だが単射でない.
(v) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \tan^{-1} x$, は全射でないが単射.

定理 2.3.4. $f : X \to Y$ が単射ならば，X の部分集合 A, A_1, A_2 に対し次が成り立つ.

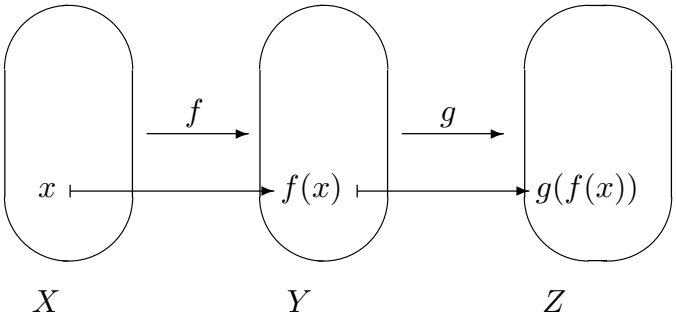
(i) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.
(ii) $f(X - A) = f(X) - f(A)$.
(iii) $A = f^{-1}(f(A))$.

証明. (i) だけ示す．他は演習に残す．
$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$ は定理 2.2.11(iii) で示したので, $f(A_1 \cap A_2) \supset f(A_1) \cap f(A_2)$ を示せば十分.
$y \in f(A_1) \cap f(A_2)$ とすると $\exists a_1 \in A_1\ f(a_1) = y$, $\exists a_2 \in A_2\ f(a_2) = y$. $f(a_1) = y = f(a_2)$ で f は単射なので $a_1 = a_2 \in A_1 \cap A_2$. よって $y = f(a_1) \in f(A_1 \cap A_2)$. □

演習 2.3.5. (ii), (iii) の証明を完成させよ.

写像の合成

写像 $f : X \to Y$ と $g : Y \to Z$ が与えられているとき $x \mapsto g(f(x))$ できまる写像 $X \to Z$ を f と g の**合成** (composition) といい $g \circ f$ であらわす.



演習 2.3.6. 写像 $f : X \to Y$, $g : Y \to Z$ に対し，次を示せ.

(i) f, g がともに全射ならば合成 $g \circ f$ は全射.
(ii) f, g がともに単射ならば合成 $g \circ f$ は単射.

例 2.3.7. 写像 $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, と写像 $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$, にたいし，合成 $g \circ f : \mathbb{R} \to \mathbb{R}$ は $g \circ f(x) = x^2 + 1$ で与えられる．また合成 $f \circ g : \mathbb{R} \to \mathbb{R}$ は $f \circ g(x) = (x + 1)^2$ で与えられる.

例 2.3.8 (線形写像の合成). a, b, c, d, p, q, r, s を実数とし，次の写像 f, g を考える.

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$
$$g : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} px + qy \\ rx + sy \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

このとき，合成 $g \circ f : \mathbb{R}^2 \to \mathbb{R}^2$ は次の式で与えられる.

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} p(ax + by) + q(cx + dy) \\ r(ax + by) + s(cx + dy) \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

定理 2.3.9. 写像 $f : X \to Y$, $g : Y \to Z$, $h : Z \to W$ に対し,

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

よってこの写像を $h \circ g \circ f$ の様に書いても，曖昧さはない.

証明. 任意の $x \in X$ に対し,

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

より従う. □

定理 2.3.10. 写像 $f : X \to Y$, $g : Y \to Z$ に対し，次が成り立つ.

(i) 合成 $g \circ f$ が全射ならば g は全射.
(ii) 合成 $g \circ f$ が単射ならば f は単射.

証明. (i) を示す．$z \in Z$ を任意にとる．$g(y) = z$ なる $y \in Y$ が存在することを示せばよい．仮定より $g \circ f$ が全射なので，$g \circ f(x) = z$ なる $x \in X$ が存在する．$y = f(x)$ が求めるものである.

(ii) を示す．$x_1, x_2 \in X$ に対し，$f(x_1) = f(x_2)$ ならば $x_1 = x_2$ を示せばよい．$f(x_1) = f(x_2)$ より $g \circ f(x_1) = g \circ f(x_2)$. $g \circ f$ は単射だから $x_1 = x_2$ である. □

演習 2.3.11. 写像 $f : X \to Y$, $g : Y \to Z$ があるとき次を示せ.

(i) 合成 $g \circ f$ が全射で g が単射ならば f は全射.
(ii) 合成 $g \circ f$ が単射で f が全射ならば g は単射.

演習 2.3.12. 写像 $f : X \to Y$ を全射とし，写像 $g : Y \to Z$, $g' : Y \to Z$ に対し $g \circ f = g' \circ f$ ならば $g = g'$ を示せ.

全単射と逆写像

定義 2.3.13 (全単射). 写像 $f : X \to Y$ が全射かつ単射であるとき，f は **全単射** (bijection) である，または**双射**であるという.

bijection も Bourbaki による造語である.

定義 2.3.14 (逆写像). 写像 $f : X \to Y$ が全単射であるとき，写像 $f^{-1} : Y \to X$ を

$$x = f^{-1}(y) \quad \Longleftrightarrow \quad f(x) = y$$

で定義することができる．f^{-1} もまた全単射である．f^{-1} を f の**逆写像** (inverse map) という．

定義 2.2.7 の記号に従うと，f が全単射であれば $f^{-1}(y)$ は一点からなる X の部分集合である．この記法によれば $\{x\} = f^{-1}(y)$ で，これは逆写像の上の記法 $x = f^{-1}(y)$ と紛らわしいが，意味をしっかり押えておけばまず混乱の恐れはない．

演習 2.3.15. 写像 $f : X \to Y$, $g : Y \to Z$ が全単射ならば $g \circ f : X \to Z$ も全単射で，$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ を示せ．

定理 2.3.16. 写像 $f : X \to Y$, $g : Y \to X$ について $g \circ f = 1_X$, $f \circ g = 1_Y$ ならば f は全単射で $g = f^{-1}$.

証明. $g \circ f = 1_X$ は単射なので，定理 2.3.10 (ii) より, f は単射である．$f \circ g = 1_Y$ は全射なので，定理 2.3.10 (i) より, f は全射である．よって f は全単射である．よって逆写像 f^{-1} が存在する．よって

$$g = g \circ 1_Y = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = 1_X \circ f^{-1} = f^{-1}.$$

□

演習 2.3.17. 写像 $f : X \to Y$, $g : Y \to X$, $g' : Y \to X$ について $g \circ f = 1_X$, $f \circ g' = 1_Y$ ならば f は全単射で $g = g' = f^{-1}$ を示せ．

例 2.3.18. 全単射の例を幾つか挙げてみよう．

(i) 写像 $f : (0,1) \to (a,b)$ を $f(x) = (b-a)x + a$ で定義すると，これは全単射である．
(ii) 写像 $f : (-\pi/2, \pi/2) \to \mathbb{R}$, $f(x) = \tan x$, は全単射である．
(iii) 写像 $f : (-1,1) \to \mathbb{R}$, $f(x) = x/(1-x^2)$, も全単射である．
(iv) $ad - bc \neq 0$ のとき，写像 $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\binom{x}{y} \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\binom{x}{y}$, も全単射である．

2.4 有限集合と無限集合

まず、単射、全射の性質を述べる.

定理 2.4.1. $f : X \to Y$ を写像とする.

(i) f が単射 $\iff g \circ f = 1_X$ なる写像 $g : Y \to X$ が存在する.
(ii) f が全射 $\iff f \circ g = 1_Y$ なる写像 $g : Y \to X$ が存在する.

証明. (i), (ii) ともに $\Longleftarrow$ は定理 2.3.10 から明らかである. (i) の $\Longrightarrow$ を示そう. $f : X \to Y$ は単射であるから, 写像 $f : X \to f(X)$ は全単射である. その逆写像 $g_0 : f(X) \to X$ とかく. X の元 x_0 を任意に決め固定する. 写像 $g : Y \to X$ を

$$g(y) = \begin{cases} g_0(y) & y \in f(X) \text{ のとき} \\ x_0 & y \notin f(X) \text{ のとき} \end{cases}$$

を定めると, これは条件をみたす.
(ii) の $\Longrightarrow$ の証明: f の全射性より、任意の $y \in Y$ に対し $f(x) = y$ となる $x \in X$ が存在する. この x を $g(y)$ と書けば $f \circ g = 1_Y$ となる. □
上述の (ii) の証明は, Y が有限集合の時はこの論法でよいが, Y が無限集合の時は完全とは言い難い. 実際, 写像 g の存在を示す事は,

$$P = \{g \in X^Y \mid g(y) \in f^{-1}(y)\ \forall y \in Y\}$$

が空集合でない事を示すことであり, 各 $y \in Y$ について $f^{-1}(y)$ が空集合でない事から、P が空集合でないことが帰結できるかどうかは直ちにはわからない. ここに選択公理の必要性があるのである. 後述の定理 2.6.20 の証明も参照のこと.

有限集合 (finite set)

$n+1$ 人の人を n 個の部屋へ入れるとどこかの部屋には 2 人以上入ることになる. これが部屋割り論法である.

補題 2.4.2 (部屋割り論法). 自然数 m, n に対し $m > n$ ならば

$$\text{集合 } \{1, 2, \ldots, m\} \text{ から } \{1, 2, \ldots, n\} \text{ への写像}$$

は単射にはなり得ない.

証明. n に関する数学的帰納法で示す．$n=1$ のときは明らかである．n のとき補題が成立すると仮定して $n+1$ のときを示す．$m>n+1$ として，単射写像

$$f:\{1,2,\ldots,m\}\longrightarrow\{1,2,\ldots,n+1\}$$

があったとして矛盾を導く．もし $n+1$ が f の像に入っていなければ，実際には f は $\{1,2,\ldots,m\}$ から $\{1,2,\ldots,n\}$ への写像で，仮定よりこれが単射なので，帰納法の仮定に矛盾する．よって $f(k)=n+1$ となる $k\in\{1,2,\ldots,m\}$ が存在しなければならない．ここで写像

$$g:\{1,2,\ldots,m-1\}\to\{1,2,\ldots,n\}\quad\text{を}$$

$$g(x)=\begin{cases} f(x) & (1\le x<k)\\ f(x+1) & (k\le x<m)\end{cases}$$

で定義すると f が単射なので g も単射となり帰納法の仮定に矛盾する． □

補題 2.4.3. 自然数 m,n に対し $m<n$ ならば集合 $\{1,2,\ldots,m\}$ から $\{1,2,\ldots,n\}$ への写像は全射にはなり得ない．

証明. 全射 $f:\{1,2,\ldots,m\}\to\{1,2,\ldots,n\}$ があったとする．各 $k\in\{1,2,\ldots,n\}$ に対し，$f^{-1}(k)$ の元を一つ選びそれを a_k と書く．このとき写像

$$g:\{1,2,\ldots,n\}\longrightarrow\{1,2,\ldots,m\},\quad k\mapsto a_k$$

は単射なので，補題 2.4.2 より $m\ge n$ となる． □

補題 2.4.4. $A_n=\{1,2,\ldots,n\}$ とする．このとき次が成り立つ．

(i) 写像 $f:A_n\to A_n$ が単射ならば，全射である．
(ii) 写像 $f:A_n\to A_n$ が全射ならば，単射である．

証明. (i): $f:A_n\to A_n$ が単射で，かつ全射でないとすると $f(A_n)$ に入らない $k\in A_n$ が存在する．よって f は n 個の元の集合から，$n-1$ 個の元の集合 $A_n-\{k\}$ への単射になり，補題 2.4.2 に矛盾．
(ii): $f:A_n\to A_n$ が全射で，かつ単射でないとすると $f(x)=f(y)$ なる相異なる A_n の元 x,y が存在する． f を $A_n-\{y\}$ に制限すればこれは $n-1$ 個の元の集合から，n 個の元をもつ集合への全射になり，補題 2.4.3 に矛盾． □

無限集合 (infinite set)

空でない集合 A と，集合 $\{1, 2, \ldots, n\}$ との間に全単射写像があるとき A は**有限集合**であるという．どんな自然数 n に対しても A と 集合 $\{1, 2, \ldots, n\}$ との間に全単射写像が存在しないとき，A は**無限集合**であるであるという．

例 2.4.5. 自然数全体の集合 $\mathbb{N}$ は無限集合である．整数全体の集合 $\mathbb{Z}$ や、有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ も無限集合である．

演習 2.4.6. 他に無限集合の例を挙げよ．

演習 2.4.7. A を無限集合とする．例えば $A = \mathbb{N}$ とする．

(i) 単射でかつ全射でない写像 $f : A \to A$ の例を挙げよ．
(ii) 全射でかつ単射でない写像 $f : A \to A$ の例を挙げよ．

無限集合の間の全単射の中には変わった写像も存在する．

例 2.4.8. 整数全体は次のように一列に並べることが出来る．

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

この事は，$\mathbb{N}$ と $\mathbb{Z}$ の間に全単射が存在することを意味している．

例 2.4.9. 正の有理数全体 $\mathbb{Q}_+$ と $\mathbb{N}$ の間に全単射が存在する．これは例えば次のようにして，構成する．まず分数を次のように並べる．

$$\begin{array}{ccccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \cdots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \cdots \\
\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

これを例えば次のようにして一列に並べる．

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \frac{3}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{4}{4}, \frac{4}{3}, \frac{4}{2}, \frac{4}{1}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{5}{5}, \frac{5}{4}, \frac{5}{3}, \frac{5}{2}, \frac{5}{1}, \frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6}, \frac{6}{5}, \frac{6}{4}, \frac{6}{3}, \frac{6}{2}, \frac{6}{1}, \ldots$$

この列から，既約でない分数をすべて消す．

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, \frac{3}{1}, \frac{1}{4}, \frac{3}{4}, \frac{4}{3}, \frac{4}{1}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{5}{4}, \frac{5}{3}, \frac{5}{2}, \frac{5}{1}, \frac{1}{6}, \frac{5}{6}, \frac{6}{5}, \frac{6}{1}, \ldots$$

これで正の有理数全体がもれも重複もなく一列に並んだ．

例 2.4.10. 開区間 $(0,1)$ と半開区間 $(0,1]$ の間に全単射が存在する．これは例えば数列 $\{x_i\}$ を $x_1 = 1$, $x_i > x_{i+1}$, $0 < x_i < 1$ $(i = 2,3,\dots)$ を満たすようにとり，$f : (0,1] \to (0,1)$ を $f(x) = x$, $x \neq x_i$, $f(x_i) = x_{i+1}$ で定めればよい．

例 2.4.11. 区間 $(0,1]$ の元を無限小数展開するとき 0.32 の様に有限項で止まる小数はわざと $0.31999\dots$ のように書き表すと約束しておく．この約束の下で定まる次の写像は単射である．

$$(0,1] \times (0,1] \to (0,1], \quad (0.a_1a_2\dots, 0.b_1b_2\dots) \mapsto (0.a_1b_1a_2b_2\dots)$$

なぜなら $(0.a_1b_1a_2b_2\dots)$ の形の小数表示は 0 が無限に続くことはなく，この表示から一意的に $(0.a_1a_2\dots, 0.b_1b_2\dots)$ が定まるからである。この写像の像は、明らかに区間 $(0,1]$ の部分集合であるが、この部分集合と、$(0,1] \times (0,1]$ の間に全単射が構成できた．

$(0,1] \times (0,1]$ と $(0,1]$ の間に全単射が構成できないだろうか? 以下工夫して構成してみよう．無限小数展開を，有限個（0 個も許す）の 0 の列の末尾に 0 でない数字をつけた塊の列にわける．例えば $0.00203025006\dots$ はその小数部分を $002|03|02|5|006|\dots$ のように分けておく．各 a_i, b_i をこのような塊とすれば，次の写像 g は全単射になる．

$$g : (0,1] \times (0,1] \to (0,1], \quad (0.a_1a_2\dots, 0.b_1b_2\dots) \mapsto (0.a_1b_1a_2b_2\dots)$$

例 2.4.10 の f を用いれば，次の写像は全単射である．

$$(0,1) \times (0,1) \to (0,1), \qquad (\alpha,\beta) \mapsto f \circ g(f^{-1}(\alpha), f^{-1}(\beta))$$

例 2.4.12. 自然数全体の集合 $\mathbb{N}$ と開区間 $(0,1)$ の間には全単射が存在しないことが証明できる．これは次のように行う．もし，全単射 $f : \mathbb{N} \to (0,1)$ があったとする．$(0,1)$ の元を例 2.4.11 のように無限小数展開することにすれば

$$\begin{aligned} f(1) &= 0.a_{11}a_{12}a_{13}\dots \\ f(2) &= 0.a_{21}a_{22}a_{23}\dots \\ f(3) &= 0.a_{31}a_{32}a_{33}\dots \\ &\dots \end{aligned}$$

と書き表される．ここで

$$b_k = \begin{cases} 1 & (a_{kk}\text{が偶数のとき}) \\ 2 & (a_{kk}\text{が奇数のとき}) \end{cases}$$

とおけば無限小数 $b = 0.b_1b_2b_3\dots$ は，開区間 $(0,1)$ の元だが $f(k)$ と b は小数第 k 位の偶奇が異なるので $f(k) = b$ となる k は存在しない．よって f が全射でないことになり矛盾．この証明は Cantor によるもので，しばしば**対角線論法**と呼ばれる．

2.5 集合族

U を全体集合とする．ある集合 Λ から 2^U への写像

$$\Lambda \to 2^U, \quad \lambda \mapsto A_\lambda$$

が与えられているとする．A_λ は全体集合 U の部分集合である．このとき $\{A_\lambda \mid \lambda \in \Lambda\}$ を Λ **を添数集合とする集合族** (family of sets indexed by Λ) という．集合族の記号として $\{A_\lambda\}_{\lambda\in\Lambda}$ を用いることもある．集合族 $\{A_\lambda\}$ のの**和集合** (union) および**共通部分** (intersection) を

$$\bigcup_{\lambda\in\Lambda} A_\lambda = \{x \in U \mid \exists\lambda \in \Lambda \text{ s.t. } x \in A_\lambda\}$$
$$\bigcap_{\lambda\in\Lambda} A_\lambda = \{x \in U \mid \forall\lambda \in \Lambda \ x \in A_\lambda\}$$

によって定義する．

例 2.5.1. $\Lambda = \{1, 2, 3, \dots, n\}$ とする．すると Λ を添数集合とする集合族とは，集合の有限列 $\{A_i\}_{i=1,2,\dots,n}$ のことである．この集合族の和集合および共通部分はそれぞれ次のようになる．

$$\bigcup_{i\in\Lambda} A_i = A_1 \cup \cdots \cup A_n$$
$$\bigcap_{i\in\Lambda} A_i = A_1 \cap \cdots \cap A_n$$

例 2.5.2. $\Lambda = \mathbb{N} = \{1, 2, 3, \dots\}$ とする．すると Λ を添数集合とする集合族とは，集合の無限列 $\{A_i\}_{i=1,2,\dots}$ のことである．この集合族の和集合および共通部分はそれぞれ次のようになる．

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

一般に，集合族というときは，このような $\Lambda = \mathbb{N}$ の場合だけではなく，任意の集合 Λ で添字づけられた集合の集まりを考える．

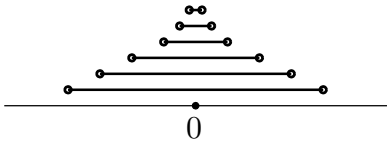
例 2.5.3. θ を実数とし $A_\theta = \{(x, y) \in \mathbb{R}^2 \mid x\cos\theta + y\sin\theta = 1\}$ とおく．A_θ は原点中

心の単位円の点 $(\cos\theta, \sin\theta)$ での接線だから，次が成り立つ．

$$\bigcup_{\theta\in\mathbb{R}} A_\theta = \{(x,y)\in\mathbb{R}^2 \mid x^2+y^2 \geq 1\}$$
$$\bigcap_{\theta\in\mathbb{R}} A_\theta = \varnothing$$

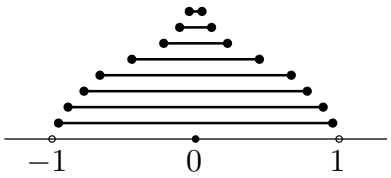
例 2.5.4. ε を正の実数として $A_\varepsilon = \{x\in\mathbb{R} \mid -\varepsilon < x < \varepsilon\}$ とおく．

$$\bigcup_{\varepsilon>0} A_\varepsilon = \mathbb{R}$$
$$\bigcap_{\varepsilon>0} A_\varepsilon = \{0\}$$



例 2.5.5. ε を正の実数として $B_\varepsilon = \{x\in\mathbb{R} \mid -\varepsilon \leq x \leq \varepsilon\}$ とおく．

$$\bigcup_{0<\varepsilon<1} B_\varepsilon = (-1,1)$$
$$\bigcap_{0<\varepsilon<1} B_\varepsilon = \{0\}$$



定理 2.5.6 (分配律). 任意の集合族 $\{A_\lambda \mid \lambda\in\Lambda\}$ と集合 B に対して，次が成立する．

$$\left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)\cap B = \bigcup_{\lambda\in\Lambda}(A_\lambda\cap B)$$
$$\left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)\cup B = \bigcap_{\lambda\in\Lambda}(A_\lambda\cup B)$$

証明. 任意の x に対し

$$\begin{aligned} x\in\left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)\cap B &\iff x\in\bigcup_{\lambda\in\Lambda} A_\lambda \text{ かつ } x\in B \\ &\iff (\exists\lambda\in\Lambda\ x\in A_\lambda) \text{ かつ } x\in B \\ &\iff \exists\lambda\in\Lambda\ (x\in A_\lambda \text{ かつ } x\in B) \\ &\iff \exists\lambda\in\Lambda\quad x\in A_\lambda\cap B \\ &\iff x\in\bigcup_{\lambda\in\Lambda}(A_\lambda\cap B) \end{aligned}$$

なので最初の式は成り立つ．二番目の式も同様である． □

定理 2.5.7 (de Morgan の法則). 集合族 $\{A_\lambda \mid \lambda\in\Lambda\}$ に対して次が成立する．

$$\left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)^c = \bigcap_{\lambda\in\Lambda} {A_\lambda}^c \qquad \left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)^c = \bigcup_{\lambda\in\Lambda} {A_\lambda}^c$$

演習 2.5.8. de Morgan の法則を示せ.

演習 2.5.9. 写像 $f : X \to Y$, $A_\lambda \in 2^X$ に対して，次を示せ.

$$f\left(\bigcup_{\lambda\in\Lambda} A_\lambda\right) = \bigcup_{\lambda\in\Lambda} f(A_\lambda)$$
$$f\left(\bigcap_{\lambda\in\Lambda} A_\lambda\right) \subset \bigcap_{\lambda\in\Lambda} f(A_\lambda)$$

さらに f が単射のときは二番目の式で等号が成立することを示せ.

演習 2.5.10. 写像 $f : X \to Y$, $B_\lambda \in 2^Y$ に対して，次を示せ.

$$f^{-1}\left(\bigcup_{\lambda\in\Lambda} B_\lambda\right) = \bigcup_{\lambda\in\Lambda} f^{-1}(B_\lambda)$$
$$f^{-1}\left(\bigcap_{\lambda\in\Lambda} B_\lambda\right) = \bigcap_{\lambda\in\Lambda} f^{-1}(B_\lambda)$$

定義 2.5.11. 集合 X, Y に対し，X から Y への写像全体の集合を Y^X と書く.

例 2.5.12. $X = \{1, 2\}$, $Y = \{1, 2, 3\}$ のとき，写像 $f : X \to Y$ は次の 9 通り考えられるので Y^X は $9(= 3^2)$ 個の元からなる集合である.

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9
1 の像	1	1	1	2	2	2	3	3	3
2 の像	1	2	3	1	2	3	1	2	3

演習 2.5.13. $X = \{1, 2, \ldots, m\}$, $Y = \{1, 2, \ldots, n\}$ のとき，集合 Y^X はいくつの元からなるか.

定義 2.5.14 (直積集合). いま Λ を添数集合とする X の部分集合族

$$\{A_\lambda \mid \lambda \in \Lambda\}$$

が与えられているとする．いま X^Λ の部分集合

$$P = \{f \in X^\Lambda \mid \forall\lambda \in \Lambda,\ f(\lambda) \in A_\lambda\}$$

を，Λ を添数集合とする集合族 $\{A_\lambda \mid \lambda \in \Lambda\}$ の**直積集合** (direct product of sets) といい

$$P = \prod_{\lambda\in\Lambda} A_\lambda$$

であらわす．P の元 f を

$$f = (a_\lambda)_{\lambda\in\Lambda}, \quad (a_\lambda = f(\lambda) \in A_\lambda)$$

または

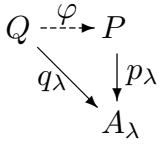
$$f = (\dots, a_\lambda, \dots)$$

とあらわす．直積集合 $P = \prod_{\lambda\in\Lambda} A_\lambda$ に対して写像 $p_\lambda : P \to A_\lambda$ を $p_\lambda(x) = a_\lambda$ で定義する．この p_λ を**射影** (projection) と呼ぶ.

直積集合の普遍性 *

$\{A_\lambda \mid \lambda \in \Lambda\}$ の直積集合 P と射影 $p_\lambda : P \to A_\lambda$ は次の性質を満たす.

Q を集合として，各 λ に対し写像 $q_\lambda : Q \to A_\lambda$ があるならば，各 λ に対し $p_\lambda \circ \varphi = q_\lambda$ を満たす写像 $\varphi : Q \to P$ が一意的に存在する．



実際，$x \in Q$ に対し，$\varphi(x) = (q_\lambda(x))$ （または $\varphi(x) : \Lambda \to X,\ \lambda \mapsto q_\lambda(x)$）と置けば，$p_\lambda \circ \varphi(x) = q_\lambda(x)$ となる．更に $p_\lambda \circ \varphi' = q_\lambda$ となる別の写像 $\varphi' : Q \to P$ があったとすると，任意の $\lambda \in \Lambda$ に対し，

$$\varphi'(x)(\lambda) = p_\lambda(\varphi'(x)) = q_\lambda(x) = p_\lambda(\varphi(x)) = \varphi(x)(\lambda)$$

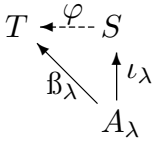
なので $\varphi'(x) = \varphi(x)$. $x \in Q$ は任意であったから $\varphi = \varphi'$ となり φ の一意性がわかる.

さて，上の枠内の性質を持つ集合 P と射影 $p_\lambda : P \to A_\lambda$ があったとする．すると．$P = Q, p_\lambda = q_\lambda$ として枠内の性質を使うと $\varphi = 1_P$ が上の性質を満たす．ところで，このような φ は一意的だから， φ は恒等写像でなければならない.

この性質を使って，上の枠内の性質を持つ集合 P と射影 $p_\lambda : P \to A_\lambda$ があったとするとき，直積 $\bar{P} = \prod_{\lambda\in\Lambda} A_\lambda$ とその射影 $\bar{p}_\lambda : \bar{P} \to A_\lambda$ に対し，逆写像を持つ写像 $\varphi : P \to \bar{P}$ が一意的に存在し．$p_\lambda = \bar{p}_\lambda \circ \varphi$ を満たす事を示そう．$\bar{P}$ は上の枠内の性質を満たすので写像 $\varphi : P \to \bar{P}$ が存在するが，P も上の枠内の性質を満たすので写像 $\phi : \bar{P} \to P$ も存在する．すると前段落で述べた性質より、$\varphi \circ \phi : P \to P$ は恒等写像でなければならない。同様に $\phi \circ \varphi : \bar{P} \to \bar{P}$ も恒等写像でなければならない。従って φ と ϕ は互いに他の逆写像である事がわかる。

演習 2.5.15. 集合族 $\{A_\lambda \mid \lambda \in \Lambda\}$ に対し，集合 S と各 $\lambda \in \Lambda$ に対し写像 $\iota_\lambda : A_\lambda \to S$ が与えられていて次の性質を満たすとする.

T を集合として，各 λ に対し写像 $ß_\lambda : A_\lambda \to T$ があるならば，各 λ に対し $\varphi \circ \iota_\lambda = ß_\lambda$ を満たす写像 $\varphi : S \to T$ が一意的に存在する．



$\bar{S} = \bigcup_{\lambda\in\Lambda}(A_\lambda \times \{\lambda\})$, $\bar{\iota}_\lambda : A_\lambda \to \bar{S}$, $x \mapsto (x, \lambda)$, と置く。$S = \bar{S}$ と置くと，この性質を満たすことを示せ．他にこの性質を満たす S があれば，逆写像を持つ写像 $\varphi : S \to \bar{S}$ があり $\varphi \circ \bar{\iota}_\lambda = \iota_\lambda$ を満たす事を示せ．(この $\bar{S}$ は集合の直和と呼ばれる事がある．)

2.6 順序集合と整列集合

定義 2.6.1 (順序集合). 集合 X で定義された**順序関係** $\preceq$ とは X の任意の 2 元 a, b に対し $a \preceq b$ であるかそうでないかが定まっていて次の条件を満たすときをいう.

(i) 反射律: $a \preceq a$.
(ii) 反対称律: $a \preceq b$ かつ $b \preceq a$ ならば $a = b$.
(iii) 推移律: $a \preceq b$ かつ $b \preceq c$ ならば $a \preceq c$.

集合 X とその順序 $\preceq$ を組にしたもの $(X, \preceq)$ を**順序集合**という. また, 順序関係のことを, 単に**順序**ということがある.

$a \preceq b$, かつ $a \neq b$ のとき, 便宜上 $a \prec b$ と書く. $b \preceq a$ を $a \succeq b$ と書き, $b \prec a$ を $a \succ b$ と書くことがある.

例 2.6.2. 自然数の集合 $\mathbb{N}$, 整数の集合 $\mathbb{Z}$, 有理数の集合 $\mathbb{Q}$, 実数の集合 $\mathbb{R}$ はいずれも次の大小の順序 $\leq$ によって順序集合になる.

$$a \preceq b \quad \overset{\text{def}}{\iff} \quad a \leq b$$

自然数の順序について厳密な定義等は 6.2.4 節で説明する. 整数の順序については定義 6.3.10 以下で説明する. 整数について順序の知識を仮定すると有理数の順序を定義することができる (定義 3.3.6).

順序の記号は $\preceq$ の代りに 記号 $\leq$ を使うことも多いが, ここでは大小の順序と区別するため, 記号 $\preceq$ を使うことにする.

大小の順序でない順序構造も定めることができる.

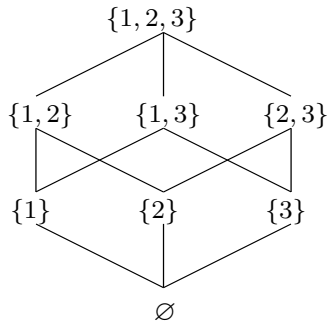
例 2.6.3. 自然数の集合 $\mathbb{N}$ は, 次により順序集合になる.

$$a \preceq b \quad \overset{\text{def}}{\iff} \quad b \text{ は } a \text{ の倍数.}$$

例 2.6.4. X を任意の集合とする. X の部分集合 A, B に対し,

$$A \preceq B \iff A \subset B$$

と定めれば $(2^X, \preceq)$ は順序集合となる. 例えば $X = \{1, 2, 3\}$ のとき, 順序関係を図示すれば次のようになる.



定義 2.6.5 (全順序集合). 任意の $a, b \in X$ に対し，$a \preceq b$ または $b \preceq a$ の少なくとも一方が成り立つとき $(X, \preceq)$ は**全順序集合** (totally ordered set) であるといいその順序 $\preceq$ を**全順序**という．全順序集合でない順序集合を**半順序集合** (partial ordered set) といいその順序 $\preceq$ を**半順序**という．

例 2.6.2 は全順序集合であるが，例 2.6.3, 例 2.6.4 は全順序集合でない．順序集合 $(X, \preceq)$ の部分集合 A も，同一の順序関係 $\preceq$ によって順序集合 $(A, \preceq)$ となる．

定義 2.6.6 (辞書式順序). $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ とする．$\mathbb{N}_0^n$ について，次で全順序を定義することができる．この順序を**辞書式順序** (lexicographic order) という．

$$(a_1, \dots, a_n) \prec_L (b_1, \dots, b_n) \quad \overset{\text{def}}{\iff} \quad \exists j \text{ s.t. } a_i = b_i \ (\forall i < j),\ a_j < b_j$$

$n = 2$ の辞書式順序は次のような全順序である．

$$\begin{aligned}
&(0,0) \prec (0,1) \prec (0,2) \prec (0,3) \prec (0,4) \prec \cdots \\
\prec &(1,0) \prec (1,1) \prec (1,2) \prec (1,3) \prec (1,4) \prec \cdots \\
\prec &(2,0) \prec (2,1) \prec (2,2) \prec (2,3) \prec (2,4) \prec \cdots \\
\prec &(3,0) \prec (3,1) \prec (3,2) \prec (3,3) \prec (3,4) \prec \cdots \\
\prec &(4,0) \prec (4,1) \prec (4,2) \prec (4,3) \prec (4,4) \prec \cdots \\
&\vdots
\end{aligned}$$

定義 2.6.7 (全次数-辞書式順序). $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ とする．$\mathbb{N}_0^n$ について，次で全順序を定義することができる．この順序を**全次数-辞書式順序** (total degree-lexicographic order) という．

$$(a_1, \dots, a_n) \prec (b_1, \dots, b_n) \quad \overset{\text{def}}{\iff}$$
$$\begin{cases} a_1 + \cdots + a_n < b_1 + \cdots + b_n & \text{または} \\ a_1 + \cdots + a_n = b_1 + \cdots + b_n, & (a_1, \dots, a_n) \prec_L (b_1, \dots, b_n) \end{cases}$$

$n = 2$ の全次数-辞書式順序は次のような全順序である.

$$\begin{aligned}(0,0) &\prec (0,1) \prec (1,0)\\ &\prec (0,2) \prec (1,1) \prec (2,0)\\ &\prec (0,3) \prec (1,2) \prec (2,1) \prec (3,0)\\ &\prec (0,4) \prec (1,3) \prec (2,2) \prec (3,1) \prec (4,0)\\ &\prec (0,5) \prec \cdots\end{aligned}$$

定義 2.6.8 (極大元，極小元). 順序集合 $(X, \preceq)$ の元 m が X の**極大元** (maximal element) であるとは,

$$m \preceq x, \quad m \neq x \quad \text{なる } X \text{ の元 } x \text{ が存在しない}$$

ときをいう.

順序集合 $(X, \preceq)$ の元 m が X の**極小元** (minimal element) であるとは,

$$m \succeq x, \quad m \neq x \quad \text{なる } X \text{ の元 } x \text{ が存在しない}$$

ときをいう.

定義 2.6.9 (最大元，最小元). 順序集合 $(X, \preceq)$ の元 m が X の**最大元** (maximum element) であるとは,

$$\text{すべての } x \in X \text{ に対し } x \preceq m$$

が成立するときをいう.

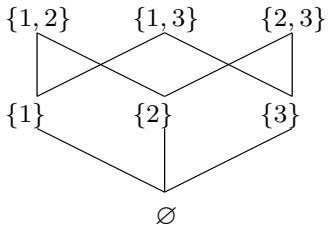
順序集合 $(X, \preceq)$ の元 m が X の**最小元** (minimum element) であるとは,

$$\text{すべての } x \in X \text{ に対し } x \succeq m$$

が成立するときをいう.

最大元は極大元であるが，逆は必ずしも真ではない．最小元についても同様である.

例 2.6.10. $A = \{1, 2, 3\}$ とし，
$X = 2^A - \{A\}$ に，例 2.6.3 のように包含関係で順序をいれる．X には極大元が 3 つあるが最大元はない.



定義 2.6.11 (上限, 下限). 順序集合 $(X, \leq)$ の部分集合 A に対し，集合

$$A^* = \{x \in X \mid \forall a \in A \ a \preceq x\}$$

に最小元が存在するときその最小元を A の**上限** (supremum) といい，$\sup A$ であらわす．A^* の元を集合 A の**上界** (upper bound) という．

同様にして集合

$$A_* = \{x \in X \mid \forall a \in A\ x \preceq a\}$$

に最大元が存在するときその最大元を A の**下限** (infimum) といい，$\inf A$ であらわす．A_* の元を集合 A の**下界** (lower bound) という．

例 2.6.12. 実数全体の集合 $\mathbb{R}$ は大小の順序で全順序集合になる．部分集合 $A = (0,1)$ には，最大元はないが，上限は存在しその値は 1 である．最小元もないが，下限は存在しその値は 0 である．

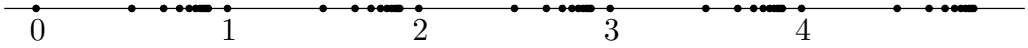
定義 2.6.13 (整列集合). 順序集合 $(X, \preceq)$ が**整列集合** (well ordered set) であるとは X の任意の空でない部分集合 A がかならず A の中に最小元をもつときをいう．

例 2.6.14. 自然数の集合 $\mathbb{N}$ は大小の順序に関して，整列集合になる．

例 2.6.15. 実数の集合 $\mathbb{R}$ は大小の順序に関しては，整列集合でない．

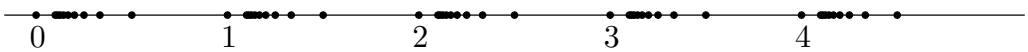
例 2.6.16. 次の集合は大小の順序に関しては，整列集合である．

$$\{m - \tfrac{1}{n} : m \text{ 正の整数}, n \text{ は } 2 \text{ 以上の整数 }\}$$



例 2.6.17. 次の集合は大小の順序に関しては，整列集合でない．

$$\{m + \tfrac{1}{n} : m \text{ 正の整数}, n \text{ は } 2 \text{ 以上の整数 }\}$$



Zorn の補題と選択公理 *

少し進んだ話題であるが Zorn の補題を紹介しておこう.

定義 2.6.18 (帰納的集合). 順序集合 $(X, \preceq)$ が**帰納的集合** (inductive set) であるとは X の空でない部分集合 A が X の順序に関して全順序集合であればかならず X の中に $\sup A$ が存在するときをいう.

定理 2.6.19. 次の命題は同値である.

(i) 任意の集合族 $\{A_\lambda \mid \lambda \in \Lambda\}$ に対し，すべての $\lambda \in \Lambda$ について $A_\lambda \neq \varnothing$ ならば $\prod_{\lambda\in\Lambda} A_\lambda \neq \varnothing$.

(ii) 任意の集合 X に対し，適当に順序関係を定義すれば, X を整列集合とすることができる.

(iii) 順序集合 $(X, \preceq)$ が帰納的であれば，X は少なくとも一つの極大元をもつ.

この定理の証明はここでは与えない．証明は集合論の教科書を見ていただきたい.

(i) は Zermelo[*4] により集合論の公理として要請されたもので**選択公理**という．(ii) は Cantor[*5] の**整列定理**，(iii) は **Zorn**[*6] **の補題**と呼ばれる.

実は、定理 2.4.1 (ii) の $\Longrightarrow$ を厳密に証明するには選択公理を仮定する必要がある．ここでその証明を与えておこう.

定理 2.6.20. $f : X \to Y$ が全射ならば，$f \circ g = 1_Y$ をみたす写像 $g : Y \to X$ が存在する.

証明. $f : X \to Y$ は全射だから，任意の $y \in Y$ に対し $A_y = f^{-1}(y)$ は空集合でない．したがって，$\{A_y \mid y \in Y\}$ は空でない集合からなる集合族である．ゆえに選択公理より，直積集合 $\prod_{y\in Y} A_y$ は空集合でなく，Y から X への写像 $g : Y \to X$ で $g(y) \in A_y$, $y \in Y$, をみたすものが存在する．(直積集合の定義を思い出すこと) この g に対して，$f \circ g = 1_Y$ となるのは示すのは容易. □

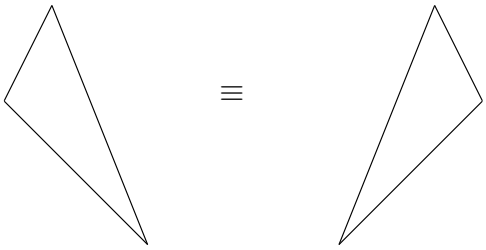
[*4] Ernst Friedrich Ferdinand Zermelo (1871–1953) はドイツの数学者・論理学者

[*5] Ferdinand Ludwig Philipp Cantor (1845–1918) は、ドイツで活躍した数学者

[*6] Max August Zorn (1906 – 1993) は、ドイツ生まれのアメリカ合衆国の数学者

第 3 章

同値関係



初等的な平面幾何学では回転や鏡映で移り合う図形を互いに合同であるといって合同かどうかの判定法や，合同な図形に共通な性質の探求がテーマであった．さらに拡大や縮小で移り合う図形は相似であるといって，相似かどうかの判定法や，相似な図形に共通な性質も考察した．

考察の２つの対象が同じである，あるいは等しいとはどういうことか図形の合同のもつ性質（等号の持つ性質といってもよい）を抽象化したものが同値関係である．この章では同値関係とクラス分けについてまとめ，いろんな例を紹介する．同値関係は数学のいろんな場面で現れるのがわかるであろう．

日本語	英語	(筆記体)
同値関係	equivalence relation	(equivalence relation)
フランス語	ドイツ語	ロシア語
relation d'équivalence	Äquivalenzrelation	отиошение èквивалентности

3.1 同値関係とクラス分け

考察するの 2 つの対象が同じである，あるいは等しいとはどういう事なのだろうか? ここでは等号の持つ性質，図形の合同のもつ性質を抽象化して同値関係を定義し，クラス分けについてまとめておく.

定義 3.1.1 (同値関係). 集合 X の元の間に関係 $\sim$ が定義されていて次の 3 つの性質が成立するとき，関係 $\sim$ は**同値関係** (equivalence relation) であるという:

(i) 反射律: 任意の $x \in X$ に対して $x \sim x$ である.
(ii) 対称律: 任意の $x, y \in X$ に対して $x \sim y \Longrightarrow y \sim x$ である.
(iii) 推移律: 任意の $x, y, z \in X$ に対して $x \sim y$, $y \sim z \Longrightarrow x \sim z$ である.

定義 3.1.2 (同値類). 集合 X に於ける同値関係 $\sim$ があるとき，元 x と同値な元すべてからなる集合 X の部分集合を $[x]$ で表し，**同値類** (equivalence class) という．すなわち,

$$[x] = \{a \in X \mid x \sim a\}.$$

注意 3.1.3. 反射律より $x \sim x$ であり $x \in [x]$ がわかる．反射律を使わないで $x \in [x]$ が結論できるだろうか? $x \sim y$ ならば対称律より $y \sim x$ であり、推移律より $x \sim x$ が結論できる．こう考えると，反射律は不要な仮定のように見える．しかし，x と同値な X の元 y が存在すればこの論法でよいが，そのような元 y の存在がわからない時は，この論法は適用できない．反射律を仮定しないと $x \in [x]$ も証明できないのである.

補題 3.1.4 (同値関係の基本性質). 集合 X に於ける同値関係 $\sim$ があるとき，次の命題は互いに同値である.

(i) $x \sim y$.
(ii) $[x] = [y]$.
(iii) $[x] \cap [y] \neq \varnothing$.

証明. (i)$\Longrightarrow$(ii): 同値類 $[x]$ の任意の元を a とすると $x \sim a$ である．仮定 $x \sim y$ と同値関係の対称律から $y \sim x$ である．同値関係の推移律により $y \sim a$ である．これは元 a が同値類 $[y]$ の元であることを示している．従って，$[x] \subset [y]$ となる．同様にして逆の包含関係 $[x] \supset [y]$ が示され $[x] = [y]$ がわかる.
(ii)$\Longrightarrow$(iii): $[x] \cap [y] = [x]$ であり，$x \in [x]$ であることから (iii) が示される.
(iii)$\Longrightarrow$(i): $a \in [x] \cap [y]$ とする．同値類の定義から $x \sim a$, $y \sim a$ である．対称律から $a \sim y$ となり．従って，推移律から $x \sim y$ がわかる. □

定義 3.1.5 (クラス分け). 集合 X がその部分集合の族 $\{A_\lambda \mid \lambda \in \Lambda\}$ にクラス分けされるとは次の 2 条件が成立することをいう.

(i) $X = \bigcup_{\lambda\in\Lambda} A_\lambda$
(ii) $A_\lambda = A_\mu$ または $A_\lambda \cap A_\mu = \varnothing$

定理 3.1.6 (クラス分けする). 集合 X 上に同値関係 $\sim$ があるということと，集合をクラス分けするということとは同値である．即ち，集合上に同値関係があればその集合は同値類にクラス分けされるし，逆に集合がクラス分けされていれば同じクラスに属する元同士を関係があると定義することでその集合上に同値関係が決まる.

定義 3.1.7 (商集合). 同値類 $[x]$ を，新たに元 (要素) と考えてできる集合をもとの集合 X の同値関係 $\sim$ による**商集合** (quotient) といい

$$X/\sim \;=\; \{[x] \mid x \in X\}$$

と書く.

定理 3.1.6 の証明. 集合 X に於ける同値関係 $\sim$ があるとき,
$X = \bigcup_{x\in X}[x]$ であり定義 3.1.5 の条件 (i) が成立する．補題 3.1.4 により，2 つの同値類は

$$[x] = [y] \quad \text{または} \quad [x] \cap [y] = \varnothing$$

であり定義 3.1.5 の条件 (ii) が成立する．これで集合がクラス分けされた．逆は各自確認する事. □

例 3.1.8. 整数の集合 $\mathbb{Z}$ に於いて，$n, m \in \mathbb{Z}$ に対して

$$n \sim m \Longleftrightarrow n - m \in 6\mathbb{Z} = \{6k \mid k \in \mathbb{Z}\}$$

と定義すると，これは同値関係である．商集合 $\mathbb{Z}/\sim$ の元の個数は 6 個となる.

$$\mathbb{Z}/\sim = \{[0], [1], [2], [3], [4], [5]\}.$$

演習 3.1.9 (同値関係?). (1) 整数の集合 $\mathbb{Z}$ に於いて，$n, m \in \mathbb{Z}$ に対して

$$n \sim m \Longleftrightarrow |n - m| \leq 6$$

と定義すると，これは同値関係ではない．反射・対称律は成立するが、推移律は成立しない.

(2) 整数の集合 $\mathbb{Z}$ に於いて，$n, m \in \mathbb{Z}$ に対して

$$n \sim m \Longleftrightarrow n \leq m$$

と定義すると，これは同値関係ではない．反射・推移律は成立するが，対称律は成立しない．

(3) 整数の集合 $\mathbb{Z}$ に於いて，$n, m \in \mathbb{Z}$ に対して

$$n \sim m \Longleftrightarrow n \neq m$$

と定義すると，これは同値関係ではない．反射律が成立しない．

集合の濃度 (基数)

同値関係の例として，個数の概念の一般化である，集合の濃度という概念を紹介する．

定義 3.1.10 (集合の対等，濃度 (cardinal number)). 一般に集合 A と B が**対等** (equivalent) であるとは A の元と B の元との間に一対一の対応がつけられること，すなわち，全単射 $f : A \to B$ が存在することをいう．集合の対等は同値関係になる．集合 A と B が対等であるとき $A \sim B$ (または $\#A = \#B$) と書く．$A \sim B$ のとき集合 A と集合 B は**同じ濃度** (equipotent) であるという．

集合 A の濃度の記号として，ここでは $\#A$ を用いたが $|A|$ を用いることもある．

演習 3.1.11. 対等であることは，同値関係であることを確認せよ．

ある自然数 n について

$$A \sim \{1, 2, \ldots, n\}$$

であるとき，**集合 A の濃度は n であるといい**，$\#A = n$ と書く．このような集合を**有限集合** (finite set) という．空でない集合 A が有限集合でないとき**無限集合** (infinite set) であるという．

集合 A が自然数の集合 $\mathbb{N}$ と対等，すなわち

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

であるとき，A の濃度は**可算** (countable) である，または A は**可算集合** (countable set) であるといい，$\#A = \aleph_0$ （アレフゼロ）と書く．なお $\aleph$ はヘブライ語の第 1 アルファベットでアレフと読む．

例 3.1.12. 例 2.4.8 より，自然数全体の集合 $\mathbb{N}$ と整数全体の集合 $\mathbb{Z}$ は対等である．例 2.4.9 より，自然数全体の集合 $\mathbb{N}$ と正の有理数全体の集合 $\mathbb{Q}_+$ は対等である．例 2.4.8 と同様にして，正の有理数全体の集合 $\mathbb{Q}_+$ と有理数全体の集合 $\mathbb{Q}$ は対等である事がわかる．

$$\aleph_0 = \#\mathbb{N} = \#\mathbb{Z} = \#\mathbb{Q}_+ = \#\mathbb{Q}.$$

例 3.1.13. 例 2.3.18 より，開区間 (a,b) と開区間 $(0,1)$ は対等である．これらは実数全体の集合 $\mathbb{R}$ と対等であることもわかる．例 2.4.11 より $(0,1)\times(0,1)$ と $(0,1)$ も対等であるから，$\mathbb{R}\times\mathbb{R}$ と $\mathbb{R}$ も（もちろん開区間 $(0,1)$ とも）対等である．この濃度を $\aleph$（アレフ）で表す．

$$\aleph = \#\mathbb{R} = \#(0,1) = \#(0,1)^2 = \#\mathbb{R}^2.$$

演習 3.1.14. $\mathbb{R}^3$ は $\mathbb{R}^2$ と対等である事を示せ．一般に自然数 n に対し $\mathbb{R}^n$ は $\mathbb{R}$ と対等である事を示せ．

例 3.1.15. 例 2.4.12 より $\mathbb{N}$ と $\mathbb{R}$ は対等でない．$\aleph_0 \neq \aleph$

$\mathbb{R}$ の濃度を $\aleph$ で表す．集合 A が有限集合であるか，または可算集合であるとき，A は**たかだか可算** (at most countable) であるという．

集合の濃度の理論は「素朴集合論」の中心となる話題である．濃度について成り立つ性質の解明は集合論の入門書に譲り，この話題にこれ以上深入りするのは，やめておこう．

順序数 (序数)*

2 つの整列集合 $(X,\preceq)$, $(Y,\preceq')$ を考える．次の条件を満たす全単射 $f: X\to Y$ が存在するとき，$(X,\preceq)$ と $(Y,\preceq')$ は**順序同型**であるという．

すべての $x, x'\in X$ について $x\preceq x'$ ならば $f(x)\preceq' f(x')$ が成り立つ．

順序同型は同値関係である．この同値関係による整列集合の同値類を，**順序数**[*1]という．

濃度は個数の概念を一般化したものと考えられるが、順序数は一列に物を並べると言う考え方を一般化して得られる数概念と考えられる．その立場から見ると、次の事実は自明であるが，注意しておく価値はあるだろう．

整列集合 $(X,\preceq)$ と $(Y,\preceq')$ が同じ順序数を定めれば，X と Y は同じ濃度である．

[*1] 公理的集合論の立場から述べれば $X\neq\varnothing$ のとき $(X,\preceq)$ と同型な整列集合の全体は集合でないことが示されている．従って、この順序数の定義の仕方は正当なものとは認められない．現代では整列集合 $(X,\preceq)$ に対し $G: X\to 2^X$ $a\mapsto G(a)=\{x\in X\mid x<a\}$ の値域を整列集合 $(X,\preceq)$ の順序数といい，ある整列集合の順序数であるような集合を順序数と呼ぶのが一般的である．

3.2 合同式

n を正の整数とする.

定義 3.2.1. 整数 x, y に対し，$x-y$ が 整数 n で割り切れるとき，整数 x, y は n を法として**合同** (congruent) であるといい

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

と書く．この式を n を法する**合同式** (congruence expression) という.

ここでひとつ記号を導入しておこう．整数 m, n に対し n が m を割り切るとき，すなわちある整数 k があって $m = kn$ と書けるとき, n は m を **整除する**といい,

$$n \mid m$$

とあらわす．定義より次が成り立つ.

$$x \equiv y \pmod{n} \iff n \mid x-y$$

定理 3.2.2. $x \equiv y \pmod{n}$ は同値関係である.

証明. $x \equiv y \pmod{n}$ を省略して $x \equiv y$ と書くことにする.

$x - x = 0 = 0 \cdot n$ より，反射律 $x \equiv x$ が成り立つ.

$x \equiv y$ とすると $x - y = kn$ をみたす整数 k が存在する．$y - x = (-k)n$ より $y \equiv x$ が成り立つ.

$x \equiv y$, $y \equiv z$ とすると, $x - y = k_1 n$, $y - z = k_2 n$ なる整数 k_1, k_2 が存在する．$x - z = (x-y) + (y-z) = k_1 n + k_2 n = (k_1 + k_2)n$ より $x \equiv z$ が成り立つ. □

n を法として合同であるというのは同値関係であるから整数全体の集合 $\mathbb{Z}$ をこれでクラス分けすることができる．その商集合を $\mathbb{Z}/n\mathbb{Z}$ または $\mathbb{Z}_n$ であらわす.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \mathbb{Z}/\equiv$$

x の同値類を $[x]_n$, または，単に $[x]$ とあらわすことにする.

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

以後しばしば $x \equiv y \pmod{n}$ を省略して $x \equiv y$ と書く．合同式について次の性質は重要である.

定理 3.2.3. $x \equiv x'$, $y \equiv y'$ ならば

(i) $x+y \equiv x'+y'$. (同値関係 $\equiv$ と加法の両立性)
(ii) $xy \equiv x'y'$. (同値関係 $\equiv$ と乗法の両立性)

証明. $x \equiv x'$ より $x-x'=kn$ なる整数 k が存在する．同様に $y \equiv y'$ より $y-y'=\ell n$ となるような整数 ℓ がある．

(i) $(x+y)-(x'+y')=(x-x')+(y-y')=kn+\ell n=(k+\ell)n$ より $x+y \equiv x'+y'$.
(ii) $xy-x'y'=(x-x')y+x'(y-y')=kny+x'\ell n=(ky+x'\ell)n$ より $xy \equiv x'y'$.

よって定理は証明された． □

この定理は商集合 $\mathbb{Z}/n\mathbb{Z}$ に対し，次で加法，乗法が定義できることを示している．

$$[x]_n+[y]_n := [x+y]_n \tag{1}$$
$$[x]_n \cdot [y]_n := [x\ y]_n \tag{2}$$

つまり，右辺は同値類 $[x]_n$, $[y]_n$ の代表元 x, y のとり方によらず同値類だけで定まる．なぜなら

$$\begin{aligned} & [x]_n=[x']_n, \quad [y]_n=[y']_n \\ \Longrightarrow\ & x \equiv x', \quad y \equiv y' \\ \Longrightarrow\ & x+y \equiv x'+y', \quad xy \equiv x'y' \quad (\text{定理 3.2.3 より}) \\ \Longrightarrow\ & [x+y]_n=[x'+y']_n, \quad [xy]_n=[x'y']_n \end{aligned}$$

となるからである．このとき加法・乗法の定義 (1), (2) は**うまく定義されている** (well-defined である) という．

例 3.2.4. $\mathbb{Z}/2\mathbb{Z}=\{[0]_2,[1]_2\}$ の加法，乗法の表をつくってみよう．

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\times$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

例 3.2.5. $\mathbb{Z}/3\mathbb{Z}=\{[0]_3,[1]_3,[2]_3\}$ の加法，乗法の表をつくってみよう．$[n]_3$ を 単に n と略記することにする．

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

例 3.2.6. $\mathbb{Z}/4\mathbb{Z}=\{[0]_4,[1]_4,[2]_4,[3]_4\}$ の加法，乗法の表をつくってみよう．ここでも $[n]_4$ を 単に n と略記することにする．

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

演習 3.2.7. $\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$ の加法，乗法の表を作れ．

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

$\times$	0	1	2	3	4
0					
1					
2					
3					
4					

演習 3.2.8. $\mathbb{Z}/6\mathbb{Z} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ の加法，乗法の表を作れ．

$+$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$\times$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

演習 3.2.9. $\mathbb{Z}/7\mathbb{Z} = \{[0], [1], [2], [3], [4], [5], [6]\}$ の加法，乗法の表を作れ．

$+$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

$\times$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

演習 3.2.10. $\mathbb{Z}/8\mathbb{Z} = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$ の加法，乗法の表を作れ．

$+$	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

$\times$	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

演習 3.2.11. $\mathbb{Z}/9\mathbb{Z}$ の乗法の表を作れ.

$\times$	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

演習 3.2.12. 上の乗法の表を見て，$n = 2, 3, \ldots, 9$ のとき，次の集合はどうなるか調べよ.

$$\{[a^k] \mid k = 1, 2, 3, \ldots\}$$

ただし a は $1 \leq a < n$ なる整数である.

3.3 有理数をつくる

整数全体の集合

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

と，その部分集合である自然数全体の集合

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

から，有理数を理論的に構成するのがここでの目的である．基本となるのは次の諸性質である．任意の整数 a, b に対して，その和 $a+b$, その積 ab が定義されていて，次の性質をみたす．

(i) 加法に関する交換律: $a + b = b + a$.
(ii) 加法に関する結合律: $(a + b) + c = a + (b + c)$.
(iii) 乗法に関する交換律: $ab = ba$.
(iv) 乗法に関する結合律: $a(bc) = (ab)c$.
(v) 分配律: $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

定義 3.3.1. 整数 p と自然数 q との順序対 (p, q) 全体の集合 $\mathbb{Z} \times \mathbb{N}$ を考える．$\mathbb{Z} \times \mathbb{N}$ に次で関係 $\sim$ を定義するとこれは同値関係になる．

$$(p, q) \sim (p', q') \quad \overset{\text{def}}{\iff} \quad pq' - p'q = 0$$

この同値関係 $\sim$ による，(p, q) の同値類を $[(p, q)]$ または p/q と書き，この同値関係 $\sim$ による，$\mathbb{Z} \times \mathbb{N}$ の商集合を $\mathbb{Q}$ と書く．

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{N}/\sim$$

$\sim$ が同値関係になることを示しておこう．推移律だけ示す．$(p_1, q_1) \sim (p_2, q_2), (p_2, q_2) \sim (p_3, q_3)$ より，$p_1q_2 - p_2q_1 = 0$, かつ $p_2q_3 - p_3q_2 = 0$ である．ところで

$$q_2(p_1q_3 - p_3q_1) = q_3(p_1q_2 - p_2q_1) + q_1(p_2q_3 - p_3q_2) = 0$$

が成り立つので，$q_2 \neq 0$ より，$p_1q_3 - p_3q_1 = 0$ でなければならず，$(p_1, q_1) \sim (p_3, q_3)$ が示された．

演習 3.3.2. $\sim$ が反射律と対称律をみたすことを確認せよ．

定義 3.3.3. $\mathbb{Q}$ の加法と乗法を次で定義する．

$$[(p, q)] + [(p', q')] := (pq' + p'q, qq')$$
$$[(p, q)] \cdot [(p', q')] := (pp', qq')$$

これがうまく定義されている (well-defined である) ことを証明しよう．すなわち代表元のとり方によらず，同値類で加法，乗法が確定していること，すなわち $(p_1, q_1) \sim (p_2, q_2)$, $(p_1', q_1') \sim (p_2', q_2')$ ならば

$$(p_1q_1' + p_1'q_1, q_1q_1') \sim (p_2q_2' + p_2'q_2, q_2q_2')$$
$$(p_1p_1', q_1q_1') \sim (p_2p_2', q_2q_2')$$

であることを示せばよい．

$(p_1, q_1) \sim (p_2, q_2)$, $(p_1', q_1') \sim (p_2', q_2')$ なので $p_1q_2 - p_2q_1 = p_1'q_2' - p_2'q_1' = 0$ である．

$$\begin{aligned}&(p_1q_1' + p_1'q_1)(q_2q_2') - (p_2q_2' + p_2'q_2)(q_1q_1')\\ &= (p_1q_2 - p_2q_1)q_1'q_2' + (p_1'q_2' - p_2'q_1')q_1q_2 = 0\end{aligned}$$

より $(p_1q_1' + p_1'q_1, q_1q_1') \sim (p_2q_2' + p_2'q_2, q_2q_2')$ がわかり，

$$(p_1p_1')(q_2q_2') - (p_2p_2')(q_1q_1') = (p_1q_2 - p_2q_1)p_1'q_2' + (p_1'q_2' - p_2'q_1')p_2q_1 = 0$$

より $(p_1p_1', q_1q_1') \sim (p_2p_2', q_2q_2')$ がわかる．

上述の加法, 乗法の定義は，小学校以来慣れ親しんでいる分数の計算

$$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}, \quad \frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$$

を書き直したものであることに気づいたであろうか?

以後 (p, q) の同値類を p/q であらわすことにする．

定理 3.3.4. $\mathbb{Q}$ の元 $a = p_1/q_1$, $b = p_2/q_2$, $c = p_3/q_3$ に対し, 次が成り立つ．

(i) 加法に関する交換律: $a + b = b + a$.
(ii) 加法に関する結合律: $(a + b) + c = a + (b + c)$.
(iii) 乗法に関する交換律: $ab = ba$.
(iv) 乗法に関する結合律: $a(bc) = (ab)c$.
(v) 分配律: $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

証明. これらは (書き下すのは面倒かもしれないが，証明は) 易しい．例えば 加法に関する交換律は次のように証明できる．

$$p_1/q_1 + p_2/q_2 = (p_1q_2 + p_2q_1)/(q_1q_2) = p_2/q_2 + p_1/q_1.$$

□

演習 3.3.5. 定理 3.3.4 の (ii)–(v) を証明せよ．

定義 3.3.6 (有理数の順序). 2 つの有理数 $p_1/q_1, p_2/q_2$ に対し $p_1/q_1 \leq p_2/q_2$ を次で定義する.

$$p_1/q_1 \leq p_2/q_2 \iff^{\text{def}} p_1q_2 \leq p_2q_1$$

演習 3.3.7. 順序がうまく定義されていること，すなわち $(p_1, q_1) \sim (p_1', q_1')$, $(p_2, q_2) \sim (p_2', q_2')$ のとき

$$p_1q_2 \leq p_2q_1 \iff p_1'q_2' \leq p_2'q_1'$$

をしめせ.

演習 3.3.8. これにより $\mathbb{Q}$ は順序集合になることを示せ.

定理 3.3.9 ($\mathbb{Z}$ の $\mathbb{Q}$ への埋め込み). 写像 $f : \mathbb{Z} \to \mathbb{Q}$ を $p \mapsto p/1$ で定義する．f は単射で

(i) $f(p) + f(p') = f(p + p')$,
(ii) $f(p)f(p') = f(pp')$.
(iii) $p \leq p'$ ならば $f(p) \leq f(p')$.

整数 p に対し $p/1$ と p を同一視し，$p/1$ をしばしば p と書く.

定理 3.3.10 (零元). $O = 0/1$ とおくと次が成立．$a + O = a$, $a \cdot O = O$

以後，しばしば，有理数の零元 O と整数の 0 を区別しないで 0 で表す.

定理 3.3.11 (反数). $\mathbb{Q}$ の任意の元 $a = p/q$ に対し，$a + a' = a' + a = 0$ をみたす $\mathbb{Q}$ の元 a' が唯一つ存在する．$a' = (-p)/q$ である．a' を a の反数といい $-a$ であらわす.

定義 3.3.12 (差). $\mathbb{Q}$ の元 a,b に対し，その**差**を次で定義する.

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

演習 3.3.13. $a = p_1/q_1$, $b = p_2/q_2$ と書くとき，次を示せ.

$$a - b = (p_1q_2 - p_2q_1)/(q_1q_2)$$

さらに $a - b$ がうまく定義されていることを示せ.

定理 3.3.14 (単位元). $1 = 1/1$ とおくとすべての $\mathbb{Q}$ の元 a に対し，$a \cdot 1 = 1 \cdot a = a$.

定理 3.3.15 (逆数). 0 とは異なる $\mathbb{Q}$ の任意の元 $a = p/q$ に対し，$aa' = a'a = 1$ をみたす $\mathbb{Q}$ の 元 a' が唯一つ存在する．$a' = q/p$ である．a' を a の逆数といい $1/a$ であらわす.

定義 3.3.16 (商). $\mathbb{Q}$ の元 a,b に対し，$b \neq 0$ のとき，その**商** $\frac{a}{b}$ を次で定義する．

$$\frac{a}{b} := a(1/b)$$

演習 3.3.17. $a = p_1/q_1$, $b = p_2/q_2$ と書くとき，次を示せ．

$$\frac{a}{b} = (p_1 q_2)/(q_1 p_2)$$

さらに $\frac{a}{b}$ がうまく定義されていることを示せ．

これで $\mathbb{Q}$ に加法，乗法，減法，0 でない数による除法が定義できたことになる．

定理 3.3.18. 有理数 a, b, c に対し，次が成り立つ．

(i) $a < b$ ならば $a + c < b + c$.
(ii) $a > 0$, $b > 0$ ならば $ab > 0$.
(iii) $a < b$, $c > 0$ ならば $ac < bc$.

演習 3.3.19. 定理 3.3.18 を証明せよ．

注意 3.3.20. $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ とおいて，集合 $\mathbb{Z} \times \mathbb{Z}^*$ に次で同値関係をいれる．

$$(p_1, q_1) \sim (p_2, q_2) \overset{\text{def}}{\iff} p_1 q_2 - p_2 q_1 = 0$$

集合 $\mathbb{Z} \times \mathbb{Z}^*$ のこの同値関係による商集合を考えても同様にして有理数が構成できる．ただしこの場合は必ずしも分母にあたるものが正でないので，順序を定義するときは注意しなければならない．

第 4 章

初等整数論から

エラストテネスのふるい[*1]

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

整数の問題は誰でも理解できて，初学者が考えやすい問題が多い．初等整数論の知識があれば簡単に解けてしまうものもあるし，一見易しそうに見えて実は手ごわい「フェルマーの最終定理」のようなものもある．整数の問題はその難易を見掛けで判断するのは難しい．

ここではかつては高校のカリキュラムに入っていた，最大公約数を求めるアルゴリズム，「ユークリッドの互除法」の周辺の話題をまとめた．

日本語	英語 (筆記体)	フランス語
数論	number theory (*number theory*)	théorie des nombres

ドイツ語	ロシア語
Zahlentheorie	теория чисел

[*1] まずこの表から，1 を消す．次に 2 以外の 2 の倍数を消す．さらに 3 以外の 3 の倍数を消し，続いて 5 以外の 5 の倍数を消す．このようにして，表に残った最小数の倍数を，順次，表から消していくと素数だけが残る．

4.1 互除法

定理 4.1.1 (余りのある割算). 任意の整数 $a, b > 0$ に対して

$$a = bq + r, \quad 0 \leq r < b$$

となる整数 q, r が唯一つ存在する.

証明. まず定理の条件を満たす q, r の存在を証明しよう．まず $a \geq 0$ として仮定する.

$$B = \{bn \mid bn > a \geq 0,\ n \in \mathbb{N}\}$$

とおくと，これは $\mathbb{N}$ の部分集合で空集合でない（$b(a+1) > a$ より $b(a+1) \in B$）ので最小数がある．それを $b(q+1)$ と書くと，最小性より

$$bq \leq a < b(q+1)$$

が成り立つ．$r = a - bq$ とおけば $0 \leq a - bq = r < b$ である．$a < 0$ のときは $-a > 0$ より

$$-a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

なる整数 q_1, r_1 があるが,

$$a = -bq_1 - r_1 = b(-q_1 - 1) + (b - r_1)$$

なので $q = -q_1 - 1, r = b - r_1$ とおけばよい.
一意性の証明：$a = bq_1 + r_1 = bq_2 + r_2, 0 \leq r_1, r_2 < b$ とすると

$$b(q_1 - q_2) = r_2 - r_1$$

となる．$-b < r_2 - r_1 < b$ かつ $b > 0$ なのでこれは零でなければならず $r_2 - r_1 = 0$. よって $q_1 - q_2 = 0$ も得る. □

整数 a, b に対し，$a = bc$ となる整数 c が存在するとき，a は b の**倍数** (multiple) である，または b は a の**約数** (divisor) であるという．b は a の**因数** (factor)，b は a を**割り切る**，ということもある．このとき次の記号で表す.

$$b \mid a$$

補題 4.1.2. (i) $a \mid b$ かつ $b \mid c$ ならば $a \mid c$.
(ii) $a \mid b$ かつ $b \mid a$ ならば $a = \pm b$.

整数 $a_1, \ldots, a_n$ が与えられたとき，すべての a_i の共通の倍数になる整数を $a_1, \ldots, a_n$ の**公倍数** (common multiples) といい，公倍数の中の最小の非負整数を**最小公倍数** (the least common multiple) という．$a_1, \ldots, a_n$ の最小公倍数を $\mathrm{LCM}(a_1, \ldots, a_n)$ で表す．

また，すべての a_i の共通の約数になる整数を $a_1, \ldots, a_n$ の**公約数** (common divisors) といい，公約数の中の最小の非負整数を**最大公約数** (the greatest common divisor) という．$a_1, \ldots, a_n$ の最小公倍数を $\mathrm{GCD}(a_1, \ldots, a_n)$ で表す．

補題 4.1.3. $a_1, \ldots, a_n$ を 0 でない整数とする．

(i) $a_1, \ldots, a_n$ の任意の公倍数は最小公倍数の倍数である．
(ii) $a_1, \ldots, a_n$ の任意の公約数は最大公約数の約数である．

証明. (i) $l = \mathrm{LCM}(a_1, \ldots, a_n)$ とおき l' を任意の公倍数とする．余りのある割算をすれば $l' = lq + r$, $0 \leq r < l$, と書ける．ここで $r = 0$ を示せばよい．各 i に対し $a_i \mid l$, $a_i \mid l'$ より $a_i \mid r$. よって $r \neq 0$ とすると l の最小性に反するので $r = 0$ でなければならない．
(ii) $d = \mathrm{GCD}(a_1, \ldots, a_n)$ とおき d' を任意の公約数とする．d と d' の最小公倍数を l とすると $d \mid a_i$, $d' \mid a_i$ より (i) を使って $l \mid a_i$. よって l は $a_1, \ldots, a_n$ の約数なので d の最大性より $l \geq d$. 一方 l は d の倍数だから $d \geq l$. よって $d = l$. l は d' の倍数でもあったから $d' \mid d$. □

補題 4.1.4. 整数 a, b, q, $b \neq 0$, に対し，$\mathrm{GCD}(a, b) = \mathrm{GCD}(a - qb, b)$.

証明. $d = \mathrm{GCD}(a, b)$, $d' = \mathrm{GCD}(a - qb, b)$ とおく．
a, b は d の倍数だから $a - qb$ も d の倍数で $d \mid d'$.
$a - qb, b$ は d' の倍数だから $a = (a - qb) + qb$ も d' の倍数で $d' \mid d$.
よって $d = d'$. □

この補題を利用した**ユークリッドの互除法**と呼ばれる最大公約数を求めるアルゴリズムを説明する．正の整数 a, b に対し，

$$\begin{array}{lcll} a & = & q_0 b + r_0 & 0 \leq r_1 < b \\ b & = & q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\ & & \cdots & \\ r_{k-1} & = & q_k r_k + r_{k+1} & 0 \leq r_k < r_{k-1} \\ & & \cdots & \end{array}$$

のように順に余りのある割算を繰り返すと，$b > r_1 > r_2 > \cdots \geq 0$ なので，この操作は

有限回で終了し $r_{n-1} = q_n r_n$ なる n が存在する．このとき前補題より

$$\mathrm{GCD}(a,b) = \mathrm{GCD}(b,r_1) = \mathrm{GCD}(r_1,r_2) = \cdots = \mathrm{GCD}(r_{n-1},r_n) = r_n$$

となる．

例 4.1.5. 7803 と 6273 の最大公約数を求めてみる．

$$\begin{aligned} 7803 =& 1 \times 6273 + 1530 \\ 6273 =& 4 \times 1530 + 153 \\ 1530 =& 10 \times 153 \end{aligned}$$

よって 153 が最大公約数である．

例 4.1.6. 637 と 507 の最大公約数を求めてみる

$$\begin{aligned} 637 =& 1 \times 507 + 130 \\ 507 =& 3 \times 130 + 117 \\ 130 =& 1 \times 117 + 13 \\ 117 =& 9 \times 13 \end{aligned}$$

よって 13 が最大公約数である．

演習 4.1.7. 2567 と 7652 の最大公約数を求めよ．

定理 4.1.8. a, b を整数とし

$$A = \{ax + by \mid x, y \in \mathbb{Z}\}$$

とおくと，A は a, b の最大公約数 d の倍数全体の集合と一致する．

証明. A に含まれる最小の自然数を d_0 とする．$c \in A$ を任意に取ると $c = d_0 q + r$, $0 \leq r < d_0$ なる整数 q, r が存在するが，$r \in A$ なので d_0 の最小性より $r = 0$ である．よって A は d_0 の倍数全体の集合である．したがって $d = d_0$ を示せばよい．

さて $a, b \in A$ なので a, b は d_0 の倍数である．よって d_0 は a, b の公約数であり，d の最大性より $d_0 \leq d$.

d は a, b の公約数だから $a = a_1 d$, $b = b_1 d$ となる整数 a_1, b_1 が存在する．$d_0 = ax + by$ なる整数 x, y をとると $d_0 = ax + by = a_1 dx + b_1 dy = (a_1 x + b_1 y)d$ は d の倍数なので $d = d_0$ がわかる． □

この定理より，整数 a, b, c に対し，次がわかる．

$$\text{方程式 } ax + by = c \text{ が整数解 } x, y \text{ をもつ} \iff \mathrm{GCD}(a,b) \mid c$$

演習 4.1.9. $32x + 57y = 1$ の整数解をすべて求めよ.

演習 4.1.10. 定理 4.1.8 の証明を真似して次を示せ：$a_1, \ldots, a_n$ を整数とし

$$A = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{Z}\}$$

とおくと，A は $a_1, \ldots, a_n$ の最大公約数 d の倍数全体の集合と一致する.

演習 4.1.10 より，整数 $a_1, \ldots, a_n, b$ に対し，次の条件は同値であることがわかる.

(i) 方程式 $a_1x_1 + \cdots + a_nx_n = b$ が整数解 $x_1, \ldots, x_n$ をもつ.
(ii) $\mathrm{GCD}(a_1, \ldots, a_n) \mid b$

演習 4.1.11. $6x + 10y + 15z = 1$ を満たす整数 x, y, z を少なくとも一つ求めよ.

$\mathrm{GCD}(a, b) = 1$ のとき a と b は**互いに素** (coprime) であるという.

補題 4.1.12. a, b が互いに素であるとき，$a \mid bc$ ならば $a \mid c$.

証明. a, b が互いに素なので $\mathrm{GCD}(a, b) = 1$, 定理 4.1.8 より $ax + by = 1$ なる $x, y \in \mathbb{Z}$ が存在する.

$$c = 1c = (ax + by)c = acx + bcy,$$

で $a \mid bc$ より $a \mid c$. □

補題 4.1.13. a, b が互いに素であるとき，$a \mid c$, $b \mid c$ であれば $ab \mid c$.

証明. a, b が互いに素なので，定理 4.1.8 より $ax + by = 1$ なる $x, y \in \mathbb{Z}$ が存在する．また仮定より $c = aa_1 = bb_1$ なる $a_1, b_1 \in \mathbb{Z}$ が存在する．よって

$$c = 1c = (ax + by)c = axc + byc = ab(b_1x + a_1y)$$

なので $ab \mid c$ である. □

4.2 素因数分解

正の整数 p が $\pm 1, \pm p$ 以外に約数を持たないとき**素数** (prime number) であるという．素数でない正の整数を**合成数** (composite number) と言う．

補題 4.2.1. 素数 p と整数 a, b に対し，$p \mid ab$ ならば $p \mid a$ または $p \mid b$.

証明. a と p の最大公約数は p の約数なので p または 1 である．
$\mathrm{GCD}(a,p) = p$ ならば $p \mid a$.
$\mathrm{GCD}(a,p) = 1$ ならば 補題 4.1.12 より $p \mid ab$ ならば $p \mid b$. □

演習 4.2.2. 素数 p と整数 $a_1, \ldots, a_n$ に対し，$p \mid a_1 \ldots a_n$ ならばある番号 i に対し $p \mid a_i$ であることを示せ.

定理 4.2.3 (素因数分解). 任意の正の整数 a は素数の積に唯一通りに分解される．ここで唯一通りというのは a が 2 通りの素数の積

$$a = p_1 \cdots p_k = q_1 \cdots q_l$$

に書けたとすると $k = l$ で適当に番号をつけ直せば $p_1 = q_1, \ldots, p_k = q_k$ となることである.

証明. まず a が素数の積に分解することを a に関する数学的帰納法で示す．$a = 2$ のときは a は素数で $k = 1, p_1 = 2$ とおけば確かに成り立つ．一般の a に対しては，もし a が素数なら $k = 1, p_1 = a$ とおけばよい．a が素数でなければ $a = a_1 a_2, 1 < a_1 < a, 1 < a_2 < a$ と書け，帰納法の仮定より a_1, a_2 は素数の積で書けるので a も素数の積で書ける.

一意性の証明をしよう．a が 2 通りの素数の積 $a = p_1 \cdots p_k = q_1 \cdots q_l$ に書けたとする．$k \leq l$ と仮定して良い．このとき $p_1 \mid q_1 \cdots q_l$ だからこのとき補題 4.2.1 より，ある q_j があって，$p_1 \mid q_j$ となる．p_1, q_j 共に素数だから $p_1 = q_j$. 番号をつけ直して $p_1 = q_1$ として一般性を失わない．このとき

$$p_2 \cdots p_k = q_2 \cdots q_l$$

が成立する．この操作を k 回続ければ，素因数分解の一意性を証明できた．($k < l$ ならば 1 が 2 以上の素数の積となり不合理．) □

素因数分解の表示において，同じ素数はまとめて冪の形に書くことにすれば

$$a = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}, \quad p_2 < p_3 < \cdots < p_k$$

の形に表される．

p, q を素数とし $a = p^4q^3$ とおく．a の約数は次の形に書ける．

$$\begin{array}{lllll} 1 & p & p^2 & p^3 & p^4 \\ q & pq & p^2q & p^3q & p^4q \\ q^2 & pq^2 & p^2q^2 & p^3q^2 & p^4q^2 \\ q^3 & pq^3 & p^2q^3 & p^3q^3 & p^4q^3 \end{array}$$

これをみると a の約数は全部で $5 \times 4 = 20$ 個あることがわかる．また a の約数すべての和は

$$\begin{array}{lllllllll} & 1 & + & p & + & p^2 & + & p^3 & + & p^4 \\ + & q & + & pq & + & p^2q & + & p^3q & + & p^4q \\ + & q^2 & + & pq^2 & + & p^2q^2 & + & p^3q^2 & + & p^4q^2 \\ + & q^3 & + & pq^3 & + & p^2q^3 & + & p^3q^3 & + & p^4q^3 \end{array}$$

$$= (1 + p + p^2 + p^3 + p^4)(1 + q + q^2 + q^3)$$

$$= \frac{p^5 - 1}{p - 1}\,\frac{q^4 - 1}{q - 1}$$

である．以上の考察を一般化して次の定理を得る．

定理 4.2.4. 2 以上の整数 $a = {p_1}^{e_1}\cdots{p_k}^{e_k}$ について次が成り立つ．

(i) a の約数の個数は (1 と a を含めて) $(1 + e_1)\cdots(1 + e_k)$ 個．

(ii) a の正の約数の総和は

$$\frac{{p_1}^{e_1+1} - 1}{p_1 - 1}\,\frac{{p_2}^{e_2+1} - 1}{p_2 - 1}\cdots\frac{{p_k}^{e_k+1} - 1}{p_k - 1}.$$

演習 4.2.5. 定理 4.2.4 を証明せよ．

定理 4.2.6. a, b を 2 以上の整数とし，その素因数分解を

$$a = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}, \quad b = {p_1}^{f_1}{p_2}^{f_2}\cdots{p_k}^{f_k}$$

と書いたとき (p_i の冪に 0 も許せばこのような書き方が許されることに注意)

$$\begin{array}{ll} \mathrm{GCD}(a,b) & = {p_1}^{d_1}{p_2}^{d_2}\cdots{p_k}^{d_k} \qquad d_i = \min\{e_i, f_i\} \\ \mathrm{LCM}(a,b) & = {p_1}^{l_1}{p_2}^{l_2}\cdots{p_k}^{l_k} \qquad l_i = \max\{e_i, f_i\} \end{array}$$

である．

演習 4.2.7. この定理を証明せよ．

次の定理は古代ギリシャのユークリッド (Euclid) の『原論』(紀元前 3 世紀?) に述べられている.

定理 4.2.8. 素数は無限に存在する.

証明. 素数は有限個しかないとしてそれらを $p_1, \ldots, p_n$ とする. このとき

$$p = p_1 p_2 \ldots p_n + 1$$

とおくと, これは $p_1, \ldots, p_n$ のいずれでも割り切れない. よって p は $p_1, \ldots, p_n$ のいずれとも異なるので p は素数でなく合成数でなければならない. よって p は $p_1, \ldots, p_n$ のいくつかの積で書けることになり矛盾. □

中国剰余定理

古代 (1 世紀頃) の中国の書『孫子算経』の中に

3 で割れば 2 余り, 5 で割れば 3 余り, 7 で割れば 2 余る数は何か?

という問とその解の求め方が述べられているという. これは, 現代数学の言葉で言い替えれば, 次の連立合同式を解くことと同じである.

$$\begin{cases} x & \equiv 2 \pmod 3 \\ x & \equiv 3 \pmod 5 \\ x & \equiv 2 \pmod 7 \end{cases}$$

この問題を目の子で解くには次のようにする. もし x_0 が連立合同式の解ならば, x_0 に $3, 5, 7$ の最小公倍数 105 を加えた $x_0 + 105$ も解である. したがって 1 から 105 まで, 順にこの合同式を満たすかどうか確かめていけば, 解を見つけることはできる筈である.

次の定理は, この問題に由来して, 中国剰余定理, または孫子の定理とよばれる.

定理 4.2.9 (中国剰余定理 (Chinese remainder theorem)). $m_1, \ldots, m_r$ を 2 つずつ互いに素であるような自然数とするとき, 次の連立合同式の解は $n = m_1 \cdots m_r$ を法として唯一つ存在する.

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ & \cdots \\ x & \equiv a_r \pmod{m_r} \end{cases}$$

証明. $M_i = n/m_i = m_1 \cdots \widehat{m_i} \cdots m_n$ とおけば, m_i と m_j $(j \neq i)$ は共通因子をもたな

いので次を満たす x_i と y_i が存在する．

$$m_i x_i + M_i y_i = 1$$

これより $m_i \mid M_i y_i - 1$ であり，$m_j \mid M_i$ $(j \neq i)$ なので，

$$\begin{cases} M_i y_i & \equiv 1 \pmod{m_i} \\ M_i y_i & \equiv 0 \pmod{m_j} \qquad (j \neq i) \end{cases}$$

となる．そこで

$$a = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

とおけばこれは求める連立合同式の解になる．

x を連立合同式の任意の解とすると $x \equiv a \pmod{m_i}$ なので $m_i \mid x - a$. 補題 4.1.13 より，$M \mid x - a$ を得る．逆に $x \equiv a \pmod{M}$ ならば $x \equiv a \equiv a_i \pmod{m_i}$ なので，x は連立合同式の解である． □

演習 4.2.10. $n, m_1, \ldots, m_r$ は前と同じとする．中国剰余定理を用いて写像

$$\begin{array}{rcl} f : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z}) \\ [a]_n & \mapsto & ([a]_{m_1}, \ldots, [a]_{m_r}) \end{array}$$

が全単射であることを示せ．（ヒント：全射を示すのに中国剰余定理を用いる．単射を示すには定理 2.4.4 を用いる．）

例 4.2.11. 中国剰余定理の証明より，連立合同式の解の求め方もわかる．先程の『孫子算経』の問題の問題を解いてみよう．$m_1 = 3$, $m_2 = 5$, $m_3 = 7$ とおくと，$M_1 = 35$, $M_2 = 21$, $M_3 = 15$ である．そこで

$$m_i x_i + M_i y_i = 1, \quad i = 1, 2, 3$$

をみたす x_i, y_i を求めたい．これは，例えば次が解である．

$$3 \cdot 13 + 35 \cdot (-1) = 1, \quad 5 \cdot (-4) + 21 \cdot (1) = 1, \quad 7 \cdot (-2) + 15 \cdot 1 = 1$$

よって $x = -35a_1 + 21a_2 + 15a_3$ に $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ を代入して，解 $x = 23$ を得る．

演習 4.2.12. $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$, $x \equiv 2 \pmod{16}$ を満たす x を求めよ．

4.3 $\mathbb{Z}/n\mathbb{Z}$ と $(\mathbb{Z}/n\mathbb{Z})^*$

第 3.2 節では $\mathbb{Z}/n\mathbb{Z}$ の表を $n \leq 8$ のとき作った．第 5.1, 5.2 節で定義する言葉を用いると，$\mathbb{Z}/n\mathbb{Z}$ は加法に関して可換群であり，加法と乗法に関して $\mathbb{Z}/n\mathbb{Z}$ は可換環であるといえる．ここでは，これらの構造をもう少し調べてみる．

演習 4.3.1. $\mathbb{Z}/10\mathbb{Z}$ の乗法の表を作れ．

×	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3										
4										
5										
6										
7										
8										
9										

演習 4.3.2. $\mathbb{Z}/11\mathbb{Z}$ の乗法の表を作れ．

×	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

演習 4.3.3. $\mathbb{Z}/12\mathbb{Z}$ の乗法の表を作れ．

×	0	1	2	3	4	5	6	7	8	9	10	11
0												
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												

演習 4.3.4. $\mathbb{Z}/13\mathbb{Z}$ の乗法の表を作れ.

×	0	1	2	3	4	5	6	7	8	9	10	11	12
0													
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													

演習 4.3.5. $n = 9, 10, 11, 12, 13$, $a = 1, 2, \ldots, n-1$ のとき，次の集合はどうなるか調べよ.

$$\{[a^k] \mid k = 1, 2, \ldots\}$$

$\mathbb{Z}/n\mathbb{Z}$ の乗法に関する可逆元全体の集合を $(\mathbb{Z}/n\mathbb{Z})^*$ であらわす．少し理論的な考察を

してみよう.

定理 4.3.6. $(\mathbb{Z}/n\mathbb{Z})^*$ は乗法に関して群になる.

証明. $(\mathbb{Z}/n\mathbb{Z})^*$ は乗法に関して閉じていることを示せばよい. $[p],[q] \in (\mathbb{Z}/n\mathbb{Z})^*$ とすると, $[s],[t] \in \mathbb{Z}/n\mathbb{Z}$ で $[ps]=[1]$, $[qt]=1$ なるものが存在する. よって $[pq][st]=[psqt]=[ps][qt]=[1][1]=[1]$ なので $[pq]$ も可逆元である. □

演習 4.3.7. $n=9,10,11,12$ のとき $(\mathbb{Z}/n\mathbb{Z})^*$ のリストを作れ.

定理 4.3.8. $(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \mid \mathrm{GCD}(a,n)=1\}$.

証明. $a \in \mathbb{Z}$ に対し次が成り立つのを確認すればよい.

$$\begin{aligned}
[a] \in (\mathbb{Z}/n\mathbb{Z})^* &\iff \exists b \in \mathbb{Z} \quad [ab]=[1] \\
&\iff \exists b,c \in \mathbb{Z} \quad ab-1=nc \\
&\iff \exists b,c \in \mathbb{Z} \quad ab+n(-c)=1 \\
&\iff \mathrm{GCD}(a,b)=1
\end{aligned}$$

最後の部分で定理 4.1.8 を用いている. □

系 4.3.9. $n=p^e$ を素数の冪とすると

$$(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} - \{[pb] \mid b=1,2,\ldots,p^{e-1}\}.$$

$n = {p_1}^{e_1}\ldots{p_r}^{e_r}$ と素因数分解しておく. 写像

$$\begin{array}{rcl}
f : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (\mathbb{Z}/{p_1}^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/{p_r}^{e_r}\mathbb{Z}) \\
[a]_n & \mapsto & ([a]_{{p_1}^{e_1}}, \ldots, [a]_{{p_r}^{e_r}})
\end{array}$$

は環としての準同型[*2]であるが, 演習 4.2.10 より, これは全単射である. $a \in \mathbb{Z}/n\mathbb{Z}$ に対し $f(a)=(a_1,\ldots,a_r)$ と書くと

$$\begin{aligned}
a \in (\mathbb{Z}/n\mathbb{Z})^* &\iff a^{-1}=({a_1}^{-1},\ldots,{a_r}^{-1}) \text{ が存在する} \\
&\iff \text{すべての } i \text{ に対し } {a_i}^{-1} \text{ が存在する} \\
&\iff \text{すべての } i \text{ に対し } a_i \in (\mathbb{Z}/{p_i}^{e_i}\mathbb{Z})^*
\end{aligned}$$

となるので $f((\mathbb{Z}/n\mathbb{Z})^*) = (\mathbb{Z}/{p_1}^{e_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/{p_r}^{e_r}\mathbb{Z})^*$ もわかる.

[*2] 定義 5.2.7 と定義 5.2.21 を参照のこと

定義 4.3.10 (オイラーの関数). 自然数 n に対し n と互いに素な n 以下の正の整数の個数を $\varphi(n)$ と書く．すなわち

$$\varphi(n) = \#\{a \in \mathbb{Z} \mid \mathrm{GCD}(a,n) = 1,\ 1 \leq a \leq n\} = \#((\mathbb{Z}/n\mathbb{Z})^*).$$

系 4.3.9 より $\varphi(p^e) = p^e - p^{e-1} = p^e(1-1/p)$. よって $n = {p_1}^{e_1} \cdots {p_r}^{e_r}$ と素因数分解すると，次のオイラー関数の計算式をを得る．

$$\begin{aligned}\varphi(n) &= \varphi({p_1}^{e_1}) \cdots \varphi({p_r}^{e_r}) \\ &= {p_1}^{e_1}\left(1 - \frac{1}{p_1}\right) \cdots {p_r}^{e_r}\left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)\end{aligned}$$

定理 4.3.11. $\mathrm{GCD}(a,n) = 1$ ならば $a^{\varphi(n)} \equiv 1 \pmod{n}$.

証明. $[a]$ は $\mathbb{Z}/n\mathbb{Z}$ の中で，乗法に関する逆元を持つから，写像

$$f_a : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*, \quad [x] \mapsto [a][x] = [ax]$$

は全単射である．（$f_{[a]^{-1}}$ が逆写像である．）よって $\mathbb{Z}/n\mathbb{Z} = \{[a_1], \ldots, [a_k]\}$, $k = \varphi(n)$, と書くと，

$$\{[a_1], \ldots, [a_k]\} = \{[aa_1], \ldots, [aa_k]\}.$$

したがって

$$[a_1 \cdots a_k] = [a_1] \cdots [a_k] = [aa_1] \cdots [aa_k] = [a^k a_1 \cdots a_k]$$

よって

$$a_1 \cdots a_k \equiv a^k a_1 \cdots a_k \pmod{n}$$

これより $n \mid a_1 \cdots a_k(a^k - 1)$ であるが，$a_1 \cdots a_k$ と n は互いに素なので $n \mid (a^k - 1)$ となる． □

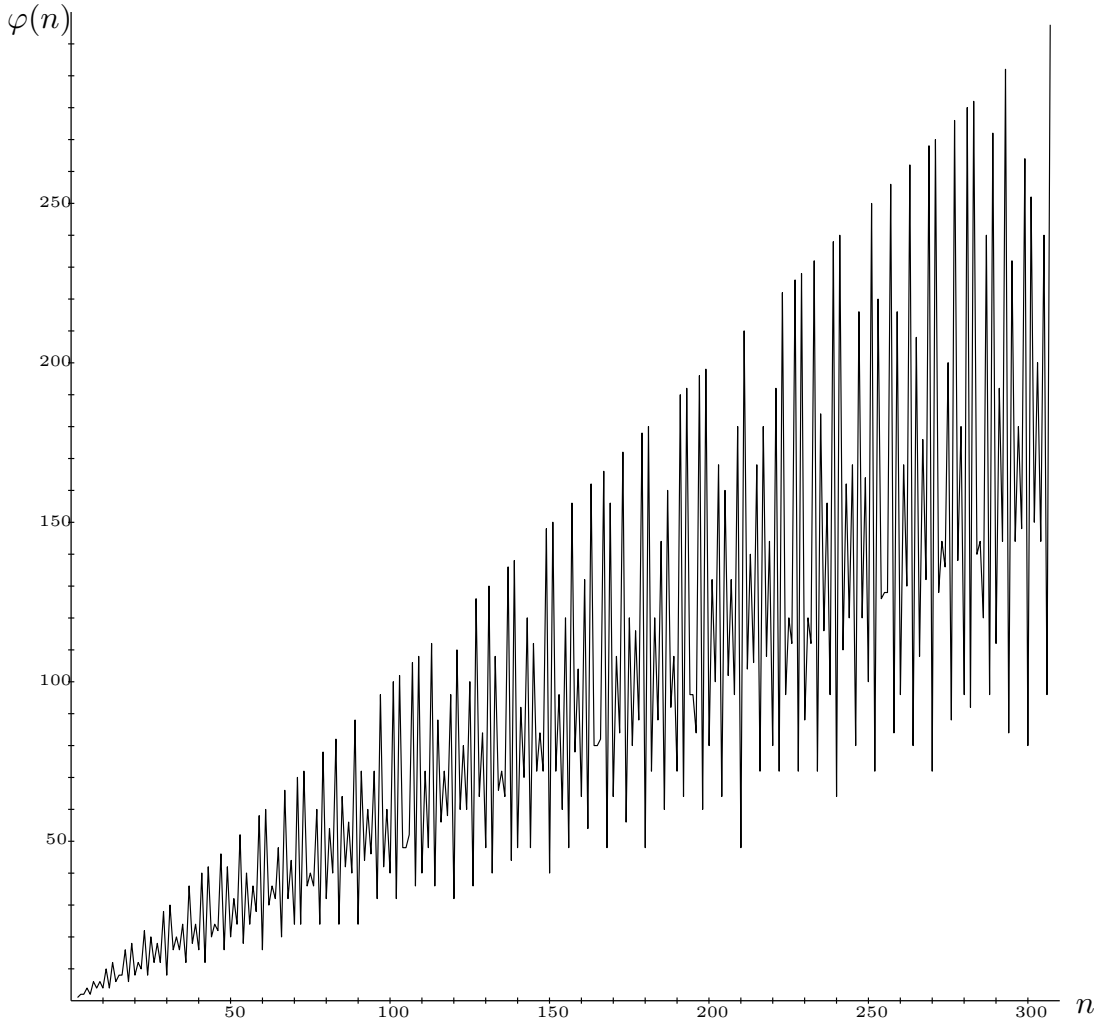
系 4.3.12. 素数 p と $1 \leq a < p$ なる整数 a に対し，$a^{p-1} \equiv 1 \pmod{p}$.

証明. $\mathrm{GCD}(a,p) = 1$, かつ $\varphi(p) = p - 1$ だから，前定理より明らか. □

系 4.3.12 は**フェルマー**[*3]**の小定理**と呼ばれることがある．

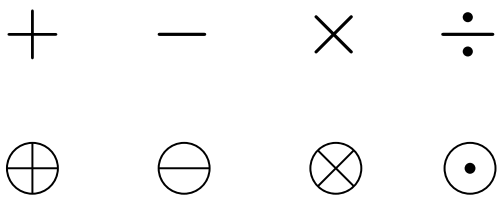
[*3] Pierre de Fermat（1607 – 1665）はフランスの数学者．職業は裁判官であり、数学は余暇に行った．

オイラーの関数 $\varphi(n)$ のグラフは以下のようになり，複雑である．



第 5 章

代数系初歩



加法，乗法といった演算を抽象化していくと群や環などの代数系の概念に行きつく．ここでは，群や環はもとより半群，体などの，基本的な代数系の定義を解説する．それぞれの具体例もいくつか説明することにする．

日本語	英語 （筆記体）	フランス語	ドイツ語	ロシア語
群	group (*group*)	groupe	Gruppe	группа
環	ring (*ring*)	anneau	Ring	колвчо
体	field (*field*)	corps	Körper	поле

5.1 半群，群

定義 5.1.1 (半群). 集合 S が**半群** (semigroup) であるとは，次の条件を満たす演算 $\cdot$ が定義されているときをいう．

(i) 任意の $a, b, c \in S$ に対し $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (結合法則)

もし演算 $\cdot$ が可換，すなわち

(ii) 任意の $a, b \in S$ に対し $a \cdot b = b \cdot a$. (交換法則)

が成り立つとき，半群 S は **可換半群** (commutative semigroup) であるという．可換半群については演算の記号 $\cdot$ を記号 $+$ であらわすのが便利なこともある．演算記号 $+$ を用いたときは**加法半群** (additive semigroup) という．

例 5.1.2. 自然数全体 $\mathbb{N} = \{1, 2, 3, \dots\}$ は加法 $+$ に関して加法半群になる．また乗法 $\times$ に対し別の可換半群をつくる．

例 5.1.3. 3.2 節で構成した $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \dots, [n-1]\}$ は加法 $+$ に関して加法半群になる．また乗法 $\times$ に対し別の可換半群をつくる．

定義 5.1.4 (単位元). S を演算 $\cdot$ をもつ半群とする．任意の $a \in S$ に対し

$$a \cdot e = e \cdot a = a$$

なる S の元 e が存在するとき e を S の**単位元** (unity) という．もし演算が加法で書かれるときには単位元は 0 であらわす．

例 5.1.5. $S = \{5a + 7b \mid a, b \text{ は非負整数 }\}$ は加法半群である．0 が S の単位元である．

補題 5.1.6 (単位元の一意性). 単位元は存在すれば一つに限る

証明. e と e' が単位元であるとする．すると 任意の $a \in S$ に対し $a \cdot e = a$, $a = e' \cdot a$ となる．$e' = e' \cdot e = e$ となり $e = e'$ がわかる． □

定義 5.1.7 (逆元). 半群 S に単位元 e が存在すると仮定する．S の元 a が**可逆元** (invertible element) であるとは,

$$a \cdot b = b \cdot a = e$$

なる $b \in S$ が存在するときをいう．b を a の**逆元** (inverse) という．次の定理より a の逆

元は存在すれば唯一つしかないのでそれを a^{-1} であらわす．もし演算が加法で書かれるときには a の逆元は $-a$ であらわす．

補題 5.1.8 (逆元の一意性). a の逆元は，存在すれば一つに限る．

証明. b と b' が a の逆元であるとする．すると 任意の $a \in S$ に対し $a \cdot b = e$, $b' \cdot a = e$ となる．

$$b' = b' \cdot e = b' \cdot (a \cdot b) = (b' \cdot a) \cdot b = e \cdot b = b$$

となり $b = b'$ がわかる． □

演習 5.1.9. b が a の逆元ならば a は b の逆元であることを示せ．

演習 5.1.10. 自然数全体の集合 $\mathbb{N}$ には加法に対する単位元は存在するか? 乗法に対する単位元は存在するか? 逆元についてはどうか?

演習 5.1.11. 3.2 節で構成した $\mathbb{Z}/n\mathbb{Z}$ には加法に対する単位元，および乗法に対する単位元は存在することを示せ．加法に対する逆元も存在することを示せ．乗法に対する逆元がいつ存在するか考察せよ．

演習 5.1.12. $(\mathbb{Z}/n\mathbb{Z})$ の乗法に関する可逆元全体の集合を $(\mathbb{Z}/n\mathbb{Z})^*$ であらわす．$n = 2, 3, \ldots, 8$ のとき $(\mathbb{Z}/n\mathbb{Z})^*$ のリストを作れ．

定義 5.1.13 (群). 演算 $\cdot$ をもつ半群 G が**群** (group) であるとは次をみたすときをいう．

(i) 演算 $\cdot$ の単位元が存在する．
(ii) 任意の $a \in G$ は可逆元である．

通常は a の逆元を a^{-1} であらわす．

演習 5.1.14. 群 G について，次を示せ．

- 任意の a に対し $ae = a$ なる元 e があれば，$ea = a$ である[*1]．
- $aa = a$ を満たす G の元 a は単位元に限る （ヒント $ab = e$ となる元 b をかけよ)．
- $ab = e$ ならば $ba = e$．($(ba)(ba) = ba$ を示す．)

可換半群が群であるとき**可換群** (commutative group) という．可換群の演算記号が $+$ で表されているとき，**加法群** (additive group) という．加法群については単位元を 0 で表し a の逆元を $-a$ で表す．

[*1] $ab = e$, $bc = e$ なる b, c をとると $ea = e(ae) = e(a(bc)) = e((ab)c) = (e(ab))c = (ee)c = ec = (ab)c = a(bc) = ae = a$.

例 5.1.15. 3.2 節で構成した $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\}$ は加法 $+$ に関して加法群になる．しかし乗法 $\times$ に対しては群にならない.

演習 5.1.16. $\mathbb{Z}/n\mathbb{Z}$ の乗法に関する可逆元全体の集合 $(\mathbb{Z}/n\mathbb{Z})^*$ は乗法に関して群をなす．$n = 2, 3, \ldots, 9$ のとき確かめよ.

例 5.1.17 (置換群). 空でない集合 M をそれ自身の上に写す全単射を M の**置換** (permutation) とよび, M の置換全体からなる集合を $\mathfrak{S}(M)$ と書く．$\mathfrak{S}(M)$ は写像の合成に関して群になり，M の**全置換群**と呼ばれる．とくに $M = \{1, 2, \ldots, n\}$ のとき $\mathfrak{S}(M)$ は次数 n の**対称群** (symmetric group) とよばれ，$\mathfrak{S}_n$ と書かれる．そして

$$i \mapsto a_i, \quad i = 1, 2, \ldots, n$$

なる置換を

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

であらわす．$\{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, n\}$ であることに注意しよう.

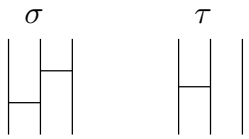
例えば $n = 3$ として

$$\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix}$$

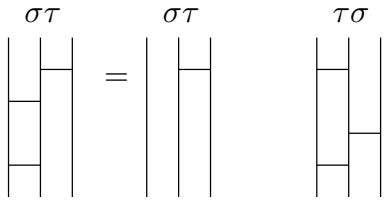
とすれば

$$\sigma\tau = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}$$

である．この例からもわかるように，一般には置換の積に対しては交換法則は成り立たない.



置換群の元はあみだくじを用いてあらわすこともできる．このとき積 $\sigma\tau$, $\tau\sigma$ はそれぞれ次のように表される.



演習 5.1.18 (3 次対称群 $\mathfrak{S}_3$).

$$e = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}$$

とおけば

$$\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix} = \beta\alpha$$

となる．このとき

$$\mathfrak{S}_3 = \{e, \sigma, \sigma^2, \alpha, \alpha\sigma, \alpha\sigma^2\}$$

を示せ．また群 $\mathfrak{S}_3$ の演算表を完成させよ．

	e	σ	σ^2	α	$\alpha\sigma$	$\alpha\sigma^2$
e						
σ						
σ^2						
α						
$\alpha\sigma$						
$\alpha\sigma^2$						

演習 5.1.19 (4 次対称群 $\mathfrak{S}_4$). 4 次対称群 $\mathfrak{S}_4$ について演習 5.1.18 と同様の考察[*2]を行え．ヒント: 次の元を用いて計算せよ．

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

演習 5.1.20. $\#\mathfrak{S}_n = n!$ を示せ．

2 つの群 G, H の間の写像 $f : G \to H$ が**群準同型** (group homomorphism) であるとは次の条件をみたすときをいう．

(i) 任意の $a, b \in R$ に対し $f(a \cdot b) = f(a) \cdot f(b)$.

演習 5.1.21. 群準同型 $f : G \to H$ は単位元を単位元に写すことを示せ．

演習 5.1.22. 群準同型 $f : G \to H$ が単射であることは $\mathrm{Ker}\, f$ が単位元のみからなることと同値であることを示せ．但し $\mathrm{Ker}\, f$ は単位元の f による逆像を表す．

演習 5.1.23. 演習 5.1.18 の記号の下で，次で定まる写像 $\varphi : \mathfrak{S}_3 \to \mathbb{Z}/2\mathbb{Z}$ は群準同型であることを示せ．

$$\varphi(e) = \varphi(\sigma) = \varphi(\sigma^2) = [0], \quad \varphi(\alpha) = \varphi(\alpha\sigma) = \varphi(\alpha\sigma^2) = [1].$$

[*2] 群の演算表を完成させるのは，$\mathfrak{S}_4$ の元が 24 個あるので，大変であろう．

5.2 環，体

定義 5.2.1 (環). 集合 R に演算 $+, \cdot$ が定義されていて, 次の条件を満たすとき R は**環** (ring) であるという.

(i) R は演算 $+$ について加法群.
(ii) R は演算 $\cdot$ について半群.
(iii) 任意の $a, b, c \in R$ について $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$. (分配法則)

加法 $+$ に関する単位元を**零元** (zero) とよび 0 であらわす．さらに，演算 $\cdot$ が可換，すなわち

(iv) 任意の $a, b \in R$ に対し $a \cdot b = b \cdot a$. (交換法則)

が成り立つとき，環 R は **可換環** (commutative ring) であるという．演算 $\cdot$ に関する単位元をもつ可換環を**単位的可換環** (commutative ring with unity) という． 通常はこの単位元を 1 と書くことが多い.

環 R の元 a, b に対して $a - b$ を次で定義する.

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

明らかに $a - a = a + (-a) = 0$ である．また,

$$x + b = a \quad \Longleftrightarrow \quad x = a - b$$

であることも明らかであろう.

演習 5.2.2. 環 R の元 a, b, c について,

$$(a - b)c = ac - bc, \quad a(b - c) = ab - ac$$

が成り立つことを示せ.

例 5.2.3. 整数全体の集合 $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ は加法 $+$ および乗法 $\times$ について単位的可換環になる．有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ はいずれも通常の加法，乗法に関して単位的可換環になる．また第 3.2 節の $\mathbb{Z}/n\mathbb{Z}$ も，単位的可換環になる.

例 5.2.4. R を $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ などのような可換環とする．R の元を要素とするような n 次正方行列全体の集合

$$M_n(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \;\middle|\; a_{ij} \in R \right\}$$

は行列の加法 $+$ および 行列の積 $\cdot$ について環になる．$n \geq 2$ のときは，正方行列全体の環は可換環ではない．

例 5.2.5. R を $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ などの可換環とする．1 変数 R 係数多項式全体の集合

$$R[x] = \left\{ f(x) \;\middle|\; \begin{array}{l} \exists n \in \mathbb{N},\ \exists\, a_1, \ldots, a_n \in R, \\ f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \end{array} \right\}$$

は通常の多項式の加法，乗法について可換環になる．一般に n 変数 $x_1, \ldots, x_n$ の多項式環

$$R[x_1, \ldots, x_n] = \left\{ \sum a_{i_1,\ldots,i_n} {x_1}^{i_1} \cdots {x_n}^{i_n} \text{ 有限和} \;\middle|\; a_{i_1,\ldots,i_n} \in R \right\}$$

も通常の多項式の加法，乗法について可換環になる．

補題 5.2.6. 環 R の任意の元 a, b に対して次が成り立つ．

(i) $0 \cdot a = 0,\ a \cdot 0 = 0.$
(ii) $a(-b) = -ab,\ (-a)b = -ab.$
(iii) $(-a)(-b) = ab.$

証明. (i): $0 \cdot a = (a-a)a = aa - aa = 0.$ $a \cdot 0 = a(a-a) = aa - aa = 0.$
(ii): $0 = a(b + (-b)) = ab + a(-b),\ 0 = a((-b) + b) = a(-b) + ab,$ より $a(-b) = -ab$ を得る．$(-a)b = -ab$ も同様.
(iii): (ii) より $(-a)(-b) = -(-a)b = -(-ab) = ab.$ 最後の等式では $-ab$ の加法に関する逆元が ab であることを用いている． □

定義 5.2.7. 2 つの可換環 R, S の間の写像 $f : R \to S$ が**環の準同型** (ring homomorphism) であるとは次の条件をみたすときをいう．

(i) 任意の $a, b \in R$ に対し $f(a+b) = f(a) + f(b).$
(ii) 任意の $a, b \in R$ に対し $f(a \cdot b) = f(a) \cdot f(b).$

さらに f が全単射ならば環 R と S は（ f により）**環同型**になるという．

演習 5.2.8. 環準同型 $f : R \to S$ が全単射のとき，f^{-1} も環準同型であることを示せ．

例 5.2.9. 写像 $f:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, $f(x)=[x]$, は環準同型である.

演習 5.2.10. 環準同型 $f:R\to S$ が単射であることは $\mathrm{Ker}\, f$ が零元のみからなることと同値であることを示せ. 但し $\mathrm{Ker}\, f$ は零元の f による逆像を表す.

定義 5.2.11 (体). 単位的可換環 F に対し, $F-\{0\}$ が演算 $\cdot$ に対して群になるとき F は**体** (field) であるという. いいかえると, 体とは 0 以外の元が可逆元であるような単位的可換環のことである.

例 5.2.12. 有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ はいずれも通常の加法, 乗法に関して体になる.

演習 5.2.13 (複素数). 複素数とは $x+y\boldsymbol{i}$, $x,y\in\mathbb{R}$ なる形の数であった. $\boldsymbol{i}^2=-1$ とし, 分配律が成り立つとして複素数に積を定義するのであった.

$$\bar{\mathbb{C}}:=\left\{\begin{pmatrix}x & y\\ -y & x\end{pmatrix}\;\middle|\; x,y\in\mathbb{R}\right\}$$

とおくと, 次の写像は準同型かつ全単射なので $\mathbb{C}$ は $\bar{\mathbb{C}}$ と環として同型であることを示せ.

$$f:\mathbb{C}\to\bar{\mathbb{C}},\quad x+y\boldsymbol{i}\mapsto\begin{pmatrix}x & y\\ -y & x\end{pmatrix}$$

演習 5.2.14 (ハミルトンの四元数). ハミルトンの四元数とは $x+y\boldsymbol{i}+z\boldsymbol{j}+w\boldsymbol{k}$, $x,y,z,w\in\mathbb{R}$, なる形の数で,

$$\boldsymbol{i}^2=\boldsymbol{j}^2=\boldsymbol{k}^2=-1,\quad \boldsymbol{ij}=-\boldsymbol{ji}=\boldsymbol{k},\quad \boldsymbol{jk}=-\boldsymbol{kj}=\boldsymbol{i},\quad \boldsymbol{ki}=-\boldsymbol{ik}=\boldsymbol{j}$$

とし, 分配律が成り立つとして積を定義することができる.
ハミルトンの四元数全体を $\mathbb{H}$ であらわすと, $\mathbb{H}$ は可換でない体となることを示せ.

$$\bar{\mathbb{H}}:=\left\{\begin{pmatrix}x & y & z & w\\ -y & x & -w & z\\ -z & w & x & -y\\ -w & -z & y & x\end{pmatrix}\;\middle|\; x,y,z,w\in\mathbb{R}\right\}$$

とおくと, 次の写像は準同型かつ全単射であることを示せ.

$$f:\mathbb{H}\to\bar{\mathbb{H}},\quad x+z\boldsymbol{i}+y\boldsymbol{j}+w\boldsymbol{k}\mapsto\begin{pmatrix}x & y & z & w\\ -y & x & -w & z\\ -z & w & x & -y\\ -w & -z & y & x\end{pmatrix}$$

特に $\mathbb{H}$ は $\bar{\mathbb{H}}$ と環として同型である.

$$\hat{\mathbb{H}}:=\left\{\begin{pmatrix}x+yi & z+wi\\ -z+wi & x-yi\end{pmatrix}\;\middle|\; x,y,z,w\in\mathbb{R}\right\}$$

とおくと，次の写像は準同型かつ全単射であることを示せ．

$$f : \mathbb{H} \to \hat{\mathbb{H}}, \quad x + z\boldsymbol{i} + y\boldsymbol{j} + w\boldsymbol{k} \mapsto \begin{pmatrix} x+yi & z+wi \\ -z+wi & x-yi \end{pmatrix}$$

特に $\mathbb{H}$ は $\hat{\mathbb{H}}$ と環として同型である．

演習 5.2.15. 一変数実多項式環 $\mathbb{R}[x]$ から実数体 $\mathbb{R}$ への環準同型 $\varphi : \mathbb{R}[x] \to \mathbb{R}$ で単位元を単位元にうつすものをすべて決定せよ．(ヒント: 準同型 $\varphi : \mathbb{R}[x] \to \mathbb{R}$ で $\varphi(1) = 1$ なるものをとる．$\varphi(x) = a$ なる実数 a をとると，多項式 $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, $c_i \in \mathbb{R}$, の φ による像は $f(a) = c_0 + c_1 a + \cdots + c_n a^n$ になる．この準同型を φ_a と書く．) また $\operatorname{Ker} \varphi_a = \operatorname{Ker} \varphi_{a'}$ なるための条件を記述せよ．ただし

$$\operatorname{Ker} \varphi = \{f \in \mathbb{R}[x] \mid \varphi(f) = 0\}.$$

演習 5.2.16. また $\mathbb{R}[x]$ から複素数体 $\mathbb{C}$ への環準同型 $\varphi : \mathbb{R}[x] \to \mathbb{C}$ で単位元を単位元にうつすものをすべて決定せよ．(ヒント: 準同型 $\varphi : \mathbb{R}[x] \to \mathbb{C}$ で $\varphi(1) = 1$ なるものをとる．$\varphi(x) = a + b\sqrt{-1}$ なる実数 a, b をとると，多項式 $f(x)$ の φ による像は $f(a + b\sqrt{-1})$ になる．この準同型を $\varphi_{a,b}$ と書く．) また $\operatorname{Ker} \varphi_{a,b} = \operatorname{Ker} \varphi_{a',b'}$ なるための条件を記述せよ．

定義 5.2.17 (分数環). 可換環 R の部分集合 S が**積閉集合**であるとは，$1 \in S$ かつ $a, b \in S$ ならば $ab \in S$ を満たすときを言う．積閉集合 S があれば，次のようにして S の元を分母にする**分数環**を考えることが出来る．まず $R \times S$ に次で同値関係を定める．

$$(a, s) \sim (a', s') \iff t(as' - a's) = 0 \text{ を満たす } t \in S \text{ が存在する．}$$

この同値関係による (a, s) の同値類を a/s, 商集合を $R[S^{-1}]$ または $S^{-1}R$ で表す．商集合には $a/s + a'/s' = (as' + a's)/(ss')$, $a/s + a'/s' = (aa')/(ss')$ で加法と乗法が定まる．

演習 5.2.18. 3.3 節を参考にして，上の $\sim$ が同値関係であること，及び加法乗法はうまく定義されている事を示せ．写像 $\varphi : R \to R[S^{-1}]$, $\varphi(a) = a/1$ で定めると $\operatorname{Ker} \varphi = \{a \in R \mid \exists s \in S \ as = 0\}$ であることを示せ．

直積

代数系の直積にはしばしば代数系の構造が入る．

定義 5.2.19 (群の直積). r 個の群 $G_1, \ldots, G_r$ の直積集合 $G_1 \times \cdots \times G_r$ に対し

$$(a_1, \ldots, a_r) \cdot (b_1, \ldots, b_r) := (a_1 b_1, \ldots, a_r b_r)$$

で演算 $\cdot$ を定義すると $G_1 \times \cdots \times G_r$ は群となり，その単位元は $(e_1, \ldots, e_r)$, e_i は G_i の単位元，と表される．

演習 5.2.20. $G_1 \times \cdots \times G_r$ の元 $a = (a_1, \ldots, a_r)$ の逆元は $({a_1}^{-1}, \ldots, {a_r}^{-1})$ で表せることを示せ.

定義 5.2.21 (環の直積). r 個の環 $R_1, \ldots, R_r$ の直積集合 $R_1 \times \cdots \times R_r$ に対し

$$(a_1, \ldots, a_r) + (b_1, \ldots, b_r) := (a_1 + b_1, \ldots, a_r + b_r)$$
$$(a_1, \ldots, a_r) \cdot (b_1, \ldots, b_r) := (a_1 b_1, \ldots, a_r b_r)$$

で加法 $+$, 乗法 $\cdot$ を定義すると $R_1 \times \cdots \times R_r$ は環となる.

5.3 擬順序

集合 X で定義された順序 $\preceq$ とは X の任意の 2 元 a,b に対し $a \preceq b$ であるかそうでないかが定まっていて次の条件をみたすときをいうのであった.

(i) 反射律: $a \preceq a$.
(ii) 反対称律: $a \preceq b$ かつ $b \preceq a$ ならば $a = b$.
(iii) 推移律: $a \preceq b$ かつ $b \preceq c$ ならば $a \preceq c$.

反射律と推移律をみたすが，必ずしも反対称律をみたさないとき，関係 $\preceq$ を**擬順序** (pseudo-order) という．また X の任意の元 a, b に対して $a \preceq b$ か $a \succeq b$ のいずれかが成り立つ擬順序を**全擬順序** (total pseudo-order) という.

定義 5.3.1 (擬順序加群). 加群 G で，次の性質をみたす擬順序 $\preceq$ があるものを**擬順序加群**という.

(i) G の任意の元 a, b, c に対し $a \preceq b$ ならば $a + c \preceq b + c$

とくに，$\preceq$ が順序であれば**順序加群**, $\preceq$ が全擬順序であれば**全擬順序加群**, $\preceq$ が全順序であれば**全順序加群**という.

定義 5.3.2 (擬順序環). 可換環 R で，次の性質をみたす擬順序 $\preceq$ があるものを**擬順序環**という.

(i) 加法に関して R は擬順序加群になる.
(ii) $a \succeq 0, b \succeq 0$ ならば $ab \succeq 0$.

とくに，$\preceq$ が順序であれば**順序環** (ordered ring), $\preceq$ が全擬順序であれば**全擬順序環**, $\preceq$ が全順序であれば**全順序環**という.

擬順序環 R に対し

$$P := \{a \in R \mid a \succeq 0\}$$

を，この擬順序の**正錐** (positive cone) という．また $-P$ を次で定義する.

$$-P := \{x \in R \mid -x \in P\}.$$

定理 5.3.3. 擬順序環 $(R, \preceq)$ の正錐 P に対し次が成り立つ.

(i) $0 \in P$
(ii) $a, b \in P$ ならば $a + b \in P$.

(iii) $a, b \in P$ ならば $ab \in P$.

逆に (i), (ii), (iii) をみたす P があれば，P を正錐とするような擬順序を R に定義することができる．

証明. 擬順序環 $(R, \preceq)$ に対し，(i), (iii) が成り立つのは明らかであろう．(ii) を示す．$a, b \in P$ より $a \succeq 0$, $b \succeq 0$. $a + b \succeq a + 0 \succeq 0 + 0 = 0$ より $a + b \in P$.

P を (i), (ii), (iii) をみたす R の部分集合とすると,

$$a \preceq b \iff^{\text{def}} b - a \in P$$

とすれば，$\preceq$ は擬順序になる． □

定理 5.3.4. 擬順序環 R の正錐 P に対し次が成り立つ.

(i) $\preceq$ が順序 $\iff P \cap (-P) = \{0\}$.
(ii) $\preceq$ が全擬順序 $\iff P \cup (-P) = R$.

証明. (i): $\preceq$ が順序ならば $P \cap (-P) = \{0\}$ は明らかであろう．逆に $P \cap (-P) = \{0\}$ とすると,

$$\begin{aligned} a \preceq b,\ a \succeq b &\iff a - b \succeq 0, b - a \succeq 0 \\ &\iff a - b \in P,\ b - a \in P \\ &\iff a - b \in P \cap (-P) = \{0\} \\ &\iff a = b. \end{aligned}$$

よって $\preceq$ は順序になった.

(ii): $\preceq$ が全擬順序であれば，R の任意の元 a に対し，$a \preceq 0$ か $a \succeq 0$ のいずれかが成立するので, $P \cup (-P) = R$. 逆に

$$\begin{aligned} a \preceq b \text{ または } a \succeq b &\iff a - b \succeq 0 \text{ または } b - a \succeq 0 \\ &\iff a - b \in P \text{ または } b - a \in P \\ &\iff a - b \in P \text{ または } a - b \in (-P) \end{aligned}$$

なので $P \cup (-P) = R$ ならば $\preceq$ は全擬順序になる． □

例 5.3.5. 有理数全体の集合 $\mathbb{Q}$ は全順序環になる．正錐 P は次で与えられる.

$$P = \{p/q \in \mathbb{Q} \mid p \geq 0\}.$$

P が定理 5.3.3(i), (ii), (iii) と $P \cup (-P) = R$, $P \cap (-P) = \{0\}$ をみたすことを確認せよ.

例 5.3.6. 実数全体の集合 $\mathbb{R}$ は大小関係で全順序環になる.

演習 5.3.7. 実係数多項式環 $\mathbb{R}[x]$ にどのような擬順序が入るか考えてみよう. a を実数とし、P_a を次で定義する. これを正錐にするような全擬順序が定まることを示せ.

$$P_a = \{f(x) \in \mathbb{R}[x] \mid f(a) \geq 0\}.$$

つまり P_a が定理 5.3.3(i), (ii), (iii) と $P \cup (-P) = \mathbb{R}[x]$ をみたすことを確認せよ. 同様にして, 次で P_{a_+}, P_{a_-} を定義すると, これらを正錐にするような全擬順序が定まることを確認せよ.

$$P_{a_+} = \{f(x) \in \mathbb{R}[x] \mid \exists \varepsilon > 0 \text{ s.t. } x < y < x + \varepsilon \text{ ならば } f(y) \geq 0\}$$
$$P_{a_-} = \{f(x) \in \mathbb{R}[x] \mid \exists \varepsilon > 0 \text{ s.t. } x > y > x - \varepsilon \text{ ならば } f(y) \geq 0\}$$

定義 5.3.8. X, Y を (擬) 順序を持つ集合とする. 写像 $f : X \to Y$ が **(擬) 順序を保つ** とは, すべての X の元 x, y に対し

$$x \preceq y \text{ ならば } f(x) \preceq f(y)$$

が成り立つときをいう.

問題: 集合 X に同値関係 $\sim$ を定め, その同値関係による商写像 $f : X \to Y := X/\sim$ を考えます.

(i) X が群のとき Y にうまく群の構造をいれて f を群準同型にすることができるか? そのための必要十分条件は何か?
(ii) X が環のとき Y にうまく環の構造をいれて f を環準同型にすることができるか? そのための必要十分条件は何か?
(iii) X に (擬) 順序があるとき Y にうまく (擬) 順序の構造をいれて f が (擬) 順序を保つようにすることができるか? そのための必要十分条件は何か?

こういった問題を考えることが代数系の理論の始まりになります.

定理 5.3.9. 半順序集合 X, Y と写像 $f : X \to Y$, $g : Y \to X$ が次の (i)–(iv) を満たすとき, $f|_{g(Y)} : g(Y) \to f(X)$ は全単射で $g|_{f(X)} : f(X) \to g(Y)$ がその逆写像になる.

(i) 任意の $x, x' \in X$ に対して $x \preceq x'$ ならば $f(x') \preceq f(x)$
(ii) 任意の $y, y' \in Y$ に対して $y \preceq y'$ ならば $g(y') \preceq g(y)$
(iii) 任意の $x \in X$ に対して $x \preceq g \circ f(x)$
(iv) 任意の $y \in Y$ に対して $y \preceq f \circ g(y)$

証明. 任意の $x \in X$ に対して

$$\begin{array}{rcll} f(x) & \preceq & f \circ g(f(x)) & ((\text{iv}) \text{ より}) \\ & = & f(g \circ f(x)) & \\ & \preceq & f(x) & ((\text{i}), (\text{iii}) \text{ より}) \end{array}$$

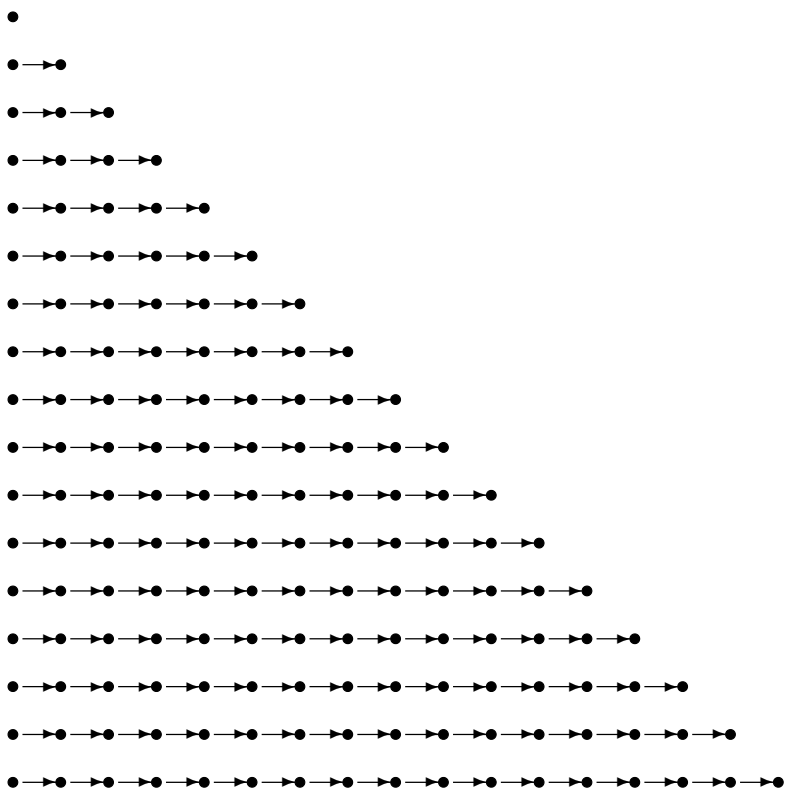
なので，$f \circ g(f(x)) = f(x)$. 同様にして任意の $y \in Y$ に対して

$$\begin{array}{rcll} g(y) & \preceq & g \circ f(g(y)) & ((\text{iii}) \text{ より}) \\ & = & g(f \circ g(y)) & \\ & \preceq & g(y) & ((\text{ii}), (\text{iv}) \text{ より}) \end{array}$$

なので $g \circ f(g(y)) = g(y)$. よって $f \circ g|_{f(X)} = 1|_{f(X)}$, $g \circ f|_{g(Y)} = 1|_{g(Y)}$ なので証明を終わる. □

第 6 章

自然数論



数体系が矛盾なく構築されているかということは，数学の基礎に関心をもつ人々がまず最初に思い浮かべる問題であろう．イタリアの数学者 Giuseppe Peano (1858 – 1932) は自然数のいくつかの基本的な性質を公理として，自然数の他のいろいろな性質を導き，自然数を論理的に構成した．本章では，その概略を紹介する．

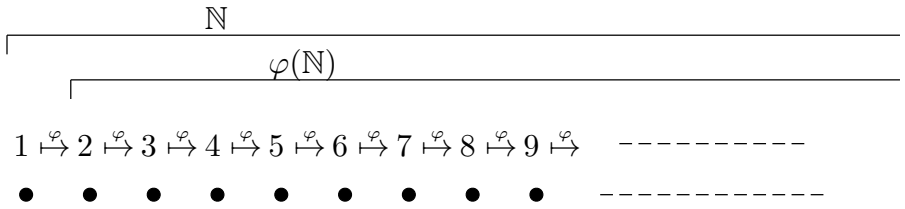
6.1 Peano の公理

Peano の公理と呼ばれるのは $\mathbb{N}$ に関する次の 5 つの命題である．

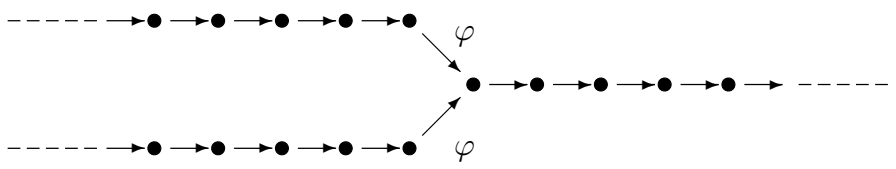
(i) $1 \in \mathbb{N}$.
(ii) 写像 $\varphi : \mathbb{N} \to \mathbb{N}$ が与えられている．
(iii) $\varphi(\mathbb{N}) \not\ni 1$.
(iv) φ は単射.
(v) $\mathbb{N}$ の部分集合 A が次の性質を持てば $\mathbb{N} = A$.

$$1 \in A, \quad \varphi(A) \subset A.$$

われわれは以上の (i)–(v) だけを基礎とし, それから $\mathbb{N}$ のすべての性質を導く事とする．この立場からは，上の (i)–(v) をみたす集合 $\mathbb{N}$ の元が自然数と名付けられる．(i) より ‘1 は自然数である’ ことがわかる．(ii) より ‘$\varphi(1)$ も自然数である’ ことがわかる．そこで $\varphi(1) = 2$ と定義すれば ‘2 も自然数である’ ことになる．同様に，$\varphi(2) = 3, \varphi(3) = 4, \ldots$ と定義すれば ‘$1, 2, 3, 4, \ldots$ は自然数であることになる．このように 1 から始めて，$\varphi(1)$, $\varphi(\varphi(1))$, $\varphi(\varphi(\varphi(1)))$, $\ldots$. とどこまでも続けていけば，自然数の全体が得られることを最後の (v) は主張している．



また自然数は一列に並んでいるのであって次図のように異なるものの φ による像が一緒になるようなことはない．(iv) はそのことを表している．



$\varphi(x)$ は 「x の次の自然数」と呼ばれる．$\varphi(x)$ は通常 $x + 1$ と書かれる自然数である．$x + 1$ と書いたほうが，馴染みやすいかもしれないので，この記法を用いて，Peano の公理を書き直しておこう．

(i) 1 は自然数である.
(ii) 自然数 x に対し x の次の元と呼ばれる 自然数 $x+1$ が定まっている.
(iii) 1 はいかなる自然数の次の元にもならない.
(iv) 次の元が等しいような 2 つの自然数は相等しい.
(v) $\mathbb{N}$ の部分集合 A が次の性質を持てば $\mathbb{N} = A$.

$$1 \in A, \quad x \in A \Longrightarrow x+1 \in A.$$

最後の (v) を**数学的帰納法の原理**ということがある.

定理 6.1.1 (数学的帰納法). 自然数 n に関する命題 $P(n)$ がすべての自然数 n に対して成り立つことを証明するには, 次の 2 つのことを示せばよい.

(i) $P(1)$ が成り立つ.
(ii) $P(n)$ が成り立てば $P(n+1)$ が成り立つ.

証明. $A = \{n \in \mathbb{N} \mid P(n)$ が成り立つ $\}$ とおいて, $A = \mathbb{N}$ を示せばよい.

$$\text{(i) より } 1 \in A, \quad \text{(ii) より } x \in A \implies x+1 \in A.$$

よって 数学的帰納法の原理 (v) より $A = \mathbb{N}$ がわかる. □

自然数の和と積

まず $x, y \in N$ に対し その和と呼ばれる自然数 $x+y$ を定義しよう.

定理 6.1.2. $\mathbb{N}$ の元 x に対し, $\mathbb{N}$ から $\mathbb{N}$ への写像 f_x で次の性質を満たすものが一意的に存在する.

$(1)_x$ $f_x(1) = \varphi(x)$.
$(2)_x$ すべての $y \in \mathbb{N}$ に対し $f_x(\varphi(y)) = \varphi(f_x(y))$.

証明. f_x の存在: A を次で定義する.

$$A = \{x \in \mathbb{N} \mid (1)_x,\ (2)_x \text{をみたす } f_x \text{ が存在 }\}.$$

$A = \mathbb{N}$ を示せばよい.
$f_1(y) = \varphi(y)$ とおけば

$(1)_1$: $f_1(1) = \varphi(1)$,
$(2)_1$: $\forall\, y \in \mathbb{N}$, $f_1(\varphi(y)) = \varphi(\varphi(y)) = \varphi(f_1(y))$.

は明らかに成立する．よって $1 \in A$.

また $x \in A$ のとき $f_{\varphi(x)}(y) = \varphi(f_x(y))$ とおけば,

$(1)_{\varphi(x)}$: $f_{\varphi(x)}(1) = \varphi(f_x(1)) = \varphi(\varphi(x))$.
$(2)_{\varphi(x)}$: $f_{\varphi(x)}(\varphi(y)) = \varphi(f_x(\varphi(y))) = \varphi(\varphi(f_x(y))) = \varphi(f_{\varphi(x)}(y))$.

が成立するので $\varphi(x) \in A$ がわかる．よって Peano の公理の (v) より $A = \mathbb{N}$ がわかる．

f_x の一意性: 同じ条件を満たす f'_x があったとして $f_x = f'_x$ を示す．A を次で定義する．

$$A = \{y \in \mathbb{N} \mid f_x(y) = f'_x(y)\}$$

$A = \mathbb{N}$ を示せばよい．$f_x(1) = \varphi(x) = f'_x(1)$ より $1 \in A$ となる．$x \in A$ とすると $f_x(y) = f'_x(y)$ なので

$$f_x(\varphi(y)) = \varphi(f_x(y)) = \varphi(f'_x(y)) = f'_x(\varphi(y))$$

なので $\varphi(y) \in A$ がわかる．よって Peano の公理の (v) より $A = \mathbb{N}$ がわかる． □

$x + y := f_x(y)$ で 和 $x + y$ を定義する．

演習 6.1.3 (F-帰納的). 写像 $F : \mathbb{N} \to \mathbb{N}$ に対して,

$$f(\varphi(y)) = F(f(y)), \quad \forall\, y \in \mathbb{N},$$

を満たす写像 $f : \mathbb{N} \to \mathbb{N}$ を F-帰納的な写像と呼ぶことにする．このとき，f_1, f_2 が共に F-帰納的で，$f_1(1) = f_2(1)$ ならば $f_1 = f_2$ であることを示せ．ヒント: $A = \{x \in \mathbb{N} \mid f_1(x) = f_2(x)\}$ とおいて, 上の一意性の証明を参考にせよ.

演習 6.1.4. $x, y, z \in \mathbb{N}$ に対し，次を示せ.

(i) $x + y = y + x$
(ii) $(x + y) + z = x + (y + z)$

ヒント: 交換律を示すには x を固定して $f_1(y) = x + y$, $f_2(y) = y + x$ として演習 6.1.3 を用いる．結合律を示すには x, y を固定して $f_1(z) = (x + y) + z$, $f_2(z) = x + (y + z)$ として演習 6.1.3 を用いる.

和の交換法則なんて当り前であるなんていわないでいただきたい．十分大きな自然数 x, y に対して $x + y = y + x$ が成立するということは, 小学校以来一度も確認する機会がなかった筈である．いまここで我々はこの法則を，証明したわけであるから，以後安心して，どんなに大きな自然数 x, y に対しても $x + y = y + x$ が成り立つといえるのである.

つぎに $x, y \in \mathbb{N}$ に対し その積と呼ばれる自然数 xy を定義しよう.

定理 6.1.5. $\mathbb{N}$ の元 x に対し，$\mathbb{N}$ から $\mathbb{N}$ への写像 g_x で次の性質を満たすものが一意的に存在する．

(i) $g_x(1) = x$.
(ii) すべての $y \in \mathbb{N}$ に対し $g_x(\varphi(y)) = g_x(y) + x$.

証明. g_x の存在: A を次で定義する．

$$A = \{x \in \mathbb{N} \mid (1)_x,\ (2)_x \text{をみたす } g_x \text{ が存在 }\}.$$

$A = \mathbb{N}$ を示せばよい．
$g_1(y) = y$ とおけば

$(1)_1$: $g_1(1) = 1$,
$(2)_1$: $\forall\, y \in \mathbb{N}$, $g_1(\varphi(y)) = \varphi(y) = y + 1$.

は明らかに成立する．よって $1 \in A$.
また $x \in A$ のとき $g_{\varphi(x)}(y) = g_x(y) + y$ とおけば,

$(1)_{\varphi(x)}$: $g_{\varphi(x)}(1) = g_x(1) + 1 = x + 1 = \varphi(x)$.
$(2)_{\varphi(x)}$: $g_{\varphi(x)}(\varphi(y)) = g_x(\varphi(y)) + \varphi(y) = g_x(y) + x + \varphi(y)$
$= g_x(y) + x + y + 1 = g_{\varphi(x)}(y) + \varphi(x)$.

が成立するので $\varphi(x) \in A$ がわかる．よって Peano の公理の (v) より $A = \mathbb{N}$ がわかる．
一意性の証明は定理 6.1.2 と同様なので省略する． □

演習 6.1.6. 定理 6.1.5 の一意性を証明せよ．

$xy := g_x(y)$ で 積 xy を定義する．

演習 6.1.7. 演習 6.1.4 と同様にして, $x, y, z \in \mathbb{N}$ に対し $xy = yx$, $(xy)z = x(yz)$ を示せ．$x(y + z) = xy + xz$, $(x + y)z = xz + yz$ も示せ.

6.2 自然数の順序

$\mathbb{N}$ における順序

定理 6.2.1. $x, y \in \mathbb{N}$ に対し，次のいずれか一つ，かつ一つだけが成り立つ.

(i) $x = y + u$ となる $\mathbb{N}$ の元 u が存在する.
(ii) $x = y$.
(iii) $y = x + v$ となる $\mathbb{N}$ の元 v が存在する.

補題 6.2.2. 任意の $x, y \in \mathbb{N}$ に対し $x + y \neq y$.

証明. $\mathbb{N}$ の元 x を固定し, $A = \{y \mid x + y \neq y\}$ とおく．$A = \mathbb{N}$ を示せばよい．Peano の公理 (iii) より $1 \in A$ である．$y \in A$ にすると $x + y \neq y$ Peano の公理 (iii) より $\varphi(x + y) \neq \varphi(y)$ である．これは $x + y + 1 \neq y + 1$ を意味するので，$y + 1 \in A$. Peano の公理 (v) より $A = \mathbb{N}$ である． □

補題 6.2.3. $x \in \mathbb{N}$ に対し $x \neq 1$ ならば $x = 1 + u$ なる $u \in \mathbb{N}$ が存在する.

証明. $A = \{1\} \cup \{x \in \mathbb{N} \mid \exists\, u \in \mathbb{N},\ x = u + 1\}$ とおくと，$A = \{1\} \cup \varphi(\mathbb{N})$ なので，Peano の公理 (v) より $A = \mathbb{N}$ である． □

定理 6.2.1 の証明. (i) と (ii) が同時に成り立つとすると $x = y + u = x + u$ となり補題 6.2.2 に反するので，(i) と (ii) が同時に成り立つことはない．同様にして (ii) と (iii) は同時に成り立つことはないことが示せる．また (i) と (iii) が同時に成り立つとすれば,

$$x = y + u = (x + v) + u = x + (u + v)$$

となるから，これも補題 6.2.2 に反する.

次に x を固定して

$$A = \{y \in \mathbb{N} \mid \text{(i),(ii),(iii) のいずれかが成り立つ }\}$$

とおき $A = \mathbb{N}$ を証明しよう．補題 6.2.3 より $y = 1$ のときは (i) または (ii) が成り立つので $1 \in A$ である.

$y \in A$ とする.

(i) $x = y + u$ なる関係が成り立つとすれば, 補題 6.2.3 より $u = 1$, または $u = 1 + u'$

なので $x = y+1$, $x = (y+1)+u'$ のいずれかが成り立ち，x と $y+1$ の間には (ii) または (i) が成り立つことになる．

(ii) $x = y$ なる関係が成り立てば $y+1 = x+1$ なので，x と $y+1$ の間には (iii) が成り立つことになる．

(iii) $y = x+1$ なる関係が成り立てば $y+1 = (x+1)+1 = x+2$ なので，x と $y+1$ の間には (iii) が成り立つことになる．

よって $y+1 \in A$ が示された． □

定義 6.2.4 ($\mathbb{N}$ の順序). $\mathbb{N}$ の元 x,y に対し,

$$\begin{aligned} x > y &\overset{\text{def}}{\iff} \text{(i) が成り立つ.} \\ x < y &\overset{\text{def}}{\iff} \text{(iii) が成り立つ.} \\ x \geq y &\overset{\text{def}}{\iff} \text{(i) または (ii) が成り立つ.} \\ x \leq y &\overset{\text{def}}{\iff} \text{(ii) または (iii) が成り立つ.} \end{aligned}$$

とする．$\mathbb{N}$ は $\leq$ に関して全順序集合の構造を持つ.

演習 6.2.5. 推移律 $x \leq y,\, y \leq z \Longrightarrow x \leq z$ を示せ.

演習 6.2.6. $\mathbb{N}$ の元 x, y, z, w に対し, 次が成り立つことを示せ.

(i) $x \leq y \Longrightarrow x+z \leq y+z$.

(ii) $x \leq y \Longrightarrow xz \leq yz$.

(iii) $x+z = y+z \Longrightarrow x = y$.

(iv) $xz = yz \Longrightarrow x = y$.

(v) $x+y = z+w,\, x < z \Longrightarrow y > w$

$\mathbb{N}$ の元 x, y に対し $x > y$ ならば定義より $x = y+u$ なる自然数 u が存在するが，定理 6.2.6(iii) よりこのような u は唯一つに限ることがわかる．この u を $x-y$ であらわす．

$\mathbb{N}$ の元 x, y に対し $x = yu$ なる自然数 u が存在すれば，定理 6.2.6(iv) よりこのような u は唯一つに限ることがわかる．この u を x/y であらわす．

定理 6.2.7. $\mathbb{N}$ は順序 $\leq$ に関して整列集合になる.

証明. A を空でない $\mathbb{N}$ の部分集合とするとき, A の最小限 $\min A$ が存在することを示せばよい.

$$A_* = \{x \in \mathbb{N} \mid \forall\, a \in A\ x \leq a\}$$

補題 6.2.3 より，$\min \mathbb{N} = 1$ だから，明らかに $1 \in A_*$. $a \in A$ に対し $a+1 \notin A_*$ だから，$A_* \neq \mathbb{N}$. このとき次をみたす $\mathbb{N}$ の元 x_* が存在する．

$$x_* \in A_*, \quad x_* + 1 \notin A_*.$$

なぜなら，このような x が存在しないとするとすべての $x \in A_*$ に対して $x+1 \in A_*$ となり, Peano の公理 (v) より $A = \mathbb{N}$ となってしまうからである．

$x_* \in A$ を示せば $x_* = \min A$ であることがわかる．$x_* + 1 \notin A_*$ より $x + 1 > a$ なるような $a \in A$ がある．よって $x \geq a$. 一方 $x_* \in A_*$ より $x \leq a$. ゆえに $x = a \in A$. □

自然数の冪

演習 6.2.8 (冪の定義). $\mathbb{N}$ の元 x に対し，$\mathbb{N}$ から $\mathbb{N}$ への写像 h_x で次の性質を満たすものが一意的に存在する事を示せ.

(i) $h_x(1) = x$.
(ii) すべての $y \in \mathbb{N}$ に対し $h_x(\varphi(y)) = h_x(y)\ x$.

$x^y = h_x(y)$ で y の x 乗，(y の x 次の冪) を定義する．

演習 6.2.9 (指数法則). 自然数 x, y, z に対し，次が成り立つことを示せ.

(i) $x^{y+z} = x^y \cdot x^z$.
(ii) $(x^y)^z = x^{yz}$.

ヒント：(i): 冪の定義 (i) より $x^1 = x$ である．冪の定義 (ii) を書き換えれば $z = 1$ の場合が証明される．あとは z に関する数学的帰納法で示す．(ii) も z に関する数学的帰納法で示せばよい.

注意 6.2.10. $F_1(x, y) = xy$ で F_1 を定義する．n を自然数とし

$$F_1(x, y), \ldots, F_n(x, y)$$

が定義されたとき次で $F_{\varphi(n)}(x, y)$ を定義する.

(i) すべての $x \in \mathbb{N}$ に対し $F_{\varphi(n)}(x, 1) = x$.
(ii) すべての $x, y \in \mathbb{N}$ に対し $F_{\varphi(n)}(x, \varphi(y)) = F_n(x, F_{\varphi(n)}(x, y))$.

すると $F_2(x, y) = x^y$ である．さて $F_n(x, y)$ はどんな関数であるか調べてみよう．

$$F_3(x, 2) = F_2(x, F_3(x, 1)) = F_2(x, x) = x^x$$

となる．順に

$$F_3(x,3) = F_2(x, F_3(x,2)) = F_2(x, x^x) = x^{x^x}$$
$$F_3(x,4) = F_2(x, F_3(x,3)) = F_2(x, x^{x^x}) = x^{x^{x^x}}$$
$$F_3(x,5) = F_2(x, F_3(x,4)) = F_2(x, x^{x^{x^x}}) = x^{x^{x^{x^x}}}$$
$$\cdots$$

となる．次に $F_4(x,2)$ について調べてみる．これは

$$F_4(2,2) = F_3(2, F_4(2,1)) = F_3(2,2) = 2^2 = 4$$
$$F_4(3,2) = F_3(3, F_4(3,1)) = F_3(3,3) = 3^{3^3} = 3^{27} = 7625597484987$$
$$F_4(4,2) = F_3(4, F_4(4,1)) = F_3(4,4) = 4^{4^4} = 4^{256} = 155 \text{ 桁の数}$$
$$\cdots$$

と急速に大きくなる関数である．$F_4(x,3)$ はどうなるであろうか?

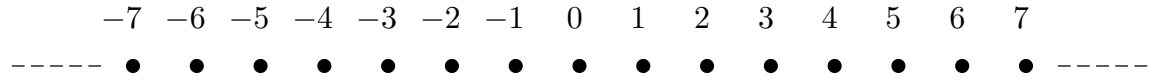
$$F_4(2,3) = F_3(2, F_4(2,2)) = F_3(2,4) = 2^{2^{2^2}} = 2^{2^4} = 2^{16} = 65536$$

であり，$F_4(3,3) = F_3(3, F_4(3,2)) = F_3(3, 3^{27})$ も，相当大きな数であることがわかる．

6.3 自然数から整数へ

自然数 x, y に対して，$x > y$ ならば $x - y$ は自然数であるが, $x \leq y$ のときは，$x - y$ は自然数の範囲の中では計算することはできない．このような計算を自由に行うため，中学では負の数を導入し，整数全体の集合

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$



なるものを考えた．ここでは，自然数全体の集合

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

を既知として，整数 $\mathbb{Z}$ を理論的に構成することを試みる．

自然数の順序対 (x, y) 全体の集合を $\mathbb{N}^2$ と書く．$\mathbb{N}^2$ に次で関係 $\sim$ を定義するとこれは同値関係になる．

$$(x, y) \sim (x', y') \quad \overset{\text{def}}{\iff} \quad x + y' = y + x'$$

この同値関係 $\sim$ による，(x, y) の同値類を $[(x, y)]$ と書き，この同値関係 $\sim$ による，$\mathbb{N}^2$ の商集合を $\mathbb{Z}$ と書く．

$$\mathbb{Z} = \mathbb{N}^2 / \sim$$

定義 6.3.1 (和). $\mathbb{Z}$ の元 $[(x_1, y_1)]$, $[(x_2, y_2)]$ に対して，その和を次で定義する．

$$[(x_1, y_1)] + [(x_2, y_2)] := [(x_1 + x_2, y_1 + y_2)].$$

演習 6.3.2. この定義がうまく定義されていること (well-definedness) を示せ．

演習 6.3.3 (和の法則). $\mathbb{Z}$ の元 $a_1 = [(x_1, y_1)]$, $a_2 = [(x_2, y_2)]$, $a_3 = [(x_3, y_3)]$ に対し，次が成り立つことを示せ．

(i) $a_1 + a_2 = a_2 + a_1$.
(ii) $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$.

ヒント: 演習 6.1.4 の結果を用いよ．

定理 6.3.4 ($\mathbb{N}$ の $\mathbb{Z}$ への埋め込み). 写像 $f : \mathbb{N} \to \mathbb{Z}$ を $a \mapsto [(\varphi(a), 1)]$ で定義すると f は単射で，次をみたす．

$$f(a + b) = f(a) + f(b), \quad \forall\, a, b \in \mathbb{N}$$

自然数 x に対し $f(x) = [(\varphi(x), 1)]$ と x を同一視し，$[(\varphi(x), 1)]$ を x と略記する．またこれにより $\mathbb{N}$ を $\mathbb{Z}$ の部分集合とみなすことにする．

定理 6.3.5 (零). $0 = [(1, 1)]$ とおくと，$\mathbb{Z}$ の任意の元 a に対し，$a + 0 = 0 + a = a$. また，$x \in \mathbb{N}$ に対し $[(x, x)] = 0$.

証明. $a = [(x, y)]$, $x, y \in \mathbb{N}$, とおくと $a + 0 = [(x + 1, y + 1)]$, $0 + a = [(1 + x, 1 + y)]$ なので

$$(x + 1, y + 1) \sim (1 + x, 1 + y) \sim (x, y)$$

を示せばよいがこれは易しい．$(x, x) \sim (1, 1)$ より $[(x, x)] = 0$ もわかる． □

自然数 x に対し $[(1, \varphi(x))]$ を，$-x$ と書く．

$$-\mathbb{N} := \{-x \mid x \in \mathbb{N}\}$$

とおくと，定理 6.2.1 より

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$$

である．

定理 6.3.6 (反数の存在). $\mathbb{Z}$ の任意の元 a に対し，$a + a' = a' + a = 0$ なる $\mathbb{Z}$ の元 a' が存在する．この a' を a の**反数**といい $-a$ であらわす．

証明. $a = [(x, y)]$, $x, y \in \mathbb{N}$, とおくと $a' = [(y, x)]$ とすれば

$$a + a' = [(x + y, x + y)] = [(1, 1)] = 0$$

□

定義 6.3.7 (差). $\mathbb{Z}$ の任意の元 a, b に対し，$a - b := a + (-b)$ とおく．このとき $a = [(x_1, y_1)]$, $b = [(x_2, y_2)]$ とおくと，$a - b = (x_1 + y_2, y_1 + x_2)$ となる．

演習 6.3.8. この定義がうまく定義されていることを確認せよ．すなわち次を確認せよ．

$$(x_1, y_1) \sim (x_1', y_1'),\ (x_2, y_2) \sim (x_2', y_2') \implies (x_1 + y_2, y_1 + x_2) \sim (x_1' + y_2', y_1' + x_2')$$

定理 6.3.9. 次の条件をみたす写像

$$\alpha : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (x, y) \mapsto \alpha(x, y)$$

が一意的に存在する．

(i) $x, y \in \mathbb{N}$ ならば $\alpha(x, y) = xy$.
(ii) $\mathbb{Z}$ は加法 $+$ と乗法 $xy = \alpha(x, y)$ について，可換環をなす.

証明. 補題 5.2.6 より，条件 (i), (ii) をみたす α は任意の $x, y \in \mathbb{N}$ と任意の $z \in \mathbb{Z}$ について,

$$\alpha(z, 0) = \alpha(0, z) = 0 \tag{6.1}$$
$$\alpha(x, -y) = \alpha(-x, y) = -\alpha(x, y) \tag{6.2}$$
$$\alpha(-x, -y) = \alpha(x, y) \tag{6.3}$$

をみたさなければならない．逆に (i) および (6.1), (6.2), (6.3) で α を定義すれば，(ii) をみたすことは容易に示される． □
これによって $\mathbb{Z}$ に乗法を定義すれば，$\mathbb{Z}$ のなかで自由に加法，乗法ができることが分かる

定義 6.3.10 ($\mathbb{Z}$ の順序). $\mathbb{Z}$ の任意の元 a, b に対し，$a = [(x_1, y_1)]$, $b = [(x_2, y_2)]$ とするとき

$$a < b \overset{\text{def}}{\iff} x_2 + y_1 > x_1 + y_2$$

で $a < b$ を定義する．これを $b > a$ とも書く．また

$$a \leq b \overset{\text{def}}{\iff} a = b \text{ または } a < b$$

とする．これを $b \geq a$ と書くこともある．$\mathbb{Z}$ は $\leq$ に関して全順序集合の構造を持つ.

演習 6.3.11. この $a < b$ がうまく定義されていることを確認せよ．さらに $\mathbb{Z}$ が全順序集合の構造が入ることを確認せよ.

演習 6.3.12. $a > 0 \iff a \in \mathbb{N}$ を示せ.

定理 6.3.13. 整数 $\mathbb{Z}$ の元 a, b, c に対し，次が成り立つ.

(i) $a > b$ ならば $a + c > b + c$.
(ii) $a > 0, b > 0$ ならば $ab > 0$.

証明. (i): $a = [(x_1, y_1)]$, $b = [(x_2, y_2)]$, $c = [(x_3, y_3)]$ とする．$a > b$ より $x_1 + y_2 > x_2 + y_1$．よって $x_1 + y_2 + x_3 + y_3 > x_2 + y_1 + x_3 + y_3$．これより

$$a + c = [(x_1 + x_3, y_1 + y_3)] > [(x_2 + x_3, y_2 + y_3)] = b + c.$$

(ii) は，演習 6.3.12 と，積の定義から明らか. □

第 7 章

有理数の完備化

1.4
1.41
1.414
1.4142
1.41421
1.414213
1.4142135
1.41421356
...

有理数の数列

$$1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, 1.41421356, \cdots \longrightarrow \sqrt{2}$$

は有理数の範囲では収束しない．数列の収束を議論する際には，数として有理数のみを考えているのでは不十分であると考えられる．ここではコーシー列の考えを用いて，有理数の完備化として実数を導入方法を説明する．実数の導入方法には有理数の切断によるものなど他にいろいろあるが，どの方法で構成しても，互いに同型であることがわかっている．実数を導入する別の方法である有理数の切断との関係も少し説明する．併せて有理数の別の完備化である p 進数も導入する．

7.1 有理数の完備化

まずはコーシー列の定義から始めよう.

定義 7.1.1. 数列 $\{a_n\}_{n=1,2,\dots}$ が**コーシー列** (Cauchy[*1] sequence) であるとは，任意の正の数 ε に対しある正の整数 N が存在して $m, n \geq N$ ならば $|a_m - a_n| < \varepsilon$ となるときをいう．論理記号を用いるとコーシー列であるための条件は次のように書ける.

$$\forall \varepsilon > 0\ \exists N\ \forall m, n\ (m, n \geq N \text{ ならば } |a_m - a_n| < \varepsilon)$$

演習 7.1.2. $\{a_n\}$ がコーシー列であると言う命題の，否定命題を作れ.

演習 7.1.3. $\{a_n\}$ がコーシー列である事は次の条件と同値であることを示せ．任意の正の数 ε に対しある正の整数 N が存在して $n \geq N$ ならば $|a_n - a_N| < \varepsilon$ となる.

以後，コーシー列であるような有理数の数列を**有理コーシー列**といい，有理コーシー列の全体を $\mathrm{Cauchy}(\mathbb{Q})$ であらわす.

$$\mathrm{Cauchy}(\mathbb{Q}) = \{\{a_n\}_{n=1,2,\dots} \mid \text{有理コーシー列}\}$$

記号を簡単にするため，しばしば $\{a_n\}_{n=1,2,\dots}$ を単に $\{a_n\}$ と略記する．2 つの有理コーシー列 $\{a_n\}, \{b_n\}$ に対して関係 $\sim$ を次で定義する.

$$\{a_n\} \sim \{b_n\} \quad \overset{\text{def}}{\iff} \quad \forall \varepsilon > 0\ \exists N \text{ s.t. } n \geq N \text{ ならば } |a_n - b_n| < \varepsilon$$

補題 7.1.4. これは同値関係である.

証明. 反射律，対称律は明らかなので，推移律のみ示す．コーシー列 $\{a_n\}, \{b_n\}, \{c_n\}$ が $\{a_n\} \sim \{b_n\}, \{b_n\} \sim \{c_n\}$ とする．すると 任意の正の数 ε に対し,

$$\exists N_1 \text{ s.t. } n \geq N_1 \text{ ならば } |a_n - b_n|_p < \varepsilon/2$$
$$\exists N_2 \text{ s.t. } n \geq N_2 \text{ ならば } |b_n - c_n|_p < \varepsilon/2$$

が成り立つ．ここで $N = \max\{N_1, N_2\}$ とおくと

$$n \geq N \text{ ならば } |a_n - c_n|_p \leq |a_n - b_n|_p + |b_n - c_n|_p < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

よって $\{a_n\} \sim \{c_n\}$ がわかる. □

[*1] Augustin Louis Cauchy, (1789 – 1857）はフランスの数学者

有理コーシー列全体の空間 Cauchy($\mathbb{Q}$) のこの同値関係による商集合を有理数の完備化といい $\widehat{\mathbb{Q}}$ であらわす.

$$\widehat{\mathbb{Q}} = \mathrm{Cauchy}(\mathbb{Q})/\sim$$

コーシー列について基本的な性質をまとめておこう.

補題 7.1.5. コーシー列 $\{a_n\}$ は有界である.

証明. $\{a_n\}$ は コーシー列だから正の数 ε_0 に対しある番号 N があって

$$\begin{array}{lrll} & m > n \geq N & \text{ならば} & |a_m - a_n| < \varepsilon_0. \\ \text{特に} & m > N & \text{ならば} & |a_m - a_N| < \varepsilon_0. \\ \text{つまり} & m > N & \text{ならば} & a_N - \varepsilon_0 < a_m < a_N + \varepsilon_0. \\ \text{よって} & m > N & \text{ならば} & |a_m| < |a_N| + \varepsilon_0 \end{array}$$

ここで $K = \max\{|a_1|, |a_2|, \ldots, |a_N|, |a_N| + \varepsilon_0\}$ とおくとすべての n に対し $|a_n| \leq K$ となるので $\{a_n\}$ は有界である. □

補題 7.1.6. $\{a_n\}, \{b_n\}$ がコーシー列ならば $\{a_n + b_n\}, \{a_n b_n\}$ もコーシー列である.

証明. まず $\{a_n + b_n\}$ がコーシー列であることを示す. $\{a_n\}, \{b_n\}$ はコーシー列であることより, 任意の正の数 ε に対し次をみたす M_1, M_2 が存在する.

$$\begin{aligned} m, n \geq M_1 \text{ ならば } |a_m - a_n| < \varepsilon/2 \\ m, n \geq M_2 \text{ ならば } |b_m - b_n| < \varepsilon/2 \end{aligned}$$

$M = \max\{M_1, M_2\}$ とおけば, $m, n \geq M$ ならば

$$\begin{aligned} |(a_m + b_m) - (a_n + b_n)| &= |(a_m - a_n) + (b_m - b_n)| \\ &\leq |a_m - a_n| + |b_m - b_n| \\ &< \varepsilon/2 + \varepsilon/2 = \varepsilon \end{aligned}$$

となるので, $\{a_n + b_n\}$ はコーシー列であることがわかる.

次に $\{a_n b_n\}$ がコーシー列であることを示す. $\{a_n\}, \{b_n\}$ はコーシー列なので有界であり, すべての n に対して

$$|a_n| < K, \quad |b_n| < K$$

をみたす正定数 K が存在する. また $\{a_n\}, \{b_n\}$ はコーシー列であることより, 任意の正の数 ε に対し次をみたす N_1, N_2 が存在する.

$$\begin{aligned} m, n \geq N_1 \text{ ならば } |a_m - a_n| < \frac{\varepsilon}{2K} \\ m, n \geq N_2 \text{ ならば } |b_m - b_n| < \frac{\varepsilon}{2K} \end{aligned}$$

$N = \max\{N_1, N_2\}$ とおけば $m, n \geq N$ ならば

$$\begin{aligned}
|a_m b_m - a_n b_n| &= |a_m(b_m - b_n) + (a_m - a_n)b_n| \\
&\leq |a_m(b_m - b_n)| + |(a_m - a_n)b_n| \\
&= |a_m||b_m - b_n| + |a_m - a_n||b_n| \\
&< K|b_m - b_n| + |a_m - a_n|K \\
&< K\frac{\varepsilon}{2K} + \frac{\varepsilon}{2K}K \\
&= \varepsilon
\end{aligned}$$

となって $\{a_n b_n\}$ はコーシー列であることがわかる. □

定義 7.1.7 (和と積). $\widehat{\mathbb{Q}}$ の元 $\alpha = [\{a_n\}]$ と $\beta = [\{b_n\}]$ に対し，その和 $\alpha + \beta$ と積 $\alpha \cdot \beta$ を次で定義する.

$$\begin{aligned}
\alpha + \beta &:= [\{a_n + b_n\}] \\
\alpha \cdot \beta &:= [\{a_n b_n\}]
\end{aligned}$$

これがうまく定義されている (well-defined である) ことを証明しよう. そのためには，代表元のとり方によらず，同値類で和，積が確定していること，すなわち $\{a_n\} \sim \{a'_n\}$, $\{b_n\} \sim \{b'_n\}$ ならば

$$\{a_n + b_n\} \sim \{a'_n + b'_n\}, \quad \{a_n b_n\} \sim \{a'_n b'_n\}$$

であることを示せばよい.

まず $\{a_n + b_n\} \sim \{a'_n + b'_n\}$ を示す. $\{a_n\} \sim \{a'_n\}$, $\{b_n\} \sim \{b'_n\}$ より，任意の正の数 ε に対し次をみたす M_1, M_2 が存在する.

$$\begin{aligned}
n \geq M_1 \quad &\text{ならば} \quad |a_n - a'_n| < \varepsilon/2 \\
n \geq M_2 \quad &\text{ならば} \quad |b_n - b'_n| < \varepsilon/2
\end{aligned}$$

$M = \max\{M_1, M_2\}$ とおけば，$n \geq M$ ならば

$$\begin{aligned}
|(a_n + b_n) - (a'_n + b'_n)| &= |(a_n - a'_n) + (b_n - b'_n)| \\
&\leq |a_n - a'_n| + |b_n - b'_n| \\
&< \varepsilon/2 + \varepsilon/2 = \varepsilon
\end{aligned}$$

となるので，$\{a_n + b_n\} \sim \{a'_n + b'_n\}$ であることがわかる.

次に $\{a_n b_n\} \sim \{a'_n b'_n\}$ を示す. $\{a_n\}$, $\{b'_n\}$ はコーシー列なので有界であり，すべての n に対して

$$|a_n| < K, \quad |b'_n| < K$$

をみたす正定数 K が存在する．また $\{a_n\} \sim \{a'_n\}$, $\{b_n\} \sim \{b'_n\}$ であることより，任意の正の数 ε に対し次をみたす N_1, N_2 が存在する．

$$\begin{aligned} n \geq N_1 \quad &\text{ならば} \quad |a_n - a'_n| < \varepsilon/(2K) \\ n \geq N_2 \quad &\text{ならば} \quad |b_n - b'_n| < \varepsilon/(2K) \end{aligned}$$

$N = \max\{N_1, N_2\}$ とおけば $n \geq N$ ならば

$$\begin{aligned} |a_n b_n - a'_n b'_n| &= |a_n(b_m - b'_n) + (a_n - a'_n)b'_n| \\ &\leq |a_n(b_n - b'_n)| + |(a_n - a'_n)b'_n| \\ &= |a_n||b_n - b'_n| + |a_n - a'_n||b'_n| \\ &< K|b_n - b'_n| + |a_n - a'_n|K \\ &< K\varepsilon/(2K) + (\varepsilon/(2K))K = \varepsilon \end{aligned}$$

となって $\{a_n b_n\} \sim \{a'_n b'_n\}$ であることがわかる．

定理 7.1.8. $\widehat{\mathbb{Q}}$ の元 $\alpha = [\{a_n\}]$, $\beta = [\{b_n\}]$, $\gamma = [\{c_n\}]$ に対し，次が成り立つ．

(i) 加法に関する交換律: $\alpha + \beta = \beta + \alpha$.
(ii) 加法に関する結合律: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
(iii) 乗法に関する交換律: $\alpha \cdot \beta = \beta \cdot \alpha$.
(iv) 乗法に関する結合律: $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.
(v) 分配律: $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$, $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$.

演習 7.1.9. 定理 7.1.8 を証明せよ．これらは，有理数の場合のそれぞれの法則の帰結である．証明したい式の両辺の代表元である有理コーシー列が，対応する等号が成り立つように取れればよい．丁寧に書き下すのは面倒かもしれないが，証明は易しい．

定義 7.1.10 (順序). $\widehat{\mathbb{Q}}$ の元 $\alpha = [\{a_n\}]$ と $\beta = [\{b_n\}]$ に対し，$\alpha \leq \beta$ を次で定義する．

$$\alpha \leq \beta \quad \overset{\text{def}}{\iff} \quad \exists N \text{ s.t. } n \geq N \text{ ならば } a_n \leq b_n$$

演習 7.1.11. この定義は well-defined で， これにより $\widehat{\mathbb{Q}}$ は順序集合になることを示せ．

定義 7.1.12 (絶対値). 実数 $\alpha = [\{a_n\}]$ に対し，その絶対値 $|\alpha|$ を次で定義する．

$$|\alpha| = \begin{cases} \alpha = [\{a_n\}] & \alpha \geq 0 \\ -\alpha = [\{-a_n\}] & \alpha < 0 \end{cases}$$

7.2 実数

前節では有理数の完備化 $\widehat{\mathbb{Q}}$ に和と積を定義し，交換律・結合律などの演算規則が成り立つ事を見た．完備化の元を普通の数と同じ様に扱いたいので，有理コーシー列 $\{a_n\}$ の前節の同値関係による同値類 $\alpha := [\{a_n\}]$ を**実数**と呼ぶ事にして，実数全体の集合を $\mathbb{R}$ で表す．次の定理は明らかであろう．

定理 7.2.1 (有理数の実数への埋め込み). 有理数 p/q に対し，数列 $a_n = p/q,\ n = 1, 2, \ldots$ は定数数列であり，特にコーシー列である．この定数数列を $\{p/q\}$ と書く．写像 $f : \mathbb{Q} \to \mathbb{R}$ を $f(p/q) = [\{p/q\}]$ で定義すると，f は単射で

(i) $f(p/q) + f(p'/q') = f(p/q + p'/q')$,
(ii) $f(p/q) \cdot f(p'/q') = f(p/q \cdot p'/q')$.
(iii) $p/q \leq p'/q'$ ならば $f(p/q) \leq f(p'/q')$.

有理数 p/q に対し p/q と $f(p/q)$ を同一視し，$f(p/q)$ をしばしば p/q と書く．
$0 = f(0) = [\{0\}]$, $1 = f(1) = [\{1\}]$ とおくとすべての実数 $\alpha = [\{a_n\}]$ に対し

$$\alpha + 0 = 0 + \alpha = \alpha, \quad \alpha \cdot 0 = 0 \cdot \alpha = 0, \quad \alpha \cdot 1 = 1 \cdot \alpha = \alpha$$

が成り立つ．

実数列に対してもコーシー列の概念が定義される．

定義 7.2.2. 実数列 $\{\alpha_n\}$ が**コーシー列**であるとは次の条件をみたすことをいう．

$$\forall \varepsilon > 0\ \exists N\ \forall m, n\ (m, n \geq N \text{ ならば } |\alpha_m - \alpha_n| < \varepsilon)$$

定理 7.2.3 (実数の完備性). 実数列 $\{\alpha_n\}$ がコーシー列ならば収束する[*2].

証明. 数列 $\{\alpha_n\}$ はコーシー列であるから，任意の正の数 ε に対し

$$\exists N\ \forall m, n\ \big(m, n \geq N \text{ ならば } |\alpha_m - \alpha_n| < \varepsilon\big)$$

となる．ここで α_n は実数なので，有理コーシー列 $\{a_{n,k}\}_{k=1,2,\ldots}$ を用いて，$\alpha_n = [\{a_{n,k}\}_{k=1,2,\ldots}]$ と書くと，この条件は次のようになる．

$$\exists N\ \forall m, n\ \big(m, n \geq N \text{ ならば } \exists M\ \forall k\ (k \geq M \text{ ならば } |a_{m,k} - a_{n,k}| < \varepsilon)\big)$$

これを次のように書き直しておく．

$$\exists N\ \forall m, n\ \exists M\ \forall k\ \big((m, n \geq N,\ k \geq M\ ) \text{ ならば } |a_{n,k} - a_{m,k}| < \varepsilon\big) \tag{7.1}$$

[*2] コーシー列が収束するときその空間は**完備** (complete) であるという．

$b_k = a_{k,k}$, $k = 1, 2, \ldots$ とおくと，$M_1 = \max\{N, M\}$ とおくことにより，

$$\exists N\ \forall n\ \exists M_1\ \forall k\ \big((n \geq N,\ k \geq M_1\ ) \text{ならば } |a_{n,k} - b_k| < \varepsilon\big)$$

を得る．もし数列 $\{b_k\}_{k=1,2,\ldots}$ が 有理コーシー列であることが示されれば，$\beta = [\{b_k\}]$ と書くとき，これは

$$\exists N\ \forall n\ \big(n \geq N \text{ ならば } |\alpha_n - \beta| < \varepsilon\big)$$

となり，実数列 $\{\alpha_n\}$ が実数 β に収束していることを示している．$\{b_k\}$ は明らかに有理数列だからコーシー列であることを示す．

さて $\{a_{n,k}\}_{k=1,2,\ldots}$ はコーシー列であるから，任意の $\varepsilon > 0$ に対し，

$$\exists N_n\ \forall i, j\ \big(i, j > N_n \text{ ならば } |a_{n,i} - a_{n,j}| < \varepsilon\big) \tag{7.2}$$

さて任意の $\varepsilon > 0$ に対し，(7.1) での N をとり N 以上の n を固定して (7.2) での N_n をとる．$N_* = \max\{N, N_n\}$ とおけば，$i, j \geq N_*$ のとき，

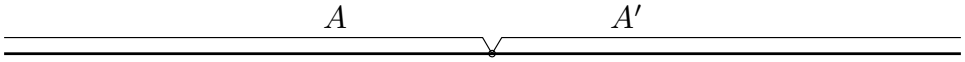
$$\begin{aligned} |b_i - b_j| &= |a_{i,i} - a_{j,j}| \\ &\leq |a_{i,i} - a_{n,i}| + |a_{n,i} - a_{n,j}| + |a_{n,j} - a_{j,j}| \\ &< \varepsilon + \varepsilon + \varepsilon = 3\varepsilon \end{aligned}$$

となり，$\{b_k\}$ がコーシー列であることが示される． □

■切断　有理数の切断で実数を定義する流儀もある．ここでは有理コーシー列を用いた実数の定義と有理数の切断を用いた実数の定義との対応を見る．

定義 7.2.4 (有理数の切断). 有理数の部分集合の対 $(A|A')$ が次を満たすとき，**切断** (cut) であるという．

(i) A' は A の補集合である．即ち $A' = \mathbb{Q} \setminus A$
(ii) $a \in A$, $a' \in A'$ ならば $a < a'$
(iii) $A \neq \varnothing$, $A' \neq \varnothing$



切断 $(A|A')$ が与えられたとき，次の 4 つの場合が一応は考えられる．

(1) A に最大の有理数なく，A' に最小の有理数なし．
(2) A に最大の有理数なく，A' に最小の有理数あり．
(3) A に最大の有理数あり，A' に最小の有理数なし．
(4) A に最大の有理数あり，A' に最小の有理数あり．

ところが，実際には (4) は起こり得ない．なぜなら A に最大の有理数 A があり， A' に最小の有理数 B があるとすると $a < b$ であり，$a < \frac{a+b}{2} < b$ なので有理数 $\frac{a+b}{2}$ が A にも A' にも属さないことになって矛盾となるからである．

(2) のとき，$a = \max A$ とおくと a は有理数で，切断 $(A|A')$ は $A = \{x \in \mathbb{Q}\, z | \, x < a\}$, $A' = \{x \in \mathbb{Q} \,|\, x \geq a\}$ と表される．このとき切断 $(A|A')$ は有理数 a を定義するという．同様に (3) のときも，切断 $(A|A')$ は $a = \min A'$ とおけば $A = \{x \in \mathbb{Q} \,|\, x \leq a\}$, $A' = \{x \in \mathbb{Q} \,|\, x > a\}$ と表される．このときも切断 $(A|A')$ は有理数 a を定義するという．(1) のとき切断 $(A|A')$ は無理数を定義するという．(3) のタイプの切断 $(A|A')$ に対しては $a = \max A$ として $(A \setminus \{a\}, A' \cup \{a\})$ を考えるとこれは (2) 型の切断になる．従って (3) のタイプの切断が現れたらこのようにして (2) のタイプの切断を考えることにする．(1) または (2) のタイプの切断を（有理数の切断で構成された）**実数**という．

有理数の切断から実数を構成する方法が，有理数の完備化と実質同じであることを示すには，コーシー列から切断を構成する方法と切断からコーシー列を構成する方法を述べそれらが互いに逆の対応であることを示せば[*3]良い．

有理コーシー列から有理数の切断を構成する事

有理コーシー列 $\{a_n\}$ に対し次で切断 $(A|A')$ を定める．

$$A = \{a \in \mathbb{Q} \mid \exists N\ \forall n \geq N\ a < a_n\}, \quad A' = \mathbb{Q} \setminus A \tag{7.3}$$

明らかに $A' = \{a' \in \mathbb{Q} \mid \forall N\ \exists n > N\ a_n \leq a'\}$ である．

演習 7.2.5. 2 つの有理コーシー列 $\{a_n\}$, $\{b_n\}$ が $\{a_n\} \sim \{b_n\}$ を満たすとき

$$B = \{b \in \mathbb{Q} \mid \exists N\ \forall n \geq N\ b < b_n\}, \quad B' = \mathbb{Q} \setminus B \tag{7.4}$$

とおけば $A = B$ である．

有理数の切断から有理コーシー列を構成する事

(1) または (2) のタイプの有理数の切断 $(B|B')$ が与えられたとき，次のようにしてコーシー列を作る．まず $a_1 \in X$, $a'_1 \in X'$ なるように a_1, a'_1 を選ぶ．$a_1 < a'_1$ である．

さて $a_i \in X$, $a'_i \in X'$ が与えられたとき，次の規則で a_{i+1}, a'_{i+1} を定める．

(i) $\frac{a_i+a'_i}{2} \in B$ のとき $a_{i+1} = \frac{a_i+a'_i}{2}$, $a'_{i+1} = a'_i$ とおく．
(ii) $\frac{a_i+a'_i}{2} \in B'$ のとき $a_{i+1} = a_i$, $a'_{i+1} = \frac{a_i+a'_i}{2}$ とおく．

いずれの場合も $0 \leq a_{i+1} - a_i \leq \frac{1}{2}(a'_i - a_i)$ である．初期値 a_1, a'_1 からこの規則で決ま

[*3] 有理数の切断から実数の加法乗法を定義して，それらが有理数の完備化の加法乗法と同じであることを示す必要があるが，長くなるので詳細は省略する．

る数列 $\{a_n\}, \{a'_n\}$ について，$n \leq m$ のとき

$$\begin{aligned} a_m - a_n =& (a_m - a_{m-1}) + \cdots + (a_{n+1} - a_n) \\ \leq& \frac{1}{2^{m-1}}(a'_1 - a_1) + \cdots + \frac{1}{2^{n-1}}(a'_1 - a_1) \\ =& \frac{a'_1 - a_1}{2^{n-1}}(2^{n-m} + \cdots + 1) < \frac{a'_1 - a_1}{2^{n-1}}\left(1 - \frac{1}{2}\right) = \frac{a'_1 - a_1}{2^n} \end{aligned}$$

なので，有理数列 $\{a_n\}$ はコーシー列である．このとき構成から次がわかる．

$$a_1 \leq a_2 \leq \cdots \leq a_n < a'_n \leq \cdots \leq a'_2 \leq a'_1, \quad a'_n - a_n = \frac{1}{2^{n-1}}(a'_1 - a_1) \tag{7.5}$$

次の 2 つの補題が，上の 2 つの構成が互いに逆である事を示している．

補題 7.2.6. 上で構成したコーシー列から (7.3) で切断 $(A|A')$ を定義すると $A = B$.

証明. $A \subset B$ **の証明:** $a \in A$ を取る．$a < a_n$ なる $a_n \in B$ が存在するので $(B|B')$ が切断であることから $a \in B$.
$A \supset B$ **の証明:** $x \in B$ をとる．上で構成した a'_n は B' の元なので $x < a'_n$ がわかる．$x \in A'$ と仮定すると，任意の n に対し $a_n \leq x$ となる．このとき，(7.5) が成り立ち，$a_n \leq x < a'_n$ である．$x < y$ なる y を取る．$\frac{1}{2^{n-1}}(a'_1 - a_1) < y - x$ なる n を取ると

$$0 < a'_n - x \leq a'_n - a_n = \frac{1}{2^{n-1}}(a'_1 - a_1) < y - x$$

なので $a'_n < y$ となり $y \in B'$ がわかる．よって x は B の最大元となり，$(B|B')$ が (1) または (2) のタイプの切断である事に反する．従って $x \in A'$ ではあり得ず $x \in A$ でなければならない． □

補題 7.2.7. 有理コーシー列 $\{b_n\}$ から (7.4) で切断 $(B|B')$ を作り，切断 $(B|B')$ から上の手続きでコーシー列 $\{a_n\}$ を作ると $\{a_n\} \sim \{b_n\}$ である．

証明. 切断 $(B|B')$ から上述の手続きで $\{a_n\}, \{a'_n\}$ を作ると (7.5) を満たす．従って，任意の正の数 ε に対し，ある N が存在して，$m, n \geq N$ ならば

$$|a_m - a_n| < \varepsilon/3, \quad |b_m - b_n| < \varepsilon/3, \quad 0 < a'_n - a_n < \varepsilon/3$$

とできる．構成より各 a_n に対し $m \geq N_n$ ならば $a_n < b_m$ を満たす N_n を取ることができる，$a'_n \in A'$ より m をうまく選んで $b_m \leq a'_n$ とできる．m はいくらでも大きく取れ $a_n \leq a_m < b_m \leq a'_n$ より $|a_m - b_m| \leq |a'_n - a_n|$ となる．従って $n \geq N$ ならば

$$\begin{aligned} |a_n - b_n| \leq& |a_n - a_m| + |a_m - b_m| + |b_m - b_n| \\ \leq& |a_n - a_m| + |a'_n - a_n| + |b_m - b_n| < \varepsilon \end{aligned}$$

となり証明を完了する． □

7.3 p 進数

前 2 節で有理数の完備化として実数を構成した．本節では有理数の p 進完備化と呼ばれる有理数の別の完備化を説明する．p 進完備化で得られる数は p 進数と呼ばれ，実数の世界に慣れた目で見ると奇妙な現象も時々起こる．しかし慣れると実は非常に統制のとれた数体系であることがわかり，解ける方程式が増える．本格的な解説は専門書に譲り，本節ではできるだけ簡単な説明をする．

p を素数とする．0 でない有理数 $x \in \mathbb{Q}$ を $x = p^k m/n$ （但し k は整数で，m と n は p で割れない整数）と書くとき，x の p **進ノルム** $|x|_p$ を次で定める．

$$|x|_p = p^{-k}$$

$x = 0$ のときはその p 進ノルムは 0, すなわち $|0|_p = 0$ としておく．

定理 7.3.1. x, y を有理数とするとき，次が成り立つ．

$$|xy|_p = |x|_p|y|_p, \qquad |x+y|_p \leq |x|_p + |y|_p$$

証明. x, y のいずれかが 0 であれば，示すべき式は自明であるから，x, y ともに 0 でないとする．$x = p^k q$, $y = p^l r$ と書く．但し k, l は整数で，q, r は分母分子が p で割れない有理数とする．$xy = p^{k+l}(qr)$ なので

$$|xy|_p = p^{-k-l} = p^{-k}p^{-l} = |x|_p|y|_q$$

必要なら x と y を入れ替える事により，$k \leq l$ と仮定してよいから，

$$|x+y|_p = p^{-k} \leq p^{-k} + p^{-l} = |x|_p + |y|_p$$

となり証明が終わる． □

この p 進ノルム $|x|_p$ を絶対値 $|x|$ の代わりに使って，$\mathbb{Q}$ の完備化を考える事ができる．以下説明しよう。

有理数列 $\{x_n\}$ が p **進コーシー列**であるとは，次の性質を満たす時をいう．

任意の $k \in \mathbb{N}$ に対しある番号 N が存在して $n \geq N$ ならば $|x_n - x_N|_p < p^{-k}$

2 つの p 進コーシー列 $\{x_n\}, \{y_n\}$ に対して関係 $\sim_p$ を次で定義する．

$$\{x_n\} \sim_p \{y_n\} \quad \overset{\text{def}}{\iff} \quad \forall k \in \mathbb{N}\ \exists N \text{ s.t. } n \geq N \text{ ならば } |x_n - y_n|_p < p^{-k}$$

演習 7.3.2. $\sim_p$ は同値関係であることを示せ.

p 進有理コーシー列全体をこの同値関係で割ったものを p **進有理数**といい $\mathbb{Q}_p$ で表す．整数コーシー列で表される $\mathbb{Q}_p$ の元を p **進整数**といい，p 進整数全体を $\mathbb{Z}_p$ で表す．

例 7.3.3. 数列 $\{p^n\}_{n=1,2,\dots}$ は $\mathbb{Z}_p$ 内で 0 に収束する．

例 7.3.4. $\{a_n\}$ を $0,1,\dots,p-1$ のいずれかの値をとる数列とし

$$x_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n$$

とおく． 任意の自然数 N に対して．$n > N$ のとき，

$$x_n - x_N = a_{N+1} p^{N+1} + \cdots + a_n p^n$$

なので，$|x_n - x_N|_p \le p^{-N-1}$ となり，$\{x_n\}$ は p 進コーシー列である事がわかる．

p 進有理数 $\alpha \in \mathbb{Q}_p$ は次の p **進展開**

$$\alpha = p^k(a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots), \quad k \in \mathbb{Z},\ a_i \in \{0,1,\dots,p-1\},\ a_0 \neq 0$$

の形に一意的に表わされる．$|\alpha|_p = p^{-k}$ で，$k \ge 0$ のとき α は p 進整数（$\alpha \in \mathbb{Z}_p$）である．

$a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots$ は各 n に対し $\mathbb{Z}/p^{n+1}\mathbb{Z}$ の元を定めていると考えることもできる．その様に考えると p 進整数は

$$x_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots \pmod{p^{n+1}}$$

の $n \to \infty$ とした極限である．

p 進有理数には上の p 進展開を用いて（或いは，定義 7.1.7 と同様にして），和と積を定義することができる．

以後 $x_n \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ $(n = 0,1,2,\dots)$ に $x_{k+1} = x_k \bmod p^{k+1}$ $(k = 0,1,2,\dots)$ という条件を課して，$\{x_n\}$ が定める p 進整数 x を $x = (x_n)_{n=1,2,\dots}$ と書く．

定理 7.3.5. $x_0 \neq 0$ ならば $xy = 1$ を満たす p 進整数 $y = (y_n)_{n=1,2,\dots}$ が存在する．

証明. $x_0 y_0 \equiv 1 \bmod p$ なる y_0 を取る．$x_0 \not\equiv 0 \bmod p$ よりこれは常に可能である．

$x_{n-1} y_{n-1} \equiv 1 \bmod p^n$ を満たす $y_{n-1} \in \mathbb{Z}/p^n\mathbb{Z}$ が存在するとして $x_n y_n = 1 \bmod p^{n+1}$ を満たす y_n が存在する事を示す．そのために x_{n-1}, y_{n-1} を整数と思って

$$x_n = x_{n-1} + a p^n, \quad y_n = y_{n-1} + b p^n, \quad a, b \in \{0,1,\dots,p-1\}$$

と置く．$x_{n-1} y_{n-1}$ も p 進展開を用いて

$$x_{n-1} y_{n-1} = 1 + c p^n \bmod p^{n+1}, \quad c \in \{0,1,\dots,p-1\}$$

と表しておくと

$$\begin{aligned} x_n y_n =& (x_{n-1} + ap^n)(y_{n-1} + bp^n) = x_{n-1}y_{n-1} + (a+b)p^n \bmod p^{n+1} \\ =& 1 + (a+b+c)p^n \bmod p^{n+1} \end{aligned}$$

を得る．従って $a+b+c = 0 \bmod p$ を満たすように b を選べば良い． □

つまり，次の p 進展開で表される p 進整数の逆元は $\mathbb{Z}_p$ の元として存在する．

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots, \quad a_i \in \{0, 1, \ldots, p-1\},\ a_0 \neq 0$$

言い換えると $|x|_p = 1$ を満たす p 進整数 x の逆元 x^{-1} は存在し $\mathbb{Z}_p$ の元である．

例 7.3.6. 3 進整数環 $\mathbb{Z}_3$ では次式が成り立つ．右辺の 2 倍が 1 になる事を確認せよ．

$$2^{-1} = 2 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + 1\cdot 3^5 + \cdots$$

$\mathbb{Z}_3$ での 4^{-1} と 5^{-1} も参考に示しておく．

$$\begin{aligned} 4^{-1} =& 1 + 2\cdot 3 + 0\cdot 3^2 + 2\cdot 3^3 + 0\cdot 3^4 + 2\cdot 3^5 + 0\cdot 3^6 + 2\cdot 3^7 + \cdots \\ 5^{-1} =& 2 + 0\cdot 3 + 1\cdot 3^2 + 2\cdot 3^3 + 0\cdot 3^4 + 1\cdot 3^5 + 2\cdot 3^6 + 0\cdot 3^7 + \cdots \end{aligned}$$

例 7.3.7. 5 進整数環 $\mathbb{Z}_5$ では次式が成り立つ．

$$\begin{aligned} 2^{-1} =& 3 + 2\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 2\cdot 5^4 + 2\cdot 5^5 + 2\cdot 5^6 + 2\cdot 5^7 + \cdots \\ 3^{-1} =& 2 + 3\cdot 5 + 1\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + 3\cdot 5^5 + 1\cdot 5^6 + 3\cdot 5^7 + \cdots \\ 4^{-1} =& 4 + 3\cdot 5 + 3\cdot 5^2 + 3\cdot 5^3 + 3\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^6 + 3\cdot 5^7 + \cdots \end{aligned}$$

例 7.3.8. 7 進整数環 $\mathbb{Z}_7$ では次式が成り立つ．

$$\begin{aligned} 2^{-1} =& 4 + 3\cdot 5 + 3\cdot 7^2 + 3\cdot 7^3 + 3\cdot 7^4 + 3\cdot 7^5 + 3\cdot 7^6 + 3\cdot 7^6 + 3\cdot 7^7 + \cdots \\ 3^{-1} =& 5 + 4\cdot 5 + 4\cdot 7^2 + 4\cdot 7^3 + 4\cdot 7^4 + 4\cdot 7^5 + 4\cdot 7^6 + 4\cdot 7^6 + 4\cdot 7^7 + \cdots \\ 4^{-1} =& 2 + 5\cdot 5 + 1\cdot 7^2 + 5\cdot 7^3 + 1\cdot 7^4 + 5\cdot 7^5 + 1\cdot 7^6 + 5\cdot 7^6 + 1\cdot 7^7 + \cdots \\ 5^{-1} =& 3 + 1\cdot 5 + 4\cdot 7^2 + 5\cdot 7^3 + 2\cdot 7^4 + 1\cdot 7^5 + 4\cdot 7^6 + 5\cdot 7^6 + 2\cdot 7^7 + \cdots \\ 6^{-1} =& 6 + 5\cdot 5 + 5\cdot 7^2 + 5\cdot 7^3 + 5\cdot 7^4 + 5\cdot 7^5 + 5\cdot 7^6 + 5\cdot 7^6 + 5\cdot 7^7 + \cdots \end{aligned}$$

例 7.3.9. $\{1 + p + p^2 + \cdots + p^n\}_{n=1,2,\ldots}$ は p 進コーシー列なので $\mathbb{Z}_p$ の元 α を定める．このとき $\alpha = (1-p)^{-1}$．同様に $\{1 - p + p^2 - \cdots + (-1)^n p^n\}_{n=1,2,\ldots}$ も p 進コーシー列なので $\mathbb{Z}_p$ の元 β を定める．このとき $\beta = (1+p)^{-1}$．

実は有理数を p 進展開するとある項から先は必ず循環する．

補題 7.3.10. $\mathbb{Q}_p$ は体になる．即ち 0 でない p 進有理数の乗法に関する逆元が存在する．

証明. 0 でない任意の $\alpha \in \mathbb{Q}_p$ は $\alpha = p^k x$ ($k \in \mathbb{Z}$, $x \in \mathbb{Z}_p$, $|x|_p = 1$) と，表わせるので，$p^{-k}x^{-1} \in \mathbb{Q}_p$ がその逆元である． □

定理 7.3.11. p が奇素数で n が p の倍数でないとき，$x_0^2 \equiv n \bmod p$ なる $x_0 \in \mathbb{Z}$ が存在すれば $x^2 = n$ を満たす $\mathbb{Z}_p$ の元 x が存在する．

証明. まず $x_0^2 \equiv n \bmod p$ なる $x_0 \in \mathbb{Z}$ を取る． p が奇素数なので $2^{-1} \in \mathbb{Z}_p$ であり，

$$x_{i+1} = 2^{-1}(x_i + n{x_i}^{-1}) \quad (i = 0, 1, 2, \dots)$$

と置く．$x_i^2 - n \equiv 0 \bmod p^{2^i}$ と仮定すると ${x_i}^{-1}$ は $\mathbb{Z}_p$ の元であり

$$x_{i+1}^2 - n = 4^{-1}(x_i + n{x_i}^{-1})^2 - n = 4^{-1}(x_i - n{x_i}^{-1})^2 = (2x_i)^{-2}(x_i^2 - n)^2$$

より，$2x_i \not\equiv 0 \bmod p^{2^i}$ に注意すると，これは $p^{2^{i+1}}$ を法として 0 となる．言い換えると

$$|x_{i+1}^2 - n|_p = |2x_i|_p^{-2}|x_i^2 - n|_p^2 = |x_i^2 - n|_p^2 \quad (|2x_i|_p = 1 \text{ なので})$$

となり，$|x_0^2 - n| \le p^{-1}$ より $|x_i^2 - n|_p \le p^{-2^i}$ がわかる．$\lim_{i\to\infty} x_i$ が求める元である． □

例 7.3.12. $1^2 \equiv 2^2 \equiv -2 \bmod 3$ であるから 3 進整数環 $\mathbb{Z}_3$ に $\sqrt{-2}$ が（2 つ）存在する．3 進展開での 3^n ($n = 0, 1, 2, \dots, 34$) の係数を示す．この和は 0 である事を確認せよ．

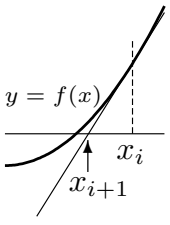
$$1, 1, 2, 0, 0, 2, 0, 1, 0, 0, 0, 2, 1, 2, 0, 1, 0, 1, 1, 0, 2, 2, 0, 1, 1, 1, 2, 2, 2, 0, 0, 0, 2, 1, 0, \dots$$
$$2, 1, 0, 2, 2, 0, 2, 1, 2, 2, 2, 0, 1, 0, 2, 1, 2, 1, 1, 2, 0, 0, 2, 1, 1, 1, 0, 0, 0, 2, 2, 2, 0, 1, 2, \dots$$

例 7.3.13. $3^2 \equiv 4^2 \equiv 2 \bmod 7$ より 7 進整数環 $\mathbb{Z}_7$ に $\sqrt{2}$ が存在し次の表示を得る．

$$3, 1, 2, 6, 1, 2, 1, 2, 4, 6, 6, 2, 1, 1, 0, 2, 1, 1, 4, 6, 1, 3, 2, 6, 6, 3, 5, 5, 6, 3, 4, 5, 0, 1, 6, 3, \dots$$
$$4, 5, 4, 0, 5, 4, 5, 4, 2, 0, 0, 4, 5, 5, 6, 4, 5, 5, 2, 0, 5, 3, 4, 0, 0, 3, 1, 1, 0, 3, 2, 1, 6, 5, 0, 3, \dots$$

■ニュートン法 $f(x)$ の根の近似値 x_0 を初期値とし

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}, \quad i = 0, 1, 2, \dots$$



で $\{x_i\}$ を定めると，この数列はしばしば $f(x)$ の根に収束する．$f(x)$ の根を求めるこの方法をニュートン法と言う．点 $(x_i, f(x_i))$ での曲線 $y = f(x)$ の接線は $y = f'(x_i)(x - x_i) + f(x_i)$ なので，この接線と x 軸との交点の x 座標は x_{i+1} である．状況が図の様であれば x_i より x_{i+1} の方が $f(x)$ の根のより良い近似であるというのがその原理である．

例えば $f(x) = x^2 - n$ とすると $f'(x) = 2x$ であり次の近似列を得る．

$$x_{i+1} = x_i - \frac{x_i^2 - n}{2x_i} = \frac{1}{2}\Big(x_i + \frac{n}{x_i}\Big), \quad i = 0, 1, 2, \dots$$

定理 7.3.11 の証明は p 進数でもニュートン法が有効であることを示している．

■Hensel の補題と Hasse-Minkowski の定理　本稿の趣旨からは大分逸脱するが，p 進数の御利益の一端を述べるため，Hensel の補題と 2 次形式についての Hasse-Minkowski の定理を証明なしに述べておこう．

定理 7.3.14 (Hensel の補題). 整数係数の多項式 $f(x)$ を考える．$f(x_0) = 0 \bmod p$ かつ $f'(x_0) \not\equiv 0 \bmod p$ を満たす整数 x_0 が存在すれば，$f(x) = 0$ かつ $x \equiv x_0 \bmod p$ を満たす $x \in \mathbb{Z}_p$ がただ 1 つ存在する．

定理 7.3.15 (Hasse-Minkowski の定理). $a_{i,j}$ を有理数とする．2 次同次方程式

$$\sum_{i \le j} a_{i,j} x_i x_j = 0 \tag{7.6}$$

が $(x_1, \ldots, x_n) = (0, \ldots, 0)$ 以外の実数解を持ち，またすべての素数 p に対して $(x_1, \ldots, x_n) = (0, \ldots, 0)$ 以外の p 進有理数解を持てば，(7.6) は $(x_1, \ldots, x_n) = (0, \ldots, 0)$ 以外の有理数解を持つ．

例 7.3.16. $p = 3, 7, 11, 19$ とする．方程式 $x^2 + y^2 = pz^2$ は $(x, y, z) = (0, 0, 0)$ 以外の p 進有理数解を持つとする．それを $x = p^a s$, $y = p^b t$, $z = p^c u$ $(a, b, c \in \mathbb{Z}$, $|s|_p = |t|_p = |u|_p = 1)$ とすると $p^{2a} s^2 + p^{2b} t^2 = p^{2c+1} u^2$ を得るが，これに適当に p の偶数冪を掛けると方程式 $x^2 + y^2 = pz^2$ の $(x, y, z) = (0, 0, 0)$ 以外の p 進整数解が構成できる．この式を p を法とした式にすると $x_0^2 + y_0^2 \equiv 0 \bmod p$ を得る．しかし $x_0^2 + y_0^2 \equiv 0 \bmod p$ を満たす整数の組 (x_0, y_0) は $(0, 0)$ 以外には存在しないので，方程式 $x^2 + y^2 = pz^2$ は $(x, y, z) = (0, 0, 0)$ 以外の p 進有理数解を持たないことがわかる．従って Hasse-Minkowski の定理より，方程式 $x^2 + y^2 = pz^2$ は $(x, y, z) = (0, 0, 0)$ 以外の有理数解を持たない．

$p = 3, 7$ のときの $x^2 + y^2 \bmod p$ の表を以下に示す．

$x \backslash y$	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

$x \backslash y$	0	1	2	3	4	5	6
0	0	1	4	2	2	4	1
1	1	2	5	3	3	5	2
2	4	5	1	6	6	1	5
3	2	3	6	4	4	6	3
4	2	3	6	4	4	6	3
5	4	5	1	6	6	1	5
6	1	2	5	3	3	5	2

付録 A

公理的集合論

集合論のパラドックス

自然数の集合 $\mathbb{N}$ の部分集合で，偶数全体からなるものを A とかく．このとき写像

$$f : \mathbb{N} \to A, \quad x \mapsto 2x$$

は全単射である．A は $\mathbb{N}$ の真部分集合であるのにこのような全単射があるのは,「部分は全体に等しい」というパラドックスの様に見えるが別に矛盾ではない．無限集合を考えるとしばしばこのようなことは生じるのである．「部分は全体に等しくない」という主張は無限集合については根拠はないのである．

深刻なパラドックスは，次の Russel[*1]のパラドックスである．まずすべての集合からなる集合 Ω を考える．つぎに Ω を 2 種類に分ける．一つは自分自身を含まない集合 (これを ‘普通’ の集合と呼ぼう), 他方は自分自身を含む集合 (これを ‘特殊’ な集合と呼ぼう) である．Ω_1 を ‘普通’ の集合全体，Ω_0 を ‘特殊’ な集合全体とする．

$$\Omega_0 = \{A \mid A \in A\}$$
$$\Omega_1 = \{A \mid A \notin A\}$$

明らかに $\Omega = \Omega_0 \cup \Omega_1$, $\Omega_0 \cap \Omega_1 = \varnothing$. さて Ω_1 は ‘普通’ の集合であろうか，または ‘特殊’ な集合であろうか?

Ω_1 が ‘普通’ の集合ならば，$\Omega_1 \in \Omega_1$ だから ‘特殊’ である．Ω_1 が ‘特殊’ な集合ならば，$\Omega_1 \notin \Omega_1$ だから ‘普通’ である．

矛盾のある仮定からはどんな命題でも証明できることは昔から知られていた．Russel のパラドックスは数学の深刻な危機と考えられ，この問題を回避するため幾つかのプログ

[*1] Bertrand Arthur William Russell, 3rd Earl Russell (1872 – 1970) イギリスの哲学者、論理学者、数学者であり、社会批評家、政治活動家である．1950 年にノーベル文学賞を受賞.

ラムが提出された．その中で現在主流となっている考えを述べておこう．問題は集合とは何かを曖昧にしたまま，すべての集合の集合のような，さらに曖昧なものを考える事から生じる．そこで集合とは何か曖昧なまま議論するのでなく, 我々が通常扱うような集合が満たすような“集合に関するよい公理系”を定め，その公理系が無矛盾であることを示そうというもので，**公理的集合論** (axiomatic set theory) とよばれている．

公理的集合論

1908 年 E. Zermelo は公理的集合論を発表し, Russel のパラドックスによって深刻な危機に陥っていた数学を救うことを考えた．それによれば，集合とは幾つかの公理をみたす, 形式的な体系である．以下その公理を述べ，いかにして Russel のパラドックスを避けるかを説明する．

これ以降，集合やその元をあらわす記号をすべて小文字のアルファベットを用いる．2 つの集合 a, x に対し $x \in a$ なる関係があれば「集合 x は集合 a の元 (または要素) である」ということにする．または 「集合 a と関係 $x \in a$ があれば x も集合である」と考えてもよい．

外延公理: $a = b \iff \forall x\ (x \in a \Leftrightarrow x \in b)$

これは「2 つの集合 a, b はその元が等しければ，相等しい」ということである．

内包公理 (分出公理): 集合 a とその元 x に関する命題 $P(x)$ が与えられれば $\{x \in a \mid P(x)\}$ は集合である．

内包公理を仮定すると次が示せる．

補題 A.0.1. すべての集合を元とする集合は存在しない．

証明. すべての集合を元とする集合 Ω があったとして矛盾を導く．$\Omega_1 = \{x \in \Omega \mid x \notin x\}$ とすると内包公理よりこれは集合である．Ω はすべての集合を含むから $\Omega_1 \in \Omega$ となる．もし $\Omega_1 \in \Omega_1$ とすれば，Ω_1 の定義より $\Omega_1 \notin \Omega_1$ となる．またもし $\Omega_1 \notin \Omega_1$ とすれば，Ω_1 の定義より $\Omega_1 \in \Omega_1$ となり，いずれの場合も矛盾となる． □

集合論の公理系としては，パラドックスが回避されると同時に，今まで展開して来た集合論の論法が展開される公理系であることが望ましい．よってそれらを保証する命題を公理として要請する必要がある．

空集合の公理: 要素を一つも含まない集合が存在する．これを空集合といい $\varnothing$ で表す．

外延公理より空集合の一意性もわかる.

対の公理: x, y が集合ならば, $\{x, y\}$ は集合である.

$\{x, x\}$ を $\{x\}$ と書く.

和集合の公理: 集合 a に対し a に含まれる集合の和集合 $\mathfrak{S}(a)$ が存在する. つまり

$$x \in \mathfrak{S}(a) \quad \Longleftrightarrow \quad \exists z\, [x \in z \in a]$$

をみたす集合 $\mathfrak{S}(a)$ (または $\cup(a)$) が存在する.

a が集合ならば 対の公理より $\{a, a\} = \{a\}$ も集合で, もう一度対の公理を使うと $a' := \{a, \{a\}\}$ も集合であることがわかる. 和集合の公理より a' に含まれる集合の和集合も集合なので, それを a^+ と書く.

$$a^+ = \mathfrak{S}\{a, \{a\}\} = a \cup \{a\}.$$

冪集合の公理: 集合 a に対し a の部分集合全体からなる集合 $\mathfrak{P}(a)$ が存在する. つまり

$$x \in \mathfrak{P}(a) \quad \Longleftrightarrow \quad \forall\, z[z \in x \to z \in a]$$

をみたす集合 $\mathfrak{P}(a)$ が存在する.

次の演算規則が成立する.

$$\mathfrak{S}\mathfrak{P}a = a, \quad \mathfrak{P}\mathfrak{S}a \supset a, \quad \mathfrak{P}\mathfrak{S}\mathfrak{P}\mathfrak{S}a = \mathfrak{P}\mathfrak{S}a$$

証明. $\mathfrak{S}\mathfrak{P}a \subset a$ の証明: $x \in \mathfrak{S}\mathfrak{P}a \Longleftrightarrow \exists z\, [x \in z \wedge z \in \mathfrak{P}a]$
$\Longleftrightarrow \exists z\, \forall w\, [x \in z \wedge (w \in z \to w \in a)] \Longrightarrow x \in a.$
$\mathfrak{S}\mathfrak{P}a \supset a$ の証明: $x \in \mathfrak{S}\mathfrak{P}a \Longleftrightarrow \exists z\, \forall w\, [x \in z \wedge (w \notin z \vee w \in a)]$
$\Longleftarrow \forall w\, [x \in a \wedge (w \notin a \vee w \in a)] \Longleftrightarrow x \in a.$
$\mathfrak{P}\mathfrak{S}a \supset a$ の証明: $x \in \mathfrak{P}\mathfrak{S}a \Longleftrightarrow \forall z\, [z \in x \to z \in \mathfrak{S}a] \Longleftrightarrow \forall z\, [z \notin x \vee z \in \mathfrak{S}a]$
$\Longleftrightarrow \forall z\, \exists w\, [z \notin x \vee (z \in w \wedge w \in a)] \Longleftrightarrow \forall z\, \exists w\, [(z \notin x \vee z \in w) \wedge (z \notin x \wedge w \in a)]$
$\Longleftarrow \forall z\, [(z \notin x \vee z \in x) \wedge (z \notin x \vee x \in a)] \Longleftrightarrow \forall z\, [z \notin x \vee x \in a] \Longleftarrow x \in a.$
$\mathfrak{P}\mathfrak{S}\mathfrak{P}\mathfrak{S}a \subset \mathfrak{P}\mathfrak{S}a$ の証明: $x \in \mathfrak{P}\mathfrak{S}\mathfrak{P}\mathfrak{S}a \Longleftrightarrow \forall z\, [z \in x \to z \in \mathfrak{S}\mathfrak{P}\mathfrak{S}a]$
$\Longleftrightarrow \forall z\, [z \notin x \vee z \in \mathfrak{S}\mathfrak{P}\mathfrak{S}a] \Longleftrightarrow \forall z\, \exists w\, [z \notin x \vee (z \in w \wedge w \in \mathfrak{P}\mathfrak{S}a)]$
$\Longleftrightarrow \forall z\, \exists w\, \forall z'\, [z \notin x \vee (z \in w \wedge [z' \in w \to z' \in \mathfrak{S}a])]$
$\Longrightarrow \forall z\, \exists w\, [z \notin x \vee (z \in w \wedge [z \in w \to z \in \mathfrak{S}a])]$

$\Longleftrightarrow \forall z\ [z \notin x \vee (z \in \mathfrak{S}a)] \Longleftrightarrow x \in \mathfrak{P}\mathfrak{S}a$ □

無限公理: $\varnothing \in a$ かつ '$x \in a$ ならば $x^+ \in a$' をみたす集合 a が存在する.

これは自然数全体を含む集合が存在することを主張している. von Neumann は集合を用いて自然数を

$$0 = \varnothing, \quad 1 = 0^+ = \{0\}, \quad 2 = 1^+ = \{0, 1\}, \quad 3 = 2^+ = \{0, 1, 2\}, \ldots$$

と定義したが, 無限公理はこれらをすべて含む集合が存在することを主張しているのである.

$\in$-帰納法の公理: 任意の集合 a に対し

$$\forall\ x \in a\ P(x) \Longrightarrow P(a)$$

ならばすべての集合 a に対し $P(a)$ が成り立つ.

この公理より $x \in x$ をみたす集合 x は存在しないことがわかる. $x \in y \wedge y \in x$ をみたすような集合 x, y も存在しない.

以上が Zermelo が考えた公理系で, 通常 Z 公理系と略称される. Frankel は Zermero の公理系では順序数などの記述が不自然になることに気付き, その欠点を改良すべく, 更に次の公理系を考えた.

置換公理: 集合 a の任意の元 x に対し $P(x, y)$ をみたすような y が存在すれば, ある集合 b があって, 集合 a の任意の元 x に対し $P(x, y)$ をみたすような $y \in b$ が存在する.

これより集合の写像による像は集合になることが従う.

以上の公理系を総称して ZF 公理系という. さらに, ZF 公理系に選択公理を加えたものを ZFC 公理系という. ZFC 公理系は, 現在の数学を記述するのに十分強力であると考えられているが, ZFC 公理系が無矛盾であるかどうかはまだ証明されていない.

付録 B

ギリシャ文字と英字の字体

ギリシャ文字

大文字	小文字	英文スペル	大文字	小文字	英文スペル
A	α	alpha	N	ν	nu
B	β	beta	Ξ	ξ	xi
Γ	γ	gamma	O	o	omicron
Δ	δ	delta	Π	π, ϖ	pi
E	ϵ, ε	epsilon	P	ρ	rho
Z	ζ	zeta	Σ	σ, ς	sigma
H	η	eta	T	τ	tau
Θ	θ, ϑ	theta	Υ	υ	upsilon
I	ι	iota	Φ	ϕ, φ	phi
K	κ	kappa	X	χ	chi
Λ	λ	lambda	Ψ	ψ	psi
M	μ	mu	Ω	ω	omega

α, β, γ, δ, ϵ は英語の a, b, c, d, e に対応して使われる．（γ は g に対応しているという話もある．）しかし、英語のアルファベットと順に対応しているわけではない．たとえば英語の p に対応するのはギリシャ文字では π で，r に対応するのは ρ である．σ, τ は英語の s, t である．英語の x, y, z に対応して使われるのは ξ, η, ζ である．

英字の字体

アルファベットにもいろいろな字体がある．参考までに数学でよく使うものをあげておこう．なお fraktur というのはドイツ文字である．

roman	italic	bold	黒板太字	caligraphic	筆記体 (frc, wela)		fraktur
A a	$A\ a$	**A a**	$\mathbb{A}$	$\mathcal{A}$	$\mathfrak{A}\ \mathfrak{a}$	$\mathfrak{A}\ \mathfrak{a}$	$\mathfrak{A}\ \mathfrak{a}$
B b	$B\ b$	**B b**	$\mathbb{B}$	$\mathcal{B}$	$\mathfrak{B}\ \mathfrak{b}$	$\mathfrak{B}\ \mathfrak{b}$	$\mathfrak{B}\ \mathfrak{b}$
C c	$C\ c$	**C c**	$\mathbb{C}$	$\mathcal{C}$	$\mathfrak{C}\ \mathfrak{c}$	$\mathfrak{C}\ \mathfrak{c}$	$\mathfrak{C}\ \mathfrak{c}$
D d	$D\ d$	**D d**	$\mathbb{D}$	$\mathcal{D}$	$\mathfrak{D}\ \mathfrak{d}$	$\mathfrak{D}\ \mathfrak{d}$	$\mathfrak{D}\ \mathfrak{d}$
E e	$E\ e$	**E e**	$\mathbb{E}$	$\mathcal{E}$	$\mathfrak{E}\ \mathfrak{e}$	$\mathfrak{E}\ \mathfrak{e}$	$\mathfrak{E}\ \mathfrak{e}$
F f	$F\ f$	**F f**	$\mathbb{F}$	$\mathcal{F}$	$\mathfrak{F}\ \mathfrak{f}$	$\mathfrak{F}\ \mathfrak{f}$	$\mathfrak{F}\ \mathfrak{f}$
G g	$G\ g$	**G g**	$\mathbb{G}$	$\mathcal{G}$	$\mathfrak{G}\ \mathfrak{g}$	$\mathfrak{G}\ \mathfrak{g}$	$\mathfrak{G}\ \mathfrak{g}$
H h	$H\ h$	**H h**	$\mathbb{H}$	$\mathcal{H}$	$\mathfrak{H}\ \mathfrak{h}$	$\mathfrak{H}\ \mathfrak{h}$	$\mathfrak{H}\ \mathfrak{h}$
I i	$I\ i$	**I i**	$\mathbb{I}$	$\mathcal{I}$	$\mathfrak{I}\ \mathfrak{i}$	$\mathfrak{I}\ \mathfrak{i}$	$\mathfrak{I}\ \mathfrak{i}$
J j	$J\ j$	**J j**	$\mathbb{J}$	$\mathcal{J}$	$\mathfrak{J}\ \mathfrak{j}$	$\mathfrak{J}\ \mathfrak{j}$	$\mathfrak{J}\ \mathfrak{j}$
K k	$K\ k$	**K k**	$\mathbb{K}$	$\mathcal{K}$	$\mathfrak{K}\ \mathfrak{k}$	$\mathfrak{K}\ \mathfrak{k}$	$\mathfrak{K}\ \mathfrak{k}$
L l	$L\ l$	**L L**	$\mathbb{L}$	$\mathcal{L}$	$\mathfrak{L}\ \mathfrak{l}$	$\mathfrak{L}\ \mathfrak{l}$	$\mathfrak{L}\ \mathfrak{l}$
M m	$M\ m$	**M m**	$\mathbb{M}$	$\mathcal{M}$	$\mathfrak{M}\ \mathfrak{m}$	$\mathfrak{M}\ \mathfrak{m}$	$\mathfrak{M}\ \mathfrak{m}$
N n	$N\ n$	**N n**	$\mathbb{N}$	$\mathcal{N}$	$\mathfrak{N}\ \mathfrak{n}$	$\mathfrak{N}\ \mathfrak{n}$	$\mathfrak{N}\ \mathfrak{n}$
O o	$O\ o$	**O o**	$\mathbb{O}$	$\mathcal{O}$	$\mathfrak{O}\ \mathfrak{o}$	$\mathfrak{O}\ \mathfrak{o}$	$\mathfrak{O}\ \mathfrak{o}$
P p	$P\ p$	**P p**	$\mathbb{P}$	$\mathcal{P}$	$\mathfrak{P}\ \mathfrak{p}$	$\mathfrak{P}\ \mathfrak{p}$	$\mathfrak{P}\ \mathfrak{p}$
Q q	$Q\ q$	**Q q**	$\mathbb{Q}$	$\mathcal{Q}$	$\mathfrak{Q}\ \mathfrak{q}$	$\mathfrak{Q}\ \mathfrak{q}$	$\mathfrak{Q}\ \mathfrak{q}$
R r	$R\ r$	**R r**	$\mathbb{R}$	$\mathcal{R}$	$\mathfrak{R}\ \mathfrak{r}$	$\mathfrak{R}\ \mathfrak{r}$	$\mathfrak{R}\ \mathfrak{r}$
S s	$S\ s$	**S s**	$\mathbb{S}$	$\mathcal{S}$	$\mathfrak{S}\ \mathfrak{s}$	$\mathfrak{S}\ \mathfrak{s}$	$\mathfrak{S}\ \mathfrak{s}$
T t	$T\ t$	**T t**	$\mathbb{T}$	$\mathcal{T}$	$\mathfrak{T}\ \mathfrak{t}$	$\mathfrak{T}\ \mathfrak{t}$	$\mathfrak{T}\ \mathfrak{t}$
U u	$U\ u$	**U u**	$\mathbb{U}$	$\mathcal{U}$	$\mathfrak{U}\ \mathfrak{u}$	$\mathfrak{U}\ \mathfrak{u}$	$\mathfrak{U}\ \mathfrak{u}$
V v	$V\ v$	**V v**	$\mathbb{V}$	$\mathcal{V}$	$\mathfrak{V}\ \mathfrak{v}$	$\mathfrak{V}\ \mathfrak{v}$	$\mathfrak{V}\ \mathfrak{v}$
W w	$W\ w$	**W w**	$\mathbb{W}$	$\mathcal{W}$	$\mathfrak{W}\ \mathfrak{w}$	$\mathfrak{W}\ \mathfrak{w}$	$\mathfrak{W}\ \mathfrak{w}$
X x	$X\ x$	**X x**	$\mathbb{X}$	$\mathcal{X}$	$\mathfrak{X}\ \mathfrak{x}$	$\mathfrak{X}\ \mathfrak{x}$	$\mathfrak{X}\ \mathfrak{x}$
Y y	$Y\ y$	**Y y**	$\mathbb{Y}$	$\mathcal{Y}$	$\mathfrak{Y}\ \mathfrak{y}$	$\mathfrak{Y}\ \mathfrak{y}$	$\mathfrak{Y}\ \mathfrak{y}$
Z z	$Z\ z$	**Z z**	$\mathbb{Z}$	$\mathcal{Z}$	$\mathfrak{Z}\ \mathfrak{z}$	$\mathfrak{Z}\ \mathfrak{z}$	$\mathfrak{Z}\ \mathfrak{z}$

最近は筆記体を学んでない学生も散見されるが、よく使われるので基本的な形や書き方は弁(わきま)えておく必要があるだろう．筆記体で書くときは word や phrase のように 1 単語をつなげて書くのが普通である．筆記体には一つの決まった型があるわけでなく上に挙げた以外もいろんなバリエーションがある事にも注意しておく．

なお数式で x を書く際，英語の小文字である x を使わず x を使うことが多いのは数学がフランスを中心として発達した学問であることと関係があるように思う．フランス語の x の小文字は x によく似ている．

付録 C

大きな数

英語で大きな数をどのように言うのだろうか? 例えば,「日本の人口は 1 億 2 千万である」 はどのように言うのであろうか?

問: 1 億 2 千万は one hundred and twenty millions であることを使ってこの文を英訳せよ.

英語における大きな数の唱え方の約束は次のようである.

	one	ten	hundred	thousand	million	milliard	billion	trillion
米・仏系	1	10	10^2	10^3	10^6	10^9	10^9	10^{12}
英・独系	1	10	10^2	10^3	10^6	10^9	10^{12}	10^{18}

quadrillion	quintillion	sextillion	septillion	octillion	nonillion	decillion
10^{15}	10^{18}	10^{21}	10^{24}	10^{27}	10^{30}	10^{33}
10^{24}	10^{30}	10^{36}	10^{42}	10^{48}	10^{54}	10^{60}

1000m を 1km といい 0.001m を 1mm という. この様に大きな量や小さな量を考えるときは単位の前に k (キロ) や m (ミリ) といった接頭辞をつけてあらわすのが普通である.

記号	名称	大きさ	記号	名称	大きさ
da	deca-	10	d	deci-	10^{-1}
h	hecto-	10^2	c	centi-	10^{-2}
k	kilo-	10^3	m	milli-	10^{-3}
M	mega-	10^6	μ	micro-	10^{-6}
G	giga-	10^9	n	nano-	10^{-9}
T	tera-	10^{12}	p	pico-	10^{-12}
P	peta-	10^{15}	f	femto-	10^{-15}
E	exa-	10^{18}	a	atto-	10^{-18}
Z	zetta-	10^{21}	z	zepto-	10^{-21}
Y	yotta-	10^{24}	y	yocto-	10^{-24}
R	ronna-	10^{27}	r	ronto-	10^{-27}
Q	quetta-	10^{30}	q	quecto-	10^{-30}

これらを見る限り西洋では「千進法」を基礎にして数を唱えている事が分かる．次の表を見てこれらの数の大きさがどのくらいか感じをつかんでいただきたい．

1 光年	9.5×10^{15}m
太陽と地球の平均距離	1.5×10^{11}m
太陽の半径	7×10^{8}m
地球の半径	6.4×10^{6}m
4 歳児の身長	1m
赤血球の直径	8×10^{-6}m
DNA	10^{-7}m
分子	10^{-9}m
原子	10^{-10}m
原子核	10^{-14}m
陽子	10^{-15}m
クオーク	10^{-18}m 以下[*1]

参考までに日本における数の唱え方を見ておこう．江戸時代における日本でも大きな数の唱え方は考えられていた．

『塵劫記』[*2] によれば次のようである．しかしあまりに大きい数 (例えば「京」から先) は実際には用いられてないようである．

一	十	百	千	万	億（をく）	兆（てう）	京（けい）	垓（がい）	秭（ぢょ）	穣（じゃう）	溝（かう）	澗（かん）
1	10	10^2	10^3	10^4	10^8	10^{12}	10^{16}	10^{20}	10^{24}	10^{28}	10^{32}	10^{36}

正（せい）	載（さい）	極（ごく）	恒河沙（ごうがしゃ）	阿僧祇（あそうぎ）	那由他（なゆた）	不可思議（ふかしぎ）	無量大数（むりょうたいすう）
10^{40}	10^{44}	10^{48}	10^{56}	10^{64}	10^{72}	10^{80}	10^{88}

これを見ると日本の大きな数の唱え方は「万進法」であったことが分かる．ついでに小さな数の唱え方は,『塵劫記』によれば, 次のようである．これもあまり小さい数は実際には用いられなかったようである．

分（ぶん）	厘（り）	毫（もう）	糸（し）	忽（こつ）	微（び）	繊（せん）	沙（しゃ）	塵（ぢん）	埃（あい）
10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}	10^{-9}	10^{-10}

[*1] これを見た物理学者は「クオークの大きさなんでどうやって測るのか」とつぶやいた．

[*2] 吉田光由著，大矢真一校注，塵劫記，岩波文庫，1977.

付録 D

TEX, 数式処理システム

最近はコンピュータが普及していて，ノートパソコンを所有している学生も多い．PC を用いれば電子的に数学の文書を作ることもできるし，グラフを描いたり，手計算では面倒な計算も気軽にやらせることができる．例えば，無料で利用できる GeoGebra は数学や科学を小学校から大学水準まで学習指導するための幾何・代数・統計・解析を結び付けた動的な数学ソフトウェアである．使わなくても構わないが，手軽に使える[*1]し，使えれば便利と思うことも多いであろう．GeoGebra 以外にも色々あるのでいくつか紹介する．

D.1 TEX

TEX(TeX; テック，テフ) はアメリカの数学者・計算機科学者であるドナルド・クヌース (Donald E. Knuth、1938 –) が開発を初めた組版(くみはん)処理システムである．TEX の最初の版は 1978 年というから，40 年以上使われていることになる．こんなに長く使われているシステムは他にあまりない．現在は様々なバージョンの TEX が存在するが，TEX は数式を含む文書を電子的に作る際のデフェクト・スタンダード「事実上の標準」である．数式を含む文書（レポート，論文，本，辞書など）を手軽に美しく作ることができる．章，節，定理，定義，数式などに自動的に番号がつけられ，手軽に相互参照できるし，その気になれば目次や索引も自動的に作ることができる．インターネットで TEX をキーワードに検索すれば多くの情報が得られる．数学科の学生なら PC にインストール[*2]しておいて損はない．

[*1] スマートフォーンに GeoGebra をインストールしておくと便利である．

[*2] インストールは難しくはないが，相応の時間がかかるので，時間に追われているときに，TEX のインストールをするのは負担に感ずるであろう．時間のあるときにやっておくと良い．

D.1.1 環境を整える

Windows または Mac の PC にインストール

- Google で 「TeX インストール」で検索して，ウェブページを読む.
  使っているコンピュータの OS もキーワードにして「TeX Windows10 インストール」「TeX Mac インストール」などで検索してもよい.
- 指示に従ってインストール.（TEX wiki を参照するのが良い.）

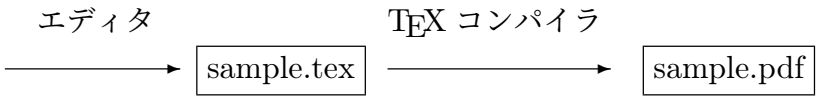
日本語化された TEX をインストールするには，システムの言語が日本語に設定されていることが必要である．海外から PC を買ったときなど，システム・ロケールも忘れずに日本語に設定しておきたい.

オンラインで TeX を使う

PC に TEX をインストールできないときでも，インターネット環境があればクラウドで TEX を使うことできる．いくつか候補があるので詳細は「TeX を Web で」を見ること.

D.1.2 TEX を使う

TEX は文書組版ソフトである．適当なエディタ[*3]で tex ファイル（例えば sample.tex）を作り，その指示に従って TEX コンパイラプログラムが文書を作成する.



現在ではエディタを含む TEX 用の統合環境 TEX works, TEX Shop, TEXstudio, GNU Emacs +YaTeX 等をインストールして使用することが多く，D.1.1 節に従ってインストールしたら，TEX works や TEX Shop 等がインストールされた筈で，TEX コンパイラがワンタッチで動くように設定されている.

作成した tex ファイル (例えば sample.tex) に文法的な問題がなければ，TEX コンパイラは tex ファイルを解釈して sample.pdf という pdf ファイルを作成する．もし，文法的な誤りがあったり，問題を検知したら TEX コンパイラはエラーメッセージを出して止まる．エラーメッセージなどコンパイル時の記録は sample.log というテキストファイルに出力されるので，そのファイルを調べることでエラーを修復する事ができる.

[*3] テキストファイルを編集するプログラム

D.1.3 例

例えば

sample.tex

```
\documentclass[12pt,dvipdfmx]{jsarticle}
% プリアンブル (preamble)
\begin{document}% これ以降に出力したい文を書く．
$a_1=1$, $a_2=1$, $a_{n+1}=a_n+a_{n-1}$ ($n=2,3,\dots$)
で定まる数列の一般項は
\[
a_n=\frac{1}{\sqrt{5}}
\biggl\{
\Bigl(\frac{1+\sqrt{5}}2\Bigr)^n
-\Bigl(\frac{1-\sqrt{5}}2\Bigr)^n
\biggr\}　% フィボナッチ数列のビネの公式
\]
となる．さらに次の式が成り立つ事が知られている．
\[
\sum_{i=1}^\infty\frac{a_n}{k^{n+1}}=\frac{1}{k^2-k-1}
\]
\end{document}
```

という内容の tex ファイルを TEX コンパイラに処理させると次の出力を得る．

sample.pdf

$a_1 = 1$, $a_2 = 1$, $a_{n+1} = a_n + a_{n-1}$ $(n = 2, 3, \dots)$ で定まる数列の一般項は

$$a_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right\}$$

となる．さらに次の式が成り立つ事が知られている．

$$\sum_{i=1}^{\infty} \frac{a_n}{k^{n+1}} = \frac{1}{k^2 - k - 1}$$

D.1.4 TEX のコマンド

TEX には沢山のコマンドがあるが，個々のコマンドを覚えようとする必要はなく，必要に応じて調べて使うという考えで使い始めると良い．コマンドを探すときは Google で調べるか，例えば次の URL などを参照して下さい．

- TEXWiki LATEX 入門
- TEX 入門（東京都立大学酒井高司先生）
- LATEX 文書（大東文化大学水谷正大先生）

D.1.5 注意事項

以下，知っていたほうが良いかもしれない注意事項です．

 [*4] ファイル名の.(period) 以降の 3 文字は**拡張子**と呼ばれ，ファイルの属性を表すのに使われる．Windows のファイル管理ソフト「エクスプローラー」や Mac のファイル管理ソフト「ファインダー」では，ファイルの拡張子を表示しない初期設定になっているので，拡張子を表示するように設定を変更しておくと便利である．

 文字など文字コードによって表されるデータだけが含まれるファイルのことを**テキストファイル**と言い，テキストファイルを作成，編集，保存するためのソフトウェアを**エディタ**と言う．テキストファイルに対し，文字コード以外の情報を含むファイルは**バイナリーファイル**と言う．tex ファイルはテキストファイルで，pdf ファイルはバイナリーファイルである．

 コンピュータは欧米文化圏で発達してきたので，テキストファイルは英数字がベースのコード体系 (ascii code[*5]) が基本である．そのため日本語を表すためのいくつかの日本語用コードが考案され使用されてきた．かつては Windows 系の OS ではシフト JIS コード，Unix 系では EUC コードが主流であったが，現在は UNICODE（utf-8 または utf-16）に統一されている．古いファイルを利用するときなど，文字コードの違いが文字化けの問題を起こすことが時々あるので，文字コードの変換などが必要な場合があると承知しておくと良い．現在は大抵の環境ではエディタはデフォルトで utf-8 コードである．付属のエディターは文字コードの自動認識や変換に対応していない事があるので，文字コードの変換機能を持っている他のエディタを必要に応じて補助的に使うと良い．

[*4]  はクヌースが作った記号である．危険な曲がり角を意味するらしい．

[*5] American Standard Code for Information Interchange

backslash 記号 \ は TEX のコマンドの先頭を表す特殊文字である．TEX コンパイラは \ から始まり空白␣までの文字列をコマンドとして解釈する．なお，日本語化された Windows 等の OS では，backslash 記号 \ は ¥と表示される．これは\ の ASCII コードと ¥ の JIS X0201 コードが同じである事から起こる現象で，意図したものではないが，承知して読み替える必要がしばしばある．

TEX コンパイラは{ と } で囲まれた部分を一纏(ひとまと)まりの塊(かたまり)として処理する．従って { は } と対になって入力する必要がある．上の sample.tex ファイルでの{ と } の対応を確認して欲しい．なお，中括弧{ } を出力したいときは \{ \}と入力すれば良い．

$ 記号で囲まれた部分は**数式モード**と呼ばれ，数式用のフォントで出力される．数式モードの a や x (aやxと入力）は数式モード以外（テキストモードといいます) の a や x とは異なる．混同して使用しない様にしたい．それから，数式モードでしか使えないコマンドやテキストモードでしか使えないコマンドがあるので注意したい．

\[と \] で囲まれた部分は **displaystyle の数式モード**と言い，囲まれた部分が改行してセンタリングして表示される．$$ と$$ で囲んでも displaystyle の数式モードになるが，スペーシング等で動作が変なことが稀(まれ)にあるので，$$ と$$ で囲んで displaystyle の数式モードにすることは推奨されない．displaystyle の数式モードに対して，前項の数式モードを textstyle の数式モードと言うことがある．

tex ファイル中に複数個の半角スペースを続けて入力しても TEX コンパイラはただ 1 つの半角スペースと同じに解釈する．なお, スペースを出力したいときは, スペースを表すコマンド\,, \␣, \quad, \qquad, \hspace{10pt} 等を使う．尚 1pt は約 0.35278mm なので 10pt は約 3.5278mm である．

改行したいときは \\を入力する．Enter キー（Return キー）を押して入力されるコード (改行コード) は TEX コンパイラは改行の指示と解釈しません．

% 以降は改行コードまで注釈とみなされ TEX コンパイラは解釈しない．出力したくないメモ書き等に利用できる．なお % を出力したいときは \% と入力する．

\begin{document}の前の部分はプリアンブルと呼ばれ，この部分に使用したいパッケージや, 追加したいコマンドの定義等を書く．例えば, 数式の記述を強化した AMS の一連のパッケージを使いたいときは次の行をプリアンブルに記述すればよい．

```
\usepackage{amsmath,amssymb,amstext,amsfonts,amsthm,amscd}
```

空集合の記号 ∅ は，アンドレ・ヴェイユが 1939 年の本で使ったのが最初らしい．何故か TEX では記号 ∅ がコマンド \emptyset に割り当てられている．記号 ∅ を使いた

いときは，amssymb パッケージを読み込んでコマンド \varnothing を使えばよい．


冒頭に相互参照のことを述べたが，TEX を使って pdf ファイルにリンクを埋め込む事もできる．インターネットに接続してある環境で pdf ファイルを読む場合，便利である．相互参照やリンクのやり方については，次のリンクを参照してほしい．
「LaTeX 入門/相互参照とリンク」
本稿にも他にいくつかリンクが埋め込んである．

D.2 数式処理システム

数式処理システムとは computer algebra system の訳語で，コンピュータを用いて数式を記号的に処理するソフトウェアである．上手に利用すれば複雑な計算も，ノートパソコン等で処理することが可能である．無償のものやオープンソースのものもあるので，幾つか紹介する．多くはインストールしないでも使えるが，頻回に使うなら PC にインストールして使うとよい．なお最近はブラウザー上で動作するプログラム実行環境である jupyter notebook 上で動作するものが増えた．なお，jupyter とは高水準の汎用プログラム言語である Python の対話的な実行を支援する入出力環境（シェル）である．

- Sage: MathSage ということもある．2005 年に公開された無償のソフトウェア．多数の定評のあるオープンソースの数学関連ソフトウェアを統合して一つのインターフェイスで使えるようにすることを目指した．juypter 上で動作する．以下の Maxima, Singular 等も mathsage で動作させることができる．
- Maxima: LISP で記述された数式処理システム．オープンソースで手軽にインストールできる．「入力例で学ぶ Maxima の使い方（入門）」等を参照．
- Singular: 多項式や可換環の演算を念頭に置いて開発された，計算機代数のフリーソフトウェア．カイザースラウテルン工科大学（ドイツ）で開発された．
- Mathematica: 汎用性が高く手軽に計算できる．ウルフラム・リサーチ社が販売．
  - Wolfram alpha: 無償の多機能な計算ツール．登録不要ですぐに計算を開始できる．「Wolfram alpha」を試してみよ．検索エンジンの様な使い方もできる．
  - Wolfram engine: 2019 年 5 月に無償で公開された Mathematica の根幹部分． Mathematica に似た数式処理が可能で，jyupter 上で動作する．「wolfram engine jyupter インストール」などで検索するとインストール法がわかる．使い方は「入力例で学ぶ Wolfram 言語の使い方（入門）」等を参照．
  - Mathics: Mathematica とほとんど同じ文法を採用した Open source の計算代数プログラム．

付録 E

参考文献

数学全般にわたって初心者向けに解説しているもの

- 数学ガイダンス 2018 日本評論社
- 寺坂英孝編，現代数学小辞典，講談社ブルーバックス，1977.
- G トス著，蟹江幸博訳，数学名所案内 上 下，シュプリンガー・フェアラーク東京，1999，2000.
- 佐藤文広，数学ビギナーズマニュアル，日本評論社，1994.
- 飯高茂・松本幸夫監修，岡部恒治編，数学英和小事典，講談社サイエンティフィク，1999.

現代数学の基礎的事柄について本格的に学習したい場合は，多くの良書があるので，そのなかから気に入った本を選べば良い．それらをすべてを紹介する能力は筆者にはないので，初等的かつ代表的と思われるものを挙げるにとどめる．

- E ハイラー/G ワナー著，蟹江幸博訳，解析教程 上 下，シュプリンガー・フェアラーク東京，1997
- 赤攝也著，集合論入門，新数学シリーズ 1，培風館，1957.
- 彌永昌吉・小平邦彦著，現代数学概説 I，岩波書店，1961.
- 河田敬義・三村征雄著，現代数学概説 II，岩波書店，1965.

なお次の数学辞典は，頼りになる情報元である．

- 日本数学会編集，数学辞典 第 4 版，岩波書店，1985.

数学の書き物をする際参考になるもの

- 一松信，数学論文の書き方， 数学 39 (1987), 276–281.
- 小林昭七，数学論文の書き方（英語編），数学 39 (1987), 348–354.
- 野水克己：How to write mathematics in English I, II, III, 数学 43 (1991), 158–164, 248–253, 362–367. この内容は加筆されて「数学のための英語案内」（サイエンス社 1993）として出版されています.
- Steven G. Krantz, A Primer of Mathematical Writing, Second Edition. この初版の和訳が「数学者の書きもの心得：英語表現から出版まで」（丸善出版 1999）として出ています。