数について

春日 悠

2018 年 9 月 10 日

目次

1 論理 **2**
- 1.1 論理 2
- 1.2 論理的原理 2
- 1.3 論理の誤り 2
- 1.4 公理主義と記号論理学 4
- 1.5 記号論理学 5
  - 1.5.1 命題 5
  - 1.5.2 演算子 5
  - 1.5.3 証明 7

2 集合 **8**
- 2.1 集合 8
- 2.2 写像 11
- 2.3 無限 11
- 2.4 公理的集合論 12

3 自然数 **14**
- 3.1 数 14
- 3.2 対等 15
- 3.3 自然数 16
- 3.4 自然数の性質 17
- 3.5 ペアノの公理 18
- 3.6 加法 19
- 3.7 乗法 20
- 3.8 べき法 23
- 3.9 大小関係 24
- 3.10 付録: 加法・乗法の一意性 26

1　論理

1.1　論理

論理とは，経験に基づく思考の規則である．論理と経験は相反するように思うかもしれないが，われわれはきっと経験からしか物事を知りえない．論理によってなにがしかを知るとしても，論理のはじまりは結局，経験からしか得られない．

論理的思考を論証といい，推論と証明の二つがある．

推論 ： ある前提からある結論を導くこと．
証明 ： 推論から得られた結論が正しいことを示すこと．

普段はあまり意識しないが，論証の前提の前提には，論理的原理がある．

1.2　論理的原理

論理は論理的原理を基礎としている．論理的原理はわれわれの経験から得られたものであり，つぎのようなものである．

同一律 ： あるものはある．
矛盾律 ： ありかつないということはない．
排中律 ： あるかないかである．

論理においては絶対的な正しさを主張できるが，経験においてはそうではない．だから，経験から得られる論理的原理に正しいということはない．論理的原理は任意であり，論理における正しさは論理的原理にしたがって変わりうるのである．たとえば，人によっては排中律の代わりに「あるか，ないか，わからない」の三分律を原理にしたほうがよいと思うかもしれない．数学において排中律を捨てると，帰謬法 (背理法) による証明は誤った証明ということになる．

一般的に科学は正しいと考えられているが，科学は論証を基盤としており，論証は論理的原理を前提としている．科学は世界を解釈する学問であるが，そもそも根っこである論理的原理の決定において世界の解釈を誤っていたら，そこからどれだけ推論しても，世界の解釈として正しいものにはならない．正しい論証は，前提が成り立つ範囲内で正しいのである．科学はその論理的原理が妥当な世界に限って正しい，と考えなければならない．

1.3　論理の誤り

論理は言葉で語られるが，言葉は曖昧であり，容易に誤った推論を導く．よく見られるのが，多義的な言葉を使った詭弁である．ある言葉 B に B′ と B″ の二つの意味があるとする．「A のとき B′ である」と「B″ のとき C である」が言えるとき，つぎのような論理が展開されることがある．

A だから B (B′) である.
B (B′′) なので C である.
ゆえに A だから C である.

正しい論理は本来単線であるが，言葉に複数の意味があると，論理が複線になってしまう．言葉の解釈を論理の途中で都合よく変えてしまうと，複数の論理の線上を移動することになり，本来つながらない論理がつながっているように見えてしまう．特に抽象的な言葉を使っている場合，こういうことが起こりやすく，また間違いに気づきにくい．

言葉の多義性は，論点のすり替えにも使われる．表現 A に，中立的な意味 A′ と偏った意味 A″ があるとする．誰かが意味 A′ の表現のつもりで「A」と言ったときに，わざと A″ の意味で解釈して「A″ とはなにごとだ！あいつはなんとか主義者に違いない」と批判するという感じである．

上の例の「なんとか主義者に違いない」などの「レッテル貼り」も，言葉の曖昧さのなせる業である．個々人の相違を無視して一つの言葉の中に放り込んでしまい，言葉の持つイメージを相手に貼り付けてしまう．

言葉の抽象度の違いを利用した詭弁も考えられる．

A は B である.
C は B である.
ゆえに A は C である.

数学ではよく使われる証明法であるが，A，B，C に単純に言葉を当てはめると，妙な論理になる．

猫は動物である．
犬は動物である．
ゆえに猫は犬である．

この論理の誤りは，抽象度の違う言葉を同列に扱っているところである．普通こんな馬鹿げた論理はありえないと思うかもしれないが，抽象的な言葉が使われているときには，こういった詭弁を見抜けない可能性がある．

以上では，言葉の曖昧さがもたらす弊害を見てきた．契約書など，言葉の解釈の違いが面倒な論争を巻き起こす心配のある場合には，まず言葉の定義から入る．数学もはじめに定義ありきである．正しい論理を展開しようとする者は，人によって解釈が違ってしまわないように，使用する言葉の意味を限定しなければならない．

具体的になにを指しているのかわからない言葉を使って展開される論理には，どこかに嘘があると思っていい．ついでながら，誰も反論できない正論にも気をつけなければならない．ペテン師ほど正論を使うものだから．

1.4　公理主義と記号論理学

認識や思考の曖昧さを克服するために考え出されたのが，公理主義と記号論理学である．

従うべきルール (公理) を設定し，それだけを用いて論理を展開するという態度を，公理主義という．公理が「正しい」かどうかは問わない．経験に反していてもよい．設定した公理からどんな理論ができあがるのかが関心の的なのである．

すべては公理だけから論理的に導かれる．感覚を差し挟む余地はない．公理と論理の方向を決めれば，結論は形式的に (機械的に) 導かれることになる．こういう考え方を形式主義という．

たとえば，円を 1 つ描く．その円上の 1 つの点を中心としてもう 1 つ円を描く．この場合，2 つの円は必ず交わるはずである．これは確かな事実であるように思うが，経験的な認識であり，論理的ではない．絵を描いてみれば，2 円が交わることは明らかではないか．確かにそうである．だが，描いた円は厳密な円ではない．頭の中で描いてみても同じである．彼と彼女の頭の中に描かれた「円」が厳密に同じ「円」であると，どうやって保証するのか？

互いの認識の不一致や，感覚的な誤りを避けるためには，個々人の主観によらない，互いに承認された約束事だけを使って論理を展開しなければならない．そのための公理であり，形式的な論理である．すべてを公理から形式的に導くことによって経験を排除し，誤謬が入り込む余地をなくそうというのが，公理主義・形式主義の目的である．

公理主義・形式主義は，公理というルールを決め，そのルールに則って形式的に行う「ゲーム」である．チェスのようなものだ．ルールが違えばゲームも違う．設定した公理が違えば，展開される論理も，導かれる結論も違う．それは単純に違うのであって，どれが正しくてどれが間違っているかという議論には意味がない．それは論理の外の話である．

そう考えると，科学と非科学の関係は，チェスと将棋のような関係であるといえる．将棋で敵の駒を取って自分の駒として使う人を見て，チェスのプレイヤーが「インチキだ！」と言ってみたところで意味はない．チェスにはチェスの，将棋には将棋の論理がある．チェスのルールで将棋のプレイの正しさを証明したりはできない．同様に，非科学的なものをすべて誤りであると言うことはできない．それは,「非チェス的」なゲームはすべて誤りであると言うに等しい無茶なのである．せいぜい「現実をうまく説明できていない」ぐらいのことしか言えない．科学的「事実」は 100 パーセント仮説である．仮説でない事実は，数学的事実のような，われわれの頭にだけ存在するものだけだ．

形式主義を実現しようとすると，言葉の曖昧さが問題になる．曖昧な言葉の代わりに，記号を使って論理を展開するのが記号論理学である．これは論理を代数に変えてしまおうという試みであり，ライプニッツが構想し，ブール，ペアノ，フレーゲらを経て，ラッセルとホワイトヘッドによって形になった．

1.5　記号論理学

1.5.1　命題

ある主張を命題という.「クジラは哺乳類である」などである．これを A などと表そう．命題は真 (1) と偽 (0) の 2 つの値をとる．

命題 A，B の真偽が一致するとき，A と B を等しいといい，$A = B$ で表す．等しい関係には，つぎのような性質がある．

$$
\begin{gathered}
A = A \\
A = B \text{ ならば } B = A \\
A = B, B = C \text{ ならば } A = C
\end{gathered}
$$

命題を構成する具体的な要素を定数という.「クジラ」などである．一方，具体的でない命題の構成要素を変数という．変数を x として,「x は…である」という表現を述語という．これを $P(x)$ と表すことにしよう．たとえば「クジラ」を a とし,「x は哺乳類である」を $P(x)$ と表すと,「クジラは哺乳類である」は $P(a)$ と表される．命題は, 定数，変数，述語と，以下で述べる演算子によって記述される．

1.5.2　演算子

命題に対して，つぎのような演算子を定義する．

否定¬

A	$\neg A$
0	1
1	0

かつ∧

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

または∨

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

「猫」と「犬」をそれぞれ a，b で表し,「x は動物である」を $P(x)$ で表すと,「猫と犬は動物である」は $P(a) \wedge P(b)$ と表される．

「かつ $\wedge$」と「または $\vee$」には，つぎのような性質がある．

$$A \wedge A = A$$
$$A \vee A = A$$

$$A \wedge B = B \wedge A$$
$$A \vee B = B \vee A$$

$$(A \wedge B) \wedge C = A \wedge (B \wedge C)$$
$$(A \vee B) \vee C = A \vee (B \vee C)$$

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$

$$\neg(A \wedge B) = \neg A \vee \neg B$$
$$\neg(A \vee B) = \neg A \wedge \neg B$$

「A ならば B」という命題を，$A \Rightarrow B$ のように表す．これは $\neg A \vee B$ と表すことができる．

ならば $\Rightarrow$

A	B	$A \Rightarrow B$	$\neg A \vee B$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

奇妙なのは， A が偽で B が真のときに $A \Rightarrow B$ が真であるということである．これは，結論が単独で真ならば，前提が真であろうと偽であろうと命題は真であると考えるということである.「猫が犬であるならば猫は哺乳類である」は真なのである．奇妙だが，ここは「正しいか正しくないか」ではなく,「真」と「偽」と便宜上よばれる 2 つの値をとる特殊な数学を扱っているのだと割り切って考える．

記号 $\Rightarrow$ には，つぎのような「推移性」がある．

$$(A \Rightarrow B \wedge B \Rightarrow C) \Rightarrow (A \Rightarrow C)$$

$A \Rightarrow B$ に対して，$B \Rightarrow A$ を逆といい，$\neg A \Rightarrow \neg B$ を裏という．裏の逆 $\neg B \Rightarrow \neg A$ を対偶という．命題が真のとき，その逆は必ずしも真ではないが，対偶はもとの命題と真偽が一致する．

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$\neg A \Rightarrow \neg B$	$\neg B \Rightarrow \neg A$
0	0	1	1	1	1
0	1	1	0	0	1
1	0	0	1	1	0
1	1	1	1	1	1

特に $(A \Rightarrow B) \wedge (B \Rightarrow A)$ を $A \Leftrightarrow B$ と表す．$A \Leftrightarrow B$ は $A = B$ のとき真である．

命題 C について，その肯定と否定が同時に成り立つとき，つまり $C \wedge \neg C$ が (本来は真になりえないにもかかわらず) 真になるとき，その論理は矛盾しているという．$A \Leftrightarrow B$ について

$$\begin{aligned} A \Leftrightarrow B &= (A \Rightarrow B) \wedge (B \Rightarrow A) \\ &= (\neg A \vee B) \wedge (\neg B \vee A) \\ &= (\neg A \vee B) \wedge (A \vee \neg B) \end{aligned} \tag{1}$$

なので，$A = C$，$B = \neg C$ とすると

$$C \Leftrightarrow \neg C = (\neg C \vee \neg C) \wedge (C \vee C) = C \wedge \neg C \tag{2}$$

つまり，$C \Leftrightarrow \neg C$ が導かれると，その論理は矛盾していることになる．

変数を限定する演算子をつぎのように定義する．

$\forall$ すべての

$\exists$ 存在する

「x は人間である」を $P(x)$ で表し,「x は哺乳類である」を $Q(x)$ で表すと,「すべての人間は哺乳類である」は $\forall x(P(x) \Rightarrow Q(x))$ と表される.「x は猫好きである」を $R(x)$ で表すと,「猫好きの人間は存在する」は $\exists x(P(x) \wedge R(x))$ と表される．

1.5.3 証明

記号論理学の基礎的な道具はそろったので，ひとつ証明に挑戦してみよう.「クジラは哺乳類である．すべての哺乳類の子供はお乳で育つならば，クジラの子供はお乳で育つ」を証明しよう.「クジラ」を a,「x は哺乳類である」を $P(x)$,「x の子供はお乳で育つ」を $Q(x)$ で表すとしよう.「クジラは哺乳類である」は $P(a)$,「すべての哺乳類の子供はお乳で育つ」は $\forall x(P(x) \Rightarrow Q(x))$,「クジラの子供はお乳で育つ」は $Q(a)$ で表される．前提である $P(a)$，$\forall x(P(x) \Rightarrow Q(x))$ から結論 $Q(a)$ を導くことができれば，証明完了である．

$P(a)$	前提
$\forall\, x(P(x) \Rightarrow Q(x))$	前提
$P(a) \Rightarrow Q(a)$	すべての x には当然 a も含まれるので, a を当てはめる．
$Q(a)$	前提 $P(a)$ と $P(a) \Rightarrow Q(a)$ が真ならば, $Q(a)$ も真である．
証明終わり	

大事なことは，上の例では経験によっておらず，ルールに則って機械的に証明が行われていることである．$P(a)$，$P(a) \Rightarrow Q(a)$ から $Q(a)$ が導かれるのは,「$P(a) \Rightarrow Q(a)$ で $P(a)$ が正しいのなら，当然 $Q(a)$ が導かれるだろう」という感覚的なものではなく，あくまで $A \Rightarrow B$ の真偽値の表によるのである．

参考文献

[1] バートランド・ラッセル: 哲学入門，筑摩書店 (2005).

[2] 野崎弘明: 詭弁論理学，中央公論新社 (1976).

[3] 金子洋之: 記号論理入門，産業図書 (1994).

2　集合

2.1　集合

集合とは，もののあつまりである．たとえば,「りんご」,「みかん」,「バナナ」の集合 A をつぎのように表す．

$$A = \{\text{ りんご}, \text{みかん}, \text{バナナ }\}$$

集合を構成する「りんご」などを集合の元 (げん) という.「りんご」が集合 A の元であることをつぎのように表す．

$$\text{りんご} \in A$$

このとき,「りんごは集合 A に属する」とか「りんごは集合 A に含まれる」などという．$\neg(\text{りんご} \in A)$ を りんご $\notin A$ と表す．

ある集合の元を表す変数を x，y とする．x と y が同じ元を表すとき $x = y$ と表す．このとき x と y は等しいという．等しい関係には，つぎのような性質があるものとする (ここで a，b，c をある集合の元とする).

$$a = a$$
$$a = b \Rightarrow b = a$$
$$(a = b) \land (b = c) \Rightarrow a = c$$

また，$\neg(x = y)$ を $x \neq y$ と表す．

集合の元は集合でもかまわない．つぎのような集合も考えられる．

$$\{\text{ いぬ}, \{\text{ ねこ}, \{\text{ チーター}, \text{ライオン }\}\}\}$$

以上のように集合の元を一つずつ指定していく方法では,「くだものすべての集合」などを表現するのは難しい．そこで,「ある性質をみたすものの集合」という表現をとる．この表現を内包的な表現という．元を表す変数 を x とし，性質 (記号論理でいえば述語) を $P(x)$ とすると，性質 $P(x)$ をみたす x の集合 A は，つぎのように表現される．

$$A = \{x | P(x)\}$$

つまり，$P(a)$ が真のとき $a \in A$ ということである．

「くだものすべての集合」F はつぎのようになる．

$$F = \{x | x \text{ はくだものである }\}$$

集合 A の元がすべて集合 B に含まれるとき，A は B の部分集合であるといい，$A \subseteq B$ と表す．

$$A \subseteq B = \forall x(x \in A \Rightarrow x \in B)$$

記号 $\Rightarrow$ の推移性より，つぎのことが成り立つ．

$$(A \subseteq B) \wedge (B \subseteq C) \Rightarrow A \subseteq C$$

$A \subseteq B$ かつ $B \subseteq A$ のとき，A と B は等しいといい，$A = B$ と表す．任意の集合 A，B，C に対して，等しい関係にはつぎのような性質がある．

$$A = A$$
$$A = B \Rightarrow B = A$$
$$(A = B) \wedge (B = C) \Rightarrow A = C$$

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

1 つも元を含まない集合を空集合といい，$\emptyset$ で表す (ギリシャ語の ϕ (ファイ) とは違うが，似ているのでよく代用される)．空集合 $\emptyset$ はつぎのように定義できる．

$$\emptyset = \{x | x \neq x\}$$

集合 A のすべての部分集合全体からなる集合を，A のべき集合という．たとえば $A = \{1, 2, 3\}$ のとき，A のべき集合はつぎのようになる．

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

集合の元の個数が n のとき，そのべき集合の元の個数は 2^n である．

集合 A と B の共通部分を $A \cap B$ と表す．また，集合 A と B を合わせた集合を和集合といい，$A \cup B$ で表す．

$$A \cap B = \{x | x \in A \wedge x \in B\}$$
$$A \cup B = \{x | x \in A \vee x \in B\}$$

集合の集合 $A = \{A_1, A_2, \cdots, A_n\}$ のすべての元の共通部分と和集合は，それぞれつぎのように表現する．

$$\bigcap_{i=1}^{n} A_i$$
$$\bigcup_{i=1}^{n} A_i$$

集合を，お互いに重ならないような部分集合に分割したものを，直和分割という．集合 A を直和分割した部分集合を A_i $(i=1,2,\cdots,n)$ と表すと，つぎの性質をみたす．

$$\bigcap_{i=1}^{n} A_i = \emptyset$$

$$A = \bigcup_{i=1}^{n} A_i$$

たとえば，$\{1,2,3,4,5\}$ に対して $\{1,3\}$，$\{2,5\}$，$\{4\}$ は直和分割である．

集合 A から集合 B の元を除いたものを A と B の差といい，$A-B$ と表す．

$$A-B=\{x|x\in A\wedge x\notin B\}$$

考えている対象について，任意の集合の元がとりうる範囲が決まっているとき，その範囲の元全体の集合を全体集合という．全体集合 U が存在するとき,「集合 A 以外の集合」を A の補集合といい，$\bar{A}$ で表す．

$$\bar{A}=U-A$$

記号 $\cap$，$\cup$ にはつぎの性質がある．すべて論理記号の性質から導かれる．

$$A\cap A=A$$
$$A\cup A=A$$

$$A\cap B=B\cap A$$
$$A\cup B=B\cup A$$

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

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

$$\overline{A\cap B}=\bar{A}\cup\bar{B}$$
$$\overline{A\cup B}=\bar{A}\cap\bar{B}$$

集合 A，B からそれぞれ元 a，b を取り出して順番にならべたもの (a,b) を順序対という．順序対 (a,b) は集合としてつぎのように定義できる．

$$(a,b)=\{\{a\},\{a,b\}\}$$

定義より $(a,b)\neq(b,a)$ である．

集合 A の元と集合 B の元がつくる順序対全体の集合を A と B の直積といい，$A\times B$ と表す．たとえば，$A=\{1,2,3\}$，$B=\{4,5\}$ とすると，$A\times B$ はつぎのようになる．

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

順序に意味があるので，一般に $A \times B \neq B \times A$ である．

$a_i \in A_i$ のとき，$A_1 \times A_2 \times \cdots \times A_n$ を $(a_1, a_2, \cdots a_n)$ と表す．$A_i = A$ のとき，$A_1 \times A_2 \times \cdots \times A_n$ を A^n と表すことがある．

幾何学的な立場では，直積を空間という．実数の集合を $\mathbf{R}$ とすると，$\mathbf{R} \times \mathbf{R} \times \mathbf{R} = \mathbf{R}^3$ を 3 次元空間といい，その元 (x, y, z) を空間の座標という．

2.2 写像

集合同士の元の対応を写像という．「集合 A から集合 B への写像」は A の部分集合と B の部分集合の直積として定義される．A から B への写像 f を $f : A \to B$ と表す．f によって $a \in A$ と対応づけられた B の元を a の像という．a の f による像は $f(a)$ と表される．

$A' \subseteq A$ のとき，$f(A') = \{f(x) | x \in A'\}$ を写像 f による A' の像という．

$f(A) = B$ のとき，写像 f は A から B への全射であるという．写像 f が A から B への 1 対 1 の写像であるとき，すなわち A の任意の元 a，a' に対して $a = a'$ のときに限って $f(a) = f(a')$ であるとき，f は A から B への単射であるという．写像 f が全射かつ単射であるとき，f は A から B への全単射であるという．

例えば，女性のグループと男性のグループがあるとしよう．女性はそれぞれ 1 人だけ好みの男性を選ぶものとする．任意の女性を指定したら，その女性の好みの男性がわかる，という写像を考える．男性の中にどの女性からも好かれていない男性がいる場合は，女性の好みの写像は全射ではない．すべての男性が誰かしらに好かれている場合，全射である．ある男性のことを好きな女性が複数いれば，写像は単射ではない．女性の好みが重なっていなければ，単射である．女性と男性の人数が同じで，女性の好みが重なっていない場合，写像は全単射である．

A の任意の元 a を a 自身と対応づける写像 $I_A(a) = a$ を，A の恒等写像という．

B の一つの元を b とする．A の任意の元 x と b を対応づける写像を，A から B への値 b への定値写像という．

写像 $f : A \to B$ が全単射であるとき，$a \in A$，$b \in B$ として $f(a) = b$ に対して $f^{-1}(b) = a$ なる $f^{-1} : B \to A$ も写像である．この f^{-1} を f の逆写像という．

集合 A，B，C に関して写像 $f : A \to B$ と写像 $g : B \to C$ があるとき，f と g を順番に適用する A から C への写像を f と g の合成写像といい，$f \circ g$ と表す．

解析学においては，数の集合どうしの写像のことを関数という．

2.3 無限

集合の元の個数を集合の濃度あるいは基数という．集合の濃度を数えるという操作について考えてみよう．

数えるという操作は，ものにそれぞれ番号をつけていくことである．たとえば，りんご集合 { りんご, りんご, りんご } (それぞれ違うりんご) のりんごの数を数える場合は,

$\{$ りんご 1, りんご 2, りんご 3$\}$ と番号をつけることによってりんごが 3 つあることがわかる．元に番号がつけば，自然数の部分集合からりんご集合への全単射写像 $f(x) =$ りんご x が定義できる．つまり，数えるとは，自然数の部分集合からの全単射写像を定義することである．

偶数の個数を数えてみよう．偶数は，自然数からの写像 $f(x) = 2x$ によって得られる．これは自然数全体で定義される．自然数の部分集合である偶数と自然数全体が，写像 f によって一対一で対応するのである．このように，全体から自身の部分集合への全単射写像が定義できるような集合を，無限集合という．無限集合でない集合を，有限集合という．

無限には，数えられる無限と数えられない無限がある．数えられる無限を可算無限，数えられない無限を不可算無限という．数えることは自然数からの全単射写像を定義することであったので，可算と不可算の違いは，自然数からの全単射写像を定義できるかどうかの違いである．

整数は自然数からの全単射写像が存在するので，可算無限集合である．単純に考えると，自然数は整数の正の数にあたるので，整数の個数は自然数よりも 2 倍は多いはずである．有限集合に関していえばそのとおりである．だが，無限集合としての濃度は自然数と整数で同じなのである (このような奇妙な話が「個数」のイメージと合わないので,「濃度」などと呼んでごまかしているわけである)．また，実数には自然数からの全単射写像が存在しないので，不可算無限集合である．このように，無限にも多い・少ないがある．

2.4　公理的集合論

集合を単なる「もののあつまり」と考えたとき，そこから導かれる集合論には矛盾が含まれる．

例えば,「ラッセルのパラドックス」というものがある.「自分自身を含まない集合」の集合 R を考えよう．R は自分自身を含むだろうか，含まないだろうか．R が自分自身を含むと仮定すると，R は「自分自身を含まない集合」ではないので，R に含まれない．R が自分自身を含まないと仮定すると，R は「自分自身を含まない集合」なので，R に含まれる．このように，集合 R の存在を認めてしまうと，にっちもさっちもいかない状況に陥る．

このような矛盾を避けるために，集合論の公理化が試みられた．現在一般的に使われている公理系はツェルメロ=フレンケルの公理系 (ZF) というもので，以下の公理からなる．

- 外延性の公理: 二つの集合の元がすべて等しいとき，二つの集合は等しい．
- 空集合の公理: 空集合は存在する．
- 非順序対の公理: A，B が集合であるとき，A，B のみを元とする集合が存在する．
- 合併の公理: 集合の元の合併からなる集合が存在する．

- 無限集合の公理: 空集合を元とし，元 x を含むとき，$x \cup \{x\}$ も含むような集合が存在する．
- べき集合の公理: べき集合は存在する．
- 分出公理: 任意の集合 A に対して，A の元で性質 $P(x)$ を満たすような x 全体は集合である．
- 置換公理: 集合と一対一の対応がある集まりは集合である．
- 正則性の公理: すべての空でない集合 A に対して，$A \cap a = \emptyset$ なる A の元 a が存在する．
- 選択公理: 空でない集合の各元から 1 つずつ元を取ってきたような集合が存在する．

正則性の公理はわかりにくい．これは，すべての集合と共通部分をもたない集合の元が存在するということである．集合の元の元の元の…とたどっていくと，その操作はどこかで止まるということで，要するに，集合でない元，集合を構成する最小の「原子」が存在するということである．

ラッセルのパラドックスの集合 R は，記号で書くと $R = \{x | x \notin x\}$ である．これは上記の公理系からは構成できない．つまり，ZF 公理系上では R はそもそも集合ではないので，パラドックスは排除される．すなわち，分出公理より，内包的に定義される集合 S は，A をある集合として $S = \{x | x \in A \wedge P(x)\}$ の形で書かなければらない．あえて R のようなものを ZF 公理系上で定義しようとすれば $R' = \{x | x \in A \wedge x \notin x\}$ となる．さて，R' は A に含まれるだろうか？ $R' \in A$ と仮定して，$R' \notin R'$ とすると，R' の定義により R' は R' に含まれるため $R' \in R'$．また，$R' \in R'$ とすると，R' の定義により R' は R' に含まれないため $R' \notin R'$ である．つまり，$R' \in R' \Leftrightarrow R' \notin R' = R' \in R' \wedge \neg(R' \in R')$ ということで矛盾．したがって $R' \notin A$ であり，R' は自分自身を明確に含まず，パラドックスにならない．また，そもそも正則性の公理のため自分自身を含む集合というものを定義できない．

参考文献

[1] 竹内外史: 集合とはなにか，講談社 (2001).

[2] 松坂和夫: 集合・位相入門，岩波書店 (1968).

[3] デーデキント: 数について，岩波書店 (1961).

[4] 齋藤正彦: 数学の基礎 集合・数・位相，東京大学出版局 (2002).

3　自然数

3.1　数

数とはなにか．人間の脳は，見たものそのものではなく，それらに共通する性質を見ようとする．ものごとを抽象化して把握しようとする．数もおそらく，同じ数のものの集まりから抽象化された量として把握されたものであろう．人間の脳は，5 つくらいのものまでは，見ただけで数を把握できるそうである．それより大きな数になると，数えないとわからない．

小さな数の概念を得た人間は，つぎは数えることを考えたであろう．ものの集まりどうしの個数の関係を調べるのは簡単である．ひとつずつペアを作っていけばよい．どちらかが余ったら，余ったほうの個数が多いとわかる．余りがでなければ，双方同じ数である．

相互の個数の関係だけで数を考えるのは不便である．誰かに「りんごはどのくらいあるか」と問われて,「そばにあったみかんと同じだけある」と応えては，答えになっていない．りんごの数を教えたくば，りんごを相手のところに持っていって，相手のそばにあるものと比べなければならない．2，3 個ならよかろうが，100 個もりんごがあった日には，大変である．

そこで，数えるための道具が考え出された．それは指や石，木の板につけた切傷などであった．指でりんごの個数を数えておけば，りんごの数を知らせたいときは，指を示せばよい．わざわざりんごを運んでくるにはおよばない．

ただ，指や石は数を保存できない．石や木の板は少しかさばる．そこで表現を節約することが考えられる．古代人で，指を使って数えた人々は，指では足りない数を指や手，腕や体の向きなどのポーズに割り当てて表現した．石を使った人々は，小さな石が 10 個集まったら大きな石 1 つと置き換える，などということをした．今のお金と同じ表現方法である．切傷を使って数えた人々も，きっと同じようなことを考えたであろう．

人間は言葉を操る生き物である．当然，数を言葉で表そうと考えた．もの 1 つから始めて，ものが 1 つ増えるたびにその状態に名前をつけていく．こうして数を言葉で表すことができるようになる．ただ，新しい数が現れるたびに新しい名前をつけていたのでは，覚えるのが大変である．そこは石と同じような方法をとる．言葉になってしまえば，数は指や石や切傷ではなく，現在われわれが考えるような「数」の概念になる．

人間が文字を持ったとき，数も文字で表そうと考えるのは自然である．はじめは木につけた切傷であったものが，節約された文字表現となる．ローマ数字は，石による数え方を文字にしたようなものだ．321 という数を考えよう．ローマ数字では $C = 100$，$X = 10$，$I = 1$ で，$321 = CCCXXI$ と表す．300 を CCC とはなんと文字の無駄遣い，3 つの C とでもすればよいではないか．そういう考え方の数字が，漢数字である．321 は「三百二十一」と表す．それでも数が大きくなると，表現がおおげさになる．1234567890 は「十二億三千四百五十六万七千八百九十」となる．

先ほどから何気なく使っている ″321″ などのわれわれになじみの表現は，位取り表記というものである．数のまとまりを文字の位置で表すことによって，文字を節約する．今のところ最も経済的な数の表記法である．アラビア数字と呼ばれているが，インド人が考えたものである．インドからアラビア人が採り入れ，アラビア人によってヨーロッパにもたらされた．それでヨーロッパの人々は「アラビアの数字」と呼んだのである．

数の認識から表記法まで見てきたが，結局，数とはなんなのか．われわれの数の認識の仕方に立ち戻れば，数とは「同じ数のものの集まりすべてを，その中のある集まりで代表し，それに名前をつけたもの」であるといえる．

3.2 対等

上では数の概念について考えた．以下では「自然数」を定義していきたい．まず，われわれは自然数を知らないという立場に立とう．

「同じ数のものの集まりすべてを，その中のある集まりで代表し，それに名前をつけたもの」が数であると考えよう．自然数を宇宙のかなたに放り投げた今のわれわれとしては,「同じ数」だの「同数」などという表現を素朴に受け入れるわけにはいかない.「ものの集まり」は集合と考えるとして (「ものの集まりすべて」を集合と考えてしまうとラッセルのパラドックスが起こりうることに注意),「同じ数」とはなにを意味するのかを考えよう．

集合 A と B の元が同じ個数である，つまり A と B が同じ濃度であるということは，A と B のすべての元でペアをつくった場合に余りがでないということである．これは，A，B に関する全単射写像が存在するということを意味する．集合 A，B に全単射写像が存在するとき，A と B は対等であるという．A と B が対等であることを $A \sim B$ と表すと，対等にはつぎのような性質がある．

$$
\begin{gathered}
A \sim A \\
A \sim B \Rightarrow B \sim A \\
(A \sim B) \wedge (B \sim C) \Rightarrow A \sim C
\end{gathered}
$$

われわれの「数」を，対等を用いて定義しよう．3 つのりんごからなるりんご集合を用意し，それと対等なるすべての集合をあつめる．この「3 つのりんごからなるりんご集合と対等なるすべての集合の集まり」(これは集合とは考えない) に ″3″ という名前をつける．そういう風にして,「1 つのりんごからなるりんご集合〜」を ″1″,「2 つのりんごからなるりんご集合〜」を ″2″…としていくと,「数」を得る．

ただし，この方法には問題がある．たとえ世界中のりんごを集めたとしても，りんご集合は有限集合である．一方，自然数は無限集合である．りんご集合を数の代表の集合とするわけにはいかない．

3.3 自然数

われわれに必要なのは，りんごの代わりとなる数えるための道具，指や石，木の板につけた切傷にあたるものである．しかも，それは無限集合でなくてはならない．

ツェルメロ=フレンケルの公理系 (ZR) には，無限集合の公理がある．これが使えそうである．数えるための集合を A と呼ぶことにする．空集合 $\emptyset$ を A の元とする．a が A の元のとき $a \cup \{a\}$ も A の元である．したがって $\emptyset \cup \{\emptyset\}$ は A の元である．それならば $\emptyset \cup \{\emptyset\} \cup \{\emptyset \cup \{\emptyset\}\}$ も A の元である…このような調子で A の元を次々と生成していき，それぞれに "0", "1", "2", …と名前をつける．

$$
\begin{aligned}
&0 : \emptyset \\
&1 : 0 \cup \{0\} = \{\emptyset, \{\emptyset\}\} \\
&2 : 1 \cup \{1\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
&3 : 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
&\cdots
\end{aligned}
$$

上の操作を続けていくと，自然数の集合 $\mathbf{N}$ を得る．

$$\mathbf{N} = \{0, 1, 2, \cdots\}$$

これでわれわれが求めるものを得た…とここで安心するわけにはいかない．自然数の集合 $\mathbf{N}$ が確定した瞬間，自然数の次の数が得られる．$\mathbf{N}$ に ω という名前をつけると，その次の数は $\omega + 1 = \mathbf{N} \cup \{\mathbf{N}\}$ であり，さらに続く．

$$
\begin{aligned}
&\omega : \mathbf{N} \\
&\omega + 1 : \mathbf{N} \cup \{\mathbf{N}\} \\
&\omega + 2 : \omega + 1 \cup \{\omega + 1\} \\
&\cdots \\
&2\omega : \{0, 1, 2, \cdots, \omega, \omega + 1, \omega + 2, \cdots\} \\
&2\omega + 1 : 2\omega \cup \{2\omega\} \\
&\cdots \\
&\omega^2 : \{0, 1, 2, \cdots, \omega, \cdots, 2\omega, \cdots, 3\omega, \cdots\} \\
&\cdots \\
&\omega^\omega : \{0, 1, 2, \cdots, \omega, \cdots, \omega^2, \cdots, \omega^3, \cdots\} \\
&\cdots \\
&\omega^{\omega^\omega} : \{0, 1, 2, \cdots, \omega, \cdots, \omega^\omega, \cdots, 2\omega^\omega, \cdots, 3\omega^\omega, \cdots\} \\
&\cdots
\end{aligned}
$$

このようにずっと続いていく．上の操作で得られる集合を超限順序数という．

われわれが欲しいのは自然数である．大きすぎる集合は必要ない．上の操作で得られる集合で，濃度が最小である集合を自然数の集合と定義しよう．すなわち

$$\forall x (0 \in x \land \forall y (y \in x \Rightarrow y \cup \{y\} \in x) \Rightarrow \mathbf{N} \subseteq x)$$

を満たす集合 $\mathbf{N}$ を自然数の集合とする．

3.4 自然数の性質

われわれが得た自然数の性質を見ていこう．

任意の自然数 n にはその次の数 (n' と表そう) が 1 つしかも唯一つ存在する．われわれの自然数の構成方法により $n' = n \cup \{n\}$ である．n の次の数を作る方法は $n \cup \{n\}$ に限るので，n' が唯一なのは当然である．これは，自然数の次の数をたどっていっても枝分かれしたりしないということである．

次の数が 0 になるような自然数は存在しない．$n' = n \cup \{n\}$ なので，この方法では 0 すなわち $\emptyset$ を構成できない．これは，自然数全体がループになっていないということである．

m，n を任意の自然数として，$m' = n'$ ならば $m = n$ である．$m' = m \cup \{m\}$，$n' = n \cup \{n\}$ なので，$m' = n'$ となるのは $m = n$ のときだけである．これは，自然数の次の数をたどっていっても以前の数に戻ってきたりしないということである．

われわれの構成した自然数では，任意の自然数 m は，その後の自然数 n の部分集合である．このことから m と n の大小関係を定義できる．$m \subseteq n$ を $m \leq n$ と定義しよう．同様に $<$，$\geq$，$>$ をつぎのように定義できる．

$$
\begin{gathered}
m \subset n \Rightarrow m < n \\
\neg(m < n) \Rightarrow m \geq n \\
\neg(m \leq n) \Rightarrow m > n
\end{gathered}
$$

部分集合の性質より，つぎのことが成り立つ (m，n,l は自然数とする).

$$
\begin{gathered}
m \leq m \\
(m \leq n) \land (n \leq m) \Rightarrow m = n \\
(m \leq n) \land (n \leq l) \Rightarrow m \leq l
\end{gathered}
$$

m と n の関係は $m = n$，$m < n$，$m > n$ のどれかである．

自然数は整列性を持つ．整列性とは「自然数の集合の任意の空でない部分集合は最小元を持つ」という性質である．集合 A の 1 つの元を a として，A のいかなる元 n に対しても $a \leq n$ が成り立つとき，a を最小元という．あっさり言えば，整列性とは，自然数の任意の範囲には最小値があるということである．とりたてて言うほどの性質ではないように思うかもしれないが，実数 x の開区間 $a < x < b$ には最小値が存在しないことを考えると，整列性は自然数特有の性質である．ある空でない自然数の集合を A とし，A のすべての元 m に関して $n < m$ となるような自然数 n の全体を B とする．このとき A の最小元は，われわれの自然数の定義によれば B である．

自然数の整列性から，数学的帰納法を導くことができる．ある自然数の集合 A が (1) A は 0 を含む (2) 自然数 m が A に含まれるならば m の次の数も A に含まれるとき，A はすべての自然数の集合 $\mathbf{N}$ と一致する (数学的帰納法の原理)．A に含まれない自然数の全体を B としよう．もし $B \neq \emptyset$ なら，整列性より B は最小元を持つ．B の最小元を b とする．(1) より $b \neq 0$ である．したがって次の数が b になるような数 b_0 が存在する．b は B の最小元なので $b_0 \in A$ である．(2) より $b_0 \in A$ ならば $b \in A$ である．

つまり $b \in B$ かつ $b \in A$．これは矛盾である．したがって $B = \emptyset$ すなわち $A = \mathbf{N}$ である．

数学的帰納法：自然数 x (次の数を x' とする) について命題 $P(x)$ が与えられたとして (1) $P(0)$ は正しい (2) 任意の自然数 n に対して $P(n)$ が正しいと仮定すれば $P(n')$ も正しいとき，$P(x)$ はすべての自然数 x に対して正しい．$P(x)$ が正しいような x すべての集合を A とすれば，上の (1)，(2) が示されたとき，A は数学的帰納法の原理の (1)，(2) を満たす．したがって $A = \mathbf{N}$．ゆえに $P(x)$ はすべての自然数 x に対して正しい．

3.5 ペアノの公理

以上でわれわれは自然数を構成した．ただ，自然数の定義の仕方には別の方法もある．構成して性質を導くのではなく，はじめに性質を決めてそこから数学的実体を定義するという公理的定義の方法である．

自然数の公理として用いられるものは，次のペアノの公理である．

- 0 は自然数である．
- 任意の自然数には「次の数」が存在し，それは自然数である．
- 任意の 2 つの自然数は，同じ次の数を持たない．
- 0 を次の数に持つ自然数は存在しない．
- 数学的帰納法の原理：S を自然数の集合とする．(1) S は 0 を含む (2) 自然数 n が S に含まれるならば n の次の数も S に含まれるとき，S はすべての自然数の集合を含む．

以上の公理を満たすようなものが自然数というものである，とするわけである．われわれが構成した $\mathbf{N}$ は，この公理を満たしている．

性質から実体を確定するというのは奇妙な感じもするが，数学が扱うものは具体も抽象も概念という抽象物である．概念はわれわれの脳が経験から作り出すものである．各人の経験が異なれば，同じ言葉を使っていても頭の中では別のものである可能性がある.「りんご」の研究者が二人いるとして,「りんご」という言葉から一方がりんごを，もう一方がみかんを思い浮かべるというような状況はありそうにないが，対象物が概念である場合には同様なことが起こりうる．それを避けるために，公理によって経験を排除してしまう必要がある．

ところで，数学的帰納法の原理は少し贅沢な公理のような気がする．整列性の公理のほうがより基本的でよいのではないかと思うかもしれない．帰納法は整列性から導かれたが，整列性は帰納法で証明することができる．つまり帰納法の原理も整列性の公理も実質同じものである．だったら，はじめから帰納法の原理を公理として認めたほうが便利ではある．

3.6 加法

自然数の加法を次のように定義する (m，n を自然数とし，n' を n の次の数とする)．

$$f_m(0) = m$$
$$f_m(n') = (f_m(n))'$$

$f_m(n)$ を $m+n$ と表すと，次のようになる．

$$m+0 = m$$
$$m+n' = (m+n)'$$

証明は省くが，上の性質を満たす写像はただ一つしか存在しない．

この定義がわれわれの知っている加法として機能することを確認しておこう．たとえば，$2+3=5$ は次のように導く．

$$\begin{aligned}
2+3 &= 2+2' \\
&= 2+(1')' \\
&= 2+((0')')' \\
&= (2+(0')')' \\
&= ((2+0')')' \\
&= (((2)')')' \\
&= ((3)')' \\
&= 4' \\
&= 5
\end{aligned}$$

われわれが日常的に用いる自然数の加法の性質を定義から導いていこう．

$0+m=m$ である．自然数の恒等写像 $I_{\mathbf{N}}$ は f_0 の性質を満たすため，$f_0 = I_{\mathbf{N}}$ である．したがって $f_0(m) = m$ すなわち $0+m=m$ である．

$m+1=m'$ である．なぜなら

$$m+1 = m+1' = (m+0)' = m'$$

$m'+n = (m+n)'$ である．これは n に関する帰納法により証明できる．$n=0$ のときは $m'=m'$ で成り立つ．$n=k$ のときに $m'+k=(m+k)'$ が成り立つと仮定すると

$$\begin{aligned}
m'+k' &= (m'+k)' \\
&= ((m+k)')' \\
&= (m+k')'
\end{aligned}$$

したがって $m'+n=(m+n)'$ はすべての $n \in \mathbf{N}$ で成り立つ．

自然数 m，n，l に対して，結合律 $m+(n+l) = (m+n)+l$ が成り立つ．m に関する帰納法によって証明する．$m=0$ のときは $n+l=n+l$ で成り立つ．任意の自然

数を k として，$m = k$ のとき $k + (n + l) = (k + n) + l$ が成り立つと仮定すると

$$\begin{aligned} k' + (n + l) &= (k + (n + l))' \\ &= ((k + n) + l)' \\ &= (k + n)' + l \\ &= (k' + n) + l \end{aligned}$$

したがって $m + (n + l) = (m + n) + l$ はすべての $m \in \mathbf{N}$ で成り立つ．

交換律 $m + n = n + m$ が成り立つ．m に関する帰納法を用いる．$m = 0$ のときは $n = n$ で成り立つ．$m = k$ のとき $k + n = n + k$ が成り立つと仮定すると

$$\begin{aligned} k' + n &= (k + n)' \\ &= (n + k)' \\ &= n + k' \end{aligned}$$

したがって $m + n = n + m$ はすべての $m \in \mathbf{N}$ で成り立つ．

m，l が与えられたとき，$m + n = l$ を満たす n はただ 1 つだけ存在する．$m + n = l$ を満たす n が n_1, n_2 の 2 つ存在すると仮定しよう．加法の定義より

$$\begin{aligned} m + n_1' &= (m + n_1)' \\ m + n_2' &= (m + n_2)' \end{aligned}$$

である．$m + n_1 = m + n_2 = l$ であるので $m + n_1' = m + n_2' = l'$，したがって $m + n_1' = (m + n_2)'$．これが成り立つのは $n_1 = n_2$ のときだけである．ゆえに $m + n = l$ を満たす n はただ 1 つだけ存在する．

$m + l = n + l$ ならば $m = n$ である．$m + l = k$ とすると，これを満たす m はただ 1 つだけ存在する．したがって $m + l = n + l$ ならば $m = n$.

以上より，自然数 m，n，l に関して次の性質を得た．

- $m + 0 = 0 + m = 0$
- 交換律 $m + n = n + m$
- 結合律 $m + (n + l) = (m + n) + l$
- m，l が与えられたとき，$m + n = l$ を満たす n はただ 1 つ存在する
- $m + l = n + l$ ならば $m = n$

3.7 乗法

自然数の乗法 を次のように定義する (加法と同様 m，n を自然数とし，n' を n の次の数とする).

$$g_m(0) = 0$$
$$g_m(n') = f_m(g_m(n))$$

$g_m(n)$ を $m \cdot n = mn$ と表すと，次のようになる．

$$m \cdot 0 = 0$$
$$mn' = mn + m$$

証明は省くが，上の性質を満たす写像はただ一つしか存在しない．

この定義がわれわれの知っている乗法として機能することを確認しておこう．たとえば，$2 \cdot 3 = 6$ は次のように導く．

$$\begin{aligned} 2 \cdot 3 &= 2 \cdot ((0')')' \\ &= 2 \cdot (0')' + 2 \\ &= 2 \cdot 0' + 2 + 2 \\ &= 2 \cdot 0 + 2 + 2 + 2 \\ &= 6 \end{aligned}$$

定義がなんだか遠まわしな気もする．もっと直接的に定義できないものか．たとえば

$$mn = \overbrace{m + m + \cdots + m}^{n \text{ 個}}$$

とでもすれば，わかりやすいではないか．だが ”$\cdots$” の部分に論理の ”隙” ができる．だから，あえて再帰的な定義をする．

われわれが日常的に用いる自然数の乗法の性質を定義から導いていこう．

$0 \cdot m = 0$ である．値 0 の定値写像は g_0 の性質を満たすため，g_0 は値 0 の定値写像に等しい．したがって $g_0(m) = 0 \cdot m = 0$ である．

$m \cdot 1 = m$ である．なぜなら

$$m \cdot 1 = m \cdot 0' = m \cdot 0 + m = m$$

$m'n = mn + n$ である．n に関する帰納法を使って証明しよう．$n = 0$ のとき $0 = 0$ で成り立つ．$n = k$ のとき $m'k = mk + k$ が成り立つと仮定すると

$$\begin{aligned} m'k' &= m'k + m' \\ &= mk + k + m' \\ &= mk + (k + m)' \\ &= mk + k' + m \\ &= mk + m + k' \\ &= mk' + k' \end{aligned}$$

したがって $m'n = mn + n$ はすべての $n \in \mathbf{N}$ で成り立つ．

交換律 $mn = nm$ が成り立つ．n に関する帰納法を用いる．$n = 0$ のとき $0 = 0$ で成り立つ．$n = k$ のとき $mk = km$ が成り立つと仮定すると

$$\begin{aligned} mk' &= mk + m \\ &= km + m \\ &= k'm \end{aligned}$$

したがって $mn = nm$ はすべての $n \in \mathbf{N}$ で成り立つ．

自然数 m，n，l に対して，分配律 $m(n+l) = mn + ml$ が成り立つ．m に関する帰納法を用いる．$m = 0$ のとき $0 = 0$ で成り立つ．$m = k$ のとき $k(n+l) = kn + kl$ が成り立つと仮定すると

$$\begin{aligned} k'(n+l) &= k(n+l) + n + l \\ &= kn + kl + n + l \\ &= kn + n + kl + l \\ &= k'n + k'l \end{aligned}$$

したがって $m(n+l) = mn + ml$ はすべての $m \in \mathbf{N}$ で成り立つ．

結合律 $(mn)l = m(nl)$ が成り立つ．m に関する帰納法を用いる．$m = 0$ のとき $0 = 0$ で成り立つ．$m = k$ のとき $(kn)l = k(nl)$ が成り立つと仮定すると

$$\begin{aligned} (k'n)l &= (kn+n)l \\ &= l(kn+n) \\ &= l(kn) + ln \\ &= (kn)l + nl \\ &= k(nl) + nl \\ &= k'(nl) \end{aligned}$$

したがって $(mn)l = m(nl)$ はすべての $m \in \mathbf{N}$ で成り立つ．

$mn = 0$ ならば $m = 0$ あるいは $n = 0$ である．これの対偶である「$m \neq 0$ かつ $n \neq 0$ ならば $mn \neq 0$」を証明しよう．$m \neq 0, n \neq 0$ なので $m = m_0'$，$n = n_0'$ となる m_0，n_0 が存在する．

$$\begin{aligned} mn &= m_0'n_0' \\ &= m_0'n_0 + m_0' \\ &= m_0n_0 + n_0 + m_0' \\ &= m_0n_0 + n_0 + m_0 + 1 \end{aligned}$$

したがって $mn \geq 1$，すなわち $mn \neq 0$ である．

$m \neq 0$，l が与えられたとき，$mn = l$ を満たす n はただ 1 つだ存在する．$mn = l$ を満たす n が n_1，n_2 の 2 つ存在すると仮定しよう．$mn_1 = mn_2$ のとき $n_1 = n_2$ であることを証明する．n_1 に関する帰納法を用いる．$n_1 = 0$ のとき $m \cdot 0 = m \cdot n_2 = 0$，$m \neq 0$ なので $n_2 = 0$，したがって $n_1 = n_2$．$n_1 = k$ のとき $mn_1 = mn_2$ ならば $n_1 = n_2 = k$ であると仮定する．$n_1 = k'$ のとき，$mk' = mk + m = mn_2$．$n_2 = (n_{20})'$ とすると $mk + m = mn_{20} + m$．これより $mk = mn_{20}$，したがって $k = n_{20}$，すなわち $k' = (n_{20})' = n_2$，よって $n_1 = n_2 = k'$．以上より，$mn_1 = mn_2$ のとき $n_1 = n_2$ が成り立つ．ゆえに $mn = l$ を満たす n はただ 1 つだけ存在する．

$l \neq 0$ かつ $ml = nl$ ならば $m = n$ である．$ml = k$ とすると，これを満たす m はただ 1 つだけ存在する．したがって $ml = nl$ ならば $m = n$.

以上より，自然数 m，n，l に関して次の性質を得た．

- $m \cdot 0 = 0 \cdot m = 0$
- $m \cdot 1 = 1 \cdot m = m$
- 交換律 $mn = nm$
- 結合律 $m(nl) = (mn)l$
- $m \neq 0$, l が与えられたとき, $mn = l$ を満たす n はただ 1 つだけ存在する
- $l \neq 0$ かつ $ml = nl$ ならば $m = n$
- $mn = 0$ ならば $m = 0$ あるいは $n = 0$

3.8 べき法

自然数のべき法 m^n を次のように定義する (加法と同様 m, n を自然数とし, n' を n の次の数とする).

$$m^0 = 1$$
$$m \cdot m^n = m^{n'}$$

この定義がわれわれの知っているべき法として機能することを確認しておこう. たとえば, $2^3 = 8$ は次のように導く.

$$\begin{aligned} 2^3 &= 2^{2'} \\ &= 2^2 \cdot 2 \\ &= 2^{1'} \cdot 2 \\ &= 2^1 \cdot 2 \cdot 2 \\ &= 2^{0'} \cdot 2 \cdot 2 \\ &= 2^0 \cdot 2 \cdot 2 \cdot 2 \\ &= 1 \cdot 2 \cdot 2 \cdot 2 \\ &= 8 \end{aligned}$$

$1^n = 1$ である. n に関する帰納法により証明する. $n = 0$ のとき $1 = 1$ で成り立つ. $n = k$ のとき $1^k = 1$ が成り立つと仮定すると

$$\begin{aligned} 1^{k'} &= 1 \cdot 1^k \\ &= 1 \cdot 1 \\ &= 1 \end{aligned}$$

したがって $1^n = 1$ が成り立つ.

$m^n \cdot m = m^{n'}$ である. n に関する帰納法により証明する. $n = 0$ のとき $m = m$ で成り立つ. $n = k$ のとき $m^k \cdot m = m^{k'}$ が成り立つと仮定すると

$$\begin{aligned} m^{k'} \cdot m &= m \cdot m^k \cdot m \\ &= m \cdot m^{k'} \\ &= m^{(k')'} \end{aligned}$$

したがって $m^n \cdot m = m^{n'}$ が成り立つ．

自然数 m，n，l に対して，$m^n m^l = m^{n+l}$ が成り立つ．n に関する帰納法を用いる．$n = 0$ のとき $m^l = m^l$ で成り立つ．$n = k$ のとき $m^k m^l = m^{k+l}$ が成り立つと仮定すると

$$\begin{aligned} m^{k'} m^l &= m \cdot m^k \cdot m^l \\ &= m \cdot m^{k+l} \\ &= m^{(k+l)'} \\ &= m^{k'+l} \end{aligned}$$

したがって $m^n \cdot m^l = m^{n+l}$ である．

$(mn)^l = m^l n^l$ が成り立つ．l に関する帰納法を用いる．$l = 0$ のとき $1 = 1$ で成り立つ．$l = k$ のとき $(mn)^k = m^k n^k$ が成り立つと仮定すると

$$\begin{aligned} (mn)^{k'} &= (mn) \cdot (mn)^k \\ &= (mn) \cdot (m^k n^k) \\ &= m \cdot m^k \cdot n \cdot n^k \\ &= m^{k'} n^{k'} \end{aligned}$$

したがって $(mn)^l = m^l n^l$ である．

$(m^n)^l = m^{nl}$ が成り立つ．n に関する帰納法を用いる．$n = 0$ のとき $1 = 1$ で成り立つ．$n = k$ のとき $(m^k)^l = m^{kl}$ が成り立つと仮定すると

$$\begin{aligned} (m^{k'})^l &= (m \cdot m^k)^l \\ &= m^l \cdot (m^k)^l \\ &= m^l \cdot m^{kl} \\ &= m^{l+kl} \\ &= m^{k'l} \end{aligned}$$

したがって $(m^n)^l = m^{nl}$ である．

以上より，自然数 m，n，l に関して次の性質を得た．

- $m^0 = 1$
- $m^n m^l = m^{n+l}$
- $(mn)^l = m^l n^l$
- $(m^n)^l = m^{nl}$

3.9 大小関係

ペアノの公理からは自然数の大小関係は導かれない．ペアノの公理により自然数を定義した場合は，大小関係を加法によって定義する．

まず，自然数 n，k に関して，$k \neq 0$ ならば，任意の n に対して $n+k \neq n$，$n+k \neq 0$ であることを証明する (ここでも n' を n の次の数とする)．n に関する帰納法を用いる．$n=0$ のとき，$0+k=k \neq 0$．$n=l$ のとき $l+k \neq l$，$l+k \neq 0$ が成り立つとすると，$l'+k=(l+k)' \neq l'$，$l'+k=(l+k)' \neq 0$．したがって，$k \neq 0$ ならば，任意の n に対して $n+k \neq n$，$n+k \neq 0$ である．

任意の自然数 m，n に対して，次の 3 つの場合のどれか 1 つしかもただ 1 つだけが成り立つ．

1. ある $k \in \mathbf{N}$，$k \neq 0$ が存在して $m=n+k$
2. $m=n$
3. ある $l \in \mathbf{N}$，$l \neq 0$ が存在して $n=m+l$

$k \neq 0$ のとき，任意の n に対して $n+k \neq n$，$n+k \neq 0$ であるので，1，2，3 はどの 2 つも両立しない．どれか 1 つが成り立つことを示すため，m に関する帰納法を用いる．$m=0$ のとき 2，3 が成り立つ．任意の m について 1 が成り立つとすれば，$m'=(n+k)'=n+k'$，$k' \neq 0$ で m' について 1 が成り立つ．任意の m について 2 が成り立つとすれば $m'=n'=n+1$ で m' について 1 が成り立つ．任意の m について 3 が成り立つとすれば，$l \neq 0$ より $l=l_0'$ となる $l_0 \in \mathbf{N}$ が存在し，$n=m+l_0'=(m+l_0)'=m'+l_0$，ゆえに m' について 2，3 が成り立つ．したがって，$m \in \mathbf{N}$ 全体について 1，2，3 のいずれか 1 つが成り立つ．

自然数 m，n について，$m=n+l$ となる自然数 $l \neq 0$ が存在するとき，$m>n$ と書いて m は n より大きいという．あるいは $n<m$ と書いて n は m より小さいという．上の証明により，$m>n$，$m=n$，$m<n$ はどれか 1 つしかもただ 1 つだけが成り立つ．

自然数 m，n，l について，$m<n$ かつ $n<l$ ならば $m<l$ である．定義より $m<n$，$n<l$ ならば $n=m+k_1$，$l=n+k_2$ となる k_1，k_2 が存在する．n の式を l の式に代入すると $l=(m+k_1)+k_2=m+(k_1+k_2)$ より $l=m+k$ となる k が存在する．したがって $m<l$ である．

$m<n$ ならば $m' \leq n$ である．$m<n$ ならば $n=m+k$，$k \neq 0$ である．$k=k_0'$ とすれば $n=m+k_0'=(m+k_0)'=m'+k_0$ したがって $m \leq n$ である．

自然数の整列性「自然数の集合の任意の空でない部分集合は最小元を持つ」を証明しよう．ある空でない自然数の集合を A とし，A のすべての元 m に関して $n \leq m$ となるような自然数 n の全体を B とする．$B \neq \mathbf{N}$ なので，帰納法の原理の対偶より $x \in B$ かつ $x' \notin B$ を満たす x が存在する．$x \in B$ なので，すべての $m \in A$ に対して $x \leq m$ である．もし $x \notin A$ であれば，すべての $m \in A$ に対して $x<m$，したがって $x' \leq m$ である．これは $x' \notin B$ に反する．ゆえに $x \in A$ であり，x は A の最小元である．

加法・乗法が大小の順序を変えないことを「単調性」という．

$m<n$ ならば，任意の l に対して $m+l<n+l$ である．$m<n$ ならば $n=m+k$，$k \neq 0$，これより $n+l=(m+k)+l=(m+l)+k$，したがって $m+l<n+l$ である．

$m < n$ かつ $l \neq 0$ ならば $ml < nl$ である．$m < n$ ならば $n = m + k$，$k \neq 0$，これより $nl = (m+k)l = ml + kl$ で，$k \neq 0$，$l \neq 0$ より $kl \neq 0$，したがって $ml < nl$ である．

以上より，自然数 m，n，l に関して次の性質を得た．

- $m < n$ かつ $n < l$ ならば $n < l$
- $m < n$ ならば $m + l < n + l$
- $m < n$ かつ $l \neq 0$ ならば $ml < nl$

3.10 付録: 加法・乗法の一意性

加法・乗法の一意性を証明する．それには帰納的定義の原理というものを用いる．

帰納的定義の原理：集合 X の 1 つの元 x_0 と写像 $\varphi : X \to X$ が与えられたとき，次の性質 1，2 を満たす写像 $f : \mathbf{N} \to X$ がただ 1 つ存在する．

1. $f(0) = x_0$
2. すべての $n \in \mathbf{N}$ に対して $f(n') = \varphi(f(n))$

n' は n の次の数である．

f の一意性を帰納法により証明する．$f : \mathbf{N} \to X$，$g : \mathbf{N} \to X$ が共に上記の性質 1，2 を満たすとする．$n = 0$ のとき $f(0) = g(0) = x_0$．$n = k$ のとき $f = g$ が成り立つとすると，$f((k')') = \varphi(f(k')) = \varphi(\varphi(f(k))) = \varphi(\varphi(g(k))) = \varphi(g(k')) = g((k')')$．したがって $f = g$ はすべての $n \in \mathrm{N}$ で成り立つ．

問題は f が存在するかどうかである．ここで，$\mathbf{N} \times X$ の部分集合で，次の性質を満たす集合 A を考える．

- $(0, x_0) \in A$
- $(n, x) \in A \Rightarrow (n', \varphi(x)) \in A$

上記の性質を満たすすべての集合の共通部分を B とすると，B はこの集合の最小部分である．$\mathbf{N}$ の各元 n に対して，$(n, x) \in B$ となるような $x \in X$ 全体の集合を X_n とする．どの n に対しても X_n はただ 1 つの元からなることを帰納法により証明する．$n = 0$ のとき，$(0, x_0) \in B$ より $x_0 \in X_0$ である．もし X_0 が x_0 以外に元 y_0 を含むとすると，B から $(0, y_0)$ を取り除いた集合も上記の性質を満たすことになり，B の最小性に反する．ゆえに $X_0 = \{x_0\}$．$n = k$ のとき $X_k = \{x_k\}$ であるとする．$(k', \varphi(x_k)) \in B$ であるが，もし $X_{k'}$ が $\varphi(x_k)$ 以外の元 $y_{k'}$ を含むとすると，B から $(k', y_{k'})$ を取り除いた集合も上記の性質を満たすことになり，B の最小性に反する．ゆえに $X'_k = \{\varphi(x_k)\}$．したがって，任意の $n \in \mathbf{N}$ に対して X_n はただ 1 つの元からなる．そこで $X_n = \{x_n\}$ とし，$f(n) = x_n$ として $f : \mathbf{N} \to X$ を定義すると，f は帰納的定義の原理の性質 1，2 を満たす．以上で帰納的定義の原理の証明は完了した．

自然数 n の次の数 n' を与える写像を $\sigma(n)$ とする．m，n を自然数とするとき，加法の定義は次のようなものであった．

$$f_m(0) = m$$
$$f_m(n') = \sigma(f_m(n))$$

X，x_0，φ をそれぞれ $\mathbf{N}$，m，σ として帰納的定義の原理を適用すると，加法の一意性が証明される．

乗法の定義は次のようなものであった．

$$g_m(0) = 0$$
$$g_m(n') = f_m(g_m(n))$$

X，x_0，φ をそれぞれ $\mathbf{N}$，0，f_m として帰納的定義の原理を適用すると，乗法の一意性が証明される．

参考文献

[1] ドゥニ・ゲージ: 数の歴史，創元社 (1998).

[2] Bertrand Russell: Introduction to Mathematical Philosophy, Dover Publications (1993).

[3] 竹内外史: 集合とはなにか，講談社 (2001).

[4] 高木貞治: 復刻版 近世数学史談・数学雑談，共立出版 (1996).

[5] 松坂和夫: 集合・位相入門，岩波書店 (1968).

[6] 松坂和夫: 代数系入門，岩波書店 (1976).