「集合」の活用

小原　實晃（おはら　じっこう）

0. 集合論の現在

集合論は数学の方法を革命的に変えた．集合論を足場として「抽象数学」と呼ばれる新しい数学が発生したのである．また，集合論は数学の基礎固めにも力を発揮した．集合さえあれば「数」さえも作り出せることがわかったのである．これは，集合論によって数学を完全に基礎から再構築できることを意味する．

数学者は，集合論こそが数学の基礎をなすものだと考えはじめた．

ところが，その集合論（素朴集合論）に「矛盾」が発見され，数学は急転危機に直面した．

現在「計算機科学」をはじめ「数論」や「解析学」にその重要な応用が注目されている数学基礎論は，カントルにはじまる素朴集合論に現われたいくつかのパラドックスを解決しようとした多くの数学者や哲学者・論理学者たちの努力の中に，その発生の源を見出すことができる．

幸い，ドイツの数学者ツェルメロが，パラドックスをうまく回避する集合論の安全基準を発見し，その仕事を発展させたフレンケルの研究によって，事実上現代の公理的集合論（ZF 集合論）が完成した（1922）．

しかし，素朴集合論の方法は，現代の数学でもなおその論理的根拠を与える有力な武器となっているのも事実である．素朴集合論は原理的な意味において，現代の数学に対する最も強力な補助手段を提供しているのである．この補助手段なしにはいかに多くの天才たちの努力によっても，今日における現代数学の威容を期待することは不可能であったと思われる．

如何なる集合に市民権を与えるべきかの判定基準が明瞭になった現在，上記のような意味でも，素朴集合論に対して決してマイナスイメージをもってはならないし，むしろ高校数学の“教材”としては「平面幾何」と並んで，着目すべき（可能性を秘めた）教材である（教材ということで言えば，例えば「ベクトル」については，物理のベクトルは良いとしても，幾何ベクトルは本質的には‘同値類’なので多くの高校生にとって抽象的すぎて『できるけど，わからない』というのが実感であろう．しかし，これについても，Z の剰余系

$$Z_p=\{C_0,\ C_1,\ C_2,\ \cdots\cdots,\ C_{p-1}\}$$

を扱った経験（有限代数など）があれば，ある程度概念理解が容易になると思う）．

また，素朴集合論と関連して‘論理記号’も積極的に扱うべきである．理系・文系の別なく，全ての高校生が使えるようになった方が良いし，比較的容易に使えるようになるものである．

1. 自然数の集合（ペアノの公理）

われわれが数として取扱っているものには，大きく分けて 5 種類あり，集合として

$$N\subset Z\subset Q\subset R\subset C\quad\text{（拡張）}$$

なる包含関係がある．これらの「数」は，N からはじめて，公理論的に完全に“構成”することができる．

一方，人類は論理的構成とは全く無関係に，‘数’を（少なくとも Q ぐらいまでは）自明のものとして実際使用して来た．このような実践活動の中でアプリオリに用いて来た‘数’は，論理的に構成された（公理系の）対象（N, …, C）のモデル（実例）と言われる．

例えば，**Peano の公理系**（1889）の対象が（論理的に構成された）N であり，N のモデルが“本来の自然数 1，2，3，……”なのである．

人間が実践活動の中でアプリオリに用いている‘数’を（唯一の）モデルとする「数」の世界を公理論的に再構成する（N から拡張していく）とき，それが合理的になされるならば，結局のところ「数の公理系」は（N の）Peano の公理系に帰着するのである．

［注］ ヒルベルトの『幾何学』の公理系（1899）の無矛盾性は実数概念の無矛盾性に帰着せしめられ，そして実数概念の無矛盾性は

- Peano の公理系
- 集合に関連した若干の公理

を総合したものの無矛盾性に帰着する．

Peano の公理系　無定義記号（術語）としての

1，数（Zahl），後者（Nachfolger）

と，次の 5 個の公理よりなる．

数全体は集合 N をつくる．それに対して

(I)　1は数である．

(II)　各数 x に対して，その後者 x' も数である．

(III)　$x'=y'$ ならば $x=y$ である．

(IV)　$x'=1$ なる数 x は存在しない．

(V)　《完全帰納法の公理》数の，ある集合 M が

i)　$1\in M$

ii)　$x\in M \longrightarrow x'\in M$

なる性質をもつならば，$M=N$ である．

[注]　数学的帰納法という論法(推論法則)

$$\frac{P(1)\quad \forall n[P(n)\longrightarrow P(n+1)]}{\forall n[P(n)]}$$

のよりどころが上の(V)なのである．

この公理系を基礎として，順序・個数・算法の全ての性質が導出('証明')されるのである．実践活動の中でアプリオリに用いて来た自然数の世界が再現されてしまうのである．

そして，N を土台として，次々に「数」を創り出し

$$N\subset Z\subset Q\subset R\subset C$$

なる「数の世界」を論理的に構成することができる(アプリオリに用いて来た'数'の世界を完全に再現することができる)のだが，(その様子は[4][5]などで見ていただくことにして)ここでは上の(V)に着目したい．

(問1)　N, Z, Q, R, C の各々の"部分集合"について考える．そのとき，N の部分集合には，他の Z や Q などにはない性質がある．それはどのような性質か(ヒント：順序についての性質．C にも順序構造はある!)．

この問は，生徒に投げかけても，答えを期待しない方がよい．注意を喚起するためぐらいの気持ちでよい．

少し時間がかかるが，次の(V')はしっかり納得させることができる(物理や化学の法則でも，自分で発見せよ，と言われても，そう易々と気づくものではない．教えられてはじめて納得するということがほとんどだと思う)．

(V')　N の部分集合には必ず最小数がある．

N のどんな部分集合($\neq\phi$)にも必ず最小数がある——なるほど，Z, …, C では，'最小数'のない部分集合がいくらでも考えられる!

しかし，こんな性質を発見しても，これが何の役に立つのだ？

"役に立つ"ところは次の節2.と3.でお見せすることにして，この節の後半では

(V) $\Longleftrightarrow$ (V')　(同値)

であることを示すことにする．

ところで，数学的帰納法には，次の形のものもある(入試問題では，これを使わねばならないものが多々ある)．

(V'')　自然数のある集合 M が

i)　$1\in M$

ii)　$s\in M(s\leqq x) \longrightarrow x'\in M$

なる性質をもつならば，$M=N$ である．

ここで

$$V'' \longrightarrow V \qquad \cdots\cdots ①$$

が成り立つ．

また，

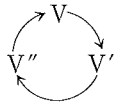
$$V \longrightarrow V' \qquad \cdots\cdots ②$$

であり

$$V' \longrightarrow V'' \qquad \cdots\cdots ③$$

であるから，結局

$$V \Longleftrightarrow V'$$



が言える．

①の証明

$s\in M(s\leqq x) \longrightarrow x\in M$　は自明．

ゆえに，V の ii)が成り立っているときは，V'' の ii)も成り立つ．

∴　V の i), ii) $\longrightarrow$ V'' の i), ii)

したがって　$V'' \longrightarrow V$　　が成り立つ．

②の証明

N の任意の部分集合を A($\neq\phi$)とする．

$M=\{x \mid x\in N,\ x$ は A の下界$\}$

とおく．$1\in M$ である．　　……㋐

また，$a\in A \longrightarrow a+1\notin M$ である．

∴　$M\subsetneqq N$　　……㋑

もし，命題

$x\in M \longrightarrow x'\in M$　　……㋒

が真であると，㋐と㋒から，V により

$M=N$

となって㋑に反する．したがって，㋒の否定

$\exists x[x\in M\wedge x'\notin M]$　　……㋓

が成り立たねばならない．そこで

$l\in M\wedge l'\notin M$　(l' は l の後者)

なる l をとると　$n\in A \longrightarrow l\leqq n$　であり，

l' はAの下界でないから，$^{\exists}m\in A[m<l']$ で

$$l\leqq m<l' \quad \therefore \quad m=l$$

が成り立つ．

ゆえに，l はAの最小数である．

すなわち $V \longrightarrow V'$ である．

③の証明

背理法による．

$M(\subset N)$ が V'' の仮定 i)，ii)を満たしているが $M\neq N$ であったとする．$M^C=A$ とおくと，$A\neq\phi$ だから，V' により，Aには最小数 l がある．仮定より $l\neq 1$ である．したがって

$$l=r'(^{\exists}r\in N)$$

と表せる．l はAの最小数であるから

$$s\leqq r \longrightarrow s\notin A \quad \therefore \quad s\in M$$

で，V'' の ii)により　$r'\in M$ となる．

$r'=l\in A=M^C$ であったのだから矛盾！

よって，$M=N$ であり

$$V' \longrightarrow V''$$

が示された．

[注]　上のいずれの証明も'難しい'と感じられるかも知れない．それは筆者の表現が拙劣だからだろう(あるいは，「'命題' ⟶ '命題'」の証明に慣れていないからかも知れない)．

たとえ「難しい」としても，それは'抽象的な概念'の「わからなさ」とは異質である．論理的な難しさは，時間はかかっても'ねばり'によって克服することができるし，「わかった！」という喜びを生み出すことにもなる．一方，大多数の高校生には理解不可能なほど高度に抽象的な概念も実際存在し，「できるけど，わからない」という"落胆"を与える結果になっている．'数学離れ'の原因の1つである．

(次の2.と3.の内容は，高2のクラスで毎年授業実践しているものである．)

2. 無理数であることの証明

$\sqrt{2}$，$\sqrt{3}$，$\sqrt{103}$，$\sqrt[3]{5}$，$\sqrt[10]{10}$ などが無理数であることの証明は，いろいろな方法が知られている．

(問2)　$\sqrt{103}$ が無理数であることを証明せよ．

(ヒント；$\sqrt{2}$，$\sqrt{3}$ のときの証明と同じパターンでできないか．)

[証明例]　$\sqrt{103}$ が有理数であると仮定すると

$$\sqrt{103}=\frac{b}{a}\ (\text{既約分数}) \qquad \cdots\cdots ①$$

と表される．①から

$$103a^2=b^2 \qquad \cdots\cdots ②$$

が成り立つ．b^2 は103の倍数だから，b そのものが103の倍数である．

したがって，$b=103c$ とおくと，②から

$$a^2=103c^2$$

が成り立つ．上の〰と同じ理由で，a も103の倍数となる．

これは，①の既約分数たることに矛盾する．

ゆえに，$\sqrt{103}$ は有理数ではない．

上の証明例のポイントは，②から〰を結論するところで，$\sqrt{3}$，$\sqrt{5}$ の場合で言えば

$3a^2=b^2$ …… b は3の倍数

$5a^2=b^2$ …… b は5の倍数

となり，一般に，$\sqrt{N}$ の場合は

$Na^2=b^2$ …… b はNの倍数

となる．つまり，

'b^2 がNの倍数だから，b はNの倍数' …… ③

という命題を使っているのである．

(問3)　命題③には反例がある．③はどのようなとき真な命題となるか．

上の証明例は，もっと厳密に直す必要があり，どうも途中が長くなりそうだ．

その他にも証明方法があり，例えば，命題

$\frac{b}{a}$ が既約分数 ⟶ $\frac{b^2}{a^2}$ も既約分数

を使う．しかし，これは，整数の基本性質

$(a,\ b)=1 \longrightarrow (a^2,\ b^2)=1$

を証明しておかねばならず，なかなかうるさい(これは，後で証明する)．

ここでは，予告しておいたように，(V')を役立てる方法(集合の活用)を考える．

(問4)　$\sqrt{6}$ が無理数であることを証明せよ．

[証明例]　$\sqrt{6}$ が有理数であると仮定すると

$$\sqrt{6}=\frac{b}{a}\ (a,\ b\in N) \qquad \cdots\cdots ④$$

と表される．集合

$$M=\{x\,|\,x\in N\wedge x\sqrt{6}\in N\}$$

を考えると，④から $M\neq\phi$ $(M\subset N)$ である．

(V')により，Mの最小数を p とする．…… ⑤

一方，平方して比べることにより，すぐ

$$2<\sqrt{6}<3$$

であることがわかり，$p>0$ より

$$2p<p\sqrt{6}<3p$$

$$\therefore\quad 0<p\sqrt{6}-2p<p \qquad \cdots\cdots ⑥$$

を得る．ところが

$$(p\sqrt{6}-2p)\sqrt{6}=6p-2(p\sqrt{6})\in \mathbf{N}$$

$$(p\sqrt{6}-2p)\in \mathbf{N}$$

であるから　$(p\sqrt{6}-2p)\in \mathbf{M}$ である．

これは，⑥により，⑤に反する．矛盾！

よって，$\sqrt{6}$ は④のように表せない．

(問5)　$\sqrt{103}$ が無理数であることを証明せよ．

[定理1]　$N\in \mathbf{N}$ のとき，$\sqrt{N}\in \mathbf{N}$ または $\sqrt{N}\notin \mathbf{Q}$ である．

(証明)　$\sqrt{N}\notin \mathbf{N}$ かつ $\sqrt{N}\in \mathbf{Q}$ と仮定すると

$$^{\exists}k\in \mathbf{N}\,[k<\sqrt{N}<k+1] \qquad \cdots\cdots ⑦$$

$$\sqrt{N}=\frac{b}{a}\quad (a,\ b\in \mathbf{N}) \qquad \cdots\cdots ⑧$$

である．集合

$$\mathbf{M}=\{x\,|\,x\in \mathbf{N}\wedge x\sqrt{N}\in \mathbf{N}\}$$

を考えると，⑧から $\mathbf{M}\neq\phi$，$\mathbf{M}\subset\mathbf{N}$ である．

M には最小数があり，それを p とする．

$$\cdots\cdots ⑨$$

一方，⑦より　$kp<p\sqrt{N}<(k+1)p$

$$\therefore\quad 0<p\sqrt{N}-kp<p \qquad \cdots\cdots ⑩$$

を得る．ところが

$$(p\sqrt{N}-kp)\sqrt{N}=Np-k(p\sqrt{N})\in \mathbf{N}$$

$$(p\sqrt{N}-kp)\in \mathbf{N}$$

であるから　$(p\sqrt{N}-kp)\in \mathbf{M}$ となる．

これは，⑩により，⑨に反する．矛盾！

よって，$\sqrt{N}\in \mathbf{N}$ または $\sqrt{N}\notin \mathbf{Q}$ である．■

[定理2]　$N\in \mathbf{N}$ のとき，$\sqrt[n]{N}\in \mathbf{N}$ または $\sqrt[n]{N}\notin \mathbf{Q}$ である．$(n\geqq 3)$

(証明)　$\sqrt[n]{N}\notin \mathbf{N}$ かつ $\sqrt[n]{N}\in \mathbf{Q}$ と仮定する．すなわち　$k<\sqrt[n]{N}<k+1$，$\sqrt[n]{N}=\frac{b}{a}$　$(a,\ b\in \mathbf{N})$

であるとする．集合

$$\mathbf{M}=\{x\,|\,x\in \mathbf{N}\wedge {}^{\forall}m\in \mathbf{N}[x(\sqrt[n]{N})^m\in \mathbf{N}]\}$$

$$=\bigcap_{m=1}^{\infty}\{x\,|\,x\in \mathbf{N}\wedge x(\sqrt[n]{N})^m\in \mathbf{N}\}$$

を考えると，$\underline{a^n\in \mathbf{M}}_{(*)}$ だから $\mathbf{M}\neq\phi$ である．

M の最小数を p とする．　$\cdots\cdots ⑪$

一方，$kp<p\sqrt[n]{N}<(k+1)p$ より

$$0<p\sqrt[n]{N}-kp<p \qquad \cdots\cdots ⑫$$

を得る．ところが

$$(p\sqrt[n]{N}-kp)\in \mathbf{N}$$

$$(p\sqrt[n]{N}-kp)(\sqrt[n]{N})^m=p(\sqrt[n]{N})^{m+1}-kp(\sqrt[n]{N})^m\in \mathbf{N}$$

であるから　$(p\sqrt[n]{N}-kp)\in \mathbf{M}$ となる．

これは，⑫により，⑪に反する．矛盾！

よって，$\sqrt[n]{N}\in \mathbf{N}$ または $\sqrt[n]{N}\notin \mathbf{Q}$ である．■

((*)の証明：$m=nq+r$，$0\leqq r<n$

とすると

$$a^n(\sqrt[n]{N})^m=a^n(\sqrt[n]{N})^{nq+r}=N^q(\sqrt[n]{N}\,a)^r a^{n-r}$$

$$=N^q b^r a^{n-r}\in \mathbf{N} \qquad)$$

3. 1次不定方程式

a_1，a_2，……，a_n，k を整数として

$$a_1x_1+a_2x_2+\cdots\cdots+a_nx_n=k$$

のような方程式を n 元の1次不定方程式という．

未知数 x_i を R で考えればあまり意味がないが，Z (とくにN)で考えれば'解'は無数・有限・無しと3つの場合があって，その現象のカラクリを解明してみるのも大変面白いことである．

(問1)　次の方程式にあてはまる x，y の整数値はどのようになるか．

(1)　$x+2y=3$　　(2)　$11x-7y=1$

(3)　$2x+4y=1$　　(4)　$13x-7y=3$

(5)　$17x-7y=23$

[解答例]　いろいろな方法があるが，'合同'を用いる方法を(5)に適用する．

$$17x-7y=23 \iff 17x-23=7y \quad (y\in \mathbf{Z})$$

$$\iff 17x\equiv 23 \pmod 7$$

$$\iff 3x\equiv 2 \pmod 7$$

$7=2\times 3+1$ だから $2\times 3x+x=7x\equiv 0$

$$\therefore\quad 2\times 2+x\equiv 0 \pmod 7$$

$$\therefore\quad x\equiv -4\equiv 3 \pmod 7$$

$$\therefore\quad x=7t+3 \quad (t\in \mathbf{Z})$$

$$\therefore\quad y=17t+4 \quad (t\in \mathbf{Z})$$

さて，上の(3)には解が無い．また，(4)で $13x$ を $14x$ に変えると解が無くなってしまう．

一見同じように見える方程式に解が在ったり無かったりするのは何故か，その判定基準はないか，など考えてみる——すごく興味をそそられることではないか．筆者などは高校生のとき「解の判別式」にすごく興味をもったものである．そして，そのことが「ガロア理論」を意欲を燃やして研究する原動力になっていたことは確かなのである．

紙数の関係で，結論だけ述べておこう．

(問2) 次の命題を証明せよ．

方程式 $ax+by+cz=k$ $(a, b, c, k \in \mathbf{Z})$ が整数解をもつ $\Longleftrightarrow$ $(a, b, c) \mid k$

(一般に n 元でも同じなので3元でやっておく．)

[証明例] 集合

$\mathrm{M}=\{ax+by+cz \mid x, y, z \in \mathbf{Z}\}$

を考える．M は次の性質をもつ．

$x, y \in \mathrm{M} \longrightarrow x+y \in \mathrm{M}$

$x \in \mathrm{M},\ n \in \mathbf{Z} \longrightarrow nx \in \mathrm{M}$

$\mathrm{M} \cap \mathbf{N} \neq \phi$ だから，$\mathrm{M} \cap \mathbf{N}$ には最小数があり，それを d とすると

$\forall m \in \mathrm{M} \longrightarrow d \mid m$ である．

$\because$ $\begin{pmatrix} m=qd+r \quad (0 \leqq r < d) \text{ とすると} \\ r=m-qd \in \mathrm{M} \\ d\,(>0) \text{の最小性から} \quad r=0 \text{ である．} \end{pmatrix}$

したがって

$\mathrm{M} \subset \{nd \mid n \in \mathbf{Z}\}\,(=[d] \text{と表す})$

である．

逆に，$nd \in \mathrm{M}$ であるから $[d] \subset \mathrm{M}$ である．

よって，$\mathrm{M}=[d]$ である．

そこで，a, b, c の任意の公約数を e とすると

$$e \mid ax+by+cz \quad (x, y, z \in \mathbf{Z})$$

であるから，$\forall a \in \mathrm{M}=[d]$ に対して

$$e \mid a$$

である．ゆえに，特に $e \mid d$ である．

また，$a, b, c \in \mathrm{M}=[d]$ だから

$$d \mid a,\ d \mid b,\ d \mid c$$

でもある．　$\therefore$ $(a, b, c)=d$

以上により，

$$\exists x, y, z \in \mathbf{Z}[ax+by+cz=k] \Longleftrightarrow k \in [d] \Longleftrightarrow d \mid k$$

が言える．

[注1] 上で用いた集合 M は Z(整数環)のイデアルの例である．2元の場合は，次のようになる．

> $a, b \in \mathbf{Z}$ とすると，$\exists d \in \mathbf{N}$
> $\{ax+by \mid x, y \in \mathbf{Z}\}=[d]$
> で，$(a, b)=d$ である．

このことから次が言える．

a, b が互いに素 $\Longleftrightarrow$ $\begin{cases} \exists x_0, y_0 \in \mathbf{Z} \\ ax_0+by_0=1 \end{cases}$

さらに，このことから，次の整数の基本性質が導かれる．

$(a, b)=1,\ (a, c)=1 \longrightarrow (a, bc)=1$ …… (☆)

$(a, b)=1 \longrightarrow (a^2, b^2)=1$

そして，ついに，「数論の基本定理」に到達する．

> 任意の正の整数は，順序を問わなければ，ただ一通りに素因数の積に分解できる．

(略証) 〈可能性〉 自然数からなる真の無限降下列が存在し得ないことから．

〈一意性〉 (☆)及び(☆)の対偶を用いる．

[注2] 上で用いた集合 M は，「差で閉じている」という性質をもっている．この性質だけに着目しても面白い結果が次々と導ける．

> Z の部分集合 $\mathrm{I}(\neq \phi, \{0\})$ が「差で閉じている」ならば
> (i) 積でも閉じている．
> (ii) $\exists d \in \mathrm{I}$ $[\mathrm{I}=[d]]$ である．

∞. 集合論のパラドックス

カントル，デデキントの集合論(素朴集合論)に発見された「パラドックス」とはどのようなことだったのか，そしてそれはどうして発生したのだろうか．

それを見るためには，素朴集合論の“論理構造”を明瞭にせねばならない．

素朴集合論の“公理”は，唯一つ

$$\exists y \forall x[x \in y \Longleftrightarrow C(x)] \qquad \cdots\cdots ①$$

だけである．

$\forall x[x \in y \Longleftrightarrow C(x)]$ は，「y は条件 $C(x)$ を満たす x の全体からなる集合である」という意味だから

$$y=\{x \mid C(x)\} \qquad \cdots\cdots ⊛$$

ということに他ならない．そこで，①は，⊛のような y が存在するヨという意味であり，われわれの研究の対象となり得る‘もの’の範囲に集合 y が存在するという宣言になっている．

①こそが，集合論にいくつかのパラドックスを生じさせる原因となっているのである．その代表が

ラッセルのパラドックス(1902)

である．

①の $C(x)$ として，$x \notin x$ を用いると

$$\exists y \forall x[x \in y \Longleftrightarrow x \notin x] \qquad \cdots\cdots (☆)$$

となる．これは

$$\forall x[x \in a \Longleftrightarrow x \notin x] \qquad \cdots\cdots ②$$

なる a がわれわれの研究の対象となり得るものの範囲に属していることを意味する．

したがって，②の x に a を代入して，特別な場合として

$$a \in a \Longleftrightarrow a \notin a \qquad \cdots\cdots ③$$

も成立せねばならない.

③からは,'$a\in a$' という命題の真偽の如何にかかわらず,常に1つの矛盾が導かれる.すなわち;

$a\in a$ が正しいと仮定すると③により $a\notin a$ も正しくなり矛盾.$a\in a$ が正しいという仮定は否定され,$a\notin a$ が正しいということになる.すると再び③により,$a\in a$ が正しいという結論が出てもはやどうにもならぬ矛盾に到達する.

さて,この論法は,カントル自身の有名な「対角線論法」と酷似している.

次にかかげるのは,濃度についてのくカントルの定理〉(1890)

'任意の集合 M に対して $|M|<|2^M|$ である'

の証明の後半の部分である.

(証明) ……

いま,M から 2^M の上への写像 f があったとすると,任意の条件 $C(x)$ に対し

$$^{\exists}y^{\forall}x[x\in f(y) \Longleftrightarrow C(x)] \quad \cdots\cdots ④$$

が成立する.$(x,\ y\in M)$

すなわち,

$$^{\exists}y\in M,\ f(y)=\{x\,|\,C(x),\ x\in M\}$$

が成り立つ.

④の $C(x)$ のところに '$x\notin f(x)$' という条件を入れると

$$^{\exists}y^{\forall}x[x\in f(y) \Longleftrightarrow x\notin f(x)]$$

が成り立つ.この y を a と名付けると

$$^{\forall}x[x\in f(a) \Longleftrightarrow x\notin f(x)]$$

が成り立つ.したがって,x に a を代入した

$$a\in f(a) \Longleftrightarrow a\notin f(a) \quad \cdots\cdots ⑤$$

も成立せねばならない.

⑤からは,$a\in f(a)$ なる命題の真偽の如何にかかわらず,常に1つの矛盾が導かれる.

以上により,M から 2^M の上への写像は存在し得ないことがわかった. ■

上記の「対角線論法」(よく読むと対角線の'図'が浮かんでくると思う!)は,巧妙な背理法にすぎないけれど,われわれを説得するに足る十分なる迫力をもっており,後にゲーデルの「不完全性定理」の証明でも決定的な役割を果たすことになるのである(カントル自身は,最初 $|N|<|R|$ の証明に用い,その後,いろいろなところで愛用している).

カントルの対角線論法は正当な数学的証明であると考える立場に立つならば,明らかに,前頁の,(☆)から矛盾を導く推論の正しさは認めざるを得ないことになる.

となると,結局,①(公理)の一般的妥当性を否認せざるを得ないことになる.

集合論を基礎におく「現代数学」と呼ばれる壮麗なる建造物にとって,①は絶対に必要な'公理'であるが,①のままではその建物を支え切れないことがわかったのである.補強工事を急がねばならなかったのである.

その結果でき上がった'土台'が,ツェルメロ・フレンケルの集合論であった.

そして,素朴集合論も,ほとんど今まで通り使っても大丈夫であることが保証されたのである.

「なんぴとたりとも,カントルが我々のために創設してくれたこの楽園から,我々を放逐することはできないだろう!」(ヒルベルト 1925)

〈参 考 文 献〉

[1] 「数学序論」(1970) 柴田敏男 (共立出版)
[2] 「数学とは何か」(1971) 前原昭二(総合科学)
[3] 「ゲーデルの謎を解く」(1993) 林晋(岩波書店)
[4] 「数学史への新しい視点」(1996) 小原實晃 (土佐塾高校研究紀要)
[5] 「数の体系」(1978) 彌永昌吉(岩波書店)

(高知県 土佐塾高等学校)