数学の基礎

Eureka GAP

2017 年 5 月 5 日

1　まえがき

あなたは数学の基礎づけに不安や疑問を持ったことはありますか．次の質問は実際に筆者が聞かれたことのある質問です：

- 数学における厳密な証明とは?
- 数学の公理系というのはどういったものなのか?
- 自然数の定義とは何か?

このような疑問は，数学の形式化という考え方を知ることで解消されると思われます．数学の形式化とは，公理や命題を単なる記号の羅列として，数学的証明を記号列の機械的操作に落としこむことですが，このような記号操作を数学の基礎づけとして採用することができます．また，その際には集合論のことばを用いると便利です．つまり，あらゆる数学的対象を集合によって定義してしまい，すべての数学的主張を集合に関する主張に書き換えてしまうのです．そこで，この記事では，集合論をベースとした数学の形式化について紹介したいと思います．

2　論理

数学では，公理とよばれる仮定たちから出発し，推論を重ねることで，様々な命題を得ています．数学を形式化するためには，まず数学で用いている推論，論理を形式化する必要があります．この章のテーマはずばり「証明とは何か」ということです．

2.1　論理式

まず我々が考えるべきなのは，命題とは何かという問題です．例えば，

(1) 1+1=2
(2) 地球は丸い
(3) この命題は偽である

という文章のうちどれが命題でしょうか? 数学的主張を命題というべきだとしたら，(2) は命題とは言えないでしょう．また，(3) が命題だとしましょう．すると，少し考えてみると分かるように，(3) は真であっても偽

であっても矛盾を引き起こします．ということは (3) も命題とはいえないでしょう．しかし，(1) と (3) の差はなんでしょうか? 自己言及の有無でしょうか?

このような議論からも，命題という文のクラスを明確に定義することの難しさを感じられると思います．しかし，このような問題は，命題の記述に自然言語を使っているからこそ生じる問題です．そこで，形式化においては，自然言語を使うのはやめます．あらかじめ用いる記号たちを指定しておいて，命題とは単に（閉）論理式と呼ばれる記号列のことだとしてしまうのです．ポイントは，論理式であるかないかということが，その意味によって決まるのではなく，その記号の並び方によってのみ決定されることです．実は，論理式を適切に定義したならば，先ほどの例のうち論理式によって表現できるのは (1) だけです．

今回は集合論のことばで数学を形式化するので，論理式に使ってよい記号は次のものだけです[*1]:

- 変数記号　$v_0, v_1, v_2, \ldots$
- 命題接続記号　$\neg$（否定），$\wedge$（かつ）, $\vee$（または）, $\to$（ならば）
- 量化記号　$\forall$（任意の），$\exists$（存在して）
- 等号　$=$
- 所属関係記号 $\in$

そして，以下のような規則で生成される記号列のみを論理式といいます：

(1) 任意の i, j に対して $v_i = v_j$ や $v_i \in v_j$ は論理式である．
(2) ϕ, ψ が論理式ならば，$\neg(\phi), (\phi) \wedge (\psi), (\phi) \vee (\psi), (\phi) \to (\psi)$ もまた論理式である．
(3) ϕ が論理式ならば，任意の i に対して $\forall v_i(\phi), \exists v_i(\phi)$ もまた論理式である．

実際は変数として x, y などを使ったり，カッコを書かなかったり，$\leftrightarrow$ や $\exists!$（一意に存在する）といったような表現を使ったりするわけですが，それらはすべて正式な論理式の略記だと考えます．

論理式に現れている変数には束縛変数と自由変数の 2 種類があります．例えば，$\exists y(x \in y)$ という論理式を考えましょう．y はその前に存在量化子がついているので，束縛変数です．一方，x には量化子がついていないので，自由変数とよばれます．自由変数の無い論理式のことを閉論理式，もしくは文といい，これがまさに我々が命題と呼びたいものであったわけです．

2.2　証明

では次に，証明を形式化しましょう．特にこの節は正確な定義を与えることが大変なので，ざっくりとした説明で済ませます．証明とは何かを定義するには，論理の公理と推論規則を与えなければなりません．

論理の公理には，例えば $\phi \wedge \psi \to \phi$，$\neg\neg\phi \to \phi$，$\phi(y) \to \exists\phi(x)$ などといった（トートロジー的な）論理式たちが入っています．ここで具体的に論理の公理のリストを書き連ねることは大変なので省きますが，どのようなトートロジーも証明するのに十分な程の論理式たちが入っていると思ってください．

推論規則とは論理式（たち）から新たな論理式を導く規則たちのことです．論理の公理に十分な数の公理を入れておけば，推論規則としては次の 2 つだけを考えれば十分です：

- 三段論法：ϕ と $\phi \to \psi$ から ψ を導く．
- 一般化法則：$\phi \to \theta(x)$ から $\phi \to \forall x\theta(x)$．ただし x は ϕ における自由変数ではない．

[*1] 補助記号としてカッコも使います．

論理の公理と推論規則が与えられたならば，証明とは何かを定義できます．文の集合 T から文 ϕ が証明可能であるとは，論理式の有限列 $\phi_1, \phi_2, \ldots, \phi_n$ が存在して，ϕ_n が ϕ と一致し，かつ各 $1 \leq k \leq n$ に対して次のいずれかが満たされることです：

(1) ϕ_k は T に含まれる．
(2) ϕ_k は論理の公理である．
(3) ある $1 \leq i, j < k$ が存在して，ϕ_i, ϕ_j から ϕ_k は推論規則によって導かれている．

以上で，証明を形式化することができました．

2 章を通じて議論してきたことは，論理の形式化です．論理にもいろいろな種類がありますし，その形式化の方法にも種類がありますから，この章の記述は論理の形式化の一例にすぎません．論理の形式体系を与えるには，記号，文法（いかなる記号列を論理式とするか），論理の公理，推論規則の 4 つの要素を指定してやる必要があります．今回扱ったのは，ごくごく普通の論理，いわゆる一階述語古典論理とよばれるものですが，これがまともな形式化になっているのかというのはまた別の議論が必要です．例えば，空集合から証明できる文全体と我々の思うトートロジー的命題全体はきちんと一致しているのかということは確かめる必要があります．それを保証するのがゲーデルの完全性定理ですが，そのためにはさらに言葉の準備が必要で，残念ながらそれを説明する紙面の余裕も筆者の体力もありません．（トートロジーであるという性質をきちんと定義しなければいけない！）ですから，我々はそろそろ論理から離れて「数学の公理とは何か」という問いに移ろうと思います．

3 集合論

前章では，文の集合 T から証明可能であるということが定義できました．数学を形式化するためには，この T としてどのような公理系を立てるべきなのかを考えなければいけません．T には，すべての数学が展開できるほどの公理が入っていなければいけませんが，人間でもリストアップできるくらいのものでないと扱うのに困ってしまいます．このような公理系を見つけるのは容易でないように思えますが，幸いにも集合論においては ZF(C) という公理系があることが知られています．そこで，この章では ZF(C) を出発点として，自然数まで定義することを目標とします．その過程を追えば，その他の数学も集合論の範疇でうまく展開できそうだと感じられることと思います．

3.1 ZF 公理系

集合論で用いられている標準的な公理系は ZFC 公理系とよばれるものです．名前の由来は，Zermelo と Frankel という 2 人の数学者と，選択公理を意味する Choice の頭文字です．ZFC から選択公理を除いた公理系を ZF とよび，こちらもまたよく使われます．選択公理について説明するのは後回しにして，ZF に含まれる公理たちを列挙していくことにします．

- **外延性公理**:
$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$
外延性公理の言いたいことは，集合はそれに含まれる元によってのみ決定されるということです．x と y が同一の集合か調べたかったら，それらに含まれている元を比較すればよいというわけです．

- **空集合**：

$$\exists z \forall x (x \notin z)$$

これは空集合の存在公理です．むしろ，空集合 $\emptyset$ とは上の公理で存在が保障される z のことだと定義します．外延性公理を仮定すれば空集合は存在すれば一意です．実際，x も y も空集合だとすると，両方とも元を持たないので，$\forall z(z \in x \leftrightarrow z \in y)$ は自明に真です．ここで外延性公理を使うと $x = y$ を得ます．

- **対**：

$$\forall x \forall y \exists z (v \in z \leftrightarrow (v = x \vee v = y))$$

ここで存在が保障されている z は $\{x, y\}$ と書かれて対集合と呼ばれます．一意性は先と同様，外延性公理を使えば言えます．また，$\{x, x\}$ は単に $\{x\}$ と書くことにします．

- **和集合**：

$$\forall x \exists z \forall v (v \in z \leftrightarrow \exists y \in x (v \in y))$$

ここで存在が保障されている z は，和集合 $\bigcup x$ のことです．つまり，$\bigcup x$ は x の元の元からなる集合のことで，x としては集合族を思い浮かべると分かりやすいかもしれません．また，$\bigcup\{x, y\}$ のことを $x \cup y$ と書くことにします．和集合の一意性はやはり外延性公理から従います．

- **冪集合**：

$$\forall x \exists z (v \in z \leftrightarrow v \subseteq x)$$

ここでの冪集合 $\mathcal{P}(x)$ の存在を保証する公理です．$v \subseteq x$ という記号は $\forall w \in v (w \in x)$ の略記と考えてください．

- **無限**：

$$\exists z (\emptyset \in z \wedge \forall v \in z (v \cup \{v\} \in z))$$

今までの集合の存在公理からは無限集合の存在が導かれないので，無限集合の存在公理が何か必要です．しかし，自然数全体の集合が定義されていない状態で，無限集合であることを表現するには一工夫必要です．この公理は $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots\}$ を部分集合として含むような集合の存在を保証することで，無限集合の存在を暗に示しています．この公理については自然数の定義のところでもう一度説明します．

- **内包性**：$\phi(v)$ を v 以外を自由変数として含まない論理式[*2]として，

$$\forall x \exists z \forall v (v \in z \leftrightarrow v \in x \wedge \phi(v)).$$

先ほどまでの公理たちは，ある集合からより大きな集合の存在を保証するものでした．内包性公理は，ある集合 x の論理式で規定された部分集合 $z = \{v \in x \mid \phi(v)\}$ の存在を保証します．内包性公理によって構成される集合は，あくまでも部分集合でなくてはいけません．この仮定を外して，つねに $\{v \mid \phi(v)\}$ という形の集合が存在するとしましょう．そして，$R = \{x \mid x \notin x\}$ という「集合」を考えると，$R \in R$ としても $R \notin R$ としても矛盾が導かれてしまいます．これはいわゆるラッセルのパラドックスです．よって，R のようなものを集合と認めてはいけないのです．また，R は集合でないという事実から，すべての集合の集まり $V = \{x \mid x = x\}$ も集合でないことが分かります．なぜなら，V が集合とすれば，$R = \{v \in V \mid v \notin v\}$ は我々の内包性公理によって，集合になってしまうからです．実

[*2] ϕ の自由変数として x を入れることも許してしまうと，矛盾が生じてしまいます．例えば，ϕ として $v \notin z$ を考えてみましょう．

は，後に述べる基礎の公理から，すべての集合 x は $x \notin x$ を満たすので，$R = V$ です．このように一見集合であっても，集合でない集まりになってしまっていることがあります．そのような集まりをクラスとよびます．[*3]範囲を指定せずに○○全体とくくってしまうことが，集合論的にいかに危ういかを覚えておくとよいでしょう．

- **置換**：ϕ を u, v 以外を自由変数として含まない論理式として，

$$\forall x(\forall u \in x \exists\, !v\phi(u, v) \to \exists z \forall v(v \in z \leftrightarrow \exists u \in x \phi(u, v)).$$

$\phi(u, v)$ という論理式が，集合 x の元 u を v へうつすような写像を定めているときに，x の像もまた集合であるということを言っています．置換公理は，内包性公理を導きます．実際，ϕ を $v = \{w \in x \mid \psi(w)\}$ という論理式として置換公理を用いると，$\{w \in x \mid \psi(w)\}$ という集合の存在が示されます．それでも普通は内包性公理と置換公理は区別してリストに入れておきます．

- **基礎**：

$$\forall x(\exists v(v \in x) \to \exists y \in x \forall z \in x(z \notin y))$$

基礎の公理は x が空集合でない限り $\in$-極小元 y が必ず存在することを意味しています．集合論においては欠かすことのできない非常に重要な公理なのですが，普通の数学ではあまり登場する機会はありません．そこで，この公理についての説明は参考文献に譲ることにします．

以上で，ZF 公理系のリストが列挙できました．ZF を使うのに慣れるため，色々な基本的概念を定義してみることにしましょう．

共通部分：$x \neq \emptyset$ のとき，

$$\bigcap x = \{v \mid \forall y \in x(v \in y)\}$$

と定義します．任意の $a \in x$ をとってくれば，$\bigcap x$ は a の部分集合となるので，内包性公理によってこの集合の存在は保証されています．

順序対：x, y を集合としたとき，その順序対 $\langle x, y\rangle$ を

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}$$

と定義する．このとき，$\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$ であることは $x_1 = x_2, y_1 = y_2$ と同値です（読者の演習）．

直積：集合 A, B に対して，

$$A \times B = \{v \mid \exists x \in A \exists y \in B v = \langle x, y\rangle\}$$

と定義します．$A \times B$ は $\mathcal{P}(A \cup B)$ の部分集合になっているので，内包性公理は適切に使えます．内包性公理の代わりに置換公理を使えば，冪集合公理なしで直積を構成することもできます．その構成方法は参考文献を参照してください．

関係：関係とは，すべての元が順序対であるような集合とします．R を関係としたとき，

$$\mathrm{dom}(R) = \{x \mid \exists y \langle x, y\rangle \in R\}$$
$$\mathrm{ran}(R) = \{y \mid \exists x \langle x, y\rangle \in R\}$$

と定めます．$\mathrm{dom}(R)$ も $\mathrm{ran}(R)$ も，$\bigcup\bigcup R$ の部分集合になっているので，これらもまた適切に内包性公理によって定義されています．

[*3] 集合もクラスだということもありますが，ここでは区別しましょう．

関数：f が関数もしくは写像であるとは，それが関係であり，

$$\forall x \in \mathrm{dom}(f) \exists! y \in \mathrm{ran}(f) \langle x, y \rangle \in f$$

となることです．

これくらいの定義さえしておけば，「集合と位相」の授業で習うような他の概念も次々に定義することが可能であることは納得できることでしょう．

3.2 自然数

では，とうとう自然数を定義します．まず，$0 = \emptyset$ と定義します．$1 = \{0\} = \{\emptyset\}, 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \ldots$ と定義していき，一般に自然数 n を $\{0, \ldots, n-1\}$ で定義します．S という操作を $x \mapsto x \cup \{x\}$ で定めると，自然数 n とは $\emptyset$ に操作 S を n 回適用したものであると言い換えることができるので，これらの集合は空集合，対，和集合の公理から存在が言えます．そして，自然数全体の集合 $\mathbb{N}$ は，0 が含まれていて，この操作 S によって閉じた最小の集合と定めましょう．すなわち，

$$\begin{aligned} \mathbb{N} &= \bigcap \{z \mid \forall v \in z (v \cup \{v\} \in z)\} \\ &= \{x \mid \forall z (\forall v \in z (v \cup \{v\} \in z) \to x \in z)\} \end{aligned}$$

と定義します．このような $\mathbb{N}$ は本当に存在するのでしょうか．このことを保証するのが，無限公理です．無限公理の主張を再掲しましょう：

$$\exists z (\emptyset \in z \wedge \forall v \in z (v \cup \{v\} \in z)).$$

ここで存在すると言われている z は 0 を含み，操作 S によって閉じています．このような集合を任意にとって，M とおくと，$\mathbb{N}$ は M の部分集合になっていますから，内包性公理によって，$\mathbb{N}$ の存在が言えました．

こうして $\mathbb{N}$ が定義されたのですが，まだこれらが自然数らしく見えないかもしれませんから，自然数に入る構造をいくつか定義してみることにします．途中でそれほど自明でない事実も用いますが，それらの証明は省きます．

まず，順序構造 $<$ を $n < m \iff n \in m$ で定義します．これは $\mathbb{N}$ 上の整列順序になっており，普通の自然数の順序と一致していることも分かります．

次に，演算 $+$ を定義しましょう．n, m を自然数とします．$A = (n \times \{0\}) \cup (m \times \{1\})$ という集合を考えます．この集合上の順序 $<^*$ を次のように定義します：

(1) 任意の $s < n, t < m$ に対して，$\langle s, 0 \rangle <^* \langle t, 0 \rangle \iff s < t$.
(2) 任意の $s < n, t < m$ に対して，$\langle s, 0 \rangle <^* \langle t, 1 \rangle$.
(3) 任意の $s < m, t < n$ に対して，$\langle s, 1 \rangle <^* \langle t, 1 \rangle \iff s < t$.

このとき，$<^*$ は A 上の整列順序です．さらに，ある自然数 x が存在し，順序集合 $(A, <^*)$ と $(x, <)$ が同型になることが示せるので，$n + m$ はこの x として定めます．定義を理解するためにも，実際に $2 + 3$ を計算してみましょう．$A = (2 \times \{0\}) \cup (3 \times \{1\})$ の元たちに順序 $<^*$ を入れると

$$\langle 0, 0 \rangle <^* \langle 1, 0 \rangle <^* \langle 0, 1 \rangle <^* \langle 1, 1 \rangle <^* \langle 2, 1 \rangle$$

となります．これは

$$0 < 1 < 2 < 3 < 4$$

と同型な順序です．よって，$2+3$ の答えは $5=\{0,1,2,3,4\}$ です．この $+$ は結合法則や交換法則を満たし，$S(n)=n+1$ なども示せます．

演算 $\cdot$ も $+$ のときと似た議論で定義します．n,m は自然数として，$B=m\times n$ という集合を考えます．この集合上の辞書式順序 $<_{\mathrm{lex}}$ を次のように定義します：任意の $s_1,s_2<m$ と $t_1,t_2<n$ に対して，

$$\langle s_1,t_1\rangle <_{\mathrm{lex}} \langle s_2,t_2\rangle \iff (s_1<s_2 \vee (s_1=s_2 \wedge t_1<t_2)).$$

このとき，$<_{\mathrm{leq}}$ は B 上の整列順序です．さらに，ある自然数 x が存在し，順序集合 $(B,<_{\mathrm{lex}})$ と $(x,<)$ が同型になることが示せるので，$n\cdot m$ はこの x として定めます．$2\cdot 3$ を計算してみましょう．$B=3\times 2$ の元たちに辞書式順序を入れると

$$\langle 0,0\rangle <_{\mathrm{lex}} \langle 0,1\rangle <_{\mathrm{lex}} \langle 0,2\rangle <_{\mathrm{lex}} \langle 1,0\rangle <_{\mathrm{lex}} \langle 1,1\rangle <_{\mathrm{lex}} \langle 1,2\rangle$$

となりますから，この順序集合は

$$0<1<2<3<4<5$$

と同型です．よって，$2\cdot 3=6$ です．この $\cdot$ も結合法則を満たし，可換で，分配法則を満たしています．

これまた詳細は省きますが，このようにして定められた $(\mathbb{N},S,+,\cdot)$ の組は，自然数の満たすべき公理系であるペアノの公理を満たすことも証明することができます．このような理由から，集合 $\mathbb{N}$ は確かに自然数全体の集合だと思えるのです．$\mathbb{N}$ が定義できてしまえば，$\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ などは全く普通の方法で定義されます．その他の数学的概念も，数学書に載っている定義を追っていくことで，集合として定義できると納得できることでしょう．

また，そういった集合による定義ができたならば，数学的主張もすべて集合論における論理式で書き下すことができるでしょう．2 章の最初に $1+1=2$ は命題だと述べました．我々は自然数とその演算について定義したので，定義をさかのぼっていくことで $1+1=2$ を表現するような論理式を書くことができます．ただ，実際に書くとなると非常に大変です．なにしろ，$n=2$ という論理式を正しく書き下すだけでも，

$$\begin{aligned} n=2 &\iff \forall x(x\in n \leftrightarrow (x=0\vee x=1))\\ &\iff \forall x(x\in n \leftrightarrow (\forall y(\neg y\in x))\vee(\forall y(y\in x\leftrightarrow (y=0))))\\ &\iff \forall x(x\in n \leftrightarrow (\forall y(\neg y\in x))\vee(\forall y(y\in x\leftrightarrow (\forall z(\neg z\in y))))) \end{aligned}$$

という長さになってしまいます．厳密にいえば，$\leftrightarrow$ も省略記号なので，本当の論理式にするには倍の長さが必要です．それでも，命題はみな論理式に書けるということは納得できるはずです．集合論の上で数学を展開できるとはこういう意味です．

3.3 選択公理

先延ばしにしてきた ZFC の C，すなわち選択公理（Axiom of Choice, AC）について一応触れておきましょう．選択公理とは，次のような論理式です：

$$\forall x\exists f(f \text{ は関数} \wedge \forall v\in x(f(v)\in v)).$$

ここに登場する f は x の選択関数とよびます．意味が分かりにくければ，$x=\{X_i \mid i\in I\}$（各 X_i は空でない）という集合族を考えるとよいかもしれません．すると，f は実際には x 上の関数ですが，I 上の関数ともみなせて，各 $i\in I$ に対して X_i の元を返すようなものになります．選択公理の妥当性は 20 世紀初めに議論を

巻き起こし，実はその議論の過程で ZF 公理系も生まれました．しかし，現在では選択公理はほぼ全ての数学者に受け入れられているといってよいでしょう．よって，何か特別な断りが無い限り，普通の数学は ZFC に基づいて展開されていて，ZFC から証明される命題を定理と言っているのです．

3.4 無矛盾性

ここまで ZFC 公理系がいかにうまく機能しているかを紹介してきたわけですが，そもそも，ZFC 公理系は無矛盾なのでしょうか? また，そのことは ZFC から証明できることなのでしょうか?

まず，「公理系 T は無矛盾である」という主張は論理式として書けることを注意しましょう．なぜなら，各記号を自然数によってコーディングして，論理式なども単なる自然数とみなすことで，ϕ は ZF(C) から証明可能であるということを自然数に関する命題として書くことができるからです．しかし，ZF や ZFC は矛盾した公理系でない限り自分自身の無矛盾性を証明できないということがゲーデルによって示されています．これがいわゆるゲーデルの（第二）不完全性定理です．これは ZF や ZFC が悪いのではありません．自然数を「きちんと」扱えるような「まともな」公理系ならば，つねに自身の無矛盾性は証明できないのです．ですから，ZF(C) 公理系が無矛盾かという問いには，「今のところ矛盾は発見されていないし，無矛盾であってもそれを確かめる方法はない」というしかありません．ただ，ひろく ZF(C) の無矛盾性は信じられていますし，ZF(C) の矛盾を見つけることに人生を費やすのもお勧めできないのですが．

そこで，集合論では ZF や ZFC の無矛盾性は仮定したうえで，他の公理系が無矛盾かどうかを調べます．例えば，ゲーデルは ZF が無矛盾ならば ZFC もまた無矛盾であることを示していますし，実は ZF が無矛盾ならば ZF+¬AC もまた無矛盾であることがコーエンによって示されています．この結果の意味するところをもう少し考えてみましょう．ZF から ¬AC が証明されたとすれば，ZF+AC は矛盾します．ゲーデルの結果を用いると，ZF もまた矛盾します．よって，ZF が矛盾しない限り，ZF からは選択公理の否定を証明できないということが言えます．同様の議論で，コーエンの結果からは，ZF が矛盾しない限り，ZF からは選択公理を証明できないということが言えます．これは要するに，選択公理は他の数学の仮定からは証明も反証もできないということです．

こういった「無矛盾であること」「証明できないこと」が証明できるということは，まさに形式化の恩恵です．証明が何か，公理が何かということが明確になっていなければ，そもそも問題を提起することすらできないのですから! 形式化は数学の基礎を築いただけでなく，新たな数学をも産み出したのです．

参考文献

[1] ケネス・キューネン（2008） 『集合論 独立性証明への案内』 藤田博司訳，日本評論社．
[2] 新井敏康（2012） 『数学基礎論』 岩波書店．
[3] 田中一之編（1997） 『数学基礎論講義—不完全性定理とその発展』 日本評論社．