まえがき

本日は「数学科展示　ますらぼ」にご来場いただき誠にありがとうございます．本企画は今年度を持ちまして 5 年目となります．私達の上の上のそのまた上の学年から始まり，今回先代から私達数学科 2016 年度進学 (現在数学科 4 年生) が引き継ぎました．受け継いだ「ますらぼ」「$e^{\pi i}sode$（えぴそーど)」の名前の重さに押しつぶされそうになりながらも，先輩方の多大なるご助力のもと，何とか一つの形にすることができました．数学科や「ますらぼ」の名前に泥を塗るようなことになっていないことを祈るばかりです．

数学科の学生は普段はここ本郷キャンパスではなく，駒場キャンパスという少し離れた別の場所で活動しています．他学部と比べて実験や実習のようなものがほとんどないため，みんな 1 日の多くの時間を数学に没入しながら，日々数学がわかったり，数学がわからなかったりに一喜一憂しています．

ところが，一人一人がどのような数学をやっているかとなると，これは人によってバラバラです．

「数学」というものはよくひっくるめて一緒くたに扱われますし，「数学は本質的には一つなのだ」という考えはごく自然なもののように思えます．しかし実際にはそんなことは無く，数学の世界にも「畑違い」「よその庭」「人には人の乳酸菌」があります．どんな大数学者も，その時代の数学を全て理解したことはいまだかつてありません．思うに，数学は統一的に意識されながらも，決して統一されることは無さそうです．そしてこれはむしろ嬉しいことのように思えます．というのも，これは数学の多種多様な楽しみ方，それも自分だけの楽しみ方を，そっくりそのまま保証してくれるからです．ただ残念なことに，全ての数学に出会うことは人の短い一生ではどうやら不可能そうです．

今回の $e^{\pi i}sode$ には，人生では出会うことがむしろ稀な数学がたくさん詰まっています．これはとても私一人のなせるわざではなく，執筆者になってくれた同期達の深くそれでいて個性的な知識の賜です．本企画・冊子が，数学との新しい出会いのきっかけになっていただけたのならば，これ以上に嬉しいことはありません．是非 1 冊お手に取ってみてください．(高木)

目　次

数学の基礎（合浦岳彦）

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．

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．

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)] 補助記号としてカッコも使います．

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．

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．

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．

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．

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**：
$$\forall x \exists z (v \in z \leftrightarrow v \subset x)$$
ここでの冪集合 $\mathcal{P}(x)$ の存在を保証する公理です．$v \subset x$ 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．

---

[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．

[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．

- **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．

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．

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．

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．

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.

和算–日本の数学 (大桑)

和算の歴史

古代から日本には数的な考え方がありました． 大和政権時代に中国・朝鮮との交易で九九を取り入れ，室町時代の勘合貿易では中国からそろばんが伝わり，商人や武士の間では生活数学が使われていたようです． 生活数学は江戸時代，貨幣社会になって計算のできる人の需要が高まったことにより，飛躍を遂げます． まず京都を中心としてそろばん塾が現れました． そこで教科書のような役割をしたのが『算用記』(1600~1620?) です． 内容は割り算，容積，土木関係，利息などの身近な数処理に関するものでした．

多くある塾の弟子たちは次第に独学で数学を学び始めます． その一人の吉田光由もそうでした． 彼は中国の数学書で独学し生活数学の本として『塵劫記(じんこうき)』(1627) を刊行します． その続編である『新篇塵劫記』(1641) において，巻末に答えのない問題 (遺題) を 12 問つけました． これがきっかけとなり，数学を研究する人たちが商人に限らず増え，和算は発達を遂げるのです． このように，答えのない問題を出す伝統を遺題継承と呼んでいます．

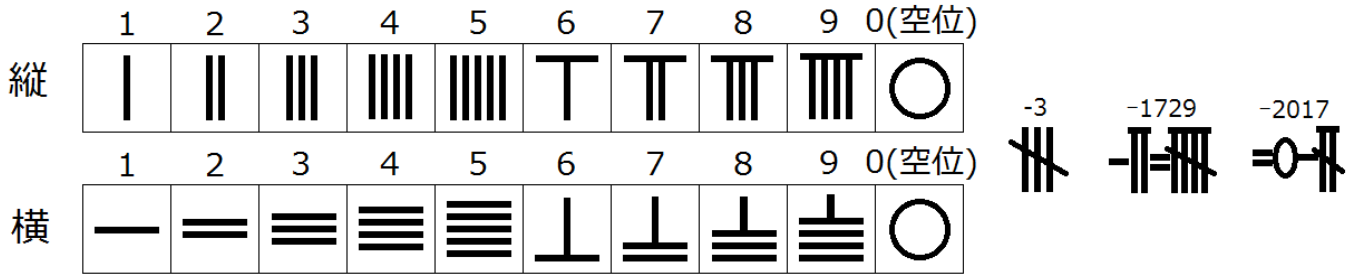
遺題継承という伝統のほかにも，和算にはもう 1 つの大きな伝統があり，それが算額奉納です．絵馬に数学の問題・解法・解答を記したものを神社仏閣に奉納するというもので，江戸初期から始まっていたようです． その目的は神への感謝と，数学の実力が付くようにという祈願だとされていますが，塾の経営者や本の著者が宣伝を兼ねて算額を掲げることもあったようです． 算額は現存するだけでも全国に 900 枚以上存在し，そこからかなり流行したことがうかがえます． どうやら江戸時代に数学は，研究者や商人だけではなく，アマチュアの愛好家にも愛されていたようです．

発達していく和算を学ぶ者の一人に関孝和 (1642?~1708) がいました． 彼は中国書を学び驚くべき業績を残しました． 例えば，円周率の小数 11 位までの計算，不定方程式，行列式の概念，ベルヌーイ数の発見などです． それらを可能にしたのは彼の発明した， 点竄術(てんざんじゅつ)と呼ばれる高次方程式を解くための書法です． 彼の発明まで，数学の計算はそろばんと算木と呼ばれる棒を使って行われていたのですが，点竄術によればそれを紙上でることができてしまいます．

和算の記法

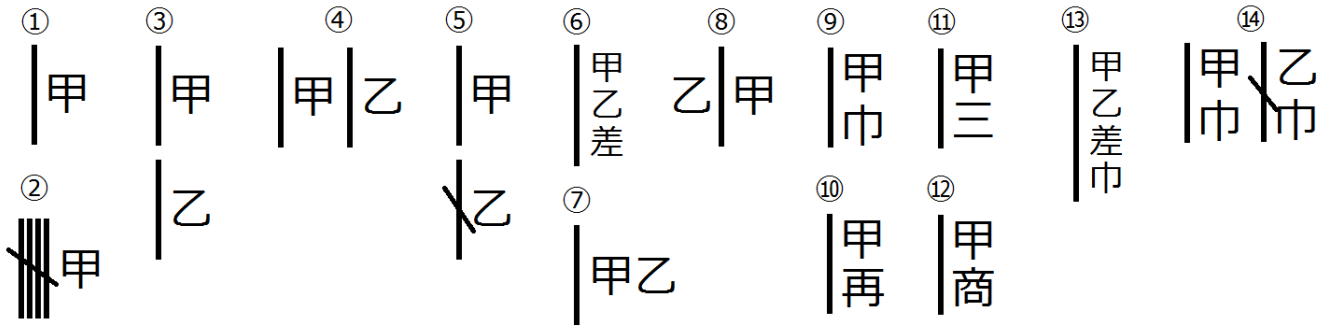
さて，その点竄術とはどのようなものでしょうか． それまでの計算はそろばんや算木と呼ばれる細い棒を使ってやっていたのですが，それでは複雑な式変形や多元高次方程式を解くのに難がありました．それを改善したのが点竄術です． 以下にその例を見ていきましょう．

数は次のように表します．

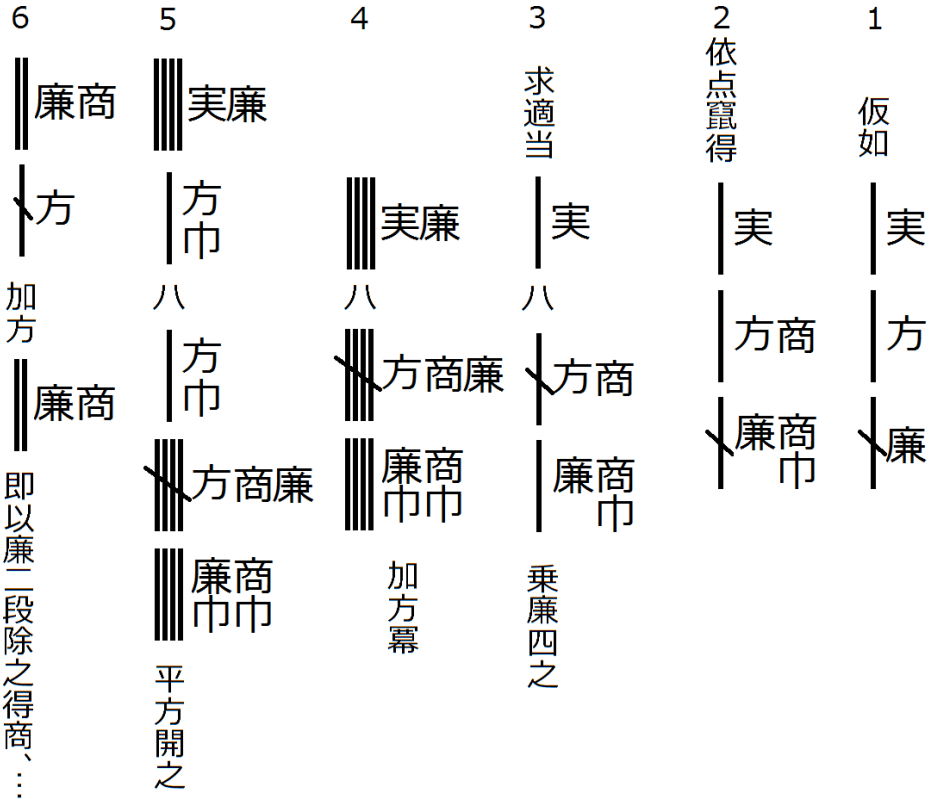


一桁の数字には縦書きを使うのですが，2 桁以上では，一，十，百，千... の位を縦，横，縦，横,... と交互に使っていきます． 123 のような数字を縦書きのみで使うと何が書いてあるか分からなくなるからですね． 負の数は一の位に斜線を引いて表します．

主な式の表し方は次のようになります．



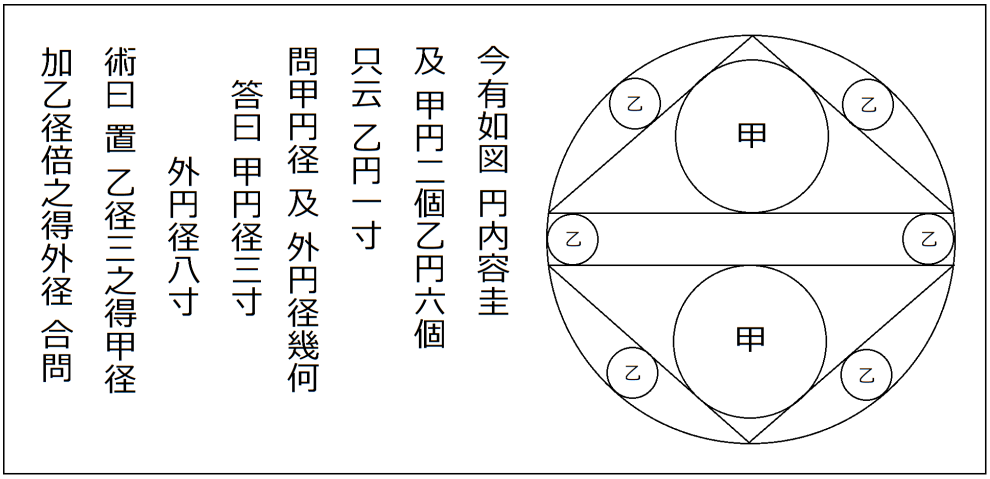
文字としては甲，乙，丙... が多く使われ，他に子，丑，寅,... 天，地，人などを使います． 問題設定によっては直角三角形の辺を勾，股，弦，円に関する問題では直径を円径などと，そのまんま文字としてしまうこともあります．さて，① は単なる甲という変数を表します． ② は単項式 $-4\times$ 甲 です． 甲 + 乙 は ③,④ の 2 つの書き方があり，⑤ は 甲 − 乙 ですね． ‖甲 − 乙‖ は ⑥ で表します． ⑦ は 甲 × 乙，⑧ は 甲 ÷ 乙 です． 現在の積や分数の書き方と似ていますね． 甲^2，甲^3，甲^4,$\sqrt{甲}$ はそれぞれ ⑨,⑩,⑪,⑫ で，甲四と縦に書けば 5 乗です． カッコの表現はないので，(甲 − 乙)^2 と 甲^2 − 乙^2 は ⑬, ⑭ のように区別しています．例えば『算法類聚(るいじゅ) 巻九』では，2 次方程式 $c+bx-ax^2=0$ の解法を次のように述べています．



1. 仮に 実，方, − 廉 が与えられたとして
2. 点竄術により 実 + 方商 − 廉商^2 とする
3. 実 = −方商 + 廉商^2 となる商を求める． 4 廉 をかける．
4. 4 実廉 = −4 方商廉 + 4 廉^{2}商^2． 方^2 を加える．
5. 4 実廉 + 方^2 = 方^2 − 4 方商廉 + 4 廉^{2}商^2． 開平して，
6. 2 廉商 − 方 に方を加えて，2 廉 を除けば商を得る．

算額の問題

和算の伝統の一つに算額奉納があると述べました． ここでは埼玉県の日枝(ひえ)神社に奉納されているものを例に，算額を見てみましょう． (文章は読みやすいようにスペースを入れています．)



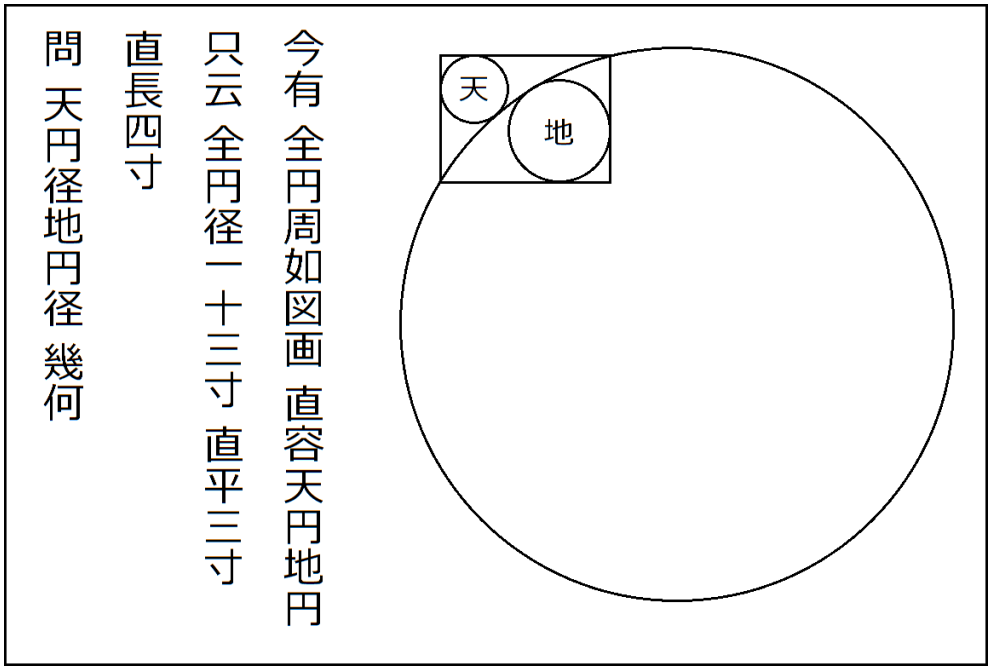
[用語]
今有如図，術曰置：それぞれ問題文，一般解始まりの慣用句
只云：数値条件始まりの慣用句
圭：二等辺三角形
円径：直径

文章は三段落 1. 問題文， 2. 答え， 3. 考え方や定理 (術文) に分かれています．訳してみると

1. 図のように外円に二等辺三角形が内接し，甲円 2 個と乙円 6 個がある． 乙円の直径を 1 寸とするとき，甲円の直径と外円の直径はいくらか．
2. 甲円の直径は 3 寸，外円の直径は 3 寸．
3. 乙円の直径を 3 倍すれば甲円の直径が得られ，それに乙円の直径を足して 2 倍すれば外円の直径を得る．

という具合です． いずれも略解のようですが，それもその通り． 算額は見学者への挑戦でもあるので，詳しい解説はほとんどされません． (皆さんもぜひ手を動かして解いてみてください！) 問題の題材としては様々な図形と円がやたら接しているものが多いようです． 円に関する問題は，円周率の計算なども含めて盛んに研究され，その理論を総称して円理と呼んでいます．

最後に私が京都で見た算額を皆さんへの遺題として終わります． ありがとうございました．



[用語]
直：長方形
容：接していること
直平：長方形の短い辺
直長：長方形の長い辺
(京都府　御香宮神社)

参考文献

[1]　大原茂 (1998)『算額を解く』さきたま出版会.
[2]　上垣渉 (2006)『はじめて読む数学の歴史』ベレ出版.
[3]　加藤平左ェ門 (1957)『和算ノ研究』日本学術振興会.
[4]　山司勝紀・西田知己編 (2009) 『和算の事典』 佐藤健一監修，朝倉書店.
[5]　近畿数学史学会編著 (1992)『近畿の算額「数学の絵馬を訪ねて」』大阪教育図書株式会社.

p進数の世界 (白井)

1,2 章は高校生程度の知識で読めるよう書いてあります．3,4 章は大学 2 年程度の内容まで入ります (距離空間という言葉を知っていれば分からない用語は無いと思います)．また，ここで p は素数とします．

p進における近さとは

p 進数体 $\mathbb{Q}_p$ は 1900 年ごろ Hensel によって導入された $\mathbb{Q}$ の拡大体です．$\mathbb{Q}_p$ は $\mathbb{R}$ とは違った「距離感」を持っています．その「ある素数 p に着目した距離感」は数論ととても相性が良く，$\mathbb{Q}_p$ は今や数論にとって欠かせない概念になっています．

では $\mathbb{Q}_p$ はどのような「距離感」を持っているのか，馴染み深い $\mathbb{R}$ と比較しながら説明していきます．

$\mathbb{R}$ の世界では，整数 a, b について非常に小さい正の数 ε を用いて，

$$|a-b| < \varepsilon$$

となるとき，a と b は非常に近いと思えます．一方 $\mathbb{Q}_p$ の世界では，整数 a, b について非常に**大きい**整数 n を用いて，

$$a - b \equiv 0 \mod p^n$$

となるとき非常に近いと感じよう，というのがルールです．差が p でたくさん割り切れるほど，二つの数は近いということです．ですので例えば，

$$1, p, p^2, p^3, p^4, \dots$$

という数列は 0 にだんだん近づいていきます．また例えば $p = 3$ としたとき，4 は 2 よりも 1 に近いですが，10 はもっと 1 に近くなります．差を計算してみれば分かりますね．

このように p 進における近さは，数直線で見る $\mathbb{R}$ における近さとは大きく異なるのですが，この「距離感」を突き詰めると $\mathbb{Q}_p$ が現れてきます．

p進展開で$\mathbb{Q}_p$を定めよう

実数は普段行われているように，(有限とは限らない) 少数表示を用いて書き表せますが，なぜ表せると言えるのでしょうか．それは例えば円周率 π は 10 進法で書き表すと $3.1415\cdots$ となりますが，これを桁の概念を自明なものとせずちゃんと書くと，

$$3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2} + 1 \times 10^{-3} + 5 \times 10^{-4} + \cdots$$

と書くことが出来ます．この数の極限，つまり行き着く先が $\mathbb{R}$ の中に入っているからです．これについては 4 章で詳しく述べることにしましょう．

ここで先ほどの $\mathbb{R}$ の世界での近さが効いています．上の表示では，

$$|\pi - 3.1415| < 10^{-4}$$

が成り立っているので，π と 3.1415 は ($\mathbb{R}$ の世界で) とても近いと言えます．右辺の 10^{-4} がもっと小さくなっても，“$\dots$” のところをもっと具体的に書いていけば π との差の絶対値がそれより小さくなるので，$3.1415\cdots$ は π に限りなく近づいていると言えます．

これを $\mathbb{Q}_p$ の世界で考えるとどうなるでしょうか．ここで $\mathbb{Q}_p$ を次のように定義してしまいましょう．

$$\mathbb{Q}_p = \Big\{ \sum_{n=m}^{\infty} a_n p^n ; m \in \mathbb{Z}, a_n \in \{0, 1, \dots, p-1\} \Big\}$$

$\mathbb{Q}_p$ の元をひとつ書いてみると (p=3 とします)，

$$\cdots 2 \times 3^2 + 1 \times 3^1 + 0 \times 3^0 + 0 \times 3^{-1} + 2 \times 3^{-2}$$

このように $\mathbb{Q}_p$ の元を $\sum_{n=m}^{\infty} a_n p^n$ の形で書き表すことを，$\mathbb{Q}_p$ の p **進展開**といいます．[1)]

先ほどとの違いは何でしょうか．10 と 3 の違いはありますが，何よりも大きいのは “$\cdots$” の位置ですね，$\mathbb{Q}_p$ では数の左についています．これは $\mathbb{Q}_p$ の世界では非常に大きい整数 n について p^n という数が 0 にとても近いからです．というわけで上の元は $\mathbb{Q}_p$ の世界で「ある数」にちゃんと収束していることがわかります．さらにその「ある数」は $\mathbb{Q}_p$ の中に入っています．

例として，$\mathbb{Q}_3$ で $-1 \in \mathbb{R}$ に対応する数を考えてみましょう．3^n たちを足し合わせて作らなければいけないので，簡単な形にはならなそうですね．そこで $-1 \in \mathbb{R}$ を

$$x \text{ についての方程式 } x+1=0 \text{ を満たす唯一の数}$$

と考え直してみましょう．足し算の筆算の形を作って右から考えていきましょう．

$$\begin{array}{rccccc} & \cdots & ? & ? & ? & ? \\ + & & & & & 1 \\ \hline & \cdots & 0 & 0 & 0 & 0 \end{array} = 0$$

ここで今は 10 ではなく 3 で桁が繰り上がることに注意しましょう。1 の位は 1 を足して 0 になるので 2 です．3 の位 [2)] は繰り上がりがあるので 1 を足して 0 になる数，つまり 2 です．3^2 の位以降も同様に考えると $\cdots$

$$\begin{array}{rccccc} & \cdots & 2 & 2 & 2 & 2 \\ + & & & & & 1 \\ \hline & \cdots & 0 & 0 & 0 & 0 \end{array} = 0$$

となり，$\cdots 2222 \in \mathbb{Q}_3$ が $-1 \in \mathbb{R}$ に対応していることがわかります．同様に任意の有理数が p 進展開でき，$\mathbb{Q} \subset \mathbb{Q}_p$ であることがわかります．

ところで，ある集合の点列がその集合の中に極限を持つとき，その集合は完備であるといいます．今考えている $\mathbb{R}$ と $\mathbb{Q}_p$ は「$\mathbb{Q}$ を含み，かつ完備な体である」という共通の性質を持っています．今度はこの完備性を用いて $\mathbb{Q}_p$ を定義する方法を考えてみましょう．

p 進距離を定める

完備性について議論するにはまず $\mathbb{Q}_p$ に距離を定めないといけません．最初に述べた「p 進における近さ」を定式化しましょう．

Def 0.1. a を 0 でない有理数とする．各 p に対し a は，

$$a = p^n \frac{s}{t} \quad (n \in \mathbb{Z}, s, t \in \mathbb{Z} \setminus p\mathbb{Z})$$

と一通りに表すことが出来る．このとき $v_p(a) = n$ と定義し，v_p を a の p **進付値**という．

ざっくりいうと，v_p は a が p で何回割り切れるかを表した関数です．また $v_p(0) = \infty$ としておきましょう．このとき次が成り立ちます．

Prop 0.2. p 進付値について，次が成り立つ．(∞ に関しての演算は直観の通り)

(1) $v_p(ab) = v_p(a) + v_p(b)$
(2) $v_p(a+b) \geqq \min(v_p(a), v_p(b))$
(3) $v_p(a) \neq v_p(b)$ ならば，$v_p(a+b) = \min(v_p(a), v_p(b))$

Proof. (1) 定義にならって，

$$a = p^n \frac{s}{t}, b = p^{n'} \frac{s'}{t'}$$

と書き表すと，

$$ab = p^{n+n'} \frac{ss'}{tt'}$$

[1)] $\mathbb{Q}_p$ がちゃんと体になること，$\mathbb{Q}_p$ の元で形は違うが値はおなじものがないことを証明しなければ $\mathbb{Q}_p$ を定義したことにはなりませんが，ここでは割愛します．

[2)] 1 つ左の桁のことなのですが，10 の位とは言えないので，暫定的にこう呼びました．

となる．$ss', tt' \in \mathbb{Z} \setminus p\mathbb{Z}$ だから，$v_p(ab) = n + n' = v_p(a) + v_p(b)$.
(2) $v_p(a) \leqq v_p(b)$ として一般性を失わない．このとき $n' - n \geqq 0$.

$$a + b = p^n \frac{s}{t} + p^{n'} \frac{s'}{t'} = p^n \frac{st' + p^{n'-n} s't}{t't}$$

よって (1) より，$v_p(a+b) = v_p(p^n) - v_p(tt') + v_p(st' + p^{n'-n} s't)$．$st' + p^{n'-n} s't \in \mathbb{Z}$ なので，付値は 0 以上．よって $v_p(a+b) \geqq n - 0 + 0 = n = v_p(a)$.

(3) $v_p(a) < v_p(b)$ として一般性を失わない．このとき (2) より，$v_p(a+b) \geqq v_p(a)$．また再び (2) より，

$$v_p(a) = v_p((a+b) - b) \geqq \min(v_p(a+b), v_p(-b))$$

いま，$v_p(a) < v_p(b) = v_p(-b)$ としているので，$v_p(a) \geqq v_p(a+b)$ がわかり，以上より $v_p(a+b) = v_p(a)$　□

次に，p 進付値を用いて p 進絶対値を定義します．

Def 0.3. $a \in \mathbb{Q}$ に対し，

$$|a|_p = \begin{cases} p^{-v_p(a)} & (a \neq 0) \\ 0 & (a = 0) \end{cases}$$

を a の p **進絶対値**という．

このとき次が成り立ちます．[3)]

Prop 0.4. p 進絶対値について，次が成り立つ．

(1) $|ab|_p = |a|_p |b|_p$
(2) $|a+b|_p \leqq \max(|a|_p, |b|_p)$

Proof. (1) Prop 3.2. (1) と指数法則よりわかる．
(2) Prop 3.2. (2) と指数法則よりわかる (大小関係に注意)．　□

p 進絶対値は乗法に関して付値っぽい性質を満たしています．(ちゃんというと，p 進絶対値は乗法付値です．)
最後に p 進絶対値を使って p 進距離を定義します．

Def 0.5. $a, b \in \mathbb{Q}$ に対し，

$$d_p(a, b) = |a - b|_p$$

を a と b の p **進距離**という．

このとき次が成り立ちます．

Thm 0.6. p 進距離について，距離の公理が成り立つ．

(1) $d_p(a, b) \geqq 0$ であり，$d_p(a, b) = 0 \iff a = b$
(2) $d_p(a, b) = d_p(b, a)$
(3) $d_p(a, c) \leqq d_p(a, b) + d_p(b, c)$

Proof. (1) $a = b$ の時は明らか．$a \neq b$ ならば，$d_p(a, b) = p^{-v_p(a-b)} \neq 0$.
(2) $d_p(a, b) = p^{-v_p(a-b)} = p^{-v_p(b-a)} = d_p(b, a)$.
(3) Prop 3.4. (2) から $x, y \in \mathbb{Q}$ について，$|x+y|_p \leqq |x|_p + |y|_p$ がわかる．$x = a-b, y = b-c$ とすると，$x+y = a-c$ となるので $d_p(a, c) \leqq d_p(a, b) + d_p(b, c)$ がわかる．　□

Thm 3.6. により，位相空間 $(\mathbb{Q}, d_p)$ は距離空間であることがわかります．これで最初に述べた「p 進における近さ」を d_p によって定式化することができました．

[3)] p 進距離が距離になるには，実は (2) は必要なく，(2) より弱い条件 $|a+b|_p \leqq |a|_p + |b|_p$ で十分なのですが，$|a+b|_p \leqq \max(|a|_p, |b|_p)$ から $\mathbb{Q}_p$ は「数列の和が収束することと数列が 0 に収束することが同値」という，$\mathbb{R}$ よりも強い収束に関しての法則を持つことがわかります．このような乗法付値には名前がついていて，**非アルキメデス付値**といいます．

完備化で $\mathbb{Q}_p$ を定めよう

Def 0.7. ある集合の数列 $\{x_n\}$ が**コーシー列**であるとは，「 任意の $\varepsilon > 0$ に対し, $m, n \geqq N$ ならば， $|x_m - x_n| < \varepsilon$ を満たすような $N \in \mathbb{N}$ が存在する」 という条件を満たす数列のことである．また，ある集合の任意のコーシー列が収束するとき，その集合は**完備**であるという．

「収束しないなんてことあるのか？」と思うかもしれませんが，例えば $\mathbb{Q}$ 上の数列

$$3, 3.1, 3.14, 3.141, 3.1415, \cdots$$

は Cauchy 列で π に収束しますが，π は有理数ではありません．ですので $\mathbb{Q}$ は完備ではありません．

ここで，$\mathbb{R}$ の定義を「有限値に収束する有理数のコーシー列全体」と考え直してみましょう．正確には，

$$S = \text{有理数のコーシー列全体の集合}$$

とし，S 上での同値関係を，

$$\{x_n\} \sim \{y_n\} \Longleftrightarrow \begin{array}{l}\text{任意の}\varepsilon > 0 \text{に対し}, n \geqq N \text{ならば} \\ \quad |x_n - y_n| < \varepsilon \text{を満たすような } N \in \mathbb{N} \text{が存在する}\end{array}$$

と定義します．そして，S を今の同値関係で割った商集合 $S/\sim$ を $\mathbb{R}$ と定義します．[4] この方法で構成した $\mathbb{R}$ はいつもの意味での $\mathbb{R}$ とちゃんと一致します．この操作のことを $\mathbb{Q}$ の通常の距離についての**完備化**といいます．同じことを $\mathbb{Q}_p$ でも考えてみるのです．

Def 0.8. 有理数の数列 $\{x_n\}$ が p **進コーシー列**であるとは，「任意の $\varepsilon > 0$ に対し, $m, n \geqq N$ ならば, $d_p(x_m, x_n) < \varepsilon$ を満たすような $N \in \mathbb{N}$ が存在する」という条件を満たす数列のことである．

さらに，

$$S_p = \text{有理数の } p \text{ 進コーシー列全体の集合}$$

とし，S_p 上での同値関係を，

$$\{x_n\} \sim_p \{y_n\} \Longleftrightarrow \begin{array}{l}\text{任意の}\varepsilon > 0 \text{に対し}, n \geqq N \text{ならば} \\ \quad d_p(x_n, y_n) < \varepsilon \text{を満たすような } N \in \mathbb{N} \text{が存在する}\end{array}$$

と定義します．そして，S_p を今の同値関係で割った商集合 $S_p/\sim_p$ を $\mathbb{Q}_p$ と定義します．この $\mathbb{Q}_p$ は p 進展開により定義したものと同じになります．

以上で $\mathbb{Q}_p$ を 2 種類の方法で定義することができました．[5]

$\mathbb{Q}_p$ で何ができるか

ここまで $\mathbb{Q}_p$ を $\mathbb{R}$ との比較で構成してきたのですが，実は $\mathbb{Q}_p$ の視点と $\mathbb{R}$ の視点を組み合わせることで，$\mathbb{Q}$ についての情報が得られることがあるということが分かっています．例えば，

$$0 \text{ でない } a, b \in \mathbb{Q} \text{ に対し}, ax^2 + by^2 = 1 \text{ となる } x, y \in \mathbb{Q} \text{ が存在するのは } a, b \text{ がどんなときか？}$$

という問題は $x, y \in \mathbb{R}$ および $x, y \in \mathbb{Q}_p$ について同じ問題を考えることで解を導くことができます．気になった方は，下の参考文献をもとに調べてみてください．数論の鮮やかさと強力さがわかっていただけると思います．

参考文献

[1]　加藤和也，黒川信重，斎藤毅『数論 I—Fermat の夢と類体論』 岩波書店，2016 年
[2]　雪江明彦『整数論 1　初等整数論から p 進数へ』　日本評論社，2013 年
[3]　雪江明彦『整数論 2　代数的整数論の基礎』　日本評論社，2013 年
[4]　J.W.S Cassels, A.Fröhlich. *Algebraic Number Theory.* London Mathematical Society, 2010.

[4] $\mathbb{R}$ の構成にはコーシー列を用いる方法の他に，デデキント切断による方法などがあります．詳しくは解析学にお任せします．
[5] $\mathbb{Q}_p$ のメジャーな定義はあともう一つ，逆極限 $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ を用いたものがあります．

四次元立方体の描き方 (マスク)

四次元立方体を描いてみよう

　四次元の立体がどのような形状をしているのか，ほとんどの方は正確にイメージすることができないと思います．それは我々が手に取って観察できる立体が，三次元より低い次元のものしかないからです．

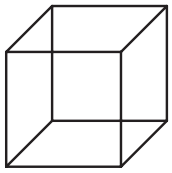
　では，我々は四次以上の次元の様子を知ることはできないのでしょうか？　いいえ，そんなことはありません．高次元のように目に見えないものの様子を調べることができる，それもまた数学の力の一つだと私は考えます．

　今回紹介する “四次元立方体の描き方” は，その中のほんの一例です．

　早速，描き方を解説していきます．

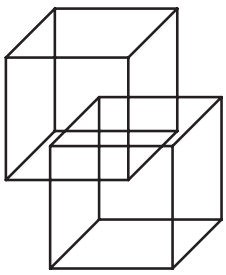
1

　普通の三次元の立方体を描きます．(これは普段あなたが描いているもので問題ありません．図は一例です．)



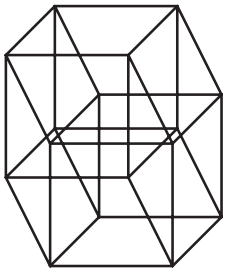
2

　同じ三次元の立方体を，ずらした位置にもう一つ描きます．



3

　頂点を線分で結びます．



　これで完成です．

前ページで何をしていたのか

前ページで四次元立方体の具体的な描き方の一例を紹介しました．それでもう満足という方は，さっさと次の記事に行っていただいて構いません．この章は先程の描き方でどうして四次元立方体を描けるのか，それを数学的に正当化するのを目的としています．

また，この章は大学一年生レベルの線型代数の知識を前提としています．

定義 1 (n 次元立方体)**.** $\mathbb{R}^n$ の部分集合 M が，以下の条件を満たすとき，M を n 次元立方体と呼ぶ．

$$^{\exists}A \in O(n), ^{\exists}b \in \mathbb{R}^n, ^{\exists}a \in \mathbb{R}_{>0} \quad s.t. \quad M = A([0,a]^n) + b$$

ただし，$O(n)$ は n 次直交行列の集合で，$[0,a]^n$ は閉区間 $[0,a]$ の n 個の直積である．

注意 1. 上の定義は，n 次元立方体が，$[0,1]^n$ を $\mathbb{R}^n$ 内で回転したり，平行移動をしたり，拡大縮小をして得られる図形であることを言っている．

注意 2. 上の理由で，今後は n 次元立方体は全て $[0,1]^n$ として考えることにする．

定義 2 (頂点)**.** 集合 $\{0,1\}^n \subset \mathbb{R}^n$ の元を n 次元立方体の**頂点**と呼ぶ．

定義 3 (辺)**.** n 次元立方体の異なる二つの頂点を結んだ線分のうち，長さが 1 になる線分のことを，n 次元立方体の**辺**と呼ぶ．

注意 3. 上の頂点，辺の定義は n 次元立方体に特化した定義であり，一般の n 次元の立体に適応できるものではない．今回は，これを紙面に図示するという観点から，イメージしやすいようにこの定義を採用している．

定義 4 (n 次元立方体を描く)**.** n 次元立方体を描くとは，次の操作のことを指す．

どの異なる二つのベクトルをとっても，線型独立となるような $\mathbb{R}^2$ のベクトルの組 $v_1, v_2, \ldots, v_n$ を一つ固定する．$\mathbb{R}^n$ の標準基底 $e_1, e_2, \ldots, e_n$ を，$v_1, v_2, \ldots, v_n$ にそれぞれうつす線型写像 $f\colon \mathbb{R}^n \to \mathbb{R}^2$ を考え，それによる n 次元立方体の頂点と辺の像を 2 次元平面に図示する．

注意 4. 上の定義を雑に説明すると，n 次元立方体を描くとは，$\mathbb{R}^n$ の標準基底を $\mathbb{R}^2$ 上のいい感じなベクトルの組にうつしたときの像を描くことである．

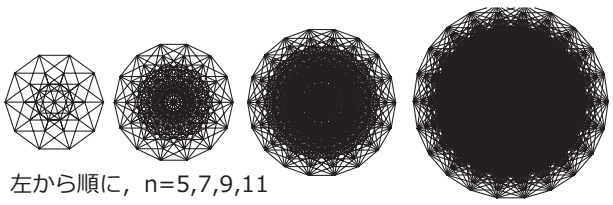
注意 5. 上の定義は前ページの描き方は含んでいるが，n 次元立方体をどう描くかは個人の自由である．当然，上の定義以外で意味を持つ描き方もこの世には存在している．よって，もし *"4 次元立方体"* と *Google* で検索して上の定義に当てはまらない図が出てきても，筆者を責めてはいけない．決して責めてはいけない．

まとめ

以上の定義により，前ページの描き方が四次元立方体を描いたものだといいうことがご理解いただけたかと思います．三次元立方体をずらした向きが，ベクトル v_4 に対応しているのです．

おまけ

せっかく n 次元立方体の描き方を定義したのだから，もっと高次元の立方体を見てみたい，という欲張りな人のためにこの章を用意した．結論から述べると，n 次元立方体の辺は $n2^{n-1}$ 本あるので，計算量のオーダーはは $n2^n$ となり，すぐに CPU が逝く．また，図を見ればわかるがぐっちょぐちょなので，まるでよくわからん．もっともっと高次元が欲しい欲しがりは，自分の手を動かしなさい．ベクトルは $e^{\frac{2\pi i}{n}}$ の組を取り，使用ソフトは Geogebra である．



左から順に，n=5,7,9,11

ラムダ計算と述語論理 (後藤)

初めに

何らかの論理体系においてある命題 Φ が真であるとする．するとしばしば，適当なラムダ計算の型付け体系が存在して，その型付け体系で Φ を何らかの型だと解釈でき，Φ を型にもつ項 M が存在することが示せる．このとき，その M は命題としての Φ の証明と対応する．このような論理とラムダ計算との対応は Curry-Howard 対応と言われ，論理学と計算機科学を結びつけるものとして非常に重要である．ここでは述語論理を取り上げ，型付きラムダ計算との対応を証明する．

なお，以下では型付きラムダ計算と多類述語論理の厳密な定義を述べるが，これは単に定義を明確化するためだけのものなので，詳しい説明 (概念の性質や定義のモチベーションなど) はほとんど省略した．したがって，読者にはラムダ計算と述語論理についてある程度の背景知識を仮定する．

型付きラムダ計算

ここでは，型付きラムダ計算の体系として λP2 と呼ばれるものを扱う．通常の単純型付きラムダ計算 $\lambda\!\rightarrow$ では初めから項と型を区別するが，ここで扱う λP2 では項と型を区別せず扱い，型付け規則によって何が項で何が型であるかを決めるという方針をとる．

定義 1. 可算集合 Var を固定し，その元を**変項**という．

定義 2. 変項以外に記号 $\star$, $\Box$ を用意し，これを**ソート**という．

定義 3. 集合 Term を以下によって再帰的に定義する．

$$
\begin{aligned}
x \in \mathrm{Var} &\Longrightarrow x \in \mathrm{Term} \\
s \in \{\star, \Box\} &\Longrightarrow s \in \mathrm{Term} \\
M, N \in \mathrm{Term} &\Longrightarrow (MN) \in \mathrm{Term} \\
A, M \in \mathrm{Term} \text{ AND } x \in \mathrm{Var} &\Longrightarrow (\lambda x{:}\, A.\, M) \in \mathrm{Term} \\
A, B \in \mathrm{Term} \text{ AND } x \in \mathrm{Var} &\Longrightarrow (\Pi x{:}\, A.\, B) \in \mathrm{Term}
\end{aligned}
$$

このとき，Term の元を**擬項**という．

以降，α-変換 (束縛変数の変換) で移り合う擬項は同一視する．

定義 4. 変項 x と擬項 A に対し，記号 $x{:}\, A$ を**型宣言**という．

定義 5. 型宣言の列 $\Gamma = \langle x_1{:}\, A_1, \ldots, x_n{:}\, A_n \rangle$ を**型環境**という．

型環境は型宣言の列であって集合ではない．したがって，重複した要素をもっている場合，それを 1 つにまとめたものとは異なる型環境であるとする．さらに，要素の順番を入れ替えたものも異なる型環境であるとする．例えば，$\langle x{:}\, A, x{:}\, A \rangle \neq \langle x{:}\, A \rangle$ および $\langle x{:}\, A, y{:}\, B \rangle \neq \langle y{:}\, B, x{:}\, A \rangle$ である．ただし，便宜上しばしば集合と同じように扱うことがある．例えば，2 つの型環境 Γ, Γ' に対して，$\Gamma \cup \Gamma'$ と書いて Γ の後に Γ' の要素を順番をそのままに付け加えた型環境を表す．

定義 6. 型環境 Γ と擬項 M, A に対し，記号 $\Gamma \vdash_{\lambda\mathrm{P2}} M{:}\, A$ を以下の 7 個の推論規則に従って定める．

$$\frac{}{\vdash \star : \Box}\ \text{Axiom}$$

$$\frac{\Gamma \vdash A : s}{\Gamma \cup \langle x : A \rangle \vdash x : A}\ \text{Start}$$

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash B : s}{\Gamma \cup \langle x : B \rangle \vdash M : A}\ \text{Weak}$$

$$\frac{\Gamma \vdash M : (\Pi x : A.\, B) \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B[x := N]}\ \text{App}$$

$$\frac{\Gamma \cup \langle x : A \rangle \vdash M : B \quad \Gamma \vdash (\Pi x : A.\, B) : s}{\Gamma \vdash (\lambda x : A.\, M) : (\Pi x : A.\, B)}\ \text{Abs}$$

$$\frac{\Gamma \vdash A : s \quad \Gamma \cup \langle x : A \rangle \vdash B : s'}{\Gamma \vdash (\Pi x : A.\, B) : s'}\ \text{Prod}$$

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash A' : s \quad A =_\beta A'}{\Gamma \vdash M : A'}\ \text{Conv}$$

なお，$\Gamma \cup \langle x : A \rangle$ などと書かれている箇所において，x は Γ の要素に含まれていないものとする．また，s は任意のソートを表すが，規則 Prod においては，

$$(s,\, s') \in \{(\star,\, \star),\, (\Box,\, \star),\, (\star,\, \Box)\}$$

とする [1]．

定義 7. 擬項 M, A に対し，ある型環境 Γ が存在して $\Gamma \vdash_{\lambda P2} M : A$ が成り立つとする．このとき，M を**項**といい，A を**型**という．

この型付け規則は以下に述べるように単純型の規則の拡張になっている．

定義 8. 擬項 A, B に対し，

$$A \to B \equiv \Pi t : A.\, B$$

と書く．ただし，t は $t \notin \mathrm{FV}(B)$ を満たす変項とする [2]．

このように定義すると，規則 App によって，

$$\frac{\Gamma \vdash M : (A \to B) \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B}\ \text{App}$$

が成立し，規則 Abs によって，

$$\frac{\Gamma \cup \langle x : A \rangle \vdash M : (A \to B) \quad \Gamma \vdash (A \to B) : \star}{\Gamma \vdash (\lambda x : A.\, M) : (A \to B)}\ \text{Abs}$$

が成立する．さらに，$x \notin \mathrm{FV}(B)$ なる適当な変項 x を選び，規則 Prod の $(s,\, s') = (\star,\, \star)$ の場合を用いれば，

$$\frac{\Gamma \vdash A : \star \qquad \dfrac{\Gamma \vdash B : \star \quad \Gamma \vdash A : \star}{\Gamma \cup \langle x : A \rangle \vdash B : \star}\ \text{Weak}}{\Gamma \vdash (A \to B) : \star}\ \text{Prod}$$

が成立する．以上により，$\Gamma \vdash A : \star$ が成り立つとき A を (単純型付きラムダ計算における) 型だと考えれば，単純型には全て $\star$ の型をつけることができ，単純型の型付け規則をそのまま行うことができる．

---

[1] 規則 Prod において $(s,\, s') = (\star,\, \Box)$ の場合を除いたものは $\lambda 2$ もしくは System F と呼ばれ，Haskell に代表される多くの関数型プログラミング言語の基盤となっている．また，規則 Prod に $(s,\, s') = (\Box,\, \Box)$ の場合をさらに加えたものは $\lambda \mathrm{C}$ もしくは calculus of constructions と呼ばれ，これをさらに拡張したものは Coq の型システムとして用いられている．このように，規則 Prod でどのような $(s,\, s')$ のパターンを許すかによって様々な型付け規則が定まる．

[2] $\mathrm{FV}(B)$ は B に含まれる自由変項全体の集合を表す．

さて，規則 Prod について少し補足をしておく．まず，$(s,\, s') = (\star,\, \star)$ の場合は，すでに述べたように単純型を構成するのに用いられる．例えば，

$$\alpha{:}\star \vdash_{\lambda P2} (\alpha \to \alpha){:}\star \tag{1}$$

$$\alpha{:}\star \vdash_{\lambda P2} (\lambda x{:}\alpha.\, x){:}(\alpha \to \alpha) \tag{2}$$

$$\alpha{:}\star,\, \beta{:}\star,\, y{:}\beta,\, z{:}\alpha \vdash_{\lambda P2} ((\lambda x{:}\alpha.\, y)z){:}\beta$$

$$\alpha{:}\star,\, \beta{:}\star \vdash_{\lambda P2} (\lambda x{:}\alpha.\, \lambda y{:}(\alpha \to \beta).\, yx){:}(\alpha \to (\alpha \to \beta) \to \beta)$$

などが成り立つ．

$(s,\, s') = (\square,\, \star)$ の場合は，型に関する量化をするために用いられる．例えば，式 1 と規則 Prod を用いることで，

$$\vdash_{\lambda P2} (\Pi\alpha{:}\star.\, \alpha \to \alpha){:}\star$$

が得られる．これと式 2 を合わせれば，規則 Abs によって，

$$\vdash_{\lambda P2} (\lambda\alpha{:}\star.\, \lambda x{:}\alpha.\, x){:}(\Pi\alpha{:}\star.\, \alpha \to \alpha)$$

が導出できる．ここで出てくる $\lambda\alpha{:}\star.\, \lambda x{:}\alpha.\, x$ は，型 α を引数にとって α 上の恒等関数を返す項である．これは単純型付き計算の範囲では成立し得ない項である．

$(s,\, s') = (\star,\, \square)$ の場合は，いわゆる依存型を構成するために用いられる．これにより，例えば，

$$\alpha{:}\star \vdash_{\lambda P2} (\alpha \to \star){:}\square$$

が成り立つので，

$$\alpha{:}\star,\, p{:}(\alpha \to \star),\, x{:}\alpha \vdash_{\lambda P2} px{:}\star$$

が得られる．依存型の解釈は様々あるが，ここではこのノートのテーマである型と命題の関係に注目する．まず，$\star$ は命題と集合を同時に表す型であると考える．すると，$\alpha{:}\star$ は α が何らかの集合であることを宣言していると見なせる．さらに，$\alpha \to \star$ は α の元を受け取り命題を返す型であると考えられる．すなわち，それは α 上の述語である．したがって，$p{:}(\alpha \to \star)$ によって p は α 上の述語だと宣言されている．最後に，$x{:}\alpha$ によって x は α の元だと宣言されている．上に示した式は，これらの宣言のもとで px は 1 つの命題だということを述べている．

別の例として，

$$\alpha{:}\star,\, p{:}(\alpha \to \star),\, x{:}\alpha \vdash_{\lambda P2} (\Pi x{:}\alpha.\, px \to px){:}\star$$

を挙げておく．$\Pi x{:}\alpha$ を x に関する全称量化だと考えることにする．すると，上の式は，集合 α とその上の述語 p について，任意の α の元 x に対し px ならば px が成り立つという主張は 1 つの命題であることを述べている．この命題は真であるが，実は，

$$\alpha{:}\star,\, p{:}(\alpha \to \star),\, x{:}\alpha \vdash_{\lambda P2} (\lambda x{:}\alpha.\, \lambda y{:}pa.\, x){:}(\Pi x{:}\alpha.\, px \to px)$$

が成り立つので，$\Pi x{:}\alpha.\, px \to px$ を型とする項が存在する．このノートの目標は，上の例のように，型を命題だと解釈したとき，その命題が真ならばその型をもつ項が実際に存在することを示すことである．

λP2 の詳しい性質についてはここでは省略する．適宜，Barendregt[1] の 5 章もしくは Hindley[2] の 13 章を参照してほしい．

多類述語論理

ここでは，述語論理に型 (ここでは類と呼ばれる) の概念を加えた多類述語論理について考える．これは，以下のように定式化される．

定義 9. 空でない有限集合 Sort を用意し，その元を**類**という．

定義 10. 有限集合 Pred を用意し，その元を**述語**という．それぞれの述語 P に対し，記号 $A_1 \times \cdots \times A_n$ を結び付け，この記号を P の**アリティ**という．

定義 11. 有限集合 Fun を用意し，その元を**関数**という．それぞれの関数 f に対し，記号 $A_1 \times \cdots \times A_n \to A$ を結びつけ，この記号を f の**アリティ**という．

定義 12. 有限集合 Con を用意し，その元を**定数**という．それぞれの定数 c に対し，類 A を 1 つ結びつける．

定義 13. 可算集合 Var を用意し，その元を**変数**という．それぞれの変数 x に対し，類 A を 1 つ結びつける．なお，各類 A に対し，A と結び付けられた変数が可算個存在するようにしておく．

定義 14. 類, 述語, 関数, 定数, 変数から成る集合の組 $\mathcal{S} = (\mathrm{Sort}, \mathrm{Pred}, \mathrm{Fun}, \mathrm{Con}, \mathrm{Var})$ を**多類構造**という．

なお，Pred, Fun, Con, Var の右下にアリティや類を明記することで，そのアリティや類をもつもの全体の集合を表すことにする．例えば，$\mathrm{Fun}_{A_1\times\cdots\times A_n\to A}$ はアリティ $A_1 \times \cdots \times A_n \to A$ をもつ関数全体の集合を表し，Con_A は類 A をもつ定数全体の集合を表す．

さらに，述語, 関数, 定数, 変数の右上にアリティや類を書くことで，それがそのアリティや類と結び付けられていることを示すことがある．例えば，述語 p に対して $p^{A_1\times\cdots\times A_n}$ と書くことで，p のアリティが $A_1 \times \cdots \times A_n$ であることを明示する．

定義 15. 多類構造 $\mathcal{S}$ をとる．各類 A に対し，集合 Term_A を以下によって再帰的に定義する．

$$\begin{aligned} x \in \mathrm{Var}_A &\implies x \in \mathrm{Term}_A \\ c \in \mathrm{Con}_A &\implies c \in \mathrm{Term}_A \\ f \in \mathrm{Fun}_{A_1\times\cdots\times A_n\to A} \text{ AND } T_i \in \mathrm{Term}_{A_i} &\implies (fT_1\cdots T_n) \in \mathrm{Term}_A \end{aligned}$$

このとき，Term_A の元を A の**論理項**という．

定義 16. 多類構造 $\mathcal{S}$ をとる．集合 Form を以下によって再帰的に定義する．

$$\begin{aligned} &\bot \in \mathrm{Form} \\ p \in \mathrm{Pred}_{A_1\times\cdots\times A_n} \text{ AND } T_i \in \mathrm{Term}_{A_i} &\implies (pT_1\cdots T_n) \in \mathrm{Form} \\ \Phi \in \mathrm{Form} &\implies (\neg\Phi) \in \mathrm{Form} \\ \Phi, \Psi \in \mathrm{Form} &\implies (\Phi \to \Psi) \in \mathrm{Form} \\ \Phi, \Psi \in \mathrm{Form} &\implies (\Phi \wedge \Psi) \in \mathrm{Form} \\ \Phi, \Psi \in \mathrm{Form} &\implies (\Phi \vee \Psi) \in \mathrm{Form} \\ \Phi \in \mathrm{Form} \text{ AND } x \in \mathrm{Var}_A &\implies (\forall x{:}\, A.\, \Phi) \in \mathrm{Form} \\ \Phi \in \mathrm{Form} \text{ AND } x \in \mathrm{Var}_A &\implies (\exists x{:}\, A.\, \Phi) \in \mathrm{Form} \end{aligned}$$

このとき，Form の元を**論理式**という．

以降，α-変換 (束縛変数の変換) で移り合う論理式は同一視する．

多類構造 $\mathcal{H}$ を，

$$\begin{aligned} \mathrm{Sort} &= \{\mathbf{N}\} \\ \mathrm{Pred} &= \{\mathbf{eq}^{\mathbf{N}\times\mathbf{N}}\} \\ \mathrm{Fun} &= \{\mathbf{s}^{\mathbf{N}\to\mathbf{N}}, \mathbf{plus}^{\mathbf{N}\times\mathbf{N}\to\mathbf{N}}\} \\ \mathrm{Con} &= \{\mathbf{0}^{\mathbf{N}}\} \end{aligned}$$

によって定義すると，これによって Heyting 算術を行うことができる．この設定のもとでは，例えば，

$$\begin{gathered} \forall x{:}\,\mathbf{N}.\,\forall y{:}\,\mathbf{N}.\,(\mathbf{eq}(\mathbf{s}x)(\mathbf{s}y)) \to (\mathbf{eq}\,xy) \\ \forall x{:}\,\mathbf{N}.\,\mathbf{eq}(\mathbf{plus}\,x\mathbf{0})x \\ \forall x{:}\,\mathbf{N}.\,\forall y{:}\,\mathbf{N}.\,\mathbf{eq}(\mathbf{plus}\,x(\mathbf{s}y))(\mathbf{s}(\mathbf{plus}\,xy)) \end{gathered}$$

は正しい論理式である．これは Heyting 算術の公理の一部を表している．

定義 17. 多類構造 $\mathcal{S}$ をとる．論理式の集合 Δ と論理式 Φ に対し，Δ から Φ が導出できることを $\Delta \vdash_{\mathcal{S}} \Phi$ と書く．これは，後の定義 24 で定められる記号 $M\colon \Delta \vdash_{\mathcal{S}} \Phi$ から M を無視したものと全く同じであるため，ここでは省略する．この論理体系を，$\mathcal{S}$ が定める**多類述語論理**という．

上の定義には二重否定除去則が含まれないことに注意すること．ラムダ計算と対応するのは直観主義論理であり，古典論理とは綺麗に対応しない．

述語論理とラムダ計算の関係

論理と型の対応

初めに，多類述語論理の論理式をラムダ計算の擬項として解釈する枠組みを定める．

定義 18. ラムダ計算の擬項 Φ, Ψ に対し，

$$\begin{aligned}
\bot &\equiv \Pi\theta\colon\star.\,\theta \\
\neg\Phi &\equiv \Phi \to \bot \\
\Phi \to \Psi &\equiv \Pi t\colon\Phi.\,\Psi \\
\Phi \wedge \Psi &\equiv \Pi\theta\colon\star.\,(\Phi \to \Psi \to \theta) \to \theta \\
\Phi \vee \Psi &\equiv \Pi\theta\colon\star.\,(\Phi \to \theta) \to (\Psi \to \theta) \to \theta \\
\forall x\colon A.\,\Phi &\equiv \Pi x\colon A.\,\Phi \\
\exists x\colon A.\,\Phi &\equiv \Pi\theta\colon\star.\,(\Pi x\colon A.\,\Phi \to \theta) \to \theta
\end{aligned}$$

と定める．なお，t は $t \notin \mathrm{FV}(\Psi)$ を満たす変項とする．

この定義により，多類構造の Sort, Pred, Fun, Con, Var をラムダ計算の Var の部分集合としてとっておけば，多種述語論理の項や式は全てラムダ計算の擬項で表現される．以降，多類述語論理の論理項や論理式とラムダ計算の擬項は特に区別しない．

標準環境

多類述語論理では，初めから使える定数が多類構造として定まっている．例えば，Heyting 算術を定める多類構造 $\mathcal{H}$ では，述語として **eq** が使え，関数として **s** や **plus** が使える．しかし，ラムダ計算ではそのような初めから使える定数はないので，型を導く前提条件すなわち型環境として，多類構造をラムダ計算に落とし込む必要がある．

定義 19. 多類構造 $\mathcal{S}$ に対し，

$$\begin{aligned}
[\![\mathcal{S}]\!]_{\mathrm{Sort}} &= \langle A\colon\star \mid A \in \mathrm{Sort}\rangle \\
[\![\mathcal{S}]\!]_{\mathrm{Pred}} &= \langle p\colon(A_1 \to \cdots \to A_n \to \star) \mid p^{A_1\times\cdots\times A_n} \in \mathrm{Pred}\rangle \\
[\![\mathcal{S}]\!]_{\mathrm{Fun}} &= \langle f\colon(A_1 \to \cdots \to A_n \to A) \mid f^{A_1\times\cdots\times A_n\to A} \in \mathrm{Fun}\rangle \\
[\![\mathcal{S}]\!]_{\mathrm{Con}} &= \langle c\colon A \mid c^{A} \in \mathrm{Con}\rangle
\end{aligned}$$

とおき，

$$[\![\mathcal{S}]\!] = [\![\mathcal{S}]\!]_{\mathrm{Sort}} \cup [\![\mathcal{S}]\!]_{\mathrm{Pred}} \cup [\![\mathcal{S}]\!]_{\mathrm{Fun}} \cup [\![\mathcal{S}]\!]_{\mathrm{Con}}$$

と定義する．$[\![\mathcal{S}]\!]$ を $\mathcal{S}$ の**標準環境**という．

なお，$[\![\mathcal{S}]\!]_{\mathrm{Sort}}$, $[\![\mathcal{S}]\!]_{\mathrm{Pred}}$, $[\![\mathcal{S}]\!]_{\mathrm{Fun}}$, $[\![\mathcal{S}]\!]_{\mathrm{Con}}$ それぞれにおいて，その元の順序は任意にとって良い．実際，例えば $[\![\mathcal{S}]\!]_{\mathrm{Sort}}$ と $[\![\mathcal{S}]\!]'_{\mathrm{Sort}}$ を異なる順序を入れた型環境とすると，

$$[\![\mathcal{S}]\!]_{\mathrm{Sort}} \vdash_{\lambda\mathrm{P2}} M\colon A \iff [\![\mathcal{S}]\!]'_{\mathrm{Sort}} \vdash_{\lambda\mathrm{P2}} M\colon A$$

が成り立つから，順序を気にする必要はない．

例として，Heyting 代数に対応する多類構造 $\mathcal{H}$ については，

$$[\![\mathcal{H}]\!] = \langle \mathbf{N}\colon\star,\ \mathbf{eq}\colon(\mathbf{N}\to\mathbf{N}\to\star),\ \mathbf{s}\colon(\mathbf{N}\to\mathbf{N}),\ \mathbf{plus}\colon(\mathbf{N}\to\mathbf{N}\to\mathbf{N}),\ \mathbf{0}\colon\mathbf{N}\rangle$$

となる．$\star$ が命題を表す型と考えれば，この定義は妥当であろう．

次に，多類述語論理での論理式の導出の前提を型環境として解釈する．そのために，論理式 Φ それぞれに対して記号 k_Φ を 1 つ新しくとって固定し，ラムダ計算の変項に加える．型環境として $k_\Phi\colon\Phi$ を与えることで，Φ を型にもつ項を強制的に作ることができるので，Φ が真だと仮定したことになる．なお，k_Φ たちはラムダ項に含めることができるが，議論を簡単にするため，以降単にラムダ計算の変項と言った場合は，ここで固定した k_Φ たちとは異なるものであるとする．

定義 20. 多類構造 $\mathcal{S}$ における式の集合 $\Delta = \{\Phi_1, \cdots, \Phi_n\}$ に対し，

$$[\![\Delta]\!] = \langle k_{\Phi_1}\colon\Phi_1,\ \cdots,\ k_{\Phi_n}\colon\Phi_n\rangle$$

と定義する．$[\![\Delta]\!]$ を Δ の**標準環境**という．

$[\![\Delta]\!]$ の元の順序は問題にならないので，任意にとって良い．

さて，多類構造 $\mathcal{S}$ が定める多類述語論理において

$$\Delta \vdash_{\mathcal{S}} \Phi \tag{3}$$

が証明できるならば，あるラムダ項 M によって

$$[\![\mathcal{S}]\!] \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} M\colon\Phi$$

が成り立つことを主張したいのであるが，Φ には $\forall$ や $\exists$ で束縛されていない変数が含まれている場合があるので，これは一般には正しくない．例えば，Heyting 代数を表す多類構造 $\mathcal{H}$ において，

$$\vdash_{\mathcal{H}} (\forall x\colon\mathbf{N}.\,\forall y\colon\mathbf{N}.\ \mathbf{eq}\,x^{\mathbf{N}}y^{\mathbf{N}}) \to \mathbf{eq}\,z^{\mathbf{N}}z^{\mathbf{N}}$$

が成り立つが，ここには自由変数として $z^{\mathbf{N}}$ が含まれている．一方ラムダ計算では，型付けられた擬項に含まれる自由変項は必ず型環境に含まれていなければならないので，

$$[\![\mathcal{H}]\!] \vdash_{\lambda\mathrm{P2}} M\colon((\forall x\colon\mathbf{N}.\,\forall y\colon\mathbf{N}.\ \mathbf{eq}\,x^{\mathbf{N}}y^{\mathbf{N}}) \to \mathbf{eq}\,z^{\mathbf{N}}z^{\mathbf{N}})$$

が成り立つなら $z\colon\mathbf{N}$ が $[\![\mathcal{H}]\!]$ に属しているはずだが，これは正しくない．

以上により，主張を弱めて，式 3 が成り立つときに，ある型環境 Γ とラムダ項 M が存在して，

$$[\![\mathcal{S}]\!] \cup \Gamma \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} M\colon\Phi \tag{4}$$

が成り立つということを主張するのだが，Γ に何の制約も課さないとこれは自明である．実際，適当な変項 k をとって $k\colon\Phi$ を Γ に加えてしまえば，$M \equiv k$ として上の主張が成り立つ．Γ が必要になるのは Φ に含まれる変数が原因なのだから，Γ には多類構造の変数に関する型宣言のみを許すことにする．

定義 21. 多類構造 $\mathcal{S}$ と型環境 Γ をとる．Γ に属する任意の型宣言 $x\colon A$ に対して A が類であるとき，Γ を**変数環境**という．

我々の主張は，式 3 が成り立つときに，ある変数環境 Γ とラムダ項 M が存在して式 4 が成り立つことである．

Curry-Howard 対応

まずは，多類構造の論理項と論理式が正しく型付けられることを示す．

命題 22. 多類構造 $\mathcal{S}$ をとる．類 A をもつ論理項 T に対し，変数環境 Γ が存在して，

$$[\![\mathcal{S}]\!] \cup \Gamma \vdash_{\lambda\mathrm{P2}} T\colon A$$
$$\mathrm{FV}(\Gamma) \subseteq \mathrm{FV}(T)$$

が成り立つ．

命題 23. 多類構造 $\mathcal{S}$ をとる．論理式 Φ に対し，変数環境 Γ が存在して，

$$[\![\mathcal{S}]\!] \cup \Gamma \vdash_{\lambda \mathrm{P2}} \Phi : \star$$
$$\mathrm{FV}(\Gamma) \subseteq \mathrm{FV}(\Phi)$$

が成り立つ．

T および Φ の構造に関する帰納法により，どちらも容易に証明ができる．

さて，多類述語論理における証明とラムダ計算における項が対応するわけだが，その対応する項を決定するために，論理式の導出過程を表現している擬項を注釈として付随させる．

定義 24. 多類構造 $\mathcal{S}$ をとる．式の集合 Δ と式 Φ と擬項 M に対し，記号 $M : \Delta \vdash_{\mathcal{S}} \Phi$ を以下の推論規則に従って定める．

$$\frac{\Phi \in \Delta}{k_\Phi : \Delta \vdash \Phi}\ \mathrm{Start}$$

$$\frac{M : \Delta \vdash \Phi}{M : \Delta \cup \{\Psi\} \vdash \Phi}\ \mathrm{Weak}$$

$$\frac{M : \Delta \vdash \bot}{M\Phi : \Delta \vdash \Phi}\ \bot\mathrm{E}$$

$$\frac{M : \Delta \cup \{\Phi\} \vdash \bot}{(\lambda k_\Phi : \Phi.\, M) : \Delta \vdash \neg\Phi}\ \neg\mathrm{I}$$

$$\frac{M : \Delta \vdash \Phi \quad N : \Delta \vdash \neg\Phi}{NM : \Delta \vdash \bot}\ \neg\mathrm{E}$$

$$\frac{M : \Delta \cup \{\Phi\} \vdash \Psi}{(\lambda k_\Phi : \Phi.\, M) : \Delta \vdash \Phi \to \Psi}\ \to\mathrm{I}$$

$$\frac{M : \Delta \vdash \Phi \to \Psi \quad N : \Delta \vdash \Phi}{MN : \Delta \vdash \Psi}\ \to\mathrm{E}$$

$$\frac{M : \Delta \vdash \Phi \quad N : \Delta \vdash \Psi}{(\lambda\theta : \star.\, \lambda u : (\Phi \to \Psi \to \theta).\, uMN) : \Delta \vdash \Phi \wedge \Psi}\ \wedge\mathrm{I}$$

$$\frac{M : \Delta \vdash \Phi \wedge \Psi}{(M\Phi(\lambda u : \Phi.\, \lambda v : \Psi.\, u)) : \Delta \vdash \Phi}\ \wedge\mathrm{E}_1$$

$$\frac{M : \Delta \vdash \Phi \wedge \Psi}{(M\Psi(\lambda u : \Phi.\, \lambda v : \Psi.\, v)) : \Delta \vdash \Psi}\ \wedge\mathrm{E}_2$$

$$\frac{M : \Delta \vdash \Phi}{(\lambda\theta : \star.\, \lambda u : (\Phi \to \theta).\, \lambda v : (\Psi \to \theta).\, uM) : \Delta \vdash \Phi \vee \Psi}\ \vee\mathrm{I}_1$$

$$\frac{M : \Delta \vdash \Psi}{(\lambda\theta : \star.\, \lambda u : (\Phi \to \theta).\, \lambda v : (\Psi \to \theta).\, vM) : \Delta \vdash \Phi \vee \Psi}\ \vee\mathrm{I}_2$$

$$\frac{M : \Delta \vdash \Phi \vee \Psi \quad N : \Delta \cup \{\Phi\} \vdash X \quad P : \Delta \cup \{\Psi\} \vdash X}{(MX(\lambda k_\Phi : \Phi.\, N)(\lambda k_\Psi : \Psi.\, P)) : \Delta \vdash X}\ \vee\mathrm{E}$$

$$\frac{M : \Delta \vdash \Phi}{(\lambda x : A.\, M) : \Delta \vdash \forall x : A.\, \Phi}\ \forall\mathrm{I}$$

$$\frac{M : \Delta \vdash \forall x : A.\, \Phi}{MT : \Delta \vdash \Phi[x := T]}\ \forall\mathrm{E}$$

$$\frac{M : \Delta \vdash \Phi[x := T]}{(\lambda\theta : \star.\, \lambda u : (\Pi x : A.\, \Phi \to \theta).\, uTM) : \Delta \vdash \exists x : A.\, \Phi}\ \exists\mathrm{I}$$

$$\frac{M : \Delta \vdash \exists x : A.\, \Phi \quad N : \Delta \cup \{\Phi[x := y]\} \vdash \Psi}{(M\Psi(\lambda y : A.\, \lambda k_\Phi : \Phi.\, N)) : \Delta \vdash \Psi}\ \exists\mathrm{E}$$

なお，規則 $\forall$I では $x \notin \mathrm{FV}(\Delta)$ とし，規則 $\exists$E では $y \notin \mathrm{FV}(\Delta) \cup \mathrm{FV}(\Phi) \cup \mathrm{FV}(\Psi)$ とする．また，T は任意の項を表し，$\Phi[x := T]$ において x と T に結びついた類は同じであるとする．

ここで定義した M が，まさに多類述語論理の証明に対応するラムダ項なのである．

定理 25. 多類構造 $\mathcal{S}$ をとる．論理式の集合 Δ と論理式 Φ と擬項 M が

$$M\colon \Delta \vdash_{\mathcal{S}} \Phi$$

を満たすならば，ある変数環境 Γ が存在して，

$$[\![\mathcal{S}]\!] \cup \Gamma \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} M\colon \Phi$$

が成り立つ．

証明は概略のみを述べる．$M\colon \Delta \vdash_{\mathcal{S}} \Phi$ の導出に関する帰納法による．以下では 1 つの場合だけを取り扱うが，他の場合も同様にして示せる．

$M\colon \Delta \vdash_{\mathcal{S}} \Phi$ が規則 $\vee$E の帰結である場合．証明の最後のステップは，

$$\frac{M\colon \Delta \vdash \Phi \vee \Psi \quad N\colon \Delta \cup \{\Phi\} \vdash X \quad P\colon \Delta \cup \{\Psi\} \vdash X}{(MX(\lambda k_\Phi\colon \Phi.\, N)(\lambda k_\Psi\colon \Psi.\, P))\colon \Delta \vdash X}\ \vee\mathrm{E}$$

となっている．帰納法の仮定は，

$$[\![\mathcal{S}]\!] \cup \Gamma_1 \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} M\colon (\Phi \vee \Psi) \tag{5}$$

$$[\![\mathcal{S}]\!] \cup \Gamma_2 \cup [\![\Delta]\!] \cup \langle k_\Phi\colon \Phi\rangle \vdash_{\lambda\mathrm{P2}} N\colon X \tag{6}$$

$$[\![\mathcal{S}]\!] \cup \Gamma_3 \cup [\![\Delta]\!] \cup \langle k_\Psi\colon \Psi\rangle \vdash_{\lambda\mathrm{P2}} P\colon X \tag{7}$$

の 3 つであり，$\Gamma_1, \Gamma_2, \Gamma_3$ は全て変数環境である．

まず，X は論理式なので，適当な変数環境 Γ_4 によって，

$$[\![\mathcal{S}]\!] \cup \Gamma_4 \vdash_{\lambda\mathrm{P2}} X\colon \star$$

が成り立つ．これと式 5 に規則 App を適用して，

$$[\![\mathcal{S}]\!] \cup \Gamma_1 \cup \Gamma_4 \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} MX\colon ((\Phi \to X) \to (\Psi \to X) \to X) \tag{8}$$

を得る．一方，$\Phi \to X$ も論理式だから，ある変数環境 Γ_5 が存在して

$$[\![\mathcal{S}]\!] \cup \Gamma_5 \vdash_{\lambda\mathrm{P2}} (\Phi \to X)\colon \star$$

が成り立つから，これと式 6 に規則 Abs を適用すれば，

$$[\![\mathcal{S}]\!] \cup \Gamma_2 \cup \Gamma_5 \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} (\lambda k_\Phi\colon \Phi.\, N)\colon (\Phi \to X) \tag{9}$$

を得る．同様にして，式 7 から，ある変数環境 Γ_6 が存在して

$$[\![\mathcal{S}]\!] \cup \Gamma_3 \cup \Gamma_6 \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} (\lambda k_\Phi\colon \Psi.\, P)\colon (\Psi \to X) \tag{10}$$

が分かる．したがって，式 8, 9, 10 に規則 App を用いて，

$$[\![\mathcal{S}]\!] \cup \Gamma_7 \cup [\![\Delta]\!] \vdash_{\lambda\mathrm{P2}} (MX(\lambda k_\Phi\colon \Phi.\, N)(\lambda k_\Psi\colon \Psi.\, P))\colon X$$

を得る．ここで，

$$\Gamma_7 = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4 \cup \Gamma_5 \cup \Gamma_6$$

とおいたが，これは変数環境であるから，定理の主張が示された．

二階論理との対応

初めに定義した多類述語論理は，述語に関する量化を許さない一階論理である．しかし，型付け規則 λP2 では，式が示すように型 $\star$ をもつ変項を量化することができる．さらに，

$$\vdash_{\lambda\mathrm{P2}} (\Pi p\colon (\alpha \to \star).\, \Pi x\colon \alpha.\, px)\colon \star$$

のように型 $\alpha \to \star$ の変項を量化することもできる．$\star$ は論理式に対応し，$\alpha \to \star$ は α 上の述語に対応するのだったから，λP2 では論理式や述語に関する量化に相当することが可能なのである．実際，初めに定義した他類述語論理を二階論理に拡張しても，定理 25 と同様の主張が成立することが知られている．

参考文献

[1] H. P. Barendregt (1992)「Lambda calculi with types」『Handbook of Logic in Computer Science』2:117–309
[2] J. R. Hindley, J. P. Seldin (2008)『Lambda-Calculus and Combinators: an Introduction』Cambridge University Press

$\mathcal{S}et$ にはちょうど9つしかモデル構造が入らない話 (小林)

はじめに

「圏」というのは大雑把にいうと頂点がたくさんあるかもしれない, ある条件を満たす有向グラフのようなものです. これは典型的には例えば, ある定義を満たす数学的対象たち一つ一つを頂点として, その構造を保つ写像を矢として構成します. 実はこの簡素な構成からは考えられないほど圏は作る元となった数学的対象らの性質を反映していて, 数学のいたるところで使われています. または圏論によって記述すると, 数学の別々のところに出てくる似た (もしくは同じ) 概念や構成を統一的に理解できることがあるという利点もあります. 詳しくは [Mac lane] を読んでください.

「モデル圏」というのはその圏に多少の付加構造を与えたもので, 例えば代数的トポロジーなどに出てくる (弱) ホモトピー同値性などのような関係性などを汲み取ることが出来ます. 詳しくは [Hovey] などを見てください.

さて本題に入ると, まずMathOverflowでのThomas Goodwillie氏の投稿でこのようなものがありました [Goodwillie].

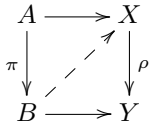
> Among the nine model structures on the category of sets, there are:
> Two in which cofibrant=empty and every set is fibrant.
> Two in which cofibrant=empty and fibrant={empty or singleton}.
> One in which every set is cofibrant and fibrant=nonempty.
> One in which every set is cofibrant and fibrant=singleton.
> One in which every set is cofibrant and fibrant={empty or singleton}.
> Two in which every set is both cofibrant and fibrant.
>
> answered Jun 27 '10 at 0:32 Tom Goodwillie

これを受けてOmar Antoln Camarena氏が自身のブログにて, この事実と実際の9つのmodel structureの分類の証明を書いていらっしゃいました [Camarena]. この記事ではその証明の紹介をしたいと思います. 最初に見るモデル圏の例としてこれが適切かは分からないので, 適切な勉強は各々やってもらうとして, モデル圏の定義を覚えるためのExcerciseとして見てみると良いと思います (この例自体はcofibrant objectとfibrant objectだけではモデル構造が定まらないという例だと思います).

諸定義: lifting propertyとWFSとモデル圏

以下の定義はすべて [Riehl] におよそ準拠しています (言葉を少なくするために多少の同値な言いかえを含みます). また基本的な圏論は行こう仮定します.

Definition 1 (Lifting Property)**.** 圏$\mathcal{C}$の射 $\pi\colon A \to B$, $\rho\colon X \to Y$ の間の *lifting problem* とは以下の図の実線部分からなるような可換図式のことである. これに対し, 点線で記されたような射が全体を可換にするように伸びるとき, この射をこのlifting problemの解と言う. π と ρ の間のすべてのlifting problemに対して解が存在するとき, π は ρ に関して *left lifting property* (以下LLP) を持つと言い, また ρ は π に関して *right lifting property* (以下RLP) を持つと言う. 記号では $\pi \perp \rho$ とここでは表すことにする. (注意:そもそも π と ρ の間にlifting problemが存在しないような場合も例外なく $\pi \perp \rho$ と書く.)



Definition 2 (Weak Factorization System)**.** 圏$\mathcal{C}$の射のクラスの組 $(\mathcal{L}, \mathcal{R})$ が以下の3つの条件を満たすとき, *weak factorization system* (以下WFS) であると言う.

(a) 任意の$\mathcal{C}$の射 f に対して, ある $g \in \mathcal{L}$ と $h \in \mathcal{R}$ が存在して, $f = h \circ g$ を満たす.
(b) $\mathcal{L} = {}^{\perp}\mathcal{R}$ かつ $\mathcal{R} = \mathcal{L}^{\perp}$ を満たす. ただし, 射のクラス $\mathcal{A}$ に対して, ${}^{\perp}\mathcal{A}$ とは $\mathcal{A}$ のすべての要素に対してLLPを持

つ射全体のクラスで, $\mathcal{A}^{\perp}$ とは $\mathcal{A}$ のすべての要素に対して RLP を持つ射全体のクラスのことである.

Definition 3 (モデル圏)**.** 圏 $\mathcal{C}$ の *model structure* とは, wide な (すべての対象を含む) 部分圏 $\mathcal{W}$ と射のクラス $\mathcal{C}$ と $\mathcal{F}$ であって, 以下の条件をみたすもののことを言う.

(1) $\mathcal{W}$ は 2-of-3 property を満たす. すなわち, $f, g, g \circ f \in \mathcal{C}$ のうち 2 つが $\mathcal{W}$ に含まれているとき, もう 1 つも $\mathcal{W}$ に含まれる.
(2) $(\mathcal{C} \cap \mathcal{W}, \mathcal{F})$ と $(\mathcal{C}, \mathcal{F} \cap \mathcal{W})$ は WFS である.

model structure が備わった完備かつ余完備な圏をモデル圏という.
$\mathcal{W}$ に含まれる射を *weak equivalence* と言う.
$\mathcal{C}$ に含まれる射を *cofibration* と言う.
$\mathcal{F}$ に含まれる射を *fibration* と言う.
(注:モデル圏の定義にはいろいろな variant がある.)

$\mathcal{S}et$ にはモデル構造がちょうど 9 つしか入らないこと

以下実際に証明していくので, せっかく圏論的なセッティングをしましたが, これからは対象とは集合であり, 射とは写像です. なので, 素朴な集合と写像の概念が分かっていれば, 読めると思います.

Lemma 4. 下図のような lifting problem が解を持つための必要十分条件は以下の 2 つである:

- すべての $b \in B$ に対して, $\pi^{-1}(b)$ の g での像は一点である.
- すべての $b \in B$ に対して, $\rho^{-1}(f(b)) \neq \emptyset$.

$$\begin{array}{ccc} A & \xrightarrow{g} & X \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \rho} \\ B & \xrightarrow{f} & Y \end{array}$$

Proof. よく見るとそうなっていることが確かめられる. □

Lemma 5. $\pi \perp \rho$ となるのは以下のいずれかのときであり, それに限る:

- $A \neq \emptyset$ かつ $X = \emptyset$.
- π と ρ のどちらか一方が単射 (mono 射) かつ, π と ρ のどちらか一方が全射 (epi 射).

Proof. $A \neq \emptyset = X$ のとき, そもそも π と ρ の間に lifting problem が存在しないので, $\pi \perp \rho$.
π と ρ のどちらか一方が単射かつ, π と ρ のどちらか一方が全射のとき, これらの間の任意の lifting problem が Lemma 4. の条件を満たすことを見れば良い.
逆も少し考えれば分かり, 例えば雰囲気を言うと $\pi^{-1}(b)$ が 2 点以上になる $b \in B$, $\rho^{-1}(y)$ が 2 点以上になる $y \in Y$ があったとすると, b を y に移すような写像を f にとって, g ではそのファイバーの点が分かれるような写像を取れば解が存在しない lifting problem が作れる. しっかりした証明をするにはこのような感じで注意深く場合分けしていけばよい. □

Proposition 6. $\mathcal{S}et$ には WFS が 6 つしか存在しない:
具体的には, $\mathcal{A}$: すべての射の成すクラス, $\mathcal{E}$: すべての全射の成すクラス, $\mathcal{I}$: すべての全単射の成すクラス, $\mathcal{M}$: すべての単射の成すクラス, $\mathcal{N}$: 始域が $\emptyset$ で終域が非空な写像全体の成すクラスとして,

$$(\mathcal{A}, \mathcal{I}), (\mathcal{A} \setminus \mathcal{N}, \mathcal{I} \cup \mathcal{N}), (\mathcal{M}, \mathcal{E}), (\mathcal{E}, \mathcal{M}), (\mathcal{M} \setminus \mathcal{N}, \mathcal{E} \cup \mathcal{N}), (\mathcal{I}, \mathcal{A}).$$

Proof. まず $\pi\colon A \to B$ に対して, $({}^{\perp}(\{\pi\}^{\perp}), \{\pi\}^{\perp})$ を考える. これは構成から明らかに WFS の条件のうち (b)(c) を満たしている. Lemma 5. より $\{\pi\}^{\perp}$ としてあり得るのは以下の 5 通り:

- π が全単射である場合, $\{\pi\}^{\perp} = \mathcal{A}$
- $A = \emptyset$ であって, B が空でない (すると π は単射であって, 全射でない) 場合, $\{\pi\}^{\perp} = \mathcal{E}$.
- $A \neq \emptyset$ で π が単射であって, 全射でない場合, $\{\pi\}^{\perp} = \mathcal{E} \cup \mathcal{N}$.

- π が全射であって, 単射でない場合 $\{\pi\}^{\perp} = \mathcal{M}$.
- π が全射でも単射でもない場合 (単射でないことから $A \neq \emptyset$ が従う), $\{\pi\}^{\perp} = \mathcal{I} \cup \mathcal{N}$.

上のような対応は Lemma 5. を π が各条件を満たすとして適用すればよい. ところで, WFS$(\mathcal{L}, \mathcal{R})$ が与えられたとすると, $\mathcal{R} = \bigcap_{\pi \in \mathcal{L}} \{\pi\}^{\perp}$ なので, 候補としては上に挙がった 5 つとその共通部分のものしか $\mathcal{R}$ には許されておらず, $\mathcal{R}$ が決まれば自動的に $\mathcal{L}$ も決まる.

上の 5 つの射のクラスの共通部分を取っても新しくできるのは $\mathcal{I}$ だけなので, $\mathcal{S}et$ に取れる WFS は高々 6 つであることが分かる. これらについて考えてみると,

${}^{\perp}\mathcal{A} = \mathcal{I}$
(∵Lemma 5. を見ながら考えると, ρ が任意に取れるので, π は全単射で取らないとすべての ρ に対して LLP を持てない.)

${}^{\perp}\mathcal{E} = \mathcal{M}$
(∵同様に Lemma 5. と見比べる)

${}^{\perp}(\mathcal{E} \cup \mathcal{N}) = \mathcal{M} \setminus \mathcal{N}$
(∵$\mathcal{E}$ の元に対して LLP を持つのは $\mathcal{M}$ の元であることが必要で, $\mathcal{N}$ の元に対して LLP を持つためには始域が $\emptyset$ でないか, 始域も終域も $\emptyset$ である必要があり, 逆に $\mathcal{M} \setminus \mathcal{N}$ の元であれば LLP を持つことも見れば分かる.)

${}^{\perp}\mathcal{M} = \mathcal{E}$
(∵これは 2 番目の場合と同様)

${}^{\perp}(\mathcal{I} \cup \mathcal{N}) = \mathcal{A} \setminus \mathcal{N}$
(∵これも 3 番目の場合と同様)

${}^{\perp}\mathcal{I} = \mathcal{A}$
(∵ 1 番目と同様)

以上の議論より 6 つの候補 $(\mathcal{I}, \mathcal{A}), (\mathcal{M}, \mathcal{E}), (\mathcal{M} \setminus \mathcal{N}, \mathcal{E} \cup \mathcal{N}), (\mathcal{E}, \mathcal{M}), (\mathcal{A} \setminus \mathcal{N}, \mathcal{I} \cup \mathcal{N}), (\mathcal{A}, \mathcal{I})$ が出てきたが, これらはいずれも WFS の条件の (a) を満たすことが確認できる. □

Theorem 7. 集合の成す圏 $\mathcal{S}et$ に入る model structure はちょうど 9 つである.

Proof. モデル圏は $(\mathcal{C} \cap \mathcal{W}, \mathcal{F})$ と $(\mathcal{C}, \mathcal{F} \cap \mathcal{W})$ の 2 つの WFS を持つわけであるが, $\mathcal{F}$ と $\mathcal{F} \cap \mathcal{W}$ の包含関係で場合分けして考える.

まず $\mathcal{F} = \mathcal{F} \cap \mathcal{W}$ の場合, 同時に $\mathcal{C} \cap \mathcal{W} = \mathcal{C}$ も成り立つことになる. すなわち, $\mathcal{W} \supseteq \mathcal{C} \cup \mathcal{F}$ ということになるが, $\mathcal{S}et$ 内のどの WFS に関してもこれを満たし, かつ 2-of-3 property を満たすような部分圏 $\mathcal{W}$ は $\mathcal{A}$ だけしかない. 逆に 6 つの WFS 各々に対して, WFS を $(\mathcal{L}, \mathcal{R})$ とすると, $\mathcal{W} = \mathcal{A}, \mathcal{C} = \mathcal{L}, \mathcal{F} = \mathcal{R}$ は model structure を定めることが分かる ($(\mathcal{C} \cap \mathcal{W}, \mathcal{F})$ と $(\mathcal{C}, \mathcal{F} \cap \mathcal{W})$ が WFS になるのは作り方から明らかで, $\mathcal{A}$ はすべての射からなるので自明に 2-of-3 property を満たす). これで 6 つ出来た.

次に $\mathcal{F} \supsetneq \mathcal{F} \cap \mathcal{W}$ の場合を考える. WFS は前に挙げた 6 つしかないので, 組み合わせは有限通りしかなく, 総当たりすることであり得る $(\mathcal{C} \cap \mathcal{W}, \mathcal{F})$ と $(\mathcal{C}, \mathcal{F} \cap \mathcal{W})$ の組で $\mathcal{F} \supsetneq \mathcal{F} \cap \mathcal{W}$ を満たす組が分かる. ところで以下の主張が成り立つ.

Lemma 8. $\mathcal{W}, \mathcal{C}, \mathcal{F}$ が model structure を与えるとき, $\mathcal{W}$ は $\mathcal{W} = (\mathcal{F} \cap \mathcal{W}) \circ (\mathcal{C} \cap \mathcal{W})$ で求められる.

Proof. $\mathcal{W}$ の 2-of-3 property より, $\mathcal{W}$ に含まれる射の合成はまた $\mathcal{W}$ に含まれる. よって, 右辺が左辺に含まれることは分かる. 逆に任意の $\mathcal{W}$ の射を取ってくると, それは $(\mathcal{C} \cap \mathcal{W}, \mathcal{F})$ が WFS である仮定より, $\mathcal{C} \cap \mathcal{W}$ の射 f と $\mathcal{F}$ の射 g の合成 $g \circ f$ で表せる. $f, g \circ f \in \mathcal{W}$ より, $\mathcal{W}$ の 2-of-3 property を使うと $g \in \mathcal{W}$ が言える. よって, $g \in \mathcal{F} \cap \mathcal{W}$. □

この Lemma より, $(\mathcal{C} \cap \mathcal{W}, \mathcal{F})$ と $(\mathcal{C}, \mathcal{F} \cap \mathcal{W})$ の候補となる組に対して, $\mathcal{W}$ の候補を $(\mathcal{F} \cap \mathcal{W}) \circ (\mathcal{C} \cap \mathcal{W})$ として計算して, それらがちゃんと model structure を与えるかどうかを調べればよい.

- $(\mathcal{C} \cap \mathcal{W}, \mathcal{F}) = (\mathcal{I}, \mathcal{A})$ の場合, $\mathcal{W} = (\mathcal{F} \cap \mathcal{W}) \circ (\mathcal{C} \cap \mathcal{W}) = \mathcal{F} \cap \mathcal{W}$ となるが, $\mathcal{F} \cap \mathcal{W}$ が 2-of-3 property を満たすような組は $(\mathcal{A}, \mathcal{I})$ しかなく, この場合は $\mathcal{C} = \mathcal{A}, \mathcal{F} = \mathcal{A}, \mathcal{W} = \mathcal{I}$ が model structure を与えているのでこれが 7 つめ.
- $(\mathcal{C} \cap \mathcal{W}, \mathcal{F}) = (\mathcal{M} \setminus \mathcal{N}, \mathcal{E} \cup \mathcal{N})$ の場合, $(\mathcal{C}, \mathcal{F} \cap \mathcal{W})$ の候補は $(\mathcal{M}, \mathcal{E}), (\mathcal{A} \setminus \mathcal{N}, \mathcal{I} \cup \mathcal{N}), (\mathcal{A}, \mathcal{I})$ の 3 つだが, $(\mathcal{F} \cap \mathcal{W}) \circ (\mathcal{C} \cap \mathcal{W})$ で 2-of-3 property を満たすのは $(\mathcal{M}, \mathcal{E})$ だけで $\mathcal{W} = (\mathcal{F} \cap \mathcal{W}) \circ (\mathcal{C} \cap \mathcal{W}) = \mathcal{E} \circ (\mathcal{M} \setminus \mathcal{N}) = \mathcal{A} \setminus \mathcal{N}$. $\mathcal{C} = \mathcal{M}, \mathcal{F} = \mathcal{E} \cup \mathcal{N}$ と定めると, $\mathcal{C} \cap \mathcal{W} = \mathcal{M} \setminus \mathcal{N}, \mathcal{F} \cap \mathcal{W} = \mathcal{E}$ となるので, これは model structure を定めることが分かる. これが 8 つめ.

- $(\mathcal{C}\cap\mathcal{W},\mathcal{F})=(\mathcal{E},\mathcal{M})$ の場合, $(\mathcal{C},\mathcal{F}\cap\mathcal{W})$ の候補は $(\mathcal{A}\setminus\mathcal{N},\mathcal{I}\cup\mathcal{N}),(\mathcal{A},\mathcal{I})$ の 2 つ. これらも一つ一つ見れば駄目なことが分かる.
- $(\mathcal{C}\cap\mathcal{W},\mathcal{F})=(\mathcal{M},\mathcal{E})$ の場合, $(\mathcal{C},\mathcal{F}\cap\mathcal{W})$ の候補は $(\mathcal{A},\mathcal{I})$ のみ. $(\mathcal{F}\cap\mathcal{W})\circ(\mathcal{C}\cap\mathcal{W})=\mathcal{I}\circ\mathcal{M}=\mathcal{M}$ とするとこれは 2-of-3 property を満たさないので駄目.
- $(\mathcal{C}\cap\mathcal{W},\mathcal{F})=(\mathcal{A}\setminus\mathcal{N},\mathcal{I}\cup\mathcal{N})$ の場合, $(\mathcal{C},\mathcal{F}\cap\mathcal{W})$ の候補は $(\mathcal{A},\mathcal{I})$ のみ. $(\mathcal{F}\cap\mathcal{W})\circ(\mathcal{C}\cap\mathcal{W})=\mathcal{I}\circ(\mathcal{A}\setminus\mathcal{N})=\mathcal{A}\setminus\mathcal{N}$ であり, これは 2-of-3 property を満たし, $\mathcal{A}\cap(\mathcal{A}\setminus\mathcal{N})=\mathcal{A}\setminus\mathcal{N},(\mathcal{I}\cup\mathcal{N})\cap(\mathcal{A}\setminus\mathcal{N})=\mathcal{I}$ となる. $\mathcal{C}=\mathcal{A},\mathcal{F}=(\mathcal{I}\cup\mathcal{N}),\mathcal{W}=\mathcal{A}\setminus\mathcal{N}$ とするとこれは model structure を定めていることが分かる. これで 9 つ.
- $(\mathcal{C}\cap\mathcal{W},\mathcal{F})=(\mathcal{A},\mathcal{I})$ の場合, そもそも $\mathcal{R}\subsetneq\mathcal{I}$ となる WFS$(\mathcal{L},\mathcal{R})$ は存在しないので, こうなるような model structure も存在ない.

9 つの model structure が見つかり, これ以外にはないことが以上の注意深い場合分けによって分かる. □

9 つの model structure を表にまとめるとこうなる.

表 7.1　$\mathcal{S}et$ に入る model structure 一覧

$\mathcal{C}$	$\mathcal{F}$	$\mathcal{W}$
$\mathcal{I}$	$\mathcal{A}$	$\mathcal{A}$
$\mathcal{M}\setminus\mathcal{N}$	$\mathcal{E}\cup\mathcal{N}$	$\mathcal{A}$
$\mathcal{E}$	$\mathcal{M}$	$\mathcal{A}$
$\mathcal{M}$	$\mathcal{E}$	$\mathcal{A}$
$\mathcal{A}\setminus\mathcal{N}$	$\mathcal{I}\cup\mathcal{N}$	$\mathcal{A}$
$\mathcal{A}$	$\mathcal{I}$	$\mathcal{A}$
$\mathcal{M}$	$\mathcal{E}\cup\mathcal{N}$	$\mathcal{A}\setminus\mathcal{N}$
$\mathcal{A}$	$\mathcal{I}\cup\mathcal{N}$	$\mathcal{A}\setminus\mathcal{N}$
$\mathcal{A}$	$\mathcal{A}$	$\mathcal{I}$

参考文献

[MacLane]　Saunders Mac Lane. *Categories for the working mathmatician, volume 5 of Graduate Texts in Mathmatics.* Springer-Verlag, New York, 1998.

[Hovey]　Mark Hovey. *Model categories, volume 63 of Mathmatical Surveys and Monographs.* American Mathmatical Society, Providence, RI, 1999.

[Goodwillie]　Thomas Googwillie の Mathoverflow への投稿. `https://mathoverflow.net/a/29653`

[Camarena]　Omar Antoln Camarena. *The nine model category structures on the category of sets.* Omar Antoln Camarena 氏のホームページより

[Riehl]　Emily Riehl. *Categorical Homotopy Theory, volume 24 of New Mathmatical Monographs.* Cambridge University Press, 2014.

三平方の定理はいつ生まれたか (高木)

直角三角形の三平方の定理 (あるいはピュタゴラスの定理) は，数学を勉強する際に最も序盤に出会う最も美しい定理の一つです．この定理と証明は，紀元前 3 世紀ごろにユークリッドによって書かれた数学書『原論』第 1 巻命題 47 に出てきます．

実は，この三平方の定理が，いつ，誰によって見つけられたかということは，数学史の大きな未解決問題の一つです．本記事では，この定理にまつわる様々な説や謎のうちの一部を紹介したいと思います．

三平方の定理と古代エジプト

ギリシア人は自分達の数学がエジプトから来たものだと思っていたようです．実際，巨大なピラミッド，年に 1 度の洪水のために高度に発達した測量術などがエジプト人の高度な学問水準に支えられていたことは疑いようもありません．しかしエジプトには定理の概念はありませんでしたから [1]，三平方の定理がそのままの形で知られていたと考えるには無理があります．

ただ，具体的な直角三角形についてなら彼らは三平方の定理を知っていた可能性があります．ドイツの数学史家 M. カントルは「縄張り師」と呼ばれる役職が神殿の建立に関わっていることから，エジプト人は三辺の長さが 3,4,5 の三角形を知っていて，縄でこれを作ることで直角を作っていたのではないかという説を出しました．この説はかなり一人歩きをしていて，エジプト人は三辺の長さが 3,4,5 の三角形を知っているということを書いてある本やネットの記事はよく目にします．しかし，実際にエジプト人がこの直角三角形を知っていたという証拠は今のところ無いようです．

三平方の定理と古代バビロニア

バビロニアとは，現在のイラク辺りをを指します．バビロニアでは，エジプトと同じくらい (あるいはそれ以上に) 数学が栄えていました．

バビロニアの数学もエジプトと同じく，定理証明の形式ではありませんでしたから，三平方の定理がそのまま出てくることはありません．しかし，バビロニアの時代に既に三平方の定理が知られていたという説を主張する人は結構います [2]．実際，粘土板に出てくる問題や解法には，解答には直接関係ないが出てくる図形が三辺 5,12,13 の直角三角形だったり，計算の課程で三平方の定理が使われているように見えるところがあったりします．

とりわけその説を大きく広めたのは，バビロニア数学史研究の鏑矢的存在であるノイゲバウアーが 1950 年代に出した『プリンプトン 322』の解釈です．『プリンプトン 322』には文章がついておらず，ただ数が並べられて表になっています [3]．この数表がどうやって作られたのかを一目で見極めるのは難しいのですが，ノイゲバウアーはこれをうまく解釈して，これはピュタゴラス数 [4] を表しているのだという説を提示しました．およそ半世紀ほどの間，この説が正しく，バビロニア人は三平方の定理を知っていたのだということが通説になっていましたが，この数表をバビロニア人が 2 次方程式を解くときに使う公式から解釈する説もあり，現在はこちらが有力なようです．

実は，バビロニアに三平方の定理の起源を探ろうとするときの最大の困難がここにあります．バビロニアの数学専門家は，恒等式

$$xy + \left(\frac{x-y}{2}\right)^2 = \left(\frac{x+y}{2}\right)^2 \tag{1}$$

をよく知っていて，2 次方程式を解くときによく使っていました．ところがこれは xy が何かの数の 2 乗になったとき，三平方の式 $a^2 + b^2 = c^2$ に他なりません．特に数だけが出てくる粘土板の場合だと，どっちのことを言っているのかはっきりしないのです [5]．

---

[1] エジプトの数学を伝える『リンド・パピルス』『モスクワ・パピルス』(どちらも紀元前 18 世紀から 16 世紀ごろ) では，賃金の分配や土地の面積の計算などの実際的な問題とその解答が書いてあります．

[2] 例えば [2] 中村滋・室井和男（2014） 『数学史　数学 5000 年の歩み』 共立出版.

[3] 実際がどんな感じか知りたい方は検索してみてください

[4] $a^2 + b^2 = c^2$ を満たす 3 数 (a, b, c) のこと

[5] 一方エジプトではこの公式は出て来ず，2 次方程式も簡単なものしか解けていないようです．

三平方の定理とピュタゴラス

私が中学生の時の数学の教科書には，ピュタゴラスが直角二等辺三角形が敷き詰められた模様を見たときに，この定理に気づいたというような説明が書いてあった記憶があります．他にも，ピュタゴラスがエジプト人やバビロニア人から数学を教えてもらっているときにこの定理に気づいたなど，この手の話はたくさんあります．ピュタゴラスが三平方の定理を見つけたとき，感動のあまりこの感謝の意を神々に示そうと犠牲を行ったそうなのですが，この犠牲は牛を 1 頭だったり，100 だったり，小麦粉で作られた牛[6] だったりはっきりしません．

ピュタゴラスはサモス出身の人で，紀元前 6 世紀ごろに活躍しました．現代の私達が直接アクセスできるピュタゴラスの生涯や業績に関する言い伝えのほとんどはディオゲネス，ポリュピュリオス，イアンブリコス，プロクロス達の記述に依っています．彼らは全員紀元後の人達であり，特に後ろの 3 人は学派的にピュタゴラスびいきなため，彼らの話をそのまま鵜呑みにはできません[7]．

ピュタゴラスは，そのおよそ 200 年後を生きたプラトンやアリストテレス達にとっても既に謎の人物だったようです．彼らも，三平方の定理を示したのがピュタゴラスだと思っていたようで，実に 2300 年に渡ってこの定理はピュタゴラスのものだと思われていたのでした．この説への批判もあるにはあったのですが，それが決定的なものになったのは，1962 年のブルケルトによる批判で，これ以降ピュタゴラスは天才数学者としてよりも天才宗教家として書かれることが多くなっています．三平方の定理を証明したのがピュタゴラスだという説も，論証的数学 (つまり定義定理証明の形式) の成立が紀元前 5 世紀という説が有力になって来たため，あまり積極的には受け入れられてません．

個人的には，ピュタゴラスの数学への内容的な貢献が少ないとしても，ピュタゴラスは数学の進歩への偉大な功労者であるように思います．ピュタゴラスの教義を極めておおざっぱにいうと「数学的な知識を得ることで精神が昇華されるよ」というようなものです．例えば，現代では数学科なんかにいたりすると「どうして数学を勉強するのか？」というような疑問にぶつかったりぶつけられたりすることがあります．ピュタゴラスの信徒は少なくともこういう疑念に悩まされる必要は無かったわけです．三平方の定理を最初に厳密に証明したのがピュタゴラスで無いにしても，ピュタゴラスの死後分裂したピュタゴラス派の誰かである可能性が高いです．

三平方の定理と無理数

現代に生きる私達にとって，三平方の定理から無理数の発見までは即時であるように思えます．直角二等辺三角形，正三角形を二等分したときに出て来る三角形などの重要な直角三角形が三辺の比に無理数を含むからです．三平方の定理の発見を早め早めにしようとする説の多くは，この考えとの両立の困難に苦しめられます．三平方の定理を知っていたのに，どうして無理数については何も知らないふうなのかと．

無理数について私達が遡ることができるのは，プラトンの対話篇『テアイテトス』までです．これが書かれたのは紀元前 360 年代，作中の年代は紀元前 420 年ごろとなっています．プラトンがもし嘘をついていないのであれば[8]，テアイテトスはこのころにいわゆる可術[9] な無理数を扱えるようになっていたということになります．この時のテアイテトスの語り方によると，彼がこの考えに気づくまでの無理数の理解はかなり未熟であったようです．そうだとすると，三平方の定理がピュタゴラスの時代に見つかっていたのに無理数の理解がそこまでしか進んでいないのは不思議だという考えが生まれます．この考えに従えば，三平方の定理の発見は早くとも紀元前 5 世紀ということになります．

参考文献

[1]　佐々木力（2010）『数学史』岩波書店.
[2]　中村滋・室井和男（2014）『数学史　数学 5000 年の歩み』共立出版.
[3]　斎藤憲（2008）『ユークリッド『原論』とは何か』岩波書店.
[4]　斎藤憲（1997）『ユークリッド『原論』の成立』東京大学出版会.
[5]　ヴァン・デル・ウァルデン (1984)『数学の黎明　オリエントからギリシアへ』村田全・佐藤勝造訳，みすず書房.
[6]　カジョリ (1997)『復刻版　初等数学史』小倉金之助訳，共立出版.
[7]　ポルピュリオス『ピタゴラスの生涯』水地宗明訳，晃洋書房.

---

[6] [7] ピュタゴラスは不殺生主義者だったので生き物を犠牲に奉げることはことは無いという解釈がねじれてこのような記述が出て来たのだと思われますが，そもそもピュタゴラスが不殺生主義なのは人間の魂が生まれ変わる中で動物の中に宿っている可能性があるからであり，犠牲獣はこの輪廻から外れているため殺してもよいという解釈もあります．つまりよくわかりません．

[7] ちょうどこの記事のようなものです.

[8] プラトンの作品には，既に死んでいるはずの時代にソクラテスが登場するものもある (『メネクセノス』) ので，過信は禁物です

[9] [4] 2 乗すると有理数になる無理数のこと．有理数面積の正方形の一辺の長さとして表せるからこの名前がつけられたのでしょうか.

[8]　プラトン『テアイテトス』田中美知太郎訳，岩波文庫.

いかにして数学を説くか (柳川)

はじめに

みなさんは数学を勉強されたことがあるでしょうか。この本を読んでくださっている方は数学になかなかの興味を持っていらっしゃるかもしれません。しかし、この記事では数学が苦手な人，得意な人，好きではあるけどテストではそんなに点数が高くない人など数学に触れたことのある方全員に読んでもらえるといいなと思っています。

この記事のテーマは，数学を学ぶ際に「分からない！」という気持ちになったときどう対処しようか、という点です。後ほど具体例を出しますが，数学には学習者がもやもやする部分がたくさんあります。数学という学問自体はもやもやをすべて取り除いて築き上げられているはずなのにこのような事態に陥るのはなぜでしょうか。一つの答えとして，次のようなものが考えられるでしょう。「数学は，結局何がしたいのかがよく分からない。」筆者自身も頻繁に感じていました。結局のところ，数学を理解する工夫を自ら試行錯誤するほかないのですが，その試行錯誤を少しでも読者の方に共有して頂き，数学の学びの足を引っ張るものを取り除けたらなと思っています。

実はもう一つテーマがあり，それは「数学に関する質問をされたとき望まれる対応」です。筆者には文学部の弟がいますが，その弟が大学受験の際ちょくちょく質問をしてくれました。それは数学に限ったことではなく，英語や古文，化学も多かったのですが，その時に感じたのは「質問者の視点と回答者の視点がそろわないと本当の解決にはならない」ということです。大事なことは，質問者の視点を想像するということであって，数学的に正しいことを述べ続ければいいというものではありません。この「視点の揃え方」が上手くいけば，数学を他者と共有するという喜びが生まれます。「分からない」というもやもやをもった人と，数学について話し合い，「なるほど！」と本心からいってもらえればこれほど嬉しいことはありません。ですから個人的には，数学が得意な人には「数学を人に教えるのが上手な人」になってほしいと思っています。そうなれば，世界が少しだけ平和になる気がします。

数学でつまずくところ

ここでは，筆者の経験から，数学でもやもやしたことのある具体例をいくつか挙げてみようと思います。数学といいつつ算数も入っていますが似たようなものですのでお気になさらないようお願いします。

分数

小学校で次のような計算を習うでしょう。

$$12 \div 3 = 4$$

この計算は日本語で解釈することができ，「12 個の石を 3 個ずつに分けると 4 グループできる」もしくは「12 個の石を 3 人の子どもに均等に分けると 4 個ずつになる」となります。一方で

$$2 \div \frac{3}{5} = \frac{10}{3}$$

という計算を日本語で解釈しようとしても「2 個の石を 5 分の 3 個ずつ (?) 分けると 3 分の 10 グループになる (? ?)」となってしまって意味が通りません。

もう一つ似た例を挙げましょう。中学校で

$$x^3 = x \times x \times x$$

という表記法を習います。これが高校になると

$$x^{\frac{2}{3}} = (x \text{ を } 3 \text{ 分の } 2 \text{ 回かけたもの } (?))$$

という怪しげなものに進化して，数学が分からないという気持ちを生むきっかけになっている気がします。

なぜもやもやするのかというと，「個」や「回数」といった，物事を数えるのに使う単位と，分数との相性がよろしくないからなのです。もっと言えば，日本語にすると変なことになる概念に対してもやもやするのです。

数学でよく出てくる文字

なぜ数学では x とか y とか θ とかがよく出てくるのでしょう。この手のいわゆる「数学の文化，慣習」に関する疑問も多いと思います。

高校数学と大学数学のギャップ

大学に入って数学が途端に分からなくなる瞬間というものがあります。大学数学の有名な障害物としては $\varepsilon - \delta$ 論法が挙げられるでしょう。「極限（limit）」を厳密に論じるために必要だと説明されると思いますが，習いたての頃はそんなことをする必要性がどこにあるのかという疑問が浮かび続けていたと思います。

大学数学では，必要とされる論理の厳密性が高校数学よりも格段に上昇します。そこに戸惑いを覚えるのだと思います。

日本語と思えない日本語

中学校辺りから関数，方程式という用語が登場します。高校では指数，対数や実数，複素数など。さらに大学では写像，全単射，基底，一次独立，n 回連続微分可能などなど。漢字で書いてはあるけど何も頭に入ってこない専門用語の洪水です。その言葉の意味が分からないまま授業に置いて行かれるなんてことも多いと思います。

(少し蛇足ですが, 大学 3,4 年生の数学を勉強していると mod や homo から始まる用語が多く登場します。module(加群), modulo(〜を法として), moduli(モジュライ), homotopy(ホモトピー), homology(ホモロジー), homogeneous(同次の) などです。もはや日本語訳が作られていないものも多いのですが，これらの言葉が使用されている意図を理解するのは容易ではないと感じています。)

数学の本は行ったり来たりが激しい

数学書を読もうとするとき，「この言葉はどういう意味だったっけ？」と数ページ前に戻り確認する，という作業がとても多く発生します。正直めんどくさくなってやる気がなくなったりした経験はありませんか。

分からない時の気持ち

では，数学でもやもやしたときの原因を突き詰めてみましょう。そして，そのもやもやにどう立ち向かえばいいのかを考えてみたいと思います。

概念の拡張に出会った瞬間

先ほど分数の例を出しました。ここには，新しい数を作るという「拡張」を受け入れられるかどうかという問題が絡んでいます。分数を習うまではほとんど自然数 (0,1,2,3,...) の世界で考えていたのに，3 を 5 で割るという自然数だけでは表せない概念を考えようとしているわけです。そこで，

$$3 \div 5$$

の答え，つまり「5 を掛けたら 3 になる数」を

$$\frac{3}{5}$$

と表すことにした，即ち「定義した」のです。自然数の世界から分数の世界に拡がったことが分かるでしょうか。同様に，「3 回掛けると x^2 になる数」を

$$x^{\frac{2}{3}}$$

と表すことにしたのです。指数 (右肩に乗った小さい数字のこと) のところに自然数のみならず分数も使えるように世界が拡がっています。初めて習う時もこのように教わるはずですが，「なぜかわかった気にならない」のはなぜなのでしょう。

それは，それまでの自分の理解の仕方では解釈できないものに出会い，新しい理解の仕方が求められているからです。これが，「日本語の解釈では上手くいかないのでよく分からない」という気持ちの正体です。ではどう対処するかというと，筆者にもよく分かりません。ただ一つ言えるのは，新しい概念に出会ったときにもやもやするのは至極当然であって，あなたが悪いわけでは決してないということです。おそらく，「このような理解の仕方があるのだな」ととりあえず受け入れてみて，しばらく時間をおいてみると，いつの間にか自然なもののように思えてくるのだと思います。(マイナスがついた数もいつの間にか受け入れていたでしょう？)

そもそもなぜこんなものを考えるのか？

分数の例で「概念の拡張」の例を挙げましたが，もう一つの顕著な例が実数から複素数への拡張です。

$$2\text{乗して}-1\text{になる数を}i\text{とする}$$

という文面を見たとき，「そんな数はないと思っていたのに急に何を言い出したんだ？」と思いませんでしたか。その後「a, bを実数とするとき$a+bi$を複素数と呼ぶ」と習って，複素数の足し算，掛け算を学びます。この頃に「なぜこんなものを考え始めたんだ」と悩む人が多いと想像します。

このようなもやもやは，何かを定義したときによく発生します。そしてこのもやもやが晴れるのは結構時間が経ってからであることが往々にしてあります。複素数の例でいうと，

$$2\text{次方程式は，複素数の範囲では必ず}2\text{個の解を持つ}$$

という定理を聞いたり，

$$e^{i\theta} = \cos\theta + i\sin\theta$$

という式を見たりした後に，どうやら複素数というものは役に立つものであるらしい，となんとなく思い始めるかもしれません。筆者の場合は，高校物理で学ぶ交流回路の電流，電圧の式が複素数を用いるととても簡単に書けることに驚いて複素数の有用性を初めて実感した覚えがあります。

概念を拡張するときのみならず，新しい定義に出会うときは「なぜこんなものを考えるのだろう」というもやもやが付きまといます。その時はぜひ，そのもやもやを大事に取っておいたまま勉強を進めてほしいと思います。学び始めの頃はイメージが湧きにくく自分が何をやっているのか分からなくなることもあると思いますが，その先に待つ応用を楽しみにして頑張るのが良いのではないでしょうか。

もう一つ役に立つ解決策は，「他の人に聞く」ことです。返ってくる答えの大半は理解出来ず，どうやらすごいものらしいなあくらいの感想になってしまうのですが，たまに雷に打たれたように腑に落ちることがあります。

なぜその文字を使うのか？

学問にはその学問特有の文化，慣習というものがあり，数学にも当てはまります。その具体例を，第2章で挙げたものよりも詳しく見てみましょう。

中学校で (現在は小学校でも？) 次のような1次方程式を習います。

$$2x + 3 = x - 1,$$
$$x = -4.$$

その時未知数は大抵xです。なぜ，他の文字や記号ではなくxなのでしょう。実はこれは数学史の話題でして，誰も確たる答えを持っていません。少し調べてみると，アラビア起源説やデカルト起源説などたくさん出てきます。デカルトとは「我思う，故に我あり」で有名な人ですが，彼の著作にxが出てくるのが現存する最古のxらしいです。というわけで，「xを使うのはそういう文化なんだな」と諦めて受け入れてもらうほかありません。そして，xの他にも未知数が出てくるときは，xの次のアルファベットであるyを使うわけです。さらに未知数があればzを使うことが多いです。でもzより後のアルファベットはないのだから，4つ目の未知数が出てきたらどうするのでしょう。いちばん多いのはwです (筆者はこれを見てずるいと思いました)。ただ，5つ以上になるとx_1, x_2, x_3, x_4, x_5のように右下に添え字を付けてしまいます。そういう文化なのです。

この「諦めて受け入れる」という解決策は (十分悩んだ後ならば) そこそこ有用です。なぜその記号を使うのか，という疑問は次のような記号に対してもよく向けられるでしょう。

$$\sin \quad \cos \quad \tan \quad \sum \quad \int$$

このような記号の起源を調べてみて下さい。「なあんだ割と適当なんだな」と思えるでしょう。そのうえで文化として受け入れてもらうのがいいと思います。

他には，

$$\text{点}\,P, \quad \text{関数}\,y = f(x), \quad \text{半径}\,r, \quad \text{曲線}\,C$$

という記号の割り当ても数学ではよく見ます。これらは対応する英単語の頭文字が使われている例です (点は point，関数は function，半径は radius，曲線は curve)。物理学でも時刻t，速度v，加速度a，力Fなどたくさん出てきますので調べてみてください。

繰り返しになりますが，この「なぜこの記号を使うのか」という疑問は大切に持ち続けて下さい。そのうちその記号の生みの親の気持ちが分かるかもしれません。一度，「等しい」という意味の記号である

$$=$$

の気持ちを考えてみてはどうでしょうか。

「証明」について

記号や文字以外にも数学特有の文化はたくさんあります。いちばん顕著なのは「証明する」という文化でしょう。他の学問は，程度の差はあれど「うまい説明方法，解釈を生み出す」という目的があります。例えば物理学では物理現象をうまく「説明できる」法則を探りますし，心理学では人心の動きをうまく「説明できる」因果関係を見出そうとします。その点，数学は「説明」では飽き足らず，「証明」してしまおうというのです。「説明」と「証明」の違いを見てみましょう。次の主張 (数学では “命題” と呼ばれます) とその証明を見て下さい。(証明の途中で「$\therefore$」という記号が出てきますが，これは「従って (therefore)」という意味の記号です。)

命題 1. *a, b を 0 より大きい実数とする。$a^2 = b^2$ が成り立っているならば，$a = b$ が成り立つ。*

(証明)

$$a^2 = b^2$$

が成り立っているとする。両辺に $-b^2$ を加えると

$$a^2 + (-b^2) = b^2 + (-b^2),$$
$$\therefore \quad a^2 - b^2 = 0$$

となる。左辺を因数分解すると

$$(a - b)(a + b) = 0$$

となる。2 つの実数 $(a - b)$ と $(a + b)$ をかけて 0 になっているから，少なくとも片方は 0 と等しいので

$$a - b = 0 \quad \text{または} \quad a + b = 0$$

が成り立つ。従って，少し変形すると

$$a = b \quad \text{または} \quad a = -b$$

が成り立つことが分かる。今，a, b はともに 0 より大きい実数なので，$a = -b$ とはなり得ない。従って

$$a = b$$

が成り立つ。(証明おわり)

一方，この命題がなぜ成り立つかを「説明」しようとすると，例えば次のようになるでしょう。

面積が等しい 2 つの正方形の，それぞれの 1 辺の長さは等しい。

2 つを見比べてどう感じられましたか。この例だと「説明」の方がよっぽど分かりやすいと思われたかもしれません。ですが，2 つの長方形の面積が等しいからと言ってそれぞれの 2 辺の長さが等しいわけではないことを考えると，「説明」の方は正しいと確信するに足る根拠を人の直感に委ねていることが感じられませんか。

このように，数学における証明は必ずしも直感的に理解しやすいものではない代わりに，人の勝手なイメージに左右されない厳密な論理で構成されます。数学を勉強する際，この証明の内容が分からなくて辛くなってくることが大変多いと思います。そんな時はいったん深呼吸をして，証明のステップ 1 つ 1 つを自分の手で確かめながら進んでみましょう。ここに時間がかかるのは当然，というよりはむしろここに時間をかけるのが数学の勉強のようなものです。1 回の試みで分からなくても大丈夫です。大抵は 3 回ほどアタックしてみてからじわじわ分かってくるものなのです。ここで必要なのは諦めない気持ちなので，どうかじっくり取り組んでほしいと思います。大学数学の関門である $\varepsilon - \delta$ 論法も，じっくり腰を落ち着けて向かい合ってみれば，希望が見えてくるはずです。3 回ほどアタックしても厳しいときは，人に頼るのもよい選択肢です。

数学の用語について

数学には，日常でも使う言葉が数学用語になっていたり，逆に日常では使わないような単語が使用されていたりします。例えば，「連続」という言葉は「3 試合連続ホームラン」などでも使いますが，「関数が連続である」，という風に数学でも使います。一方で，「3 と 5 は互いに素である」とか「2 と 14 は 12 を法として合同である」などのような，日常では聞くことの無い日本語が使われます。(個人的に，このような謎の数学用語の極め付けだと思うのは「環」です。) やはり，使い慣れない言葉を用いて勉強を進めるのは骨が折れます。このような時はどうすればいいのでしょうか。

一つの解決策は，「言葉を使い慣れる」ことです。そのための秘訣は，見慣れない言葉に出会ったとき，もしくはよく意味を覚えていない単語に出会ったときの対応にあります。数学書には，初めて使う用語に対してはちゃんと「定義」がしてあるはずなので，それをノートに書き写します。そして，その単語が出たときには，いったん自力で定義が思い出せるか確認してみて，よく分からなければ (本を戻るのではなく) ノートを参照するようにして見て下さい。すると，何回か繰り返しているうちに単語の意味がしみ込んでくるでしょう。

英単語を覚えるときも，毎回意味が思い出せるか確認していたと思います。同じように，数学用語を見たときには毎回定義が思い出せるかをチェックしてみてください。同じ本を行ったり来たりするのは面倒なので，別のノートに書き出して参照できるようにしておくのです。コツは，本に出てくる順番通りにきれいにノートにまとめようと思ったりせずに，疑問に思った順にドカドカノートに書き込んでいくことです。最初の内は，ある単語の定義に別の数学用語が含まれていたりして芋づる式に単語を調べる羽目になると思いますが，そこを乗り越えればあなたの数学力はぐんぐん上昇するでしょう。

自分が何をやっているのか分からない

「何を計算しているんだこれは？」という状態になることがよくあります。その時は，何が与えられていて，何を知りたいのかを紙に書き出してみるのがいいと思います。「図形が与えられていて，○○の長さを知りたい」「式が与えられていて，□□の最大値を求めたい」など，最初は大雑把でもよいので目的意識をはっきりさせてみるとよいでしょう。授業中であれば，先生に「今，何から出発して何をしようとしているんですか」と直接聞くのがよい方法です (この質問はできるだけ早い方がよい)。数学の授業は (特に大学では) 伏線を開けっ広げにしてある推理小説のようなものですから，「この伏線は将来どう使われるのか」という質問は内容理解にとても役立つはずです。

「そもそもなぜ数学を勉強するんだ？」という疑問が頭から離れないときはいったん机から離れましょう。この疑問に対する筆者なりの答えはこの記事の最後に回してあります。

何が分かっていないのかが分からない

「なんとなく納得していないんだけど，何が分かっていないのかうまく説明できない」という状態になることはとても多いでしょう。そんな時は他の人に「分かっていない気がするところがあるから少し話を聞いてほしい」と頼んで静かに話を聞いてもらうのが吉です。その時大切なのは，とりあえず自分が考えているところまでしどろもどろでもいいので話し切ることです。その後に質疑応答を行い，勘違いを正したり，自分の理解と不理解の境界線を探りましょう。この状況で聞き手側に求められる姿勢については第 4 章に書いてみました。

話を聞いてもらう相手がいない場合は，教科書などをいったん全部閉じて，白紙のノートに考えていることを書き出してみることをお勧めします。結局のところ，「何を分かっていないのか」を言葉として外に出すことができれば半分問題は解決したようなものなので，そこを目指しましょう。

質問をされた側の目線

数学について分からなくなった時，人に聞くことも有用だと何回か書いてきましたが，では質問を受けた側はどう対応するのが良いのでしょう。ここからは 2 つ目のテーマである，「数学を伝える側に分かっておいてほしいこと」について書こうと思います。筆者が数学について質問した時，された時の経験が元になっていますので一般論とは程遠いですが，さらっと読み流して頂ければ嬉しいです。

質問者の話を最後まで聞く

質問する側は，質問をしている瞬間にも自分の分かっていないところが何なのか探し続け，整理し続けています。なので，できれば中断せずに最後まで聞きましょう。質問の途中で「それはだって○○じゃないか」のように応答し

てしまうと，質問者は整理しかけた問題点を崩して再度練り直さなくてはならなくなります。

疑問点を一緒に炙り出す

疑問解決の第一歩は，質問者のもやもやを回答者がしっかり共有することです。質問者が分かっているところから始めて，順にステップを踏み，質問者の理解の最前線に回答者も立つことが必要です。

質問者の知識と回答に必要な知識を擦り合わせる

質問に対しての回答に，質問者の知らない事項が必要である場合がよくあります。その場合の回答の仕方には注意が必要です。なぜかというと，「それを知らないんじゃ無理だよ」のような回答だと，質問者に「やはり自分は数学が出来ないんだ」と思わせかねません。なので，ここまでは大丈夫か，ここまでは知っているか，聞いたことがあるか，という具合に質問者の持っている知識を確認して，質問者の知識と回答をどうにかして繋げる作業が必要なのです。

質問者の反応をよく見る

質問者は，自分の分かっていないところを整理するのと同時に，回答者の言葉を咀嚼し理解を試みるというなかなか複雑な思考を巡らせています。そこへ，回答者から言葉の洪水を浴びせてしまうと，質問者を理解しきれない文章で溺れさせてしまうことになります。なので，回答者は一回発言するごとに質問者の反応をよく見るようにしましょう。質問者が 5 秒くらい黙ってしまっても，我慢して待っていて下さい。疑問解決のための質疑応答の主役は質問者側であることを常に意識するのが大切です。質問者に数学をしてもらうことが肝要です。

いきなり答えを出すのではなく，ヒントによって導く

例えば，ピタゴラスの定理を使えば解ける問題があったとしましょう。そして，質問者が，ピタゴラスの定理に気付いていなかったとしましょう。このとき，回答者側から「ピタゴラスの定理」と口に出してしまうのはヒントではなく答えです。重要なのは，質問者に「ピタゴラスの定理を使えば良さげだ」と気付かせることであり，将来似たような問題に出会ったときにも質問者の中にピタゴラスの定理を使う動機が生まれるように導くことです。なのでこの場合のヒントとしては，長さの分かっている辺，分かっていない辺がどこか確認させたり，直角三角形に気付くよう誘導するのが良いでしょう。井戸を掘るのではなく，井戸の掘り方を教えるのです。

質問をしてくれたことに対する感謝を伝える

これは筆者が嬉しかったので入れておきました。

さいごに

この記事のタイトルは，「How to Solve It(G.Polya 著)」の邦訳である「いかにして問題を解くか（柿内賢信訳)」のタイトルをもじらせて頂きました。筆者の拙い文章よりよっぽど読みやすく，しかもまとまっていますので，ぜひ読んで頂きたいです (原著は 70 年も前に書かれていることに驚いています)。他にも，「数学ガールシリーズ (結城浩著)」「数の悪魔ー算数・数学が楽しくなる 12 夜 (エンツェンスベルガー著，丘沢静也訳)」に影響を受けています。数学ガールシリーズからは，数学の対話や数学が分からないときの心情について，数の悪魔からは数学を楽しく伝えることの魅力を学びました。この記事に魅力があるとは正直思えませんが，これをきっかけに今挙げた 3 つの本のどれかでも手に取って頂ければ望外の喜びです。

筆者は一浪していまして，大学入試に落ちた時の数学の点数は 120 点満点中 6 点でした。ですがこうして数学科で元気に数学を勉強しています。人と比べて自分は数学ができないと思う瞬間があると思いますが (無いならそれはそれで素晴らしいです)，そこで数学を勉強することを見限ってほしくありません。記事の説明の中で「高校数学」「大学数学」という言葉を使っていましたが，本来数学はそのような区別ができるものではありません。いつ，どこから勉強をしてもよい広大な学問ですから，地道に，そして貪欲に勉強してもらえればと思います。筆者もそうしたいです。これまで書いてきた数学におけるもやもやは，嫌悪されるものではなくむしろ大事に扱われるべきものであって，そのもやもやをきっかけに好奇心に火をつけて勉強してもらえるといいなと思います。

「なぜ数学を勉強する必要があるのか？」この問いに対する筆者の現在の答えは，「自分の考えを表現する方法を身に付けるため」です。数学には，概念を表現する手法が山のように含まれています。そして，表現された概念に数回，数十回の手続きを加える (計算する) ことで，結論を得ます。このようにして得られた結論は，誰が見ても正しいものです。つまり，自分の頭の中をそのまま人に伝える手段の一つを数学は与えてくれているのです。筆者はまだ大学

生という若輩者なわけですが，自分の考えを人に伝えることの難しさと重要性を (主に部活の仕事で) 痛感しています。言葉を尽くしても尽くしても思ったように伝わっていないことは多々あります。自分の考えと相手の受け取り方を鑑みて最適な表現法を探すのは，数学において概念を表現するのに似ています。むしろ人の心情を想像する方が数学よりもよっぽど難しいのですが，深くまで突き詰めて考えて表現する思考回路は，自分の考えを表現するのにきっと役立つでしょう。そして，他の人が表現しようとしていることを読み取ろうとするときにも大きな威力を発揮するでしょう。

筆者も数学科で勉強させて頂いているくらいには数学の世界に浸っていますので，伝わりにくいところも多い文章だったと想像しますが，ここまで読んで下さってありがとうございました。

$e^{\pi i}sode$ **Vol.5**

2017 年 5 月 20 日発行

著　者・・・・・東京大学理学部数学科有志

発行人・・・・・高木航平