まえがき

前書きを書く前書き (前書き著者より)

目　次

まえがき **i**

数学の基礎（合浦岳彦） **1**

p **進数の世界 (白井)** **7**

ラムダ計算と述語論理 (後藤) **11**

数学の基礎（合浦岳彦）

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] 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．

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．

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**:
$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to x = y)$$
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．

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：

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

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 $<_{\text{lex}}$ 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，

$$\langle s_1, t_1\rangle <_{\text{lex}} \langle s_2, t_2\rangle \iff (s_1 < s_2 \lor (s_1 = s_2 \land t_1 < t_2)).$$

このとき，$<_{\text{leq}}$ 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 $(B, <_{\text{lex}})$ 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

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

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，

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

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：

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

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.

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．

1　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，

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

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．

2　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，“$\cdots$” 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．

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

$\mathbb{Q}_p$ 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．筆算の形を作って右から考えていくと $\cdots$

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

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．

3　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 3.1. 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 3.2. 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，

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

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 $v_p(a+b) \geqq n - 0 + 0 = n = v_p(a)$.

[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．

(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，

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

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 3.3. $a \in \mathbb{Q}$ 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．[2)]

Prop 3.4. 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 3.5. $a, b \in \mathbb{Q}$ 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 3.6. 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，$d_p(a,b) = 0 \Longleftrightarrow a = b$
(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．

4　完備化で $\mathbb{Q}_p$ を定めよう

Def 4.1. 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

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

[2)] 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．

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，

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

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．[3] 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 4.2. 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，

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

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．[4]

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.

---

3) $\mathbb{R}$ 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．

4) $\mathbb{Q}_p$ 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．

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．このノート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．

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 λ→ 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．

Def 0.1. 可算集合 Var を固定し，その元を**変項**という．

Def 0.2. 変項以外に記号 $\star$, $\square$ を用意し，これを**ソート**という．

Def 0.3. 集合 Term を以下によって再帰的に定義する．

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

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．

Def 0.4. 変項 x と擬項 A に対し，記号 $x{:}\,A$ を**型宣言**という．

Def 0.5. 型宣言の列 $\Gamma = \langle x_1{:}\,A_1, \cdots, x_n{:}\,A_n\rangle$ 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．

Def 0.6. 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．

$$\frac{}{\vdash \star\colon \Box}\,\text{Axiom}$$

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

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

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

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

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

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

なお，$\Gamma \cup \langle x\colon A\rangle$ 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]．

Def 0.7. 擬項 M, A に対し，ある型環境 Γ が存在して $\Gamma \vdash_{\lambda\mathrm{P2}} M\colon A$ 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．

Def 0.8. 擬項 A, B に対し，

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

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

このように定義すると，規則 App によって，

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

が成立し，規則 Abs によって，

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

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，

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

が成立する．以上により，$\Gamma \vdash A\colon \star$ 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 λC 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．

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，

$$\alpha{:}\,\star \vdash_{\lambda\mathrm{P2}} (\alpha \to \alpha){:}\,\star \tag{1}$$
$$\alpha{:}\,\star \vdash_{\lambda\mathrm{P2}} (\lambda x{:}\,\alpha.\,x){:}\,(\alpha \to \alpha) \tag{2}$$
$$\alpha{:}\,\star,\ \beta{:}\,\star,\ y{:}\,\beta,\ z{:}\,\alpha \vdash_{\lambda\mathrm{P2}} ((\lambda x{:}\,\alpha.\,y)z){:}\,\beta$$
$$\alpha{:}\,\star,\ \beta{:}\,\star \vdash_{\lambda\mathrm{P2}} (\lambda x{:}\,\alpha.\,\lambda y{:}\,(\alpha \to \beta).\,yx){:}\,(\alpha \to (\alpha \to \beta) \to \beta)$$

などが成り立つ．

$(s, s') = (\Box, \star)$ 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，

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

が得られる．これと式 2 を合わせれば，規則 Abs によって，

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

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．

$(s, s') = (\star, \Box)$ 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，

$$\alpha{:}\,\star \vdash_{\lambda\mathrm{P2}} (\alpha \to \star){:}\,\Box$$

が成り立つので，

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

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，

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

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，

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

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[?] の 5 章もしくは Hindley[?] 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．

Def 0.9. 空でない有限集合 Sort を用意し，その元を**類**という．

Def 0.10. 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．

Def 0.11. 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．

Def 0.12. 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．

Def 0.13. 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．

Def 0.14. 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．

Def 0.15. 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．

Def 0.16. 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，

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

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．

Def 0.17. 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 0.24 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．

Def 0.18. 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．

Def 0.19. 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，

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

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 $k_\Phi{:}\Phi$ 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．

Def 0.20. 多類構造 $\mathcal{S}$ における式の集合 $\Delta = \{\Phi_1, \cdots, \Phi_n\}$ に対し，

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

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

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

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，

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

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，

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

が成り立つなら $z{:}\mathbf{N}$ 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，

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

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 $k{:}\Phi$ 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．

Def 0.21. 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 $x{:}A$ 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．

Prop 0.22. 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，

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

が成り立つ．

Prop 0.23. 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．

Def 0.24. 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 $M\colon \Delta \vdash_{\mathcal{S}} \Phi$ を以下の推論規則に従って定める．

$$\frac{\Phi \in \Delta}{k_\Phi\colon \Delta \vdash \Phi}\,\mathrm{Start}$$
$$\frac{M\colon \Delta \vdash \Phi}{M\colon \Delta \cup \{\Psi\} \vdash \Phi}\,\mathrm{Weak}$$
$$\frac{M\colon \Delta \vdash \bot}{M\Phi\colon \Delta \vdash \Phi}\,\bot\mathrm{E}$$
$$\frac{M\colon \Delta \cup \{\Phi\} \vdash \bot}{(\lambda k_\Phi{:}\,\Phi.\,M)\colon \Delta \vdash \neg\Phi}\,\neg\mathrm{I}$$
$$\frac{M\colon \Delta \vdash \Phi \quad N\colon \Delta \vdash \neg\Phi}{NM\colon \Delta \vdash \bot}\,\neg\mathrm{E}$$
$$\frac{M\colon \Delta \cup \{\Phi\} \vdash \Psi}{(\lambda k_\Phi{:}\,\Phi.\,M)\colon \Delta \vdash \Phi \to \Psi}\,\to\mathrm{I}$$
$$\frac{M\colon \Delta \vdash \Phi \to \Psi \quad N\colon \Delta \vdash \Phi}{MN\colon \Delta \vdash \Psi}\,\to\mathrm{E}$$
$$\frac{M\colon \Delta \vdash \Phi \quad N\colon \Delta \vdash \Psi}{(\lambda\theta{:}\,\star.\,\lambda u{:}\,(\Phi \to \Psi \to \theta).\,uMN)\colon \Delta \vdash \Phi \wedge \Psi}\,\wedge\mathrm{I}$$
$$\frac{M\colon \Delta \vdash \Phi \wedge \Psi}{(M\Phi(\lambda u{:}\,\Phi.\,\lambda v{:}\,\Psi.\,u))\colon \Delta \vdash \Phi}\,\wedge\mathrm{E}_1$$
$$\frac{M\colon \Delta \vdash \Phi \wedge \Psi}{(M\Psi(\lambda u{:}\,\Phi.\,\lambda v{:}\,\Psi.\,v))\colon \Delta \vdash \Psi}\,\wedge\mathrm{E}_2$$
$$\frac{M\colon \Delta \vdash \Phi}{(\lambda\theta{:}\,\star.\,\lambda u{:}\,(\Phi \to \theta).\,\lambda v{:}\,(\Psi \to \theta).\,uM)\colon \Delta \vdash \Phi \vee \Psi}\,\vee\mathrm{I}_1$$
$$\frac{M\colon \Delta \vdash \Psi}{(\lambda\theta{:}\,\star.\,\lambda u{:}\,(\Phi \to \theta).\,\lambda v{:}\,(\Psi \to \theta).\,vM)\colon \Delta \vdash \Phi \vee \Psi}\,\vee\mathrm{I}_2$$
$$\frac{M\colon \Delta \vdash \Phi \vee \Psi \quad N\colon \Delta \cup \{\Phi\} \vdash X \quad P\colon \Delta \cup \{\Psi\} \vdash X}{(MX(\lambda k_\Phi{:}\,\Phi.\,N)(\lambda k_\Psi{:}\,\Psi.\,P))\colon \Delta \vdash X}\,\vee\mathrm{E}$$
$$\frac{M\colon \Delta \vdash \Phi}{(\lambda x{:}\,A.\,M)\colon \Delta \vdash \forall x{:}\,A.\,\Phi}\,\forall\mathrm{I}$$
$$\frac{M\colon \Delta \vdash \forall x{:}\,A.\,\Phi}{MT\colon \Delta \vdash \Phi[x := T]}\,\forall\mathrm{E}$$
$$\frac{M\colon \Delta \vdash \Phi[x := T]}{(\lambda\theta{:}\,\star.\,\lambda u{:}\,(\Pi x{:}\,A.\,\Phi \to \theta).\,uTM)\colon \Delta \vdash \exists x{:}\,A.\,\Phi}\,\exists\mathrm{I}$$
$$\frac{M\colon \Delta \vdash \exists x{:}\,A.\,\Phi \quad N\colon \Delta \cup \{\Phi[x := y]\} \vdash \Psi}{(M\Psi(\lambda y{:}\,A.\,\lambda k_\Phi{:}\,\Phi.\,N))\colon \Delta \vdash \Psi}\,\exists\mathrm{E}$$

なお，規則 $\forall\mathrm{I}$ では $x \notin \mathrm{FV}(\Delta)$ とし，規則 $\exists\mathrm{E}$ 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．

Thm 0.25. 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 0.25 と同様の主張が成立することが知られている．

$e^{\pi i}sode$ **Vol.4 !!!vol を変える!!!**

2016 年 11 月 25 日発行!!!変更する!!!
著　者・・・・・東京大学理学部数学科有志
発行人・・・・・!!!名前を書く!!!