高階算術における逆数学

井澤昇平*

東北大学理学研究科数学専攻

今回は城崎新人セミナーに参加させていただきありがとうございました。毎日朝から夜遅くまでいろんな人にいろんな話を聞けて、他分野の人のものの見方がより一層見えてきた気がしています。また自分の話も熱心に聞いてもらえてうれしかったですし、そのときの様々な反応を見れて、自分の専門について話すときに気をつける点についていろいろ考えさせられました。そういういろんな意味で今回は非常にいい勉強になったと思っています。では本題に入って以下本稿では私の普段研究していることの紹介をしたいと思います。

1　概要：逆数学と高階算術体系

数学には感覚的にいかにも正しそうな命題－公理－から決して自明ではない多くの命題－定理－を証明するという側面がある。では定理を一つ持ってきたときに、どれくらいの公理を仮定すればその定理の証明は可能だろうか？このような問題に数学的にアプローチするには例えば次のような手続きを踏めばよいであろう。

公理の中でも何らかの意味でより自明である度合いが高いもののみを取り出す（それを基礎の公理と呼ぶ)。基礎の公理より強い公理 T と φ を考える。公理 T から定理 φ が導け基礎の公理の下で φ から公理 T 導けることを証明する。このことが言えると（基礎の公理の選び方に関する恣意性に目をつむれば)、φ を証明するのに必要十分な公理は T_i であると結論づけることができるわけである。このような方法による研究は逆数学と呼ばれている。「定理から公理を証明する」という普通とは逆の議論が研究の最重要部分となるためである。

以上の議論を数学的に扱うためには「定理から公理が導ける」ということを定式化しなければならない。数学基礎論では形式体系という概念を用いてこれを行なっている。

数学の議論を取り扱うことができる形式体系として最も有名なのは（公理的）集合論であろう。しかしそれ以外にもさまざまな体系が提唱されており、本稿のタイトルにある高階算術もその一つである。高階算術体系は大雑把に言うと自然数の全体 $\mathbb{N}$（本稿では 0 も自然数として扱う）と、$\mathbb{N}$ から $\mathbb{N}$ への写像の全体 $\mathbb{N}^{\mathbb{N}}$、以下 $\mathbb{N}^{\mathbb{N}^{\mathbb{N}}}$ や $(\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}$・・・というものに関する言葉を備えた体系である（正確な定義は後に述べる)。

これくらいの言葉（と自然数における基本的な演算）が扱えると自然数の対を扱うことができ、自然数の対を適当な同値関係で割ったものとして整数全体 $\mathbb{Z}$ が取り扱え、整数の対の同値類として有理数が扱え、コーシーの完備化（あるいはデデキントの切断）の全体として実数を取り扱うことができる。さらに、実数の対として $\mathbb{R}^n$ のような表現も取り扱えて、一つ集合 M を固定しておいて M の部分集合と $\mathbb{R}^n$ の部分集合との間の写像の集合を考えれば多様体なども取り扱うことができる。このようにして高階算術の体系では多くの数学の議論を取り扱うことができるわけである。

2　高階算術体系

形式体系とは、言語と呼ばれる一つの集合 $\mathcal{L}$ とその他の多少の付加的な情報と、それに関連する諸定義を指す言葉である。集合 M と $\mathcal{L}$ の元ごとに対応する M 上の関係や演算を集めたものを $\mathcal{L}$ 構造と呼び、$\mathcal{L}$ 構造に関

* sa9m02@math.tohoku.ac.jp

するある種の命題（論理式）の集合 T を全て成立させる $\mathcal{L}$ 構造を T のモデルと呼ぶ。そして論理式 φ が T のモデルで常に成り立つ場合に T は φ を証明するというのである。正確な定義は以下のとおり。

定義 2.1.

1. 言語とは以下のような対 $(S, \mathcal{L}, a, v)$ のことをいう：$S, \mathcal{L}$ は集合であり、a は $\mathcal{L}$ から $\mathbb{N}^S$ への写像であって $f \in \mathcal{L}$ を固定するたびに $a(r)(s) \neq 0$ となる $s \in S$ は有限個しかないものであり、v は $\mathcal{L}$ から S への写像である。
2. $(S, \mathcal{L}, a, v)$ 構造とは以下のような対 $(\{M_s\}_{s\in S}, \{f_M\}_{f\in\mathcal{L}})$ のことをいう：各 M_s は集合であり、各 f_M は $\prod_{s\in S} M_s^{a(f)(s)}$ から $M_{v(f)}$ への写像である。

本稿では S の元を sort、$\mathcal{L}$ の元を関数記号、$a(f)$ を $f \in \mathcal{L}$ の定義域、$v(f)$ を f の値域と呼ぶことにする。$a(f)(s) \neq 0$ となる $s \in S$ が $s_1, \cdots, s_k$ のときに $a(f)$ を $(s_1^{((a(f)(s_1))}, \cdots s_k^{(a(f)(s_k))})$ と表記することもある。また $k = 0$ のときには f は $v(f)$ 値定数記号であるということにする。

$(S, \mathcal{L}, a, v)$ 文というのは f と $=$（等号）、$\wedge$（かつ）、$\neg$（否定）、$\forall x^s$ などの表記を用いて表すことができる意味の通る命題のことをいう。

「文 φ が構造 $M = (\{M_s\}, \{f_M\})$ で成立する」ということを f を f_M，$\forall x^s$ を $\forall x \in M_s$ というように置き換えた命題が成立することと定め、$M \models \varphi$ と書く。文の集合 T に対しても $M \models T$ という書き方をする。この場合任意の $\varphi \in T$ に対して $M \models \varphi$ となるという意味である。

文の集合 T と文 φ に対し、任意の $M \models T$ に対して $M \models \varphi$ が成り立つとき、$T \vdash \varphi$ と書き、T は φ を導く、T から φ が証明できるなどという。

次に高階算術の体系の定義を与えよう。まず準備として以下では $Type$ を ϕ を自由生成元とする rank 1 の自由亜群（一つの 2 項演算の構造が入った代数系で何ら関係式がないもの）を表すことにする。$Type$ の 2 項演算は $\to$ で表す。

高階算術体系は $Type$ の元を sort として sort ϕ を自然数の全体、$\sigma \to \tau$ を σ の元を与えられたら τ の元を返す関数の全体と見立てる。そのイメージをある程度持てるようにいくつかの構造と公理を導入するのである。

まず写像については λ-calculus を用いてそれらしい構造を導入する。それは変数記号を $\sigma \in Type$ 毎に可算個 $\{x_n^\sigma\}_{\sigma\in Type, n\in\mathbb{N}}$ 用意し、次に述べる λ-term というものを用いて記述されるものである。

定義 2.2. 集合 Λ と写像 $type : \Lambda \to Type$ を以下をみたすもののうち最小の集合とその上で定義された写像とする。

$$\begin{array}{rll} \{x_n^\sigma | n \in \mathbb{N}, \sigma \in Type\} \subset \Lambda, & & type(x_n^\sigma) = \sigma \\ t \in \Lambda & \Rightarrow (\lambda x_n^\sigma.t) \in \Lambda, & type(\lambda x_n^\sigma.t) = \sigma \to type(t) \\ t, s \in \Lambda, type(t) = \sigma \to \tau, type(s) = \sigma & \Rightarrow t(s) \in \Lambda, & type((t(s)) = \tau \end{array}$$

Λ の元を λ-term と呼ぶ。

λ-term $\lambda x.t$ の直感的な意味は x に t を対応させる写像であり、$t(s)$ の直感的意味は s の写像 t による像である。

二変数関数 $f : (x, y) \mapsto z$ は自然に $x \mapsto (y \mapsto z)$ と同一視できるので以下の記述では意味がとりやすさを考慮して $\sigma \to (\tau \to \nu)$ を $(\sigma, \tau) \to \nu$ と書いたり $(f(x))(y)$ を $f(x, y)$ と書いたりする場合がある。

定義 2.3. 高階算術体系の言語 $\mathcal{L}^\omega$ は以下のようなもののことをいう。

- sort の集合は $type$.
- 関数記号の集合は $\{0, S, \mathcal{R}_\phi\} \cup \Lambda \cup \{App_{\sigma,\tau}\}_{\sigma,\tau\in Type}$.
- App 以外は定数記号でその値域は $v(0) = \phi, v(S) = \phi \to \phi, v(\mathcal{R}_\phi) = (\phi, (\phi, \phi) \to \phi) \to (\phi \to \phi)$, $t \in \Lambda$ にたいしては $v(t) = type(t)$ とする。App の定義域は $a(App_{\sigma,\tau}) = ((\sigma \to \tau)^1, \sigma^1)$，値域は

$v(App_{\sigma,\tau}) = \tau$ とする。

$0, S$ はそれぞれ自然数の 0 と自然数 x に 1 を足す写像 $x \mapsto x+1$ に対応するもので、$App(x,y)$ は写像 x に元 y を代入したものに対応するものを表現するためのものである。($\mathcal{R}_0$ については次の定義の後のコメント参照。)以下では $App(x,y)$ は $x(y)$ と表記することにする。

例 2.4.

$$\begin{array}{rcl} M_0 & := & \mathbb{N} \\ M_{\sigma\to\tau} & := & \{f : M_\sigma \to M_\tau\} \end{array}$$

で定まる構造を高階算術の標準モデルという。

高階算術における逆数学とは標準モデルにおいて成り立つ、“公理っぽい”文の集合を公理として採用する。その上で与えられた定理に対してそれがどれくらい少ない公理で証明可能であるのかを調べるわけである。

以上で高階算術体系の枠組みの定義が終わった。次に高階算術における逆数学において用いられるいくつかの公理の定義を与えよう。

定義 2.5. 以下の $\mathcal{L}^\omega$ 文の集合を RCA_0^ω と書く:

1. $\forall x^{\sigma\to\tau}\forall y^{\sigma\to\tau}(\forall z^\sigma; (x(z) = y(z) \leftrightarrow x = y))$.
2. $\forall y^\sigma; ((\lambda x.t)(y) = t[y/x])$.
3. $\forall a^\phi; S(a) \neq 0$.
4. $\forall a^\phi \forall b^\phi (S(a) = S(b) \to a = b)$.
5. $$\forall a^\phi \forall f^{(\phi,\phi)\to\phi} \forall b^\phi \left[\begin{array}{rcl} \mathcal{R}_0(a,f)(0) & = & a \\ \mathcal{R}_0(a,f)(S(b)) & = & f(b, \mathcal{R}_0(a,f)(b)) \end{array} \right].$$
6. $\forall A^{(\phi\to\phi,\phi)\to\phi}[(\forall x^{\phi\to\phi}\exists y^\phi; A(x,y) \neq 0) \to (\exists F^{(\phi\to\phi)\to\phi}\forall x; A(x, F(x)) \neq 0)$.

1. は写像の等号が元の行き先が常に等しいこととして定義されることに対応している。2. の右辺 $t[y/x]$ は t に現れる x を y に置き換えたものを表し、2. の全体としての意味は先に述べた λ と App の意味に対応している。3. と 4. は自然数の基本的な性質を取り出したもので、5. は $g(0) := a, g(b+1) := f(b, g(b))$ という漸化式により関数 g が定義が可能であることを表している。6. は $\prod_{x\in M_{\phi\to\phi}}\{y | A(x,y) \neq 0\}$ という直積集合が空でないという選択公理に対応している。

RCA_0^ω は二階算術という逆数学の中で最もよく研究されている体系における RCA_0(recursive comprehension axiom)というおおよそ計算可能なものの範囲で議論できることのみ証明できるような公理系の類似として提唱されたものである。

二階算術での逆数学の多くの結果が RCA_0 を基礎の公理としたものであることから、RCA_0^ω を基礎の公理の候補として Kohlenbach [2] は提示している。

RCA_0^ω ではそれほど多くの定理を示すことはできない。例えば次の論理式は普通の感覚からいえば公理として良さそうなものであるが、(σ, τ の rank(後述)が低い場合を除いて)RCA_0^ω では証明できない。

定義 2.6.

1. 次の論理式を $\mathcal{E}_\sigma$ と書く:

$$\exists E^{(\sigma\to\phi)\to\phi}\forall f^{\sigma\to\phi}(E(f) \neq 0 \leftrightarrow \forall x^\sigma; f(x) = 0)$$

2. 次の論理式を $\mathrm{AC}^{\sigma,\tau}$ と書く:

$$\forall A^{(\sigma,\tau)\to 0}[(\forall x^\sigma \exists y^\tau; A(x,y) \neq 0) \to (\exists F^{\sigma\to\tau}\forall x^\sigma; A(x, F(x)) \neq 0)]$$

これらの公理は定理との同値性を示す際の候補になることが期待される。

集合をその特性関数と同一視する $x \in A \Leftrightarrow A(x) \neq 0$ という視点で見ると $\mathcal{E}_{\sigma\to 0}$ は既に得られた集合などから $\wedge, \neg$ と $\forall^{\sigma}$ を用いて記述できる条件をみたす元の全体という集合が常に存在するという公理に実はなっている。

$\mathrm{AC}^{\sigma,\tau}$ は $\mathrm{AC}^{1,0}$ の場合と同様にある種の選択公理である。以下ではそう記述した方が意味が捉えやすい場合には $A(x) \neq 0$ を $x \in A$ と書くなどの表記を用いることにする。

3 RCA_0^{ω} の下で成り立つ基本的な事実

$\mathcal{E}$ や AC に関して最も基本的な結果は強さが sort の集合の“濃度”とちょうど対応することである。

定義 3.1. $\mathrm{rank} : \mathit{Type} \to \mathbb{N}$ を帰納的に次のように定める。

- $\mathrm{rank}(\phi) := 0,$
- $\mathrm{rank}(\sigma \to \tau) := \max(\mathrm{rank}(\sigma) + 1, \mathrm{rank}(\tau)).$

$\mathrm{rank}(\sigma) = n$ は標準モデル $\{M_\sigma\}_\sigma$ において M_σ の濃度が可算集合から n 回べき集合をとった濃度になっていることを意味する。そして形式体系の中では次のことが証明できる。

命題 3.2. $\sigma_1, \sigma_2, \tau_1, \tau_2 \in \mathit{Type}$ に対して $\mathrm{rank}(\sigma_1) \leq \mathrm{rank}(\sigma_2), \mathrm{rank}(\tau_1) \leq \mathrm{rank}(\tau_2)$ が成り立っているとする。

1. RCA_0^{ω} の下で $\mathcal{E}_{\sigma_2}$ は $\mathcal{E}_{\sigma_1}$ を導く（すなわち $\mathrm{RCA}_0^{\omega} \cup \{\mathcal{E}_{\sigma_2}\}$ は $\mathcal{E}_{\sigma_1}$ を導く）。
2. RCA_0^{ω} の下で $\mathrm{AC}^{\sigma_2,\tau_2}$ は $\mathrm{AC}^{\sigma_1,\tau_1}$ を導く。

特に RCA_0^{ω} の下では $\mathcal{E}_\sigma$ の強さは σ の rank のみによって決まり、σ そのものには依存しないことがわかる。そのため $\mathcal{E}_\sigma$ を $\mathcal{E}_{\mathrm{rank}(\sigma)}$ のように書くことがある。AC についても同様である。

この表記の下で次のことが成り立つ。

定理 3.3. $n \geq 1, 0 \leq k \leq n-2, 0 \leq l \leq n-1$ のとき

$$\mathrm{RCA}_0^{\omega} \cup \{\mathcal{E}_{n+1}, \mathrm{AC}^{k,l}\} \vdash \mathrm{Con}(\mathrm{RCA}_0^{\omega} \cup \{\mathcal{E}_n, \mathrm{AC}^{k,l}\}).$$

が成り立つ。特に第二不完全性定理により $\mathrm{RCA}_0^{\omega} \cup \{\mathcal{E}_n\} \not\vdash \mathcal{E}_{n+1}$ が成り立つ。

ここで $\mathrm{Con}(T)$ は「T をみたす構造が存在する」という意味の文である。(高階算術体系は特性関数と集合を同一視することで集合の概念を表現することができる。また写像や対などの概念も記述できる構造を有しているので「・・・という構造」という意味のことを論理式として表現することができる。単純な例で言えば「半群が存在する」ということは

$$\exists A^{\phi\to\phi}\exists p^{(\phi,\phi)\to\phi}\left[\begin{array}{l}\forall x^{\phi}\forall y^{\phi}; \{(x\in A \wedge y \in A) \to p(x,y) \in A\} \\ \forall x^{\phi}\forall y^{\phi}\forall z^{\phi}\{(x \in A \wedge y \in A \wedge z \in A) \to p(p(x,y),z) = p(x,p(y,z))\}\end{array}\right]$$

のように書くことができるわけである。)

4 整列可能定理に関する逆数学

最後に整列可能定理に関連した逆数学現象を筆者が調べた結果を述べ、本稿を終える。

定義 4.1. 以下の論理式を σ-WO と書く。

$$\exists R^{(\sigma,\sigma)\to 0}\exists F^{(\sigma\to 0)\to 0}\left[\begin{array}{l}\forall x;(x,x)\in R\\ \forall x\forall y((x,y)\in R\to(x,y)\notin R)\\ \forall x,y,z((x,y)\in R\wedge(y,z)\in R\to(x,z)\in R)\\ \forall A^{\sigma\to 0}\forall x(x\in A\to(F(A),x)\in R)\end{array}\right]$$

ただし x,y,z はいずれも sort σ の変数とする。

$M\models\sigma$-WO は M_σ の整列順序 R と R に関する $A\in M_{\sigma\to 0}$ （感覚的には $A\subset M_\sigma$）の最小元を対応させる写像 F がいずれも M の中に存在することを意味する。

σ-WO も $\mathcal{E}_\sigma$ などと同様に RCA_0^ω の下では σ の rank のみで強さが決まることが分かる。そのため以下では n-WO ($n\in\mathbb{N}$) という表記を用いる。

定理 4.2. $n\in\mathbb{N}$ に対し次が成り立つ。

1. $\mathrm{RCA}_0^\omega\cup\{\mathcal{E}_{n+2},\mathrm{AC}^{n+1,n}\}\vdash n\text{-WO}$.
2. $\mathrm{RCA}_0^\omega\cup\{n\text{-WO}\}\vdash\mathcal{E}_{n+1}\wedge\mathrm{AC}^{n+1,n}$.
3. $\mathrm{RCA}_0^\omega\cup\{\mathcal{E}_{n+2},\mathrm{AC}^{n+1,n}\}\vdash\mathrm{Con}(\mathrm{RCA}_0^\omega+n\text{-WO})$. 特に $\mathrm{RCA}_0^\omega\cup\{n\text{-WO}\}\nvdash\mathcal{E}_{n+2}$.

$\mathrm{RCA}_0^\omega\cup\{\mathcal{E}_{n+1},\mathrm{AC}^{n+1,n}\}$ から n-WO が導けるかどうかは（少なくとも私には）分かっていない。

この例のように始めに挙げた逆数学研究のスローガンである公理のどれかと定理が同値であることを示すところまでは行かず、強い公理と弱い公理の中間に定理があることで止まってしまうケースも多い。

参考文献

[1] Stephen G. Simpson, *Subsystems of Second Order Arithmetic second edition*, Springer-Verlag, 2009

[2] Ulrich Kohlenbach, *Higher Order Reverse Mathematics*, Lecture Notes in Logic, 2001

[3] James Hunter, *Higher-Order Reverse Topology*, Ph.D Thesis University of Wisconsin, 2008