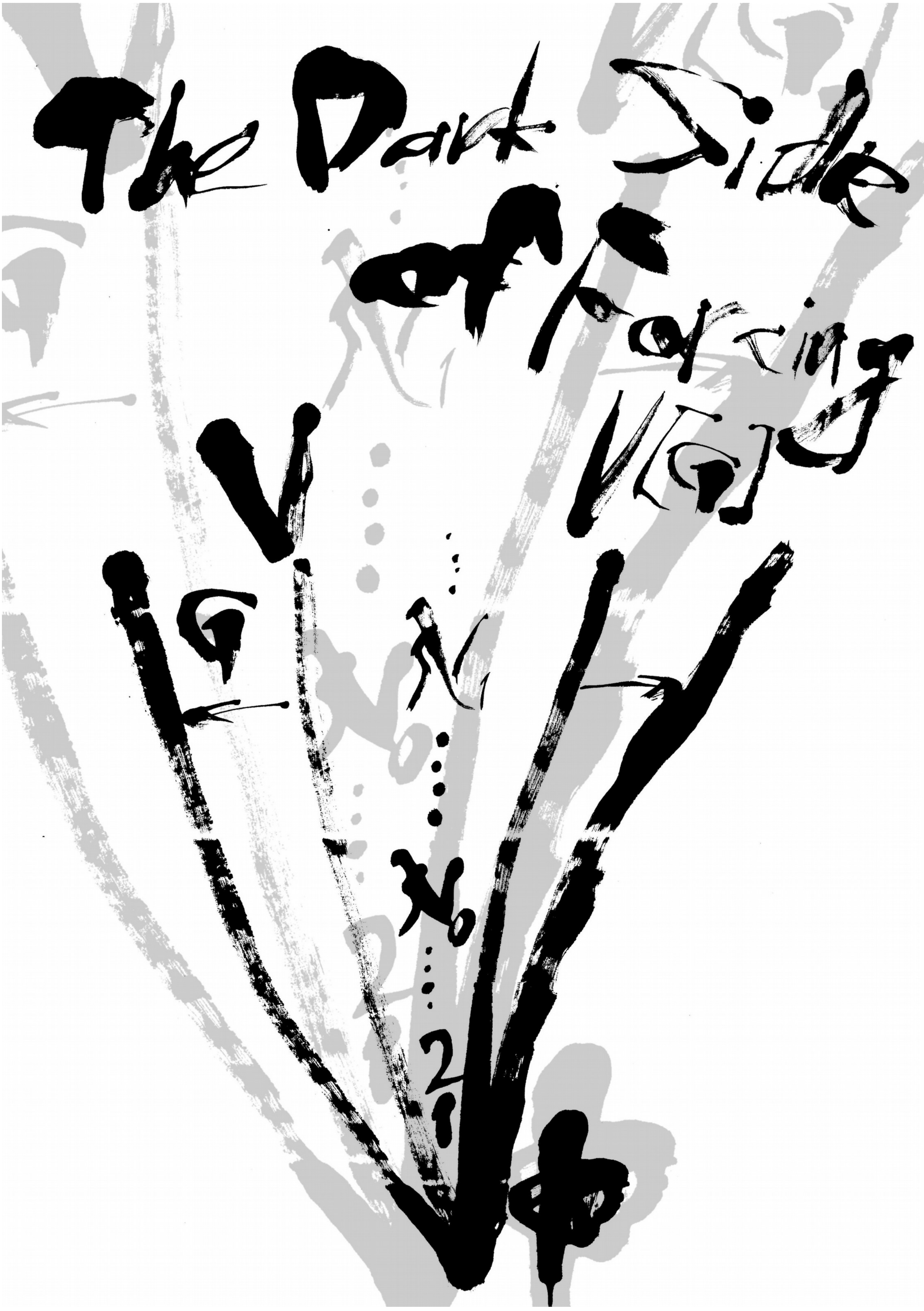

The Dark Side of Forcing
V[G]
No 21

Welcome to the darkside of Forcing!

淡中　圏

この度, The Darkside of Forcing Vol.V をお買い上げありがとうございました．こんなこと初めてもう 3 年目と考えると感慨深いものがこみ上げるような気がしないでもありません.

今回の内容もいろいろ盛りだくさん.

まず鈴木佑京さんによる,『ゲンツェンの洞察——証明は列か, ツリーか？』.

「証明論」とは, 証明自体を数学の対象としてしまおうという面白い学問ですが, 証明をどう形式化するかは, いろいろなやりかたがあります．その一つ一つを歴史的経緯も含めてわかりやすく対比し,「証明って何だろう」という疑問の答えへと接近しています．その中から「形式化って何だろう」というもっと根深い疑問へもアプローチしちゃいますよ.

続いては私, 淡中圏の『評論　小島寛之の浅さと卑怯さ』.

なんか書いた自分が言うのもなんだけどキツい言葉使ってますね．まあ, はっきりいや怒ってるんですよ．辛口です.

次は古賀実さんによる『Grothendieck トポスの基本性質に関するノート』.

このジャンルでは基本図書である Mac Lane と Moerdijk による『Sheaves in Geometry and Logic』（略称 SGL）ですが, 読んでみると頭の周りをたくさんの疑問符が回ることになりがち．それを丁寧に読み解き, 記号を整理し, ギャップを埋めてくれています．早くこのノートが完成し, SGL を風呂の薪にすることができるようになる日が来るといいですね.

そして才川隆文の『Δ-system lemmma (“スタート集合論 “ノート WIP2)』.

IT 企業と連携して開いている集合論の勉強会という, なんだか面妖な代物の成果物ですが, 内容はいたって真っ当. 強制法の教科書としてこれまた非常に有名な Kunen の『集合論』（通称 Kunen 本）の中の「Δ-system lemma」の証明を, 再整理しようとしています. Kunen のやり方がうますぎて, 再構成するのに苦労していましたが, その成果やいかに？

（ネタバレ：未完成）

最後に恒例の私, 淡中圏のちょっとした創作が入っております．もっとちゃんとしたのを書きたいといつも思いつつ, 適当なものでお茶を濁してますので, 肩の力を抜いて読んでくださいな.

表紙と裏表紙は数学書道家の平野智博さんに書いてもらいました。集合論の宇宙と、topos の subobject classifier の pull back のダイアグラムです。こういうのとてもいいと思うので、もっとコラボしていきたいですね。

さて, 前説が長くなりすぎると観客は白けるばかり．ちょっと毛色の違う数学の世界をご覧あれ！

目次

第 1 章

ゲンツェンの洞察――証明は列か、ツリーか？

鈴木佑京

1.1 はじめに

数理論理学におけるいわゆる「証明論」とは、数学的議論や論理的議論において登場する論理的推論――これをまとめて以下では「証明」と呼ぶことにするが――を対象とし、証明が持っている性質や、証明同士が形成する構造などを研究する分野である。

現代の証明論は、歴史上の偉大な論理学者による次の三つの洞察を前提して展開されている。すなわち、

- 証明はそれ自体数学的構造を持つ数学的対象である。
- 証明は、その「真の姿」（正規形）に向かって計算することができるプログラムである。
- 論理を定式化する方法は複数存在し、それぞれ異なった証明論的性質を持つ。

という三つの洞察である。このうち、一つ目はヒルベルトによって [7]、三つ目はゲンツェン [6] によって発見されたものである（二つ目の洞察は通常ゲンツェンに帰されるが、ヒルベルトの考えていた無矛盾性証明の方法――いわゆるイプシロン代入――の中にも同様の発想はすでに存在したのではないかと私は考えている [8, chapter 3]）。

本稿は、この三つの洞察のうちの三つ目が実際にどのように現象として現れるのかを、論理を定式化するための二つのパラダイムに注目する形で見てみることを目標とする。ここでいう論理を定式化するためのパラダイムとは、証明の形をどう考えるかという事に関する選択を指す。論理を定式化する上では、証明というものを、**列の形をしている**と考える考え方と、**ツリーの形をしている**と考える考え方があり[*1]に、どちらの考え方を取るかによって同じ論理（帰結関係が同一であるという意味で）でも性質が異なってくる。本稿では、それぞれのパラダイムに基づく論理の定式化の特徴を、証明の形に注目する形で紹介していくことで、二つのパラダイムを比較する。この作業を通じて、ゲンツェンの洞察

[*1] 全ての形式体系がこの二つのパラダイムのどちらかに基づくわけではない。例えば、証明網で定式化された形式体系は、列でもツリーでもない。

を具体化してみることが本稿の目標である。

本稿は二種類の読者を念頭に置いている。まず、大学の授業などで数理論理学の基礎的な知識を身につけ、自然演繹による証明などについて簡単な練習はしたが、証明論という下位分野にはそれほど馴染みのない人。初級の授業で複数の形式体系を比較することはあまりないだろうから、本稿を読んでもらえば、上記のゲンツェンの洞察について理解することができ、証明論という分野の雰囲気を掴んでもらえると思う。また、証明論についてある程度知識を持っている人にも、本稿を読んでもらいたいと考えている。個々の形式体系ではなく、「列」と「ツリー」という形で抽象的に形式体系を比較する議論はそれほど多くないので、普段とは少し違った視野から体系同士の関係を掴んでもらえるだろう。

最後に、本稿で登場する論理の定式化を列挙しておく。ヒルベルト式、自然演繹、シークエント計算、構造計算、以上四つの体系がもつ特徴を、「列」と「ツリー」という観点から比較していく。個々の形式体系や定式化に関しては厳密な定義はせず、必要な範囲でアイデアだけを述べていく形で議論を進めたい。

1.2 論理の定式化とはなにか？

「列」と「ツリー」の間の比較に入る前に、そもそもここで言う「論理を定式化する方法」とは何を指しているのかを説明しておいたほうがいいだろう（先述した「ヒルベルト式」とか「自然演繹」とか「シークエント計算」という語の意味がすぐにピンとくる人は、この節は読み飛ばしてもらって構わない)。

論理学においてもっとも基礎的な関係は、命題と命題の間の帰結関係である。つまり、どんな命題からどんな命題が論理的に帰結すると考えるのか、この点をはっきりさせておくことは、論理学の研究においてなによりもまず前提となる。例えば、$\neg\neg A$ から A が論理的に帰結するのか、そうではないのか。二重否定を除去できると考える論理と考えない論理は同一視しがたい。従ってまず、論理的帰結関係を明確化することで、どんな論理が問題になっているのかを明確化する必要がある。特に、論理を数学的に研究するのが数理論理学である以上、論理的帰結関係は数学的に厳密な形で定義されなければならない。

論理的帰結関係を定義する方法の一つが証明可能性を利用するものである。つまり、ある命題からある命題を論理的に証明する方法をまず定義し、このような証明が可能である時に、命題の間に論理的帰結関係が成り立つ、と定義するわけである。典型的には、実質的な証明なしに認められるような命題である**公理**と、命題と命題をつなぐ、論理的な推論の最小ステップとなる**推論規則**の二つを定義し、この二つを使って作られる、命題を**ある形**に並べた図像を**証明**と定義する。このように、論理に対して証明の概念と証明可能性の概念を定義し、帰結関係を定めることを、論理の形式化と言う。さらに、このように定義された証明の概念を指して、**形式体系**と呼ぶ。

具体例を使って説明しよう。例えば、古典論理の形式体系の一つに、次のようなものがある。

- 形式体系 CL0
- 公理
  - $A \to (B \to A)$
  - $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

  - $(\neg B \to \neg A) \to (A \to B)$
- 推論規則
  - A と $A \to B$ から B を推論してよい。(Modus Ponens, MP)

$\wedge, \vee$ といった論理結合子は他の二つから定義できるので、今は無視する。以上の公理と推論規則をもとに、証明は、命題の列として定義される。つまり、命題群 Γ から命題 A への証明とは、現れる命題の全てが、1) 公理の一例であるか、2) Γ の一例であるか、3) その命題よりも前に登場する命題（群）から推論規則によって生成される命題であるか、のどれかであるような、命題の列である。

ところで、古典論理は、別の形式体系によっても形式化できる。例えば、次のように公理と推論規則を変える。

- 形式体系 CL1
- 公理
  - $((((P \to Q) \to (\neg R \to \neg S)) \to R) \to T) \to ((T \to P) \to (S \to P))$
- 推論規則
  - A と $A \to B$ から B を推論してよい。(MP)
  - A から、A に出てくる原子式に、別の式を代入した式 B を推論してよい。

この体系は公理が一つしかないが、先の形式体系と証明可能性においては変わらないので、古典論理の形式化になっている。先の形式化とこの形式化は、違う公理と推論規則を持っているので、形式化として異なったものである。

しかし、先の形式化と今回の形式化は、根本的な枠組みにおいては変わらない。それは、Γ を仮定して A を導く証明を 1) 公理の一例であるか、2) Γ の一例であるか、3) その命題よりも前に登場する命題（群）から推論規則によって生成される命題であるか、のどれかであるような、命題の列として定義するという点で、同じである。このような場合、つまり、公理と推論規則は違うが、証明を定める枠組み自体は変化しない場合を、「定式化が同じ」と表現することにしよう。先の形式化と今回の形式化は、形式化としては異なるが、定式化は同じである。そして、ここで同じと言われているもの——つまり、証明を定める枠組みのことを、「定式化」と呼ぶ。

定式化が異なる形式体系とは例えばどのようなものだろうか。たとえば、おそらく古典論理の形式体系として最も知名度が高い、自然演繹 NK はその一つである。NK は公理をもたず、それぞれの結合子に対して、I-rule と E-rule の二種類の推論規則を定めた体系である。たとえば、$\wedge$ の規則は次の三つである。

$$\frac{A \qquad B}{A \wedge B}\,(\wedge I) \quad \frac{A \wedge B}{A}\,(\wedge E0) \quad \frac{A \wedge B}{B}\,(\wedge E1)$$

後にもう少し詳しく見るが、NK における証明は、先ほどの二つの形式体系と異なり、列ではなくツリー（木）の形をしている。この意味で、NK と先ほどの二つの公理系は、単に異なる形式化であるだけでなく、定式化自体が異なるのである。

一つの論理に複数の形式化が存在するということにはフレーゲがすでに気づいていた [3, p.42] が、一つの論理に複数の定式化が存在し、それぞれ異なる性質を持つ、ということに気づいたのはゲンツェンである [6]。以下では、様々な定式化を、証明の形という点に注目して比較し、ゲンツェンの洞察を具体化してみよう。

1.3　代表選手を比較してみる

まず、列パラダイムの代表選手であるヒルベルト式と、ツリーパラダイムの代表選手である自然演繹及びシークエント計算を導入した上で、両者を証明の形に注目する形で比較してみよう。

1.3.1　列パラダイム—ヒルベルト式

歴史的に言えば、最初に現れたのは「列」パラダイムの方である。論理の形式化を最初に成し遂げたのはフレーゲ [3] だが、彼が使った定式化が、現在「ヒルベルト式」と呼ばれる定式化であり、「列」パラダイムの代表選手と言うべきものであった。

ヒルベルト式の定式化とは、前節で述べた CL0 と CL1 においても使われているものであるので、ここで再度詳しく説明し直すことはしない。核となる部分だけ確認しておくならば、ヒルベルト式の定式化は、公理と推論規則を幾つか定めた上で、証明を、1) 公理の一例であるか、2) 仮定の一例であるか、3) その命題よりも前に登場する命題（群）から推論規則によって生成される命題であるか、のどれかであるような、命題の**列**として定義する[*2]。

1.3.2　ツリーパラダイム—自然演繹、シークエント計算

フレーゲやヒルベルトによる公理系が登場した後に、ゲンツェンは、全く異なるパラダイムに基づく論理の定式化を提案した [6]。それがツリー型のパラダイムに基づく「自然演繹」と「シークエント計算」である。

自然演繹については、先に簡単に言及したが、もう一度確認しておこう。自然演繹は（理想的には）、公理をもたず、それぞれの結合子に対して、I-rule と E-rule の二種類の推論規則を定めた体系である。この二種類の規則によって作られる**ツリー**を証明として定義する。自然演繹はヒルベルト式に比べると推論規則が多く、証明の厳密な定義も面倒であるので、ここでは詳しく説明しないが、証明の具体例を挙げておこう。例えば、$A, B, (A \wedge B) \to C$ から C に至る証明の一つは次のようになる。

$$\dfrac{\dfrac{A \qquad B}{A \wedge B}\,(\wedge I) \qquad (A \wedge B) \to C}{C}\,(\to E)$$

これは、仮定から二つの推論規則を使って結論を出している証明であるが、注目すべきは、証明の形である。この証明には、枝分かれが存在するので、単なる列ではなく、ツリー（木）の構造を持っている。従って、ヒルベルト式の「列」パラダイムと異なり、自然演繹は「ツリー」パラダイムに基づく定式化であるといえる。

シークエント計算の方は自然演繹に比べると知名度が低いが、証明論的には同程度に重要な体系である。シークエント計算は、命題ではなく、帰結関係を表す式・シークエント

[*2] なお、推論規則として MP だけを採用し、仮定の discharge を認めないが、証明の形としてはツリーを採用するような定式化もあり、これも「ヒルベルト式」と呼ぶことがある。実はヒルベルト自身が、形式体系に対する無矛盾性証明を遂行する中でツリーの形をした証明を導入していた [8, chapter 3]。だがここでは、「列」と「ツリー」の比較という趣旨から、最初にヒルベルトが考えた定式化、つまり、証明を列として捉えるものだけをヒルベルト式と呼ぶことにする。

を単位とする定式化である。シークエントは、例えば $A, B, C \vdash A \land B, D$ というように、帰結関係を表す $\vdash$ を挟んで式の列をつなげたものであり、このシークエントは、「A と B と C が同時に成立しているなら、$A \land B$ か D のどちらかが成立している」ことを意味する。

公理となる、実質的な証明なしに成立するシークエントとして同一律 $(A \vdash A)$ が置かれ、これを変形する推論規則として、個々の論理結合子にかかわらない構造規則と、個々の結合子について R-rule と L-rule が置かれる。$\land$ の規則だけ述べておこう。

$$\frac{\Gamma_0 \vdash A, \Delta_0 \qquad \Gamma_1 \vdash B, \Delta_1}{\Gamma_0, \Gamma_1 \vdash A \land B, \Delta_0, \Delta_1} (\land R) \quad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \land B \vdash \Delta} (\land L0) \quad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \land B \vdash \Delta} (\land L1)$$

自然演繹と同様に、これらの規則から作られるツリーが証明である、と定義される。規則が枝分かれを含むため、証明図は単純な列にはならない。

1.3.3　比較

以上で、列パラダイムとツリーパラダイムの代表選手というべき、ヒルベルト式の定式化と、自然演繹・シークエント計算の定式化を導入した。では次に、両者を比較してみよう。

まず顕著な違いとしてあげられるのは、公理と推論規則のうち、どちらの量が多いか、ということである。自然演繹やシークエント計算は、それぞれの論理結合子に二種類の推論規則を要求するので、推論規則の数が膨れ上がってしまう。代わりに、公理は少なくて済む。これに対して、ヒルベルト式は推論規則について特に制限がない。そのため、公理を多くすることで、推論規則を単純化することができる。

この違いは、証明を対象として、証明論的な議論をする際の場合分けに現れる。証明論的な議論の中には、「この命題がこの推論規則によって導出されていた場合……」「この命題がこの公理の一例として導出されていた場合……」というような場合分けがしばしば現れるが、ヒルベルト式の場合は、推論規則に関する場合分けが少なくて済む。逆に、自然演繹やシークエント計算は、推論規則に関する場合分けが面倒になる代わりに、公理の場合分けが少なくて済む。

また、仮定の操作が可能かどうか、という点も両者の顕著な違いであろう。自然演繹には例えば、次のような推論規則が登場する。

$$\frac{\begin{matrix}[A]\\ \cdots \\ B\end{matrix}}{A \to B} (\to I)$$

これは、「A を仮定して B に至る証明」を、「（仮定のない）$A \to B$ に至る証明」に変換する推論規則である。この推論規則を適用することによって、証明が持っていた仮定が減る、という点が重要である。

シークエント計算にも同様の規則がある。例えば、

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta} (\to R)$$

は、「A を仮定すると B が帰結することの証明」を「（仮定なしに）$A \to B$ が帰結することの証明」に変換する規則であり、やはり仮定を減らすことができる。

つまり、自然演繹やシークエント計算には、証明のもつ仮定を操作することができるような推論規則が登場する。対してヒルベルト式には、このような規則は登場しない。というのも、ヒルベルト式においては、推論規則は「すでに証明に登場した命題から別の命題を証明に登場させる」という役割を果たす（ヒルベルト式における証明の定め方の三つ目の条項を参照)。つまり、ある仮定 Γ のもとでこれこれの式が証明されたなら、**同じ仮定** Γ のもとでどれどれの式を証明してよい、というのがヒルベルト式における推論規則の内容である。従って、仮定を操作することができないのである。

もう一つ、両者の違い、というより、自然演繹やシークエント計算の側の利点としてしばしば言及されるのは、推論規則の対称性である。自然演繹においては、それぞれの結合子について「上から下に結合子を登場させる」(「下から上に結合子を除去する」) I-rule と、「下から上に結合子を登場させる」(「上から下に結合子を除去する」) E-rule の二つが存在しており、つまり、ある種の対称性を持った二つのルールが個々の結合子に存在する。またシークエント計算では、$\vdash$ の右に作用する R-rule と、左に作用する L-rule という形で、やはり、左右に対称性を持った二つのルールが個々の結合子に存在する。このように、ルールの間にある種の対称性が存在することが自然演繹とシークエント計算の最大の特徴であり、結果として、証明の構造が数学的に（ないし哲学的に）興味深いものになっている。

ヒルベルト式と自然演繹・シークエント計算の間の特徴としては以上の三点が有名である。しかし、これらはどちらも、証明の形に起因する特徴とはいえない。なぜならまず前者の、「ヒルベルト式では推論規則が/自然演繹・シークエント計算では公理が少なくて済むことが多い」という方については、ヒルベルト式において自然演繹のような規則の形に関する理想（I-rule と E-rule の二種を個々の結合子に定める…というような）がない、ということに起因する特徴であると考えるべきであり、これは証明の形とは直接関係はない。「ヒルベルト式においては仮定の操作ができない/自然演繹やシークエント計算ではできる」という特徴も、証明の形というよりは、推論規則のもつ役割に起因することがらである。さらに、「自然演繹やシークエント計算ではルールの間に対称性が現れる」という方についても、ツリーという構造そのものと直に関係する特徴ではない。Logic of Paradox の自然演繹のように、ツリー構造を持っていても、こうした対称的な構造を持たない形式体系は存在するからである。「列」と「ツリー」という証明の形に注目するという本稿の趣旨を前提するならば、注目すべきは別のところである。

列構造を持つヒルベルト式に対して、ツリー構造を得たことによって自然演繹やシークエント計算が獲得した新たな特徴はなんだろうか。それは、どの式が推論のどのタイミングでどのように使われたかということが、図形的に明確化するということである。ヒルベルト式の体系においては、複数の命題を前提に単一の命題を結論する推論規則を使用する場合、前提になる命題は、結論になる命題よりも**前に**あればよかった。しかしこの場合、結論となる命題と使われた推論規則を見ても、**どれだけ前に**前提があるのかは直接わからない。これに対して、ツリー型の構造を持つ自然演繹やシークエント計算においては、複数の命題が前提となるケースであっても、前提はつねに結論の**直前**に登場する。従って、どの命題がどのタイミングでどんな推論規則によって使用されたのかということ、ひいては、推論のもつ論理的な構造が、図形的に明快に表示されることができる。

この結果として、自然演繹においては「証明図に対する操作」が直感的にイメージしやすいものになっているといえるだろう。例えば、次の図に表現されている証明図の

reduction という操作がある。

$$
\cfrac{\cfrac{\begin{array}{cc}\Pi_0 & \Pi_1 \\ A & B\end{array}}{A \wedge B}\,(\wedge I)}{\begin{array}{c}A \\ \Pi_2\end{array}}\,(\wedge E)
\quad \rightsquigarrow \quad
\begin{array}{c}\Pi_0 \\ A \\ \Pi_2\end{array}
$$

これは、証明図の中で $(\wedge I), (\wedge E)$ が連続的に適用されている部分について、図に表現されているような形で証明図を「切り貼り」することで、この連続的な適用を削除するという操作である。この図は、$(\wedge I)$ の二つの前提に至る推論 Π_0, Π_1 のうち、Π_1 を切り捨て、Π_0 の方を下の Π_2 とくっつける、という操作を表現している。

もしも列の形をした証明において、証明図に対する同様の操作を考えるとしよう。だがこの場合、まず推論規則 $(\wedge I)$ の前提 A, B、及びそこに至る推論 Π_0, Π_1 がどれだけ前に出てくるのかわからない。さらに、$(\wedge E)$ や Π_2 が $A \wedge B$ のどれだけ後にどのタイミングで現れるかもわからない。そのため、証明図の切り貼りを先に示したような図によって表現することは、不可能ではないにせよ、やや面倒になる。逆に言えば、ある推論規則の前提・結論に注目した証明図の切り貼りのような操作を図形的にイメージしやすいのが、ツリー型パラダイムの利点であるといえるだろう。

なお、列パラダイムにおいても、前提が結論の直前にだけ登場するように制約をかけることはできないだろうか？という疑問があるかもしれない。もしこれが可能であるのなら、ここで列パラダイムにはなくツリーパラダイムにある特徴として述べたことは、証明の形そのものに起因するというよりは、ヒルベルト式と自然演繹・シークエント計算という特定の定式化のあり方に起因するする特徴であるということになる。残念ながら、複数の前提を持つ推論規則を使用する限り、これは不可能である。というのも、前提を複数取る推論規則を適用する場合、どちらの前提も何らかの証明を経由して登場しているはずなので、この証明の分だけ二つの前提の間に距離が出てくる。そのため、片方の前提だけを結論の直前に置くことができたとしても、もう一方の前提が結論からどれだけ離れているかを指定することはできない。従って、MP を推論規則として認めるような通常のセッティングにおいては、列パラダイムにおいて「前提が結論の直前に登場しなければならない」という制約をかけることはできない。

1.4　列の逆襲——構造計算

ここまで、ヒルベルト式、自然演繹、シークエント計算の三つの体系を見る形で、「列」と「ツリー」という証明の形に関する二つのパラダイムを比較してきた。列パラダイムに比べてツリーパラダイムにおいては、命題がいつ、どこで、どのように使われたのか、図形的に明快に表示されることができる。

こう考えると、単純に証明の形だけ考えるなら、ツリーパラダイムの方が優れているのではないか、というふうに見えてくる。実際証明論において研究対象となっているのは、多くの場合ツリーパラダイムの体系である。しかしながら、ここまで述べてきた列パラダイムの問題点を（部分的に）解消しつつ、さらに、ヒルベルト式の体系では隠れていた列パラダイムのさらなる利点を明るみに出した体系が現在研究されている。それが構造計算 (calculus of structures) である。

構造計算は元々線形論理などとの関連で導入されたものであるが、ここではまず古典論

理の範囲内でもできる単純な議論でモチベーションを説明しよう*3。シークエント計算を思い出してほしい。シークエント計算には、個々の結合子についての L-rule や R-rule 以外に、公理と構造規則というものが存在する。ここで、公理である同一律と、構造規則であるカットを見てみよう。

$$\frac{}{A \vdash A}\,(identity) \quad \frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\,(cut)$$

古典論理においては、$A \vdash B$ と、$\vdash \neg A, B$ が同値である。この同値性を念頭に置いて上記の規則を書き直すと次のようになる。

$$\frac{}{\vdash A, \neg A}\,(identity') \quad \frac{\vdash A, \Gamma \qquad \vdash \neg A, \Gamma}{\vdash \Gamma}\,(cut')$$

このように書いてみると、カットと同一律の間にある対称性に気づかないだろうか。同一律は、上から下に向かって、命題とその否定を同時に導入する。逆にカットは、下から上に向かって、命題とその否定を同時に導入する規則である。この意味で同一律とカットは、対称的な側面を持つ規則である。

しかし、カットと同一律の間には完全な対称性があるわけではない。まず、カットに現れる Γ という文脈は、同一律の方には現れない。そしてもう一つより重要な難点として、同一律が枝分かれを含まないのに対して、カットが枝分かれを含む規則であるということがある。

しかし、この枝分かれはそんなに重要なことであろうか。カットにおいて前提が二股にわかれているのはつまるところ、「こうした前提が両方共同時に成り立っているとする」という意味であり、論理結合子の $\wedge$ と同等の意味を持つ。また、$\vdash$ の右側のカンマは、「右側の式のどれかが成り立つ」という意味であり、$\vee$ と同等の意味を持つ。そこで、証明の枝分かれや、シークエントに登場するカンマを全て結合子に書き直すと、次のようになる。

$$\frac{\vdash \Gamma}{\vdash (A \vee \neg A) \wedge \Gamma}\,(identity'') \quad \frac{\vdash (A \wedge \neg A) \vee \Gamma}{\vdash \Gamma}\,(cut'')$$

ここまでくると対称性はもう明らかであろう。つまり、この形にすると、カットと同一律は、$\neg A$ と A を逆転させ $\wedge$ と $\vee$ を逆転させ、最後に上下を逆転させただけの関係になる。このように、$\neg A$ と A、$\wedge$ と $\vee$ の間の逆転が絡む対称性のことを「双対性」と呼ぶが、カットと同一律は、上下に双対な規則であるということになる*4。

この発想を推し進め、シークエント計算をもとに、枝分かれ・カンマ・$\vdash$ の左右と言った要素を全て $\vee, \wedge, \neg$ を使って書き換えたものが構造計算である。構造計算の体系をきちんと定義するのもやはり面倒なのでここでは行わないが、規則の例を一つ挙げておこう。古典論理の構造計算*5には例えば次のようなスイッチ則が登場する。

$$\frac{\vdash S[((R \vee U) \wedge T)]}{\vdash S[((R \wedge T) \vee U)]}\,(\mathrm{switch})$$

これは、シークエントの一部に「$((R \vee U) \wedge T)$」という部分があれば、それを「$((R \wedge T) \vee U)$」

*3 以下の議論は [2] を元にしている。

*4 $(identitiy'')$ に突然 Γ が登場したのは何故か、という声があるかもしれない。だが、もともとシークエント計算における同一律は証明のどのタイミングでも使うことができるのだから、同一律が適用された後に枝分かれが起こることがありうる。同一律が適用された後、左や右に現れる枝別れを、$\wedge$ を使って同一律を適用している枝の中にまとめた結果が、この Γ であると理解してほしい。

*5 古典論理の構造計算の完全な定義は [2] を参照。

と書き換えてよい、という規則であり、もちろん古典論理において妥当な規則である。

シークエント計算の証明は全て構造計算の規則を使って書き換えることができる。たとえば、シークエント計算の $(\wedge R)$ の規則を使って書かれる証明は、構造計算では次のようにスイッチ則で書き換えることができる (なお構造計算では、$\wedge, \vee$ の結合法則・交換法則は明示せずに使用する)。

$$\dfrac{\Gamma_0 \vdash A, \Delta_0 \qquad \Gamma_1 \vdash B, \Delta_1}{\Gamma_0, \Gamma_1 \vdash A \wedge B, \Delta_0, \Delta_1} (\wedge R) \rightarrow \dfrac{\dfrac{\vdash (\neg\Gamma_0 \vee A \vee \Delta_0) \wedge (\neg\Gamma_1 \vee B \vee \Delta_1)}{\vdash ((\neg\Gamma_1 \vee B \vee \Delta_1) \wedge A) \vee \neg\Gamma_0 \vee \Delta_0} \text{(switch)}}{\vdash \neg\Gamma_0 \vee \neg\Gamma_1 \vee (B \wedge A) \vee \Delta_0 \vee \Delta_1} \text{(switch)}$$

「列」パラダイムと「ツリー」パラダイムの話に戻ろう。構造計算は枝分かれを排除するので、列の構造を持つ。つまり、構造計算は「列」パラダイムに基づく定式化である。

しかしながら、構造計算はシークエント計算をもとにしている体系であるため、ヒルベルト式にはなくシークエント計算にはあった特徴を保持している。推論規則がつねに直前の式だけに適用される、という特徴である。

先に、推論規則の前提が複数存在する場合には、列パラダイムですべての前提が直前に現れるように制約をかけることはできない、と述べた。だが構造計算の場合は、枝分かれを $\wedge$ で表現することによって、複数の前提を取るような推論規則も全て単一の前提を取る規則に変換することができる。そのため構造計算では、推論規則の前提は常に単一であるため、列パラダイムでありながら、推論規則が常に直前の式だけに適用されるように制約をかけることができるのである。

そして、構造計算は、ヒルベルト式では隠れていた、「列」パラダイムの特徴を浮かび上がらせる。それは、「ツリー」が上下非対称であるのに対し、「列」は**上下対称**であるという特徴である。ツリーは枝分かれがあるために上下非対称なので、ツリーパラダイムにおいては、証明や規則の間の上下の対称性は完全なものにはならない（同一律とカットを思い出してほしい)。これに対して、「列」は上下対称なので、上下の対称性は完全なものとなる。実際古典論理の構造計算においては、証明の上下をひっくり返し、$\vee$ と $\wedge$、$\neg A$ と A を逆転させても、やはり証明のままである。このような上下の双対性・対称性は、「列」パラダイムにおいて初めて可能なものである。

もちろん、構造計算と推論規則の定め方が異なっているヒルベルト式においては、証明をひっくり返しても証明のまま、ということはない。つまり、「列」パラダイムが持つ上下の対称性という特徴は、構造計算によって初めて利用・明示化されたものであると言える。

とすると、構造計算は一見、「ツリー」パラダイムと「列」のいいとこ取りをした最高の体系であるようにも思える。残念ながら、これは見かけだけのことにすぎない。というのも、構造計算が保持しているようにみえるツリーパラダイムの利点、「どの式が推論のどのタイミングでどのように使われたかということが明確化する」という特徴は、あくまで部分的なものにとどまっている。さらに、ツリーパラダイムやヒルベルト式では扱えるにもかかわらず、構造計算では扱えない推論規則がある。

確かに構造計算でもツリーパラダイムでも、推論規則はつねに直前の式だけに適用される。しかし、ツリーパラダイムに基づく体系において、推論規則は主結合子（もっとも外側に存在する論理結合子のこと。例えば $((A \vee (B \rightarrow \neg C)) \wedge D)$ の主結合子は $\wedge$）だけに作用する。これに対し、構造計算では、推論規則は主結合子以外の結合子にも作用する ($(switch), (cut''), (identity'')$ を参照)。そのため、推論規則が**直前の式**に作用した、とい

うことはわかるのだが、直前の式の**どの結合子**に作用したのか、というところまではわからない。構造計算ではカンマや枝分かれが全て結合子に変換されているので、そのことを念頭に置いてシークエント計算のセッティングで言い換えると、これはカンマや枝分かれによって分けられた式のうちどの式に規則が作用しているのかわからないという事態に相当する。もちろん、**直前の式の中に現れる結合子のどれか**に規則が作用しているということはわかるのだが、しかしシークエント計算や自然演繹に比べると、「どの式が推論のどのタイミングでどのように使われたかということが明確化する」という特徴は、完全に保持されているとは言えない[*6]。

さらに、枝分かれをなくすと同時に直前の式だけに規則の適用を限ったことによって、規則が前提をただ一つしか取れなくなってしまった。もちろん、前提が有限個しかない規則であれば、結合子で前提をつなげることによって前提を一つにまとめることができる。しかし、前提が無限個ある規則の場合、このトリックは使えない (無限の長さを持つ式は存在しないから)。従って例えば、算術の証明論で登場する ω-rule（$A(0), A(1), A(2)...$ という無限個の前提から、$\forall x A(x)$ を結論する規則）のような規則は、構造計算では定式化できない。無限個の前提をもつ規則を使うためには、枝分かれを回復するか、直前の式だけに前提を限るという限定を解除するかしなければならないが、枝分かれを回復すればツリーパラダイムとなるし、直前の式以外にも前提を取れるようにすればヒルベルト式と同様になってしまう。

1.5　まとめ——抽象化としての形式体系

以上、証明を列と捉える考え方と、ツリーと捉える考え方を比較してきた。結論だけまとめると、ツリーパラダイムでは、命題がいつどのように使われたのかということが図形的に明らかであるという利点があった。対して列パラダイムにおいては、上下に対称性が導入できることなどの利点があった。構造計算は両者の利点を保持しているような体系に見えるが、しかし、「命題がいつどのように使われたのかが明確である」という特徴はあくまで部分的にしか実現しておらず、さらに、無限の前提を持つ推論規則が扱えないという新たな問題点が生まれてしまっていた。

以上の議論から、冒頭に述べた「論理を定式化する方法は複数存在し、それぞれ異なった証明論的性質を持つ」というゲンツェンの洞察を、証明の形に注目する形で具体化することができただろう。現代の証明論においては、このゲンツェンの洞察のもとに、既存の体系にはない良い性質を持った論理の定式化を探す試みが行われている。例えば、ジラールの提案した証明網（proof nets) [5] は、証明を列でもツリーでもなく、グラフとして捉える新しいパラダイムであり、本稿で紹介した定式化にはない特徴を備えている。こうした探求はゲンツェンの発見なくしてありえないものであり、その意味で彼の洞察は、現代の証明論研究の基盤にある。

最後に、ゲンツェンの洞察を前提した時に現れてくる方法論的な問題を提起しておく。冒頭に、証明論は、数学的議論や論理的議論において登場する論理的推論を研究する分野である、と述べた。ここまでで明らかになったように、数学的議論や論理的議論に登場す

[*6] とはいえ、構造計算における証明論的な議論は、十分図像的にイメージしやすいものが多い。特に、[2] における古典論理の構造計算のカット除去定理は、自然演繹ともシークエント計算とも趣の異なる特徴的な証明図の切り貼りによって成立しており、見ていて非常に楽しい証明である。

る論理的推論は、それを数学的にどのように定式化するのかによって、全く異なる性質を見せる。すると、次のような疑問が生まれるかもしれない。こうした定式化のうち、**正しい**定式化はどれなのか。我々が行っている推論実践の性質を適切に反映しているのはどの定式化なのか。もっとはっきり言えば、我々が実際に行っている推論は列なのかツリーなのか。上下に対称なのか、非対称なのか。命題がいつ使われたのかどうかは推論の構造から明らかになるようなものなのだろうか。いやそもそも、列であるとかツリーであるとか、上下に非対称であるとかないとかというのは、我々の推論実践に内在する性質ではなく、それを証明論者が形式化する時に新しく現れた外的な性質であり、まったく人工的なものなのではないか？

私は（哲学者であるせいもあるが）こうした問題は考える価値があると思う。そして、ここでは詳しい議論はせず断言だけするが、私はどの定式化も**部分的に**正しいものである、と考えている。私が思うに、論理の様々な定式化は、社会科学における「理念型」や、経済学や自然科学における「モデル」のようなものである。つまり、現実に発生している事象のうち、余計な特徴は捨象した上で、いくつかの顕著な特徴に注目し、その特徴が引き立つような形で理論的に再構成された抽象的な構築物である。ここで、現実に発生している事象のうち、どの特徴に注目するべきかということに関しては、答えは一つではない。命題が推論においてどのタイミングで使われたのか、これを明示化し分析したいと望むなら、ツリー型の体系がモデルとして相応しい。推論に内在する上下の対称性を分析したいと望むなら、構造計算がよりよい体系となるだろう。つまり、様々な論理の定式化は、我々の複雑な推論実践の中のそれぞれ別の側面に注目した結果として立ち上がってくるものなのであって、どれか一つが特権的に実践を表象するというようなものではないのではないだろうか。

従って、証明論の研究を進めたり、勉強をしたりする上で念頭に置くべきは、どの定式化が**正しいか**ではなく、どの定式化が**どのような眼目を持っているのか**、ということである。その点を明らかにする上で、本稿で述べたような、証明の形に注目した視点は、一つ役に立つだろう。

参考文献

[1] 田中一之編 (2006)『ゲーデルと 20 世紀の論理学』第二巻、東京大学出版会

[2] Brünnler, K. 2006, "Deep Inference and Symmetry in Classical Proofs", PhD thesis, available on `http://cs.bath.ac.uk/ag/kai/phd.pdf`

[3] フレーゲ, G(1999)『概念記法』藤村龍雄訳、勁草書房

[4] Girard, J.-Y. 1989, Proofs and Types, Cambridge University Press.

[5] Girard, J.-Y. 1987, "Linear Logic", Theoretical Computer Science 50:1-102.

[6] Gentzen, G. 1935, "Untersuchungen über das logische schliessen", Mathematische Zeitschrift,39:176-210,405-431 translated in The Collected Papers of Gerhard

Gentzen(eds. Szabo).

[7] 岡本健吾 (2007)「数学基礎論の展開とその哲学」、『哲学の歴史』第十一巻（飯田隆編)、中央公論新社

[8] Zach, R. 2001, Hilbert's Finitism, PhD thesis, available on `http://people.ucalgary.ca/~rzach/static/hilbert.pdf`

第 2 章

評論　小島寛之の浅さと卑怯さ

淡中圏

2.1　introduction

日本の数学ライターとして小島寛之の名をまず挙げる人も多いのではないかと思う. 実際本はよく出ているし, そこから考えるによく売れているのだとも思われる.

しかし, 私はこの人の本に疑問がある.

疑問があるというのは, 内容が正しくないというより, 適切ではない, という意味だ.

間違ったことは書いていないのだが, 必ずしも論理的とは言いかねる自分の意見を通すために, あまり褒められないレトリックを弄しているように見える.

もし日本の読者にそのことを見破るだけの能力がないとしたら, それはとても困ったことに思える.

私は小島寛之の著作は正直なところ, 今回素材とする 2 冊しか読んでいないので, これだけで彼の物書きとしての実力を云々する気はない.

しかし今回紹介する 2 冊は明らかに問題を含んでいる.

そこで筆を取ることにした.

2.2　『数学で考える』の中の実数論に見る「浅さ」

この本,『数学で考える』(以下 [1]) は小島寛之が彼の専門である経済に主に絡めて数学の様々な話題について語った著作である. 村上春樹についても語っている（彼の文章, 数学的なんだってさ. へ〜っ）.

それを一つ一つ語っていては話題がばらけるので, その中から一つ, ４章の「偽装現実のテクノロジー　ワルラスの定理と実数の連続性」([1] ６３ページから) のの章を取り上げよう.

「偽装現実」という言葉で何を表しているかというと, 著作中の言葉を私なりに翻案するならば,

「数学の概念は, 必ずしも現実と一致しない《捏造》されたもの」

ということだと思われる.

そして小島寛之が数学を「偽装現実のテクノロジー」だと考えることで何を主張したい

のかというと,

「数学の概念自体は現実と一致しないとしても, それが現実との何らかの類似を持つことにより, 現実を理解するのに役に立つ」

ということであると私は読んだ.

そして, これ自体には私も同意したい. 実にまっとうな意見であると思う.

しかしそれを踏まえるからこそ, どういう意味で現実との類似を持つか（それは当然数学の外の話だ）, についてしっかり議論する必要がある.

たとえば現実のモデルを作って議論をするとき, モデルの評価基準は「現実と似ているかどうか」だけではない. そのモデルが「扱いやすいものかどうか」という重要な基準がある.

この二つの基準の間のトレードオフに対する意識が小島寛之には欠けているように見える, というのがこの節での私の批評の中心だ.

正確だが扱いにくいモデルは『フィネガンズ・ウェイク』と一緒で「現実を読み取った結果ではなく, 読み取るべき何か」になってしまい, 芸術ならともかく, 学問としてはあまり意味がない.

「科学とは街灯の下で鍵を探すようなもの」という言葉があるように, どうにもこうにも「我々に理解できそうなこと」から始めなくてはいけないのだ. もちろん, だからと言って「科学の目的は世界を理解することではない」と断ずるのは下司の勘繰り. 「科学とは街灯の下に街灯を立てるようなもの」. 扱いやすいところからはじめることによって, 扱いにくいところにも光が届くようにするのも大事な仕事だ.

しかしだからと言って扱いやすさだけを求めて, 現実との乖離が大きいモデルを, さも現実の似姿として細部を知らない非専門家に提出するのは不誠実というもの.

はっきり言って小島寛之はこの論考で, その罪を犯していると思う. ZFC の宇宙*1という強力すぎるモデルを, 細部を無視して経済学の正当化に使おうとするのは, 嘘とは言わないまでも, ある種の欺瞞に見える.

では本題に入ろう.

話はまず**中間値の定理**から始まる.

定理（中間値の定理）　関数 $f(x)$ を閉区間 $[a,b]$ で定義された連続な関数とする. このとき, $f(a)$ の値が負で $f(b)$ の値が正ならば, $f(c)=0$ をとなる c が開区間 (a,b) に存在する.([1] ６４ページより引用)

これは, x 軸の下からスタートした連続な曲線が, x 軸の上へ行くためには, x 軸と交わらなくてはいけない, と考えると（正確性はともかく）直感的にはよく分かる.

実に分かりやすく自然な定理だ.

ところが, この本では返す刀で次の定理を紹介する.

定理（不動点定理）　$D=\{x\in\mathbb{R}^n;|x|\leq 1\}$ として, 写像 $g(x)$ を, D から D への連続写像とする. このとき, ある点 c があって, $g(c)=c$ となる.([1] ６７ページの文章を短く書き直した)

この 2 次元版がいわゆる**ブラウアーの不動点定理**である.

---

*1 この同人誌の表紙にその絵が墨と筆で描いてあるので, どうかよくよく玩味していただきたい

そしてこの１次元版と中間値の定理は同値になる*2.

ここまではよい．ここからこの本では,「二次元以上の不動点定理も要は中間値の定理なのだ」という結論に導いていこうとする.

そこで二次元版のブラウアーの不動点定理の証明の大雑把な説明をしているのだが, 本質的にホモロジー論の話を, ホモロジーの言葉を明示的に使わずに展開している.

ちゃんと理解したければちゃんと初歩のホモロジー論の勉強をしたほうがいい気がする．お勧めはフルトンの『代数的位相幾何学入門』[3] だ．初歩から分かりやすく説明してある.

証明の概略に戻ると ([1] ６９ページから７２ページの証明のスケッチをさらに私なりに再構成した), まず, もし g に不動点がないとする．つまり**背理法**を使うのだ.

そうすると, x と $g(x)$ の値はいつも違うので, $g(x)$ から x へ向けての半直線が引け, それと単位円周との交点を $h(x)$ とすれば．連続関数 h（x を小さく動かすと, $h(x)$ も小さくしか動かない）が定義できることになる．．ここで x を半径 $l \leq 1$ の円周上一回転させる. このとき, $h(x)$ もスタート地点に戻ってくるはずなので, 整数回回転するはずである．その数を $r(l)$ とする．この r も連続関数である．そして $r(1)$ の値は単位円周上をただ一回転するだけなので, 1 である．さらに $r(0)$ はそもそも動かないので 0 である.

ところが r は定義より整数値しかとらない.

すると中間値の定理によれば, l は 1 と 0 の間で, 任意の中間値を取るはずである．これは矛盾．よって, 不動点は存在することが証明されたわけだ.

さて, この証明を読んで,「証明の鍵は中間値の定理だな」と思う人がどれだけいるであろうか.

私は最初に見たときそう思わなかったし, そう説明する数学の教師にも出会ったことはもない.

この証明の鍵は, 前半の背理法の仮定から, 回転数が well-defined であることを導くところだと思う.

特に「背理法を使っている」ということは重要だ．これによりどういう計算が行われているかが見えなくなる.

中間値の定理の証明の場合, どんな計算しているかは見て明らかだ．区間を２つに分け, 中間地点での関数の値が正か負かで, 区間を縮めていけばいい（**区間縮小法**）. *3それによって, 中間値をとる点へ収束するコーシー列が計算できるので, 中間値の存在が証明できる.

つまり, 中間値の定理は, 中間値をとる点を計算することによって証明できるのだ. *4

---

*2 $g(x) = f(x) - x$ として, g に中間値の定理を適用すると１次元の不動点定理が出てくる．逆もほぼ同様

*3 もちろん値が 0 ならそこで終了

*4 どうやって, 値が正か負か決めるの？ という疑問を持った人は偉い! 実はごまかしを糾弾するはずが、自分でごまかしちゃってるんだよね．政治的ではないけど．もし「値は必ず正か負か 0 か」なんて言おうものなら, それは**排中律**で, 背理法とほぼ同じ．構成的解析学では, 中間値の定理すら証明できないのはここに起因する．ただそれは「全ての関数」を考えるからで, この「全て」がどんな領域なのかも文脈依存だ．あくまで非形式的に,「私たちが数学するとき, なにしてるか」に則って考えれば, 関数とは任意の関数なんかではなく, 計算機で近似可能な実数での値くらいは計算機で近似可能なものだと思いたい．例えば有理係数の有理関数で, 区間の端点が有理数なら, その中点での値の符号は代入すれば分かる．もう少し複雑な関数でも同様．文中で言いたい「計算の仕方が分かる」とはこのくらいの意味だ．背理法の有無という形式的区別とは決して一致しない概念ではあるが, 背理法は分岐点の目印にはなる．要は背理法をどう使っているかだ．そしてこの非形式的で直感的な区別が, 先ほどの「すべての関数」や「すべての実数」の領域をどう絞るかによって, ある程度正当化できる, という話をこの後する.

しかし，2 次元以上の不動点定理はそうではない．先ほどの証明からは，背理法を使ってしまっている時点で，（ブラウアーには悪いが）実際に不動点を計算していく方法は分からない．

これを，「二次元以上の不動点定理も要は中間値の定理」と言い切ってしまうことは大いに問題がある．

そしてこの本はそれにどんどん問題のある記述を重ねていく．中間値の定理こそ，実数の連続性の要であり，その他の実数の連続性の表現，例えば**ボルツァーノ・ワイエルシュトラスの定理**もこれと同値なのだ，というのだ．

定理（ボルツァーノ・ワイエルシュトラスの定理） 有界な実数列は収束部分列を持つ.([1] 内では「公理」と表現される)

これは，なかなかすごいね．

だって，この定理，実際にそういう実数列が与えられたとして，どういう部分列を選ぶのか，全然分からないんだもの．計算可能性の見えなさでは，二次元の不動点定理以上だ．

いったい何が問題なのかというと，小島寛之がここで「同値」と言っているのは，いったいどういう仮定の下で同値なのか，いまいち明らかではないことだ．

おそらく ZFC が仮定されているのだろう．そしたらここで言っていることは，とりあえず間違いじゃない．

しかしそれを黙ってみていられるのは，数学内部で収まっているときだけで，これが数学の外部と関係しようとするならば，とても看過しえないことになる．

この本では，実はこの一般次元の不動点定理が，資本主義経済つまり，自分の効用を追及する消費者と自分の利潤を追求する企業が調停者もなく勝手に動いている経済システムで，みんなが納得する価格付けが存在するよ，という定理「**ワルラスの一般均衡定理**」の証明に使われる，という話になっている．実際問題設定の仕方を見れば，かなり明らかな話だ.([1] の７３ページから７４ページに説明が載っている．ここでは詳しい話は省略する)

そして，これが要は中間値の定理から来てるんだよね，という議論になっているのだ．

そんな馬鹿な，である．

中間値の定理という計算するだけで証明できる，実に手軽で直感的な定理だけで経済が基礎づけされていると，ZFC という超強力な道具を隠したまま一般人に信じさせようとするのは，あきらかな印象操作だ．

お前はブルジョア経済学者か，と言いたい．経済学者の仕事は，愚かな民衆に今の経済システムこそが唯一のものだと信じさせることで，今の経済システムを安定させようとすることなのか？[*5]

しかも逆に考えるなら，もしこの議論だと，ワルラスの一般均衡定理が正しいことを信じるには ZFC を信じることが必要になってしまうではないか．キューバ亡命不可避．そんな経済システム私はいやだ．

しかし安心してよい．

この手の「実数の連続性」の公理の強さを，もっときめ細かに調べる技術は今どんどん発達している．その一つが**逆数学**と言われる分野だ．

例えば逆数学の初歩によれば，計算可能な実数の存在だけを仮定する公理 RCA_0 でも，

[*5] 本当にそうだったら，ごめんなさい

中間値の定理は証明できる．しかし，2 次元以上の不動点定理は証明できないのだ．これは先ほど直感的にした説明と一致している．

当然, この段階ではワルラスの定理は証明できない．ここまで見ると, 小島寛之の議論の乱暴さがあらわになるだろう．

この公理に**弱ケーニヒの補題**, つまり「すべての無限二分木は無限路を持つ」という公理（非常に弱い選択公理）を付け加えると, なんと任意次元の不動点定理を証明できる．

これならワルラスの定理も証明できる．

つまり, 資本主義の安定性を信じるには, だいたい「すべての無限二分木は無限路を持つ」ことを信じればいいわけだ．これはそんなに困難なことではなさそうに思える．

さらにこれに弱でないケーニヒの定理, 「すべての枝分かれが有限な無限木は無限路を持つ」を加えて, 初めてボルツァーノ・ワイエルシュトラスの定理が証明できるのだ．

ZFC は強すぎて, これらの違いがすべて塗りつぶされてしまっていたのだ．

数学をするのにもフルに使うことはほとんどないくらい ZFC は超強力だ．そんなものを経済学の基礎づけに使おうとするなんて, 狂気の沙汰．

おそらく一番の問題なのは, 小島寛之が「自分の議論の仮定はなんなのか？」ということに充分意識的になれなかったことではなかろうか．論理学で一番重要なのは, 議論が上手になることではなく, どんなときでも議論の仮定は何か, 議論の形式は何か, ということに意識的になれることである．それによって, 議論がかみ合わない時に, 互いの共通地点まで戻ってそこからもう一度議論を組み立てなおすことができるのだ．

例えば今回で言うと, 背理法という形式が出てきたら必ず注意すべきだし, 「同値」という言葉にも「どんな仮定の下で同値なのか」と必ず問うべきだ．

その基本がなっていない以上, 論理的を装っているだけとしか言いようがない．

そのことに腹を立てながら他の章を読んでいた時に大変なことに気が付いた．これより後に収録されている『「知っていることを知っている」のトポロジー』の参考文献に田中一之『数の体系と超準モデル』[4] が「基礎論の勉強に最適」などという文句で紹介されているのだ．この本には上で説明した逆数学の初歩がまさに説明されているのだが．本当にちゃんと読んだのか？時系列的にこちらを書いた時が後とはいえ, ゲラを読み直してる時に気づかなかったのか．

私たちだって参考文献に書いてあることを隅から隅まで理解したり読んだりしているわけではないことくらい分かっているが, それでも参考文献に書こうとしていることに関係することがまだ書いてないかチェックするし, 参考文献にそれを否定することが書いてあったら, 内容について大きな疑義がでるのは当然だ．

逆数学を部分的にでも知っていて, こんな乱暴な議論を公表したのなら, ますます罪は重いと言える．

2.3 『数学でつまずくのはなぜか』の中の卑怯なレトリック

次に俎上に載せる『数学でつまずくのはなぜか』(以下 [2]), もう少し一般向けの著作である．

著者が塾などで教えた経験から得た知見や経験則を主に書いており, その中には聞くべき意見も多いと感じた．初等幾何で証明を教えるのは間違い, という話は私もまったくその通りだと思うし, 証明はもっと形式的に行うべきというのも肯える．

しかしウィトゲンシュタインなどを引用し始めたり, フレーゲやラッセルやデデキントなど,「数学の危機」の歴史的な経緯について書き始めると, とたんに著者の経験的な裏付けが消え, ペダンチックなおしゃべりとロマンチックな思い込みにあふれた香ばしい文章になっていく.

いろいろ言いたいことはあるが, この本も雑多な話題を取り扱っているので, やはり一点に絞りたい.

アフォーダンスについてだ.

アフォーダンスとは, 認知科学から出てきた考え方で, 様々な生物の活動の原因を生物ではなく, 外部の環境に見ようとするものである. 例えば, ある種の動物が泳げることを, その動物の「泳ぐことができる」能力ではなく, 水の「その中を泳げる特性」により注目して説明しようとするものだ.

他の例もあげると, 脊椎動物の目と節足動物の目はずいぶん違う. 片方は凹であり, もう片方はなんと凸だ. その間に共通点を調べようとしても, 相違点がどうしても目立つ. どうしてどちらも,「目」と呼べるのか. どうしてどちらも,「見ている」と言えるのか.

もし, 我々の目の構造から「見る」ことを定義しようとするならば, 節足動物たちはあの大きな目でものを見ていないことになりかねない. しかし, 両方の特性を取り込んだとしても, いつ何時宇宙から我々が思いもよらなかったやり方で「ものを見る」存在がやってくるとも限らない.

それならば, 外部の世界に「見られる性質」があるとし, 我々はそれを様々なやり方で取り出し利用している, と考えたらどうか, というのがアフォーダンスの肝だ.

多くの人はこれが「単なる言い換え」に見えるだろう. 実際これは「言い換え」である. しかし「単なる言い換え」ではない.

この概念の重要さは, 人工知能研究などをするときに, 我々が陥りやすい間違いに気づかせてくれることにある. 初期の人工知能研究は行動決定を全て知能の内部で行おうとした. すると我々は行動を決定するために, 世界のモデルをそのまま脳の中に持っていなくてはいけないことになる. そんなことはとても不可能だ, というのがなかなかわからなかったのだ.

実際我々が行っているのは, 様々なものを外部に投げ出してしまっているのだ. 例えば歩くときに, 足の動かし方をいちいち計算していない. ただ前に放り出すと重力がかってに足をおろしてくれる. うまくいくやり方はちょっとしたフィードバックですぐに見つかる.

谷の一番底を見つけたければ, 谷の輪郭を計算するのではなく, ただ石を投げて落ちていくところを見つければいいのだ.

つまり, 人工知能を開発しようとするならば, それは世界と繋がりを持つ必要があり, つまり何らかの肉体が必要なのだ, ということをアフォーダンスの考え方は教えてくれる.

我々が神のごとく明晰な存在なら, すべての言い換えは単に無意味だ. 数学の証明だって単なるトートロジーだろう. しかし, 我々は神ではない. ある方向から見ていると見えないものが, 別の方向からは見えることがある. そういう意味で, 言い換えは大きな意味を持ちうるのだ.

では, この著作ではアフォーダンスはどのように使われているのか？

引用してみよう.([2] ３６ページ８行目から３７ページ１０行目まで)

> 自然や社会の特定の事物たちには,「数理的に表現できる」という性質が備わっているのではあるまいか. そして数学認識とは, このような「数理的に表現できる」という環境の持つ性質を受け取る感覚器官だと考えることはできないだろうか.
> ……(中略)……
> このように考えれば, たいていの子どもが数学に熟達できることも納得できる. それは教師たちに教えられたからでも, 自分でがんばって適応したからでもなく, 事物からそれをアフォードされるからなのである. この仮説が正しいなら, 動物の眼の多様さと同じように,「数理的に表現できる」という性質を受け取る感覚器も多様であっていいはずだ. つまり,「数理的なものごと」のわかり方, 受け取り方は多様にある, ということなのだ.
> このようなアフォーダンス的な見方に立脚すれば,「数学ができる子・できない子」のような分類に, ほとんど意味がないことに気づくだろう. なぜなら「能力」は人の側ではなく, 事物の側にあるからだ. 学習障害や知的障害は,「健常者に共通する感覚器からは数学を受け取ることはできない」ということを意味しているにすぎない. 決して数理的なものごとの受容の完全な欠如を意味しているわけではないのだ. 教育者は, 自分の(数理的)感覚器を普遍的なものと思いこまず, 子どもの側だけではなく事物の側にも備わるアフォーダンスのあり方にも注意を払うべきなのである.

さてこの文章を読んだ私は, 結局何をすればいいのだろうか？正直この記述からは何も分からない.

だいたいこの理屈だと「泳げる子・泳げない子」のような分類にもほとんど意味がないことになりはしないか？

自分の書くことに反例がないかくらい気にしてほしい.

いったい教師は彼の数理的感覚器を超えて, どのように事物に備わるアフォーダンスにアクセスすることができるのか. 我々は自分の眼を信頼するからこそ, 昆虫もものが見えているとわかるし, ある種の動物には目が見えないことを理解できるのだ. あ, そうか, 目が見える・見えないという分類にもほとんど意味がないのか.

じゃあ, やっぱり結局どうすりゃいいんだよ！？

そもそもアフォーダンスの言い換えが, ここで何か論理的に意味のある効果を発しているだろうか. つまり言い換える前にはなかった情報がここに付け加わっているか？

ない.

なんにもない.

言い換える前に戻すと,「この子には我々と同じ数学的能力は持っていませんが, それとは別の数学的能力を持っているかもしれないので, 心配いりません」となるだけだ. 親への慰めか何かだろうか.

この言い換えが効果を発するとしたら, ロジックではなく, レトリックのレベルでのことだ.

実際これはレトリックの定番の一つ「よく分からない言葉で相手を煙に巻いて思考力を鈍らせる. 難しい専門用語で権威付けをして信用させる」という戦略だ. それによって, 普通に言うと納得してくれない親が,「なんだか分からないけどうちの子どもは大丈夫だ」と納得して帰ってくれるかもしれない. 素晴らしいね. でもこの本に書くべき話か.

この本はこの手の, 本来一般向けとはいえ学術的な書籍には似つかわしくない, 卑怯なレトリックに満ちている.

しかも読み手の多くはその手のレトリックを見破る訓練を受けていないがために, 何の警戒感もなく受け入れてしまっているようだ. これは困ったことだ.

卑怯なレトリックはサマンサ・アビールの話で最高潮に達する.([2] １６３ページから)

詩人である彼女は『１３歳の冬, 誰にも言えなかったこと　ある学習障害の少女の手記』という本で, 時計を読むことや計算をすることに非常な困難を持つことを告白した. 数を数えることはできるのに, 数えるという行為から「数」という概念を抽象することができず, 当然簡単な計算や, 数の大小の比較もできないというのだ.

そういう人がいることは事実であり, 脳がどのように数を認識しているのかを考えるうえで興味深いし, 計算をすることに多大な困難を抱えているからと言って, 知能に問題があるとは限らないことを示すうえでも面白い.

しかし小島寛之はここから自分で「独善的」と断って（これ自体批判しにくくする卑怯なレトリックだ）, 独善的というよりでたらめなことを書き始める. ([2] １６９ページ８行目から１３行目)

> 筆者は, 彼女の本を読みながら, その文体のなかに, 独特の「数理性」を感じ取った. 詩人であるにもかかわらず, その文章は, 情緒的なものというよりはむしろ, 非常に論理的なものであった. 彼女の詩のほうも, 修辞や韻や特殊な語感を駆使する「ことば遊び」というタイプではなく, 逆に, 独特な論理による「世界の描写」だ. だから筆者には, 彼女の脳は普通の人とは違う形式で,「世界の数理性」を感じとっているように思えてならない.

詩人だから情緒的, という決めつけにも辟易がするが, 論理的だから数学的, というのは本当にラッセルとかフレーゲとかについて少しでも読んだのか, と言いたい. 論理と数学が同じだったら, 逆にフレーゲがやろうとしたことはなんだったんだ？

あと, 修辞や韻や語感を駆使する「ことば遊び」が数学的ではないと思わせかねない文章もいかがなものか. ルイス・キャロルって知ってる？

この文章はさらにこう続く. ここからは怒りを抑えることが不可能だ.([2] １６９ページ１４行目から１７０ページ５行目)

> もちろん, このような言説を否定する読者もいるだろう. 数の加減もできず, 方程式も解けないような人間に「数理性」などあるはずがない, 買いかぶりか, 妄想だ, そう言うかもしれない. 筆者はそのような批判に抗する理屈は持ち合わせていない. ただ, そういう人にはこういう風にだけ答えておきたい,
>
> あなたは, 昆虫の眼は人間とは全く異なるから, 昆虫は世界の情景を見ていない, きっと, そう言うことだろう. 本当にそうだろうか. 筆者は, 昆虫も別の方法で, 世界のあるべき姿を見ていて, 人間が見ている姿も, 昆虫が見ている姿も, どちらも世界の発している本当の姿なのじゃないかと思う.

卑怯なレトリックの見本市の様相を呈してきたぞ.

まず,「買いかぶりだ, 妄想だ」とこちらが言うであろう言葉を少しずつ乱暴な言葉にずらすのはやめろ.

「妄想だ」なんて言わない. 「間違いだ」というだけだ.

しかし,「あなたはくそみそにいうかもしれないが」とか「あなたは馬鹿にするかもしれないが」などといわれると人はどうしても「そこまで言う気はないよ」と譲歩から入ってしまう. もしそのまま反論しようものなら, 相手が言う通りのひどいことをしているように他人からも, それどころか自分からも思われてしまうからだ.

自分の反論者を人でなしに見せる, よく使われる(無意識な場合も多い)テクニックだ.

「筆者はそのような批判に抗する理屈は持ち合わせていない」などと偽の譲歩をするのもむかつく. どうしても議論においては, 相手が譲歩をすると, こちらも何か譲歩できないかという心情が動きがちだ. しかし実際にはなんの譲歩もしてない連中が多い.

「あなたは, 昆虫の眼は人間とは全く異なるから, 昆虫は世界の情景を見ていない, きっと, そういうことだろう」

そんなこと言いません. 勝手に決めつけるな.

要は自分の言説を否定するものは, こういうことを主張していることになるのだぞ, と脅しているわけだが, どう考えたらそんな結論になるのか.

昆虫はどう見たってものを見ている. 一見ものを見ていないように見える生物ももしかしたら, 我々の知らないやり方でものを見ているかもしれない. しかし, いろいろと観察をした結果, たぶんものを見ていないであろう生物を, ものを見ていないと判断することになんの問題があろうか.

小島寛之が彼女に数学的能力を与えたがるのは, 論理と数学の混同によるが, この彼女が我々の知る数学ができないことを, 数学的能力がないことの証拠としてなにが悪いのだろうか.

まとめてみよう. 我々の持っているものとは「別の数学的能力」の存在を仮定するのはいいにしても, 何か具体的な例[*6]を出してくれなければ, 結局我々は「我々の数学的能力」を基準に考えるしかない. この「健全な自文化中心主義」を否定しておいて, なお「別の数学的能力」の例も出してくれないなら, それは空論以外の何物でもない.

逆に考えるなら小島寛之は, なぜそこまでの空論を弄してまで, 彼女に数学的能力を付加したがるのか. 数学的能力のあるなしに, 変に重きを置きすぎているのではなかろうか. 数学的能力がないことは, たしかに現代社会を生きるうえでいろいろ困るが, それで人生終わりというような悲劇ではないのに.

手足がなかったり, 生まれつき目が見えなかったりするのと同じ, 時々ある不幸の一つだ.

それとも小島寛之は視覚障碍者が目が見えないこと, 一見手足がないように見える人たちの手足が本当にないことも, 否定する気なのか.

「情景」とか「本当の姿」とかセンチメンタルな多元主義とかで, 論理の弱点をごまかそうとする態度に本当に腹が立つ.

ここ以外にもロマンチックなことを書いてごまかそうという雰囲気がこの本には満ち満ちている. 本の最後近くにある次の文章など最たるものだ.

そこで著者は, デデキントが無限集合を「自らの中への単射を持つ集合」と定義し,「対象 x」から「対象 x に関する思考」への中への単射を構成することにより, すべての対象

[*6] 視覚における「昆虫の視覚」の例は, 我々の持つ視覚とはずいぶん違うかもしれないが, それが視覚だということを我々は容易に同意できる. 同様に, それが数学的能力だと我々が容易に同意できるにもかかわらず, 何らかの点で, それまで我々が数学的能力に必要不可欠だと考えていたものに欠けるようなものが必要だ.

の集合は無限であることを示そうとしたことを踏まえて[*7], 次のように書く.([2] ２２７ページ５行目から９行目)

> こどもたちが自然数を理解できるのは, 自然数の源が, そもそもこどもたちのなかにあり, しかもそれは「無限」という実在だからだ. そして, それは人間がものを考え, ものを考えることを考え, ものを考えることを考えることを考える, そういうことができるからなのだ.
>
> 数と無限の深遠は, 他ならない, こどもたちの, そしてわたしたちのなかにある.

最初の方でウィトゲンシュタインの直感主義的数学観を紹介しておいてこれかよ, というのもあるが, なによりこの文章, アフォーダンスを全否定している気がするのだがいいのか？「数理性」の根源は我々の外部の世界にあると言ったかと思ったら, 今度は我々の内部にあると言う. 矛盾はなはだしい. しかも今度は参考文献どころか, その本の中でだぞ？編集者は読んでないのか？下読みをしてくれる友達はいないのか？

ここまで付き合った結果, 怒りを超えて, 私はへなへなと崩れ落ちるのだった.

怒っても無駄だわ, これは.

小島先生, 私はあなたの数学的能力に関しては全く知りませんが, とにかくあなたの文章には何の論理性も感じられませんでした.

2.4　提言: 日本語教育に論理学と修辞学を

さて今回紹介した二つの本に共通する病根は, 論理の破綻と, レトリックによるごまかしである. そしてこれは, 現代日本の教育における病根に繋がっている気がする.

結局, 日本の教育で, 論理学と修辞学に長いこと重きを置かれなかったのが, このようなものが世にはびこっていることの一つの原因だと思いたくなるのだ.

私は小説をよく読んだり書いたりする関係でレトリックには敏感だが, 多くの人はそうではないのだ. さらに小島寛之も同じ間違いを犯していることをすでに指摘したが, 論理を数学の一部と勘違いする人間も多い. 小説を書く身としては, 論理がなくてどうやって小説内の事実を組み立てていけばいいのか. 論理とは論証についての学問であり, 言葉をどう使うかの問題である以上, 「まさに文系」という学問なのだ.

知り合いで, 文学部で修士まで学んだにも関わらず, 私が「論理的に話してよ」と言ったら「文系だから無理」と言い放った馬鹿がいるが, あいつはどうやって論文を書くつもりだったのだろう. 「信じてください」とでもいうつもりか. あほか.

そもそも論を行うならば, 論理学も修辞学も説得の技法のはずだ. 大雑把に言うと, 理性に訴えるのが論理学, 感情に訴えるのが修辞学である. さらに論理学には, 形式・非形式の二つがあり, 必然性を扱う演繹論理学と, 蓋然性を扱う帰納論理学という風にも分けられる. 形式演繹論理学が要は形式論理学で, 非形式演繹論理学がそれを踏まえた弁論行為と言えるだろう. 対して形式帰納論理学とはおそらく統計学のことで, 非形式帰納論理学とは統計データを使ったプレゼンを意味するといえる. さらに, 様々な議論の失敗について議論する**虚偽論**も重要だ. 現代哲学の進むべき道ではないか, と考えている.

これらはあくまで言葉を使って, 相手をどう説得するのかなのだから, 日本語教育の時

[*7] ちなみに, この議論をまともに受け取っている数学者は（哲学者すらも）いない.

間にやるべきだろう．数学の中で証明を最初に学ばせるのは間違いだ．数学のなかで最初に出会うから「証明とか自分たちとは何の関係もない」という恐ろしく間違った印象を子どもたちに与えてしまうのだ.

日本語の時間に, 形式論理学からきちんとやってほしい．文学教育をしている時間は残念ながら少なくなるだろうけどね.

さらに数学の授業で統計学をやるなら, そのプレゼンまで持ち込まないと, なんの意味もないこともよく言われることだが, 重ねて指摘しておく．今のままではそもそも何を目的に統計をやるのか全く分からない．やはり日本語教育との連携が望まれる.

そしてそれらが修辞学と地続きであることを, 説得の演習の中できちんと理解させる必要がある.

あまりにレトリックに免疫のない国民は民主主義の根幹にかかわる問題だ.

「《まず足を踏んづけてびっくりさせる法》を使って, このオレンジがみかんであることを説得せよ」などの課題をこなすことにより, 現実世界で使える様々な卑怯な手口を学び, 同時にそれを使うのが似つかわしくない場所（アカデミズムとか, 日常の友達関係とか）もあることを実感, そしてそういう場所で相手が卑怯な手を使ったときは, 敏感に察知できるようにしたいものだ.

そうすれば世の中も多少ましになるかもしれない.

参考文献

[1] 小島寛之 (2007)『数学で考える』, 青土社.
[2] 小島寛之 (2008)『数学でつまずくのはなぜか』, 講談社現代新書.
[3] W. フルトン, 三村護訳 (2012)『代数的位相幾何学入門 (上下)』, 丸善出版.
[4] 田中一之 (2002)『数の体系と超準モデル』, 裳華房.

第 3 章

Grothendieck トポスの基本性質に関するノート

古賀 実

このノートは，Grothendieck 位相の入った圏であるサイト（site）上の層に関する理論の基礎を述べた，Mac Lane と Moerdijk による Sheaves in Geometry and Logic [2] の第 III 章 6 節 First Properties of the Category of Sheaves, 7 節 Subobject Classifiers for Sites と 8 節 Subsheaves の定義と定理を述べ，証明の行間を淡々と埋めた物です．第 6,7 節では，サイト上の層がなす圏（Grothendieck トポス）が，有限極限（finite limit）と有限余極限（finite colimit），冪乗（exponential）と部分対象分類子（subobject classifier）をもつこと，すなわち，初等トポス（elementary topos）であることが示されます．特に第 7 節では，ある層の部分対象が再び層であるための有用な必要十分条件を与えます．また，部分対象分類子の存在の応用として，層の間の自然変換がエピ射（epimorphism）であるための必要十分条件「local surjectivity」が与えられます．前者は，第 8 節で部分層（Subsheaves）を調べるために有用で，後者は，圏が Grothendieck トポスであるための「代数的」な必要十分条件を与える Giraud の定理の証明に使われます．

本は紙面の都合上細々とした事実の証明に頁を割けず，証明なしに主張が述べられている事がしばしばあります．このノートがそのような行間を埋め，理解の一助となれば幸いです．

尚，圏論に関する前提知識は Mac Lane による Categories for the Working Mathematician [1] と C87 で頒布した「The Dark Side of Forcing IV」の第三章「Grothendieck 位相・サイト上の層・層化関手に関するノート」を想定しています．上記のノートは以下の Web サイトから入手できます[*1]：`http://forcing.nagoya/`

ノートの本文は英語で書かれていますが，これは洋書である原書の形式・言葉遣いに合わせるためです．

[*1] C87 で頒布したものに含まれていた誤植を訂正しました．また，一部表現を変更した箇所がありますが，定義・定理の内容や証明の流れは変更していません．

3.1 First Properties of the Category of Sheaves

Let $(\mathbf{C}, J)$ be a site. Then for the inclusion functor $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, there exists a left exact left adjoint $\mathbf{a}$ (see [3, Theorem 3.3.1]), i.e.,

$$\begin{tikzcd} \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \arrow[r, shift left, "\mathbf{a}"] \arrow[r, phantom, "\perp"] & \mathrm{Sh}(\mathbf{C}, J). \arrow[l, shift left, "i"] \end{tikzcd}$$

The aim of the succeeding two sections is to prove the following theorem:

Theorem 3.1.1. *The category* $\mathrm{Sh}(\mathbf{C}, J)$ *of sheaves on a site* $(\mathbf{C}, J)$ *is an elementary topos, i.e.,*

(i) $\mathrm{Sh}(\mathbf{C}, J)$ *has finite limits and finite colimits;*
(ii) $\mathrm{Sh}(\mathbf{C}, J)$ *has exponentials;*
(iii) $\mathrm{Sh}(\mathbf{C}, J)$ *has a subobject classifier.* □

Lemma 3.1.1. $\mathrm{Sh}(\mathbf{C}, J)$ *has limits and colimits.* □

Proof. Let $\{F_j\}_{j\in I}$ be a diagram in $\mathrm{Sh}(\mathbf{C}, J)$. Then $\{i(F_j)\}_{j\in I}$ is a diagram in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Since $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is complete, there exists the limit $\varprojlim_{j\in I} i(F_j) = \varprojlim_{j\in I} F_j$ in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. By [3, Lemma 3.2.1], $\varprojlim_{j\in I} F_j \in \mathrm{Sh}(\mathbf{C}, J)$. Therefore, $\mathrm{Sh}(\mathbf{C}, J)$ has limits.

Similarly, let $\{F_j\}_{j\in I}$ be a diagram in $\mathrm{Sh}(\mathbf{C}, J)$. Then $\{i(F_j)\}_{j\in I}$ is a diagram in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Since $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is cocomplete, there exists the colimit $\varinjlim_{j\in I} i(F_j) \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Since the associated sheaf functor $\mathbf{a}$ has the right adjoint i, $\mathbf{a}$ preserves colimits. Moreover, by [3, Corollary 3.3.1], $\mathbf{a}i$ is naturally isomorphic to $\mathrm{id}_{\mathrm{Sh}(\mathbf{C},J)}$. Thus, we have

$$\begin{aligned} \mathrm{Sh}(\mathbf{C}, J) \ni \mathbf{a}(\varinjlim_{j\in I} i(F_j)) &\cong \varinjlim_{j\in I} \mathbf{a}i(F_j) \\ &\cong \varinjlim_{j\in I} F_j. \end{aligned}$$

Therefore, there exists the colimit $\varinjlim_{j\in I} F_j$ in $\mathrm{Sh}(\mathbf{C}, J)$. The proof is complete. ■

Fact 3.1.1. *Let* $\phi : F \to G$ *be a natural transformation. Then* ϕ *is a monomorphism in* $\mathrm{Sh}(\mathbf{C}, J)$ *iff* ϕ *is a monomorphism in* $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. □

Proof. (⇒) Let ϕ be a monomorphism in $\mathrm{Sh}(\mathbf{C}, J)$. Note that ϕ in $\mathrm{Sh}(\mathbf{C}, J)$ is a monomorphism iff the following diagram is a pullback square in $\mathrm{Sh}(\mathbf{C}, J)$:

$$\begin{tikzcd} F \arrow[r, "\mathrm{id}_F"] \arrow[d, "\mathrm{id}_F"'] \arrow[dr, phantom, "\text{p.b.}"] & F \arrow[d, "\phi"] \\ F \arrow[r, "\phi"'] & G. \end{tikzcd}$$

Since the inclusion functor i has a left adjoint, i preserves limits, in particular, pullbacks. Hence, ϕ is a monomorphism in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$.

(⇐) Conversely, let ϕ be a monomorphism in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ and $\psi_1, \psi_2 : E \to F$ two natural transformations in $\mathrm{Sh}(\mathbf{C}, J)$ such that $\phi\psi_1 = \phi\psi_2$. Note that ψ_1 and ψ_2

are, in particular, natural transformations in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Since ϕ is a monomorphism in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, we have $\psi_1 = \psi_2$. This implies that ϕ is a monomorphism in $\mathrm{Sh}(\mathbf{C}, J)$.

The proof is complete. ■

Next, we shall show that $\mathrm{Sh}(\mathbf{C}, J)$ has exponentials. Before proceeding, we observe that if exponentials were to exist for all $F, G \in \mathrm{Sh}(\mathbf{C}, J)$, then they are constructed by the same way as is the case for presheaves, i.e.,

$$i(F^G) \cong i(F)^{i(G)}.$$

In fact, for all $P \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, we have the following natural bijections:

$$\begin{array}{c} P \to i(F^G) \\ \hline \mathbf{a}(P) \to F^G \\ \hline \mathbf{a}(P) \times G \to F \\ \hline \mathbf{a}(P) \times \mathbf{a}i(G) \to F \\ \hline \mathbf{a}(P \times i(G)) \to F \\ \hline P \times i(G) \to i(F) \\ \hline P \to i(F)^{i(G)}, \end{array}$$

since $\mathbf{a}$ is the left exact left adjoint of i, and by the definition of exponentials and $\mathbf{a}i \cong \mathrm{id}_{\mathrm{Sh}(\mathbf{C},J)}$ ([3, Corollary 3.3.1]).

Recall that $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ has exponentials.

Lemma 3.1.2. *Let P be a presheaf on $\mathbf{C}$ and F a sheaf on $(\mathbf{C}, J)$. Then the exponential F^P in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is a sheaf on $(\mathbf{C}, J)$.* □

Proof. Recall that the exponential $F^P \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is defined as

$$F^P(C) = \mathrm{Hom}_{\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}}(\mathbf{y}(C) \times P, F) \quad (C \in \mathbf{C}).$$

Hence, each $\tau \in F^P(C)$ is a natural transformation $\tau : \mathbf{y}(C) \times P \to F$.

First, we shall prove some basic facts about $\tau \in F^P(C)$. By the naturality of τ, for any $h : E \to D$, the following diagram is commutative:

$$\begin{tikzcd} \mathbf{y}(C)(D) \times PD \arrow[r, "\tau_D"] \arrow[d, "\mathbf{y}(C)(h) \times Ph"'] \arrow[dr, phantom, "\circlearrowleft"] & FD \arrow[d, "Fh"] \\ \mathbf{y}(C)(E) \times PE \arrow[r, "\tau_E"'] & FE, \end{tikzcd}$$

i.e., for all $g : D \to C \in \mathbf{y}(C)(D)$ and all $x \in PD$,

$$(Fh)(\tau_D(g, x)) = \tau_E(gh, (Ph)(x)) \quad ((g, x) \in \mathbf{y}(C)(D) \times PD). \tag{3.1.1}$$

Recall that the action of F^P for morphisms is defined for $f : C' \to C$ by for all $\tau \in F^P(C)$, all $g' : D \to C' \in \mathbf{y}(C')(D)$ and all $x \in PD$,

$$(F^P(f)(\tau))_D(g', x) = \tau_D(fg', x). \tag{3.1.2}$$

Next, we claim that if F is separated, then F^P is also separated. To show this, let $C \in \mathbf{C}$ and $\tau, \sigma \in F^P(C)$ be such that for all $S \in J(C)$ and all $f : C' \to C \in S$, $(F^P(f))(\tau) = (F^P(f))(\sigma)$, i.e.,

$$\tau_D(fg', x) = \sigma_D(fg', x),$$

by (3.1.2). In particular, for $g' = \mathrm{id}_{C'}$

$$\tau_{C'}(f, x) = \sigma_{C'}(f, x) \quad (f \in S,\ x \in PC'). \tag{3.1.3}$$

Let $k : C' \to C$ and $x \in PC'$. By the stability axiom of J, $k^*(S) \in J(C')$. For all $g' : D \to C' \in k^*(S)$,

$$\begin{aligned}(Fg')(\tau_{C'}(k, x)) &= \tau_D(kg', (Pg')(x)) \quad (\text{by } (3.1.1)) \\ &= \sigma_D(kg', (Pg')(x)) \quad (\text{by } (3.1.3)) \\ &= (Fg')(\sigma_{C'}(k, x)) \quad (\text{by } (3.1.1)).\end{aligned}$$

Since F is separated, $\tau_{C'}(k, x) = \sigma_{C'}(k, x)$ for all $k : C' \to C$ and all $x \in PC'$. Hence, $\tau = \sigma$. Therefore, F^P is separated.

Finally, we shall show that all matching families have an amalgamation. Let $S \in J(C)$ and $\{\tau_f\}_{f \in S}$ be a matching family of F^P for S. Note that each τ_f $(f \in S)$ is a natural transformation $\tau_f : \mathbf{y}(D) \times P \to F$. Since $\{\tau_f\}_{f \in S}$ is a matching family of F^P, for all $h : E' \to E$ and all $x \in PE'$,

$$((F^P(g))(\tau_f))_{E'}(h, x) = (\tau_{fg})_{E'}(h, x).$$

On the other hand, by the definition of F^P,

$$((F^P(g))(\tau_f))_{E'}(h, x) = (\tau_f)_{E'}(gh, x).$$

Therefore, we have

$$(\tau_{fg})_{E'}(h, x) = (\tau_f)_{E'}(gh, x). \tag{3.1.4}$$

We shall construct an amalgamation of $\{\tau_f\}_{f \in S}$. To this end, we shall define a natural transformation $\tau' : \mathbf{y}(C) \times P \to F^{+}$[*2] so that for all $f : D \to C \in S$ the following diagram is commutative:

$$\begin{tikzcd} \mathbf{y}(D) \times P \arrow[r, "\tau_f"] \arrow[d, "\mathbf{y}(f) \times \mathrm{id}_P"'] \arrow[dr, phantom, "\circlearrowleft"] & F \arrow[d, "\eta_F"] \\ \mathbf{y}(C) \times P \arrow[r, "\tau'"'] & F^{+}. \end{tikzcd} \tag{3.1.5}$$

Since F is a sheaf, η_F is an isomorphism (see [3, Lemma 3.3.1 (ii)]). If τ' were to exists, an amalgamation is given by $(\eta_F)^{-1}\tau'$. Indeed, let $\tau := (\eta_F)^{-1}\tau' : \mathbf{y}(C) \times P \to F$.

*2 Recall that $F^+C = \coprod_{S \in J(C)} \mathrm{Match}(S, F)/\sim_C$ $(C \in \mathbf{C})$, where $\mathrm{Match}(S, F)$ is the set of all matching families for S of F, and $\sim_C$ is an equivalence relation defined as follows: for $\boldsymbol{x} = \{x_f\}_{f \in S} \in \mathrm{Match}(S, F)$ and $\boldsymbol{y} = \{y_g\}_{g \in T} \in \mathrm{Match}(T, F)$ for some $S, T \in J(C)$ $(C \in \mathbf{C})$,

$$\boldsymbol{x} \sim_C \boldsymbol{y} \overset{\text{def}}{\Longleftrightarrow} \exists R \in J(C), \quad R \subseteq S \cap T \quad \text{and} \forall r \in R, x_r = y_R.$$

We shall write $[\boldsymbol{x}]$ for the equivalence class with a representative matching family $\boldsymbol{x}$. See [3, Definition 3.3.3] for details.

Then for all $f : D \to C \in S$, $(F^P(f))(\tau) = (F^P(f))(\eta_F^{-1}\tau')$. For all $g : E \to D$ and all $x \in PE$,

$$\begin{aligned}((F^P(f))(\tau))_E(g,x) &= \tau_E(fg,x)\\ &= (\tau_E \circ (\mathbf{y}(f)_E \times \mathrm{id}_{PE}))(g,x)\\ &= (\tau_f)_E(g,x).\end{aligned}$$

Hence, $(F^P(f))(\tau) = \tau_f$. Therefore, τ is an amalgamation of $\{\tau_f\}_{f\in S}$.

Accordingly, we shall show that there does exist τ' as above. To this end, we define

$$\tau'_B : \mathbf{y}(C)(B) \times PB \to F^+B \quad (B \in \mathbf{C})$$

for $k : B \to C$ and $x \in PB$ by

$$\tau'_B(k,x) := [\{(\tau_{kh})_{\mathrm{dom}(h)}(\mathrm{id}_{\mathrm{dom}(h)}, (Ph)(x))\}_{h\in k^*(S)}].$$

First, we must verify the well-definedness of $\tau'_B \in F^+B$, i.e.,

$$\{(\tau_{kh})_{\mathrm{dom}(h)}(\mathrm{id}_{\mathrm{dom}(h)}, (Ph)(x))\}_{h\in k^*(S)} \in \mathrm{Match}(k^*(S), F).$$

Let $h : B' \to B \in k^*(S)$. Then for all $m : B'' \to B'$,

$$\begin{aligned}&(Fm)((\tau_{kh})_{B'}(\mathrm{id}_{B'}, (Ph)(x)))\\ &= (\tau_{kh})_{B''}(m, (Pm)((Ph)(x))) \quad \text{(by (3.1.1))}\\ &= (\tau_{kh})_{B''}(m, (P(hm))(x))\\ &= (\tau_{khm})_{B''}(\mathrm{id}_{B''}, (P(hm))(x)) \quad \text{(by (3.1.4))}.\end{aligned}$$

Therefore, $\{(\tau_{kh})_{B'}(\mathrm{id}_{B'}, (Ph)(x))\}_{h\in k^*(S)}$ is a matching family for $k^*(S)$.

Next, we shall show that $\tau' = (\tau'_B)_{B\in\mathbf{C}}$ is a natural transformation from $\mathbf{y}(C) \times P$ to F^+, i.e., for each $l : D \to B$, the following diagram is commutative:

$$\begin{tikzcd}
\mathbf{y}(C)(B) \times PB \arrow[r, "\tau'_B"] \arrow[d, "\mathbf{y}(C)(l)\times Pl"'] \arrow[dr, phantom, "\circlearrowleft"] & F^+B \arrow[d, "F^+l"] \\
\mathbf{y}(C)(D) \times PD \arrow[r, "\tau'_D"'] & F^+D.
\end{tikzcd}$$

Indeed, for all $k : B \to C$ and all $x \in PB$,

$$\begin{aligned}&(F^+l)(\tau'_B(k,x))\\ &= (F^+l)([\{(\tau_{kh})_{\mathrm{dom}(h)}(\mathrm{id}_{\mathrm{dom}(h)}, (Ph)(x))\}_{h\in k^*(S)}]) \quad \text{(by the definition of } \tau')\\ &= [\{(\tau_{klh'})_{\mathrm{dom}(h')}(\mathrm{id}_{\mathrm{dom}(h')}, (Plh')(x))\}_{h'\in l^*(k^*(S))}] \quad \text{(by the definition of } F^+l).\end{aligned}$$

On the other hand,

$$\begin{aligned}\tau'_D(\mathbf{y}(C)(l) \times (Pl))(k,x) &= \tau'_D(kl, (Pl)(x))\\ &= [\{\tau_{klh'}(\mathrm{id}_{\mathrm{dom}(h')}, (Ph')((Pl))(x))\}_{h'\in(kl)^*(S)}] \quad \text{(by the definition of } \tau')\\ &= [\{\tau_{klh'}(\mathrm{id}_{\mathrm{dom}(h')}, (P(lh'))(x))\}_{h'\in l^*(k^*(S))}].\end{aligned}$$

Therefore, $(F^+l)(\tau'_B) = \tau'_D(\mathbf{y}(C)(l) \times (Pl))$.

Finally, we shall show that τ' has the required commutativity (3.1.5). To this end, let $B \in \mathbf{C}$, $m : B \to D$ and $x \in PB$. Then

$$\begin{aligned}((\eta_F) \circ (\tau_f))_B(m, x) &= (\eta_F)_B((\tau_f)_B(m, x)) \\ &= [\{(Fl)(\tau_f)_B(m, x)\}_{l \in t_B}] \quad \text{(by the definition of } \eta_F) \\ &= [\{(\tau_f)_{\mathrm{dom}(l)}(ml, (Pl)(x))\}_{l \in t_B}] \quad \text{(by (3.1.1))}.\end{aligned}$$

On the other hand,

$$\begin{aligned}&\tau'_B(\mathbf{y}(f)_B \times \mathrm{id}_{PB})(m, x) \\ &= \tau'_B(fm, x) \\ &= [\{(\tau_{fmh})_{\mathrm{dom}(h)}(\mathrm{id}_{\mathrm{dom}(h)}, (Ph)(x))\}_{h \in (fm)^*(S)}] \quad \text{(by the definition of } \tau') \\ &= [\{(\tau_f)_{\mathrm{dom}(h)}(mh, (Ph)(x))\}_{h \in (fm)^*(S)}] \quad \text{(by (3.1.4))}.\end{aligned}$$

Since $(fm)^*(S) \subseteq t_B$, this implies

$$[\{(\tau_f)_{\mathrm{dom}(l)}(ml, (Pl)(x))\}_{l \in t_B}] = [\{(\tau_f)_{\mathrm{dom}(h)}(mh, (Ph)(x))\}_{h \in (fm)^*(S)}],$$

i.e.,

$$((\eta_F)_B \circ ((\tau_f)_B(m, x)) = \tau'_B(\mathbf{y}(f)_B \times \mathrm{id}_{PB})(m, x).$$

Consequently, τ' is the required natural transformation. The proof is complete. ■

3.2 Subobject Classifiers for Sites

In this section, we shall prove the category $\mathrm{Sh}(\mathbf{C}, J)$ of sheaves on a site $(\mathbf{C}, J)$ has a subobject classifier.

Let M be a sieve on $C \in \mathbf{C}$. Recall that $f \in M$ iff $f^*(M)$ is the maximal sieve, and M covers $f : D \to C$ iff $f^*(M) \in J(D)$.

Definition 3.2.1 (closed sieves). Let M be a sieve on $C \in \mathbf{C}$. Then M is said to be *closed* (for J) if for all f in $\mathbf{C}$, M covers f implies that $f \in M$. ◊

Note that M is closed for J iff for all $f : D \to C$, if $f^*(M)$ covers D, then $f \in M$.

The closedness is stable under pullbacks:

Fact 3.2.1. *Let M be a sieve on $C \in \mathbf{C}$ and $h : B \to C$. If M is closed, then $h^*(M)$ is closed.* □

Proof. Suppose that $h^*(M)$ covers $f : D \to B$, i.e., $f^*(h^*(M)) \in J(D)$. Namely, M covers hf. Since M is closed, $hf \in M$, i.e., $f \in h^*(M)$. Therefore, $h^*(M)$ is closed. The proof is complete. ■

Let S be a sieve on $C \in \mathbf{C}$ and we define

$$\begin{aligned}\overline{S} &:= \{h \mid \mathrm{cod}(h) = C \text{ and } S \text{ covers } h\} \\ &= \{h \mid \mathrm{cod}(h) = C \text{ and } h^*(S) \in J(\mathrm{dom}(h))\}.\end{aligned}$$

Fact 3.2.2. *$\overline{S}$ is a closed sieve on C.* □

Proof. First, we shall show that $\overline{S}$ is a sieve on C. Let $h : D \to C \in \overline{S}$. Then $h^*(S) \in J(D)$. For any $f : E \to D$, by the stability axiom, $(hf)^*(S) = f^*(h^*(S)) \in J(E)$, i.e., S covers hf, and $\mathrm{cod}(hf) = C$. Hence, $hf \in \overline{S}$. Therefore, $\overline{S}$ is a sieve on C.

Next, we shall show that $\overline{S}$ is closed. Suppose that $\overline{S}$ covers $f : D \to C$. By the definition of $\overline{S}$, S covers h for all $h \in \overline{S}$. By the transitivity axiom of the arrow form of a Grothendieck topology, S covers f. Therefore, $f \in \overline{S}$. The proof is complete. ■

Fact 3.2.3. *$\overline{S}$ is the smallest closed sieve on $C \in \mathbf{C}$ containing S.* □

Proof. First, we shall show that $S \subseteq \overline{S}$. Let $f : D \to C \in S$. Then $f^*(S) = t_D \in J(D)$, $f^*(S) \in J(D)$. Hence, S covers f. Therefore, $f \in \overline{S}$.

Next, suppose that there exists a closed sieve M on C such that $S \subseteq M$. Let $h : D \to C \in \overline{S}$. Then $h^*(S) \in J(D)$. Since $S \subseteq M$, $h^*(S) \subseteq h^*(M)$. This implies $h^*(M) \in J(D)$ (see [3, Fact 3.1.1]). Hence, M covers h. Since M is closed, $h \in M$. Therefore, $\overline{S} \subseteq M$. The proof is complete. ■

Accordingly, we shall call $\overline{S}$ the *closure* of S.

Fact 3.2.4. *For all $g : D \to C$,*

$$\overline{g^*(S)} = g^*(\overline{S}).$$

Proof. Let $g : D \to C$. Since $S \subseteq \overline{S}$, we have $g^*(S) \subseteq g^*(\overline{S})$. Since $\overline{S}$ is closed, by Fact 3.2.1, $g^*(\overline{S})$ is closed. By Fact 3.2.3, $\overline{g^*(S)} \subseteq g^*(\overline{S})$.

Conversely, let $f : B \to D \in g^*(\overline{S})$. Then $gf \in \overline{S}$, i.e., $(gf)^*(S) = f^*(g^*(S)) \in J(B)$. This implies that $g^*(S)$ covers f, i.e., $f \in \overline{g^*(S)}$. Hence, $g^*(\overline{S}) \subseteq \overline{g^*(S)}$. Therefore, $\overline{g^*(S)} = g^*(\overline{S})$. The proof is complete. ■

Definition 3.2.2 (truth value object). We define a mapping

$$\Omega : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets} \tag{3.2.1}$$

as follows:

(i) $\Omega C := \{M \mid M \text{ is a closed sieve on } C\}$ for $C \in \mathbf{C}$;
(ii) $\Omega h : \Omega C \ni M \mapsto h^*(M) \in \Omega D$ for a morphism $h : D \to C$. ◊

Note that the definition is well-defined, since $h^*(M)$ is closed for any morphism h if M is closed. Since $\mathrm{id}_C^*(M) = M$ for all $C \in \mathbf{C}$ and all closed sieve M, $\Omega(\mathrm{id}_C) = \mathrm{id}_{\Omega C}$. Since $(\Omega(fg))(M) = (fg)^*(M) = g^*(f^*(M)) = (\Omega g)((\Omega f)(M))$ for all f, g, $\Omega(fg) = \Omega(g)\Omega(f)$. Therefore, Ω is a presheaf on $\mathbf{C}$.

Lemma 3.2.1. *Ω is a sheaf on $(\mathbf{C}, J)$.* □

Proof. First, we shall show that Ω is separated. Suppose $M, N \in \Omega C$ ($C \in \mathbf{C}$) and $S \in J(C)$ such that for all $g \in S$ $(\Omega g)(M) = (\Omega g)(N)$, i.e., $g^*(M) = g^*(N)$. Let $f \in M \cap S$. Then, by assumption and $f \in S$, $f^*(N) = f^*(M)$. On the other hand,

$f^*(M) = t_{\mathrm{dom}(f)}$, since $f \in M$. Thus, $f^*(N) = t_{\mathrm{dom}(f)}$. Hence, $f \in N$. Therefore, $M \cap S \subseteq N \cap S$. By symmetry, $N \cap S \subseteq M \cap S$. Consequently, $M \cap S = N \cap S$. Let $h : D \to C \in M$. Then $h^*(M) = t_D \in J(D)$, i.e., M covers h. On the other hand, since $S \in J(C)$, S covers h, by the stability axiom of J. Therefore, both M and S cover h. This implies that $M \cap S$ covers h (see [3, Fact 3.1.4 (iva)]). On the other hand, since $M \cap S = N \cap S \subseteq N$, N covers h (see [3, Fact 3.1.1]). Since N is closed, $h \in N$. Hence, $M \subseteq N$. By symmetry, $N \subseteq M$. From the above, $M = N$. Therefore, Ω is separated.

Next, we shall show that every matching family of Ω has an amalgamation. Let $S \in J(C)$ and $\{M_f\}_{f \in S}$ be a matching family of Ω, i.e., $\{M_f\}_{f\in S} \in \prod_{f\in S} \Omega(\mathrm{dom}(f))$ and

$$\forall f \in S,\, \forall g : E \to D, \quad (\Omega g)(M_f) = g^*(M_f) = M_{fg}. \tag{3.2.2}$$

Let $M := \{fg \,|\, g \in M_f \text{ and } f \in S\}$. We claim that the closure $\overline{M}$ of M is the required amalgamation of $\{M_f\}_{f\in S}$. First, we claim that $f^*(M) = M_f$ for all $f \in S$. Note that $f^*(M) = \{g \mid fg \in M\} \supseteq M_f$. Conversely, let $u \in f^*(M)$, i.e., $fu \in M$. Then there exists $f' \in S$ and $g \in M_{f'}$ such that $fu = f'g$. Thus, $M_{fu} = M_{f'g}$. By (3.2.2), $u^*(M_f) = (\Omega g)(M_{f'})$, i.e., $u^*(M_f) = g^*(M_{f'})$. Since $g \in M_{f'}$, $g^*(M_f)$ is the maximal sieve, so is $u^*(M_f)$. Hence, $u \in M_f$. Therefore, $f^*(M) \subseteq M_f$. From the above, we have $f^*(M) = M_f$. Since the closure operation $\overline{\cdot}$ preserves pullbacks and M_f is closed, $f^*(\overline{M}) = \overline{f^*(M)} = \overline{M_f} = M_f$. Therefore, $\overline{M}$ is an amalgamation of $\{M_f\}_{f\in S}$. The proof is complete. ■

We shall call Ω the *truth value object* of $\mathrm{Sh}(\mathbf{C}, J)$.

Lemma 3.2.2. *Let F be a sheaf on $(\mathbf{C}, J)$ and A a subfunctor of F. Then A is a sheaf on $(\mathbf{C}, J)$ iff for all $C \in \mathbf{C}$, all $x \in FC$ and all $S \in J(C)$,*

$$[\forall f : D \to C \in S, \quad (Ff)(x) \in AD] \Rightarrow x \in AC. \qquad \square$$

Proof. Suppose that A is a sheaf on $(\mathbf{C}, J)$. Let $C \in \mathbf{C}$, $x \in FC$ and $S \in J(C)$. Suppose that for all $f : D \to C \in S$, $(Ff)(x) \in AD$. Then $\{(Ff)(x)\}_{f\in S}$ is a matching family of both F and A for S. Since A is a sheaf on $(\mathbf{C}, J)$, there exists a unique amalgamation $y \in AC$ such that

$$\forall f : D \to C \in S, \quad (Ff)(y) = (Ff)(x). \tag{3.2.3}$$

On the other hand, since F is also a sheaf on $(\mathbf{C}, J)$, $x \in FC$ is the unique amalgamation such that (3.2.3) holds. Hence, $y = x$. Therefore, $x = y \in AC$.

Conversely, to show that A is a sheaf on $(\mathbf{C}, J)$, we shall prove that every matching family of A has an unique amalgamation. To this end, let $\{x_f\}_{f\in S}$ be a matching family of A for some $S \in J(C)$. Then $\{x_f\}_{f\in S}$ is also a matching family of F for S. Since F is a sheaf on $(\mathbf{C}, J)$, there exists a unique amalgamation $x \in FC$ of $\{x_f\}_{f\in S}$, i.e.,

$$\forall f : D \to C \in S, \quad (Ff)(x) = x_f \in AD.$$

By assumption, $x \in AC$. Suppose that there exists another amalgamation $y \in AC$ of $\{x_f\}_{f \in S}$. Then we have

$$\forall f : D \to C \in S, \quad (Ff)(y) = x_f = (Ff)(x).$$

Since F is separated, we have $y = x$. Therefore, $x \in AC$ is the unique amalgamation of $\{x_f\}_{f \in S}$. This implies that A is a sheaf on $(\mathbf{C}, J)$. The proof is complete. ■

We shall call a subfunctor A of a sheaf F on $(\mathbf{C}, J)$ a *subsheaf* of F if A is a sheaf on $(\mathbf{C}, J)$.

Definition 3.2.3 (truth arrow). We define a mapping $\mathrm{true} : 1 \rightarrowtail \Omega$ for $C \in \mathbf{C}$ by

$$\mathrm{true}_C : 1C = \{*\} \ni * \mapsto t_C \in \Omega C. \tag{3.2.4}$$

◊

Note that the mapping true is a natural transformation from the terminal object 1 to Ω, since $h^*(t_C) = t_D$ for all $h : D \to C$.

Lemma 3.2.3. *The natural transformation* $\mathrm{true} : 1 \rightarrowtail \Omega$ *is a subobject classifier for* $\mathrm{Sh}(\mathbf{C}, J)$. □

Proof. Let $F \in \mathrm{Sh}(\mathbf{C}, J)$ and A a subsheaf of F. We shall prove that there exists a unique natural transformation $\chi_A : F \to \Omega$ such that the following diagram is a pullback square:

$$\begin{tikzcd} A \arrow[r, "!^A"] \arrow[d, tail] \arrow[dr, phantom, "\text{p.b.}"] & 1 \arrow[d, tail, "\mathrm{true}"] \\ F \arrow[r, "\chi_A"'] & \Omega, \end{tikzcd} \tag{3.2.5}$$

where $!^A$ is a unique morphism from A to the terminal object 1.

First, we define a mapping $\chi_A : F \to \Omega$ for each $C \in \mathbf{C}$ by

$$(\chi_A)_C : FC \ni x \mapsto \{f : D \to C \mid (Ff)(x) \in AD\}.$$

We must verify the well-definedness of χ_A, i.e., $(\chi_A)_C(x)$ is a closed sieve on C for all $C \in \mathbf{C}$ and all $x \in FC$. Since A is a subsheaf of F, by Lemma 3.2.2,

$$\forall f : D \to C \in S, \quad (Ff)(x) \in AD \Rightarrow x \in AC.$$

Let $(\chi_A)_C(x)$ cover $g : E \to C$, i.e.,

$$\begin{aligned} & g^*((\chi_A)_C(x)) \in J(E) \\ \Leftrightarrow\ & \{h \mid gh \in (\chi_A)_C(x)\} \in J(E) \\ \Leftrightarrow\ & \{h \mid (Fh)((Fg)(x)) \in A(\mathrm{dom}(h))\} \in J(E). \end{aligned}$$

By Lemma 3.2.2, for all $h \in g^*((\chi_A)_C(x))$, $(Fh)((Fg)(x)) \in A(\mathrm{dom}(h))$ implies $(Fg)(x) \in AE$. Hence, $g \in (\chi_A)_C(x)$. Therefore, $(\chi_A)_C(x)$ is a closed sieve on C.

Next, we shall show that $\chi_A : F \to \Omega$ is a natural transformation. Let $g : B \to C$. Then $(\chi_A)_B((Fg)(x)) = \{f : D \to B \mid (Ff)((Fg)(x))\} \in AD$ for all $x \in FC$. Thus, for all $x \in FC$,

$$\begin{aligned} & f \in (\chi_A)_B((Fg)(x)) \\ \Leftrightarrow\ & (Ff)((Fg)(x)) \in AD \\ \Leftrightarrow\ & (F(gf))(x) \in AD \\ \Leftrightarrow\ & gf \in (\chi_A)_C(x) \\ \Leftrightarrow\ & f \in g^*((\chi_A)_C(x)). \end{aligned}$$

This implies the following commutativity:

$$\forall x \in FC, \quad g^*((\chi_A)_C(x)) = (\chi_A)_B((Fg)(x)) :$$

$$\begin{tikzcd} FC \arrow[r, "(\chi_A)_C"] \arrow[d, "Fg"'] \arrow[dr, phantom, "\circlearrowleft"] & \Omega C \arrow[d, "\Omega g"] \\ FB \arrow[r, "(\chi_A)_B"'] & \Omega B. \end{tikzcd}$$

Next, we shall prove that χ_A satisfies the above pullback condition (3.2.5). Recall that limits in $\mathrm{Sh}(\mathbf{C}, J)$ are computed as limits in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ and are given by pointwise. Therefore, the following diagram is a pullback square:

$$\begin{tikzcd} A \arrow[r, "!^A"] \arrow[d, tail] \arrow[dr, phantom, "\text{p.b.}"] & 1 \arrow[d, tail, "\mathrm{true}"] \\ F \arrow[r, "\chi_A"'] & \Omega \end{tikzcd}$$

in $\mathrm{Sh}(\mathbf{C}, J)$ iff for each $C \in \mathbf{C}$, the following diagram is a pullback square:

$$\begin{tikzcd} AC \arrow[r, "!^{AC}"] \arrow[d, tail] \arrow[dr, phantom, "\text{p.b.}"] & \{*\} \arrow[d, tail, "\mathrm{true}_C"] \\ FC \arrow[r, "(\chi_A)_C"'] & \Omega C. \end{tikzcd} \tag{3.2.6}$$

We shall show that for all $C \in \mathbf{C}$ and all $x \in FC$,

$$x \in AC \Leftrightarrow (\chi_A)_C(x) = t_C.$$

($\Rightarrow$) Let $x \in AC$. Then for all $f : D \to C \in t_C$, $(Ff)(x) \in AD$, since A is a subfunctor of F. By the definition of χ_A, $f \in (\chi_A)_C(x)$. Thus, $t_C \subseteq (\chi_A)_C(x)$. Since t_C is maximal, we have $(\chi_A)_C(x) = t_C$.

($\Leftarrow$) Let $(\chi_A)_C(x) = t_C$. Then for all $f : D \to C \in t_C$, $(Ff)(x) \in AD$. By Lemma 3.2.2, $x \in AC$.

Consequently, the above diagram (3.2.6) is a pullback diagram for each $C \in \mathbf{C}$.

Finally, we shall show that χ_A is a unique natural transformation such that the above diagram (3.2.6) is a pullback diagram for each $C \in \mathbf{C}$. Let $\psi_A : F \to \Omega$ be a natural transformation such that the following diagram is a pullback square for each

$C \in \mathbf{C}$:

$$\begin{tikzcd} AC \arrow[r, "!^{AC}"] \arrow[d, tail] \arrow[dr, phantom, "\text{p.b.}"] & \{*\} \arrow[d, tail, "\mathrm{true}_C"] \\ FC \arrow[r, "(\psi_A)_C"'] & \Omega C. \end{tikzcd}$$

Since $x \in AC \Leftrightarrow (\psi_A)_C(x) = t_C \Leftrightarrow \mathrm{id}_C \in (\psi_A)_C(x)$, for all $f : D \to C$,

$$\begin{aligned} (Ff)(x) \in AD &\Leftrightarrow \mathrm{id}_D \in (\psi_A)_D((Ff)(x)) \\ &\Leftrightarrow \mathrm{id}_D \in f^*((\psi_A)_C(x)) \quad \text{(by the naturality of } \psi_A) \\ &\Leftrightarrow f \in (\psi_A)_C(x). \end{aligned}$$

Hence, $(\psi_A)_C(x) = \{f \mid (Ff)(x) \in AD\} = (\chi_A)_C(x)$. Therefore, $\psi_A = \chi_A$.

Consequently, the natural transformation $\mathrm{true} : 1 \rightarrowtail \Omega$ is a subobject classifier for $\mathrm{Sh}(\mathbf{C}, J)$. The proof is complete. ■

With the above lemmas, the proof of Theorem 3.1.1 is complete.

Corollary 3.2.1. *Every Grothendieck topos is an elementary topos.* □

Let $(\mathbf{C}, J)$ be a site.

Definition 3.2.4 (local surjectivity). Let P and Q be two presheaves on $\mathbf{C}$ and $\phi : P \to Q$ a natural transformation. Then we shall say that ϕ is *locally surjective* for J if for all $C \in \mathbf{C}$ and all $y \in QC$, there exists $S \in J(C)$ such that for all $f : D \to C \in S$, $(Qf)(y) \in \phi_D[PD]$*3. ♢

Corollary 3.2.2. *Let F and G be two sheaves on $(\mathbf{C}, J)$ and $\phi : F \to G$ be a natural transformation. Then ϕ is an epimorphism in* $\mathrm{Sh}(\mathbf{C}, J)$ *iff ϕ is locally surjective for J.* □

Proof. Suppose that $\phi : P \to Q$ is locally surjective for J. Let $\alpha, \beta : G \to H$ be two natural transformations between two sheaves G and H such that $\alpha\phi = \beta\phi$. Let $C \in \mathbf{C}$ and $y \in GC$. Since ϕ is locally surjective for J, there exists $S \in J(C)$ such that for all $f : D \to C \in S$, $(Gf)(y) \in \phi_D[FD]$. Since $\alpha\phi = \beta\phi$, we have

$$\forall f : D \to C \in S, \quad \alpha_D((Gf)(y)) = \beta_D((Gf)(y)) \quad (C \in \mathbf{C},\ y \in GC).$$

By the naturality of α and β, we have

$$\forall f : D \to C \in S, \quad (Hf)(\alpha_C(y)) = (Hf)(\beta_C(y)) \quad (C \in \mathbf{C},\ y \in GC).$$

Since H is a sheaf on $(\mathbf{C}, J)$, in particular separated, this implies that

$$\alpha_C(y) = \beta_C(y) \quad (C \in \mathbf{C},\ y \in GC).$$

Hence, $\alpha = \beta$. Therefore, ϕ is an epimorphism.

*3 $\phi_D[PD]$ is the image of PD under ϕ_D.

Conversely, suppose that $\phi : F \to G$ is an epimorphism. We define a subfunctor A of G for $C \in \mathbf{C}$ by

$$AC := \{y \in GC \mid \exists S \in J(C),\ \forall f : B \to C \in S,\ (Gf)(y) \in \phi_B[FB]\}. \tag{3.2.7}$$

First, we shall prove that A is indeed a subfunctor of G. By definition, $AC \subseteq GC$. Let $f : D \to C$ and $x \in AC$. Then, by the definition of A, there exists $S \in J(C)$ such that for all $h \in S$, $(Gh)(x) \in \phi_B[FB]$. Consider $f^*(S) \in J(D)$. Then for all $g \in f^*(S)$, $(Gg)((Gf)(x)) = (G(fg))(x) \in \phi_B[FB]$. This implies that $(Gf)(x) \in AD$. Therefore, A is a subfunctor of G.

Next, we claim that A is a subsheaf of G, by Lemma 3.2.2. To show this, let $C \in \mathbf{C}$, $x \in GC$ and $S \in J(C)$. Suppose that for all $f : D \to C \in S$, $(Gf)(x) \in AD$. We must prove that $x \in AC$. By the definition of A, for all $f : D \to C \in S$, there exists $T_f \in J(D)$ such that for all $g : B \to D \in T_f$, $(Gg)((Gf)(x)) \in \phi_B[FB]$. We fix this T_f for each $f \in S$. Consider $T := \{fg \mid f \in S,\ g \in T_f\}$. Then T is a sieve on C and for all $f : D \to C \in S$, $f^*(T) = \{g \mid fg \in T\} \supseteq T_f \in J(D)$. Hence, $f^*(T) \in J(D)$ for all $f : D \to C$. By the transitivity axiom of J, we have $T \in J(C)$. Therefore, $(G(fg))(x)) \in \phi_B[FB]$ for all $fg : B \to C \in T \in J(C)$. Thus, we have $x \in AC$.

Let $\chi_A : G \to \Omega$ be the classifying map for $A \rightarrowtail G$. We shall show that $\phi_C[FC] \subseteq AC$ $(C \in \mathbf{C})$. To this end, let $y \in \phi_C[FC]$, i.e., there exists $x \in FC$ such that $y = \phi_C(x)$. Then for all $f : B \to C \in t_C$,

$$\begin{aligned}(Gf)(y) &= (Gf)(\phi_C(x)) \\ &= \phi_B((Ff)(x)) \in \phi_B[FB] \quad \text{(by the naturality of } \phi).\end{aligned}$$

Hence, we have the following pullback square:

$$\begin{tikzcd}
F \arrow[r, "\phi"] \arrow[dr, dashed, "\exists!"] \arrow[ddr, bend right, "\phi"'] & G \arrow[dr, "!^G"] \arrow[d, phantom, "\circlearrowright"] & \\
\arrow[r, phantom, "\circlearrowright"] & A \arrow[r, "!^A"] \arrow[d, tail] \arrow[dr, phantom, "\text{p.b.}"] & 1 \arrow[d, tail, "\text{true}"] \\
& G \arrow[r, "\chi_A"'] & \Omega.
\end{tikzcd}$$

Therefore, we have

$$\chi_A \circ \phi = \text{true} \circ !^G \circ \phi.$$

Since ϕ is an epimorphism, we obtain $\chi_A = \text{true} \circ !^G$. On the other hand, we also have the following pullback square:

$$\begin{tikzcd}
G \arrow[r, "!^G"] \arrow[d, tail, "\mathrm{id}_G"'] \arrow[dr, phantom, "\text{p.b.}"] & 1 \arrow[d, tail, "\text{true}"] \\
G \arrow[r, "\chi_G"'] & \Omega.
\end{tikzcd}$$

Therefore, $\chi_G = \text{true} \circ !^G = \chi_A$. Thus, $A = G$, since there exists a one-to-one correspondence between subobjects and their classifying maps. This implies that $\phi : F \to G$ is locally surjective for J, by the definition of A. The proof is complete.■

Corollary 3.2.3. *Let P and Q be two presheaves on $\mathbf{C}$ and $\phi : P \to Q$ be a natural transformation. Then $\mathbf{a}(\phi) : \mathbf{a}(P) \to \mathbf{a}(Q)$ is an epimorphism in $\mathrm{Sh}(\mathbf{C}, J)$ iff ϕ is locally surjective for J, where $\mathbf{a}$ is the associated sheaf functor for the inclusion functor $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$.* □

Proof. Let $\phi : P \to Q$ be locally surjective for J. Let $\alpha, \beta : \mathbf{a}(Q) \to F$ be two natural transformation such that

$$\alpha(\mathbf{a}(\phi)) = \beta(\mathbf{a}(\phi)).$$

By the naturality of the unit $\tilde{\eta} : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \ni P \to i\mathbf{a}(P) = \mathbf{a}(P) \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ of the adjoint $\mathbf{a} \dashv i$, we have the following commutative diagram:

$$\begin{tikzcd}
P \arrow[r, "\tilde{\eta}_P"] \arrow[d, "\phi"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbf{a}(P) \arrow[d, "\mathbf{a}(\phi)"] & \\
Q \arrow[r, "\tilde{\eta}_Q"'] & \mathbf{a}(Q) \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & F.
\end{tikzcd}$$

Hence, we have

$$\alpha \circ \tilde{\eta}_Q \circ \phi = \alpha \circ \mathbf{a}(\phi) \circ \tilde{\eta}_P = \beta \circ \mathbf{a}(\phi) \circ \tilde{\eta}_P = \beta \circ \tilde{\eta}_Q \circ \phi. \tag{3.2.8}$$

On the other hand, since $\phi : P \to Q$ is locally surjective for J, for all $C \in \mathbf{C}$ and all $y \in QC$, there exists $S \in J(C)$ such that

$$\forall f : D \to C \in S, \quad (Qf)(y) \in \phi_D[PD].$$

By (3.2.8), for all $f : D \to C \in S$ and all $y \in QC$,

$$\begin{aligned}
&(\alpha\tilde{\eta}_Q)_D((Qf)(y)) = (\beta\tilde{\eta}_Q)_D((Qf)(y)) \\
\Leftrightarrow\ &(Ff)((\alpha\tilde{\eta}_Q)_C(y)) = (Ff)((\beta\tilde{\eta}_Q)_C(y)) \quad \text{(by the naturality of } \alpha \text{ and } \beta\text{)}.
\end{aligned}$$

Since F is separated, we have $\alpha\tilde{\eta}_Q = \beta\tilde{\eta}_Q$, i.e.,

$$\begin{tikzcd}
Q \arrow[r, "\tilde{\eta}_Q"] \arrow[dr, "\alpha\tilde{\eta}_Q = \beta\tilde{\eta}_Q"'] \arrow[dr, phantom, shift left=4ex, "\circlearrowleft"] & \mathbf{a}(Q) \arrow[d, dashed, shift right, "\alpha"'] \arrow[d, dashed, shift left, "\beta"] \\
& F.
\end{tikzcd}$$

Since F is a sheaf, by the universal mapping property of $\tilde{\eta}_Q$, we obtain $\alpha = \beta$. Therefore, ϕ is an epimorphism.

Conversely, let $\mathbf{a}(\phi) : \mathbf{a}(P) \to \mathbf{a}(Q)$ be an epimorphism and A a subsheaf of Q defined as (3.2.7):

$$AC := \{y \in QC \mid \exists S \in J(C), \forall f : B \to C \in S, (Qf)(y) \in \phi_B[FB]\}.$$

Let $\Omega^{(p)}$ be the subobject classifier for the presheaf category $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, Ω the subobject classifier for $\mathrm{Sh}(\mathbf{C}, J)$ and $\iota : \Omega \hookrightarrow \Omega^{(p)}$ the inclusion functor. Recall that $\Omega^{(p)}C :=$

$\{S \mid S \text{ is a sieve on } C\}$ $(C \in \mathbf{C})$ and $\Omega C := \{M \mid M \text{ is a closed sieve on } C\}$ $(C \in \mathbf{C})$. Let $\chi_A^{(p)} : Q \to \Omega^{(p)}$ be the classifying map for $A \rightarrowtail Q$ in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Recall that

$$(\chi_A^{(p)})_C(y) = \{f : D \to C \mid (Qf)(y) \in AD\} \quad (C \in \mathbf{C},\ y \in QC).$$

We claim that $(\chi_A^{(p)})_C(y)$ is a closed sieve for all $C \in \mathbf{C}$ and $y \in QC$. Let $(\chi_A^{(p)})_C(y)$ covers $f : D \to C$, i.e.,

$$\begin{aligned} f^*((\chi_A^{(p)})_C(y)) &= \{g \mid fg \in (\chi_A^{(p)})_C(y)\} \\ &= \{g \mid (Qg)((Qf)(y)) \in A(\mathrm{dom}(g))\} \in J(D). \end{aligned}$$

Hence, for all $g : B \to D \in f^*((\chi_A^{(p)})_C(y))$, $(Qg)((Qf)(y)) \in AB$. By the definition of A, this implies that $(Qf)(y) \in AD$, i.e., $f \in (\chi_A^{(p)})_C(y)$. Therefore, $(\chi_A^{(p)})_C(y)$ is a closed sieve. This implies that $\chi_A^{(p)}$ factors through $\iota : \Omega \hookrightarrow \Omega^{(p)}$, i.e., there exists a mapping $\chi_A : Q \to \Omega$ such that $\chi_A^{(p)} = \iota \circ \chi_A$. Then as is the case for the proof of Corollary 3.2.2, we have the following commutative square:

$$\begin{tikzcd} P \arrow[r, "!^P"] \arrow[d, "\phi"'] \arrow[dr, phantom, "\circlearrowleft"] & 1 \arrow[d, tail, "\mathrm{true}"] \\ Q \arrow[r, "\chi_A"'] & \Omega. \end{tikzcd}$$

Hence, we have

$$\chi_A \circ \phi = \mathrm{true} \circ !^P = \mathrm{true} \circ !^Q \circ \phi. \tag{3.2.9}$$

On the other hand, since Ω is a sheaf, by the universal mapping property of $\tilde{\eta}_Q$, there exists a unique mapping $\overline{\chi}_A : \mathbf{a}(Q) \to \Omega$ such that $\chi_A = \overline{\chi}_A \circ \tilde{\eta}_Q$. By the naturality of $\tilde{\eta}$ and (3.2.9), we have

$$\begin{tikzcd} P \arrow[r, "\phi"] \arrow[d, "\phi"'] \arrow[dr, "\tilde{\eta}_P"] & Q \arrow[dr, "!^Q"] & \\ Q \arrow[dr, "\tilde{\eta}_Q"'] & \mathbf{a}(P) \arrow[r, "!^{\mathbf{a}(P)}"] \arrow[d, "\mathbf{a}(\phi)"] & 1 \arrow[d, "\mathrm{true}"] \\ & \mathbf{a}(Q) \arrow[r, "\overline{\chi}_A"'] & \Omega, \end{tikzcd}$$

$$\begin{aligned} & \chi_A \circ \phi = \mathrm{true} \circ !^Q \circ \phi \\ \Leftrightarrow\ & \overline{\chi}_A \circ \tilde{\eta}_Q \circ \phi = \mathrm{true} \circ !^{\mathbf{a}(P)} \circ \tilde{\eta}_P \\ \Leftrightarrow\ & \overline{\chi}_A \circ \mathbf{a}(\phi) \circ \tilde{\eta}_P = \mathrm{true} \circ !^{\mathbf{a}(P)} \circ \tilde{\eta}_P. \end{aligned}$$

Since Ω is a sheaf again, by the universal mapping property of $\tilde{\eta}_P$, we have

$$\overline{\chi}_A \circ \mathbf{a}(\phi) = \mathrm{true} \circ !^{\mathbf{a}(P)} = \mathrm{true} \circ !^{\mathbf{a}(Q)} \circ \mathbf{a}(\phi).$$

Now, by assumption, $\mathbf{a}(\phi)$ is an epimorphism. Hence, we have $\overline{\chi}_A = \mathrm{true} \circ !^{\mathbf{a}(Q)}$. Therefore, we have

$$\chi_A^{(p)} = \iota \circ \chi_A = \iota \circ \overline{\chi}_A \circ \tilde{\eta}_Q = \iota \circ \mathrm{true} \circ !^{\mathbf{a}(Q)} \circ \tilde{\eta}_Q = \iota \circ \mathrm{true} \circ !^Q.$$

This implies that $\chi_A^{(p)}$ is also the classifying map of $\mathrm{id}_Q : Q \to Q$. Thus, $A = Q$. Consequently, ϕ is locally surjective for J. The proof is complete. ■

Corollary 3.2.4. $(\{f_i : C_i \to C\}_{i\in I})^{*4} \in J(C)$ *iff*

$$\coprod_{i\in I} \mathbf{ay}(C_i) \to \mathbf{ay}(C) \tag{3.2.10}$$

is an epimorphism in $\mathrm{Sh}(\mathbf{C}, J)$. □

Proof. Consider the coproduct $\coprod_{i\in I}^{(\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}})} \mathbf{y}(C_i)$ of $\{\mathbf{y}(C_i)\}$ in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Since the associated sheaf functor $\mathbf{a}$ preserves colimits, we have

$$\mathbf{a}\Big(\coprod_{i\in I}^{(\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}})} \mathbf{y}(C_i)\Big) \cong \coprod_{i\in I} \mathbf{ay}(C_i) \in \mathrm{Sh}(\mathbf{C}, J).$$

Let $\phi : \coprod_{i\in I}^{(\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}})} \mathbf{y}(C_i) \to \mathbf{y}(C)$ be a natural transformation induced by $\{f_i\}_{i\in I}$, i.e., for $D \in \mathbf{C}$ and $h : D \to C_i \in \mathbf{y}(C_i)(D)$, $\phi_D(g) := f_i h$. By Corollary 3.2.3, $\mathbf{a}(\phi) : \coprod_{i\in I} \mathbf{ay}(C_i) \to \mathbf{ay}(C)$ is an epimorphism in $\mathrm{Sh}(\mathbf{C}, J)$ iff ϕ is locally surjective for J.

Suppose that $(\{f_i\}_{i\in I}) = \{f_i g \,|\, i \in I,\, g \in \mathbf{C}\} \in J(C)$. Let $D \in \mathbf{C}$ and $f \in \mathbf{y}(C)(D)$. Then, by the transitivity axiom of J, we have $f^*((\{f_i\}_{i\in I})) \in J(D)$. Then for all $g : B \to D \in f^*((\{f_i\}_{i\in I}))$, there exists $i \in I$ and $h : B \to C_i \in \mathbf{y}(C_i)(B)$ such that $fg = f_i h$. Hence, we have

$$(\mathbf{y}(C)(g))(f) = fg = f_i h \in \phi_B \left[\coprod_{i\in I}^{(\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}})} \mathbf{y}(C_i)(B)\right].$$

Therefore, ϕ is locally surjective for J.

Conversely, suppose that ϕ is locally surjective for J. Then for $\mathrm{id}_C \in \mathbf{y}(C)(C)$ there exists $S \in J(C)$ such that for all $f : D \to C \in S$,

$$(\mathbf{y}(C)(f))(\mathrm{id}_C) = f \in \phi_D \left[\coprod_{i\in I}^{(\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}})} \mathbf{y}(C_i)(D)\right],$$

that is, there exists $i \in I$ and $g : D \to C_i$ such that $f = f_i g \in (\{f_i\}_{i\in I})$. Hence, $S \subseteq (\{f_i\}_{i\in I})$. Since $S \in J(C)$, this implies that $(\{f_i\}_{i\in I}) \in J(C)$. The proof is complete. ■

3.3 Subsheaves

Let $(\mathbf{C}, J)$ be a site and $E \in \mathrm{Sh}(\mathbf{C}, J)$. Let $\mathrm{Sub}(E)$ be the set of all subobjects A of E in $\mathrm{Sh}(\mathbf{C}, J)$.

Since monomorphisms in $\mathrm{Sh}(\mathbf{C}, J)$ coincide with monomorphisms in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, a subobject $A \in \mathrm{Sub}(E)$ is represented by a subfunctor $A : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets}$ of E such that A is a sheaf on $(\mathbf{C}, J)$. That is, $A \in \mathrm{Sub}(E)$ is a subsheaf A of E (cf. Lemma 3.2.2):

[*4] where $(\{f_i : C_i \to C\}_{i\in I})$ is the sieve on C generated by $\{f_i\}_{i\in I}$, i.e., $(\{f_i : C_i \to C\}_{i\in I}) := \{f_i g \,|\, i \in I,\, g \in \mathbf{C}\}$.

(i) for all $C \in \mathbf{C}$, $\quad AC \subseteq EC$;

(ii) for all $f : D \to C$, the following diagram is commutative:

$$\begin{tikzcd} AC \arrow[r, hook] \arrow[d, "Af"'] \arrow[dr, phantom, "\circlearrowleft"] & EC \arrow[d, "Ef"] \\ AD \arrow[r, hook] & ED; \end{tikzcd}$$

(iii) for all $C \in \mathbf{C}$, all $e \in EC$, all $S \in J(C)$ and all $f : D \to C \in S$,

$$(Ef)(e) \in AD \Rightarrow e \in AC.$$

We define an order in $\mathrm{Sub}(E)$ as follows:

Definition 3.3.1. Let E be a sheaf on $(\mathbf{C}, J)$ and A, B two subobjects of E.

$$A \le B \overset{\text{def}}{\Longleftrightarrow} \forall C \in \mathbf{C}, \quad AC \subseteq BC. \tag{3.3.1}$$

◊

Fact 3.3.1. *Let E be a sheaf on $(\mathbf{C}, J)$. Then $(\mathrm{Sub}(E), \le)$ is a poset. Moreover, $(\mathrm{Sub}(E), \le)$ is a complete lattice with respect to $\le$.* □

Proof. Let $A, B \in \mathrm{Sub}(E)$. Then $A \wedge B$ is defined as follows:

(i) $(A \wedge B)C := (AC) \cap (BC)$ for $C \in \mathbf{C}$;

(ii) $(A \wedge B)f : (AC) \cap (BC) \ni x \mapsto (Ef)(x) \in (AD) \cap (BD)$ for $f : D \to C$.

Then $A \wedge B \in \mathrm{Sub}(E)$. More generally, for any family $\{A_i\}_{i \in I} \in \mathrm{Sub}(E)^I$ (I is any small set), the infimum $\bigwedge_{i \in I} A_i$ is defined as follows:

(i) $\left(\bigwedge_{i \in I} A_i\right)C := \bigcap_{i \in I} A_i C$ for $C \in \mathbf{C}$;

(ii) $\left(\bigwedge_{i \in I} A_i\right)f := Ef : \bigcap_{i \in I} A_i C \to \bigcap_{i \in I} A_i D$ for $f : D \to C$.

Then $\bigwedge_{i \in I} A_i \in \mathrm{Sub}(E)$ and then the supremum $\bigvee_{i \in I} A_i$ is given by as usual:

$$\bigvee_{i \in I} A_i := \bigwedge \{B \in \mathrm{Sub}(E) \mid \forall i \in I,\ A_i \le B\}.$$

Therefore, $(\mathrm{Sub}(E), \le)$ is a complete lattice. The proof is complete. ■

Fact 3.3.2. *The supremum $\bigvee_{i \in I} A_i$ of subobjects $\{A_i\}_{i \in I}$ of E can be described explicitly as follows: for all $C \in \mathbf{C}$ and all $e \in EC$,*

$$\begin{aligned} & e \in \Big(\bigvee_{i \in I} A_i\Big)C \\ \Leftrightarrow\ & \{f : D \to C \mid \exists i \in I,\ (Ef)(e) \in A_i D\} \in J(C). \end{aligned} \tag{3.3.2}$$

□

Proof. Let $S := \{f : D \to C \mid \exists i \in I,\ (Ef)(e) \in A_i D\}$. First, we shall verify that S is a sieve on C. To this end, let $f : D \to C \in S$. Then there exists $i \in I$ such that $(Ef)(x) \in A_i D$. Since A_i is a subfunctor of E, for all $g : E \to D$, $(E(fg))(e) \in A_i D$. This implies $fg \in S$. Hence, S is a sieve on C.

Next, we shall verify that $\bigvee_{i\in I} A_i$ described by (3.3.2) is indeed a subfunctor of E. To this end, let $S = \{f : D \to C \mid \exists i \in I,\ (Ef)(e) \in A_iD\} \in J(C)$ and $g : C' \to C$. Then $g^*(S) \in J(S)$, by the stability axiom of J. We claim that $g^*(S) = \{h : D \to C' \mid \exists i \in I,\ (E(gh))(e) = (Eh)((Eg)(e)) \in A_iD\}$. Let $h : D \to C' \in g^*(S)$, i.e., $gh \in S$. Then, by the condition of S,

$$\exists i \in I, \quad (E(gh))(e) \in A_iD.$$

Conversely, let $h : D \to C'$ such that

$$\exists i \in I, \quad (Eh)(e) \in A_iD.$$

Then $gh \in S$, i.e., $h \in g^*(S)$. Hence, $\{h : D \to C' \mid \exists i \in I,\ (E(gh))(e) = (Eh)((Eg)(e)) \in A_iD\} = g^*(S) \in J(D)$, i.e., $(Eg)(e) \in (\bigvee_{i\in I} A_i)C'$. Therefore, $\bigvee_{i\in I} A_i$ is a subfunctor of E.

Next, we must prove that $\bigvee_{i\in I} A_i$ is a subsheaf of E. To this end, let $C \in \mathbf{C}$, $S \in J(C)$ and $e \in EC$ and suppose that for all $f : D \to C \in S, (Ef)(e) \in \big(\bigvee_{i\in I} A_i\big)D$, i.e.,

$$\{g : B \to D \mid \exists i \in I,\ (Eg)(E(f)(e)) \in A_iD\} \in J(D).$$

Put $R := \{h : D \to C \mid \exists i \in I,\ (Eg)(e) \in A_iD\}$. Then, as we have seen in the above,

$$\forall f : D \to C \in S, \quad f^*(R) = \{g : B \to D \mid \exists i \in I,\ (Eg)(E(f)(e)) \in A_iD\} \in J(D).$$

Hence, by the transitivity axiom of J, $R \in J(C)$, i.e., $e \in \big(\bigvee_{i\in I} A_i\big)C$. Therefore, by Lemma 3.2.2, $\bigvee_{i\in I} A_i$ is a subsheaf of E.

Finally, we shall verify that $\bigvee_{i\in I} A_i$ described as (3.3.2) is the smallest subsheaf containing all the $A_i (i \in I)$. To this end, let $C \in \mathbf{C}$ and $e \in EC$. Suppose that $e \in A_iC$ for some $i \in I$. Then, for all $f : D \to C$, $(Ef)(e) \in A_iD$, since A_i is a subfunctor of E. Hence, $\{f : D \to C \mid \exists i \in I,\ (Ef)(e) \in A_iD\} = t_C \in J(C)$. Therefore, $e \in \big(\bigvee_{i\in I} A_i\big)C$. Thus, $A_i \leq \bigvee_{i\in I} A_i$. Suppose that there exists a subsheaf U of E such that $A_i \leq U$ for all $i \in I$. Let $e \in \big(\bigvee_{i\in I} A_i\big)C$. Then we have $S = \{f : D \to C \mid \exists i \in I,\ (Ef)(e) \in A_iD\} \in J(C)$. Since $A_i \leq U$ for all $i \in I$, for all $f : D \to C \in S$, $(Ef)(e) \in UD$. This implies that $e \in UC$, since U is a subsheaf of E. The proof is complete. ■

Fact 3.3.3. *Let E be a sheaf on $(\mathbf{C}, J)$. Then $(\mathrm{Sub}(E), \leq)$ is a complete Heyting algebra.* □

Proof. Since $(\mathrm{Sub}(E), \leq)$ is a complete lattice, it is sufficient to prove the following distributive law:

$$\forall \{A_i\}_{i\in I} \in \mathrm{Sub}(E)^I,\ \forall B \in \mathrm{Sub}(E), \quad B \wedge \bigvee_{i\in I} A_i = \bigvee_{i\in I} (B \wedge A_i). \tag{3.3.3}$$

Since $B \wedge A_i \leq B,\ A_i$ for all $i \in I$, we have

$$\bigvee_{i\in I} (B \wedge A_i) \leq B,\ \bigvee_{i\in I} A_i.$$

Hence, by the definition of the infimum, we obtain

$$\bigvee_{i\in I}(B\wedge A_i)\le B\wedge\big(\bigvee_{i\in I}A_i\big).$$

Now, we shall prove the converse:

$$B\wedge\big(\bigvee_{i\in I}A_i\big)\le\bigvee_{i\in I}(B\wedge A_i).$$

To this end, suppose that $e\in BC$ and $e\in\big(\bigvee_{i\in I}A_i\big)C$ $(C\in\mathbf{C}, e\in EC)$. Then, by Fact 3.3.2,

$$S:=\{f:D\to C\mid \exists i\in I,\ (Ef)(e)\in A_iD\}\in J(C).$$

On the other hand, since B is a subfunctor of E, we have $(Ef)(e)\in BD$ for all $f:D\to C\in S$. By the definition of the infimum, we have

$$\forall f:D\to C\in S,\ \exists i\in I,\quad (Ef)(e)\in(B\wedge A_i)D.$$

This implies that $e\in\bigvee_{i\in I}(B\wedge A_i)$. The proof is complete. ■

Fact 3.3.4. *The implication operator $\to$ in $(Sub(E),\le)$ can be described explicitly for $A,B\in\mathrm{Sub}(E)$ and $e\in EC$ $(C\in\mathbf{C})$ by*

$$e\in(A\to B)C\Leftrightarrow[\forall f:D\to C,\quad (Ef)(e)\in AD\Rightarrow(Ef)(e)\in BD].\tag{3.3.4}$$

□

Proof. We shall prove that the operator $\to$ described by (3.3.4) is indeed the implication operator in $(\mathrm{Sub}(E),\le)$. First, we must verify that $A\to B$ is a subfunctor of E, i.e., for all $g:C'\to C$, $(Eg)(e)\in(A\to B)C'$ for all $e\in(A\to B)C$. To this end, let $e\in(A\to B)C$ and $g:C'\to C$. Suppose that $h:D\to C'$ satisfies that $(Eh)((Eg)(e))\in AD$. Then, by (3.3.4), $(Eh)((Eg)(e))=(E(gh))(e)\in BD$. This implies that $(Eg)(e)\in(A\to B)C$. Therefore, $A\to B$ is a subfunctor of E.

Next, we shall prove that $A\to B$ is a subsheaf of E. To this end, let $C\in\mathbf{C}$, $e\in EC$ and $S\in J(C)$. Suppose that

$$\forall f:D\to C\in S,\quad (Ef)(e)\in(A\to B)D.$$

Then we must prove that $e\in(A\to B)C$. To this end, let $g:C'\to C$ and $(Eg)(e)\in AC'$. By the stability axiom of J, $g^*(S)\in J(C')$. Then for all $h:D\to C'\in g^*(S)$, $gh\in S$. Hence, by assumption, we have $(Eh)((Eg)(e))=(E(gh))(e)\in(A\to B)D$. by the definition of $A\to B$, we obtain $(Eh)((Eg)(e))\in BD$. Therefore,

$$\forall h:D\to C'\in g^*(S),\quad (Eh)((Eg)(e))\in BD.$$

This implies that $(Eg)(e)\in BC'$, since B is a subsheaf of E. Consequently, for all $g:C'\to C$, $(Eg)(e)\in AC'$ implies that $(Eg)(e)\in BC'$, i.e., $e\in(A\to B)C$. Thus, $A\to B$ is a subsheaf of E.

Finally, we shall prove that $\to$ describes the implication in $\mathrm{Sub}(E)$, i.e.,

$$\forall A,\ \forall B,\ \forall U\in\mathrm{Sub}(E),\quad U\le(A\to B)\Leftrightarrow U\wedge A\le B.$$

(⇒) Suppose that $U \leq (A \to B)$, i.e.,

$$\forall C \in \mathbf{C},\ \forall u \in UC,\ \forall f : D \to C, \quad (Ef)(u) \in AD \Rightarrow (Ef)(u) \in BD. \tag{3.3.5}$$

Let $C \in \mathbf{C}$ and $u \in (UC) \cap (AC)$. In particular, $(Ef)(u) \in UD$. By assumption, $u \in (A \to B)C$. Let $f : D \to C$. Since $u \in AC$, $(Ef)(u) \in AD$. Note that $u \in (A \to B)C$ and $(Ef)(u) \in AD$ implies that $(Ef)(u) \in BD$, by (3.3.5). Hence, for all $f : D \to C \in t_C \in J(C)$, we obtain $(Ef)(u) \in BC$. Therefore, $u \in BC$, since B is a subsheaf of E. Thus, $U \wedge A \leq B$.

(⇐) Suppose that $U \wedge A \leq B$. Let $C \in \mathbf{C}$, $u \in UC$ and $f : D \to C$. Then $(Ef)(u) \in UD$. Suppose that $(Ef)(u) \in AD$. Then $(Ef)(u) \in (UD) \cap (AD)$. By assumption, $(Ef)(u) \in BD$. Hence, for all $f : D \to C$, $(Ef)(u) \in AD$ implies that $(Ef)(u) \in BD$. Therefore, $u \in (A \to B)C$. Thus, $U \wedge A \leq B$.

The proof is complete. ■

Definition 3.3.2 (pullback functors). Let $E, F \in \mathrm{Sh}(\mathbf{C}, J)$ and $\phi : E \to F$ a natural transformation. We define a mapping $\phi^{-1} : \mathrm{Sub}(F) \to \mathrm{Sub}(E)$ for $C \in \mathbf{C}$, $e \in EC$ and $B \in \mathrm{Sub}(F)$ by pullback:

$$e \in \phi^{-1}(B)C \Leftrightarrow \phi_C(e) \in BC. \tag{3.3.6}$$

♢

We must verify that $\phi^{-1}(B)$ is a subsheaf of F for all $B \in \mathrm{Sub}(F)$. First, we shall verify that $\phi^{-1}(B)$ is a subfunctor of E for all $B \in \mathrm{Sub}(F)$. Let $B \in \mathrm{Sub}(F)$. Then $\phi^{-1}(B)C \subseteq EC$ for all $C \in \mathbf{C}$, by definition. Let $f : D \to C$ and $e \in \phi^{-1}(B)C$. Then $\phi_C(e) \in BC$. Since B is a subfunctor of F and ϕ is natural, we have

$$\phi_D((Ef)(e)) = (Ff)(\phi_C(e)) \in BD.$$

Hence, $(Ef)(e) \in \phi^{-1}(B)D$, by the definition of ϕ^{-1}. Therefore, $\phi^{-1}(B)$ is a subfunctor of E.

Next, we shall verify that $\phi^{-1}(B)$ is a subsheaf of E for all $B \in \mathrm{Sub}(F)$. To this end, let $B \in \mathrm{Sub}(F), C \in \mathbf{C}$, $e \in EC$ and $S \in J(C)$. Suppose that

$$\forall f : D \to C \in S, \quad (Ef)(e) \in \phi^{-1}(B)D.$$

Since ϕ is natural, for all $f : D \to C \in S$, $(Ff)(\phi_C(e)) = \phi_D((Ef)(e)) \in BD$. Since B is a subsheaf of F, we have $\phi_C(e) \in BC$, i.e., $e \in \phi^{-1}(B)C$. Therefore, $\phi^{-1}(B)$ is a subsheaf of E.

We shall call ϕ^{-1} the *pullback functor* of ϕ.

Fact 3.3.5. *The pullback functor ϕ^{-1} of $\phi : E \to F$ is order-preserving, i.e.,*

$$\forall A,\ \forall B \in \mathrm{Sub}(F), \quad A \leq B \Rightarrow \phi^{-1}(A) \leq \phi^{-1}(B). \tag{3.3.7}$$

□

Proof. Let $A, B \in \mathrm{Sub}(F)$ such that $A \leq B$. Suppose that $e \in \phi^{-1}(A)C$ ($C \in \mathbf{C}$). Then $\phi_C(e) \in AC \subseteq BC$, since $A \leq B$. Hence, $e \in \phi^{-1}(B)C$. Therefore, $\phi^{-1}(A) \leq \phi^{-1}(B)$. The proof is complete. ■

Fact 3.3.6. *Let E and F be two sheaves on $(\mathbf{C}, J)$. For any natural transformation $\phi : E \to F$, the pullback functor $\phi^{-1} : \mathrm{Sub}(F) \to \mathrm{Sub}(E)$ has both a left adjoint $\exists_\phi$ and a right adjoint $\forall_\phi$:*

$$\exists_\phi \dashv \phi^{-1} \dashv \forall_\phi. \tag{3.3.8}$$

The left adjoint $\exists_\phi$ is described explicitly as follows: for $C \in \mathbf{C}$ and $y \in FC$,

$$y \in \exists_\phi(A)C \Leftrightarrow \{f : D \to C \mid \exists a \in AD,\ \phi_D(a) = (Ff)(y)\} \in J(C). \tag{3.3.9}$$

The right adjoint $\forall_\phi$ is described explicitly as follows: for $C \in \mathbf{C}$ and $y \in FC$,

$$\begin{aligned} y \in \forall_\phi(A)C &\Leftrightarrow \forall f : D \to C, \quad \phi_D^{-1}(\{(Ff)(y)\}) \subseteq AD; \\ &\Leftrightarrow \forall f : D \to C, \forall x \in EC, [\phi_D(x) = (Ff)(y) \Rightarrow x \in AD]. \end{aligned} \tag{3.3.10}$$

□

Proof. We shall prove that $\exists_\phi$ and $\forall_\phi$ described as (3.3.9) and (3.3.10) are indeed a left and a right adjoint of the pullback functor ϕ^{-1} of ϕ.

($\exists_\phi$) First, we must verify that $\exists_\phi(A)$ is a subfunctor of F for all $A \in \mathrm{Sub}(E)$. By definition, $\exists_\phi(A)C \subseteq FC$ for all $C \in \mathbf{C}$. Let $g : C' \to C$ and $y \in \exists_\phi(A)C$. We must prove that $(Fg)(y) \in \exists_\phi(A)C'$. To this end, put

$$S := \{f : D \to C \mid \exists a \in AD,\ \phi_D(a) = (Ff)(y)\}.$$

Then $S \in J(C)$, since $y \in \exists_\phi(A)C$. By the stability axiom of J, $g^*(S) \in J(C')$. We claim that $g^*(S) = \{h : D \to C' \mid \exists a \in AD, \phi_D(a) = (Fh)((Fg)(y))\}$. Let $h : D \to C' \in g^*(S)$. Then $gh \in S$. Hence,

$$\exists a \in AD, \quad \phi_D(a) = (F(gh))(y) = (Fh)((Fg)(y)).$$

Conversely, let $h : D \to C'$ and suppose that

$$\exists a \in AD, \quad \phi_D(a) = (F(gh))(y) = (Fh)((Fg)(y)).$$

Then $gh \in S$, i.e., $h \in g^*(S)$. Therefore, we obtain

$$g^*(S) = \{h : D \to C' \mid \exists a \in AD, \phi_D(a) = (Fh)((Fg)(y))\} \in J(C'),$$

that is, $(Fg)(y) \in \exists_\phi(A)C'$.

Next, we shall prove that $\exists_\phi(A)$ is a subsheaf of F for all $A \in \mathrm{Sub}(E)$. To this end, let $C \in \mathbf{C}$, $y \in FC$ and $S \in J(C)$. Suppose that for all $f : D \to C \in S$, $(Ff)(y) \in \exists_\phi(A)D$. Consider a sieve on C

$$R := \{h : D \to C \mid \exists a \in AD,\ \phi_D(a) = (Fh)(y)\}.$$

If we can show that $f^*(R) \in J(D)$ for all $f : D \to C \in S$, then, by the transitivity axiom of J, $R \in J(C)$ and we obtain $y \in \exists_\phi(A)C$. To this end, let $f : D \to C \in S$ and consider $f^*(R)(= \{g : D' \to D \mid fg \in R\})$. We claim that

$$f^*(R) = \{g : D' \to D \mid \exists a \in AD',\ \phi_{D'}(a) = (Fg)((Ff)(y))\}.$$

Indeed,

$$\begin{aligned}
&g : D' \to D \in f^*(R) \\
\Leftrightarrow\ & fg \in R \\
\Leftrightarrow\ & \exists a \in AD', \quad \phi_{D'}(a) = (F(fg))(y) = (Fg)((Ff)(y)) \quad \text{(by the definition of } R\text{).}
\end{aligned}$$

Since $(Ff)(y) \in \exists_\phi(A)D$, we have

$$\{g : D' \to D \mid \exists a \in AD',\, \phi_{D'}(a) = (Fg)((Ff)(y))\} \in J(D).$$

From the above, we obtain $y \in \exists_\phi(A)C$. Therefore, $\exists_\phi(A)$ is a subsheaf of F.

Finally, we shall prove that $\exists_\phi$ is a left adjoint of ϕ^{-1}, i.e., $\exists_\phi$ satisfies the following condition:

$$\forall A \in \mathrm{Sub}(E),\, \forall B \in \mathrm{Sub}(F), \quad \exists_\phi(A) \leq B \Leftrightarrow A \leq \phi^{-1}(B). \tag{3.3.11}$$

To show this, let $A \in \mathrm{Sub}(E)$ and $B \in \mathrm{Sub}(F)$.

($\Rightarrow$) Suppose that $\exists_\phi(A) \leq B$. Let $C \in \mathbf{C}$ and $a \in AC$. Then for all $f : D \to C \in t_C \in J(C)$, $(Ef)(a) \in AD$. By the naturality of ϕ, $(Ff)(\phi_C(a)) = \phi_D((Ef)(a))$. Hence,

$$\{f : D \to C \mid \exists a \in AD,\, \phi_D(a) = (Ff)(\phi_C(a))\} = t_C \in J(C).$$

Therefore, $\phi_C(a) \in \exists_\phi(A)C$. By assumption, $\exists_\phi(A)C \subseteq BC$. Thus, we obtain $\phi_C(a) \in BC$, i.e., $a \in \phi^{-1}(B)C$.

($\Leftarrow$) Suppose that $A \leq \phi^{-1}(B)$. Let $C \in \mathbf{C}$ and $y \in \exists_\phi(A)C$. Then

$$\{f : D \to C \mid \exists a \in AD,\, \phi_D(a) = (Ff)(y)\} \in J(C).$$

Put $S := \{f : D \to C \mid \exists a \in AD,\, \phi_D(a) = (Ff)(y)\}$ for short. By assumption, $AD \subseteq \phi^{-1}(B)D$. Hence, if $a \in AD$, then $\phi_D(a) \in BD$. Therefore, we have

$$\forall f : D \to C \in S, \quad (Ff)(y) \in BD.$$

Since B is a subsheaf of F, we obtain $y \in BC$.

From the above, the proof of (3.3.11) is complete and $\exists_\phi$ is a left adjoint of ϕ^{-1}.

($\forall_\phi$) We shall consider the right adjoint $\forall_\phi$. First, we must verify that $\forall_\phi(A)$ is a subfunctor of F for all $A \in \mathrm{Sub}(E)$. By definition, $\forall_\phi(A)C \subseteq FC$ for all $C \in \mathbf{C}$. Let $g : C' \to C$ and $y \in \forall_\phi(A)C$. Then for all $h : D \to C'$, $\phi_D^{-1}(\{(Fh)((Fg)(y))\}) = \phi_D^{-1}(\{(F(gh))(y)\}) \subseteq AD$, since $y \in \forall_\phi(A)C$. This implies that $(Fg)(y) \in \forall_\phi(A)C'$.

Next, we shall prove that $\forall_\phi(A)$ is a subsheaf of F for all $A \in \mathrm{Sub}(E)$. To this end, let $C \in \mathbf{C}$, $y \in FC$ and $S \in J(C)$ and suppose that

$$\forall f : D \to C \in S, \quad (Ff)(y) \in \forall_\phi(A)D.$$

Let $g : C' \to C$ and $x \in ED$ such that

$$\phi_{C'}(x) = (Fg)(y). \tag{3.3.12}$$

It is sufficient to prove that $x \in AC'$. Consider $g^*(S) \in J(C')$. Then for all $h : D \to C' \in g^*(S)$, $gh \in S$ and hence, $(F(gh))(y) \in \forall_\phi(A)D$, by assumption. By (3.3.12) and the naturality of ϕ,

$$(Fh)((Fg)(y)) = (Fh)(\phi_{C'}(x)) = \phi_D((Eh)(x)).$$

Since $(F(gh))(y) \in \forall_\phi(A)D$, this implies that $(Eh)(x) \in AD$ for all $h : D \to C' \in g^*(S) \in J(D)$. Since A is a subsheaf of E, we obtain $x \in AC'$. Hence, $y \in \forall_\phi(A)C$. Therefore, $\forall_\phi(A)$ is a subsheaf of F.

Finally, we shall prove that $\forall_\phi$ is a right adjoint of ϕ^{-1}, i.e., $\forall_\phi$ satisfies the following condition:

$$\forall A \in \mathrm{Sub}(E),\ \forall B \in \mathrm{Sub}(F), \quad \phi^{-1}(B) \leq A \Leftrightarrow B \leq \forall_\phi(A). \tag{3.3.13}$$

($\Rightarrow$) Suppose that $\phi^{-1}(B) \leq A$. Let $y \in BC\,(C \in \mathbf{C})$, $f : D \to C$ and $x \in EC$ such that

$$\phi_D(x) = (Ff)(y).$$

It is sufficient to prove that $x \in AD$. Since $\phi_D(x) = (Ff)(y) \in BD$. By the definition of ϕ^{-1}, we have $x \in \phi^{-1}(B)(D)$. By the assumption that $\phi^{-1}(B) \leq A$, we obtain $x \in AD$. Hence, $y \in \forall_\phi(C)$. Therefore, $B \leq \forall_\phi(A)$.

($\Leftarrow$) Suppose that $B \leq \forall_\phi(A)$. Let $x \in \phi^{-1}(B)C$ $(C \in \mathbf{C})$, i.e., $\phi_C(x) \in BC$. By assumption, $x \in \forall_\phi(A)C$. Hence, for all $f : D \to C \in t_C \in J(C)$,

$$AD \supseteq \phi_D^{-1}(\{(Ff)(\phi_C(x))\}) = \phi_D^{-1}(\{\phi_D((Ef)(x))\}) \quad (\because \phi \text{ is natural}).$$

Therefore, $(Ef)(x) \in AD$ for all $f : D \to C \in t_C \in J(C)$. Since A is a subsheaf of E, we obtain $x \in AC$. Thus, $\phi^{-1}(B) \leq A$.

From the above, the proof of (3.3.13) is complete and $\forall_\phi$ is a right adjoint of ϕ^{-1}.

The proof is complete. ■

To conclude this section, we shall consider some examples.

Fact 3.3.7. *Let* $\mathbf{H}$ *be a complete Heyting algebra and* J *the sup topology (see [3, Example 3.1.3] on* $\mathbf{H}$. *Let* 1 *be the terminal object of* $\mathrm{Sh}(\mathbf{H}, J)$ *(fix the representation of* 1 *as* $1(a) := \{0\}$ *for all* $a \in \mathbf{H}$). *Then a mapping* $\varphi : \mathrm{Sub}(1) \to \mathbf{H}$ *defined for* $S \in \mathrm{Sub}(1)$ *by*

$$\varphi(S) := \bigvee \{c \mid 0 \in S(c)\} \tag{3.3.14}$$

is an order isomorphism. That is, any complete Heyting algebra can be realized as the complete Heyting algebra of subobjects of the terminal object in a Grothendieck topos. □

Proof. First of all, we shall prove that

$$\forall a \in \mathbf{H},\ \forall S \in \mathrm{Sub}(1), \quad a \leq \varphi(S) \Leftrightarrow 0 \in S(a).$$

Let $a \in \mathbf{H}$ and $S \in \mathrm{Sub}(1)$.

($\Rightarrow$) Suppose that $a \le \varphi(S)$. Since J is the sup topology, $\{c \mid 0 \in S(c)\} \in J(\varphi(S))$. Since S is a subsheaf of 1, $0 \in S(\varphi(S))$. By the assumption that $a \le \varphi(S)$, this implies that $0 \in S(a)$.

($\Leftarrow$) Suppose that $0 \in S(a)$. Then $a \le \bigvee\{c \mid 0 \in S(c)\} = \varphi(S)$.

Next, we shall prove that φ is injective. To this end, let $S, T \in \mathrm{Sub}(E)$ such that $\varphi(S) = \varphi(T)$. It is sufficient to prove that $0 \in S(a) \Leftrightarrow 0 \in T(a)$ for all $a \in \mathbf{H}$. If $0 \in S(a)$, then $a \le \varphi(S) = \varphi(T)$, i.e., $0 \in T(a)$. By symmetry, $0 \in T(a)$ implies that $0 \in S(a)$. Hence, $S = T$. Therefore, φ is injective.

Next, we shall prove that φ is surjective. To this end, let $s \in A$. Define $S \in \mathrm{Sub}(1)$ for $a \in \mathbf{H}$ by

$$S(a) := \begin{cases} \{0\} & (a \le s), \\ \emptyset & (a \not\le s). \end{cases}$$

We must verify that S is a subsheaf of 1. By definition, $S(a) \subseteq \{0\}$ for all $a \in \mathbf{H}$. Let $a \le b$ $(a, b \in \mathbf{H})$. If $0 \in S(b)$, then $a \le b \le s$. Hence, $0 \in S(a)$. Therefore, S is a subfunctor of 1. Let $a \in \mathbf{H}$ and $\{a_i\}_{i \in I} \in J(a)$, i.e., $a = \bigvee_{i \in I} a_i$. Suppose that for all $i \in I$, $0 \in S(a)$, i.e., $a_i \le s$. Then $a = \bigvee_{i \in I} a_i \le s$, by the definition of the supremum. Hence, $0 \in S(a)$. Therefore, S is a subsheaf of 1. Since $\varphi(S) = \bigvee\{c \mid 0 \in S(c)\} = s$, φ is surjective.

Finally, we shall prove that φ is an order isomorphism, i.e.,

$$\forall S, \forall T \in \mathrm{Sub}(1), \quad S \le T \Leftrightarrow \varphi(S) \le \varphi(T).$$

Let $S, T \in \mathrm{Sub}(1)$.

($\Rightarrow$) Suppose that $S \le T$. Then for all $a \in \mathbf{H}$, $S(a) \subseteq T(a) \subseteq \{0\}$. This implies that
$$\varphi(S) = \bigvee\{a \mid 0 \in S(a)\} \le \bigvee\{a \mid 0 \in T(a)\} = \varphi(T).$$

($\Leftarrow$) Suppose that $\varphi(S) \le \varphi(T)$. Let $a \in \mathbf{H}$. If $0 \in S(a)$, then $a \le \varphi(S) = \varphi(T)$, i.e., $0 \in T(a)$. Hence, $S(a) \subseteq T(a)$ for all $a \in \mathbf{H}$, i.e., $S \le T$.

The proof is complete. ■

Let $(\mathbf{C}, J)$ be a site and E be a sheaf on $(\mathbf{C}, J)$. Since a product over the empty-set $\emptyset$ is a singleton, if $\emptyset \in J(C)$ $(C \in \mathbf{C})$, then the sheaf condition for E is described as the following equalizer diagram for some two morphisms a and p (see [3, Remark 3.2.1] for details):

$$EC \xrightarrow{e} \{*\} \overset{p}{\underset{a}{\rightrightarrows}} \{*\}.$$

This implies that EC is also a singleton. Accordingly, we shall write x_C for this unique element of EC.

Fact 3.3.8. *A mapping* $0 : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets}$ *defined for* $C \in \mathbf{C}$ *by*

$$0C := \begin{cases} \{x_C\} & (\emptyset \in J(C)), \\ \emptyset & (\emptyset \notin J(C)) \end{cases} \tag{3.3.15}$$

is the smallest subsheaf of E, where $x_C \in EC$ is the unique element of the matching family for $\emptyset \in J(C)$ of E. □

Proof. Let $f : D \to C$. First, note that if $\emptyset \in J(C)$, then $f^*(\emptyset) = \emptyset \in J(D)$, by the stability axiom of J. Hence, $(Ef)(x_C) = x_D$. This implies that 0 is a subfunctor of E.

Next, we shall prove that 0 is a subsheaf of E. To this end, let $C \in \mathbf{C}$, $x \in EC$ and $S \in J(C)$. Suppose that for all $f : D \to C \in S$, $(Ef)(x) \in 0D$. Then $(Ef)(x) = x_D \in 0D$. Hence, $\emptyset \in J(D)$. This implies that for all $f : D \to C \in S$, $f^*(\emptyset) = \emptyset \in J(D)$. By the transitivity axiom of J, $\emptyset \in J(C)$. Therefore, $EC = \{x_C\}$, i.e., $x = x_C \in 0C$. Thus, 0 is a subsheaf of E, by Lemma 3.2.2. Clearly, 0 is the smallest subsheaf of E. The proof is complete. ■

Let $E \in \mathrm{Sh}(\mathbf{C}, J)$ and $B \in \mathrm{Sub}(E)$.

Definition 3.3.3 (pseudo-complements). The *pseudo-complement* $\neg B$ of B is defined by

$$\neg B := B \to 0 = \bigvee \{U \in \mathrm{Sub}(E) \mid U \wedge B = 0\}. \tag{3.3.16}$$

◊

Recall that

$$x \in (B \to 0)C \Leftrightarrow \forall f : D \to C, \quad (Ef)(x) \in BD \Rightarrow (Ef)(x) \in 0D.$$

Since $0D \neq \emptyset \Leftrightarrow \emptyset \in J(D)$, we have the following fact:

Fact 3.3.9. *The pseudo-complement $\neg B$ of B is described explicitly as follows: for $C \in \mathbf{C}$ and $x \in EC$,*

$$x \in (\neg B)C \Leftrightarrow \forall f : D \to C, \quad (Ef)(x) \in BD \Rightarrow \emptyset \in J(D). \tag{3.3.17}$$

□

Definition 3.3.4 (dense topologies). A sieve S on $C \in \mathbf{C}$ is said to be *dense below* C if

$$\forall f : D \to C, \exists g : D' \to D, \quad fg \in S. \tag{3.3.18}$$

A mapping J defined for $C \in \mathbf{C}$ by

$$J(C) := \{S \mid S \text{ is a sieve on } C \text{ and dense below } C\} \tag{3.3.19}$$

is called the *dense topology* on $\mathbf{C}$. ◊

Fact 3.3.10. *The dense topology J is a Grothendieck topology.* □

Proof. We shall prove that the dense topology J satisfies all the axioms of a Grothendieck topology, i.e., (i) $t_C \in J(C)$ for all $C \in \mathbf{C}$; (ii) stability axiom; (iii) transitivity axiom.

(i) Since for all $f : D \to C$, $f = f\mathrm{id}_D \in t_C$, the maximal sieve t_C is dense below C.

(ii) Let $S \in J(C)$ and $h : C' \to C$. We shall prove that $h^*(S)$ is dense below C'. To this end, let $f : D' \to C'$. Then, since S is dense below C, for $hf : D' \to C$, there exists $g : D'' \to D'$ such that $hfg \in S$, i.e., $fg \in h^*(S)$. This implies that $h^*(S)$ is dense below C'.

(iii) Let $S \in J(C)$ and R be a sieve on C. Suppose that for all $h : D' \to C \in S$, $h^*(R) \in J(D')$, i.e., $h^*(R)$ is dense below D'. Let $f : D \to C$. Since S is dense below C, there exists $g : D' \to D$ such that $fg \in S$. By assumption, $(fg)^*(R)$ is dense below D'. Therefore, for $\mathrm{id}_{D'} : D' \to D'$, there exists $k : D'' \to D'$ such that $k = \mathrm{id}_{D'}k \in (fg)^*(R)$, i.e., $f(gk) \in R$. This implies that R is dense below C.

The proof is complete. ■

Note that if a sieve S on C is dense below C, then $S \neq \emptyset$. Therefore, for the dense topology J, $\emptyset \notin J(C)$ for all $C \in \mathbf{C}$.

Fact 3.3.11. *Let J be the dense topology. Then for all $C \in \mathbf{C}$,*

$$(\neg B)C = \{x \in EC \mid \forall f : D \to C, \quad (Ef)(x) \notin BD\}. \tag{3.3.20}$$

Moreover, for all $E \in \mathrm{Sh}(\mathbf{C}, J)$, $(\mathrm{Sub}(E), \leq)$ is a complete Boolean algebra. □

Proof. We shall prove that $(\mathrm{Sub}(E), \leq)$ is a complete Boolean algebra. Let $x \in EC$ $(C \in \mathbf{C})$. Put

$$S_x := \{f : D \to C \mid (Ef)(x) \in BD \text{ or } (Ef)(x) \in (\neg B)D\}.$$

We claim that S_x is dense below C, i.e., for all $f : D \to C$, there exists $g : E \to D$ such that $gh \in S_x$. To show this, let $f : D \to C$. We have the following two cases:

(i) There exists $g : D' \to D$ such that $(Eg)((Ef)(x)) \in BD'$. Then $(E(fg))(x) \in BD'$, i.e., $fg \in S_x$.

(ii) For all $g : D' \to D$, $(Eg)((Ef)(x)) \notin BD'$. Then $(Eg)(x) \in (\neg B)D'$, i.e., $g\mathrm{id}_D = g \in S_x$.

We shall prove that $B \vee \neg B = E$. Recall that

$$x \in (B \vee \neg B)C \Leftrightarrow S_x = \{f : D \to C \mid (Ef)(x) \in BD \text{ or } (Ef)(x) \in (\neg B)D\} \in J(C).$$

As we have seen in the above, $S_x \in J(C)$ for all $x \in EC$. Thus, we obtain

$$x \in (B \vee \neg B)C \Leftrightarrow x \in EC.$$

This implies that $B \vee \neg B = E$. The proof is complete. ■

Fact 3.3.12. *Let J be the atomic topology. Then for each sheaf E on $\mathrm{Sh}(\mathbf{C}, J)$, $(\mathrm{Sub}(E), \leq)$ is a complete atomic Boolean algebra.* □

Proof. Recall that the atomic topology J is defined for a category $\mathbf{C}$ such that for all $f : D \to C$ and all $g : D' \to C$, there exists $h : D'' \to D$ and $k : D'' \to D'$ such that $fh = gk$:

$$\begin{tikzcd} D'' \arrow[r, dashed, "\exists k"] \arrow[d, dashed, "\exists h"'] \arrow[dr, phantom, "\circlearrowleft"] & D' \arrow[d, "\forall g"] \\ D \arrow[r, "\forall f"'] & C, \end{tikzcd}$$

and then the atomic topology J is defined for $C \in \mathbf{C}$ by

$$S \in J(C) \overset{\text{def}}{\iff} S \text{ is a non-empty sieve on } C.$$

We claim that the atomic topology J is the dense topology. To prove this, let S be a non-empty sieve on C, $f : D \to C$ and $g : D' \to C \in S$. By the assumption for $\mathbf{C}$, there exists $h : D'' \to D$ and $k : D'' \to D'$ such that $fh = gk$. Since $g \in S$, $fh = gk \in S$. Hence, S is dense below C. Therefore, every non-empty sieve on C is dense below C. As we have seen in the above, $(\mathrm{Sub}(E), \leq)$ is a complete Boolean algebra.

We shall prove that $(\mathrm{Sub}(E), \leq)$ is atomic, i.e., for all $B(\neq 0) \in \mathrm{Sub}(E)$, there exists an atom $A(\neq 0) \in \mathrm{Sub}(E)$ such that $A \leq B$. To this end, let $B(\neq 0) \in \mathrm{Sub}(E)$. Then, since $B \neq 0$, there exists $C \in \mathbf{C}$ such that $BC \neq \emptyset$. Then we fix such $C \in \mathbf{C}$ and $x \in BC$. Define $A_x \in \mathrm{Sub}(E)$ for $D \in \mathbf{C}$ by

$$y \in A_x D \overset{\text{def}}{\iff} \exists f : D' \to C, \exists g : D' \to D, \quad (Eg)(y) = (Ef)(x).$$

We must verify that A_x is a subsheaf of E. First, we shall prove that A_x is a subfunctor of E. To this end, let $h : D'' \to D$ and $y \in A_x D$. Then there exists $f : D' \to C$ and $g' : D' \to D$ such that $(Eg)(y) = (Ef)(x)$. By assumption for $\mathbf{C}$, there exists $k : D''' \to D'$ and $l : D''' \to D''$ such that $gk = hl$:

$$\begin{tikzcd} D''' \arrow[r, "k"] \arrow[d, "l"'] \arrow[dr, phantom, "\circlearrowleft"] & D' \arrow[r, "f"] \arrow[d, "g"] & C \\ D'' \arrow[r, "h"'] & D. & \end{tikzcd}$$

Since $(Eg)(y) = (Ef)(x)$, this implies that

$$\begin{aligned} (El)((Eh)(y)) &= (E(hl))(y) = (E(gk))(y) = (Ek)((Eg)(y)) = (Ek)(Ef)(x) \\ &= (E(fk)(x)). \end{aligned}$$

Hence, $(Eh)(y) \in A_x D''$. Therefore, A_x is a subfunctor of E.

Next, we shall prove that A_x is a subsheaf of E. To this end, let $D \in \mathbf{C}$, $y \in ED$ and $S \in J(D)$. Suppose that for all $h : D' \to D \in S$, $(Eh)(y) \in A_x D'$. Since S is non-empty, we can take $h : D' \to D \in S$ and fix it. Then there exists $k : D'' \to C$ and $l : D'' \to D'$ such that $(E(hl)(y)) = (El)((Eh)(y)) = (Ek)(x)$. This implies that $y \in A_x D$. Hence, A_x is a subsheaf of E. Moreover, since $x \in BC$ satisfies that $x = (E\mathrm{id}_C)(x)$, we have $x \in A_x C \neq \emptyset$. Therefore, $A_x \neq 0$.

Next, we shall prove that A_x is an atom of $\mathrm{Sub}(E)$, i.e., for all $A(\neq 0) \in \mathrm{Sub}(E)$, if $A \leq A_x$, then $A = A_x$. To this end, let $A(\neq 0) \in \mathrm{Sub}(E)$. Suppose that $A \leq A_x$. It is sufficient to prove that $A_x \leq A$. Since $A \neq 0$, there exists $x' \in AC'$ for some $C' \in \mathbf{C}$. By the assumption $A \leq A_x$, we have $x' \in A_x C'$. Hence, there exits $f' : D'' \to C$ and $g' : D'' \to C'$ such that

$$(Eg')(x') = (Ef')(x) \in AD'''.$$

To prove that $A_x \leq A$, let $D \in \mathbf{C}$ and $y \in A_x D$. Then there exists $f : D' \to C$ and $g : D' \to D$ such that

$$(Eg)(y) = (Ef)(x).$$

By the condition for $\mathbf{C}$, for $f : D' \to C$ and $f' : D'' \to C'$, there exists $h : D''' \to D'$ and $k : D''' \to D''$ such that $fh = f'k$:

$$\begin{tikzcd}
D''' \arrow[r, "h"] \arrow[d, "k"'] \arrow[dr, phantom, "\circlearrowleft"] & D' \arrow[r, "g"] \arrow[d, "f"] & D \\
D'' \arrow[r, "f'"'] & C. &
\end{tikzcd}$$

From the above, we have

$$(Ek)((Eg')(x')) = (E(f'k))(x) = (E(fh))(x) = (Eh)((Ef)(x)) = (Eh)((Eg)(y)).$$

Therefore, $(E(gh))(y) \in AD'''$. Since A is a subsheaf of E for the atomic topology, this implies that $y \in AD$. To prove this, consider the sieve (gh) generated by $\{gh\}$. Since J is the atomic topology, we have $(gh) \in J(D)$. Hence, for all $ghl \in (gh)$, $(E(ghl))(y) = (El)(E(gh)(y)) \in A(\mathrm{dom}(l))$, since A is a subfunctor of E. Since A is a subsheaf of E, this implies that $y \in AD$. Thus, $A = A_x$.

Finally, we shall prove that $A_x \leq B$, i.e., $A_x D \subseteq BD$ for all $D \in \mathbf{C}$. To this end, let $y \in A_x D$. Then there exists $f : D' \to C$ and $g : D' \to C$ such that $(Eg)(y) = (Ef)(x)$. Since $x \in BC$, $(Eg)(y) = (Ef)(x) \in BD'$. Consider the sieve (g) generated by $\{g\}$. Since J is the atomic topology, $(g) \in J(D)$. Hence, for all $gh \in (g) \in J(D)$, $(E(gh))(y) = (Eh)((Eg)(y)) \in BD''$. Since B is a subsheaf of E, we obtain $y \in BD$. Therefore, $A_x D \subseteq BD$. The proof is complete. ■

参考文献

[1] S. Mac Lane, *Categories for the Working Mathematician*, Springer-Verlag, 1971.

[2] S. Mac Lane and I. Moerdijk, *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*, corrected 2nd ed., Springer, 1994.

[3] 古賀 実,「Grothendieck 位相・サイト上の層・層化関手に関するノート」, The Dark Side of Forcing vol. IV, 第 3 章, 2014, (http://forcing.nagoya/).

第 4 章

Δ-system lemma (“スタート集合論” ノート WIP2)

才川 隆文

昨年から名古屋で開催している集合論勉強会 (“スタート集合論”) は, 参加者の方々の多大なご協力により, 当初の目標であった, Con(ZFC) → Con(ZFC+¬CH) の証明を終えることができました. ただし途中にいくつか飛ばした補題や議論もあり, そのうちの一つが Δ-system lemma でした. 準備したものの日の目を見なかった Δ-system についてのノートを整理したものが, 本稿の内容です.

4.1 notations

本ノートは, 構成, 定義, 定理などについて Kunen 本 [1] を参考にしていますが, いくつか特に異なる記法を採用しています.

1. 量化子を含む式の括弧の省略方法について, Coq [2] と同様の扱いをします. すなわち量化子による変数束縛は, 可能なかぎり式の終わりの方まで範囲を広げることにします. 例えば
$$\exists x,\ 0 \in x\ \land\ \forall y \in x,\ S(y) \in x$$
に括弧をつけると
$$\exists x,\ (0 \in x\ \land\ (\forall y \in x,\ (S(y) \in x)))$$
となります.
2. 内包記法の区切り文字がセミコロンではなく縦棒です. つまり $\{x \in X;\ \varphi(x)\}$ ではなく $\{x \in X \mid \varphi(x)\}$ と書きます.

4.2 Δ-system lemma

本節では Δ-system lemma の証明を目標とします. まず Δ-system の定義から.

Definition 1 集合 A が Δ-system であるとは, 集合 r が存在して, A の相異なる 2 要素 x, y について, その共通部分がつねに r になること. 即ち,

$$\boxed{\dfrac{A : \text{set}}{A\text{ が }\Delta\text{-system である} \overset{def}{\iff} \exists r,\ \forall x, y \in A,\ x \neq y \to x \cap y = r}}\ .$$

r を, この Δ-system の root という.

例えば, $\{\{0,1\}, \{0,1,2\}, \{0,1,3\}\}$ は $\{0,1\}$ を root とする Δ-system ですが, $\{\{0,1\}, \{0,1,2\}, \{0,1,2,3\}\}$ は Δ-system ではありません.

目標の定理は次のようになります.

Theorem 1 (Δ-system lemma) 有限集合を要素とする非可算集合 A に対して, A の部分集合 B で, 非可算かつ Δ-*system* であるものが存在する.

$$\boxed{\dfrac{A : \mathit{uncountable} \qquad \forall x \in A,\ x : \mathit{finite}}{\exists B \subset A,\ B : \mathit{uncountable}\ \wedge\ B : \Delta\text{-}\mathit{system}}}\ .$$

このままだと証明しにくいので, いくつかの変形をします. まず, A, B の濃度を ω_1 に固定します. 固定した形で証明ができれば, 一般の A についても, A の, 濃度 ω_1 の部分集合を考えることで, 濃度 ω_1 の B が得られ, これは非可算です.

$$\boxed{\dfrac{|A| = \omega_1 \qquad \forall x \in A,\ x : \text{finite}}{\exists B \subset A,\ |B| = \omega_1\ \wedge\ B : \Delta\text{-system}}}\ .$$

次に, A を, その要素の大きさで切り分けます.

$$A = \bigcup_{n<\omega} A_n, \quad \text{where } A_n = \{x \in A \mid |x| = n\}\ .$$

ω_1 は regular ですから, 少なくとも一つの A_n は ω_1 です. よって, A の要素の濃度を固定した次の goal を示せば, 元の goal も得られることになります.

$$\boxed{\dfrac{|A| = \omega_1 \qquad n \in \omega \qquad \forall x \in A,\ |x| = n}{\exists B \subset A,\ |B| = \omega_1\ \wedge\ B : \Delta\text{-system}}}\ .$$

もう一つ仮定を入れますが, 準備として, A を一回 flatten [*1] した集合を X とします（A を文字列のようなものの集合だと思うと, X は文字の集合）.

$$X = \bigcup A$$

すると次が成り立ちます.

[*1] ここでいう flatten は, 木構造を 1 段階つぶす関数であり, 使用例を挙げると, `flatten`$(\{\{1,2\}, \{3, \{4\}\}\}) = \{1, 2, 3, \{4\}\}$ となります.

Lemma 1 *1.* $A \subset X^n$.

2. $|X| \leq |A|$.

3. $|X| = \omega_1$.

Proof. 1. X^n は X の要素からなる濃度 n の有限集合を全て集めた集合なので, A はその部分集合になる.

2. $n \times A$ から X への写像を $\langle k, x\rangle \mapsto x(k)$ （ただし $x(k)$ は x の k 番目の要素）とすると, これは A の要素の要素を全て取り出すので X への全射であり, $|A| = |n \times A|$ であるので, $|X| \leq |A|$ となる.

3. 1 と $|X^n| = |X|$ から $|A| \leq |X|$ が得られ, 2 および $|A| = \omega_1$ とあわせて, $|X| = \omega_1$ となる. ■

今後 X を整列して扱いますが, X の要素の中身まで立ち入ることはないので, 仮定として $X \subset \omega_1$ を入れ, 次の goal を示すことにします.

$$\boxed{\begin{array}{l} |A| = \omega_1 \\ X := \bigcup A \\ X \subset \omega_1 \text{ , uncountable} \\ n \in \omega \\ \forall x \in A,\ |x| = n \\ \hline \exists B \subset A,\ |B| = \omega_1 \ \wedge\ B : \Delta\text{-system} \end{array}}\ .$$

さてここから証明に入りますが, 方針は,

1. root の候補を探し,
2. root の長さについて帰納法を回し,
3. base case として ω_1 についての帰納法で Δ-system を作る.

として進めます.

root の候補 r は, 以下のように定義できます.

$$\begin{cases} r_0 := 0; \\ X_k := \{x \in X - r_k \mid \exists B \subset A,\ |B| = \omega_1\ \wedge\ (r_k \cup \{x\}) \subset \bigcap B\}\,; \\ \begin{cases} X_k \text{ が空でなければ, その最小元を } x_k \text{ として, } r_{k+1} := r_k \cup \{x_k\}. \\ X_k \text{ が空ならばループおわり.} \end{cases} \end{cases}$$

$$r_{A,n} := r := \bigcup_k r_k$$

各 r_k について, A の非可算部分集合 B で, 共通部分が r_k となるようなものを取ることができます. X_k は, そのような非可算部分集合 B を取ることができるという条件を維持しつつ r_k に付け加えることのできる文字 x を集めたものです. r はループ終了時点の r_k に一致し, このとき $k = |r|$ です.

A の要素の濃度は n なので, r の濃度は n 未満です. ここで r の濃度について帰納法を回し, goal を証明することを試みてみましょう. まず帰納ステップについて, $|r| = m$ のときに goal が成り立つと仮定して, $|r| = m + 1$ のときを示します. すなわち,

$$
\boxed{\begin{array}{l}
m \in \omega \\
\mathrm{IH} : \forall A,\ \forall n \in \omega,\ |A| = \omega_1\ \wedge\ \bigcup A = \omega_1\ \wedge\ (\forall x \in A,\ |x| = n)\ \wedge\ |r_{A,n}| = m \\
\qquad\qquad \to \exists B \subset A,\ |B| = \omega_1\ \wedge\ B : \Delta\text{-system} \\
|A| = \omega_1 \\
X := \bigcup A \\
X \subset \omega_1\ \text{, uncountable} \\
n \in \omega \\
\forall x \in A,\ |x| = n \\
r := r_{A,n} \\
|r| = m + 1 \\
\hline
\exists B \subset A,\ |B| = \omega_1\ \wedge\ B : \Delta\text{-system}
\end{array}}
$$

という subgoal を示します．

$r = r_{m+1}$ であり，x_m，X_m の定義より A の部分集合 B で，$|B| = \omega_1$ と $(r_m \cup \{x_m\}) \subset \bigcap B$ をみたすものが存在します．B の各要素から x_m を削除したものを集め，$B_0 := \{b - \{x_m\} \mid b \in B\}$ とすると，$|r_{B_0,n-1}| = m$ であり，帰納法の仮定 IH を使うのに必要な他の仮定も全てみたしています．そこで IH を使うと，B_0 の部分集合 B_1 で，非可算な Δ-system であるものが得られます．B_1 の各要素に再び x_m を付け足して，$B_2 := \{b \cup \{x_m\} \mid b \in B_1\}$ とすれば，これは非可算な Δ-system で，A の部分集合となります．

残りは base case, $|r| = 0$ の場合です．これを言いかえると，

$$
\begin{aligned}
|r| = 0 &\iff \left\{x \in X - r_0 \;\middle|\; \exists B \subset A,\ |B| = \omega_1\ \wedge\ (r_0 \cup \{x\}) \subset \bigcap B\right\} = 0 \\
&\iff \left\{x \in X \;\middle|\; \exists B \subset A,\ |B| = \omega_1\ \wedge\ x \in \bigcap B\right\} = 0 \\
&\iff \neg\exists x \in X,\ \exists B \subset A,\ |B| = \omega_1\ \wedge\ x \in \bigcap B \\
&\iff \forall x \in X,\ \forall B \subset A,\ x \in \bigcap B \to |B| \leq \omega
\end{aligned}
$$

となります．この言いかえを含めて，goal を整理しておきます．

$$
\boxed{\begin{array}{l}
|A| = \omega_1 \\
X := \bigcup A \\
X = \omega_1 \\
n \in \omega \\
\forall x \in A,\ |x| = n \\
\forall x \in X,\ \forall B \subset A,\ x \in \bigcap B \to |B| \leq \omega \\
\hline
\exists B \subset A,\ |B| = \omega_1\ \wedge\ B : \Delta\text{-system}
\end{array}}
$$

技術的な理由で $X \subset \omega_1$ という仮定を $X = \omega_1$ と変えましたが，やはり X の要素の中身まで見ないので，この変更で goal は強くも弱くもなりません．

ここまで準備すると, 帰納法で Δ-system をつくることができます (Δ-system といっても今回は root が空なので, 各要素が互いに disjoint な A の部分集合を作ることになります). 以下の ω_1 上の帰納法による定義を見てみましょう. 最終的には $\{s_\alpha \in A \mid \alpha \in \omega_1\}$ が Δ-system となるような定義です.

$$
\text{型}\begin{cases}\{b_\alpha\}_\alpha : \omega_1 \to X \\ \{B_\alpha\}_\alpha : \omega_1 \to \mathcal{P}(A) \\ \{s_\alpha\}_\alpha : \omega_1 \to A\end{cases}
$$

$$
\text{値}\begin{cases}\begin{cases}b_0 := 0 \\ b_{\alpha+1} := \max(s_\alpha) + 1 \\ b_\lambda := \sup_{\alpha<\lambda}(b_\alpha) \qquad \text{for } \lambda : \text{limit}\end{cases} \\ B_\alpha := \{s \in A \mid \min(s) \geq b_\alpha\} \\ s_\alpha := \phi(B_\alpha)\end{cases}
$$

ただし, ϕ は $\mathcal{P}(A)$ 上の choice function とする.

あってないようなものですが型を考えると, b_α は $X = \omega_1$ の要素（文字）, B_α は A の部分集合（文字列の集合）, s_α は A の要素 (文字列) です. 作りかたを見ると, B_α は, どの要素 s のどの文字をとっても b_α 以上となるように作っています. s_α は, B_α が空でないとき, その要素を一つ選んだものです. b_α は, s_α に含まれるどの文字よりも大きい文字として定義しています.

この定義が上手く行くためには, B_α がどれも空でないことが示されなければなりません. これを示しましょう.

Lemma 2 任意の $\alpha \in \omega_1$ について, $B_\alpha \neq 0$.

Proof. $\alpha \in \omega_1$ とする. B_α が空だと仮定すると, B_α の定義より,

$$
\forall s \in A,\ \min(s) < b_\alpha
$$

となる. このとき A を分解すると, 次のようになる.

$$
A = \bigcup_{\beta < b_\alpha} A_\beta, \quad \text{where } A_\beta = \{s \in A \mid \min(s) = \beta\}.
$$

仮定

$$
\forall x \in X,\ \forall B \subset A,\ x \in \bigcap B \to |B| \leq \omega
$$

を用いると, 各 A_β は可算だが, 一方で仮定 $|A| = \omega_1$ と, ω_1 の regularity より, 少なくとも一つは非可算な A_β が存在するので, 矛盾が生じる. よって, B_α は空ではない. ■

これで定義はうまくゆきました. $\{s_\alpha \in A \mid \alpha \in \omega_1\}$ が Δ-system であるためには, 任意の $\beta < \alpha \in X$ に対して,

$$
\max(s_\beta) < b_{\beta+1} \leq b_\alpha \leq \min(s_\alpha)
$$

という式がみたされれば十分です. 実際, これが成り立てば, $s_\beta \cap s_\alpha = 0$ であり, よって $\{s_\alpha \in A \mid \alpha \in \omega_1\}$ は各要素が互いに disjoint となって, Δ-system です.

この式のうち, いまだ示されていないのは中央の $b_{\beta+1} \leq b_\alpha$ です. これを示しましょう.

Lemma 3 任意の $\beta, \alpha \in \omega_1$ について, $\beta < \alpha$ ならば $b_{\beta+1} \leq b_\alpha$.

Proof. α について帰納法を行う.

$\alpha = 0$ **のとき**　$\beta < \alpha$ が成りたたない.

$\alpha = \gamma + 1$ **のとき**　$b_\gamma \leq \min(s_\gamma) < b_{\gamma+1} = b_\alpha$ が成りたつ. $\beta < \gamma$ のときは帰納法の仮定から $b_{\beta+1} \leq b_\gamma$ となり, $\beta = \gamma$ のときは $b_\beta = b_\gamma$ となり, いずれの場合も $b_{\beta+1} \leq b_\alpha$ となる.

α **が limit のとき**　α が limit なので, $\beta < \alpha$ から $\beta + 1 < \alpha$ が得られる. 定義より $b_\alpha = \sup_{\beta<\alpha}(b_\beta)$ であったので, $b_{\beta+1} \leq b_\alpha$ となる. ■

これで $\{s_\alpha \in A \mid \alpha \in \omega_1\}$ は A の中の Δ-system であることがわかりました. 添字が ω_1 を渡るので, 濃度も予定通りの ω_1 です.

「以上で Δ-system lemma の証明が終わり, cardinal の保存まで含めて, Cohen forcing による $\mathrm{Con(ZFC)} \to \mathrm{Con(ZFC} + \neg\mathrm{CH)}$ の証明は完結です. 」 こう締め括ることができたら格好よいのですが, 他の部分が未完成なので括弧つきです. 完成版も作成予定なのでご期待下さいませ.

参考文献

[1] Kunen, Kenneth. Set Theory : An Introduction to Independence Proofs. Elsevier North-Holland. 1980.

[2] The Coq Proof Assistant. `http://coq.inria.fr/`

第 5 章

小説　蛇の補題

淡中　圏

蛇は古来より生まれ変わり, 永遠の生命の象徴である. その蛇が川を遡る姿は, 二つの小完全系列の流れに逆らって, 未来から過去への射を構成しようとしているようにも見える.

時間の流れは引き戻せない. どこまでも一方向に流れていく. 人生とはただただその残酷な流れへのわずかな抵抗に過ぎない.

真夜中, 橋の袂の川岸から水の流れを見つめる. 上流に振った雨の濁流が橋脚にぶつかってできるカルマン渦が, 自分の後ろに回り込もうと蛇行していくのが, 灯の下にうっすら光る. 左右に身をゆすぶりながら, 渦巻きは夜の闇の中に, 境目のない媒質の中に消えていく. エントロピーが増大していくのが一目でわかるそのさまは, 時間の空間化として非常に優秀で, ずっと見ていても飽きが来ないのには助かった.

そんな中, 何かが強く光ったのが見えた. 波が光を強く反射したのだろうか. いや違う. それは早い流れの中を, 懸命にサインカーブを描こうとしながら, こちらに向かって川を渡ってくる. 速い流れに飲まれては再び現れ, カルマン渦に巻き取られながらも, しかし前進を諦めない.

それは背中を街灯の明りに光らせた蛇だ. 流れに耐える蛇のその美しさに私の目は釘づけになる. それは抽象的な美さえその身に帯びているように見えた.

水辺に潜む蛇は古来豊穣の象徴であり, 脱皮するその生態は永遠の生命の可能性を人々に思いめぐらさせた. 一方では蛇を失楽園の象徴として悪魔と同一視するユダヤ・キリスト教も, 「青銅の蛇」など復活の象徴としての蛇を持ち合わせている. また蛇を人間に知恵を授け, 邪悪な造物主であるヤルダバオトから我々を開放する救い主と考えるグノーシス主義者も存在したらしい. ギリシャではアスクレピオスの一匹の蛇が絡まった杖は医学の象徴であり, その娘ヒュギエイアの持つ蛇の絡まった杯は薬学の象徴である. さらにヘレニズム思想に起源を持つ錬金術において自らの尾を飲み込む蛇「ウロボロス」は, 相反するものの合一を意味していた.

そして私にとっては？

私にとっては蛇と言えば**蛇の補題**である. 蛇の補題とは二つの短完全系列（図にもあるように実際にはもう少し弱い条件で良いが）の間に系列間の射が存在しているとき, 核の

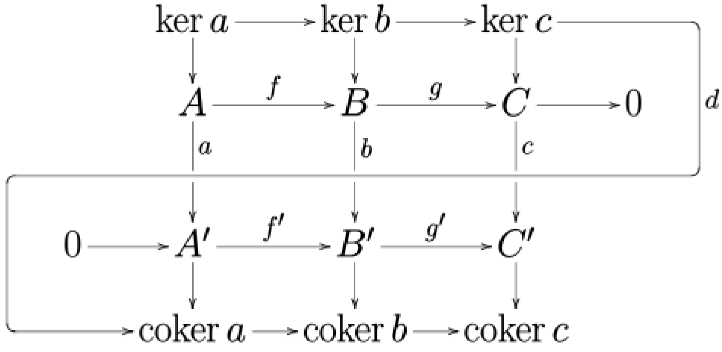


図 5.1
出典: `https://commons.m.wikimedia.org/wiki/File:Snake_lemma_complete.svg`
著作権者: ikamusumeFan
ライセンス: CC BY-SA

系列の最後から, 余核の系列の最初への**連結射**が存在して, その系列が完全になる, という定理である. またこの射はこの梯子型の図式に対して自然性を持つ.

これをコチェイン複体の短完全系列

$$0 \to L^\bullet \to M^\bullet \to N^\bullet \to 0$$

すなわち,

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & L^{p-1} & \to & M^{p-1} & \to & N^{p-1} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & L^{p} & \to & M^{p} & \to & N^{p} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & L^{p+1} & \to & M^{p+1} & \to & N^{p+1} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

に適用すると, コホモロジーの長完全系列

$$\cdots \mathrm{H}^{p-1}(L) \to \mathrm{H}^{p-1}(M) \to \mathrm{H}^{p-1}(N) \xrightarrow{\delta} \mathrm{H}^{p}(L) \to \mathrm{H}^{p}(M) \to \mathrm{H}^{p}(N) \to \cdots$$

ができる. これにより, コホモロジーの計算できているコチェイン複体を使って, いまだ計算のできていないコチェイン複体のコホモロジーを計算していくのだ. 代数的位相幾何や複素幾何、可換環論、代数幾何、など様々な分野にとってなくてはならない道具である. [1]

見方によってはこれは, 短完全系列の強い流れに逆らって, 未来から過去へと作用しようとしているようにも見えるのではなかろうか. 懸命に川を遡ろうとしながらも果しえず, ジグザグにズレていく蛇の蛇行運動が見えないだろうか.

例えば局所体 k とその有限次拡大 E/k を考えよう. すると, 最大不分岐拡大体を完備化した体 $\bar{K} = \bar{k_{\mathrm{ur}}}$ とその有限次拡大 $\bar{L} = E\bar{K}$ は完全分岐拡大になる. そのガロア群 $\mathrm{Gal}(\bar{L}/\bar{K})$ はちょうど拡大 E/k の最大不分岐拡大 $k_0 = E \cap K$ から E への拡大のガロア群と同型になり, 当然これは $\bar{L}$ に作用する. その作用の仕方を $\bar{L}$ の素元 π に対して

$\sigma(\pi)/\pi$ として, 取り出すことにより（これは実はコホモロジー的演算だ）, $\mathrm{Gal}(\bar{\mathrm{L}}/\bar{\mathrm{K}})^{\mathrm{ab}}$ から $\bar{L}$ の整数環の単元群 $U_{\bar{L}}$ を適当な部分群で割った群 $U_{\bar{L}}/V_{\bar{L}}$ に単射が作れる. この像で $U_{\bar{L}}$ を割ると, 射影がノルム写像 $N_{\bar{L}/\bar{K}}$ になり小完全系列

$$1 \to \mathrm{Gal}(\bar{L}/\bar{K})^{\mathrm{ab}} \to U_{\bar{L}}/V_{\bar{L}} \to U_{\bar{K}} \to 1$$

ができる. もう一つ小完全系列を並べて, 蛇の補題を使うことにより, U_{k_0} から $\mathrm{Gal}(\bar{L}/\bar{K})^{\mathrm{ab}}$ への射 $\delta_{E/k}$ を作るのが, 局所類体論の大きなステップである.

これは同型 $\delta_{E/k} : U_k/N_{E/k}(U_E) \cong \mathrm{Gal}(\bar{L}/\bar{K})^{\mathrm{ab}}$ をもたらし, この L による射影極限を取れば, $\delta U_K \cong \mathrm{Gal}(k_{\mathrm{ab}}/k_{\mathrm{ur}})$ ができる.

これに $k^* \cong U_k \times \mathbb{Z}$ であることと, $\mathrm{Gal}(k_{\mathrm{ur}}/k) = \hat{\mathbb{Z}}$ であることを考えると, アルティンの相互写像までもう一歩である. [2]

ここでも短完全系列の流れに逆らおうとする蛇の力が見て取れる. この蛇の力が, すべてのアーベル拡大を支配する類体論の力になるのだ.

蛇はだんだんと流れに流されながら, 橋脚を縫うように川を渡り切って, 川岸の草むらに消えていく. ただそれだけの光景だ. しかし私はその蛇になんとなく力を得たような気がした.

生まれ変わるなどという, 大げさなことは言いたくないが, 少しは流れに抵抗してやろう. ただ流されていく存在ではないことを示してやろう.

しかし安心はできない. 多くのコホモロジーは十分高い次元で消えてしまう. いわゆる消滅定理. これがあるおかげで意味のある次元が定義でき, 具体的計算もできるが, それが我々の限界でもある.

抵抗を続けても, 結局は消えていってしまうのが人の命だ.

だが希望はある.

非可換化だ.

非可換なコホモロジーを考えると, 多くの場合に消滅定理は成り立たない. 次元というものの定義がそもそも意味を成すのか分からなくなる. 空間とは何かという根深い問いに投げ出されてしまう.

しかし, そこに我々の限界を超える何かがあるのもまた確かだ.

不老長生を祈って, 非可換化, 量子化を邁進しようではないか. 蛇が我々を連れていく場所に目を据えながら.

参考文献

[1] B. イヴァセン, 前田博信訳 (1997)『層のコホモロジー』, 丸善出版.

[2] 岩澤健吉 (1980)『局所類体論』, 岩波書店.

淡中 圏　本名：田中健策　前回書くと言っていたことは全く書けなかった。次こそ、次こそ、と呟きながら日々生きている。いい人生だ。

よく分からないブログ　`http://blog.livedoor.jp/kensaku_gokuraku/`

鈴木 佑京　東大大学院総合文化研究科修士一年鈴木・“アルティメット・スパイダーマン面白いよ”・佑京（@otb_btb）です。

就活楽しい!!!　みんなも就活しよう!!

才川 隆文　書道整数論講義とかやりたいですね。著作権保護期間が延長されるまでにやらなきゃ。

古賀 実　制作の始めに Redmine で皆さんにチケットをお配りする係をしました．git の色々な操作にも少しずつ慣れてきました．

平野 智博　この度, 本書を最後まで読んでいただき誠にありがとうございます．今回, 大事と表紙を担当させていただきました．墨と筆で芸術として書くにあたって, 数式やダイアグラムの意味を理解しているかが重要である, と改めて感じさせられました．例えば集合論の宇宙 V の図では, 半順序 p による p-ジェネリックフィルター G を用いてモデル V を拡張する, という流れをもう一度思い返すことで, 確固たるイメージを持って製作することができました．今回作品依頼をしていただいた, 淡中さん, 著者の鈴木さん, 才川さん, 古賀さんにはお礼申し上げます．今後の作品制作の参考にもなるので, また機会があれば, よろしくお願いします．

編集後記:

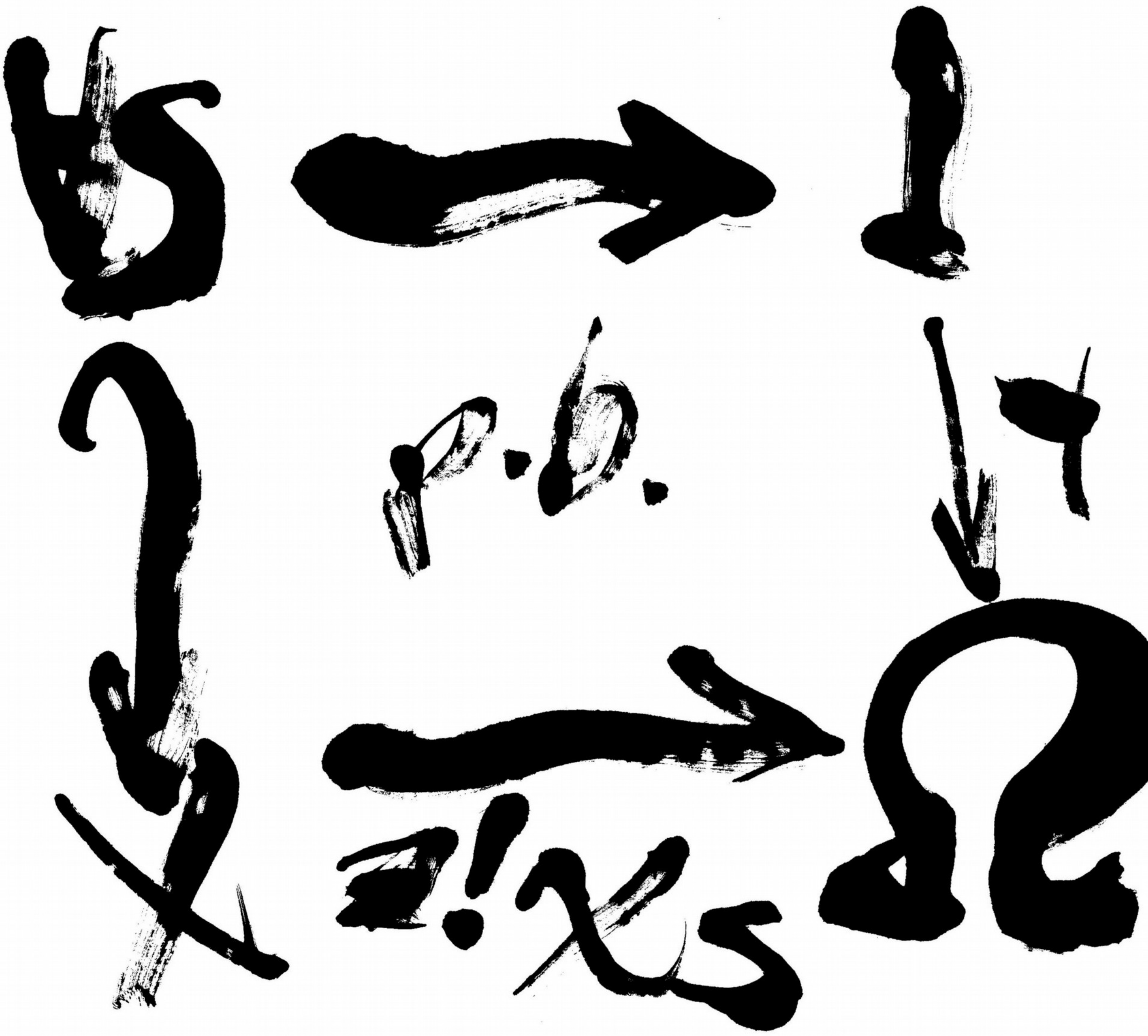
どうにか今回も本が出せそうでなによりです．でも逆に言えば, いろいろとギリギリになりながらも, 本が出せるのは本を出す「形」が決まってきたからに思えます．vps,git,redmine の同人誌製作三種の神器の使い方にもかなり慣れてきました．だからこそ, 次回は何か冒険がしたい! とりあえず原稿集めるの早くしてオフセット本にするのは規定としても, なんか馬鹿な企画が立てられないものか．先進的でマニアックなソフトで本を作るとか, 高度すぎる内容を高校生に教えようとする授業計画書を付録につけるとか．数学書道の tumblr 開くとかもいいかもなあ．

うはー　夢が広がりんぐ（淡中圏）

発行者 ： The dark side of Forcing

連絡先 ： http://forcing.nagoya

発行日 ： 2015 **年** 8 **月** 14 **日**


p.b.