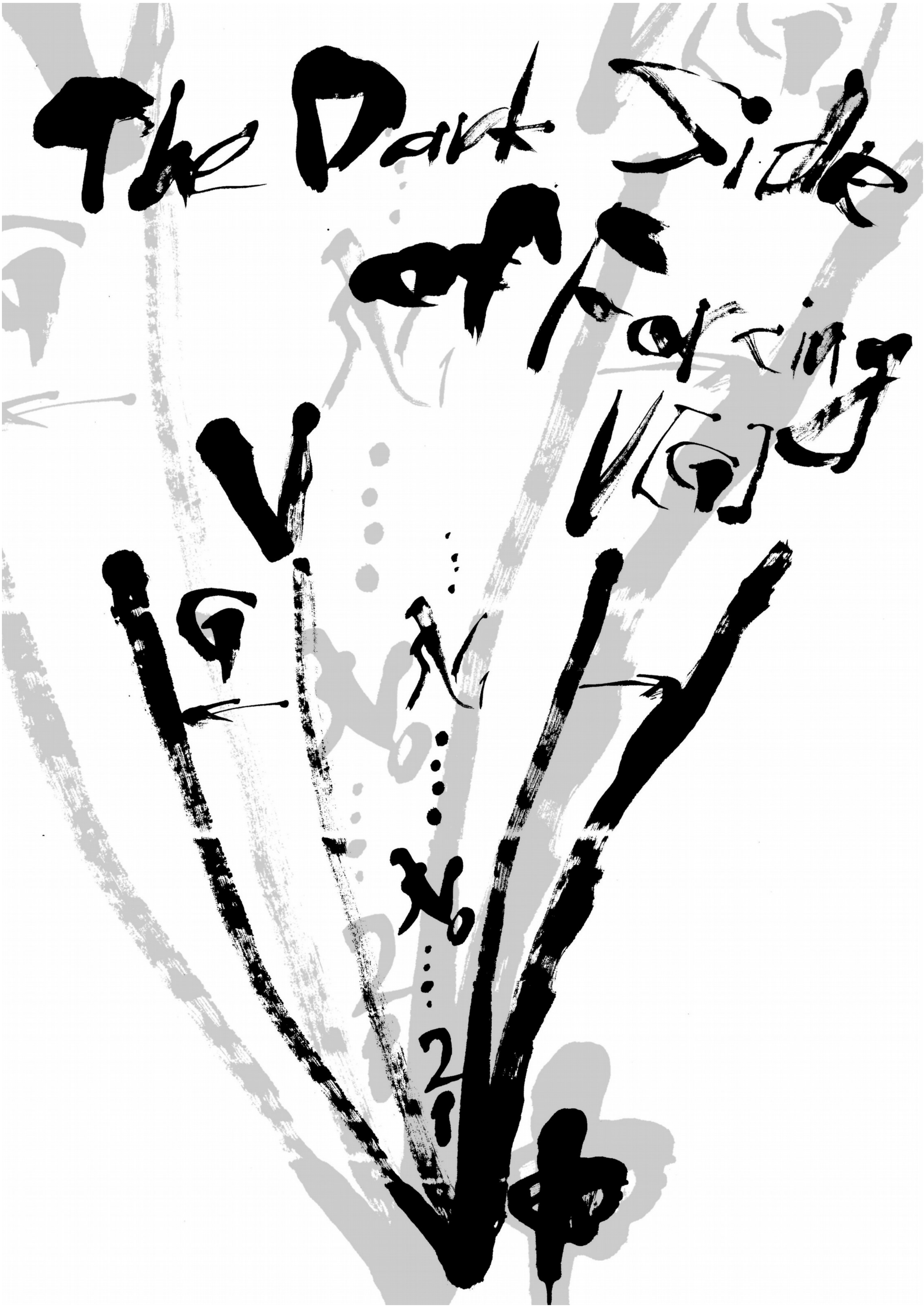

The Dark Side of Forcing
V[G]
V
G
21

(preface)

なまえ

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

test

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、三つ目はゲンツェン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）。

この原稿は、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。また、一方の考え方では定式化できないが、他方の考え方では定式化可能な論理もある。この二つのパラダイムを比較することを通じて、ゲンツェンの洞察を具体化してみる

[*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。

ことがこの原稿の目標である。

この原稿は二種類の読者を念頭に置いている。まず、大学で数理論理学の基礎的な授業は受け、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、この原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、この原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。

定式化が異なる論理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。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　最初は列から——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。つまり、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。

ヒルベルト式の特徴は、公理が複雑化しやすいこと、仮定の discharge ができないことなど様々に存在するが、「列」という証明の形から直に起因する特徴に絞って考えるのであれば、やはりなんといっても証明の構造の単純性が挙げられる。以下で紹介するツリー型の証明が二次元的な構造を持つのに対して、ヒルベルト式の証明は一次元的な構造しか持っていない。

この単純性のおかげで、ヒルベルト式の体系では、**メタ数学的な**定義や証明がラクで、わかりやすいものになりやすい。ツリー型の証明を数学的に厳密に定義しようとすると、ツリーを定義し、ツリーに対するラベルを定義し…とやや面倒な定義を踏まなくてはならないが、ヒルベルト式であれば、単純に式を並べたものとして定義できる。このおかげで、証明も楽になる。ヒルベルト式の**中での**証明は、ツリー型の場合よりもたいてい大変なのだが、ヒルベルト式に**ついての**証明は、ツリー型の場合よりも簡単であることが多い。

さらに、これに対応する形で、コード化がラク、という利点もある。コード化とは一般的に、証明図を別の数学的対象（典型的には自然数）によって代表させ、証明図についての議論を別の数学的対象についての議論として行う証明論における技法であるが、ツリー型の証明よりも列の形をした証明のほうがコード化はラクでわかりやすい。

1.4　ツリー型の登場——自然演繹とシークエント計算

フレーゲが提示し、ヒルベルトが自らの証明論の基礎としたのが「列」パラダイムに基づくヒルベルト式の定式化であったが、その後ゲンツェンは、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。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。自然演繹はヒルベルト式に比べると推論規則が多く、先述したように、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形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・シークエントを単位とする公理系である。シークエントは、例えば $A, B, C \vdash A \wedge B, D$ 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 かつ 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。$\wedge$ の規則だけ述べておこう。

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

この規則を見ればわかると思うが、シークエントにおける証明も枝分かれを含むツリーの構造を持つ。

ゲンツェンは、従来のヒルベルト式とは異なる新たな論理の定式化として自然演繹とシークエント計算を発見した。もちろん、単に新たな定式化を発見するだけでは意味が無い。従来のヒルベルト式にはない特徴が自然演繹やシークエント計算になければならない。

このような特徴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、この対称性の研究は、現在も証明論研究の最大のトピックである。

ただし、ルールの間の対称性は、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)。「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。

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。一つは、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が、図形的に明快に表示されることができる。

二つ目は、一つ目に関連する論点ではあるが、式が推論において何回使われたかということが明確化することである。ヒルベルト式の体系では、証明において一度現れた命題は、その証明において何度も何度も規則を適用することができる。これに対してツリー型の体系では、推論規則は直前の命題にしか適応できないから、同じ命題を何度も使いたいときは、そのたびに何度もその命題を導出し、証明に登場させる必要がある。これは証明が複雑化するという点では欠点のように見えるが、むしろ、同じ命題が証明の中で何回使われるのかという、証明のなかに内在している構造を明示化するという意味で、プラスと捉えることもできる。

1.5　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。列パラダイムにおいては、証明の構造が単純化することで、メタ数学やコード化が楽になる。一方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、そして、同じ命題が何度使われたのかといったことが、図形的に明快に表示されることができる。

このように見ると、証明論者が証明や定義を行う労力（そして、読者が証明や定義を理解する労力）さえ厭わなければ、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式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 (calulus 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[*2]。シークエント計算には、論理規則以外に、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。

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

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。

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

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、

*2 以下の議論は [2] を元にしている。

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。

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

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[*3]。

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 $\vee, \wedge$ 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[*4]には例えば次のようなスイッチ則が登場する。

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

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「$((R \wedge T) \vee T)$」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基本的に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)。

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

「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。そのため、ヒルベルト式と同様、証明の構造は単純である。

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。具体的には、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。そのため、どの式がどこでどのように使われたのは明らかである。また、同じ式を二度使うなら、二度証明に登場させる

[*3] 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。

[*4] 古典論理の構造計算の完全な定義は [2] を参照。

必要がある。

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。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は同様の特徴はない。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と同時に、構造計算によって初めて明示化されたものである。

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、特に、「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」という一つ目の特徴は、あくまで部分的なものにとどまっている。さらに、構造計算では、ツリーパラダイムやヒルベルト式では扱える推論規則が扱えない。

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。

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。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。

1.6　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、列パラダイムにおいては、証明の構造が単純になること、上下に対称性が存在することなどの利点があった。対して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、何回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。構造計算はこの四つの利点を全て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使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) [3] 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、この原稿で紹介した定式化にはない特徴を備えている。その意味で、ゲンツェンの洞察は、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、論理の様々な形式化は、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、いくつかの顕著な特徴に注目し、余計な特徴は捨象し、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。同じ命題が推論において何度も使われているということに注目し、それを明示化したいと望むなら、ツリー型の体系がモデルとして相応しい。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、この原稿で述べたような、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

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 Brünnler, K. 2006, ”Deep Inference and Symmetry in Classical Proofs”, PhD thesis, available on http://cs.bath.ac.uk/ag/kai/phd.pdf Girard, J. 1989, Proofs and Types, Cambridge University Press.

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] Girard, J. 1989, Proofs and Types, Cambridge University Press.

第 2 章

(chapter の例)

なまえ

なんとかかんとか

参考文献

[1] キューネン, ケネス./藤田博司 訳. 集合論—独立性証明への案内. 日本評論社. 2008.

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 Classiferies 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．部分対象分類子の存在の応用として，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と，層の間の自然変換がエピ射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：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．

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 3.1]), i.e.,

$$\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \underset{\mathbf{a}}{\overset{i}{\underset{\longrightarrow}{\overset{\longleftarrow}{\perp}}}} \mathrm{Sh}(\mathbf{C}, J). \tag{3.1.1}$$

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

Similarly, let $\{F_i\}_{i\in I}$ be a diagram in $\mathrm{Sh}(\mathbf{C}, J)$. Then $\{i(F_i)\}_{i\in I}$ is a diagram in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Since $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is cocomplete, there exists the colimit $\varinjlim_{i\in I} i(F_i) \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. 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

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

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

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

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

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

Note that monicity is described by pullbacks, in particular, limits. Since the inclusion functor i has a left adjoint, pullbacks are preserved by i. Hence, ϕ is a monomorphism in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$.

($\Leftarrow$) 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 monomophism 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 of 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:

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

by $\mathbf{a} \dashv i$, 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 $\tau : \mathbf{y}(C) \times P \to F$. By the naturality of τ, for any $h : E \to D$,

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

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

$$(Fh)(\tau_D(g, x)) = \tau_E(gh, (Ph)(x)) \quad ((g, x) \in \mathbf{y}(C)(D) \times PD). \tag{3.1.2}$$

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 $x \in PD$,

$$(F^P(f)(\tau))_D(g', x) = \tau_D(fg', x). \tag{3.1.3}$$

First, we claim that if F is separated, then F^P is also separated. To show this, let $\tau, \sigma \in F^P(C)$ 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.,

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

in particular, for $g' = \mathrm{id}_{C'}$

$$\tau_{C'}(f, x) = \sigma_{C'}(f, x) \quad (f \in S,\ x \in PC'). \tag{3.1.4}$$

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

$$\begin{aligned}(Fg')(\tau_{C'}(k, x)) &= \tau_D(kg', (Pg')(x)) \quad (\text{by } (3.1.2)) \\ &= \sigma_D(kg', (Pg')(x)) \quad (\text{by } (3.1.4)) \\ &= (Fg')(\sigma_{C'}(k, x)) \quad (\text{by } (3.1.2)).\end{aligned} \tag{3.1.5}$$

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.

Next, we shall show that all matching families have an amalgamation. Let $S \in J(C)$ and $\{\tau_f\}_{f \in S}$ 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

$$(\tau_{fg})_{E'}(h, x) = (\tau_f)_{E'}(gh, x). \tag{3.1.6}$$

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

$$\begin{tikzcd} \mathbf{y}(D) \times P \arrow[r, "\tau_f"] \arrow[d, "\mathbf{y}(f) \times \mathrm{id}_P"'] \arrow[dr, phantom, "\circlearrowleft"] & F \arrow[d, "\eta_F"] \\ \mathbf{y}(C) \times P \arrow[r, "\tau'"'] & F^+. \end{tikzcd} \tag{3.1.7}$$

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 $\tau := (\eta_F)^{-1}\tau' : \mathbf{y}(C) \times P \to F$. 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

$$\tau'_B(k, x) := [\{(\tau_{kh})_{\mathrm{dom}(h)}(\mathrm{id}_{\mathrm{dom}(h)}, (Ph)(x))\}_{h\in k^*(S)}]. \tag{3.1.8}$$

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 $m : B'' \to B'$,

$$\begin{aligned}
&(Fm)((\tau_{kh})_{B'}(\mathrm{id}_{B'}, (Ph)(x)))\\
&= (\tau_{kh})_{B''}(m, (Pm)((Ph)(x))) \quad \text{(by (3.1.2))}\\
&= (\tau_{kh})_{B''}(m, (P(hm))(x))\\
&= (\tau_{khm})_{B''}(\mathrm{id}_{B''}, (P(hm))(x)) \quad \text{(by (3.1.6))}.
\end{aligned}$$

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 all $l : D \to B$,

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

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 requiring commutativity (3.1.7). To this end, let $B \in \mathbf{C}$, $m : B \to D$ and $x \in PB$. Then

$$\begin{aligned}
((\eta_F) \circ (\tau_f))_B(m, x)) &= (\eta_F)_B((\tau_f)_B(m, x))\\
&= [\{(Fl)(\tau_f)_B(m, x)\}_{l\in t_B}] \quad \text{(by the definition of } \eta_F)\\
&= [\{(\tau_f)_{\mathrm{dom}(l)}(ml, (Pl)(x))\}_{l\in t_B}] \quad \text{(by (3.1.2))}
\end{aligned}$$

On the other hand,

$$\begin{aligned}&\tau'_B(\mathbf{y}(f)_B \times \mathrm{id}_{PB})(m,x)\\ &= \tau'_B(fm,x)\\ &= [\{(\tau_{fmh})_{\mathrm{dom}(h)}(\mathrm{id}_{\mathrm{dom}(h)},(Ph)(x))\}_{h\in(fm)^*(S)}] \quad \text{(by the definition of } \tau'\text{)}\\ &= [\{(\tau_f)_{\mathrm{dom}(h)}(mh,(Ph)(x))\}_{h\in(fm)^*(S)}] \quad \text{(by (3.1.6)).}\end{aligned}$$

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 requiring 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 sieve). 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

$$\overline{S} := \{h \mid \mathrm{cod}(h) = C \text{ and } S \text{ covers } h\} = \{h \mid \mathrm{cod}(h) = C \text{ and } h^*(S) \in J(\mathrm{dom}(h))\}. \tag{3.2.1}$$

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 arrom 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

$$\Omega : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets} \tag{3.2.2}$$

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

$$\forall f \in S, \forall g : E \to D, \quad (\Omega g)(M_f) = g^*(M_f) = M_{fg}. \tag{3.2.3}$$

Let $M := \{fg \mid g \in M_f \text{ and } f \in S\}$. 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 (3.2.3), $u^*(M_f) = (\Omega g)(M_{f'})$, i.e, $u^*(M_f) = g^*(M_{f'})$. Since $g \in M_{f'}$, $g^*(M_f)$ is the maximal sieve, thus 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 a *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 $S \in J(C)$,*

$$\forall f : D \to C \in S, \quad (Ff)(x) \in AD \Rightarrow x \in AC. \tag{3.2.4}$$

□

Proof. Supposet that A is a sheaf on $(\mathbf{C}, J)$. Let $C \in \mathbf{C}$, $x \in FC$ and $S \in J(C)$. Supposet that for all $f : D \to C \in S$, $(Ff)(x) \in AD$ implies that $x \in AC$. Then $\{(Ff)(x)\}_{f\in S}$ is a matchng 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

$$\forall f : D \to C \in S, \quad (Ff)(y) = (Ff)(x). \tag{3.2.5}$$

On the other hand, since F is also a sheaf on $(\mathbf{C}, J)$, $x \in FC$ is the unique amalgamation such that (3.2.5) holds. Hence, $y = x$, since $y \in AC \subseteq FC$.

Conversely, 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.,

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

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 true : $1 \rightarrowtail \Omega$ as follows:

$$\mathrm{true}_C : 1C = \{*\} \ni * \mapsto t_C \in \Omega C. \tag{3.2.6}$$

$\Diamond$

Note that 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. true : $1 \rightarrowtail \Omega$ *is a subobject classifier for* $\mathrm{Sh}(\mathbf{C}, J)$. $\square$

Proof. Let $F \in \mathrm{Sh}(\mathbf{C}, J)$ and A a subsheaf of F. We define a mapping $\chi_A : F \to \Omega$ for each $C \in \mathbf{C}$ by

$$(\chi_A)_C : FC \ni x \mapsto \{f : D \to C \mid (Ff)(x) \in AD\}. \tag{3.2.7}$$

First, we shall 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 $(\chi_A)_C(x)$ covers $g : E \to C$, 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 $(\chi_A)_B((Fg)(x)) = \{f : D \to B \mid (Ff)((Fg)(x))\} \in AD$. Thus,

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

This implies the following commutativity:

$$g^*((\chi_A)_C(x)) = (\chi_A)_B((Fg)(x)),$$

i.e.,

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

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,

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

in $\mathrm{Sh}(\mathbf{C}, J)$ iff for all $C \in \mathbf{C}$

$$\begin{tikzcd} AC \arrow[r, "!^{AC}"] \arrow[d, tail] \arrow[dr, phantom, "\text{p.b.}"] & \{*\} \arrow[d, tail, "\mathrm{true}_C"] \\ FC \arrow[r, "(\chi_A)_C"'] & \Omega C, \end{tikzcd} \tag{3.2.8}$$

where $!^A$ is a unique morphism from A to the terminal object. 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 (3.2.8) is a pullback diagram.

Finally, we shall show that χ_A is a unique natural transformation such that the above diagram (3.2.8) is a pullback diagram. Let $\psi_A : F \to \Omega$ be a natural transformation such that the following diagram is a pullback square:

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

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

$$\begin{aligned} (Ff)(x) \in AD &\Leftrightarrow \mathrm{id}_D \in (\psi_A)_D((Ff)(x)) \\ &\Leftrightarrow \mathrm{id}_D \in f^*((\psi_A)_C(x)) \quad (\because \psi_A : F \to \Omega \text{ is natural}) \\ &\Leftrightarrow f \in (\psi_A)_C(x). \end{aligned}$$

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

Consequently, true : $1 \to \Omega$ 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 $f : D \to C \in S$, $(Qf)(y) \in (\phi_D)[PD]$. ◊

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

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

By 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.

Conversely, suppose that $\phi : F \to G$ is an epimorphism. We define a subfunctor A of G by

$$AC := \{y \in GC \mid \exists S \in J(C),\ \forall f : B \to C \in S,\ (Gf)(y) \in \phi_B[FB]\}. \tag{3.2.9}$$

First, we shall prove that A is indeed a subfunctor of G. By definitin, $AC \subseteq GC$. 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 $g : B \to D \in T_f$, $(Gg)((Gf)(x)) \in \phi_B[FB]$ and fix 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 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 $f : B \to C \in t_C$,

$$\begin{aligned}(Gf)(y) &= (Gf)(\phi_C(x)) \\ &= \phi_B((Ff)(x)) \in \phi_B[FB]. \quad (\because \phi \text{ is natural})\end{aligned}$$

Hence, we have the following pullback square:

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

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, $A = G$. This implies that $\phi : F \to G$ is locally surjective for J. 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:

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

Hence, we have

$$\alpha \circ \tilde{\eta}_Q \circ \phi = \alpha \circ \mathbf{a}(\phi) \circ \tilde{\eta}_P = \beta \circ \mathbf{a}(\phi) \circ \tilde{\eta}_P = \beta \circ \tilde{\eta}_Q \circ \phi. \tag{3.2.10}$$

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

$$\begin{aligned} &(\alpha\tilde{\eta}_Q)_D((Qf)(y)) = (\beta\tilde{\eta}_Q)_D((Qf)(y)) \\ \Leftrightarrow\ &(Ff)((\alpha\tilde{\eta}_Q)_C(y)) = (Ff)((\beta\tilde{\eta}_Q)_C(y)) \quad (\because \alpha \text{ and } \beta \text{ are natural}). \end{aligned}$$

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

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

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 (3.2.9):

$$AC := \{y \in QC \mid \exists S \in J(C),\ \forall f : B \to C \in S,\ (Qf)(y) \in \phi_B[FB]\}. \tag{3.2.11}$$

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 $i : \Omega \hookrightarrow \Omega^{(p)}$ 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 $i : \Omega \hookrightarrow \Omega^{(p)}$, i.e., there exists a mapping $\chi_A : Q \to \Omega$ such that $\chi_A^{(p)} = i \circ \chi_A$. Then as is the case for the proof of Corollary 3.2.2, we have the following commutative square:

$$\begin{tikzcd} P \arrow[r, "!^P"] \arrow[d, "\phi"'] \arrow[dr, phantom, "\circlearrowright"] & 1 \arrow[d, tail, "\mathrm{true}"] \\ Q \arrow[r, "\chi_A"'] & \Omega. \end{tikzcd} \tag{3.2.12}$$

Hence, we have

$$\chi_A \circ \phi = \mathrm{true} \circ !^P = \mathrm{true} \circ !^Q \circ \phi. \tag{3.2.13}$$

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 (3.2.13), we have

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

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

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

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

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. *$(\{f_i : C_i \to C\}_{i \in I}) = \{f_i g \mid i \in I,\ g \in \mathbf{C}\} \in J(C)$ iff*

$$\coprod_{i \in I} \mathbf{ay}(C_i) \to \mathbf{ay}(C) \tag{3.2.14}$$

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.

Supposet 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 transitivity axiom, $f^*((\{f_i\}_{i \in I})) \in J(D)$. 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 monomorphims 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 $(\mathbf{C}, J)$, i.e., a subsheaf A of E (cf. Lemma 3.2.2):

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

(ii) for all $f : D \to C$,

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

(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.

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

$\Diamond$

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

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

(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 by

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

(ii) $\big(\bigwedge_{i\in I} A_i\big)(f) := Ef : \bigcap_{i\in I} A_iC \to \bigcap_{i\in I} A_iD$ 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 $e \in EC$,*

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

□

Proof. Let $S := \{f : D \to C \mid \exists i \in I,\ (Ef)(e) \in A_iD\}$. 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 $(Ef)(x) \in A_iD$. Since A_i is a subfunctor of E, for all $g : E \to D$, $(E(fg))(e) \in A_iD$. 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 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, $A_i \le \bigvee_{i\in I} A_i$. Suppose that there exists a subsheaf U of E such that $A_i \le U$ 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 $A_i \le U$ 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. ■

Lemma 3.3.1. *Let E be a sheaf on a site $(\mathbf{C}, J)$. Then $(\mathrm{Sub}(E), \le)$ is a complete Heyting algebra.* □

Proof. Since $(\mathrm{Sub}(E), \le)$ 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 $B \wedge A_i \le B, A_i$ for all $i \in I$, we have

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

Hence, by the definition of 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

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

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

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

Conversely, let $e \in EC$ and $f : D \to C$. Suppose that $(Ef)(e) \in (B \wedge A_i)(D)$ for some $i \in I$. Then, in particular, $(Ef)(e) \in A_iD(i \in I)$. Hence, we obtain

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

that is, $e \in \big(\bigvee_{i\in I}(B \wedge A_i)\big)(C)$, by (3.3.2). The proof is complete. ■

Fact 3.3.3. *The implication operator $\to$ in $(Sub(E), \le)$ can be explicitly described 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 $(\mathrm{Sub}(E), \leq)$. 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 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.,

$$\forall A,\ \forall B,\ \forall U \in \mathrm{Sub}(E), \quad U \leq (A \to B) \Leftrightarrow U \wedge A \leq B. \tag{3.3.5}$$

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

$$\forall C \in \mathbf{C},\ \forall u \in UC,\ \forall f : D \to C, \quad (Ef)(u) \in AD \Rightarrow (Ef)(u) \in BD. \tag{3.3.6}$$

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 (3.3.6). 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, $U \wedge A \leq B$.

($\Leftarrow$) 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:

$$e \in \phi^{-1}(B)C \Leftrightarrow \phi_C(e) \in BC. \tag{3.3.7}$$

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

Fact 3.3.4. *The pullback functor ϕ^{-1} of $\phi : E \to F$ is order-preserving, i.e.,*

$$\forall A,\, \forall B \in \mathrm{Sub}(F), \quad A \le B \Rightarrow \phi^{-1}(A) \le \phi^{-1}(B). \tag{3.3.8}$$

$\square$

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

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

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.

Finally, we shall prove that ϕ^{-1} is order-preserving. To this end, let $A, B \in \mathrm{Sub}(F)$ such that $A \le B$. Suppose that $e \in \phi^{-1}(A)C$ ($C \in \mathbf{C}$). Then $\phi_C(e) \in AC \subseteq BC$, since $A \le B$. Hence, $e \in \phi^{-1}(B)C$. Therefore, $\phi^{-1}(A) \le \phi^{-1}(B)$. The proof is complete. $\blacksquare$

Fact 3.3.5. *Let E and F be two sheaves on $(\mathbf{C}, J)$. For any natural transformation $\phi : F \to G$, the pullback functor $\phi^{-1} : \mathrm{Sub}(F) \to \mathrm{Sub}(E)$ has both a left adjoint $\exists_\phi$ and a right adjoint $\forall_\phi$:*

$$\exists_\phi \dashv \phi^{-1} \dashv \forall_\phi. \tag{3.3.9}$$

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

$$y \in \exists_\phi(A)C \Leftrightarrow \{f : D \to C \mid \exists a \in AD,\, \phi_D(a) = (Ff)(y)\} \in J(C). \tag{3.3.10}$$

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

$$\begin{aligned} y \in \forall_\phi(A)C &\Leftrightarrow \forall f : D \to C, \quad \phi_D^{-1}(\{(Ff)(y)\}) \subseteq AD; && (3.3.11)\\ &\Leftrightarrow \forall f : D \to C, \forall x \in EC, \quad \phi_D(x) = (Ff)(y) \Rightarrow x \in AD && (3.3.12)\end{aligned}$$

$\square$

Proof. We shall prove that $\exists_\phi$ and $\forall_\phi$ described as (3.3.10) and (3.3.12) are indeed a left and a right adjoint of the pullback functor ϕ^{-1} of *phi*.

($\exists_\phi$) 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 $f^*(R) = \{g : D' \to C \mid gh \in R\}$. We claim that

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

Let $g : D' \to D \in f^*(R)$, i.e., $fg \in R$. Then

$$\exists a \in AD', \quad \phi_{D'}(a) = (F(fg))(y) = (Fg)((Ff)(y)).$$

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

$$\exists a \in AD',\ \phi_{D'}(a) = (Fg)((Ff)(y)) = (F(fg))(y).$$

Then, by the definition of R, $fg \in R$, i.e., $g \in f^*(R)$. 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:

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

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

($\Rightarrow$) Suppose that $\exists_\phi(A) \le B$. 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 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

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

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 (3.3.13) 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

$$\phi_{C'}(x) = (Fg)(y). \tag{3.3.14}$$

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 (3.3.14) and 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:

$$\forall A \in \mathrm{Sub}(E),\ \forall B \in \mathrm{Sub}(F), \quad \phi^{-1}(B) \leq A \Leftrightarrow B \leq \forall_\phi(A). \tag{3.3.15}$$

($\Rightarrow$) 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 (3.3.15) 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 3.3.6. *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*

$$\varphi(S) := \bigvee\{c \mid 0 \in S(c)\} \tag{3.3.16}$$

is an order isomorphism, i.e., 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 $a \leq \varphi(S)$. 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 $a \leq \varphi(S)$, this implies that $0 \in S(a)$.

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

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 $a \leq \varphi(S) = \varphi(T)$, i.e., $0 \in T(a)$. By symmetry, $0 \in T(a)$ implies that $0 \in T(a)$. 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

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

We must verify that S is a subsheaf of 1. By definition, $S(a) \subseteq \{0\}$ for all $a \in \mathbf{H}$. Let $b \leq a$ $(a, b \in \mathbf{H})$. If $0 \in S(b)$, then $a \leq b \leq s$. 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., $a_i \leq s$. Then $a = \bigvee_{i \in I} a_i \leq s$, 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.,

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

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

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

$$\varphi(S) = \bigvee\{a \mid 0 \in S(a)\} \leq \bigvee\{a \mid 0 \in T(a)\} = \varphi(T).$$

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

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 diagram is an equalizer diagram for some two morphisms a and p (see [3, Remark 3.2.1] for detail):

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

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

Fact 3.3.7. *A mapping* $0 : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets}$ *defined for* $C \in \mathbf{C}$ *by*

$$0C := \begin{cases} \{x_C\} & (\emptyset \in J(C)), \\ \emptyset & (\emptyset \notin J(C)) \end{cases} \tag{3.3.17}$$

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-complement). The *pseudo-complement* $\neg B$ of B is defined by

$$\neg B := B \to 0 = \bigvee\{U \in \mathrm{Sub}(E) \mid U \wedge B = 0\}. \tag{3.3.18}$$

◊

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

$$x \in (\neg B)C \Leftrightarrow \forall f : D \to C, \quad (Ef)(x) \in BD \Rightarrow \emptyset \in J(D). \tag{3.3.19}$$

□

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

$$\forall f : D \to C, \exists g : D' \to D, \quad fg \in S. \tag{3.3.20}$$

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

$$J(C) := \{S \mid S \text{ is a sive on } C \text{ and dense below } C\} \tag{3.3.21}$$

is called a *dense topology.* ◊

Fact 3.3.9. *A dense topology J is a Grothendieck topology.* □

Proof. (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 a dense topology J, $\emptyset \notin J(C)$ for all $C \in \mathbf{C}$.

Fact 3.3.10. *Let J be a dense topology. Then for all $C \in \mathbf{C}$,*

$$(\neg B)C = \{x \in EC \mid \forall f : D \to C, \quad (Ef)(x) \notin BD\}. \tag{3.3.22}$$

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

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

The proof is complte. ■

Fact 3.3.11. *Let J be an atomic topology. Then $E \in \mathrm{Sh}(\mathbf{C}, J)$, $(\mathrm{Sub}(E), \leq)$ is a complete atomic Boolean algebra.* □

Proof. Recall that an 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 $fh = gk$:

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

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

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

We claim that an atomic topology J is 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 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 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 $A(\neq 0) \in \mathrm{Sub}(E)$ 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

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

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

$$(El)((Eh)(y)) = (E(hl))(y) = (E(gk))(y) = (Ek)((Eg)(y)) = (Ek)(Ef)(x) = (E(fk)(x)).$$

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 $x = (E\mathrm{id}_C)(x)$, $x \in A_x C \neq \emptyset$, $A_x \neq 0$.

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 an 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*, 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

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がこうとしながら, 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も同一視するユダヤ・キリスト教も, 「青銅の蛇」など復活の象徴としての蛇も持ち合わせている. 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す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

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.

$$
\begin{tikzcd}
 & \ker a \arrow[r] \arrow[d] & \ker b \arrow[r] \arrow[d] & \ker c \arrow[d] \arrow[dddll, "d"] & \\
 & A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] \arrow[d] & B' \arrow[r, "g'"] \arrow[d] & C' \arrow[d] & \\
 & \operatorname{coker} a \arrow[r] & \operatorname{coker} b \arrow[r] & \operatorname{coker} c &
\end{tikzcd}
$$

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,

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

に適用すると, コホモロジーの長完全系列

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

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

(appendix)

なまえ

王様の大好物は卵焼き。朝も、昼も、夜も卵焼きを食べています。そんな王様に、世継ぎの王子様が生まれました。王様は大喜びです。早速、国中の人間をお城に集めて、ご馳走を振舞うことにしました。ご馳走は、やっぱり卵焼きに決まっています。

でも、国には国中の皆が食べられるような、沢山の卵はありません。ニワトリも一度にそんなに沢山の卵を産めないので、他のご馳走にしようと大臣たちは言います。でも、王様は『絶対に卵焼きでなければならない！』と言うのです。とうとう『ぞうの卵なら、一度に沢山の卵焼きができるじゃないか』と言い出したので、さあ大変！

ワン大臣は、ぞうの卵を見つけてくることになりました。ツウ大臣は、ぞうの卵焼きを作る大きなフライパンを作ることになりました。ホウ大臣は、大きなフライパンを載せて焼くかまどを作ることになりました。

巨大なフライパンと、小山のようなかまどは作ることが出来ました。でも、ぞうの卵を探しに出掛けたワン大臣、中々卵が見つかりません・・・。

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シルバー・”今期はクロスアンジュ推し”・ポーク（@silver_pork,@otb_btb）です．今回も前回同様マニアックな内容になりましたが、マニアックなだけならまだしも、数学的実質に乏しくなってしまい反省してます。次はもっと読んだ人を幸せにできる原稿を書きます。アンジュ様格好いいです。

才川 隆文 Redmine ちゃんの slave bot であり号令係でした。commit log が飛び交いチケットが増減するダイナミズムに身を任せるのは快感です。

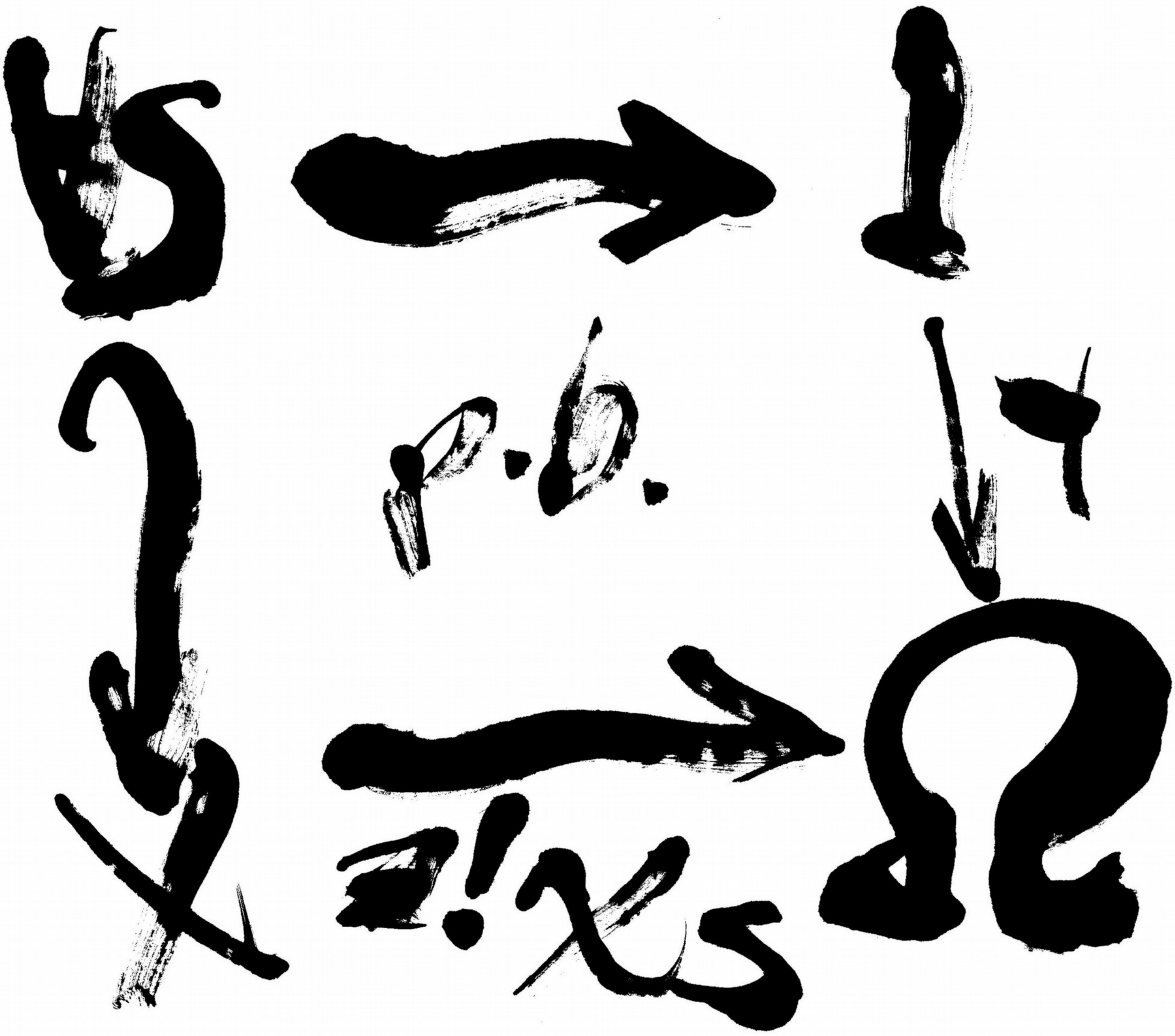
古賀 実 今回初めて表紙絵を担当しました．構図の元ネタは STAR WARS episode VII のキービジュアルです．同人誌作成で使用し始めた git が便利で今では常用してます.

平野 智博

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.