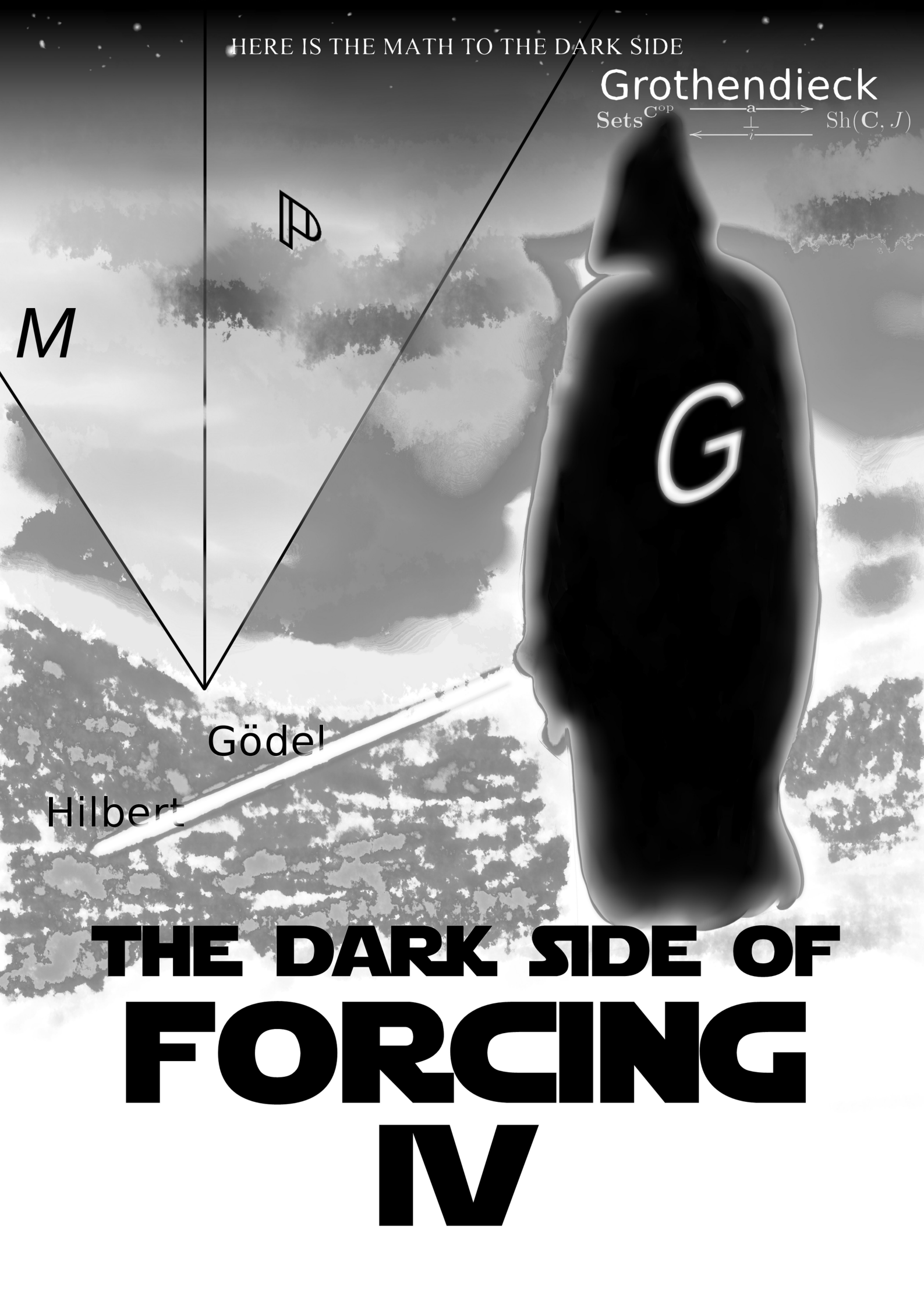

HERE IS THE MATH TO THE DARK SIDE
Grothendieck
$\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ $\underset{i}{\overset{a}{\rightleftarrows}}$ $\mathrm{Sh}(\mathbf{C}, J)$
$\mathbb{P}$
M
G
Gödel
Hilbert
THE DARK SIDE OF
FORCING
IV

There is a small cat from Topoi,

And her name is Joy.

She looks for the path

to the darkside of math.

It's going to be her favorite toy.

目次

第 1 章

掛け算の順序について　初等算数教育における「意味」の意味

淡中　圏

掛け算の順序を間違えた生徒を正解にするかどうかという、不毛な議論が終わらないのは、数学の哲学的理解の不足による。大雑把にだが、議論に何が足りないかを述べる。

1.1　introduction

たしか去年の冬コミ (C85) に出した The Darkside of Forcing で那須さんが、

「田中さん (私の本名) が需要のないことを書いてよ、って言ったから云々」

というようなことを書いていた。実際、私も今まで何の需要も見込めなさそうな代物を書くことに邁進していたわけだが、今年の夏コミ (C86) で手八丁口八丁であっという間に 50 冊売りきってしまったときに、明らかにこの本を買っても仕方なさそうな人々にまで売りつけてしまったことに、石木ならぬ身としては、さすがに罪悪感を感じてしまった。

そこで多少は需要があるかもやしれないことを書いてみようと思う。

と言うわけで、今回は掛け算の順序についてだ。

恐ろしい話だが、小学校の算数で積の立式において、順序を指導要領通りに書かない場合に、正解にすべきか否か、という問題が何年も続いている。

あまりに何年も続いているせいで、知り合い (というかこの同人誌の執筆陣の一人) は、

「もしかして、これで食っていけるのでは？」

などと言い始める始末。

学問の大事な役割は、その学問の最初の問題設定が間違っていたがゆえに発生した擬似問題によって、才能のない学者の食い扶持を稼ぐことである。言語設計の不備によって、メンテナンス要員の雇用を発生させるプログラミング言語も同様であるし、官僚制度の中にも似た機構がある。

そういう意味では、これは正しい学問の姿と言って言えないことはないが、言いたくない。絶対に言いたくない。才能のある人間にこんな糞下らないことに係わせるのは、罪悪

以外の何物でもない。

これに関しては何人もの頭の良い人々がいろいろと書いていて、概ね戦いの趨勢は決まっているように見えるが、それでも足りていない議論があるように思えるので、ここに雑文を加えることをお許し願いたい。

なお、参考文献を本気で漁ったことはないので、ここでの議論がすでにどこかで出ていることは十分にあり得る。またここでの議論の参考文献を挙げることもしない。

そんなことしたくないくらい、これは下らない問題だと考えているが故である。

暇な人がいたらやってくださいな。

1.2　問題設定

次のような問題があったとする。

問題　りんご 2 個が乗った皿が 3 枚ある。りんごは全部で何個あるか？

この問題に対して、式を書く場所と答えを書く場所がある。

答えは「6 個」に決まっている。そこにこの問題の問題はない。

この問題の問題は、式だ。現在の指導要領においては、次が正しい式である。

$$2 \times 3 = 6$$

これがもし次の式だと、不正解とされてしまう。

$$3 \times 2 = 6$$

不正解の理由は、2×3 とはそもそも $2 + 2 + 2$ の略であり、3×2 は $3 + 3$ の略なので、前者でなければ題意に適合しない、というものだ。

果たしてこれは正しい処置なのだろうか？

まずは賛成派の言い分、続いて反対派の言い分を大雑把に紹介し、最後にその二つを止揚した私の言い分を紹介するという弁証法的な筋立てで話を進めようと思う。

1.3　賛成派の意見

まず第一に、この計算を逆にするということは、ちゃんと掛け算が同じ数を足しつづけることの省略であることを理解していないから駄目だ、という意見がある。これは指導要綱にある内容を消化していない、ということなので、正解にするわけにはいかない、というわけだ。

たださすがに指導要綱に従っていないから不正解ではあまりに官僚的と考えたのか、これに幾つかの教育方法論的な話がつく、

例えば、

「掛け算の可換性を最初から認めてしまうと、割り算でつまずく」

などの意見があるらしい。伝え聞きなので私にも確たることは分からないのだが、おそらく掛け算に可換性を最初から認めると、割り算も可換だと児童が勘違いする、ということを意味していると思われる。

また単位の重要性を挙げるものも多い。先ほどの例で、りんご 2 個の皿が三個で何個かという問題なら、掛け算の一つ目の数の単位と、答えの単位が同じでなければいけない、

と考えているようだ。これを「単位の同じ数でサンドイッチする」と教えている人もいるらしい。このように教えることによって、子どもの単位に対する理解を深められる、ということを考えているのだろう。

単位に関する理解を深める、ということはつまり、計算の「意味」に関する理解を深める、ということだ。結局教師たちの言い分を短くまとめると、「掛け算の順序を間違える、ということは、掛け算の意味を理解していないことを意味する。意味を理解していなければ、算数ができているとは言えない」となるのではなかろうか。

1.4　反対派の意見と寸評

まずよくある反対理由として、欧米圏における掛け算の順番は逆であることを挙げるものがあるだろう。英語で、2×3 は「2 times 3」と読む。つまり、3 の 2 倍であり、これは 3 が 2 個あるわけだから、日本の掛け算とは順序が逆である。

ここから、掛け算の順序を重要視することの馬鹿らしさを示していこうという戦略である[*1]。

---

*1

これに対する再反論として、日本式の右作用（つまり、2×3 なら 3 が作用する数で、すなわち 2 の 3 倍）の方が、西洋式の左作用（つまり、2×3 なら 2 が作用する数で、すなわち 3 の 2 倍）なら、日本式のほうが合理的だという反論がある。事実問題としては私もこのことに賛成である。西洋式だと、足し算と掛け算で作用の方向が違う ($2 + 3$ はやはり、2 に 3 を足していると考えている）し、電卓などで計算していると、作用させるものを予め計算しておいて、先に入力する、というのはやはり変だ。

しかし、だからといってことは簡単にはいかない。

中学以降の数学の文字式では、$\times$ を省略して、x が 2 個あることを $2x$ と書くが、これは明らかに左作用である。

もし、小学校教師が、意味と形式の一致を高らかに謳い続けたいなら、中学以降の教育にも圧力を掛けて、$x2$ と書かせるべきなのではなかろうか。

もし、何かの間違いでそんなことになったら、ぜひとも関数の作用の向きも右にしてもらいたい。つまり、$f(x)$ と書くのではなく、xf と書くことにしよう。

従来のやり方は、矢印 $\xrightarrow{f}$ の合成と関数の合成が逆向きになって気持ち悪かったのだ。

$$f : X \xrightarrow{f} Y, g : Y \xrightarrow{g} Z \Rightarrow g \circ f : X \xrightarrow{f} Y \xrightarrow{g} Z$$

逆に書けば、$(xf)g = x(f \circ g)$ となって矢印の合成と平仄が合う。

こちらのほうがずっと合理的だ。実際にすでにこう書いている進歩的な人も結構いる。

もちろん、絶対にそうはならない。

我々の慣習とは、様々な歴史的理由で作り上げられており、必ずしも現在において最適とは限らない。

これは必ずしも非合理とは言えない。

最適化のコストが高く、ランニング・コストが十分に低ければ、そのままにしておいたほうが合理的だとすら言える。

電流の向きが逆向きにならないのと同じ理由だ。

そして様々なゴミを身にまとっているからこそ、我々の文化は豊穣なのだとすら言える。それは我々の文化が、恣意的な決めごとでできていることを教えてくれる。また、新しいことが、古いことの衣替えから生まれた事例の多いことを考えれば、将来的に、何が役に立つかはわからないのだ。

人類の歴史においては、どんな最適化も、「早すぎる最適化」の可能性があることを肝に銘じるべきである。

今回のような左作用と右作用の混乱だって、うまく扱えば、怪我の功名と出来るかも知れない。大学で数学を学ぶものが、左作用にはすぐに馴染めても、右作用にしっくりこないのは、偏に中学以降左作用しか扱ってこなかったからだ。右か左かなら、単なる表記の違いに過ぎないとも言えるが、群論などでは、両側からの作用がどうしても必要になるのでこれは困る。

むしろ、早めに右作用の存在を知らしめてもいいのかも知れない。日本人は、その点、西洋人より有利なのだ。なにしろ、日本語の文法がそもそも逆ポーランド式なのだから。

もしそうなったら、関数の右作用をお進めしたい。プログラミング教育と絡めれば、関数を値ではなく、「対応や操作の抽象化」として正しくとらえる機運を高められるかもしれない。

しかし、これはもし欧米圏においては、正解の式が逆になっているだけだ、ということなのかも知れない。

ただ、ちゃんと調べた分けではないが、欧米圏では特に掛け算の順序に気を使っているわけではなさそうである。個人的には、もっと形式的に教えている印象だ。

教育学的には、これだけいろいろな国があれば掛け算の順序を気にするか否かで、算数の成績に差が付くかどうか統計が取れそうなものである。私の直感では差はつかないと思うが、誰か一度やってみていただきたい。学問的にはこれで決着がつく。

ただし、今回の問題が根深いのは、これがただ学問内部の話なのではなく、一種政治的な話だからなのだ、という点は後述する。

おそらく一番強力であるにも関わらず、あまり教師に顧みられない反論として、算数及び数学ができた人たちが、自分たちを反例として差し出すものがある。

私も含めて、数学ができた人間達はたいがい、掛け算の順序というものに気をつけた覚えはない。もしそれで、実際には小学校教師たちが考えている順序に無意識にしたがっているのだとすれば、ただ単に我々の自己認識が間違っているだけになるのだが、そんなこともない。

大体、掛け算の順序に気をつけていては、交換則結合則分配則を駆使した効率的な計算の工夫ができない[*2]。

また、掛け算の順序を気にしなかったために、割り算に苦労した記憶も全くないし、むしろ割り算においては、割る数と答が交換可能なことに人より早く気づけて良いくらいかもしれない。

そもそも、小学生に算数を教えると、繰り下がりのある引き算をさせると、彼らの多くは、筆算で下から上を引こうとしてしまう。もし、彼らの言うとおり、これが可換性の弊害ならば、足し算においても計算の順序に気をつけなければいけないはずだが、そんな話は聞いたことがない。

おそらく、割り算に躓くのと、掛け算の可換性とも、あまり関係がないのではなかろうか。

1.5　ここまでの議論に足りないこと。そもそも数学を使うとはどんな行為なのか?

まず私なりの結論から言うと、正しいのはやはり数学者側、つまり、掛け算の順序などどうでもよい、という側である。そして、その判断をするのに、上で出た反論で十分だと思っている。ではなぜ、それで話が終わらないのか？　もしくは、終わってしまっている議論が延々と続いてしまったりするのか？

それは反論側の議論の不手際だと思っている。総じて、この議論において、自らの態度をちゃんとした言葉で表現しようとしているのは、賛成側、すなわち掛け算の順序を大事だと考えている教師側である。

それに対して、反対者の数学者及び数学ができる人間の側は、相手の考えを一蹴に伏すことに拘泥するあまり、議論が侮蔑的感情的になりがちで、ちゃんとした言葉で表現できていない。

[*2] 計算の工夫についてはよりラディカルな視点から後で取り上げる。

上で紹介した反論も、一つ一つは全くそのとおりなのだが、結局根拠が、「私はこれでちゃんと数学が出来た」「諸外国で掛け算の順序に拘っている国はほとんどないが、数学の成績が落ちるということはない」という実例及び証拠によっている。

実例に則った議論は、強い説得力を持ち、証拠に則った議論は、科学の基本だが、理論に凝り固まっている人間には届かないこともある。「論より証拠」という科学の原則が相手に届くとは限らない。

これはすでに科学の外の問題なので、証拠を持ち出せば勝ちになるとは限らない世界なのだ。そもそも何を証拠とするかは、その人の世界観に依ってしまう。こちらが確かな証拠と思って提出したものが、相手を説得させるとは限らない。これはもう、科学ではなく、より広い政治の世界なのだ。

彼らが掛け算の順序に拘らないと算数が出来なくなる、という事実無根の現象の存在を支持する理論を持ち出してくるなら、相手の土俵に上がり込み、理論の領域で、その理論のどこが間違いなのか、そして正しい数学教育の理論的支柱はなんなのかを明らかにしてやる必要がある。

そのためには、そもそも「数学ができる、数学を使う、とはどういうことなのか」を解きほぐして説明してやらないといけないのだ。

つまり大雑把に言うと、これらの議論の紛糾は、教師及び数学者双方の、「哲学の貧困」が原因である。教師は誤った哲学を持ってしまった、という意味で。数学者はその誤った哲学を正す哲学を持っていなかった、という意味で。

私はクワイン以降、例えばラカトシュだったり、より最近ならソーバーなどの科学哲学をもっと一般に教えておくべきだと考えている。これらの知見を基礎教養とすべきである。そうしておけば、このような下らない問題が、必要以上に長続きすることなどなかったろうに。

そもそも、一番問題にしなくてはいけないのは、教師側の

「意味が分かっていないといけない」

という部分だ、というのが皆正しく認識できていない。

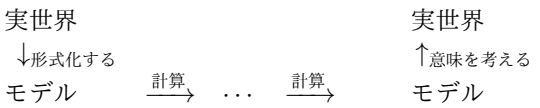
そもそも数学ができる人は、数学の問題を解くときに、いちいち意味など考えていない。そしてそれこそが、彼らが数学が出来る理由の一つなのだろうと思われる。

近年の科学哲学では、科学理論というものは、世界を直接記述するものだとは考えられていない。科学理論は実世界によく似た仮想世界、「モデル」を記述するものなのだ。簡単な例を出すと、物理における「理想気体」などがそうである。あれは実際に世界について語っていると見なせば単なる偽になってしまう。あれはモデルについて語っているのであって、そのモデルが世界と似ていることにより、我々は世界について予測したり、さらには世界についての知識も得られる、というわけなのだ。同人の一人古賀氏も大学学部生に物理を教える場合、そこから入ると証言している。

そして、数学の有用性は、このモデルを記述する言語の一部として輝く。

そして数学の意味が問題になる時とは、この世界とモデルをつなげるときである[*3]。

[*3] 論理学等における普通の言葉遣いでは、理論の「意味」とはそのモデルである。しかし、ここでは「モデルと世界の対応」を「意味」を考えているので、かなり慣用とは違う。というのも、理論と形式的なモデルを対応付けて、理論の「意味」だと主張するのは、日常的な用例と乖離が大きすぎる気がしているのだ。何らかの形でモデルが現実との類似を持たないと、理論は日常的な意味での「意味」は持てない。集合論が数学の意味だと言われても、普通は困るし、それは日常的な意味での「意味」では絶対にない。もし、まるで現実があまりにも確たるものであるかのような語り方が気になるなら、理論を満たす状態（モ



このとき、途中の計算において、必ずしも世界との対応（つまり意味）があるとは限らない。先述した古賀氏は、途中計算の一つ一つの式に対して意味を聞いてくるがいる、という話をしていたが、たとえそのモデルとこの実世界がよく似ていたとしても、モデルの側でまるで「物」のように見えているものが、現実でも「物」と言える存在とは限らない[*4]。それは世界の構造とかパターンのようなものに過ぎず、地と図で言ったら地であるがゆえに、よほど注意しないと見えてこないものかも知れない。それに対していちいち意味を考えるのは苦痛だし、苦行である。もちろん、このモデルにおける操作に現実との対応物があるのは歓迎すべき事態である。

抽象的な議論が続くと、今自分が何を考えているのかが分からなくなるし、間違っていることを延々と続けてしまうこともあり得る。数学や哲学などの抽象学問が人をノイローゼにする理由である。

その長い道行の途中で現実との接点があることは、良い休憩になる。

しかし、全てのステップで現実との対応を考えてしまうと、数学の旨味がなくなる。

数学の旨味、それは「意味を考えなくてすむ」ということだ。

意味を考えないからこそ、思考の節約が出来、意味を考えていたら届かないほど遠くへと思考を飛ばせるのだ。

いちいち意味を考えていたら数学を使う必要がない。ラピュタの住人のように、たくさんの実物を持って、それを提示しながら議論したら結構だろう。

意味を考えないからこそ、意味を考えたらどう見ても別々の概念たちに、共通の構造があることが見えるのである。

意味を考えないから、人工知能と呼ぶほどには高級でないコンピュータにも自動化させることが出来る。

デル）を我々がイメージでき、それが我々が持つ世界のイメージと関係を持てる、と言うことが「意味」だと言える。だから、ここではモデルはかなり理論の側にあり、ただ理論と現実の世界との関係が、「満たす・満たさない」ではなく、理論を満たすモデルと世界が「似ている・似ていない」関係であることを言うために必要なアダプターの役割を持っているにすぎない。先ほどの言い換えではさらに「イメージ」という言葉をさらにアダプターにしている。

化学や生物の理論は特定のイメージと強い関係を持つが故に「意味が濃い」が、数学はそのような特定なイメージがなく、むしろ様々なイメージと弱い関係を持つが故に「意味が浅い」。それでも数学は様々なイメージと浅い関係を持っているので、単なる言語操作ととは言えない（単なる言語操作にしてしまえる、という話とは別）。この論考は普通に数学が出来る人の直感に哲学を与えたいと思ったもので、普通に数学が出来る人は、自分がやっていることは単なる言語操作だとはあまり考えない。「数」という物を操作していると思っている。これは何も実在論を擁護しようとしているわけではなく、ただ、数学が出来る人は、まるで数を操作しているように感じる、と言っているだけだ。そして、これは数学を学ぶ生徒に会得してほしい感覚である。そのためには、数学が様々なモデルやイメージと浅い繋がりを持つことを体験して欲しい。そこに数学の自由がある。これが、「単なる言語操作の話にしては？」という有益なアドバイスがあったにもかかわらず、通常の言葉遣いを曲げてまで、モデルの話を残した理由である。

[*4] 正確に言えば、ここではモデルの話と、計算の話をごっちゃにしている。モデルとは、理論を満たす状態という抽象的なもので、目に見えるものではないが、計算は、理論を構成する言語や図形の操作であり、目に見える。モデルは操作できないし、当然計算も出来ない。計算の途中経過が、モデルに対応物を持っているとは限らないし、モデルに対応物を持っているからと言って、現実に対応物があるとは限らない。ここの部分は後日全面的な書き換えが必要とされると思われる。ひとまず、実世界とモデル以外に前の脚注で少し書いたような層がいくつも必要とされるだろう。

数学が出来る人も、意味を考えないからこそ、素早く計算が出来るのである。

これはもちろん程度問題で、数学が出来る人も意味は考えるし、答えが合っていればいいというわけではなく、例えばリンゴ 2 個とみかん 3 個を足す問題で、「$1+4=5$」と答えたら、どう考えてもおかしい。

先ほどの閑話で少しかいたように、関数の意味、つまり「対応、もしくは操作の抽象化」という「意味」は逆にもっと時間を掛けて教えなくては行けないと考えている。

しかし、四角形を９０度回転しても面積が変わらないことを納得したら、掛け算の順番なんかどうだっていいのだ。単位の問題はむしろ、計算と独立して考えた方がいいだろう。単位こそ意味の問題であり、形式と意味を分離した方が扱いやすくなるからだ。小学校程度の簡単な問題なら、答の単位は立式の前にすでに分かるはずだ。１００円が 2 枚だったら、２００円であって、２００枚でないことは、立式以前の問題である。それ以前に解決していなければ行けないことを、立式まで持ち込むのは無用な混乱の元になる。掛け算の順序を間違えたら（つまり 2×100 と書いてしまったら)、ついでに答えの単位も間違える（つまり２００枚と答えてしまう）ようなら、むしろそちらのほうが意味が分かっていないのである。単位のサンドイッチ方式は、分離すべき意味と形式をまぜこぜにしようとする点で害悪なのだ。

意味から形式を抽象し、形式を選ぶときにはもちろん意味を見て選ぶのだが、一度形式の世界に移行してしまえば、形式はまるで意味から独立しているように振る舞える。

そしてこのような面にこそ、数学の自由さがある。以前何かの塾の CM で見た話なのだが（あやふやな記憶ですまない)、イギリスかどこかの初等教育では「$2+3=\square$」ではなく「$\square+\square=5$」を解かせるという話を、「創造性を養う教育」という文脈で語られていた。ここでは意味は希薄である。もちろんこの程度なら容易に意味づけ出来るが、これを考えるのに「りんご」や「みかん」を持ち出すのが補助にはあまりならない。むしろだんだんと桎梏になっていく。また、これは「9×99」を「$9\times(100-1)$」と考えることへの萌芽が感じられるが、このような計算の工夫にも意味は足かせとなっていく。例えば、「5 円のガムが 45 個と５５円のチョコを 5 個で何円」という問題だったら、一度小学校教師の言う正しい意味を忘れないと計算の工夫が出来ない。そうして、意味の呪縛から離れたからこその自由さがある。先ほどの CM の言うことには一理あって、意味を一度忘れてしまうことと、創造性には明らかな関係がある。殊数学の創造性に限って言えば、まさに意味を忘れることに本質がある。

さきほどの「$\square+\square=5$」には単なる計算の工夫だけではなく、負の数概念の胞芽も含まれていると考えられる。足すと 0 になる数を捏造すればいいのだ。負の数や複素数は、今となっては容易に意味づけ可能だが、歴史上これらの概念は意味から離れた形式的な思考によって発見された。だからこそ大きな抵抗感を人々は感じつづけたのだ。高等数学まで進めば、累乗を自然数から整数へ、有理数へ、実数へ、そして複素数まで拡張したことにより、美しいオイラーの公式「$e^{i\pi}+1=0$」に至ることが出来る。実はこの式には、e^x を $f'=f, f(0)=1$ の解と捉えることにより、意味付け可能なのだが、やはりそれでも最初から最後まで厳密な意味を求めていたら、なかなか到達できなかったであろう。

また階乗を複素数に拡張したガンマ関数や、フーリエ変換を利用した「分数階微分」なども数学の自由さの興味深い例であろう。

この自由さこそ、ルイス・キャロルやレイモン・クノーなどのナンセンスや言語遊戯と相性がよい理由であり、数学者のフランソワ・ル・リヨネーがレイモン・クノーを師範格

として発起した「ウリポ」では、数学的・機械的な手法で、通常の発想法を超えた文学を作ろうとしたのも、ここに起因する。もちろん遡れば、ユダヤのカバラ、ライムンドゥス・ルルスの「大いなる術」、タロット・カードなどとも関連付けられるだろう。これらの技術も、最後には解釈によって、世界と結び付けられることがゴールなのだが、その途中で意味から離陸することによって、通常よりも遠くへと想像の翼を広げることができるのだ。

数学においても、意味を置いてけぼりにして、あまりに遠くまで行ってしまうからこそ、そこに意味を求めざるを得ない。例えば、リーマンゼータ関数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

において、

$$\begin{aligned}\zeta(2) &= 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots \\ &= \frac{\pi^2}{6} \\ \zeta(4) &= 1 + \frac{1}{16} + \frac{1}{81} + \frac{1}{256} + \cdots \\ &= \frac{\pi^4}{90}\end{aligned}$$

などの、特殊値を見ると、どうしてここに円周率が出るのであろうかと、意味を考えないではいられないのである。

ことほどさように、数学において、意味が分かれば出来る、などという単純な公式は成り立たない。

ではなぜ、小学校の教師は意味に拘ってしまうのであろうか。

邪推であるが、多くの小学校教師は数学が出来なかった人間で、そして同時に数学の意味が分からなかったのではないか、と考える。だから、「意味がわかれば算数や数学が出来る」という勘違いをしてしまうのではなかろうか。

そして意味を考えさせる教育が、小学生の抽象思考能力の発達を阻害していないだろうか。単位をいちいち考えさせるから、割合や比など単位を持たない量の理解が遅れているのではなかろうか。そもそも割合の計算に、彼らの言う単位のサンドイッチは成り立っていない。そして、面積の計算にも、単位のサンドイッチは成り立たない。

抽象化とは簡単に言ってしまえば、物事から意味を抜き取っていくことだ。意味を抜き取れば、どんどん形式だけが残っていく。正しい形式化をすれば、大概の物事は自明になってしまう。それこそ、数学の方法である。

もちろん、数学を使うためには、最初と最後に、世界とモデルを行き来する工程が必ずある。それを教える必要もあるだろう。

しかし実はここは普通に数学をするよりよほど難しいところで、この難しいところを、全ての生徒がマスターしないといけないところと考えるのは間違っている。

教育においては、重要なことを教えることももちろん重要なのだが、もしその重要なことが難しいことだったら、すこし立ち止まって考えないといけない。

生徒というものは、自分には出来ないと思ってしまったら、やらなくなってしまう生き物なのだ。だからこそ、彼らには成功体験を積まさなくてはいけない。

それならば、数学の応用には重要でも、数学自体の本質とは言えない部分は、優秀な生

徒用にとっておいて、それ以外の生徒には、もっと簡単な形式的な計算をさせて、彼らを
褒めてやるべきなのではなかろうか。

第 2 章

ヒルベルト・プログラムと不完全性定理の微妙なカンケイ

鈴木佑京

2.1　はじめに

本稿では、タイトルに有るように、ヒルベルト・プログラムと不完全性定理の間の関係について検討する。「関係って、ヒルベルト・プログラムが不完全性定理によって打ち砕かれたって話じゃないの？わざわざ今さら検討するような話ってあるの？」と思われるかもしれない。もちろん、ヒルベルト・プログラムが不完全性定理によって打ち砕かれたということは、衆目の一致するところである。しかし、両者の関係について書かれた本の中でも、不完全性定理がヒルベルト・プログラムに対して具体的にどのような打撃を与えたのか、そしてなぜそのような打撃を与えることができるのか、という点まで、十分突っ込んで書かれたものは少ない。さらに、全体としては良心的に書かれた文献の中にも、注意深くその主張内容を見定めなければ、ヒルベルト・プログラムおよび不完全性定理に関する誤解につながりかねないような言説が、ないわけではなかったりするのである。

そういうわけで本稿では、現在までに主張されてきた不完全性ベースの議論（不完全性定理によってヒルベルト・プログラムが打ち砕かれた主張する議論）のうち代表的な三タイプを取り上げ、それぞれの主張をサーヴェイするとともに、問題点を（あるなら）指摘する。そのことを通して、ヒルベルト・プログラムと不完全性定理に関する誤解を取り除き、歴史的・概念的理解を深めることを目標とする。特に数学畑の読者にとっては、ちょっと偏執狂的と思えるような細かい検討になるかもしれないが、まあ哲学や歴史についての議論というのはそういうものなのだと思って許して欲しい。

最後にもう一言。たまに、不完全性定理をヒルベルト・プログラムとの関連で取り上げることを嫌う人がいる。曰く、そのような記述は、不完全性定理のもっぱら破壊的な側面を取り上げており、一面的である。むしろ不完全性定理は、ゲーデル数化、対角化、無矛盾性を使った理論の比較、といった道具立てを論理学に導入し、その後の発展の基礎を築いた、創造的・建設的な結果として捉えられるべきである。

私自身もこうした考え方に共感しないわけではない。数学的にはもちろん、私の専門である哲学においても、不完全性定理が建設的な役立ち方をしてきたことは疑い得ない（後

者については、「知の欺瞞」のほうが目立ってしまっているのが残念だが)。しかし、それと同程度に、次のことも確実なことである。すなわち、ヒルベルト・プログラムという、おそらく歴史上もっとも精妙に練り上げられた数学の基礎付けプログラムがかつて存在し、多くの数学者を惹きつけたこと、ゲーデルの不完全性定理が彼らに壊滅的な打撃を与えたということ。そしてそれが、少なくとも歴史的・哲学的観点から見たとき、興味深くまたドラマティックな出来事であったこと。つまり、破壊的な側面だけではなく、建設的な側面もあった、と言いうるのと同じように、建設的な側面だけではなく、破壊的な側面があった、とも言いうるはずである。双方の記述は補完的であって、どちらが悪でどちらが善というようなものではない。

さらに、不完全性定理の創造的側面と破壊的側面は、実は複雑に絡み合っており、そう簡単に切り離せない。我々は、不完全性定理の破壊的な効力を論じていく中で、全数学を形式体系に埋め込むことが困難であるという考えや、一つのメタ数学的概念を複数の形で形式化する可能性といったことに言及する。前者は、与えられた形式体系の自然な拡大を考え、その拡大を一定回数繰り返した体系がいかなるものになるのか、という問題意識を証明論に導入した（例えば、[5] はこのような問題意識に基づく研究である）と考えられるし、後者も、算術化の方法を変えることによって形式化されたメタ数学がどのように変化するのかを調べる研究につながっている（例えば、[10] を見よ)。つまり、不完全性定理の破壊的側面について立ち入った検討をしようとすれば、その過程で我々は、不完全性定理の創造的側面とも出会うことになる。従って、一見「破壊的」と見える側面を全く無視してしまうことは、逆に不完全性定理の創造的側面の一部を無視してしまう結果になりかねないのである。

そういうわけで、私自身は、不完全性定理の「破壊的」側面を語ることもまた、十分な意義があることだと思っている。その意義がどのようなものになるか、以下の記述によって少しでも伝われば幸いである。

2.2　ヒルベルト・プログラム概観

まず、そもそもヒルベルト・プログラムがどのような計画だったかを見なおしておこう。以下は読者にある程度の知識が有ることを仮定した極めて簡潔なまとめになっているので、より初心者向けの解説としては例えば [14] を見て欲しい。また、ヒルベルト・プログラムをどう解釈するかは研究者によって様々なスタンスがあるが、あくまでスタンダードな解釈を提示する[*1]。

2.2.1　有限の立場

ヒルベルト・プログラムは、有限の立場と呼ばれる弱い数学をまず範囲づけた上で、それを基礎として、他の数学を基礎づけるプログラムである。有限の立場は、命題と証明の両面から範囲づけられる。

- 有限の立場において理解可能な命題は、1) 具体的な記号についての、有限ステップ

[*1] 実を言えば、私自身もこのスタンダードな解釈には誤りがあると思っている。が、この原稿ではその点には触れない。

でチェック可能な命題（以下、決定可能な命題）か、２）具体的な記号についての、有限ステップで決定可能な述語（以下、決定可能な述語）を全称化した命題、のどちらかである。１）の例は、例えば 3+2=5 のような等式であり、これは ||| と || を並べると ||||| になるという記号についての命題であると考えられる。２）の例は、例えば $\forall xy(x+y=y+x)$ である。

- 有限の立場において妥当な証明は、直観的な明証性を与えることのできる推論原理だけを使ったものである。具体的にどの範囲の推論原理が直観的な明証性を持つのかは、ヒルベルトの文献の中でも判然としないが、決定可能な述語についての数学的帰納法はそのなかに含まれるとされている。また通常、有限の立場において妥当な証明原理は、少なくとも直観主義的に妥当な証明原理よりは弱い、と考えられている。

以上のように範囲づけられた有限的な命題（有限の立場で理解可能な命題）について、有限的な証明（有限の立場において妥当な証明）を行うのが、有限の立場である（有限的数学とも呼ばれる）。

有限の立場からは、例えば、有限的な命題に対する全面的な排中律は妥当ではないどころか理解不可能である（決定可能な述語 $\mathrm{A}(x)$ に対し、$\forall x\mathrm{A}(x)$ は有限的命題だが、$\neg\forall x\mathrm{A}(x)$ は有限的命題ではないから）ことに注意。

2.2.2 理念的数学

有限の立場を超える数学は理念的数学と呼ばれ、すべて、形式体系における無意味な記号のゲームであると考えられる[*2]。例えば、二階の自然数論や、集合論などは理念的数学とみなされる。

有限的数学が、有限的命題に対して有限的な証明を行う活動であったように、理念的数学も、理念的な命題に対して理念的な証明を行う活動であると特徴づけることができる。ただし、理念的数学において登場する理念的命題は、単にある特別な仕方で形成された記号表現としての文に過ぎず、意味を持たない（従って、これを「命題」と呼ぶのは本来不適切である）。また、理念的な証明は、単なる記号である式を、形式体系において定められた条件に則って並べた記号の列に過ぎず、有限的証明のような直観的な妥当性を持たない。つまり理念的数学とは、言語と証明のシンタクティカルな定義を備えたなんらかの形式体系 T のなかで、T における式の証明を構成していく活動である、とまとめることができる。

そういうわけで、理念的数学はそれ自体としては単に記号遊びであって、何の意義もないのだが、しかし、有限の立場における命題を導出するための道具としては役立ちうる。つまり、理念的数学の形式体系で、意味を持たない記号としての理念的命題を経由した証明によって、有限的命題を表現する文を示す、ということは可能である。有限の立場において使える論法が非常に限られたものであるゆえ、理念的数学の道具としての価値は非常に高いものとみなすことができる。

だが、理念的数学における形式的証明は直観の裏付けのない、規則に従って並んだ単な

[*2] ヒルベルトが理念的数学が本当に無意味であると考えていたかどうかは議論がある [17]。だが意味のないゲームであるかのようにみなせると考えていたのは間違いがないだろう。

る記号列にすぎないので、そのままでは証明としての力を持たない。そこで、次の保存拡大性を示してやる必要がある。

（T-保存拡大性）任意の有限的命題 A に対し、A に対応する文 A が理念的数学の形式体系 T で証明できるなら、A は有限的に証明できる

（T-保存拡大性）が示されたなら、理念的数学の形式体系 T において A が示されたということをもって、有限的な証明の存在も結論できる。そして、有限的な証明は、直観の裏付けによって証明としての力を持っている。従って、理念的証明も、有限的証明から派生したものとして、証明としての力を得ることができるようになる。これで晴れて、形式体系 T における理念的数学を道具として使用できることになる[*3]。

但し、（T-保存拡大性）それ自体は、有限的に証明される必要がある。というのも、本来証明としての力を持っているのは有限的証明だけであり、理念的証明が有限的証明と同等の力を持つものとみなすことができるのは、（T-保存拡大性）が示された後のことだからだ。

2.2.3　保存拡大性と無矛盾性

ここまででヒルベルト・プログラムの主要目標は出揃った。

1. 基礎づけの対象としたい数学を、形式体系 T として形式化する。
2. (T-保存拡大性) を有限的に証明する。

ここでもし、T が、決定可能な命題に対する完全性（つまり、有限的に証明できる決定可能な命題は、T で証明できるということ）を備えており、さらに、それを有限的に証明できる、としてみよう。決定可能な命題というのは、本質的には先程述べた $3+2=5$ のような等式にすぎないので、この想定はそれほど奇妙なものではない。

すると、この想定のもとでは、(T-保存拡大性) を有限的に示すことと、T の無矛盾性（T-無矛盾性）を有限的に示すことが同じことになる。以下、決定可能な命題に対しては、排中律の各インスタンスを有限的に示すことができる、ということを利用する。

- 保存拡大→無矛盾　保存拡大性が有限的に示されたとして、以下のように無矛盾性の有限的証明を行う。有限的命題 $0=1$ について保存拡大性を適用すると、T で $0=1$ が示されたなら、$0=1$ である、ということができる。これは、T で $0=1$ を示すことができるとすると矛盾する、ということにほかならない。つまり、T が無矛盾である、ということにほかならない。
- 無矛盾→保存拡大　任意の有限的命題 A と、T における A の証明から、A の有限的証明を構築する方法を示せば、保存拡大性を有限的に示したことになる。そこで、無矛盾性が有限的に示されていることを前提して、A の有限的証明を構築する仕方を以下のように提示する。1）有限的命題 A が決定可能な命題の場合は次のような証明を作る。決定可能な命題を否定した命題も決定可能なので、¬A も決定可能な命題である。¬A なら、完全性より、T で $\neg A$ が証明できる。だが、T で A

[*3] ただし、ヒルベルト・プログラムの目標を保存拡大性として定式化することに関しては、[3] が異論を唱えている。

も証明することができるので、無矛盾性に矛盾する。よって、¬¬A。決定可能な命題に対しては、排中律を使っても良いので、二重否定を除去できる。従って A。２）決定可能な述語 B(x) について、A ≡ $\forall x$B(x) と表せる場合は、次のような証明を構築する。決定可能な述語に数を代入した命題は決定可能な命題になる。つまり、任意の x について、B(x) は決定可能な命題である。そこで、x が与えられたとして、¬B(x) を仮定すると、完全性より、T で ¬$B(x)$ が示せる。先ほどと同様の理屈で、¬¬B(x)、B(x) が有限的に示せる。以上の証明は x を完全に任意のものとしているので、全称汎化して、$\forall x$B(x)。さて、任意の有限的命題 A が与えられた時、１）か２）の対応するどちらか一方を持ちだして、A の有限的証明を構築することができる。従って、任意の有限的命題 A と、T における A の証明から、A の有限的証明を構築する方法を示すことができたので、保存拡大性を有限的に示すことが出来た。

従って、ヒルベルト・プログラムの遂行は、実質的には、次のように置き換えられる。

1. 基礎づけの対象としたい数学を、形式体系 T として形式化する。
2. (T-無矛盾性) を有限的に証明する。

いちおう注意しておくと、ヒルベルトプログラムの第一義的な目標は、無矛盾性を示すことそれ自体ではなく、あくまで保存拡大性を示すことにある。無矛盾性はそのための中間ステップにすぎない。この点は誤解されやすい。

2.3　不完全性ベースの議論その１　全数学の公理化？

では早速不完全性ベースの議論の検討に移ろう。まず一つ目のタイプは、第一不完全性定理が、ヒルベルトプログラムに対する打撃を与えると主張する。第一不完全性定理のステートメントを確認しておこう。

(G1) 再帰的に公理化できるような形式体系で、ロビンソン算術を含むような任意の T に対し、T が無矛盾ならば、T において、証明も反証もできないような文 G_T が存在する。

そして、このタイプの議論が利用するのは、G1 の主張を次のように強めたものである。

(G1+) 再帰的に公理化できるような形式体系で、ロビンソン算術を含むような任意の T に対し、T が無矛盾ならば、T において、証明も反証もできないが、真である文 G_T が存在する。

「真である」という意味論的な主張が入っていることに注意して欲しい。さて、この G1+ を武器にして、このタイプの主張は、ヒルベルトプログラムの第一ステップが遂行不可能であることを主張する。このタイプの主張の例として、『論理の哲学』（名著です）の遠山茂郎の議論を引用してみよう。

> まず第一不完全性定理の方から見よう。ヒルベルト・プログラムはまず、数学のさまざまな分野に対して公理系を設定し、その上でそれらの公理系が無矛盾であるということを示すという二段構えであった。数学で用いられるあらゆる論法が公理

> 系という形で表せること、もし全数学の基礎づけを与えようとするならばこの作業が必要である。しかしこの定理により PA[引用者注、ペアノ算術のこと] から独立な命題が存在するわけだが、この命題はじつは自然数の世界で真なのである。そして有限の立場で認められる仕方で PA をいくら拡張しても（じつはこれが「PA の公理を含む公理系」の精確な内容である)、こうした命題は常に存在するのである。これは真と判断するために用いられている論法が公理系という形式的な手段では捉えられないということを表しており、全数学の基礎づけに必要な作業がうまく進まないことになろう。（pp.101-102）[9]

ものすごく大雑把に言うと、このタイプの議論は、ヒルベルト・プログラムは全数学の公理化の可能性を前提しているが、しかし、G1+ によってそれが不可能であることが示された、従ってヒルベルト・プログラムは実行不可能である、というものである。不完全性定理が全数学の公理化の夢を砕いたという話は、ヒルベルト・プログラムと無関係にもよくなされる話である。

「全数学の公理化」と呼びうるような活動には、実は正確には二つの異なった理解の仕方があることに注意しよう。第一は、あらゆる数学的真理を証明するような形式体系を構築することであり、第二には、我々のもつ認識手段によって認識可能なあらゆる数学的命題を証明するような形式体系を構築することである。数学的真理と、認識可能な数学的命題が、ぴったり一致するのでない限り、二つの活動は異なった目標を持つことになる。それぞれの活動について、1）G1+ は本当にそれが不可能であることを示したのか、示したと言えるとしたらなぜなのか、2）そもそもヒルベルト・プログラムはその活動を必要としているのか、をチェックしてみよう。

2.3.1　全数学的真理の公理化

まず、全数学的真理の公理化というとき、ここで言われている数学的真理が、1）ヒルベルト・プログラムの数学観を受け入れた上での「真理」なのか、2）古典的数学観を受け入れた上での「真理」なのか、に注意しておく必要がある。というのも、ヒルベルト・プログラムの背景にある構成主義においては、真理と証明可能性は一致している。そして、ヒルベルト・プログラムにおいて本当に証明としての力を持っているのは有限的証明だけなので、結局のところ、有限の立場において理解可能で、かつ有限的に証明できるような命題だけが真であると言われうることになる。つまり、古典的数学観において真理と言えるような命題であっても、ヒルベルト・プログラムの数学観においては真理といえない命題が存在する。前者を「古典的真理」、後者を「有限的真理」と呼んでおくことにしよう。現在問題になっている批判が念頭に置いているのは、このうち、前者のほうであると考えられる。ヒルベルト・プログラムで問題になる形式体系は、有限的数学ではなく、古典的数学を形式化したものだからである。

1）では、G1+ は、すべての古典的真理を網羅し、かつ、それだけしか証明しない形式体系は存在しない、ということを示しているだろうか。おそらく、それは次のような議論によって示されるだろう。すべての古典的真理を網羅した、再帰的な形式体系 T が存在するとする。ロビンソン算術の定理はすべて古典的に真なので、T はロビンソン算術を含む。さらに、T は無矛盾であるということは、古典的真理である。G1+ より、T が

無矛盾なら、G_T は真であるということが、古典的真理である。従って、G_T は古典的真理である。だが、G1+ より、G_T は T で証明できない。これは仮定に矛盾する。

この論法はそれだけでは問題がある。どこが問題かというと、「T は無矛盾であるということは、古典的真理である」というステップが、どこから出てきたのか不明であることである。つまり、あらゆる古典的真理を網羅し、かつ、それだけしか証明しない体系 T が、必ず無矛盾になるという、隠された前提がここで働いていると考えなければならない。そしてこの前提は、まあ常識的には正しいといえるだろうが、哲学的には疑えないこともない。例えば、A も ¬A も真であるような A が存在するという真矛盾主義を取ったり、また、T が無矛盾であるという命題が、真理値を欠いている（つまり、T は無矛盾だとも、無矛盾でないとも言えない）と考えるなら、この前提を拒否する余地が出てくるかもしれない。従って、こういう哲学的可能性を念頭に置くと、G1+ だけをとってきて、古典的真理を網羅する形式体系の可能性が潰れた、とは、直ちには言えない（常識的には言えるが)。

ただし、ヒルベルト・プログラムの目標を念頭に置くと、この前提は自然に擁護できる。つまり、このような T に対してヒルベルト・プログラムが可能であるためには、T の無矛盾性が有限的に証明可能でなくてはならない。だが、有限的に証明できること、つまり有限的真理は、古典的真理でもあると言えるだろう。従って、T に対してヒルベルト・プログラムが実行可能であるのならば、体系 T が無矛盾になるということは古典的真理になるはずであり、不完全性定理は、すべての古典的真理を、そしてそれだけを形式化した体系が存在しないことを言える。まとめると、この議論が確定的に示したといえるのは、ヒルベルト・プログラムが実行可能で、再帰的に公理化でき、かつ、古典的真理を、そしてただそれだけを証明する体系 T が存在しない、ということである。

2）全古典的真理を形式化することが、ヒルベルト・プログラムにとっていかなる意味で本質的といえるのかは、かなり理解が困難である。というのも、ヒルベルト・プログラムが問題にしているのは、我々の行っている数学活動を正当化することである。従って、正当化の対象は、数学的認識活動であって、数学的真理そのものではない。もちろん、ヒルベルト自身は、あらゆる数学的真理は証明可能である、と考える傾向を持っていたが、その考えはヒルベルト・プログラム自体には本質的ではない。よって、全古典的真理を形式化できようができまいが、ヒルベルト・プログラムに直接の関係はないと結論できる。

2.3.2　全数学的認識の公理化

次に、全数学的認識を公理化することが不可能である、という主張を考えてみる。先の引用はこちらの主張を念頭に置いているだろう。認識可能な数学的命題についても、古典的に認識可能な命題と、有限的に認識可能な数学的命題とを区別できるが、問題になっているのは前者の、古典的に認識可能な命題[*4]である。

1）G1+ は、すべての数学的に認識可能な命題を網羅し、かつ、それだけしか証明し

[*4] 「認識可能」という言葉は多義的である。一つには、公理から証明されうる命題だけが認識可能である、という解釈がある。もう一つには、証明と異なる認識手段を認め、これによって真とわかる命題も認識可能なものとみとめてよい、という解釈がある。ここで新たに持ち出すことのできる認識手段としては、例えば「数学的直観」や、あるいは正しいと分かっている定理からそれを説明する原理への「アブダクション」などがある。こうした複数の解釈のうちどれを採用するかは、以下ではオープンにしておきたい。実際、どのような解釈を採用したとしても、議論は通用するはずである。

ない体系が存在しないということを示しているだろうか。議論は数学的真理の場合と全く同様に進む。もし、そのような体系 T が存在するなら、T はロビンソン算術を含んでいる。そして、T の無矛盾性を、我々は数学的に認識できる。G1+ も認識できるので、ここから、G_T の正しさを認識することができるが、T は G_T を示せないので、矛盾する。

問題の所在も数学的真理の場合と同じである。すなわち、「T の無矛盾性を、我々は数学的に認識できる」ということは、なぜ言えるのだろうか。T が弱い体系、それこそロビンソン算術やペアノ算術の場合は、その無矛盾性を認識していると言っていいだろう。だが、T の候補として例えば ZFC のような強い体系を考えてみると、この前提は、明らかな誤りとまでは言わないものの、かなり怪しくなってくる[*5]。もちろん、ZFC の無矛盾性を、我々は経験からの帰納によって認識しているとは言えるかもしれない。だが、これを数学的な認識といっていいかどうかは疑問の余地がある。

しかし、やはり数学的真理の場合と同じく、ヒルベルト・プログラムの目標を念頭に置くと、この前提も擁護できる。つまり、ヒルベルト・プログラムが T について実行可能であるのなら、T の無矛盾性は有限的に認識できる。有限的に認識できるものは古典的にも認識できると考えられるので、T の無矛盾性を我々は数学的に認識できることになる。従って、この議論が示すのは、ヒルベルト・プログラムが実行可能で、再帰的に公理化でき、かつ、古典的に認識可能な命題を、そしてただそれだけを証明する体系 T が存在しない、ということである。

2）このことから、古典的に認識可能な命題のすべてを一つの形式体系 T にまとめ、T の無矛盾性を有限的に示すことによって、古典数学の全域を一挙に正当化するということは不可能になる。だが、ヒルベルト・プログラムを実行する上で、こんなことをする必要があるかどうかはかなり疑問である。例えば一階算術、例えば二階算術、例えば集合論と、正当化したい数学の領域のそれぞれについて形式化を行い、それぞれについて無矛盾性を示すことの可能性は否定されていない。そして、もしこれができれば、ヒルベルト・プログラムの意義は十二分にあるはずである。従って、数学的真理の場合と同じく、認識可能な命題のすべてを形式化することができないということもまた、ヒルベルト・プログラムにとって本質的ではない。

2.3.3　この節のまとめ

以上より、一つ目のタイプ、全数学の形式化の不可能性を主張する議論については、問題になっている「全数学」を「全数学的真理」と解釈しようが、「認識可能な全数学的命題」と解釈しようが、ヒルベルト・プログラムの批判としてはポイントを外していると結論できる。また、全数学を形式化した体系は存在しないという主張自体も、正しくは、「全数学を形式化し、かつ、ヒルベルト・プログラムを実行できるような体系は存在しない」と弱めた形でしか擁護できない。

2.4　不完全性ベースの議論その２　保存拡大性への反例

二つ目のタイプは、G1+ で存在が主張される G_T が、保存拡大性に対する反論になっていることを主張するものである。このタイプの議論は、例えば [7][13] によって主張さ

[*5] 以上の議論は [8] による

れている。前提として、G_T が、決定可能な述語の全称化として理解できること、つまり、G_T は、有限的命題を表現しているとみなせることを押さえておいて欲しい。議論は以下のように進む。

1. 有限的数学を網羅した無矛盾な再帰的形式体系 F が存在するとする。
2. ロビンソン算術の定理は有限的に証明できるので、F はロビンソン算術を含む。
3. G1 より、G_F は F で証明できない。
4. 従って、G_F は有限的に証明できない。
5. ところが、任意の形式体系 T について、もし、F の無矛盾性と、F についての G1+(つまり、「F が無矛盾なら、G_F」ということ) を、T において示すことができ、かつ、T において modus ponens が可能なら、 G_F は T で証明できる。
6. 従って、任意の形式体系 T について、もし、F の無矛盾性と、F についての G1+ を、T において示すことができ、かつ、T において modus ponens が可能なら、G_F は T-保存拡大性の反例となる。

この議論を理解する上で幾つか注意すべきことを挙げておこう。まず、議論の一つ目のステップだが、これは、有限的数学が形式化できるという前提ではない。有限的数学にピッタリ対応する形式体系がある必要はない。ただ、有限的数学を含むような形式体系が存在する、ということだけが確保されていればよい。少なくとも、このような体系が存在することは間違いないだろう（例えば ZFC を考えれば明らかである)。次に、五つ目のステップから登場する、「F の無矛盾性と、F についての G1+ を、T において示すことができ」という条件だが、これは、無矛盾性や G1+ のようなメタ数学的定理を形式化して示すということを含んでいる。だが、この後第二不完全性定理との関連で問題にするように、メタ数学的概念を形式化するやり方には実は複数選択肢があり、どのような形式化を採用するかによって、与えられた体系で無矛盾性や G1+ を示すことができるかどうかは変わってくる。なので、問題の条件は、より正確には、「ある形式化の下で、F の無矛盾性と、F についての G1+ を、T において示すことができ」と書くべきである[*6]。

以上を念頭に置いて、この議論の持つ力を見定めてみよう。この議論は、ヒルベルト・プログラムの最終目標である T-保存拡大性に直接反例を提示するものになっているので、一つ目のタイプの議論とは異なり、ヒルベルト・プログラムの本質をついた批判になっている。従って、一つ目のタイプの議論よりも遥かに重要な議論であると言うことができる。だがしかし、この議論の結論は、ある条件を満たす形式体系 T について T-保存拡大性が成り立たない、という形になっている。つまり、ある範囲の形式体系についてはヒルベルト・プログラムが実行できない、と言っているだけとも言える。なので問題は、この範囲がどれだけ広い（狭い）か、ということである。

一言で言えば、この範囲の広さを決定するのは、一つ目のステップで F として何を取ってくるかである。例えばこの F が PRA のような弱い体系だったとするならば、F についての無矛盾性と、G1+ を示すことのできる理論はかなり幅広くなる。この想定のもとで

[*6] ただし、様々な形式化の選択肢を考えた場合であっても、F の無矛盾性を示すのがどれだけラクかということと、G1+ を示すのがどれだけラクかということは、だいたいバーターの関係にある（一方が大変だと、もう一方はラクになる）ので、形式化を変えたからといって、両方を示せる理論がそれほどドラスティックに変化するわけではない。そういうわけで、この批判の強さを見定める上では、この点にそれほど神経質になる必要はない。

は、例えば一階の PA などが、保存拡大性が成り立たない理論となる。つまり、かなりの範囲の理論について、ヒルベルト・プログラムが実行不可能になる。逆に、F が強い体系なら——例えば ZFC であるのなら——その無矛盾性と、G1+ を示すのはかなり困難になる。従って、保存拡大性が成り立たないとされる理念的数学の体系は、かなり強い体系に限られる。

しかし、すでに述べたように、有限の立場が特別な安全性を持つとされるのは、それが特別弱い体系だからである。このことを念頭に置くと、1 ステップ目で取れる体系 F も、かなり弱い体系になることが予想できる。従って、この批判はかなりの有効性を持つものと予想できるだろう。

次のように言い抜ける道もあるかもしれない。確かに、例えば F として原始帰納算術（以下、PRA）を取ることができれば、PA のような比較的弱い理論についても保存拡大性が成り立たなくなる。だがここで、次のように新しい理論 PA-を定義する。PA-の証明は、PA の証明の中で、G_{PRA} を結論とするものをすべて除いたものである。従って、PA-は、G_{PRA} を証明しない。なので、PA-は、PA のほぼすべての力を保存したまま、先の批判を逃れた形式体系になっている。ヒルベルト・プログラムを実行したい形式体系のそれぞれについて、このようにその都度 G_{PRA} を除いた体系を作りなおせば、先の批判をかわせるのではないか？

だが、この抜け道は殆ど完璧に塞がれている。今問題になっている批判は、F に PRA 以外の何を容れても成立するようになっていることに注意しよう。つまり、PRA とは異なる形式体系であるが、しかし、有限的数学を含み、かつ、PA において G_F が示せるような体系 F が存在するとしよう（このような体系 F の候補として上げられるのは例えば逆数学の体系 RCA_0 である）。すると、PA-でも G_F が示せるが、G_F は有限的に示せない。結局、PA-において保存拡大性は成り立たない。従って、PA から問題の有りそうな証明だけを抜いていって批判をくぐり抜けるには、

1. 有限的数学を含む形式体系 F で、
2. PA において、F の無矛盾性と、F についての G1+ が示せる

ようなすべての F についての G_F を、PA から抜いた体系 PA*を作らなければならない。だが、これをシステマティックに行うことは、ほとんど不可能だろう。

従ってまとめると、二つ目のタイプの議論は、有限の立場を網羅するような形式体系としてどれだけ弱いものが取れるかに依存した形ではあるが、しかし、かなりの範囲の形式体系について、ヒルベルト・プログラムが実行不可能であることを示しているものであると考えることができる。

2.5　不完全性ベースの議論その３　無矛盾性証明の不可能性

三つ目のタイプの議論は最もポピュラーである。この議論は、第二不完全性定理をベースとして、ヒルベルト・プログラムを攻撃する。第二不完全性定理の内容を確認しておこう。

(G2)PRA を含み、かつ、再帰的に公理化可能な形式体系 T について、T が無矛盾であるならば、T の無矛盾性は T で証明できない。

これをもとに、次のように議論が構築される。

1. PRA を含み、かつ、T の無矛盾性を有限的に示せ、かつ、有限的数学を含む体系 T があるとする。
2. G2 より、T の無矛盾性を T で示せない。
3. 従って、T の無矛盾性を有限的に示せない。
4. 仮定に矛盾するので、PRA を含み、かつ、T の無矛盾性を有限的に示せ、かつ、有限的数学を含む体系 T は存在しない。

第二のタイプの議論と同様、こちらも、ある範囲の理論に対して、ヒルベルト・プログラムが実行不可能であることを主張している。こちらで範囲に入ってくるのは、PRA を含み、かつ、有限的数学を含むような体系 T である。

前節でも述べたように、有限的数学は、弱い論法しか使っていないところにポイントがある。なので、ヒルベルト・プログラムの対象となる理念的数学は多くの場合、有限的数学を含むものと考えられるから、この議論は、もし成功していれば非常に強力である。

このようなシンプルで、かつ一番有名な議論をなぜ最後に回したのかといえば、じつは一見する印象に反し、この議論の検討が一番面倒だからである。以下で問題になりうるトピックだけを簡単に紹介するが、まじめに検討しようとすると本当に泥沼としか言いようがない細かい論点に入っていかねばならないので、ここでは深くは追求しない。

2.5.1 議論の正確な形を見定める

問題の所在をはっきりさせるために、第二不完全性定理をより正確な形で書き直す。

(G2+)PRA を含み、かつ、再帰的に公理化可能で、無矛盾な形式体系 T があるとする。この時、T の言語における可導性条件を満たす任意の式 $Pr_T(x)$ について、$ConT \equiv \neg Pr_T([0=1])$ を、T において示すことができない。

可導性条件とは以下の DC1 から DC3 を指す。ただし、$[A]$ は、A のゲーデル数のこと。

(DC1)T の言語の任意の文 A について、T$\vdash A$ なら、T$\vdash Pr_T([A])$。
(DC2)T の言語の任意の文 A について、T$\vdash Pr_T([A]) \to Pr_T([Pr_T[A]])$ が示せる。
(DC3)T の言語の任意の文 A について、T$\vdash Pr_T([A \to B]) \wedge Pr_T([A]) \to Pr_T([B])$

つまり正確には、G2+ は、形式体系で示すことのできる文についての主張である。しかし、ヒルベルト・プログラムで問題になるのは、有限的数学において証明できる命題に関する主張である。したがって、両者を結び合わせる原理を補って、議論を次のように書き換えなければならない。

1. PRA を含み、かつ、T の無矛盾性を有限的に示せ、かつ、有限的数学を含む体系 T があるとする。
2. 任意の有限的数学を含む体系 S について次が成り立つ。任意の有限的命題 A に対して、S の言語で A を表現する文 A' が存在し、A が有限的に証明可能であるならば、$S \vdash A'$。
3. 従って、任意の有限的命題 A に対して、T の言語で A を表現する文 A' が存在し、A が有限的に証明可能であるならば、S$\vdash A'$。

4. 特に、T の無矛盾性を表す命題 ConT に対しては、G2+ の条件を満たすようなある文 $ConT$ が、ConT を表現する文として存在する。
5. 従って、ConT が有限的に証明可能であるなら、$T \vdash ConT$。
6. だが、G2+ より、$T \nvdash ConT$
7. 従って、ConT を有限的に示すことはできない。
8. 仮定に矛盾するので、PRA を含み、かつ、T の無矛盾性を有限的に示せ、かつ、有限的数学を含む体系 T は存在しない。

このように正確に定式化すると、問題になるのがどこかはっきりわかる。つまり、4 番目である。T の無矛盾性を示す命題 ConT を表現する文が、G2+ の条件を満たす $ConT$ であるのは、どういうわけか？

この問題が悩ましいのは、一見無矛盾性を表現しているように見えて、しかし、G2+ の条件を満たしていないような文、従って、T で証明できる文というものが、実際に存在するからである。まず、普通 G2+ の証明において実際に構成される $ConT$ は、次のように作られる。T の公理と推論規則に従って作られた式の列のゲーデル数 x と、その式列の最後の項のゲーデル数 y の間の関係を表す述語 $Prv_T(x,y)$ をまず構成する。次に、証明可能性述語 $Pr_T(x)$ を、$Pr_T(x) \equiv \exists y Prv_T(y,x)$ として定義する。最後に、$ConT$ を、$\neg Pr_T([0=1])$ と定義する。このように作られた $ConT$ は、G2+ の条件を満たしているので、$T \nvdash ConT$ となる。

これに対し、次のようにロッサー証明可能性述語というものを定義する。まず、$RPrv_T(x,y) \equiv Prv_T(x,y) \wedge \forall z \leq x \neg Prv_T(z, \neg y)$ と定義する。ここで、$\neg y$ とは、$y = [A]$ のとき、$\neg y = [\neg A]$ となるような関数である。さらに、T の無矛盾性を前提すれば、$RPr_T(x,y)$ が真であることと、$Pr_T(x,y)$ が真であることは同値であることに注意。さらに、ロッサー証明可能性述語 $RPr_T(x)$ を、$RPr_T(x) \equiv \exists y RPrv_T(y,x)$ として定義する。やはり、T の無矛盾性を前提すれば、$Pr_T(x)$ が真であることと、$RPr_T(x)$ が真であることは同値である。最後に、ロッサー無矛盾性文を、$RConT \equiv \neg RPr_T([0=1])$ として定義する。T の無矛盾性を前提すれば、$ConT$ が真であることと、$RConT$ が真であることは同値である。するとなんと、$T \vdash RConT$ となる。

すると、もしも $ConT$ でなく、$RConT$ のほうが、ConT を表現するのだとすると、上の議論は成り立たなくなる。従って、上の議論がうまくいくためには、$RConT$ のような文を、T の無矛盾性を表現する文として排除しなければならない。つまり、

- ある文が、ConT を表現していると言えるための一般的な基準を示した上で、
- G2+ の条件を満たす $ConT$ のような文だけが、ConT に対してその基準を満たすことができ、$RConT$ のような文はそれを満たすことができない、ということを示す

ことが必要になる。しかし、この二つを首尾良く行うことはできるだろうか？

実はこれは意外と難しい。例えば、次のように議論することができるかもしれない。ある述語 P が T における証明可能性を表現しているためには、「任意の式[*7] A について、$T \vdash A$ と、$P([A])$ が真であることが、同値である」ことを、有限的に知ることができなけ

[*7] 「式」と言った時は開いた論理式も指すが、「文」は閉じた論理式だけを指すことにしておく

ればならない。さて今、理論 T の証明が、通常通り、公理と推論規則に沿って作られた記号列として定義され、そして、T$\vdash A$ を、A の証明が存在すること、として定義したとしよう。さらに、証明図λに対応するゲーデル数を $[\lambda]$、ゲーデル数 a に対応する証明図を$/a/$と呼ぶことにする（証明図のゲーデル数になっていない場合は、なにか適当なダミー証明図を指すことにしておく）。すると、Prv は、公理と推論規則による証明図の定義を、ぴったりそのままなぞって作られているので、「任意の式 A と、任意の証明図λについて、λが A のT における証明図であるなら、$Prv_T([\lambda],[A])$ である」ことを、有限的に見て取ることができる。これをもとに、「任意の A について、T$\vdash A$ なら、$Pr_T([A])$」を有限的に示すことができる。逆に、「任意の A と、任意の自然数 x について、$Prv_T(x,[A])$ なら、$/x/$がTにおける A の証明となる」こともみてとることができる。ここから、「任意の式 A について、$Pr_T([A])$ なら、T$\vdash A$」を有限的に示すことができる。以上より、「任意の式 A について、T$\vdash A$ と $Pr_T([A])$ が同値である」ことを、有限的に知ることができる。そのため、$Pr_T(x)$ は、T における証明可能性を表現する式であると言ってよい。

これに対して 、$RPr_T(x)$ の場合は、「任意の式 A について、T$\vdash A$ なら、$RPr_T([A])$」(以下、@と呼ぶ) ということを、有限的に知ることはできない。今、逆に、@を有限的に証明できたとしてみよう。すると、有限的証明の構成的性格により、この証明においては、適切な有限的手続き f について、「任意の A と、任意の証明図λについて、λがTにおける A の証明であるのなら、$RPrv_T(f(\lambda),A)$」が示されているはずだろう。しかし、前段落で、「任意の A と、任意の自然数 x について、$Prv_T(x,y)$ なら、$/x/$がTにおける A の証明となる」が有限的に示せることを確認した。すると合わせて、「任意の A と、任意の自然数 x について、$Prv_T(x,[A])$ なら、$RPrv_T(f(/x/),A)$」を有限的に示すことができる。さらに $RPrv_T$ の定義を分解すれば、これは、「任意の A と、任意の自然数 x について、$Prv_T(x,[A])$ なら、$Prv_T(f(/x/),[A])\wedge\forall z\leq f(/x/)\neg Prv_T(z,[\neg A])$」(以下、@′) を有限的に示すことができるということになる。このような条件を満たす f としてもっとも有望なのはゲーデル数化関数 $[\lambda]$ である。そこで、f をこれに置き換えると、「任意の A と、任意の自然数 x について、$Prv_T(x,[A])$ なら、$Prv_T(x,[A])\wedge\forall z\leq x\neg Prv_T(z,[\neg A])$」を有限的に示すことができることになる。だがこれは結局のところ、「$\forall xy(Prv_T(y,x)\rightarrow\forall z\leq y\neg Prv_T(z,\neg x))$」が真であることを有限的に示すことができるということであり、これは実質的には、(数論的文としての) $ConT$ が真であることを有限的に示すことと同じである[*8]。つまり、@を有限的に示すことができるとすると、$ConT$ が真であることを有限的に知ることができる。だが、有限的数学を含むTで $ConT$ が示せないのだから、$ConT$ が真であることを有限的に知ることは不可能であろう(メタ数学的命題としての ConT を示せるかどうかという問題ではないので、ここでは、形式化をどうするか考える必要はない)。従って、@を有限的に示すことはできなさそうだ。となれば、$RPr_T(x)$ は、T における証明可能性を表現している式とはいえない。したがって、$RPr_T(x)$ をもとに作られた $RConT$ も、T の無矛盾性を表現している文とは言えない。

[*8] $ConT$ はだいたい、「任意の自然数 x について、x は矛盾のゲーデル数ではない」というような文であり、これに対して「$\forall xy(Prv_T(y,x)\rightarrow\forall z\leq y\neg Prv_T(z,\neg x))$」は、だいたい「任意の自然数 y と x、及び y 以下の z について、y は x が表す式の証明であり、かつ、z は x が表す式の否定の証明である、ということはない」というような文である。ある式とその式の否定の証明がある場合、そこから矛盾の証明を作ることができることを念頭に置けば、両者が実質的に同じであるということがなんとなくわかってもらえるだろう。

この議論は一見妥当に見えるし、実際、常識的なレベルならこれを決定的なものとみなしていいと思うが、しかし、文句をつける余地は十分にある。一つ目の問題点は、条件を満たす f として、単純なゲーデル数化関数以外の候補を全く念頭に置いていない点である。もしも、@′を示すことができるような f として、単純なゲーデル数化関数以外のものを取れるなら、@′が $ConT$ と実質的に同じになってしまうという帰結を避ける事ができるかもしれない。このような f として有望な候補は、証明図をそのままゲーデル数化するのでなく、結論を保持したまま、証明図を一旦別の証明図に変形した上で（つまり、カット除去のような操作を行った上で）、ゲーデル数を取るような関数である。もしも適当な変形を行うことができるなら、@′の後件である「$Prv_T(f(/x/),[A]) \wedge \forall z \leq f(/x/) \neg Prv_T(z,[\neg A])$」が、ほとんどトリビアルに成り立つ可能性がある。

もっと明確な二つ目の問題点は、証明可能性を表現した述語 P について、「任意の式 A について、T$\vdash A$ と $P([A])$ が同値である」ことを、有限的に知ることができなければならないのはなぜなのか、皆目わからないということである。特に我々は今、有限主義的プログラムとしてのヒルベルト・プログラムを評価する立場に立っているのであって、今実際にヒルベルト・プログラムを実行しているわけではない。とすれば、我々は有限主義的でない認識手段を自由自在に使っていいはずである。なのになぜ、「任意の式 A について、T$\vdash A$ と $P([A])$ が同値である」ことが、有限的に知られなければならないのだろうか。もちろん、P が証明可能性を表現していることを知るためにはまず、「任意の式 A について、T$\vdash A$ と $P([A])$ が同値である」ことを知らなければならない。だからもし、「任意の式 A について、T$\vdash A$ と $P([A])$ が同値である」ことが、有限的に知られ得ないとしたら、有限主義者は、P が証明可能性を表現している述語であることを知ることができないだろう。だが、ヒルベルト・プログラムの実行にとって、証明可能性を形式化することは本質的な要素ではない。従って、もし $RPr_T(x)$ が証明可能性を表現する述語だったとすると、有限主義者はそれがわからないわけだが、それはヒルベルト・プログラムの進行になんの困難ももたらさない。

もうそろそろ読者もうんざりしてきたかと思うが、とにかく、$RConT$ のような例を排除するような基準（$RConT$ を排除するだけではダメであり、G2+ を満たさない文全部を一挙に倒してくれるような基準が必要であることにも注意）を提出し、それをきちんと擁護するのは、見た目ほど簡単ではない。なので、ここには困難がある。そしてこの困難は、議論を続けようとすればいくらでも議論を続けることのできる泥沼である[*9]。しかし、きちんとした議論ではなく、常識的な感覚のレベルで言えば、無矛盾性を形式化した式として $ConT$ を採用するのがもっとも自然だろう。というのも、すでに見てきたように、$ConT$ は、証明とはなにか、証明可能であるとはどういうことか、無矛盾であるとはどういうことかについての、我々のメタ数学的定義に、いわば「沿って」作られている式だからである。これに対して、ロッサー証明可能性は、与えられた証明図のゲーデル数よりも小さいゲーデル数について何事かをチェックするという、余計なステップを踏んで定義されている。従って、$RConT$ も、こうした余計なステップをふんだ定義になっている。$ConT$ 以外の式はすべて、このような妙で余計なステップを含めて定義しなければ、G2+ の基準を逃れることができないことが予想される。従って、次のような、常識的な

[*9] たとえば、[2][4][11] を参照せよ。ちなみに私は、こういう議論に意味が無いと言いたいわけではなく、真面目に論じようとすると非常に骨が折れるということを言いたいだけである。

感覚に基づく、議論もどきを提案することができる。

- メタ数学的概念を表現する式は、その概念のメタ数学的定義に、「沿って」形成されている必要がある。(「沿って」の基準)
- 無矛盾性に対する定義に「沿って」作られているのは、$ConT$ だけであり、$ConT$ は G2+ の基準を満たす。
- 従って、無矛盾性を表現している式は、G2+ の基準を満たす。

これが議論もどきでしかないのは、(「沿って」の基準)に登場する、「沿って」という概念をどう理解したらいいのか曖昧であることと、なぜ(「沿って」の基準)を採用せねばならないかの理由が明確にはわからないことによる。しかし、繰り返しになるが、常識的なレベルで言えば、この議論もどきは十分な説得力があるだろう(但し、「沿って」の基準を受け入れてもなお、まだこの議論もどきの二ステップ目にはまだ抵抗する可能性がある。だが、本文でこれ以上細かい話をするとあまりにまとまりが悪くなるので、この点の検討は注に回す[*10])。そういうわけで、常識的な感覚に基づく形でではあるが、G2 ベースの議論は、PRA を含み、かつ有限的数学を含んでいるような理念的数学の体系に対し、ヒルベルト・プログラムを実行することが不可能であることを示しており、これはヒルベルト・プログラムにとってある程度の打撃であると言うことができる。

2.6 まとめ

以上で、冒頭に述べた目標を達成した。つまり、不完全性ベースの議論の代表的な三つのタイプを紹介し、それぞれの議論構造を明確化するとともに、ヒルベルト・プログラム

[*10] (「沿って」の基準)を受け入れてもなお、ConT を表す式が G2+ を満たさなくて良い可能性がある。それは、証明及び証明可能性というメタ数学的概念の定義の仕方自体を変更するという道である。例えば、通常の仕方で証明・証明可能性を定義された理論 T があることを前提して、次のように T' の証明と証明可能性を定義する。

- T の証明に対して適当に自然数を振り分ける。これを証明の「順序」と呼ぶ。
- 式の列 α が T' における A の証明であるのは、α が T における A の証明であり、かつ、α より順序が小さい任意の証明 β について、β が T における $\neg A$ の証明でない時である。
- 式 A が T' で証明できるのは、T' における A の証明が存在するときである。

このように証明と証明可能性を定義された理論を一般にロッサー理論という。T' の証明や証明可能性の定義に「沿った」証明可能性述語、及びそれから作られる無矛盾性の式は、$RConT$ になる。従って、(「沿って」の基準)に従うと、T' の無矛盾性を表現した式は $RConT$ であるが、しかし、T が無矛盾なら、T'$\vdash RConT$ となる。つまり、$RConT$ は G2+ の基準を逃れている。[3] は、この路線でヒルベルト・プログラムを擁護しようとしている。

従って、ロッサー理論は G2 ベースの議論を逃れていると言えるだろう。だが、この場合の問題は、そもそもロッサー理論はヒルベルト・プログラムの実行対象として適切かどうかという点にある。というのも、ロッサー理論においてある記号列が A の証明であることを確かめるには、その記号列より順序が小さいすべての証明を構成し、それが $\neg A$ の証明になっていないことをいちいち確かめなければならない。これは有限的なステップではあるが、しかし、非常に煩雑なステップである。従って、ロッサー理論において命題を証明するのは極めて困難を伴い、有限的数学の補助のための道具としてみなすにはあまりに効率が悪い。なので、ロッサー理論にヒルベルト・プログラムを実行するのは可能であるが、しかし、意味が無い。

ただし、以上の再反論は、ロッサー理論の個別的特徴に本質的に依存している。従って、1) 通常とは異なる証明・証明可能性の定義を持つ理論であり、2) その定義にそって作られた無矛盾性を表現する式が G2+ の基準を逃れており、かつ、3) 有限的数学を補助する道具として十分な効率性を持つ、ような理論があれば、G2+ を逃れながら、かつ、ヒルベルト・プログラムを実行する意義を保持し続けることができるかもしれない。このような可能性が閉ざされたわけではない。だが、ちょっと無さそうだなとは思える。

に対する批判としての力を評価した。

結論だけもういちど繰り返しておくならば、まず、一つ目の、第一不完全性定理に基づく議論は、ヒルベルト・プログラムに対する批判としては的を外している。二つ目の、第一不完全性定理に基づく議論は、殆ど疑いを容れないような前提に基づいている上、かなり大きな範囲の形式体系について、ヒルベルト・プログラムの実行不可能性を言うことができそうである。三つ目の、第二不完全性定理に基づく議論は、おそらく、二つ目の議論以上に広い適用範囲を持ちそうではあるが、しかし、メタ数学的概念の適切な形式化に関する極めて困難な問題を孕んでおり、正確な評価は困難である。だが、常識的には妥当であると言えるだろう。

結局のところ、不完全性定理が、ヒルベルト・プログラムが普通目標とするような形式体系に対して、ヒルベルト・プログラムを実際に実行する可能性を、絶望的にした、ということについては、特に二つ目の議論によって、十分な説得力をもって主張できると言っていい。従って、ヒルベルト・プログラムが大きな打撃を受けた、という結論自体は疑いを容れない。だが、通常ヒルベルト・プログラムに対して浴びせられる批判（三つ目の議論）は、一見した論理構造のシンプルさに反して、決定的なアーギュメントを立てることが難しい。そして、その困難さの検討は、メタ数学的概念の形式化における複数の選択肢の性質を調べ比較するという、哲学的にも数学的にも興味深い問題と結びついている。従ってここには、まだまだ議論するべき余地も意義も残っていると言えるだろう。

2.7　文献紹介

ここまで読んだだけでこのトピックの泥沼感が伝わったと思うが、この泥沼でもう少し遊んでみたいという読者には、参考文献に挙げておいた、デトレフセンの一連の論文を勧める。デトレフセンは一貫して、ゲーデルの不完全性定理を前提してもヒルベルト・プログラムが実行可能であることを主張しており、その立場から、今回取り上げた主張について、私よりも遥かに細かな精度で検討し、批判している。彼のヒルベルト・プログラム解釈は非常に独特であり、目の覚めるような洞察を含んでいる部分と、極めてエキセントリックな部分の双方を含んでいるが、いずれにしても愉快なことは確かだ。

不完全性定理との関連に主眼をおいた文献ではないが、もっとスタンダードなヒルベルト・プログラムの理解について知りたい読者には、ザックの論文 [16][17] がよい。ヒルベルト・プログラムの歴史的に正確な理解を学ぶことができる。逆に、ヒルベルト・プログラムに拘らず、より広い文脈から不完全性定理を解説した文献として、[8] は必読である。

本文中では、いわゆる「修正されたヒルベルト・プログラム」——不完全性ベースの議論の正しさを認めた上でなお、ヒルベルト・プログラムに近い基礎論的プログラムを実行しようとする研究——、については言及しなかった。この動きについては、[7] や [15] のような古典的な証明論の教科書とともに、The Journal of Symbolic Logic の Vol.53, No.2 に掲載されたシンプソン [12] とフェファマン [6] の論文を見るとよい。シンプソンはヒルベルト・プログラムの部分的実現としての逆数学を論じており、フェファマンは伝

統的な還元的証明論の結果をサーヴェイしている。

参考文献

[1] Detlefsen, M. 1979, On Interpreting Gödel's Second Theorem, *Journal of Philosophical Logic* 8(1):297-313

[2] Detlefsen, M. 1986, *Hilbert's Program*, Dordrecht.

[3] Detlefsen, M. 1990, On an Alleged Refutation of Hilbert's Program Using Gödel's First Incompleteness Theorem, *Journal of Philosophical Logic*, 19(4):343-377

[4] Detlefsen, M. 2001, What Does Gödel's Second Theorem Say, *Philosophia Mathematica*, 9(1):37-71

[5] Feferman, S. 1962, Transfinite Recursive Progressions of Axiomatic Theories, *The Journal of Symbolic Logic*, 27(3):259-316

[6] Feferman, S. 1988, Hilbert's Program Relativized, *The Journal of Symbolic Logic*, 55(2):364-384

[7] Girard, J-Y. *Proof Theory and Logical Complexity*, Bibliopolis.

[8] フランセーン, T. 2011,『ゲーデルの定理　利用と誤用の不完全ガイド』田中一之訳, みすず書房.

[9] 飯田隆. 2005,『論理の哲学』講談社.

[10] 倉橋大志. 2014, Rosser 可証性述語について, 科学基礎論研究, 41(2):13-21

[11] Ryota, A. 2009, On a Relationship between Gödel's Second Incompleteness Theorem and Hilbert's Program, *Annals of the Japan Association for Philosophy of Science*, 17:13-29

[12] Simpson, S. 1988, Partial Realizations of Hilbert's Program, *The Journal of Symbolic Logic*, 55(2):349-363

[13] Smorynski, C. 1977, The Incompleteness Theorems, in *Handbook of Mathematical Logic*, (ed. Barwise and Keisler), North-Holland.

[14] シャピロ, S. 2001,『数学を哲学する』筑摩書房.

[15] 竹内外史・八杉満利子. 2010,『復刊　証明論入門』共立出版.

[16] Zach, R. 2001, Hilbert's Finitism: Historical, Philosophical, and Metamathematical Perspectives, PhD thesis, University of California.

[17] Zach, R. 2006, Hilbert's Program Then and Now, in *Philosophy of Logic*, (ed. Jacquette), Elsevier.

第 3 章

Grothendieck 位相・サイト上の層・層化関手に関するノート

古賀 実

このノートは，Grothendieck 位相の入った圏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 [1] の第 III 章 2 節 Grothendieck Topologies，4 節 Sheaves on a Site と 5 節 The Associated Sheaf Functor の定義と定理を述べ，証明の行間を淡々と埋めた物です．これらの概念の，具体例を交えたわかりやすい解説などといった，過度な期待はしないで下さい．特に，第 III 章 1 節 Generalized Neighborhoods や 3 節 The Zariski Site では Grothendieck 位相が導入された動機，代数幾何との関連が紹介されており，2, 4, 5 節でも折々具体例が紹介されていますが，これらはこのノートでは省略されています．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 [2] を想定しています．

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~~元々ただの忘備録だったものを冬コミ原稿として提出したから~~です．

3.1 Grothendieck Topologies

Let $\mathbf{C}$ be a small category [*1]. We shall denote the Yoneda embedding by $\mathbf{y} : \mathbf{C} \to \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Recall that a sieve S on $C \in \mathbf{C}$ is a collection of morphisms with codomain

[*1] In this paper, we assume that there is a universe U in which we can perform usual set theoretic operations and U itself is a set. We shall call each element of U a small set. A small category is a category such that the both collections of all objects and all morphisms are small sets. We shall denote by **Sets** the category of small sets whose objects are all small sets and morphisms are all maps between small sets. See [2] for details.

C such that for all $f : D \to C$ in S and all $g : E \to D$ in $\mathbf{C}$ [*2], $fg \in S$. Equivalently, S is a sieve on C iff S is a subfunctor of $\mathbf{y}(C)$.

Let S be a sieve on $C \in \mathbf{C}$ and $f : D \to C$. Then $f^*(S) := \{h | \mathrm{cod}(h) = D, fh \in S\}$ [*3] is a sieve on D.

Definition 3.1.1 (Grothendieck topologies) A *Grothendieck topology* on a small category $\mathbf{C}$ is a mapping J which assigns to each object C in $\mathbf{C}$ a collection $J(C)$ of sieves on C such that

(i) the maximal sieve $t_C = \{f \mid \mathrm{cod}(f) = C\}$ on C is an element of $J(C)$;
(ii) (stability axiom) If $S \in J(C)$ and $f : D \to C$ in $\mathbf{C}$, then $f^*(S) \in J(D)$;
(iii) (transitivity axiom) If $S \in J(C)$ and R is a sieve on C such that $f^*(R) \in J(D)$ for all $f : D \to C$ in S, then $R \in J(C)$. ◇

Definition 3.1.2 (sites) We shall call a pair $(\mathbf{C}, J)$ of a small category $\mathbf{C}$ and a Grothendieck topology J on $\mathbf{C}$ a *site*. ◇

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

Fact 3.1.1 *Let $S \in J(C)$ and R a sieve on C such that $S \subseteq R$. Then $R \in J(C)$.* □

Proof By the transitivity axiom of J, it is sufficient to show that for all $f : D \to C \in S$, $f^*(R) \in J(D)$. Note that for a sieve S on C, the condition that $\mathrm{id}_C \in S$ is equivalent to $S = t_C$. Let $f : D \to C \in S$. Since $\mathrm{cod}(\mathrm{id}_D) = D$, $f = f\mathrm{id}_D \in S$, so $\mathrm{id}_D \in f^*(S)$. Hence, $f^*(S) = t_D \in J(D)$. It is easy to show that $S \subseteq R$ implies $f^*(S) \subseteq f^*(R)$. By the maximality of $f^*(S)$, $f^*(R) = f^*(S) = t_D \in J(D)$. The proof is complete. ■

Fact 3.1.2 (iii′) *If $S \in J(C)$ such that for all $f : D_f \to C$ in S, there exists $R_f \in J(D_f)$, then $\{fg \mid f \in S,\ g \in R_f\} \in J(C)$.* □

Proof Let $T := \{fg | f \in S,\ g \in R_f\}$. Then T is a sieve on C and $R_f \subseteq f^*(T) (f \in S)$. Since $R_f \in J(D_f)$, by Fact 3.1.1, $f^*(T) \in J(D_f)$ $(f \in S)$. By the transitivity axiom of J, $T \in J(C)$. The proof is complete. ■

Example 3.1.1 Let X be a topological space equipped with a topology $\mathcal{O}(X)$. A mapping $J : \mathcal{O}(X) \ni U \mapsto J(U)$(a collection of sieves on U) defined for a sieve S on $U \in \mathcal{O}(X)$ by

$$S \in J(U) \overset{\mathrm{def}}{\Longleftrightarrow} U \subseteq \bigcup S \left(= \bigcup_{V \in S} V\right) \tag{3.1.1}$$

is a Grothendieck topology on $\mathcal{O}(X)$ [*4]. We shall call this Grothendieck topology *open cover topology*. ◇

[*2] Hereafter, we shall omit "in $\mathbf{C}$" if the category under consideration is obvious.
[*3] Hereafter, we do not write the composability condition like $\mathrm{cod}(h) = D$ explicitly, that is, if we write fh, then we assume $\mathrm{cod}(h) = \mathrm{dom}(f)$.
[*4] For a poset, seen as a category, we can identify morphisms with its domains.

Let S be a sieve on C. We shall say that S covers C if $S \in J(C)$. Similarly, for $f : D \to C$ we shall say that S covers f if $f^*(S)$ covers D. S covers C iff S covers id_C. If $f : D \to C \in S$, then $f^*(S)$ is the maximal sieve t_D on D.

Definition 3.1.3 (Grothendieck topologies (arrow form)) An *arrow form of a Grothendieck topology* on a small category $\mathbf{C}$ is a mapping J which assigns to each object C in $\mathbf{C}$ a collection $J(C)$ of sieves on C such that

(ia) If S is a sieve on C and $f \in S$, then S covers f;
(iia) (stability axiom) If S covers $f : D \to C$, then for all $g : E \to D$, S covers fg;
(iiia) (transitivity axiom) If S covers $f : D \to C$ and R is a sieve on C such that R covers g for all g in S, then R covers f. ◇

Fact 3.1.3 *The definition of Grothendieck topologies and its arrow form are equivalent. More precisely,* (i) ⇔ (ia), (ii) ⇔ (iia) *and* (iii) ⇔ (iiia)*, where the numbers are those of Definition 3.1.1 and Definition 3.1.3.* □

Proof (i)⇒(ia) Let S be a sieve on C and $f : D \to C \in S$. Then $f^*(S)$ is the maximal sieve t_D. By (i), $f^*(S) = t_D \in J(D)$, i.e., S covers f.

(ia)⇒(i) The maximal sieve t_C on C is a sieve on C. Then $\mathrm{id}_C \in t_C$. By (ia), t_C covers C, i.e., $t_C \in J(C)$.

(ii)⇒(iia) Let S covers $f : D \to C$, i.e., $f^*(S) \in J(D)$. Then, by the stability axiom (ii), for any $g : E \to D$, $g^*(f^*(S)) = (fg)^*(S) \in J(E)$, i.e., S covers fg.

(iia)⇒(ii) Let $S \in J(C)$, i.e., S covers C. Then S covers id_C. By (iia), for any $f : D \to C$, S covers $\mathrm{id}_C f = f$, i.e., $f^*(S) \in J(D)$.

(iii)⇒(iiia) Let S covers $f : D \to C$ and R a sieve on C such that for all g in S R covers g. By the definition of $f^*(S)$, for all $h : E \to D$ in $f^*(S)$, $fh \in S$. By assumption, R covers fh, i.e., $h^*(f^*(R)) = (fh)^*(R) \in J(E)$ ($h \in f^*(S) \in J(D)$). By the transitivity axiom (iii), $f^*(R) \in J(D)$, i.e., R covers f.

(iiia)⇒(iii) Let $S \in J(C)$ and R a sieve on C such that for all $f : D \to C$ in S, $f^*(R) \in J(D)$. Then S covers id_C and for all f in S, R covers f. By (iiia), R covers id_C, i.e., $R \in J(C)$.

The proof is complete. ■

Fact 3.1.4 (iv) *Let $R, S \in J(C)$. Then $R \cap S \in J(C)$.*
(iva) *Let R and S cover f. Then $R \cap S$ covers f.* □

Proof (iv) Let $R, S \in J(C)$. Then $R \cap S$ is a sieve on C. By the stability axiom of J,

$$\forall f : D \to C \in R, \quad f^*(R \cap S) = \{g | fg \in R \cap S\} = \{g | fg \in S\} = f^*(S) \in J(D).$$

Since $R \in J(C)$, by the transitivity axiom J, $R \cap S \in J(C)$.

(iva) Let R and S cover $f : D \to C$, i.e., $f^*(R)$, $f^*(S) \in J(D)$. Then, by (iv),

$$f^*(R \cap S) = \{g \mid fg \in R \cap S\} = f^*(R) \cap f^*(S) \in J(D).$$

The proof is complete. ■

Definition 3.1.4 (bases for a Grothendieck topology) A *basis for a Grothendieck topology* on a small category $\mathbf{C}$ with pullbacks is a mapping K which assigns to each object C in $\mathbf{C}$ a collection $K(C)$ of morphisms with codomain C such that

(i′) if $f : C' \to C$ is an isomorphism, then the singleton $\{f : C' \to C\}$ is an element of $K(C)$;

(ii′) (stability axiom) If $\{f_i : C_i \to C\}_{i\in I} \in K(C)$, then for each $g : D \to C$, the pullbacks $\{\pi_i^2 : C_i \times_C D \to D\}_{i\in I}$ of f_i along g is element of $K(D)$:

$$\begin{array}{ccc} C_i \times_C D & \xrightarrow{\pi_i^2} & D \\ {\scriptstyle \pi_i^1}\downarrow & \text{p.b.} & \downarrow{\scriptstyle g} \\ C_i & \xrightarrow[f_i]{} & C; \end{array}$$

(iii′) (transitivity axiom) If $\{f_i : C_i \to C\}_{i\in I} \in K(C)$ and if for each $i \in I$, there exists $\{g_{ij} : D_{ij} \to C_i\}_{j\in I_i} \in K(C_i)$, then $\{f_i g_{ij} : D_{ij} \to C\}_{j\in I_i, i\in I} \in K(C)$. ◇

We shall also call a pair $(\mathbf{C}, K)$ of a small category $\mathbf{C}$ with pullbacks and a basis K for a Grothendieck topology a *site*.

Example 3.1.2 Let X be a topological space equipped with a topology $\mathcal{O}(X)$. A mapping $K : \mathcal{O}(X) \ni U \mapsto K(U)$(a collection of open subsets of U) defined by

$$\{U_i\}_{i\in I} \in K(U) \overset{\text{def}}{\iff} U = \bigcup_{i\in I} U_i \tag{3.1.2}$$

is a basis for the open cover topology on $\mathcal{O}(X)$. ◇

The name *basis* for a Grothendieck topology is justified in the following sense:

Fact 3.1.5 *Let K be a basis for a Grothendieck topology on $\mathbf{C}$. Then the mapping J defined for a sieve S on $C \in \mathbf{C}$ by*

$$S \in J(C) \overset{\text{def}}{\iff} \exists R \in K(C),\ R \subseteq S \tag{3.1.3}$$

is a Grothendieck topology on $\mathbf{C}$. □

Proof Let J be defined as (3.1.3). We shall show that J satisfies all the axioms of Grothendieck topologies.

(i) Since id_C is an isomorphism, by (i′) of Definition 3.1.4, $\{\mathrm{id}_C\} \in K(C)$. Since $\{\mathrm{id}_C\} \subseteq t_C$, by the definition of J, $t_C \in J(C)$.

(ii) (stability axiom) Let $S \in J(C)$ and $g : D \to C$. By the definition of J, there exists $R \in K(C)$ such that $R \subseteq S$. Let $R := \{f_i : C_i \to C\}_{i\in I}$. by the stability axiom (ii′) of Definition 3.1.4,

$$T := \{\pi_i^2 : C_i \times_C D \to D\}_{i\in I} \in K(D),$$

where π_i^2 is the pullbacks of f_i along g. By the commutativity of the pullback square, $g\pi_i^2 = f_i\pi_i^1$ for all $i \in I$. Since for all $f_i \in R$ $f_i\pi_i^1 \in R$, $g\pi_i^2 \in R$. Namely, $T \subseteq g^*(R)$. On the other hand, by $R \subseteq S$, $g^*(R) \subseteq g^*(S)$. Therefore, $K(D) \ni T \subseteq g^*(S)$. By the definition of J, $g^*(S) \in J(D)$.

(iii) (transitivity axiom) Let $S \in J(C)$ and R a sieve on C such that for all $f : D \to C$ in S, $f^*(R) \in J(D)$. Then, by the definition of J, there exists $T \in K(C)$ such that $T \subseteq S$. Let $T := \{f_i : C_i \to C\}_{i\in I}$. Since for all $i \in I, f_i \in S$, by assumption, $f_i^*(R) \in J(C_i)$, by the definition of J again, for all $i \in I$, there exists $T_i \in K(C_i)$ such that $T_i \subseteq f_i^*(R)$. Let $T_i := \{g_{ij} : D_{ij} \to C_i\}_{j\in I_i}$. By the transitivity axiom (iii′) of Definition 3.1.4,

$$\{f_i g_{ij} : D_{ij} \to C\}_{j\in I_i, i\in I} \in K(C).$$

Since for all $i \in I$ and all $j \in I_i$, $g_{ij} \in f_i^*(R)$, i.e., $f_i g_{ij} \in R$, $R \supseteq \{f_i g_{ij}\}_{i\in I, j\in I_j} \in K(C)$. Therefore, by the definition of J, $R \in J(C)$.

The proof is complete. ■

We shall say that a basis K generates J if K satisfies (3.1.3) for all $C \in \mathbf{C}$. Conversely, we have the following fact:

Fact 3.1.6 *Let J be a Grothendieck topology on $\mathbf{C}$. Then there exists a maximal basis K generating J defined by*

$$R \in K(C) \overset{\text{def}}{\Longleftrightarrow} (R) \in J(C) \quad (C \in \mathbf{C}), \tag{3.1.4}$$

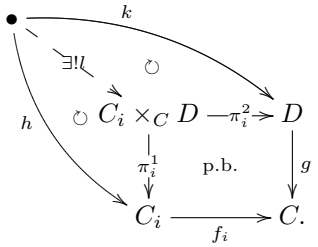
where $(R) := \{fg \mid f \in R\}$ is the sieve generated by R, i.e., the minimum sieve containing R, and the maximality of K means that if there exists another basis K' generating J, then for all $C \in \mathbf{C}$, $K'(C) \subseteq K(C)$. □

Proof First, we must verify the mapping K defined by (3.1.4) is a basis for a Grothendieck topology.

(i′) Let $f : C' \to C$ be an isomorphism. Then $(\{f\}) = t_C \in J(C)$, by the definition (i) of J. By the definition (3.1.4) of K, $\{f\} \in K(C)$.

(ii′) (stability axiom) Let $R := \{f_i : C_i \to C\}_{i\in I} \in K(C)$ and $g : D \to C$. Then, by the definition of K, $(R) \in J(C)$. To prove the stability axiom of K, i.e., $R' := \{\pi_i^2 : C_i \times_C D \to D\}_{i\in I} \in K(D)$, we shall show that $(R') \in J(D)$. Since $(R) \in J(C)$, by the stability axiom of J, $g^*((R)) = \{k \mid gk \in (R)\} \in J(D)$. We shall show that $(R') = g^*((R))$. Let $k \in g^*((R))$. Then $gk = f_i h$ for some $i \in I$ and h. By the pullback condition, there exists a unique l such that

$k = \pi_i^2 l$, $h = \pi_i^1 l$:



Since k is of the form $k = \pi_i^2 l$, $k \in (R')$. Hence, $g^*((R)) \subseteq (R')$.

Conversely, take $\pi_i^2 m \in (R')$ arbitrarily. Then, by the commutativity of the pullback square, $g\pi_i^2 m = f_i \pi_i^1 m \in (R)$. Hence, $\pi_i^2 m \in g^*((R))$. Therefore, $(R') \subseteq g^*((R))$. From the above, $(R') = g^*((R)) \in J(D)$.

(iii′) (transitivity axiom) Let $R := \{f_i : C_i \to C\}_{i\in I} \in K(C)$ such that for all $i \in I$, there exists $R_i := \{g_{ij} : D_{ij} \to C_i\}_{j\in I_i} \in K(C_i)$. Then $(R) \in J(C)$, $(R_i) \in J(C_i)$. To prove the transitivity axiom of K, i.e., $R' := \{f_i g_{ij} : D_{ij} \to C\}_{j\in I_i, i\in I} \in K(C)$, we shall show that $(R') \in J(C)$. Let $f_i h \in (R)$ for some h. Then $(f_i h)^*((R')) = \{l \,|\, f_i hl \in (R')\}$. Since $(R_i) \in J(C_i)$, by the stability axiom of J, $h^*((R_i)) = \{l \mid hl \in (R_i)\} \in J(\mathrm{dom}(h))$. Note that for all $l \in h^*((R_i))$, there exists $j \in I_i$ and k such that $hl = g_{ij}k$. Then $f_i hl = f_i g_{ij} k \in (R')$. Hence, $l \in (f_i h)^*((R'))$. Therefore, $h^*((R_i)) \subseteq (f_i h)^*((R'))$. Since $h^*((R_i)) \in J(\mathrm{dom}(h))$, $h^*((R_i)) \subseteq (f_i h)^*((R'))$ implies $(f_i h)^*((R')) \in J(\mathrm{dom}(h))$. Since $f_i h$ is an arbitrary element of $(R) \in J(C)$, by the transitivity axiom of J, $(R') \in J(C)$.

From the above, K is a basis for J. Next, we shall show that K generates J. Let $S \in J(C)$. Then, since S is a sieve, $(S) = S \in J(C)$. By the definition of K, $S \in K(C)$.

Conversely, let S be a sieve on C. Then if there exists $R \in K(C)$ such that $R \subseteq S$, then $(R) \subseteq S$. Since $(R) \in J(C)$, $(R) \subseteq S$ implies $S \in J(C)$.

Finally, we shall show the maximality of K. To this end, suppose that there exists another basis K' which generates J. Let $R \in K'(C)$. Then, since $R \subseteq (R)$ and by (3.1.3), $(R) \in J(C)$. This implies $R \in K(C)$. The proof is complete. ■

Definition 3.1.5 (refinements) We shall say that $\{f_i : C_i \to C\}_{i\in I}$ refines $\{g_j : D_j \to C\}_{j\in I'}$ if for all $i \in I$, there exists $j \in I'$ and $h_{ij} : C_i \to D_j$ such that $f_i = g_j h_{ij}$. ◇

Fact 3.1.7 *For all $P, T \in K(C)$, there exists $R \in K(C)$ such that R refines P and T.* □

Proof Let J be the Grothendieck topology generated by K. Then, since $P \subseteq (P)$, $T \subseteq (T)$, $(P), (T) \in J(C)$. By (iv) of Fact 3.1.4, $(P) \cap (T) \in J(C)$. By the definition of J, there exists $R \in K(C)$ such that $R \subseteq (P) \cap (T)$. In particular, $R \subseteq (P) = \{fg \,|\, f \in P, \}$. Hence, for all $r \in R$, there exists $f_r \in P$ and g_r such that $r = f_r g_r$. This implies

R refines P. Similarly, since $R \subseteq (T)$, R refines T. The proof is complete. ■

Example 3.1.3 (Grothendieck topologies) (trivial topology) Let $\mathbf{C}$ be a small category. A mapping J defined by

$$J(C) = \{t_C\} \quad (C \in \mathbf{C})$$

is a Grothendieck topology on $\mathbf{C}$ and is called the *trivial topology*.

(sup topology) Let $\mathbf{H}$ be a complete Heyting algebra. A mapping defined by

$$\{a_i\}_{i\in I} \in K(c) \overset{\text{def}}{\iff} \bigvee_{i\in I} a_i = c \quad (c \in \mathbf{H}) \tag{3.1.5}$$

is a basis for a Grothendieck topology. The Grothendieck topology generated by K is called the *sup topology*. In particular, if $\mathbf{H}$ is a topology $\mathcal{O}(X)$ for a topological space X, then the sup topology coincides with the open cover topology on $\mathcal{O}(X)$.

(dense topology) Let $\mathbf{P}$ be a poset and $p \in \mathbf{P}$. We shall call a subset $D \subseteq \mathbf{P}$ *dense below* p if

$$\forall r \leq p,\ \exists q \in D, \quad q \leq r. \tag{3.1.6}$$

A mapping J on $\mathbf{P}$ defined by

$$J(p) := \{D \mid D \text{ is a sieve on } p \text{ such that dense below } p\} \quad (p \in \mathbf{P}) \tag{3.1.7}$$

is a Grothendieck topology on $\mathbf{C}$ and is called the *dense topology*.

(atomic topology) Let $\mathbf{C}$ be a small category such that for all $f : D \to C$ and all $g : E \to C$, there exists $h : F \to D$ and $k : F \to E$ such that $fh = gk$:

$$\begin{array}{ccc} F & \overset{\exists k}{\dashrightarrow} & E \\ {\scriptstyle \exists h}\downarrow & \circlearrowright & \downarrow{\scriptstyle \forall g} \\ D & \underset{\forall f}{\longrightarrow} & C. \end{array}$$

Then a mapping J defined by

$$S \in J(C) \overset{\text{def}}{\iff} S \text{ is a non-empty sieve on } C \quad (C \in \mathbf{C}) \tag{3.1.8}$$

is a Grothendieck topology on $\mathbf{C}$ and is called the *atomic topology*. ◇

3.2 Sheaves on a Site

Let $(\mathbf{C}, J)$ be a site, P a presheaf on $\mathbf{C}$ and $S \in J(C)$ $(C \in \mathbf{C})$.

Definition 3.2.1 (matching families) A *matching family* for S (of elements) of P is a mapping

$$S \ni (f : D \to C) \mapsto x_f \in PD$$

such that

$$\forall f : D \to C \in S,\ \forall g : E \to D, \quad (Pg)(x_f) = x_{fg}. \tag{3.2.1}$$

We shall also call a family $\{x_f\}_{f\in S}$ satisfying (3.2.1) a matching family for S.

Definition 3.2.2 (amalgamations) An *amalgamation* of a matching family $\{x_f\}_{f\in S}$ for $S \in J(C)$ is an element $x \in PC$ such that

$$\forall f \in S, \quad (Pf)(x) = x_f. \tag{3.2.2}$$

Definition 3.2.3 (sheaves on a site) Let P be a presheaf on $\mathbf{C}$. Then we shall call P a *sheaf* on $(\mathbf{C}, J)$ if every matching family for any $S \in J(C)$ $(C \in \mathbf{C})$ has a unique amalgamation. ◇

Fact 3.2.1 *Matching families $\{x_f\}_{f\in S}$ are described by natural transformations from S to P, where a sieve S is identified with a subfunctor of $\mathbf{y}(C) = \mathrm{Hom}_{\mathbf{C}}(-, C)$.* □

Remark 3.2.1 The definition of sheaves can be formulated diagrammatically as follows: a presheaf P is a sheaf on $(\mathbf{C}, J)$ iff for all $C \in \mathbf{C}$ and all $S \in J(C)$,

$$PC \xrightarrow{e} \prod_{f\in S} P(\mathrm{dom}(f)) \underset{a}{\overset{p}{\rightrightarrows}} \prod_{fg\in S} P(\mathrm{dom}(g)) \tag{3.2.3}$$

is an equalizer diagram, where $e(x) := \{(Pf)(x)\}_{f\in S} (x \in PC)$, $p(\{x_f\}_{f\in S}) := \{x_{fg}\}_{(f,g)}$ and $a(\{x_f\}_{f\in S}) := \{(Pg)(x_f)\}_{(f,g)}$ $(\{x_f\}_{f\in S} \in \prod_{f\in S} P(\mathrm{dom}(f)))$.

We shall say that P satisfies the sheaf condition with respect to $S \in J(C)$ $(C \in \mathbf{C})$ if P satisfies (3.2.3) for S. ◇

Let K be a basis for a Grothendieck topology on $\mathbf{C}$ with pullbacks, $R := \{f_i\}_{i\in I} \in K(C)$ and $\{x_i\}_{i\in I} \in \prod_{i\in I} PC_i$.

Definition 3.2.4 (matching families for a basis) We shall call $\{x_i\}_{i\in I}$ a matching family for R if

$$\forall i, \forall j \in I, \quad (P\pi^1_{ij})(x_i) = (P\pi^2_{ij})(x_j), \tag{3.2.4}$$

where π^1_{ij} and π^2_{ij} are the pullback of f_j along f_i and the pullback of f_i along f_j, respectively. ◇

Definition 3.2.5 (amalgamations for a basis) We shall call $x \in PC$ an amalgamation of a matching family $\{x_i\}_{i\in I}$ for R if

$$\forall i \in I, \quad (Pf_i)(x) = x_i. \tag{3.2.5}$$

Fact 3.2.2 *Let P be a presheaf on $\mathbf{C}$ with pullbacks, K a basis for a Grothendieck topology on $\mathbf{C}$ and J the Grothendieck topology generated by K. Then the following conditions are equivalent:*

(i) *P is a sheaf on $(\mathbf{C}, J)$;*
(ii) *For all $C \in \mathbf{C}$ and all $R := \{f_i : C_i \to C\}_{i\in I} \in K(C)$, all matching families of P for R have a unique amalgamation;*

(iii) *For all* $C \in \mathbf{C}$ *and all* $\{f_i : C_i \to C\}_{i\in I} \in K(C)$,

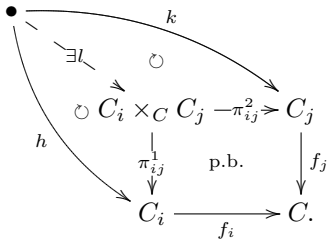
$$PC \xrightarrow{e} \prod_{i\in I} PC_i \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{(i,j)\in I\times I} P(C_i \times_C C_j) \tag{3.2.6}$$

is an equalizer diagram, where $e(x) := \{(Pf_i)(x)\}_{i\in I} (x \in PC)$, $p_1(\{x_i\}_{i\in I}) := \{(P\pi^1_{ij}(x))\}_{(i,j)}$ *and* $p_2(\{x_i\}_{i\in I}) := \{(P\pi^2_{ij})(x_j)\}_{(i,j)}$ $(\{x_i\}_{i\in I} \in \prod_{i\in I} PC_i)$. □

Proof The conditions (ii) and (iii) are just rephrasing of each other.

(i) ⇒ (ii) Suppose P is a sheaf on $(\mathbf{C}, J)$. Let $R = \{f_i : C_i \to C\}_{i\in I} \in K(C)$ and $\{x_i\}_{i\in I}$ a matching family for R. Consider the sieve $S := (R) = \{f_i k \mid f_i \in R\}$. Define $\{y_g\}_{g\in S}$ by $y_g := (Pk)(x_i)$ if g is represented as $g = f_i k$ for some $i \in I$ and k. The definition does not depend on a particular representation of g. To show this, let $g = f_i h = f_j k$ $(i, j \in I)$ for some $i, j \in I$, h and k. By the pullback condition, there exists l such that

$$h = \pi^1_{ij} l, \quad k = \pi^2_{ij} l :$$



Since $\{x_i\}_{i\in I}$ is a matching family of R, $(P\pi^1_{ij})(x_i) = (P\pi^2_{ij})(x_j)$. Therefore,

$$(Ph)(x_i) = (P(\pi^1_{ij} l))(x_i) = (Pl)((P\pi^1_{ij})(x_i)) = (Pl)((P\pi^2_{ij})(x_j)) = (Pk)(x_j).$$

Next, we shall show that $\{y_g\}_{g\in S}$ is a matching family for S. Let $g = f_i k$ for some $i \in I$ and k. Then

$$(Ph)(y_g) = (Ph)((Pk)(x_i)) = (P(kh))(x_i).$$

Since $gh = f_i kh$, by the definition of y_{gh},

$$y_{gh} = P(kh)(x_i).$$

Since P is a sheaf on $(\mathbf{C}, J)$,

$$\exists! y \in PC,\ \forall g \in S, \quad (Pg)(y) = y_g.$$

In particular, since $R \ni f_i = f_i \mathrm{id}_{C_i}$ $(i \in I)$, for all $i \in I$,

$$(Pf_i)(y) = y_{f_i} = (P\mathrm{id}_{C_i})(x_i) = x_i.$$

Therefore, y is an amalgamation of $\{x_i\}_{i\in I}$.

Next, we shall show that $\{x_i\}_{i\in I}$ have a unique amalgamation. Let $y' \in PC$ be another amalgamation of $\{x_i\}_{i\in I}$. Then we have

$$(Pg)(y') = (P(f_i h))(y') = (Ph)((Pf_i)(y')) = (Ph)(x_i) = y_g.$$

Thus, y' is also an amalgamation of $\{y_g\}_{g\in S}$. Since P is a sheaf on $(\mathbf{C}, J)$, the matching family $\{y_g\}_{g\in S}$ have a unique amalgamation. Hence, we have $y = y'$. Therefore, $\{x_i\}_{i\in I}$ has a unique amalgamation.

(ii) $\Rightarrow$ (i) Suppose that $S \in J(C)$ $(C \in \mathbf{C})$, i.e., there exists $R \in K(C)$ such that $R \subseteq S$ and let $R := \{f_i : C_i \to C\}_{i\in I}$. Let $\{y_g\}_{g\in S}$ be a matching family for S. Then we must show that there exists a unique $y \in PC$ such that for all $g \in S$, $(Pg)(y) = y_g$. Firstly, we shall show that $\{y_f\}_{f\in R}$ is a matching family for R, i.e.,

$$\forall f_i, \forall f_j \in R, \quad (P\pi^1_{ij})(y_{f_i}) = (P\pi^2_{ij})(y_{f_j}).$$

Since $\{y_g\}_{g\in S}$ is a matching family for S, in particular, for all $f_i : C_i \to C \in R \subseteq S$ and all $g : D \to C_i$, $(Pg)(y_{f_i}) = y_{f_i g}$. By the commutativity of the pullback square, $f_i\pi^1_{ij} = f_j\pi^2_{ij}$. Taking g as π^1_{ij} for f_i and π^2_{ij} for f_j, respectively, $(P\pi^1_{ij})(y_{f_i}) = y_{f_i\pi^1_{ij}} = y_{f_j\pi^2_{ij}} = (P\pi^2_{ij})(f_j)$. Therefore, $\{y_{f_i}\}_{i\in I}$ is a matching family for R. By assumption, there exists a unique $y \in PC$ such that for all $f_i \in R$, $(Pf_i)(y) = y_{f_i}$. It is sufficient to show that

$$\forall g \in S, \quad (Pg)(y) = y_g.$$

Let $g \in S$. Then, for all $f_i \in R$,

$$\begin{aligned}
&(P\pi^2_{f_i g})((Pg)(y)) \\
&= (P(g\pi^2_{f_i g}))(y) \\
&= (P(f_i\pi^1_{f_i g}))(y) \qquad (\because f_i\pi^1_{f_i g} = g\pi^2_{f_i g}) \\
&= (P\pi^1_{f_i g})((Pf_i)(y)) \\
&= (P\pi^1_{f_i g})(y_f) \\
&= y_{f\pi^1_{f_i g}} \qquad (\because \{y_{f_i}\}_{i\in I} \text{ is a matching family for } R) \\
&= y_{g\pi^2_{f_i g}} \qquad (\because f_i\pi^1_{f_i g} = g\pi^2_{f_i g}) \\
&= (P\pi^2_{f_i g})(y_g) \qquad (\because \{y_{f_i}\}_{i\in I} \text{ is a matching family for } R)\ . \qquad (3.2.7)
\end{aligned}$$

On the other hand, by the stability axiom of the basis K,

$$R' := \{\pi^2_{f_i g} : C_i \times_C D \to D\}_{i\in I} \in K(D).$$

Since a functor P satisfies the associative law, $\{(P\pi^2_{f_i g})(y_g)\}_{i\in I}$ is a matching family for R'. By assumption, $\{(P\pi^2_{f_i g})(y_g)\}_{i\in I}$ has a unique amalgamation. On the other hand, (3.2.7) shows that both $(Pg)(y)$ and y_g are amalgamations of $\{(P\pi^2_{f_i g})(y_g)\}_{i\in I}$. By uniqueness, $(Pg)(y) = y_g$ $(g \in S)$. The proof is complete. ■

Let $\mathbf{C}$ be a small category such that for all $f : D \to C$ and all $g : E \to C$, there exists $h : F \to D$ and $k : F \to E$ such that $fh = gk$:

$$\begin{array}{ccc}
F & \overset{\exists k}{\dashrightarrow} & E \\
{\scriptstyle \exists h}\,\vdots & \circlearrowright & \downarrow{\scriptstyle \forall g} \\
D & \xrightarrow[\forall f]{} & C.
\end{array}$$

Then there exists the atomic topology J on $\mathbf{C}$, i.e.,

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

Fact 3.2.3 *Let P be a presheaf on $\mathbf{C}$. Then the following two conditions are equivalent:*

(i) *P is a sheaf on the site $(\mathbf{C}, J)$;*

(ii) *For any $f : D \to C$ and any $y \in PD$, if $(Pg)(y) = (Ph)(y)$ for all g and h with $fg = fh$, then there exists a unique $x \in PC$ such that $(Pf)(x) = y$.* □

Proof (i) ⇒ (ii) Suppose $f : D \to C$ and $y \in PD$ satisfies for all $g, h : E \to D$ with $fg = fh$, $(Pg)(y) = (Ph)(y)$. Consider the sieve $S := (f) = \{fk\}_k =: \{t\}_{t\in S}$ generated by $\{f\}$. Define $\{x_t\}_{t\in S}$ by

$$x_t := (Pk)(y) \qquad (t = fk \text{ for some } k).$$

Then x_t does not depend on a particular representation of t and $\{x_t\}_{t\in S}$ is a matching family for S. Since P is a sheaf on $(\mathbf{C}, J)$,

$$\exists! x \in PC, \quad \forall t \in S, \quad (Pt)(x) = x_t.$$

In particular, $(Pf)(x) = x_f = (P\mathrm{id}_D)(y) = y$. Let $x' \in PC$ such that $(Pf)(x') = y$. Then for all $t \in S$ with $t = fk_t$ for some k_t,

$$(Pt)(x') = (P(fk_t))(x') = (Pk)((Pf)(x')) = (Pk)(y) = x_t.$$

Therefore, x' is also an amalgamation of $\{x_t\}_{t\in S}$. Since P is a sheaf, $x = x'$.

(ii) ⇒ (i) Let $S \in J(C)$, i.e., S is a non-empty sieve on C and $\{x_f\}_{f\in S}$ be a matching family for S. We shall show that there exits a unique amalgamation of $\{x_f\}_{f\in S}$. Since $S \neq \emptyset$, we can chose $f_0 : B \to C \in S$. Since $\{x_f\}_{f\in S}$ is a matching family, for all $g, h : E \to D$ with $fg = fh$, $(Pg)(x_{f_0}) = (Ph)(x_{f_0})$. By assumption, there exists a unique $x \in PC$ such that $(Pf_0)(x) = x_{f_0}$. It is sufficient to show that for all $f \in S, (Pf)(x) = x_f$. Take $f : A \to C \in S$. By assumption, there exists $u : D \to A$ and $v : D \to B$ such that $fu = f_0 v$. Let $y := (Pv)(x_{f_0}) = (Pv)((Pf_0)(x)) = (P(f_0 v)(x)) \in PD$. If $g, h : E \to D$ such that $ug = uh$, then $f_0 vg = fug = fuh = f_0 vh$:

$$\begin{array}{ccccc} E & \underset{h}{\overset{g}{\rightrightarrows}} & D & \xrightarrow{v} & B \\ & & {\scriptstyle u}\downarrow & \circlearrowright & \downarrow{\scriptstyle f_0} \\ & & A & \xrightarrow[f]{} & C. \end{array}$$

Hence,

$$(Pg)(y) = (P(f_0 vg)(x)) = (P(f_0 vh)(x)) = (Ph)(y).$$

By assumption, there exists a unique $z \in PA$ such that

$$(Pu)(z) = y = (P(f_0 v)(x)) = (P(fu)(x)) = (Pu)((Pf)(x)).$$

By uniqueness, $z = (Pf)(x)$. On the other hand, since $\{x_f\}_{f\in S}$ is a matching family for S, $(Pu)(x_f) = x_{fu} = ((Pfu)(x)) = y$. Therefore, $z = x_f$ and we obtain $(Pf)(x) = x_f$ $(f \in S)$.

The proof is complete. ■

Definition 3.2.6 Let $(\mathbf{C}, J)$ be a site. We shall denote by $\mathrm{Sh}(\mathbf{C}, J)$ the category whose objects are sheaves on $(\mathbf{C}, J)$ and morphism are natural transformations. Therefore, $\mathrm{Sh}(\mathbf{C}, J)$ is a full subcategory of the category of presheaves $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ and there exists the inclusion functor $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. ◇

Definition 3.2.7 (Grothendieck topoi) We shall call a category $\mathcal{G}$ which is equivalent to the category of sheaves on a site $(\mathbf{C}, J)$, i.e. $\mathcal{G} \cong \mathrm{Sh}(\mathbf{C}, J)$, a *Grothendieck topos*. ◇

Lemma 3.2.1 *Let $(\mathbf{C}, J)$ be a site and $I \ni i \mapsto P_i \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ a diagram of presheaves P_i $(i \in I)$. If for all $i \in I$, $P_i \in \mathrm{Sh}(\mathbf{C}, J)$, then the limit $\varprojlim_{i\in I} P_i$ in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is a sheaf on $\mathrm{Sh}(\mathbf{C}, J)$.* □

Proof Note that for $P_i \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ $(i \in I)$, the limit $\varprojlim_{i\in I} P_i$ in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ is given by pointwise:

$$(\varprojlim_{i\in I} P_i)(C) \cong (\varprojlim_{i\in I})(P_iC) \quad (C \in \mathbf{C})$$

and sheaves are obtained by equalizers as (3.2.3), in particular, limits. By the commutativity of limits [2, p. 227], the statements follows. The proof is complete. ■

3.3 The Associated Sheaf Functor

The main theorem in this section is the following theorem:

Theorem 3.3.1 *Let $(\mathbf{C}, J)$ be a site. Then the inclusion functor $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ has a left adjoint*

$$\mathbf{a} : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \to \mathrm{Sh}(\mathbf{C}, J), \tag{3.3.1}$$

i.e., $\mathbf{a} \dashv i$. Moreover, $\mathbf{a}$ preserves finite limits, i.e., $\mathbf{a}$ is left exact. □

Definition 3.3.1 (separated presheaves) Let $(\mathbf{C}, J)$ be a site and P a presheaf on $\mathbf{C}$. Then P is called a separated presheaf on $(\mathbf{C}, J)$ if for any $C \in \mathbf{C}$, any $x, y \in PC$ and any $S \in J(C)$,

$$\forall f \in S, \quad (Pf)(x) = (Pf)(y) \;\Rightarrow\; x = y. \tag{3.3.2}$$

Let P be a sheaf on $(\mathbf{C}, J)$, $S \in J(C)$ $(C \in \mathbf{C})$ and $\boldsymbol{x} = \{x_f\}_{f\in S}$ a matching family for S, then $\boldsymbol{x}$ has a unique amalgamation $x \in PC$. If $R \in J(C)$ is a refinement of S, i.e., $R \subseteq S$, then the subfamily $\{x_f\}_{f\in R}$ necessarily has the same amalgamation x. That is, we may extract a unique amalgamation by collecting such matching families.

We shall denote the set of all matching families of P for S by $\mathrm{Match}(S, P)$.

Definition 3.3.2 Let $\boldsymbol{x} = \{x_f\}_{f\in S} \in \mathrm{Match}(S,P)$ and $\boldsymbol{y} = \{y_g\}_{g\in T} \in \mathrm{Match}(T,P)$ for some $S,T \in J(C)$ ($C \in \mathbf{C}$). We define $\boldsymbol{x} \sim_C \boldsymbol{y}$ as follows:

$$\boldsymbol{x} \sim_C \boldsymbol{y} \overset{\mathrm{def}}{\Longleftrightarrow} \exists R \in J(C), \quad R \subseteq S \cap T \quad \text{and} \quad \forall r \in R,\ x_r = y_r. \tag{3.3.3}$$

Fact 3.3.1 *$\sim_C$ is an equivalence relation on $\coprod_{S\in J(C)} \mathrm{Match}(S,P)$ for each $C \in \mathbf{C}$.*□

Proof The reflexivity and symmetry may be obvious. We shall show only the transitivity here. Let $\boldsymbol{x} = \{x_f\}_{f\in S} \in \mathrm{Match}(S,P)$, $\boldsymbol{y} = \{y_g\}_{g\in T} \in \mathrm{Match}(T,P)$ and $\boldsymbol{z} = \{z_h\}_{h\in U} \in \mathrm{Match}(U,P)$ be three matching families for some $S,T,U \in J(C)$ ($C \in \mathbf{C}$) such that $\boldsymbol{x} \sim_C \boldsymbol{y}$, $\boldsymbol{y} \sim_C \boldsymbol{z}$. Then there exists $R, R' \in J(C)$ such that $R \subseteq S \cap T$, $R' \subseteq T \cap U$ and

$$\forall r \in R,\ x_r = y_R, \quad \forall r' \in R',\ y_{r'} = z_{r'}.$$

Consider $W := R \cap R'$. Then $W \in J(C)$ and for all $w \in W$, $x_w = y_w = z_w$. Therefore, $\boldsymbol{x} \sim_C \boldsymbol{z}$. The proof is complete. ■

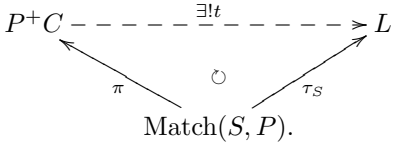
We shall denote the equivalence class with a representative matching family $\boldsymbol{x}$ by $[\boldsymbol{x}]$.

Definition 3.3.3 Let P be a presheaf on $\mathbf{C}$. Define a mapping $P^+ : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets}$ by

$$P^+C := \coprod_{S\in J(C)} \mathrm{Match}(S,P)/\sim_C . \tag{3.3.4}$$

Fact 3.3.2 *$P^+C \cong \varinjlim_{S\in J(C)} \mathrm{Match}(S,P)$, where the colimit is taken over all $S \in J(C)$ ordered by reverse inclusion, and then there exists a morphism $i_{RS} : \mathrm{Match}(S,P) \ni \{x_f\}_{f\in S} \mapsto \{x_f\}_{f\in R} \in \mathrm{Match}(R,P)$ if $R \subseteq S$.* □

Proof To prove P^+C has the universal mapping property, suppose that there exists a cocone $\{\tau_S : \mathrm{Match}(S,P) \to L\}_{S\in J(S)}$ under L such that $\tau_T = \tau_S i_{ST}$ for all $S,T \in J(C)$ with $S \subseteq T$. We must show that there exists a unique map $t : P^+C \to L$ such that $\tau_S = t\pi$ for all τ_S ($S \in J(C)$), where $\pi : \mathrm{Match}(S,P) \to P^+C$ is the quotient map for the equivalence relation $\sim_C$, as in the following diagram:



Define $t : P^+C \to L$ for $\boldsymbol{x} = \{x_f\}_{f\in S} \in \mathrm{Match}(S,P) (S \in J(C))$ by

$$t([\boldsymbol{x}]) := \tau_S(\boldsymbol{x}).$$

We must verify that the definition of t does not depend on the choice of a particular representative $\boldsymbol{x} \in \mathrm{Match}(S,P)$. To this end, let $\boldsymbol{y} = \{y_g\}_{g\in T} \in \mathrm{Match}(T,P)$ ($T \in J(C)$) such that $\boldsymbol{x} \sim_C \boldsymbol{y}$. Then there exists $R \in J(C)$ such that $R \subseteq S \cap T$ and $x_r = y_r$ for all $r \in R$. Hence, $i_{RS}(\boldsymbol{x}) = \{x_r\}_{r\in R} = \{y_r\}_{r\in R} = i_{RT}(\boldsymbol{y})$. Therefore,

$$t([\boldsymbol{y}]) = \tau_T(\boldsymbol{y}) = (\tau_R i_{RT})(\boldsymbol{y}) = \tau_R(i_{RT}(\boldsymbol{y})) = \tau_R(i_{RS}(\boldsymbol{x})) = (\tau_R i_{RS})(\boldsymbol{x}) = \tau_S(\boldsymbol{x}) = t([\boldsymbol{x}]).$$

Since $t([\boldsymbol{x}]) = (t\pi)(\boldsymbol{x})$, t satisfies the commutativity $\tau_S = t\pi$ for all τ_S. To prove the uniqueness of t, suppose that there is another mapping $t' : P^+C \to L$ such that $\tau_S = t'\pi$ for all τ_S. Then $t'([\boldsymbol{x}]) = t'\pi(\boldsymbol{x}) = \tau_S(\boldsymbol{x}) = t([\boldsymbol{x}])$ for all $\boldsymbol{x} \in \mathrm{Match}(S, P)$. Therefore, $t' = t$. The proof is complete. ■

For $h : C' \to C$, $P^+h : P^+C \to P^+C'$ is defined by

$$(P^+h)([\{x_f\}_{f\in S}]) := [\{x_{hf'}\}_{f'\in h^*(S)}] \quad (\{x_f\}_{f\in S} \in \mathrm{Match}(S, P)\ (S \in J(C))).$$

We claim that $\{x_{hf'}\}_{f'\in h^*(S)} \in \mathrm{Match}(h^*(S), P)$. Indeed, for all $f' : D' \to C' \in h^*(S)$, $hf' \in S$ and for all $g' : E' \to D'$, $(Pg')(x_{hf'}) = x_{hf'g'}$, since $\{x_f\}_{f\in S}$ is a matching family.

We claim that the definition of P^+h is well-defined. Let $h : C' \to C$, $\boldsymbol{x} = \{x_f\}_{f\in S}$ and $\boldsymbol{y} = \{y_g\}_{g\in T}$ be two matching families such that $\boldsymbol{x} \sim_C \boldsymbol{y}$, i.e., there exists $R \in J(C)$ such that $R \subseteq S \cap T$ and $x_r = y_r$ for all $r \in R$. We must show that $\{x_{hf}\}_{f'\in h^*(S)} \sim_{C'} \{y_{hg'}\}_{g'\in h^*(T)}$. Consider $h^*(R) \subseteq h^*(S) \cap h^*(T)$, by the stability axiom of J, $h^*(R) \in J(C')$. It is sufficient to show that

$$\forall r' \in h^*(R), \quad x_{hr'} = y_{hr'}.$$

Note that $h^*(R) = \{r' \mid hr' \in R\}$. Since for all $r \in R$, $x_r = y_r$ and for all $r' \in h^*(R)$, we have $x_{hr'} = y_{hr'}$. Therefore, P^+h is well-defined.

We claim that $P^+ : \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets}$ is a contravariant functor.

(i) Let $S \in J(C)$. Note that for id_C, $\mathrm{id}_C^*(S) = S$. Then

$$(P^+\mathrm{id}_C)([\{x_f\}_{f\in S}]) = [\{x_f\}_{f\in S}].$$

(ii) Let $h : C' \to C$ and $k : C'' \to C'$. Since $(hk)^*(S) = \{f' \mid hkf' \in S\}$,

$$(P^+(hk))([\{x_f\}_{f\in S}]) = [\{x_{hkf'} \mid f' \in (hk)^*(S)\}].$$

On the other hand, since $k^*(h^*(S)) = \{g \mid kg \in h^*(S)\} = \{f' \mid hkf' \in S\} = (hk)^*(S)$,

$$\begin{aligned}(P^+(k))((P^+h)([\{x_f\}_{f\in S})]) &= (P^+k)([\{x_{hf'}\}_{f'\in h^*(S)}]) \\ &= [\{x_{hkf'}\}_{f'\in k^*(h^*(S))}].\end{aligned}$$

Let P, Q be two presheaves and $\phi : P \to Q$ a natural transformation. We define a mapping $\phi^+ : P^+ \to Q^+$ for $C \in \mathbf{C}$ by

$$\begin{aligned}&\phi_C^+ : P^+C \to Q^+C \\ &\phi_C^+([\{x_f\}_{f\in S}]) := [\{\phi_{\mathrm{dom}(f)}(x_f)\}_{f\in S}] \quad (S \in J(C),\ [\{x_f\}_{f\in S}] \in P^+C). \quad (3.3.5)\end{aligned}$$

First, we must verify the well-definedness of ϕ^+. We claim that $\{\phi_{\mathrm{dom}(f)}(x_f)\}_{f\in S}$ is a matching family of Q for S. Let $f : D \to C \in S$ and $g : E \to D$. Then, since ϕ is a natural transformation and $\boldsymbol{x}$ is a matching family, we obtain

$$(Qg)(\phi_D(x_f)) = \phi_E((Pg)(x_f)) = \phi_E(x_{fg}) = \phi_{\mathrm{dom}(fg)}(x_{fg}).$$

Hence, $\{\phi_{\mathrm{dom}(f)}(x_f)\}_{f\in S}$ is a matching family of Q for S. Let $\boldsymbol{x} = \{x_f\}_{f\in S}$ and $\boldsymbol{y} = \{y_g\}_{g\in T}$ be two matching families such that $\boldsymbol{x} \sim_C \boldsymbol{y}$, i.e., there exists $R \in J(C)$ such that $R \subseteq S\cap T$ and $x_r = y_r$ for all $r \in R$. Then $\phi_{\mathrm{dom}(r)}(x_r) = \phi_{\mathrm{dom}(r)}(y_r)$. This implies that $[\{\phi_{\mathrm{dom}(f)}(x_f)\}_{f\in S}] = [\{\phi_{\mathrm{dom}(g)}(y_g)\}_{g\in T}]$. Therefore, $\phi^+ : P^+ \to Q^+$ is well-defined.

Next, we shall prove that ϕ^+ is a natural transformation. Let $\{x_f\}_{f\in S} \in \mathrm{Match}(S, P)$ $(S \in J(C))$. Then for any $h : D \to C$,

$$(Q^+h)(\phi_C^+([\{x_f\}_{f\in S}])) = (Q^+h)([\{\phi_{\mathrm{dom}(f)}(x_f)\}_{f\in S}]) = [\{\phi_{\mathrm{dom}(hf')}(x_{hf'})\}_{f'\in h^*(S)}]$$

and

$$\phi_D(P^+h([\{x_f\}_{f\in S}])) = \phi_D^+([\{x_{hf'}\}_{f'\in h^*(S)}]) = [\{\phi_{\mathrm{dom}(hf')}(x_{hf'})\}_{f'\in h^*(S)}] :$$

$$\begin{array}{ccc} P^+C & \xrightarrow{\phi_C^+} & Q^+C \\ {\scriptstyle P^+h}\downarrow & \circlearrowright & \downarrow{\scriptstyle Q^+h} \\ P^+D & \xrightarrow[\phi_D]{} & Q^+D. \end{array}$$

Hence, $(Q^+h)(\phi_C^+([\{x_f\}_{f\in S}])) = \phi_D^+(P^+h([\{x_f\}_{f\in S}]))$. Therefore, ϕ^+ is a natural transformation.

The functorial property of $\cdot^+$, i.e., $\mathrm{id}_P^+ = \mathrm{id}_{P^+}$ and $(\psi\circ\phi)^+ = \psi^+\circ\phi^+$ for composable two natural transformations ϕ and ψ may be clear by definition.

From the above, the mapping

$$+ : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \ni P \mapsto P^+ \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$$

is a functor and is called the *plus construction*.

Definition 3.3.4 (canonical maps of presheaves) Let P be a presheaf on $\mathbf{C}$. We define a family of mappings $\eta_P = ((\eta_P)_C)_{C\in\mathbf{C}} : P \to P^+$ for each $C \in \mathbf{C}$ by

$$(\eta_P)_C(x) := [\{(Pf)(x)\}_{f\in t_C}] \quad (x \in PC). \tag{3.3.6}$$

We claim that η_P is a natural transformation from P to P^+, i.e., for any $h : C' \to C$, the following diagram is commutative:

$$\begin{array}{ccc} PC & \xrightarrow{(\eta_P)_C} & P^+C \\ {\scriptstyle Ph}\downarrow & \circlearrowright & \downarrow{\scriptstyle P^+h} \\ PC' & \xrightarrow[(\eta_P)_{C'}]{} & P^+C'. \end{array} \tag{3.3.7}$$

Since $t_{C'} = h^*(t_C)$, we have

$$\begin{aligned} (P^+h)((\eta_P)_C(x)) &= (P^+h)([\{(Pf)(x)\}_{f\in t_C}]) \\ &= [\{(P(hg))(x)\}_{g\in h^*(t_C)}] \\ &= [\{(Pg)((Ph)(x))\}_{g\in t_{C'}}]. \end{aligned}$$

On the other hand,

$$(\eta_P)_{C'}((Ph)(x)) = [\{(Pg)((Ph)(x))\}_{g\in t_{C'}}].$$

Hence, $(P^+h)((\eta_P)_C(x)) = (\eta_P)_{C'}((Ph)(x))$. Therefore, $\eta_P = ((\eta_P)_C)_{C\in\mathbf{C}}$ is a natural transformation. We shall call η_P the *canonical map* of P.

Lemma 3.3.1 *Let P be a presheaf on $\mathbf{C}$ and η_P the canonical map of P. Then*

(i) *P is a separated presheaf on $(\mathbf{C}, J) \Leftrightarrow \eta_P$ is a monomorphism.*
(ii) *P is a sheaf on $(\mathbf{C}, J) \Leftrightarrow \eta_P$ is an isomorphism.* □

Proof (i) ($\Rightarrow$) Suppose that P is separated. Let $x, y \in PC$ $(C \in \mathbf{C})$ such that

$$(\eta_P)_C(x) = (\eta_P)_C(y) \Leftrightarrow [\{(Pf)(x)\}_{f\in t_C}] = [\{(Pf)(y)\}_{f\in t_C}]. \tag{3.3.8}$$

Then $\exists R \in J(C)$ such that $\forall r \in R$, $(Pr)(x) = (Pr)(y)$. Since P is separated $x = y$. Hence, $(\eta_P)_C$ is injective for all $C \in \mathbf{C}$. Therefore, η_P is a monomorphism.

($\Leftarrow$) Conversely, suppose that η_P is a monomorphism, i.e., for all $C \in \mathbf{C}$, $(\eta_P)_C$ is injective. Let $x, y \in PC$ $(C \in \mathbf{C})$ and $S \in J(C)$ such that for all $f \in S$, $(Pf)(x) = (Pf)(y)$. Since $[\{(Pf)(x)\}_{f\in S}] = [\{(Pf)(x)\}_{f\in t_C}] = (\eta_P)_C(x)$ and $[\{(Pf)(y)\}_{f\in S}] = [\{(Pf)(y)\}_{f\in t_C}] = (\eta_P)_C(y)$, $(\eta_P)_C(x) = (\eta_P)_C$. Since η_C is injective, $x = y$. Therefore, P is separated.

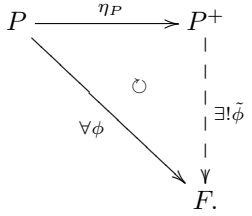
(ii) ($\Rightarrow$) Suppose that P is a sheaf on $(\mathbf{C}, J)$. Then P is separated. Hence, by (i), η_P is a monomorphism. Hence, it is sufficient to show that η_P is an epimorphism. Let $C \in \mathbf{C}$, $S \in J(C)$ and $\{x_f\}_{f\in S} \in \mathrm{Match}(S, P)$. Then, since P is a sheaf, there exists a unique $x \in PC$ such that $\{(Pf)(x)\}_{f\in S} = \{x_f\}_{f\in S}$. On the other hand, $(\eta_P)_C(x) = [\{(Pf)(x)\}_{f\in t_C}] = [\{(Pf)(x)\}_{f\in S}] = [\{x_f\}_{f\in S}]$. Hence, $(\eta_P)_C$ is surjective for all $C \in \mathbf{C}$. Therefore, η_P is an epimorphism. Consequently, η_P is an isomorphism.

($\Leftarrow$) Conversely, suppose that η_P is an isomorphism. In particular, η_P is a monomorphism. By (i), P is separated. Thus, it is sufficient to show that P has an amalgamation for all matching families. Let $\{x_f\}_{f\in S} \in \mathrm{Match}(S, P)$ $(C \in \mathbf{C},\ S \in J(C))$. Since $(\eta_P)_C$ is surjective, there exists $x \in PC$ such that $(\eta_P)_C(x) = [\{(Pf)(x)\}_{f\in t_C}] = [\{x_f\}_{f\in S}]$. Hence, there exists $R \in J(C)$ such that $R \subseteq S$ and $x_r = (Pr)(x)$ for all $r \in R$. Let $f : D \to C \in S$. Then $f^*(R) = \{h \mid fh \in R\} \in J(D)$, by the stability axiom of J. Thus, for all $h \in f^*(R)$, $(P(fh))(x) = x_{fh}$. This implies that $\{(Pfh)(x))\}_{h\in t_D} \sim_D \{x_{fh}\}_{h\in t_D} = \{(Ph)(x_f)\}_{h\in t_D}$. Hence, $(\eta_P)_D((Pf)(x)) = [\{(Ph)((Pf)(x))\}_{h\in t_D}] = [\{(Ph)(x_f)\}_{h\in t_D}] = (\eta_P)_D(x_f)$. Since η_P is a monomorphism, $(Pf)(x) = x_f$ $(f \in S)$. Therefore, x is an amalgamation of $\{x_f\}_{f\in S}$.

The proof is complete. ■

Lemma 3.3.2 *Let F be a sheaf on $(\mathbf{C}, J)$ and P a presheaf on $\mathbf{C}$. Then for any natural transformation $\phi : P \to F$, there exists a unique natural transformation*

$\tilde{\phi} : P^+ \to F$ *such that* $\phi = \tilde{\phi} \circ \eta_P$*, i.e.,* η_P *has the universal mapping property:*



(3.3.9)

Proof Let $C \in \mathbf{C}$, $S \in J(C)$ and $[\{x_f\}_{f\in S}] \in P^+C$. For any $h : D \to C$ in S, by the definition of P^+,

$$(P^+h)([\{x_f\}_{f\in S}]) = [\{x_{hf'}\}_{f'\in h^*(S)}] = [\{x_{hf'}\}_{f'\in t_D}],$$

since $h \in S$ implies $h^*(S) = t_D$. On the other hand, by the definition of η_P,

$$(\eta_P)_D(x_h) = [\{(Pf')(x_h)\}_{f'\in t_D}] = [\{x_{hf'}\}_{f'\in t_D}].$$

Hence,

$$\forall h : D \to C \in S, \quad (P^+h)([\{x_f\}_{f\in S}]) = (\eta_P)_D(x_h). \tag{3.3.10}$$

If the natural transformation $\tilde{\phi} : P^+ \to F$ such that $\phi = \tilde{\phi} \circ \eta_P$ were to exist, for any $h : D \to C$ in S,

$$\begin{aligned}
&(Fh)(\tilde{\phi}_C)([\{x_f\}_{f\in S}]) \\
&= \tilde{\phi}_D((P^+h)([\{x_f\}_{f\in S}])) \quad \text{(by the naturality of } \tilde{\phi}) \\
&= \tilde{\phi}_D((\eta_P)_D)(x_h) \quad \text{(by (3.3.10))} \\
&= \phi_D(x_h).
\end{aligned}$$

On the other hand, $\{\phi_{\mathrm{dom}(h)}(x_h)\}_{h\in S}$ is a matching family of F for S and since F is a sheaf,

$$\exists! y \in PC,\ \forall h \in S,\ (Fh)(y) = \phi_{\mathrm{dom}(h)}(x_h).$$

Accordingly, we define $\tilde{\phi} : P^+ \to F$ for each $C \in \mathbf{C}$ and $[\{x_f\}_{f\in S}] \in P^+C$ by

$$\tilde{\phi}_C([\{x_f\}_{f\in S}]) = y.$$

To verify that $\tilde{\phi}$ is a natural transformation from P^+ to F, we must show that for any $g : D \to C$ in $\mathbf{C}$, the following diagram is commutative:

$$\begin{array}{ccc}
P^+C & \xrightarrow{\tilde{\phi}_C} & FC \\
{\scriptstyle P^+g}\downarrow & \circlearrowright & \downarrow{\scriptstyle Fg} \\
P^+D & \xrightarrow[\tilde{\phi}_D]{} & FD.
\end{array}$$

Let $[\{x_h\}_{h\in S}] \in P^+C$. Then $\tilde{\phi}_D((P^+g)([\{x_h\}_{h\in S}])) = \tilde{\phi}_D([\{x_{gh'}\}_{h'\in g^*(S)}])$ is a unique $z \in FD$ such that

$$\forall h' \in g^*(S), \quad (Fh')(z) = \phi_{\mathrm{dom}(gh')}(x_{gh'}).$$

On the other hand, by the definition of $\tilde{\phi}$, for any $h' \in g^*(S)$,

$$(Fh')((Fg)(\tilde{\phi}_C)([\{x_h\}_{h\in S}])) = (F(gh'))(\tilde{\phi}_C)([\{x_h\}_{h\in S}])) = \phi_{\mathrm{dom}(gh')}(x_{gh'}).$$

Hence,

$$\forall h' \in g^*(S), \quad (Fh')(\tilde{\phi}_D((P^+g)([\{x_h\}_{h\in S}]))) = (Fh')((Fg)(\tilde{\phi}_C)([\{x_h\}_{h\in S}])).$$

Since $g^*(S) \in J(C)$ and F is separated, this implies that

$$\tilde{\phi}_D((P^+g)([\{x_h\}_{h\in S}]))) = ((Fg)(\tilde{\phi}_C)([\{x_h\}_{h\in S}])),$$

i.e., $\tilde{\phi}$ is a natural transformation from P^+ to F.

Next, we verify $\phi = \tilde{\phi} \circ \eta_P$. Let $C \in \mathbf{C}$ and $x \in PC$. Then $(\tilde{\phi}_C \circ (\eta_P)_C)(x) = \tilde{\phi}_C(\{(Ph)(x)\}_{h\in t_C})$ is a unique $y \in FC$ such that

$$\forall h \in t_C, \quad (Fh)(y) = \phi_{\mathrm{dom}(h)}(Ph)(x). \tag{3.3.11}$$

On the other hand, since ϕ is a natural transformation from P to F,

$$\forall h \in t_C, \quad (Fh)((\phi_C)(x)) = \phi_{\mathrm{dom}(h)}((Ph)(x)) = (Fh)(y) \quad \text{(by (3.3.11))}.$$

Since $t_C \in J(C)$ and F is separated, this implies that $y = \phi_C(x)$. Therefore, $\phi = \tilde{\phi} \circ \eta_P$. The proof is complete. ■

The following two lemmas are central results to prove Theorem 3.3.1.

Lemma 3.3.3 *Let P be a presheaf on $\mathbf{C}$. Then P^+ is a separated presheaf on $(\mathbf{C}, J)$.* □

Proof Let $C \in \mathbf{C}$, $Q \in J(C)$ and $\boldsymbol{x} = \{x_f\}_{f\in S}, \boldsymbol{y} = \{y_g\}_{g\in T}$ matching families for some $S, T \in J(C)$ such that for all $h \in Q$, $(P^+h)([\boldsymbol{x}]) = (P^+h)([\boldsymbol{y}])$. Namely, by the definition of P^+,

$$\forall h \in Q, \quad [\{x_{hf'}\}_{f'\in h^*(S)}] = [\{y_{hg'}\}_{g'\in h^*(T)}].$$

For each $h : D \to C \in Q$, by the definition of $\sim_C$, there exists $R_h \in J(D)$ such that $R_h \subseteq h^*(S) \cap h^*(T)$ and $x_{hr} = y_{hr}$ for all $r \in R_h$. To show that P^+ is separated, we must show that there exists $R \in J(C)$ such that $R \subseteq S \cap T$ and $x_r = y_r \in PC$ for all $r \in R$. To this end, let $R := \{hr \mid h \in Q,\ r \in R_h\}$. Then R is a sieve on C and for all $h \in Q$, $h^*(R) = \{s \mid hs \in R\} \supseteq R_h \in J(D)$, so $h^*(R) \in J(D)$. By the transitivity axiom of J, $R \in J(C)$. On the other hand, let $hr \in R$ for some $h \in Q$ and $r \in R_h$. Then $r \in R_h \subseteq h^*(S) \cap h^*(T)$, i.e., $hr \in S \cap T$. Therefore, $J(C) \ni R \subseteq S \cap T$ and for all $r \in R, x_r = y_r$, i.e., $[\boldsymbol{x}] = [\boldsymbol{y}]$. The proof is complete. ■

Lemma 3.3.4 *Let P be a separated presheaf on $(\mathbf{C}, J)$. Then P^+ is a sheaf on $(\mathbf{C}, J)$.* □

Proof Let $C \in \mathbf{C}$ and $\{[\boldsymbol{x}_f]\}_{f\in S}$ a matching family of P^+ for $S \in J(C)$. Note that for all $f : D \to C \in S$, $\boldsymbol{x}_f$ is a matching family of P for some $S_f \in J(D)$ and denote it by $\boldsymbol{x}_f = \{x_{f,h}\}_{h\in S_f}$. The condition that $\{[\boldsymbol{x}_f]\}_{f\in S} \in \mathrm{Match}(S, P^+)$ implies that

$$\forall f : D \to C \in S,\ \forall g : D' \to D, \quad (P^+g)([\boldsymbol{x}_f]) = [\boldsymbol{x}_{fg}],$$

that is,

$$\forall f : D \to C \in S,\ \forall g : D' \to D, \quad [\{x_{f,gh'}\}_{h' \in g^*(S_f)}] = [\{x_{fg,h}\}_{h \in S_{fg}}].$$

By the definition of the equivalence relation, there exists $R_{f,g} \in J(D')$ such that $R_{f,g} \subseteq g^*(S_f) \cap S_{fg}$ and

$$\forall r \in R_{f,g}, \quad x_{f,gr} = x_{fg,r}. \tag{3.3.12}$$

Let $T := \{fg \mid f \in S,\ g \in S_f\}$. Then T is a sieve on C. For each $f : D \to C \in S$, $f^*(T) = \{t \mid ft \in T\} \supseteq S_f \in J(D)$. By the transitivity axiom of J, $T \in J(C)$. Now, we define a matching family $\boldsymbol{y} = \{y_t\}_{t \in T}$ of P for T by

$$y_t := x_{f,g} \quad (t = fg,\ f \in S,\ g \in S_f).$$

Firstly, we must show that the definition does not depend on the choice of f and g such that $t = fg \in T$. Let $t = fg = f'g'$ for some $f, f' \in S$, $g \in S_f$ and $g' \in S_{f'}$. Then there exists $R_{f,g}, R_{f',g'} \in J(D')$ and $R_{f,g} \cap R_{f',g'} \in J(D')$. If $r \in R_{f,g} \cap R_{f',g'}$, then

$$\begin{aligned}(Pr)(x_{f,g}) &= x_{f,gr} \\ &= x_{fg,r} \quad \text{(by (3.3.12))} \\ &= x_{f'g',r} \\ &= x_{f',g'r} \quad \text{(by (3.3.12))} \\ &= (Pr)(x_{f',g'}).\end{aligned}$$

Since P is separated, $x_{f,g} = x_{f',g'}$. Hence, $\boldsymbol{y}$ is well-defined.

Next, we verify that $\boldsymbol{y}$ is a matching family. To this end, let $fg \in T$ for some $f : D \to C \in S$ and $g : D' \to D \in S_f$ and $h : E \to D'$. Then

$$(Ph)(y_{fg}) = (Ph)(x_{f,g}) = x_{f,gh} = y_{fgh}.$$

Hence, $\boldsymbol{y} \in \mathrm{Match}(T, P)$. Therefore, $[\boldsymbol{y}] \in P^+C$.

We shall show that $[\boldsymbol{y}]$ is an amalgamation of $\{x_f\}_{f \in S}$, i.e., for all $f : D \to C \in S$, $(P^+f)([\boldsymbol{y}]) = [\boldsymbol{x}_f]$, i.e.,

$$[\{y_{fg}\}_{g \in f^*(T)}] = [\{x_{f,g}\}_{g \in S_f}] \in P^+D.$$

Since for all $f : D \to C \in S$, $S_f \subseteq f^*(T) = \{t \mid ft \in T\}$ and for all $g \in S_f \in J(D)$, $y_{fg} = x_{f,g}$. This implies that $\{y_{fg}\}_{g \in f^*(T)} \sim_D \{x_{f,g}\}_{g \in S_f}$. Hence, $[\boldsymbol{y}]$ is an amalgamation of $[\{\boldsymbol{x}_f\}_{f \in S}]$. By Lemma 3.3.3, P^+ is separated. Therefore, this amalgamation is unique. Consequently, P^+ is a sheaf on $(\mathbf{C}, J)$. The proof is complete. ■

Definition 3.3.5 (the associated sheaf functor) We define a mapping

$$\mathbf{a} : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \to \mathrm{Sh}(\mathbf{C}, J)$$

as follows:

(i) $\mathbf{a}(P) := (P^+)^+$ for $P \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$;

(ii) $\mathbf{a}(\phi) := (\phi^+)^+$ for a natural transformation $\phi : P \to Q$ in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. ◇

Since plus construction $+$ is a functor, so is $\mathbf{a}$ and is called *the associated sheaf functor*.

By applying Lemma 3.3.2 twice, for any presheaf P on $\mathbf{C}$, $\tilde{\eta}_P := \eta_{P^+} \circ \eta_P$ also has the universal mapping property.

We claim that $\tilde{\eta} := (\tilde{\eta}_P)_{P \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}} : \mathrm{id}_{\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}} \to i\mathbf{a}$ is a natural transformation. To show this, it is sufficient to show the following commutativity in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$:

$$\begin{array}{ccc} P & \xrightarrow{\eta_P} & P^+ \\ {\scriptstyle\phi}\downarrow & \circlearrowright & \downarrow{\scriptstyle\phi^+} \\ Q & \xrightarrow[\eta_Q]{} & Q^+ \end{array}$$

for all $P, Q \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ and all natural transformations $\phi : P \to Q$. To this end, let $C \in \mathbf{C}$ and $x \in PC$. Then

$$\begin{aligned} ((\phi^+)_C \circ (\eta_P)_C)(x) &= (\phi^+)_C((\eta_P)_C(x))) \\ &= (\phi^+)_C([\{(Pf)(x)\}_{f \in t_C}]) \\ &= [\{\phi_{\mathrm{dom}(f)}((Pf))(x))\}_{f \in (t_C)}]. \end{aligned}$$

On the other hand,

$$\begin{aligned} ((\eta_Q)_C \circ (\phi_C))(x) &= (\eta_Q)_C(\phi_C(x)) \\ &= [\{(Qf)(\phi_C(x))\}_{f \in t_C}] \\ &= [\{\phi_{\mathrm{dom}(f)}((Pf)(x))\}_{f \in t_C}] \quad \text{(by the naturality of } \phi). \end{aligned}$$

Thus, $((\phi^+)_C \circ (\eta_P)_C)(x) = ((\eta_Q)_C \circ (\phi_C))(x)$ for all $C \in \mathbf{C}$ and all $x \in PC$. Hence, $\phi^+ \circ \eta_P = \eta_Q \circ \phi$. By replacing P, Q and ϕ by P^+, Q^+ and ϕ^+, respectively, we have $(\phi^+)^+ \circ \eta_{P^+} = \eta_{Q^+} \circ \phi^+$. Therefore, we obtain the following commutative diagram:

$$\begin{array}{ccccc} P & \xrightarrow{\eta_P} & P^+ & \xrightarrow{\eta_{P^+}} & (P^+)^+ \\ {\scriptstyle\phi}\downarrow & \circlearrowright & \downarrow{\scriptstyle\phi^+} & \circlearrowright & \downarrow{\scriptstyle(\phi^+)^+} \\ Q & \xrightarrow[\eta_Q]{} & Q^+ & \xrightarrow{\eta_{Q^+}} & (Q^+)^+. \end{array}$$

Consequently, $\tilde{\eta}$ is a natural transformation from $\mathrm{id}_{\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}}$ to $i\mathbf{a}$.

In conclusion, for the inclusion functor $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, there exists the associated sheaf functor $\mathbf{a} : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \to \mathrm{Sh}(\mathbf{C}, J)$ and a natural transformation $\tilde{\eta} : \mathrm{id}_{\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}} \to i\mathbf{a}$ such that for each $P \in \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, $\tilde{\eta}_P : P \to i\mathbf{a}(P)$ has the universal mapping property. Consequently, $\mathbf{a}$ is a left adjoint of the inclusion functor $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$, i.e., $\mathbf{a} \dashv i$ and $\tilde{\eta}$ is the unit of $\mathbf{a} \dashv i$.

By Lemma 3.3.1 (ii), for any sheaf F on $(\mathbf{C}, J)$, η_F is an isomorphism. Hence, we can construct a natural isomorphism $\tilde{\varepsilon} = (\tilde{\varepsilon}_F)_{F \in \mathrm{Sh}(\mathbf{C}, J)} : \mathbf{a}i \to \mathrm{id}_{\mathrm{Sh}(\mathbf{C}, J)}$ by setting $\tilde{\varepsilon}_F := (\tilde{\eta}_F)^{-1}$. Then $\tilde{\varepsilon}$ is the counit of $\mathbf{a} \dashv i$. We have the following corollary:

Corollary 3.3.1 *Let $(\mathbf{C}, J)$ be a site, $i : \mathrm{Sh}(\mathbf{C}, J) \hookrightarrow \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ the inclusion functor and $\mathbf{a} : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \to \mathrm{Sh}(\mathbf{C}, J)$ the associated sheaf functor. Then*

$$\mathbf{a} \circ i : \mathrm{Sh}(\mathbf{C}, J) \to \mathrm{Sh}(\mathbf{C}, J) \tag{3.3.13}$$

is naturally isomorphic to $\mathrm{id}_{\mathrm{Sh}(\mathbf{C},J)}$. □

To complete the proof of Theorem 3.3.1, we shall show the following lemma:

Lemma 3.3.5 *The associated sheaf functor* **a** *preserves finite limits.* □

Proof It is sufficient to show that the plus construction $+$ preserves finite limits. To this end, let $C \in \mathbf{C}$ and $S \in J(C)$. Then $\mathrm{Match}(S,-) : \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \ni P \mapsto \mathrm{Match}(S,P) \in \mathbf{Sets}$ is a functor. Since every matching family can be identified with a natural transformation, i.e., there is a natural isomorphism

$$\mathrm{Match}(S,P) \cong \mathrm{Hom}_{\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}}(S,P),$$

where we identify S with the subfunctor $S \subseteq \mathbf{y}(C)$, and the Hom-functor $\mathrm{Hom}_{\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}}(S,-)$ preserves limits, we have

$$\mathrm{Match}(S, \varprojlim_{i\in I} P_i) \cong \varprojlim_{i\in I} \mathrm{Match}(S,P_i)$$

for any finite diagram $\{P_i\}_{i\in I}$ (I is finite) in $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$. Recall that $P^+C \cong \varinjlim_{S\in J(C)} \mathrm{Match}(S,P)$ and $J(C)$ is a filtered category equipped with reverse inclusions, since for all $S,T \in J(C)$, $S\cap T \in J(C)$. Since filtered colimits commute with finite limits in **Sets** [2, p. 211], we obtain

$$\begin{aligned}
(\varprojlim_{i\in I} P_i)^+C &\cong \varinjlim_{S\in J(C)} \mathrm{Match}(S, \varprojlim_{i\in I} P_i) \\
&\cong \varinjlim_{S\in J(C)} \varprojlim_{i\in I} \mathrm{Match}(S,P_i) \\
&\cong \varprojlim_{i\in I} \varinjlim_{S\in J(C)} \mathrm{Match}(S,P_i) \\
&\cong \varprojlim_{i\in I} (P_i^+C) \\
&\cong (\varprojlim_{i\in I} P_i^+)C \quad (\because \text{limits in } \mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}} \text{ are computed pointwise}).
\end{aligned}$$

This implies that $(\varprojlim_{i\in I} P_i)^+ \cong \varprojlim_{i\in I} P_i^+$, i.e., $+$ preserves finite limits. The proof is complete. ■

With the above lemmas, the proof of Theorem 3.3.1 is complete.

参考文献

[1] S. Mac Lane and Iake Moerdijk, *Sheaves in Geometry and Logic*, corrected 2nd. ed., Springer, 1994.

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

There is a large cardinal in St. Louis,

and there is no word about how mad his family is.

They are inaccessible, indescribable, ineffable,

shrewd, ethereal, subtle, and remarkable.

It is what forced him to disclose his vice.

淡中 圏　本名：田中健策　冬コミは忙しくて大したものが書けないが、この口惜しさが次の夏コミの原動力になるのである、否、原動力にしなくてはいけないのである。と言うわけで次回予告。次回教育における「論証」の扱いへの疑問を述べるのと、いくつかの睡棄すべき数学関連書籍を一刀両断しようと思う。もう少し高等な数学の話としては「層化」の話をしたい。本当は去年の冬コミに書く予定だったのにね。まあとにかくこうご期待である。

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佑京（@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．

発行者 ： The dark side of Forcing

連絡先 ： http://forcing.nagoya/ , http://proofcafe.org/forcing/

発行日 ： 2014 年 12 月 30 日