Pizzaseminar zu konstruktiver Mathematik

27. Oktober 2014

in Entstehung befindlich, nur grobe Zusammenfassung

Vor langer, langer Zeit begab sich im fernen, fernen Möbiusland folgende Geschichte. Eines Tages holte die Königin des Landes und aller Möbiusschleifen ihren Haus- und Hof-Philosophen zu sich.

Königin. Philosoph! Ich habe folgenden Auftrag an dich: Beschaffe mir den Stein der Weisen, oder alternativ finde heraus, wie man mithilfe des Steins unbegrenzt Gold herstellen kann!

Philosoph. Aber meine Königin! Ich habe nichts Brauchbares studiert! Wie soll ich diese Aufgabe erfüllen?

Königin. Das ist mir egal! Wir sehen uns morgen wieder. Erfüllst du deine Aufgabe nicht, sollst du gehängt werden. Oder wir hacken deinen Kopf ab und verwenden ihn als Cricket-Ball.

Nach einer schlaflosen Nacht voller Sorgen wurde der Philosoph erneut zur Königin berufen.

Königin. Nun! Was hast du mir zu berichten?

Philosoph. Ich habe es tatsächlich geschafft, herauszufinden, wie man den Stein verwenden könnte, um unbegrenzt Gold herzustellen. Aber nur ich kann dieses Verfahren durchführen, Eure Hoheit.

Königin. Nun gut, dann sei es so!

Und so vergingen die Jahre, in denen sich der Philosoph in Sicherheit wähnte und die Angst vor Cricket-Schlägern langsam verlor. Die Königin suchte nun selbst nach dem Stein, aber solange sie ihn nicht fand, hatte der Philosoph nichts zu befürchten.

Doch eines Tages passierte das Unfassbare: Die Königin hatte den Stein gefunden! Und lies prompt den Philosophen zu sich rufen.

Königin. Philosoph, sieh! Ich habe den Stein der Weisen gefunden, hier! Nun erfülle du deinen Teil der Abmachung! *[übergibt den Stein]*

Philosoph. Danke. Ihr hattet von mir verlangt, Euch den Stein der Weisen zu beschaffen oder herauszufinden, wie man mit ihm unbegrenzt Gold herstellen kann. Hier habt Ihr den Stein der Weisen. *[übergibt den Stein zurück]*

Inhaltsverzeichnis

1. Was ist konstruktive Mathematik? 4
- 1.1. Widerspruchsbeweise vs. Beweise von Negationen . . . 5
- 1.2. Informale Bedeutung logischer Aussagen . . . 6
- 1.3. Erste Beispiele . . . 8
- 1.4. Nutzen konstruktiver Mathematik . . . 12

2. Die Schlussregeln intuitionistischer Logik 16
- 2.1. Formale logische Sprache . . . 17
- 2.2. Sequenzen . . . 18
- 2.3. Ableitungen . . . 18
- 2.4. Peano-Arithmetik und Heyting-Arithmetik . . . 23

3. Beziehung zu klassischer Logik 24
- 3.1. Die Doppelnegationsübersetzung . . . 24
- 3.2. Interpretation der übersetzten Aussagen . . . 26
- 3.3. Die umgekehrte Richtung: Modelle für intuitionistische Logik . . . 29

4. Beziehung zur theoretischen Informatik: die Curry–Howard-Korrespondenz 31
- 4.1. Beispiele . . . 32
- 4.2. Interpretation . . . 33
- 4.3. Genauere Formulierung . . . 33

5. Hilberts Programm 33
- 5.1. Die mathematische Welt um 1900 . . . 33
- 5.2. Beispiel aus der Zahlentheorie: Friedmans Trick . . . 36
- 5.3. Beispiel aus der Algebra: dynamische Methoden . . . 39

6. Ein topostheoretischer Zugang zu Quantenmechanik: der Bohr-Topos 46
- 6.1. Gelfand-Dualität zwischen topologischen Räumen und C^*-Algebren . . . 47
- 6.2. Örtlichkeiten für punktfreie Topologie . . . 48
- 6.3. Algebraische Sicht auf klassische Mechanik und Quantenmechanik . . . 50
- 6.4. Topoi als mathematische Alternativuniversen . . . 52
- 6.5. Der Bohr-Topos zu einer nichtkommutativen C^*-Algebra . . . 57

A. Das Auswahlaxiom impliziert das Prinzip vom ausgeschlossenen Dritten 61

B. Ideale in Ringen 62
- B.1. Grundlegende Konzepte . . . 62
- B.2. Historische Motivation für Idealtheorie . . . 64
- B.3. Die Ideale im Ring der ganzen Zahlen . . . 64
- B.4. Primideale und Nilpotenz . . . 64
- B.5. Radikalideale . . . 66

C. Garben **67**
C.1. Prägarben und Garben 67
C.2. Monomorphismen und Epimorphismen von Garben 69

Übungsaufgaben integrieren, dann nicht mehr auf die Übungsblätter verweisen Aufzählungszeichen

Liste der Mottos

Motto 1.13. Eine Aussage gilt genau dann konstruktiv, wenn es ein Computerprogramm gibt, welches sie in endlicher Zeit bezeugt.

Motto 1.24. Intuitionistische Logik ist schwächer, aber auch feiner als klassische Logik.

Motto 2.7. Alle Beweise gewöhnlicher Mathematik, die man gemeinhin als „vollständig und präzise ausformuliert“ bezeichnet, lassen sich als Ableitungen im Sinne von Definition 2.5 formalisieren (ggf. unter Hinzunahme klassischer logischer Axiome, Mengentheorieaxiome oder Typtheorieaxiome).

Motto 2.13. Das optimistische Motto 2.7 stimmt nur in erster Näherung. Es gibt mathematische Gedanken, die nicht formalisierbar sind.

Motto 3.8. Eine Aussage φ intuitionistisch zu behaupten, bedeutet, in jedem Dialog φ belegen zu können.

Motto 3.9. Eine Aussage φ klassisch zu behaupten (also φ° intuitionistisch zu behaupten), bedeutet, in jedem Dialog φ belegen zu können, wobei man aber beliebig oft Zeitsprünge in die Vergangenheit durchführen darf.

Motto 4.1. Eine Aussage φ ist genau dann intuitionistisch ableitbar, wenn es ein Computerprogramm vom Typ φ gibt.

Motto 5.3. In einem *Beweis* einer Aussage steckt viel mehr Inhalt als die bloße Information, dass die Aussage wahr ist.

Motto 5.18. Die *generische* Verwendung ideeller Konzepte (Primideale, maximale Ideale, Bewertungen, . . .) lässt sich eliminieren.

Motto 6.19. Ein Topos ist eine Kategorie, die dadurch, dass sie ähnliche kategorielle Eigenschaften wie die Kategorie der Mengen hat, über eine *interne Sprache* verfügt.

Motto 6.38. Nichtkommutative C^*-Algebren A besitzen zwar keine zugehörige Örtlichkeit im üblichen mathematischen Universum, wohl aber im speziell auf sie zugeschnittenen Topos $\mathrm{Bohr}(A)$.

1. Was ist konstruktive Mathematik?

Proposition 1.1. *Es gibt irrationale Zahlen x und y, sodass x^y rational ist.*

Beweis 1. Die Zahl $\sqrt{2}^{\sqrt{2}}$ ist rational oder nicht rational. Setze im ersten Fall $x := \sqrt{2}$, $y := \sqrt{2}$. Setze im zweiten Fall $x := \sqrt{2}^{\sqrt{2}}$, $y := \sqrt{2}$. □

Beweis 2. Setze $x := \sqrt{2}$ und $y := \log_{\sqrt{2}} 3$. Dann ist die Potenz $x^y = 3$ sicher rational. Die Irrationalität von y lässt sich sogar einfacher als die von $\sqrt{2}$ beweisen: Gelte $y = p/q$ mit $p, q \in \mathbb{Z}$ und $q \neq 0$. Da $y > 0$, können wir sogar $p, q \in \mathbb{N}$ annehmen. Dann folgt $3 = (\sqrt{2})^{p/q}$, also $3^{2q} = 2^p$. Das ist ein Widerspruch zum Satz über die eindeutige Primfaktorzerlegung, denn auf der linken Seite kommt der Primfaktor 3 vor, auf der rechten aber nicht. □

Der erste Beweis war *unkonstruktiv*: Einem interessierten Gegenüber kann man immer noch nicht ein Zahlenpaar mit den gewünschten Eigenschaften nennen. Der zweite Beweis dagegen war konstruktiv: Die Existenzbehauptung wurde durch explizite Konstruktion eines Beispiels nachgewiesen.

Es stellt sich heraus, dass von den vielen Schlussregeln klassischer Logik genau ein Axiom für die Zulässigkeit unkonstruktiver Argumente verantwortlich ist, nämlich das *Prinzip vom ausgeschlossenen Dritten*:

Axiom 1.2 (vom ausgeschlossenen Dritten, LEM)**.** Für jede Aussage φ gilt: $\varphi \vee \neg\varphi$.

Unter konstruktiver Mathematik im engeren Sinn, genauer *intuitionistischer Logik*, versteht man daher klassische Logik ohne das Prinzip vom ausgeschlossenen Dritten. Das *Prinzip der Doppelnegationselimination*, dem zufolge man für jede Aussage φ voraussetzen darf, dass $\neg\neg\varphi \Rightarrow \varphi$ gilt, ist zum Prinzip vom ausgeschlossenen Dritten äquivalent (Übungsaufgabe) und kann daher ebenfalls nicht verwendet werden.

In konstruktiver Mathematik behauptet man *nicht*, dass das Prinzip vom ausgeschlossenen Dritten falsch wäre: Intuitionistische Logik ist abwärtskompatibel zu klassischer Logik – jede konstruktiv nachweisbare Aussage gilt auch klassisch – und manche konkrete Instanzen des Prinzips lassen sich sogar konstruktiv nachweisen (siehe Proposition 1.14 für ein Beispiel). Stattdessen verwendet man das Prinzip einfach nur nicht. (Tatsächlich kann man leicht zeigen, dass es keine Gegenbeispiele des Prinzips geben kann: Für jede Aussage φ gilt $\neg(\neg\varphi \wedge \neg\neg\varphi)$.)

Bemerkung 1.3. Manche Dozenten erzählen Erstsemestern folgende vereinfachte Version der Wahrheit: Eine *Aussage* erkennt man daran, dass sie entweder wahr oder falsch ist. Diese Charakterisierung mag bei klassischer Logik noch irgendwie vertretbar sein, ist aber in einem konstruktiven Kontext offensichtlich unsinnig. Stattdessen erkennt man eine Aussage daran, dass sie rein von ihrer grammatikalischen Struktur her ein Aussagesatz ist (und dass alle vorkommenden Begriffe eine klare Bedeutung haben).

Bemerkung 1.4. In konstruktiver Mengenlehre muss man auf das Auswahlaxiom verzichten, denn in Gegenwart des restlichen Axiome impliziert dieses das Prinzip vom ausgeschlossenen Dritten: siehe Anhang A.

Aufgabe 1.5. Zeige mit einem Widerspruchsbeweis: Mindestens eine der Zahlen $e + \pi$, $e - \pi$ ist irrational.

1.1. Widerspruchsbeweise vs. Beweise von Negationen

Ein übliches Gerücht über konstruktive Mathematik besagt, dass der Begriff *Widerspruch* konstruktiv generell verboten ist. Dem ist nicht so. Man muss zwischen zwei für das klassische Auge sehr ähnlich aussehenden Beweisfiguren unterscheiden:

1. „Angenommen, es gilt $\neg\varphi$. Dann ..., Widerspruch; also gilt $\neg(\neg\varphi)$ und somit φ."
2. „Angenommen, es gilt ψ. Dann ..., Widerspruch; also gilt $\neg\psi$."

Argumente der ersten Form sind tatsächlich Widerspruchsbeweise und daher konstruktiv nicht pauschal zulässig – wenn man nicht anderweitig für die untersuchte Aussage φ begründen kann, dass aus ihrer Doppelnegation schon sie selbst folgt, beweist ein solches Argument nur die Gültigkeit von $\neg\neg\varphi$; das ist konstruktiv schwächer als φ.

Argumente der zweiten Form sind dagegen konstruktiv völlig einwandfrei: Sie sind Beweise negierter Aussagen und nicht Widerspruchsbeweise im eigentlichen Sinn. Die Zulässigkeit erklärt sich direkt nach Definition: Die Negation wird (übrigens auch in klassischer Logik) als

$$\neg\psi :\equiv (\psi \Rightarrow \bot)$$

festgelegt. Dabei steht „$\bot$" für *Falschheit*, eine kanonische falsche Aussage. Wer mag, kann $1 = 0$ oder $\lightning$ denken.

Hier ein konkretes Beispiel aus der Zahlentheorie, um den Unterschied zu demonstrieren:

Proposition 1.6. *Die Zahl $\sqrt{2}$ ist nicht rational.*

Beweis (nur klassisch zulässig). Angenommen, die Behauptung ist falsch, d. h. die Zahl $\sqrt{2}$ ist nicht nicht rational. Dann ist $\sqrt{2}$ also rational. Somit gibt es ganze Zahlen p und q mit $\sqrt{2} = p/q$. Daraus folgt die Beziehung $2q^2 = p^2$, die einen Widerspruch zum Satz über die Eindeutigkeit der Primfaktorzerlegung darstellt: Auf der linken Seite kommt der Primfaktor 2 ungerade oft, auf der rechten Seite aber gerade oft vor. □

Beweis (auch konstruktiv zulässig). Angenommen, die Zahl $\sqrt{2}$ ist rational. Dann gibt es ganze Zahlen ..., Widerspruch. (Der verwendete Satz über die Eindeutigkeit der Primfaktorzerlegung lässt sich konstruktiv beweisen.) □

1.2. Informale Bedeutung logischer Aussagen

... über Belege (die Brouwer–Heyting–Kolmogorov-Interpretation)

Die Ablehnung des Prinzips vom ausgeschlossenen Dritten erscheint uns durch unsere klassische Ausbildung als völlig verrückt: *Offensichtlich* ist doch jede Aussage entweder wahr oder falsch! Die Verwunderung löst sich auf, wenn man akzeptiert, dass konstruktive Mathematiker zwar dieselbe *logische Sprache* verwenden ($\wedge, \vee, \Rightarrow, \neg, \forall, \exists$), aber eine andere Bedeutung im Sinn haben: Wenn eine konstruktive Mathematikerin eine Aussage φ behauptet, meint sie, dass sie einen *expliziten Beleg* für φ hat.

Den Basisfall bilden dabei die sog. *atomaren Aussagen*, von denen wir intuitiv wissen, wie ein Beleg ihrer Gültigkeit aussehen sollte. Atomare Aussagen sind solche, die nicht vermöge der logischen Operatoren $\wedge, \vee, \Rightarrow$ und der Quantoren $\forall, \exists$ aus weiteren Teilaussagen zusammengesetzt sind. In der Zahlentheorie sind atomare Aussagen etwa von der Form

$$n = m,$$

wobei n und m Terme für natürliche Zahlen sind; in der Mengenlehre sind atomare Aussagen von der Form

$$x \in M.$$

Für *zusammengesetzte Aussagen* zeigt Tafel 1, was unter Belegen jeweils zu verstehen ist. (An manchen Stellen steht dort „$x : X$“ – das hat einen Grund, aber momentan soll das einfach etwas seltsame Notation für „$x \in X$“ sein.) Etwa ist ein Beleg für eine Aussage der Form

$$\forall n : \mathbb{N}.\ \varphi(x) \Rightarrow \psi(x)$$

eine Vorschrift, wie man für jede natürliche Zahl $n : \mathbb{N}$ aus einem Beleg für $\varphi(x)$ einen Beleg für $\psi(x)$ erhalten kann. Dies soll tatsächlich nur *eine* Vorschrift sein (welche mit allen natürlichen Zahlen zurechtkommt), nicht für jede natürliche Zahl jeweils eine. Das ist mit dem Qualifikator *gleichmäßig* in der Tabelle gemeint.

Beispiel 1.7. Unter dieser Interpretation meint das Prinzip vom ausgeschlossenen Dritten, dass wir für jede Aussage Beleg für sie oder ihre Negation haben. Das ist aber offensichtlich nicht der Fall.

Beispiel 1.8. Die Interpretation von $\neg\neg\varphi$ ist, dass es keinen Beleg für $\neg\varphi$ gibt. Daraus folgt natürlich noch nicht, dass wir tatsächlich Beleg für φ haben; gewissermaßen ist eine solche Aussage φ nur „potenziell wahr“.

Beispiel 1.9. Wenn wir wissen, dass sich unser Haustürschlüssel irgendwo in der Wohnung befinden muss (da wir ihn letzte Nacht verwendet haben, um die Tür aufzusperren), wir ihn momentan aber nicht finden, so können wir konstruktiv nur folgende doppelt negierte Aussage vertreten:

$$\neg\neg(\exists x.\ \text{der Schlüssel befindet sich an Position } x)$$

	klassische Logik	intuitionistische Logik
Aussage φ	Die Aussage φ gilt.	Wir haben Beleg für φ.
$\bot$	Es stimmt Falschheit.	Wir haben Beleg für Falschheit.
$\varphi \wedge \psi$	φ und ψ stimmen.	Wir haben Beleg für φ und für ψ.
$\varphi \vee \psi$	φ oder ψ stimmt.	Wir haben Beleg für φ oder für ψ.
$\varphi \Rightarrow \psi$	Sollte φ stimmen, dann auch ψ.	Aus Belegen für φ können wir (gleichmäßig) Belege für ψ konstruieren.
$\neg\varphi$	φ stimmt nicht.	Es kann keinen Beleg für φ geben.
$\forall x : X.\ \varphi(x)$	Für alle $x : X$ stimmt jeweils $\varphi(x)$.	Wir können (gleichmäßig) für alle $x : X$ Belege für $\varphi(x)$ konstruieren.
$\exists x : X.\ \varphi(x)$	Es gibt mindestens ein $x : X$, für das $\varphi(x)$ stimmt.	Wir haben ein $x : X$ zusammen mit Beleg für $\varphi(x)$.

Tafel 1: Informale rekursive Definition des Belegbegriffs.

Beispiel 1.10. Wir stehen im Supermarkt und erinnern uns, dass wir unbedingt gewisse Zutaten einkaufen müssen. Leider fällt uns momentan keine einzige der Zutaten mehr ein. Dann können wir zwar die Aussage, dass die Menge der zu besorgenden Zutaten nicht leer ist, vertreten, nicht jedoch die stärkere Aussage, dass diese Menge ein Element enthält.

Beispiel 1.11 ([45, 42])**.** Es war ein Video aufgetaucht, dass Kate Moss beim Konsumieren von Drogen zeigte, und zwar entweder solche von einem Typ A oder solche von einem Typ B. Welcher Typ aber tatsächlich vorlag, konnte nicht entschieden werden. Also gab es für keine der beiden Straftaten einen Beleg, Kate Moss wurde daher nicht strafrechtlich verfolgt.

Bemerkung 1.12. Die Formulierung mit dem generischen *Wir* in Tafel 1 ist etwas irreführend. Wie auch in klassischer Mathematik hängen intuitionistische Urteile nicht von *uns* oder anderen Mathematikern ab. Aussagen, die bisher noch nicht konstruktiv bewiesen wurden, können durchaus einen (noch unbekannten) Beleg besitzen. Eine genauere Diskussion findet sich etwa in [36, Seite 42f.]. Die Brouwer–Heyting–Kolmogorov-Interpretation kann im Rahmen der *Realisierbarkeitstheorie* formalisiert werden [6].

. . . über Berechenbarkeit

Es gibt noch eine zweite Interpretation, die beim Verständnis der konstruktiven Sichtweise sehr hilfreich ist:

Motto 1.13. *Eine Aussage gilt genau dann konstruktiv, wenn es ein Computerprogramm gibt, welches sie in endlicher Zeit bezeugt.*

Etwa ist mit dieser Interpretation klar, dass die formale Aussage

$$\forall n \in \mathbb{N}.\ \exists p \geq n.\ p \text{ ist eine Primzahl},$$

eine Formulierung der Unendlichkeit der Primzahlen, auch konstruktiv stimmt: Denn man kann leicht ein Computerprogramm angeben, das eine natürliche Zahl n als Eingabe erwartet und dann, etwa über die Sieb-Methode von Eratosthenes, eine Primzahl $p \geq n$ produziert (zusammen mit einem Nachweis, dass p tatsächlich prim ist).

Das Motto kann man tatsächlich zu einem formalen Theorem präzisieren, das ist Gegenstand der gefeierten Curry–Howard-Korrespondenz (Abschnitt 4).

1.3. Erste Beispiele

Diskretheit der natürlichen Zahlen

Manche konkrete Instanzen des Prinzips vom ausgeschlossenen Dritten lassen sich konstruktiv nachweisen:

Proposition 1.14. *Für beliebige natürliche Zahlen x und y gilt: $x = y \vee \neg(x = y)$.*

Beweis. Das ist konstruktiv *nicht* klar, aber beweisbar durch eine Doppelinduktion. □

Diese Eigenschaft wird auch als Diskretheit der Menge der natürlichen Zahlen bezeichnet: Allgemein heißt eine Menge X genau dann *diskret*, wenn für alle $x, y \in X$ die Aussage $x = y \vee \neg(x = y)$ gilt. Klassisch ist jede Menge diskret.

Die reellen Zahlen sind in diesem Sinne nicht diskret. Das macht man sich am einfachsten über die algorithmische Interpretation klar: Es kann kein Computerprogramm geben, dass *in endlicher Zeit* zwei reelle Zahlen auf Gleichheit testet. Denn in endlicher Zeit kann ein Programm nur endlich viele Nachkommaziffern (besser: endlich viele rationale Approximationen) abfragen; haben die beiden zu vergleichenden Zahlen dieselben Nachkommaziffern, so kann sich das Programm aber in endlicher Zeit nie sicher sein, ob irgendwann doch noch eine Abweichung auftreten wird.

Übrigens ist die Menge der algebraischen Zahlen durchaus diskret: Man kann ein Programm angeben, dass zwei algebraische Zahlen x und y zusammen mit *Zeugen* ihrer Algebraizität (also Polynomgleichungen mit rationalen Koeffizienten und x bzw. y als Lösung) als Eingabe erwartet und dann entscheidet, ob x und y gleich sind oder nicht. Der Beweis ist nicht trivial, aber auch nicht fürchterlich kompliziert; siehe etwa [43, Prop. 1.6] oder [41, Kapitel VI.1, Seite 140].

Minima von Teilmengen der natürlichen Zahlen

In klassischer Logik gilt folgendes Minimumsprinzip:

Proposition 1.15 (in klassischer Logik)**.** *Sei $U \subseteq \mathbb{N}$ eine bewohnte Teilmenge. Dann enthält U ein kleinstes Element.*

Dabei heißt eine Menge U *bewohnt*, falls $\exists u \in U$. In konstruktiver Mathematik kann man die Gültigkeit dieses Prinzips nicht nachweisen – wegen der Abwärtskompatibilität kann man zwar auch nicht ihr Gegenteil nachweisen, aber man kann ein sog. *brouwersches Gegenbeispiel* anführen:

Proposition 1.16. *Besitze jede bewohnte Teilmenge der natürlichen Zahlen ein Minimum. Dann gilt das Prinzip vom ausgeschlossenen Dritten.*

Beweis. Sei φ eine beliebige Aussage. Wir müssen zeigen, dass φ oder $\neg\varphi$ gilt. Dazu definieren wir die Teilmenge

$$U := \{n \in \mathbb{N} \mid (n = 1) \vee \varphi\}.$$

Die Zugehörigkeitsbedingung ist etwas komisch, da die Aussage φ ja nicht von der frischen Variable n abhängt, aber völlig okay. Da U sicherlich bewohnt ist (durch $1 \in U$), besitzt U nach Voraussetzung ein Minimum $z \in U$.

Wegen der diskutierten Diskretheit der natürlichen Zahlen gilt $z = 0$ oder $z \neq 0$. Im ersten Fall folgt φ (denn $0 \in U$ ist gleichbedeutend mit $(0 = 1) \vee \varphi$, also mit φ), im zweiten Fall folgt $\neg\varphi$ (denn wenn φ gälte, wäre $U = \mathbb{N}$ und somit $z = 0$ im Widerspruch zu $z \neq 0$). □

Wir können das Minimumsprinzip retten, wenn wir eine klassisch triviale Zusatzbedingung stellen:

Definition 1.17. Eine Teilmenge $U \subseteq X$ heißt genau dann *herauslösbar*, wenn für alle $x \in X$ gilt: $(x \in U) \vee \neg(x \in U)$.

Proposition 1.18. *Sei $U \subseteq \mathbb{N}$ eine bewohnte und herauslösbare Teilmenge. Dann enthält U ein kleinstes Element.*

Beweis. Da U bewohnt ist, liegt eine Zahl n in U. Da ferner U herauslösbar ist, gilt für jede Zahl $0 \leq m < n$: $m \in U$ oder $m \notin U$. Daher können wir diese Zahlen der Reihe nach durchgehen; die erste Zahl mit $m \in U$ ist das gesuchte Minimum. □

Weg mag, kann diesen Beweis auch präzisieren und einen formalen Induktionsbeweis führen. Gut erkennbar ist, wie im Beweis ein expliziter Algorithmus zur Findung des Minimums enthalten ist.

Bemerkung 1.19. Statt eine Zusatzbedingung einzuführen, kann man auch die Behauptung abschwächen. Man kann nämlich mittels Induktion zeigen, dass jede bewohnte Teilmenge der natürlichen Zahlen *nicht nicht* ein Minimum besitzt. Der algorithmische Inhalt eines Beweises dieser abgeschwächten Aussage ist sehr interessant und wir werden noch lernen, wie man ihn deuten kann (Abschnitt 3).

Potenzmengen

Klassisch ist die Potenzmenge der einelementigen Menge $\{\star\}$ völlig langweilig: Sie enthält genau zwei Elemente, nämlich die leere Teilmenge und $\{\star\}$ selbst. Konstruktiv lässt sich das nicht zeigen, die Potenzmenge hat (potenziell!) viel mehr Struktur: Ist φ eine beliebige Aussage, so ist

$$M_\varphi := \{x \in \{\star\} \mid \varphi\},$$

wobei x eine nicht in φ vorkommende Variable sei, eine Teilmenge von $\{\star\}$. Diese ist genau dann leer, wenn φ falsch ist; und genau dann gleich ganz $\{\star\}$, wenn φ gilt. Ohne das Prinzip vom ausgeschlossenen Dritten gibt es aber keine allgemeine Rechtfertigung dafür, wieso der eine oder der andere Fall eintreten sollte.

Für verschiedene Aussagen φ können die so konstruierten Teilmengen M_φ miteinander in Relation stehen. Etwa gilt:

$$\emptyset \quad \subseteq \quad M_{\varphi\wedge\psi} \quad \subseteq \quad M_\varphi, M_\psi \quad \subseteq \quad M_{\varphi\vee\psi} \quad \subseteq \quad \{\star\}.$$

In konkreten *Modellen* intuitionistischer Logik können die Teilmengen von $\{\star\}$ eine anschauliche Bedeutung haben (siehe Bemerkung 6.30).

Die De-Morganschen Gesetze

In klassischer Logik verwendet man oft die De-Morganschen Gesetze, manchmal sogar implizit, um verschachtelte Aussagen zu vereinfachen. In konstruktiver Mathematik lässt sich nur noch eines der beiden Gesetze in seiner vollen Form nachweisen. Den Beweis der folgenden Proposition führen wir mit Absicht recht ausführlich, damit wir eine Imitationsgrundlage für die Bearbeitung des ersten Übungsblatts haben. Es wird das Wort „Widerspruch“ vorkommen, aber wir haben ja schon in Abschnitt 1.1 diskutiert, dass das nicht automatisch unkonstruktiv ist.

Proposition 1.20. *Für alle Aussagen φ und ψ gilt*

(a) $\neg(\varphi \vee \psi) \iff \neg\varphi \wedge \neg\psi$,

(b) $\neg(\varphi \wedge \psi) \impliedby \neg\varphi \vee \neg\psi$.

Beweis. (a) „$\Rightarrow$“: Wir müssen $\neg\varphi$ und $\neg\psi$ zeigen:

- Angenommen, es gilt doch φ. Dann gilt auch $\varphi \vee \psi$. Da nach Voraussetzung $\neg(\varphi \vee \psi)$, folgt ein Widerspruch.
- Analog zeigt man $\neg\psi$.

„$\Leftarrow$“: Wir müssen zeigen, dass $\neg(\varphi \vee \psi)$. Dazu nehmen wir an, dass $\varphi \vee \psi$ doch gilt, und streben einen Widerspruch an. Wegen $\varphi \vee \psi$ gibt es zwei Fälle:

- Falls φ gilt: Aus der Voraussetzung $\neg\varphi \wedge \neg\psi$ folgt insbesondere $\neg\varphi$. Somit folgt ein Widerspruch.

- Falls ψ gilt, folgt ein Widerspruch auf analoge Art und Weise.

(b) Wir müssen zeigen, dass $\neg(\varphi \wedge \psi)$. Dazu nehmen wir an, dass doch $\varphi \wedge \psi$ (also dass φ und dass ψ), und streben einen Widerspruch an. Nach Voraussetzung können wir zwei Fälle unterscheiden:

- Falls $\neg\varphi$: Dann folgt ein Widerspruch zu φ.
- Falls $\neg\psi$: Dann folgt ein Widerspruch zu ψ. □

Die Hinrichtung in Regel b) lässt sich konstruktiv nicht nachweisen. Im Belegdenken ist das plausibel: Wenn wir lediglich wissen, dass es keinen Beleg für $\varphi \wedge \psi$ gibt, wissen wir noch nicht, ob es keinen Beleg für φ oder keinen Beleg für ψ gibt. Tatsächlich ist die Hinrichtung in Regel b) äquivalent zu einer schwächeren Version des Prinzips vom ausgeschlossenen Dritten:

Proposition 1.21. *Folgende Prinzipien sind zueinander äquivalent:*

1. *Prinzip vom ausgeschlossenen Dritten für negierte Aussagen: Für alle Aussagen φ gilt $\neg\varphi \vee \neg\neg\varphi$.*
2. *Für alle Aussagen φ und ψ gilt $\neg(\varphi \wedge \psi) \Longrightarrow \neg\varphi \vee \neg\psi$.*

Es ist besser, diese Proposition selbstständig zu beweisen als den folgenden Beweis zu lesen. Denn wenn man nicht genau den Beweisvorgang mitverfolgt, verirrt man sich leicht in den vielen Negationen.

Beweis. „1. ⇒ 2.“: Seien φ und ψ beliebige Aussagen. Gelte $\neg(\varphi\wedge\psi)$. Nach Voraussetzung gilt $\neg\varphi$ oder $\neg\neg\varphi$. Im ersten Fall sind wir fertig. Im zweiten Fall folgt tatsächlich $\neg\psi$: Denn wenn ψ gälte, gälte auch $\neg\varphi$ (denn wenn φ, folgt ein Widerspruch zu $\neg(\varphi \wedge \psi)$), aber das wäre ein Widerspruch zu $\neg\neg\varphi$.

„2. ⇒ 1.“: Sei φ eine beliebige Aussage. Da $\neg(\varphi \wedge \neg\varphi)$ (wieso?), folgt nach Voraussetzung $\neg\varphi \vee \neg\neg\varphi$, das war zu zeigen. □

Weitere Beispiele

Wer auf den Geschmack gekommen ist, kann die Bücher [41] und [10] studieren. Das erste entwickelt einen konstruktiven Zugang zu kommutativer Algebra, das zweite einen zu Analysis. Außerdem ist das Blog von Andrej Bauer [5] eine leicht verständliche Quelle interessanter Beispiele. Von ihm gibt es auch eine seheswerte Videoaufzeichnung eines Vortrags mit dem Titel *Five Stages of Accepting Constructive Mathematics* [4]. Das nLab-Wiki [18], das allgemein ein gutes Nachschlagewerk ist, wenn man an tieferen Hintergründen und Zusammenhängen interessiert ist, diskutiert in vielen Artikeln auch die konstruktive Situation.

1.4. Nutzen konstruktiver Mathematik

Spaß. Konstruktive Mathematik ist erfrischend anders und macht Spaß!

Philosophie. Konstruktive Logik ist philosophisch einfacher zu rechtfertigen als klassische Logik. Das hängt damit zusammen, dass konstruktiv der sonst nebulöse Begriff klassischer Wahrheit durch den konkreteren Begriff der Belegbarkeit ersetzt wird [26].

Eleganzassistenz. Konstruktive Mathematik kann einen dabei unterstützen, Aussagen, Beweise und ganze Theoriegebäude eleganter zu formulieren. Etwa hat man manchmal *Angst vor Spezialfällen* wie etwa der leeren Menge, einem nulldimensionalen Vektorraum oder einer leeren Mannigfaltigkeit. Aussagen formuliert dann nur für nichtleere Mengen, nichttriviale Vektorräume und so weiter, obwohl diese Einschränkungen tatsächlich aber oftmals gar nicht notwendig und unelegant sind.

In konstruktiver Mathematik wird man nun insofern auf diese Problematik aufmerksam gemacht, als dass der Nachweis, dass diese Einschränkungen in bestimmten Fällen erfüllt sind, nicht mehr trivial ist, sondern Nachdenken erfordert. Das möchte man natürlich vermeiden – und so wird man darauf gestoßen, die unnötigen Fallunterscheidungen wegzulassen.

Ein konkretes Beispiel liefert folgende Proposition, die oft als Übungsaufgabe in einer Anfängervorlesung gestellt wird:

Proposition 1.22. *Sei $f : X \to Y$ eine Abbildung und $f^{-1}[\_] : \mathcal{P}(Y) \to \mathcal{P}(X)$ die Urbildoperation (welche eine Teilmenge $U \in \mathcal{P}(Y)$ auf $\{x \in X \mid f(x) \in U\}$ schickt). Dann gilt: Genau dann ist f surjektiv, wenn $f^{-1}[\_]$ injektiv ist.*

Beweis der Rückrichtung (umständlich, nur klassisch zulässig). Angenommen, die Abbildung f ist nicht surjektiv. Dann gibt es ein Element $y \in Y$, welches nicht im Bild von f liegt. Wenn wir die spezielle Teilmenge $\{y\} \in \mathcal{P}(Y)$ betrachten, sehen wir

$$f^{-1}[\{y\}] = \emptyset = f^{-1}[\emptyset].$$

Wegen der vorausgesetzten Injektivität folgt $\{y\} = \emptyset$; das ist ein Widerspruch. □

Beweis der Rückrichtung (elegant, auch konstruktiv zulässig). Bezeichne $\operatorname{im} f$ die Bildmenge von f. Dann gilt $f^{-1}[\operatorname{im} f] = f^{-1}[Y]$ und damit $\operatorname{im} f = Y$, also ist f surjektiv. □

Angst vor der leeren Menge zeigt sich manchmal auch in Beweisen von Mengeninklusionen $X \subseteq Y$. Diese sehen gelegentlich so aus:

> *Falls X leer ist, ist die Behauptung klar. Sei andernfalls ein Element $x \in X$ gegeben. Dann ..., also gilt $x \in Y$.*

Konstruktiv ist die Fallunterscheidung nicht zulässig – das Prinzip, dass jede Menge leer oder nicht leer ist, ist äquivalent zum Prinzip vom ausgeschlossenen Dritten. Tatsächlich kann man solche Beweise stets stromlinienförmiger formulieren:

Sei $x \in X$ gegeben. Dann ..., also gilt $x \in Y$.

Sollte X tatsächlich leer sein, hat man hierbei eine leere Aussage getätigt. Die formale Rechtfertigung für dieses Vorgehen steckt in den Ableitungsregeln für den Allquantor, auf die wir in Abschnitt 2 eingehen. Relevant ist auch eine Diskussion auf MathOverflow zum Thema [25].

Bemerkung 1.23. Wer die leere Menge als Quelle oder Ziel von Abbildung ausschließt muss sich damit abfinden, dass die Kategorie der Mengen dann nicht mehr vollständig und kovollständig ist, denn es fehlen initiale Objekte und viele Differenzkerne. Ohne leere Mannigfaltigkeiten bilden reguläre Urbilder nicht immer Untermannigfaltigkeiten. Ohne triviale Vektorräume besitzen nicht alle linearen Abbildungen einen Kern. Von Richman gibt es einen sehr zugänglichen Artikel über die Nützlichkeit trivialer Ringe [**richman:trivial-rings**] und in der Informatik werden leere Graphen diskutiert [**empty-graph**].

Mentale Hygiene. Arbeit in konstruktiver Logik ist gut für die mentale Hygiene: Man lernt, genauer auf die Formulierung von Aussagen zu achten, nicht unnötigerweise Verneinungen einzuführen und aufzupassen, an welchen bestimmten Stellen klassische Axiome nötig sind. Bei passenden Formulierungen ist das nämlich viel seltener, als man auf den ersten Blick vielleicht vermutet.

Wertschätzung. Klassische Mathematik kann man besser wertschätzen, wenn man verstanden hat, wie anders sich konstruktive Mathematik anfühlt. Die Frage, *inwieweit genau* ein konstruktiver Beweis einer Aussage mehr Inhalt als ein klassischer Beweis hat, kann in Einzelfällen diffizil und interessant sein. Wir werden zu diesem Thema noch einen mathematischen Zaubertrick kennenlernen (Abschnitt 5).

Feinere Unterschiede. Konstruktiv kann man feinere Unterscheidungen treffen. Etwa kann man intuitionistisch den Bedeutungsunterschied zwischen

- *Ich weiß, wo der Haustürschlüssel liegt.* und
- *Ich weiß, dass der Schlüssel hier irgendwo sein muss, ich weiß aber nicht, wo.*

abbilden: Die erste Aussage übersetzt sich als

$$(\exists x.\ \text{der Schlüssel befindet sich an Position } x),$$

die zweite als deren doppelte Verneinung. Klassisch sind diese beiden Übersetzungen dagegen äquivalent, klassisch kann man den Unterschied also nicht formalisieren.

Motto 1.24. *Intuitionistische Logik ist schwächer, aber auch feiner als klassische Logik.*

Wer konstruktive Mathematik abtun möchte, da ein Lieblingstheorem nicht intuitionistisch ableitbar ist, kann noch Abschnitt 3 abwarten, in dem wir verstehen, dass sich klassische Logik in intuitionistische einbetten lässt.

Programmextraktion. Aus jedem konstruktiven Beweis einer Behauptung kann man maschinell, ohne manuelles Zutun, ein Computerprogramm extrahieren, welches die bewiesene Behauptung bezeugt (und selbst bewiesenermaßen korrekt arbeitet). Etwa ist in jedem konstruktiven Beweis der Behauptung

> Sei S eine endliche Menge von Primzahlen. Dann gibt es eine weitere Primzahl, welche nicht in S liegt.

ein Algorithmus versteckt, welcher zu endlich vielen gegebenen Primzahlen ganz konkret eine weitere Primzahl berechnet. Unterschiedliche Beweise können dabei in unterschiedlich effizienten Algorithmen resultieren.

Solch maschinelle Programmextraktion ist wichtig in der Informatik: Anstatt in einem ersten Schritt ein Programm per Hand zu entwickeln und dann in einem zweiten Schritt umständlich seine Korrektheit bezüglich einer vorgegebenen Spezifikation zu zeigen, kann man auch direkt einen konstruktiven Beweis der Erfüllbarkeit der Spezifikation führen und dann automatisch ein entsprechendes Programm extrahieren lassen. In der akademischen Praxis wird dieses Vorgehen tatsächlich angewendet, etwa im Rahmen des Coq-Systems [50].

Auch kann Programmextraktion didaktisch sinnvoll sein: Um etwa eine Existenzbehauptung zu verstehen, ist es bekanntermaßen oftmals hilfreich, sie in einem konkreten Beispielfall durchzudenken – beispielsweise übungshalber ein primitives Element zu einer Körpererweiterung zu berechnen. Einen konstruktiven Beweis der Existenzbehauptung kann man für diesen Zweck stets Schritt für Schritt durchgehen und so am Ende das gesuchte Objekt erhalten.

Mit einem Beweis, der nur klassisch zulässig ist, ist das dagegen im Allgemeinen nicht möglich. Etwa weist man im Verlauf des klassischen Beweises der Tatsache, dass Zahlkörper Ganzheitsbasen besitzen, nach, dass jede Basis bestehend aus ganzen Elementen, deren Diskriminante unter all solchen Basen minimal ist, eine Ganzheitsbasis ist. Wie man eine solche Basis mit minimaler Diskriminante finden kann, wird aber nicht erklärt.[1]

Traummathematik. Nur in einem konstruktiven Kontext ist die Arbeit mit sog. *Traumaxiomen*, wie etwa

> Jede Abbildung $\mathbb{R} \to \mathbb{R}$ ist stetig.

oder

> Es gibt infinitesimale reelle Zahlen ε mit $\varepsilon^2 = 0$, aber $\varepsilon \neq 0$.

[1] Das Beispiel ist nicht perfekt, denn es gibt durchaus konstruktive Beweise dieses Resultats.

möglich: Denn in klassischer Logik sind diese Axiome offensichtlich schlichtweg falsch. Sie sind aber durchaus interessant – sie können die Arbeit rechnerisch und konzeptionell vereinfachen (man muss nur einen Blick zu den Physikern werfen), und es gibt Meta-Theoreme, die garantieren, dass Folgerungen aus diesen Axiomen, welche nur mit konstruktiven Schlussregeln getroffen wurden und eine bestimmte logische Form aufweisen, auch im üblichen klassischen Sinn gelten. Zu *glatter infinitesimaler Analysis* gibt es von John Bell eine leicht verständliche Einführung [9] und ein Buch [8]. Es gibt auch einen Text, der für Schüler verständlich sein soll [**mathezirkel:sdg**].

Bemerkung 1.25. Hier ein kurzer Einschub, wieso das erstgenannte Traumaxiom in einem konstruktiven Kontext zumindest nicht offensichtlich widersprüchlich ist. Man könnte denken, dass die Signumfunktion

$$x \longmapsto \begin{cases} -1, & \text{falls } x < 0, \\ 0, & \text{falls } x = 0, \\ 1, & \text{falls } x > 0 \end{cases}$$

ein triviales Gegenbeispiel ist. Konstruktiv kann man aber nicht zeigen, dass diese Funktion tatsächlich auf ganz $\mathbb{R}$ definiert ist: Die Definitionsmenge ist nur

$$\{x \in \mathbb{R} \mid x < 0 \vee x = 0 \vee x > 0\}.$$

Andrej Bauer diskutiert dieses Beispiel in seinem Blog ausführlicher [7].

Alternative Mathematik-Universen. Wenn man ganz normal Mathematik betreibt, arbeitet man tatsächlich *intern im Topos der Mengen*: Alle üblicherweise untersuchten mathematischen Objekte sind aus Mengen aufgebaut. Es gibt aber auch andere interessante Topoi; diese kommen mit einer *internen Sprache*, welche der üblichen formalen mathematischen Sprache stark ähnelt, sodass man fast wie gewohnt in diesen Topoi arbeiten kann – mit der einzigen Einschränkung, dass diese interne Sprache fast immer nicht klassisch ist. Das liefert einen rein sachlichen Grund, konstruktive Mathematik zu betreiben.

- Vielleicht hat man einen bestimmen topologischen Raum X besonders gern und möchte daher, dass alle untersuchten Objekte vom aktuellen Aufenthaltsort in dem Raum abhängen. Dann möchte man im *Topos der Garben auf X* arbeiten.
- Vielleicht ist man auch ein besonderer Freund einer bestimmten Gruppe G. Dann möchte man vielleicht, dass alle untersuchten Objekte eine G-Wirkung tragen und dass alle untersuchten Abbildungen G-äquivariant sind. Dann sollte man im *Topos der G-Mengen* arbeiten.
- Vielleicht interessiert man sich vor allem dafür, was Turingmaschinen berechnen können. Dann kann man im *effektiven Topos* arbeiten, der nur solche Morphismen enthält, die durch Turingmaschinen algorithmisch gegeben werden können.

Eine genauere Diskussion würde an dieser Stelle zu weit führen. Es seien nur noch zwei Beispiele dafür erwähnt, was mit der Topossichtweise möglich ist:

- Aus dem recht einfach nachweisbaren Faktum konstruktiver linearer Algebra, dass jeder endlich erzeugte Vektorraum *nicht nicht* eine endliche Basis besitzt, folgt *ohne weitere Arbeit* sofort folgende offensichtlich kompliziertere Aussage, wenn man nur das Faktum intern im Garbentopos eines reduzierten Schemas X interpretiert: Jeder $\mathcal{O}_X$-Modul, der lokal von endlichem Typ ist, ist auf einer dichten Teilmenge sogar lokal frei [**blechschmidt:internal-methods**].
- In der Ringtheorie vereinfacht sich etwa die Arbeit mit prüferschen Bereichen. Das sind Ringe, in denen Ideale nur lokal – bezüglich Zerlegungen der Eins – Hauptideale sein müssen. Im *kleinen Zariski-Topos* zu einem solchen Ring erscheint dieser wie ein einfacherer Hauptidealbereich [**pizzaseminar:zariski**].
- Zu quantenmechanischen Systemen kann man eine C^*-Algebra assoziieren. Wichtiges Merkmal ist, dass diese in allen interessanten Fällen *nichtkommutativ* ist. Nun gibt es aber ein alternatives Universum, den sog. *Bohr-Topos*, aus dessen Sicht diese Algebra kommutativ erscheint; auf diese Weise vereinfacht sich manches (Abschnitt 6).

Der Kurzüberblick [3] und die informale Einführung [38] bieten sich als nächste Anlaufstellen zu Topostheorie an. Das Lehrbuch [40] diskutiert auch ausführlich die interne Sprache. Als Referenzen sind [32] für Topostheorie und [37] speziell für kategorielle Logik geeignet.

Hilfe! *Konstruktiv bricht mein Lieblingsteilgebiet der Mathematik zusammen!* Vermutlich ist dem in Wahrheit nicht so, zumindest nicht in einem Ausmaß, der die Aufregung rechtfertigen würde. Wahrscheinlicher ist, dass die konstruktive Perspektive neue Aspekte deines Lieblingsgebiets beleuchtet.

2. Die Schlussregeln intuitionistischer Logik

In den folgenden Abschnitten wollen wir *Meta-Mathematik* betreiben: In Abgrenzung von der sonst betriebenen Mathematik wollen wir nicht die üblichen mathematischen Objekte wie Mengen, Vektorräume, Mannigfaltigkeiten untersuchen, sondern *Beweise*. Dazu müssen wir präzise festlegen, was unter einem (intuitionistischen oder klassischen) Beweis zu verstehen ist.

2.1. Formale logische Sprache

Variablenkontexte

Definition 2.1. Ein *Kontext* ist eine endliche Folge von Variablendeklarationen der Form

$$x_1 : A_1,\ \ldots,\ x_n : A_n.$$

Dabei sind die A_i *Typen* des untersuchten formalen Systems.

Wir werden Kontexte oft kürzer als $\vec{x} : \vec{A}$ notieren. Etwa ist die Aussage

$$n = m$$

eine Aussage im Kontext $n : \mathbb{N}, m : \mathbb{N}$. Dagegen ist die Aussage

$$\forall m : \mathbb{N}.\ n = m$$

eine Aussage im reduzierten Kontext $n : \mathbb{N}$: Die Variable m kommt nicht mehr *frei*, sondern nur noch *gebunden* vor. Wir vereinbaren, dass kollisionsfreie Umbenennung gebundener Variablen nicht als Veränderung einer Aussage zählen soll. Die anders geschriebene Aussage

$$\forall u : \mathbb{N}.\ n = u$$

sehen wir also als dieselbe Aussage an. Wenn wir auch noch über die Variable n quantifizieren, erhalten wir eine Aussage im *leeren Kontext*:

$$\forall n : \mathbb{N}.\ \forall u : \mathbb{N}.\ n = u.$$

Substitution von Variablen

Sei φ eine Aussage im Kontext $x_1, \ldots, x_n$. Sind dann Terme $s_1, \ldots, s_n$ (in einem neuen Kontext $y_1, \ldots, y_m$) gegeben, so kann man die x_i *simultan durch die* s_i *ersetzen*. Als Ergebnis erhält man eine Aussage im Kontext $y_1, \ldots, y_m$, die man „$\varphi[s_1/x_1, \ldots, s_n/x_n]$“ oder kürzer „$\varphi[\vec{s}/\vec{x}]$“ schreibt.

Bei der Substitution muss man Variablenkollisionen verhindern. Etwa gilt für die Aussage

$$\varphi :\equiv (\forall n : \mathbb{N}.\ n = m)$$

im Kontext $m : \mathbb{N}$, dass

$$\varphi[n^2/m] \equiv (\forall \tilde{n} : \mathbb{N}.\ \tilde{n} = n^2).$$

Bemerkung 2.2. In der Logik-Literatur ist die übliche Bezeichnung für das, was wir *Aussagen* nennen, *Formel*.

2.2. Sequenzen

Definition 2.3. Eine *Sequenz* in einem Kontext $\vec{x} : \vec{A}$ ist ein Ausdruck der Form

$$\varphi \vdash_{\vec{x}} \psi,$$

wobei φ und ψ Aussagen in diesem Kontext sind. Aussprache: *Aus der Voraussetzung φ ist die Aussage ψ ableitbar.*

Welche Aussagen aus welchen Voraussetzungen ableitbar sind, entscheiden die *Ableitungsregeln* des untersuchten formalen Systems. Auf diese kommen wir gleich, wollen aber vorher einen rein formalen Aspekt genauer beleuchten.

Sequenzen vs. Implikationen

Wenn man das erste Mal mit der Definition einer Sequenz konfrontiert wird, fragt man sich vielleicht, was der Unterschied zwischen

$$\varphi \vdash_{\vec{x}} \psi \qquad \text{und} \qquad \top \vdash_{\vec{x}} (\varphi \Rightarrow \psi)$$

ist. Tatsächlich ist es bei Kenntnis der Ableitungsregeln für Implikation und Konjunktion eine leichte Übungsaufgabe, die Äquivalenz der beiden Urteile zu zeigen. Die Interpretation ist aber eine völlig andere:

- Die erste Sequenz besagt, dass unter der Globalvoraussetzung φ die Aussage ψ ableitbar ist. Eine typische Übungsaufgabe nach diesem Muster sieht wie folgt aus:

  Sei n eine Primzahl ≥ 3. Zeige, dass $n + 1$ nicht prim ist.

- Die zweite Sequenz besagt, dass unter keiner besonderen Voraussetzung (zur Verfügung stehen also nur die gegebenen Ableitungsregeln) die hypothetische Implikation $\varphi \Rightarrow \psi$ folgt. Eine Beispielformulierung für diese Art ist folgende:

  Zeige, dass wenn n eine Primzahl ≥ 3 ist, die Zahl $n + 1$ nicht prim ist.

Der Unterschied ist subtil, aber sprachlich durchaus vorhanden.

Bemerkung 2.4. Logiker untersuchen auch formale Systeme, die deutlich weniger sprachliche Mittel haben als klassische oder intuitionistische Logik – etwa solche, in denen Implikation als Junktor nicht vorkommt. Das antike System der *Syllogismen* (siehe Abbildung 1) ist ein Beispiel. Dann ist das Sequenzkonzept unverzichtbar.

2.3. Ableitungen

Definition 2.5. Seien φ und ψ Aussagen in einem Kontext $\vec{x} : \vec{A}$. Genau dann ist ψ aus der Voraussetzung φ *ableitbar*, in Symbolen $\varphi \vdash_{\vec{x}} \psi$, wenn es eine entsprechende endliche *Ableitung* gibt, welche nur die in Tafel 2 aufgeführten Ableitungsregeln verwendet.

Abbildung 1: Ein Beispiel für einen (ungültigen) Syllogismus (Randy Glasbergen, verwendet ohne Erlaubnis).

Aus dem Kontext muss hervorgehen, ob man eine Sequenz nur als solche diskutiert oder ob man ihre Ableitbarkeit unterstellt. Außerdem muss man sich an die Notation der Ableitungsregeln gewöhnen. Drei Beispiele seien im Folgenden genauer erklärt.

Die Schnittregel

Oberhalb des horizontalen Strichs in der sog. *Schnittregel*

$$\frac{\varphi \vdash_{\vec{x}} \psi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \chi}$$

sind, nur durch horizontalen Freiraum getrennt, die Voraussetzungen der Regel aufgeführt. Unterhalb des Strichs steht dann das Urteil, das man aus diesen Voraussetzungen ziehen darf. Die Schnittregel besagt also: Ist in einem Kontext $\vec{x}$ aus φ die Aussage ψ ableitbar, und ist ferner aus ψ die Aussage χ ableitbar, so ist auch aus φ direkt χ ableitbar. Die Schnittregel rechtfertigt also die Modularisierung mathematischer Argumente in Lemmata.

Eine der Disjunktionsregeln

Die Disjunktionsregel

$$\frac{\varphi \vdash_{\vec{x}} \chi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vee \psi \vdash_{\vec{x}} \chi}$$

Strukturelle Regeln

$$\frac{}{\varphi \vdash_{\vec{x}} \varphi} \qquad \frac{\varphi \vdash_{\vec{x}} \psi}{\varphi[\vec{s}/\vec{x}] \vdash_{\vec{y}} \psi[\vec{s}/\vec{x}]} \qquad \frac{\varphi \vdash_{\vec{x}} \psi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \chi}$$

Regeln für Konjunktion

$$\frac{}{\varphi \vdash_{\vec{x}} \top} \qquad \frac{}{\varphi \wedge \psi \vdash_{\vec{x}} \varphi} \qquad \frac{}{\varphi \wedge \psi \vdash_{\vec{x}} \psi} \qquad \frac{\varphi \vdash_{\vec{x}} \psi \qquad \varphi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \psi \wedge \chi}$$

Regeln für Disjunktion

$$\frac{}{\bot \vdash_{\vec{x}} \varphi} \qquad \frac{}{\varphi \vdash_{\vec{x}} \varphi \vee \psi} \qquad \frac{}{\psi \vdash_{\vec{x}} \varphi \vee \psi} \qquad \frac{\varphi \vdash_{\vec{x}} \chi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vee \psi \vdash_{\vec{x}} \chi}$$

Doppelregel für Implikation

$$\frac{\varphi \wedge \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \psi \Rightarrow \chi}$$

Doppelregeln für Quantifikation

$$\frac{\varphi \vdash_{\vec{x},y} \psi}{\exists y : Y.\, \varphi \vdash_{\vec{x}} \psi} \ (y \text{ keine Variable von } \psi) \qquad \frac{\varphi \vdash_{\vec{x},y} \psi}{\varphi \vdash_{\vec{x}} \quad \forall y : Y.\, \psi} \ (y \text{ keine Variable von } \varphi)$$

Tafel 2: Die Schlussregeln intuitionistischer Logik.

Regeln für Gleichheit

$$\frac{}{\top \vdash_x x = x} \qquad \frac{}{(\vec{x} = \vec{y}) \wedge \varphi \vdash_{\vec{z}} \varphi[\vec{y}/\vec{x}]}$$

(Dabei steht „$\vec{x} = \vec{y}$“ für $x_1 = y_1 \wedge \cdots \wedge x_n = y_n$.)

Prinzip vom ausgeschlossenen Dritten

$$\frac{}{\top \vdash_{\vec{x}} \varphi \vee \neg\varphi}$$

Tafel 3: Weitere Schlussregeln mancher formaler Systeme.

besagt, dass, wenn aus φ die Aussage χ ableitbar ist, und wenn ferner auch aus ψ die Aussage χ ableitbar ist, dass dann auch aus $\varphi \vee \psi$ die Aussage χ ableitbar ist. Diese Regel rechtfertigt also, bei einer Disjunktion als Voraussetzung einen Beweis durch Unterscheidung der beiden möglichen Fälle zu führen.

Die Doppelregel für den Allquantor

Der Doppelstrich in der Regel

$$\frac{\varphi \vdash_{\vec{x},y} \psi}{\varphi \vdash_{\vec{x}} \quad \forall y : Y.\, \psi}$$

für den Allquantor, die nur angewendet werden darf, wenn y keine freie Variable in φ ist, deutet an, dass die Regel sowohl wie üblich von oben nach unten, als auch von unten nach oben gelesen werden kann. Sie besagt, dass die beiden Urteile

- „Im Kontext $\vec{x} : \vec{A}$, $y : Y$ ist aus φ die Aussage ψ ableitbar."
- „Im Kontext $\vec{x} : \vec{A}$ ist aus φ die Allaussage $\forall y : Y.\ \psi$ ableitbar."

äquivalent sind. Sie rechtfertigt daher das bekannte Standardvorgehen, um Allaussagen nachzuweisen: Man nimmt sich ein „beliebiges, aber festes" $y : Y$, von dem man außer der Zugehörigkeit zu Y keine weiteren Eigenschaften unterstellt, und weist die Behauptung dann für *dieses* y nach.

Aufgabe 2.6. Wieso sind die Variablenbeschränkungen in den Regeln für den Existenz- und Allquantor nötig?

Umfang der Ableitungsregeln

Motto 2.7. *Alle Beweise gewöhnlicher Mathematik, die man gemeinhin als „vollständig und präzise ausformuliert" bezeichnet, lassen sich als Ableitungen im Sinne von Definition 2.5 formalisieren (ggf. unter Hinzunahme klassischer logischer Axiome, Mengentheorieaxiome oder Typtheorieaxiome).*

Aufgabe 2.8. Überzeuge dich von dieser Behauptung. *Tipp:* Formalisiere so viele Beweise deiner Wahl, bis du keine Lust mehr hast.

Wer nicht so viel Zeit hat, dem sei verraten, dass Tafel 2 kein Haufen ungeordneter Ableitungsregeln ist. Stattdessen sind die Axiome nach den sie betreffenden Junktoren bzw. Quantoren gruppiert: Sie legen für jedes sprachliche Konstrukt ist fest, wie man es *einführt* (etwa: „kann man sowohl φ als auch ψ ableiten, so auch $\varphi \wedge \psi$") und *eliminiert* (etwa: „aus $\varphi \wedge \psi$ folgt schlicht φ").

Bemerkung 2.9. Neben den strukturellen Regeln sticht einzig das Prinzip vom ausgeschlossenen Dritten aus diesem System von Einführungs- und Eliminationsprinzipien heraus. Das ist ein rein formal-ästhetisches Argument gegen klassische Logik.

Beispiel 2.10. Dass in jedem Kontext die Sequenz $\varphi \wedge \psi \vdash_{\vec{x}} \psi \wedge \varphi$ ableitbar ist, zeigt folgende Ableitung:

$$\frac{\varphi \wedge \psi \vdash_{\vec{x}} \psi \qquad \varphi \wedge \psi \vdash_{\vec{x}} \varphi}{\varphi \wedge \psi \vdash_{\vec{x}} \psi \wedge \varphi}$$

Die beiden Sequenzen oberhalb des Strichs sind Instanzen des Eliminationsprinzips für die Konjunktion, die Begründung für den Schritt von oben nach unten ist das Einführungsprinzip.

Beispiel 2.11. Folgende Ableitung zeigt, dass $\top \vdash_{\vec{x}} (\varphi \Rightarrow \varphi)$ ableitbar ist:

$$\frac{\top \wedge \varphi \vdash_{\vec{x}} \varphi}{\top \vdash_{\vec{x}} (\varphi \Rightarrow \varphi)}$$

Hierbei wurde das Eliminationsprinzip für die Konjunktion und die Doppelregel für die Implikation angewendet.

Beispiel 2.12. Hier ein längeres Beispiel für eine Ableitung (ein Scan aus [32, Seite 832]):

$$\dfrac{\dfrac{((\phi \wedge \psi) \vdash_{\vec{x},y} \phi)}{((\exists y)(\phi \wedge \psi) \vdash_{\vec{x}} \phi)} \qquad \dfrac{\dfrac{((\phi \wedge \psi) \vdash_{\vec{x},y} \psi) \qquad \dfrac{((\exists y)\psi \vdash_{\vec{x}} (\exists y)\psi)}{(\psi \vdash_{\vec{x},y} (\exists y)\psi)}}{((\phi \wedge \psi) \vdash_{\vec{x},y} (\exists y)\psi)}}{((\exists y)(\phi \wedge \psi) \vdash_{\vec{x}} (\exists y)\psi)}}{((\exists y)(\phi \wedge \psi) \vdash_{\vec{x}} (\phi \wedge (\exists y)\psi))}$$

Diese Ableitung beweist (eine Richtung des) *Frobenius-Prinzips*. Dabei darf die Variable y nicht in ϕ vorkommen.

Nicht verschwiegen werden sollte folgende Ergänzung des formalistischen Kredos:

Motto 2.13. *Das optimistische Motto 2.7 stimmt nur in erster Näherung. Es gibt mathematische Gedanken, die nicht formalisierbar sind.*

Zu solchen Gedanken gehören etwa die Überzeugung, jede Art finitistischer Überlegung könne in Peano-Arithmetik formalisiert werden; die Church–Turing-These, der zufolge jede „algorithmisch berechenbare“ Funktion $\mathbb{N} \to \mathbb{N}$ durch eine Turing-Maschine gegeben werden könne [19, 28, 44]; und manche allgemeinen mathematischen Prinzipien. Außerdem ist seit Gödel allgemein bekannt, dass es Beispiele für Aussagen gibt, die zwar in einem formalen System formalisierbar und von einem höheren Standpunkt aus betrachtet wahr sind (gewissermaßen also einen informalen Beweis besitzen), im gegebenen System aber nicht formal bewiesen werden können.

In diesem Kontext ist auch die *chaitinsche Haltekonstante* interessant, die die Wahrscheinlichkeit dafür angibt, dass ein zufällig gezogenes Programm einer festen Programmiersprache terminiert. Jedes formale System kann nur endlich viele Nachkommaziffern dieser (durchaus wohldefinierten) Zahl bestimmen **??**.

Einschub: Der Quantor für eindeutige Existenz

Der Quantor $\exists!$ für eindeutige Existenz kommt in den Ableitungsregeln aus Tafeln 2 und 3 nicht vor. Das ist nicht weiter schlimm, da man diesen durch die anderen sprachlichen Mittel ausdrücken kann: Die Aussage „$\exists! y : Y.\ \varphi$“ steht für

$$\exists y : Y.\ \varphi \quad \wedge \quad \forall y : Y.\ \forall y' : Y.\ \varphi \wedge \varphi[y'/y] \Rightarrow y = y'.$$

Aufgabe 2.14. Zeige, dass diese Formalisierung äquivalent ist zur ebenfalls naheliegenden Umschreibung

$$\exists y : Y.\ \Big(\varphi \wedge (\forall y' : Y.\ \varphi[y'/y] \Rightarrow y = y')\Big).$$

2.4. Peano-Arithmetik und Heyting-Arithmetik

Definition 2.15. Das formale System *Heyting-Arithmetik* ist gegeben durch

- intuitionistische Logik,
- die Gleichheitsregeln (siehe Tafel 3),
- einem einzigen Typ $\mathbb{N}$,
- einer Termkonstante $0 : \mathbb{N}$,
- einem 1-adischen Termkonstruktor S (für *successor*): Ist $n : \mathbb{N}$ ein Term vom Typ $\mathbb{N}$, so ist $S(n) : \mathbb{N}$ ebenfalls ein Term vom Typ $\mathbb{N}$,
- die Axiome

  $$\frac{}{S(n) = 0 \vdash_n \bot} \qquad\qquad \frac{}{S(n) = S(m) \vdash_{n,m} n = m}$$

  und das Induktionsprinzip

  $$\frac{\varphi \vdash_{\vec{x}} \psi[0/m] \qquad \varphi \vdash_{\vec{x},m} \psi \Rightarrow \psi[S(m)/m]}{\varphi \vdash_{\vec{x}} \forall m : \mathbb{N}.\ \psi}$$

- sowie Regeln für alle primitiv-rekursiven Funktionen, insbesondere also die erwarteten Regeln für Addition und Multiplikation.

Definition 2.16. Das formale System *Peano-Arithmetik* ist genau wie Heyting-Arithmetik gegeben, nur mit klassischer statt intuitionistischer Logik.

Definition 2.17. Ein formales System heißt genau dann *inkonsistent*, wenn es in ihm eine Ableitung der Sequenz $\top \vdash \bot$ (im leeren Kontext) gibt. Andernfalls heißt es *konsistent*.

Aufgabe 2.18. Wieso ist es für formale Systeme im Allgemeinen keine interessante Frage, ob es in nichtleeren Kontexten eine Ableitung von $\top \vdash_{\vec{x}} \bot$ gibt?

Bemerkung 2.19. Intuitionistische formale Systeme haben oft besondere Meta-Eigenschaften. Etwa hat Heyting-Arithmetik die *Disjunktionseigenschaft*: Gibt es in Heyting-Arithmetik eine Ableitung einer Disjunktion $\varphi \vee \psi$, so gibt es schon eine Ableitung

von φ oder eine von ψ. Klassische Systeme dagegen haben wegen des Gödelschen Unvollständigkeitssatzes diese Eigenschaft in der Regel nicht. Denn besitzt ein solches System eine Gödelaussage φ, so zeigt das System trivialerweise $\varphi \vee \neg\varphi$, aber nach Voraussetzung an φ gibt es weder eine Ableitung von φ noch eine von $\neg\varphi$.

3. Beziehung zu klassischer Logik

Auf den ersten Blick scheint intuitionistische Logik schlichtweg weniger mächtig als klassische Logik zu sein: Viele Aussagen sind klassisch, aber nicht intuitionistisch ableitbar. Das ist aber nur die halbe Wahrheit: Es gibt nämlich die *Doppelnegationsübersetzung*, die Aussagen derart umformt, dass die Übersetzung einer Aussage genau dann konstruktiv gilt, wenn die ursprüngliche Aussage klassisch gilt. In diesem Sinn lässt sich also klassische Logik in intuitionistische einbetten – man hat also klassische Logik zur Verfügung, wenn man sie ausnahmsweise verwenden möchte.

Eine Übersetzung in die andere Richtung gibt es leider nicht, man muss größeren Aufwand treiben, um in einem klassischen Kontext die Sichtweise konstruktiver Mathematiker zu verstehen. Darauf gehen wir am Ende dieses Abschnitts ein.

3.1. Die Doppelnegationsübersetzung

Definition 3.1. Die *Doppelnegationsübersetzung* (nach Kolmogorov, Gentzen, Gödel und anderen) wird rekursiv wie folgt definiert:

$$\begin{aligned}
\varphi^\circ &:\equiv \neg\neg\varphi \text{ für atomare Aussagen } \varphi \\
\top^\circ &:\equiv \top \\
\bot^\circ &:\equiv \bot \\
(\varphi \wedge \psi)^\circ &:\equiv \neg\neg(\varphi^\circ \wedge \psi^\circ) \\
(\varphi \vee \psi)^\circ &:\equiv \neg\neg(\varphi^\circ \vee \psi^\circ) \\
(\varphi \Rightarrow \psi)^\circ &:\equiv \neg\neg(\varphi^\circ \Rightarrow \psi^\circ) \\
(\forall x : X.\ \varphi)^\circ &:\equiv \neg\neg\forall x : X.\ \varphi^\circ \\
(\exists x : X.\ \varphi)^\circ &:\equiv \neg\neg\exists x : X.\ \varphi^\circ
\end{aligned}$$

Bemerkung 3.2. Da $\neg\varphi :\equiv (\varphi \Rightarrow \bot)$, gilt $(\neg\varphi)^\circ \equiv \neg(\varphi^\circ)$.

Aufgabe 3.3. Beweise durch Induktion über den Aussageaufbau, dass man auf die grau gesetzten Doppelnegationen verzichten kann. Gewissermaßen besteht also der einzige Unterschied zwischen klassischer und intuitionistischer Logik in der Interpretation der Disjunktion und der Existenzquantifikation: Diese sagen konstruktiv mehr aus als in klassischer Logik.

Satz 3.4. *Seien φ und ψ beliebige Aussagen in einem Kontext $\vec{x}$.*

(a) *Klassisch gilt:* $\varphi^\circ \iff \varphi$.

(b) *Intuitionistisch gilt:* $\neg\neg\varphi^\circ \implies \varphi^\circ$.

(c) *Wenn* $\varphi \vdash_{\vec{x}} \psi$ *klassisch, dann* $\varphi^\circ \vdash_{\vec{x}} \psi^\circ$ *intuitionistisch; und umgekehrt.*

Beweis. (a) Klar, für jede Aussage χ ist $\neg\neg\chi \Leftrightarrow \chi$ eine klassische Tautologie.

(b) In der Variante mit den grau gesetzten Doppelnegationen ist das klar, denn für jede Aussage χ ist $\neg\neg\neg\neg\chi \Rightarrow \neg\neg\chi$ eine intuitionistische Tautologie. (Es gilt sogar schon $\neg\neg\neg\chi \Leftrightarrow \neg\chi$.)

(c) Die Rückrichtung ist wegen der Abwärtskompatibilität intuitionistischer Logik und Teilaussage a) trivial.

Für die Hinrichtung müssen wir in einer Induktion über den Aufbau klassischer Ableitungen nachweisen, dass wir jeden logischen Schluss klassischer Logik in der Doppelnegationsübersetzung intuitionistisch nachvollziehen können. (Aus diesem Grund mussten wir im vorherigen Abschnitt formal definieren, was wir unter Ableitungen verstehen wollen.)

Etwa müssen wir zeigen, dass die übersetzte Schnittregel gültig ist:

$$\frac{\varphi^\circ \vdash_{\vec{x}} \psi^\circ \qquad \psi^\circ \vdash_{\vec{x}} \chi^\circ}{\varphi^\circ \vdash_{\vec{x}} \chi^\circ}$$

Aber das ist klar, denn das ist wieder eine Instanz der intuitionistisch zulässigen Schnittregel. Ein interessanteres Beispiel ist die übersetzte Form von einer der Disjunktionsregeln:

$$\frac{}{\varphi^\circ \vdash_{\vec{x}} \neg\neg(\varphi^\circ \vee \psi^\circ)}$$

Die Gültigkeit dieser Regel folgt aus der Disjunktionsregel und der intuitionistischen Tautologie $\chi \Rightarrow \neg\neg\chi$. Als letztes und wichtigstes Beispiel wollen wir die Übersetzung des klassischen Axioms vom ausgeschlossenen Dritten diskutieren:

$$\frac{}{\top \vdash_{\vec{x}} \neg\neg(\varphi^\circ \vee \neg\varphi^\circ)}$$

Dass diese Regel intuitionistisch zulässig ist, haben wir in Übungsblatt 1 gesehen. Die Untersuchung aller weiteren Schlussregeln sparen wir uns an dieser Stelle (aber siehe Übungsblatt 2). □

Korollar 3.5. *Zeigt Peano-Arithmetik einen Widerspruch, so auch Heyting-Arithmetik.*

Beweis. Man kann leicht nachprüfen, dass die Doppelnegationsübersetzungen der Peano-Axiome wiederum Instanzen den Peano-Axiome sind und daher auch in Heyting-Arithmetik gelten. Daher kann man eine Ableitung von $\bot$ in Peano-Arithmetik in eine Ableitung von $\bot^\circ \equiv \bot$ in Heyting-Arithmetik überführen. □

Unter gewissen Bedigungen an die Aussageform kann man die vielen durch die Übersetzung eingeführten Doppelnegationen zu einer einzigen „nach vorne ziehen“. Das ist Gegenstand von folgendem Lemma, das in Abschnitt 5.2 über Friedmans Trick noch eine wesentliche Rolle spielen wird.

Lemma 3.6. *Sei φ eine Aussage, in der nur $\top$, $\bot$, $\wedge$, $\vee$ und $\exists$, aber nicht $\Rightarrow$ und $\forall$ vorkommen. Dann gilt intuitionistisch: $\varphi^\circ \iff \neg\neg\varphi$.*

Beweis. Induktion über den Aussageaufbau. Exemplarisch sei der Fall für den Existenzquantor vorgeführt. Bei diesem ist zu zeigen, dass $(\exists x : X.\ \varphi)^\circ$ äquivalent zu $\neg\neg\exists x : X.\ \varphi$ ist. Nach Definition der Übersetzung und der Induktionsvoraussetzung ist die erste Aussage äquivalent zu $\neg\neg\exists x : X.\ \neg\neg\varphi$. Die Behauptung folgt daher aus den intuitionistischen Tautologien $\neg\exists \Leftrightarrow \forall\neg$ und $\neg\neg\neg \Leftrightarrow \neg$. □

Bemerkung 3.7. Der Artikel [**oconnor:exact**] demonstriert, wie man das Zusammenspiel zwischen klassischer und intuitionistischer Logik im Rahmen exakter Numerik ausnutzen kann.

3.2. Interpretation der übersetzten Aussagen

Die konstruktive Bedeutung übersetzter Aussagen lässt sich wegen der Vielzahl vorkommender nichttrivialer doppelter Verneinungen nicht sofort überblicken. Es gibt aber eine aus der theoretischen Informatik stammende *Zeitsprungmetapher*, mit der man den Inhalt übersetzter Aussagen doch verstehen kann.

Dazu erinnern wir zunächst an die Dialogmetapher zur Interpretation logischer Aussagen: Wir stellen uns ein besonders kritisches Gegenüber vor, das unsere Behauptung bezweifelt. In einem Dialog versuchen wir dann, das Gegenüber zu überzeugen. Eine typische Stetigkeitsüberzeugung sieht etwa wie folgt aus:

Eve: Ich gebe dir $x = \cdots$ und $\varepsilon = \cdots$ vor.
Alice: Gut, dann setze ich $\delta = \cdots$.
Eve: Dann ist hier ein $\tilde{x} = \cdots$ zusammen mit einem Beleg von $|x - \tilde{x}| < \delta$.
Alice: Dann gilt tatsächlich $|f(x) - f(\tilde{x})| < \varepsilon$, wie von mir behauptet, denn ...

In Tafel 1 (Seite 7) ist festgelegt, nach welchen Spielregeln Alice und Eve bei solchen Dialogen miteinander kommunizieren müssen. Exemplarisch seien einige nochmal betont:

- Wenn Eve von Alice einen Beleg von $\varphi \vee \psi$ fordert, muss Alice einen Beleg von φ oder einen Beleg von ψ präsentieren. Sie darf sich nicht mit einem „angenommen, keines von beiden gälte“ herausreden.
- Wenn Eve von Alice einen Beleg von $\varphi \Rightarrow \psi$ fordert, muss Alice ihr versprechen, Belege von φ in Belege von ψ überführen zu können. Dieses Versprechen kann Eve herausfordern, indem sie einen Beleg von φ präsentiert; Alice muss dann in der Lage sein, mit einem Beleg von ψ zu antworten.

- Für die Negation als Spezialfall der Implikation gilt folgende Spielregel: Wenn Eve von Alice einen Beleg von $\neg\varphi \equiv (\varphi \Rightarrow \bot)$ verlangt, muss Alice in der Lage sein, aus einem präsentierten Beleg von φ einen Beleg von $\bot$ zu produzieren. Wenn das betrachtete formale System konsistent ist, gibt es keinen solchen Beleg (zumindest nicht im leeren Kontext); Alice kann unter der Konsistenzannahme also nur dann $\neg\varphi$ vertreten, wenn es keinen Beleg von φ gibt.

Als Motto können wir festhalten:

Motto 3.8. *Eine Aussage φ intuitionistisch zu behaupten, bedeutet, in jedem Dialog φ belegen zu können.*

Dank der Doppelnegationsübersetzung können wir damit auch eine Dialoginterpretation klassischer Behauptungen angeben. Es stellt sich heraus, dass die folgende Metapher sehr tragfähig ist. Diese wollen wir dann erst an einem Beispiel veranschaulichen, bevor wie sie rechtfertigen.

Motto 3.9. *Eine Aussage φ klassisch zu behaupten (also φ° intuitionistisch zu behaupten), bedeutet, in jedem Dialog φ belegen zu können, wobei man aber beliebig oft Zeitsprünge in die Vergangenheit durchführen darf.*

Beispiel: das Prinzip vom ausgeschlossenen Dritten

Wir wollen sehen, wie man das klassische Prinzip $\varphi \vee \neg\varphi$ mit Hilfe von Zeitsprüngen vertreten kann.

Eve: Zeige mir $\varphi \vee \neg\varphi$!

Alice: Gut! Es gilt $\neg\varphi$.

Wenn φ eine allgemeine Aussage ist, kann Alice nicht wissen, ob φ oder $\neg\varphi$ gilt. Sie hat daher an dieser Stelle geblufft. Da sie eine Implikation behauptet – nämlich $(\varphi \Rightarrow \bot)$ –, ist nun Eve wieder an der Reihe. Sie kann nur dann in ihrem Vorhaben, Alice zu widerlegen, fortfahren, wenn sie einen Beleg von φ präsentiert und dann Alice herausfordert, ihr Versprechen, daraufhin einen Beleg von $\bot$ zu präsentieren, einzulösen.

Wenn es keinen Beleg von φ gibt, ist das Streitgespräch daher an dieser Stelle beendet, und Alice hat sogar die Wahrheit gesagt. Andernfalls geht es weiter:

Eve: Aber hier ist ein Beleg von φ: x. Belege mir nun $\bot$!

Wenn Alice nicht die Inkonsistenz des untersuchten formalen Systems nachweisen kann, hat sie nun ein Problem: Ihre Lüge von Beginn straft sich, sie kann das Gespräch nicht fortsetzen. Sie muss daher in einem Logikwölkchen verschwinden und in der Zeit zurückspringen:

Eve: Zeige mir $\varphi \vee \neg\varphi$!

Alice: Gut! Es gilt φ, hier ist ein Beleg: x.

Damit ist das Gespräch abgeschlossen.

Wer Zeitsprünge dieser Form betrügerisch findet, hat die Grundüberzeugung konstruktiver Mathematik bereits verinnerlicht: In diesem (und nur diesem) Sinn ist klassische Logik tatsächlich betrügerisch. Das macht klassische Logik aber nicht trivial: Auch mit Zeitsprüngen kann man nicht jede beliebige Aussage in einem Dialog vertreten. Wenn man etwa obiges Vorgehen mit der im Allgemeinen ungerechtfertigten Aussage $\varphi \vee \neg\psi$ versucht, wird man sehen, dass auch die Fähigkeit zu Zeitsprüngen nicht hilft.

Dasselbe Beispiel, konservativer interpretiert

Um zu sehen, dass die Zeitsprungmetapher berechtigt ist, wollen wir exemplarisch dasselbe Beispiel erneut untersuchen, diesmal aber ohne die Metapher. Wir wollen also einen Dialog zur Doppelnegationsübersetzung des Prinzips vom ausgeschlossenen Dritten, also zu $\neg\neg(\varphi^\circ \vee \neg\varphi^\circ)$, führen. Da wir für beliebige Aussagen φ sogar das Prinzip $\neg\neg(\varphi \vee \neg\varphi)$ intuitionistisch gilt, ausgeschrieben

$$((\varphi \vee \neg\varphi) \Rightarrow \bot) \Rightarrow \bot,$$

und dieses geringfügig übersichtlicher ist, wollen wir tatsächlich dieses in Dialogform belegen.

Eve: Zeige mir $\neg\neg(\varphi \vee \neg\varphi)$! Präsentiere mir also einen Beleg von $\bot$, wobei du auf mich zurückkommen kannst, wenn du einen Beleg von $\varphi \vee \neg\varphi$ hast; dann würde ich Beleg von $\bot$ produzieren.

Alice: Gut! Dann komme ich sofort auf dich zurück, denn ich habe einen Beleg von $\neg\varphi$. $(\star)$

Wie oben ist das Gespräch an dieser Stelle beendet, wenn Eve nicht einen Beleg von φ produzieren kann, mit dem sie Alice herausfordern könnte. Falls sie das doch schafft, geht es wie folgt weiter:

Eve: Ach wirklich? Hier ist ein Beleg von φ: x. Zeige mir nun einen Beleg von $\bot$!

Alice: Dann komme ich auf deine Verpflichtung mir gegenüber ein zweites Mal zurück – hier ist ein Beleg von $\varphi \vee \neg\varphi$: x.

Eve: Stimmt. Dann ist hier Beleg von $\bot$: y.

Alice: Danke. Dann ist hier ein Beleg von $\bot$: y. Damit habe ich meine Pflicht erfüllt.

Eve: Stimmt. Dann erfülle ich meinen Teil der Verpflichtung (Stelle $(\star)$), hier ist Beleg von $\bot$: z.

Alice: Danke. Dann ist hier Beleg von $\bot$, wie gefordert: z.

Hintergrund aus der theoretischen Informatik

Fazit

Curry-Howard

Doppelnegationsübersetzung, Continuation-Passing-Style Transformation, LCM, Stein der Weisen, ...

3.3. Die umgekehrte Richtung: Modelle für intuitionistische Logik

Mit der Doppelnegationsübersetzung kann eine konstruktive Mathematikerin auf eine sehr einfache Art und Weise einen klassischen Kollegen verstehen: Wenn ein klassischer Mathematiker eine Aussage φ behauptet, muss sie sich nur vorstellen, φ° gehört zu haben.

Für die umgekehrte Richtung gibt es keine Übersetzung: Es gibt keine Aussagentransformation $\varphi \mapsto \varphi^\#$ mit den Eigenschaften

(a) $\varphi \iff \varphi^\#$ intuitionistisch und

(b) genau dann $\varphi \vdash_{\vec{x}} \psi$ intuitionistisch, wenn $\varphi^\# \vdash_{\vec{x}} \psi^\#$ klassisch.

Denn aus der ersten Eigenschaft würde wegen der Abwärtskompatibilität intuitionistischer Logik zu klassischer Logik ja klassisch die Äquivalenz $\varphi \Leftrightarrow \varphi^\#$ folgen; das ist mit Eigenschaft b) unverträglich.

Eine klassische Mathematikerin hat es also schwerer, konstruktiv arbeitende Kollegen zu verstehen. Sie muss dazu geeignete *Modelle* betrachten.

Topologische Modelle für propositionale intuitionistische Logik

Mit *propositionaler* Logik bezeichnet man das Fragment, in dem keine Variablen und daher insbesondere keine Quantoren vorkommen. (Ihre klassische Variante kann man noch mit Wahrheitstafeln vollständig verstehen.)

Jeder topologischer Raum X liefert ein Modell $\mathrm{Ouv}(X)$ für propositionale intuitionistische Logik: Wenn man jeder atomaren Aussage φ eine bestimmte offene Menge $[\![\varphi]\!] \subseteq X$ zuordnet, kann man die Interpretation der restlichen Aussagen gemäß folgender Definition festlegen.

Definition 3.10 (topologische Interpretation zusammengesetzter Aussagen)**.**

$$\begin{aligned}
[\![\top]\!] &:= X \\
[\![\bot]\!] &:= \emptyset \\
[\![\varphi \wedge \psi]\!] &:= [\![\varphi]\!] \cap [\![\psi]\!] \\
[\![\varphi \vee \psi]\!] &:= [\![\varphi]\!] \cup [\![\psi]\!] \\
[\![\varphi \Rightarrow \psi]\!] &:= \cancel{[\![\varphi]\!]^c \cup [\![\psi]\!]} = \mathrm{int}([\![\varphi]\!]^c \cup [\![\psi]\!])
\end{aligned}$$

Dabei bezeichnet U^c das Komplement von U in X. Die Verwendung von $([\![\varphi]\!]^c \cup [\![\psi]\!])$ würde die Menge der offenen Mengen von X verlassen und ist daher schon aus diesem formalen Grund keine gute Idee; Abhilfe schafft der innere Kern.

Anschaulich kann man sich $[\![\varphi]\!]$ als den Ort, wo φ erfüllt ist, vorstellen. Wenn $[\![\varphi]\!] = \emptyset$, gilt φ also nirgendwo; wenn $[\![\varphi]\!] = X$ gilt, gilt φ überall; wenn X nicht gerade nur zwei offene Mengen besitzt, sind aber auch viele weitere Abstufungen möglich. In diesem Sinn ist $\mathrm{Ouv}(X)$ ein Modell mit mehr als zwei Wahrheitswerten.

Beispiel 3.11. Sei X die Erdoberfläche. Dann kann man zwei atomare Aussagen A und B mit den Interpretationen

$$[\![A]\!] := \{x \in X \mid \text{an der Stelle } x \text{ regnet es}\}$$
$$[\![B]\!] := \{x \in X \mid \text{an der Stelle } x \text{ hat es mehr als 20 Grad}\}$$

definieren. Die Aussage $A \wedge B$ hat dann die Interpretation $[\![A \wedge B]\!] = [\![A]\!] \wedge [\![B]\!]$, beschreibt also den Ort derjenigen Stellen auf der Erde, an denen es bei mehr als 20 Grad regnet.

Die folgende Proposition zeigt, dass die Definition 3.10 die Regeln intuitionistischen Schließens respektiert und daher sinnvoll ist:

Proposition 3.12. *Wenn $\varphi \vdash \psi$ intuitionistisch ableitbar ist (im Fragment ohne Variablen), dann $[\![\varphi]\!] \subseteq [\![\psi]\!]$.*

Beweis. Wir müssen zeigen, dass die offenen Mengen von X den Schlussregeln propositionaler intuitionistischer Logik gehorchen. Etwa lautet die Interpretation der Schnittregel

$$\frac{[\![\varphi]\!] \subseteq [\![\psi]\!] \qquad [\![\psi]\!] \subseteq [\![\chi]\!]}{[\![\varphi]\!] \subseteq [\![\chi]\!]}$$

und ist offensichtlich erfüllt: Wenn $[\![\varphi]\!] \subseteq [\![\psi]\!]$ und $[\![\psi]\!] \subseteq [\![\chi]\!]$, dann auch $[\![\varphi]\!] \subseteq [\![\chi]\!]$. Die Interpretation einer der Konjunktionsregeln lautet

$$\frac{}{[\![\varphi \wedge \psi]\!] \subseteq [\![\varphi]\!]}$$

und ist ebenfalls erfüllt: Denn $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!] \subseteq [\![\varphi]\!]$. Die restlichen Fälle führen wir nicht aus. □

Eine andere Definition als die oben gegebene ist im Übrigen gar nicht möglich, wenn man möchte, dass diese Proposition gültig bleibt. Schnell kann man das wie folgt einsehen: Die Schlussregeln beschreiben *universelle Eigenschaften* für $\top$, $\bot$, $\wedge$, $\vee$ und $\Rightarrow$ und legen daher ihre Interpretationen schon eindeutig fest.

Bemerkung 3.13. Wenn man auch in der Meta-Logik konstruktiv arbeiten möchte, sollte man besser

$$[\![\varphi \Rightarrow \psi]\!] := \bigcup \{U \mid U \subseteq X \text{ offen}, U \cap [\![\varphi]\!] \subseteq [\![\psi]\!]\}$$

definieren. Da in klassischer Logik genau dann $U \subseteq V^c \cup W$, wenn $U \cap V \subseteq W$, ist diese Definition in klassischer Logik zu obiger äquivalent.

Bemerkung 3.14. Die Menge $\mathrm{Ouv}(X)$ der offenen Teilmengen von X hat die Struktur einer *Heyting-Algebra*. Etwas allgemeiner kann man Modelle intuitionistischer propositionaler Logik in beliebigen Heyting-Algebren untersuchen (und nicht nur solchen, die von topologischen Räumen stammen).

Topologische Interpretation des Prinzips vom ausgeschlossenen Dritten

Die topologische Interpretation von $\varphi \vee \neg\varphi$ ist die offene Menge

$$[\![\varphi \vee \neg\varphi]\!] = [\![\varphi]\!] \cup \mathrm{int}([\![\varphi]\!]^c),$$

also die Vereinigung von $[\![\varphi]\!]$ mit dem Inneren ihres Komplements. Es ist klar, dass diese Vereinigung in den meisten interessanten Fällen nicht gleich ganz X ist – es fehlt der Rand von $[\![\varphi]\!]$; das Prinzip vom ausgeschlossenen Dritten gilt also in den wenigsten topologischen Modellen.

Ausblick: Kategorielle Modelle für intuitionistische Prädikatenlogik

Ein Modell für intuitionistische Prädikatenlogik benötigt nicht nur Wahrheitswerte, sondern auch Objekte, aus denen die Variablenwerte gezogen werden können. Grundlage für ein solches Modell ist daher eine Kategorie, in der jeder Typ des untersuchten intuitionistischen Systems durch ein Objekt der Kategorie repräsentiert werden kann. Um die Junktoren $\wedge$, $\vee$ und $\Rightarrow$ interpretieren zu können, muss für jedes Objekt A der Kategorie die Menge der Unterobjekte von A die Struktur einer Heyting-Algebra tragen. Den All- und den Existenzquantor interpretiert man als Rechts- bzw. Linksadjungierte zu induzierten Rückzugsabbildungen.

Wichtige Beispiele für solche Kategorien sind *Topoi*. In Abschnitt 6.4 gehen wir genauer darauf ein, wie man in ihnen intuitionistische Logik interpretiert. Zur weiterführenden Lektüre eignen sich das Vorlesungsskript [49] und der Artikel [52].

4. Beziehung zur theoretischen Informatik: die Curry–Howard-Korrespondenz

Unter der Curry–Howard-Korrespondenz versteht man grob folgendes fundamentale Motto, das intuitionistische Logik und theoretische Informatik in Beziehung setzt:

Motto 4.1. *Eine Aussage φ ist genau dann intuitionistisch ableitbar, wenn es ein Computerprogramm vom Typ φ gibt.*

Hierbei wird φ einerseits als Aussage, andererseits als Typ interpretiert. Beispiele sollen diesen Doppelgebrauch deutlich machen.

4.1. Beispiele

Beispiel 1

Konstruktiv gilt offensichtlich $A \Rightarrow A$. Ein expliziter Beweis verläuft wie folgt: *Gelte A. Dann gilt A.* Wenn man dem Leser noch weiter helfen möchte, kann man den zweiten Schritt noch explizit begründen:

> *Gelte A.* $(\star)$
> *Wegen $(\star)$ gilt dann auch A.*

Man kann sich auch trauen, den gegebenen Zeugen von A mit einem Kleinbuchstaben statt einem Symbol zu bezeichnen. Dann kann man schreiben:

> *Sei $p : A$. Dann gilt $p : A$.*

Hieraus ist nun folgendes Computerprogramm ableitbar:

$$\begin{array}{rcl} A & \longrightarrow & A \\ p & \longmapsto & p \end{array}$$

Dieses Computerprogramm hat den *Typ* $(A \to A)$. Man beachte, dass dasselbe Symbol „A“ hier je nach Kontext als *Aussage* oder als *Typ* (den man sich in erster Näherung als Menge der Zeugen der Aussage A vorstellen kann) verwendet wird.

Beispiel 2

Konstruktiv gilt $A \Rightarrow (B \Rightarrow A)$. Ein Beweis verläuft wie folgt:

> *Sei $p : A$, dann ist $(B \Rightarrow A)$ zu zeigen. Sei dazu $q : B$ gegeben, dann ist A zu zeigen. Das ist klar wegen $p : A$.*

Daraus kann man folgendes Programm ableiten:

$$\begin{array}{rcl} A & \longrightarrow & B^A \\ p & \longmapsto & (q \mapsto p) \end{array}$$

Dabei bezeichnet „B^A“ den Typ der Funktionen von A nach B.

Beispiel 3

Konstruktiv gilt $A \wedge B \Rightarrow A$, mit folgendem Beweis:

> *Sei $r : (A \wedge B)$. Dann steckt in r ein Zeuge von A.*

Das zugehörige Computerprogramm lautet wie folgt:

$$\begin{array}{rcl} A \times B & \longrightarrow & A \\ (p, q) & \longmapsto & p \end{array}$$

Hierfür ist der zu $A \wedge B$ gehörige Typ $A \times B$.

Logik	Typtheorie
$\top$	Singletontyp: ()
$\bot$	leerer Typ
$\varphi \wedge \psi$	Produkttyp: $A \times B$, (A, B)
$\varphi \vee \psi$	Summentyp: $A + B$, Either A B
$\varphi \Rightarrow \psi$	Funktionstyp: B^A, $(A \to B)$
Doppelnegationsübersetzung	Continuation-Passing-Transform

Tafel 4: Einige Entsprechungen unter der Curry–Howard-Korrespondenz.

4.2. Interpretation

Die Curry–Howard-Korrespondenz hat einen ganz praktischen Nutzen: Aus intuitionistischen Beweisen kann man Computerprogramme extrahieren und umgekehrt. Beide Richtungen sind interessant: Etwa kann man offensichtlich ein Computerprogramm schreiben, das zu einer Eingabe $n : \mathbb{N}$ eine Primzahl $p \geq n$ produziert. Daher ist auch die entsprechende Aussage intuitionistisch ableitbar: $\forall n{:}\mathbb{N}.\ \exists p \geq n.\ p$ prim.

Die Umkehrung ist im Kontext formaler Methoden in der Informatik wichtig.

4.3. Genauere Formulierung

Eine genauere Formulierung ist folgende: Es gibt eine Eins-zu-Eins-Korrespondenz zwischen *Ableitungen* einer Aussage φ einerseits und *Termen* vom Typ φ andererseits. Für eine völlig präzise Formulierung muss man nur noch das gewählte Ableitungssystem und den gewählten Termkalkül sowie die Übersetzung von Aussagen zu Typen festlegen. Als Termkalkül kann man etwa den einfach getypten λ-Kalkül verwenden.

Als Korollar folgt aus der präziseren Formulierung das oben angegebene Motto: Genau dann gibt es eine Ableitung, wenn es einen entsprechenden Term gibt.

Der Beweis ist übrigens trivial, wenn man die Behauptung nur präzise genug formuliert hat. Denn die Ableitungsregeln entsprechen Eins-zu-Eins den Termkonstruktionsregeln.

Für Details sei der Übersichtsartikel [53] von Philip Wadler (einem der Väter der Programmiersprache Haskell) empfohlen. Wer die Curry–Howard-Korrespondenz wirklich verstehen möchte, kann das Vorlesungsskript [48] zurate ziehen. Es enthält auch eine Einführung in den λ-Kalkül.

5. Hilberts Programm

5.1. Die mathematische Welt um 1900 [unvollständig und fehlerhaft]

Man erzählt sich folgende Geschichte. Im letzten Viertel des 19. Jahrhunderts kamen in der Mathematik neue, abstrakte Methoden auf. Dazu gehörte vor allem Cantors

Mengenlehre, die mit ihrer Akzeptanz des *aktual Unendlichen* ein Tabu brach: Es war zwar jeder mit dem Konzept *potenzieller* Unendlichkeit vertraut, wie etwa der Vorstellung, dass die natürlichen Zahlen „nie aufhören“, dass man „immer weiter zählen könnte“. Aber manche hatten Angst davor, unendlich viele Objekte zu einer vollendeten Menge zusammenzufassen.

Insbesondere wurde die Verwendung des Prinzips

$$\neg\forall x : X.\ \neg\varphi(x) \quad \Longrightarrow \quad \exists x : X.\ \varphi(x)$$

kritisiert. Diese Kritik erscheint von unserem heutigen Standpunkt verwunderlich, denn dieses Prinzip folgt ja sofort aus dem Prinzip vom ausgeschlossenen Dritten, welches man stets als evident annahm. Man muss aber zwischen verschieden mächtigen Instanzen des Prinzips unterscheiden. Etwa ist für natürliche Zahlen n die Aussage

$$n = 0 \quad \vee \quad n \neq 0$$

völlig unkritisch, sie ist ja sogar konstruktiv beweisbar (Proposition 1.14). Die analoge Aussage für reelle Zahlen x ist zwar nicht konstruktiv haltbar, aber im 19. Jahrhundert war noch nicht der Rahmen gegeben, um das einzusehen bzw. überhaupt die Frage nach formaler konstruktiver Ableitbarkeit zu stellen. Stattdessen wurde diese Aussage ebenfalls als einleuchtend empfunden und akzeptiert.

Widerspruchsbeweise wurden also durchaus akzeptiert. (Die manchmal behauptete Aussage, klassische Schlussweisen seien erst im 20. Jahrhundert aufgekommen, ist also nicht richtig.) Angst bestand nur vor Anwendungen des Prinzips vom ausgeschlossenen Dritten in Kombination mit unendlich großen Mengen. So zerfielen die Mathematiker in zwei Lager: Solche, die neue abstrakte Methoden mit Begeisterung aufnahmen, und solche, die den neuen Entwicklungen kritisch gegenüber standen.

David Hilbert gehörte zu den Fans, nicht zuletzt deswegen, weil er selbst mit nichtkonstruktiven Methoden seinen *Basissatz* bewies, mit dem er international bekannt wurde: Dieser besagt, dass jedes Ideal des Polynomrings $k[X_1, \ldots, X_n]$ endlich erzeugt ist. Vor Hilberts Beweis war das überhaupt nicht klar, und es gab eine große Industrie, um explizit Erzeuger in konkreten Fällen zu bestimmen. Da Hilbert kein Verfahren angeben konnte, um die Erzeuger zu berechnen, sondern lediglich zeigte, dass die Annahme, es gäbe kein endliches Erzeugendensystem, zu einem Widerspruch führte, vertrat etwa Paul Gordan, der *König der Invariantentheorie*, folgende Meinung über Hilberts Resultat:

> *Das ist nicht Mathematik, das ist Theologie.*

Um seine Kritiker zufrieden zu stellen, wollte Hilbert daher zeigen, dass man die neuen abstrakten Methoden *eliminieren* konnte. Damit hat er nicht die Abschaffung derselbigen gemeint – im Gegenteil: Er wollte ihre Zulässigkeit rechtfertigen, indem er zeigen wollte, dass man aus jedem Beweis einer konkreten Aussage, der abstrakte Methoden verwendet, einen Beweis erhalten kann, der nur finitistisch zulässige Schlussweisen verwendet.

Aufgabe 5.1 (Hilberts Programm). Zeige, dass man aus jedem Beweis einer konkreten Aussage, welcher beliebige ideelle Prinzipien verwendet (etwa das Prinzip vom ausge-

schlossenen Dritten für beliebige Aussagen, das Auswahlaxiom oder maximale Ideale in der Algebra), einen finitistisch zulässigen Beweis erhalten kann.

Dabei ist eine *konkrete Aussage* eine solche, in deren Formulierung nur die natürlichen Zahlen, aber keine höheren Konzepte wie Mengen natürlicher Zahlen oder gar Mengen von Mengen vorkommen. Diese Beschränkung in Hilberts Programm ist sicherlich notwendig: Etwa kann man offensichtlich keine interessante Aussage über Mengen ohne Verwendung von Mengen beweisen.

Beispiel 5.2. Die Aussage, dass die Menge der Primzahlen nicht endlich ist, ist nicht konkret. Äquivalent ist aber die Aussage, dass zu jeder vorgegebenen Schranke eine Primzahl existiert, die größer als die Schranke ist; diese ist konkret.

In voller Allgemeinheit gilt Hilberts Programm seit 1931 als *gescheitert*. Denn in diesem Jahr veröffentlichte Gödel sein Unvollständigkeitsresultat: Die Aussage *Peano-Arithmetik ist konsistent* lässt sich als konkrete Aussage formulieren und leicht mit abstrakten Methoden beweisen (in üblicher Mengenlehre liefert die unendliche Menge $\mathbb{N}$ ein Modell), kann aber keinen finitistisch zulässigen Beweis besitzen, da es nach Gödels Unvollständigkeitssatz nicht einmal einen Beweis in der stärkeren Peano-Arithmetik geben kann.

Teilweise kann Hilberts Programm jedoch schon realisiert werden, unter anderem in Analysis und Algebra: Mittels *proof mining* kann aus klassischen Beweisen mehr oder weniger systematisch noch konstruktiver Inhalt extrahiert werden. Dabei kann je nach Situation *konstruktiver Inhalt* etwa explizite Schranken für Konstanten, stetige (oder noch bessere) Abhängigkeit von Parametern, explizite Zeugen von Existenzbehauptungen oder Algorithmen umfassen.

Motto 5.3. *In einem* Beweis *einer Aussage steckt viel mehr Inhalt als die bloße Information, dass die Aussage wahr ist.*

Dieses Motto ist keine tiefe Einsicht: *Natürlich* steckt in einem Beweis einer Aussage viel mehr Inhalt als in einer bloßen Wahrheitsbekundung – nämlich ein *Grund*, wieso die Aussage stimmt. Interessant ist, dass man dieses Motto auch formal ernst nehmen kann.

Siehe [54, 55, 46] für ausführlichere Darstellungen von Hilberts Programm und [36] für ein Lehrbuch zu proof mining. Einen kurzen Überblick geben auch die Vortragsfolien [2].

Später änderte Gordan übrigens seine Meinung:

> *Ich habe erkannt, dass auch Theologie nützlich sein kann.*

Bemerkung 5.4. Es ist lehrreich, Originalliteratur zu heutzutage im ersten Semester gelehrten Sätzen zu studieren. Etwa kann man in der Arbeit Bolzanos **??** zum Zwischenwertsatz Einblicke in die Haltung der damaligen Mathematiker zu Widerspruchsbeweisen und nichtkonstruktiven Methoden gewinnen. Bolzanos Beweis ist überaus verständlich geschrieben, wohl um die Rezeption seines allgemeinen Resultats zu erleichtern.

5.2. Beispiel aus der Zahlentheorie: Friedmans Trick

Definition 5.5. Die *Friedmanübersetzung* wird für eine feste Aussage F wie folgt rekursiv definiert:

$$\begin{aligned}
\varphi^F &:\equiv \varphi \vee F \text{ für atomare Aussagen } \varphi \\
\top^F &:\equiv \top \\
\bot^F &:\equiv F \\
(\varphi \wedge \psi)^F &:\equiv (\varphi^F \wedge \psi^F) \vee F \\
(\varphi \vee \psi)^F &:\equiv (\varphi^F \vee \psi^F) \vee F \\
(\varphi \Rightarrow \psi)^F &:\equiv (\varphi^F \Rightarrow \psi^F) \vee F \\
(\forall x : X.\ \varphi)^F &:\equiv (\forall x : X.\ \varphi^F) \vee F \\
(\exists x : X.\ \varphi)^F &:\equiv (\exists x : X.\ \varphi^F) \vee F
\end{aligned}$$

Wenn in F Variablen vorkommen, muss man gegebenenfalls manche Variablen umbenennen, um Variablenkollisionen zu vermeiden.

Bemerkung 5.6. Da $\neg\varphi :\equiv (\varphi \Rightarrow \bot)$, gilt $(\neg\varphi)^F \equiv (\varphi^F \Rightarrow F)$.

Aufgabe 5.7. Beweise durch Induktion über den Aussageaufbau, dass man auf die grau gesetzten Disjunktionen verzichten kann.

Satz 5.8. *(a) Sei φ eine Aussage. Dann gilt intuitionistisch: $F \Longrightarrow \varphi^F$.*

(b) Sei φ eine Aussage, in der nur $\top$, $\bot$, $\wedge$, $\vee$ und $\exists$, aber nicht $\Rightarrow$ oder $\forall$ vorkommen. Dann gilt intuitionistisch: $\varphi^F \Longleftrightarrow \varphi \vee F$.

(c) Seien φ und ψ beliebige Aussagen in einem Kontext $\vec{x}$. Wenn $\varphi \vdash_{\vec{x}} \psi$ intuitionistisch, dann auch $\varphi^F \vdash_{\vec{x}} \psi^F$ intuitionistisch.

Beweis. (a) Ist in der Variante mit den grauen Disjunktionen klar.

(b) Induktion über den Aussageaufbau.

(c) Induktion über den Aufbau intuitionistischer Ableitungen. Wie beim analogen Theorem über die Doppelnegationsübersetzung (Satz 3.4) muss man zeigen, dass die Friedmanübersetzungen der Schlussregeln gültig sind. Das ist sogar einfacher als bei der Doppelnegationsübersetzung. □

Bemerkung 5.9. Im Fall, dass intuitionistisch ableitbar ist, dass X ein bewohnter Typ ist, kann man die Disjunktion auch im $\exists$-Fall weglassen, es gilt dann also

$$(\exists x : X.\ \varphi)^F \Longleftrightarrow (\exists x : X.\ \varphi^F).$$

In der Literatur wird die Friedmanübersetzung oft ohne die Disjunktionen angegeben (weder die unnötigen grau gesetzten noch die wesentliche bei $\exists$), etwa in [20]. Das ist nur dann sinnvoll, wenn man ausschließlich bewohnte Typen zulässt.

Korollar 5.10. *Peano-Arithmetik ist für Aussagen der Form $\forall(\cdots \Rightarrow \cdots)$, wobei die Teilaussagen den Beschränkungen aus Satz 5.8(b) unterliegen müssen,* konservativ *über Heyting-Arithmetik: Aus jedem Beweis in Peano-Arithmetik lässt sich ein Beweis in Heyting-Arithmetik gewinnen.*

Beweis. Gelte $\top \vdash (\forall x : X.\ \varphi \Rightarrow \psi)$ in Peano-Arithmetik. Dann gilt auch

$$\varphi \vdash_x \psi$$

in Peano-Arithmetik; so schaffen wir den Allquantor und die Implikation weg. Nach dem Satz über die Doppelnegationsübersetzung (Satz 3.4) folgt die Ableitbarkeit der übersetzten Sequenz in Heyting-Arithmetik. Da φ und ψ den genannten Einschränkungen unterliegen, sind φ° und ψ° intuitionistisch äquivalent zu ihren Doppelnegationen (Lemma 3.6); also ist die Sequenz

$$\neg\neg\varphi \vdash_x \neg\neg\psi$$

in Heyting-Arithmetik ableitbar. Nun können wir die Friedmanübersetzung bezüglich einer erst noch unspezifizierten Aussage F anwenden. Da sich leicht die Friedmanübersetzungen der Peano-Axiome in Heyting-Arithmetik zeigen lassen, folgt die Ableitbarkeit von

$$((\varphi^F \Rightarrow F) \Rightarrow F) \vdash_x ((\psi^F \Rightarrow F) \Rightarrow F)$$

in Heyting-Arithmetik. Dass φ und ψ den genannten Einschränkungen unterliegen, können wir ein weiteres Mal ausnutzen: Heyting-Arithmetik kann die Sequenz

$$((\varphi \vee F \Rightarrow F) \Rightarrow F) \vdash_x ((\psi \vee F \Rightarrow F) \Rightarrow F)$$

zeigen. *Friedmans Trick* besteht nun darin, für F speziell ψ zu wählen. Die rechte Seite vereinfacht sich dann zu ψ, und die linke wird von φ impliziert. Wir erhalten also in Heyting-Arithmetik die Ableitbarkeit von $\varphi \vdash_x \psi$, also von $\top \vdash (\forall x : X.\ \varphi \Rightarrow \psi)$. □

Bemerkenswert ist, dass dieses Konservativitätsresultat nur eine Forderung an die Form der untersuchten Aussage stellt, nicht aber an die Form des gegebenen klassischen Beweises. Dieser kann Hilfsaussagen beliebiger Form verwenden. Somit kann man das Resultat als eine (limierte) partielle Realisierung von Hilberts Programm ansehen: Denn es besagt, dass für Aussagen der beschriebenen Form das ideelle Prinzip des ausgeschlossenen Dritten eliminiert werden kann.

Ebenso bemerkenswert ist, dass für das Konservativitätsresultat *klassische Wahrheit* der untersuchten Aussage nicht genügt. Vielmehr wird wirklich ein klassischer *Beweis* der Aussage benötigt. Gödels Unvollständigkeitssatz zufolge ist das eine echt stärkere Forderung.

Beispiel 5.11. Die Aussage der Zahlentheorie, dass es unendlich viele Primzahlen gibt, lässt sich in der Form

$$\forall n : \mathbb{N}.\ \exists p : \mathbb{N}.\ (p \geq n) \wedge (p \text{ ist prim})$$

schreiben. Zur Formalisierung der Primalitätsaussage benötigt man nur *beschränkte Allquantifikation*, für welche die Konservativitätsaussage ebenfalls gilt (Aufgabe 5.14). Also kann man aus jedem klassischen Beweis der Unendlichkeit der Primzahlen einen konstruktiven extrahieren.

Beispiel 5.12. Das Konservativitätsresultat trifft insbesondere auf Π^0_2-Aussagen zu – das sind solche der Form

$$\forall \cdots \forall\ \exists \cdots \exists\ (\cdots),$$

wobei die abschließende Teilaussage keine Quantoren mehr enthält. Zu diesen gehört die Aussage, dass eine gegebene Turingmaschine bei jeder beliebigen Eingabe schlussendlich terminiert („∀ Eingaben ∃ Stoppzeitpunkt"). Wenn man also beweisen möchte, dass eine Turingmaschine terminiert, kann man ruhigen Gewissens klassische Logik verwenden: Dabei verwendete Instanzen des ideellen Prinzips vom ausgeschlossenen Dritten lassen sich auf maschinelle Art und Weise eliminieren, sodass man automatisch auch einen konstruktiven Terminierungsbeweis erhält. Aus einem solchen kann man für jede Eingabe eine explizite Schranke für die Anzahl der bis zum Stopp benötigten Verarbeitungsschritte gewinnen.

Bemerkung 5.13. In der Toposttheorie gibt es den *Satz von Barr*, der in seiner schwachen Formulierung besagt, dass jeder Topos durch einen boolschen Topos überdeckt werden kann. Da Aussagen, die den Beschränkungen aus Satz 5.8(b) unterliegen, genau dann in einem Topos gelten, wenn sie in einem überdeckenden Topos gelten, ist der Satz von Barr eine toposttheoretische Version von Friedmans Trick. Für seinen Beweis verwendet man auch Ideen der Friedmanübersetzung, allerdings nicht angewendet auf eine bestimmte Aussage F, sondern auf eine *generische* Aussage.

Aufgabe 5.14. Eine beschränkte Allquantifikation ist eine Aussage der Form $\forall n : \mathbb{N}.\ (n \leq N \Rightarrow \varphi)$, wobei N ein Term sein muss, in dem n nicht vorkommt. Zeige, dass für solche Aussagen die Behauptungen in Lemma 3.6 und Satz 5.8(b) ebenfalls korrekt sind.

Bemerkung 5.15. Doppelnegations- und Friedmanübersetzungen sind Spezialfälle einer allgemeinen Übersetzung für beliebige *modale Operatoren* [1, 27]. Die Doppelnegationsübersetzung gehört zum Operator $\varphi \mapsto \neg\neg\varphi$, die Friedmanübersetzung zu $\varphi \mapsto (\varphi \vee F)$.

Markovs Regel

In klassischer Logik gilt *Markovs Prinzip*: Für jede Aussage φ (in der unter anderem die Variable x vorkommt) gilt

$$\neg\neg\exists x.\ \varphi \quad \Longrightarrow \quad \exists x.\ \varphi.$$

Dieses Prinzip folgt sofort aus dem Prinzip vom ausgeschlossenen Dritten. Konstruktiv lässt sich dieses Prinzip nicht zeigen (etwa liefert fast jeder Garbentopos ein Gegenbeispiel). In Heyting-Arithmetik gilt aber zumindest Markovs *Regel*:

Korollar 5.16 (Markovs Regel)**.** *Sei φ eine Aussage, die den Beschränkungen aus Satz 5.8(b) unterliegt. Wenn intuitionistisch $\vdash_{\vec{x}} \neg\neg(\exists y : \mathbb{N}.\ \varphi)$ ableitbar ist, so ist auch $\vdash_{\vec{x}} (\exists y : \mathbb{N}.\ \varphi)$ intuitionistisch ableitbar.*

Beweis. Nach Teil (c) von Satz 5.8 ist die Friedmanübersetzung der Voraussetzung $\neg\neg\exists y : \mathbb{N}.\ \varphi$ intuitionistisch ableitbar. Wegen Teil (b) ist diese äquivalent zu

$$((\exists y : \mathbb{N}.\ (\varphi \vee F)) \Rightarrow F) \Rightarrow F.$$

Wählt man daher trickreich $F :\equiv (\exists y : \mathbb{N}.\ \varphi)$, so folgt die Behauptung. Alternativ kann man auch direkt das Konservativitätsresultat 5.10 verwenden. □

Erstaunlicherweise steckt also in jedem intuitionistischen Beweis der doppelt negierten und daher eigentlich schwachen Aussage $\neg\neg(\exists y : \mathbb{N}.\ \varphi)$ wider Erwarten doch eine Konstruktionsvorschrift für ein $y : \mathbb{N}$, das φ erfüllt. Diese lässt sich rein maschinell aus einem gegebenen Beweis extrahieren, indem man den Beweis, dass Markovs Regel zulässig ist, Schritt für Schritt durchgeht.

Für ein abgerundetes Verständnis sollte man praktische Implementierungen von Markovs Regel studieren, etwa gibt es eine in Haskell von Oleg Kiselyov. Es lohnt sich, den begleitenden Artikel [35] durchzulesen, der Code ist kurz und wundersam.

5.3. Beispiel aus der Algebra: dynamische Methoden

In der kommutativen Algebra sind einige Techniken gebräuchlich, mit deren Hilfe man konkrete Aussagen beweisen kann, deren Zulässigkeit man aber nur in klassischer Logik und unter Verwendung starker Auswahlprinzipien beweisen kann. Vier Beispiele sind folgende:

- Um zu zeigen, dass ein Element x eines Rings R nilpotent ist (dass also eine gewisse Potenz x^n Null ist), genügt es zu zeigen, dass x in allen Primidealen von R liegt (siehe Proposition B.14).
- Um zu zeigen, dass ein Element x im Jacobson-Radikal liegt (dass also $1 - rx$ für alle $r \in R$ invertierbar ist), genügt es zu zeigen, dass x in allen maximalen Idealen von R liegt.
- Um zu zeigen, dass ein Element x eines Körpers K ganz über einem Unterring R ist, genügt es zu zeigen, dass x in allen Bewertungsringen liegt.
- Um zu zeigen, dass zwischen Polynomen $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$, wobei K ein algebraisch abgeschlossener Körper ist, eine Relation der Form $1 = p_1 f_1 + \cdots + p_m f_m$ besteht, genügt es zu zeigen, dass die f_i keine gemeinsame Nullstelle besitzen.

Mit sog. *dynamischen Methoden* kann man aus Beweisen, die diese Prinzipien verwenden, noch konstruktiven Inhalt retten. Siehe [23, 22] für relevante Originalartikel und [21, 39] für Vortragsfolien zum Thema.

Standardbeispiel: Nilpotente Polynome

Die Nützlichkeit des Nilpotenzkriteriums wird oft an folgendem Standardbeispiel demonstriert. Alle benötigten Vorkenntnisse aus der Idealtheorie sind in Anhang B zusammengefasst.

Proposition 5.17 (auch konstruktiv)**.** *Sei $f \in R[X]$ ein Polynom über einem Ring R. Dann gilt:*

$$f \text{ ist nilpotent} \quad \Longleftrightarrow \quad \text{alle Koeffizienten von } f \text{ sind nilpotent.}$$

Beweis (nur klassisch). Die Rückrichtung ist einfach: Sei $f = \sum_{i=0}^{n} a_i X^i$ mit $a_i^m = 0$ für alle $i = 0, \ldots, n$. Dann überzeugt man sich durch Ausmultiplizieren und dem Schubfachprinzip, dass die Potenz $f^{(m-1)(n+1)+1}$ Null ist.

Interessant ist die Hinrichtung. Gelte $f^m = 0$. Sei ein beliebiges Primideal $\mathfrak{p} \subseteq R$ gegeben. Dann liegen alle Koeffizienten von f^m in $\mathfrak{p}$. Nach einem allgemeinem Lemma (Lemma B.16) liegen dann schon alle Koeffizienten von einem der Faktoren, also von f, in $\mathfrak{p}$. Das zeigt schon die Behauptung. □

Der Beweis gelingt also völlig mühelos: Man muss nur das Nilpotenzkriterium (Proposition B.14) und das auch anderweitig nützliche Lemma B.16 verwenden. Allerdings ist der Beweis in dieser Form *ineffektiv*: Man erhält keine Abschätzung der Nilpotenzindizes der Koeffizienten, also der minimal möglichen Exponenten m_i mit $a_i^{m_i} = 0$. Auch ist die Abhängigkeit der m_i von den Daten nicht klar: Gibt es eine universelle Schranke, die für jeden Ring und jedes Polynom gültig wäre? Oder kann der Nilpotenzindex bei schlimmen Ringen oder Polynomen beliebig hoch werden?[2]

Diese Fragen könnte man durch eine manuelle Untersuchung, etwa mit verschachtelten Induktionsbeweisen, klären. Es gibt aber auch ein systematisches Verfahren, das ganz ohne weitere Arbeit direkt aus obigem Beweis die gesuchten Schranken extrahiert. Der Schlüssel zu diesem Verfahren liegt in folgender Erkenntnis: Der Beweis verwendet gar nicht die speziellen Eigenschaften der Primideale des Rings R (welche das auch immer sein mögen). Stattdessen verwendet er nur die *allgemeinen Primidealaxiome*. Gewissermaßen zeigt er also nicht nur, dass die Koeffizienten in allen Primidealen enthalten sind, sondern dass sie in *dem generischen Primideal* enthalten sind.

Motto 5.18. *Die* generische *Verwendung ideeller Konzepte (Primideale, maximale Ideale, Bewertungen, ...) lässt sich eliminieren.*

[2] Zumindest diese Sorge kann man mit furchtloser Anwendung von etwas Ringtheorie zerstreuen: Über dem speziellen Ring $S := \mathbb{Z}[A_0, \ldots, A_n]/(A_0^{m_0}, \ldots, A_n^{m_n})$ gibt es das *universelle Polynom* $f_{\text{univ}} := \sum_{i=0}^{n} A_i X^i$. *Universell* heißt es deswegen, da es zu jedem Polynom der Form $f = \sum_{i=0}^{n} a_i X^i$ über einem beliebigen Ring R, dessen Koeffizienten die Gleichungen $a_i^{m_i} = 0$ erfüllen, genau einen Ringhomomorphismus $\varphi : S \to R$ mit $\varphi(f_{\text{univ}}) = f$ gibt. (Dieser schickt die Unbestimmte A_i auf den konkreten Wert a_i.) Jedes solche Polynom ist also Bild des universellen Polynoms. Nach der Proposition gibt es nun einen Exponenten m mit $f_{\text{univ}}^m = 0$, der nur von n und den Exponenten m_i, nicht aber von den Werten der a_i eines solchen Polynoms f abhängen kann. Es folgt $f^m = \varphi(f_{\text{univ}})^m = \varphi(f_{\text{univ}}^m) = \varphi(0) = 0$.

Axiomatisierung des generischen Primideals

Sei R ein Ring.

Definition 5.19. Die Axiome für das *generische Primideal* sind folgende (lese „$Z(x)$“ als „$x \in \mathfrak{p}$“).

1. $\top \vdash Z(0)$.
2. $Z(x) \wedge Z(y) \vdash Z(x+y)$ für alle $x, y \in R$.
3. $Z(x) \vdash Z(rx)$ für alle $r, x \in R$.
4. $Z(1) \vdash \bot$.
5. $Z(xy) \vdash Z(x) \vee Z(y)$ für alle $x, y \in R$.

Satz 5.20. *Aus einem Beweis der Sequenz*

$$Z(a_1) \wedge \cdots \wedge Z(a_n) \vdash Z(b)$$

welcher als sprachliche Mittel nur $\top$, $\bot$, $\wedge$ und $\vee$, nicht aber $\Rightarrow$ oder die Quantoren, und als Schlussregeln neben den Axiomen aus Definition 5.19 nur die strukturellen Regeln und die Regeln für Konjunktion und Disjunktion verwendet (siehe Tafel 2 auf Seite 20), kann man einen expliziten Zeugen der Aussage

$$b \in \sqrt{(a_1, \ldots, a_n)}$$

extrahieren (siehe Definitionen B.6 und B.17 für die Notation), also eine natürliche Zahl $m \geq 0$ und Ringelemente $u_1, \ldots, u_n \in R$ mit

$$b^m = u_1 a_1 + \cdots + u_n a_n.$$

Der Satz ist eine beeindruckende Demonstration von Motto 5.3, dem zufolge in Beweisen viel mehr Inhalt steckt als die bloße Information über die Wahrheit der Behauptung. Bevor wir den Beweis des Satzes führen (welcher erstaunlich einfach ist), wollen wir das Resultat noch genauer diskutieren.

Korollar 5.21. *Aus einem Beweis der Sequenz*

$$\top \vdash Z(x)$$

folgt die Nilpotenz von x, und man kann sogar eine explizite Schranke für den Nilpotenzindex von x, d. h. eine Zahl $m \geq 0$ mit $x^m = 0$, extrahieren.

Beweis des Korollars. Mit den Axiomen kann man die Äquivalenz von $\top$ mit $Z(0)$ zeigen. Nach dem Satz folgt daher, dass man einen expliziten Zeugen der Zugehörigkeit $x \in \sqrt{(0)}$ extrahieren kann. □

Mit der Interpretation des Korollars und des Satzes muss man ein wenig vorsichtig sein. Die Aussage ist *nicht*, dass aus der Zugehörigkeit von x zu allen Primidealen konstruktiv die Nilpotenz von x folgt. Diese stärkere Aussage kann man (bewiesenermaßen) nur in einem klassischen Rahmen zeigen. Man kann lediglich aus einem entsprechend formalisierten *Beweis*, dass x in allen Primidealen enthalten ist, die Nilpotenz von x folgern.

Bemerkung 5.22. Man kann sich die Frage stellen, ob das generische Primideal durch ein gewöhnliches Primideal realisiert werden kann, ob es also ein Primideal $\mathfrak{p} \subseteq R$ gibt, das genau die Eigenschaften hat, die auch das generische Primideal hat. Das ist nicht zu erwarten – jedes konkrete Primideal kann nicht die Vorstellung des generischen Primideals fassen – und in der Tat im Allgemeinen auch nicht der Fall. Denn wenn ein Primideal $\mathfrak{p}$ für alle $x \in R$ die Äquivalenz

$$x \in \mathfrak{p} \quad \Longleftrightarrow \quad \top \vdash Z(x)$$

erfüllt, gilt schon $\mathfrak{p} = \sqrt{(0)} =$ (Ideal aller nilpotenten Elemente). Also ist jeder Nullteiler in R nilpotent. Das ist aber eine besondere Eigenschaft, die nur wenige Ringe haben. (Etwa ist in $\mathbb{Z} \times \mathbb{Z}$ das Element $(1, 0)$ ein Nullteiler, aber nicht nilpotent. In der algebraischen Geometrie lernt man, dass ein Ring R genau dann diese besondere Eigenschaft hat, wenn sein Spektrum als topologischer Raum irreduzibel ist.) Wenn man das generische Primideal unbedingt durch ein tatsächliches Ideal realisieren möchte, muss man bereit sein, den Topos zu wechseln.[3]

Bemerkung 5.23. Die Beschränkungen in Satz 5.20 an die Form des gegebenen Beweises sind unnötig restriktiv, insbesondere können anders als dort beschrieben durchaus Quantoren verwendet werden. Das diskutieren wir im übernächsten Abschnitt.

Beweis des Satzes

Beweis von Satz 5.20. Wir geben ein explizites *Modell* des in der Formulierung des Satzes beschriebenen Axiomensystems an. Die Aussagen φ der Sprache wollen wir als gewisse Radikalideale $[\![\varphi]\!] \subseteq R$ interpretieren, die Ableitungsrelation $\vdash$ als umgekehrte

[3] In dem Topos der Garben auf $\operatorname{Spec} R$ gibt es den Ring $\underline{R}$, auf offenen Mengen U definiert durch $\Gamma(U, \underline{R}) := \{f : U \to R \mid f \text{ stetig}\}$, wobei man R mit der diskreten Topologie versieht. In diesem kann man das Ideal Z, definiert durch $\Gamma(U, Z) := \{f \in \Gamma(U, \underline{R}) \mid f(\mathfrak{p}) \in \mathfrak{p} \text{ für alle } \mathfrak{p} \in U\}$, betrachten. Mit den Regeln der Kripke–Joyal-Semantik kann man nun nachrechnen, dass für Ringelemente $a_1, \ldots, a_n, b \in R$ genau dann in der internen Sprache die Implikation

$$\operatorname{Spec} A \models a_1, \ldots, a_n \in Z \Rightarrow b \in Z$$

gilt, wenn $b \in \sqrt{(a_1, \ldots, a_n)}$. Also ist das Ideal Z im Topos der Garben auf $\operatorname{Spec} R$ eine Verkörperung des generischen Primideals. Die Lokalisierung von $\underline{R}$ an diesem Primideal ist übrigens die Strukturgarbe $\mathcal{O}_{\operatorname{Spec} R}$. XXX

Idealinklusion. Lemma B.20 ist für das Verständnis der folgenden Übersetzungstabelle hilfreich. Konkret definieren wir

$$\begin{aligned}
[\![Z(x)]\!] &:= \sqrt{(x)} \\
[\![\top]\!] &:= \sqrt{(0)} \\
[\![\bot]\!] &:= (1) \\
[\![\varphi \wedge \psi]\!] &:= \sup\{[\![\varphi]\!], [\![\psi]\!]\} = \sqrt{[\![\varphi]\!] + [\![\psi]\!]} \\
[\![\varphi \vee \psi]\!] &:= \inf\{[\![\varphi]\!], [\![\psi]\!]\} = [\![\varphi]\!] \cap [\![\psi]\!]
\end{aligned}$$

und

$$\varphi \models \psi \quad :\Longleftrightarrow \quad [\![\varphi]\!] \supseteq [\![\psi]\!].$$

Dann kann man nachrechnen, dass diese semantisch definierte Relation $\models$ die geforderten Axiome erfüllt. Etwa gilt

$$\begin{aligned}
Z(x) \wedge Z(y) \models Z(x+y), &\quad \text{denn } \sqrt{\sqrt{(x)} + \sqrt{(y)}} \supseteq \sqrt{(x+y)}, \text{ und} \\
Z(xy) \models Z(x) \vee Z(y), &\quad \text{denn } \sqrt{(xy)} \supseteq \sqrt{(x)} \cap \sqrt{(y)},
\end{aligned}$$

die restlichen Nachweise sparen wir hier aus. Jeden Beweis, der nur die angegebenen Schlussregeln verwendet, kann man also in der Menge der Radikalideale nachbauen. Nun ist es leicht, die Behauptung zu zeigen:

$$\begin{aligned}
Z(a_1) \wedge \cdots \wedge Z(a_n) \vdash Z(b) &\Longrightarrow [\![Z(a_1) \wedge \cdots \wedge Z(a_n)]\!] \models [\![Z(b)]\!] \\
&\Longleftrightarrow \sqrt{(b)} \subseteq \sqrt{(a_1, \ldots, a_n)} \\
&\Longleftrightarrow b^m = u_1 a_1 + \cdots + u_n a_n \\
&\qquad \text{für gewisse } m \geq 0,\ u_1, \ldots, u_n \in R. \qquad \square
\end{aligned}$$

Nur zur Illustration wollen wir auch noch einen Alternativbeweis des Satzes führen, welcher die speziellen Möglichkeiten klassischer Logik nutzt, daher keinen expliziten Zeugen liefert und somit völlig witzlos ist:

Beweis von Satz 5.20 (nur klassisch). Da die einzelnen Axiome des generischen Primideals von jedem tatsächlichen Primideal $\mathfrak{p}$ erfüllt werden, folgt aus dem gegebenen Beweis von $Z(a_1) \wedge \cdots \wedge Z(a_n) \vdash Z(b)$, dass für jedes Primideal $\mathfrak{p}$ die Implikation

$$a_1, \ldots, a_n \in \mathfrak{p} \quad \Longrightarrow \quad b \in \mathfrak{p}$$

gilt. In klassischer Logik folgt daraus die Behauptung: Für $n = 0$ ist das gerade die Aussage der nur klassisch gültigen Proposition B.14; für $n > 0$ ist das ebenfalls eine Standardaussage aus kommutativer Algebra (welche man mit Übergang zum Faktorring $R/(a_1, \ldots, a_n)$ durch Rückführung auf den Spezialfall beweist). $\square$

Ausführliches Beispiel

Um die Wirkungsweise der Zeugenextraktion zu verstehen, wollen wir ein Beispiel diskutieren: Wir wollen durch Introspektion eines Beweises der für beliebige Primideale $\mathfrak{p}$ und Ringelemente a, b gültigen Implikation

$$ab^2,\ 1-a,\ ba+b-a \in \mathfrak{p} \quad \Longrightarrow \quad b-a \in \mathfrak{p}$$

auf maschinelle Art und Weise einen expliziten Zeugen der Implikation gewinnen. Wir untersuchen dazu folgenden Beweis, der der Einfachheit halber in informaler Sprache wiedergegeben ist, prinzipiell aber in dem benötigten logischen Fragment formuliert werden könnte.

> Da $ab^2 \in \mathfrak{p}$, gilt $a \in \mathfrak{p}$ oder $b^2 \in \mathfrak{p}$ und wir können eine Fallunterscheidung führen: Falls $a \in \mathfrak{p}$, folgt $1 = a+(1-a) \in \mathfrak{p}$ (da $(1-a) \in \mathfrak{p}$). Dieser Fall kann also nicht eintreten, oder anders formuliert: Daraus folgt trivialerweise $b-a = (b-a)\cdot 1 \in \mathfrak{p}$.
>
> Falls $b^2 \in \mathfrak{p}$, folgt $b \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ und wir können eine Fallunterscheidung führen: Falls $b \in \mathfrak{p}$, folgt $b-a = (ba+b-a)+(-a)b \in \mathfrak{p}$ (da $(ba+b-a) \in \mathfrak{p}$). Der zweite Fall geht genau gleich.

In Abbildung 2 ist der Beweisverlauf grafisch dargestellt. Zu jedem einzelnen Beweisschritt können wir nun auf rein maschinelle Art und Weise Zeugen angeben und so einen Zeugen für die gesamte Behauptung erhalten.

Zeuge für $a \in \mathfrak{p} \Longrightarrow (b-a) \in \mathfrak{p}$:

$$b-a = (b-a)\cdot(a+(1-a)) =: x(a).$$

Zeuge für $b \in \mathfrak{p} \Longrightarrow (b-a) \in \mathfrak{p}$:

$$b-a = (ba+b-a)+(-a)b =: y(b).$$

Zeuge für $b^2 \in \mathfrak{p} \Longrightarrow (b-a) \in \mathfrak{p}$:

$$\begin{aligned}(b-a)^2 &= y(b)\cdot y(b) = (ba+b-a)^2 + 2(ba+b-a)(-a)b + a^2b^2 \\ &= (b-a-ab)\cdot(ba+b-a) + a^2b^2 =: z(b^2).\end{aligned}$$

Zeuge für $(b-a) \in \mathfrak{p}$:

$$(b-a)^3 = (b-a)\cdot(b-a)^2 = x(a)\cdot z(b^2) = \cdots .$$

Multiplizieren wir den Ausdruck $x(a)\cdot z(b^2)$ aus, erhalten wir eine Darstellung von $(b-a)^3$ als Summe von Vielfachen von ab^2, $1-a$ und $ba+b-a$. Diese Darstellung ist der gesuchte explizite Zeuge der Implikation.

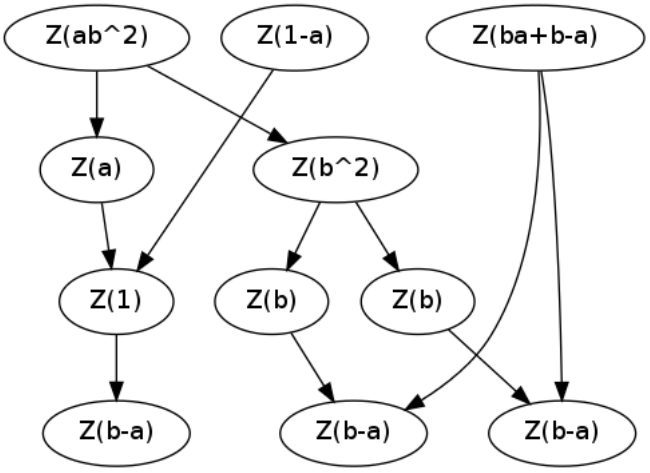


Abbildung 2: Grafische Darstellung des Beispielbeweises.

Erweiterungen

Satz 5.20 hat gezeigt, dass man die klassische Vorgehensweise

> *Um zu zeigen, dass ein Element $x \in R$ nilpotent ist, zeige, dass es in allen Primidealen liegt.*

konstruktiv rechtfertigen kann – obwohl konstruktiv nicht bewiesen werden kann, dass der Schnitt aller Primideale nur die Menge der nilpotenten Elemente ist. Klassisch gibt es aber auch noch folgendes stärkeres Prinzip:

Lemma 5.24 (in dieser Form nur klassisch)**.** *Sei $x \in R$ ein Element eines Rings R. Wenn x in jedem algebraisch abgeschlossenen Oberkörper von R Null ist, wenn also für jeden Ringhomomorphismus $\varphi : R \to K$, wobei K ein algebraisch abgeschlossener Körper ist, das Element $\varphi(x) \in K$ Null ist, dann ist x nilpotent.*

In diesem Abschnitt wollen wir zeigen, dass auch dieses Prinzip in einem konstruktiven Kontext verwendbar ist – obwohl die Existenz algebraischer Abschlüsse, und schon die Existenz von Zerfällungskörpern, konstruktiv eine diffizile Angelegenheit ist. In diesem Abschnitt setzen wir etwas mehr Vorwissen aus kommutativer Algebra voraus.

Beweis des Lemmas (nur klassisch). Wir weisen nach, dass x in allen Primidealen von R liegt, klassisch genügt das ja. Sei also $\mathfrak{p}$ ein beliebiges Primideal. Dann ist der Faktorring $R/\mathfrak{p}$ ein Integritätsbereich und wir können seinen Quotientenkörper betrachten. Diesen wiederum können wir in einen algebraisch abgeschlossenen Oberkörper K einbetten (hier geht klassische Logik ein). Wir haben also Ringhomomorphismen

$$R \longrightarrow R/\mathfrak{p} \hookrightarrow \mathrm{Quot}(R/\mathfrak{p}) \hookrightarrow K.$$

Nach Voraussetzung ist das Bild von x in K Null. Daher ist auch das Bild von x in $\mathrm{Quot}(R/\mathfrak{p})$ Null, somit auch das Bild von x in $R/\mathfrak{p}$, und daher liegt x in $\mathfrak{p}$. □

Die konstruktive Umsetzung dieses Prinzips im Rahmen der dynamischen Methoden ist folgende:

Satz 5.25. *Aus einem Beweis der Sequenz*

$$Z(a_1) \wedge \cdots \wedge Z(a_n) \vdash Z(b)$$

welcher als sprachliche Mittel nur $\top$, $\bot$, $\wedge$, $\vee$ sowie $\exists$, nicht aber $\Rightarrow$, und als Schlussregeln

1. *die Axiome aus Definition 5.19 (jetzt in beliebigen Kontexten, nicht nur im leeren),*
2. *$\top \vdash_{\vec{x}} Z(s) \vee (\exists y.\ Z(1 - sy))$ für alle Terme s im Kontext $\vec{x}$ (also etwa Elemente von R),*
3. *$\top \vdash_{\vec{x}} \exists y.\ Z(y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0)$ für alle $n \geq 1$ und $a_0, \ldots, a_{n-1}$ Terme im Kontext $\vec{x}$ und*
4. *die strukturellen Regeln, die Regeln für Konjunktion, Disjunktion und Existenzquantifikation*

verwendet, kann man einen expliziten Zeugen der Aussage

$$b \in \sqrt{(a_1, \ldots, a_n)} \subseteq R$$

extrahieren.

Die anschauliche Bedeutung von „$Z(x)$“ ist nun, dass x im generischen algebraisch abgeschlossenen Oberkörper von R Null ist. Axiom 2 drückt aus, dass in diesem Oberkörper jedes Element Null oder invertierbar ist. Axiom 3 besagt, dass jedes normierte und nichtkonstante Polynom über R eine Nullstelle im Oberkörper besitzt.

Beweis. Die Idee ist wieder, ein Modell anzugeben. Die Interpretation einer Aussage im Kontext $x_1, \ldots, x_n$ soll dabei ein Radikalideal im Polynomring $R[x_1, \ldots, x_n]$ in n formalen Variablen sein. Neu zu definieren ist

$$[\![\exists y.\ \varphi]\!]_{\vec{x}} := R[x_1, \ldots, x_n] \cap [\![\varphi]\!]_{\vec{x},y}.$$

Auf der rechten Seite ist dabei $[\![\varphi]\!]$ ein Radikalideal in $R[x_1, \ldots, x_n, y]$. Damit kann man alle nötigen Nachweise führen. Dazu ist die Identität $[\![\varphi]\!]_{\vec{x},y} = \sqrt{[\![\varphi]\!]_{\vec{x}} R[x_1, \ldots, x_n, y]}$ für Aussagen φ im Kontext $\vec{x}$ hilfreich, welche man mit Induktion beweisen kann. □

6. Ein topostheoretischer Zugang zu Quantenmechanik: der Bohr-Topos

Als Anwendung konstruktiver Mathematik wollen wir einen topostheoretischen Zugang zu (manchen Grundlagen von) Quantenmechanik vorstellen. Dieser geht auf eine wegweisende Arbeit von Jeremy Butterfield, John Hamilton und Chris Isham zurück [14],

welche dann von weiteren mathematischen Physikern, unter anderen Andreas Döring, Chris Heunen und Nicolaas Landsman, sowie den konstruktiven Mathematikern Thierry Coquand und Bas Spitters aufgegriffen wurde. Unsere Darstellung ist im Wesentlichen eine Zusammenfassung der Artikel [31] und [15]. Ein genauerer Abriss der Entwicklung findet sich in [15] und den dort genannten Referenzen.

Die grundlegende Idee ist folgende: Klassisch-mechanische Systeme können durch kommutative C*-Algebren und dazugehörige Phasenräume beschrieben werden. Die C*-Algebra zu quantenmechanischen Systemen ist dagegen im Allgemeinen nichtkommutativ und die schöne Idee eines Phasenraums bricht zusammen. Man kann nun das das mathematische Universum, in dem man arbeitet, wechseln; ein geeignetes Alternativuniversum enthält ein Abbild der nichtkommutativen C*-Algebra, welches dort kommutativ erscheint und dort auch einen Phasenraum zulässt. In diesem (restriktiven) Sinn wird Quantenmechanik in diesem anderen Universum zu klassischer Mechanik.

Um diesen Ansatz zu verstehen, sind drei Zutaten nötig: die Dualität zwischen Räumen und Algebren; eine für diese Zwecke geeignete Formulierung von klassischer Mechanik und Quantenmechanik; und die Auffassung von Topoi als mathematische Alternativuniversen. Diese Zutaten wollen wir in den folgenden Abschnitten grob umreißen.

6.1. Gelfand-Dualität zwischen topologischen Räumen und C*-Algebren

Grundlegend für das Wechselspiel zwischen Geometrie und Algebra ist folgende Erkenntnis: Einem geometrischen Objekt X kann man die Menge der (reellwertigen, komplexwertigen, allgemeineren) Funktionen auf X zuordnen. Diese Menge trägt algebraische Struktur (ist etwa durch punktweise Operationen ein Ring) und kann daher mit Mitteln der Algebra untersucht werden. Dabei besteht die Hoffnung, dadurch etwas über X zu lernen; in guten Fällen legt die Algebra von Funktionen das geometrische Objekt X sogar schon eindeutig fest.

Dieses Motto hat in mehreren Teilgebieten der Mathematik konkrete Ausprägungen. Etwa ist in algebraischer Geometrie folgende Proposition fundamental:

Proposition 6.1. *Die Kategorie der affinen Schemata ist dual äquivalent zur Kategorie der Ringe:*

$$\begin{array}{rcl} (\text{Kat. der affinen Schemata})^{\text{op}} & \simeq & (\text{Kat. der Ringe}) \\ X & \mapsto & \Gamma(X, \mathcal{O}_X) = \text{Ring der regulären Funktionen auf } X \\ \text{Spektrum von } A & \leftarrow\!\shortmid & A \end{array}$$

Für unsere Zwecke ist die *Gelfand-Dualität* wichtig, die zwischen kompakten Hausdorffräumen einerseits und C*-Algebren andererseits vermittelt.

Definition 6.2. Eine C*-Algebra A ist ein Banachraum über $\mathbb{C}$ (also ein vollständiger normierter Vektorraum über $\mathbb{C}$) zusammen mit einer Multiplikationsoperation $A \times A \to A$ und einer Involution $(\_)^* : A \to A$, sodass gewisse natürliche Axiome erfüllt sind.

Prototypbeispiele für C*-Algebren sind $\mathbb{C}$ mit der komplexen Konjugation als Involution und $L(H,H) = \{f : H \to H \mid f \text{ linear und stetig}\}$ mit der Zuordnung $f \mapsto f^\star$ (adjungierter Operator zu f) als Involution. Siehe [30] für eine Einführung in die Theorie der C*-Algebren.

Satz 6.3 (Gelfand-Dualität, so nur klassisch)**.** *Die Kategorie der kompakten Hausdorffräume ist dual äquivalent zur Kategorie der kommutativen C*-Algebren (mit Eins):*

$$\begin{array}{rcl} (\text{Kat. der kompakten Hausdorffräume})^{\text{op}} & \simeq & (\text{Kat. der kommutativen C}^*\text{-Algebren}) \\ X & \mapsto & C(X,\mathbb{C}) = \{f : X \to \mathbb{C} \mid f \text{ stetig}\} \\ \operatorname{Spec} A & \leftarrow\!\shortmid & A \end{array}$$

Dabei wird $C(X,\mathbb{C})$ vermöge der punktweisen Addition, Multiplikation und Konjugation sowie der Supremumsnorm zu einer C-Algebra. Die Punkte von* Spec A *sind genau die C*-Algebrenhomomorphismen $A \to \mathbb{C}$.*

Beweis. Führt hier zu weit. Wir wollen nur anmerken, dass der Homöomorphismus $X \to \operatorname{Spec} C(X,\mathbb{C})$ durch $x \longmapsto \_(x)$ mit $\_(x) = (f \mapsto f(x))$ gegeben ist. An einer Stelle im Beweis muss man geeignete Algebrenhomomorphismen $A \to \mathbb{C}$ konstruieren; dazu benötigt man das Auswahlaxiom. □

Unter der Korrespondenz des Satzes entsprechen die selbstadjungierten Elemente $a \in A$ gerade den stetigen Abbildungen $X \to \mathbb{R}$.

Bemerkung 6.4. Die Gelfand-Dualität liefert einen Ansatz für *nichtkommutative Geometrie*: Wie man die Definition eines topologischen Raums abändern sollte, sodass sie nicht mehr „kommutativ“ wäre, ist völlig unklar, denn in der Definition kommen ja gar keine binären Verknüpfungen vor. Auf der algebraischen Seite ist es dagegen einfach. Daher kann man das formale Duale zur Kategorie der (nicht notwendigerweise kommutativen) C*-Algebren als erste Approximation für eine Kategorie nichtkommutativer Räume verwenden.

6.2. Örtlichkeiten für punktfreie Topologie

In der obigen Formulierung gilt die Gelfand-Dualität leider nur in einem klassischen Kontext. Da wir sie später in einem alternativen Mathematik-Universum (dem Bohr-Topos zu einer nichtkommutativen C*-Algebra) nutzen möchten, in dem das Auswahlaxiom unabhängig von unseren philosophischen Vorlieben schlichtweg *nicht gilt*, ist das unzureichend. Im Zeitraum von etwa 20 Jahren wurde glücklicherweise auch folgende konstruktiv zulässige Variante entwickelt:

Satz 6.5 (auch konstruktiv)**.** *Die Kategorie der kompakten und vollständig regulären Örtlichkeiten (Locales) ist dual äquivalent zur Kategorie der kommutativen C*-Algebren. Dabei geht analog zur klassischen Formulierung eine Örtlichkeit X auf die Algebra der stetigen Abbildungen $X \to \mathbb{C}$. (Auf die hierfür nötige konstruktiv geeignete Definition der komplexen Zahlen gehen wir nicht ein.)*

Dabei ist das Konzept einer *Örtlichkeit* (Locale) eine milde Verallgemeinerung des Konzepts eines topologischen Raums, bei dem *Punkte* nicht im Vordergrund stehen: Während ein topologischer Raum bekanntlich durch eine Menge von Punkten sowie der Deklaration gewisser Mengen von Punkten als offen gegeben ist, besteht eine Örtlichkeit nur aus der Angabe von gewissen *offenen Dingen*, welche nicht notwendigerweise Mengen von Punkten sein müssen. Von den offenen Teilmengen eines topologischen Raums schaut man sich die Axiome ab, die die offenen Dinge einer Örtlichkeit erfüllen sollen:

Definition 6.6. Eine *Örtlichkeit* X besteht aus einem Verband $\mathrm{Ouv}(X)$ *offener Dinge* (also einer Halbordnung zusammen mit Operationen $\wedge$ und $\vee$, die geeignete Axiome erfüllen), in dem zusätzliche beliebige Suprema existieren und für diese folgendes Distributivgesetz gilt:

$$u \wedge \bigvee_i v_i = \bigvee_i (u \wedge v_i).$$

Beispiel 6.7. Jeder topologischer Raum X liefert ein Beispiel für eine Örtlichkeit X mit $\mathrm{Ouv}(X) = \{U \subseteq X \mid U \text{ offen}\}$ und $\wedge = \cap$, $\vee = \cup$, $\bigvee = \bigcup$.

Beispiel 6.8. Speziell ist der einpunktige Raum pt als Örtlichkeit durch $\mathrm{Ouv}(\mathrm{pt}) = \mathcal{P}(\{\star\})$ gegeben.

Das Konzept eines Punkts ist in der Theorie der Örtlichkeiten nicht grundlegend, kann aber sehr wohl definiert werden: Ein *Punkt* einer Örtlichkeit X ist ein Morphismus $\mathrm{pt} \to X$ von Örtlichkeiten. Die Menge aller Punkte einer Örtlichkeit kann man mit einer natürlichen Topologie versehen; der so entstehende topologische Raum spiegelt aber nur dann die Örtlichkeit getreu wieder, wenn diese *räumlich* war. Insbesondere gibt es nichttriviale und interessante Örtlichkeiten, die keinen einzigen Punkt besitzen: Die Vorstellung eines Punkts ist gewissermaßen ein ideelles und schwerer fassbares Konzept als das eines offenen Teils eines Raums. Auch, wenn es einem Raum an Punkten mangelt, kann man manchmal dennoch von offenen Teilbereichen sprechen.

Beispiel 6.9. Folgende Örtlichkeiten sind nichttrivial und besitzen keine Punkte: die Örtlichkeit aller Surjektionen $\mathbb{N} \twoheadrightarrow \mathbb{R}$, die Örtlichkeit aller zufälligen 0/1-Folgen [**random**], der örtlichkeitstheoretische Schnitt beliebig vieler dichter Unterörtlichkeiten einer nichttrivialen Örtlichkeit.

Umgekehrt spiegelt auch die Örtlichkeit zu einem topologischen Raum diesen nur dann getreu wieder, wenn dieser *nüchtern* war. Jeder Hausdorffraum ist nüchtern (in klassischer Logik). Stattet man aber etwa eine aus mehr als nur einem Element bestehende Menge mit der indiskreten Topologie aus, erhält man einen topologischen Raum, der nicht nüchtern ist: Die Vielzahl seiner Punkte schlägt sich nicht in seiner Topologie nieder. Seine *Nüchternifizierung* (*Ausnüchterung*?) ist der einpunktige Raum.

Hier ist nicht der richtige Ort, um auf die vielen Vorteile (und die Nachteile) von Örtlichkeiten gegenüber topologischen Räumen einzugehen. Es sei nur erwähnt, dass durch den Wegfall von Punkten als grundlegendes Konzept diese auch seltener konstruiert

werden müssen. Da man zur Angabe spezieller Punkte oft das Auswahlaxiom oder andere klassische Prinzipien benötigt, eignen sich Örtlichkeiten also besser, wenn man solche nicht verwenden möchte oder (wie bei der Arbeit in anderen Topoi) nicht verwenden kann. Es gibt auch Vorteile, die nichts mit dem Auswahlaxiom oder Logik zu tun haben und rein topologischer Natur sind [33, 34].

Wir schließen mit einem Zitat von Alexander Grothendieck über Topoi [29], das aber genauso gut auf Örtlichkeiten anwendbar ist:[4]

> Ces "nuages probabilistes", remplaçant les rassurantes particules matérielles d'antan, me rappellent étrangement les élusifs "voisinages ouverts" qui peuplent les topos, tels des fantômes évanescents, pour entourer des "points" imaginaires, [...].

6.3. Algebraische Sicht auf klassische Mechanik und Quantenmechanik

Klassische Mechanik

Zu einem klassisch-mechanischen System gehört ein Phasenraum Σ, dessen Punkte die reinen Zustände des Systems sind.

Beispiel 6.10. Der Phasenraum des freien Teilchens im $\mathbb{R}^3$ ist $\Sigma = \mathbb{R}^3 \times \mathbb{R}^3$, denn durch Position und Impuls ist die Systemkonfiguration eindeutig festgelegt. Die beiden Projektionen $\Sigma \to \mathbb{R}^3$ sind die Observablen *Position* und *Impuls*.

Auf der algebraischen Seite gehört zum Phasenraum Σ eine C*-Algebra $A := C(\Sigma, \mathbb{C})$; es ergibt sich dann folgendes Wörterbuch zwischen Formulierungen auf der geometrischen und der algebraischen Seite [16]:

- *Reine Zustände* sind Punkte $x \in \Sigma$ oder, da $\Sigma \cong \operatorname{Spec} A$, äquivalent C*-Algebrenhomomorphismen $A \to \mathbb{C}$.
- *Gemischte Zustände* sind Wahrscheinlichkeitsmaße μ auf Σ oder äquivalent lineare Abbildungen $\rho : A \to \mathbb{C}$, welche normiert (d. h. $\rho(1) = 1$) und positiv sind (d. h. $\rho(a^\star a) \geq 0$ für alle $a \in A$). (Solche Abbildungen sind automatisch stetig.)

  Der Zusammenhang zwischen den beiden Sichtweisen wird durch

  $$\rho(f) = \int_\Sigma f(x)\, d\mu(x)$$

  für alle $f \in A$ vermittelt: Ein Wahrscheinlichkeitsmaß μ definiert über diese Setzung eine normierte, positive und lineare Abbildung; dass umgekehrt jedes

[4] „Diese ‚Wahrscheinlichkeitswolken', welche die beruhigenden materiellen Partikel von früher ersetzen, erinnern mich irgendwie an die flüchtigen ‚offenen Umgebungen' der Topoi – wie dahinschwindende Phantome, um die fiktiven ‚Punkte' zu umgeben, [...]."

solche Funktional von dieser Form ist, garantiert der Darstellungssatz von Riesz–Markov–Kakutani.

Unter dieser Korrespondenz entspricht ein reiner Zustand $x \in \Sigma$ dem in x konzentrierten Dirac-Maß bzw. der Abbildung ρ mit $\rho(f) = f(x)$.

- *Observable* sind stetige Funktionen $\Sigma \to \mathbb{R}$ oder äquivalent selbstadjungierte Elemente $a \in A$.

  Eine spezielle Observable ist die Eins von A, also die Funktion, die konstant den Wert $1 \in \mathbb{R}$ annimmt.

- Der Erwartungswert einer Observablen a in einem (gemischten) Zustand ρ ist $\rho(a)$. Ist ρ durch ein Wahrscheinlichkeitsmaß μ gegeben, lässt sich dieser Ausdruck auch als $\int_\Sigma a(x)\, d\mu(x)$ schreiben; diese Form ist vielleicht vertrauter.

  Die Forderung, dass ρ normiert ist, ist dann anschaulich: Denn der Erwartungswert der konstanten Observable $1 \in A$ sollte auch tatsächlich 1 sein.

  Ist $\rho = \_(x)$ ein reiner Zustand, so ist $\rho(a) = a(x)$ nicht nur der Erwartungswert, sondern der tatsächliche Wert von a.

Bemerkung 6.11. In Anwendungen ist der Phasenraum sogar eine (Poisson-)Mannigfaltigkeit. Diese zusätzliche Struktur sollte man nicht ignorieren. Machen wir hier aber trotzdem.

Quantenmechanik

Quantenmechanische Systeme können nicht mehr durch einen Phasenraum im traditionellen Sinn beschrieben werden. Es bleibt aber die Möglichkeit, sie durch nichtkommutative C*-Algebren zu beschreiben.

Beispiel 6.12. Wird ein System durch einen Hilbertraum H beschrieben, so ist $A := L(H, H) = \{f : H \to H \mid f \text{ linear und stetig}\}$ die zugehörige C*-Algebra.

Grundlegende Konzepte können also nicht mehr geometrisch über einen Phasenraum verstanden werden, sondern müssen algebraisch formuliert werden. In Analogie zur klassischen Situation könnte man definieren:

- *Reine Zustände* sind C*-Algebrenhomomorphismen $A \to \mathbb{C}$.
- *Gemischte Zustände* sind normierte, positive und lineare Abbildungen $A \to \mathbb{C}$.
- *Observablen* sind selbstadjungierte Elemente von A.
- Der Erwartungswert einer Observablen a in einem Zustand ρ ist $\rho(a)$.

Beispiel 6.13. Jeder reine Zustand ist auch ein gemischter Zustand, da C*-Algebrenhomomorphismen $\rho : A \to \mathbb{C}$ automatisch normiert (da sie das Einselement auf die komplexe Zahl 1 schicken müssen) und positiv sind (da $\rho(a^*a) = \rho(a)^*\rho(a) = |\rho(a)|^2 \geq 0$).

Beispiel 6.14.
- Ist $\psi \in H$ eine normierte Wellenfunktion, so ist ρ mit $\rho(a) = (\psi, a(\psi))$ ein gemischter Zustand, im Allgemeinen aber kein reiner.
- Ist $(\psi_i)_i$ eine Familie normierter Wellenfunktionen und $(p_i)_i$ eine Familie nichtnegativer Zahlen mit $\sum_i p_i = 1$, so ist ρ mit $\rho(a) = \sum_i p_i \cdot (\psi_i, a(\psi_i))$ ein gemischter Zustand.
- Ist $a : H \to H$ ein selbstadjungierter Operator, so ist $a \in A$ eine Observable.

Bei näherer Betrachtung stellt sich dieser Ansatz jedoch als zu naiv heraus. Das Problem steckt in der unscheinbaren Bedingung

$$\rho(a + b) = \rho(a) + \rho(b) \quad \text{für alle } a, b \in A$$

an gemischte Zustände ρ bzw. der analogen Forderung der Multiplikativität an reine Zustände. Man kann nämlich argumentieren [31, Seite 27], dass zwei Observable a und b nur dann physikalisch sinnvoll addierbar sind, wenn sie gemeinsam messbar sind, also miteinander kommutieren. Die mathematischen Physiker, die nicht nur vorgeben, sich mit diesem Thema auszukennen, begründen das mit einer Referenz auf Bohrs *Doktrin klassischer Konzepte*, auf die wir weiter unten eingehen. Jedenfalls sollte man besser folgende Definition treffen:

Definition 6.15. (a) Ein *reiner Quasi-Zustand* einer C*-Algebra A ist eine Abbildung $A \to \mathbb{C}$, die auf jeder kommutativen Unter-C*-Algebra $C \subseteq A$ ein C*-Algebrenhomomorphismus ist.

(b) Ein *gemischter Quasi-Zustand* einer C*-Algebra A ist eine Abbildung $A \to \mathbb{C}$, welche normiert, positiv und auf jeder kommutativen Unter-C*-Algebra $C \subseteq A$ linear ist.

Bemerkung 6.16. In der Praxis ist der Unterschied zwischen Zuständen und den besser motivierten Quasi-Zuständen nicht so groß: Denn nach Gleasons Theorem ist jeder gemischte Quasi-Zustand auf $A = L(H, H)$ mit $\dim H \geq 3$ schon ein gemischter Zustand [17].

Bemerkung 6.17. Es gibt einen Grund, wieso wir kein Beispiel eines reinen Quasi-Zustands angeführt haben: Das Kochen–Specker-Theorem besagt, dass es zumindest im interessanten Fall $A = L(H, H)$ mit $\dim H \geq 3$ keinen solchen gibt. Das hat eine physikalische Interpretation: Ein reiner Quasi-Zustand würde allen Observablen konsistente Zahlenwerte als Messwerte zuweisen. So etwas ist nicht möglich.

6.4. Topoi als mathematische Alternativuniversen

Toposttheorie hat viele Facetten. Hier betonen wir nur eine, nämlich die Auffassung von Topoi als mathematische Alternativuniversen. Unter anderem hat Toposttheorie aber auch eine geometrische Komponente: Topoi kann man als verallgemeinerte Räume ansehen. Eine informale Einführung in Toposttheorie von Tom Leinster [38] diskutiert auch diese anderen Standpunkte.

In diesem und im folgenden Abschnitt setzen wir etwas Grundkenntnisse in Kategorientheorie voraus. Alle benötigten Konzepte kann man etwa im Skript zum vorherigen Pizzaseminar [11] nachlesen. Gelegentlich werden wir auch über Garben sprechen; die wesentlichen Definitionen dazu sind in Anhang C zusammengestellt. Man kann solche Passagen aber auch überlesen.

Was ist ein Topos?

Definition 6.18. Ein *Topos* ist eine Kategorie, die endliche Limiten besitzt, kartesisch abgeschlossen ist und über einen Unterobjektklassifizierer verfügt.

Notwendig und hinreichend für die Existenz endlicher Limiten ist die Existenz von einem terminalen Objekt (einem Objekt 1, sodass für jedes Objekt X genau ein Morphismus $X \to 1$ existiert), von Produkten $X \times Y$ für je zwei Objekte X und Y und von Differenzkernen für je zwei parallele Morphismen $X \rightrightarrows Y$.

Kartesisch abgeschlossen bedeutet, dass es zu je zwei Objekten X und Y nicht nur wie in jeder Kategorie eine Menge (oder Klasse) $\mathrm{Hom}(X, Y)$ von Morphismen zwischen X und Y gibt, sondern dass man sinnvoll von einem internen *Hom-Objekt* $\underline{\mathrm{Hom}}(X, Y)$ der Kategorie sprechen kann. Das ist etwa in der Kategorie der Mengen und beinahe in der Kategorie der topologischen Räume der Fall (da man die Hom-Mengen mit einer Topologie versehen kann).

Ein *Unterobjektklassifizierer* ist ein spezielles Objekt Ω, sodass Unterobjekte eines Objekts X in Eins-zu-Eins-Korrespondenz zu Morphismen $X \to \Omega$ stehen. In der Kategorie der Mengen ist $\Omega = \mathcal{P}(\{\star\})$ ein solches, in klassischer Logik also $\Omega = \{0, 1\}$: Denn bekanntlich können Teilmengen U einer Menge X ja eindeutig durch ihre klassifizierende Abbildung $X \to \Omega,\ x \mapsto \{\star \mid x \in U\}$ (also $x \mapsto 1$, falls $x \in U$, und $x \mapsto 0$, falls $x \notin U$) beschrieben werden.

Obige Definition ist völlig korrekt, für unsere Zwecke aber aus zwei Gründen nicht gut geeignet: Zum einen ist sie nur dann anschaulich verständlich, wenn man schon einige Erfahrung mit Kategorientheorie hat. Zum anderen ist sie in einem gewissen Sinn sogar irreführend, denn ein Topos hat viel mehr Struktur, als die auf Minimalität getrimmte Definition vermuten ließe. Eine umfassendere Definition, die diese weiteren wesentlichen Strukturen nicht verschweigt, ist etwa folgende: Ein *Topos* ist eine lokal kartesisch abgeschlossene, endlich vollständige und kovollständige Heyting-Kategorie, welche exakt und extensiv ist und über einen Unterobjektklassifizierer verfügt.

Für unsere Zwecke genügen ein Motto und Beispiele für Topoi.

Motto 6.19. *Ein Topos ist eine Kategorie, die dadurch, dass sie ähnliche kategorielle Eigenschaften wie die Kategorie der Mengen hat, über eine* interne Sprache *verfügt.*

Beispiel 6.20. Archetypisches Beispiel für einen Topos ist die Kategorie Set der Mengen und Abbildungen.

Beispiel 6.21. Ist X ein topologischer Raum (oder eine Örtlichkeit), so ist die Kategorie der mengenwertigen Garben auf X und der Garbenmorphismen ein Topos. Das terminale Objekt ist die konstante Garbe $U \mapsto \{\star\}$, das initiale die Garbe $U \mapsto \{\star \,|\, U = \emptyset\}$ und der Unterobjektklassifizierer ist die Garbe $U \mapsto \{V \subseteq U \,|\, V \text{ offen}\}$.

Beispiel 6.22. Die Kategorien der Gruppen, der Vektorräume und der topologischen Räume sind keine Topoi.

Bemerkung 6.23. *Sei G eine Gruppe.* Wenn man diese Phrase liest, stellt man sich keine bestimmte Gruppe vor. Man denkt sich auch nicht: *Ich lese erst mal ohne eine Vorstellung weiter. Erst, wenn dieser Abschnitt irgendwann auf eine konkrete Gruppe angewendet wird, lese ich diese Passage mit der konkreten Gruppe im Hinterkopf erneut.* Stattdessen denkt man an die *generische Gruppe*. Möchte man dieses Konzept formalisieren, so kann man den *klassifizierenden Topos der Theorie der Gruppen* betrachten. In diesem gibt es eine bestimmte Gruppe, welche genau die Eigenschaften hat, welche alle Gruppen (in allen Topoi) haben. Im üblichen Universum, dem Topos der Mengen, lässt sich die generische Gruppe nicht auf diese Art und Weise verkörpern.

Was ist die interne Sprache?

Die interne Sprache eines Topos $\mathcal{E}$ erlaubt es, Objekte und Morphismen des Topos zu konstruieren, Eigenschaften über diese zu formulieren und gegebenenfalls solche Eigenschaften zu beweisen – und zwar in einer *naiven*, *element-basierten* Sprache, die der üblichen formalen mathematischen Sprache sehr stark ähnelt.

Etwa erscheint ein Objekt von $\mathcal{E}$, das also vielleicht eine komplizierte Garbe von Mengen ist, aus Sicht der internen Sprache wie eine gewöhnliche Menge[5]. Folgerichtig erscheint ein Morphismus von $\mathcal{E}$, der tatsächlich vielleicht ein Garbenmorphismus und daher eine komplizierte unendliche Familie von Abbildungen ist, aus Sicht der internen Sprache wie eine gewöhnliche Abbildung zwischen Mengen.

Diese Auffassung ist sehr tragfähig: Etwa sieht das initiale Objekt aus Sicht der internen Sprache auch in der Tat wie die leere Menge, ein Monomorphismus wie eine injektive Abbildung und ein Epimorphismus wie eine surjektive Abbildung aus, siehe Tafel 5.

Wichtige Eigenschaft der internen Sprache ist, dass sie *korrekt* (engl. *sound*) bezüglich konstruktiver Logik ist. Jeder konstruktive Beweis lässt sich also auch in der internen Sprache beliebiger Topoi interpretieren. Im Folgenden Abschnitt illustrieren wir das anhand des anschaulichen Garbentopos zu einem topologischen Raum.

Die interne Sprache eines Garbentopos

Sei X ein topologischer Raum (oder eine Örtlichkeit). Dann definieren wir rekursiv

$$U \models \varphi \quad (\text{„}\varphi \text{ gilt auf } U\text{“})$$

[5]Besser sollte man hier *Typ* schreiben. Auf den Unterschied wollen wir hier nicht eingehen.

externe Sicht	interne Sicht
Objekt von $\mathcal{E}$	gewöhnliche Menge
Morphismus von $\mathcal{E}$	gewöhnliche Abbildung zwischen Mengen
initiales Objekt von $\mathcal{E}$	leere Menge
terminales Objekt von $\mathcal{E}$	einelementige Menge
Unterobjektklassifizierer von $\mathcal{E}$	Menge $\mathcal{P}(\{\star\})$ der Wahrheitswerte
Monomorphismus in $\mathcal{E}$	injektive Abbildung
Epimorphismus in $\mathcal{E}$	surjektive Abbildung

Tafel 5: Externe und interne Sicht auf Objekte und Morphismen eines Topos $\mathcal{E}$.

für offene Teilmengen $U \subseteq X$ und Aussagen φ gemäß der Regeln in Tafel 6 (der *Kripke–Joyal-Semantik*).

Beispiel 6.24. Seien $s, t \in \Gamma(X, \mathcal{F})$ globale Schnitte einer Garbe $\mathcal{F}$. Dann gilt $U \models s = t$ genau dann, wenn $s|_U = t|_U$, und $U \models \neg\neg(s = t)$ genau dann, wenn es eine dichte offene Teilmenge $V \subseteq U$ mit $s|_V = t|_V$ gibt.

Auf den ersten Blick erscheinen die Regeln der Kripke–Joyal-Semantik völlig willkürlich. Tatsächlich sind sie aber fein aufeinander abgestimmt, schon kleine Änderungen führen dazu, dass das gesamte System zusammenbricht. Nur so gilt folgende grundlegende Proposition.

Satz 6.25. *Die interne Sprache von* $\mathrm{Sh}(X)$ *hat folgende Eigenschaften:*

(a) Lokalität: *Sei* $U = \bigcup_i U_i$ *eine offene Überdeckung. Dann gilt genau dann* $U \models \varphi$*, wenn für alle* i *jeweils* $U_i \models \varphi$ *gilt.*

(b) Korrektheit: *Wenn* $U \models \varphi$ *und intuitionistisch* $\varphi \vdash \psi$ *ableitbar ist, dann gilt auch* $U \models \psi$*.*

Diese Proposition ist der Grund für die Nützlichkeit der internen Sprache: Wenn man eine garbentheoretische Implikation $A \Rightarrow B$ beweisen möchte, kann man vielleicht Voraussetzung und Behauptung als Interpretationen gewisser naiv-sprachlicher Aussagen $\tilde{A}$ bzw. $\tilde{B}$ mit der Kripke–Joyal-Semantik erkennen. Um dann die Implikation zu beweisen, genügt es, in naiver Sprache einen konstruktiven Beweis von $\tilde{A} \Rightarrow \tilde{B}$ zu führen.

Beispiel 6.26. In einer Grundvorlesung zeigt man, dass die Verkettung surjektiver Abbildungen wieder surjektiv ist. Da der Beweis konstruktiv ist, folgt durch Interpretation im Garbentopos daraus sofort, dass die Verkettung von Epimorphismen von Garben wieder ein Epimorphismus ist. (Natürlich kann man diese Aussage auch direkt und viel allgemeiner, in jeder Kategorie, beweisen.)

Beispiel 6.27. Der Beweis der Aussage, dass jede surjektive Abbildung f einen Schnitt s (eine Abbildung in die umgekehrte Richtung mit $f \circ s = \mathrm{id}$) zulässt, erfordert dagegen das

$$
\begin{aligned}
U \models f = g : \mathcal{F} \quad &:\Longleftrightarrow \quad f|_U = g|_U \in \Gamma(U, \mathcal{F}) \\
U \models \top \quad &:\Longleftrightarrow \quad U = U \text{ (gilt stets)} \\
U \models \bot \quad &:\Longleftrightarrow \quad U = \emptyset \\
U \models \varphi \wedge \psi \quad &:\Longleftrightarrow \quad U \models \varphi \text{ und } U \models \psi \\
U \models \varphi \vee \psi \quad &:\Longleftrightarrow \quad \cancel{U \models \varphi \text{ oder } U \models \psi} \\
&\qquad\qquad \text{es gibt eine Überdeckung } U = \textstyle\bigcup_i U_i \text{ sodass für alle } i\text{:} \\
&\qquad\qquad\qquad U_i \models \varphi \text{ or } U_i \models \psi \\
U \models \varphi \Rightarrow \psi \quad &:\Longleftrightarrow \quad \text{für alle offenen } V \subseteq U\text{: } V \models \varphi \text{ impliziert } V \models \psi \\
U \models \forall f : \mathcal{F}.\ \varphi(f) \quad &:\Longleftrightarrow \quad \text{für alle Schnitte } f \in \Gamma(V, \mathcal{F}), V \subseteq U\text{: } V \models \varphi(f) \\
U \models \exists f : \mathcal{F}.\ \varphi(f) \quad &:\Longleftrightarrow \quad \cancel{\text{es gibt einen Schnitt } f \in \Gamma(U, \mathcal{F}) \text{ mit } U \models \varphi(f)} \\
&\qquad\qquad \text{es gibt eine Überdeckung } U = \textstyle\bigcup_i U_i \text{ sodass für alle } i\text{:} \\
&\qquad\qquad\qquad \text{es gibt } f_i \in \Gamma(U_i, \mathcal{F}) \text{ sodass } U_i \models \varphi(f_i)
\end{aligned}
$$

Tafel 6: Die Kripke–Joyal-Semantik eines Garbentopos $\mathrm{Sh}(X)$.

Auswahlaxiom und lässt sich daher nicht in der internen Sprache interpretieren; tatsächlich haben Epimorphismen von Garben auch nur in den seltensten Fällen Rechtsinverse.[6]

Beispiel 6.28. Nur um Neugierde zu wecken hier ein komplexeres Beispiel: Konstruktiv kann man nicht zeigen, dass jeder endlich erzeugte Vektorraum über einem Körper eine Basis besitzt. Das liegt nicht etwa daran, dass solche plötzlich unendlichdimensional werden, sondern schlichtweg daran, dass man konstruktiv keine Basis explizit angeben kann. Man kann aber die schwächere Behauptung zeigen, dass jeder endlich erzeugte Vektorraum *nicht nicht* eine Basis besitzt. Diese Aussage zieht durch Interpretation im Garbentopos $\mathrm{Sh}(X)$ eines reduzierten Schemas X sofort folgendes Korollar nach sich: Jeder $\mathcal{O}_X$-Modul, der lokal von endlichem Typ ist, ist zwar nicht unbedingt lokal frei, aber zumindest auf einer dichten offenen Teilmenge lokal frei. (Die Reduziertheitsvoraussetzung geht insofern ein, als dass $\mathcal{O}_X$ aus Sicht der internen Sprache genau dann ein geeignetes Körperaxiom erfüllt, wenn X reduziert ist.)

Aufgabe 6.29. Sei $\alpha : \mathcal{F} \to \mathcal{G}$ ein Morphismus von Garben auf X. Zeige:

(a) Der Morphismus α ist genau dann ein Monomorphismus von Garben, wenn $X \models \forall x, y : \mathcal{F}.\ \alpha(x) = \alpha(y) \Rightarrow x = y$.

(b) Der Morphismus α ist genau dann ein Epimorphismus von Garben, wenn $X \models \forall y : \mathcal{G}.\ \exists x : \mathcal{F}.\ \alpha(x) = y$.

[6] Die Übersetzung ist eigentlich, dass Epimorphismen in einem geeigneten Sinn *lokal* Rechtsinverse besitzen. Aber auch diese schwächere Aussage stimmt fast nie.

Bemerkung 6.30. Jede offene Menge U stiftet einen Wahrheitswert von $\mathrm{Sh}(X)$, also aus interner Sicht eine Teilmenge von $\{\star\}$.

Bemerkung 6.31. In dem Garbentopos eines (T_1-)Raums X gilt genau dann das Prinzip vom ausgeschlossenen Dritten, wenn X diskret ist. Das ist ein langweiliger Fall. Garbentopoi zu interessanten topologischen Räumen liefern also einen völlig sachlichen Grund, wieso es nützlich ist, sich mit konstruktiver Logik zu beschäftigen.

Kann man mit der Toppssprache Sätze beweisen, die man ohne sie nicht beweisen könnte?

Im Beweis von Satz 6.25 ist ein Verfahren versteckt, wie man aus jedem intern geführten Beweis einen Beweis der entsprechenden übersetzten Aussagen im gewöhnlichen extern Sinn gewinnen kann. Daher kann man mit der Toppssprache sicherlich *nicht* Sätze beweisen, die man ohne sie nicht beweisen könnte.

Allerdings kann es sehr viel einfacher sein, in der internen Welt zu denken und zu arbeiten. Dieser Vorteil ist nicht zu unterschätzen: Wenn man sich etwa einmalig ein Wörterbuch zwischen externen Begriffen der algebraischen Geometrie und zugehörigen internen Begriffen geeigneter Topoi anlegt, kann man fortan viele Beweise von grundlegenden Aussagen kurz und konzeptionell führen, anstatt wie sonst mit affinen Überdeckungen, Übergängen zu Halmen und ähnlichen Techniken hantieren zu müssen.

6.5. Der Bohr-Topos zu einer nichtkommutativen C*-Algebra

Sei A die nichtkommutative C*-Algebra eines quantenmechanischen Systems.

Definition 6.32. (a) Ein *klassischer Kontext* von A ist eine kommutative Unter-C*-Algebra $C \subseteq A$.

(b) Die bezüglich der Inklusion geordnete Menge aller klassischen Kontexte von A ist $\mathcal{C}(A)$.

Die Idee hinter dieser Namensgebung ist folgende: Die Observablen (selbstadjungierten Elemente) einer kommutativen Unteralgebra $C \subseteq L(H,H)$ lassen sich *simultan* diagonalisieren und erlauben daher einen konsistenten Satz von Messwerten – ohne, dass Heisenbergs Unschärferelation in die Quere kommt.

Definition 6.33. Der *Bohr-Topos* zur C*-Algebra A ist die Koprägarbenkategorie

$$\mathrm{Bohr}(A) := [\mathcal{C}(A), \mathrm{Set}]$$

aller Funktoren $\mathcal{C}(A) \to \mathrm{Set}$ und natürlichen Transformationen zwischen ihnen.[7]

[7] Äquivalent kann man den Bohr-Topos auch als den Garbentopos über dem Raum $\mathcal{C}(A)$, versehen mit der Alexandroff-Topologie, auffassen: Die offenen Mengen sind dabei die nach oben abgeschlossenen

Ein solcher Funktor $F : \mathcal{C}(A) \to \mathrm{Set}$ ordnet auf konsistente Art und Weise jedem klassischen Kontext $C \subseteq A$ eine Menge $F(C)$ zu. Gewissermaßen setzt daher der Topos solcher Funktoren Bohrs Doktrin klassischer Konzepte um – in Bohrs eigenen Worten [12, Seite 209] (Hervorhebung im Original)[8]:

> [...] *however far the phenomena transcend the scope of classical physical explanation, the account of all evidence must be expressed in classical terms.* The argument is simply that by the word "experiment" we refer to a situation where we can tell others what we have done and what we have learned and that, therefore, the account of the experimental arrangements and of the results of the observations must be expressed in unambiguous language with suitable application of the terminology of classical physics.

Bemerkung 6.34. Wer die Definition von Garben auf topologischen Räumen X als Funktoren $\mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$ kennt, findet die unterschiedliche Wahl der Varianz an dieser Stelle vielleicht überraschend. Tatsächlich aber ist diese zu erwarten: Offene Mengen werden umso interessanter, je kleiner sie werden, da sie dann genauere Information über die Lage ihrer enthaltenen Punkte vermitteln. Kommutative Unteralgebren werden dagegen umso interessanter, je größer sie werden, denn für Elemente wird es umso schwerer, miteinander zu kommutieren, je mehr sie werden. Man bedenke auch, dass beliebige Vereinigungen (aber nicht beliebige Schnitte) offener Mengen offen sind, und dass umgekehrt beliebige Schnitte (aber nicht beliebige Summen) kommutativer Unteralgebren kommutativ sind.

Die nichtkommutative C*-Algebra A besitzt nun ein Abbild $\underline{A}$ im Bohr-Topos (siehe Abbildung 3). Diese *interne* C*-Algebra ist *kommutativ*. In diesem (restriktiven) Sinn wird Quantenmechanik bei interner Betrachtung zu klassischer Mechanik.

Definition 6.35. Die tautologisch definierte Koprägarbe

$$\begin{array}{rccc} \underline{A}: & \mathcal{C}(A) & \longrightarrow & \mathrm{Set} \\ & C & \longmapsto & C \end{array}$$

heißt *Bohrifizierung* von A.

Proposition 6.36. *Die Bohrifizierung von A ist aus der internen Sicht des Bohr-Topos eine* kommutative *C*-Algebra.*

Teilmengen, und eine Basis der Topologie ist durch die Teilmengen der Form $\uparrow(C) := \{C' \in \mathcal{C}(A) \mid C \subseteq C'\}$ für $C \in \mathcal{C}(A)$ gegeben. Unter dieser Äquivalenz induziert eine Garbe F auf diesem Raum einen Funktor $\mathcal{C}(A) \to \mathrm{Set}$ durch die Setzung $C \mapsto F(\uparrow(C))$.

[8] „*Inwieweit auch die Phänomene die Grenzen klassischer physikalischer Erklärungen sprengen, die Darstellung aller Anhaltspunkte muss trotzdem in klassischer Sprache ausgedrückt werden.* Das Argument ist einfach: Mit dem Wort ‚Experiment' drücken wir eine Situation aus, in der wir anderen erzählen können, was wir getan und gelernt haben. Deshalb müssen Versuchsanordnung und Beobachtungsresultate in unmissverständlicher Sprache ausgedrückt werden – unter passender Anwendung der Terminologie klassischer Physik."

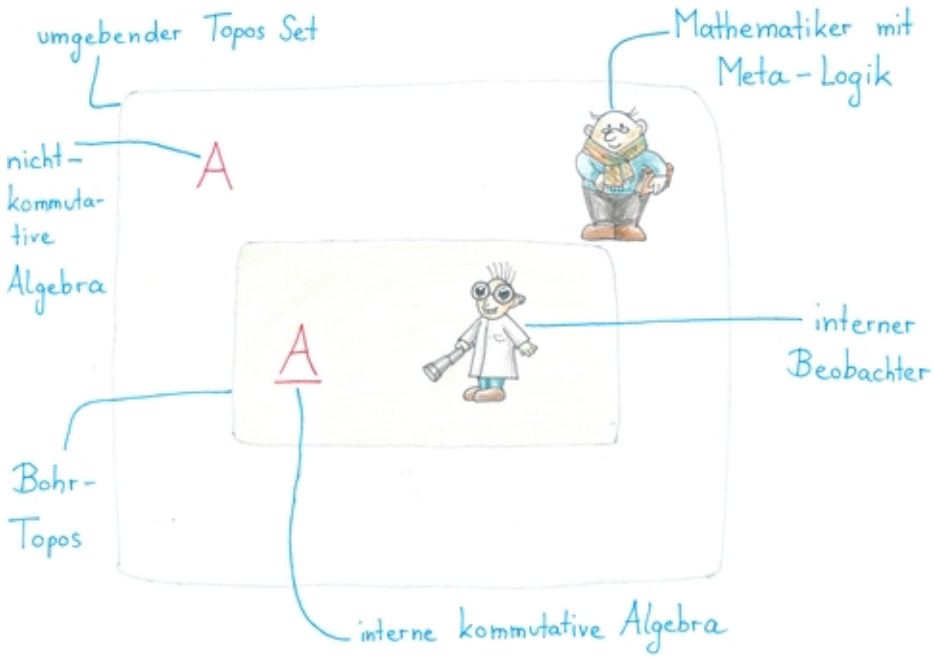


Abbildung 3: In dem Bohr-Topos zu A gibt es ein kommutatives Abbild der nichtkommutativen C*-Algebra A.

Beweis. Die additive und multiplikative Struktur erhält $\underline{A}$ objektweise: Für jeden klassischen Kontext $C \subseteq A$ gibt es auf $\underline{A}(C) = C$ offensichtlich eine Addition und Multiplikation. Da diese mit den Inklusionen $C \subseteq C'$ verträglich sind, werden so Morphismen $\underline{A} \times \underline{A} \to \underline{A}$ festgelegt.

An Eigenschaften weisen wir nur die Kommutativität nach, denn um die restlichen Eigenschaften zu diskutieren, müssten wir sie zunächst auf geeignete Art und Weise formulieren, und das würde unnötig ablenken. (Man kann nicht die klassische Definition einer C*-Algebra naiv übernehmen, da diese sich in einem konstruktiven Kontext wie dem Bohr-Topos nicht gut verhält. Die geeignet umformulierte Definition ist in klassischer Logik äquivalent zur üblichen Definition.)

Wir zeigen also

$$\mathrm{Bohr}(A) \models \forall a, b : \underline{A}.\ ab = ba.$$

Nach der Kripke–Joyal-Semantik in Koprägarbentopoi (in diesem Skript nicht angegeben, aber etwa in [49, Seite 100f.] zu finden) müssen wir dazu

$$\forall C \in \mathcal{C}(A).\ \forall a, b \in \underline{A}(C).\ ab = ba$$

nachweisen. Das ist trivial. □

Mit dem Bohr-Topos können wir also das formale Kunststück vollführen, die Familie aller kommutativen Unteralgebren von A als eine einzige kommutative Algebra anzusehen.

Vielleicht sollte man sagen: Quantenmechanik im Bohr-Topos ist klassische Mechanik, implizit parametrisiert über alle klassischen Kontexte.

Gemischte Quasi-Zustände

Die Bohrifizierung $\underline{A}$ wäre nicht interessant, wenn sich die Quasi-Zustände von A nicht irgendwie in $\underline{A}$ wiederspiegeln würden. Tatsächlich gibt es folgendes schönes Resultat:

Proposition 6.37. *Die gemischten Quasi-Zustände von A stehen in Bijektion mit den gemischten Zuständen von $\underline{A}$.*

Beweis. Mit dem internen Objekt komplexer Zahlen $\underline{\mathbb{C}}$ meinen wir die konstante Koprägarbe $C \mapsto \mathbb{C}$. Sei $\rho : A \to \mathbb{C}$ ein Quasi-Zustand von A. Dann definiert die Familie $(\rho|_C)_{C \in \mathcal{C}(A)}$ von Einschränkungen eine natürliche Transformation $\underline{\rho} : \underline{A} \to \underline{\mathbb{C}}$, also einen Morphismus im Bohr-Topos. Es ist klar, dass dieser aus interner Sicht normiert, positiv und homogen ist. Dass er aus interner Sicht additiv ist, dass also

$$\mathrm{Bohr}(A) \models \forall a, b : \underline{A}.\ \underline{\rho}(a + b) = \underline{\rho}(a) + \underline{\rho}(b)$$

gilt, bedeutet extern

$$\forall C \in \mathcal{C}(A).\ \forall a, b : \underline{A}(C).\ \rho_C(a + b) = \rho_C(a) + \rho_C(b).$$

Das ist gerade die Aussage, dass ρ auf kommutativen Unteralgebren additiv ist.

Sei umgekehrt ein Morphismus $\eta : \underline{A} \to \underline{\mathbb{C}}$ gegeben, der aus Sicht der internen Sprache normiert, positiv und linear ist. Dann können wir eine Abbildung $\rho : A \to \mathbb{C}$ durch die Setzung

$$\rho(a) := \eta_C(a), \quad \text{wobei } C \in \mathcal{C}(A) \text{ beliebig mit } a \in C,$$

definieren. Denn für jedes $a \in A$ existiert eine solche kommutative Unteralgebra (man kann etwa die von a erzeugte nehmen), und die Wahl von C spielt wegen der Natürlichkeitseigenschaft von η keine Rolle. Man kann nachrechnen, dass diese Abbildung ρ normiert, positiv und auf allen kommutativen Unteralgebren linear ist.

Es ist klar, dass diese Zuordnungen zueinander invers sind. □

Eine geometrische Interpretation

Da die interne C*-Algebra $\underline{A}$ kommutativ ist, ist auf diese wieder – wie in der Situation klassischer Mechanik – Gelfand-Dualität anwendbar. Die *interne Örtlichkeit* $\underline{\Sigma} := \mathrm{Spec}\,\underline{A}$ des Bohr-Topos ist also eine Art Phasenraum für das gegebene quantenmechanische System.

Folglich lassen sich Quasi-Zustände von A geometrisch als interne Wahrscheinlichkeitsmaße auf $\underline{\Sigma}$ deuten – ganz so, wie es bei klassischen Systemen auch im üblichen mathematischen Universum möglich ist.

Motto 6.38. *Nichtkommutative C^*-Algebren A besitzen zwar keine zugehörige Örtlichkeit im üblichen mathematischen Universum, wohl aber im speziell auf sie zugeschnittenen Topos* $\mathrm{Bohr}(A)$.

Observable

Proposition 6.39. *Jede Observable von A induziert eine interne stetige Abbildung $\underline{\Sigma} \to \underline{\mathbb{IR}}$. Diese Zuordnung von Observablen zu internen Örtlichkeitsmorphismen ist injektiv.*

Beweis. Siehe [31, Prop. 15]. Mit $\underline{\mathbb{IR}}$ ist eine spezielle Art eines Objekts reeller Zahlen gemeint. □

Reine Quasi-Zustände

Analog zu den gemischten Zuständen stehen die reinen Quasi-Zustände in Eins-zu-Eins-Korrespondenz zu den internen reinen Zuständen von $\underline{A}$, bzw. wegen Gelfand-Dualität äquivalent zu internen Punkten von $\underline{\Sigma}$ (stetigen Abbildungen $\underline{\mathrm{pt}} \to \underline{\Sigma}$). Da es, wir in Bemerkung 6.17 schon festgehalten haben, im interessanten Fall $A = L(H, H)$ mit $\dim H \geq 3$ keine reinen Quasi-Zustände gibt, ist $\underline{\Sigma}$ also eine exotische Örtlichkeit: Sie ist nichttrivial, besitzt aber trotzdem keine Punkte.

Der Witz: Auf kommutativen Unteralgebren von A kann es durchaus Bewertungen geben. Das spiegelt die Tatsache wieder, dass es in klassischer Mechanik kein Problem ist, eindeutige Messwerte zu allen Observablen zuzuordnen.

Topologie

A. Das Auswahlaxiom impliziert das Prinzip vom ausgeschlossenen Dritten

Axiom A.1 (Auswahlaxiom, kategoriell formuliert)**.** Jede surjektive Abbildung f besitzt einen Schnitt s, d. h. eine Abbildung in die umgekehrte Richtung mit $f \circ s = \mathrm{id}$.

Ein solcher Schnitt ist automatisch injektiv.

Proposition A.2 (Satz von Diaconescu)**.** *Aus dem Auswahlaxiom folgt das Prinzip vom ausgeschlossenen Dritten.*

Beweis. Sei φ eine beliebige Aussage. Dann definieren wir die Teilmengen

$$U = \{x \in X \mid (x = 0) \vee \varphi\}$$
$$V = \{x \in X \mid (x = 1) \vee \varphi\}$$

von $X := \{0,1\}$. Die Definition ist so gemacht, dass genau dann $U = V$ gilt, wenn φ gilt: Wenn $U = V$, so liegt 0 in V, also gilt $(0 = 1) \vee \varphi$. Da $0 \neq 1$, ist das äquivalent zu φ. Wenn umgekehrt φ gilt, so sind U und V beide gleich X.

Da die Abbildung

$$\begin{array}{rccc} f & : & X & \longrightarrow & \{U,V\} \\ & & 0 & \longmapsto & U \\ & & 1 & \longmapsto & V \end{array}$$

surjektiv ist, besitzt sie nach Voraussetzung einen Schnitt $s : \{U,V\} \to \{0,1\}$. Da s injektiv ist, gilt

$$s(U) = s(V) \quad \Longleftrightarrow \quad U = V \quad \Longleftrightarrow \quad \varphi.$$

Da $s(U)$ und $s(V)$ Elemente der diskreten Menge X sind, gilt $s(U) = s(V)$ oder $s(U) \neq s(V)$, also φ oder $\neg\varphi$. □

Aufgabe A.3. Zeige, dass die kategorielle Formulierung des Auswahlaxioms äquivalent zu folgender Formulierung ist: *Jede Familie $(X_i)_{i\in I}$ von bewohnten Teilmengen einer Menge Y besitzt eine Auswahlfunktion, d. h. eine Abbildung $f : I \to Y$ mit $f(i) \in X_i$ für alle $i \in I$.*

B. Ideale in Ringen

B.1. Grundlegende Konzepte

Definition B.1. Ein *kommutativer Ring mit Eins* (kurz *Ring*) besteht aus

- einer Menge R,
- einer additiv geschriebenen Verknüpfung $+ : R \times R \to R$,
- einer multiplikativ geschriebenen Verknüpfung $\cdot : R \times R \to R$,
- einem ausgezeichneten Element $0 \in R$ und
- einem ausgezeichneten Element $1 \in R$,

sodass

- Addition und Multiplikation assoziativ sind,
- Addition und Multiplikation kommutativ sind,
- Addition über Multiplikation distribuiert,
- das Element 0 neutral bezüglich der Addition ist,
- das Element 1 neutral bezüglich der Multiplikation ist und
- jedes Element ein bezüglich der Addition inverses Element besitzt.

Definition B.2. Ein *Körper* ist ein Ring, in dem jedes Element *entweder* Null *oder* (bezüglich der Multiplikation) invertierbar ist.

Beispiel B.3. Die Mengen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/(n)$, $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ bilden bezüglich ihrer üblichen Additionen und Multiplikationen Ringe. Für n prim ist $\mathbb{Z}/(n)$ sogar ein Körper. Die Menge $\mathbb{N}$ bildet bezüglich der üblichen Addition und Multiplikation noch keinen Ring, da bis auf die Null kein Element ein Negatives besitzt. (Die natürlichen Zahlen bilden etwas, das man *Rig* nennt – einen Ring ohne Negative.)

Definition B.4. Ein *Ideal* eines Rings R ist eine Teilmenge $\mathfrak{a} \subseteq R$, die

- die Null enthält: $0 \in \mathfrak{a}$,
- abgeschlossen unter (binärer) Addition ist: $x + y \in \mathfrak{a}$ für alle $x, y \in \mathfrak{a}$, und
- die *Magneteigenschaft* hat: $rx \in \mathfrak{a}$ für alle $r \in R$ und $x \in \mathfrak{a}$.

Die ersten beiden Axiome kann man natürlich zusammenfassen: Ein Ideal soll unter (beliebiger) Addition abgeschlossen sein. Die leere Summe ist das Nullelement.

Die Axiome werden durch folgendes Beispiel motiviert:

Beispiel B.5. Sei R ein Ring (zum Beispiel $R = \mathbb{Z}$) und $u \in R$ ein Element (zum Beispiel deine Lieblingszahl). Dann ist die Menge

$$(u) := \{ru \,|\, r \in R\} \subseteq R$$

aller Vielfachen von u ein Ideal, das sog. *von u erzeugte Ideal*. Denn die Null ist ein Vielfaches von u (das Null-fache), die Summe zweier Vielfachen von u ist ein Vielfaches von u, und ist x ein Vielfaches von u, so ist rx für ein beliebiges Element $r \in R$ „umso mehr“ ein Vielfaches von u.

In Körpern K ist der Idealbegriff langweilig: Körper besitzen stets nur genau zwei Ideale, nämlich das sog. Nullideal $(0) = \{0\}$ und das sog. Einsideal $(1) = K$.

Definition B.6. Seien $x_1, \ldots, x_n$ Elemente eines Rings R. Dann heißt das Ideal

$$(x_1, \ldots, x_n) := \{r_1 x_1 + \cdots + r_n x_n \,|\, r_1, \ldots, r_n \in R\} \subseteq R$$

das *von $x_1, \ldots, x_n$ erzeugte Ideal*.

Beispiel B.7. Für den Ring der ganzen Zahlen gilt $(2, 3) = (1) = \mathbb{Z}$.

Definition B.8. Ein Ideal $\mathfrak{p} \subseteq R$ heißt genau dann *Primideal*, wenn

- die Eins nicht enthalten ist: $1 \notin \mathfrak{p}$, und
- wann immer ein Produkt in $\mathfrak{p}$ enthalten ist, schon ein Faktor in $\mathfrak{p}$ liegt:

$$xy \in \mathfrak{p} \quad \Longrightarrow \quad x \in \mathfrak{p} \ \vee \ y \in \mathfrak{p} \qquad \text{für alle } x, y \in R.$$

Auch diese beiden Axiome kann man zusammenfassen: Liegt ein Produkt aus beliebig vielen (auch Null vielen) Faktoren in $\mathfrak{p}$, so soll schon einer der Faktoren in $\mathfrak{p}$ liegen.

Beispiel B.9. Sei $u \in \mathbb{Z}$. Dann ist das von u erzeugte Ideal $(u) \subseteq \mathbb{Z}$ genau dann ein Primideal, wenn u Null ist oder wenn u oder $-u$ eine Primzahl ist.

B.2. Historische Motivation für Idealtheorie

Historisch gab es eine große Motivation, das Idealkonzept einzuführen. Vom Ring der ganzen Zahlen war natürlich bekannt, dass sich (bis auf die Null) jedes Element auf eindeutige Weise als Produkt von Primfaktoren schreiben lässt (bis auf Assoziiertheit). Man fragte sich nun, ob gewisse für die Zahlentheorie relevante Ringe dieselbe Eigenschaft hatten: Das wäre zum einen recht nett, zum anderen aber auch enorm nützlich: Denn man kannte schon einfache Beweise von Fermats letztem Satz, welche als einzige ungesicherte Zutat diese Eigenschaft voraussetzten.

Leider stellte es sich heraus, dass diese Eigenschaft vielen der interessanten Ringe *nicht* zu kommt. Kronecker hatte nun die geniale Einsicht, von Zahlen zu Idealen und von Primzahlen zu Primidealen zu verallgemeinern. Denn in diesen Ringen gilt zumindest noch, dass sich jedes *Ideal* eindeutig als Produkt von Prim*idealen* schreiben lässt. Mit dieser schwächeren Eigenschaft lässt sich zwar kein allgemeiner Beweis von Fermats letztem Satz führen, zumindest lässt sich jedoch eine große Klasse von Spezialfällen damit behandeln.

Wer sich für dieses Thema interessiert, dem sei das deutschsprachige Buch [47] von Alexander Schmidt empfohlen. Als Vorwissen setzt es nur Schulkenntnisse voraus.

B.3. Die Ideale im Ring der ganzen Zahlen

Tafel 7 zeigt die endlich erzeugten Ideale des Rings $\mathbb{Z}$. Ergänzt man die aus Platzgründen ausgelassenen Ideale, ist das sogar eine vollständige Übersicht über *alle* Ideale von $\mathbb{Z}$ – wenn man klassische Logik voraussetzt.

Aufgabe B.10. Zeige, dass wenn alle Ideale von $\mathbb{Z}$ von der Form (x) für eine ganze Zahl x sind, das Prinzip vom ausgeschlossenen Dritten gilt. *Tipp:* Betrachte für eine beliebige Aussage φ das Ideal $\{x \in \mathbb{Z} \mid (x = 0) \vee \varphi\} \subseteq \mathbb{Z}$ (wieso sind die Idealaxiome erfüllt?).

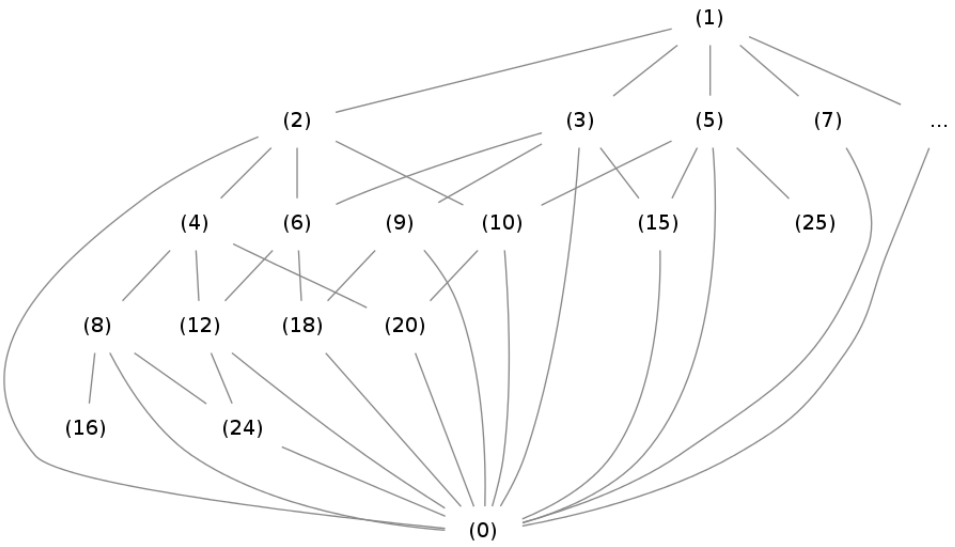
B.4. Primideale und Nilpotenz

Definition B.11. Ein Element $x \in R$ eines Rings R heißt genau dann *nilpotent*, wenn eine gewisse Potenz Null ist: $x^n = 0$ für ein $n \geq 0$.

Beispiel B.12. Im Ring $\mathbb{Z}/(4)$ ist die Äquivalenzklasse $[2]$ nilpotent.

Proposition B.13. *Die nilpotenten Elemente eines Rings liegen in allen Primidealen des Rings.*

Beweis. Sei x mit $x^n = 0$ ein nilpotentes Element. Sei $\mathfrak{p}$ ein beliebiges Primideal. Dann ist also x^n in $\mathfrak{p}$ enthalten. Wegen der Primalitätsbedingung ist daher auch x in $\mathfrak{p}$ enthalten. Das war zu zeigen. □



Tafel 7: Modulo Platz und klassische Logik eine vollständige Übersicht über alle Ideale von $\mathbb{Z}$.

Interessant ist nun, dass – in einem klassischen Kontext – auch die Umkehrung dieser Proposition gilt. Somit hat man ein einfaches Kriterium an der Hand, um die Nilpotenz eines Ringelements nachzuweisen.

Proposition B.14 (nur klassisch)**.** *Im Schnitt aller Primideale eines Rings liegen nur die nilpotenten Elemente.*

Beweis. Sei x ein Element von R, welches in allen Primidealen liegt. Wir wollen zeigen, dass x nilpotent ist; dazu führen wir einen Widerspruchsbeweis, nehmen also an, dass x nicht nilpotent ist. Dann enthält die Menge

$$S := \{x^n \,|\, n \geq 0\} \subseteq R$$

also nicht die Null. Wir betrachten nun das bezüglich der Teilmengeninklusionsrelation partiell geordnete Mengensystem

$$\mathcal{U} := \{\mathfrak{a} \subseteq R \,|\, \mathfrak{a} \text{ ist ein Ideal mit } \mathfrak{a} \cap S = \emptyset\}.$$

Dieses ist bewohnt: Das Nullideal liegt wegen $0 \notin S$ in $\mathcal{U}$. Außerdem liegt die Vereinigung $\bigcup_i \mathfrak{a}_i$ einer in $\mathcal{U}$ liegenden Kette von Elementen aus $\mathcal{U}$ wieder in $\mathcal{U}$. Damit sind alle Voraussetzung des Lemmas von Zorn erfüllt, womit $\mathcal{U}$ also ein maximales Element $\mathfrak{m}$ enthält.

Man kann nun nachrechnen, dass $\mathfrak{m}$ ein Primideal ist.[9] Da $x \notin \mathfrak{m}$ (wegen $x \in S$), ist das ein Widerspruch zur Voraussetzung. □

Dieser Beweis ist aus zwei Gründen inhärent klassisch: Zum einen, weil er ein echter Widerspruchsbeweis ist; zum anderen, weil das Lemma von Zorn verwendet wird (dieses ist zum Auswahlaxiom äquivalent). Man kann sogar zeigen, dass ein konstruktiver Beweis dieser Proposition nicht möglich ist. Daher ist folgendes Meta-Theorem absolut erstaunlich:

Wunder B.15. *Sei $x \in R$ ein Element eines Rings. Sei ein* klassischer Beweis *(einer gewissen Form) der Aussage $x \in \mathfrak{p}$, wobei man von $\mathfrak{p}$ nur die Axiome eines Primideals voraussetzen darf, gegeben. Dann ist x nilpotent (konstruktiv!). Aus dem klassischen Beweis kann man also auf konstruktive Art und Weise einen konstruktiven Beweis der Nilpotenzbehauptung extrahieren.*

Die genaue Formulierung steht im Haupttext als Satz 5.20.

Polynome mit Koeffizienten in Primidealen

Für das Beispiel in Abschnitt 5.3 benötigen wir folgendes Lemma.

Lemma B.16. *Seien $f, g \in R[X]$ Polynome über einem Ring R. Sei $\mathfrak{p} \subseteq R$ ein Primideal. Wenn alle Koeffizienten von fg in $\mathfrak{p}$ liegen, so liegen schon alle Koeffizienten von f oder alle Koeffizienten von g in $\mathfrak{p}$.*

Wenn man mit der Faktorringkonstruktion vertraut ist, lässt sich das Lemma einfacher formulieren: Ist ein Produkt in $(R/\mathfrak{p})[X]$ Null, so ist schon einer der Faktoren in $(R/\mathfrak{p})[X]$ Null. Diese Aussage ist Instanz eines noch allgemeineren Lemmas: Ist ein Ring S ein Integritätsbereich, so auch $S[X]$.

B.5. Radikalideale

Definition B.17. (a) Ein Ideal $\mathfrak{a} \subseteq R$ eines Rings R heißt genau dann *Radikalideal*, wenn für alle $x \in R$ und $n \geq 0$ aus $x^n \in \mathfrak{a}$ schon $x \in \mathfrak{a}$ folgt.

(b) Sei $\mathfrak{a} \subseteq R$ ein Ideal. Dann heißt das Ideal

$$\sqrt{\mathfrak{a}} := \{x \in R \mid \exists n \geq 0.\ x^n \in \mathfrak{a}\}$$

das *Radikal von* $\mathfrak{a}$. Es ist stets ein Radikalideal, und zwar das kleinste, das $\mathfrak{a}$ umfasst.

[9] Wäre $\mathfrak{m} = (1)$, so wäre $S = \emptyset$. Liegt ein Produkt ab in $\mathfrak{m}$, so gilt $a \in \mathfrak{m}$ oder $a \notin \mathfrak{m}$; im zweiten Fall folgt $b \in \mathfrak{m}$, denn dann liegt $\mathfrak{m} + (b)$ in $\mathcal{U}$ (wieso?), womit die Maximalität von $\mathfrak{m}$ schon $\mathfrak{m} + (b) = \mathfrak{m}$, also $b \in \mathfrak{m}$, impliziert.

Beispiel B.18. Das Ideal $(12) \subseteq \mathbb{Z}$ ist kein Radikalideal, $\sqrt{(12)} = (6)$ dagegen schon.

Bemerkung B.19. Die Zuordnung von Radikalen zu Idealen bildet einen Linksadjungierten zum Vergissfunktor der Kategorie der Radikalideale von R in die Kategorie aller Ideale von R.

Lemma B.20. *Für die bezüglich der Inklusionsbeziehung partiell geordnete Menge* $\mathrm{Rad}(R)$ *der Radikalideale eines Rings R gilt:*

(a) Das kleinste Element ist $\sqrt{(0)}$, das Ideal aller nilpotenten Elemente.

(b) Das größte Element ist (1), das Einsideal.

(c) Das Supremum zweier Elemente $\mathfrak{a}, \mathfrak{b}$, also das kleinste Radikalideal, das $\mathfrak{a}$ und $\mathfrak{b}$ umfasst, ist

$$\sqrt{\mathfrak{a} + \mathfrak{b}} := \{x \in R \mid x^n = u + v \text{ für ein } n \geq 0, u \in \mathfrak{a}, v \in \mathfrak{b}\}.$$

(d) Das Infimum zweier Elemente $\mathfrak{a}, \mathfrak{b}$, also das größte Radikalideal, das in $\mathfrak{a}$ und $\mathfrak{b}$ enthalten ist, ist $\mathfrak{a} \cap \mathfrak{b}$.

Beweis. Nachrechnen. □

Beispiel B.21. Für den Ring der ganzen Zahlen gilt $(6) \cap (5) = (30)$ und $(6) \cap (15) = (30)$.

Beispiel B.22. Allgemein gilt

$$\sup\Big\{\sqrt{(x)}, \sqrt{(y)}\Big\} = \sqrt{\sqrt{(x)} + \sqrt{(y)}} = \sqrt{(x, y)}.$$

C. Garben

C.1. Prägarben und Garben

Definition C.1. (a) Eine *Prägarbe* auf einem topologischen Raum X (oder einer Örtlichkeit) ist eine Prägarbe im kategoriellen Sinn auf der als dünne Kategorie aufgefassten Halbordnung $\mathrm{Ouv}(X)$ der offenen Teilmengen (bzw. offenen Dinge) von X, also ein Funktor $\mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$.

(b) Ein *Morphismus von Prägarben* $\mathcal{F} \to \mathcal{G}$ ist eine natürliche Transformation $\mathcal{F} \to \mathcal{G}$.

Ist $\mathcal{F}$ eine Prägarbe auf X und $U \subseteq X$ eine offene Menge, so schreibt man auch „$\Gamma(U, \mathcal{F})$“ für $\mathcal{F}(U)$ und nennt die Elemente dieser Menge *Schnitte von $\mathcal{F}$ auf U*. Wenn $V \subseteq U$, schreibt man die induzierte Abbildung $F(\text{„}V \subseteq U\text{“}) : \mathcal{F}(U) \to \mathcal{F}(V)$ auch als „$(\_)|_V$“. Diese Schreibweise rührt von den wichtigsten Beispielen für Prägarben her.

Die Prototyp-Beispiele für Prägarben stammen nämlich von verschiedenen Funktionsbegriffen. Etwa gibt es auf jedem topologischen Raum X die Prägarbe $\mathcal{C}^0$ der stetigen Funktionen, definiert über

$$\begin{array}{rcl} \mathrm{Ouv}(X)^{\mathrm{op}} & \longrightarrow & \mathrm{Set} \\ U & \longmapsto & \{U \xrightarrow{f} \mathbb{R} \mid f \text{ stetig}\} \\ \text{„}V \subseteq U\text{“} & \longmapsto & \mathrm{res}_V^U \end{array}$$

mit $\mathrm{res}_V^U : \mathcal{C}^0(U) \to \mathcal{C}^0(V), f \mapsto f|_V$ der Einschränkungsabbildung. Trägt X sogar die Struktur einer glatten Mannigfaltigkeit, kann man analog auch die Garbe $\mathcal{C}^\infty$ der glatten Funktionen definieren – man setzt $\Gamma(U, \mathcal{C}^\infty) := \{U \xrightarrow{f} \mathbb{R} \mid f \text{ glatt}\}$.

Die Garbenbedingung

Definition C.2. (a) Eine Prägarbe $\mathcal{F}$ auf X heißt genau dann *Garbe*, wenn folgendes Verklebeaxiom erfüllt ist: Ist $U = \bigcup_i U_i \subseteq X$ eine offene Überdeckung einer offenen Teilmenge und ist $(s_i)_{i \in I}$ eine Familie von Schnitten mit $s_i \in \Gamma(U_i, \mathcal{F})$, welche auf Überlappungen übereinstimmen, also $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ für alle Indizes i, j erfüllen, so soll es genau einen Schnitt $s \in \Gamma(U, \mathcal{F})$ mit $s|_{U_i} = s_i$ für alle i geben.

(b) Ein *Morphismus von Garben* ist ein Morphismus der zugrundeliegenden Prägarben.

Die Kategorie der Garben auf X, $\mathrm{Sh}(X)$, ist also eine volle Unterkategorie der Kategorie der Prägarben auf X, $\mathrm{PSh}(X)$.

Beispiel C.3. Die Prägarben $\mathcal{C}^0$ und $\mathcal{C}^\infty$ (sofern definierbar) sind Garben: Man kann stetige bzw. glatte Funktionen, die auf Überlappungen übereinstimmen, miteinander *verkleben*; die resultierende Funktion wird wieder stetig bzw. glatt sein.

Beispiel C.4. Die Prägarbe $\mathcal{C}_{\mathrm{const}}$ der konstanten Funktionen,

$$\Gamma(U, \mathcal{C}_{\mathrm{const}}) = \{U \xrightarrow{f} \mathbb{R} \mid f \text{ konstant}\},$$

ist außer in pathologischen Fällen keine Garbe. Denn wenn zwei konstante Funktionen $f_1 : U_1 \to \mathbb{R}$ und $f_2 : U_2 \to \mathbb{R}$ auf zwei sich nicht überlappenden offenen Mengen definiert sind, ist die Kompatibilitätsbedingung leer, sie lassen sich jedoch im Allgemeinen trotzdem nicht zu einer konstanten Funktion auf $U_1 \cup U_2$ zusammensetzen: Das geht genau dann, wenn sie denselben konstanten Wert haben. Die analog definierte Prägarbe $\mathcal{C}_{\mathrm{lc}}$ der lokal konstanten Funktionen ist dagegen durchaus eine Garbe. (Eine Funktion heißt genau dann lokal konstant, wenn es eine Überdeckung ihres Urbildbereichs gibt, sodass die Einschränkungen der Funktion auf die Überdeckungsmengen jeweils konstant sind.)

Bemerkung C.5. Es gibt ein allgemeine Technik, die *Garbifizierung*, mit der man auf universelle Art und Weise aus Prägarben Garben machen kann. (Genauer ist der Garbifizierungsfunktor linksadjungiert zum Vergissfunktor $\mathrm{Sh}(X) \to \mathrm{PSh}(X)$.) Die Garbifizierung der Prägarbe der konstanten Funktionen ist dann gerade die Garbe der lokal konstanten Funktionen.

Globale Schnitte

Historisch eine der wichtigsten Garben ist die Garbe $\mathcal{O}_X$ der holomorphen Funktionen auf einer komplexen Mannigfaltigkeit X (etwa $X = \mathbb{C}$ oder $X = \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, der riemannschen Zahlenkugel), definiert über

$$\Gamma(U, \mathcal{O}_X) = \{U \xrightarrow{f} \mathbb{C} \mid f \text{ holomorph}\}.$$

Sie hat die für viele Garben typische Eigenschaft, oftmals nur recht wenige *globale Schnitte* (Elemente von $\Gamma(X, \mathcal{O}_X)$) zu besitzen – im Fall der riemannschen Zahlenkugel sind das nach dem Satz von Liouville etwa nur die konstanten Funktionen. Nichttrivial sind nur Schnitte, die auf kleineren offenen Teilmengen definiert sind.

Sinnvolle Bedingungen an Garben oder Garbenmorphismen erhält man in der Regel also nur dann, wenn man alle offenen Mengen einbezieht, nicht nur X selbst. Die Kripke–Joyal-Semantik zur Interpretation der internen Sprache eines Garbentopos achtet von selbst darauf (siehe Abschnitt 6.4).

C.2. Monomorphismen und Epimorphismen von Garben

Proposition C.6. *Sei $\alpha : \mathcal{F} \to \mathcal{G}$ ein Morphismus von Prägarben. Dann gilt:*

(a) Der Morphismus α ist genau dann ein Monomorphismus in $\mathrm{PSh}(X)$*, wenn für alle offenen Teilmengen $U \subseteq X$ die Komponente $\alpha_U : \Gamma(U, \mathcal{F}) \to \Gamma(U, \mathcal{G})$ eine injektive Abbildung ist, wenn also gilt:*

$$\forall U \subseteq X \text{ offen. } \forall s, t \in \Gamma(U, \mathcal{F}).\ \alpha_U(s) = \alpha_U(t) \Rightarrow s = t.$$

(b) Der Morphismus α ist genau dann ein Epimorphismus in $\mathrm{PSh}(X)$*, wenn für alle offenen Teilmengen $U \subseteq X$ die Komponente $\alpha_U : \Gamma(U, \mathcal{F}) \to \Gamma(U, \mathcal{G})$ eine surjektive Abbildung ist, wenn also gilt:*

$$\forall U \subseteq X \text{ offen. } \forall s \in \Gamma(U, \mathcal{G}).\ \exists t \in \Gamma(U, \mathcal{F}).\ \alpha_U(t) = s.$$

Proposition C.7. *Sei $\alpha : \mathcal{F} \to \mathcal{G}$ ein Morphismus von Garben. Dann gilt:*

(a) Der Morphismus α ist genau dann ein Monomorphismus in $\mathrm{Sh}(X)$*, wenn für alle offenen Teilmengen $U \subseteq X$ die Komponente $\alpha_U : \Gamma(U, \mathcal{F}) \to \Gamma(U, \mathcal{G})$ eine injektive Abbildung ist.*

(b) Der Morphismus α ist genau dann ein Epimorphismus in $\mathrm{Sh}(X)$*, wenn jeder Schnitt von $\mathcal{G}$* lokal *ein Urbild besitzt, d. h. wenn für alle offenen Teilmengen $U \subseteq X$ und Schnitte $s \in \Gamma(U, \mathcal{G})$ eine Überdeckung $U = \bigcup U_i$ und Schnitte $t_i \in \Gamma(U_i, \mathcal{F})$ mit $\alpha_{U_i}(t_i) = s|_{U_i}$ existieren.*

Wenn man sich das erste Mal mit Garben beschäftigt, verwundert vielleicht die Charakterisierung von Epimorphismen in der Garbenkategorie: Vielleicht hätte man eher

die Bedingung, dass alle Komponentenabbildungen α_U surjektiv sind, erwartet. Diese stärkere Bedingung ist zwar ebenfalls hinreichend für Epimorphie, aber nur in der größeren Kategorie aller *Präg*arben notwendig.

Beispiel C.8. Sei $\mathcal{O}_X$ die Garbe der holomorphen Funktionen auf $X = \mathbb{C}$. Sei $\mathcal{O}_X^\times$ die Untergarbe der bezüglich der Multiplikation invertierbaren holomorphen Funktionen, also der nirgends verschwindenden Funktionen. Dann ist der „exp“ genannte Garbenmorphismus

$$\begin{array}{rcl} \mathcal{O}_X & \longrightarrow & \mathcal{O}_X^\times \\ \text{auf } U \subseteq X\colon \quad f \in \mathcal{O}_X(U) & \longmapsto & \exp \circ f \in \mathcal{O}_X^\times(U) \end{array}$$

ein Epimorphismus (da man *lokal* die Exponentialfunktion mittels eines geeigneten Zweigs des Logarithmus umkehren kann). Aber seine Komponentenabbildungen $\exp_U$ sind nicht alle surjektiv, etwa für solche Teilmengen U nicht, die einen Kreisring um den Ursprung umfassen.

Bemerkung C.9. Mit *Garbenkohomologie* kann man *messen*, inwieweit ein Epimorphismus von Garben davon entfernt ist, auch ein Epimorphismus von Prägarben zu sein: Sei $\alpha : \mathcal{F} \to \mathcal{G}$ ein Epimorphismus von Garben abelscher Gruppen. Dann liefert eine *lange exakte Sequenz* einen Morphismus $\partial : \Gamma(X, \mathcal{G}) \to H^1(X, \ker \alpha)$. Dieser ist genau dann Null, wenn α sogar ein Epimorphismus von Prägarben abelscher Gruppen ist. Es gilt sogar die feinere Aussage, dass ein Schnitt $s \in \Gamma(X, \mathcal{G})$ genau dann ein Urbild unter α_X besitzt, wenn $\partial(s) = 0$.

Bemerkung C.10. In den meisten Lehrbüchern über Garben sind *Mono-* und *Epimorphismus* speziell definierte Begriffe: Ein Morphismus $\alpha : \mathcal{F} \to \mathcal{G}$ von Garben heißt dort genau dann mono- bzw. epimorph, wenn die induzierten Abbildungen $\alpha_x : \mathcal{F}_x \to \mathcal{G}_x$, $x \in X$, auf allen *Halmen* injektiv bzw. surjektiv sind. Diese Definition ist äquivalent zur allgemeinen kategoriellen Definition und somit zur Charakterisierung aus der Proposition. Sie hat allerdings den Nachteil, dass sie nicht unmittelbar auf Örtlichkeiten übertragbar ist.

Literatur

[1] P. Aczel. „The Russell–Prawitz modality“. In: *Math. Structures Comput. Sci* 11.4 (2001), S. 541–554.

[2] J. Avigad. *Proof mining*. Vortragsfolien. 2004. URL: `http://www.andrew.cmu.edu/user/avigad/Talks/asl04.pdf`.

[3] J. Baez. *Topos Theory in a Nutshell*. 2006. URL: `http://math.ucr.edu/home/baez/topos.html`.

[4] A. Bauer. *Five Stages of Accepting Constructive Mathematics*. Vortrag am Institute for Advanced Study. 2013. URL: `http://video.ias.edu/members/1213/0318-AndrejBauer`.

[5] A. Bauer. *Mathematics and computation*. Blog. URL: `http://math.andrej.com/category/constructive-math/`.

[6] A. Bauer. *Realizability as the connection between computable and constructive mathematics*. 2005. URL: http://math.andrej.com/data/c2c.pdf.

[7] A. Bauer. *Sometimes all functions are continuous*. Artikel des Blogs *Mathematics and computation*.

[8] J. Bell. *A Primer of Infinitesimal Analysis*. 2. Aufl. Cambridge University Press, 2008.

[9] J. Bell. *An invitation to smooth infinitesimal analysis*. 2003. URL: http://publish.uwo.ca/~jbell/invitation%20to%20SIA.pdf.

[10] E. Bishop und D. Bridges. *Constructive Analysis*. Springer, 1985.

[11] I. Blechschmidt. *Pizzaseminar zu Kategorientheorie*. 2013. URL: http://pizzaseminar.speicherleck.de/skript1/pizzaseminar.pdf.

[12] N. Bohr. „Discussion with Einstein on epistemological problems in atomic physics“. In: *Albert Einstein: Philosopher–Scientist*. Hrsg. von P. A. Schilpp. Cambridge University Press, 1949, S. 200–241. URL: http://www.tuhh.de/rzt/rzt/it/QM/schilpp.html.

[13] B. Bolzano. „Rein analytischer Beweis des Lehrsatzes, daß zwischen je zwey Werthen, die ein entgegengesetztes Resultat gewähren, wenigstens eine reelle Wurzel der Gleichung liege“. In: *Abhandlungen der Königlichen Böhmischen Gesellschaft der Wissenschaften*. Übersetzung in modernes Englisch auf http://books.google.com/books?id=zp7cLQn0x3gC&pg=PA251. 1817. URL: https://eudml.org/doc/202403.

[14] J. Butterfield, J. Hamilton und C. Isham. „A topos perspective on the Kochen-Specker theorem, I. quantum states as generalized valuations“. In: *Internat. J. Theoret. Phys.* 37.11 (1998), S. 2669–2733. URL: http://arxiv.org/abs/quant-ph/9803055.

[15] The nLab contributors. *Bohr topos*. 2013. URL: http://ncatlab.org/nlab/show/Bohr+topos.

[16] The nLab contributors. *Classical mechanics*. 2013. URL: http://ncatlab.org/nlab/show/classical+mechanics.

[17] The nLab contributors. *Gleason's theorem*. 2014. URL: http://ncatlab.org/nlab/show/Gleason's+theorem.

[18] The nLab contributors. *nLab*. 2013. URL: http://ncatlab.org/.

[19] B. Copeland. „The Church-Turing Thesis“. In: *The Stanford Encyclopedia of Philosophy*. Hrsg. von N. Zalta. 2008. URL: http://plato.stanford.edu/entries/church-turing/.

[20] T. Coquand. „Computational content of classical logic“. In: *Semantics and Logics of Computation*. Hrsg. von A. Pitts und P. Dybjer. Cambridge University Press, 1997, S. 33–78. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.49.3492&rep=rep1&type=pdf.

[21] T. Coquand. *Dynamical methods in algebra*. Vortragsfolien *Calculemus, 11th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning*. 2003. URL: http://www.cse.chalmers.se/~coquand/sitesur.pdf.

[22] T. Coquand und H. Lombardi. „A logical approach to abstract algebra“. In: *Math. Structures Comput. Sci* 16.5 (2006), S. 885–900. URL: http://www.cse.chalmers.se/~coquand/FISCHBACHAU/AlgebraLogicCoqLom.pdf.

[23] M. Coste, H. Lombardi und M.-F. Roy. „Dynamical method in algebra: effective Nullstellensätze“. In: *Ann. Pure Appl. Logic* 111.3 (2001), S. 203–256. URL: http://perso.univ-rennes1.fr/michel.coste/publis/clr.pdf.

[24] D. van Dalen. „Intuitionistic logic“. In: *The Blackwell Guide to Philosophical Logic*. Hrsg. von L. Goble. Blackwell Publishers, 2011, S. 224–257. URL: http://www.phil.uu.nl/~dvdalen/articles/Blackwell(Dalen).pdf.

[25] *Diskussion über Beweise leerer Allaussagen auf MathOverflow*. 2010. URL: http://mathoverflow.net/questions/47090/let-x-in-a-beginning-a-proof-of-forall-x-in-a-if-a-were-empty.

[26] M. Dummett. „The Philosophical Basis of Intuitionistic Logic“. In: *Truth and Other Enigmas*. Duckworth, 1973, S. 215–247.

[27] M. Escardó und P. Oliva. „The Peirce translation and the double negation shift“. In: *Programs, Proofs, Processes*. Hrsg. von F. Ferreira u. a. Bd. 6158. Lecture Notes in Comput. Sci. Springer, 2010, S. 151–161.

[28] D. Goldin und P. Wegner. „The Church-Turing Thesis: Breaking the Myth“. In: *New Computational Paradigms*. Hrsg. von S. Cooper, B. Löwe und L. Torenvliet. Bd. 3526. Lect. Notes in Comput. Sci. Springer, 2005, S. 152–168. URL: http://www.cse.uconn.edu/~dqg/papers/cie05.pdf.

[29] A. Grothendieck. *Récoltes et Semailles, Réflexions et témoignages sur un passé de mathématicien*. 1986. URL: http://www.math.jussieu.fr/~leila/grothendieckcircle/RetS.pdf.

[30] P. de la Harpe und V. Jones. *An introduction to C^*-algebras*. 1995. URL: http://www.unige.ch/math/biblio/preprint/cstar/liste.html.

[31] C. Heunen, N. Landsman und B. Spitters. „A Topos for Algebraic Quantum Theory“. In: *Comm. Math. Phys.* 291.1 (2009), S. 63–110. URL: http://link.springer.com/article/10.1007/s00220-009-0865-6.

[32] P. T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium*. Oxford University Press, 2002.

[33] P. T. Johnstone. „The art of pointless thinking: a student's guide to the category of locales“. In: *Category theory at work (Bremen, 1990)*. Res. Exp. Math. 18. Heldermann, 1991, S. 85–107.

[34] P. T. Johnstone. „The point of pointless topology“. In: *Bull. Amer. Math. Soc.* 8.1 (1983), S. 41–53.

[35] O. Kiselyov. *Constructive law of excluded middle*. 2009. URL: http://okmij.org/ftp/Computation/lem.html.

[36] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer-Verlag, 2008.

[37] J. Lambek und P. Scott. *Introduction to Higher-Order Categorical Logic*. Bd. 7. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1988.

[38] T. Leinster. „An informal introduction to topos theory". In: *Publications of the nLab* 1.1 (2011). URL: http://ncatlab.org/publications/published/Leinster2011.

[39] H. Lombardi. *Hilbert's Program for Abstract Algebra does work*. Vortragsfolien *International conference on abelian groups and modules over commutative rings*. 2007. URL: http://hlombardi.free.fr/publis/AGAMOCRSlide.pdf.

[40] S. Mac Lane und I. Moerdijk. *Sheaves in Geometry and Logic: a First Introduction to Topos Theory*. Universitext. Springer-Verlag, 1992.

[41] R. Mines, F. Richman und W. Ruitenburg. *A Course in Constructive Algebra*. Universitext. Springer-Verlag, 1988.

[42] BBC NEWS. *Blair 'misunderstands drug laws'*. 2008. URL: http://news.bbc.co.uk/2/hi/uk_news/england/london/7440111.stm.

[43] M. Nieper-Wißkirchen. *Galoissche Theorie*. 2013. URL: http://alg.math.uni-augsburg.de/lehre/vorlesungsskripte/einfuhrung-in-die-algebra/at_download/file.

[44] A. Olszewski, J. Wolenski und R. Janusz. *Church's Thesis After 70 Years*. Ontos Mathematical Logic. De Gruyter, 2006.

[45] D. Piponi. *Drugs, Kate Moss, and Intuitionistic Logic*. Artikel des Blogs *A Neighbourhood of Infinity*. 2008. URL: http://blog.sigfpe.com/2008/06/drugs-kate-moss-and-intuitionistic.html.

[46] P. Raatikainen. „Hilbert's Program Revisited". In: *Synthese* 137.1-2 (2003), S. 157–177. URL: http://www.mv.helsinki.fi/home/praatika/Hilbert's%20Program%20Revisited.pdf.

[47] A. Schmidt. *Einführung in die algebraische Zahlentheorie*. Springer-Verlag, 2007.

[48] M. Sørensen und P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*. Bd. 149. Stud. Logic Found. Math. Elsevier, 2006. URL: http://disi.unitn.it/~bernardi/RSISE11/Papers/curry-howard.pdf.

[49] T. Streicher. *Introduction to category theory and categorical logic*. 2004. URL: http://www.mathematik.tu-darmstadt.de/~streicher/CTCL.pdf.

[50] The Coq development team. *The Coq proof assistant reference manual*. Version 8.4pl3. 2013. URL: http://coq.inria.fr/distrib/current/refman/.

[51] A. S. Troelstra und D. van Dalen. *Constructivism in Mathematics: An Introduction*. North-Holland Publishing, 1988.

[52] S. Vickers. „Locales and toposes as spaces“. In: *Handbook of Spatial Logics*. Hrsg. von M. Aiello, I. Pratt-Hartmann und J. van Benthem. Springer-Verlag, 2007, S. 429–496. URL: http://www.cs.bham.ac.uk/~sjv/LocTopSpaces.pdf.

[53] P. Wadler. *Proofs are Programs: 19th Century Logic and 21st Century Computing*. 2000. URL: http://homepages.inf.ed.ac.uk/wadler/papers/frege/frege.pdf.

[54] R. Zach. „Hilbert's program“. In: *The Stanford Encyclopedia of Philosophy*. Hrsg. von N. Zalta. 2009. URL: http://plato.stanford.edu/entries/hilbert-program/.

[55] R. Zach. *Hilbert's program then and now*. 2005. URL: http://people.ucalgary.ca/~rzach/papers/hptn.pdf.