

Pizzaseminar zu konstruktiver Mathematik

21. August 2013

in Entstehung befindlich, nur grobe Zusammenfassung

Inhaltsverzeichnis

1 Was ist konstruktive Mathematik?	1
1.1 Widerspruchsbeweise vs. Beweise von Negationen	2
1.2 Informale Bedeutung logischer Aussagen	3
2 Beispiele	5
2.1 Diskretheit der natürlichen Zahlen	5
2.2 Minima von Teilmengen der natürlichen Zahlen	6
2.3 Potenzmengen	7
2.4 Die De Morganschen Gesetze	7
3 Nutzen konstruktiver Mathematik	8
4 Die Schlussregeln intuitionistischer Logik	11
5 Beziehung zu klassischer Logik	13

1 Was ist konstruktive Mathematik?

Proposition 1.1. *Es gibt irrationale Zahlen x, 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 $x := \sqrt{2}^{\sqrt{2}}$, $y := \sqrt{2}$. \square

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. \square

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 LEM. Das *Prinzip der Doppelnegationselimination*, demnach man für jede Aussage φ voraussetzen darf, dass $\neg\neg\varphi \Rightarrow \varphi$ gilt, ist zu LEM 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 2.1 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 einen eindeutigen Wahrheitswert hat. Diese Charakterisierung mag bei klassischer Logik noch 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 natürlich 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.

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

$$\neg\psi := (\psi \Rightarrow \perp)$$

festgelegt. Dabei steht „ \perp “ für *Falschheit*, eine kanonische falsche Aussage. Wer mag, kann $1 = 0$ oder $\frac{1}{2}$ denken.

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

Proposition 1.5. *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. \square

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

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 Teilformeln 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

$$x \in M.$$

	klassische Logik	intuitionistische Logik
Aussage φ	Die Aussage φ gilt.	Wir haben Beleg für φ .
\perp	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.

Für *zusammengesetzte Aussagen* zeigt Tabelle 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 Belegen für $\varphi(x)$ Belege 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 *gleichmäßig* in der Tabelle gemeint.

Beispiel 1.6. 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 1.7. 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 1.8. 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 die doppelt negierte Aussage

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

vertreten.

Beispiel 1.9 ([7]). 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. Daher gab es für keine der beiden Straftaten einen Beleg, Kate Moss wurde daher nicht strafrechtlich verfolgt.

...über Berechenbarkeit

Es gibt noch eine zweite Interpretation, die beim Verständnis konstruktiver Mathematik sehr hilfreich ist:

Motto 1.10. *Eine Aussage gilt konstruktiv genau dann, 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).

Bemerkung 1.11. Das Motto kann man tatsächlich zu einem formalen Theorem präzisieren, das ist Gegenstand der gefeierten Curry–Howard-Korrespondenz.

2 Beispiele

2.1 Diskretheit der natürlichen Zahlen

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

Proposition 2.1. *Für beliebige natürlichen Zahlen $x, y \in \mathbb{N}$ gilt: $x = y \vee \neg(x = y)$.*

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

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, 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 Proposition 1.6 in [6].

2.2 Minima von Teilmengen der natürlichen Zahlen

In klassischer Logik gilt folgendes Minimumsprinzip:

Proposition 2.2 (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 diese Aussage nicht zeigen – wegen der Abwärtskompatibilität kann man zwar auch nicht ihr Gegenteil nachweisen, aber man kann ein sog. *brouwersches Gegenbeispiel* anführen:

Proposition 2.3. *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 Diskrettheit 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 $z \neq 0$). \square

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

Definition 2.4. 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 2.5. *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 diskret ist, gilt für jede Zahl $0 \leq m \leq n$: $m \in U$ oder $m \notin U$. Daher können wir diese Zahlen der Reihe nach durchgehen; die erste Zahl mit $m \in U$ ist das gesuchte Minimum. \square

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 2.6. 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.

2.3 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. Das ist Gegenstand einer Übungsaufgabe.

2.4 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 man eine Imitationsgrundlage für die Bearbeitung des ersten Übungsblatts hat. Es wird das Wort „Widerspruch“ vorkommen, aber wir haben ja schon in Abschnitt 1.1 diskutiert, dass das nicht automatisch unkonstruktiv ist.

Proposition 2.7. *Für alle Aussagen φ und ψ gilt*

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

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

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. Dann 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 2.8. *Folgende Prinzipien sind zueinander äquivalent:*

1. *LEM für negierte Aussagen: Für alle Aussagen φ gilt $\neg\varphi \vee \neg\neg\varphi$.*
2. *Für alle Aussagen φ und ψ gilt $\neg(\varphi \wedge \psi) \implies \neg\varphi \vee \neg\psi$.*

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. \implies 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. \implies 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. \square

3 Nutzen konstruktiver Mathematik

Spaß. Konstruktive Mathematik macht Spaß!

Philosophie. Konstruktive Logik ist philosophisch einfacher zu rechtfertigen als klassische Logik.

Eleganzassistentz. Konstruktive Mathematik kann einen dabei unterstützen, Aussagen, Beweise und ganze Theoriegebäude eleganter zu formulieren. Etwa hat man klassisch oft *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 sind. In konstruktiver Mathematik wird man nun insofern darauf aufmerksam gemacht, als dass der Nachweis, dass diese Einschränkungen in bestimmten Fällen erfüllt sind, nicht mehr trivial ist, sondern Nachdenken erfordert.

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

Proposition 3.1. *Sei $f : X \rightarrow Y$ eine Abbildung und $f^{-1}[_] : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ 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 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. \square

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

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 sehr diffizil und interessant sein. Wir werden zu diesem Thema noch einen mathematischen Zaubertrick kennenlernen.

Programmextraktion. Aus jedem konstruktiven Beweis einer Behauptung kann man maschinell, ohne manuelles Zutun, ein Computerprogramm extrahieren, welches die untersuchte Behauptung bezeugt (und 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.

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.

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

Jede Abbildung $\mathbb{R} \rightarrow \mathbb{R}$ ist stetig.

oder

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

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 Metatheoreme, 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.

Bemerkung 3.2. Hier ein kurzer Einschub, wieso das erstgenannte Traumaxiom in einem konstruktiven Kontext zumindest nicht offensichtlich widersprüchlich ist. Man könnte denken, dass die Signumsfunktion

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

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 [2].

Alternative Mathematik-Universen. Wenn man ganz normal Mathematik betreibt, arbeitet man tatsächlich *intern im Topos der Mengen*. Es gibt aber auch andere interessante Topoi; deren interne Sprache ist aber fast immer nicht klassisch.

- Vielleicht hat man einen bestimmten topologischen Raum X besonders lieb und möchte daher, dass alle untersuchten Objekte vom aktuellen Aufenthaltsort auf 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 sehr 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 erwähnt, was mit der Topossichtweise möglich ist:

- Aus dem recht einfach nachweisbaren Faktum konstruktiver linearer Algebra, dass jeder endlich erzeugte Vektorraum nicht eine endliche Basis besitzt, folgt *ohne weitere Arbeit* sofort folgende offensichtlich kompliziertere Aussage, wenn man 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.

- Zu quantenmechanischen Systemen kann man eine C^* -Algebra assoziieren. Wichtiges Merkmal ist, dass diese in allen interessanten Fällen *nichtkommutativ* sein wird. Nun gibt es aber ein alternatives Universum, den sog. *Bohr-Topos*, aus dessen Sicht diese Algebra kommutativ ist; auf diese Weise vereinfacht sich manches. (Was genau, werden wir noch gemeinsam herausfinden.)

4 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.

Variablenkontexte

Definition 4.1. Ein *Kontext* ist eine endliche Folge von Variablendeklarationen der Form

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

Dabei sind die A_i *Typen* der 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

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

lediglich eine Aussage im reduzierten Kontext $n : \mathbb{N}$: Die Variable m kommt nicht mehr *frei*, sondern nur noch *gebunden* vor. Wir vereinbaren, dass die kollisionsfreie Umbenennung gebundener Variablen die Aussage nicht verändert. 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

Ist φ eine Aussage im Kontext x_1, \dots, x_n . Sind dann Terme s_1, \dots, s_n (in einem neuen Kontext y_1, \dots, y_m) gegeben, so kann man die x_i *simultan durch die s_i ersetzen*. Als Ergebnis erhält man eine Formel im Kontext y_1, \dots, y_m , die man „ $\varphi[s_1/x_1, \dots, s_n/x_n]$ “ 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

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

Ableitungen

Definition 4.2. 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.

Beispiel 4.3. Werde noch ein Beispiel überlegen. In der Zwischenzeit ein Scan aus dem Elephant-Buch (Seite 832):

$$\frac{\frac{((\phi \wedge \psi) \vdash_{\vec{x}, \mathbf{y}} \phi)}{((\exists \mathbf{y})(\phi \wedge \psi) \vdash_{\vec{x}} \phi)} \quad \frac{\frac{((\phi \wedge \psi) \vdash_{\vec{x}, \mathbf{y}} \psi) \quad \frac{((\exists \mathbf{y})\psi \vdash_{\vec{x}} (\exists \mathbf{y})\psi)}{(\psi \vdash_{\vec{x}, \mathbf{y}} (\exists \mathbf{y})\psi)}}{((\phi \wedge \psi) \vdash_{\vec{x}, \mathbf{y}} (\exists \mathbf{y})\psi)}}{((\exists \mathbf{y})(\phi \wedge \psi) \vdash_{\vec{x}} (\exists \mathbf{y})\psi)}}{((\exists \mathbf{y})(\phi \wedge \psi) \vdash_{\vec{x}} (\phi \wedge (\exists \mathbf{y})\psi))}$$

Diese Ableitung beweist (eine Richtung des) *Frobenius-Prinzips*.

Peano-Arithmetik und Heyting-Arithmetik

Definition 4.4. Das formale System *Heyting-Arithmetik* ist gegeben durch

- intuitionistische Logik,
- die Gleichheitsregeln (siehe Tafel 3),
- einem einzigen Typ \mathbb{N} ,
- einer Termkonstante $0 : \mathbb{N}$,

Strukturelle Regeln

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

Regeln für Konjunktion

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

Regeln für Disjunktion

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

Doppelregel für Implikation

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

Doppelregeln für Quantifikation

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

Tafel 2: Die Schlussregeln intuitionistischer Logik.

- 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

$$\frac{}{S(n) = 0 \vdash_n \perp} \quad \frac{}{S(n) = S(m) \vdash_{n,m} n = m}$$

und das Induktionsprinzip

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

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

Definition 4.5. Das formale System *Peano-Arithmetik* ist genau wie Heyting-Arithmetik gegeben, nur mit klassischer statt intuitionistischer Logik.

5 Beziehung zu klassischer Logik

Doppelnegationsübersetzung, Continuation-Passing-Style Transformation, historische Einordnung: Hilberts Programm, ...

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 $x_1 = y_1 \wedge \dots \wedge x_n = y_n$.)

Prinzip vom ausgeschlossenen Dritten

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

Tafel 3: Weitere Schlussregeln mancher formaler Systeme.

Literatur

- [1] A. Bauer. *Mathematics and computation*. Blog. URL: <http://math.andrej.com/category/constructive-math/>.
- [2] A. Bauer. *Sometimes all functions are continuous*. Artikel des Blogs *Mathematics and computation*.
- [3] 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.
- [4] D. van Dalen. „Intuitionistic logic“. In: *The Blackwell Guide to Philosophical Logic*. Hrsg. von L. Goble. Blackwell Publishers, 2011, S. 224–257.
- [5] R. Mines, F. Richman und W. Ruitenburg. *A Course in Constructive Algebra*. Universitext. Springer-Verlag, 1988.
- [6] M. Nieper-Wißkirchen. *Galoissche Theorie*. 2013. URL: http://alg.math.uni-augsburg.de/lehre/vorlesungsskripte/einfuehrung-in-die-algebra/at_download/file.
- [7] sigfpe. *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>.
- [8] A. S. Troelstra und D. van Dalen. *Constructivism in Mathematics: An Introduction*. North-Holland Publishing, 1988.