Pizzaseminar zu konstruktiver Mathematik

6. September 2013

in Entstehung befindlich, nur grobe Zusammenfassung

Inhaltsverzeichnis

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 $x := \sqrt{2}^{\sqrt{2}}$, $y := \sqrt{2}$. □

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 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 entweder wahr oder falsch ist. 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

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

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 1.5. *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. □

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 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

$$x \in M.$$

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

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

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.

	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.
$\forall x : X\colon \varphi(x)$	Für alle $x : X$ stimmt jeweils $\varphi(x)$.	Wir können (gleichmäßig) für alle $x : X$ Belege für $\varphi(x)$ konstruieren.
$\exists x : X\colon \varphi(x)$	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 1.9 ([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 Strafttaten 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

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

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. □

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 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 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. □

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

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. 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. $\Rightarrow$ 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. $\Rightarrow$ 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. □

3. Nutzen konstruktiver Mathematik

Spaß. Konstruktive Mathematik macht Spaß!

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

Eleganzassistenz. 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 $f : X \to Y$ 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 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 $f^{-1}[\operatorname{im} f] = f^{-1}[X]$ und damit $\operatorname{im} f = X$, also ist f surjektiv. □

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 $\mathbb{R} \to \mathbb{R}$ 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

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

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 [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 bestimmen 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 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.

4.1. Formale logische Sprache

Variablenkontexte

Definition 4.1. 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* 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

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

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

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

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

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

Substitution von Variablen

Ist 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 Formel im Kontext $y_1, \ldots, y_m$, die man „$\varphi[s_1/x_1, \ldots, x_n/x_n]$“ oder kürzer „$\varphi[\vec{s}/\vec{x}]$“ schreibt.

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

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

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

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

4.2. Sequenzen

Definition 4.2. 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 $n + 1$ keine Primzahl 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 $n + 1$ keine Primzahl ist.

Der Unterschied ist subtil, aber sprachlich durchaus vorhanden.

Bemerkung 4.3. 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.

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

4.3. Ableitungen

Definition 4.4. 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.

Aus dem Kontext muss hervorgehen, ob man eine Sequenz nur als solche diskutieren möchte 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.

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

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

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.

Eine der Disjunktionsregeln

Die Disjunktionsregel

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

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

Umfang der Ableitungsregeln

Motto 4.6. Alle *Beweise gewöhnlicher Mathematik, die man gemeinhin als „vollständig und präzise ausformuliert", lassen sich als Ableitungen im Sinne der Definition formalisieren (ggf. unter Hinzunahme klassischer logischer Axiome, Mengentheorieaxiome oder Typtheorieaxiome).*

Aufgabe 4.7. 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: „aus $\varphi \wedge \psi$ folgt schlicht φ“) und *eliminiert* (etwa: „kann man sowohl φ als auch ψ ableiten, so auch $\varphi \wedge \psi$“).

Bemerkung 4.8. 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 4.9. Hier ein längeres Beispiel für eine Ableitung (ein Scan aus dem Elephant-Buch, 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*.

Nicht verschwiegen werden sollte folgende Ergänzung des formalistischen Kredos:

Motto 4.10. *Das optimistische Motto 4.6 stimmt nur in erster Näherung. Es gibt mathematische Gedanken, die nicht formalisierbar sind.*

Das ausführen!

4.4. Peano-Arithmetik und Heyting-Arithmetik

Definition 4.11. 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

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

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

Definition 4.13. 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*.

5. Beziehung zu klassischer Logik: die Doppelnegationsübersetzung

Aus den Augen einer konstruktiven Mathematikerin sind manche Aussagen ihrer klassisch arbeitenden Kollegen falsch. Es gibt aber eine einfache Übersetzung, die *Doppelnegationsübersetzung*, die Aussagen derart umformt, dass die Übersetzung genau dann konstruktiv gilt, wenn die ursprüngliche Aussage klassisch gilt. Mit dieser kann die konstruktive Mathematikern daher ihre Kollegen verstehen, ohne ihre Logik verlassen zu müssen.

Definition 5.1. Die *Doppelnegationsübersetzung* (nach Kolmogorov, Gentzen, Gödel und anderen) wird rekursiv wie folgt definiert:

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

Bemerkung 5.2. Da $\neg\varphi :\equiv (\varphi \Rightarrow \bot)$, gilt $(\neg\varphi)^\circ \equiv \neg(\varphi^\circ)$.

Aufgabe 5.3. 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.

Satz 5.4. *Seien φ, 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. Wegen der Abwärtskompatibilität intuitionistischer Logik und Teilaussage a) gilt trivialerweise auch die Umkehrung.

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

b) Induktion über den Aussageaufbau, ausgelassen.

c) Wir müssen 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 überlassen wir den Leser (Übungsblatt 2). □

Korollar 5.5. *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 einer Ableitung von $\bot^\circ \equiv \bot$ in Heyting-Arithmetik überführen. □

Folgendes Lemma werden wir erst später, im Abschnitt über Friedmans Trick, benötigen:

Lemma 5.6. *Sei φ eine Aussage, in der nur $\top$, $\bot$, $\wedge$, $\vee$ und $\exists$ (über bewohnte Typen), aber nicht $\Rightarrow$ oder $\forall$ vorkommen. Dann gilt intuitionistisch: $\varphi^\circ \iff \neg\neg\varphi$.*

Beweis. Induktion über den Aussageaufbau. □

5.1. Interpretation der übersetzten Aussagen

Uns allen ist die Dialogmetapher zur Interpretation logischer Aussagen bekannt: 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 5) 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; Alice kann unter der Konsistenzannahme also nur dann $\neg\varphi$ vertreten, wenn es keinen Beleg von φ gibt.

Als Motto können wir festhalten:

Motto 5.7. *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 begründen.

Motto 5.8. *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 kann.*

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 muss daher an dieser Stelle bluffen. Da sie die Implikation $(\varphi \Rightarrow \bot)$ behauptet, 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. Genauer betrachten wir einen Dialog zur Doppelnegationsübersetzung des Prinzips vom ausgeschlossenen Dritten, also zu $\neg\neg(\varphi^\circ \vee \neg\varphi^\circ)$. Wir können sogar für beliebige Aussagen φ das Prinzip $\neg\neg(\varphi \vee \neg\varphi)$ nachweisen, ausgeschrieben

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

das ist geringfügig übersichtlicher.

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.

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

6. Beziehung zur theoretischen Informatik: die Curry-Howard-Korrespondenz

7. Hilberts Programm

7.1. Die mathematische Welt um 1900

Unvollständig und falsch.

Hilberts Programm: Zeige, dass man aus jedem Beweis einer konkreten Aussage, welcher beliebige ideelle Prinzipien (Prinzip vom ausgeschlossenen Dritten für beliebige Aussagen, Auswahlaxiom, maximale Ideale in der Algebra) verwendet, einen finitistisch zulässigen Beweis erhalten kann.

In voller Allgemeinheit gilt Hilberts Programm als *gescheitert*. Denn 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 doch realisiert werden, unter anderem in Analysis und Algebra: Mittels *proof mining* kann aus klassischen Beweisen mehr oder weniger systematisch noch konstruktiver Inhalt extrahiert werden. Je nach Situation kann *konstruktiver Inhalt* etwa

- explizite Schranken für Konstanten,
- stetige (oder noch bessere) Abhängigkeit von Paramtern,
- explizite Zeugen von Existenzbehauptungen oder
- Algorithmen

umfassen.

Motto 7.1. *In einem* Beweis *einer Aussage steckt viel mehr Inhalt als die bloße Information, dass die Aussage wahr ist.*

7.2. Beispiel aus der Zahlentheorie: Friedmans Trick

Definition 7.2. Die *Friedmanübersetzung* wird für eine feste Aussage F wie folgt rekursiv definiert:

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

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

Bemerkung 7.3. Da $\neg\varphi :\equiv (\varphi \Rightarrow \bot)$, gilt $(\neg\varphi)^F \equiv (\varphi^F \Rightarrow F)$.

Satz 7.4. *a) Sei φ eine Aussage, in der Existenzquantoren nur über bewohnte Typen gehen. Dann gilt intuitionistisch: $F \Longrightarrow \varphi^F$.*

b) Sei φ eine Aussage, in der nur $\top$, $\bot$, $\wedge$, $\vee$ und $\exists$ (über bewohnte Typen), 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 $\vec{x}$, in der Existenzquantoren nur über bewohnte Typen gehen. Wenn $\varphi \vdash_{\vec{x}} \psi$ intuitionistisch, dann gilt auch $\varphi^F \vdash_{\vec{x}} \psi^F$ intuitionistisch.

Beweis. a) Induktion über den Aussageaufbau. Exemplarisch zeigen wir den Fall

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

Gelte also F. Da X bewohnt ist, gibt es ein $x : X$. Nach Induktionsvoraussetzung können wir $F \Rightarrow \varphi^F$ voraussetzen. Somit folgt φ^F, das war zu zeigen.

b) Induktion über den Aussageaufbau.

c) Induktion über den Aufbau intuitionistischer Ableitungen. Wie beim analogen Theorem über die Doppelnegationsübersetzung (Satz 5.4) muss man zeigen, dass die Friedmanübersetzungen der Schlussregeln gültig sind. Das ist sogar einfacher als bei der Doppelnegationsübersetzung. □

Korollar 7.5. *Peano-Arithmetik ist für Aussagen der Form $\forall(\cdots \Rightarrow \cdots)$, wobei die Teilaussagen den Beschränkungen aus 7.4b) unterliegen müssen, konservativ über Heyting-Arithmetik: Aus jedem Beweis in Peano-Arithmetik lässt sich ein Beweis in Heyting-Arithmetik gewinnen.*

Beweis. Gelte $\top \vdash (\forall x : X\colon \varphi \Rightarrow \psi)$ 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 5.4) 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 5.6); also ist die Sequenz

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

in Heyting-Arithmetik ableitbar. Nun können wir die Friedmanübersetzung bezüglich einer 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 φ zu wählen. Dann vereinfachen sich die Ausdrücke und wir erhalten die Ableitbarkeit von $\varphi \vdash_x \psi$, also von

$$\top \vdash (\forall x : X\colon \varphi \Rightarrow \psi)$$

in Heyting-Arithmetik. □

Beispiel 7.6. Die Aussage der Zahlentheorie, dass es unendlich viele Primzahlen gibt, lässt sich in der Form

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

schreiben. Zur Formalisierung der Primalitätsaussage benötigt man nur *beschränkte Allquantifikation*, für welche die Konservativitätsaussage ebenfalls gilt. Also kann man

aus jedem klassischen Beweis der Unendlichkeit der Primzahlen einen konstruktiven extrahieren.

Beispiel 7.7. 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“).

7.3. Beispiel aus der Algebra: dynamische Methoden

In der kommutativen Algebra sind viele Techniken gebräuchlich, mit deren Hilfe man bestimmte konkrete Aussagen beweisen kann, deren Gültigkeit man aber nur in klassischer Logik und unter Verwendung starker Auswahlprinzipien beweisen kann. Drei 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 A.13).
- 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.

Standardbeispiel: Nilpotente Polynome

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

Proposition 7.8 (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 A.15) 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 nur das Nilpotenzkriterium und das auch anderweitig nützliche Lemma A.15 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?

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

Axiomatisierung des generischen Primideals

Sei R ein Ring.

Definition 7.10. Die Axiome für das *generische Primideal* sind folgende.

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 7.11. *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 7.10 nur die strukturellen Regeln

und die Regeln für Konjunktion und Disjunktion verwendet (siehe Tafel 2), kann man einen expliziten Zeugen der Aussage

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

extrahieren (siehe Definitionen A.6 und A.16 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 7.1, demnach in Beweisen von Aussagen viel mehr Inhalt steckt als die bloße Information über die Wahrheit der Behauptung. Bevor wir den Beweis führen (welcher erstaunlich einfach ist), wollen wir das Resultat aber noch genauer diskutieren.

Korollar 7.12. *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 die Nilpotenz von x folgt. Diese stärkere Aussage kann man (bewiesenermaßen) nur in einem klassischen Rahmen zeigen. Stattdessen kann man lediglich aus einem entsprechend formalisierten *Beweis*, dass x in allen Primidealen enthalten ist, die Nilpotenz von x folgern.

Bemerkung 7.13. 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.)

Beweis des Satzes

Beweis von Satz 7.11. Wir geben ein explizites *Modell* der 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 Idealinklusion. Lemma A.19 ist für das Verständnis der folgenden Übersetzungstabelle hilfreich. Konkret definieren wir

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

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 überlassen wir dem Leser. 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:

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

□

A. Ideale in Ringen

A.1. Grundlegende Konzepte

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

Beispiel A.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.

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

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

Die Axiome werden durch folgendes Beispiel motiviert:

Beispiel A.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 dagegen langweilig: Körper besitzen stets nur genau zwei Ideale, nämlich das sog. Nullideal $(0) = \{0\}$ und das sog. Einsideal $(1) = K$.

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

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

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

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

Beispiel A.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.

A.2. Historische Motivation für Idealtheorie

Historisch gab es eine große Motivation, dieses Konzept 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. 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 unsicherte Voraussetzung diese Eigenschaft hatten.

Leider stellte es sich heraus, dass diese Eigenschaft vielen der interessanten Ringe *nicht* zu kam. 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 Primidealen 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 [8] von Alexander Schmidt empfohlen. Als Vorwissen setzt es nur Schulkenntnisse voraus.

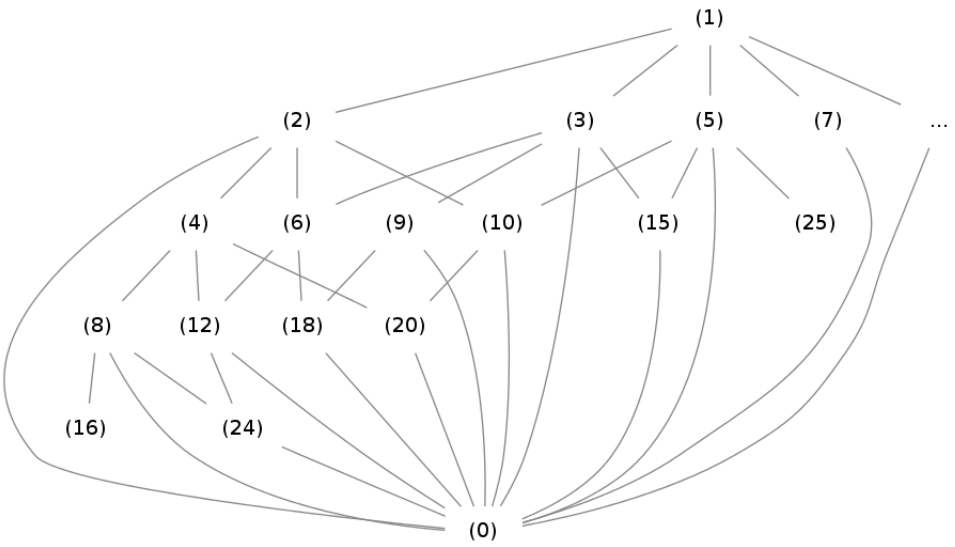
A.3. Die Ideale im Ring der ganzen Zahlen

Die Tafel 4 zeigen die Ideale des Rings $\mathbb{Z}$. Ergänzt man die aus Platzgründen ausgelassenen Ideale, ist das sogar eine vollständig Übersicht über *alle* Ideale von $\mathbb{Z}$ – wenn man klassische Logik voraussetzt.

A.4. Primideale und Nilpotenz

Definition A.10. Ein Element $x \in R$ eines Rings R heißt genau dann *nilpotent*, wenn eine gewisse Potenz Null ist:

$$x^n = 0 \qquad \text{für ein } n \geq 0.$$



Tafel 4: Modulo Platz und klassische Logik eine vollständige Übersicht über alle Ideale von $\mathbb{Z}$.

Beispiel A.11. Im Ring $\mathbb{Z}/(4)$ ist das Element $[2]$ nilpotent.

Proposition A.12. *Die nilpotenten Elemente eines Rings liegen in allen Primidealen des Rings.*

Beweis. Sei x mit $x^n = 0$ ein nilpotentens 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. □

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 A.13 (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

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

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

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

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. 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 Metatheorem absolut erstaunlich:

Wunder A.14. *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.*

Polynome mit Koeffizienten in Primidealen

Für das Beispiel in Abschnitt 7.3 benötigen wir folgendes Lemma.

Lemma A.15. *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 $S[X]$.

A.5. Radikalideale

Definition A.16. 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 Ring. Dann heißt das Ideal

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

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

Beispiel A.17. Das Ideal $(12) \subseteq \mathbb{Z}$ ist kein Radikalideal, $\sqrt{(12)} = (6)$ dagegen schon.

Bemerkung A.18. 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 A.19. *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*

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

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 A.20. Für den Ring der ganzen Zahlen gilt $(6) \cap (5) = (30)$ und $(6) \cap (15) = (30)$.

Beispiel A.21. Allgemein gilt

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

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/einfuhrung-in-die-algebra/at_download/file`.

[7] 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`.

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

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