Spiel und Spaß mit der internen Welt des kleinen Zariski-Topos

Ingo Blechschmidt

19. Dezember 2013

$R \models x = y : \mathcal{O}$	$:\Longleftrightarrow$	Für die gegebenen Elemente $x, y \in R$ gilt $x = y$.
$R \models \top$	$:\Longleftrightarrow$	$1 = 1 \in R$. (Das ist stets erfüllt.)
$R \models \bot$	$:\Longleftrightarrow$	$1 = 0 \in R$. (Das ist genau in Nullringen erfüllt.)
$R \models \phi \wedge \psi$	$:\Longleftrightarrow$	$R \models \phi$ und $R \models \psi$.
$R \models \phi \vee \psi$	$:\Longleftrightarrow$	~~$R \models \phi$ oder $R \models \psi$.~~
$R \models \phi \vee \psi$	$:\Longleftrightarrow$	Es gibt eine Zerlegung $\sum_i s_i = 1 \in R$ sodass für alle i jeweils $R[s_i^{-1}] \models \phi$ oder $R[s_i^{-1}] \models \psi$.
$R \models \phi \Rightarrow \psi$	$:\Longleftrightarrow$	Für jedes $s \in R$ gilt: Aus $R[s^{-1}] \models \phi$ folgt $R[s^{-1}] \models \psi$.
$R \models \forall x : \mathcal{O}.\ \phi$	$:\Longleftrightarrow$	Für jedes $s \in R$ und jedes $x \in R[s^{-1}]$ gilt: $R[s^{-1}] \models \phi(x)$.
$R \models \exists x : \mathcal{O}.\ \phi$	$:\Longleftrightarrow$	Es gibt eine Zerlegung $\sum_i s_i = 1 \in R$ und Elemente $x_i \in R[s_i^{-1}]$ sodass für alle i: $R[s_i^{-1}] \models \phi(x_i)$.

Die Kripke–Joyal-Semantik des kleinen Zariski-Topos.

Zusammenfassung

Neben der üblichen mathematischen Welt gibt es alternative mathematische Universen, sog. *Topoi*. In diesen gelten leicht andere Gesetze der Logik. Speziell gibt es zu jedem kommutativen Ring seinen zugehörigen *kleinen Zariski-Topos*, der darauf zugeschnitten ist, um *lokal* über den Ring zu sprechen. In diesen informalen Notizen wollen wir verstehen, wie man in diesem alternativen Universum arbeiten kann.

Illustrationen: Carina Willbold

Inhaltsverzeichnis

1. Vorbereitungen

1.1. Etwas formale Logik

Im Folgenden wollen wir über mathematische Aussagen sprechen, in denen

$$= \quad \top \quad \bot \quad \wedge \quad \vee \quad \Rightarrow \quad \forall \quad \exists$$

die einzigen vorkommenden logischen Symbole sind. Dabei steht „$\bot$“ für eine ausgezeichnete falsche und „$\top$“ für eine ausgezeichnete wahre Aussage. Negation ist ebenfalls wichtig, muss aber nicht als primitiv angenommen werden, da man sie über die Beziehung

$$\neg\phi \quad :\equiv \quad (\phi \Rightarrow \bot)$$

durch $\Rightarrow$ und $\bot$ ausdrücken kann: Zu behaupten, dass ϕ nicht stimmt, ist gleichbedeutend damit, zu behaupten, dass aus der Annahme von ϕ ein Widerspruch folgt. Wir schreiben die universelle und existenzielle Quantifikation nicht mit dem Elementsymbol, sondern dem in der Typtheorie üblichen Doppelpunkt:

$$\forall x : X.\ \phi(x).$$

Gelegentlich werden wir die Abhängigkeit von $\phi(x)$ von x in der Notation unterdrücken und kurz nur „ϕ“ schreiben. Ferner verwenden wir den Quantor der eindeutigen Existenz, formal definiert als

$$\exists! x : X.\ \phi(x) \quad :\equiv \quad \big(\exists x : X.\ \phi(x)\big) \ \wedge\ \big(\forall x : X.\ \forall x' : X.\ (\phi(x) \wedge \phi(x') \Rightarrow x = x')\big).$$

1.2. Geometrische Vorstellung von Ringen

Zu einem kommutativen Ring R können wir uns einen geometrischen Raum $\operatorname{Spec} R$ vorstellen, und zwar auf solche Art und Weise, dass ein Ringelement $s \in R$ einer „guten“ Funktion auf $\operatorname{Spec} R$ entspricht. Den Ort, wo diese Funktion nicht verschwindet, wollen wir mit „$D(s)$“ bezeichnen. Dieser Ort ist stets eine offene Menge.

Beispiel 1.1. Den Ring $K[X, Y]$ stellen wir uns geometrisch als K^2 vor. Zum Element $s := 2X + 3Y$ gehört dann die Funktion $(x, y) \mapsto 2x + 3y$. Die Menge $D(s)$ ist das Komplement einer schrägen Gerade in K^2.

In diesem Bild können wir uns eine Zerlegung $1 = \sum_i s_i \in R$ der Eins als eine Überdeckung $\bigcup_i D(s_i)$ von $\operatorname{Spec} R$ vorstellen: Da die Einsfunktion nirgendwo Null ist, können an keinem Punkt alle s_i zugleich verschwinden.

2. Die Kripke–Joyal-Semantik des kleinen Zariski-Topos

Zu jedem kommutativen Ring R gehört ein alternatives Mathematik-Universum, der *kleine Zariski-Topos zu R*. Uns fehlen kategorientheoretische Konzepte, um dieses Universum explizit anzugeben (obwohl das nicht intrinsisch schwer ist). Wir können aber beschreiben, was es bedeuten soll, dass *eine Aussage ϕ in dem kleinen Zariski-Topos zu R gilt*, in Formeln ausgedrückt als

$$R \models \phi.$$

Definition 2.1. Die Bedeutung von Aussagen der *internen Sprache des Zariski-Topos* soll durch Rekursion über den Aussageaufbau durch die auf der ersten Seite angegebenen Übersetzungsregeln festgelegt sein.

Auf den ersten Blick erscheinen diese Regeln völlig willkürlich. Tatsächlich aber sind sie fein aufeinander abgestimmt, schon kleine Änderungen führen dazu, dass das gesamte System zusammenbricht. In diesem Rahmen wollen wir sie schlichtweg als gegeben hinnehmen. Durch die Beispiele im folgenden Abschnitt werden wir uns schnell an sie gewöhnen.

In dem kleinen Zariski-Topos zu R gibt es ein Abbild des Rings R, das wir „$\mathcal{O}$“ schreiben. (Diese Bezeichnung hat nichts mit Ganzheitsringen zu tun.)

3. Erste Gehversuche in der internen Welt

3.1. Interne Kommutativität

Mit den Übersetzungsregeln an der Hand können wir beginnen, die interne Welt zu erkunden. Folgende Beobachtung macht den Anfang:

Proposition 3.1. *Der Ring $\mathcal{O}$ des kleinen Zariski-Topos zu R ist wieder kommutativ – das heißt:*

$$R \models \forall x, y : \mathcal{O}.\ xy = yx.$$

Beweis. Die Doppelquantifikation in der Behauptung ist eine Kurzschreibweise für

$$R \models \forall x : \mathcal{O}.\ \forall y : \mathcal{O}.\ xy = yx.$$

Gemäß den Regeln bedeutet das:

> Für alle $s \in R$ und alle $x \in R[s^{-1}]$ gilt:
>
> > Für alle $t \in R[s^{-1}]$ und alle $y \in R[s^{-1}][t^{-1}]$ gilt:
> >
> > > In $R[s^{-1}][t^{-1}]$ gilt $xy = yx$.

Das erscheint vielleicht etwas verklausuliert, ist aber auch offensichtlich wahr. □

3.2. Interne Invertierbarkeit

Das folgende Lemma ist ähnlich. Es besagt, dass es keinen Unterschied zwischen Invertierbarkeit aus interner und externer (also üblicher) Sicht gibt.

Proposition 3.2. *Genau dann ist ein Ringelement $f \in R$ invertierbar, wenn es als Element von $\mathcal{O}$ invertierbar ist, wenn also*

$$R \models \exists g : \mathcal{O}.\ fg = 1.$$

Beweis. Die Übersetzung der internen Aussage lautet:

> Es gibt eine Zerlegung $1 = \sum_i s_i \in R$, sodass für jeden Index i ein Element $g_i \in R[s_i^{-1}]$ mit $fg_i = 1$ in $R[s_i^{-1}]$ existiert.

Damit ist es nur noch eine Übungsaufgabe in elementarer Ringtheorie, die behauptete Äquivalenz nachzuweisen. □

3.3. Interne Lokalität

Diese beiden Propositionen waren noch nicht besonders beeindruckend. Die folgende Proposition ist dagegen beim ersten Kontakt völlig verblüffend und illustriert gut den kuriosen Charakter der internen Welt. Dazu erinnern wir an das Konzept eines lokalen Rings:

Definition 3.3. Ein Ring heißt genau dann *lokal*, wenn, wann immer eine Summe von Ringelementen invertierbar ist, schon mindestens ein Summand invertierbar ist.

Beispiel 3.4. Die vertrauten Ringe $\mathbb{Z}$ und $K[X, Y]$ sind nicht lokal. Oft erhält man lokale Ringe durch geeignete Lokalisierung: Jeder Körper ist lokal, die Lokalisierung $\mathbb{Z}_{(p)}$ nach einem Primideal (p) ist lokal, der Ring $K[X, Y]_{(X-a,Y-b)} = \{f/g \mid f, g \in K[X, Y], g(a, b) \neq 0\}$ der in beliebig kleinen Umgebungen von $(a, b) \in K^2$ definierten rationalen Funktionen ist lokal.

Bemerkung 3.5. Die Namensgebung erklärt sich durch folgende Beobachtung: Ein lokaler Ring R ist ein solcher, sodass jede offene Überdeckung von $\operatorname{Spec} R$ schon eine einelementige Teilüberdeckung besitzt.

Proposition 3.6. *Unabhängig davon, ob R lokal ist oder nicht, ist der Ring $\mathcal{O}$ der internen Zariski-Welt stets lokal.*

Beweis. Wir zeigen, dass

$$R \models \forall x, y : \mathcal{O}.\ \ulcorner x + y \text{ inv.}\urcorner \implies \ulcorner x \text{ inv.}\urcorner \vee \ulcorner y \text{ inv.}\urcorner.$$

Die Häkchen sollen andeuten, dass der entsprechende Teil nur umgangssprachlich vorliegt und daher von der Leserin formalisiert werden muss. Unter Verwendung von Proposition 3.2 (angewendet auf R' statt R) weisen uns die Übersetzungsregeln also an, folgende Behauptung zu zeigen:

Für alle $s \in R$ und $x \in R[s^{-1}]$ gilt:

Für alle $t \in R[s^{-1}]$ und $y \in R[s^{-1}][t^{-1}]$ gilt:

Für alle $u \in R[s^{-1}][t^{-1}]$ gilt: Falls $x + y$ in $R[s^{-1}][t^{-1}][u^{-1}] =: R'$ invertierbar ist, so gibt es eine Zerlegung der Eins von R', $1 = v_1 + \cdots + v_n \in R'$, sodass in den weiter lokalisierten Ringen $R'[v_i^{-1}]$ jeweils x oder y invertierbar ist.

Der Nachweis dieser Behauptung ist eine Übungsaufgabe. □

Mit der internen Welt des kleinen Zariski-Topos kann man also jeden beliebigen Ring als einen lokalen Ring auffassen.

4. Vereinfachungsregeln

In den bisherigen Beispielen waren die übersetzten Aussagen von recht verschachtelter Form. Bevor wir fortfahren, wollen wir daher Vereinfachungsregeln festhalten, die den praktischen Umgang mit internen Aussagen angenehmer gestalten.

Lemma 4.1. *Für folgende Quantorenfiguren kann man die Regeln vereinfachen:*

$$
\begin{array}{lll}
R \models \forall x\colon\mathcal{O}.\ \forall y\colon\mathcal{O}.\ \phi & :\Longleftrightarrow & \textit{Für alle } s \in R \textit{ und } x, y \in R[s^{-1}] \textit{ gilt } R[s^{-1}] \models \phi(x, y). \\
R \models \forall x\colon\mathcal{O}.\ \phi \Rightarrow \psi & :\Longleftrightarrow & \textit{Für alle } s \in R \textit{ und } x \in R[s^{-1}] \textit{ gilt:} \\
 & & \quad \textit{Aus } R[s^{-1}] \models \phi(x) \textit{ folgt } R[s^{-1}] \models \psi(x). \\
R \models \exists x\colon\mathcal{O}.\ \exists y\colon\mathcal{O}.\ \phi & :\Longleftrightarrow & \textit{Es gibt eine Zerlegung } 1 = \sum_i s_i \in R \textit{ und} \\
 & & \quad \textit{für jeden Index } i \textit{ Elemente } x_i, y_i \in R[s_i^{-1}] \\
 & & \quad \textit{mit } R[s_i^{-1}] \models \phi(x_i, y_i). \\
R \models \exists! x\colon\mathcal{O}.\ \phi & :\Longleftrightarrow & \textit{Für alle } s \in R \textit{ existiert genau ein } x \in R[s^{-1}] \textit{ mit} \\
 & & \quad R[s^{-1}] \models \phi(x). \\
R \models \forall x\colon\mathcal{O}.\ \exists! y\colon\mathcal{O}.\ \phi & :\Longleftrightarrow & \textit{Für alle } s \in R \textit{ und } x \in R[s^{-1}] \textit{ existiert} \\
 & & \quad \textit{genau ein } y \in R[s^{-1}] \textit{ mit } R[s^{-1}] \models \phi(x, y).
\end{array}
$$

Beweis. Sobald man die internen Aussagen übersetzt hat, muss man nur ein paar allgemeine Fakten über die Lokalisierung von Ringen nachweisen. Das ist nicht schwer, aber auch nicht besonders erhellend. □

5. Fundamentale Eigenschaften der internen Sprache

5.1. Lokalität der internen Sprache

In einem gewissen Sinn gilt $R \models \phi$ genau dann, wenn ϕ auf ganz $\operatorname{Spec} R$ gilt. Dagegen bedeutet $R[s^{-1}] \models \phi$ nur, dass ϕ auf $D(s)$ gilt.

Die interne Welt des kleinen Zariski-Topos zu R fasst nun gewissermaßen die *lokalen Aspekte* von R – solche, die genau dann ganz $\operatorname{Spec} R$ betreffen, wenn sie die einzelnen Überdeckungsmengen einer offenen Überdeckung betreffen. Die folgende Proposition macht dieses Motto präzise:

Proposition 5.1. *Sei $1 = \sum_i s_i \in R$ eine Zerlegung der Eins und ϕ eine Aussage. Dann gilt genau dann $R \models \phi$, wenn für alle i jeweils $R[s_i^{-1}] \models \phi$ gilt.*

Beweis. Induktion über den Aufbau von ϕ. □

Eine Aussage ϕ muss also nicht unbedingt im Wortlaut erfüllt sein, um in der internen Welt des kleinen Zariski-Topos zu gelten. Es genügt, dass es eine Zerlegung der Eins gibt, sodass sie in den jeweils lokalisierten Ringen gilt. Die technische Verwaltung der Zerlegungen übernimmt dabei der Übersetzungsapparat; mit der internen Welt ist es also möglich, *lokal* mit Ringen zu arbeiten, ohne manuell Zerlegungen einführen und mitschleppen zu müssen.

Beispiel 5.2. Sei R ein prüferscher Bereich. Dann ist ein endlich erzeugtes Ideal $\mathfrak{a}$ zwar nicht unbedingt ein Hauptideal, aber *lokal* ein Hauptideal – in dem Sinn, dass es eine Zerlegung $1 = \sum_i s_i$ der Eins gibt, sodass die erweiterten Ideale $\mathfrak{a}[s_i^{-1}]$ jeweils in $R[s_i^{-1}]$ Hauptideale sind. Der Ring $\mathcal{O}$ der internen Welt spiegelt diese Eigenschaft viel einfacher wieder: Er ist *bézoutsch* – jedes endlich erzeugte Ideal ist selbst schon ein Hauptideal.

5.2. Verträglichkeit mit konstruktiver Logik

Bisher haben wir die interne Welt des kleinen Zariski-Topos allein dadurch erkundet, indem wir mit den Kripke–Joyal-Regeln die Rückübersetzung in unsere gewohnte mathematische Sprache vorgenommen haben. Wenn das unsere einzige Interaktionsmöglichkeit mit der internen Welt wäre, wäre das ganze Thema nicht besonders spannend. Tatsächlich aber können wir in der internen Welt auch *mathematisch argumentieren* – fast genau so, wie wir es gewohnt sind.

Satz 5.3. *Wenn $R \models \phi$ gilt und konstruktiv aus ϕ eine weitere Aussage ψ folgt, so gilt auch $R \models \psi$.*

Beweis. Wir müssen uns zunächst überlegen, aus welchen grundlegenden Argumentationsschritten Beweise aufgebaut sind. Dann müssen wir von jedem solchen Baustein nachweisen, dass er in der internen Welt ebenfalls erfüllt ist. Etwa gibt es das logische Prinzip

Wenn $\phi \wedge \psi$ gilt, so gilt auch ϕ.

Dieses ist in der internen Sprache ebenfalls erfüllt, denn aus $R \models \phi \wedge \psi$ folgt nach den Übersetzungsregeln sofort $R \models \phi$.

Die Hauptschwierigkeit eines präzisen Beweises des Satzes liegt darin, eine übersichtliche Liste von Kernbeweisschritten derart zusammenzustellen, dass jede denkbare Argumentation so formalisiert werden kann, dass sie nur diese Bausteine verwendet. Danach ist es nur noch ein einfacher Induktionsbeweis über den Aufbau formal niedergeschriebener konstruktiver Beweise. □

Beispiel 5.4. Man kann konstruktiv zeigen, dass jede Matrix über einem lokalen Ring, die einen Rang besitzt, mittels elementarer Zeilen- und Spaltentransformationen auf eine Diagonalgestalt gebracht werden kann. Daraus folgt *ohne weiteres Zutun* sofort, dass man jede Matrix (die einen Rang besitzt) über einem *beliebigen* Ring *lokal* auf eine Diagonalgestalt bringen kann – in dem Sinn, dass es eine Zerlegung der Eins gibt, sodass in den lokalisierten Ringen die Matrix jeweils äquivalent zu einer Diagonalmatrix ist: Denn nach Proposition 3.6 ist der Ring $\mathcal{O}$ der internen Welt ja stets lokal.

Bemerkung 5.5. Ein direkter Beweis der Behauptung über die Diagonalisierbarkeit über beliebigen Ringen ist natürlich ebenfalls möglich. Er erfordert jedoch die Einführung, Verwaltung und Kombination mehrerer Zerlegungen der Eins. Diese technischen Schritte fallen bei Arbeit in der internen Welt ersatzlos weg. Um Zerlegungen der Eins muss man sich nur ein einziges Mal kümmern, nämlich im Beweis des allgemeinenen Satzes 5.3.

6. Der nichtklassische Charakter der internen Welt

Satz 5.3 erlaubt es, über den Ring $\mathcal{O}$ der internen Welt wie üblich mathematisch zu argumentieren – solange man dabei nur konstruktive Logik verwendet, also sich *nicht* auf die sonst üblichen Axiome

- *Prinzip vom ausgeschlossenen Dritten:* $\phi \vee \neg\phi$
- *Prinzip der Doppelnegationselimination:* $\neg\neg\phi \Rightarrow \phi$
- *Auswahlaxiom*

beruft. Das ist anfangs ungewohnt, bedeutet in Anwendungen der Mathematik aber oftmals keine große Einschränkung.

Die Beschränkung auf konstruktive Logik ist dabei keine Frage der Einstellung – die interne Welt erfüllt nun mal nicht die genannten klassischen Axiome. Das wollen wir in diesem Abschnitt einsehen.

Lemma 6.1. *Sei $f \in R$. Genau dann ist f in der internen Welt nicht invertierbar, wenn f im gewöhnlichen Sinn nilpotent ist.*

Beweis. Die Aussage $R \models \neg(\ulcorner f \text{ inv.}\urcorner)$ lautet ausgeschrieben

$$R \models \Big(\exists g\,{:}\,\mathcal{O}.\ fg = 1\Big) \Rightarrow \bot$$

und übersetzt sich unter Zuhilfenahme der Vereinfachungsregeln aus Lemma 4.1 und Lemma 3.2 wie folgt:

> Für alle $s \in R$ gilt:
>
> > Sollte f in $R[s^{-1}]$ invertierbar sein, so gilt $1 = 0$ in $R[s^{-1}]$ (das ist gleichbedeutend damit, dass s nilpotent ist).

Durch die Spezialisierung $s := f$ erhalten wir daher sofort die Hinrichtung. Wenn umgekehrt f nilpotent ist, enthalten die lokalisierten Ringe $R[s^{-1}]$ ein invertierbares und trotzdem nilpotentes Element. Das geht nur, wenn sie Nullringe sind. □

Proposition 6.2. *In der internen Welt des kleinen Zariski-Topos eines Rings gilt im Allgemeinen* nicht*, dass jedes Element von $\mathcal{O}$ invertierbar oder nicht invertierbar ist. Insbesondere gilt im kleinen Zariski-Topos das Prinzip vom ausgeschlossenen Dritten also* nicht*.*

Beweis. Ein Gegenbeispiel liefert der Ring $R := \mathbb{Z}$ mit dem Element $f := 2$. Denn

$$R \models \ulcorner f \text{ inv.}\urcorner \vee \neg(\ulcorner f \text{ inv.}\urcorner)$$

bedeutet, dass es eine Zerlegung $1 = s_1 + \cdots + s_n$ der Eins von $\mathbb{Z}$ gibt, sodass in den lokalisierten Ringen $\mathbb{Z}[s_i^{-1}]$ die Zahl 2 jeweils invertierbar oder nilpotent ist. In einer solchen Zerlegung muss eine der Zahlen s_i ungerade sein. In den Nennern der Elemente des zugehörigen lokalisierten Rings $\mathbb{Z}[s_i^{-1}]$ dürfen also gewisse ungerade Zahlen stehen (Potenzen von s_i). Daher ist die Zahl 2 dort weiterhin nicht invertierbar. Sie ist aber auch nicht nilpotent. □

7. Ausblick

Weitere Objekte des kleinen Zariski-Topos

Bisher haben wir nur über die Eigenschaften des Rings $\mathcal{O}$ der internen Welt des kleinen Zariski-Topos gesprochen. Genau wie in der üblichen mathematischen Welt gibt es aber auch im Zariski-Topos noch viele weitere Objekte, etwa den Polynomring $\mathcal{O}[X]$ und den Matrizenringoid $\amalg_{n,m}\mathcal{O}^{n\times m}$ sowie Objekte, die nicht zur Ringtheorie gehören, wie Analoga zu Potenzmengen.

Es ist leicht, die Regeln der Kripke–Joyal-Semantik so zu erweitern, dass man auch über diese weiteren Objekte nativ sprechen kann. In der vollen internen Sprache kann man sogar, wie im üblichen mathematischen Universum auch, aus gegebenen Objekten über Operationen wie Potenzmengenbildung, Ausschneidung von Teilmengen, Bildung von Faktormengen und so weiter neue konstruieren. Damit steht die interne Sprache der üblichen mathematischen Sprache in keiner Hinsicht nach – bis auf die Einschränkung auf konstruktive Logik.

Verständnis für konstruktive Logik

Wir haben gesehen, dass in der internen Welt des kleinen Zariski-Topos nur die Gesetze konstruktiver Logik gelten. Möchten wir in der internen Welt mathematisch argumentieren, haben wir also keine andere Wahl, als auf das klassische Prinzip des ausgeschlossenen Dritten und verwandte Prinzipien zu verzichten.

Es gibt eine Möglichkeit, diesen Verzicht auch ohne topostheoretischen Hintergrund anschaulich zu deuten: Dass eine Aussage konstruktiv gilt, kann man sich so vorstellen, dass man einen *expliziten Beleg* für die Gültigkeit der Aussage hat. Dann bedeutet eine zusammengesetzte Aussage wie $\phi \vee \psi$, dass man einen Beleg für ϕ oder einen Beleg für ψ hat – das ist schwächer als die klassische Interpretation derselben Aussage, nach der ϕ oder ψ lediglich wahr sind.

Die negierte Aussage

$$\neg\phi \quad \equiv \quad (\phi \Rightarrow \bot)$$

bedeutet, dass man aus einem Beleg von ϕ einen Beleg der falschen Aussage $\bot$ produzieren könnte. Da es einen solchen nicht gibt, bedeutet $\neg\phi$ also, dass es keinen Beleg für ϕ gibt. In diesem Bild besagt das Prinzip der Doppelnegationselimination,

$$\neg\neg\phi \Longrightarrow \phi,$$

dass man, wenn man weiß, dass es nicht sein kann, dass es keinen Beleg für ϕ gibt, sofort einen Beleg für ϕ produzieren kann. Das ist aber offensichtlich eine absurde Behauptung.

Die Aussage $\neg(\neg\phi \wedge \neg\psi)$ bedeutet konstruktiv, dass es keinen Beleg dafür gibt, dass sowohl ϕ als auch ψ falsch sind. Wenn man das weiß, kennt man aber noch lange nicht einen Beleg für ϕ oder einen Beleg für ψ. Das De-Morgansche Gesetz

$$\neg(\neg\phi \wedge \neg\psi) \quad \Longrightarrow \quad \phi \vee \psi$$

kann man also konstruktiv nicht rechtfertigen.

Beispiel 7.1. Wenn wir wissen, dass sich unser Haustürschlüssel irgendwo in der Wohnung befinden muss (da wir ihn letzte Nacht verwendet haben, um die Tür aufzusperren), wir ihn momentan aber nicht finden, so können wir konstruktiv nur folgende doppelt negierte Aussage vertreten:

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

Beispiel 7.2. 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 nicht strafrechtlich verfolgt.

Abschließend sei bemerkt, dass einige üble Gerüchte um konstruktive Logik im Umlauf sind, etwa, dass das Wort *Widerspruch* pauschal verboten sei und man daher nicht mal die Irrationalität von $\sqrt{2}$ zeigen könne. Das Pizzaseminarskript räumt mit diesen Gerüchten auf.

Eine besondere Klasse von Aussagen: geometrische Formeln

Aussagen der Form

$$\forall \cdots \forall .\ (\cdots) \Rightarrow (\cdots),$$

wobei in den eingeklammerten Teilaussagen die logischen Zeichen $\forall$ und $\Rightarrow$ nicht vorkommen dürfen, heißen *geometrische Formeln.* (Die Bezeichnung rührt von einem indirekten Zusammenhang mit der geometrischen Vorstellung von Ringen her.)

Das besondere an geometrischen Formeln ist, dass sie genau dann in der internen Welt des kleinen Zariski-Topos zu R gelten, wenn sie im gewöhnlichen Sinn bei jedem Halm von R gelten. Ein *Halm* von R ist dabei eine Lokalisierung der Form $R_\mathfrak{p} = (R \setminus \mathfrak{p})^{-1} R$ für ein beliebiges Primideal $\mathfrak{p} \subseteq R$.

Etwa ist die Bedingung, (in einem schwachen Sinn) ein Integritätsbereich zu sein,

$$\forall x, y.\ xy = 0 \Rightarrow (x = 0) \vee (y = 0),$$

eine geometrische Formel. Deswegen erfüllt der interne Ring $\mathcal{O}$ sie genau dann, wenn alle Halme $R_\mathfrak{p}$ sie erfüllen.

Kategorientheoretischer Hintergrund

Offiziell ist ein Topos eine Kategorie, die gewisse Eigenschaften mit der Kategorie der Mengen gemeinsam hat. Insbesondere ist die Kategorie der Mengen selbst ein Topos. Jeder Topos hat eine interne Sprache, wobei die Übersetzungsregeln eine leichte Verallgemeinerung der Regeln des kleinen Zariski-Topos darstellen. Die interne Sprache der Kategorie der Mengen fällt mit der gewöhnlichen mathematischen Sprache zusammen.

Zu einem topologischen Raum X gibt es die Kategorie der *Garben auf X*. Kategorien dieser Art bilden die Prototypbeispiele für interessante Topoi. Der kleine Zariski-Topos zu einem kommutativen Ring R ist auch von dieser Form: Er ist der Topos der Garben auf $\operatorname{Spec} R$, dem zu R assoziierten geometrischen Raum. Der interne Ring $\mathcal{O}$ entspricht dann der *Strukturgarbe*, auf einer Basis offener Mengen explizit gegeben durch

$$\Gamma(D(s), \mathcal{O}) = R[s^{-1}].$$

Die interne Sprache des Garbentopos zu einem topologischen (T_1-)Raum X ist genau dann klassisch, erfüllt also das Axiom vom ausgeschlossenen Dritten und das Axiom der Doppelnegationselimination, wenn X ein diskreter Raum ist. Das ist ein langweiliger Fall.

Der Topos der Garben über dem einpunktigen Raum ist äquivalent zur Kategorie der Mengen. Daher hört man manchmal das Motto *gewöhnliche Mathematik ist Mathematik über dem Punkt.*

Weitere alternative Mathematik-Universen

In diesen Notizen haben wir nur über den kleinen Zariski-Topos zu einem kommutativen Ring gesprochen. Es gibt aber noch viele weitere Topoi, die ebenfalls interessant sind:

- Vielleicht hat man einen bestimmen topologischen Raum X besonders gern und möchte daher, dass alles vom aktuellen Aufenthaltsort in dem Raum abhängt. 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 Objekte eine G-Wirkung tragen und dass alle Abbildungen G-äquivariant sind. Dann sollte man im *Topos der G-Mengen* arbeiten.
- Vielleicht interessiert man sich vor allem dafür, was Turingmaschinen berechnen können. Dann kann man im *effektiven Topos* arbeiten, der nur solche Abbildungen enthält, die durch Turingmaschinen algorithmisch gegeben werden können.
- Vielleicht möchte man mit Schemata über $\operatorname{Spec} R$ in einer einfachen Sprache arbeiten. Dann kann man den *großen Zariski-Topos zu R* verwenden.

Mithilfe von *geometrischen Morphismen* kann man auch zwischen verschiedenen Topoi wechseln. Dabei bleiben wahre geometrische Formeln unter Rückzug wahr.

Abstrakte Motivation für den kleinen Zariski-Topos

Sei R ein kommutativer Ring mit einer multiplikativ abgeschlossenen Teilmenge S. Dann kann man sich fragen, ob es einen Ring R' zusammen mit einem Ringhomomorphismus $R \to R'$, der die Elemente aus S auf Einheiten abbildet, gibt, sodass jeder Ringhomomorphismus $R \to T$ in einen weiteren Ring T, welcher die Elemente aus S auf invertierbare Elemente schickt, eindeutig über $R \to R'$ *faktorisiert*. Das bedeutet, dass in dieser Situation genau ein Ringhomomorphismus $R' \to T$ existieren soll, sodass das Diagramm

$$\begin{tikzcd} R \arrow[rr] \arrow[dr] & & T \\ & R' \arrow[ur, dashed] & \end{tikzcd}$$

kommutiert. Die Antwort auf diese Frage ist *ja*: Einen solchen speziellen Ring R' gibt es, nämlich $R' = S^{-1}R$.

Wenn man keine multiplikativ abgeschlossene Teilmenge besonders auszeichnen möchte, kann man sich analog auch folgende Frage stellen: Gibt es einen lokalen Ring R' zusammen mit einem Ringhomomorphismus $R \to R'$, sodass jeder Ringhomomorphismus $R \to T$ in einen *lokalen Ring T* eindeutig über $R \to R'$ faktorisiert?[1]

[1]Der Homomorphismus $R' \to T$ soll dabei ein *lokaler* Ringhomomorphismus sein, d. h. er soll Invertierbarkeit nicht nur bewahren, sondern auch reflektieren: Immer, wenn das Bild eines Elements aus R' in T invertierbar ist, soll schon das Element selbst in R' invertierbar sein.

Im wörtlichen Sinn lautet die Antwort auf diese Frage leider *nein*: Im gewöhnlichen mathematischen Universum gibt es keinen Ring R' mit dieser Eigenschaft.[2] Wenn man aber bereit ist, die Lösung dieses Optimierungsproblems auch in einem anderen Topos zu suchen, so fällt die Antwort wieder positiv aus: Der gesuchte Ring R' ist der interne Ring $\mathcal{O}$ des kleinen Zariski-Topos zu R.

Um das präzise zu formulieren, müssten wir erklären, was unter Ringhomomorphismen zwischen Ringen verschiedener Topoi zu verstehen ist.

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

Im Beweis von Satz 5.3 ist ein Verfahren versteckt, wie man aus jedem intern geführten Beweis einen Beweis der entsprechenden übersetzten Aussagen im gewöhnlichen Sinn gewinnen kann. Daher kann man mit der Topossprache sicherlich *nicht* Sätze beweisen, die man ohne sie nicht beweisen könnte.

Allerdings kann es sehr viel einfacher sein, in der internen Welt zu denken und zu arbeiten und erst am Ende die Übersetzung mit der Kripke–Joyal-Semantik durchzuführen. Etwa folgt aus der einfach zu beweisenden Aussage konstruktiver linearer Algebra

> *Jeder endlich erzeugte Vektorraum über einem Körper besitzt* nicht nicht *eine endliche Basis.*

durch Interpretation in einem geeigneten Topos sofort folgende offensichtlich komplizierte Aussage aus der algebraischen Geometrie:

> *Jede $\mathcal{O}_X$-Modulgarbe auf einem reduzierten Schema X, die von endlichem Typ ist, ist auf einer dichten offenen Teilmenge sogar lokal frei von endlichem Rang.*

Ähnliche Anwendungen gibt es auch in der Differentialgeometrie.

Auf den Geschmack gekommen?

Im Skript zum Pizzaseminar der Sommersemesterferien 2013 gibt es Hintergründe, Details und Literaturverweise. Ferner steht die Tür von Büro 2031/L1 für topostheoretische Diskussionen immer offen.

`http://pizzaseminar.speicherleck.de/`

[2] Etwas präziser: Es gibt einen solchen Ring genau dann, wenn R genau ein Primideal enthält. Übungsaufgabe!

A. Aufgaben

Aufgabe 1. *Nichttrivialität des internen Rings*

Sei R ein beliebiger kommutativer Ring. Zeige, dass $\mathcal{O}$ stets ein nichttrivialer Ring ist, zeige also:

$$R \models \neg(1 = 0).$$

Aufgabe 2. *Der kleine Zariski-Topos des Nullrings*

Zeige, dass im kleinen Zariski-Topos des Nullrings jede beliebige Aussage gilt. Zeige also, dass wenn R ein Ring mit $1 = 0 \in R$ und ϕ eine beliebige Aussage ist, $R \models \phi$ gilt.

Tipp: Man kann eine sehr einfache Zerlegung der Eins hinschreiben.

Aufgabe 3. *Der kleine Zariski-Topos eines Körpers*

Sei K ein Körper. Zeige, dass die interne Sprache des kleinen Zariski-Topos zu K mit der gewöhnlichen mathematischen Sprache zusammenfällt. Zeige also für beliebige Aussagen ϕ (wobei man auf der rechten Seite „K“ statt „$\mathcal{O}$“ lesen soll):

$$K \models \phi \quad \Longleftrightarrow \quad \phi.$$

Tipp: Induktion über den Aufbau von ϕ. Was ist an Zerlegungen der Eins von Körpern besonders?

Aufgabe 4. *Integritätsbereichseigenschaft des internen Rings*

Ein *Integritätsbereich* ist ein Ring, in dem, wann immer ein Produkt von Ringelementen Null ist, schon mindestens ein Faktor Null ist. (Das ist konstruktiv schwächer als zu verlangen, dass jedes Element entweder Null oder regulär ist.)

Sei R ein Integritätsbereich. Zeige, dass dann auch $\mathcal{O}$ ein Integritätsbereich ist.

Aufgabe 5. *Körpereigenschaften des internen Rings*

Ein Ring heißt genau dann *reduziert*, wenn, wann immer ein Element nilpotent ist, dieses schon gleich Null ist. Sei R ein beliebiger kommutativer Ring.

a) Zeige, dass der interne Ring $\mathcal{O}$ in folgendem Sinn beinahe ein Körper ist:

$$R \models \forall x\,{:}\,\mathcal{O}.\ \neg(\ulcorner x \text{ inv.}\urcorner) \Rightarrow \ulcorner x \text{ nilpotent}\urcorner.$$

b) Zeige, dass R genau dann reduziert ist, wenn $\mathcal{O}$ reduziert ist.

c) Sei R reduziert. Zeige, dass dann $\mathcal{O}$ ein Körper in folgendem Sinn ist:

$$R \models \forall x\,{:}\,\mathcal{O}.\ \neg(\ulcorner x \text{ inv.}\urcorner) \Rightarrow x = 0.$$

d) Zeige, dass die Umkehrung der Aussage in c) ebenfalls gilt.

Aufgabe 6. *Diskretheit des internen Rings*

Ein Ring heißt genau dann *diskret*, wenn jedes Element Null ist oder nicht Null ist. Natürlich ist jeder Ring der gewöhnlichen mathematischen Welt diskret.

Ein Ringelement f heißt genau dann *pseudoregulär*, wenn, wann immer ein Produkt von f mit einem weiteren Ringelement g Null ist, g nilpotent ist.

a) Sei f ein Element eines kommutativen Rings R. Zeige, dass f genau dann in der internen Welt nicht Null ist (also $R \models \neg(f = 0)$ gilt), wenn f im gewöhnlichen Sinn pseudoregulär ist.

b) Zeige, dass der interne Ring $\mathcal{O}$ im Allgemeinen nicht diskret ist.

Aufgabe 7. *Eine geometrische Körperbedingung*

Ein *diskreter Körper* ist ein kommutativer Ring, sodass jedes Element entweder Null oder invertierbar ist. Das besondere an dieser Körperbedingung ist, dass sie eine geometrische Formel ist.

a) Rechtfertige die Namensgebung, indem du zeigst, dass diskrete Körper stets diskret im Sinn der vorherigen Aufgabe sind.

b) Zeige, dass der interne Ring $\mathcal{O}$ des kleinen Zariski-Topos zu einem beliebigen Ring im Allgemeinen *kein* diskreter Körper ist.

Aufgabe 8. *Vorwissen zu Bewertungsbereichen*

Sei R ein *Bewertungsbereich*, also ein Integritätsbereich im Sinn von Aufgabe 4, sodass von je zwei Elementen stets eines das andere teilt.

a) Zeige, dass von je endlich vielen Elementen von R stets eines ein Teiler aller anderen ist.

b) Zeige, dass jede Matrix über R äquivalent zu einer (rechteckigen) Diagonalmatrix ist.

Aufgabe 9. *Prüfersche Bereiche aus interner Sicht*

In dieser Aufgabe wollen die Behauptung über die interne Welt in Beispiel 5.2 verstehen. Sei R ein kommutativer Ring, in dem jedes endlich erzeugte Ideal lokal ein Hauptideal ist.

a) Zeige, dass jedes endlich erzeugte Ideal von $\mathcal{O}$ selbst schon ein Hauptideal ist, zeige also:

$$R \models \forall x_1, \ldots, x_n : \mathcal{O}.\ \exists d : \mathcal{O}.\ (x_1, \ldots, x_n) = (d).$$

Da wir nicht diskutiert haben, wie man in der internen Sprache über Teilmengen sprechen kann, muss die Idealgleichheitsbedingung als Kurzschreibweise für folgende Bedingung gelesen werden:

$$\big(\exists u_1 : \mathcal{O}.\ x_1 = u_1 d\big) \wedge \cdots \wedge \big(\exists u_n : \mathcal{O}.\ x_n = u_n d\big) \wedge \big(\exists a_1, \ldots, a_n : \mathcal{O}.\ a_1 x_1 + \cdots + a_n x_n = d\big)$$

b) Sei R ferner ein Integritätsbereich im Sinn von Aufgabe 4. Zeige, dass $\mathcal{O}$ ein Bewertungsbereich ist.

c) Was kann man in diesem Fall über Matrizen über R folgern?

Aufgabe 10. *Aussagen über Kerne von Matrizen*

a) Sei $M \in R^{n\times m}$ eine Matrix über einem lokalen Ring R, die als lineare Abbildung $R^m \to R^n$ surjektiv ist, sodass es also zu jedem $y \in R^n$ ein $x \in R^m$ mit $Mx = y$ gibt.

Zeige, dass M äquivalent zu einer (rechteckigen) Diagonalmatrix mit genau n Einsern auf der Hauptdiagonale ist. Folgere, dass der Kern von M eine Basis aus $(m-n)$ Vektoren besitzt. (Man sagt auch: Der Kern von M ist *frei vom Rang* $(m-n)$.)

b) Überlege, wie folgende Aussage sinnvoll zu interpretieren ist, und erkläre, wieso aus einer konstruktiven Behandlung von Teilaufgabe a) sofort ihre Gültigkeit folgt: Der Kern einer $(n \times m)$-Matrix über einem beliebigen kommutativen Ring, die als lineare Abbildung surjektiv ist, ist *lokal frei* vom Rang $(m-n)$.

Aufgabe 11. *Idempotente Matrizen*

a) Sei $P \in R^{n\times n}$ eine idempotente Matrix über einem lokalen Ring R, gelte also $P^2 = P$. Zeige, dass P äquivalent zu einer Diagonalmatrix mit Einträgen 1 und 0 ist.

Tipp: Betrachte die Ideale der i-Minoren von P. Diese sind idempotent und (zum Beispiel nach dem Lemma von Nakayama) daher jeweils das Null- oder Einsideal.

b) Sei $P \in R^{n\times n}$ eine idempotente Matrix über einem beliebigen kommutativen Ring R. Zeige, dass der Kokern von P lokal frei ist.