

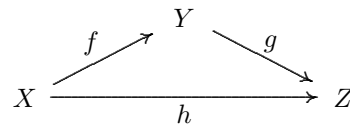
Was sind und was sollen Kategorien ?

Eva Richter

13.04.2004

1 Einführung

Die Theorie der Kategorien beginnt mit der Beobachtung, daß sich durch die Darstellung mittels Diagrammen von Pfeilen viele Eigenschaften mathematischer Systeme einheitlich erfassen und vereinfachen lassen. Betrachten wir zwei Mengen X und Y , so stellt ein Pfeil $f : X \rightarrow Y$ eine Abbildung dar, d.h. es gibt eine Vorschrift $x \mapsto f(x)$, die jedem Element $x \in X$ ein Element $y = f(x) \in Y$ zuordnet. Ein typisches Diagramm von Mengen und Abbildungen ist:

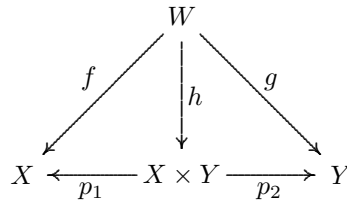


Ein solches Diagramm ist kommutativ, wenn h von der Form $h = g \circ f$ ist, wobei $g \circ f$ die übliche zusammengesetzte Abbildung $g \circ f : X \rightarrow Z$ ist, die vermöge $x \mapsto g(fx)$ definiert wird.

Die gleichen Diagramme treten auch in anderen Zusammenhängen auf. So stellen in der "Kategorie" der geordneten Verbände X, Y und Z Verbände dar, während f, g, h monotone Abbildungen sind. Wir werden auch Kategorien kennenlernen, in der die Pfeile dem Abbildungs- oder Funktionsbegriff nur sehr wenig ähneln. Beispielsweise kann man eine Gruppe als Kategorie auffassen, indem man die Gruppenelemente als Pfeile in einem einzigen Objekt betrachtet. Die Komposition $\circ$ wird dann zur Gruppenoperation.

Was die Kategorientheorie so universell einsetzbar macht, ist ihre Methode, mathematische Konstruktionen als universelle Eigenschaften von Diagrammen darzustellen. Man betrachte das kartesische Produkt $X \times Y$ zweier Mengen X und Y . Es besteht wie üblich aus der Menge der geordneten Paare $\langle x, y \rangle$ von Elementen $x \in X$ und $y \in Y$. Die Projektionen der Produktmenge auf ihre "Koordinatenachsen" X und Y sind Abbildungen $p_1 : X \times Y \rightarrow X$ und $p_2 : X \times Y \rightarrow Y$. Eine beliebige auf einer dritten Menge W definierte Abbildung $h : W \rightarrow X \times Y$ wird eindeutig bestimmt durch ihre Komposita $p_1 \circ h$ und $p_2 \circ h$.

Sind umgekehrt die Menge W und zwei Abbildungen f, g gegeben, so existiert eine eindeutig bestimmte Abbildung h , die das besagte Diagramm kommutativ macht, nämlich $hw = \langle fw, gw \rangle$:



Sind also X und Y gegeben, so ist $\langle p_1, p_2 \rangle$ "universell" unter den Paaren von Abbildungen einer beliebigen Menge in X bzw. Y , da jedes solche Paar $\langle f, g \rangle$ eindeutig über das Paar $\langle p_1, p_2 \rangle$ (durch h) faktorisiert. Durch diese Eigenschaft ist das Produkt $X \times Y$ eindeutig (bis auf Bijektion) bestimmt.

Wird das gleiche Diagramm als Diagramm von Elementen eines geordneten Verbandes $(L, \leq_L)$ gelesen, stellt das Produkt gerade das Infimum der beiden Elemente bzgl. der Ordnung $\leq_L$ dar, d.h. $X \times Y = X \wedge_L Y$. Für zwei Verbandselemente W, Y steht ein Pfeil $f : W \rightarrow Y$ für die Beziehung $W \leq_L Y$. Haben wir also ein Verbandselement W und zwei Pfeile f, g mit $f : W \rightarrow X$ und $g : W \rightarrow Y$ so bedeutet dies, daß $W \leq_L X$ und $W \leq_L Y$ dann gilt aber auch, daß $W \leq_L X \wedge Y$. Das wiederum bedeutet, es existiert ein Pfeil $h : W \rightarrow X \wedge Y$.

Es ist die universelle Eigenschaft des "Produktes", die höchst effektiv seinen Verwendungszweck und seine Funktion im Verhältnis zu den beiden Objekten aus denen es gebildet wird bestimmt. Wenn diese "operationale" Beschreibung bekannt ist, ist seine interne Struktur - der Weg, auf dem es konstruiert wurde - weniger wichtig.

Kategorientheorie wurde ursprünglich als Sprache zur Beschreibung von mathematischen Strukturen entwickelt. Eingeführt wurde sie in den 40-er Jahren des 20. Jahrhunderts von Samuel Eilenberg und Saunders MacLane. Ihre Wurzeln liegen in der algebraischen Topologie, wo Konstruktionen entwickelt wurden, die das Gebiet der Topologie mit dem der Algebra, insbesondere der Gruppentheorie verbinden. Sie wurde jedoch bald auch für andere Bereiche der Mathematik benutzt und ist inzwischen ein eigener wesentlicher Zweig der reinen Mathematik.

Was für uns noch viel wichtiger ist, ist daß sie einen bemerkenswerten Einfluß auf die konzeptionellen Grundlagen der Mathematik und die Sprache der mathematischen Praxis hatte.

Während die Welt der Mathematik die Kategorie der Mengen ist, d.h. die Mengenlehre als Grundlage der Mathematik betrachtet werden kann, ist sie für die Informatik nicht unbedingt der geeignetste Ausgangspunkt. Der Gegenstand der theoretischen Informatik sind Algorithmen und Funktionen, und es ist wichtig zu unterscheiden zwischen solchen Funktionen, die berechenbar sind und solchen, die es nicht sind. Eng damit verknüpft ist die Frage nach rekursiven Mengen, also Mengen, für die es eine berechenbare Funktion bzw. einen Algorithmus gibt, die ihre Elemente konstruiert.

Eine wichtige Frage ist es also, eine Welt mit konstruierbaren Mengen zu beschreiben. Kategorientheoretische Versuche, die Grundlagen der Mengenlehre zu axiomatisieren haben zu einer Verallgemeinerung des Mengenbegriffs geführt.

Betrachtet wurden dazu Kategorien die sich "mengenähnlich" verhalten, wobei zunächst genauer geklärt werden mußte was mit "ähnlich" gemeint sein soll.

Erste Antworten auf diese Frage hat F. William Lawvere 1964 gegeben. Sein ursprüngliches Ziel war, Mengentheorie kategorial zu axiomatisieren, d.h. Begriffe wie Elementbeziehung, leere Menge, Teilmenge und Potenzmenge mit Hilfe von Universalitätseigenschaften zu beschreiben. Das Ergebnis war jedoch nicht befriedigend, da er als Grundlage seiner Betrachtungen selbst Mengentheorie benutzen mußte.

1969 begann Lawvere zusammen mit Myles Tierney, Kategorien zu studieren, die über eine bestimmte Art von Pfeilen verfügten, die sie "Subobject Classifier" nannten. Wie sich später herausstellte, war dieser Begriff gerade der Schlüssel zu seinem früheren Problem. Das Ergebnis ihrer Untersuchungen war das abstrakte axiomatische Konzept eines elementaren Topos. Das Wort stammt aus dem Griechischen und heißt soviel wie "Platz" oder "Ort". Es wurde schon von Grothendieck für bestimmte algebraische Konstruktionen verwendet, und von Lawvere und Tierney übernommen, nachdem sich herausstellte, daß Grothendiecks Topoi alle einen solchen Subobject Classifier besaßen.

1.1 Warum sollte sich ein Informatiker für Topostheorie interessieren?

Wie wir schon früher bemerkt haben, liefert die Mengentheorie ein grundlegendes Begriffsgebäude für die Mathematik. Mit dem Begriff des Topos haben wir eine verallgemeinerte Mengenlehre. Das ergibt eine vollkommen neue kategorielle Grundlage der Mathematik.

Der kategorientheoretische Standpunkt, eher Funktionen und Relationen als Mengenzugehörigkeit in den Mittelpunkt der Aufmerksamkeit zu stellen, ist auch für die Informatik vielversprechend.

Ein weiterer (für den Informatiker) bedeutender Bereich, der sich mit dem Begriff des Topos neu erschließt, ist der Bereich der Logik, also das Studium des deduktiven Schließens. Die Prinzipien der klassischen Logik werden als Operationen auf einer bestimmten Menge, nämlich der Booleschen Algebra dargestellt. Jeder Topos hat ein Analogon zu dieser Algebra und somit kann man sagen, daß jeder Topos seine eigene Logik trägt. Eine solche Topos-Logik kann von der klassischen Logik ziemlich stark abweichen. Im (allgemeinen) Topos sind die logischen Prinzipien die der intuitionistischen Logik.

Intuitionismus ist eine konstruktivistische Philosophie, die sich mit der Natur der mathematischen Objekte, ihrer Bedeutung, sowie der Gültigkeit mathematischer Aussagen beschäftigt. Ihr wichtigstes Paradigma ist die Forderung, daß jede Existenzaussage durch eine direkte Konstruktion bewiesen werden soll, d.h. man kann von einem Objekt nur dann behaupten, daß es existiert, wenn man eine Konstruktion dafür angeben kann.

In der klassischen Mathematik wird ein Existenzbeweis jedoch oft als indirekter Beweis geführt, indem man zeigt, daß die Annahme der Nichtexistenz zu einem Widerspruch führt. Vom konstruktivistischen Ansatz her ist ein solcher Beweis nicht zulässig. Das klassische Axiom $\alpha \vee \neg \alpha$ bedeutet dort-da Wahrheit

als Konstruierbarkeit interpretiert wird-daß entweder α oder $\neg\alpha$ konstruiert werden kann. Wenn wir nun für α eine unentschiedene Frage einsetzen, z.B. $\mathcal{P} = \mathcal{NP}$, dann ist $\alpha \vee \neg\alpha$ zum gegenwärtigen Zeitpunkt weder wahr noch falsch. Der indirekte Beweis wird klassisch als die Tautologie $\neg\neg\alpha \Rightarrow \alpha$ dargestellt. Um zu zeigen daß α gilt, zeigt man, daß es nicht sein kann daß $\neg\alpha$ wahr ist, d.h. man zeigt $\neg\neg\alpha$ ist wahr und schließt dann α ist wahr. Vom intuitionistischen Standpunkt her bedeutet die Wahrheit der Aussage $\alpha \Rightarrow \beta$ anzunehmen, "Ich habe eine Konstruktion entwickelt, mit deren Hilfe ich aus einer Konstruktionsmethode für α eine Konstruktionsmethode für β herleiten kann. Zeigt man dann, daß es widersprüchlich ist, daß ein bestimmtes Ding nicht existiert ($\neg\neg\alpha$), so ist das nicht dasselbe, wie α zu konstruieren. D.h. $\neg\neg\alpha \Rightarrow \alpha$ ist keine Tautologie im intuitionistischen Sinne.

Der Zusammenhang zwischen Topos-Theorie und intuitionistischer Logik war zunächst ziemlich überraschend, da auf den ersten Blick nicht zu erkennen war, was die eher philosophischen Betrachtungen die zur intuitionistischen Logik geführt hatten, mit den kategorialen Untersuchungen der Mengentheorie, die in Begriff des elementaren Topos mündeten, zu tun hatte.

Dieser Zusammenhang zwischen intuitionistischer (nämlich Topos-) Logik und Kategorientheorie wird besonders als theoretischer Hintergrund für den Programmiersprachenentwurf benutzt. So gibt es Ansätze zur Beschreibung von Semantiken von funktionalen Programmiersprachen, die kategoriale Methoden benutzen. kategorientheorie stellt eine formale Sprache zur Verfügung, die bestens geeignet ist, abstrakte Eigenschaften von Strukturen auszudrücken.

1.2 Inhalt des Seminars

- Einführung in die Kategorientheorie als Beschreibungssprache und Abstraktionsmethode,
- Verallgemeinerte Mengenlehre und Begriff des elementaren Topos,
- Klassische Logik versus Toposlogik,
- Arithmetik: Natürliche-Zahl-Objekt und primitive Rekursion

2 Erste Definitionen und Beispiele

Zunächst wollen wir definieren, was wir unter einer Kategorie verstehen wollen:

Definition 1 *Eine Kategorie $\mathcal{C}$ ist eine Kollektion von Objekten $\text{Obj}(\mathcal{C})$, (bezeichnet mit $A, B, \dots$) und eine Kollektion von Morphismen (oder Pfeilen) $\text{Mor}(\mathcal{C})$ (bezeichnet mit $f, g, h \dots$).*

Es gibt zwei Operationen dom und cod , die jedem Pfeil f zwei Objekte-seine Quelle $\text{dom}(f)$ und sein Ziel $\text{cod}(f)$ -zuordnen.

Eine Operation id ordnet jedem Objekt A aus $\mathcal{C}$ einen Pfeil id_A zu sd. $\text{dom}(\text{id}_A) = \text{cod}(\text{id}_A) = A$.

Es gibt eine Kompositionsoperation $\circ$, die jedem Paar f, g von Pfeilen mit $\text{dom}(g) = \text{cod}(f)$ einen Morphismus $h = g \circ f$ zuordnet sd. $\text{dom}(h) = \text{dom}(f)$ und $\text{cod}(h) = \text{cod}(g)$. Identität und Komposition müssen folgenden Bedingungen genügen:

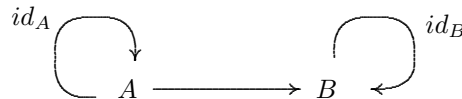
(Identität): für jedes Paar von (zusammensetzbaren) Pfeilen f, g mit $\text{cod}(f) = B = \text{dom}(g)$ gilt $g \circ \text{id}_B = g$, $\text{id}_B \circ \text{cod}(g)$,

(Assoziativgesetz): $(h \circ g) \circ f = h \circ (g \circ f)$ für Pfeile f, g, h mit $\text{cod}(f) = \text{dom}(g)$ und $\text{cod}(g) = \text{dom}(h)$.

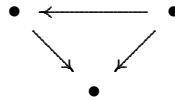
Wir schreiben $f : A \rightarrow B$ um einen Morphismus mit Quelle A und Ziel B zu bezeichnen.

2.1 1, 2 und 3

Die Kategorie 1 hat ein Objekt, sein einziger Morphismus ist der identische Pfeil auf diesem Objekt. Die Kategorie 2 hat zwei Objekte und drei Pfeile, dargestellt durch:



Die Kategorie 3 besteht aus drei Objekten und sechs Pfeilen, wobei die drei nicht identischen Pfeile im Dreieck angeordnet sein sollen. Es gibt nur einen möglichen Weg, die Komposita zu definieren.



2.2 Partiiell geordnete Mengen

Das besondere an den obigen Beispielen war, daß es nur eine Art gibt, die Komposition zu definieren. Das liegt daran, daß es zwischen je zwei Objekten p und q höchstens einen Pfeil $p \rightarrow q$ gibt. Eine Kategorie mit dieser Eigenschaft heißt Präordnung. Sei P eine Menge von Objekten einer Präordnungskategorie. Man definiert eine Relation $R \subseteq P \times P$ durch $\langle p, q \rangle \in R$ falls es einen Pfeil $p \rightarrow q$ in der Präordnungskategorie gibt. Diese Relation ist reflexiv (da zu jedem Objekt ein Identitäts-Pfeil existiert) und transitiv (wegen der Assoziativität der Komposition). Eine assoziative und transitive binäre Relation heißt *Präordnung*.

Eine Präordnung heißt partielle Ordnung, wenn sie außerdem noch antisymmetrisch ist, d.h. aus pRq und qRp folgt, daß $p = q$.

Die Menge $\{0\}$ wird zur partiell geordneten Menge mit der Relation R , wenn wir $0R0$ setzen. Die entsprechende Kategorie ist 1.

Die Kategorie 2 entspricht einer partiellen Ordnung auf der Menge $\{0, 1\}$, mit der üblichen Ordnung $\leq$.

Die Kategorie 3 entspricht einer partiellen Ordnung auf der Menge $\{0, 1, 2\}$

Das läßt sich fortsetzen mit jeder natürlichen Zahl. Genausogut kann man die unendliche Menge $\omega = \{0, 1, 2, 3, \dots\}$ aller natürlicher Zahlen mit der üblichen Ordnung $\leq$ betrachten, gegeben durch das folgende Diagramm:

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \dots$$

Hierbei wurden Identitätspfeile und Kompositionen weggelassen.

Ein einfaches Beispiel für eine Präordnung, die keine partielle Ordnung ist, wird definiert durch das Diagramm:

$$P \begin{array}{c} \xleftarrow{\quad} \\ \xrightarrow{\quad} \end{array} Q$$

Es gibt je einen Pfeil $P \rightarrow Q$ und $Q \rightarrow P$, aber es gilt $P \neq Q$.

2.3 SET

Die Objekte dieser Kategorie sind Mengen, Morphismen der Kategorie sind Funktionen.

Zu beachten ist hierbei, daß Kategorientheorie Funktionen anders auffaßt als Mengenlehre, nämlich hat jeder Pfeil f in der Kategorie der Mengen SET eine eindeutig zugeordnete Quelle und Ziel. Betrachte man beispielsweise die Menge $\mathbb{Q}$ der rationalen Zahlen und $\mathbb{R}$ der reellen Zahlen. In einem mathematischen Text gibt es eine wohldefinierte Funktion auf $\mathbb{Q}$ die jeder rationalen Zahl x ihr Quadrat x^2 zuordnet. In der Kategorientheorie ist eine Funktion, d.h. ein Pfeil in SET nicht vollständig definiert, ohne daß ihr Ziel spezifiziert ist. Es gibt also zwei verschieden Pfeile $-^2 : \mathbb{Q} \rightarrow \mathbb{Q}$ und $-^2 : \mathbb{Q} \rightarrow \mathbb{R}$ und viele andere, die alle x sein Quadrat zuordnen, aber jedesmal in einer anderen Kodomäne.

2.4 Data

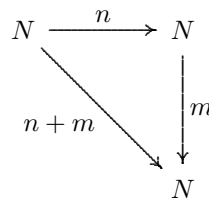
Die Objekte dieser Kategorie sind Datentypen einer gegebenen Programmiersprache, die Morphismen sind berechenbare Funktionen zwischen ihnen. Wir schreiben $f : A \rightarrow B$ um zu sagen, daß f eine berechenbare Funktion von A nach B ist, d.h. irgendein Programm unserer Sprache akzeptiert eine Eingabe vom Typ A und liefert für jedes $x : A$ einen Wert $f(x) : B$. Für jeden Datentyp ist die Identität id_A berechenbar. Komposition ist die Anwendung von g auf die Ergebnisse von f . natürlich kann ein Programm verschiedene Eingaben haben. Das kann mit Hilfe eines Instruments modelliert werden, das in den meisten Programmiersprachen existiert.: Records. Für jedes Paar von Datentypen A und B nehmen wir an, es gäbe einen Datentypen $A \times B$, von dem wir uns vorstellen, daß ein Wert von diesem Typ ein Paar $\langle x, y \rangle$ ist mit $x : A$ und $y : B$. Haben wir dann ein Programm, daß einen Wert vom Typ A und einen Wert vom Typ B als Eingabe nimmt und einen Wert vom Typ C zurückgibt, dann kann das auch betrachtet werden, als würde es einen Wert vom Typ $A \times B$ nehmen und kann so dargestellt werden als Pfeil $A \times B \rightarrow C$. Weder wir noch der Benutzer der Sprache fragen dabei danach, wie die Daten abgespeichert werden. Was uns interessiert ist, daß wir die Werte in jedem Feld des Records

wiedererlangen können. Dazu brauchen wir Funktionen: $p_1 : A \times B \rightarrow A$ und $p_B : A \times B \rightarrow B$. Wenn wir außerdem einen Typ T und eine je berechenbare Funktionen $g : T \rightarrow A$ und $h : T \rightarrow B$ haben, dann muß eine berechenbare Funktion $f : T \rightarrow A \times B$ existieren, nämlich $f(t) = \langle g(t), h(t) \rangle$ für jedes $t : T$.

Die Kategorie Data unterstützt das strenge Typisieren, auch wenn nicht jede Programmiersprache das auch vollständig benutzt. So behandeln viele Sprachen die $x+y$ Funktion als eine einzige Funktion, wohingegen man in Data unterscheiden kann zwischen $+: \mathbb{I} \times \mathbb{I} \rightarrow \mathbb{I}$ $+: \mathbb{I} \times \mathbb{R} \rightarrow \mathbb{I}$ $+: \mathbb{R} \times \mathbb{I} \rightarrow \mathbb{R}$ $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$

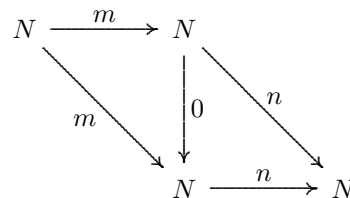
2.5 Die Kategorie N

Diese Kategorie hat nur ein Objekt N aber eine unendliche Anzahl von Pfeilen. Die Pfeile sind nach Definition die natürlichen Zahlen. Jeder Pfeil hat dieselbe Quelle und dasselbe Ziel, nämlich N , daher sind alle Pfeile kompositionierbar. Die Definition ist $n \circ m = n + m$, d.h. das Diagramm



kommutiert per definitionem. Die Assoziativgesetze der Komposition sind erfüllt, da die Addition assoziativ ist.

Der Identitätspfeil auf dem Objekt N ist definiert als die Zahl 0. Das Diagramm



kommutiert wegen $0 + m = m$ und $n + 0 = n$.

2.6 Grp

Die Kategorie N aus dem vorherigen Beispiel ist eine Kategorie, da die Struktur $(N, +, 0)$ ein Beispiel für das abstrakte algebraische Konzept eines Monoids ist.

Definition 2 Ein Monoid ist ein Tripel $\mathbf{M} = (M, *, e)$ wobei

1. M eine Menge ist,
2. $*$ eine binärer Operation auf M , d.h. eine Funktion von $M \times M$ nach M ist, die jedem Paar $(x, y) \in M \times M$ ein Element $x * y \in M$ zuordnet. Diese operation ist assoziativ, d.h. $x * (y * z) = (x * y) * z$ für alle $x, y, z \in M$.

3. *e ist ein Element aus M , das sich neutral bzgl der Operation $*$ verhält, d.h $x * e = e * x = x$ für alle $x \in M$.*

Jedes Monoid erzeugt eine Kategorie, mit genau einem Objekt. Als Objekt nehmen wir die Grundmenge M und als Menge der Pfeile $M \rightarrow M$ betrachten wir die Elemente von M . Wir setzen $e = 1_M$. Die Komposition zweier Pfeile $x, y \in M$ ist gegeben durch $x \circ y = x * y$.

Umgekehrt, falls $\mathcal{C}$ eine Kategorie mit nur einem Objekt a ist, M die Menge der Pfeile von $\mathcal{C}$ ist, dann ist $(M, \circ, id_a)$ ein Monoid. Alle Pfeile haben dieselbe Quelle und Ziel, damit sind alle Paare zusammensetzbar. Wegen Assoziativität und Identitätsgesetzen für Kategorien, gelten die entsprechenden Gesetze für die Monidoperationen.