Making Proof

Das Problem ist uralt, um genau zu sein, in Bayreuth ist es in diesem Jahr 20 Jahre alt: Übungen in Mathematik. Die Rechnungen sind meist kein Problem, jedoch Beweise zu führen ist schon schwieriger - wenn man sie nicht gerade abschreibt; aber wozu studiert man Mathematik, wenn man sich ums Beweisen drücken will? Hier fangen die Unsicherheiten an. Einmal ist die Aussage anschaulich völlig klar, aber wie beweist man sie? Ein anderes Mal ist die Beweisidee völlig klar, aber wie schreibt man sie am besten hin? Und wie kommt man eigentlich auf solche Sätze? Welche Sätze sind in einer Theorie die wichtigen? Fragen über Fragen, deren Antworten höchstens am Rande irgendeiner Vorlesung einmal anklingen. Eigentlich aber sind sie die Quintessenz eines Studiums der Mathematik. Deshalb: **Making Proof** .

Es gibt aber noch viel pragmatischere Gründe, dieses Heft zu lesen. Oftmals müssen die Korrektoren an den mißglückten Formulierungen und an fehlender innerer Logik in Lösungsversuchen von Übungsaufgaben verzweifeln - ich weiß das selbst aus eigener Erfahrung. Beweisen ist aber das täglich Brot des Mathematikers, und wenn man es richtig anstellt - mir gelingt das oft genug auch nicht - kann dieses Brot das reinste Feinschmeckermenu werden. Dafür gibt es einige Kniffs, Tricks und Tips, die ich hier vorstellen möchte.

Außerdem macht es einfach Spaß, nach getaner Arbeit einmal über seine Arbeit - die Mathematik - nachzudenken. Dabei sieht man dann doch (manchmal nicht ganz so ernst gemeinte) Gesetzmäßigkeiten.

Also: es führt kein Weg mehr an **Making Proof** vorbei.

Viel Spaß beim Lesen wünscht Euch

Marco

Inhaltsverzeichnis

1 Psychologie des Beweises **3**
- 1.1 Sinn und Bedeutung . . . 3
- 1.2 Axiom und Definition . . . 4
- 1.3 Die Logische Elementarform . . . 5
- 1.4 Zeit in der Logik . . . 6
- 1.5 Ausdruckshierarchien . . . 8
  - 1.5.1 Lemmata (Hilfssätze) . . . 8
  - 1.5.2 Korollare . . . 8
  - 1.5.3 Folgerungen . . . 8
  - 1.5.4 Bemerkungen . . . 8
  - 1.5.5 Beispiele . . . 9
- 1.6 Logische Kausalität . . . 9
- 1.7 Erlaubte Symbole . . . 9
- 1.8 Mathematische Diplomatie . . . 11

2 Häufige Satzstrukturen **12**
- 2.1 Äquivalenztabellen . . . 12
- 2.2 Existenzsätze . . . 13
- 2.3 Eindeutigkeitssätze . . . 14
- 2.4 Universelle Eigenschaft . . . 15
- 2.5 Klassifikationen . . . 16

3 Häufige Beweisstrukturen **17**
- 3.1 Abbildungen . . . 17
- 3.2 Induktion . . . 18
- 3.3 Widerspruch . . . 20
- 3.4 Konstruktion . . . 22
- 3.5 ε und Diagonalfolge . . . 22
- 3.6 Idee . . . 23

Kapitel 1

Psychologie des Beweises

How to make others believe to know something

Das erste, worüber wir uns klar werden sollten, ist, was eigentlich ein Beweis ist. Dazu müssen wir wissen, was wir eigentlich beweisen wollen. Das ist immer ein Satz, z.B. *„Das Wetter ist schön“*, *„Die Wiese ist grün“*, *„Der Professor ist blau“* etc. Dies sind aber (offensichtlich) keine Sätze der Mathematik - auch, wenn im letzten Satz ein Mathe-Prof gemeint ist. *„x ist genau dann Primzahl und gerade, wenn x=2 ist“* ist sicherlich ein mathematischer Satz. Aber woran erkennen wir den Unterschied zwischen einem Satz und einem mathematischen Satz? Man könnte meinen, nur in mathematischen Sätzen kämen Variablen vor. Dann ist aber zu fragen, was eine Variable ist und warum dann zum Beispiel *„x redet schon wieder schlecht über y“* kein mathematischer Satz ist. Aus der analytischen Philosophie kommt eine Idee, der wir uns bedienen können, um die mathematischen Sätze (und damit die Mathematik) zu definieren.

1.1 Sinn und Bedeutung

What's mathematics?

Die Bedeutung eines Satzes faßt man wohl am besten als die Bedingungen seiner Wahrheit auf. *„Die Wiese ist grün“* ist genau dann wahr, wenn die (eindeutig bezeichnete) Wiese den Farbeindruck grün bei den Beobachtern hervorruft. Das ist hier nicht ganz unproblematisch, man müßte noch viel weiter in die Bedeutung von Farbwörtern einsteigen, um die Wahrheitsbedingungen wirklich exakt formulieren zu können, aber darum geht es uns hier nicht. Wir brauchen den Bedeutungsbegriff ja nur für die Mathematik. Betrachten wir zwei Mengen von Sätzen: A und B. Wir sagen nun, A bedeutet mehr als B, wenn die Wahrheit der Sätze in B logisch aus der Wahrheit der Sätze von A folgt. Wir sagen in diesem Fall auch, daß B weniger als A bedeutet. Erfahrungsgemäß bedeutet zum Beispiel *„x ist betrunken“* mehr als *„x lallt“*. Denn x könnte ja auch einen Sprachfehler haben, der ihn lallen lässt. Wir haben hier allerdings vorausgesetzt, daß jeder Betrunkene lallt. Und daß x Primzahl ungleich 2 ist, bedeutet mehr als daß x ungerade ist. Größere Bedeutung heißt also, daß der Satz unter weniger Bedingungen wahr ist, daß sein Gelten also ungewöhnlicher ist.

Der Sinn eines Satzes ist die Art und Weise, wie seine Bedeutung gegeben ist. Zum Beispiel haben im $\mathbb{R}^2$ die Sätze *„A und B sind parallele Geraden“* und *„A und B sind Geraden, die sich nicht schneiden“* dieselbe Bedeutung, aber verschiedene Sinne. Die Bedeutung ist dieselbe, weil man aus den Wahrheitsbedingungen der Sätze genau die gleichen Geradenpaare, die sie erfüllen, bekommt. Der Sinn ist verschieden, weil man für den ersten Satz den Begriff der Richtung kennen muß und den des Schnittpunktes nicht, für den zweiten Satz es sich aber gerade umgekehrt verhält. Natürlich kann man argumentieren, daß der Begriff des Schnittpunktes den Begriff der Richtung/des Winkels zwischen zwei Geraden impliziert und „dieselbe Richtung“ auch nur den Begriff der relativen Richtung zwischen zwei Geraden benötigt. Aber die Einführung des Sinnes ist auch nicht logisch motiviert, sondern psychologisch. Es geht beim Sinn nicht um logische Unterschiede - denn die beiden Sätze sind ja logisch äquivalent - sondern um den Standpunkt. Wenn man von Richtungen redet, redet man eben nicht von Schnittpunkten. Zudem ist es ja so, daß beide Konzepte in höheren Dimensionen auseinanderfallen. Hinter den exakten, logischen Definitionen stehen also auch in der

Mathematik Konzepte, die eher psychologisch zusammenhängen. Dieser Unterschied im Sinn läßt sich nicht wegdiskutieren, denn er ist die Grundlage der Mathematik, wie wir gleich sehen werden.

Wir sagen, ein Satz ist a priori wahr oder eine Tautologie, wenn er unter allen Bedingungen wahr ist. Nun können wir sagen, was Mathematik ist, nämlich die Menge aller Tautologien. Wenn Sätze A und B dieselbe Bedeutung haben, so ist $A \Longleftrightarrow B$ eine Tautologie, also ein Satz der Mathematik. Und tatsächlich müßte uns diese Struktur vertraut vorkommen. Die Bedeutung der Mathematik läßt sich also nach unserer Definition in $x = x$ zusammenfassen. Die Mathematik ist eine einzige Proposition. Was aber leistet die Mathematik noch, wenn $x = x$ ihre einzige Aussage ist? Wie ich oben schon erwähnte, liegt die Grundlage der Mathematik im Sinn. Denn die Leistung von $A \Longleftrightarrow B$ liegt ja darin, daß zwischen den verschiedenen Sinnen vermittelt wird. Die Mathematik sagt eben, daß die Konzeption der Schnittpunkte zu den gleichen Ergebnissen führt wie die der Richtungen. Das ist ja logisch, wird man jetzt sagen. Und genau deswegen liegt der Grund für die Bedeutung der Mathematik in unserer Gesellschaft allein in der Psyche des Menschen. Kraß gesagt: Wäre das Hirn des Menschen nicht so begrenzt, gäbe es keine Mathematik. Nur weil es möglich ist, daß wir uns verschiedene Sinne einer Bedeutung einbilden können - die ja logisch gar nicht existieren - ist Mathematik interessant und wichtig.

So, nachdem jetzt die Illusion der absoluten Wissenschaft Mathematik zerstört ist, frage ich nocheinmal: Was ist ein Beweis? Vom logischen Standpunkt aus kann man klar sagen, daß ein Beweis zeigen muß, daß der Satz unter allen Bedingungen wahr ist. Man sollte sich bereits an dieser Stelle davon trennen, Beweise in der Mathematik als Erläuterung von Kausalbeziehungen - wie es in der Physik geschieht - zu verstehen. Zum Beispiel ist der Satz *„3 ist eine Primzahl* $\Rightarrow \sin x$ *ist differenzierbar“* zweifellos wahr, denn sowohl, daß 3 eine Primzahl ist, ist immer wahr als auch, daß $\sin x$ differenzierbar ist. Also ist erst recht die Implikation immer wahr (eine Implikation $A \Rightarrow B$ ist genau dann wahr, wenn die Menge der Wahrheitsbedingungen für A eine Teilmenge der Wahrheitsbedingungen für B ist). Aber natürlich ist es abwegig, eine Ursache der Differenzierbarkeit von $\sin x$ darin zu sehen, daß 3 eine Primzahl ist. Meistens ist die Anzahl der Bedingungen, die für einen Beweis zu prüfen wären, unendlich groß und oft sogar überabzählbar. Man sollte also einen pragmatischeren Beweisbegriff haben. Von unserem psychologischen Standpunkt aus müssen wir einen Beweis als die Vermittlung zweier Sinne auffassen. Diese Vermittlung geschieht wiederum durch Tautologien, aber durch „kleinere“ Tautologien. Wir bezeichnen das Einsetzen einer Definition oder eines Axioms zusammen mit den logischen Grundgesetzen als unzerlegbare Tautologie. Somit sind jetzt schon Sätze, die mit endlich vielen unzerlegbaren Tautologien folgen, beweisbar. Mit Induktionsargumenten und Auswahlaxiomen kann man die Klasse beweisbarer Sätze auf Ketten unendlich vieler Tautologien erweitern. Man sieht trotzdem ein, daß es wohl wahre Sätze geben kann, zu denen kein Beweis möglich ist. Allerdings dürfte es auch schwer fallen, solche Sätze aufzuschreiben.

Jetzt wissen wir zwar, was ein Beweis ist, aber immer noch nicht, wie man ihn am besten aufschreibt.

1.2 Axiom und Definition
Basic Instincts

Gibt man einem Mathematiker ein Problem, so werden sofort seine Urinstinkte geweckt: er definiert und stellt Axiome auf. Was aber sind Definitionen und Axiome? Zu Archimedes Zeiten waren Axiome noch etwas sehr Greifbares. Es waren einfach evidente Wahrheiten. Das Parallelenaxiom war zum Beispiel keine abstrakte Forderung, sondern eine evidente Wahrheit. Man sah in der Welt, daß es gelten müsse. (Da Archimedes es aber nie selbst nachgemessen hat, war das Axiom damals wohl eher ein Glaubenssatz.) Erst seit Hilbert sind Axiome keine Evidenzen im physikalischen Raum mehr, sondern Forderungen im abstrakten logischen Raum. Axiome sind weder wahr noch falsch. Es sind Sätze, die für die Theorie vorausgesetzt werden. Sie sind sozusagen per definitionem wahr. Um aber zu vermeiden, daß Sätze der Theorie zugleich wahr und falsch sind, muß das Axiomensystem widerspruchsfrei sein. Dieses Problem ist nicht geringzuschätzen. Soweit ich weiß, ist erst für die Zahlentheorie die Widerspruchsfreiheit des Axiomensystems bewiesen. (Bei solchen Beweisen werden natürlich die Axiome der Logik vorausgesetzt.) In der Analysis weiß kein Mensch, ob die Axiome sich nicht widersprechen. (Es interessiert allerdings auch keinen einzigen Analytiker.)Man kann nun die

Frage stellen, wieviele verschiedene Beweise für einen bestimmten Satz das Axiomensystem zuläßt. Natürlich sollen dabei keine unnötig eingebauten Umwege dazuzählen. Wir nennen also einen Beweis einen kleinsten Beweis, wenn man nicht durch Weglassen von Schritten immer noch einen Beweis für den Satz erhält. Um zu garantieren, daß es für einen Satz nur einen einzigen kleinsten Beweis gibt, braucht man die Reduziertheit des Axiomensystems. Das heißt, daß für je zwei Axiome $A_1 \neq A_2$ gilt: $\forall A : (A_1 \Rightarrow A), (A_2 \Rightarrow A)$ wahr $\Rightarrow A$ wahr.

Während die Axiome eher die logische Struktur der Mathematik liefern, bilden die Definitionen eher die psychologsiche Struktur. Indem in Definitionen Axiomensystemen ein Name gegeben wird (Körper, angeordnet, vollständig...) werden diese Eigenschaften interpretiert. Und damit meistens auf bekannte Erscheinungen der physikalischen Welt zurückgeführt (zusammenhängend, Ring (ordnet man die Zahlen in $\mathbb{Z}_n$ ringförmig an, so kann man genauso anschaulich addieren und multiplizieren durch Abzählen wie in $\mathbb{Z}$), Fahne (Befestigungspunkt, Mast, Fahnentuch [siehe Fischer]), Garbe ...). Umgekehrt übrigens haben schon abstrakte mathematische Konzepte dazu geführt, die Welt neu zu interpretieren (z.B. Relativitätstheorie). Interessanterweise tragen einfache Strukturen oft komplizierte (meist lateinisch-griechische) Namen (Endomorphismus, Augmentation), während abstraktere, unübersichtlichere Strukturen oft sehr anschauliche Namen besitzen (Garbe, Aufblasung).

Definitionen sind die Teile der Mathematik, die die Konzeptionen tragen. Geometrie wird nicht wegen ihrer logischen Struktur so genannt, sondern weil man die Elemente Gerade, Kreis, Kurve, Fläche etc. nennt. Daß auch Objekte, die auf diese Weise anschaulich nicht zu fassen sind, dieselben logischen Strukturen tragen können, zeigt zum Beispiel die Algebra. Ebenso zeigt sie, daß viele Eigenschaften der ganzen Zahlen auch ganz andere Ringe tragen, die mit Zahlen nichts zu tun haben. Wenn man einen Studenten der Mathematik fragen würde, womit sich die Mathematik beschäftigt, so wird man wohl zwei verschiedene Antworten unterscheiden können: der eine denkt sofort an die Konzeptionen der Mathematik und sagt, daß Flächen im Raum, Kurven auf Flächen, Zahlen, Strömungen, Probleme der Mechanik ... die Themen der Mathematik sind, ein anderer wird sagen, daß sich die Mathematik mit Denkstrukturen und Arten des logischen Denkens beschäftigt. Beide haben recht. Der erste ging vom psychologischen Standpunkt aus und erinnerte sich an die Definitionen, die er gelernt hat. Er ist wohl auch derjenige, der auf Außenstehende einen besseren Eindruck hinterläßt . Der zweite ging von der Logik aus und sagt, die Mathematik ist die Menge aller Tautologien. Er erinnert sich der Axiome, die er einmal gesehen hat und kommt zu dem Schluß, daß jedes Axiomensystem eine andere Art des Denkens verlangt, die Mathematik sich also mit den Arten des Denkens beschäftigt.

1.3 Die Logische Elementarform
How to make people crazy

Die Logische Elementarform, wie ich sie hier einführe, bestätigt mal wieder die Vorurteile gegen Mathematiker: was sie machen, ist absolut exakt und zu absolut nichts zu gebrauchen. Nichtsdestotrotz bin ich der Ansicht, man sollte einmal einen Beweis in dieser Form gesehen und selbst gemacht haben.

Jetzt aber zur Logischen Elementarform. Als Logischen Elementarschritt bezeichne ich das Einsetzen einer Definition oder eines Axioms. In der schriftlichen Form des Beweises muß dann jeder Elementarschritt numeriert werden und die Definition oder das Axiom, das verwendet wird, eindeutig benannt werden.

Beispiel: Gegeben seien die Axiome eines angeordneten Körpers:

Sei K eine Menge,

$$+ : K^2 \to K : \tag{1.1}$$

$$\forall a, b, c \in K; \quad a + (b + c) = (a + b) + c \tag{1.2}$$

$$\forall a, b \in K : \qquad a + b = b + a \tag{1.3}$$

$$\exists 0 \in K \; \forall a \in K : \qquad a + 0 = a \tag{1.4}$$

$$\forall a \in K \; \exists - a \in K : \qquad a + (-a) = 0 \tag{1.5}$$

$$* : (K \setminus \{0\})^2 \to K \setminus \{0\} : \tag{1.6}$$
$$\forall a, b, c \in K : \quad a * (b * c) = (a * b) * c \tag{1.7}$$
$$\forall a, b \in K : \quad a * b = b * a \tag{1.8}$$
$$\exists 1 \neq 0 \in K \ \forall a \in K : \quad a * 1 = a \tag{1.9}$$
$$\forall a \in K \ \exists a^{-1} \in K : \quad a * a^{-1} = 1 \tag{1.10}$$

$$\forall a, b, c \in K : \quad a * (b + c) = a * b + a * c \tag{1.11}$$

$$\exists K_+ \subset K : \tag{1.12}$$
$$\forall a \in K \setminus \{0\} : \quad (a \in K_+ \iff -a \notin K_+) \tag{1.13}$$
$$0 \notin K_+ \tag{1.14}$$
$$\forall a, b \in K_+ : \quad a + b \in K_+ \tag{1.15}$$
$$\forall a, b \in K_+ : \quad a * b \in K_+ \tag{1.16}$$

Definition: *1) Man sagt $a > b$, falls $a - b \in K_+$.*
2) K mit den obigen Axiomen heißt angeordneter Körper.
Der zu beweisende Satz soll sein:
Satz: *Sei K ein angeordneter Körper. Dann ist $1 > 0$.*
Der Beweis in der Logischen Elementarform ist auf Seite 10 abgedruckt.

Man kann sich leicht vorstellen, daß diese Form bei echten großen Beweisen leicht unübersichtlich wird. Die Schritte sind zwar völlig einfach, dennoch bleiben die wichtigen Ideen auf der Strecke. Einen solchen Beweis sollte man vielleicht einmal gesehen haben oder einmal selbst gemacht haben, um das Gefühl für das Elementare zu bekommen. Um aber eigene Ergebnisse darzustellen, ist diese Form reichlich ungeeignet, es sei denn, Du willst Deine Leser in den Wahnsinn treiben.

1.4 Zeit in der Logik
How to disturb people

So unübersichtlich und umständlich die Logische Elementarform auch erscheinen mag, eines sollten wir trotzdem aus ihr lernen: Es reicht nicht, einfach die Menge der Axiome und Definitionen mit ihren Vielfachheiten hinzuschreiben, die man im Beweis verwendet hat, die Reihenfolge spielt eine große Rolle. Manchmal sind Schritte erst möglich, wenn man vorher etwas anderes bewiesen hat, manchmal lassen sich zwar Schritte vertauschen, ergeben jedoch dann Beweise für verschiedene Sätze.
Beispiel: Es soll einmal bewiesen werden, daß f stetig ist und ein anderes Mal, daß f gleichmäßig stetig ist. Im ersten Fall wird irgendwann die Schrittfolge

$$\forall x \ \forall \epsilon > 0 \ \exists \delta > 0 \ \forall y : (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon)$$

benötigt, das heißt, in der Logischen Elementarform müssen zuerst x und ϵ gewählt werden, bevor ich δ habe. Im Fall, daß gleichmäßige Stetigkeit zu zeigen ist, benötigt man die Schrittfolge

$$\forall \epsilon > 0 \ \exists \delta > 0 \ \forall x \ \forall y : (|x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon)$$

das heißt, daß ich das δ vor dem x habe. Wahl von x und Bestimmung von δ ergeben bei Vertauschung zwei verschiedene Beweise.
Bei anderen Beweisen kann es wiederum passieren, daß sich Schritte vertauschen lassen, ohne daß sich etwas logisch ändert.
Beispiel: Es soll bewiesen werden, daß ein Raum wegzusammenhängend ist. Dann muß man also für je zwei Punkte x und y einen Weg von x nach y finden. Ob ich im Beweis nun zuerst x wähle und dann y oder umgekehrt ist egal.
In Vorlesungen wird wahrscheinlich schon oft die Floskel „man kann sich gleichzeitig a_i wählen, sodaß...“ oder „man nimmt erst x und dann y, sodaß...“ oder auch „so zeigt man nacheinander“. Sie

Beweis: $1 > 0$

Nummer	Axiom	Schritt
1	Annahme	$-1 \in K_+$
2	1.16	$(-1)(-1) \in K_+$
3	1.15	$(-1) + (-1)(-1) \in K_+$
4	1.9	$(-1) * 1 + (-1) * (-1) \in K_+$
5	1.11	$(-1) * (1 + (-1)) \in K_+$
6	1.8	$(1 + (-1)) * (-1) \in K_+$
7	1.5	$0 * (-1) \in K_+$
8	1.4	$0 * (-1) + 0 \in K_+$
9	1.5	$0 * (-1) + (0 - 0) \in K_+$
10	1.2	$(0 * (-1) + 0) - 0 \in K_+$
11	1.3	$(0 + 0 * (-1)) - 0 \in K_+$
12	1.9	$(0 * 1 + 0 * (-1)) - 0 \in K_+$
13	1.11	$0 * (1 + (-1)) - 0 \in K_+$
14	1.5	$0 * 0 - 0 \in K_+$
15	1.4	$(0 * 0 + 0) - 0 \in K_+$
16	1.9	$(0 * 0 + 0 * 1) - 0 \in K_+$
17	1.11	$0 * (0 + 1) - 0 \in K_+$
18	1.3	$0 * (1 + 0) - 0 \in K_+$
19	1.4	$0 * 1 - 0 \in K_+$
20	1.9	$0 - 0 \in K_+$
21	1.5	$0 \in K_+$
22	1.14	Widerspruch!
23	Annahme	$-1 = 0$
24	22	$1 + (-1) = 1 + 0$
25	1.5	$0 = 1 + 0$
26	1.4	$0 = 1$
27	1.9	Widerspruch!
28	1.13	$1 \in K_+$
29	1.4	$1 + 0 \in K_+$
30	1.5	$1 + (0 - 0) \in K_+$
31	1.3	$(1 + 0) - 0 \in K_+$
32	1.4	$1 - 0 \in K_+$
33	Def1	$1 > 0$

Allein für diesen Satz werden schon 33 Schritte benötigt. Der Beweis ist chronologisch angeordnet. Die Blöcke 1-22 und 23-27 kann man vertauschen, sie sind gleichzeitig. Im zweiten Block kann man Schritt 25 mit Schritt 26 vertauschen. Das Einsetzen von 1.4 und 1.5 an dieser Stelle geschieht also gleichzeitig.

alle verwenden zeitliche Begriffe in der Logik, was ja eigentlich absurd ist (wo in der Logik gibt es Zeit und Raum?). Aber wir können das nun exakt auffassen. Zwei Beweisschritte sollen gleichzeitig heißen, wenn sie logisch vertauschbar sind. Sind sie es nicht, so läßt sich eine eindeutige Reihenfolge im Beweis festlegen. Muß Schritt a vor Schritt b erfolgen, so nennen wir a früher als b und b später als a. Diese Einteilung verlangt die Logik nicht und so etwas ist ihr auch völlig fremd. Denn allein der Begriff des Beweises ist ja logisch absurd. Es ist zu betonen, daß die zeitliche Denkgewohnheit „erst muß ich etwas haben, um dann damit arbeiten zu können" nicht der Logik entspringt, sondern der Psyche bzw. der Welt, in der wir Menschen leben, in der es eben Zeit gibt. Man könnte einmal überlegen, wie es sich auf die Mathematik auswirken würde, gäbe es keine Zeit. Aber das ist hier nicht mein Thema. Um einen Beweis verständlich darzustellen, sollte er allerdings die Denkgewohnheiten berücksichtigen, er sollte daher chronologisch geordnet sein.

Regel 1: Ordne die Beweisschritte chronolgisch an!

Das ist nicht immer selbstverständlich. Oft genug liest man in Beweisen „Wähle x so, daß ... Das geht, weil..." Dies kann Übersicht schaffen, aber auf Kosten des logischen Stroms. Besser ist es, im logischen Strom chronologisch fortzufahren und an entsprechender Stelle hervorzuheben „Also kann man x so wählen, daß...". Das ist genauso übersichtlich und wahrt die Chronologie. Damit kann der Leser besser folgen.

1.5 Ausdruckshierarchien
How to pronounce sentences

Bis jetzt haben wir immer vereinfachend vom Satz, der bewiesen werden soll, gesprochen. Aber um einen Satz ranken sich traditionell viele andere Formen des Ausdrucks, z.B. die Bemerkung, das Lemma, das Korollar, ...

1.5.1 Lemmata (Hilfssätze)

Das Lemma oder der Hilfssatz dient dazu, einen Satz zu beweisen. Das Ergebnis des Lemmas für sich ist meist unwichtig, wichtig ist die Anwendung als Beweisschritt zu einem Satz. Im Satz dagegen ist das Ergebnis an sich wichtig. In großen Beweisen kann es auch im Grundstudium vorkommen, daß zu einem Beweis mehrere Lemmata (zum Beispiel zum Satz von Sylow) formuliert werden. Manchmal formulieren Professoren die Lemmata erst im Beweis des Satzes oder gar erst hinterher. Im Hinblick darauf gilt auch wie oben, daß die Lemmata besser vor dem Satz zu sagen und zu beweisen sind. Dann kann der Leser/Zuhörer ihre Aussage und Idee gleich an der Stelle im Beweis des Satzes verstehen, an der das Lemma benötigt wird.

1.5.2 Korollare

Ein Korollar ist ein Satz, der in enger Beziehung zu einem anderen Satz steht. Manchmal versteht man auch eine äquivalente Formulierung des Satzes als Korollar. Es kann aber auch nur eine Folgerung sein, dann allerdings eine mit hohem theoretischen Wert. Ein Korollar muß für Argumentationen im Rahmen der Theorie genauso nützlich sein wie der Satz selbst.

1.5.3 Folgerungen

Eine Folgerung ist ein Satz, der aus einem anderen Satz nur unter Hinzunahme einfacher, gewöhnlicher Argumente folgt. Meistens stehen in den Folgerungen die Lösungen der Probleme, durch die die ganze Theorie motiviert worden ist. Zum Beispiel kann in einer Algebravorlesung der Fundamentalsatz (sic!) der Zahlentheorie als Folgerung auftauchen.

1.5.4 Bemerkungen

Eine Bemerkung zeichnet sich dadurch aus, daß ihr Beweis nur aus einfachen, gewöhnlichen Argumenten besteht. Oftmals steht eine Bemerkung auch in der Nähe eines Beispiels, manchmal stellt sie eine Spezialsierung des Satzes dar.

1.5.5 Beispiele

In einem Beispiel sollen die theoretischen Strukturen des Satzes durch greifbare, „anschauliche“ Objekte ersetzt werden (zum Beispiel $\mathbb{R}^n$ statt Vektorraum). Der Satz wird einfach auf einen sehr speziellen Fall angewandt. Die Beispiele sind die eigentlichen Quellen der Erkenntnis. Prof. Peternell: „Man kennt eine Struktur genau so gut, wie viele Beispiele man dazu kennt.“ Es ist logisch, daß die absolute Kenntnis der Struktur und die Kenntnis aller Beispiele zusammenfallen.

1.6 Logische Kausalität
Nature in mathematics

Wir haben oben schon gesehen, daß wir mit dem Begriff Kausalität vorsichtig sein müssen. Im Beispiel war ja *„3 ist Primzahl* $\Rightarrow \sin x$ *ist differenzierbar“* ein wahrer Satz, aber daß 3 Primzahl ist, kann man wohl nicht als Ursache der Differenzierbarkeit des Sinus ansehen. Andererseits stellen Mathematiker immer wieder Fragem nach dem Warum. Warum ist eine Abbildung stetig? Warum ist $e^{-\frac{1}{x^2}}$ nicht taylorentwickelbar um 0? Die Frage ist hier nicht die Frage nach einem Beweis, sondern es geht hier darum, „Ursachen“ zu finden. Was aber sind jetzt logische Ursachen? Es ist mir bis jetzt nicht gelungen, den Begriff Ursache logisch adäquat zu erfassen. Wenn wir ehrlich sind, meinen wir mit Ursache doch immer ein allgemeineres Prinzip als das, das die Wirkung verkörpert. Diese allgemeinen Prinzipien sind aber die mathematischen Konzepte wie Schnittpunkte, Richtungen, Irreduzibilität ... Und die sind, wie ich oben schon gesagt habe, eher psychologisch motiviert als logisch. Wir tun also gut daran, auch Kausalität (übrigens auch Kausalität in der Physik) psychologisch aufzufassen anstatt logisch. Eben die Ursache als ein allgemeines mathematisches Konzept.

Beispiel: Warum ist $e^{-\frac{1}{x^2}}$ *um 0 nicht taylorentwickelbar? Den Beweis zu diesem Satz hört man normalerweise im zweiten Semester. Er beruht darauf, daß alle Ableitungen im Nullpunkt 0 werden. Das ist aber keine Ursache dafür. Warum kann eine Funktion zu „flach“ sein, um schön glatt zu sein? Eine Ursache lernt man dann im vierten Semester kennen. Betrachtet man nämlich die Funktion im Komplexen, so stellt sich heraus, daß sie in 0 eine wesentliche Singularität hat, das heißt die Menge der Grenzwerte, die Bilder von Nullfolgen annehmen können, liegt dicht in* $\mathbb{C}$*. Wenn man also gegen 0 wandert, beginnt die Funktion sich völlig wild zu verhalten. Daß sie auf der reellen Achse gerade unendlich oft differenzierbar ist, ist sozusagen Zufall. Und dieses Konzept erscheint plausibler. Weil sich die Funktion in 0 völlig wild verhält, kann sie nicht so glatt sein, daß es eine Taylorentwicklung gibt.*

Regel 2: Versuche, einen Beweis so darzustellen, dass möglichst allgemeine Prinzipien (Ursachen) zu erkennen sind.

1.7 Erlaubte Symbole
Why ε is bigger than 0

Wir wissen nun einiges über die Psychologie eines Beweises, aber etwas Formales fehlt noch: die Bezeichnungsweisen. Natürlich kann jeder seine Objekte mit Symbolen belegen, wie er mag, aber es gibt einige stillschweigende Übereinkünfte in der Mathematik, an die man sich größtenteils halten sollte. Natürlich halte ich nichts von einem durchkonstruierten Formalismus, bei dem es länger dauert, die richtigen Zeichen zu wählen, als den Beweis zu finden. Aber wie die Definitionen Abkürzungen für Konzepte sind, können auch bestimmte Symbole bestimmte Konzepte in der Mathematik wiederspiegeln. Hier mit zwinkerndem Auge eine kleine Liste der festgelegten Symbole:

α	Isomorphismus von V^{**} nach V, Dreieckswinkel
β	Dreieckswinkel
γ	Dreieckswinkel
δ	existiert immer zu einem ϵ und ist positiv
ε	ist immer größer als 0, Anfang jedes analytischen Beweises: Sei $\varepsilon > 0$
ζ	transformierte z-Koordinate oder auch Integrationsvariable in der Funktionentheorie
η	tranformierte y-Koordinate, manchmal auch im Sinne von ϵ eine positive reelle Zahl
θ	Winkel in Polarkoordinaten, Funktion in der algebraischen Geometrie
ι	Inklusionsabbildung
κ	manchmal kanonische Restklassenabbildung, Summationsindex, Koeffizient in Linearkombinationen
λ	Abzähl-/Summationsindex, Koeffizient in Linearkombinationen
μ	Koeffizient in Linearkombinationen, Maß, Index
ν	Index, natürliche Zahl
ξ	transformierte x-Koordinate, Integrationsvariable
π	Kreiszahl, Projektionen
ρ	Abbildung, Konvergenzradius, Radius von Integrationsgebieten
σ	Abbildung, zahlentheoretische Funktion, Permutation
τ	Abbildung, Transposition, transformierte t-Variable
ϕ, φ	Potential; Funktion, die variiert wird; Abbildung
χ	charakteristisches Polynom, charakteristische Funktion, Charakteristik
ψ	Potential, Abbildung
ω	Krümmungsform
i,j,k,l	zusammen auftretende Indizes
m,n	"
p,q,r,s	"
r,s,t	"
u,v,w	zusammen auftretende Funktionen
x,y,z	zusammen auftretende Koordianten

Diese Tabelle erhebt keinen Anspruch auf Vollständigkeit.

1.8 Mathematische Diplomatie
How to get readers despaired

Im letzten Abschnitt des „psychologischen“ Kapitels widme ich mich nocheinmal der Psychologie des Lesers. Solange man nur Lehrbücher liest, mag man ja noch keine Probleme haben. Beginnt man jedoch irgendwann, einen Artikel für ein Proseminar oder ein Seminar zu lesen, so wird sich schnell eine gewisse Frustration einstellen. Und schuld daran sind meist Formulierungen wie „offenbar gilt“, „it is obvious that“, „Beweis: trivial.“. Denn oftmals sind die beschriebenen Sachverhalte dem Leser nicht offensichtlich und trivial. Und das liegt nur zum Teil daran, daß man den Stoff nicht verstünde. Ein Hauptgrund ist einfach die mangelnde Gewohnheit des Studenten. Man muß es sich nur einfach vorstellen: Ein Professor, gerade 50 geworden, die besten Ideen hatte er wahrscheinlich schon, entschließt sich, einen Überblick über irgendein Gebiet zu geben und schreibt ein Buch darüber. Dann interessiert ihn dabei zum Beispiel, warum der Satz von Lebesgue gilt, und nicht, wie man genau beweist, warum $\frac{1}{\sqrt{x}}$ nicht in L^+ ist. Denn die Argumente für letzteres sind für ihn völlig gewöhnlich und uninteressant. Also wird er in seinem Buch dies auch nur kurz erwähnen, wahrscheinlich mit ähnlichen Floskeln wie die oben genannten. Deswegen müssen die Argumente aber noch lange nicht für den Studenten gewöhnlich sein. Er kann durchaus seine Schwierigkeiten haben, den Beweis dafür zu finden. Manchmal kann die erforderliche Rechnung, die in einem Buch als „trivial“ weggelassen wird, durchaus eine halbe oder ganze Seite beanspruchen, wenn man sie ausführt. Man sei also nicht gleich frustriert, wenn man auf solche Stellen stößt.

Kapitel 2

Häufige Satzstrukturen

How to say something without meaning

Die Struktur der Sätze, die in einer Theorie auftreten, sollten der Struktur der Theorie entsprechen. Man kann ein Ergebnis auf viele verschiedene Arten und Weisen darstellen, aber nur wenige davon sind dem Problem angemessen. Das kann man zum Beispiel in den Analysis-Vorlesungen beobachten. In den ersten beiden Semestern werden nur Funktionen für sich allein untersucht. Die Sätze sind dann auch von der Form „f ist stetig“ oder „f ist Riemann-integrierbar“. Ab dem dritten Semester fängt man in der Analysis an, die Funktionenräume zu untersuchen und gleichzeitig beginnt man auch, eine Lebesgue-integrierbare Funktion als „$f \in L^1(G)$“ zu schreiben. Je nach Interesse der Theorie ändert sich so also die angemessene Form, Sätze darzustellen. Die wichtigsten Satzstrukturen will ich hier kurz erläutern.

2.1 Äquivalenztabellen

I think if I am

Der erhebendste Augenblick einer Mathematikvorlesung ist, wenn man monatelang verschiedenste Objekte definiert, axiomatisiert, Hilfssätze darüber beweist und am Schluß ein großer Satz steht, der sagt: Es ist doch alles dasselbe!

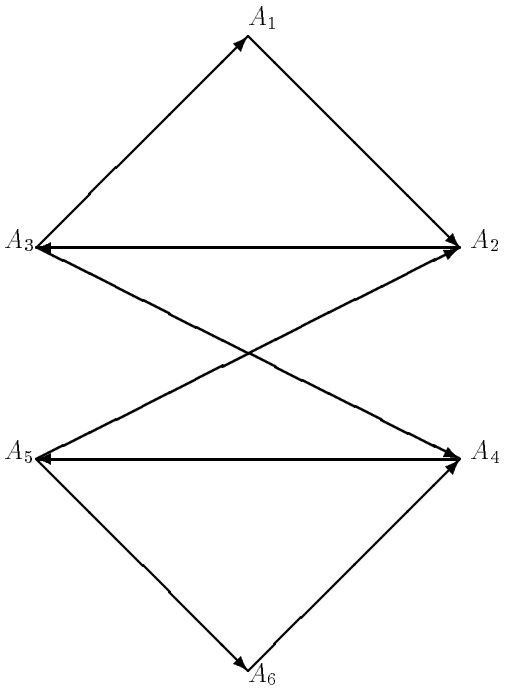
Dieser große Satz wird meistens eingeleitet durch die Zauberworte „Sei dies und das gegeben. Dann sind äquivalent: ... “ Solche Äquivalenztabellen treten bevorzugt in der Algebra auf. (Das liegt wohl daran, daß man in der Algebra besonders viele Definitionen hat.) Diese Form von Sätzen muß dem Mathematiker eigentlich am liebsten sein. Denn wenn sie gelten, bedeutet dies ja, daß die verschiedenen Sinne vollständig, ohne Verlust von Information, vermittelt werden können. Und damit ist das dahinter stehende mathematische Problem vollständig gelöst.

Beim Beweisen solcher Äquivalenztabellen muß man natürlich nicht für alle Aussagen A_i und A_j die Äquivalenz nachrechnen. Hat man Aussagen A_1,...,A_n und soll ihre Äquivalenz nachweisen, so ist der kürzeste Beweisweg $A_1 \Rightarrow A_2 \Rightarrow ... \Rightarrow A_n \Rightarrow A_1$. Aber oftmals geht es nicht so direkt und man muß weitere Wege gehen.

Beispiel: Es soll die Äquivalenz von A_1, A_2, A_3, A_4 gezeigt werden. Dann reicht es zu zeigen:

$$A_1 \Longleftrightarrow A_2, A_3 \Rightarrow A_2, A_3 \Longleftrightarrow A_4, A_1 \Rightarrow A_4.$$

Allgemein: Stellt man die A_n als Punkte dar und Implikationen $A_i \Rightarrow A_j$ als Pfeil von A_i nach A_j, so sind alle Aussagen äquivalent, wenn es einen geschlossenen Weg gibt, der alle Punkte enthält. Man darf freilich nur in Pfeilrichtung laufen. Ein solches Bild einer Beweisstruktur kann dann etwa so aussehen:



In diesem Fall haben wir 8 Implikationen nachzuweisen. Die minimale Anzahl liegt aber bei 6 Implikationen, nämlich der Fall $A_1 \Rightarrow A_2 \Rightarrow A_3 \Rightarrow A_4 \Rightarrow A_5 \Rightarrow A_6 \Rightarrow A_1$(dies entspricht im Diagramm dem Sechseck). Daß dies wirklich die minimale Anzahl ist, zeigt man, indem man annimmt, es würden $r < n$ Implikationen zu zeigen ausreichen, um eine Äquivalenztabelle mit n Aussagen zu beweisen. Dann gibt es natürlich ein A_i, so daß keine Implikation der Form $A_i \Rightarrow A_j$ bewiesen wird. Insbesondere wird also $A_i \Longleftrightarrow A_j$ nicht bewiesen. Wir können nun also mit Recht sagen, daß eine Äquivalenztabelle mit n Aussagen n Informationen trägt. Es ist klar, daß jeder kürzeste Beweisweg (mit n Schritten) im Diagramm durch eine Permutation der Aussagen in ein n-Eck übergehen können muß. Umgekehrt liefert natürlich jede Permutation einen kürzesten Beweisweg, indem man im Diagramm erst die Aussagen permutiert und dann zum n-Eck verbindet. Also gibt es genauso viele kürzeste Beweiswege wie Permutationen von n Aussagen, also genau $n!$ Stück. Neben diesen einfachen geschlossenen Wegen gibt es natürlich noch kompliziertere Beweise. Zum Beispiel könnte ein Schritt auch darin bestehen, die Implikation $A_1 \wedge A_2 \Rightarrow A_3$ zu zeigen. Dies führt aber höchstens zu längeren Beweisen als solche der obigen Art. In der Praxis spielen die komplizierteren Beweise auch nur selten eine Rolle.

2.2 Existenzsätze
I think, so I exist

Eigentlich liegt es jetzt nahe, philosophisch anzufangen und zu fragen, was Existenz ist. Ich werde das auch tun, bevor ich auf die mathematische Existenz zu sprechen komme. Im Alltag sagen wir, daß ein Glas existiert, oder ein Haus, ein Tisch, eine Stadt. Und was wir meinen ist nicht, daß wir das Glas wahrnehmen können (dann würden wir sagen, daß die Wahrnehmung existiert), denn auch wenn uns eine Fata Morgana Wasser vorspiegelt, existiert dieses Wasser ja nicht. Mit dem Begriff der Existenz des Glases verbinden wir spontan auf jeden Fall, daß wir das Glas wahrnehmen (sehen, fühlen, hören (wenn Wind darüber streicht)) können, daß ein Fußtritt in seine Scherben uns verletzen würde, daß auch andere das Glas sehen und fühlen können.

Schwieriger wird die Lage, wenn wir Existenz von Dingen wie schönem Wetter, Konzerten, dem Bösen ... aussagen wollen. Wenn wir nämlich sagen, „Es gibt schönes Wetter“ oder „Es gibt Klavierkonzerte“, dann meinen wir ja nicht eine momentane Präsenz des schönen Wetters oder des Konzerts,

sondern seine prinzipielle Möglichkeit. Auch wenn es jetzt gerade regnet, weiß jedes Kind, daß es schönes Wetter gibt. Wenn wir genau hingeschaut haben, merken wir, daß die Existenz des Glases sich auch in der *Möglichkeit* des Gesehenwerdens, Gefühltwerdens und Verletzens besteht, nicht darin, daß es tatsächlich wahrgenommen wird.

Noch komplizierter wird es bei Dingen wie dem Bösen. Denn das kann ich gar nicht mehr konkret fassen. Konnte man bei Konzerten noch sagen, wann und wo sie stattfinden (so konnte man ihre Existenz beweisen), so ist das bei dem Bösen ganz und gar unmöglich. Das liegt vor allem daran, daß verschiedene Menschen gleiche Sachverhalte verschieden bewerten. Für den einen ist vorehelicher Sex Sünde, für den anderen das Natürlichste der Welt. Diese Überlegung zeigt uns also, daß Existenz von Dingen durch die eigene Existenz definiert wird. Auch vorhin schon war das eigentlich sichtbar. Auch wenn die Existenz des Glases nicht seine Wahrnehmbarkeit ist, so läßt sich aber Existenz erst dadurch definieren, daß etwas wahrgenommen wird. Und die Wahrnehmung hängt von der Existenz des Wahrnehmenden ab. Die Behauptung, Existenz sei dann doch schließlich unabhängig vom Wahrnehmenden, ist eine unbewiesene Hypothese. Die Überprüfung, ob etwas existiert, macht essentiellen Gebrauch vom wahrnehmenden Subjekt.

Wir halten also zwei Punkte fest: Existenz ist eine prinzipielle Möglichkeit (der Wahrnehmung, Veränderung ...) und Existenz von Dingen ist abhängig von der Existenz des Subjekts.

Diese beiden Prinzipien kommen auch in mathematischer Existenz vor. Denn, was ist mathematische Existenz? Sie ist eine Möglichkeit im logischen Raum. Wir sagen zum Beispiel, daß zu jeder Indexmenge ein freier Modul mit der Menge als Basis existiert - und meinen damit, daß ein solcher Modul logisch widerspruchsfrei denkbar ist. Solche Existenzsätze, die nur Gebrauch vom logischen Raum - den logischen Axiomen - machen, sind aber sehr selten. Wesentlich öfters werden dabei noch mehr Axiome vorausgesetzt, etwa, wenn man die Existenz einer Lösung einer Differentialgleichung beweisen will. Wie oben schon einmal erwähnt, ist die Widerspruchsfreiheit der Axiome der Analysis noch nicht bewiesen. Das heißt, daß eine Lösung einer Differentialgleichung keine Möglichkeit im logischen Raum sein muß, sondern nur im analytischen Raum. Was heißt das aber, wenn der analytische Raum vielleicht Widersprüche hat? Das muß uns nicht stören. Wenn die Axiome widersprüchlich sind, heißt das nur, daß auch die Nichtexistenz der Lösung eine Möglichkeit ist. Das Prinzip des ausgeschlossenen Dritten gilt dann einfach nicht mehr. Noch einmal deutlich: im logischen Raum, der vorausgesetzt wird, gilt das Prinzip des ausgeschlossenen Dritten. Es darf also in Beweisen auch im analytischen Raum benutzt werden. Nur kann daraus nicht geschlossen werden, daß die verneinte Aussage im analytischen Raum nicht bewiesen werden könnte. Also: wenn A wahr ist, ist zwar $nicht - A$ falsch. Aber $nicht - A$ könnte gleichzeitig wahr sein. Zurück zum Thema. Wenn Existenzsätze mehr Axiome als die logischen brauchen, setzen sie eine Existenz anderer Objekte voraus. Die Existenz der Lösung von Differentialgleichungen hängt von der Existenz des analytischen Raumes und der Voraussetzungen ab.

Also haben wir insgesamt: Existenz ist eine Möglichkeit (im logischen Raum, analytischen Raum...) und Existenz von mathematischen Objekten hängt von der Existenz anderer mathematischer Objekte ab.

Welche Bedeutung haben Existenzsätze für die Mathematik? Ich würde sagen, sie stellen eine Art Reiseführer durch das Land der Logik dar. Sie zeigen einem, was es alles gibt. Wie ein Reiseführer alle wichtigen und sehenswerten Stätten eines Landes beschreibt, beschreiben Existenzsätze alle interessanten Konstruktionen und Objekte der Mathematik.

2.3 Eindeutigkeitssätze

I think there is at most one person who is me

Der Eindeutigkeitssatz ist das Pendant zum Existenzsatz. Oftmals treten beide gemeinsam auf. Während der Existenzsatz nur sagt, daß es ein bestimmtes Objekt gibt, aber nicht, wieviele davon, sagt der Eindeutigkeitssatz, daß es höchstens ein Objekt der Art geben kann, wenn überhaupt. Ob es eines gibt, läßt er offen. Das Ziel der Mathematiker ist es natürlich, die Definition so zu wählen, daß es ein so definiertes Objekt gibt. Wenn es aber zuviele davon gibt, gefällt es ihnen auch nicht. Denn dann heißt das, daß sie erstens Schwierigkeiten haben, alle Beispiele zu kennen und zweitens, daß sie in ihrer Definition noch viel mehr hätten verlangen können. Sie haben Eigenschaften

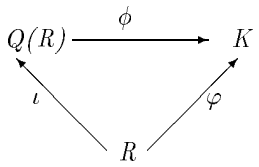
hergeschenkt - und das in der derzeitigen Rezession. (Da haben die Analytiker wieder mal Glück gehabt: es gibt genau einen vollständigen, angeordneten Körper: die reellen Zahlen.) Deswegen ist der Mathematiker immer heilfroh, wenn er weiß, daß es (bis auf Isomorphie) genau ein Objekt gibt, das seiner Definition entspricht. (Wenn er soweit ist, kann er in Ruhe alle Sinne der Definition erforschen und Äquivalenztabellen aufstellen (siehe 2.1).) Manchmal passiert es aber auch, daß zwar die Eindeutigkeit bekannt ist, die Existenz aber nicht. Dann ist es interessant, wie die Objekte aussehen, die existieren.
Beispiel: Man kann alle Darstellungen von Primzahlen p als Differenz zweier n-ter Potenzen untersuchen. Also: finde alle $x, y \in \mathbf{N}$ mit

$$p = x^n - y^n$$

Es gilt: Für alle n und Primzahlen p ist $\{x, y\}$ eindeutig bestimmt und für $n = 2$ existiert eine Lösung, wenn $p \neq 2$. Für größere n kann man zeigen, daß solche p, für die eine Lösung der Gleichung existiert, niemals Summe zweier n-ter Potenzen sein können. Für $n = 3$ müssen Primzahlen, für die eine Lösung der Gleichung existiert von der Form $6m + 1$ sein. (Übung: Beweise dies alles!)
Das Beispiel zeigt, daß Eindeutigkeitssätze dadurch interessant werden können, daß die Existenzbedingungen im Dunkeln liegen. (Umgekehrt werden Existenzsätze dadurch interessant, daß die Eindeutigkeitsbedingungen nicht klar sind.)

2.4 Universelle Eigenschaft
The fittest who survives

Eine universelle Eigenschaft sollte man ab dem dritten Semester eigentlich kennen. Im zweiten Semester Lineare Algebra kommt zum Beispiel das q-fache äußere Produkt $\Lambda^q M$ vor. Man kann es zum Beispiel mit Hilfe einer universellen Eigenschaft definieren. Aber auch der Quotientenkörper (aus Algebra I) hat eine universelle Eigenschaft:
Beispiel: Für einen Integritätsring R definiert man einen Quotientenkörper so: Ein Paar $(Q(R), \iota)$, $Q(R)$ Körper und ι ein Monomorphismus von R nach $Q(R)$, heißt Quotientenkörper von R, wenn folgende universelle Eigenschaft gilt: **Zu jedem** *Körper K und* **jedem** *Mono***morphismus** $\varphi : R \longrightarrow K$ **gibt es genau einen** *Mono***morphismus** $\phi : Q(R) \longrightarrow K$, **so daß das Diagramm**



kommutiert.

Was ist die allgemeine Struktur einer universellen Eigenschaft? Ich habe die Passagen im Beispiel, die unverändert bleiben fett gedruckt. Es geht darum, innerhalb einer Kategorie ein Objekt auszuzeichnen. Deswegen muß diese Abbildungseigenschaft für alle anderen Objekte dieser Kategorie (im Beispiel Körper) erfüllt sein. Die zweite Allbedingung („für alle Monomorphismen“ im Beispiel) stellt die besondere Eigenschaft heraus. Daß es sich hier um *Mono*morphismen handeln muß, bedeutet, daß R in $Q(R)$ eingebettet werden soll. Die Existenz des Monomorphismus ϕ bedeutet, daß Q(R) der kleinste Körper ist, in den der Ring R eingebettet werden kann. Also: Die Eigenschaft, die die Abbildungen φ, ι und ϕ haben (immer gleichzeitig), definiert die Eigenschaft des Objektes, das die universelle Eigenschaft haben soll. Beim äußeren Produkt wäre diese Eigenschaft Multilinearität und Alterniertheit der Abbildungen, beim Tensorprodukt nur Multilinearität. Genauso essentiell wie die Angabe der Eigenschaften der Abbildungen ist natürlich die Angabe der Grundstruktur, von der aus ι und ϕ abbilden. Beim Tensorprodukt und äußeren Produkt wäre das M^q. Ist beides gegeben, so weiß man also, in welcher Beziehung das Objekt mit der universellen Eigenschaft zur Grundstruktur steht.

Das Konzept der universellen Eigenschaft ist vergleichbar mit dem Konzept der Invarianten der Physik. Früher hat man Naturgesetze formuliert, wie Newton zum Beispiel $F = ma$. Heute versucht

man vielfach, Bewegungsabläufe durch Erhaltungsgrößen zu beschreiben: Energie, Impuls, Drehimpuls, ... bleiben konstant. Das ist einfach ein anderes Konzept, eine andere Darstellung. Ebenso hatte man früher den Objekten die Eigenschaft direkt zugeschrieben, etwa „der kleinste Körper, der R enthält“ oder „die größte offene Menge, die noch in A liegt“. Heute geht man dazu über, so etwas mit Hilfe von Abbildungen und deren Eigenschaften zu beschreiben. Sowohl im physikalischen als auch hier im mathematischen Fall liegen die Vorteile klar auf der Hand: man kann damit besser theoretisch rechnen, also besser beweisen. Allgemein kann man sagen, daß man in Abbildungen ganz gut Information lagern kann. Ein immer wieder benutztes Konzept ist es ja zum Beispiel, wenn man zeigen soll, daß irgendwas ein Normalteiler ist, zu zeigen, daß es ein Kern eines Homomorphismus ist. Und in der ganzen algebraischen Geometrie und Topologie werden geometrische Objekte durch bestimmte Abbildungen, die es darauf gibt, charakterisiert.

2.5 Klassifikationen
What a number can look like

Eine Klassifikation ist eigentlich nur eine Aneinanderreihung von Existenz- und Eindeutigkeitssätzen. Man sagt, welche Beispiele alle existieren und in welcher Hinsicht sie eindeutig sind. So besteht eine Klassifikation aus zwei Komponenten: Man gibt erstens an, nach welchem Kriterium man klassifizieren will (zum Beispiel erlaubt man meistens Koordinatentransformationen in der Linearen Algebra oder Homöomorphien in der Topologie), das heißt, man gibt eine Äquivalenzrelation vor, eine Bedingung, die sagt, welche Fälle man miteinander identifzieren soll. Danach gibt man alle Äquivalenzklassen an. Die Äquivalenzrelation kann manchmal auch nur irgendwo versteckt stehen und nicht explizit genannt sein.
Beispiel: Man gebe alle Gruppen der Ordnung 8 an. Dabei ist gemeint: alle bis auf Isomorphie. Die Äquivalenzrelation ist hier also Isomorphie. Die Äquivalenzklassen sind repräsentiert durch $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4$ *und* Q*, wobei* D_4 *die Symmetriegruppe des Quadrats und* Q *die sogenannte Quaternionengruppe ist.*

Klassifikationen stehen meist am Ende einer Theorie. Nachdem man schon einige Existenzaussagen kennt, kann man, wenn man Glück hat, sie alle zu einer großen Klassifikation zusammenfassen. Daher sind Klassifikationen, wenn sie existieren, die wichtigsten Sätze einer Theorie.

Oftmals aber gibt es noch gar keine fertigen Klassifikationen. Zum Beispiel kennt man bezüglich Isomorphie noch keine allgemeine Klassifikation endlicher Gruppen. (Nur die einfachen Gruppen sind klassifiziert. Der Beweis benötigte 254 Seiten.) Bezüglich Homöomorphie sind die Klassen von Mannigfaltigkeiten völlig unbekannt. An vielen Stellen der Mathematik ist auch die Äquivalenzrelation, nach der untersucht wird, keineswegs eindeutig. Zum Beispiel in der Zahlentheorie. Es gibt noch kein Konzept, das die Primzahlen klassifiziert. Da ist von Mersenneschen Primzahlen die Rede oder von Fermatschen. Das sind alles Primzahlen, die einer gewissen Formel genügen und deshalb schöne Eigenschaften haben. Aber man konnte noch keine Familie von nützlichen Formeln finden, so daß jede Primzahl mindestens einer der Formeln genügt. Unser Beispiel im Abschnitt Eindeutigkeitssätze gibt uns zum Beispiel die Möglichkeit, Primzahlen so einzuteilen: Sei $\mathbb{P}_n := \{p \in \mathbb{P} | \exists x, y \in \mathbb{N} : p = x^n - y^n\}$ mit $\mathbb{P}$ die Menge der Primzahlen. Dann ist $\mathbb{P}_2 \cup \{2\} = \mathbb{P}$. Setzt man nun $\pi_n := \{p \in \mathbb{P} | p \in \mathbb{P}_n, p \notin \mathbb{P}_k \text{ für } k > n\}$, so ist

$$\mathbb{P} = \bigcup_{i=1}^{\infty} \pi_n$$

wobei die Vereinigung sogar disjunkt ist. Wir haben aber für die π_n keine explizite Beschreibung. Deshalb ist diese Klassifikation (im Moment) relativ sinnlos.

Kapitel 3

Häufige Beweisstrukturen

How to proof something without meaning

Um einen Satz zu beweisen, haben sich die Mathematiker einiges einfallen lassen. Natürlich dadurch motiviert, sich Arbeit zu sparen. Überhaupt glaube ich, daß die Mathematik nur aus der Faulheit entstand. Da haben sich einige Leute einfach gedacht, wenn sie ein bißchen mehr nachdenken und allgemeine Sätze beweisen, können sie sich viel (Rechen-)Arbeit sparen. Und irgendwann ist dann das Nachdenken und Beweisen zur Arbeit geworden. (Dann haben sie wahrscheinlich angefangen, über Beweismethoden nachzudenken, um sich (Beweis-)Arbeit zu sparen...) Jedenfalls scheint sich ein Prinzip immer wieder zu bewahrheiten: Der **Energieerhaltungssatz der Mathematik**: egal, wie auch immer man den Satz beweist, man muß immer die gleiche Menge Arbeit hineinstecken. Irgendwo muß man arbeiten.

Aber manchmal haben eben andere schon so weit vorgearbeitet, daß man es auf dem von ihnen beschrittenen Weg etwas einfacher hat. Und auch manche Beweisprinzipien haben sich als recht bequemen Weg für manche Probleme erwiesen. Um die wichtigsten erfolgreichen Prinzipien soll es hier gehen.

3.1 Abbildungen

How to get a good image

Häuig werden in Beweisen irgendwelche Abbildungen konstruiert und der Satz dann darauf zurückgespielt, daß diese Abbildung irgendwelche Eigenschaften hat. Da gibt es vier standardmäßige Punkte: Wohldefiniertheit, Surjektivität, Injektivität und Homomorphie.
Wenn es darum geht, zu zeigen, daß eine implizit gegebene Abbildung wohldefiniert ist, muß man beweisen, daß

1.) jedes Element aus der Defintionsmenge wirklich abgebildet wird,

2.) daß es auch immer auf ein Element der angegebenen Bildmenge geht und

3.) daß jedes Element aus der Definitionsmenge tatsächlich nur einmal abgebildet wird, also ein eindeutiges Bild hat.

Der letzte Punkt ist meist der entscheidende, wenn es um Abbildungen zwischen Quotienten geht. Dann gibt man meistens die Abbildung an, indem man sie auf Repräsentanten der Äquivalenzklassen erklärt. Man muß dann nachrechnen, daß die Abbildung unabhängig vom gewählten Repräsentanten ist.
Beispiel: Seien V, W Moduln und

$$\alpha : V^* \otimes W \longrightarrow Hom(V, W)$$

induziert durch

$$\phi \otimes w \mapsto (v \mapsto \phi(v) \cdot w)$$

Dann ist für die Wohldefiniertheit 1.) bis 3.) nachzurechnen. Jeder Tensor wird abgebildet, da „induzieren“ das ja gerade bedeutet. Für den zweiten Punkt muß man nachrechnen, daß die angegebenem Abbildungen $v \mapsto \phi(v) \cdot w$ tasächlich Homomorphismen sind. Als dritten Punkt ist zu zeigen, daß das

Bildelement tatsächlich nur vom Tensor $\phi \otimes w$ abhängt und nicht vom Paar (ϕ, w). (Das heißt, die Multiplikation von Ringelementen mit ϕ oder mit w muß im Bild dasselbe ergeben.)

Wenn es um die Surjektivität einer Abbildung geht, ist prinzipiell immer die Aufgabe, zu jedem Element der angegebenen Bildmenge ein Urbild zu konstruieren. Manchmal kann man sich die Mühe aber sparen, wenn man schon einiges über die an der Abbildung beteiligten Strukturen weiß. Ein injektiver Homomorphismus zwischen zwei gleichdimensionalen Vektorräumen ist zum Beispiel immer surjektiv. Projektionen auf Quotienten sind ebenfalls immer surjektiv.
Beispiel: Wir nehmen α von oben und nehmen ab jetzt an, daß V und W endlichdimensionale Vektorräume sind, unser Ring also ein Körper. Dann ist ein Homomorphismus ω von V nach W durch die Bilder einer Basis von V induziert. Sei $\{v_1, ..., v_n\}$ eine Basis von V, $\phi_i : V \longrightarrow K$, $\phi_i(v_j) = \delta_{ij}$ und $w_i = \omega(v_i)$. Ist dann $v = r_1v_1 + r_2v_2 + ... + r_nv_n$, so gilt:

$$\omega(v) = \sum_{i=1}^{n} r_i\omega(v_i) = \sum_{i=1}^{n} r_iw_i = \sum_{i=1}^{n} \phi_i(v)w_i$$

das heißt aber genau

$$\omega = \alpha(\sum_{i=0}^{n} \phi_i \otimes w_i)$$

Deshalb ist α surjektiv.

Injektivität ist meistens leichter nachzuprüfen. Im allgemeinen muß man ansetzen: $f(a) = f(b)$ und dann irgendwie folgern, daß $a = b$. Nur im Fall, daß man weiß, daß f ein Homomorphismus ist, reicht es, nachzuprüfen, ob $f(a) = 0 \Rightarrow a = 0$ gilt. Deshalb sollte man die Homomorphismus-Eigenschaft eigentlich immer zuerst überprüfen. Auch hier können strukturelle Eigenschaften der an der Abbildung beteiligten Mengen wichtige Hilfen sein. Ein Körperhomomorphismus, der nicht die Nullabbildung ist, ist zum Beispiel immer injektiv. (Allgemein: Je mehr Struktur eine Menge hat, desto weniger Homomorphismen gibt es zwischen solchen Mengen.)
Beispiel: α ist injektiv. Denn die Dimensionen stimmen überein: $dim(V^* \otimes W) = dimV \cdot dimW$; wenn wieder $\{v_1, ..., v_n\}$ Basis von V und $\{w_1, ..., w_m\}$ Basis von W ist, so bilden die Homomorphismen ϕ_{ij} induziert durch $\phi_{ij}(v_i) = w_j$ eine Basis von $Hom(V, W)$. Also ist $dim(Hom(V, W)) = dimV \cdot dimW$. Weil aber nun α surjektiv ist und gilt: $dim(Hom(V, W)) = dim(V^* \otimes W) = dim(Im\alpha) + dim(Ker\alpha)$ folgt $dim(Ker\alpha) = 0$, also $Ker\alpha = 0$, das heißt α ist injektiv. Hierbei wurde freilich schon verwendet, daß α ein Homomorphismus ist.

Die Homomorphismus-Eigenschaft ist meistens das Leichteste. „Homomorphismus " bedeutet „Gleichgestalt" und damit weiß man eigentlich schon, was zu einer gegebenen Struktur ein Homomorphismus ist: eben eine Abbildung, unter der die vom Urbild induzierte Struktur der Struktur der Bildmenge gleicht. Hat man zum Beispiel eine Abbildung f von einer Gruppe G in eine Menge M, so wird man versuchen, auf M eine Verknüpfung einzuführen, indem man die von G „rüberschaufelt": Zu $m, n \in M$ sucht man Urbilder $g, h \in G$ und versucht dann $m \bullet n := f(gh)$ zu definieren. Wenn das gut geht hat man schon so etwas wie einen halben Homomorphismus (nämlich einen Homomorphismus von G auf M mit der eben definierten Struktur). War M von vornherein Gruppe, so kann man untersuchen, ob die Struktur von M mit der von f induzierten übereinstimmt: Hat man m, n aus dem Bild von f, etwa $m = f(g), n = f(h)$, so sollte dann die Multiplikation übereinstimmen: $m \cdot n = m \bullet n$, das heißt $f(g) \cdot f(h) = f(gh)$. Also: man muß sich gar nicht merken, welche Bedingung ein Gruppenhomomorphismus erfüllen muß, man kann sie einfach ableiten aus der Bedingung, daß die von der Abbildung induzierte („rübergeschaufelte") Struktur auf der Bildmenge mit der bereits gegebenen Struktur darauf übereinstimmen muß. Dieses Rezept ist natürlich auf jede beliebige Kategorie anwendbar (Körper, Vektorräume, Moduln, Garben, Komplexe...).

In unserem Beispiel sieht man sehr leicht, daß α ein Homomorphismus ist.

3.2 Induktion

Today is today, because yesterday was yesterday

Eigentlich hat das Induktionsprinzip ja etwas mit Physik zu tun. Es ist die alte Frage, die man sich immer wieder stellt, wenn man ein Naturgesetz liest: Gut, bei Newton fielen alle Steine nach

unten, als ich klein war, war das auch noch so und gestern, als mir in der Bibliothek das Buch aus der Hand glitt, fand ich es auf dem Boden wieder; aber was garantiert mir, daß auch morgen noch die Gravitiationskraft $F = mg$ ist ? Gibt die Physik mir dafür einen Grund an? Nein, im Gegenteil: sie setzt das voraus! Diese physikalische Grundannahme, daß es unveränderliche Naturgesetze gibt, nennt man das Induktionsprinzip. Diese Formulierung ist manchen vielleicht etwas seltsam. Richtig, man hat eigentlich Induktion immer anders beschrieben. Aber darauf komme ich jetzt. Die Annahme, daß die Naturgesetze unveränderlich sind, bedeutet ja nichts anderes, als daß man annimmt, aus Erfahrung lernen zu können: Weil gestern die Turmuhr um 12 Uhr schlug, und vorgestern auch, und ebenfalls vor drei Tagen und auch schon in meiner Kindheit, glaube ich zu wissen, daß sie morgen um 12 auch wieder schlagen wird. Ich habe *gelernt* , daß die Turmuhr jeden Tag um 12 Uhr schlägt. Diese Art der Folgerung, ich weiß ein Ereignis $E(t_1)$ zur Zeit t_1, $E(t_2)$ zur Zeit t_2, ..., $E(t_n)$ zur Zeit t_n mit $t_i < t_j$ für $i < j$ und daraus kann ich zur Zeit t_n schließen, daß es ein Ereignis $E(t_{n+1})$ zur Zeit $t_{n+1} > t_n$ geben wird, ist das Induktionsprinzip, wie man es kennt.

Während nun das Induktionsprinzip der Physik tatsächlich eine empirische Aussage ist, ist das Induktionsprinzip in der Mathematik eine rein logische Sache, obwohl die Formulierung fast dieselbe ist. In der Mathematik formuliert man es in seiner einfachsten Form normalerweise so: Sei zu jeder natürlichen Zahl n eine Aussage $A(n)$ gegeben. Dann ist $\{A(n)|n \in \mathbb{N}\}$ genau dann wahr, wenn $A(1)$ wahr ist und für alle $n \in \mathbb{N}$ der Satz $(A(n) \Rightarrow A(n+1))$ wahr ist.
Beispiel: Normalerweise läßt kein Professor in Analysis I die trivialen Beispiele zur Anwendung des Induktionsprinzips aus. Trotzdem - vielleicht hat ja einer nicht aufgepaßt - will ich ein triviales Exempel zeigen. Die Aussage $A(n)$ soll sein:

$$A(n) = (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$$

Dann ist $A(1) = (1 = 1)$ sicherlich wahr. Also zum Beweis von $(A(n) \Rightarrow A(n+1))$. Es gelte $A(n)$. Dann ist auch wahr:

$$(\sum_{i=1}^{n+1} i = n+1+\sum_{i=1}^{n} i \overset{A(n)wahr}{=} n+1+\frac{n(n+1)}{2} = \frac{(n+1)(n+2)}{2}) = A(n+1)$$

Damit wäre der Satz bewiesen.

Ich will nicht verpassen, noch einmal eindringlichst darauf hinzuweisen, daß beide Schritte im Induktionsbeweis - daß $A(1)$ wahr ist und daß $(A(n) \Rightarrow A(n+1))$ wahr ist - gleich wichtig sind. Läßt man den ersten Schritt weg, so läßt sich alles beweisen. Einen etwas fieseren falschen Induktionsbeweis möchte ich zur Warnung vorführen:
Falsches Beispiel: Der zu beweisende Satz soll lauten:

Entweder sind alle Menschen Frauen oder es sind alle Menschen Männer.

Unser „Induktionsbeweis“ geht nun so: Die Aussagen $A(n)$ sind

$$A(n)=(\text{Unter } n \text{ Menschen sind entweder alle Frauen oder alle sind Männer})$$

Dann ist natürlich $A(1)$ wahr. Sei nun $A(n)$ wahr. Man wähle nun beliebige $n+1$ Menschen $M_0, ..., M_n$ aus. Nach Voraussetzung sind die Menschen $M_0, ..., M_{n-1}$ allesamt Frauen oder allesamt Männer. Ebenso sind die Menschen $M_1, ..., M_n$ allesamt Frauen oder allesamt Männer. Nun ist aber M_{n-1} in beiden Mengen enthalten und daher ist das Geschlecht von M_{n-1} und M_n dasselbe. Also haben alle Menschen $M_0, ..., M_n$ gleiches Geschlecht, was $A(n+1)$ war. Wo ist der Haken? Hast Du es schon? Wenn nicht, denk nochmal nach, bevor Du weiterliest! Gut, so schwierig war es ja gar nicht. Zur Lösung verrate ich nur soviel: Der Satz $(A(n) \Rightarrow A(n+1))$ muß **für alle** $n \in \mathbb{N}$ wahr sein.

Neben dieser einfachen Version von Induktion gibt es noch weitergehende. Zum Beispiel kann man statt über $\mathbb{N}$ auch über $\mathbb{Z}$ induzieren. Das geht so: Sei $A(z)$ eine Aussage für jedes $z \in \mathbb{Z}$ und $z_0 \in \mathbb{Z}$ beliebig. Dann gilt:

$\{A(z)|z \in Z\}$ wahr $\iff$ $A(z_0)$ ist wahr und für jedes $z \in \mathbb{Z}$ ist der Satz $(A(z) \iff A(z+1))$ wahr

Nun liegt natürlich die Frage nahe, was passiert, wenn die Aussagen $A(n)$ in irgendeinem Sinne für $n \to \infty$ gegen eine Aussage $A(\infty)$ konvergiert. Reicht dann als Induktionsanfang die Wahrheit von $A(\infty)$? Im allgemeinen ist das nicht so, wie auch zu erwarten war. Denn es erscheint zutiefst plausibel, daß man irgendetwas wie „Offenheit“ der Aussagen braucht. Unter solch starken Bedingungen kann man tasächlich so etwas formulieren:
Sei X ein topologischer Raum, $A_z \subset X$ für alle $z \in \mathbb{Z}$, $A := \bigcap_{n=0}^{\infty} A_n$, $(a_z)_{z \in \mathbb{Z}}$ eine Familie von Punkten in X und $A(z) = (a_z \in A_z)$. a sei ein Häufungspunkt der Folge $(a_n)_{n \in \mathbb{N}}$. Dann sei

$$A(\infty) := (a \in \overset{\circ}{A})$$

Es gilt:

$\{A(z) | z \in \mathbb{Z} \cup \{\infty\}\}$ ist wahr $\iff$ $A(\infty)$ ist wahr und für alle $z \in \mathbb{Z}$ ist der Satz $(A(z) \iff A(z+1))$ wahr

Der Beweis dieses Induktionsprinzips ist einfach. Ist nämlich $A(\infty)$ wahr, also $a \in \overset{\circ}{A}$, so existiert eine Umgebung von a, die noch ganz in $\overset{\circ}{A}$ liegt, weil $\overset{\circ}{A}$ offen ist. Weil a aber Häufungspunkt ist, liegt insbesondere ein a_n in dieser Umgebung, also auch in A. Damit aber ist a_n insbesondere in A_n. Also ist $A(n)$ wahr. Und so folgt die Wahrheit des Induktionsprinzips aus dem Induktionsprinzip für $\mathbb{Z}$.
Beispiel: Seien $k \in \mathbb{N}, z \in \mathbb{Z}$, $b > 1$. Dann ist

$$\sum_{i=z-k}^{z} b^i \leq \frac{b^{z+1}}{b-1}$$

Um dies mit unserer Limesinduktion zu zeigen, sei $\varepsilon > 0$ und wir definieren $A_z := \{r \in \mathbb{R} | r < \frac{b^{z+1}}{b-1} + \varepsilon\}$ und $a_{zk} = \sum_{i=z-k}^{z} b^i$. Dann ist $(a_{-nk})_{n \in \mathbb{N}}$ sicherlich eine Nullfolge für alle k und damit $a = 0$ ein Häufungspunkt. $A = \bigcap_{n=1}^{\infty} A_{-n} = \{r \in \mathbb{R} | r \leq \varepsilon\}$ und damit gilt, daß $A(\infty) = (a \in \overset{\circ}{A})$ wahr ist. Bleibt also noch zu zeigen, daß $A(z) \iff A(z+1)$. Es ist zu beachten, daß nur über z induziert wird. Das heißt, für jedes z wird die Aussage für alle k gezeigt. Zuerst zeige ich $A(z) \Rightarrow A(z+1)$: Sei k beliebig. Dann ist nach Induktionsvoraussetzung $a_{z,k-1} \in A_z$. Also ist

$$a_{z+1,k} = a_{z,k-1} + b^{z+1} \overset{Ind.vor}{<} \frac{b^{z+1}}{b-1} + \varepsilon + b^{z+1} = \frac{b^{z+2}}{b-1} + \varepsilon$$

also $a_{z+1,k} \in A_{z+1}$ für beliebiges k. Umgekehrt: sei k wieder gegeben. Dann ist wiederum

$$a_{zk} = a_{z+1,k+1} - b^{z+1} \overset{Ind.vor.}{<} \frac{b^{z+2}}{b-1} + \varepsilon - b^{z+1} = \frac{b^{z+1}}{b-1} + \varepsilon$$

also ist a_{zk} in A_z für alle k. Die Induktion wäre damit für beliebiges $\varepsilon > 0$ durchgeführt. Wenn aber die Behauptung

$$\sum_{i=z-k}^{z} b^i < \frac{b^{z+1}}{b-1} + \varepsilon$$

für alle $\varepsilon > 0$ richtig ist, so muß gelten:

$$\sum_{i=z-k}^{z} b^i \leq \frac{b^{z+1}}{b-1}$$

□

3.3 Widerspruch

If it was not, it was. So it is.

Eine der häufigsten und unter Studenten am beliebtesten Beweisstrukturen sind die Widerspruchsbeweise. Logisch aber sind sie gar nicht einmal so einfach zu verstehen.

Betrachten wir zunächst das Problem des Irrealis in der Sprache. Wie kann man einen Satz wie zum Beispiel *„Wenn ich meinen Flug noch erreicht hätte, wäre ich jetzt auch abgestürzt“* verstehen? Die naivste Idee ist freilich, den Satz als logische Implikation aufzufassen: *„Ich habe meinen Flug erreicht ⇒ Ich bin abgestürzt“* . Dann ist der Satz aber natürlich wahr, denn die Voraussetzung *„Ich habe meinen Flug erreicht“* ist ja nicht erfüllt, ihre Wahrheitsbedingungen damit leer. Also sind sie insbesondere eine Teilmenge der Wahrheitsbedingungen von *„Ich bin abgestürzt“* . Es ist aber offenbar nicht Sinn des Irrealis gewesen, eine trivialerweise wahre Aussage zu treffen. Der Satz *„Wenn ich meinen Flug erreicht hätte, wäre ich abgestürzt“* soll ja eine Bedeutung haben. Es soll nämlich damit gesagt werden, daß *„Wenn ich meinen Flug erreicht hätte, wäre ich jetzt bei meiner Tante in New York“* falsch ist. Fassen wir diesen Satz aber wieder als logische Implikation auf, so wäre auch er wahr. Denn die Voraussetzung ist ja wieder falsch. Wir sehen also, daß der Irrealis der Sprache nicht der Implikation in der Logik entspricht.

Und damit beginnen unsere Probleme. Wie kann man einen Irrealis logisch verstehen? Soweit mir bekannt ist, gibt es dafür noch kein schlüssiges Konzept. Was hat dies alles nun mit Widerspruchsbeweisen zu tun? Gewöhnlich fangen solche Beweise mit einer Widerspruchsannahme an, die man sprachlich gerne wiedergibt als „Wäre $x \notin M$, dann wäre...“. Man fängt also mit einem Irrealis an und behandelt ihn wie eine logische Implikation. Das aber, haben wir gerade gezeigt, ist Unsinn. Denn wenn die Voraussetzung falsch ist, hat die Implikation keine Bedeutung. Doch wir haben Glück: Das stört in der Mathematik tatsächlich nicht. Denn der Mathematiker benötigt ja nur die Wahrheit seiner Implikationen, nicht die Bedeutung. Und wahr ist die Implikation ja auf jeden Fall: wenn die Voraussetzung falsch ist, ist jede Folgerung daraus wahr, wie wir oben gesehen haben. Ist sie aber wahr, so treffen die logischen Argumente zu und die Implikation ist wieder wahr.
Wir dürfen uns also auch im Widerspruchsbeweis der Wahrheit unserer Implikationen sicher sein. Am Ende, wenn man den Widerspruch zu irgendeiner Voraussetzung erreicht hat, wissen wir also, daß die Implikation *[Voraussetzungen] ⇒ [Widerspruch zu einer Voraussetzung]* wahr ist. Gilt aber nun das Prinzip das ausgeschlossenen Dritten, so müssen die Voraussetzungen schon falsch gewesen sein. Nur dann kann die Implikation wahr sein. Damit das Prinzip aber gilt, muß das Axiomensystem widerspruchsfrei sein!
Also, was sehen wir hier ganz deutlich: **Ein Widerspruchsbeweis setzt die Widerspruchsfreiheit des Axiomensystems voraus!** Streng genommen, sind daher Widerspruchsbeweise in der Analysis keine echten Beweise! In der Zahlentheorie dagegen kann man sie guten Gewissens benutzen. Widerspruchsbeweise haben noch einen weiteren Nachteil. Sie tragen nicht zum Verständnis der Materie bei. Man kann durch sie oft keine Ursachen sehen. Sie sind in keinster Weise konstruktiv.
Beispiel: Man soll zeigen, daß es unendlich viele Primzahlen gibt. Dafür nimmt man an, es gebe nur endlich viele: $p_1, ..., p_n$. Dann betrachtet man $p := \prod_{i=1}^{n} p_i + 1$. Alle p_i teilen p nicht, also muß p selbst Primzahl sein. Widerspruch!
Wir wissen jetzt, daß es zu jedem M eine Primzahl p gibt mit $p > M$. Aber konstruieren können wir keine. Denn die Konstruktion im Beweis setzte etwas Falsches voraus, sie klappt in Wirklichkeit nicht. Man kennt bis heute keine Konstruktion, die nur Primzahlen erzeugt.
Der Widerspruch muß nicht unbedingt direkt zu der Aussage, die man beweisen will, auftreten. Es kann auch passieren, daß man bei irgendeinem Beweis der Analysis auf den Widerspruch $8 > 13$ kommt. Das ist so in einer Übung zur Analysis im Grundstudium passiert. Man achte darauf, daß auch die Grundaxiome immer zu den Voraussetzungen zählen, zu denen ein Widerspruch erreicht werden kann.
Eine offene Frage ist noch, ob man alle Sätze der Mathematik auch ohne Widerspruchsbeweise zeigen kann. Ich denke ja nicht, daß das geht, aber logische Gründe dafür kann ich nicht angeben. Es gibt nur ein Beispiel, das diese Mythologie rechtfertigen könnte:
Beispiel: Der obige Beweis, daß es unendlich viele Primzahlen gibt, geht nur per Widerspruch. Da bis heute keine Konstruktion von Primzahlen bekannt ist, ist dies vielleicht ein Beispiel für einen Satz, der ohne Widerspruch nicht bewiesen werden kann. Um ein Gefühl dafür zu bekommen: Außer X gibt es kein Polynom P in $\mathbb{Z}[X]$, für das $P(\mathbb{P}) \subset \mathbb{P}$, wobei $\mathbb{P}$ die Menge der Primzahlen sein soll.
Zum Schluß möchte ich vor einer zu häufigen Anwendung des Widerspruchs warnen. Ich weiß selbst, daß man am liebsten gleich die Widerspruchsannahme aufs Blatt schreibt (dann steht ja wenigstens schon etwas darauf). Aber nach meiner Erfahrung ist dieser Schritt in 70% der Fälle unnötig. Die Widerspruchsannahme steht dann zwar da, und am Schluß auch der Widerspruch dazu, aber zwi-

schendrin wird die Annahme nicht mehr benutzt. Der Beweis wurde also direkt geführt und nur als Widerspruchsbeweis getarnt. So etwas sollte vermieden werden. Es ist auch sonst besser, wenn es möglich ist, einen Beweis direkt (und konstruktiv) zu führen. Allein schon deshalb, weil man dann besser sieht, was eigentlich passiert.

3.4 Konstruktion
I am me, so I exist

Der konstruktive Beweis ist das genaue Gegenteil zum Widerspruchsbeweis. Hier wird das Objekt mit den gewünschten Eigenschaften einfach konstruiert. Das hat viele Vorteile: man weiß, was mathematisch passiert und man hat eine konkrete Beschreibung, die meist zum Rechnen gut geeignet ist.
Was passiert bei einer Konstruktion? Meistens ist es so, daß man sich bekannte Objekte nimmt, sie zu irgendeiner Menge zusammenfaßt, dieser Menge eine Struktur zuweist und das muß es dann tun. Wir sehen also drei problematische Punkte:
Erstens: Eine Konstruktion setzt die Existenz anderer Objekte voraus. Wenn diese Objekte nicht konstruiert wurden, sondern ihre Existenz nur per Widerspruch gezeigt wurde, dann sieht man der Konstruktion auch jetzt nicht vollständig an, was passiert.
Zweitens: Bei der Zusammenfassung zu einer Menge ist darauf zu achten, daß es auch wirklich eine Menge wird. Das klingt trivial, ist es aber nicht. Zum Beispiel ist $R := \{r | r \notin r\}$ keine Menge. Denn wäre dann $R \in R$, so wäre nach Definition $R \notin R$. Wäre aber umgekehrt $R \notin R$, so wäre nach Defintion $R \in R$. Die Annahme, R sei etwas, was eine Elementbeziehung zu etwas haben kann (eine Menge), führt also zum Widerspruch. Konstruiert man sich irgendeine Klasse, so muß man streng genommen nachprüfen, ob diese Klasse eine Menge ist. Zu dieser Nachprüfung stehen natürlich allgemeine Mengenaxiome zur Verfügung. Man weiß übrigens auch bei den Mengenaxiomen noch nicht, ob sie widerspruchsfrei sind. In den ersten 70 Jahren der Mengentheorie mußten die Axiomatisierungen immer wieder geändert werden, weil Widersprüche auftraten. In den letzten 30 Jahren hat man keine mehr gefunden.
Drittens: Die Zuweisung einer Struktur benutzt natürlich die Existenz anderer Strukturen. Das sollte man deutlich hervorheben. Oftmals wird diese *andere* Struktur vertuscht. Ein Beispiel zur Verdeutlichung:
Beispiel: Sei R ein Ring. Zu jeder Menge I existiert eine freier R-Modul, der I als Basis hat. Konstruktion: Sei $F := \bigcup_{i=0}^{\infty} (R \times I)^i$, *wobei* $(R \times I)^0 = \{0\}$ *sein soll. Eine Skalarmultiplikation sei eingeführt durch*

$$r \bullet ((r_1, i_1), (r_2, i_2), ..., (r_n, i_n)) := ((r \cdot r_1, i_1), (r \cdot r_2, i_2), ..., (r \cdot r_n, i_n))$$

Eine Addition auf F führt man ein durch

$$((r_1, i_1), ...(r_n, i_n)) \oplus ((s_1, j_1), ..., (s_m, j_m)) := ((r_1, i_1), ..., (r_n, i_n), (s_1, j_1), ..., (s_m, j_m))$$

Dann ist F ein freier Modul. B sei der von allen Elementen $(h \oplus f \oplus g) \ominus (h \oplus g \oplus f), (r_1 \bullet f \oplus r_2 \bullet f) \ominus (r_1 + r_2) \bullet f$ *erzeugte Untermodul. Dann ist* $M := F/B$ *der gesuchte freie Modul. Man beachte die Unterscheidung der Addition im Ring R und im Modul F.*

3.5 ε und Diagonalfolge
A puzzle of know-how

Über das ε wissen wir ja schon, daß es immer größer als Null ist. Aber das ε ist nicht irgendeine positive reelle Zahl, nein, das ε ist die wichtigste Erfindung der Analysis. (Manche behaupten ja, die Griechen hätten das ε schon lange vor den Mathematikern verwendet. Aber das glaube ich eigentlich nicht.) Das Entscheidende am ε ist, daß es beliebig klein werden kann. Dieses Rezept „Zu jedem ε existiert...“ ist seit seiner Erfindung im 19. Jahrhundert bis heute ungeschlagen. Auch heutige Analytiker, die längst die höheren Weihen der Funktionalanalysis und der Potentialtheorie

erlangt haben, beginnen ihre Beweise immer wieder mit „Sei $\varepsilon > 0$“. (Wenn sie dies einmal nicht tun, dann nur dann, weil sie Stetigkeit oder ähnliches einfach einmal glauben, nicht aber, weil sie es hätten anders beweisen können.) Die einzige Schwierigkeit ist eigentlich, daß das zugehörige δ bei der Stetigkeit gewählt werden muß, bevor man weiß, wie es auszusehen hätte. Oftmals kann man aber einfach so tun, als ob man das δ schon hätte und dann daraus eine explizite Bedingung für δ herleiten.

Das ist übrigens auch immer wieder ein Erfolgsrezept der Mathematik: Wenn man ein Problem hat, tut man erst mal so, als ob es gelöst wäre. Dann ergeben sich manchmal wie von selbst Bedingungen für die Lösung, aus denen man dann ersehen kann, wann eine Lösung existiert oder wie sie aussieht.

Ein anderes Erfolgsrezept der Analysis ist die „Diagonalfolge“. Die Situation ist die, daß man $(a_{nk})_{nk}$ hat, die sowohl im ersten Index als auch im zweiten konvergieren. Dann könnte man oft ganz gut gebrauchen, daß auch die Diagonalfolge $(a_{nn})_n$ konvergiert. Manchmal reicht auch eine Abwandlung davon (daß $(a_{n,N(n)}$ konvergiert).
Beispiel: Man hat einen metrischen Raum M und definiert seinen Abschluß

$$\overline{M} := \{a | a = \lim_{n\to\infty} a_n, a_n \in M\}$$

Dann gilt:

$$\overline{\overline{M}} = \overline{M}$$

Zum Beweis nehme man sich eine Folge $(a_n)_n$ in $\overline{M}$ mit Grenzwert a. Dann existieren Folgen $(a_{ni})_i$ in M, die gegen a_n konvergieren. Nun existieren zu i $N(i)$ und N_i, so daß

$$|a - a_j| < \frac{1}{2i}, |a_i - a_{ij}| < \frac{1}{2i}$$

für $j > N(i)$ im ersten Fall und $j > N_i$ im zweiten Fall. Man fordert nun $j_i > max\{N(i), N_i, j_{i-1}\}$. Dann ist für alle $k > j_i$:

$$|a - a_{k,j_k}| \leq |a - a_k| + |a_k - a_{k,j_k}| < \frac{1}{2i} + \frac{1}{2i} = \frac{1}{i}$$

Also ist a Grenzwert der Folge (a_{k,j_k}) und daher schon in $\overline{M}$.
Ein anderes Beispiel - das wahrscheinlich jeder kennt - benutzt direkt eine Diagonalfolge:
Beispiel: $\mathbb{R}$ ist überabzählbar.
Wir nehmen an, $\mathbb{R}$ wäre abzählbar: $\mathbb{R} = \{c_i | i \in \mathbb{N}\}$. Die c_i stellen wir als Dezimalzahl dar und nennen c_{ij} die j-te Dezimalstelle von c_i nach dem Komma. Nun konstruieren wir folgende Zahl d: Es reicht aus, die Dezimalstellen d_i zu definieren. Dann ist auch d eindeutig gegeben. Wir setzen $d_i = 2$, wenn $c_{ii} \neq 2$ und $d_i = 7$, wenn $c_{ii} = 2$. Wäre nun $d \in \mathbb{R}$, so müßte es ein i geben, sodaß $d = c_i$. Dann ist aber insbesondere $d_i = c_{ii}$, was aber nach Konstruktion unmöglich ist.

3.6 Idee
Art of Mathematics

Bei allen Tips, Rezepten und Methoden, die ich hier weitergeben kann, muß ich doch gestehen, daß die Intuition eine wichtige Rolle in der Mathematik spielt. Man kann eben nicht immer sagen, wie man auf dies und das kam, man weiß es manchmal selbst nicht. Irgendwann nachts hatte man die Idee eben. Das ist der Teil der Mathematik, den man Kunst nennen könnte. Man kann aber lernen, ein Gefühl für die Objekte zu bekommen. Dazu ist es sehr nützlich, sich die pathologischen Fälle einer Theorie anzuschauen: eine nicht-meßbare Menge, eine nicht-integrierbare Funktion, die überall beschränkt bleibt, eine überall stetige, aber nirgends differenzierbare Funktion, ... Diese Intuition schärft sich mit den Jahren. Ich habe schon einige FĎlle erlebt, wo Studenten Fragen gestellt haben, die auch der Professor nicht sofort beantworten konnte. Hat er aber gewagt, eine Vermutung dazu zu Ďuáern, so stellte sich spĎter oft heraus, daá er richtig lag, oft auch im Widerspruch zu dem von Studenten erwarteten Ergebnis. Ich denke, es gibt tatsächlich eine „Erfahrung“ in der

Mathematik, die einem intuitiv die richtige Richtung weist. Und sie ist um so zuverlässiger, je länger man Mathematik macht.

Mein Schlußwort muß daher lauten: Beweist, sucht Beispiele, macht einfach Mathematik und findet dabei die Intuition und den Spaß, der Mathematik so faszinierend macht.