Vorkurs Mathematik: Logik und Beweis

Andreas Knauf*

Wintersemester 2013/14

Zusammenfassung

Dieser Text beinhaltet unter anderem Kapitel 2.4 (Aussagen) meines Analysis-I-Skripts und lehnt sich teilweise an Kapitel 3 von Schichl und Steinbauer [SchSt] an. Ein weiterführender Text zur Logik ist Hoffmann [Ho].

Inhaltsverzeichnis

*Department Mathematik, Universität Erlangen-Nürnberg, Cauerstr. 11, 91 058 Erlangen, Raum 02.321, e-mail: knauf@math.fau.de, web: http://math.fau.de/knauf

Warum stellen wir vor das Mathematikstudium den Vorkurs, und warum beginnen wir mit Logik? Zunächst, hier wird es nicht darum gehen, Schulstoff zu wiederholen. Wir werden statt dessen, oberflächlich gesehen, im gesamten ersten Semester in der 'Analysis' fast nur Themen bringen, die in irgendeiner Form schon in der Schule behandelt wurden.

Die Universitätsmathematik unterscheidet sich aber darin von dem, was Sie gewohnt sind, dass im Idealfall jede Aussage bewiesen wird. Wo soll man da anfangen, wenn nicht mit der Logik?

In Wirklichkeit ist dieses Argument nicht ganz so zwingend. Die meisten MathematikerInnen würden wohl eher in der Mengenlehre als in der Logik die Basis ihrer Disziplin sehen[1]. Zwar ist die Logik eine Teildisziplin der Mathematik, in der aktiv geforscht wird. Aber man muss sich nicht viel intensiver als im Rahmen des Vorkurses mit ihr beschäftigen, um in anderen Bereichen der Mathematik erfolgreich tätig zu werden.

Eigentlich fangen wir mit dem Vorkurs damit an, das folgerichtige Argumentieren und Aufschreiben von Beweisen zu üben. Das ist eine Aufgabe für das ganze erste Semester und erfordert eben auch elementare Logikkenntnisse.

Ein gutes Buch zum Einüben dieser Techniken ist das von Schichl und Steinbauer [SchSt]. Das habe ich auch auf meiner *website* zu diesem Vorkurs verlinkt. Sie können es von der Uni aus herunterladen.

1 Aussagen und Junktoren

1.1 Eine oder mehrere Logiken?

Für unsere Zwecke ist eine *Aussage* A ein Element der zweielementigen Menge $\{$wahr, falsch$\}$ und eine *Aussageform* oder *Prädikat* eine Abbildung

$$A : M \to \{\text{wahr, falsch}\}$$

einer (oft nicht explizit angegebenen) Menge M in diese zweielementige Menge.

1.1 Beispiele 1. "6 ist eine Primzahl" ist eine Aussage und zwar eine falsche.

2. $A : \mathbb{N} \to \{\text{wahr, falsch}\} \quad , \quad A(x) := \begin{cases} \text{wahr} & , \ x \text{ ist Primzahl} \\ \text{falsch} & , \ x \text{ ist nicht Primzahl.} \end{cases}$

[1] Die Mengenlehre ist nebenbei auch sparsamer und fußt auf nur einem Objekt, der *leeren Menge*, während die Logik ja auf der Unterscheidung zwischen den zwei Objekten *wahr* und *falsch* aufbaut...

A ist eine Aussageform, die die Menge $\mathbb{N} = \{1, 2, 3, \ldots\}$ der natürlichen Zahlen auf die Menge {wahr, falsch} abbildet. Also ist etwa $A(1) =$ falsch und $A(11) =$ wahr. $\diamond$

1.2 Bemerkung (mehrwertige Logiken) Dass Aussagen nur wahr oder falsch sein können, ist — wie alles in der Mathematik — eine Festlegung. Es gibt auch Logiken, bei denen neben diesen Alternativen der Wahrheitswert 'unbekannt' vorkommt. Die auf einer solchen dreiwertigen Logik aufbauende *Intuitionistische Mathematik* wurde vor etwa hundert Jahren vom Mathematiker Luitzen Brouwer begründet. In ihr kann man aber viel weniger beweisen als in der 'üblichen', auf der zweiwertigen Logik basierenden Mathematik. Wohl deshalb wird sie heute nur von wenigen Mathematikern verwendet.

Dagegen ist die *Quantenlogik* praktisch wichtig. Wie der Name schon sagt, beschreibt sie die Struktur der Quantenphysik. Statt zwei oder drei benutzt sie unendlich viele Werte. Man kann sich das etwa so vorstellen:

Bei der Messung des Spins eines Elektrons legt man ein inhomogenes Magnetfeld an. Dessen Nordpol zeigt in eine Richtung, zum Beispiel nach oben. Zwar ergibt jede Messung nur eins von zwei Resultaten, nämlich entweder 'Spin in Richtung des Nordpols', entsprechend 'wahr', oder 'in Richtung des Südpols', entsprechend 'falsch'. Für die Beschreibung einer solchen Einzelmessung reicht also die klassische zweiwertige Logik aus.

Aber die gleiche Alternative ergibt sich für jede Magnetfeldausrichtung, also jeden Punkt auf der Kugeloberfläche, die diese Richtungen parametrisiert. Die Kugeloberfläche parametrisiert damit die in diesem Experiment möglichen Wahrheitswerte. $\diamond$

1.2 Junktoren

Sind A, B zwei Aussagen, so lassen sich mittels der *Junktoren* (d.h. 'Verbinder') neue Aussagen herstellen. Wichtige Beispiele von Junktoren sind:

Junktor	Bedeutung	Zeichen
Negation	nicht A	$\neg A$
Konjunktion	A und B	$A \wedge B$
Disjunktion	A oder B	$A \vee B$
Implikation	wenn A, dann B	$A \Rightarrow B$
Äquivalenz	A genau dann, wenn B	$A \Leftrightarrow B$

Die Wahrheitswerte der so zusammengesetzten Aussagen sind durch die folgende Tabelle festgelegt. (Eine Tabelle dieser Art heißt *Wahrheitstabelle* oder *Wahrheitstafel*). Wir schreiben kurz w statt 'wahr' und f statt 'falsch'.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

Die Negation wird *einstellig* genannt, weil sie aus einer Einzelaussage eine neue Aussage formt. Die anderen aufgelisteten Junktoren[2] sind *zweistellig*, weil sie zwei Einzelaussagen verknüpfen.

Es gibt auch drei-, vier- und für jede natürliche Zahl n sogar n-stellige Junktoren. Dabei ist es gar kein Problem, dass man für diese nicht wie bei der Negation das Symbol vor die Einzelaussage oder für die zweistelligen Junktoren zwischen die beiden Aussagen schreiben kann. Denn statt $A \wedge B$ könnte man ja etwa $\bigwedge(A, B)$ oder einfach $\mathrm{and}(A, B)$ schreiben, und so eine Klammernotation lässt sich auf beliebig viele Argumente erweitern.

1.3 Aufgabe Wie viele einstellige und wie viele zweistellige Junktoren kann man definieren? Wie viele n-stellige? ◇

Bis jetzt kennen wir nur vier der 16 zweistelligen Junktoren. Zwei weitere spielen noch eine wichtige praktische Rolle: xor und nand. Sie haben die folgenden Wahrheitstafeln:

A	B	$A \,\mathrm{xor}\, B$	$A \,\mathrm{nand}\, B$
w	w	f	f
w	f	w	w
f	w	w	w
f	f	f	w

Umgangssprachlich wird xor mit "entweder - oder" umschrieben. Es ist nur wahr, wenn genau eine der Aussagen A, B wahr ist. Es unterscheidet sich darin vom nicht exklusiven 'oder', denn $A \vee B$ ist auch dann wahr, wenn A und B gleichzeitig wahr sind.

Der Junktor nand entspricht dem "nicht beide". Es ist also nur wahr, wenn mindestens eine der Aussagen A, B falsch ist. Wie der Name nand (not and) schon sagt, ist er die Verneinung der 'und'-Verknüpfung. Es gilt also $A \,\mathrm{nand}\, B = \neg(A \wedge B)$, unabhängig davon ob die Aussagen A und B wahr oder falsch sind.

Wenn Sie aufgepasst haben, haben Sie festgestellt, dass auf der rechten Seite der Gleichung zum ersten Mal zwei Junktoren miteinander verknüpft wurden. Hier ist Klammersetzung wichtig. Sie besagt, dass die Auswertung des Klammerinhalt Vorrang vor anderen Junktoren (wie hier $\neg$) hat.

[2] Die Implikation und die Äquivalenz werden morgen genauer besprochen werden.

1.4 Aufgabe Welche Wahrheitstafel hätte der Ausdruck $\neg A \wedge B$, also ohne Klammer? $\diamond$

Die Verknüpfung von Junktoren in komplizierteren Ausdrücken kommt in der Mathematik dauernd vor. Bei den einstelligen Operatoren kommt man damit nicht weit. Man notiert immerhin die elementare Tatsache, dass doppelte Verneinung die ursprüngliche Aussage liefert, also immer $\neg\neg A = A$ gilt.

Bei den zweistelligen Junktoren passiert etwas Neues. Man kann mit zwei von ihnen einen dreistelligen Junktor bauen.

1.5 Beispiel ('und'-Verknüpfung dreier Aussagen A, B, C)

$$\bigwedge(A, B, C) := (A \wedge B) \wedge C = A \wedge (B \wedge C).$$

Diese Aussage $\bigwedge(A, B, C)$ ist genau dann wahr, wenn alle drei Aussagen A, B und C wahr sind. Hier sehen sie ein Gleichheitszeichen mit einem Doppelpunkt. Was links von diesem Definitionszeichen steht, wird durch das, was rechts steht, definiert. Das zweite Gleichheitszeichen kommt ohne Doppelpunkt. Hier wird also nichts definiert, sondern nur Gleichheit der beiden Seiten festgestellt. In diesem Fall kommt es also auf die Klammerung nicht an, weshalb man sie hier auch weglassen könnte. $\diamond$

Tatsächlich kann man jeden Junktor als eine geeignete Verknüpfung von Negation, 'und' und 'oder' darstellen.

1.6 Beispiel (Äquivalenz) Es gilt immer $A \Leftrightarrow B \;=\; (A \wedge B) \vee \neg(A \vee B)$, denn das ergibt sich aus folgender Wahrheitstafel:

A	B	$A \wedge B$	$\neg(A \vee B)$	$(A \wedge B) \vee \neg(A \vee B)$	$A \Leftrightarrow B$
w	w	w	f	w	w
w	f	f	f	f	f
f	w	f	f	f	f
f	f	f	w	w	w

Diese Darstellung der Äquivalenz ist sicher nicht eindeutig.

1.3 Disjunktive und konjunktive Normalform

Wie können wir uns davon überzeugen, dass es immer so eine Darstellung gibt, wir also mit den drei Junktoren auskommen?

Dazu gibt es den Algorithmus der *disjunktiven Normalform*.

Gegeben sei ein n-stelliger Quantor, also eine Abbildung

$$q : \{w, f\}^n \to \{w, f\}.$$

Die Menge $\{w, f\}^n$ besteht dabei aus allen Zeichenketten der Länge n, gebildet aus den Symbolen w und f. Etwa für die Äquivalenz wäre also $n = 2$ und

$$q(w,w) = q(f,f) = w \quad , \quad q(w,f) = q(f,w) = f.$$

Wir stellen q in Form einer Wahrheitstafel mit 2^n Zeilen und $n+1$ Spalten dar. Dabei sind in den ersten n Spalten die n Aussagen eingetragen, die in der $n+1$-ten Spalte als Argument der Funktion q benutzt werden.

1. Jetzt werden alle Zeilen gestrichen, bei denen f als Wert von q auftaucht.

2. Die Variablen A_i, die in dieser Zeile den Wert f annehmen, werden zu $\neg A_i$ negiert, die anderen Variablen belassen, und alle so entstehenden Variablen durch $\wedge$ (also 'und') verknüpft.

3. Diese den Zeilen zugeordneten Ausdrücke werden geklammert und mit $\vee$ (also 'oder') verknüpft.

1.7 Beispiel (disjunktive Normalform) $A \Leftrightarrow B \;=\; (A \wedge B) \vee (\neg A \wedge \neg B)$. Ausgesprochen kann diese Identität so: Die Äquivalenz von A und B bedeutet, dass A und B beide wahr oder beide falsch sind. $\diamond$

Die *konjunktive Normalform* ist umgekehrt eine 'und'-Verknüpfung von 'oder'-Ausdrücken. Letzere entsprechen die Zeilen der Wahrheitstabelle, die das Ergebnis 'falsch' liefern. Es wird also vor die Variablen, die in der Zeile den Wert w annehmen, das Negationszeichen geschrieben.

1.8 Beispiel (konjunktive Normalform der Äquivalenz) Wir streichen aus der Wahrheitstafel von $\Leftrightarrow$ die den Wert w ergebenden Zeilen:

A	B	$A \Leftrightarrow B$	$\neg A \vee B$	$A \vee \neg B$
w	f	f	f	w
f	w	f	w	f

Es ergibt sich also die Formel

$$A \Leftrightarrow B \;=\; (\neg A \vee B) \wedge (A \vee \neg B). \qquad \diamond$$

Die disjunktive Normalform eines n-stelligen Quantors verknüpft im schlimmsten Fall 2^n Klammern (nämlich für die *Tautologie* q, die nur den Wert 'wahr' annimmt). Analoges gilt für die konjunktive Normalform. Im Einzelfall kann eine wesentlich kürzere Darstellung des Quantors durch Umformung erreicht werden. Solche Verfahren sind wichtig beim Design von Schaltkreisen (und sie werden unter dem Stichwort 'Logiksynthese' beschrieben).

1.4 Rechenregeln für Junktoren

Dafür dienen die folgenden Regeln, von denen wir die erste schon gesehen haben.

Doppelnegationsgesetz: $\neg(\neg A) = A$

Kommutativgesetze: $A \wedge B = B \wedge A \quad , \quad A \vee B = B \vee A$

Assoziativgesetze: $(A \wedge B) \wedge C = A \wedge (B \wedge C) \quad , \quad (A \vee B) \vee C = A \vee (B \vee C)$

Distributivgesetze: $(A \wedge B) \vee C = (A \vee C) \wedge (B \vee C)$
$(A \vee B) \wedge C = (A \wedge C) \vee (B \wedge C)$

Verschmelzungsgesetze: $A \wedge (A \vee B) = A \quad , \quad A \vee (A \wedge B) = A$

Idempotenzgesetze: $A \wedge A = A \quad , \quad A \vee A = A$

Neutralitätsgesetze: $A \wedge w = A \quad , \quad A \vee f = A$

Absorptionsgesetze: $A \wedge f = f \quad , \quad A \vee w = w$

Komplementaritätsgesetze: $A \wedge \neg A = f \quad , \quad A \vee \neg A = w$

De Morgansche Gesetze: $\neg(A \wedge B) = (\neg A) \vee (\neg B)$,
$\neg(A \vee B) = (\neg A) \wedge (\neg B)$

All' diese Regeln kann man mit Wahrheitstafeln verifizieren (d.h. beweisen).

1.9 Aufgabe Beweisen Sie eine der Regeln durch Verwendung der disjunktiven Normalform, eine weitere mit der konjunktiven Normalform.
Beispiel (Erstes de Morgansches Gesetz und disjunktive Normalform):

$$\neg(A \wedge B) = (A \wedge \neg B) \vee (\neg A \wedge B) \vee (\neg A \wedge \neg B) = (\neg A) \vee (\neg B). \qquad \diamond$$

Die de Morgan-Gesetze zeigen, dass man statt mit dem Tripel von Junktoren $\neg, \wedge, \vee$ auch mit dem Paar $\neg, \wedge$ oder dem Paar $\neg, \vee$ auskommt. Denn es gilt ja

$$A \wedge B \;=\; \neg\big((\neg A) \vee (\neg B)\big) \quad \text{und} \quad A \vee B \;=\; \neg\big((\neg A) \wedge (\neg B)\big).$$

Man kann also 'und' bzw. 'oder' ersetzen.

1.10 Aufgabe (nand) Zeigen Sie, dass sich allein mit dem Junktor nand alle Junktoren bilden lassen (daher seine Bedeutung in der Schaltkreistechnik). $\diamond$

1.11 Bemerkung (Logik, Elektrotechnik und Informatik) In elektrischen Schaltkreisen können logische Operationen realisiert werden. Interpretiert man etwa 'wahr/falsch' als 'Strom fließt/ fließt nicht', dann ermöglicht ein geschlossener Schalter das Fließen des Stroms, kann also selbst mit 'w' identifiziert werden.

In diesem Sinn ist dann die Reihenschaltung zweier Schalter ihre Verknüpfung durch 'und', während die Parallelschaltung der 'oder'-Verknüpfung entspricht.

Eine zweite Identifikation ist die von 'w' mit der Zahl 1, und von 'f' mit der 0. Dann wird man die Menge $\{0, 1\}$ möglicher Wahrheitswerte ein *Bit* nennen. Die Negation entspricht der Veränderung des Bitwerts, die 'und'-Verknüpfung der Bildung des Minimums bzw. der Multiplikation, 'oder' der des Maximums:

$$1 \wedge 1 = 1,\ 1 \wedge 0 = 0 \wedge 1 = 0 \wedge 0 = 0 \quad , \quad 0 \vee 0 = 0,\ 1 \vee 0 = 0 \vee 1 = 1 \vee 1 = 1.$$

xor entspricht der Addition modulo 2, geschrieben mit einem Pluszeichen im Kreis:

$$0 \oplus 0 = 0 \quad , \quad 1 \oplus 0 = 0 \oplus 1 = 1 \quad , \quad 1 \oplus 1 = 0. \qquad \diamond$$

2 Quantoren

Bisher haben wir die *Aussagenlogik* betrachtet. Jetzt wenden wir uns der *Prädikatenlogik* zu.

2.1 Existenz- und Allquantor

Aus Aussageformen $A : M \to \{\text{wahr, falsch}\}$ kann man durch die so genannten *Quantoren* "für alle", abgekürzt mit $\wedge$ oder $\forall$, und "es existiert", abgekürzt mit $\vee$ oder $\exists$, Aussagen machen:

$$\big(\forall x \in M : A(x)\big) \quad := \quad \begin{cases} \text{wahr} & , \ \text{falsch} \notin A(M) \\ \text{falsch} & , \ \text{falsch} \in A(M) \end{cases}$$

$$\big(\exists x \in M : A(x)\big) \quad := \quad \begin{cases} \text{wahr} & , \ \text{wahr} \in A(M) \\ \text{falsch} & , \ \text{wahr} \notin A(M) \end{cases} .$$

2.1 Beispiel Für die eingangs erwähnte Aussageform[3]

$$A : \mathbb{N} \to \{\text{wahr, falsch}\} \quad , \quad A(n) := \begin{cases} \text{wahr} & , \ n \text{ ist Primzahl} \\ \text{falsch} & , \ n \text{ ist nicht Primzahl} \end{cases}$$

[3] In Formeln und Definitionen kann man beliebige Variablennamen verwenden. Hier habe ich teilweise x durch n ersetzt. *Innerhalb* einer Formel muss man natürlich bei der jeweiligen Bezeichnung bleiben.

gilt: $\big(\forall x \in \mathbb{N} : A(x)\big) =$ falsch, aber $\big(\exists x \in \mathbb{N} : A(x)\big) =$ wahr, denn zwar ist nicht jede natürliche Zahl prim, aber es gibt Primzahlen. $\diamond$

Weitere gebräuchliche Quantoren sind $\nexists$ (*es gibt kein*) und $\exists!$ (*es gibt genau ein*).
Oft werde ich in der Vorlesung statt der Aussage $\forall x \in M : A(x)$ schreiben:

$$A(x) \qquad (x \in M),$$

und mit einer ähnlichen Schreibweise Abbildungen definieren.

2.2 Rechenregeln für Quantoren

Zum Beweis von Formeln der Prädikatenlogik sind Wahrheitstafeln nicht sehr nützlich. Stattdessen benutzt man Umformungsregeln. Es gilt

$$\big(\neg(\forall x \in M : A(x))\big) \;=\; \big(\exists x \in M : \neg A(x)\big)$$

oder kurz $\neg\forall = \exists\neg$, und umgekehrt: $\neg\exists = \forall\neg$.
In den folgenden Rechenregeln werden die Klammern und die Bezugnahme auf die Grundmenge M weggelassen.

2.2 Satz *Seien $P : M \to \{w, f\}$ und $Q : M \to \{w, f\}$ Aussageformen, sowie q eine Aussage. Dann gilt:*

1. $\neg\forall x : P(x) \;=\; \exists x : \neg P(x)$,
2. $\neg\exists x : P(x) \;=\; \forall x : \neg P(x)$,
3. $\exists x : P(x) \vee Q(x) \;=\; (\exists x : P(x)) \vee (\exists x : Q(x))$,
4. $\forall x : P(x) \wedge Q(x) \;=\; (\forall x : P(x)) \wedge (\forall x : Q(x))$,
5. $\forall x : q \vee P(x) \;=\; q \vee \forall x : P(x)$,
6. $\exists x : q \wedge P(x) \;=\; q \wedge \exists x : P(x)$,
7. $(\forall x : P(x)) \Longrightarrow q \;=\; \exists x : (P(x) \Longrightarrow q)$,
8. $(\exists x : P(x)) \Longrightarrow q \;=\; \forall x : (P(x) \Longrightarrow q)$,
9. $q \Longrightarrow \forall x : P(x) \;=\; \forall x : (q \Longrightarrow P(x))$,
10. $q \Longrightarrow \exists x : P(x) \;=\; \exists x : (q \Longrightarrow P(x))$.

Beweis: In Kapitel 3.2 von [SchSt] findet man Beweise von 3.) und 8.). $\square$

3 Mathematische Beweise

Mathematik ist eine menschliche Aktivität. Was die korrekte Formulierung einer Aussage, was die angemessene Form eines Beweises ist, unterliegt historischen Veränderungen. Etwa in der altägyptischen Mathematik wurden Gesetze eher nicht allgemein ausgesprochen, sondern durch Zahlenbeispiele belegt.

Sicherheit erhält man durch Zeichenumformungen nach formalen Regeln. Damit werden Beweise für den Computer zugänglich, aber für uns Menschen oft unlesbar und unverstehbar.

Sie werden im Lauf dieses Semesters lernen, korrekt und verständlich zu beweisen. Das ist eine komplexe Angelegenheit, bei der das Wichtigste das eigene klare Denken ist.

In diesem Kapitel werden einige gängige Beweistechniken vorgestellt.

3.1 Konstruktive und nicht konstruktive Beweise

In einem konstruktiven Beweis wird die Existenz eines Objektes gezeigt, indem eine Methode zu seiner Konstruktion angegeben wird. Dagegen wird in einem nicht konstruktiven Beweis nur seine Existenz gezeigt.

3.1 Beispiel (Konstruktive und nicht konstruktive Beweise) Ein konstruktiver Beweis der Behauptung, dass die Gerade $y = f(x) = 3x - 2$ im Intervall $(0, 1)$ (mindestens) eine Nullstelle x_0 besitzt, ist die Angabe $x_0 := 2/3$.

Ein nicht konstruktiver Beweis besteht aus den Feststellungen, dass

- $f(0) = -2 < 0 < 1 = f(1)$ ist, f also auf $[0, 1]$ sein Vorzeichen ändert,
- und dass die Funktion $f : \mathbb{R} \to \mathbb{R}$ stetig ist.

Nach dem Zwischenwertsatz der Analysis muss sie also in $(0, 1)$ mindestens einmal den Wert 0 annehmen. $\diamond$

Sieht man das Beispiel, ist man wohl geneigt, dem direkten Beweis den Vorzug zu geben. Denn er liefert mit der direkten Angabe der Lösung viel mehr Information. Andererseits gilt der indirekte Beweis für *alle* stetigen reellen Funktionen f mit $f(0) < 0 < f(1)$, ist also verallgemeinerbar. Das weiß man zu schätzen, wenn man etwa $f(x) = 2x^3 + 3x - 2$ betrachtet, mit der Nullstelle

$$\frac{\sqrt[3]{2+\sqrt{6}}}{2^{2/3}} - \frac{1}{\sqrt[3]{2\left(2+\sqrt{6}\right)}} \approx 0.553574.$$

Wenn auch in einer Klausur jeder richtige Beweis gleich viel zählt, gibt es doch in der Mathematik nützliche und weniger nützliche Beweise, schöne und weniger schöne. Einige besonders elegante Beweise sind in [AiZi] gesammelt.

3.2 Indirekte oder Widerspruchsbeweise

Sie kennen hoffentlich den Beweis der Irrationalität von $\sqrt{2}$. Dass es überhaupt eine reelle Zahl w im Intervall $(1, 2)$ gibt mit $w^2 = 2$, lässt sich analog der nichtkonstruktiven Version von Beispiel 3.1 zeigen, denn die reelle Funktion $f(x) := x^2 - 2$ ist stetig, mit $f(1) = -1 < 0 < 2 = f(2)$.

Dass w keine rationale Zahl ist, wird mit einem Widerspruchsbeweis gezeigt. Man nimmt also die zu widerlegende Aussage an und führt sie zu einem Widerspruch. Dieser Beweis stammt von Euklid und ist der erste bekannte Widerspruchsbeweis in der Geschichte der Mathematik.

3.2 Satz (Irrationalität von $\sqrt{2}$) *Es gibt keine Zahl $w \in \mathbb{Q}$ mit $w^2 = 2$.*

Beweis: Sei $w \in \mathbb{Q}$ mit $w^2 = 2$.

- Wir schreiben w in der Form $w = p/q$ mit teilerfremden ganzen Zahlen p, q.
- Es gilt also $p^2 = 2q^2$. 2 teilt also $p^2 = p \cdot p$. Da 2 eine Primzahl ist, muss sie einen der Faktoren im Produkt $p \cdot p$ teilen. Damit ist p gerade, $p = 2r$ für eine ganze Zahl r.
- Also ist $4r^2 = 2q^2$, also $2r^2 = q^2$. Eine Wiederholung des eben benutzten Arguments zeigt, dass q gerade ist.
- Damit sind p und q nicht teilerfremd, in Widerspruch zur Annahme. □

Ein weiteres bekanntes Beispiel ist der ebenfalls von Euklid stammende Beweis, dass es unendlich viele Primzahlen gibt.

> "'Reductio ad absurdum', die Euklid so sehr mochte, ist eine der schärfsten Waffen der Mathematiker. Es ist ein viel exquisiteres Gambit als jedes Gambit im Schach: Ein Schachspieler bietet vielleicht ein Bauernopfer oder sogar das Opfer einer Figur an, aber ein Mathematiker bietet *das Spiel* an." G. H. Hardy (1877-1947)

3.3 Aufgabe Als ganz einfaches Beispiel soll indirekt bewiesen werden, dass für jede natürliche Zahl n gilt: Wenn n^2 gerade ist, ist auch n gerade. ◇

3.3 Induktionsbeweise

Oft ist nicht nur die Wahrheit einer oder weniger Aussagen, sondern von unendlich vielen Aussagen zu beweisen, z.B. von einer Formel wie

$$1 + \ldots + n = \frac{n(n+1)}{2},$$

mit $n \in \mathbb{N}$ Summanden. Die zu beweisende k-te Aussage $A(k)$ ist hier also: Es gilt $1 + \ldots + k = \frac{k(k+1)}{2}$. Etwa $A(3)$ lautet: $1 + 2 + 3 = \frac{3 \cdot 4}{2}$.

Ziel ist es, zu zeigen, dass

$$\forall n \in \mathbb{N} : A(n) \tag{3.1}$$

gilt, also diese Aussage (nicht mehr: Aussageform) wahr ist.
Im Induktionsbeweis wird dazu zunächst im

Induktionsanfang $A(1)$ bewiesen, und dann,

Induktionsschritt , dass für alle $k \in \mathbb{N}$ die Implikation $A(k) \Rightarrow A(k+1)$ gilt. Dabei heißt $A(k)$ die *Induktionsannahme* und $A(k+1)$ die *Induktionsbehauptung*.

Damit folgt dann (3.1), also die Richtigkeit aller Aussagen $A(n)$.

In unserem Fall lautet $A(1)$: $1 = \frac{1 \cdot 2}{2}$, ist also wahr. Gilt nun $A(k)$, also $1 + \ldots + k = \frac{k(k+1)}{2}$, dann folgt $A(k+1)$, also $1 + \ldots + (k+1) = \frac{(k+1)(k+2)}{2}$. Denn

$$1+\ldots+(k+1) = (1+\ldots+k)+(k+1) = \frac{k(k+1)}{2}+(k+1) = \frac{(k+2)(k+1)}{2}.$$

3.4 Aufgabe Beweisen Sie für alle natürlichen Zahlen n die Formel

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}. \qquad \diamond$$

Wir werden den Induktionsbeweis in der Vorlesung ausführlich behandeln.

3.4 Mathematische Forschung

Mathematiker beweisen nicht nur Sätze, sie finden auch Vermutungen (englisch: conjectures), deren Plausibilität sie überprüft haben, und von denen sie glauben, dass es sich lohnt, sie zu beweisen. Spätestens bei Ihrer Master-Arbeit werden Sie das auch tun. Warum also nicht gleich damit anfangen?

Die Frage ist, wie man Satz 3.2 sinnvoll verallgemeinern kann. Man könnte etwa fragen, welche natürlichen Zahlen eine rationale Wurzel besitzen. Offensichtlich mindestens die, die selbst Quadrate natürlicher Zahlen sind, also 1,4,9,16 etc.

Ob eine natürliche Zahl n Quadratzahl ist oder nicht, stellt man fest, indem man eine natürlich Zahl m mit $m^2 \leq n < (m+1)^2$ findet. Wenn dann $m^2 < n$, kann n keine Quadratzahl sein, denn für natürliche Zahlen $m_1 < m_2$ ist auch $m_1^2 < m_2^2$. Das ist also auch bei großen Werten von n einfach.

Gibt es noch weitere Lösungen? Wenn wir uns Satz 3.2 genau anschauen, stellen wir zunächst fest, dass der Widerspruchsbeweis statt auf 2 auf jede Primzahl anwendbar ist. Diese haben also keine rationalen Wurzeln. Wie steht es mit Zahlen wie 6 oder 8, die weder Quadratzahlen noch prim sind?

Die Quadratwurzeln einer natürlichen Zahl k lassen sich als Nullstelle des quadratischen Polynoms x^2-k mit ganzzahligen Koeffizienten und Leitkoeffizient 1 auffassen. In diesem Sinn werden unsere bisherigen Ergebnisse durch folgenden, auf Gauss zurückgehenden Satz verallgemeinert.

3.5 Satz (Satz über rationale Nullstellen)

$$r(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$$

sei ein reelles Polynom mit ganzzahligen Koeffizienten $a_0, a_1, \ldots, a_{n-1}$*. Ist* x_0 *eine rationale Nullstelle von* r *(also* $x_0 \in \mathbb{Q}$ *und* $r(x_0) = 0$*), dann ist* x_0 *ganzzahlig.*

Beweis: Die Behauptung stimmt sicher für $n = 0$, denn dann hat r keine Nullstelle. Sei also $n \in \mathbb{N}$. Wir setzen $x_0 = p/q$ (mit p, q teilerfremd) ein und erhalten

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + a_{n-2}\left(\frac{p}{q}\right)^{n-2} + \ldots + a_1\frac{p}{q} + a_0 = 0.$$

Jetzt erweitern wie mit q^n und bringen den q-unabhängigen Term auf die rechte Seite:

$$a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1pq^{n-1} + a_0q^n = -p^n.$$

Auf der linken Seite klammern wir den Faktor q aus:

$$q\big(a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + \ldots + a_1pq^{n-2} + a_0q^{n-1}\big) = -p^n.$$

Da p, q teilerfremd sind und die Klammer ganzzahlig ist, gilt $q = \pm 1$. □

Wir haben also viel mehr gezeigt, als dass jede rationale Wurzel einer natürlichen Zahl ganzzahlig ist.

3.6 Aufgabe Für die Fälle $k = 1$ und $k = 2$ kennen wir schon Formeln für $1^k + 2^k + \ldots + n^k$. Können wir solche Formeln auch für $k = 3$ oder sogar für beliebige $k \in \mathbb{N}$ finden? Letzteres ist nicht einfach. Zumindest können wir erwarten, dass das Ergebnis ein Polynom in n vom Grad $k+1$ und Leitkoeffizient $1/(k+1)$ ist, es also mit $\frac{n^{k+1}}{k+1}$ beginnt (warum?). ◇

4 G. Polya: Wie sucht man die Lösung?

1. **Verstehen der Aufgabe**

    - *Was ist unbekannt? Was ist gegeben? Wie lautet die Bedingung?*
    - Ist es möglich, die Bedingung zu befriedigen? Ist die Bedingung ausreichend, um die Unbekannte zu bestimmen? Oder ist sie unzureichend? Oder überbestimmt? Oder kontradiktorisch?
    - Zeichne eine Figur! Führe eine passende Bezeichnung ein!
    - Trenne die verschiedenen Teile der Bedingung! Kannst Du sie hinschreiben?

2. **Ausdenken eines Plans**

    - Hast Du die Aufgabe schon früher gesehen? Oder hast Du dieselbe Aufgabe in einer wenig verschiedenen Form gesehen?
    - *Kennst Du eine verwandte Aufgabe?* Kennst Du einen Lehrsatz, der förderlich sein könnte?
    - *Betrachte die Unbekannte!* Und versuche, Dich auf eine Dir bekannte Aufgabe zu besinnen, die dieselbe oder eine ähnliche Unbekannte hat.
    - *Hier ist eine Aufgabe, die der Deinen verwandt und schon gelöst ist. Kannst Du sie gebrauchen?* Kannst Du ihr Resultat verwenden? Kannst Du ihre Methode verwenden? Würdest Du irgendein Hilfselement einführen, damit Du sie verwenden kannst?
    - Kannst Du die Aufgabe anders ausdrücken? Kannst Du sie auf noch verschiedene Weise ausdrücken? Geh auf die Definition zurück!
    - Wenn Du die vorliegende Aufgabe nicht lösen kannst, so versuche, zuerst eine verwandte Aufgabe zu lösen. Kannst Du Dir eine zugänglichere verwandte Aufgabe denken? Eine allgemeinere Aufgabe? Eine speziellere Aufgabe? Eine analoge Aufgabe? Kannst Du einen Teil der Aufgabe lösen? Behalte nur einen Teil der Bedingung bei und lasse den anderen fort; wie weit ist die Unbekannte dann bestimmt, wie kann ich sie verändern? Kannst Du etwas Förderliches aus den Daten ableiten? Kannst Du Dir andere Daten denken, die geeignet sind, die Unbekannte zu bestimmen? Kannst Du die Unbekannte ändern oder die Daten oder, wenn nötig, beide, so dass die neue Unbekannte und die neuen Daten einander näher sind?
    - Hast Du alle Daten benutzt? Hast Du die ganze Bedingung benutzt? Hast Du alle wesentlichen Begriffe in Rechnung gezogen, die in der Aufgabe enthalten sind?

3. **Ausführen des Plans**

    - Wenn Du Deinen Plan der Lösung durchführst, so *kontrolliere jeden Schritt*. Kannst Du deutlich sehen, dass der Schritt richtig ist? Kannst Du beweisen, dass er richtig ist?

4. **Rückschau**

    - Kannst Du das *Resultat kontrollieren?* Kannst Du den Beweis kontrollieren?
    - Kannst Du das Resultat auf verschiedene Weise ableiten? Kannst Du es auf den ersten Blick sehen?
    - Kannst Du das Resultat oder die Methode für irgend eine andere Aufgabe gebrauchen?

Zitiert nach [Pol].

Literatur

[AiZi] M. Aigner, G. Ziegler: Das BUCH der Beweise. Springer, Berlin, 2002

[Ho] D. Hoffmann: Grenzen der Mathematik. Eine Reise durch die Kerngebiete der mathematischen Logik. Springer Spektrum, Berlin, 2013

[Pol] G. Polya: Schule des Denkens. Vom Lösen mathematischer Probleme. Francke Verlag, Tübingen, 1995

[SchSt] H. Schichl, R. Steinbauer: Einführung in das mathematische Arbeiten, Springer, Berlin, 2009