

Vorlesungsskript von *Einführung in das mathematische
Arbeiten*

Professor Karlheinz Gröchenig
Universität Wien
Fakultät für Mathematik

Wintersemester 2022/2023

0 Einleitung und Perspektive ¹

Man kann sich die gesamte Mathematik als ein Gedankengebäude vorstellen, das aus Aussagen besteht. Diese Aussagen bestehen aus anderen Grundaussagen die schon durch logische Schlussfolgerungen abgeleitet werden. Dieser Vorgang heißt **beweisen**. Gilt eine Aussage A als bewiesen, und kann man eine weitere Aussage B logisch aus A ableiten. Anders ausgedrückt kann man sich einen **Beweis** als eine Kette logischer Argumente vorstellen, die die Gültigkeit einer mathematischen Aussage sicherstellt. Das Beste ist, sich immer bei einem solcherart logischen Vorgang fragen: welche Teile von den Voraussetzungen berechtigt mich so was zu behaupten?

Ein Beispiel von einer mathematischen Aussage:

Das Quadrat einer geraden Zahl ist gerade

0.1 Mathematische Begriffe

Unterschiedliche mathematische Begriffe sind:

- **Satz**
- **Definition**

Definition 0.1. Eine ganze Zahl $n \in \mathbb{Z}$ heißt **gerade**, wenn es eine ganze Zahl m gibt, so dass $n = 2m$.

- **Proposition**
- **Lemma (Hilfsatz)**

Lemma 0.2. Wenn $n \in \mathbb{Z}$ gerade ist, dann ist auch n^2 gerade. (kurzschriftweise: $2|n \Rightarrow 2|n^2$)

Beweis (Voraussetzung \rightarrow Folgerung). Da n gerade ist, gibt es $m \in \mathbb{Z}$ so dass $n = 2m$. Dann

$$n^2 = (2m)^2 = 4m^2 = 2(\underbrace{2m^2}_{\in \mathbb{Z}}) \stackrel{0.1}{\implies} 2|n^2$$

□

Hinweis. Wir haben die **Rechenfolge** für \mathbb{Z} verwendet:

- $ab = ba$ (Kommutativität)
- $(ab)c = a(bc)$ (Assoziativität)

¹Einige Teile stammen aus dem Buch "Einführung in das mathematische Arbeiten"

Lemma 0.3. *Ebenso: Das Quadrat einer ungeraden Zahl ist ungerade.*

Beweis. Bevor wir den Beweis durchgehen, sei darauf hingewiesen, dass "n ungerade" so heißt: es existiert $m \in \mathbb{Z}$, so dass $n = 2m + 1$. Dann

$$\begin{aligned} n^2 &= (2m + 1)^2 = 4m^2 + 4m + 1 \\ &= 2(\underbrace{2m^2 + 2m}_{=m' \in \mathbb{Z}}) + 1 \\ &= 2m' + 1 \end{aligned}$$

□

- **Wesentlicher Objekt:** Menge der natürlichen Zahlen

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

Menge der ganzen Zahlen

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Menge der rationalen Zahlen:

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$$

Eine Denksportaufgabe

Frau Miller hat drei Töchter:

FRAU MILLER: Das Produkt des Alters meiner Töchter ist 36 und die Summe ergibt meine Hausnummer.

NACHBARIN: Daraus kann ich das Alter der Töchter nicht bestimmen.

FRAU MILLER: Richtig, die älteste spielt Cello.

Wie alt sind die Töchter?

Lösung. Zu Beginn, nehmen wir an, dass Alter eine natürliche Zahl $(1, 2, 3, \dots)$ ist. Vorgehensweise, schreiben wir mit allen Fallunterscheidungen:

				Summe
1	1	36		38
1	2	18		21
1	3	12		16
1	4	9		14
1	6	6		13
2	2	9		13
2	3	6		11
3	3	4		10

Aus den Daten der Tabelle, kann man herausfinden, dass die Hausnummer 13 ist. sonst wäre die Nachbarin eindeutig. Es gibt zwei Auswahlmöglichkeiten, die einer Summe von 13 entsprechen:

1	6	6
2	2	9

aber frau Miller hat gesagt: "*Die älteste spielt Cello*". Aber nur in "*2 2 9*" gibt es eine explizite Maximalelement. Da es eine älteste Tochter gibt, kommt nur $(2, 2, 9)$ als Lösung in Frage.

1 Zahlentheorie

Definition 1.1 (Teilbarkeit). Sei $n \in \mathbb{Z}$:

1. $d \in \mathbb{Z}$ heißt **teilbar von m** , wenn es $m \in \mathbb{Z}$ gibt, so dass $n = dm$. (Schreibweise: $d|n$ bedeutet: $\exists m \in \mathbb{Z} : n = dm$)
2. n heißt Primzahl, wenn ± 1 und $\pm n$ die einzige Teiler von n sind und $n > 1$.

Definition 1.2. \mathbb{P} ist die Menge der Primzahlen und ist eine Teilmenge von \mathbb{N} .

Beispiel.

$$\begin{array}{ll} 2|n & n \text{ gerade} \\ 2|10 & 5|10 \\ 3 \nmid 10 & 3 \text{ ist kein Teiler von } 10 \end{array}$$

Lemma 1.3. Seien $d, m, n \in \mathbb{Z}$ wenn $d|m$ und $d|n$ dann gilt auch $d|m+n$.

Beweis. Nach Voraussetzung gibt es $k, l \in \mathbb{Z}$, so dass $m = kd$ und $n = ld$. Dann ist $m+n = kd + ld = (k+l)d$. Da $k+l \in \mathbb{Z}$ gilt $d|m+n$. \square

Bemerkung 1.4 (Wohlordnung von \mathbb{N}). Jede Menge von natürlichen Zahlen hat ein kleinstes Element.

Satz 1.5 (Primzahlzerlegung der natürlichen Zahlen). Sei $n \in \mathbb{N}$, $n > 1$ dann gibt es endlich viele Primzahlen (nicht notwendigerweise verschieden) P_1, P_2, \dots, P_n sodass $n = P_1 P_2 \cdots P_n$.

Beweis. Versuchen wir indirekten Beweis. Angenommen Behauptung stimmt nicht; wir müssen ein Widerspruch herleiten (Wenn ein Widerspruch abgeleitet wird, bedeutet das, dass aus $\neg B$, $\neg A$ das Ergebnis ist und das bedeutet, dass $\neg B \Rightarrow \neg A$ und damit sein Äquivalent $A \Rightarrow B$ wahr ist). Angenommen, es gilt $n \in \mathbb{N}$ sodass sich n nicht als Produkt von endlich vielen Primzahlen schneiden lässt. Dann gilt es ein kleinstes $n \in \mathbb{N}$. Beachten Sie, dass es eine Eigenschaft von der Menge der natürlichen Zahlen (1.4) ist.

Fall 1. n ist eine Primzahl, dann ist n bereits Produkt aus Primzahlen. Angenommen $n = P_1$ und P_1 ist eine Primzahl. Dann können wir schreiben:

$$n = \prod_{k=1}^1 P_k$$

also n ist Produkt aus Primzahlen.

Fall 2. n ist keine Primzahl. Dann besitzt n einen Teiler d und $d|n$. es gibt also $m \in \mathbb{N}$, so dass $n = d \cdot m$. Da $m = \frac{n}{d}$, gilt $1 < m < n$.

Da $d < n$ und $m < n$, lassen sich d und m als Produkt von Primzahlen schneiden. Als $d = q_1 q_2 \cdots q_k$ und $m = r_1 r_2 \cdots r_l$ dann insgesamt ist die Zahl $n = md$ selbstverständlich hergestellt von endlich vielen Primzahlen. Es ist ein Widerspruch zur Eigenschaft von n , die wir schon angenommen haben.

\square

Satz 1.6. Es gibt unendlich viele Primzahlen.

Ein indirekter Beweis. Angenommen Behauptung stimmt nicht. Bilde die Zahl $m = p_1 \cdots p_n + 1$. Nach Satz 1.5 lässt sich m als Produkt von Primzahlen schneiden. Insbesondere gibt es eine Primzahl die m teilt. Diese Primzahl kommt unter den Primzahlen P_1, P_2, \dots, P_n vor, also gibt es P_j so dass $P_j | m$. Dann gilt einerseits $P_j | m$ und andererseits $P_j | P_1 P_2 \cdots P_n$. Dann gilt $P_j | m - (P_1 P_2 \cdots P_n)$. Dann gilt $P_j | 1$ und das heißt, dass es eine Zahl m in der natürlichen Menge gibt, so dass $1 = P_j m$. Dann $0 < m = \frac{1}{P_j} < 1$ und das ist ein Widerspruch. Denn m ist eine natürliche Zahl und kann nicht kleiner als 1 sein. \square