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 $n = m$.

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

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

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

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

□

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

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

[1] Einige 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

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

$\square$

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

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

  Menge der ganzen Zahlen

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

  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 $(1, 2, 3, \ldots)$ 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. sont wäre die Nachbarin eindeutig. Es gibt zwei Auswahlmöglichkeiten, die einer Summe von 13 entsprechen:

$$\begin{matrix} 1 & 6 & 6 \\ 2 & 2 & 9 \end{matrix}$$

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

1.1 Allgemeine Regeln und Fundamentalsätze

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.

$2\|n$		n gerade
$2\|10$	$5\|10$	
$3 \not| 10$		3 ist kein Teiler von 10

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 $d|m + n$. □

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) $P_1, P_2, \ldots, P_n$ 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 einem 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 $n = md$ selbstverstätndlich hergestellt von endlich vielen Primzahlen. Es ist ein Widerspruch zur Eigenschaft von n, die wir schon angenommen haben.

□

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. Insbesonders gibt es eine Primzahl die m teilt. Diese Primzahl kommt unter den Primzahlen $P_1, P_2, \ldots, P_n$ vor, also gibt es P_j so dass $P_j | m$. Dann gilt einerseits $P_j | m$ und anderseits $P_j | P_1 P_2 \cdots P_n$. 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. □

Bemerkung 1.7. Die Menge der rationale Zahlen ist $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$. Durch Kürzen können wir immer annehmen, dass m und n keinen echten gemeinsamen Teiler besitzen. Dass heißt falls $d|m$ und $d|n$, gilt $d = \pm 1$ und falls $m = dh$, $n = dl$ und $d \neq \pm 1$, gilt $\frac{m}{n} = \frac{dh}{dl} = \frac{h}{l}$.

Satz 1.8. $\sqrt{2} \notin \mathbb{Q}$ *($\sqrt{2}$ ist irrational).*

Beweis. Angenommen $\sqrt{2}$ ist rational. D.h. es gibt $m, n \in \mathbb{N}$, so dass $\sqrt{2} = \frac{m}{n}$. Dann gilt $2 = \frac{m^2}{n^2}$ oder $m^2 = 2n^2$. Dann ist m^2 gerade, daher ist auch m gerade. Dann gibt es $k \in \mathbb{N}$ so dass $m = 2k$. Dann gilt

$$m^2 = (2k)^2 = 2 \cdot 2k^2 = 2n^2$$

und Kürzen liefert $n^2 = 2k^2$. Daher muss wieder n gerade sein. Also $n = 2l$ für ein $l \in \mathbb{N}$. $m = 2k$ und $n = 2l$ heißt 2 ist ein gemeinsamer Teiler von m und n. Widerspruch zur Wahl von m und n. □

Satz 1.9 (Division mit Rest)**.** *Sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$ und $n \neq 0$, Dann gibt es eindeutige $q, r \in \mathbb{Z}, 0 \leq r \leq n$ so dass $a = qn + r$.*

Beweis von Existenz. Betrachte die Menge S als

$$\begin{aligned} S &= \{\ldots, a-n, a, a+n, a+2n, \ldots\} \cap \mathbb{N} \\ &= \{m = a + qn : q \in \mathbb{Z}\} \cap \mathbb{N} \end{aligned}$$

Da $S \subseteq \mathbb{N}$, gibt es ein kleinstes Element r in S. Es gibt

- $n \geq 0$
- $r = a - qn$ für ein $q \in \mathbb{Z}$ also $a = qn + r$
- $r < n$. falls $r \geq n$ wäre, gilt

  $$a - (q+1)n = \underbrace{a - qn - n}_{\in S} = r - n \geq 0$$

  und das ist ein Widerspruch zu der Annahme, die r als das kleinste Element beurteilt. Weil $a - qn - n$, ein positives Element der Menge S und kleiner als r ist. Dann $r < n$.

□

Die nächste Schritt ist, die Zahlen q und m und r eindeutig bestimmen. **im Generell wenn man die Eindeutigkeit zeigen will, sollte man zwei Darstellungen annehmen und beweisen, dass sie gleich sind.**

Beweis von Eindeutigkeit. Nehmen wir an, dass $a = a_1 n + r_1 = a_2 n + r_2$. Dann gilt

$$r_1 - r_2 = q_2 n - q_1 n = (q_2 - q_1)n \Rightarrow n | r_1 - r_2$$

und dass bedeutet, dass die Differenz $r_1 - r_2$ ist eine der Zahlen $\{\dots, -n, 0, n, \dots\}$. aber wir wissen schon von den Eigenschaften eines Restes, dass für beide r_1 und r_2 gilt $0 \leq r_1, r_2 < n$. Dann

$$\begin{cases} 0 \leq r_1 < n \\ 0 \leq r_2 < n \end{cases} \Rightarrow 0 \leq |r_1 - r_2| < n$$

von diesen Zahlen ist nur 0 durch n teilbar. Daher muss die Differenz 0 sein. Dann $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$ und auch gilt $q_1 = q_2$. wir sind von zwei verschiedenen Darstellungen ausgegangen und habe gezeigt, die sind schon gleich. und daher ist die Darstellung eindeutig. □

Bemerkung 1.10. Wir haben verwendet Wohlordnung von $\mathbb{N}$, Rechenregeln und die Ordnung $\leq$.

Bemerkung 1.11. Der Beweis ist Konstruktiv. Wir haben die Existenz des Restes und des Vielfaches konstruiert. Wir haben in die Menge nach den natürlichen Elementen gesucht und die kleinste gefunden.

Beispiel. $a = 29$ und $n = 9$. Wir werden die Menge S für a und n konstruieren:

$$S = \{\dots, 29 - 36, 29 - 27, 29 - 18, 29 - 9, 29, 29 + 9, 29 + 18, \dots\}$$

Dann $S \cap \mathbb{N}$ ist:

$$S \cap \mathbb{N} = \{29 - 27, 29 - 18, 29 - 9, 29, \dots\}$$

und das kleinste Element von $S \cap \mathbb{N}$ ist $29 - 27 = 2$. Dann gehen wir davon aus, dass $r = 2$ und

$$r = 2 \Rightarrow 29 - 27 = r \xRightarrow{n=9} 29 - 3 \cdot n = 2 \Rightarrow \boxed{p = 3, r = 2}$$

1.2 Restklassen

Definition 1.12. Sei $n \in \mathbb{N}$, $n > 1$ und $a \in \mathbb{Z}$ beliebig. **Restklasse** von a modulo n ist die Menge

$$\bar{a} = \{\dots, a - n, a, a + n, a + 2n, \dots\} = a + n\mathbb{Z}.$$

Und jede Zahl aus dieser Menge heißt ein **Repräsentant** der Restklasse $\overline{a}$

Bemerkung 1.13. $\overline{a + n} = \overline{a}$. Meist werden wir die Restklassen mit $\overline{0}, \overline{1}, \dots, \overline{n-1}$ zeigen.

Beispiel. $n = 3$:

$$\overline{0} = \{-9, -6, -3, 0, 3, 6, 9, ...\}$$

Bemerkung 1.14. Für $r = 0, 1, \dots, n - 1$ ist $\overline{r}$ die Menge der ganzen Zahlen, die nach Division durch n, den Rest r ergibt.

Beispiel. $\overline{a} = \overline{a + n} = \overline{a + pn}$.

Bemerkung 1.15. Sei $p, q \in \mathbb{Z}$, $0 \leq r < n$ und $a = pn + r$ und $b = qn + r$, dann gilt

$$a - b = pn - qm = n(p - q) \Rightarrow n|p - q$$

und $\overline{a} = \overline{b}$.

Definition 1.16. $a \equiv b \mod n$. a ist **kongruent modulo n** wenn $n|a - b$.

Lemma 1.17. *$a, b, n \in \mathbb{Z}$, $n > 1$. es gilt dann*

$$\overline{a} = \overline{b} \iff a \equiv b \mod n$$

Bemerkung 1.18. Wenn wir eine Aussage wie $p \iff q$ beweisen wollen, müssen wir zeigen, dass p und q äquivalent sind. Daher sollte man sowohl $p \to q$ als auch $q \to p$ beweisen.

Bemerkung 1.19. $\overline{a}$ ist eine **Menge**. Es ist die Menge von Repräsentanten der Restklasse $\overline{a}$.

Beweis. ***Voraussetzung:*** $\overline{a} = \overline{b} \Rightarrow$ ***Folgerung:*** $a \equiv b \mod n$. Sei $\overline{a} \equiv \overline{b}$ dann ist $b \in \overline{a}$ (b ist ein Element von $\overline{a}$) und das heißt $\exists q \in \mathbb{Z}$ so dass $b = a + qr$ und das heißt

$$b - a = qn \Rightarrow n|a - b \Rightarrow a \equiv b \mod n$$

Voraussetzung: $a \equiv b \mod n \Rightarrow$ ***Folgerung:*** $\overline{a} = \overline{b}$. Um zu beweisen, dass zwei Mengen gleich sind, muss man zwei Aussagen beweisen. Erstens, die Aussage, dass ein beliebiges Element von der Menge a, auch ein Element in b ist und zweitens die Aussage, dass ein beliebiges Element von b auch ein Element von der Menge a ist. Daher beweisen wir zuerst, dass ein beliebiges Element von $\overline{b}$ namens b ist auch ein Element von der Menge $\overline{a}$:
$a \equiv b \mod n$ und das heißt $n|a - b$ und es gibt $q \in \mathbb{Z}$ so dass $b - a = qn$. dann $b = nq + a$ und daher ist die Zahl b ein Element von $\overline{a}$. Beliebiges Element in $\overline{b}$ hat die Form $b + pn$. dann gilt

$$b + pn = a + qn + pn = a + (p + q)n \Rightarrow b + pn \in \overline{a} \Rightarrow \overline{b} \subseteq \overline{a}.$$

Vertauschen von a und b liefert, dass $\overline{a} \subseteq \overline{b}$. Daher $\overline{a} = \overline{b}$ □

Satz 1.20. *Eigenschaften von Kongruenzen sind:*

1.	$a \equiv a \mod n$	*(Identität)*
2.	*Wenn* $a \equiv b \mod n$ *dann* $b \equiv a \mod n$	*(Symmetrie)*
3.	*Wenn* $a \equiv b \mod n$ *und* $b \equiv c \mod n$ *dann ist* $a \equiv c \mod n$	*(Transitivität)*

Beweis von 1. $n|\underbrace{a - a}_{=0}$ also $a \equiv a \mod n$. □

Beweis von 2. $a \equiv b \mod n$ heißt, dass $n|a - b$. Daher gibt es eine Zahl $q \in \mathbb{Z}$ so dass $a - b = nq$. Dann gilt

$$\begin{aligned} b - a &= -nq = (-q)n \\ &\Rightarrow n|b - 1 \\ &\Rightarrow \boxed{b \equiv a \mod n} \end{aligned}$$

□

Beweis von 3.

$$\begin{array}{l} a \equiv b \mod n \Rightarrow n | a - b \\ b \equiv c \mod n \Rightarrow n | b - c \end{array}.$$

Wir wissen schon, wenn n zwei Zahlen teilt, teilt es auch die Summe. Daher

$$\begin{aligned} n|(a-b)+(b-c) &\Rightarrow n|a-c \\ &\Rightarrow a \equiv c \mod n \end{aligned}$$

□

Satz 1.21 (Addieren und Multiplizieren von Restklassen)**.** $a, b, n \in \mathbb{Z}, n > 1$

- $\overline{a} + \overline{b} = \overline{a+b}$
- $\overline{a} \cdot \overline{b} = \overline{ab}$

Beispiel. $n = 3$

$$\begin{array}{rcrcc} \bar{1} & + & \bar{2} & = \bar{3} & = \bar{0} \\ +2 \cdot n \downarrow & & +2 \cdot n \downarrow & & \\ \bar{7} & + & \bar{5} & = \overline{12} & = \bar{0} \end{array}$$