Lineare Algebra und Analytische Geometrie 1

Vorlesung Wintersemester 2022/23

Prof. Meinolf Geck, Lehrstuhl für Algebra, Universität Stuttgart
https://pnp.mathematik.uni-stuttgart.de/idsr/idsr1/geckmf

Dies ist das Skript zur Vorlesung Lineare Algebra und Analytische Geometrie 1 im Wintersemester 2022/23 (V4Ü2, 15 Wochen). Eines der Hauptziele ist natürlich die Vermittlung von Grundwissen und Rechenfertigkeiten in einem zentralen Teilgebiet der Mathematik.

Etwas genereller geht es auch um die Vermittlung einer mathematischen Denkweise. Dazu gehört es zu lernen, wie man mathematische Sachverhalte formal korrekt aufschreibt und diese beweist, also ihre Richtigkeit nach logischen Prinzipien herleitet. Dies sind übrigens Fähigkeiten, die sich auch in diversen anderen Situationen als sehr hilfreich erweisen!

Außerdem sollen natürlich Beispiele für die Nützlichkeit von mathematischen Konzepten in Anwendungen gegeben werden.

Im Durchschnitt werden pro Woche etwa 7 Seiten dieses Skriptes behandelt. (In den einführenden Abschnitten am Anfang vielleicht etwas mehr.)

Kommentare sehr willkommen! (Insbesondere Druckfehler, sonstige Unklarheiten, Verbesserungsvorschläge etc.)

Stuttgart, Oktober 2022

Ziele/Inhalt der Vorlesung

- **Lösen von linearen Gleichungssystemen:**

$$\begin{array}{rcrcrcl} x_1 & + & 3x_2 & - & 2x_3 & = & 1 \\ 2x_1 & + & 2x_2 & & & = & 2 \\ 4x_1 & + & 6x_2 & + & x_3 & = & 8 \end{array}$$

  (Anwendungen in Natur- und Ingenieurwissenschaften, ...)

- **Allgemeine Theorie der Vektorräume und linearen Abbildungen**
- **Hinführung auf neue Zahlsysteme und Strukturen:**
  Zum Beispiel "binäres" Zahlensystem $\{0, 1\}$ mit $1 + 1 = 0$ ($\rightsquigarrow$ Informatik).
- **Die Kapitelüberschriften:**
  - Kapitel I: Grundlagen.
  - Kapitel II: Matrizen.
  - Kapitel III: Algebraischen Strukturen.
  - Kapitel IV: Vektorräume und lineare Abbildungen.
  - Kapitel V: Determinanten und Determinantenfunktionen.
- **Modell für den axiomatischen Aufbau einer Theorie:**
  - Festlegung von grundlegenden Begriffen und Regeln ("Axiomen"), die als wahr vorausgesetzt werden.
  - Herleiten ("Beweisen") von Aussagen aus den Axiomen sowie bereits bewiesenen Aussagen nach bestimmten logischen Regeln.
  - Präzises Formulieren und Argumentieren.
    (Anwendungen im Studium und in allen späteren Berufen!)

  (Obiges gilt genauso für die Vorlesung Analysis I.)

- **"Axiom" für diese Vorlesung:**
  - Das Zahlensystem der ganzen Zahlen, also der Zahlen $0, \pm 1, \pm 2, \pm 3, \ldots$, sowie das Rechnen mit diesen Zahlen (Addition, Multiplikation) werden als bekannt vorausgesetzt. Ebenso das Rechnen mit rationalen Zahlen, also Brüchen $\pm n/m$ mit natürlichen Zahlen n, m.
  - Mengentheoretische Sprechweisen und Grundlagen aus der mathematischen Logik werden schrittweise eingeführt wenn sie gebraucht werden.

Literatur

Besonders geeignet für diese Vorlesung:

- S. Axler, Linear Algebra done right. Undergraduate texts in mathematics, Springer-Verlag, 2015.
- G. Fischer, Lineare Algebra: Eine Einführung für Studienanfänger, Vieweg + Teubner Verlag; 17. Auflage 2010.
- B. Huppert und W. Willems, Lineare Algebra: Mit zahlreichen Anwendungen in Kryptographie, Codierungstheorie, Mathematischer Physik und Stochastischen Prozessen, Vieweg + Teubner Verlag, 2. Auflage 2010.
- R. Kaye and R. Wilson, Linear Algebra. Oxford University Press, New York, 1998.
- M. Koecher, Lineare Algebra und analytische Geometrie, Grundwissen Mathematik, Springer-Verlag, 4. Auflage, 2002.
- P. Petersen, Linear Algebra. Undergraduate texts in mathematics, Springer-Verlag, 2012.

Zum Auffrischen von Schulwisssen und Grundlagen:

- T. Glosauser, (Hoch)Schulmathematik, Ein Sprungbrett vom Gymnasium zur Uni. Springer-Spektrum, 2015.
- M. Liebeck, A Concise Introduction to Pure Mathematics. Chapman Hall/CRC Mathematics Series, CRC Press, 3rd edition 2010.
- MINT Kolleg Baden-Württemberg, Mathematik-Vorkurs (Online), siehe http://www.mint-kolleg.de/stuttgart/angebote/online_kurse

Frei verfügbare mathematische Software zum Ausprobieren/Experimentieren:

- GAP - Groups, Algorithms, and Programming, siehe http://www.gap-system.org/ (Exaktes Rechnen mit Zahlen und diskreten algebraischen Strukturen.)
- SageMath, siehe https://www.sagemath.org/ (Basiert auf der Programmiersprache Python; siehe https://www.python.org/)

Einige weiterführende Texte (Auswahl, wird laufend ergänzt):

- M. Artin, Algebra. Aus dem Englischen übersetzt von Annette A'Campo. Birkhäuser Verlag, 1993.
- N. L. Biggs, Discrete Mathematics, 2nd Edition. Oxford University Press, 2002.

- N. Bourbaki, Éléments de Mathématiques. Algèbre. Chap. 1 à 3, Masson, Paris, 1970; Chap. 4 à 7, Masson, Paris, 1981.
- J. G. Broida and S. Gill Williamson, Comprehensive Introduction to Linear Algebra, 2012; Web Version, Creative Commons CC0 1.0; see https://cseweb.ucsd.edu/~gill/CILASite/.
- H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel und R. Remmert, Zahlen. Grundwissen Mathematik, vol. 1, Springer-Verlag, Berlin, 1983.
- S. H. Friedberg, A. J. Insel und L. E. Spence, Linear Algebra, 4th ed., Pearson, 2002.
- P. R. Halmos, Naive Mengenlehre, Vandenhoeck & Ruprecht, 5. Auflage, 1994.
- F. Lorenz, Lineare Algebra, 2 Bände. Spektrum Akademischer Verlag; 1. Band, 4. Auflage 2008; 2. Band, 3. Auflage, 1992.
- D. Poole, Linear Algebra: A Modern Introduction. Brooks Cole Pub Co., 3. Auflage, 2010.
- D. Serre, Matrices: Theory and Applications. Graduate Texts in Mathematics 216, Springer-Verlag, 2. Auflage, 2010.

Inhaltsverzeichnis

Kapitel I: Grundlagen

Mathematik beruht auf den Grundpfeilern Mengenlehre und Logik. Wir können und wollen hier keine formale Einführung in die abstrakte Mengenlehre und mathematische Logik geben. (Dazu wäre eine eigene Vorlesung nötig, die auch in einem Mathematik-Studium oft erst später angeboten wird, wenn überhaupt.) Für den Anfang und die meisten Zwecke genügt es, sich auf einige grundlegende Sprech- und Schreibweisen zu verständigen, mit denen wir im weiteren Verlauf mathematische Sachverhalte präzise formulieren und beweisen können.

1. *Mengen und Aussagen*

Eine ***Menge*** ist für uns einfach eine Zusammenfassung von bestimmten Objekten, die als ***Elemente*** der Menge bezeichnet werden. Eine solche Zusammenfassung wird durch geschweifte Klammern $\{\ldots\}$ bezeichnet, zum Beispiel:

$$S = \{ \text{ alle Einwohner von Stuttgart } \},$$
$$\mathbb{N} = \{1, 2, 3, 4, \ldots\} \quad \text{die natürlichen Zahlen},$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\} \quad \text{die natürlichen Zahlen mit } 0,$$
$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\} \quad \text{die ganzen Zahlen}.$$

Mengen können also nur eine bestimmte Anzahl von Elementen enthalten (wie im 1. Beispiel) oder auch unendlich viele Elemente (wie im 2., 3. und 4. Beispiel).

Schreibweisen:

"$a \in A$" bedeutet: Das Objekt a ist ein Element der Menge A;
analog bedeutet "$a \notin A$", dass a nicht zu A gehört.

"$A \subseteq B$" bedeutet: Die Menge A ist eine Teilmenge der Menge B, und dies wiederum bedeutet, dass jedes Element von A auch ein Element von B ist.

"$A = B$" bedeutet: Die Menge A enthält die gleichen Elemente wie die Menge B, oder anders ausgedrückt: Es gilt $A \subseteq B$ und $B \subseteq A$.

Zum Beispiel gilt $-5 \notin \mathbb{N}$ und $\mathbb{N} \subseteq \mathbb{Z}$. Ist $A \subseteq B$ und $A \neq B$, so schreiben wir $A \subsetneq B$.

Das Symbol "$\varnothing$" steht für die ***leere Menge***, also die Menge, die überhaupt kein Element enthält. Wir können dies auch mit $\{\}$ bezeichnen. Es gilt $\varnothing \subseteq A$ für jede Menge A.

Unter einer ***Aussage*** verstehen wir einen Satz (auf deutsch, englisch oder in sonst irgendeiner Zeichensprache), der entweder wahr oder falsch ist.

BEISPIEL: Der Satz "Der 19.10.2022 ist ein Mittwoch" ist eine wahre Aussage. Aber der Satz "Bitte stellen Sie Fragen, wenn etwas nicht klar ist" ist keine Aussage.

Natürlich ist ein in der mathematischen Zeichensprache verfasster Satz wie "$1+1=3$" eine Aussage, die in diesem Fall falsch ist.

Beachte: Es kann dabei sein, dass wir vielleicht nicht wissen, ob die fragliche Aussage nun wahr oder falsch ist, oder dass es extrem schwierig ist, die Antwort zu finden; es kommt nur darauf an, dass etwas gesagt wird, das entweder wahr oder falsch ist. – Beispiele:

- "Es gibt Außerirdische".
- $2^{277232917}-1$ (eine Zahl mit 23249425 Ziffern) ist eine Primzahl.

Mengenbildung mit Aussagen: Gegeben sei eine Menge A und, für jedes $a \in A$, eine Aussage $P(a)$. Dann können wir die Menge aller derjenigen $a \in A$ bilden, für die $P(a)$ wahr ist, und dies ist eine Teilmenge von A; in Zeichen:

$$\{a \in A \mid P(a) \text{ ist wahr}\} \subseteq A.$$

BEISPIEL: Sei A die Menge aller Anwesenden im Hörsaal V47.02. Für jedes $a \in A$ sei $P(a)$ die Aussage: "a trägt einen blauen Pullover". Dann ist also $\{a \in A \mid P(a) \text{ ist wahr}\}$ genau die Menge der hier Anwesenden, die einen blauen Pullover tragen.

Hier sehen wir auch die Nützlichkeit der leeren Menge: Trägt nämlich niemand einen blauen Pullover, so ist $\{a \in A \mid P(a) \text{ ist wahr}\} = \varnothing$.

BEISPIEL: Sei $A = \mathbb{N}$ und $P(n)$ die Aussage: "n ist eine gerade Zahl". Dann ist also

$$\{n \in A \mid P(n) \text{ ist wahr}\} = \{2,4,6,8,\ldots\} = \text{ Menge der geraden Zahlen.}$$

Sei nun $Q(n)$ die Aussage: "$P(n)$ ist falsch". Dann ist

$$\{n \in A \mid Q(n) \text{ ist wahr}\} = \{n \in A \mid P(n) \text{ ist falsch}\} = \{1,3,5,7,\ldots\}$$

die Menge der ungeraden Zahlen.

Beachten Sie: Es ist offenbar egal, ob wir $P(a)$ oder $P(n)$ schreiben, denn das Symbol "a" bzw. "n" ist hier ja nur ein Platzhalter (also so etwas wie eine lokale Variable beim Programmieren), der auf ein Element von A verweist.

Verknüpfung von Aussagen.

Ist P eine Aussage, so wird mit $\neg P$ die Negation von P bezeichnet.

Beispiel: Ist P : "Heute ist Dienstag", so ist $\neg P$ die Aussage "Heute ist nicht Dienstag".

Sind P und Q Aussagen, so erhalten wir neue Aussagen durch folgende Verknüpfungen:

"$P \vee Q$" ist die Aussage: "P ist wahr oder Q ist wahr oder beide sind wahr."

"$P \wedge Q$" ist die Aussage: "P ist wahr und Q ist wahr."

"$P \Rightarrow Q$" ist die Aussage: "Aus P folgt Q" oder anders ausgedrückt: "Wann immer P wahr ist, so muss auch Q wahr sein."

Es ist manchmal nützlich, diese Verknüpfungen durch ***Wahrheitstabellen*** zu beschreiben, die angeben, welchen Wahrheitswert die Verknüpfung in Abhängigkeit von den möglichen Kombinationen der Wahrheitswerte von P und Q hat, also etwa:

P	$\neg P$
1	0
0	1

P	Q	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$
1	1	1	1	1
1	0	1	0	0
0	1	1	0	1
0	0	0	0	1

(wobei 1 für "wahr" steht und 0 für "falsch"). Vielleicht kommt Ihnen die letzte Spalte etwas ungewohnt vor! Dazu beachten Sie, dass aus falschen Aussagen durchaus wahre Aussagen gefolgert werden können; es geht ja nur darum, dass die Folgerung als solche korrekt ist.

Beispiel: Für $a, b \in \mathbb{Z}$ ist die folgende Verknüpfung eine wahre Aussage:

$$a = b \quad \Rightarrow \quad a^2 = b^2.$$

Beweis: Wenn $a = b$ gilt, so können wir im Produkt $a^2 = a \cdot a$ beide Faktoren durch b ersetzen und erhalten $b \cdot b = b^2$, also die rechte Seite.

Nehmen wir konkret $a = 2$ und $b = -2$, so ist "$a = b$" falsch, aber "$a^2 = b^2$" wahr; nehmen wir $a = 2$ und $b = 3$, so ist "$a = b$" falsch und auch "$a^2 = b^2$" falsch. Aber der obige Beweis ist natürlich immer richtig, egal in welcher Beziehung a und b zueinander stehen.

Das Beispiel $a = 2$, $b = -2$ zeigt auch, dass die Umkehrung "$a^2 = b^2 \Rightarrow a = b$" falsch ist.

Allgemein sagen wir, dass P und Q ***äquivalente Aussagen*** sind (in Zeichen: "$P \Leftrightarrow Q$"), wenn sowohl "$P \Rightarrow Q$" als auch "$Q \Rightarrow P$" wahr sind.
Wir drücken dies auch so aus, dass P genau dann gilt, wenn Q gilt.

Mit Hilfe der Werte in den entsprechenden Wahrheitstabellen stellen Sie sofort fest:

- "$P \Leftrightarrow Q$" ist äquivalent zu: Entweder P, Q beide wahr oder beide falsch.
- "$P \Rightarrow Q$" ist äquivalent zu: "$(\neg P) \vee Q$".
- "$P \Rightarrow Q$" ist auch äquivalent zu: "$(\neg Q) \Rightarrow (\neg P)$".

Letztere Verknüpfung heißt ***Kontraposition***.

Weitere Konstruktionen zum Bilden neuer Mengen: Seien A, B zwei Teilmengen einer Menge M. Dann ist die ***Durchschnittsmenge*** von A und B definiert durch

$$A \cap B := \{x \in M \mid x \in A \wedge x \in B\};$$

dieser besteht also genau aus den Elementen, die sowohl in A als auch in B enthalten sind.

Hierbei (und auch sonst in diesem Skript) steht der Doppelpunkt in ":=" für eine Definition: Es wird keine Gleichheit behauptet, sondern das Symbol "$A \cap B$" ist lediglich ein Name für die Menge auf der rechten Seite.

Die ***Vereinigungsmenge*** von A und B ist definiert als

$$A \cup B := \{x \in M \mid x \in A \vee x \in B\};$$

diese besteht also genau aus den Elementen, die in A oder in B enthalten sind (oder sowohl in A als auch in B). Das ***Komplement*** von B in A bezeichnet ist definiert als

$$A \setminus B := \{x \in A \mid x \notin B\} \qquad \text{(oft auch } A^c \text{ geschrieben)}.$$

Schließlich können wir zu jeder Menge A auch ihre ***Potenzmenge*** $\mathcal{P}(A)$ bilden, d.h., die Menge aller Teilmengen von A.

Zum Beispiel besteht die Potenzmenge von $A = \{1, 2, 3\}$ aus 8 Elementen:

$$\mathcal{P}(A) = \{\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\},\ \{1, 2, 3\}\}.$$

Hier gilt dann etwa $\{1, 2\} \in \mathcal{P}(A)$ und $\{\varnothing, \{1\}\} \subseteq \mathcal{P}(A)$, d.h., Mengen können auch selbst wieder Elemente von anderen Mengen sein.

Ein etwas komplexeres Beispiel: Sei A eine nicht-leere Menge und B eine beliebige Teilmenge von $\mathcal{P}(A)$, d.h., B ist eine Menge von Teilmengen von A. Dann können wir die Vereinigung aller $X \in B$ bilden.

Dies wird mit obigen Mengenbildungsprinzipien wie folgt begründet. Betrachte für $a \in A$ die Aussage $P(a)$: "Es gibt ein $X \in B$ mit $a \in X$".

Dann ist $\displaystyle\bigcup_{X \in B} X := \{a \in A \mid \text{es gibt ein } X \in B \text{ mit } a \in X\}$

Konkretes Beispiel: $A =$ Menge aller Menschen auf der Erde.

$$B = \Big\{\big\{\text{Menschen in Deutschland}\big\},\ \big\{\text{Menschen in Frankreich}\big\},$$
$$\big\{\text{Menschen in Polen}\big\},\ \ldots \text{usw. für alle (nur noch) 27 Länder der EU}\Big\}.$$

Dann ist $\displaystyle\bigcup_{X \in B} X = \big\{\text{alle Menschen in der EU}\big\}.$

Quantoren: Dies sind die mathematischen Kurzzeichen $\exists$, welches für "es existiert" steht, und $\forall$, welches für "für alle" steht. Beispiele:

Die Aussage "Es gibt eine natürliche Zahl n mit $n^3 = 8$" lässt sich kurz schreiben als: $\exists n \in \mathbb{N} : n^3 = 8$.

Die Aussage "Das Quadrat einer beliebigen ganzen Zahl ist entweder 0 oder positiv" lässt sich kurz schreiben als: $\forall n \in \mathbb{Z} : n^2 \geqslant 0$.

Etwas formaler: Gegeben sei eine Menge A und, für jedes $a \in A$, eine Aussage $P(a)$.

"$\forall a \in A : P(a)$" bedeutet, dass die Aussage $P(a)$ für alle $a \in A$ wahr ist.

"$\exists a \in A : P(a)$" bedeutet, dass es (mindestens) ein $a \in A$ gibt, für welches $P(a)$ wahr ist.

Für die Negation von Aussagen mit Quantoren gilt:

$$\neg\big(\forall a \in A : P(a)\big) \Leftrightarrow \exists\, a \in A : \neg P(a) \quad \text{und} \quad \neg\big(\exists\, a \in A : P(a)\big) \Leftrightarrow \forall a \in A : \neg P(a)$$

Im Prinzip sollte man sämtliche mathematischen Aussagen in dieser Vorlesung in einer Formelsprache ausdrücken können, in denen nur Aussagen über Elemente in Mengen, Verknüpfungen von Aussagen und Quantoren vorkommen. Aber bei komplizierteren Sachverhalten wird man der besseren Verständlichkeit halber stets versuchen, diese Sachverhalte so weit wie möglich in "normalen", möglichst einprägsamen Sätzen auszudrücken.

Schließlich erwähnen wir hier nur, dass man in logische Schwierigkeiten geraten kann, wenn man die obigen Mengenbildungsprinzipien verlässt. Berühmtes Beispiel ist die ***Russell'sche Antinomie***; siehe dazu https://en.wikipedia.org/wiki/Russell's_paradox. Man kann so etwas auch in der Umgangssprache formulieren:

"*Definieren wir einen Barbier als jemanden, der all jene und nur jene rasiert, die sich nicht selbst rasieren. Frage: Rasiert der Barbier sich selbst?*"

Nimmt man an, er rasiert sich selbst, so erhält man einen Widerspruch; aber ebenso, wenn man annimmt, er rasiert sich nicht selbst ...

2. *Beweistechniken*

Wir stellen grundlegende Beweistechniken vor und illustrieren diese durch einige Beispiele, in denen Aussagen über ganze Zahlen (die zum Teil bereits aus der Schule vertraut sein mögen) mathematisch korrekt hergeleitet werden. Dabei setzen wir lediglich die Kenntnis der Grundrechenarten für natürliche und ganze (und später auch rationale) Zahlen voraus.

Definition 2.1. Seien $n, m \in \mathbb{Z}$. Wir schreiben $n \mid m$ und sagen "n teilt m" oder "m ist ein Vielfaches von n", wenn es ein $a \in \mathbb{Z}$ gibt mit $m = a \cdot n$.

Beispiele: $2 \mid 6$ (denn $6 = 3 \cdot 2$), $5 \mid 0$ (denn $0 = 0 \cdot 5$) und $3 \nmid 10$ (denn die positiven Vielfachen von 3 sind $3, 6, 9, 12, \ldots$).

Lemma 2.2 (oder auch "Hilfssatz")**.**
(a) *Seien* $n, m, k \in \mathbb{Z}$. *Gilt* $n \mid m$ *und* $m \mid k$*, so auch* $n \mid k$.
(b) *Seien* $n, m, k \in \mathbb{Z}$ *und* $a, b \in \mathbb{Z}$. *Gilt* $n \mid m$ *und* $n \mid k$*, so auch* $n \mid (a \cdot m + b \cdot k)$.

Beweis. Dies ist ein Beispiel eines "Routine-Beweises", wo es darum geht, die Richtigkeit von vorgegebenen Formeln durch einfaches Nachrechnen zu bestätigen.

(a) Nach Voraussetzung gibt es $a, b \in \mathbb{Z}$ mit $m = a \cdot n$ und $k = b \cdot m$. Dann ist $k = b \cdot m = b \cdot (a \cdot n) = (b \cdot a) \cdot n$. (Hier haben wir benutzt, dass man Produkte von ganzen Zahlen beliebig klammern darf.) Setzen wir $c = b \cdot a \in \mathbb{Z}$, so gilt also $k = c \cdot n$ und damit $n \mid k$.

(b) Voraussetzung ist: $n \mid m$ und $n \mid k$. Also gibt es $u, v \in \mathbb{Z}$ mit $m = u \cdot n$ und $k = v \cdot n$. Dann folgt: $a \cdot m + b \cdot k = a \cdot (u \cdot n) + b \cdot (v \cdot n) = (a \cdot u) \cdot n + (b \cdot v) \cdot n = (a \cdot u + b \cdot v) \cdot n$. (Hier haben wir wiederum benutzt, dass man Produkte beliebig klammern darf; außerdem haben wir eine Distributivregel verwendet, die besagt, dass man in einer Summe von zwei Produkten gemeinsame Faktoren ausklammern darf.) Setzen wir $c = a \cdot u + b \cdot v \in \mathbb{Z}$, so gilt also $a \cdot m + b \cdot k = c \cdot n$ und damit $n \mid (a \cdot m + b \cdot k)$. $\square$ ($\leftarrow$ zeigt Ende des Beweises an)

Im Folgenden werden wir nicht mehr explizit wie im obigen Beweis erwähnen, wenn wir eine der üblichen Regeln beim Rechnen mit ganzen Zahlen verwenden. Außerdem lassen wir den Punkt bei der Multiplikation der besseren Lesbarkeit wegen einfach weg.

Lemma 2.3. (a) *Ist* $n \in \mathbb{N}_0$ *ungerade, so ist auch* n^2 *ungerade.*
(b) *Ist* $n \in \mathbb{N}_0$ *so dass* n^2 *gerade ist, so ist auch* n *selbst gerade.*

Beweis. (a) Da n ungerade ist, gilt $n = 2m + 1$ mit einem $m \in \mathbb{N}_0$. Damit erhalten wir $n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$. Setzen wir $k = 2m^2 + 2m \in \mathbb{N}_0$, so gilt also $n^2 = 2k + 1$, d.h., n^2 ist auch ungerade.

(b) Folgt sofort aus (a) durch "Kontraposition". Sei P die Aussage "n ist ungerade" und Q die Aussage "n^2 ist ungerade". In (a) wurde gezeigt, dass "$P \Rightarrow Q$" gilt. Kontraposition bedeutet, dass dann auch "$(\neg Q) \Rightarrow (\neg P)$" gilt, also genau die Aussage in (b). $\square$

Lemma 2.4 (Kürzungsregel)**.** *Seien* $n, m, k \in \mathbb{Z}$. *Gilt* $k \neq 0$ *und* $kn = km$*, so folgt* $n = m$.

Beweis. Wir betrachten die Aussagen P: "$kn = km$" und Q: "$n = m$".
Um "$P \Rightarrow Q$" zu zeigen, können wir auch genauso gut "$(\neg Q) \Rightarrow (\neg P)$" zeigen.

Nehmen wir also an, es gelte $\neg Q$, d.h., es sei $n \neq m$. Dann ist $n - m \neq 0$ und $k(n-m) \neq 0$ (weil das Produkt von zwei ganzen Zahlen ungleich 0 wieder ungleich 0 ist). Nun ist $kn - km = k(n-m) \neq 0$ also folgt $kn \neq km$, d.h., $\neg P$. □

Beweise durch Kontraposition werden auch oft als "Widerspruchsbeweise" dargestellt. Man nimmt dazu an, dass die gewünschte Aussage falsch ist, und leitet dann daraus einen Widerspruch ab (d.h., eine Aussage, von der wir bereits wissen, dass sie falsch ist). Per Kontraposition ist damit die gewünschte Aussage wahr. — Mehr Beispiele später ...

Satz 2.5. *Sei* $n \in \mathbb{N}$. *Dann gilt* $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$.

Beweis. Dies ist ein Beispiel eines Beweises, bei dem es nicht nur um routine-mässiges Nachrechnen geht, sondern irgendeine Idee oder ein Trick verwendet werden muss.

Zum Umgang mit Summen führen wir zunächst die allgemeine Summenschreibweise ein: Sind $a_1, \ldots, a_n$ ganze Zahlen, so schreiben wir: $a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i$.

Mit $a_i = i$ für $i = 1, \ldots, n$ wollen wir also eine Formel für folgende Summe finden:

$$S := 1 + 2 + \ldots + n = \sum_{i=1}^{n} i.$$

Der "Trick" dieses Beweises besteht nun darin, auszunutzen, dass man die Reihenfolge in einer Summe von ganzen Zahlen beliebig ändern kann. Also gilt auch $S = n + (n-1) + \ldots + 2 + 1$. Der i-te Term in dieser Summe ist gegeben durch $b_i = n + 1 - i$; damit erhalten wir

$$S = \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (n + 1 - i).$$

Nun bilden wir
$$\begin{aligned} 2S = S + S &= (a_1 + a_2 + \ldots + a_n) + (b_1 + b_2 + \ldots + b_n) \\ &= (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_n + b_n) \qquad \text{(noch einmal der Trick!)} \\ &= \sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} \big(i + (n + 1 - i)\big) = \sum_{i=1}^{n} (n+1) = n(n+1). \end{aligned}$$

Damit ist $2S = n(n+1)$, also $S = \frac{1}{2}n(n+1)$, wie gewünscht. □

Die folgende Eigenschaft von $\mathbb{N}_0$ erscheint intuitiv einsichtig; sie wird explizit formuliert, damit wir darauf verweisen und präzise damit argumentieren können.

Wohlordnungsprinzip für $\mathbb{N}_0$ ***(WOrP)***. *Jede nicht-leere Teilmenge von* $\mathbb{N}_0$ *besitzt ein kleinstes Element. Oder, anders ausgedrückt mit Hilfe der Formelsprache in §1:*

$$\forall\, A \in \mathcal{P}(\mathbb{N}_0): \quad A \neq \varnothing \quad \Rightarrow \quad \big(\exists\, a \in A: \quad \big(\forall\, b \in A: a \leqslant b\big)\big).$$

Zur Erinnerung: natürliche und ganze Zahlen sind angeordnet

$$\ldots < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < \ldots$$

Formal: Für $a, b \in \mathbb{Z}$ gilt $a \leqslant b$, wenn es ein $c \in \mathbb{N}_0$ gibt mit $b = a + c$.

Zum Beispiel gilt $kn \geqslant n$ für alle $k, n \in \mathbb{N}$.
(Denn: Ist $k \in \mathbb{N}$, so ist $k - 1 \geqslant 0$ und damit $kn = n + \underbrace{(k-1)n}_{\geqslant 0} \geqslant n$.)

Als erste Anwendung des obigen Prinzips zeigen wir folgende Aussage:

Satz 2.6 (Teilen mit Rest)**.** *Sei* $n \in \mathbb{Z}$ *und* $m \in \mathbb{N}$. *Dann gibt es* $q, r \in \mathbb{Z}$ *mit* $n = qm + r$ *und* $0 \leqslant r < m$. *Hier sind* q, r *eindeutig bestimmt. (Ist* $n \geqslant 0$*, so auch* $q \geqslant 0$*.)*

Ist $n = qm + r$ wie oben, so wird der "Rest" r auch mit $n \bmod m$ bezeichnet. Diese "mod" Funktion ist eine grundlegende arithmetische Operation; es gibt sie auch in den meisten modernen Programmierspachen, zum Beispiel `17 % 5` in Python oder C.

Beispiel. Für die Division von 17 mit Rest durch 5 erhalten wir:

$$17 = 3 \cdot 5 + 2, \qquad \text{also} \quad q = 3 \text{ und } r = 2 \quad \rightsquigarrow \quad 17 \bmod 5 = 2.$$

(Dazu zieht man so lange 5 von 17 ab, bis noch etwas $\geqslant 0$ herauskommt.)
Für die Division von -17 mit Rest durch 5 erhalten wir:

$$-17 = (-4) \cdot 5 + 3, \qquad \text{also} \quad q = -4 \text{ und } r = 3 \quad \rightsquigarrow \quad -17 \bmod 5 = 3.$$

(Dazu addiert man so lange 5 zu -17, bis man eine Zahl $\geqslant 0$ erhält.)

Dieses "so lange ... bis" scheint intuitiv klar. Typischerweise benötigt man allerdings das Wohlordnungsprinzip für einen formalen Beweis. Wir führen dies hier einmal explizit aus.

Ab hier Woche 2

Index