Mathematik I für Informatikstudiengänge

Vorlesung Wintersemester 2024/25

Anda Degeratu, Lehrstuhl für Differential Geometry, Universität Stuttgart
https://www.idsr.uni-stuttgart.de/institut/Degeratu/
(nach dem Skript von Prof. Meinolf Geck)

Dies ist das Skript zur Vorlesung Mathematik I (für Informatikstudiengänge) im Wintersemester 2024/25 (V4Ü2, 15 Wochen). Es ist ziemlich genau das Vorlesungsskript von Prof. Meinolf Geck aus dem Wintersemester 2021/22, https://pnp.mathematik.uni-stuttgart.de/idsr/idsr1/geckmf/SkriptMathInf1.pdf. Ich werde es im Laufe des Semesters noch ein wenig ändern.

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

Anda Degeratu *Stuttgart, Oktober 2024*

Eines der Hauptziele dieser Vorlesung ist natürlich die Vermittlung von Grundwissen und Rechenfertigkeiten in der Mathematik. Etwas genereller geht es auch um die Vermittlung einer mathematischen Denkweise für Studierende, deren erstes Fach nicht Mathematik selbst ist aber wo diese Denkweisen dennoch eine wichtige Rolle spielen.

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 beim Programmieren (und in diversen anderen Situationen) als sehr hilfreich erweisen! Außerdem sollen natürlich Beispiele für die Nützlichkeit von mathematischen Konzepten in Anwendungen gegeben werden.

Die Gebiete, die in diesem Skript behandelt werden, umfassen Lineare Algebra (Matrix-Theorie), die ersten Grundlagen zur Analysis (reelle und komplexe Zahlen), sowie diskrete algebraische Strukturen (zum Beispiel das "binäre" Zahlensystem $\{0, 1\}$ mit $1 + 1 = 0$). Ganz am Anfang gibt es zunächst eine kurze Einführung in die Mengenlehre und mathematische Logik. Bei der Auswahl des konkreten Stoffes habe ich mich an den Skripten von Herrn Künzer und Herrn Lesky aus früheren Semestern orientiert und auch explizit weite Teile daraus übernommen. Allerdings gibt es hier und da Änderungen in der Präsentation.

Danke an Herrn Rainer Häußling für die regelmäßigen Listen mit Druckfehlern und Verbesserungsvorschlägen.

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

Meinolf Geck *Stuttgart, Oktober 2021*

Literatur

Besonders geeignet für diese Vorlesung:

- G. Teschl und S. Teschl, Mathematik für Informatiker. Band 1: Diskrete Mathematik und Lineare Algebra, 4. Auflage, Springer Vieweg, 2013.
- G. Teschl und S. Teschl, Mathematik für Informatiker. Band 2: Analysis und Stochastik, 3. Auflage, Springer Vieweg, 2014.

Skripte aus früheren Durchgängen an der Uni Stuttgart:

- P. Lesky, Mathematik I für inf, swt, msv. Skript zur Vorlesung im WiSe 2018/19; siehe http://info.mathematik.uni-stuttgart.de/Mathe1InfWS1819.
- M. Künzer, Mathematik I für inf, swt, msv, dsc. Skript zum WiSe 2020/21; siehe https://info.mathematik.uni-stuttgart.de/Mathe-1-Inf-WiSe20.
- M. Geck, Mathematik I für inf, swt, msv. Skript zur Vorlesung im WiSe 2021/22; siehe https://pnp.mathematik.uni-stuttgart.de/idsr/idsr1/geckmf/SkriptMathInf1.pdf.

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/)
- Julia - The Julia Programming Language, siehe https://julialang.org

Einige weiterführende Texte (wird laufend ergänzt):

- S. Axler, Linear Algebra done right. Undergraduate Texts in Mathematics, Springer-Verlag, 2015.

- N. L. Biggs, Discrete Mathematics, 2nd Edition. Oxford University Press, 2002.
- 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.
- O. Forster, Analysis 1, 12. Auflage, Grundkurs Mathematik, Springer–Sektrum, 2016; e-Book frei verfügbar über https://doi.org/10.1007/978-3-658-11545-6.
- R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics: A foundation for Computer Science, 2nd edition, Addison–Wesley 1994.
- R. Haggarty, Principles of Mathematical Analysis, 2nd Edition. Prentice Hall, Addison–Wesley, 1993.
- P. R. Halmos, Naive Mengenlehre, Vandenhoeck & Ruprecht, 5. Auflage, 1994.
- B. Huppert und W. Willems, Lineare Algebra: Mit zahlreichen Anwendungen in Kryptographie, Codierungstheorie, Mathematischer Physik und Stochastischen Prozessen, Vieweg + Teubner Verlag, 2. Auflage 2010.
- M. Koecher, Lineare Algebra und analytische Geometrie (Neuauflage überarbeitet, aktualisiert und ergänzt), Grundwissen Mathematik, Springer–Verlag, 1985.
- 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[1]. Eine solche Zusammenfassung wird durch geschweifte Klammern $\{\ldots\}$ bezeichnet, zum Beispiel:

$S = \{$ alle Einwohner von Stuttgart $\}$,

$\mathcal{W} = \{$Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag$\}$,

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ die natürlichen Zahlen,

$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$ die natürlichen Zahlen mit 0,

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ die ganzen Zahlen.

Mengen können also nur eine bestimmte Anzahl von Elementen enthalten (wie im 1. und 2. Beispiel) oder auch unendlich viele Elemente (wie im 3., 4. und 5. 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 $A \subsetneqq B$. In unserem Beispiel oben gilt $\mathbb{N} \subsetneqq \mathbb{Z}$

[1] Der Begriff der Menge ist ein relativ junger Begriff in der Geschichte der Mathematik, der in den 1830er Jahren von Bolzano und Cantor eingeführt wurde. Siehe dazu https://de.wikipedia.org/wiki/Menge_(Mathematik).

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 14.10.2024 ist ein Montag" 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 V47.01. 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

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

die Menge der geraden 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.

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.

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 ist 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). Die (mengentheoretische)***Differenz*** von A und B ist definiert als

$$A \setminus B := \{x \in A \mid x \notin B\} \qquad \text{(lies: "}A \text{ ohne } B\text{")}.$$

Für $M \setminus B$ schreibt man auch B^c (***Komplement*** von B). 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 $\bigcup_{X \in B} X := \{a \in A \mid \text{es gibt ein } X \in B \text{ mit } a \in X\}$

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

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

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

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 ...

Mathematische Formulation: Nehmen wir an, wir könnten die Menge aller Mengen bilden; sei X diese Menge. Dann können wir auch die Menge $Y := \{A \in X \mid A \notin A\}$ bilden.

Frage: Gehört Y selbst zu Y oder nicht ?

Nun, wäre $Y \in Y$, so müsste nach Definition $Y \notin Y$ gelten; wäre $Y \notin Y$, so müsste $Y \in Y$ gelten.

D.h., in jedem Fall erhalten wir etwas, das zugleich wahr und falsch ist. Das Problem lag in der Annahme, dass wir X bilden können – diese Annahme ist allerdings auch durch keines der obigen Prinzipien erfasst.

2. *Beweistechniken und elementare Arithmetik*

Wir stellen grundlegende Beweistechniken vor und illustrieren diese durch einige Beispiele, in denen wichtige 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 ist

$$a \cdot m + b \cdot k = a \cdot (u \cdot n) + b \cdot (v \cdot n) = (a \cdot u) \cdot n + (b \cdot v) \cdot n = (a \cdot u + b \cdot v) \cdot n.$$

(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., $\neg P$. $\square$

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

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

Der "Trick" dieses Beweises besteht nun darin, auszunutzen, dass man die Reihenfolge in einer Summe von ganzen Zahlen beliebig ändern kann. Also gilt auch $S = n + (n-1) + \dots + 2 + 1$. 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
$$\begin{aligned} 2S = S + S &= (a_1 + a_2 + \dots + a_n) + (b_1 + b_2 + \dots + b_n) \\ &= (a_1 + b_1) + (a_2 + b_2) + \dots + (a_n + b_n) \qquad \text{(noch einmal der Trick!)} \\ &= \sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} \big(i + (n + 1 - i)\big) = \sum_{i=1}^{n} (n + 1) = n(n + 1). \end{aligned}$$

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 als "Axiom" formuliert, damit wir darauf verweisen und präzise damit argumentieren können.

Axiom 2.6 (***Peano's Induktionsaxiom***)**.** *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

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

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 Axioms zeigen wir folgende Aussage:

Satz 2.7 (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 Peano Axiom für einen formalen Beweis. Wir führen dies hier einmal explizit aus.

Beweis von Satz **??**. Sei zuerst $n \geqslant 0$. Dann betrachten wir die Menge

$$A := \{r \in \mathbb{N}_0 \mid \exists\, q \in \mathbb{N}_0 :\ r = n - qm\}.$$

Diese Menge ist nicht leer, denn z.B. können wir $q = 0$ setzen und erhalten $r = n - 0\cdot m = n \in A$. Nach Peano besitzt A also ein kleinstes Element; sei dieses r_0. Dazu gibt es ein $q_0 \in \mathbb{N}_0$ mit $r_0 = n - q_0 m$. Es gilt also $n = q_0 m + r_0$ und $r_0 \geqslant 0$.

Wir müssen noch zeigen, dass auch $r_0 < m$ gilt. Annahme, es wäre $r_0 \geqslant m$. Dann ist aber

$$r := n - (q_0 + 1)m = n - q_0 m - m = r_0 - m \geqslant 0, \qquad \text{also auch } r \in A.$$

Aber $r = r_0 - m < r_0$, und damit Widerspruch dazu, dass r_0 das kleinste Element von A ist. Also war die Annahme falsch, d.h., es gilt $n = q_0 m + r_0$ mit $q_0, r_0 \in \mathbb{N}_0$ und $0 \leqslant r_0 < m$.

Sei nun $n < 0$. Dann ist $-n > 0$, also wissen wir bereits, dass es $q_1, r_1 \in \mathbb{Z}$ gibt mit $-n = q_1 m + r_1$ und $0 \leqslant r_1 < m$. Dann ist $n = (-q_1)m - r_1$. Ist $r_1 = 0$, so sind wir fertig (mit $q := -q_1$ und $r := r_1 = 0$). Ist $r_1 \geqslant 1$, so erhalten wir

$$n = (-q_1)m - r_1 = (-q_1)m - m + m - r_1 = (-q_1 - 1)m + (m - r_1).$$

Mit $q := -q_1 - 1$ und $r := m - r_1$ ist $n = qm + r$ und $1 \leqslant r < m$, wie gewünscht.

Nur zur Eindeutigkeit von q, r: Es gelte also auch $n = q'm + r'$ mit $q', r' \in \mathbb{Z}$ und $0 \leqslant r' < m$. Behauptung: $q = q'$. Annahme, dies wäre falsch, also $q \neq q'$, d.h., $q < q'$ oder $q > q'$. Sei zuerst $q < q'$. Dann ist $q' - q > 0$ und damit $(q' - q)m \geqslant m$. Mit $qm + r = n = q'm + r'$ folgt auch $r - r' = q'm - qm = (q' - q)m \geqslant m$. Andererseits ist $r - r' \leqslant r < m$, Widerspruch. Analog erhält man einen Widerspruch für $q > q'$. Also war die Annahme falsch, d.h., es gilt $q = q'$ und damit auch $r = n - qm = n - q'm = r'$. □

Beispiel 2.8. Eine Anwendung: Prüfziffern bei IBAN

(Siehe https://de.wikipedia.org/wiki/Internationale_Bankkontonummer)

(Deutsche) Konto-Nr. 0356843503
Bankleitzahl (BLZ) 37010050

$\rightsquigarrow$ IBAN: DE12 $\underbrace{37010050}_{\text{BLZ}}$ $\underbrace{0356843503}_{\text{Konto-Nr.}}$

"DE" steht für das Land, die "Prüfziffer" 12 wird nach folgendem Verfahren berechnet:

- Schreibe BLZ, gefolgt von Konto-Nr., Land und 00: 370100500356843503DE00.
- Wandle Buchstaben in Zahlen um:

A	B	C	D	...	Z
10	11	12	13	...	35

- Berechne $37010050035684350313140\underline{0} \bmod 97 = 86$; ziehe dies von 98 ab; Ergebnis ist 12. (Falls Ergebnis einstellig, ergänze führende Null.)

Weiteres Beispiel: Formeln zur Berechnung des Osterdatums $\rightsquigarrow$ Übung 2.

Zurück zur allgemeinen Theorie. Seien $d, n \in \mathbb{Z}$ gegeben mit $d \neq 0$ und $n \neq 0$. Gilt $d \mid n$, so folgt natürlich auch $(-d) \mid n$. Um alle Teiler d von n zu bestimmen, brauchen wir also nur den Fall $d > 0$ zu betrachten. Sei nun $d > 0$. Aus $d \mid n$ folgt offenbar auch $d \leqslant |n|$ (= Absolutbetrag von n); also hat n nur endlich viele Teiler. Sind $n, m \in \mathbb{Z}$ mit $n \neq 0$ oder $m \neq 0$ gegeben, so definieren wir

$$\mathrm{ggT}(n, m) := \max\{a \in \mathbb{N} \mid a \text{ teilt } n \text{ und } a \text{ teilt } m\} \quad \text{„}\textbf{\textit{größter gemeinsamer Teiler}}\text{“}.$$

Gilt $\mathrm{ggT}(n, m) = 1$, so bezeichnen wir m und n als ***teilerfremd***.

Lemma 2.9 (Lemma von Bézout)**.** *Gegeben seien $n, m \in \mathbb{Z}$ mit $n \neq 0$ oder $m \neq 0$. Dann gibt es $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = an + bm$. Ist auch $d' \in \mathbb{Z}$ ein gemeinsamer Teiler von n und m, so folgt $d' \mid \mathrm{ggT}(n, m)$.*

Beweis. Ist $n = 0$ oder $m = 0$, so ist die Aussage sehr einfach zu sehen. (Ist z.B. $n = 0$ und $m < 0$, so ist $-m = \mathrm{ggT}(n, m) = 0 \cdot n + (-1) \cdot m$.) Sei also jetzt $n \neq 0$ und $m \neq 0$. Wir beschreiben einen Algorithmus, genannt (erweiterter) ***Euklidischer Algorithmus***, zur Bestimmung von $\mathrm{ggT}(n, m)$ und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = an + bm$. Dazu berechnen wir rekursiv eine endliche Folge von Tripeln (r_k, a_k, b_k) für $k = 0, 1, 2, 3, \ldots$, wie folgt. Ist $n > 0$ und $m > 0$, so initialisieren wir $r_0 := n,\ a_0 := 1,\ b_0 := 0$ und $r_1 := m,\ a_1 := 0,\ b_1 := 1$. (Ist $n < 0$, so setze $r_0 := -n, a_0 := -1, b_0 := 0$; ist $m < 0$, so setze $r_1 := -m$, $a_1 := 0$, $b_1 := -1$.) In jedem Fall gilt dann $r_0 = a_0 n + b_0 m \geqslant 1$ und $r_1 = a_1 n + b_1 m \geqslant 1$. Sei nun $k \geqslant 1$ und r_i, a_i, b_i bereits konstruiert für $0 \leqslant i \leqslant k$, wobei jeweils $r_i = a_i n + b_i m \geqslant 1$ gelte. Division mit Rest liefert

$$r_{k-1} = q_k r_k + r_{k+1} \qquad \text{mit} \qquad q_k, r_{k+1} \in \mathbb{Z} \quad \text{und} \quad 0 \leqslant r_{k+1} < r_k;$$

dies definiert r_{k+1}; dann setze $a_{k+1} := a_{k-1} - q_k a_k$ und $b_{k+1} := b_{k-1} - q_k b_k$. Damit gilt wieder

$$r_{k+1} = r_{k-1} - q_k r_k = (a_{k-1} n + b_{k-1} m) - q_k (a_k n + b_k m) = a_{k+1} n + b_{k+1} m.$$

Dieses Verfahren wird so lange fortgesetzt, bis $r_{k+1} = 0$ gilt. (Wegen $r_1 > r_2 > \ldots \geqslant 0$ muss es ein solches k geben. Hier ist wieder ein solcher Fall von "so lange ... bis"; überlegen Sie sich selbst, wie man dies hier mit Hilfe des Peano Axioms formal rechtfertigt.) Dann ist $r_k > 0$ und $r_{k-1} = q_k r_k$. Im vorherigen Schritt ist $r_{k-2} = q_{k-1} r_{k-1} + r_k$; wegen $r_k \mid r_{k-1}$ folgt also auch $r_k \mid r_{k-2}$. Dies setzt sich entsprechend in alle vorherigen Schritte fort, also gilt $r_k \mid r_i$ für $0 \leqslant i \leqslant k-1$. Insbesondere ist $r_k \mid n = \pm r_0$ und $r_k \mid m = \pm r_1$, also

$r_k \leqslant \mathrm{ggT}(n,m)$. Wegen $r_k = a_k n + b_k m$ folgt aber auch $d \mid r_k$ für jeden gemeinsamen Teiler d von n und m. Also ist $\mathrm{ggT}(n,m) = r_k = a_k n + b_k m$. (Für mehr Details siehe https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm). □

Sei zum Beispiel $n = 1071$ und $m = 462$. Dann initialisieren wir $r_0 = 1071$, $a_0 = 1$, $b_0 = 0$ und $r_1 = 462$, $a_1 = 0$, $b_1 = 1$. Das obige Verfahren liefert nun nacheinander:

$$\begin{aligned} r_0 &= 1071 = 2 \cdot 462 + 147 = q_1 r_1 + r_2, && \text{also } q_1 = 2,\ r_2 = 147 \text{ und } a_2 = 1,\ b_2 = -2, \\ r_1 &= \ \ 462 = 3 \cdot 147 + 21 \ \ = q_2 r_2 + r_3, && \text{also } q_2 = 3,\ r_3 = 21 \ \ \text{und } a_3 = -3,\ b_3 = 7, \\ r_2 &= \ \ 147 = 7 \cdot 21 + 0 \ \ \ \ = q_3 r_3 + r_4, && \text{also } q_3 = 7,\ r_4 = 0. \end{aligned}$$

Damit bricht das Verfahren bei $k = 3$ mit $r_3 = 21$, $a_3 = -3$, $b_3 = 7$ ab und wir erhalten $21 = \mathrm{ggT}(1071, 462) = (-3) \cdot 1071 + 7 \cdot 462$. Versuchen Sie, dieses Verfahren möglichst effizient zu programmieren (in Python oder einer beliebigen anderen Programmiersprache).

Als nächstes betrachten wir die ***rationalen Zahlen*** $\mathbb{Q}$. Zur Erinnerung:

- Jedes $x \in \mathbb{Q}$ lässt sich schreiben als Bruch $x = n/m$ mit $n \in \mathbb{Z}$ und $m \in \mathbb{N}$.
- Ist $x = n/m \in \mathbb{Q}$ und teilt man den Zähler und Nenner durch $\mathrm{ggT}(n,m)$, so erhält man einen "gekürzten" Bruch $x = n'/m'$ mit $n' \in \mathbb{Z}$, $m' \in \mathbb{N}$ und $\mathrm{ggT}(n',m') = 1$. (Beispiel: $2/3$ ist gekürzt, $4/6$ und $10/15$ sind nicht gekürzt.)
- Zwei Brüche $n/m \in \mathbb{Q}$ und $n'/m' \in \mathbb{Q}$ sind gleich genau dann, wenn sie auf den gleichen gekürzten Bruch führen. (Beispiel: $4/6 = 10/15$, denn sowohl $4/6$ als auch $10/15$ führen auf den gekürzten Bruch $2/3$.)
- Sei $x \in \mathbb{Q}$. Wir schreiben $x \geqslant 0$, falls $x = n/m$ mit $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$.
  Sind $x, y \in \mathbb{Q}$, so schreibe $x \leqslant y$ falls $y - x \geqslant 0$ $\quad\rightsquigarrow\quad$ Anordnung von $\mathbb{Q}$.

Hier ist nun das klassische Beispiel eines Widerspruchsbeweises.

Satz 2.10 (Euklid, etwa 3. Jahrhundert v. Chr.). *Es gibt keine positive rationale Zahl* $x \in \mathbb{Q}$ *mit* $x^2 = 2$.

Beweis. Nehmen wir an, es gibt doch ein $x \in \mathbb{Q}$ mit $x > 0$ und $x^2 = 2$. Wir versuchen, einen Widerspruch zu einer bekannten Aussage zu produzieren.

Wir nehmen eine gekürzte Bruchdarstellung $x = n/m$ mit $n, m \in \mathbb{N}$. Dann ist $2 = x^2 = (n/m)^2 = n^2/m^2$. Multiplizieren auf beiden Seiten mit m^2 ergibt $2m^2 = n^2$. Nun ist $2m^2$ gerade, also auch n^2. Mit Lemma ??(b) folgt, dass n auch selbst gerade ist, also gilt $n = 2l$ mit einem $l \in \mathbb{N}$. Dann ist aber $2m^2 = n^2 = (2l)^2 = 4l^2$. Hier können wir eine 2 auf beiden Seiten kürzen (siehe Lemma ??) und erhalten $m^2 = 2l^2$. Wie vorher folgt, dass m^2 gerade

und dann auch m selbst gerade ist. Also sind n und m gerade, d.h., beide durch $k = 2$ teilbar, im Widerspruch zur Annahme, dass $x = n/m$ gekürzt ist. □

3. *Vollständige Induktion und Primzahlen*

In der oben formulierten Fassung ist Peano's Induktionsaxiom oftmals etwas umständlich. Sehr nützlich ist folgende Variante.

Satz 3.1 (Vollständige Induktion)**.** *Sei $n_0 \in \mathbb{N}_0$ fest und für jedes $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ eine Aussage $P(n)$ gegeben. Die folgenden beiden Voraussetzungen seien erfüllt:*

(I1) *Induktionsanfang.* $P(n_0)$ *ist wahr.*

(I2) *Induktionsschritt.* $\forall n \in \mathbb{N}_0 : (n \geqslant n_0$ *und* $P(n)$ *wahr)* $\Rightarrow P(n+1)$ *wahr.*

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}_0$ mit $n \geqslant n_0$.

Beweis. Wir zeigen dies wieder mit einem Widerspruchbeweis. Angenommen, es gäbe ein $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ und so, dass $P(n)$ falsch ist. Dann ist

$$A := \{n \in \mathbb{N}_0 \mid n \geqslant n_0 \text{ und } P(n) \text{ ist falsch}\} \neq \varnothing.$$

Nach Peano's Induktionsaxiom besitzt A ein kleinstes Element; sei dieses k. Wegen (I1) ist $k > n_0$. Dann ist $k-1 \geqslant n_0$ und $k-1 \notin A$, d.h., $P(k-1)$ ist wahr.
Wende (I2) auf $n = k-1$ an. Es folgt, dass auch $P(k)$ wahr ist, Widerspruch. □

Als Beispiel geben wir einen neuen Beweis von Satz **??**, wobei wir für $n \in \mathbb{N}$ die folgende Aussage betrachten:

$$P(n): \quad 1 + 2 + \ldots + n = \tfrac{1}{2}n(n+1).$$

Startwert ist hier $n_0 = 1$. Wir müssen nun nachweisen, dass (I1) und (I2) erfüllt sind.

Zu (I1), Induktionsanfang: Ist $n = n_0 = 1$, so ist die linke Seite von $P(1)$ gleich 1 und die rechte Seite gleich $\frac{1}{2}(1+1) = 1$. Also ist $P(1)$ wahr.

Zu (I2), Induktionsschritt: Sei $n \in \mathbb{N}_0$ mit $n \geqslant n_0 = 1$ beliebig. Wir nehmen an, dass $P(n)$ wahr ist und müssen dann zeigen, dass auch $P(n+1)$ wahr ist.

Beginnen wir mit der linken Seite von $P(n+1)$ und formen diese um:

$$\begin{aligned} 1 + 2 + \ldots + (n+1) &= (1 + 2 + \ldots + n) + (n+1) \\ &= \tfrac{1}{2}n(n+1) + (n+1) \quad \text{(da } P(n) \text{ als wahr vorausgesetzt ist)}, \\ &= \tfrac{1}{2}(n^2 + n) + \tfrac{1}{2}(2n+2) = \tfrac{1}{2}(n^2 + 3n + 2). \end{aligned}$$

Andererseits ist die rechte Seite von $P(n+1)$ gleich

$$\tfrac{1}{2}(n+1)\big((n+1)+1\big) = \tfrac{1}{2}(n+1)(n+2) = \tfrac{1}{2}(n^2 + 3n + 2).$$

Also erhalten wir das gleiche Ergebnis wie vorher; damit ist (I2) gezeigt. Mit Satz **??** folgt also, dass $P(n)$ für alle $n \geqslant 1$ wahr ist.

Bemerkung 3.2. Wir sehen hier gleichzeitig eine Stärke und eine Schwäche der vollständigen Induktion. Ist bereits bekannt, was man zeigen will, so ist dies eine sehr effiziente Beweismethode. Wenn man allerdings die Formel noch nicht kennt und erst herausfinden muss, so benötigt man in der Tat einen "Trick" – wie im ursprünglichen Beweis von Satz **??**. Versuchen Sie etwa, Formeln für $1^2 + 2^2 + \cdots + n^2$ und $1^3 + 2^3 + \cdots + n^3$ zu finden. (Siehe dazu auch https://de.wikipedia.org/wiki/Faulhabersche_Formel.)

Die folgende Variante der vollständigen Induktion ist ebenfalls sehr oft nützlich.

Satz 3.3 (Starke vollständige Induktion)**.** *Sei $n_0 \in \mathbb{N}_0$ fest und für jedes $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ eine Aussage $P(n)$ gegeben. Die folgenden beiden Voraussetzungen seien erfüllt:*

(SI1) *$P(n_0)$ ist wahr.*

(SI2) *$\forall n \in \mathbb{N}_0 : \big(P(m)$ wahr für alle $m \in \mathbb{N}_0$ mit $n_0 \leqslant m < n\big) \Rightarrow P(n)$ wahr.*

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}_0$ mit $n \geqslant n_0$.

Beweis. Wir brauchen nur den Beweis von Satz **??** etwas zu verändern. Angenommen, es wäre $A := \{n \in \mathbb{N}_0 \mid n \geqslant n_0$ und $P(n)$ ist falsch$\} \neq \varnothing$. Nach Peano besitzt A ein kleinstes Element; sei dieses k. Wegen (SI1) ist $k > n_0$. Sei nun $m \in \{n_0, n_0 + 1, \ldots, k - 1\}$. Dann ist $m \notin A$, d.h., $P(m)$ ist wahr. Mit (SI2) angewandt auf $n = k$ folgt, dass auch $P(k)$ wahr ist, Widerspruch. □

Definition 3.4. Sei $n \in \mathbb{N}$, $n \geqslant 2$. Dann heißt n eine ***Primzahl***, wenn n nur durch 1 und sich selbst teilbar ist.

Zum Beispiel sind $2, 3, 5, 7, 11$ Primzahlen, aber 1 und 12 sind keine Primzahlen.

Satz 3.5 (Primfaktorzerlegung in $\mathbb{N}$)**.** *Sei $n \in \mathbb{N}$, $n \geqslant 2$. Dann lässt sich n als Produkt von Primzahlen schreiben; es gibt also $r \geqslant 1$ Primzahlen $p_1, p_2, \ldots, p_r$ mit $n = p_1 p_2 \cdots p_r$ und $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$.*

Beweis. (Starke Induktion mit $n_0 = 2$.) Für $n \geqslant 2$ betrachten wir die Aussage:

$$P(n): \quad \text{"}n \text{ ist Produkt von Primzahlen"}.$$

Wir müssen zeigen, dass die Voraussetzungen (SI1) und (SI2) erfüllt sind.

Zu (SI1): Sei also $n = n_0 = 2$. Da 2 eine Primzahl ist, ist $n = 2$ offenbar auch ein Produkt von Primzahlen (mit nur einem Faktor).

Zu (SI2): Sei $n > 2$ und vorausgesetzt, dass $P(m)$ wahr ist für $m = 2, 3, \ldots, n - 1$. Wir müssen dann zeigen, dass $P(n)$ wahr ist. Dazu unterscheiden wir zwei Fälle.

1. Fall: n ist selbst eine Primzahl. Dann ist (siehe oben) n offenbar auch ein Produkt von Primzahlen (mit nur einem Faktor), also die Behauptung gezeigt.

2. Fall: n ist keine Primzahl. Nach Definition einer Primzahl bedeutet dies, dass $n = ab$ gilt

mit $a, b \in \mathbb{N}$ und $2 \leqslant a, b \leqslant n-1$. Nach Voraussetzung sind $P(a)$ und $P(b)$ wahr, also sind a und b Produkte von Primzahlen. Wir schreiben $a = p_1 p_2 \cdots p_r$ und $b = q_1 q_2 \cdots q_s$ mit $r, s \geqslant 1$ und Primzahlen p_i, q_j.
Dann ist aber auch $n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ ein Produkt von Primzahlen (mit $r+s$ Faktoren). Schließlich sortieren wir die Faktoren im Endprodukt der Größe nach um. □

Satz 3.6 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Dies ist wieder ein klassisches Beispiel eines Widerspruchsbeweises. Angenommen, es gäbe nur endlich viele Primzahlen; seien diese $p_1, p_2, \ldots, p_r$.
Damit bilden wir $N := p_1 p_2 \cdots p_r + 1 \in \mathbb{N}$. (Dies ist der Trick des Beweises.) Es gilt sicherlich $N \geqslant 2$, also besitzt N nach Satz ?? eine Primfaktorzerlegung. In dieser können aber nur die Primzahlen $p_1, \ldots, p_r$ vorkommen, und mindestens eine kommt vor. Es gibt also ein $i \in \{1, \ldots, r\}$ mit $p_i \mid N$. Andererseits ist $N - 1 = p_1 p_2 \cdots p_r$, also gilt $p_i \mid N - 1$. Mit Lemma ??(b) folgt dann aber auch $p_i \mid N - (N-1) = 1$, also $p_i = 1$, Widerspruch. □

Bemerkung 3.7. Für $n \in \mathbb{N}$ sei p_n die n-te Primzahl. Zum Beispiel $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, …, $p_{100} = 541$, … Es ist keine allgemeine Formel bekannt, mit der man zu beliebigem n die entsprechende Primzahl p_n berechnen könnte.
Pierre de Fermat vermutete um 1640, dass $F_n := 2^{2^n}+1$ eine Primzahl ist für alle $n \in \mathbb{N}_0$.

n	F_n	
0	3	ok
1	5	ok
2	17	ok
3	257	ok
4	65537	ok
5	$2^{32}+1 = 4294967297$	nicht ok: $641 \cdot 6700417$ (Leonhard Euler 1732)

Es ist bekannt, dass $F_5, \ldots, F_{32}$ keine Primzahlen sind. Für größere Werte von n ist nicht bekannt, ob F_n eine Primzahl ist oder nicht.

Lemma 3.8 ("Lemma von Euklid")**.** *Sei $p \in \mathbb{N}$ eine Primzahl und seien $a, b \in \mathbb{N}$. Gilt $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.*

Das Lemma von Euklid kommt in nahezu jeder Argumentation mit Primzahlen vor; es ist genau das "richtige" technische Hilfsmittel.

Beispiel. In Lemma ?? haben wir gezeigt: "n ungerade $\Rightarrow n^2$ ungerade" und dann mit Kontraposition geschlossen: "n^2 gerade $\Rightarrow n$ gerade". Mit dem Lemma von Euklid folgt dies auch direkt: Ist n^2 gerade, so gilt $2 \mid n^2 = nn$, also folgt $2 \mid n$.

Beweis von Lemma ??. Seien $a, b \in \mathbb{N}$ gegeben mit $p \mid ab$. Nehmen wir an, es gilt $p \nmid a$. Dann müssen wir $p \mid b$ zeigen. Da p nur die Teiler 1 und p hat, ist $\mathrm{ggT}(p, a) = 1$ oder p. Also

$\mathrm{ggT}(p, a) = 1$ wegen $p \nmid a$. Nach dem ***Lemma von Bézout*** gibt es $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Multiplikation mit b ergibt $b = rpb + sab$. Wegen $p \mid rpb$ und $p \mid sab$ folgt mit Lemma **??**, dass auch $p \mid rpb + sab = b$ gilt. □

Folgerung 3.9. *Sei $p \in \mathbb{N}$ eine Primzahl, $n \in \mathbb{N}$ und seien $c_1, \ldots, c_n \in \mathbb{N}$.*
Gilt $p \mid c_1 c_2 \cdots c_n$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $p \mid c_i$.

Beweis. (Vollständige Induktion über n mit Startwert $n_0 = 1$.) Induktionsanfang: Sei $n = 1$, also ist nur eine Zahl c_1 gegeben mit $p \mid c_1$. Dann gilt die Aussage. (Es ist nichts zu zeigen.)

Induktionsschritt: Sei $n \geqslant 1$ und angenommen, dass die Aussage bereits für n Zahlen gilt. Dann müssen wir zeigen, dass sie auch für $n+1$ Zahlen gilt. Gegeben seien also $c_1, \ldots, c_{n+1} \in \mathbb{N}$ mit $p \mid c_1 c_2 \ldots c_{n+1}$. Setze nun $a := c_1 c_2 \cdots c_n$. Dann ist $c_1 c_2 \cdots c_{n+1} = a c_{n+1}$ und $p \mid a c_{n+1}$. Nach Lemma **??** folgt also $p \mid a$ oder $p \mid c_{n+1}$. Im 2. Fall sind wir fertig. Im 1. Fall gilt $p \mid c_1 \cdots c_n$, also gibt es nach Induktionsannahme ein $i \in \{1, \ldots, n\}$ mit $p \mid c_i$, und wir sind wieder fertig. □

Satz 3.10 (Hauptsatz der elementaren Arithmetik)**.** *Die Primfaktorzerlegung einer natürlichen Zahl $n \geqslant 2$ (siehe Satz **??**) ist eindeutig.*

Beweis. (Starke Induktion mit Startwert $n_0 = 2$.) Für $n \in \mathbb{N}$, $n \geqslant 2$, ist folgende Aussage $P(n)$ zu beweisen:

> "Gegeben seien Primzahlen $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$ und $q_1 \leqslant q_2 \leqslant \ldots \leqslant q_s$ (wobei $r, s \geqslant 1$) mit $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. Dann gilt $r = s$ und $p_i = q_i$ für $1 \leqslant i \leqslant r$."

Induktionsanfang: Sei $n = 2$. Dann ist n selbst eine Primzahl, und die Aussage ist klar nach Definition einer Primzahl.
Induktionsschritt: Sei $n > 2$ und angenommen, dass $P(m)$ bereits gilt für alle m mit $2 \leqslant m < n$. Dann müssen wir zeigen, dass auch $P(n)$ gilt. Ist n selbst eine Primzahl, so ist die Aussage wieder klar nach Definition einer Primzahl. Sei also nun n keine Primzahl und betrachten wir zwei Faktorisierungen wie oben:

$$(*) \qquad n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (\text{mit } r, s \geqslant 2).$$

1. Fall: $p_1 = q_1$. Dann können wir p_1 auf beiden Seiten kürzen und erhalten $m := p_2 \cdots p_r = q_2 \cdots q_s$. Wegen $2 \leqslant m < n$ ist $P(m)$ nach Induktionsannahme wahr, also $r = s$ und $p_i = q_i$ für $2 \leqslant i \leqslant r$. Da auch $p_1 = q_1$ gilt, ist also $P(n)$ wahr.
2. Fall: $p_1 < q_1$. Nun ist $p_1 \mid p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, also gibt es nach Folgerung **??** ein $i \in \{1, \ldots, s\}$ mit $p_1 \mid q_i$. Aber p_1 und q_i sind Primzahlen, also muss $p_1 = q_i$ gelten. Andererseits ist $p_1 < q_1 \leqslant q_2 \leqslant \ldots \leqslant q_i$, also $p_1 < q_i$, Widerspruch.
3. Fall: $p_1 > q_1$. Man erhält Widerspruch völlig analog zum 2. Fall. (Es ist $q_1 \mid p_1 \cdots p_r$ usw.)

Also treten der 2. und 3. Fall gar nicht auf. □

4. *Relationen und Restklassen*

Wir führen eine weitere grundlegende mengentheoretische Konstruktion ein. Das ***kartesische Produkt*** von zwei nicht-leeren Mengen A und B wird mit $A \times B$ bezeichnet. Dies ist eine Menge, die aus allen Paaren (a, b) mit $a \in A$ und $b \in B$ besteht:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Für zwei Paare (a, b) und (a', b') gilt $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$. (Formal korrekt wird das Paar (a, b) als die Menge $\{a, \{a, b\}\}$ definiert.) Zum Beispiel ist

$$\{1, 2\} \times \{2, 3, 4\} = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}.$$

Beachten Sie, dass die Reihenfolge wichtig ist: $(2, 4)$ ist nicht das Gleiche wie $(4, 2)$. Sie sind vermutlich vertraut mit dem kartesischen Produkt $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, das man sich üblicherweise als Ebene mit 2 Koordinatenachsen vorstellt.

Definition 4.1. Sind A, B nicht-leere Mengen, so heißt eine Teilmenge $R \subseteq A \times B$ eine ***Relation*** auf A und B. Für $a \in A$ und $b \in B$ schreiben wir $a \sim b$, wenn $(a, b) \in R$ gilt (und sagen: "a steht in Relation zu b"). Ist $A = B$, so heißt R eine Relation auf A.

Beispiel 4.2. (a) Sei A die Menge aller Punkte der Ebene und B die Menge aller Geraden in der Ebene. Die Eigenschaft, dass ein Punkt auf einer Geraden liegt, definiert eine Relation:

$$R = \{(a, b) \in A \times B \mid \text{Der Punkt } a \text{ liegt auf der Geraden } b\}.$$

(b) Hier sind Beispiele von Relationen auf $A = B = \mathbb{Z}$:

$$R_1 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n < m\},$$
$$R_2 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid \ n \text{ teilt } m\},$$
$$R_3 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid \ n = m \text{ oder } n + m \geqslant 0\}.$$

Beispiel 4.3. Sei wieder $A = B = \mathbb{Z}$. Für festes $m \in \mathbb{N}$ definieren wir die Relation

$$R_m := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod m = b \bmod m\}.$$

Es gilt hier also $a \sim b$ genau dann, wenn a und b den gleichen Rest bei Division durch m haben. Wir behaupten, dass diese Relation auch wie folgt charakterisiert werden kann:

$$(a, b) \in R_m \qquad \Leftrightarrow \qquad m \mid b - a. \tag{$*$}$$

Beweis von $(*)$: Seien $a, b \in \mathbb{Z}$. Es gibt $q, q', r, r' \in \mathbb{Z}$ mit $a = qm + r$, $b = q'm + r'$ und $0 \leqslant r, r' < m$. Sei zuerst $(a, b) \in R_m$, d.h., $r = r'$. Dann folgt $a - qm = r = r' = b - q'm$ und damit $b - a = (q' - q)m$; also ist $m \mid b - a$. Sei umgekehrt $m \mid b - a$, also $b - a = cm$ mit $c \in \mathbb{Z}$, also $b = cm + a = cm + qm + r = (c + q)m + r$. Aus der Eindeutigkeit des Restes folgt also $r = r'$ und damit $(a, b) \in R_m$. □

Anstelle von $(n, n') \in R_m$ schreiben wir künftig $n \equiv n' \pmod{m}$.
Dies wird gelesen als: "n und n' sind ***kongruent modulo*** m."
Ist etwa $m = 2$ und $n \in \mathbb{Z}$ beliebig, so ist der Rest $n \bmod 2$ entweder 0 oder 1. Also:

$$n \bmod 2 = 0 \quad \Leftrightarrow \quad n \equiv 0 \pmod{2} \quad \Leftrightarrow \quad n \text{ ist gerade,}$$
$$n \bmod 2 = 1 \quad \Leftrightarrow \quad n \equiv 1 \pmod{2} \quad \Leftrightarrow \quad n \text{ ist ungerade.}$$

Definition 4.4. Sei A eine nicht-leere Menge und $R \subseteq A \times A$ eine Relation auf A, geschrieben $a \sim b$ für $a, b \in A$. Die Relation R heißt:

- ***reflexiv***, wenn $a \sim a$ für alle $a \in A$ gilt;
- ***symmetrisch***, wenn für $a, b \in A$ aus $a \sim b$ stets $b \sim a$ folgt;
- ***anti-symmetrisch***, wenn für $a, b \in A$ aus $a \sim b$ und $b \sim a$ stets $a = b$ folgt;
- ***transitiv***, wenn für $a, b, c \in A$ aus $a \sim b$ und $b \sim c$ stets $a \sim c$ folgt.

Ist R reflexiv, symmetrisch und transitiv, so heißt R eine ***Äquivalenzrelation***.
Ist R reflexiv, anti-symmetrisch und transitiv, so heißt R eine ***Ordnungsrelation***.

Beispiel 4.5. (a) Sei $A = \mathbb{Z}$ und betrachte die Relationen R_1, R_2, R_3 in Beispiel **??**(b).

$R_1 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n < m\}$ ist transitiv, aber weder reflexiv noch symmetrisch;

$R_2 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n \text{ teilt } m\}$ ist transitiv, reflexiv aber nicht symmetrisch;

$R_3 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n = m \text{ oder } n + m \geqslant 0\}$ ist reflexiv, symmetrisch, aber nicht transitiv (denn z.B. $(-1, 2) \in R_3$, $(2, 0) \in R_3$, aber $(-1, 0) \notin R_3$).

(b) Die übliche Relation "$\leqslant$" auf $A = \mathbb{Z}$ ist eine Ordnungsrelation.

(c) Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$ fest. Wir behaupten, dass die Kongruenz-Relation R_m in Beispiel **??** eine Äquivalenzrelation ist. Prüfen wir dies nach. Die Relation ist

- reflexiv, denn $m \mid a - a = 0$, also $a \sim a$;
- symmetrisch, denn aus $a \sim b$ folgt $m \mid b - a$ und damit auch $m \mid -(b - a) = a - b$ (siehe Lemma **??**(b)), also $b \sim a$;
- transitiv, denn aus $a \sim b$ und $b \sim c$ folgt $m \mid b - a$ und $m \mid c - b$; also auch $m \mid (c - b) + (b - a) = c - a$ (siehe Lemma **??**(b)) und damit $a \sim c$.

Definition 4.6. Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Für $a \in A$ heißt dann

$$K(a, R) := \{b \in A \mid (a, b) \in R\}$$

die ***Äquivalenzklasse*** von a. Dies ist also eine Teilmenge von A, d.h., ein Element von $\mathcal{P}(A)$. Sei $\mathcal{K}(A, R)$ die Menge aller Äquivalenzklassen von Elementen in A, d.h.,

$$\mathcal{K}(A, R) = \{S \in \mathcal{P}(A) \mid \exists a \in A : S = K(a, R)\}.$$

Sei zum Beispiel A die Menge aller Menschen auf dem Planeten Erde und

$$R = \{(a, b) \in A \times A \mid a \text{ und } b \text{ leben im gleichen Land}\}.$$

Sie überprüfen leicht, dass dies eine Äquivalenzrelation ist. Eine Äquivalenzklasse besteht genau aus allen Menschen, die in einem Land leben. Die Menge der Äquivalenzklassen entspricht also den verschiedenen Ländern.

In Beispiel **??** mit $m = 2$ ist $K(0, R_2)$ = Menge aller geraden Zahlen und $K(1, R_2)$ = Menge aller ungeraden Zahlen. Also $\mathcal{K}(\mathbb{Z}, R_2) = \{K(0, R_2), K(1, R_2)\}$.

Satz 4.7. *Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Dann gilt:*
(a) *Jedes $a \in A$ liegt in einer Äquivalenzklasse.*
(b) *Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.*
("disjunkt" bedeutet: der Durchschnitt ist leer).

Beweis. (a) Sei $a \in A$. Da R reflexiv ist, gilt $a \sim a$ also $a \in K(a, R)$.

(b) Seien $a, b \in A$ und $K_a = K(a, R)$, $K_b = K(b, R)$. Nehmen wir an, es ist $K_a \cap K_b \neq \varnothing$. Dann müssen wir zeigen, dass $K_a = K_b$ gilt. Sei dazu $d \in K_a \cap K_b$.

Ist $c \in K_a$ beliebig, so gilt $a \sim c$. Wegen $d \in K_a$ ist $a \sim d$ und wegen der Symmetrie dann auch $d \sim a$. Mit der Transitivität folgt $d \sim c$. Wegen $d \in K_b$ gilt $b \sim d$, also folgt mit der Transitivität schließlich $b \sim c$, d.h., $c \in K_b$. Damit ist gezeigt, dass $K_a \subseteq K_b$ gilt. Auf völlig analoge Weise wird $K_b \subseteq K_a$ gezeigt. Also gilt $K_a = K_b$, wie behauptet. □

Für $a \in A$ sei $K_a = K(a, R) = \{b \in A \mid (a, b) \in R\}$ die Äquivalenzklasse von a.
Der letzte Satz zeigt: A ist Vereinigung aller Äquivalenzklassen. In dieser Vereinigung sind im Allgemeinen viele Terme gleich. Sind $a, b \in A$, so gilt $K_a = K_b \Leftrightarrow b \in K_a$.

Definition 4.8. Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Teilmenge $B \subseteq A$ heißt ***Repräsentantensystem der Äquivalenzklassen***, wenn es zu jedem $a \in A$ genau ein $b \in B$ gibt mit $(b, a) \in R$. Oder anders ausgedrückt:

$$A = \bigcup_{b \in B} K(b, R), \quad \text{und in dieser Vereinigung sind die Terme alle disjunkt.}$$

Beispiel 4.9 (Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$)**.** Sei $A = \mathbb{Z} \times \mathbb{N}$ und betrachte folgende Relation:

$$R := \big\{\big((n, m), (n', m')\big) \in A \times A \mid nm' = n'm\big\}.$$

(Nach Übung 3 ist dies eine Äquivalenzrelation.) Für $(n, m) \in A$ schreiben wir anstelle von $K((n, m), R)$ einfach kurz n/m. Mit Hilfe des ggT sieht man leicht, dass jede Äquivalenzklasse ein *gekürztes* Paar (n, m) enthält, d.h., es gibt keine natürliche Zahl $k > 1$ mit $k \mid n$ und $k \mid m$. Nach Übung 3 ist ein Repräsentantensystem der Äquivalenzklassen gegeben durch

$$B := \{(n, m) \in A \mid (n, m) \text{ ist gekürzt}\},$$

d.h., die Äquivalenzklassen entspechen genau den ***rationalen Zahlen*** ! Auf diese Weise erhält man in der Tat eine mathematisch korrekte Konstruktion: *Man definiert* $\mathbb{Q} := \mathcal{K}(A, R)$.

Eine Gleichheit wie $2/3 = 4/6 = 100/150$ entspricht dann einfach der Tatsache, dass die Paare $(2, 3)$, $(4, 6)$, $(100, 150)$ zur gleichen Äquivalenzklasse gehören.
Ist $n \in \mathbb{Z}$, so schreiben wir einfach n anstelle von $n/1$. Vermöge dieser Identifizierung ist dann $\mathbb{Z} \subseteq \mathbb{Q}$. (Überlegen Sie sich selbst, wie man auf ähnliche Weise $\mathbb{Z}$ aus $\mathbb{N}$ konstruiert.)

Beispiel 4.10. Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$. Die Äquivalenzklassen bezüglich der Äquivalenzrelation R_m (siehe Beispiel **??**) werden auch als ***Restklassen*** (modulo m) bezeichnet.
Sofern m fest vorgegeben ist, werden wir die Restklasse von $n \in \mathbb{Z}$ einfach mit $\overline{n}$ bezeichnen, also $\overline{n} = \{a \in \mathbb{Z} \mid m \text{ teilt } n - a\} = \{a \in \mathbb{Z} \mid a \bmod m = n \bmod m\}$.

Repräsentantensystem? Ein solches ist gegeben durch $B = \{0, 1, 2, \ldots, m - 1\}$, denn bei der Division mit Rest durch m kommen nur die Reste $0, 1, 2, \ldots, m - 1$ vor (und der Rest ist eindeutig bestimmt). Anders formuliert: Für jedes $n \in \mathbb{Z}$ gibt es genau ein $r \in B$ mit $n \bmod m = r$, also $n \in \overline{r}$ und $\overline{n} = \overline{r}$. Es gilt also

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \ldots \cup \overline{(m-1)} \qquad \text{(disjunkte Vereinigung)}.$$

Ist etwa $m = 5$, so gilt $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$.
Es ist $-17 \in \overline{3}$ und $38 \in \overline{3}$ (weil -17 und 38 beide den Rest 3 modulo 5 haben).

Genauso, wie man Brüche (also letztlich gewisse Äquivalenzklassen) addieren und multiplizieren kann, werden wir sehen, dass man auch Restklassen modulo m addieren und multiplizieren kann. Grundlage dafür ist:

Lemma 4.11. *Sei $m \in \mathbb{N}$. Wie oben bezeichnen wir die Restklasse (modulo m) von $n \in \mathbb{Z}$ mit $\overline{n}$. Seien $a, b, c, d \in \mathbb{Z}$. Gilt $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$, so folgt $\overline{a + b} = \overline{c + d}$ und $\overline{ab} = \overline{cd}$.*

Beweis. Sei $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$, also $m \mid c - a$ und $m \mid d - b$. Seien $r, s \in \mathbb{Z}$ mit $c - a = rm$ und $d - b = sm$, also $c = a + rm$ und $d = b + sm$. Damit erhalten wir

$$(c + d) - (a + b) = (a + rm) + (b + sm) - a - b = rm + sm = (r + s)m,$$

also $m \mid (c + d) - (a + b)$, d.h., $\overline{a + b} = \overline{c + d}$. Außerdem ist

$$\begin{aligned} cd - ab &= (a + rm)(b + sm) - ab = (ab + asm + rmb + rmsm) - ab \\ &= asm + rmb + rmsm = (as + rb + rsm)m, \end{aligned}$$

also $m \mid cd - ab$, d.h., $\overline{ab} = \overline{cd}$. □

Sei zum Beispiel $m = 6$. Wir wollen $(17 \cdot 14) \bmod 6$ berechnen.
Dazu: Es gilt $17 \bmod 6 = 5$ und $14 \bmod 6 = 2$, also $\overline{17} = \overline{5}$ und $\overline{14} = \overline{2}$. Damit

$$\overline{17 \cdot 14} = \overline{5 \cdot 2} = \overline{10} = \overline{4}$$

wobei wir Lemma **??** für die 1. Gleichheit benutzt haben. Also gilt $(17 \cdot 14) \bmod 6 = 4$. (Man muss also nicht erst $17 \cdot 14$ ausrechnen und dann mit Rest durch 6 teilen.)

Beispiel 4.12. Ist 7513 durch 3 teilbar? Nach der (vielleicht bekannten) ***Dreierregel*** müssten wir uns dazu nur die Quersumme von 7513 anschauen:
Diese ist $7 + 5 + 1 + 3 = 16$, und wegen $3 \nmid 16$ folgt auch $3 \nmid 7513$.

Begründung: Sei $m = 3$ und betrachte $\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3}$.
Nun ist $10 \bmod 3 = 1$, also $\overline{10} = \overline{1}$. Mit Lemma **??** folgt daher auch $\overline{100} = \overline{10 \cdot 10} = \overline{1 \cdot 1} = \overline{1}$; genauso $\overline{1000} = \overline{10 \cdot 100} = \overline{1 \cdot 1} = \overline{1}$, und damit

$$\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3} = \overline{7 \cdot 1 + 5 \cdot 1 + 1 \cdot 1 + 3} = \overline{7 + 5 + 1 + 3} = \overline{16}.$$

D.h., die Zahl 7513 hat den gleichen Rest (modulo 3) wie ihre Quersumme.

5. *Abbildungen und die Mächtigkeit von Mengen*

Seien A, B nicht-leere Mengen. Eine ***Abbildung*** f von A nach B ist eine Zuordnung, die jedem Element von A genau ein Element von B zuordnet. In Zeichen $f\colon A \to B, \quad a \mapsto f(a)$.

Das ***Bild*** von f ist definiert als $\mathrm{Bild}(f) := \{b \in B \mid \exists a \in A : f(a) = b\}$. Für eine beliebige Teilmenge $A' \subseteq A$ sei $f(A') := \{b \in B \mid \exists a \in A' : f(a) = b\}$. Damit ist also $\mathrm{Bild}(f) = f(A)$.

Die Abbildung f heißt ***surjektiv***, wenn $f(A) = B$ gilt.
Die Abbildung f heißt ***injektiv***, wenn für alle $a, a' \in A$ gilt: Aus $f(a) = f(a')$ folgt $a = a'$. (Oder umgekehrt: Gilt $a \neq a'$, so auch $f(a) \neq f(a')$.)
Die Abbildung heißt ***bijektiv***, wenn sie sowohl injektiv als auch surjektiv ist.

Ist $A = \mathbb{N}$, so bezeichnet man f auch als ***Folge*** und schreibt vereinfachend $f = (a_n)_{n \in \mathbb{N}}$, wobei $a_n = f(n)$ für alle $n \in \mathbb{N}$. (Analog für $A = \mathbb{N}_0$.)

Bemerkung 5.1. (a) Implizit haben wir bereits Abbildungen betrachtet. Zum Beispiel ist die Addition in $\mathbb{N}$ eine Abbildung $\alpha\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, n') \mapsto n + n'$.

(b) Ist $f\colon A \to B$ eine Abbildung, so heißt $\mathcal{G}(f) := \{(a, f(a)) \mid a \in A\} \subseteq A \times B$ der ***Graph*** von f. Dies ist also eine Relation auf $A \times B$.

(c) Umgekehrt: Formal korrekt ist eine Abbildung $f\colon A \to B$ durch eine Relation $R \subseteq A \times B$ gegeben, welche folgende Bedingungen erfüllt:

(i) Zu jedem $a \in A$ gibt es ein $b \in B$ mit $(a, b) \in R$;

(ii) sind $a \in A$ und $b, b' \in B$ mit $(a, b) \in R$ und $(a, b') \in R$ gegeben, so folgt $b = b'$.

Diese beiden Bedingungen besagen gerade, dass zu jedem $a \in A$ genau ein $b \in B$ gehört, und dieses b wird dann mit $f(a)$ bezeichnet. Dann ist $R = \mathcal{G}(f)$.
Also: Eine Abbildung $f\colon A \to B$ ist eine Relation mit speziellen Eigenschaften.

Beispiel 5.2. (a) Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$, ist weder injektiv noch surjektiv, denn es gilt zum Beispiel $f(1) = 1 = f(-1)$ und $2 \notin f(\mathbb{Z})$.

(b) Sei $A = \{n \in \mathbb{Z} \mid n \text{ gerade}\}$ und $B = \{n \in \mathbb{Z} \mid n \text{ ungerade}\}$. Dann erhalten wir eine Abbildung $f\colon A \to B$, $n \mapsto n+1$. Diese Abbildung ist bijektiv (wie Sie selbst leicht zeigen).

(c) Die Abbildung $f\colon \mathbb{N}_0 \to \mathbb{N}_0$, $n \mapsto 2n$, ist injektiv aber nicht surjektiv.

(d) Seien $k, n \in \mathbb{N}_0$. Dann ist $2^k(2n+1) \geqslant 1$, also $2^k(2n+1) - 1 \in \mathbb{N}_0$. Damit erhalten wir eine Abbildung $\quad f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, \qquad (k,n) \mapsto 2^k(2n+1) - 1$.
Wir überlassen es als Übung zu zeigen, dass diese Abbildung bijektiv ist.

Definition 5.3. Seien A, B nicht-leere Mengen und $f\colon A \to B$ eine Abbildung.
Für $b \in B$ heißt $f^{-1}(b) := \{a \in A \mid f(a) = b\}$ das ***Urbild*** von b. Allgemeiner:
Ist $B' \subseteq B$ eine Teilmenge, so ist $f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$ das Urbild von B'.

- Sei $b \in B$. Dann gilt: $\quad f^{-1}(b) \neq \varnothing \quad \Leftrightarrow \quad b \in f(A)$.

Beispiel: Für $f\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$, gilt $f^{-1}(3) = \varnothing$.

- Ist f injektiv und $b \in f(A)$, so gilt $|f^{-1}(b)| = 1$.
- Seien $b, b' \in B$ und $b \neq b'$. Dann ist $f^{-1}(b) \cap f^{-1}(b') = \varnothing$.
- Sei f surjektiv. Dann ist $f^{-1}(b) \neq \varnothing$ für alle $b \in B$ und $A = \bigcup_{b \in B} f^{-1}(b)$.

Beispiel: $f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, $(n,m) \mapsto n+m$, ist surjektiv. Es gilt
$f^{-1}(0) = \{(0,0)\}$, $\quad f^{-1}(2) = \{(2,0),(1,1),(0,2)\}$,
$f^{-1}(\{\text{gerade Zahlen}\}) = \{(n,m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n, m \text{ beide gerade oder } n, m \text{ beide ungerade}\}$.

Definition 5.4. Seien A, B, C nicht-leere Mengen und $f\colon A \to B$, $g\colon B \to C$ Abbildungen.
Durch ***Hintereinanderausführung*** erhalten wir auch eine Abbildung

$$g \circ f\colon A \to C, \qquad a \mapsto g\big(f(a)\big).$$

Wir bezeichnen mit $\mathrm{id}_A\colon A \to A$ die ***identische Abbildung***, d.h., $\mathrm{id}_A(a) = a$ für alle $a \in A$.

Lemma 5.5. *Sei $f\colon A \to B$ eine Abbildung. Dann gilt:*
(a) *Gibt es eine Abbildung $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$, so ist f injektiv.*
(b) *Gibt es eine Abbildung $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$, so ist f surjektiv.*
(c) *f ist bijektiv $\quad \Leftrightarrow \quad$ es gibt eine Abbildung $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$.*
*In diesem Fall heißt g die **Umkehrabbildung** von f.*

Beweis. (a) Sei also angenommen, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$. Wir wollen zeigen, dass f injektiv ist. Seien $a, a' \in A$ mit $f(a) = f(a')$. Dann folgt

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = g\big(f(a)\big) = g\big(f(a')\big) = (g \circ f)(a') = \mathrm{id}_A(a') = a'.$$

(b) Es gebe $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$. Wir wollen zeigen, dass f surjektiv ist. Sei dazu $b \in B$ und setze $a := g(b) \in A$. Dann gilt $f(a) = f\big(g(b)\big) = (f \circ g)(b) = \mathrm{id}_B(b) = b$.

(c) Wir müssen die beiden Richtungen der Äquivalenz zeigen. Nehmen wir zuerst an, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Also erfüllt g die Bedingungen in (a) und (b). Dann ist f injektiv und surjektiv, also bijektiv.
Umgekehrt sei nun f als bijektiv angenommen. Wir müssen zeigen, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Wir definieren g wie folgt. Sei $b \in B$. Da f surjektiv ist, gibt es ein $a \in A$ mit $f(a) = b$. Da f injektiv ist, gibt es nur eine Möglichkeit für dieses a; wir setzen $g(b) := a$. Dann folgt $g\big(f(a)\big) = a$ für alle $a \in A$ und $f\big(g(b)\big) = b$ für alle $b \in B$. □

Für jedes $n \in \mathbb{N}$ können wir die Menge $\{k \in \mathbb{N} \mid k \leqslant n\} = \{1, 2, \ldots, n\}$ bilden, diese hat offenbar genau n Elemente. Allgemein definieren wir:

Definition 5.6. (a) Seien A, B nicht leere Mengen. Dann heißen A, B ***gleichmächtig***, wenn es eine bijektive Abbildung $f\colon A \to B$ gibt. Wir schreiben in diesem Fall $|A| = |B|$.

(b) Gibt es ein $n \in \mathbb{N}$, so dass A gleichmächtig zu $\{1, \ldots, n\}$ ist, so schreiben wir einfach $|A| = n$ und sagen, dass A eine ***endliche Menge*** ist. Es gibt dann also eine bijektive Abbildung $f\colon \{1, \ldots, n\} \to A$, und A besteht genau aus den n Elementen $f(1), \ldots, f(n)$.

(c) Wenn es kein n wie in (b) gibt, so schreiben wir $|A| = \infty$. In diesem Fall hat A unendlich viele Elemente. Schließlich: Ist $A = \varnothing$, so setzen wir $|A| = 0$.

Zum Beispiel ist $\mathbb{N} \subsetneqq \mathbb{N}_0$, aber dennoch $|\mathbb{N}| = |\mathbb{N}_0|$, denn $f\colon \mathbb{N}_0 \to \mathbb{N}$, $n \mapsto n + 1$, ist eine Bijektion ($\rightsquigarrow$ "Hilberts Hotel"). Bleiben wir zunächst bei endlichen Mengen.

Bemerkung 5.7. Seien A und B nicht-leere endliche Mengen. Dann ist auch $A \cup B$ endlich.
(a) Gilt $A \cap B = \varnothing$, so folgt $|A \cup B| = |A| + |B|$.
(b) Im Allgemeinen ist $|A \cup B| = |A| + |B| - |A \cap B|$.

Beweis. (a) Sei $n \in \mathbb{N}$ so, dass es eine bijektive Abbildung $f\colon \{1, \ldots, n\} \to A$ gibt. Sei $m \in \mathbb{N}$ so, dass es eine bijektive Abbildung $g\colon \{1, \ldots, m\} \to B$ gibt. Definiere dann die Abbildung $h\colon \{1, \ldots, n + m\} \to A \cup B$ durch $h(i) := \begin{cases} f(i) & \text{falls } 1 \leqslant i \leqslant n, \\ g(i - n) & \text{falls } n < i \leqslant n + m. \end{cases}$
Man prüft sofort nach, dass h eine bijektive Abbildung ist.

(b) Sei $A' := A \setminus (A \cap B)$. Dann gilt $A = A' \cup (A \cap B)$, und die Vereingung ist disjunkt. Mit (a) folgt $|A| = |A'| + |A \cap B|$. Außerdem ist $A \cup B = A' \cup B$, und die Vereinigung ist disjunkt. Damit $|A \cup B| = |A'| + |B| = |A| - |A \cap B| + |B|$. □

Lemma 5.8. *Seien A, B nicht-leere, endliche Mengen und $f\colon A \to B$ eine Abbildung.*
(a) *Ist f injektiv, so gilt $|A| \leqslant |B|$.*
(b) *Ist f surjektiv, so gilt $|A| \geqslant |B|$.*
(c) *Es gelte $|A| = |B|$. Ist f injektiv oder surjektiv, so ist f bijektiv.*

Beweis. Sei $|A| = n \in \mathbb{N}$ und $|B| = m \in \mathbb{N}$. Also ist $A = \{a_1, \ldots, a_n\}$ und $B = \{b_1, \ldots, b_m\}$.

(a) Ist f injektiv, so sind $f(a_1), \ldots, f(a_n)$ alle verschieden, also ist $|f(A)| = n$. Wegen $f(A) \subseteq B$ folgt $|A| = n = |f(A)| \leqslant |B|$.
(b) Ist f surjektiv, so wähle zu jedem $j \in \{1, \ldots, m\}$ ein $i_j \in \{1, \ldots, n\}$ mit $f(a_{i_j}) = b_j$. Dann sind $a_{i_1}, \ldots, a_{i_m} \in A$ alle verschieden, also $|A| \geqslant m = |B|$.
(c) Sei $|A| = |B|$. Ist f injektiv, so ist wie oben $|A| = |f(A)|$. Wegen $|A| = |B|$ folgt also $|f(A)| = |B|$, und damit $f(A) = B$, d.h., f ist auch surjektiv. Ist f surjektiv, so folgt $A = f^{-1}(b_1) \cup \ldots \cup f^{-1}(b_m)$, wobei jedes $f^{-1}(b_j)$ nicht leer ist und die Vereinigung disjunkt ist. Damit $m = |A| = |f^{-1}(b_1)| + \ldots + |f^{-1}(b_m)|$ (siehe Bemerkung **??**), wobei jeder Summand $\geqslant 1$ ist. Da die ganze Summe gleich m ist, muss jeder Summand gleich 1 sein, also f injektiv. □

Im Folgenden bestimmen wir nun noch die Mächtigkeiten von endlichen Mengen bei einigen weiteren Konstruktionen.

Beispiel 5.9. Seien A, B nicht-leere Mengen. Mit $\mathrm{Abb}(A, B)$ bezeichnen wir die Menge aller Abbildungen $f\colon A \to B$. Seien nun A, B endlich. Dann gilt $|\mathrm{Abb}(A, B)| = |B|^{|A|}$.
Denn: Seien $|A| = n$ und $|B| = m$; sei $A = \{a_1, \ldots, a_n\}$. Um $f\colon A \to B$ zu definieren, haben wir für $f(a_1)$ genau m Möglichkeiten (nämlich eines der m Elemente von B), ebenso für $f(a_2)$ und so fort. Also insgesamt m^n Möglichkeiten.

Beispiel 5.10. Seien A, B nicht-leere, endliche Mengen. Dann gilt $|A \times B| = |A| \cdot |B|$.
Denn: Seien $|A| = n$ und $|B| = m$. Für $(a, b) \in A \times B$ gibt es n Möglichkeiten für die erste Komponente $a \in A$, und für jede Wahl von $a \in A$ dann jeweils m Möglichkeiten für die zweite Komponente, also insgesamt nm Möglichkeiten.

Beispiel 5.11. Seien A_1, A_2, A_3 nicht-leere Mengen. Dann definieren wir $A_1 \times A_2 \times A_3 := (A_1 \times A_2) \times A_3$, und schreiben $\big((a_1, a_2), a_3\big)$ einfach als (a_1, a_2, a_3). Die Elemente von $A_1 \times A_2 \times A_3$ sind damit Tripel (a_1, a_2, a_3) mit $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$. Allgemeiner: Ist $n \geqslant 2$ und sind $A_1, A_2, \ldots, A_n$ nicht-leere Mengen, so definieren wir rekursiv $A_1 \times A_2 \times \ldots \times A_n := (A_1 \times \ldots \times A_{n-1}) \times A_n$. Die Elemente von $A_1 \times \ldots \times A_n$ schreiben wir als $(a_1, \ldots, a_n)$ mit $a_i \in A_i$ für $1 \leqslant i \leqslant n$; diese Elemente heißen n-***Tupel***. Mit einer einfachen vollständigen Induktion nach n folgt: Sind $A_1, \ldots, A_n$ endlich, so gilt $|A_1 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$.

Bemerkung 5.12. Sei $n \in \mathbb{N}$ und seien $A_1, \ldots, A_n$ nicht-leere Mengen. Rekursiv haben wir oben $A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } 1 \leqslant i \leqslant n\}$ definiert. Wir sehen nun:

Sei $A := A_1 \cup \ldots \cup A_n$. Dann können wir ein n-Tupel $(a_1, \ldots, a_n)$ auch als Abbildung $f\colon \{1, \ldots, n\} \to A$ auffassen, mit $a_i = f(i) \in A_i$ für $1 \leqslant i \leqslant n$.
Mit dieser Identifizierung können wir auch definieren:

$$A_1 \times A_2 \times \ldots \times A_n := \{f \in \mathrm{Abb}(\{1, 2, \ldots, n\}, A) \mid f(i) \in A_i \text{ for } 1 \leqslant i \leqslant n\}.$$

Definition 5.13. Seien $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$. Dann bezeichnen wir mit dem Symbol $\binom{n}{k}$ die Anzahl der Teilmengen von $\{1, \ldots, n\}$ mit genau k Elementen. Für $n = 0$ setzen wir $\binom{0}{0} = 1$, und $\binom{0}{k} = 0$ falls $k \geqslant 1$. Die Symbole $\binom{n}{k}$ heissen ***Binomialkoeffizienten***.

Beispiele: $\binom{n}{0} = 1 = \binom{n}{n}$ für alle $n \in \mathbb{N}_0$. Ist $k > n$, so gilt offenbar $\binom{n}{k} = 0$.
Es gilt $\binom{4}{2} = 6$, denn es gibt 6 Teilmengen von $\{1, 2, 3, 4\}$ mit 2 Elementen, nämlich $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$.

Satz 5.14 (***Pascal–Dreieck***, um 1655)**.** *Für alle* $n, k \in \mathbb{N}$ *gilt* $\displaystyle\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Beweis. Ist $n = 1$, so gilt $\binom{1}{0} = \binom{1}{1} = 1$ und die Formel folgt mit den obigen Konventionen für $\binom{0}{k}$. Wir führen folgende Bezeichnungen ein:

$T(n, k) :=$ Menge der Teilmengen von $\{1, \ldots, n\}$ mit genau k Elementen,
$T_1(n, k) := \{S \in T(n, k) \mid n \in S\}$.
$T_0(n, k) := \{S \in T(n, k) \mid n \notin S\} = T(n-1, k)$ (für $n \geqslant 2$).

Sei nun $n \geqslant 2$. Es ist offenbar $T(n, k) = T_1(n, k) \cup T_0(n, k)$ und die Vereinigung ist disjunkt. Mit Bemerkung **??** erhalten wir

$$\binom{n}{k} = |T(n, k)| = |T_1(n, k)| + |T_0(n, k)| = |T_1(n, k)| + |T(n-1, k)| = |T_1(n, k)| + \binom{n-1}{k}.$$

Wir müssen jetzt noch zeigen, dass $|T_1(n, k)| = \binom{n-1}{k-1}$ gilt. Nun ist die rechte Seite gleich $|T(n-1, k-1)|$, also bleibt $|T_1(n, k)| = |T(n-1, k-1)|$ zu zeigen. Dazu definieren wir Abbildungen:

$$\begin{array}{lccccccc} f\colon & T(n-1,k-1) & \to & T_1(n,k), & S & \mapsto & S \cup \{n\}, \\ g\colon & T_1(n,k) & \to & T(n-1,k-1), & S' & \mapsto & S' \setminus \{n\}. \end{array}$$

Dann sind $f \circ g$ und $g \circ f$ jeweils die identischen Abbildungen, also ist f bijektiv (siehe Lemma **??**(c)) und damit $|T_1(n, k)| = |T(n-1, k-1)| = \binom{n-1}{k-1}$. □

Für $m \in \mathbb{N}$ heißt $m! := 1 \cdot 2 \cdot \ldots \cdot m$ die ***Fakultät*** von m; Konvention: $0! := 1$.

Folgerung 5.15. *Für alle* $n, k \in \mathbb{N}_0$ *mit* $0 \leqslant k \leqslant n$ *gilt* $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Beweis. (Vollständige Induktion über n mit Startwert $n_0 = 1$.) Induktionsanfang: Für $n = 1$ $\binom{1}{1} = 1!/(1!0!)$ und $\binom{1}{0} = 1!/(0!1!)$. Induktionsschritt: Sei nun $n \geqslant 2$ und die Behauptung bereits für $n - 1$ bewiesen. Sei $0 \leqslant k \leqslant n$. Ist $k = n$, so gilt $\binom{n}{n} = 1 = n!/(n!0!)$, also die Behauptung. Sei nun $0 \leqslant k \leqslant n - 1$. Nach Induktion und mit Satz **??** erhält man

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!}.$$

Mit einer einfachen Rechnung sieht man, dass die rechte Seite gleich $n!/(k!(n-k)!)$ ist. □

Lemma 5.16. *Sei* $n \in \mathbb{N}$. *Dann ist* $n! = |\{f\colon \{1,\dots,n\} \to \{1,\dots,n\} \mid f \text{ bijektiv }\}|$.

Beweis. Um eine injektive Abbildung $f\colon \{1,\dots,n\} \to \{1,\dots,n\}$ zu definieren, gibt es zunächst n Möglichkeiten für $f(1)$ (nämlich irgendeine der Zahlen $1,\dots,n$).
Damit f injektiv wird, gibt es dann noch $n-1$ Möglichkeiten für $f(2)$ (nämlich irgendeine der Zahlen $1,\dots,n$ außer $f(1)$).
Für $f(3)$ gibt es dann noch $n-2$ Möglichkeiten (alle Zahlen außer $f(1), f(2)$).
Nach $n-1$ Schritten sind dann bereits $n-1$ Zahlen für die Werte $f(1),\dots,f(n-1)$ verbraucht, also bleibt für $f(n)$ noch genau eine Möglichkeit übrig.

Damit hat man also insgesamt $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$ Möglichkeiten für f. Mit Lemma **??** ist jedes solche injektive f automatisch bijektiv. □

Für mehr dazu siehe https://de.wikipedia.org/wiki/Abz%C3%A4hlende_Kombinatorik.

6. *Unendliche Mengen*

In diesem (kurzen) Abschnitt stellen wir einige Aussagen und Beispiele zu Mengen mit unendlich vielen Elementen zusammen, die teilweise ziemlich verblüffend sind. Zunächst gibt es zwei Arten von "Unendlichkeit". Eine nicht-leere, unendliche Menge A, die gleichmächtig zu $\mathbb{N}$ ist (oder zu $\mathbb{N}_0$), heißt ***abzählbar unendlich***. Sonst heißt A ***überabzählbar***. Ist A abzählbar, so gibt es eine Bijektion $f\colon \mathbb{N} \to A$. Setzen wir $a_n := f(n)$ für alle $n \in \mathbb{N}$, so ist also $A = \{a_1, a_2, a_3, \dots\}$ eine "Aufzählung" der Elemente von A.

- $\mathbb{Z}$ ist abzählbar unendlich, denn wir können eine bijektive Abbildung $f\colon \mathbb{Z} \to \mathbb{N}$ zum Beispiel wie folgt definieren: $$f(n) = \begin{cases} 2n+1 & \text{falls } n \geqslant 0, \\ -2n & \text{falls } n < 0. \end{cases}$$
- $\mathbb{N}_0 \times \mathbb{N}_0$ ist abzählbar, siehe Beispiel **??**(d);
- $\mathbb{Q}$ ist ebenfalls abzählbar (siehe Übungen).

Wir werden im nächsten Kapitel sehen, dass $\mathbb{R}$ überabzählbar ist. Weiteres Beispiel (das wirklich Erstaunliche am folgenden Satz ist der genial einfache Beweis):

Satz 6.1 (Georg Cantor, um 1880)**.** *Ist* A *eine nicht-leere Menge, so gibt es keine surjektive Abbildung* $f\colon A \to \mathcal{P}(A)$. *Also kann* A *auch nicht gleichmächtig zu* $\mathcal{P}(A)$ *sein.*
Insbesondere ist die Potenzmenge $\mathcal{P}(\mathbb{N})$ *überabzählbar.*

Beweis. Annahme, es gibt eine surjektive Abbildung $f\colon A \to \mathcal{P}(A)$. Betrachte dann die Menge $B := \{x \in A \mid x \notin f(x)\} \in \mathcal{P}(A)$. Da f surjektiv ist, gibt es ein $a \in A$ mit $B = f(a)$. Nun gilt aber: $a \in f(a) \Leftrightarrow a \in B \Leftrightarrow a \notin f(a)$. Also erhalten wir einen Widerspruch.

Nun betrachte $A = \mathbb{N}$. Die Abbildung $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$, $n \mapsto \{n\}$, ist injektiv, also ist $\mathcal{P}(\mathbb{N})$ unendlich. Da $\mathbb{N}$ nicht gleichmächtig zu $\mathcal{P}(\mathbb{N})$ ist, folgt also, dass $\mathcal{P}(\mathbb{N})$ überabzählbar ist. □

Die Frage, ob es zwischen der Mächtigkeit von $\mathbb{N}$ und der von $\mathcal{P}(\mathbb{N})$ noch weitere "Mächtigkeiten" gibt, wird als ***Kontinuumshypothese*** bezeichnet, siehe https://de.wikipedia.org/wiki/Kontinuumshypothese.

Satz 6.2. *Sei A eine unendliche Menge. Dann gibt es eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$, d.h., setzt man $a_n := f(n)$ für $n \in \mathbb{N}_0$, so erhält man eine unendliche Folge von paarweise verschiedenen Elementen $a_0, a_1, a_2, \ldots$ in A.*

Idee des Beweises: Zuerst wähle irgendeinen Startwert $a_0 \in A$.

- Jetzt betrachte $A_1 := A \setminus \{a_0\}$. Dann ist immer noch $|A_1| = \infty$, also $A_1 \neq \varnothing$. Wähle irgendein $a_1 \in A_1$; dann ist auch $a_1 \neq a_0$.
- Jetzt betrachte $A_2 := A_1 \setminus \{a_1\} = A \setminus \{a_0, a_1\}$. Dann ist immer noch $|A_2| = \infty$, also $A_2 \neq \varnothing$. Wähle irgendein $a_2 \in A_2$; dann ist auch $a_2 \neq a_0$ und $a_2 \neq a_1$.
- Jetzt betrachte $A_3 := A_2 \setminus \{a_2\} = A \setminus \{a_0, a_1, a_2\}, \ldots$ usw. usw.

Aber das Problem ist hier das "usw. usw." ! Wie macht man so etwas präzise? Dazu brauchen wir zwei Hilfsmittel (auf die wir aber nur kurz eingehen werden).

Das erste dieser Hilfsmittel hat mit ***rekursiven Definitionen*** zu tun, mit denen Sie vermutlich vertraut sind. Als Beispiel betrachten wir die Folge $(a_n)_{n\in\mathbb{N}}$ von natürlichen Zahlen, die nach folgendem Schema gebildet wird. Sei $a_1 \in \mathbb{N}$ ein fest gewählter Startwert und dann

$$a_{n+1} = \begin{cases} 3a_n + 1 & \text{falls } a_n \text{ ungerade,} \\ a_n/2 & \text{falls } a_n \text{ gerade.} \end{cases}$$

Mit $a_1 = 19$ erhält man z.B. die Folge $19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$ (Übrigens: Versuchen Sie das Gleiche mit einem anderen a_1; fällt Ihnen etwas auf? Siehe dazu auch https://de.wikipedia.org/wiki/Collatz-Problem.)

Wenn man sich eine solche "Definition" genauer anschaut, so haben wir streng genommen lediglich eine Vorschrift, mit der man das jeweils nächste Folgenglied aus dem vorherigen berechnet. Dass man damit eine auf ganz $\mathbb{N}$ definierte Abbildung erhält, ist zunächst — und überhaupt — nicht klar. Die formale Begründung wird durch folgenden Satz geliefert.

Satz 6.3 (Rekursionssatz)**.** *Sei A eine nicht-leere Menge, $a_0 \in A$ fest. Für jedes $n \in \mathbb{N}_0$ sei eine Abbildung $h_n\colon A \to A$ gegeben. Dann gibt es genau eine Abbildung $F\colon \mathbb{N}_0 \to A$ mit*

$$F(0) = a_0 \qquad \text{und} \qquad F(n+1) = h_n\big(F(n)\big) \quad \text{für alle } n \in \mathbb{N}_0.$$

(Für einen formalen Beweis siehe §12 im Buch von Halmos.) Weiteres Beispiel:
Sei $A = \mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ und $h\colon \mathbb{Q}_{>0} \to \mathbb{Q}_{>0}$ gegeben durch

$$h(x) = \tfrac{1}{2}\big(x + \tfrac{2}{x}\big) \qquad \text{für alle } x \in \mathbb{Q},\ x > 0.$$

Sei $a_0 = 2$ und $h_n = h$ für $n \in \mathbb{N}_0$. Sei F die zugehörige Abbildung aus Satz **??**. Setze $a_n := F(n)$ für $n \in \mathbb{N}$. Dann ist $(a_n)_{n\in\mathbb{N}_0}$ eine Folge mit $a_0 = 2$ und

$$a_{n+1} = F(n+1) = h(F(n)) = h(a_n) = \frac{1}{2}\Big(a_n + \frac{2}{a_n}\Big) \quad \text{für alle } n \geqslant 0.$$

Diese Folge kommt Ihnen vielleicht bekannt vor: Sie konvergiert gegen $\sqrt{2}$. (Mehr zu Grenzwerten folgt im 2. Semester.)
Die Abbildungen h_n sind also die Vorschriften, mit denen man das jeweils nächste Folgenglied aus dem vorherigen berechnet; diese Abbildungen können sogar selbst von n abhängen.

Beispiel 6.4 (Siehe auch https://de.wikipedia.org/wiki/Fibonacci-Folge).
Sei $(f_n)_{n\in\mathbb{N}_0}$ die von Leonardo Fibonacci (um 1202!) rekursiv definierte Folge mit

$$f_0 := 0, \qquad f_1 := 1 \qquad \text{und} \qquad f_{n+1} := f_n + f_{n-1} \quad \text{für alle } n \geqslant 1.$$

Also $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots, 12586269025\ (n = 50), \ldots$
Hier braucht mal also jeweils zwei vorhergehende Folgenglieder, um ein neues Folgenglied auszurechnen. — Wie passt dies in den Rekursionssatz?
Dazu sei $A := \mathbb{N}_0 \times \mathbb{N}_0$; definiere $h\colon A \to A$ durch $h(i,j) := (j, i+j)$ für alle $(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0$. Nach dem Rekursionssatz gibt es eine Abbildung $F\colon \mathbb{N}_0 \to A$ mit $F(0) = (0,1)$ und $F(n+1) = h(F(n))$ für alle $n \geqslant 0$. Dann erhält man:

$$F(1) = h(F(0)) = h(0,1) = (1,1), \qquad F(2) = h(F(1)) = h(1,1) = (1,2),$$
$$F(3) = h(F(2)) = h(1,2) = (2,3), \qquad F(4) = h(F(3)) = h(2,3) = (3,5), \qquad \ldots$$

Schreibe nun $F(n) = (x_n, y_n)$ für alle $n \in \mathbb{N}_0$. Dann ist $x_0 = 0$, $y_0 = 1$ und $y_n = x_{n+1} = x_n + x_{n-1}$ für alle $n \geqslant 1$. Also ist $f_n = x_n$ für alle $n \in \mathbb{N}_0$.

Das zweite Hilfsmittel ist ein weiteres, berühmtes Axiom der Mengenlehre.

Axiom 6.5 (***Auswahlaxiom***, Ernst Zermelo 1904). *Sei A eine nicht-leere Menge und $\mathcal{P}(A)^\natural := \mathcal{P}(A) \setminus \{\varnothing\}$. Dann gibt es eine Abbildung $\alpha\colon \mathcal{P}(A)^\natural \to A$ mit $\alpha(B) \in B$ für alle nicht-leeren Teilmengen $B \subseteq A$.*

Eine solche Abbildung α heißt ***Auswahlfunktion***, denn sie "wählt" aus jeder nicht-leeren Teilmenge $B \subseteq A$ ein Element $\alpha(B) \in B$ aus.

Beispiel. Sei $A = \mathbb{N}$. Hier ist eine Auswahlfunktion $\alpha\colon \mathcal{P}(\mathbb{N})^\natural \to \mathbb{N}$ durch Peano's Induktionsaxiom gegeben: $\alpha(B) = \min(B)$ für jede nicht-leere Teilmenge $B \subseteq \mathbb{N}$.

Hier sehen wir jetzt, wo das Problem liegt: Versuchen Sie, eine Auswahlfunktion für $A = \mathbb{R}$ hinzuschreiben — Das ist bisher noch niemandem gelungen !

Das Auswahlaxiom garantiert also die Existenz von Etwas, das man in vielen Fällen (vor allem wenn man mit unendlichen Mengen zu tun) gar nicht konkret hinschreiben oder mit

einer expliziten Formel bestimmen kann. Für eine weitere Diskussion siehe

https://de.wikipedia.org/wiki/Auswahlaxiom.

Skizzieren wir kurz, wie man damit Satz **??** beweist. Sei also $A \neq \varnothing$ und $|A| = \infty$. Zu zeigen: Es gibt eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Nun, nach dem Auswahlaxiom gibt es eine Auswahlfunktion $\alpha\colon \mathcal{P}(A)^\natural \to A$. Sei $a_0 := \alpha(A)$. Mit Hilfe des Rekursionssatzes können wir dann eine Folge $(a_n)_{n\in\mathbb{N}_0}$ definieren mit

$$a_{n+1} = \alpha(A \setminus \{a_0, a_1, \ldots, a_n\}) \qquad \text{für alle } n \geqslant 0.$$

Dann gilt $a_{n+1} \notin \{a_0, a_1, \ldots, a_n\}$ für alle $n \geqslant 0$, also sind die Elemente $a_0, a_1, a_2, \ldots$ in A alle verschieden. Damit ist $f\colon \mathbb{N}_0 \to A$, $n \mapsto a_n$, die gesuchte injektive Abbildung. □

Zum Schluss noch eine weitere verblüffende Eigenschaft von unendlichen Mengen:

Folgerung 6.6 (Richard Dedekind, um 1888)**.** *Sei A eine nicht-leere Menge. Dann ist A unendlich genau dann, wenn es eine echte Teilmenge $B \subsetneqq A$ gibt mit $|A| = |B|$.*

Beweis. Sei zuerst angenommen, dass es eine Teilmenge $B \subsetneqq A$ mit $|B| = |A|$ gibt. Dann ist $f\colon B \to A$, $b \mapsto b$, injektiv. Wäre A endlich, so müsste f auch surjektiv sein (siehe Satz 5.9(c)), Widerspruch. Also ist A unendlich.

Umgekehrt: Sei A als unendlich angenommen. Nach Satz **??** gibt es eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Sei $a_n := f(n)$ für alle $n \in \mathbb{N}_0$, und $A' := f(\mathbb{N}_0) = \{a_0, a_1, a_2, \ldots\} \subseteq A$.

Setze nun $B := A \setminus \{a_0\}$. Wir definieren eine Abbildung $g\colon A \to B$ durch

$$g(a) := \begin{cases} a & \text{falls } a \notin A', \\ a_{n+1} & \text{falls } a \in A' \text{ und } a = a_n. \end{cases}$$

Man sieht sofort, dass g injektiv und surjektiv ist. Also ist $|A| = |B|$ aber $B \subsetneqq A$. □