Skript **Version 10. Februar 2024**

Elementarmathematik I
Zahlen, Beweise, Mengen, Abbildungen

Goethe–Universität Frankfurt — Wintersemester 2023/24

für Lehramt L2/L5-Mathematik

JAKOB STIX

Zusammenfassung. — Das Lehramtstudium verlangt einen durchdachten und souveränen Umgang mit Mathematik und daher die Auseinandersetzung mit Hochschulmathematik, um ein tieferes Vverständnis zu erlagen. Die Vorlesung Elementarmathematik 1 bereitet dafür die Grundlage, indem mathematische Begriffe und Methoden besprochen und eingeübt werden.

Inhaltsverzeichnis

1. Organisatorisches

1.1. **Wie geht studieren?** Auf diese Frage muß letztliche jede/r selbst eine Antwort finden. Hier sind meine Empfehlungen:

- Mitschreiben. Man zwingt sich, aufmerksam zu bleiben und kann Ergänzungen notieren. Das spontane Formulieren von Mathematik wird eingeübt, wenn man nicht nur passiv mitschreibt sondern aktiv.
- Fragen stellen. Wer etwas nicht versteht, sollte sich bemühen, dieses Unverständnis in eine Frage zu packen. Dies hilft allen im Raum, dem Dozenten als Rückmeldung, was angekommen ist und welche Verständnisprobleme auftreten, den Mitstudierenden, weil sie auch Fragen haben, aber es noch nicht genau in Worte fassen können, was sie nicht verstehen. Und: jede Frage ist erlaubt.
- Nacharbeiten. Die Veranstaltungen im Studium sind mit CP (credit points) ausgestattet. Ein CP entspricht dabei dem durchschnittlichen Zeitaufwand von 30 Zeitstunden, also ca. 2h pro Semestervorlesungswoche. Die Elementarmathematik 1 hat 5CP, also geschätzte 10h Aufwand pro Vorlesungswoche. Bleiben bei 4h Vorlesung und Übung noch 6h für eigenständige Beschäftigung mit dem Stoff.

  Nacharbeiten funktioniert am besten in Kleingruppen. Durch das gegenseitige Erklären lernen beide Seiten und Sie üben das sprechen von Mathematik.
- Mathematik selbst machen. Lösen sie Übungsaufgaben! Nutzen Sie dazu das wöchentliche Übungsblatt und auch Aufgaben aus anderen Quellen, derer Sie habhaft werden können.
- Versuchen Sie zu verstehen. Mathematik lernt man nicht, man versteht sie und dann trägt sie sich selbst. Geben Sie sich nicht zufrieden, wenn Sie mechanisch Dinge reproduzieren können. Gehen Sie den Dingen auf den Grund und durchdenken Sie diese, bis Sie es wirklich verstanden haben.

  Ein guter Test, ob man etwas verstanden hat, besteht darin, es jemandem zu erklären. Sie können im Prinzip auch gegen eine Wand reden — die andere Person muss es nicht verstehen — aber das ist nicht so sozial. Wenn Sie ehrlich mit sich sind, merken Sie genau, ob ihre Argumentation oder Ihre Beschreibung wasserdicht ist, oder ob Sie schummeln. Also: reden Sie miteinander Mathematik!

1.2. **Mathematik im Netz.**

- Quanta magazine: https://www.quantamagazine.org/mathematics/
- Numberphile von Brady Haran: https://www.youtube.com/@numberphile
- ARTE, Mathewelten: https://www.arte.tv/de/videos/097454-007-A/mathewelten/
- Ralph Caspers, ein mit dem Medienpreis der DMV ausgezeichnetes Video zu Fibonaccizahlen: Kann die Natur Mathe? | Quarks: Dimension Ralph.

1.3. **Literaturempfehlungen.** Es gibt keine Quelle außer diesem unpolierten Kurzskript, das den genauen Inhalt der Vorlesung abdeckt. Die beiden folgenden Bücher enthalten viel Nützliches und vom Niveau passendes Material. Des weiteren sind sie über die Universitätsbibliothek für Studiernede als Volltext frei verfügbar. Besonders empfehlen möchte ich auch das Buch von Enzensberger für Kinder und Erwachsene.

Literatur

[GK23] Felix Göbler, Alex Küronya
Einstieg in die beweisorientierte Mathematik
Springer Spektrum, 2023, xxix+320 Seiten.

[SchSt18] Hermann Schichl, Roland Steinbauer
Einführung in das mathematische Arbeiten
Springer Spektrum, 3. Auflage, 2018, xvii+534 Seiten.

[Enz14] Hans Magnus Enzensberger
Der Zahlenteufel: ein Kopfkissenbuch für alle, die Angst vor der Mathematik haben
gestaltet und mit Bildern versehen von Rotraut Susanne Berner, verschiednen Ausgaben, 262 Seiten.

- In der Einleitung von [GK23] findet man weitere Anregungen zu Literatur.
- Von Zeit zu Zeit wird es in der Vorlesung eine Ansage geben, aus den obigen Quellen einen Abschnitt vorbereitend zu lesen.

2. Ein Springer auf dem Schachbrett

Wir machen in der ersten Vorlesung eine Aufwärmübung. Wir streifen viele Themen, die später aufgegriffen und vertieft werden.

2.1. **Ein Springer auf Reisen.** Wir lernen oder rufen uns in Erinnerung, dass ein Springer auf dem Schachbrett einen **Springerzug** ausführen darf. Um den Springerzug zu beschreiben, vereinbaren wir, das Schachbrett in Reihen (horizontal) und Spalten (vertikal) aufzuteilen. Die Reihen werden tradtionell von 1 bis 8 durchnummeriert, und die Spalten erhalten Namen a bis h. Im Wesentlichen handelt es sich um Koordinaten, bei der man die Spaltenkoordinate anstelle von Zahlen mit Buchstaben bezeichnet (Descartes hätte das anders gelöst). Wir machen eine Definition.

Definition 2.1. Ein **Springerzug** auf einem Schachbrett besteht aus der Kombination von einem Zug über 2 Felder entlang entweder einer Spalte oder Reihe in belibiger Richtung, gefolgt von einem Zug um 1 Feld in eine dazu senkrechte Richtung. Der Springer muss dabei wieder auf einem Feld des Schachbretts landen, ansonsten ist der Zug ungültig.

Wir haben uns überlegt, dass ein Springer, wenn er in der Mitte des Schachbretts steht $4 \cdot 2 = 8$ Felder in einem Springerzug erreichen kann. Die 4 steht für die Wahlen im ersten Schritt, die 2 für die anschließenden möglichkeiten im zweiten Schritt, multipliziert wird, weil beide Wahlen unabhängig voneinander sind und das Ergebnis überzählt die erreichten Felder nicht, weil keine zwei Kombinationen auf demselben Feld landen.

Wir wollen nun mit dem Springer das ganze Schachbrett bereisen. Dazu machen wir eine weitere Definition.

Definition 2.2. Eine **vollständige Springerreise** auf dem Schachbrett ist eine Abfolge von Springerzügen, im Laufe derer der Springer jedes Feld des Schachbretts genau einmal besucht.

Bemerkung 2.3.

(1) Definitionen sind wichtig. Sie sollen neue Begriffe festlegen. Die jeweiligen neuen Begriffe in einer Definition werden in diesem Skript in Fettdruck hervorgehoben.

> ⚠ Dabei müssen Definitionen den neuen Begriff mit bereits festgelegten Begriffen eindeutig beschreiben.

Wenn man eine Eigenschaft definiert, dann bedeutet es, dass die Eigenschaft für alle Dinge, auf die sie per Definition anwendbar sein soll, auch immer eindeutig entscheidbar ist, ob sie gilt oder nicht. Wenn das gelingt, dann spricht man davon, dass die Definition **wohldefiniert** ist. Aber dieser Begriff wohldefiniert ist selbst nicht so einfach zu definieren. Er bedeutet jedenfalls nicht, dass die Definition wohlgeraten, also schön oder brauchbar oder einleuchtend ist. (Guten) Geschmack kann man nicht wohldefinieren.

(2) Schlüsselwörter in Definitionen sind Ausdrücke wie
- jedes,
- genau einmal.

Dieses sind harte Vorgaben und nicht verhandelbar, ansonsten ändert sich der definierte Begriff. „Jedes genau einmal“ bedeutet ohne Ausnahme „alle mindestens einmal, aber keines ein zweites Mal“.

(3) Vorgriff auf die Vorlesung „Elementare Angewandte Mathematik“: Man kann die Felder des Schachbretts als Ecken eines Graphen auffassen, bei dem die Kanten zwischen den Ecken den möglichen Springerzügen entsprechen[1]. Eine vollständige Springerreise entspricht einem Hamiltonweg in diesem Graph. Einen solchen per Algorithmus in einem beliebigen Graphen zu finden ist ein NP-hartes Problem.

[1] Stellen Sie sich Ecken als Städte und die Kanten als Straßen, die sich nur in den Städten treffen, vor.

Satz 2.4. *Auf dem Schachbrett gibt es eine vollständige Springerreise.*

Haben wir alles vorher definiert? Ist der Gehalt des Satzes entweder wahr der falsch? Ist es ein vollständiger Satz?

Wir haben mit Satz 2.4 eine mathematische **Aussage**. Diese erfordert einen Beweis. Was ist dazu nötig? Müssen wir alle Springerreisen bestimmen? Nein! Eine reicht! Und wir müssen noch nicht einmal eine angeben. Wenn wir auf irgendeine Weise eine Formel für die Anzahl der Springerreisen angeben könnten und dann zeigen könnten, dass deren Wert positiv ist, dann hätten wir gewonnen. Aber: in so einem Fall ist es das einfachste, wenn man ein Beispiel für das „Ding“ mit den geforderten Eigenschaften angibt. Und das klappt hier, darum

⚠ **beweisen wir den Satz hier per Beispiel**

(und das ist hier legal und sogar oft elegant).

Beweis. Auf https://de.wikipedia.org/wiki/Springerproblem# finden Sie ein Beispiel einer vollständigen Springerreise. □

Beweise sollten einen markierten Anfang und ein markiertes Ende haben. Hier □.

2.1.1. *Varianten.* Ein sehr typisches mathematisches Vorgehen besteht darin, in Aussagen, die man verstanden hat, die Parameter zu variieren. Was ist mit $n \times n$-Schachbrett als Variante?

Problemlösestrategien: vereinfachen und probieren! Also ein Springer auf einem $n \times m$-Scahchbrett mit kleinen n und m. Etwa 3×3 geht nicht, weil man die Mitte nicht einbinden kann.

Sprache: wie kommuniziere/schreibe ich so etwas auf, dass es mathematisch sauber ist und verstanden werden kann. Es gibt einen wesentlichen Unterschied zwischen gesprochenem Dialog und geschriebenem Text. Beim Text hat man die Pflicht, alle möglichen Mißverständnisse mitzudenken und durch die gewählte Ausdrucksweise zu vermeiden. Daher hat mathematische Sprache einige Regeln und Wendungen mit speziellen Bedeutungen. Und mathematische Sprache wird fortlaufend neu geschaffen! Zum Beispiel haben wir vorhin den Begriff vollständigeSpringerreise definiert. Manchmal werden Begriffe mit „Verfallsdatum“ definiert, z.B. am Ende eines Kapitels.

2.2. **Der Springer auf dem angeknabberten Schachbrett.** Wir sind zurück auf dem 8×8-Schachbrett, nur hat jemand zwei diagonal gegenüberliegende Eckfelder entfernt, sagen wir a1 und h8 (Koordinaten! c5 steht für den Punkt $(3|5)$, siehe Beispiel 9.23). Kann der Springer immer noch eine vollständige Springerreise auf diesem Brett durchhführen?

Satz 2.5. *Auf dem 8×8-Schachbrett ohne die Ecken a1 und h8 ist keine vollständige Springerreise möglich.*

Also es geht nicht. Aber wie beweist man sowas. Wenn etwas geht, dann kann man ein Beispiel konstruieren. Reicht es auch hier aus, ein Beispiel vorzuführen, bei dem der Springer irgendwann nicht weiter kommt? Nein! Man muss schon alle Möglichkeiten durchprobieren. Das geht theoretisch, praktisch sind es aber zu viele. Man muß schlauer vorgehen. Wir spielen mit dem Problem herum, bis uns etwas auffällt.

Symmetrien! Das Schachbrett hat schwarze und weiße Felder, und der Springer wechselt bei jedem Zug die Farbe. Das sieht man! Aber man kann es auch in mathematische Sprache packen und beweisen! Das machen wir später mit der Lehre von Gerade und Ungerade. Jetzt bringen wir erstmal die Springerreise zu Ende.

Beweis. Die Springerreise ist durch eine Folge von Feldern, identifiziert durch Koordinaten, beschrieben. Wenn wir uns von der Springerreise nur merken, welche Feldfarbe die Springerposition hat, dann verlieren wir viel Information, aber dafür vereinfacht sich das Bild. Die Springerreise sieht so aus

■, □, ■, □, ■, □, ■, □, ■, □, ■, □, ■, □, ■, □, . . . ,

oder so

$$\square, \blacksquare, \square, \blacksquare, \square, \blacksquare, \square, \blacksquare, \square, \blacksquare, \square, \blacksquare, \square, \blacksquare, \square, \blacksquare, \ldots \ .$$

Das angeknabberte Schachbrett hatt $8 \cdot 8 - 2 = 62$ Felder. Die Reise dauert also 62 Springerzüge lang und in der Zeit hat der Springer 31 weiße und 31 schwarze Felder besucht. Die ausgelassenen Felder a1 und h8 sind beide schwarz, also hat das angeknabberte Schachbrett 32 weiße und 30 schwarze Felder. Eine vollständige Springerreise auf dem angeknabberten Schachbrett ist nicht möglich. □

Take home message Kapitel §2.

- Definitionen legen neue Begriffe fest. Eine Definition muß wohldefiniert sein.
- Beweis per Beispiel für Behauptungen der Form „Es gibt ein/e . . . “.
- Beweis per Beispiel funktioniert NICHT für Behauptungen der Form „Es gibt kein/e . . . “.

3. Stellenwertsysteme

3.1. **Die natürlichen Zahlen.** Irgendwo müssen wir anfangen und halten es da mit Leopold Kronecker (7.12.1823 – 29.12.1891): „Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk“.

⚠ Die natürlichen Zahlen sind die Zahlen

$$0, 1, 2, 3, 4, 5, 6, 7, \dots$$

zum Zählen von Dingen. Das ist keine gute Definition und daher schreiben wir sie auch nicht als formale Definition auf, um keinen falschen Eindruck zu hinterlassen. Diese Definition beschreibt nämlich etwas Neues, den Begriff der natürlichen Zahl, mit etwas ebenso noch nicht definierten, die Symbole $0, 1, 2, \dots$ und was das Zählen bedeuten soll. Natürliche Zahlen sind gegeben.

3.1.1. *Die Null.* Manchmal wird so getan, als ob es einen Streitfall gäbe, ob die Null 0 zu den natürlichen Zahlen gehört. Es gibt keine universell anerkannte Antwort auf diese Frage, und es ist auch reichlich unerheblich. Wichtig ist nur, dass man festlegt, wie man die Null behandeln möchte, ob also die 0 dabei ist, wenn man über alle natürlichen Zahlen redet, oder eben nicht. Egal wie man sich entscheidet, es wird immer Fälle geben, bei denen die eine Konvention oder die andere Konvention Vorteile hat. Wenn Sie im Zweifel sind, wie Ihre Quelle die Null behandelt, dann müssen Sie bei den Konvetionen nachsehen. Ein gutes Buch verrät dies an prominenter Stelle.

3.2. **Addition und Multiplikation.** Damit wir mit den natürlichen Zahlen etwas anfangen können und damit üben können, Mathematik zu machen, müssen wir ein wenig Rechnen können. Wir legen also auch fest, dass wir bereits wissen, wie man natürliche Zahlen addiert und wie man multipliziert. Die Subtraktion erlauben wir uns auch, genauso wie einige Rechenregeln wie das Ausklammern/Ausmultplizieren etc.

3.3. **Das Zehnersystem.** Das Zehnersystem ist eine Schreibweise, um auf ökonomische und zum Rechnen praktische Art und Weise Zahlen zu schreiben. Man stelle sich Zahlen als Worte vor, bei der die Buchstaben Ziffern sind.

Definition 3.1. Die **Ziffern** im Zehnersystem sind die Symbole

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

(Hier ist es ein Vorteil, dass wir die 0 bereits eingeführt haben.)

Man kann nun aus diesen „Buchstaben“ $0, 1, \dots, 9$ Worte bilden wie

$$1234567890123456789.$$

Wir werden bald echte Buchstaben als Platzhalter benutzen. Daher vereinbaren wir die folgende Schreibweise. Beispielsweise wird 1234567890123456789 als

$$(1234567890123456789)_{10}$$

geschrieben. Die Klammern umfaßt die Abfolge von Ziffern und die kleine angehängte 10 erinnert uns daran, dass es sich um eine Zahl im Zehnersystem handelt[2]. Allgemeiner:

Definition 3.2. Eine **Zahl im Zehnersystem** ist eine Folge von Ziffern $a_0, a_1, a_2, \dots, a_k$ geschrieben als

$$(a_k a_{k-1} a_{k-2} \dots a_2 a_1 a_0)_{10}$$

mit der Bedingung, dass die **führende Ziffer** a_k nicht die 0 ist, es sei denn es handelt sich um die Zahl $(0)_{10}$.

[2]Und diese Schreibweise läßt sich dann gut verallgemeinern für andere Stellenwertsysteme

Man sagt, diese Zahl hat $k+1$ **Stellen** (und k ist eine natürliche Zahl, die wir zuerst wählen müssen).

Beispiel 3.3. Wenn wir die Zahl 321, also Dreihunderteinundzwanzig, darstellen wollen, dann ist $k = 2$ und $t = a_0 = 1$, $a = a_1 = 2$ und $t = a_2 = 3$, so dass

$$(cat)_{10} = (a_2a_1a_0)_{10} = (321)_{10}$$

die 321 beschreibt. Wir sehen, dass $(321)_{10}$ ulkig aussieht und zusätzlichen Balast mit herumschleppt, weil wir gewohnt sind, immer im Zehnersystem zu rechnen. Bei $(cat)_{10}$, was eine nicht näher ausgewählte dreistellige Zahl beschreibt (wenn wir mal die obigen Wahlen der Ziffern c, a und t vergessen) ist es schon weniger ulkig, wenn wir das Wort „cat“ nicht mit einer Zahl $(cat)_{10}$ verwechseln wollen.

Bemerkung 3.4. In der Definition einer Zahl im Zehnersystem tauchen unbestimmt viele unbekannte Ziffern auf. Wenn wir diese nur mit Buchstaben bezeichneten, dann wären wir schnell am Ende. Eine 100-stellige Zahl könnten wir so nicht darstellen. Man bedient sich eines Tricks und indiziert einen Buchstaben, hier das a, mit einer natürlichen Zahl, und erhält somit eine unbestimmte Ansammlung von unbestimmten Zahlbezeichnungen $a_0, a_1, a_2, \dots, a_k$.

Jetzt haben wir eine Schreibweise eingeführt, aber welchen Wert hat eine solche Zahl? Darüber haben wir uns noch nicht ausgelassen. Das symbolische $(a_ka_{k-1}a_{k-2}\dots a_2a_1a_0)_{10}$ hat auch einen Wert, eine natürliche Zahl, die dadurch dargestellt wird. Machen wir zuerst ein einfaches Zahlenbeispiel.

$$2023 = 2\cdot 1000 + 0\cdot 100 + 2\cdot 10 + 3\cdot 1 = 2\cdot 10^3 + 0\cdot 10^2 + 2\cdot 10^1 + 3\cdot 10^0.$$

Die verschiedenen Stellen haben also unterschiedliche Wertigkeiten (daher Stellenwertsysteme). Die erste 2 steht an der Tausenderstelle und bedeutet 2 mal die 1000, während die zweite Ziffer 2 and der Zehnerstelle steht und 2 mal die 10 bedeutet. Allgemeiner steht mit Ziffern $a_0, \dots, a_k$

$$(a_k, a_{k-1}, \dots, a_2, a_1, a_0)_{10}$$

für die Zahl

$$a_k\cdot 10^k + a_{k-1}\cdot 10^{k-1} + \dots + a_2\cdot 10^2 + a_1\cdot 10^1 + a_0\cdot 10^0.$$

Dabei sind die Pünktchen wohlmeinend zu ergänzen. Dafür gibt es sauber die Summenschreibweise

$$\sum_{i=0}^{k} a_i\cdot 10^i,$$

bei welcher der Index i von 0 bis k läuft, und für jeden der Indizes ein Summand $a_i\cdot 10^i$ in der Summe zu berücksichtigen ist. Wir betrachten die Zahl im Zehnersystem als einen Namen für ihren Wert und schreiben als Gleichheit

$$(a_k, a_{k-1}, \dots, a_2, a_1, a_0)_{10} = a_k\cdot 10^k + a_{k-1}\cdot 10^{k-1} + \dots + a_2\cdot 10^2 + a_1\cdot 10^1 + a_0\cdot 10^0 = \sum_{i=0}^{k} a_i\cdot 10^i.$$

Satz 3.5. *Jede natürliche Zahl besitzt eine eindeutige Darstellung als Zahl im Zehnersystem.*

Das ist vermutlich eine Aussage, die Sie für offensichtlich halten. Man kann sie dennoch beweisen. Allerdings fehlt uns streng genommen hier noch eine wesentliche definierende Eigenschaft der natürlichen Zahlen, die wir erst im Kapitel über die vollständige Induktion lernen. Wir „beweisen“ hier nur die Eindeutigkeit.

Beweis der Eindeutigkeit. Die Darstellung als Zahl im Zehnersystem ist eindeutig, wenn wir für zwei Darstellungen, welche die gleiche natürliche Zahl beschreiben, zeigen können, dass sie aus der gleichen Abfolge von Ziffern besteht. Wir nehmen daher an, dass es eine natürliche Zahl gibt, nennen wir sie n, die der Wert von zwei Zahlen im Zehnersystem ist. Also, die eine hat $k+1$

viele Stellen und Ziffern $a_0, \ldots, a_k$; und die andere hat $\ell + 1$ viele Stellen und Ziffern $b_0, \ldots, b_\ell$. Das bedeutet, wir können mit der Gleichung

$$(a_k a_{k-1} \ldots a_1 a_0)_{10} = n = (b_\ell b_{\ell-1} \ldots b_1 b_0)_{10} \tag{3.1}$$

arbeiten.

Jetzt machen wir einen Widerspruchsbeweis. Wir nehmen an, dass die beiden Zahlen im Zehnersystem unterschiedlich sind (dieselbe natürliche Zahl, aber auf verrückte Art und Weise zwei verschiedene Schreibweisen im Zehnersystem). Wenn wir daraus durch gültige Argumente etwas Unsinniges zeigen können, dann haben wir gewonnen, denn der einzige Fehler im Argument kann dann nur die Anfangsannahme sein. Diese war dann fehlerhaft. Die Gegenposition zur Annnahme, dass die beiden Zahlen im Zehnersystem unterschiedlich sind, ist aber genau die Behauptung, dass beide Zahlen im Zehnersystem gleich sein müssen.

Also, angenommen die Ziffernfolgen $a_k, a_{k-1}, \ldots, a_1, a_0$ und $b_\ell, b_{\ell-1}, \ldots, b_1, b_0$ sind nicht gleich. Dann muß es einen kleinsten Index t geben, bei der eine Abweichung auftritt. Zum Beispiel, wenn wir $(123456789)_{10}$ mit $(103456789)_{10}$ vergleichen, dann ist dies an der Stelle mit der 2 bzw. 0. Das ist die Stelle mit dem Index 7. Wenn wir $(123)_{10}$ mit $(9874123)_{10}$ vergleichen, dann scheint es eine solche Stelle nicht zu geben. Doch, sie gibt es: es ist die Stelle mit der 4, die in der einen Zahl existiert und in der anderen Zahl an eben der 1000er-Stelle nicht mehr existiert. Hier ist $b_3 = 4$ und a_3 gibt es nicht, stimmt also nicht mit b_3 überein.

Wenn t der Index mit der ersten Abweichung $a_t \neq b_t$ ist, dann sind für alle Stellen mit kleinerer Wertigkeit, also die i mit $0 \leq i \leq t-1$ die Ziffern gleich, also $a_i = b_i$. Wir ziehen nun von beiden Seiten der Gleichung (3.1) die Zahl

$$(a_{t-1} a_{t-2} \ldots a_1 a_0)_{10} = (b_{t-1} b_{t-2} \ldots b_1 b_0)_{10}$$

ab. Das ergibt auf der linken Seite

$$\begin{aligned}
&(a_k a_{k-1} \ldots a_1 a_0)_{10} - (a_{t-1} a_{t-2} \ldots a_1 a_0)_{10} \\
=&\Big(a_k \cdot 10^k + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0\Big) - \Big(a_{t-1} \cdot 10^{t-1} + a_{t-2} \cdot 10^{t-2} + a_1 \cdot 10^1 + a_0 \cdot 10^0\Big) \\
=&a_k \cdot 10^k + \ldots + a_{t+1} \cdot 10^{t+1} + a_t \cdot 10^t \\
=&10^t \cdot \Big(a_k \cdot 10^{k-t} + a_{k-1} \cdot 10^{k-t-1} + \ldots + a_{t+1} \cdot 10^1 + a_t \cdot 10^0\Big).
\end{aligned}$$

Auf der rechten Seite genauso, so dass sich die folgende Gleichung ergibt:

$$10^t \cdot \Big(a_k \cdot 10^{k-t} + \ldots + a_{t+1} \cdot 10^1 + a_t \cdot 10^0\Big) = 10^t \cdot \Big(b_\ell \cdot 10^{\ell-t} + \ldots + b_{t+1} \cdot 10^1 + b_t \cdot 10^0\Big).$$

Diese Gleichung teilen wir durch 10^t und entdecken, dass wir aus den ursprünglichen Zahlen im Zehnersystem nur die t gleichen Stellen (beginnend von der Einerstelle ganz rechts) gestrichen haben:

$$(a_k a_{k-1} \ldots a_{t+1} a_t)_{10} = (b_\ell b_{\ell-1} \ldots b_{t+1} b_t)_{10}. \tag{3.2}$$

Es scheint, als ob wir nicht wirklich etwas bewegt haben. Aber das stimmt nicht. Mit der Gleichung in (3.2) haben wir nun zwei Darstellungen im Zehnersystem der gleichen natürlichen Zahl gefunden, die sich bereits in der Einerstelle unterscheiden! Die neuen Zahlen haben die Einerstelle a_t und b_t, und hier liegt ja eine Abweichung vor. Wir haben somit gelernt: wenn die Eindeutigkeit schief geht, dann sogar in einem Fall sogar mit Abweichung bei der Einerstelle. Wir ersetzen nun unsere ursprüngliche Zahl und die zwei Darstellungen durch diese neue und dürfen daher in der Notation von oben annehmen, dass $t = 0$ ist. Das machen wir nun. (im Beispiel des Vergleichs $(123456789)_{10}$ mit $(103456789)_{10}$ haben wir die Zahlen durch $(12)_{10}$ und $(10)_{10}$ ersetzt.)

Wir haben jetzt also

$$(a_k a_{k-1} \ldots a_1 a_0)_{10} = n = (b_\ell b_{\ell-1} \ldots b_1 b_0)_{10} \tag{3.3}$$

mit $a_0 \neq b_0$. Nehmen wir einmal an, dass $b_0 > a_0$. Den anderen Fall $a_0 > b_0$ behandelt man analog (oder durch Vertauschen der beiden Darstellungen im Zehnersystem). Dann folgt aus (3.3) durch Definition und Umstellen:

$$\begin{aligned}
&\Longrightarrow \quad \left(a_k \cdot 10^k + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0\right) = \left(b_\ell \cdot 10^\ell + \ldots + b_1 \cdot 10^1 + b_0 \cdot 10^0\right) \\
&\Longrightarrow \quad \left(a_k \cdot 10^k + \ldots + a_1 \cdot 10^1\right) - \left(b_\ell \cdot 10^\ell + \ldots + b_1 \cdot 10^1\right) = b_0 - a_0 \\
&\Longrightarrow \quad 10 \cdot \underbrace{\left(\left(a_k \cdot 10^{k-1} + \ldots + a_1 \cdot 10^0\right) - \left(b_\ell \cdot 10^{\ell-1} + \ldots + b_1 \cdot 10^0\right)\right)}_{=:x} = b_0 - a_0,
\end{aligned}$$

denn auf der linken Seite ist im mittleren Schritt in jedem Summanden ein Faktor 10 zu holen, den wir im letzten Schritt ausgeklammer haben. Zur Vereifachung haben wir die natürliche Zahl in der großen Klammer mit x bezeichnet. Die Gleichung ist dann einfach

$$10 \cdot x = b_0 - a_0. \tag{3.4}$$

Jetzt müssen wir überlegen, dass dies nicht sein kann. Die linke Seite ist ein Zehnfaches einer natürlichen Zahl. Damit ist dies entweder $10 \cdot 0 = 0$ oder mindestens $10 \cdot 1 = 10$. Die rechte Seite hingegen ist die Differenz von zwei Ziffern, wobei wir die größere von der kleineren abziehen. Der Unterschied ist also mindestens 1 aber höchstens $9 - 0 = 9$:

$$1 \leq b_0 - a_0 \leq 9 - 0 = 9.$$

Damit können rechte und linke Seite in (3.4) nicht übereinstimmen. Der Widerspruch ist gefunden und der Beweis der Eindeutigkeit erbracht. □

Frage 3.6. An welcher Stelle im obigen Beweis schummeln wir mit unserem Verständnis von natürlichen Zahlen?

Take home message Kapitel §3.

- Natürliche Zahlen $0, 1, 2, 3, 4, 5, 6, \ldots$.
- Variablenvorrat vergrößern durch einen Index (Plural Indices): $a_0, a_1, a_2, \ldots$.
- Der Wert einer Zahl $(a_k \ldots a_1 a_0)_{10}$ im Zehnersystem ist $\sum_{i=0}^{k} a_i 10^i$. Hierbei sind für $0 \leq i \leq k$ die a_i Ziffern, also 0, 1, 2, 3, 4, 5, 6, 7, 8 oder 9. Die Stelle mit Index i hat den Wert 10^i. Stellenwertsystem.
- Die Darstellung einer natürlichen Zahl im Zehnersystem ist eindeutig. Regel: führende Ziffer $\neq 0$, außer bei 0.

4. Die Lehre von gerade und ungerade

4.1. **Kriterien.** Das Rechnen mit gerade und ungerade beherrschten schon die alten Griechen (siehe das Buch *Elemente* von Euklid).

Definition 4.1. Ein **gerade** Zahl ist eine natürliche Zahl, die das zweifache einer natürlichen Zahl ist. In Formeln: eine natürliche Zahl n ist gerade, wenn es eine natürlichen Zahl a gibt, so dass

$$n = 2 \cdot a.$$

Eine natürliche Zahl die nicht gerade ist, nennt man **ungerade**.

Beispiel 4.2. Beispiele für gerade Zahlen sind $64, 300, 2024, \ldots$, und ungerade Zahlen sind zum Beispiel $57, 103, 1001, \ldots, 2023, \ldots$.

Betrachten wir alle einstelligen Zahlen. Dann sehen wir, dass von diesen 0, 2, 4, 6 oder 8 gerade sind, und ungerade sind genau 1, 3, 5, 7 oder 9. Man sieht, es geht $5:5$ aus, wenn wir die Anzahl vergleichen, Unentschieden. Ist das Zufall?

Wie sieht man einer Zahl an, ob sie gerade ist? Das kann man an der Darstellung als Zahl im Zehnersystem direkt sehen!

Satz 4.3 (Einerziffernkriterium)**.** *Eine natürliche Zahl ist genau dann gerade, wenn ihre Darstellung im Zehnersystem als Einerziffer eine* 0*,* 2*,* 4*,* 6 *oder* 8 *hat.*

Bemerkung 4.4. Der obige Satz behauptet eine „genau dann, wenn“-Aussage. Das bedeutet eigentlich zwei Aussagen:

(1) Eine gerade natürliche Zahl hat als Einerziffer eine der Ziffern 0, 2, 4, 6 oder 8.
(2) Eine natürliche Zahl, die im Zehnersystem als Einerziffer eine 0, 2, 4, 6 oder 8 hat, ist gerade.

Eine solche „genau dann, wenn“-Aussage nennt man auch eine Äquivalenz (Gleichwertigkeit). Bei einer solchen Äquivalenz kann man versuchen, gleichzeitig beide Richtungen zu beweisen. Besser ist es, weil man sich in der Argumentation fokussiert, beide Richtungen nacheinander zu beweisen. Das machen wir nun.

Beweis des Einerziffernkriteriums für gerade. Wir wollen die Äquivalenz von zwei Aussagen über eine beliebige Zahl n zeigen. Sprechen wir sie nochmals aus.

(a) Die Zahl n ist gerade.
(b) Die Einerziffer a_0 in der Darstellung $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$ im Zehnersystem ist gerade, also 0, 2, 4, 6 oder 8.

Zeigen wir zunächst $(b) \Longrightarrow (a)$. Sei also a_0 gerade, d.h. der Form $a_0 = 2 \cdot a$ für eine natürliche Zahl a. Wir müssen eine natürliche Zahl m finden, so dass $n = 2m$. Wir setzen an:

$$\begin{aligned} n = (a_k a_{k-1} \ldots a_1 a_0)_{10} &= a_k \cdot 10^k + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0 \\ &= 10 \cdot \left(a_k \cdot 10^{k-1} + \ldots + a_1 \cdot 10^0 \right) + a_0 \\ &= 2 \cdot 5 \cdot \left(a_k \cdot 10^{k-1} + \ldots + a_1 \cdot 10^0 \right) + 2 \cdot a \\ &= 2 \cdot \underbrace{\left(5 \cdot \left(a_k \cdot 10^{k-1} + \ldots + a_1 \cdot 10^0 \right) + a \right)}_{=:m} = 2m. \end{aligned}$$

Da m eine natürliche Zahl ist, folgt die Behauptung (a).

Wir zeigen nun die umgekehrte Richtung $(a) \Longrightarrow (b)$. Nach Voraussetzung ist n gerade. Es gibt also eine natürliche Zahl m mit $n = 2 \cdot m$. Wir wollen daraus die Einerziffer von n in der Darstellung im Dezimalsystem bestimmen.

Dazu benutzen wir die Darstellung von m im Zehnersystem; sei diese $m = (b_\ell b_{\ell-1} \dots b_1 b_0)_{10}$. Dann ist

$$\begin{aligned} n = 2 \cdot m &= 2\Big(b_\ell \cdot 10^\ell + \dots + b_1 \cdot 10^1 + b_0 \cdot 10^0\Big) \\ &= 2\Big(b_\ell \cdot 10^\ell + \dots + b_1 \cdot 10^1\Big) + 2b_0 \\ &= 10 \cdot \underbrace{\Big(2 \cdot \big(b_\ell \cdot 10^{\ell-1} + \dots + b_1 \cdot 10^0\big)\Big)}_{=:x} + 2b_0 \\ &= 10 \cdot x + 2b_0. \end{aligned}$$

Jetzt machen wir eine Fallunterscheidung. Im Prinzip berechnen wir die Einerstelle von $2m$. Das ist wie beim schriftlichen Addieren von Zahlen im Zehnersystem, und zwar $m + m$. Das beginnt mit der Einerstelle und da kann es einen Übertrag geben, oder auch nicht. Das sind die zwei Fälle.

Fall 1, es gibt keinen Übertrag: Das bedeutet, unser b_0 ist eine Ziffern ≤ 4. Damit ist $c = 2b_0$ eine gerade Ziffer, also eine Ziffer 0, 2, 4, 6 oder 8.

Wir schreiben x im Zehnersystem als $x = (c_s c_{s-1} \dots c_1 c_0)_{10}$. Dann rechnen wir

$$\begin{aligned} n = 10 \cdot x + 2b_0 &= 10 \cdot \Big(c_s \cdot 10^s + c_{s-1} \cdot 10^{s-1} + \dots + c_1 \cdot 10^1 + c_0 \cdot 10^0\Big) + 2b_0 \\ &= c_s \cdot 10^{s+1} + c_{s-1} \cdot 10^s + \dots + c_1 \cdot 10^2 + c_0 \cdot 10^1 + c \\ &= (c_s c_{s-1} \dots c_1 c_0 c)_{10}. \end{aligned}$$

Der letzte Schritt funktioniert, weil c auch eine Ziffer ist. Somit haben wir in der Tat die Darstellung von n im Zehnersystem gefunden. Diese hat die Einerstelle $c = 2b_0$, und das ist gerade. Damit sind wir in diesem Fall fertig.

Fall 2, es gibt einen Übertrag: Das bedeutet, unser b_0 ist eine Ziffern ≥ 5. Damit ist $2b_0$ eine der Zahlen 10, 12, 14, 16 oder 18. Es gibt damit eine gerade Ziffer c mit $2b_0 = (1c)_{10} = 10 + c$.

Jetzt haben wir

$$n = 10 \cdot x + 2b_0 = 10 \cdot x + 10 + c = 10 \cdot (x + 1) + c.$$

(Die 1 ist der Übertrag!) Wir schreiben $x + 1$ im Zehnersystem als $x + 1 = (c_s c_{s-1} \dots c_1 c_0)_{10}$. Dann rechnen wir

$$\begin{aligned} n = 10 \cdot (x + 1) + c &= 10 \cdot \Big(c_s \cdot 10^s + c_{s-1} \cdot 10^{s-1} + \dots + c_1 \cdot 10^1 + c_0 \cdot 10^0\Big) + c \\ &= c_s \cdot 10^{s+1} + c_{s-1} \cdot 10^s + \dots + c_1 \cdot 10^2 + c_0 \cdot 10^1 + c \\ &= (c_s c_{s-1} \dots c_1 c_0 c)_{10}. \end{aligned}$$

Der letzte Schritt funktioniert, weil c auch eine Ziffer ist.. Somit haben wir in der Tat die Darstellung von n im Zehnersystem gefunden. Diese hat als Einerstelle die gerade Ziffer c. Damit sind wir auch in diesem Fall fertig. □

Ein Korollar ist eine unmittelbare Folgerung aus einem Satz, einer Proposition oder ähnlichem, oder manchmal sogar aus deren Beweis. Es handelt sich im Prinzip um ein Abstaubertor. Ein solches können wir nun sch(l)ießen.

Korollar 4.5. *Eine natürliche Zahl ist genau dann ungerade, wenn ihre Darstellung im Zehnersystem als Einerziffer eine* 1, 3, 5, 7 *oder* 9 *hat.*

Beweis. Das folgt sofort aus Satz 4.3. □

Gerade Zahlen sind durch eine darstellende Formel (Zahlen der Form $2m$) beschrieben, sogar definiert. Für ungerade Zahlen möchten wir eine analoge Beschreibung.

Lemma 4.6. *Eine ungerade Zahl hat die Form $2 \cdot m + 1$ für eine natürliche Zahl m.*
Genauer gilt: sei n eine natürliche Zahl. Dann sind äquivalent:
(a) Die Zahl n ist ungerade.
(b) Es gibt eine natürliche Zahl m mit der Eigenschaft $n = 2 \cdot m + 1$.

Beweis. Wir zeigen zuerst $(a) \Longrightarrow (b)$: Sei n ungerade. Dann endet die Darstellung von n im Zehnersystem nach Korollar 4.5 auf 1, 3, 5, 7 oder 9. Wenn wir nun 1 subtrahieren, dann ergibt sich kein Übertrag, wir müssen also nur die Einerziffer um 1 vermindern. Somit endet $n-1$ auf 0, 2, 4, 6, oder 8. Nach Satz 4.3 ist $n-1$ gerade.

Zwischenüberlegung: ist $n-1$ überhaupt noch eine natürliche Zahl, für die gerade und ungerade definiert sind? Ja! Hier geht es darum, dass auffällt, dass noch etwas zu beachten ist, bevor man Satz 4.3 anwenden kann. Alle natürlichen Zahlen n außer der 0 haben eine natürliche Zahl $n-1$ als Vorgänger (lernen wir in Kaptiel §8). Da unser n als ungerade Zahl nicht 0 ist, hat n also einen solchen Vorgänger.)

Weiter geht's. Weil $n-1$ gerade ist, daher es eine natürliche Zahl m mit $n-1 = 2m$. Auflösen nach n liefert die gewünschte Gleichung $n = 2m + 1$.

Jetzt zeigen wir $(b) \Longrightarrow (a)$: Wir haben nun also eine natürliche Zahl m mit $n = 2m + 1$. Die Zahl $2m$ ist eine gerade Zahl (per Definition). Daher ist die Einerziffer von $2m$ im Zehnersystem eine der Ziffern 0, 2, 4, 6 oder 8, das wissen wir aus Satz 4.3. Wenn wir 1 dazuaddieren, dann ergibt sich kein Übertrag und die Einerziffer von $2n+1$ berechnet sich zu 1, 3, 5, 7 oder 9. Nach Korollar 4.5 ist n dann ungerade. □

4.2. Rechnen mit gerade und ungerade.

⚠ Mit gerade und ungerade kann man aufgrund der folgenden Propositionen sinnvoll rechnen: Addition und Multiplikation hängt nicht von den konkreten Zahlenwerten ab, nur von den Eigenschaften gerade und ungerade.

Proposition 4.7 (Multiplikation)**.** *Seien a und b natürliche Zahlen. Dann gilt:*

$$a \cdot b \text{ ist } \begin{cases} \text{gerade} & \text{wenn } a \text{ oder } b \text{ gerade sind,} \\ \text{ungerade} & \text{wenn } a \text{ und } b \text{ ungerade sind,} \end{cases}$$

Proposition 4.8 (Addition)**.** *Seien a und b natürliche Zahlen. Dann gilt:*

$$a + b \text{ ist } \begin{cases} \text{gerade} & \text{wenn } a \text{ und } b \text{ gerade, oder} \\ & \text{wenn } a \text{ und } b \text{ ungerade sind,} \\ \text{ungerade} & \text{wenn } a \text{ gerade und } b \text{ ungerade, oder} \\ & \text{wenn } a \text{ ungerade und } b \text{ ungerade sind.} \end{cases}$$

Beweis. Wir beweisen nur ein paar dieser Aussagen. Seien a und b gerade. Dann gibt es per Definition natürliche Zahlen a' und b' mit $a = 2a'$ und $b = 2b'$. Wir rechnen dann

$$a + b = 2a' + 2b' = 2(a' + b'),$$
$$a \cdot b = (2a') \cdot (2b') = 2 \cdot (2a'b').$$

Da $a' + b'$ und $2a'b'$ auch natürliche Zahlen sind, sind in diesem Fall $a + b$ und $a \cdot b$ gerade.

Seien a und b beide ungerade. Dann gibt es nach Lemma 4.6 natürliche Zahlen a' und b' mit $a = 2a' + 1$ und $b = 2b' + 1$. Wir rechnen dann

$$a + b = (2a' + 1) + (2b' + 1) = 2(a' + b' + 1),$$
$$a \cdot b = (2a' + 1) \cdot (2b' + 1) = 4a'b' + 2a' + 2b' + 1 = 2 \cdot (2a'b' + a' + b') + 1.$$

Da $a'+b'+1$ und $2a'b'+a'+b'$ auch natürliche Zahlen sind, sind in diesem Fall $a+b$ gerade und $a\cdot b$ nach Lemma 4.6 ungerade. □

Bemerkung 4.9. Die Aussagen von Proposition 4.7 und Proposition 4.8 faßt man kurz so zusammen:

- gerade plus gerade ist gerade,
- gerade plus ungerade ist ungerade,
- ungerade plus ungerade ist gerade,
- gerade mal egal was ist gerade, und
- ungerade mal ungerade ist ungerade.

Eine weitere Möglichkeit, die Aussagen übersichtlich darzustellen ist eine Verknüpfungstafel. In den Feldern steht das Ergebnis der angegebenen Verknüpfung (Addition oder Multiplikation), und zwar mit a aus der ersten Spalte und b aus der obersten Zeile; etwa so:

$a+b$	gerade	ungerade
gerade	gerade	ungerade
ungerade	ungerade	gerade

$a\cdot b$	gerade	ungerade
gerade	gerade	gerade
ungerade	gerade	ungerade

Noch eindrücklicher wird es, wenn man anstelle von gerade und ungerade die jeweils kleinsten Vertreter dieser Eigenschaften nimmt, nämlich 0 für gerade und 1 für ungerade. Dann werden die Verknüpfungstafeln zu

$a+b$	0	1
0	0	1
1	1	0

$a\cdot b$	0	1
0	0	0
1	0	1

Hier ist nun mehr nur noch $1+1=0$ merkwürdig, besagt aber eigentlich nur, dass ungerade + ungerade wieder gerade ist.

4.3. **Nochmal Springerzüge.** Wir kehren nochmals zum Springer auf dem Schachbrett zurück. Dazu statten wir das Schachbrett mit Koordinaten aus bei dem statt $a,b,c,\dots,h$ mit $1,2,\dots,8$ durchnummeriert wird. Die Felder sind dann $(a|b)$ mit natürlichen Zahlen a,b mit $1\le a,b\le 8$.

Proposition 4.10. *Das Feld $(a|b)$ auf dem Schachbrett ist*
(1) schwarz, wenn $a+b$ gerade ist, und
(2) weiß, wenn $a+b$ ungerade ist.

Dies beweisen wir im Prinzip mit vollständiger Induktion. Mehr dazu im Kapitel §8.

Beweis. Zunächst stellen wir fest, dass die Aussage für das Feld $(1|1)$, aka a1, richtig ist, denn $1+1=2$ ist gerade und das Feld ist schwarz.

Wir laufen nun wie ein Turm über die Felder, aber immer nur einen Schritt. Sei $(c|d)$ das Feld auf dem der Turm aktuell steht und für das der Satz bereits gelten soll, und sei $(a|b)$ das Nachbarfeld, auf das der Turm im nächsten Schritt zieht. Diese Nachbarfelder unterscheiden sich nun in genau einer Koordinate um genau 1. Damit ist $a+b$ entweder $c+d+1$ oder $c+d-1$. Weil 1 ungerade ist, ist also $a+b$ gerade, wenn $c+d$ ungerade ist, und $a+b$ ungerade, wenn $c+d$ gerade ist. Außerdem haben Nachbarfelder auf dem Schachbrett unterschiedliche Farben. Damit gibt es nun zwei Fälle

(1) Sei $(a|b)$ weiß. Dann ist $(c|d)$ als Nachbarfeld schwarz. Hier gilt die Aussage schon, also ist $c+d$ gerade, somit ist $a+b=c+d\pm 1$ ungerade, und der Satz gilt auch für $(a|b)$.
(2) Sei $(a|b)$ schwarzs. Dann ist $(c|d)$ als Nachbarfeld weiß. Hier gilt die Aussage schon, also ist $c+d$ ungerade, somit ist $a+b=c+d\pm 1$ gerade, und der Satz gilt auch für $(a|b)$.

Mit dem Turm können wir nun von a1 startend im Schneckentempo über das ganze Schachfeld laufen. Bei jedem Schritt „beweisen“ wir die Aussage für das Feld, das wir betreten. Am Ende ist die Aussage für das ganze Schachfeld beweisen. □

Proposition 4.11. *Ein Springer ändert bei jedem Zug seine Feldfarbe.*

Beweis. Der Springer zieht bei einem Zug in eine Koordinatenrichtung um 2 Felder und in der anderen um 1 Feld. Ausgehend vom Feld $(a|b)$ erreicht der Springer daher die Felder

$$(a \pm 2|b \pm 1) \text{ und } (a \pm 1|b \pm 2),$$

wobei jeweils alle möglichen Vorzeichen vorkommen. Sei $(c|d)$ das Zielfeld, dann ist

$$c + d = a + b \pm 2 \pm 1 = \begin{cases} a+b+3 \\ a+b+1 \\ a+b-1 \\ a+b-3 \end{cases}$$

Weil 1 und 3 ungerade sind, ist $c + d$ ungerade, falls $a + b$ gerade ist, und $c + d$ ist gerade, falls $a + b$ ungerade ist. Daher wechselt die Feldfarbe nach Proposition 4.10. □

Take home message Kapitel §4.

- gerade Zahlen: $2a$ mit natürlicher Zahl a.
- ungerade Zahlen: $2b + 1$ mit natürlicher Zahl b.
- gerade und ungerade: Test über die Einerziffer im Zehnersystem.
- Mit gerade und ungerade kann man rechnen (Addition/Subtraktion(!) und Multiplikation): wie mit 0 (gerade) und 1 (ungerade) und der Spezialregel $1 + 1 = 0$.

5. Teilbarkeitsregeln

Quellen: [GK23] Kapitel 7.1, 7.4 und 9

Wir haben im vorherigen Kapitel §4.2 gelernt, wie man einer natürlichen Zahl im Zehnersystem an der Einerziffer ansehen kann, dass sie von der Form $2m$ ist, also eine gerade Zahl. Dies wollen wir in diesem Kapitel ausbauen.

5.1. Teilbarkeit.

Definition 5.1. Seien a und m natürliche Zahlen. Dann ist a durch m **teilbar**, wenn es eine natürliche Zahl x gibt mit

$$a = m \cdot x.$$

Wir schreiben das kurz $m \mid a$, gelesen „m teilt a“. Wenn a nicht durch m teilbar ist, dann schreiben wir $m \nmid a$, gelesen „m teilt nicht a“.

Beispiel 5.2.

(1) Es ist $7 \cdot 13 = 91$, also ist 91 durch 7 teilbar.
(2) $7 \mid 123.123.123.123$.
(3) 9 teilt nicht 123.123.123.123.
(4) Es ist $11 \cdot 9 < 100 = 11 \cdot 9 + 1 < 11 \cdot 10$, somit 100 nicht durch 11 teilbar. Hier schummeln wir ein wenig und benutzen Division mit Rest, hier 100 ist $9 \cdot 11$ mit Rest 1, oder wir benutzen die folgenden Ungleichungen. Angenommen $100 = 11 \cdot x$ mit einer natürlichen Zahl x. Dann folgt aus
$$11 \cdot 9 < 11 \cdot x < 11 \cdot 10$$
auch $9 < x < 10$. aber zwischen 9 und 10 liegt keine natürliche Zahl: Widerspruch.
(5) Eine Zahl ist genau dann gerade, wenn sie durch 2 teilbar ist. Die Definition von gerade ist genau der Spezialfall der Definition von Teilbarkeit mit $m = 2$.

Lemma 5.3. *Jede natürliche Zahl teilt* 0.

Beweis. Sei n eine belibige natürliche Zahl. Dann gilt $n \cdot 0 = 0$. Also gilt $n \mid 0$. □

Bemerkung 5.4. Warum gilt denn die so selbverständlich hingeschriebene Gleichung $n \cdot 0 = 0$? Das sieht man am besten so ein. Aus der Geleichung $0 + 0 = 0$ folgt mittels des Distributivgesetzes (Ausklammern/Ausmultiplizieren)

$$n \cdot 0 = n \cdot (0 + 0) = n \cdot 0 + n \cdot 0.$$

Wenn wir in dieser Gleichung auf beiden Seiten die gleiche, noch unbekannte Zahl, $n \cdot 0$ abziehen, erhalten wir die Behauptung

$$0 = n \cdot 0.$$

Lemma 5.5. *Die* 1 *teilt jede natürliche Zahl.*

Beweis. Sei n eine belibige natürliche Zahl. Dann gilt $1 \cdot n = n$. Also gilt $1 \mid n$. □

5.2. Teiler.

Definition 5.6. Die **Teiler** einer natürlichen Zahl n sind alle natürlichen Zahlen a, welche n teilen.

Beispiel 5.7.

(1) Die Teiler von 49 sind $1, 7$ und 49.
(2) Die Teiler von 128 sind $1, 2, 4, 8, 16, 32, 64$ und 128.
(3) Die Teiler von 24 sind $1, 2, 3, 4, 6, 8, 12$ und 24.

Bemerkung 5.8. Die Teiler einer Zahl treten immer in Paaren auf, denn aus $a \mid n$ folgt die Existenz einer Faktorisierung $n = a \cdot b$ und dann ist auch $b \mid n$.

Man bestimmt daher die Teiler einer Zahl am besten gleichzeitig „von unten und von oben“:

$$24 = 1 \cdot 24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6$$

zeigt die Teiler $1, 2, 3, 4, 6, 8, 12$ und 24. Man kann bei 5, was nicht teilt aufhören, weil dann der zweite Faktor kleiner als der erste Faktor geworden ist.

5.3. **Teilbarkeitsregeln.**

Proposition 5.9. *Eine natürliche Zahl wird genau dann durch* 10 *geteilt, wenn die Einerziffer im Zehnersystem* 0 *ist.*

Beweis. Wir rechnen im Zehnersystem für eine beliebeige natürliche Zahl $(a_k a_{k-1} \dots a_1 a_0)_{10}$

$$\begin{aligned} 10 \cdot (a_k a_{k-1} \dots a_1 a_0)_{10} &= 10 \cdot \left(a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \right) \\ &= a_k \cdot 10^{k+1} + a_{k-1} \cdot 10^k + \dots + a_2 \cdot 10^3 + a_1 \cdot 10^2 + a_0 \cdot 10^1 \\ &= a_k \cdot 10^{k+1} + a_{k-1} \cdot 10^k + \dots + a_2 \cdot 10^3 + a_1 \cdot 10^2 + a_0 \cdot 10^1 + 0 \cdot 10^0 \\ &= (a_k a_{k-1} \dots a_1 a_0 0)_{10}. \end{aligned}$$

Diese Rechnung zeigt die Proposition. Wir haben zwei Richtungen zu zeigen. Wenn n als Einerziffer eine 0 hat, dann ist es von der Form $(a_k a_{k-1} \dots a_1 a_0 0)_{10}$, also nach der Rechnung (rúckwärts betrachtet) von der Form $10 \cdot x$.

Umgekehrt, wenn unser n von der Form $10 \cdot x$ ist, dann zeigt die Rechnung mit

$$x = (a_k a_{k-1} \dots a_1 a_0)_{10},$$

dass n als Einerziffer eine 0 hat. □

Der Beweis beruht auf der Herleitung einer nützlichen und sicher wohlbekannten, aber nun bewiesenen Formel für die Multiplikation mit 10 einer natürlichen Zahl im Zehnersystem. Diese halten wir als Korollar zum Beweis fest.

Korollar 5.10. *Sei $n = (a_k \dots a_1 a_0)_{10}$ eine natürliche Zahl mit Darstellung im Zehnersystem. Dann gilt*

$$10 \cdot (a_k a_{k-1} \dots a_1 a_0)_{10} = (a_k a_{k-1} \dots a_1 a_0 0)_{10}.$$

Beweis. Auch Korollare muß man beweisen. Aber in diesem Fall haben wir im Text davor darauf verwiesen, dass die Behauptung des Korollars aus dem Beweis von Proposition 5.9 folgt. Dieser Verweis reicht als Beweis, denn dem ist nun wirklich nichts hinzuzufügen. □

Teilen hat etwas mit fairem Austeilen zu tun. Wenn eine Zahl durch 7 teilbar ist, dann kann man sie auf 7 Mitspieler:innen fair verteilen, etwa Spielkarten. Das Austeilen kann dabei in Paketen erfolgen: zuerst bekommt jeder 10 Karten, das brauch $7 \cdot 10$ Karten, dann jeder nochmal 5, das brauch $7 \cdot 5$ Karten, und dann nochmal jeder eine: $7 \cdot 1$ Karten. Zusammen haben wir dann

$$(7 \cdot 10) + (7 \cdot 5) + (7 \cdot 1) = 7 \cdot (10 + 5 + 1)$$

Karten verteilt.

Beispiel 5.11.

(1) 7 teilt 777.714.777, dennn $7 \cdot 111.100.111$ ergibt 777.700.777 und wenn wir das abziehen, dann bleiben $14.000 = 7 \cdot 2.000$.

(2) 3 teilt nicht 369.724, denn $3 \cdot 123.000$ ergibt 369.000 und wenn wir das abziehen bleibt 724. Weiter ist $24 = 3 \cdot 8$, und wenn wir das abziehen, bleibt $700 = 7 \cdot 10 \cdot 10$, und das ist nicht durch 3 teilbar. (Vorgriff: eindeutige Primfaktorzerlegung!)

Satz 5.12. *Seien $a \geq b$ und m natürliche Zahlen. Wir nehmen an, dass m ein Teiler von $a-b$ ist. Dann gilt:*

a ist durch m teilbar genau dann, wenn b durch m teilbar ist.

Beweis. Nach Voraussetzung gibt es eine natürliche Zahl x mit $a - b = m \cdot x$. Wir haben wieder zwei Richtungen zu beweisen. Wir nehmen zuerst an, dass b durch m teilbar ist, und zeigen, dass dann auch a durch m teilbar ist. Sei also y eine natürliche Zahl mit $b = m \cdot y$. Dann gilt

$$a = (a-b) + b = m \cdot x + m \cdot y = m \cdot (x+y). \tag{5.1}$$

Weil $x + y$ auch eine natürliche Zahl ist, folgt aus (5.1) per Definition, dass a durch m teilbar ist.

Die andere Richtung (wenn a durch m teilbar ist, dann ist b durch m teilbar) geht genauso und wird zur Übung überlassen. Die entscheidende Rechnung verraten wir:

$$b = a - (a-b). \qquad \square$$

Frage 5.13. Ist die folgende Zahl durch 9 teilbar?

$$123000000000000000000\ldots0000000000000000000000000000000000000003$$

Definition 5.14. Die **Quersumme** einer natürlichen Zahl is die Summe der Ziffern im Zehnersystem. Also, wenn $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$, dann ist die Quersumme $a_k + a_{k-1} + \ldots + a_1 + a_0$.

Wir schreiben zur Abkürzung für die Quersumme von n das Symbol $Q(n)$.

Beispiel 5.15. Die Quersumme von 1234 ist $1 + 2 + 3 + 4 = 10$.

Satz 5.16. *Eine natürliche Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.*

Beweis. Nach Satz 5.12 reicht es aus, zu zeigen, dass die Differenz $n - Q(n)$ durch 9 teilbar ist. (Warum ist stets $n \geq Q(n)$?)

Sei $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$ die Darstellung im Zehnersystem. Dann rechnen wir

$$\begin{aligned} n - Q(n) &= (a_k a_{k-1} \ldots a_1 a_0)_{10} - (a_k + \ldots + a_0) \\ &= \left(a_k \cdot 10^k + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0\right) - (a_k + \ldots + a_0) \\ &= (a_k \cdot 10^k - a_k) + \ldots + (a_1 \cdot 10^1 - a_1) + (a_0 \cdot 10^0 - a_0) \\ &= a_k \cdot (10^k - 1) + \ldots + a_1 \cdot (10^1 - 1) + a_0 \cdot (10^0 - 1). \end{aligned}$$

Die Summanden enthalten alle einen Faktor der Form $10^i - 1$ mit $0 \leq i \leq k$. Das ist

$$10^i - 1 = (\underbrace{99\ldots99}_{i \text{ viele Stellen}})_{10} = 9 \cdot (\underbrace{11\ldots11}_{i \text{ viele Stellen}})_{10}.$$

Hier steckt also in jedem Summanden ein Faktor 9 (überlegen Sie sich, dass das auch für $i = 0$ richtig ist!). Diese Faktor 9 kann man ausklammern, um damit eine Formel

$$n - Q(n) = 9 \cdot x$$

zu erhalten. Hier ist x die natürliche Zahl, die beim Ausklammern der 9 übrig bleibt. Die genaue Form tut nichts zur Sache und verwirrt nur. Daher haben wir uns nicht bemüht, sie genau zu ermitteln. Jedenfalls sagt die erhaltene Formel, dass $n - Q(n)$ durch 9 teilbar ist, und das war zu beweisen. $\square$

Beispiel 5.17. Die Quersumme von

$$n = 123000000000000000000\ldots0000000000000000000000000000000000000003$$

ist 9, somit ist n durch 9 teilbar.

Satz 5.18. *Eine natürliche Zahl ist genau dann durch* 3 *teilbar, wenn ihre Quersumme durch* 3 *teilbar ist.*

Beweis. Das geht fast wörtlich genauso wie der Beweis von Satz 5.16. Formulieren sie den Beweis zur Übung aus. □

Beispiel 5.19. Wir bestimmen die kleinste 7-stellige Zahl, die durch 9 teilbar ist und in der keine Ziffer mehr als einmal vorkommt. Wir suchen also 7 Ziffern, keine zwei gleich, so dass die daraus in einer geeigneten Reihenfolge gebildete Zahl möglichst klein ist. Für die Größe der Zahl sind die führenden Ziffern verantwortlich. Wenn die Zahl klein sein soll, müssen diese möglichst klein sein, also am wichtigsten ist die führende Ziffer, dann die nächste und so weiter. Da wir jede Ziffer nur einmal benutzen können, würden also gerne die Zahl

$$(0123456)_{10}$$

betrachten. Das ist aber keine gültige natürliche Zahl, wegen der führenden 0. Korrigieren wir dies, so erhalten wir

$$(1023456)_{10}.$$

Das ist die kleinste 7-stellige Zahl, die keine Ziffer mehr als einmal enthält. Jetzt fragt sich, ob diese Zahl durch 9 teilbar ist. Das testen wir mit der Quersumme

$$Q(1023456) = 1 + 0 + 2 + 3 + 4 + 5 + 6 = 21.$$

Das ist nicht durch 9 teilbar. Wir müssen also die Ziffern etwas erhöhen, so dass wir auf eine durch 9 teilbare Quersumme kommen. Die nächste durch 9 teilbare Zahl > 21 ist 27. Es fehlen also 6. Am wenigsten größer wird die Zahl, wenn wir die Einerziffer vergrößern. Das erreicht

$$(1023459)_{10}$$

mit Quersumme 24. Fehlen weiterhin 3. Also ist

$$(1023489)_{10}$$

die richtige Antwort.

Bemerkung 5.20. Manchmal ist die Quersumme einer Zahl immer noch zu groß, um daran die Teilbarkeit durch 9 (oder 3) direkt ablesen zu können. In diesem Fall wiederholen Sie das Bilden der Quersumme! Beispielsweise ist für

$$n = (4444444444\ldots444444)_{10}$$

aus 10.000.000 Stellen die Quersumme $Q(n) = 40.000.000$. Davon die Quersumme ist 4. Weil 4 nicht durch 9 teilbar ist, kann auch $Q(n)$ nicht durch 9 teilbar sein, und das wiederum erzwingt, dass n nicht durch 9 teilbar ist.

Satz 5.21. *Eine natürliche Zahl ist genau dann durch* 5 *teilbar, wenn ihre Einerziffer im Zehnersystem* 0 *oder* 5 *ist.*

Beweis. Die Ziffern 0 und 5 sind genau die durch 5 teilbaren Ziffern. Sei n die natürliche Zahl und $n = (a_k a_{k-1}\ldots a_1 a_0)_{10}$ die Darstellung im Zehnersystem. Dann reicht es nach Satz 5.12 zu zeigen, dass $n - a_0$ durch 5 teilbar ist. Dazu rechnen wir

$$\begin{aligned} n - a_0 &= (a_k a_{k-1}\ldots a_1 a_0)_{10} - a_0 \\ &= (a_k a_{k-1}\ldots a_1 0)_{10} = 10 \cdot (a_k a_{k-1}\ldots a_1)_{10} \\ &= 5 \cdot \Big(2 \cdot (a_k a_{k-1}\ldots a_1)_{10}\Big). \end{aligned}$$

□

Satz 5.22. *Eine natürliche Zahl ist genau dann durch 4 teilbar, wenn die aus Zehner- und Einerziffer gebildete zweistellige Zahl durch 4 teilbar ist.*

Beweis. Das gilt wieder nach Satz 5.12, denn betrachten wir $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$, so sollen wir mit der zweistelligen Zahl $(a_1 a_0)_{10}$ vergeleichen. Die Differenz ist nun

$$\begin{aligned} n - (a_1 a_0)_{10} &= (a_k a_{k-1} \dots a_2 00)_{10} \\ &= 100 \cdot (a_k a_{k-1} \dots a_2)_{10} \\ &= 4 \cdot \Big(25 \cdot (a_k a_{k-1} \dots a_2)_{10}\Big). \end{aligned}$$

□

Bemerkung 5.23. Die Teilbarkeitsregeln durch 2, 4, 5 und 10 laufen alle nach dem gleichen Muster. Das kann man Verallgemeinern. Diese Zahlen sind von der Form $2^a \cdot 5^b$. Sei m das Maximum der beiden Exponenten a und b. Dann gilt für eine natürliche Zahl $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$:

(a) n ist genau dann durch $2^a 5^b$ teilbar, wenn
(b) die aus den letzten m Stellen von n gebildete Zahl durch $2^a 5^b$ teilbar ist.

Der Beweis geht wie gehabt mit Satz 5.12 und beruht auf der Rechnung

$$\begin{aligned} n - (a_{m-1} \dots a_0)_{10} &= (a_k a_{k-1} \dots a_m 0 \dots 0)_{10} \\ &= 10^m \cdot (a_k a_{k-1} \dots a_m)_{10} \\ &= 2^a 5^b \cdot \Big(2^{m-a} 5^{m-b} \cdot (a_k a_{k-1} \dots a_m)_{10}\Big). \end{aligned}$$

Es ist nämlich wegen $m \geq a$ und $m \geq b$ der Faktor $2^{m-a} 5^{m-b}$ eine natürliche Zahl.

5.4. **Weiterführende Fragen.**

Frage 5.24. Warum gibt es keine bekannte Teilbarkeitsregel durch 11 oder durch 7?

5.5. **Märchenstunde: vollkommene Zahlen.** Die Spielerei mit natürlichen Zahlen ist so alt wie die Mathematik. Schon den alten Griechen (siehe Euklids Elemente) fiel auf, dass für manche Zahlen eine merkwürdige Beziehung zwischen den Teilern einer Zahl n und er Zahl n selbst besteht. Teiler von n sind ja multiplikative Teile von n. Wenn man diese nun addiert, dann gibt es keinen Grund, dass man wieder n herauskommt. Nun, so naiv tut man das natürlich nur bei $n = 1$. Denn $n = n \cdot 1$ zeigt ja $n \mid n$ und $1 \mid n$, und so sind is die Summe der Teiler $\geq 1 + n$. (Warum ist $n = 1$ eine Ausnahme? Wo liegt die UNgenauigkeit in der Argumentation?) Also präzisieren wir die Eigenschaft, die wir vollkommen nennen wollen, in der folgenden Definition.

Definition 5.25. Eine natürliche Zahl n heißt **vollkommen**, wenn sie die Summe ihrer Teiler, die kleiner als n sind, ist.

Beispiel 5.26. Wir berechnen einige Teilersummen.

(1) $n = 6$ hat Teiler $1, 2, 3$ und 6. Die zu betrachtende Summe ist $1 + 2 + 3 = 6$. Die 6 is vollkommen. Prüfen Sie, dass 6 die kleinste vollkommene Zahl ist.
(2) $n = 10$ hat Teiler $1, 2, 5$ und 10. Die zu betrachtende Summe ist $1 + 2 + 5 = 8$. Das ist zu klein.
(3) $n = 12$ hat Teiler $1, 2, 3, 4, 6$ und 12. Die zu betrachtende Summe ist $1 + 2 + 3 + 4 + 6 = 16$. Das ist zu groß.
(4) $n = 81$. Das ist 3^4, hat also nur Teiler der Form 3^a, also $1, 3, 9, 27$ und 81. Die zu betrachtende Summe ist $1 + 3 + 9 + 27 = 40$.
(5) $n = 28$ hat Teiler $1, 2, 4, 7, 14$ und 28. Die zu betrachtende Summe ist $1 + 2 + 4 + 7 + 14 = 28$. Die 28 is vollkommen. Prüfen Sie, dass 28 die zweitkleinste vollkommene Zahl ist.

Wir müssen kurz an Primzahlen erinnern, über die noch zu sprechen sein wird.

Definition 5.27. Eine **Primzahl** ist eine natürliche Zahl $p \geq 2$, die nur durch 1 und sich selbst teilbar ist, d.h. wenn $p = ab$ mit natürlichen Zahlen a und b, dann gilt $a = 1$ oder $b = 1$.

Nun können wir erzählen, was man seit Euklid und Euler über vollkommene Zahlen weiß.

Satz 5.28 (Euklid und Euler)**.** *Eine gerade natürliche Zahl n is vollkommen genau dann, wenn es eine Primzahl p gibt, so dass $2^p - 1$ auch Primzahl ist und*

$$n = 2^{p-1} \cdot (2^p - 1).$$

Der Satz gibt eine vollständige Antwort für gerade Zahlen. Trotz der befriedigenden Charakterisierung gerader vollkommener Zahlen ist unbekannt, ob es von diesen unendlich viele gibt, denn die Bedingung an die Primzahl p, dass $2^p - 1$ auch Primzahl ist, scheint sehr stark zu sein. Wir wissen nicht, ob es von diesen unendlich viele gibt.

Bei den ungeraden vollkommenen Zahln sind die Fragen noch in viel größerem Maß offen: es ist keine einzige bekannt, und niemand weiß, ob es solche geben muß. Das ist eine offene Forschungsfrage.

Take home message Kapitel §5.

- Begriffe: teilbar, nicht teilbar, Teiler. Notation $a \mid n$ und $a \nmid n$.
- gerade ist dasselbe wie teilbar durch 2.
- Teilbarkeitsregeln durch $2, 3, 4, 5, 9, 10$.
- Die Quersumme einer natürlichen Zahl im Zehnersystem.

6. Mathematische Sprache und Aussagenlogik

Quellen: [GK23] Kapitel 1, [SchSt18] Kapitel 1.2 und 3.1+2

⚠ Mathematik hat eine **eigene Sprache**. Diese ist hochpräzise und hochverdichtet, also effektiv. Auch das mathematische Argumentieren hat strenge Regeln, die **Aussagenlogik**, deren strikte Befolgung zu einem äußerst stabilen Gebäude der Mathematik führt.

Was einmal korrekt bewiesen wurde, stimmt bis in alle Ewigkeit. Das geht weit über das inflationär gebrauchte „Ist doch logisch!“ der Alltagssprache hinaus.

6.1. **Symbole und Syntax: mathematisches Alphabet und Grammatik.** Mathematik wird geschrieben mit

(1) eigenen Symbolen: zum Beispiel
- $+, \cdot, =, <, >, \dots$
- Zahlen: 0, 1, 2, $\dots \infty, \dots$
- komplizierter $\int_a^x f(t)dt$, $\lim_{x\to\infty} h(x)$, oder noch komplizierter $\mathrm{H}^i_{\text{ét}}(X_{\bar{k}}, \mathbb{Q}_\ell)$ $\dots$
- $(,), [,], \{,\}, \dots$, hauptsächlich zur Hervorhebung von hierarchischer Struktur

(2) Variablen: zum Beispiel
- x, y, n, a, b $\dots$
- a_0, a_1, $\dots a_k$ $\dots$ (Variablen mit Index).

(3) mathematischen Begriffen (die vorher definiert wurden): zum Beispiel
- natürliche Zahl
- gerade, ungerade
- teilt, Teiler
- vollständige Springerreise

(4) logische Schlüsselwörtern: zum Beispiel
- und
- oder
- nicht
- dann, wenn
- dann und nur dann, wenn
- genau dann, wenn (gdw.)
- für $\dots$ gilt: $\dots$
- daraus folgt
- dann gilt
- dies impliziert

(5) und Quantoren:
- für alle (abgekürzt $\forall$)
- jeder/s (gleichbedeutend zu $\forall$)
- es existiert (abgekürzt $\exists$)
- es gibt (gleichbedeutend mit $\exists$).

6.1.1. *Definitionen.* Mittels einer Definition erschafft man neue Begriffe aus alten. Es ist sorgfältig darauf zu achten, dass die Definition **wohldefiniert** ist. Darüber wurde schon in früheren Vorlesungen gesprochen.

6.1.2. *Syntax.* Es gelten spezifische „grammatikalische Regeln“, die festlegen, welche Kombination von Symbolen, Begriffen, logischen Schlüsselwörtern, Quantorenund Variablen erlaubt sind. Einen solchen erlaubten Ausdruck nennt man eine **Formel** oder eben einen **(syntaktisch korrekten) mathematischen Ausdruck**.

Beispiel 6.1. Erlaubte mathematische Ausdrücke sind zum Beispiel:
- $x + y$ [unbestimmt, aber syntaktisch ok]

- es gibt eine Primzahl p mit $p = 4$ [inhaltlich falsch, aber syntaktisch ok]
- für alle natürlichen Zahlen n gilt: n ist gerade genau dann, wenn $\exists m$ natürliche Zahl mit $n = 2m$.

Keine erlaubte mathematische Ausdrücke sind zum Beispiel:

- $(x + \lim_{n\to\infty})^2$ [Addition nimmt nur Zahlen oder **Terme** als Summanden]
- es gibt: $x + y = 1$. [es fehlen die Dinge, auf die sich das „es gibt“ bezieht].

6.2. **Aussagen, Semantik: wahr und falsch.** Mathematische Sprache wird in Aussagen formuliert. Die Regeln für den Umgang mit diesen Aussagen nennt man Aussagenlogik.

Fake Definition 6.2. Eine **(mathematische) Aussage** ist ein erlaubter mathematischer Ausdruck, der einen Wahrheitswert hat: eine Aussage ist entweder wahr (W) oder falsch (F); aber auf keinen Fall beides.

In [SchSt18] wird statt W die Notation 1 und für F die Notation 0 verwendet.

Bemerkung 6.3. Bei einer Aussage ist es nicht erforderlich, ob man entscheiden kann, ob die Aussage wahr oder falsch ist, solange sie eindeutig eines der beiden ist. (Machen Sie sich den Unterschied klar! Etwa an Beispiel (4).)

Beispiel 6.4. Beispiele für Aussagen sind:

(1) Kochsalz enthät Natrium oder Chlor.
(2) 6 ist eine ungerade Zahl.
(3) Für jede natürliche Zahl x ist x^2 durch 4 teilbar oder $x^2 - 1$ durch 4 teilbar.
(4) Es gibt eine ungerade vollkommene Zahl.
(5) Sei $x = 0$. Dann ist $e^x = 1$.

Die (1) ist wahr (man sagt auch richtig), denn Kochsalz ist eine Ionenverbindung aus Natrium und Chlor. Zum logischen „oder“ später mehr. Die (2) ist falsch, die (3) ist wahr und benuzt die Form „für jede“ als Ersatz für $\forall$. Bei der (4) weiss man nicht ob es wahr oder falsch ist, aber es ist eins von beidem.

Keine Aussagen sind:

(6) $e^x = 1$
(7) Ist heute Montag? (Fragen)
(8) Ich wünsche, es wäre heute Samstag. (Wünsche)
(9) Manchmal verstehe ich etwas nicht.
(10) 5 ist durch 2 teilbar.

Die (6) hängt die Wahrheit von x ab, also keine Aussage. Der Ausruf (9) beinhaltet mindestens zwei undefinierte Begriffe: manchmal und etwas. Abgesehen davon ist auch nicht klar, was „verstehen“ wirklich ausmacht. Oft bedeutet es einfach nur, dass man sich an etwas gewöhnt.

Zu (10). Umgangssprachlich ist „5 ist durch 2 teilbar.“ durchaus eine Aussage, denn wir ergänzen implizit wesentliche Informationen. Wir lesen das als

Die natürliche Zahl 5 ist in den natürlichen Zahlen durch 2 teilbar.

Dies ist eine Aussage, sie ist falsch. Wir könnten aber auch

Die natürliche Zahl 5 ist in den rationalen Zahlen durch 2 teilbar.

lesen, und dann ist es richtig. Ob etwas als Aussage gemeint ist, entscheidet nicht darüber, ob es eine Aussage ist. Man muss es unmißverständlich als Aussage verstehen, dann ist es eine Aussage. Präzision ist entscheidend.

6.3. **Neue Aussagen aus alten Aussagen bauen.**

Definition 6.5. (1) Die **Negation** (oder Verneinung) einer Aussage A ist die Aussage

$$\neg A,$$

gelesen „nicht A“. Es ist $\neg A$ genau dann wahr, wenn A falsch ist.

(2) Das logische **und** (die **Konjunktion**) zweier Aussagen A, B ist genau dann wahr, wenn beide Aussagen A und B wahr sind. Man findet die Notation

$$A \wedge B.$$

(3) Das logische **oder** (die **Disjunktion**) zweier Aussagen A, B ist genau dann wahr, wenn eine der beide Aussagen A oder B wahr ist. Gemeint ist hier mindestens eine, also „eine“ im Sinne von „es gibt eine“. Wenn mehr als eine Teilaussage wahr ist, dann ist das auch gut. Man findet die Notation

$$A \vee B.$$

Bemerkung 6.6.

⚠ Vorsicht: das **mathematische oder** ist nicht dasselbe wie das sich gegenseitig ausschließende **entweder oder** (auch **exklusiv oder** genannt).

Umgangssprachlich wird leider oft auf das „entweder“ verzichtet. Fragen Sie also nie Mathematiker:innen eine oder-Frage wenn etwas ausgewählt werden soll.

Frage: „Mögen Sie Mayo oder Ketchup?“
Antwort: „Ja!“(Gemeint ist die Bestätigung, dass die Aussage der Frage wahr ist.)

Damit weiß man nicht wirklich weiter. Es kann sein, dass Mayo bevorzugt wird, oder Ketchup, oder sogar beides!

Am einfachsten erklärt man eine logische Operation durch eine **Wahrheitstafel** wie in Abbildung 1.

A	B	$\neg A$	A und B	A oder B	(A und $\neg B$) oder ($\neg A$ und B)
W	W	F	W	W	F
W	F	F	F	W	W
F	W	W	F	W	W
F	F	W	F	F	F

Abbildung 1. Wahrheitstafel für Negation, *und* und *oder*, sowie *entweder oder*

Bemerkung 6.7. Für die Logik von und/oder/nicht gelten die folgenden hoffentlich intuitiv klaren Regeln:

(1) Doppelte Verneinung:

$$\neg\neg A \quad \text{hat gleichen Wahrheitsgehalt wie} \quad A.$$

Ein Beispiel: „Anna hat die Klausur nicht nicht bestanden“ bedeutet dasselbe wie „ Anna hat die Klausur bestanden“.

(2) Verneinung von und: „nicht beides“

$$\neg(A \text{ und } B) \quad \text{hat gleichen Wahrheitsgehalt wie} \quad \neg A \text{ oder } \neg B.$$

Ein Beispiel: „Es ist nicht so, dass die Mannschaft viel gelaufen ist und super gekämpft hat“ bedeutet dasselbe wie „Die Mannschaft ist nicht viel gelaufen oder die Mannschaft hat nicht super gekämpft“.

(3) Verneinung von oder: „weder noch“

$$\neg(A \text{ oder } B) \quad \text{hat gleichen Wahrheitsgehalt wie} \quad \neg A \text{ und } \neg B.$$

Ein Beispiel: „Es ist nicht so, dass wir alles versucht haben oder wir einfach Glück gehabt haben“ bedeutet dasselbe wie „Wir haben nicht alles versucht und wir hatten dazu auch kein Glück“.

(4) Ausklammern I:

$$A \text{ und } (B \text{ oder } C) \quad \text{hat gleichen Wahrheitsgehalt wie} \quad (A \text{ und } B) \text{ oder } (A \text{ und } C).$$

Ein Beispiel: „Morgen scheint die Sonne und ich gehe ins Schwimmbad oder ans Meer“ bedeutet dasselbe wie „Morgen scheint die Sonne und ich gehe ins Schwimmbad, oder morgen scheint die Sonne und ich gehe ans Meer “.

(5) Ausklammern II:

$$A \text{ oder } (B \text{ und } C) \quad \text{hat gleichen Wahrheitsgehalt wie} \quad (A \text{ oder } B) \text{ und } (A \text{ oder } C).$$

Ein Beispiel: „Der Hund hat Flöhe oder die Katze hat Läuse und Zecken“ bedeutet dasselbe wie „Der Hund hat Flöhe oder die Katze hat Läuse, und der Hund hat Flöhe oder die Katze hat Zecken“.

Bessere Vorschläge für die Beispiele werden gerne entgegen genommen.

Formale Beweise für logisch gleichwertige Ausdrücke von Aussagen bekommt man durch Anlegen einer Wahrheitstafel. Ein Beispiel liefert Abbildung 2.

A	B	$\neg(A \text{ und } B)$	$(\neg A) \text{ oder } (\neg B)$	$\neg(A \text{ oder } B)$	$(\neg A) \text{ und } (\neg B)$
W	W	F	F	F	F
W	F	W	W	F	F
F	W	W	W	F	F
F	F	W	W	W	W

Abbildung 2. Wahrheitstafel für De Morgan’sche Regeln

6.4. **Implikationen, logisches Argumentieren.** Auch das mathematische Argumentieren mit Aussagen läßt sich formalisieren. Dazu muß man festlegen, wann eine Argumentation, also eine Beweisführung, aus einer Voraussetzung eine Behauptung ableitet.

Definition 6.8. Sei V eine Aussage, genannt Voraussetzung, und B eine Aussage, genannt Behauptung. Die **Implikation**

$$V \Longrightarrow B,$$

ist die Aussage, dass von der Wahrheit der Aussage V auf die Wahrheit der Aussage B geschlossen werden kann.

⚠ Für den Wahrheitswert von $V \Longrightarrow B$ muß man die Implikation als ein **Versprechen** begreifen. Das Aussage $V \Longrightarrow B$ ist wahr, wenn das Versprechen gehalten wird, und sie ist falsch, wenn das Versprechen gebrochen wird.

Es ergeben sich die folgenden Wahrheitswerte in Tabelle 3 (oft als per Definition gültig angegeben).

V	B	$V \implies B$	$\neg V$ oder B
W	W	W	W
W	F	F	F
F	W	W	W
F	F	W	W

ABBILDUNG 3. Wahrheitstafel für Implikation und alternative logische Formulierung

Wir gehen die Zeilen der Tabelle 3 der Reihe nach durch.

(1) Aus einer wahren Aussage V folgt eine wahre Aussage B: hier haben wir unser Versprechen gehalten, somit ist $V \implies B$ hier wahr.
(2) Aus einer wahren Aussage V folgt eine falsche Aussage B: hier haben wir unser Versprechen gebrochen, somit ist $V \implies B$ hier falsch.
(3) Aus einer falschen Aussage V folgt eine wahre oder eine falsche Aussage B. Da die Voraussetzung falsch ist, haben wir gar nichts versprochen, also ist es auch egal of B wahr oder falsch ist: das Versprechen ist gehalten worden, somit ist $V \implies B$ hier wahr.

Zum Thema der Wahrheitswerte von Implikationen verweise ich auch auf [SchSt18] Kapitel 3.2.2. Wenn Sie sich mit dem Konzept unwohl fühlen, lesen Sie darüber in unterschiedlichen Quellen nach.

Beispiel 6.9. Die Aussage

$$\text{Für alle ganzen Zahlen } a \text{ und } b \text{ gilt: } (a = b) \quad \implies \quad (a^2 = b^2)$$

ist sicherlich richtig, d.h. wahr. Wenn sie für alle ganzen Zahlen wahr ist, bleibt sie sicherlichh auch wahr, wenn wir spezielle a und b wählen. Sei also $a = -5$ und $b = 5$. Dann erhalten wir die richtige Aussage

$$(-5 = 5) \quad \implies \quad ((-5)^2 = 5^2).$$

Hier wird aus einer falschen Aussage eine wahre Aussage gefolgert.
Spezialisieren wir obige Aussage mit $a = 3$ und $b = 5$ zu

$$(3 = 5) \quad \implies \quad (3^2 = 5^2).$$

Dann ist die Implikation immer noch korrekt, auch wenn sowohl die Voraussetzung als auch die Behauptung falsch sind.

Proposition 6.10. *Seien A und B zwei Aussagen. Dann ist die Implikation $A \implies B$ gleichwertig mit ($\neg A$ oder B).*

Beweis. Das folgt sofort aus der Tabelle 3. □

Bemerkung 6.11. Sprachlich kann man $A \implies B$ auf vielfältige Weise lesen:

- wenn A, so B,
- aus A folgt B,
- A impliziert B,
- B ist notwendige Bedingung für A,
- A ist hinreichende Bedingung für B,
- B gilt dann, wenn A gilt.

Bemerkung 6.12. Aus falschen Aussagen kann man alles folgern. Wenn V falsch ist, dann ist $V \implies B$ wahr und aus V folgt B, egal of B wahr ist, oder nicht. Das ist kein Problem, denn weil V nicht wahr ist, und daher das Versprechen $V \implies B$, nicht eingelöst werden kann.

6.4.1. *Äquivalenz.*

Definition 6.13. Unter der **Äquivalenz** von Aussagen A und B verstehen wir

$$(A \Longrightarrow B) \quad \text{und} \quad (B \Longrightarrow A).$$

Als Notation wird $A \iff B$ verwendet. Sprachlich formuliert man $A \iff B$ als

- A ist äquivalent zu B,
- A gilt dann und nur dann, wenn B gilt,
- A gilt genau dann, wenn B gilt.

A	B	$A \Longrightarrow B$	$B \Longrightarrow A$	$A \iff B$
W	W	W	W	W
W	F	F	W	F
F	W	W	F	F
F	F	W	W	W

Abbildung 4. Wahrheitstafel für Implikation und Äquivalenz

Bemerkung 6.14. Das Symbol $A \iff B$ darf nur genau dann verwendet werden, wenn die Aussagen A und B den gleichen Wahrheitswert haben: beide wahr oder beide falsch.

6.5. **Quantoren.** In der mathematischen Sprache möchte man gerne quantifizierende Aussagen treffen. Davon gibt es zwei Typen.

6.5.1. *Allaussagen.* Alle Dinge einer bestimmten Sorte (Elemente einer Menge!) haben die Eigenschaft „blup“. Dies kann man mit dem **Allquantor** symbolisch schreiben. Der Allquantor hat das Symbol $\forall$, gelesen „für alle“. Hier ist ein Beispiel:

$$\forall\ x \text{ gerade Zahl} : x^2 \text{ ist gerade.}$$

Der : ist als „gilt, dass “ zu lesen. Mit der Menge der geraden Zahlen G geht das noch knapper als $\forall x \in G : x^2 \in G$.

⚠ Die Bedeutung von $\forall$ ist wirklich alle ohne Ausnahme, nicht einmal die kleinste.

Weil es sich im Text besser liest, wenn die Sprache nicht zu symbollastig wird, verwenden wir oft die ausgesprochene Bedeutung von $\forall$:

Für alle geraden Zahlen x gilt, dass x^2 eine gerade Zahl ist.

Sieht einfach besser aus und das verständige Lesen ist einfacher.

6.5.2. *Existenzaussagen.* Es gibt ein Ding mit einer bestimmten Eigenschaft (ein Element einer Menge!). Dies kann man symbolisch mit dem **Existenzquantor** $\exists$ schreiben, den man „es existiert ein/e“ lesen soll (oder auch salop „es gibt“). Hier ist ein Beispiel:

$$\exists\ x \in \mathbb{N}_0 : x \in G.$$

⚠ Die mathematische Bedeutung von $\exists$ ist nur die reine qualitative Existenz, nichts quantitatives. Das ein/e in „es existiert ein/e“ ist keine Anzahl sondern ein unbestimmter Artikel. Die umgangsprachliche Bedeutung ist *mindestens ein/e.*

In ausgesprochener Bedeutung von $\exists$:

$$\text{Es existiert eine natürliche Zahl } x\text{, so dass } x \text{ gerade ist.}$$

Wenn man etwas verwandtes ausdrücken mag, dann gibt es an $\exists$ angelehnte Symbole. So bedeutet $\exists^{\leq 1}$ nämlich „es existiert höchstens ein/e "(und das kann auch bedeuten, dass gar nichts existiert!). Und wenn man die Eindeutigkeit des existierenden Dings ausdrücken möchte, dann geht das mit dem Symbol $\exists!$, was man „es existiert genau ein/e" liest.

Bemerkung 6.15. Grammatikregel: Bei beiden Quantoren ist es wichtig, dass nach dem Quantor eine bisher unbenutzte Variable genannt wird, die ein Ding einer bestimmten Sorte sein soll (ein Element einer Menge!), von dem dann bestimmte Eigenschaften gefordert werden. Und zwar entweder alle diese Dinge bei $\forall$, oder wenigstens eins bei $\exists$.

6.5.3. *Regeln für das Verneinen von Quantoren.* Eine $\forall$-Aussage wird verneint zu einer $\exists$-Aussage:

$$\text{nicht } \Big(\forall x \text{ ein bla} : x \text{ ist ein blup}\Big)$$

entspricht

$$\exists x \text{ ein bla} : \text{ nicht } \Big(x \text{ ist ein blup}\Big)$$

oder besser

$$\exists x \text{ ein bla} : x \text{ ist kein blup.}$$

Eine (für alle)-Aussage wird falsch, sobald auch nur ein Gegenbeispiel existiert.

Eine $\exists$-Aussage wird verneint zu einer $\forall$-Aussage:

$$\text{nicht } \Big(\exists x \text{ ein bla} : x \text{ ist ein blup}\Big)$$

entspricht

$$\forall x \text{ ein bla} : \text{ nicht } \Big(x \text{ ist ein blup}\Big)$$

oder besser

$$\forall x \text{ ein bla} : x \text{ ist kein blup.}$$

Eine (es gibt)-Aussage wird falsch, wenn man absolut kein Beispiel finden kann, weil alle Dinge ein Gegenbeispiel sind.

Bemerkung 6.16. Etwas formaler aufgeschrieben sieht das so aus. Sei M eine Menge und sei $A(x)$ ein Ausdruck, der bei Wahl eines Elements $x \in M$ zu einer Aussage wird. Dann gelten die folgenden Regeln:

$$\begin{aligned} \neg\forall x \in M : A(x) \quad &\text{hat den gleichen Wahrheitsgehalt wie} \quad \exists x \in M : \neg A(x), \\ \neg\exists x \in M : A(x) \quad &\text{hat den gleichen Wahrheitsgehalt wie} \quad \forall x \in M : \neg A(x). \end{aligned}$$

6.5.4. *Auf die Reihenfolge kommt es an.* Es sind typischerweise völlig verschieden:

$$\forall x \in A\ \exists y \in B : \ldots \quad \neq \quad \exists y \in B\ \forall x \in A : \ldots.$$

Beispiel 6.17. Es ist sicherlich nicht dassselbe zu behaupten

„Für alle Tage x gibt es ein Paar Socken S: an Tag x ziehe ich das Paar S an."

wie zu sagen

„Es gibt ein Paar Socken S für das an allen Tagen x gilt: an Tag x ziehe ich das Paar S an."

6.6. **Märchenstunde: Paradoxien und Unvollständigkeit.** Eine Paradoxie ist eine in sich widersprüchliche Aussage. Auf den ersten Bilck sollte sie wahr oder falsch sein, aber beide Varianten führen zu einem logischen Problem.

6.6.1. *Das Epimenidis Paradoxon.*

Epidemides der Kreter sagt: „alle Kreter sind Lügner.“

besser:

Ein Mensch sagt: „ich lüge gerade.“

6.6.2. *Der Barbier von Sevilla.*

Der Barbier von Sevilla rasiert alle, die sich nicht selbst rasieren. Frage: wer rasiert den Barbier von Sevilla?

Allen diesen Paradoxien ist eigen, dass sie die syntaktische gegen die semantische Ebene ausspielen. Die Aussage spricht über sich selbst auf einer formalen (syntaktischen) Ebene als auch in ihrer Interpretation (semantisceh Ebene).

6.7. **Märchenstunde: Proof checker.** Erwähnt werden soll auch, dass man mittlerweile Computern beigebracht hat, Mathematik in formaler Sprache nachzubauen. Der Beweisassitent Lean hat sogar auf spektakuläre Art und Weise durch den Einsatz einer ganzen Gruppe von Mathematiker:innen ein schwieriges Theorem aus der aktuellen Forschung über *condensed mathematics* verifiziert. Nachlesen kann man das, wie auch andere spannende Geschichten über Mathematik, im gut recherchierten und aufbereiteten Quanta Magazine.

Take home message Kapitel §6.

- Eine mathematische Aussage ist entweder wahr oder falsch.
- Das mathematische oder ist NICHT daselbe wie das entweder oder.
- Die Implikation $A \Longrightarrow B$ ist nur dann falsch, wenn das Versprechen nicht eingelöst wird: das ist der Fall A wahr und B trotzdem falsch.
- Mit Wahrheitstafeln kann man logische Ausdrücke vergleichen.
- Syntax und Semantik zu vermischen, kann zu Paradoxien führen.
- Quanta Magazine

7. Mathematische Beweise

Quellen: [SchSt18] Kapitel 2.1, 2.4 und 3.3

7.1. **Die subjektive Hierarchie der Sätze.** Mathematische Sätze werden typischerweise durch eine Art Titelstichwort eingeleitet, wodurch eine subjektive Wichtigkeit vermittelt werden soll. Das gliedert den Text und setzt Betonungen. Die Reihenfolge der subjektiven Wichtigkeit ist die folgende:

$$\text{Theorem} > \text{Satz} > \text{Proposition} > \text{Lemma} > \text{Hilfslemma}\,.$$

Ob eine Aussage ein Satz oder eine Proposition oder whatever ist, hat keinen Einfluß auf die erwartete Strenge an den Beweis oder die Gültigkeit der Aussage. Die genaue Einordnung ist subjektiv und verhandelbar; also nicht so wichtig.

Dann gibt es noch das Korollar, quasi ein Abstaubertor. Bei einem Korollar handelt es sich um eine recht unmittelbare aber bemerkenswerte Konsequenz einer eben bewiesenen Aussage, oder sogar aus dem eben geführten Beweis.

7.2. **Beweistypen.** Mathematische Lehrsätzen haben im Wesentlichen die folgende Form:

Satz 7.1 (manchmal hat ein Satz einen Namen, oder eine Person ist mit dem Satz verbunden)**.**

(V) Liste von Voraussetzungen: Dinge und ihre angenommenen Eigenschaften.

$$\Longrightarrow$$

(B) Die behauptete Aussage.

Der Satz macht also das Versprechen $V \Longrightarrow B$, und das verlangt dann einen Beweis. Beweise nutzen Aussagenlogik, um aus bekannten Aussagen neue Aussagen abzuleiten. Elementaren Umformulierungen von $V \Longrightarrow B$ lassen sich mittels einer Wahrheitstafel leicht beschreiben. Diese führen zu verschiedenen Beweisansätzen.

V	B	$V \Longrightarrow B$	$\neg V$ oder B	$\neg B \Longrightarrow \neg V$	$\neg(V$ und $\neg B)$
W	W	W	W	W	W
W	F	F	F	F	F
F	W	W	W	W	W
F	F	W	W	W	W

Abbildung 5. Wahrheitstafel für Implikation und Umformulierungen

Die logische Äquivalenz der Wahrheitstafel in Tabelle 5 ablesbaren Aussagen, sollte man nicht nur formal sondern unbedingt intuitiv verinnerlichen. Diese Perspektivwechsel (in alle Richtungen!) sind wesentlicher Bestandteil mathematischen Denkens und Formulierens.

$V \Longrightarrow B$:	wenn V wahr ist, ... (Begründung) ... ist auch B wahr.
$\neg B \Longrightarrow \neg V$:	wenn B falsch ist, ... (Begründung) ... ist auch V falsch.
$\neg V \vee B$:	(Begründung) ..., also ist B wahr oder V falsch.
$\neg(V \wedge \neg B)$:	Angenommen V ist wahr und B ist falsch, dann ... (Begründung) ...
	... finden wir einen Widerspruch! Also ist
	nicht gleichzeitig V wahr und B falsch.

Jede dieser Umformulierungen ist Grundlage eines Beweisansatzes.

Bemerkung 7.2. Die logische Äquivalenz von $\neg V \vee B$ mit $V \Longrightarrow B$ benutzen wir nicht. Die nutzt man vermutlich besser in der Form, dass man $A \vee B$ zeigen soll und stattdessen $\neg A \Longrightarrow B$ oder symmetrisch dazu $\neg B \Longrightarrow A$ zeigt.

7.2.1. *Direkter Beweis.*

⚠ Ein **direkter Beweis** argumentiert vorwärts. Ausgehend von einer wahren Aussage A, der Voraussetzung, und einem wahren Beweis $A \Longrightarrow B$ wird auf die Wahrheit von B geschlossen:

wenn A und $(A \Longrightarrow B)$ wahr sind, dann ist auch B wahr.

Umgangssprachlich: die Voraussetzung A trifft zu, die Argumentation $A \Longrightarrow B$ ist nicht fehlerhaft, also gilt B. Wir schauen uns ein Beispiel an.

Proposition 7.3. *Sei a eine Ziffer mit $a \geq 3$. Dann ist $a \cdot (a+1)$ zweistellig, also $a \cdot (a+1) = (c,d)_{10}$. Dann gilt*

$$\big((a5)_{10}\big)^2 = (cd25)_{10}.$$

Beweis. Aus $3 \leq a \leq 9$ folgt

$$12 = 3 \cdot 4 \leq a(a+1) \leq 9 \cdot 10 = 90.$$

Also ist $a(a+1)$ in der Tat zweistellig.

Die Ziffern c und d erfüllen $a(a+1) = 10c + d$, und $(a5)_{10} = 10a + 5$. Damit gilt

$$\begin{aligned}\big((a5)_{10}\big)^2 &= (10a+5)^2 = 100a^2 + 100a + 25 = 100 \cdot a(a+1) + 25 \\ &= 100 \cdot (10c + d) + 25 = 1000c + 100d + 2 \cdot 10 + 5 = (cd25)_{10}.\end{aligned}$$

□

7.2.2. *Indirekter Beweis.*

⚠ Der **indirekte Beweis** argumentiert gewissermaßen verneinend rückwärts. Wir nutzen aus, dass laut Tabelle 5 gilt

„$A \Longrightarrow B$“ genau dann wenn „$\neg B \Longrightarrow \neg A$“.

Die Implikation $\neg B \Longrightarrow \neg A$ nennt man die **Kontraposition** zu $A \Longrightarrow B$. Das Standardbeispiel hier ist die Gleichwertigkeit von

(a) Wenn es regnet (A) wird die Straße naß (B).
(b) Wenn die Straße trocken ist $(\neg B)$, dann hat es nicht geregnet $(\neg A)$.

Es folgt ein mathematisches Beispiel.

Proposition 7.4. *Seien x, y natürliche Zahlen und $xy \neq 0$. Dann gilt $x \neq 0$ und $y \neq 0$.*

Beweis. Anstelle von $A \implies B$ mit $A =$ „$xy \neq 0$“ und $B =$ „$x \neq 0$ und $y \neq 0$“ zeigen wir die Kontraposition $\neg B \implies \neg A$. Zu zeigen ist also

$$(x = 0 \text{ oder } y = 0) \implies (xy = 0),$$

und das ist trivial, weil multiplizieren mit 0 immer den Wert 0 ergibt, siehe Bemerkung 5.4. □

Bemerkung 7.5. Analysieren wir den Beweis von Proposition 7.4. Warum benutzen wir einen indirekten Beweis? Wenn man etwas beweisen will, dann muss man Aussagen in die Hand bekommen, mit denen man weiter argumentieren kann. Ein direkter Beweis von Proposition 7.4 startete mit der Aussage A: das Produkt xy ist von 0 verschieden. Damit läßt sich weniger anfangen (was ist xy denn dann?) als mit dem Start des indirekten Beweis, der Negation von B: mindestens einer der beiden Werte x und y ist 0. Das ist konkret und damit läßt sich arbeiten.

Diese Bemerkung ist mehr Intuition als feste Regel. Nichtsdestotrotz vermittelt sie einen Eindruck davon, was man gewinnen könnte, wenn man einen Beweis indirekt anzugehen versucht, wenn man direkt nicht weiter kommt.

7.2.3. *Widerspruchsbeweis.* Der **Beweis durch Widerspruch** ist eine Stärke der Mathematik, um die uns die anderen Wissenschaften beneiden. Das funktioniert nur, weil wir an die **Widerspruchsfreiheit** der Mathematik glauben (mehr dazu in der Märchenstunde zu Gödel in Kapitel §7.4). Hierbei geht es zunächst um Lehrsätze der folgenden Form.

Satz 7.6 (manchmal hat ein Satz einen Namen, oder eine Person ist mit dem Satz verbunden)**.**

Die Aussage (A) ist wahr.

Der Beweis durch Widerspruch nimmt das Gegenteil als wahr an: „Angenommen $\neg A$ ist wahr …“, und schaut, was daraus folgt. Wenn es gelingt, eine Aussage B zu folgern

$$\neg A \implies B,$$

⚠ von der wir wissen, dass B falsch ist, dann haben wir gewonnen. Die Widerspruchsfreiheit der Mathematik duldet das nicht, also muß $\neg A$ falsch sein. Wäre nämlich $\neg A$ wahr, dann würde das bewiesene Versprechen $\neg A \implies B$ die Wahrheit von B nach sich ziehen. Gleichzeitig wahr und falsch kann B nicht sein (das ist die Widerspruchsfreiheit). Somit muss $\neg A$ falsch sein, und damit $A = \neg(\neg A)$ wahr.

Alternativ kann man so argumentieren. Der Beweis $\neg A \implies B$ ist korrekt (wahr), also auch die Kontraposition $\neg B \implies A$. Nun ist B falsch, also $\neg B$ wahr, und damit wegen der korrekten Implikation $\neg B \implies A$ auch A wahr.

Bemerkung 7.7. Der Methode des Widerspruchsbeweises wohnt eine **besondere Fehleranfälligkeit** inne. Ein Fehler in einem direkten Beweis führt vom Weg ab und typischerweise nicht zu dem angestrebten Resultat. Man merkt sofort, dass der Beweis falsch ist. Bei einem Widerspruchsbeweis führt ein Fehler in der Regel zu einer falschen Aussage. Aber das ist genau das gewünschte Ergebnis! Und schon hat man sich vertan.

Hier ist das mit Recht berühmteste Beispiel eines Widerspruchsbeweises.

Theorem 7.8 (Euklid, Elemente, Buch IX Proposition 20, ca. 300 BC)**.**
Es gibt unendlich viele Primzahlen.

Beweis. Schritt 1: **Angenommen, die Behauptung ist falsch**: es gäbe nur endlich viele Primzahlen. Die Anzahl dieser Primzahlen sei die (unbekannte) natürliche Zahl n. Dann kann man diese auf eine endliche Liste schreiben, sagen wir $p_1, p_2, \ldots, p_n$ sei die Liste[3] aller Primzahlen. Weil $p = 2$ eine Primzahl ist, ist diese Liste nicht leer ($n \geq 1$).

[3]Konkret $p_1 = 2$, $p_2 = 3$, unsw. — die konkreten Zahlen tun nichts zur Sache und blähen den Beweis nur auf.

Schritt 2: Wir betrachten nun die natürliche Zahl $N = P + 1$, wobei P für das Produkt

$$P = p_1 \cdot p_2 \cdot \ldots \cdot p_n$$

steht. Dieses N ist eine natürliche Zahl $N \geq 2$, weil P mindestens 1 ist. Daher hat N einen Primteiler[4]. Einen solchen Primteiler von N wählen wir aus und nennen ihn ℓ.

Schritt 3: Weil unsere Liste der Primzahlen vollständig ist, kommt ℓ in der Liste vor und somit im Produkt P: es teilt ℓ das Produkt P. Daher läßt N bei Division durch ℓ den Rest 1, denn die Division von P durch ℓ geht auf und $N = P + 1$.

Schritt 4: Das ist der gesuchte Widerspruch, denn ℓ kann nicht gleichzeitig ein Primteiler von N sein und N bei Division durch ℓ den Rest 1 lassen. □

Bemerkung 7.9. In der Wochenzeitung *Die ZEIT* wurde einmal der Frage nachgegangen, was denn zum Kanon des Allgemeinwissens in den verschiedenen wissenschaftlichen Disziplinen gehören soll. Der vielfach ausgezeichnete Journalist Gero von Randow, der den Abschnitt über die Mathematik vertrat, hat daraufhin einzig und allein den Beweis Euklids über die unendlich vielen Primzahlen abgedruckt.

Dieser Beweis von Theorem 7.8 ist gleichermaßen alt (ca. 2300 Jahre), wie unverrückbar wahr, und von einer Eleganz und Tiefe über ein fundamentales abstraktes mathematisches Konzept, dem Konzept der Primzahl, das gerade in der heutigen digitalen Zeit (Kryptographie) und der mathematischen aktuellen Forschung (p-adische Geometrien) von unfaßbarer Relevanz ist.

Angehende Lehrende der Mathematik, egal auf welcher Ebene, müssen diesen Beweis gründlich verstanden haben, denn er gehört zum Kanon des Allgemeinwissens.

7.2.4. *Widerspruchsbeweis einer Implikation.* Man kann einen Satz der Form $V \Longrightarrow B$ mittels Widerspruchsbeweis zeigen. Und zwar nehmen wir dazu an, dass $V \Longrightarrow B$ falsch ist. Dann ist die Negation wahr, und das ist nach Tabelle 5 gerade

$$\neg(V \Longrightarrow B) \text{ gdw. } (V \text{ und } \neg B).$$

Man darf also sowohl V als auch $\neg B$ annehmen, womit man mehr zum Argumentieren in der Hand hat, als nur die reine Voraussetzung V. Dann legt man los und findet hoffentlich einen Widerspruch. Das bedeutet nämlich, dass $(V$ und $\neg B)$ falsch ist und deshalb die Negation davon, also $V \Longrightarrow B$, wahr sein muss. Dazu ein Beispiel, das wir schon kennen.

Proposition 7.10. *Sei a eine natürliche Zahl. Dann ist $N = 2a + 1$ ungerade.*

Beweis. Was ist hier Voraussetzung, und was Behauptung? Das ist nicht so leicht zu sehen. Sicherlich ist „Sei a eine natürliche Zahl“ Voraussetzung. Und sicher ist „ist ungerade“ Behauptung. Aber man muß genauer lesen:

(V) Die natürliche Zahl N hat die Form $2a + 1$, wobei a natürliche Zahl ist.
(B) Die Zahl N ist ungerade.

Ungerade ist die Negation von gerade. Wir können also so vorgehen, dass wir annehmen, die Zahl N sei gerade $(\neg B)$, und daraus zusammen mit (V) einen Widerspruch ableiten. Per Definition bedeutet N gerade, dass es eine natürliche Zahl b gibt mit $N = 2b$. Jetzt haben wir zwei Gleichungen, mit denen wir arbeiten können:

$$N = 2a + 1, \qquad (V)$$
$$N = 2b. \qquad (\neg B)$$

Daraus folgt $2b = 2a + 1$ und nach Umstellen und Ausklammern

$$1 = 2(b - a).$$

[4]Das muß man auch noch beweisen! Wird in Proposition 12.15 nachgeholt.

Das bedeutet, dass 1 eine gerade Zahl ist. Die 1 hat aber als Einerziffer die 1, was dem Einerziffernkriterium aus Satz 4.3 für gerade/ungerade widerspricht. Wir haben also den gesuchten Widerspruch gefunden. Damit ist alles bewiesen. □

7.3. **Beweisstrategien.** Strategien zum Beweisen gibt es viele. Wir besprechen hier einmal nur eine. Einige Beweistricks sind in [SchSt18] Kapitel 3.3.9 aufgeschrieben.

7.3.1. *Rückwärtsarbeiten.*

⚠ Das Rückwärtsarbeiten ist eine Beweistechnik, die bei der Behauptung anfängt, und man sich fragt, was der letzte Beweisschritt sein könnte.

Ziel dabei ist es, eine einfachere Aussage zu finden, die die Behauptung impliziert und die man nun als neue Behauptung ansehen kann. Wenn man die neue Behauptung zeigen kann, dann ist man fertig, denn diese impliziert ja die gewünschte Behauptung. Und das wiederholt man einige Male.

Als Beispiel schauen wir uns die Ungleichung zwischen arithmetischem Mittel und geometrischem Mittel an.

Proposition 7.11. *Seien a, b positive Zahlen. Dann gilt*

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Beweis. Wir fangen beim Beweis bei der Behauptung an.

$$\frac{a+b}{2} \geq \sqrt{ab} \tag{7.1}$$
$$\implies \quad \Big(\frac{a+b}{2}\Big)^2 \geq \big(\sqrt{ab}\big)^2 \tag{7.2}$$
$$\implies \quad \frac{a^2+2ab+b^2}{4} \geq ab \tag{7.3}$$
$$\implies \quad a^2+2ab+b^2 \geq 4ab \tag{7.4}$$
$$\implies \quad a^2-2ab+b^2 \geq 0 \tag{7.5}$$
$$\implies \quad (a-b)^2 \geq 0 \tag{7.6}$$

Hierbei folgt von oben nach unten jeweils die nächste Zeile aus der vorherigen. Am Schluß steht eine wahre Aussage, denn Quadrate sind stets nichtnegativ.

Aber das beweist gar nichts! Wir haben nicht $V \implies B$ gezeigt, sondern $B \implies$ wahre Aussage. Um daraus einen Beweis zu machen, nutzen wir die Rechnung, die zielgeleitet war vom Bestreben, die Terme sukzessive zu Vereinfachen, und drehen diese um, so dass wir aus einer wahren Aussage unsere Behauptung zeigen. Das geht aber NICHT automatisch, denn $A \implies B$ hat in der Regel nichts mit $B \implies A$ zu tun. Hier waren alle Schritte zufälligerweise Äquivalenzumformungen, so dass diese Strategie klappt.

$$(a-b)^2 \geq 0 \tag{7.7}$$
$$\implies \quad a^2-2ab+b^2 \geq 0 \tag{7.8}$$
$$\implies \quad a^2+2ab+b^2 \geq 4ab \tag{7.9}$$
$$\implies \quad \frac{a^2+2ab+b^2}{4} \geq ab \tag{7.10}$$
$$\implies \quad \Big(\frac{a+b}{2}\Big)^2 \geq ab \tag{7.11}$$
$$\implies \quad \frac{a+b}{2} \geq \sqrt{ab}. \tag{7.12}$$

Hierbei ist nur der letzte Schritt problematisch. In diesem wird das Quadrieren rückgängig gemacht. Das geht nur, weil wir hier mit positiven Zahlen zu tun haben. Daher kommt die Voraussetzung! Ein gut aufgeschriebener Beweis betont diese Stelle und erklärt, warum man schließen darf. □

Man beachte auch das Thema Gleichungsumformungen in Beweisen [SchSt18] Kapitel 2.4.

7.3.2. *Wie schreibt man einen Beweis auf?* Was macht einen korrekten Beweis aus? Welche Funktion erfüllt ein aufgeschriebener Beweis?

- Man überzeugt sich selbst, dass eine mathematische Aussage richtig ist. Dazu muss man beim Aufschreiben alle (kleinsten) Details prüfen.
- Man kommuniziert den Beweis nachvollziehbar an jemanden anderen. Am besten immer nur ein Argument pro Satz. Ganze Sätze schreiben, und den richtigen Grad an Detailtiefe verwenden. Einzelne Schritte begründen! Nicht nur sagen, dass eine Folgerung gilt, sondern auch warum.
- Ein gut aufgeschriebener Beweis vermittelt auch die Intuition, warum die behauptete Aussage stimmt. Der Beweis ist dann nicht nur korrekt, sondern auch erklärend.

Das gelingt nur durch Üben und Studieren von bereits aufgeschriebenen Beweisen.

7.4. **Märchenstunde: Gödel und die Unvollständigkeit der Mathematik.** In exakter Forschungsmathematik wird alles aus Axiomen gefolgert (Euklid, David Hilbert). Zur Überraschung der Mathematik gibt es Grenzen dieser Methode.

Auftritt Kurt Gödel (28.04.1906 – 14.01.1978). Einer der bedeutensten Logiker des zwanzigsten Jahrhunderts. Ein Freund von Einstein am IAS in Princeton. Leider war Gödel psychisch krank, litt an Depression und hypochondrischen Zwangsvorstellungen: er hat sich im wahrsten Sinne des Wortes zu Tode gehungert aus Angst davor, vergiftet zu werden.

Gödel bewies mittels einer Zahlenvariante der selbstbezüglichen Paradoxien aus Kaitel §6.6 bahnbrechende Sätze in der Logik. Der erste Unvollständigkeitssatz besagt, dass es in hinreichend reichhaltigen mathematischen wiederspruchsfreien Theorien stets Aussagen A gibt, für die weder A noch ihr Gegenteil $\neg A$ beweisbare sind. Der zweite Unvollständigkeitssatz besagt, dass eine hinreichend reichhaltige mathematische Theorie ihre eigene Wiederspruchsfreiheit nicht beweisen kann.

In beiden Sätzen bedeutet *hinreichend reichhaltig* erstaunlich wenig, nämlich dass man in den Theorien über die natürlichen Zahlen und ihre Arithmetik sprechen kann. Die Strategie des Beweises für den ersten Unvollständigkeitssatz ist die folgende. Jeder mathematische Satz in der Theorie bekommt eine natürliche Zahl zugewiesen, eine **Gödelisierung**. Und dann zeigt man, dass es einen Satz der Form

„Der Satz mit der Nummer n hat keinen Beweis“

gibt, der äquivalent ist zum Satz mit Nummer n. Nennen wir die Aussage dieses Satzes mit der Nummer n einmal A. Dann ist

$$A \iff \text{„}A \text{ hat keinen Beweis“}.$$

Wenn A wahr ist, dann kann man es nicht beweisen. Wenn A falsch ist, dann hat A einen Beweis und ist somit wahr, Widerspruch.

Über Gödel und die Unvollständigkeit gibt es bei ARTE unter der Rubrik Mathewelten in der Mediathek einen empfehlenswerten Beitrag.

Take home message Kapitel §7.

- Direkter Beweis
- Indirekter Beweis (Kontraposition)

- Widerspruchsbeweis
- Es gibt unendlich viele Primzahlen (mit Beweis!)
- Jeder Schritt in einer Argumentationskette muß analysiert werden, ob es ein $\Longrightarrow$, ein $\Longleftarrow$ oder ein $\Longleftrightarrow$ ist. Und dann sollte man notieren und begründen, was man für die Beweislogik braucht.

8. Natürliche Zahlen und vollständige Induktion

Quellen: [GK23] Kapitel 5, [SchSt18] Kapitel 2.5 und Kapitel 6 bis vor 6.1.1.

Zur Vorbereitung [SchSt18] Kapitel 2.5 und Kapitel 6 bis vor 6.1.1. lesen

8.1. **Motivation: Was macht die natürlichen Zahlen aus?** Gibt es eine größte natürliche Zahl? Diese häufig von Kindern gestellte Frage hat eine einfache Antwort, die auf eine wichtige Eigenschaft der natürlichen Zahlen führt.

⚠ Es gibt keine größte natürliche Zahl, denn man kann zu jeder Zahl n eine 1 dazuaddieren, und bekommt mit $n+1$ die nächste noch größere Zahl.

Man nennt $n+1$ den **Nachfolger** von n. Die natürlichen Zahlen haben nun die folgenden Eigenschaften;

(PA1) Die 0 ist eine natürliche Zahl.

(PA2) Jede natürliche Zahl hat einen Nachfolger.

(PA3) Die 0 ist kein Nachfolger einer natürlichen Zahl.

(PA4) Wenn zwei natürliche Zahlen n und m den gleichen Nachfolger haben, dann gilt $n = m$.

(PA5) **Induktionsprinzip:** Wenn man einen Teil der natürlichen Zahlen betrachtet, der die 0 und mit jeder Zahl auch ihren Nachfolger beinhaltet, so handelt es sich um alle natürlichen Zahlen.

⚠ Diese Eigenschaften der natürlichen Zahlen vermittelt ein Bild einer Kette, die bei 0 startet und in die andere Richtung unendlich lang weiter geht. Dabei ist wesentlich, dass man entlang dieser Kette bei JEDER natürlichen Zahl vorbei kommt.

Bemerkung 8.1. Man kann zeigen, dass die Liste der Eigenschaften (PA1) – (PA5) die natürlichen Zahlen charakterisiert. Es handelt sich um die Peano-Axiome (siehe [SchSt18] Kapitel 6.1.1.). Im Rahmen der Mengenlehre kann man die natürlichen Zahlen auch konstruieren. Darauf verzichten wir hier. Stattdessen übersetzen wir insbesondere (PA5) in das Beweisprinzip der vollständigen Induktion.

8.2. **Das Beweisprinzip der vollständigen Induktion.** Die vollständige Induktion ist eine Option immer dann (oft!), wenn man unendlich viele Aussagen beweisen soll, die abgezählt sind: Aussagen

$$A_0, A_1, A_2, A_3, \dots, A_n, A_{n+1}, \dots$$

Und das geht so:

Dominos auf der Baustelle 1, Dominos auf der Baustelle 2.

Wir machen das nun exemplarisch an einem Beispiel.

Proposition 8.2. *Sei n eine natürliche Zahl. Die Summe ersten n ungeraden Zahlen berechnet sich als*

$$1 + 3 + 5 \dots + (2n-1) = n^2.$$

Hier haben wir offenbar mit einem Aussagentyp zu tun, für den die vollständige Induktion paßt. Die n-te Aussage ist

$$A_n: \text{ es gilt die Gleichung } 1 + 3 + 5 \dots + (2n-1) = n^2.$$

Wir wollen das mittels (PA5) beweisen. Dazu betrachten wir den Teil der natürlichen Zahlen, für den die entsprechende Aussage A_n richtig ist, sowas wie die Indizes n mit wahrem A_n. Den Satz zu beweisen, bedeutet, dass dieser Teil aus allen natürlichen Zahlen besteht. Nach (PA5) bedarf es dazu zweier Eigenschaften:

(1) Den **Induktionsanfang** (auch **Induktionsverankerung** genannt):
A_0 is wahr, denn dann gehört 0 zu dem betrachteten Teil.
(2) Den **Induktionsschritt** (auch **Induktionsschluss** genannt:
$A_n \Longrightarrow A_{n+1}$, bestehend aus
Induktionsannahme (auch **Induktionsvoraussetzung** genannt): A_n,
Induktionsbehauptung: A_{n+1}.
Damit gehört mit n auch $n+1$ zum Teil der natürlichen Zahlen, für den die Aussage wahr ist.

⚠ Der eigentliche **Induktionsbeweis** besteht aus diesen zwei Teilen, dem Beweis des Induktionsanfangs und dem Beweis des Induktionsschritts.

Beweis. Induktionsanfang: Sei $n = 0$. Die Aussage A_0 besagt, dass die Summe der ersten 0 ungeraden natürlichen Zahlen die Zahl $0^2 = 0$ ist. Nun, Wenn wir keine Zahlen aufsummieren, dann kommt in der Summe 0 raus. Paßt.

Induktionsschritt: Wir schließen von n auf $n+1$. Die Induktionsannahme (IA) ist

$$1 + 3 + 5 \ldots + (2n-1) = n^2.$$

Die Induktionsbehauptung (IB) ist dieselbe Formel, aber mit n durch $n+1$ ersetzt. Das rechnen wir nun aus.

$$\begin{aligned} 1 + 3 + 5 \ldots + (2(n+1)-1) &= 1 + 3 + 5 \ldots + (2n-1) + (2n+1) \\ &= \Big(1 + 3 + 5 \ldots + (2n-1)\Big) + (2n+1) \\ &= n^2 + (2n+1) \qquad \text{(IA)} \\ &= n^2 + 2n + 1 = (n+1)^2, \end{aligned}$$

und das ist gerade die Formel in der Behauptung A_{n+1}, also IB. □

Bemerkung 8.3.

(1) Die Aussage A_0 in Proposition 8.2 mit der leeren Summe kann Bauchweh verursachen. Haben wir eine korrekte Interpretation von A_0, so dass beim Beweis von A_1 aus A_0 im Induktionsschritt die richtige Aussage A_0 verwendet wird? Wenn die Kette der Induktion einmal reißt, dann beweist sie gar nichts mehr ab der Stelle des Kettenrisses. Zur Sicherheit beweisen wir den Schritt $A_0 \rightsquigarrow A_1$ alternativ durch direkten Beweis von A_1. Das ist die triviale Aussage $1 = 1^2$.
(2) Die Aussage von Proposition 8.2 ist besser mit der Summenschreibweise zu fassen.

$$\sum_{k=1}^{n} 2k - 1 = n^2.$$

Der Beweis des Induktionsschritts paßt dann in eine Zeile.

$$\sum_{k=1}^{n+1} 2k - 1 = (2(n+1)-1) + \sum_{k=1}^{n} 2k - 1 \overset{\text{IA}}{=} (2n+1) + n^2 = (n+1)^2.$$

(3) Proposition 8.2 hat einen einfachen geometrischen Beweis.

8.3. **Algebraische Beispiele.** Der Lehrer von Carl-Friedrich Gauß soll einmal versucht haben, die Klasse mit einer rechenaufwendigen Aufgabe ruhig zu Stellen. Die Kinder sollten die Summe der Zahlen von 1 bis 100 bestimmen. Nun, Gauß war bereits als Schüler ein Genie und entwickelte sich zu einem der größten Mathematiker seiner Zeit und darüber hinaus. Er kam auf die Formel der folgenden Proposition und war in kürzester Zeit fertig.

Proposition 8.4. *Sei n eine natürliche Zahl. Dann gilt*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Insbesondere ist die rechte Seite eine natürliche Zahl.

Beweis. Die per Induktion zu beweisende Aussage A_n ist gerade die Formel der Proposition.

Induktionsanfang: Hier ist A_0 die Summe der ersten 0 natürlichen Zahlen beginnende von 1. Das ist 0 und stimmt mit $0\cdot(0+1)/2$ überein. Zur Sicherheit, wegen der leeren Summe, berechnen wir auch A_1. Das ist die Behauptung $1 = 1\cdot(1+1)/2$, die auch wahr ist.

Induktionsschritt: Wir nehmen A_n an und haben A_{n+1} zu zeigen. Das geht mit der Rechnung

$$\sum_{k=1}^{n+1} k = (n+1) + \sum_{k=1}^{n} k \overset{\text{IA}}{=} (n+1) + \frac{n(n+1)}{2} = \frac{n+1}{2}\cdot(2+n) = \frac{(n+1)(n+2)}{2}. \qquad \square$$

Bemerkung 8.5. Der Beweis von Gauß ist viel eleganter. Wir berechnen die Summe zweimal, aber gegenläufig. Also

$$\begin{array}{rccccccccc} & 1 & + & 2 & + & \dots & + & (n-1) & + & n \\ + & n & + & (n-1) & + & \dots & + & 2 & + & 1 \\ \hline = & (n+1) & + & (n+1) & + & \dots & + & (n+1) & + & (n+1) \quad = (n+1)\cdot n. \end{array}$$

Hier haben wir jeweils zuerst die übereinanderliegenden Zahlen zu $n+1$ addiert. Zum Schluß teilen wir das Ergebnis durch 2. Das kann man auch geometrisch mit einer Treppenfrom veranschaulichen, die man zweimal nimmt und dann zu einem Rechteck zusammenlegt.

Bemerkung 8.6. Es ist nicht nötig, eine vollständige Induktion bei der Aussage für $n = 0$ beginnen zu lassen. Die Aussagen gelten halt dann nur ab der Zahl n_0 für die man die Induktionsverankerung A_{n_0} beweisen kann.

Proposition 8.7. *Sei $n \geq 5$ eine natürliche Zahl. Dann gilt*

$$2^n > n^2.$$

Beweis. Diesmal beweisen wir zuerst den Induktionsschritt. Die Aussage A_n ist $2^n > n^2$. Das geht so:

$$2^{n+1} = 2\cdot 2^n \overset{\text{IA}}{>} 2\cdot n^2 = (n+1)^2 + (n^2 - 2n - 1).$$

Jetzt müssen wir kurz überlegen. Wir wären fertig, wenn $n^2 - 2n - 1 \geq 0$ ist. Aber das kónnen wir schreiben als

$$n^2 - 2n - 1 = (n-1)^2 - 2 \geq 4^2 - 2 = 14,$$

weil $n \geq 5$. Moment, das ist auch schon für $n \geq 3$ richtig. Das bedeutet, unser Beweis des Induktionsschritts liefert die Kette von Implikationen

$$A_3 \Longrightarrow A_4 \Longrightarrow A_5 \Longrightarrow A_6 \Longrightarrow A_7 \Longrightarrow \dots$$

Schauen wir uns nun den Induktionsanfang an. Wir müssen A_5 nachweisen. Aus Neugierde schauen wir uns auch $A_0, \dots, A_5$ an.

n	0	1	2	3	4	5
2^n	1	2	4	8	16	32
n^2	0	1	4	9	16	25

Die Aussagen A_0 und A_1 sind sogar wahr! Aber in dem Bereich gilt unser Beweis des Induktionsschritts nicht. Wir brauchen $n \geq 3$. Und in der Tat, A_2, A_3 und A_4 sind falsch. Erst bei A_5 gilt die Aussage und der Beweis des Induktionsschritts greift. Das erklärt die Einschränkung an n in der Aussage der Proposition. $\square$

8.4. **Arithmetische Beispiele.** Jetzt beweisen wir etwas Nützliches per vollständiger Induktion.

Satz 8.8 (Division mit Rest)**.** *Seien n und d natürliche Zahlen mit $d \neq 0$. Dann existieren natürliche Zahlen q und r mit den Eigenschaften*

(i) $n = q \cdot d + r$
(ii) $0 \leq r < d$.

*Man sagt, dass n durch d mit **Rest** r geteilt wird.*
Die Zahlen q und r mit den obigen Eigenschaften sind eindeutig.

Beweis. Jetzt sind sehr viele Variablen im Spiel. Welche nehmen wir für die Induktion? Naja, irgendetwas muss man sich halt immer noch überlegen. Wir fixieren d und nennen die Aussage

$$A_n : \text{Es gibt } q \text{ und } r \text{ mit den Eigenschaften (i) und (ii) für } n \text{ und } d.$$

Die Aussagen A_n beweisen wir nun per vollständiger Induktion. Die behauptete Eindeutigkeit machen wir nachher.

Induktionsanfang: Bei $n = 0$ ist alles einfach: $q = 0$ und $r = 0$ tuen das verlangte.

Induktionsschritt: Wir nehmen nun an, dass wir bereits n mit Rest teilen können. Dann gibt es also p und s mit $n = pd + s$ und $0 \leq s < d$. Dann gilt

$$n + 1 = (pd + s) + 1 = pd + (s + 1).$$

Aus den Schranken für s ergibt sich $1 \leq s + 1 \leq d$. Jetzt gibt es zwei Fälle.

Fall 1: Es ist sogar $s + 1 < d$. Dann setzen wir $q = p$ und $r = s + 1$ und haben natürliche Zahlen mit den gewünschten Eigenschaften gefunden.

Fall 2: Es ist $s + 1 = d$. Dann müssen wir weiterrechnen:

$$n + 1 = (pd + s) + 1 = pd + (s + 1) = pd + d = (p + 1)d.$$

Hier setzen wir $q = p + 1$ und $r = 0$, und wieder sind wir fertig.

Jetzt fehlt noch die Eindeutigkeit. Angenommen es gäbe auch q', r' mit den geforderten Eigenschaften. OBdA dürfen wir (nach eventuellem vertauschen von q, r mit q', r' annehmen, dass $r \geq r'$ ist. Dann gilt

$$d > r - r' = (n - qd) - (n - q'd) = (q' - q)d,$$

und das ist dazu ≥ 0, weil ja $r \geq r'$. Die Zahl $r - r'$ ist also durch d teilbar und es gilt $0 \leq r - r' < d$. Das geht nur für die 0. Damit ist $r = r'$. Jetzt folgt aus der Rechnung auch $(q' - q)d = 0$, also $q = q'$. Damit ist alles bewiesen. □

8.5. **Varianten der vollständigen Induktion.**

Bemerkung 8.9. Oft ist es in einem Beweis des Induktionsschritts gar nicht die Aussage A_n auf die man die Aussage A_{n+1} zurückspielen kann. Man braucht hingegen irgendeine der Aussagen mit kleinerem Index. Das geht und ist einfach die folgende Variante von vollständiger Induktion. Aus den Aussagen A_n machen wir die Aussagen

$$B_n \coloneqq A_0 \text{ und } A_1 \text{ und } \ldots \text{ und } A_n.$$

Wenn wir per Induktion die Aussagen B_n zeigen, dann haben wir nichts anderes als die Aussagen A_n gezeigt. Bei $B_n \rightsquigarrow B_{n+1}$ muß man auch nur dasselbe zeigen, wie bei $A_n \rightsquigarrow A_{n+1}$, nämlich A_{n+1}. Aber man hat mehr Voraussetzungen als nur A_n, nämlich alle A_i mit $i \leq n$.

Für ein Beispiel brauchen wir ein wenig Geometrie. Wir appellieren an die geometrische Anschauung aus der Schule für den Begriff des Winkels und eines n-Ecks mit $n \geq 3$. Außerdem wollen wir als bekannt voraussetzen, dass die Winkelsumme im Dreieck 180° beträgt.

Satz 8.10 (Winkelsumme)**.** *Sei $n \geq 3$ eine natürliche Zahl. Die Summe der Innenwinkel in einem n-Eck beträgt*

$$(n-2) \cdot 180^\circ.$$

Beweis. Die Aussage für $n = 3$ ist als bekannt angenommen worden. Die Induktionsverankerung bei $n = 3$ ist damit bereits bewiesen.

Eine **Diagonale** im n-Eck ist eine Strecke zwischen zwei Ecken P, Q, die keine Seite des n-Ecks ist und auch keine Seite des n-Ecks außer in den Ecken P und Q trifft.

Beweisen wir den Induktionsschritt von n auf $n+1$. Dazu teilen wir das n-Eck in zwei kleinere ?-Ecke, indem wir entlang einer Diagonalen schneiden.

Vorsicht! Das wurde gerade so leicht dahingesagt. Zu zeigen, dass es eine solche Diagonale gibt, ist die eigentliche Schwierigkeit des Beweises. Da wir vollständige Induktion üben wollen, übergehen wir dies, aber eben nicht ohne darauf hinzuweisen, dass hier eine Argumentationsschwierigkeit liegt.

Sei das eine entstehende Teil ein a-Eck und das andere ein b-Eck. Weil wir eine Diagonale genommen haben, haben beide Teile mindestens 3 Ecken. Außerdem sind genau zwei Ecken in beiden Teilen im Einsatz. Daher gilt

$$a + b = n + 2.$$

Weil $a, b \geq 3$ folgt $a, b \leq (n+2) - 3 = n - 1$. Nach Indukttionsannahme gilt der Satz bereits für die Teile. Außerdem werden die Innenwinkel vom n-Eck auf die beiden Teile verteilt, und zwei davon in einer Summe von Winkeln aufgeteilt. Di Winkelsumme im n-Eck ist daher die Summe der Winkelsummen in den beiden Teilen. Dann gilt per Induktionsannahme die Winkelsumme

$$(a-2) \cdot 180^\circ + (b-2) \cdot 180^\circ = (a+b-4) \cdot 180^\circ = (n-2) \cdot 180^\circ. \qquad \square$$

8.6. **Gefahrenstellen bei der vollständigen Induktion.** Wir schauen uns zwei Beispiel vovn fehlerhaften Induktionsbeweisen an.

Beispiel 8.11. Das erste Beispiel ist [SchSt18] Beispiel 2.5.11. Die Behauptung ist:

> A_n: In einem Hörsaal mit n ausschließlich L2 und L5-Studierenden studieren alle Leute den gleichen Studiengang.

Hier sieht man den Induktionsindex nicht. Das soll die Anzahl n der Studierenden im Hörsaal sein.

Induktionsanfang: wir stellen uns vor, alle bis auf eine/n verlassen den Raum. Dann haben wir die Situation $n = 1$ und da ist die Behauptung sicherlich richtig.

Induktionsschritt. Angenommen, für n Studierende gilt die Behauptung, und wir wollen sie für n+1 viele beweisen. Dann bitten wir eine Person P, den Hörsaal zu verlassen. Per Induktionsannahme studieren dann die restlichen den gleichen Studiengang. Jetzt holen wir die erste Person P wieder rein und schicken eine andere Person Q raus. Jetztt sind es wieder nur n Personen und per Induktionsannahme studieren wieder alle den gleichen Studiengang. Aber dann studfiert Person P das gleiche wie die $(n-1)$-vielen Personen die nie den Raum verlassen haben und die wiederum das gleiche wie Q. Also studieren alle das gleiche.

Wo liegt der Fehler? Wir haben eine **unbegründete Existenzaussage** nicht hinterfragt. Damit das Argument stimmt, muss es eine Person geben, die gleichzeitig mit P und mit Q im Raum ist. Das ist bei $n = 2$, wenn es nur P und Q gibt, nicht gegeben.

Beispiel 8.12. Das zweite Beispiel ist [SchSt18] Beispiel 2.5.10.

> Alle Menschen sind blond.

Wir führen den Beweis per Induktion über die Anzahl der Menschen.

Induktionsanfang: Es gibt blonde Menschen. Einen solchen nehmen wir als Induktionsanfang.

Induktionsschritt: Angenommen, bei n Menschen sind alle blond. Wir zeigen das nun für $n+1$. Wenn wir die Menschen der Reihe nach aufstellen, dann sind nach Induktionsannahme die ersten n Menschen alle blond. Genauso sind aber die letzten n Menschen alle blond. Somit sind alle $n+1$ Menschenm blond.

Und wo liegt hier der Fehler? Der Induktionsanfang wurde fehlerhaft bewiesen. Die Aussage, welche per Induktion bewiesen werden soll lautet genauer:

A_n: in **jeder** Ansammlung von n Menschen sind alle Menschen blond.

Wir haben A_1 nur für günstige Ansammlungen von 1 Menschen gezeigt. Aber **nicht für jede!** Es hätte geholfen, die Aussage A_n vorher sorgfältig zu formulieren.

8.7. **Märchenstunde: Katzenvideo.** Dominos und Katzen 1, Dominos und Katzen 2.

8.8. **Märchenstunde: Geschlossene Formel für Fibonaccizahlen.** Die Fibonaccizahlen[5] sind die Folge von natürlichen Zahlen F_n, welche man rekursiv aus $F_0 = 0$, $F_1 = 1$ und

$$F_{n+1} = F_n + F_{n-1}, \qquad \text{für alle } n \geq 1$$

bekommt. Das sind also die Zahlen

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Satz 8.13. *Für alle $n \in \mathbb{N}_0$ gilt:*

$$F_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Beweis. Für $n = 0$ haben wir $\frac{1}{\sqrt{5}} \cdot (1-1) = 0$, und das ist F_0. Für $n = 1$ rechnen wir

$$\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right) \right) = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2} \right) = \frac{1}{\sqrt{5}} \cdot \frac{2\sqrt{5}}{2} = 1,$$

und das stimmt mit $F_1 = 1$ überein. Das war die Induktionsverankerung.

Weil $n = 0$ und $n = 1$ bereits erledigt sind, ist der erste Index, für den wir was beweisen müssen 2. Für den Induktionsschritt nehmen wir an, dass die Formel bis n gilt und wir zeigen sie für $n+1 \geq 2$. Insbesondere gilt die Formel für n und für $n-1$ (denn das ist immer noch eine natürliche Zahl).

Um beim Beweis des Induktionsschritts kompakt argumentieren zu können, stellen wir fest, dass

$$x = \frac{1+\sqrt{5}}{2} \quad \text{und } y = \frac{1-\sqrt{5}}{2}$$

[5] Von Ralph Caspers gibt es ein mit dem Medienpreis der DMV ausgezeichnetes Video zu Fibonaccizahlen: Kann die Natur Mathe? | Quarks: Dimension Ralph.

die beiden Nullstellen der Gleichung $X^2 = X + 1$ sind. Es gilt also $x^2 = x + 1$ und $y^2 = y + 1$. Jetzt rechnen wir

$$\begin{aligned}
\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right) &= \frac{1}{\sqrt{5}} \cdot \left(x^{n+1} - y^{n+1} \right) \\
&= \frac{1}{\sqrt{5}} \cdot \left(x^2 \cdot x^{n-1} - y^2 \cdot y^{n-1} \right) \\
&= \frac{1}{\sqrt{5}} \cdot \left((x+1) \cdot x^{n-1} - (y+1) \cdot y^{n-1} \right) \\
&= \frac{1}{\sqrt{5}} \cdot \left(x^n + x^{n-1} - y^n - y^{n-1} \right) \\
&= \frac{1}{\sqrt{5}} \cdot \left(x^n - y^n \right) + \frac{1}{\sqrt{5}} \cdot \left(x^{n-1} - y^{n-1} \right) \\
&= F_n + F_{n-1} \qquad \text{(IA)} \\
&= F_{n+1}.
\end{aligned}$$

Damit gilt die Formel auch für $n + 1$, und das beendet den Induktionsbeweis. □

Take home message Kapitel §8.

- Die natürlichen Zahlen sind entlang einer Kette aufgereiht, die bei 0 beginnt und bei der man nach und nach bei jeder natürlichen Zahl vorbeikommt.
- Vollständige Induktion als Beweismethode für unendlich viele Aussagen gleichzeitig.
- Existenz und Eindeutigkeit von Division mit Rest in den natürlichen Zahlen.

9. Naive Mengenlehre

Quellen: [GK23] Kapitel 2, [SchSt18] Kapitel 4.1

9.1. **Der Begriff der Menge.** Der für die Mathematik fundamentale Mengenbegriff geht auf Georg Cantor (3. März 1845 – 6. Januar 1918) zurück.

Fake Definition 9.1 (Pseudo-Definition von Cantor, 1895, [Can95, §1])**.** Unter einer **Menge** verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die **Elemente** von M genannt werden) zu einem Ganzen.

In unserem strengen Sinne ist dies keine Definition, denn die Begriffe *Menge* und *Element* werden aus den undefinierten Begriffen *Zusammenfassung* und *Objekt* heraus beschrieben. Die Begriffe Menge und Element sind so grundlegend, dass man sie nicht definieren kann. Sie stellen im *Schöpfungsbericht* der Mathematik das Fundament dar, auf dem der ganze Rest aufgebaut wird.

⚠ Anstelle einer Definition von Element und Menge betrachten wir lieber die Spielregeln, nach denen man mit Mengen und Elementen umgehen muß.

Und natürlich Beispiele.

9.1.1. *Mengen beschreiben durch Aufzählen.* Mengen enthalten Elemente. Genauer ist eine Menge nichts anderes als die Zusammenfassung seiner Elemente. Wir notieren das in etwa so:

$$M = \{\dots \text{Liste aller Elemente von } M \dots\}.$$

Ist 🐟 ein Element einer Menge M, so schreiben wir das

$$🐟 \in M.$$

Das Gegenteil, wenn 📦 kein Element von M ist, schreiben wir als $📦 \notin M$. Zum Beispiel: sei

$$M := \{🐟, 🎵, 🎶, ⚡, ✉, 🔊, ☎\}.$$

Dann gilt $⚡ \in M$ und $📦 \notin M$.

Definition 9.2 (Gleichheit von Mengen)**.** Zwei Mengen sind genau dann **gleich**, wenn sie die gleichen Elemente enthalten.

Sind A und B Mengen, dann ist $A = B$ per Definition genau dann, wenn für alle Dinge x gilt: $x \in A \iff x \in B$.

Beispiel 9.3.

(1) Die Menge $A = \{✉, 🔊, ☎\}$ ist verschieden von der oben definierten Menge M, denn zum Beispiel

$$🐟 \in M \quad \text{aber} \quad 🐟 \notin A.$$

Die Menge $\{✉, 🔊, ☎, ✉\}$ ist hingegen gleich A, denn durch das Mehrfachaufzählen von ✉ bekommt die Frage, welche Elemente enthalten sind, keine von der Frage für A abweichende Antwort. Und es gilt auch

$$A = \{✉, ☎, 🔊\},$$

denn die Reihenfolge der Elemente ändert nichts daran, welche Dinge Elemente sind und welche Dinge nicht.

(2) Die natürlichen Zahlen (mit 0) haben die übliche Notation

$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots\}.$$

Üblich ist auch nur $\mathbb{N}$, aber dann muß man im Kontext nachlesen, ob 0 dabei ist, oder nicht. Wir bezeichnen die positiven natürlichen Zahlen als

$$\mathbb{N}_{>0} = \{1, 2, 3, 4, 5, 6, 7, \ldots\}.$$

(3) Die ganzen Zahlen haben die übliche Notation

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

(4) Die rationalen Zahlen haben die übliche Notation $\mathbb{Q}$ und die reellen Zahlen haben die übliche Notation $\mathbb{R}$.

(5) Die **leere Menge** ist die Menge, die keine Elemente enthält. Sie ist ungefähr so wichtig wie die Zahl 0 und hat die Notationen

$$\varnothing = \{\}.$$

(6) Wir definieren ein paar Mengen. Beginnen wir mit

$$[0] := \{\}.$$

Das ist nochmals eine andere Bezeichnung für die leere Menge. Weiter sei

$$[1] := \{[0]\} = \{\varnothing\}.$$

Das ist NICHT die leere Menge, denn $[0] \in [1]$, aber die leere Menge enthält ja nichts, also auch nicht $[0]$. Weiter geht es mit

$$[2] := \{[0], [1]\}.$$

Das ist nun eine Menge, die sowohl $\varnothing$ als auch das davon verschiedene $\{\varnothing\}$ enthält. Und als nächstes

$$[3] := \{[0], [1], [2]\},$$

und so weiter. Auf diese Art und Weise werden die natürlichen Zahlen formal in der Mengenlehre definiert!

Definition 9.4. Eine **Teilmenge** einer Menge M ist eine Menge A mit der Eigenschaft, dass jedes Elemente $x \in A$ auch in M enthalten ist.

Als Notation schreiben wir $A \subseteq B$ oder $B \supseteq A$. Man findet auch $A \subset B$ oder $B \supset A$. Wenn wir weiter ausdrücken wollen, dass zwar A Teilmenge von B ist, aber A nicht gleich B, dann schreiben wir $A \subsetneq B$, oder $B \supsetneq A$. Und wenn A keine Teilmenge von B ist, dann schreiben wir $A \not\subseteq B$.

Lemma 9.5. *Seien A und B. Dann ist $A = B$ gdw.*

$$A \subseteq B \quad \textit{und} \quad B \subseteq A.$$

Beweis. Wenn $A = B$, dann enthalten A und B die gleichen Elemente und es gilt per Definition sicherlich $A \subseteq B$ und $B \subseteq A$. (Es gilt immer $A \subseteq A$.)

Nehmen wir nun umgekehrt an, dass $A \subseteq B$ und $B \subseteq A$ gelten. Aus $x \in A$ folgt wegen $A \subseteq B$ auch $x \in B$. Aus $x \in B$ folgt wegen $B \subseteq A$ auch $x \in A$. Also gilt $x \in A \iff x \in B$. Das bedeutet per Definition aber nichts anderes als $A = B$. □

Bemerkung 9.6. Das Induktionsprinzip (PA5) besagt das folgende über Teilmengen von $\mathbb{N}_0$. Die einzige Teilmenge $M \subseteq \mathbb{N}_0$ mit den beiden Eigenschaften

(i) $0 \in M$, und

(ii) für alle $x \in M$ gilt $x + 1 \in M$,

ist die Menge $\mathbb{N}_0$ selbst.

9.1.2. *Mengen beschreiben durch Eigenschaften.* Oft ist es nicht praktisch, alle Elemente einer Menge aufzulisten. Zum Beispiel mußten wir vorhin bei $\mathbb{N}_0$ mit … arbeiten. Das ist nicht sehr befriedigend, weil wir implizit darauf bauen, dass alle die … durch das gleiche ersetzen. Besser ist es, wenn man die Elemente einer Menge durch eine Eigenschaft beschreiben kann und dadurch die Menge festlegt. Das nimmt dann die folgende Form an:

$$M = \{ \text{ alle Dinge } x \ ; \ x \text{ hat die Eigenschaft blup}\}.$$

Anstelle von ; kommt auch die Notation | vor. Man kann auch zuerst die Dinge auf eine andere Menge einschränken und dann nach einer Eigenschaft filtern:

$$L = \{x \in M \ ; \ x \text{ hat die Eigenschaft bla}\}.$$

Dann landen in der Menge L alle Elemente die blup und bla haben.

Beispiel 9.7.

(1) $\mathbb{N}_0 = \{x \ ; \ x \text{ ist natürliche Zahl }\}$.
(2) $G = \{x \in \mathbb{N}_0 \ ; \ x \text{ ist gerade Zahl }\}$.
(3) $G \subseteq \mathbb{N}_0$.

Definition 9.8. Die **Potenzmenge** einer Menge M ist die Menge aller Teilmengen von M. Wir schreiben

$$\mathscr{P}(M) := \{A \ ; \ A \subseteq M\}.$$

Beispiel 9.9.

(1) $\mathscr{P}(\{$🐟, ☎$\}) = \{\varnothing, \{$🐟$\}, \{$☎$\}, \{$🐟, ☎$\}\}$,
(2) $\mathscr{P}([2]) = \{\varnothing, [0], \{[1]\}, \{[2]\}, [1], \{\varnothing, [2]\}, \{[1], [2]\}, [2]\}$.

9.2. **Mengenoperationen.** Entsprechend den logischen Operationen *und, oder, nicht* von beschreibenden Aussagen gibt es Operationen Schnitt ($\cap$ entsprechend $\wedge$), Vereinigung ($\cup$ entsprechend $\vee$) und Differenz ($\smallsetminus$ entsprechend $\neg$) für Mengen. Zur Veranschaulichung der Operationen eignen sich Venn-Diagramme.

Definition 9.10. Die **Vereinigung** zweier Mengen A und B ist die Menge mit Notation $A \cup B$, gesprochen A vereinigt B, definiert als

$$A \cup B := \{x \ ; \ x \in A \text{ oder } x \in B\}.$$

Beispiel 9.11.

(1) $\{$🐟, 🗲, ✉, ☎$\} \cup \{$🐟, 🎷, ♫, 🔊$\} = \{$🐟, 🎷, ♫, 🗲, ✉, 🔊, ☎$\}$,
(2) $[3] = [2] \cup \{[2]\}$,
(3) $\{n \in \mathbb{N}_0 \ ; \ n \text{ ist gerade}\} \cup \{n \in \mathbb{N}_0 \ ; \ n \text{ ist ungerade}\} = \mathbb{N}_0$,
(4) für alle $n \in \mathbb{N}_0$ ist per (rekursiver[6]) Definition: $[n+1] := [n] \cup \{[n]\}$.

Definition 9.12. Der **Schnitt** zweier Mengen A und B ist die Menge mit Notation $A \cap B$, gesprochen A geschnitten B, definiert als

$$A \cap B := \{x \ ; \ x \in A \text{ und } x \in B\}.$$

Beispiel 9.13.

(1) $\{$🐟, 🗲, ✉, ☎$\} \cap \{$🐟, 🎷, ♫, 🔊$\} = \{$🐟$\}$,
(2) $[2] = [3] \cap [2]$,
(3) $\{n \in \mathbb{N}_0 \ ; \ n \text{ ist gerade}\} \cap \{n \in \mathbb{N}_0 \ ; \ n \text{ ist ungerade}\} = \varnothing$,

[6]Das ist eine clevere Definitionsmethode, bei der man unendlich viele Definitionen gleichzeitig machen kann, obwohl diese Definitionen alle der Reihe nach voneinander abhängen. Das ist quasi vollständige Induktion für Definitionen.

(4) $\{n \in \mathbb{N}_0 \ ; \ 2 \mid n\} \cap \{n \in \mathbb{N}_0 \ ; \ 3 \mid n\} = \{n \in \mathbb{N}_0 \ ; \ 6 \mid n\}$.

Definition 9.14. Der **Differenz** zweier Mengen A und B ist die Menge mit Notation $A \setminus B$ (auch $A - B$), gesprochen A ohne B, definiert als

$$A \setminus B := \{x \in A \ ; \ \neg(x \in B)\}.$$

Für eine Teilmenge $B \subseteq A$ spricht man vom **Komplement von B (in A)** und notiert dieses Komplement als $B^c = A \setminus B$. In der Notation B^c muß die Obermenge A mitgedacht werden. Diese muß also aus dem Kontext klar sein.

Beispiel 9.15.

(1) $\{$🐟, 🗲, ✉, ☎$\} \setminus \{$🐟, 🎵, 🎶, 👂$\} = \{$🗲, ✉, ☎$\}$,
(2) $[3] \setminus [2] = \{[2]\}$,
(3) $\{n \in \mathbb{N}_0 \ ; \ n \text{ ist gerade}\} \setminus \{n \in \mathbb{N}_0 \ ; \ n \text{ ist ungerade}\} = \{n \in \mathbb{N}_0 \ ; \ n \text{ ist gerade}\}$,
(4) $\{n \in \mathbb{N}_0 \ ; \ 3 \mid n\} \setminus \{n \in \mathbb{N}_0 \ ; \ 2 \mid n\} = \{n \in \mathbb{N}_0 \ ; \ \exists a \in \mathbb{N}_0 : \ n = 6a + 3\}$,
(5) In $\mathbb{N}_0$ ist das Komplement von $\{n \in \mathbb{N}_0 \ ; \ n \text{ ist gerade}\}$ gegeben durch

$$\{n \in \mathbb{N}_0 \ ; \ n \text{ ist gerade}\}^c = \{n \in \mathbb{N}_0 \ ; \ n \text{ ist ungerade}\}.$$

Proposition 9.16. *Sei n eine natürliche Zahl und sei M eine Menge mit genau n Elementen. Dann enthält die Potenzmenge $\mathscr{P}(M)$ genau 2^n Elemente.*

Beweis. Induktionsverankerung: Wenn $n = 0$, dann muß $M = \varnothing$ sein. Die Potenzmenge der leeren Menge ist

$$\mathscr{P}(\varnothing) = \{\varnothing\},$$

also mit genau $1 = 2^0$ vielen Elementen. Die Behauptung stimmt also für $n = 0$.

Induktionsschritt. Wir nehmen an, dass die Behauptung für Mengen mit n Elementen gilt und zeigen sie für Mengen M mit $n+1$ vielen Elementen. Sei $P \in M$ ein Element. Das gibt es, weil unser M genau $n + 1 \geq 1$ viele Elemente hat. Sei $M_0 = M \setminus \{P\}$, also ohne das Element P. Dann hat M_0 genau n Elemente.

Die Teilmengen $A \subseteq M$ unterscheiden wir nun danach, ob sie P enthalten, oder nicht. Es gilt

- Entweder: $P \notin A$, also $A \subseteq M_0$. Dann ist A bereits eine Teilmenge von M_0, und jede Teilmenge B von M_0 kommt vor, nämlich als $A = B$.
- Oder: $P \in A$, also $A = (A \setminus \{P\}) \cup \{P\}$ mit der Teilmenge $B = A \setminus \{P\}$ von M_0. Und jede Teilmenge B von M_0 kommt vor, nämlich für $A = B \cup \{P\}$.

Von beiden Sorten gibt es genausoviele wie es Teilmengen B von M_0 gibt. Also ist die Anzahl von $\mathscr{P}(M)$

$$\begin{aligned} \text{Anzahl von } \mathscr{P}(M) &= \text{ Anzahl von } \{A \subseteq M \ ; \ P \notin A\} + \text{ Anzahl von } \{A \subseteq M \ ; \ P \in A\} \\ &= \text{ Anzahl von } \mathscr{P}(M_0) + \text{ Anzahl von } \mathscr{P}(M_0) \\ &= 2^n + 2^n \qquad \text{(IA)} \\ &= 2^{n+1}. \end{aligned}$$

Damit ist der Induktionsschritt gezeigt. □

Es gelten die folgenden algebraische Rechenregeln für Mengenoperationen. Vergleichen Sie diese mit den Regeln der Aussagenlogik.

Proposition 9.17. *Seien X, Y, Z Mengen. Dann gelten:*

(1) Kommutativgesetz: $X \cup Y = Y \cup X$,
(2) Assoziativgesetz: $X \cup (Y \cup Z) = (X \cup Y) \cup Z$,
(3) Kommutativgesetz: $X \cap Y = Y \cap X$,

(4) Assoziativgesetz: $X \cap (Y \cap Z) = (X \cap Y) \cap Z$,
(5) Distributivgesetz: $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,
(6) Distributivgesetz: $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

Beweis. Wir beweisen exemplarisch (5). Für alle P gilt

$$\begin{aligned} P \in X \cup (Y \cap Z) &\iff P \in X \text{ oder } P \in Y \cap Z \\ &\iff (P \in X) \text{ oder } (P \in Y \text{ und } P \in Z) \\ &\iff (P \in X \text{ oder } P \in Y) \text{ und } (P \in X \text{ oder } P \in Z) \\ &\iff (P \in X \cup Y) \text{ und } (P \in X \cup Z) \\ &\iff P \in (X \cup Y) \cap (X \cup Z). \end{aligned}$$

Die anderen Beweise gehen genauso. Man formuliert die Behauptung, ein Element P sein enthalten in der linken Seite in einen logischen Ausdruck um, nutzt in der Aussagenlogik die verwandte algebraische Regel und übersetzt dies wieder in das Enthaltensein des Elements in einen Ausdruck mit den beteiligten Mengen, dann der rechten Seite der Gleichung. □

Proposition 9.18. *Seien A und B Teilmengen einer Menge M. Dann gelten die de Morgan'schen Regeln:*
(1) $(A \cup B)^c = A^c \cap B^c$,
(2) $(A \cap B)^c = A^c \cup B^c$.
Weiter gilt
(3) $(A^c)^c = A$,
(4) $A \smallsetminus B = A \cap B^c$,
(5) $A \smallsetminus B = B^c \smallsetminus A^c$.

Beweis. Wir beweisen exemplarisch (1). Für alle $P \in M$ gilt

$$\begin{aligned} P \in (A \cup B)^c &\iff P \notin A \cup B \iff \neg(P \in A \cup B) \\ &\iff \neg(P \in A \text{ oder } P \in B) \\ &\iff \neg(P \in A) \text{ und } \neg(P \in B) && \text{(de Morgan)} \\ &\iff (P \in A^c) \text{ und } (P \in B^c) \\ &\iff P \in A^c \cap B^c. \end{aligned}$$

Die anderen Beweise gehen wieder genauso. Wir zeigen auch noch exemplarisch (5), weil wir dies aus (3) und (4) ableiten können.

$$\begin{aligned} A \smallsetminus B &= A \cap B^c && \text{(nach (4))} \\ &= B^c \cap A && \text{(kommutativ)} \\ &= B^c \cap (A^c)^c && \text{(nach (3))} \\ &= B^c \smallsetminus A^c. && \text{(nach (4) für } B^c \text{ und } A^c \text{ statt } A \text{ und } B) \end{aligned}$$

□

Übungsaufgabe 9.1. Zeichnen Sie für jede der algebraischen Rechenregeln ein Venn-Diagramm.

Auch das exklusive oder hat eine Ensprechung bei Mengen.

Definition 9.19. Die symmetrische **Differenz** zweier Mengen A und B ist die Menge mit Notation $A \triangle B$ definiert als Die **symmetrische Differenz** von U und V ist die Menge

$$A \triangle B := (A \smallsetminus B) \cup (B \smallsetminus A) = \{x \in A \cup B \ ; \ x \notin A \text{ oder } x \notin B\}.$$

9.3. **Tupel, Produkte.** Die Tupelschreibweise kennen wir bereits von Koordinaten. Wenn man einen Punkt in der Ebene beschreiben möchte, dann braucht man zwei Koordinaten, sagen wir 1 und 3. Die Menge $\{1,3\}$ ist ein schlechter Speicher für diese Information, denn hierbei geht die Reihenfolge verloren: $\{1,3\} = \{3,1\}$, und auf die Reihenfolge kommt es an. Wir brauchen also eine Datenstruktur, die ein geordnetes Paar von Zahlen, oder allgemeiner Elementen aufnehmen kann. Weil alles aus Mengen aufgebaut werden soll, muß man eine Methode finden, über so ein geordnetes Paar in der Mengensprache zu sprechen.

Definition 9.20. Ein **Tupel** von Elementen a, b ist das **geordnete Paar** (a,b) definiert als die ein- oder zweielementige Menge

$$(a,b) := \{\{a\},\{a,b\}\}.$$

Bemerkung 9.21. Man macht sich schnell klar, dass für Elemente a, b, c, d gilt:

$$(a,b) = (c,d) \iff a = c \text{ und } b = d.$$

Also tun die so definierten Tupel genau das, was wir von ihnen wollen. Sie merken sich beide Elmente und auch, welches zuerst genannt werden soll.

So, und nun vergessen Sie die Definition eines Tupels wieder und merken sich nur noch die Eigenschaft, nach der die Tupel (a,b) unterschieden werden, und dass man beliebige Elmente in ein Tupel packen kann. Dass im Maschinenraum der Mathematik die Menge $\{\{a\},\{a,b\}\}$ arbeitet, ist für uns irrelevant.

Definition 9.22. Das **cartesische Produkt** zweier Mengen A und B ist die Menge aller Tupel

$$A \times B := \{(a,b) \ ; \ a \in A \text{ und } b \in B\}.$$

Die Mengen A und B heißen Faktoren des Produkts.

Beispiel 9.23.

- Die Felder auf dem Schachbrett haben Koordinaten, die zu einer Beschreibung als Element der Menge
$$S = \{a,b,c,d,e,f,g,h\} \times \{1,2,3,4,5,6,7,8\}.$$
führen. Es gilt $(a,1) \in S$, aber $(3,d) \notin S$, denn auf die Reihenfolge kommt es an. Der erste Eintrag des Tupels kommt aus dem ersten Faktor und der zweite Eintrag kommt aus dem zweiten Faktor.
- Die Punkte der Ebene werden mit Koordinaten aus den reellen Zahlen $\mathbb{R}$ beschrieben. Das sind die Elemente von
$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}.$$

Definition 9.24. Seien Mengen $M_1, \ldots, M_n$ gegeben. Das **cartesische Produkt** ist die Menge aller n**-Tupel**

$$M_1 \times \ldots \times M_n := \{(a_1, \ldots, a_n) \ ; \ a_i \in M_i \text{ für alle } 1 \le i \le n\}.$$

Beispiel 9.25. Wir können nun leicht auch über den 4-dimensionalen Raum sprechen. Die Punkte darin sind die Elemente von

$$\mathbb{R}^4 := \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}.$$

Und warum in Dimension 4 stehenbleiben? Sei n eine natürliche Zahl. Dann ist der n-dimensionale Raum

$$\mathbb{R}^n := \underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{n\text{-viele}}.$$

Bemerkung 9.26. Ein n-Tupel für $n = 2$ ist einfach ein Tupel. Für $n = 3$ heißt es ein Tripel, für $n = 4$ ein Quadrupel, ...

9.4. **Märchenstunde: Russelsche Antinomie.** Die **Russelsche Antinomie**[7] spricht über die Menge R mit der folgenden Definition.

$$R = \{A \ ; \quad A \text{ ist eine Menge, die sich nicht selbst enthält. }\}.$$

In unserer naiven Form der Mengenlehre können wir ein solches Element A mit $A \in A$ rekursiv definieren. Wir fordern zum Beispiel, dass

$$A = \{\text{}, A\}$$

ist. Dann ist klar $A \in A$, haben wir ja so aufgeschrieben. Aber was A ist, wissen wir noch nicht. Setzen wir A in die Beschreibung ein, erhalten wir

$$A = \{\text{}, \{\text{}, A\}\},$$

und so weiter

$$A = \{\text{}, A\} = \{\text{}, \{\text{}, A\}\} = \{\text{}, \{\text{}, \{\text{}, A\}\}\} \dots$$

Wir bekommen eine ungefähre Ahnung, wie kompliziert A aussieht. Und vielleicht sind wir ja auch überzeugt, dass es so ein A mit der absurden Eigenschaft $A \in A$ geben kann.

Enthält R sich selbst? Machen wir eine Fallunterscheidung: nehmen wir an $R \notin R$. Dann erfüllt R die beschreibende Eigenschaft für Elemente von R. Folglich gilt $R \in R$. Aber das geht nicht, denn für eines muß sich R entscheiden: $R \in R$ und $R \notin R$ geht nicht beides.

Der andere Fall ist $R \in R$. Als Element von R erfüllt R die Eigenschaft, welche die Elemente von R beschreibt, R enthält sich nicht: $R \notin R$. Und wieder haben wir den gleichen Widerspruch.

Die Russelsche Antinomie ist die Reinkarnation in Mengensprache der Paradoxie des Barbiers von Sevilla. Wenn man mit Mengen hantiert, dann muß man aufpassen. Es gibt mathematische Lösungen für die Russelsche Antinomie in der Mathematik, die den Bereich der naiven Mengenlehre verlassen und uns im Detail daher nicht zu interessieren brauchen. Ein Stichwort wäre Mengenlehre nach dem Axiomensystem von Zermelo-Fraenkel. In dieser Form der Mengenlehre gibt es keine Menge, die sich selbst enthält (Konsequenz des Fundierungsaxiom). Die Menge R wäre dann die Menge aller Mengen, aber diese gibt es in ZF-Mengenlehre auch nicht. Die Beschreibung durch die Eigenschaft $A \notin A$ wird in ZF verboten.

Take home message Kapitel §9.

- Definition einer Menge.
- Mengen sind gleich $\iff$ sie enthalten die gleichen Elemente.
- Veranschaulichung einer Menge mit Venn-Diagramm.
- $\cup, \cap, \smallsetminus, \mathscr{P}(-)$ mit Rechenregeln wie logische Operationen.
- Tupel von Elementen und Produkte von Mengen.

[7] Antinomie ist ein Begriff aus der philosophischen Logik, der einen ableitbaren Widerspruch beschreibt. Umgangssprachlich spricht man von einer Paradoxie.

10. Äquivalenzrelationen, rationale und ganze Zahlen

Quellen: [GK23] Kapitel 2.5, [SchSt18] Kapitel 4.2.1 und Kapitel 6.2+3

10.1. **Motivation: was ist eine rationale Zahl?** Rationale Zahlen sind diejenigen Zahlen aus der Schule, die man als Bruch mit ganzzahligem Zähler und Nenner schreiben kann. Man braucht also zuerst die ganzen Zahlen

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

dafür; die behandeln wir naiv und nehmen sie als gegeben an. Formal konstruiert werden die ganzen Zahlen später.

Eine rationale Zahl läßt sich also schreiben als, beispielsweise

$$\frac{1}{2}, \frac{355}{113}, \frac{17}{1}, \frac{-3}{7}, \frac{9234156}{123454321456}, \frac{0}{1}, \frac{3}{-7}, \frac{6}{12}, \dots$$

also allgemein als ein $\frac{a}{b}$ mit $b \neq 0$. Die rationalen Zahlen sind demnach die Menge aller solcher Ausdrücke

$$\mathbb{Q} = \left\{ \frac{a}{b} \ ; \ (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \right\}.$$

Aber jetzt fangen die Probleme an, denn es gilt doch sicherlich

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{17}{34} = \frac{-19}{-38} = \dots$$

Was bedeutet hier gleich? Diese unscheinbare Frage ist die alles entscheidende mathematische Frage hier. Denn offenbar sind die Symbole $\frac{1}{2}$ und $\frac{-19}{-38}$ nicht gleich. Trotzdem wollen wir diese Ausdrücke als gleich ansehen, damit wir die rationale Zahl, welche die Lösung der Gleichung $2x = 1$ ist, nur einmal in der Menge $\mathbb{Q}$ haben.

⚠ Die Kunst, **verschiedene Dinge als gleich** anzusehen, wird mittels des Begriffs der Äquivalenzrelation gemeistert.

10.2. **Äquivalenzrelationen.** Wenn die Elemente einer Menge miteinander in Beziehung stehen, dann drückt man dies durch eine Relation aus. Es gibt verschiedene Arten von Relationen, die für uns wichtigste formalisiert Eigenschaften der Gleichheit.

Definition 10.1. Eine **(binäre) Relation** auf einer Menge X ist eine Teilmenge

$$R \subseteq X \times X.$$

Bemerkung 10.2. Eine Relation R hebt eine Teilmenge der Tupel (a, b) mit $a, b \in X$ hervor. Dies sind die Paare, die bezüglich R „zueinander in Relation stehen“.

Beispiel 10.3. $X = \{\text{Schere, Stein, Papier}\}$ und

$$R = \{(a, b) \ ; \ \ a \text{ gewinnt gegen } b \text{ beim Spiel „Schere, Stein, Papier“}\}.$$

Wir können $X \times X$ als Tabelle ansehen und markieren, welche Tupel zu R gehören:

R	Schere	Stein	Papier
Schere			•
Stein	•		
Papier		•	

Dabei muss man vereinbaren, wie die Tabelle zu lesen ist. Hier haben wir vertikal den ersten Eintrag des Tupels und horizontal den zweiten Eintrag vermerkt.

Definition 10.4. Eine **Äquivalenzrelation** auf einer Menge X ist eine Relation R auf X mit den folgenden Eigenschaften, die sich am besten in der suggestive Notation $\sim$ für die Relation definiert durch

$$a \sim b :\iff (a,b) \in R$$

formulieren lassen.

(i) **reflexiv:** für alle $x \in X$ gilt $x \sim x$.
(ii) **symmetrisch:** für alle $x, y \in X$ gilt: $x \sim y \iff y \sim x$.
(iii) **transitiv:** für alle $x, y, z \in X$ gilt: aus $x \sim y$ und $y \sim z$, folgt $x \sim z$.

Notation 10.5. Eine Äquivalenzrelation ist eine Relation, welche gewisse Eigenschaften der Gleichheit formalisiert. Die Schreibweise $a \sim b$ anstelle von $(a,b) \in R$ erinnert daran. Andere übliche Symbole für eine Äquivalenzrelation sind $\equiv, \simeq, \cong, \ldots$. Das gewählte Symbol sollte einen symmetrischen Charakter haben. Asymmetrische Symbole wie $>$, $<$, etc. sind nicht gut für Äquivalenzrelationen.

Beispiel 10.6. Machen Sie sich bei jedem Beispiel klar, dass es sich um eine Äquivalenzrelation handelt (oder eben nicht).

(1) Auf der Menge der Schülerinnen und Schüler (SuS) einer Schule definieren wir eine Äquivalenzrelation dadurch, dass zwei SuS als äquivalent bezeichnet werden, wenn sie in die gleiche Klasse gehen. Wir nennen das die **Schulklassenäquivalenzrelation**.
(2) In einer Bücherei könnte die folgende Äquivalenzrelation zum Tragen kommen. Wir gehen mal davon aus, dass jedes Buch einem eindeutigen Genre zugeordnet werden kann. Wir definieren dann für Bücher A und B

$$A \sim B :\iff A \text{ und } B \text{ gehören zum gleichen Genre.}$$

Das definiert eine Äquivalenzrelation. Oft werden die zueinander äquivalenten Bücher im Regal zusammengestellt.
(3) Die Relation „Schere, Stein, Papier“ aus Beispiel 10.3 ist weder reflexiv noch symmetrisch noch transitiv.
(4) Gleichheit von Elementen von X ist eine Äquivalenzrelation. Diese Relation wird durch die Diagonale

$$X \times X \supseteq \Delta := \{(a,a) \in X \times X \;;\; a \in X\}$$

dargestellt und $a = b \iff (a,b) \in \Delta$ geschrieben.
(5) Gleichheit von Mengen ist eine Äquivalenzrelation.
(6) Logische Äquivalenz von Aussagen ist eine Äquivalenzrelation.

Bemerkung 10.7. Ein subtiler Fehler ist in der folgenden Argumentation versteckt.

Behauptung: aus den Eigenschaften symmetrisch und transitiv einer Relation $\sim$ folgt bereits die Eigenschaft reflexiv.

Beweis: Für ein beliebiges x und irgendein y mit $x \sim y$ folgt aus Symmetrie $y \sim x$. Transitivität zeigt aus $x \sim y$ und $y \sim x$ bereits $x \sim x$, fertig.

Der Fehler besteht darin, ohne Begründung für seine Existenz das Element y aus dem Hut gezaubert zu haben. Wenn es ein solches y nicht gibt, dann funktioniert das Argument nicht. Aus diesem Beispiel soll mensch lernen, dass die Existenz von Elementen mit gewissen Eigenschaften stets zu begründen ist.

Definition 10.8. Sei $\sim$ eine Äquivalenzrelation auf der Menge X. Die **Äquivalenzklasse** zu einem $a \in X$ bezüglich $\sim$ ist die Teilmenge von X

$$[a] := \{x \in X \;;\; a \sim x\}.$$

Beispiel 10.9.

(1) Die Äquivalenzklassen der Schulklassenäquivalenzrelation sind die Schulklassen der Schule.
(2) Auf der Menge der Lebewesen ist die biologische Einteilung nach Arten eine Äquivalenzrelation. Zwei Lebewesen heißen äquivalent, wenn sie zur gleichen Art gehören. Eine Äquivalenzklasse besteht aus allen Lebewesen einer Art.

Proposition 10.10. *Sei $\sim$ eine Äquivalenzrelation auf der Menge X. Seien $a, b \in X$. Dann:*
(1) $a \in [a]$,
(2) $a \in [b]$ genau dann, wenn $b \in [a]$.

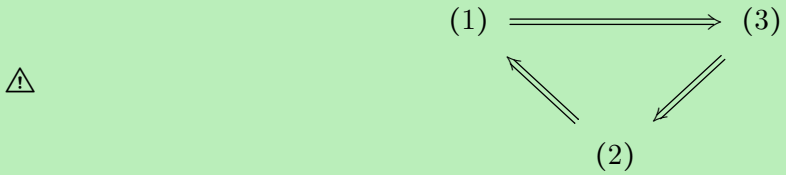
Beweis. Aussage (1): Weil $\sim$ reflexiv ist, folgt $a \sim a$. Per Definition der Klasse $[a]$ folgt $a \in [a]$.
Für Aussage (2) benutzen wir die Symmetrie:

$$a \in [b] \iff b \sim a \overset{\text{symmetrisch}}{\iff} a \sim b \iff b \in [a].$$ □

Satz 10.11. *Sei $\sim$ eine Äquivalenzrelation auf der Menge X. Seien $a, b \in X$. Dann sind die folgenden Aussagen äquivalent.*
(1) $[a] = [b]$.
(2) $a \sim b$.
(3) $[a] \cap [b]$ ist nicht leer.

Beweis. Bevor wir das beweisen, interpretieren wir die Aussagen für die Schulklassenäquivalenzrelation. Seien also a und b aus der Menge der SuS. Dann (1) stimmt die Klasse von a mit der Klasse von b überein, genau dann wenn (2) a und b in die gleiche Klasse gehen, genau dann wenn (3) es ein x aus der Menge der SuS gibt, der sowohl in die Klasse von a als auch in die Klasse von b geht. Ja, das paßt.

Wir wollen zeigen, dass die drei Aussagen (1) – (3) äquivalent sind durch einen Ringschluss.



Das zeigt auch alle Implikationen! und damit die Äquivalenz der Aussagen.

(1) $\Longrightarrow$ (3): Wenn $[a] = [b]$ gilt, dann ist $[a] \cap [b] = [a]$, und das enthält das Element a nach Proposition 10.10 (1). Also ist der Schnitt $[a] \cap [b]$ nicht leer.

(3) $\Longrightarrow$ (2): Wenn $[a] \cap [b]$ nicht leer ist, dann gibt es ein $x \in [a] \cap [b]$, also $x \in [a]$ und $x \in [b]$. Per Definition der Klassen heißt das $a \sim x$ und $b \sim x$. Aus Symmetrie folgt $x \sim b$, und wegen transitiv auch $a \sim b$ (via x).

(2) $\Longrightarrow$ (1): Es gilt also nun $a \sim b$. Weil $\sim$ symmetrisch ist, gilt auch $b \sim a$. Wir zeigen nun $[a] \subseteq [b]$. Die umgekehrte Aussage $[b] \subseteq [a]$ geht genauso, und beide zusammen zeigen $[a] = [b]$.
Sei $x \in [a]$ beliebig. Das bedeutet $a \sim x$. Zusammen mit $b \sim a$ folgt aus Transitivität $b \sim x$. Per Definition von $[b]$ bedeutet das $x \in [b]$. Weil das Element x beliebig war, folgt $[a] \subseteq [b]$. □

Korollar 10.12. *Sei $\sim$ eine Äquivalenzrelation auf der Menge X. Seien $a, b \in X$. Dann gilt genau eine der beiden Aussagen:*
(1) $[a] \cap [b] = \varnothing$,
(2) $[a] = [b]$.

Zwei Äquivalenzklassen sind entweder gleich (alle Elemente gemeinsam), oder sie schneiden sich nicht (kein Element gemeinsam).

Beweis. Genau eine der beiden Aussagen bedeutet, die eine ist falsch genau dann, wenn die andere wahr ist. Wir müssen also zeigen

$$[a] = [b] \iff \neg([a] \cap [b] = \varnothing).$$

Das ist Teil von Satz 10.11, nämlich (1) $\iff$ (3). □

Bemerkung 10.13. Die Äquivalenzklassen bezüglich einer Relation auf einer Menge X zerlegen diese Menge X in disjunkte (d.h. verschiedene Äquivalenzklassen schneiden sich nur leer!) Teile. Man nennt soetwas eine **Partition** von X.

In der Tat, jedes Element von X sitzt in einer Äquivalenzklasse, nämlich seiner eigenen. Und sobald sich zwei Äquivalenzklassen treffen, sind sie nach Korollar 10.12 bereits gleich. Eine Äquivalenzrelation ist also nichts anderes als eine Klasseneinteilung einer Menge, so wie die Schulklassen in der Schulklassenäquivalenzrelation.

Bemerkung 10.14. Äquivalenzrelationen und Äquivalenzklassen eignen sich hervorragend, um Dinge mathematisch zu klassifizieren. Man reduziert die Komplexität, weil man sich nur noch mit den für gewissen Fragen wesentlichen Aspekten beschäftigen muß. So führt die Betrachtung der Parität einer natürlichen Zahl zum Konzept gerade und ungerade, also nur noch zwei Elementen, viel weniger als es natürlich Zahlen gibt. Damit läßt sich zum Beispiel die Frage nach Lösungen in natürlichen Zahlen der Gleichung

$$x(x+1) = 1 + 2y^5$$

beantworten. Die linke Seite ist stets gerade, aber die rechte Seite ist stets ungerade. Ergo gibt es keine Lösung $(x, y) \in (\mathbb{N}_0)^2$. Das Argument hat anstelle von $\mathbb{N}_0$ mit den Äquivalenzklassen gerade/ungerade der Äquivalenzrelation modulo 2 gearbeitet.

10.3. **Formale Definition der rationalen Zahlen.**

Definition 10.15. Eine **rationale Zahl** ist eine Äquivalenzklasse der folgenden Relation auf der Menge $X = \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, und zwar

$$(a, b) \sim (c, d) :\iff ad = bc.$$

Die Äquivalenzklasse von (a, b) schreiben wir als

$$\frac{a}{b} := [(a, b)].$$

Die **Menge der rationalen Zahlen** ist daher

$$\mathbb{Q} = \left\{ \frac{a}{b} \;;\; (a, b) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}) \right\}.$$

Wir kürzen wie folgt ab: $0 = \frac{0}{1}$, und $1 = \frac{1}{1}$.

Bemerkung 10.16. Wie sieht es aus mit der eingangs angeführten Problematik, wie

$$\frac{1}{2} = \frac{-19}{-38}$$

zu verstehen ist? Nun, das sind nun Äquivalenzklassen. Und für Äquivalenzklassen von Elementen gilt, dass sie gleich sind, sobald die Elemente äquivalent sind. Die Bruchgleichung ist also tatsächlich eine Gleichheit der Äquivalenzklassen, sobald wir nachgeprüft haben, dass

$$(1, 2) \sim (-19, -38)$$

mit dem $\sim$ aus der Definition der rationalen Zahlen. Per Definition ist das so, genau wenn

$$1 \cdot (-38) = 2 \cdot (-19).$$

Das ist korrekt, also haben wir wirklich die gleiche Äquivalenzklasse. Die Symbole mögen verschieden sein, aber das Ding an sich ist das gleiche!

Die Definition 10.15 ist problematisch, denn sie enthält Behauptungen, die nicht unmittelbar klar sind. Diese Definition verlangt daher nach einem Beweis, dass sie wohldefiniert ist.

Beweis der Wohldefiniertheit von Definition 10.15. Wir müssen zeigen, dass durch $\sim$ auf X tatsächlich eine Äquivalenzrelation definiert wird.

• *reflexiv*: Sei $(a,b) \in X$ beliebig. Dann gilt $(a,b) \sim (a,b)$, denn $ab = ba$.

• *symmetrisch*: Seien (a,b) und (c,d) Elemente von X. Weiter sei $(a,b) \sim (c,d)$, gleichbedeutend per Definition $ad = bc$. Wir wollen zeigen, dass $(c,d) \sim (a,b)$ gilt. Per Definition müssen wir nachweisen

$$cb = da.$$

Aber die Multiplikation ist kommutativ: $cb = bc$, nach Voraussetzung gilt $bc = ad$ und $ad = da$. Das zeigt zusammen, die Behauptung.

• *transitiv*: Seien $(a,b),(c,d),(e,f) \in X$ mit $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$. Das bedeutet per Definition, es gilt

$$ad = bc \quad \text{und} \quad cf = de.$$

Wir wollen $(a,b) \sim (e,f)$ zeigen. Per Definition müssen wir nachweisen

$$af = be.$$

Wir rechnen zuerst

$$d(af - be) = daf - dbe = (ad)f - b(de) = (bc)f - b(cf) = 0.$$

Weil $d \neq 0$ ist, und ein Produkt nur dann 0 ist, wenn einer der Faktoren 0 ist[8], folgt aus $d \cdot (af - be) = 0$ bereits $af - be = 0$. Das ist nach Umstellen die behauptete Gleichung. □

Bemerkung 10.17. Rationale Zahlen sollen sich nicht ändern, wenn man erweitert oder kürzt. Das bedeutet, dass für alle $a \in \mathbb{Z}$ und $b, x \in \mathbb{Z} \setminus \{0\}$ gelten soll:

$$\frac{a}{b} = \frac{ax}{bx}.$$

Das prüfen wir leicht anhand der Definition von $\sim$ nach:

$$a(bx) = (ab)x = (ba)x = b(ax).$$

Definition 10.18. Auf $\mathbb{Q}$ sind Addition und Multiplikation wie folgt definiert. Für rationale Zahlen $\frac{a}{b}$ und $\frac{c}{d}$ gilt

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

und

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Auch hier muss man die Wohldefiniertheit der Definition prüfen.

[8] Das ist für die ganzen Zahlen eine wohlbekannte Eigenschaft und hier entscheidend. Wir müssen das also bei Gelegenheit beweisen!

Beweis. Seien $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$ jeweils alternative Beschreibungen der entsprechenden rationalen Zahlen. Dann ist mittels Erweitern und Kürzen

$$\begin{aligned}
\frac{ad+bc}{bd} &= \frac{(ad+bc)b'd'}{bdb'd'} && \text{(Erweitern mit } b'd'\text{)}\\
&= \frac{(ab')dd' + bb'(cd')}{bdb'd'}\\
&= \frac{(ba')dd' + bb'(dc')}{bdb'd'} && \text{(}\tfrac{a}{b} = \tfrac{a'}{b'} \text{ und } \tfrac{c}{d} = \tfrac{c'}{d'}\text{)}\\
&= \frac{bd(a'd' + b'c')}{bdb'd'}\\
&= \frac{a'd' + b'c'}{b'd'} && \text{(Kürzen mit } bd\text{)}
\end{aligned}$$

Die Addition ist somit als Äquivalenzklasse unabhängig von der Wahl der Repräsentaten der zu addierenden Klassen.

$$\begin{aligned}
\frac{ac}{bd} &= \frac{acb'd'}{bdb'd'} && \text{(Erweitern mit } b'd'\text{)}\\
&= \frac{(ab')(cd')}{bdb'd'}\\
&= \frac{(ba')(dc')}{bdb'd'} && \text{(}\tfrac{a}{b} = \tfrac{a'}{b'} \text{ und } \tfrac{c}{d} = \tfrac{c'}{d'}\text{)}\\
&= \frac{bd(a''c')}{bdb'd'}\\
&= \frac{a'c'}{b'd'} && \text{(Kürzen mit } bd\text{)}
\end{aligned}$$

und auch die Multiplikation ist wohldefiniert. □

Wir erinnern an die Abkürzungen $0 = \frac{0}{1}$, und $1 = \frac{1}{1}$.

Proposition 10.19. *Addition und Multiplikation von $\mathbb{Q}$ erfüllt die folgenden algebraischen Gesetze. Zuerst die Addition alleine:*

(1) kommutativ: für all $x, y \in \mathbb{Q}$ gilt: $x + y = y + x$
(2) assoziativ: für all $x, y, z \in \mathbb{Q}$ gilt: $(x + y) + z = x + (y + z)$
(3) additives neutrales Element: für alle $x \in \mathbb{Q}$ gilt: $x + 0 = 0 + x = x$.
(4) additives Inverses: für alle $x \in \mathbb{Q}$ gibt es $y \in \mathbb{Q}$ mit $x + y = y + x = 0$.

Als nächstes die Multiplikation alleine:

(5) kommutativ: für all $x, y \in \mathbb{Q}$ gilt: $x \cdot y = y \cdot x$
(6) assoziativ: für all $x, y, z \in \mathbb{Q}$ gilt: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(7) multiplikatives neutrales Element: für alle $x \in \mathbb{Q}$ gilt: $x \cdot 1 = 1 \cdot x = x$.
(8) multiplikatives Inverses: für alle $x \in \mathbb{Q}$, $x \neq 0$, gibt es $y \in \mathbb{Q}$ mit $x \cdot y = y \cdot x = 1$.

Und dann noch für beide zusammen:

(9) distributiv: für all $x, y, z \in \mathbb{Q}$ gilt: $x \cdot (y + z) = x \cdot y + x \cdot z$

Beweis. Das rechnet man alles ohne Probleme direkt nach. Die Existenz der Inversen geben wir an. Zu $\frac{a}{b}$ ist das additive Inverse $\frac{-a}{b}$ und das multiplikative Inverse $\frac{b}{a}$. In beiden Fällen ist die beschriebene Äquivalenzklasse unabhängig von der Wahl des Paars (a, b) mit dem man den Bruch darstellt.

Details findet man zum Beispiel in [SchSt18] Kapitel 6.3. □

10.4. **Konstruktion der ganzen Zahlen.**

Definition 10.20. Eine **ganze Zahl** ist eine Äquivalenzklasse der folgenden Relation auf $\mathbb{N}_0 \times \mathbb{N}_0$, und zwar

$$(a,b) \sim (c,d) :\iff a+d = b+c.$$

Die Menge der ganzen Zahlen $\mathbb{Z}$ ist die Menge aller Äquivalenzklassen dieser Relation

$$\mathbb{Z} = \{[(a,b)] \ ; \ a,b \in \mathbb{N}_0\}.$$

Beweis. Die angegebene Definition von $\sim$ definiert einer Äquivalenzrelation:

- reflexiv: $(a,b) \sim (a,b)$ weil $a+b = b+a$. Addition in $\mathbb{N}_0$ ist kommutativ.
- symmetrisch: sei $(a,b) \sim (c,d)$, also $a+d = b+c$. Dann gilt auch $c+b = d+a$, und damit $(c,d) \sim (a,b)$.
- transitiv: seien $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$. Dann gilt $a+d = b+c$ und $c+f = d+e$. Daraus folgt

  $$(a+f)+d = (a+d)+f = (b+c)+f = b+(c+f) = b+(d+e) = (b+e)+d.$$

  Hier können wir nun d auf beiden Seiten d subtrahieren und erhalten das gewünschte $a+f = b+e$, somit $(a,b) \sim (e,f)$.

□

Wir erkennen vermutlich in der Definition 10.20 die ganzen Zahlen nicht wieder. Dafür müssen wir noch ein wenig arbeiten, damit die ganzen Zahlen wieder so aussehen, wie wir sie kennen.

Definition 10.21. Die Äquivalenzklasse von $(n,0)$ schreiben wir als n und die Äquivalenzklasse von $(0,n)$ schreiben wir als $-n$.

Satz 10.22. *Jeder ganze Zahl außer der* $0 = [(0,0)]$ *hat eine eindeutige Beschreibung als* n *oder* $-n$ *für eine eindeutige natürliche Zahl* n*. Es gilt*

$$\mathbb{Z} = \{n \ ; \ n \in \mathbb{N}_{>0}\} \cup \{0\} \cup \{-n \ ; \ n \in \mathbb{N}_{>0}\}.$$

Beweis. Die ganzen Zahlen n, 0 und $-n$ für $n \in \mathbb{N}_{>0}$ sind genau die Äquivalenzklassen von Elementen (a,b) mit $ab = 0$. Wir zeigen zuerst, dass jedes $(x,y) \in \mathbb{N}_0 \times \mathbb{N}_0$ zu so einem (a,b) mit $ab = 0$ äquivalent ist. Das zeigen wir per Induktion nach dem ersten Eintrag x von (x,y).

Induktionsanfang: Hier ist $x = 0$. Damit ist nichts zu zeigen, denn $(0,y)$ erfüllt bereits die Bedingung.

Induktionsschritt: Wir dürfen nun annehmen, dass für alle Paare mit erstem Eintrag $< x$ die Aussage bereits stimmt. Wenn $y = 0$, ist nichts zu zeigen, denn dann ist $(x,0)$ von der gewünschten Form. Sei daher $x \geq 1$ und $y \geq 1$. Weil $x+(y-1) = (x-1)+y$ gilt

$$(x,y) \sim (x-1, y-1).$$

Das Paar $(x-1, y-1)$ erfüllt per Induktionsannahme die Aussage. Es gibt also (a,b) mit $ab = 0$ und $(x-1,y-1) \sim (a,b)$. Aus Transitivität folgt $(x,y) \sim (a,b)$ und wir sind fertig.

Jetzt fehlt noch die Eindeutigkeit. Das sind verschiedene Fälle. Wir machen exemplarisch ein paar davon.

- Wenn $[(n,0)] = [(m,0)]$, dann gilt per Definition $n+0 = 0+m$, also $n = m$.
- Wenn $[(n,0)] = [(0,0)]$, dann gilt per Definition $n+0 = 0+0$, also $n = 0$.
- Wenn $[(n,0)] = [(0,m)]$, dann gilt per Definition $n+m = 0+0$. Weil $n+m$ als Summe von natürlichen Zahlen nur dann 0 sein kann, wenn beide Summanden 0 sind, folgt $n = m = 0$.
- usw. □

Lemma 10.23. *Es gilt additives Erweitern und Kürzen: für alle $a, b, x \in \mathbb{N}_0$ gilt*
$$[(a,b)] = [(a+x, b+x)].$$

Beweis. Man rechnet die Definition nach: $a + (b + x) = b + (a + x)$, und das folgt aus dem Kommutativ- und dem Assoziativgesetz der Addition von natürlichen Zahlen. □

Definition 10.24. Auf $\mathbb{Z}$ sind **Addition** und **Multiplikation** wie folgt definiert. Für ganze Zahlen $[(a,b)]$ und $[(c,d)]$ gilt
$$[(a,b)] + [(c,d)] := [(a+c, b+d)]$$
und
$$[(a,b)] \cdot [(c,d)] := [(ac+bd, ad+bc)].$$

Auch hier muss man die Wohldefiniertheit der Definition prüfen.

Beweis. Seien $[(a,b)] = [(a',b')]$ und $[(c,d)] = [(c',d')]$ jeweils alternative Beschreibungen der entsprechenden ganzen Zahlen. Dann ist mittels additives Erweitern und Kürzen

$$\begin{aligned}
[(a+c, b+d)] &= [(a+c+b'+d', b+d+b'+d')] && \text{(Erweitern mit } b'+d') \\
&= [((a+b')+(c+d'), b+d+b'+d')] \\
&= [((b+a')+(d+c'), b+d+b'+d')] && ([(a,b)] = [(a',b')] \text{ und } [(c,d)] = [(c',d')]) \\
&= [(b+d+a'+c', b+d+b'+d')] \\
&= [(a'+c', b'+d')] && \text{(Kürzen mit } b+d)
\end{aligned}$$

Die Addition ist somit als Äquivalenzklasse unabhängig von der Wahl der Repräsentaten der zu addierenden Klassen.

$$\begin{aligned}
[(ac+bd, ad+bc)] &= [(ac+b'c+bd+a'd, ad+a'd+b'c+bc)] && \text{(Erweitern mit } b'c+a'd) \\
&= [((a+b')c+(b+a')d, ad+a'd+b'c+bc)] \\
&= [((b+a')c+(a+b')d, ad+a'd+b'c+bc)] && ([(a,b)] = [a',b']) \\
&= [(bc+a'c+ad+b'd, ad+a'd+b'c+bc)] \\
&= [(a'c+b'd, a'd+b'c)] && \text{(Kürzen mit } bc+ad) \\
&= [(a'(c+d')+b'(c'+d), a'd'+a'd+b'c+b'c')] && \text{(Erweitern mit } a'd'+b'c') \\
&= [(a'(c'+d)+b'(c+d'), a'd'+a'd+b'c+b'c')] && ([(c,d)] = [(c',d')]) \\
&= [(a'c'+a'd+b'c+b'd', a'd'+a'd+b'c+b'c')] \\
&= [(a'c'+b'd', a'd'+b'c')] && \text{(Kürzen mit } ad'+b'c)
\end{aligned}$$

und auch die Multiplikation ist wohldefiniert. □

Proposition 10.25. *Addition und Multiplikation von $\mathbb{Z}$ erfüllt die folgenden algebraischen Gesetze. Zuerst die Addition alleine:*

(1) kommutativ: für all $x, y \in \mathbb{Z}$ gilt: $x + y = y + x$
(2) assoziativ: für all $x, y, z \in \mathbb{Z}$ gilt: $(x + y) + z = x + (y + z)$
(3) additives neutrales Element: für alle $x \in \mathbb{Z}$ gilt: $x + 0 = 0 + x = x$.
(4) additives Inverses: für alle $x \in \mathbb{Z}$ gibt es $y \in \mathbb{Z}$ mit $x + y = y + x = 0$.

Als nächstes die Multiplikation alleine:

(5) kommutativ: für all $x, y \in \mathbb{Z}$ gilt: $x \cdot y = y \cdot x$
(6) assoziativ: für all $x, y, z \in \mathbb{Z}$ gilt: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(7) multiplikatives neutrales Element: für alle $x \in \mathbb{Z}$ gilt: $x \cdot 1 = 1 \cdot x = x$.
Und dann noch für beide zusammen:
(8) distributiv: für all $x, y, z \in \mathbb{Z}$ gilt: $x \cdot (y + z) = x \cdot y + x \cdot z$

Beweis. Alle Gesetze rechnet man leicht nach. Sie folgen aus den entsprechenden Eigenschaften der Addition und Multiplikation der Natürlichen zahlen $\mathbb{N}_0$. Das additive Inverse zu $[(a,b)]$ ist $[(b,a)]$, denn

$$[(a,b)] + [(b,a)] = [(a+b, b+a)] = [(0,0)] = 0.$$

□

Bemerkung 10.26. Die richtige Interpretation von $[(a,b)]$ ist die folgende:

$$[(a,b)] = [(a,0)] + [(0,b)] = a + (-b) =: a - b$$

mit der vertrauten Subraktion von natürlichen Zahlen, wobei eben zur Ausführung der Subraktiion im Allgemeinen auf die ganzen Zahlen erweitert werden muss. Mit dieser Interpretation erschließen sich alle Formeln: die Defintion der Äquivalenzrelation:

$$(a,b) \sim (c,d) \iff a + d = b + c \iff a - b = c - d,$$

die Addition:

$$[(a,b)] + [(c,d)] = (a-b) + (c-d) = (a+c) - (b+d) = [(a+c, b+d)],$$

und der Multiplikation:

$$[(a,b)] \cdot [(c,d)] = (a-b) \cdot (c-d) = ac - ad - bc + ad = (ac + bd) - (ad + bc) = [(ac+bd, ad+bc)].$$

10.5. **Märchenstunde: Welche Dezimalzahlen sind rationale Zahlen?** Wir kennen aus der Schule Dezimalzahlen, und dass man jeden Bruch in eine Dezimalzahl umwandeln kann. Welche Dezimalzahlen entstehen dabei?

⚠ Eine abbrechende Dezimalzahl x entspricht einem Bruch mit Nenner der Form $2^a \cdot 5^b$.

In der Tat gibt es eie Zehnerpotenz 10^k, so dass die Kommaverschiebung $z = 10^k \cdot x$ zu einer ganzen Zahl wird. Dann ist aber

$$x = \frac{z}{10^k}$$

mit Nenner $10^k = 2^k \cdot 5^k$, was nach eventuellem Kürzen zu $2^a \cdot 5^b$ mit $a, b \le k$ wird. Das gilt auch umgekehrt. Ein Bruch mit Nenner der Form $2^a \cdot 5^b$ führt nach Erweitern zu einem Bruch $\frac{z}{10^k}$, und damit zu einer abbrechenden Dezimalzahl mit höchstens k Stellen hinter dem Komma.

⚠ Alle anderen rationalen Zahlen werden zu periodischen Dezimalzahlen und jede periodische Dezimalzahl ist rational.

Wir zeigen den einfachen Teil: Sei x eine periodische Dezimalzahl, sagen wir mit Periodenlänge ℓ. Dann ist $10^\ell \cdot x$ eine Dezimalzahl mit derselben Periode. Daher heben sich ab der Stelle, wo beide Zahlen x und $10^\ell \cdot x$ periodisch werden in der Differenz $y = 10^\ell \cdot x - x$ alle Stellen auf. Damit ist $y = \frac{z}{10^k}$ eine abbrechende Dezimalzahl, also ein Bruch von spezieller Sorte. Wir können daraus x berechnen, den $\frac{z}{10^k} = 10^\ell x - x = (10^\ell - 1)x$ führt zu

$$x = \frac{z}{10^k(10^\ell - 1)},$$

also einem Bruch! Der Nenner hat eine Spezielle Form, er besteht nur aus anfänglichen ℓ-vielen 9en und dann k-vielen 0. Das k ist die Anzahl der Stellen, bis die Periode einsetzt, und ℓ ist die Periodenlänge.

Um die umgekehrte Aussage zu beweisen, dass jede rationale Zahl eine periodische Dezimalzahl liefert, analysieren wir die Methode, wie man einen Bruch $\frac{a}{b}$ in eine Dezimalzahl umwandelt: man dividiert a durch b und fährt mit den Resten fort, indem man eine 0 hinzufügt und eine

Stelle weiter hinter das Komma rückt. Die Reste sind zwischen 0 und $b-1$. Davon gibt es nur endlich viele. Wird der Rest einmal 0, so bricht das Verfahren ab und wir haben eine abbrechende Dezimalzahl erhalten. Tritt die 0 nicht auf, so muss sich doch irgendwann ein Rest ein zweites mal einstellen. Ab da wiederholt sich alles! Das bedeutet, dass wir dann eine periodische Dezimalzahl erhalten.

Korollar: jede rationale Zahl läßt sich zu einem Bruch erweitern, dessen Nenner aus ℓ anfänglichen Ziffern 9 gefolgt von k-vielen Ziffern 0 besteht.

Take home message Kapitel §10.

- Äquivalenzrelationen als formale Version von Gleichheit: Vereinfachung durch Übergang zu Äquivalenzklassen.
- reflexiv, symmetrisch, transitiv.
- Kongruenz modulo m ist Äquivalenzrelation.
- Konstruktion der rationalen Zahlen
- Konstruktion der ganzen Zahlen

11. Kongruenzrechnung

Quellen: [GK23] Kapitel 7.2, 7.4 und 9

11.1. **Motivation: neue Zahlsysteme.** Das Rechnen mit Kongruenzen erlaubt einen klarern Blick auf Teilbarkeitsregeln und erklärt die 9er-Probe. Als Konzept üben Sie den Umgang mit Äquivalenzklassen und mit allgemeineren Zahlsystemen. Rechnen mit Kongruenzen geben auch Einsichten in periodische Vorgänge wie den Umgang mit der Uhr oder der Frage, welcher Wochentag an einem bestimmten Datum sein wird oder war.

11.2. **Teilbarkeit bei ganzen Zahlen.**

⚠ Auch bei ganzen Zahlen kann man von Teilbarkeit sprechen.

Zum Beispiel ist

$$-35 = (-7) \cdot 5,$$

also ist -35 durch -7 teilbar.

Definition 11.1. Seien a und m ganze Zahlen. Dann ist a durch m **teilbar** in $\mathbb{Z}$, wenn es eine ganze Zahl x gibt mit

$$a = m \cdot x.$$

Wir schreiben das kurz $m \mid a$, gelesen „m teilt a“. Wenn a nicht durch m teilbar ist, dann schreiben wir $m \nmid a$, gelesen „m teilt nicht a“.

Bemerkung 11.2. Wenn a und m natürliche Zahlen sind, dann stimmt diese Teilbarkeit in $\mathbb{Z}$ mit der Teilbarkeit in $\mathbb{N}_0$ überein. Wir haben also die alte Definition nicht verändert.

11.3. **Die Äquivalenzrelation modulo m.** Sei m eine ganze Zahl. Eine wichtige Äquivalenzrelation auf der Menge der ganzen Zahlen

$$\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$$

ist die Relation **kongruent modulo** m.

Definition 11.3. Sei m eine ganze Zahl und seien $a, b \in \mathbb{Z}$. Dann definieren wir

$$a \equiv b \pmod{m} :\iff \exists m \mid a - b.$$

Dies wird „a **ist kongruent zu** b **modulo** m“ gesprochen.

Beispiel 11.4. Sei $m = 5$. Dann ist beispielsweise modulo 5:

$$2 \equiv 7 \equiv -3 \equiv -103 \equiv 17 \equiv \ldots,$$
$$4 \equiv -1 \equiv -11 \equiv -21 \equiv 14 \equiv 9 \equiv 1004 \equiv \ldots,$$
$$3 \not\equiv 2,$$
$$1 \not\equiv 23.$$

Bemerkung 11.5. Teilbarkeit durch m und $\equiv 0 \pmod{m}$ sind das gleiche. Es gilt für alle $a \in \mathbb{Z}$:

$$a \text{ ist durch } m \text{ teilbar} \iff a \equiv 0 \pmod{m}.$$

Das folgt sofort aus der Definition: wir haben $m \mid a$ genau dann wenn $m \mid a - 0$, und das ist genau die Definition von $a \equiv 0 \pmod{m}$.

Satz 11.6. *„Kongruenz modulo m“ ist eine Äquivalenzrelation.*

Beweis. Für Äquivalenzrelation müssen wir drei Dinge nachweisen:

- *Reflexiv:* $a - a = m \cdot 0$.

- *Symmetrisch:* wenn $a \equiv b \pmod m$, dann gibt es $x \in \mathbb{Z}$ mit $a - b = mx$, somit auch
$$b - a = -mx = m(-x)$$
und damit $b \equiv a \pmod m$.
- *Transitiv:* wenn $a \equiv b \pmod m$ und $b \equiv c \pmod m$, dann gibt es $x, y \in \mathbb{Z}$ mit $a - b = mx$ und $b - c = my$. Daraus folgt
$$a - c = (a - b) + (b - c) = mx + my = m(x + y),$$
und weil $x + y \in \mathbb{Z}$, folgt $a \equiv c \pmod m$. □

Bemerkung 11.7.

⚠ Die Umformung
$$a - c = (a - b) + (b - c),$$
bei der man sich b leiht, um es gleich wieder zurückzugeben, ist ein häufiger anzutreffender Trick.

Beispiel 11.8. Liegt zwischen einem Tag im Jahr x und demselben Datum im darauffolgenden Jahr $x+1$ kein Schalttag, dann ist der Wochentag im Folgejahr $x+1$ gerade der nächst Wochentag. Also war das Datum im Jahr x ein Sonntag, dann ist es im Jahr $x + 1$ ein Montag, etc.

Das sieht man sofort ein, weil die beiden Daten nach Annahme über die Abwesenheit von Schalttagen genau 365 Tage auseinander liegen. Die Wochentage sind „periodisch modulo 7“. Das bedeutet, wenn zwischen zwei Daten eine durch 7 teilbare Zahl von Tagen liegt, dann handelt es sich um ganze Wochen und die beiden Daten haben den gleichen Wochentag. Oder anders ausgedrückt, alle 7 Tage wiederholen sich die Wochentage. Wir müssen also nur 365 modulo 7 besser verstehen. Es ist $365 - 15 = 350 = 7 \cdot 50$ durch 7 teilbar, also
$$365 \equiv 15 \pmod 7.$$
Weiter gilt $15 - 1 = 14 = 2 \cdot 7$ und daher $15 \equiv 1 \pmod 7$. Zusammen ergibt sich
$$365 \equiv 15 \equiv 1 \pmod 7.$$
Daher stimmt der Wochentag in 365 Tagen mit dem Wochentag in 1 Tag überein.

Proposition 11.9. *Sei $m \geq 1$. Dann sind $a, b \in \mathbb{Z}$ genau dann kongruent modulo m, wenn sie bei Division mit Rest durch m den gleichen Rest lassen.*

Beweis. Das ist eine gdw. Aussage. Wir müssen also zwei Implikationen zeigen. Wir nehmen zuerst an, dass a und b bei Division durch m den gleichen Rest lassen. Dann gibt es eine Rest $0 \leq r < m$ und $x, y \in \mathbb{Z}$ mit $a = mx + r$ und $b = my + r$. Damit ist
$$a - b = (mx + r) - (my + r) = mx - my + r - r = m(x - y).$$
Das zeigt $a \equiv b \pmod m$.

Jetzt zeigen wir die andere Richtung. Wir nehmen also nun an, dass $a \equiv b \pmod m$. Das bedeutet, es gibt $x \in \mathbb{Z}$ mit $a - b = mx$. Sei nun $b = my + r$ die Division von b durch m mit Rest r, also $0 \leq r < m$. Dann gilt
$$a = (a - b) + b = mx + my + r = m(x + y) + r,$$
und das ist die Division mit Rest von a durch m. Offenbar ist der Rest hier auch r. Das zeigt die Behauptung. □

Bemerkung 11.10. In Proposition 11.9 haben wir heimlich den Begriff der Division mit Rest von natürlichen Zahlen auf ganze Zahlen ausgedehnt. Satz 8.8 gilt weiter sinngemäß: für $a \in \mathbb{Z}$ und $m \geq 1$ gibt es eindeutig $q, r \in \mathbb{Z}$ mit

(i) $\quad a = q \cdot m + r,$

(ii) $0 \le r < m$.

Definition 11.11. Die Äquivalenzklassen von „Kongruenz modulo m“ heißen **Kongruenzklassen modulo** m (oder **Restklassen modulo** m). Wir vereinbaren die Notation

$$[a]_m$$

für die Restklasse von $a \in \mathbb{Z}$ modulo m.

Bemerkung 11.12. Die Kongruenzklassen modulo 2 sind genau die foglenden zwei:

- **gerade** = $[0]_2$: die geraden Zahlen (Rest 0), und
- **ungerade** = $[1]_2$: die ungeraden Zahlen (Rest 1).

Korollar 11.13. *Sei $m \ge 1$. Dann gibt es genau m viele Restklassen modulo m, nämlich*

$$[0]_m, [1]_m, [2]_m, \dots, [m-1]_m.$$

Beweis. Das folgt sofort aus Proposition 11.9, weil a und sein Rest bei Division durch m die gleiche Kongruenzklasse beschreibt. Und genauer, dass diese durch die möglichen Rest beschriebenen Kongruenzklassen alle verschieden sind. □

11.4. Rechnen mit Kongruenzen.

⚠ „Kongruenz modulo m“ ist deshalb so praktisch, weil man mit Kongruenzklassen so rechnen kann, wie mit ganzen Zahlen. Gewisserweise kann man also ein „Rechnen mit Resten“ erklären. Alle Rechnungen werden nur bis auf Kongruenz modulo m ausgeführt.

Dadurch werden die Ergebnisse weniger aussagekräftig, weil man zum Beispiel $1, m+1, 2m+1, \dots$ nicht mehr unterscheiden kann, aber es ergeben sich Vereinfachungen, die nützlich sein können.

Beispiel 11.14. Einen Spezialfall haben wir bereit früher in §4.2 kennen gelernt: modulo 2 Rechnen ist wie Rechnen mit gerade und ungerade.

⚠ **Rechnen durch die „Brille modulo m“**: wir machen uns nun klar, dass man beim Rechnen in den ganzen Zahlen $\mathbb{Z}$, also bei Addition, Subtraktion und Multiplikation, Zahlen durch modulo m kongruente Zahlen ersetzen kann und dann ein modulo m kongruentes Ergebnis bekommt.

Satz 11.15. *Sei $m \ge 1$. Seien a, a' und b, b' ganze Zahlen mit*

$$a \equiv a' \pmod m,$$
$$b \equiv b' \pmod m.$$

Dann gilt

$$a + b \equiv a' + b' \pmod m,$$
$$a - b \equiv a' - b' \pmod m,$$
$$a \cdot b \equiv a' \cdot b' \pmod m.$$

Beweis. Nach Voraussetzung gibt es $x, y \in \mathbb{Z}$ mit $a - a' = xm$ und $b - b' = ym$. Dann rechnen wir

$$(a+b) - (a'+b') = a + b - a' - b' = (a - a') + (b - b') = xm + ym = (x+y)m,$$
$$(a-b) - (a'-b') = a - b - a' + b' = (a - a') - (b - b') = xm - ym = (x-y)m,$$
$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') = xmb + a'ym = (xb + a'y)m.$$

Dies zeigt die Behauptung. □

Beispiel 11.16. Modulo 12 (oder 24) kennen wir bereits seit dem Zeitpunkt, da wir gelernt haben mit Uhrzeiten umzugehen. Rechnungen mit Stunden und Uhrzeiten auf der (klassischen Zeiger-)Uhr zu vollen Stunden sind Rechnungen modulo 12. Zeitangaben am Tag sind Rechungen modulo 24.

Wenn wir um 11 Uhr in San Francisco mit dem Auto in Richtung New York losfahren und dafür 45 Stunden brauchen, dann ist es bei Ankunft $11 + 45 = 56$ Uhr. Nun, das müssen wir modulo 24 betrachten, und da ist das $56 \equiv 8 \pmod{24}$. Es ist also eine Ankunft gegen morgen (des überübernächsten Tages) zu erwarten. Das kann man auch ausrechnen, indem man zuerst die 45 wegen $45 \equiv -3$ modulo 24 durch -3 ersetzt und dann $11 + 45 \equiv 11 + (-3) \equiv 8$ beachtet, was aufgrund der kleineren Zahlen leichter zu rechnen ist.

Beispiel 11.17. Welchen Wochentag hat derselbe Kalendertag in 12 Jahren? In dieser Zeit wird es 4 Schalttage geben, und damit vergehen $12 \cdot 365 + 4$ Tage. Das interessiert uns modulo 7. Also rechnen wir

$$12 \cdot 365 + 4 \equiv (-2) \cdot 1 + 4 \equiv 2 \pmod{7}.$$

Es wird also derselbe Wochentag sein wie übermorgen.

11.5. **Teilbarkeitsregeln und Proben.**

Satz 11.18. *Sei $m \geq 1$. Sei $n \in \mathbb{N}_0$ und seien $a, b \in \mathbb{Z}$ mit $a \equiv b \pmod{m}$. Dann gilt*

$$a^n \equiv b^n \pmod{m}.$$

(Hier gilt $0^0 = 1$.)

Beweis. Das beweisen wir per Induktion nach n. Der Anfang $n = 0$ ist leicht, denn $a^0 = 1$ ist sogar gleich $b^0 = 1$ (und hier brauchen wir die Konvention $0^0 = 1$).

Der Induktionsschritt von n auf $n+1$. Die Induktionsannahme besagt $a^n \equiv b^n \pmod{m}$. Und dann gilt nach Satz 11.15

$$a^{n+1} \equiv a^n \cdot a \overset{\text{IA}}{\equiv} b^n \cdot a \equiv b^n \cdot b \equiv b^{n+1} \pmod{m}.$$

Das war zu zeigen. □

Beispiel 11.19. Es gilt für alle $k \geq 0$

$$10^k \equiv 1^k \equiv 1 \pmod{9}.$$

Daher gilt für eine beliebige natürliche Zahl $n = (a_k a_{k-1} \dots a_2 a_1 a_0)_{10}$ im Zehnersystem

$$n \equiv a_k \cdot 10^k + \dots + a_1 \cdot 10 + a_0 \equiv a_k \cdot 1 + \dots + a_1 \cdot 1 + a_0 \equiv Q(n) \pmod{9}.$$

Hier bezeichnet $Q(n)$ wie in Definition 5.14 die Quersumme von n im Zehnersystem. Diese Rechnung zeigt nochmals die Teilbarkeitsregel durch 9:

$$9 \mid n \iff n \equiv 0 \pmod{9} \iff Q(n) \equiv 0 \pmod{9} \iff 9 \mid Q(n).$$

Allerdings gibt die Rechnung viel mehr: es gilt sogar $n \equiv Q(n) \pmod{9}$, also bestimmt die Quersumme (oder die iterierte Quersumme) den Rest bei Division durch 9, und nicht nur den Fall, wenn dieser Rest gleich 0 ist.

Bemerkung 11.20. Die folgenden „Proben“ sind **kein** Nachweis der Korrektheit sondern nur Tests, die manche fehler erkennen können. Aber eben nicht alle Fehler.

(1) Satz 11.15 ist die Basis für die 9**er-Probe**. Eine Rechnung mit Addition, Subtraktion und Multiplikation mit natürlichen Zahlen muß auch modulo 9 stimmen. Man berechnet also für jeden Summanden und Faktor den 9er-Rest durch iteriertes Quersummenbilden. Sodann berechnet man für diese Reste den vorgegebenen Ausdruck aus Addition, Subtraktion und Multiplikation. Dabei darf man in jedem Zwischenschritt wieder durch iteriertes Quersummenbilden den 9er-Rest bestimmen. Zum Schluß vergleicht man das Ergebnis der Rechnung mit den 9er-Resten mit dem 9er-Rest der Rechnung mit den

ursprünglichen Zahlen. Da muß dann dasselbe rauskommen, ansonsten hat man sich verrechnet. Ein Beispiel:

$$1234567 \cdot 7654321 = 9449872114007 \ ?$$

kann nicht stimmen, denn $Q(1234567) = Q(7654321) = 28$ und $28 \equiv 1 \pmod 9$, während $Q(9449872114007) = 56$ und $56 \equiv 2 \pmod 9$. Aber $1 \cdot 1 \not\equiv 2 \pmod 9$.

(2) Analog zur 9er-Probe gibt es die schnellere 10er-Probe. Hier schaut man nur auf die Einerziffer, denn

$$(a_k a_{k-1} \dots a_2 a_1 a_0)_{10} \equiv a_0 \pmod{10}.$$

Eine Rechnungen mit Addition, Subtraktion und Multiplikation mit natürlichen Zahlen muss auch modulo 10 stimmen. Man ersetzt jede Zahl durch ihre Einerziffer, und vereinfacht auch jedes Zwischenergebnis auf diese Art und Weise. Das Ergebnis muss mit dem Ergebnis dieser Rechnung mit den Einerziffern die gleiche Einerziffer haben. Ein Beispiel:

$$1234567 \cdot 7654321 = 9449872114006 \ ?$$

kann nicht stimmen, weil $7 \cdot 1 \not\equiv 6$ modulo 10.

Die 9er-Probe ist sensibler in Bezug auf Flüchtigkeitsfehler, weil alle Ziffern miteinbezogen werden. Die 10er-Probe benutzt nur die Einerziffer.

(3) Analog zu obigem entspricht die Rechnen mit gerade und ungerade der 2er-Probe. Man spricht auch von der Kontrolle der Parität.

Definition 11.21. Die **alternierende Quersumme** im Zehnersystem einer natürlichen Zahl $n = (a_k a_{k-1} \dots a_2 a_1 a_0)_{10}$ ist definiert als

$$A(n) := a_0 - a_1 + a_2 - a_3 + a_4 - \dots + (-1)^k a_k.$$

Beispiel 11.22. Die alternierende Quersumme von 12345678 ist $8 - 7 + 6 - 5 + 4 - 3 + 2 - 1 = 4$.

Satz 11.23 (Teilbarkeitsregel durch 11)**.** *Sei n eine natürliche Zahl. Es gilt*

$$n \equiv A(n) \pmod{11}.$$

Insbesondere ist n genau dann durch 11 teilbar, wenn $A(n)$ durch 11 teilbar ist.

Beweis. Es gilt für alle $k \geq 0$ nach Satz 11.18 wegen $10 \equiv -1 \pmod{11}$

$$10^k \equiv (-1)^k \pmod{11}.$$

Damit gilt für eine beliebige natürliche Zahl $n = (a_k a_{k-1} \dots a_2 a_1 a_0)_{10}$ im Zehnersystem

$$n \equiv a_k \cdot 10^k + \dots + a_1 \cdot 10 + a_0 \equiv a_k \cdot (-1)^k + \dots - a_1 \cdot 1 + a_0 \equiv A(n) \pmod{11}. \qquad \square$$

Beispiel 11.24. Die 12345674 ist durch 11 teilbar, denn die alternierende Quersumme ist $4 - 7 + 6 - 5 + 4 - 3 + 2 - 1 = 0$.

11.6. **Gleichungen mit Kongruenzen.** Man kann nun auch einfach lineare Gleichungen von Kongruenzen lösen.

⚠ Weil man beim Teilen aufpassen muss, gelingt das nicht immer. Aber unter genau verstandenen Bedingungen kann man sich mit einem Trick behelffen, indem man Teilen durch Multiplizieren ersetzt.

Wir machen einfach ein paar Beispiele mit wachsender Komplexität.

Bemerkung 11.25. Dividieren ist bei Kongruenzen mamchmal problematisch. So folgt aus $2x \equiv 6 \pmod{12}$ nicht notwendigerweise $x \equiv 3 \pmod{12}$, denn $x \equiv 9$ erfüllt auch

$$2 \cdot 9 \equiv 18 \equiv 6 \pmod{12}.$$

Beispiel 11.26. Eine einfache lineare Kongrunezgleichung. Für welche $x \in \mathbb{Z}$ gilt:

$$x + 17 \equiv 2 \pmod 7.$$

Nun, wir addieren auf beiden Seiten $-17 \equiv 4 \pmod 7$ und erhalten

$$x \equiv 6 \pmod 7.$$

Die Lösungen bestehen daher in der Elementen der Äquivalenzklasse $[6]_7$ modulo 7, als Teilmenge von $\mathbb{Z}$ beschrieben durch

$$[6]_7 = \{7n + 6 \ ; \ n \in \mathbb{Z}\} = \{\ldots -8, -1, 6, 13, \ldots\}.$$

Die letzte Beschreibung mit ... ist nicht wirklich gut verständlich.

Beispiel 11.27. Für welche $x \in \mathbb{Z}$ gilt:

$$3x + 17 \equiv 2 \pmod{13}.$$

Nun, wir addieren auf beiden Seiten $-17 \equiv 9 \pmod{13}$ und erhalten

$$3x \equiv 11 \pmod{13}.$$

Nun müssen wir durch 3 teilen. Das können wir nicht. Aber wir können mit 9 multiplizieren. Warum? Weil dann aus den $3x$ ein $27x$ wird und $27 \equiv 1 \pmod{13}$, also $27x \equiv x \pmod{13}$ wird. Auf der rechten Seite bekommen wir $11 \cdot 9 \equiv (-2) \cdot (-4) \equiv 8 \pmod{13}$, zusammen

$$x \equiv 8 \pmod{13}.$$

⚠ Vorsicht! Dies ist mit diesem Argumentationsstand nur notwendig für eine Lösung.

Ob es auch hinreichend ist, müssen wir klären. Was ist das Problem? Wir haben einen Schritt in unserer Lösungsstrategie, den wir nicht so ohne weiteres umkehren können: Das Multiplizieren mit 9. Die Umkehrung wäre das Dividieren durch 9 und das ist unklar. Warum haben wir mit 9 multipliziert? Weil wir durch 3 dividieren wollten. Das lag an $3 \cdot 9 \equiv 1 \pmod{13}$. Damit ist nun Multiplizieren mit 3 dasjenige, was den richtigen Effekt hat und das Dividieren durch 9 imitiert. Diese Argumentation zeigt, dass in der Tat $x \equiv 8 \pmod{13}$ die Lösungen beschreibt. Wir können aber auch die Probe machen:

$$3 \cdot 8 + 17 \equiv 24 + 17 \equiv -2 + 4 \equiv 2 \pmod{13},$$

stimmt! Die Lösung besteht daher aus der Äquivalenzklasse $[8]_{13}$ modulo 13, als Teilmenge von $\mathbb{Z}$ beschrieben durch

$$[8]_{13} = \{13n + 8 \ ; \ n \in \mathbb{Z}\}.$$

Bemerkung 11.28. Wenn der Modulus m eine Primzahl ist, dann klappt es immer, einen Faktor zu finden, mit dem man das Dividieren durch ein $a \not\equiv 0 \pmod m$ ersetzen kann mit Multiplizieren mit b modulo m. Man muß nur ein b finden mit $ab \equiv 1 \pmod m$, und das geht dann immer!

Beispiel 11.29. Jetzt betrachten wir ein lineares Gleichungssystem modulo 5.

$$\begin{cases} \text{(I)} & 3x + 2y \equiv 17, \\ \text{(II)} & 7x - 4y \equiv 14. \end{cases}$$

Wir wollen y loswerden. Dazu multiplizieren wir (I) mit 2 und addieren dies zu (II). Das kann man auch rückgängig machen, also liefert dies eine Äquivalenzumformung. Wir erhalten

$$\begin{cases} \text{(I')} & 3x + 2y \equiv 2, \\ \text{(II')} & 3x \qquad \equiv 3. \end{cases}$$

Jetzt multiplizieren wir die Gleichung (II') mit 2. Das kann man durch Mulitplikation mit 3 auch rückgängig machen, also wieder eine Äquivalenzumformung.

$$\begin{cases} \text{(I')} & 3x + 2y \equiv 2, \\ \text{(II')} & x \qquad\quad \equiv 1. \end{cases}$$

Wir setzen $x \equiv 1$ in die erste Gleichung ein und subtrahieren 3 auf beiden Seiten. Dann folgt

$$\begin{cases} \text{(I'')} & 2y \equiv 4, \\ \text{(II'')} & x \equiv 1. \end{cases}$$

Die erste Gleichung lösen wir nach y auf, indem wir mit 3 multiplizieren. Nun lesen wir ab, dass die Lösung für (x, y) aus

$$(x, y) \in [1]_5 \times [2]_5$$

besteht. Jetzt überlegen wir uns kurz, dass wir wirklich immer Äquivalenzumformungen gemacht haben, oder wir machen die Probe.

$$\begin{cases} \text{(I)} & 3 \cdot 1 + 2 \cdot 2 \equiv 17, \\ \text{(II)} & 7 \cdot 1 - 4 \cdot 2 \equiv 14. \end{cases}$$

Beispiel 11.30. Was passiert, wenn wir dividieren müssen, aber nicht können? Ein Beispiel. Für welche $x \in \mathbb{Z}$ gilt:

$$6x \equiv 2 \pmod 8.$$

Vielfache von 6 sind immer gerade und daher nie 1 modulo 8, was ungerade wäre. Aber die 3 in $6 = 2 \cdot 3$ bekommen wir weg. Multiplizieren wir als erstes mit 3, wegen $3 \cdot 3 \equiv 1 \pmod 8$. Dann erhalten wir wegen $18 \equiv 2 \pmod 8$

$$2x \equiv 6 \pmod 8.$$

Das schreiben wir als $8 \mid 2x - 6 = 2(x - 3)$. Wir brauchen einen Faktor 8 und einen Faktor 2 sehen wir schon. Fehlt noch ein Faktor 4. Und in der Tat kann man sich überlegen, dass gilt:

$$2x \equiv 6 \pmod 8 \iff 8 \mid 2(x-3) \iff 4 \mid x - 3 \iff x \equiv 3 \pmod 4.$$

Beim Teilen hat sich hier nun der Modulus von 8 auf 4 verändert! Genauer gehen wir auf diese Problematik hier nicht ein.

Beispiel 11.31. Zum Schluß besprechen wir eine einfache quadratische Gleichung.

$$x^2 \equiv -1 \pmod 5.$$

Hier können wir nicht mit der p/q-Formel und Wurzeln arbeiten. Wie geht es sonst?

- Die erste Möglichkeit ist billig: durchprobieren! Es gibt gar nicht so viele verschiedene Restklassen modulo 5, und das Ergebnis von x^2 hängt ja nur von der Restklasse modulo 5 ab, in der x liegt. Machen wir also eine Tabelle, alles modulo 5:

x	0	1	2	3	4
x^2	0	1	−1	−1	1

  Wir sehen also, dass die Lösungen aus den $x \in [2]_5 \cup [3]_5$ bestehen.
- Die zweite Methode erfordert ein wenig Wissen aus dem späteren Kapitel über Primzahlen, und dass der Modulus eine Primzahl ist. Wir formen um (alles modulo 5):

$$\begin{aligned} & x^2 \equiv -1 \\ \iff \quad & x^2 - 4 \equiv 0 \\ \iff \quad & (x-2)(x+2) \equiv 0 \end{aligned}$$

  Die letzte Gleichung bedeutet, dass unser x

$$5 \mid (x-2)(x+2)$$

erfüllen muß. Weil 5 eine Primzahl ist, muß 5 nun ein Teiler eines der Faktoren sein! Also

$$x - 2 \equiv 0 \pmod 5 \qquad \text{oder} \qquad x + 2 \equiv 0 \pmod 5.$$

Das führt zu den Lösungen

$$x \in [2]_5 \cup [-2]_5,$$

was das gleiche ist wie oben, weil $3 \equiv -2$ modulo 5.

11.7. **Rechnen mit Kongruenzklassen.**

Satz 11.32. *Sei $m \geq 1$. Auf der Menge der Kongruenzklassen modulo m, die wir mit*

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1_m]\}$$

bezeichnen, ist die Addition durch

$$[a]_m + [b]_m := [a+b]_m$$

und die Multiplikation durch

$$[a]_m \cdot [b]_m := [a \cdot b]_m$$

wohldefiniert

Beweis. Wenn $[a]_m = [a']_m$ und $[b]_m = [b']_m$ ist, dann müssen wir $[a+b]_m = [a'+b']_m$ und $[ab]_m = [a'b']_m$ nachweisen. Sei $a - a' = mx$ und $b - b' = my$. Dann folgt

$$(a+b) - (a'+b') = (a-a') + (b-b') = mx + my = m(x+y).$$

Also ist $a + b \equiv a' + b' \pmod m$.

Weiter gilt

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b' = amy + mxb' = (ay + xb')m.$$

Also gilt auch $ab \equiv a'b' \pmod m$. □

Bemerkung 11.33. Die Summe (bzw. das Produkt) der Reste bei Division durch m von a und b hat den selben Rest modulo m wie die Summe $a+b$ (bzw. das Produkt ab). Das beschreibt eine mögliche notwendige (aber nicht hinreichende) Kontrolle für Rechnungen in ganzen Zahlen.

Satz 11.34. *Addition und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ sind assoziativ, kommutativ und distributiv. Die $0 := [0]_m$ ist ein neutrales Element für die Addition, die $1 := [1]_m$ ist ein neutrales Element für die Multiplikation. Außerdem hat jedes $[a]_m$ die Klasse $[-a]_m$ als additives Inverses.*

Beweis. Diese Rechenregeln erbt das Rechnen mit Kongruenzen/Kongruenzklassen sofort vom Rechnen in $\mathbb{Z}$. □

Bemerkung 11.35. Man kann Kongruenzklassen auch subtrahiere, denn

$$[a]_m - [b]_m := [a]_m + [-1]_m[b]_m = [a + (-1)b]_m = [a-b]_m.$$

11.8. **Stellenwertsysteme zu einer anderen Basis als** 10**.**

⚠ Anstatt zur Basis 10 kann man natürliche Zahlen auch in einem Stellenwertsystem zu anderen Basen schreiben. Beispielsweise benutzt ein Computer Binärzahlen, das ist zur Basis 2, bei dem nur die Ziffern 0 (kein Strom) oder 1 (Strom) benötigt werden.

Man trifft im Informatikbereich auch auf das Hexadezimalsystem, also zur Basis 16. Dort werden als Ziffern die

$$\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$$

verwendet. Man muß sich nur zu helfen wissen, wenn die üblichen Ziffern ausgehen.

Wir beschreiben nun die Darstellung zu einer beliebigen Basis $b \geq 2$.

Definition 11.36. Sei $b \geq 2$ eine natürliche Zahl. Die **„Ziffern" im Stellenwertsystem zur Basis** b sind die natürlichen Zahlen $0, 1, 2, \ldots, b-1$. Mit dem Symbol

$$(a_k a_{k-1} \ldots a_1 a_0)_b$$

für Ziffern $a_0, \ldots, a_k$ beschreiben wir die natürliche Zahl

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \ldots + a_1 \cdot b^1 + a_0 \cdot b^0.$$

Satz 11.37. *Sei $b \geq 2$. Jede natürliche Zahl hat eine eindeutige Darstellung als Zahl im Stellenwertsystem zur Basis b.*

Beweis. Wir zeigen zuerst, dass jede Zahl eine Darstellung im Stellenwertsystem zur Basis b hat. Der Beweis erklärt auch, wie man die Darstellung bekommt. Das beweisen wir per Induktion.

Induktionsanfang: Wenn $n = 0$ ist, dann haben wir einfach $n = (0)_b$. Fertig.

Induktionsschritt: Wir nehmen an, für alle Zahlen $< n$ haben wir bereits eine Darstellung. Wir teilen n durch b mit Rest, und zwar als

$$n = m \cdot b + a_0$$

mit $0 \leq a_0 < b$. Dann ist $m < n$ eine natürliche Zahl, die daher per Induktionsvoraussetzung eine Dartstellung hat. Diese sei

$$m = (a_k a_{k-1} \ldots a_1)_b = a_k \cdot b^{k-1} + a_{k-1} \cdot b^{k-2} + \ldots + a_1 \cdot b^0.$$

Wir haben den Indizes absichtlich von 1 bis k laufen lassen, wie sich geleich erweisen wird. Jetzt berechnen wir n:

$$\begin{aligned} n =& m \cdot b + a_0 = b \cdot (a_k a_{k-1} \ldots a_1)_b + a_0 \\ &= (a_k a_{k-1} \ldots a_1 0)_b + a_0 \\ &= (a_k a_{k-1} \ldots a_1 a_0)_b. \end{aligned}$$

Im letzten Schritt ist wichtig, dass $0 \leq a_0 < b$ ist, damit wir a_0 als Ziffer benutzen können. Dies zeigt die Existenz.

Für die Eindeutigkeit überlegt man sich, dass

$$(a_k a_{k-1} \ldots a_1 a_0)_b \equiv a_0 \pmod{b},$$

und dass a_0 der eindeutige Rest bei Division durch b ist. Damit ist die Einerstelle eindeutig. Die kann man dann abziehen, durch b teilen und sodann mit der nun an die Einerstelle getretenen b-Stelle weiterverfahren. Und so weiter per Induktion nach der Anzahl der Stellen. (Beweis ausbaufähig). □

Bemerkung 11.38. So wie man algorithmisch mit Zahlen im Zehnersystem addieren, subtrahieren und multiplizieren kann, so kann man das analog auch mit Zahlen in anderen Stellenwertsystemen.

Wir schauen uns nun eine Teilbarkeitsregel an, welche mit der Quersumme als Summe der Ziffern in der Darstellung im Stellenwertsystem zur Basis b arbeitet.

Satz 11.39. *Sei $b \geq 2$. Für $n = (a_k a_{k-1} \ldots a_1 a_0)_b$ gilt*

$$n \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod{b-1}.$$

Beweis. Das funktioniert genauso wie bei der Diskussion der Quersumme im Zehnersystem bezüglich modulo 9. Weil $b \equiv 1 \pmod{b-1}$ ist, folgt nach Satz 11.18

$$\begin{aligned} n &\equiv a_k \cdot b^k + \ldots + a_1 \cdot b^1 + a_0 \cdot b^0 \\ &\equiv a_k \cdot 1^k + \ldots + a_1 \cdot 1^1 + a_0 \cdot 1^0 \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod{b-1}. \end{aligned}$$

□

11.9. **Märchenstunde: Zählen mit Binärzahlen.** Video aus der Sendung mit der Maus

11.10. **Märchenstunde: p-adische Zahlen.** Diskussion der Darstellung von -1 zur Basis p.

$$\begin{aligned} -1 &= -p + (p-1) = -p^2 + (p-1)p + (p-1) = \dots \\ &= -p^{k+1} + (p-1)p^k + (p-1)p^{k-1} + \dots + (p-1)p + (p-1). \end{aligned}$$

Jetzt betrachten wir den p-adischen Limes. Das bedeutet, dass wir p^k als immer kleiner betrachten, je größer k wird, und im Limes wird es zu 0. Dann wird aus -1 für zum Beispiel $p = 7$

$$-1 = (\dots 666666666)_7$$

mit unendlich vielen Ziffern vor dem Komma. Im p-adischen geht alles in die umgekehrte Richtung: man erlaubt unendlich viele Stellen vor dem Komma, aber nur endlich viele nach dem Komma.

11.11. **Märchenstunde: RSA.** Das RSA-Verfahren zur Verschlüsselung wurde in den 1970er Jahren von Rivest, Shamir und Adleman entwickelt.

⚠ Das RSA-Verfahren gehört zur **Public Key Kryptographie**. Die tatsächlich auf Ihren digitalen Geräten für die Sicherheit von z.B, online banking verantwortlichen Algorithmen sind mit RSA verwandt.

Von Public Key Kryptographie spricht man bei Protokollen zur Nachrichtenübermittlung, bei denen die benötigten Schlüssel zur Verschlüsselung öffentlich ist, aber keine in vernünftiger Zeit brauchbaren Hinweise die geheimen zur Entschlüsselung nötigen Schlüssel verrät. Jeder Teilnehmer, der gerne Post bekommen möchte, hängt seinen persönlichen Verschlüsselungsmechanismus an eine öffentliche Pinnwand. Dort muß man nachsehen, wenn man verschlüsselte Post verschicken möchte. Hat man die Post erst einmal verschlüsselt, kann man als Absender auch nicht mehr Korrektur lesen. Das kann nur noch der Empfänger.

Insbesondere werden bei Kommunikation mit Public Key Protokollen zwischen zwei Parteien für jede Richtung ein eigener Schlüssel benutzt. Es ist jeweils nur dem Empfänger bekannt, wie die Nachrichten zu entschlüsseln sind.

Definition 11.40 (RSA-Verschlüsselung)**.** Wir beschreiben nun, wie Alice eine RSA-codierte Nachricht an Bob übermittelt.

- Der Empfänger Bob macht für alle, die ihm eine Nachricht schicken wollen, einen öffentlichen Schlüssel verfügbar: das sind bei RSA
  (i) ein Modulus n, genannt der **RSA-Modul**, und
  (ii) ein **Verschlüsselungsexponent** e (von *encrypt*, engl. für *verschlüsseln*).
  Dabei gilt, und das ist nicht öffentlich,
  $$n = pq$$
  ist Produkt zweier Primzahlen $p \neq q$, und e ist teilerfremd zu $(p-1)(q-1)$.
- Alice codiert ihren Text auf einfache Weise als Ziffernfolge, z.B. durch eine öffentliche umkehrbare Funktion von Buchstaben zu Zahlen $1, \dots, 26$ (bei Sonderzeichen entsprechend mehr). Dann unterteilt sie die Ziffernfolge in Blöcke, so dass der maximal mögliche Wert in einem Block $< n$ ist. Diese Ziffernfolge mit Blockstruktur nennen wir den **Klartext**.
  Sei B ein Block des Klartextes. Dann übermittelt Alice den Wert C, bestimmt als
  $$C \equiv B^e \pmod{n}$$
  und zwar den eindeutigen Repräsentanten $0 \leq C < n$. Die Ziffernfolge der C-Blöcke nennen wir den **Geheimtext**.
- Der Geheimtext kommt bei Bob an, der in der Zwischenzeit nicht untätig war. Aus der Kenntnis der Faktorisierung $n = pq$ kann Bob den **Entschlüsselungsexponenten** d

(von *decrypt*, engl. für *entschlüsseln*), mit dem für alle B gilt (Satz von Euler–Fermat):

$$B^{de} \equiv B \pmod{n}.$$

Wie genau Bob das macht, erklären wir hier nicht.

- Auf die Geheimtextblöcke C wendet Bob nun

$$B' \equiv C^d \pmod{n}$$

an und bestimmt dabei wieder für B' den Repräsentanten im Bereich $0 \leq B' < n$.

- Es folgt unmittelbar, dass

$$B' \equiv C^d \equiv (B^d)^e \equiv B^{de} \equiv B \pmod{n}$$

ist. Damit gilt aufgrund der Wahl der minimal nicht-negativen Repräsentanten:

$$B' = B,$$

und Bob kann seine Nachricht lesen, nachdem er die Ziffern wieder durch Buchstaben ersetzt hat.

Take home message Kapitel §11.

- Konguenz modulo m.
- Rechnen mit Kongruenzen.
- Die (iterierte) Quersumme liefert den Rest bei Division durch 9, und 9er-Probe.
- Teilbarkeit durch 11.
- Stellenwertsystem bezüglich einer Basis $b \geq 2$. Binärsystem.

12. Arithmetik der ganze Zahlen

Quellen: [GK23] Kapitel 7.1, 7.2 und 8, [SchSt18] Kapitel 2.1

12.1. Der größte gemeinsame Teiler.

Definition 12.1. Der **größte gemeinsame Teiler (ggT)** von $a, b \in \mathbb{Z}$, geschrieben $\mathrm{ggT}(a,b)$, ist die größte natürliche Zahl in der Menge der gemeinsamen Teiler

$$\{t \in \mathbb{Z} \ ; \ t \mid a \text{ und } t \mid b\}$$

von a und von b. Mit einer Ausnahme: wenn $a = b = 0$, dann definieren wir $\mathrm{ggT}(0,0) := 0$.

Allgemeiner ist für ganze Zahlen $a_1, \dots, a_n \in \mathbb{Z}$ der größte gemeinsame Teiler, geschrieben $\mathrm{ggT}(a_1, \dots, a_n)$, die größte natürliche Zahl in der Menge

$$\{t \in \mathbb{Z} \ ; \ t \mid a_i \text{ für alle } i = 1, \dots, n\}$$

der gemeinsamen Teiler. Wenn alle $a_i = 0$ sind, definieren wir den ggT als 0.

Bemerkung 12.2. Der größte gemeinsame Teiler ist wohldefiniert. Für jede ganze Zahl $a \neq 0$ ist die Menge der Teiler von a eine endliche Menge

$$\{t \in \mathbb{Z} \ ; \ t \mid a\}.$$

Damit ist auch die Menge der gemeinsamen Teiler von a und b als Schnittmenge

$$T := \{t \in \mathbb{Z} \ ; \ t \mid a \text{ und } t \mid b\} = \{t \in \mathbb{Z} \ ; \ t \mid a\} \cap \{t \in \mathbb{Z} \ ; \ t \mid b\}$$

eine endliche Menge (sofern nicht $a = 0$ und $b = 0$). Die Menge T der gemeinsamen Teiler ist auch nicht leer, denn sie enthält 1, und damit besitzt T auch ein Maximum.

Beispiel 12.3. Es gilt $\mathrm{ggT}(26, 91) = 13$. Weiter haben wir $\mathrm{ggT}(100, -1001) = 1$, und als Beispiel mit einer der Zahlen 0: $\mathrm{ggT}(0, 17) = 17$.

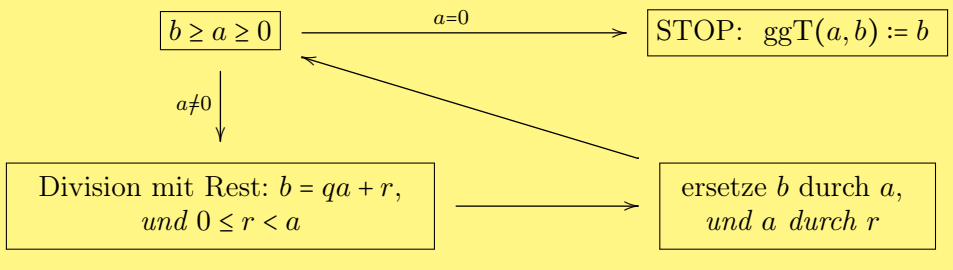
Bemerkung 12.4. Es gilt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(-a,b) = \mathrm{ggT}(-a,-b) = \mathrm{ggT}(a,-b) = \mathrm{ggT}(b,a).$$

12.2. Euklidischer Algorithmus.

⚠ Zur Bestimmung des ggT gibt es einen unglaublich effektiven Algorithmus, bei dem zur Überraschung kein einziger Teiler bestimmt werden muß.

Satz 12.5 (Euklidischer Algorithmus)**.** *Seien $b \geq a \geq 0$ und $b \neq 0$ natürliche Zahlen. Dann berechnet der folgende Algorithmus den größten gemeinsamen Teiler* $\mathrm{ggT}(a,b)$*:*



Bemerkung 12.6. Der euklidische Algorithmus ist schnell und man braucht die Primfaktorzerlegung der beteiligten Zahlen nicht zu kennen!

Beispiel 12.7. Bevor wir das beweisen, führen wir ein Beispiel durch. Wir wollen den ggT von 156 und −100 bestimmen. Dann ist $a = 100$ (das Vorzeichen ist für den ggT egal) und $b = 156$ (damit die Anordnung nach Größe stimmt). Und dann berechnen wir der Reihe nach

$$\begin{aligned} b = 156 &= 1 \cdot 100 + 56 \\ a = 100 &= 1 \cdot 56 + 44 \\ 56 &= 1 \cdot 44 + 12 \\ 44 &= 3 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \\ 4 & \end{aligned}$$

und damit ist der $\mathrm{ggT}(156, -100) = 4$. Die Divisionen mit Rest in den jeweiligen Zeilen kann man immer erst mit einer Zeile Verzögerung durchführen, weil man ja die Zahl braucht, durch die man teilen soll.

Beweis. Der Algorithmus ist **wohldefiniert**, denn Division mit Rest führt zu $0 \le r < a$, so dass die neuen Werte für a, b wieder die Annahme $b \ge a \ge 0$ erfüllen.

Der Algorithmus **terminiert**, denn im Iterationsschritt gilt $a > r \ge 0$. Die neue kleiner Zahl r ist also kleiner also die alte kleinere Zahl a. Da es nur endlich viele natürliche Zahlen unterhalb einer gegebenen gibt, muß nach endlich vielen Schritten die Abbruchbedingung $a = 0$ des Algorithmus erreicht werden.

Der Algorithmus ist **korrekt**, das heißt, er berechnet, was er zu berechnen vorgibt. Das müssen wir nun genauer beweisen. Dazu zeigen wir zwei Dinge:

(1) Bei jedem Schritt, wenn mit $b = qa + r$ das Paar (b, a) durch das Paar (a, r) ersetzt wird, bleibt der ggT erhalten:
$$\mathrm{ggT}(a, b) = \mathrm{ggT}(r, a).$$
(2) Wenn der Algorithmus stoppt, bei $a = 0$, dann gibt der Algortihmus von diesem letzten Paar $(0, b)$ den ggT korrekt an:
$$\mathrm{ggT}(0, b) = b.$$

Punkt (2): Wenn $a = 0$ ist, dann teilt jede natürliche Zahl a. Die gemeinsamen Teiler von b und 0 sind also genau die Teiler von b. Davon ist b der größte. Also stimmt (2).

Punkt (1) formulieren wir als eigenständiges Lemma 12.9. Damit sind wir fertig. □

Bemerkung 12.8. Der Beweis von Satz 12.5 ist eigentlich ein Induktionsbeweis. Das haben wir nur ein wenig versteckt. Versuchen Sie den Beweis als Induktionsbeweis mit Induktion nach a zu formulieren.

Lemma 12.9. *Seien $q, r, a \in \mathbb{Z}$. Dann gilt*
$$\mathrm{ggT}(a, qa + r) = \mathrm{ggT}(r, a).$$

Beweis. Wir zeigen, dass die gemeinsamen Teiler von a und r dieselben sind, wie die gemeinsamen Teiler von a und $qa + r$. Sobald wir das wissen, stimmen die größten unter den gemeinsamen Teilern dann auch überein.

Also wollen wir zeigen:
$$t \mid a \text{ und } t \mid r \iff t \mid a \text{ und } t \mid qa + r.$$
Dazu fixieren wir $t > 0$ und rechnen modulo t. Dann haben wir modulo t zu zeigen:
$$a \equiv 0 \text{ und } r \equiv 0 \iff a \equiv 0 \text{ und } qa + r \equiv 0.$$

Die Teilaussage $a \equiv 0$ kommt auf beiden Seiten vor. Die folgt jeweils automatisch, wenn wir beide Einzelrichtungen beweisen.

„$\Longrightarrow$“: aus $a \equiv 0$ und $r \equiv 0$ folgt sofort

$$qa + r \equiv q \cdot 0 + 0 \equiv 0.$$

„$\Longleftarrow$“: aus $a \equiv 0$ und $qa + r \equiv 0$ folgt sofort

$$r \equiv q \cdot 0 + r \equiv q \cdot a + r \equiv 0. \qquad \square$$

Bemerkung 12.10. In Lemma 12.9 verlangen wir nicht, dass $b = qa + r$ die Division von b durch a mit Rest r ist. Einzig die Beziehung $b = qa + r$ ist wichtig. Das bedeutet, dass der euklidische Algorithmus auch läuft, wenn man nicht vollständig mit Rest teilt. Genausowenig verlangt Lemma 12.9, dass die beteiligten Zahlen positiv sind. Man kann auch mit negativen Zahlen arbeiten, und dann für den ggT das Vorzeichen wieder vergessen. Das erlaubt nützliche, die Komplexität reduzierende Zwischenschritte. Ein Beispiel:

$$\begin{aligned}
\operatorname{ggT}(30031260, 1001) &= \operatorname{ggT}(1260, 1001) \\
&= \operatorname{ggT}(259, 1001) \\
&= \operatorname{ggT}(35, 259) \\
&= \operatorname{ggT}(14, 35) \\
&= \operatorname{ggT}(7, 14) = 7.
\end{aligned}
\qquad
\begin{aligned}
30031260 - 3000 \cdot 1001 &= 1260, \\
1260 - 1 \cdot 1001 &= 259, \\
1001 - 4 \cdot 259 &= -35, \\
259 - 7 \cdot 35 &= 14, \\
35 - 2 \cdot 14 &= 7,
\end{aligned}$$

Lemma 12.11 (Lemma von Bézout[a]). *Seien $a, b \in \mathbb{Z}$ ganze Zahlen. Dann gibt es $x, y \in \mathbb{Z}$ mit*

$$\operatorname{ggT}(a, b) = xa + yb.$$

[a] Étienne Bézout (1730–1783), französischer Mathematiker.

Beweis. Wir dürfen $a, b \geq 0$ annehmen. Ansonsten ersetzen wir zum Beispiel a durch $-a$ und x durch $-x$. Außerdem können wir a und b vertauschen (und dann x mit y). Das führt auf oBdA $b \geq a \geq 0$. Jetzt beweisen wir das Lemma per Induktion nach a.

Induktionsanfang: Wenn $a = 0$ ist, dann ist $\operatorname{ggT}(b, 0) = b$ und mit $x = 0$ und $y = 1$ haben wir

$$\operatorname{ggT}(b, 0) = 0 \cdot 0 + 1 \cdot b.$$

Induktionsschritt: Wir nehmen an, dass für alle Paare (b', a') mit $a' < a$ die Aussage des Lemmas bereits richtig ist. Seien $q.r$ mit $b = qa + r$ und $0 \leq r < a$. Für a und r ist $a > r \geq 0$ und somit gilt die Aussage des Lemma für a und r. Es gibt somit x' und y' mit

$$\operatorname{ggT}(a, r) = x'r + y'a.$$

Nach Lemma 12.9 folgt

$$\operatorname{ggT}(a, b) = \operatorname{ggT}(a, r) = x'r + y'a = x'(b - qa) + y'a = (y' - qx')a + x'b.$$

Wir setzen $x = y' - qx'$ und $y = x'$. Dann haben wir die Aussage des Lemma von Bézout für a, b und damit den Induktionsschritt bewiesen. $\square$

Bemerkung 12.12. Die Zahlen x, y aus den Lemma von Bézout mit $\operatorname{ggT}(a, b) = xa + yb$ kann man parallel im Euklidischen Algorithmus mitberechnen. Das ist nicht schwer, aber ein wenig verwickelter als der euklidische Algorithmus. Daher machen wir das hier nicht.

Beispiel 12.13. In Sikinien gibt es nur zwei Geldmünzen, eine hat den Wert von 28 Sikinischen Pfund und die andere den Wert von 15 Sikinischen Pfund. Kann man jeden ganzzahligen Betrag von Skinischen Pfund mit diesen Münzen bezahlen? Mit herausgeben, natürlich.

Der ggT von 28 und 15 berechnet sich nach dem euklidischen Algorithmus zu

$$28,\ 15,\ 28-15=13,\ 15-13=2,\ 13-6\cdot 2=1,\ 2-2\cdot 1=0,$$

also 1. Nach dem Lemma von Bézout gibt es $x,y\in\mathbb{Z}$ mit $1=28x+15y$. Ein konkretes Beispiel ist

$$1=28\cdot 7+15\cdot(-13).$$

Damit kann man 1 Sikinisches Pfund bezahlen: man gibt 7 von den Münzen mit Wert 28 und bekommt 13 von denen mit Wert 15 heraus. Wenn man 3 Pfund bezahlen will, dann macht man das 3mal. Oder allgemeiner n-mal für den Wert n Pfund. Es geht also immer.

Korollar 12.14. *Seien $a,b\in\mathbb{Z}$ ganze Zahlen. Dann sind die gemeinsamen Teiler von a und b genau die Teiler von* $\mathrm{ggT}(a,b)$.

Beweis. Wir kürzen ab $d=\mathrm{ggT}(a,b)$. Die Aussage ist eine gdw.-Aussage. Also müssen wir zwei Richtungen zeigen. Die erste folgt aus der Transitivität von „teilen“. Wenn $t\in\mathbb{Z}$ ein Teiler von d ist, dann folgt wegen $d\mid a$ auch $t\mid a$. Und analog aus $t\mid d$ und $d\mid b$ auch $t\mid b$. Das zeigt die erste Richtung.

Jetzt müssen wir noch zeigen, dass ein gemeinsamer Teiler $t\in\mathbb{Z}$ von a und b ein Teiler von d ist. Sei also $a=tu$ und $b=tv$ mit $u,v\in\mathbb{Z}$. Aus Lemma 12.11 erhalten wir $x,y\in\mathbb{Z}$ mit $d=xa+yb$. Dann folgt

$$d=xa+yb=x(tu)+y(tv)=t\cdot(xu+yv).$$

Also ist t ein Teiler von d, und das beendet den Beweis. □

12.3. **Fundamentalsatz der Arithmetik.**

Proposition 12.15. *Sei $n\in\mathbb{N}_0$, $n\geq 2$. Dann gibt es eine Primzahl p, die n teilt.*

Beweis. Das zeigen wir per Induktion. Der Induktionsanfang ist diesmal $n=2$. Dann teilt $p=2$.

Induktionsschritt: Wir nehmen an, dass für alle natürlichen Zahlen kleiner als n bereits ein Primteiler nachgewiesen wurde. Wenn n selbst Primzahl ist, dann ist $p=n$ und teilt n. In dem Fall sind wir sind fertig. Andernfalls ist n keine Primzahl. Dann gibt es eine Faktorisierung $n=ab$ mit $2\leq a,b<n$. Die Induktionsvoraussetzung trifft daher auf a zu. Es gibt also eine Primzahl p mit $p\mid a$. Sei $x\in\mathbb{N}_0$ mit $a=px$. Dann folgt $n=ab=(xb)p$, folglich $p\mid n$. Das zeigt die Induktionsbehauptung. □

Satz 12.16 (Existenz der Primfaktorzerlegung)**.** *Sei $n\in\mathbb{N}_0$, $n\geq 1$. Dann gibt es $t\geq 0$ und Primzahlen $p_1,\ldots,p_t$ mit*

$$n=p_1\cdot\ldots\cdot p_t.$$

Der Fall $t=0$ führt zum leeren Produkt mit dem Wert 1. Dies ist die Primfaktorzerlegung von $n=1$.

Beweis. Das beweisen wir wieder per Induktion. Der Induktionsanfang $n=1$ führt zu $t=0$ und keinem Primfaktor.

Induktionsschritt: Wir nehmen an, dass für alle natürlichen Zahlen kleiner als n bereits eine Primfakttorzerlegung gefunden ist. Wenn n selbst Primzahl ist, dann ist $t=1$ und $p_1=n$ eine Primfaktorzerlegung. In dem Fall sind wir sind fertig. Andernfalls ist n keine Primzahl. Dann gibt es einen Primteiler $p\mid n$, weil $n\geq 2$ und mit Proposition 12.15. Sei $n=p\cdot m$. Dann ist $1\leq m<n$ und per Induktionsannahme hat m eine Primfaktorzerlegung. Seien $p_2,\ldots,p_t$ Primzahlen mit

$$m=p_2\cdot\ldots\cdot p_t.$$

Mit $p_1=p$ folgt dann

$$n=p_1\cdot m=p_1\cdot p_2\cdot\ldots\cdot p_t,$$

und das ist eine Primfaktorzerlegung von n. □

Lemma 12.17 (Lemma von Euklid)**.** *Sei p ein Primteiler eines Produkts ab von natürlichen Zahlen a und b. Dann ist p ein Teiler von a oder ein Teiler von b.*

Beweis. Wir zeigen: wenn $p \mid ab$ und $p \nmid a$, dann gilt $p \mid b$. Das ist logisch äquivalent zur Behauptung des Lemmas.

Es gilt $\mathrm{ggT}(p, a)$ ist 1 oder p, denn es ist ja ein Teiler von p und eine Primzahl hat nur diese zwei Teiler. Weil $p \nmid a$ gilt, scheidet $\mathrm{ggT}(p, a) = p$ aus. Also ist $\mathrm{ggT}(p, a) = 1$. Nach dem Lemma von Bézout, Lemma 12.11, gibt es $x, y \in \mathbb{Z}$ mit $1 = px + ay$. Sei ferner $ab = pz$. Dann gilt

$$b = b \cdot 1 = b \cdot (px + ay) = p(bx) + (ab)y = p(bx) + (pz)y = p(bx) + p(zy) = p(bx + zy).$$

Das zeigt $p \mid b$, wie behauptet. □

Korollar 12.18. *Teilt eine Primzahl p ein Produkt $a_1 \cdot \ldots a_t$ von natürlichen Zahlen $a_i \in \mathbb{N}_0$, dann gibt es einen Faktor, der von p geteilt wird: es gibt ein i, so dass p ein Teiler von a_i ist.*

Beweis. Per Induktion nach der Anzahl der Faktoren. □

Theorem 12.19 (Fundamentalsatz der Arithmetik)**.** *Jede natüurliche Zahl $n \geq 1$ ist auf eindeutige Weise ein Produkt von Primzahlen, bis auf die Reihenfolge der Faktoren.*

Beweis. Die Exisatenz haben wir in Satz 12.16 bereits beweisen.

Die behauptete Eindeutigkeit ist die folgende Aussage. Wenn $p_1, \ldots, p_s$ und $q_1, \ldots, q_t$ Primzahlen sind und

$$p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_t$$

gilt, dann haben wir $s = t$ und nach geeignetem Umnummerieren und Vertauschen der Reihenfolge der Faktoren des Produkts ist $p_i = q_i$ für alle $1 \leq i \leq s$.

Diese Aussage beweisen wir per Induktion nach der Anzahl $s + t$ der Faktoren auf beiden Seiten zusammen.

Induktionsverankerung $s + t = 0$: Dann haben wir die leeren Produkte auf beiden Seiten, das heißt $s = t = 0$ und keine Primzahlen. Das ist ok.

Induktionsannahme: Sei die Aussage bewiesen für alle $s' + t' < n$ und Gleichungen von Primzahlprodukten der Länge s' mit Primzahlprodukten der Länge t'.

Induktionsschritt: Wir nehmen nun eine solche Gleichung mit $s + t = n$ vielen Faktoren. Dabei ist $n \geq 1$. Sei oBdA $s > 0$. Dann teilt p_s die linke Seite, also auch die rechte. Weil p_s Primzahl ist, folgt aus Lemma von Euklid, dass p_s einen der Faktoren der rechten Seite teilt, insbesondere ist $t > 0$. Wir sortieren um, und nehmen daher oBdA an, es sei der letzte q_t. Weil q_t Primzahl ist, geht das nur, wenn $p_s = 1$ oder $p_s = q_t$. Ersteres scheidet aus, weil als Primzahl $p_s \geq 2$. Also ist $p_s = q_t$. Dann können wir kürzen und erhalten

$$p_1 \cdot \ldots \cdot p_{s-1} = q_1 \cdot \ldots \cdot q_{t-1}.$$

Das ist jetzt der Vergleich von zwei Faktorisierungen mit Gesamtanzahl von Faktoren $(s-1) + (t-1) = (s+t) - 2 = n - 2$. Also weniger als n. Hier schlägt die Induktionnsannahme zu und zeigt $s - 1 = t - 1$ und nach eventuellem Umsortieren $p_i = q_i$ für alle $1 \leq i \leq s - 1$. Das zeigt aber bereits alles, denn es gilt dann $s = t$ und das fehlende $p_s = q_t = q_s$ haben wir ja bereits. □

Bemerkung 12.20. Die Eindeutigkeit der Primfaktorzerlegung ist nicht offensichtlich. In der algebraischen Zahlentheorie lernt man sinnvoll mit Zahlen der Form $a + b\sqrt{-5}$ und $a, b \in \mathbb{Z}$ zu rechnen. Und dann hat die 6 zwei Primfaktorzerlegungen:

$$2 \cdot 3 = 6 = 1 - (-5) = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

nach der dritten binomischen Formel.

12.4. **Kleinstes gemeinsames Vielfaches.** In die im Vergleich zum ggT entgegengesetzte Richtung bewegt sich das kleinste gemeinsame Vielfache.

Definition 12.21. Das **kleinste gemeinsame Vielfache (kgV)** ganzer Zahlen $a, b \neq 0$ ist die natürliche Zahl

$$\mathrm{kgV}(a,b) = \min\{T \in \mathbb{Z} \; ; \; T > 0 \text{ und } a \mid T \text{ und } b \mid T\}.$$

Allgemeiner ist für $a_1, \ldots, a_n \in \mathbb{Z}$, alle $a_i \neq 0$, das kleinste gemeinsame Vielfache

$$\mathrm{kgV}(a_1, \ldots, a_n) = \min\{T \in \mathbb{Z} \; ; \; T > 0 \text{ und } a_i \mid T \text{ für alle } i = 1, \ldots, n\}.$$

Proposition 12.22. *Seien $a, b > 0$ natürliche Zahlen. Dann gilt*

$$ab = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b).$$

Beweisskzze. Das folgt aus der eindeutigen Primfaktorzerlegung. Eine Primzahl p komme mit genau r-vielen Faktoren in der Primfaktorisierung von a und mit s-vielen Faktoren in der Primfaktorisierung von b vor. Dann kommen in der Primfaktorzerlegung des $\mathrm{ggT}(a,b)$ genau $\min\{r,s\}$-viele Faktoren p und in der von $\mathrm{kgV}(a,b)$ genau $\max\{r,s\}$-vielen Faktoren p auf. Weil $r + s = \min\{r,s\} + \max\{r,s\}$ gilt, folgt die Behauptung. □

Bemerkung 12.23. Das kgV braucht man, um ökonomisch Brüche zu addieren. Der beste Hauptnenner ist der kgV der Nenner der zu addierenden Brüche. Weil man den ggT mit dem euklidischen Algorithmus gut bestimmen kann, folgt aus der obigen Proposition nun auch eine Methode, den Hauptnenner effektiv zu bestimmen.

12.5. **Einige irrationale Zahlen.** Wir betrachten ein Quadrat mit Kantenlännge 1 Sikinischer Meter, das blaue Quadrat in Abbildung 6. Auf der Diagonale des blauen Quadrats bauen wir ein Quadrat mit der Kantenlänge x Sikinische Meter, der Länge der Diagonalen, auf.

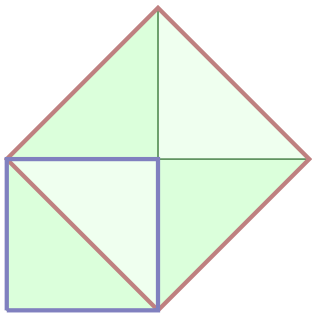


Abbildung 6. Die Verdopplung des Quadrats

Anhand der ein in der Abbildung hervorgehobenen Zerlegung in gleich große Dreiecke, können wir die Flächen der beiden Quadrate vergleichen. Zusammen mit der Formel für die Fläche eines Quadrats ergibt sich

$$x^2 = 2.$$

Aus geometrischen Gründen muß es also eine Zahl geben, deren Quadrat 2 ergibt. Wir nennen diese hypothetische Zahl $\sqrt{2}$, Wurzel aus 2.

Satz 12.24. *In den rationalen Zahlen $\mathbb{Q}$ gibt es $\sqrt{2}$ nicht: es gibt keine rationale Zahl $\frac{a}{b}$ mit*

$$\left(\frac{a}{b}\right)^2 = 2.$$

Beweis. Wir nehmen an, as gibt $a, b \in \mathbb{Z}$, $b \neq 0$ und $\frac{a}{b} = \sqrt{2}$. Dann folgt

$$2 = (\sqrt{2})^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}.$$

Wir multiplizieren mit b^2 und erhalten die Gleichung

$$a^2 = 2b^2$$

zwichen ganzen Zahlen. Die Quadrate a^2 und b^2 sind sogar natürliche Zahlen. Weil $b \neq 0$, und weil ein eventuelles Vorzeichen von a und b bei a^2 und b^2 keine Rolle spielt, dürfen wir annehmen, dass a, b natürliche Zahlen > 0 sind.

Dann hat a eine Primfaktorzerlegung. Aus dieser berechnet sich die Primfaktorzerlegung des Quadrats a^2 wegen der Eindeutigkeit der Primfaktorzerlegung: Jeder Primfaktor kommt in a^2 zweimal sooft wie in a vor. Das bedeutet, dass jeder Primfaktor von a^2 gerade oft vorkommt. Dasselbe gilt für b.

Jetzt zählen wir, wie oft der Primfaktor 2 in $a^2 = 2b^2$ vorkommt. Auf der linken Seite gerade oft. Auf der rechten Seite in b^2 gerade oft, aber im zusätzlichen Fakltor 2 noch 1 mal, also insgesamt ungerade oft. Das ist ein Widerspruch zur eindeutigen Primfaktorzerlegung, denn in der natürlichen Zahl $a^2 = 2b^2$ kann es nur eines geben, entweder eine gerade oder eine ungerade Anzahl von Faktoren 2 in der Primfaktorzerlegung. Das ist der gesuchte Widerspruch. □

Bemerkung 12.25. Jetzt haben wir eine fundamentale Einsicht[9] der griechischen Mathematik der Antike angetroffen. Die alten Griechen dachten geometrisch, verstanden aber auch ganze und rationale Zahlen ausreichend gut, um zu sehen, dass diese nicht ausreichen, um alle in der Geometrie anzutreffenden Größenverhältnisse als Zahl behandlen zu können. Die $\sqrt{2}$ is nicht rational, damit gibt es $\sqrt{2}$ in der antiken griechischen Mathematik nicht, obwohl es natürlich Quadrate und deren Diagonalen, somit das Längenverhältnis $\sqrt{2}$ gibt.

⚠ Es gibt nur einen Ausweg: man muß weitere Zahlen konstruieren! Brüche sind nicht genug. Die Zahl $\sqrt{2}$ ist keine rationale Zahl und muss erst noch konstruiert werden, um Zahl zu sein.

Die reellen Zahlen lösen diese Mißgeschick auf. Dazu braucht es aber einen Grenzwertbegriff, der erst eine Erfindung der Neuzeit ist (auch wenn er intuitiv bei Archimedes bereits vorhanden sein muss).

Bemerkung 12.26. Was ist der Kern des Arguments im Beweis von Satz 12.24? Für welche Zahlen funktioniert das Argument auch? Wie steht es mit

$$\sqrt[3]{17},$$

derjenigen Zahl x mit $x^3 = 17$?

Bemerkung 12.27. Auch kompliziertere Ausdrücke wie $x = \sqrt{2} + \sqrt{5}$ sind manchmal als nicht rational zu enlarven. Angenommen, x wäre rational. Dann ist auch x^2 rational, also

$$x^2 = 2 + 2\sqrt{10} + 5.$$

Mit x^2 ist aber auch $(x^2 - 7)/2$ rational, und das ist

$$\frac{x^2 - 7}{2} = \sqrt{10}.$$

Ab hier geht es weiter wie im Beweis von Satz 12.24 zum angestrebten Widerspruch. also ist $x = \sqrt{2} + \sqrt{5}$ nicht rational.

[9] Früher wurde diese Erkenntnis als Krise der griechischen Mathematik beschrieben, was sie nach neueren Erkenntnissen wohl nicht war.

12.6. **Bonus.** Der folgende Satz beleuchtet die Erkenntnis über rationale Zahlen aus der in Abschnitt §10.5 diskutierten Frage, welche Dezimalzahlen den rationalen Zahlen entsprechen.

Satz 12.28. *Jede rationale Zahl wird durch einen Bruch der Form*

$$\frac{z}{10^k \cdot (10^\ell - 1)}$$

dargestellt.

Beweis. Sei $\frac{a}{b}$ eine beliebige rationale Zahl. Wir dürfen annehmen, dass $b > 0$ ist. Dann können wir aus der Primfaktorzerlegung von b die Faktoren 2, die Faktoren 5 und alle anderen Faktoren zusammenfassen:

$$b = 2^x \cdot 5^y \cdot c$$

mit $x, y \in \mathbb{N}_0$ und $c > 0$ eine natürliche Zahl ohne Primteiler 2 und 5. Insbesondere ist

$$\operatorname{ggT}(10, c) = 1,$$

denn es muss ein Teiler von 10 sein, also eine der Zahlen $1, 2, 5, 10$, und davon teilt nach Konstruktion von c nur 1 die Zahl c. Nach dem Lemma von Bézout, Lemma 12.11, gibt es $u, v \in \mathbb{Z}$ mit

$$1 = 10u + cv.$$

Das schreiben wir als Kongruenz:

$$1 \equiv 10u \pmod{c}.$$

Jetzt schauen wir uns die Potenzen von 10 modulo c an. Die Menge $\{10^n \,;\, n \in \mathbb{N}_0\}$ ist unendlich, aber es gibt nur c-viele verschiedene Reste modulo c. Demnacht muss es zwei Zahlen $r < s$ geben mit

$$10^r \equiv 10^s \pmod{c}.$$

Wir bringen alles auf eine Seite und klammern aus:

$$0 \equiv 10^r \cdot (10^{s-r} - 1) \pmod{c}.$$

Jetzt setzen wir $\ell = s - r$, und multiplizieren mit u^r. Dann erhalten wir

$$0 \equiv u^r \cdot 10^r \cdot (10^\ell - 1) \equiv (10u)^r \cdot (10^\ell - 1) \equiv 1^r \cdot (10^\ell - 1) \equiv 1 \cdot (10^\ell - 1) \equiv (10^\ell - 1) \pmod{c}.$$

Das bedeutet, dass c ein Teiler von $10^\ell - 1$ ist, sagen wir $cd = 10^\ell - 1$.

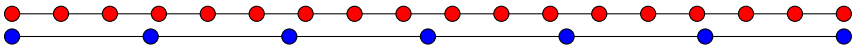
Jetzt setzen wir $k = x + y$ und finden nach Erweitern mit $2^y \cdot 5^x \cdot d$:

$$\frac{a}{b} = \frac{a}{2^x \cdot 5^y \cdot c} = \frac{a \cdot 2^y \cdot 5^x \cdot d}{2^{x+y} \cdot 5^{x+y} \cdot cd} = \frac{a \cdot 2^y \cdot 5^x \cdot d}{10^k \cdot (10^\ell - 1)},$$

was mit $z = a \cdot 2^y \cdot 5^x \cdot d$ die Behauptung beweist. □

12.7. **Märchenstunde: rechnende Zikaden.**

Die Population der Zikade *Magicicada septendecim* (USA) hat einen Primzahlrhythmus. Die Zikade verbringt 17 Jahre im Larvenstadium, um für nur wenige Wochen als adulte Zikade aufzutreten. Das bietet der Population als ganzes einen wichtigen Schutz. Die Freßfeinde der Zikade haben z.B. einen 6-jährigen Rhythmus. Haben sich in einem Jahr mit vielen Zikaden die Freßfeinde satt gefressen und entsprechend viele Nachkommen produziert, kommen 6 Jahre später eine große Population von Freßfeinden, die aber auf wenige Zikaden stoßen. Weil 6 und 17 teilerfremd sind (das ist der Vorteil der 17 als Primzahl: alles < 17 ist dazu teilerfemd), dauert es $6 \cdot 17 = 102$ Jahre(!), bis sich die Populationen von Zikaden und Freßfeinden wieder „treffen“. Die Zikade hungert also ihre Freßfeinde aus!



Freßfeinde (rot): alle 6 Jahre. Zikade (blau): alle 17 Jahre.

ABBILDUNG 7. (Martin Hauser/ Wikipedia)

Take home message Kapitel §12.

- Definition von ggT und kgV
- Der euklidische Algorithmus: schnell, einfach, effektiv zur Berechnung des ggT
- Fundamentalsatz der Arithmetik: Existenz und Eindeutigkeit der Primfaktorzerlegung für $n \in \mathbb{N}$
- Das Verhältnis von Diagonale zur Kantenlänge in einem Quadrat ist keine rationale Zahl. Die rationalen Zahlen $\mathbb{Q}$ sind nicht genug!

13. Abbildungen

Quellen: [GK23] Kapitel 3, [SchSt18] Kapitel 4.3

13.1. **Motivation: ganzen Zahlen als Teilmenge der rationalen Zahlen?** Die ganzen Zahlen sollten eine Teilmenge der rationalen Zahlen sein. Schließlich soll $\mathbb{Q}$ den Rechenbereich $\mathbb{Z}$ sinnvoll ausbauen (so dass alle Divisionen durch Zahlen ungelich 0 möglich werden). Formal ist aber eine rationale Zahl eine Äquivalenzklasse von Paaren ganzer Zahlen, und damit eine ganze Zahl niemals eine rationale Zahl. Wir brauchen eine Methode, wie wir die Elemente von $\mathbb{Z}$ mit gewissen Elementen von $\mathbb{Q}$ vergleichen können. Es sollte

$$n \mapsto \frac{n}{1}$$

in Beziehung zueinander stehen.

13.2. **Abbildungen.**

⚠ Mengen sind statisch. Sie werden lebendig, indem man Beziehungen zwischen Mengen durch Abbildungen herstellt.

Definition 13.1. Eine **Abbildung** von einer Menge A, dem **Definitionsbereich**, in eine Menge B, dem **Wertebereich**, ist eine Teilmenge (genannt **Graph** der Abbildung)

$$F \subseteq A \times B$$

mit der Eigenschaft

$$\text{für alle } a \in A \text{ gibt es genau ein } b \in B\colon\ (a,b) \in F.$$

Wir schreiben eine Abbildung als

$$F\colon A \to B$$

und schreiben

$$F(\alpha) = \beta,$$

wenn $(\alpha,\beta) \in F$ gilt. Wenn F aus dem Kontext klar ist, dann schreiben wir für $F(\alpha) = \beta$

$$\alpha \mapsto \beta.$$

Das Element $\alpha \in A$ aus dem Definitionsbereich nennt man **Argument**, das $F(\alpha) \in B$ aus dem Wertebereich nennt man **Wert**, oder **Bild** von α.

Bemerkung 13.2. Es gibt verschiedene Möglichkeiten, sich eine Abbildung $F\colon A \to B$ vorzustellen.

(1) Als Wertetabelle: wir notieren der Reihe nach für jedes $\alpha \in A$, das zugehörige $F(\alpha) \in B$. Eine Abbildung

$$F\colon \{🐟, ⚡, ✉, ☎\} \to \{0,1\}$$

ist vollständig erfaßt, ja dadurch definiert, dass man angibt:

α	🐟	⚡	✉	☎
$F(\alpha)$	0	1	1	1

(2) Durch den Graph der Abbildung: Das klappt am besten für Abbildungen $F\colon A \to B$, wenn man $A \subseteq \mathbb{R}$ und $B \subseteq \mathbb{R}$ Teilmengen der reellen Zahlen sind. Dann ist

$$F \subseteq A \times B \subseteq \mathbb{R} \times \mathbb{R}$$

ein Teil der Ebene, indem man den Punkt $(x,y) \in A \times B$ als Punkt mit den cartesischen Koordinaten (x,y) auffaßt.

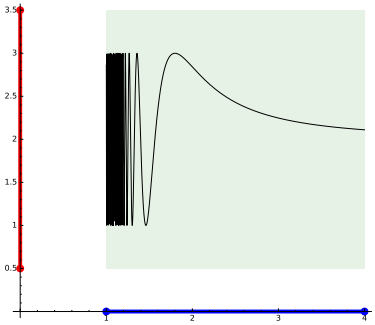


ABBILDUNG 8. Graph von $S : \{a \in \mathbb{R}\ ; 1 < a \leq 4\} \to \{b \in \mathbb{R}\ ;\ 0.5 \leq b \leq 3.5\}$ mit $S(x) = 2 + \sin(1/(x-1)^2)$.

(3) Gesamtheit aller Beziehungen zwischen Argument und Wert.
(Definitionsbereich A und Wertebereich B der Abbildung $F : A \to B$ als Mengen mit Elementen. Für jede Beziehung $F(a) = b$ einen Pfeil vom Element a nach $F(a)$.)

Beispiel 13.3. Ein paar arithmetische Abbildungen.

(1) Abschnittsweise definierte Abbildung: zum Beispiel die **Parität**

$$P : \mathbb{N}_0 \to \{0, 1\}$$
$$P(n) = \begin{cases} 0 & \text{falls } n \text{ gerade,} \\ 1 & \text{falls } n \text{ ungerade.} \end{cases}$$

(2) Die Addition natürlicher Zahlen ist eine Abbildung

$$+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0,$$
$$(a, b) \mapsto a + b.$$

(3) Wir fixieren ein $m \in \mathbb{N}_0$ mit $m \geq 1$. Dann gibt es die Abbildung, die einer natürlichen Zahl seinen Rest bei Division durch m zuordnet. Wir definieren

$$\mathbb{Z}/m\mathbb{Z} := \{0, 1, 2, 3, \ldots, m-1\}$$

als Menge der möglichen Reste. Die Abbildung „**Rest modulo** m“ ist (der Name R_m ist kein Standard!)

$$R_m : \mathbb{N}_0 \to \mathbb{Z}/m\mathbb{Z} := \{0, 1, 2, 3, \ldots, m-1\}.$$

mit $R_m(n) = r$ wenn es $q, r \in \mathbb{N}_0$ gibt mit $n = qm + r$ und $0 \leq r < m$.

- Zahlenbeispiel $R_5(17) = 2$.
- Die Parität $P : \mathbb{N}_0 \to \{0, 1\}$ ist identisch mit R_2.

Beispiel 13.4. Geometrische und kombinatorische Beispiele.

(1) Symmetrien eines geometrischen Objekts kann man als Abbildungen der Objekte als Punktmengen betrachten.
(2) Ein digitales Bild ist eine Abbildung von der Menge der Pixel des Bildes auf die Menge der digital definierten Farben.
(3) Im Schach gibt es viele, aber trotzdem nur endlich viele mögliche Stellungen. Diese Menge nennen wir hier einmal C. Dann ist also eine Schachstellung S ein Element $S \in C$. Ein legaler Zug bewegt die Stellung S in eine andere Stellung. Die Menge der aus der Stellung S heraus legalen Züge ist also eine Teilmenge von C. Nennen wir diese Teilmenge $L(S)$. Als Teilmenge ist $L(S)$ ein Element der Potenmenge von C. Damit ist die Abbildung „Legale Züge“ definiert:

$$L : C \to \mathscr{P}(C), \qquad S \mapsto L(S).$$

(4) An der Goethe Universität gibt es eine Menge F von Studienfächern und eine Menge S von Studierenden. Jede/r Studierende hat möglicherweise im eingeschriebenen Studiengang (oder mehreren gelichzeitig) mehr als ein Studienfach. Die zu mensch $M \in S$ gehörenden Studienfächer sind daher eine Teilmenge von F, nennen wir sie $f(M)$. Das definiert eine Abbildung

$$f: S \to \mathscr{P}(F), \qquad M \mapsto f(M).$$

Beispiel 13.5. Sei $F : A \to B$ eine Abbildung. Dann definiert

$$x \sim_F y :\iff F(x) = F(y)$$

auf A eine Äquivalenzrelation.

13.2.1. *Funktionen.* Manchmal wird der Begriff **Funktion** synonym mit dem Begriff der Abbildung verwendet. Wir verwenden den Begriff Funktion als einen speziellen Namen für Abbildungen mit Wertebereich in eine Sorte von Zahlen.

Beispiel 13.6. Bewertungsfunktion: Google pagerank für das Sortieren der Suchtreffer.
Schach: Stellungsbewertung.

13.2.2. *Ein Beispiel: Ungerichtete Graphen.*

Definition 13.7. Sei X Menge und $k \in \mathbb{N}_0$. Dann bezeichne $\binom{X}{k}$ die Menge der k-elementigen Teilmengen von X.

Am Beispiel des Begriffs eines Graphen zeigen wir auf, wie man in der Mengensprache kompliziertere mathematische Objekte präzise definieren kann.

Definition 13.8. Ein **(ungerichteter) Graph (ohne Schleifen)** ist ein Tripel (E, K, ∂), wobei

(i) E die Menge der Ecken des Graphen ist,
(ii) K die Menge der Kanten des Graphen ist, und
(iii) $\partial : K \to \binom{E}{2}$ die Abbildung ist, die einer Kante $k \in K$ das ungeordnete Paar $\partial k \subseteq E$ seiner Ränder zuordnet, welches zwei verschiedene Ecken sind.

Beispiel 13.9. Der Graph, welcher dem Haus vom Nikolaus zugrunde liegt, hat Ecken $E = \{A, B, C, D, F\}$ und Kanten $K = \{u, l, r, o, d, e, f, g\}$ mit $\partial : K \to \binom{E}{2}$ gegeben durch

α	u	l	r	o	d	e	f	g
$\partial(\alpha)$	$\{A,B\}$	$\{A,D\}$	$\{B,C\}$	$\{C,D\}$	$\{D,F\}$	$\{C,F\}$	$\{A,C\}$	$\{B,D\}$.

Das Dach ist z.B. durch die Ecken DFC mit den Kanten d und e beschrieben.

13.3. **Eigenschaften von Abbildungen.**

Definition 13.10. Sei $F : A \to B$ eine Abbildung.

(1) Das **Bild** von F ist die mit $F(A)$ bezeichnete Teilmenge von B definiert durch

$$F(A) := \{b \in B \ ; \ \text{ es gibt } a \in A \text{ mit } b = F(a)\} = \{F(a) \ ; \ a \in A\}.$$

Das ist die Teilmenge der angenommenen Werte von f.

(2) Sei $U \subseteq B$ eine Teilmenge. Das **Urbild** von U unter F ist die Teilmenge von A mit Bezeichnung $F^{-1}(U)$ definiert durch

$$F^{-1}(U) := \{a \in A \ ; \ F(a) \in U\}.$$

Das umfaßt diejenigen Elemente aus dem Definitionsbereich, die von der Abbildung F nach U abgebildet werden.

(3) Sei $x \in B$ ein Element. Das **Urbild** von x unter F, bezeichnet mit $F^{-1}(x)$, ist das Urbild der Teilmenge $\{x\} \subseteq B$, also
$$F^{-1}(x) = \{a \in A \; ; \; F(a) = x\}.$$

Definition 13.11. Sei $F\colon A \to B$ eine Abbildung von Mengen.

(1) Wir sagen F ist **injektiv**, wenn jedes Element von B höchstens ein Mal als Bild vorkommt:
$$\forall a_1, a_2 \in A: \quad F(a_1) = F(a_2) \implies a_1 = a_2.$$
Eine injektive Abbildung wird **Injektion** genannt.

(2) Wir sagen F ist **surjektiv**, wenn jedes Element von B mindestens ein Mal als Bild vorkommt:
$$\forall b \in B : \exists a \in A : F(a) = b,$$
oder kürzer $F(A) = B$. Eine surjektive Abbildung wird **Surjektion** genannt.

(3) Wir sagen F ist **bijektiv**, wenn jedes Element von B genau ein Mal als Bild vorkommt:
$$\forall b \in B : \exists^! a \in A : \; F(a) = b.$$
Eine bijektive Abbildung wird **Bijektion** genannt.

Bemerkung 13.12. Eine Abbildung $F : A \to B$ ist

(1) genau dann injektiv, wenn für alle $x \in B$ die Urbildmenge $F^{-1}(x)$ aus höchstens einem Element besteht.
Life of Brian: „Jeder nur ein Kreuz“ (nur ein im Sinne von höchstens ein).

(2) genau dann surjektiv, wenn für alle $x \in B$ die Urbildmenge $F^{-1}(x)$ aus mindestens einem Element besteht.
Life of Brian, Variante: „Jeder mindestens ein Kreuz“.

(3) genau dann bijektiv, wenn für alle $x \in B$ die Urbildmenge $F^{-1}(x)$ aus genau einem Element besteht.
Life of Brian, Variante: „Jeder genau ein Kreuz“.

In der Beschreibung über die Kreuze ist gedacht, dass ein $x \in B$ kommt und sich entweder höchstens, mindestens oder genau ein Urbild (Kreuz) nehmen soll.

Satz 13.13. *Eine Abbildung $F : A \to B$ ist genau dann bijektiv, wenn sie injektiv und surjektiv ist.*

Beweis. Das folgt sofort aus der Bemerkung 13.12, weil „aus höchstens einem“ und „aus mindestens einem“ äquivalent zu „aus genau einem“ ist. □

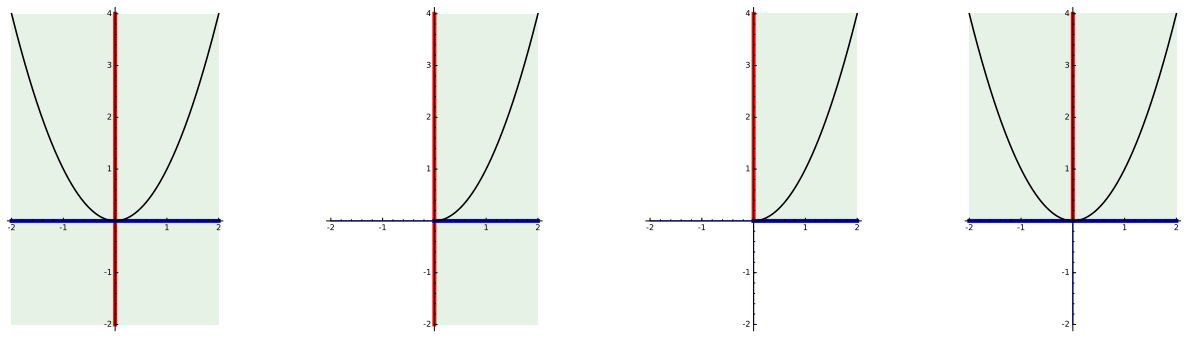
Bemerkung 13.14. Die Begriffe injektiv, surjektiv und bijektiv haben alle geometrische Beschreibungen als Eigenschaften der zugehörigen Graphen.

Beispiel 13.15.

(1) Für zwei Mengen X, Y ist die Projektion $\mathrm{pr}_1\colon X \times Y \to X$ auf den ersten Faktor definiert durch
$$\mathrm{pr}_1((a, b)) = a$$
für alle $a \in X$ und $b \in Y$. Wenn $Y \neq \varnothing$ gilt, dann ist die Projektion surjektiv.

(2) Die Multiplikationsabbildung $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ definiert durch $(x, y) \mapsto xy$ ist surjektiv.

(3) Die Abbildung $\mathbb{R} \to \mathbb{R}$ definiert durch $x \mapsto x^2$ ist weder injektiv noch surjektiv.



(a) $\mathbb{R} \to \mathbb{R}$ (b) $\mathbb{R}_{\geq 0} \to \mathbb{R}$ (c) $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ (d) $\mathbb{R} \to \mathbb{R}_{\geq 0}$

ABBILDUNG 9. Graph von $x \mapsto x^2$ mit verschiedenen Defintions- und Wertebereichen.

(4) Die Abbildung $\mathbb{R}_{\geq 0} \to \mathbb{R}$ definiert durch $x \mapsto x^2$ ist injektiv aber nicht surjektiv.
(5) Die Abbildung $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ definiert durch $x \mapsto x^2$ ist sowohl injektiv als auch surjektiv.
(6) Die Abbildung $\mathbb{R} \to \mathbb{R}_{\geq 0}$ definiert durch $x \mapsto x^2$ ist surjektiv aber nicht injektiv.

Die letzten vier Beispiele zeigen die Relevanz des Definitions- (blau) und des Wertebereichs (rot) für das Verhalten einer Abbildung.

Beispiel 13.16. Jede Menge hat eine ausgezeichnete Abbildung, die **Identität**, welche jedes Element auf sich selbst abbildet. Für eine Menge X ist das die Abbildung

$$\mathrm{id}_X : X \to X, \qquad \mathrm{id}_X(a) = a \text{ für alle } a \in X.$$

13.3.1. *Komposition und Umkehrfunktion.*

Definition 13.17. Die **Komposition** (oder **Hintereinanderausführung** oder **Verkettung**) zweier Abbildungen $G : A \to B$ und $F : X \to Y$ ist genau dann definiert, wenn $B = X$ gilt, und zwar dann als Abbildung mit der Bezeichnung und Definition

$$F \circ G : A \to Y$$
$$(F \circ G)(a) = F(G(a)) \text{ für alle } a \in A.$$

Übungsaufgabe 13.1. Wie bekommt man den Graphen $F \circ G \subseteq A \times Y$ aus den Graphen $G \subseteq A \times B$ und $F \subseteq B \times Y$?

Tipp: betrachten Sie $A \times B \times Y$ und die verschiedenen Projektionen durch weglassen einer Koordinate. Sodann nehmen Sie Urbilder und Bilder bekannter Teilmengen.

Bemerkung 13.18.

⚠ Bei der Komposition von Abbildungen kommt es auf die Reihenfolge an!

Zum ersten kann man im allgemeinen die Komposition gar nicht in beiden Reihenfolgen durchführen, denn die erste Bedingung ist ja, dass der Wertebereich der zuerstdurchgeführten Abbildung der Definitionsbereich der als zweites durchgeführten Abbildung sein muß.

Wenn $G : A \to B$ und $F : B \to A$ die Abbildungen sind, die dadurch in beide Richtungen komponierbar sind, dann sind die Kompositionen Abbildungen

$$F \circ G : A \to A$$
$$G \circ F : B \to B.$$

Wenn $A \neq B$, dann sind die Kompositionen Abbildungen zwischen verschiedenen Mengen! Sie können gar nicht gleich sein.

Und auch wenn $A = B$ ist, gitl im allgemeinen $F \circ G \neq G \circ F$. Ein konkretes Beispiel: die Abbildungen

$$F : \mathbb{R} \to \mathbb{R}, \qquad F(x) = x^2,$$
$$G : \mathbb{R} \to \mathbb{R}, \qquad G(x) = x + 1,$$

haben die Kompositionen

$$F \circ G : \mathbb{R} \to \mathbb{R}, \qquad F \circ G(x) = F(G(x)) = F(x+1) = (x+1)^2,$$
$$G \circ F : \mathbb{R} \to \mathbb{R}, \qquad G \circ F(x) = G(F(x) = G(x^2) = x^2 + 1.$$

Proposition 13.19. *Die komposition mit der Identität ändert die Abbildung nicht: sei $F : A \to B$ eine Abbildung. Dann ist*

$$F \circ \mathrm{id}_A = F,$$
$$\mathrm{id}_B \circ F = F.$$

Beweis. Das folgt sofort aus der Definition. Für alle Elemente $x \in A$ gilt

$$F \circ \mathrm{id}_A(x) = F(\mathrm{id}_A(x)) = F(x),$$

weil $\mathrm{id}_A(x) = x$, und, mit der entsprechenden Eigenschaft von id_B folgt

$$\mathrm{id}_B \circ F(x) = \mathrm{id}_B(F(x)) = F(x).$$

□

Proposition 13.20. *Komposition ist assoziativ. Für komponierbare Abbildungen*

$$A \xrightarrow{H} B \xrightarrow{G} C \xrightarrow{F} D$$

gilt als Abbildungen $A \to D$

$$F \circ (G \circ H) = (F \circ G) \circ H.$$

Beweis. Sei $x \in A$ beliebig. Dann gilt

$$F \circ (G \circ H)(x) = F(G \circ H(x)) = F(G(H(x))) = (F \circ G)(H(x)) = (F \circ G) \circ H(x).$$ □

Definition 13.21. Eine Abbildung $F : A \to B$ heißt **umkehrbar**, wenn es eine Abbildung $G : B \to A$ gibt, genannt **Umkehrabbildung**, so dass gilt:

$$G(F(a)) = a \quad \text{für alle } a \in A, \text{ und} \quad F(G(b)) = b \quad \text{für alle } b \in B.$$

Proposition 13.22. *Wenn eine Umkehrabbildung existiert, dann ist sie eindeutig.*

Beweis. Wir nehmen an, dass sowohl G als auch H Umkehrabbildungen zur Abbildung $F : A \to B$ sind. Zu zeigen ist, dass $G = H$ als Abbildungen $B \to A$. Per Definition ist $G \circ F = \mathrm{id}_A$ und $F \circ H = \mathrm{id}_B$. Damit folgt

$$G = G \circ \mathrm{id}_B = G \circ (F \circ H) = (G \circ F) \circ H = \mathrm{id}_A \circ H = H,$$

wobei wir einmal Proposition 13.20 und zweimal Proposition 13.19 benutzt haben. □

Satz 13.23. *Eine Abbildung ist genau dann umkehrbar, wenn sie bijektiv ist.*

Beweis. Sei $F : A \to B$ die fragliche Abbildung. Wir zeigen die Äquivalenz schrittweise als Implikation in beide Richtungen.

Notwendig: Wir wollen zeigen, dass aus der Existenz einer Umkehrabbildung, nennen wir sie $G : B \to A$, folgt, dass F bijektiv ist. Dazu müssen wir injektiv und surjektiv nachweisen.

- injektiv: Wenn für $a_1, a_2 \in A$ gilt $F(a_1) = F(a_2)$, dann folgt
$$a_1 = G(F(a_1)) = G(F(a_2) = a_2.$$
Also ist F injektiv.
- surjektiv: Wenn $b \in B$ beliebig ist, dann ist mit $a = G(b)$
$$F(a) = F(G(b)) = b.$$
Also ist F surjektiv.

Hinreichend: Jetzt wollen wir zeigen, dass eine bijektive Abbildung eine Umkehrabbildung hat. Diese müssen wir definieren. Sei $G : B \to A$ dadurch definiert, dass wir dem Element $b \in B$ dasjenige $a \in A$ zuordnen, für das gilt $F(a) = b$. Die Surjektivität von F garantiert, dass es so ein a gibt, und die Injektivität sagt, dass es höchstens so ein a gibt. Es gibt also genau ein solches $a \in A$, und das macht unsere Definition wohldefiniert. Dieses G ist tatsächlich eine Umkehrabbildung, denn per Definition ist
$$G(F(a)) = a, \text{ für alle } a \in A$$
denn für Elemente der Form $F(a)$ ist ja gerade a dasjenige durch die Definition von G herausgefilterete Element von A. Weiter ist
$$F(G(b)) = b, \text{ für alle } b \in B,$$
denn $G(b)$ ist per Definition dasjenige Element, das unter F auf b abbildet. □

Beispiel 13.24. Als Abbildung $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ ist $x \mapsto x^2$ bijektiv. Die Umkehrabbildung ist die Wurzelfunktion $x \mapsto \sqrt{x}$. Für andere Definitons- und Wertebereiche der Abbildung $x \mapsto x^2$ wie in Beispiel 13.15 gibt es keine Umkehrfunktion!

Notation 13.25. Für das wiederholte Verketten einer Abbildung $f : X \to X$ mit sich selbst verwenden wir eine Potenzschreibweise. Also
$$f^2 = f \circ f : X \to X, \qquad f^2(a) = f(f(a)) \text{ für alle } a \in X.$$
und allgemeiner für alle $n \in \mathbb{N}_{>0}$
$$f^n = \underbrace{f \circ \ldots \circ f}_{n} : X \to X, \qquad f^n(a) = \underbrace{f(\ldots f}_{n}(a)) \text{ für alle } a \in X.$$
Dazu definieren wir
$$f^0 = \mathrm{id}_X .$$
Das paßt zu folgendem Potenzgesetz.

Proposition 13.26. *Sei $f : X \to X$ eine Abbildung. Dann gilt für alle $n, m \in \mathbb{N}_0$*
$$f^{n+m} = f^n \circ f^m$$
als Abbildungen $X \to X$.

Beispiel 13.27. Statt eines Beweises machen wir ein Beispiel. Wir betrachten $f : \mathbb{R} \to \mathbb{R}$ gegeben durch
$$f(x) = x + 1,$$
die Abbildung „addiere 1“. Wenn wir die n-mal ausführen, dann entsteht die Abbildung
$$f^n(x) = x + n.$$
Es gilt dann
$$f^n \circ f^m(x) = f^n(x + m) = (x + m) + n = x + (m + n) = x + (n + m) = f^{n+m}(x).$$
Dieses Beispiel ersetzt den Beweis nicht.

13.4. **Märchenstunde: Collatz.** Das Collatz $3n+1$-Problem betrachtet die folgende Abbildung $c : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ definiert durch

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

Mit dieser Abbildung c betrachtet man nun die Kompositionen $c \circ c$, und $c \circ c \circ c$, ..., usw. Man wendet also immer wieder $c(-)$ auf die Ergebnisse an. Was passiert? Egal wo man startet, man scheint in die Schleife

$$1 \rightsquigarrow c(1) = 4 \rightsquigarrow c(4) = 2 \rightsquigarrow c(2) = 1 \rightsquigarrow c(1) = 4 \ldots$$

hineinzulaufen. Das kann aber niemand beweisen.

Take home message Kapitel §13.

- Abbildungen setzen Mengen miteinander in Verbindung.
- Abbildungen kann man darstellen: Wertetabelle, Graph, Pfeildiagramm.
- Funktionen sind Abbildungen.
- injektiv, surjektiv, bijektiv.

14. Mächtigkeiten und Kombinatorik

Quellen: [GK23] Kapitel 4 und 6, [SchSt18] Kapitel 2.5 und 4.4

14.1. **Motivation: Kombinatorik ist die Kunst des Zählens.** Natürliche Zahlen sind nicht nur dafür geeignet, Dinge abzuzählen und damit in eine Reihenfolge zu bringen:

- Platz 1, Platz 2, Platz 3, ... bei einem Wettkampf, oder
- Aussage 1, Aussage 2, Aussage 3, ... bei der vollständigen Induktion.

Eine erstmal von der Bedeutung (Reihenfolge) losgelöste alternative Bedeutung besteht im Gebrauch der natürlichen Zahlen als Antwort auf die Frage: wieviele?

- Man braucht 4 Eier für das Rezept, oder
- die Klasse hat 27 SuS ....

Letzteres ist zum Beispiel wichtig bei einer Klassenfahrt, um zu wissen, ob auch alle SuS da sind. Man kontrolliert das durch Nachzählen, und das verbindet die beiden Bedeutungen „Welche Reihenfolge?“ und „Wieviele?“: man erstellt eine Reihenfolge, welche ist egal, und nur die Länge der Liste entscheidet über die Anzahl.

Sofort ergeben sich Fragen nach: was bedeutet endlich? Und dann, was bedeutet unendlich? Und wenn unendlich, dann wieviele unendlich? Sind alle unendlich gleich groß?

14.2. **Endliche Mächtigkeiten.**

⚠ Das Rechnen mit Zahlen, Addition und Multiplikation hat einfache Entsprechungen wenn es um Anzahlen geht.

Fake Definition 14.1. Eine Menge A ist eine endliche Menge, wenn es eine natürliche Zahl $n \in \mathbb{N}_0$ gibt, so dass A genau n verschiedene Elemente enthält.

Wir haben zu einer natürlichen Zahl $n \in \mathbb{N}_0$ die Menge $[n]$ definiert, die durch Aufzählen der Elemente als

$$[n] = \{[0], [1], [2], \dots, [n-1]\}.$$

beschrieben wird. Wir vereinfachen die Notation nun zu

$$[n] = \{0, 1, 2, \dots, n\}.$$

Diese Menge enthält genau n Elemente. Wir nehmen sie als „Maßstab“ für eine Menge mit n Elementen. Diesen Maßstab an eine Menge A anzulegen, bedeutet, eine bijektive Abbildung $[n] \to A$ zu finden.

Definition 14.2. Eine Menge A ist eine endliche Menge, wenn es eine natürliche Zahl $n \in \mathbb{N}_0$ und eine bijektive Abbildung $f\colon [n] \to A$ gibt.

Eine bijektive Abbildung $f : [n] \to A$ führt zu Elementen $x_i := f(i) \in A$ für alle $i = 0, \dots, n-1$. Bijektiv bedeutet hier, dass

- erstens die x_i lauter verschiedene Elemente sind, und
- zweitens alle Elemente von A.

Das sind dann die n verschiedenen Elemente aus der fake Definition, die A ausmachen. Man kann die Bijektion auch als eine Auflistung der Elemente von A mit einer Liste der Länge n betrachten:

$$x_0, x_1, \dots, x_{n-1}.$$

Wir haben gewissermaßen die Elemente wie die SuS auf Klassenfahrt abgezählt (nur würden wir normalerweise bei 1 zu zählen beginnen).

Die Definition der Mächtigkeit enthält eine Behauptung: die Anzahl der Elemente einer Menge ist eindeutig. Das klingt plausibel, kann aber bewiesen werden.

Proposition 14.3. *Seien verschiedene Elemente $x_1, \dots, x_n$, und weitere verschiedene Elemente $y_1, \dots, y_m$ gegeben. Dann folgt aus*

$$\{x_1, \dots, x_n\} = \{y_1, \dots, y_m\}$$

bereits $n = m$.

Definition 14.4. Die Anzahl n der Elemente ist für die endliche Menge A eindeutig. Sie wird die **Mächtigkeit** von A genannt und mit $\#A$ oder $|A|$ notiert.

Beweis. Wir beweisen das per Induktion nach n.

Induktionsanfang: Wenn $n = 0$ ist, dann ist die linke Menge leer. Dann muss die rechte Menge auch leer sein, denn sie sind ja gleich. Also ist $m = 0$.

Induktionsschritt: Wir nehmen jetzt an, dass die Aussage für $n-1$ bereits bewiesen ist, und betrachten den Fall mit Elementen $x_1, \dots, x_n$. Dann ist x_n ein Element der linken Seite, also auch der rechten Seite, denn die Mengen sind gleich. Also muss eines der y's mit x_n übereinstimmen. Wir sortieren die y's so um, und das ändert die Anzahl nicht, dass oBdA $y_m = x_n$. Insbesondere ist $m \geq 1$, denn ein y muss es geben. Jetzt löschen wir das Element x_n aus der Menge. Dann folgt

$$\{x_1, \dots, x_{n-1}\} = \{x_1, \dots, x_n\} \smallsetminus \{x_n\} = \{y_1, \dots, y_m\} \smallsetminus \{y_m\} = \{y_1, \dots, y_{m-1}\}.$$

Damit vergleichen wir nun zwei Mengen, wobei die linke nur noch $n-1$ Elemente hat. Das können wir bereits per Induktionsannahme. Also gilt $n-1 = m-1$ per Induktioinsannahme. Wir addieren 1 und erhalten daraus $n = m$. Das zeigt die Behauptung. □

Bemerkung 14.5. Die Mächtigkeit der leeren Menge ist 0. Ein Glück gibt es diese Zahl bereits, sonst müßten wir sie spätestens jetzt erfinden.

Die leere Menge ist übrigens die einzige Menge mit Mächtigkeit 0.

Bemerkung 14.6. Die Addition von natürlichen Zahlen entspricht der Vereinigung von endlichen Mengen ohne gemeinsame Elemente. Sei A eine Menge mit $n = \#A$ Elementen und b eine Menge mit $m = \#B$ Elementen. Wenn $A \cap B = \varnothing$ leer ist, dann gilt

$$\#(A \cup B) = \#A + \#B = n + m.$$

Man könnte also sagen, dass die Addition nur die Abstraktion davon ist, dass zwei Leute (Mengen) sich mit ihrem jeweiligen Hab und Gut (Elementen) zusammentun.

Die Multiplikation hat auch eine Entsprechung für Mengen.

Proposition 14.7. *Seien A und B endliche Mengen. Dann gilt*

$$\#(A \times B) = \#A \cdot \#B.$$

Beweis. Wenn Sie an den Setzkasten für die Intuition von $A \times B$ denken, dann handelt es sich bei der Proposition nur um die Formel für die Fläche eines Rechtecks.

Wir beweisen das per Induktion nach der Anzahl $\#A$, die wir n nennen. *Induktionsanfang*: Wenn $\#A = 0$ istm, dann ist $A = \varnothing$ leer. Dann kann es auch kein Tupel $(a, b) \in A \times B$ geben, denn woher soll den ein benötigtes $a \in A$ kommen? Also ist dann auch $A \times B$ leer. Die Gleichung gilt, weil $0 = 0 \cdot \#B$ egal wie viele Elemente B hat.

Induktionsschritt: Wir nehmen an, dass die Aussage für $n-1$ bereits gilt. Sei $x \in A$. Das gibt es, weil wir jetzt im Fall $\#A = n$ sind und $n \geq 1$. Wir entfernen das Element x aus A: sei $A_0 = A \smallsetminus \{x\}$. Dann gilt $A_0 \cap \{x\} = \varnothing$, also

$$\#A_0 + \#\{x\} = \#A$$

und das bedeutet $\#A_0 = n - 1$. Die Menge $A \times B$ kann man jetzt aufteilen: die Tupel (a, b) mit $a = x$. Davon gibt es $\#B$ viele. Und die Tupel mit $a \neq x$, also $a \in A_0$. Diese Tupel sind gerade die

Elemente von $A_0 \times B$. Es folgt

$$\begin{aligned}\#(A \times B) &= \#\{(a,b) \in A \times B \ ; \ a = x\} + \#A_0 \times B \\ &\overset{\text{IA}}{=} \#B + (n-1) \cdot \#B \\ &= n \cdot \#B = \#A \cdot \#B.\end{aligned}$$

Das beweist den Induktionsschritt und damit die Proposition. □

14.3. **Kombinatorik des Auswählens.**

Definition 14.8. Die **Fakultät** einer natürlichen Zahl n ist die Zahl $n!$, die rekursiv definiert ist durch

$$\begin{aligned}0! &= 1, \\ n! &= n \cdot (n-1)! \qquad \text{für } n \geq 1.\end{aligned}$$

Die Definition wird informell zu

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 4 \cdot 3 \cdot 2 \cdot 1.$$

mit $0! = 1$, denn hier hat man das leere Produkt und das hat den Wert der multiplikativen Einheit.

Bemerkung 14.9. Die rekursive Definition funktioniert als Konsequenz des Induktionsaxioms (PA5) der natürlichen Zahlen. Man muss den Anfang definieren ($0! = 1$) und den rekursiven Definitionsschritt, also bei $n-1$ ist es bereits definiert und dann kennt man auch bei n. Das Axiom (PA5) sorgt dafür, dass man auch bei allen natürlichen Zahlen mit dieser Methode früher oder später vorbeikommt.

Satz 14.10. *Sei $n \geq 1$. Die Anzahl der Möglichkeiten, n verschiedene Dinge in eine Reihenfolge zu bringen, ist $n!$.*

Beweis. Das beweisen wir per Induktion. Für $n = 1$ gibt es nur die eine Reihenfolge, also $1! = 1$ viele Mïglichkeiten. Angenommen, für $n-1$ viele Dinge haben wir es schon bewiesen. Dann nehmen wir n Dinge. Es gibt n Möglichkeiten für die Position 1. Bei jeder der so begonnenen Reihenfolgen steht dann eine Sortierung von $n-1$ vielen Dingen an. Das geht dann jeweils auf $(n-1)!$ viele Möglichkeiten. Zusammen ergeben sich $n \cdot (n-1)!$ viele Anorndungen. Und das sind $n!$ viele. □

Wieviele verschiedene Lottoscheine kann man beim Lotto „6 aus 49“ausfüllen? Wieviele Lottoscheine muß man ausfüllen, um ganz sicher bei einem der Lottoscheine 6 Richtige zu haben? Hier geht es um die folgende Frage für $n = 49$ und $k = 6$.

Definition 14.11. Seien $n, k \in \mathbb{N}_0$ natürliche Zahlen. Die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge wird bezeichnet mit

$$\binom{n}{k},$$

nennt sich **Binomialkoeffizient** und wird gelesen **„n über k“** (engl. n choose k).

Jetzt haben wir einen Namen und ein Symbol aber keine Ahnung, wie man die Zahl konkret bekommt. Es gibt

$$\binom{49}{6} = 13.983.816 \approx 14 \cdot 10^6$$

viele Lottoscheine, aber wie haben wir das ausgerchnet?

Satz 14.12. *Für alle $n, k \in \mathbb{N}_0$ gilt*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Hierbei legen wir fest, dass $\binom{n}{k} = 0$ gilt, sobald n oder k negativ sind.

Beweis. Wir betrachten eine Menge A mit n Elementen und markieren ein Element davon, etwa $x \in A$. Jetzt sortieren wir die k-elementigen Teilmengen in zwei Schubladen:

- Die k-elementigen Teilmengen der ersten Sorte sind diejenigen, die das x nicht enthalten. Dies sind also k-elementige Teilmengen von $A \smallsetminus \{x\}$, einer $n-1$-elementigen Menge. Von dieser Sorte gibt es daher
$$\binom{n-1}{k}$$
viele.
- Die k-elementigen Teilmengen der zweiten Sorte sind diejenigen, die das x enthalten. Dies sind also $k-1$-elementige Teilmengen von $A \smallsetminus \{x\}$ vereinigt mit $\{x\}$. Von dieser Sorte gibt es daher
$$\binom{n-1}{k-1}$$
viele.

Das zeigt die behauptete Formel. □

Satz 14.13. *Für alle $n, k \in \mathbb{N}_0$ gilt*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Beweis. Jede Teilmenge bestimmt und ist eindeutig bestimmt durch ihr Komplement. Das Komplement einer k-elementigen Teilmenge in einer n-elementigen Teilmenge hat $(n-k)$-viele Elemente. Daher gibt es genausoviele k-elementige Teilmengen wie es $(n-k)$-elementige gibt. □

Satz 14.12 erlaubt das rekursive Berechnen aller Binomialkoefffizienten. Es gilt sicher

$$\binom{n}{0} = 1$$

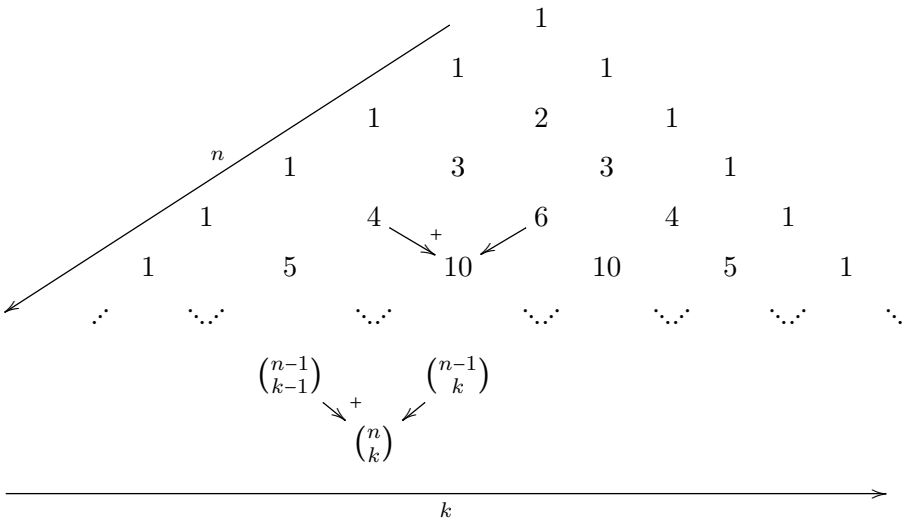
für alle $n \in \mathbb{N}_0$, denn es gibt immer genau eine 0-elementige Teilmenge: die leere Menge! Genauso ist

$$\binom{n}{n} = 1,$$

denn die einzige n-elementige Teilmenge in einer n-elementigen ist die Menge selbst. Das paßt zu Satz 14.13.

⚠ Das **Pascal'sche Dreieck** organisiert die $\binom{n}{k}$ auf eine Weise, mit der man sie gut rekursiv berechnen kann.

Die Zeilen des Pascal'schen Dreiecks werden beginnend mit 0 durch n angegeben. Entlang einer Zeile zählt man mit k. Dann steht an der k-ten Position Zeile n der Wert $\binom{n}{k}$.



Haben wir $\binom{n}{k}$ für alle k in der Zeile n berechnet, dann ergibt sich nach Satz 14.12 die nächste Zeile. Die Randterme sind gerade $\binom{n}{0} = \binom{n}{n} = 1$.

Bemerkung 14.14. Im populären youtube Kanal **numberphile** von Brady Haran finden Sie ein empfehlenswertes Video zum Pascalschen Dreieck mit Casandra Monroe.

Es ist nicht so schwer, mit dem Pascalschen Dreieck die Binomialkoeffizienten $\binom{n}{k}$ für kleine k und n auszurechnen. Aber wie macht man das mit $\binom{49}{6}$?

Proposition 14.15. *Für alle natürlichen Zahlen $n, k \geq 1$ gilt*

$$\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}$$

Beweis. Wir haben einen Verein n Mitgleidern, einem Vorstand aus k Mitgliedern und einer Präsidentin, die Teil des Vorstands ist. Auf wieviele Arten kann man im Verein den Vorstand und die Präsidentin auswählen? Das können wir auf zwei Arten zählen, die beide das gleiche Ergebnis liefern müssen.

- In der ersten Methode wählen wir als erstes den Vorstand ($\binom{n}{k}$-viele Möglichkeiten) und der wählt dann die Präsidentin (k-viele Möglichkeiten). Das geht insgesamt auf
$$k \cdot \binom{n}{k}$$
viele Arten.
- In der zweiten Methode wählen wir als erstes die Präsidentin (n-viele Möglichkeiten), und ergänzen dann die $(k-1)$-vielen restlichen Vorstandsmitglieder aus den $(n-1)$-vielen verbliebenen Mitgliedern ($\binom{n-1}{k-1}$-viele Möglichkeiten). Das geht insgesamt auf
$$n \cdot \binom{n-1}{k-1}$$
viele Arten.

Damit gilt

$$k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}.$$

Umstellen führt auf die behauptete Formel. □

Satz 14.16. *Für alle $n, k \in \mathbb{N}_0$ gilt*

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

Beweis. Per Induktion nach k folgt aus Proposition 14.15

$$\begin{aligned}\binom{n}{k} &= \frac{n}{k} \cdot \binom{n-1}{k-1} = \frac{n \cdot (n-1)}{k \cdot (k-1)} \cdot \binom{n-2}{k-2} = \ldots = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1} \cdot \binom{n-k}{0} \\ &= \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1} = \frac{n!/(n-k)!}{k!} = \frac{n!}{k!(n-k)!}.\end{aligned}$$

□

14.4. **Die binomische Formel.**

⚠ In der Schule lernt man die binomische Formel für Exponent 2. In Wahrheit ist dies ein Spezialfall einer viel allgemeineren Formel.

Satz 14.17 (Binomische Formel)**.** *Seien X und Y Variablen und $n \in \mathbb{N}_0$. Dann gilt*

$$(X+Y)^n = \sum_{k=0}^{n} \binom{n}{k} X^k Y^{n-k}.$$

Wir geben zwei Beweise, einen kombinatorischen und einen per Induktion. Der kombinatorische Beweis erklärt, warum die Formel so aussieht, wie sie aussieht.

Kombinatorischer Beweis. Wir müssen Ausklammern, und zwar gleichzeitig aus n-vielen Faktoren.

$$\underbrace{(X+Y) \cdot (X+Y) \cdot \ldots \cdot (X+Y)}_{n}$$

Das bedeutet, dass wir die Summe bilden aus den Produkten, wobei wir aus jeder Klammer einen der Summanden auswählen. Und das machen wir auf alle erdenklichen Art und Weisen. Die Faktoren sind entweder X oder Y, also kommt als Beitrag

$$X^k \cdot Y^{n-k}$$

heraus, wenn wir aus k-vielen der Klammern $(X+Y)$ den Summanden X und dann logischerweise aus den restlichen $(n-k)$-vielen Klammern das Y gewählt haben. Diese Auswahl von k-vielen der Klammerausdrücke (wo wir das X wählen) geht auf $\binom{n}{k}$-viele Arten. Also ist der Beitrag insgesamt

$$\binom{n}{k} \cdot X^k \cdot Y^{n-k}.$$

Das summieren wir über alle k auf und sind fertig. □

Beweis per Induktion nach n. Die Induktionsverankerung bei $n = 0$ hat

$$(X+Y)^0 = 1,$$

und

$$\binom{0}{0} \cdot X^0 Y^0 = 1 \cdot 1 \cdot 1 = 1.$$

Das stimmt.

Induktionsschritt: Angenommen, die binomische Formel gilt bereits für Exponent $n-1$. Dann Rechnen wir

$$\begin{aligned}
(X+Y)^n &= (X+Y)\cdot(X+Y)^{n-1} \overset{\text{IA}}{=} (X+Y)\cdot\sum_{k=0}^{n-1}\binom{n-1}{k}X^kY^{n-1-k}\\
&= X\cdot\sum_{k=0}^{n-1}\binom{n-1}{k}X^kY^{n-1-k} + Y\cdot\sum_{k=0}^{n-1}\binom{n-1}{k}X^kY^{n-1-k}\\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}X^{k+1}Y^{n-1-k} + \sum_{k=0}^{n-1}\binom{n-1}{k}X^kY^{n-k}\\
&= \sum_{k=1}^{n}\binom{n-1}{k-1}X^kY^{n-k} + \sum_{k=0}^{n-1}\binom{n-1}{k}X^kY^{n-k} && \text{(1. Summe: Index } k\rightsquigarrow k-1)\\
&= \sum_{k=0}^{n}\binom{n-1}{k-1}X^kY^{n-k} + \sum_{k=0}^{n}\binom{n-1}{k}X^kY^{n-k} && \text{(Extra Summanden sind 0)}\\
&= \sum_{k=0}^{n}\left(\binom{n-1}{k-1}+\binom{n-1}{k}\right)X^kY^{n-k} && \text{(und mit Satz 14.12)}\\
&= \sum_{k=0}^{n}\binom{n}{k}X^kY^{n-k}. && \square
\end{aligned}$$

Proposition 14.18. *In einer endlichen Menge gibt es genause viele Teilmengen mit gerade vielen Elementen, wie solche mit ungerade vielen Elementen.*

Beweis. Sei n die Mächtigkeit der endlichen Menge. Dann behauptet die Proposition

$$\sum_{2|k}\binom{n}{k} = \sum_{2\nmid k}\binom{n}{k}.$$

Das folgt aus Satz 14.17 mit $X=-1$ und $Y=1$:

$$0 = (-1+1)^n = \sum_{k}\binom{n}{k}(-1)^k(\cdot 1^{n-k} = \sum_{2|k}\binom{n}{k} - \sum_{2\nmid k}\binom{n}{k}. \qquad \square$$

14.5. **Märchenstunde: Hilbertsches Hotel.** Seit Cantor sagen wir, dass zwei Mengen gleichmächtig sind, wenn es eine bijektive Abbildunge zwischen ihnen gibt. Gleiche Mächtigkeit in deser Form definiert eine Äquivalenzrelation auf Mengen!

Die Mächtigkeit der natürlichen Zahlen wird mit den hebräischen Buchstaben *Aleph* als

$$\#\mathbb{N}_0 = \aleph_0$$

bezeichnet. Der Index 0 gibt an, dass diese Unendlichkeit die kleinste aller möglichen Unendlichkeiten ist. Man nennt diese Mächtigkeit **abzählbar unendlich**.

Über die Unendlichkeit und Cantor gibt es bei ARTE unter der Rubrik Mathewelten in der Mediathek einen empfehlenswerten Beitrag mit dem Titel *Auf dem Weg in die Unendlichkeit.*

- Gibt es mehr natürliche Zahlen oder mehr ganze gerade Zahlen?

  Wir benutzten die geraden natürlichen Zahlen, um die negativen ganzen Zahlen abzuzählen, und die ungeraden natürlichen Zahlen um die natürlichen Zahlen abzuzählen. Das ergibt eine bijektive Abbildung

$$\begin{aligned}
\mathbb{N}_0 &\longrightarrow \mathbb{Z}\\
0,1,2,3,4,5,6,7,8,9,\ldots &\mapsto -1,0,-2,1,-3,2,-4,3,-5,4\ldots
\end{aligned}$$

- Gibt es mehr natürliche oder mehr rationale Zahlen? Anstelle einer bijektiven Abbildung geben wir eine eventuell unerwartete injektive Abbildung $\mathbb{Q} \to \mathbb{N}_0$ an.
$$\begin{aligned} \mathbb{Q} &\hookrightarrow \mathbb{N}_0 \\ \frac{a}{b} &\mapsto 2^{|a|} \cdot 3^{|b|} \cdot 5^{1+\operatorname{sign}(a/b)} \end{aligned}$$
wobei der Bruch $\frac{a}{b}$ in gekürzter From vorliegen soll und $\operatorname{sign}(ab)$ das Vorzeichen von a/b sein soll. Die Abbildung ist wohldefiniert und aufgrund der eindeutigen Primfaktorzerlegung injektiv. Man kann daraus zeigen, dass
$$\aleph_0 = \#\mathbb{N}_0 = \#\mathbb{Q}.$$
- Mit dem berühmten Cantorschen Diagonalverfahren kann man zeigen, dass es mehr (im Sinne von Mächtigkeiten nach Cator) Dezimalzahlen als natürliche Zahlen gibt. Dies zeigt, dass es verschieden große Unendlichkeiten gibt:
$$\aleph_0 = \#\mathbb{N}_0 < \#\mathbb{R}.$$
- Unendliche Mächtigkeit: Hilbertsches Hotel. Veranschaulicht die folgenden Aussagen zu Mächtigkeiten:
$$\begin{aligned} \aleph_0 + 1 &= \aleph_0, \\ \aleph_0 + \aleph_0 &= \aleph_0, \\ \aleph_0 \cdot \aleph_0 &= \aleph_0. \end{aligned}$$

Take home message Kapitel §14.

- Mächtigkeit einer endlichen Menge
- Fakultät $n!$
- Binomialkoeffizient $\binom{n}{k}$, Pascalsches Dreieck, Binomische Formel
- Mächtigkeit bei unendlichen Mengen; Hilbertsches Hotel
- abzählbar unendlich $\aleph_0$; es gilt $\aleph_0 = \#\mathbb{N}_0 = \#\mathbb{Z} = \#\mathbb{Q} < \#\mathbb{R}$

15. Primzahlen

15.1. **Motivation:** Primzahlen sind die multiplikativen Atome der natürlichen Zahlen. Sie sind wie Atome unteilbar, und jede natürliche Zahl ist das Produkt einer eindeutigen Liste von Primzahlen. Primzahlen scheinen in der Menge aller natürlichen Zahlen ohne Ordnung zufällig verteilt aufzutreten.

- Wie bestimmt man, ob eine natürliche Zahl eine Primzahl ist?
- Wie kann man eine Liste aller Primzahlen aufstellen?
- Gibt es Regelmäßigkeitten im Chaos der Primzahlen?
- Wozu kann man Primzahlen gebrauchen?

15.2. **Primzahlen aussieben.** Das **Sieb des Eratosthenes** ist eine ganz alte Methode, um die Primzahlen in einem Bereich $1, \dots, N$ für eine obere Schranke N zu bestimmen. Im Prinzip kann man N nach unendlich laufen lassen und dadurch letzliche alle Primzahlen bestimmen. Nur, es gibt ja bekanntlich unendlich viele Primzahlen, so dass sie eh nicht auf ein Papier oder Tafel passen, und daher hören wir bei einer Schranke N auf.

Erste Version: wir nehmen an, wir kennen die der Größe nach ersten Primzahlen 2, 3 und 5. Wir wollen die Primzahlen bis $N = 100$ bestimmen.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Dann beginnen wir mit dem 2-Sieb. Durch dieses Sieb fallen alle Zahlen durch, die durch 2 teilbar sind, mit Ausnahme der 2 selber.

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

Weil durch 2 teilbare Zahlen größer als 2 keine Primzahlen sind, haben wir mit diesem 2-Sieb nur Nichtprimzahlen durchs Sieb fallen lassen. Die Primzahlen sind weiter im Sieb vorhanden. Jetzt machen wir das 2-Sieb zum 3-Sieb und schütteln wieder. Es fallen nun die durch 3 teilbaren Zahlen durchs Sieb, mit Ausnahme der 3 selber.

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

Wieder sind alle Primzahlen im Sieb geblieben. Weiter geht es mit dem 5-Sieb analog.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

Wenn wir dies mit allen Primzahlen machen würden, dann würden alle Nichtprimzahlen irgendwann an die Reihe kommen und durchs Sieb fallen. in der Tat, wenn die Zahl a zusammengesetzt ist, dann hat sie einen Primfaktor $p < a$ und fällt damit durchs p-Sieb. Am Ende des Siebens bleiben im Sieb also nur Primzahlen übrig, geschafft! Denkste. Wir suchen die Primzahlen und brauchen bereits alle Primzahlen, um alle Siebe benutzen zu können. Es fehlt also noch eine entscheidende Idee.

Angenommen wir haben die ersten soundsoviele Primzahlen bereits zum Sieben benutzt, z.B. die 2, 3 und die 5. Dann müssen wir ja nur wissen, wie die nächste Primzahl aussieht, die wir zum Sieben benutzen sollen. Und das ist einfach: das ist die kleinste Zahl, die noch im Sieb ist und die noch nicht zum Sieben benutzt wurde. Im Beispiel ist das die 7 (die 2 und 3 haben wir benutzt, die 4 ist ausgesiebt, die 5 haben wir benutzt und die 6 ist wieder ausgesiebt). Wir erweitern mit der 7 die Liste der bekannten Primzahlen und sieben weiter mit dem 7-Sieb.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Und mit diesem Verfahren geht es immer weiter.

Satz 15.1. *Sei N eine natürliche Zahl. Das Sieben mit dem Sieb des Eratosthenes im Bereich $1, \ldots, N$ kommt zum Ende, sobald man alle Primzahlen p mit $p \leq \sqrt{N}$ zum Sieben benutzt hat.*

Beweis. Man muß für alle zusammengesetzten Zahlen $n = ab$, mit $1 < a$ und $1 < b$ und $n \leq N$ mit einem Primteiler gesiebt haben. Die Behauptung ist also: jede Zusammengesetzte Zahl $n \leq N$ hat einen Primteiler $\leq \sqrt{N}$. Das beweisen wir jetzt.

Sei p der kleinste Primteiler von $n = ab$ eine echte Faktorisierung (kein Faktor 1). Dann ist sicher $p \leq a$ und $p \leq b$, denn Primteiler von a oder b sind Primteiler von n und damit mindestens so groß wie p nach der Minimalitätseigenschaft von p. Dann gilt aber

$$p^2 = p \cdot p \leq a \cdot b = n \leq N$$

indem ich den ersten Faktor p durch den höchstens größeren Faktor a und den zweiten durch b ersetze wir das Produkt nur höchstens größer. Nehmen wir die Wurzel dieser positiven Zahlen und benutzen, dass die positive Wurzel die Ungleichung erhält, so erhalten wir wie bhauptet

$$p \leq \sqrt{N}.$$

□

Wenn wir Primzahlen aus $1, \ldots, 100$ aussieben, dann müssen wir also nur die Siebe zu Primzahlen $p \leq \sqrt{100} = 10$ bemühen. Wir sind also in unserem Beispiel schon fertig und alle noch im Sieb vorhandenen Zahlen sind Primzahlen!

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Auf Wikipedia gibt es dazu eine nette Animation: Sieve_of_Eratosthenes_animation.gif

15.3. **Märchenstunde: Gleichverteilung auf Restklassen.** Die Restklassen modulo 10 werden durch die Einerziffer bestimmt. Das entspricht gerade den Spaten in der Tabelle

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Zählen wir die Anzahl der Primzahlen bis 100 sortiert nach der Einerziffer a, also

$$\pi_a(100) = \#\{p \ ; \ p \text{ Primzahl }, \ p \leq 100, \ p \equiv a \pmod{10}\},$$

dann finden wir

a	1	2	3	4	5	6	7	8	9	0
$\pi_a(100)$	5	1	7	0	1	0	6	0	5	0

Hierbei fällt auf, dass wenn man die 2 und die 5 mal rausnimmt, nur in den Restklassen $\equiv 1$ oder 3 oder 7 oder 9 $\pmod{10}$ Primzahlen auftreten, und dann aber ungefähr gleich viele. Das ist ein allgemeiner Satz von Dirichlet. Die „Eimer“ der Primzahlen in einer vorgegebenen Restklasse füllen sich gar nicht, oder ungefähr gleich schnell.

Behandeln wir auf elementare Wiese als Beispiel den Modulus 4. Primzahlen ≥ 3 sind ungerade, den eine gerade Primzahl p hat den Teiler 2 und muss daher selbst $p = 2$ sein. Damit verteilen sie sich die Primzahlen auf die Restklassen $\equiv 1$ oder 3 modulo 4. Weil es unendlich viele Primzahlen gibt, muss es folglich von einer Sorte unendlich viele geben! Es gfibt also unendlich viele Primzahlen der Form $4k+1$ oder unendlich viele Primzahlen der Form $4k+3$. Welche nun? Beide, sagt der Satz von Dirichlet! Und zwar im Prinzip gleich viele. Elementar beweisen können wir immerhin, dass der Eimer mit den Primzahlen $\equiv 3 \pmod{4}$ unendlich viele enthält.

Satz 15.2. *Es gibt unendlich viele Primzahlen der Form $4k+3$.*

Beweis. Angenommen es gibt nur endlichh viele. Diese Primzahlen sind dan eine endliche Liste, sagen wir $p_1, \ldots, p_n$. Jetzt definieren wir N durch

$$N = 4 \cdot p_1 \cdot \ldots \cdot p_n - 1.$$

Dieses N ist von der Form $4K+3$ (weil $-1 \equiv 3 \pmod{4}$) und hat daher einen Primteiler der Form $\ell = 4k+3$. Denn 2 teilt N nicht, und ansonsten wären alle Primteiler von N kongruent 1 modulo 4, so dass ihr Produkt auch 1 modulo 4 wäre, ein Widerspruch. Dieses ℓ steht somit auf unserer Liste und damit gilt gleichzeitig $N \equiv 0 \pmod{\ell}$ nach Wahl von ℓ. Es gilt auch $N \equiv -1 \pmod{\ell}$, weil ersichtlich das Produkt $p_1 \cdot \ldots \cdot p_n$ durch ℓ geteilt wird und modulo ℓ der Rest -1 bleibt. Das geht nicht gleichzeitig. Widerspruch! □

Der Beweis von Satz 15.2 ist eine Adaption des ursprünglichen Beweis von Euklid für die Unendlichkeit der Primzahlmenge.

Bemerkung 15.3. Feinere Aussagen zu der Frage, wie gleichmäßig die Primzahlen sich auf die beiden Restklassen verteilen, sind Gegenstand aktueller Forschung. In diesem Zusammenhang treffen wir auf eine der bedeutendsten offenen Fragen der Zahlentheorie oder sogar der Mathematik: die Riemannschen Vermutung. Die Riemannsche Vermutung gehört zu den Milleniumproblemen, für deren Lösung zur Jahrtausendwende vom Fields Institute,Toronto, jeweils eine Million Dollar als Preisgeld ausgelobt wurde.

15.4. **Märchenstunde: Primzahlsatz.** Die Primzahlzählfunktion ist die Funktion

$$\pi : \mathbb{R}_{\geq 0} \to \mathbb{N}_0$$

gegeben durch

$$\pi(x) = \#\{p \ ; \ p \text{ Primzahl und } p \leq x\}.$$

Der Primzahlsatz gibt Auskunft über die asymptotische Größe dieser primzahlzählenden Funktion. Schon 1793 hat der 15-jährige Gauß[10] (und unabhängig davon Legendre[11]) die Vermutung geäußert, die Primzahlzählfunktion verhielte sich für $x \to \infty$ wie $x/\ln(x)$ beziehungsweise genauer wie der Integrallogarithmus

$$\mathrm{Li}(x) := \int_2^x \frac{1}{\ln(t)} dt.$$

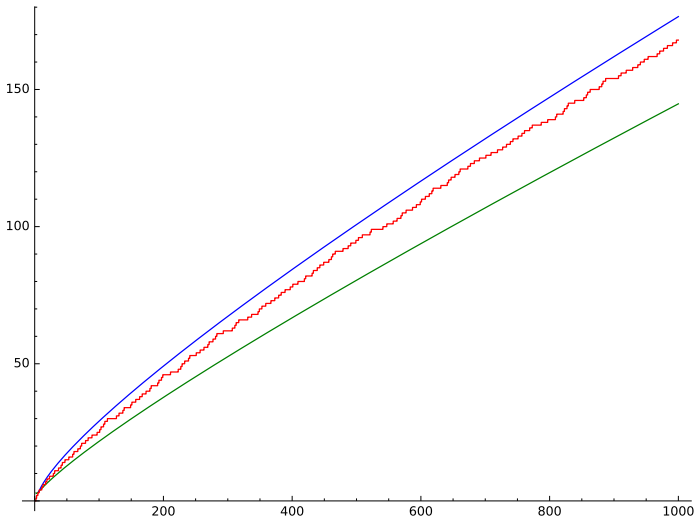


Abbildung 10. Die vorgeschlagenen Approximationen der Primzahlzählfunktion $\pi(x)$, in grün durch $x/\ln(x)$ und in blau die bessere Approximation durch $\mathrm{Li}(x)$.

Wir schreiben $f(x) \sim g(x)$, wenn sich die Funktion $f(x)$ asymptotisch für $x \to \infty$ wie die Funktion $g(x)$ verhält. Das bedeutet, daß der Quotient den folgenden Limes hat:

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Der Primzahlsatz bestätigt die Vermutung zur Asymptotik der Primzahlzählfunktion.

Theorem 15.4 (Primzahlsatz, Hadamard[a] und de La Vallée Poussin[b] 1896)**.** *Es gilt asymptotisch für* $x \to \infty$

$$\pi(x) \sim \frac{x}{\ln x}.$$

[a] Jacques Hadamard (1865–1963), französischer Mathematiker.
[b] Charles-Jean de La Vallée Poussin (1866–1962), belgischer Mathematiker.

Bemerkung 15.5. Es ist bemerkenswert, dass in der Welt der Primzahlen die Analysis durch den Logarithmus und das Integral, die ja nichts mit Teilbarkeit zu tun haben, etwas mitzureden hat.

15.5. **Märchenstunde: elementare offene Fragen zu Primzahlen.**

[10] Johann Carl Friedrich Gauß (1777–1855), deutscher Mathematiker, Astronom, Geodät und Physiker.
[11] Adrien-Marie Legendre (1752–1833), französischer Mathematiker.

15.5.1. *Primzahlzwillinge.* Beispiele sind einfach: 3 und 5, oder 11 und 13, oder 59 und 61, oder 107 und 109, und so weiter.

Definition 15.6. Primzahlzwillinge sind Primzahlen der Form p und $p+2$, also die genau 2 auseinander liegen.

Bemerkung 15.7. Es ist unbekannt, ob es unendlich viele Primzahlzwillinge gibt. Man weiß erst seit 2014, dass es eine Schranke gibt (konkret 246) so dass der Abstand $p_{i+1} - p_i$ aufeinanderfolgender Primzahlen unendlich oft kleiner gleich dieser Schranke ist. Unter anderem dafür hat James Maynard im Jahr 2022 die Fields Medaille gewonnen. Die Frage nach unendlich vielen Primzahlzwillingen ist die, ob man die Schranke 246 auf 2 drücken kann. Das weiß im Moment niemand.

15.5.2. *Goldbach-Vermutung.* Primzahlen $\neq 2$ sind ungerade. Addiert man zwei davon, dann bekommt man eine gerade Zahl. Welche? Die Goldbach-Vermutung von 1742 behauptet, dass man jede gerade Zahl ≥ 4 dadurch bekommen kann.

Rechnen wir ein paar Beispiele:

$$\begin{aligned}
4 &= 2+2\\
6 &= 3+3\\
8 &= 3+5\\
10 &= 3+7 = 5+5\\
12 &= 5+7\\
14 &= 3+11 = 7+7\\
16 &= 3+13 = 5+11\\
18 &= 5+13 = 7+11\\
20 &= 3+17 = 7+13\\
22 &= 3+19 = 5+17 = 11+11
\end{aligned}$$

Bemerkung 15.8. Die Goldbachvermutung ist offen. Sie hat Eingang in das Kino gefunden: es handelt sich um das Doktorarbeitsthema der Hauptdarstellering im Film *Le Théorème de Marguerite* von Anna Novion, welcher von der französischen Mathematikerin Ariane Mézard wissenschaftlich begleitet wurde und daher eine Menge echter Mathematik enthält. Er spielt an Originalschauplätzen und die Mathematik auf den Papieren und Tafeln im Film wurde von Mathematikern an der École Normale Supérieure in Paris erstellt.

Im Gegensatz zur offenen Frage der Goldbach-Vermutung ist die folgende Aussage ein bemerkenswertes Theorem (gegenwärtig 2024 immer noch im peer review process).

Theorem 15.9 (Ternäre Goldbachvermutung, Harald Helfgott 2013)**.**
Jede ungerade Zahl $n \geq 7$ ist die Summe dreier Primzahlen: es gibt Primzahlen p_1, p_2, p_3 mit

$$n = p_1 + p_2 + p_3.$$

Take home message Kapitel §15.

- Sieb des Eratosthenes
- Offene Frage: gibt es unendlich viele Primzahlzwillinge?
- Offene Frage: Goldbach-Vermutung
- Freiwillige Zeitverschwendung: https://isthisprime.com/game/

Literatur

[Abe26] N. H. Abel. *Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen.* J. Reine Angew. Math. **1** (1826), 65–84.

[Can95] Georg Cantor. *Beiträge zur Begründung der transfiniten Mengenlehre.* Mathematische Annalen **46** (1895), no. 4, 481–512.

[Enz14] Hans Magnus Enzensberger
Der Zahlenteufel: ein Kopfkissenbuch für alle, die Angst vor der Mathematik haben
gestaltet und mit Bildern versehen von Rotraut Susanne Berner, verschiednen Ausgaben, 262 Seiten.

[GK23] Felix Göbler, Alex Küronya
Einstieg in die beweisorientierte Mathematik: Mit Versuch und Irrtum zum Beweis
Springer Spektrum, 2023, xxix+320 Seiten.

[SchSt18] Hermann Schichl, Roland Steinbauer
Einführung in das mathematische Arbeiten
Springer Spektrum, 3. Auflage, 2018, xvii+534 Seiten.

Jakob Stix, Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Str. 6–8, 60325 Frankfurt am Main, Germany
Email address: stix@math.uni-frankfurt.de