

1 Aussagenlogik und Mengenlehre

*"Das Gegenteil einer wahren Aussage ist eine falsche Aussage. Das Gegenteil einer tiefen Wahrheit kann eine andere tiefe Wahrheit sein."
[Niels Bohr, Physiker, 1885-1962]*

1.1 Wozu Informatiker Aussagenlogik brauchen

Zum einen gehören Aussagenlogik und Mengenlehre zur Grundgrammatik der "Sprache" Mathematik, die wir immer wieder brauchen werden.

Weiter: Ohne Aussagenlogik keine Schaltkreise und ohne Schaltkreise keine Computer.

Die Aussagenlogik spielt aber auch ganz aktuell beim Arbeiten mit Informationen (Information Retrieval) eine Rolle: Bei Anfragen an **Suchmaschinen** formuliert man logische Kombinationen von Stichwörtern, dies ist eine Form der Aussagenlogik. Die Robots und Crawler der Suchmaschinen mussten vorher die Millionen von Seiten im WWW indizieren. Auch hierbei kommt Aussagenlogik zum Tragen.

Spezialfall **Prädikatenlogik**: spielt eine große Rolle beim **Semantic Web** (maschinelle Schlussfolgerungen über Inhalte des WWW).¹ Ebenso bei **Software-Tests** (Korrektheit von Programmen formal beweisen)

1.2 Aussagenlogik

[Hartmann04, S. 25-43]

Def D 1-1 Aussage(form)

Eine **Aussage A** ist ein sprachliches Gebilde, das entweder wahr oder falsch ist. Steht in einer Aussage anstelle einer Konstanten eine Variable (z.B. x), so spricht man von einer **Aussageform A(x)**. Eine Aussageform heißt auch **Prädikat**, die zugehörige Logik die **Prädikatenlogik**.

Def D 1-2 Verknüpfung von Aussagen

Seien A und B Aussagen. Dann definiert man folgende Verknüpfungen:

$\neg A, \bar{A}$	gelesen "nicht A". Diese "Negation von A" ist wahr, wenn A falsch ist. Sie ist falsch, wenn A wahr ist.
$A \wedge B$	gelesen "A und B". $A \wedge B$ ist wahr, wenn A und B beide wahr sind, und sonst falsch.
$A \vee B$	gelesen "A oder B". $A \vee B$ ist wahr, wenn A oder B (d. h. mindestens eins von beiden) wahr ist, und sonst falsch.
$A \Leftrightarrow B$	gelesen "A äquivalent zu B", "A gleichwertig mit B" oder "A genau dann, wenn B". $A \Leftrightarrow B$ ist wahr, wenn A und B den gleichen Wahrheitswert haben, andernfalls falsch.
$A \Rightarrow B$	gelesen "aus A folgt B", "wenn A, dann B", "A impliziert B", "A ist hinreichend für B" oder "B ist notwendig für A". $A \Rightarrow B$ ist wahr, wenn A und B beide wahr sind und ebenfalls wahr, wenn A falsch ist (unabhängig von B). Nur wenn A wahr und B falsch ist, dann ist $A \Rightarrow B$ falsch.

¹ Genauer: "**Semantisch**" heißt "den Inhalt betreffend". Die Semantic-Web-Initiative des WWW-Schöpfers **Tim Berners-Lee** beruht auf der Grundidee, Web-Dokumente mit Semantik in Form von **Metadaten ("tags")** zu versehen, die ihren Inhalt näher beschreiben, und daraus durch Ableitungsregeln (Prädikatenlogik) weitere Schlüsse zu ziehen.

Eine gute Übersicht über Aussagen erhält man mit **Wahrheitstafeln** ("1" für wahr und "0" für falsch):

A	B	\bar{A}	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Satz S 1-1 Regeln für Aussagen

Seien A und B Aussagen. Dann gelten folgende Regeln:

- $\bar{\bar{A}} \Leftrightarrow A$
- De Morgan'sche Regeln: $\overline{A \vee B} \Leftrightarrow \bar{A} \wedge \bar{B}$
 $\overline{A \wedge B} \Leftrightarrow \bar{A} \vee \bar{B}$
- $(A \Rightarrow B) \Leftrightarrow (\bar{A} \vee B) \Leftrightarrow (\bar{B} \Rightarrow \bar{A})$
- $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$
- "Ausmultiplizieren 1": $(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$
- "Ausmultiplizieren 2": $(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$

Beweis u. weitere Regeln in Übungen (via Wahrheitstafeln)

Übung 1: Stellen Sie die Wahrheitstafel auf für $A \vee (B \wedge \bar{C})$ und $\bar{A} \wedge (B \Rightarrow C)$!



			$B \wedge \bar{C}$	$A \vee (B \wedge \bar{C})$	$B \Rightarrow C$	$\bar{A} \wedge (B \Rightarrow C)$

Wichtiges Element der **Prädikatenlogik** sind **Quantoren**:

Bei einer Aussageform $A(x)$ kann man direkt noch nichts über den Wahrheitsgehalt aussagen. Neben dem direkten Einsetzen (z.B. $A(5)$) kann man aber auch über sog. Quantoren zu quantifizierbaren Aussagen kommen

Def D 1-3 Quantoren

Sei $A(x)$ eine Aussageform (ein Prädikat). Dann sind

- $\forall x : A(x) \Leftrightarrow$ "Für alle x gilt $A(x)$ " (\forall : All-Quantor)
- $\exists x : A(x) \Leftrightarrow$ "Es gibt ein x, für das $A(x)$ gilt" (\exists : Existenz-Quantor)

gültige, d.h. quantifizierbare Aussagen.

Beispiel

x ist gerade.	... ist ein Prädikat
Für alle $x \in \mathbf{N}$ ist x gerade.	... ist eine falsche Aussage
Es gibt $x \in \mathbf{N}$ für die gilt: x ist gerade.	... ist eine wahre Aussage

Übung 2: Negieren Sie folgende Aussageformen für $x \in \mathbf{R}$ korrekt!

$$A(x) \Leftrightarrow x > 1 \vee x < -2$$

$$B(x) \Leftrightarrow x \in [1,3]$$

$$C(x) \Leftrightarrow x > 1 \wedge x < -2$$

Übung 3: Negieren Sie folgende Quantoren-Aussagen 1) sprachlich und 2) indem Sie sie in Formeln übersetzen. Verwenden Sie bei der Negierung jeweils den anderen Quantor!

- Für alle $n \in \mathbf{N}$ gilt: $2n$ ist gerade.
- Für alle $x \in \mathbf{R}$ gilt: $x = 2$.
- Es existiert ein $n \in \mathbf{N}$ für das gilt: n^2 ist gerade.

Logik und Sprache: Ein kleines Rätsel ([pdf](#))

1.2.1 Indirekter Beweis (Widerspruchsbeweis)

Müssen sich Informatiker wirklich mit den Beweisen der Mathematik auseinandersetzen? Es genügt doch, die Formeln zu kennen. – 'Beweisen' ist eine logische Auseinandersetzung mit einem Stoffgebiet und das tun Informatiker ständig, sie nennen es nur nicht so: Sie analysieren, ob ein Protokoll das tun kann, was es soll, sie grübeln, ob ein Algorithmus in allen Spezialfällen richtig arbeitet ("was wäre, wenn ...") u.v.a.m. All das ist nichts anderes als "Beweisen" [Hartmann04].

Satz S 1-2 Indirekter Beweis

Beim indirekten Beweis (Widerspruchsbeweis) wird eine Aussage ($A \Rightarrow B$) dadurch bewiesen, dass man zeigt: "Aus \bar{B} folgt \bar{A} , also ein Widerspruch zu A".

Beispiel: Beweisen Sie das **Schubfachprinzip** für $n \in \mathbf{N}$:

Hat man $n+1$ Objekte in n Schubfächer verteilt, so gibt es mindestens ein Schubfach, in dem zwei (oder mehr) Objekte liegen.

Lösung: Der Satz hat die Form " $A \Rightarrow B$ " mit:

A: $n+1$ Objekte sind in n Schubfächer verteilt.

B: Es gibt mindestens ein Schubfach mit 2 (oder mehr) Objekten.

Angenommen, es gälte \bar{B} : Jedes Schubfach enthält höchstens 1 Objekt. Dann wären in allen Schubladen zusammen n mal höchstens 1 Objekt, also höchstens n Objekte. Dies ist ein Widerspruch zu A, dass $n+1$ Objekte in den Schubfächern liegen. Also gilt $\bar{B} \Rightarrow \bar{A}$, mithin ist ($A \Rightarrow B$) richtig. ♦

Eine spezielle Form des Widerspruchsbeweises ergibt sich für $A=1$: Wenn man $(1 \Rightarrow B)$ zeigen will (also B selbst), dann lautet der Widerspruch $(\overline{B} \Rightarrow 0)$. D.h. man startet mit \overline{B} und versucht einen allgemeinen Widerspruch (0) herzuleiten.

Beispiele in den Übungen.

1.3 Mengen

-- dieses Kapitel im Selbststudium (Vorkurswissen) --

In diesem Kapitel werden grundlegende Begriffe der Mengenlehre, die im Folgenden immer wieder benötigt werden, bereitgestellt. Zunächst die Begriffe „Menge, Teilmenge, Vereinigungsmenge“ etc.:

Def D 1-4

Eine **Menge M** ist die Gesamtheit von irgendwelchen Objekten, die durch ein gemeinsames Merkmal charakterisiert werden. Objekte der Menge werden als **Elemente** bezeichnet.

$x \in M$ Objekt x ist Element der Menge M
 $x \notin M$ Objekt x ist nicht Element der Menge M

Beispiele:

$A = \{1,2,3,4\}$

$B = \{2,4,6,8,\dots,2n,\dots\}$

$C = \{x \mid x \text{ eine natürliche Zahl und } x > 10\}$

$\emptyset = \{ \}$ leere Menge (kein Element)

Def D 1-5

Teilmenge: Menge A ist Teilmenge der Menge B (bzw. Menge A ist in der Menge B enthalten), wenn jedes Element von A auch Element der Menge B ist

$$A \subset B \Leftrightarrow (a \in A \Rightarrow a \in B) \quad A \text{ Teilmenge } B$$

Def D 1-6

Vereinigungsmenge: $V = A \cup B \Leftrightarrow (a \in V \Leftrightarrow a \in A \vee a \in B)$

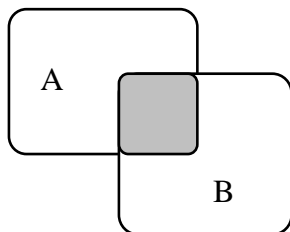
"A vereinigt B"

Def D 1-7

Schnittmenge: $S = A \cap B \Leftrightarrow (a \in S \Leftrightarrow (a \in A \wedge a \in B))$

"A geschnitten B"

Beispiel: VENN-Diagramme zur Darstellung von Mengen



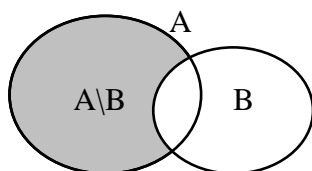
Def D 1-8

Differenzmenge:

$$D = A \setminus B \Leftrightarrow (a \in D \Leftrightarrow (a \in A \wedge a \notin B))$$

"A ohne B"

Beispiel:



1.4 Relationen und Abbildungen

-- dieses Kapitel im Selbststudium (Vorkurswissen) --

Das Mengenprodukt $A \times B$ (gelesen: "A kreuz B") machen wir uns zunächst an einem Beispiel klar:

$$A = \{a, b, c\} \quad B = \{1, 2\}$$

$$C = A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

$(a, 1)$ ist ein geordnetes Paar. An erster Stelle steht ein Element von A, an zweiter Stelle ein Element von B. Die Reihenfolge ist dabei wesentlich, d.h. $(a, 1)$ und $(1, a)$ sind im allgemeinen verschieden.

Def D 1-9: Mengenprodukt (oder Produktmengen) und Relationen

Das Mengenprodukt $A \times B$ ist die Menge aller geordneten Paare mit $a \in A$ und $b \in B$.

Jede Teilmenge eines Mengenproduktes heißt Relation!

Wieviele Elemente hat die Produktmenge? – Offensichtlich soviele, wie es Möglichkeiten gibt, die 1. Position zu besetzen mal der Anzahl der Möglichkeiten für die zweite Position:

$$N_{A \times B} = N_A \cdot N_B$$

Daher auch der Name "Produktmenge".

Eine wichtige Produktmenge ist $\mathbf{R} \times \mathbf{R}$, die Menge der reellen Zahlen \mathbf{R} mit sich selbst gekreuzt. Sie bildet den Definitionsbereich der reellen Funktionen mit 2 Veränderlichen (s. Kap. 7 in Mathe 2)

$$T: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R}$$

$$T(x, y) \in \mathbf{R}$$

Zuordnung von Mengen, Abbildungen:

Beispiel: $A = \{a,b,c,d\}$ Menge der Lieferanten der Firma Muster.
 $B = \{u,v,w,x,y,z\}$ Menge der Zukaufprodukte der Firma Muster

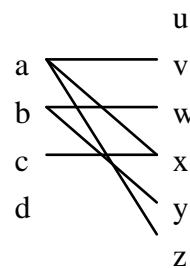
Jedem Lieferanten werden die Zukaufprodukte zugeordnet, die durch ihn bedient werden. Möglichkeiten:

a) $\{ (a,v), (a,x), (a,z), (b,w), (b,y), (c,x) \}$

b)

A	B
	u
a	v,x,z
b	w,y
c	x
d	

c)



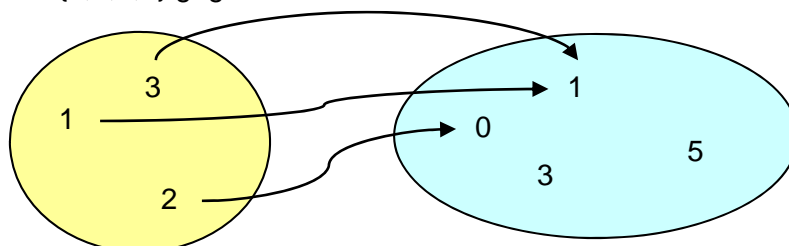
d)

Lieferant	Edukt
a	v
a	x
a	z
b	w
USW....	...

Bem.: Der Begriff Relation hat im Zusammenhang mit der Datenbanktechnik als relationales Datenmodell, bzw. relationale Datenbank in der Informatik spezielle Bedeutung erlangt. Relationen werden durch Tabellen dargestellt. Eine Zeile einer Tabelle bezeichnet man als Tupel.

Def D 1-10: Abbildung (Funktion)
 D und B seien Mengen. Eine **Abbildung von D in B, $f: D \rightarrow B$** ist eine Relation, die jedem $x \in D$ (**Definitionsbereich**) eindeutig ein $y \in B$ (**Bildbereich**) zuordnet. Die Teilmenge W von B aller $y \in B$, zu denen es ein $x \in D$ mit $y=f(x)$ gibt, heisst **Wertebereich W** von f.

Beispiel: Durch die Funktionsvorschrift $f: D \rightarrow B$ mit $y = f(x) = (2-x)^2$ ist eine Abbildung von $D=\{1,2,3\}$ nach $B=\{0,1,3,5\}$ gegeben:



Beachte: Nicht jedes $y \in B$ hat ein Urbild x (z.B. 3, 5), der Wertebereich ist $\{0, 1\} \subset B$.
 Es können aber mehrere x auf das gleiche y verweisen, im Beispiel $y=1$.

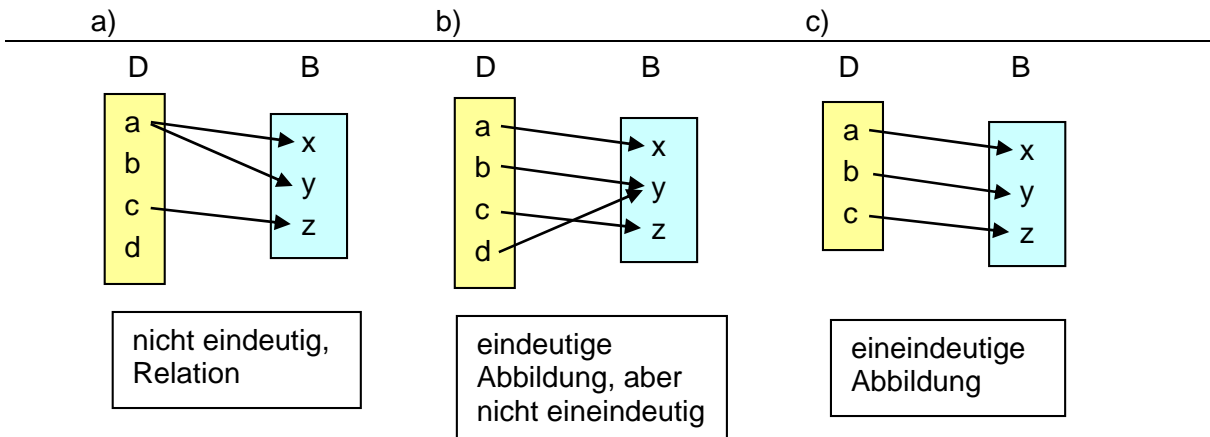
Andere Namen:

Urbildmenge = Definitionsbereich

Bildmenge = Wertebereich

Eineindeutige Abbildungen: Jedes Urbild hat genau ein Bild und jedes Bild genau ein Urbild.

Verschiedene Beispiele:



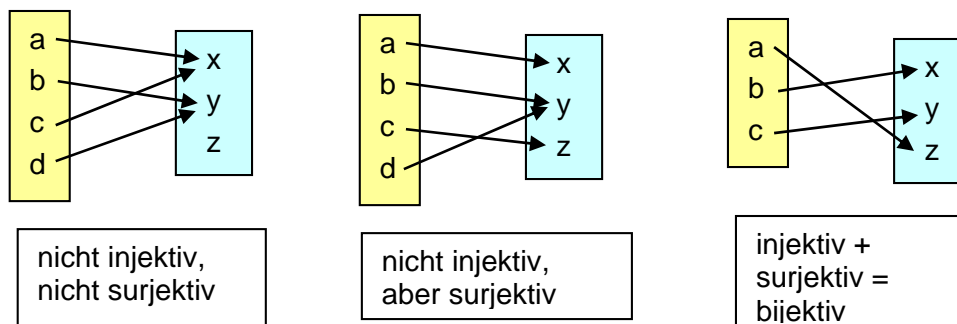
Eine andere geläufige Klassifizierung von Abbildungen ist die folgende:

- **injektive Abbildung:** jedes Bild hat genau ein Urbild (jedes $y \in B$ wird höchstens einmal getroffen, jedes $y \in W$ genau einmal)
- **surjektive Abbildung:** jedes Element des Bildbereiches B ist Bild, Wertebereich $W=B$ (jedes $y \in B$ wird getroffen)
- **bijektive Abbildung:** sowohl injektiv als auch surjektiv (bijektiv=eineindeutig)

Im obigen Bild ist die Abb. c) injektiv und die Abb. b) und c) sind surjektiv.

Was ist mit a)? – Hier hat zwar jedes Bild genau ein Urbild, aber a) ist keine Abbildung, daher auch keine injektive Abbildung.

Weitere Beispiele, die allesamt Abbildungen sind:



1.5 *Where to go from here*

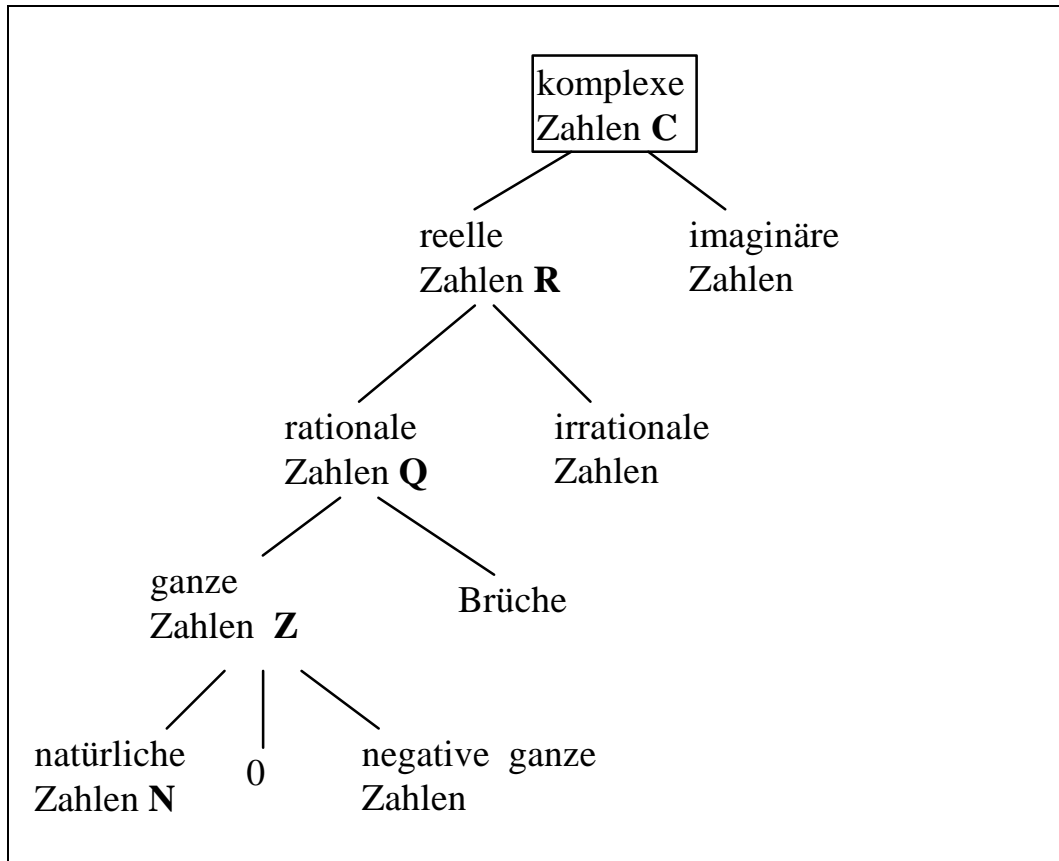
- Kurze Einführung in Prädikatenlogik: [Hartmann04, S. 36-39]
- Test von Programmen auf Korrektheit: [Hartmann04, S. 40-42]
- [Prädikatenlogik bei de.wikipedia.org](#): hier auch weitere Links
- [Semantic Web bei de.wikipedia.org](#)

2 Zahlssysteme

"Nicht alles, was gezählt werden kann, zählt, und nicht alles, was zählt, kann gezählt werden."

[Albert Einstein, Physiker, 1879-1955]

Wir unterscheiden die folgenden Zahlenbereiche:



2.1 Natürliche Zahlen

-- dieses Kapitel im Selbststudium --

Ursprünglich entstanden die natürlichen Zahlen, um die Mächtigkeit von Mengen zu bewerten ("Diese Schafherde hat 25 Tiere."). Wir führen die natürlichen Zahlen an dieser Stelle im Dezimalsystem ein. Sie können jedoch auch unabhängig von der speziellen Wahl einer Zahlendarstellung definiert werden.

Def D 2-1:

Menge der natürlichen Zahlen $\mathbf{N} = \{1,2,3,\dots\}$
 $\mathbf{N}_0 = \{0,1,2,3,\dots\}$

Die Addition hat dann den Zweck, die Elementzahl s der Vereinigungsmenge S der beiden elementfremden (!) endlichen Mengen A und B mit den Elementzahlen a und b anzugeben:

Def D 2-2: Addition natürlicher Zahlen

$$S = A \cup B \quad \wedge \quad A \cap B = \emptyset$$

$$|S| = |A| + |B| \quad \text{oder} \quad s = a + b$$

Diese Definition hängt nicht an einer speziellen Zahlendarstellung. Für die Addition natürlicher Zahlen gelten die bekannten **Grundgesetze der Addition**:

1. Die Addition ist unbeschränkt ausführbar, d.h. zu je zwei Zahlen a und b gibt es stets ein c mit

$$c = a + b.$$

2. Die Summe ist eindeutig bestimmt:

$$a = a' \quad \wedge \quad b = b' \quad \Rightarrow \quad a + b = a' + b'$$

Das bedeutet: "Ich darf auf beiden Seiten einer Gleichung das Gleiche tun"

3. Assoziativgesetz:

$$a + (b + c) = (a + b) + c$$

Das Assoziativgesetz ist nicht so selbstverständlich, wie man vielleicht meint. Bei anderen Operationen gilt es nicht unbedingt. Beispiel: $5^{(3^2)} \neq (5^3)^2$

4. Kommutativgesetz:

$$a + b = b + a$$

(kommutativ: vertauschbar). Es gibt auch Verknüpfungen mathematischer Objekte, für die das Kommutativgesetz nicht gilt (Subtraktion, Division u.a.m.)

Die Menge der natürlichen Zahlen ist geordnet. D.h. es gibt eine Vergleichsoperation \leq , genannt "kleiner-gleich", so dass für je zwei Zahlen a, b mindestens eine der Beziehungen $a \leq b$ oder $b \leq a$ gilt. Die Vergleichsoperation ist durch die folgenden Eigenschaften definiert:

Def D 2-3: kleiner-gleich

Für \leq gilt:

$$\begin{aligned} a &\leq a && \text{"reflexiv"} \\ a &\leq b \wedge b \leq a \Rightarrow a = b && \text{"antisymmetrisch"} \\ a &\leq b \wedge b \leq c \Rightarrow a \leq c && \text{"transitiv"} \end{aligned}$$

Die Addition erfüllt in Zusammenhang mit der Vergleichsoperation ein Monotoniegesetz:

5. Monotoniegesetz: $a \leq b \Rightarrow a + c \leq b + c$

Weiter gilt noch: $a + 0 = a$

Die Subtraktion führt man nun ein, indem man sie auf die Addition zurückführt.

Def D 2-4 Subtraktion

Die Differenz $d = a - b$ ist die Zahl, die zu b addiert a ergibt.

Die Rechenregeln für die Subtraktion folgen aus denen der Addition. Subtraktion ist in den natürlichen Zahlen nicht unbeschränkt ausführbar, denn in \mathbf{N}_0 muß $b \leq a$ sein.

Die Multiplikation kann frei von jeder speziellen Zahlendarstellung mit Hilfe des Mengenprodukts definiert werden. Wir hatten ja bereits gesehen, daß das Mengenprodukt gerade die Anzahl von Elementen besitzt, die dem Produkt der Elementzahlen der Einzelmengen entspricht. Man mache sich klar, daß die Multiplikation gerade die entsprechende Zahl von Zuordnungsmöglichkeiten beschreibt.

Def D 2-5: Multiplikation

Die Elementzahl p des Mengenprodukts P der beiden endlichen Mengen A und B mit den Elementzahlen a und b heißt Produkt der Zahlen a und b und wird durch $a \cdot b$ oder kurz ab bezeichnet:

$$\begin{aligned} P &= A \times B \\ |P| &= |A| \cdot |B| \quad \text{oder} \quad p = a \cdot b \end{aligned}$$

Rechenregeln der Multiplikation:

1. Die Multiplikation ist unbeschränkt ausführbar. Zu zwei Zahlen a und b gibt es stets ein c mit

$$c = a \cdot b.$$

2. Das Produkt ist eindeutig bestimmt:

$$a = a' \wedge b = b' \Rightarrow a \cdot b = a' \cdot b'$$

3. Assoziativgesetz:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

4. Kommutativgesetz:

$$a \cdot b = b \cdot a$$

5. **Distributivgesetz:** (Ausmultiplizieren oder Ausklammern)

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$a \cdot (b - c) = a \cdot b - a \cdot c$$

6. Monotoniegesetze:

$$a \leq b, c > 0 \Rightarrow a \cdot c \leq b \cdot c$$

$$a < b, c > 0 \Rightarrow a \cdot c < b \cdot c$$

Dabei wird der Ausdruck $a > b$ wie folgt definiert: $a > b \Leftrightarrow b \leq a \wedge b \neq a$

Aus dem Distributivgesetz folgt:

7. $a \cdot 0 = 0$

Bew: $a \cdot 0 = a \cdot (b - b) = a \cdot b - a \cdot b = 0$

Die Division läßt sich nun analog zur Subtraktion einführen:

Def D 2-6: Division

Der Quotient $c = a : b$ (bzw a/b) ist die Zahl, die mit b multipliziert a ergibt, d.h. für die $b \cdot c = a$ gilt.

Die Rechenregeln für die Division folgen aus denen der Multiplikation. Wie die Subtraktion ist die Division in den natürlichen Zahlen nicht unbeschränkt ausführbar. Aus diesem Grund werden die natürlichen Zahlen entsprechend erweitert.

2.2 Ganze und rationale Zahlen

-- dieses Kapitel im Selbststudium --

Bei der Lösung von Gleichungen in den natürlichen Zahlen tritt das Problem auf, daß die für die Lösung benötigten Operationen Subtraktion und Division nicht unbeschränkt ausführbar

sind. Wenn wir den Zahlenbereich entsprechend erweitern, kommen wir zu den ganzen und den rationalen Zahlen.

Für die Subtraktion werden die Zahlen $0 - n =: -n$ für $n \in \mathbf{N}$ hinzugefügt. Dies liefert die ganzen Zahlen:

Def D 2-7: Ganze Zahlen

Der Bereich \mathbf{Z} der ganzen Zahlen wird von den Zahlen $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$ gebildet.

Satz S 2-1: Rechenregeln für ganze Zahlen:

1. $a + (-a) = 0$ (-a ist nach Definition die Zahl, die zu a addiert 0 ergibt.)
2. $-(-a) = a$ (mit 1.)
3. $a + (-b) = a - b$
4. $a - (-b) = a + b$
5. $-(a + b) = -a - b$
6. $-(a - b) = -a + b$
7. $a \cdot (-b) = -ab$
8. $(-a) \cdot (-b) = ab$
9. $a < b \wedge c < 0 \Rightarrow ac > bc$

Def D 2-8: Rationale Zahlen

Eine Zahl heißt rational, wenn sie sich als Bruch $\frac{g}{h}$ (bzw. g/h) zweier ganzer Zahlen g und h schreiben lässt, wobei h ungleich 0 ist. Dabei ist g/h die Zahl, die mit h multipliziert g ergibt, d.h. $(g/h) \cdot h = g$. Die Menge der rationalen Zahlen wird mit \mathbf{Q} bezeichnet.

Satz S 2-2: Zusätzliche Rechenregeln für rationale Zahlen

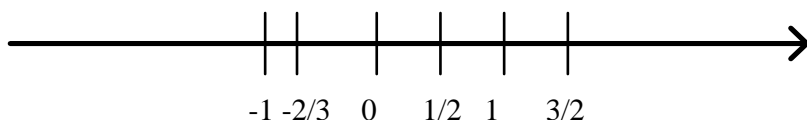
1. $g/h = g'/h' \Leftrightarrow gh' = g'h$
2. $\frac{g}{h} \cdot \frac{k}{l} = \frac{g \cdot k}{h \cdot l}$ (gemeinsamer Bruchstrich)
3. $\frac{g}{h} : \frac{k}{l} = \frac{\left(\frac{g}{h}\right)}{\left(\frac{k}{l}\right)} = \frac{\frac{g}{h}}{\frac{k}{l}} = \frac{g}{h} \cdot \frac{l}{k}$ (mit Kehrwert multiplizieren)

$$4. \quad \frac{g}{h} \pm \frac{k}{h} = \frac{g \pm k}{h}$$

(auf Hauptnenner bringen)

Also sind die vier Grundrechenarten bis auf die Division durch Null unbeschränkt ausführbar. Ein Zahlenbereich mit dieser Eigenschaft heißt **Körper** (hier also Körper der rationalen Zahlen **Q**). **Q** ist der kleinste Zahlenkörper, der die natürlichen Zahlen enthält. Dennoch sind die Mächtigkeiten von rationalen und natürlichen Zahlen gleich.

Die rationalen Zahlen lassen sich als Punkte auf dem Zahlenstrahl darstellen:



Frage: Ist jeder Punkt des Zahlenstrahls eine rationale Zahl ?

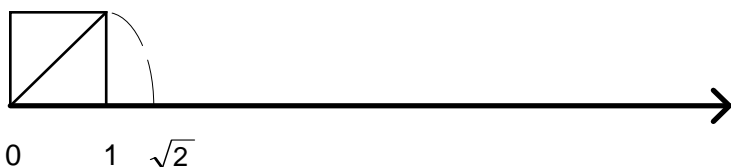
2.3 Reelle Zahlen

Frage: Welche rationale Zahl ergibt mit sich selbst multipliziert den Wert 2, d.h. für welche p und q ($p, q \in \mathbf{Z}$, $q \neq 0$) ist $\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = 2$? Anders ausgedrückt: **Ist $\sqrt{2}$ eine rationale Zahl?**

Behauptung: Es gibt keine rationale Zahl, deren Quadrat gleich 2 ist. Die Zahl 2 hat keine rationale Wurzel.

Beweis in Vorlesung

Eine Zahl, deren Quadrat gleich 2 ist (d.h. $\sqrt{2}$) lässt sich jedoch auf dem Zahlenstrahl mit Zirkel und Lineal konstruieren.



Die Diagonale im Einheitskreis hat nach dem Satz von Pythagoras die Länge $\sqrt{2}$. Also gibt es Punkte auf dem Zahlenstrahl, die keiner rationalen Zahl entsprechen. Diese Zahlen werden als nicht rationale (bzw. irrationale), reelle Zahlen bezeichnet. Bevor wir die reellen Zahlen definieren können, benötigen wir hier noch den Begriff der Zahlenfolge, auf den später noch genauer eingegangen wird.

Def D 2-9: Zahlenfolgen

Unter einer (unendlichen) Zahlenfolge versteht man eine eindeutige Abbildung der Menge \mathbf{N} der natürlichen Zahlen auf einen Zahlenbereich.

Beispiel:

1)

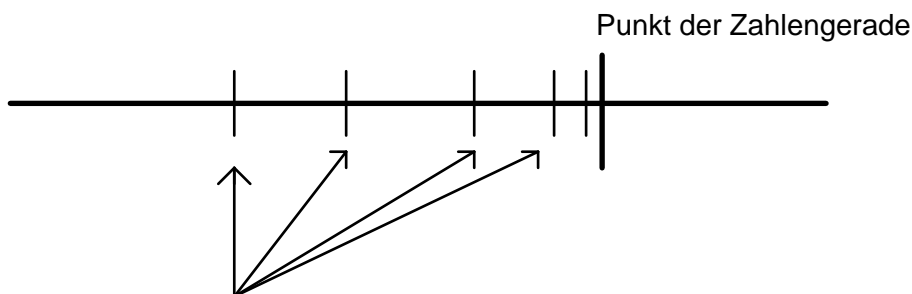
N	1	2	3	4	5	6	7	...	n	Grenzwert
A	1/2	2/3	3/4	4/5	5/6	6/7	7/8		$n/(n+1)$	$\rightarrow 1$

In Beispiel 1) ist jedes Element der Folge eine Zahl < 1 , der Grenzwert 1 dagegen nicht (der Begriff des Grenzwerts wird später in Kapitel 3.2 über Folgen genauer erklärt). Die Zahl 1 läßt sich beliebig genau durch Folgenglieder $n/(n+1)$ annähern.

2)

N	1	2	3	4	5	6	...	
A	1	1.4	1.41	1.414	1.4142	1.41421	...	ist kleiner als $\sqrt{2}$
B	2	1.5	1.42	1.415	1.4143	1.41423	...	ist größer als $\sqrt{2}$

Beispiel 2) ist nach dem Schema der **Intervallschachtelung** aufgebaut: Ergänze jeweils die nächste Dezimale, so daß die neue Zahl zum Quadrat gerade noch kleiner als 2 ist (A) bzw. gerade noch größer als 2 ist (B). Jedes Element der Folge ist dann eine rationale Zahl, der Grenzwert $\sqrt{2}$ dagegen nicht. Aber $\sqrt{2}$ läßt sich beliebig genau durch rationale Zahlen annähern. $\sqrt{2}$ ergibt sich als unendlicher Dezimalbruch, d.h. als Dezimalzahl mit unendlich vielen Nachkommastellen. Auf diese Weise lassen sich alle reellen Zahlen darstellen:



Folge rationaler Zahlen, bei denen jeweils eine Dezimale angefügt wird.

Def D 2-10: Reelle Zahlen


Eine Zahl heißt reell, wenn sie als **unendlicher Dezimalbruch** geschrieben werden kann. Die Menge der reellen Zahlen wird mit **R** bezeichnet. Die Rechenregeln für rationale Zahlen gelten auch für reelle Zahlen (**Permanenzprinzip**).

Satz S 2-3:

Jede rationale Zahl lässt sich als periodischer Dezimalbruch schreiben und jeder periodische Dezimalbruch ist eine rationale Zahl.

(Bem.: auch ein endlicher Dezimalbruch ist periodisch: $1.32 = 1.32\bar{0}$)

Zur Erläuterung betrachten wir die Zahl

$$x = 1.\overline{32438}$$


Wir multiplizieren x zuerst so, dass der Dezimalpunkt hinter die Periode wandert (hier: mit 100 000, **blauer Pfeil**), und dann so, dass der Dezimalpunkt direkt vor der Periode landet (hier: mit 100, **roter Pfeil**). Nun subtrahieren wir beide Gleichungen voneinander:

$$\left. \begin{array}{r} 100000x = 132438\overline{438} \\ 100x = 132.\overline{438} \end{array} \right\} -$$

Beim Subtrahieren fällt die Periode heraus und wir erhalten

$$99900 x = 132306$$

$$\Leftrightarrow x = \frac{132306}{99900}$$

Satz S 2-4:

Die reellen Zahlen sind eineindeutig den Punkten der Zahlengeraden zugeordnet. Sie bilden ein "Kontinuum" (keine Lücken).

Bem. Den komplexen Zahlen wollen wir uns später zuwenden!

2.3.1 Schreibweisen für Zahlmengen und Intervalle

Intervall-Schreibweise	Mengen-Schreibweise	Beschreibung ("{ } " = "Menge aller ...", " " = "... für die gilt: ...")
(ex. nicht)	$\{x \in \mathbf{N} \mid x \text{ ist gerade}\} = \{2,4,6,8,\dots\}$	Menge aller x aus den natürlichen Zahlen, für die gilt: x ist gerade
[2,7]	$\{x \in \mathbf{R} \mid 2 \leq x \leq 7\}$	abgeschlossenes Intervall aller reellen Zahlen zwischen 2 und 7
]3,a[oder (3,a)	$\{x \in \mathbf{R} \mid 3 < x < a\}$	offenes Intervall aller reellen Zahlen zwischen 3 und a
[3,a[oder [3,a)	$\{x \in \mathbf{R} \mid 3 \leq x < a\}$	halboffenes Intervall aller reellen Zahlen zwischen 3 (inklusive) und a (exklusive)
$(-\infty,5]$	$\{x \in \mathbf{R} \mid x \leq 5\}$	halboffenes Intervall aller reellen Zahlen kleiner-gleich 5
	$\{x \in \mathbf{R} \mid c < x < -5\}$	
(-10, -8]		
		offenes Intervall aller reellen Zahlen zwischen 0 und 5
		alle positiven reellen Zahlen



Übung: Füllen Sie die Lücken in obiger Tabelle aus!

Bem.:

- Bei Intervallen sind immer implizit die reellen Zahlen gemeint.
- Will man "bis ins Unendliche" alle Zahlen mitnehmen, so benutzt man ∞ (die "liegende Acht") als Zeichen für "Unendlich"
- Runde Klammer und eckige Klammer "falschherum" sind gleichberechtigte Schreibweisen für offene Intervallseiten: $]3,a[$ ist gleich $(3,a)$.

2.4 Potenzen, Wurzeln und Logarithmen reeller Zahlen

-- dieses Kapitel im Selbststudium (Vorkurswissen) --

Im Folgenden sind Zahlen, wenn nichts anderes angegeben, immer aus \mathbf{R} .

Für natürlichen Exponenten definiert man

Def D 2-11: Potenz
 Für $a \in \mathbf{R}$ und $n \in \mathbf{N}$ ist die n-te Potenz von a (gelesen a hoch n) definiert durch:

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n\text{-mal Faktor } a}$$

a heißt **Basis**, n **Exponent**.

Dies erweitern wir zunächst auf ganze Zahlen:

Def D 2-12:
 $a \neq 0, n \in \mathbf{N}: a^{-n} := \frac{1}{a^n},$

$$a^0 := 1$$

Die Definition ist sinnvoll wegen $\frac{a^n}{a^m} = \frac{\overbrace{a \cdot a \cdot \dots \cdot a}^n}{\underbrace{a \cdot a \cdot \dots \cdot a}_m} = a^{n-m}$. Setzt man $n=m$, so folgt $a^0 = 1$.

Def D 2-13: n-te Wurzel

$$a > 0, n \in \mathbb{N} : w = \sqrt[n]{a} \Leftrightarrow w^n = a$$

$w = \sqrt[n]{a} = a^{1/n}$ ist diejenige positive Zahl, für die gilt: $w^n = a$.

Bemerkung: 1) a heißt Radikand

2) Für $\sqrt[2]{a}$ wird \sqrt{a} geschrieben.

3) Die Schreibweise $w = a^{1/n}$ ist sinnvoll, denn mit den üblichen

Rechenregeln für Potenzen (s.u. Nr. 5) ist dann: $(a^{1/n})^n = a^{\frac{1}{n}n} = a^1 = a$

Mit diesen beiden Definitionen können wir nun rationale Exponenten von positiven reellen Zahlen definieren:

Def D 2-14: rationaler Exponent

$$a > 0, m \in \mathbb{Z}, n \in \mathbb{N} : a^{\frac{m}{n}} := \sqrt[n]{a^m}$$

Wir benötigen auch reelle Exponenten reeller Zahlen, z.B. $\sqrt{2}^{\sqrt{2}}$. $\sqrt{2}$ wird angenähert durch eine Folge rationaler Zahlen:

$a_1 = 1$	$a_1^{a_1} = 1$
$a_2 = 1.4$	$a_2^{a_2} = 1.60169\dots$
$a_3 = 1.41$	$a_3^{a_3} = 1.620169\dots$
$a_4 = 1.414$	$a_4^{a_4} = 1.63206\dots$
$a_5 = 1.4142$	$a_5^{a_5} = 1.63249\dots$
$a_{13} = 1.4142135623$	$a_{13}^{a_{13}} = 1.632526919438\dots$

Offensichtlich nähert sich diese Folge einem Grenzwert an, der dann den Wert $\sqrt{2}^{\sqrt{2}}$ repräsentiert. Dieses Vorgehen führt allgemein zur Definition reeller Potenzen:

Def D 2-15: reeller Exponent

Für $a > 0$, b reelle Zahlen, wird a^b erklärt als Grenzwert, der sich ergibt, wenn für a und b immer bessere Näherungen durch rationale Zahlen eingesetzt werden.

Satz S 2-5 Rechengesetze für Potenzen ($a, b > 0$)

$$1. a^s \cdot a^t = a^{s+t}$$

$$2. a^s / a^t = a^{s-t} \quad \text{Spezialfall: } \left(\frac{1}{a}\right)^t = \frac{1}{a^t} = a^{-t}$$

$$3. a^s b^s = (ab)^s$$

$$4. a^s / b^s = (a/b)^s$$

$$5. (a^s)^t = a^{st}$$

Vorsicht: es ist i.a. $a^{(s^t)} \neq (a^s)^t$

Satz S 2-6 Rechengesetze für Wurzeln ($a, b > 0$)

$$1. \sqrt[n]{a} \sqrt[n]{b} = \sqrt[n]{ab}$$

$$2. \sqrt[n]{a} / \sqrt[n]{b} = \sqrt[n]{a/b}$$

$$3. \sqrt[n]{a^t} = \sqrt[n]{a^t}$$

$$4. \sqrt[m]{\sqrt[n]{a}} = \sqrt{mn}{a}$$

Bew.: folgt direkt aus den Rechenregeln für Potenzen, wenn man die Identität $\sqrt[n]{a} = a^{1/n}$ benutzt.

Wozu braucht man n-te Wurzeln beliebiger reeller Zahlen und Logarithmen? Dazu Beispiele und Übungen in Vorlesung ausführlich:

1. Klavier: wohltemperierte Stimmung
2. Autobatterie

Übung: Wo liegt der Fehler im nachfolgenden "Beweis", dass $-8 = +8$ ist?

$$-8 = (-2)^3 = (-2)^{\frac{6}{2}} = \left((-2)^6\right)^{\frac{1}{2}} = 64^{\frac{1}{2}} = +8$$



Nachdem wir nun allgemeine Potenzen erklärt haben, können wir entsprechend dem Vorgehen bei der Einführung der Subtraktion bzw. Division den Logarithmus definieren:

Def D 2-16: Logarithmus

Für $a, b > 0, b \neq 1$ ist der Logarithmus definiert durch:

$$c = \log_b a \Leftrightarrow b^c = a$$

$c = \log_b a$ ist diejenige positive Zahl, für die gilt $b^c = a$

c heißt Logarithmus a zur Basis b . Für den Logarithmus zur Basis 10 (dekadischer Logarithmus) wird anstelle von $\log_{10} a$ auch **lga** geschrieben.

Weitere gängige Abkürzungen:

- natürlicher Logarithmus: $\ln a$ für $\log_e a$ (e = Eulersche Zahl, s. Kap. 4)
- Logarithmus dualis: $\text{ld } a$ für $\log_2 a$ (Basis 2, kommt in der Informatik häufig vor)

Satz S 2-7 Rechengesetze für Logarithmen

($a, b, c, u, v > 0$)

1. (i) $\log_b b^c = c$ und (ii) $a = b^{\log_b a}$

2. $\log_b (uv) = \log_b u + \log_b v$

3. $\log_b \frac{u}{v} = \log_b u - \log_b v$

4. $\log_b (u^t) = t \log_b u$

5. $\log_b \sqrt[n]{u} = \frac{1}{n} \log_b u$

6. $\log_b u = \frac{\log_a u}{\log_a b}$

7. $a = c \Leftrightarrow \log_b a = \log_b c$

Beweis für 1. und 6. in Vorlesung!

Regel 1 heißt: "b hoch" und "log_b" heben sich weg, wenn sie hintereinander ausgeführt werden.

Spezialfall $c=1$ für Regel 1(i): $\log_b b = 1$ (gilt für **jede** Basis b !).

Spezialfall $c=0$ für Regel 1(i): $\log_b 1 = 0$ (gilt für **jede** Basis b !).

Nr. 6. braucht man immer dann, wenn \log_b nicht auf dem Taschenrechner ist, und man deshalb als Ersatz auf \log_a zurückführt (z.B. $\log_a = \ln$ oder $\log_a = \lg$)

Beispiele:

$$1.) \left(\sqrt{2}^{\sqrt{2}} \right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^{\sqrt{2 \cdot 2}} = \sqrt{2}^2 = 2$$

2.) Berechne ohne und mit Taschenrechner!

$$\text{ohne: } \log_{\sqrt{2}} \frac{1}{2} = \log_{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \right)^2 = \log_{\sqrt{2}} (\sqrt{2})^{-2} \stackrel{\text{Regel 1a}}{=} -2$$

$$\text{mit: } \log_{\sqrt{2}} \frac{1}{2} = \log_{\sqrt{2}} 0.5 \stackrel{\text{Regel 6}}{=} \frac{\ln 0.5}{\ln \sqrt{2}} = -2$$



zur Übung: Berechnen Sie $\log_{\sqrt[3]{3}}(27)$ ohne und mit Taschenrechner

Für den exponentiellen Zerfall gilt das Gesetz:

$$\text{Ladezustand (Konzentration) } L(w) = \left(\frac{1}{2} \right)^{w/T_{\text{halb}}}$$

T_{halb} ist die **Halbwertszeit**. Haben wir also zum Zeitpunkt 0 von einer Menge (Anzahl Ladungsträger in Autobatterie, Konzentration radioaktiver Teilchen in Präparat) 100% = 1.0, so ist zum Zeitpunkt w davon noch $L(w)$ da, z.B. gilt bei $w = T_{\text{halb}}$, dass $L(w) = 50\% = 0.5$ ist.

Damit können Sie nachfolgende Aufgaben lösen:



Aufgabe Autobatterie:

Eine Autobatterie entlädt sich, wenn sie nicht gefahren wird. Nehmen wir an, die Halbwertszeit sei 1 Woche. Ist sie also heute voll geladen (100%), so hat sie nach einer Woche noch 50%, nach 2 Wochen noch 25% usw. Nehmen wir an, wir können das Auto noch starten, solange die Batterie mindestens 20% aufgeladen ist. Wieviele Wochen (als Dezimalzahl) dürfen wir dann längstens warten?

[Lösung: 2.322 Wochen]



Aufgabe Halbwertszeit ^{14}C :

In Lebewesen hat das Isotop ^{14}C eine bestimmte Konzentration K . Nach dem Tod dieser Lebewesen wird es durch radioaktiven Zerfall (exponentielles Zerfallsgesetz) abgebaut. Nach einer Halbwertszeit T ist von der ^{14}C -Anfangskonzentration noch $K/2$ übrig, nach $2T$ noch $K/4$ usw. Von einer Mumie sei bekannt, dass sie $s = 8130$ Jahre tot ist. Ihre aktuelle ^{14}C -Konzentration ist $0.35K$. Wie groß ist die Halbwertszeit von ^{14}C ?

[Lösung: 5367 Jahre]

2.4.1 Spezielle Funktionen

Einige spezielle Funktionen werden wir öfters brauchen

Def D 2-17 Spezielle Funktionen

Für $x \in \mathbf{R}$ definiert man

(1) **Betragsfunktion** $|x| = \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x < 0 \end{cases}$

(2) **Gauss-Klammer** $\lfloor x \rfloor = \text{floor}(x) =$ größte Ganzzahl kleiner x (Abrunden)
 $\lceil x \rceil = \text{ceil}(x) =$ kleinste Ganzzahl größer x (Aufrunden)

(3) **Sprungfunktion** $H(x) = \theta(x) = \begin{cases} 1 & \text{für } x > 0 \\ 0 & \text{für } x \leq 0 \end{cases}$ (Heaviside-Funktion)

(4) **Signumfunktion** $\text{sgn}(x) = \begin{cases} 1 & \text{für } x > 0 \\ 0 & \text{für } x = 0 \\ -1 & \text{für } x < 0 \end{cases}$ (Signum = "sign" = Vorzeichen)

2.5 Gleichungen und Ungleichungen

-- (Vorkurswissen) --

Das Auflösen von Gleichungen und Ungleichungen gehört zu den Voraussetzungen.

Wer sich hier unsicher fühlt, dem sei das Buch [Knorrenschild: *Vorkurs Mathematik*, S. 88ff] wärmstens empfohlen!

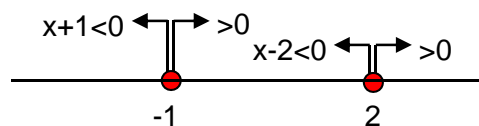
Hier wiederholen wir nur noch einmal kurz einige Besonderheiten:

Satz S 2-8:

Die Division durch Null ist in keinem Zahlenbereich möglich.

Betragsgleichungen: Wie löst man $|x + 1| = 2|x - 2|$?

1. Umschlagpunkte für alle N Beträge bestimmen
2. Skizze machen
3. N+1 Fallunterscheidungen: jeweils Gleichung lösen
4. Probe: Passt Lösung in Bereich?



Übung: Man löse $|x - 1| - 3|x + 3| = 1$

Nullstellen finden: Ein wichtiger Spezialfall beim Lösen von Gleichungen ist die Bestimmung von Nullstellen $f(x) = 0$

Strategie: Man versucht, f als Produkt mehrerer Terme zu schreiben (**Faktorenzerlegung**) und benutzt dann den folgenden Satz:

Satz S 2-9

$$a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$$

Beispiel: Es seien die Nullstellen des Ausdrucks $f(x) = x^2 - 2x$ zu bestimmen.

Das Distributivgesetz erlaubt die Umformung $f(x) = \underbrace{x}_a \cdot \underbrace{(x-2)}_b$ Nach Satz S 2-9

wird $f(x)=0$, falls $x=0$ oder $x-2=0$. Damit sind die zwei Nullstellen von $f(x)$ ermittelt.

WICHTIG: Man darf bei $x^2 - 2x = 0$ NICHT einfach durch x dividieren und sagen "Die Lösung ist $x - 2 = 0$, also $x = 2$, sondern muss beide Fälle betrachten!!

Übung: Lösen Sie durch Faktorenerlegung: Welche Nullstellen hat

(a) $x^2 - 25 = 0$ (b) $x \ln(x^2 + 1) + x^2 \ln(x^2 + 1) = 0$

(c) $x \ln x + x^2 \ln(x^2) = 0$?

log- und exp-Gleichungen:

1. möglichst alle Terme mit log und Variable x (bzw. exp und Variable x) zus.fassen
2. auf beiden Seiten "e hoch" (bzw. "log") (ist Äquivalenzumformung)
3. Probe, ob Lösungen im Def. bereich

Übung: Lösen Sie nach x auf!

(a) $e^x = 2e^{-x+2}$ (b) $\ln(x) + \ln(x+2) = 0$

Lösung erfolgt in den Übungen (Ergebnis: (a) $x = 1 + \ln(2)/2$, (b) $x = -1 + \sqrt{2}$).

Transzendente Gleichungen sind Gleichungen, in denen Logarithmus, e-Funktion oder Sinus, Cosinus usw. auftauchen. Viele dieser Gleichungen lassen sich nicht analytisch auflösen, insbesondere dann, wenn z.B. x sowohl isoliert als auch im \ln auftritt

$$x - 2 = 5 \ln(x)$$

Wir werden in Kap. 3.3 eine "quick-n-dirty"-Methode, die sog. **Fixpunkt-Iteration**, kennenlernen, mit der man sich in solchen Fällen eine Näherungslösung verschafft.

Weitere Themen werden in Übungen aufgefrischt:

Wurzelgleichungen**Ungleichungen**

Beim Durchmultiplizieren mit negativer Zahl dreht sich das Ungleichungszeichen.

Betragsungleichung: Wie löst man $|x+1| > 4$?

Umschlagspunkt Betrag ist $x=-1$. Fallunterscheidung

a) $x > -1$: $x+1 > 4 \Leftrightarrow x > 3$. Also: $x > -1 \wedge x > 3 \Rightarrow x > 3$

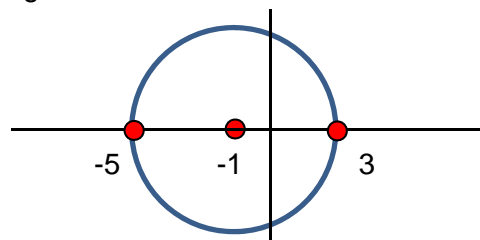
b) $x < -1$: $-(x+1) > 4 \Leftrightarrow x+1 < -4$ (Ungleichzeichen drehen!) $\Leftrightarrow x < -5$.

Also: $x < -1 \wedge x < -5 \Rightarrow x < -5$.

Insgesamt ist Lösungsmenge $L = \{x \in \mathbf{R} \mid x < -5 \vee x > 3\}$.

Man kann die Betragsungleichung auch sprachlich-geometrisch lösen: Schlägt man auf der Zahlengerade einen Kreis um Zentrum -1 (den Umschlagspunkt) mit Radius 4, so gehören alle Zahlen außerhalb (wg. „>“-Zeichen) zur Lösungsmenge. Dies führt wieder auf

$$\mathbf{L} = \{x \in \mathbf{R} \mid x < -5 \vee x > 3\}.$$



Quadratische Betragsungleichung: Es gilt die sehr nützliche Äquivalenz

$$a^2 > b^2 \Leftrightarrow |a| > |b|. \quad [\text{Knorrenschild, S. 97, 115}]$$

Beispiel: $(x + 1)^2 > 16 \Leftrightarrow |x + 1| > 4$

Weiter wie im Beispiel Betragsungleichung, dies führt wieder auf

$$\mathbf{L} = \{x \in \mathbf{R} \mid x < -5 \vee x > 3\}.$$

2.6 Modulare Arithmetik

Die modulare Arithmetik ist Grundlage der Kryptographie.

Def D2-18: Der **Rest von a** bei Division durch $m \in \mathbf{N}$ ist diejenige Zahl $r \in \{0, 1, \dots, m-1\}$, für die $a - r$ ein Vielfaches von m ist. Man schreibt:

$$r = a \bmod m$$

Wenn zwei ganze Zahlen a und b bei Division durch $m \in \mathbf{N}$ denselben Rest haben, also wenn $a - b$ ein Vielfaches von m ist, so schreibt man dafür

$$a = b \pmod{m}.$$

Man sagt auch, a und b gehören zur selben **Restklasse**.

In Worten: Die Terme a und b sind gleich, bis auf möglicherweise Vielfache von m . Die modulare Arithmetik rechnet nur mit ganzen Zahlen. Bei der Division treten keine Kommazahlen auf, sondern höchstens ein Rest:

$$2 \text{ dividiert durch } 5 = 0 \text{ Rest } 2$$

$$7 \text{ dividiert durch } 5 = 1 \text{ Rest } 2$$

$$\rightarrow 7 \text{ und } 2 \text{ haben den gleichen Rest bei Division } 5 \Leftrightarrow 7 = 2 \pmod{5}$$

Beispiel: Zum Teiler $m=5$ gibt es genau 5 Restklassen:

$\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$ Restklasse zu Rest 0

$\{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}$ Restklasse zu Rest 1

usw. Alle Zahlen innerhalb der gleichen Restklasse sind "(mod m)-gleich".

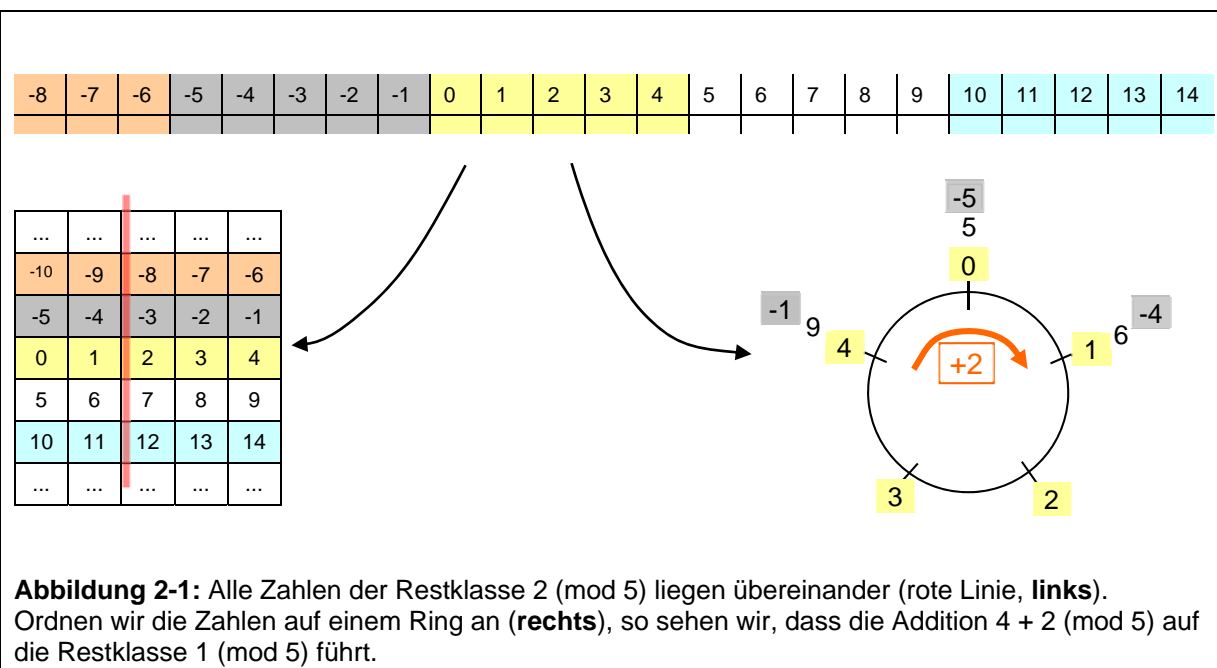


Abbildung 2-1: Alle Zahlen der Restklasse 2 (mod 5) liegen übereinander (rote Linie, links). Ordnen wir die Zahlen auf einem Ring an (rechts), so sehen wir, dass die Addition $4 + 2 \pmod{5}$ auf die Restklasse 1 (mod 5) führt.

Satz S 2-10 Wenn $a = b \pmod{m}$ und $c = d \pmod{m}$, dann folgt

$$\begin{aligned} a + c &= b + d \pmod{m} \\ ac &= bd \pmod{m} \end{aligned} \quad \text{und} \quad a^c = b^c \pmod{m}$$

Dieser Satz bedeutet: Wenn man die Restklasse eines größeren Terms ausrechnen will, kann man erst möglichst einfache Restklassenvertreter der einzelnen Operanden wählen

$$\begin{aligned} \text{Beispiel: } (117 \cdot 76 + 303) \pmod{5} &= \\ (2 \cdot 1 + 3) \pmod{5} &= 5 \pmod{5} = 0 \end{aligned}$$

Weiterhin bedeutet dieser Satz:

- Man darf auf beiden Seiten einer \pmod{m} -Gleichung eine beliebige ganze Zahl addieren oder mit ihr multiplizieren.

denn $a = b \pmod{m} \Leftrightarrow a + c = b + c \pmod{m}$.

- Man darf auf einer Seite ein beliebiges Vielfaches von m addieren

denn $a = a + 0 = a + d \cdot m \pmod{m}$.

Man beachte: "Kürzen" ist i.a. nicht erlaubt. D.h. aus $a \cdot c \equiv b \cdot c \pmod{m}$ folgt **NICHT**

$a \equiv b \pmod{m}$.

Beispiele in Vorlesung.

2.6.1 Prüfziffern

Wenn Sie bei einer ISBN (International **S**tandard **B**ook **N**umber) eine Ziffer falsch eingeben oder zwei Ziffern vertauschen, erkennt der Rechner in Buchhandlung das. Wie macht er das?

In jeder ISBN $a\text{-}bcd\text{-}efghi\text{-}p$ ist die letzte Ziffer p eine Prüfziffer, die wie folgt berechnet wird:

$$10a + 9b + 8c + 7d + 6e + 5f + 4g + 3h + 2i + p = 0 \pmod{11}$$

(Falls der Rest 10 auftritt, wird für p das Symbol X vereinbart.)

Beispiel: Welche Prüfziffer hat das Buch von S. Singh "Geheime Botschaften" (ein übrigens ausgezeichnetes, richtig spannendes Buch zu modularer Arithmetik und Kryptographie) mit ISBN 3-446-19873- p ?

Lösung in Vorlesung.

Warum bildet man nicht einfach nur die Summe $a + b + \dots + p = 0 \pmod{11}$? – Weil man auch "Zifferndreher" (Vertauschungsfehler) erkennen möchte. Jede Ziffer hat ein anderes Gewicht, beim Vertauschen kommt eine andere Prüfziffer heraus.

Übung: Rechnen Sie nach, dass die Singh-ISBN mit Zifferndreher 3-446-**91**873-3 **keine** gültige ISBN ist.

Übung(+): Alles kann die kleine Prüfziffer natürlich nicht erkennen: Wenn zusätzlich zum Zifferndreher gleichzeitig die 1. Ziffer falsch ist, kommt manchmal wieder eine (scheinbar) richtige ISBN heraus. Für welche x ist $x\text{-}446\text{-}91873\text{-}3$ eine gültige ISBN? Gibt es mehrere solcher x ?

2.7 Binomialkoeffizient und Summenzeichen

2.7.1 Rechnen mit Summen

Für InformatikerInnen: Summen sind eigentlich nichts anderes als spezielle for-Schleifen:

$s = \sum_{k=1}^{50} k^4$	\Leftrightarrow	<pre>s=0; for (k=1; k<=50; ++k) s = s + k*k*k*k;</pre>
---------------------------	-------------------	---

Satz S 2-11 Regeln für Summen

$$\sum_{k=1}^m (A_k \pm B_k) = \left(\sum_{k=1}^m A_k \right) \pm \left(\sum_{k=1}^m B_k \right)$$

Wenn Term a in der Summe konstant bzgl. k ist:

$$\sum_{k=U}^O a = S \cdot a$$

Hierbei ist $S = O - U + 1$ die Zahl der Summenterme („Schleifendurchläufe“).

Im Zweifelsfall kann man sich eine Summe immer klarmachen, indem man sie „ausschreibt“

$$\sum_{k=1}^m A_k = A_1 + A_2 + \dots + A_m$$

und macht sich damit sofort die Gleichungen aus Satz S 2-11 klar.

Aufgabe: (a) $\sum_{k=1}^{50} k^4 - \sum_{k=4}^{54} (k-2)^4 = ?$ (b) [als Übung] $\sum_{i=1}^{50} i(i-1) - \sum_{i=3}^{52} i(i+1) = ?$

Lösung über Ausschreiben der Summen:

$$\begin{aligned} & 1^4 + 2^4 + \dots + 50^4 \\ & - 2^4 - \dots - 50^4 - 51^4 - 52^4 \\ = & 1^4 - 51^4 - 52^4 = -14\,076\,816 \end{aligned}$$

Kontrolle in Maple: `sum(k^4, k=1..50) - sum((k-2)^4, k=4..54);` und `sum((i-1)*i, i=1..50) - sum(i*(i+1), i=3..52);`

Satz S 2-12 Doppelsummen

Bei endlichen Summen darf man Klammern auflösen und Reihenfolgen vertauschen:

$$\sum_{k=1}^m \left(\sum_{i=1}^n c_{ik} \right) = \sum_{k=1}^m \sum_{i=1}^n c_{ik} = \sum_{i=1}^n \sum_{k=1}^m c_{ik} = \sum_{i=1}^n \left(\sum_{k=1}^m c_{ik} \right)$$

Hängt ein Term nicht vom Summenindex ab, darf er vor die Summe gezogen werden (gilt auch für Einfachsummen):

$$\sum_{k=1}^m \sum_{i=1}^n (a \cdot c_{ik}) = \sum_{k=1}^m \left(a \sum_{i=1}^n c_{ik} \right) = a \cdot \sum_{k=1}^m \sum_{i=1}^n c_{ik}$$

Sonderfall separierbare Summen (Term in der Summe muss **PRODUKT** sein):

$$\sum_{k=1}^m \sum_{i=1}^n a_k \cdot b_i = \sum_{k=1}^m \left(a_k \cdot \sum_{i=1}^n b_i \right) = \left(\sum_{k=1}^m a_k \right) \cdot \left(\sum_{i=1}^n b_i \right)$$

von i
unabhängig
von k
unabhängig

Übung: Berechnen Sie

(a) $\sum_{k=1}^2 \sum_{i=1}^{10} k \cdot i$ (b) $\sum_{k=1}^3 \sum_{i=1}^4 ((k \cdot i)^2 + 5)$

2.7.2 Fakultät und Binomialkoeffizienten

Def D2-19: Für $n, k \in \mathbb{N}_0$ mit $k \leq n$ definiert man:

- die **Fakultät** $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$ für $n > 0$ sowie $0! = 1$
- den **Binomialkoeffizienten** $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k \cdot (k-1) \cdot \dots \cdot 2 \cdot 1}$

Die letzte Umformung gilt nur für $k > 0$. [Merkregel: Im Nenner genau k Terme, von k abwärts; im Zähler genau k Terme, aber von n abwärts.]

Folgerungen und Beispiele:

- $\binom{n}{0} = \binom{n}{n} = 1$ für alle n und $\binom{n}{k} = \binom{n}{n-k}$ (Symmetrie des Binomialkoeffizienten)
- Für kleine k und für k knapp unter n ist der Binomialkoeffizient auch für große n recht leicht zu berechnen, "in der Mitte" kann es aufwendiger werden:

$$\binom{100}{98} = \binom{100}{2} = \frac{100 \cdot 99}{2 \cdot 1} = 4950$$

$$\binom{20}{10} = 184756 \text{ (nur mit Taschenrechner! – oder Additionstheorem)}$$

Satz S2-13 Additionstheorem Binomialkoeffizienten: Für $n, k \in \mathbf{N}$ gilt:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Beweis in Vorlesung [\[durch Nachrechnen, auf HN bringen\]](#)

Auf dem Additionstheorem beruht das **Pascal'sche Dreieck** (s. Vorlesung)

2.7.3 Binomischer Satz

Stellen Sie sich vor, Sie müssen $(a + b)^7$ berechnen. Alles ausmultiplizieren? Ganz schön mühsam (2^7 Terme !) und außerdem höchst fehleranfällig. Wir lernen eine bessere Methode kennen:

Satz S2-14 (Binomischer Satz): Für $n \in \mathbf{N}$ und $a, b \in \mathbf{R}$ gilt:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

Beweis: kommt später im Kapitel Kombinatorik.

Beispiele:

- [gute alte Binomische Formel](#)

$$\bullet \quad (a + b)^3 = \binom{3}{0} a^0 b^3 + \binom{3}{1} a^1 b^2 + \binom{3}{2} a^2 b^1 + \binom{3}{3} a^3 b^0 = b^3 + 3ab^2 + 3a^2b + a^3$$

$$\bullet \quad (a - b)^3 = \binom{3}{0} a^0 (-b)^3 + \binom{3}{1} a^1 (-b)^2 + \binom{3}{2} a^2 (-b)^1 + \binom{3}{3} a^3 (-b)^0 = -b^3 + 3ab^2 - 3a^2b + a^3$$



Berechnen Sie $(a + b)^7$ über Binomischen Satz und Pascal'sches Dreieck.

2.8 Fazit

Die wichtigsten **Besonderheiten beim Rechnen mit reellen Zahlen:**

- Die Division durch Null ist in keinem Zahlbereich definiert.
- Eine Potenz der Form 0^0 ist nicht definiert.
- Wurzeln können in \mathbf{R} nur aus nichtnegativen Zahlen gezogen werden. Ergebnis nichtnegativ.
- Potenzgesetze mit nicht-ganzzahligem Exponenten gelten nur für positive Basis.
- Logarithmen können in \mathbf{R} nur von positiven Zahlen angegeben werden. Ergebnis reell.
- Logarithmen zur Basis 10 werden durch **lg**, zur Basis 2 durch **ld** und zur Basis **e** durch **ln** abgekürzt.
- In vielen Mathematikbüchern wird log oft ohne Basisangabe benutzt. Gemeint ist dann meist die Basis **e**, d.h. der natürliche Logarithmus. (Vorsicht: Manchmal ist auch die Basis 10 gemeint, also nachschauen)